## Running sshd

# systemctl enable sshd

# systemctl start sshd

## SSH to a remote server

> ssh-keygen

copy ~/.ssh/id\_rsa.pub to ~/.ssh/authorized\_keys for users account on the server

## SSH To Remote Client behind NAT ssh'ed to remote server

The remote client runs ssd listening on some port, say 22. Then we setup port forwarding from the local client passing through the server.  
  
The sshd can be set to run on boot, but more work needs to be done so that the tunnel

will also come back up.

ssh to a remote client that is behind a NAT firewall and currently ssh'ed into a shared *server* (aka *host*):

https://superuser.com/questions/277218/ssh-access-to-office-host-behind-nat-router

https://www.linux.com/news/keeping-your-ssh-connections-alive-autossh

remote-client$ autossh -R 2222:localhost:22 user@server

local$ autossh -L 2223:localhost:2222 user@server

local$ ssh user@server -p 2223

these fail because autossh requires a -M option -M 0 for example

just replaced these with ssh for now. ssh needs -N or it logs in.

remote-client$ ssh -N -R 2222:localhost:22 user@server

local$ ssh -N -L 2223:localhost:2222 user@server

local$ ssh user@server -p 2223

https://www.everythingcli.org/ssh-tunnelling-for-fun-and-profit-tunnel-options/

https://linuxconfig.org/how-to-install-start-and-connect-to-ssh-server-on-fedora-linux

https://www.everythingcli.org/