Lesson Module Status

- Wall updated and emailed

- Slides –
- Properties -
- Flashcards -
- 1st minute quiz –
- Web Calendar summary –
- Web book pages –
- Commands –
- Howtos –

- Lab tested –
- Lab template in depot -
- Youtube Videos uploaded –

- VM (Classroom PC) –
- VMs (VLab) - extra gondor and arnor switches made for each pod

- Headset charged –

[ ] Has the phone bridge been added?

[ ] Is phone being used for voice input?

[ ] Is recording on?

[ ] Share slides, multiple Putties started, Chrome, vlab192.rdp, VMware Workstation, wireshark

[ ] Disable spelling on PowerPoint

[ ] Repeat all ?'s for remote students

[ ] Remote student proxy

Course history and credits

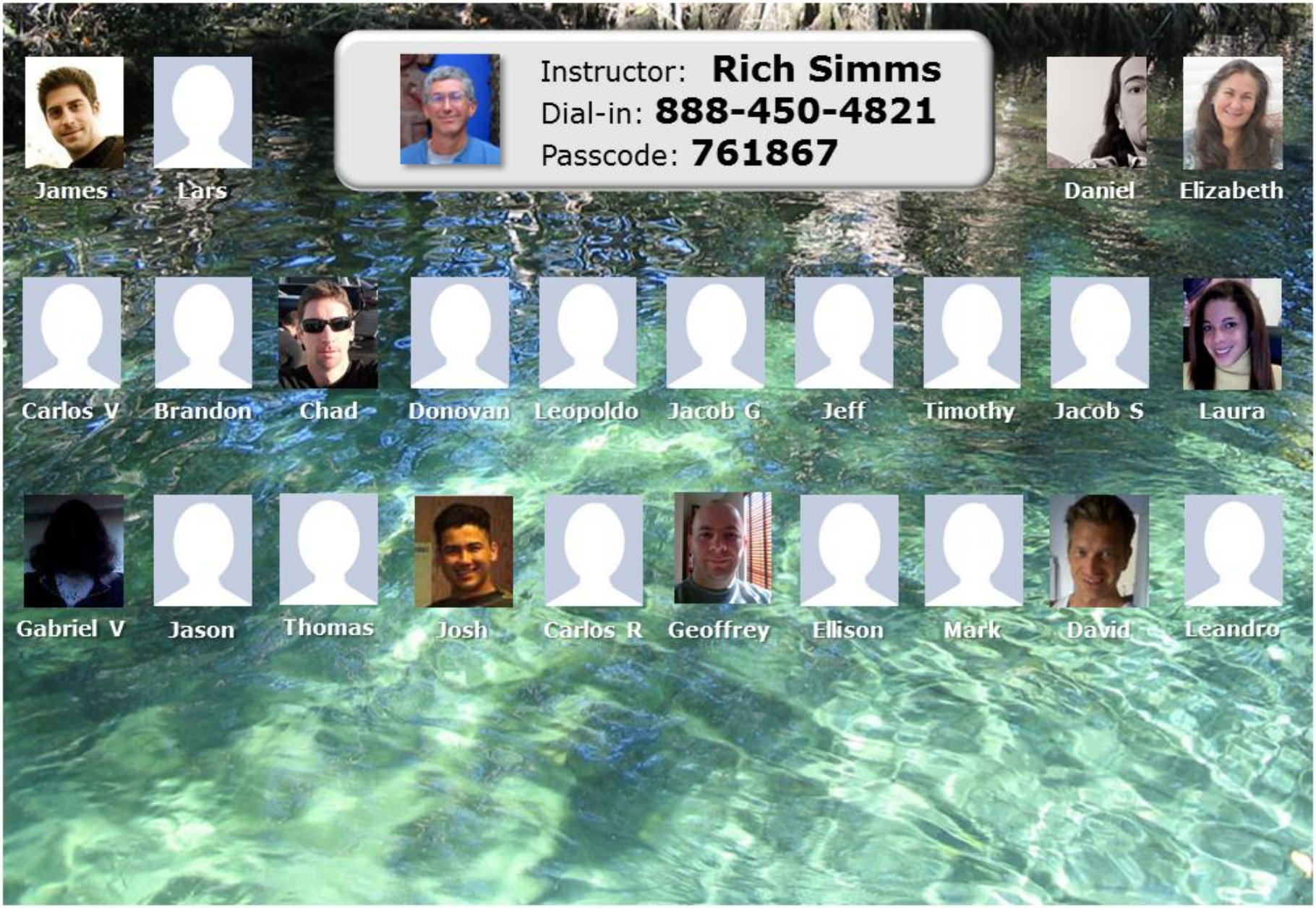
Jim Griffin

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

Rick Graziani

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

CIS 192 – Lesson 6



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

First Minute Quiz

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

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

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 • Housekeeping • Troubleshooting vsftp • FTP (more) • Firewalls (more) • DHCP • DHCP Lab • Wrap

Questions on previous material

Questions?

- Previous lesson material
- Lab assignments

Brainteasers (from last week)

1. NIC order vs eth*n* order – watch out!
   - Observed mismatch on Pods 1, 4, 6
   - Check MAC address on NIC (VM Settings) with interface (ifconfig)
   - Compare with: /etc/udev/rules.d/70-persistent-net.rules

2. Can't ping a systems "far interface" when the return route is different
   - Replaced RIP with static routes = same behavior
   - Set SELinux to permissive = same behavior
   - Some kind of reflexive DOS prevention? ... TBD
   - /etc/resolv.conf (10.240.1.2 vs 192.168.0.8) … TBD
   - Try using older distros, like good ole RH9 ... TBD
   - Try physical computers … TBD

Lab 4 update

Re: May others avoid my mistakes

by **Rich Simms** » Thu Nov 24, 2011 2:15 pm

> **ellison marks wrote:**
> Also, an interesting special case, when the lab should be completed, elrond is unable to successfully ping legolas' .5 interface. The routing table have the ping going out elrond's .10 to arwen's .9, out arwen's .6 to legolas' .5, and out legolas' .2 to elrond's .1. It should have got there, but tcpdump doesn't show anything leaving legolas, though it shows the echo request arriving.

Ahhh ... found the reason for this. This ping behavior doesn't happen with older distributions, like RH9. It does happen though with our CentOS 6.0 VMs. The replies are being dropped whenever the ping return path differs from the path the ping arrived on. This filtering can be disabled by doing the following on Elrond, Legolas and Arwen:

CODE: SELECT ALL

```
[root@arwen ~]# echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
[root@arwen ~]# echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
```

For more details see: http://lartc.org/howto/lartc.kernel.html

Ok ... mystery solved, its time to enjoy Thanksgiving dinner now!

Housekeeping

- Lab 5 due midnight tonight!
- One more class, then final exam
- Final exam
  - Is time based (2 hours 50 minutes)
  - You get a copy of the exam a week in advance.
  - If you cannot take the exam in the classroom, then you need to make alternate arrangements with the instructor.
  - Multiple levels – the more you complete the more points you earn.
  - Some "uncapped" extra credit will be available for doing some additional levels.
  - Collaboration on the forum is OK prior to taking the test, but during the test no giving or receiving assistance is allowed.

aragorn	191
arwen	180
bombadil	195
denethor	159
dwalin	118
elrohir	180
elrond	202
eomer	162
faramir	103
frodo	189
gimli	154
goldberry	111
gwaihir	154
ioreth	154
legolas	221
nazgul	107
pippin	137
samwise	135
saruman	166
strider	157
theoden	185
treebeard	129

Grades Check

(as of 11/29/2011)

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	293 or higher	A	pass
80% to 89.9%	260 to 292	B	pass
70% to 79.9%	228 to 259	C	pass
60% to 69.9%	195 to 227	D	no pass
0% to 59.9%	0 to 194	F	no pass

Remaining Points to earn

Lab 5 = 30 points
Lab 6 = 30 points
Final Exam = 60 points
Forum 2 = 20 points
Quiz 4 = 3 points
Quiz 5 = 3 points

} 146 points

Extra credit maximum = 60 points

Group Troubleshooting

A friend of ours has installed FTP and says nothing is working!

Let's figure out what is wrong and get it going

FTP (revised)

vsftpd

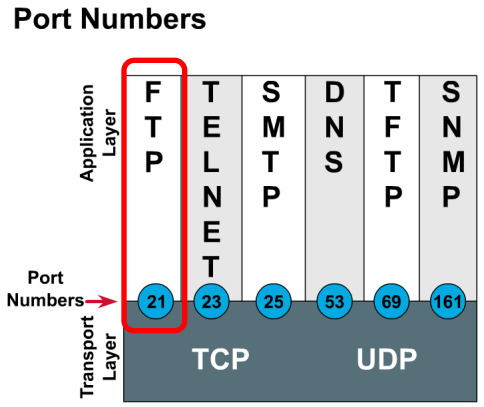
Installing and Configuring Telnet (Red Hat Family)

FTP

- File transfer protocol
- Client-server model
- Uses port 20 (for data) and 21 (for commands)
- Not secure, uses clear text over the network that can be sniffed

FTP uses ports 20 and 21

```
[root@elrond bin]# cat /etc/services
< snipped >
ftp-data        20/tcp
ftp-data        20/udp
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
< snipped >
[root@elrond bin]#
```



FTP

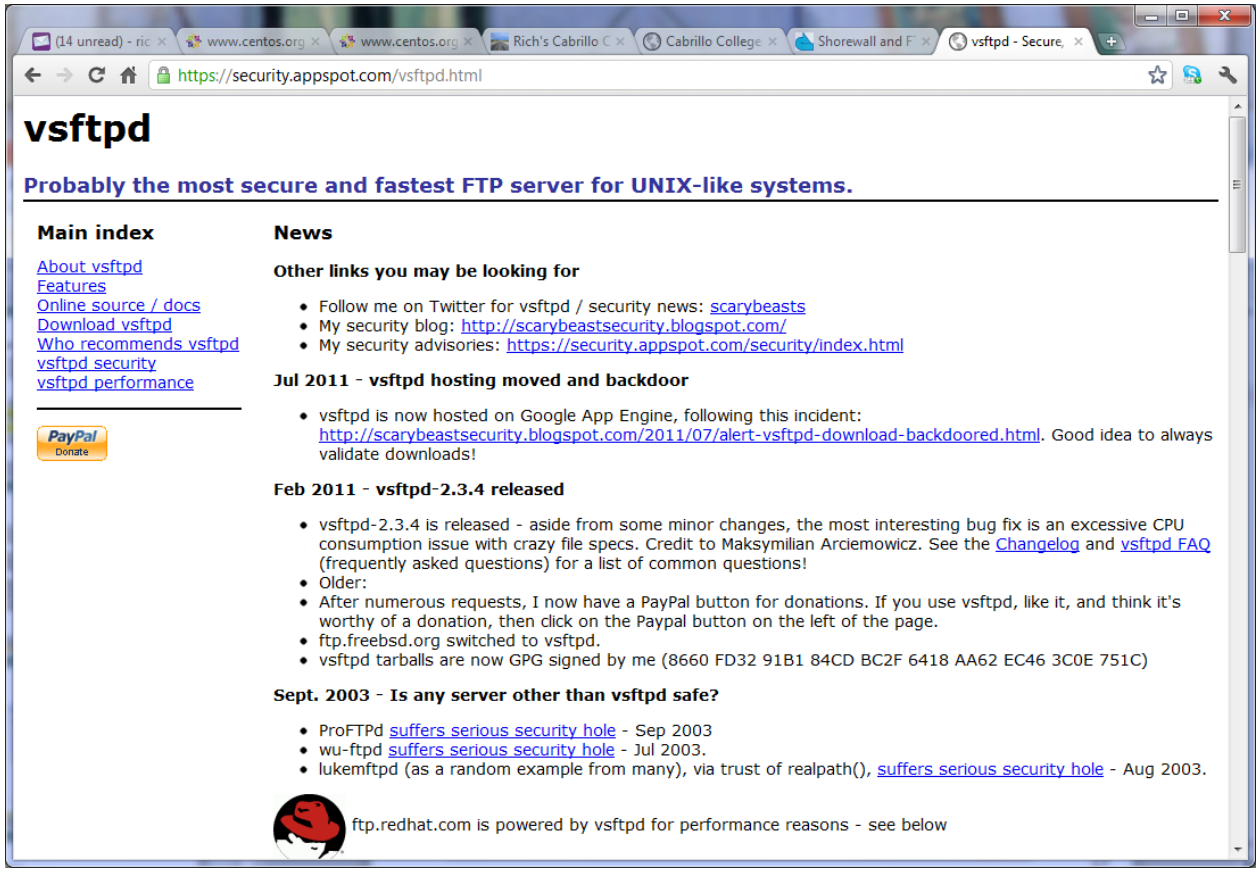
Two sockets are used
- One for commands (requests and responses)
- One for data transfer

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 connections
- Load nf_conntrack_ftp module (ip_conntrack_ftp for kernel version 2.6.19 or earlier) for the firewall to recognize the "related" connection

vsftpd

- vsftpd = Very Secure FTP Daemon
- Licensed under the GNU General Public License
- http://vsftpd.beasts.org/



vsftpd summary

Packages
rpm -qa | grep vsftpd
vsftpd-2.2.2-6.el6_0.1.i686

Configuration file: /etc/vsftpd/vsftpd.conf

Firewall Ports Used: 21/TCP (incoming) , 20/TCP (outgoing)
Firewall helper modules: (permanently configure in /etc/sysconfig/iptables-config)
- nf_conntrack_ftp, nf_nat_ftp
- for kernel versions 2.6.19 or earlier: ip_conntrack_ftp, ip_nat_ftp

SELinux
Context type for anonymous FTP content: **public_content_t**
Boolean to enable user directories: **ftp_home_dir**

Services and reloading configuration file changes
service vsftpd restart
```
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
```

Autostart the service
chkconfig vsftpd on

Anonymous public content in: /var/ftp/pub/

Sniffing: ftp, ip-host == 172.30.4.240 (wireshark)

Installing and Configuring vsftpd (Red Hat Family)

Is it installed?

```
[root@celebrian ~]# rpm -qa | grep vsftpd
vsftpd-2.0.5-12.el5
```

No response means it is not installed

*Use **dpkg –l | grep vsftpd** on the Debian family*

vsftpd

Installing vsftpd

Step 1 *Installing service*

yum install vsftpd

vsftpd

```
[root@celebrian ~]# yum install vsftpd
Loading "fastestmirror" plugin
Loading mirror speeds from cached hostfile
 * base: mirror.hmc.edu
 * updates: mirrors.easynews.com
 * addons: mirrors.cat.pdx.edu
 * extras: centos.cogentcloud.com
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.i386 0:2.0.5-12.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

vsftpd

```
Dependencies Resolved

================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 vsftpd                  i386       2.0.5-12.el5     base              137 k

Transaction Summary
================================================================================
Install       1 Package(s)
Update        0 Package(s)
Remove        0 Package(s)

Total download size: 137 k
Is this ok [y/N]: y
Downloading Packages:
(1/1): vsftpd-2.0.5-12.el 100% |=========================| 137 kB    00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing: vsftpd                       ########################## [1/1]

Installed: vsftpd.i386 0:2.0.5-12.el5
Complete!
[root@celebrian ~]#
```

Installing and Configuring vsftpd

Step 2 *Customize the configuration file*

```
[root@celebrian ~]# cat /etc/vsftpd/vsftpd.conf
[root@celebrian ~]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.

< snipped >

# You may fully customise the login banner string:
ftpd_banner=Welcome to the Simms FTP service.

< snipped >

tcp_wrappers=YES
[root@celebrian ~]#
```

Make your custom banner message here

Installing and Configuring vsftpd

Step 3 *Customize the firewall*

From the command line:

iptables -I INPUT 4 -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT

varies depending on your firewall

To make the firewall change permanent

service iptables save

Installing and Configuring vsftpd
(for kernel versions 2.6.19 or earlier)

Step 3 *Customize the firewall (continued)*

ip_conntrack_ftp is a kernel module. It is used to track related FTP connections so they can get through the firewall.

From the command line (temporary)

```
[root@celebrian ~]# modprobe ip_conntrack_ftp
[root@celebrian ~]# lsmod | grep ftp
ip_conntrack_ftp        11569  0
ip_conntrack            53281  3 ip_conntrack_ftp,ip_conntrack_netbios_ns,xt_state
[root@celebrian ~]#
```

To load at system boot (permanent), edit this file to include:

```
[root@celebrian ~]# 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"
< snipped >
```

Installing and Configuring vsftpd
(for kernel versions after 2.6.19)

Step 3 *Customize the firewall (continued)*

nf_conntrack_ftp and **nf_nat_ftp** are kernel modules. They are used to track related FTP connections so they can get through the firewall.

From the command line (temporary)

```
[root@celebrian ~]# modprobe nf_conntrack_ftp
[root@celebrian ~]# modprobe nf_nat_ftp

[root@beast pub]# lsmod | grep ftp
nf_nat_ftp              2544  0
nf_nat                 18618  1 nf_nat_ftp
nf_conntrack_ftp       10449  1 nf_nat_ftp
nf_conntrack           66010  6
nf_nat_ftp,nf_nat,nf_conntrack_ftp,nf_conntrack_ipv4,nf_conntrack_ipv6,xt_state
```

To load at system boot (permanent), edit this file to include:

```
[root@celebrian ~]# 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="nf_conntrack_ftp nf_nat_ftp"
< snipped >
```

Firewall for FTP

Current firewall settings

CentOS Modified

```
[root@celebrian ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
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

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

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

FTP port is now open

Firewall for FTP

CentOS Modified

```
[root@celebrian ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue Nov 22 09:21:11 2011
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [96:7209]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Tue Nov 22 09:21:11 2011
```

Permanent firewall settings

FTP port is now open

```
[root@beast pub]# lsmod | grep ftp
nf_nat_ftp              2544  0
nf_nat                 18618  1 nf_nat_ftp
nf_conntrack_ftp       10449  1 nf_nat_ftp
nf_conntrack           66010  6
nf_nat_ftp,nf_nat,nf_conntrack_ftp,nf_conntrack_ipv4,nf_conntrack_ipv6,xt_stat
e
```

Modules to track related FTP connections are loaded

SELinux for FTP (CentOS)

Step 4 *Configure SELinux*

```
[root@celebrian ~]# getenforce
Enforcing
[root@celebrian ~]#
```

Leave as enforcing

SELinux for vsftpd (CentOS)

Step 4 ***SELinux***

```
[root@elrond bin]# setenforce enforcing
[root@elrond bin]# getenforce
Enforcing
```

required for anonymous public content

```
[root@elrond bin]# ls -ldZ /var/ftp /var/ftp/pub
drwxr-xr-x  root root system_u:object_r:public_content_t
/var/ftp
drwxr-xr-x  root root system_u:object_r:public_content_t
/var/ftp/pub
```

Note: The /var/ftp directory and below is set by default with the public_content_t context. If necessary to set the context again use:
chcon -R -v -t public_content_t /var/ftp

```
[root@elrond bin]# setsebool -P ftp_home_dir=1
[root@elrond bin]# getsebool ftp_home_dir
ftp_home_dir --> on
```

required for users to access their home directories

Installing and Configuring vsftpd (Red Hat Family)

Step 5 *Start or restart service*

```
[root@celebrian ~]# service vsftpd start
Starting vsftpd for vsftpd:                                [  OK  ]
[root@celebrian ~]#
```

Step 6 *Automatically start at system boot*

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

Installing and Configuring vsftpd

Step 7 *Verify service is running*

vsftpd processes

```
[root@celebrian ~]# service vsftpd status
vsftpd (pid 7979 6475) is running...
```

```
[root@celebrian ~]# ps -ef | grep vsftpd
root      6475     1  0 08:28 ?        00:00:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
nobody    7975  6475  0 09:55 ?        00:00:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
cis192    7979  7975  0 09:55 ?        00:00:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
root      7995  7866  0 09:56 pts/3    00:00:00 grep vsftpd
[root@celebrian ~]#
```

Individual vsftpd daemons are run for each session

Installing and Configuring vsftpd

netstat

```
[root@celebrian ~]# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:6000                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:23                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:792                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:2207              0.0.0.0:*                   LISTEN
tcp        0      0 :::6000                     :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
[root@celebrian ~]#
```

Use netstat command to see what ports your system is listening for requests on

Installing and Configuring vsftpd

netstat

```
[root@celebrian ~]# netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 r1.localdomain:2208        *:*                         LISTEN
tcp        0      0 *:sunrpc                   *:*                         LISTEN
tcp        0      0 *:x11                      *:*                         LISTEN
tcp        0      0 *:ftp                      *:*                         LISTEN
tcp        0      0 *:telnet                   *:*                         LISTEN
tcp        0      0 r1.localdomain:ipp         *:*                         LISTEN
tcp        0      0 *:792                      *:*                         LISTEN
tcp        0      0 r1.localdomain:smtp        *:*                         LISTEN
tcp        0      0 r1.localdomain:2207        *:*                         LISTEN
tcp        0      0 *:x11                      *:*                         LISTEN
tcp        0      0 *:ssh                      *:*                         LISTEN
[root@celebrian ~]#
```

Use netstat command to see what ports your system is listening for requests on

Installing and Configuring vsftpd

Try it! *Create sample files on celebrian*

```
[root@celebrian ~]# cd /var/ftp/pub
[root@celebrian pub]# echo Contents > file1
[root@celebrian pub]# echo Contents > file2
[root@celebrian pub]# chmod 644 *
[root@celebrian pub]# ls -l
total 16
-rw-r--r-- 1 root root 9 Mar 17 09:09 file1
-rw-r--r-- 1 root root 9 Mar 17 09:09 file2
[root@celebrian pub]#
```

Installing and Configuring vsftpd

Try it! *On Elrond, download the files using **lftp** client from celebrian*

```
cis192@frodo:~$ lftp 172.30.4.240
lftp 172.30.4.240:~> ls
drwxr-xr-x    2 0        0            4096 Nov 22 17:10 pub
lftp 172.30.4.240:/> cd pub
lftp 172.30.4.240:/pub> ls
-rw-r--r--    1 0        0               9 Nov 22 17:10 file1
-rw-r--r--    1 0        0               9 Nov 22 17:10 file2
lftp 172.30.4.240:/pub> mget file*
18 bytes transferred
Total 2 files transferred
lftp 172.30.4.240:/pub> exit
cis192@frodo:~$
```

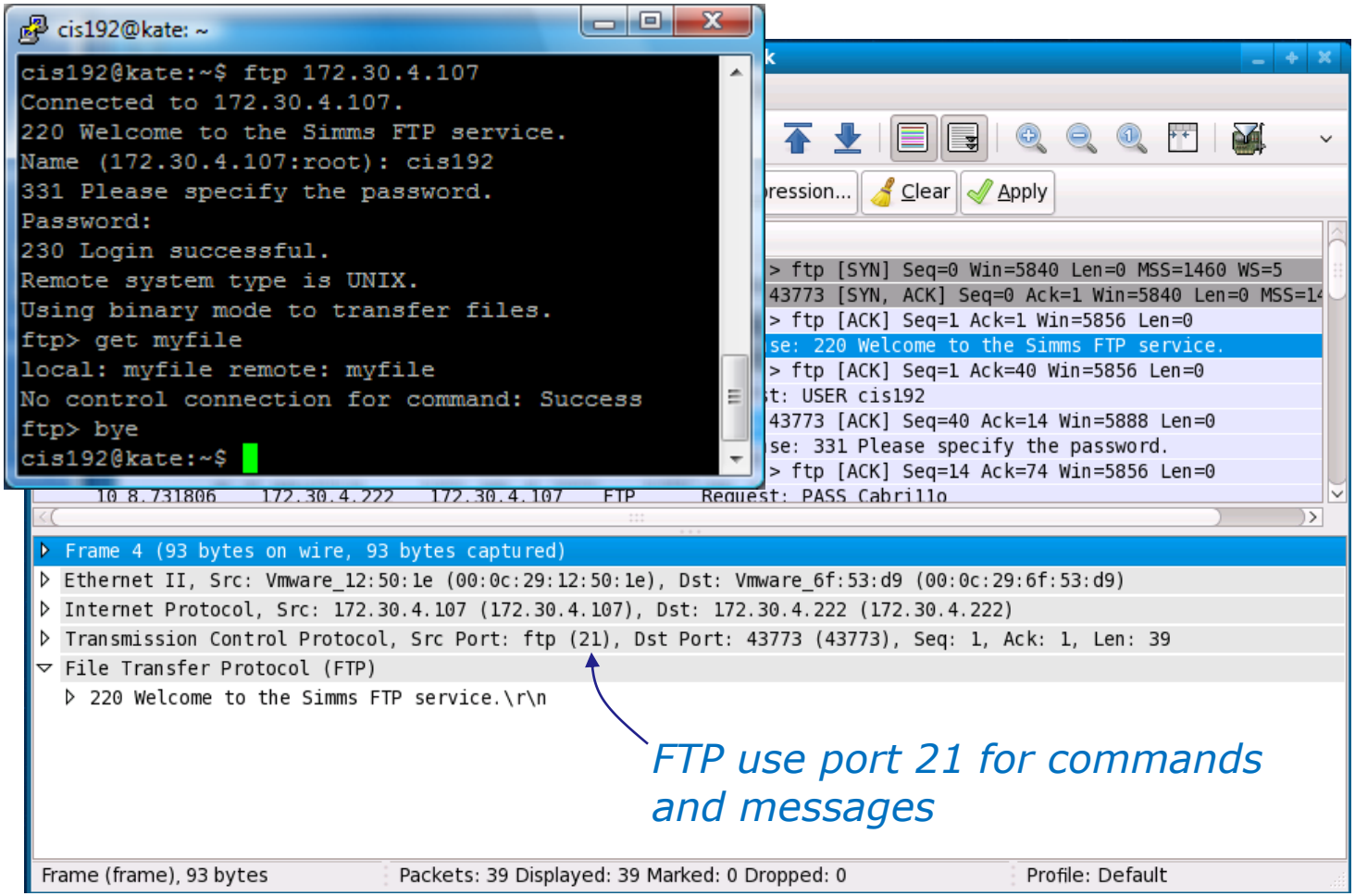
lftp is a ftp client that can run in the background, download multiple files at once and keep trying if the connection fails

Try it! Installing and Configuring vsftpd

```
cis192@frodo:~$ ftp 172.30.4.240
Connected to 172.30.4.240.
220 Welcome to Benji Simms FTP service.
Name (172.30.4.240:cis192): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 22 17:10 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0               9 Nov 22 17:10 file1
-rw-r--r--    1 0        0               9 Nov 22 17:10 file2
226 Directory send OK.
ftp> mget file*
mget file1? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for file1 (9 bytes).
226 Transfer complete.
9 bytes received in 0.00 secs (4.8 kB/s)
mget file2? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for file2 (9 bytes).
226 Transfer complete.
9 bytes received in 0.00 secs (19.9 kB/s)
ftp> exit
221 Goodbye.
cis192@frodo:~$
```

*On Elrond, download the files using regular **ftp** client from Celebrian*

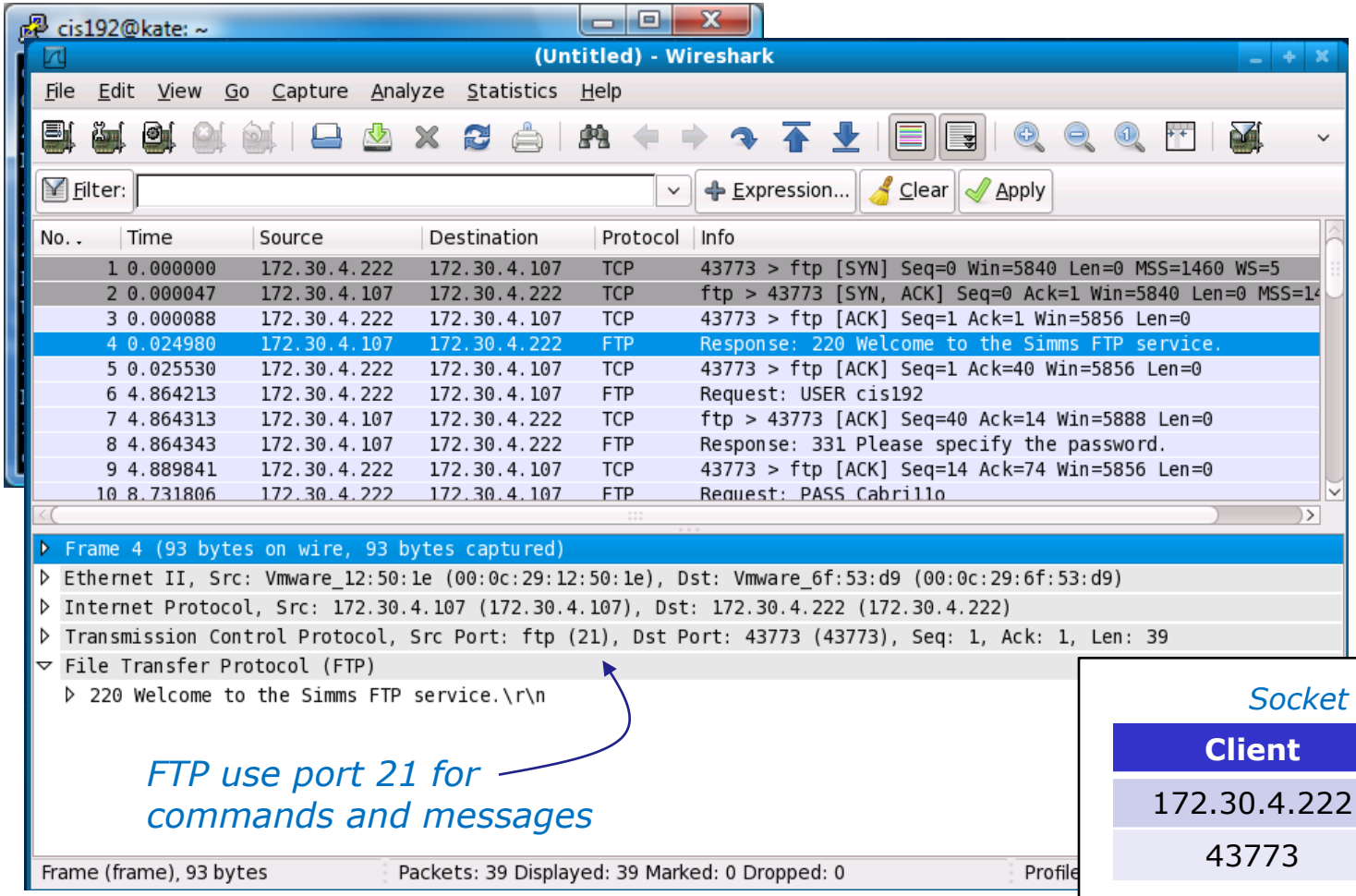
Installing and Configuring vsftpd



3-way handshake

Login is transmitted in clear text

Installing and Configuring vsftpd



FTP use port 21 for commands and messages

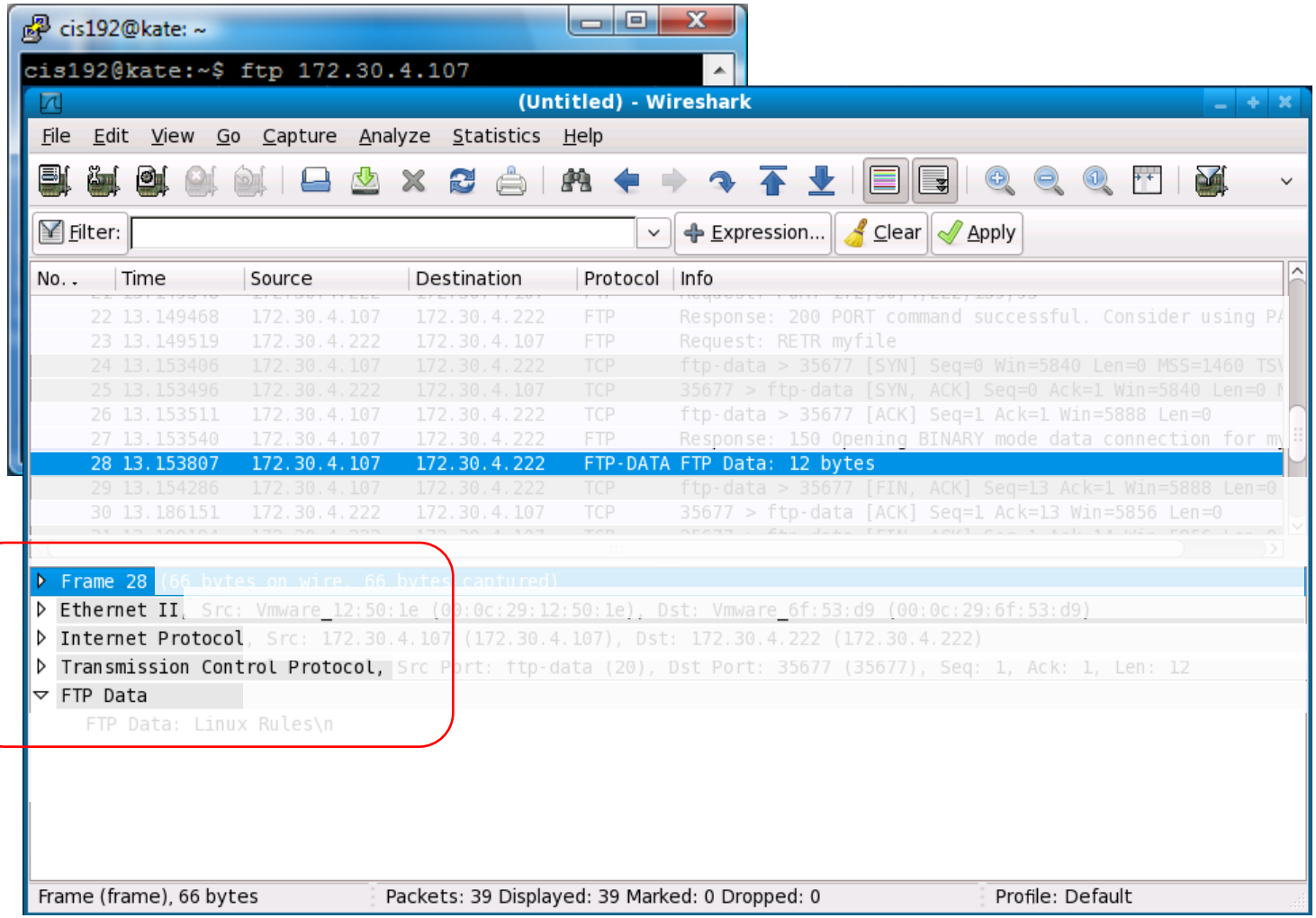
3-way handshake

Login is transmitted in clear text

Socket for commands

Client	Server
172.30.4.222	172.30.4.107
43773	21

Installing and Configuring vsftpd



Encapsulation:

FTP data (layer 5) is encapsulated in a TCP segment

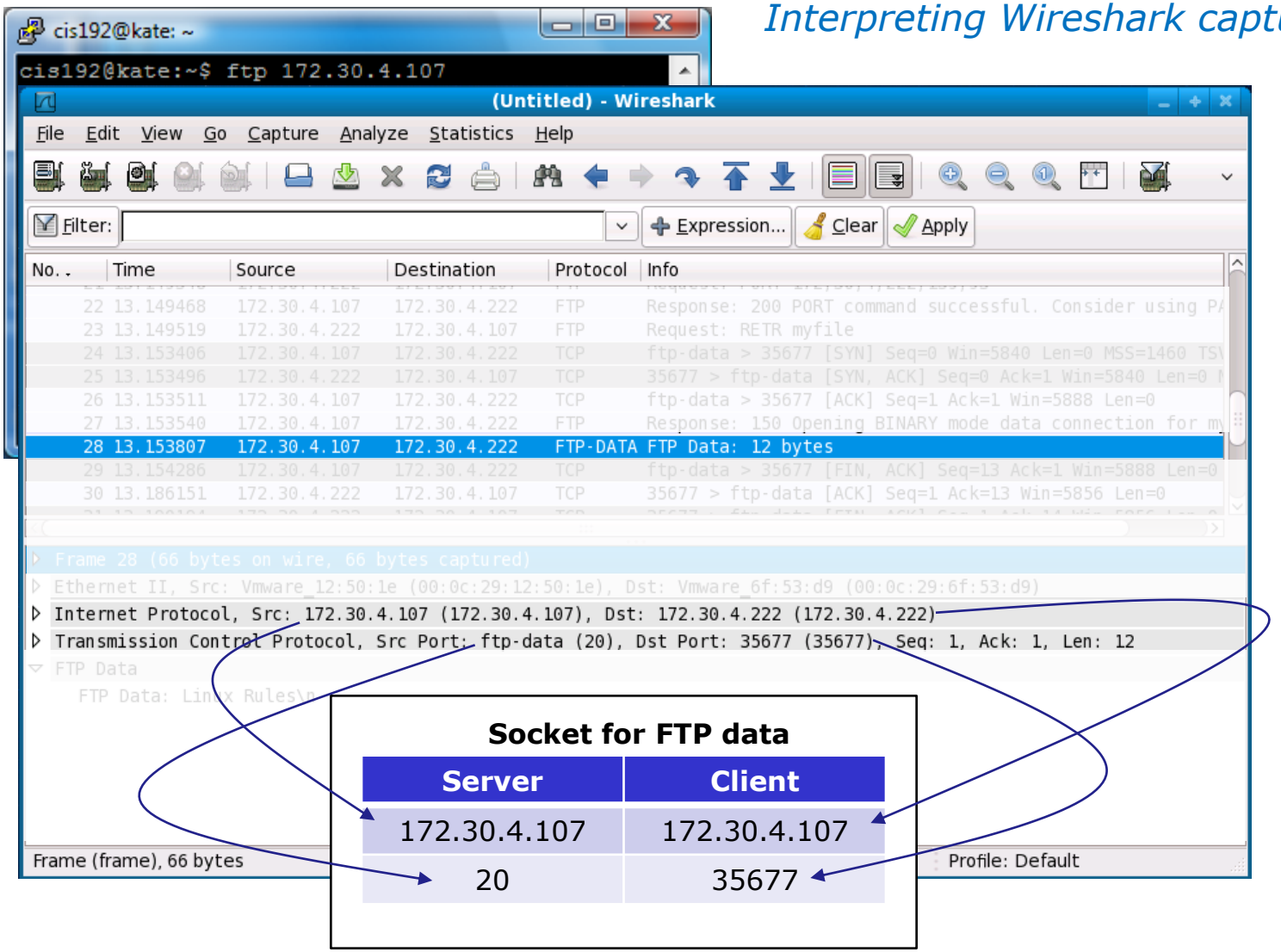
The **TCP segment (layer 4)** is encapsulated in an IP packet

The **IP packet (layer 3)** is encapsulated in Ethernet frame

The **Ethernet frame (layer 2)** is placed in a low level frame that travels via electrical signals on a **physical cable (Layer 1)**

Installing and Configuring vsftpd

Interpreting Wireshark captures - sockets



Socket for FTP data

Server	Client
172.30.4.107	172.30.4.107
20	35677

Installing and Configuring vsftpd

Step 8 Troubleshooting

Useful Wireshark filters:

- ftp (to see just FTP packets)
- ip.host == 172.30.4.240 (to see all traffic into and out of a FTP server)

Useful tcpdump filters:

- port ftp (to see just FTP packets)
- host 172.30.4.240 (to see all traffic into and out of a FTP server)

Installing and Configuring vsftpd

Step 8 Troubleshooting

```
[root@elrond ~]# lftp celebrian
lftp celebrian:~> ls
`ls' at 0 [Delaying before reconnect: 27]
```

On the FTP server:

- *Check FTP service is running,*
- *Check TCP port 21 is open*
- *Check ip_conntrack_ftp kernel module is loaded*

Installing and Configuring vsftpd

Step 8 Troubleshooting

```
[root@elrond ~]# ftp celebrian
ftp: connect: No route to host
ftp>
```

Open the firewall on the FTP sever to accept incoming FTP connections (TCP 21)

Use ***iptables -I INPUT 5 -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT***

Installing and Configuring vsftpd

Step 8 Troubleshooting

```
[root@elrond ~]# ftp celebrian
ftp: connect: Connection refused
ftp>
```

Make sure service is up and running on FTP server.
*Use **service vsftpd start***

Installing and Configuring vsftpd

Step 8 Troubleshooting

```
[root@elrond ~]# ftp celebrian
Connected to celebrian.
220 Welcome to the SIMMS FTP service.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (celebrian:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192,168,2,9,106,150)
ftp: connect: No route to host
ftp>
```

Make sure ip_conntrack_ftp kernel module has been loaded on FTP server. Use ***modprobe nf_conntrack_ftp***

Installing and Configuring vsftpd

Step 9 Monitor log files

```
[root@celebrian ~]# tail -f /var/log/xferlog
Wed Mar 17 15:50:41 2010 1 127.0.0.1 9 /pub/file1 b _ o a lftp@ ftp 0 * c
Wed Mar 17 15:50:41 2010 1 127.0.0.1 9 /pub/file2 b _ o a lftp@ ftp 0 * c
Wed Mar 17 16:03:00 2010 1 127.0.0.1 9 /pub/file1 b _ o a ? ftp 0 * c
Wed Mar 17 16:03:01 2010 1 127.0.0.1 9 /pub/file2 b _ o a ? ftp 0 * c
Wed Mar 17 16:35:06 2010 1 192.168.2.1 0 /pub/f* b _ o a lftp@ ftp 0 * i
Wed Mar 17 16:35:17 2010 1 192.168.2.1 0 /pub/file* b _ o a lftp@ ftp 0 * i
Wed Mar 17 16:35:21 2010 1 192.168.2.1 9 /pub/file1 b _ o a lftp@ ftp 0 * c
Wed Mar 17 16:35:21 2010 1 192.168.2.1 9 /pub/file2 b _ o a lftp@ ftp 0 * c
Wed Mar 17 16:39:27 2010 1 192.168.2.1 9 /pub/file1 b _ o a ? ftp 0 * c
Wed Mar 17 16:39:28 2010 1 192.168.2.1 9 /pub/file2 b _ o a ? ftp 0 * c
```

```
[root@celebrian ~]# cat /var/log/secure | grep -i  vsftpd
Mar 17 07:47:27 celebrian vsftpd: pam_unix(vsftpd:auth): authentication
failure; logname= uid=0 euid=0 tty=ftp ruser=cis192 rhost=elrond
user=cis192
Mar 17 08:02:56 celebrian vsftpd: pam_unix(vsftpd:auth): authentication
failure; logname= uid=0 euid=0 tty=ftp ruser=cis192 rhost=elrond
user=cis192
[root@celebrian ~]#
```

Installing and Configuring vsftpd

Does vsftpd use TCP Wrappers?

```
[root@celebrian ~]# type vsftpd
vsftpd is /usr/sbin/vsftpd
[root@celebrian ~]# ldd /usr/sbin/vsftpd
        linux-gate.so.1 =>  (0x0074c000)
        libssl.so.6 => /lib/libssl.so.6 (0x0012a000)
        libwrap.so.0 => /usr/lib/libwrap.so.0 (0x005cb000)
        libnsl.so.1 => /lib/libnsl.so.1 (0x00913000)
        libpam.so.0 => /lib/libpam.so.0 (0x00b11000)
        libcap.so.1 => /lib/libcap.so.1 (0x0084a000)
        libdl.so.2 => /lib/libdl.so.2 (0x00110000)
        libc.so.6 => /lib/libc.so.6 (0x0016f000)
        libcrypto.so.6 => /lib/libcrypto.so.6 (0x002b2000)
        libgssapi_krb5.so.2 => /usr/lib/libgssapi_krb5.so.2 (0x00bb4000)
        libkrb5.so.3 => /usr/lib/libkrb5.so.3 (0x003e5000)
        libcom_err.so.2 => /lib/libcom_err.so.2 (0x0092c000)
        libk5crypto.so.3 => /usr/lib/libk5crypto.so.3 (0x0054c000)
        libresolv.so.2 => /lib/libresolv.so.2 (0x00114000)
        libz.so.1 => /usr/lib/libz.so.1 (0x00478000)
        libaudit.so.0 => /lib/libaudit.so.0 (0x004c5000)
        /lib/ld-linux.so.2 (0x0085a000)
        libkrb5support.so.0 => /usr/lib/libkrb5support.so.0 (0x00fb5000)
        libkeyutils.so.1 => /lib/libkeyutils.so.1 (0x00961000)
        libselinux.so.1 => /lib/libselinux.so.1 (0x0048b000)
        libsepol.so.1 => /lib/libsepol.so.1 (0x004da000)
[root@celebrian ~]#
```

yes it does

Installing and Configuring vsftpd

Step 10 *Configure additional security with TCP wrappers*

TCP Wrappers and vsftpd

vsftpd is compiled with TCP wrappers

- **/etc/hosts.allow** – for permitted hosts
- **/etc/hosts.deny** – to ban hosts

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

celebrian


```
[root@arwen ~]# cat /etc/hosts.allow
sshd: frodo 192.168. 10.0.0.0/255.0.0.0
in.telnetd:  192.168.2.10  127.0.0.1
vsftpd: frodo arwecelebrianron
```

For vsftpd, only Frodo, celebrian and Sauron hosts are allowed

Nosmo at 172.30.1.1 is NOT included

```
[root@celebrian ~]# cat /etc/hosts.deny
ALL: ALL
```

Everyone else is denied (this includes Nosmo)

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

celebrian


```
[root@celebrian ~]# cat /etc/hosts.allow
sshd: frodo 192.168. 10.0.0.0/255.0.0.0
in.telnetd:  192.168.2.10  127.0.0.1
vsftpd: frodo celebrian sauron

[root@celebrian ~]# cat /etc/hosts.deny
ALL: ALL
```

Sauron

Access permitted

```
root@sauron:~# ftp celebrian
Connected to celebrian.
220 Welcome to the Cabrillo Super FTP service.
Name (celebrian:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
root@sauron:~#
```

Nosmo

Access denied

```
[root@nosmo root]# ftp 192.168.2.9
Connected to 192.168.2.9 (192.168.2.9).
421 Service not available.
ftp>
```

More FTP (module)

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

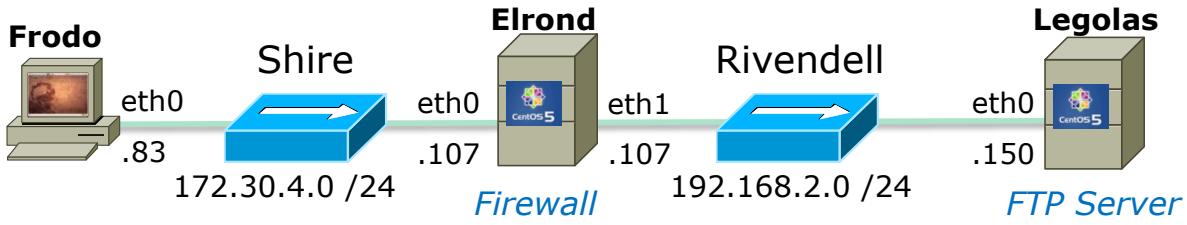
Initialize

*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

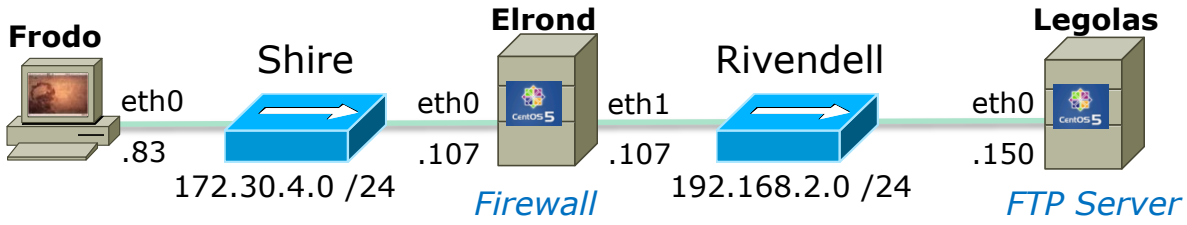
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [SYN] Seq=0 Win=58
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [SYN, ACK] Seq=0 A
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 220 (vsFTPd 2.0.5)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

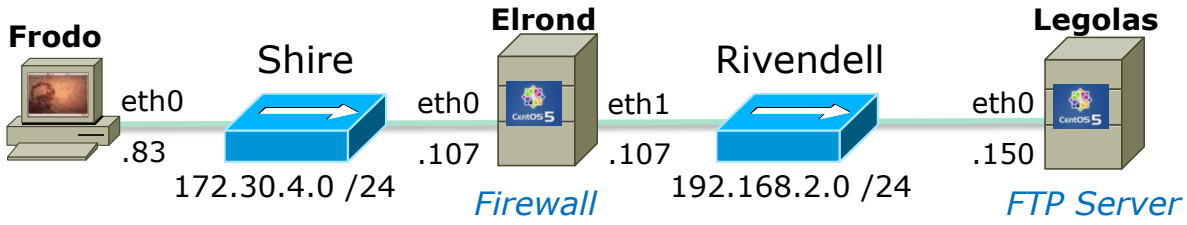
username

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



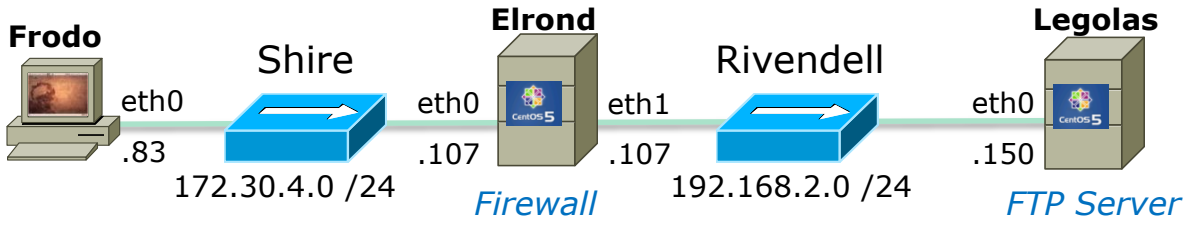

```
Remote system type is UNIX.
Using binary mode to transfer files.
```

- *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)
```

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

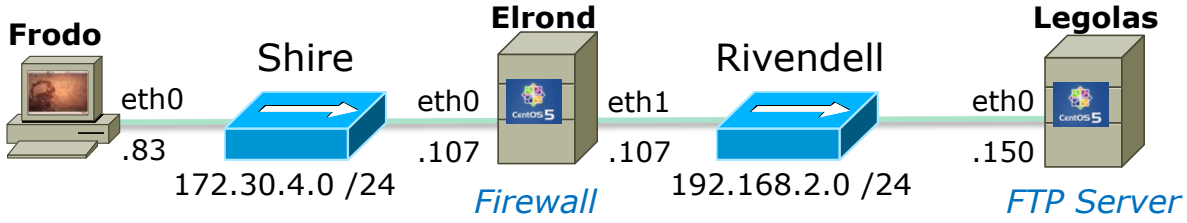
PORT command to listen on 166, 75 = A64B = 42571

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

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
41025	51283

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

```
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

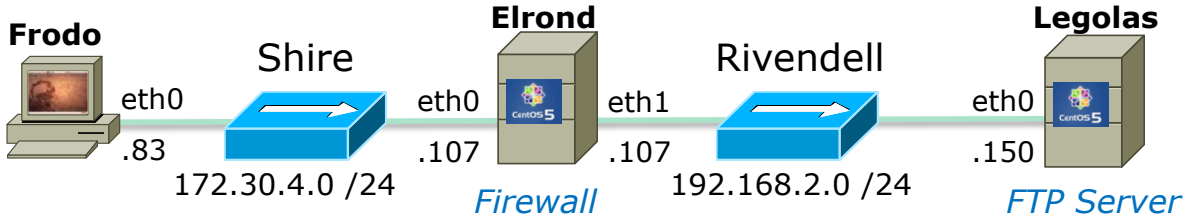
Passive reply to listen on 200, 83 = C853 = 51283

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)
```

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

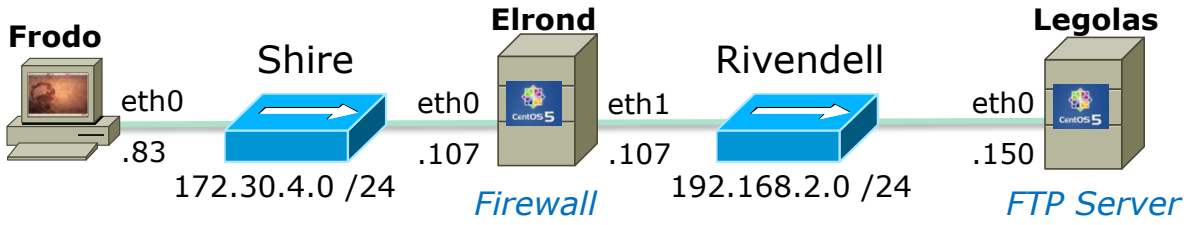
PORT command to listen on 133, 50 = 8532 = 34098

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

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

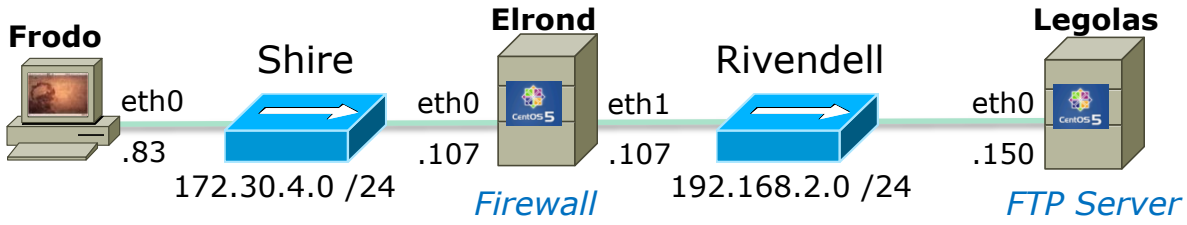
Save to make changes persist across restarts

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

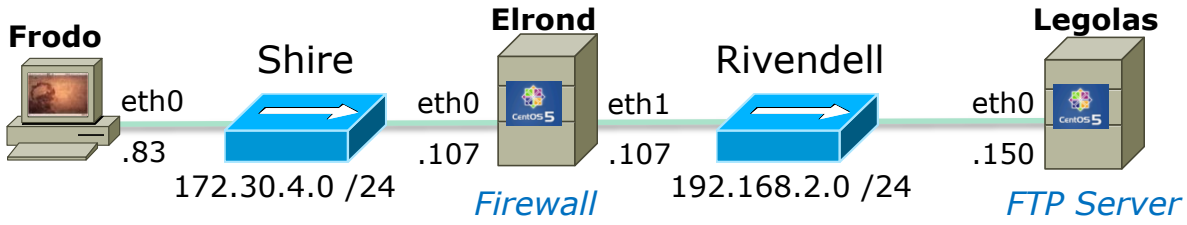



```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination

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

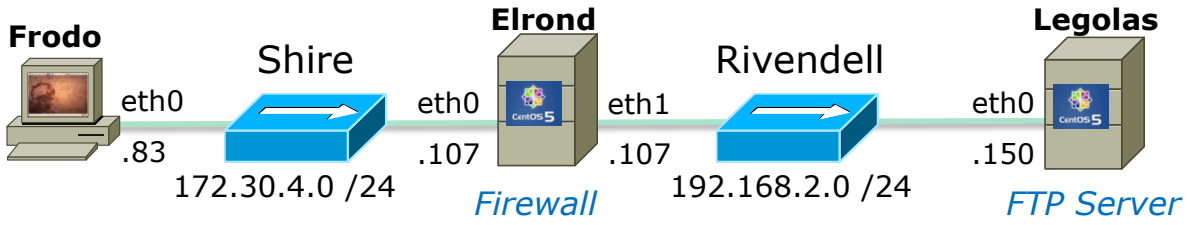
This firewall setting allows external clients (Frodo) to access the FTP server (Legolas)

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

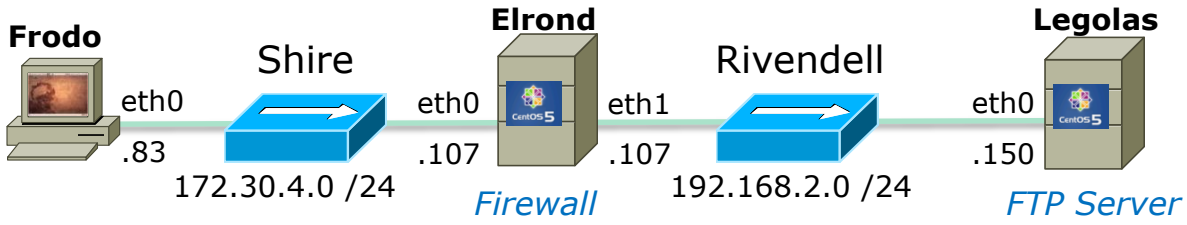


What If? *We remove the firewall opening for the DNS lookups sent by the FTP server*

```
[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 ~]#
```

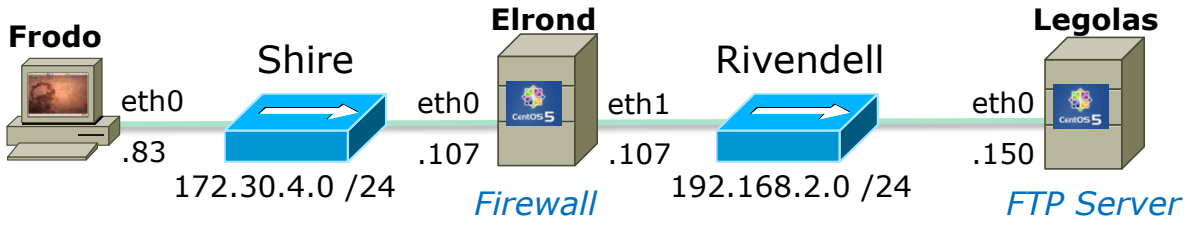
```
[root@elrond ~]# iptables -D FORWARD 1
```

Now DNS lookups are blocked




```
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

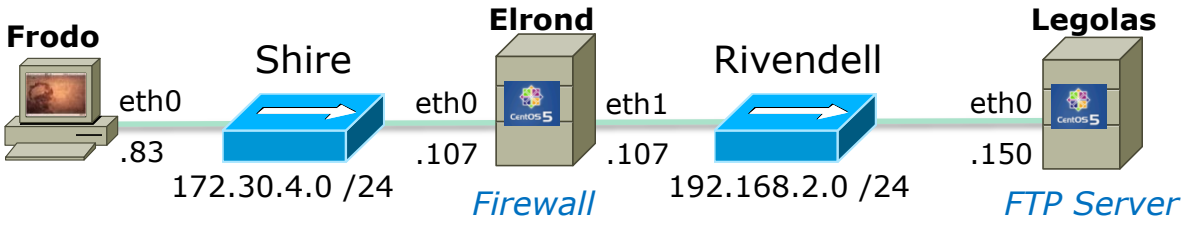



```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
```

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

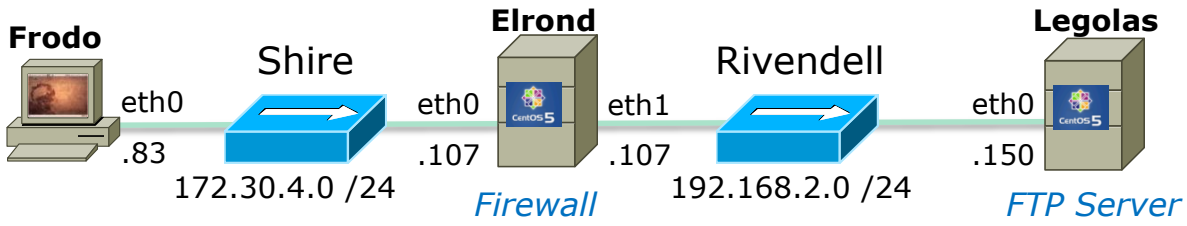
The login is delayed while the two DNS requests time-out.



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.

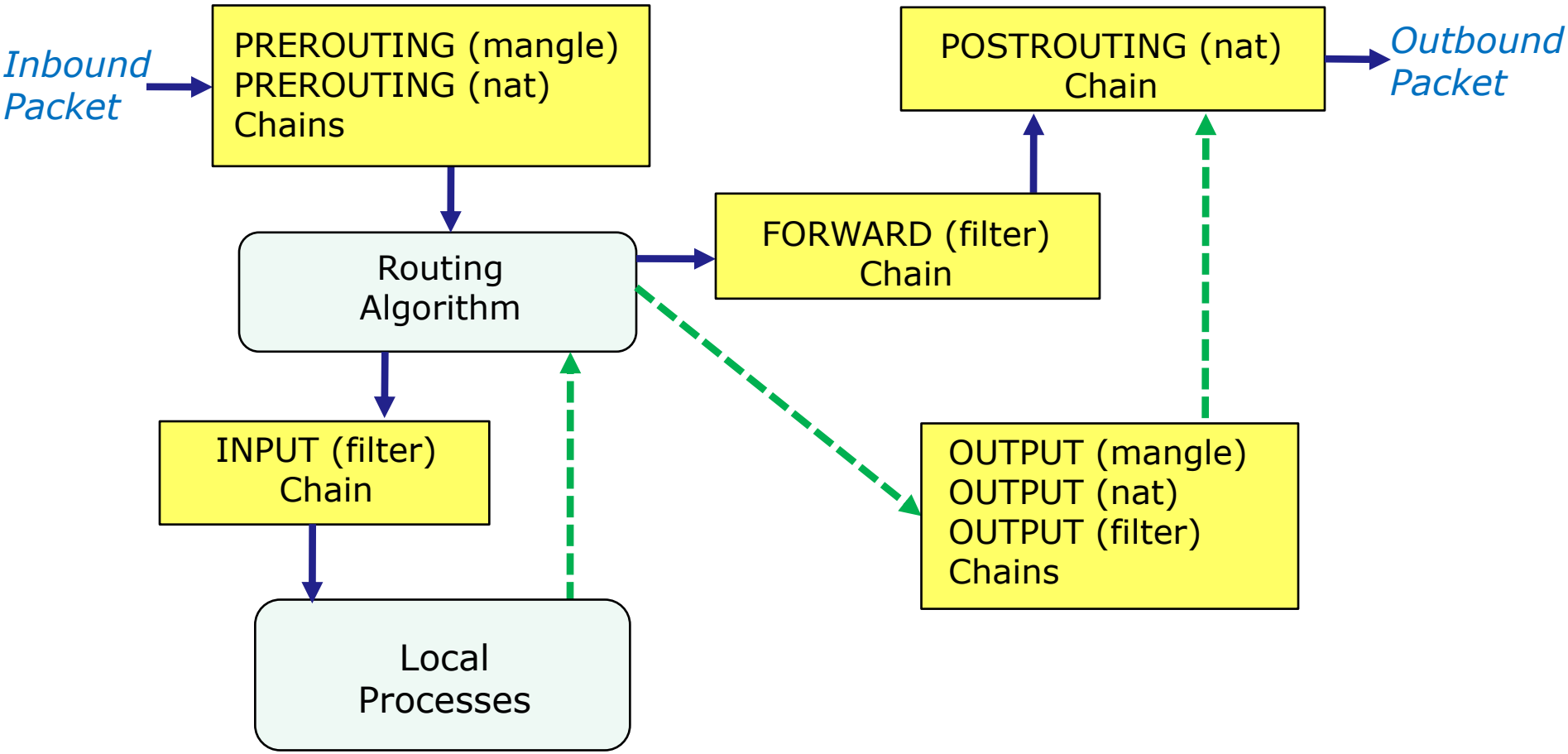
Gives up after 5 tries of attempting to do a 3-way handshake

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

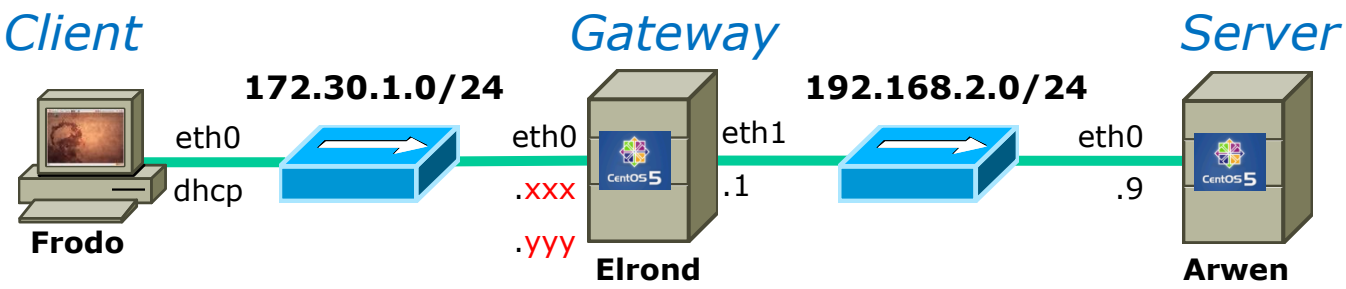
NAT port forwarding (module)

NAT port forwarding

Netfilter – all tables and chains



Use the PREROUTING NAT table chain for port forwarding

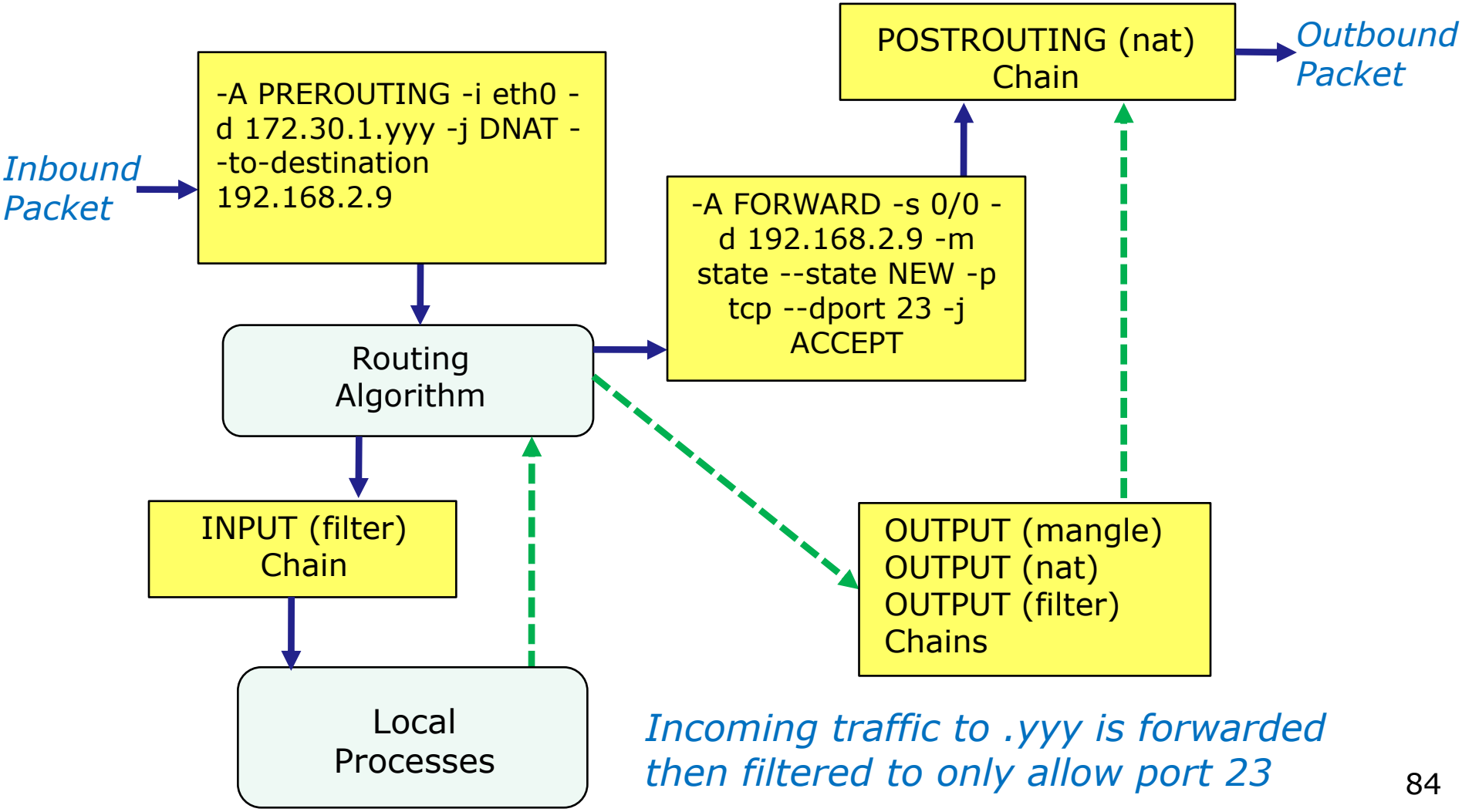


In Lab 5, all incoming traffic to .yyy is forwarded to Arwen

```
iptables -t nat -A PREROUTING -i eth0 -d 172.30.1.yyy -j DNAT --to-destination 192.168.2.9

iptables -A FORWARD -s 192.168.2.0/24 -d 0/0 -m state --state NEW -j ACCEPT
iptables -A FORWARD -s 0/0 -d 192.168.2.9 -m state --state NEW -p tcp --dport 23 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -j LOG --log-level info --log-prefix "iptables FORWARD: "
iptables -P FORWARD DROP

iptables -A INPUT -i eth1 -s 192.168.2.0/24 -d 192.168.2.1 -m state --state NEW -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j LOG --log-level info --log-prefix "iptables INPUT: “
iptables -P INPUT DROP

iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -P OUTPUT DROP

iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.9 -j SNAT --to-source 172.30.1.yyy
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to-source 172.30.1.xxx
```

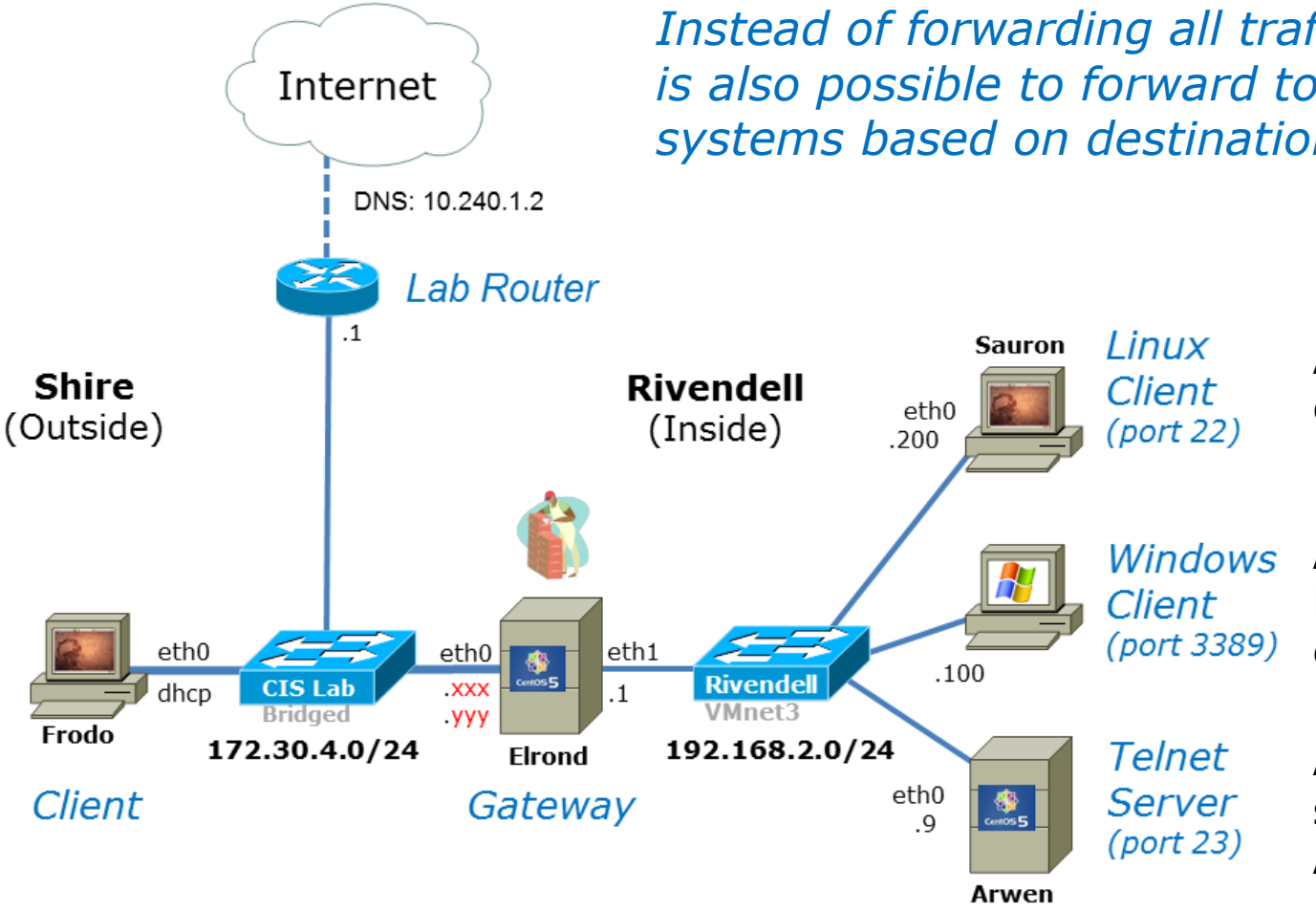
Lab 5

Incoming traffic is forwarded to Arwen



Incoming traffic to .yyy is forwarded then filtered to only allow port 23

Lab 5 modification



Instead of forwarding all traffic to Arwen it is also possible to forward to different systems based on destination port

All SSH traffic goes to Sauron

All Remote Desktop traffic goes to William

All Telnet traffic still goes to Arwen

Lab 5 modification

~~iptables -t nat -A PREROUTING -i eth0 -d 172.30.1.yyy -j DNAT --to-destination 192.168.2.9~~
iptables -A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.2.200
iptables -A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 23 -j DNAT --to-destination 192.168.2.9
iptables -A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 3389 -j DNAT --to-destination 192.168.2.100

Forward to different systems based on destination port

iptables -A FORWARD -s 192.168.2.0/24 -d 0/0 -m state --state NEW -j ACCEPT
~~iptables -A FORWARD -s 0/0 -d 192.168.2.9 -m state --state NEW -p tcp --dport 23 -j ACCEPT~~
iptables -A FORWARD -d 192.168.2.200/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
iptables -A FORWARD -d 192.168.2.9/32 -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
iptables -A FORWARD -d 192.168.2.100/32 -p tcp -m state --state NEW -m tcp --dport 3389 -j ACCEPT

Open the firewall to allow the selected destination port traffic to be forwarded

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -j LOG --log-level info --log-prefix "iptables FORWARD: "
iptables -P FORWARD DROP

iptables -A INPUT -i eth1 -s 192.168.2.0/24 -d 192.168.2.1 -m state --state NEW -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -j LOG --log-level info --log-prefix "iptables INPUT: "
iptables -P INPUT DROP

iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -P OUTPUT DROP

iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.9 -j SNAT --to-source 172.30.1.yyy
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to-source 172.30.1.xxx

Lab 5 modification

```
[root@elrond sysconfig]# cat iptables
# Generated by iptables-save v1.4.7 on Sat Nov 19 08:25:01 2011
*nat
:PREROUTING ACCEPT [1216:196031]
:POSTROUTING ACCEPT [8:510]
:OUTPUT ACCEPT [3:210]
# Redirect incoming public IP traffic based on destination port
-A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 22 -j DNAT --to-destination 192.168.2.200
-A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 23 -j DNAT --to-destination 192.168.2.9
-A PREROUTING -d 172.30.4.253/32 -p tcp -m tcp --dport 3389 -j DNAT --to-destination 192.168.2.100
# Internet for Rivendell hosts using NAT
-A POSTROUTING -s 192.168.2.9/32 -o eth0 -j SNAT --to-source 172.30.4.253
-A POSTROUTING -s 192.168.2.0/24 -o eth0 -j SNAT --to-source 172.30.4.252
COMMIT
# Completed on Sat Nov 19 08:25:01 2011
# Generated by iptables-save v1.4.7 on Sat Nov 19 08:25:01 2011
*filter
:INPUT DROP [894:156935]
:FORWARD DROP [7:668]
:OUTPUT DROP [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.2.0/24 -d 192.168.2.1/32 -i eth1 -m state --state NEW -j ACCEPT
-A INPUT -j LOG --log-prefix "iptables INPUT:" --log-level 6
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -s 192.168.2.0/24 -m state --state NEW -j ACCEPT
-A FORWARD -d 192.168.2.200/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 192.168.2.9/32 -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT
-A FORWARD -d 192.168.2.100/32 -p tcp -m state --state NEW -m tcp --dport 3389 -j ACCEPT
-A FORWARD -j LOG --log-prefix "iptables FORWARD:" --log-level 6
-A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Sat Nov 19 08:25:01 2011
[root@elrond sysconfig]#
```

Lab 5 modified to support port forwarding

DHCP module

DHCP Overview

DHCP

Dynamic Host Configuration Protocol

Defined by RFC 1541

- Extension of the bootstrap (bootp) protocol

Updated by RFC 2131

- adds DHCPINFORM and vendor specific options

Benefits:

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

DHCP

DHCP Architecture

DHCP Servers

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

DHCP Relay Agents

DHCP Clients

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

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

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

DHCP

DHCP Architecture

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

DHCP Relay Agents

DHCP Clients

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

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

DHCP

DHCP Architecture

DHCP Servers

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

DHCP Relay Agents

DHCP Clients

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

DHCP

DHCP Architecture

DHCP Servers

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

DHCP Relay Agents

DHCP Clients

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

The lease has a time limit but it can be renewed

DHCP

DHCP Architecture

DHCP Servers

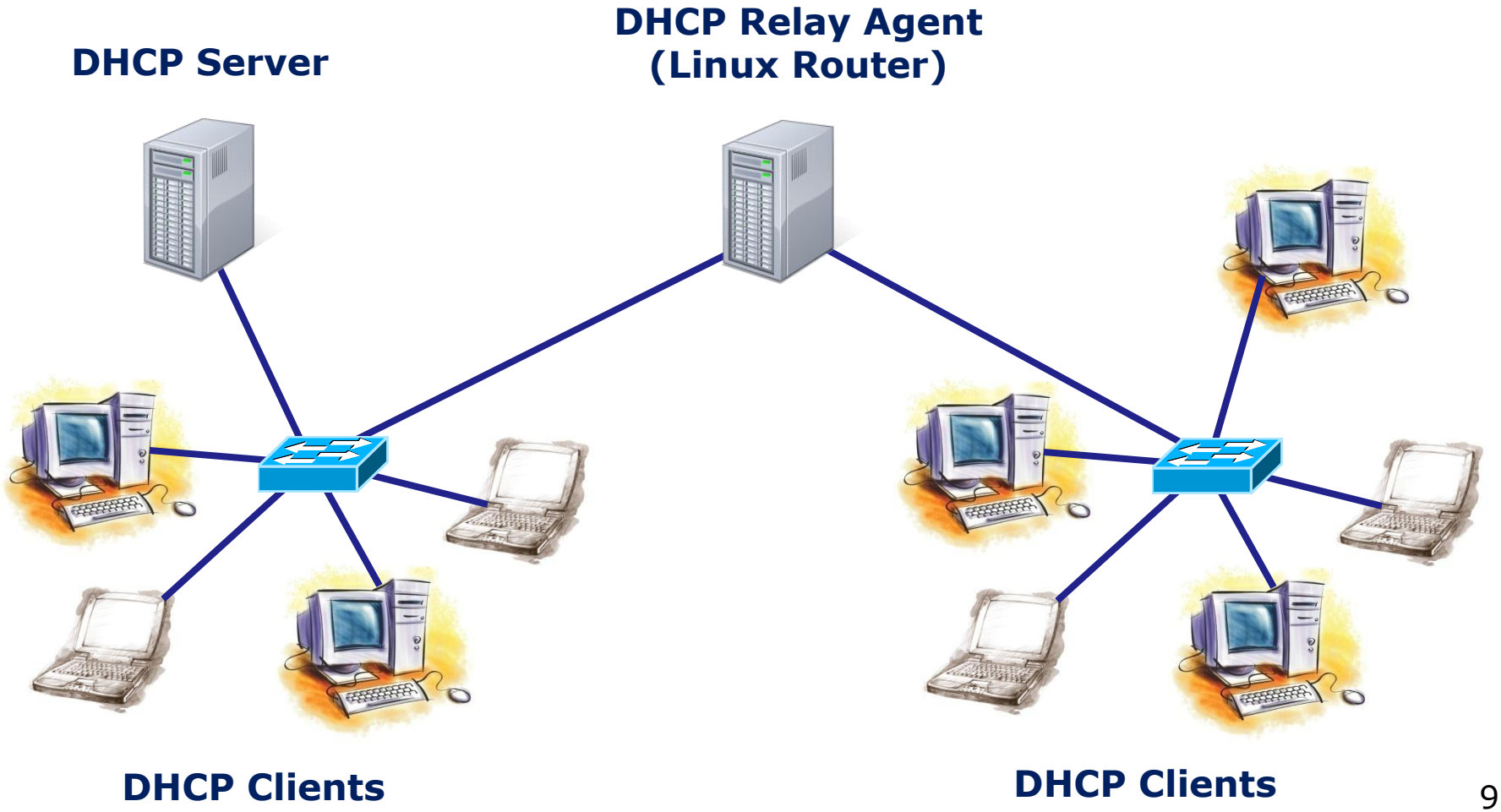
- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

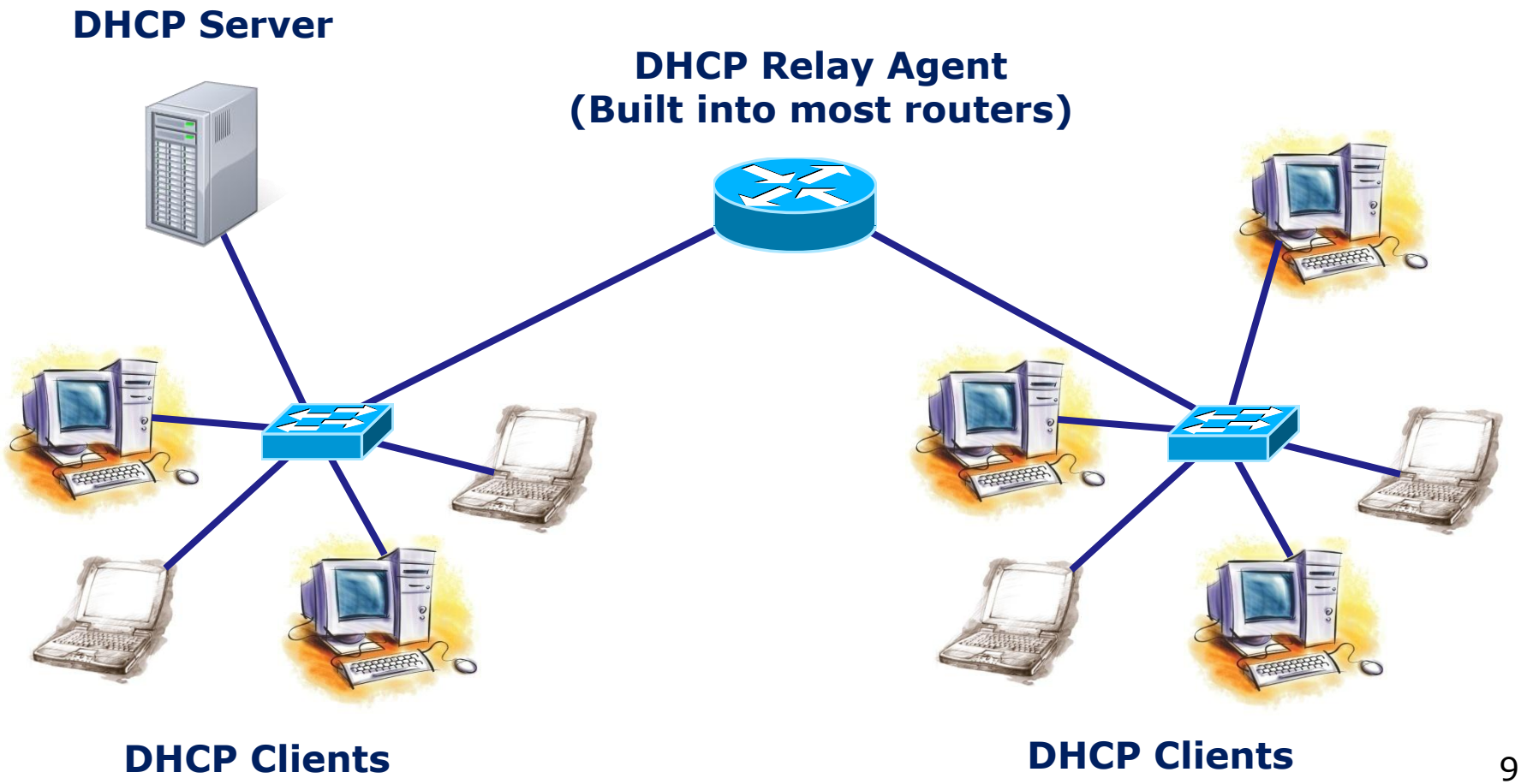
DHCP Clients

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

DHCP


DHCP 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

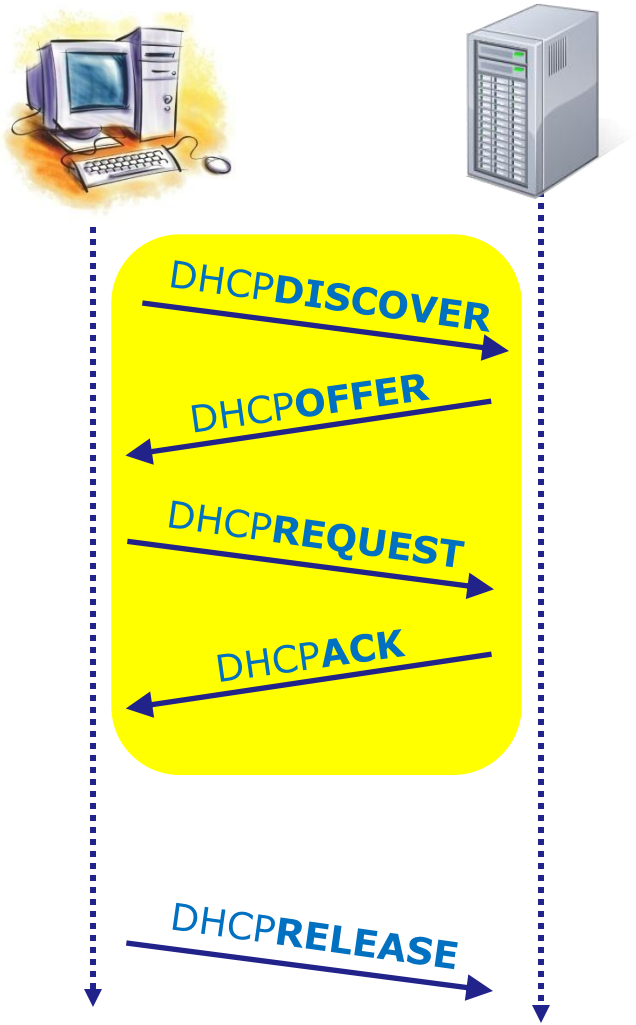
The DORA sequence is used by to join a new client to the network

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



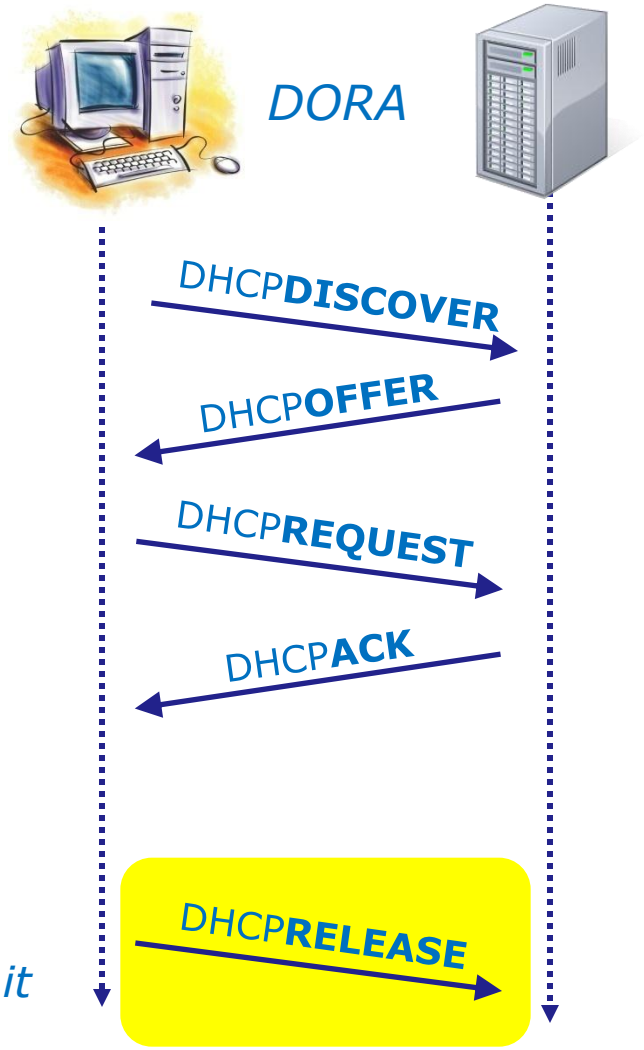
D *iscover*

O *ffer*

R *equest*

A *cknowledge*

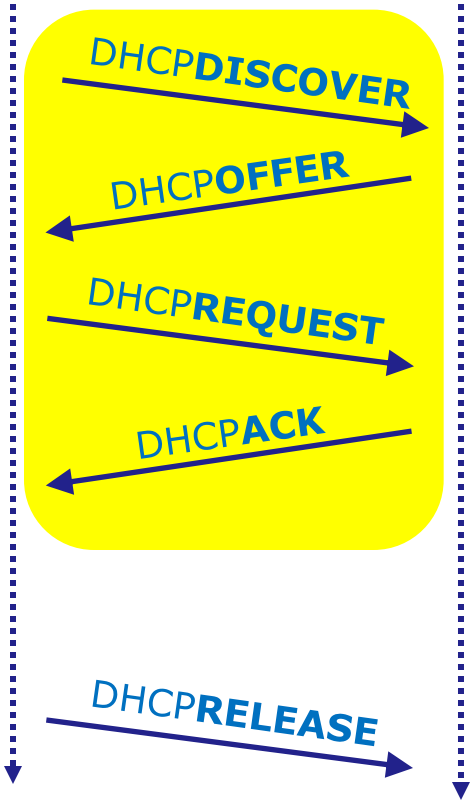
DHCP



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

DHCP

DORA



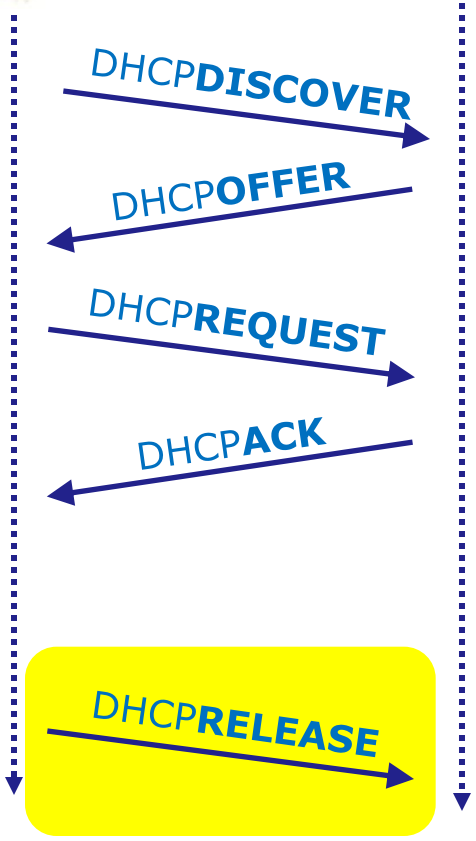
*The **dhclient** command illustrates the DORA steps*

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

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

Use the –v option on newer distributions to see the activity

DHCP

DORA

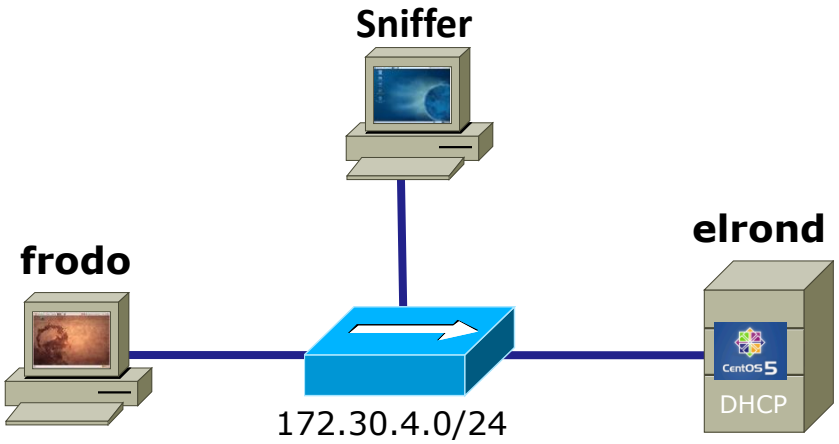


*The **dhclient –r** command does a DHCP release*

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

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

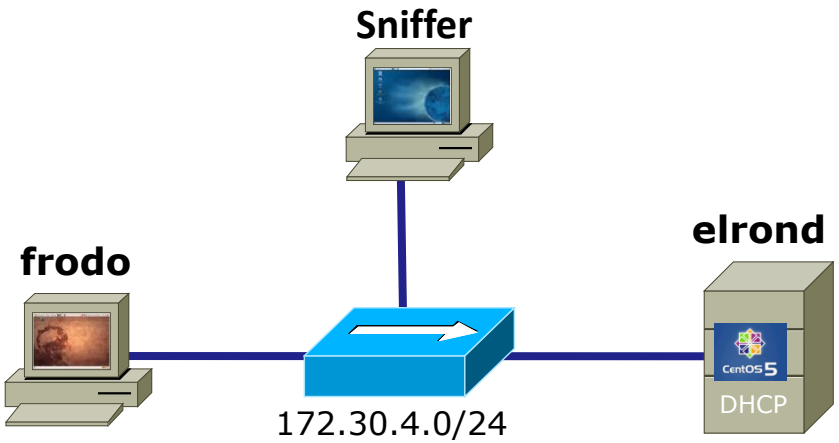
DHCP

Wireshark view of example DHCP operations



DHCP Client *DHCP Server*

Frodo starting up (needs IP address)



DHCP Client *DHCP Server*

frodo

*DHCP**DISCOVER** (broadcast)*

Hey, I need an IP address!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

UDP datagram is broadcast to port 67

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

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

frodo

*DHCP**DISCOVER***
(broadcast)

Hey, I need an IP address!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

Frodo sends its hostname

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

frodo

*DHCP**DISCOVER***
(broadcast)

Hey, I need an IP address!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

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

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

elrond

*DHCP**OFFER***
(unicast)

Here is an IP address, want it?

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

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

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

elrond

*DHCP**OFFER***
(unicast)

Here is an IP address, want it?

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

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

Additional network configuration is included in the offer

frodo

*DHCP**REQUEST** (broadcast)*

Yes, I want that one

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

Request is broadcast back

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

frodo

*DHCP**REQUEST** (broadcast)*

Yes, I want that one

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
```

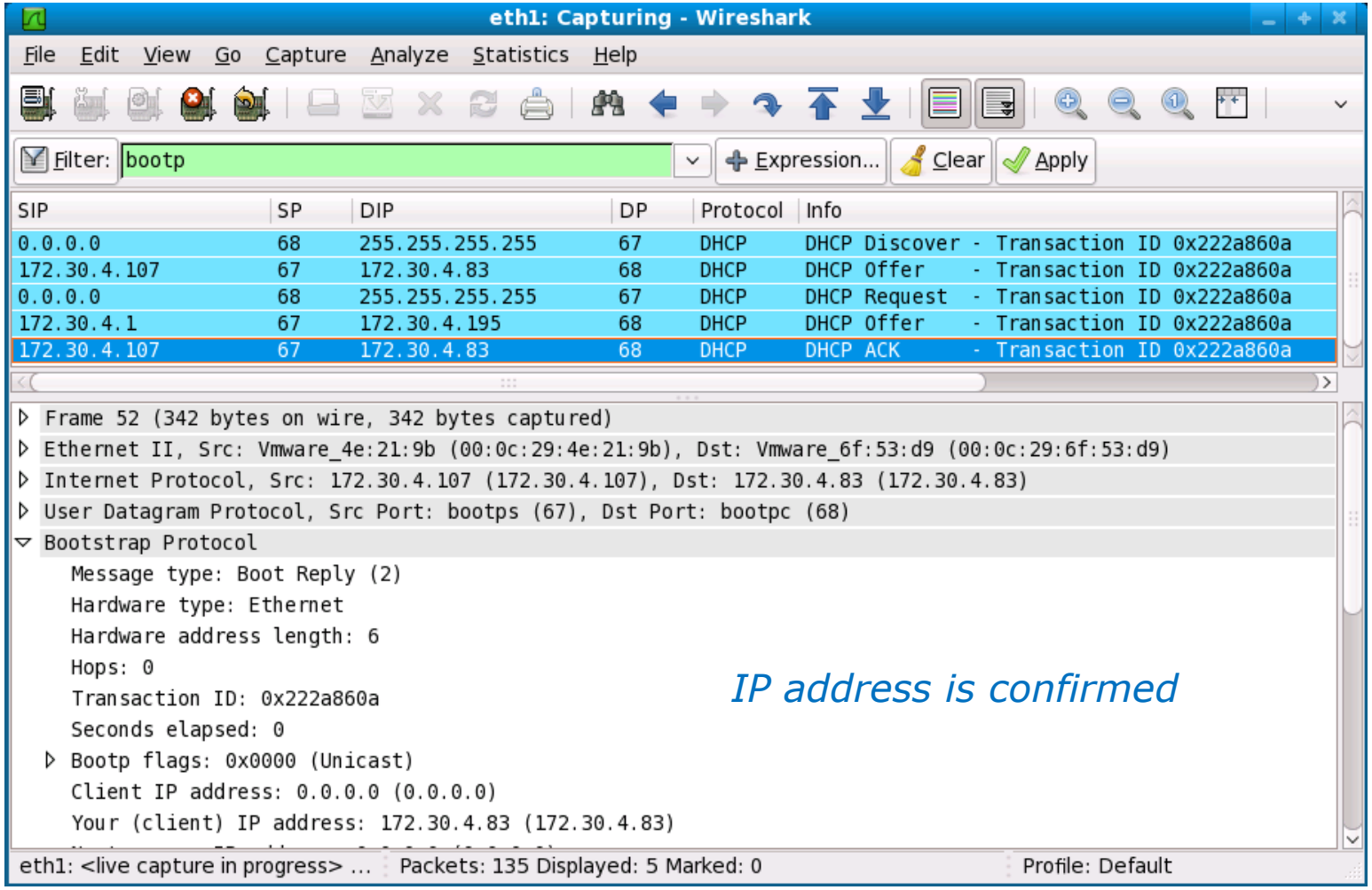
eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

Includes IP address and DHCP server that made the offer

elrond

*DHCP**ACK***
(unicast)

You got it!



IP address is confirmed

elrond

*DHCP**ACK***
(unicast)

You got it!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

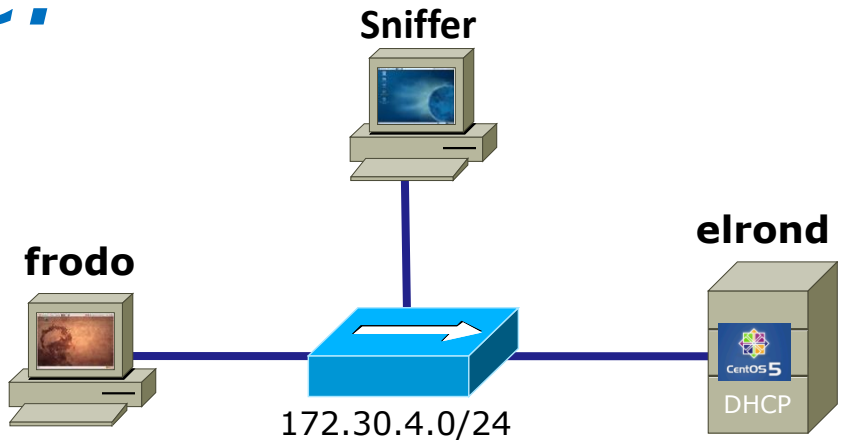
SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer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

```
    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 ACK
  ▷ 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
```

Lease time is 6 hours

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

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



DHCP Client *DHCP Server*

frodo

*DHCP**REQUEST***
(unicast)

I want to renew the lease!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

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

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

Request unicast to the DHCP server

IP address

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

frodo

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

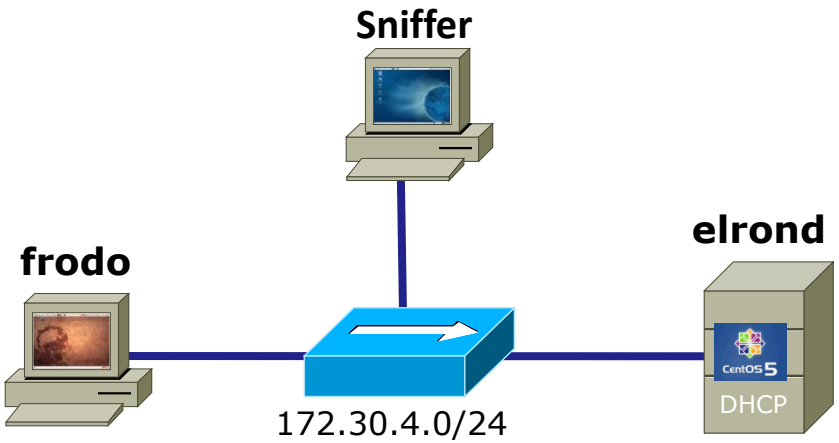
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction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

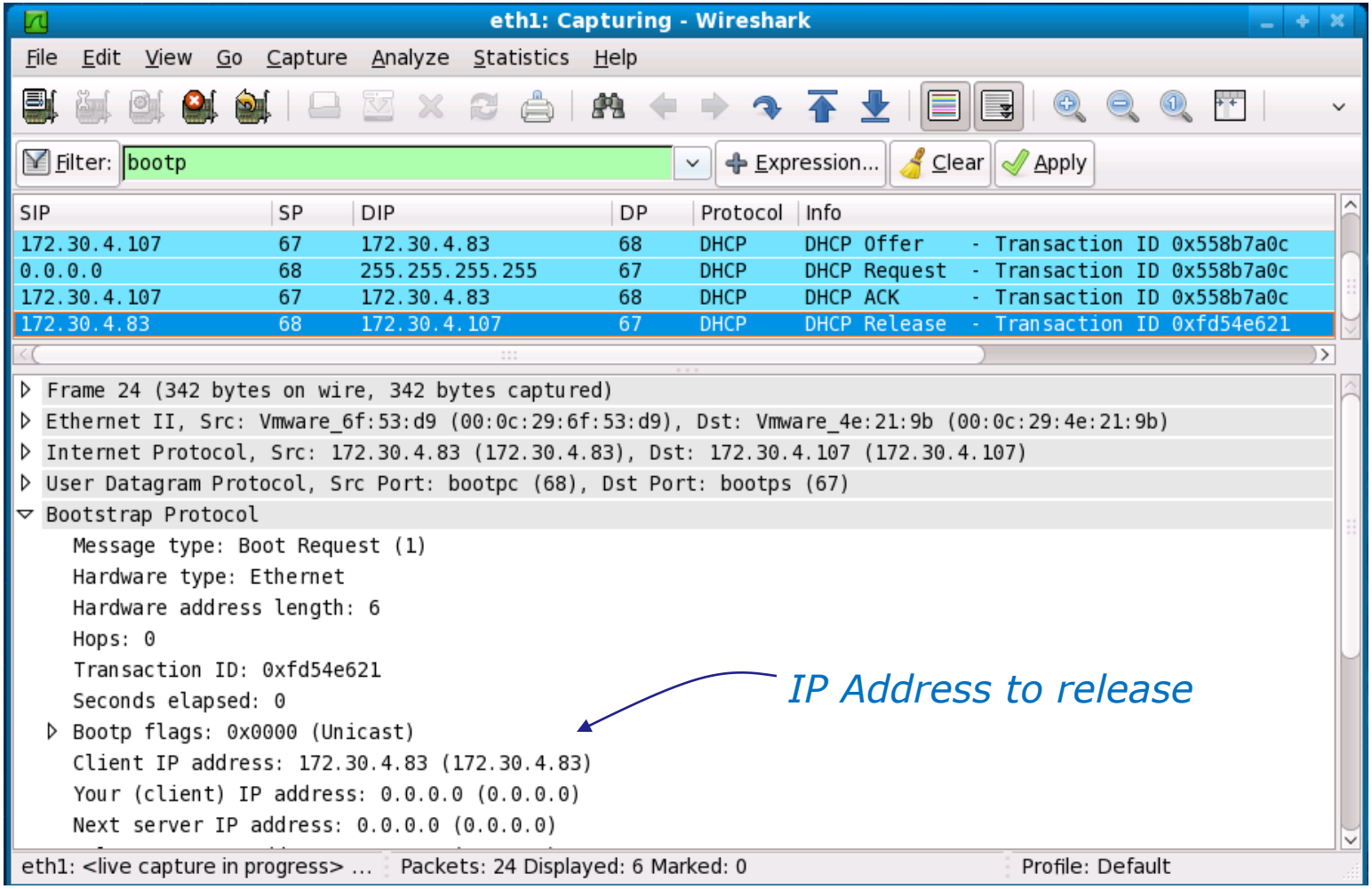


DHCP Client *DHCP Server*

frodo

*DHCP**RELEASE***
(unicast)

I want out!



frodo

*DHCP**RELEASE***
(unicast)

I want out!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

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

SIP	SP	DIP	DP	Protocol	Info
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x558b7a0c
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x558b7a0c
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x558b7a0c
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Release - Transaction ID 0xfd54e621

```
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 172.30.4.83 (172.30.4.83)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    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 Release
  ▷ Option: (t=54,l=4) Server Identifier = 172.30.4.107
  ▷ Option: (t=12,l=5) Host Name = "frodo"
    End Option
    Padding
```

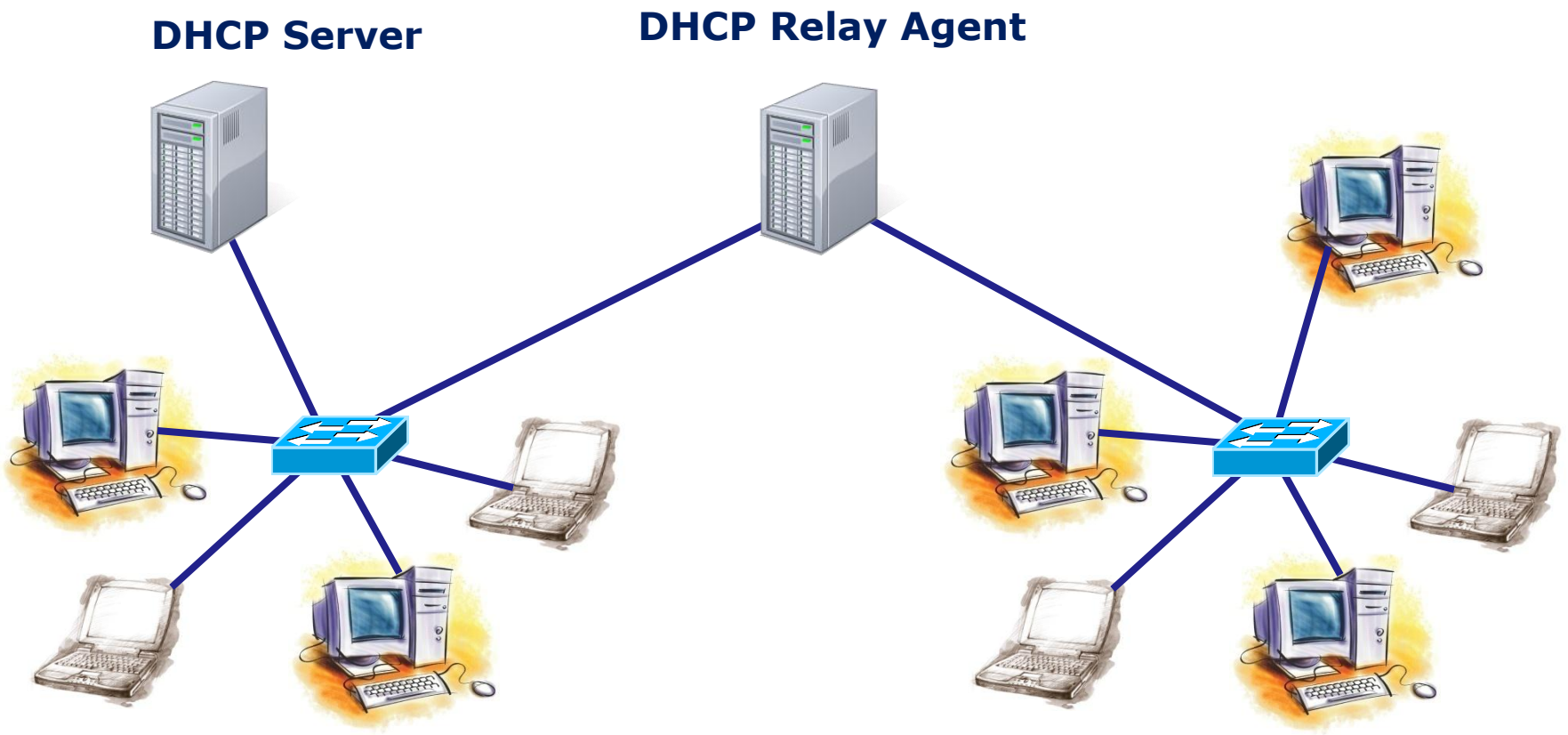
DHCP server and client hostname

eth1: <live capture in progress> ... | Packets: 24 Displayed: 6 Marked: 0 | Profile: Default

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 ~]# _
```

Use the –v option on newer distributions to see the activity

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 ~]# _
```

Use the –v option on newer distributions to see the activity

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
```

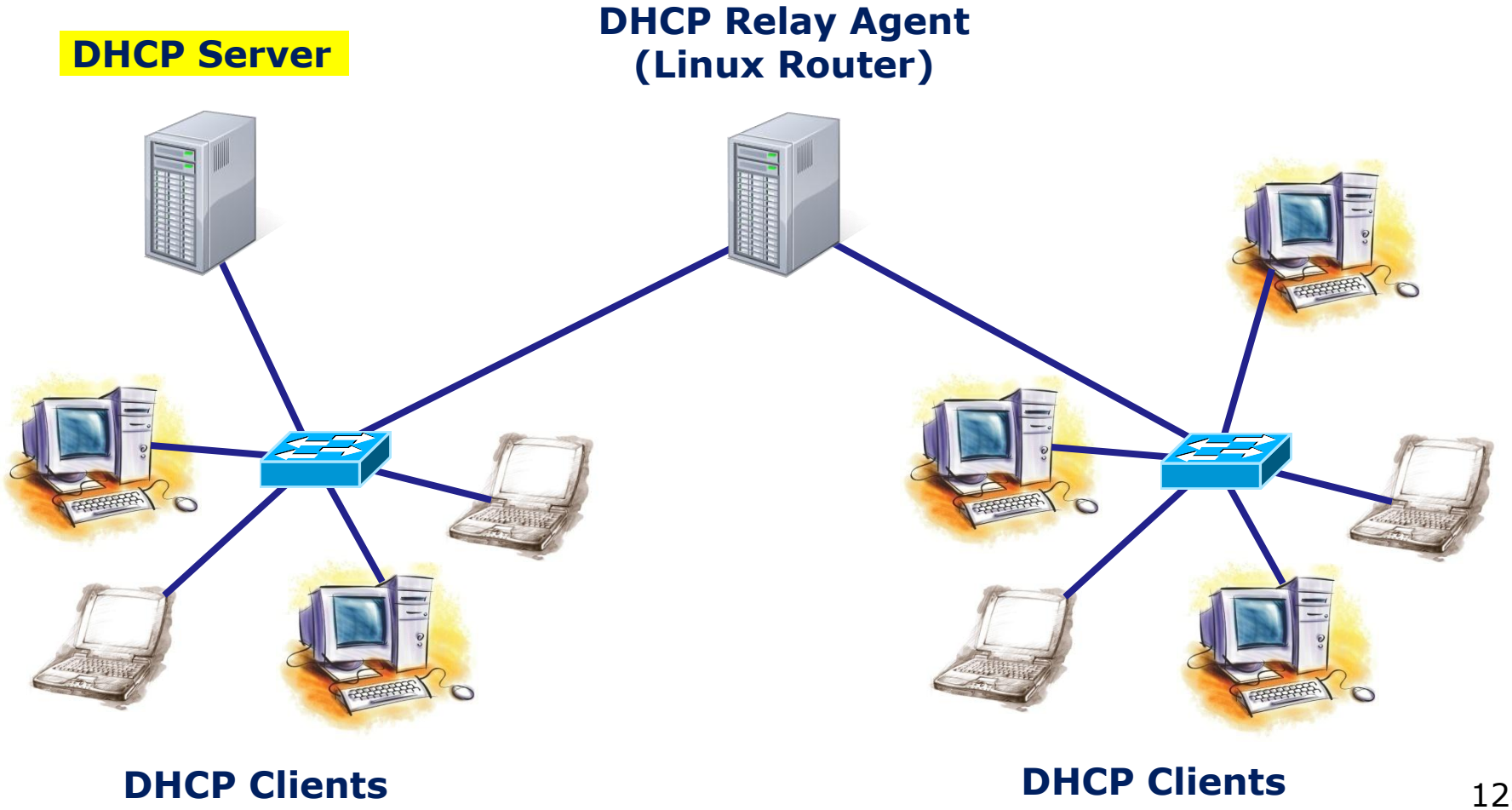
Red Hat Family DHCP client example

```
[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]#
```

Step 2 Edit configuration file

dhcpd.conf sample walkthrough

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

Global settings

```
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 ~]#
```

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

Subnet specific settings

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

DHCP options that can be assigned to clients

```
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 ~]#
```

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

Default gateway to assign for this subnet

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

Default netmask to assign for this subnet

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

The DNS server to assign

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

Offset in seconds from GMT

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

Pool of IP addresses to assign

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

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

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

subnet 192.168.0.0 netmask 255.255.255.0 {

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

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

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

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

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

IP reservation based on MAC address

dhcpd.conf
for
the DHCP lab
(old)

elrond

DHCP

Global and specific settings for DHCP Lab Rivendell subnet

Note new location of configuration file

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

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

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

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

Will be the eth1 interface on your station's Elrond

DHCP

elrond

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

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

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

DHCP

elrond

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

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

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

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

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

dhcpd.conf
for
the DHCP lab
(latest)

elrond

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

Global and specific settings for CIS Lab subnet

Note new location of configuration file

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

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

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

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

elrond

Settings for Rivendell and Mordor subnets

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

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

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

Installing and Configuring DHCP

Step 3 *Configure firewall*

Open UDP port 67 as a destination
iptables -I INPUT 1 -p udp -m udp --dport 67 -j ACCEPT

Save current settings with revised port 67 rule
service iptables save

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@celebrian ~]# getenforce
Enforcing
[root@celebrian ~]#
```

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

Step 8 Troubleshooting with tcpdump

```
[root@L6-Elrond ~]# tcpdump -i eth1 -nevv udp port 67
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
16:53:15.864882 00:0c:29:1f:b1:48 > Broadcast, ethertype IPv4 (0x0800), length 342: (tos 0x10, ttl 128, id 0,
offset 0, flags [none], proto UDP (17), length 328)
    0.0.0.0.bootpc > 255.255.255.255.bootps: [udp sum ok] BOOTP/DHCP, Request from 00:0c:29:1f:b1:48, length
300, xid 0x96dfc713, Flags [none] (0x0000)
          Client-Ethernet-Address 00:0c:29:1f:b1:48
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 172.30.4.51
            Parameter-Request Option 55, length 12:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Hostname, YD
              YS, NTP, MTU, Option 119
<snipped >
```

Installing and Configuring vsftpd

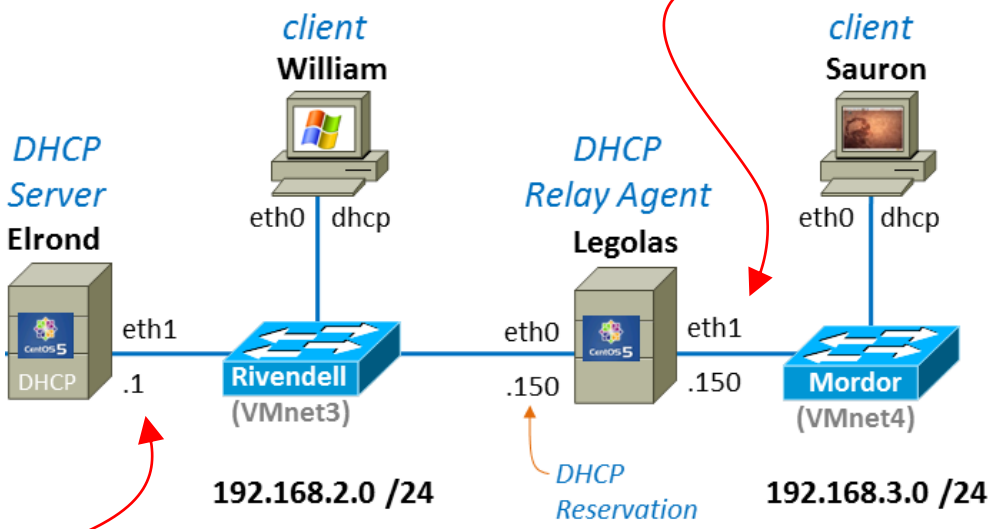
Step 9 Monitor log files

```
[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

DORA via DHCP Relay

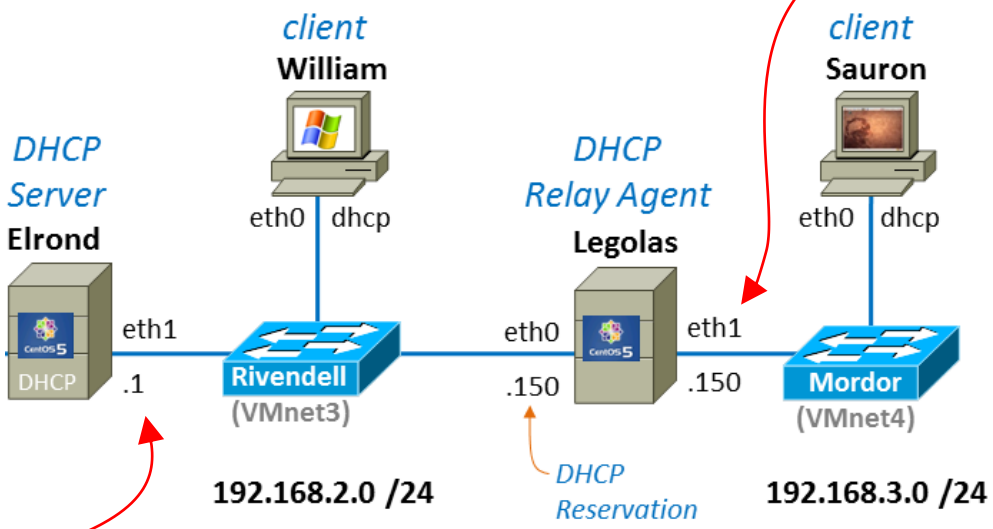
Source	SP	Destination	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0xad210e79
192.168.3.150	67	192.168.3.50	68	DHCP	DHCP Offer - Transaction ID 0xad210e79
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0xad210e79
192.168.3.150	67	192.168.3.50	68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



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

Release via DHCP Relay

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



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

DHCP

DHCP Architecture

DHCP Servers

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

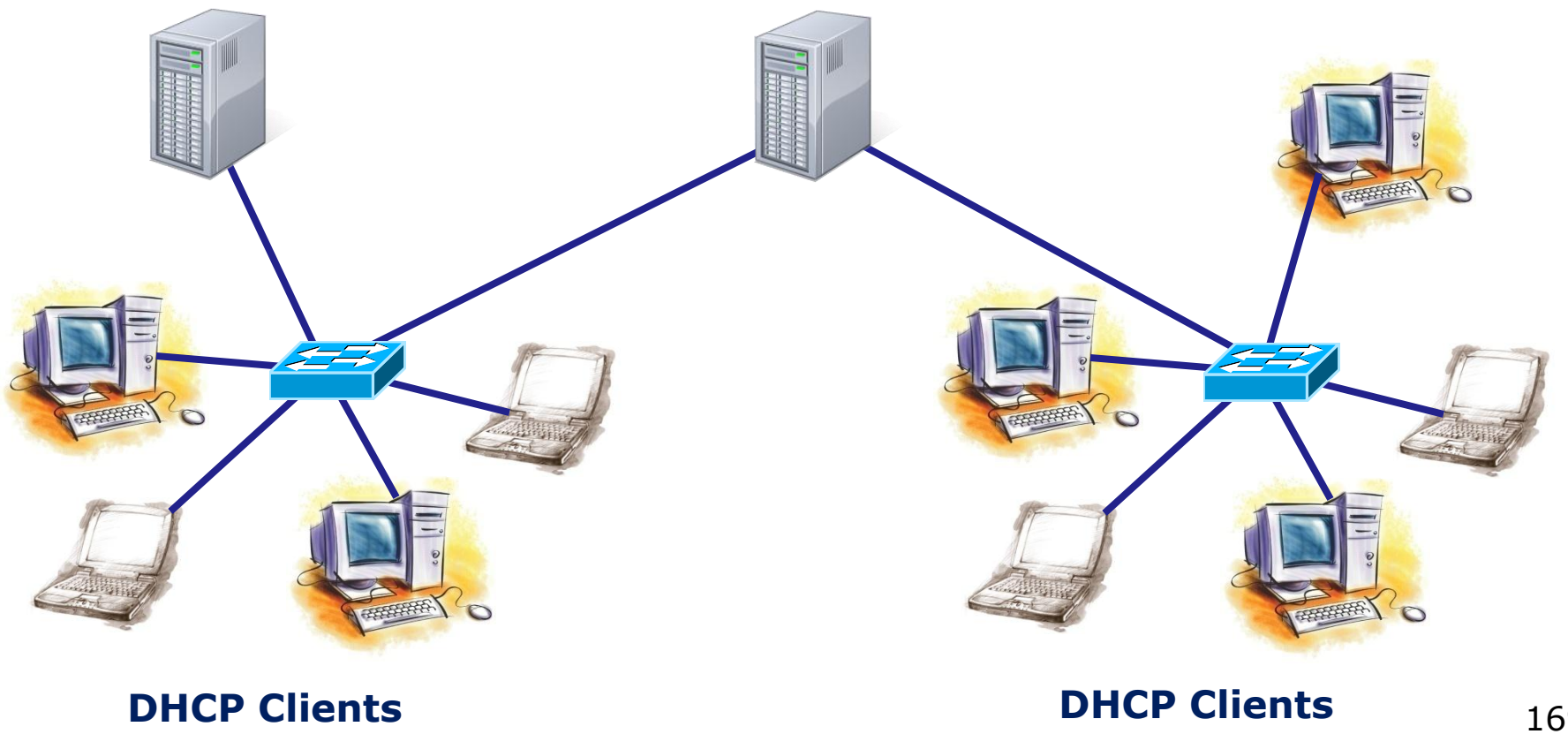
DHCP Relay Agents

DHCP Clients

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

DHCP

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

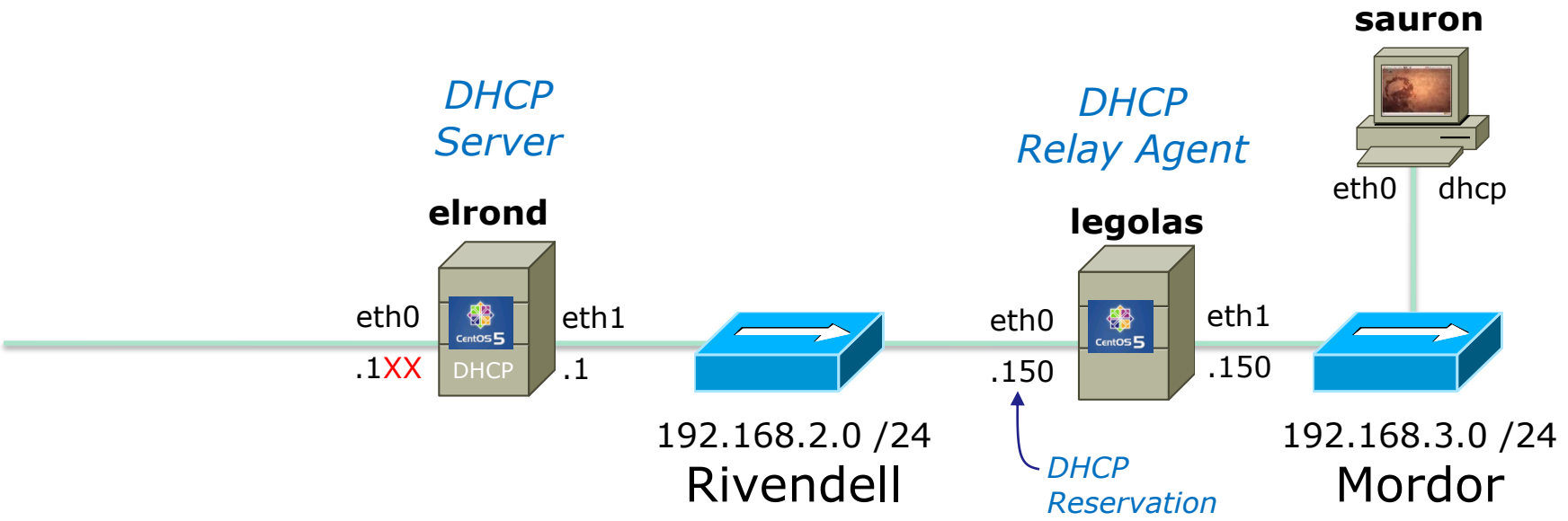
Is it installed?

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

Save current settings with revised port 67 rule
service iptables save

Restart firewall using revised permanent settings
service iptables restart

SELinux for DHCP relay agent (CentOS)

Step 4 *Configure SELinux*

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

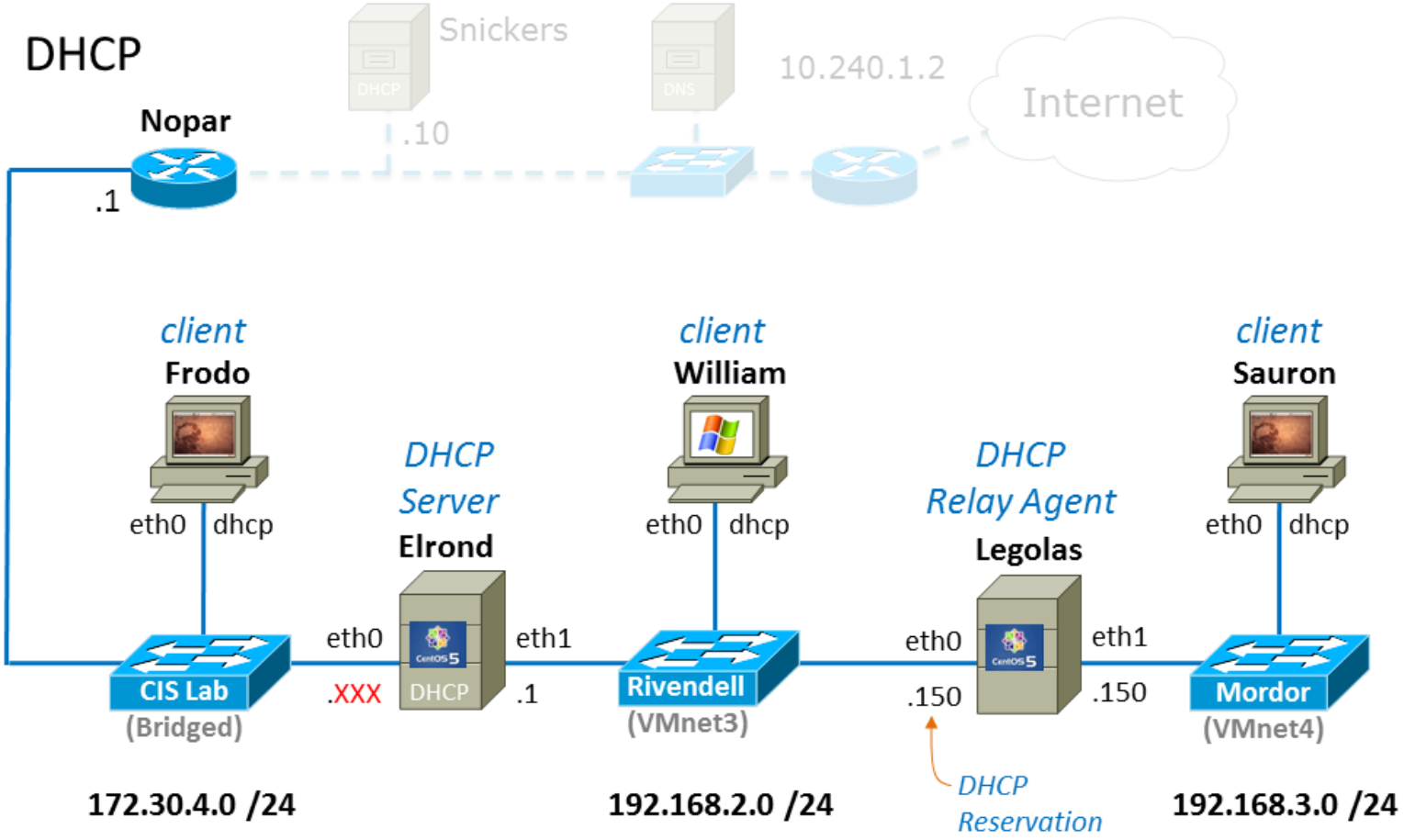
legolas

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 >
```

DHCP Lab

DHCP Lab


DHCP
Snickers
DHCP
DNS
10.240.1.2
Internet
Nopar
.10
.1
client
Frodo
eth0
dhcp
DHCP
Server
Elrond
eth0
eth1
.XXX
DHCP
.1
CIS Lab
(Bridged)
client
William
eth0
dhcp
Rivendell
(VMnet3)
DHCP
Relay Agent
Legolas
eth0
eth1
.150
.150
client
Sauron
eth0
dhcp
Mordor
(VMnet4)
DHCP
Reservation
172.30.4.0 /24
192.168.2.0 /24
192.168.3.0 /24

Wrap

New commands, daemons:

service dhcpd restart

service dhcrelay restart

Daemons and related configuration files

/etc/dhcp/dhcpd.conf

/etc/sysconfig/dhcrelay

/var/lib/dhcpd/dhcpd.leases

/var/lib/dhclient/dhclient.leases

/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?

Backup