Steps required to set-up the Raspberry Pi cameras:

You will need the following:

1. A switch with as many ports as raspberry Pi's as you want to link together
2. Number and length of network cable as required
3. A computer with either only the one ethernet port on the mother board or a dedicated ethernet card with 1 or more ports

Connect everything needed but the power cords for the raspberry pis and the ethernet switch. Make sure the RPs are connected through the switch and that the switch is connected to the an ethernet port on the computer that you want to use. Turn on the network switch, wait 2 mins and then turn on the computer.

Set a static ip address to your Raspberry pi(s) to be on the same subnet as your switch (192.168.0.XX)

USE - *sudo nano /etc/network/interfaces*, to configure your raspberry pi to look like this:

*auto lo*

*iface lo inet loopback*

*iface eth0 inet static*

*address 192.168.0.10*

*netmask 255.255.255.0*

*broadcast 192.168.0.255*

On the main computer, configure your ethernet port to be on the same subnet as your switch (192.168.0.XX), again using *sudo nano /etc/network/interfaces*:

*auto eth1*

*iface eth1 inet static*

*address 192.168.0.200*

*netmask 255.255.255.0*

*network 192.168.0.0*

*broadcast 192.168.0.255*

After, in the command line enter:

*sudo /etc/init.d/networking restart*

*sudo ifup eth1*

Now that all the items can communicate through the same subnet and the network is set up. You should test the system by pinging in the following order: the ethernet port on your computer and then the raspberry pi. USE *ping 192.168.0.XX*  in the command line.

**Some useful commands for networking with ssh:**

SSH on the client computer keeps a record of a key it uses to make sure the client trying to connect has been validated in the past. If you try to use the Raspberry pi with a different sd card (for example a fresh noobs installation and a new ip address) then ssh will give you a nasty error saying you might being attacked by a man-in-the-middle.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

bb:74:b8:d4:21:fc:8f:5c:f2:ad:99:19:ea:7e:25:13.

Please contact your system administrator.

Add correct host key in /home/jason/.ssh/known\_hosts to get rid of this message.

Offending ECDSA key in /home/jason/.ssh/known\_hosts:1

remove with: ssh-keygen -f "/home/jason/.ssh/known\_hosts" -R 192.168.0.10

ECDSA host key for 192.168.0.10 has changed and you have requested strict checking.

All you need to do to correct this is use the command:

ssh key-gen -R 192.168.0.10 (or the offending IP address that is causing the conflict). The next time you try to ssh into the pi it will ask you if you accept to place a key in the known\_hosts registry (**~/.ssh/known\_hosts** file. "~" is a shortcut for your home directory).