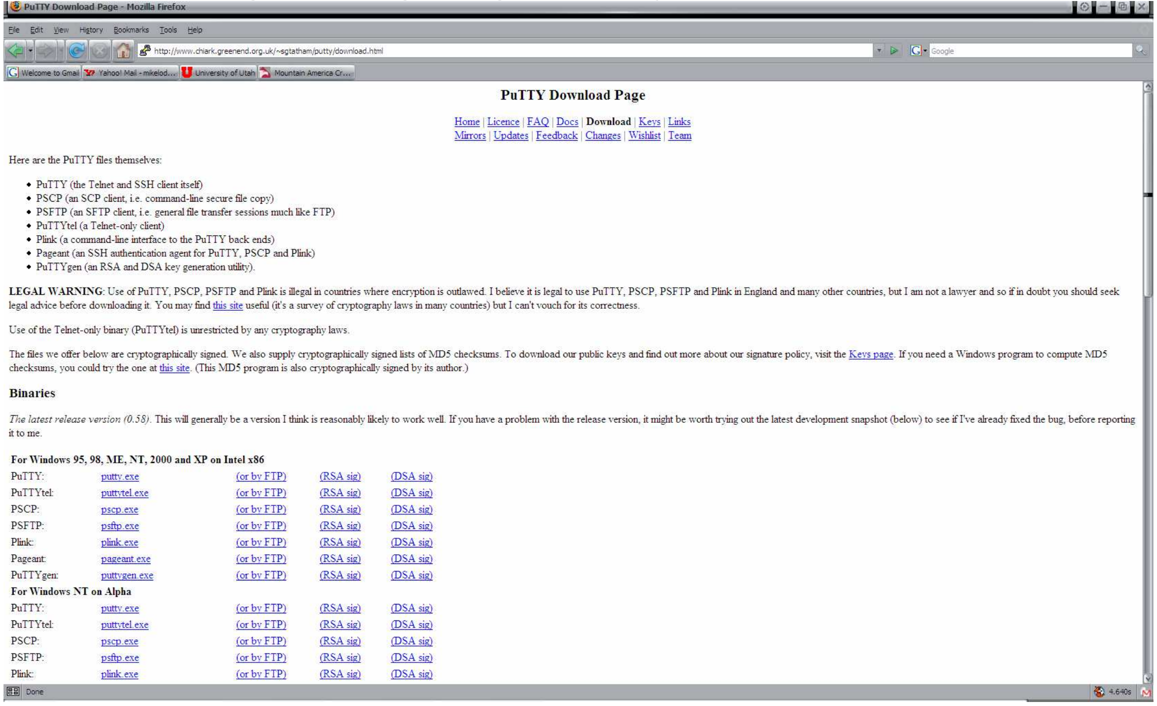
To remotely use the tools in the CADE lab, do the following:

Windows:

PUTTY:

Putty happens to be the easiest ssh client to use since it requires no installation.
You can download it at:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html


PuTTY Download Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Google
Welcome to Gmail
Yahoo! Mail - mikelod...
University of Utah
Mountain America Cr...
Done
4.640s

PuTTY Download Page

Home | Licence | FAQ | Docs | **Download** | Keys | Links
Mirrors | Updates | Feedback | Changes | Wishlist | Team

Here are the PuTTY files themselves:

- PuTTY (the Telnet and SSH client itself)
- PSCP (an SCP client, i.e. command-line secure file copy)
- PSFTP (an SFTP client, i.e. general file transfer sessions much like FTP)
- PuTTYtel (a Telnet-only client)
- Plink (a command-line interface to the PuTTY back ends)
- Pageant (an SSH authentication agent for PuTTY, PSCP and Plink)
- PuTTYgen (an RSA and DSA key generation utility).

LEGAL WARNING: Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. I believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and many other countries, but I am not a lawyer and so if in doubt you should seek legal advice before downloading it. You may find this site useful (it's a survey of cryptography laws in many countries) but I can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

The files we offer below are cryptographically signed. We also supply cryptographically signed lists of MD5 checksums. To download our public keys and find out more about our signature policy, visit the Keys page. If you need a Windows program to compute MD5 checksums, you could try the one at this site. (This MD5 program is also cryptographically signed by its author.)

Binaries

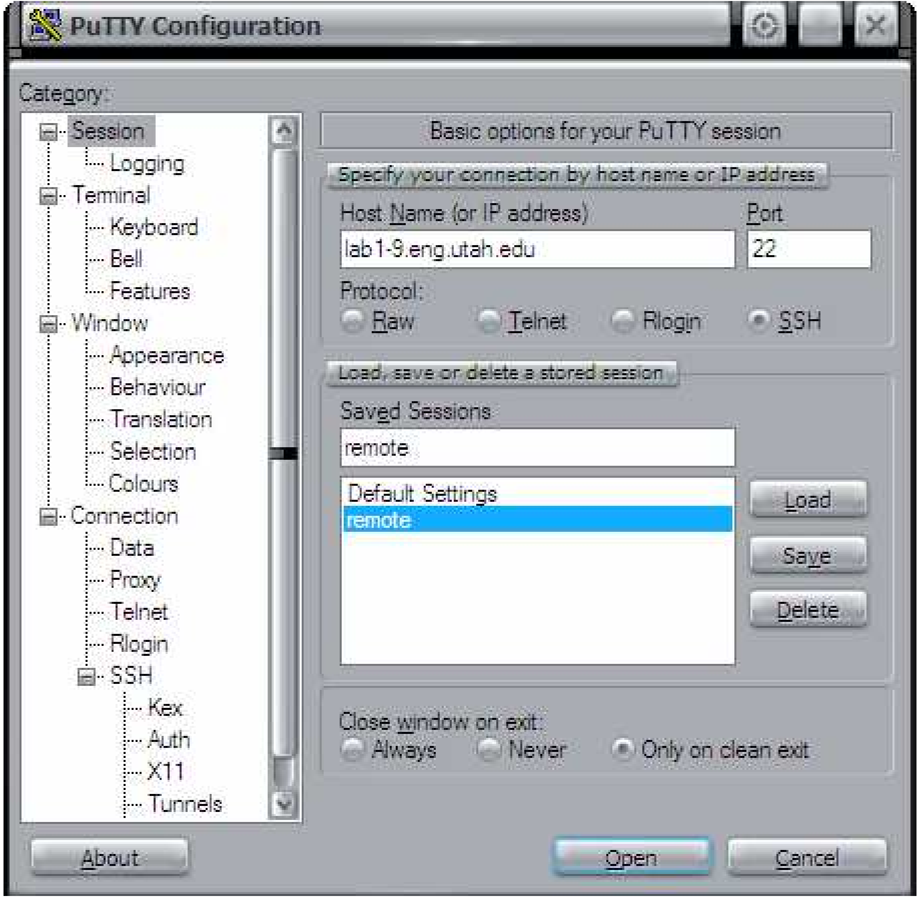
The latest release version (0.58). This will generally be a version I think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if I've already fixed the bug, before reporting it to me.

For Windows 95, 98, ME, NT, 2000 and XP on Intel x86				
PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink:	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)
Pageant:	pageant.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYgen:	puttygen.exe	(or by FTP)	(RSA sig)	(DSA sig)
For Windows NT on Alpha				
PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink:	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)

Under the section **For Windows 95, 98, ME, NT, 2000 and XP on Intel x86**
Click on putty.exe to download it.

Setting up Putty:

Double click on putty.exe and the following window should come up



Host Name (or IP address): lab1-9.eng.utah.edu
Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Saved Sessions: remote

Default Settings
remote

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

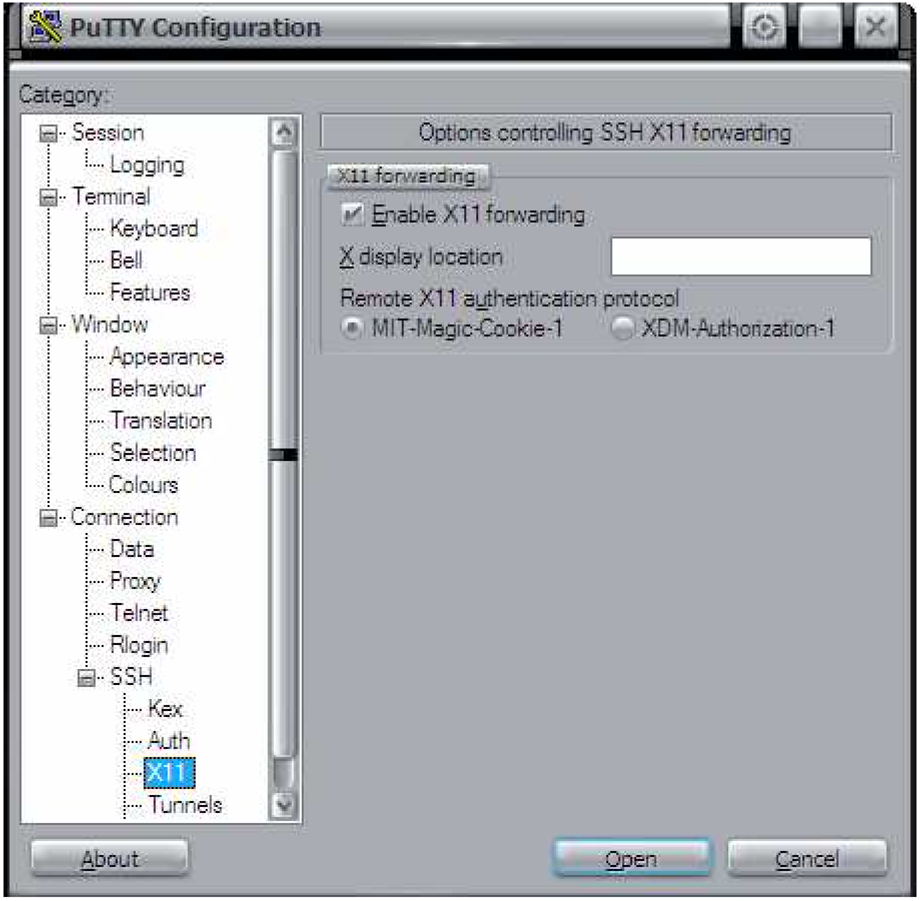
In the Host Name (or IP address) field you put the name of the computer you want to connect to in the CADE lab. lab# - # . eng . utah . edu

In my case I want to connect to lab1-9.eng.utah.edu

Leave the port settings on default at 22.

Leave the protocol on ssh as this is secure and will keep your password secure.

Next, in the left hand window select X11 tab



Options controlling SSH X11 forwarding

X11 forwarding

☑ Enable X11 forwarding

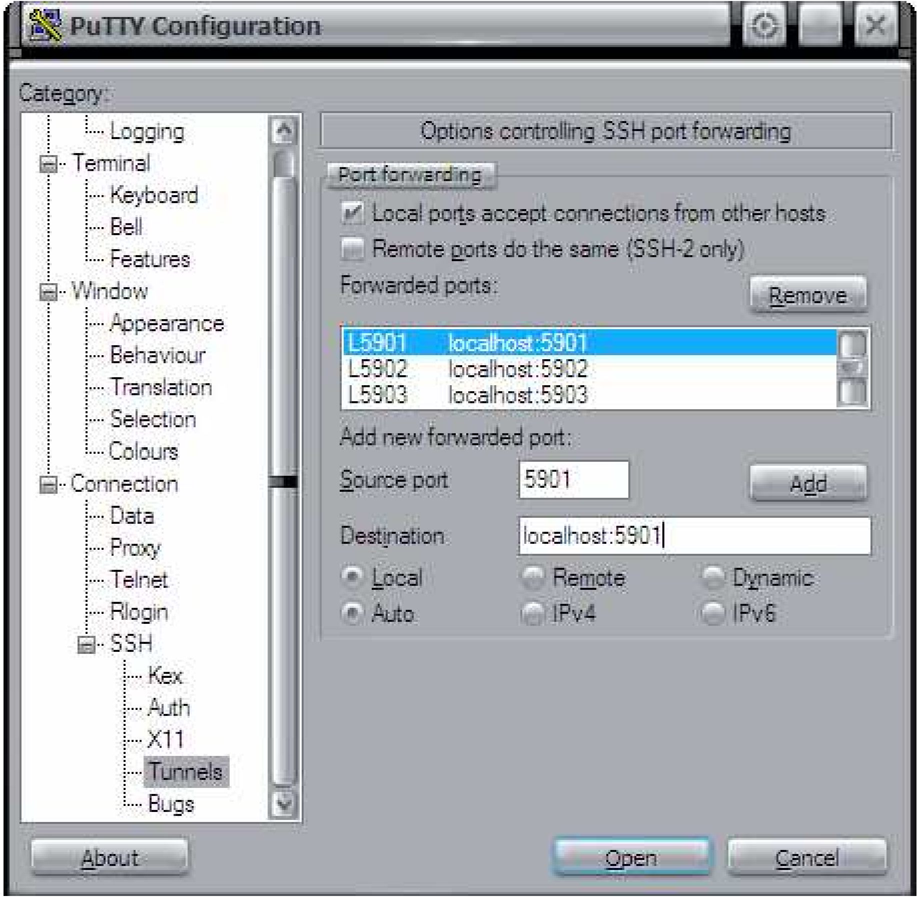
X display location

Remote X11 authentication protocol

● MIT-Magic-Cookie-1 ○ XDM-Authorization-1

Make sure the Enable X11 forwarding box is checked as this forwards the necessary packets to your computer.

Next, in the left hand window select Tunnels tab
Check the box that says Local ports accept connections from other hosts



☑ Local ports accept connections from other hosts
☐ Remote ports do the same (SSH-2 only)

Forwarded ports:

```
L5901   localhost:5901
L5902   localhost:5902
L5903   localhost:5903
```

Add new forwarded port:

Source port: 5901

Destination: localhost:5901

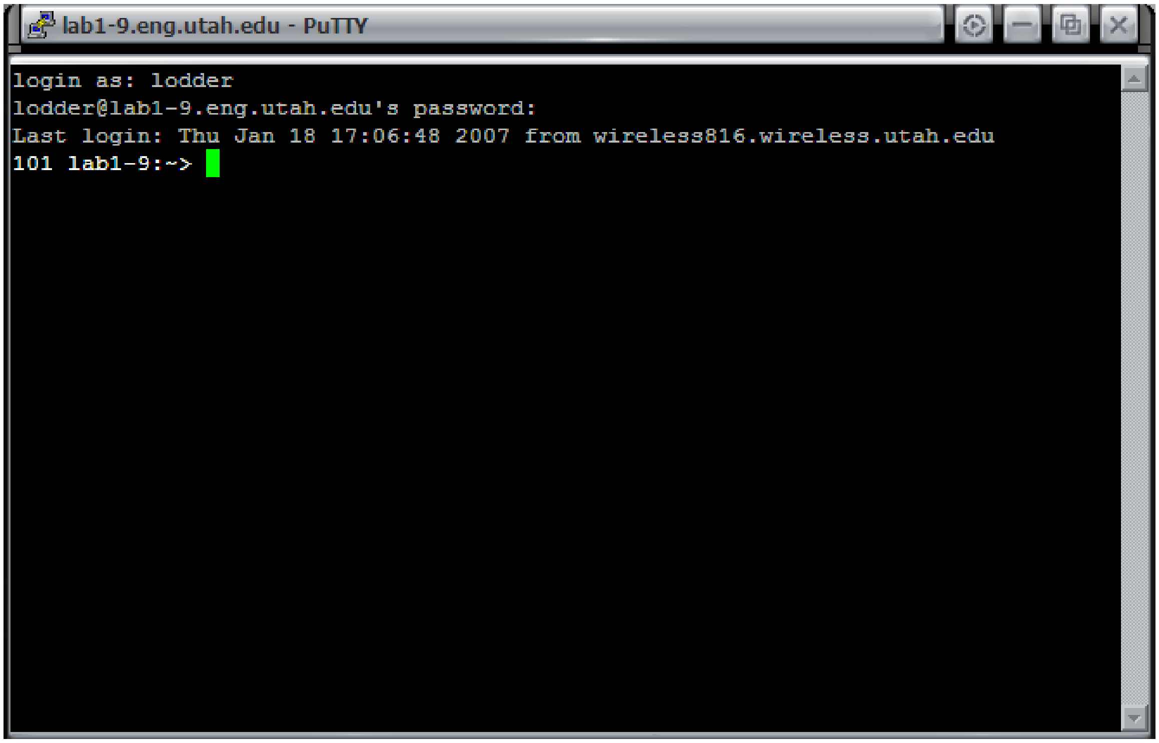
● Local ○ Remote ○ Dynamic
● Auto ○ IPv4 ○ IPv6

Now, in the box that says Source port, you want to put the starting port number that the CADE computers forward from i.e. the port you want to read the packets from. This happens to be 5901 and up. So I put 5901. In the box that says Destination, this is where you want to forward the packets to, i.e. your home computer ip address and port. In this case localhost:5901. **The Port numbers must match in the destination and source or the this won't work.** Then click add.

NOTE
You may type 127.0.0.1:(port number) instead of localhost as this means the same thing.

Another NOTE
You may want to read more than one port to read from by repeating what you did above. Just change the port number, 5902, 5903, 5904 etc. 3 ports is usually sufficient depending how many people are running VNCServer remotely.

When done click open and the following window should appear asking you to log in...



```
login as: lodder
lodder@lab1-9.eng.utah.edu's password:
Last login: Thu Jan 18 17:06:48 2007 from wireless816.wireless.utah.edu
101 lab1-9:~>
```

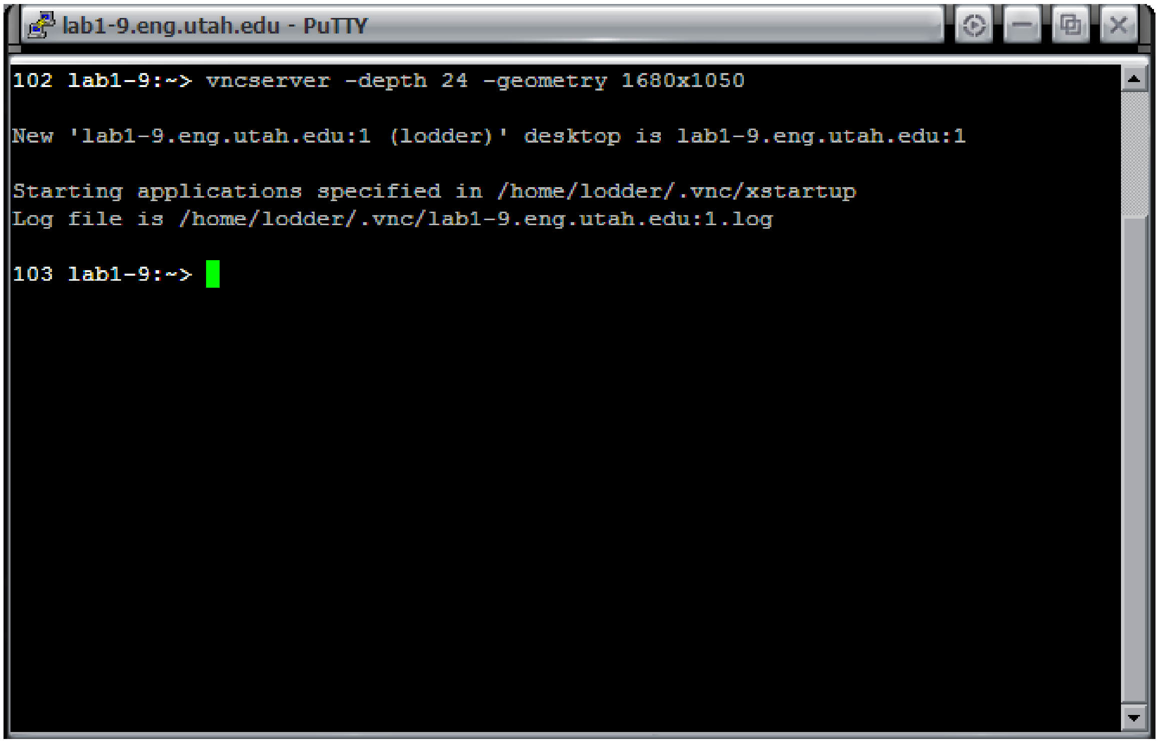
In this new window, you need to start the VNCserver on the CADE lab machine.
Do this by typing the following

vncserver -depth 24

where vncserver is the command, depth is the number of colors you want the screen to use, 24 is the highest number they go, sorry. (**Note** you may even change the size of the screen by adding the following argument.

vncserver -depth 24 -geometry 1280x1024

where the two numbers is the screen size you want to view)
When done hit return and the following should be returned.



```
102 lab1-9:~> vncserver -depth 24 -geometry 1680x1050

New 'lab1-9.eng.utah.edu:1 (lodder)' desktop is lab1-9.eng.utah.edu:1

Starting applications specified in /home/lodder/.vnc/xstartup
Log file is /home/lodder/.vnc/lab1-9.eng.utah.edu:1.log

103 lab1-9:~> 
```

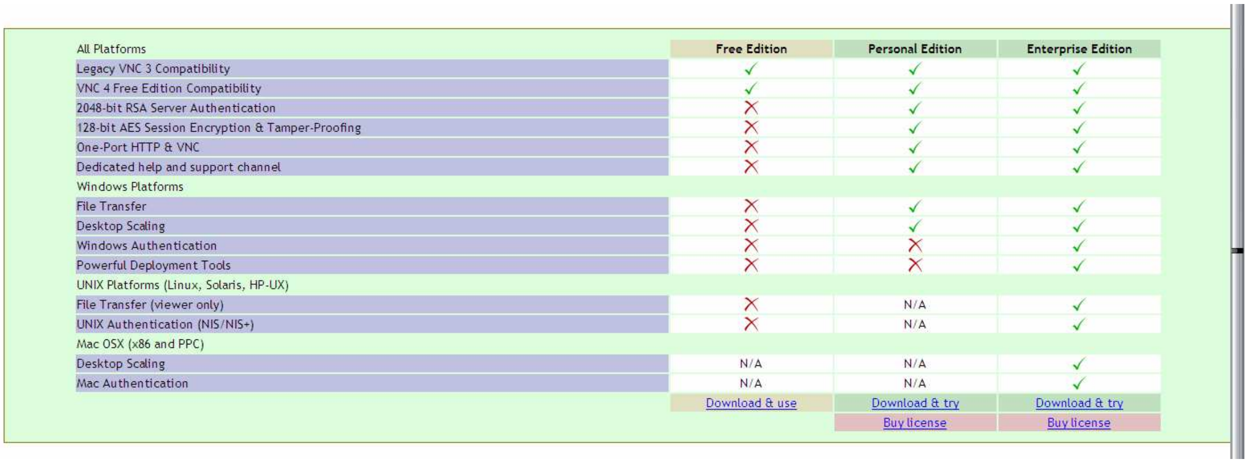
The number after the computer name is the open port that vncserver is forwarding on. This is usually the first open port available, in this case **:1**

Remember this number as this is the port vncserver needs to read.

VNCServer:

If VNCserver is not installed on your computer you can get it for free at

http://www.realvnc.com/download.html



All Platforms	Free Edition	Personal Edition	Enterprise Edition
Legacy VNC 3 Compatibility	✓	✓	✓
VNC 4 Free Edition Compatibility	✓	✓	✓
2048-bit RSA Server Authentication	✗	✓	✓
128-bit AES Session Encryption & Tamper-Proofing	✗	✓	✓
One-Port HTTP & VNC	✗	✓	✓
Dedicated help and support channel	✗	✓	✓
Windows Platforms			
File Transfer	✗	✓	✓
Desktop Scaling	✗	✓	✓
Windows Authentication	✗	✗	✓
Powerful Deployment Tools	✗	✗	✓
UNIX Platforms (Linux, Solaris, HP-UX)			
File Transfer (viewer only)	✗	N/A	✓
UNIX Authentication (NIS/NIS+)	✗	N/A	✓
Mac OSX (x86 and PPC)			
Desktop Scaling	N/A	N/A	✓
Mac Authentication	N/A	N/A	✓
	Download & use	Download & try	Download & try
		Buy license	Buy license

On the free version click Download & use

On the next page that asks you to register just click **Proceed to download**

On the next page, download the appropriate version for the operating system you have. In my case, I would click executable for V**NC Free Edition for Windows.**

Once you have installed VNCserver proceed.

Opening the window to view remote desktop:

Start VNCserver if it is not running, start it in windows by

Start -> All Programs -> RealVNC -> VNCserver

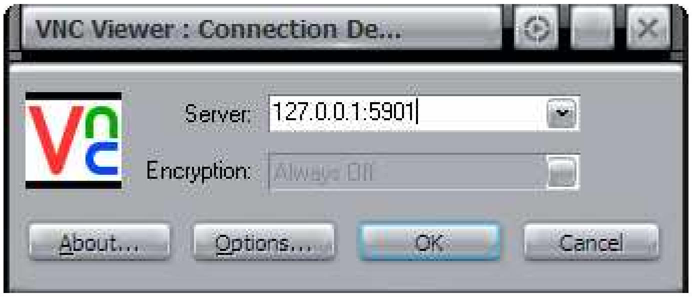
In Linux, you type the exact same command as you did above.

vncserver -depth 24

Next start a VNCViewer. In windows

Start -> All Programs -> RealVNC -> Run VNCViewer

The following window should come up



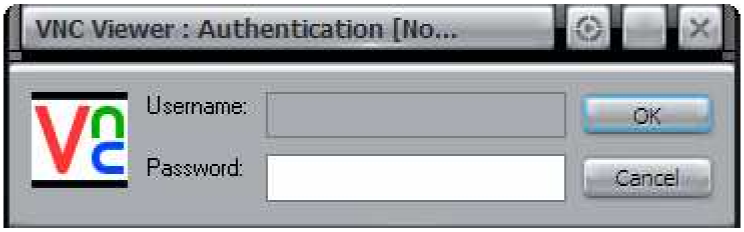
Server: 127.0.0.1:5901

Encryption: Always Off

In the server field you are going to type localhost or 127.0.0.1 and the 590# where # is the number generated from the CADE lab machine when you started vncserver.

In this case its 1. Then click OK

If the following window comes up, type your CADE lab password in the box and click OK. (This may be set to whatever password you want. This is the password to use VNCserver. You definitely want to set this to something as no password will allow anyone to VNC onto your computer. I just set it to the CADE lab password as its easy to remember).



For Linux users type the following

vncviewer   lab1-9.eng.utah.edu:5901

The machine name should be what you are logged into. In this case lab1-9.

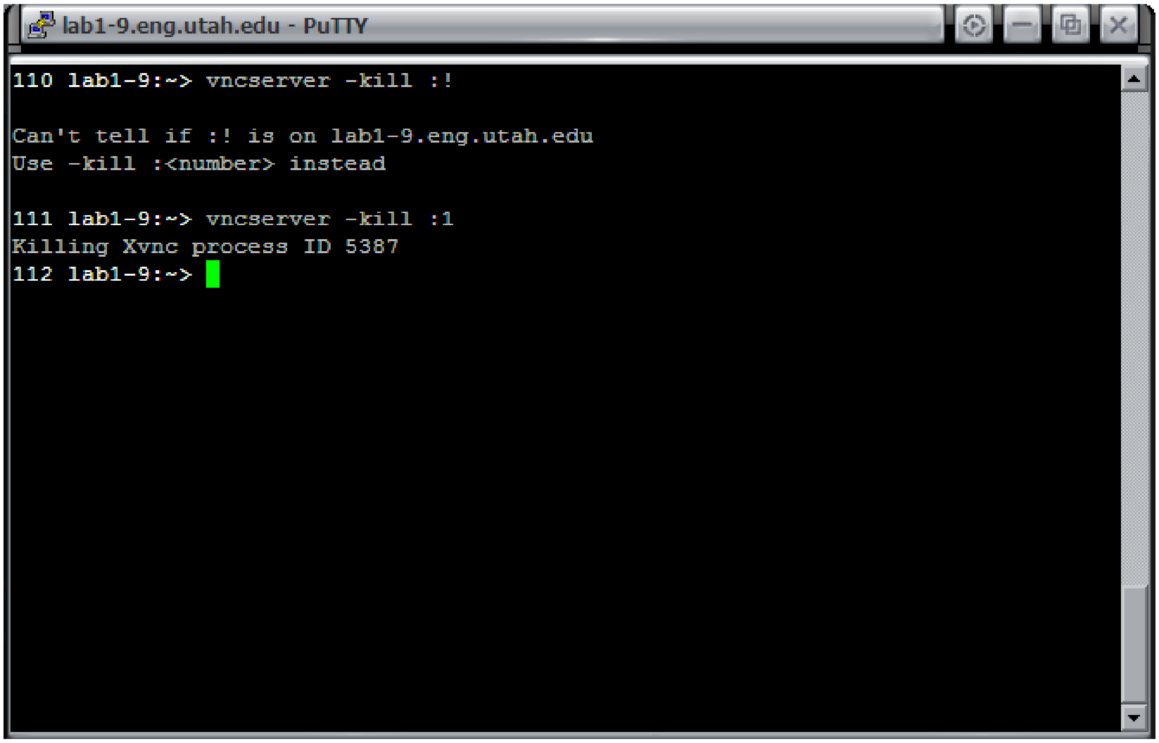
It should prompt you for your CADE lab password then hit enter.

Bingo, your done until its time to close down the machine.

MAKE SURE YOU DO THIS STEP WHEN YOU CLOSE DOWN VNCSERVER. IF YOU DON'T THEN VNCSERVER WILL GET REALLY SLOW AND INEFFICIENT

Close down the VNCViewer. To close down the vncserver, type the following

vncserver -kill :1 or whatever port you where using.
This frees the port for someone else to use.



```
110 lab1-9:~> vncserver -kill :!

Can't tell if :! is on lab1-9.eng.utah.edu
Use -kill :<number> instead

111 lab1-9:~> vncserver -kill :1
Killing Xvnc process ID 5387
112 lab1-9:~>
```