Tunneling & UW Oshkosh

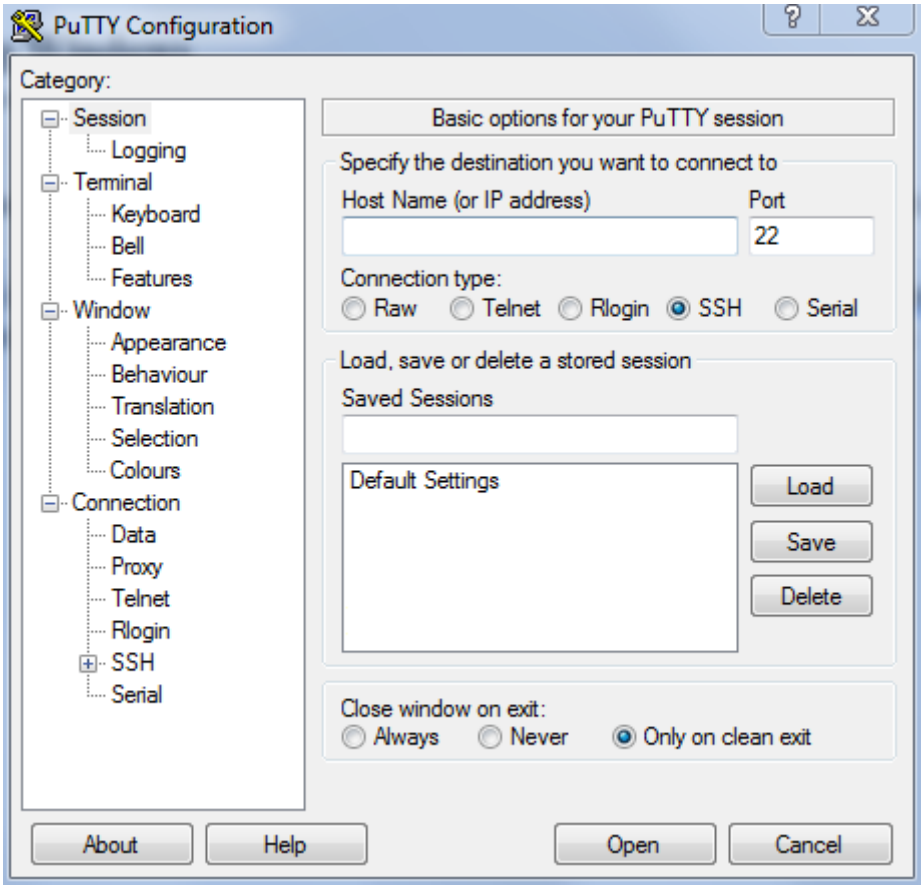
By Cooper Walbrun

Tunneling on Windows

See Page 5 for Linux tunneling

1. Download and install PuTTY if it is not installed already on your current computer.

2. When you launch it, you will see a screen similar to the one below. *If at any point you encounter problems with PuTTY, try re-launching it with Administrative privileges.*

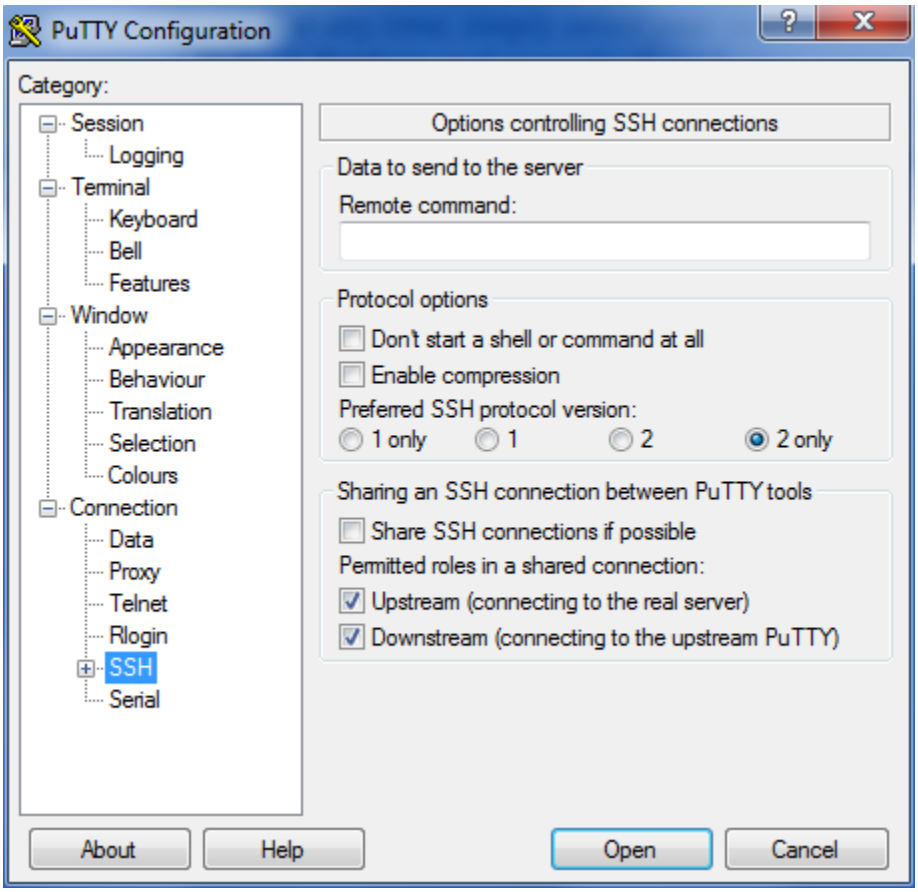


3. Create a new Saved Session so you don't have to set up PuTTY for tunneling every time. Do this by typing something like *softeng tunnel* in the textbox below **Saved Sessions**. Click **Save**. You should see your session appear in the listbox below **Default Settings**.

4. In the **Host Name (or IP address)** textbox, type *ssh.acs.uwosh.edu*. This is the server that you log into in the Linux lab in Halsey. Type *1022* in the **Port** textbox right next to it.

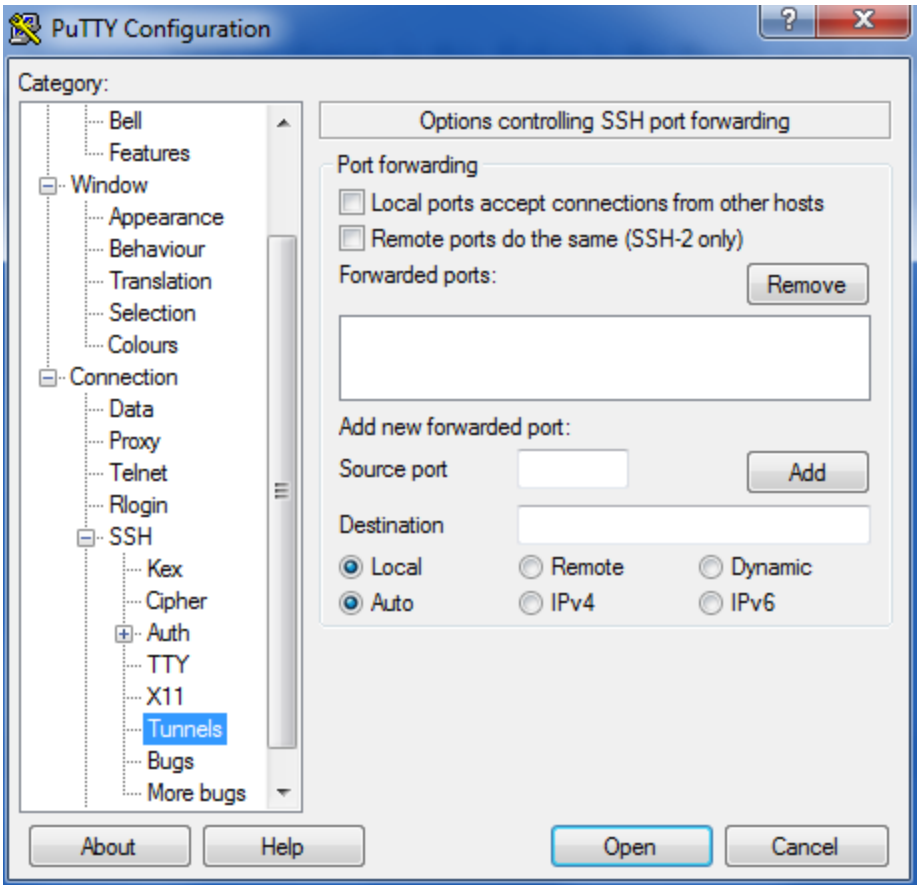
*Tip: to save your session changes at any time, return to this window and select your session's name in the listbox containing **Default Settings**, then press the **Save** button again.*

5. From the option tree on the left, click on **SSH** under the **Connection** branch. You will see the following window.



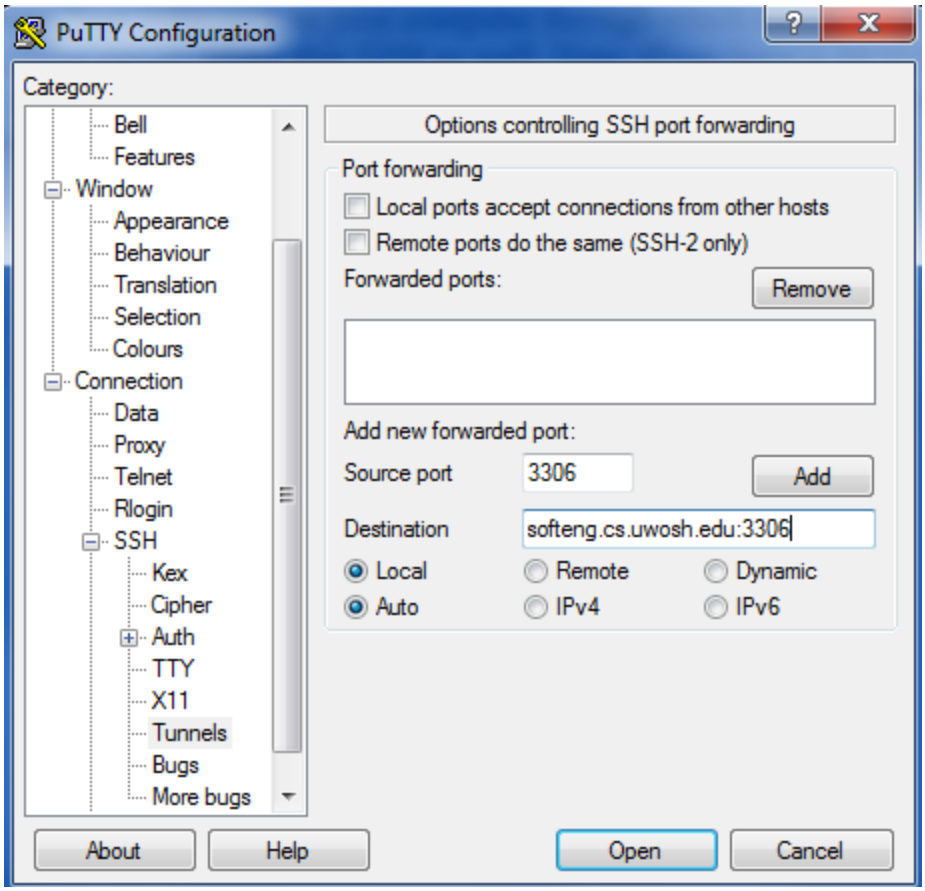
6. The only thing you have to change in this window is the **Don't start a shell or command at all** checkbox. Tick it.

7. Click the plus button to the left of **SSH** in the option tree. In the subtree that appears, click **Tunnels**. Now you should see the window shown on the next page.



8. This is where the actual tunnel is defined. The MySQL server for CS 341 is on *softeng.cs.uwosh.edu*, so you should type that into the **Destination** textbox. However, we are forwarding traffic to the MySQL port on this server, so you also have to append *:3306* to the end of this address.

9. The **Source Port** is the port on your computer through which traffic will be sent to the port on the *softeng* server. Make this *3306* as well. *Note: if you have a MySQL server running on your computer, change the port to 3307 and see* this document *for more details.* After you complete this step, the window should look like the one on the next page.



10. Click the **Add** button to the right of the **Source Port**. Now is a good time to save your session again, because you are done setting up your tunnel!

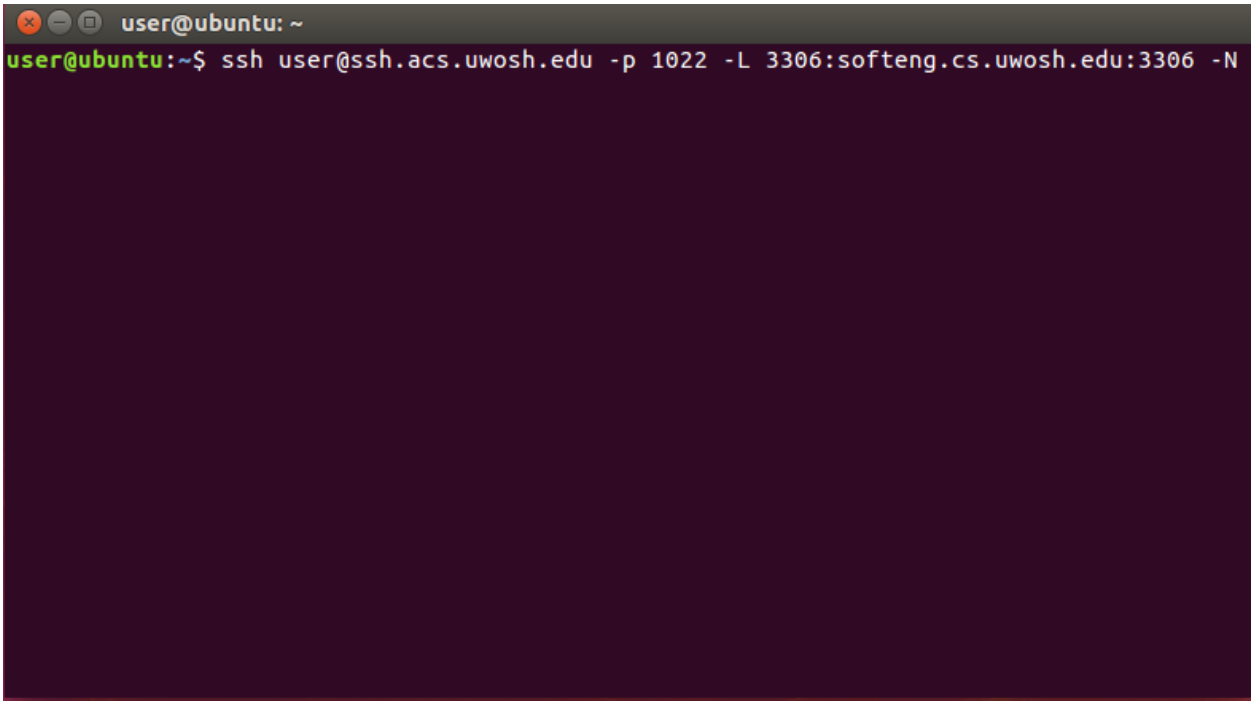
11. Click the **Open** button and in the terminal that opens, enter your **Halsey Linux lab login credentials**. The terminal hides your password from you, so do not be alarmed if you do not see characters appearing when you type your password. After you press enter to login, the terminal will appear to hang and do nothing. This is good; that means the tunnel is established. *Note: the tunnel is only established as long as the terminal window is open. Once you close out of it, the tunnel closes.* Now you can proceed with accessing your database via Visual Studio or whatever other means available (using localhost for your MySQL connection address).

If you get an "Access Denied" error while trying to do Step 11, it is almost always because your credentials were invalid. Be careful when typing your password.

Tunneling on Linux

1. Make sure you have SSH installed on your computer. If you do not, issue the command `sudo apt-get install openssh-client` (on Debian-based Linux distributions).

2. Now, all you have to do to establish a tunnel is issue a single *ssh* command, as shown below.



This single command does exactly the same thing PuTTY does (per the setup described on Pages 1 through 4 of this document). Here's a breakdown of the command:

- The *user* part of *user@ssh.acs.uwosh.edu* should be changed to whatever your Halsey Linux lab username is.
- *-p 1022* tells the SSH client to connect to *ssh.acs.uwosh.edu* on port *1022*.
- *-L* tells the SSH client to create a tunnel to the address that follows, using the given ports.
- *3306:softeng.cs.uwosh.edu:3306* is, in this order: *local-machine-port:host:host-machine-port*. *Note: if you have a MySQL server running on your computer, change the local-machine-port to 3307 and see* this document *for more details.*
- *-N* simply tells the SSH client to not start a command shell on the target server (accomplishes the same thing as Step 6 in the Windows tunneling guide).

3. After you issue the command, you will be prompted for your Halsey Linux lab password. The terminal hides your password from you, so do not be alarmed if you do not see characters appearing when you type your password. After you press enter to login, the terminal will appear to hang and do nothing. This is good; that means the tunnel is

established. *Note: the tunnel is only established as long as the terminal window is open. Once you close out of it, the tunnel closes.*

If you get a "Permission Denied" error while trying to do Step 3, it is almost always because your credentials were invalid. Be careful when typing your password.