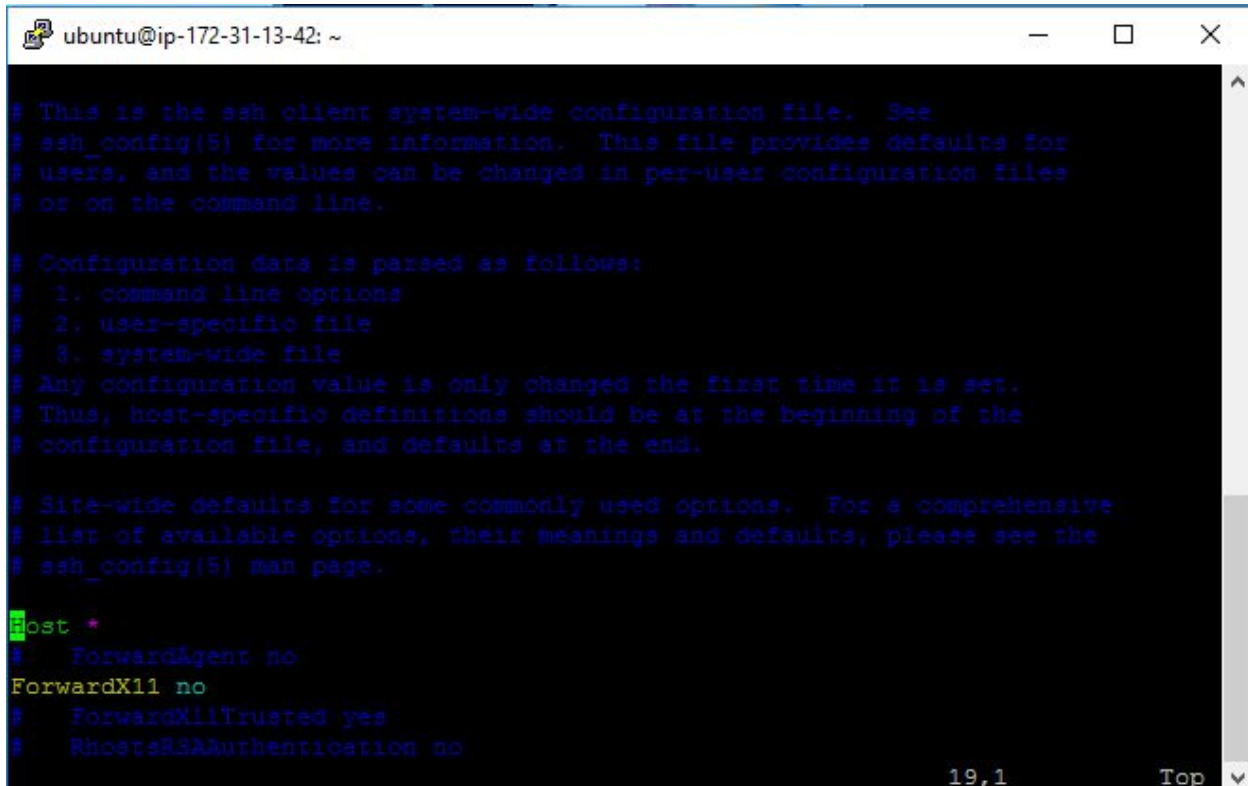


## Prerequisites

- Set up Xming X Server: <http://sourceforge.net/projects/xming>

### Step 1:

Log in to your AWS instance. Using nano or vi, edit /etc/ssh/ssh\_config. Uncomment ForwardX11 and save the file.



```
ubuntu@ip-172-31-13-42: ~
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information. This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file
# 3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

Host *
# ForwardAgent no
ForwardX11 no
# ForwardX11Trusted yes
# RhostsRSAAuthentication no

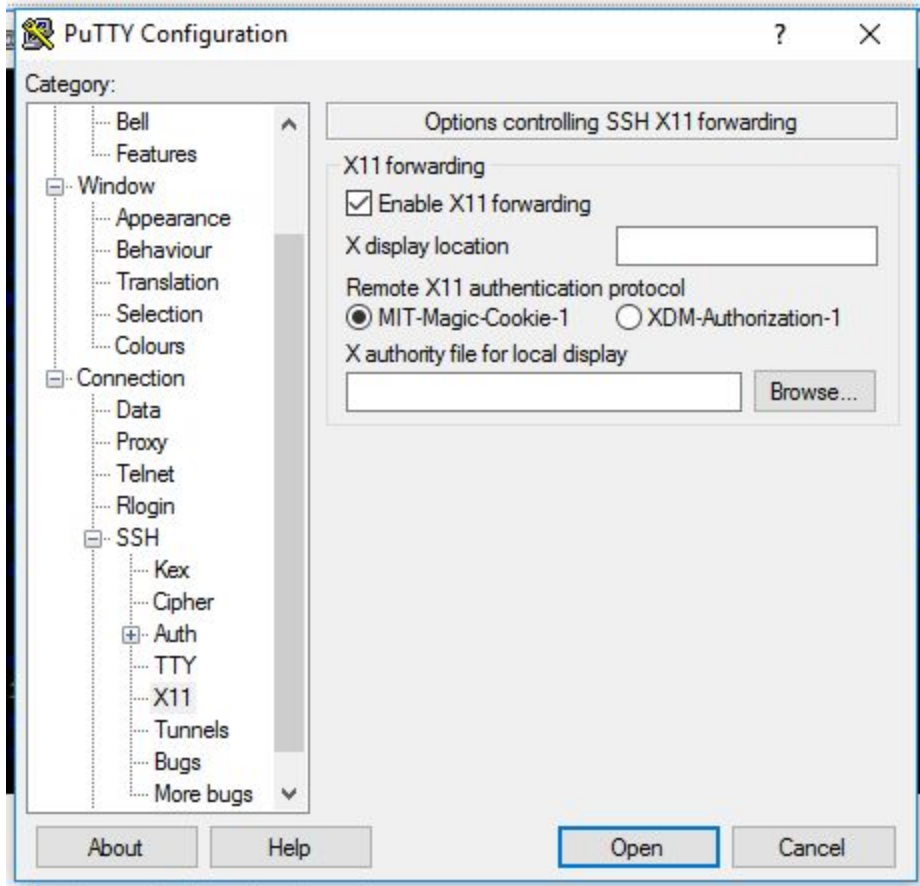
19,1 Top
```

### Step 2:

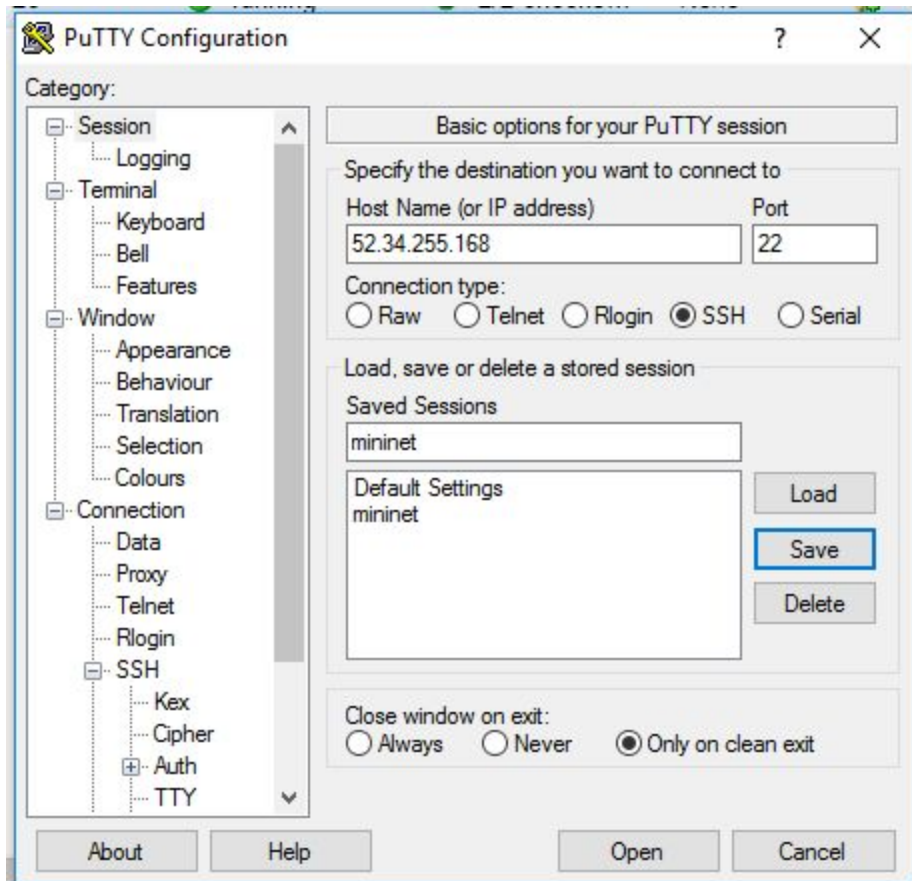
Reboot your instance (sudo reboot now)

### Step 3:

Make sure Xming is running. Open PuTTY and set it up as before (using your IP and key file.). This time, also enable X11 Forwarding in Connection > SSH > X11.



To make this easier to do later, you should save a profile. Go back to the first tab, type a name, and select Save. You can click this when you need to use it in the future and select Load to restore the configuration.



#### Step 4:

Install wireshark

```
sudo apt-get update
```

```
sudo apt-get install wireshark
```

#### Step 5:

Set up OpenFlow plugin

Run commands:

```
sudo apt-get install libgtk2.0-dev
```

```
cd ~/openflow/utilities/wireshark_dissectors
```

Edit file: packet-openflow.c

Change line 769 from:

```
dissector_add(TCP_PORT_FILTER, global_openflow_proto, openflow_handle);
```

to

```
dissector_add_uint(TCP_PORT_FILTER, global_openflow_proto, openflow_handle);
```

Run command:

```
make
```

```
sudo cp packet-openflow.so /usr/lib/wireshark/libwireshark1/plugins/
```

**Conclusion:**

At this point, you should be all set. To do labs, open up two SSH sessions. In one, you can run Wireshark (sudo wireshark), and in the other you can do the modifications/run Mininet.