Raspberry Pi OS Setup

Contents

Usernames and Passwords

Default Username: pi Password: raspberry

Raspberry Pi Install

1. Use Raspberry Pi Imager to Create a MicroSD card image.
    a. Choose OS: Raspberry Pi OS

b. Choose Storage: MicroSD adapter

c. Click the Gear at the bottom right.

d. Set hostname

e. Enable SSH → Use password authentication

f. Set username and password: pi Password01

g. Configure wireless LAN

h. Set local settings.

i. Write file to MicroSD card

2. Insert MicroSD card → turn on Pi.
3. Use a port scanner to find the IP address.
4. Go to https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
5. Download the **PuTTY** client.
6. Start the **PuTTY** client. Type in the **IP address** of the GiPiGo3 → Click **Open**.
7. **Accept** the **PuTTY Security Alert**.
8. Login as: **pi** Password: **Password01**
9. Type: **sudo raspi-config**
10. **Display Options** → **VNC Resolution** (Set resolution for monitor and RealVNC)

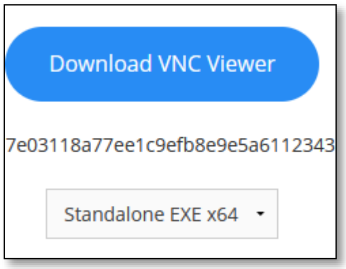
    a. **1280x1024** (pi)

    b. **1024x768** (pi zero)

11. **Interface Options → VNC** → Select **Yes.**
12. **Interface Options -> I2C →** Select **Yes.**
13. **Advanced Options** → **A1 Expand Filesystem**
14. Select **Finish** to reboot and resize disk.

RealVNC Viewer

RealVNC viewer allows us to remotely control the GoPiGo3 in headless mode.



1. Go to https://www.realvnc.com/en/connect/download/viewer/
2. Download the VNC Viewer Standalone EXE anywhere you want to run the program from. You don't have to install it.
3. Double Click **VNC Viewer**.
4. Type in the IP address of your robot → Click **Connect**.

Update Raspberry Pi OS

At a terminal:

sudo apt update

sudo apt dist-upgrade -y

sudo apt autoremove

Configure Raspberry Pi OS

1. **Change Clock Display:** Right Click Clock, Digital Clock Settings
    a. To show seconds, **%r**
    b. To show minutes: **%I:%M %p**
2. **Add Temperature Monitor:** Right Click Task Bar → Panel Settings → Panel Applets tab.
    a. **Add** → **Temperature Monitor** → **Add**.
    b. Click **Up** to move the Temperature Monitor to the left on the taskbar.
    c. Click **Preferences**.
        i. **Normal color**: **#00008b** (Dark blue)
        ii. **Warning1 temperature**: 60
        iii. **Warning2 temperature**: 80

Email IP on Boot

1. Create a Code folder → **home/pi/Code**
2. Copy **startup_mailer.py** to this folder
3. Open a terminal.
4. Type in the following to make the script executable.

```
sudo chmod 755 /home/pi/Code/startup_mailer.py
```

5. There should not be any errors if the command was successful.
6. Test the script with the following command.

```
python3 /home/pi/Code/startup_mailer.py
```

7. In a few moments, you should receive an email with your Raspberry Pi IP address.

Run startup_mailer.py Script on Startup

1. At the terminal, type in the following command to access the Raspbian scheduler. (Don't add sudo)

```
crontab -e
```

2. Press **Enter** to edit the file with nano.
3. Cursor to the bottom of the file. (The mouse will not work.)
4. Enter the following information. (**sleep 15** waits 15 seconds after startup to run the script.)

```
@reboot sleep 15 && python3 /home/pi/Code/startup_mailer.py
```

5. Type **CTRL+S** to Save the file.
6. Press **CTRL+X** to Exit nano.
7. Type **sudo reboot**
8. You should receive an email with your IP address.

Disable Onboard Wi-Fi

Any external Wi-Fi antenna will have better signal strength and range. To use an external Wi-Fi antenna only, disable the internal Wi-Fi.

```
# Edit this file with nano
sudo nano /boot/config.txt
# Add this line to the end of the file and save it
dtoverlay=disable-wifi
```

After you have disabled the on-board Wi-Fi, you must always plug a Wi-Fi adapter into a USB port.

Wi-Fi Signal Strength

The **iwconfig** command will give you a snapshot of Wi-Fi quality.

wavemon will monitor Wi-Fi signal strength in real time.

```
# Install wavemon
sudo apt install wavemon -y
# Run wavemon
wavemon
# Quit wavemon
q
```

```
iwconfig
```

```
sudo iwlist wlan0 scan | egrep "Cell|ESSID|Signal|Rates"
```

Signal Strength

The higher the signal strength, the more reliable the connection and higher speeds are possible. The signal strength is specified as -dBm (decibels related to one milliwatt).

Values between 0 and -100 are possible, with more being better. -51 dBm is a better signal strength than -60 dBm.

The value 0 is not realistic. Even -30 dBm is hard to reach, and you must stand almost directly next to the access point.

Some guidance on how to read the results:

- 50 dBm is considered an excellent signal strength.
- 67 dBm is said to be the minimum signal strength for reliable and relatively fast packet delivery.

- 70 dBm is the minimum signal strength for reliable packet delivery.
- The minimum value for a basic connection is -80 dBm. However, packet delivery is no longer necessarily reliable.
- 90 dBm is already very close to the basic noise. Here a connection probably does not work anymore.

Link Quality

A network can have very good signal strength without good link quality.

This is how much of the data you send and receive will make it to the destination in good condition.

The quality indicator includes data like Bit Error Rate (BER), i.e., the number of bit errors in received bits that have been altered due to noise, interference, distortion, or bit synchronization errors. Others are Signal-to-Noise and Distortion Ratio (SINAD).

It is measured in percentage or on a scale of up to 70. So you will see a value like “60/70”.

Unlike signal strength, it is somewhat harder to say which values are still considered to be ok.

If the value is low and your signal strength is high, you may have interference from, e.g., kitchen appliances or other electronic devices. Moving them further away may improve the link quality.

Frequency

Another interesting indicator is the Wi-Fi frequency.

This shows if your Raspberry Pi connects to the slower and longer range 2.4 GHz network, or the faster but shorter range 5 GHz version, provided, of course, that your router offers both networks.

Filesystem Checks and Repair

The Linux filesystem can be damaged under various circumstances, e.g., system crash, power loss, disconnected disk, accidentally overwritten i-node, etc. Thus it is a good idea to check the integrity of the filesystem regularly to minimize the risk of filesystem corruption.

The Linux filesystem can be damaged under various circumstances, e.g., system crash, power loss, disconnected disk, accidentally overwritten i-node, etc. Thus it is a good idea to check the integrity of the filesystem regularly to minimize the risk of filesystem corruption.
Add the following to `/boot/cmdline.txt`:

```
fsck.mode=force
```

Make sure that file remains all one line. Parameters should be separated with spaces.

You'll probably notice `fsck.repair=yes` is already there; these are not the same thing. From `man systemd-fsck` (these are parameters that are passed on by the kernel to init, i.e., systemd):

fsck.mode=

One of "auto", "force", "skip". Controls the mode of operation. The default is "auto", and ensures that file system checks are done when the file system checker deems them necessary. "force" unconditionally results in full file system checks. "skip" skips any file system checks.

fsck.repair=

One of "preen", "yes", "no". Controls the mode of operation. The default is "preen", and will automatically repair problems that can be safely fixed. "yes " will answer yes to all questions by fsck and "no" will answer no to all questions.

To do a filesystem check on the next reboot, do the following

```
sudo touch /forcefsck
```

Once you create an empty file named `forcefsck` in the root directory, it will force filesystem check the next time you boot up. After successful booting, `/forcefsck` will automatically be removed.

An alternative is to shut down the system with the `-F` option like this:

```
sudo shutdown -r -F now
```

Install Orange Pi Lite Armbian

http://www.armbian.com/orange-pi-lite/ Install image

https://docs.armbian.com/ Documentation

To connect to console, use usb mouse and keyboard, direct HDMI monitor

1. Download armbian Buster desktop
2. Logon: root Password: raspberry
3. Change root password: OrangePiLite1
4. Create new account: bill OrangePiLite1

5. Don’t change the display settings.
6. sudo apt-get update
7. sudo apt-get dist-upgrade -y

Setup Armbian

Connect with TightVNC: IP address:1

Change Time Zone: sudo timedatectl set-timezone America/Denver

Install Kali Linux 2.0

1. Install gparted: apt-get install gparted
2. Enter gparted at the command line. Use gparted to expand the partition to the whole drive.
3. **Install package:**
   a. apt-get update
   b. apt-get install kali-linux-full
4. **Normal update:**
   a. apt-get update
   b. apt-get upgrade
5. Remove unneeded packages: apt autoremove
6. Fix update: apt-get update –fix-missing

kali-linux-full

When you download a Kali Linux ISO, you are essentially downloading an installation that has the ***kali-linux-full*** metapackage installed. This package includes all of the tools you are familiar with in Kali.
Installation Size: 9.0 GB

kali-linux

The ***kali-linux*** metapackage is a completely bare-bones installation of Kali Linux and includes various network services such as Apache and SSH, the Kali kernel, and a number of version control applications like git, svn, etc. All of the other metapackages listed below also

contain ***kali-linux***.
Installation Size: 1.5 GB

kali-linux-all

In order to keep our ISO sizes reasonable, we are unable to include every single tool that we package for Kali and there are a number of tools that are not able to be used depending on hardware, such as various GPU tools. If you want to install every available Kali Linux package, you can install the ***kali-linux-all*** metapackage.
Installation Size: 15 GB

kali-linux-top10

In Kali Linux, we have a sub-menu called "Top 10 Security Tools". The ***kali-linux-top10*** metapackage will install all of these tools for you in one fell swoop.
Installation Size: 3.5 GB

kali-linux-forensic

If you are doing forensics work, you don't want your analysis system to contain a bunch of unnecessary tools. To the rescue comes the ***kali-linux-forensic*** metapackage, which only contains the forensics tools in Kali.
Installation Size: 3.1 GB

kali-linux-gpu

GPU utilities are very powerful but need special hardware in order to function correctly. For this reason, they are not included in the default Kali Linux installation but you can install them all at once with ***kali-linux-gpu*** and get cracking.
Installation Size: 4.8 GB

kali-linux-pwtools

The ***kali-linux-pwtools*** metapackage contains over 40 different password cracking utilities as well as the GPU tools contained in ***kali-linux-gpu***.
Installation Size: 6.0 GB

kali-linux-rfid

For our users who are doing RFID research and exploitation, we have the ***kali-linux-rfid*** metapackage containing all of the RFID tools available in Kali Linux.
Installation Size: 1.5 GB

kali-linux-sdr

The ***kali-linux-sdr*** metapackage contains a large selection of tools for your Software Defined Radio hacking needs.
Installation Size: 2.4 GB

kali-linux-voip

Many people have told us they use Kali Linux to conduct VoIP testing and research so they will be happy to know we now have a dedicated ***kali-linux-voip*** metapackage with 20+ tools.
Installation Size: 1.8 GB

kali-linux-web

Web application assessments are very common in the field of penetration testing and for this reason, Kali includes the ***kali-linux-web*** metapackage containing dozens of tools related to web application hacking.
Installation Size: 4.9 GB

kali-linux-wireless

Like web applications, many penetration testing assessments are targeted towards wireless networks. The ***kali-linux-wireless*** metapackage contains all the tools you'll need in one easy to install package.
Installation Size: 6.6 GB

Motorola LapDock

Default resolution for Motorola LapDock: 1366x768

Connect to the IP address with VNC Viewer. Username: pi Password: raspberry

Insert HDMI cable with lid open to power up Pi.

Fastest Cards

Samsung Evo+, SanDisk Extreme

Static IP

We now need to plug this information into the Pi's network configuration file using a text editor. I always use nano text editor. . .

```
sudo nano /etc/network/interfaces
```

Simply change the line that reads:

iface eth0 inet dhcp to **iface eth0 inet static**

Then directly below this line enter the following (Please Note. **You will need your own addresses we gathered in Part B, more details below**). . . .

```
address 192.168.9.30
netmask 255.255.255.0
network 192.168.9.0
broadcast 192.168.9.255
gateway 192.168.9.1
```

CTRL X to save and exit