

深圳市安信可科技 无线模块专家 无敌性价比！

MT7681 无线模块成品价格：

批量价格大于500： 30元

大于5K： 28元

大于10K： 25元

以上价格只降不涨，每隔6个月降低10%

网址：<http://www.ai-thinker.com>

MT7681

802.11 b/g/n single chip

Preliminary datasheet

Version: 0.00

Release date: 2014-01-08

© 2010 - 2014 MediaTek Inc.

This document contains information that is proprietary to MediaTek Inc.

Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Specifications are subject to change without notice.



MT7681 IoT FAQ

Version: 0.02
Release date: 2014-5-17

© 2014 MediaTek Inc.

This document contains information that is proprietary to MediaTek Inc.

Unauthorized reproduction or disclosure of this information in whole or in part is strictly prohibited.

Specifications are subject to change without notice.

Revision History

Date	Revision	Author	Description
04.12.2014	First v0.01	Jinchuan	Initial draft for MT7681 IoT FAQ
05.17.2014	V0.02	Jinchuan	

mediatek Confidential

Contents

1	Source Code Compile	5
1.1	How to Setup AndeSight SDK.....	5
1.2	How to create new project in AndeSight / How to import MTK7681 SDK to AndeSight.....	5
1.3	How to compile source code for Recovery FW , Sta FW, AP FW	6
1.4	SDK编译后生成ap , sta , recovery , all等文件，哪个文件才是我最终要烧录的，	6
1.5	Compile Source Code fail -- .BSS is not within region SRAM	6
2	FW Upgrade.....	6
2.1	FW upgrade method.....	6
2.2	How to change AP mode and Station Mode.....	6
2.3	Why there is a Recovery Mode.....	7
2.4	How to set recovery mode duration.....	7
3	APK Install and usage	8
3.1	手机安装IoTManager_v0.94_1_android4.0.apk，显示是“解析包时出现问题”	8
4	System Coding	8
4.1	Printf_High() /DBGPRINTF_HIGH() 输出LOG的开关	8
4.2	flash分区里reserved的区域有没有其他特殊用途？可不可以拿来保存一些数据	8
4.3	打开 CFG_SUPPORT_TCPIP 宏使用AT命令的TCP功能。编译时出现错误.....	9
4.4	为什么使用IoT_gpio_output() 设定某个GPIO为 1 后，一会后莫名其妙又被拉低	9
5	Connection Development.....	9
5.1	MT7681 Support mode 和Bandwidth	9
5.2	一般 C程式有entry point,即main(), 請問一個IoT application 的entry point在哪裡?.....	9
5.3	How to get mt7681 MAC address.....	9
5.4	在sta模式下连接ap，但是我要怎么来判断连接成功与否？？？	10
5.5	如何自动获取IP，是通过uip中的dhcpc相关函数吗？？？	10
5.6	如何進行SW reset. 將IP/SSID 等參數 reset成出廠設定值	10

5.7	现在的 1.10 版本好像没有mem_alloc及mem_free函数	11
5.8	结构体_WIFI_STATE的说明性文档，每个状态代表什么意义	11
5.9	Smart Connection的station config数据结构	11
5.10	Smart Connection的(station config)数据存取及清除	12
5.11	使用宏 CFG_SUPPORT_MTK_SMNT=1 来控制是否使用 MTK的smart connection	12
5.12	How to get PMK	13
6	Application Development.....	14
6.1	How to send TCP/UDP packet.....	14
6.2	IoT application內要scan AP, 連到AP, 建TCP + SSL ...等,要参考哪些 APIs document?.....	14
6.3	数据从服务器转发到 7681，数据包格式是怎样的，经过解包之后是怎样的数据类型？	14
6.4	SDK中有TCP和UDP两种方式， UDP/TCP是什么情况下使用的呢？	14
6.5	MT7681 透过AP Router与Internet Server，请问这个Internet Server做"转发"作用外，还有哪些作用呢？	15
6.6	是否有获取网络时间的协议Support SNTP, NTP	15
6.7	Set up the TCP connection on MT7681	15
6.8	Cannot use AT Cmd "Netmode ,Channel, SoftAPConf and TCP_Connect "	16

1 SOURCE CODE COMPILE

1.1 How to Setup AndeSight SDK

Refer to the document: MTK_AndesToolChains_Usage_v0.0*_*****.pdf

Q1: AndeSight IDE 我 download 的版本是: Andestech\AndeSight201MCU , 你们文档中提到要用版本 C:\Andestech\AndeSight14\, 是不是有问题?

A1: 没有问题, 只是我们在准备文档的时候 还是用的 1.4 的 AndeSight,

您 download 的是最新的 2.01 版本, 我们有实验过, 配置方法同 1.4 一样, 所以文档没有再做更新

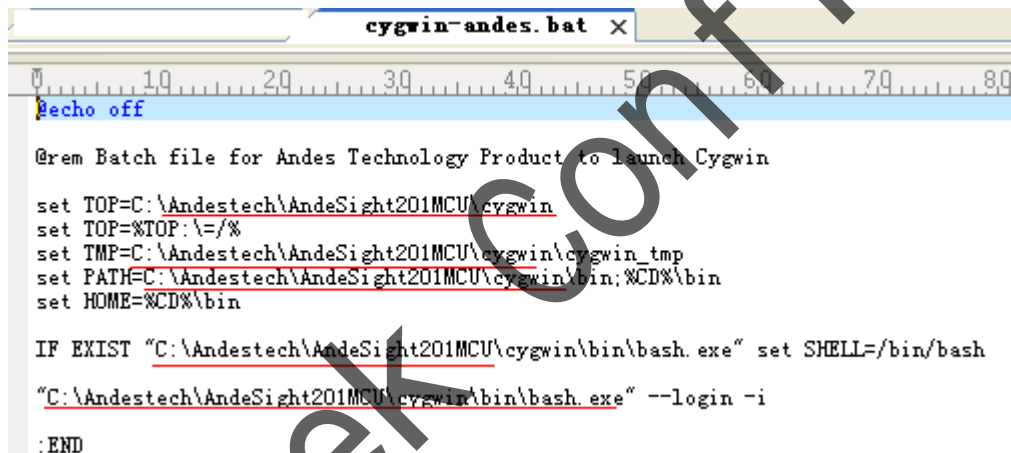
Q2: 按照文档《MTK_AndesToolChains_Usage_20140212.pdf》的方法用 MTK 的“nds32le-elf-newlib-v2j”替换了原始的 toolchain, 启动后马上退出, 没有打开窗口。

A2: 这里先了解下, 您实验的操作系统是 win7 还是 XP ?

在 XP 32bit OS 上 安装了 AndeSight201MCU 是 OK 的, (有人员在 Win7 64bit OS 中也有安装成功) 使用默认的安装路径 C:\Andestech\AndeSight201MCU\toolchains

下图是我修改后的 cygwin-andes.bat 档, 如果您的安装路径 以及 Toolchain 替换路径 同我一样 可以将如下路径的 bat 中 的红色底线位置改成和我一样。

C:\Andestech\AndeSight201MCU\toolchains\nds32le-elf-newlib-v2j



```
@rem Batch file for Andes Technology Product to launch Cygwin

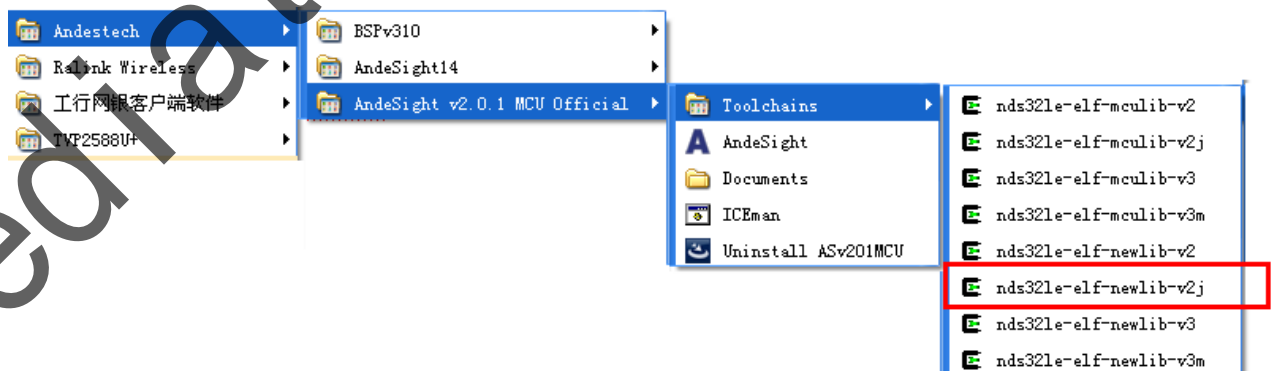
set TOP=C:\Andestech\AndeSight201MCU\cygwin
set TOP=%TOP:\/=%
set TMP=C:\Andestech\AndeSight201MCU\cygwin\cygwin_tmp
set PATH=C:\Andestech\AndeSight201MCU\cygwin\bin;%CD%\bin
set HOME=%CD%\bin

IF EXIST "C:\Andestech\AndeSight201MCU\cygwin\bin\bash.exe" set SHELL=/bin/bash

"C:\Andestech\AndeSight201MCU\cygwin\bin\bash.exe" --login -i

:END
```

然后点击 红色方框的连接 启动即可。



1.2 How to create new project in AndeSight / How to import MTK7681 SDK to AndeSight

AndeSight SDK 我现在也只是 使用它的 Cygwin 环境, 并未使用它来 Create new project 。

Create new project 我还是通过 source insight 这些 tool 来创建

1.3 How to compile source code for Recovery FW , Sta FW, AP FW

```
make b=0 clean;make b=0    -> create  recovery bin
make b=1 clean;make b=1    -> create  sta bin
make b=2 clean;make b=2    -> create  ap bin
```

1.4 SDK编译后生成ap, sta, recovery, all等文件, 哪个文件才是我最终要烧录的,

MT7681_IoT_Package_v1.10\Src 中 Readme-ForEachBinDescript.xlsx 文件会介绍产生出的 binary 关系

编译后 会 生成: MT7681_sta.bin, MT7681_recovery_old.bin, MT7681_ap.bin ,
这些文件会再加上(loader_0322_94973.bin, MT7681E2_EEPROM layout_20140330.bin)
按照 Flash layout 中指定的位置 生成 MT7681_all.bin

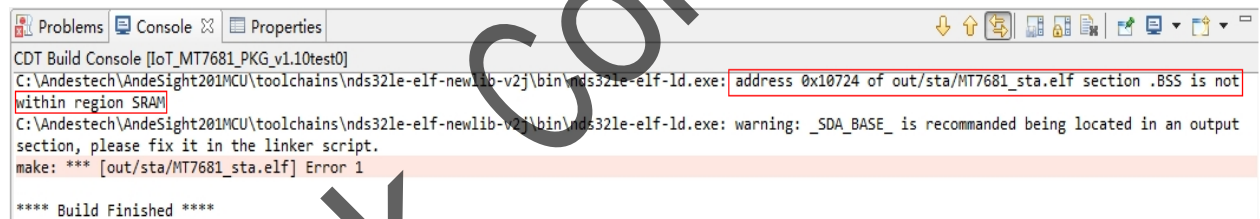
MT7681_all.bin 就是我们通过 flash 烧录器 进行整个 flash 烧录的程序

编译后还会生成: MT7681_recovery_header.bin, MT7681_sta_header.bin, MT7681_ap_header.bin
另外 Package 中 有我手动对 loader 和 Recovery 的 binary 加上 header,

生成的 loader_header_0322_94973.bin, MT7681_recovery_header.bin
这些文件是 用于 Uart FW upgrade 的,
具体 Uart 升级方法, 以及 *_Header_*.bin 与*.bin 的 差异
在 MT7681_IoT_Package_v1.10\Doc\MT7681_Uart_Firmware_Upgrade_v0.0*_*****.pdf 有描述

1.5 Compile Source Code fail -- .BSS is not within region SRAM

这个表明当前程序 已经超过 ram 的大小



```
CDT Build Console [IoT_MT7681_PKG_v1.10test0]
C:\Andestech\AndeSight201MCU\toolchains\nds32le-elf-newlib-v2j\bin\nds32le-elf-lld.exe: address 0x10724 of out/sta/MT7681_sta.elf section .BSS is not
within region SRAM
C:\Andestech\AndeSight201MCU\toolchains\nds32le-elf-newlib-v2j\bin\nds32le-elf-lld.exe: warning: _SDA_BASE_ is recommended being located in an output
section, please fix it in the linker script.
make: *** [out/sta/MT7681_sta.elf] Error 1

**** Build Finished ****
```

以 Package v1.10 的 SDK 来看

在默认的 flag_sta.mk (for Station mode) 功能配置下, 可供使用的 memory 大小为 11KB

在默认的 flag_ap.mk (for AP mode)功能配置下, 可供使用的 memory 大小为 13KB

2 FW UPGRADE

2.1 FW upgrade method

1: FW upgrade by Flash Writer

2: FW upgrade by Uart

Just like descript in “1.4”, 也请先阅读MT7681_Uart_Firmware_Upgrade_v0.0*_*****.pdf

- Not support FOTA yet, 客户可通过现有 API 开发

2.2 How to change AP mode and Station Mode

通过 AT#FLASH -s98305 -v* 命令, 修改 Flash Offset: 0x18001 的值, 再关开机即可实现 AP/STA 切换
[0x18001]=[0x00] → 表示 Boot as STA mode,
[0x18001]=[0x01] → 表示 Boot as AP mode

Example: AP Mode 的切换比较简单, 就是修改 Flash Offset: 0x18001 的值为 1

Step1: 通过 Flash Writer 烧录 MT7681_all_v1.10.bin 到 Flash

Step2: 开机后显示 如下信息, 表示进入到 STA Mode

==> Recovery Mode

<== RecoveryMode

(-)

SM=0, Sub=0

SM=1, Sub=0

[WTask]9811

Step3: 可通过 AT#Flash 命令读取 0x18001 位置的 BootIndex 值 double Check

AT#FLASH -r98305

[0x18001]=[0x00] → 表示 Boot as STA mode, 如为[0x18001]=[0x01]表示 Boot as AP mode

Step4: 通过 AT#Flash 命令修改 0x18001 位置的 BootIndex 值 为 1

AT#FLASH -s98305 -v1

Step5: 7681 重新上电后, 会以 AP mode 方式启动,

SSID name 为“MT7681_Softap”, 只 Support Open Mode

==> Recovery Mode

<== RecoveryMode

(-)

APStartUp ok

Start AP ...

[WTask]9318

[WTask]14322

如果此时有手机连接上来, 会显示如下连线信息

Assoc request sanity success

i = 5, j = 0

client ip addr: 192.168.81.2

[WTask]39372

2.3 Why there is a Recovery Mode

主要目的是用于 Uart FW Upgrade 和 Production Calibration

上电/重启后会自动进入到 Recovery Mode, 并停留 4s (default), 在这 4s 内 通过 Uart 输入

AT#UpdateFW → 会启动 Uart FW upgrade Process, 通过 xmodem 进行 FW 升级

AT#ATECAL -S → 会进入 Calibration Mode, 进行 Tx/Rx 的 Calibration

我们需考量到 STA FW 如果更新失败, 系统如何恢复, 此时 Recovery Mode 的存在就比较关键

Recovery Mode 的 4s 等待时间, 是考虑到目前 HDK v1.0 不能接上 Uart Rx 开机, 所以上电后, 暂时保留足够的时间让 开发者可以输入 AT#UpdateFW 等命令

这 4s 的时间是可以调整的, 如 2.4

2.4 How to set recovery mode duration

现在 recovery 模式下, 如果不做任何操作, 会在 4s 后 自动跳出 recovery 模式

这个 4s 的时间 在 v1.2 SDK 中可以由 通过设定变量 来控制


```

[!ot_custom.c (src\api)]
ew Window Help
00111: /*Default setting of STA Config Block*/
00112:
00113: /*Default setting of AP Config Block*/
00114:
00115:
00116: /*bit0- read Calibration settings (TxPower/Tx Freq Offset) from [0:Flash, 1:Efuse]*/
00117: UINT8 gCaliFrEfuse = 0x00;
00118:
00119:
00120: /*unit:ms indicated recovery mode duration*/
00121: #if (ATCMD_RECOVERY_SUPPORT==1)
00122: UINT16 gRecoveryModeTime = 4000;
00123: #endif
00124:

```

3 APK INSTALL AND USAGE

3.1 手机安装IoTManager_v0.94_1_android4.0.apk，显示是“解析包时出现问题”

IoTManager_v0.94_1_android4.0.apk 是 for Android 4.0 及以上的手机 都可以
很可能出现问题的手机不是 android4.0 及以上的版本

APK 的 SourceCode 也有放在 Package v1.10 中， 您也可自己编译出对应的 APK for demo

4 SYSTEM CODING

4.1 Printf_High() /DBGPRINTF_HIGH() 输出LOG的开关

V1.2 SDK 中，会在 lot_custom.c 加上如下 Boolean 全局变量，来控制是否打印 LOG

```

/*TRUE: Printf_High()/DBGPRINT_HIGH() is enabled, FALSE: Printf_High/DBGPRINT_HIGH() is disabled*/
BOOLEAN PRINT_FLAG = TRUE;

```

4.2 flash分区里reserved的区域有没有其他特殊用途？可不可以拿来保存一些数据

12 FLASH PARTITIONS

Offset	Section	Size (K)	HEX (Byte)	DEC Offset	
0x0000	Loader	20	0x0000	0	Store Loader program
0x5000	reserved 1	4	0x1000	20480	
0x6000	Recovery Mode FW	64	0x10000	24576	Store Recovery Mode program
0x16000	reserved 2	4	0x1000	90112	
0x17000	EEPROM	4	0x1000	94208	Store Calibration Settings
0x18000	Common Config	4	0x1000	98304	
0x19000	Station Mode Config	4	0x1000	102400	
0x1A000	AP Mode Config	4	0x1000	106496	
0x1B000	User Config	4	0x1000	110592	
0x1C000	reserved 3	12	0x3000	114688	
0x1F000	STA Mode FW	64	0x10000	126976	
0x2F000	reserved 4	4	0x1000	192512	
0x30000	STA Mode-XIP FW	60	0xF000	196808	Store Station Mode Program
0x3F000	STA Mode-OVL FW	60	0xF000	258048	
0x4E000	reserved 5	4	0x1000	319488	
0x4F000	AP Mode FW	64	0x10000	323584	
0x5F000	reserved 6	4	0x1000	389120	Store AP Mode Program
0x60000	AP Mode-XIP FW	60	0xF000	393216	
0x6F000	AP Mode-OVL FW	60	0xF000	454464	
0x7E000	reserved 7	4	0x1000	516096	
0x7F000	Flash Write Buffer	4	0x1000	520192	
0x80000	reserved 8	0	0x0	524288	Flash Write时的Data中转，以减少RAM BufSize

Reserved 主要用于 各区域之间的有效隔离

如果您在 flash 中 需要额外的使用空间， 建议可以用 0x1C000 这个位置的 reserved， total 12KB
只是需注意 不要越界到 0x1F000 即STA FW 的位置。

还有，我们 Chip 能 Access 到的 Flash Size 是 1MB， 目前 Flash Layout 中定义的是 512KB 的排列
如果您的产品 采用 1MB Flash ， 那么 [0x8000 ~ 0xFFFFF] 这个区域(512KB) 也是可以使用的。

4.3 打开 CFG_SUPPORT_TCPIP 宏使用AT命令的TCP功能。编译时出现错误

因为我们有开放出 uIP 的 SourceCode

ATCMD_TCPIP_SUPPORT 就没有再维护了，所以目前是把它给关掉的

4.4 为什么使用 IoT_gpio_output() 设定某个GPIO为 1 后，一会后莫名其妙又被拉低

原因很可能是：有地方调用到 IoT_gpio_input()的缘故

IoT_gpio_input() à

如果当前 GPIOx 是 Output mode，则会将其设定为 Input mode，此时得到的 input 值会改成 0

如果当前 GPIOx 是 Input mode，此时得到的 input 值 就是外面电路给到该 GPIO 的状态

在 v1.2 SDK ,会再提供 API: IoT_gpio_read (INT32 GPIONum, UINT8 *Val, UINT8 *Polarity)

可以只对 gpio 做 read 的操作，而不改变 gpio 状态/mode

5 CONNECTION DEVELOPMENT

5.1 MT7681 Support mode 和 Bandwidth

在 Package v1.10 中，Channel 选择的 API: IoT_Cmd_Set_Channel

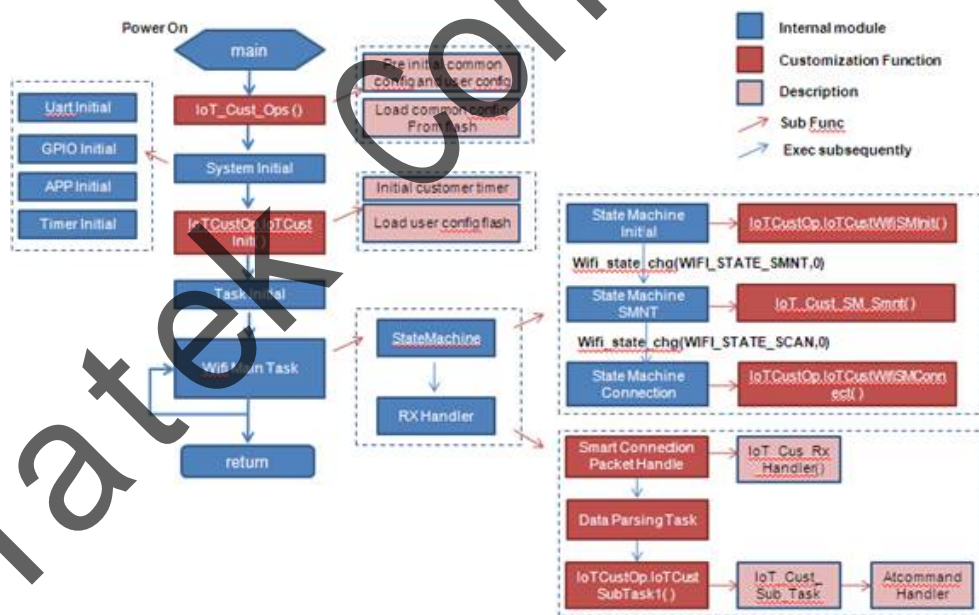
对于 Mode 和 Bandwidth: 目前 Support 80.211 b/g , BW_20M

5.2 一般 C程式有entry point,即main(), 請問一個IoT application 的entry point在哪裡？

是的，我们也有 main(), 只是我们未完全开放 main function

但我们有 创建 hook function 以便客户可以开发自己的程序，大部分集中在 iot_custom.c 中

可参考 MT7681_IoT_WIFI_Firmware_Programming_Guide_v0.0*.pdf 的 Section 5 “Customer Hook Function”



5.3 How to get mt7681 MAC address

The MAC address of 7681 is stored on Flash offset [0x17004~0x17009],

and this MAC shall be set to global parameter gCurrentAddress[MAC_ADDR_LEN]

Flash Layout				
Offset	Section	Size (KB)	HEX (Byte)	DEC Offset
0x0000	Loader	20	0x5000	0
0x5000	reserved 1	4	0x1000	20480
0x6000	Recovery Mode FW	64	0x10000	24576
0x16000	reserved 2	4	0x1000	90112
0x17000	EEPROM	4	0x1000	94208
0x18000	Common config	4	0x1000	98304

```

00056: #define VALID_EEPROM_VERSION 1
00057: #define EEPROM_VERSION_OFFSET 0x02
00058:
00059: #define EEPROM_MAC_12_OFFSET 0x04
00060: #define EEPROM_MAC_34_OFFSET 0x06
00061: #define EEPROM_MAC_56_OFFSET 0x08
00062:
00063: #define EEPROM_NIC1_OFFSET 0x34
00064: #define EEPROM_NIC2_OFFSET 0x36
00065:

```

5.4 在sta模式下连接ap，但是我要怎么来判断连接成功与否？？？

A1: 目前系统会有 Initial-> Smart Connection -> Scan -> Auth-> Assoc -> 4 way -> Connected 的过程，这个 State 会 设定在 ploTMLme->CurrentWifiState 这个变量中。以此来控制状态机的 flow
如果 ploTMLme->CurrentWifiState = WIFI_STATE_CONNED (6)，即表示与 AP 的连线成功
下一步会开始获取 IP

5.5 如何自动获取IP，是通过uip中的dhcpc相关函数吗？？？

A2: 进入到 Connected 的 State 后，会开始调用 tcpip_periodic_timer 进行 TCP/UDP 的相关数据交互
这里会开始做 DHCP 以获取 IP，具体文件和 function 如下图

```

- Source Insight - [Iot_udp_app.c (src\...\iot_udp_app)]
Options View Window Help

00043: void
00044: iot_udp_appcall(void)
00045: {
00046:     struct uip_udp_conn *udp_conn = uip_udp_conn;
00047:     u16_t lport, rport;
00048:
00049:     lport=HTONS(udp_conn->lport);
00050:     rport=HTONS(udp_conn->rport);
00051:
00052:     if(lport == DHCP_CLIENT_PORT) {
00053:         handle_dhcp();
00054:     } else if (rport == DNS_SERVER_PORT) {
00055:         handle_resolve();
00056:     }
00057: #endif
00058: /* Customer APP start.*/
00059:
00060:     else if (lport == 7682) {
00061:         udp_server_sample();
00062:     } else if (lport == 6666) {
00063:         udp_client_sample();
00064:     } else if (lport == 8888) {
00065:         resolv_usage_sample();
00066:     }
00067: /* Customer APP end.*/
00068: }

```

5.6 如何进行SW reset. 将IP/SSID 等参数 reset成出厂设定值

目前的 Code 已经有提供 AT#Default 的功能

对于参数设定 我们会在 Flash 的如下绿色 方框区域 来存储，
在 MT7681_IoT_WIFI_Firmware_Programming_Guide_v0.0*.pdf 的 Section “11 FLASH PARTITIONS “
有对 里面的每个 Byte 做定义

另外，在 iot_customer.c 中，有 common cfg, AP cfg, user cfg 的参数 load, reset 的函数实现，这部分有开放出来 对于 station cfg，也有 reset_sta_cfg() 来做初始化

Flash Layout					
Offset	Section	Size (KB)	HEX (Byte)	DEC Offset	
0x0000	Loader	20	0x5000	0	Store Loader program
0x5000	reserved 1	4	0x1000	20480	
0x6000	Recovery Mode FW	64	0x10000	24576	Store Recovery Mode program
0x16000	reserved 2	4	0x1000	90112	
0x17000	EEPROM	4	0x1000	94208	Store Calibration Settings
0x18000	Common config	4	0x1000	98304	
0x19000	Station Mode Config	4	0x1000	102400	
0x1A000	AP Mode Config	4	0x1000	106496	
0x1B000	User Config	4	0x1000	110592	
0x1C000	reserved 3	12	0x3000	114688	
0x1F000	STA Mode RAM FW	64	0x10000	126976	
0x2F000	reserved 4	4	0x1000	192512	Store Station Mode Program
0x30000	STA Mode-XIP FW	60	0xF000	196608	
0x3F000	STA Mode-OVL FW	60	0xF000	258048	
0x4E000	reserved 5	4	0x1000	319488	
0x4F000	AP Mode FW	64	0x10000	323584	
0x5F000	reserved 6	4	0x1000	389120	Store AP Mode Program
0x60000	AP Mode-XIP FW	60	0xF000	393216	
0x6F000	AP Mode-OVL FW	60	0xF000	454656	
0x7E000	reserved 7	4	0x1000	516096	
0x7F000	Flash Write Buffer	4	0x1000	520192	Flash Write时的Data中转，以减少RAM Buf Size
0x80000	reserved 8	0	0x0	524288	

5.7 现在的 1.10 版本好像没有 mem_alloc 及 mem_free 函数

因为没有 OS 的 support, 我们并没有完整的 mem_alloc 及 mem_free 的 API
目前的 malloc, free 函数 有限制 不能做嵌套的调用, 即

malloc(A) -> free(A) -> malloc(B) -> free(B) === OK

malloc(A) -> malloc(B) -> free(A) -> free(B) === NG

所以该 API 现在只在很少的地方用到, 但考虑到 MTK 和客户 都会开发代码, 建议不要使用该 API

目前大部分情况 大的 buffer 都是用全局/局部 数组 来申请!

所以在程序设计时, 我们对数组的 size 会多做一些考量。

5.8 结构体 _WIFI_STATE 的说明性文档, 每个状态代表什么意义

```
typedef enum _WIFI_STATE{
```

WIFI_STATE_INIT = 0, -> //进行 wifi state machine 的初始化, 会去读 flash 中存取的 sta cfg

设定, 如果已读到有效地 SSID, Password, PMK, AuthMode, 则直接跳到 SCAN 阶段, 否则到 SMNT 阶段

WIFI_STATE_SMTCNT, -> //执行 smart connection, 收集 sta cfg 中的设定

WIFI_STATE_SCAN, -> //通过 Init 或 Smnt 阶段得到的 sta cfg, 去 scan 特定 ssid ,
然后固定 channel

WIFI_STATE_AUTH, -> //向该 ssid AP, 发送 Auth Request frame 并获取 Auth Response

WIFI_STATE_ASSOC, -> //向该 ssid AP, 发送 Assoc Request frame 并获取 Assoc Response

WIFI_STATE_4WAY, -> //与该 ssid AP 进行 4-way handshark, 产生 GTK,PTK

WIFI_STATE_CONNED -> //会开始出发 dhcpc, 获取 AP 分配的 IP

```
}WIFI_STATE;
```

5.9 Smart Connection 的 station config 数据结构

如果不使用 MTK 的 smart connection

在 IoT_Cust_SM_Smnt 中有 如下处理, 可填写 IoTSmntInfo 结构体, 并 call wifi_state_chg 到 SCAN 状态, 此后系统会自动完成 Scan->Auth->Assoc 。。。。。的过程


```

00642:      }
00643:      /* Smnt connection done */
00644:
00645:
00646:      /* After smnt connection done */
00647:      /* need set Smnt connection information and start to scan*/
00648:      1 IoTSmntInfo.AuthMode      = 0;
00649:      IoTSmntInfo.SsidLen       = strlen(Ssid);
00650:      IoTSmntInfo.PassphraseLen = strlen(Passphrase); //sizeof(Passphrase);
00651:      memcpy(IoTSmntInfo.Ssid,   Ssid,       IoTSmntInfo.SsidLen);
00652:      memcpy(IoTSmntInfo.Passphrase, Passphrase, IoTSmntInfo.PassphraseLen);
00653:      memcpy(IoTSmntInfo.PMK,     PMK,       strlen(PMK));
00654:
00655:      IoT_Cust_smnt_info(); /*Sync the IoTSmntInfo to other StateMachine, must call this func if IoT Smnt connection done*/
00656:
00657:      2 /* change wifi state to SCAN*/
00658:      wifi_state_chg(WIFI_STATE_SCAN, 0);
00659:  #endif

```

5.10 Smart Connection的(station config)数据存取及清除

有关 cfg 存放每家客户 也可能有自己的做法

我们默认的做法是：存储到 Flash 中的 SSID/Password/PMK... 在绝大多数情况下 是不允许被改掉的

- 只有在 处理 AT cmd: Default ， 及处理 Data Cmd: Offline 时才清除
清除调用 function: reset_sta_cfg ()
- 或在使用原有 flash 中的值，无法连接 AP， 重新做 Smart Connection， 连接到新的 AP 获得 IP 时 才会覆盖旧的 flash sta cfg 值
存储调用 function 有： 在 smnt 阶段先 call IoT_Cust_smnt_info(VOID)， 到获得 IP 后会再由 ws_got_ip() call 到 store_sta_cfg(VOID)

```

==> Recovery Mode
<== RecoveryMode
(-)
SM=0, Sub=0
SM=1, Sub=0
SM=2, Sub=0
SM=3, Sub=0
SM=3, Sub=1
SM=4, Sub=0
SM=4, Sub=1
SM=5, Sub=0
SM=6, Sub=0
Got IP:192.168.43.61
[wTask]11782
[wTask]19640
[wTask]27246
==> Recovery Mode
<== RecoveryMode
(-)
SM=0, Sub=0
SM=2, Sub=0
SM=3, Sub=0
SM=3, Sub=1
SM=4, Sub=0
SM=4, Sub=1
SM=5, Sub=0
SM=6, Sub=0
Got IP:192.168.43.61
[wTask]9945
[wTask]15083
[wTask]20497

```

第一次上电 开始做
Smart Connection

连接成功 此时会存储
Smart Connection的数据
这样下次再上电就不用再做
smart connect了

再次上电后，直
接进入Scan状态

5.11 使用宏 CFG_SUPPORT_MTK_SMNT=1 来控制是否使用 MTK的smart connection

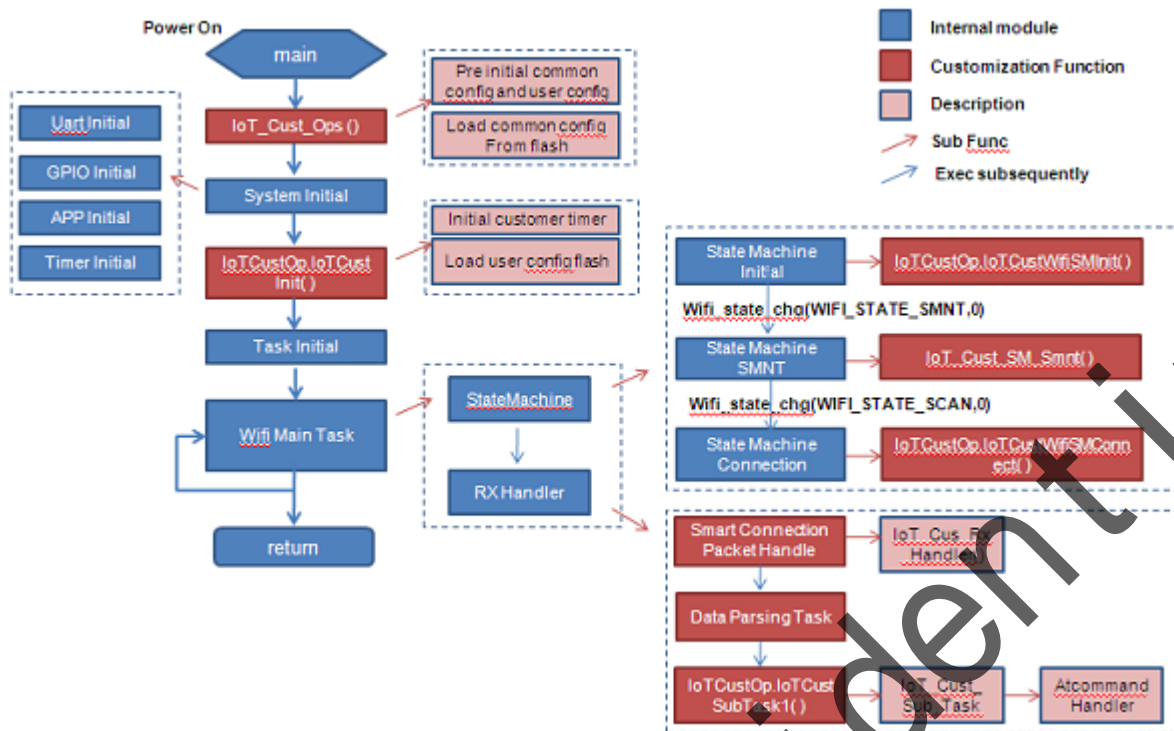
如果客户有自己的 Smart Connection，就可将该宏 值设为 0

在 MT7681_IoT_WIFI_Firmware_Programming_Guide_v0.05.pdf 中， 有列出当前 Smart connection 开放出的对应 callback，

其中 IoT_Cus_Rx_Handler() 可看到每一包 Rx Packet 的内容，并可对其做进一步处理

IoT_Cut_SM_Smnt() 是 smart connection 的状态机。

结合代码可做进一步了解



5.12 How to get PMK

PMK 会由 SSID, Passphase 通过 SHA1 算法 计算得到
我们之前试验 7681 软件来计算该值，但会花费近 6s 的时间

所以我们有修改 smart connection 的做法，
让手机端先计算好 PMK， 然后通过 smart connection 将 SSID, Passphase, PMK, AuthMode 传递出来。
这样 7681 就不用再计算 PMK， 节省时间， 所以后面 7681 是将软件计算 PMK 的 function 给拿掉

如果您需要使用，可以在 IoT_Cust_SM_Smnt() 中 调用 API: RtmpPasswordHash()

```

00646: /* After smnt connection done */
00647: /* need set Smnt connection information and start to scan*/
00648: IoTSmntInfo.AuthMode = 0;
00649: IoTSmntInfo.SsidLen = strlen(Ssid);
00650: IoTSmntInfo.PassphaseLen = strlen(Passphase); //sizeof(Passphase);
00651: memcpy(IoTSmntInfo.Ssid, Ssid, IoTSmntInfo.SsidLen);
00652: memcpy(IoTSmntInfo.Passphase, Passphase, IoTSmntInfo.PassphaseLen);
00653:
00654:
00655:
00656: {
00657: /*Deriver PMK by AP 's SSID and Password*/
00658: UCHAR keyMaterial[40] = {0};
00659: if (IoTSmntInfo.AuthMode != Ndis802_11AuthModeOpen)
00660: {
00661: RtmpPasswordHash(IoTSmntInfo.Passphase, IoTSmntInfo.Ssid,
00662: IoTSmntInfo.SsidLen, keyMaterial);
00663: NdisMoveMemory(IoTSmntInfo.PMK, keyMaterial, 32);
00664: }
00665: //memcpy(IoTSmntInfo.PMK, PMK, strlen(PMK));
00666:
00667: IoT_Cust_smnt_info(); /*Sync the IoTSmntInfo to other StateMachine, must call this func if IoTSmntInfo changed*/
00668:
00669: /* change wifi state to SCAN*/
00670: wifi_state_chg(WIFI_STATE_SCAN, 0);
00671: #endif
}

/*
* password - ascii string up to 63 characters in length
* ssid - octet string up to 32 octets
* ssidlength - length of ssid in octets
* output must be 40 octets in length and outputs 256 bits of key
*/
int RtmpPasswordHash(PSTRING password, PCHAR ssid, INT ssidlength, PCHAR output)

```

6 APPLICATION DEVELOPMENT

6.1 How to send TCP/UDP packet

UDP, TCP app 的开发 包括 connection 建立和 packet 发送
都应该在 Tcpiplib_main.c 中 uip_process() → UIP_APPCALL / UIP_UDP_APPCALL 中进行,
目前 uIP 完成 Code 是有开出来的, 可以进行自定义的开发

在其他地方 (AT cmd handler 中) 直接调用 uip_send() 发送 Packet 会失败,
因为直接调用该 function, 不会指定具体发给哪个 connection.

```
void IoT_Cust_uart2wifi_data_handler(UCHAR *uart_content, UINT16 uart_content_count)
{
    IoT_uart_output(uart_content, uart_content_count);

    /*should not call uip_send here, all uip_send need to be implemented
    in iot_udp_appcall() / iot_tcp_appcall(), as the reason of the uIP app
    management (Connection/Port...) is controlled in the iot_***_appcall()*/
    //uip_send(uart_content, uart_content_count); //mask

    /*here should allocate a buffer or flag,
    Let iot_***_appcall() detected it and call uip_send()*/

    return;
}
```

6.2 IoT application 内要 scan AP, 连到 AP, 建 TCP + SSL ... 等, 要参考哪些 APIs document?

MTK 代码中, 有 Initial → Smart Connection → Scan → Auth → Assoc → 4 way → DHCP 的过程,
手机上安装的 APK 会 发送出 SSID, Password, PMK, MT7681 在 Smart Connect 阶段会获取这些信息
然后依此来 Scan 对应的 AP, 并进行连线 和从 AP 获得 IP.
前面这些基本很少客制化, 所以未开发出对应的 API

获得 IP 后, 可以使用现有的 uip 进行 TCP/UDP Connection 的建立,
这部分有 Source Code 和 Sample Code 开放出来, 他们的 .c / .h 档有放在如下目录
IoT_MT7681_PKG\cust\tcpip\, IoT_MT7681_PKG\src\tcpip\
您可参考 Package 中的 文档 MT7681_TCP_IP_*****_ToCust.pdf
并结合这些 Source File 来了解

6.3 数据从服务器转发到 7681, 数据包格式是怎样的, 经过解包之后是怎样的数据类型?

可参考 Release Package v1.10 的 IoT_Control_Protocol_v0.2.pdf 了解数据包的具体格式
解包后的数据 会在 iot_parse.c 的 iot_process_app_packet() 中做进一步处理
客户也可定义直接的格式

6.4 SDR 中有 TCP 和 UDP 两种方式, UDP/TCP 是什么情况下使用的呢?

是的会有两种方式, 不过这些方式都可以是客户来确定的

有关 TCP, UDP 的 API 和 Source Code 我们并未采用标准 socket, 而使用 uip
主要原因是当前 MT7681 并未采用 multi task 或复杂的 OS

这部分有 Source Code 和 Sample Code 开放出来, 它们的 .c / .h 档有放在如下目录
IoT_MT7681_PKG\cust\tcpip\, IoT_MT7681_PKG\src\tcpip\
您可参考 Package v1.10 中的 文档 MT7681_TCP_IP_*****_ToCust.pdf
结合这些 Source File 来了解具体的使用

6.5 MT7681 透过 AP Router 与 Internet Server, 请问这个 Internet Server 做"转发"作用外, 还有哪些作用呢?

同 4.3 一样, Internet Server 实际也是客户来确定的
它可以做简单的转发, 也可以做其他更多的事情,

6.6 是否有获取网络时间的协议 Support SNTP, NTP

应该需要 SNTP, NTP 协议, 在 MTK 的当前代码中并未包含这些 比较上层的协议

6.7 Set up the TCP connection on MT7681

Behavior example:

- (1) Connection Type: TCP on port 12345 with data payload "0" or "1" only.
- (2) Send data to MT7681 to Pull GPIO high/Low

相关修改如下:

Step1:

在 `iot_custom.c` 中有如下 default 定义

```
00060: #define DEFAULT_IOT_TCP_SRV_PORT 7681 /*The IoT Server TCP Port in the internet */
00061:
00062: #define DEFAULT_TCP_UDP_CS 1 /*0: UDP, 1:TCP (Default 3*Client, 1*Server is Open)*/
00063: // #define DEFAULT_IOT_TCP_SRV_PORT 7681 /*The IoT Server TCP Port in the internet */
00064: #define DEFAULT_IOT_TCP_SRV_PORT 12345 /*The IoT Server TCP Port in the internet */
00065: #define DEFAULT_LOCAL_TCP_SRV_PORT 7681 /*The TCP Port if 7681 as a TCP server */
00066: #define DEFAULT_IOT_UDP_SRV_PORT 7681 /*The IoT Server UDP Port in the internet */
00067: #define DEFAULT_LOCAL_UDP_SRV_PORT 7681 /*The UDP Port if 7681 as a UDP server */
00068:
00069: #define DEFAULT_USE_DHCP 1 /*0: Static IP, 1:Dynamic IP*/
00070: #define DEFAULT_STATIC_IP {192,168,0,99}
00071: #define DEFAULT_SUBNET_MASK_IP {255,255,255,0}
00072: #define DEFAULT_DNS_IP {192,168,0,1}
00073: #define DEFAULT_GATEWAY_IP {192,168,0,1}
00074: // #define DEFAULT_IOT_SERVER_IP {192,148,123,91}
00075: // #define DEFAULT_IOT_SERVER_IP {172,26,74,63}
00076: #define DEFAULT_IOT_SERVER_IP {192,168,1,89}
00077:
00078: #define DEFAULT_IOT_CMD_PWD {0xFF,0xFF,0xFF,0xFF}
```

首先 修改 方框 1 的 Server Port 为 12345, 然后修改方框 2 的 Server IP

修改方框 2 的 Server IP 最后会被 赋值给 `IoTpAd.ComCfg.IoT_ServerIP`

这样在 7681 上电 获取 IP address 后, 会与该 TCP server 建立连接
正常的话, LOG 中会有如下提示:

```
SM=2, Sub=0
SM=3, Sub=0
SM=3, Sub=1
SM=4, Sub=0
SM=4, Sub=1
SM=6, Sub=0
Got IP:192.168.1.102
[Task]185880
Connected fd:0,lp:7682,ra:192.168.1.89,rp:8888
```

Step2:

TCP Connection 建立连接后, TCP Server 就可以 发送 Data Command 来控制 7681 的 GPIO 了
Data Command 的 Protocol 可以参考 Package v1.10 的文档: `IoT_Control_Protocol_v0.*.pdf`

Packet	Source	Destination	BSSID	Protocol	Flags	Channel	Signal	Data R
703	192.168.1.102	192.168.1.89	1C:FA:68:B8:93:B4	TCP		11	100%	6.0
709	192.168.1.89	192.168.1.102	1C:FA:68:B8:93:B4	TCP		11	100%	54.0
711	192.168.1.102	192.168.1.89	1C:FA:68:B8:93:B4	TCP		11	100%	6.0

Packet: 709

[x] ?

Packet Info

Packet Number=709 Flags=0x00000000 Status=0x00000000 Pa

802.11 MAC Header

Version=0 Type=10 Data Subtype=0000 Data Only Dur:

802.2:

D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information

IP:

S=192.168.1.89 D=192.168.1.102

TCP:

S=ddi-tcp-1 D=7682 SEQ=3955996178 ACK=122 W=5840

HTTP:

Binary Data=(36 bytes)

FCS:

FCS=0xD8D788D1 Calculated

0000:

08 02 2C 00 00 0C 43 26 60 40 1C FA 68 B8 93 B4

0016:

D8 D3 85 38 63 FF A0 00 AA AA 03 00 00 00 08 00

0032:

45 00 00 4C 30 96 40 00 04 06 86 06 C0 A8 01 59

0048:

C0 A8 01 66 22 B8 1E 02 EB CB B6 12 00 00 00 7A

0064:

50 18 16 D0 E2 93 00 00 50 43 81 76 FF FF FF FF

0080:

FF FF 1C FA 68 B8 93 B4 FF FF FF FF 0B 00 10 01

0096:

03 00 08 00 1F 00 00 00 1F 00 00 00 00 00 00 00

GPIO Set request

GPIO Information

set GPIO(0-4) to High

Data Control Header

Data Control Header							Data			
4B	6B	6B	4B	2B	4bit	4bit	3bit	2B	2B	4B
Magic	Receive MAC	Send MAC	Session ID	Sequence Number	flag	Control type	subtype	Data Type	Data Length	Data Value

Seq Num: 需要递增

if set GPIO(0-4) to low

Data: 1F 00 00 00 00 00 00 00

Tcp_Connect 命令等 TCP_IP 配置的条件是?

Tcp Connect 命令等 TCP IP 配置命令是否还能再配置?

A3-1: SoftAPConf 命令 有在代码中被 CONFIG_SOFTAP 宏给包起来， 该宏只在 flag_ap.mk 中指定上， 所以 SoftAPConf 命令 只在 SoftAP mode 才会 enable 起来

A3-2: 因为有开放出所有的 UIP source code， 所以 AT cmd 中 Tcp Connect 命令 现在是默认 disable 的，