NB-IOT CAT-M1 modem(SIM7000C) 網路連接應用

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

有個奇怪的問題是SIM7000C有時候都沒有UART反映, 必須重usb插拔一下才能有反映(感覺是reset), 從Raspberry Pi 電源重置或reboot都沒用; 現象是無論發送TXD任何訊息, 但卻收RXD不到任何訊息

...................................開機檢測..................................

AT #串列傳輸速率同步

OK

AT+CPIN? #檢查SIM卡

+CPIN: READY

OK

AT+CSQ #查詢信號強度

AT+CSQ: 20,0

OK

AT+CGATT? #查詢業務是否附著，確保卡不欠費

AT+CGATT: 1

OK

..........................設置NB-IOT CAT-M1 .............................

AT+CNMP=<mode> #工作模式選擇命令

13：GSM only

38：LTE only（使用NB-IOT網路時CNMP需要設置38）

AT+CMNB=<mode> #CAT-M 與 NB-IOT 選擇命令

1: CAT-M

2: NB-IOT

AT+NBSC=<mode> #擾碼設置（需與基站的擾碼設置一致、大部分基站打開的）

0: 關閉

1: 打開

...........................設置APN 連接到網路.........................

AT+CGNAPN #查詢模組和網路協商註冊時獲取的APN資訊

+CGNAPN: 1,"internet.iot"

OK

AT+CSTT=" internet.iot " #設置網路APN CHT>"internet.iot” or CM>"CMNET"

OK

.................................開始連接流程..............................

AT+CIICR #啟動移動場景

OK

AT+CIFSR #獲取本地 IP 地址

10.173.180.170 #基本上若可以取得IP就是連接置網路了

AT+CIFSR

10.175.62.133

..................................TCP連接流程..................................

AT+CIPSTART="TCP","xx.xx.xx.xx",xx //連接TCP伺服器

OK

CONNECT OK //收到CONNECT表示已經連接成功

AT+CIPSEND=12 //發送資料(12 代表只發送 12 位元組資料)

> 1234567890ABCDEFGHIJ //輸入對應的資料(12 位元組後的資料被丟棄)

SEND OK

1234567890AB //伺服器返回資料

AT+CIPCLOSE=1 //關閉TCP連接CLOSE

OK

AT+CIPSHUT //關閉移動場景

SHUT OK

注：在啟動移動場景後再次啟動就會返回error，需要確保已經關閉移動場景，連接TCP時候需要適當延遲，返回CONNECT OK才算連接成功

**2020 8/17測試結果:**

AT+COPS? #查詢基地台(可註冊之LTE基地台) 幾乎都一致

+COPS: 1,0,"466 92",7

OK



AT+COPS=? #查詢基地台(所有LTE基地台?)

+COPS: (2,"466 92","466 92","46692",7),(3,"466 05","466 05","46605",0),,(0,1,2,3,4),(0,1,2)

OK

AT+COPS=?

有時候出現: (每次訊息可能都不同)或是(沒有資訊表示尚未完成搜尋) 如:

+COPS: (1,"466 12","466 12","46612",7),(2,"466 92","466 92","46692",7),(3,"466 05","466 05","46605",0),(3,"466 05","466 05","46605",7),,(0,1,2,3,4),(0,1,2)

OK

AT+COPS=?



查詢相關資訊(基地台): 底下查詢在取得IP前後都是一樣的反饋

AT+CPSI? #取得連線之註冊訊息

+CPSI: LTE CAT-M1,Online,466-92,0x2CEC,28608801,434,EUTRAN-BAND3,1750,5,5,-7,-84,-60,13

OK

AT+CGATT?

+CGATT: 1

OK

AT+CGNAPN

+CGNAPN: 1,"internet.iot"

OK

**連接場景測試Ping:**

AT+CIPPING="168.95.1.1",50 #取得本地IP地址後也可以AT+CIPPING="iot.cht.com.tw"

>>> ping50()

AT+CIPPING="168.95.1.1",50

+CIPPING: 1,"168.95.1.1",185,248

+CIPPING: 2,"168.95.1.1",91,248

+CIPPING: 3,"168.95.1.1",79,248

+CIPPING: 4,"168.95.1.1",79,248

+CIPPING: 5,"168.95.1.1",78,248

+CIPPING: 6,"168.95.1.1",87,248

+CIPPING: 7,"168.95.1.1",71,248

+CIPPING: 8,"168.95.1.1",79,248

+CIPPING: 9,"168.95.1.1",79,248

+CIPPING: 10,"168.95.1.1",79,248

+CIPPING: 11,"168.95.1.1",79,248

+CIPPING: 12,"168.95.1.1",79,248

+CIPPING: 13,"168.95.1.1",80,248

+CIPPING: 14,"168.95.1.1",79,248

+CIPPING: 15,"168.95.1.1",79,248

+CIPPING: 16,"168.95.1.1",80,248

+CIPPING: 17,"168.95.1.1",79,248

+CIPPING: 18,"168.95.1.1",79,248

+CIPPING: 19,"168.95.1.1",79,248

+CIPPING: 20,"168.95.1.1",79,248

+CIPPING: 21,"168.95.1.1",79,248

+CIPPING: 22,"168.95.1.1",79,248

+CIPPING: 23,"168.95.1.1",79,248

+CIPPING: 24,"168.95.1.1",80,248

+CIPPING: 25,"168.95.1.1",78,248

+CIPPING: 26,"168.95.1.1",79,248

+CIPPING: 27,"168.95.1.1",79,248

+CIPPING: 28,"168.95.1.1",79,248

+CIPPING: 29,"168.95.1.1",80,248

+CIPPING: 30,"168.95.1.1",80,248

+CIPPING: 31,"168.95.1.1",80,248

+CIPPING: 32,"168.95.1.1",79,248

+CIPPING: 33,"168.95.1.1",79,248

+CIPPING: 34,"168.95.1.1",80,248

+CIPPING: 35,"168.95.1.1",80,248

+CIPPING: 36,"168.95.1.1",79,248

+CIPPING: 37,"168.95.1.1",80,248

+CIPPING: 38,"168.95.1.1",80,248

+CIPPING: 39,"168.95.1.1",80,248

+CIPPING: 40,"168.95.1.1",79,248

+CIPPING: 41,"168.95.1.1",80,248

+CIPPING: 42,"168.95.1.1",79,248

+CIPPING: 43,"168.95.1.1",80,248

+CIPPING: 44,"168.95.1.1",78,248

+CIPPING: 45,"168.95.1.1",79,248

+CIPPING: 46,"168.95.1.1",79,248

+CIPPING: 47,"168.95.1.1",80,248

+CIPPING: 48,"168.95.1.1",79,248

+CIPPING: 49,"168.95.1.1",81,248

+CIPPING: 50,"168.95.1.1",78,248

OK

**2021 3/17測試結論: (更換SIM7000C firmware “1351B08SIM7000C”)**

<https://m2msupport.net/m2msupport/data-call-at-commands-to-set-up-gprsedgeumtslte-data-call/>

AT+CGMR #查詢一下firmware version

AT+CREG? #查詢一下網路註冊情況

firmware必須先激活PDP否則往後HTTP應用,網絡會看似正常但永遠出現反饋 +HTTPACTION: 0,601,0

AT+CGDCONT=1,”IP”,”internet.iot” #模組激活, 前後如下:



HTTP一直反饋 +HTTPACTION: 0,601,0

AT+SAPBR=0,1

AT+SAPBR=1,1

模塊連接電信基站時最好先檢查SIM card & 基站狀態才進行基站連接, 如

AT #模塊硬件反映

AT+CPIN? #Sim Card ready

AT+CGNAPN #APN ?

電信基站連接條件最好先檢查AT+CGATT? 是否=1(可連接狀態) 才進行網路服務連接及取得本地IP.

本地IP取得會因為很多原因而消失(尤其是測試AT command) 在 +CGATT: 1條件下, 簡單指令即可重新取得本地IP ,指令如下:

AT+CSTT=”internet.iot”

AT+CIICR

**9.1.1 普通 TCP/TP 发送步骤**

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+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。