
1.BC28 硬件板准备.....	2
2.基本介绍.....	3
3.电信定向 IP 发数据 UDP.....	7
4.电信转发 IP 发数据 UDP.....	10
5.TCP 发数据测试.....	11
6.常见问题.....	12

网络安全技术

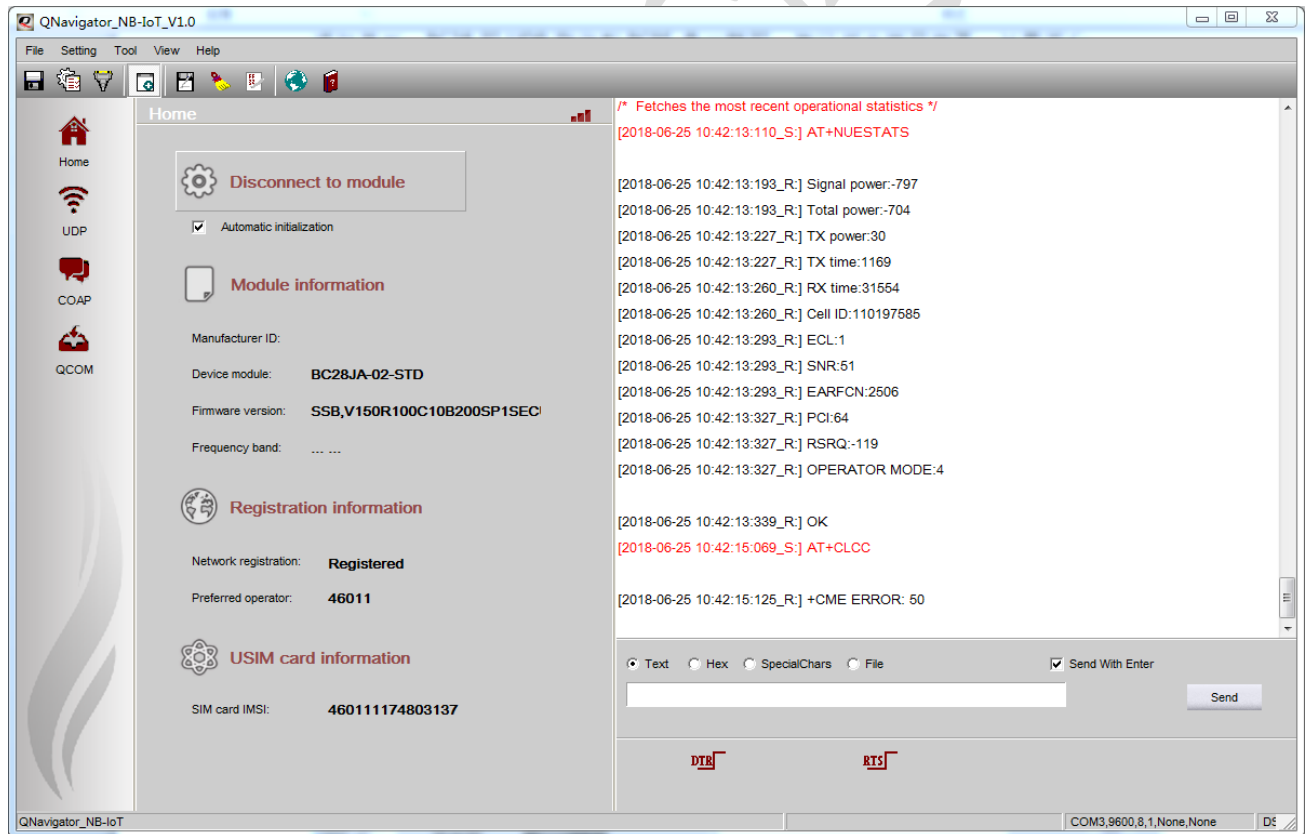
1.BC28 硬件板准备

1.拿到 BC28 开发板之后，开发板的默认单片机代码是下载成“单片机串口透传 USART1 控制_默认代码”，这个是为了方便单片机作为一个透传模块来将电脑端的数据接收并发给 BC28 模块。模块收到数据之后，执行指令响应之后返回给单片机，单片机将数据再给电脑进行显示。BC28 的 UDP 指令和 BC95 是一样的，所以对于用户而言，只要关心

2.准备一条 USB 转 RS232 的线接到板子上，注意要将板子上的 232_VCC 的跳线帽要跳接上。这样是为了让 RS232 能够正常工作。**注意一定要接，不然 RS232 是不工作的！**

3.NB-IOT 电信专用卡要插接到板子上，否则是没法进行测试的。NB 卡可以在电信运营商进行购买或者其他渠道获取。但是一定要注意所在地区是否已经有 NB 网络的覆盖。否则即便有卡，也没法进行实际调试使用。移动的 NB 用普通的手机卡物联网都是可以的。电信的必须是专用的。

4.打开提供的工具软件 QNavigator_NB-IoT_V1.0 来进行测试。下图就是我们已经插入 SIM 卡并且能够正常工作的。目前我们提供的模块版本是最新的，板子也预留了升级接口，方便用户做模块升级。一开始调试的时候可以先用串口调试助手把模块先熟悉起来。



5.需要测试 UDP 传输，我们需要准备一个公网 IP，**这点注意花生壳是不支持 UDP 传输的。所以我们是推荐用户去申请一个远程服务器比如是阿里云或者是华为云。**我们这里测试是申请了华为云服务器来做 UDP 数据传输的。所以大家如果有条件的话可以申请一个云服务器来实现 UDP 数据传输。对于 TCP 而言，花生壳是支持的。


2.基本介绍

这里推荐大家使用移远官方的这个调试工具，直观方便使用。因为他是自动发送 AT 指令去获取模块的相关信息，并将相关的信息打印到界面上，可以直观的进行查看。

那么我们将对相关的信息进行对应的介绍。



重点就是这些。我们对每个图标说明下。

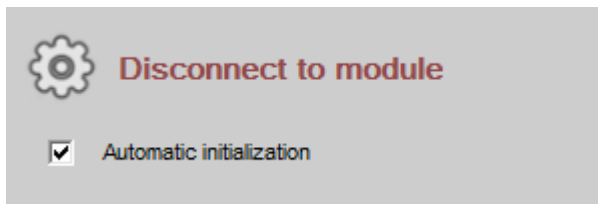
 这个应该大家都认识，他就是信号强度的意思。类似手机信号强度的标识符是一样。从三个图标来看，说明模块已经加入到网络了。当然我们此时可以通过指令来查询下模块当前的信号强度值。从而更直观的进行学习认识。

```
[2017-09-15 12:04:45:187_S:] AT+CSQ
```

```
[2017-09-15 12:04:45:399_R:] +CSQ:20,99
```

```
[2017-09-15 12:04:45:399_R:] OK
```

通过发送 AT+CSQ 可以获取到信号强度值当前是 20，说明此时模块注册上了网络。如果网络很差的时候，或者基站根本没有覆盖，一般信号强度值是 99。说明此时是没有注册上网络。需要查找相关的原因。



这个按钮就是连接模块的意思。下面

有一个自动初始化选择框，如果我们选中了。一定要点击，有的客户不点击就问怎么没数据，不点击链接，怎么与板子通讯呢！软件会自动发送相关的指令给到模块。从而让模块返回对应的信息给到界面来。



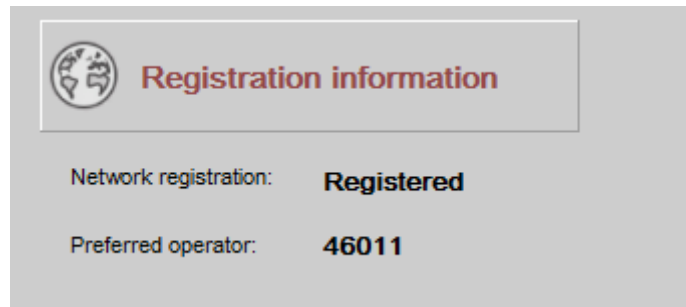
这个就是模块的相关信息了。可以看到当前模块的版本号，版本号目前查看不了，因为是全网通，支持所有的版本系列。当然此时如果出现这样的界面，那么恭喜你。你当前的模块是正常工作了。硬件和软件已经打通了基础第一步。

```
/* Query module support Bands */
```

```
[2018-06-25 10:42:08:698_S:] AT+NBAND?
```

```
[2018-06-25 10:42:08:779_R:] +NBAND:5,8,3,28,20,1
```

```
[2018-06-25 10:42:08:779_R:] OK
```



这个地方获取的是网络注册信息，注意这里主要是由 SIM 卡来决定的。如果说当前卡正常连接到电信基站之后，模块会返回对应的注册信息给回来。这个的注册 **Registered** 就类似我们做 MC20 做 CGREG 是一个意思。所以我们此时可以在输入栏输入查询信息来看下当前模块的注册信息。

```
[2017-09-15 12:12:29:S:] AT+CEREG?
```

```
[2017-09-15 12:12:29:542_R:] +CEREG:1,1
```

```
[2017-09-15 12:12:29:542_R:] OK
```

A screenshot of a web interface for sending AT commands. It has radio buttons for "Text", "Hex", "SpecialChars", and "File", and a checked checkbox for "Send With Enter". The input field contains the text "AT+CEREG?".

通过 AT+CEREG? 来查询当前的网络信息。如果返回 1 表明此时注册是正常的。同样也可以用 AT+CGATT?来查询，如果返回 1 表明网络注册成功。

下面有一个 46011 这个可以说明一下，这个就是卡的段号，换句话说卡不但有自己的手机卡号，也有他的是联通，电信，移动的区分号码。通过 AT+CIMI 来查询。

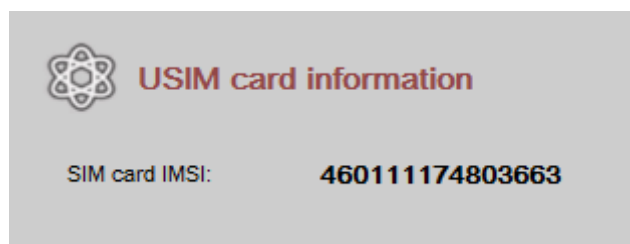
```
[2017-09-15 12:18:50:394_S:] AT+CIMI
```

```
[2017-09-15 12:18:50:612_R:] 460111174803663
```

```
[2017-09-15 12:18:50:612_R:] OK
```

A screenshot of a web interface for sending AT commands. It has radio buttons for "Text", "Hex", "SpecialChars", and "File", and a checked checkbox for "Send With Enter". The input field contains the text "AT+CIMI".

可以查询当前返回的是 46011，联通移动的返回的是不一样的。当然这个查询也适用 2G 的 GSM 模块。大家如果有我们的 2G 的板子的话也可以进行查询。



这个就是这 SIM 卡卡的唯一 ID。通过这个 ID 来区分每张卡。就是我们上面通过指令获取到的。

以上的界面大家在调试的时候，一定要全部都有，如果说有一个没有那么当前一定是有问题的。所以推荐大家可以去处理一下。按照我说的这个方式来操作。

网络安全技术

3.电信定向 IP 发数据 UDP

The screenshot shows a 'UDP' configuration window. It contains several input fields and buttons. Five red boxes with numbers 1 through 5 are overlaid on the interface to highlight specific areas:

- Box 1:** Encloses the 'Access Point Name' field (containing 'HUAWEI.COM') and the 'PDP Type' dropdown menu (set to 'IP').
- Box 2:** Encloses the 'P address' field and the 'DEACT' button.
- Box 3:** Encloses the 'Server IP' field (containing '185 . 4 . 11 . 122'), the 'Server port' field (containing '10005'), the 'Local port' field (containing '3005'), and the 'Connect' button.
- Box 4:** Encloses the 'Data to be sent to remote' section, which includes radio buttons for 'Text', 'Hex', and 'AutoQuery' (selected), a large text input area, and 'Send' and 'Clear all' buttons.
- Box 5:** Encloses the 'Data received from remote' section, which includes a large text input area and a 'Clear all' button.

At the bottom of the window, there is a 'Message statistics' section with a 'Statistics' button.

对于定向发 IP，就是用户可以任意发数据到公网服务器端，目前电信对于 IP 还是存在一定的限制。所以这里的定向 IP 如果用户有自己的卡并绑定了对应的公网服务器即可使用。对于移动联通目前并没有相关的限制，可以任意发到公网 IP。电信对 IP 的限制不光是 UDP 也会对 TCP 端发送进行限制。

这个地方就是我们发 UDP 数据的地方，需要掌握并且了解这 5 个框图分别的含义。1 就是 PDP 激活，就是我们要连接服务器，需要首先设置 APN。那么这里的 APN 就是需要连接到华为的地址上来。所以首先第一步先去激活 PDP，让模块具备发数据的基础。

```
/* Use AT+CGDCONT=1,"IP","HUAWEI.COM", to configuration PDP */
```

```
[2017-09-15 14:05:52:264_S:] AT+CGDCONT=1,"IP","HUAWEI.COM"
```

```
[2017-09-15 14:05:52:489_R:] OK
```

```
/* User "AT+CGATT=1"to activate context profile */
```

```
[2017-09-15 14:05:52:997_S:] AT+CGATT=1
```

```
[2017-09-15 14:05:53:198_R:] OK
```

```
/* Query the status of the context profile,You may have to wait for several seconds */
```

```
[2017-09-15 14:05:53:206_S:] AT+CGATT?
```

```
[2017-09-15 14:05:53:418_R:] +CGATT:1
```

这个就是 PDP 激活的具体操作指令，通过调节成功之后呢，图片上的 2 号位置会出现模块注册到服务器所分配的 IP 地址，这个就是和调试 2G 模块是一个道理。所以熟悉 2G 模块，再来调试 NB LOT 其实并没那么复杂。



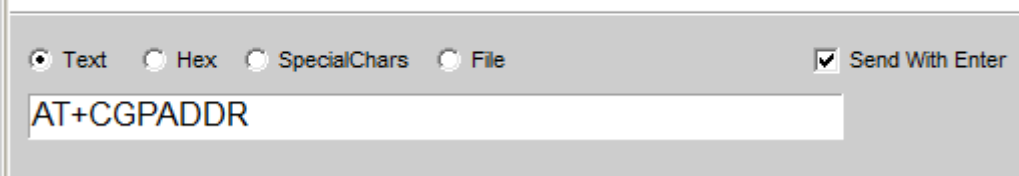
此时我们就获取到了模块的 IP 地址了。有了 IP 地址之后，那么下面的发数据就水到渠成了。

```
[2017-09-15 14:10:47:536_S:] AT+CGPADDR
```

```
[2017-09-15 14:10:47:764_R:] +CGPADDR:0,10.34.164.35
```

```
[2017-09-15 14:10:47:764_R:] +CGPADDR:1
```

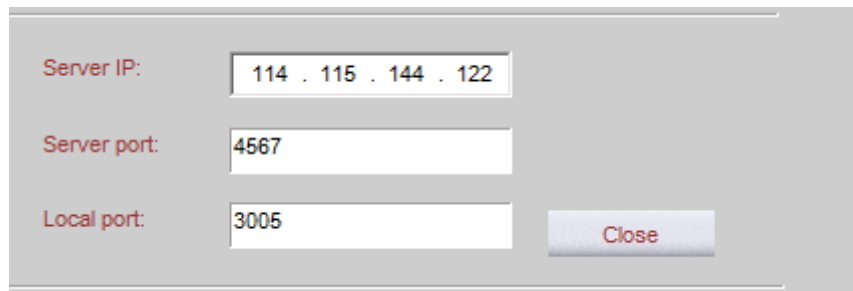
```
[2017-09-15 14:10:47:780_R:] OK
```



通过发送获取 IP 地址的指令，可以看到获取到 IP 地址是与图片上的是一致的。同样 IP 地址也是测试的一个很重要的参考条件。如果说有了 IP 地址，那么数据发送那应该就会必然成功。

图片位置的 3 号就是我们z需要登录的服务器 IP 和端口号了。因为电信目前都是定向 IP。

所以这里的 IP 地址根据你现在拿到的卡所指定的 IP 地址来实现对应的登录。



图中就是服务器的 IP 和端口号了。这个 IP 号一定要是公网，如果想用花生壳，处在电信网络情况下 UDP 才可以正常使用。移动和联通宽带是没法测试 UDP 的。由于 BC28 支持 TCP,所以 TCP 情况下用户可以选择用花生壳。我们这里测试的是申请的华为云服务器进行测试的。所以输入 IP 和端口之后就显示连接成功了。当然 UDP 是无连接模式。如果你服务器不存在或者有问题，他也会显示连接 OK 的。

```
/* Use AT+NSOCR to create a socket on the UE and associates with specified protocol */
[2017-09-15 16:41:51:987_S:] AT+NSOCR=DGRAM,17,3005,1

[2017-09-15 16:41:52:209_R:] 0

[2017-09-15 16:41:52:209_R:] OK
[2017-09-15 16:41:53:316_S:] AT+NSOST=0,114.115.144.122,4567,4,31323334

[2017-09-15 16:41:53:561_R:] 0,4

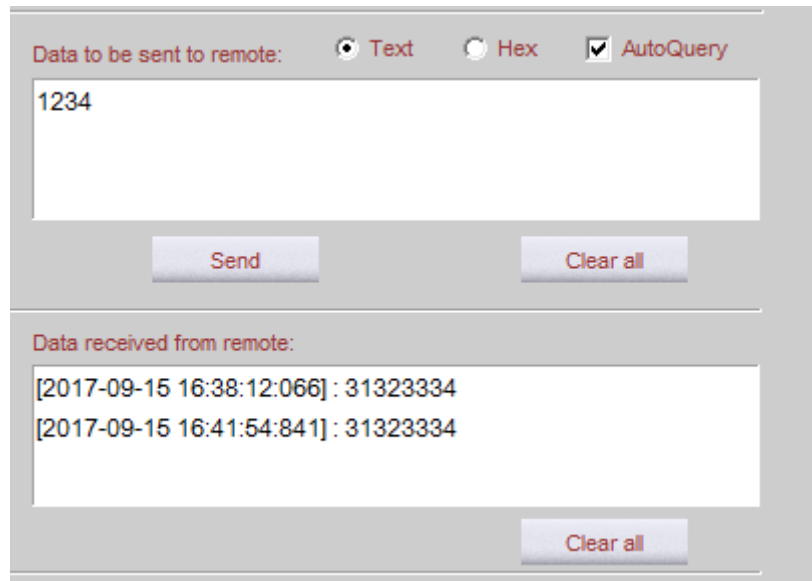
[2017-09-15 16:41:53:561_R:] OK
```

建立一个 UDP 连接，先在 DGRAM 里面创建 UDP 协议，并写入本地端口号。首先是先创建一个 Socket，然后通过 AT+NSOST 指令输入对应的 Socket 号码以及服务器的 IP 地址和端口号码。后面跟的数据都是十六进制的。

AT+NSOST=0,//0 是 socket 号码。因为目前只创建了一个 Socket，所以此处填写 0。

114.115.144.122,4567 就是服务器的 IP 和端口号。

4,31323334,对应就是 4 个数据长度，31 对应就是字符 1.所以此处跟的数据都是十六进制的。与之前调 2G 的时候还有些区别。

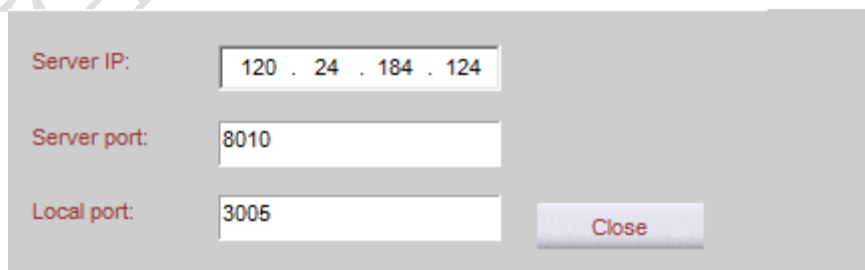


这里就是输入的数据，以及接收到的数据，因为服务器做了发什么数据回什么数据的工作。那么到此处基本的 NB LOT 就基本上调试成功了。

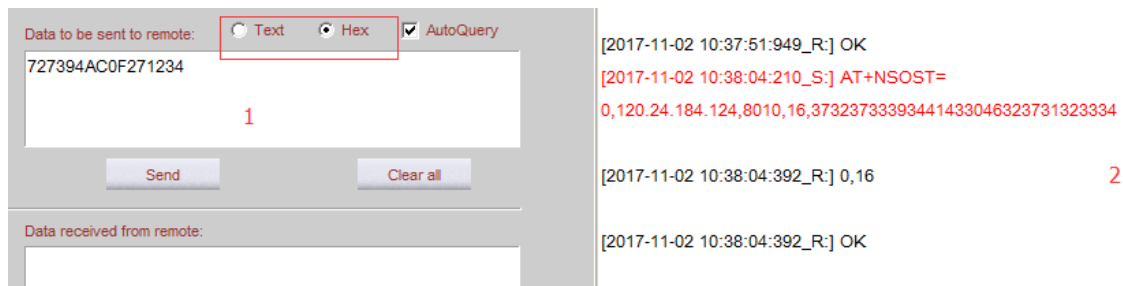
极力推荐大家使用官方这个调试软件。因为目前 BC95 是指令不带回显的。通过此软件比串口助手会显示的更直观更好调试。这样大家理解好这个地方，去调试单片机代码也就非常方便了。

4. 电信转发 IP 发数据 UDP

转发 IP 的意思就是现在手中的卡所绑定的地址并不是任意的指定 IP。而是将卡的地址被绑定在固定的 IP 上，像我们提供的卡就是绑定在固定的 IP 上，而我们的卡绑定的 IP 地址是阿里云服务器。此阿里云服务器支持对数据的转发。这样就可以实现将数据转发到任意的公网 IP 上进程显示了。具体可以参考《UDP 转发网关数据格式》这个资料来看具体的数据转发的方式。主要注意端口大小端的问题，就是先把十进制数据转成十六进制。比如 9999 转成 270F，在输入框输入数据的时候要写出 0F27。而有时候大家直接分拆成 2 个 99，那是大错特错了。一定要注意这个问题。



注意看这个图，这个图当中的 IP 地址和服务器端口都必须要是这样。因为这个就是我们提供的非定向 IP 卡所默认绑定的 IP 地址。注意其实非定向 IP 卡就是固定的 IP 地址卡，只是我们的服务器具备数据转发功能，可以将数据任意转发到指定的 IP 地址去而已。



注意在数据输入框当中需要使用 HEX 方式去发数据,注意由于软件存在 bug, 在后面的发送命令框中 2 显示的是字符型的数据,他被软件解析成了字符型,所以显示发送出去 16 个字节数据,实际我们应该是 8 个字节。这个解决方法就是先选择 Text 然后再选择 Hex 发送即可解决。



看左边和右边发送的数据保持一致了。并且最后的数据长度就是 8, 这样就是发送的 8 个字节属于正常了。如果发送正确,服务器会自动下发相同的数据给到模块来。然后在下面的解析框就可以看到对应的解析数据了。



可以看到模块接收到数据了,并通过指令对数据进行了对应的读取,并显示在左边的接收框。如果出现这样的情况,表明 NB IOT 整个思路就打通了。模块就没问题了。

5.TCP 发数据测试

电信目前我们所提供的转发卡在做 TCP 测试的时候也会受到一定的限制。所以用到电信卡需要确认卡是否也会对 IP 进行对应的限制。但是对于移动卡而言发 TCP 数据就不会存在限制,这样就方便用户做 TCP 测试了。

对于 TCP 测试,需要自己主动手敲指令的方式进行测试。QN 软件目前提供的版本只是支持 UDP 与 COAP 方面的测试。不支持 TCP 自动设置。

```
[2018-06-25 12:06:11:910_S:] AT+NSOCR=STREAM,6,56000,1

[2018-06-25 12:06:11:954_R:] 1

[2018-06-25 12:06:11:954_R:] OK
[2018-06-25 12:06:18:414_S:] AT+NSOCO=1,114.115.148.172,8888

[2018-06-25 12:06:18:459_R:] OK
[2018-06-25 12:06:23:846_S:] AT+NSOSD=1,4,01020304

[2018-06-25 12:06:23:890_R:] 1,4

[2018-06-25 12:06:23:890_R:] OK

[2018-06-25 12:06:24:689_R:] +NSONMI:1,4
[2018-06-25 12:06:24:692_S:] AT+NSORF=0,4

[2018-06-25 12:06:24:721_R:] ERROR
[2018-06-25 12:06:30:998_S:] AT+NSORF=1,4

[2018-06-25 12:06:31:049_R:] 1,114.115.148.172,8888,4,01020304,0

[2018-06-25 12:06:31:063_R:] OK
```



TCP 测试的基本流程,首先是建立 socket 链接,建立成功之后,会返回 socket num 号码。下面的 TCP 连接与收发数据都需要使用此号码。所以非常重要。

这个 TCP 发送与 UDP 基本上是一样的。并且移远官方也给出了 TCP 发送的例程说明。对于电信而言会出现 TCP 限制问题。跟 UDP 一样。如果要用 TCP 尽量选择移动卡。

我们的转发卡也支持 UDP 转发, TCP 转发同样会限制。这里就不存在转发问题。可以直接发到目的地 IP。

我们这里给出的测试 IP 与端口是 114.115.148.172:8888, 发什么回什么。注意读取的 Socket num 号码。软件默认是 0, 读取的会报错, 根据实际是多少进行设定。

6. 常见问题

其实 NB IOT 网络并不复杂,主要复杂在于目前 NB 商用时间较短。所以对于卡方面的使用存在一些注册的问题。经常会出现 CSQ 信号没有以及没法收发数据等问题。下面主要将几个重要的问题给梳理一下。

1. CSQ 值一直是 99。

- (1) 此问题首先要看当地电信网络是否开通, 以及你目前拿到的电信 NB 卡是否已经商用并注册了。这个可以跟当地的电信运营商进行沟通。

- (2) 模块天线是否被正常插着了。默认我们出货是不插 SMA 天线的。需要用户自己手动接好天线。**切记天线一定要插!**同样也要检查 SIM 卡是否被插好。卡的方向是芯片朝下缺口朝外。

2. 服务器问题

- (1) 操作 BC28 的时候, 支持 UDP 协议, TCP 协议。对于用户而言, 使用云服务器, 一定要配置安全组, 比如配置一个端口 8888, 那么你需要让你的安全组让这个端口的 UDP 输入输出都支持, 否则即便你代码正确, 也是无法将数据发到云服务器的。这一点很重要, 一定要注意。并需要将防火墙关闭使用。
- (2) 推荐大家可以购买云服务器或者是使用电信网络或者是公网电信的网络。

3. 定向 IP 和转发 IP (针对电信 UDP)

因为电信公司目前商用卡的严格研制, 导致大家在测试的时候, 显得有点不方便。我们现在提供出售的卡都是非定向的 IP 地址, 就是说没有办法让模块直接把数据发到指定的 IP 地址当中来。所以需要通过服务器进行转发。这样就可以发到任意一个 IP 地址去, 不用非常麻烦的去办理 SIM 卡。这样对于开发而言, 相对会迅速很多。

注意: 转发 IP 对于发送数据而言, 不受影响, 对数据下发的时候, 用户也要严格按照转发的方式来进行数据的下发。

目前电信已经不再支持用户申请定向 IP 卡, 必须所有的卡都通过电信 IOT 平台进行数据的收发管理。那只能走 COAP 协议。这里我们也是推荐大家按照电信的要求走平台。不过移动目前是放开 IP 限制, 任意发地址都是支持的。所以说如果想要简单的方式做移动还是比较好的选择, 不过移动有的地方网络覆盖不佳, 这一点需要注意。

The image shows a software interface for configuring network settings. It has three input fields for 'Server IP:', 'Server port:', and 'Local port:'. The 'Server IP' field contains '120 . 24 . 184 . 124', 'Server port' contains '8010', and 'Local port' contains '3005'. There is a 'Close' button to the right of the 'Local port' field. Below these fields, there is a section for 'Data to be sent to remote:' with three radio buttons: 'Text', 'Hex', and 'AutoQuery'. The 'AutoQuery' radio button is selected. Below the radio buttons is a text input field containing the hexadecimal string '727394ACB8221234'. At the bottom of the interface, there are two buttons: 'Send' and 'Clear all'.

Server IP:	120 . 24 . 184 . 124
Server port:	8010
Local port:	3005

Close

Data to be sent to remote: ☐ Text ☒ Hex ☒ AutoQuery

727394ACB8221234

Send Clear all



图 4-3 转发 IP 接收数据示意图

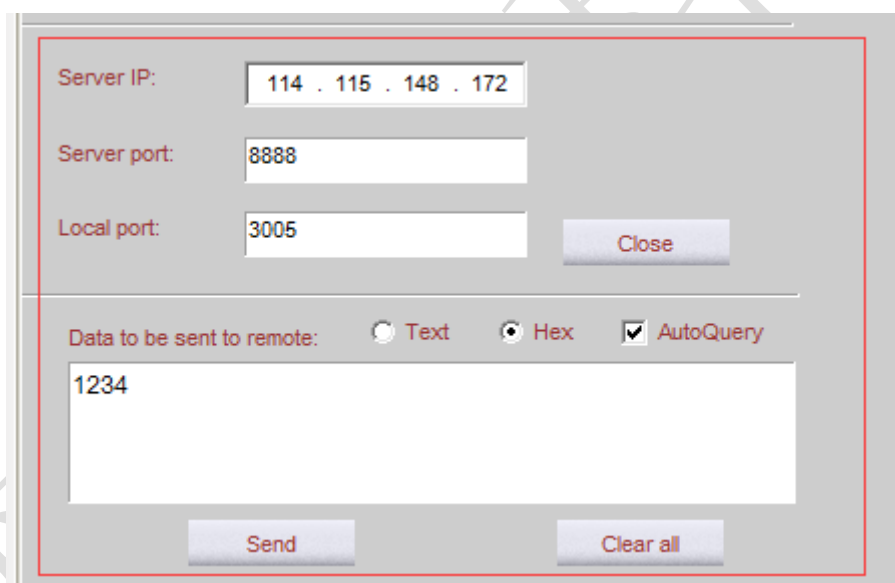




图 4-4 定向 IP 接收数据示意图

从上面两张图可以很好的区分出定向和非定向之间的差异。非定向发数据的时候，发的服务器 IP 和端口不是客户指定的 IP 地址和端口，而是转发服务器的 IP 和端口。这一点一定要注意。后面跟的数据里面就是要包含实际要发到的 IP 地址和端口号。主要要采用十六进制方式发送。然后服务器端接收到的数据里面就包含了转发的地址和端口号。这里默认是占用 6 个字节。后面跟进的才是数据。所以非定向设计程序的时候一定要注意。**而且数据只能支持十六进制的方式发送。不能采用字符型!!!**

定向发服务器端数据就相对简单了，只要填入需要发送的服务器端口和 IP 之后就可以发送数据了。数据填入区只要填写数据内容即可。支持字符和十六进制。服务器收到的数据将与发送的数据内容保持一致。并重要的一点是支持服务器下发数据。这一点对有需求做数据下发的客户是极为重要的。