

## Linux Howtos

### Network Installation using PXE (201)

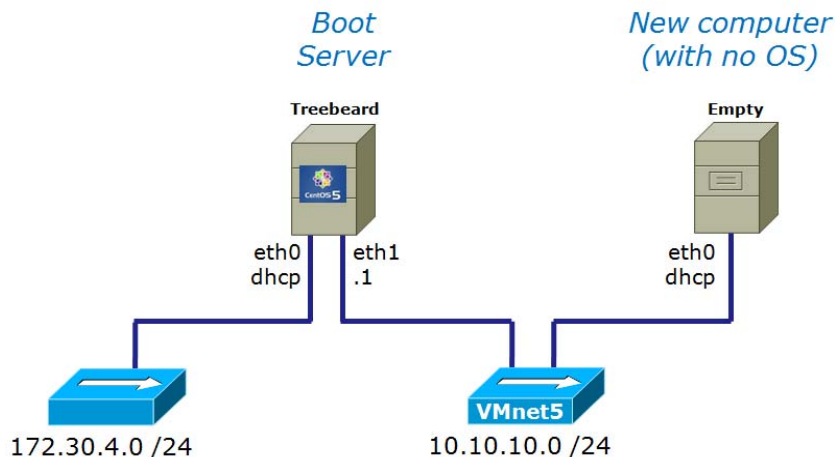
CIS 192 – Spring 2010

#### Network Installation using PXE (201)

This Howto documents the configuration of a PXE based boot server for doing Linux installations. PXE (Preboot Execution Environment) allows a new “empty” computer to use the network to boot up and install an operating system.

The PXE-based boot server (Treebeard) will have DHCP, TFTP and a web server configured and running. The “empty” computer will do a PXE boot, get an IP address using DHCP, then get the Linux kernel and initial RAM disk files using tftp. Next, HTTP is used to get installation files via the web server to do the install.

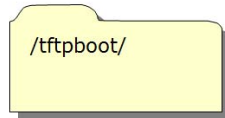
PXELINUX (a derivative of SYSLINUX) will be used to orchestrate the initial boot. The Anaconda installer using a kickstart file will automate the Linux installation.



The boot server, named Treebeard, will have repositories for the PXELINUX boot files, a kickstart file and all the files normally found on a Linux Distribution installation CD/DVD.

The Linux kernel (**vmlinuz**), initial RAM disk (**initrd.img**) and PXELINUX boot files are placed in the **/tftpboot** directory. These files will be transferred using TFTP to the new empty client when it first boots.

The kickstart file (**ks.cfg**) and all the files found on a Linux distribution installation CD/DVD are placed in the **/var/www/html** directory. These files will be transferred using HTTP via the Apache web server to the new empty client.



/tftpboot/

*These files are transferred using TFTP*

```
chain.c32
images/centos/i386/5.3/initrd.img
images/centos/i386/5.3/vmlinuz
mboot.c32
memdisk
menu.c32
pxelinux.0
pxelinux.cfg/default
```



/var/www/html/

*These files are transferred using HTTP*

```
mirrors/CentOS-5.3-i386/ks.cfg
mirrors/CentOS-5.3-i386/CentOS/*
mirrors/CentOS-5.3-i386/EULA
mirrors/CentOS-5.3-i386/GPL
mirrors/CentOS-5.3-i386/isolinux/*
mirrors/CentOS-5.3-i386/NOTES
mirrors/CentOS-5.3-i386/RELEASE-NOTES*
mirrors/CentOS-5.3-i386/repodata/*
mirrors/CentOS-5.3-i386/RPM-GPG-KEY*
mirrors/CentOS-5.3-i386/TRANS.TBL
```

## Supplies

VMs:

- Treebeard (CentOS 5.3 installed)
  - Choose Custom mode when creating
  - Select Red Hat Enterprise Linux 4 or 5 (32 bit)
  - Not private
  - Run as user who powers on the VM
  - One processor
  - 512 MB RAM
  - SCSI Adapter: LSI Logic
  - 10 GB SCSI HD
    - Don't allocate space now
    - Split disk into 2 GB files (for USB flash drive transport)
  - 2 NICs (add 2<sup>nd</sup> NIC and configure after creating VM)
    - Ethernet – bridged (shares host's NIC)
    - Ethernet 2 – connects to VMnet5 (a virtual network)
- Empty (no OS installed)
  - Choose Custom mode when creating
  - Select Red Hat Enterprise Linux 4 or 5 (32 bit)
  - Not private
  - Run as user who powers on the VM
  - One processor
  - 512 MB RAM
  - SCSI Adapter: LSI Logic
  - 5 GB SCSI HD
    - Don't allocate space now
    - Split disk into 2 GB files (for USB flash drive transport)

- 1 NIC
  - Ethernet - connects to VMnet5 (a virtual network)

Virtualization: VMWare Server 1.0X or 2.X

## PXE Boot Sequence

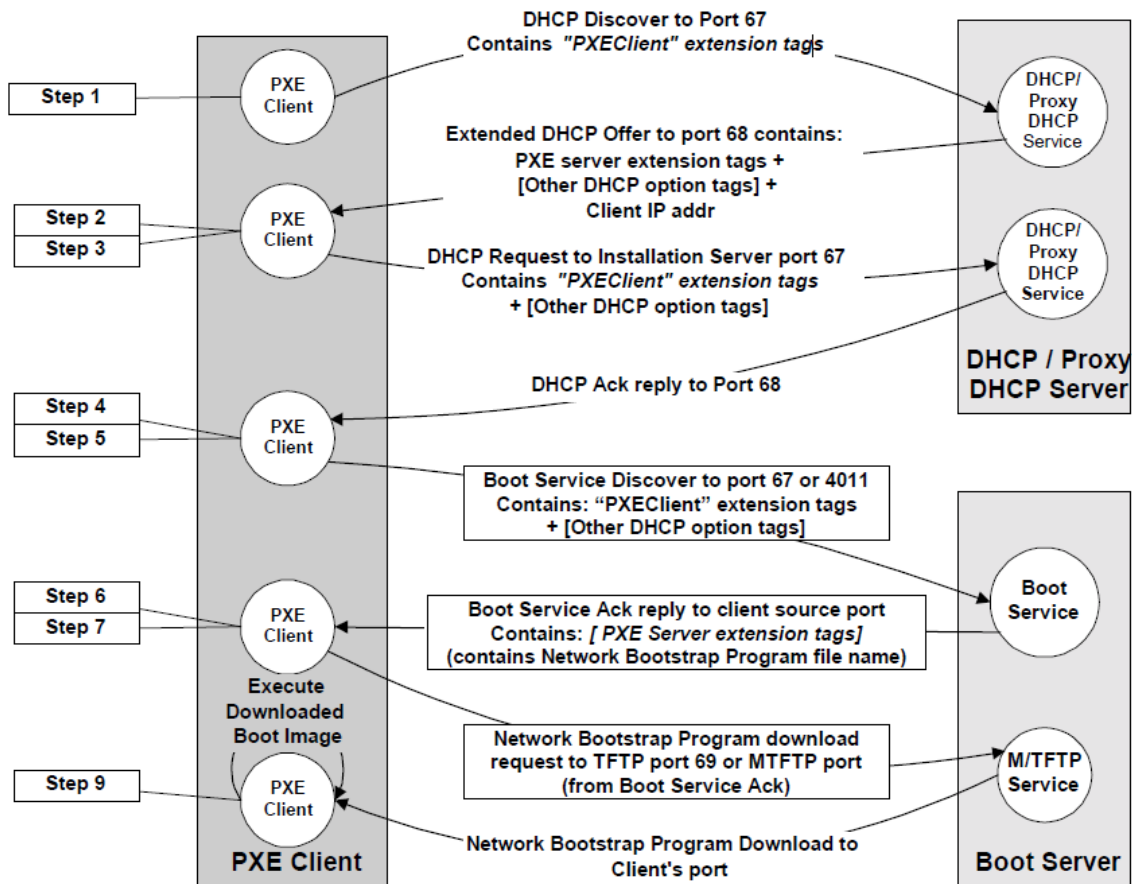


Figure 2-1 PXE Boot

Source: <http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf>

## Configure Treebeard to be a PXE boot server

- 1) Configure the network interfaces:
  - eth0 is dhcp
  - eth1 is static 10.10.10.1/24
  - enable IP forwarding (`echo 1 > /proc/sys/net/ipv4/ip_forward`)

Note: eth0 will connect to your physical network. eth1 will connect to the virtual VMnet5 network. The Empty VM will also be connected to the VMnet5 virtual network.

Forwarding is enabled so the Empty VM will be able to get to the Internet via Treebeard.

See Treebeard Network Interface Configuration below for more information.

2) Install (if necessary) and configure the DHCP service.

```
[root@treebeard ~]# yum install dhcp
```

You will need to create a **/etc/dhcpd.conf** file on your DHCP server. See the Treebeard DHCP Service Configuration section below for the complete configuration file used in this example. If you already have a **/etc/dhcpd.conf** file add the following lines to it in the global section. Make sure the next-server entry has the IP address of the boot (tftp) server. In this example we are using Treebeard at 10.10.10.1:

```
# Added for PXE boot support
allow booting;
allow bootp;
option option-128 code 128 = string;
option option-129 code 129 = text;
next-server 10.10.10.1;
filename "pxelinux.0";
```

Use **service dhcpd restart** after making the changes.

Use **chkconfig dhcpd on** so the service starts automatically during system boot.

3) Install and configure the tftp-server package. After a client gets an IP address using dhcp then tftp is used to pull down the linux kernel and initial RAM disk files.

```
[root@treebeard ~]# yum install tftp-server
```

tftp runs under the xinetd super-daemon umbrella. By default it is disabled. Edit the **/etc/xinetd.d/tftp** file and set "**disable**" to "**no**". In addition, add the **-vvv** option to increase what gets logged.

```
[root@treebeard ~]# cat /etc/xinetd.d/tftp
# default: off
# description: The tftp server serves files using the trivial file transfer \
#      protocol. The tftp protocol is often used to boot diskless \
#      workstations, download configuration files to network-aware printers, \
#      and to start the installation process for some operating systems.
service tftp
{
    socket_type           = dgram
    protocol              = udp
    wait                  = yes
    user                  = root
    server                = /usr/sbin/in.tftpd
    server_args           = -vvv -s /tftpboot
    disable               = no
    per_source            = 11
    cps                   = 100 2
    flags                 = IPv4
}
[root@treebeard ~]#
```

Note: the **-s** is the *secure* option so tftp runs under chroot. **-vvv** is *very very verbose* so all transferred files get logged in **/var/log/messages**.

Restart the xinetd service so the tftp configuration change takes effect:

```
[root@treebeard ~]# service xinetd restart
Stopping xinetd:                [ OK ]
Starting xinetd:                [ OK ]
[root@treebeard ~]#
```

4) Install (if necessary) the http service (Apache web server) and configure it.

If you need to install the Apache web server:

- [root@treebeard ~]# **yum install httpd**
- Set the **ServerName** directive in **/etc/httpd/conf/httpd.conf** to your server's IP address and port 80 (e.g. **ServerName 10.10.10.1:80**)
- Start Apache with: **service httpd start**

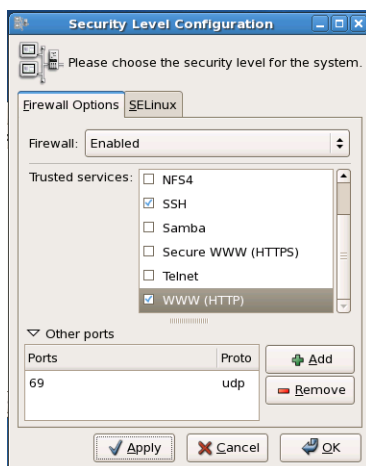
To check status:

```
[root@treebeard ~]# service httpd status
httpd (pid 4092 4091 4090 4089 4088 4087 4086 4085 4083) is running...
[root@treebeard ~]#
```

To start Apache web server:

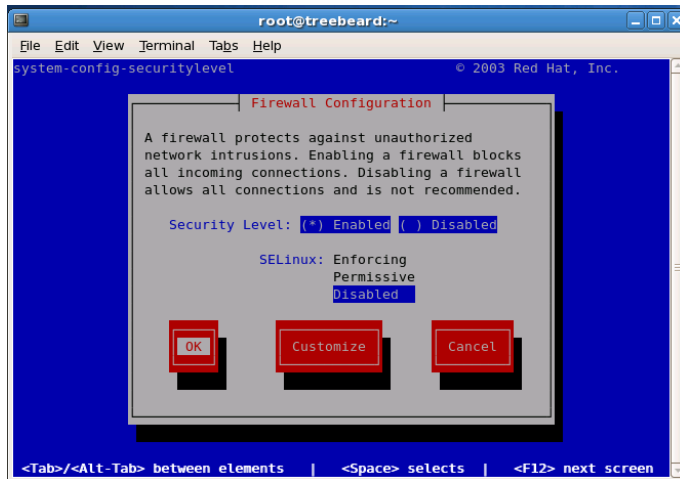
```
[root@treebeard ~]# service httpd start
Starting httpd:                [ OK ]
[root@treebeard ~]#
```

5) The firewall needs to be adjusted to allow incoming http and tftp requests. Open TCP port 80 and UDP port 69 in the firewall. These changes can be made with the Security Level Configuration tool (System > Administration) or the command line.



Using the command line is preferable. In addition to opening the ports 69 and 80 you can set up a NAT service for the 10.10.10.0/24 network and allow packets to be forwarded. See the Treebeard Firewall Configuration section below for how to do this.

6) Set SELinux to Disabled. One way to do this is to run **lokkit** and make the change if necessary:



7) Install the syslinux package. The Syslinux project produces lightweight bootloaders that can be used to boot OS's from hard drives, CDs (ISOLINUX) and over the network (PXELINUX).

```
[root@treebeard ~]# yum install syslinux
```

8) Copy Syslinux files to the `/tftpboot` directory

```
[root@treebeard ~]# cp /usr/lib/syslinux/pxelinux.0 /tftpboot
[root@treebeard ~]# cp /usr/lib/syslinux/menu.c32 /tftpboot
[root@treebeard ~]# cp /usr/lib/syslinux/memdisk /tftpboot
[root@treebeard ~]# cp /usr/lib/syslinux/mboot.c32 /tftpboot
[root@treebeard ~]# cp /usr/lib/syslinux/chain.c32 /tftpboot
[root@treebeard ~]#
```

9) Make a new directory for the PXE boot menus

```
[root@treebeard ~]# mkdir /tftpboot/pxelinux.cfg
[root@treebeard ~]#
```

10) Create a file named `default` in that directory. Note the kernel and append commands must be on one line (even though they may be shown as wrapped in the examples below):

```
[root@treebeard CentOS-5.3-i386]# cat /tftpboot/pxelinux.cfg/default
default menu.c32
prompt 0

# Bug in menu.c32 breaks timeout
# http://syslinux.zytor.com/archives/2005-September/005812.html
#timeout 300
#ONTIMEOUT minimal
```

```
MENU TITLE PXE Menu
```

```
LABEL minimal
```

```
    MENU LABEL CentOS 5.3 x86 (gets kickstart file using HTTP)
```

```
    MENU DEFAULT
```

```
    kernel images/centos/i386/5.3/vmlinuz
```

```
    append initrd=images/centos/i386/5.3/initrd.img
```

```
ks=http://10.10.10.1/mirrors/CentOS-5.3-i386/ks.cfg
```

```
LABEL interactive
```

```
    MENU LABEL CentOS 5.3 x86 (interactive install, no kickstart file)
```

```
    kernel images/centos/i386/5.3/vmlinuz
```

```
    append initrd=images/centos/i386/5.3/initrd.img ks ip=dhcp
```

```
[root@treebeard CentOS-5.3-i386]#
```

For details on above see: <http://syslinux.zytor.com/wiki/index.php/SYSLINUX>

11) Place Linux kernel(s) and initial RAM disk image(s) into `/tftpboot` directory for tftp transfers. For each Linux distribution to install make a directory for the kernel and initial ram disk images:

```
[root@treebeard ~]# mkdir -p /tftpboot/images/centos/i386/5.3
```

12) For each Linux distribution to install, copy the **vmlinuz** (kernel) and **initrd.img** (initial RAM disk) image files from disc 1 of the distribution CD. In the example below the CentOS 5.3 DVD has been mounted and the mount command shows the actual mount point. Use this mount information to copy the **vmlinuz** and **initrd.img** files.

```
[root@treebeard ~]# mount
```

```
/dev/mapper/VolGroup00-LogVol00 on / type ext3 (rw)
```

```
proc on /proc type proc (rw)
```

```
sysfs on /sys type sysfs (rw)
```

```
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
```

```
/dev/sda1 on /boot type ext3 (rw)
```

```
tmpfs on /dev/shm type tmpfs (rw)
```

```
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
```

```
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
```

```
/dev/hdc on /media/CentOS_5.3_Final type iso9660 (ro,noexec,nosuid,nodev,uid=0)
```

```
[root@treebeard ~]# cd /tftpboot/images/centos/i386/5.3/
```

```
[root@treebeard 5.3]# cp /media/CentOS_5.3_Final/images/pxeboot/vmlinuz .
```

```
[root@treebeard 5.3]# cp /media/CentOS_5.3_Final/images/pxeboot/initrd.img .
```

```
[root@treebeard 5.3]#
```

13) Copy all the files on the Linux distribution DVD/CDs to your web document root location. These files will now be available using the http protocol to new clients.

```
[root@treebeard ~]# mkdir -p /var/www/html/mirrors/CentOS-5.3-i386/
```

```
[root@treebeard ~]# cd /var/www/html/mirrors/CentOS-5.3-i386/
```

```
[root@treebeard CentOS-5.3-i386]# cp -r /media/CentOS_5.3_Final/* .
```

You can name these directories as you wish but they need to be configured in your PXELINUX **default** file and Linux kickstart file (**ks.cfg**)

14) Place your kickstart file where it can be retrieved using your web server. A kickstart file contains the answers to questions you normally answer during an interactive install. This

allows the entire installation to be automated. In this example, the kickstart file is placed in the same location as the distribution files.

```
[root@treebeard CentOS-5.3-i386]# cat ks.cfg
#platform=x86, AMD64, or Intel EM64T
# System authorization information
auth --useshadow --enablemd5
# System bootloader configuration
bootloader --location=mbr --driveorder=sda
# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel --drives=sda
# Use text mode install
text
# Firewall configuration
firewall --enabled --ssh
# Run the Setup Agent on first boot
firstboot --disable
# System keyboard
keyboard us
# System language
lang en_US
# Installation logging level
logging --level=info
# Use network installation
url --url=http://10.10.10.1/mirrors/CentOS-5.3-i386
# Network information
network --bootproto=dhcp --device=eth0 --onboot=on --hostname empty.localdomain
# Reboot after installation
reboot
#Root password
rootpw --iscrypted $1$oePUsywv$AqPrr7o4nHsq.eCY4TJsjl

# SELinux configuration
selinux --enforcing
# System timezone
timezone --isUtc America/Los_Angeles
# Install OS instead of upgrade
install
# Disk partitioning information
autopart

%packages
@core
%post
Add initial user
useradd -p '$1$ea6cJkZL$7Q8E8Di4CSKJ3fsCiFVQR1' cis192
#
# Make unique hostname
#
# Treebeard has a web page with a hit counter. The count is incremented
# each time the page is served. wget is used by then new system to request this
# web page via HTTP.
#
# The sed command extracts the count from the downloaded html page which
# is surrounded by span tags <span> and </span>. The count is then used to
# make a unique hostname.cp
#
file="10.10.10.1/counter/pxe-boot-counter.shtml"
num=$(wget -O - $file | sed -n 's/.*<span>\(.*\)</span>.*\n/ip;T;q')
hostname="seedling$num"
```



```
# Backup original network file
cp /etc/sysconfig/network /etc/sysconfig/network.bak

# Modify the hostname in the network file
sed "s/empty/$hostname/g" < /etc/sysconfig/network.bak > /etc/sysconfig/network

echo "New hostname is $hostname"
```

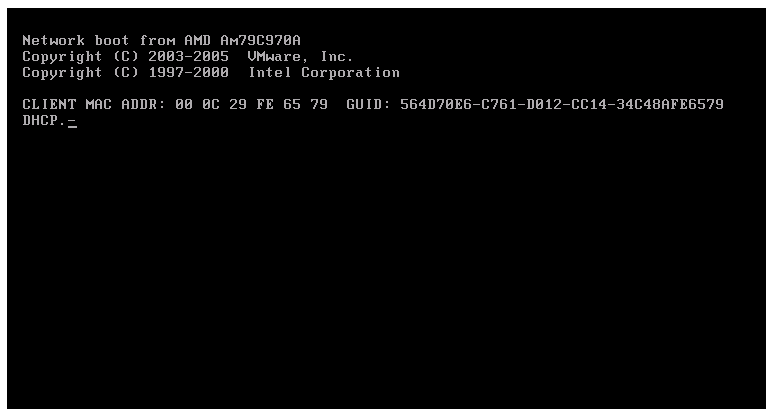
```
[root@treebeard CentOS-5.3-i386]#
```

Note: this kickstart file, ks.cfg, does a text based installation of just the minimal core packages. Note it handles the disk partitioning and the reboot at the end automatically.

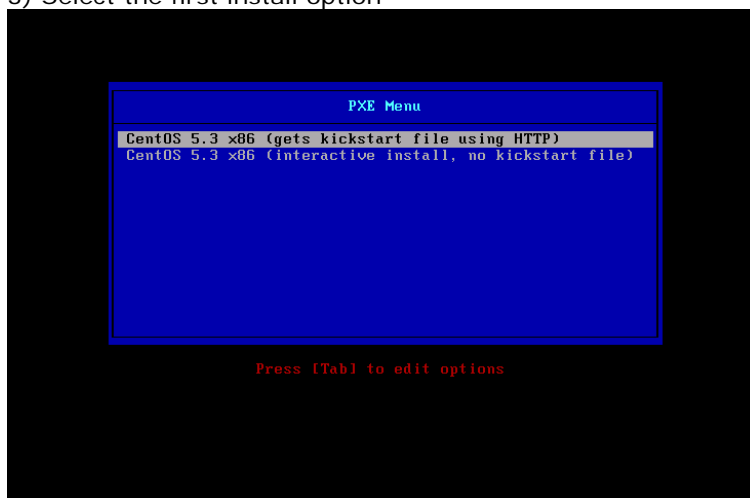
## Installing Linux into new VMs

Now that you have the PXE boot server configure it is time to try it out.

- 1) Create a new VM named empty with at least 384 MB of RAM and 5 GB for the hard drive.
- 2) Edit the VM settings and configure the Ethernet device to connect to VMnet5.
- 3) Start the VM



- 3) Select the first install option



- 4) Sit back and enjoy the install. The hard drive is partitioned, the OS packages are copied.



## Treebeard Network Interface Configuration

The two NICs are permanently configured for dhcp and static addresses. Note your MAC addresses will differ as they are randomly generated by VMware for each VM:

```
[root@treebeard ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:A7:73:E7
ONBOOT=yes
```

```
[root@treebeard ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth1
BOOTPROTO=static
BROADCAST=10.10.10.255
IPADDR=10.10.10.1
NETMASK=255.255.255.0
ONBOOT=yes
HWADDR=00:0c:29:a7:73:f1
```

Remember to use the following command to have the NIC configuration files take effect:

```
[root@treebeard ~]# service network restart
Shutting down interface eth0: [ OK ]
Shutting down interface eth1: [ OK ]
Shutting down loopback interface: [ OK ]
Disabling IPv4 packet forwarding: net.ipv4.ip_forward = 0 [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0:
Determining IP information for eth0... done. [ OK ]
Bringing up interface eth1:
```

IP forwarding is enabled permanently by editing the `/etc/sysctl.conf` file:

```
[root@treebeard ~]# cat /etc/sysctl.conf
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls IP packet forwarding
net.ipv4.ip_forward = 1

# Controls source route verification
net.ipv4.conf.default.rp_filter = 1

# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0

# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0

# Controls whether core dumps will append the PID to the core filename
# Useful for debugging multi-threaded applications
kernel.core_uses_pid = 1

# Controls the use of TCP syncookies
```

```
net.ipv4.tcp_syncookies = 1

# Controls the maximum size of a message, in bytes
kernel.msgmnb = 65536

# Controls the default maximum size of a message queue
kernel.msgmax = 65536

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 4294967295

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 268435456
[root@treebeard ~]#
```

Remember to use the following command to have the `/etc/sysctl.conf` configuration changes take effect:

```
[root@treebeard ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 4294967295
kernel.shmall = 268435456
[root@treebeard ~]#
```

Use `ifconfig` to make sure your network settings are active:

```
[root@treebeard ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:A7:73:E7
          inet addr:172.30.4.194  Bcast:172.30.4.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea7:73e7/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1273 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1383 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:546158 (533.3 KiB)  TX bytes:195164 (190.5 KiB)
          Interrupt:177 Base address:0x1400

eth1      Link encap:Ethernet  HWaddr 00:0C:29:A7:73:F1
          inet addr:10.10.10.1  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea7:73f1/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:16846 (16.4 KiB)
          Interrupt:185 Base address:0x1480

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2226 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5103450 (4.8 MiB)  TX bytes:5103450 (4.8 MiB)
```

```
[root@treebeard ~]#
```

## Treebeard DHCP Service Configuration

The DHCP service is configured using the `/etc/dhcpd.conf` file.

In the global section at the top add lines to enable booting, specify the IP address of the boot server and provide the name of the boot program file to download and run.

Setup the 10.10.10.0/24 subnet by specifying the default gateway, network mask, domain name, DNS servers and a range of IP address to assign. The DNS servers in the example below allow Treebeard to operate at Cabrillo College or on my home network.

### DHCP information

```
[root@treebeard ~]# cat /etc/dhcpd.conf
ddns-update-style interim;
```

```
# Added for PXE boot support
```

```
allow booting;
```

```
allow bootp;
```

```
option option-128 code 128 = string;
```

```
option option-129 code 129 = text;
```

```
next-server 10.10.10.1;
```

```
filename "pxelinux.0";
```

```
ignore client-updates;
```

```
option time-offset -25200; #PDT
```

```
subnet 10.10.10.0 netmask 255.255.255.0 {
```

```
option routers 10.10.10.1;
```

```
option subnet-mask 255.255.255.0;
```

```
option domain-name "tarchari";
```

```
option domain-name-servers 207.62.187.53, 207.62.187.54, 192.168.0.1;
```

```
range dynamic-bootp 10.10.10.150 10.10.10.199;
```

```
default-lease-time 21600;
```

```
max-lease-time 43200;
```

```
}
```

```
[root@treebeard ~]#
```

Restart the DHCP server so the changes made in `/etc/dhcpd.conf` take effect:

```
[root@nosmo root]# service dhcpd restart
```

```
Shutting down dhcpd: [ OK ]
```

```
Starting dhcpd: [ OK ]
```

```
You have new mail in /var/spool/mail/root
```

```
[root@nosmo root]#
```

## Treebeard Firewall Configuration

The default CentOS 5.3 firewall needs to be modified to:

- o Allow new incoming tftp requests (UDP port 69)
- o Allow new incoming http requests (TCP port 80)
- o Provide NAT service for the 10.10.10.0/24 network (using MASQUERADE)

- o Allow forwarding of packets (delete rule that send forwarded packets through the RH-Firewall-1-INPUT filter)

First backup iptables configuration:

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

Make the four changes mentioned above:

```
iptables -I RH-Firewall-1-INPUT 9 -m state --state NEW -m udp -p udp --dport 69 -j ACCEPT
iptables -I RH-Firewall-1-INPUT 9 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -D FORWARD 1
```

Save the new configuration:

```
iptables-save > /etc/sysconfig/iptables
```

Reload the firewall from the configuration file:

```
service iptables restart
```

Display the revised firewall rules:

```
cat /etc/sysconfig/iptables
iptables -L
iptables -t nat -L
```

```
[root@treebeard sysconfig]# iptables-save > /etc/sysconfig/iptables.bak
[root@treebeard sysconfig]# iptables -I RH-Firewall-1-INPUT 9 -m state --state
NEW -m udp -p udp --dport 69 -j ACCEPT
[root@treebeard sysconfig]# iptables -I RH-Firewall-1-INPUT 9 -m state --state
NEW -m tcp -p tcp --dport 80 -j ACCEPT
[root@treebeard sysconfig]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@treebeard sysconfig]# iptables -D FORWARD 1
```

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

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

```
[root@treebeard sysconfig]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.3.5 on Tue Nov 3 09:53:04 2009
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [1:70]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Tue Nov 3 09:53:04 2009
# Generated by iptables-save v1.3.5 on Tue Nov 3 09:53:04 2009
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [664:72586]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p esp -j ACCEPT
```

```

-A RH-Firewall-1-INPUT -p ah -j ACCEPT
-A RH-Firewall-1-INPUT -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m state --state NEW -m udp --dport 69 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Tue Nov  3 09:53:04 2009
[root@treebeard sysconfig]#

```

```

[root@treebeard sysconfig]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
RH-Firewall-1-INPUT  all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain RH-Firewall-1-INPUT (1 references)
target     prot opt source                destination
ACCEPT    all  --  anywhere              anywhere
ACCEPT    icmp --  anywhere              anywhere          icmp any
ACCEPT    esp  --  anywhere              anywhere
ACCEPT    ah   --  anywhere              anywhere
ACCEPT    udp  --  anywhere              224.0.0.251          udp dpt:mdns
ACCEPT    udp  --  anywhere              anywhere              udp dpt:ipp
ACCEPT    tcp  --  anywhere              anywhere              tcp dpt:ipp
ACCEPT    all  --  anywhere              anywhere              state RELATED,ESTABLISHED
ACCEPT    tcp  --  anywhere              anywhere              state NEW tcp dpt:http
ACCEPT    udp  --  anywhere              anywhere              state NEW udp dpt:tftp
ACCEPT    tcp  --  anywhere              anywhere              state NEW tcp dpt:ssh
REJECT    all  --  anywhere              anywhere              reject-with icmp-host-
prohibited

```

```

[root@treebeard sysconfig]# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

```

## PXE Boot (screen shots with network captures)

```
Network boot from AMD Am79C970A
Copyright (C) 2003-2005 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation

CLIENT MAC ADDR: 00 0C 29 FE 65 79  GUID: 564D70E6-C761-D012-CC14-34C48AFE6579
DHCP. _
```

The VM cannot find boot code on any of the drives so it does a PXE boot.

```
CLIENT MAC ADDR: 00 0C 29 FE 65 79  GUID: 564D70E6-C761-D012-CC14-34C48AFE6579
CLIENT IP: 10.10.10.199  MASK: 255.255.255.0  DHCP IP: 10.10.10.1
GATEWAY IP: 10.10.10.1

PXELINUX 3.11 2005-09-02 Copyright (C) 1994-2005 H. Peter Anvin
UNDI data segment at: 0009C7F0
UNDI data segment size: 2400
UNDI code segment at: 0009ECC0
UNDI code segment size: 0A00
PXE entry point found (we hope) at 9ECC:0106
My IP address seems to be 0A0A0AC7 10.10.10.199
ip=10.10.10.199:10.10.10.1:10.10.10.1:255.255.255.0
TFTP prefix:
Trying to load: pxelinux.cfg/01-00-0c-29-fe-65-79
Trying to load: pxelinux.cfg/0A0A0AC7
Trying to load: pxelinux.cfg/0A0A0AC
Trying to load: pxelinux.cfg/0A0A0A
Trying to load: pxelinux.cfg/0A0A0
Trying to load: pxelinux.cfg/0A0A
Trying to load: pxelinux.cfg/0A0
Trying to load: pxelinux.cfg/0A
Trying to load: pxelinux.cfg/0
Trying to load: pxelinux.cfg/default
_
```

It gets an IP address from the DHCP server then contacts the boot (TFTP) server.



Applications Places System eth2: Capturing - Wireshark CIS 192 Fri Oct 23, 5:44 AM

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	SIP	SP	DIP	DP	Protocol	Info
1	0.000000	10.10.10.198	51535	209.132.176.12	80	TCP	51535 > http [FIN, ACK] Seq=1 Ack=1 Win=436 Len=0 TSV=183920 TSER=174254464
2	0.158029	10.10.10.198	37329	66.35.62.166	80	TCP	37329 > http [FIN, ACK] Seq=1 Ack=1 Win=454 Len=0 TSV=184079 TSER=173863167
3	0.252763	0.0.0.0	68	255.255.255.255	67	UDP	Client Discovery Transaction ID 0x2af6579
4	0.252769	Vmware_a7:73:f1				Broadcast	ARP Who has 10.10.10.199? Tell 10.10.10.1
5	1.172007	10.10.10.1	67	255.255.255.255	68	DHCP	DHCP Offer - Transaction ID 0x2af6579
6	1.703354	Vmware_a7:73:f1				Broadcast	ARP Who has 10.10.10.199? Tell 10.10.10.1
7	2.308898	0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x2af6579
8	2.333960	10.10.10.1	67	255.255.255.255	68	DHCP	DHCP ACK - Transaction ID 0x2af6579
9	2.342474	Vmware_fe:65:79				Broadcast	ARP Who has 10.10.10.17? Tell 10.10.10.199
10	2.342944	10.10.10.1		10.10.10.199		TCP	Echo (ping) request
11	2.343719	Vmware_a7:73:f1				Broadcast	ARP Who has 10.10.10.17? Tell 10.10.10.199
12	2.344493	10.10.10.199	2070	10.10.10.1	69	TFTP	Read Request, File: pxelinux.0/000, Transfer type: octet/000, tsize/000=0/000
13	2.350996	10.10.10.1	48967	10.10.10.199	2070	TFTP	Option Acknowledgement, tsize/000=13148/000
14	2.354510	10.10.10.199	2070	10.10.10.1	48967	TFTP	Error Code, Code: Not defined, Message: TFTP Aborted/000
15	2.354538	10.10.10.199	2071	10.10.10.1	69	TFTP	Read Request, File: pxelinux.0/000, Transfer type: octet/000, blksize/000=1456/000
16	2.369018	10.10.10.1	37756	10.10.10.199	2071	TFTP	Option Acknowledgement, blksize/000=1456/000
17	2.371944	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 0
18	2.373836	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 1
19	2.375740	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 1
20	2.377801	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 2
21	2.378261	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 2
22	2.379655	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 3
23	2.380894	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 3
24	2.381978	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 4
25	2.383549	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 4
26	2.384594	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 5
27	2.386324	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 5
28	2.387046	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 6
29	2.388496	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 6
30	2.389621	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 7
31	2.390521	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 7

Frame 3 (590 bytes on wire, 590 bytes captured)  
 Ethernet II, Src: Vmware\_fe:65:79 (00:0c:29:fe:65:79), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
 User Datagram Protocol, Src Port: bootps (68), Dst Port: bootps (67)  
 Bootstrap Protocol

Shows VM getting IP address and downloading of the **pxelinux.0** boot file.

Applications Places System eth2: Capturing - Wireshark CIS 192 Fri Oct 23, 5:45 AM

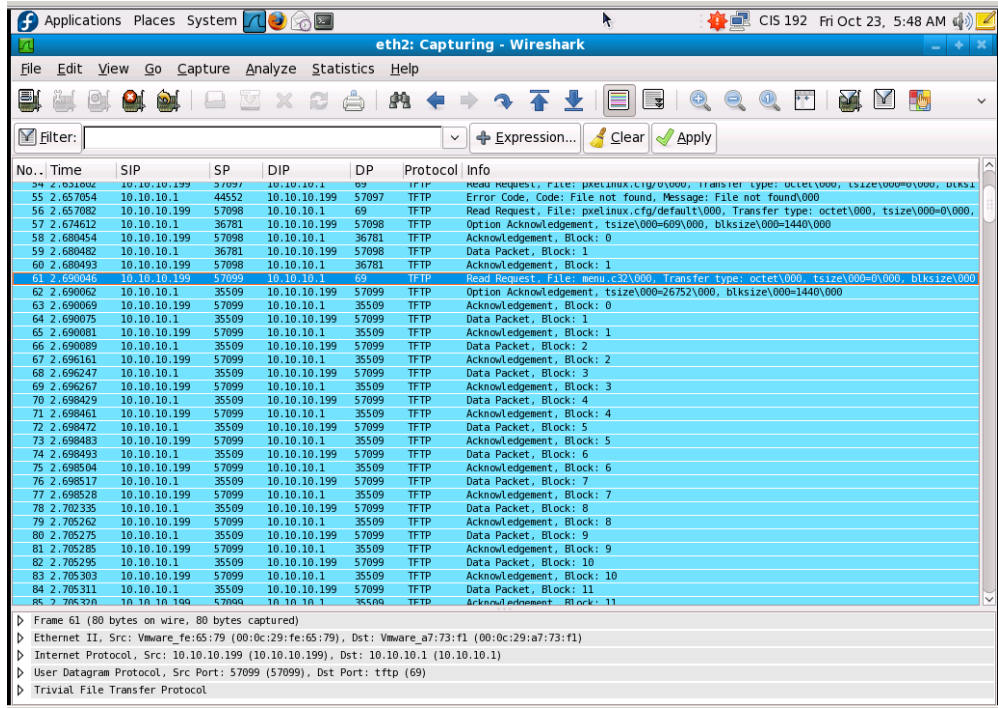
File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

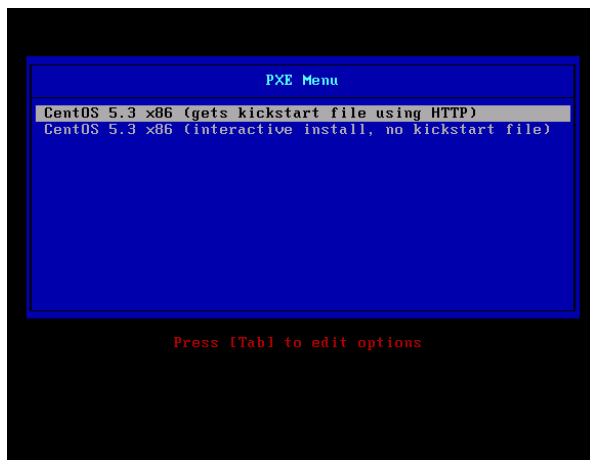
No.	Time	SIP	SP	DIP	DP	Protocol	Info
30	2.389621	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 7
31	2.390521	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 7
32	2.391783	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 8
33	2.393324	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 8
34	2.393985	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 9
35	2.396141	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 9
36	2.397214	10.10.10.1	37756	10.10.10.199	2071	TFTP	Data Packet, Block: 10 (last)
37	2.397547	10.10.10.199	2071	10.10.10.1	37756	TFTP	Acknowledgement, Block: 10
38	2.469559	10.10.10.199	57089	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/01-00-0c-29-fe-65-79/000, Transfer type: octet/000, tsize/000=0/000
39	2.481008	10.10.10.1	53197	10.10.10.199	57089	TFTP	Error Code, Code: File not found, Message: File not found/000
40	2.487063	10.10.10.199	57090	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A00AC7/000, Transfer type: octet/000, tsize/000=0/000
41	2.497699	10.10.10.1	43654	10.10.10.199	57090	TFTP	Error Code, Code: File not found, Message: File not found/000
42	2.503679	10.10.10.199	57091	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A00AC/000, Transfer type: octet/000, tsize/000=0/000, blk
43	2.512101	10.10.10.1	55702	10.10.10.199	57091	TFTP	Error Code, Code: File not found, Message: File not found/000
44	2.517350	10.10.10.199	57092	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A00A/000, Transfer type: octet/000, tsize/000=0/000,
45	2.530015	10.10.10.1	33576	10.10.10.199	57092	TFTP	Error Code, Code: File not found, Message: File not found/000
46	2.533932	10.10.10.199	57093	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A00/000, Transfer type: octet/000, tsize/000=0/000, b
47	2.541706	10.10.10.1	54712	10.10.10.199	57093	TFTP	Error Code, Code: File not found, Message: File not found/000
48	2.549528	10.10.10.199	57094	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A0A/000, Transfer type: octet/000, tsize/000=0/000, bl
49	2.561259	10.10.10.1	45296	10.10.10.199	57094	TFTP	Error Code, Code: File not found, Message: File not found/000
50	2.571063	10.10.10.199	57095	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A0/000, Transfer type: octet/000, tsize/000=0/000, blk
51	2.598432	10.10.10.1	50515	10.10.10.199	57095	TFTP	Error Code, Code: File not found, Message: File not found/000
52	2.607076	10.10.10.199	57096	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0A/000, Transfer type: octet/000, tsize/000=0/000, blk
53	2.631771	10.10.10.1	39752	10.10.10.199	57096	TFTP	Error Code, Code: File not found, Message: File not found/000
54	2.631802	10.10.10.199	57097	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/0/000, Transfer type: octet/000, tsize/000=0/000, blk
55	2.657054	10.10.10.1	44552	10.10.10.199	57097	TFTP	Error Code, Code: File not found, Message: File not found/000
56	2.657082	10.10.10.199	57098	10.10.10.1	69	TFTP	Read Request, File: pxelinux.cfg/default/000, Transfer type: octet/000, tsize/000=0/000,
57	2.674612	10.10.10.1	36781	10.10.10.199	57098	TFTP	Option Acknowledgement, tsize/000=609/000, blksize/000=1440/000
58	2.680454	10.10.10.199	57098	10.10.10.1	36781	TFTP	Acknowledgement, Block: 0
59	2.680482	10.10.10.1	36781	10.10.10.199	57098	TFTP	Data Packet, Block: 1
60	2.680493	10.10.10.199	57098	10.10.10.1	36781	TFTP	Acknowledgement, Block: 1

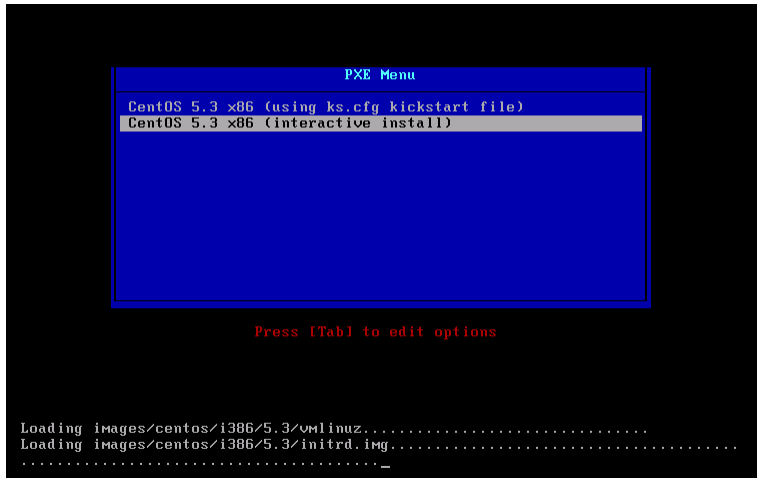
Frame 56 (92 bytes on wire, 92 bytes captured)  
 Ethernet II, Src: Vmware\_fe:65:79 (00:0c:29:fe:65:79), Dst: Vmware\_a7:73:f1 (00:0c:29:a7:73:f1)  
 Internet Protocol, Src: 10.10.10.199 (10.10.10.199), Dst: 10.10.10.1 (10.10.10.1)  
 User Datagram Protocol, Src Port: 57098 (57098), Dst Port: tftp (69)  
 Trivial File Transfer Protocol

Keeps trying (and failing) to download additional files until it downloads the **default** file.



Downloading the **menu.c32** boot file





Applications Places System CIS 192 Fri Oct 23, 6:18 AM

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:  + Expression... Clear Apply

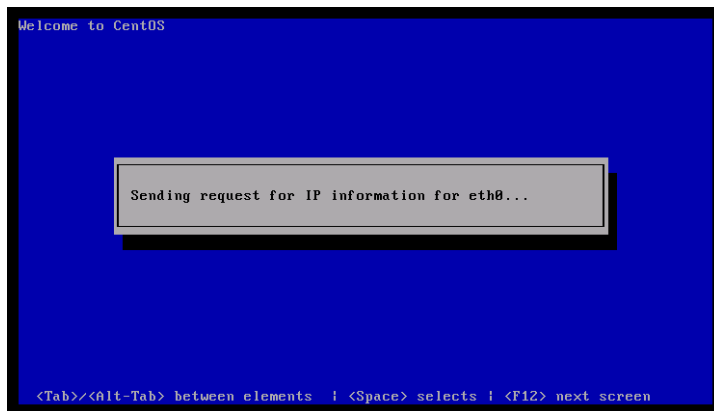
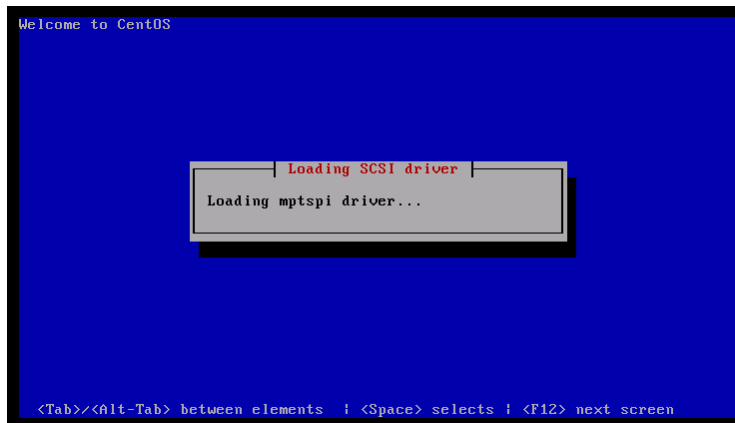
No.	Time	SIP	SP	DIP	DP	Protocol	Info
104	2.460929	10.10.10.199	57100	10.10.10.1	46573	TFTP	Acknowledgement, Block: 1
105	9.450551	Vmware_a7:73:f1		Vmware_fe:65:79		ARP	Who has 10.10.10.199? Tell 10.10.10.1
106	10.097511	10.10.10.199	57101	10.10.10.1	69	TFTP	Read Request (1) Filter: tcp[0:65535] <=> 5.3/vmlinuz[0:0], Transfer Type: octet[0:0], tsize[0:0]
107	10.057689	Vmware_fe:65:79		Vmware_a7:73:f1		ARP	10.10.10.199 is at 00:0c:29:fe:65:79
108	10.064461	10.10.10.1	51662	10.10.10.199	57101	TFTP	Option Acknowledgement, tsize[0:0]=1826484[0:0], blksize[0:0]=1440[0:0]
109	10.065450	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 0
110	10.089446	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 1
111	10.089485	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 1
112	10.090164	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 2
113	10.091174	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 2
114	10.091228	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 3
115	10.091952	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 3
116	10.095231	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 4
117	10.095269	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 4
118	10.097271	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 5
119	10.097290	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 5
120	10.098555	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 6
121	10.098583	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 6
122	10.099518	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 7
123	10.099545	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 7
124	10.101075	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 8
125	10.101103	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 8
126	10.101110	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 9
127	10.101119	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 9
128	10.102252	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 10
129	10.102279	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 10
130	10.105517	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 11
131	10.105552	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 11
132	10.105562	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 12
133	10.105570	10.10.10.199	57101	10.10.10.1	51662	TFTP	Acknowledgement, Block: 12
134	10.110275	10.10.10.1	51662	10.10.10.199	57101	TFTP	Data Packet, Block: 13

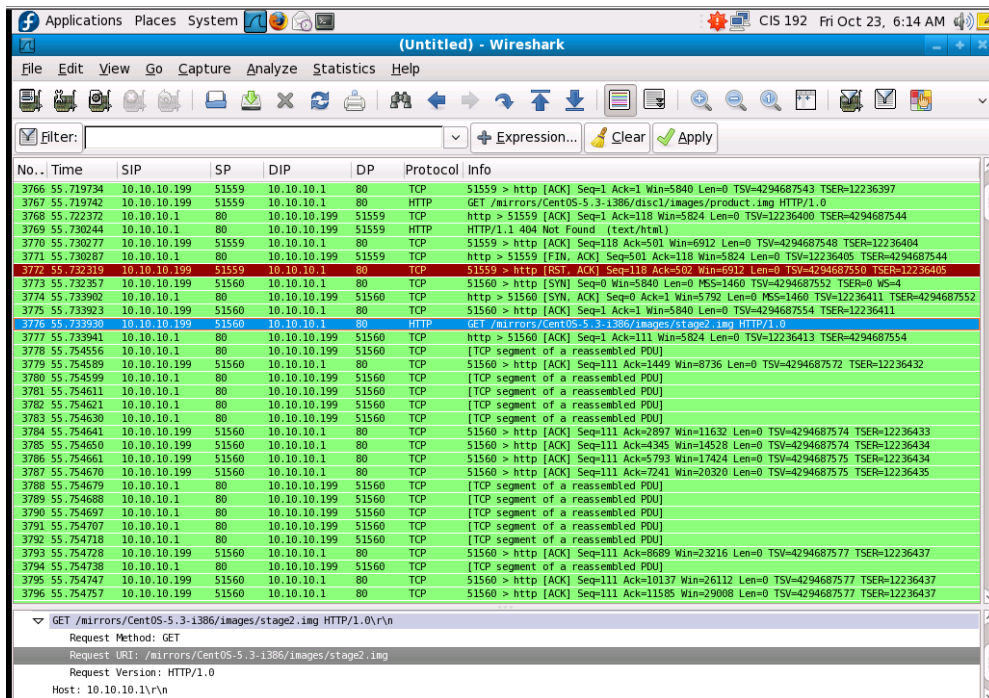
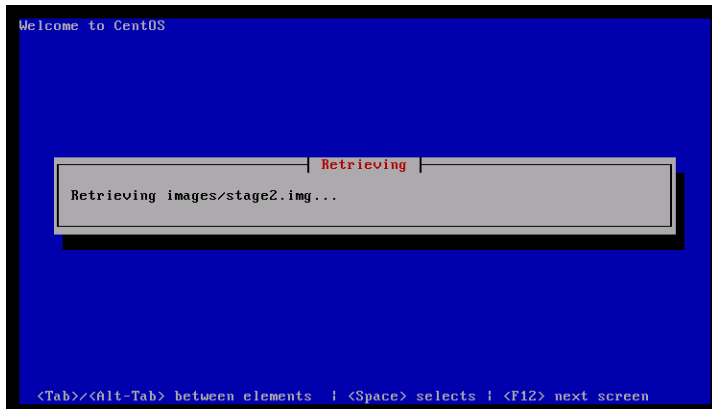
Ethernet II, Src: Vmware\_fe:65:79 (00:0c:29:fe:65:79), Dst: Vmware\_a7:73:f1 (00:0c:29:a7:73:f1)  
 Internet Protocol, Src: 10.10.10.199 (10.10.10.199), Dst: 10.10.10.1 (10.10.10.1)  
 User Datagram Protocol, Src Port: 57101 (57101), Dst Port: tftp (69)  
 Trivial File Transfer Protocol  
 Opcode: Read Request (1)

Retrieving **vmlinuz** using TFTP.

```
ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Processor #0 15:2 APIC version 17
ACPI: LAPIC_NMI (acpi_id[0x00] high edge lint[0x1])
ACPI: IOAPIC (id[0x01] address[0xfec00000] gsi_base[0])
IOAPIC[0]: apic_id 1, version 17, address 0xfec00000, GSI 0-23
ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 high edge)
Enabling APIC mode: Flat. Using 1 I/O APICs
Using ACPI (MADT) for SMP configuration information
Allocating PCI resources starting at 30000000 (gap: 20000000:dec00000)
Detected 2592.947 MHz processor.
Built 1 zonelists. Total pages: 131072
Kernel command line: initrd=images/centos/i386/5.3/initrd.img ks ip=dhcp BOOT_I
MAGE=images/centos/i386/5.3/vmlinuz
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Initializing CPU#0
CPU 0 irqstacks, hard=c0754000 soft=c0734000
PID hash table entries: 4096 (order: 12, 16384 bytes)
Console: colour VGA+ 80x25
Dentry cache hash table entries: 65536 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 5, 131072 bytes)
Memory: 508064k/524288k available (2122k kernel code, 14792k reserved, 884k data
, 228k init, 0k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
-
```

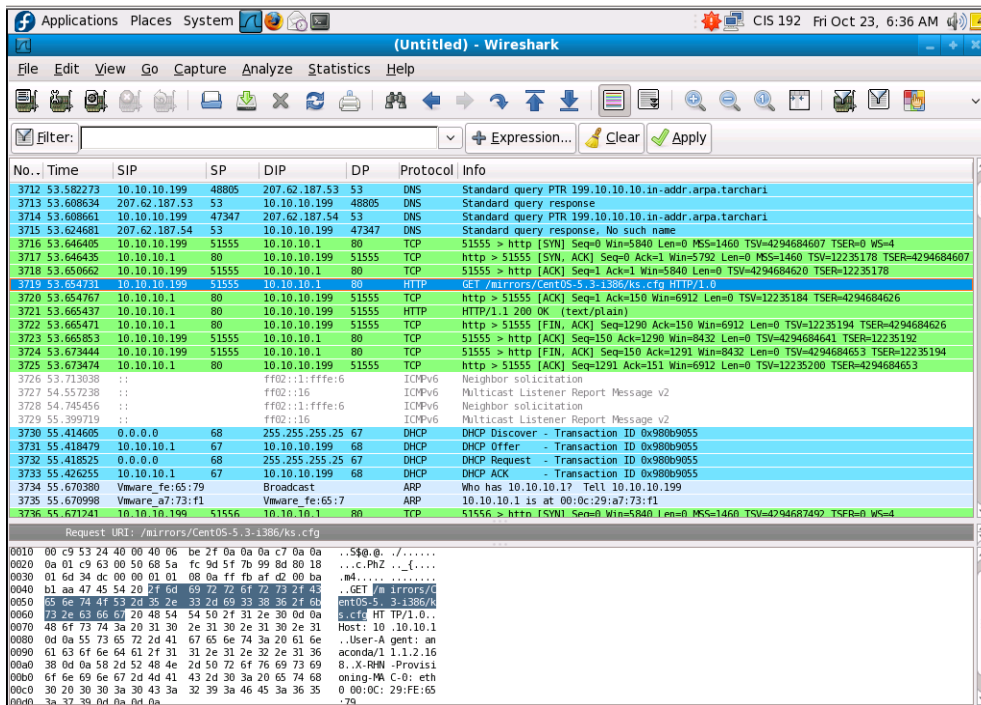
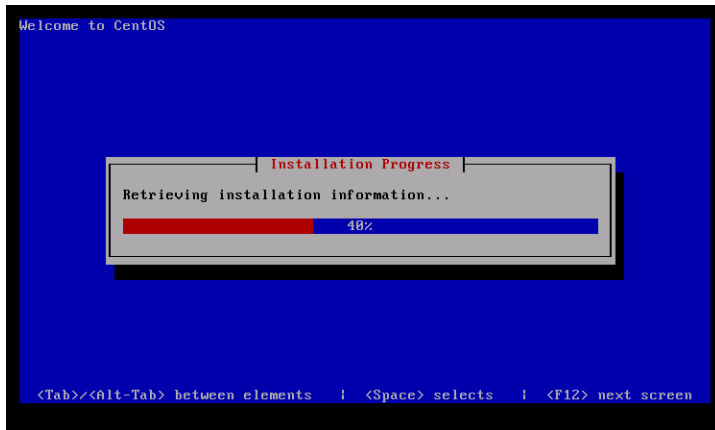
## Loading kernel



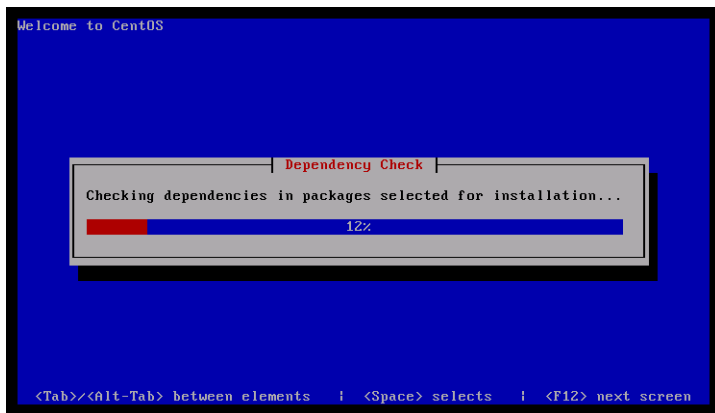


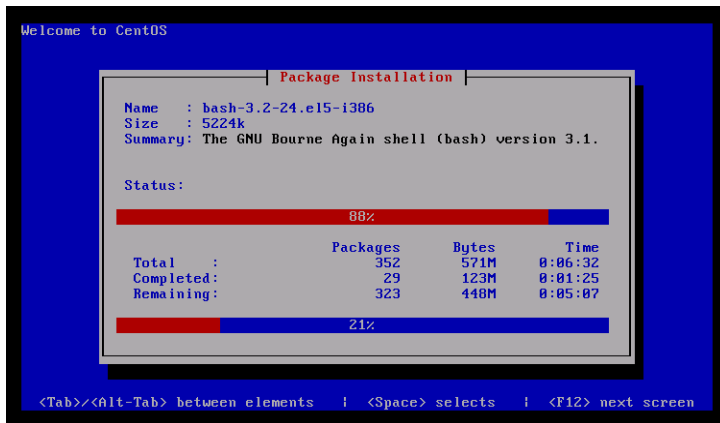
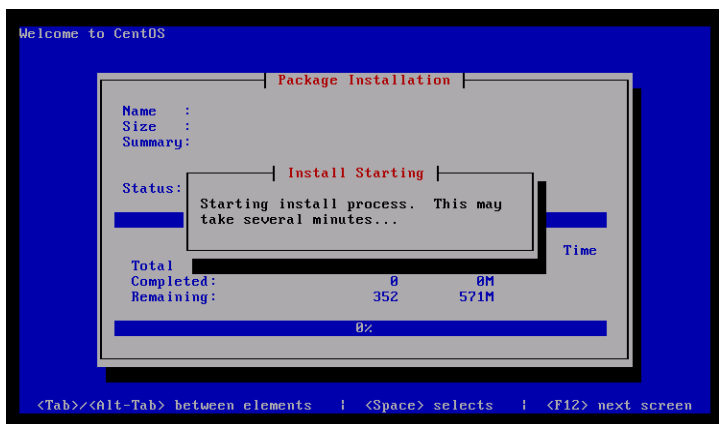
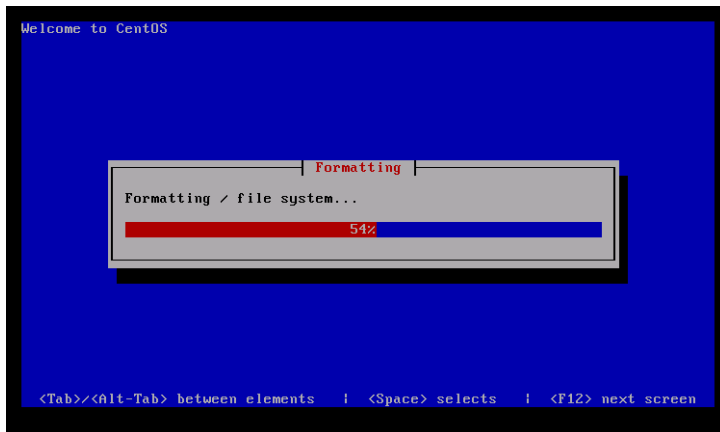
Retrieving /mirrors/CentOS-5.3-i386/images/stage2.img file using HTTP





Retrieving **ks.cfg** kickstart file using HTTP





Applications Places System (Untitled) - Wireshark CIS 192 Fri Oct 23, 6:31 AM

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	SIP	SP	DIP	DP	Protocol	Info
22933	163.050658	10.10.10.199	51691	10.10.10.1	80	TCP	51691 > http [ACK] Seq=211 Ack=6979 Win=20320 Len=0 TSV=4294790798 TSER=12326265
22934	163.050667	10.10.10.1	80	10.10.10.199	51691	TCP	http > 51691 [FIN, ACK] Seq=6979 Ack=211 Win=6912 Len=0 TSV=12326266 TSER=4294790797
22935	163.050665	10.10.10.199	51691	10.10.10.1	80	TCP	51691 > http [FIN, ACK] Seq=211 Ack=6980 Win=20320 Len=0 TSV=4294790805 TSER=12326266
22936	163.072855	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=4294790817 TSER=0 MS=4
22937	163.074186	10.10.10.1	80	10.10.10.199	51691	TCP	http > 51691 [ACK] Seq=6980 Ack=212 Win=6912 Len=0 TSV=12326271 TSER=4294790805
22938	163.074405	10.10.10.1	80	10.10.10.199	51692	TCP	http > 51692 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=12326271 TSER=4294790817
22939	163.076298	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=4294790819 TSER=12326271
22940	163.076329	10.10.10.199	51692	10.10.10.1	80	HTTP	GET /mirrors/centos-5.3-1386/CentOS/bash-3.2-24.el5.i386.rpm HTTP/1.1
22941	163.077867	10.10.10.1	80	10.10.10.199	51692	TCP	http > 51692 [ACK] Seq=1 Ack=203 Win=6912 Len=0 TSV=12326274 TSER=4294790820
22942	163.091609	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22943	163.091615	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22944	163.091618	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=1449 Win=8736 Len=0 TSV=4294790825 TSER=12326277
22945	163.091621	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22946	163.091623	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=2897 Win=11632 Len=0 TSV=4294790825 TSER=12326278
22947	163.091624	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=4345 Win=14528 Len=0 TSV=4294790826 TSER=12326278
22948	163.091625	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22949	163.091626	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22950	163.091627	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=5793 Win=17424 Len=0 TSV=4294790827 TSER=12326279
22951	163.091895	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22952	163.091907	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=7241 Win=20320 Len=0 TSV=4294790827 TSER=12326279
22953	163.091916	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=8689 Win=23216 Len=0 TSV=4294790827 TSER=12326279
22954	163.091924	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22955	163.091933	10.10.10.1	80	10.10.10.199	51692	TCP	[TCP segment of a reassembled PDU]
22956	163.091942	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=10137 Win=26112 Len=0 TSV=4294790828 TSER=12326281
22957	163.091951	10.10.10.199	51692	10.10.10.1	80	TCP	51692 > http [ACK] Seq=203 Ack=11585 Win=29008 Len=0 TSV=4294790829 TSER=12326281

Request URI: /mirrors/CentOS-5.3-1386/CentOS/bash-3.2-24.el5.i386.rpm

```

0040 15 7f 47 45 54 20 1f 6d 69 72 72 6f 72 73 2f 43 ..GET /m irrors/C
0050 5c 0c 74 41 53 2d 35 2e 33 2d 69 33 38 36 2f 43 centOS-5.3-1386/C
0060 65 6e 74 4f 53 2f 62 61 73 68 2d 33 2e 32 2d 32 entOS/ba sh-3.2-2
0070 34 2e 65 6c 35 2e 69 33 38 36 2e 72 70 6d 20 48 4.el5.i386.rpm #
0080 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 70 74 2d TTP/1.1. .Accept-
0090 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e 74 69 Encoding : identI
00a0 74 79 0d 0a 52 61 6e 67 65 3a 20 62 79 74 65 73 ty, Rang e: bytes
00b0 3d 34 34 30 2d 35 37 33 34 30 0d 0a 43 6f 6e 6e =440-573 40. Conn
00c0 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 48 ection: close. H
00d0 6f 73 74 3a 20 31 30 2e 31 30 2e 31 30 2e 31 0d ost: 10.10.1.
00e0 0a 55 73 65 72 2d 61 67 65 6e 74 3a 20 75 72 6c User-ag ent: url
00f0 67 72 61 62 62 65 72 2f 33 2e 31 2e 30 20 79 75 grabber/ 3.1.0 yu
0100 64 7e 32 7a 27 27 21 30 0a 0a 0a 0a
  
```

Retrieving bash package via HTTP

```

Welcome to CentOS

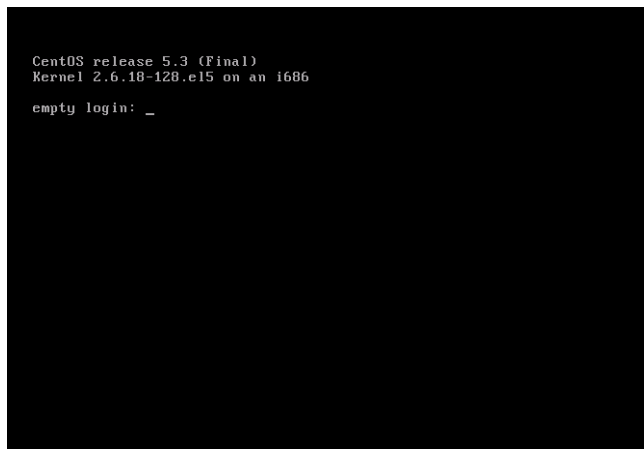
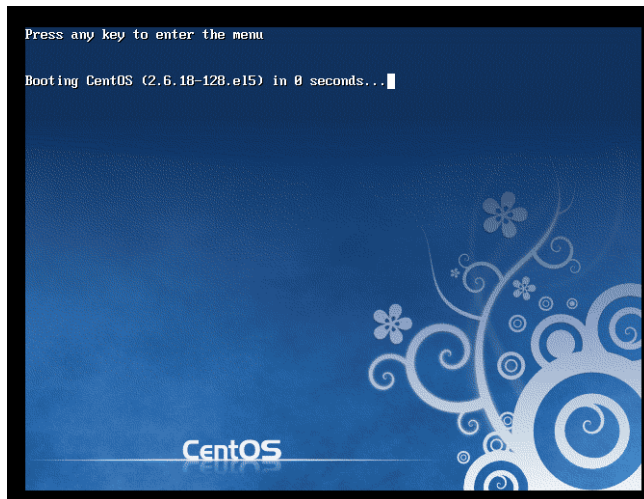
          Bootloader
    -----
    Installing bootloader...

<Tab><Alt-Tab> between elements | <Space> selects | <F12> next screen
  
```

```

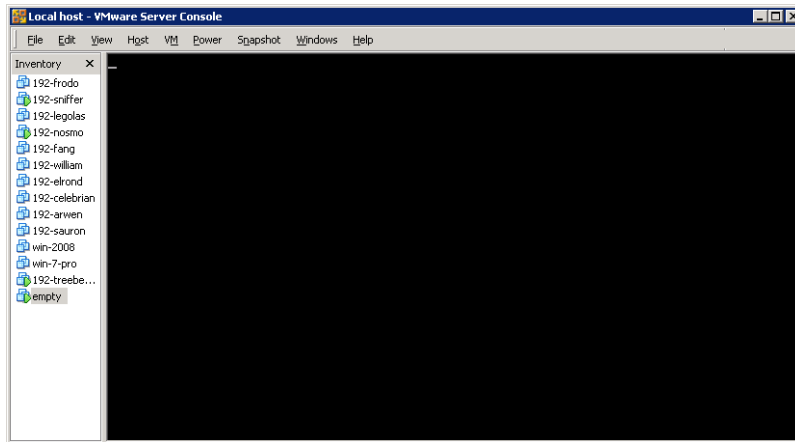
sending termination signals...done
sending kill signals...done
disabling swap...
/dev/mapper/VolGroup00-LogVol01
unmounting filesystems...
/mnt/runtime done
disabling /dev/loop0
/proc done
/dev/pts done
/sys done
/tmp/ramfs done
/selinux done
/mnt/sysimage/boot done
/mnt/sysimage/sys done
/mnt/sysimage/proc done
/mnt/sysimage/selinux done
/mnt/sysimage/dev done
/mnt/sysimage done
rebooting system
-
  
```





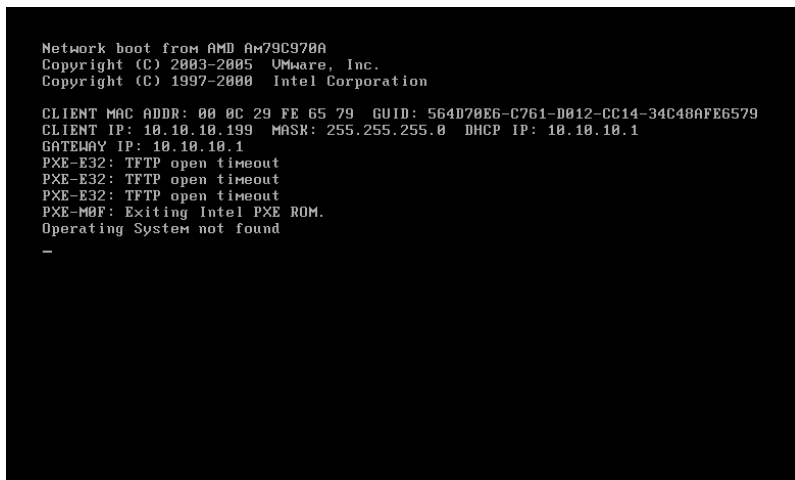
## Troubleshooting

Problem: Your installation did not complete successfully and the Empty VM will no longer boot using PXE mode. All you have is a back screen with the cursor blinking.



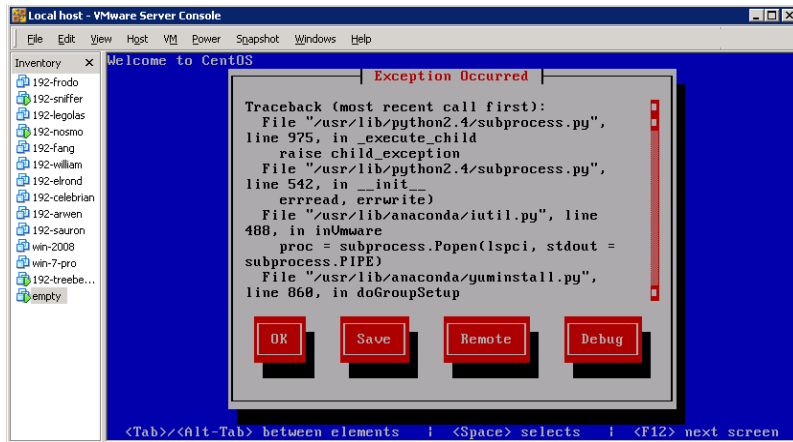
Workaround: You probably got the MBR setup but no OS installed. To force a PXE boot, reset the Empty VM, quickly click inside the VM during the BIOS boot sequence and then press the F12 function key. You have about 2 seconds to do this so don't dawdle.

Problem: TFTP times out trying to download boot files.



Workaround: Make sure your firewall has UDP port 69 open and SELinux is disabled.

Problem: Installation fails with an exception.

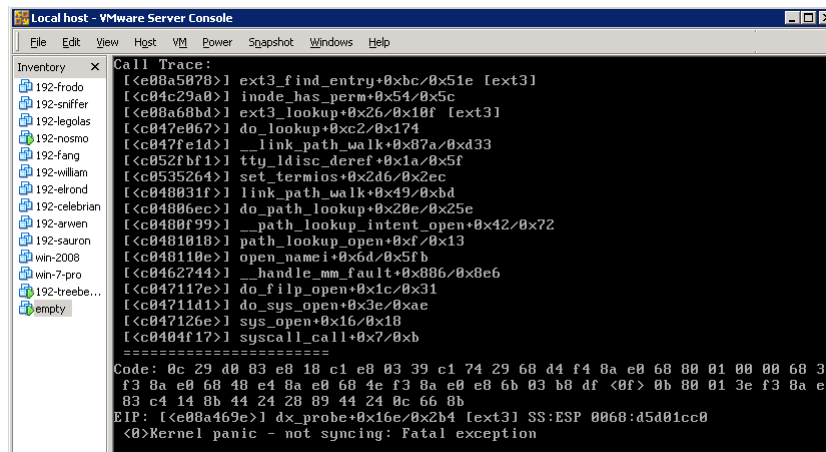


Workaround: Make sure your memory on the Empty VM is at least 384MB

## Nuking a Linux System Observations

I ended up re-installing the Empty VM several times to play with different PXE and kernel command line combinations. Here are some of the commands that you normally would NEVER use on a real system! The second method was the easiest and fastest.

- **rm -rf /**
  - This leaves the MBR and swap partition intact. Most of the files are deleted from the / partition however not all. bash is still running and you can navigate what is left of the file tree using shell built-in echo \* and cd commands.
- **dd if=/dev/zero of=/dev/sda bs=512 count=1 sync**
  - Blows away the MBR. Use the sync command to force the write to disk of the buffered zero's.
- **dd if=/dev/zero of=/dev/sda**
  - Zeros out hard drive which results eventually in a Kernel Panic:



## References

### CentOS PXE Setup

- [http://wiki.centos.org/HowTos/PXE/PXE\\_Setup](http://wiki.centos.org/HowTos/PXE/PXE_Setup)

### SYSLINUX

- <http://syslinux.zytor.com/wiki/index.php/SYSLINUX>

### Fedora Anaconda/Kickstart

- <http://fedoraproject.org/wiki/Anaconda/Kickstart>

### RedHat EL4 Kickstart Options

- <http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/s1-kickstart2-options.html>

### Intel PXE 2.1 Specification

- <http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf>

### Setting up a PXE-Boot Server (Net Llama!)

- [http://linux-sxs.org/internet\\_serving/pxeboot.html](http://linux-sxs.org/internet_serving/pxeboot.html)