



Lesson Module Status

- Slides – draft
- Properties - done
- Flashcards – I wish
- 1st minute quiz – NA
- Web Calendar summary – done
- Web book pages –
- Commands –
- Howtos –
- Skills pacing - NA
- Lab – done
- Depot (VMs) – NA
- Test T3 printed and copied
- Hershey configured as NIS server for cismud.net

Course history and credits

Jim Griffin



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

Rick Graziani



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



Joe A.



Joe P.



Chuck



Kay



Joe B.



Chris H.



Edwin



Lieven



Rich



Jesus



Josh

Teach & Confer is a live interactive classroom to meet with your students.

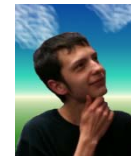
STUDENT LOG IN

View Teach & Confer Archives

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



John



Robert



Junious



Edgar



Casady



Brynden



Jack



Ryan



VMs for tonight
**(Revert, 384MB RAM
and Power up)**
Celebrian



No more quizzes!



Internet Services

Objectives

- Setup and configure a FTP service
- Setup and configure a web server

Agenda

- Quiz
- Questions on previous material
- Housekeeping
- NIS recap
- FTP review
- Apache web server
- Test 3
- Wrap

Questions on previous material



Questions?

- Previous lesson material
- Lab assignments
- Test 3 material

Housekeeping



- Last class on May 27
- Lab 10 due on May 27
- Rich's lab hours for next week:
 - ~~Monday 5/24 1-4~~ ==> Wednesday 5/26 2-5pm
 - Wednesday 5/26 5-7pm
- Final on June 3
- Recovery plan for power outage:
 - Moving troubleshooting activity to 5/27
 - NIS lecture (short) and Apache lecture tonight
 - Minimal changes to Test 3 from practice test

Summer Internship Workshop

- **Internship Benefits:**

- Gain real world experience
- May lead to a permanent job after graduation
- Very helpful in this VERY tough job market

- **You will learn:**

- Making the transition from college student to working professional in your field !
- Practice Interviewing Skills
- Much, much more !!



- **Where & When:**

Friday **21 May** 2 pm - 4:30
Saturday **22 May** 10am-12:30
Room 2501

- **Register:**

- ronorden@cabrillo.edu

Attend either session...

Snacks included!

Please register...

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

You can copy and paste the grades page into Excel at anytime to check your current progress

Code Name	Grading Choice	Quizzes & Tests										Forum				Labs										Final	Extra Credit	Total	Grade			
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	T1	T2	T3	F1	F2	F3	F4	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10				
Max Points		3	3	3	3	3	3	3	3	3	3	30	30	30	20	20	20	20	30	30	30	30	30	30	30	30	30	30	60	90	560	
Arwen	Grade	3	3	3	3	3	3		3	3	3	33	34		20	20	20		30	30	30	30	30	30	30	30	30			90	514	
Aragorn	Grade	3	3	3		3			3	3	3	30	28		8	8	16		30	30	28	30		30	29	30	30			36	384	
Balrog	P/NP		3	3	3	3	3	3	3	3	3	27	28		0	0	0				27	30	28	30	29	30	30			62	348	
Donethor	Grade	3	3	3	3	3				3	3	17	21		12	0			30	24	22		27	3	30	25	30			5	267	
Dwalin	Grade										3	18	15		20	20			30	28	26	29	27	3						3	222	
Elrond	Grade	3	3	3	3	3	3	3	3	3	3	22	27		20	20	20		29	28	30	29	27	30	27	30	30			32	431	
Eomer	Grade	3	3	3		3		3			3	32	32		8	12	20		30	30	28	30	29	30	30	30	22				381	
Frodo	Grade	3	3	3	3	3			3	3	3	34	30		20	20	20		30	30	30	30	30	30	30	30	30			90	508	
Goldberry	P/NP	3									3				4	0			28	30										5	73	
Gwaihir	Grade		3	3	3	3		3	3	3	3	32	32		20	20	20		30	30	30	26	29	30	30	29	30			75	487	
Ioreth	Grade	3	3	3	3	3	3	3	3	3	3	29	30		20	20	20		30	30	30	27	28	30	30	30	30			20	434	
Legolas	Grade		3			3		3	3	3	3	27	29		0	16	20			20				30	29	30	30			33	282	
Pippen	Grade	1	3	3	3		3	3	3	3	3	32	30		20	20	20		30	12	30		27	19	30	22			41	358		
Samwise	Grade			3							3	30	27		20	20	16		28	29	29	27	25						3	260		
Saruman	Grade	3	3	3	3	3	3	3	3	3	3	29	26		16	20	16		30	30	30	30	30	30	30	30	30			90	497	
Smeagol	Grade	3	3	3	3	3	3	3	3	3	3	25	30		20	20	20		30	30	26	30	29	30	28	30	30				408	
Strider	Grade	3	3	3	3	3	3	3	3	3	3	31	30		20	20	20		30	30	30	30	30	27	30	30	30			58	476	
Theoden	Grade		3	3	3	3	3	3	3	3	3	30	31		20	20	20		30	28	30	27	29	30	30	30	30			74	486	
Treebeard	Grade	3		3	3	3					3	28			20	20			30		26	30								32	201	



- Remaining point earning opportunities

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

NIS

(from Lesson 13)

<http://simms-teach.com/docs/cis192/cis192lesson13.pdf#page=29>

Vsftpd Review

Installing and Configuring Telnet (Red Hat Family)

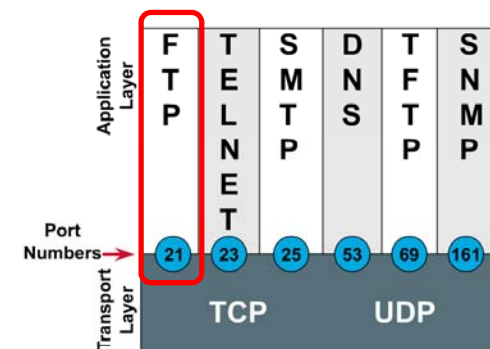
FTP

- 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]#
```

Port Numbers



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 (must load `ip_conntrack_ftp` module)

vsftpd

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

vsftpd
Probably the most secure and fastest FTP server for UNIX-like systems.

Main index

- [About vsftpd](#)
- [Features](#)
- [Online source / docs](#)
- [Download vsftpd](#)
- [Who recommends vsftpd](#)
- [vsftpd security](#)
- [vsftpd performance](#)

News

Kindly hosted by [Mythic Beasts Ltd.](#)

Other links you may be looking for


- My security blog: <http://scarybeastsecurity.blogspot.com/>
- My security advisories: <http://www.scary.beasts.org/security/>


Nov 2009 - vsftpd-2.2.2 released

- vsftpd-2.2.2 is released - with a fix for a regression where heavily loaded sites could see the occasional client get kicked out just after connect. This regression is believed to be introduced in v2.1.0, affecting the inbuilt listener mode. Please refer to the v2.2.2 [Changelog](#) and [vsftpd FAQ](#) (frequently asked questions) for a list of common questions!
- After numerous requests, I now have a PayPal button for donations. If you use vsftpd, like it, and think it's worthy of a donation, then click on the PayPal button on the left of the page.
- ftp.freebsd.org switched to vsftpd.
- vsftpd tarballs are now GPG signed by me.

Sept. 2003 - Is any server other than vsftpd safe?

- ProFTPD [suffers serious security hole](#) - Sep 2003
- wu-ftp [suffers serious security hole](#) - Jul 2003.
- lukemftpd (as a random example from many), via trust of realpath(), [suffers serious security hole](#) - Aug 2003.

 ftp.redhat.com is powered by vsftpd for performance reasons - see below

 ftp.openbsd.org is powered by vsftpd because it needs to be very secure! - see below

vsftpd summary

Packages

```
# rpm -qa | grep vsftpd  
vsftpd-2.0.5-12.el5
```

Configuration file: `/etc/vsftpd/vsftpd.conf`

Firewall Ports Used: 21/TCP (incoming) , 20/TCP (outgoing)

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/`

Installing and Configuring vsftpd (Red Hat Family)

Is it installed?

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

No response means it is not installed

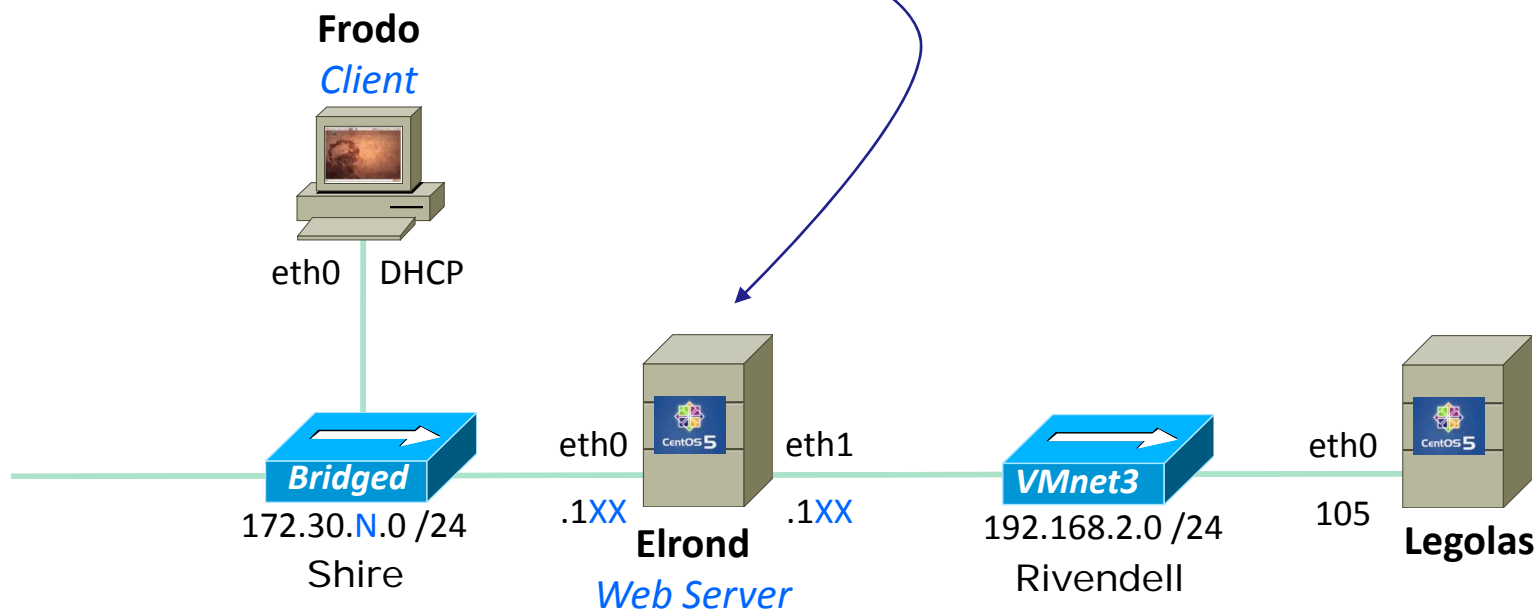
*Use **dpkg -I | grep telnet** on the Debian family*

vsftpd

To install:

Step 1 *Installing software*

`yum install vsftpd`



vsftpd

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

Dependencies Resolved
```

vsftpd

Dependencies Resolved

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

Transaction Summary

```
=====
Install      1 Package(s)
Update       0 Package(s)
Remove       0 Package(s)
=====
```

Total download size: 137 k

Is this ok [y/N]: y

Downloading Packages:

(1/1): vsftpd-2.0.5-12.el 100% |=====| 137 kB 00:00

Running rpm_check_debug

Running Transaction Test

Finished Transaction Test

Transaction Test Succeeded

Running Transaction

Installing: vsftpd ##### [1/1]

Installed: vsftpd.i386 0:2.0.5-12.el5

Complete!

[root@elrond ~]#

vsftpd

Step 2 *Customize the configuration file*

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

< snipped >

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

< snipped >

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

Installing and Configuring vsftpd

Step 3 *Firewall settings*

1. Modify the firewall to allow incoming new FTP (TCP port 21) connections.
2. Load `ip_conntrack_ftp` kernel module to track related connections

Firewall Configuration for FTP



Open port 21 in the firewall

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

```
[root@elrond home]# iptables -nL RH-Firewall-1-INPUT
```

```
Chain RH-Firewall-1-INPUT (2 references)
```

target	prot	opt	source	destination	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0	icmp type 255
ACCEPT	esp	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	ah	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	udp	--	0.0.0.0/0	224.0.0.251	udp dpt:5353
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp dpt:631
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:631
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:21
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:22
REJECT	all	--	0.0.0.0/0	0.0.0.0/0	reject-with icmp-host-prohibited

```
[root@elrond home]#
```

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

```
[root@elrond home]#
```

iptables-save stores the current firewall rules (in memory) to the hard drive. The rules saved in `/etc/sysconfig/iptables` will be used after the next system reboot or **service iptables restart**

Installing and Configuring vsftpd

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, but immediate)

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

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

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

Add this module name 

Firewall - passive mode



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

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

When permanently configured you will see it listed when the firewall service is started.

Firewall for FTP

/etc/sysconfig/iptables

CentOS Modified

```
root@arwen ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
[root@arwen ~]#
```

*Viewing this file not only shows
the permanent firewall settings, it
also shows the actual commands*

*FTP port is
open*

SELinux for vsftpd (CentOS)

Step 4 *SELinux*

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

*required for
anonymous public
content*



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

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

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

*required for users to
access their home
directories*



Installing and Configuring vsftpd (Red Hat Family)

Step 5 *Start or restart service*

```
[root@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

The image shows a terminal window on the left and a network packet capture tool on the right. The terminal window shows a user logging into an FTP server and downloading a file. The network packet capture tool shows the corresponding network traffic, including a 3-way handshake and the transmission of the login message.

```
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:~$
```

The network packet capture tool shows the following traffic:

- > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
- 43773 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
- > 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
- st: 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

The packet capture tool also shows the following details for 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

An arrow points from the text "FTP use port 21 for commands and messages" to the FTP layer in the packet capture tool.

*3-way
handshake*

*Login is
transmitted in
clear text*

*FTP use port 21 for commands
and messages*

Installing and Configuring vsftpd

The screenshot shows a Wireshark capture of an FTP session. The packet list pane displays the following traffic:

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=1460 WS=5
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

The packet details pane for Frame 4 shows the FTP response: "220 Welcome to the Simms FTP service.\r\n". A blue arrow points from this text to the note: "FTP use port 21 for commands and messages".

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

The screenshot shows a terminal window with the command `ftp 172.30.4.107` and a Wireshark network traffic capture. The capture shows a list of packets, with packet 28 highlighted. Packet 28 is an FTP-DATA packet from 172.30.4.107 to 172.30.4.222, containing 12 bytes of data: `Linux Rules\n`. A blue arrow points from the text "Port 20 (and higher) is used for FTP data transfers" to the "ftp-data" protocol field in the packet details pane.

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
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

The Wireshark capture illustrates encapsulation and sockets

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

Installing and Configuring vsftpd

The screenshot shows a terminal window with the command `ftp 172.30.4.107` and a Wireshark capture of the network traffic. The terminal output shows the following sequence of events:

```

cis192@kate:~$ ftp 172.30.4.107
ftp>
22 13.149468 172.30.4.107 172.30.4.222 FTP Response: 200 PORT command successful. Consider using P
23 13.149519 172.30.4.222 172.30.4.107 FTP Request: RETR myfile
24 13.153408 172.30.4.107 172.30.4.222 TCP ftp-data > 35677 [SYN] Seq=0 Win=0 Len=0 MSS=1460 T
25 13.153498 172.30.4.222 172.30.4.107 TCP 35677 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
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 13.154796 172.30.4.107 172.30.4.222 TCP ftp-data > 35677 [FIN, ACK] Seq=13 Ack=1 Win=0 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
  
```

The Wireshark interface shows the selected packet (Frame 28) with the following details:

- Frame 28
- Ethernet II, Src: Vmware_12:50:1e (08:0c:29:12:50:1e), Dst: Vmware_6f:53:d9 (08:0c: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

The status bar at the bottom of Wireshark indicates: 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

The screenshot shows a terminal window with the command `ftp 172.30.4.107` and a Wireshark window displaying a network capture. The selected packet (No. 28) is an FTP-DATA packet. The details pane shows the following information:

- 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: Linux Rules...

A table titled "Socket for FTP data" is overlaid on the packet details, showing the connection between the server and client:

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_contrack_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 RH-Firewall-1-INPUT 9 -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*

- More control variable settings in `/etc/vsftpd/vsftpd.conf`
 - `anonymous_enable`
 - `local_enable`
 - `write_enable`
 - `anon_upload_enable`
 - `anon_mkdir_write_enable`
 - `dirmessage_enable`
 - `deny_email_enable`
 - ... etc.
- TCP Wrappers
 - `/etc/hosts.allow` – for permitted hosts
 - `/etc/hosts.deny` – to ban hosts

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>
```

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 licenses are fundamentally incompatible.

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

Web Server Survey Archives - Netcraft - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resizer Tools View Source Options

Rich's Cabr... W Apache HT... Apache Lic... Web Server... Web S... x [Chapter 1... ypmatch(1) Yahoo! Cal... ProLiant T...

NETCRAFT

SSL **NETCRAFT** Secure Server Survey 24 hr 小 24 小時 BANKING 銀行服務

Rackspace Managed Hosting - Web Hosting - Hosting

Site Search:

What's that site running?
e.g. google.com →

Get our RSS Feed
News Updates by Email

Netcraft Services

Phishing & Security

- Anti-Phishing Toolbar
- Phishing Site Feed
- Hosting Phishing Alerts
- Bank Fraud Detection
- Phishing Site Countermeasures
- Audited by Netcraft
- Open Redirect Detection
- Web Application Security Testing
- Web Application Security Course

Internet Data Mining

- Hosting Provider Analysis
- Million Busiest Websites

April 2009 Web Server Survey

In the **April 2009** survey we received responses from **231,510,169** sites. This represents an increase of over 6 million sites when compared with last month, with Google and nginx accounting for almost all of the changes. Apache remains in the lead, as it has since 1996, with a total of over 106 million sites, followed by Microsoft-IIS with over 67 million and QQ with almost 29 million.

Some interesting language specific servers which can be seen in this month's survey include the Ruby application specific servers which can be seen in this month's survey include the Ruby application server **Mongrel**, with just over 41 thousand sites, and the python based **Zope** with almost 46 thousand. The **Pike** and C based **Caudium** has almost 14 thousand sites, the **Erlang** based **Yaws** has about 70, and a newcomer, **Salvia**, which is a lightweight web server framework written in **Haskell**, has one.

Following on from last month's mention of fake server headers, where we saw the venerable **ZX_Spectrum/1997 (Sinclair_BASIC)**, this month we have **hi**, appearing as the server banner for **twitter**, which is currently the **432nd** most popular site amongst our **toolbar** community.

Total Sites Across All Domains August 1995 - April 2009

Year	Hostnames	Active
1995	162400000	162400000
2000	185600000	185600000
2005	208800000	208800000
2008	232000000	232000000

Hostnames
Active

NETCRAFT

OUTAGE ALERTS

PERFORMANCE MONITORING

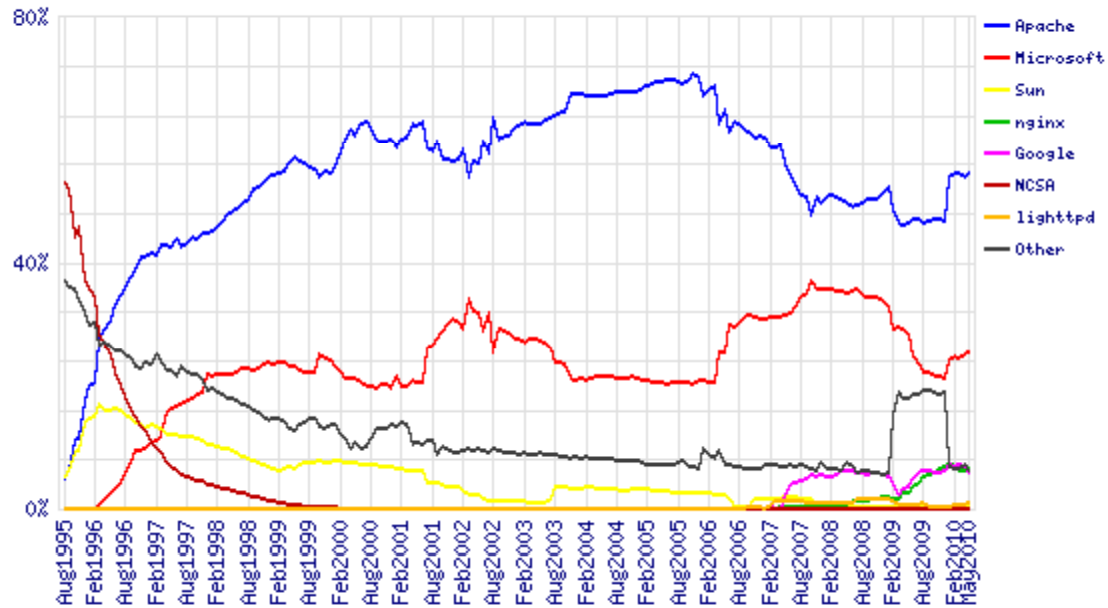
SEE NO HACK

Find: telnet Next Previous Highlight all Match case

Done

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

**Market Share for Top Servers Across All Domains
August 1995 - May 2010**



Developer	April 2010	Percent	May 2010	Percent	Change
Apache	110,752,854	53.93%	112,663,533	54.68%	0.75
Microsoft	51,284,570	24.97%	52,062,154	25.27%	0.30
nginx	12,977,486	6.32%	13,490,726	6.55%	0.23
Google	13,749,829	6.70%	12,357,212	6.00%	-0.70
lighttpd	1,078,403	0.53%	1,869,658	0.91%	0.38

Continue Reading...

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



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

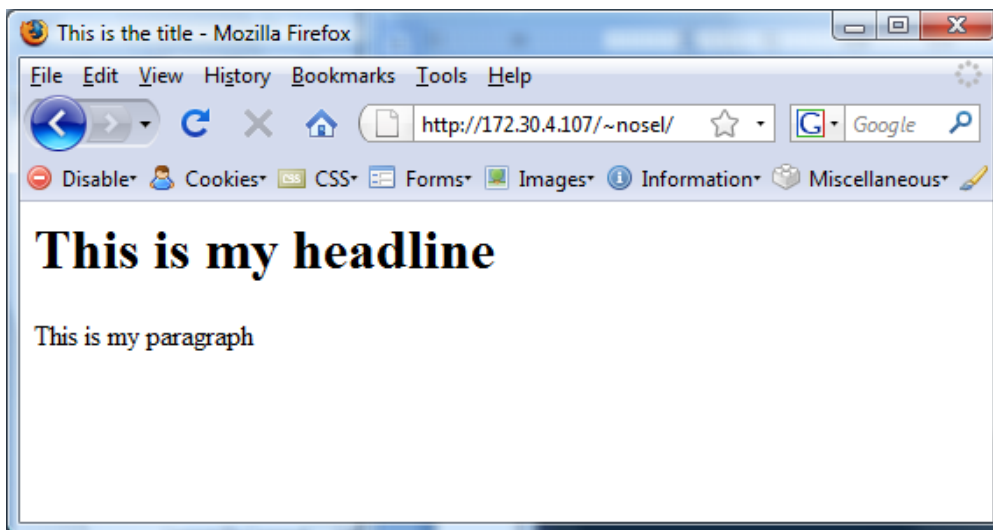
```
# chkconfig httpd on
```

How does a web server work

Web Pages

```
[root@elrond public_html]# cat
index.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 render them into a graphical format.



The default page is usually named index.html

```
[root@elrond home]# cd /home/arwen/public_html/
[root@elrond public_html]# cat 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>

</div>

<p>Spring 2009</p>

<div>
<a href="http://validator.w3.org/check/referer"
style="background-color: transparent">
</a>
&nbsp;&nbsp; 
<a href="http://jigsaw.w3.org/css-validator/check/referer"
style="background-color: transparent">
</a>
</div>

</body>
</html>
```

This web page has an image

```

<!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>

</div>

<p>Spring 2009</p>

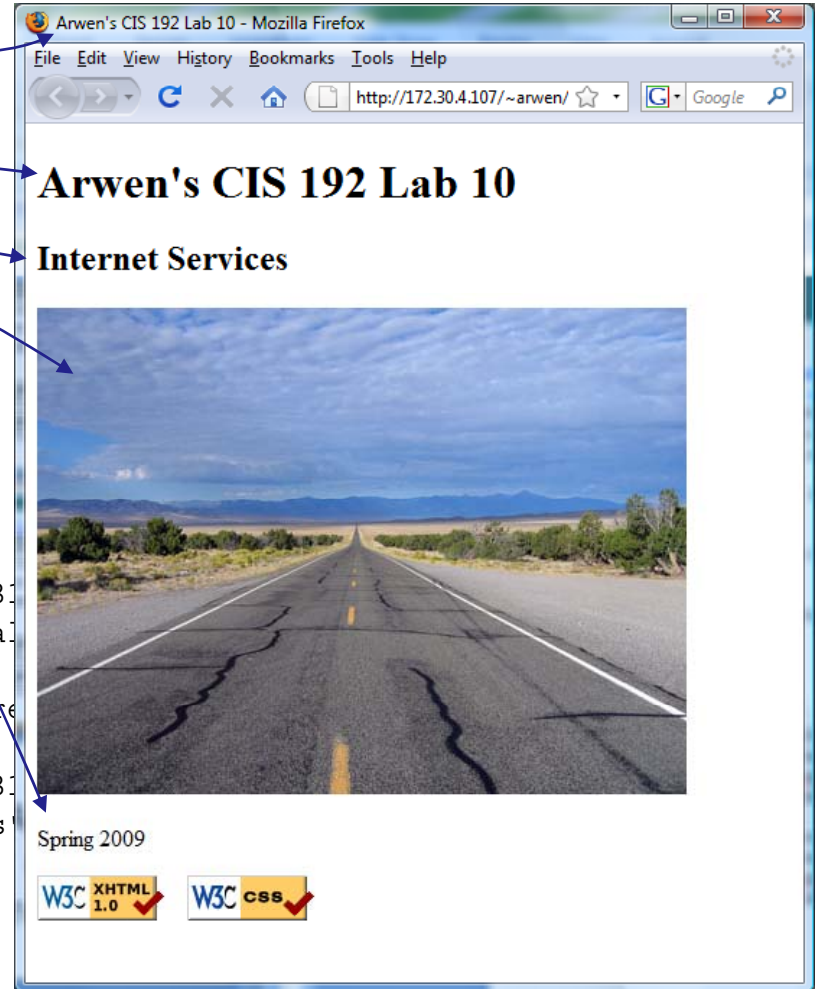
<div>
<a href="http://validator.w3.org/check/referer"
style="background-color: transparent">

</a>
<a href="http://jigsaw.w3.org/css-validator/check/referer"
style="background-color: transparent">

</a>
</div>

</body>
</html>

```



Sample web page available for Lab 10

Serving a Web Page

Destination port is 80

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 Firefox/3.0.10\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
  
```

3-way open handshake

The GET request

Socket	
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 (GET) the default web page from Arwen's home directory.

Serving a Web Page

Source port is 80

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
\r\n
</div>\r\n
\r\n
<p>Spring 2009</p>\r\n
\r\n
</div>\r\n

```

The contents of the web page can be seen in 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, after which the connection is closed.

A new and different connection (and socket) will be used to transfer the jpeg image file used in the web page.

Serving a Web Page

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
```

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

```
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
```

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

```
<!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>

</div>
```

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

Apache 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.

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 or permissive

`httpd_enable_homedirs=1` (for user `public_html` directories)

`httpd_sys_content_t` context type for published files & directories

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 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/`
- Note, in Linux the `~` is used to specify home directories
 - `cd ~` *will change to your own home directory*
 - `cd ~arwen` *will change to Arwen's home directory*



Elrond
Web Server

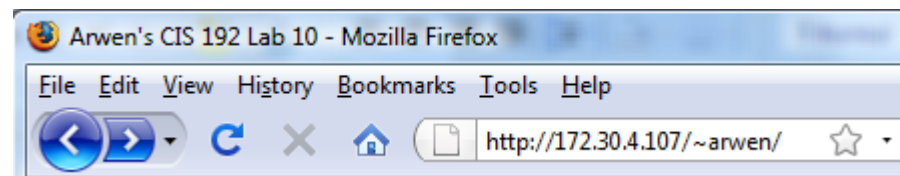
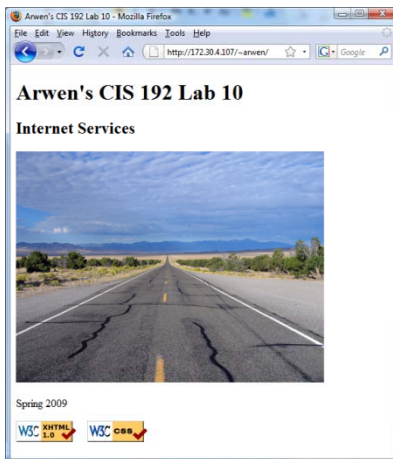
Apache User Directories

```
[root@elrond home]# ls -l Home directories
total 40
drwxr-x--x  5 arwen      users  4096 Apr 14 12:26 arwen
drwxr-x--x  4 celebrian users  4096 Apr 14 07:53 celebrian
drwxr-x--x 16 cis192    cis192 4096 May 16 21:20 cis192
drwxr-x--x  5 elrond    users  4096 Apr 14 12:26 elrond
drwxr-x--x  4 legolas   users  4096 Apr 14 08:10 legolas
```

```
[root@elrond home]# ls -ld arwen/public_html/
drwxr-x--x 2 arwen users 4096 Apr 14 07:37 arwen/public_html/
```

Arwen's public_html directory contains a web page (index.html) and an image (hwy50.jpg)

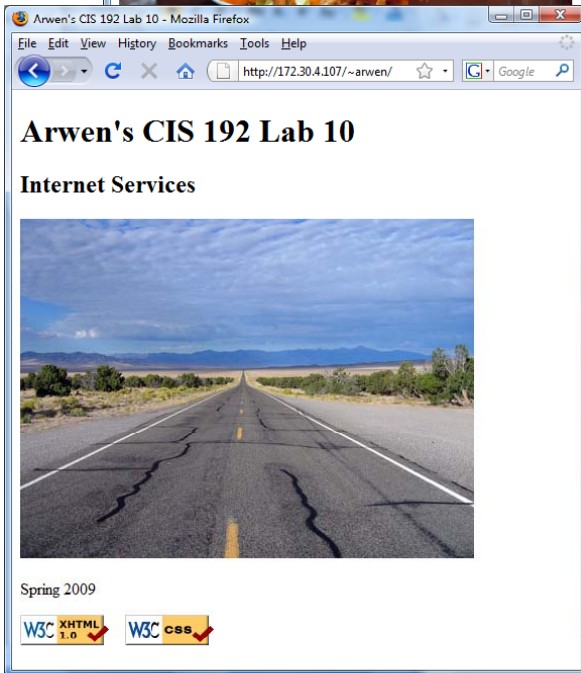
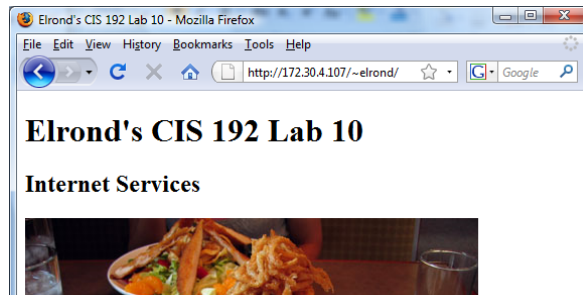
```
[root@elrond home]# ls -l arwen/public_html/
total 220
-rw-r--r-- 1 arwen users 37445 Apr 14 07:36 hwy50.jpg
-rw-r--r-- 1 arwen users   895 Apr 14 07:36 index.html
```



Requesting the default page from Arwen's directory

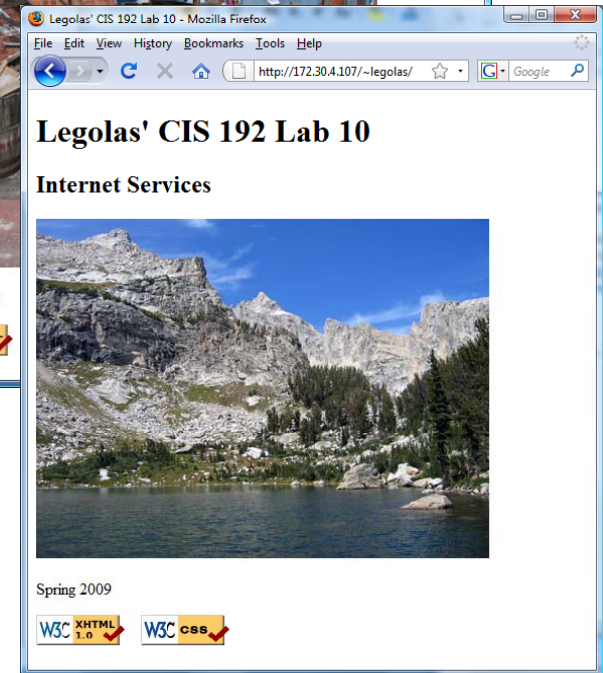
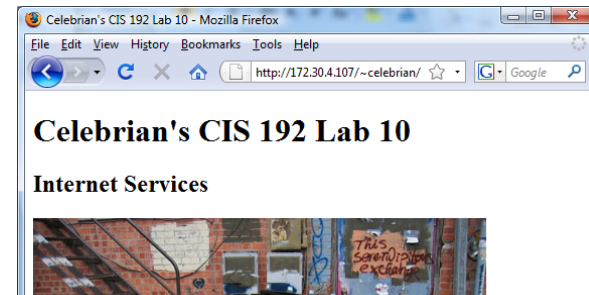
Apache User Directories

<http://172.30.4.107/~elrond>



<http://172.30.4.107/~arwen>

<http://172.30.4.107/~celebrian>



<http://172.30.4.107/~legolas>



Elrond

*One Web Server
Multiple web sites*

Apache User Directories

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

- 1) Edit `/etc/httpd/conf/httpd.conf`:
 - Set the **ServerName** directive with your hostname and port
 - Comment out the **UserDir disable** directive
 - Uncomment the **UserDir public_html** directive
- 2) Restart Apache: **service httpd restart**
- 3) Set 751 permissions on the user's home directory
- 4) Set 751 permissions on the user's `public_html` directory
- 5) Open port **80** in the firewall
- 6) For SELinux (enforcing mode), change published directory and file context types to **httpd_sys_content_t** and verify the boolean **httpd_enable_homedirs** is on

Apache User Directories

*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 elrond.rivendell:80
```

```
[root@elrond home]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1      elrond.rivendell elrond localhost.rivendell localhost
::1           localhost6.rivendell6 localhost6
[root@elrond home]#
```

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

Apache User Directories

*Comment out the **UserDir disable** directive, uncomment the **UserDir public_html** directive in /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

    #
    # 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
```

Apache User Directories

Set 751 permissions on the user's home directory

```
[root@elrond home]# chmod 751 /home/*
[root@elrond home]# ls -l /home
total 40
drwxr-x--x  5 arwen      users  4096 Apr 14 12:26 arwen
drwxr-x--x  4 celebrian users  4096 Apr 14 07:53 celebrian
drwxr-x--x 16 cis192     cis192 4096 May 16 21:20 cis192
drwxr-x--x  5 elrond     users  4096 Apr 14 12:26 elrond
drwxr-x--x  4 legolas    users  4096 Apr 14 08:10 legolas
[root@elrond home]#
```

Apache User Directories

Set 751 permissions on the user's public_html directory

```
[root@elrond home]# chmod 751 /home/*/public_html
[root@elrond home]# ls -ld /home/*/public_html
drwxr-x--x 2 arwen      users 4096 Apr 14 07:37 /home/arwen/public_html
drwxr-x--x 2 celebrian users 4096 Apr 14 07:53 /home/celebrian/public_html
drwxr-x--x 2 cis192    users 4096 Apr 13 19:08 /home/cis192/public_html
drwxr-x--x 2 elrond    users 4096 Apr 14 08:36 /home/elrond/public_html
drwxr-x--x 2 legolas   users 4096 Apr 14 08:10 /home/legolas/public_html
[root@elrond home]#
```


Firewall Configuration for Apache



Open port 80 in the firewall

```
[root@elrond home]# iptables -I RH-Firewall-1-INPUT 9 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

```
[root@elrond home]# iptables -nL RH-Firewall-1-INPUT
```

```
Chain RH-Firewall-1-INPUT (2 references)
```

target	prot	opt	source	destination	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0	icmp type 255
ACCEPT	esp	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	ah	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	udp	--	0.0.0.0/0	224.0.0.251	udp dpt:5353
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp dpt:631
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:631
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:80
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:22
REJECT	all	--	0.0.0.0/0	0.0.0.0/0	reject-with icmp-host-prohibited

```
[root@elrond home]#
```

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

```
[root@elrond home]#
```

iptables-save command will store the current rules in memory so they will be loaded again after the next system reboot (or service iptables restart)

Apache SELinux Configuration

When trying to access home directories without changing the SELinux context

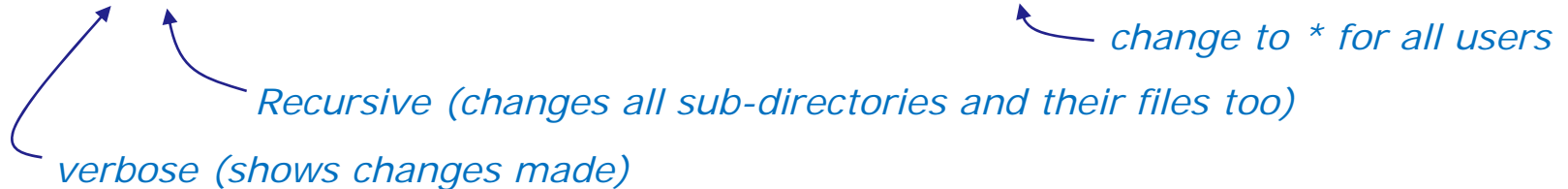


```
[root@elrond nosel]# ls -dZ public_html/
drwxr-xr-x  root root root:object_r:user_home_t public_html/

[root@elrond nosel]# ls -Z public_html/
-rw-r--r--  root root root:object_r:user_home_t index.html
```

Change the SELinux context to fix:

```
chcon -vR -t httpd_sys_content_t /home/nosel/public_html
```



```
[root@elrond nosel]# ls -Z public_html/
-rw-r--r--  root root root:object_r:httpd_sys_content_t index.html

[root@elrond nosel]# ls -dZ public_html/
drwxr-xr-x  root root root:object_r:httpd_sys_content_t public_html/
```

Apache User Directories

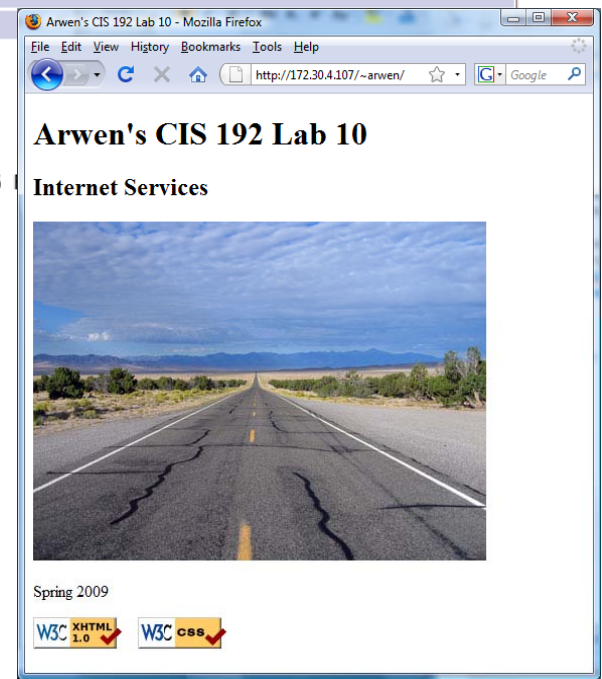
No.	Time	SIP	SP	DIP	DP	Protocol	Info
1	0.000000	192.168.0.24	52935	172.30.4.107	80	TCP	52935 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2	0.000027	172.30.4.107	80	192.168.0.24	52935	TCP	http > 52935 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=6
3	0.001117	192.168.0.24	52935	172.30.4.107	80	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

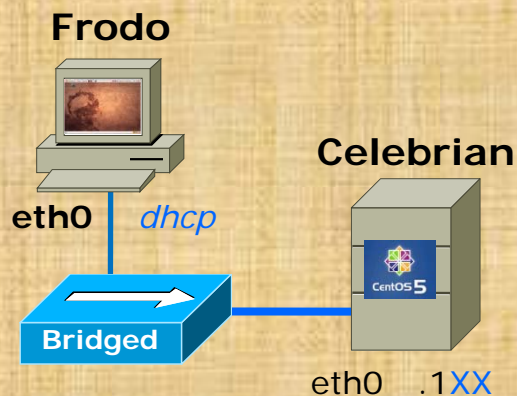

```

> 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

Because the URI was ~arwen the web page served will be /home/arwen/public_html/index.html





Setting up a web server

Celebrian

- Configure /etc/httpd/conf/httpd.conf
 - Line 265: *Un-comment and make* **ServerName celebrian.localdomain:80**
 - Line 355: *comment out*
 - Line 362: *Un-comment this line*
- Put simple web page in /home/cis192/public_html
 - **su - cis192**
 - **mkdir public_html; cd public_html**
 - **scp username@opus.cabrillo.edu:/home/cis192/depot/* .**
 - **chmod 751 /home/cis192**
 - **exit**
 - **service httpd start**
 - **service iptables stop**
 - **setenforce permissive**

In Lab 10 we will configure SELinux to work in enforcing mode and only open port 80 in the firewall.

Frodo:

- Browse to Celebrian/~cis192

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>



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}
/wwww/ando:
index.html
```

```
/www/hiro:
index.html
```

```
[root@elrond ~]# ls -l /www/{hiro,ando}
/wwww/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 TSEF
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
```

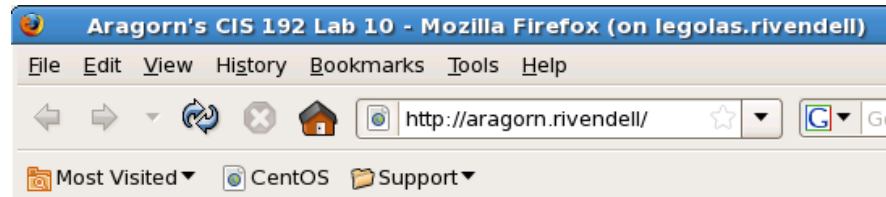
Different web sites

```
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>
```

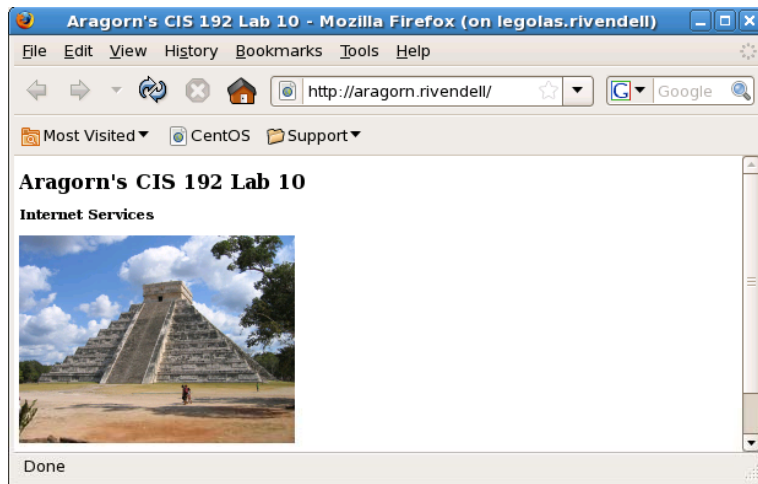
This VirtualHost directive associates the aragorn.rivendell name with files in /www/aragorn



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*

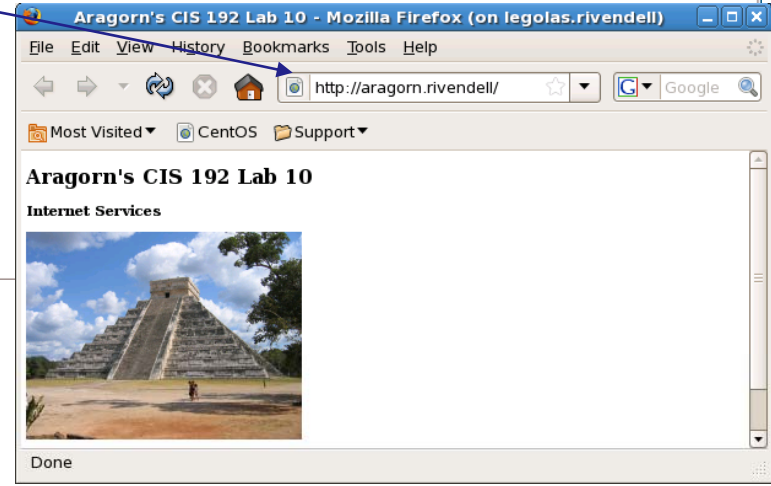
Websites by Names

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 eIrrond.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 TSEF
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

Wrap

References

Jim Griffin

- <http://www.cabrillo.edu/~jgriffin/CIS192/files/lesson14.html>



Next Class

Assignment: Lab 10

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



Test 3

Open book, notes, computer

Backup

Classroom Static IP addresses for VM's

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

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



Note the static IP address for your station to use in the next class exercise

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 <i>Retrieve legolas file</i>
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Win=0 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq=19 Ack=1 Win=5888 Len=0 <i>3 way handshake initiated by server</i>
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=19 Ack=1 Win=5888 Len=0
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 <i>File transfer</i>
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] Seq=20 Ack=2 Win=5888 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [FIN, ACK] Seq=20 Ack=2 Win=5888 Len=0 <i>4 way handshake to close connection</i>
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

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=0 Len=0
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [SYN, ACK] Seq=0 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 Win=0 Len=0
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 legolas
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 Ack=102 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 Win=0 Len=0
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=378 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [FIN, ACK] Seq=1 Ack=19 Win=0 Len=0
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


```
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:~#
```

Example FTP Session

Connect to server

Login

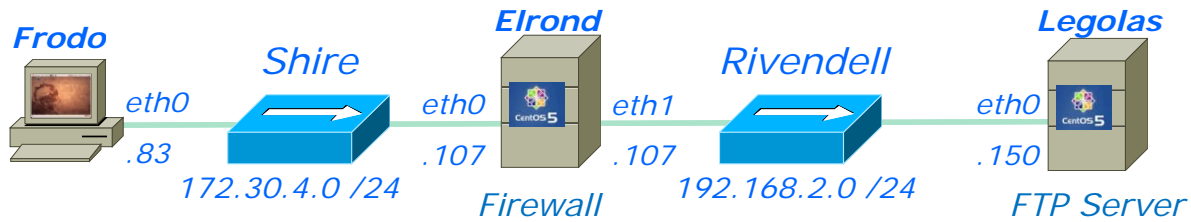
Initialize

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

*Get legolas file using **passive** mode*

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

End



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

Frodo FTP's into Legolas

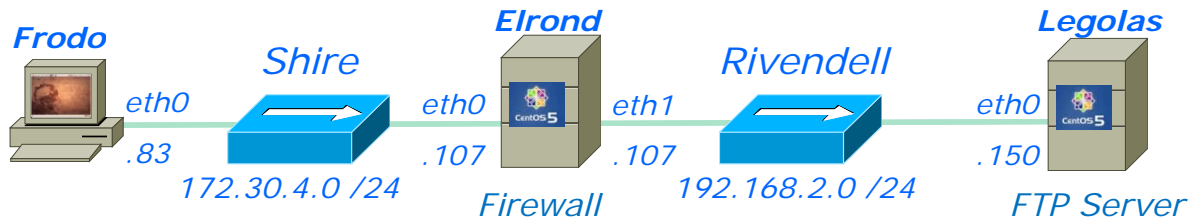
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [SYN] Seq=0 Win=58
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [SYN, ACK] Seq=0 A
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=1 Ack=1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 220 (vsFTPd 2.0.5)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

3 way handshake initiated by client

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

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21



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

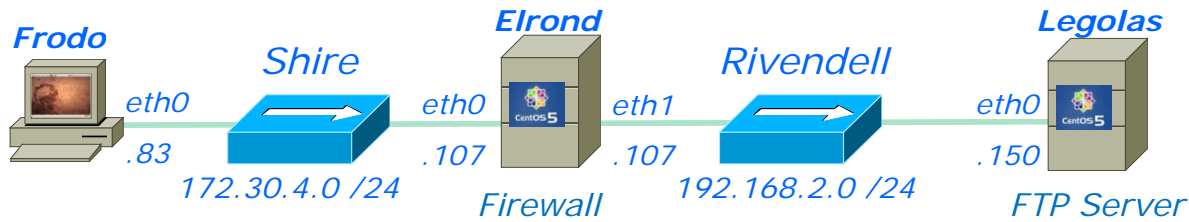
Note the login happens over the wire in clear "sniffable" text

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: USER cis192 username ★
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 password ★
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

Socket for commands

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

Client	Server
172.30.4.83	192.168.2.150
42855	21



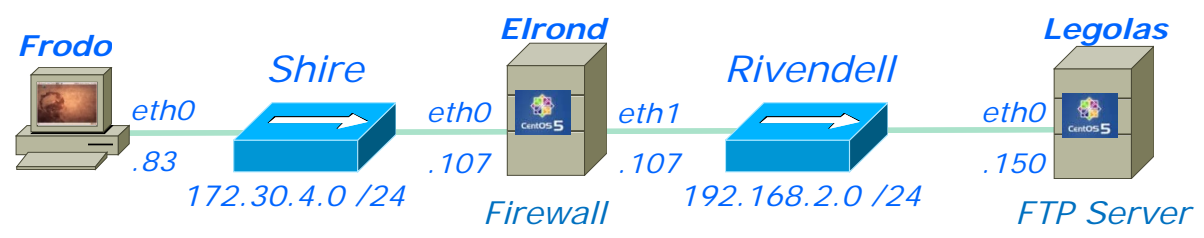
Remote system type is UNIX.
Using binary mode to transfer files.

- 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

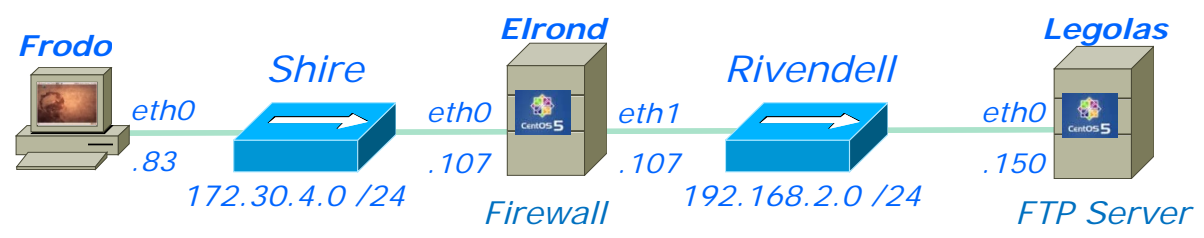
Client	Server
172.30.4.83	192.168.2.150
42571	20

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 PASV
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas <i>Retrieve legolas file</i>
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Win=0 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq=0 Win=0 Len=0 <i>3 way handshake initiated by server</i>
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=1 Ack=1 Win=5888 Len=0
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 <i>File transfer</i>
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] Seq=0 Win=0 Len=0
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [FIN, ACK] Seq=0 Win=0 Len=0 <i>4 way handshake to close connection</i>
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



```
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)
```

Passive Mode is when client initiates new connection for data transfer

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

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=0 Len=0
192.168.2.150	51283	172.30.4.83	41025	TCP	51283 > 41025 [SYN, ACK] Seq=0 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 Win=0 Len=0
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 legolas
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 Ack=19 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [ACK] Seq=1 Ack=19 Win=0 Len=0
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=102 Ack=378 Win=0 Len=0
172.30.4.83	41025	192.168.2.150	51283	TCP	41025 > 51283 [FIN, ACK] Seq=1 Ack=19 Win=0 Len=0
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

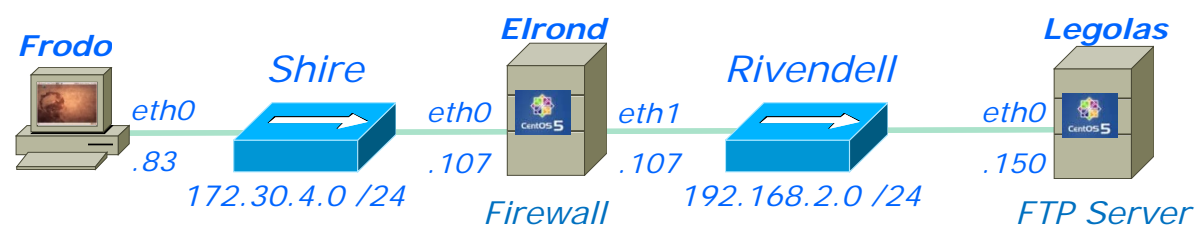
Passive reply to listen on 200, 83 = C853 = 51283

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

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

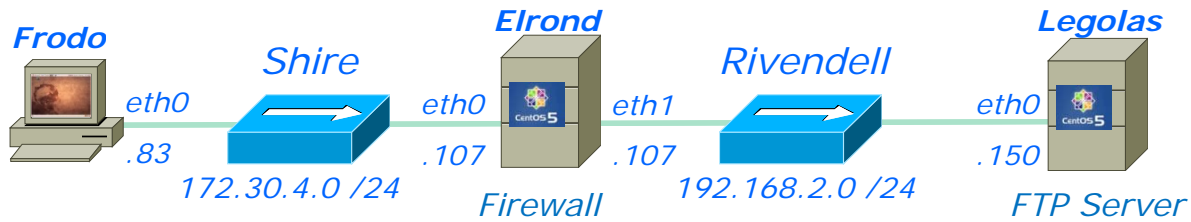
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,133,50
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PASV.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=127 Ack=448 Win=5856 Len=0
172.30.4.83	42855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

Retrieve legolas file

3 way handshake initiated by server

File transfer

4 way handshake to close connection



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

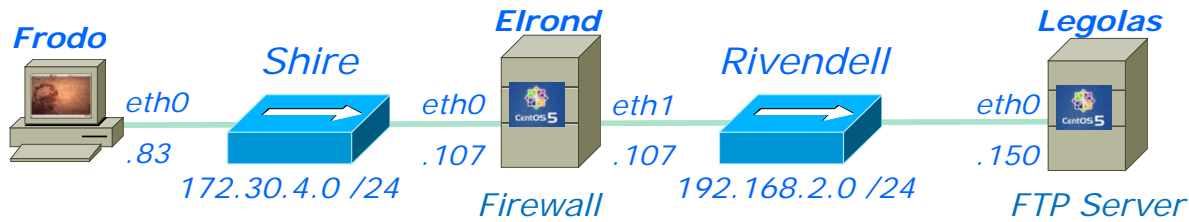
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	42855	192.168.2.150	21	FTP	Request: QUIT
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 221 Goodbye.
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=147 Ack=546
192.168.2.150	21	172.30.4.83	42855	TCP	ftp > 42855 [FIN, ACK] Seq=546 Ac
172.30.4.83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

4 way
handshake to
close connection

Socket for commands

Client	Server
172.30.4.83	192.168.2.150
42855	21

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
```

```
ACCEPT      all  --  0.0.0.0/0             0.0.0.0/0
```

```
ACCEPT      tcp  --  0.0.0.0/0             0.0.0.0/0
```

```
Chain OUTPUT (policy DROP)
```

```
target      prot opt source                destination
```

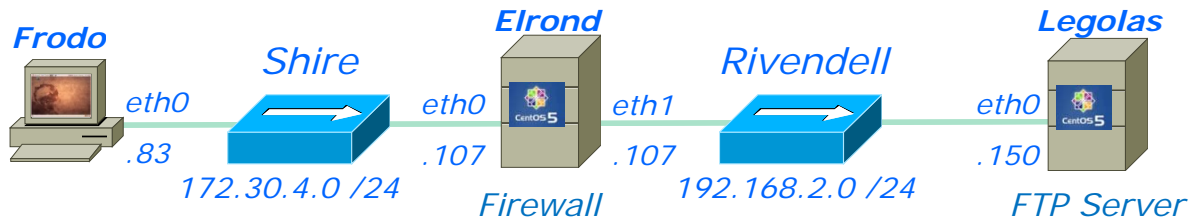
```
[root@elrond ~]#
```

For DNS lookups by
FTP server

udp dpt:53
state RELATED,ESTABLISHED
state NEW tcp dpt:21

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

Note: The FTP data port 20 is not specified



```

root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPD 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

```

ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (15.1 kB/s)

```

```

ftp> passive
Passive mode on.

```

```

ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,224,164)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (8.6 kB/s)

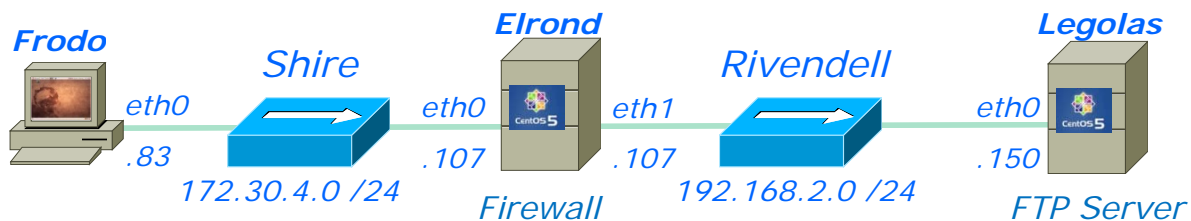
```

```

ftp> bye
221 Goodbye.
root@frodo:~#

```

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



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

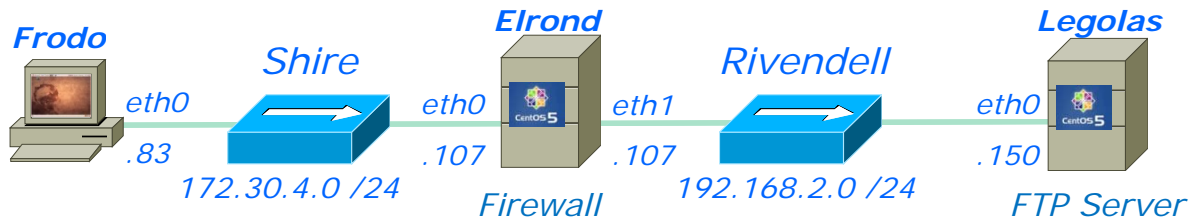
```
[root@elrond ~]# iptables -nL
Chain INPUT (policy DROP)
target      prot opt source                destination

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

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

*Now DNS lookups
are blocked*

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



```

root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPD 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

```

ftp> get legolas
local: legolas remote: legolas
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (15.1 kB/s)

```

```

ftp> passive
Passive mode on.

```

```

ftp> get legolas
local: legolas remote: legolas
227 Entering Passive Mode (192,168,2,150,224,164)
150 Opening BINARY mode data connection for legolas (18 bytes).
226 File send OK.
18 bytes received in 0.00 secs (8.6 kB/s)

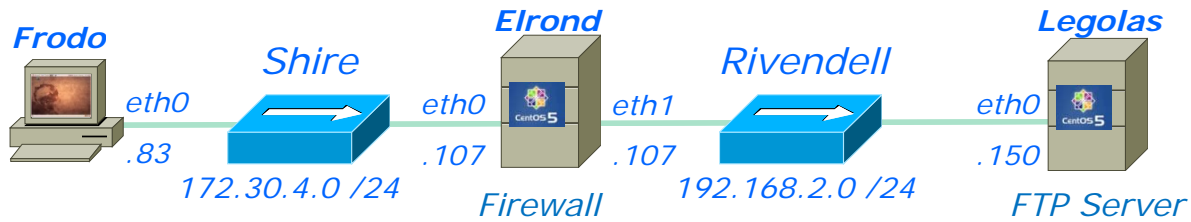
```

```

ftp> bye
221 Goodbye.
root@frodo:~#

```

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



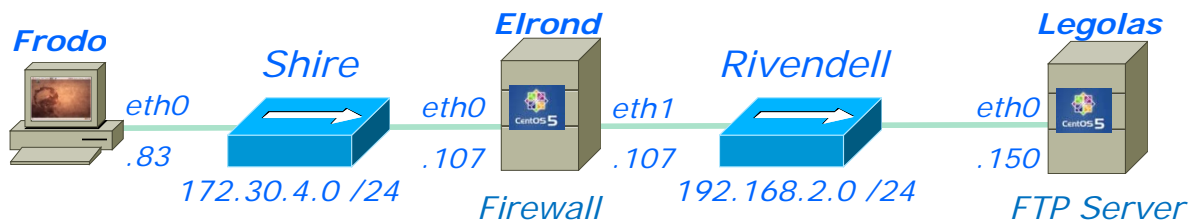
```

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

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

SIP	SP	DIP	DP	Protocol	Info	No.	Time
172.30.4.195	40823	192.168.2.150	21	FTP	Request: PASS Cabrillo	12	8.920738
192.168.2.150	58200	207.62.187.54	53	DNS	Standard query PTR 195.4.30.172.in-addr.ar	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.ar	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.



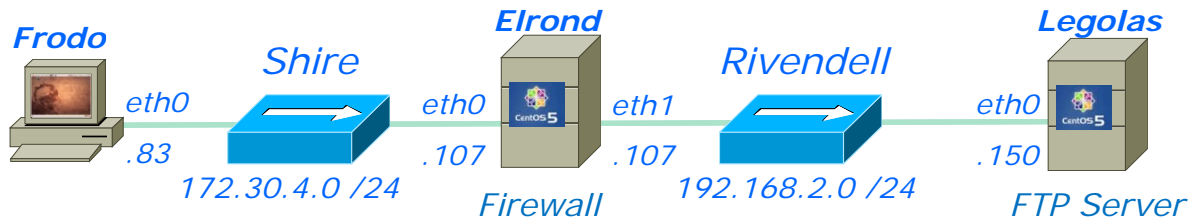
What If? We next remove the related state condition from the firewall?

```
[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 ACCEPT119
```



```

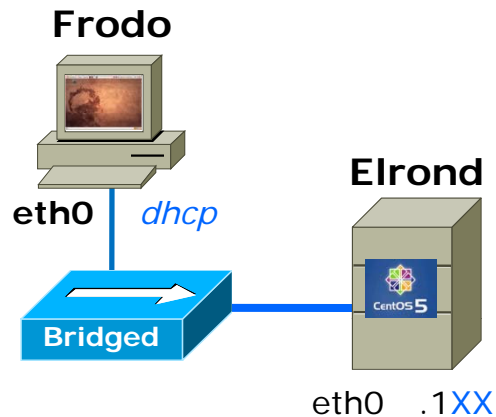
root@frodo:~# ftp legolas
Connected to legolas.
220 (vsFTPD 2.0.5)
Name (legolas:cis192): cis192
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get legolas
local: legolas remote: legolas
200 PORT command successful.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

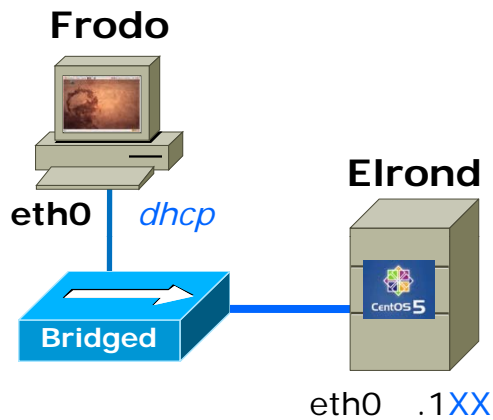


172.30.N.0 /24

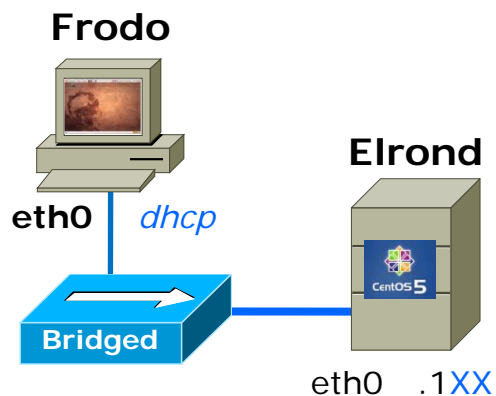
.1XX is based on your station number and the IP Table
 N=1 for the classroom and N=4 for the CIS lab or CTC
<http://simms-teach.com/docs/static-ip-addr.pdf>

- 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

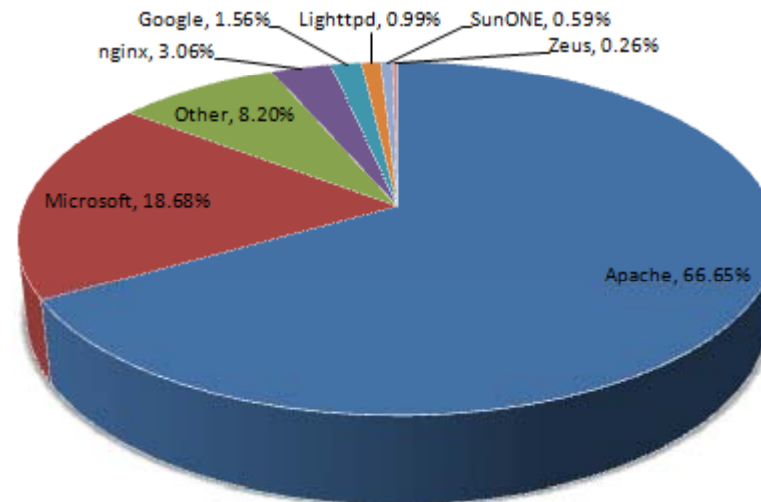
Elrond

- **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 servers do the busiest sites use?



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