Lesson Module Status

- Slides
- Whiteboard with 1st minute quiz

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

- Lab tested - NA
- Lab template in depot - NA

- Real Test ready
- Leaflock ready
- Post eval form from Susan

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

Course history and credits

Jim Griffin

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

Rick Graziani

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

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

Solomon

Sean C.

Chris

Corey

Bryan

Sean F.

Tony

David

Donna

Dave

Evan

Gabriel

Elia

Tajvia

Carlos

Adam

Ben

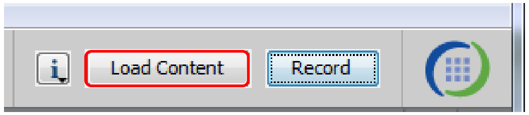
Laura

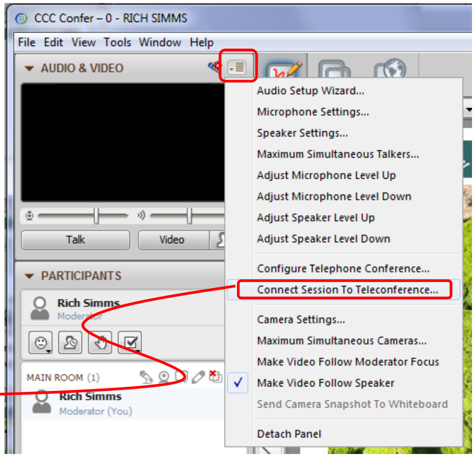
For tonight everyone join CCC Confer
and power up Frodo and Celebrian

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

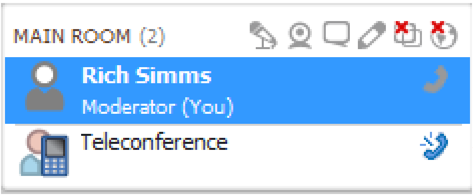
CCC Confer

[ ] **Preload White Board with _cis*lesson??*-WB_**



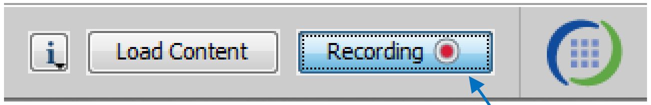

CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)

[ ] **Connect session to Teleconference**

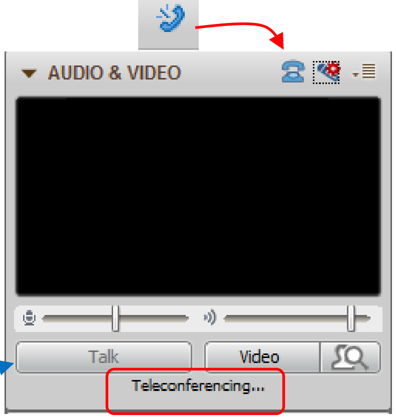


Session now connected to teleconference

[ ] **Is recording on?**



Red dot means recording



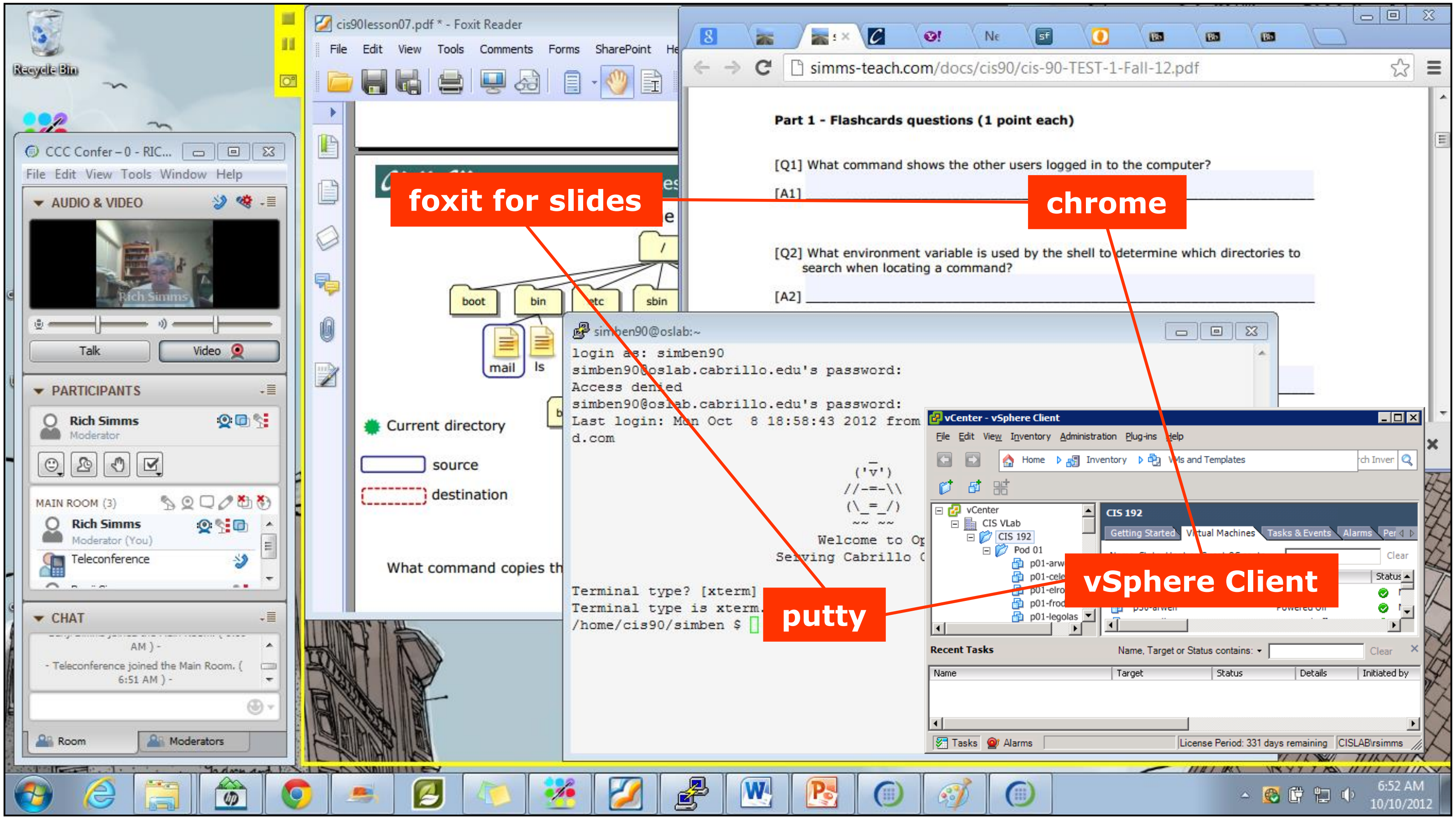
[ ] **Use teleconferencing, not mic**

Should be greyed out

CCC Confer

[ ] **Video (webcam) optional**

[ ] **layout and share apps**



simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashcards questions (1 point each)

[Q1] What command shows the other users logged in to the computer?

[A1] ______________________________

[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ______________________________

Current directory

source

destination

What command copies th

simben90@oslab:~

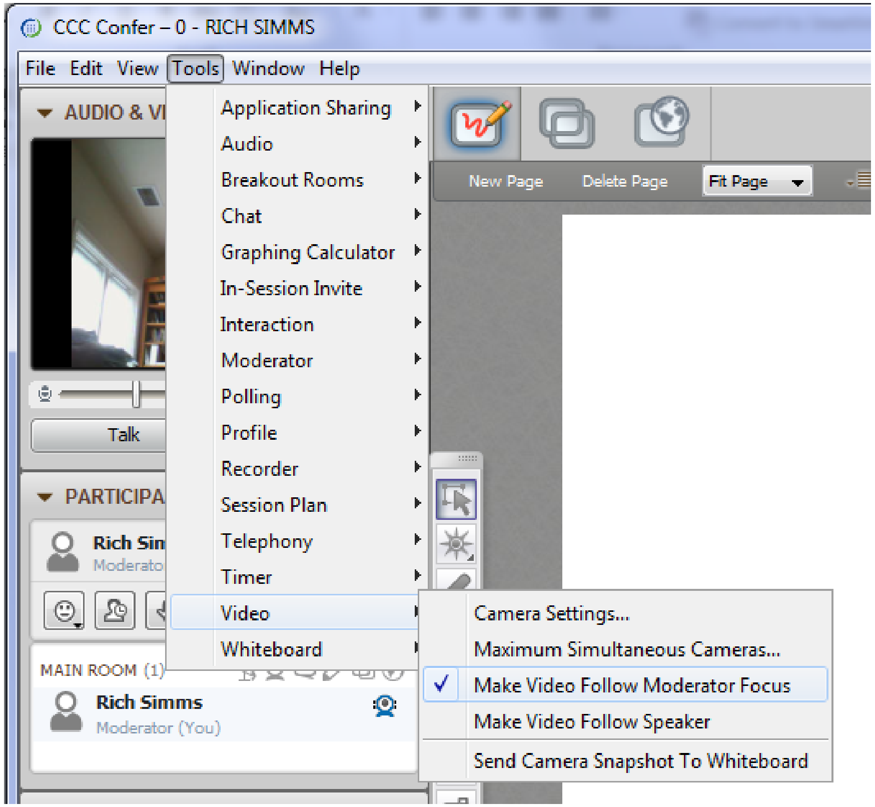
```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 2012 from
d.com

                                 ('v')
                                //-=-\\
                                (\_=_/)
                                 ~~ ~~
                            Welcome to Op
                        Serving Cabrillo C

Terminal type? [xterm]
Terminal type is xterm.
/home/cis90/simben $
```

CCC Confer

[ ] Video (webcam) optional

[ ] Follow moderator

[ ] Double-click on postages stamps

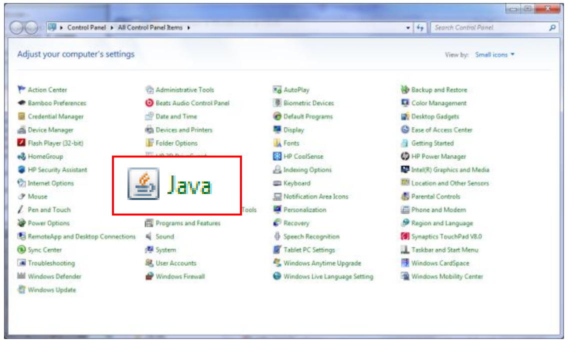


✓ Make Video Follow Moderator Focus

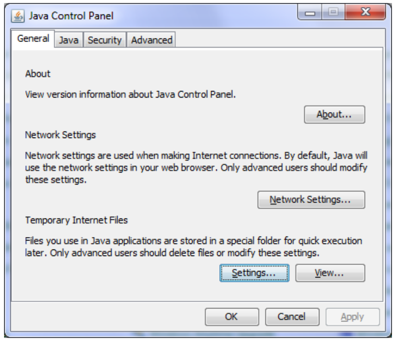
Universal Fix for CCC Confer:

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

Control Panel (small icons)



General Tab > Settings…


Java Control Panel

About

View version information about Java Control Panel.

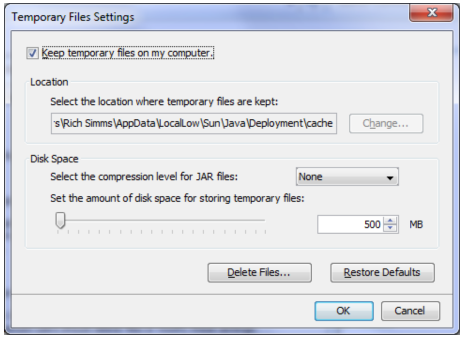
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size


Temporary Files Settings

☑ Keep temporary files on my computer.

Location

Select the location where temporary files are kept:

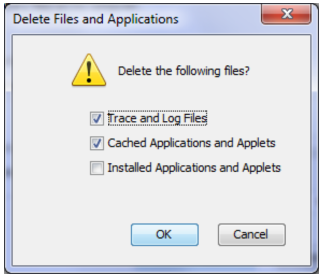
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

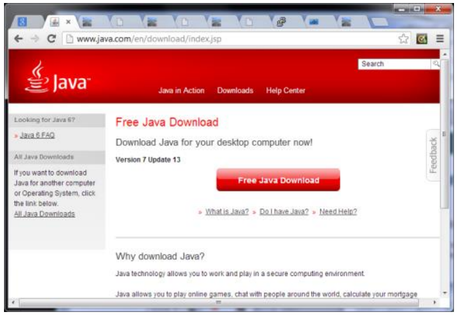
Delete these


Delete Files and Applications

Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
□ Installed Applications and Applets

Google Java download


www.java.com/en/download/index.jsp

If you want to download Java for another computer or Operating System, click the link below.
All Java Downloads

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

First Minute Quiz

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

No quiz today … test instead!

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

The Application Layer

Objectives

- Use basic network terminology to describe the five layers of the TCP/IP Reference Model, and describe at least one major function of each layer.
- Configure a network service with security restrictions for its use using either TCP Wrappers or a superdaemon.

Agenda

- No quiz today
- Questions on previous material
- Housekeeping
- Review
- Transport layer continued
- Tuning kernel parameters
- Security issues
- Application Layer
- Super daemons
- Telnet
- FTP
- Test 1
- Wrap

Questions on previous material

Questions

Lesson material?

Labs?

How this course works?

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

Taming the Beast

(Lab 4)

Hurdles

1. NIC order vs eth*n* order – watch out!
   - Check MAC address on NIC (VM Settings) with interface (ifconfig)

2. Can’t ping a systems “far interface” when the return route is different
   - echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
   - echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter

   - or edit /etc/sysctl.conf:

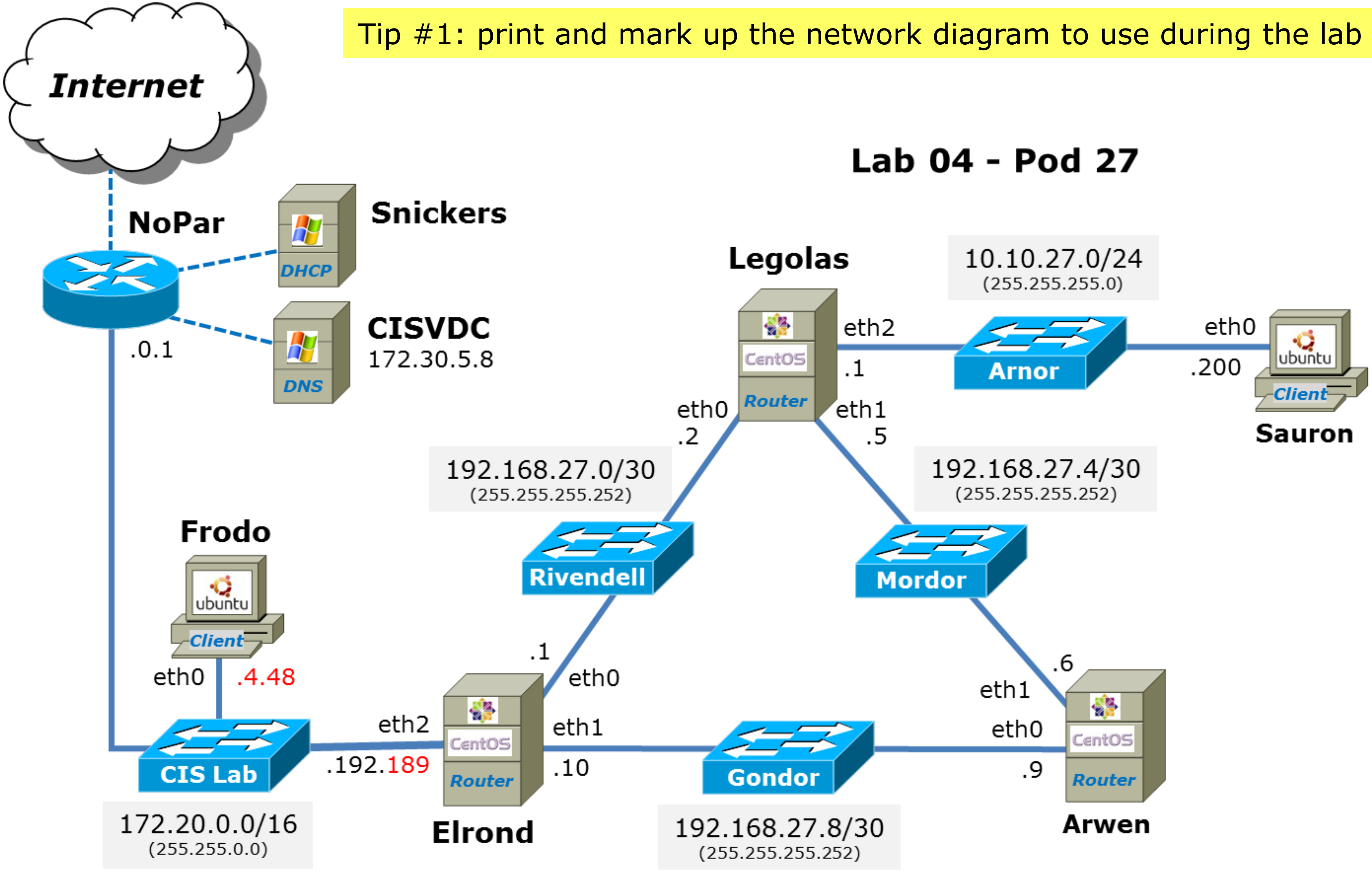
     ```
     # Controls source route verification
     net.ipv4.conf.default.rp_filter = 0
     ```

3. Sauron loses its IP address and default route
   - service network-manager stop

4. /etc/init.d/networking restart is deprecated
   - stop and start are not deprecated, but vShere Client loses console and you must work in the dark for awhile!

Lab 4 – Taming with the Beast

Tip #1: print and mark up the network diagram to use during the lab



Lab 4 – Taming the Beast

Tip #2: Populate /etc/hosts files with names used in Lab 4

On Elrond …

```
[root@p27-elrond ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain
localhost6 localhost6.localdomain6

192.168.27.2 legolas
192.168.27.9 arwen
172.20.4.48 frodo
10.10.27.200 sauron
172.20.0.1 nopar
[root@p27-elrond ~]#
```

On Legolas …

```
[root@p27-legolas ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain
localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain
localhost6 localhost6.localdomain6

192.168.27.6    arwen
192.168.27.1    elrond
172.20.4.48     frodo
10.10.27.200    sauron
[root@p27-legolas ~]#
```

Do the same for Arwen, Frodo, and Sauron and then you can use names rather than IP address for testing and troubleshooting

Lab 4 – Taming the Beast

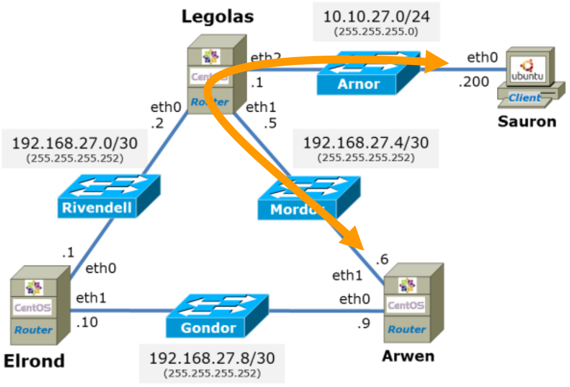
Tip #3: Create, in a one text file, key commands and all configuration files before doing lab then use scp, copy & paste or as a reference to configure systems.

Playing with the Beast

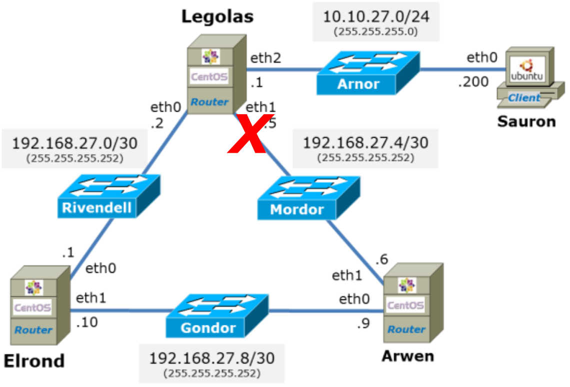
(Lab 4)

Lab 4 – Playing with the Beast

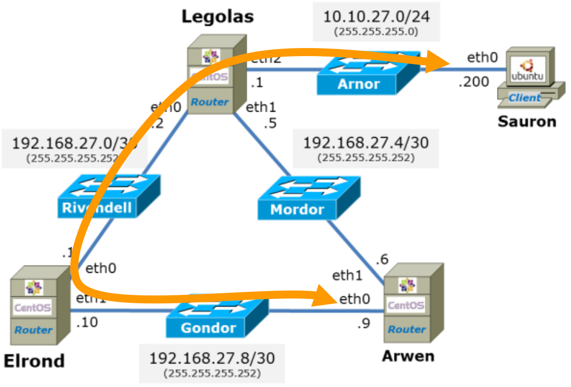
Playing #1: Force routing table to adapt to network changes you make



Pinging Arwen from Sauron via Legolas



Making trouble: The eth1 interface on Legolas is brought down with ***ifconfig eth0 down***



After a number of failed pings (and about 2.5 minutes), routing tables adjust and a new, longer route via Legolas and Elrond is used

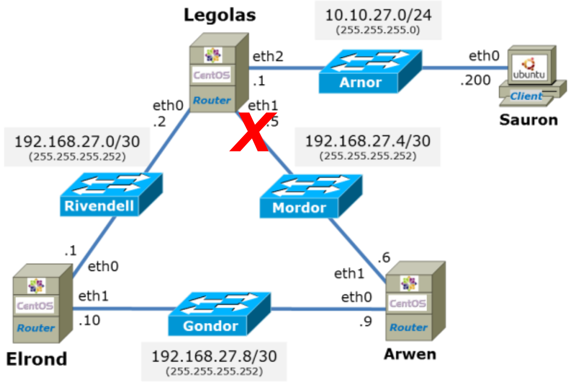
In Lab 4 you can observe routing tables update themselves as the network changes

Lab 4 – Playing with the Beast

Pinging Arwen from Sauron

```
cis192@p27-sauron:~$ while true; do ping -Rc2 arwen; sleep 10; done
PING arwen (192.168.27.6) 56(124) bytes of data.
64 bytes from arwen (192.168.27.6): icmp_req=1 ttl=63 time=0.562 ms
RR:     10.10.27.200             Sauron
        192.168.27.5             Legolas
        arwen (192.168.27.6)     Arwen
        arwen (192.168.27.6)     Arwen
        10.10.27.1               Legolas
        10.10.27.200             Sauron

64 bytes from arwen (192.168.27.6): icmp_req=2 ttl=63 time=0.545 ms

--- arwen ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.545/0.553/0.562/0.025 ms

PING arwen (192.168.27.6) 56(124) bytes of data.

--- arwen ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1008ms

< snipped >

PING arwen (192.168.27.6) 56(124) bytes of data.
64 bytes from arwen (192.168.27.6): icmp_req=1 ttl=62 time=0.646 ms
RR:     10.10.27.200            Sauron
        192.168.27.2            Legolas
        192.168.27.10           Elrond
        arwen (192.168.27.6)    Arwen
        arwen (192.168.27.6)    Arwen
        elrond (192.168.27.1)   Elrond
        10.10.27.1              Legolas
        10.10.27.200            Sauron

64 bytes from arwen (192.168.27.6): icmp_req=2 ttl=62 time=0.924 ms

--- arwen ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.646/0.785/0.924/0.139 ms
```

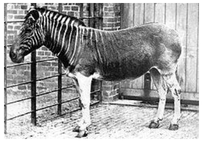
Trouble: Legolas eth1 is brought down



After a number of failed pings, routing tables adjust and now use longer route via Legolas and Elrond

Lab 4 – Playing with the Beast

Playing #2: Debug RIP events and packets with Quagga



http://en.wikipedia.org/wiki/Quagga

```
[root@p27-arwen ~]# vtysh

Hello, this is Quagga (version 0.99.15).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

p27-arwen.rivendell# debug rip events
p27-arwen.rivendell# debug rip packet
p27-arwen.rivendell# exit
```

Use the debug command to enable debugging

```
[root@p27-arwen ~]# tail -f /etc/quagga/ripd.conf
2013/03/10 17:54:19 RIP: ignore packet comes from myself
2013/03/10 17:54:23 RIP: RECV packet from 192.168.27.5 port 520 on eth1
2013/03/10 17:54:23 RIP: RECV RESPONSE version 2 packet size 104
2013/03/10 17:54:23 RIP:   0.0.0.0/0 -> 0.0.0.0 family 2 tag 0 metric 2
2013/03/10 17:54:23 RIP:   10.10.27.0/24 -> 0.0.0.0 family 2 tag 0 metric 1
2013/03/10 17:54:23 RIP:   172.20.0.0/16 -> 0.0.0.0 family 2 tag 0 metric 2
2013/03/10 17:54:23 RIP:   192.168.27.0/30 -> 0.0.0.0 family 2 tag 0 metric 1
2013/03/10 17:54:23 RIP:   192.168.27.8/30 -> 0.0.0.0 family 2 tag 0 metric 2
```

*Use **tail** with the **–f** option to monitor debug messages as they are written to **/var/quagga/ripd.conf***

Lab 4 – Playing with the Beast

Playing #3 Debug RIP events and packets with tcpdump

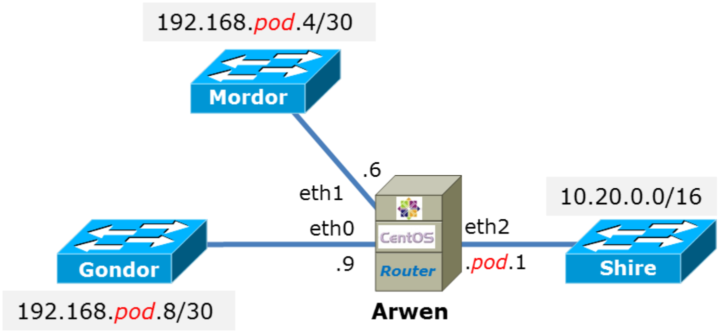
http://www.zyconmodels.com/museum/caterpillar.php

```
[root@p27-arwen ~]# tcpdump -v -i any port 520
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes

17:54:19.649009 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 152)
    10.20.27.1.router > 224.0.0.9.router:
        RIPv2, Response, length: 124, routes: 6
          AFI IPv4,          0.0.0.0/0 , tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,       10.10.27.0/24, tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,       172.20.0.0/16, tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,     192.168.27.0/30, tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,     192.168.27.4/30, tag 0x0000, metric: 1, next-hop: self
          AFI IPv4,     192.168.27.8/30, tag 0x0000, metric: 1, next-hop: self

17:54:23.674111 IP (tos 0xc0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 132)
    legolas.router > 224.0.0.9.router:
        RIPv2, Response, length: 104, routes: 5
          AFI IPv4,          0.0.0.0/0 , tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,       10.10.27.0/24, tag 0x0000, metric: 1, next-hop: self
          AFI IPv4,       172.20.0.0/16, tag 0x0000, metric: 2, next-hop: self
          AFI IPv4,     192.168.27.0/30, tag 0x0000, metric: 1, next-hop: self
          AFI IPv4,     192.168.27.8/30, tag 0x0000, metric: 2, next-hop: self
```

Use the tcpdump command to sniff rip packets

Lab 4 – Playing with the Beast

Connecting Pods for Extra Credit



Cable your Arwen to my Shire-27 switch

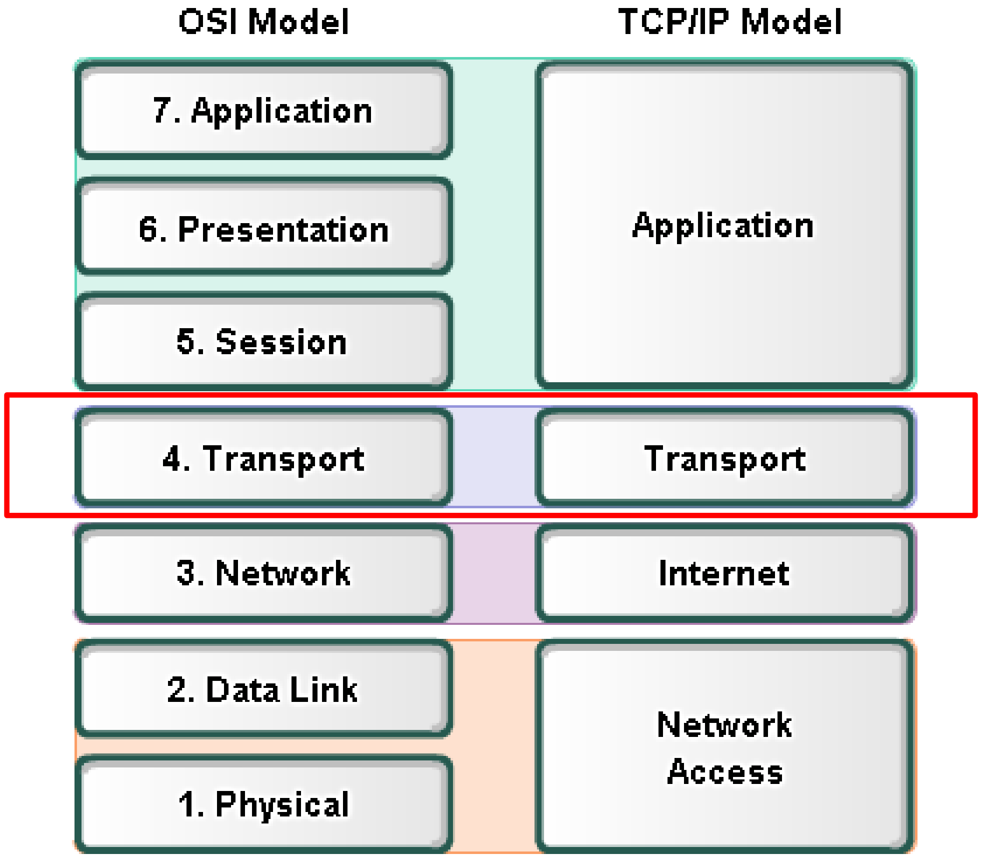
```
[root@p27-arwen ~]# cat /etc/quagga/ripd.conf
hostname p27-arwen
log file /var/log/quagga/ripd.log
router rip
  network eth0
  network eth1
  network eth2
  redistribute connected
line vty
  password quagga
[root@p27-arwen ~]#
```

Configure eth2 to participate in the RIP protocol

Transmission Control Protocol

(Review)

Protocol and Reference Models

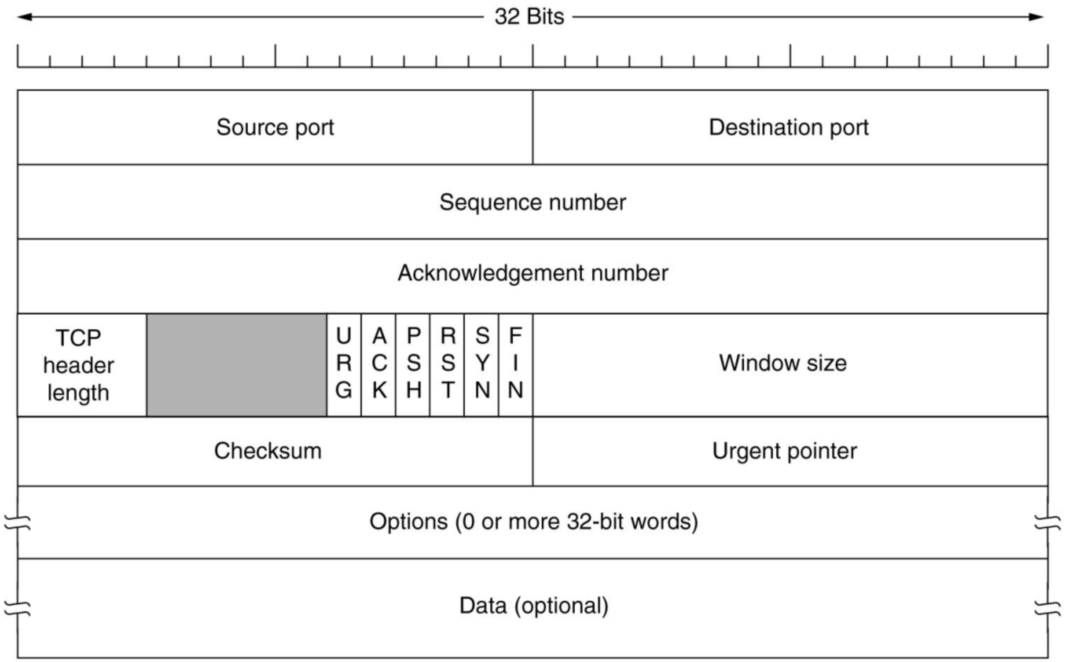


- The **Open Systems Interconnection (OSI)** model is the *most widely known internetwork reference model*.

Transport Layer

The Transmission Control Protocol

TCP Header



*The source and destination addresses at this level are **ports***

Sequence and acknowledgement numbers are used for flow control.

ACK, SYN and FIN flags are used for initiating connections, acknowledging data received and terminating connections

Window size is use to communicate buffer size of recipient.

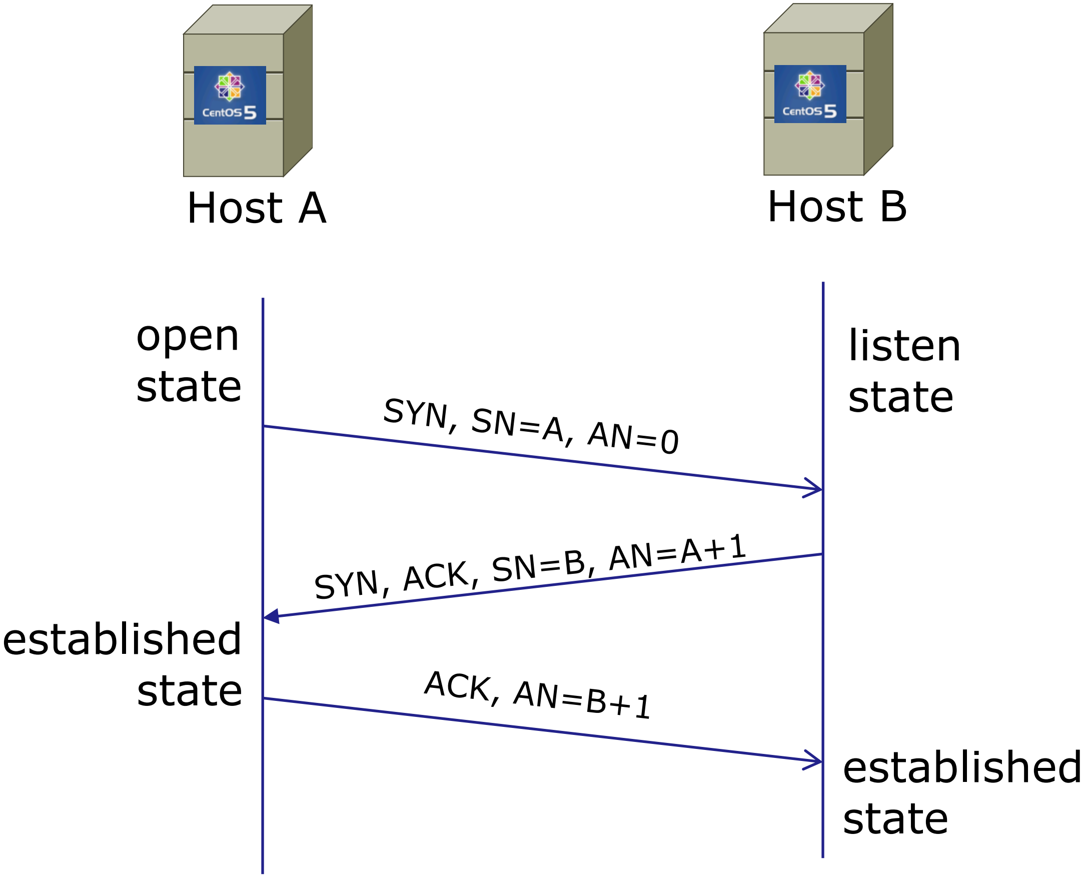
Options like SACK permit selective acknowledgement

Transport Layer

3-Way Handshake

Initiating a new TCP Connection

1. SYN
2. SYN-ACK
3. ACK



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
SYN=SYN flag set

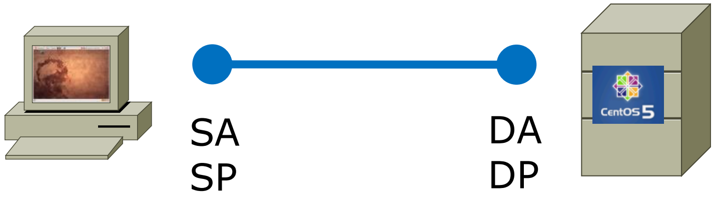
Transport Layer

Sockets

Sockets are communication endpoints which define a network connection between two computers (RFC 793).

- Source IP address
- Source port number

- Destination IP address
- Destination port number



The socket is associated to a port number so that the TCP layer can identify the application to send data to.

Application programs can read and write to a socket just like they do with files.

Transport Layer

The Transmission Control Protocol (TCP)

Continuing communications on an established connection

- The Sliding Window

  Used for flow control - allows sending additional segments before an acknowledgement is received based on recipients buffer size

- Flow Control (cumulative acknowledgment)

  Recipient tells sender the size of its input buffer and sends acknowledgements (ACKs) when data has been received. Sequence numbers are used to detect missing segments.

- The SACK option

  Selective acknowledgement so only the dropped segments need to be retransmitted.

- The RST Flag

  Used to terminate a connection when an abnormal situation happens

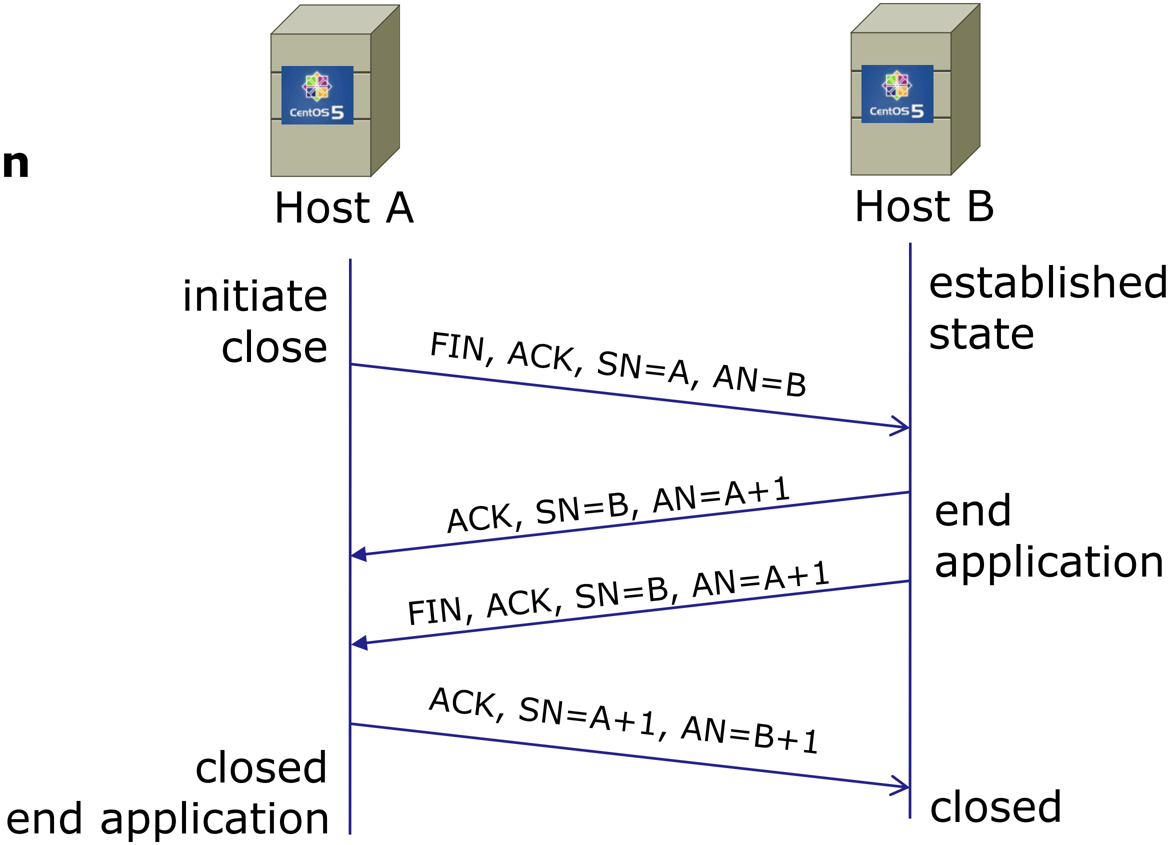
Transport Layer

Closing a TCP Connection

Four-Way Handshake

1. FIN, ACK
2. ACK
3. FIN, ACK
4. ACK

Closing with a shorter three-way handshake is also possible, where the Host A sends a FIN and Host B replies with a FIN & ACK (combining two steps into one) and Host A replies with an ACK.



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
FIN=FIN flag set

Telnet Example

(Review)

Example telnet session

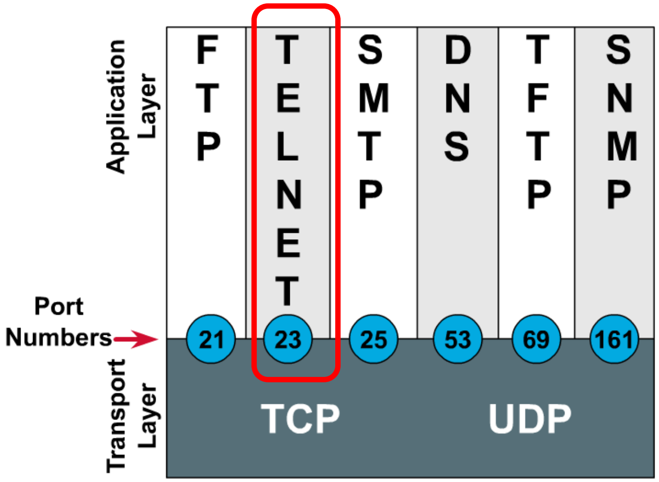
Telnet

- Provides command line interface to a remote host
- Client-server model
- Uses port 23
- Not secure, uses clear text over the network that can be sniffed

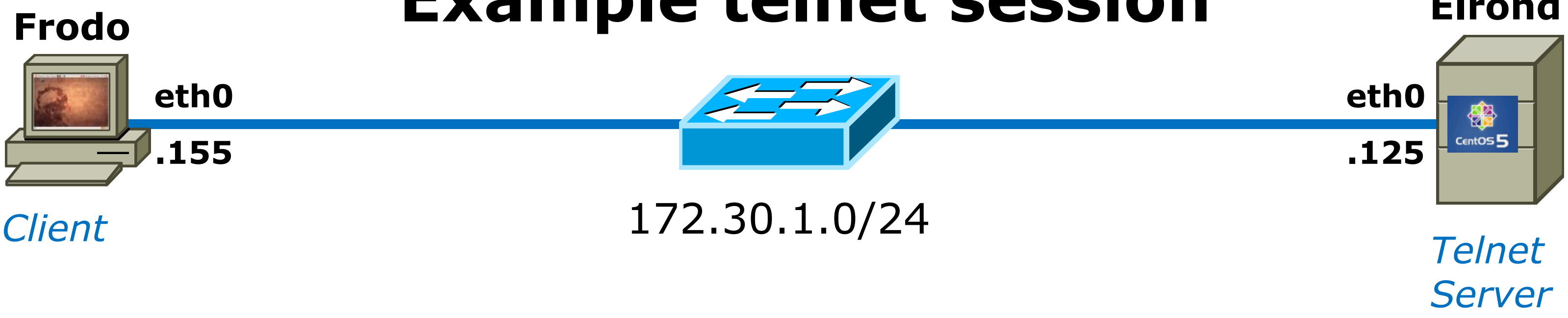
Telnet uses port 23

```
[root@elrond bin]# cat /etc/services
< snipped >
telnet          23/tcp
telnet          23/udp
< snipped >
[root@elrond bin]#
```

Port Numbers



Example telnet session



Frodo’s console

```
root@frodo:~# telnet 172.30.1.125
Trying 172.30.1.125...
Connected to 172.30.1.125.
Escape character is '^]'.
CentOS Linux release 6.0 (Final)
Kernel 2.6.32-71.el6.i686 on an i686
login: cis192
Password:
Last login: Sat Nov 19 17:45:01 from 172.30.1.155
[cis192@elrond ~]$ who
root     tty1         2011-11-19 15:44
root     pts/0        2011-11-19 15:54 (172.30.1.199)
cis192   pts/1        2011-11-19 18:15 (172.30.1.155)
[cis192@elrond ~]$ exit
logout
Connection closed by foreign host.
root@frodo:~#
```

The telnet client is installed on Frodo.

The telnet server is installed on Elrond.

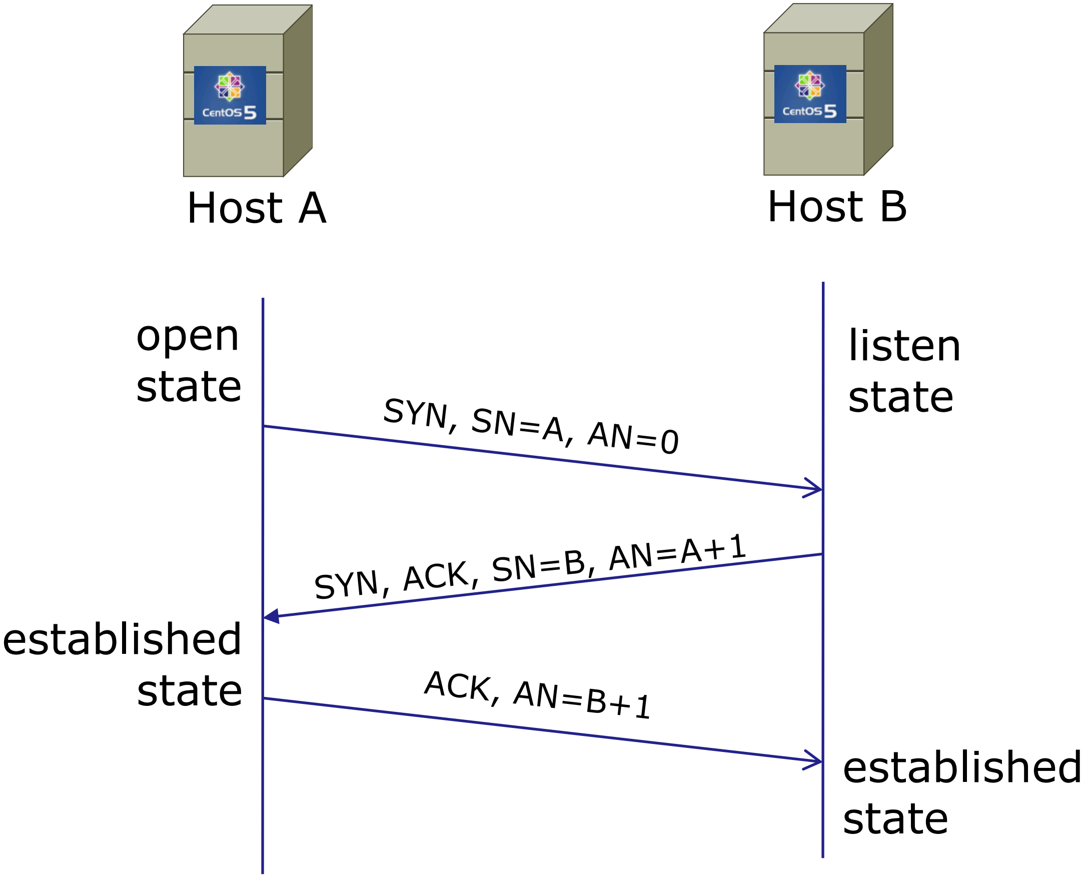
In this example, Telnet is used to login to Elrond from Frodo

Transport Layer

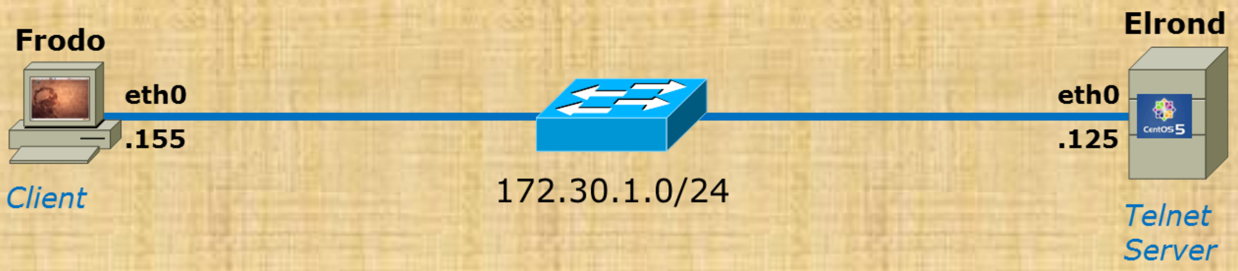
3-Way Handshake

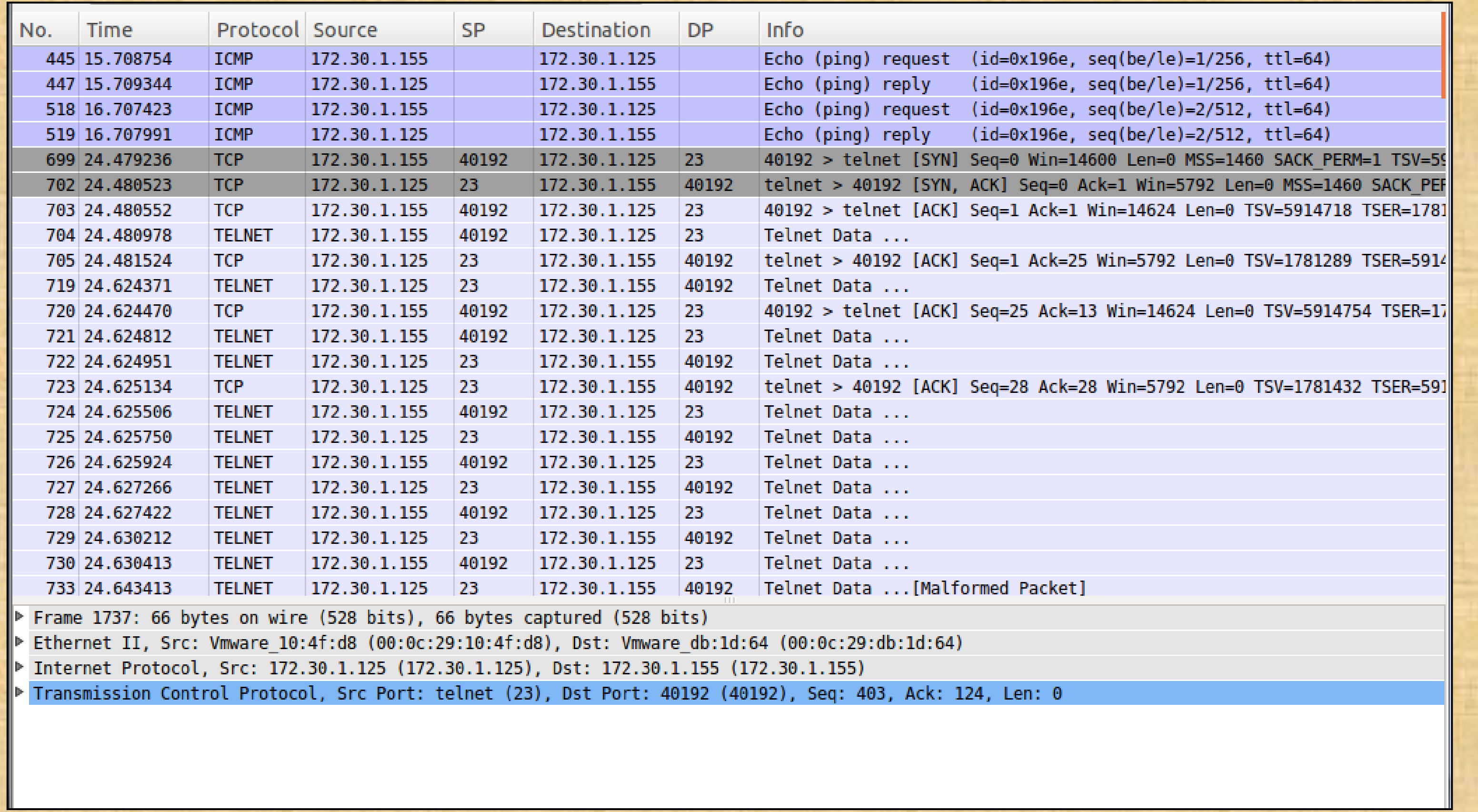
Initiating a new TCP Connection

1. SYN
2. SYN-ACK
3. ACK



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
SYN=SYN flag set

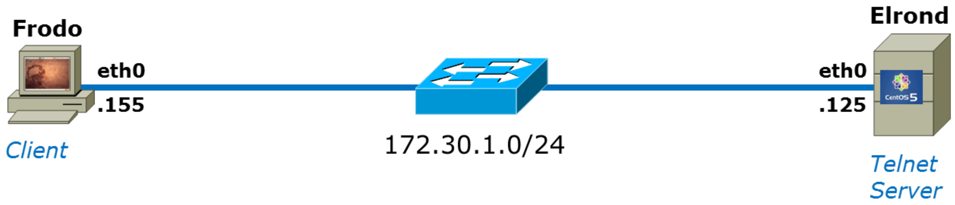


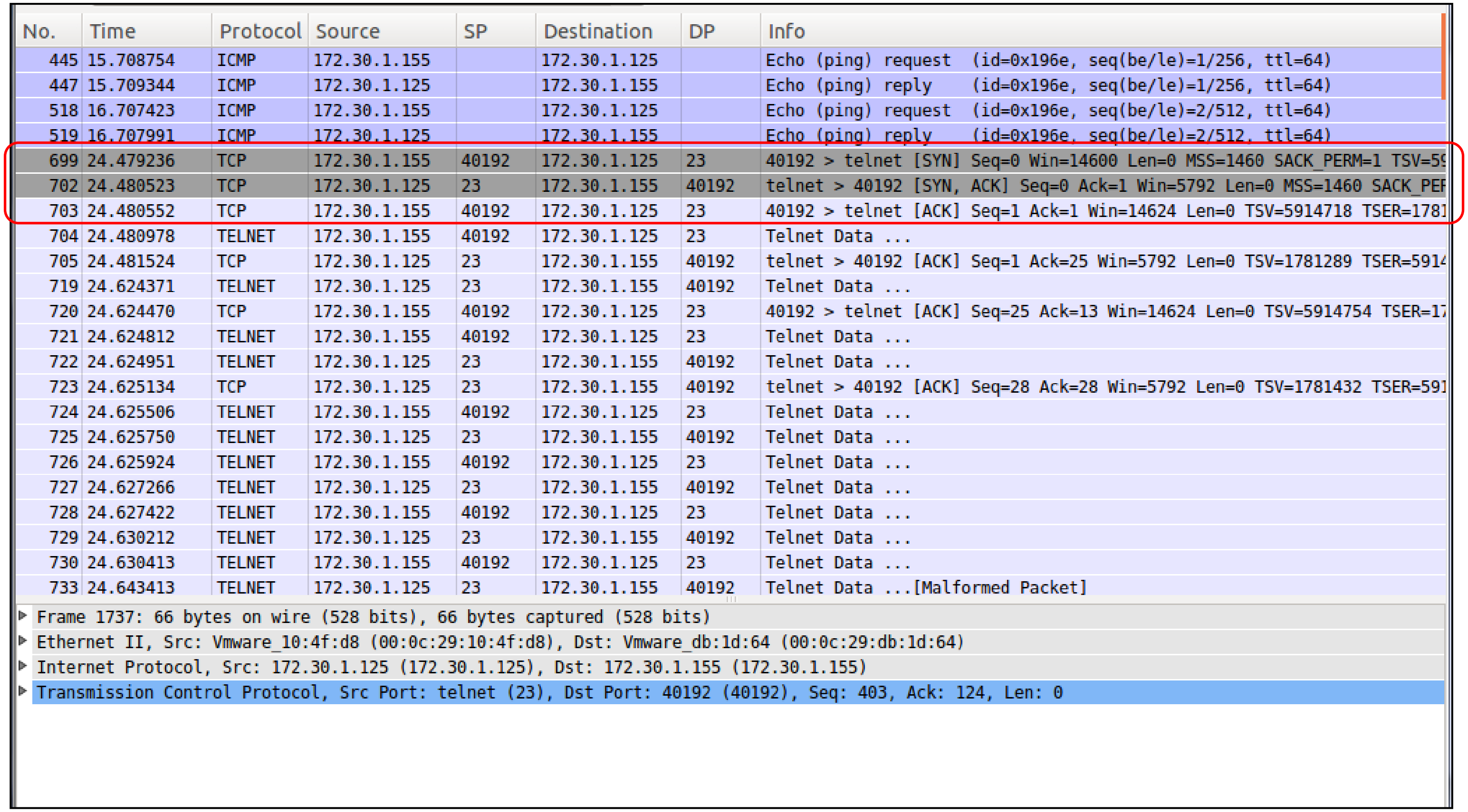


```
No.  Time       Protocol Source        SP    Destination   DP    Info
 445 15.708754  ICMP     172.30.1.155        172.30.1.125        Echo (ping) request  (id=0x196e, seq(be/le)=1/256, ttl=64)
 447 15.709344  ICMP     172.30.1.125        172.30.1.155        Echo (ping) reply    (id=0x196e, seq(be/le)=1/256, ttl=64)
 518 16.707423  ICMP     172.30.1.155        172.30.1.125        Echo (ping) request  (id=0x196e, seq(be/le)=2/512, ttl=64)
 519 16.707991  ICMP     172.30.1.125        172.30.1.155        Echo (ping) reply    (id=0x196e, seq(be/le)=2/512, ttl=64)
 699 24.479236  TCP      172.30.1.155  40192 172.30.1.125  23    40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
 702 24.480523  TCP      172.30.1.125  23    172.30.1.155  40192 telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
 703 24.480552  TCP      172.30.1.155  40192 172.30.1.125  23    40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
 704 24.480978  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 705 24.481524  TCP      172.30.1.125  23    172.30.1.155  40192 telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
 719 24.624371  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 720 24.624470  TCP      172.30.1.155  40192 172.30.1.125  23    40192 > telnet [ACK] Seq=25 Ack=13 Win=14624 Len=0 TSV=5914754 TSER=17
 721 24.624812  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 722 24.624951  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 723 24.625134  TCP      172.30.1.125  23    172.30.1.155  40192 telnet > 40192 [ACK] Seq=28 Ack=28 Win=5792 Len=0 TSV=1781432 TSER=591
 724 24.625506  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 725 24.625750  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 726 24.625924  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 727 24.627266  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 728 24.627422  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 729 24.630212  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 730 24.630413  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 733 24.643413  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...[Malformed Packet]

▸ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▸ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▸ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

Point to the start and end of the three way handshake

Example telnet session





No.	Time	Protocol	Source	SP	Destination	DP	Info
445	15.708754	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=1/256, ttl=64)
447	15.709344	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=1/256, ttl=64)
518	16.707423	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=2/512, ttl=64)
519	16.707991	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=2/512, ttl=64)
699	24.479236	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
702	24.480523	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
703	24.480552	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
704	24.480978	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
705	24.481524	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
719	24.624371	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
720	24.624470	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=25 Ack=13 Win=14624 Len=0 TSV=5914754 TSER=17
721	24.624812	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
722	24.624951	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
723	24.625134	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=28 Ack=28 Win=5792 Len=0 TSV=1781432 TSER=591
724	24.625506	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
725	24.625750	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
726	24.625924	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
727	24.627266	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
728	24.627422	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
729	24.630212	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
730	24.630413	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
733	24.643413	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...[Malformed Packet]

```
▸ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▸ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▸ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▸ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

3-way handshake that initiates TCP connection

Connection established

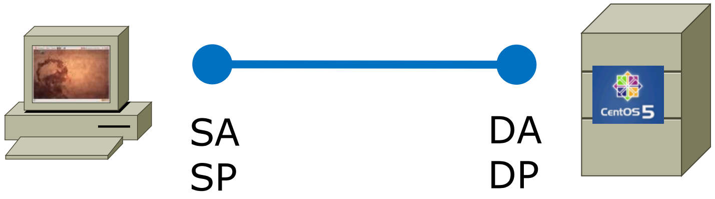
Transport Layer

Sockets

Sockets are communication endpoints which define a network connection between two computers (RFC 793).

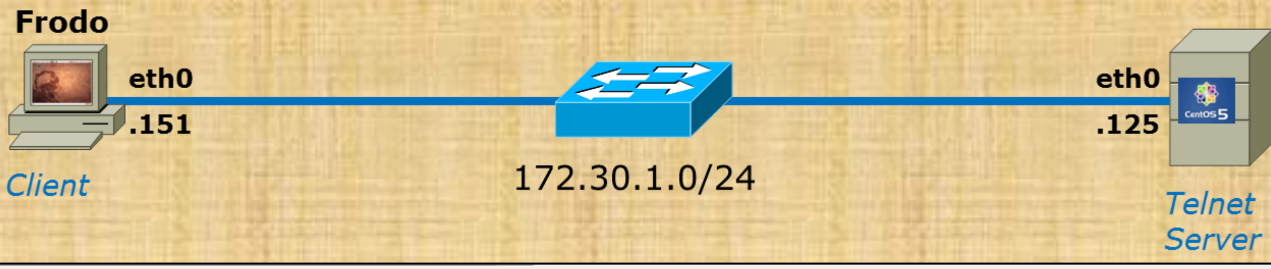
- Source IP address
- Source port number

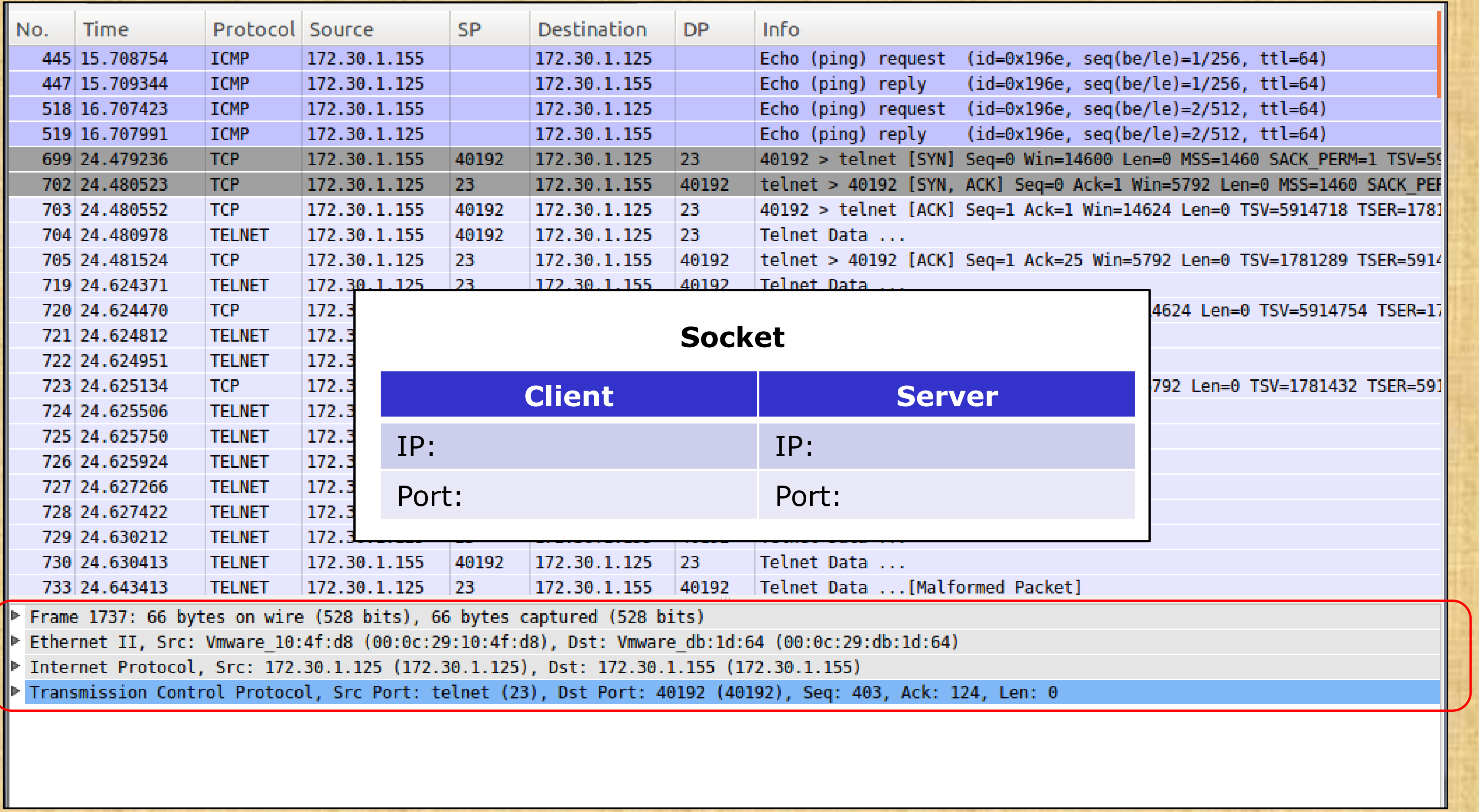
- Destination IP address
- Destination port number



The socket is associated to a port number so that the TCP layer can identify the application to send data to.

Application programs can read and write to a socket just like they do with files.





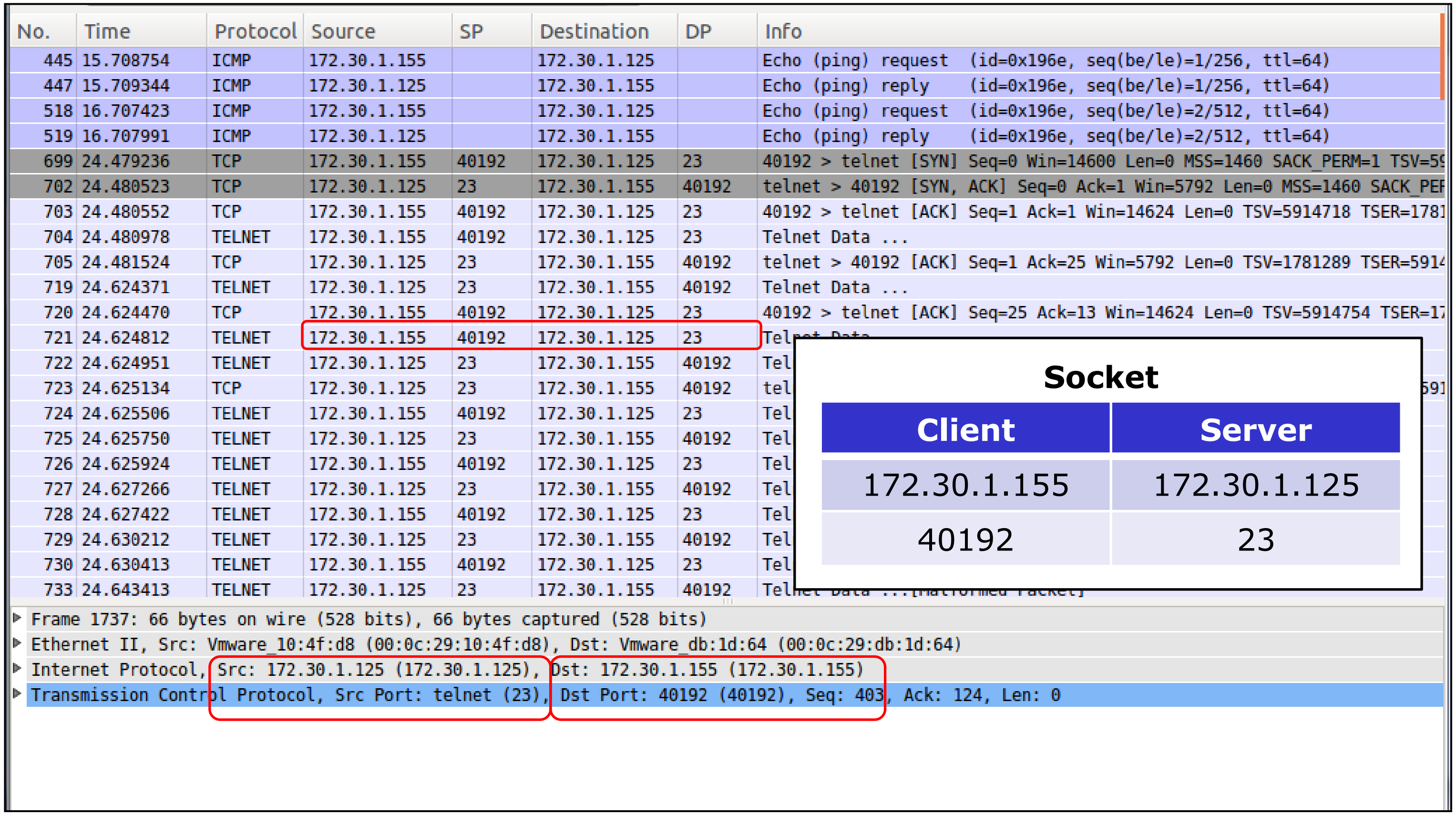
```
No.  Time       Protocol Source        SP    Destination   DP    Info
 445 15.708754  ICMP     172.30.1.155        172.30.1.125        Echo (ping) request  (id=0x196e, seq(be/le)=1/256, ttl=64)
 447 15.709344  ICMP     172.30.1.125        172.30.1.155        Echo (ping) reply    (id=0x196e, seq(be/le)=1/256, ttl=64)
 518 16.707423  ICMP     172.30.1.155        172.30.1.125        Echo (ping) request  (id=0x196e, seq(be/le)=2/512, ttl=64)
 519 16.707991  ICMP     172.30.1.125        172.30.1.155        Echo (ping) reply    (id=0x196e, seq(be/le)=2/512, ttl=64)
 699 24.479236  TCP      172.30.1.155  40192 172.30.1.125  23    40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
 702 24.480523  TCP      172.30.1.125  23    172.30.1.155  40192 telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
 703 24.480552  TCP      172.30.1.155  40192 172.30.1.125  23    40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
 704 24.480978  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 705 24.481524  TCP      172.30.1.125  23    172.30.1.155  40192 telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
 719 24.624371  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...
 720 24.624470  TCP      172.3                                   4624 Len=0 TSV=5914754 TSER=17
 721 24.624812  TELNET   172.3
 722 24.624951  TELNET   172.3
 723 24.625134  TCP      172.3                                   792 Len=0 TSV=1781432 TSER=591
 724 24.625506  TELNET   172.3
 725 24.625750  TELNET   172.3
 726 24.625924  TELNET   172.3
 727 24.627266  TELNET   172.3
 728 24.627422  TELNET   172.3
 729 24.630212  TELNET   172.3
 730 24.630413  TELNET   172.30.1.155  40192 172.30.1.125  23    Telnet Data ...
 733 24.643413  TELNET   172.30.1.125  23    172.30.1.155  40192 Telnet Data ...[Malformed Packet]

▶ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

Socket

Client	Server
IP:	IP:
Port:	Port:

What unique socket is being used for this connection?

Example telnet session



```
No.  Time       Protocol Source       SP    Destination  DP    Info
 445 15.708754  ICMP     172.30.1.155       172.30.1.125       Echo (ping) request  (id=0x196e, seq(be/le)=1/256, ttl=64)
 447 15.709344  ICMP     172.30.1.125       172.30.1.155       Echo (ping) reply    (id=0x196e, seq(be/le)=1/256, ttl=64)
 518 16.707423  ICMP     172.30.1.155       172.30.1.125       Echo (ping) request  (id=0x196e, seq(be/le)=2/512, ttl=64)
 519 16.707991  ICMP     172.30.1.125       172.30.1.155       Echo (ping) reply    (id=0x196e, seq(be/le)=2/512, ttl=64)
 699 24.479236  TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
 702 24.480523  TCP      172.30.1.125 23    172.30.1.155 40192 telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PEF
 703 24.480552  TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
 704 24.480978  TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...
 705 24.481524  TCP      172.30.1.125 23    172.30.1.155 40192 telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
 719 24.624371  TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
 720 24.624470  TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=25 Ack=13 Win=14624 Len=0 TSV=5914754 TSER=17
 721 24.624812  TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data
 722 24.624951  TELNET   172.30.1.125 23    172.30.1.155 40192 Tel
 723 24.625134  TCP      172.30.1.125 23    172.30.1.155 40192 tel                                                        591
 724 24.625506  TELNET   172.30.1.155 40192 172.30.1.125 23    Tel
 725 24.625750  TELNET   172.30.1.125 23    172.30.1.155 40192 Tel
 726 24.625924  TELNET   172.30.1.155 40192 172.30.1.125 23    Tel
 727 24.627266  TELNET   172.30.1.125 23    172.30.1.155 40192 Tel
 728 24.627422  TELNET   172.30.1.155 40192 172.30.1.125 23    Tel
 729 24.630212  TELNET   172.30.1.125 23    172.30.1.155 40192 Tel
 730 24.630413  TELNET   172.30.1.155 40192 172.30.1.125 23    Tel
 733 24.643413  TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...[Malformed Packet]

▶ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

Socket

Client	Server
172.30.1.155	172.30.1.125
40192	23

The socket used for the Telnet session

Transport Layer

The Transmission Control Protocol (TCP)

Continuing communications on an established connection

o The Sliding Window

Used for flow control - allows sending additional segments before an acknowledgement is received based on recipients buffer size

o Flow Control (cumulative acknowledgment)

Recipient tells sender the size of its input buffer and sends acknowledgements (ACKs) when data has been received. Sequence numbers are used to detect missing segments.

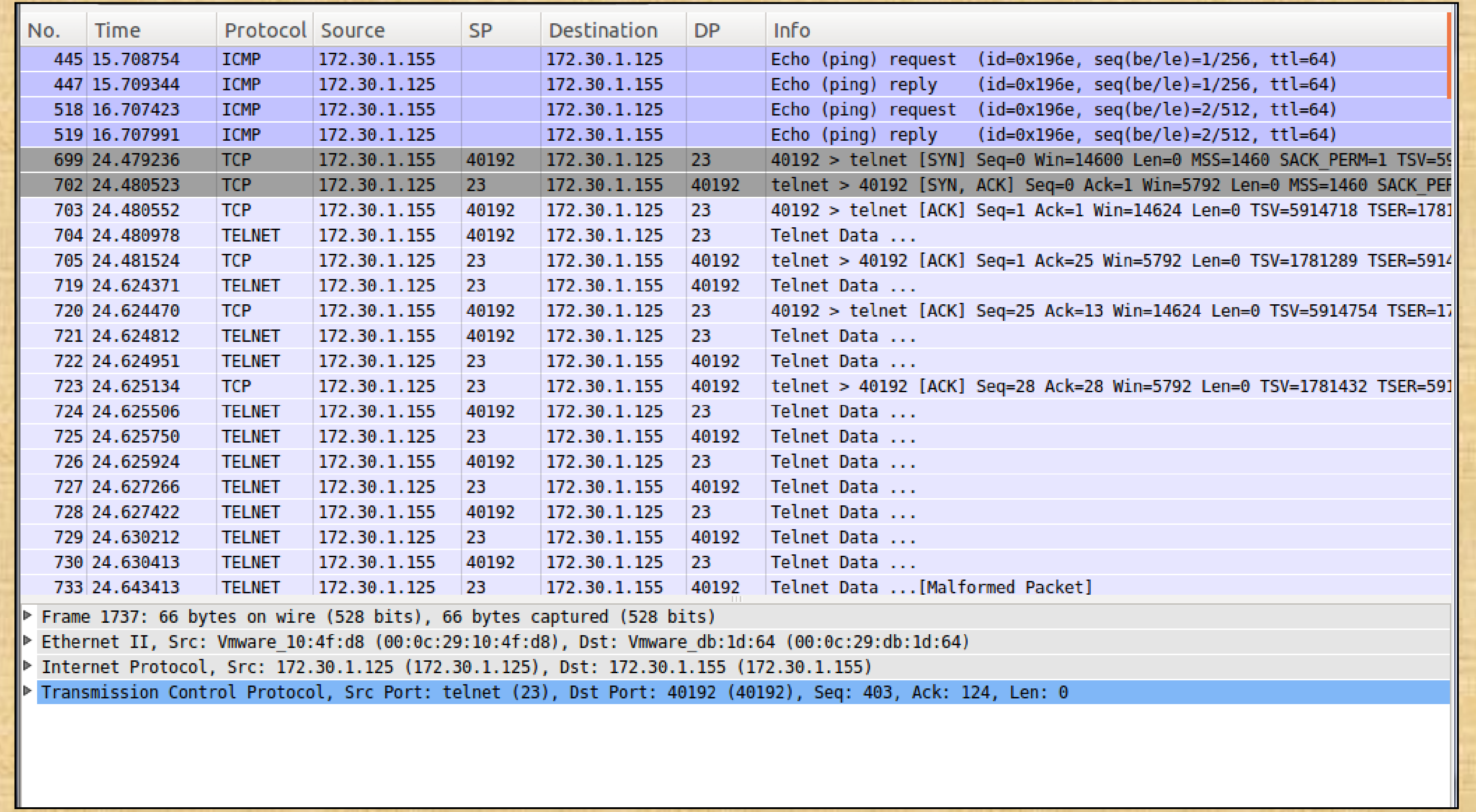
o The SACK option

Selective acknowledgement so only the dropped segments need to be retransmitted.

o The RST Flag

Used to terminate a connection when an abnormal situation happens

Example telnet session

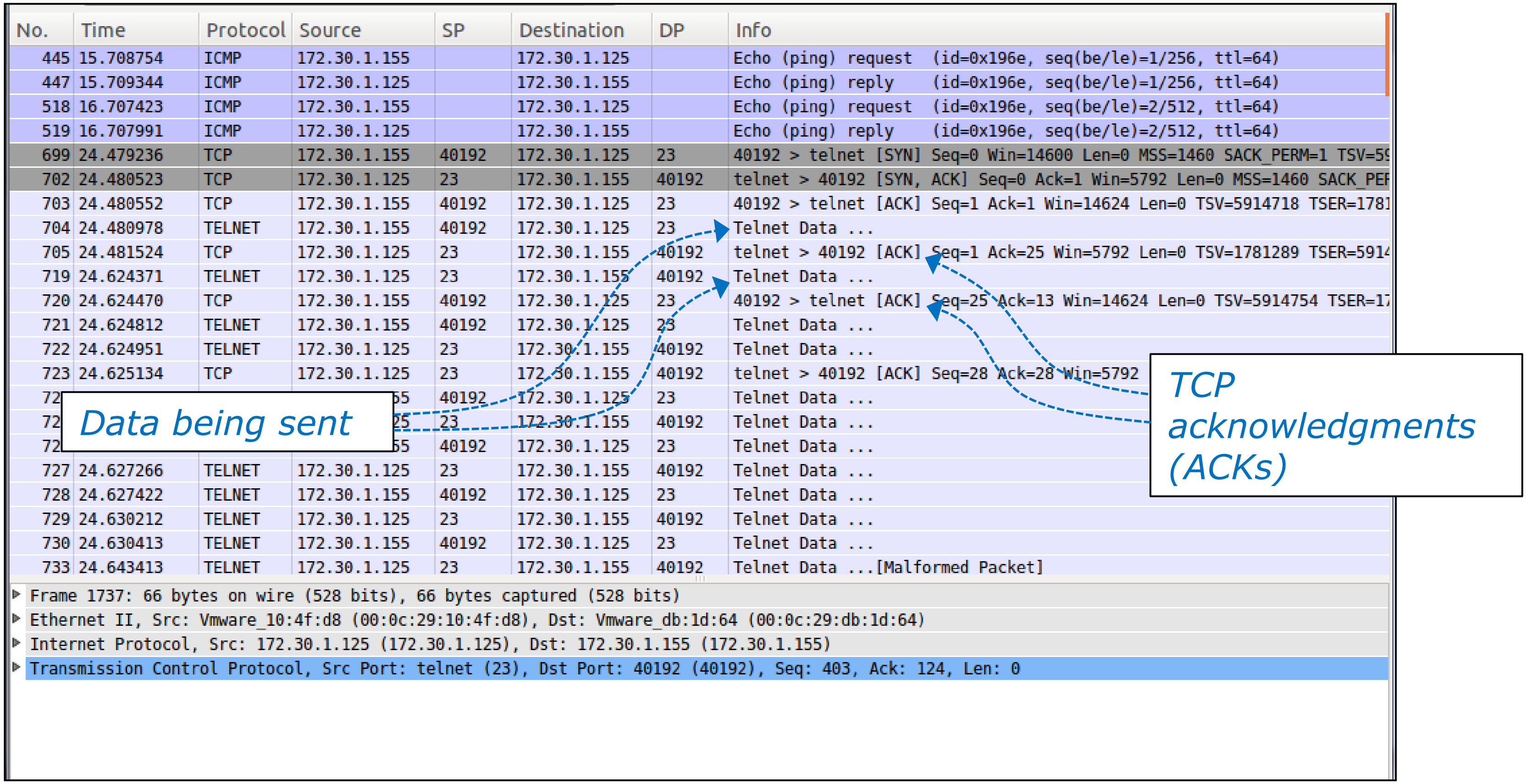


No.	Time	Protocol	Source	SP	Destination	DP	Info
445	15.708754	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=1/256, ttl=64)
447	15.709344	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=1/256, ttl=64)
518	16.707423	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=2/512, ttl=64)
519	16.707991	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=2/512, ttl=64)
699	24.479236	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
702	24.480523	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
703	24.480552	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
704	24.480978	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
705	24.481524	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
719	24.624371	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
720	24.624470	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=25 Ack=13 Win=14624 Len=0 TSV=5914754 TSER=17
721	24.624812	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
722	24.624951	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
723	24.625134	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=28 Ack=28 Win=5792 Len=0 TSV=1781432 TSER=591
724	24.625506	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
725	24.625750	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
726	24.625924	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
727	24.627266	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
728	24.627422	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
729	24.630212	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
730	24.630413	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
733	24.643413	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...[Malformed Packet]

```
▶ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

Point out data being sent and the acknowledgments

Example telnet session



No.	Time	Protocol	Source	SP	Destination	DP	Info
445	15.708754	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=1/256, ttl=64)
447	15.709344	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=1/256, ttl=64)
518	16.707423	ICMP	172.30.1.155		172.30.1.125		Echo (ping) request (id=0x196e, seq(be/le)=2/512, ttl=64)
519	16.707991	ICMP	172.30.1.125		172.30.1.155		Echo (ping) reply (id=0x196e, seq(be/le)=2/512, ttl=64)
699	24.479236	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSV=59
702	24.480523	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
703	24.480552	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSV=5914718 TSER=1781
704	24.480978	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
705	24.481524	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=1 Ack=25 Win=5792 Len=0 TSV=1781289 TSER=5914
719	24.624371	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
720	24.624470	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=25 Ack=13 Win=14624 Len=0 TSV=5914754 TSER=17
721	24.624812	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
722	24.624951	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
723	24.625134	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=28 Ack=28 Win=5792
72			55	40192	172.30.1.125	23	Telnet Data ...
72			25	23	172.30.1.155	40192	Telnet Data ...
72			55	40192	172.30.1.125	23	Telnet Data ...
727	24.627266	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
728	24.627422	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
729	24.630212	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
730	24.630413	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
733	24.643413	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...[Malformed Packet]

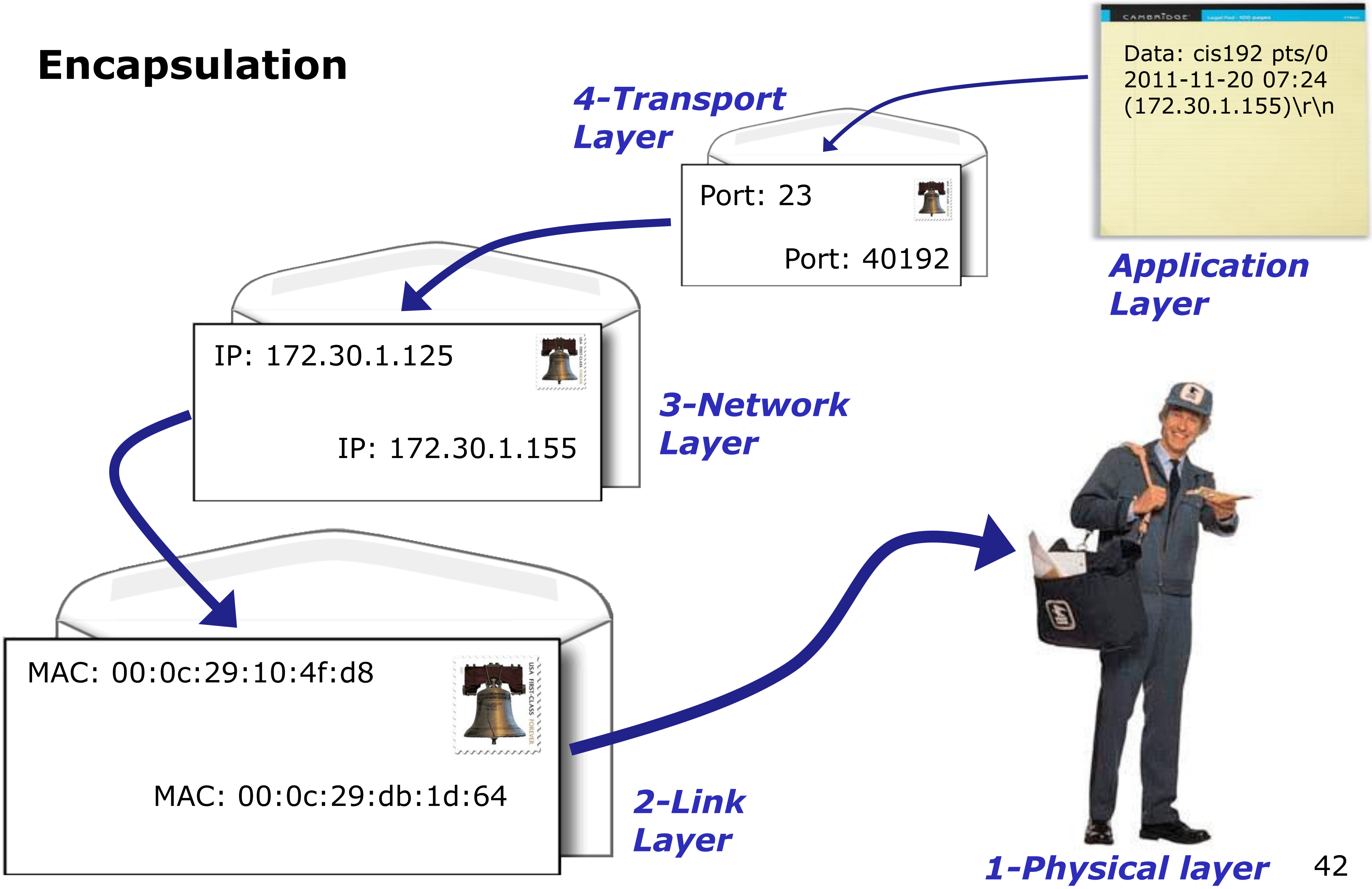
```
▶ Frame 1737: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 403, Ack: 124, Len: 0
```

Data being sent

TCP acknowledgments (ACKs)

Observing TCP acknowledgements sent as data is received

Encapsulation



Data: cis192 pts/0 2011-11-20 07:24 (172.30.1.155)\r\n

Application Layer

4-Transport Layer

Port: 23

Port: 40192

3-Network Layer

IP: 172.30.1.125

IP: 172.30.1.155

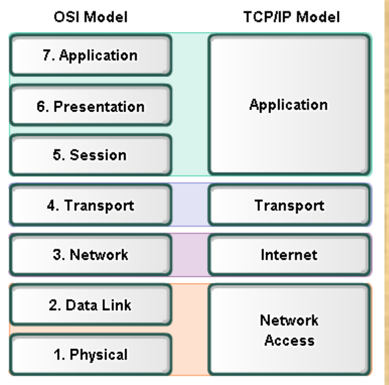
2-Link Layer

MAC: 00:0c:29:10:4f:d8

MAC: 00:0c:29:db:1d:64

1-Physical layer

Example telnet session



OSI Model

TCP/IP Model

7. Application

6. Presentation

5. Session

Application

4. Transport

Transport

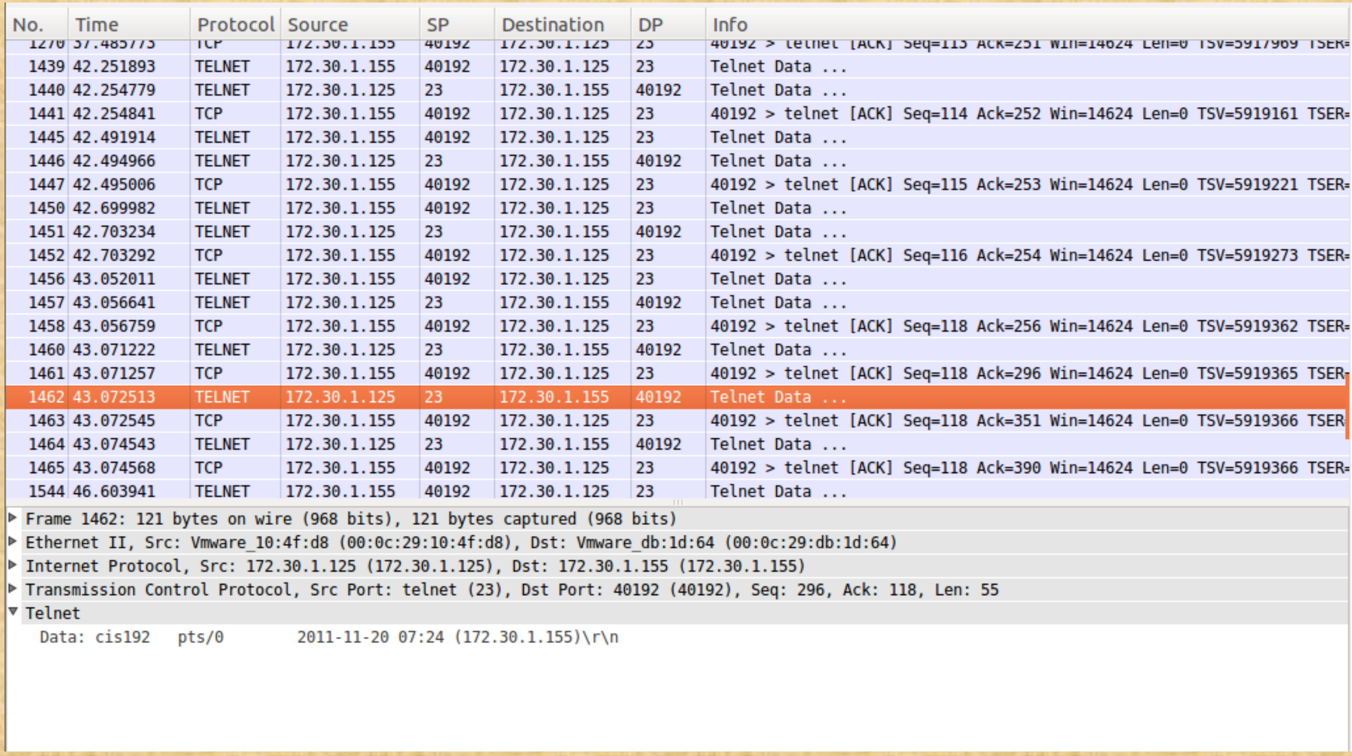
3. Network

Internet

2. Data Link

1. Physical

Network Access

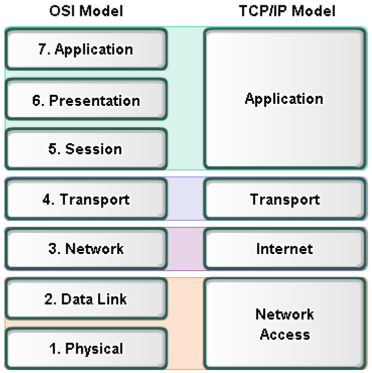


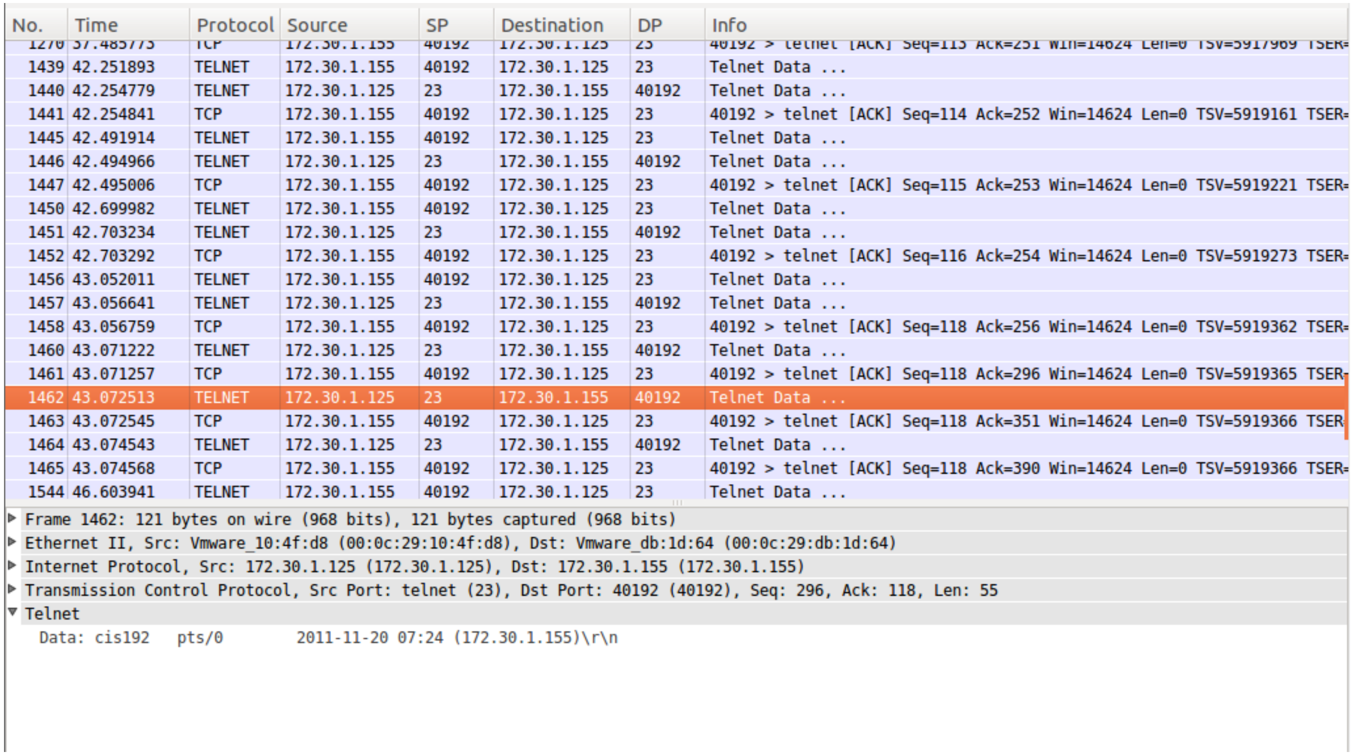
No.	Time	Protocol	Source	SP	Destination	DP	Info
1270	37.485773	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=113 Ack=251 Win=14624 Len=0 TSV=5917969 TSER=
1439	42.251893	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1440	42.254779	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1441	42.254841	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=114 Ack=252 Win=14624 Len=0 TSV=5919161 TSER=
1445	42.491914	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1446	42.494966	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1447	42.495006	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=115 Ack=253 Win=14624 Len=0 TSV=5919221 TSER=
1450	42.699982	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1451	42.703234	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1452	42.703292	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=116 Ack=254 Win=14624 Len=0 TSV=5919273 TSER=
1456	43.052011	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1457	43.056641	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1458	43.056759	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=256 Win=14624 Len=0 TSV=5919362 TSER=
1460	43.071222	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1461	43.071257	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=296 Win=14624 Len=0 TSV=5919365 TSER
1462	43.072513	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1463	43.072545	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=351 Win=14624 Len=0 TSV=5919366 TSER
1464	43.074543	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1465	43.074568	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=390 Win=14624 Len=0 TSV=5919366 TSER=
1544	46.603941	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...

```
▶ Frame 1462: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 296, Ack: 118, Len: 55
▼ Telnet
    Data: cis192    pts/0        2011-11-20 07:24 (172.30.1.155)\r\n
```

Point out the layers 2-5 in the decoded packet

Example telnet session





```
No.  Time      Protocol Source       SP    Destination  DP    Info
1270 37.485773 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=113 Ack=251 Win=14624 Len=0 TSV=5917969 TSER=
1439 42.251893 TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...
1440 42.254779 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1441 42.254841 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=114 Ack=252 Win=14624 Len=0 TSV=5919161 TSER=
1445 42.491914 TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...
1446 42.494966 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1447 42.495006 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=115 Ack=253 Win=14624 Len=0 TSV=5919221 TSER=
1450 42.699982 TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...
1451 42.703234 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1452 42.703292 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=116 Ack=254 Win=14624 Len=0 TSV=5919273 TSER=
1456 43.052011 TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...
1457 43.056641 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1458 43.056759 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=118 Ack=256 Win=14624 Len=0 TSV=5919362 TSER=
1460 43.071222 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1461 43.071257 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=118 Ack=296 Win=14624 Len=0 TSV=5919365 TSER
1462 43.072513 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1463 43.072545 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=118 Ack=351 Win=14624 Len=0 TSV=5919366 TSER
1464 43.074543 TELNET   172.30.1.125 23    172.30.1.155 40192 Telnet Data ...
1465 43.074568 TCP      172.30.1.155 40192 172.30.1.125 23    40192 > telnet [ACK] Seq=118 Ack=390 Win=14624 Len=0 TSV=5919366 TSER=
1544 46.603941 TELNET   172.30.1.155 40192 172.30.1.125 23    Telnet Data ...

▶ Frame 1462: 121 bytes on wire (968 bits), 121 bytes captured (968 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 296, Ack: 118, Len: 55
▼ Telnet
    Data: cis192    pts/0        2011-11-20 07:24 (172.30.1.155)\r\n
```

Data Link
Layer 2
(MAC addresses)

Internet
Layer 3
(IP addresses)

Network
Layer 4
(ports)

Application
Layer 5
(application data)

Observing the network layers of encapsulation in the Telnet session

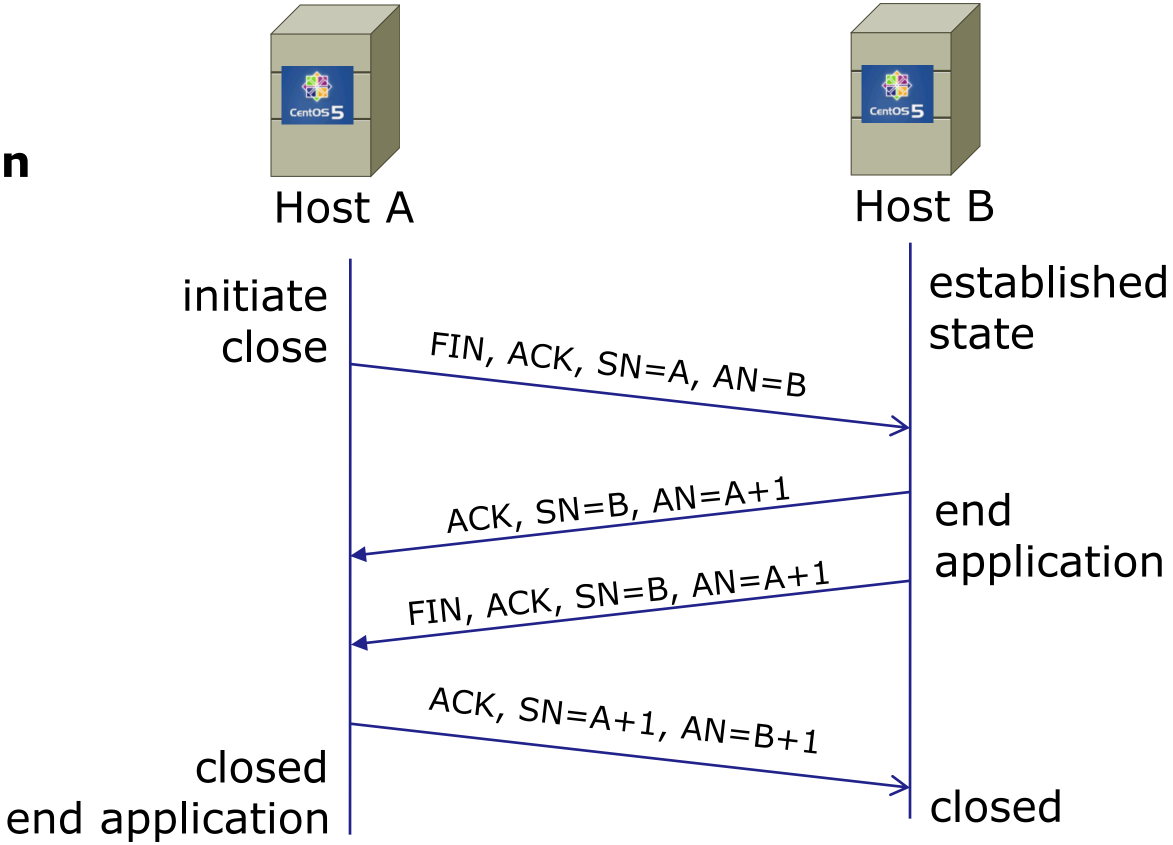
Transport Layer

Closing a TCP Connection

Four-Way Handshake

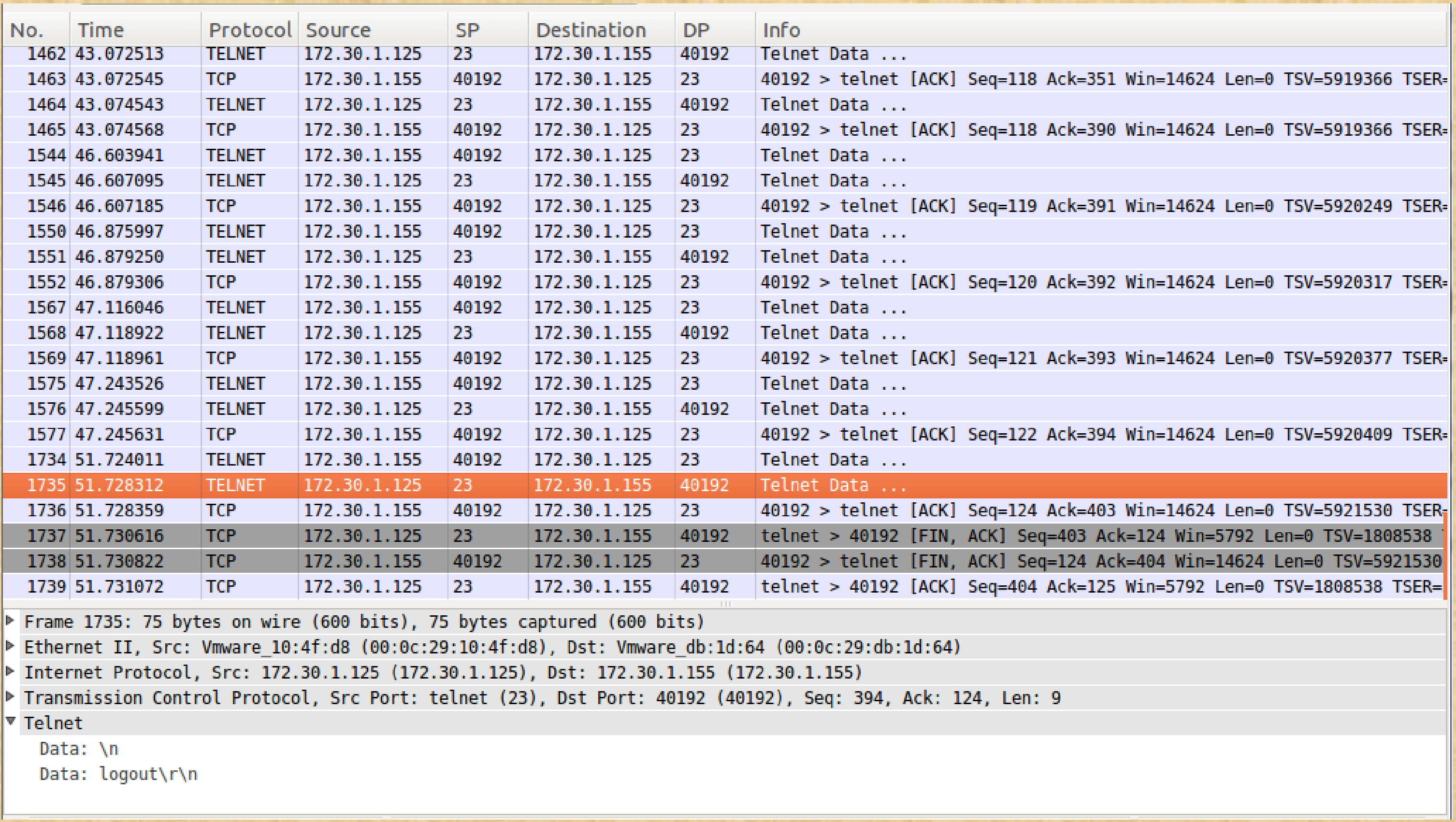
1. FIN, ACK
2. ACK
3. FIN, ACK
4. ACK

Closing with a shorter three-way handshake is also possible, where the Host A sends a FIN and Host B replies with a FIN & ACK (combining two steps into one) and Host A replies with an ACK.



AN=Acknowledgment Number
SN=Sequence Number
ACK=ACK flag set
FIN=FIN flag set

Example telnet session

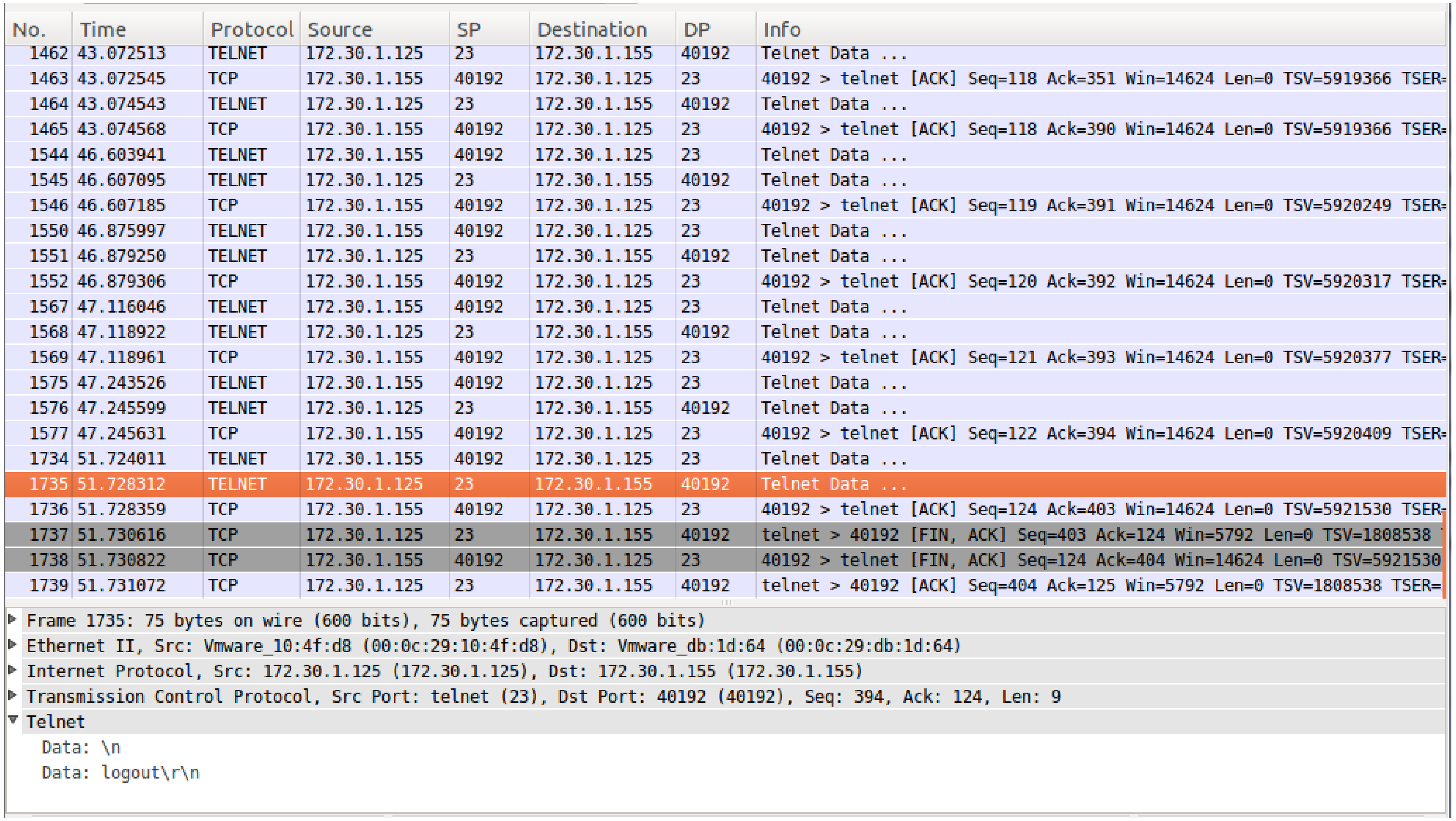


No.	Time	Protocol	Source	SP	Destination	DP	Info
1462	43.072513	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1463	43.072545	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=351 Win=14624 Len=0 TSV=5919366 TSER=
1464	43.074543	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1465	43.074568	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=390 Win=14624 Len=0 TSV=5919366 TSER=
1544	46.603941	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1545	46.607095	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1546	46.607185	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=119 Ack=391 Win=14624 Len=0 TSV=5920249 TSER=
1550	46.875997	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1551	46.879250	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1552	46.879306	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=120 Ack=392 Win=14624 Len=0 TSV=5920317 TSER=
1567	47.116046	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1568	47.118922	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1569	47.118961	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=121 Ack=393 Win=14624 Len=0 TSV=5920377 TSER=
1575	47.243526	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1576	47.245599	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1577	47.245631	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=122 Ack=394 Win=14624 Len=0 TSV=5920409 TSER=
1734	51.724011	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1735	51.728312	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1736	51.728359	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=124 Ack=403 Win=14624 Len=0 TSV=5921530 TSER=
1737	51.730616	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [FIN, ACK] Seq=403 Ack=124 Win=5792 Len=0 TSV=1808538
1738	51.730822	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [FIN, ACK] Seq=124 Ack=404 Win=14624 Len=0 TSV=5921530
1739	51.731072	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=404 Ack=125 Win=5792 Len=0 TSV=1808538 TSER=

```
▶ Frame 1735: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 394, Ack: 124, Len: 9
▼ Telnet
    Data: \n
    Data: logout\r\n
```

Point to the start and end of the handshake closing the connection

Example telnet session



No.	Time	Protocol	Source	SP	Destination	DP	Info
1462	43.072513	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1463	43.072545	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=351 Win=14624 Len=0 TSV=5919366 TSER=
1464	43.074543	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1465	43.074568	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=118 Ack=390 Win=14624 Len=0 TSV=5919366 TSER=
1544	46.603941	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1545	46.607095	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1546	46.607185	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=119 Ack=391 Win=14624 Len=0 TSV=5920249 TSER=
1550	46.875997	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1551	46.879250	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1552	46.879306	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=120 Ack=392 Win=14624 Len=0 TSV=5920317 TSER=
1567	47.116046	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1568	47.118922	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1569	47.118961	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=121 Ack=393 Win=14624 Len=0 TSV=5920377 TSER=
1575	47.243526	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1576	47.245599	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1577	47.245631	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=122 Ack=394 Win=14624 Len=0 TSV=5920409 TSER=
1734	51.724011	TELNET	172.30.1.155	40192	172.30.1.125	23	Telnet Data ...
1735	51.728312	TELNET	172.30.1.125	23	172.30.1.155	40192	Telnet Data ...
1736	51.728359	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [ACK] Seq=124 Ack=403 Win=14624 Len=0 TSV=5921530 TSER
1737	51.730616	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [FIN, ACK] Seq=403 Ack=124 Win=5792 Len=0 TSV=1808538
1738	51.730822	TCP	172.30.1.155	40192	172.30.1.125	23	40192 > telnet [FIN, ACK] Seq=124 Ack=404 Win=14624 Len=0 TSV=5921530
1739	51.731072	TCP	172.30.1.125	23	172.30.1.155	40192	telnet > 40192 [ACK] Seq=404 Ack=125 Win=5792 Len=0 TSV=1808538 TSER=

```
▶ Frame 1735: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
▶ Ethernet II, Src: Vmware_10:4f:d8 (00:0c:29:10:4f:d8), Dst: Vmware_db:1d:64 (00:0c:29:db:1d:64)
▶ Internet Protocol, Src: 172.30.1.125 (172.30.1.125), Dst: 172.30.1.155 (172.30.1.155)
▶ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 40192 (40192), Seq: 394, Ack: 124, Len: 9
▼ Telnet
    Data: \n
    Data: logout\r\n
```

Handshake to close connection

Connection closed

Class Activity

Can you ping 172.20.192.182 ?

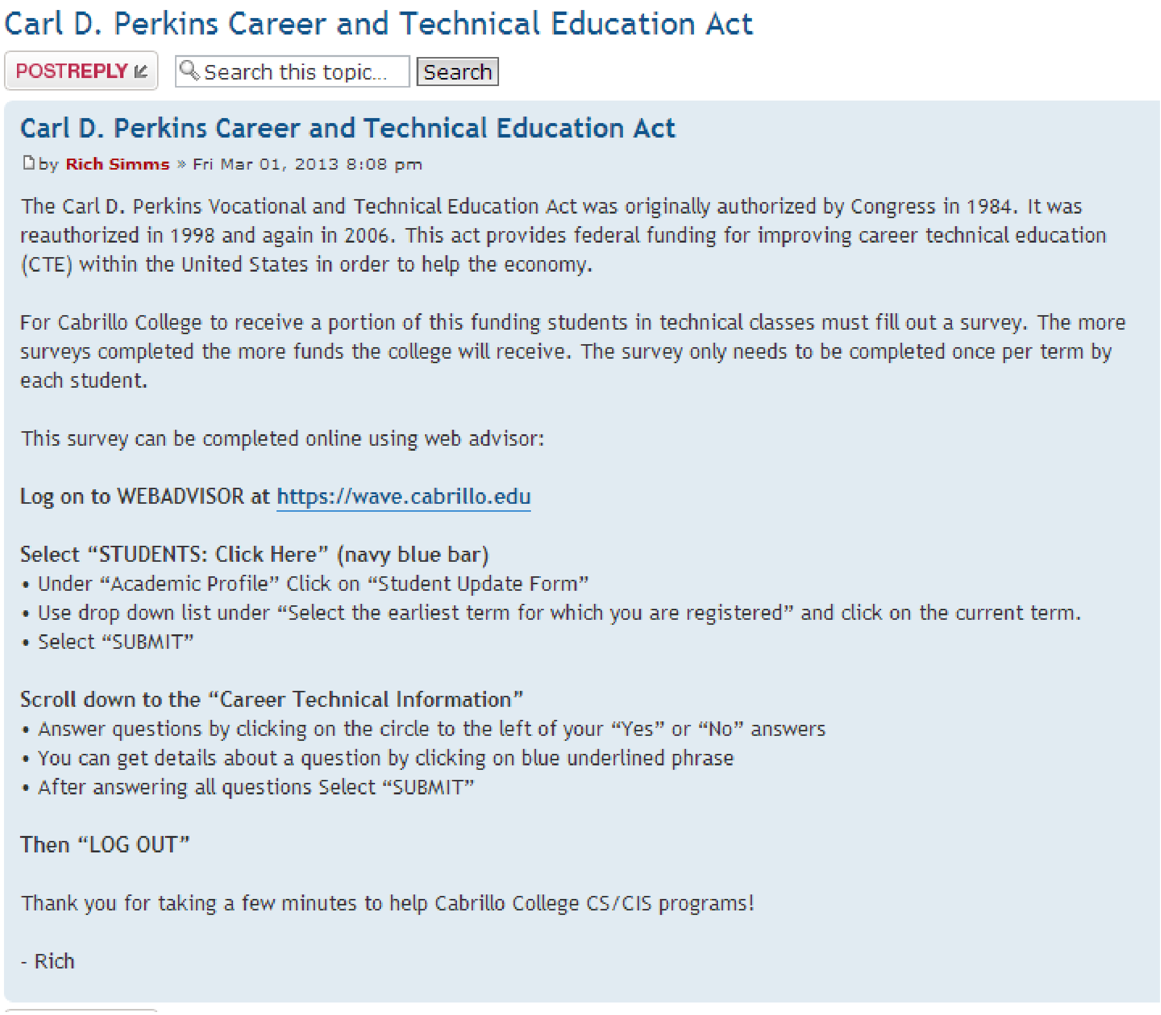
Can you log into ssh (as cis192) into 172.20.192.182 ?

Can you telnet (as cis192) to 172.20.192.182 ?

Housekeeping

- Test tonight (last part of class)
- Lab 4 due next week

Perkins/VTEA Survey



Carl D. Perkins Career and Technical Education Act

Carl D. Perkins Career and Technical Education Act

by **Rich Simms** » Fri Mar 01, 2013 8:08 pm

The Carl D. Perkins Vocational and Technical Education Act was originally authorized by Congress in 1984. It was reauthorized in 1998 and again in 2006. This act provides federal funding for improving career technical education (CTE) within the United States in order to help the economy.

For Cabrillo College to receive a portion of this funding students in technical classes must fill out a survey. The more surveys completed the more funds the college will receive. The survey only needs to be completed once per term by each student.

This survey can be completed online using web advisor:

Log on to WEBADVISOR at https://wave.cabrillo.edu

Select "STUDENTS: Click Here" (navy blue bar)
- Under "Academic Profile" Click on "Student Update Form"
- Use drop down list under "Select the earliest term for which you are registered" and click on the current term.
- Select "SUBMIT"

Scroll down to the "Career Technical Information"
- Answer questions by clicking on the circle to the left of your "Yes" or "No" answers
- You can get details about a question by clicking on blue underlined phrase
- After answering all questions Select "SUBMIT"

Then "LOG OUT"

Thank you for taking a few minutes to help Cabrillo College CS/CIS programs!

- Rich

http://oslab.cabrillo.edu/forum/viewtopic.php?f=63&t=1883

This is an important source of funding for Cabrillo College.

*Send me an email that you completed this survey for **3 points extra credit!***

Help with labs

Like some help with labs?

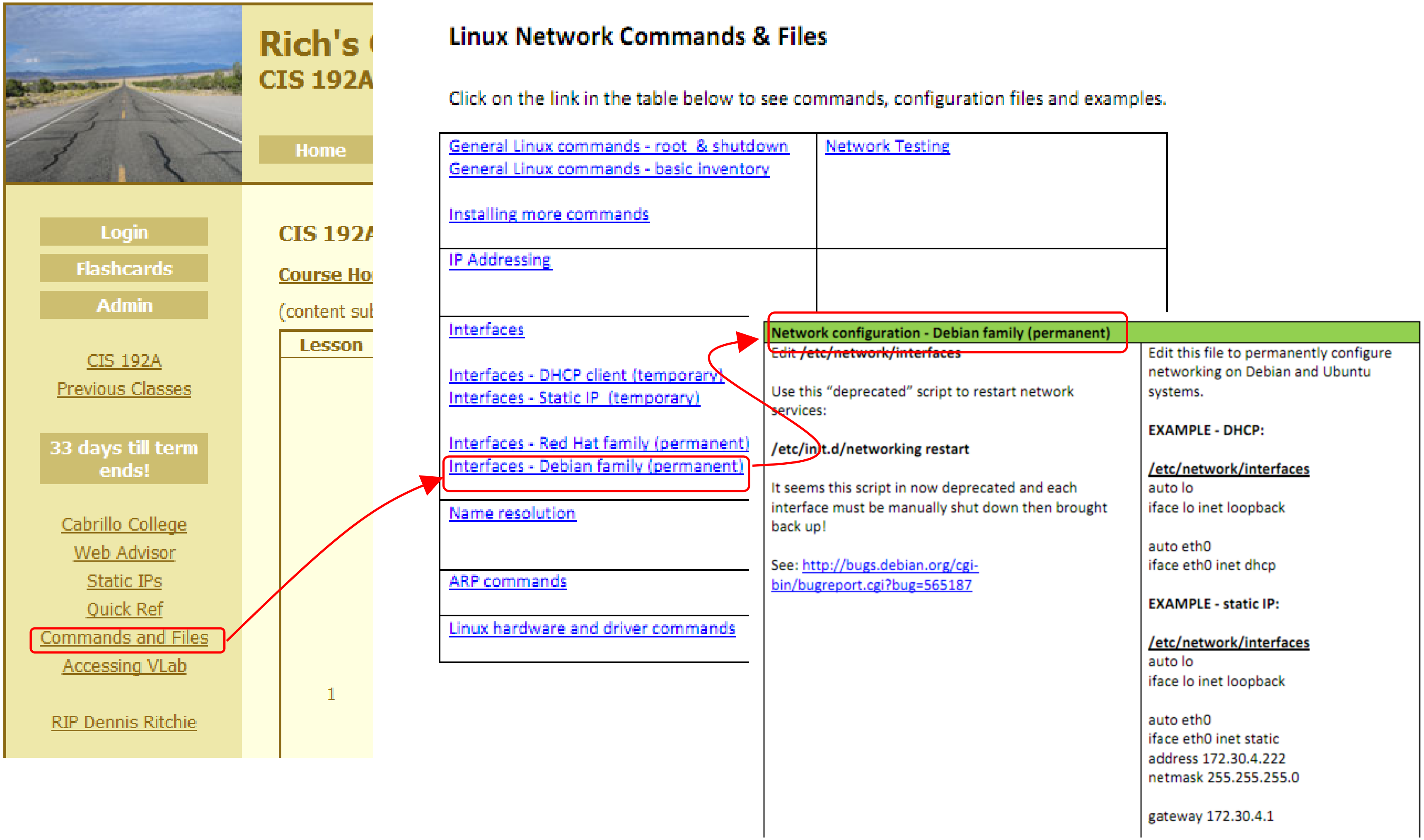
I'm in the CIS Lab Monday afternoons

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

or see me during office hours

or contact me to arrange another time online

Commands and Files
Quick Reference and Examples



Linux Network Commands & Files

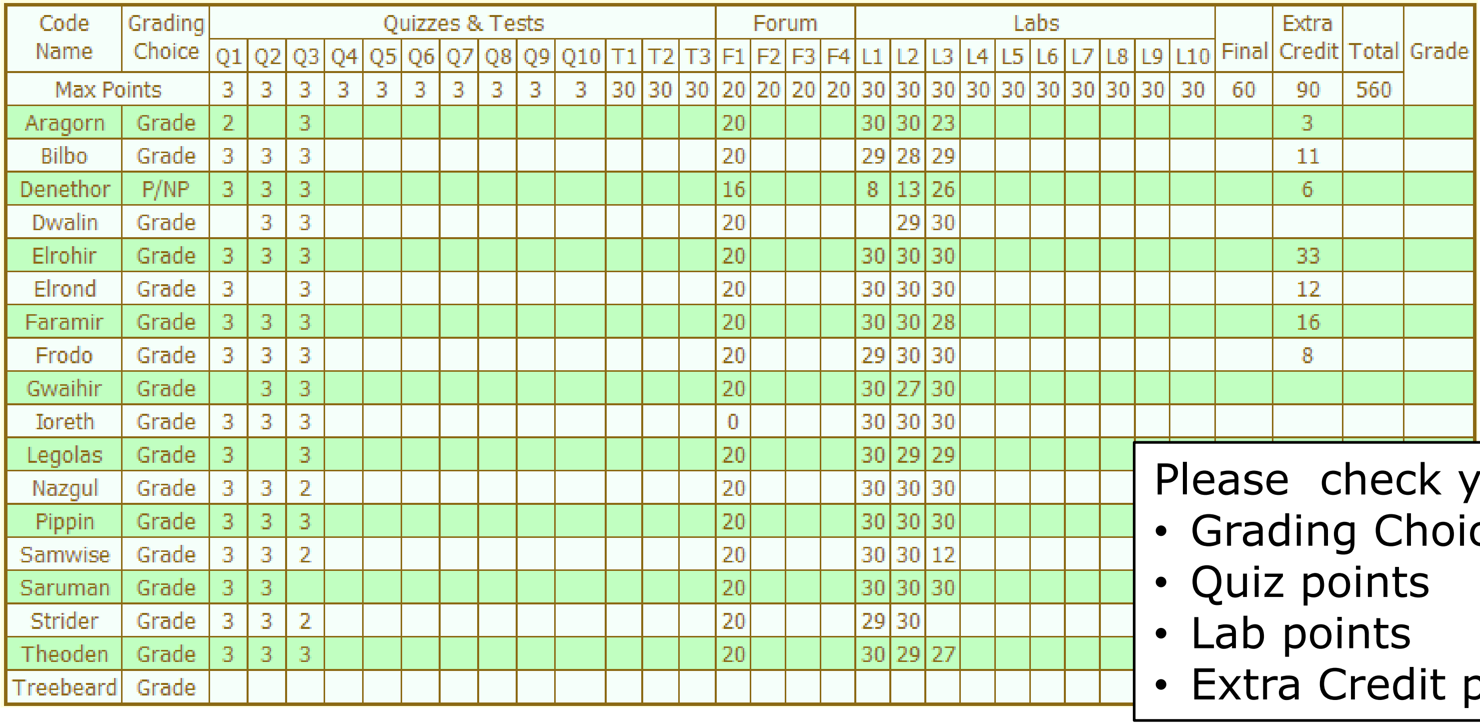
Click on the link in the table below to see commands, configuration files and examples.

General Linux commands - root & shutdown General Linux commands - basic inventory Installing more commands	Network Testing
IP Addressing	
Interfaces Interfaces - DHCP client (temporary) Interfaces - Static IP (temporary) Interfaces - Red Hat family (permanent) Interfaces - Debian family (permanent)	
Name resolution	
ARP commands	
Linux hardware and driver commands	

Network configuration - Debian family (permanent)	
Edit **/etc/network/interfaces** Use this "deprecated" script to restart network services: **/etc/init.d/networking restart** It seems this script in now deprecated and each interface must be manually shut down then brought back up! See: http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=565187	Edit this file to permanently configure networking on Debian and Ubuntu systems. **EXAMPLE - DHCP:** **/etc/network/interfaces** auto lo iface lo inet loopback auto eth0 iface eth0 inet dhcp **EXAMPLE - static IP:** **/etc/network/interfaces** auto lo iface lo inet loopback auto eth0 iface eth0 inet static address 172.30.4.222 netmask 255.255.255.0 gateway 172.30.4.1

Grades Web Page

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



Code Name	Grading Choice	Quizzes & Tests													Forum				Labs										Final	Extra Credit	Total	Grade
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	T1	T2	T3	F1	F2	F3	F4	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10				
Max Points		3	3	3	3	3	3	3	3	3	3	30	30	30	20	20	20	20	30	30	30	30	30	30	30	30	30	30	60	90	560	
Aragorn	Grade	2		3											20				30	30	23									3		
Bilbo	Grade	3	3	3											20				29	28	29									11		
Denethor	P/NP	3	3	3											16				8	13	26									6		
Dwalin	Grade		3	3											20					29	30											
Elrohir	Grade	3	3	3											20				30	30	30									33		
Elrond	Grade	3		3											20				30	30	30									12		
Faramir	Grade	3	3	3											20				30	30	28									16		
Frodo	Grade	3	3	3											20				29	30	30									8		
Gwaihir	Grade		3	3											20				30	27	30											
Ioreth	Grade	3	3	3											0				30	30	30											
Legolas	Grade	3		3											20				30	29	29											
Nazgul	Grade	3	3	2											20				30	30	30											
Pippin	Grade	3	3	3											20				30	30	30											
Samwise	Grade	3	3	2											20				30	30	12											
Saruman	Grade	3	3												20				30	30	30											
Strider	Grade	3	3	2											20				29	30												
Theoden	Grade	3	3	3											20				30	29	27											
Treebeard	Grade																															

Please check your:
- Grading Choice
- Quiz points
- Lab points
- Extra Credit points

Don't know you secret LOR code name?

… then email me your student survey to get it!

Reviewing graded work

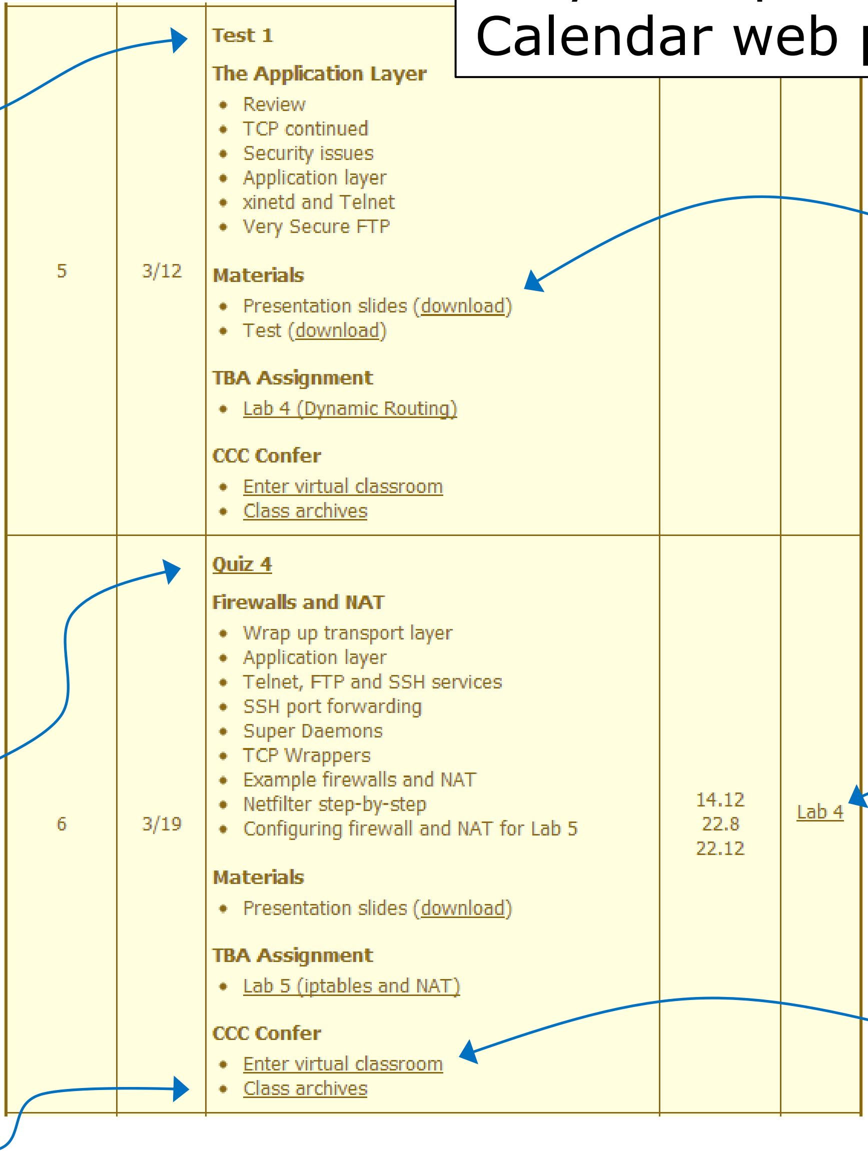
Review graded work in your home directories

```
[simben192@opus ~]$ ls -l
total 60
-rw-r-----. 1 simben192 cis192  3012 Feb 13 16:10 lab01
-r--------. 1 simben192 staff   3251 Feb 20 11:38 lab01.graded
-rw-r-----. 1 simben192 cis192  5245 Feb 23 11:21 lab02
-r--------. 1 simben192 staff   5491 Feb 27 10:17 lab02.graded
-rw-r-----. 1 simben192 cis192 10973 Mar  3 14:28 lab03
-r--------. 1 simben192 staff  11456 Mar 10 19:14 lab03.graded
-rwxr-x---. 1 simben192 cis192   395 Feb 12 09:51 monitor
-rw-r-----. 1 simben192 cis192  6757 Feb 23 10:27 netcap
```

See example correct answers in the answers directory:

```
[simben192@oslab ~]$ ls /home/cis192/answers/
lab01  lab02  lab03  quiz01  quiz02  quiz03
```

Stay on top of deliverables with the Calendar web page



5	3/12	**Test 1** **The Application Layer** • Review • TCP continued • Security issues • Application layer • xinetd and Telnet • Very Secure FTP **Materials** • Presentation slides (download) • Test (download) **TBA Assignment** • Lab 4 (Dynamic Routing) **CCC Confer** • Enter virtual classroom • Class archives		
6	3/19	**Quiz 4** **Firewalls and NAT** • Wrap up transport layer • Application layer • Telnet, FTP and SSH services • SSH port forwarding • Super Daemons • TCP Wrappers • Example firewalls and NAT • Netfilter step-by-step • Configuring firewall and NAT for Lab 5 **Materials** • Presentation slides (download) **TBA Assignment** • Lab 5 (iptables and NAT) **CCC Confer** • Enter virtual classroom • Class archives	14.12 22.8 22.12	Lab 4

Test tonight

Download the Lesson slides

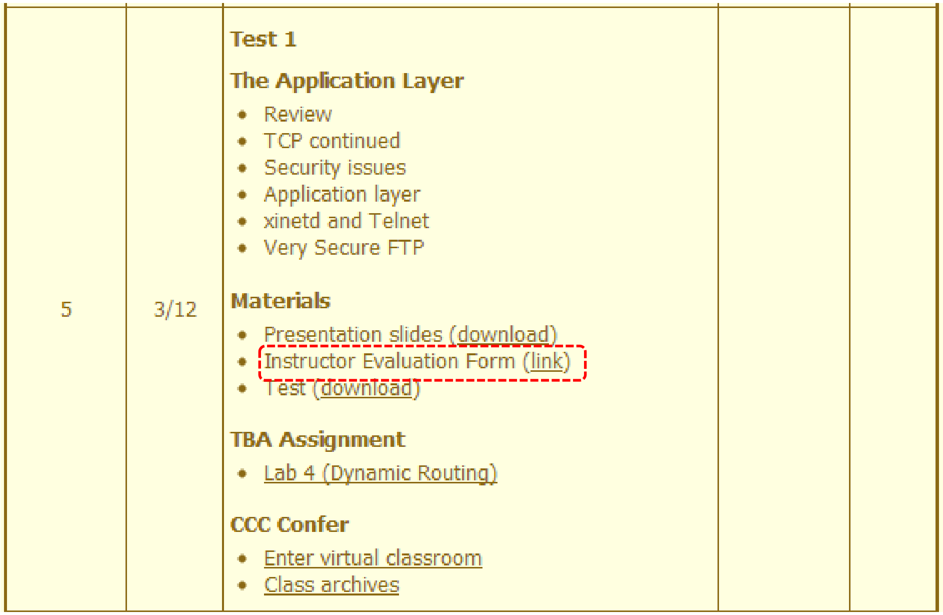
First minute quiz again next week

Lab 4 due 11:59PM March 19th

Watch the archived recording of the class at any time

Join the class in real time using CCC Confer

Evaluate Your Instructor Tonight



5	3/12	**Test 1** **The Application Layer** - Review - TCP continued - Security issues - Application layer - xinetd and Telnet - Very Secure FTP **Materials** - Presentation slides (download) - Instructor Evaluation Form (link) - Test (download) **TBA Assignment** - Lab 4 (Dynamic Routing) **CCC Confer** - Enter virtual classroom - Class archives		

Please fill out the survey form using link on the website

or type this link into your browser

https://www.surveymonkey.com/s/RichSimms-CIS-192AB-79995

Tunable Kernel Parameters

Tunable kernel parameters

There are a large number of kernel parmeters than can be tuned to optimize and customize network operation.

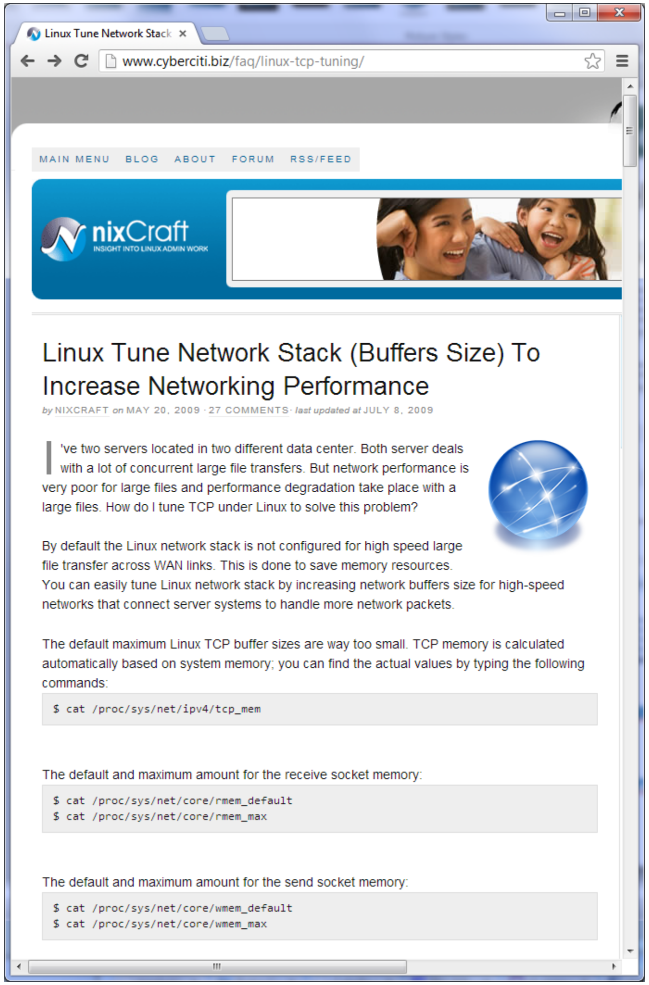
- Use **ls /proc/sys/net/ipv4/tcp*** to see TCP parameters
- Use **ls /proc/sys/net/ipv4/ip*** to see IP parameters
- Use **ls /proc/sys/net/ipv4/icmp*** to see IP parameters
- Use **ls /proc/sys/net/ipv4/conf/eth0/*** to see interface configuration parameters on eth0

- Use **ls -R /proc/sys/net/** to see all network parameters for ipv4 and ipv6

Tunable kernel parameters

Why tune?

- Optimize performance
  - Example: http://www.cyberciti.biz/faq/linux-tcp-tuning/
- Configure network stack
  - **/proc/sys/net/ipv4/ip_forward** was used in Lab 3 to control IP packet forwarding.
  - **/proc/sys/net/ipv4/conf/eth0/rp_filter** was used in Lab 4 to configure the reverse-path filter to disable spoof protection.


Linux Tune Network Stack
www.cyberciti.biz/faq/linux-tcp-tuning/
MAIN MENU
BLOG
ABOUT
FORUM
RSS/FEED
nixCraft
INSIGHT INTO LINUX ADMIN WORK

Linux Tune Network Stack (Buffers Size) To Increase Networking Performance

by NIXCRAFT *on* MAY 20, 2009 · 27 COMMENTS· *last updated at* JULY 8, 2009

I've two servers located in two different data center. Both server deals with a lot of concurrent large file transfers. But network performance is very poor for large files and performance degradation take place with a large files. How do I tune TCP under Linux to solve this problem?

By default the Linux network stack is not configured for high speed large file transfer across WAN links. This is done to save memory resources. You can easily tune Linux network stack by increasing network buffers size for high-speed networks that connect server systems to handle more network packets.

The default maximum Linux TCP buffer sizes are way too small. TCP memory is calculated automatically based on system memory; you can find the actual values by typing the following commands:

```
$ cat /proc/sys/net/ipv4/tcp_mem
```

The default and maximum amount for the receive socket memory:

```
$ cat /proc/sys/net/core/rmem_default
$ cat /proc/sys/net/core/rmem_max
```

The default and maximum amount for the send socket memory:

```
$ cat /proc/sys/net/core/wmem_default
$ cat /proc/sys/net/core/wmem_max
```

Tunable kernel parameters

Examples:

/proc/sys/net/ipv4/

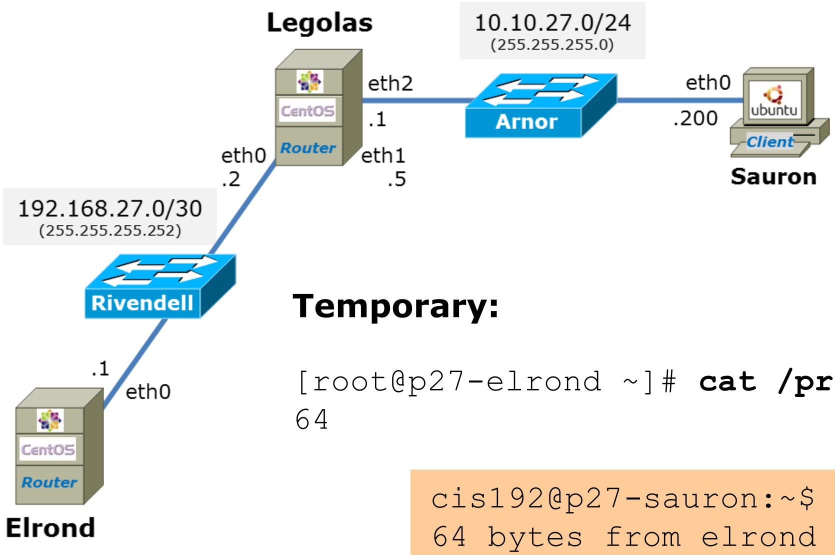
tcp_fin_timeout *how long to keep in FIN-WAIT-2 state*
tcp_keepalive_time *how long to keep an unused connection alive*
tcp_sack *enable/disable selective acknowledgments*
tcp_timestamps *enable RFC 1323 definition for round-trip measurement*
tcp_window_scaling *enable RFC 1323 window scaling*
tcp_retries1 *how many times to retry before reporting an error*
tcp_retries2 *how many times to retry before killing connection*
tcp_syn_retries *how many times to retransmit the SYN, ACK reply*

ip_forward *enable/disable selective acknowledgments*
ip_default_ttl *starting number for TTL*

icmp_echo_ignore_broadcasts *enable/disable responding to broadcast pings*

conf/eth0/rp_filter *enable/disable reverse-path filter*

Setting kernel parameters



Temporarily changing the default TTL value

Temporary:

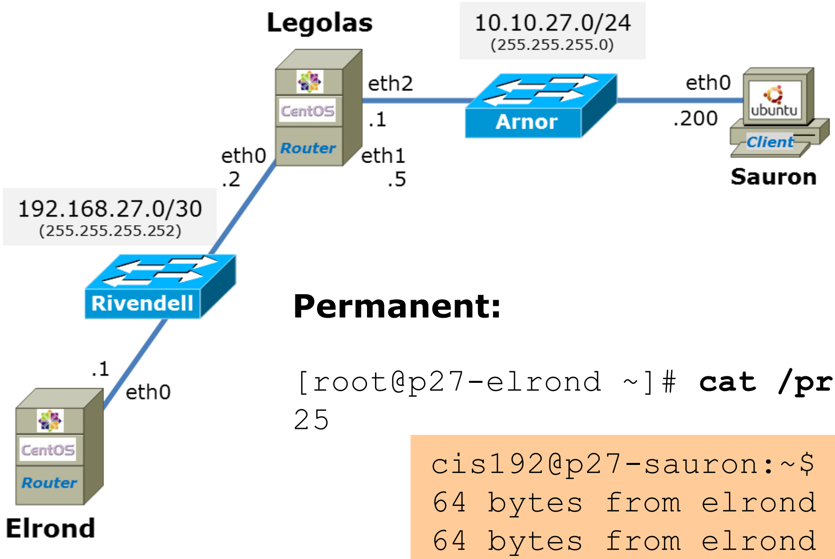
```
[root@p27-elrond ~]# cat /proc/sys/net/ipv4/ip_default_ttl
64
```

```
cis192@p27-sauron:~$ ping elrond -c2 | grep ttl
64 bytes from elrond (192.168.27.1): icmp_req=1 ttl=63 time=0.457 ms
64 bytes from elrond (192.168.27.1): icmp_req=2 ttl=63 time=0.567 ms
```

```
[root@p27-elrond ~]# echo 25 > /proc/sys/net/ipv4/ip_default_ttl
```

```
cis192@p27-sauron:~$ ping elrond -c2 | grep ttl
64 bytes from elrond (192.168.27.1): icmp_req=1 ttl=24 time=0.314 ms
64 bytes from elrond (192.168.27.1): icmp_req=2 ttl=24 time=0.453 ms
```

Setting kernel parameters



Permanently changing the default TTL value

Permanent:

```
[root@p27-elrond ~]# cat /proc/sys/net/ipv4/ip_default_ttl
25
```

```
cis192@p27-sauron:~$ ping elrond -c2 | grep ttl
64 bytes from elrond (192.168.27.1): icmp_req=1 ttl=24 time=0.314 ms
64 bytes from elrond (192.168.27.1): icmp_req=2 ttl=24 time=0.453 ms
```

Edit /etc/sysctl.conf add the line:

```
net.ipv4.ip_default_ttl = 90
```

```
[root@p27-elrond ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.ip_default_ttl = 90
net.ipv4.conf.default.rp_filter = 0
```

< snipped >

```
cis192@p27-sauron:~$ ping elrond -c2 | grep ttl
64 bytes from elrond (192.168.27.1): icmp_req=1 ttl=89 time=0.400 ms
64 bytes from elrond (192.168.27.1): icmp_req=2 ttl=89 time=0.520 ms
```

Activity

On Celebrian:

1) Examine all the kernel IP parameters using:

    head /proc/sys/net/ipv4/ip*

    Locate *ip_default_ttl* and *ip_forward* in the output

2) Look at the kernel parameters in /etc/sysctl.conf using:

    grep net.ipv4 /etc/sysctl.conf

3) Ping Celebrian from Frodo and observe the TTL values

4) Set *ip_default_ttl* to 130 with:

    echo 130 > /proc/sys/net/ipv4/ip_default_ttl

5) Ping Celebrian from Frodo and observe the TTL values

Security Issues

Transport Layer

Security Issues

Resource: *www.securityfocus.org*

- SYN Flooding

  " … Bombarding a system with, say, dozens of falsified connection requests a minute can seriously degrade its ability to give service to legitimate connection requests. This is why the attack is said to "deny service" to the system's users. …"

  Source: http://www.securityfocus.com/advisories/141

- Falsifying TCP Communications

  "… In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine. …"

  Source: http://www.securityfocus.com/infocus/1674

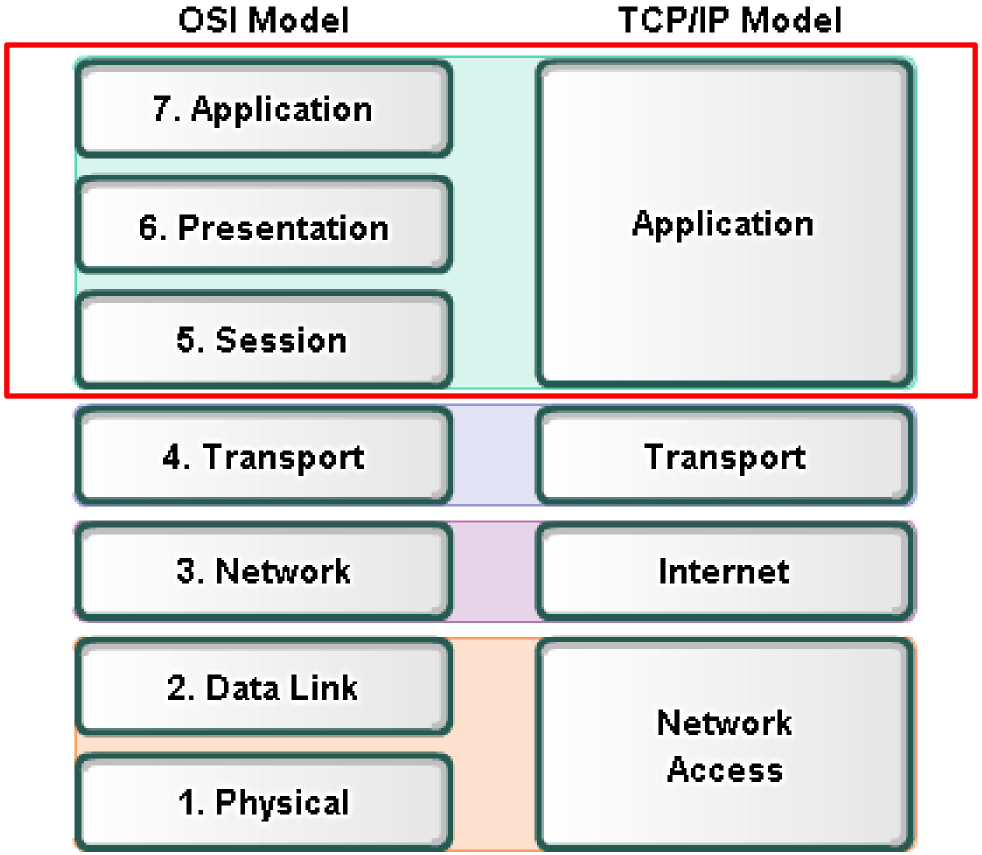
- Hijacking connections

  "… Another consequence, specific to TCP, is sequence number prediction, which can lead to session hijacking or host impersonating. This method builds on IP spoofing, since a session, albeit a false one, is built. …

  source: http://www.securityfocus.com/infocus/1674

Application Layer

Protocol and Reference Models



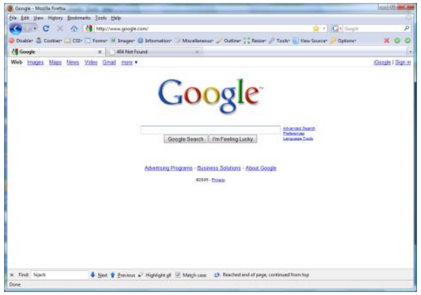
- The **Open Systems Interconnection (OSI)** model is the *most widely known internetwork reference model*.

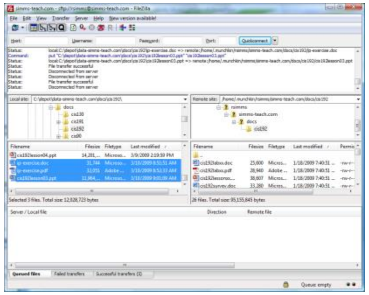
Application Layer

Applications

Examples:

- Web servers
- FTP servers
- SSH daemon
- Telnet server
- email


Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/
Web Images Maps News Video Gmail more ▾
iGoogle | Sign in
Google
Google Search I'm Feeling Lucky
Advanced Search Preferences Language Tools
Advertising Programs - Business Solutions - About Google
Done


simms-teach.com - sftp://rsimms@simms-teach.com - FileZilla
File Edit View Transfer Server Help New version available!
Host: Username: Password: Port: Quickconnect

```
Status:   local:C:\depot\data-simms-teach.com\docs\cis192\ip-exercise.doc => remote:/home/.munchkin/rsimms/simms-teach.com/docs/cis192/ip-exercise.doc
Command:  put "C:\depot\data-simms-teach.com\docs\cis192\cis192lesson03.ppt" "cis192lesson03.ppt"
Status:   local:C:\depot\data-simms-teach.com\docs\cis192\cis192lesson03.ppt => remote:/home/.munchkin/rsimms/simms-teach.com/docs/cis192/cis192lesson03.ppt
Status:   File transfer successful
Status:   Disconnected from server
Status:   Disconnected from server
Status:   File transfer successful
Status:   Disconnected from server
```

Local site: C:\depot\data-simms-teach.com\docs\cis192\

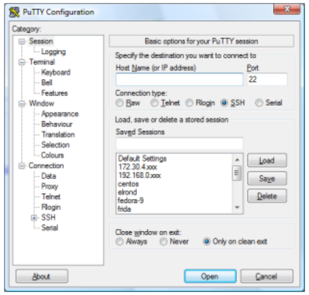
Remote site: /home/.munchkin/rsimms/simms-teach.com/docs/cis192

Filename	Filesize	Filetype	Last modified
cis192lesson04.ppt	14,201,...	Microso...	3/9/2009 2:19:59 PM
ip-exercise.doc	31,744	Microso...	3/10/2009 8:51:51 AM
ip-exercise.pdf	32,051	Adobe ...	3/10/2009 8:52:33 AM
cis192lesson03.ppt	11,984,...	Microso...	3/10/2009 9:01:09 AM

Selected 3 files. Total size: 12,028,723 bytes

Filename	Filesize	Filetype	Last modified	Permis
..				
cis192labxx.doc	25,600	Micros...	1/18/2009 7:40:51 ...	-rw-r--
cis192labxx.pdf	28,940	Adobe ...	1/18/2009 7:40:51 ...	-rw-r--
cis192lessonxx...	38,607	Micros...	1/18/2009 7:40:51 ...	-rw-r--
cis192survey.doc	33,280	Micros...	1/18/2009 7:40:51 ...	-rw-r--

26 files. Total size: 95,155,845 bytes



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

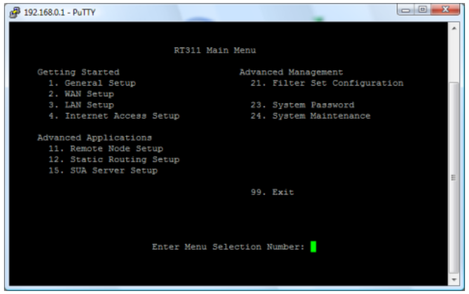
Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

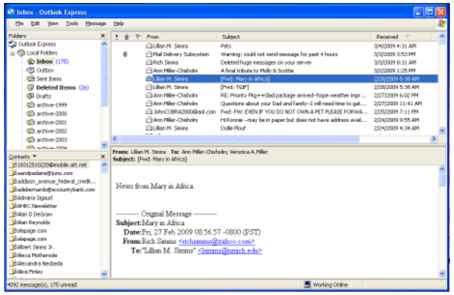
Saved Sessions

Default Settings
172.30.4.xxx
192.168.0.xxx
centos
elrond
fedora-9
frida

Close window on exit:
○ Always ○ Never ● Only on clean exit



```
                         RT311 Main Menu

   Getting Started                      Advanced Management
     1. General Setup                     21. Filter Set Configuration
     2. WAN Setup
     3. LAN Setup                         23. System Password
     4. Internet Access Setup             24. System Maintenance

   Advanced Applications
     11. Remote Node Setup
     12. Static Routing Setup
     15. SUA Server Setup

                                          99. Exit



                     Enter Menu Selection Number:
```



From	Subject	Received
Lillian M. Simms	Pets	3/4/2009 4:31 AM
Mail Delivery Subsystem	Warning: could not send message for past 4 hours	3/3/2009 3:53 PM
Rich Simms	Deleted huge messages on your server	3/3/2009 8:31 AM
Ann Miller-Chisholm	A final tribute to Molly & Scottie	3/2/2009 1:25 PM
Lillian M. Simms	[Fwd: Mary in Africa]	2/28/2009 5:38 AM
Lillian M. Simms	[Fwd: TGIF]	2/28/2009 5:38 AM
Ann Miller-Chisholm	RE: Priority Pkg++Glad package arrived--hope weather impr...	2/27/2009 6:02 PM
Ann Miller-Chisholm	Questions about your Dad and family--I will need time to gat...	2/27/2009 11:41 AM
JohnCOBRA2000@aol.com	Fwd: FW: EVEN IF YOU DO NOT OWN A PET PLEASE FORWA...	2/25/2009 7:11 PM
Ann Miller-Chisholm	Hi Ronnie --may be in paper but does not have address avail...	2/24/2009 9:55 AM
Lillian M. Simms	Dollie Plouf	2/24/2009 4:34 AM

From: Lillian M. Simms To: Ann Miller-Chisholm; Veronica A. Miller
Subject: [Fwd: Mary in Africa]

News from Mary in Africa.

--------- Original Message ---------
Subject: Mary in Africa
Date: Fri, 27 Feb 2009 08:56:57 -0800 (PST)
From: Rich Simms <richsimms@yahoo.com>
To: "Lillian M. Simms" <lsimms@umich.edu>

Application Layer

Responsibilities of Applications
Network connections, routing, and transfer of data are all taken care of by the lower layers of the protocol stack. What must applications do?

- Authenticate users
- Control access
- Log important information
- Format data (compress/encrypt)
- Provide whatever functionality is desired.

Application Layer

The Client-Server Model

Clients

Programs that are generally run on demand, and initiate the network connection to the server.

Examples: telnet, ftp, ssh, browsers, email clients.

Servers

Programs (services/daemons) that are constantly running in the background waiting for client connections.

- Services and Ports: */etc/services*
- Architecture:
  - Direct or iterative servers – listens to a particular port and directly responds to requests
  - Indirect or concurrent servers (e.g. super daemons) – listens to a particular port and then starts up another server program to process the request

Service Ports

Last week we talked about Layer 4 ports. Ports are used to direct requests to the appropriate service/application

< snipped >

```
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
telnet          23/udp
# 24 - private mail system
lmtp            24/tcp                          # LMTP Mail Delivery
lmtp            24/udp                          # LMTP Mail Delivery
smtp            25/tcp          mail
smtp            25/udp          mail
```

< snipped >

```
domain          53/tcp                          # name-domain server
domain          53/udp
whois++         63/tcp
whois++         63/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp          dhcpc           # BOOTP client
bootpc          68/udp          dhcpc
tftp            69/tcp
tftp            69/udp
finger          79/tcp
finger          79/udp
http            80/tcp          www www-http    # WorldWideWeb HTTP
http            80/udp          www www-http    # HyperText Transfer Protocol
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
```

< snipped >

Application Layer

The Super Daemons

- There are three primary super-daemons controlling server services.
- Super daemons spawn other daemons to handle specific client requests.

1. inetd - From early UNIX days, this was the primary daemon for handling tcp application services. It is being replaced by xinetd.

2. portmap - portmapper operates with Remote Procedure Call (RCP) applications.

3. xinetd - Extended Internet Services Daemon: used by modern distributions of Linux.

Application Layer

xinetd Daemon

Advantages

1. provides access control for TCP, UDP, and RPC services
2. Access limitations based on time
3. Extensive logging capabilities
4. Implements RFC 1413 username retrievals
5. Provides for hard reconfiguration
6. Provides numerous mechanisms to prevent denial of service attacks
7. Allows compiled in TCP_Wrappers through libwrap
8. Services may be bound to specific interfaces
9. Services may be forwarded (proxied) to another system
10. Supports ipv6

10 Steps for installing Network Service

(review)

Service Applications

Steps to installing network services

1. Install software package using **yum**, **rpm, apt-get** 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

Telnet Server Installation

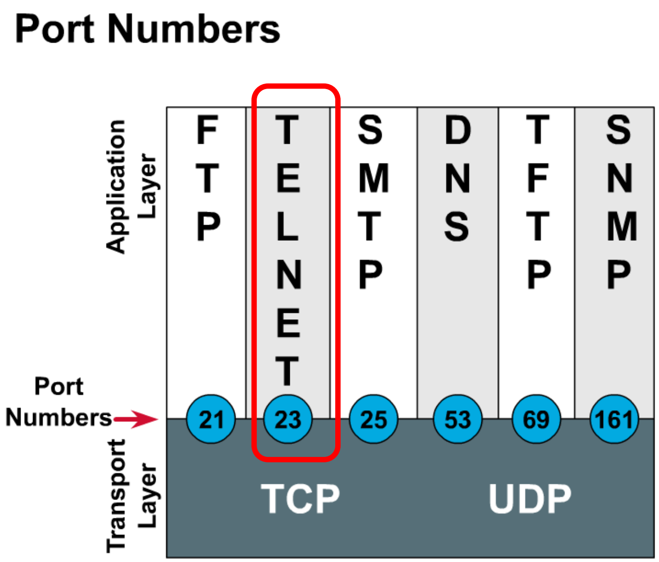
Installing and Configuring Telnet (Red Hat Family)

Telnet

- Provides command line interface to a remote host
- Client-server model
- Uses port 23
- Not secure, uses clear text over the network that can be sniffed

Telnet uses port 23

```
[root@elrond bin]# cat /etc/services
< snipped >
telnet          23/tcp
telnet          23/udp
< snipped >
[root@elrond bin]#
```



Is it installed?

Step 1 *Install software*

```
[root@elrond ~]# rpm -qa | grep telnet
telnet-0.17-46.el6.i686
telnet-server-0.17-46.el6.i686
[root@elrond ~]#
```

client

server

No response means it is not installed

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

Installing Telnet

Step 1 *Install software*

client

```
[root@elrond ~]# yum install telnet
```

```
[root@elrond ~]# yum install telnet-server
```

server

Installing Telnet

Step 1 *Install software (continued)*

```
[root@elrond ~]# yum install telnet-server
Loading mirror speeds from cached hostfile
 * base: mirrors.sonic.net
 * extras: mirrors.xmission.com
 * updates: mirror.nwresd.org
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package telnet-server.i686 1:0.17-46.el6 set to be updated
--> Processing Dependency: xinetd for package: 1:telnet-server-0.17-46.el6.i686
--> Running transaction check
---> Package xinetd.i686 2:2.3.14-29.el6 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved
```

Note that the telnet server uses xinetd

Installing Telnet

Step 1 *Install software (continued)*

```
Dependencies Resolved

================================================================================
 Package               Arch         Version                  Repository    Size
================================================================================
Installing:
 telnet-server         i686         1:0.17-46.el6            base          36 k
Installing for dependencies:
 xinetd                i686         2:2.3.14-29.el6          base         121 k

Transaction Summary
================================================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 156 k
Installed size: 307 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): telnet-server-0.17-46.el6.i686.rpm                |  36 kB     00:00
(2/2): xinetd-2.3.14-29.el6.i686.rpm                     | 121 kB     00:00
--------------------------------------------------------------------------------
Total                                           109 kB/s | 156 kB     00:01
```

Note, that xinetd, the super daemon, is also installed because it is a dependency of the telnet server

Installing Telnet

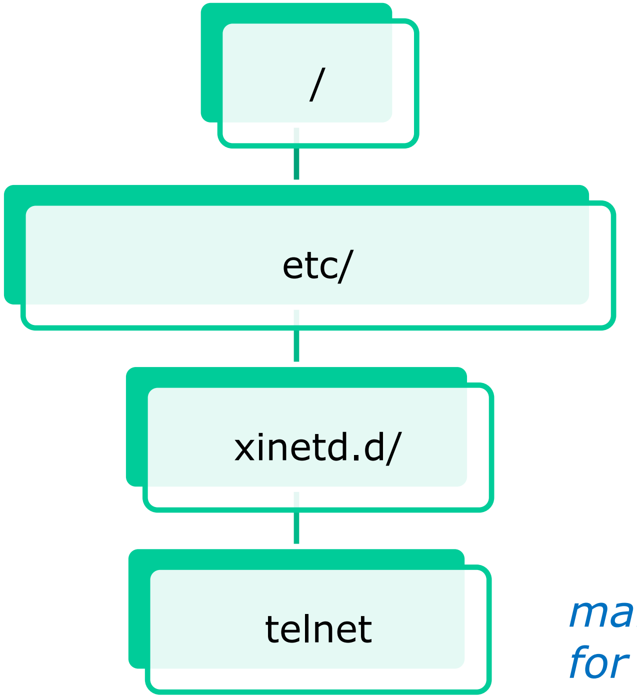
Step 1 *Install software (continued)*

```
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : 2:xinetd-2.3.14-29.el6.i686                              1/2
  Installing     : 1:telnet-server-0.17-46.el6.i686                         2/2

Installed:
  telnet-server.i686 1:0.17-46.el6

Dependency Installed:
  xinetd.i686 2:2.3.14-29.el6

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

Note, that xinetd, the super daemon, is also installed because it is a dependency of the telnet server

Configuring Telnet

Step 2 *Customize the configuration files*



main configuration file for telnet

Configuring Telnet

Step 2 *Customize the configuration file*

```
[root@elrond ~]# cat /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
```

Change to no to enable service

Configuring Telnet

Step 2 *Customize the configuration file*

Attribute	**Description**
flags	Sets any of a number of attributes for the connection. *REUSE* instructs xinetd to reuse the socket for a Telnet connection.
socket_type	Sets the network socket type to *stream*.
wait	Defines whether the service is single-threaded (*yes*) or multi-threaded (*no*).
user	Defines what user *ID* the process runs under.
server	Defines the binary executable to be launched.
log_on_failure	Defines logging parameters for *log_on_failure* in addition to those already defined in xinetd.conf.
disable	Defines whether the service is active.

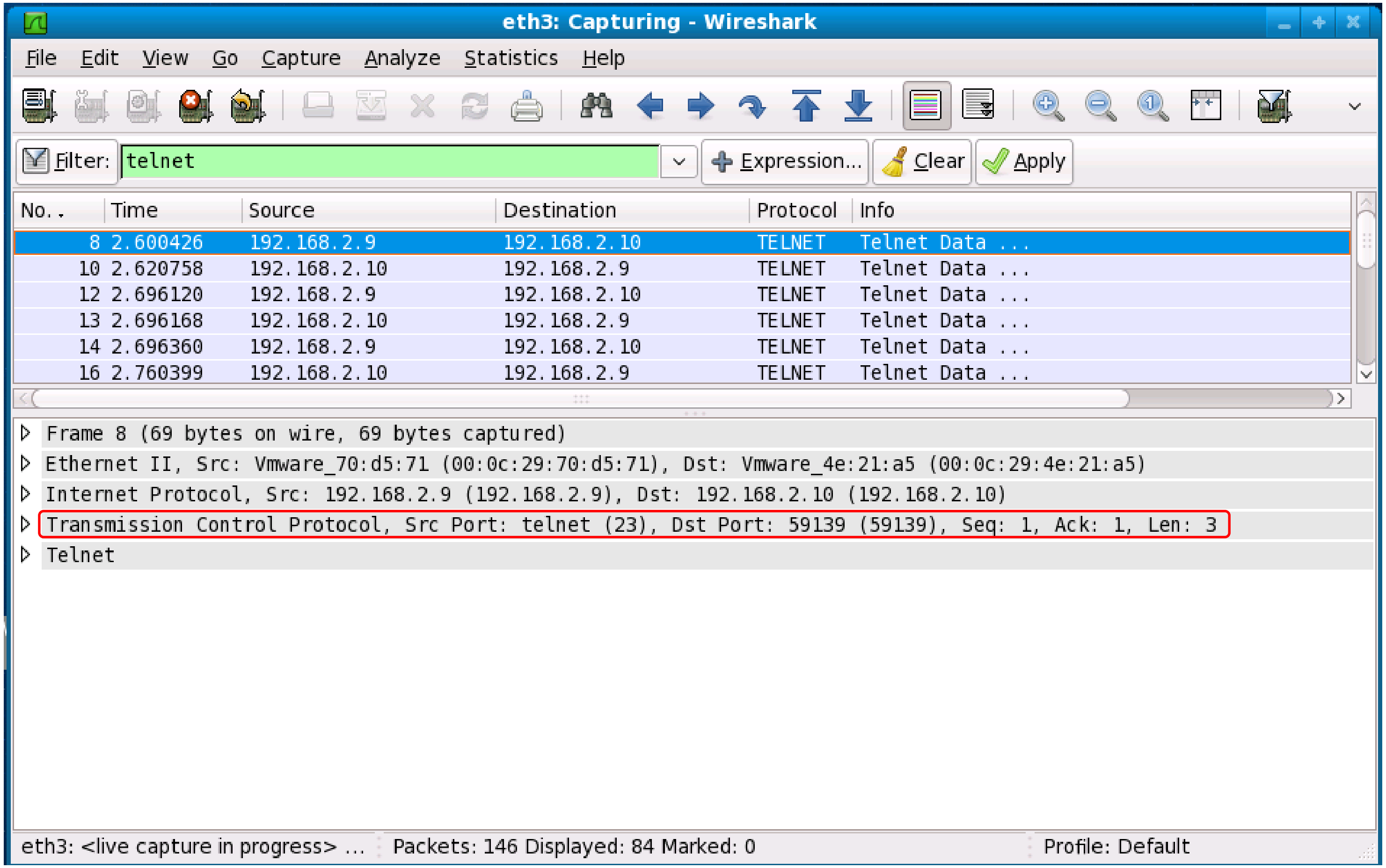
Great reference is "LINUX TCP/IP Network Administration" by Scott Mann

or use: man xinetd.conf

Firewall for Telnet

Step 3 *Modify the firewall*

Firewall must be modified to accept new packets to TCP port 23



eth3: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: telnet

```
No. .  Time      Source        Destination   Protocol  Info
    8 2.600426  192.168.2.9   192.168.2.10  TELNET    Telnet Data ...
   10 2.620758  192.168.2.10  192.168.2.9   TELNET    Telnet Data ...
   12 2.696120  192.168.2.9   192.168.2.10  TELNET    Telnet Data ...
   13 2.696168  192.168.2.10  192.168.2.9   TELNET    Telnet Data ...
   14 2.696360  192.168.2.9   192.168.2.10  TELNET    Telnet Data ...
   16 2.760399  192.168.2.10  192.168.2.9   TELNET    Telnet Data ...
```

```
▷ Frame 8 (69 bytes on wire, 69 bytes captured)
▷ Ethernet II, Src: Vmware_70:d5:71 (00:0c:29:70:d5:71), Dst: Vmware_4e:21:a5 (00:0c:29:4e:21:a5)
▷ Internet Protocol, Src: 192.168.2.9 (192.168.2.9), Dst: 192.168.2.10 (192.168.2.10)
▷ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 59139 (59139), Seq: 1, Ack: 1, Len: 3
▷ Telnet
```

eth3: <live capture in progress> ... Packets: 146 Displayed: 84 Marked: 0 Profile: Default

Firewall for Telnet

Step 3 *Modify the firewall*

Show the firewall rules with line numbers

iptables -L --line-numbers

Insert rule to allow new incoming telnet connections

iptables -I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 23 -j ACCEPT

Line number (varies) to insert new rule

Verify

```
[root@celebrian ~]# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     udp  --  anywhere             anywhere            udp dpt:router
5    ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:telnet
6    ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
7    REJECT     all  --  anywhere             anywhere            reject-with icmp-host-prohibited

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

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

SELinux for Telnet

Step 4 *Configure SELinux*

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

Leave as enforcing

Starting Telnet service manually

Step 5 *Start the service*

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

Starting Telnet service manually

Step 5 *Start the service*

If service is already running use the following to reread configuration files:

```
[root@elrond ~]# service xinetd restart
```

or

```
[root@elrond ~]# killall -1 xinetd
```

hangup signal

Starting Telnet service automatically

Step 6

To automatically start service at system boot use:

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

To later not start service at system boot use:

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

Note telnet runs under the superdaemon xinetd umbrella

Starting Telnet service automatically

```
[root@elrond ~]# chkconfig --list
```

< snipped >

```
xinetd based services:
        chargen-dgram:        off
        chargen-stream:       off
        daytime-dgram:        off
        daytime-stream:       off
        discard-dgram:        off
        discard-stream:       off
        echo-dgram:           off
        echo-stream:          off
        tcpmux-server:        off
        telnet:               on
        time-dgram:           off
        time-stream:          off
```

xinetd is a super daemon which acts as an umbrella for many other services

```
[root@elrond ~]#  chkconfig --list | grep telnet
        telnet:         on
```

Monitor Telnet service

Step 7 *Verify service is running*

telnetd processes

```
[cis192@elrond ~]$ ps -ef | grep telnet
root      6156  6118  0 07:52 ?        00:00:00 in.telnetd: kate
root      6268  6118  0 07:53 ?        00:00:00 in.telnetd: 192.168.0.27
root      6299  6118  0 07:56 ?        00:00:00 in.telnetd: 192.168.0.23
cis192    6325  6270  0 07:56 pts/2    00:00:00 grep telnet
[cis192@elrond ~]$
```

Individual telnetd daemons are run for each session

Monitor Telnet service

Step 7 *Verify service is running*

netstat

Show TCP ports listening

```
[root@p26-celebrian ~]# netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:telnet                    *:*                         LISTEN
```

Option n to show ports using numbers

```
[root@p26-celebrian ~]# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::23                       :::*                        LISTEN
```

Option p to show programs listening on ports

```
[root@p26-celebrian ~]# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program
name
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1427/sshd
tcp        0      0 :::22                       :::*                        LISTEN      1427/sshd
tcp        0      0 :::23                       :::*                        LISTEN      2633/xinetd
```

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

Troubleshooting Telnet

Step 8 *Troubleshooting*

```
root@frodo:~# telnet 172.30.1.125
Trying 172.30.1.125...
telnet: Unable to connect to remote host: No route to host
root@frodo:~#
```

Check routing tables (route –n) and connectivity (ping).

Check firewall and make sure TCP port 23 on the Telnet sever will accept new incoming Telnet connections.

Troubleshooting Telnet

Step 8 *Troubleshooting (continued)*

```
root@frodo:~# telnet 172.30.1.125
Trying 172.30.1.125...
Connected to 172.30.1.125.
Escape character is '^]'.
Connection closed by foreign host.
root@frodo:~#
```

Check:

1. /etc/xinetd.d/telnet attributes may be blocking access:
   - only_from
   - no_access
   - access-times

2. TCP wrappers files may be blocking access:
   - /etc/hosts.allow
   - /etc/hosts.deny

Telnet Logs

Step 9 *Monitor log files*

```
[root@elrond ~]# cat /var/log/messages | grep xinetd
Nov 20 07:24:20 elrond xinetd[1391]: START: telnet pid=1855
from=::ffff:172.30.1.155
Nov 20 07:24:47 elrond xinetd[1391]: EXIT: telnet status=0 pid=1855
duration=27(sec)
Nov 20 13:33:14 elrond xinetd[1391]: Starting reconfiguration
Nov 20 13:33:14 elrond xinetd[1391]: Swapping defaults
Nov 20 13:33:14 elrond xinetd[1391]: readjusting service telnet
Nov 20 13:33:14 elrond xinetd[1391]: Reconfigured: new=0 old=1 dropped=0
(services)
Nov 20 14:22:08 elrond xinetd[1391]: START: telnet pid=3676
from=::ffff:172.30.1.155
Nov 20 14:22:16 elrond xinetd[1391]: EXIT: telnet status=0 pid=3676
duration=8(sec)
Nov 20 15:36:17 elrond xinetd[1391]: START: telnet pid=4008
from=::ffff:172.30.1.155
Nov 20 15:36:29 elrond xinetd[1391]: EXIT: telnet status=0 pid=4008
duration=12(sec)
```

Record of xinetd service stop, start, or errors

Telnet Logs

Step 9 *Monitor log files*

```
[root@elrond ~]# cat /var/log/messages | grep telnet
Nov 20 07:24:20 elrond xinetd[1391]: START: telnet pid=1855 from=::ffff:172.30.1.155
Nov 20 07:24:47 elrond xinetd[1391]: EXIT: telnet status=0 pid=1855 duration=27(sec)
Nov 20 13:33:14 elrond xinetd[1391]: readjusting service telnet
Nov 20 14:22:08 elrond xinetd[1391]: START: telnet pid=3676 from=::ffff:172.30.1.155
Nov 20 14:22:16 elrond xinetd[1391]: EXIT: telnet status=0 pid=3676 duration=8(sec)
Nov 20 15:36:17 elrond xinetd[1391]: START: telnet pid=4008 from=::ffff:172.30.1.155
Nov 20 15:36:29 elrond xinetd[1391]: EXIT: telnet status=0 pid=4008 duration=12(sec)
Nov 20 15:50:29 elrond xinetd[1391]: START: telnet pid=4096 from=::ffff:172.30.1.155
Nov 20 15:51:40 elrond xinetd[1391]: START: telnet pid=4121 from=::1
```

Record of logins by IP address

Telnet additional security

Step 10 *Configure additional security*

Attribute	Description
only_from	Allows only the specified hosts to use the service.
no_access	Blocks listed hosts from using the service.
access_times	Specifies the time range when a particular service may be used. The time range must be stated in 24-hour format notation, HH:MM-HH:MM. Example: 08:00-18:00 means the service is available from 8AM to 6PM.

Additional security attributes can be added to /etc/xinetd.d/telnet

Telnet additional security

Step 10 *Configure additional security (continued)*

```
[root@elrond ~]# cat /etc/xinetd.d/telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        only_from       = 192.168.0.23
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
}
[root@elrond ~]#
```

Use only_from to restrict clients that can access the Telnet service

Telnet additional security

Step 10 *Configure additional security (continued)*

Only_ from examples

`only_from = arwen` *hostname*

`only_from = arwen legolas` *multiple hostnames*

`only_from = 192.168.3.12 192.168.3.14` *or IP addresses*

`only_from = 192.168.3.{12, 14}` *same as above*

`only_from = 192.168.0.0` *0's are wildcards*

`only_from = sauron 172.30.4.0 10.10.10.{1, 200}` *mixes*

`only_from = 192.168.16.0/22` *network/prefix*

Telnet additional security

Step 10 *Configure additional security (continued)*

TCP Wrappers

```
[root@elrond ~]# type xinetd
xinetd is /usr/sbin/xinetd
[root@elrond ~]# ldd /usr/sbin/xinetd
        linux-gate.so.1 =>  (0x00d00000)
        libselinux.so.1 => /lib/libselinux.so.1 (0x002fe000)
        libwrap.so.0 => /lib/libwrap.so.0 (0x005cb000)
        libnsl.so.1 => /lib/libnsl.so.1 (0x005e4000)
        libm.so.6 => /lib/libm.so.6 (0x00ed3000)
        libcrypt.so.1 => /lib/libcrypt.so.1 (0x00a7c000)
        libc.so.6 => /lib/libc.so.6 (0x00130000)
        libdl.so.2 => /lib/libdl.so.2 (0x006e9000)
        /lib/ld-linux.so.2 (0x00110000)
        libfreebl3.so => /lib/libfreebl3.so (0x0031d000)
[root@elrond ~]#
```

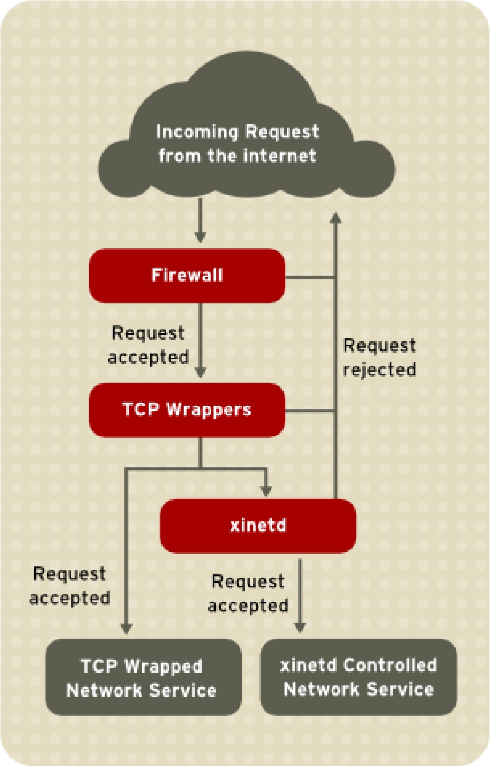
xinetd, which invokes telnet, is compiled with TCP wrappers

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

Telnet additional security

Step 10 *Configure additional security (continued)*

TCP Wrappers


Incoming Request from the internet
Firewall
Request accepted
Request rejected
TCP Wrappers
xinetd
Request accepted
Request accepted
TCP Wrapped Network Service
xinetd Controlled Network Service

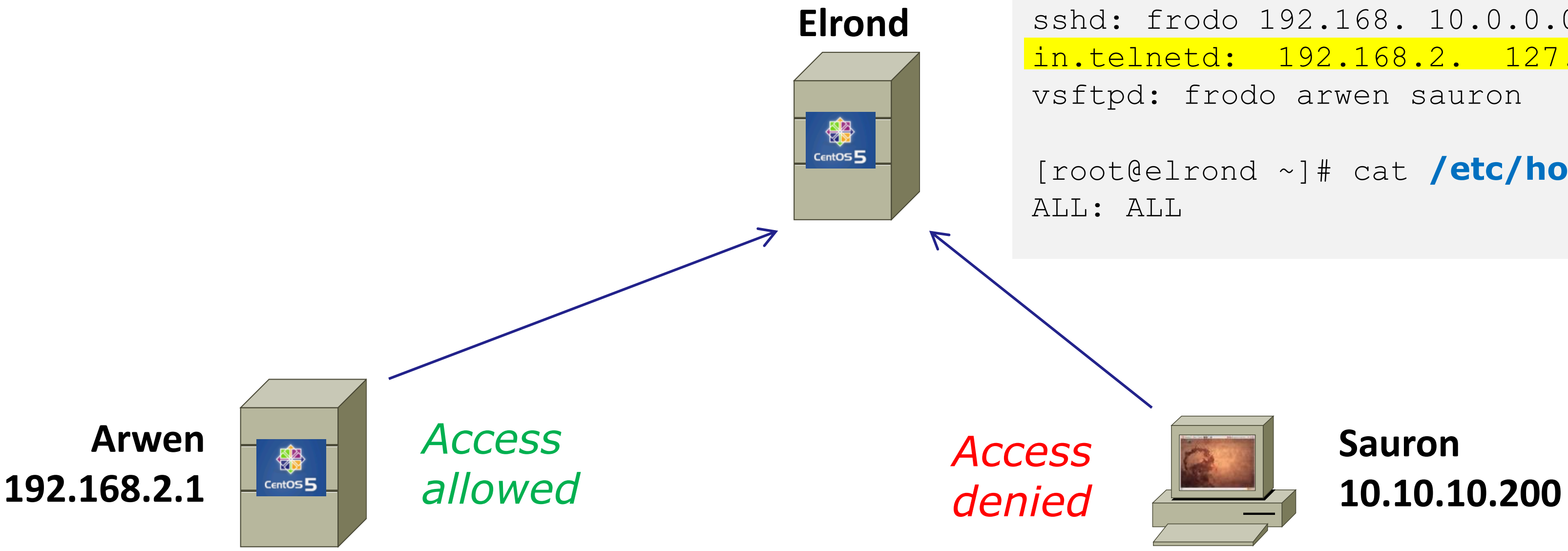
http://www.centos.org/docs/5/html/Deployment_Guide-en-US/ch-tcpwrappers.html

Telnet additional security

Step 10 *Configure additional security (continued)*

TCP Wrappers

```
[root@elrond ~]# cat /etc/hosts.allow
sshd: frodo 192.168. 10.0.0.0/255.0.0.0
in.telnetd:  192.168.2.  127.0.0.1
vsftpd: frodo arwen sauron

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



```
[root@elrond ~]# telnet arwen
Trying 192.168.2.9...
Connected to arwen (192.168.2.9).
Escape character is '^]'.
CentOS release 5.2 (Final)
Kernel 2.6.18-92.1.22.el5 on an i686
login: cis192
Password:
Last login: Mon Mar 16 00:03:58 from arwen
[cis192@arwen ~]$
```

```
root@sauron:~# telnet arwen
Trying 192.168.2.9...
Connected to arwen.
Escape character is '^]'.
Connection closed by foreign host.
```

Class Activity

Work in teams of your choice to build a telnet server

Allow telnet access only from hosts on the 172.20.0.0/16 network and block everyone else using TCP Wrappers

When finished let me know your IP address so I can test logging into it from Frodo and Opus

vsftpd

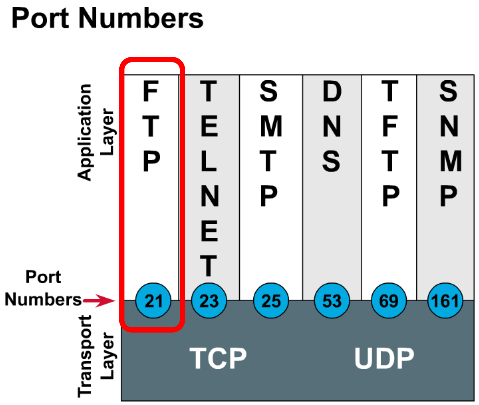
Installing and Configuring Telnet (Red Hat Family)

FTP

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

FTP uses ports 20 and 21

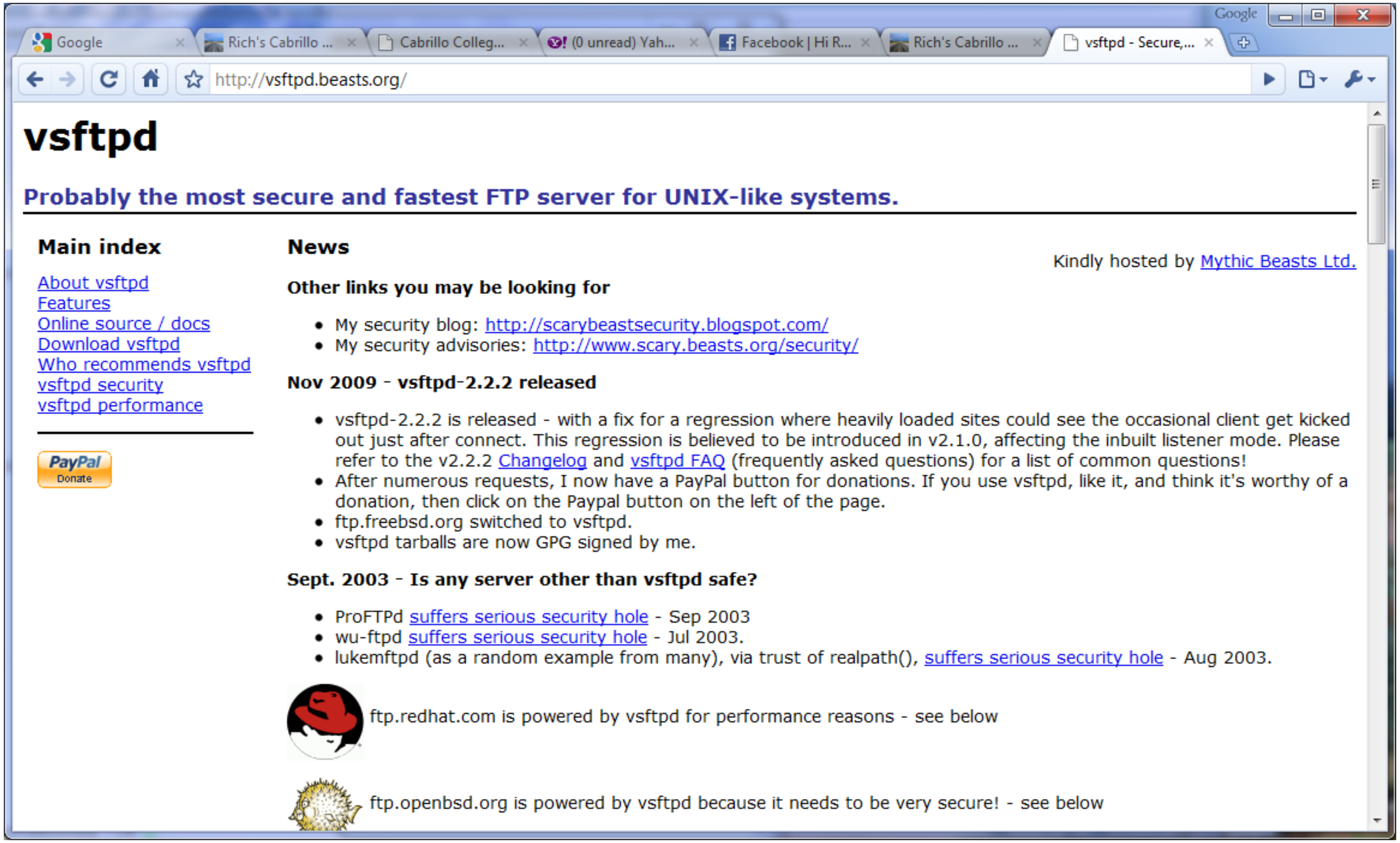
```
[root@elrond bin]# cat /etc/services
< snipped >
ftp-data        20/tcp
ftp-data        20/udp
# 21 is registered to ftp, but also used by fsp
ftp             21/tcp
ftp             21/udp          fsp fspd
< snipped >
[root@elrond bin]#
```



Port Numbers

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

PayPal Donate

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-ftpd 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

Installing and Configuring vsftpd (Red Hat Family)

Is it installed?

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

No response means it is not installed

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

vsftpd

Installing vsftpd

Step 1 *Installing service*

```
yum install vsftpd
```

vsftpd

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

Dependencies Resolved
```

vsftpd

```
Dependencies Resolved

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

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

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

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

Installing and Configuring vsftpd

Step 2 *Customize the configuration file*

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

< snipped >

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

< snipped >

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

Make your custom banner message here

Installing and Configuring vsftpd

Step 3 *Customize the firewall*

From the command line:

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

varies

```
service iptables save
```

Installing and Configuring vsftpd

Step 3 *Customize the firewall (continued)*

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

From the command line (temporary)

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

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

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

Firewall for FTP

Current firewall settings

CentOS Modified

```
[root@celebrian ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

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

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

FTP port is now open

Firewall for FTP

CentOS Modified

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

Permanent firewall settings

FTP port is now open

```
[root@celebrian ~]# lsmod | grep ftp
nf_conntrack_ftp        10449  0
nf_conntrack            66010  4 nf_conntrack_ftp,nf_conntrack_ipv4,nf_conntrack_ipv6,xt_state
[root@celebrian ~]#
```

Module to track related FTP connections is loaded

SELinux for FTP (CentOS)

Step 4 *Configure SELinux*

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

Leave as enforcing

Installing and Configuring vsftpd
(Red Hat Family)

Step 5 *Start or restart service*

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

Step 6 *Automatically start at system boot*

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

Installing and Configuring vsftpd

Step 7 *Verify service is running*

vsftpd processes

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


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

Individual vsftpd daemons are run for each session

Installing and Configuring vsftpd

netstat

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

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

Installing and Configuring vsftpd

netstat

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

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

Installing and Configuring vsftpd

Try it! *Create sample files on celebrian*

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

Installing and Configuring vsftpd

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

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

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

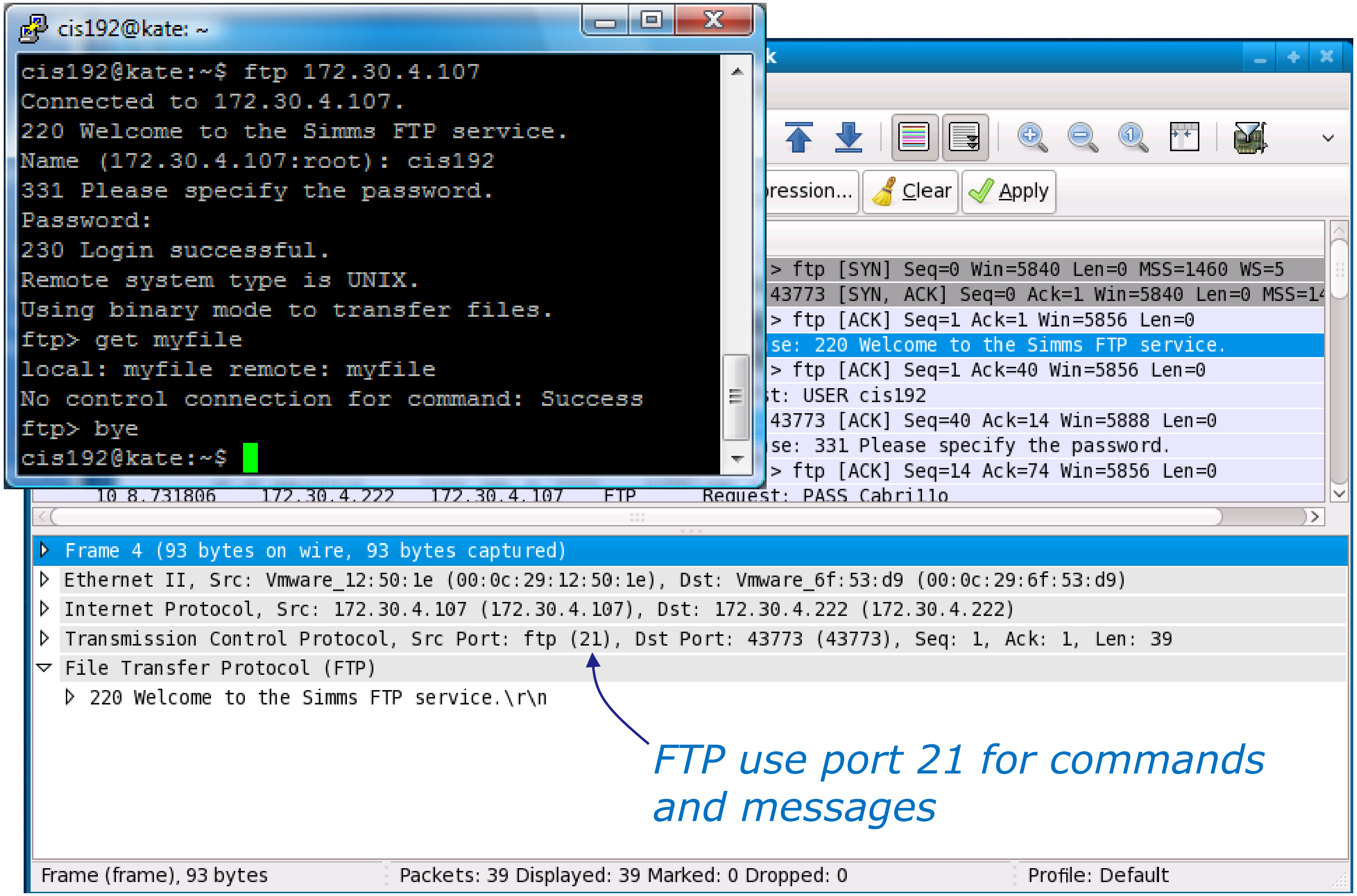
Try it!

Installing and Configuring vsftpd

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

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

Installing and Configuring vsftpd



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

```
> ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=5
43773 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=14
> ftp [ACK] Seq=1 Ack=1 Win=5856 Len=0
se: 220 Welcome to the Simms FTP service.
> ftp [ACK] Seq=1 Ack=40 Win=5856 Len=0
t: USER cis192
43773 [ACK] Seq=40 Ack=14 Win=5888 Len=0
se: 331 Please specify the password.
> ftp [ACK] Seq=14 Ack=74 Win=5856 Len=0
  10 8.731806     172.30.4.222     172.30.4.107     FTP       Request: PASS Cabrillo
```

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

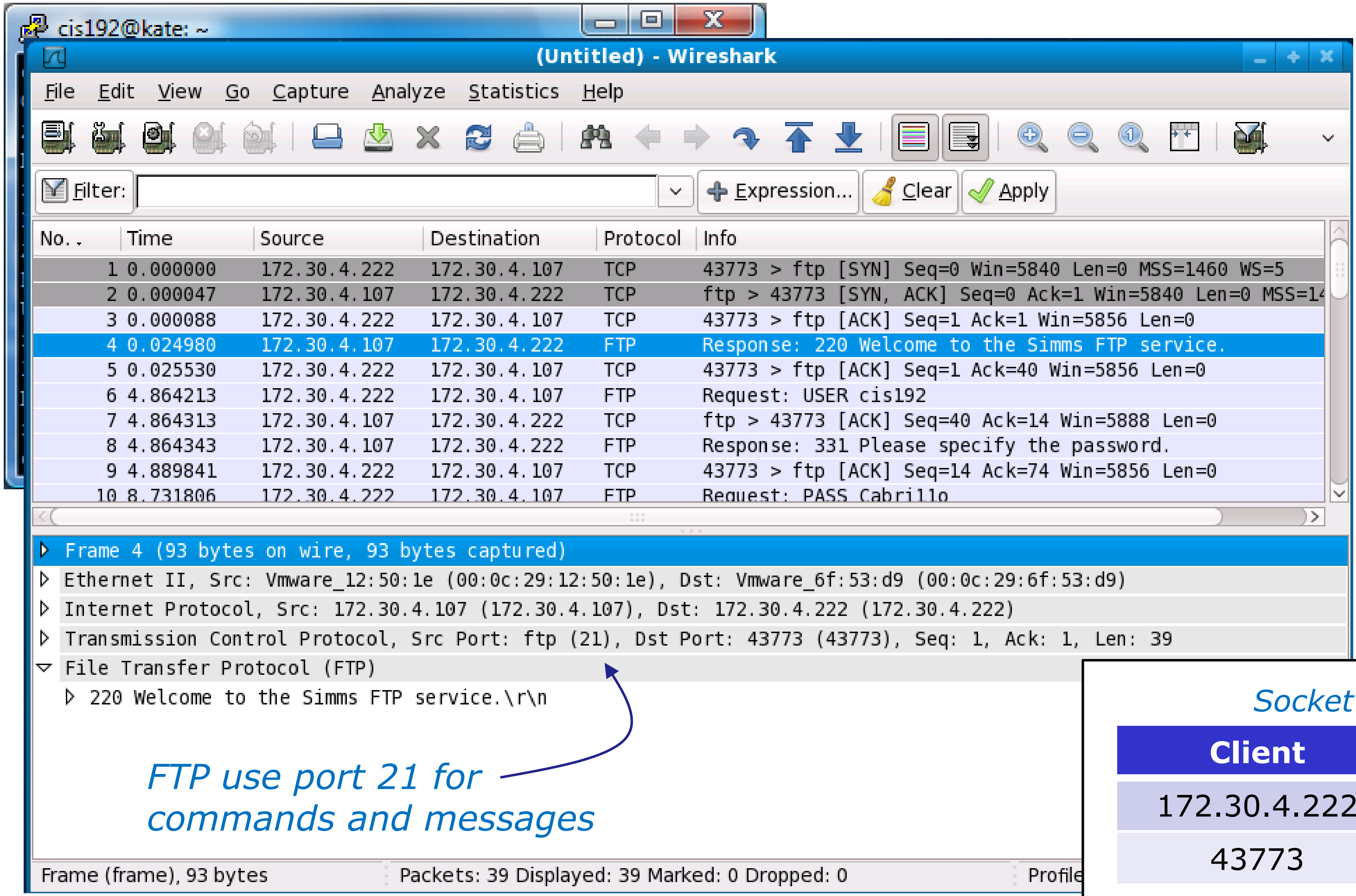
Frame (frame), 93 bytes Packets: 39 Displayed: 39 Marked: 0 Dropped: 0 Profile: Default

FTP use port 21 for commands and messages

3-way handshake

Login is transmitted in clear text

Installing and Configuring vsftpd



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

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

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

FTP use port 21 for commands and messages

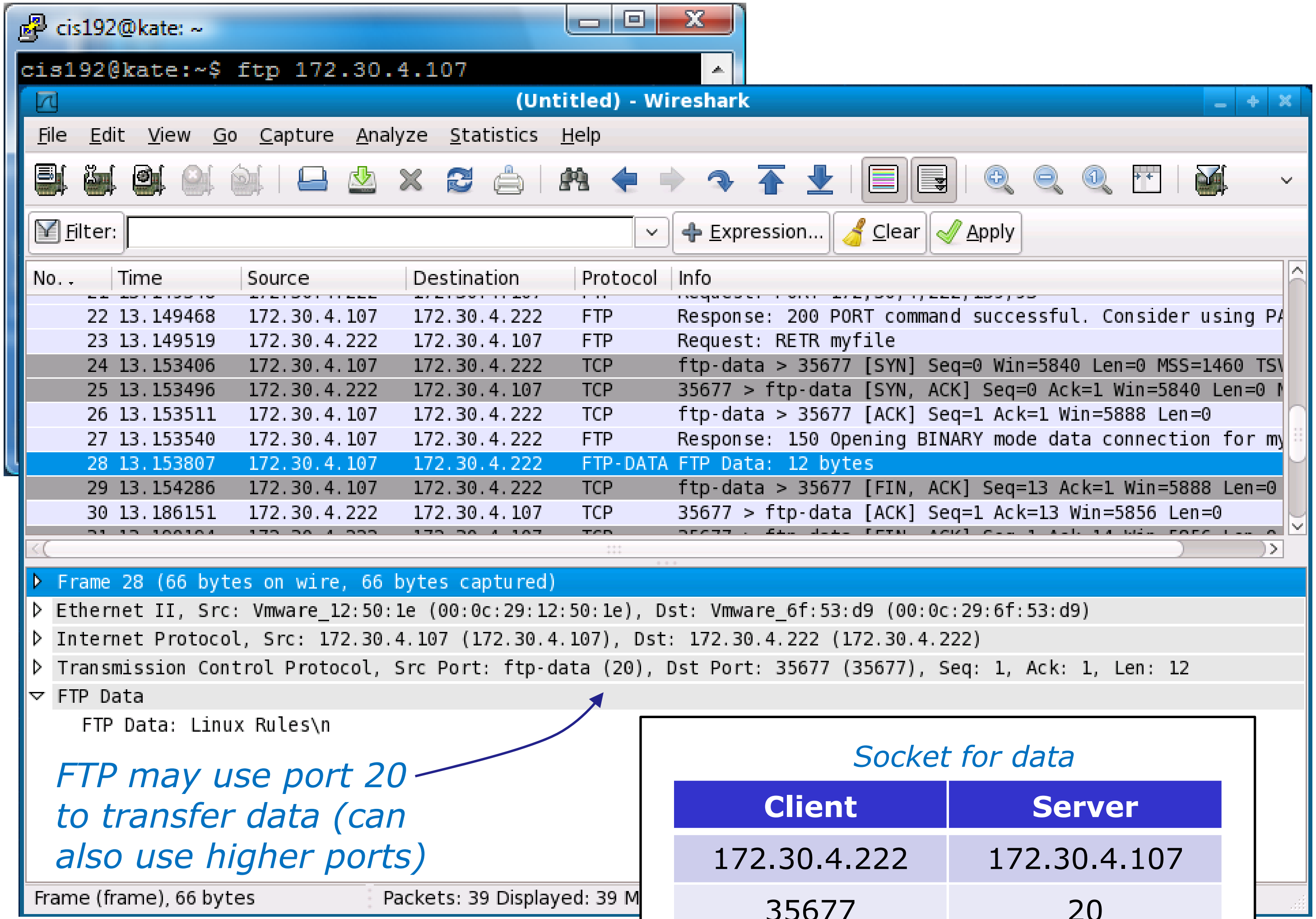
3-way handshake

Login is transmitted in clear text

Socket for commands

Client	Server
172.30.4.222	172.30.4.107
43773	21

Installing and Configuring vsftpd



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

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

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

```
Frame (frame), 66 bytes      Packets: 39 Displayed: 39 M
```

FTP may use port 20 to transfer data (can also use higher ports)

Socket for data

Client	Server
172.30.4.222	172.30.4.107
35677	20

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

Step 8 Troubleshooting

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

On the FTP server:

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

Installing and Configuring vsftpd

Step 8 Troubleshooting

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

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

Use ***iptables -I 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 celebrian
ftp: connect: Connection refused
ftp>
```

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

Installing and Configuring vsftpd

Step 8 Troubleshooting

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

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

Installing and Configuring vsftpd

Step 9 Monitor log files

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

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

Installing and Configuring vsftpd

Does vsftpd use TCP Wrappers?

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

yes it does

Installing and Configuring vsftpd

Step 10 *Configure additional security with TCP wrappers*

TCP Wrappers and vsftpd

vsftpd is compiled with TCP wrappers

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

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

```
[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 celebrian
```

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

Nosmo at 172.30.1.1 is NOT included

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

Everyone else is denied (this includes Nosmo)

Installing and Configuring vsftpd

TCP Wrappers and vsftpd example

celebrian

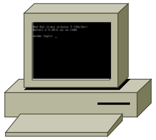
```
[root@celebrian ~]# cat /etc/hosts.allow
sshd: frodo 192.168. 10.0.0.0/255.0.0.0
in.telnetd:  192.168.2.10  127.0.0.1
vsftpd: frodo celebrian sauron

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

Sauron

Access permitted

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

Nosmo



Access denied

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

Class Activity

Work in teams to build a ftp server

When finished let me know your IP address so I can test downloading some files from it

Almost Wrap (test coming)

New commands, daemons and files:

- service
- chconfig
- killall
- netstat
- iptables
- netstat
- service
- yum

Daemons and related configuraton files

inetd	/etc/inetd.conf
portmap	/etc/etc/rpc
xinetd	/etc/etc/xinetd.d
service	/etc//etc/init.d
chconfig	/etc/rc.d/rc*.d
tcpd	/etc/hosts.allow,hosts.deny
iptables	/etc/sysconfig/iptables

New commands, daemons and files:

- iptables
- netstat
- service
- yum

Daemons and related configuration files

tcpd	/etc/hosts.allow,hosts.deny

Next Class

Lab 4 due

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

Quiz questions for next class:

- How do you find out if vsftpd is installed?
- What two ports does FTP use?
- What command shows the ports on your system that are open and listening for requests?

Test

Next Class

Test on lessons 1 through 4

- Open book, open notes, open VMs
- Do not request or give assistance on any of the test questions
- If you would like extra time you can take it home and turn it in by 11:59PM

Test 1

Backup

super daemons

Application Layer

inet Daemon

- */etc/inetd.conf*
- */etc/services*
- */etc/protocols*

Application Layer

xinetd Daemon

Syntax:

```
service service_name
{
        attribute operator value value ...
}
```

Application Layer

xinetd Daemon

Required Attributes

1. socket_type
2. wait
3. user
4. server
5. port
6. protocol
7. rpc_version - only for RPC services
8. rpc_number - only for RPC services

Application Layer

xinetd Daemon

- Access Attributes
  1. only_from
  2. no_access
- The bind Attribute
- The redirect Attribute
- Incorporating TCP_Wrappers

Application Layer

xinetd Daemon

The xinetd Daemon command line options

1. -d
2. -syslog
3. -loop rate
4. -reuse
5. -limit
6. -logproc