Lesson Module Status

- Slides
- Whiteboard with 1st minute quiz

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

- Test T3 uploaded
- Lab 10 uploaded
- Hershey configured as NIS server for test

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

Course history and credits

Jim Griffin

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

Rick Graziani

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

CIS 192 - Lesson 14

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


Solomon


Sean C.


Chris


Corey


Bryan

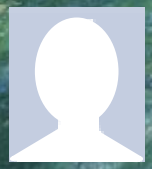

Sean F.


Tony


David


Donna

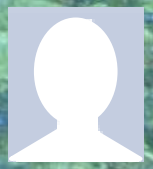

Dave


Evan


Gabriel


Elia


Tajvia


Carlos


Adam


Ben

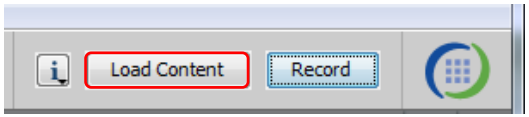

Laura

VMs for tonight
Celebrian, Frodo

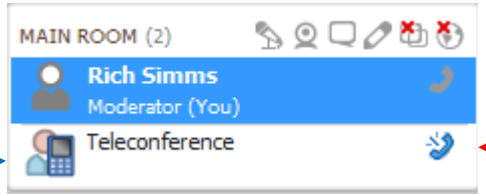
Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

CCC Confer

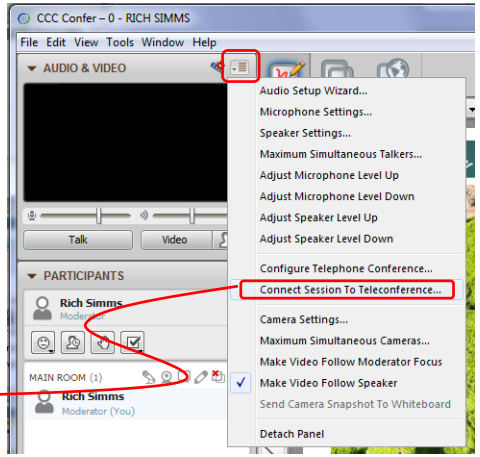
[ ] Preload White Board with *cis*lesson??*-WB*



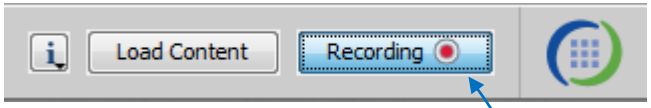
[ ] Connect session to Teleconference



Session now connected to teleconference

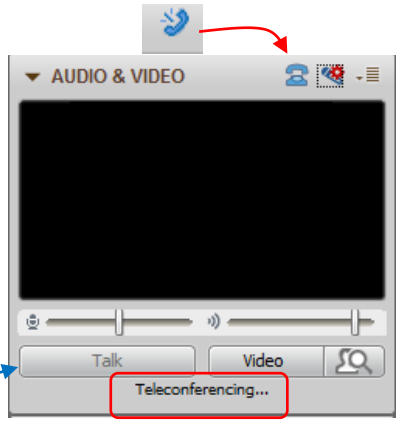


[ ] Is recording on?



Red dot means recording

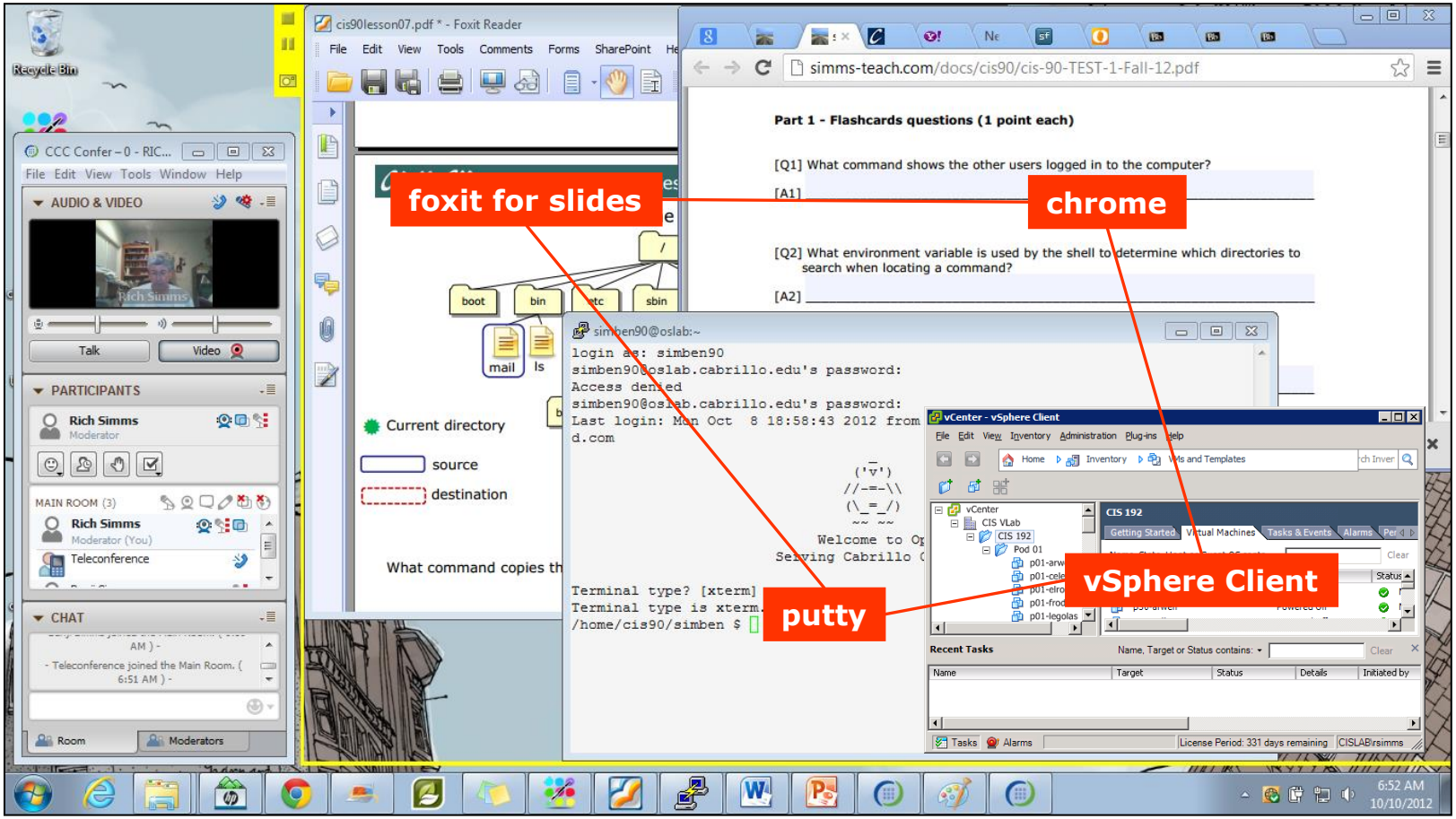
[ ] Use teleconferencing, not mic



Should be greyed out

[ ] **Video (webcam) optional**

[ ] **layout and share apps**

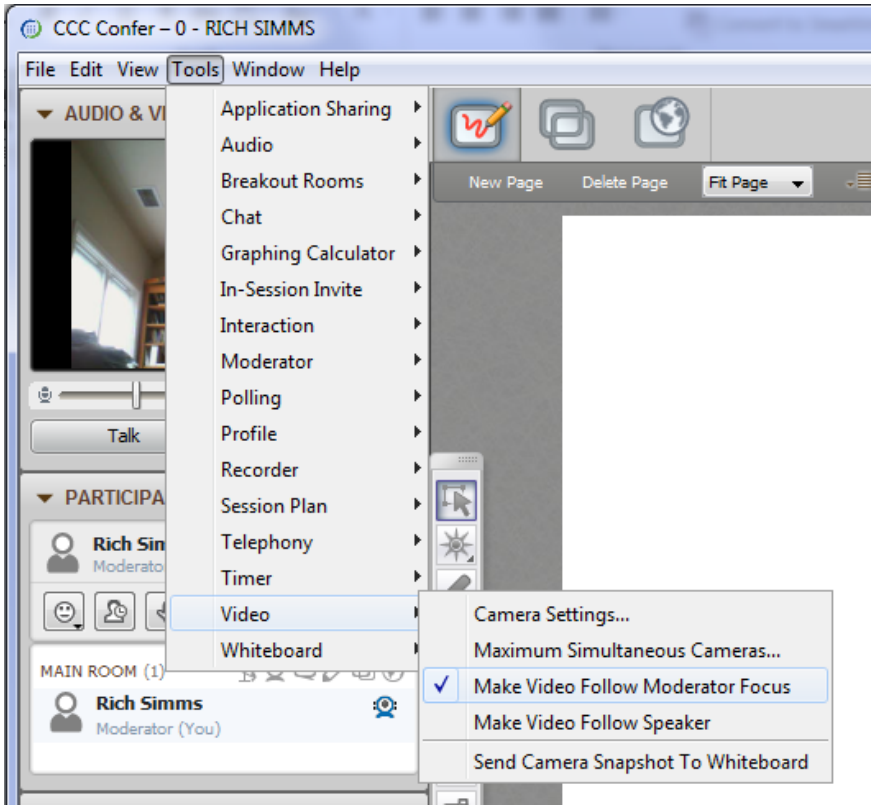


CCC Confer

[ ] **Video (webcam) optional**

[ ] **Follow moderator**

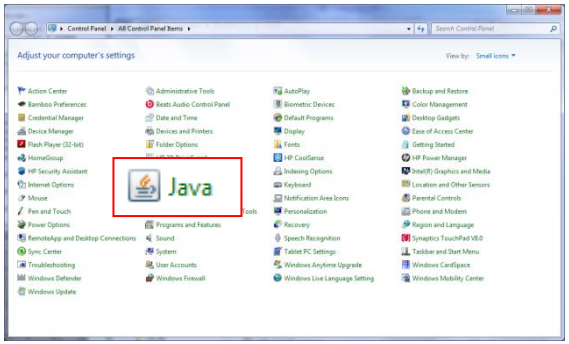
[ ] **Double-click on postages stamps**



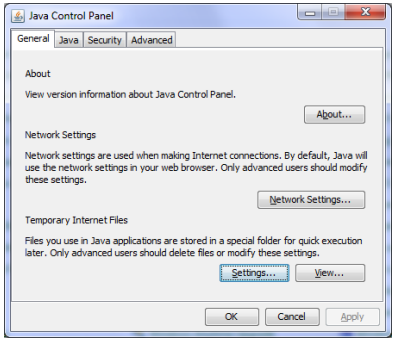
Universal Fix for CCC Confer:

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

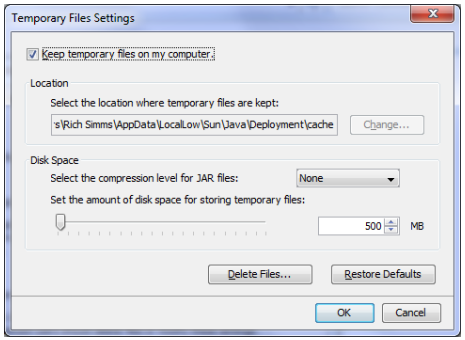
Control Panel (small icons)



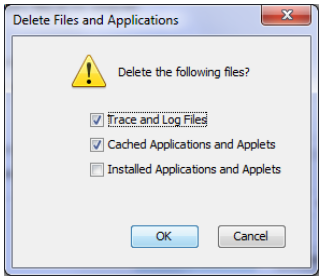
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Internet Services

Objectives	Agenda
• Setup and configure a FTP service • Setup and configure a web server	• Quiz • Questions on previous material • Housekeeping • NIS recap • FTP review • Apache web server • Test 3 • Wrap

First Minute Quiz

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

NO MORE QUIZZES!

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

Questions on previous material

Questions?

- Graded work in home directories
- Answers in /home/cis192/answers

Lesson material?

Labs? Tests?

How this course works?

Who questions much, shall learn much, and retain much.
- Francis Bacon

If you don't ask, you don't get.
- Mahatma Gandhi

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

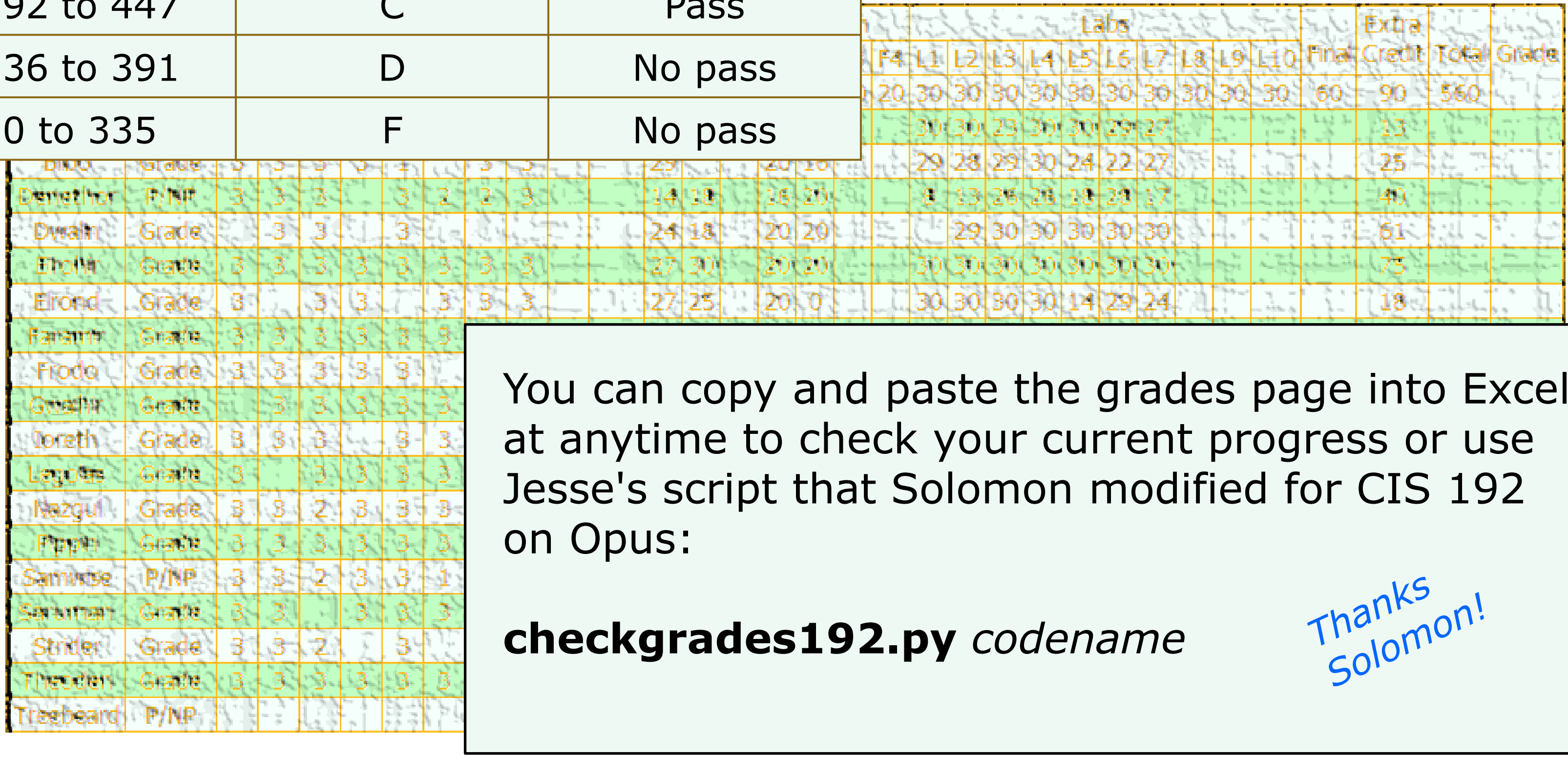
Housekeeping

- Test 3 tonight
- Lab 10 due next week
- Final in two weeks

Grades Check

504 or higher	A	Pass
448 to 503	B	Pass
392 to 447	C	Pass
336 to 391	D	No pass
0 to 335	F	No pass

Your grade in this course is based solely on how many points you earn



You can copy and paste the grades page into Excel at anytime to check your current progress or use Jesse's script that Solomon modified for CIS 192 on Opus:

checkgrades192.py *codename*

Thanks Solomon!

- Remaining point earning opportunities

Work	Points
Test T3	30
Forum F4	20
Lab L10	30
Final	60
Extra Credit	up to 90

Extra Credit

- Note you can earn up to 90 points of extra credit (labs, typos, HowTos, etc.)
- 3 extra credit labs
- HowTos
  - Up to 20 points extra credit for a publishable HowTo document (will be published on the class website)
  - 10 points additional if you do a class presentation
  - Topics must be pre-approved with instructor

Final Exam

- Timed test
- Open book, notes and computer
- You will be provided with a pristine exam pod
- There will be a number of tasks to implement
    - Some mandatory
    - Some optional
    - Some extra credit
    - Task specifications available one week in advance
- 60 points - the more tasks completed, the more points earned

- -	6/4	**Final Exam for CIS 192** **Time** • 5:30PM - 8:20PM in Room 2501 **Materials** • Presentation slides (download) • Test (download)		5 posts Extra Credit Labs

Preparing for the final exam

- Know where to locate information quickly
- Make a network map & crib sheet
- "Muscle memory" for basic commands
- Practice makes perfect

Help with labs

Like some help with labs?

I'm in the CIS Lab Monday afternoons

- See schedule at http://webhawks.org/~cislab/

or see me during office hours

or contact me to arrange another time online

vsftpd review & troubleshooting

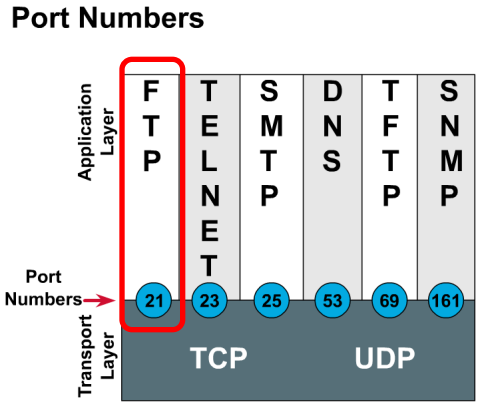
Installing and Configuring Telnet (Red Hat Family)

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

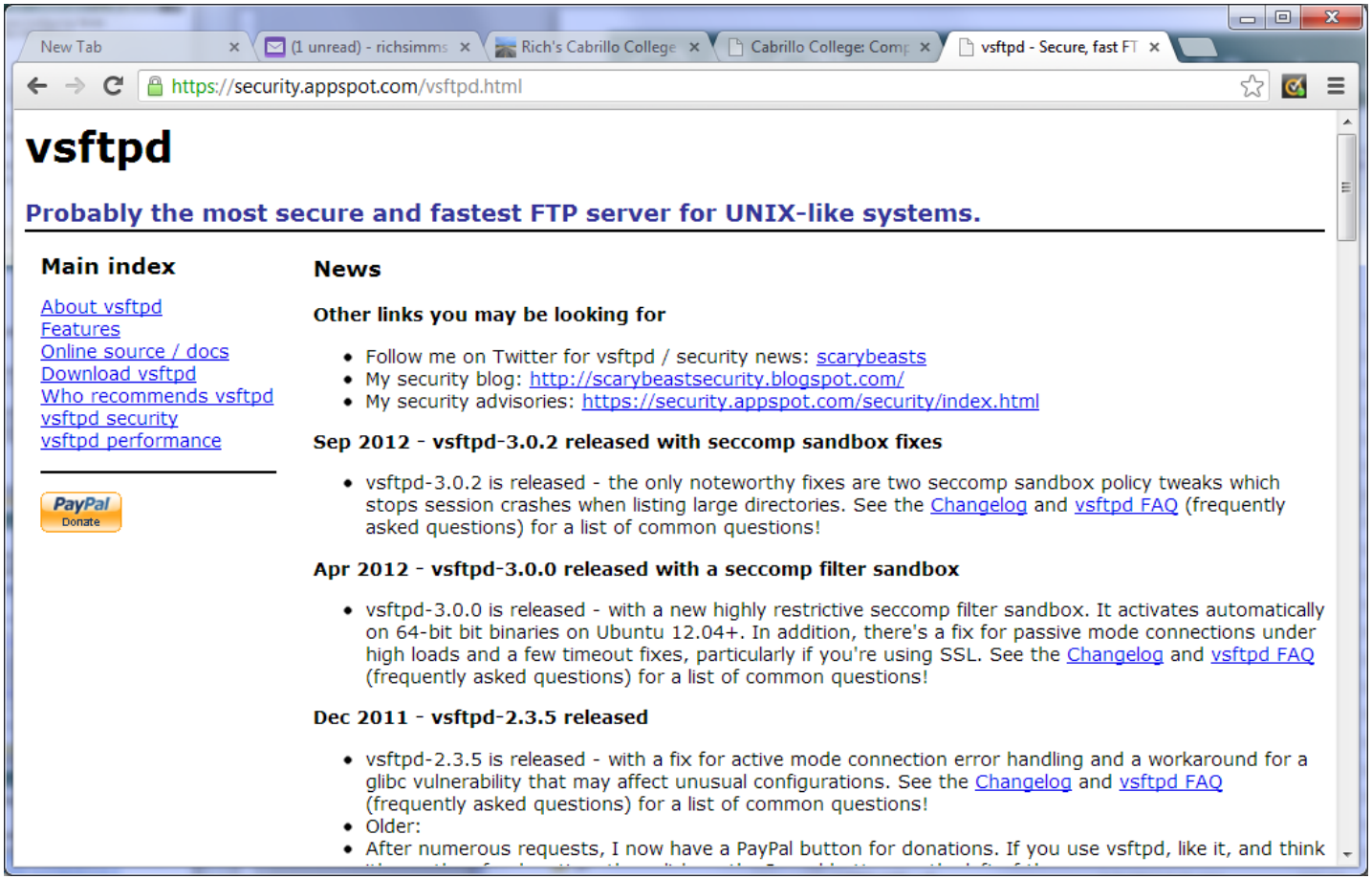
Two sockets are used
- One for commands (requests and responses)
- One for data transfer

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
yum install vsftpd

Configuration file: /etc/vsftpd/vsftpd.conf

Firewall Ports Used: 21/TCP (commands) , 20/TCP (data)
Firewall helper modules: nf_conntrack_ftp, nf_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)

Step 1 ***Installing software***

Is it installed?

```
[root@elrond ~]# rpm -qa | grep vsftpd
vsftpd-2.2.2-11.el6_4.1.x86_64
```

No response means it is not installed

To install:

yum install vsftpd

vsftpd

Step 2 Customize the configuration file

/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 >

ftpd_banner=Welcome to the Simms FTP service. *(modify this to customize welcome banner)*

< snipped >

chroot_local_user=YES *(uncomment this to put users in "chroot jail")*

< snipped >

tcp_wrappers=YES *(this is uncommented by default)*

Installing and Configuring vsftpd

Step 3 ***Firewall settings***

1. Modify the firewall to allow incoming new FTP (TCP port 21) connections.

2. Load nf_conntrack_ftp kernel and nf_nat_ftp modules to track related connections

Firewall Configuration for FTP

Step 3 *Customize the firewall*

Open port 21 in the firewall

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

this line number varies depending on your firewall

To make the firewall change permanent

service iptables save

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.

modprobe nf_conntrack_ftp **modprobe nf_nat_ftp**	*Use modprobe command to load (temporary)*
lsmod	*Use lsmod command to verify if loaded*

/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 >
```

To load modules at system boot (permanent), modify this line in /etc/sysconfig/iptables-config

Firewall - passive mode

```
# service iptables restart
iptables: Flushing firewall rules:                          [  OK  ]
iptables: Setting chains to policy ACCEPT: filter           [  OK  ]
iptables: Unloading modules:                                [  OK  ]
iptables: Applying firewall rules:                          [  OK  ]
iptables: Loading additional modules: nf_conntrack_ftp nf_n[  OK  ]
```

In passive mode, the client initiates the connection for the data transfer. The nf_conntrack_ftp module must be loaded so the firewall will see the passive connections to random ports as "related" connections and allow them.

Firewall for FTP

/etc/sysconfig/iptables

CentOS Modified

/etc/sysconfig/iptables

```
# Generated by iptables-save v1.4.7 on Mon May 20 15:41:45 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-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 Mon May 20 15:41:45 2013
```

FTP port is open

Viewing this file not only shows the permanent firewall settings, it also shows the actual arguments used on the iptables commands.

SELinux for vsftpd (CentOS)

Step 4 ***SELinux***

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

[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
```

required for anonymous public content

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

Step 6 ***Automatically start at system boot***

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

Installing and Configuring vsftpd

Step 7 ***Verify service is running***

vsftpd processes

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

```
[root@arwen ~]# 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@arwen ~]#
```

Individual vsftpd daemons are run for each session

Installing and Configuring vsftpd

netstat

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

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

Installing and Configuring vsftpd

netstat

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

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

Installing and Configuring vsftpd

```
cis192@kate: ~
cis192@kate:~$ ftp 172.30.4.107
Connected to 172.30.4.107.
220 Welcome to the Simms FTP service.
Name (172.30.4.107:root): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get myfile
local: myfile remote: myfile
No control connection for command: Success
ftp> bye
cis192@kate:~$
```

```
> ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
43773 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
> ftp [ACK] Seq=1 Ack=1 Win=5856 Len=0
se: 220 Welcome to the Simms FTP service.
> ftp [ACK] Seq=1 Ack=40 Win=5856 Len=0
t: USER cis192
43773 [ACK] Seq=40 Ack=14 Win=5888 Len=0
se: 331 Please specify the password.
> ftp [ACK] Seq=14 Ack=74 Win=5856 Len=0
10.8.731806  172.30.4.222  172.30.4.107  FTP  Request: PASS Cabrillo
```

```
Frame 4 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: Vmware_12:50:1e (00:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.222 (172.30.4.222)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 43773 (43773), Seq: 1, Ack: 1, Len: 39
File Transfer Protocol (FTP)
  220 Welcome to the Simms FTP service.\r\n
```

Frame (frame), 93 bytes | Packets: 39 Displayed: 39 Marked: 0 Dropped: 0 | Profile: Default

3-way handshake

Login is transmitted in clear text

FTP use port 21 for commands and messages

Installing and Configuring vsftpd

cis192@kate: ~

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.30.4.222	172.30.4.107	TCP	43773 > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
2	0.000047	172.30.4.107	172.30.4.222	TCP	ftp > 43773 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
3	0.000088	172.30.4.222	172.30.4.107	TCP	43773 > ftp [ACK] Seq=1 Ack=1 Win=5856 Len=0
4	0.024980	172.30.4.107	172.30.4.222	FTP	Response: 220 Welcome to the Simms FTP service.
5	0.025530	172.30.4.222	172.30.4.107	TCP	43773 > ftp [ACK] Seq=1 Ack=40 Win=5856 Len=0
6	4.864213	172.30.4.222	172.30.4.107	FTP	Request: USER cis192
7	4.864313	172.30.4.107	172.30.4.222	TCP	ftp > 43773 [ACK] Seq=40 Ack=14 Win=5888 Len=0
8	4.864343	172.30.4.107	172.30.4.222	FTP	Response: 331 Please specify the password.
9	4.889841	172.30.4.222	172.30.4.107	TCP	43773 > ftp [ACK] Seq=14 Ack=74 Win=5856 Len=0
10	8.731806	172.30.4.222	172.30.4.107	FTP	Request: PASS Cabrillo

```
Frame 4 (93 bytes on wire, 93 bytes captured)
Ethernet II, Src: Vmware_12:50:1e (00:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.222 (172.30.4.222)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 43773 (43773), Seq: 1, Ack: 1, Len: 39
File Transfer Protocol (FTP)
  220 Welcome to the Simms FTP service.\r\n
```

Frame (frame), 93 bytes | Packets: 39 Displayed: 39 Marked: 0 Dropped: 0 | Profile

3-way handshake

Login is transmitted in clear text

FTP use port 21 for commands and messages

Socket for commands

Client	Server
172.30.4.222	172.30.4.107
43773	21

Installing and Configuring vsftpd

cis192@kate: ~

```
cis192@kate:~$ ftp 172.30.4.107
```

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	13.149468	172.30.4.107	172.30.4.222	FTP	Response: 200 PORT command successful. Consider using PA
23	13.149519	172.30.4.222	172.30.4.107	FTP	Request: RETR myfile
24	13.153406	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV
25	13.153496	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
26	13.153511	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [ACK] Seq=1 Ack=1 Win=5888 Len=0
27	13.153540	172.30.4.107	172.30.4.222	FTP	Response: 150 Opening BINARY mode data connection for my
28	13.153807	172.30.4.107	172.30.4.222	FTP-DATA	FTP Data: 12 bytes
29	13.154286	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [FIN, ACK] Seq=13 Ack=1 Win=5888 Len=0
30	13.186151	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [ACK] Seq=1 Ack=13 Win=5856 Len=0

```
Frame 28 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Vmware_12:50:1e (00:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.222 (172.30.4.222)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 35677 (35677), Seq: 1, Ack: 1, Len: 12
FTP Data
    FTP Data: Linux Rules\n
```

Port 20 (and higher) is used for FTP data transfers

Frame (frame), 66 bytes | Packets: 39 Displayed: 39 Marked: 0 Dropped: 0 | Profile: Default

The Wireshark capture illustrates encapsulation and sockets

Installing and Configuring vsftpd

cis192@kate: ~

```
cis192@kate:~$ ftp 172.30.4.107
```

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	13.149468	172.30.4.107	172.30.4.222	FTP	Response: 200 PORT command successful. Consider using PA
23	13.149519	172.30.4.222	172.30.4.107	FTP	Request: RETR myfile
24	13.153406	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV
25	13.153496	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
26	13.153511	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [ACK] Seq=1 Ack=1 Win=5888 Len=0
27	13.153540	172.30.4.107	172.30.4.222	FTP	Response: 150 Opening BINARY mode data connection for my
28	13.153807	172.30.4.107	172.30.4.222	FTP-DATA	FTP Data: 12 bytes
29	13.154286	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [FIN, ACK] Seq=13 Ack=1 Win=5888 Len=0
30	13.186151	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [ACK] Seq=1 Ack=13 Win=5856 Len=0

```
Frame 28 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Vmware_12:50:1e (00:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.222 (172.30.4.222)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 35677 (35677), Seq: 1, Ack: 1, Len: 12
FTP Data
    FTP Data: Linux Rules\n
```

Frame (frame), 66 bytes | Packets: 39 Displayed: 39 Marked: 0 Dropped: 0 | Profile: Default

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

cis192@kate: ~

```
cis192@kate:~$ ftp 172.30.4.107
```

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	13.149468	172.30.4.107	172.30.4.222	FTP	Response: 200 PORT command successful. Consider using PA
23	13.149519	172.30.4.222	172.30.4.107	FTP	Request: RETR myfile
24	13.153406	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TS\
25	13.153496	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
26	13.153511	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [ACK] Seq=1 Ack=1 Win=5888 Len=0
27	13.153540	172.30.4.107	172.30.4.222	FTP	Response: 150 Opening BINARY mode data connection for m
28	13.153807	172.30.4.107	172.30.4.222	FTP-DATA	FTP Data: 12 bytes
29	13.154286	172.30.4.107	172.30.4.222	TCP	ftp-data > 35677 [FIN, ACK] Seq=13 Ack=1 Win=5888 Len=0
30	13.186151	172.30.4.222	172.30.4.107	TCP	35677 > ftp-data [ACK] Seq=1 Ack=13 Win=5856 Len=0

```
Frame 28 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Vmware_12:50:1e (00:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.222 (172.30.4.222)
Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 35677 (35677), Seq: 1, Ack: 1, Len: 12
FTP Data
  FTP Data: Linux Rules\n
```

Frame (frame), 66 bytes Profile: Default

Socket for FTP data

Server	Client
172.30.4.107	172.30.4.107
20	35677

Installing and Configuring vsftpd

Step 8 *Troubleshooting*

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

Fix:

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

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

Installing and Configuring vsftpd

Step 8 *Troubleshooting*

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

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

Installing and Configuring vsftpd

Step 8 *Troubleshooting*

```
[root@elrond ~]# ftp arwen
Connected to arwen.
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 (arwen: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>
```

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

Installing and Configuring vsftpd

Step 9 Monitor log files

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

Installing and Configuring vsftpd

Step 10 Configure additional security

- Use OpenSSL encyption -
see: http://wiki.vpslink.com/Configuring_vsftpd_for_secure_connections_(TLS/SSL/SFTP)

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

- Enable chroot jail for local users (uncomment `chroot_local_user=YES` in /etc/vsftps/vsftpd.conf

vsftpd

Does it use TCP Wrappers?

```
[root@elrond ~]# type vsftpd
vsftpd is /usr/sbin/vsftpd
[root@elrond ~]# 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@elrond ~]#
```

yes it does

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

Arwen


```
[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 arwen sauron
```

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

Nosmo at 172.30.1.1 is NOT included

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

Everyone else is denied (this includes Nosmo)

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

Arwen


```
[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 arwen sauron

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

Sauron


```
root@sauron:~# ftp arwen
Connected to arwen.
220 Welcome to the Cabrillo Super FTP service.
Name (arwen: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


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

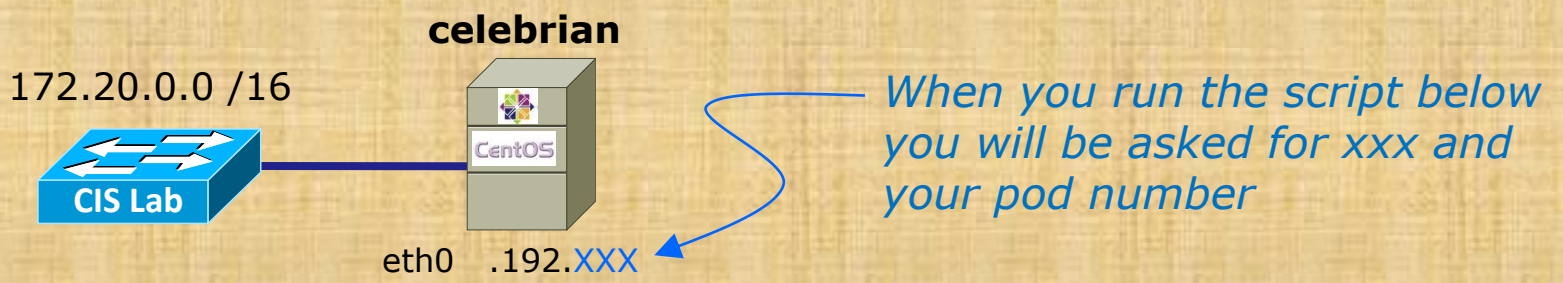
Make a fresh Celebrian

celebrian

On Celebrian

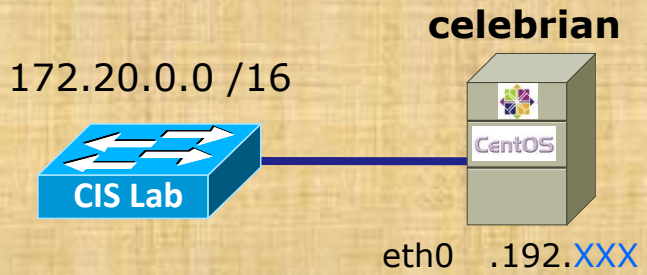
1. Revert to the Pristine snapshot
2. Power up the reverted VM and check the prompt
3. If the prompt contains "Celebrian" you are done
4. If the prompt contains "centos-master" then you must:
    - Run the **me** script and make it into a Celebrian VM for your pod
    - **init 0**
    - Take a second snapshot named Pristine-2 for future use

Configure your Celebrian for tonight



1. Revert and power-up Celebrian (if you haven't already)
2. Cable as shown
3. Log in as root
   - **dhclient -v eth0** (to join the CIS Lab network)
   - **scp *logname*@opus:/home/cis192/scripts/down* .**

Configure your Celebrian for tonight



When you run the script below you will be asked for xxx and your pod number

- **chmod 700 download-scripts-packages** (use tab complete)
- **./download-scripts-packages** (use tab complete)
- **cd bin**
- **./do-act14A-celebrian** (use tab complete)

*When finished, run **ifconfig eth0** and type your IP address into the chat window for me to ping*

Troubleshooting vsftpd

Why can't Opus users FTP into your Celebrian FTP server?

Make the fix and type your Celebrian IP address into the chat window for me (or others) to test

[optional] If that was too easy and you finish early, customize your FTP server to put local users into chroot jail when they connect

Type your Celebrian IP address into the chat window for me (or others) to test

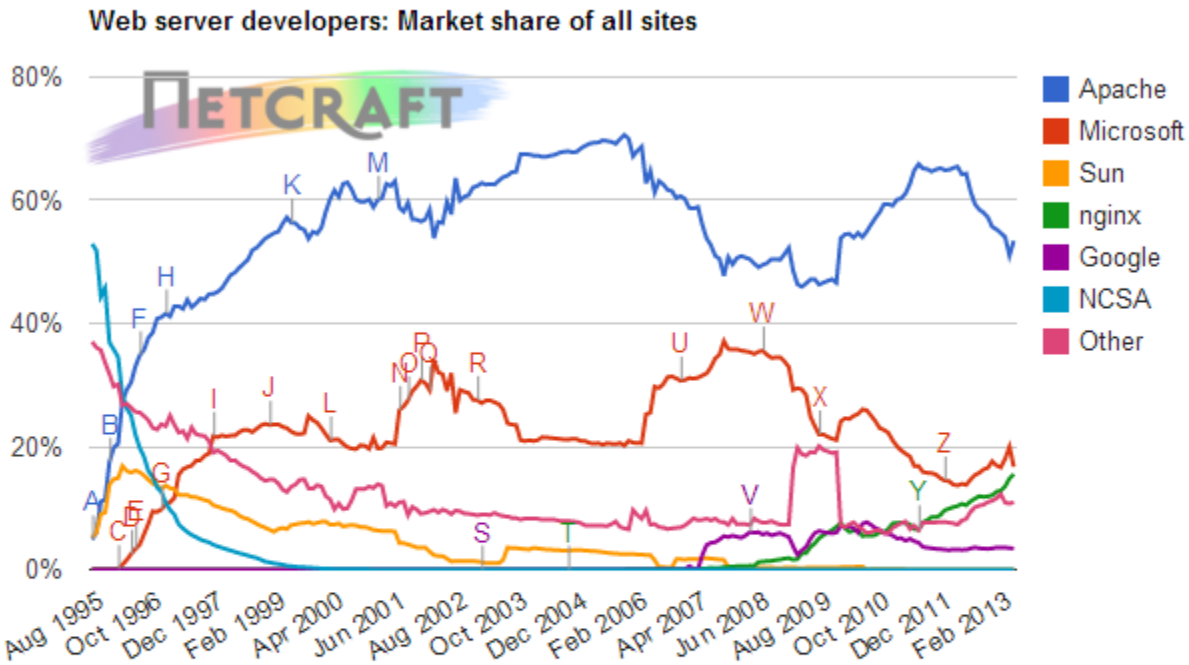
Apache

Apache Web Server

- Most widely used web server in the world
- Open-source software
- Royalty free
- Runs on UNIX, Linux, Windows, MAC OS X and others
- License is less restrictive than the GPL (can distribute closed-source derivations of the source code)
- The Apache and GPL "licensing philosophies are fundamentally incompatible".

See: http://www.apache.org/licenses/GPL-compatibility.html

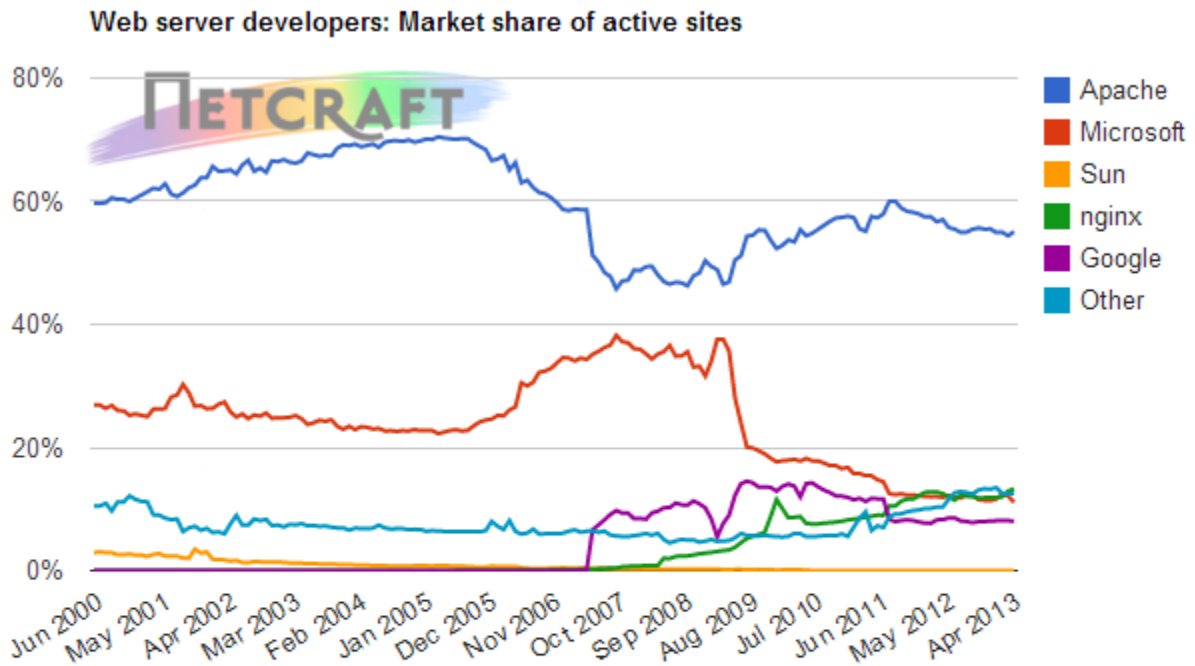
Netcraft: Market share of all sites



Developer	April 2013	Percent	May 2013	Percent	Change
Apache	331,112,893	51.01%	359,441,468	53.42%	2.41
Microsoft	129,516,421	19.95%	112,303,412	16.69%	-3.26
nginx	96,115,847	14.81%	104,411,087	15.52%	0.71
Google	22,707,568	3.50%	23,029,260	3.42%	-0.08

Source: http://news.netcraft.com/archives/web_server_survey.html

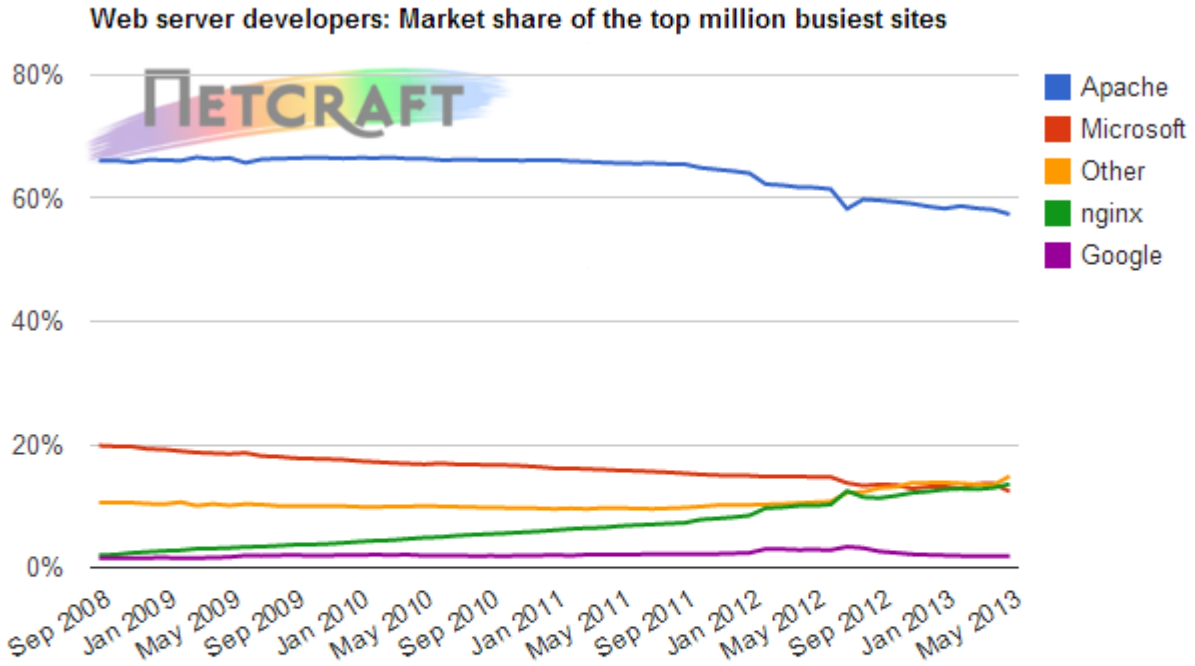
Netcraft: Market share of active sites



Developer	April 2013	Percent	May 2013	Percent	Change
Apache	101,671,575	54.37%	102,659,819	55.07%	0.69
nginx	24,138,825	12.91%	24,746,458	13.27%	0.36
Microsoft	22,686,924	12.13%	20,664,767	11.08%	-1.05
Google	15,178,507	8.12%	14,946,935	8.02%	-0.10

Source: http://news.netcraft.com/archives/web_server_survey.html

Netcraft: Market share of top million busiest sites



Developer	April 2013	Percent	May 2013	Percent	Change
Apache	581,497	58.15%	573,985	57.40%	-0.75
nginx	129,561	12.96%	135,445	13.54%	0.59
Microsoft	136,552	13.66%	123,487	12.35%	-1.31
Google	18,387	1.84%	18,721	1.87%	0.03

Source: http://news.netcraft.com/archives/web_server_survey.html

The Apache Software Foundation
http://www.apache.org/

Packages

```
# rpm -qa | grep http
httpd-manual-2.2.3-22.el5.centos
httpd-2.2.3-22.el5.centos
```

Configuration file: **/etc/httpd/conf/httpd.conf**

Firewall Ports Used: 80/TCP

SELinux

Context type for published pages: **httpd_sys_content_t**
Boolean for user home directories: **httpd_enable_homedirs**

Services and reloading configuration file changes

```
# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

Autostart the service

```
# chkconfig httpd on
```

How does a web server work

Tim Berners-Lee

Best known as the inventor of the World Wide Web

(1 unread) - richsimms - Y | Rich's Cabrillo College CIS | Linux Network Administra | Cabrillo College: Comput | W Tim Berners-Lee - Wikipe

en.wikipedia.org/wiki/Tim_Berners-Lee

Create account | Log in

Article | Talk | Read | View source | View history | Search

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages
Afrikaans
Alemannisch
العربية
Aragonés
Azərbaycanca
বাংলা
Bân-lâm-gú
Беларуская
Беларуская

Tim Berners-Lee

From Wikipedia, the free encyclopedia

Sir Timothy John "Tim" Berners-Lee, OM, KBE, FRS, FREng, FRSA (born 8 June 1955),[1] also known as "**TimBL**," is a British computer scientist, best known as the inventor of the World Wide Web. He made a proposal for an information management system in March 1989,[4] and he implemented the first successful communication between a Hypertext Transfer Protocol (HTTP) client and server via the Internet sometime around mid November.[5]

Berners-Lee is the director of the World Wide Web Consortium (W3C), which oversees the Web's continued development. He is also the founder of the World Wide Web Foundation, and is a senior researcher and holder of the Founders Chair at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL).[6] He is a director of the Web Science Research Initiative (WSRI),[7] and a member of the advisory board of the MIT Center for Collective Intelligence.[8][9]

In 2004, Berners-Lee was knighted by Queen Elizabeth II for his pioneering work.[10] In April 2009, he was elected a foreign associate of the United States National Academy of Sciences.[11][12] He was honoured as the "Inventor of the World Wide Web" during the 2012 Summer Olympics opening ceremony, in which he appeared in person, working at a NeXT Computer at the London Olympic Stadium.[13] He tweeted "This is for everyone",[14] which was instantly spelled out in LCD lights attached to the chairs of the 80,000 people in the audience.[13]

Contents [hide]

Sir Tim Berners-Lee

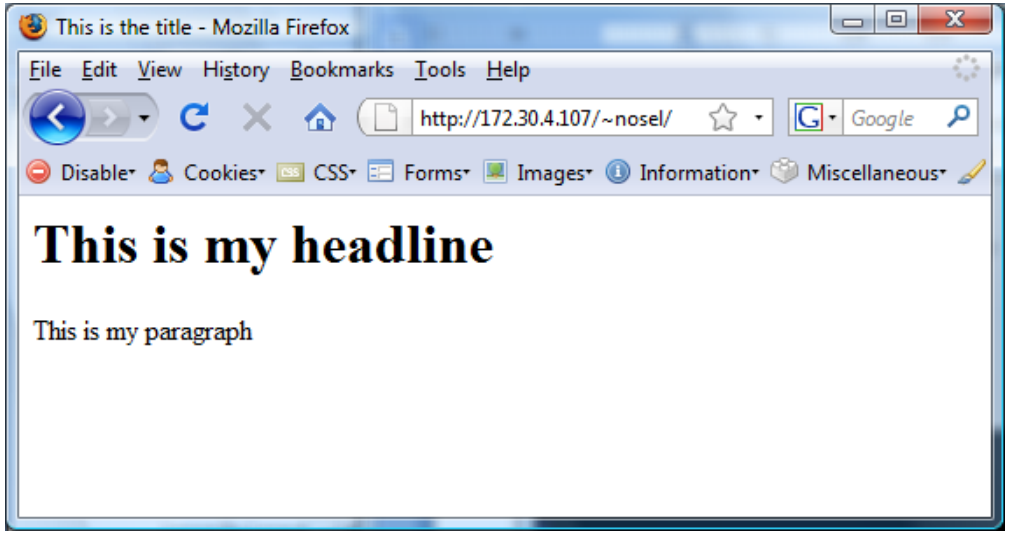
Berners-Lee in 2008

Born	Timothy John Berners-Lee 8 June 1955 (age 57)[1] London, England United Kingdom[1]
Residence	United States and United Kingdom[2]
Nationality	British
Alma mater	Queen's College, Oxford
Occupation	Computer scientist
Employer	World Wide Web Consortium

HTML Web Pages - Example 1

```
[root@elrond # cat simple.html
<html>
<head>
 <title>This is the title</title>
</head>
<body>
 <h1>This is my headline</h1>
 <p>This is my paragraph</p>
</body>
</html>
```

- A web developer will make HTML web pages (ASCII text files) on the web server.
- The web server serves these files to client browsers which renders them into a graphical format.



The default page is usually named index.html

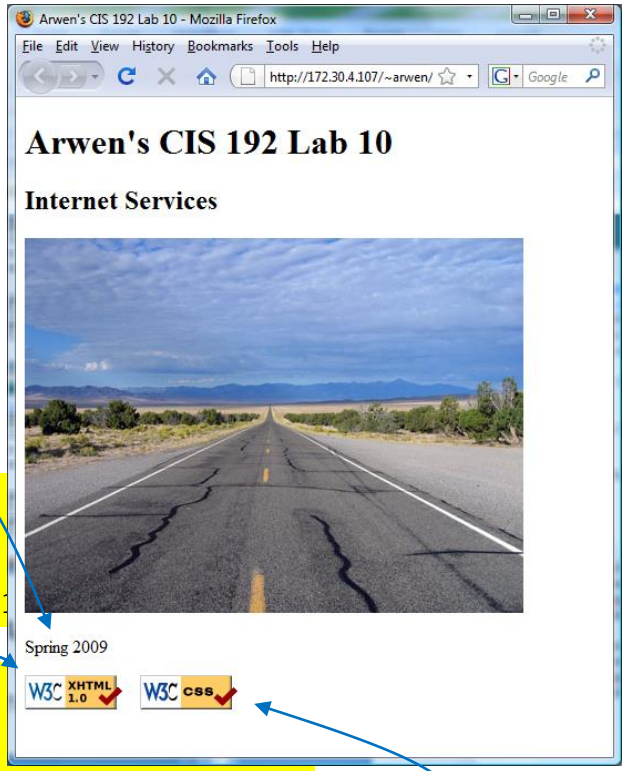
HTML Web Pages - Example 2

```
[root@elrond public_html]# cat /home/arwen/public_html/index.html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Arwen's CIS 192 Lab 10</title>
</head>
<body>
<h1>Arwen's CIS 192 Lab 10</h1>
<h2>Internet Services</h2>
<div>
<img src="hwy50.jpg" alt="Highway 50" />
</div>

<p>Spring 2009</p>

<div>
<a href="http://validator.w3.org/check/referer"
style="background-color: transparent">
<img style="border-style:none" width="88" height="31"
src="http://www.w3.org/Icons/valid-xhtml10" alt="Valid XHTML 1.0 Strict" /></a>
  
<a href="http://jigsaw.w3.org/css-validator/check/referer"
style="background-color: transparent">
<img style="border-style:none" width="88" height="31"
src="http://jigsaw.w3.org/css-validator/images/vcss" alt="Valid CSS!" /></a>
</div>

</body>
</html>
```

This is a slightly more complex html web page with an image and links to HTML and CSS validators

HTML Web Pages - Example 2

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Arwen's CIS 192 Lab 10</title>
</head>
<body>
<h1>Arwen's CIS 192 Lab 10</h1>
<h2>Internet Services</h2>
<div>
<img src="hwy50.jpg" alt="Highway 50" />
</div>

<p>Spring 2009</p>

<div>
<a href="http://validator.w3.org/check/referer"
style="background-color: transparent">
<img style="border-style:none" width="88" height="31"
src="http://www.w3.org/Icons/valid-xhtml10" alt="Valid XHTML 1
  
<a href="http://jigsaw.w3.org/css-validator/check/referer"
style="background-color: transparent">
<img style="border-style:none" width="88" height="31"
src="http://jigsaw.w3.org/css-validator/images/vcss" alt="Valid CSS!" /></a>
</div>

</body>
</html>
```



Sample web page available

Serving a Web Page

Destination port is 80

Open connection and GET command

No.	Time	SIP	SP	DIP	DP	Protocol	Info
1	0.000000	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2	0.000027	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=6
3	0.001117	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001768	192.168.0.24	52935	172.30.4.107	80	HTTP	GET /~arwen/ HTTP/1.1
5	0.002857	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1 Ack=378 Win=6912 Len=0
6	0.008379	172.30.4.107	80	192.168.0.24	52935	HTTP	HTTP/1.1 200 OK (text/html)
7	0.008412	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [FIN, ACK] Seq=1159 Ack=378 Win=6912 Len=0
8	0.010210	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [FIN, ACK] Seq=378 Ack=1159 Win=64540 Len=0
9	0.010309	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1160 Ack=379 Win=6912 Len=0
10	0.011629	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=379 Ack=1160 Win=64540 Len=0

3-way open handshake

The GET request

```
▷ Frame 4 (431 bytes on wire, 431 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_e3:93:8a (00:0c:29:e3:93:8a)
▷ Internet Protocol, Src: 192.168.0.24 (192.168.0.24), Dst: 172.30.4.107 (172.30.4.107)
▷ Transmission Control Protocol, Src Port: 52935 (52935), Dst Port: http (80), Seq: 1, Ack: 1, Len: 377
▽ Hypertext Transfer Protocol
  ▽ GET /~arwen/ HTTP/1.1\r\n
      Request Method: GET
      Request URI: /~arwen/
      Request Version: HTTP/1.1
    Host: 172.30.4.107\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.10) Gecko/2009042316 F
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
```

HTTP operates at Layer 5

Socket (layers 3 & 4)	
Client	Server
IP: 192.168.0.24	IP: 172.30.4.107
Port: 52935	Port: 80

The browser (the client) begins by initiating a 3-way handshake to open a new connection with the web server.

The highlighted packet above shows the browser requesting the default web page from Arwen's home directory using the HTTP protocol

Serving a Web Page

Source port is 80

transfer page and close connection

No.	Time	SIP	SP	DIP	DP	Protocol	Info
1	0.000000	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2	0.000027	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=6
3	0.001117	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001768	192.168.0.24	52935	172.30.4.107	80	HTTP	GET /~arwen/ HTTP/1.1
5	0.002857	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1 Ack=378 Win=6912 Len=0
6	0.008379	172.30.4.107	80	192.168.0.24	52935	HTTP	HTTP/1.1 200 OK (text/html)
7	0.008412	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [FIN, ACK] Seq=1159 Ack=378 Win=6912 Len=0
8	0.010210	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [FIN, ACK] Seq=378 Ack=1159 Win=64540 Len=0
9	0.010309	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1160 Ack=379 Win=6912 Len=0
10	0.011629	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=379 Ack=1160 Win=64540 Len=0

web page

4-way close handshake

```
Line-based text data: text/html
    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">\r\n
    <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">\r\n
    <head>\r\n
    <title>Arwen's CIS 192 Lab 10</title>\r\n
    </head>\r\n
    <body>\r\n
    <h1>Arwen's CIS 192 Lab 10</h1>\r\n
    <h2>Internet Services</h2>\r\n
    <div>\r\n
    <img src="hwy50.jpg" alt="Highway 50" />\r\n
    </div>\r\n
    \r\n
    <p>Spring 2009</p>\r\n
    \r\n
```

The contents of the web page can be seen in the layer 5 of the packet

Socket (to get web page)	
Client	Server
IP: 192.168.0.24	IP: 172.30.4.107
Port: 52935	Port: 80

The highlighted packet above shows the web page being served to the browser, using the HTTP protocol, after which the connection is closed.

Serving a Web Page via HTTP protocol

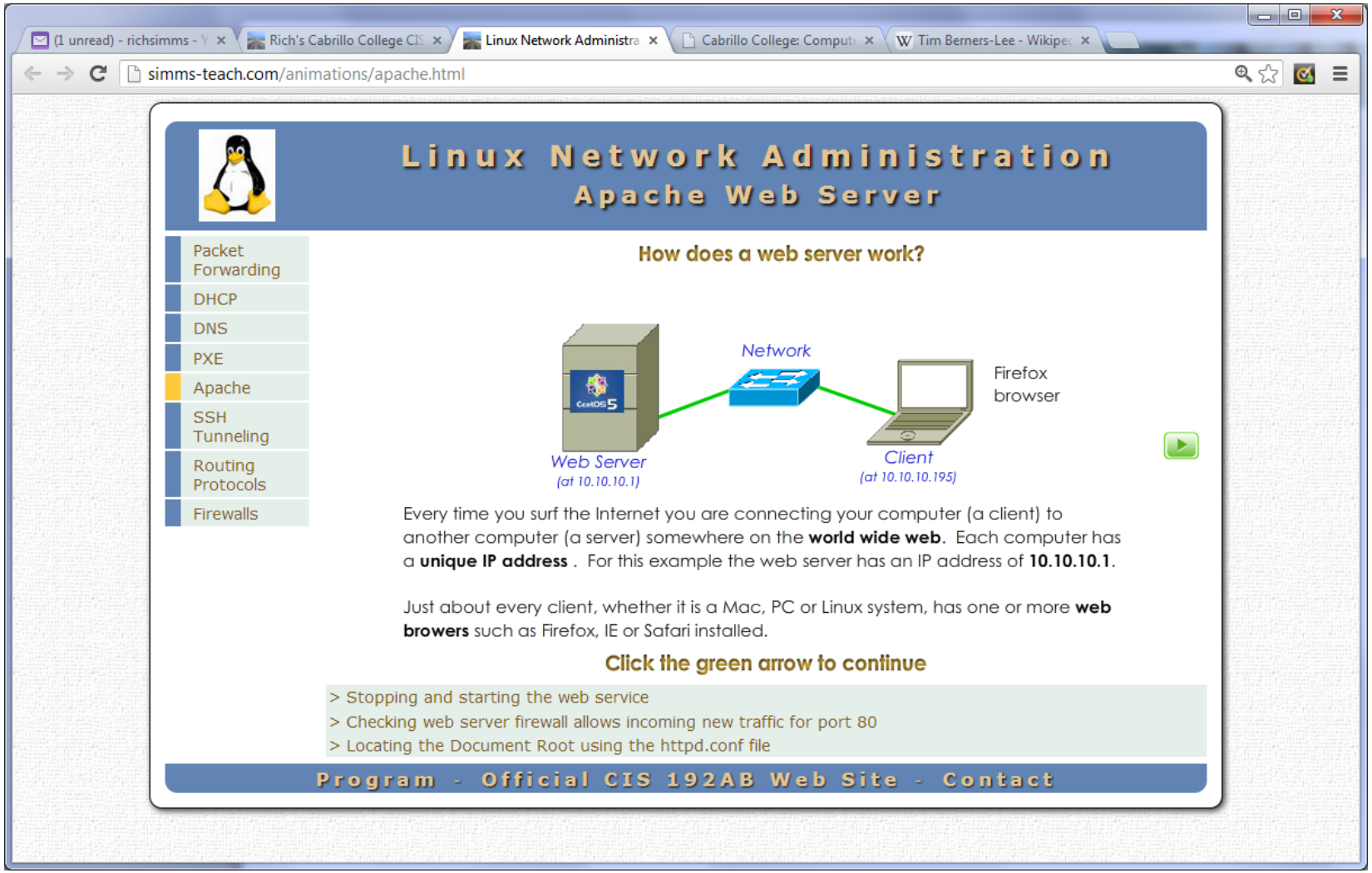
Stream Content

```
GET /~arwen/ HTTP/1.1
Host: 172.30.4.107
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.10) Gecko/2009042316 Firefox/3.0.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive

HTTP/1.1 200 OK
Date: Sun, 17 May 2009 06:40:26 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Tue, 14 Apr 2009 14:36:34 GMT
ETag: "a8b2c-37f-c1f14080"
Accept-Ranges: bytes
Content-Length: 895
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<title>Arwen's CIS 192 Lab 10</title>
</head>
<body>
<h1>Arwen's CIS 192 Lab 10</h1>
<h2>Internet Services</h2>
<div>
<img src="hwy50.jpg" alt="Highway 50" />
</div>
```

The browser's request for a web page, notice the header information passed to the web

The web server sends the requested page which includes a number of headers followed by the actual web page

This portion of the stream capture shows the HTTP request from the browser followed by the web server sending the default web page.



Link is on Lesson 14 of the CIS 192 Calendar page of website

Setting up Apache

Service Applications

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

Apache Summary

Step 1 **yum install httpd** (if not already installed)
Optional: httpd-manual (for man pages)

Step 2 Configuration file:
/etc/httpd/conf/httpd.conf

Step 3 Firewall: Open TCP 80

Step 4 SELinux: enforcing
httpd_enable_homedirs=1 (for user public_html directories)
httpd_sys_content_t and **httpd_user_content_t** context types

Step 5 **service httpd start** (also **stop** and **restart**)

Step 6 **chkconfig httpd on** (or **off**)

Step 7 Monitor or verify service is running:
service httpd status
ps –ef | grep httpd
netstat –tln | grep 631

Step 8 Troubleshoot (check logs, firewall & network settings)

Step 9 Log files: /var/log/httpd/*

Step 10 Additional security:
http://httpd.apache.org/docs/2.0/misc/security_tips.html

Apache basic setup

(publish from /var/www/html)

Apache Configuration

Step 1 **yum install httpd httpd-manual**

Step 2 Edit /etc/httpd/conf/httpd.conf:
Set the **ServerName** directive with your hostname and port

Step 3 Open port **80** in the firewall

Step 4 No changes to SELinux (yet)

Step 5 Start Apache: **service httpd start**

Step 6 **chkconfig httpd on**

Step 6 **service httpd status**

Installing Apache

Step 1 ***Installing software***

To install:

yum install httpd httpd-manual

Optional but useful for having local Apache documentation

Step 2 Apache User Directory Configuration

*Set the **ServerName** directive for your server in /etc/httpd/conf/httpd.conf*

```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
ServerName p35-celebrian.cis192pods.cislab.net:80
```

```
[root@p35-celebrian ~]# cat /etc/hosts
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 p35-celebrian.cis192pods.cislab.net p35-celebrian localhost
```

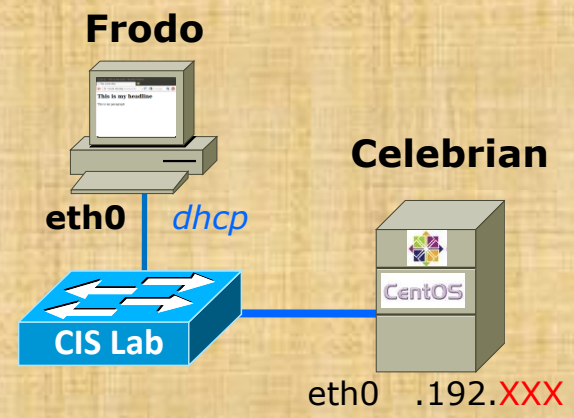
Should match exactly what you have in /etc/hosts or DNS

Step 3 Firewall Configuration for Apache

Open port 80 in the firewall

```
[root@p35-celebrian ~]# iptables -I INPUT 4  -m state --state NEW -m tcp -p tcp --
  dport 80 -j ACCEPT

[root@p35-celebrian ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

[root@p35-celebrian ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Sun May 19 21:08:17 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [42:4296]
-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 80 -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 Sun May 19 21:08:17 2013
```

service iptables save *rules in memory ==> /etc/sysconfig/iptables*
service iptables restart *rules in /etc/sysconfig/iptables ==> memory*



Setting up a web server

Celebrian

1. **yum clean all**

2. **yum install httpd httpd-manual**

3. Configure /etc/httpd/conf/httpd.conf
   - Line 276 ==> **ServerName pxx-celebrian.cis192pods.cislab.net:80**

4. **iptables -I INPUT 4 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT**

5. **service httpd start**

6. Put simple web page in /var/www/html
   - **cp ~/depot/simple.html /var/www/html**

Frodo:

1. Browse to 172.20.192.xxx/simple.html

Frodo

p35-frodo on vmserver3.cislab.net

File View VM

Firefox File Edit View History Bookmarks Tools Help 11:01 AM CIS 192 Student

This is the title - Mozilla Firefox

This is the title

172.20.192.246/simple.html

This is my headline

This is my paragraph

Celebrian

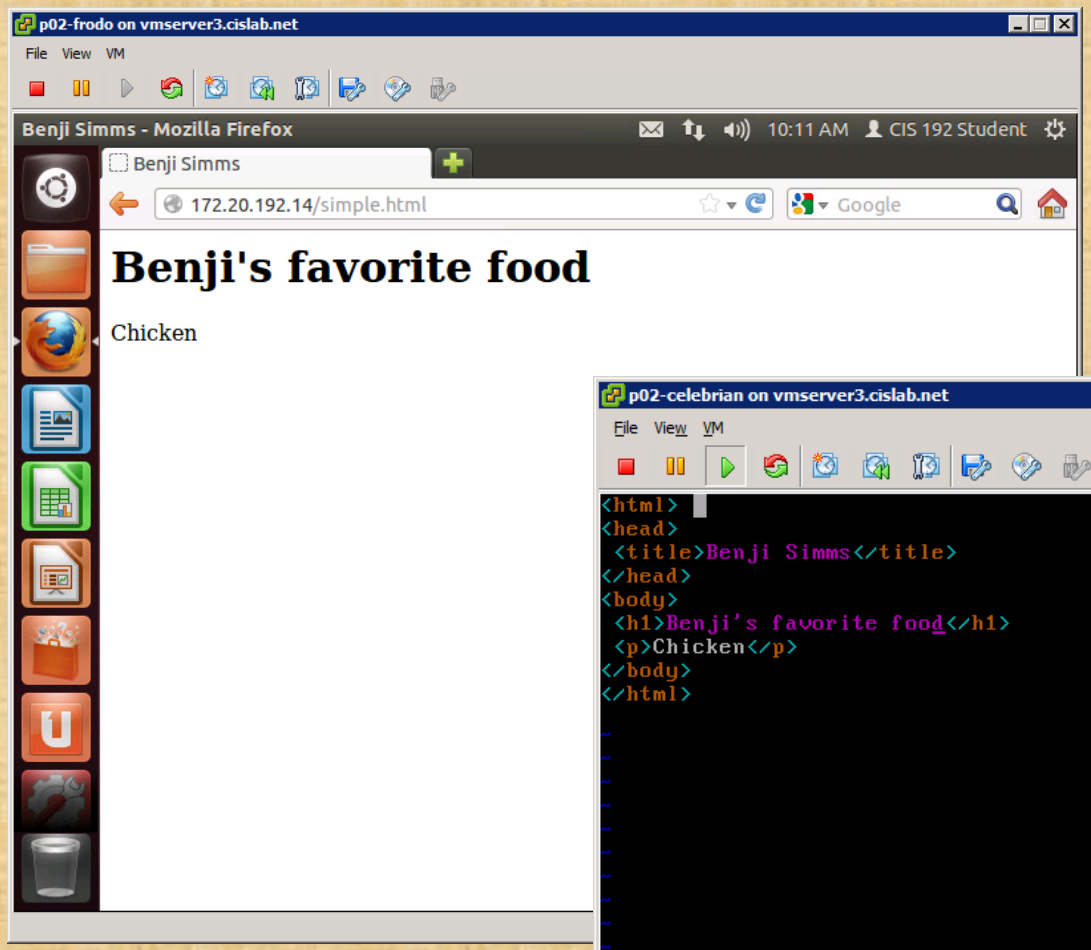
p02-celebrian on vmserver3.cislab.net

File View VM

```
<html>
<head>
 <title>This is the title</title>
</head>
<body>
 <h1>This is my headline</h1>
 <p>This is my paragraph</p>
</body>
</html>
```

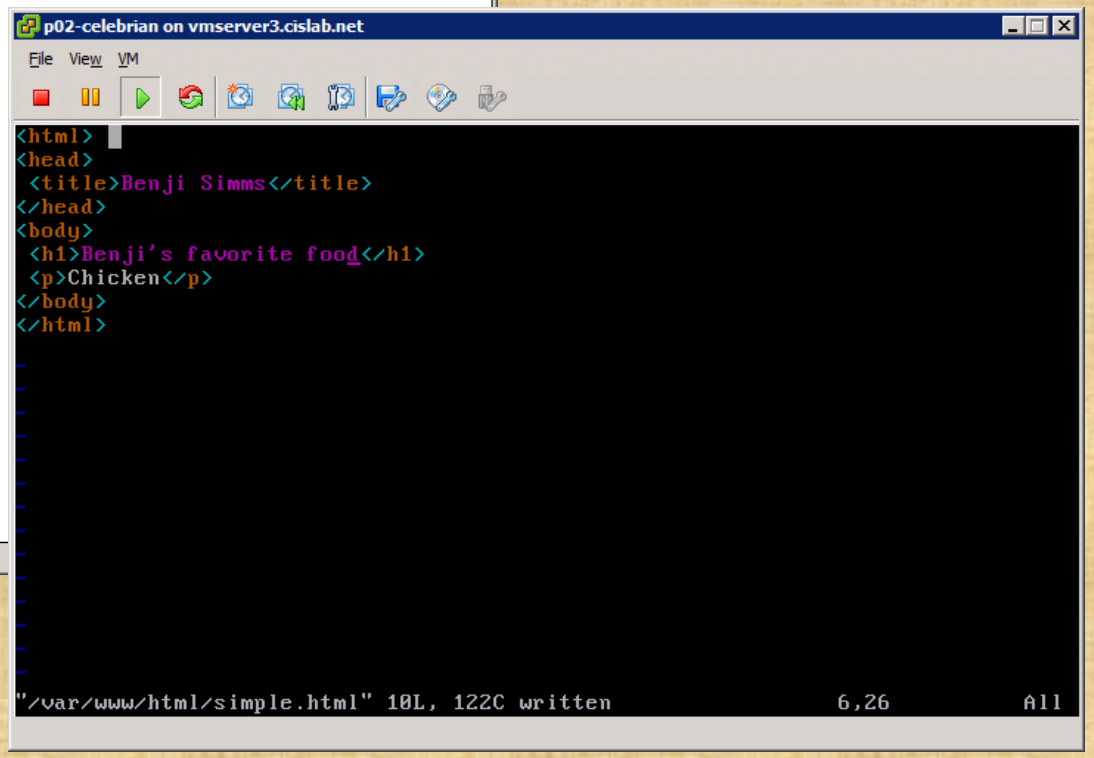
10,0-1 All

Frodo



Try making some changes to your web page

Celebrian



Multiple Websites on One Web Server

How can one web server be used to host multiple web sites?

- By user directories - each user on the system can have their own web site
- By IP address - add multiple IP aliases to the web server and then associate different web sites with each IP address
- By web server hostname - create multiple hostnames for the same web server using DNS aliases. Then associate each hostname with a different web site.

Apache user directories

Apache User Directories

User directories

- Each user can publish files from the *public_html* directory in their home directory.

- The pages are accessed by adding a /~*username* after the hostname in the URL.

- Examples:
  - http://cabrillo.edu/~jgriffin/
  - http://cabrillo.edu/~gbrady/
  - http://webhawks.org/~dm60astudent/

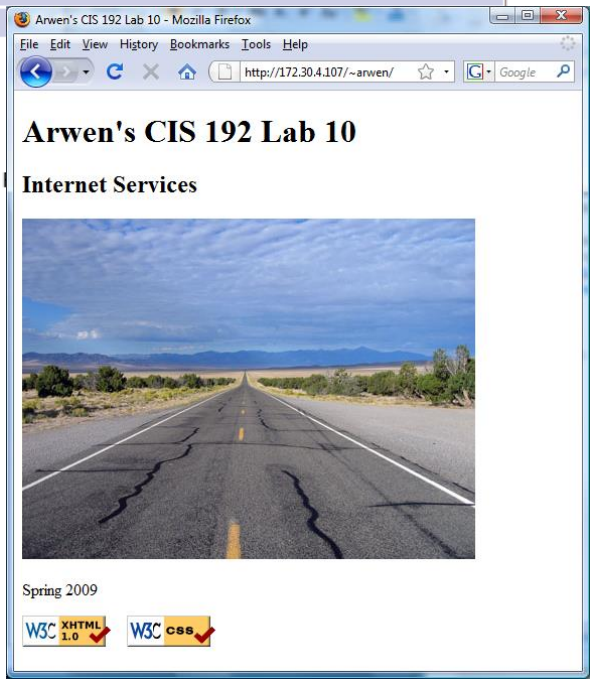
- Note, in Linux the ~ is used by Linux to specify home directories
  - cd ~ *will change to your own home directory*
  - cd ~cis192 *will change to cis192's home directory*

URL's with ~usernames

No.	Time	SIP	SP	DIP	DP	Protocol	Info
1	0.000000	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2	0.000027	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=6
3	0.001117	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001768	192.168.0.24	52935	172.30.4.107	80	HTTP	GET /~arwen/ HTTP/1.1
5	0.002857	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1 Ack=378 Win=6912 Len=0
6	0.008379	172.30.4.107	80	192.168.0.24	52935	HTTP	HTTP/1.1 200 OK (text/html)
7	0.008412	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [FIN, ACK] Seq=1159 Ack=378 Win=6912 Len=0
8	0.010210	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [FIN, ACK] Seq=378 Ack=1159 Win=64540 Len=0
9	0.010309	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [ACK] Seq=1160 Ack=379 Win=6912 Len=0
10	0.011629	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [ACK] Seq=379 Ack=1160 Win=64540 Len=0

```
▷ Frame 4 (431 bytes on wire, 431 bytes captured)
▷ Ethernet II, Src: Vmware_30:16:94 (00:0c:29:30:16:94), Dst: Vmware_e3:93:8a (00:0c:29:e3:93:8a)
▷ Internet Protocol, Src: 192.168.0.24 (192.168.0.24), Dst: 172.30.4.107 (172.30.4.107)
▷ Transmission Control Protocol, Src Port: 52935 (52935), Dst Port: http (80), Seq: 1, Ack: 1, Len: 377
▽ Hypertext Transfer Protocol
  ▽ GET /~arwen/ HTTP/1.1\r\n
      Request Method: GET
      Request URI: /~arwen/
      Request Version: HTTP/1.1
    Host: 172.30.4.107\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.10) Gecko/2009042316
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
```

~arwen



The ~arwen results in serving the web page at /home/arwen/public_html/index.html

~username webpage examples

http://172.20.192.245/~elrond

http:// 172.20.192.245/~celebrian

http:// 172.20.192.245/~arwen

http:// 172.20.192.245/~legolas

Elrond

(From Lab 10 where you configure multiple user directories)

How to Configure Apache User Directories

This enables each local user on the web server to publish their own websites

1. Edit /etc/httpd/conf/httpd.conf:
    1. Comment out the **UserDir disable** directive
    2. Uncomment the **UserDir public_html** directive

2. Set 751 permissions on the user's home directory

3. Set 751 permissions on the user's *public_html* directory

4. For SELinux (enforcing mode), change published directory and file context types to **httpd_user_content_t** and verify the boolean **httpd_enable_homedirs** is on

These are changes to the basic Apache installation and configuration

Step 2

Apache User Directory Configuration

/etc/httpd/conf/httpd.conf:

```
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    #UserDir disable
```

*Comment out the **UserDir disable** directive,*

```
    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disable" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html
```

*Uncomment the **UserDir public_html** directive*

Step 2 Apache User Directory Permissions

chmod 751 /home/* /home/*/public_html

The user's home and public_html directories permissions should be: ***751***

Celebrian
Web Server

```
[root@p35-celebrian ~]# ls -ld ~cis192 ~cis192/public_html/
drwxr-x--x. 3 cis192 cis192 4096 May 19 10:14 /home/cis192
drwxr-x--x. 2 cis192 cis192 4096 May 19 17:52
/home/cis192/public_html/
```

The user's content file permissions should be: ***644***

```
[root@p35-celebrian ~]# ls -l ~cis192/public_html/
total 12
-rw-r--r--. 1 cis192 cis192 4778 May 19 17:52 cis192.jpg
-rw-r--r--. 1 cis192 cis192  924 May 19 17:52 index.html
```

Step 4 Apache SELinux Configuration For User Directories

1) Recursively change the SELinux context on the *public_html* directories in each user's directory

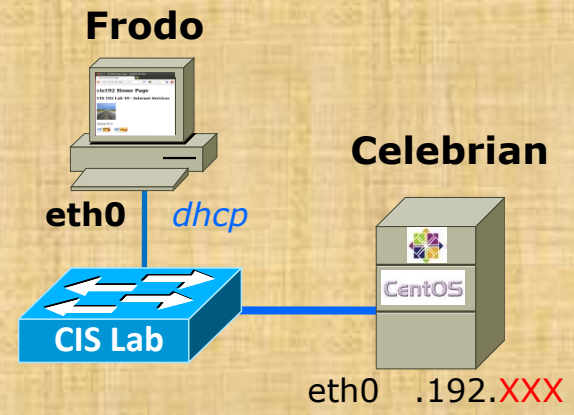
chcon -vR -t httpd_user_content_t /home/*/public_html

Recursive (changes all sub-directories and their files too)

verbose (shows changes made)

2) Set the SELinux boolean to allow publishing from home directories

setsebool -P httpd_enable_homedirs=1



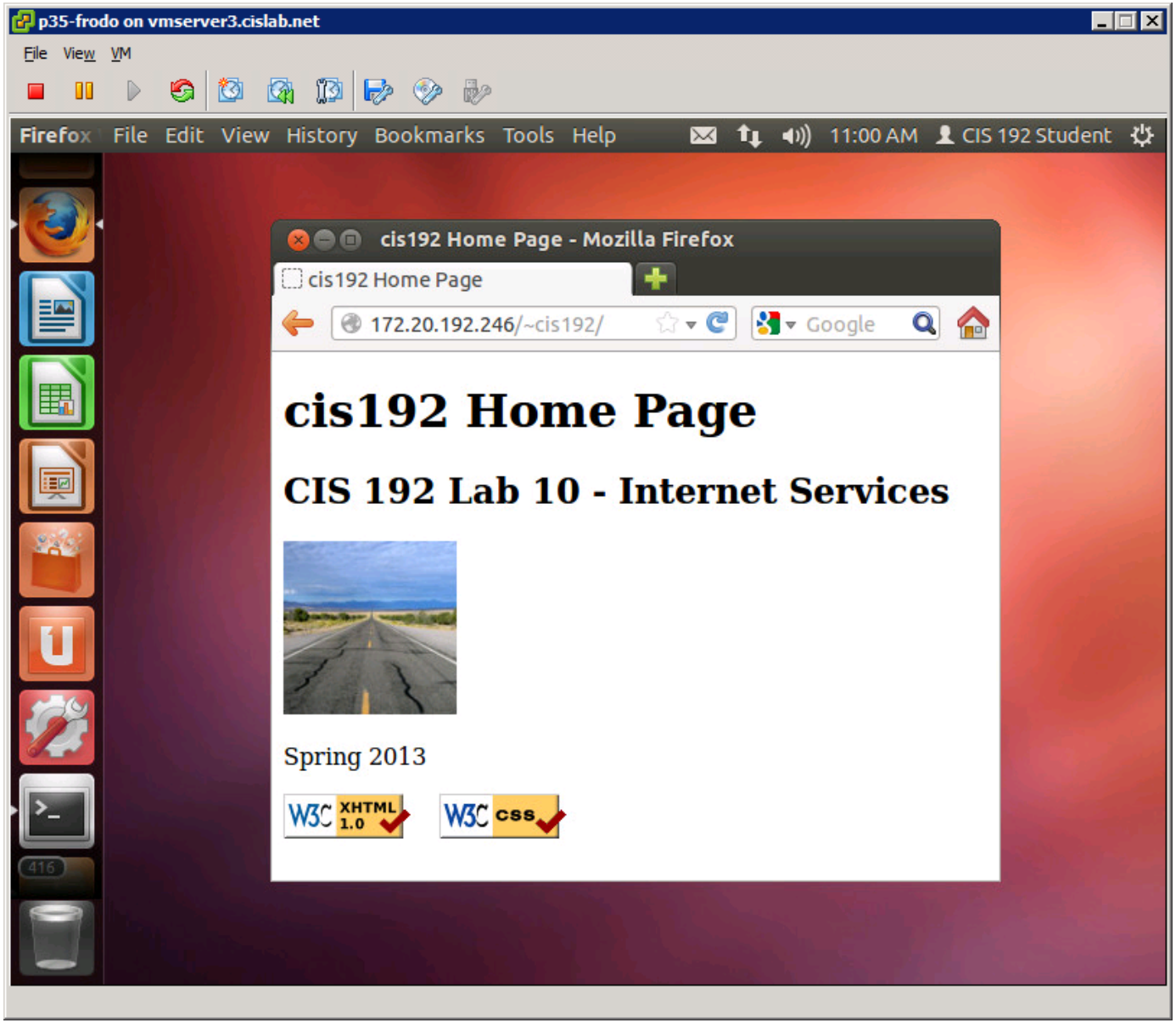
Setting up a web server to publish from user directories

Celebrian

1. Configure /etc/httpd/conf/httpd.conf
   - Line 366 ==> **#UserDir disabled**
   - Line 373 ==> **UserDir public_html**
2. **service httpd restart**
3. **chcon -vR -t httpd_user_content_t /home/*/public_html**
4. **setsebool -P httpd_enable_homedirs=1**
5. Set permissions on cis192 user's website
   - **su - cis192**
   - **chmod 751 ~ public_html**
   - **exit**

Frodo:

1. Browse to 172.20.192.xxx/~cis192


p35-frodo on vmserver3.cislab.net
File View VM
Firefox File Edit View History Bookmarks Tools Help
11:00 AM
CIS 192 Student
cis192 Home Page - Mozilla Firefox
cis192 Home Page
172.20.192.246/~cis192/
Google
cis192 Home Page
CIS 192 Lab 10 - Internet Services
Spring 2013
W3C XHTML 1.0
W3C CSS

Apache IP Aliases

Apache IP Aliases

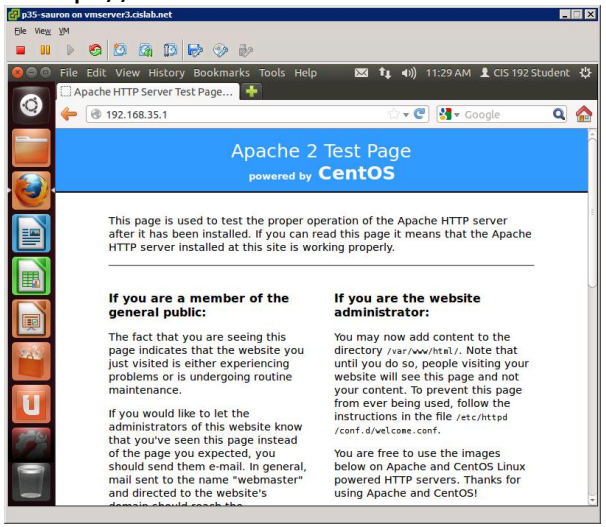
Multiple web sites served using different IP addresses.

- This approach is based on virtual domains
- Each IP address is associated with a different virtual domain
- Examples:
  - http://192.168.2.1
  - http://192.168.2.99
  - http://192.168.2.100

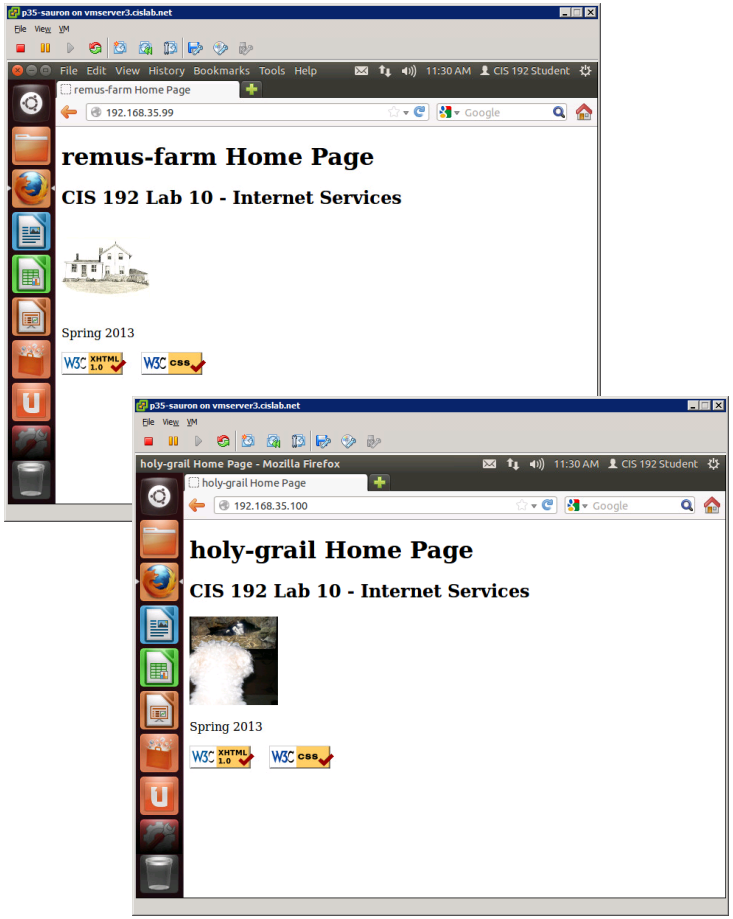
One web server has been configured with multiple IP addresses using IP aliases

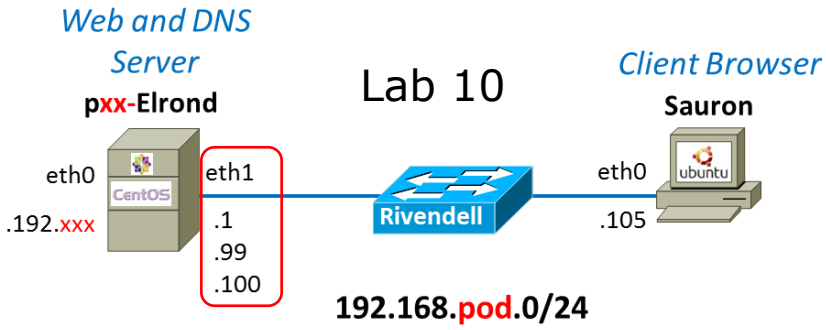
IP Aliases webpage examples

http://192.168.35.1



http://192.168.35.99



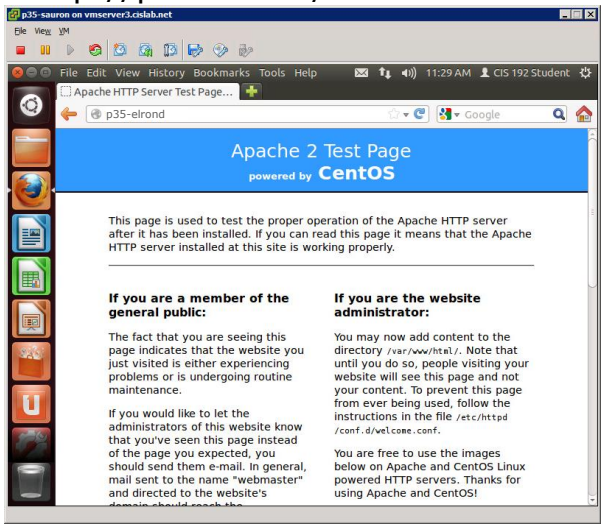


http://192.168.35.100

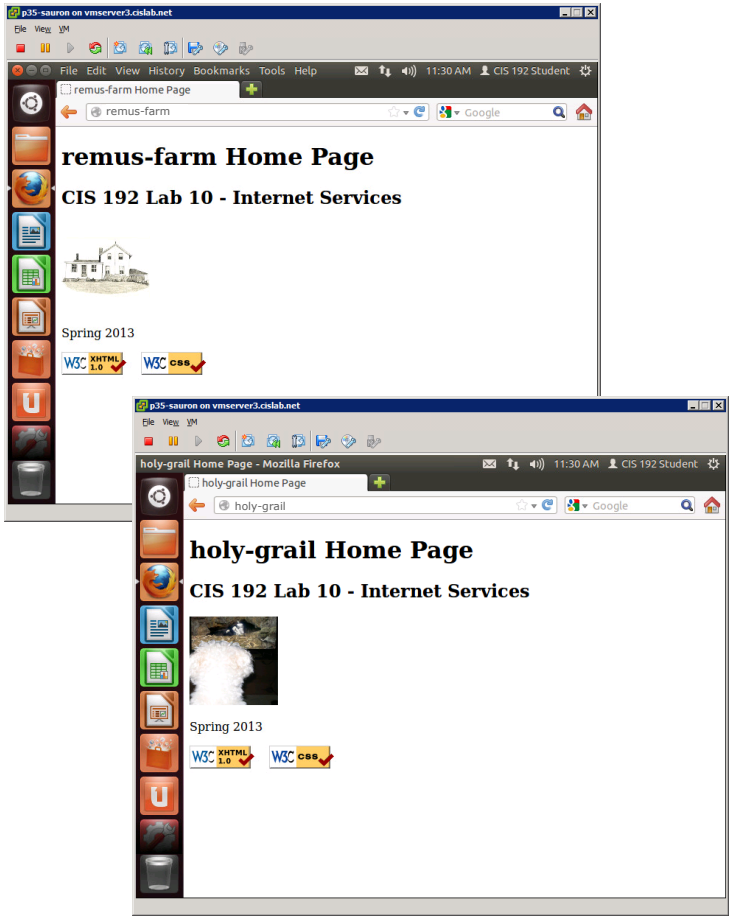
Elrond eth1 has multiple IP addresses on Rivendell network

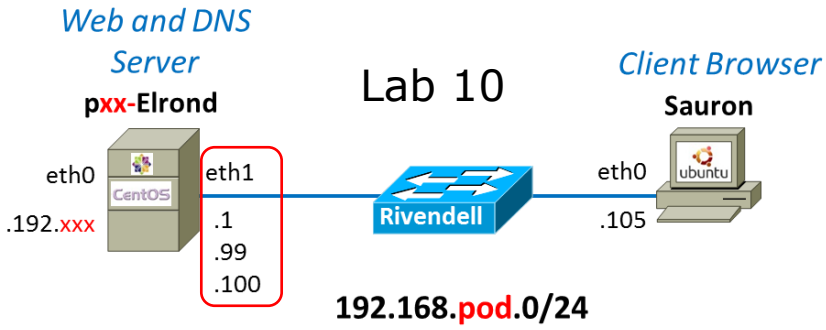
IP Aliases webpage examples

http://p35-elrond/



http://remus-farm/





http://holy-grail/

The DNS server resolves each name to different IP addresses on Elrond's eth1

Apache IP Aliases

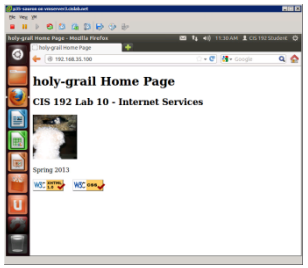
Elrond

Web Server

Different web sites

```
[root@p35-elrond ~]# ls -l /www
total 8
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 holy-grail
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 remus-farm
```

```
[root@p35-elrond ~]# ifconfig eth1:1
eth1:1    Link encap:Ethernet  HWaddr 00:50:56:BD:83:A6
          inet addr:192.168.35.99  Bcast:192.168.35.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

[root@p35-elrond ~]# ifconfig eth1:2
eth1:2    Link encap:Ethernet  HWaddr 00:50:56:BD:83:A6
          inet addr:192.168.35.100  Bcast:192.168.35.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```




```
[root@p35-elrond ~]# tail -10 /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.35.99>
    ServerName remus-farm.rivendell
    DocumentRoot /www/remus-farm
</VirtualHost>

<VirtualHost 192.168.35.100>
    ServerName holy-grail.rivendell
    DocumentRoot /www/holy-grail
</VirtualHost>
```

How to Configure Apache IP Aliases

To enable a web server to publish a different website on each of it's IP addresses:

1) Create different web sites e.g. in a new directory such as /www

2) Set 751 permissions on the directories being published

3) Create multiple IP addresses using IP aliases

4) Configure new IP addresses in DNS zone file or /etc/hosts files.

5) Create a VirtualHost directive in the Apache configuration file that maps the IP address to the document root for the website

6) For SELinux (enforcing mode), change context types to **httpd_sys_content_t** on any published directories and files

These are changes to the basic Apache installation and configuration

Apache IP Aliases

Create different web pages

```
[root@p35-elrond ~]# ls -lR /www
/www:
total 8
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 holy-grail
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 remus-farm
```

751 permissions

```
/www/holy-grail:
total 28
-rw-r--r--. 1 cis192 cis192 23071 May 21 11:13 holy-grail.jpg
-rw-r--r--. 1 cis192 cis192   940 May 21 11:13 index.html
```

644 permissions

```
/www/remus-farm:
total 28
-rw-r--r--. 1 cis192 cis192   940 May 21 11:13 index.html
-rw-r--r--. 1 cis192 cis192 20770 May 21 11:13 remus-farm.jpg
```

644 permissions

Two websites are created in Lab 10

Apache IP Aliases

Create additional IP addresses for the web server with IP aliases

```
[root@p35-elrond ~]# head /etc/sysconfig/network-scripts/ifcfg-eth1*
==> /etc/sysconfig/network-scripts/ifcfg-eth1 <==
NM_CONTROLLED="no"
TYPE="Ethernet"
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.35.1
NETMASK=255.255.255.0

==> /etc/sysconfig/network-scripts/ifcfg-eth1:1 <==
DEVICE=eth1:1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.35.99
NETMASK=255.255.255.0

==> /etc/sysconfig/network-scripts/ifcfg-eth1:2 <==
DEVICE=eth1:2
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.35.100
NETMASK=255.255.255.0
[root@p35-elrond ~]#
```

Used in Lab 10

Add Name/IPs to DNS server zone file

```
[root@p35-elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA p35-elrond.rivendell. root.rivendell. (
                2013051800      ; serial number
                8H              ; refresh rate
                2H              ; retry
                1W              ; expire
                1D)             ; minimum
;
;Name Server Records
Rivendell.      IN NS p35-elrond.rivendell.

;
;Address Records
localhost       IN A 127.0.0.1
p35-elrond      IN A 192.168.35.1
legolas         IN A 192.168.35.105

remus-farm IN A 192.168.35.99
holy-grail IN A 192.168.35.100
[root@p35-elrond ~]#
```

Apache IP Aliases

Define virtual domains using the VirtualHost directive in /etc/httpd/conf/httpd.conf

```
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
```

```
<VirtualHost 192.168.35.99>
    ServerName remus-farm.rivendell
    DocumentRoot /www/remus-farm
</VirtualHost>
```

Map requests to 192.168.35.99 to files in /www/remus-farm

```
<VirtualHost 192.168.35.100>
    ServerName holy-grail.rivendell
    DocumentRoot /www/holy-grail
</VirtualHost>
```

Map requests to 192.168.35.100 to files in /www/holy-grail

SELinux Settings

```
[root@p35-elrond ~]# chcon -R -v -t httpd_sys_content_t /www
changing security context of `/www/remus-farm/index.html'
changing security context of `/www/remus-farm/remus-farm.jpg'
changing security context of `/www/remus-farm'
changing security context of `/www/holy-grail/holy-grail.jpg'
changing security context of `/www/holy-grail/index.html'
changing security context of `/www/holy-grail'
changing security context of `/www'

[root@p35-elrond ~]# ls -ZR /www
/www:
drwxr-x--x. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 holy-grail
drwxr-x--x. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 remus-farm

/www/holy-grail:
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 holy-grail.jpg
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 index.html

/www/remus-farm:
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 index.html
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 remus-farm.jpg
```

Changing the SELinux contexts for Lab 10

Apache Virtual Hostnames

Apache Virtual Hostnames

Multiple web sites served using different server hostnames

- This approach is based on virtual domains
- Each virtual hostname is associated with a different virtual domain
- Examples:
  - http://remus-farm.rivendell
  - http://holy-grail.rivendell

One web server has been configured with multiple hostnames on a single IP address

Apache Virtual Hostnames Example

http://remus-farm.rivendell

Different virtual hostnames on the same IP address

http://holy-grail.rivendell

```
cis192@p35-sauron:~$ host remus-farm.rivendell
remus-farm.rivendell is an alias for p35-elrond.rivendell.
p35-elrond.rivendell has address 192.168.35.1
cis192@p35-sauron:~$
```

remus-farm Home Page - Mozilla F

remus-farm.rivendell

remus-farm Hom

CIS 192 Lab 10 - Intern

Spring 2013

```
cis192@p35-sauron:~$ host holy-grail.rivendell
holy-grail.rivendell is an alias for p35-elrond.rivendell.
p35-elrond.rivendell has address 192.168.35.1
cis192@p35-sauron:~$
```

holy-grail Home Page - Mozilla Firefox

holy-grail.rivendell

holy-grail Home Page

CIS 192 Lab 10 - Internet Services

Spring 2013

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.35.105	192.168.35.1	DNS	80	Standard query A holy-grail.rivendell
2	0.000925	192.168.35.1	192.168.35.105	DNS	135	Standard query response CNAME p35-elrond.rivendell A 192.168.35.1
3	0.003450	192.168.35.105	192.168.35.1	DNS	80	Standard query A holy-grail.rivendell
4	0.003718	192.168.35.1	192.168.35.105	DNS	135	Standard query response CNAME p35-elrond.rivendell A 192.168.35.1
5	0.003953	192.168.35.105	192.168.35.1	TCP	74	54931 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=
6	0.004369	192.168.35.1	192.168.35.105	TCP	74	http > 54931 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PE
7	0.004396	192.168.35.105	192.168.35.1	TCP	66	54931 > http [ACK] Seq=1 Ack=1 Win=14600 Len=0 TSval=947855627 TSec
8	0.004531	192.168.35.105	192.168.35.1	HTTP	458	GET / HTTP/1.1
9	0.005385	192.168.35.1	192.168.35.105	TCP	66	http > 54931 [ACK] Seq=1 Ack=393 Win=15552 Len=0 TSval=10234641 TSe
10	0.006352	192.168.35.1	192.168.35.105	HTTP	216	HTTP/1.1 304 Not Modified

```
▶ Frame 8: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)
▶ Ethernet II, Src: Vmware_bd:b7:c2 (00:50:56:bd:b7:c2), Dst: Vmware_bd:83:a6 (00:50:56:bd:83:a6)
▶ Internet Protocol Version 4, Src: 192.168.35.105 (192.168.35.105), Dst: 192.168.35.1 (192.168.35.1)
▶ Transmission Control Protocol, Src Port: 54931 (54931), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: holy-grail.rivendell\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:14.0) Gecko/20100101 Firefox/14.0.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 21 May 2013 18:13:56 GMT\r\n
    If-None-Match: "22e89-3ac-4dd3e699dba2e"\r\n
    \r\n
    [Full request URI: http://holy-grail.rivendell/]
```

Apache finds out the hostname used because it's included in the Layer 5 HTTP headers

Apache Virtual Hostnames

Elrond

Web Server

Different web sites

```
[root@p35-elrond ~]# ls -l /www
total 8
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 holy-grail
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 remus-farm
```

One IP address

```
[root@p35-elrond ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:50:56:BD:83:A6
          inet addr:192.168.35.1  Bcast:192.168.35.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:febd:83a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41049 (40.0 KiB)  TX bytes:280127 (273.5 KiB)
```


```
<VirtualHost 192.168.35.1>
    ServerName remus-farm.rivendell
    DocumentRoot /www/remus-farm
</VirtualHost>

<VirtualHost 192.168.35.1>
    ServerName holy-grail.rivendell
    DocumentRoot /www/holy-grail
</VirtualHost>
```

Multiple websites

How To Configure Apache Virtual Hostnames

To enable publishing a different website for each virtual hostname of the web server

1) Create different web sites in a directory like /www

2) Set 751 permissions on the directory being published

3) Create multiple hostnames for the web server using CNAME records in the DNS zone file

4) Create a VirtualHost directive in the Apache configuration file that maps the hostnames to the document root

5) Open port **80** in the firewall

6) For SELinux (enforcing mode), change context types to **httpd_sys_content_t** on any published directories and files

These are changes to the basic Apache installation and configuration

Apache Virtual Hostnames

Create different web pages

```
[root@p35-elrond ~]# ls -lR /www
/www:
total 8
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 holy-grail
drwxr-x--x. 2 cis192 cis192 4096 May 21 11:13 remus-farm
```

751 permissions

```
/www/holy-grail:
total 28
-rw-r--r--. 1 cis192 cis192 23071 May 21 11:13 holy-grail.jpg
-rw-r--r--. 1 cis192 cis192   940 May 21 11:13 index.html
```

644 permissions

```
/www/remus-farm:
total 28
-rw-r--r--. 1 cis192 cis192   940 May 21 11:13 index.html
-rw-r--r--. 1 cis192 cis192 20770 May 21 11:13 remus-farm.jpg
```

644 permissions

Two websites are created in Lab 10

Apache Virtual Hostnames

Create additional IP addresses for the web server with IP aliases

```
[root@p35-elrond ~]# head /etc/sysconfig/network-scripts/ifcfg-eth1
NM_CONTROLLED="no"
TYPE="Ethernet"
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.35.1
NETMASK=255.255.255.0
[root@p35-elrond ~]#
```

Only one IP address is needed

Apache Virtual Hostnames

Add CNAME records to DNS server zone file

```
[root@p35-elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA p35-elrond.rivendell. root.rivendell. (
                2013051800      ; serial number
                8H              ; refresh rate
                2H              ; retry
                1W              ; expire
                1D)             ; minimum
;
;Name Server Records
Rivendell.      IN NS p35-elrond.rivendell.

;
;Address Records
localhost       IN A 127.0.0.1
p35-elrond      IN A 192.168.35.1
legolas         IN A 192.168.35.105

remus-farm IN CNAME p35-elrond
holy-grail IN CNAME p35-elrond
[root@p35-elrond ~]#
```

Both names will resolve to Elrond's IP address

Apache Virtual Hostnames

Make virtual domains using the VirtualHost directive in /etc/httpd/conf/httpd.conf

```
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
```

```
<VirtualHost 192.168.35.1>
    ServerName remus-farm.rivendell
    DocumentRoot /www/remus-farm
</VirtualHost>
```

Map requests to remus-farm.rivendell to files in /www/remus-farm

```
<VirtualHost 192.168.35.1>
    ServerName holy-grail.rivendell
    DocumentRoot /www/holy-grail
</VirtualHost>
```

Map requests to holy-grail.rivendell to files in /www/holy-grail

SELinux Settings

```
[root@p35-elrond ~]# chcon -R -v -t httpd_sys_content_t /www
changing security context of `/www/remus-farm/index.html'
changing security context of `/www/remus-farm/remus-farm.jpg'
changing security context of `/www/remus-farm'
changing security context of `/www/holy-grail/holy-grail.jpg'
changing security context of `/www/holy-grail/index.html'
changing security context of `/www/holy-grail'
changing security context of `/www'

[root@p35-elrond ~]# ls -ZR /www
/www:
drwxr-x--x. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 holy-grail
drwxr-x--x. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 remus-farm

/www/holy-grail:
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 holy-grail.jpg
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 index.html

/www/remus-farm:
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 index.html
-rw-r--r--. cis192 cis192 unconfined_u:object_r:httpd_sys_content_t:s0 remus-farm.jpg
```

Changing the SELinux contexts for Lab 10

Logs

Apache Logging

```
<VirtualHost 192.168.35.1>
    ServerName remus-farm.rivendell
    DocumentRoot /www/remus-farm
    TransferLog /www/remus-farm/transfer_log
    ErrorLog /www/remus-farm/error_log
</VirtualHost>

<VirtualHost 192.168.35.1>
    ServerName holy-grail.rivendell
    DocumentRoot /www/holy-grail
    TransferLog /www/holy-grail/transfer_log
    ErrorLog /www/holy-grail/error_log
</VirtualHost>
```

Who has visited your website?

Who requested pages you didn't have?

Additional directives used in Lab 10 to log errors and transfers

Wrap

References

Jim Griffin
- http://www.cabrillo.edu/~jgriffin/CIS192/files/lesson14.html

Next Class

Assignment: Lab 10

http://simms-teach.com/cis192calendar.php

No Quiz next week!

Download the test PDF to your desktop and open with Adobe Reader

Honor Code:
This test is open book, open notes, and open computer. **HOWEVER, you must work alone. You may not share answers. You may not receive or give assistance to others.**

Name: _____
(Type your name to indicate your agreement to abide by the honor code above)

Instructions:
Download and save this test to your computer. Fill out the form using **Adobe Reader**, save it and email it as an attachment to **risimms@cabrillo.edu** using your regular (non-Opus) email.

Mac users please note:

DON'T FILL IT OUT IN YOUR BROWSER

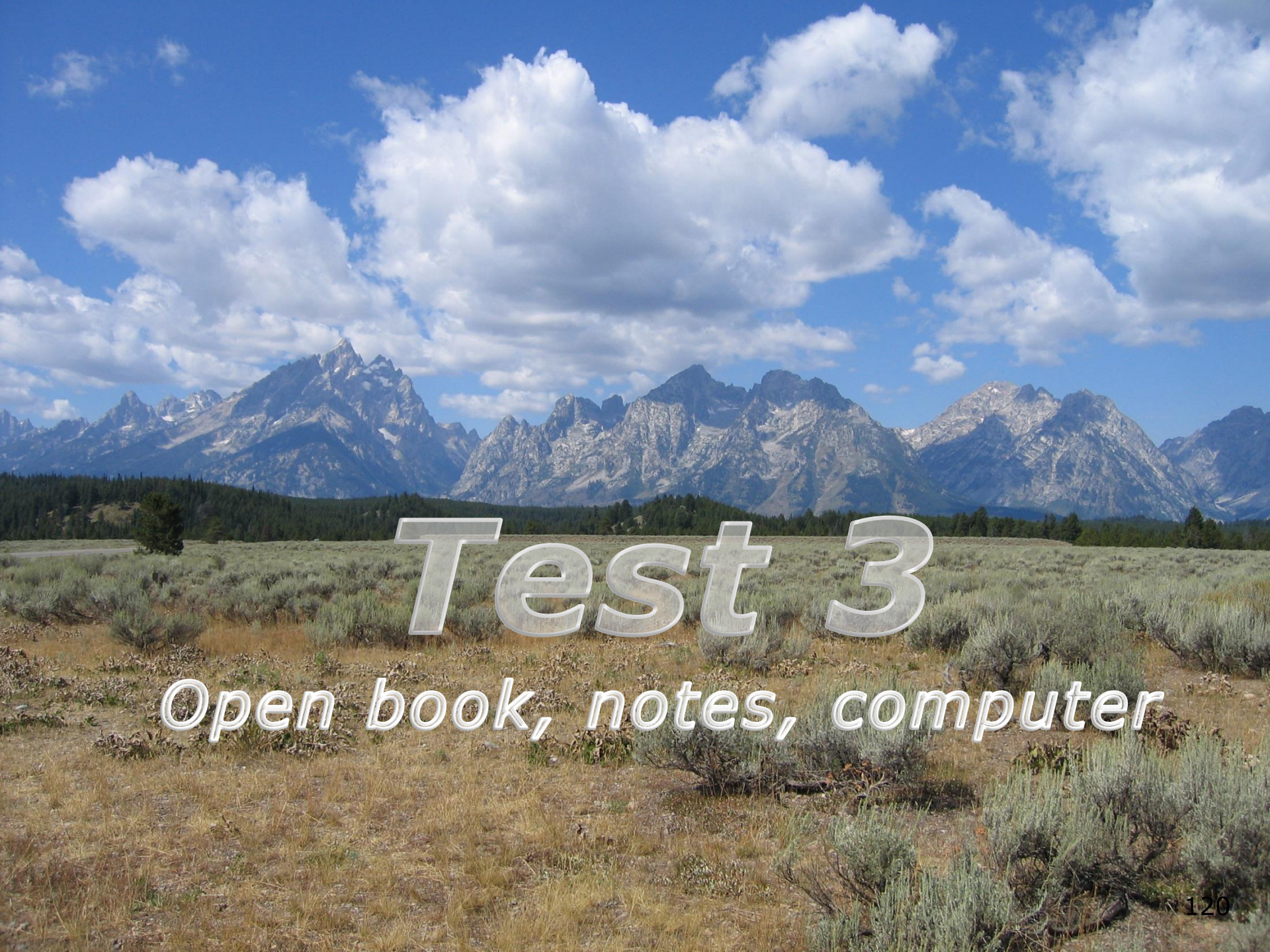
DON'T FILL IT OUT WITH MAC PREVIEW

PLEASE VERIFY YOU ACTUALLY SENT A NON-BLANK TEST WITH COMPLETE ANSWERS TO BE GRADED!

Everyone should submit their test (completed or not) by the end of class.

If you need extra time, you can submit again by no later than 11:59PM. Only the last submittal will be graded.

MAC users: please don't fill out test PDF form using Preview!



Test 3

Open book, notes, computer

Backup

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 >
```

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

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 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	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 Len=0
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

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

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

Passive command 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

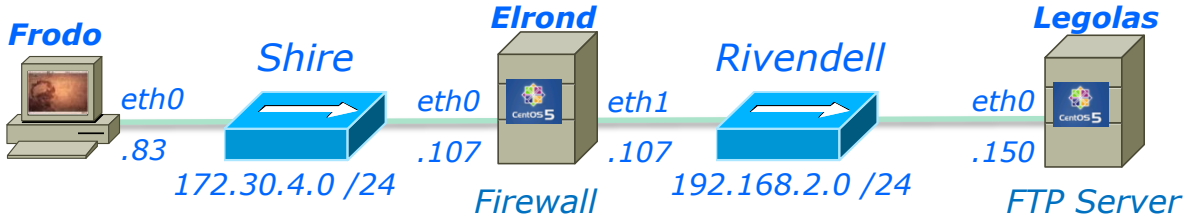
Initialize

*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

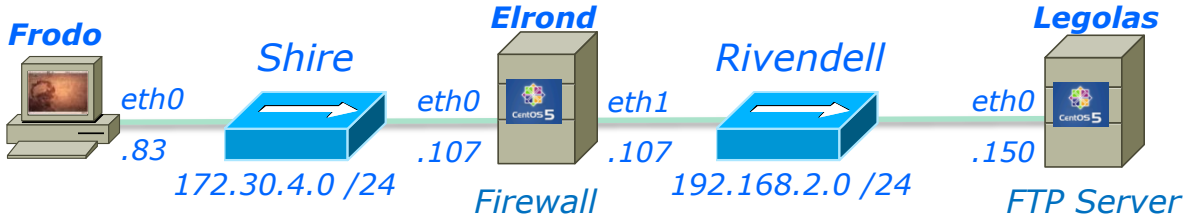
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [SYN] Seq=0 Win=58
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [SYN, ACK] Seq=0 A 46
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 220 (vsFTPd 2.0.5)
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=21 Win=5856 Len=0

3 way handshake initiated by client

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

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21




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

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

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

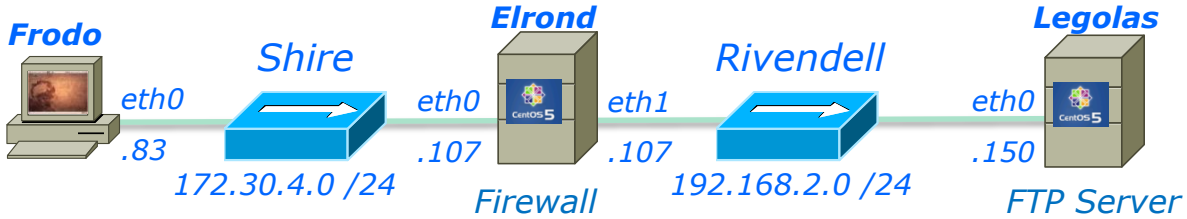
username

password

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

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21



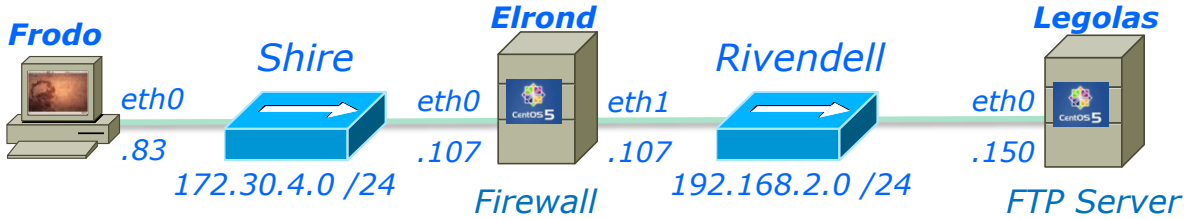

```
Remote system type is UNIX.
Using binary mode to transfer files.
```

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

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

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21



Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

Socket for data transfer

Client	Server
172.30.4.83	192.168.2.150
42571	20

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

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

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

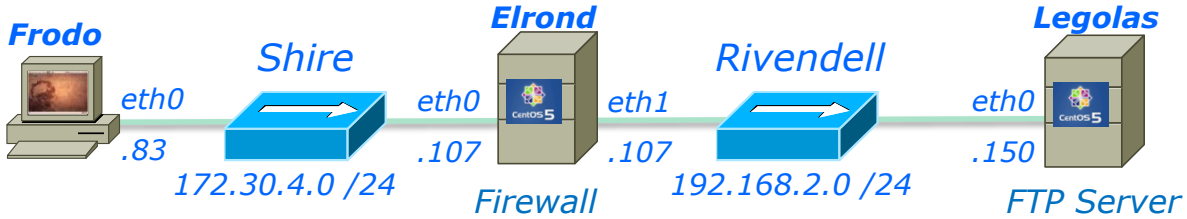
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,166,75
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PAS
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Wi
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=1 Ack
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 Len=0
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=20 Ack=2 Win=5888 Len=0
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=82 Ack=263 Win=5856 Len=0

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection



Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

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 =1
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

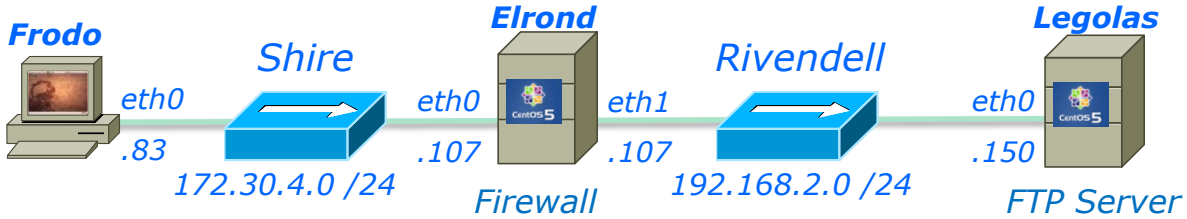
Passive reply to listen on 200, 83 = C853 = 51283

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

```
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)
```

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

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

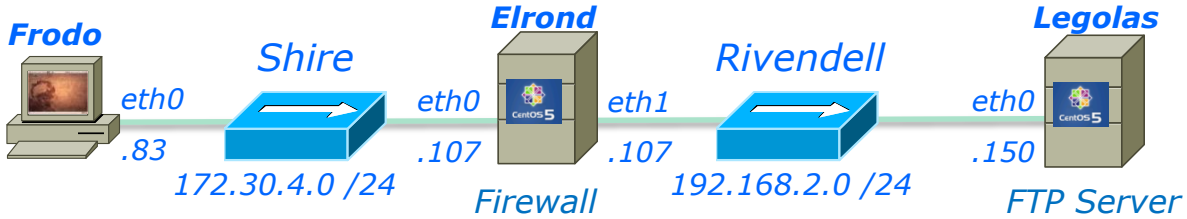
PORT command to listen on 133, 50 = 8532 = 34098

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection




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

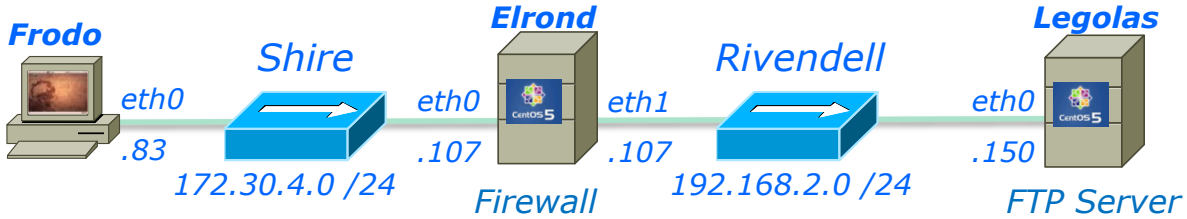
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: QUIT
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 221 Goodbye.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=147 Ack=546
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [FIN, ACK] Seq=546 Ac
172.30.4.83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

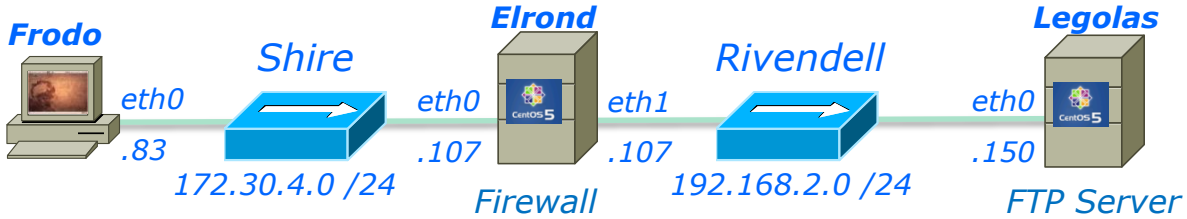



```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source               destination

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

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

For DNS lookups by FTP server

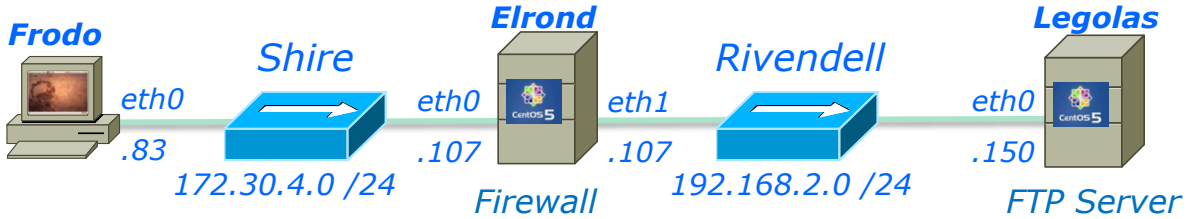
This firewall setting allows external clients (Frodo) to access the FTP server (Legolas)

Note: The FTP data port 20 is not specified




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

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

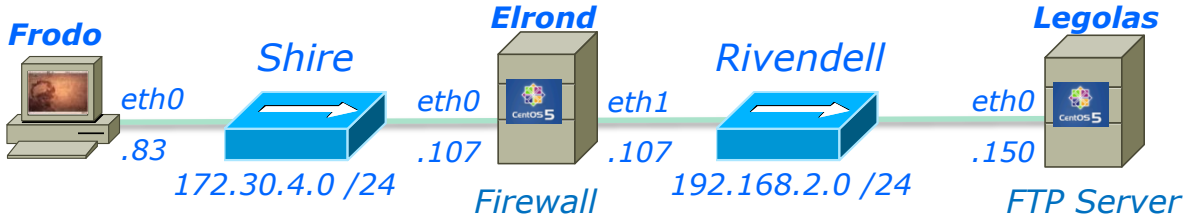


What If? *We remove firewall opening for the DNS lookups sent by the FTP server*

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

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

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

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

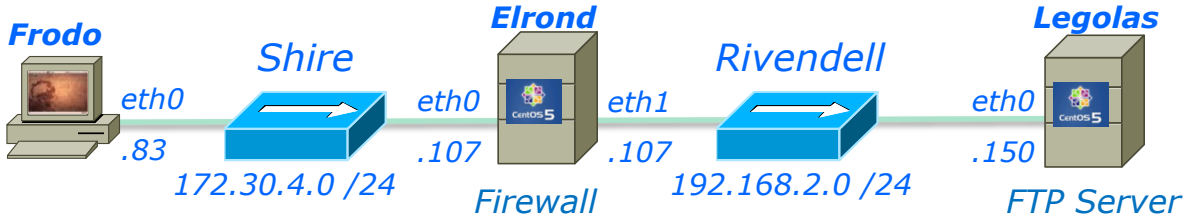
Now DNS lookups are blocked




```
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.
```

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

```
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:~#
```

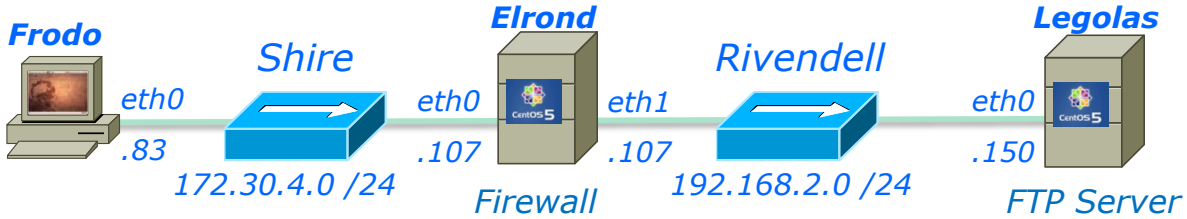



```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
```

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

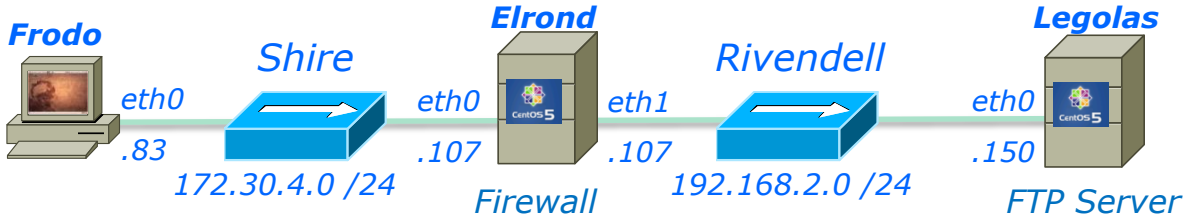
The login is delayed while the two DNS requests time-out.



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
```



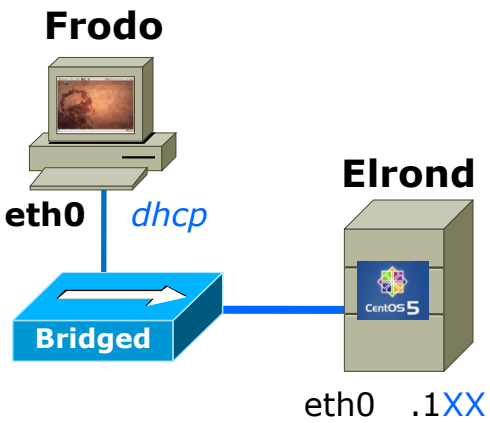

```
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPd 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful.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

Warmup



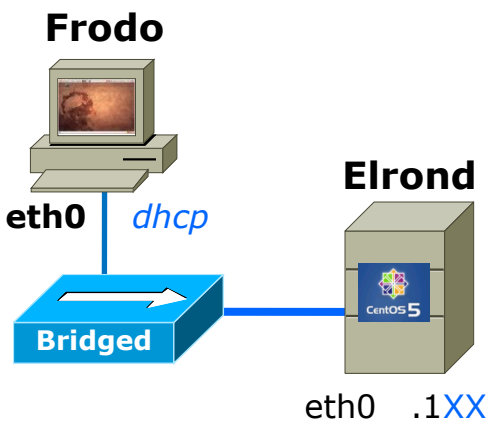
172.30.N.0 /24

.1XX is based on your station number and the IP Table
N=1 for the classroom and N=4 for the CIS lab or CTC
http://simms-teach.com/docs/static-ip-addrs.pdf

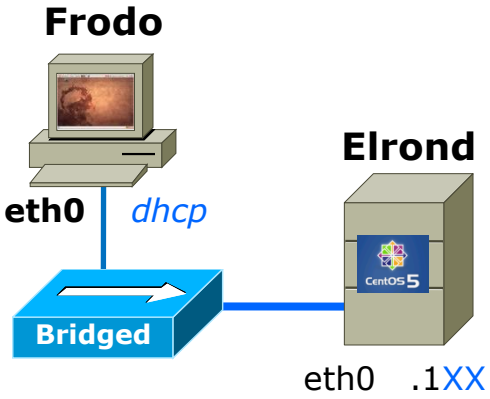
- Cable as shown
- Configure NICs
  - Frodo eth0: use DHCP
    - This is the default
  - Elrond eth0: use DHCP
    - **dhclient eth0**
- Add Elrond's IP address to Frodo's /etc/hosts

- Test:
  - **ping 172.30.N.1**
  - **ping google.com**
  - Check that Frodo and Elrond can ping each other

Fire Up



- Restart your Windows station
- Revert to VM's to snapshot
- Power them ON



Setting up a FTP server

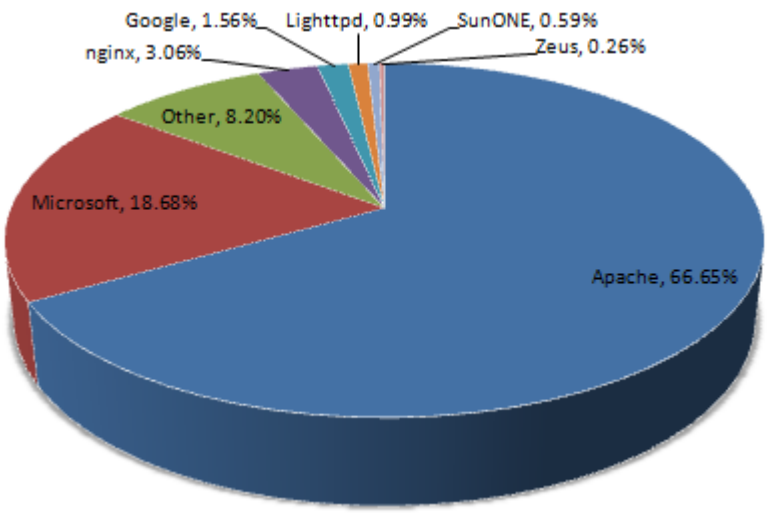
Elrond

- **yum install vsftpd**
- Configure the banner (line 83 in /etc/vsftpd/vsftpd.conf)
- Either configure or disable the firewall
- Either configure contexts or disable for SELinux
- Put some sample files in /var/ftp/pub on Elrond
  cd /var/ftp/pub; echo almost > almost; echo there > there
- **service vsftpd start**

Frodo:

- Do an anonymous FTP get from Frodo
  ftp elrond
  Name: **anonymous**
  Password: ***email-address***
  ls
  cd pub
  ls
  get almost
  bye

Which web severs do the busiest sites use?



Source: http://news.netcraft.com/archives/web_server_survey.html

Apache IP Aliases

Apache IP Aliases

Multiple web sites served using different IP addresses.

- This approach is based on virtual domains
- Each IP address is associated with a different virtual domain
- Examples:
  - http://192.168.2.107
  - http://192.168.2.99
  - http://192.168.2.100

One web server has been configured with multiple IP addresses using IP aliases

Apache IP Aliases

Elrond

Web Server

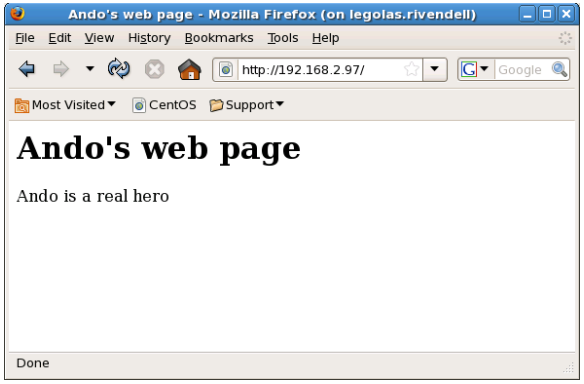
```
[root@elrond ~]# ls -l /www
total 32
drwxr-xr-x 2 root root 4096 May 17 10:35 ando
drwxr-x--x 2 root root 4096 Apr 14 21:48 aragorn
drwxr-x--x 2 root root 4096 Apr 14 21:48 gandalf
drwxr-xr-x 2 root root 4096 May 17 10:25 hiro
```

Different web sites

```
[root@elrond ~]# ifconfig eth1:3
eth1:3    Link encap:Ethernet  HWaddr 00:0C:29:E3:93:94
          inet addr:192.168.2.97  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:185 Base address:0x1480
```

```
[root@elrond ~]# tail -4 /etc/httpd/conf/httpd.conf
<VirtualHost 192.168.2.97>
    ServerName hiro.rivendell
    DocumentRoot /www/ando
</VirtualHost>
```

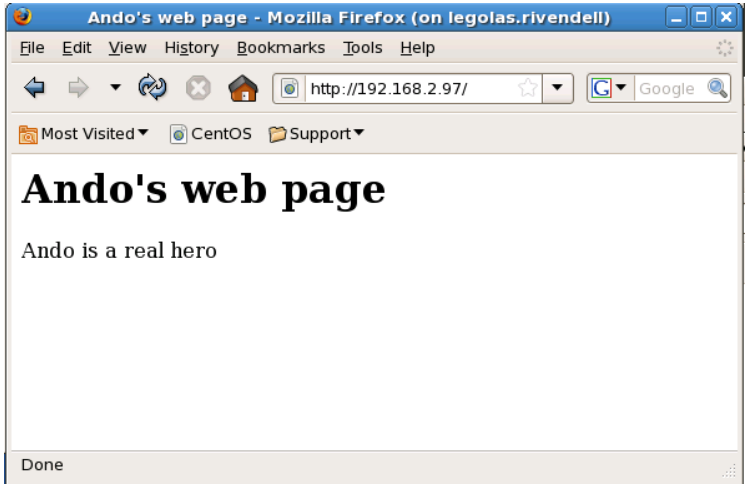
This VirtualHost directive associates the 192.168.2.97 IP address with files in /www/ando



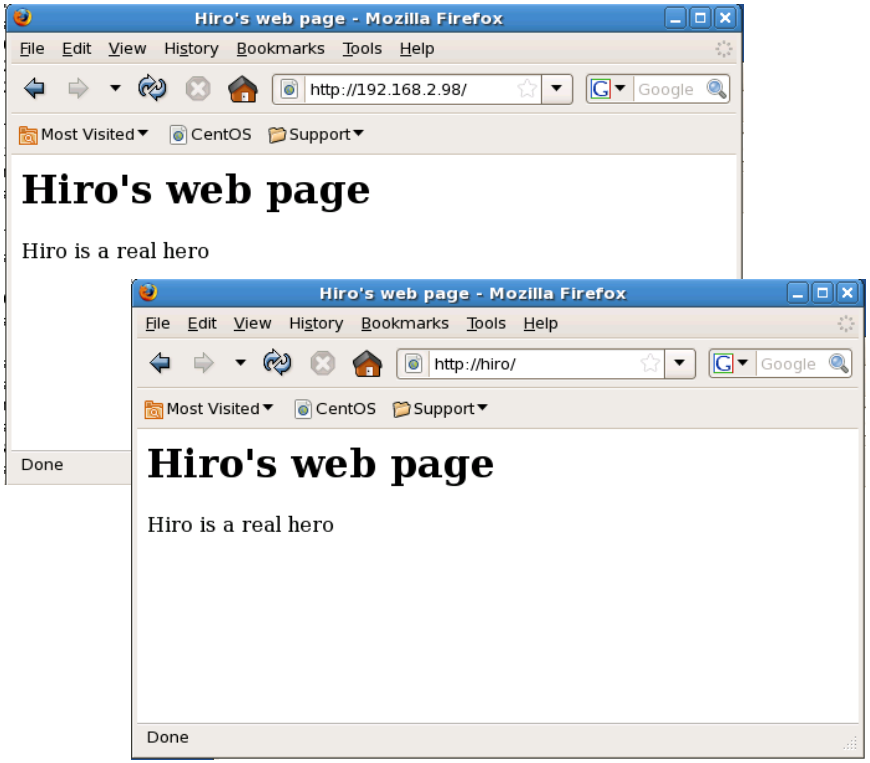
Client requesting the default page from web site at 192.168.2.97

Apache IP Aliases

http://192.168.2.97



http://192.168.2.98



http://hiro/

Elrond has multiple IP addresses. The IP address specified by the URL determines which web page is served

Elrond

One Web Server

Multiple web sites

Apache IP Aliases

To enable users to publish web pages from their home directories:

1) Create different web sites in a directory like /www

2) Create multiple IP addresses using IP aliases

3) Configure new IP addresses in DNS zone file or /etc/hosts files.

4) Create a VirtualHost directive in the Apache configuration file that maps the IP address to the document root

5) Set 751 permissions on the directory being published

6) Open port **80** in the firewall

7) For SELinux (enforcing mode), change context types to **httpd_sys_content_t** on any published directories and files

Apache IP Aliases

Create different web pages

```
[root@elrond ~]# ls /www/{hiro,ando}
/www/ando:
index.html

/www/hiro:
index.html
[root@elrond ~]# ls -l  /www/{hiro,ando}
/www/ando:
total 8
-rw-r--r-- 1 root root 131 May 17 10:35 index.html

/www/hiro:
total 8
-rw-r--r-- 1 root root 131 May 17 10:25 index.html
[root@elrond ~]#
```

We will create a Hiro web site and a Ando web site in /www

Apache IP Aliases

Create additional IP addresses for the web server with IP aliases

Adding 192.168.2.97 to eth1:3

Example:

```
[root@elrond ~]# ifconfig eth1:3 192.168.2.97 netmask 255.255.255.0 broadcast 192.168.2.255
```

Verify:

```
[root@elrond ~]# ifconfig eth1:3
eth1:3    Link encap:Ethernet  HWaddr 00:0C:29:E3:93:94
          inet addr:192.168.2.97  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:185 Base address:0x1480
```

Make permanent:

```
[root@elrond ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1:3
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth1:3
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.2.97
NETMASK=255.255.255.0
NETWORK=192.168.2.0
BROADCAST=192.168.2.255
```

Apache IP Aliases

Make virtual domains using the VirtualHost directive in /etc/httpd/conf/httpd.conf

```
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
```

```
<VirtualHost 192.168.2.98>
    ServerName hiro.rivendell
    DocumentRoot /www/hiro
</VirtualHost>
```

Map requests to 192.168.2.98 to files in /www/hiro

```
<VirtualHost 192.168.2.97>
    ServerName hiro.rivendell
    DocumentRoot /www/ando
</VirtualHost>
```

Map requests to 192.168.2.97 to files in /www/ando

Apache IP Aliases

IP address is 192.168.2.97

No..	Time	SIP	SP	DIP	DP	Protocol	Info
3	0.000225	192.168.2.105	38976	192.168.2.97	80	TCP	38976 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=317190553 TSER
4	0.000832	192.168.2.97	80	192.168.2.105	38976	TCP	http > 38976 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=161
5	0.001777	192.168.2.105	38976	192.168.2.97	80	TCP	38976 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=317190556 TSER=16
6	0.003615	192.168.2.105	38976	192.168.2.97	80	HTTP	GET / HTTP/1.1
7	0.003878	192.168.2.97	80	192.168.2.105	38976	TCP	http > 38976 [ACK] Seq=1 Ack=387 Win=6912 Len=0 TSV=161077028 TSER=
8	0.010213	192.168.2.97	80	192.168.2.105	38976	HTTP	HTTP/1.1 200 OK (text/html)
9	0.010243	192.168.2.97	80	192.168.2.105	38976	TCP	http > 38976 [FIN, ACK] Seq=394 Ack=387 Win=6912 Len=0 TSV=16107703

```
▷ Frame 6 (452 bytes on wire, 452 bytes captured)
▷ Ethernet II, Src: Vmware_30:86:76 (00:0c:29:30:86:76), Dst: Vmware_e3:93:94 (00:0c:29:e3:93:94)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.97 (192.168.2.97)
▷ Transmission Control Protocol, Src Port: 38976 (38976), Dst Port: http (80), Seq: 1, Ack: 1, Len: 386
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: 192.168.2.97\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.5) Gecko/2008121911 CentOS/3.0.5-1.el5.centos Firefox/3.0.5\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
```

Because the IP address was 192.168.2.97 the web page served will be /www/ando/index.html

Apache Names

Websites by Names

Multiple web sites served using different server hostnames

- This approach is based on virtual domains
- Each name is associated with a different virtual domain
- Examples:
  - http://aragorn.rivendell
  - http://gandalf.rivendell

One web server has been configured with multiple hostnames

Websites by Names

Elrond

Web Server

```
[root@elrond ~]# ls -l /www
total 32
drwxr-xr-x 2 root root 4096 May 17 10:35 ando
drwxr-x--x 2 root root 4096 Apr 14 21:48 aragorn
drwxr-x--x 2 root root 4096 Apr 14 21:48 gandalf
drwxr-xr-x 2 root root 4096 May 17 10:25 hiro
```

Different web sites

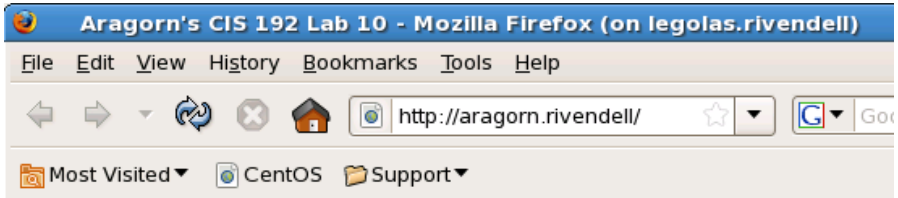
From /var/named/db.rivendell:

```
;CNAME records
gandalf          IN CNAME elrond
aragorn          IN CNAME elrond
```

DNS zone file has aragorn name aliased to Elrond

```
<VirtualHost 192.168.2.107>
    ServerName aragorn.rivendell
    DocumentRoot /www/aragorn
    TransferLog /www/aragorn/transfer_log
    ErrorLog /www/aragorn/error_log
</VirtualHost>
```

This VirtualHost directive associates the aragorn.rivendell name with files in /www/aragorn



Client requesting the default page from the aragorn.rivendell web site

Websites by Names

http://aragorn.rivendell

http://gandalf.rivendell

Aragorn and Gandalf are DNS aliases for Elrond. The host name used in the URL will determine which web page is served.

Elrond

One Web Server

Multiple web sites

Websites by Names

To enable users to publish web pages by names:

1) Create different web sites in a directory like /www

2) Create multiple hostnames for the web server using CNAME records in the DNS zone file

3) Create a VirtualHost directive in the Apache configuration file that maps the hostnames to the document root

4) Set 751 permissions on the directory being published

5) Open port **80** in the firewall

6) For SELinux (enforcing mode), change context types to **httpd_sys_content_t** on any published directories and files

Websites by Names

Create different web pages

```
[root@elrond gandalf]# ls -l /www/{aragorn,gandalf}
/www/aragorn:
total 76
-rw-r--r-- 1 root root   404 Apr 14 21:56 error_log
-rw-r--r-- 1 root root   900 Apr 14 15:01 index.html
-rw-r--r-- 1 root root 45536 Apr 14 14:13 pyramid.jpg
-rw-r--r-- 1 root root  1383 May 17 12:21 transfer_log
```

```
/www/gandalf:
total 88
-rw-r--r-- 1 root root   714 May 16 21:21 error_log
-rw-r--r-- 1 root root   898 Apr 14 15:01 index.html
-rw-r--r-- 1 root root 56481 Apr 14 14:13 temple.jpg
-rw-r--r-- 1 root root  2710 May 17 12:21 transfer_log
```

We will create a Aragorn web site and a Gandalf web site in /www

Websites by Names

Create additional names for the web server in the DNS zone file

Example:

```
[root@elrond gandalf]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2009041701      ; serial number
                8H              ; refresh rate
                2H              ; retry
                4W              ; expire
                1D)             ; minimum
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.

;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.105
elrond          IN A 192.168.2.107
< snipped >
;
;CNAME records
; Used in Lab 10 Part 3
gandalf         IN CNAME elrond
aragorn         IN CNAME elrond
```

Elrond is the web server

Use CNAME records to add hostname aliases of Elrond

Websites by Names

Make virtual domains using the VirtualHost directive in /etc/httpd/conf/httpd.conf

```
### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# <URL:http://httpd.apache.org/docs/2.2/vhosts/>
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-S' to verify your virtual host
# configuration.
```

```
<VirtualHost 192.168.2.107>
    ServerName gandalf.rivendell
    DocumentRoot /www/gandalf
</VirtualHost>
```

Map requests to gandalf.rivendell to files in /www/gandalf

```
<VirtualHost 192.168.2.107>
    ServerName aragorn.rivendell
    DocumentRoot /www/aragorn
</VirtualHost>
```

Map requests to aragorn.rivendell to files in /www/aragorn

Websites by Names

IP address resolved to 192.168.2.107

No.	Time	SIP	SP	DIP	DP	Protocol	Info
5	0.047793	192.168.2.105	60474	192.168.2.107	53	DNS	Standard query A aragorn.rivendell
6	0.047825	192.168.2.107	53	192.168.2.105	60474	DNS	Standard query response CNAME elrond.rivendell A 192.168.2.107
7	0.056575	192.168.2.105	44829	192.168.2.107	80	TCP	44829 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=320913151 TSER
8	0.057226	192.168.2.107	80	192.168.2.105	44829	TCP	http > 44829 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=164
9	0.058032	192.168.2.105	44829	192.168.2.107	80	TCP	44829 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=320913153 TSER=16
10	0.065473	192.168.2.105	44829	192.168.2.107	80	HTTP	GET / HTTP/1.1
11	0.065816	192.168.2.107	80	192.168.2.105	44829	TCP	http > 44829 [ACK] Seq=1 Ack=392 Win=6912 Len=0 TSV=164553537 TSER=

```
▷ Frame 10 (457 bytes on wire, 457 bytes captured)
▷ Ethernet II, Src: Vmware_30:86:76 (00:0c:29:30:86:76), Dst: Vmware_e3:93:94 (00:0c:29:e3:93:94)
▷ Internet Protocol, Src: 192.168.2.105 (192.168.2.105), Dst: 192.168.2.107 (192.168.2.107)
▷ Transmission Control Protocol, Src Port: 44829 (44829), Dst Port: http (80), Seq: 1, Ack: 1, Len: 391
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.1\r\n
    Host: aragorn.rivendell\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.5) Gecko/2008121911 CentOS/3.0.5-1.el5.centos Firefox/3.0.5\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
```

Header shows hostname the user specified in the URL

Because the URL specified the aragorn.rivendell hostname the web page served is /www/aragorn/index.html