1. 硬件准备
   1. 树莓派

树莓派是一个微型电脑，但没有硬盘，系统可通过SD卡加载，网上有教程。可以连显示器，鼠标、键盘、网线当普通电脑使用。开发过程中还是远程登陆比较方便。VNC View远程桌面配置教程参见

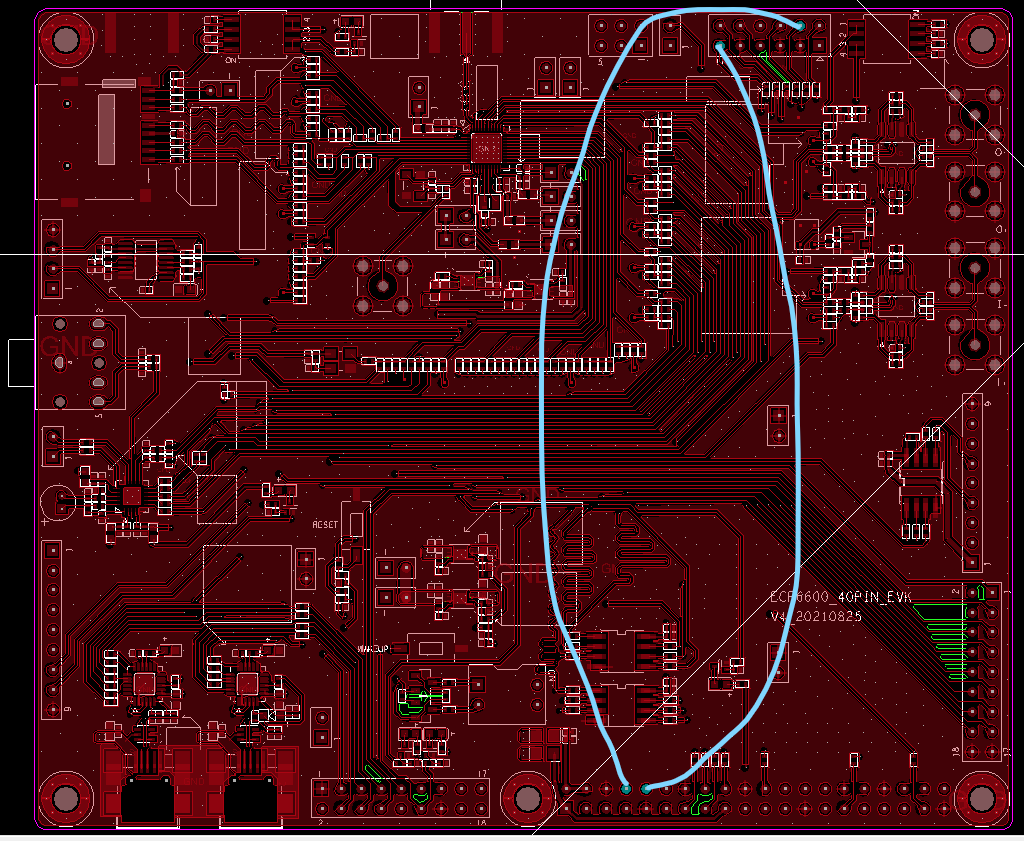
[树莓派 VNC Viewer 远程桌面配置教程 | 树莓派实验室 (nxez.com)](https://shumeipai.nxez.com/2018/08/31/raspberry-pi-vnc-viewer-configuration-tutorial.html)

* 1. 树莓派与ecr6600连接

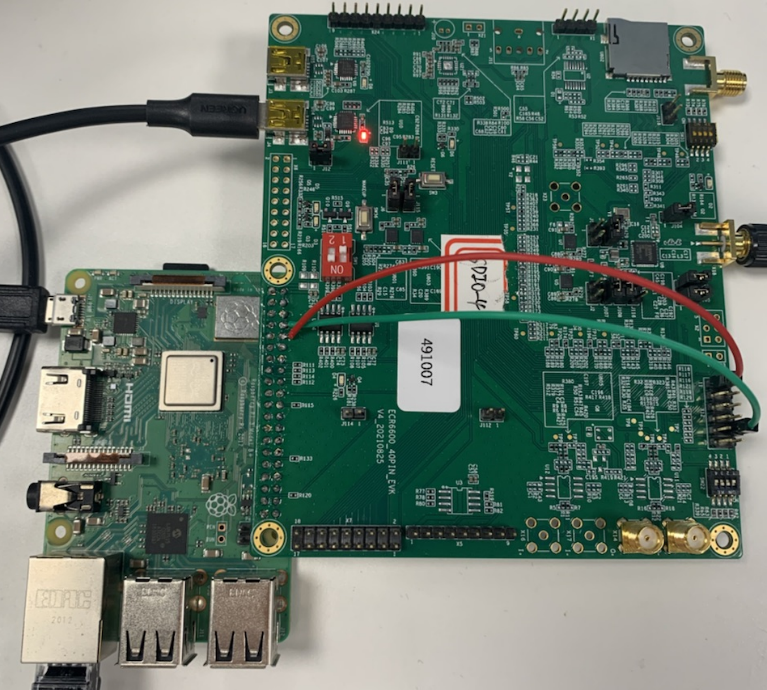
树莓派与ecr6600通过40pin引脚进行连接，ecr6600需要SDIO版本。（SDIO板）从测试同事那里拿到已改造好的SDIO板子，该板是用于wifi测试用的，还需要将树莓派的物理串口与ecr6600的uart1连接。

uart1跳线方式如下：

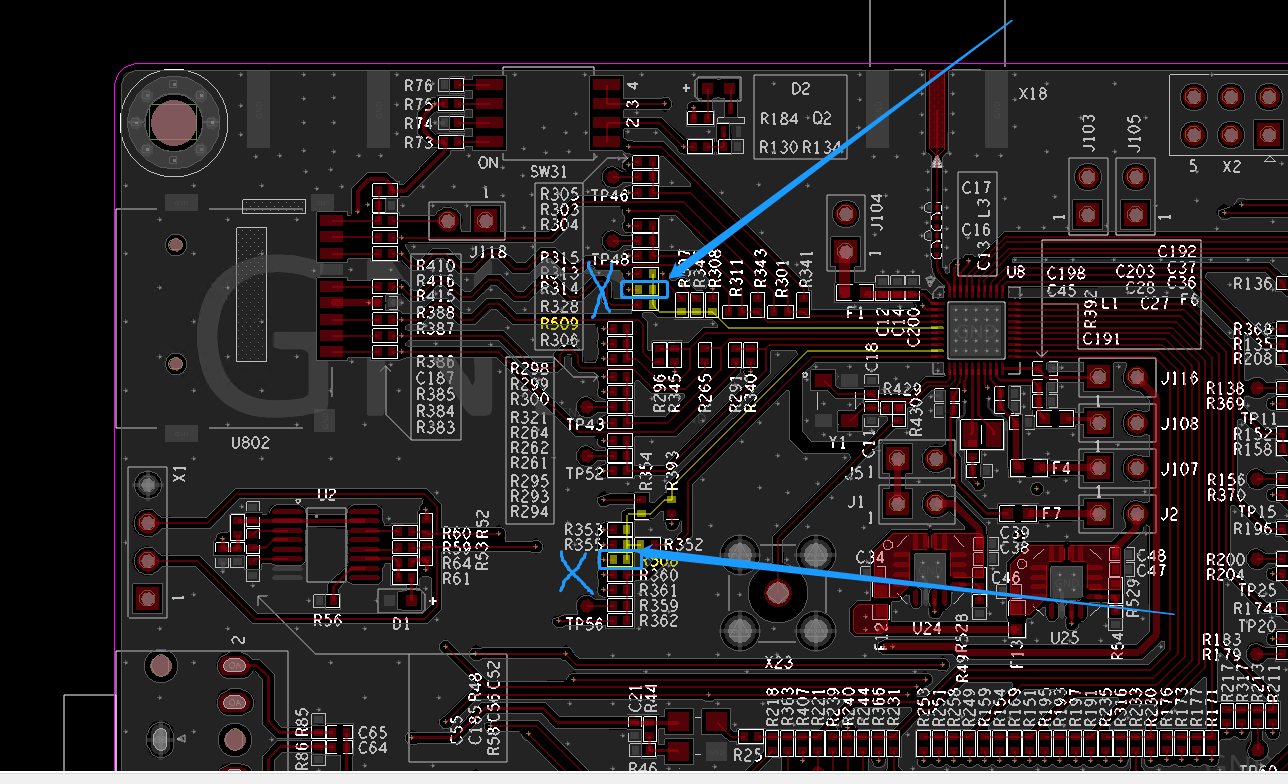
x12的pin4接x10的pin8，x12的pin11接x10的pin10



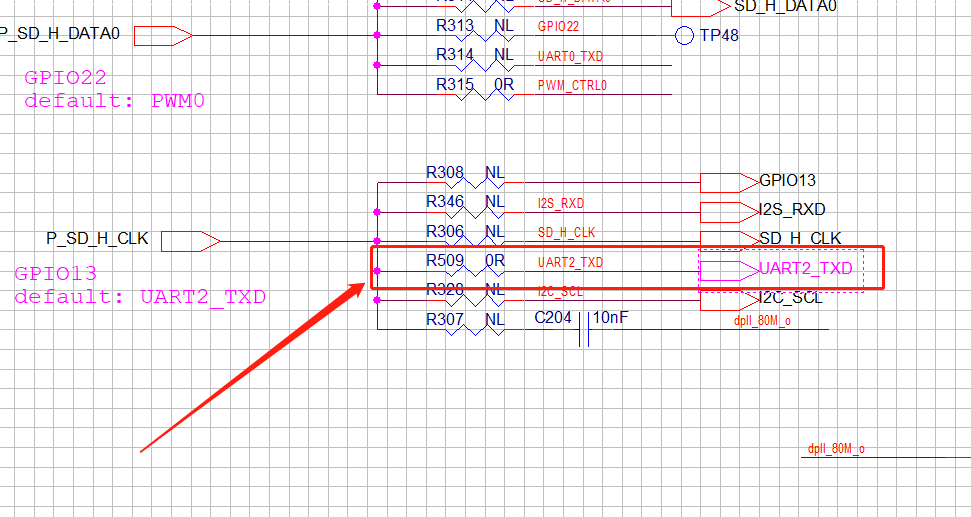
两块板子连接如下图

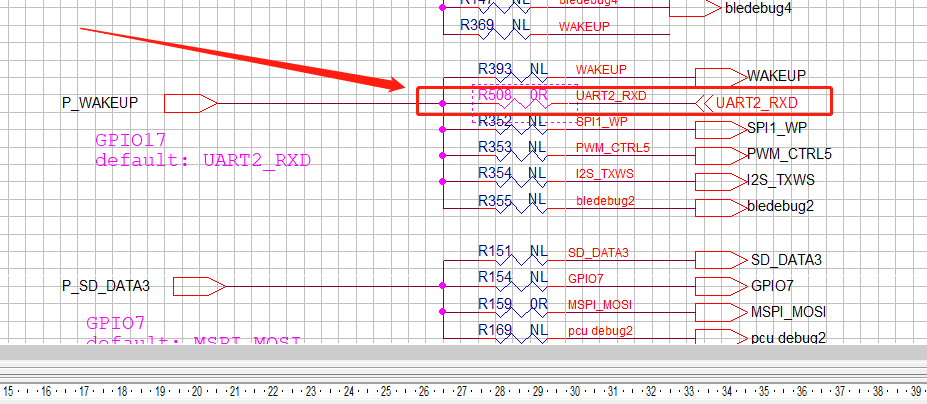


uart2跳线方式如下（使用uart2是因为uart1和jtag复用，为了保证jtag的正常使用，ble可以换用uart2通信）：



去掉R508/R509 蓝色箭头处焊接导线，R509是 6600 TX，R508是6600 RX





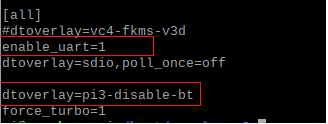
1. 软件配置

树莓派3B+外设中一共包含两个串口，一个称之为硬件串口（dev/ttyAMA0）,一个称之为mini串口（dev/ttyS0）。硬件串口由硬件实现，有单独的波特率时钟源，性能高、可靠；mini串口性能低，功能也简单，并且没有波特率专用的时钟源而是由CPU内核时钟提供，因此mini串口有个致命的弱点是：波特率受到内核时钟的影响。

在树莓派3代中，内置了蓝牙模块，硬件串口被默认分配给与蓝牙模块通信了，排线引出的GPIO Tx Rx是mini串口。

树莓派要使用ecr6600进行蓝牙透传，需要先将硬件串口映射到GPIO 14/15上，禁掉板载的蓝牙模块，再通过硬件串口连接ecr6600，加载hci设备。具体操作

1. 编辑/boot目录下的config.txt文件



2）禁用串口控制台功能

在树莓派命令窗口中分别通过如下两个命令停止和禁用串口的控制台功能：

sudo systemctl stop serial-getty@ttyAMA0.service

sudo systemctl disable serial-getty@ttyAMA0.service

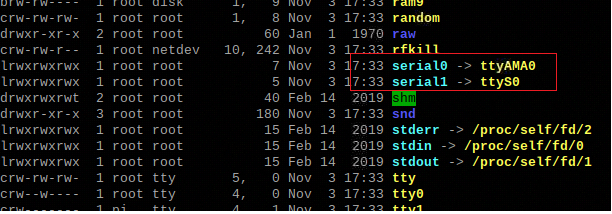
编辑/boot目录下的cmdline.txt,

将console=serial0,115200字样删掉，改后如下图

C:\Users\E0005411\AppData\Local\Temp\企业微信截图_16359895715006.png

保存文件重启树莓派

通过ls –l /dev查看修改后的映射关系：



参考

[树莓派串口通信设置 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/38853178)

[树莓派3串口(UART)使用问题的解决方法！！！！\_大西瓜Blog-CSDN博客](https://blog.csdn.net/qq562029186/article/details/75303832)

1. 版本下载

SDIO板子的版本需要编译transport版本，该版本打开CONFIG\_STANDALONE\_UART，版本下载无法通过download工具，需要通过SDIO口加载。方法参考SDIOeco4.txt（软件测试团队提供，测试WIFI使用）。

1. 下载sdio host driver，代码路径

<http://192.168.128.235/>ecr6600u/wifi\_host\_driver

1. 拷贝到树莓派中/home/samba/share/code/wifi\_host\_driver
2. sudo vi fullmac/Makefile 修改：q ?=n保存退出，./build\_wifi.sh编译，fullmac目录下生成wlan\_ecr6600.ko
3. cp transport\_transport.bin /lib/firmware
4. 复位6600,进入sdio boot mode
5. cd /lib/firmware,

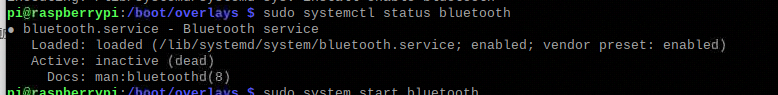
sudo insmod /home/samba/share/code/wifi\_host\_driver/fullmac/wlan\_ecr6600.ko dl\_fw=1 fw\_name=transport\_transport.bin

6600显示sdio\_init，表明加载正常。

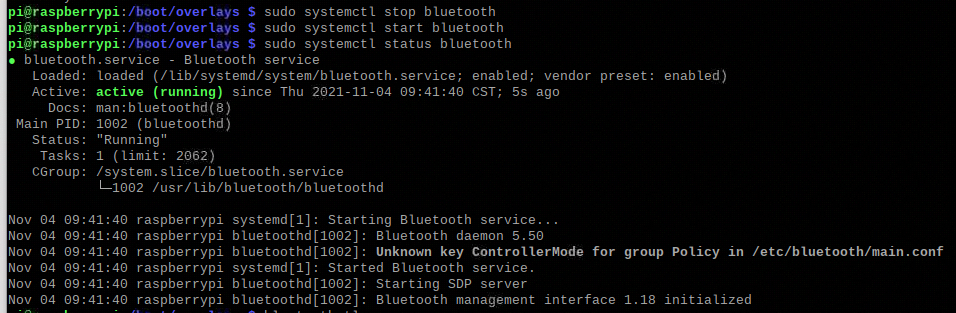
1. 启动蓝牙服务和蓝牙模块

树莓派自带蓝牙协议栈BlueZ, BlueZ中提供了工具bluetoothctl。

1. 输入sudo systemctl status bluetooth查看bluetooth.service状态

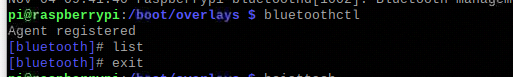


出现inactive，可以先停止服务再重新启动



1. 查看蓝牙设备

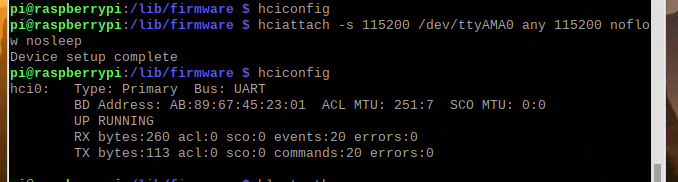
初始查看蓝牙设备是空的



通过hciattach配置通过串口连接蓝牙设备

hciattach -s 115200 /dev/ttyAMA0 any 115200 noflow nosleep

操作完后可以看到蓝牙设备了



此时可以通过bluetoothctl指令操作蓝牙设备。

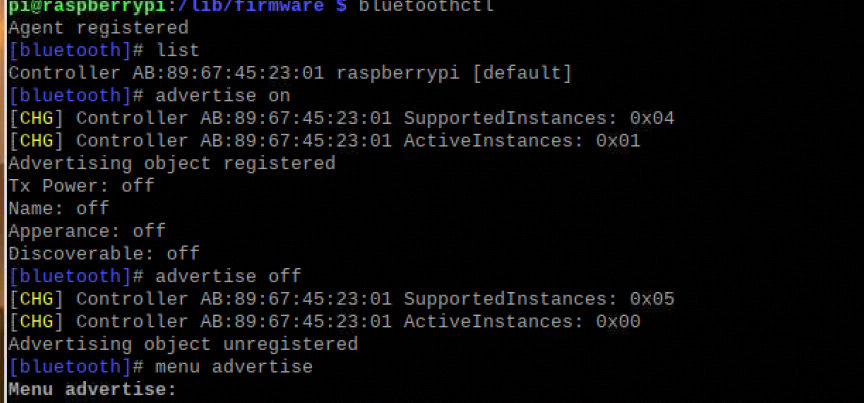
1. 利用bluetooth工具进行操作

Bluetooth进入后，可通过help查看支持的指令。

menu advertise 设置广播参数，back回到上级菜单

advertise on，开始广播

scan on 开始扫描



1. HCI log分析

bluez-hcidump Kali Linux提供一款分析工具，不仅可以从蓝牙接口实时读取数据，还可以读取蓝牙的抓包文件

从BlueZ官网[www.bluez.org/download](http://www.bluez.org/download)下载bluez-hcidump-2.5.tar.xz

tar –xvf bluez-hcidump-2.5.tar.xz

cd bluez-hcidump-2.5

执行 sudo ./configure --disable-system

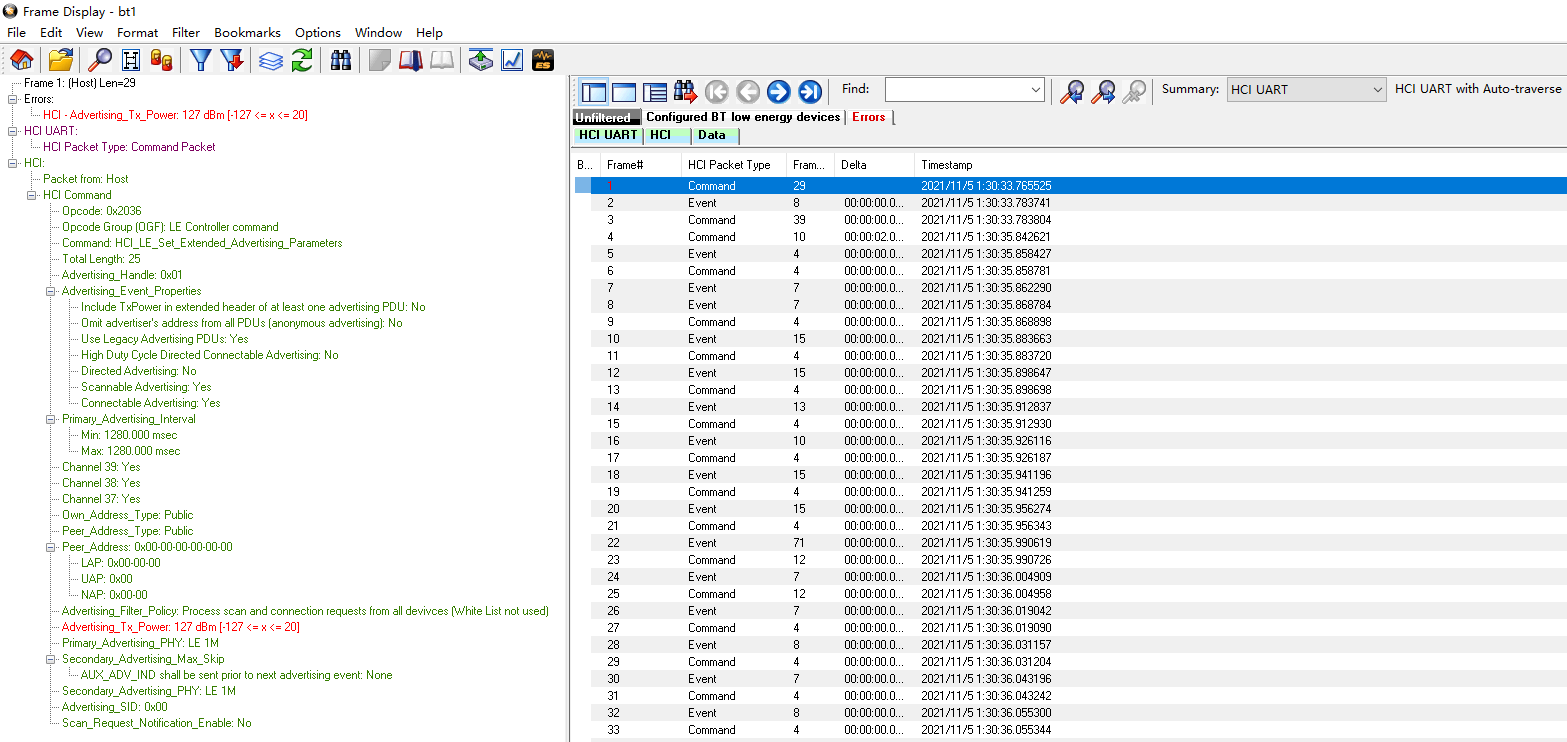
编译： sudo make

安装：sudo make install

hcidump –Xt 显示HCI EVENT

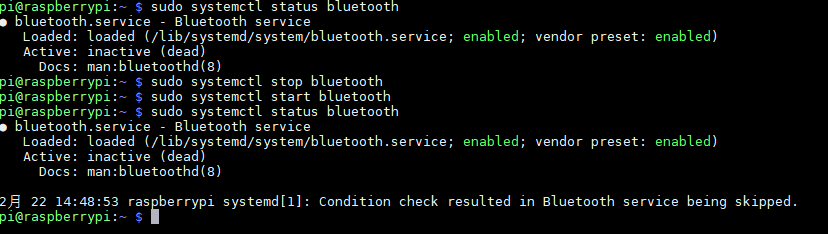
hcidump –Xw /home/samba/share/mylog/bt1.cfa log输出到文件

log文件可以通过ComProbe Protocol Analysis System工具进行查看



调试遇到问题：

1. bt怎么都是inactive



解决方法：

sudo modprobe btusb  
sudo systemctl start bluetooth.service  
sudo systemctl status bluetooth