

Beijing BOCON GW800 Developer's Guide Hardware and Software Description

September 20, 2009
gw800-ds-A

Chapter 1 简介	1
1.1 GW800 综述	1
1.2 接口部分	2
1.3 应用接口	4
1.4 通讯协议	4
1.5 硬件参数	4
1.6 无线参数	4
1.7 调试软件介绍	5
1.7.1 iChipconfig	5
1.7.2 PduReceiver	6
Chapter 2 如何启动	7
2.1 硬件连接	7
2.2 使用环境	7
Chapter 3 AT+i 指令集	8
3.1 指令集简介	8
3.2 指令格式	8
3.3 指令返回码	9
3.4 常用指令	10
3.4.1 AT+i 握手指令	10
3.4.2 +iEn 回显模式 (Echo Mode)	10
3.4.3 +iFD 恢复出厂设置 (Factory Defaults)	10
3.4.4 +iBDRA 设置使用自动波特率 (Auto Baud Rate Mode)	10
3.4.5 +iBDRF 设置串口波特率 (Fixed Baud Rate)	10
3.4.6 +iDOWN 软复位 (Software Reset)	11
3.4.7 +iPING PING指令 (PING Request)	11
Chapter 4 状态报告 (Report Status)	12
4.1 状态报告指令 (Report Status Command)	12
4.2 状态报告格式 (Report Status Format)	12
Chapter 5 无线网络设置 (Wireless LAN)	16
5.1 +iWLCH — 设置通讯信道 (Wireless LAN Communication Channel)	16
5.2 +iWLSI — 设置SSID (Wireless LAN Service Set Identifier)	16
5.3 +iWLWM — 设置WEP方式加密 (Wireless LAN WEP Mode)	16
5.4 +iWLKI — WEP密码索引 (Wireless LAN Transmission WEP Key Index)	16
5.5 +iWLKn — WEP密码 (Wireless LAN WEP Key Array)	16
5.6 +iWLPP — WPA/WPA2密码设置 (Personal Shared Key Pass-Phrase)	17
5.7 +iWSEC — Wireless LAN WPA Security	17
5.8 +iWSTn — Wireless LAN Security Type Array	17
Chapter 6 IP地址设置 (IP Address)	18
6.1 +iDIP — 手工设置IP地址 (设备 Default IP Address)	18
6.2 +iIPA — IP地址 (Active IP Address)	18
6.3 +iIPG — 网关 (IP Address of the Gateway)	18
6.4 +iSNET — 子网掩码 (Subnet Address)	18

Chapter 7 串口转WiFi网桥/透明串口模式 (SerialNET Mode)	19
7.1 +i[!]SNMD—进入透明串口模式 (SerialNET Mode)	20
7.2 +iHSRV +iHSRn —透明串口模式的服务器地址 (Host Server Name/IP)	20
7.3 +iHSS —透明串口模式特殊控制字符 (Assign Special Characters to Hosts)	20
7.4 +iLPRT —透明传输模式下的侦听地址 (SerialNET Device Listening Port)	20
7.5 +iDSTR —透明串口模式下断开当前连接 (Disconnect for SerialNET Mode)	21
7.6 +iMBTB —透明传输模式下的缓冲区最大字节数 (Max Bytes To Buffer)	21
7.7 +iFCHR —透明串口模式下的特定缓冲字符 (Flush Character)	21
7.8 +iMCBF —透明串口模式下最大缓冲字符数 (Max Characters before Flush)	21
7.9 +iMTTF —透明串口模式下的最大缓冲超时 (Max Timeout to Socket Flush)	21
7.10 +iIATO —透明串口模式的通讯中断超时 (Inactivity Timeout)	21
7.11 +iSNSI —透明串口模式的串口通讯格式 (SerialNET Device Serial Interface)	22
7.12 +iSTYP —透明串口模式的通讯协议 (SerialNET Device Socket Type)	22
7.13 +iSNRD —透明串口模式的初始化延迟 (Device Re-Initialization Delay)	22
7.14 +iHIF —主机接口 (Host Interface)	22
8 LAN转WiFi网桥 (Lan to WiFi Bridge Mode)Chapter	23
9 多Socket通讯模式 (Direct Socket Interface)	25
9.1 +ISTCP — 打开并连接一个TCP Socket (Open 和 Connect a TCP Socket)	25
9.2 +ISUDP — 打开并连接一个UDP Socket (A UDP SOCKET)	25
9.3 +iLTCP — 打开一个TCP侦听Socket (Open a TCP Listening Socket)	26
9.4 +iLSST —获取一个监听端口的状态 (Get a Listening Socket Active Connection Status)	26
9.5 +iSSST —获取一个监听端口的连接状态 (Get a Single Socket Status Report)	26
9.6 +iSCS —获取一个套接字状态报告 (Get a Socket Connection Status Report)	26
9.7 +iSSND[%] — Socket发送指令 (SEND A BYTE STREAM TO A SOCKET)	27
9.8 +iSRCV — Socket接收指令 (Receive a String from a Socket's Input Buffer)	27
9.9 +iGPNM — 为一个指定的套接字获取对等机名 (Get Peer name for a Specified Socket)	27
9.10 +iSDMP — 转储套接字缓冲 (DUMP SOCKET BUFFER)	27
9.11 +iFSH[%] —立即输出套接字中的输出数据 (Flush Socket's Outbound Data)	28
9.12 +iSCLS —关闭Socket (Close Socket)	28
Chapter 10 节能模式 (Power Save Mode)	29
Chapter 11 漫游模式 (Roaming Mode)	30
11.1 +iWROM — Enable Roaming in WiFi	30
11.2 +iWPSI — Periodic WiFi Scan Interval	30
11.3 +iWSRL — SNR Low Threshold	30
11.4 +iWSRH — SNR High Threshold	30
11.5 +iWSIn — Wireless LAN Service Set Identifier Array	30
11.6 +iWPPn — Pre-Shared Key Passphrase Array	30
11.7 +iWKYn — Wireless LAN WEP Key Array	31
11.8 +iWSTn — Wireless LAN Security Type Array	31
Chapter 12 远程控制 (Remote Control)	32
Chapter 13 操作样例	33
附录 A 错误返回码	34

1.1 简介

GW800系列是北京博讯科技有限公司推出的工业级Wi-Fi设备服务器（WiFi网关）。可以十分方便的连接现有串口设备或10/100M以太网设备到802.11b/g无线局域网。适合任何需要对设备增加WiFi网络接入功能，且对IP安全有较高要求的M2M应用。

GW800的透明传输模式提供一种真正的“即插即用”，使现有的串口或以太网设备不需要任何修改就可以进行数据通讯，显著减少了嵌入式系统开发的工作量。

本系列的多Socket工作模式可以建立最多10条的TCP/UDP Socket，其中包括两条可以建立侦听的Socket，以及可进行SSL3加密的Socket，灵活的Socket配置方式可以让通讯方式更加灵活。

GW800固件和配置参数可以通过 Web 界面或远程Socket进行远程配置。配套的“iChipConfig”程序可以通过串口进行可视化的操作，简便易行。

支持两种网络形式：可以通过AP或无线路由器接入WiFi网络进行通讯，也可以设备间通过ad-hoc直接相连实现“点对点”通讯。

提供WEP,WPA,WPA2鉴权加密，并能实现SSL3/TLS1硬件加密。保障数据安全。

金属壳体，工业级温度范围，可更换天线设计，电磁隔离（多路，可选），宽电压供电，使本系列产品足以应对各种严酷的工作环境。

视具体功能，包含5款产品：

GW810(RS-232型)：提供RS-232串口转WiFi功能；

GW820(RS-485型)：提供RS-485串口转WiFi功能；

GW830(以太网型)：提供以太网那个功能，提供以太网转WiFi功能。

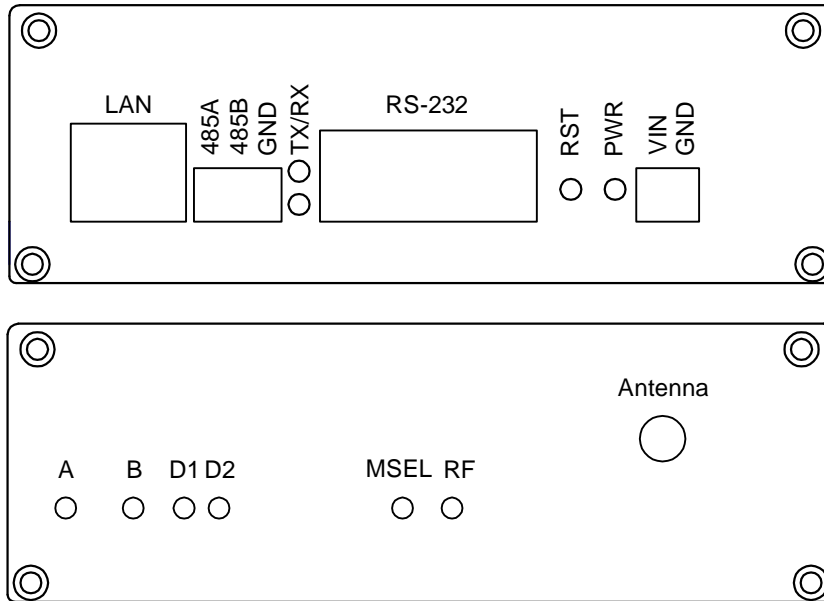
GW810和GW820型号可选隔离功能，相对应的型号为GW810i，GW820i。



接口

1.2 接口部分

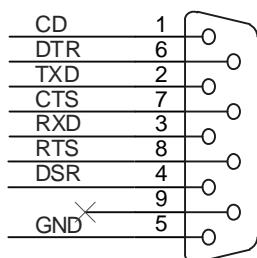
GW800 系列支持多种硬件接口：RS-232,RS-485和以太网接口(RJ-45)。分别对应本系列的三款产品：GW810,GW820,GW830。



- RJ-45: 以太网接口
- RS-485: 485串口 (可选隔离)
- RS-232: 232串口 (可选隔离)
- POWER: 电源插头,左正右负
- Antenna: SMA天线接头
- RST: 复位按键
- PWR: 电源指示灯
- MSEL: MSEL按键 (Mode Select)
- RF: 射频指示灯
- TX/RX: 发射/接收指示灯
- A: NC
- B: NC
- D1: NC
- D2: NC

1.2.1 接口介绍

RS-232:采用的是标准的RS-232串口
针脚定义:



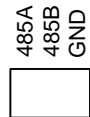
接口

9芯	信号方向来自	缩写	描述
1	GW800	CD	载波检测
2	GW800	RXD	接收数据
3	串口设备	TXD	发送数据
4	串口设备	DTR	数据终端准备好
5		GND	信号地
6	GW800	DSR	通讯设备准备好
7	串口设备	RTS	请求发送
8	GW800	CTS	允许发送
9		保留	

- 串行数据格式
 AT+i 模式: 异步; 二进制; 8位数据位; 无校验; 1位停止位。
 透明串口模式: 异步; 二进制; 7或8位数据位; 奇/偶/无校验; 1位停止位。
- 流控: (-RTS, -CTS)和软件流控。

RS-485:

RS-485采用3.81mm间距的插拔端子。
 在定义485A和485B针脚外, 还定义了一个GND针脚。
 内部RS-485的电磁隔离电路提供了对(485A,485B)电路的保护。



LAN(RJ-45):

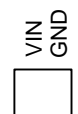
以太网 10/100Base-T 接口, 10/100M自适应。
 具有AUTO MDIX功能, 可以TX+/-和RX+/-自动切换。
 使用网线或者是交叉网线都可以通讯。

Pin	Name	描述
1	TX+	Tranceive Data+ (发信号+)
2	TX-	Tranceive Data- (发信号-)
3	RX+	Receive Data+ (收信号+)
4	N/C	Not connected (空脚)
5	N/C	Not connected (空脚)
6	RX-	Receive Data- (收信号-)
7	N/C	Not connected (空脚)
8	N/C	Not connected (空脚)



电源:

GW800采用宽压供电(8-24V), 推荐 9-12V DC。
 采用3.81mm间距的插拔端子, 方便工业现场安装。
 定义为左正右负:



硬件参数

天线:

本设备采用SMA天线接头。默认为4.15dBi增益直弯两用型天线，并可根据现场需要选用更高增益的天线。

1.3 应用接口

- AT+I 协议
- 透明串口网桥
- LAN-WiFi 透明网桥(只限GW820)

1.4 通讯协议

- 因特网通讯协议: ARP, ICMP, IP, UDP, TCP, DHCP, DNS, NTP, SMTP, POP3, MIME, HTTP, FTP 和 TELNET
- 加密协议: SSL3/TLS1, HTTPS, FTPS, RSA, AES-128/256, 3DES, RC-4, SHA-1, MD-5, WEP, WPA/WPA2 (PSK 和 Enterprise)
- 硬件加速协议: AES, 3DES 和 SHA

1.5 硬件参数

- 尺寸: 147 x 103 x 40 mm
- 重量: 340g(视具体型号而定)
- 外壳: 铝合金
- 防护等级: IP30
- 工作电压: 8-24V DC 输入, 推荐 9-12V DC
- 湿度范围: 90% 最大 (非结露)
- 温度范围: -40°C to +85°C (-40° to 185°F)
- 能耗:
 - 0.8W @ 9V DC (典型)
 - 180mW @ 9V DC (节能模式)
- 天线接头: SMA头天线

1.6 无线参数

- 无线标准: IEEE 802.11b/g
- 频率范围: 2.412-2.472GHz
- 信道: 13 channels (Europe)
- 天线: 4.15 dBi SMA接口天线 (可更换)

1.7 调试软件介绍

本设备提供了配套软件，供测试时或者配置参数使用。

配置程序：iChipconfig，TCP/UDP Socket通讯工具 PduReceiver。

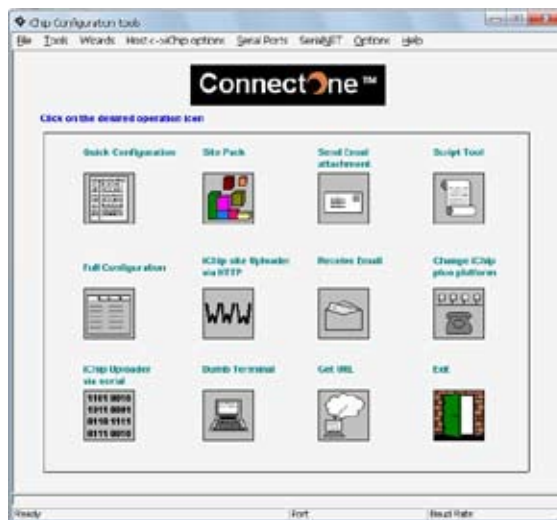
1.7.1 iChipconfig

iChipconfig是一个可视化的配置软件，可以通过串口对设备进行调试。

对设备的各项参数进行配置以及修改，

主界面包含12个应用图标，分别为：

- 1,Quick Configuration
- 2,Full Configuration
- 3,Firmware Update
- 4,Site Pack
- 5,iChip Website Uploader via HTTP
- 6,Dumb Terminal
- 7,Send email attachment
- 8,Receive emails
- 9,Get URL
- 10,Script Tool
- 11,Change iChip communication platform
- 12,Exit



测试中主要使用的是Full Configuration，Firmware Update 和 Dumb Terminal。

Full Configuration可以对设备的所有参数和设置进行可视化配置。

Firmware Update 可以升级设备的固件和BOOT文档。具体升级步骤见附件B。

Dumb Terminal是一个串口通讯程序，和超级终端的功能类似。

操作步骤：

- 1，点击菜单栏中的“Serial Ports”选择串口及其波特率，如跳出提示框显示“iChip found Port : baud rate:”表示串口已经可以通讯；
- 2，点击“Full Configuration”图标，然后等待窗口下部的进度条走到最后；可以在窗口上部看到有15个选项卡：“User Fields” “RAS” “Wireless LAN” “SSL” “Router” “ISP Connection” “HTTP” “Serial NET” “IP registrion” “Emial Format” “Server Profiles” “Operational” “LAN” “Romote FW” 每个选项卡对应相关的设置选项；我们初步设置模块需要了解“Wireless LAN”“LAN” “Serial NET” “Operational”等选项卡的内容，分别对应设备的“无线网络设置”“IP相关设置”“透明串口模式”“一般设置”等内容的设置，相关设置可以查看相关的文档。
- 3，“Wireless LAN”中设置的主要是无线网络相关的内容，主要包含 SSID，加密方式加密密码等内容，相关设置见章节5“无线网络设置”，设置更改后，点击窗口最下方的“SAVE”按钮，相关设置就保存在设备内部的FLASH中。如无需更改，则点击下面的“CLOSE”按键。

设备这时可以连接无线路由器，设备的RF灯应该已经长亮，如果继续闪烁，就需要检查相关设置是否正确。

- 4, 如果这时重新进入“Full Configuration”，如果网络是DHCP自动分配IP，这时可以在IPA（IP Address）选项中看到设备当前的IP地址，没有的话就需要返回步骤3检查设置或者手工设置地址IP。此选项卡中还可以设置子网掩码，网关等。



- 5, 点击“SerialNET”选项卡，可以看到与透明串口模式的相关配置信息。参照 章节 7“串口转WiFi网桥/透明串口模式”中可以看到相关选项的说明。然后在“Operational”选项卡里细节设置进行一些补充（如：HIF，BDRF等）。点击“SAVE”保存退出
- 6, 在菜单栏的“SerialNET”选项卡里选择“Enter SerialNET Mode and stay online”，这时设备就进入透明传输模式，进行串口数据的透明传输。同理，点击“SerialNET”里的“Exit SerialNET Mode”可以退出这种模式。

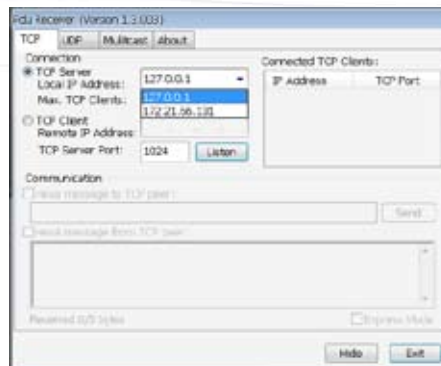
1.7.2 PduReceiver

PduReceiver是一个TCP/UDP的Socket通讯工具，可以分别建立TCP/UDP的服务器侦听与客户端Socket。为设备建立一个Socket通讯环境。

使用步骤：

（以建立TCP Server Socket为例）

- 1, 选择TCP/UDP协议
- 2, 选择PC作为“Server”或“Client”
比如作为“TCP Server”，在“TCP Server IP Address”框体内选择PC当前的IP地址，在TCP Server Port内填写本PC需要开放的端口地址。
- 3, 点击“Listen”。

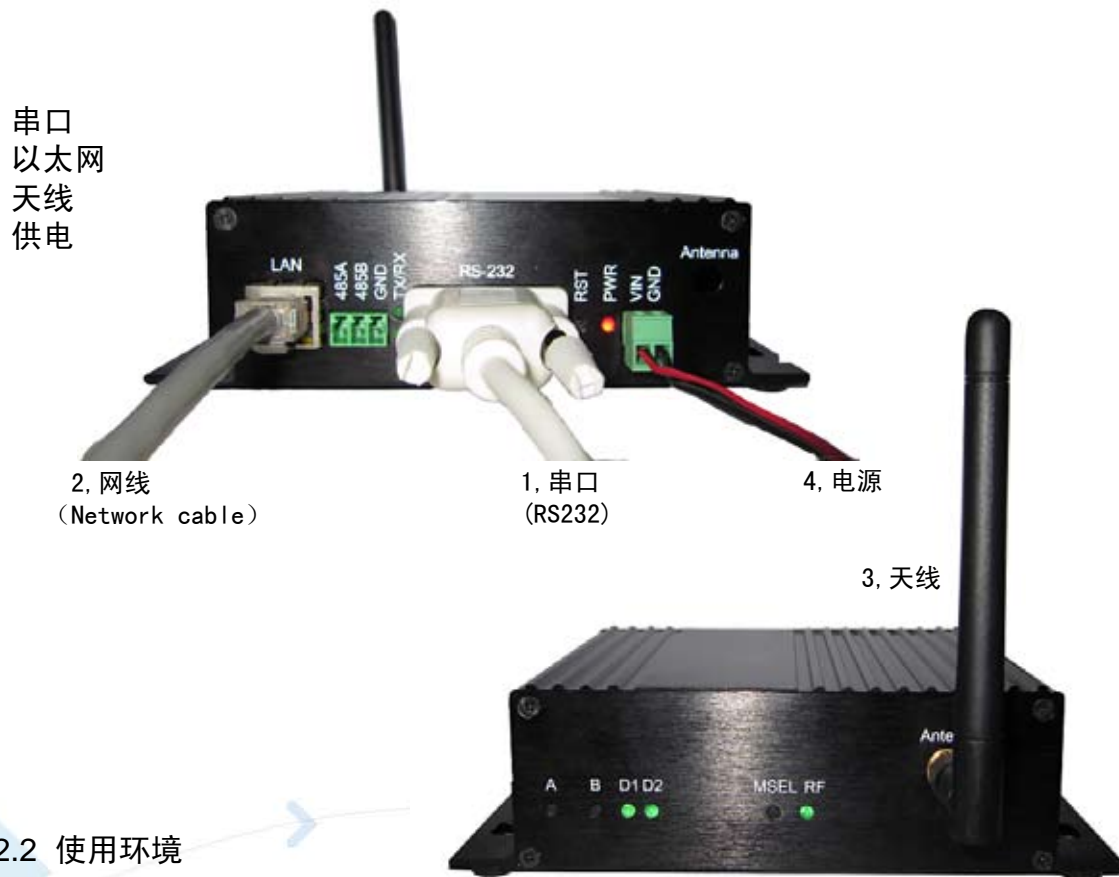


这时一个TCP的侦听已经建立，当你用设备建立面向这个Socket的连接时，就可以直接进行Socket通讯。

Chapter 2 如何启动

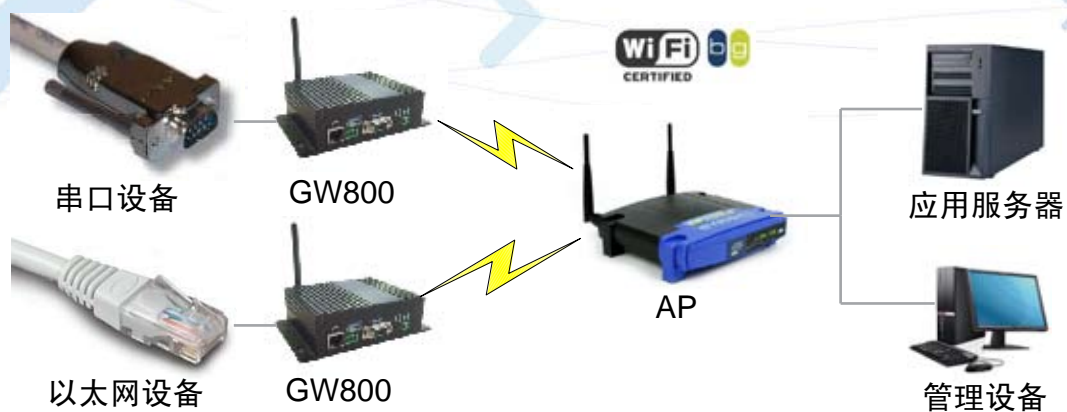
本章节介绍如何连接GW800的硬件，以及测试环境的搭建。

2.1 硬件连接



2.2 使用环境

测试及使用环境是串口设备或以太网设备通过GW800连接AP，从而和局域网建立通讯连接。通过GW800的应用程序接口，将主机接口数据（串口/以太网）和服务器间进行数据交互。



3.1 指令集简介

AT+i指令集是基于AT指令方式，并对AT方式做了明显的扩充。
 本章节说明了AT+i 指令集的构成，返回码，响应状态以及相关代码的详细描述。
 可以对GW800的各项参数进行设置和查询，可以查询设备当前的运行状态，设置GW800的工作模式以及工作状态.....

3.2 指令格式

AT+i指令不区分大小写，大小写格式均可执行。
 AT+i指令集所有的指令都是以AT+i开头，后跟2~4个字符的指令名<cc>，然后是指令类型的符号,以及与指令名有关的相关参数<parameter>，指令以回车符<CR>结尾。如下：

AT+i<cc>[<parameter>]<CR>

相关说明如下：

<cc>	2~4个字符的指令码或者参数名 (<cc>)
	定义符: '=', '~', '?', ':', '_'
<parameter>	可选参数或数据。如果<parameter>内容包括一个, 像上面定义的那样, 它必须括在单引号 (') 或双引号 (") 之内。表示结束的<CR>也被作为结束引号。
<CR>	回车符 (ASCII 13)

参数的赋值及查询：

<par>=value 或 <par>:value	设定参数值	赋值给参数<par>, 并将设定值保存到内部的flash中。
<par>~value	对一个会话分配参数值 (只在此会话中生效)	给一个互联网会话的参数赋值。 会话结束后, 会恢复原始的参数值。
<par>?	查询参数当前设定值	会返回参数<par>当前的设定值。
<par>=?	查询参数允许设置值的范围或格式	返回当前参数允许的设定值。

对一个参数<Par>进行配置的指令是： AT+iPAR=****

查询参数<Par>当前设定值的指令是： AT+iPAR?

查询参数<Par>有效范围的指令是： AT+iPAR=?

清空参数<Par>当前设定值的指令是： AT+iPAR=""

3.3 指令返回码

根据设备对于指令执行的情况，设备会返回不同的代码，分别代表对指令执行的不同情况，如下：

响应字符串		
I/OK	指令成功执行。	
I/BUSY	设备忙. 指令被丢弃。	
I/DONE	设备完成互联网活动并返回到命令模式，或已进入SerialNET模式。	
I/ONLINE	设备完成互联网活动并返回到命令模式，或已进入SerialNET模式。设备一直保持在线状态或作为Web服务器保持在线。	
I/OFFLINE	设备被设置进入SerialNET保持在线模式，但未能发现一个网络连接。	
I/ERROR(nnn)	nnn	指令的执行发生错误，指令被丢弃。

如果出于某种原因，设备对于指令的指令出现故障的话，设备会返回一个错误码。

格式如上：I/ERROR(nnn)

其中 nnn 代表的就是设备的错误码。不同错误码对应设备发生的不同错误，可以根据错误码来分析出现错误的原因。

附录A对错误码分别进行了详细描述，请查阅。

3.4 常用指令

3.4.1 AT+i 握手指令

格式: AT+i

描述: AT+i是所有指令的指令头, 也是一个握手指令。是检验串口是否已经可以通讯以及设备是否在正常工作的最基本指令。

3.4.2 +iEn 回显模式 (Echo Mode)

格式: AT+iEn

描述: n=0 不显示主机回显

n=1 显示所有主机回显

此指令与ATEn等效。

3.4.3 +iFD 恢复出厂设置 (Factory Defaults)

格式: AT+iFD

描述: 完全恢复出厂默认设置。

3.4.4 +iBDRA 设置使用自动波特率 (Auto Baud Rate Mode)

格式: AT+iBDRA

描述: 使设备使用波特率自动侦测模式。

根据上电后接受到的第一个字符的通讯波特率来确定设备自身的通讯波特率。

采用下列的波特率都可以和设备直接进行串口通讯:

2400, 4800, 9600, 19200, 38400, 57600, 115200 和 230400。

AT+iBDRA指令 和 at+iBDRF=a 等效。

3.4.5 +iBDRF 设置串口波特率 (Fixed Baud Rate)

格式: AT+iBDRF=<n>

描述: 设置设备的串口通讯波特率。(注意和SNSI参数相区分)

可以设置为: a, 3, 4, 5, 6, 7, 8, 9, h 等值。

其中:

<n>=a 设置串口波特率为自动侦测;

<n>=3 设置串口波特率为2400;

<n>=4 设置串口波特率为4800;

<n>=5 设置串口波特率为9600;

<n>=6 设置串口波特率为19200;

<n>=7 设置串口波特率为38400;

<n>=8 设置串口波特率为57600;

<n>=9 设置串口波特率为115200;

<n>=h 设置串口波特率为230400;

按MSEL按键5秒以上, 可将波特率参数恢复为自动侦测模式, BDRF参数将在本操作的下次上电时重新生效。

3.4.6 +iDOWN 软复位 (Software Reset)

格式: AT+iDOWN

描述: 执行一个软复位, 断开当前所有的网络会话, 下线并返回指令模式。

执行这个指令, 设备会下线并重新初始化, 此过程需要大概2.5秒的时间。

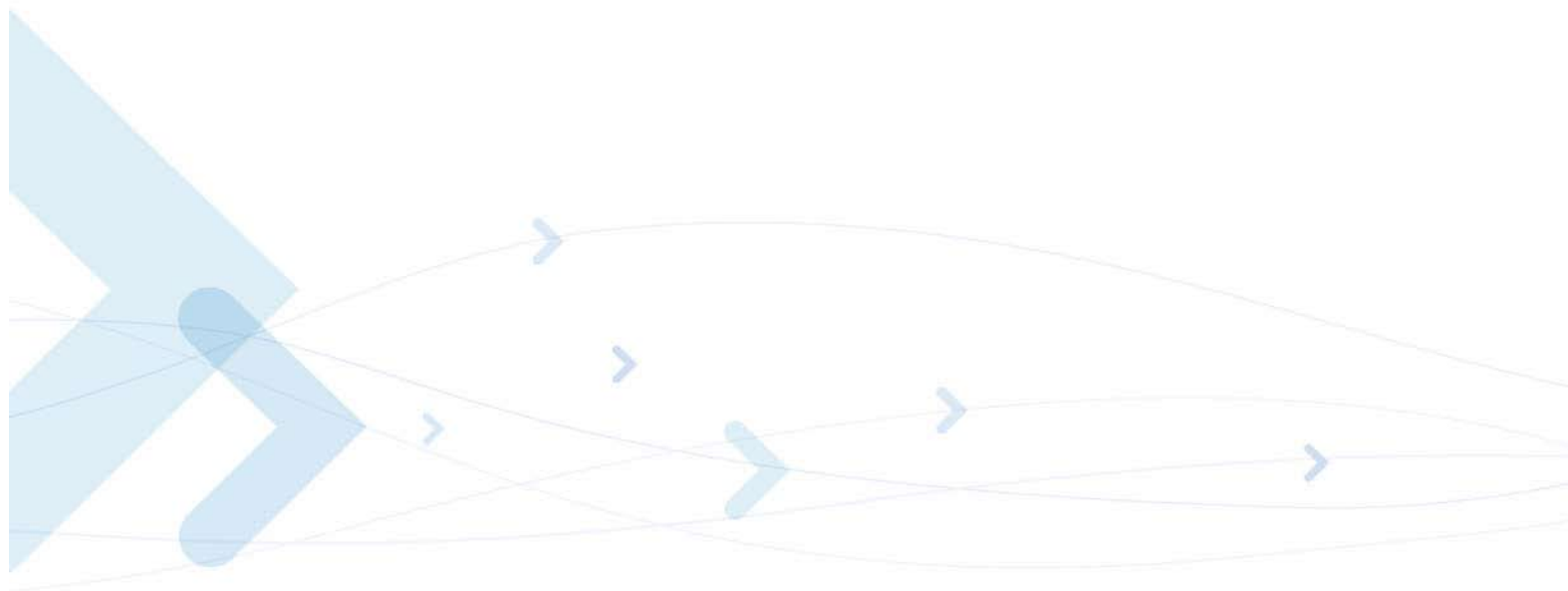
3.4.7 +iPING PING指令 (PING Request)

格式: AT+iPING:<host>

描述: 发送一个PING包到远程的<host>,

设备会返回: I/<RTT>

<RTT>表示PING包来回设备间的时间, 单位毫秒。



Chapter 4 状态报告 (Report Status)

4.1 状态报告指令 (Report Status Command)

格式: AT+i[!]RP<i>

描述: 根据<i>的值返回相应的状态报告。

- <i>=0 返回设备器件号。
- <i>=1 返回当前固件和修订日期。
- <i>=2 返回连接状态。
- <i>=3 返回BOOT文档版本和修订日期
- <i>=4 返回设备所有套接字的数据接收状态。
- <i>=5 返回独有序列号。
- <i>=6 返回一个当前ARP表格。
- <i>=7 返回套接字缓冲利用位图。设备的DATA_RDY信号可以用于通知更改硬件中套接字缓冲状态。当一个或多个套接字中有可用的新数据时该信号将发出。阅读过所有套接字之后它将被拉低。这个信号会在一个或多个Socket 接收到新数据或远程浏览器更改了参数配置时被拉高，当Socket总数有数据被读取后重新拉低。
- <i>=8 返回当前时间，它基于从网络时间服务器上获取到的时间以及当前GMT时间偏移量，如果在上次上电后没有与远程的时间服务器连接上的话，会返回一个全零值。
- <i>=9 保留
- <i>=10 和 AT+i!RP10 返回当前无线网络连接的两种不同的状态报告。
- <i>=11 返回一个附件存在的无线AP的列表。
- AT+i!RP11 返回一个附近存在的ad-hoc无线网络的列表。
- <i>=14 返回一个与设备连接的所有DHCP服务器的MAC和IP地址表格。
- <i>=20 返回附近存在的所有AP和ad-hoc网络的列表。

4.2 状态报告格式(Status Message Format)

<i>	格式
0	COnnnAD-ii nnn – Version number; ii – Interface code: S-Serial, L-LAN, D-Dual
1	liimmmTss (<version-date>) lii – Interface code; mmm – Major Version; T – Version type code; ss – Sub-version
2	Status string: "Modem data<CR/LF>" "Command mode<CR/LF>" "<CR/LF>Connecting to ISP<CR/LF>" "<CR/LF>Connected to ISP<CR/LF>" "<CR/LF>Connecting as RAS<CR/LF>" "<CR/LF>RAS Connected<CR/LF>""<CR>Closing PPP<CR/LF>" "<CR/LF>Establishing SMTP<CR/LF>" "<CR/LF>Sending Email<CR/LF>"

<i><i></i>	格式																																	
	- 接上文 "<CR/LF>Establishing POP3<CR/LF>" "<CR/LF>POP3 Open<CR/LF>" "<CR/LF>Establishing HTTP<CR/LF>" "<CR/LF>Receiving HTTP<CR/LF>" "<CR/LF>Carrier Lost<CR/LF>" "<CR/LF>Link Lost<CR/LF>"																																	
3	nnmm – Boot block version number																																	
4	I/(<sock0sz>, <sock1sz>, ... ,<sock9sz>) sock<i>sz >=0 : Number of bytes pending in socket's input buffer <0 : Negative value of socket's error code																																	
5	nnnnnnnn – Hexadecimal representation of iChip serial number.																																	
6	Current ARP table listing: INTERNET ADDRESS PHY ADDRESS STATE TTL nnn.nnn.nnn.nnn xxxxxxxxxxxx VALID nnn sec. For debugging purposes.																																	
7	I/xxxx xxxx – 16 bit Hex Value Bitmap A bit set to "1" indicates that the corresponding socket contains buffered data, which needs to be read by the host. <table border="1" style="margin: 10px auto; border-collapse: collapse;"> <tr> <td>bit</td> <td>15</td> <td></td> <td></td> <td></td> <td></td> <td>10</td> <td></td> <td></td> <td>7</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>0</td> </tr> <tr> <td>socket</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>WEB</td> <td>9</td> <td>8</td> <td>7</td> <td>6</td> <td>5</td> <td>4</td> <td>3</td> <td>2</td> <td>1</td> <td>0</td> </tr> </table> Bit 10 is set to "1", when the remote browser updates one or more application website parameter tags. It will be reset to "0" when the host reads any application website parameter, using AT+i<Parameter Tag>?	bit	15					10			7						0	socket						WEB	9	8	7	6	5	4	3	2	1	0
bit	15					10			7						0																			
socket						WEB	9	8	7	6	5	4	3	2	1	0																		
8	The current time-of-day is returned according to ISO 8601: <YYYY-MM-DD>T<HH:MM:SS> <TZD> YYYY-MM-DD -- Year-Month-Day ; "T" – Fixed Separator ; HH:MM:SS - Hrs:Mins:Secs ; TZD - Time Zone Designator: +hh:mm or -hh:mm All-zeros response: 0000-00-00T00:00:00 <TZD>.																																	
9	Reserved																																	
10	I/(<port stat>, <xfer rate>, <sig level>, <lnk qual>) port stat -Port Status: 0: Wireless LAN adapter not present 1: Wireless LAN adapter disabled 2: Searching for initial connection 4: Connected 5: Out of range xfer rate -- Transfer rate in the range 1..54 sig level -- Signal level [%], in the range 0..100 lnk qual -- Link quality [%], in the range 0..100																																	

<i><i></i>	格式
AT+!IRP10	<p>Returns a report of the current WLAN connection. <SSID>,<BSSID>,<security type>,<WPA status>,<channel>,<SNR> I/OK where <input type="checkbox"/> <security type>=NONE WEP64 WEP128 WPA WPA2 <input type="checkbox"/> <WPA status>=Completed Not Completed <WPA status> indicates, when WPA/WPA2 security is specified, whether WPA negotiation completed or not. Notes: <input type="checkbox"/> For Ad-Hoc networks, SSID starts with (!). <input type="checkbox"/> WPA status is reported whether WPA negotiation completed or not. For example: Jetta,06:14:6C:69:4A:7C,WPA,Completed,1,68 I/OK</p>
11	<p>iChip scans all available Access Points (APs) in the surrounding area and returns a list of APs. Each line contains the following comma-separated fields: SSID, security scheme, and signal strength. The AP having the strongest signal appears first.</p> <p><SSID>,<security_scheme>,<signal_strength><CR><LF> <SSID>,<security_scheme>,<signal_strength><CR><LF> . . <SSID>,<security_scheme>,<signal_strength><CR><LF> I/OK<CR><LF></p> <p>where, SSID – Up to 32 alphanumeric characters security_scheme – None WEP WPA signal_strength 0 - low, 1 - good, 2 - excellent</p> <p>Note: If no APs are detected, only I/OK<CR><LF> is returned.</p>
AT+!IRP11	<p>Returns a list of all Ad-Hoc networks available in the surrounding area. Each line contains the following comma-separated fields: SSID, security scheme, and signal strength. Security scheme for Ad-Hoc networks is NONE. The Ad-Hoc network having the strongest signal appears first.</p> <p><SSID>,NONE,<signal_strength><CR><LF> <SSID>,NONE,<signal_strength><CR><LF> . . <SSID>,NONE,<signal_strength><CR><LF> I/OK<CR><LF></p> <p>where,</p>

Chapter 5 无线网络设置 (Wireless LAN)

无线部分设置是设备配置的第一步，目的是将设备与无线AP建立硬件的通讯链路。需要设置的参数为SSID, 加密方式 (WEP/WPA/WPA2), 加密密钥……。

5.1 +iWLCH — 设置通讯信道 (Wireless LAN Communication Channel)

格式: AT+iWLCH=<channel>

描述: 设置无线局域网的通讯信道, 可以设置为0~13
设置为0时, 可以根据所连接AP的信道自动选择,
设置为1~13时, 设置为固定的信道。

5.2 +iWLSI — 设置SSID (Wireless LAN Service Set Identifier)

格式: AT+iWLSI=<ssid>

描述: 设置无线局域网的SSID, 就是网络名。

注意: SSID区分大小写。

5.3 +iWLWM — 设置WEP方式加密 (Wireless LAN WEP Mode)

格式: AT+iWLWM=<md>

描述: 设置WEP方式的加密方式,
<md>=0 不使用WEP加密。
<md>=1 使用64位 WEP加密。
<md>=2 使用128位 WEP加密。

5.4 +iWLKI — WEP密码索引 (Wireless LAN Transmission WEP Key Index)

格式: AT+iWLKI=<ki>

描述: 设置WEP密码索引位置。

<ki> 可以设置为1~4, 设置后设备才会采用对应位置的密码。

5.5 +iWLKn — WEP密码 (Wireless LAN WEP Key Array)

格式: AT+iWLKn=<keyString>

描述: 设置WEP加密的密码。“n”需要对应WLKI指令的密码位。

如果采用的是64位加密的话, 须为10个16进制数密码;

如果采用的是128位加密的话, 须为26个16进制数密码。

如果AP采用ASCII码密码, 则需要将此密码转换成16进制数密码再填写。

需要注意的是, 如果WEP加密和WPA/WPA2加密选项都进行了设置的话, WPA/WPA2加密具有优先级, 此时WEP密码即使设置了也不会生效。

也就是说需要从WPA/WPA2加密切换到WEP加密, 需要先清空WPA/WPA2加密设置。

5.6 +iWLPP — WPA/WPA2密码设置 (Personal Shared Key Pass-Phrase)

格式: AT+iWLPP=<passphrase>

描述: 设置WPA/WPA2密码。

需要注意的是, 如果WEP加密和WPA/WPA2加密选项都进行了设置的话, WPA/WPA2加密具有优先级, 此时WEP密码即使设置了也不会生效。

也就是说需要从WPA/WPA2加密切换到WEP加密, 需要先清空WPA/WPA2加密设置。

5.7 +iWSEC — WPA或者WPA2设置(Wireless LAN WPA Security)

格式: AT+iWSEC=<n>

描述: 设置WPA加密方式或者WPA2加密。

此指令只在WPA/WPA2加密时生效。

<n> =0 WPA-TKIP 加密

<n> =1 WPA2-AES 加密

5.8 +iWSTn — 无线加密设置(Wireless LAN Security Type Array)

格式: AT+iWSTn=<sec>

描述: 综合设置无线的加密设置方式。

此指令可为多个SSID进行加密方式的设置。

n=0时, 设置的是默认SSID的加密方式,

n=1~9, 设置的是漫游模式下多SSID的加密方式的设置,

分别对应WSIn的1~9号SSID的加密方式的设置。

<sec>=0~6, 设置对应SSID的加密方式。

<sec>=0 无加密

<sec>=1 WEP-64

<sec>=2 WEP-128

<sec>=3 WPA-TKIP-PSK

<sec>=4 WPA2-AES-PSK

<sec>=5 WPA-TKIP-Enterprise

<sec>=6 WPA2-AES-Enterprise

默认: <sec>=0

Chapter 6 IP地址设置 (IP Address)

这个部分叙述和设备的IP地址相关的选项设置，包括设备IP地址，子网掩码，网关等。

可以设置设备从DHCP服务器分配IP地址，也可以设置为固定的IP地址。DHCP设置为自动获取的时候，所有与IP相关的参数都可从DHCP服务器获得，包括IP地址，子网掩码，网关等。如果需要手工设置IP地址的话，这些相关设置都需要人工设置，包括DIP,IPG,SNET等参数。

6.1 +iDIP — 手工设置IP地址 (设备 Default IP Address)

格式：AT+iDIP=<IP address>

描述：设置设备的默认IP地址，设定后将以此IP地址进行通讯，也即手工设置IP地址。

如果需要设备从网络的DHCP服务器来获取IP地址，则需要设置DIP参数为0.0.0.0

DIP参数在复位或重新上电后仍然有效。

6.2 +iIPA — IP地址 (Active IP Address)

格式：AT+iIPA= <IP address>

描述：设置设备当前在网络中使用的IP地址。

如果使用iIPA参数设定当前IP地址，在复位或重新上电后失效。

这个参数主要是用AT+iIPA?指令来查询当前IP地址使用的较多。

6.3 +iIPG — 网关 (IP Address of the Gateway)

格式：AT+iIPG=<IP address>

描述：设置网关地址。

根据网络的实际网关地址填写。

如无需和外网通讯，不用设置此选项。

如果不设置此选项，这无法和外网进行通讯。

6.4 +iSNET — 子网掩码 (Subnet Address)

格式：AT+iSNET=<IP mask>

描述：设置子网掩码。

根据网络的实际子网掩码填写。

Chapter 7 串口转WiFi网桥/透明串口模式 (SerialNET Mode)

模块在进入透明串口模式(SerialNET Mode)后，在重新上电后还会自动进入透明串口模式模式，并且会作为客户端自动连接已设定的服务器地址（HSRV），或者作为服务器自动建立侦听端口（LPRT）。然后将串口输入的字符发送到已建立的Socket。这样的话可以最小程度的减少对主机程序的更改，实现即擦即用（plug-and-play）。

借助本设备的串口转WIFI联网能力，现有设备无需任何更改就可以直接将现有的串口通讯切换为无线通讯，而且可以实现一个服务器设备对所有串口设备的管理。

根据透明串口模式的实现原理，我们需要事先设定好设备的串口通讯格式，数据的触发方式，相通讯的Socket信息，以及一些细节设置。

所需配置的参数分别为：

串口通讯格式：SNSI, HIF

数据触发方式：FCHR, MCBF, MTTF

相通讯的Socket信息：HSRV, LPRT

通讯协议选择：STYP

透明串口模式进入指令：SNMD

退出串口模式进入指令：+++

其它参数：HSS, MBTB, IATO.....

FCHR/MCBF/MTTF 三个指令都与缓冲区有关系，从三个角度（字符/长度/时间）来确定清空发送缓冲区（也就是发送）的时机。三个参数可以单一使用，三个参数也共同起作用。具体使用方法应参照具体应用。而且需要说明的是，这3个命令都是只对串口过来的数据起作用。特别是FCHR，只有串口发送的FCHR才会起作用。三个参数要根据实际使用环境进行搭配使用。

DSTR需要和Escape Sequence (+++)相区分，模块在接收到DSTR时，只会断开当前的socket链接，而不会退出透明串口模式，在再次上电时还会正常建立链接。但是模块在接收到Escape Sequence (+++)时，模块便直接退出透明串口模式。

在进入透明传输格式后，所有从串口输入的数据都将会被发送到所建立Socket，如果需要更改设备的配置参数，需要先退出透明传输，然后再进行相关配置。

退出透明传输模式的方法：

使用ESC sequence (+++)，即在串口输入+++字符（前后分别有500毫秒的间隔）；按住MSEL键5秒钟（即使MSEL按键保持5秒低电平）。

退出SerialNET模式后，设备会返回AT+i指令模式

7.1 +i[!/]SNMD—进入透明串口模式 (SerialNET Mode)

格式: AT+i[!/@]SNMD

描述: AT+i!SNMD

可选自动连接模式。进入此模式后, 设备立即上网时激活SerialNET模式 (即使串行数据尚未抵达)。如果LPRT (侦听端口) 参数已定义, 设备打开侦听端口, 并等待连接。如果LPRT没有界定, 但HSRV (服务器地址) 被定义, 设备立即打开一个Socket连接到服务器。

AT+i@SNMD

任择递延连接模式。进入此模式后, 设备自动上线。如果HSRV参数被定义, 串行端口有数据到达前socket不会打开。如果SerialNET模式侦听端口被定义 (LPRT), 设备在等待远程连接的数据到达本地串口之前会打开一个侦听套接字。

如果socket类型 (STYP) 是TCP, 并且有串行数据到达时, 设备会将数据暂时保存在MBTB缓冲区, 并尝试连接到HSR0。如果HSR0没有回应, 设备尝试HSR1, 然后HSR2如果所有三个都连接失败, 重试, 经过三轮尝试后。设备丢弃MBTB缓冲区中的数据并保持闲置, 直到新的串行数据到达。

7.2 +iHSRV | +iHSRn —透明串口模式的服务器地址 (Host Server Name/IP)

格式: AT+i{HSRV | HSRn} = server_name:port

描述: 设置设备在透明串口模式下所要连接的服务器地址。

n=0~2, 可以设定三个服务器地址与相应的端口。

在SNMD模式下, 设备会尝试按0~2的顺序去连接这三个服务器, 只到其中一个服务器响应连接请求, 停止尝试然后与此服务器地址建立链接。

At+iHSRV=server_name:port 和 At+iHSR0=server_name:port等效。

7.3 +iHSS —透明串口模式特殊控制字符 (Assign Special Characters to Hosts)

格式: AT+iHSS= <control_characters>

描述: 透明串口模式下, 如果设备当前连接到了HSRn (其中n = 0 .. 2), 但如果接收到有从主机发过来的字符<Cm> (如HSS=<C1> <C2> <C3>), 就会关闭与远端服务器HSRn的连接, 并发送所有先前从此服务器收到的字符, 并建立一个面向远端服务器HSRm的socket, 但是如果n=m的话, 设备不会做任何动作。在任何情况下, 这个控制字符不会被发送到远端服务器。设备不会执行软件复位, 并存储所有从服务器接收的字符到MBTB(如果设定的话)。此外, 在这种情况下, SNRD参数没有任何影响。

例如: at+ihss=\x23\x24\x00

当接收到从主机发过来的字符“#” (ASCII 023 in hexadecimal notation), 设备会把socket通讯切换到(HSR0)。以此类推, 接收到字符“\$”, 切换到HSR1.....。

7.4 +iLPRT —透明传输模式下的侦听地址 (SerialNET Device Listening Port)

格式: AT+iLPRT=<n>

描述: 设定透明传输模式下模块作为服务器的侦听地址, 如果模块进入透明传输后作为服务器来进行通讯的话, 这个参数就是模块作为服务器来建立侦听的端口。(n=0-65535)

7.5 +iDSTR —透明串口模式下断开当前连接 (Disconnect for SerialNET Mode)

格式: AT+iDSTR:<disconnect_string>

描述: 透明串口的模式下, 如果串口收到这个断开字符的话, 会断开当前的连接链路, 但是仍工作在透明串口模式下。

7.6 +iMBTB —透明传输模式下的缓冲区最大字节数 (Max Bytes To Buffer)

格式: AT+iMBTB=n (0-2048)

描述: 设定这个缓冲区的大小。

一旦socket连接建立, 设备就会传输在建立连接的这段时期所收集的字符(之前被保存在MBTB缓冲区中)。MBTB参数就是设定这个缓冲区的大小, 也就是能缓冲的最大字节数。如果串行端口建立连接之前收到额外的字节, 它们将被丢弃。

7.7 +iFCHR —透明串口模式下的特定缓冲字符 (Flush Character)

格式: AT+iFCHR=<flush_chr>

描述: 设定发送缓冲区的缓冲字符, 每当遇到这个字符, 所有当前缓冲区中的字符都将被发送。可以理解为发送字符。可以设置为a-z|A-Z|0-9|<hex_char> 16进制的格式为“\x<hh>”

例如: 但我们设定为*, 我们可以在我们需要发送的字符串后面嵌入一个*, 模块遇到*就会把前面的字符串发送。

7.8 +iMCBF —透明串口模式下最大缓冲字符数 (Max Characters before Flush)

格式: AT+iMCBF=<n>

描述: 设定最大缓冲区字节数, 当缓冲区的字符数到达设定值时, 就将自动缓冲。可以理解为发送缓存的池大小。

例如: 我们设定MCBF参数为30, 当从串口传送到模块的字符累计到30个字符时, 这30个字符就会一起发送。

7.9 +iMTTF —透明串口模式下的最大缓冲超时 (Max Timeout to Socket Flush)

格式: AT+iMTTF=n

描述: 设定最大缓存超时时间, 就是设定缓冲的时间, 单位(毫秒)。

当到达这个时间后, 当前缓冲区内的字符被发送。

例如: 当MTTF设定为50时, 模块将每50毫秒清空一次发送缓冲区, 也就是将发送缓冲区的字符全部发送出去。

7.10 +iIATO —透明串口模式的通讯中断超时 (Inactivity Timeout)

格式: AT+iIATO=<n>

描述: 设置设备的通讯中断超时, <n> = 0 .. 65535, 单位: 秒。

如果设备在<n>秒内没有数据通讯的话, 设备会断开当前的链接, 然后根据所设置的HSRV参数与LPRT参数的情况重新上线并建立链接。超时在设备打开侦听端口后开始计时, 超时后就会断开当前的socket连接, 然后尝试重新连接。当Web server被激活(AWS=1), 外部设备对模块访问也会重启IATO超时计时。

例如: IATO参数设定为20, 透明传输过程中, 如果20秒内没有数据交换, 就将断开当前连接, 重新尝试建立侦听。

7.11 +iSNSI — 透明串口模式的串口通讯格式 (SerialNET Device Serial Interface)

格式: AT+iSNSI=<settings_str>

描述: 设置设备在透明串口模式下的数据传输格式。

<settings_str> = "<baud>,<data_bits>,<parity>,<stop_bits>,<flow>

其中: <baud> = 0..9 or h

<data_bits> = 7 | 8

<parity> = N | E | O

<stop_bits> = 1

<flow> = 0 | 1

波特率和<baud>参数对应关系如下:

<baud>	波特率	<baud>	波特率
1	600	6	19200
2	1200	7	38400
3	2400	8	57600
4	4800	9	115200
5	9600	h	230,400

建议和AT指令模式的波特率(BDRF)设定一致。

默认值: 5,8,n,1,0

7.12 +iSTYP — 透明串口模式的通讯协议 (SerialNET Device Socket Type)

格式: AT+iSTYP=<v>

描述: 设置在透明串口模式下的通讯协议类型。

<v> =0 TCP协议,

<v> =1 UDP协议。

默认值: 0 (TCP)

7.13 +iSNRD — 透明串口模式的初始化延迟 (Device Re-Initialization Delay)

格式: AT+iSNRD=<n>

描述: 设定SerialNET模式重新初始化延迟时间。单位(秒)允许设定值(0-3600)

进入透明串口模式后, 在这个时间段内, 模块不会进行初始化。这段时间后, 模块才会进行自身的初始化, 然后才会视透明串口模式的不同模式建立通讯链接。

7.14 +iHIF — 主机接口(Host Interface)

格式: AT+iHIF=1

描述: 设定主机通讯接口, SerialNET Mode下需要设定和主机通讯的接口。

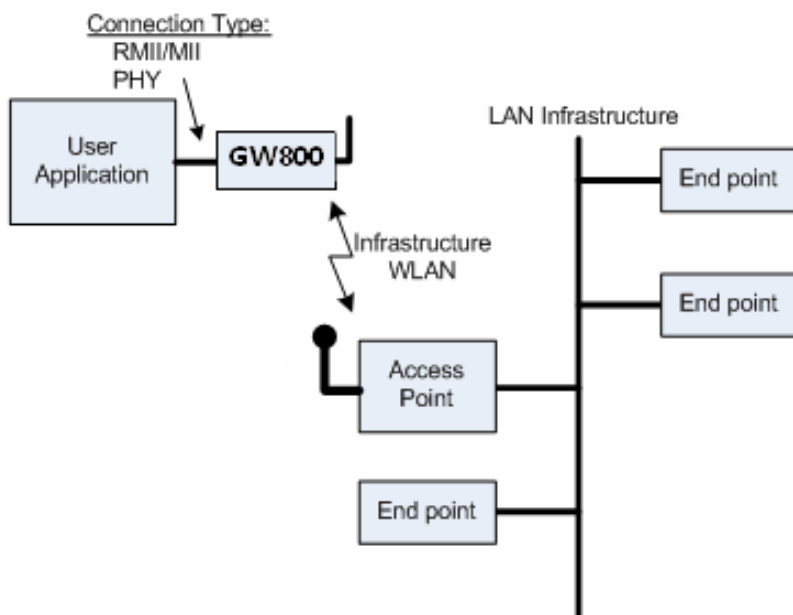
设定为1, 代表以串口0进行通讯。

透明串口模式设置必须设置这个参数。

Chapter 8 LAN转WiFi网桥 (Lan to WiFi Bridge Mode)

LAN to WiFi Bridge模式，传统以太网接口可以作为主机接口。也就意味着传统的以太网接口连接网络的设备都可以借助GW800系列（GW830）的无线网络接入能力来进行WiFi的无线数据传输。

下图中的是应用的网络拓扑，可以根据这张图找到GW800系列(GW830)在这种应用中的应用位置：



指令方面需要通过串口设定，但是只要不退出这种模式，再次上电后还是在LAN to WiFi Bridge 模式下，不用每次上电都重新设定。

LAN to WiFi Bridge模式切换指令：

格式: AT+iBRM=<n>

描述: LAN to WiFi Bridge模式切换指令n=0, 2

n=0 不使用LAN to WiFi Bridge模式;

n=1 Cable replacement PHY to WIFI ADHOC mode

n=2 使用LAN to WiFi Bridge模式

默认: <n>=0

相关设置步骤如下：

1, 首先需要将设备模块的主机端口设置为COM0,波特率设置为固定的波特率。

相关设置如下：

AT+iHIF=1 // 设置COM0为HOST通讯端口

AT+iBDRF=n // 设置COM0的通讯波特率，

注：此步骤不是可选操作，而是必要的操作步骤。否则模式工作会不稳定，虽然串口在设定完成后可悬空。

2, 设置WiFi (WIRELESS LAN) 相关的各项参数:

```
AT+iWLSI=**** // 设置SSID,如不确定可不设, 设备会自动接入与下列
                加密方式一致的AP。
AT+iWST0=n // 设置加密方式
              n=0 No security
              n=1 WEP-64
              n=2 WEP-128
              n=3 WPA-TKIP
              n=4 WPA2-AES
AT+iWLPP=***** // 设定WPA/WPA2加密密钥。
AT+iWLK1=***** // 设定WWEK加密密钥。
```

3, 进入LAN to WiFi Bridge模式需要使用+iBRM指令, 指令说明如下:

```
AT+iBRM =n //n=0 Bridge mode disable
            n=2 PHY LAN to WiFi AP mode
```

我们当前使用的多数是AT+iBRM=2,也即 LAN to WiFi AP mode, 也就是通过原有设备的网线来连接或者是PHY层来连接设备模块的方式来介入WiFi。

4, 重新对设备上电后, 模块的LAN to WiFi Bridge模式被正式激活; 连接设备模块的以太网连接会在连接成功建立的时候得到属于本地IP网段的IP地址, 此时可以借用设备的WiFi接入能力来进行通讯 (这时的RF_LED指示灯应该长亮)

在此模式下, 设备会以借助以太网端的MAC去连接网络, 所有以前的应用都可直接应用。如果需要固定的IP地址, 直接在以太网端设置IP地址即可。

Chapter 9 多Socket通讯模式 (Direct Socket Interface)

AT+i 指令模式可以实现多Socket通讯模式，可以实现更为灵活的应用；可以实现最多10个同时的Socket，其中两个可以分配为侦听的Socket使用，并可根据需要自由分配端口使用。

本章节使用频率较高的符号：

<host>：目标服务器的逻辑名称或主机的IP地址。
 <port>：目标端口
 <lport>：设备上的本地可选端口
 <rport>：设备上的远程可选端口
 <sock handle>：一个套接字句柄
 <backlog>：设定通过监听套接字建立的活跃的最大同时连接数
 <hn>：一个打开的监听套接字的一个TCP监听套接字句柄
 <sz>：其后的字节流的具体大小
 <stream>：字节流

9.1 +ISTCP — 打开并连接一个TCP Socket (Open 和 Connect a TCP Socket)

格式：AT+iSTCP:<host>,<port>[,<lport>]

描述：此命令会使目前的设备作为TCP/IP的客户端去连接已建立侦听的服务器Socket。<host> 服务器名可以是任何合法的Internet服务器名，它可以被Internet控制器的DNS（域名服务器）解析。服务器名也可以设定为DOT表格中指定的绝对IP地址。<port> 假定服务器系统正在“监听”某个端口。<lport> 可能需要设定以强制设备使用lport作为本地端口，当打开TCP套接口的时候。如果尚未设定，设备将从它自己内部池1中分配一个端口。

参数：<host> =目标服务器的逻辑名称或主机的IP地址。

<port> = 0..65535，目标端口

<lport> = 设备上的本地可选端口。

结果代码：l/<sock handle> 成功打开TCP端口并将它连接到<host>:<port>之后将返回一个套接字句柄。套接字句柄<sock handle>的适用范围是从0到9，并用于在后面所述套接字命令中引用这些套接字。

9.2 +ISUDP — 打开并连接一个UDP Socket (A UDP SOCKET)

格式：AT+iSUDP:<host>,<rport>[,<lport>]

描述：<host>远程系统名可以是任何合法的Internet服务器名，它可以被Internet控制器的DNS（域名服务器）解析。服务器名称也可以设置为DOT表格中指定的绝对IP地址。当设定<host>之后，将创建并连接一个UDP套接字。如果<host>='0.0.0.0'，创建的套接字将保持无连接。第一个到达的UDP信息包将自动锁定发送一方的IP端口，有效连接套接字。<rport> 设定远程系统端口。<lport> 设定要使用的本地端口。如果尚未设定，设备将从它的内部池中分配一个端口。

参数：<host> =目标服务器逻辑名称或主机IP地址。或0.0.0.0以打开一个无连接的套接字。

<rport> = 发送到的远程端口号。或0打开一个无连接套接字。

<lport> = 使用的可选择的本地UDP端口。

结果代码： I/<sock handle> 成功打开TCP端口并将它连接到<host>:<port>之后将返回一个套接字句柄。套接字句柄<sock handle>的适用范围是从0到9，并用于在后面所述套接字命令中引用这些套接字。

9.3 +iLTCP — 打开一个TCP侦听Socket (Open a TCP Listening Socket)

格式： AT+iLTCP:<port>,<backlog>

描述： <port> 在连接到设备上时远程系统使用的监听端口。<backlog> 设定通过监听套接字建立的活跃的最大同时连接数。一旦监听套接字打开，它将自动接受远程系统的连接请求，直到达到所允许的最大数目。当一个远程系统通过监听套接字建立连接的时候，在内部将产生一个新的TCP套接字，并且准备接收和发送数据。参阅AT+iLSST命令以获取有关重新获取通过监听套接字连接的活跃套接字的句柄的详细信息。当连接套接字关闭的时候，监听套接字将允许新的连接代替它。

参数： <backlog>设定允许同时通过监听套接字的远程连接的最大数目。

<port> = 0..65535 <backlog> = 1..10

结果代码： I/<sock handle> 在成功打开一个TCP监听套接字后，将返回一个套接字句柄。该套接字句柄<sock handle>范围是10..11并用于在后面的所有套接字命令中引用该套接字。

9.4 +iLSST — 获取一个监听端口的状态 (Get a Listening Socket Active Connection Status)

格式： AT+iLSST:<hn>

描述： 重新获取通过<hn>设定的套接字建立的活跃的套接字连接的句柄。<hn> 在当前Internet会话期间必须被前一个AT+iLTCP命令所获取。

参数： <hn> = 一个打开的监听套接字的一个TCP监听套接字句柄。

结果代码： I/ (<hn1>,... ,<hnBacklog>) 活跃套接字句柄列表。该列表包括所有<backlog>元素。<backlog>用于在打开<hn>识别的监听套接字之时。<hni> >= 0: 活跃的连接套接字句柄。= -1: 无连接建立。如果返回 I/ERROR 如果<hn>不是一个打开的监听套接字，或出现其他错误。

9.5 +iSST — 获取一个监听端口的连接状态 (Get a Single Socket Status Report)

格式： : AT+iSST:<hn>

描述： 重新获取一个单个套接字的状态报告。它是AT+iRP4报告命令的子集。<hn> 必须在当前Internet模式会话期间被前一个AT+iSTCP或AT+iSUDP命令获取。或一个被监听套接字接受的套接字。

参数： <hn> = 一个TCP/UDP套接字句柄。

结果代码： I/ (<sockstat>) 其中， <sockstat> >= 0: 套接字<hn>的输入缓冲中未决字节数< 0: 套接字错误代码。

9.6 +iSCS — 获取一个套接字状态报告 (Get a Socket Connection Status Report)

格式： AT+iSCS:<hn>

描述： 重新获取一个套接字<hn>的连接状态报告。<hn>必须在当前Internet模式会话期间被前一个AT+iSTCP或AT+iSUDP命令获取。或一个被监听套接字

接受的套接字。

参数: <hn> = A TCP/UDP 套接字句柄。

结果代码: I/ (<sockstat>) 其中, <sockstat> = 000: 套接字被连接并且没有出现相关错误。 < 0: 套接字错误代码。

9.7 +ISSND[%] — Socket发送指令 (SEND A BYTE STREAM TO A SOCKET)

格式: AT+ISSND[%]:<hn>,<sz>:<stream>

描述: 向套接字句柄<hn>指定的套接字发送一个<sz>大小的字节流。

<hn>必须在当前Internet模式会话期间被前一个AT+iSTCP或AT+iSUDP命令获取。或一个被监听套接字接受的套接字。 <sz> 0..4GB.<stream> 一个8位<sz>大小的字节流。

'%'标记当自动刷新 ('%') 标记被设定的时候, 套接字在接收到<stream>后立即自动刷新。否则, 数据将只在达到指定MTU (最大传输单元) 的量或者当发出AT+iSFSH命令的时候才被传输到Internet上。

参数: <hn> = 一个打开的套接字的TCP/UDP套接字句柄。

<sz> = 其后的字节流的具体大小。

<stream> = 发送给指定套接字的<sz>大小的字节流。

结果代码: I/OK 在<sz>大小的字节被成功传送到套接字的输出缓冲之后。

9.8 +ISRCV — Socket接收指令 (Receive a String from a Socket's Input Buffer)

格式: AT+ISRCV:<hn>[,<max>]

描述: 从套接字句柄<hn>指定的TCP/UDP套接字接收字节流。只有当在发出该命令的时候接收数据已经存在于Internet控制器的套接字输入缓冲中, 该数据才是有效的。 <hn>必须在当前Internet模式会话期间被前一个AT+iSTCP或AT+iSUDP命令获取。或一个被监听套接字接受的套接字。 <max> 如果<max>尚未设定, 所有存在于套接字输入缓冲中的可用字节都将被返回。

参数: <hn> = 一个打开的套接字的TCP/UDP套接字句柄。

<max> = 可选择地设定要传输的最大字节。执行本命令之后多余字节将停留在套接字输入缓冲中。

结果代码: I/ERROR 如果<hn>不是一个打开的套接字。否则是出现了错误。

I/<sz>[:<binary data stream>] 其中, <sz>是二进制数据流的准确大小。

如果套接字输入缓冲是空的, 设备将返回I/0。在这种情况下 ':'和<binary data stream>被忽略。在进行设定时, 确保<sz>等于或小于<max>。

9.9 +IGPNM — 为一个指定的套接字获取对等机名 (Get Peer name for a Specified Socket)

格式: AT+IGPNM:<hn>

描述: 重新获得一个连接到套接字句柄<hn>指定的TCP/UDP套接字上的远程连接的对等机名 (<IP>:<Port>)。 <hn>必须在当前Internet模式会话期间被前一个AT+iSTCP或AT+iSUDP命令获取。或一个被监听套接字接受的套接字。

参数: <hn> = 一个打开的套接字的TCP/UDP套接字句柄。

结果代码: I/ (<IP>:<Port>) 其中, <IP>是远程对等的IP地址, 而<Port>是该连接远程对等的端口。

9.10 +ISDMP — 转储套接字缓冲 (DUMP SOCKET BUFFER)

格式: AT+ISDMP:<hn>

描述: 转储当前套接字的输入缓冲当中积累的所有缓冲数据。

Chapter 10 节能模式 (Power Save Mode)

节能模式下可最大限度的减少功耗，适合手持设备等需要电池供电的设备使用。

10.1 +IPSE 节能模式进入指令 (Power Save Mode)

格式：at+IPSE=<n> 描述：本指令设置设备是否进入休眠模式。

如果n等于0，设备的Power Save Mode不启动；

如果n等于1-255间的任意值，则设备等待n秒，如果在n秒钟没有任何的数据通讯，则设备会进入Power Save Mode，此模式下设备会关闭大部分电路，只到串口部分侦测到有活动（命令活动，TX,RX皆可），然后设备会恢复为全速的数据通讯模式。

10.2 +iWLPS — 节能模式设置 (Wireless LAN Power Save)

格式：at+iWLPS=<m>

描述：设置Power Save Mode下的 Beacon period的数量（1~5）。

Beacon period的时间长度一般由AP或者是ad-hoc网络的发起者决定，典型值为100毫秒。

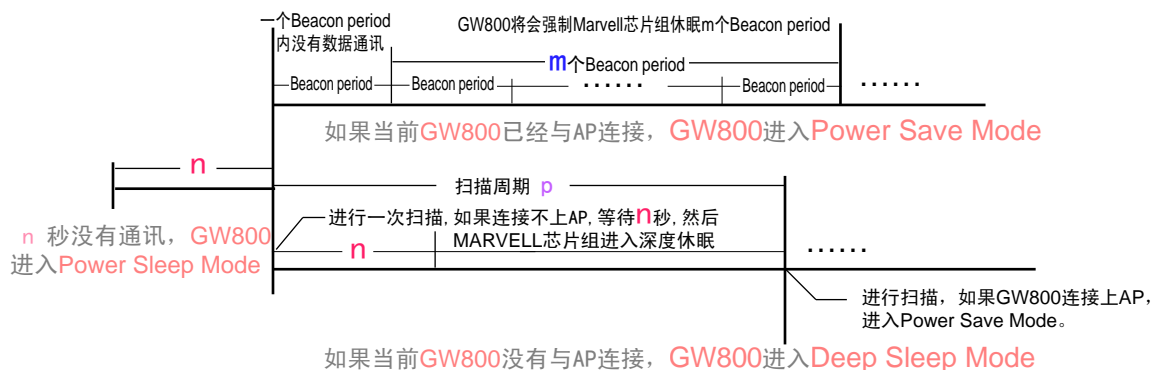
这个参数设置为0的话，设备将不启动MARVELL芯片组的Power Save Mode，但如果WLPS参数设置为1~5的话，设备将会根据与AP的连接情况来判断强制MARVELL芯片组进入Power Save Mode或者是Deep Sleep Mode；如果在进入休眠模式时，设备已经与AP建立了连接，则设备会强制MARVELL芯片组进入Power Save Mode，此模式下，如果在一个Beacon period内没有数据通讯的话，MARVELL芯片组将会休眠m个Beacon period长度的时间。这样的不断循环，一旦串口端有数据，设备会强制MARVELL芯片组恢复为全速的数据通讯模式。

如果在进入休眠模式时，设备没有与AP建立了连接，则设备会强制MARVELL芯片组进入Deep Sleep Mode。此模式下，设备将会让MARVELL芯片组定时p秒（WPSI指定）扫描周围存在的AP，没有连接到的AP的话，设备会等待n秒，然后设备会强制MARVELL芯片组休眠，下一个扫描周期重新扫描。一旦设备连接到AP，则设备会强制MARVELL芯片组进入Power Save Mode。

10.3 +iWPSI — 网络扫描扫描时间(Periodic WiFi Scan Interval)

格式：at+iWPSI=<p>

描述：设置在设备没有与AP建立连接时，MARVELL芯片组定时扫描的时间值，有效值：0~3600,单位：秒。



Chapter 11 漫游模式 (Roaming Mode)

11.1 +iWROM — 漫游模式 (Enable Roaming in WiFi)

格式: AT+iWROM=<n>

描述: 漫游模式的打开/关闭指令

<n>=0 关闭漫游模式

<n>=1 打开漫游模式

默认值: <n>=0

11.2 +iWPSI — 无线扫描周期 (Periodic WiFi Scan Interval)

格式: AT+iWPSI=<n>

描述: 设定设备无线扫描周围AP的周期, 单位: 秒。

<n>可以设置为1-3600 seconds

默认值: <n>=5 seconds

11.3 +iWSRL — 设定漫游模式的通讯最低SNR (SNR Low Threshold)

格式: AT+iWSRL=<n>

描述: 设定在漫游模式时设备通讯的最低信噪比 (SNR) 值。如果目前设备与AP通讯的信噪比低于此参数, 设备主动断开当前的链路。

<n>=0-255 dB

默认值: <n>=10 dB

11.4 +iWSRH — 设定漫游模式建链的最低SNR (SNR High Threshold)

格式: AT+iWSRH=<n>

描述: 设置漫游模式时设备建立通讯信噪比的门槛。设备将只与信噪比比<n>更高的接入点进行通讯。

<n>=0-255 dB

默认值: <n>=30 dB

11.5 +iWSIn — 漫游模式的SSID列表 (Wireless LAN Service Set Identifier Array)

格式: AT+iWSI<n>=<ssid>

描述: 设置为位置n的无线网络服务设置标识符 (SSID)

设备会按照<n>的持续尝试连接一个AP或Ad-hoc网络。

<n>=0-9, 只设置<n>=0时, WSI0参数与WLSI参数等效。

<n>=1-9, 设置为一个列表, 设备会逐个尝试与列表中的<SSID>建立通讯链路。该SSID的配置必须连续。

例如, 如果WSI0和WSI2设置, 但WSI1没有, 设备自动忽略WSI2。

另外: WSI0的相关设置, 如果设置WSI0为“, 则设备连接周围信号最强的AP;

如果设置WSI0为!, 则设备连接周围信号最强的AD-HOC网络;

11.6 +iWSTn — 漫游模式的各SSID加密方式 (Wireless LAN Security Type Array)

格式: AT+iWSTn=<sec>

描述: 设置<n>对应的SSID各自的加密方式。

<sec>=0 No security

<sec>=1 WEP-64

<sec>=2 WEP-128

<sec>=3 WPA-TKIP

<sec>=4 WPA2-AES

如果设置的<sec>=1或<sec>=2，则选择的是WEP加密，密码应该选择<n>对应的WKYn填写，如果设置的<sec>=3或<sec>=4，则选择的是WPA/WPA2加密，密码应该选择<n>对应的WPPn填写。

11.7 +iWPPn — 对应WSI<n>的WPA加密密码阵列 (Pre-Shared Key Passphrase Array)

格式：AT+iWPPn=<passphrase>

描述：设置WSI<n>对应的WPA加密密码阵列。

设置SSID阵列各自的WPA加密密码。

<passphrase>为8~32个字符的密码字符串。

11.8 +iWKYn — 对应WSI<n>的WEP加密密码阵列 (Wireless LAN WEP Key Array)

格式：AT+iWKYn=<KeyString>

描述：设置WSI<n>对应的WEP加密密码阵列。

设置SSID阵列各自的WEP加密密码。

WEP加密密码有两种格式：

如果AP设置的是WEP 64位加密，并采用的16进制密码（10个16进制数）。

则直接将此密码设置成WSIn对应的WKYn密码；如果AP采用的是ASCII码密码，（5个ASCII码），则需要将这5个ASCII码转换为10个16进制数设置到WKYn。

如果AP设置的是WEP 128位加密，并采用的16进制密码（26个16进制数）。

则直接将此密码设置成WSIn对应的WKYn密码；如果AP采用的是ASCII码密码，（13个ASCII码），则需要将这13个ASCII码转换为26个16进制数设置到WKYn。

Chapter 12 远程控制 (Remote Control)

该设备可以实现远程控制的功能，利用一个可进行远程连接的端口建立远程配置的通讯链路，该通讯链路建立后可以响应远程发送的AT+i指令，并能将设备所响应的结果通过该通讯链路返回通讯发起端。

LATI参数如果设置为一个非零值，设备打开一个端口<LATI>建立TCP侦听Socket。

如果已经打开此远程控制链路，即使设备此时工作在自动波特率模式下(BDRA)，但如果主机需要断开当前的远程控制链路，也只能在9600波特率下发送退出字符(+++)从而关闭远程会话。而在关闭远程会话后，设备仍然会是在BDRA模式下。

如果在该会话中使用了AT+iBDRA指令，模块会返回I/ok，但不会立即启动波特率侦测过程。

如果设备工作在透明串口模式下，无法启动此远程控制会话。

+iLATI — 远程控制会话侦听端口

格式：AT+iLATI=<port>

描述：设置设备建立远程控制会话的侦听端口。当此参数设置后，一旦设备接到互联网，设备就会打开一个本地IP地址和指定的端口(IATO)建立远程通讯的特殊链路。这条特殊的通讯链路会接受远程发来的AT+i指令，在执行此指令后，执行结果也会通过此链路返回。<LATI>=0..65535

Chapter 14 操作实例 (operation example)

设备配置信息如下:

SSID: Bocon

加密: WEP64位

密码: 1234567890

IP地址: 192.168.1.5

子网掩码: 255.255.255.0

网关: 192.168.1.1

波特率: 115200

数据触发方式: 时间触发 (20ms一个包)

服务器地址: 192.168.1.6

侦听端口: 1000

操作命令如下:

```
at+iwlsi=Bocon
I/OK
at+iwlwm=1
I/OK
at+iwlk1=1234567890
I/OK
at+idip:192.168.1.5
I/OK
at+isnet:255.255.255.0
I/OK
at+iipg:192.168.1.1
I/OK
at+isnsi="9,8,n,1,0
I/OK
at+imttf=20
I/OK
at+ihsrv:192.168.1.6:1000
I/OK
at+ihif=1
I/OK
at+!snmd
I/OK
I/ONLINE
```

附录 A 错误返回码

AT+I 错误码综述

如果出于某种原因，设备对于指令的指令出现故障的话，设备会返回一个错误码。

格式如上：I/ERROR(nnn)

其中 nnn 代表的就是设备的错误码。不同错误码对应设备发生的不同错误，可以根据不同错误码来分析出现错误的原因。

I/ERROR(nnn) 命令执行出错,被丢弃。			
41	非法的分隔符	42	非法的参数值
43	缺回车符	44	缺数字
45	缺回车符或者“,”	46	缺DNS设置
47	缺“:”或者“~”	48	缺字符串
49	缺“:”或者“=”	50	缺文本
51	语法错误	52	缺“,”
53	非法指令代码	54	参数设置错误
55	参数值获得错误	56	用户中断
57	建立PPP连接中断	58	建立SMTP连接错误
59	建立POP3连接错误	60	超过单个邮件附件的最大体积
61	内存错误	62	用户退出系统
63	~CTSH必须拉低来更换硬件流控	64	用户已通过‘---’来中断三个指令
65	保留	66	保留
67	无关指令	68	设备序列号已经存在
69	主机连接超时	70	Modem没有响应
71	没有拨号音	72	远端Modem没有响应
73	拨号失败	74	Modem与ISP连接失败 或 以太网连接失败 或 WiFi连接失败
75	ISP服务器拒绝访问	76	找不到POP3 服务器
77	POP3服务超时	78	POP3服务器拒绝访问
79	POP3 失败	80	邮箱中无所需文件
81	找不到SMTP服务	82	SMTP服务超时
83	SMTP失败	84	保留
85	保留	86	参数保存失败
87	IP地址Web server注册失败	88	IP地址Socket 注册失败
89	IP地址E-mail 注册失败	90	所有IP注册方法失败
91	保留	92	保留
93	保留	94	在永远在线模式，连接丢失和重新初始化
		96	一个通过LATI端口接管设备的远

			程主机当前被断开
		98	保留
99	保留	100	恢复默认参数错误
101	ISP号码未定义	102	用户名未定义
103	密码未定义	104	DNS未定义
105	POP3服务器未定义	106	邮箱未定义
107	MPWD邮箱密码没有定义	108	TOA未定义
109	REA未定义	110	SMTP服务器未定义
111	串口数据溢出	112	在线指令错误
113	尝试通过E-mail升级固件，但升级尚未完成，原来的固件保持完整。	114	通过电子邮件更新参数的申请被驳回
115	透明传输模式参数设置不完整	116	错误剖析一个新的值得信赖的CA证书
117	保留	118	
119	WPA密码太短，要8-63字符	120	保留
121	保留	122	透明传输错误：HIF参数未定义
123	透明传输错误:主机端口的波特率无法定义	124	SerialNET over TELNET 错误：HIF参数必须被设定为1或2
		200	Socket连接不存在
201	Socket接收为空	202	Socket不可用
203	Socket连接下线	204	非法Socket连接
		206	PPP错误
207	错误建立Socket	208	Socket发送错误
209	Socket接收错误	210	PPP错误
		212	Socket缓冲错误
215	No carrier error on socket operation	216	SMTP服务器未定义
217	内存溢出	218	STCP指定的端口已被占用
219	SSL初始化错误或者内部CA证书加载错误	220	SLL3谈判失败
221	非法的SSL套接字句柄，必须是一个已打开的套接字。	222	可信任的CA证书不存在
223	保留	224	输入的SSL数据解码错误
225	没有额外的SSL socket可用	226	超出最大SSL数据包的大小（2K）
227	AT+iSSND执行失败，因为字符串大小超过2048 bytes	228	AT+iSSND命令执行失败，因为校验和主机发出的校验不匹配
		300	HTTP服务器未知
301	HTTP服务器超时	302	HTTP失败

305	非法的HTTP端口号码	306	非法的URL地址
307	URL地址过长	308	AT+iWWW命令失败, 因为设备当前没有加载主页
		400	MAC地址已存在
401	没有得到IP地址	402	无线局域网Power设定失败
403	无线局域网Radio控制失败	404	Wireless LAN 复位失败
405	无线局域网硬件安装失败	406	因为WiFi模块当前正忙, 指令执行失败
407	非法的WiFi通道	408	非法信噪比阈值
		500	保留
501	通讯平台已激活	502	保留
503	保留	504	保留
505	无法打开额外的FTP会话-所有FTP套接字都被占用	506	不是一个FTP会话套接字
507	无法找到FTP服务器	508	连接FTP服务器超时
509	登录FTP失败	510	FTP指令无法完成
511		512	无法传输数据到FTP socket
513	FTP被远程服务器关闭	514	保留
		550	没有找到Telnet Server
551	Telnet Server连接超时	552	Telnet 命令不能被完成
553	Telnet被远程服务器关闭	554	Telnet会话目前没有激活
555	已打开了一个Telnet会话	556	Telnet服务器拒绝切换到二进制模式
557	Telnet 服务器拒绝切换到ASCII模式	558	保留
559	保留	560	客户端无法检索戒指响应电子邮件
561	SerialNET Socket被远程关闭		
		570	PING的目的地没有定义
571	PING包没有回复		