NB-IOT CAT-M1 modem(SIM7000C) TCP連接應用

參考:

<https://frankchang.me/2018/12/18/sim7000c/>

...................................开机检测..................................

AT //波特率同步

OK

AT+CPIN? //检查卡

+CPIN: READY

OK

AT+CSQ //查询信号强度

AT+CSQ: 20,0

OK

AT+CGATT? //查询业务是否附着，确保卡不欠费

AT+CGATT: 1

OK

...................................设置NB模..................................

AT+CNMP=<mode> //工作模式选择命令

13：GSM only

38：LTE only（使用NB-IOT网络时CNMP需要设置38）

AT+CMNB=<mode> //CAT-M 与 NB-IOT 选择命令

1: CAT-M

2: NB-IOT

AT+NBSC=<mode> //扰码设置（需与基站的扰码设置一致、大部分基站打开的）

0: 关闭

1: 打开

...................................设置APN..................................

AT+CGNAPN //查询模块和网络协商注册时获取的APN信息

+CGNAPN: 1,"internet.iot"

OK

AT+CSTT=" internet.iot " //设置对应的 APN "internet.iot”

OK

...................................开始连接流程..................................

AT+CIICR //激活移动场景

OK

AT+CIFSR //获取本地 IP 地址

10.173.180.170

AT+CIPSTART="TCP","xx.xx.xx.xx",xx //连接TCP服务器

OK

CONNECT OK //收到CONNECT表示已经连接成功

AT+CIPSEND=12 //发送数据(12 代表只发送 12 字节数据)

> 1234567890ABCDEFGHIJ //输入对应的数据(12 字节后的数据被丢弃)

SEND OK

1234567890AB //服务器返回数据

AT+CIPCLOSE=1 //关闭TCP连接CLOSE

OK

AT+CIPSHUT //关闭移动场景

SHUT OK

注：在激活移动场景后再次激活就会返回error，需要确保已经关闭移动场景，连接TCP时候需要适当延迟，返回CONNECT OK才算连接成功

測試結果: 取得本地IP地址後也可以ping cht

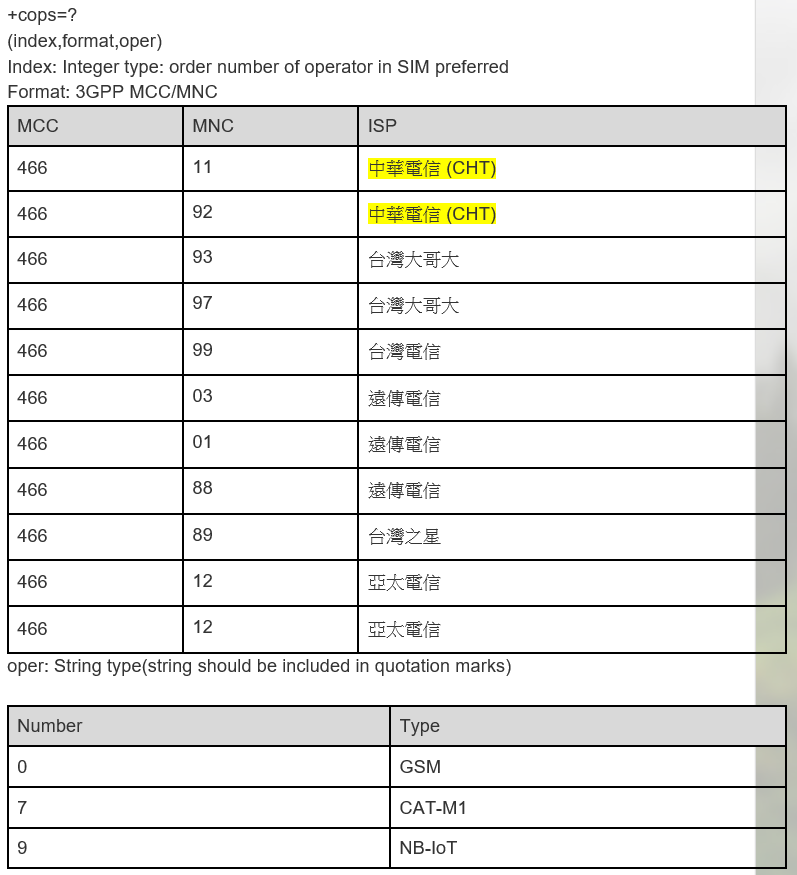
AT+CIPPING="168.95.1.1"

or

AT+CIPPING="iot.cht.com.tw"

AT+CPSI?

+CPSI: LTE CAT-M1,Online,466-9,0x2CEC,28608801,434,EUTRAN-BAND3,1750,5,5,-6,-81,-58,14



**9.1.1 普通 TCP/TP 发送步骤**

AT+CGDCONT=1,"IP","CMNET" //设置 APN

OK

AT+CSQ //查询信号

+CSQ: 31,99

OK

AT+CREG? //查注册网络状态

+CREG: 0,1

OK

AT+CPSI? //注册信息

+CPSI: LTE,Online,460-01,0x5303,52467969,125,EUTRAN-BAND3,1650,5,5,-84,-693,-386,24

OK

AT+CGREG?

+CGREG: 0,1

OK

AT+CIPMODE=1 //设置 TCP/IP 模式

OK

AT+CSOCKSETPN=1

OK

AT+CIPMODE=0

OK

AT+NETOPEN

OK

+NETOPEN: 0

AT+CIPOPEN=0,"TCP","211.149.158.237",8011 设置 TCP 、IP 和端口号

OK

+CIPOPEN: 0,0

AT+CIPSEND=0,5 //发数据数据 5 是数据格式 发送 HELLO

>HELLO

OK

+CIPSEND: 0,5,5

RECV FROM:211.149.158.237:8011

+ IPD19

HOE-7600CE-TCP-TEST //服务器发回的数据

AT+CIPCLOSE=0//结束 TCP 连接

OK

CLOSED

+ CIPCLOSE: 0,0

AT+NETCLOSE// Close socket

OK

+NETCLOSE: 0

**9.1.2 TCP/IP 透传模式发送数据**

AT+CGDCONT=1,"IP","CMNET"

OK

AT+CIPMODE=1

OK

AT+NETOPEN

OK

+NETOPEN: 0

AT+CIPOPEN=0,"TCP","211.149.158.237",8011

CONNECT 115200

进入串口透传模式，此时串发过来的任何数据均直接发到服务器上（除+++外）

服务器发过来的数据：

服务器返回数据 HOE-7600CE-TCP-TEST

+++ 退出透传指令不带回车，发过去串口返回 OK 表示退出透传

OK

ATO// 重新进入透传

CONNECT 115200

又可以发数据了 如果透传 TCPIP 连接 先发送+++返回 OK 后发送如下指令

AT+CIPCLOSE=0//结束 TCP 连接

OK

CLOSED

+CIPCLOSE: 0,0

AT+NETCLOSE// Close socket

OK +NETCLOSE: 0

**//ensure GPRS network is available before**

AT+CSQ

+CSQ: 23,0

OK

AT+CREG?

+CREG: 0,1

OK

AT+CPSI?

+CPSI: GSM,Online,460-00 0x1816,63905,81 EGSM 900,-68,0,31-31

OK

AT+CGREG?

+CGREG: 0,1

OK

//PDP Context Enable/Disable

APN setting：

AT+CGSOCKCONT=1,"IP","CMNET"

OK

AT+CSOCKSETPN=1

OK

Note, usually CSOCKAUTH and CSOCKSETPN parameter are kept default if not care about.

Enable PDP context:

AT+CIPMODE=0 // command mode, if not configured, it is 0 by default. If customers want

data mode, please configure before Net open.

OK

AT+NETOPEN

OK

+NETOPEN: 0

AT+IPADDR

+IPADDR: 10.113.43.157

OK

Disable PDP context:

AT+NETCLOSE

OK

+NETCLOSE: 0

//Command Mode

2.3.1 TCP Client

AT+CIPOPEN=0,"TCP","116.236.221.75",8011//only IP address is supported

OK

+CIPOPEN: 0,0

AT+CIPSEND=0,5

>HELLO

OK

+CIPSEND: 0,5,5

AT+CIPSEND=0, //the second parameter is empty which means using <Ctrl+Z> to check the

end

>HELLO<Ctrl+Z>

OK

+CIPSEND: 0,5,5

AT+CIPCLOSE=0 // close by local

OK

+CIPCLOSE: 0,0

Note:

if connection closed by remote server, following URC will return:

+IPCLOSE: 0, 1

Here, the meaning of second parameter in this URC is as following,

0 - closed by local, active

1 - closed by remote, passive

3 – Reset

**2.3.3 Extended Information**

Command AT+CIPHEAD is used to show IP head (data length) information, and command

AT+CIPSRIP is used to show remote IP address and port once data are received.

AT+CIPHEAD=1

AT+CIPSRIP=0

AT+CIPOPEN=0,"TCP","116.236.221.75",8011

OK

+CIPOPEN: 0,0

AT+CIPSEND=0,5

>11111

OK

+CIPSEND: 0,5,5

// here, remote data is coming

+IPD13

hello from pc

AT+CIPSRIP=1

OK

// here, remote data is coming

RECV FROM:116.236.221.75:8011

+IPD15

hello from pc 2

AT+CIPCLOSE=0

OK

+CIPCLOSE: 0,0

2.3.5 Connection Status Checking

AT+CIPOPEN?

+CIPOPEN: 0

+CIPOPEN: 1

+CIPOPEN: 2

+CIPOPEN: 3

+CIPOPEN: 4

+CIPOPEN: 5

+CIPOPEN: 6

+CIPOPEN: 7

+CIPOPEN: 8

+CIPOPEN: 9

OK

AT+CIPOPEN=0,"TCP","116.236.221.75",8011

OK

+CIPOPEN: 0,0

+IPD15

hello from pc 3

AT+CIPOPEN?

+CIPOPEN: 0, "TCP","116.236.221.75",8011,-1 // last parameter of -1 indicates this

connection is active, this socket acts as a client

+CIPOPEN: 1

+CIPOPEN: 2

+CIPOPEN: 3

+CIPOPEN: 4

+CIPOPEN: 5

+CIPOPEN: 6

+CIPOPEN: 7

+CIPOPEN: 8

+CIPOPEN: 9

OK

2.4 Data Mode

2.4.1 TCP Client

AT+NETOPEN

OK

+NETOPEN: 0

AT+CIPOPEN=0,"TCP","116.236.221.75",8011//only <link\_num>=0 is allowed to operate with

transparent mode.

CONNECT 115200

// sequence of +++ to quit data mode

OK

ATO // command ATO to quit command mode

CONNECT 115200

// sequence of +++ to quit data mode

OK

AT+CIPCLOSE=0

OK

CLOSED

+CIPCLOSE: 0,0

AT+NETCLOSE

OK

+NETCLOSE: 0

**2.5 Switch between Data Mode and Command Mode**

Hardware flow control is recommended.

Currently, USB->modem port, USB->AT port and UART port all support hardware flow control.

Software switching: escape sequence +++. Please take care, this is a complete command, do not

separate each character, also take care that the time delay before and after this sequence should be

more than 1000 milliseconds, the interval of each character should not be more than 900

milliseconds.

Hardware switching: DTR pin could be used to trigger data mode and command mode.Command

AT&D1 should be configured before application.

**2 查询模块网络注册状态**

AT+CPIN?

+CPIN: READY // 查询SIM 卡是否识别

OK

AT+CSQ

+CSQ: 27,99 // 查询信号强度

OK

AT+CNSMOD=1 // 设置模块网络制式状态自动上报功能

OK

AT+CNSMOD?

+CNSMOD: 0,8 // 查询模块注册网

络制式。8 表示注册在LTE 网络模式

OK

AT+CEREG?

+CEREG: 0,1 // 此时，表示可以

进行数据业务了。

OK

AT+CNSMOD?

+CNSMOD: 0,10 // 查询模块注册在非

LTE 网络下

OK

AT+CGREG?

+CGREG: 0,1 // 此时，表示可以进

行数据业务了。

OK

注意：在LTE 网络模式下，请使用AT+CEREG?判断模块数据是否可以使用。

如果是在其它网络模式下, 请使用AT+CGREG 判断模块数据是否可以使用。

参数2：返回1(或5)表示数据业务可以使用；返回2、3、4 表示数据业务不可

用。