**CSCI 2930: Practical System Administration**

**Final Project**

**Spring 2014**

You have been tasked with setting up a small Development environment for an application development team. You have only one physical server to do this with. As such, it will be up to you to deploy a virtual environment containing:

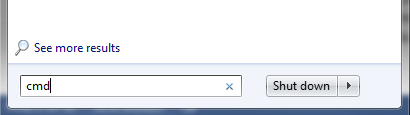
* Firewall/Router - pfSense virtual appliance that will be protecting your systes based on a set of rules you can configure.
* Windows 2008 R2 DHCP server - Easy to use graphical interface. Will hand out IP addresses to any clients connected to your private network.
* FreeBSD-based BIND DNS server - Internal name server running the latest ISC version of the BIND software. It will act as your internal master DNS server and forward any requests it does not know about to the firewall to be passed on to outside DNS systems.
* CentOS graphical Workstation for testing and management.

Total Completion Time is 2 Hours and 35 min at the shortest.

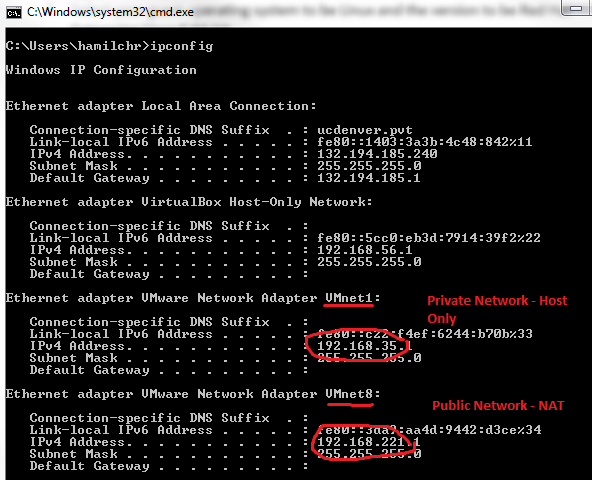
When creating new guest VM’s and installing their operating systems you may want to have all other VM’s turned off so your hard drive runs at its peak in order to get the OS files copied as quickly as possible.

The DHCP section is the most difficult as it requires ZERO typing errors to get working properly. You will most likely need to come in outside of class to complete this project.

1. Plan your deployment (Time to complete: 5 min)
   1. Open start menu on your host and type cmd in the search bar and hit enter



* 1. Type ipconfig in the command window and hit enter



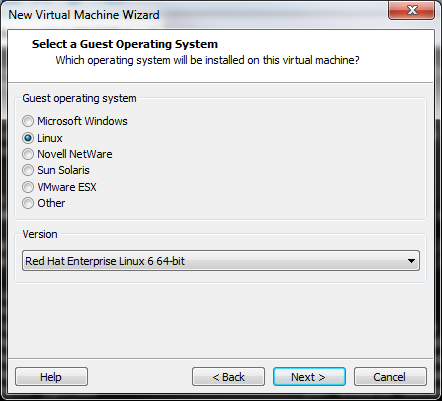
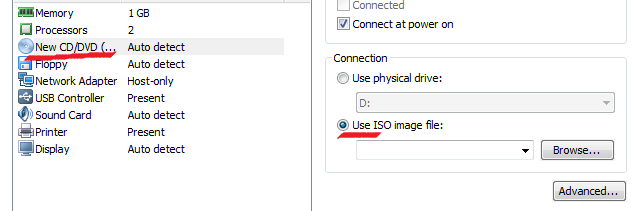
* 1. What is the Network address for your Host Only virtual network VMnet1 (referred to from this point forward as the “Private Network”)? 192.168.211.1
  2. What is the Network address for your NAT virtual network VMnet8 (referred to from this point forward as the “Public Network”)? 192.168.13.1

Based on the above information, fill in the blanks below with the private IP addresses that your servers will have:

* 1. Firewall Private network ip address 192.168.211.5
  2. DHCP Server Private Address 192.168.211.10
     1. DHCP SCOPE NAME: CSCI\_DEVEL
     2. DHCP SCOPE Starting IP Address: 192.168.211.128
     3. DHCP SCOPE Ending IP Address: 192.168.211.254
     4. DHCP SCOPE Subnet mask: 255.255.255.0
     5. DHCP SCOPE Default Gateway: 192.168.211.5
  3. FreeBSD DNS server Private address 192.168.211.15
  4. CentOS Workstation Private network address 192.168.211.20

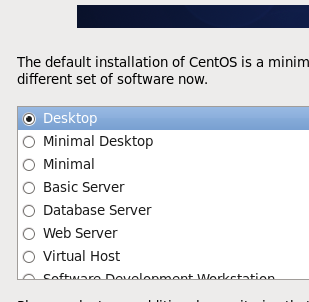
1. Deploy CentOS 6.5 graphical workstation with GNOME window manager

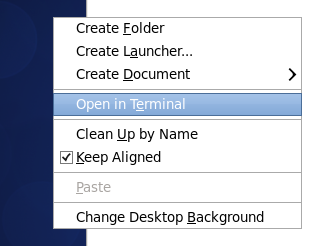
(Time to complete: 20 min)

* 1. Open VMware Workstation and click File -> New Virtual Machine
  2. Click the radio button next to Custom
  3. Click Next
  4. Verify it is a Workstation 10 Hardware compatibility and click Next
  5. Select the Radio Button next to I will install the operating system later and click next
  6. Select your guest operating system to be Linux and the version to be Red Hat Enterprise Linux 6 64-bit 
  7. Change the virtual machine name to be CentOS64\_Workstation and click next
  8. Select 1 processor and 2 cores click next
  9. Select 1024 MB of memory click next
  10. Select Host-only networking and click next
  11. Click next (LSI Logic)
  12. Click next (SCSI)
  13. Click next (Create new virtual disk)
  14. Click Next (Max Disk size 20GB and Split virtual disk into multiple files)
  15. Click Next (Disk Name)
  16. Click Customize hardware
  17. Click on New CD/DVD and select the radio button next to use ISO image file and click browse 
  18. Browse to \\milo\StudentSoftware\CentOS and select CentOS-6.5-x86\_64-bin-DVD1.iso and click Open
  19. Close the Hardware customization window
  20. Click Finish
  21. Click Power on this virtual machine



* 1. When the boot menu comes up just hit enter
  2. Select Skip and hit enter
  3. Click Next (English)
  4. Click Next (US English)
  5. Click Next (Basic Storage)
  6. Click Yes Discard any data
  7. Set hostname to be centos65.csci.pvt click next
  8. Select America/Denver for the timezone city and click Next
  9. Enter the root password as 12345678 and click next and click Use Anyway
  10. Select Use All Space and click Next
  11. Write Changes to disk
  12. Click on the Desktop radio button and click next



* 1. Installation will begin.
  2. Click Reboot after it is done.
  3. Click Forward
  4. Click Forward (License)
  5. Click Forward and then Yes to tell the system you don’t want to make another user
  6. Set the time and click Forward
  7. Click Finish (ignore the error regarding Kdump)
  8. Log in as root
  9. Right click on the desktop background and select Open in Terminal 
  10. cd to /etc/sysconfig/network-scripts
  11. Make a backup of the original eth0 configuration file using the copy command:
      1. # cp ifcfg-eth0 ifcfg-eth0.dhcp.bak
  12. edit ifcfg-eth0 using either vi or nano to look like this (filling the blanks in with you private subnet address):

TYPE=Ethernet

DEVICE=eth0

BOOTPROTO=static

ONBOOT=yes

IPADDR=192.168.\_\_\_\_\_\_.20

NETMASK=255.255.255.0

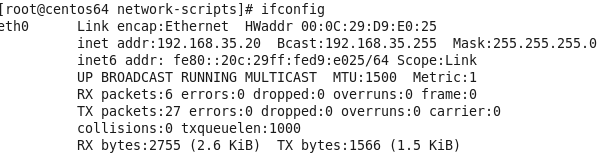
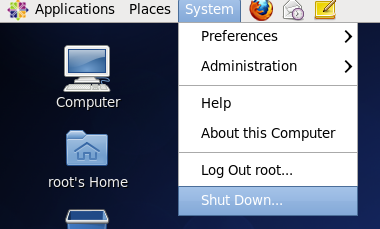
GATEWAY=192.168.\_\_\_\_\_\_\_.5

DNS1=192.168.\_\_\_\_\_\_.15

DOMAIN="csci.pvt"

DEFROUTE=yes

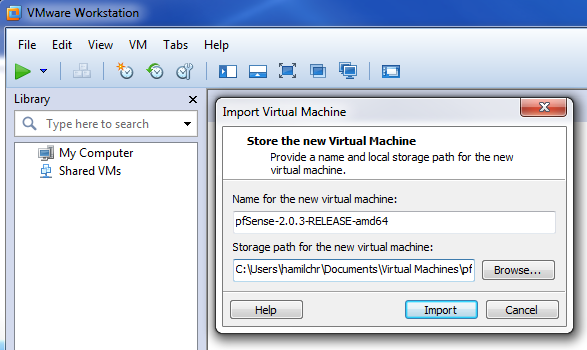
NAME="eth0"

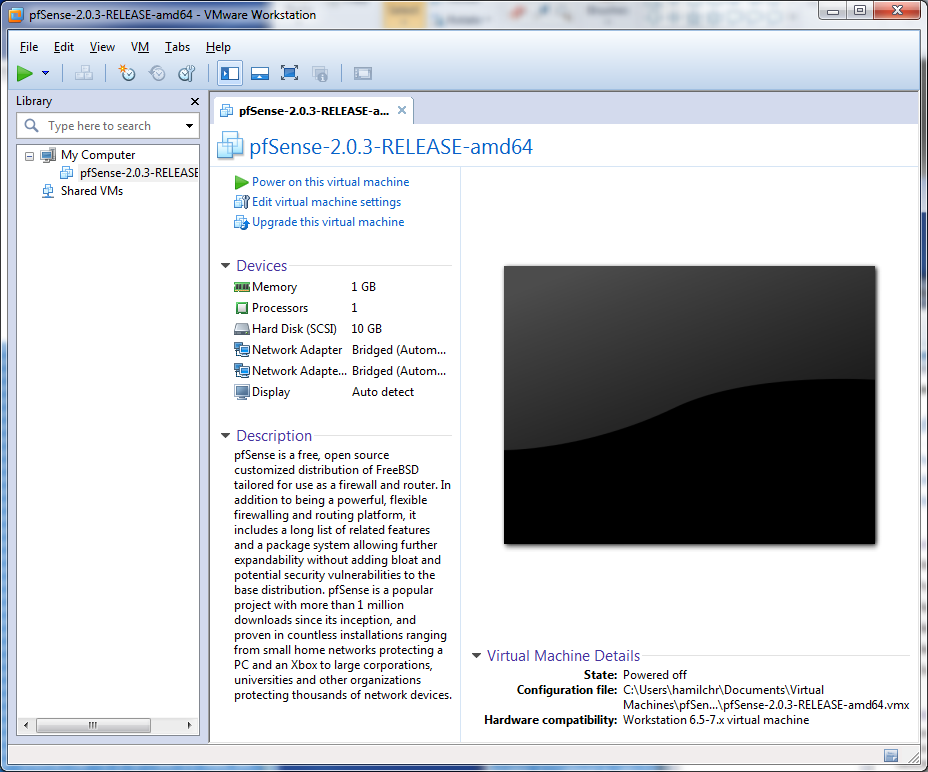
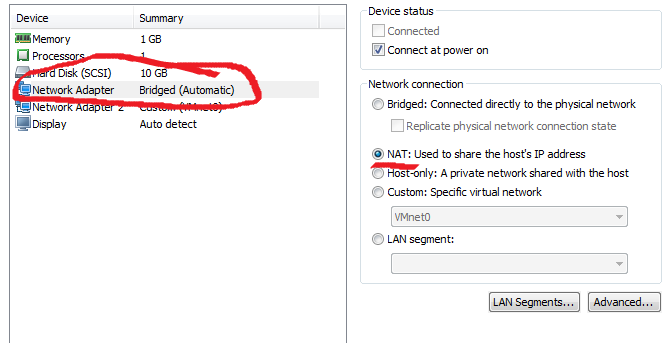
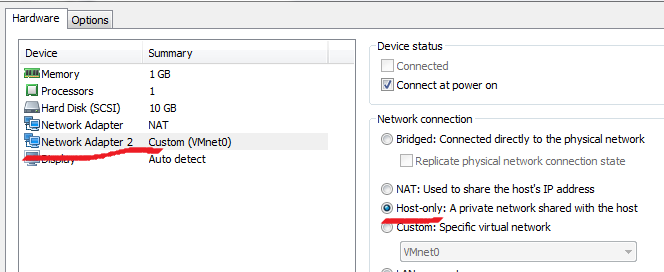
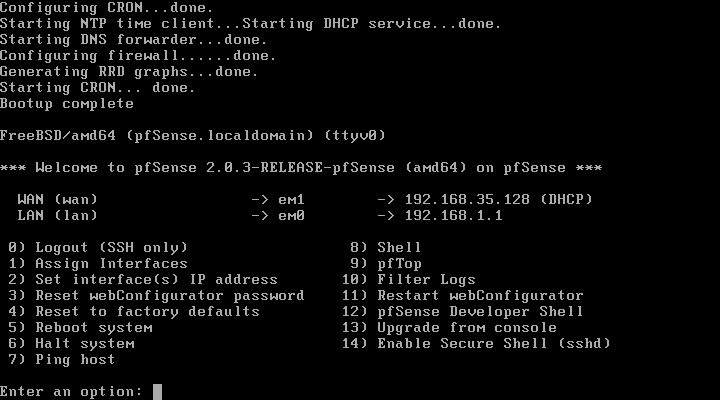
* 1. Save changes to file and quit back to the command line
  2. Issue the command “service network restart” to restart networking and read the new config file
  3. Use the ifconfig command to make sure your configuration changes took place 
  4. Shutdown your CentOS 6.4 system 

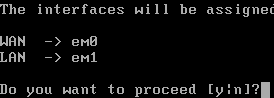
1. Deploy Firewall OVA Appliance for protection of your new environment

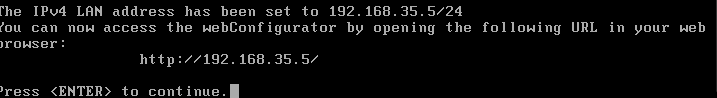
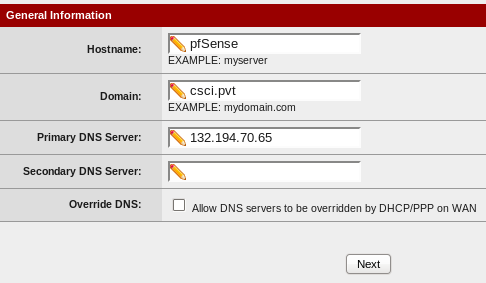
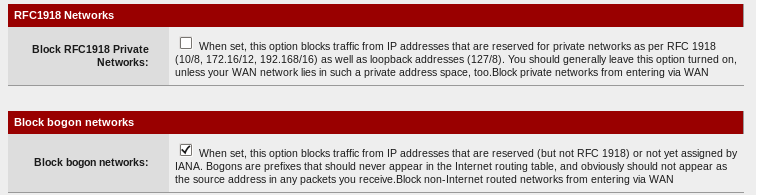
(Time to complete: 20 min)

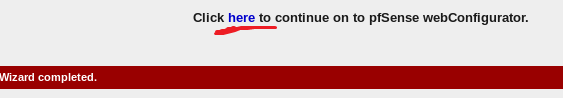
* 1. Browse to the file [\\milo\StudentSoftware\pfSense\pfSense-2.0.3-RELEASE-amd64.ova](file:///\\milo\StudentSoftware\pfSense\pfSense-2.0.3-RELEASE-amd64.ova) and double-click it.
     1. This will open VMware Workstation (it will be simulating your VMware vSphere DR server) and start the appliance import wizard



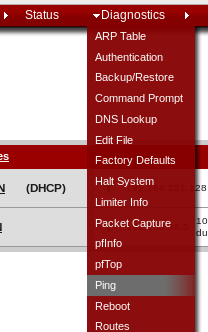
* 1. Click on the import button
  2. When the license agreement pops up click on Accept and wait until the appliance is done importing  
       
     
  3. You will see the above screen after the appliance has been imported. Click on “Edit virtual machine settings”
  4. Select the hardware device called Network Adapter and set it to use the NAT network
  5. Select the hardware device called Network Adapter 2 and set it to use the Host-only network
  6. Close the VM settings window and click Power on this virtual machine
  7. After the firewall boots you will see the management console. Type 1 for Assign Interfaces to properly set your WAN (public interface) and LAN (private interface) devices 
  8. Answer n for No to setting up VLANS
  9. You will then be asked to enter the interface to use for the WAN. Type em0 and hit enter
  10. For the LAN interface type em1 and hit enter
  11. When asked to enter an optional interface do not type anything just hit the enter key
  12. You should then see the summary of what you are going to set. It should look like this



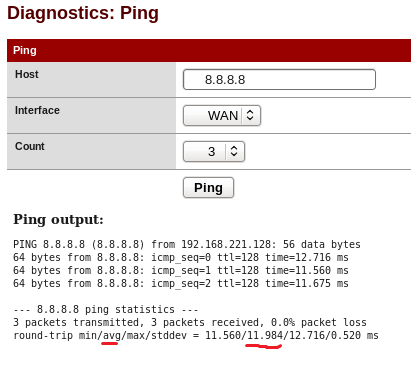
* 1. Type y to proceed
  2. Your WAN interface should now have a DHCP address from your Host Only or Public Network. If not first reboot the system and if still not properly configured redo the configuration but switch the assignment of the NICS
  3. We now need to set an address for the LAN interface. Type 2 to Set Interface IP Address
  4. Select the LAN interface by typing 2 and hitting enter
  5. Enter the IP address you wrote down in 1(e) of this document
  6. Enter your number of bits for your subnet mask
  7. Say n for No to the question “Do you want to enable DHCP server on LAN?”
  8. Say y to the webConfigurator protocol question
  9. You will now see a summary similar to the one below including the web address of your firewall where you will be able to login to finish the configuration
  10. Power on you CentOS workstation if it is off and connect to the internal web address of your firewall (<http://192.168._____.5>) using the Firefox web browser 
  11. Login to the pfSense firewall with the default credentials login: admin password: pfsense
  12. Go through the initial configuration setting the following fields:
      1. Hostname: pfSense
      2. Domain: csci.pvt
      3. Primary DNS: 132.194.70.65
      4. Uncheck Allow DNS servers to be overridden by DHCP 
      5. Time Server Hostname: 132.194.10.82
      6. Timezone: America\Denver 
      7. Leave the WAN interface configuration to DHCP but uncheck Block RFC1918 Private Networks 
      8. Leave your LAN address as 192.168.211.5 and the subnet mask 24 bits
      9. Set the admin password to 12345678 and click next
      10. click reload to load the new configuration into the firewall
      11. After the reload click on the “click here to go to the webconfigurator”



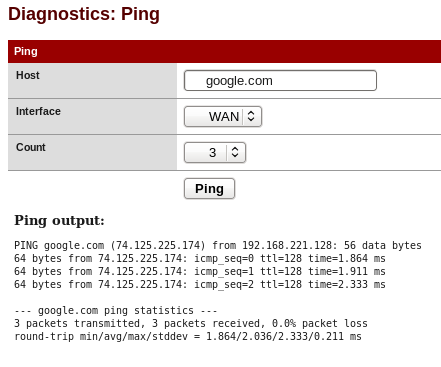
* + 1. Click on Diagnostics -> Ping



* + 1. Enter 8.8.8.8 as the host to ping and click on the ping button. You should see 3 successful pings. What was your average ping time? 12.004 ms



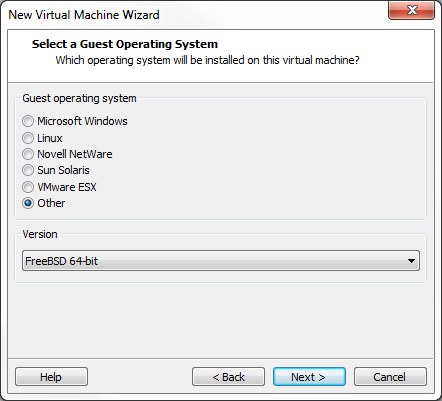
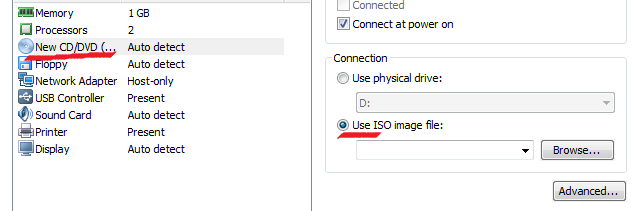
* + 1. Now try to ping google.com. What was your average ping time? 1.896 ms



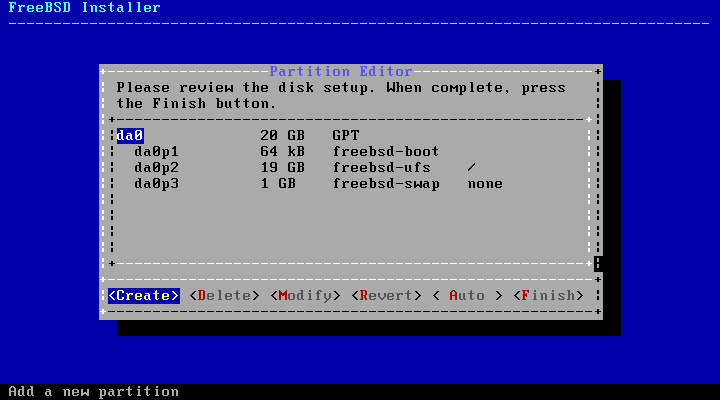
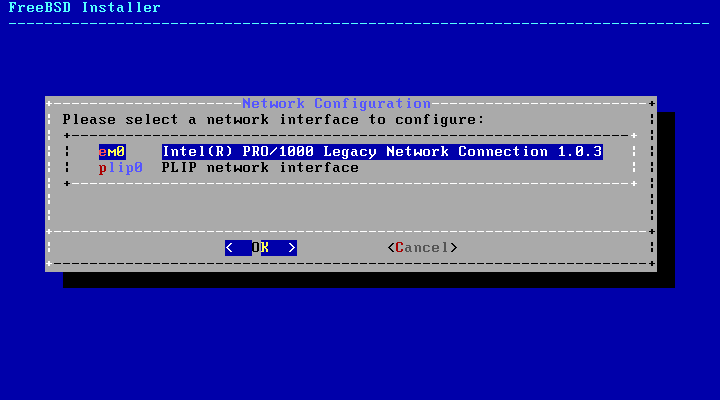
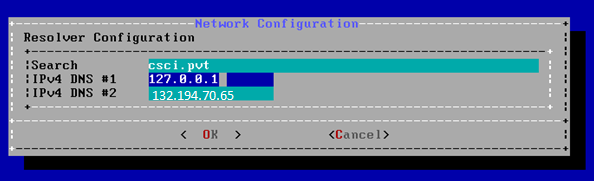
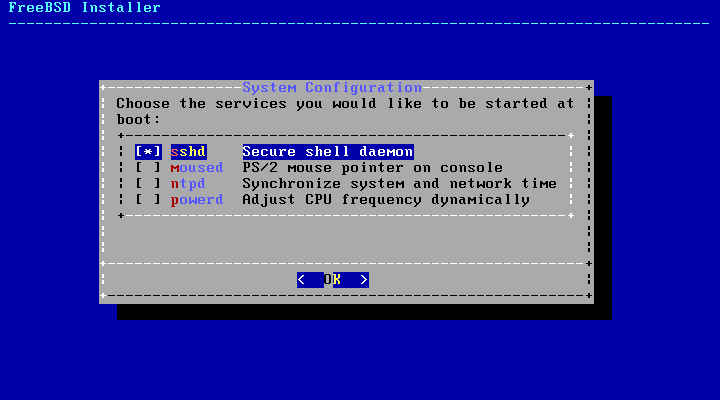
* + 1. Open up a terminal on the CentOS workstation and try to ping 8.8.8.8   
       Let a few pings go through and then hit control-c to stop the pings. What was your average ping time from the CentOS system? 12.054 ms (note: pinging google.com will not work yet.)

1. Deploy a FreeBSD DNS server (Time to complete: 60 min): You will be deploying an Internet Systems Consortium (ISC) BIND (Berkeley Internet Name Domain) server. BIND is the most widely used DNS server application on the Internet. The domain name system is responsible for the conversion of domain names such as <http://www.google.com> to its routable IP address like 74.125.225.180. It is considered one of the most critical components of the Internet.

Your server will be what is called a local master authoritative name server for your development domain. The system will have a small zone file (a list of known IP addresses) for your domain as well as act as a forwarder for any requests it does not specifically know about. When a DNS query is received for your domain BIND looks at your zone file and returns the requested information. If the query is for a domain other than yours, the query is forwarded to other DNS specified in your forwarder’s configuration.

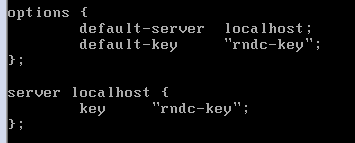
* 1. Open VMware Workstation and click File -> New Virtual Machine
  2. Click the radio button next to Custom
  3. Click Next
  4. Verify it is a Workstation 10 Hardware compatibility and click Next
  5. Select the Radio Button next to I will install the operating system later and click next
  6. Select your guest operating system to be Other and the version to be FreeBSD 64-bit  
      
  7. Change the virtual machine name to be FreeBSD\_DNS and click next
  8. Select 1 processor and 2 cores click next
  9. Select 512 MB of memory click next
  10. Select Host-only networking and click next
  11. Click next (LSI Logic)
  12. Click next (SCSI)
  13. Click next (Create new virtual disk)
  14. Click Next (Max Disk size 20GB and Split virtual disk into multiple files)
  15. Click Next (Disk Name)
  16. Click Customize hardware
  17. Click on New CD/DVD and select the radio button next to use ISO image file and click browse 
  18. Browse to \\milo\StudentSoftware\FreeBSD and select FreeBSD-10.0-RELEASE-amd64-dvd1.iso and click Open
  19. Close the Hardware Customization window
  20. Click Finish
  21. Click Power on this virtual machine



* 1. When the boot menu comes up just hit enter
  2. Select Install
  3. Hit Continue to select the Default keymap.
  4. Enter ns1.csci.pvt as the hostname
  5. **Uncheck GAMES AND PORTS** but leave lib32 checked (arrow down and hit Space).
  6. Use guided partitioning
  7. Select the Entire Disk
  8. Select Finish and the Commit 
  9. The OS will begin to install 
  10. Set Root password to 12345678
  11. Network Configuration:
      1. Select em0 click ok 
      2. Yes to configure IPv4
      3. No to using DHCP
      4. IP Address 192.168.211.15
      5. Subnet mask 255.255.255.0
      6. Gateway 192.168.211.5
      7. Say no to IPv6 configuration
      8. Resolver configuration set csci.pvt for the Search and 127.0.0.1 as the DNS #1 since we want our system to look to itself and also include 132.194.70.65 as DNS#2
  12. Set time America (2) -> United States (49) -> Mountain (18)
  13. Check sshd to start at boot and uncheck Crash Dumps.
  14. do not add other user accounts
  15. Exit the installer
  16. No to manual configuration
  17. Reboot
  18. login as root
  19. Check that /etc/rc.conf has your hostname ns1.csci.pvt and your ip address 192.168.211.15 (you can use a text editor or ‘cat’)
  20. ping 8.8.8.8 to verify network is working
  21. ping google.com to verify DNS is working
  22. Install BIND 9.9 with the pkg install command.
      1. First, install pkg:
         1. # pkg
         2. Select yes when asked if you want to install.
      2. # pkg install bind99
      3. BIND uses a utility called “rndc,” which allows command line administration of the “named” daemon (which is your DNS service). Rndc uses a shared secret key authentication method to prevent unauthorized access to the “named” daemon. As such, we’ll need to create and configure this key:
         1. # rndc-confgen –a
            1. This command generates the “rndc.key” file with an encrypted secret.
         2. # ee /usr/local/etc/namedb/rndc.key
            1. This will open the key file you just generated. Note down its EXACT contents – we need to copy this over to a configuration file. Exit the text editor when you’re finished.
         3. Next, we’ll open the configuration file and have it use the same shared secret key:
            1. # ee /usr/local/etc/namedb/rndc.conf
            2. Scroll through the page to the section that says “options.”
            3. Change the line that says “default-key” to read:

Default-key “rndc-key”;

* + - * 1. Scroll down to the “server localhost” section.
        2. Change the line that says “key” to read:

Key “rndc-key”;  
  


* + - * 1. Scroll down to the bottom of the file and add the entire contents of the rndc.key file to the endgNuNUZu97BQZzUd+v6DH/g==  
             
           The secret for your file will be different, as it’s randomly generated each time.
        2. Save and exit your text editor.
    1. Now let’s move forward with the DNS configuration:
    2. # ee /usr/local/etc/namedb/named.conf
    3. Scroll down and comment out the *listen-on* declaration by putting to forward slashes (//). This will tell the system to listen for external DNS requests not just local ones. The line should look like:

// listen-on { 127.0.0.1; };

* + 1. Scroll down and remove the forward slash and asterisk (/\*) on the line above the *forwarders* declaration. Replace 127.0.0.1 with your pfSense firewall’s address. Also remove the \*/ that follows the *forwarders* declaration. This declaration tells the system to forward any request it doesn’t know to the pfSense firewall

forwarders {

192.168.\_\_\_\_\_\_\_\_.5;

};

* + 1. Scroll down to the bottom of named.conf and add the following lines to add your forward lookup zone and a reverse lookup zone (used to translate IP to Name). Fill the blank space in with your private subnet number.

zone “csci.pvt” {

type master;

file “/usr/local/etc/namedb/master/csci.pvt”;

};

zone “\_\_\_\_\_\_.168.192.in-addr.arpa” {

type master;

file “/usr/local/etc/namedb/master/csci.pvt.rev”;

};

* + 1. Save and exit editing file
    2. # cd /usr/local/etc/namedb/master

Create your zone file and make its contents be the same as the screen capture below except replace 35 with your private subnet number:

* + 1. # ee csci.pvt

$TTL 3600

csci.pvt. IN SOA ns1.csci.pvt. root.csci.pvt. (

1 ; Serial

10800 ; Refresh

3600 ; Retry

604800 ; Expire

86400 ) ; Minimum TTL

; DNS Server

csci.pvt. IN NS ns1.csci.pvt.

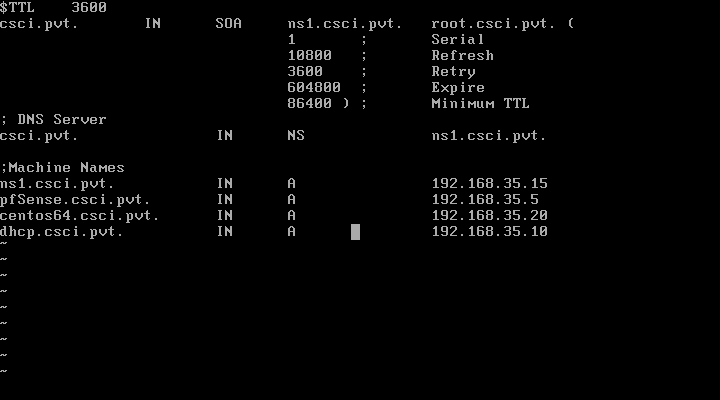
;Machine Names

ns1.csci.pvt. IN A 192.168.35.15

pfSense.csci.pvt. IN A 192.168.35.5

centos64.csci.pvt. IN A 192.168.35.20

dhcp.csci.pvt. IN A 192.168.35.10



We are going to create the Reverse lookup file make its contents be the same as the screen capture below except replace 35 with your private subnet number

* + 1. # vi /var/named/etc/namedb/master/csci.pvt.rev

$TTL 3600

35.168.192.in-addr.arpa. IN SOA ns1.csci.pvt. root.csci.pvt. (

1 ; Serial

10800 ; Refresh

3600 ; Retry

604800 ; Expire

86400 ) ; Minimum TTL

; DNS Server

35.168.192.in-addr.arpa. IN NS ns1.csci.pvt.

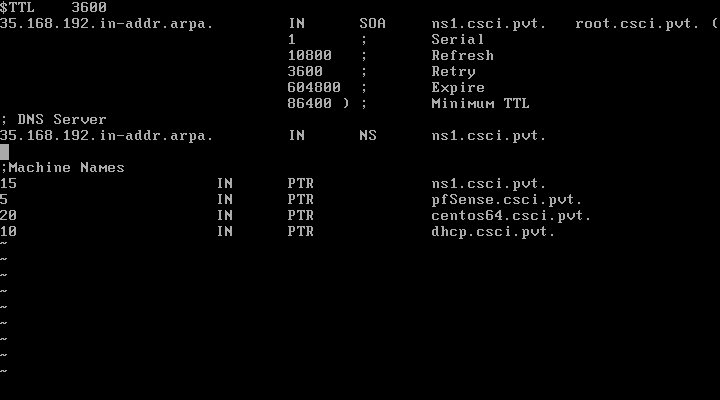
;Machine Names

15 IN PTR ns1.csci.pvt.

5 IN PTR pfSense.csci.pvt.

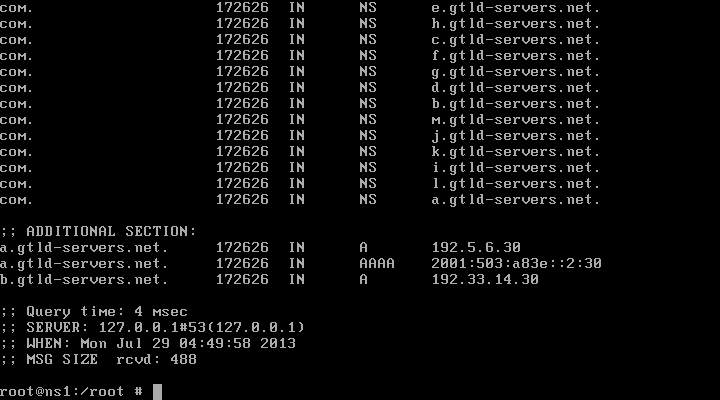
20 IN PTR centos64.csci.pvt.

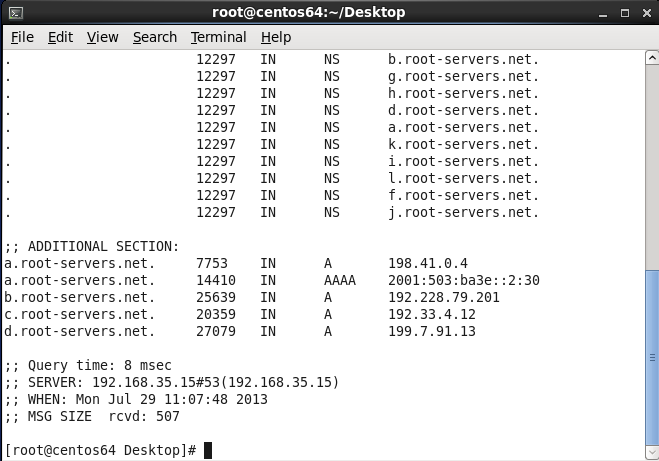
10 IN PTR dhcp.csci.pvt.



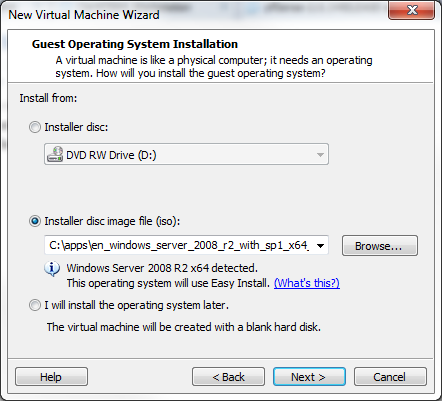
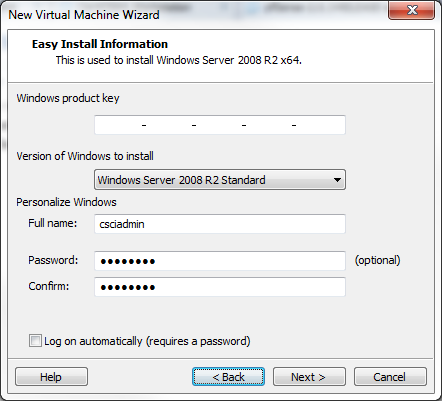
* + 1. Configure named (BIND service) to start automatically at boot time.
       1. # ee /etc/rc.conf
       2. add the following line:

named\_enable=”YES”

* + - 1. Save and Exit
    1. Edit /etc/resolv.conf and comment out the University name server
       1. # ee /etc/resolv.conf
       2. Put a # in front of nameserver 132.194.70.65 
       3. Save and exit file
    2. Start named service and test
       1. # /usr/local/etc/rc.d/named start
       2. # dig google.com 
       3. If successful you should see the above output with the line SERVER: 127.0.0.1#53
       4. Power on your CentOS 6.4 system if it is off log in, open a terminal terminal (right click desktop and select Open in terminal) and run “dig google.com”



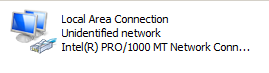
You should see the line SERVER: 192.168.35.15 #53 which means our DNS server fetched the results and forwarded them to your CentOS system.

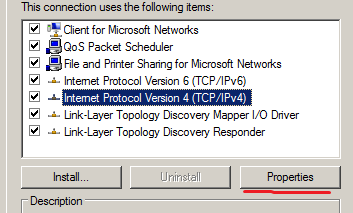
1. Deploy a Windows Server 2008 R2 DHCP server (Time to complete: 30 min)
   1. Open VMware Workstation and click File -> New Virtual Machine
   2. Click the radio button next to Custom
   3. Click Next
   4. Verify it is a Workstation 10 Hardware compatibility and click Next
   5. Select the Radio Button next to Installer disc image file and click browse
   6. Browse to \\milo\StudentSoftware and select the eng\_windows\_server\_2008\_r2\_st\_ent\_dc\_web\_retail\_x64\_X15-50365 file (you may need to “view all files” as it’s not an iso) and click Open then click Next 
   7. Set the windows version to R2 Standard and set the username as csciadmin and password 12345678 click next and say continue when it asks about the code
   8. Change the virtual machine name to be Win2008r2\_DHCP and click next
   9. Select 1 processor and 2 cores click next
   10. Select 1024 MB of memory click next
   11. Select Host-only networking and click next
   12. Click next (LSI Logic SAS)
   13. Click next (SCSI)
   14. Click next (Create new virtual disk)
   15. Click Next (Max Disk size 40GB and Split virtual disk into multiple files)
   16. Click Next (Disk Name)
   17. Click Finish
   18. System should power itself on if not click



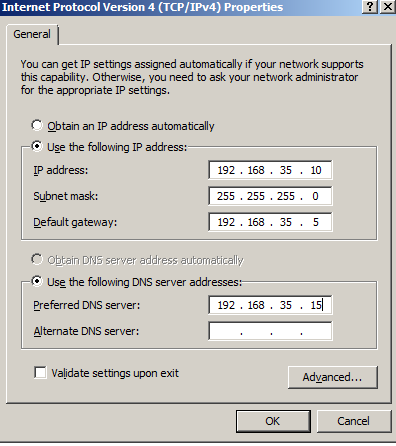
* 1. OS installation will be complete automatically and reboot itself
  2. Upon first start up the system will login and install VMware tools automatically and again reboot the system…be patient and let the VMware tools install finish before continuing.
  3. After the system reboots begin configuration
     1. Click on Configure Networking



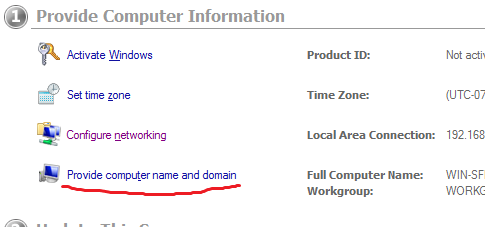
* + 1. Right click on the Local Area Connection and select Properties
    2. Select Internet Protocol Version 4 and click the properties button



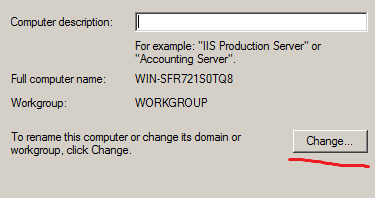
* + 1. Click the radio button next to Use the following IP address: and configure as shown below but replace 35 with your private subnet address and click OK



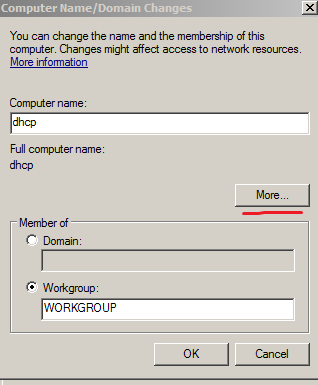
* + 1. Now click on Provide Computer name and domain



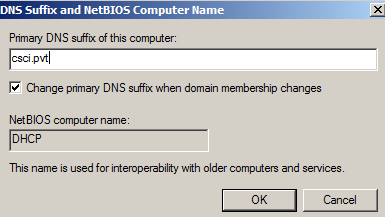
* + 1. Click on the Change button



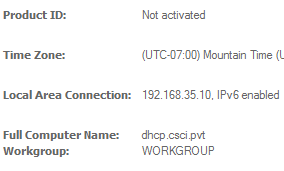
* + 1. Change the computer name to dhcp and click on the More button



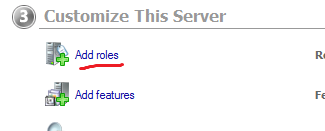
* + 1. Set the Primary DNS suffix to csci.pvt (so when you try to ping a hostname it will append this domain without asking)



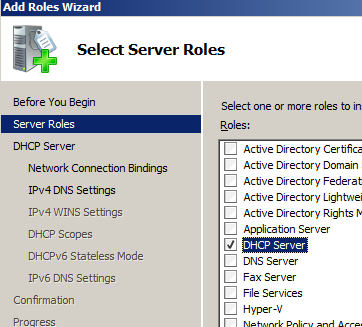
* + 1. Click Ok
    2. Click OK
    3. Click OK (Reboot Required Message)
    4. Click Close
    5. Click Restart Now
    6. After the reboot log in and your screen should now display your new IP address and domain name



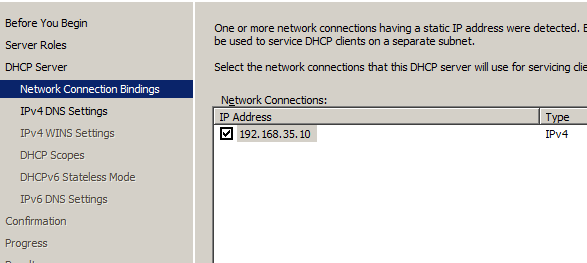
* 1. Install DHCP Server Role
     1. Click on Add Roles



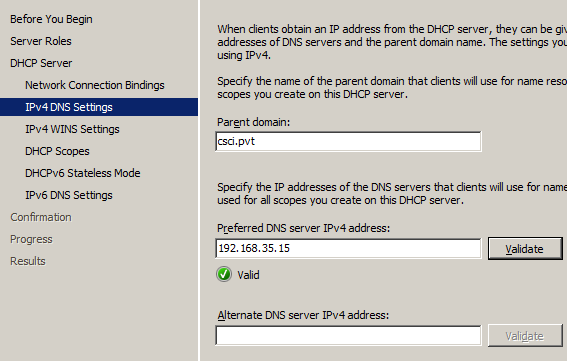
* + 1. Click Next
    2. Check the box next to DHCP Server and click Next



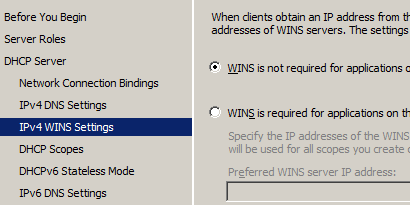
* + 1. Read the following screen and click Next
    2. Make sure you have a Network Connection list and click Next



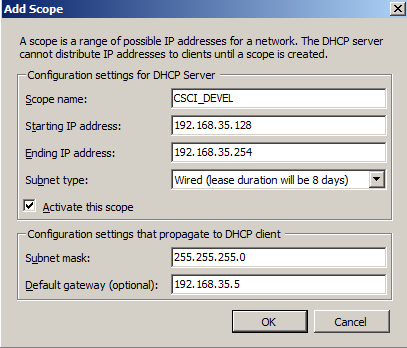
* + 1. Set the Parent Domain to csci.pvt and the Preferred DNS Server IPv4 address to 192.168.35.15 click validate and if Valid click Next



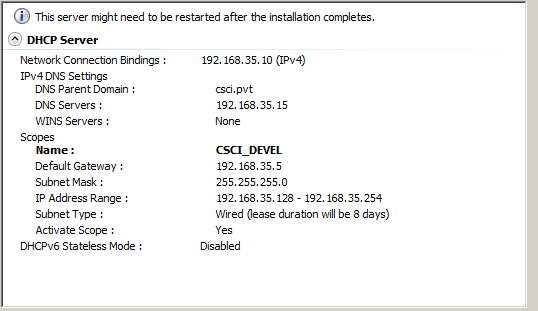
* + 1. Make sure radio button next to WINS is not required is check and click Next



* + 1. Add a scope or range of possible IP addresses for our network
       1. Click Add
       2. Enter information based on Section 1 (d) of this worksheet’s planning section (replace 35 below with your private subnet)



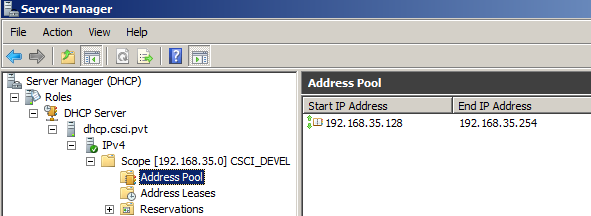
* + 1. Click Next
    2. Select Disable DHCPv6 stateless mode for this server and click Next
    3. You should now see a summary of your configuration that looks similar to the one below.



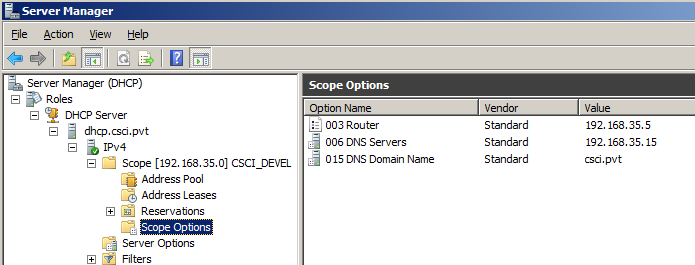
* + 1. Click the Install button
    2. When the Installation succeeded message appears click on Close and reboot the server
    3. After the reboot log in to the system and you will see DHCP Server listed next to Roles



* + 1. Click the close button on the initial configuration screen
    2. The Server Manager page will display
    3. Expand the Tree on the right by clicking on the plus signs next to Roles - > DHCP Server -> dhcp.csci.pvt -> IPv4 ->Scope ->Address Pool
    4. Verify your address range is listed



* + 1. Verify your scope options that will be sent to hosts that request IP addresses are correct…Click on Scope Options Router should be .5 DNS server .15 and domain csci.pvt



1. Testing and verification of environment (Time to complete: 20 min)
   1. Set CentOS to DHCP and verify address
      1. Log in to your CentOS 6.4 workstation and open a terminal (right click desktop and select Open in terminal)
      2. # cd /etc/sysconfig/network-scripts

Rename ifcfg-eth0 in order to keep a backup of the file

* + 1. # mv ifcfg-eth0 ifcfg-eth0.static.bak

Copy our original file with DHCP configuration to ifcfg-eth0

* + 1. # cp ifcfg-eth0.dhcp.bak ifcfg-eth0

Edit ifcfg-eth0 to enable the device and stop Network Manager control

* + 1. # vi ifcfg-eth0

DEVICE=eth0

HWADDR=00:0C:29:E7:91:29

TYPE=Ethernet

UUID=0173e644-613c-4347-a94c-4f0180bcddcb

ONBOOT=**yes**

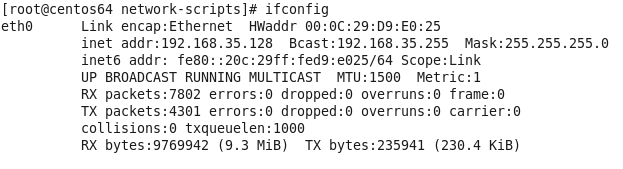
NM\_CONTROLLED=**no**

BOOTPROTO=dhcp

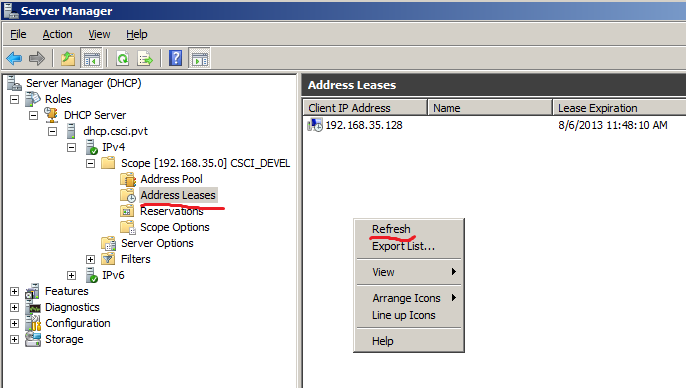
* + 1. Edit /etc/resolv.conf
       1. # vi /etc/resolv.conf
       2. Remove the line nameserver 192.168.211.1
       3. Save and exit

Restart networking

* + 1. # service network restart
    2. # ifconfig
    3. You should now see a configuration similar to the one below with the address 192.168.211.128



* + 1. Go back to your Windows 2008 R2 server and click on Address Leases, Right click in the white area where the leases get listed and select Refresh. You should now see your CentOS 6.4 systems lease listed



* 1. TEST DNS: On your CentOS 6.4 system ping all hosts by their csci.pvt DNS names
     1. Open terminal and issue the following commands
     2. # ping pfSense.csci.pvt
     3. # ping ns1.csci.pvt
     4. # ping centos64.csci.pvt
     5. # ping dhcp.csci.pvt
     6. Which system will not answer pings? Nothing pings now.
     7. Can you guess why? I believe we can’t ping now(like we were able to before) because of our firewall.