Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards -
- 1st minute quiz – done
- Web Calendar summary – done
- Web book pages – done
- Commands –
- Howtos –
- Skills pacing -na
- Lab – done
- Depot (VMs) – restored

- RPM CD (telnet-server, vsftpd, xinetd, dhcp)
- Mike Brogan from Cruzio 6:30 – 7:00

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/


Joe A.

Joe P.

www.cccconfer.org
dial-in: 888-886-3951
passcode: 439080


John


Chris B.


Chuck

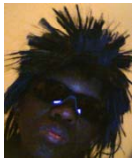

Rich


Josh

Robert


Casady

Chris H.


Lieven

Jesus


Jack

Edwin

Julio


Drew


Edgar

Kay


Ryan

Aaron


Joe B.

Junious

Brynden

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

Quiz

Please take out a blank piece of paper, switch off your monitor, close your books, put away your notes and answer these questions:

Dynamic Host Configuration

Objectives	Agenda
• Install and configure DHCP to assign reserved and dynamic IP addresses, a gateway, a DNS server, and a domain name to a client.	• Quiz • Questions on previous material • Review Test 1 answers • Housekeeping • FTP (more) • Cruzio – Mike Brogan • Firewalls and FTP • DHCP • DHCP Lab • Wrap

Questions on previous material

Questions?
- Previous lesson material
- Lab assignments

Test 1 walkthrough
- Answers posted on web site

Housekeeping

- Lab 5 due today!
- Spring break next week
  - DHCP Lab 6 is due in 2 weeks
  - Or do it tonight in class (after short lecture)
- Guest speaker at 6:30PM
- Extra credit opportunity using system pods in CIS Lab (no VMs, just real computers, switches and cables)
  - Original NIC lab (20 points)
    http://simms-teach.com/docs/cis192/original-lab-on-nics.pdf
  - Original routing lab (20 points)
    http://simms-teach.com/docs/cis192/original-lab-on-routing.pdf
  - Original port forwarding lab (20 points)
    http://simms-teach.com/docs/cis192/original-lab-on-port-forwarding.pdf
  - Original firewall lab (20 points)
    http://simms-teach.com/docs/cis192/original-lab-on-firewalls.pdf

FTP
(more)

vsftp

Step 10 *Additional security*

This is why root cannot login for ftp access

```
[root@legolas ~]# cat /etc/vsftpd/user_list
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@legolas ~]#
```

```
[root@legolas ~]# cat /etc/vsftpd/ftpusers
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
[root@legolas ~]#
```

FTP

Two sockets are used

- Commands (requests and responses)
- Data transfer

Active mode

- Server initiates new connection for data transfer
- Client firewall must allow incoming connection

Passive mode

- Client initiates new connection for data transfer
- Server firewall must allow incoming connection

FTP

Active mode

- Client sends PORT command to indicate port it will listen on
- Server initiates new connection to that port for data transfer

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,166,75

PORT 172, 30,4, 83, 166, 75
166 decimal = A6 hex
75 decimal = 4b hex
A64B hex = 42571 (decimal)

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
42571	20

FTP

Active mode

- Client sends PORT command to indicate port it will listen on
- Server initiates new connection for data transfer to that port

PORT command to listen on port 166, 75
166 decimal = A6 hex
75 decimal = 4b hex
A64B hex = 42571 (decimal)

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,166,75
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PAS
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Wi
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=1 Ack
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg
192.168.2.150	20	172.30.4.83	42571	FTP-DATA	FTP Data: 18 bytes
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [FIN, ACK] Seq=19 Ack=1 Win=5888 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [ACK] Se
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [FIN, AC
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=82 Ack=263 Win=5856 Len=0

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection

FTP

Passive mode

- Client send PASV request
- Server replies with port it will listen on
- Client initiates new connection to that port for data transfer

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PASV
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 227 Entering Passive Mode (192,168,2,150,200,83

Response 192, 168, 2, 150, 200, 83
200 decimal = C8 hex
83 decimal = 53 hex
C853 hex = 51283 (decimal)

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
41025	51283

FTP

Passive mode

- Client send PASV request
- Server replies with port it will listen on
- Client initiates new connection to that port for data transfer

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PASV
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 227 Entering Passive Mode (192,168,2,150,200,83
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=88 Ack=313 Win=5856 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [SYN] Seq=0 Win=
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [SYN, ACK] Seq=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg
192.168.2.150	51283	172.30.4.83	41025	FTP-DATA	FTP Data: 18 bytes
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [FIN, ACK] Seq=19 Ac
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 W
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=378
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [FIN, ACK] Seq=1 Ack
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=397 Win=5856 Len=0

Server to listen on 200, 83 = C853 = 51283

3 way handshake initiated by client

Retrieve legolas file

File transfer

4 way handshake to close connection

Example FTP Session

```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.04 secs (0.5 kB/s)
ftp> passive
Passive mode on.
ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,200,83)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (5.1 kB/s)
ftp> passive
Passive mode off.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (23.8 kB/s)
ftp> bye
221 Goodbye.
root@frodo:~#
```

Connect to server

Login

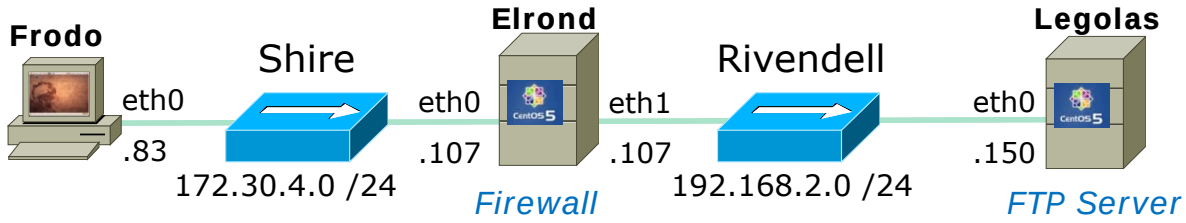
Initialize

*Get legolas file using **active** mode*

Get legolas file using passive mode

*Get legolas file using **active** mode*

End




```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
```

Frodo FTP's into Legolas

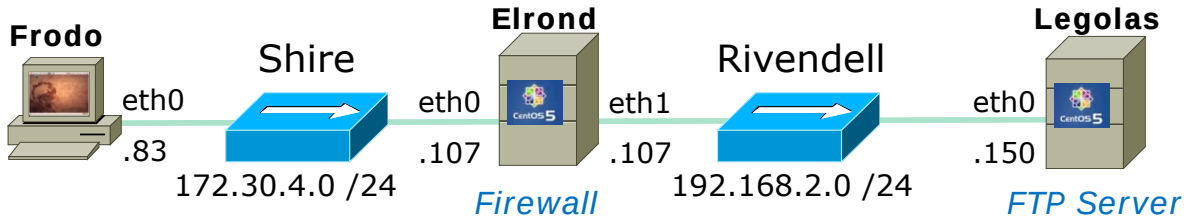
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [SYN] Seq=0 Win=58
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [SYN, ACK] Seq=0 A
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 220 (vsFTPd 2.0.5)
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=21 Win=5856 Len=0

3 way handshake initiated by client

- *3 way handshake*
- *New connection initiated by client*

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21




```
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
```

Note the login happens over the wire in clear "sniffable" text

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: USER cis192
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [ACK] Seq=21 Ack=14 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 331 Please specify the password.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=14 Ack=55 Win=5856 Len=0
Vmware_4e:21::		Vmware_7c:18:f5		ARP	Who has 192.168.2.150? Tell 192.168.2.107
Vmware_7c:18:'		Vmware_4e:21:a5		ARP	192.168.2.150 is at 00:0c:29:7c:18:f5
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PASS Cabrillo
192.168.2.150	52916	207.62.187.54	53	DNS	Standard query PTR 83.4.30.172.in-addr.arpa
207.62.187.54	53	192.168.2.150	52916	DNS	Standard query response, No such name
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [ACK] Seq=55 Ack=29 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 230 Login successful.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=29 Ack=78 Win=5856 Len=0

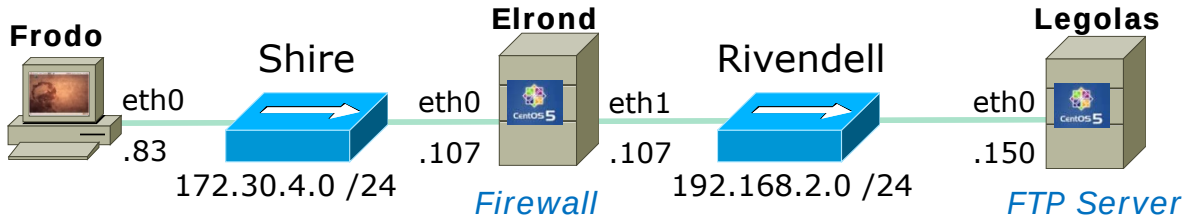
username

password

Login with username and password.
Note the reverse DNS lookup attempt by the FTP server

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21



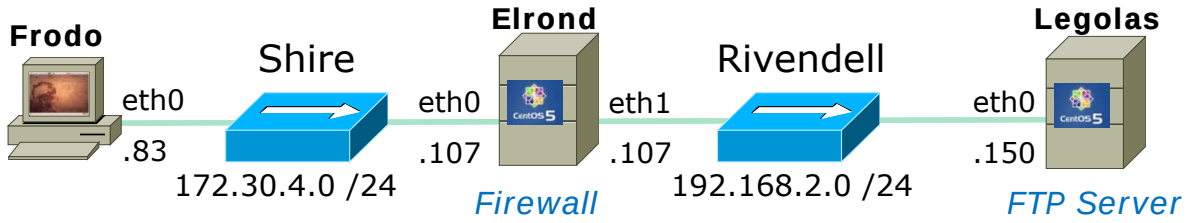

```
Remote system type is UNIX.
Using binary mode to transfer files.
```

- *Client requests system type and server replies UNIX.*
- *Client requests binary mode (Type I) transfers and server changes to binary mode*

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: SYST
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [ACK] Seq=78 Ack=35 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 215 UNIX Type: L8
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=35 Ack=97 Win=5856 Len=0
172.30.4.83	42855	192.168.2.150	21	FTP	Request: TYPE I
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 Switching to Binary mode.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=43 Ack=128 Win=5856 Len=0

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21



Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
42571	20

***Active Mode** is when server initiates new connection for data transfer*

```
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.04 secs (0.5 kB/s)
```

PORT command to listen on 166, 75 = A64B = 42571

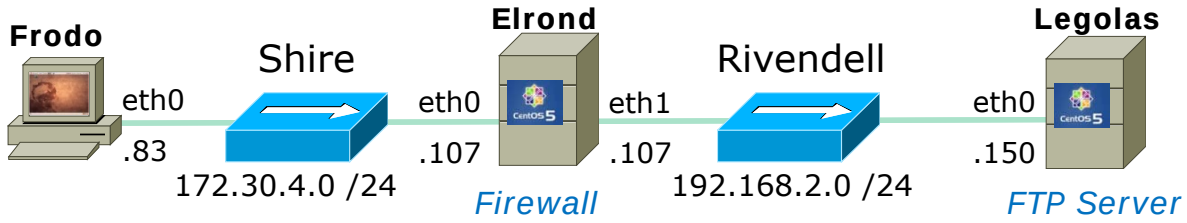
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,166,75
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PAS
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Wi
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=1 Ack=1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg
192.168.2.150	20	172.30.4.83	42571	FTP-DATA	FTP Data: 18 bytes
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [FIN, ACK] Seq=19 Ack=1 Win=5888 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [ACK] Se
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [FIN, AC
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=82 Ack=263 Win=5856 Len=0

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection



Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

***Passive Mode** is when client initiates new connection for data transfer*

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
41025	51283

```
ftp> passive
Passive mode on.
ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,200,83)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (5.1 kB/s)
```

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PASV
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 227 Entering Passive Mode (192,168,2,150,200,83
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=88 Ack=313 Win=5856 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [SYN] Seq=0 Win=
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [SYN, ACK] Seq=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg
192.168.2.150	51283	172.30.4.83	41025	FTP-DATA	FTP Data: 18 bytes
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [FIN, ACK] Seq=19 Ac
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 W
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=378
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [FIN, ACK] Seq=1 Ack
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=397 Win=5856 Len=0

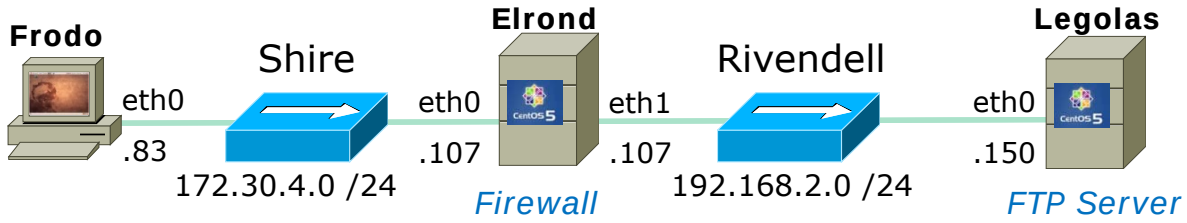
Passive reply to listen on 200, 83 = C853 = 51283

3 way handshake initiated by client

Retrieve legolas file

File transfer

4 way handshake to close connection



Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
34098	20

***Active Mode** is when server initiates new connection for data transfer*

```
ftp> passive
Passive mode off.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (23.8 kB/s)
```

PORT command to listen on 133, 50 = 8532 = 34098

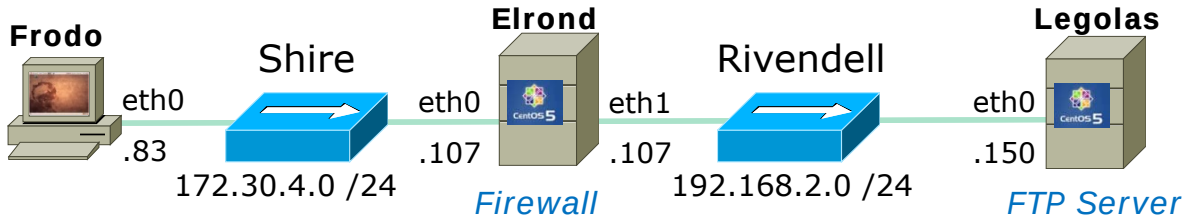
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,133,50
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PAS
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=127 Ack=448 Win=5856 Len=0
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	20	172.30.4.83	34098	TCP	ftp-data > 34098 [SYN] Seq=0 Wi
172.30.4.83	34098	192.168.2.150	20	TCP	34098 > ftp-data [SYN, ACK] Seq
192.168.2.150	20	172.30.4.83	34098	TCP	ftp-data > 34098 [ACK] Seq=1 Ac
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg
192.168.2.150	20	172.30.4.83	34098	FTP-DATA	FTP Data: 18 bytes
192.168.2.150	20	172.30.4.83	34098	TCP	ftp-data > 34098 [FIN, ACK] Seq=19 Ack=1 Win=5888 Len=0
172.30.4.83	34098	192.168.2.150	20	TCP	34098 > ftp-data [ACK] Seq=1
172.30.4.83	34098	192.168.2.150	20	TCP	34098 > ftp-data [ACK] Seq=1
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=141 Ack=513 Win=5856 Len=0
172.30.4.83	34098	192.168.2.150	20	TCP	34098 > ftp-data [FIN, ACK] Seq=1 Ack=20 Win=5856 Len=0
192.168.2.150	20	172.30.4.83	34098	TCP	ftp-data > 34098 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=141 Ack=532 Win=5856 Len=0

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection




```
ftp> bye
221 Goodbye.
```

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: QUIT
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 221 Goodbye.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=147 Ack=546
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [FIN, ACK] Seq=546 Ac
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [FIN, ACK] Seq=147 Ac
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [ACK] Seq=547 Ack=148

4 way handshake to close connection

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

Cruzio
Mike Brogan

Firewalls and FTP

Firewall - FTP Command port

```
[root@elrond pub]# iptables -I RH-Firewall-1-INPUT 9 -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT

[root@elrond pub]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited


[root@elrond pub]# iptables-save > /etc/sysconfig/iptables
[root@elrond pub]#
```

Open TCP port 21 for FTP

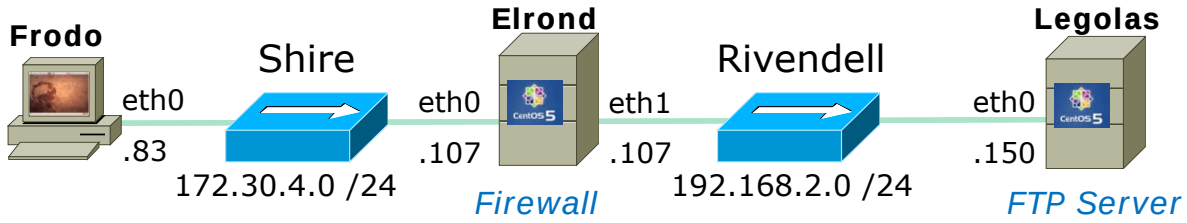
Save to make changes persist across restarts

Firewall - passive mode

In passive mode, the client initiates the connection for the data transfer. The ip_conntrack_ftp module must be loaded so the firewall will allow the passive connections to random ports

```
[root@elrond pub]# cat /etc/sysconfig/iptables-config
# Load additional iptables modules (nat helpers)
#   Default: -none-
# Space separated list of nat helpers (e.g. 'ip_nat_ftp ip_nat_irc'), which
# are loaded after the firewall rules are applied. Options for the helpers are
# stored in /etc/modprobe.conf.
IPTABLES_MODULES="ip_conntrack_netbios_ns ip_conntrack_ftp"
 Add
< snipped >

[root@elrond pub]#

[root@elrond pub]# service iptables restart
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: filter                    [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]ntrack_ftp
[root@elrond pub]#
```

Add this to load the module to track related FTP connections

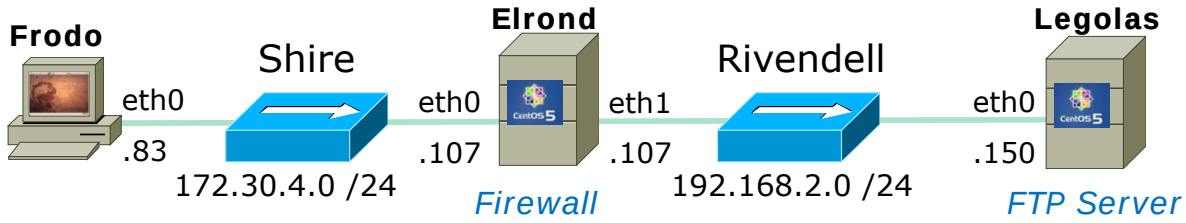



```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21

Chain OUTPUT (policy DROP)
target     prot opt source               destination
[root@elrond ~]#
```

For DNS lookups by FTP server

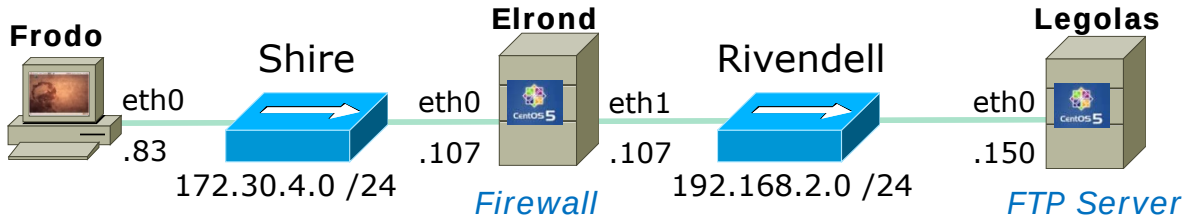
This firewall setting allows external clients (Frodo) to access the FTP server (Legolas)

Note: The FTP data port 20 is not specified




```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (15.1 kB/s)
ftp> passive
Passive mode on.
ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,224,164)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (8.6 kB/s)
ftp> bye
221 Goodbye.
root@frodo:~#
```

Successful downloads using both active and passive mode using the firewall settings in previous slide

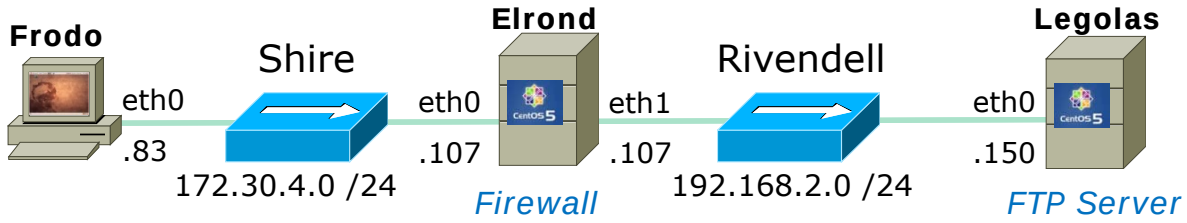


What If? *We remove firewall opening for the DNS lookups sent by the FTP server*

```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21

Chain OUTPUT (policy DROP)
target     prot opt source               destination
[root@elrond ~]#
```

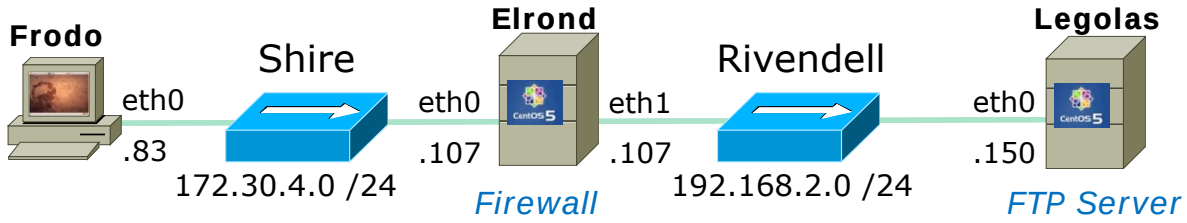
Now DNS lookups are blocked

```
[root@elrond ~]# iptables -D FORWARD 1
```




```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (15.1 kB/s)
ftp> passive
Passive mode on.
ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,224,164)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (8.6 kB/s)
ftp> bye
221 Goodbye.
root@frodo:~#
```

Result: Instead of a fast login, now there is a delay of about 15 seconds before the successful login messages and ftp prompt are displayed

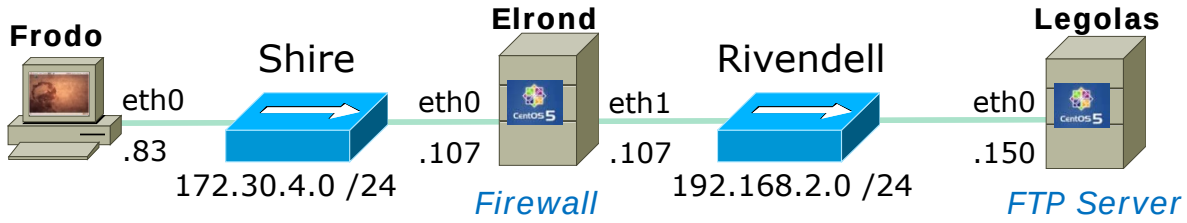



```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
```

Delay encountered (~15 seconds) here after dropping DNS lookups in firewall

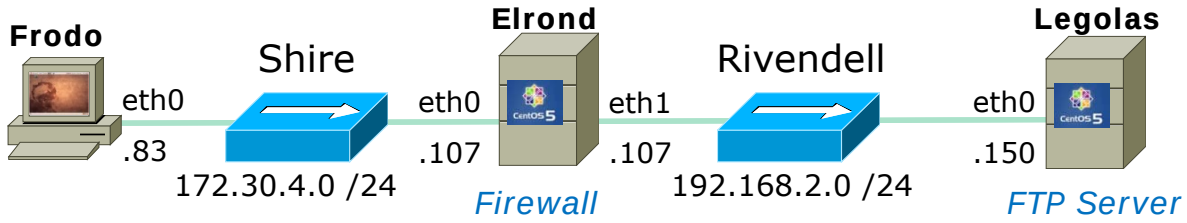
SIP	SP	DIP	DP	Protocol	Info	No.	Time
172.30.4.195	40823	192.168.2.150	21	FTP	Request: PASS Cabrillo	12	8.920738
192.168.2.150	58200	207.62.187.54	53	DNS	Standard query PTR 195.4.30.172.in-addr.arp	13	8.938715
192.168.2.150	21	172.30.4.195	40823	TCP	ftp > 40823 [ACK] Seq=55 Ack=29 Win=5888 Le	14	8.951876
192.168.2.150	58200	207.62.187.54	53	DNS	Standard query PTR 195.4.30.172.in-addr.arp	15	16.612474
192.168.2.150	21	172.30.4.195	40823	FTP	Response: 230 Login successful.	16	24.336986

The login is delayed while the two DNS requests time-out.



What If? *We next remove the related state condition from the firewall?*

```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21

Chain OUTPUT (policy DROP)
target     prot opt source               destination
[root@elrond ~]#


[root@elrond ~]# iptables -D FORWARD 1
[root@elrond ~]# iptables -I FORWARD 1 -m state --state ESTABLISHED -j ACCEPT
```




```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
425 Failed to establish connection.
ftp>
```

Hangs up here, because the related connection for the data transfer is now blocked by the firewall.

Gives up after 5 tries of attempting to do a 3-way handshake

SIP	SP	DIP	DP	Protocol	Info	No.	Time
172.30.4.195	59956	192.168.2.150	21	FTP	Request: RETR legolas	123	383.241428
192.168.2.150	20	172.30.4.195	58333	TCP	ftp-data > 58333 [SYN] Seq=0 Win=5840 Len=(	124	383.242944
192.168.2.150	21	172.30.4.195	59956	TCP	ftp > 59956 [ACK] Seq=179 Ack=84 Win=5888 l	125	383.316282
192.168.2.150	20	172.30.4.195	58333	TCP	ftp-data > 58333 [SYN] Seq=0 Win=5840 Len=(	129	388.071827
192.168.2.150	20	172.30.4.195	58333	TCP	ftp-data > 58333 [SYN] Seq=0 Win=5840 Len=(	134	397.449484
192.168.2.150	20	172.30.4.195	58333	TCP	ftp-data > 58333 [SYN] Seq=0 Win=5840 Len=(	143	416.129995
Vmware_7c:18:		Vmware_4e:21:a5		ARP	Who has 192.168.2.107? Tell 192.168.2.150	154	443.727874
Vmware_4e:21::		Vmware_7c:18:f5		ARP	192.168.2.107 is at 00:0c:29:4e:21:a5	155	443.727967
192.168.2.150	20	172.30.4.195	58333	TCP	ftp-data > 58333 [SYN] Seq=0 Win=5840 Len=(	159	453.553314
192.168.2.150	21	172.30.4.195	59956	FTP	Response: 425 Failed to establish connectic	167	476.875137
172.30.4.195	59956	192.168.2.150	21	TCP	59956 > ftp [ACK] Seq=84 Ack=216 Win=5856 l	168	476.916311

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

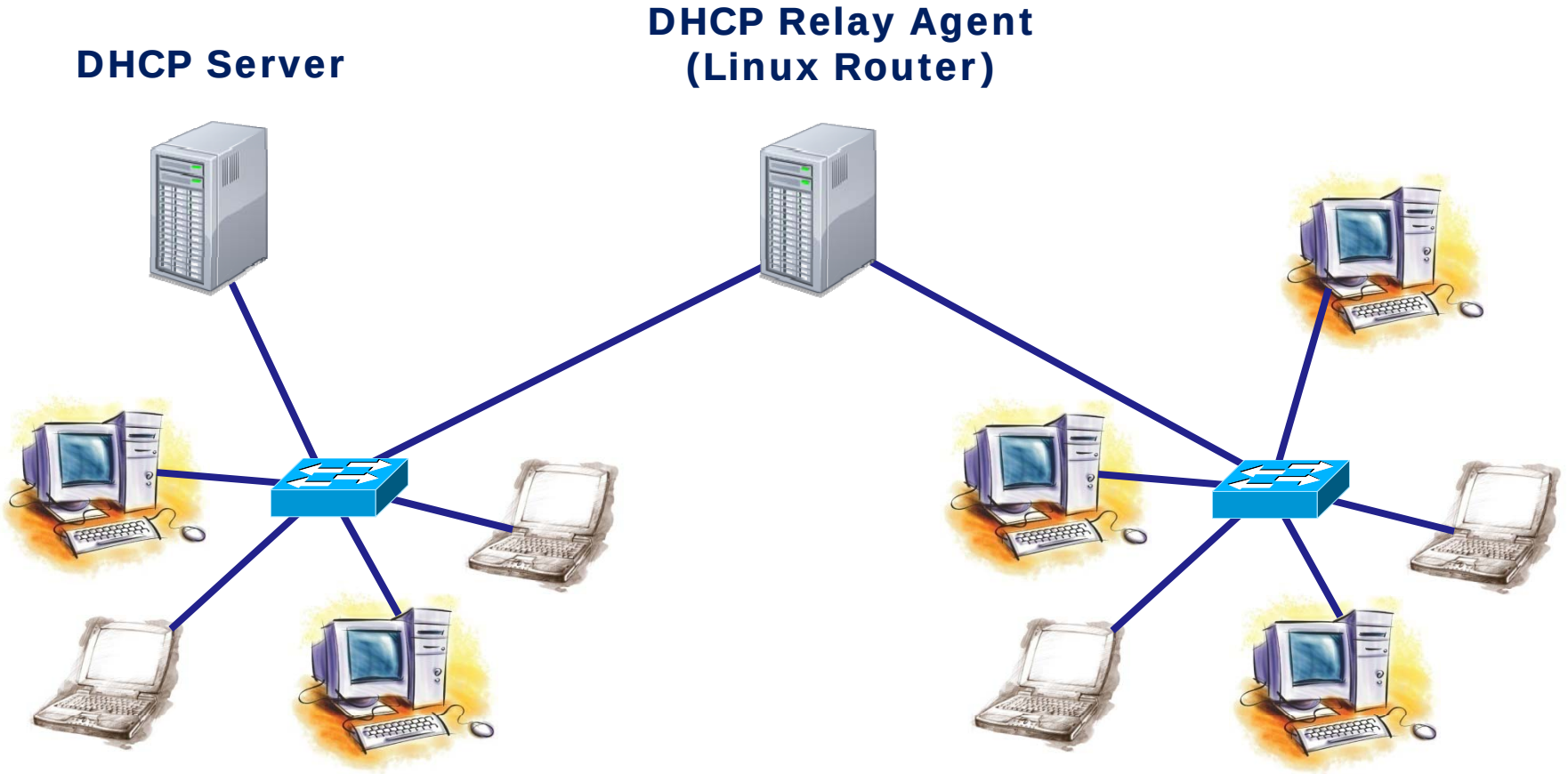
- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

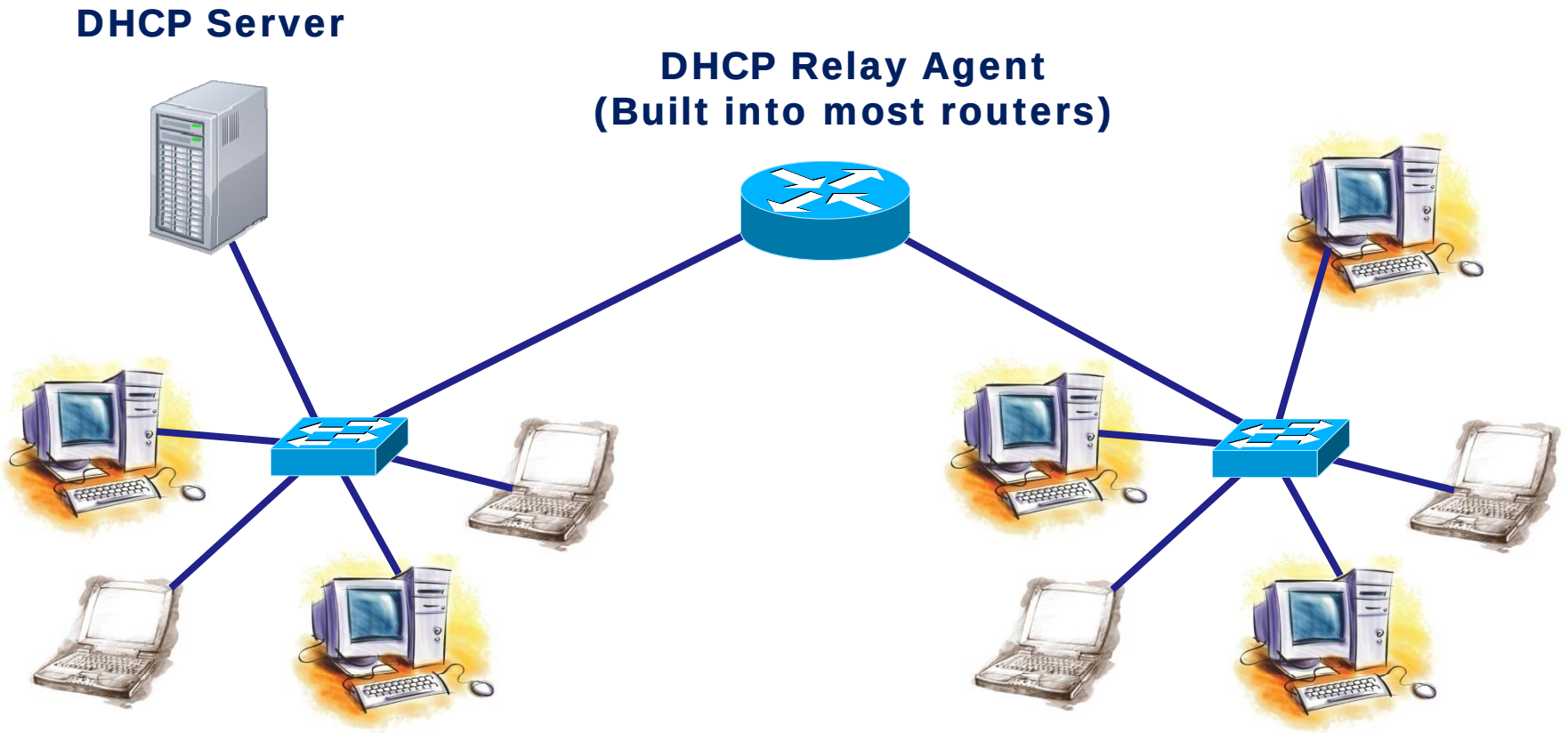
DHCP Clients

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

DHCP


DHCP Server
DHCP Relay Agent
(Linux Router)
DHCP Clients
DHCP Clients

DHCP


DHCP Server
DHCP Relay Agent
(Built into most routers)
DHCP Clients
DHCP Clients

DHCP

DHCP Protocol

DORA

- Discover
- Offer
- Request
- Acknowledge

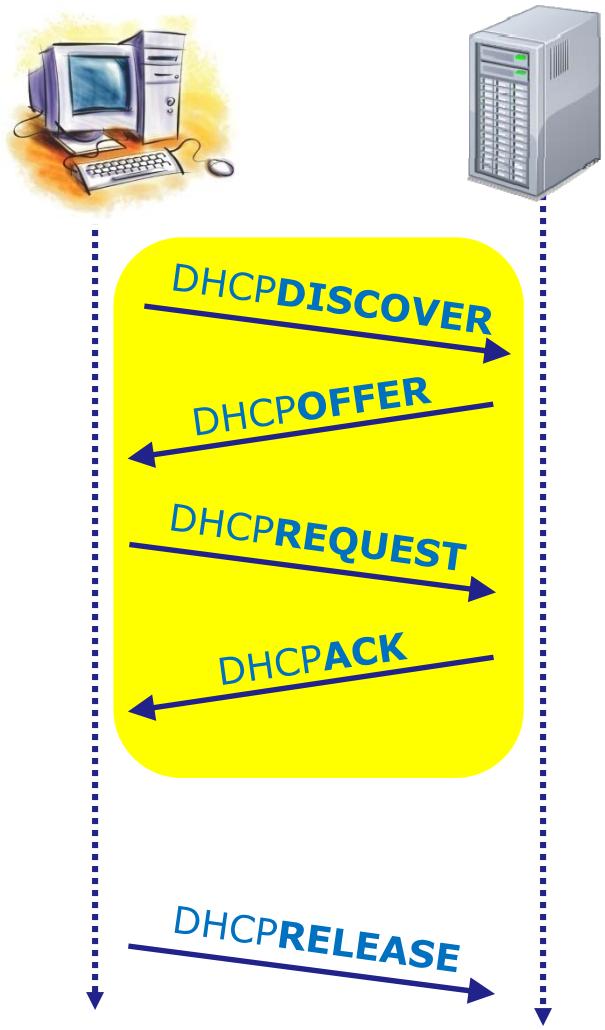
The DORA sequence is used by to join a new client to the network

And

- Release, Decline, NAck, Inform

DHCP

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



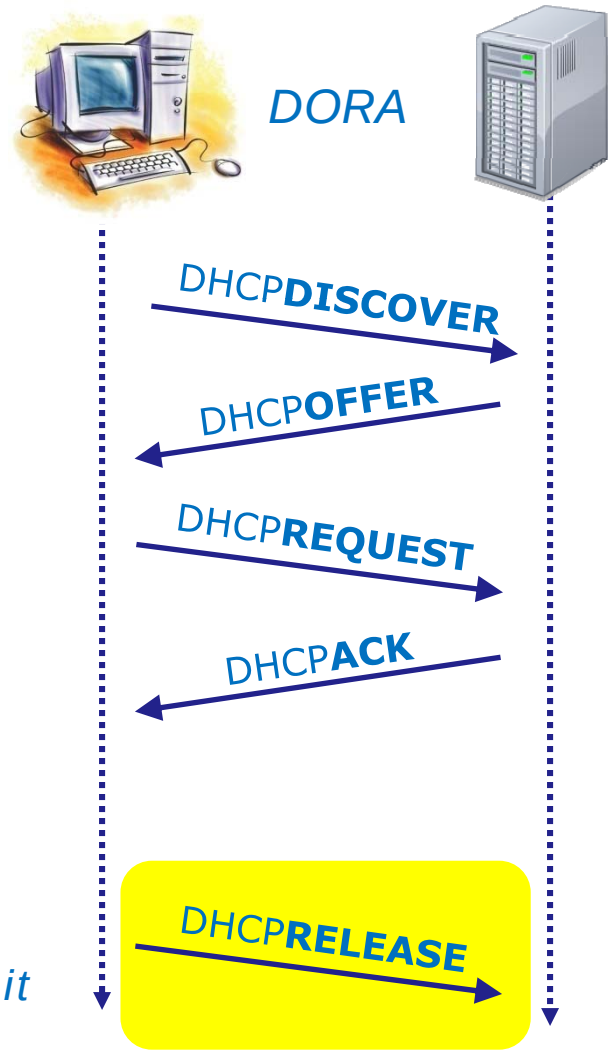
D *iscover*

O *ffer*

R *equest*

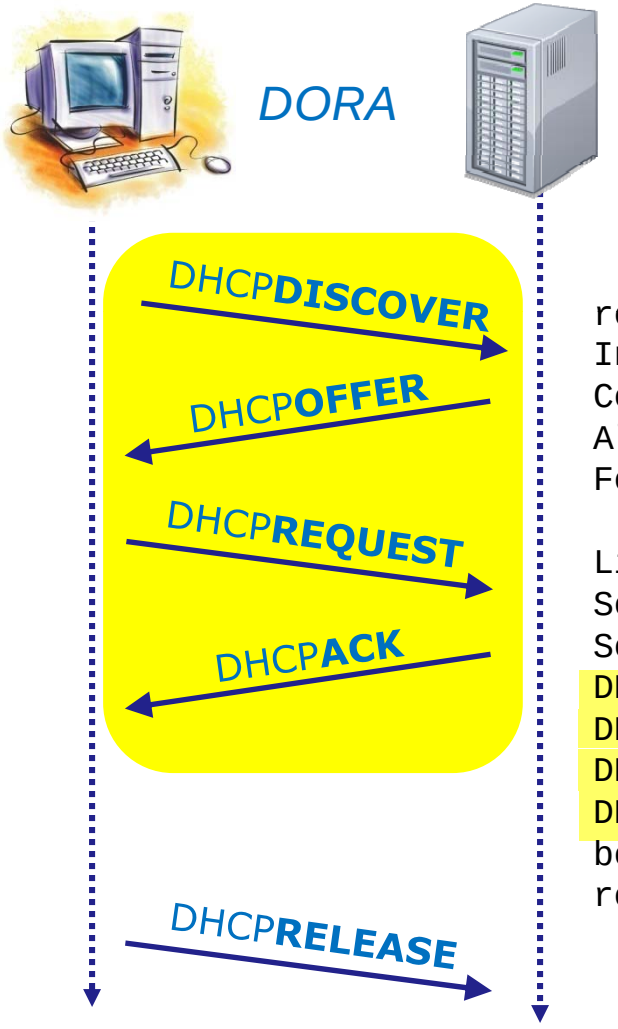
A *cknowledge*

DHCP



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

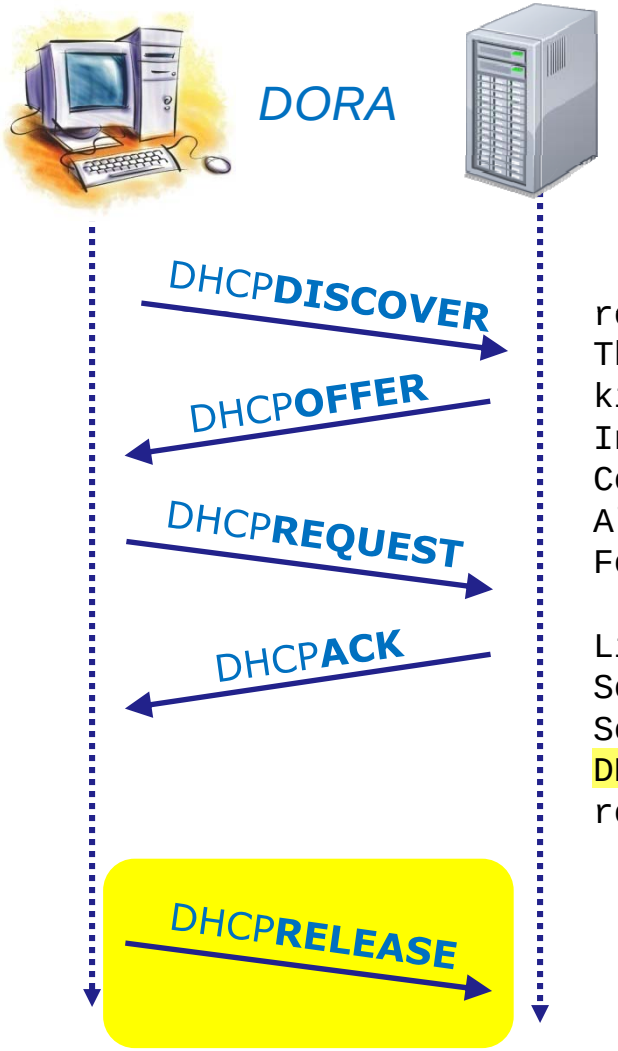
DHCP



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

```
root@frodo:~# dhclient
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

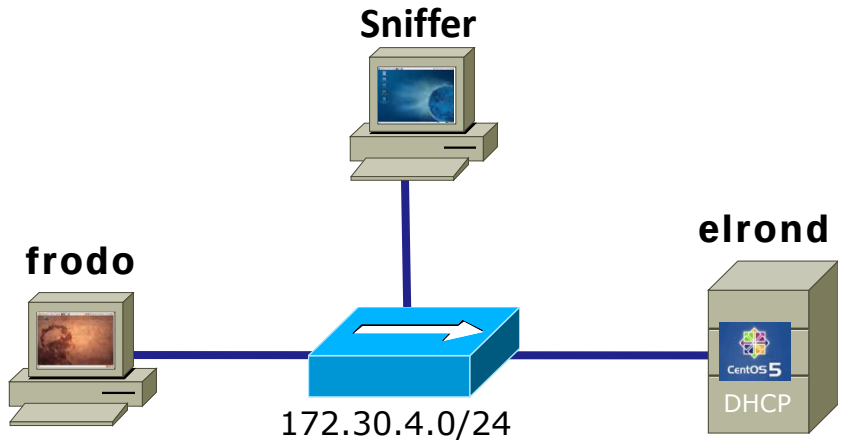


*The **dhclient –r** command does a DHCP release*

```
root@frodo:~# dhclient -r
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:~#
```

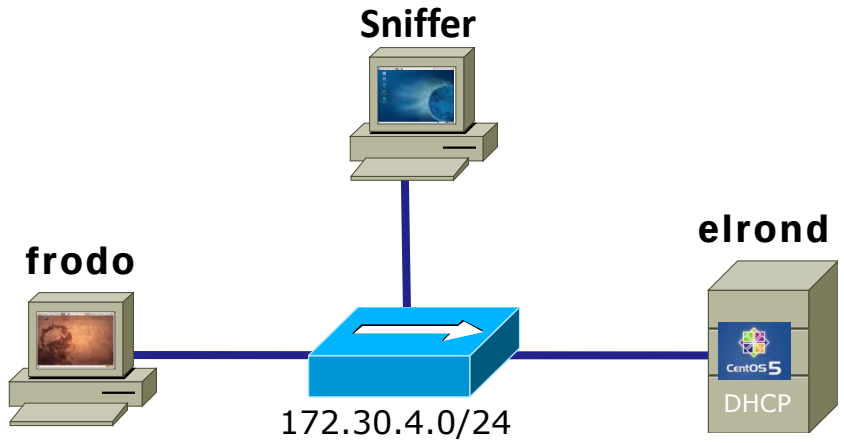
DHCP

Wireshark view of example DHCP operations



DHCP Client *DHCP Server*

Frodo starting up (needs IP address)



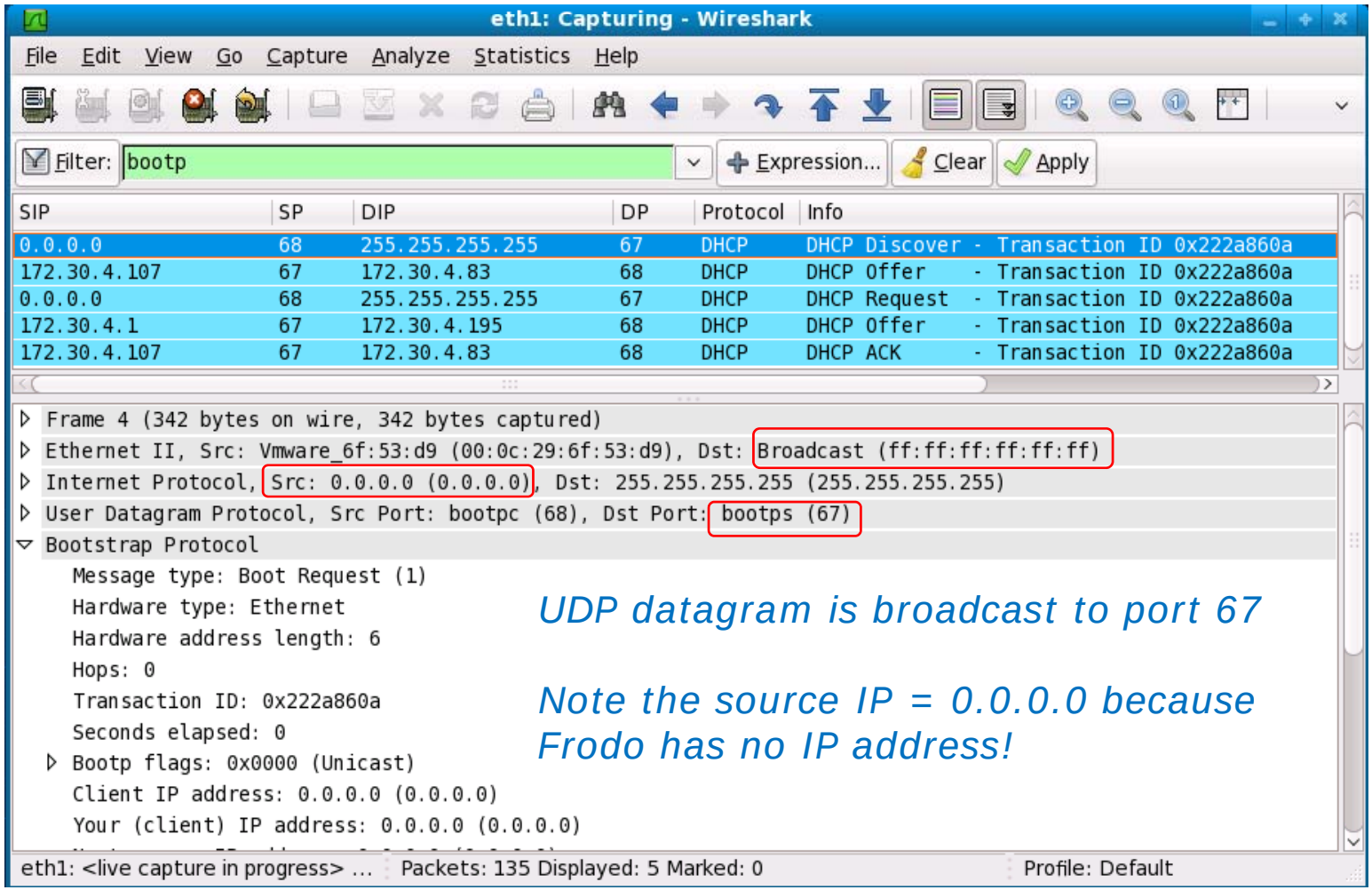
DHCP Client

DHCP Server

frodo

*DHCP**DISCOVER***
(broadcast)

Help, I need an IP address!



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)

Help, 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
```

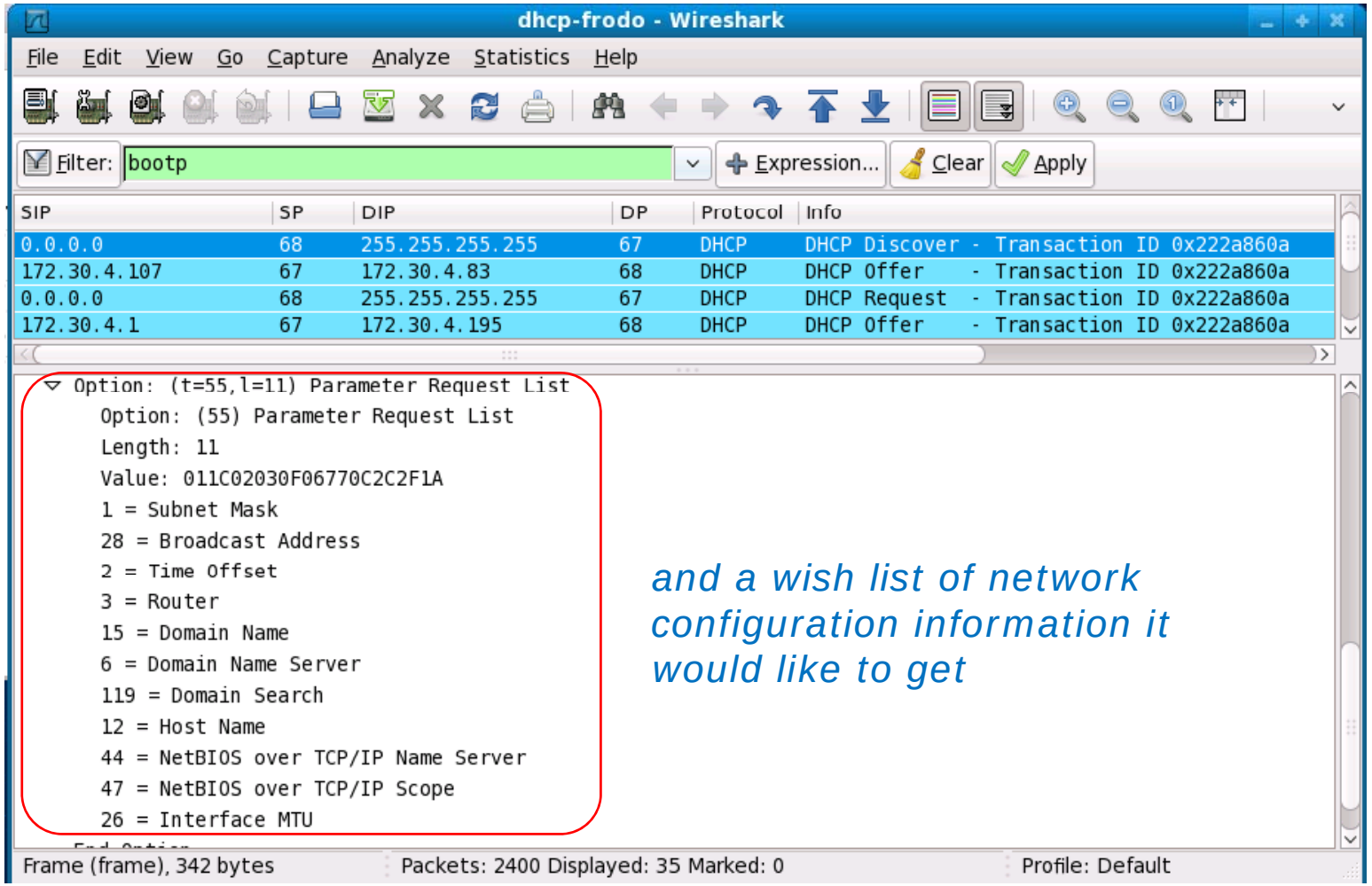
Frodo sends its hostname

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

frodo

*DHCP**DISCOVER***
(broadcast)

Help, I need an IP address!

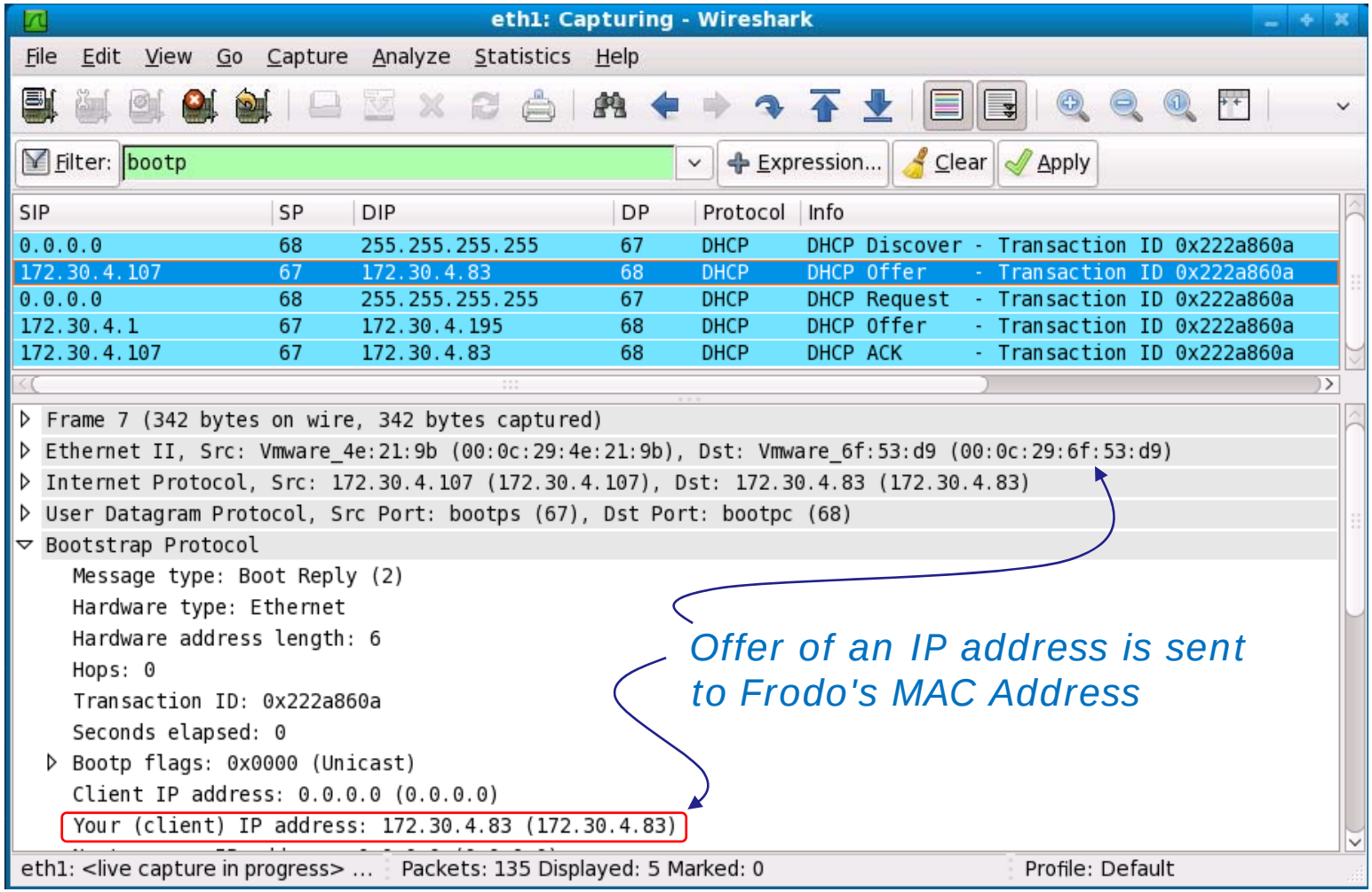


and a wish list of network configuration information it would like to get

elrond

*DHCP**OFFER***
(unicast)

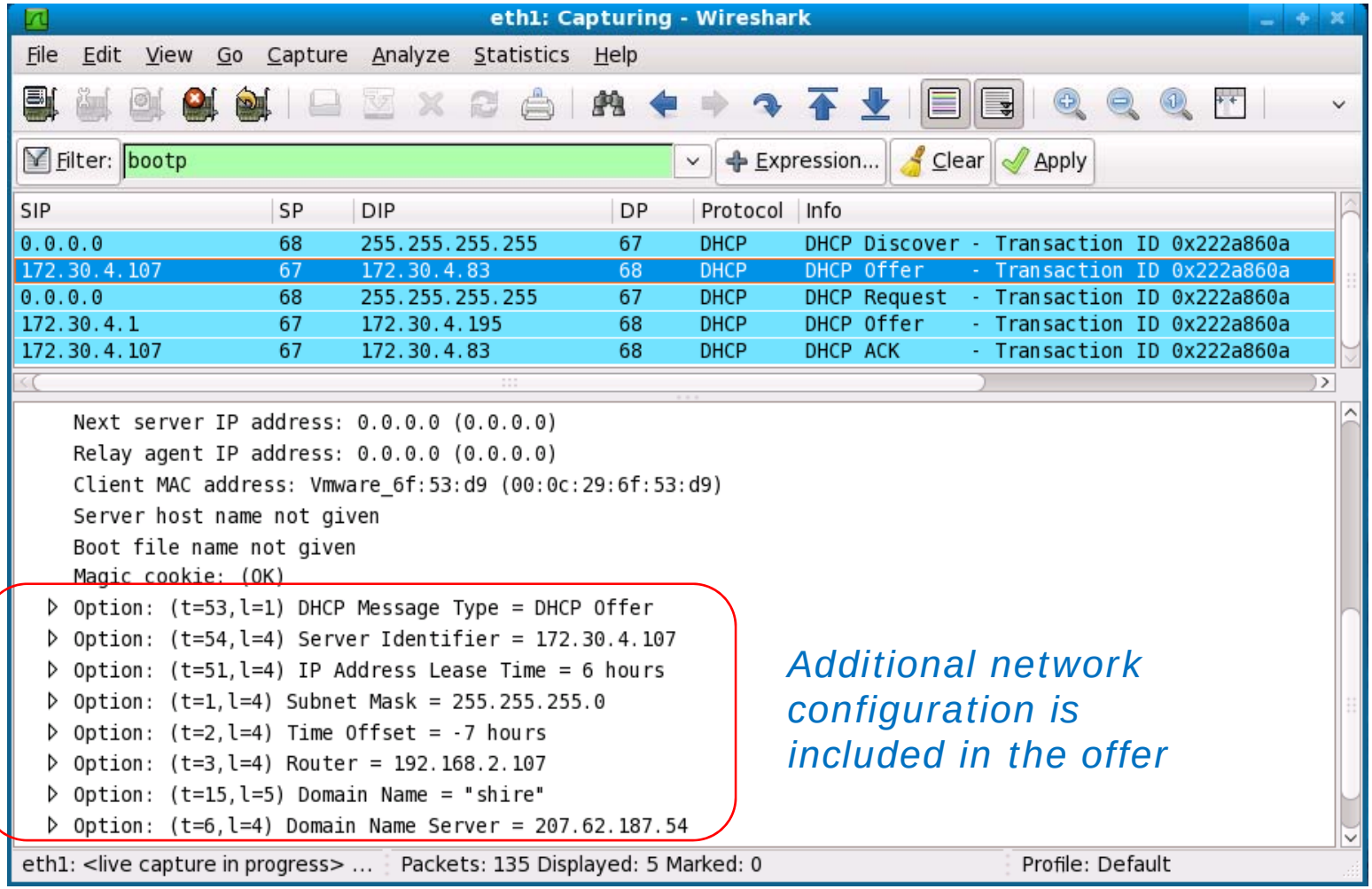
Here is an IP address, want it?



elrond

*DHCP**OFFER***
(unicast)

Here is an IP address, want it?

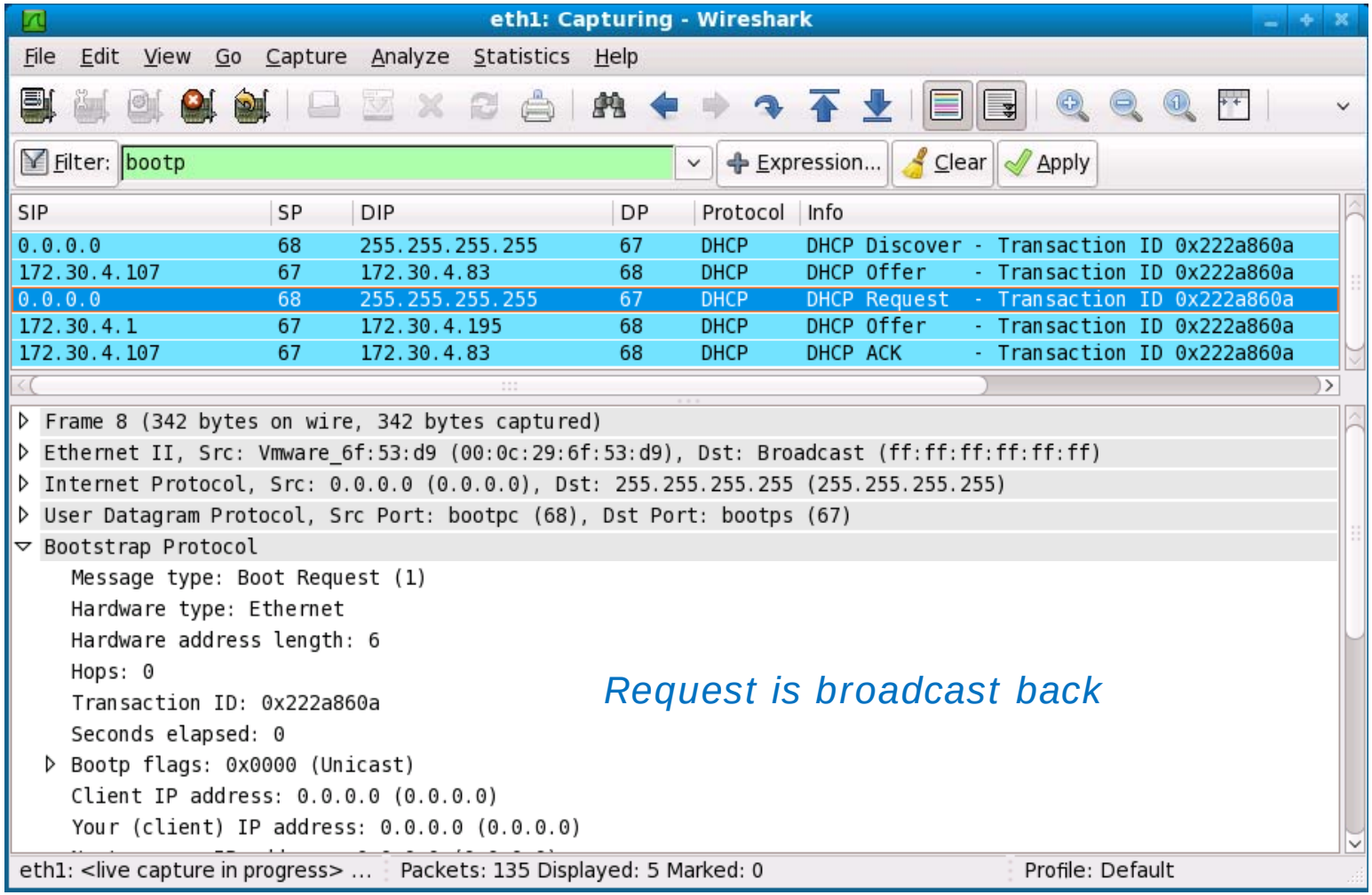


Additional network configuration is included in the offer

frodo

*DHCP**REQUEST***
(broadcast)

Yes, I want that one



Request is broadcast back

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

```
    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 Request
  ▷ Option: (t=54,l=4) Server Identifier = 172.30.4.107
  ▷ Option: (t=50,l=4) Requested IP Address = 172.30.4.83
  ▷ Option: (t=12,l=5) Host Name = "frodo"
  ▷ Option: (t=55,l=11) Parameter Request List
    End Option
    Padding
```

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

Includes IP address and DHCP server that made the offer

elrond

*DHCP**ACK***
(unicast)

You got 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 52 (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)
```

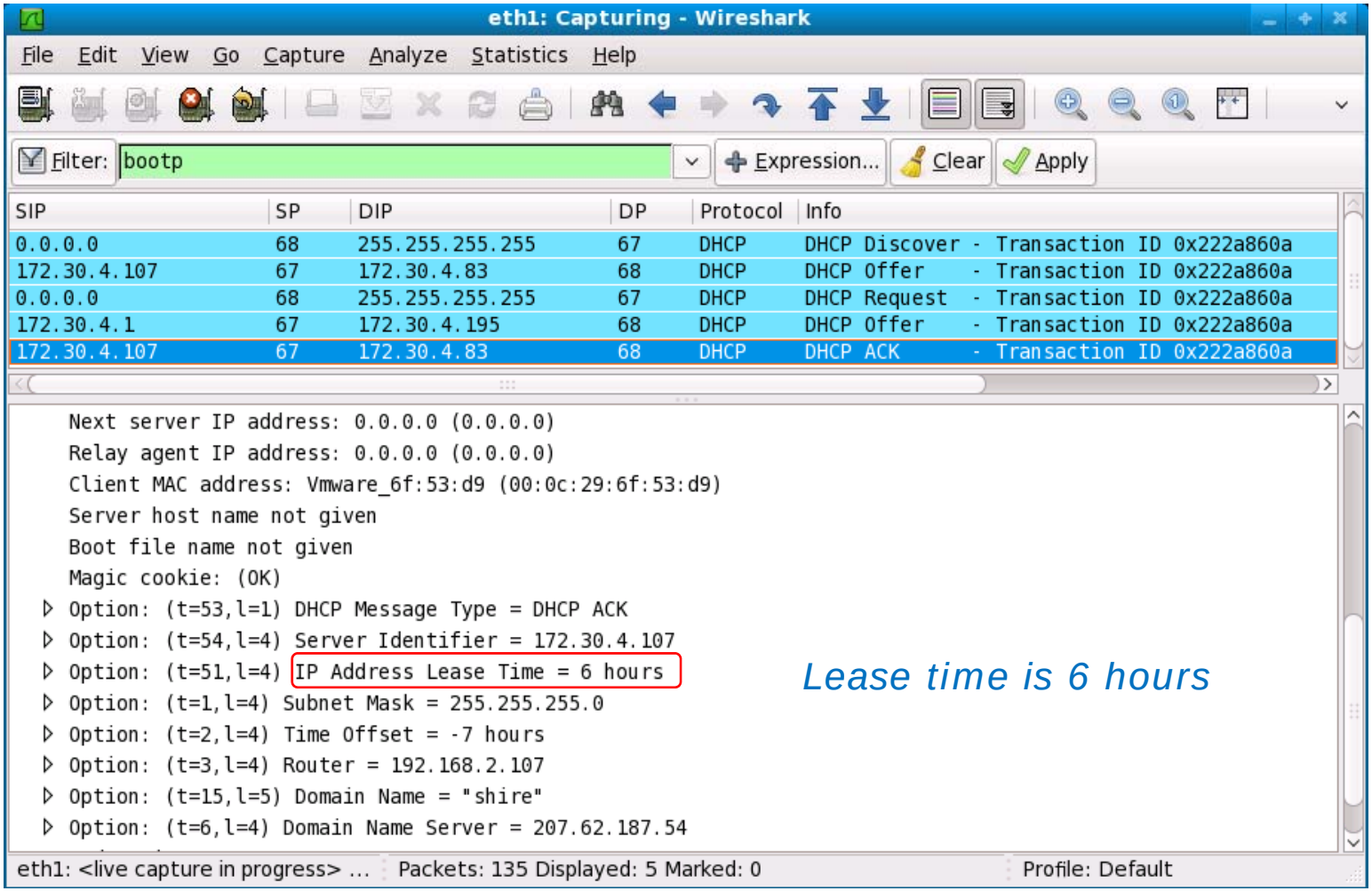
IP address is confirmed

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

elrond

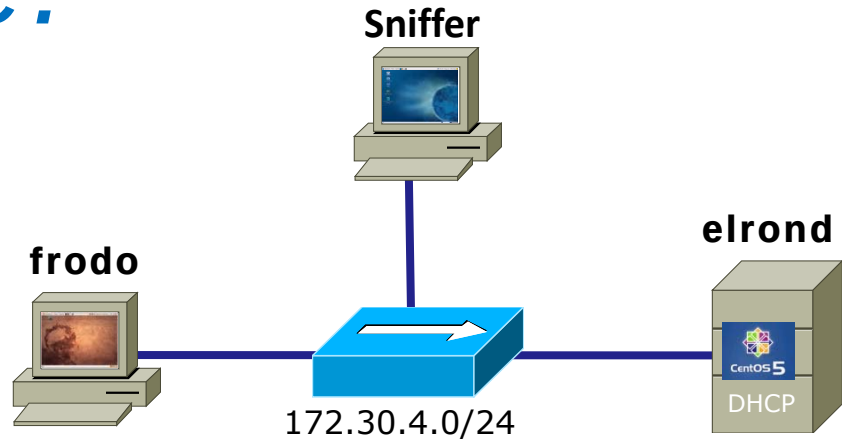
*DHCP**ACK***
(unicast)

You got it!



Lease time is 6 hours

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

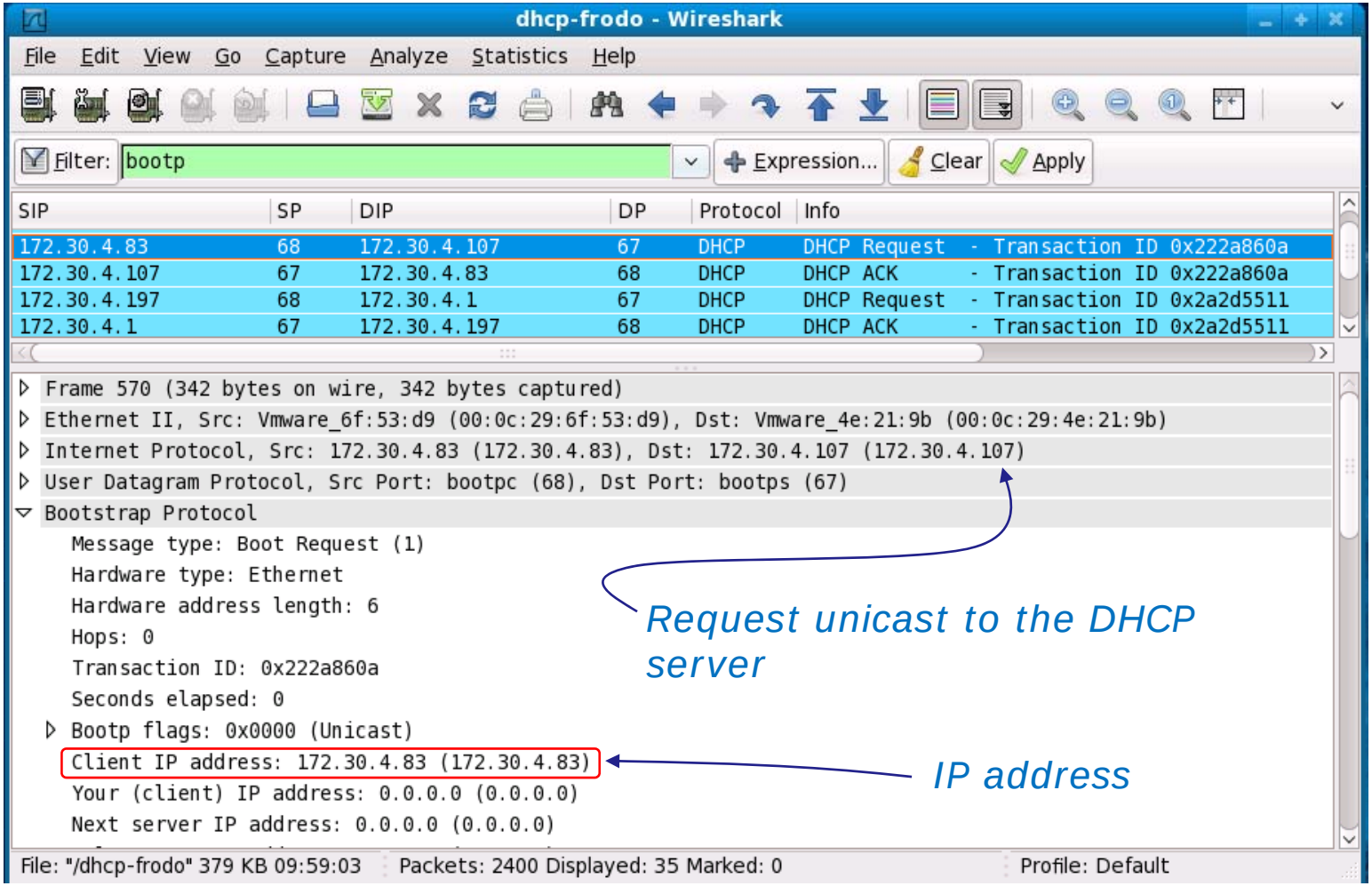


DHCP Client *DHCP Server*

frodo

*DHCP**REQUEST***
(unicast)

I want to renew the lease!



frodo

DHCPREQUEST
(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

DHCPACK (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

DHCPACK (unicast)

You got it!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

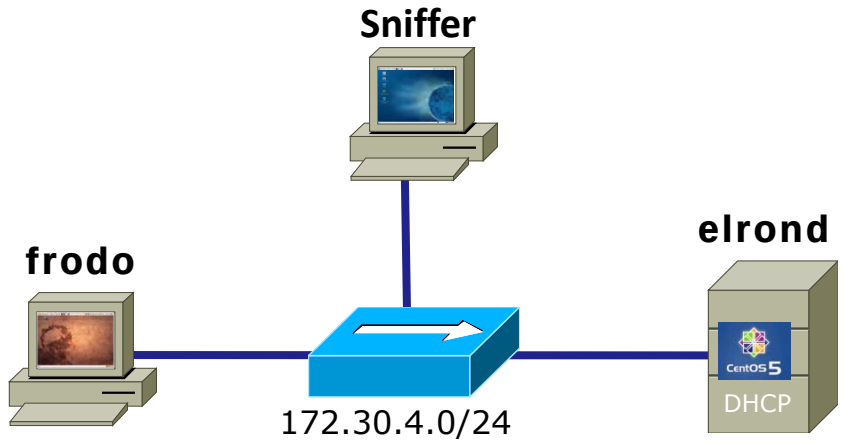
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction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

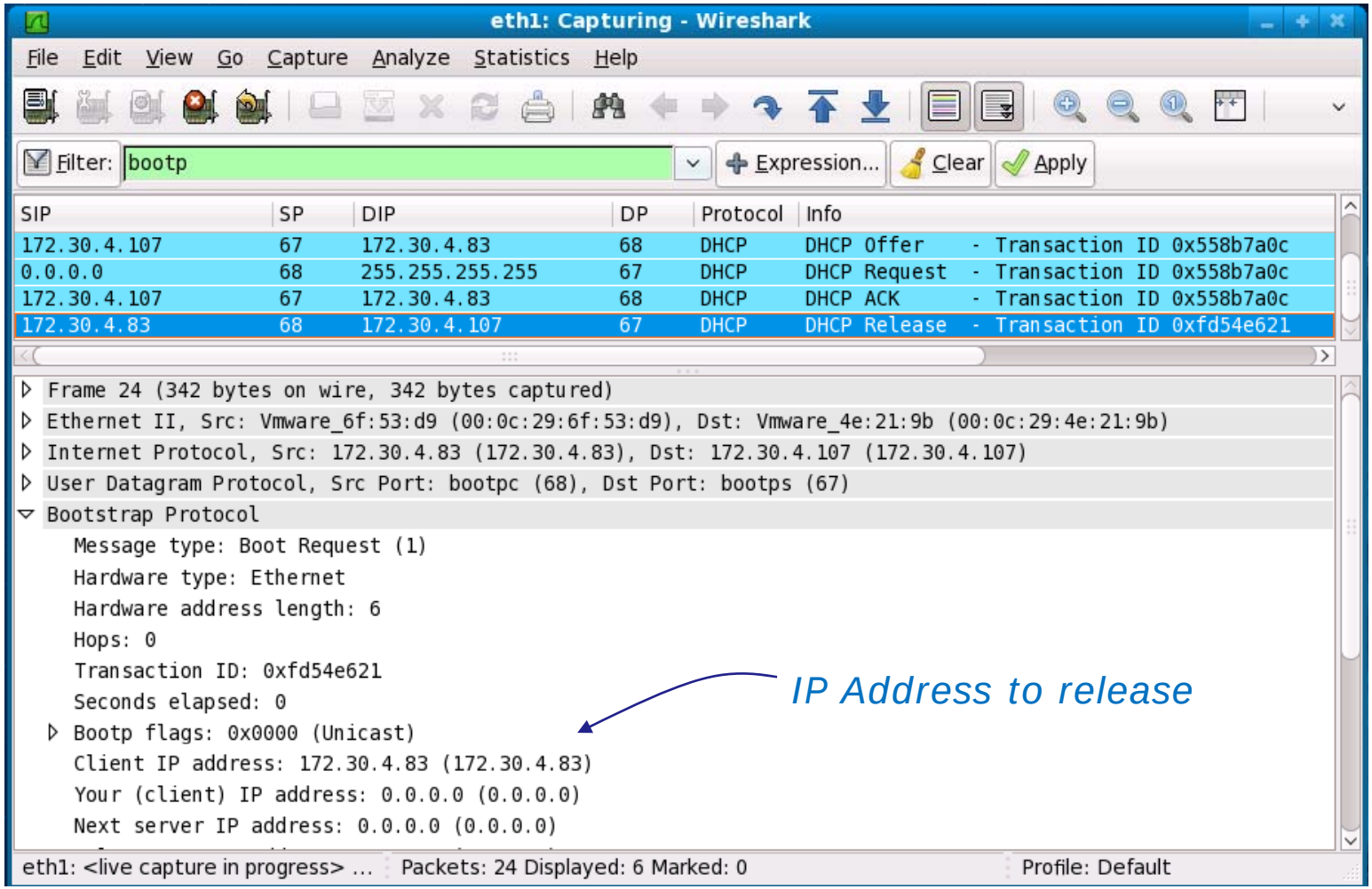


DHCP Client *DHCP Server*

frodo

*DHCP**RELEASE***
(unicast)

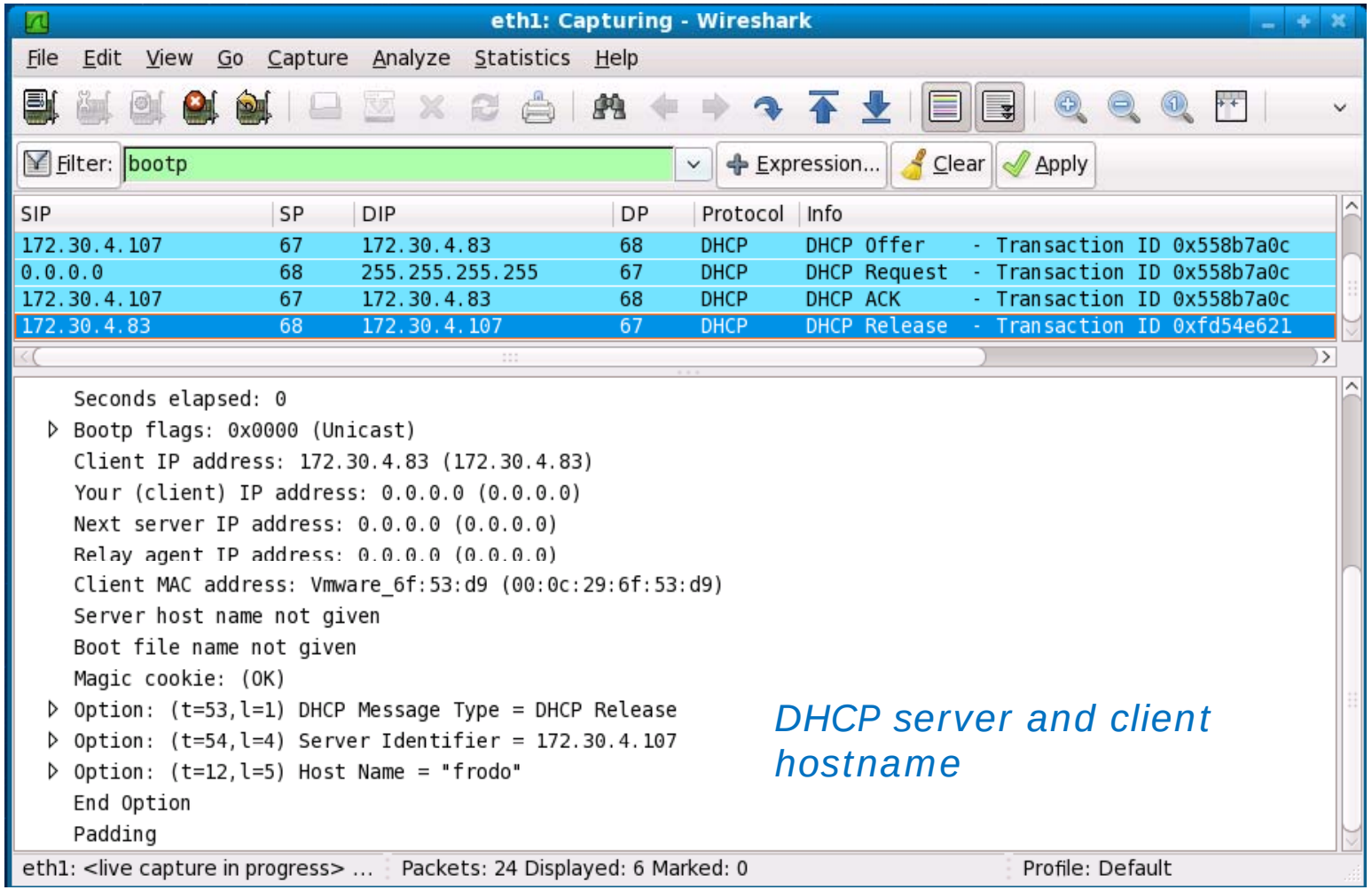
I want out!



frodo

*DHCP**RELEASE***
(unicast)

I want out!

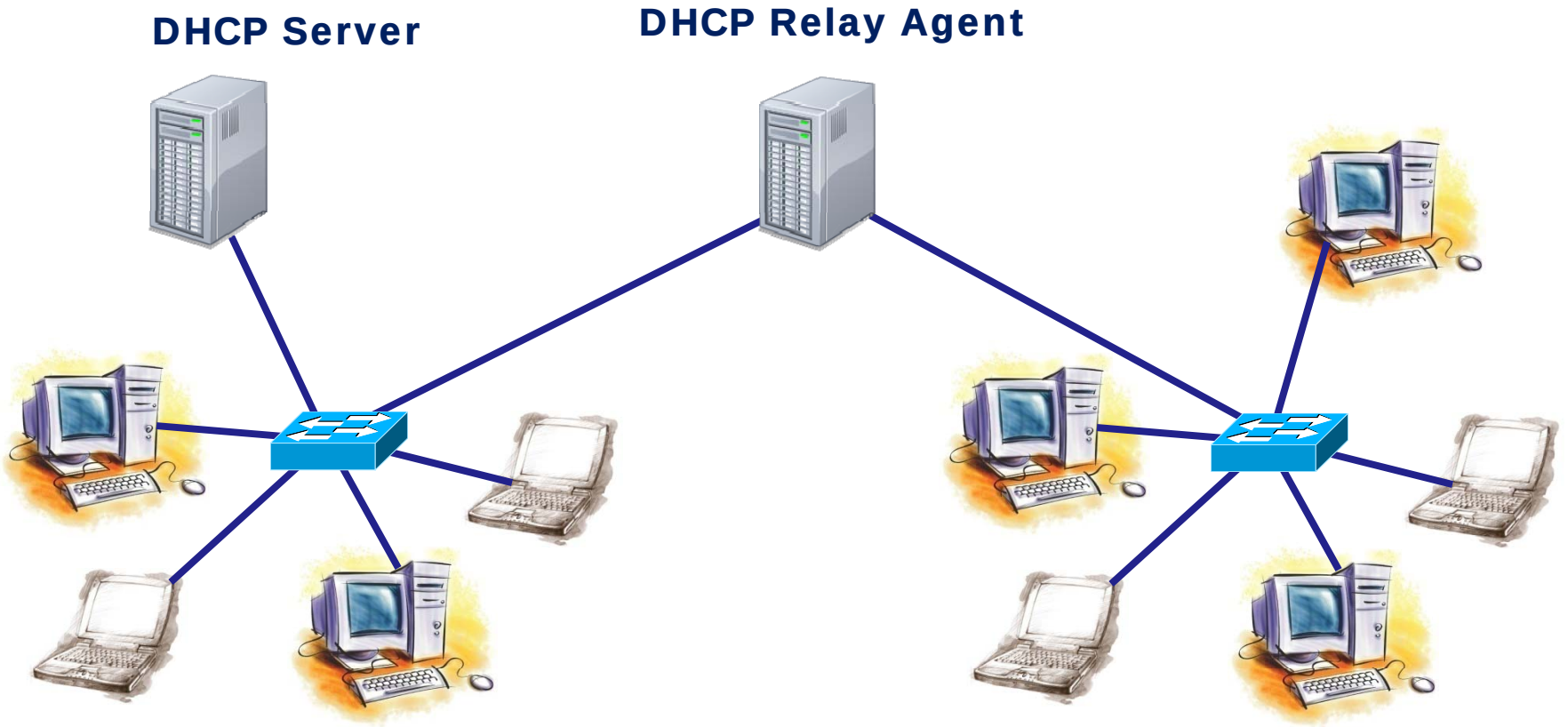


DHCP server and client hostname

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 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 -r** 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
```

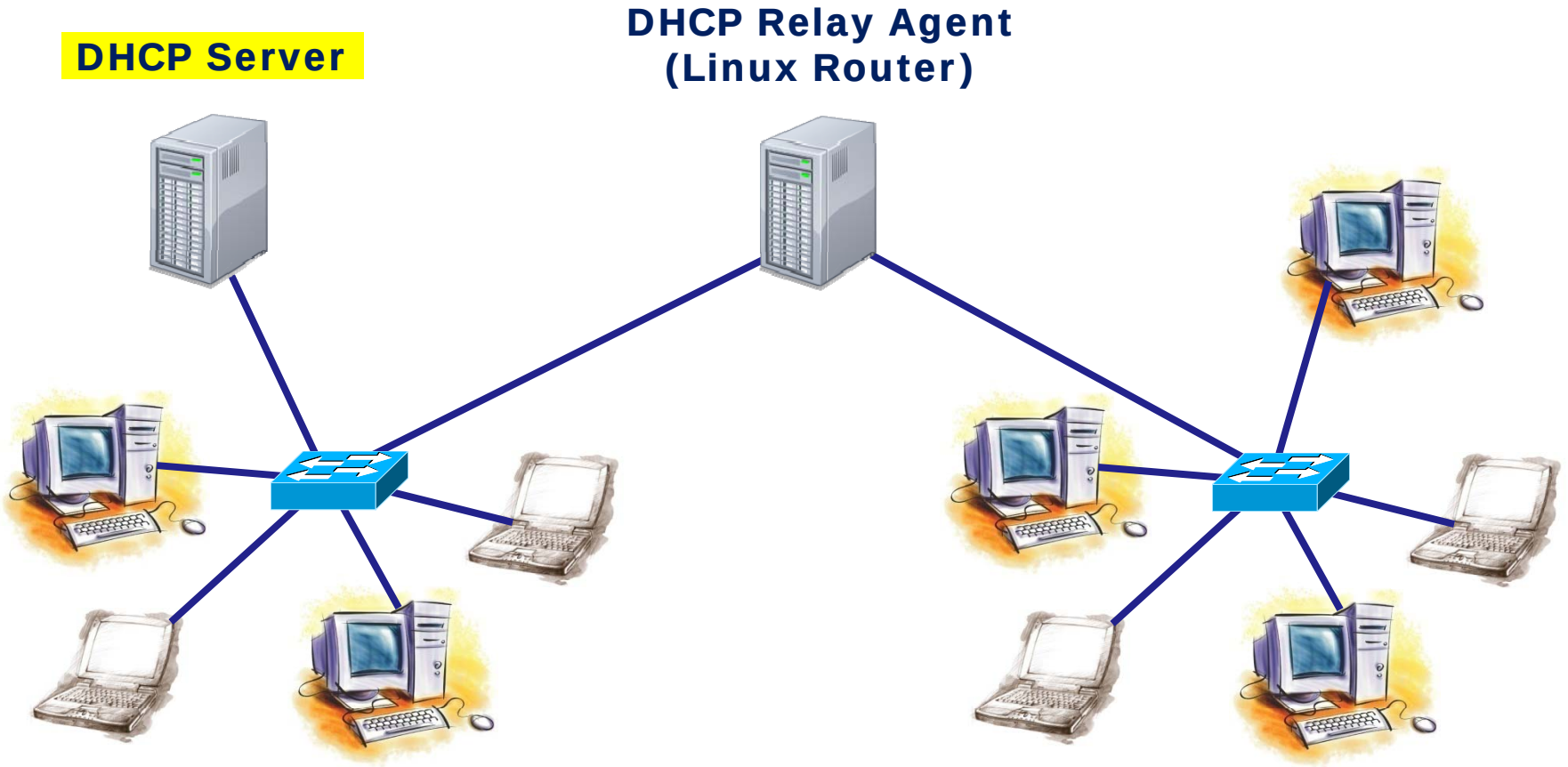
Red Hat Family DHCP client example

```
[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 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 dhcps

DHCP

Is it already installed?

```
[root@elrond ~]# rpm -qa | grep dhcp
dhcpv6-client-1.0.10-17.el5          client
dhcp-3.0.5-21.el5_4.1                server
[root@elrond ~]#
```

Is it already running?

```
[root@elrond ~]#[root@elrond ~]# ps -ef | grep dhc
root      5587     1  0 15:50 ?        00:00:00 /usr/sbin/dhcpd
root      9911  5505  0 18:18 pts/0    00:00:00 grep dhc
[root@elrond ~]#
```

```
[root@elrond ~]# service dhcpd status
dhcpd (pid 5587) is running...
[root@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@elrond ~]# mount /dev/cdrom /media
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@elrond ~]# cd /media
[root@elrond media]# ls dhcp*
dhcp-3.0.5-21.el5_4.1.i386.rpm
[root@elrond media]# rpm -hiv dhcp-3.0.5-21.el5_4.1.i386.rpm
Preparing...                ########################################### [100%]
   1:dhcp                   ########################################### [100%]
[root@elrond media]#
```

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 {
                                                    Subnet specific settings
# --- 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 ~]#
```

```
[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

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!

Classroom DHCP IP allocation pools table by station number
http://simms-teach.com/docs/static-ip-addrs.pdf

IP Address Assignments for Classroom PCs (Room 2501)

		Static		DHCP Pool	
Station	Station IP	Static 1	Static 2	Start	End
x	172.30.1.	172.30.1.	172.30.1.	172.30.1.	172.30.1.
0	100	125	200	50	52
1	101	126	201	53	55
2	102	127	202	56	58
3	103	128	203	59	61
4	104	129	204	62	64
5	105	130	205	65	67
6	106	131	206	68	70
7	107	132	207	71	73
8	108	133	208	74	76
9	109	134	209	77	79
10	110	135	210	80	82
11	111	136	211	83	85
12	112	137	212	86	88
13	113	138	213	89	91
14	114	139	214	92	94
15	115	140	215	95	97
16	116	141	216	225	227
17	117	142	217	228	230
18	118	143	218	231	233
19	119	144	219	234	236
20	120	145	220	237	239
21	121	146	221	240	242
22	122	147	222	243	245
23	123	148	223	246	248
24	124	149	224	249	251

Use these pools of addresses based on your station number to avoid conflicts on the classroom network

Lab DHCP IP allocation pools table by station number
http://simms-teach.com/docs/static-ip-addrs.pdf

IP Address Assignments for Lab PCs (CIS Lab and CTC)

		Static		DHCP Pool	
Station	Station IP	Static 1	Static 2	Start	End
CIS-Lab-	172.30.4.	172.30.4.	172.30.4.	172.30.4.	172.30.4.
1	101	121	122	50	54
2	102	123	124	55	59
3	103	125	126	60	64
4	104	127	128	65	69
5	105	129	130	70	74
6	106	131	132	75	79
7	107	133	134	80	84
8	108	135	136	85	89
9	109	137	138	90	94
10	110	139	140	95	99
11	111	141	142	200	204
12	112	143	144	205	209
13	113	145	146	210	214
14	114	147	148	215	219
15	115	149	150	220	224
16	116	151	152	225	229

Use these pools of addresses based on your station number to avoid conflicts on the classroom network

Installing and Configuring DHCP

Step 3 *Configure firewall*

Open UDP port 67 as a destination

iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 67 -j ACCEPT

for default CentOS firewall

To make the firewall settings permanent, backup current permanent settings

iptables-save > /etc/sysconfig/iptables.bak

Save current settings with revised port 67 rule

iptables-save > /etc/sysconfig/iptables

Restart firewall using revised permanent settings

service iptables restart

Installing and Configuring DHCP

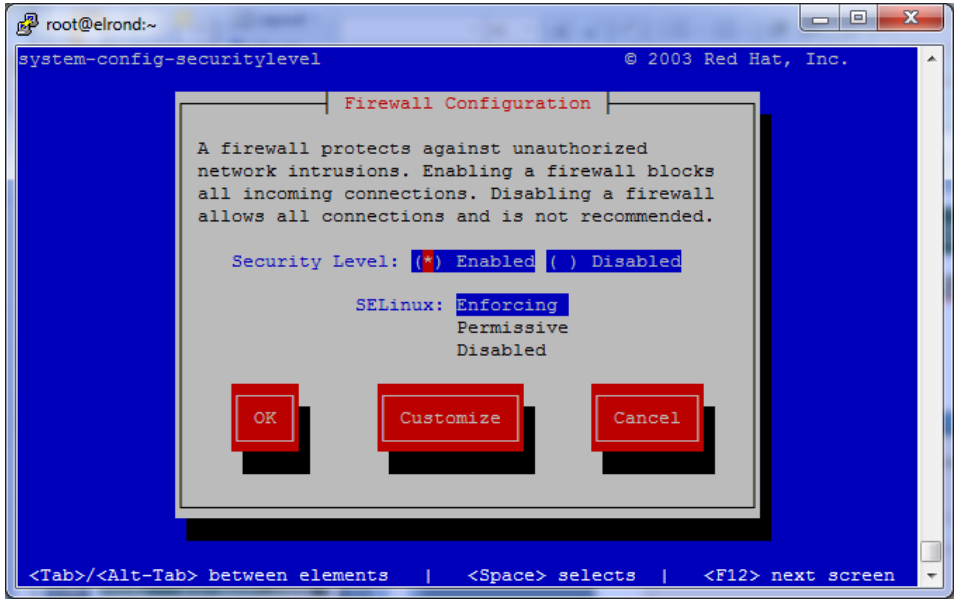
Step 3 *Configure firewall to open port 67*

```
[root@elrond ~]# iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  0.0.0.0/0            0.0.0.0/0

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

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

Chain RH-Firewall-1-INPUT (1 references)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0            0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0            224.0.0.251         udp dpt:5353
6    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:67
7    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:631
8    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:631
9    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
10   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
11   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited
[root@elrond ~]#
```

SELinux for DHCP (CentOS)

Step 4 *Configure SELinux*


```
[root@elrond ~]# lokkit
```




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

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  ]
[root@elrond ~]#
```

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
[root@elrond ~]#
```

DHCP

Step 7 *Verify service is running*

```
[root@elrond ~]# ps -ef | grep dhc
root      5587     1  0 15:50 ?        00:00:00 /usr/sbin/dhcpd
root      9911  5505  0 18:18 pts/0    00:00:00 grep dhc

[root@elrond ~]# service dhcpd status
dhcpd (pid 5587) is running...

[root@elrond ~]# netstat -uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address
State
udp        0      0 0.0.0.0:67                  0.0.0.0:*
udp        0      0 0.0.0.0:858                 0.0.0.0:*
udp        0      0 0.0.0.0:861                 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 0.0.0.0:53238               0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 :::42624                    :::*
udp        0      0 :::5353                     :::*
```

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 to observe DORA

Installing and Configuring vsftpd

Step 9 **Monitor log files**

```
[root@arwen ~]# tail /var/log/secure | grep dhcp
[root@elrond ~]# tail /var/log/messages | grep dhcp
Mar 24 04:14:21 elrond dhcpd: DHCPACK on 192.168.2.150 to 08:00:27:f5:e0:5f
via eth1
Mar 24 04:14:21 elrond dhcpd: DHCPREQUEST for 192.168.2.150 from
08:00:27:f5:e0:5f via 192.168.2.150
Mar 24 04:14:21 elrond dhcpd: DHCPACK on 192.168.2.150 to 08:00:27:f5:e0:5f
via 192.168.2.150
Mar 24 04:15:05 elrond dhcpd: Unable to add forward map from sauron.mordor
to 192.168.3.98: timed out
Mar 24 04:15:05 elrond dhcpd: DHCPREQUEST for 192.168.3.98 from
08:00:27:ad:6f:50 (sauron) via 192.168.3.150
Mar 24 04:15:05 elrond dhcpd: DHCPACK on 192.168.3.98 to 08:00:27:ad:6f:50
(sauron) via 192.168.3.150
Mar 24 04:16:47 elrond dhcpd: DHCPREQUEST for 192.168.2.150 from
08:00:27:f5:e0:5f via eth1
Mar 24 04:16:47 elrond dhcpd: DHCPACK on 192.168.2.150 to 08:00:27:f5:e0:5f
via eth1
Mar 24 04:16:47 elrond dhcpd: DHCPREQUEST for 192.168.2.150 from
08:00:27:f5:e0:5f via 192.168.2.150
Mar 24 04:16:47 elrond dhcpd: DHCPACK on 192.168.2.150 to 08:00:27:f5:e0:5f
via 192.168.2.150
```

dhcrelay

DHCP

DHCP Architecture

DHCP Servers

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

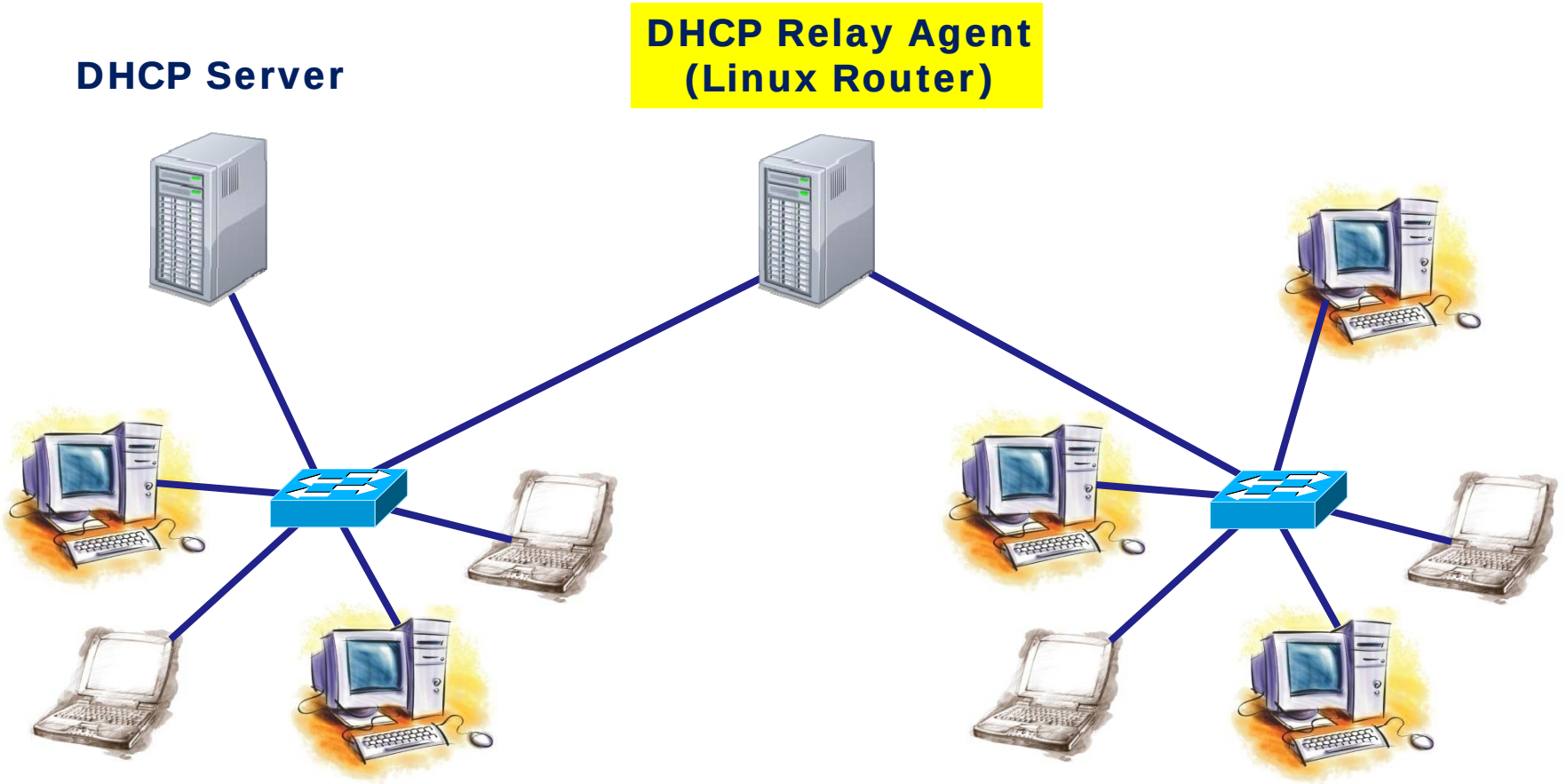
DHCP Relay Agents

DHCP Clients

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

DHCP

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



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

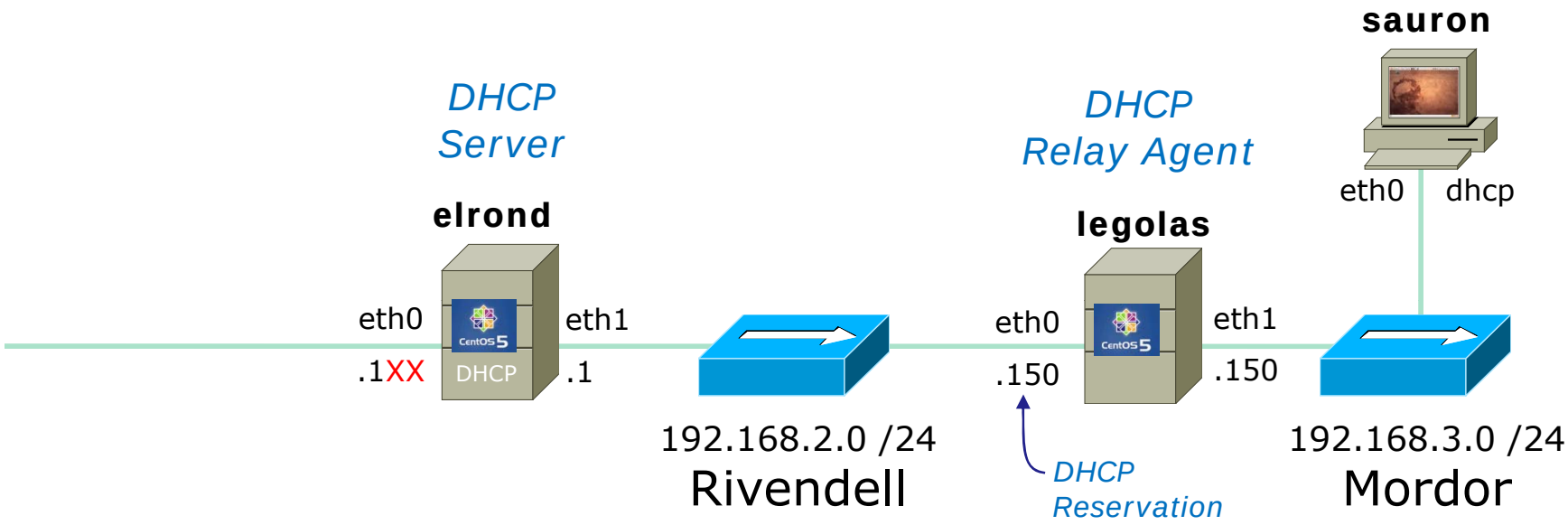
Is it installed?

```
[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 RH-Firewall-1-INPUT 6 -p udp -m udp --dport 67 -j ACCEPT

for default CentOS firewall

To make the firewall settings permanent, backup current permanent settings

iptables-save > /etc/sysconfig/iptables.bak

Save current settings with revised port 67 rule

iptables-save > /etc/sysconfig/iptables

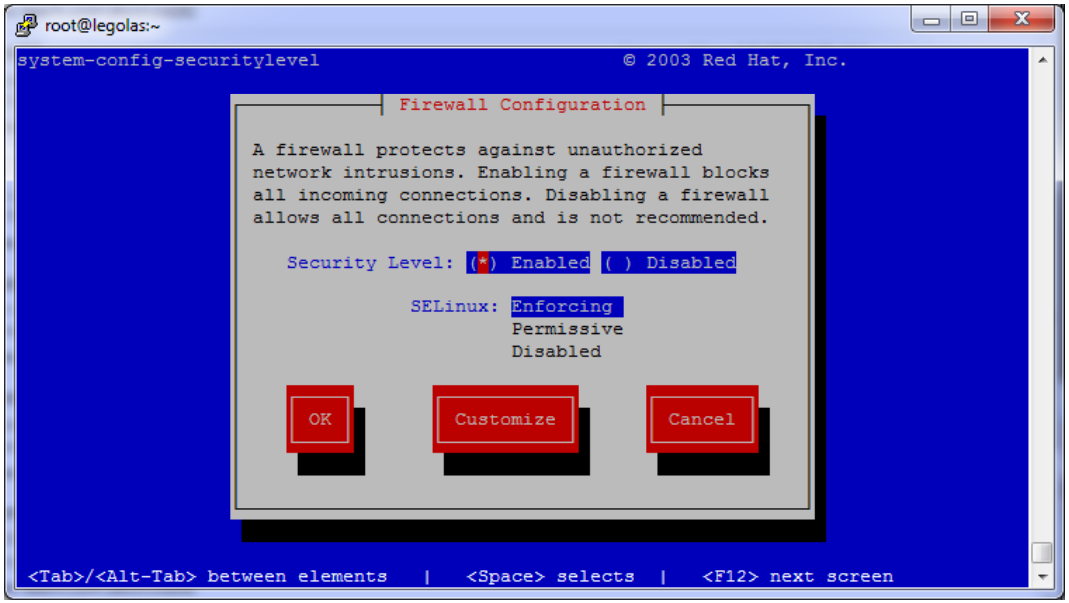
Restart firewall using revised permanent settings

service iptables restart

SELinux for DHCP relay agent (CentOS)

Step 4 *Configure SELinux*


```
[root@legolas ~]# lokkit
```




```
[root@legolas ~]#
```

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
[root@legolas ~]#
```

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 vsftpd

Step 9 Monitor log files

```
[root@arwen ~]# cat /var/log/messages | grep dhcrelay
< snipped >
Mar 24 16:35:02 legolas dhcrelay: Copyright 2004-2006 Internet Systems
Consortium.
Mar 24 16:35:02 legolas dhcrelay: All rights reserved.
Mar 24 16:35:02 legolas dhcrelay: For info, please visit
http://www.isc.org/sw/dhcp/
Mar 24 16:35:03 legolas dhcrelay: Listening on LPF/eth1/08:00:27:dc:43:44
Mar 24 16:35:03 legolas dhcrelay: Sending on   LPF/eth1/08:00:27:dc:43:44
Mar 24 16:35:03 legolas dhcrelay: Listening on LPF/eth0/08:00:27:f5:e0:5f
Mar 24 16:35:03 legolas dhcrelay: Sending on   LPF/eth0/08:00:27:f5:e0:5f
Mar 24 16:35:03 legolas dhcrelay: Sending on   Socket/fallback
[root@legolas ~]#
```

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

```
[root@elrond ~]# cat /var/lib/dhcpd/dhcpd.leases
# All times in this file are in UTC (GMT), not your local timezone.   This is
# not a bug, so please don't ask about it.   There is no portable way to
# store leases in the local timezone, so please don't request this as a
# feature.   If this is inconvenient or confusing to you, we sincerely
# apologize.   Seriously, though - don't ask.
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.0.5-RedHat

lease 172.30.4.83 {
  starts 5 2009/03/20 18:24:00;
  ends 5 2009/03/20 18:33:55;
  tstp 5 2009/03/20 18:33:55;
  binding state free;
  hardware ethernet 00:0c:29:6f:53:d9;
}
lease 172.30.4.83 {
  starts 5 2009/03/20 18:34:02;
  ends 6 2009/03/21 00:34:02;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:6f:53:d9;
  client-hostname "frodo";

< snipped >
```

DHCP

frodo

Lease tracking on Ubuntu client

```
root@frodo:~# cat /var/lib/dhcp3/dhclient.leases
lease {
  interface "eth0";
  fixed-address 172.30.4.83;
  option subnet-mask 255.255.255.0;
  option time-offset -25200;
  option routers 192.168.2.107;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;
  option domain-name-servers 207.62.187.54;
  option dhcp-server-identifier 172.30.4.107;
  option domain-name "shire";
  renew 6 2009/03/21 19:08:50;
  rebind 6 2009/03/21 19:08:50;
  expire 6 2009/03/21 19:08:50;
}
lease {
  interface "eth0";
  fixed-address 172.30.4.83;
  option subnet-mask 255.255.255.0;
  option time-offset -25200;
  option routers 192.168.2.107;

< snipped >
```

DHCP

legolas

Lease tracking on Red Hat client

```
[root@legolas ~]# cat /var/lib/dhclient/dhclient.leases
lease {
  interface "eth0";
  fixed-address 192.168.2.150;
  option subnet-mask 255.255.255.0;
  option time-offset -25200;
  option routers 192.168.2.107;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;
  option domain-name-servers 207.62.187.54;
  option dhcp-server-identifier 192.168.2.107;
  option domain-name "rivendell";
  renew 5 2009/3/20 20:05:02;
  rebind 5 2009/3/20 20:05:02;
  expire 5 2009/3/20 20:05:02;
}
lease {
  interface "eth0";
  fixed-address 192.168.2.150;
  option subnet-mask 255.255.255.0;
  option time-offset -25200;
  option routers 192.168.2.107;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;

< snipped >
```

Wrap

New commands, daemons:

service dhcpd restart

service dhcrelay restart

Daemons and related configuration files

/etc/dhcpd.conf

/etc/sysconfig/dhcrelay

/var/lib/dhcpd/dhcpd.leases

/var/lib/dhclient/dhclient.leases

/var/lib/dhcp3/dhclient.leases (ubuntu)

Next Class

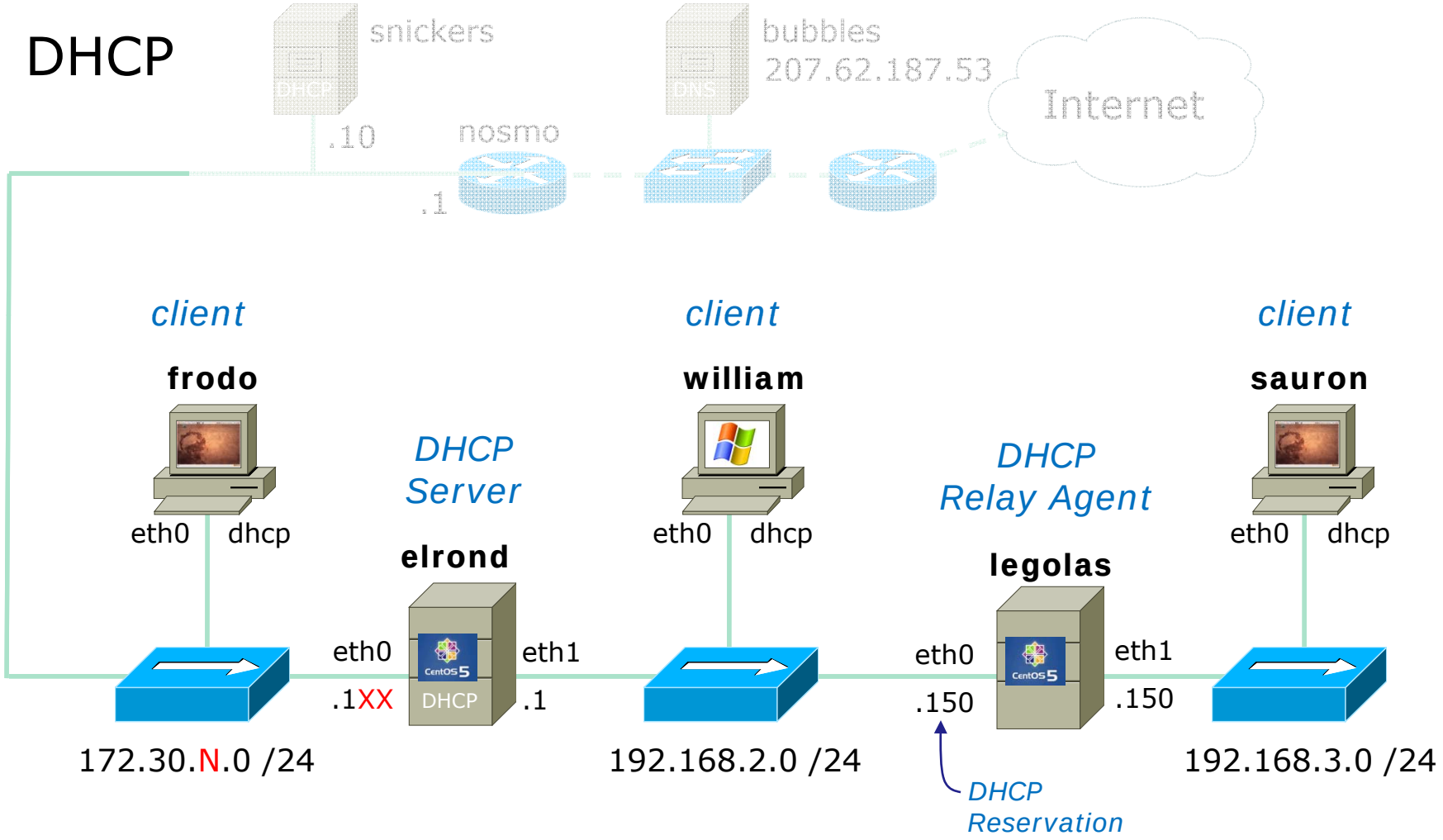
Assignment: Check Calendar Page
http://simms-teach.com/cis192calendar.php

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 6 workshop

DHCP


snickers
DHCP
.10
nosmo
.1
bubbles
207.62.187.53
DNS
Internet
client
frodo
eth0
dhcp
DHCP Server
elrond
eth0
eth1
.1XX
DHCP
.1
client
william
eth0
dhcp
DHCP Relay Agent
legolas
eth0
eth1
.150
.150
client
sauron
eth0
dhcp
172.30.N.0 /24
192.168.2.0 /24
192.168.3.0 /24
DHCP Reservation
Shire
Rivendell
Mordor

Classroom DHCP IP allocation pools table by station number

http://simms-teach.com/docs/static-ip-addrs.pdf

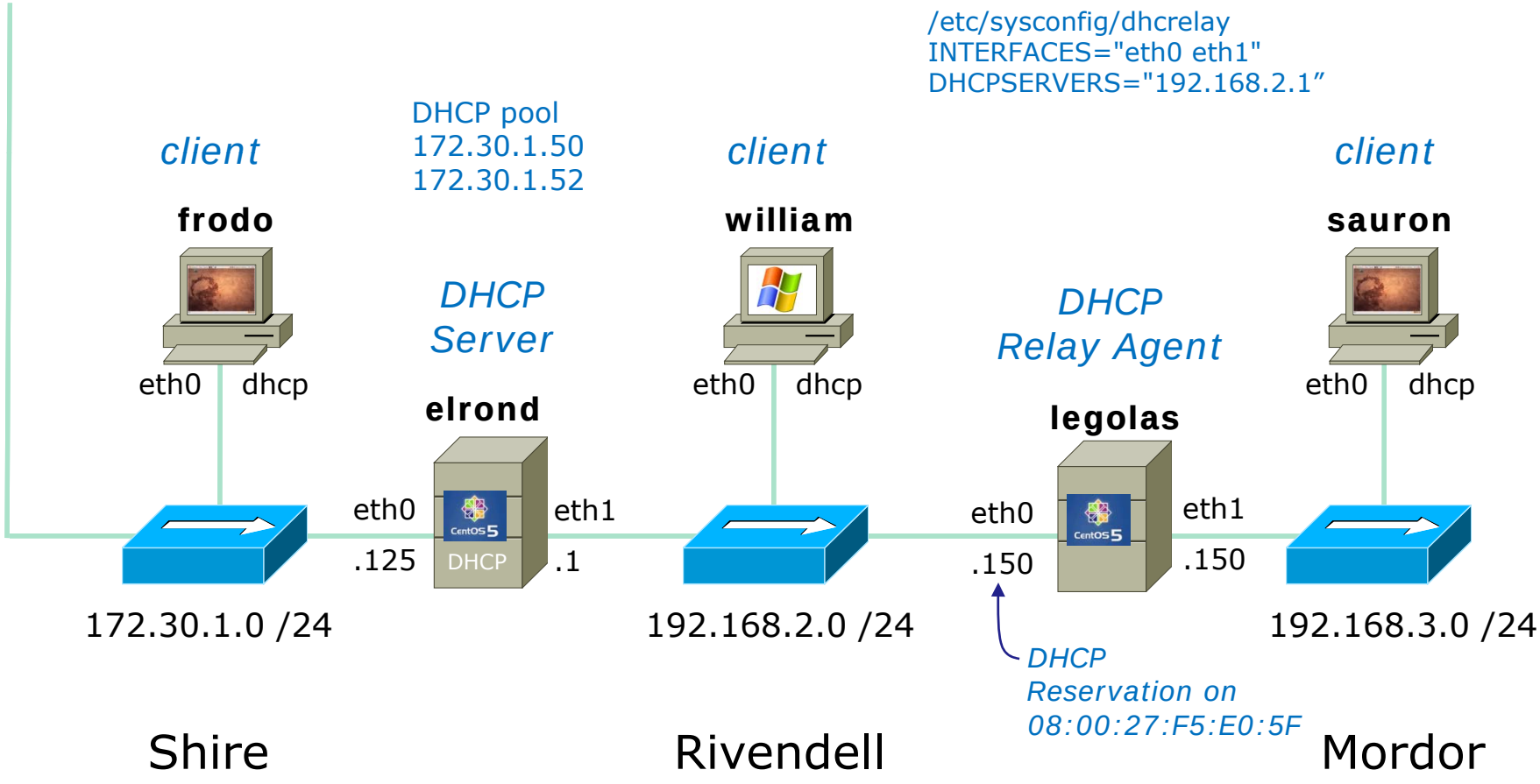
IP Address Assignments for Classroom PCs (Room 2501)

		Static		DHCP Pool	
Station	Station IP	Static 1	Static 2	Start	End
x	172.30.1.	172.30.1.	172.30.1.	172.30.1.	172.30.1.
0	100	125	200	50	52
1	101	126	201	53	55
2	102	127	202	56	58
3	103	128	203	59	61
4	104	129	204	62	64
5	105	130	205	65	67
6	106	131	206	68	70
7	107	132	207	71	73
8	108	133	208	74	76
9	109	134	209	77	79
10	110	135	210	80	82
11	111	136	211	83	85
12	112	137	212	86	88
13	113	138	213	89	91
14	114	139	214	92	94
15	115	140	215	95	97
16	116	141	216	225	227
17	117	142	217	228	230
18	118	143	218	231	233
19	119	144	219	234	236
20	120	145	220	237	239
21	121	146	221	240	242
22	122	147	222	243	245
23	123	148	223	246	248
24	124	149	224	249	251

Use these pools of addresses based on your station number to avoid conflicts on the classroom network

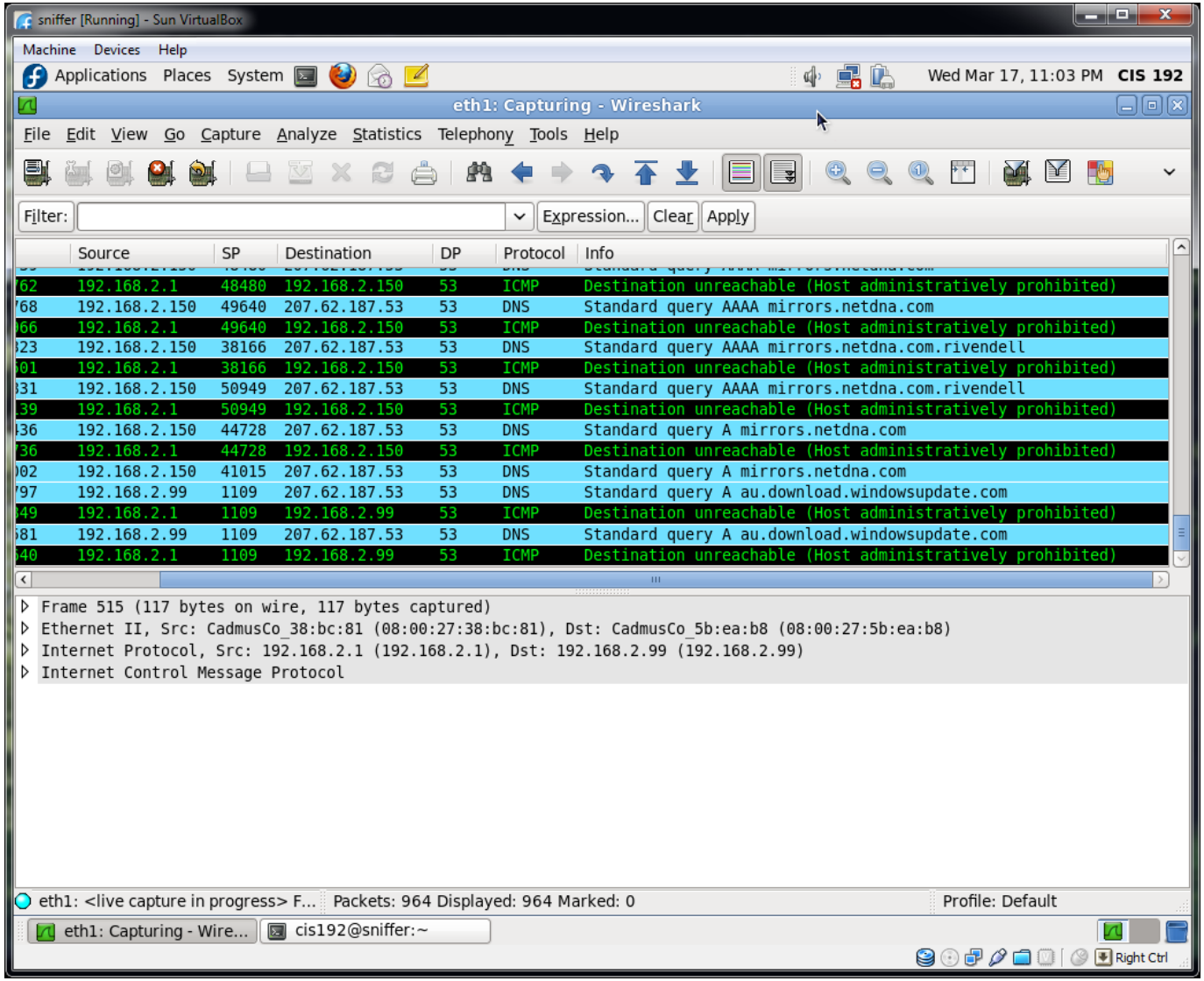
router: 172.30.1.1
dns: 207.62.187.53

iptables –I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 67 -j ACCEPT



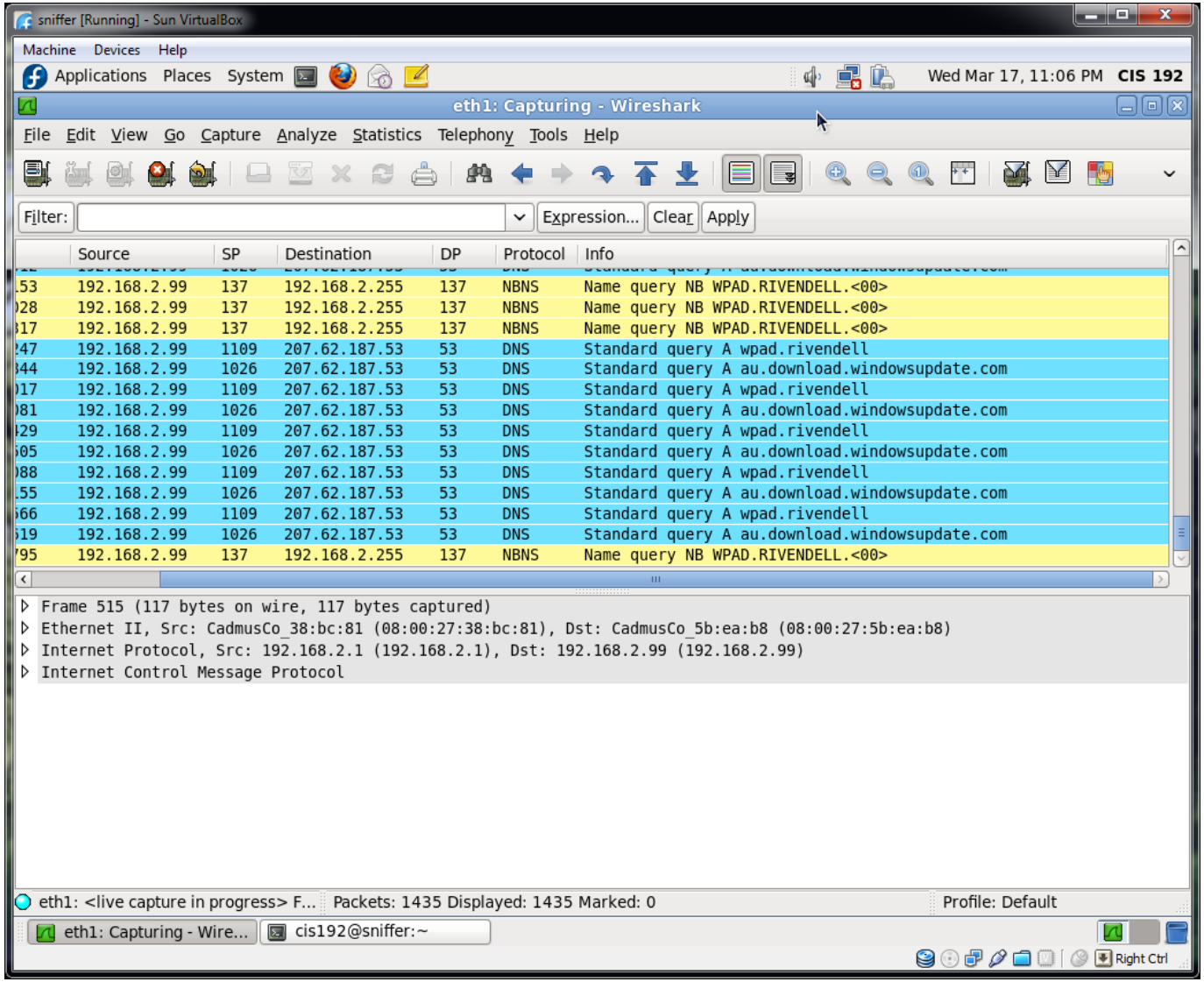
Backup

Note Elrond with default firewall is blocking DNS requests to bubbles and sending back an ICMP error

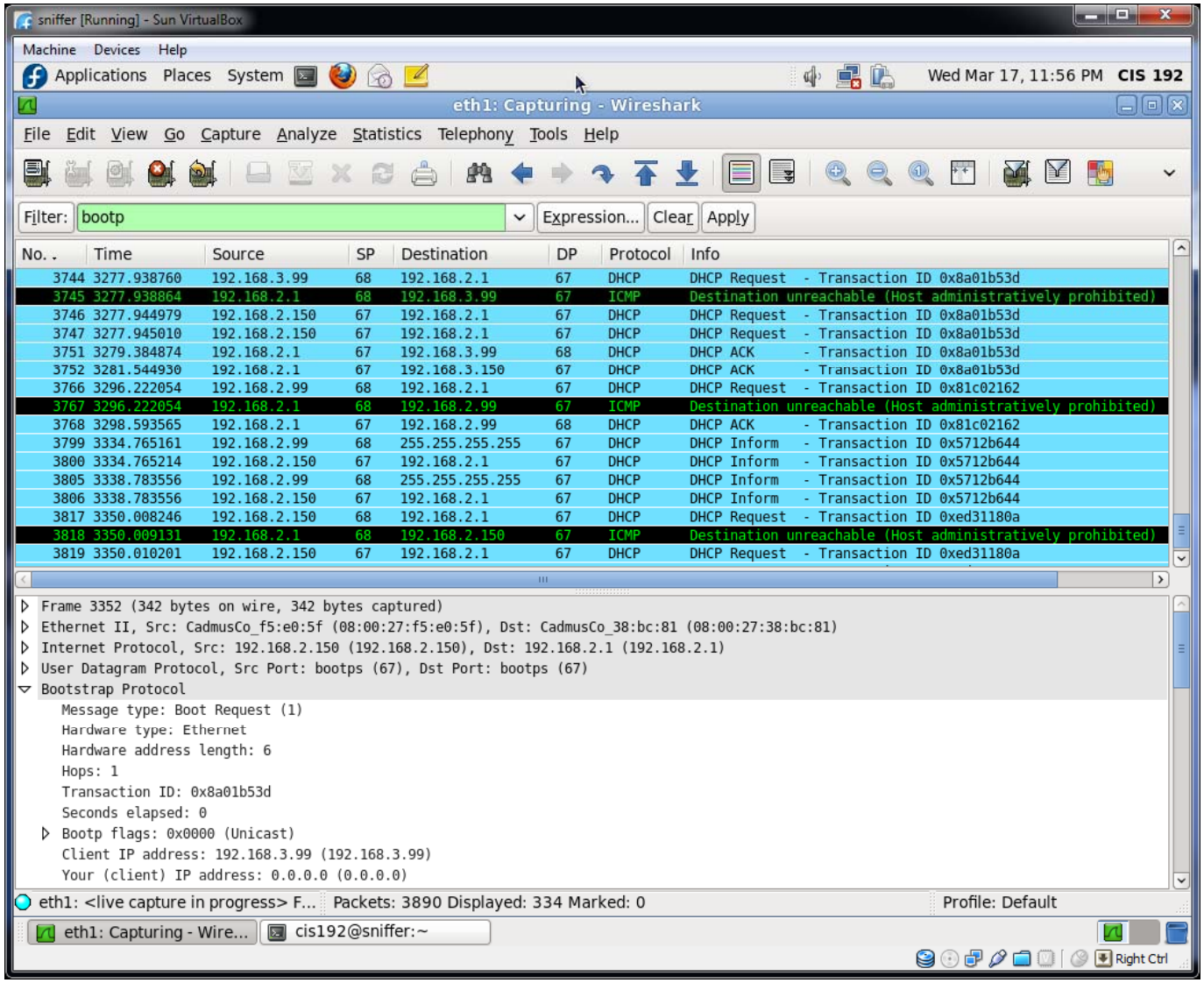


Lab 6, Rivendell network traffic

*After using **iptables –D FORWARD 1** on Elrond allows the packets to be forwarded.*



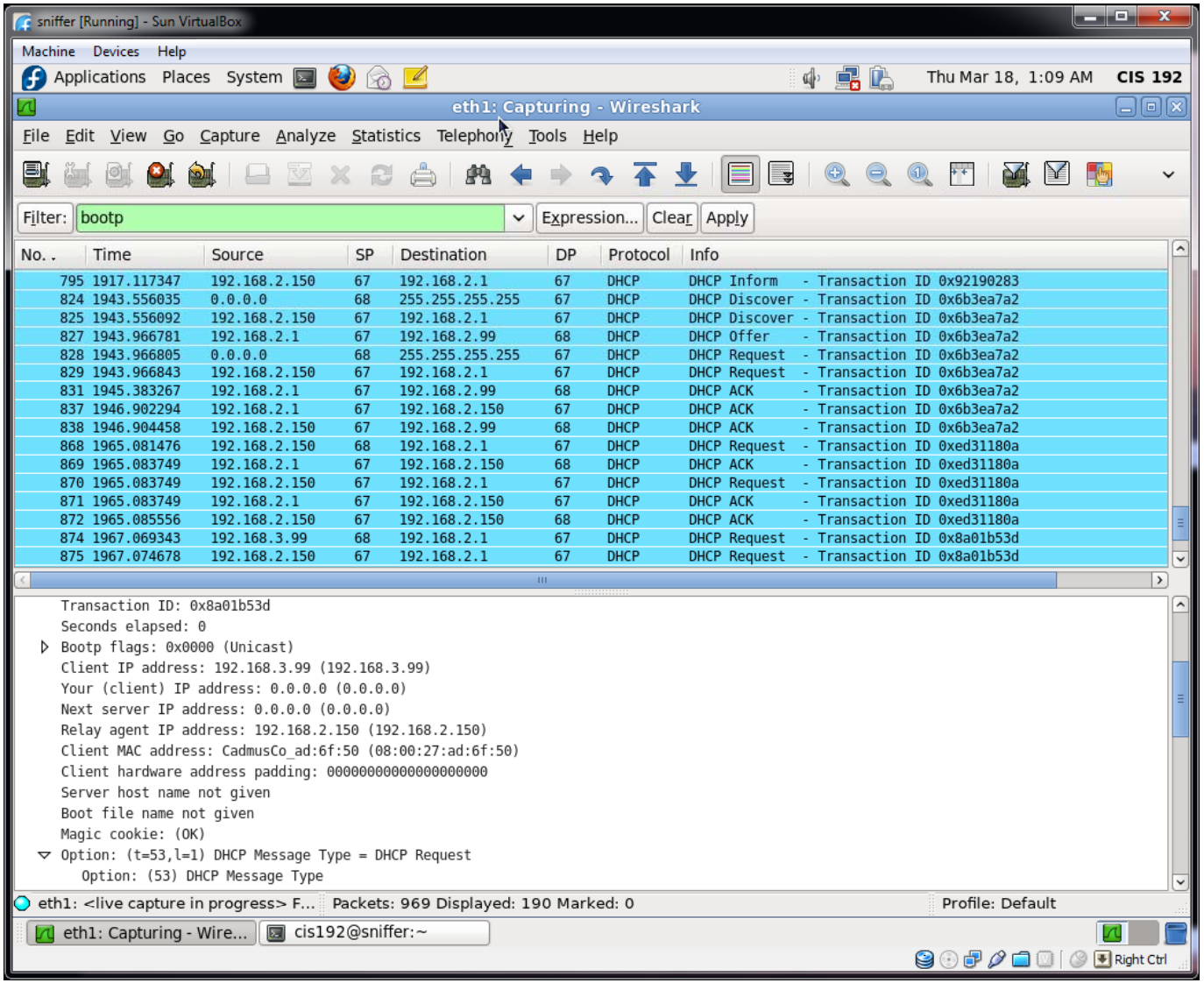
Incoming DHCP Requests to Elrond's UDP port 67 are being rejected



Lab 6, Rivendell network traffic, with 4 minute lease times

After opening port 67 on Elrond with:

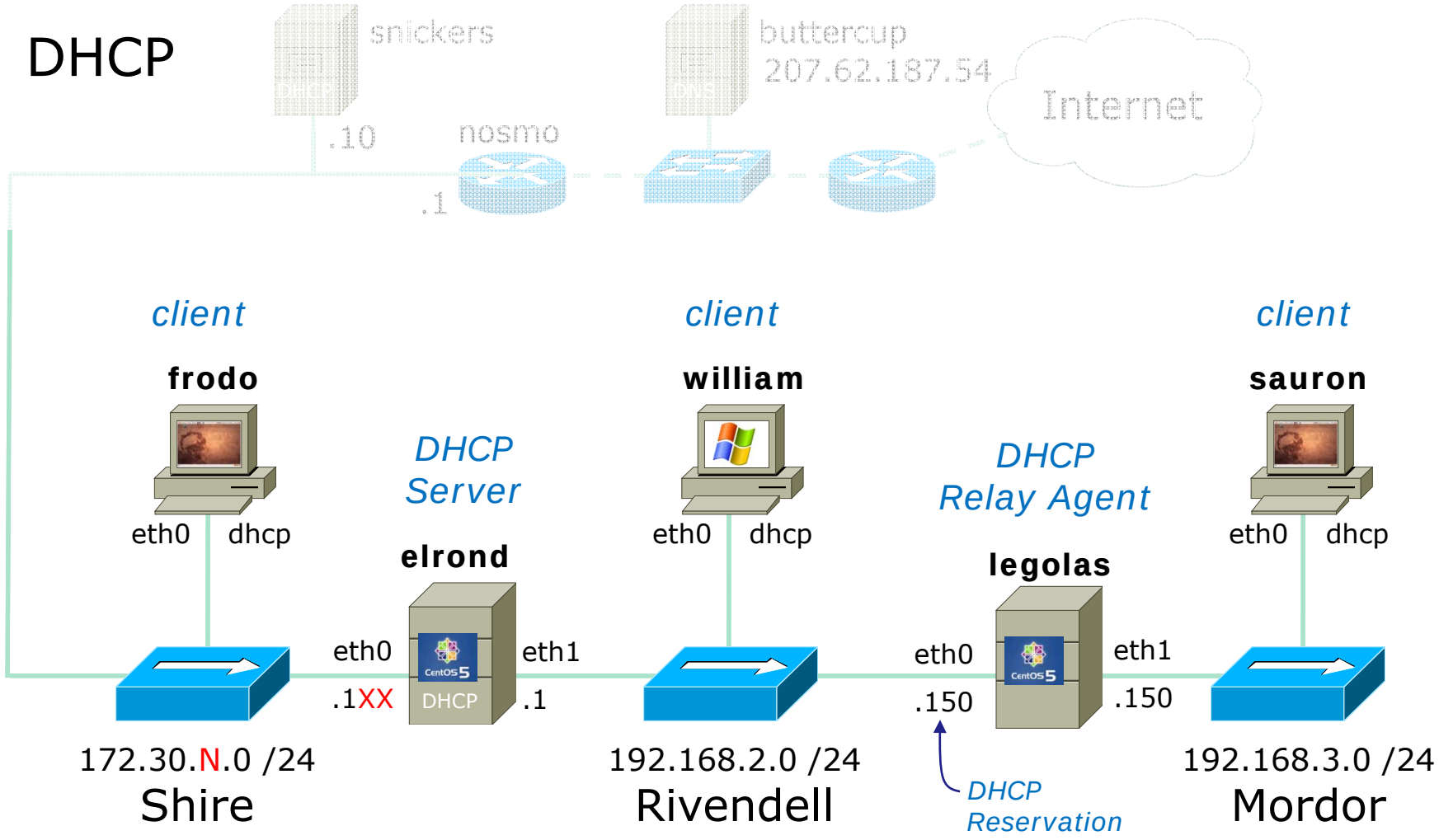
iptables -I RH-Firewall-1-INPUT 9 -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
or ***iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 67 -j ACCEPT***



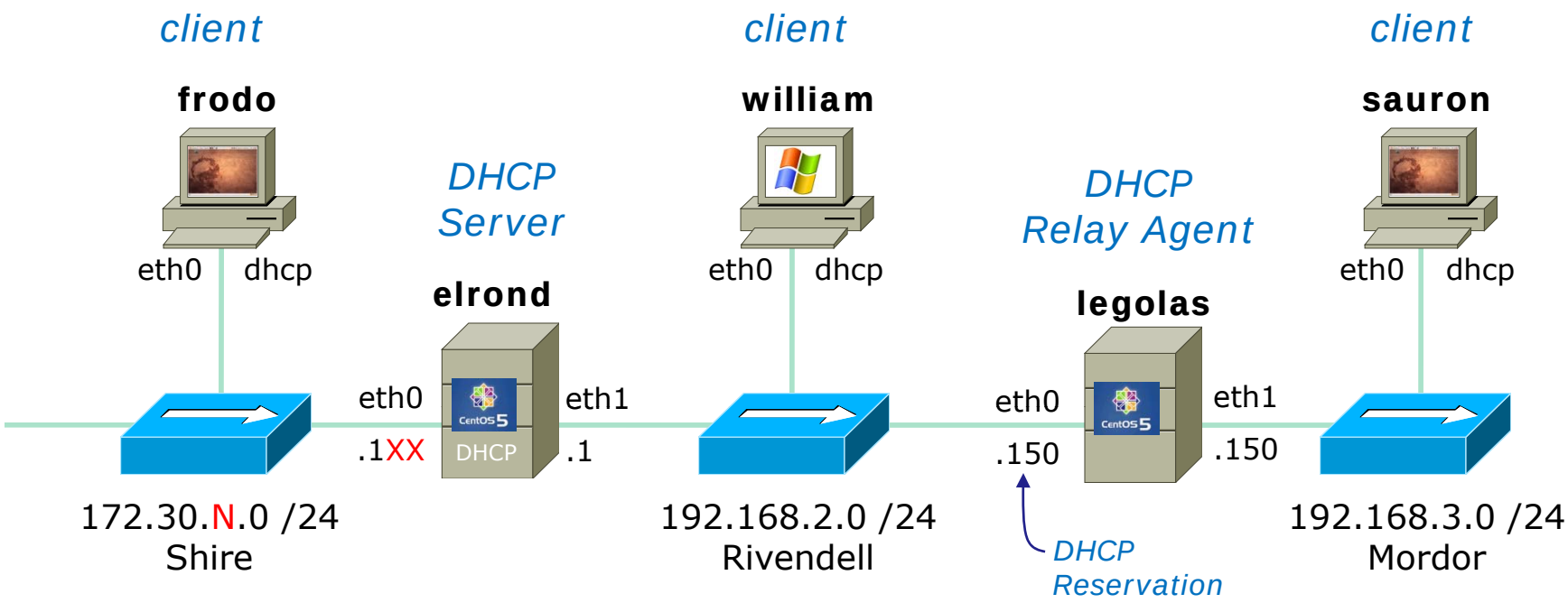
Lab 6, Rivendell network traffic, with 4 minute lease times

DHCP
Lab Prep

DHCP



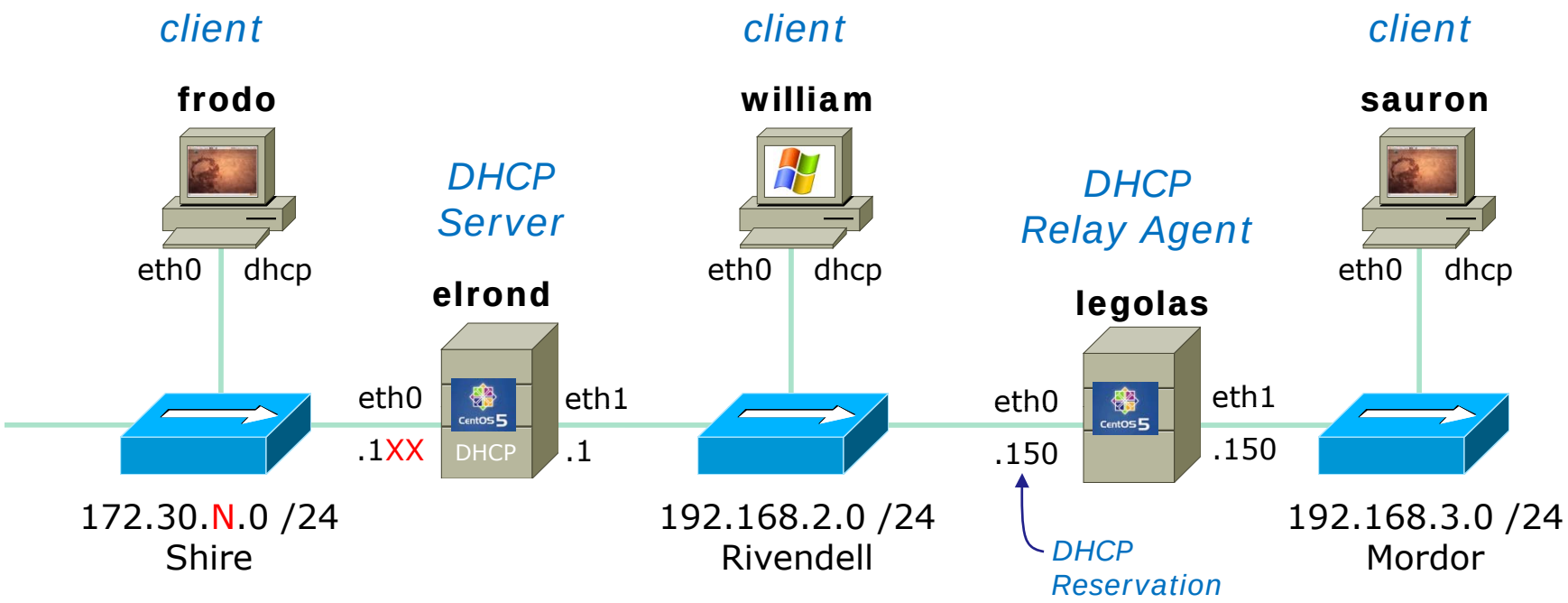
This is what we build for the DHCP lab



VM preparation:

- Revert VMs to the original state
- Cabling

Use VM settings to connect with bridged or specific VMnets



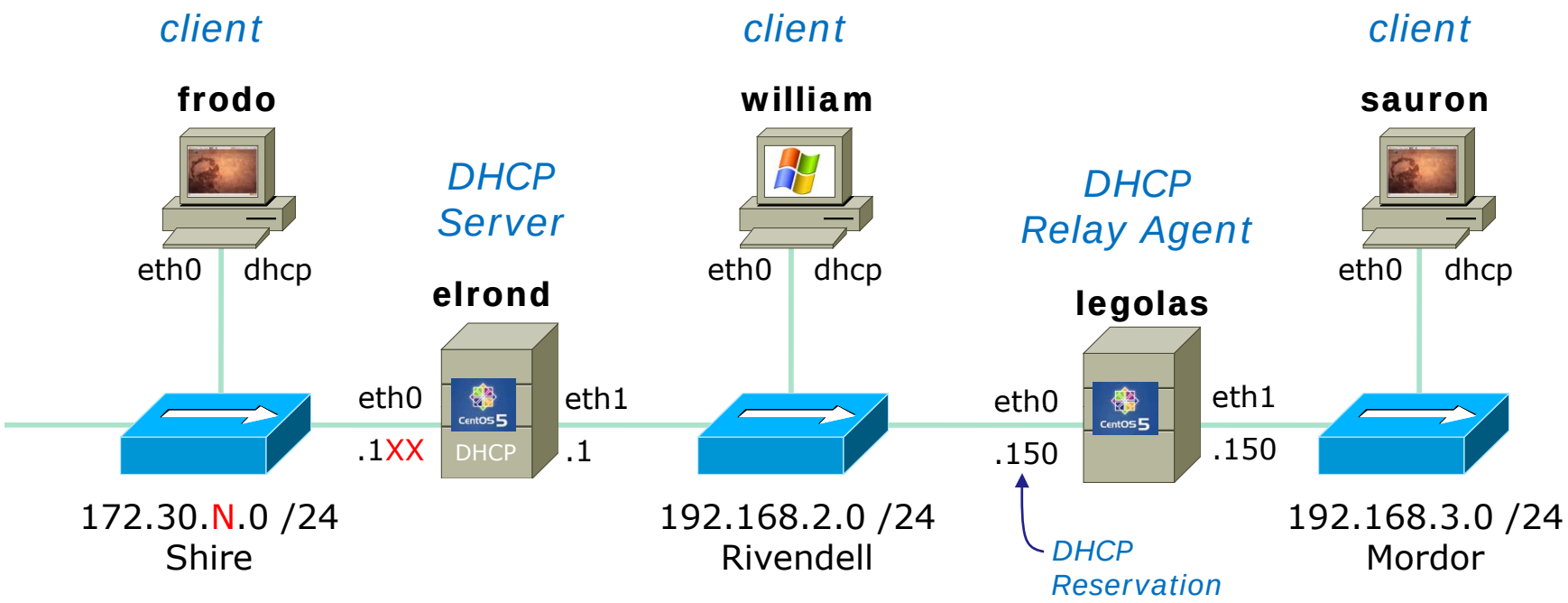
NIC Configuration:

- Frodo, William and Sauron – no changes
- Configure Elrond eth0 and eth1 as shown
- Configure Legolas eth0 as dhcp and eth1 as shown
- Add static routes to get to private networks
- Add default gateways

/etc/sysconfig/network
*/etc/sysconfig/network-scripts/ifcfg-eth**
*/etc/sysconfig/network-scripts/route-eth**
/etc/resolv.conf
/etc/sysctl.conf

service network restart
sysctl –p

ifconfig
route –n
cat /proc/sys/net/ipv4/ip_forward



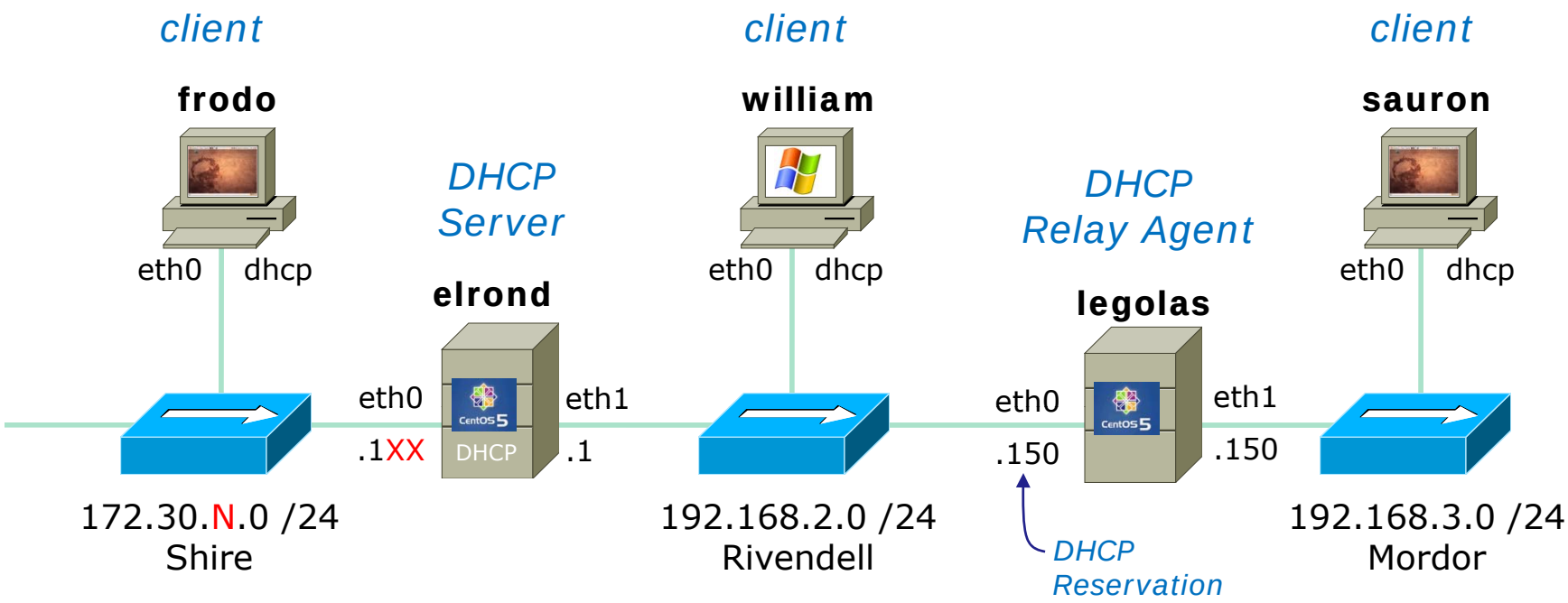
NIC Configuration:

- Frodo, William and Sauron – no changes
- Configure Elrond eth0 and eth1 as shown
- Configure Legolas eth0 as dhcp and eth1 as shown
- Add static routes to get to private networks
- Add default gateways

Ubuntu/Debian:
/etc/network/interfaces
/etc/resolv.conf

/etc/init.d/networking restart

ifconfig
route –n

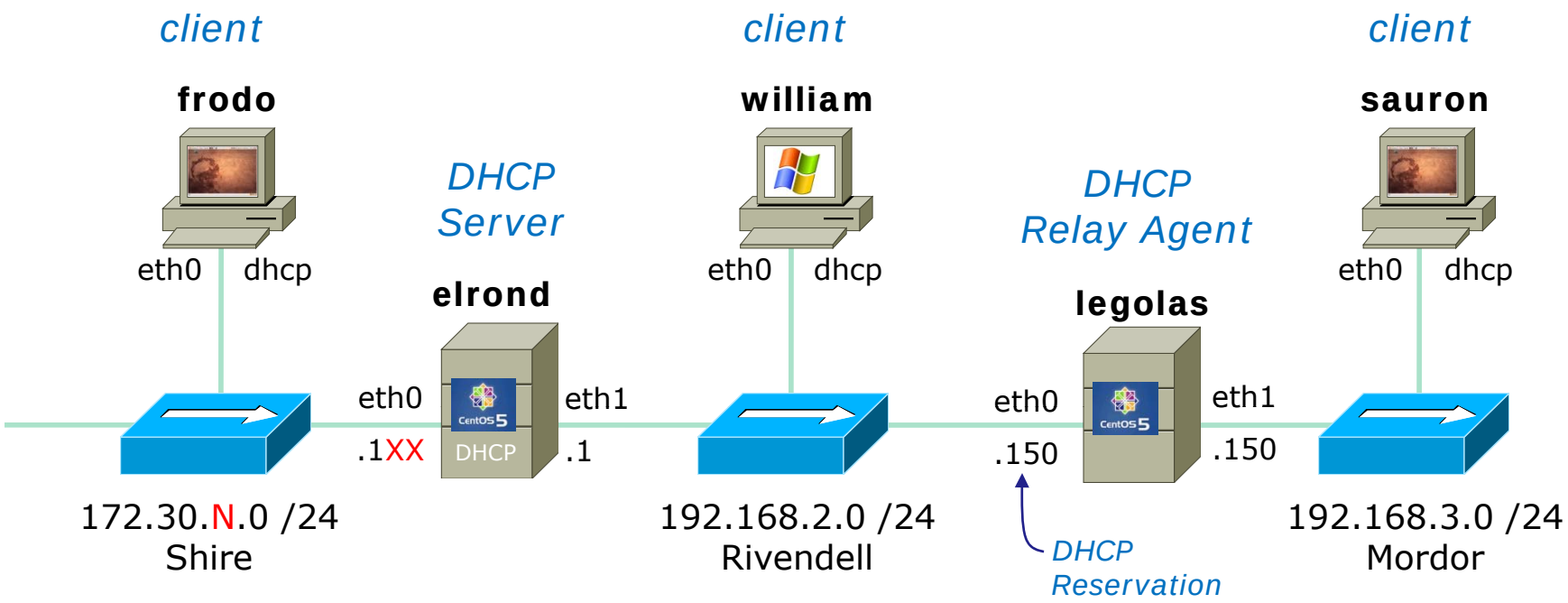


Software Installation:

- Install the dhcp package on Elrond
- Temporarily cable Legolas eth0 to Shire and install dhcp package

yum install xxxxx
rpm –qa | grep xxxxx

Temporary hookups:
- *Use bridged connection*
- *use dhclient (to get an IP)*
- *Install software*
- *dhclient –r (to release IP)*

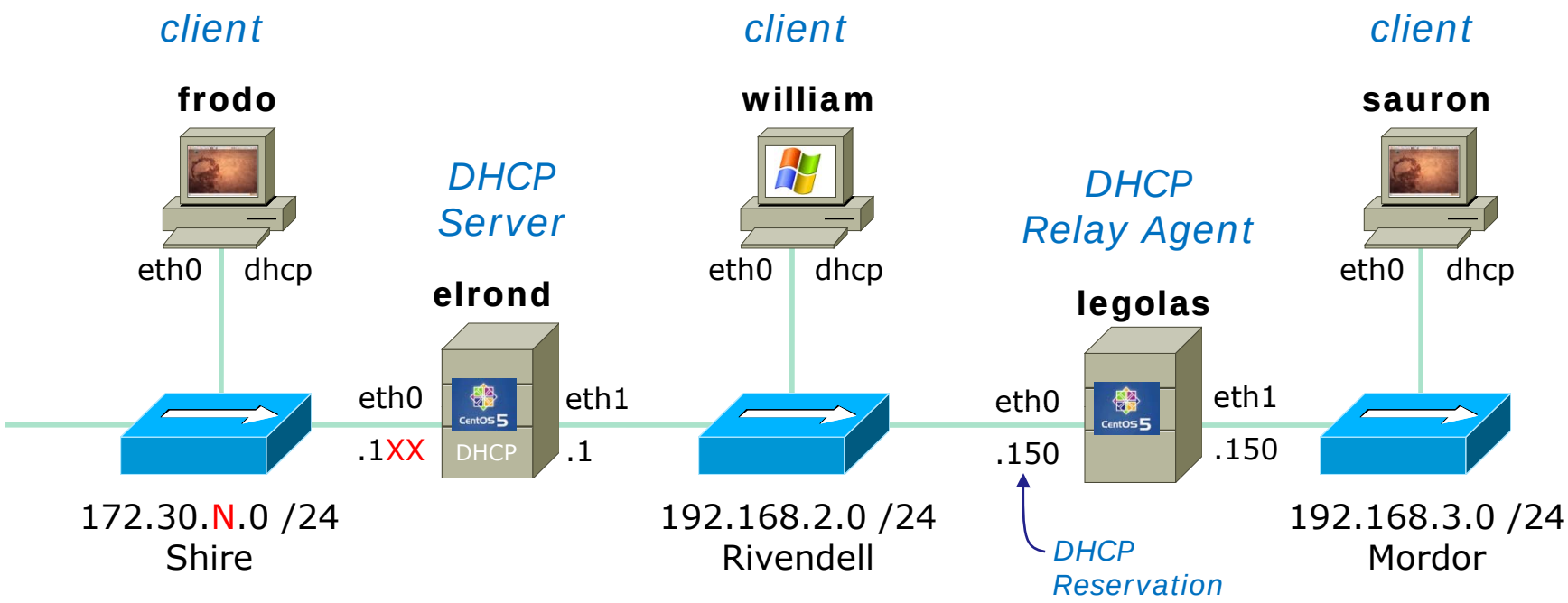


Configure service:

- Edit /etc/dhcpd.conf on Elrond
- Edit /etc/sysconfig/dhcrelay on Legolas
- Start services

vi /etc/xxxx.xxxx
service xxxx start
chkconfig xxxxx on

service xxxxx status
chkconfig --list

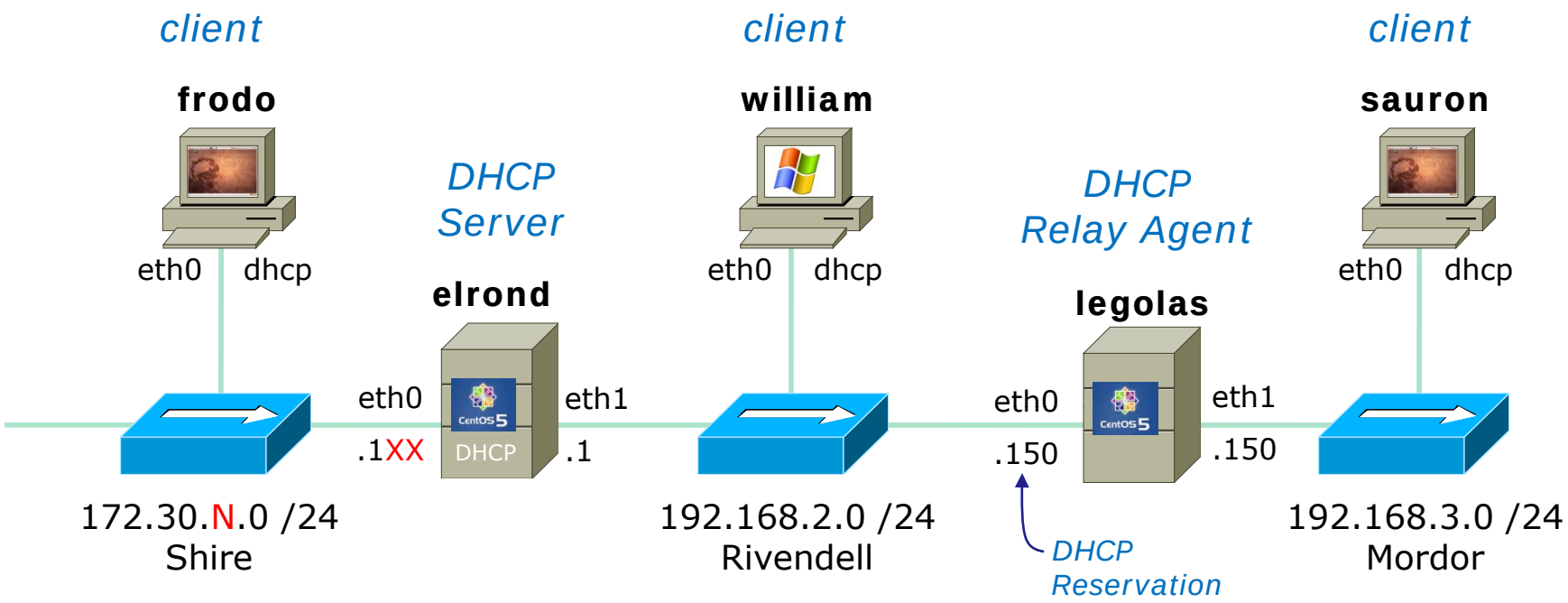


Configure security:

- Firewalls
- SELinux setting

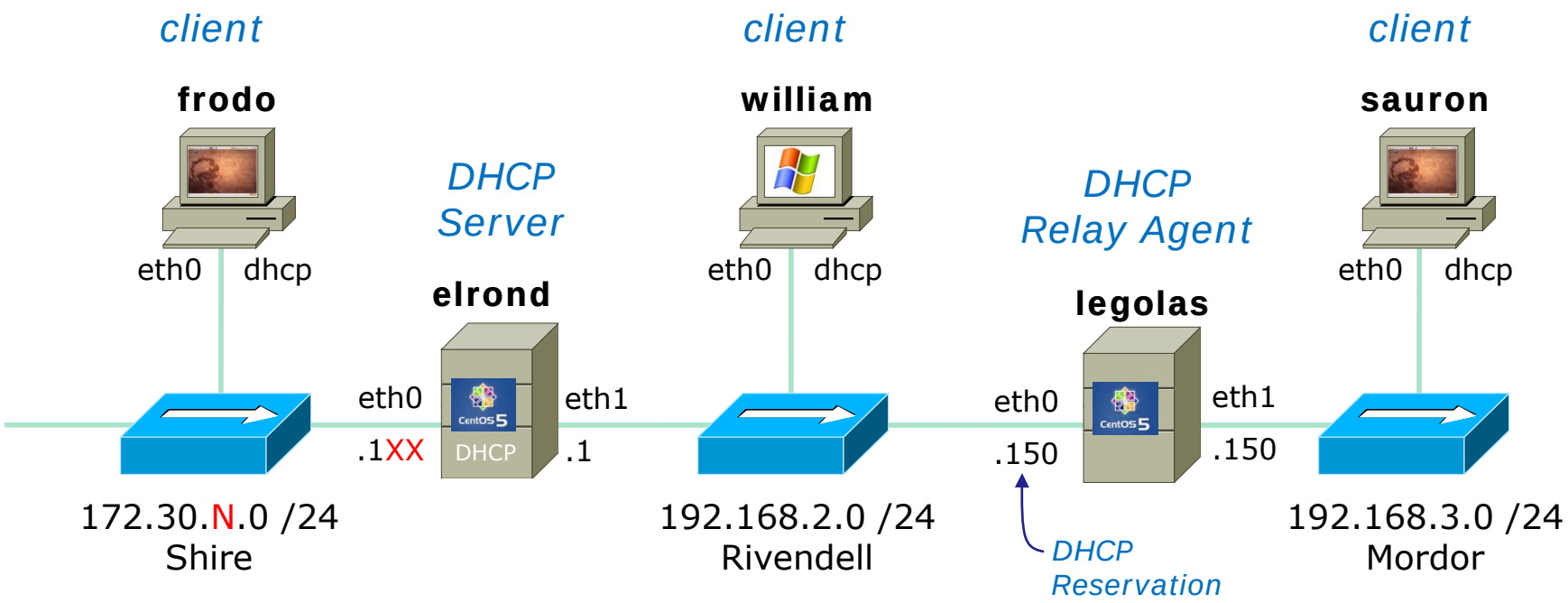
When doing lab assignments it may be helpful to temporarily disable security settings while you initially implement a new service. If real life this may not be possible!

lokkit
iptables –F
iptables –L
Graphical security utility



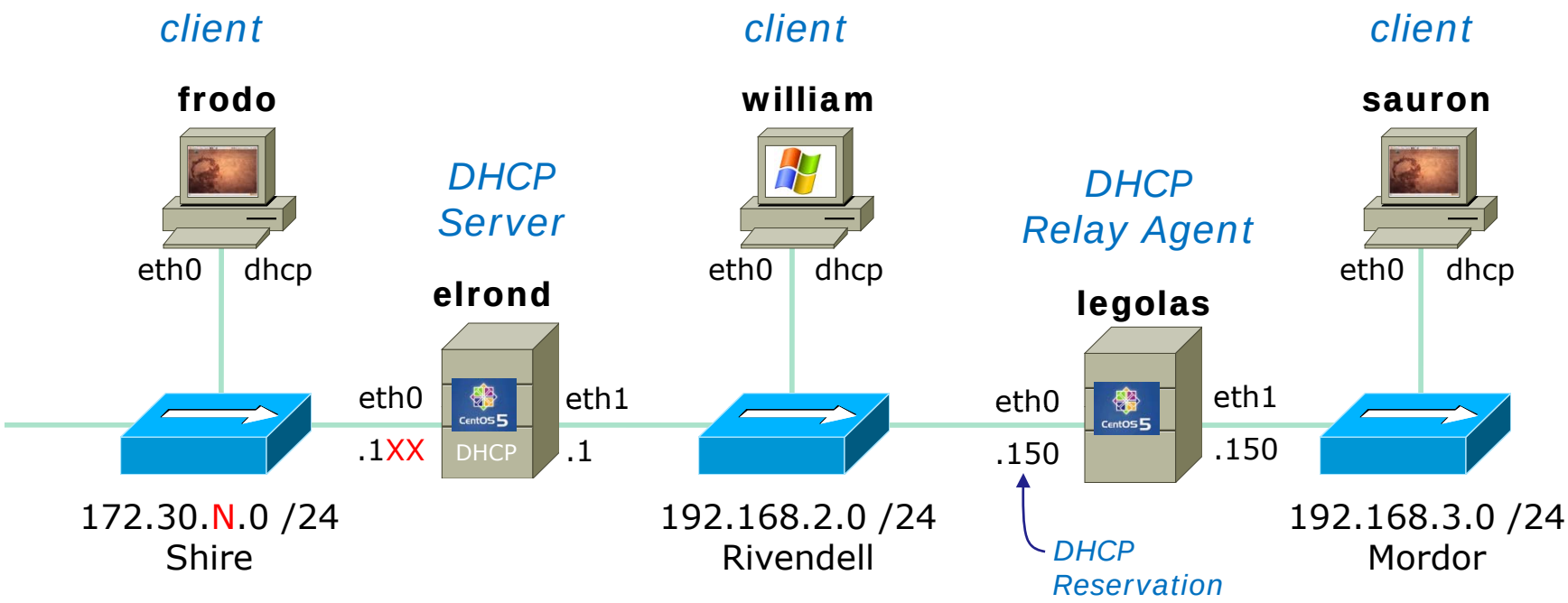
Test new service:

- Power up Frodo, William and Sauron and check if they get IP and related settings via your DHCP service
- Check that Legolas eth0 got it's reserved IP address



Troubleshoot:

- Cabling
- NIC configuration
- Routing tables and IP forwarding
- Firewall/SELinux
- Configuration files edits
- /var/log messages
- Rogue Nosmos
- Duplicate IP addresses
- Incomplete ARP tables (arp –n)



Document:

- Network map
- NIC configuration files
- ifconfig and route –n output
- Service configuration files
- Specific files for the lab

Red Hat server
/var/lib/dhcpd/dhcpd.leases

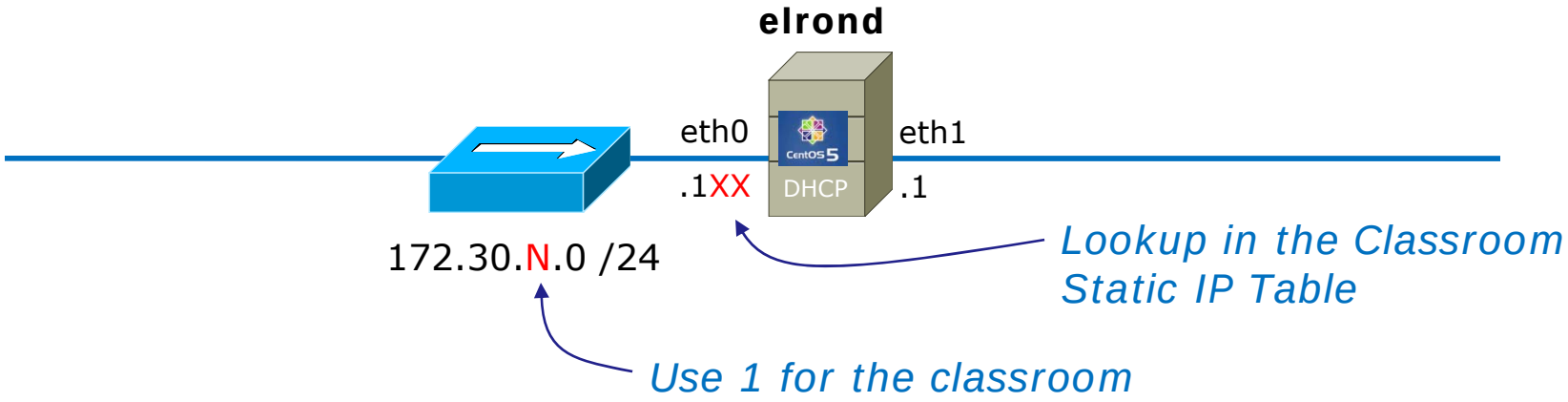
Red Hat client
/var/lib/dhclient/dhclient.leases

Ubuntu client
/var/lib/dhcp3/dhclient.leases

Exercise

elrond

- Revert Elrond to it's snapshot
- Power up Elrond
- Login as root, **startx &** (for graphical desktop)
- Graphical terminal, use **vmware-toolbox &**
- Configure Elrond (use following slides)
- **service network restart** (enable configured network settings)
- **sysctl –p** (enable forwarding)
- Install the dhcp server with **yum install dhcp**



Exercise

elrond


```
[root@elrond ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
ONBOOT=yes
HWADDR=00:0c:29:4e:21:9b
BOOTPROTO=static
IPADDR=172.30.N.1XX
NETMASK=255.255.255.0
BROADCAST=172.30.N.255
[root@elrond ~]#

[root@elrond ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth1
ONBOOT=yes
HWADDR=00:0c:29:4e:21:a5
BOOTPROTO=static
IPADDR=192.168.2.1
NETMASK=255.255.255.0
BROADCAST=192.168.2.255
[root@elrond ~]#
```

Use you own MAC addresses!

Use you own MAC addresses!

.1XX is based on your station number and the Classroom IP Table
N=1 for the classroom and N=4 for the CIS lab or CTC

IP addresses for VM's in the classroom

Station	IP	Static 1
Instructor	172.30.1.100	172.30.1.125
Station-01	172.30.1.101	172.30.1.126
Station-02	172.30.1.102	172.30.1.127
Station-03	172.30.1.103	172.30.1.128
Station-04	172.30.1.104	172.30.1.129
Station-05	172.30.1.105	172.30.1.130
Station-06	172.30.1.106	172.30.1.131
Station-07	172.30.1.107	172.30.1.132
Station-08	172.30.1.108	172.30.1.133
Station-09	172.30.1.109	172.30.1.134
Station-10	172.30.1.110	172.30.1.135
Station-11	172.30.1.111	172.30.1.136
Station-12	172.30.1.112	172.30.1.137

Station	IP	Static 1
Station-13	172.30.1.113	172.30.1.138
Station-14	172.30.1.114	172.30.1.139
Station-15	172.30.1.115	172.30.1.140
Station-16	172.30.1.116	172.30.1.141
Station-17	172.30.1.117	172.30.1.142
Station-18	172.30.1.118	172.30.1.143
Station-19	172.30.1.119	172.30.1.144
Station-20	172.30.1.120	172.30.1.145
Station-21	172.30.1.121	172.30.1.146
Station-22	172.30.1.122	172.30.1.147
Station-23	172.30.1.123	172.30.1.148
Station-24	172.30.1.124	172.30.1.149

Only use the static IP address shown in this table for your classroom PC VM to avoid IP address conflicts

Exercise

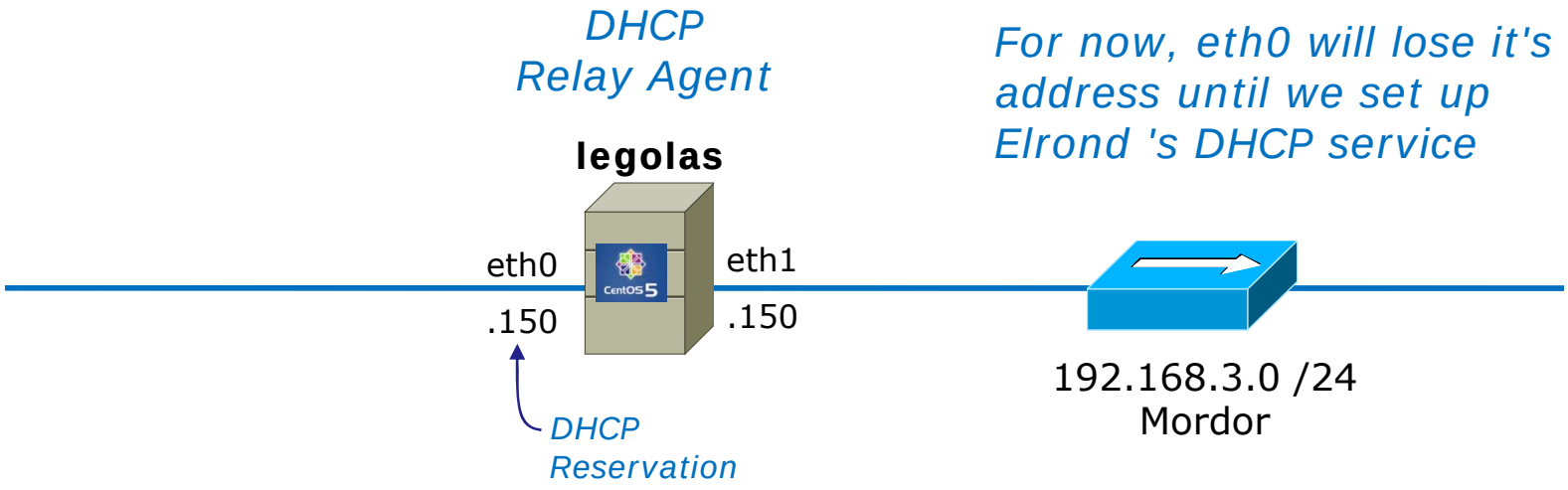
elrond


```
[root@elrond ~]# cat /etc/sysconfig/network-scripts/route-eth1
192.168.3.0/24 via 192.168.2.150
[root@elrond ~]#

[root@elrond ~]# cat /etc/resolv.conf
nameserver 207.62.187.54
[root@elrond ~]#

[root@elrond ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=elrond.localdomain
GATEWAY=172.30.N.1
[root@elrond ~]#

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

N=1 for the classroom and N=4 for the CIS lab or CTC

Exercise

- Revert Legolas to it's snapshot
- Power up Legolas
- Login as root, **startx &** (for graphical desktop)
- Graphical terminal, use **vmware-toolbox &**
- Temporarily cable eth0 to the classroom network (bridged)
- Temporarily connect with dhclient eth0
- Install the dhcp server with **yum install dhcp**
- Recable and finish configuring Legolas (use following slides)
- **service network restart** (enable configured network settings)
- **sysctl –p** (enable forwarding)



Exercise

legolas


```
[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
```

Use you own MAC addresses!

```
[root@legolas ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth1
HWADDR=00:0C:29:7C:18:FF
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.3.150
NETMASK=255.255.255.0
BROADCAST=192.168.3.255
```

Use you own MAC addresses!

Exercise

legolas


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

Don't configure /etc/sysconfig/network or /etc/resolv.conf

We will get default route, DNS settings using DHCP instead