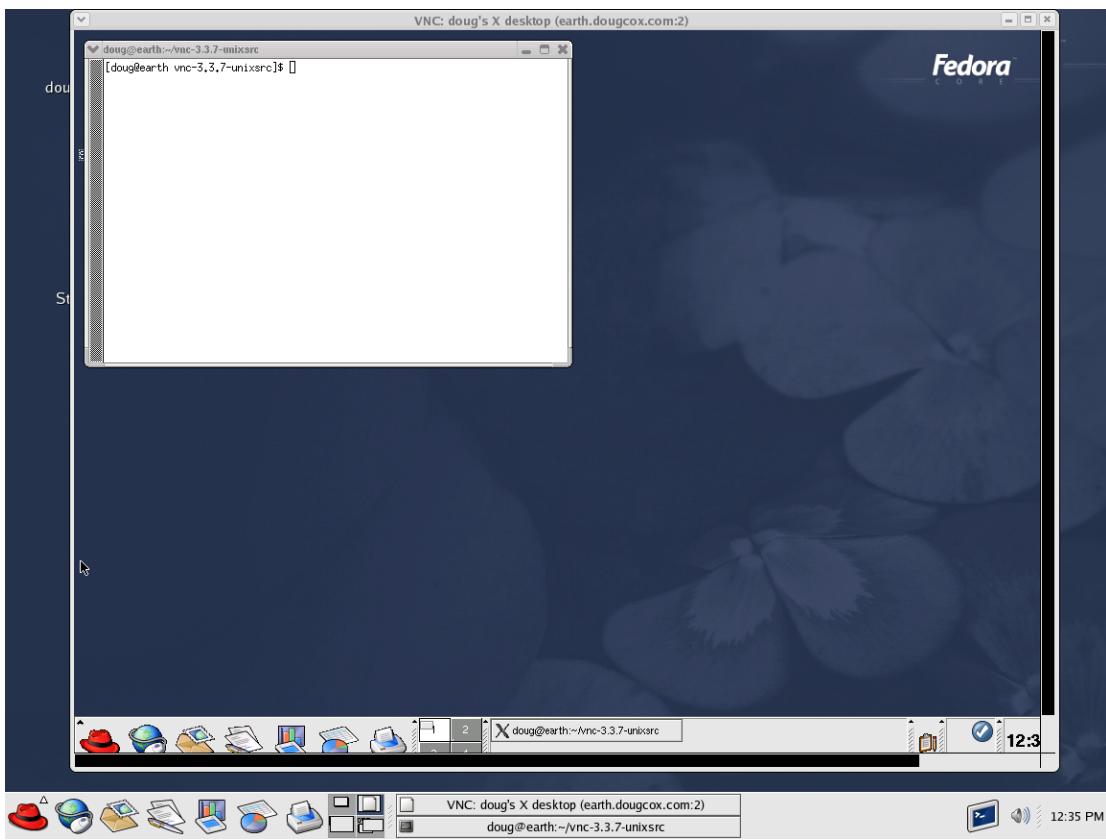


### 7.3.1

## Remote Desktop Monitoring (VNC)



## Laboratory Overview

### Objective

At the end of this lab students will be able to configure software to remotely monitor, access applications, and verify connected ports.

This lab will review the various remote options and walk through the installation on a Windows XP platform and a Linux platform.

### Information for Laboratory

Students will research the following remote access applications:

PC-Anywhere	<a href="http://www.symantec.com/pcanywhere/">http://www.symantec.com/pcanywhere/</a>
Remote-Anything	<a href="http://www.remote-anything.com/">http://www.remote-anything.com/</a>
TridaiVNCpro	<a href="http://www.tridiavncpro.com/">http://www.tridiavncpro.com/</a>
TightVNC	<a href="http://www.tightvnc.com/">http://www.tightvnc.com/</a>
VNC	<a href="http://www.realvnc.com/">http://www.realvnc.com/</a>

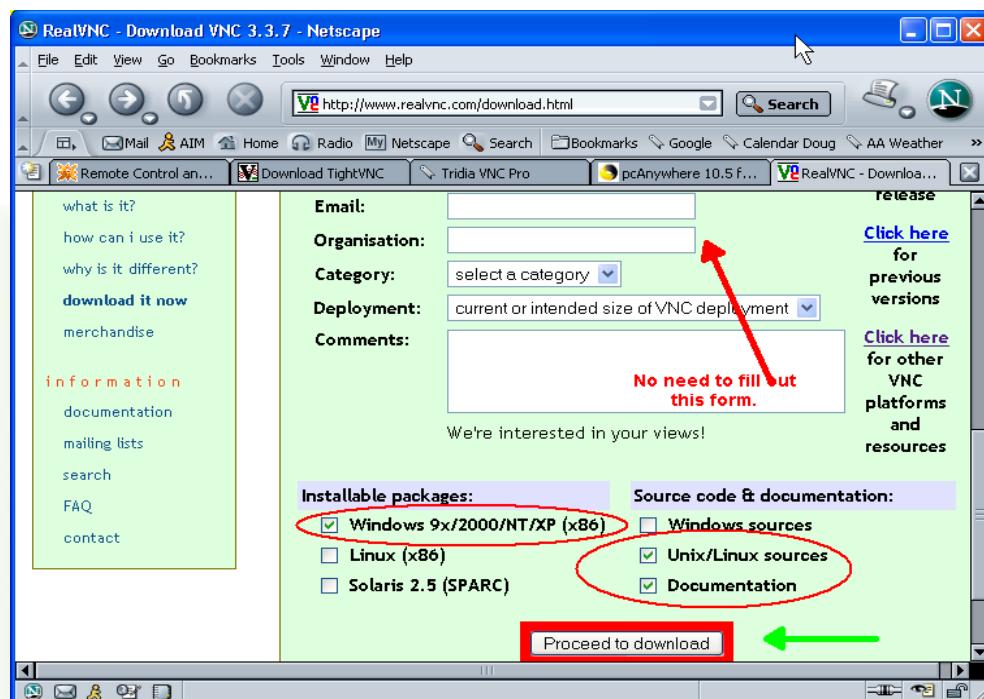
### Student Preparation

- 1) Which products are commercial or require a license?
- 2) Which products are open source?
- 3) Which products are currently cross platform?
- 4) Which products will transfer files between client and server?
- 5) Which products are secure?
  - a. Number of and strength of user name and password?
  - b. Is the transmission encrypted?
- 6) Which products use a Browser as a client interface?
- 7) Which products offer a java client?
- 8) Which products support Palm, Zaurus, WindowsCE other devices?
- 9) Develop a comparison chart of the different features and discuss when it might be more appropriate to use one product over the other.



Students will need access to two computers, one with Linux (with development tools installed) and the other with Windows XP machines on the same network with a current browser and a zip utility (Winzip or PowerArchiver). Students will need admin, root and user accounts on the platforms.

Have available the following VNC software on a local server or CD (<http://www.realvnc.com/download.html> )



The screenshot shows the 'Download Area' section of the RealVNC website. It features a sidebar with links: 'documentation', 'mailing lists', 'search', 'FAQ', and 'contact'. The main area is titled 'Download Area' and contains four download options:

- x86 Win32 full installation (server and viewer)**: Includes links for 'executable (.exe)' (563K) and 'zip archive (.zip)' (534K).
- x86 Win32 viewer program only**: Includes links for 'executable (.exe)' (228K) and 'zip archive (.zip)' (92K).
- Copy of online documentation**: Includes links for 'gzipped tar (.tar.gz)' (197K) and 'zip archive (.zip)' (223K).
- Unix source**: Includes links for 'gzipped tar (.tar.gz)' (2.1M) and 'compressed tar (.tar.Z)' (3.6M).

Yellow circles highlight the download links for each category: 'executable (.exe)', 'zip archive (.zip)', 'gzipped tar (.tar.gz)', and 'compressed tar (.tar.Z)'.

## **Estimated Completion Time**

90-120 Minutes (perhaps up to 240 Minutes to really explore)

### **How it works**

The software creates a server that listens for connections on a predetermined port. The client software then connects to the server which may ask for authentication. We will install a server VNC on both a Linux and a Windows platform, use a browser to connect and also a client package. The server will share its desktop to the viewer application running on the client. Depending on the configuration of the server, multiple clients can connect to one server which can be useful in a training application.

## **PART I**

### **Step I: Install server on a Linux platform:**

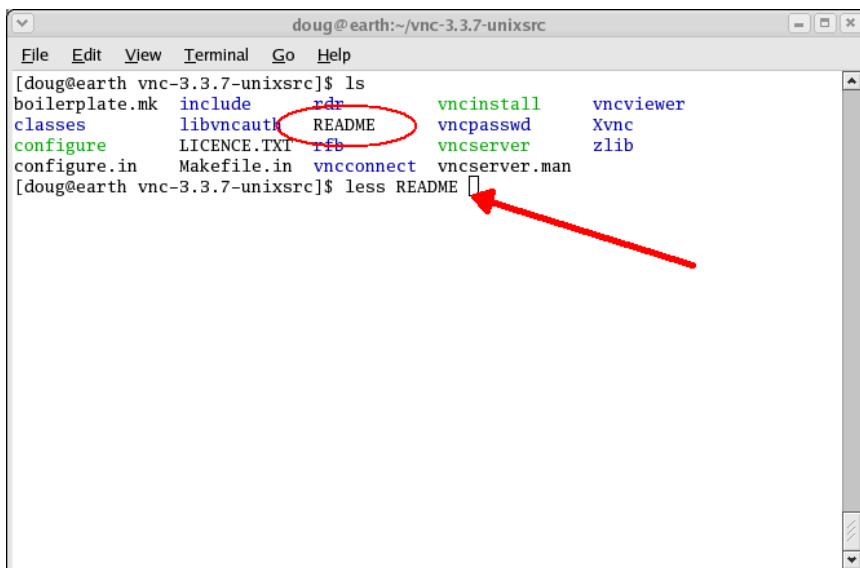
As a user (not root) log into the Linux box and in your home directory copy the vnc source code from the course CD, course server or the [www.realvnc.com](http://www.realvnc.com) (see above Instructors section).

Untar the source code and cd into the source directory

```
tar xfz vnc-3.3.7-unixsrc.tar.gz  
cd vnc-3.3.7-unixsrc
```

Review the vnc README





```
doug@earth:~/vnc-3.3.7-unixsrc
File Edit View Terminal Go Help
[doug@earth vnc-3.3.7-unixsrc]$ ls
boilerplate.mk  include  rdr  vncinstall  vncviewer
classes          libvncauth  README  vncpasswd  Xvnc
configure        LICENCE.TXT  rfb  vncserver  zlib
configure.in     Makefile.in  vncconnect  vncserver.man
[doug@earth vnc-3.3.7-unixsrc]$ less README
```

## Step 2: Compile (build) the vnc server and client

Issue the following commands. If you have trouble, see the FAQ and READMEs

```
./configure --with-installed-zlib
make
cd Xvnc
make World
cd ..
```

## Step 3: Install the vnc server and client

Issue the following commands from the vnc directory



doug@earth:/home/doug/vnc-3.3.7-unixsrc - Shell - Konsole

Session Edit View Bookmarks Settings Help

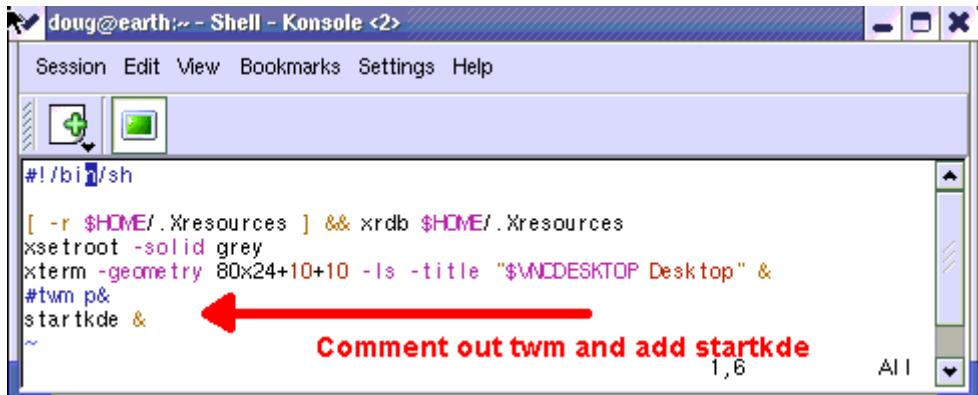
[doug@earth vnc-3.3.7-unixsrc]\$ pwd  
/home/doug/vnc-3.3.7-unixsrc  
[doug@earth vnc-3.3.7-unixsrc]\$ su  
Password:  
[root@earth vnc-3.3.7-unixsrc]# ./vncinstall /usr/local/bin

*su  
./vncinstall /usr/local/bin  
mkdir -p /usr/local/vnc/classes  
cp classes/\* /usr/local/vnc/classes  
exit*



## Step 4: Start the vnc server

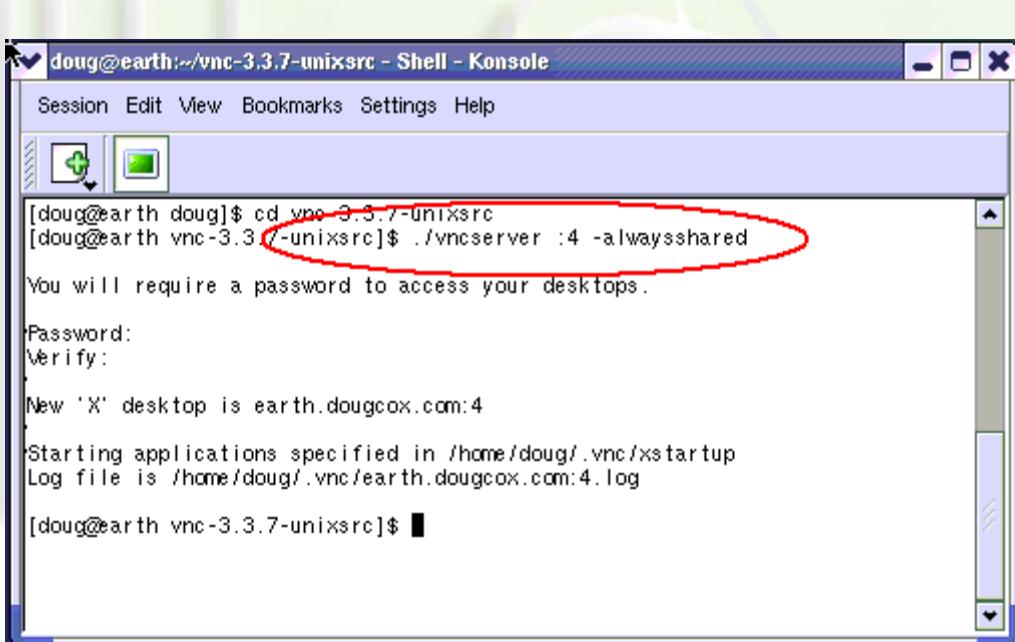
First edit the ./vnc/xstartup file to set the display manager to KDE



```
#!/bin/sh
[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources
xsetroot -solid grey
xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &
#twm p&
startkde &
~
```

Comment out twm and add startkde

From the vnc directory start the server on screen 4



```
[doug@earth doug]$ cd vnc-3.3.7-unixsrc
[doug@earth vnc-3.3.7-unixsrc]$ ./vncserver :4 -alwaysshared
You will require a password to access your desktops.

Password:
Verify:

New 'X' desktop is earth.dougox.com:4

Starting applications specified in /home/doug/.vnc/xstartup
Log file is /home/doug/.vnc/earth.dougox.com:4.log

[doug@earth vnc-3.3.7-unixsrc]$
```

- 1) Where is the session being logged?
- 2) What happens if you don't put in a password?
- 3) What is the significance of ":4"?
- 4) If the server does not start what should you do?



## Step 5: Verify that the server is up and running

Issue the following command: *netstat -tupan*

```
[doug@earth doug]$ netstat -tupan
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 0.0.0.0:32770            0.0.0.0:*
tcp      0      0 127.0.0.1:32771          0.0.0.0:*
tcp      0      0 0.0.0.0:5801             0.0.0.0:*
tcp      0      0 0.0.0.0:5802             0.0.0.0:*
tcp      0      0 0.0.0.0:3306             0.0.0.0:*
tcp      0      0 0.0.0.0:5804             0.0.0.0:*
tcp      0      0 0.0.0.0:5901             0.0.0.0:*
tcp      0      0 0.0.0.0:5902             0.0.0.0:*
tcp      0      0 127.0.0.1:783              0.0.0.0:*
tcp      0      0 0.0.0.0:111               0.0.0.0:*
tcp      0      0 0.0.0.0:5904             0.0.0.0:*
tcp      0      0 0.0.0.0:6001             0.0.0.0:*
tcp      0      0 0.0.0.0:6002             0.0.0.0:*
tcp      0      0 0.0.0.0:6004             0.0.0.0:*
tcp      0      0 0.0.0.0:22                0.0.0.0:*
tcp      0      0 127.0.0.1:631               0.0.0.0:*
tcp      0      0 127.0.0.1:25                0.0.0.0:*
tcp      0      0 127.0.0.1:33160            127.0.0.1:5902
tcp      0      0 127.0.0.1:631               127.0.0.1:33168
tcp      0      0 127.0.0.1:5902            127.0.0.1:33160
tcp      0      0 216.144.214.179:22           68.40.57.196:3720
tcp      0      0 216.144.214.179:5902            68.40.57.196:3725
tcp      0      0 127.0.0.1:33168            127.0.0.1:631
tcp      1      0 127.0.0.1:33155            127.0.0.1:631
tcp      1      0 127.0.0.1:33145            127.0.0.1:631
udp      0      0 0.0.0.0:32768              0.0.0.0:*
udp      0      0 0.0.0.0:868               0.0.0.0:*
udp      0      0 0.0.0.0:111               0.0.0.0:*
udp      0      0 0.0.0.0:631               0.0.0.0:*
udp      0      0 216.144.214.179:123            0.0.0.0:*
udp      0      0 127.0.0.1:123               0.0.0.0:*
udp      0      0 0.0.0.0:123               0.0.0.0:*
[doug@earth doug]$
```

- 1) What are ports 580x, 590x, 600x?
- 2) Are there any connected sessions in the screen shot?
- 3) Are there any connected sessions on your system?

## Step 6: Connect from localhost

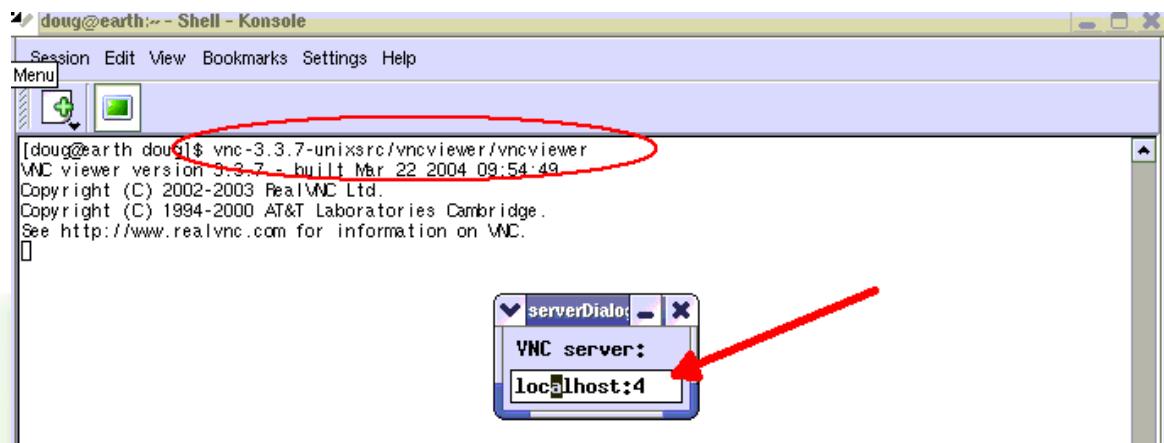
Issue the following commands:

*cd*

*vnc-3.3.7-unixsrc/vncviewer/vncviewer*

When the server Dialog box opens put in:

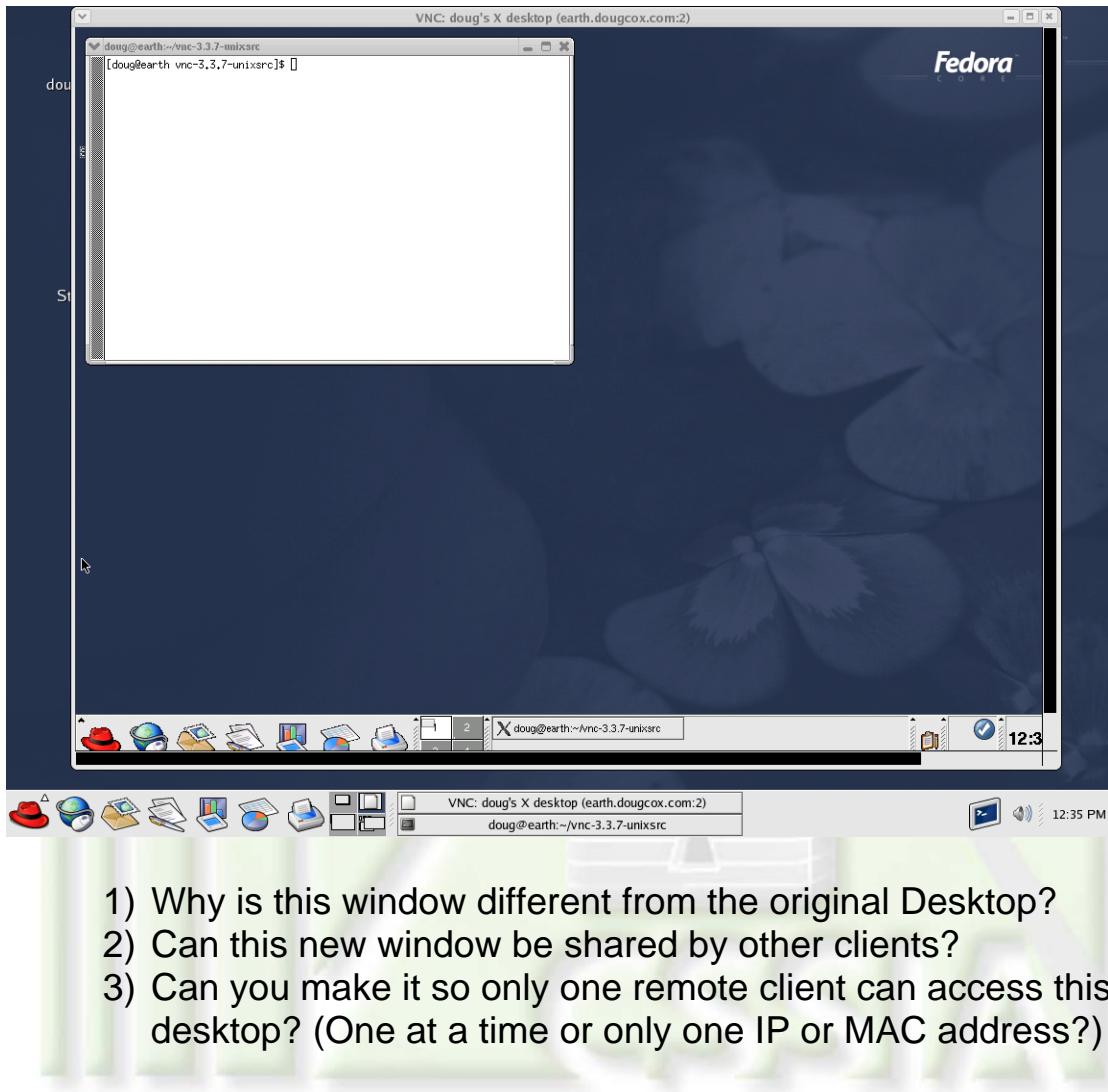
*localhost:4*



Enter Password



If all went well you should have another Desktop within your current desktop.



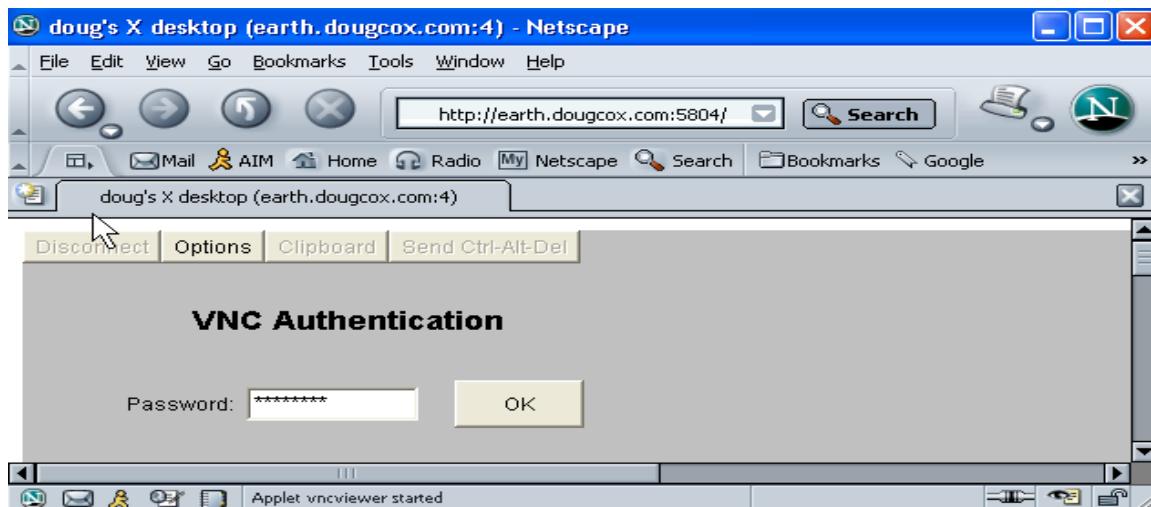
- 1) Why is this window different from the original Desktop?
- 2) Can this new window be shared by other clients?
- 3) Can you make it so only one remote client can access this desktop? (One at a time or only one IP or MAC address?)

## Step 7: Connecting from a browser on a Windows machine

Open a browser to the address of the Linux machine

*http://earth1.dougcox.com:5804*

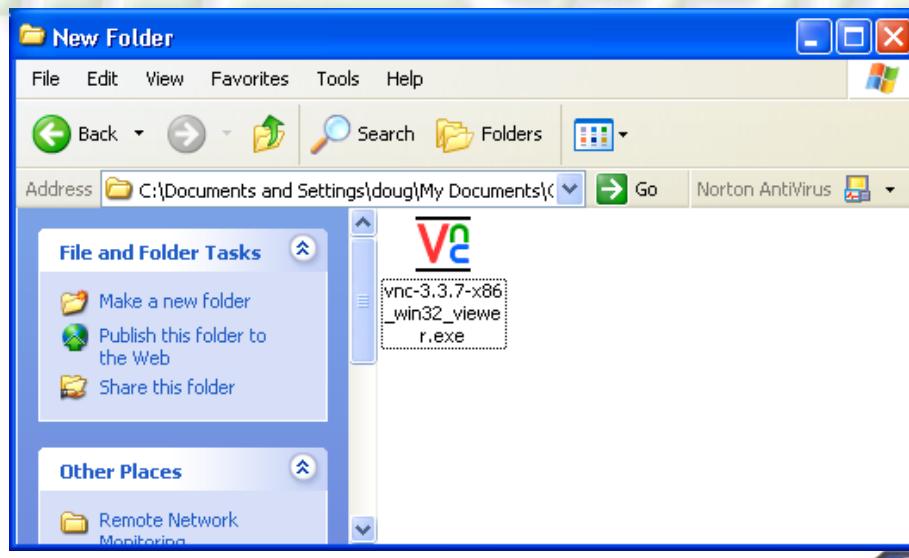
Enter password if you supplied one



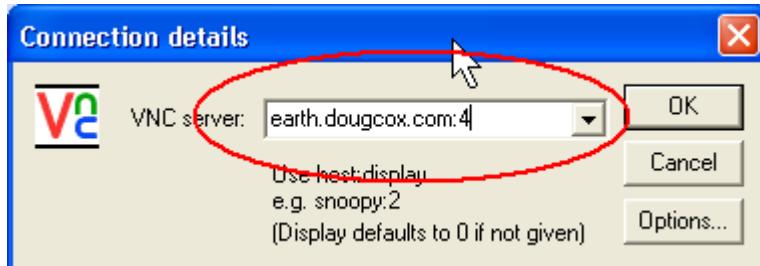
- 1) What is the significance of :5804?
- 2) How many different users can attach to this system?

## Step 8: Using vnc viewer on a Windows machine

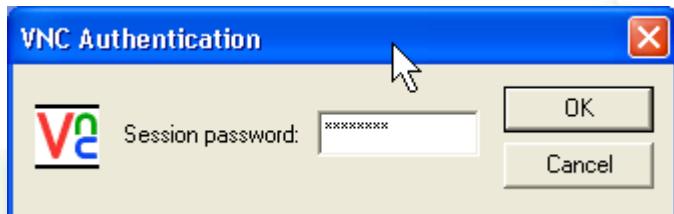
From the course CD, course server or the [www.realvnc.com](http://www.realvnc.com) find vnc-3.3.7-x86\_win32\_viewer.exe



Open the viewer and enter the machine name and desktop you wish to attach. Then select OK.



At this point you will be asked for the password.



Enter the password and compare to the web session.

- 1) What port are you attaching to on the Linux box?
- 2) What port are you coming from on the Windows box?
- 3) How could this be helpful for desktop support?

## Step 9: Verifying connections

On the Windows box issues the command: `netstat -anp tcp`

```
C:\WINDOWS\System32\cmd.exe
statistics. If omitted, netstat will print the current
configuration information once.

C:\Documents and Settings\doug>netstat -anp tcp
Active Connections

Proto Local Address          Foreign Address        State
TCP   0.0.0.0:135            0.0.0.0:0           LISTENING
TCP   0.0.0.0:445            0.0.0.0:0           LISTENING
TCP   0.0.0.0:1025           0.0.0.0:0           LISTENING
TCP   0.0.0.0:1026           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3476           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3560           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3582           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3583           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3720           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3725           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3775           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3777           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3806           0.0.0.0:0           LISTENING
TCP   0.0.0.0:3845           0.0.0.0:0           LISTENING
```

C:\WINDOWS\System32\cmd.exe

TCP	Local Address	Foreign Address	State
TCP	0.0.0.0:4910	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3001	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3002	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3003	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3013	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3559	0.0.0.0:0	LISTENING
TCP	127.0.0.1:3559	127.0.0.1:3560	ESTABLISHED
TCP	127.0.0.1:3560	127.0.0.1:3559	ESTABLISHED
TCP	127.0.0.1:5180	0.0.0.0:0	LISTENING
TCP	192.168.69.123:139	0.0.0.0:0	LISTENING
TCP	192.168.69.123:3554	0.0.0.0:0	LISTENING
TCP	192.168.69.123:3582	64.12.24.213:5190	ESTABLISHED
TCP	192.168.69.123:3583	205.190.157.105:5003	ESTABLISHED
TCP	192.168.69.123:3613	0.0.0.0:0	LISTENING
TCP	192.168.69.123:3720	216.144.214.179:22	ESTABLISHED
TCP	192.168.69.123:3725	216.144.214.179:5902	ESTABLISHED
TCP	192.168.69.123:3806	216.144.214.179:5904	ESTABLISHED
TCP	192.168.69.123:3845	216.144.214.179:5904	ESTABLISHED
TCP	192.168.69.123:3848	192.168.69.1:143	ESTABLISHED
TCP	192.168.69.123:3879	192.168.69.1:143	ESTABLISHED
TCP	192.168.69.123:4039	198.111.176.4:143	ESTABLISHED
TCP	192.168.69.123:16868	0.0.0.0:0	LISTENING

Find the connections to the vnc server.

- 1) Can you tell which viewing method the connection is? How?  
(viewer or browser)

From the Linux box issue the command: *netstat -tupan*

doug@earth vnc-3.3.7-unixsrc\$ netstat -tupan

(Not all processes could be identified, non-owned process info  
will not be shown, you would have to be root to see it all.)

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address	Foreign Address	State	PID/Program name
tcp 0 0 0.0.0.0:32770	0.0.0.0:*	LISTEN	-
tcp 0 0 127.0.0.1:32771	0.0.0.0:*	LISTEN	-
tcp 0 0 0.0.0.0:5801	0.0.0.0:*	LISTEN	12556/Xvnc
tcp 0 0 0.0.0.0:5802	0.0.0.0:*	LISTEN	12942/Xvnc
tcp 0 0 0.0.0.0:3306	0.0.0.0:*	LISTEN	-
tcp 0 0 0.0.0.0:5804	0.0.0.0:*	LISTEN	13873/Xvnc
tcp 0 0 0.0.0.0:5901	0.0.0.0:*	LISTEN	12556/Xvnc
tcp 0 0 0.0.0.0:5902	0.0.0.0:*	LISTEN	12942/Xvnc
tcp 0 0 127.0.0.1:783	0.0.0.0:*	LISTEN	-
tcp 0 0 0.0.0.0:111	0.0.0.0:*	LISTEN	-
tcp 0 0 0.0.0.0:5904	0.0.0.0:*	LISTEN	13873/Xvnc
tcp 0 0 0.0.0.0:6001	0.0.0.0:*	LISTEN	12556/Xvnc
tcp 0 0 0.0.0.0:6002	0.0.0.0:*	LISTEN	12942/Xvnc
tcp 0 0 0.0.0.0:6004	0.0.0.0:*	LISTEN	13873/Xvnc
tcp 0 0 0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp 0 0 127.0.0.1:631	0.0.0.0:*	LISTEN	-
tcp 0 0 127.0.0.1:25	0.0.0.0:*	LISTEN	-
tcp 0 0 216.144.214.179:5904	68.40.57.196:3845	ESTABLISHED	13873/Xvnc
tcp 0 0 127.0.0.1:33160	127.0.0.1:5902	ESTABLISHED	13087/vncviewer
tcp 0 0 127.0.0.1:5902	127.0.0.1:33160	ESTABLISHED	12942/Xvnc
tcp 0 0 216.144.214.179:22	68.40.57.196:3720	ESTABLISHED	-
tcp 0 0 216.144.214.179:902	68.40.57.196:3725	ESTABLISHED	12942/Xvnc
tcp 0 0 216.144.214.179:5904	68.40.57.196:3806	ESTABLISHED	13873/Xvnc
tcp 1 0 127.0.0.1:33168	127.0.0.1:631	CLOSE_WAIT	14019/eggcups
tcp 1 0 127.0.0.1:33155	127.0.0.1:631	CLOSE_WAIT	13006/eggcups
tcp 1 0 127.0.0.1:33145	127.0.0.1:631	CLOSE_WAIT	12703/eggcups
udp 0 0 0.0.0.0:32768	0.0.0.0:*	-	
udp 0 0 0.0.0.0:888	0.0.0.0:*	-	
udp 0 0 0.0.0.0:111	0.0.0.0:*	-	
udp 0 0 0.0.0.0:631	0.0.0.0:*	-	
udp 0 0 216.144.214.179:123	0.0.0.0:*	-	
udp 0 0 127.0.0.1:123	0.0.0.0:*	-	
udp 0 0 0.0.0.0:123	0.0.0.0:*	-	

[doug@earth vnc-3.3.7-unixsrc]\$ P

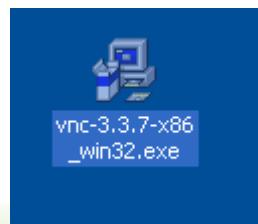


- 1) Can you tell how many sessions are open to the same desktop?
- 2) Connect from the browser and viewer and verify the server port connections 590x and 5800x.

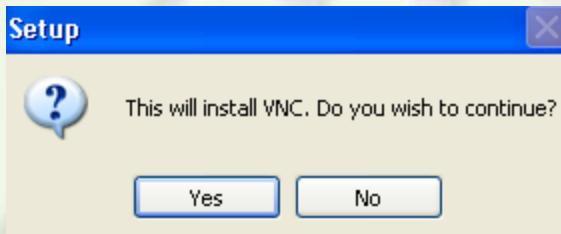
## Part II

### Step 1: Installing vnc server on the Windows Platform

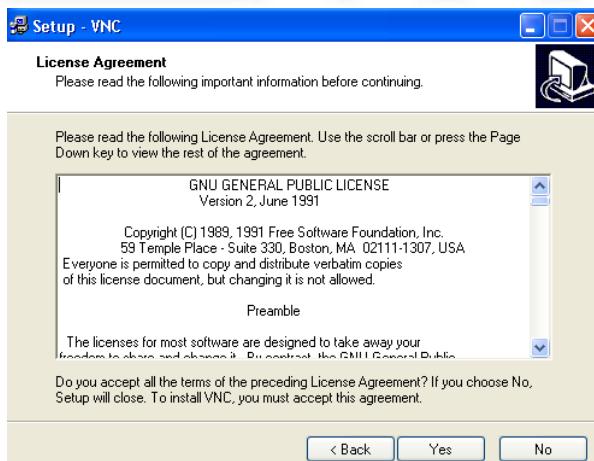
From the course CD, course server or the [www.realvnc.com](http://www.realvnc.com) copy the vnc-3.3.7-x86\_win32.exe to the desktop.



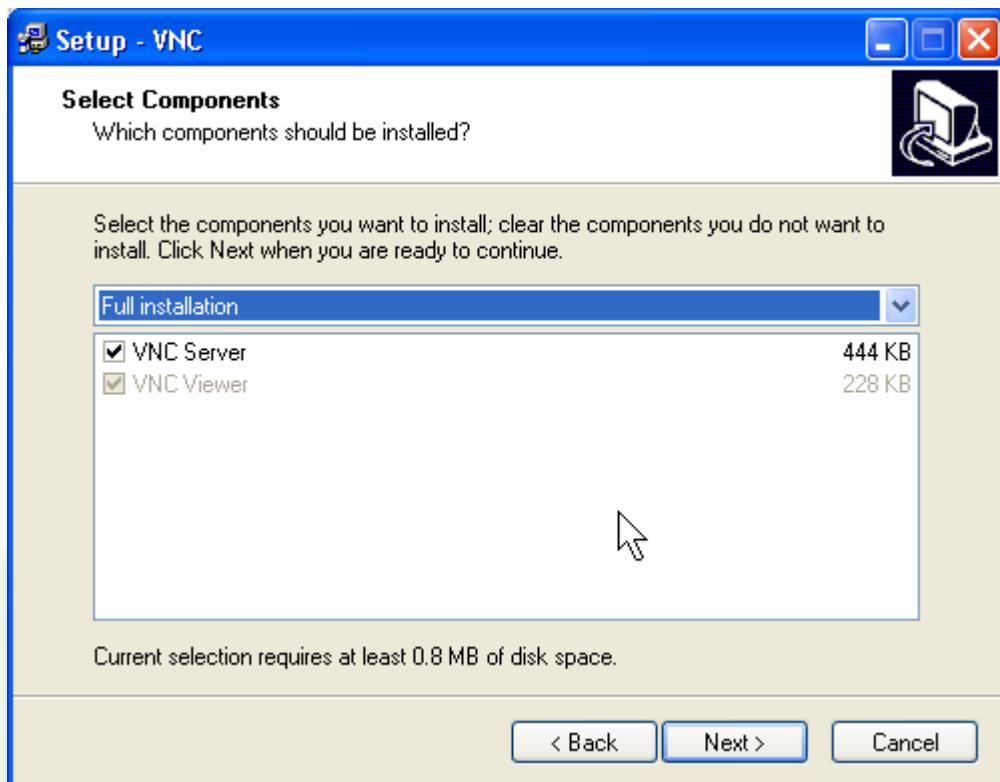
Open vnc-3.3.7-x86\_win32.exe by double clicking.



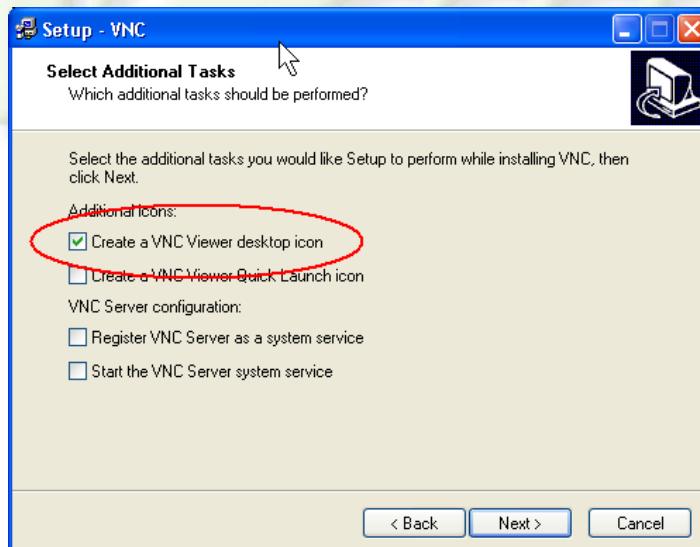
Click next  
Agree to the license



Click next  
Select server and full installation (default)



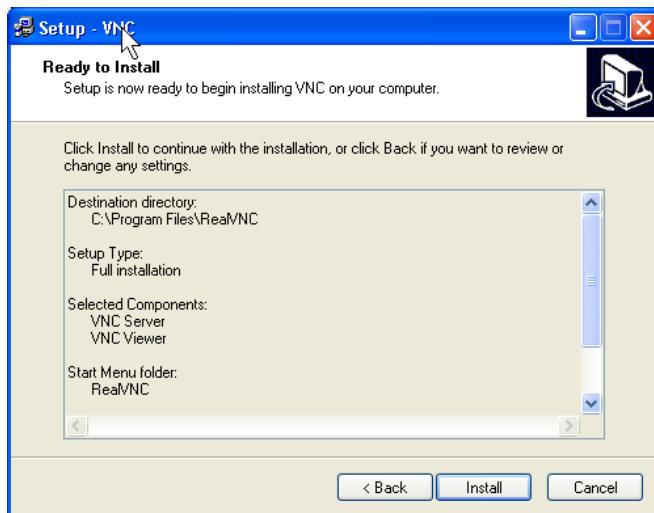
Click Next until you get to this screen  
You may want to choose some of these options.



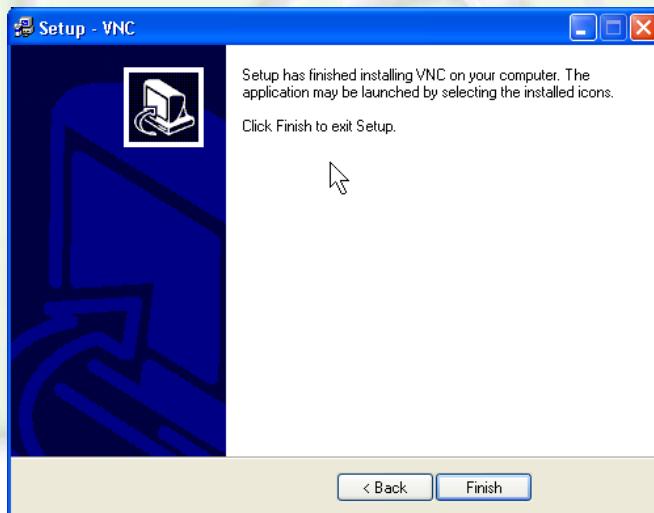
- 1) Why would you want to register as a service?



Finish the install.



Review the information page



Finish

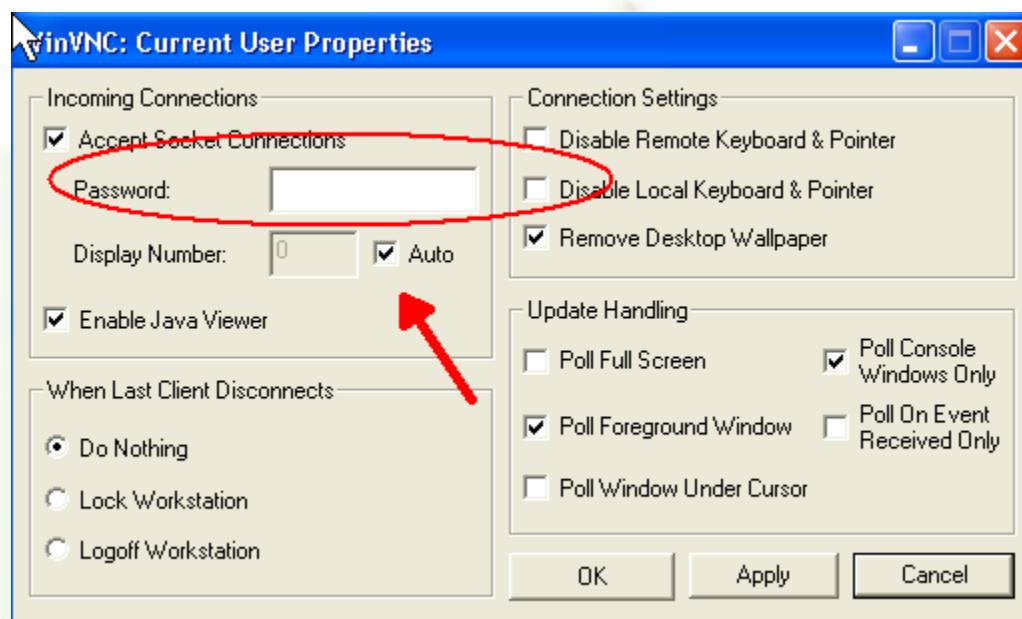
## STEP 2: Start the server

Select start programs and find the vnc server:



Configure the connection type

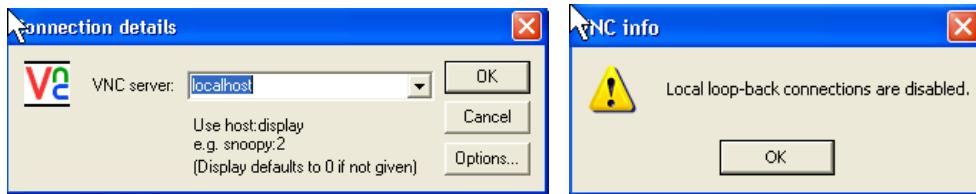
Set the password



- 1) How do these options compare to the Linux server options?
- 2) Why would you need to lock the workstation?
- 3) Why would you want to disable either the Remote or Local Keyboard & Pointer?
- 4) Explore the other options.

## STEP 3: Attempt to connect to the localhost

Open the vnc viewer on the local machine



- 1) Why does the connection fail?
- 2) Discuss how this may prevent misuse of the server.
- 3) Can you use the browser to connect?

Hint use localhost:5800

## STEP 4: Verify server started

```
C:\ Command Prompt
C:\Documents and Settings\doug>
C:\Documents and Settings\doug>netstat -an

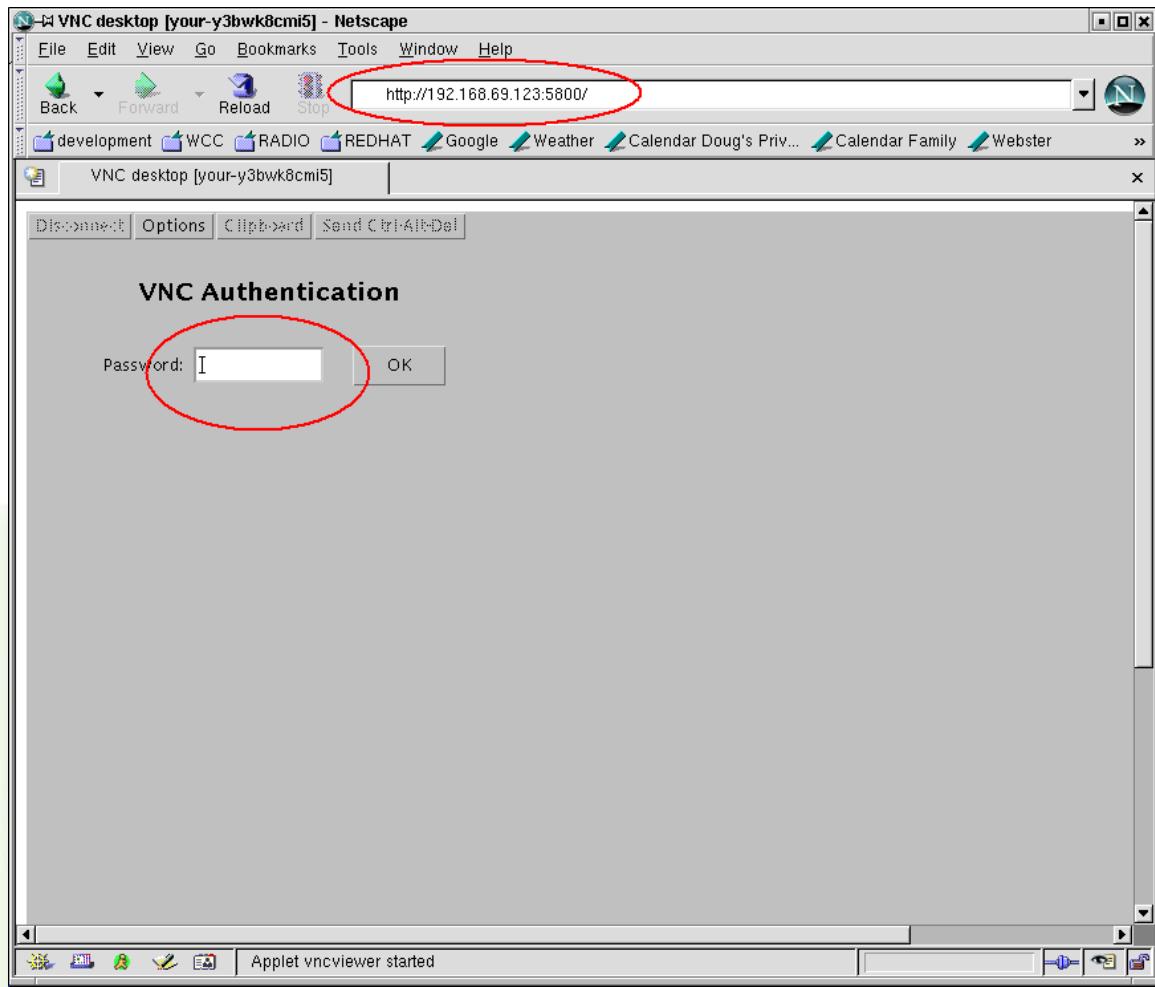
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
  TCP    0.0.0.0:1025          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:1026          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3476          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3560          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3582          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3583          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3720          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3725          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3777          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:3806          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:4081          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:4082          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:4100          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:4111          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:4910          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5000          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5800          0.0.0.0:0             LISTENING
  TCP    0.0.0.0:5900          0.0.0.0:0             LISTENING
  TCP    127.0.0.1:3001         0.0.0.0:0             LISTENING
  TCP    127.0.0.1:3002         0.0.0.0:0             LISTENING
```

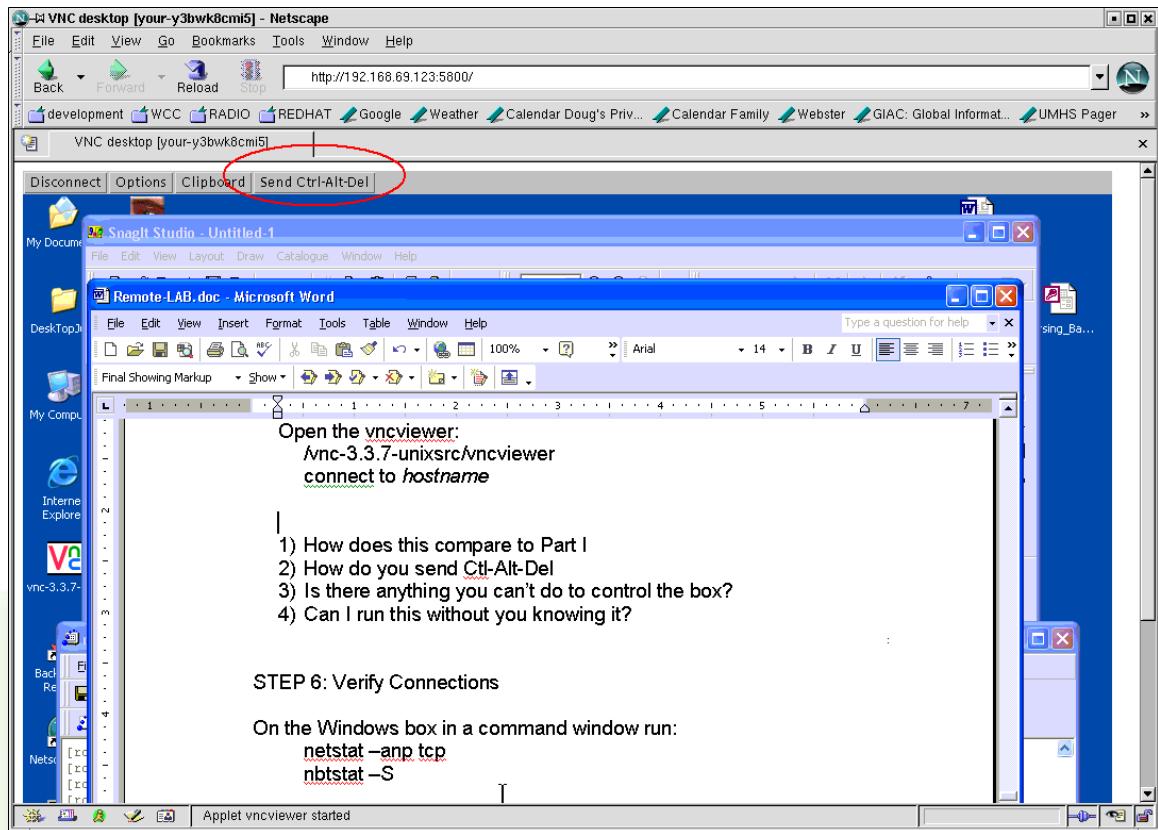
The screenshot shows a Windows Command Prompt window with the title 'Command Prompt'. The command 'netstat -an' is entered and its output is displayed. The output lists various network connections. Two specific entries are highlighted with red circles: the first entry 'C:\Documents and Settings\doug>netstat -an' at the top of the list, and the second entry 'TCP 0.0.0.0:4910 0.0.0.0:0 LISTENING' further down. The rest of the output shows other standard listening ports like 135, 445, 1025, etc.

## STEP 5: Connect from a Linux box

Open a browser and connect to *http://hostname:5800*



## Enter the password



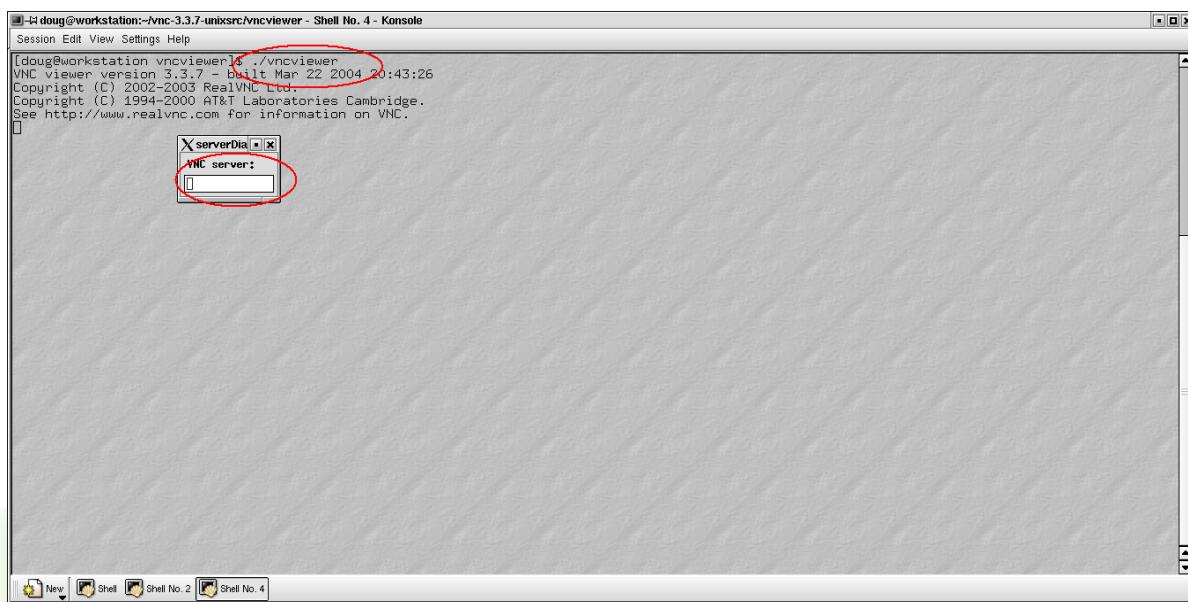
- 1) Why is 5800 used for the port number?
- 2) What would happen if you used 5804?
- 3) Can you change this port number?



Open the vncviewer:

/vnc-3.3.7-unixsrc/vncviewer/vncviewer

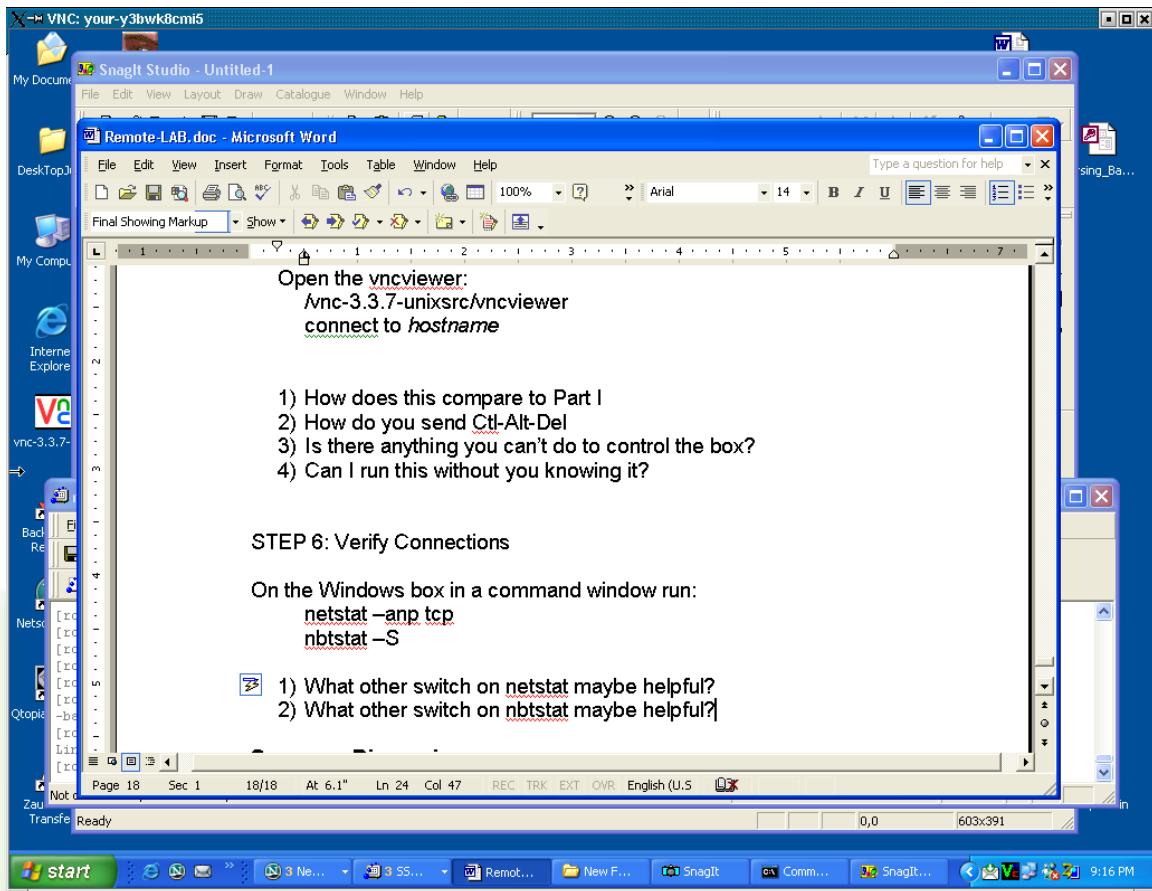
Connect to *hostname*



Enter password



Are you connected?

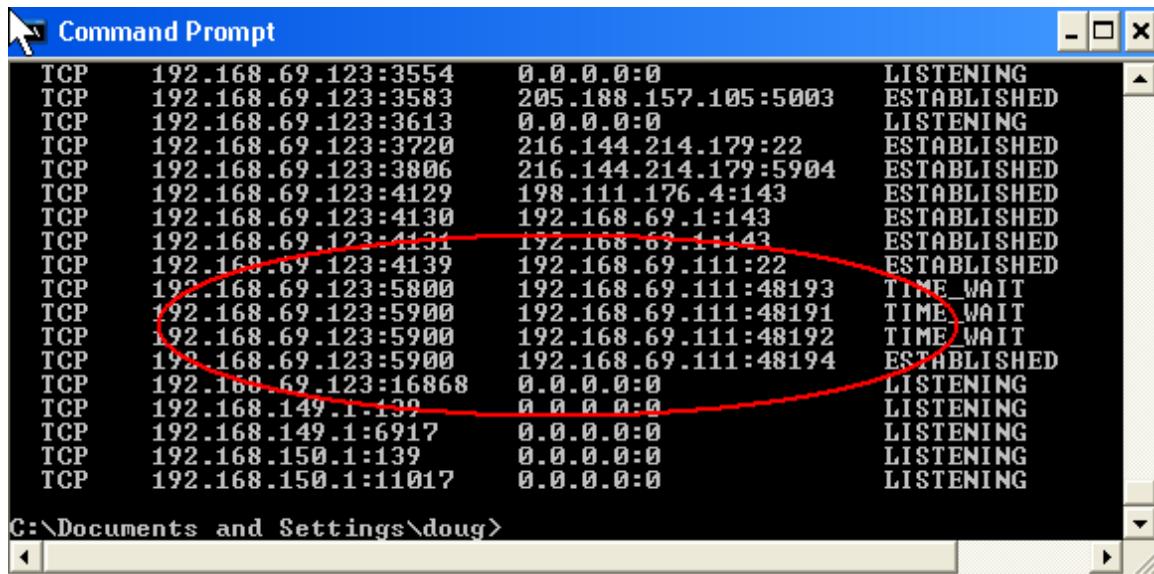


- 1) How does this compare to Part I
- 2) Do you need a Desktop number?
- 3) How do you send Ctrl-Alt-Del
- 4) Is there anything you can't do to control the box?
- 5) Can I run this without you knowing it?



## STEP 6: Verify Connections

On the Windows box in a command window run:  
netstat -anp tcp



```
Command Prompt
TCP    192.168.69.123:3554      0.0.0.0:0          LISTENING
TCP    192.168.69.123:3583      205.188.157.105:5003  ESTABLISHED
TCP    192.168.69.123:3613      0.0.0.0:0          LISTENING
TCP    192.168.69.123:3720      216.144.214.179:22  ESTABLISHED
TCP    192.168.69.123:3806      216.144.214.179:5904  ESTABLISHED
TCP    192.168.69.123:4129      198.111.176.4:143   ESTABLISHED
TCP    192.168.69.123:4130      192.168.69.1:143   ESTABLISHED
TCP    192.168.69.123:4131      192.168.69.1:143   ESTABLISHED
TCP    192.168.69.123:4139      192.168.69.111:22   ESTABLISHED
TCP    192.168.69.123:5800      192.168.69.111:48193  TIME_WAIT
TCP    192.168.69.123:5900      192.168.69.111:48191  TIME_WAIT
TCP    192.168.69.123:5900      192.168.69.111:48192  TIME_WAIT
TCP    192.168.69.123:5900      192.168.69.111:48194  ESTABLISHED
TCP    192.168.69.123:16868     0.0.0.0:0          LISTENING
TCP    192.168.149.1:139       0.0.0.0:0          LISTENING
TCP    192.168.149.1:6917      0.0.0.0:0          LISTENING
TCP    192.168.150.1:139       0.0.0.0:0          LISTENING
TCP    192.168.150.1:11017     0.0.0.0:0          LISTENING

C:\Documents and Settings\doug>
```

- 1) What other switch on netstat maybe helpful?
- 2) What are the connected ports?
- 3) Is nbtstat useful in this case?
- 4) Can realvnc transfer files? Is there a version that can?

## CHALLENGE

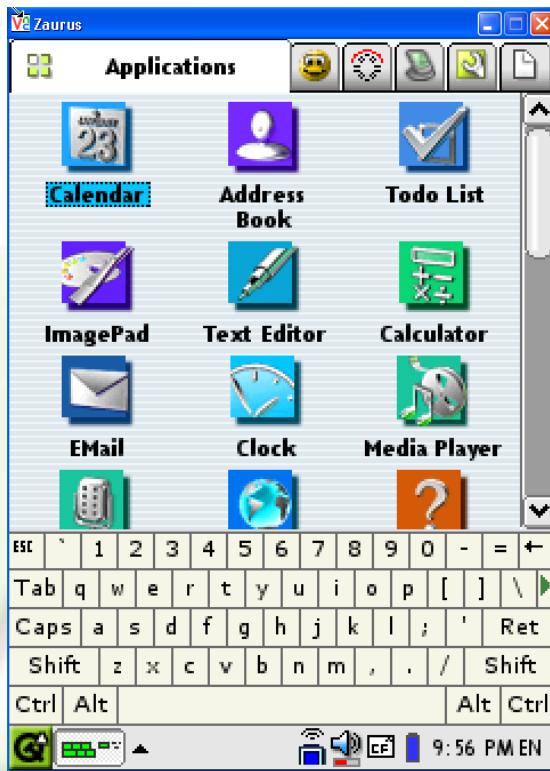
Configure two machines as both client and server then connect to each other. What happened? What did you expect?

Configure vnc to use an ssh tunnel.

## Summary Discussion

This lab is a practical exercise using realvnc to connect cross platform. Try to connect Windows to Windows and Linux to Linux with both the viewer and browser.

VNC is available on many platforms. It can be used as an administration tool or remote access. Here is an example of connecting from a Windows box to a Zaurus.



There are versions out for PocketPC and Palm OS. Additionally there are several companies that make enhancements to the original product. They will allow for PC control of the PDA and give you full size screen and keyboard.

## **Appendix:**

This lab was developed using VNC 3.3.7. The latest version as of this writing is version 4.1.1, which can be obtained from,

[www.realvnc.com](http://www.realvnc.com)

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

