CPE 操作手册

CPE User Manual

Version：	2.1
Author：	Samson Sun
Time：	2018/9/7

文件变更履历表

Document Revision History

版次 version	修订日期 date	修订作者 author	修订理由及内容摘要 reasons and contents
1.0	2017/05/08	孙朝阳 Samson Sun	Initial Version
1.1	2017/05/18	左琪 Zack Zuo	1.Translate to English 2.Add Senior maintenance
1.2	2017/05/19	Samson Sun	1. Modify some expression .
1.3	2017/07/03	Samson Sun	1. Update LED spec 2. Update snapshot base on new style . 3. Add multi PDN configuration 4. Add KPI analysis
1.4	2017/07/18	Leanshaw Zhao	1. Add Configure working band
1.5	2017/08/10	Phoebe Ge	1.How to disable PIN
1.6	2017/10/18	Binary Xue	1. Add ARM1 upgrade method
1.7	2018/02/09	Phoebe Ge	1. Add save PM log to Flash
1.8	2018/3/30	Sally Luo	1.Add ssl test
1.9	2018/4/4	Phoebe Ge	1.Add Host_cm Enable
2.0	2018/08/27	Sandy Yang	1. Add 2.7 SAS 相关参数配置 2. Add 2.SAS Test
2.1	2018/09/07	Sandy Yang	1. 更新 2.7 SAS 相关参数配置 2. 更新 2.SAS Test

目录

Index

初级维护

Primary Maintenance

1.检查 CPE 的设备状态

CPE Status Check

本章节主要指导用户检查 CPE 的设备状态，包括检查外部环境、USIM 卡指示、如何获取 CPE 网络状态信息、检查 LED 状态这 4 部分的内容。

This chapter guides users to check the status of CPE, which includes environment check, USIM card check, network status check and LED check.

1.1.CPE 外部环境确认

Environment check

在 CPE 运行之前，需要确认附近是否有 B42、43 或者 B48 小区覆盖。

There should be B42,B43 or B48 Cells nearby .

1.2.检查 USIM 卡状态

USIM Card check

（1）查看 USIM 卡是否插入，如果有，插入位置是否正确（目前支持的 USIM 卡为标准 SIM 卡）。

USIM Card should be properly inserted.

（2）查看插入的 USIM 卡是否合法，即 USIM 卡是当前运营商发放的。

The USIM Card should be a registered card by current network.

（3）检查 USIM 卡是否锁 PIN，目前 CPE 不支持自动解 PIN，若 USIM 卡为锁 PIN 状态，需要对 USIM 卡进行手动解 PIN。

The PIN lock should be disabled with the USIM Card, if not , do PIN unlock before insert it into device .

1.3.手动解 PIN

Disable PIN

（1）访问：http://10.10.2.254:8080/

Visit：http://10.10.2.254:8080/

（2）切换到 LTE→SIM PIN 界面

Locate to LTE→SIM PIN

（3）在 PIN Management 下的 PIN Code 输入框中输入 PIN Code

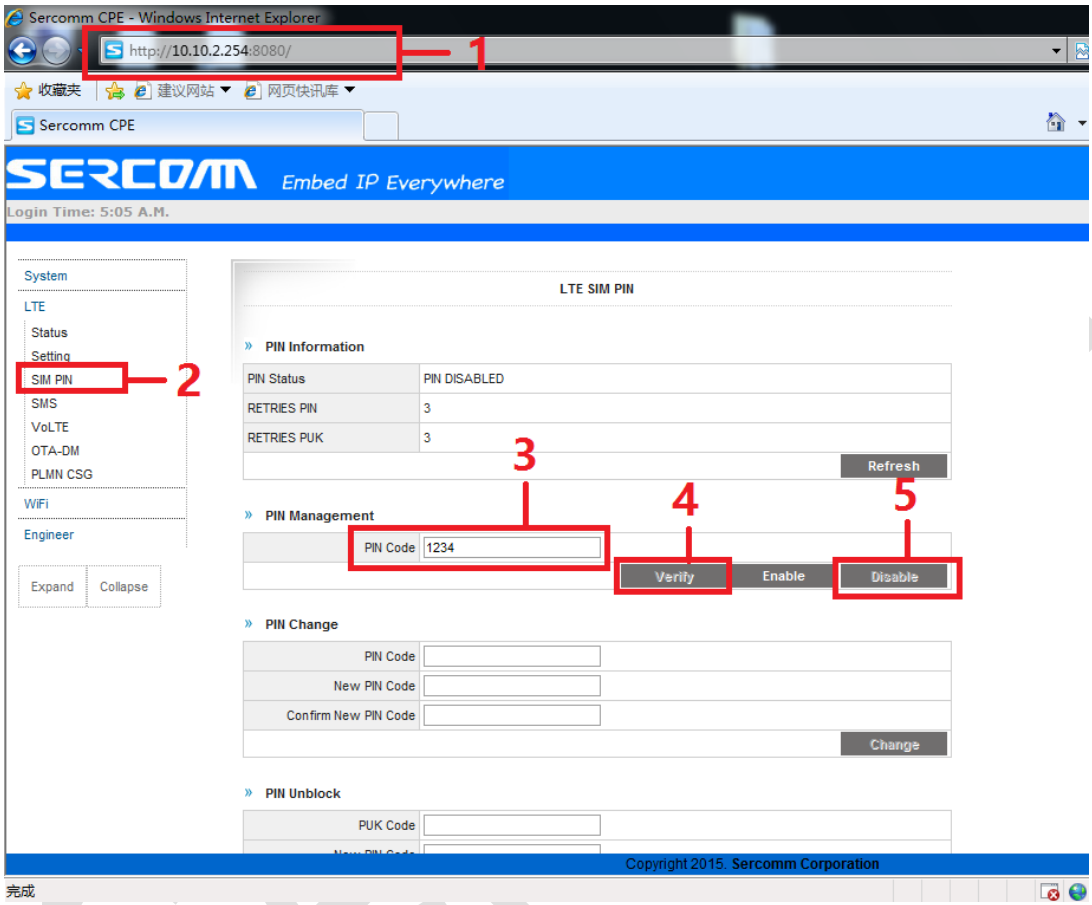
Enter the PIN Code in PIN Management

（4）点击 Verify

Click the Verify button.

（5）点击 Disable

Click the Disable button.



1.4.获取 CPE 的网络状态信息

Network information

在定位问题之前，需要获取 CPE 的状态信息以帮助调查问题。通过网页获取 CPE 的网络状态信息，步骤如下：

CPE status information would be helpful to investigate issue . You can get basic information from GUI, steps as follow：

（1）PC 需要 fix IP:10.10.2.2；

Fix 10.10.2.2 to PC.

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码 admin）；

Log-in to device by web browser , URL is https://10.10.2.254

User name : admin / Password : admin

（3）进入【Status】页面。如 fig 1-1 所示，在该图中可以看到 CPE 的网络状态信息：

Click [Status] on the left menu. As shown in fig1-1, it contains CPE basic network information.

Status Cause:	LTE 连接状态，指示 CPE 目前的连接行为原因 LTE connection status, indicate current CPE behavior
Connection Status:	显示 CPE 的连接状态 Indicates the connection status of CPE
APN:	APN 名称 APN name
Internet IP Address:	CPE 上线后获取到的 IP 地址 IP address assigned from network
IMEI:	国际移动装备辨识码 International Mobile Equipment Identity
IMSI:	USIM 卡的国际移动用户识别码 International Mobile Subscriber Identification Number
EARFCN(UL):	驻留到的小区的上行载波频点信息（由于是 TDD 的小区，所以上行频点和下行频点是一样的） UL EARFCN of serving LTE cell
EARFCN(DL):	驻留到的小区的下行载波频点信息（包括主载波频点和辅载波频点） DL EARFCN of serving LTE cell
PCI:	驻留小区的物理小区标识 Physical Cell ID of serving LTE cell
RSSI:	无线信号的接收信号强度指示 Received Signal Strength Indication of serving LTE cell
TAC:	跟踪区域码 Tracking Area Code of serving LTE cell
RSRQ:	无线信号的参考信号接收质量 Reference Signal Received Quality
SINR:	无线信号的信噪比 Signal to Interference plus Noise Ratio

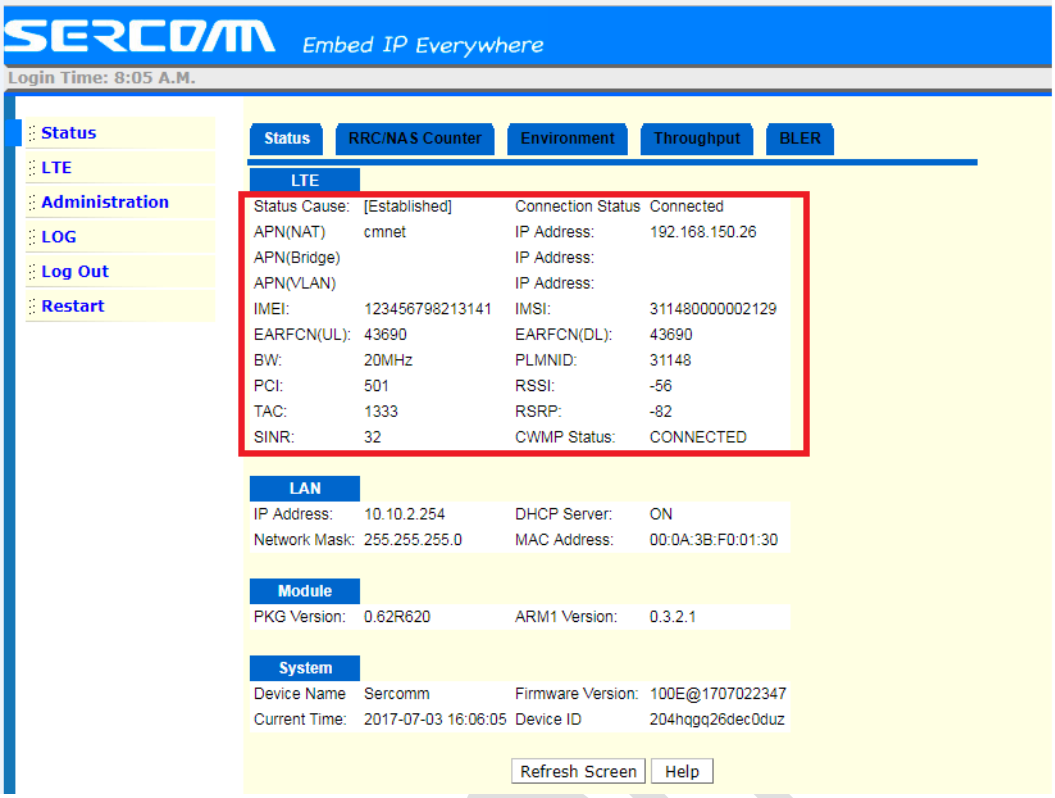


Fig1-1 CPE network information

1.5.查看 CPE 版本号

CPE Version

CPE 版本号如图 fig 1-2 的红色方框中所示：

CPE version is shown in the red area in fig 1-2.

Firmware Version: CPE 版本号
CPE Version

PKG Version: SDK 版本号
SDK version

ARM1 Version: Stack Version
Stack version

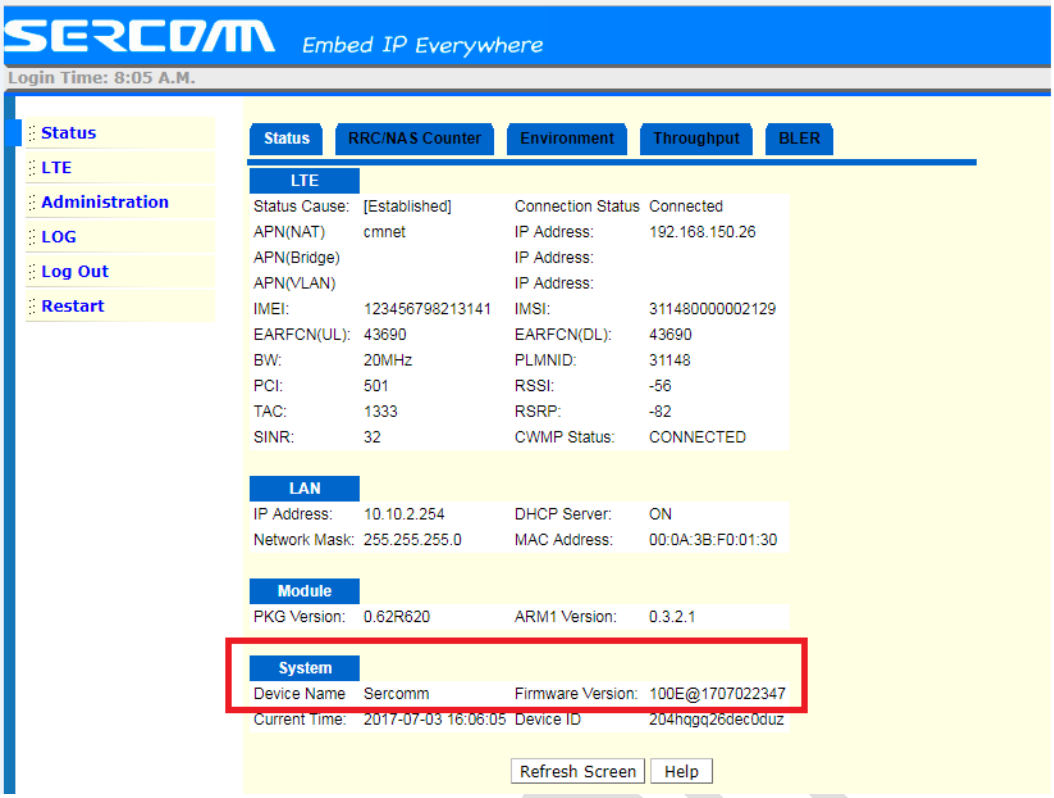


Fig 1-2 CPE and Module version

1.6.LED

LED

STATUS	POWER LED		SIGNAL LED		
	GREEN	RED	BLUE	GREEN	ORANGE
Power On	ON	OFF	OFF	OFF	OFF
Power Off	OFF	OFF	OFF	OFF	OFF
No USIM Card	OFF	ON	OFF	OFF	OFF
SIM PIN	ON	Blink 2 times in 6.4 seconds	OFF	OFF	OFF
No Available Cell	ON	Blink 3 times in 6.4 seconds	OFF	OFF	OFF
Attach Fail	ON	Blink 4 times in 6.4 seconds	OFF	OFF	OFF
Invalid APN Name	ON	Blink 5 times in 6.4 seconds	OFF	OFF	OFF
Upgrading	BLINK	OFF	OFF	OFF	OFF
Upgrading Fail	ON	BLINK	OFF	OFF	OFF
PLMN Search /Attaching	ON	OFF	OFF	BLINK	OFF
RSSI (< -106)	ON	OFF	OFF	OFF	ON
RSRP (-106 ~ -87)	ON	OFF	OFF	ON	OFF
RSRP (> -87)	ON	OFF	ON	OFF	OFF

2.修改 CPE 的配置

Configure CPE

本章节主要描述如何通过 UI 对 CPE 进行配置，包括基本配置和高级配置，其中基本配置描述了通过 UI 能够对 CPE 的哪些内容进行配置，高级配置描述了具体功能的配置。

This chapter guides users to configure CPE, includes basic and advanced configuration, basic describes how to configure on GUI and the advanced describes how to configure specific function.

2.1.APN 名称配置

Configure APN Name

（1）PC 需要 fix IP:10.10.2.2；

Fix 10.10.2.2 to PC.

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；

Log-in to device by web browser

URL:https://10.10.2.254

User name : admin

Password : admin

（3）请进入【LTE】页面，对 CPE 的 APN name 进行配置，配置方法如 fig 2-1 所示：

Click [LTE] on the left menu, the method is shown in fig2-1:

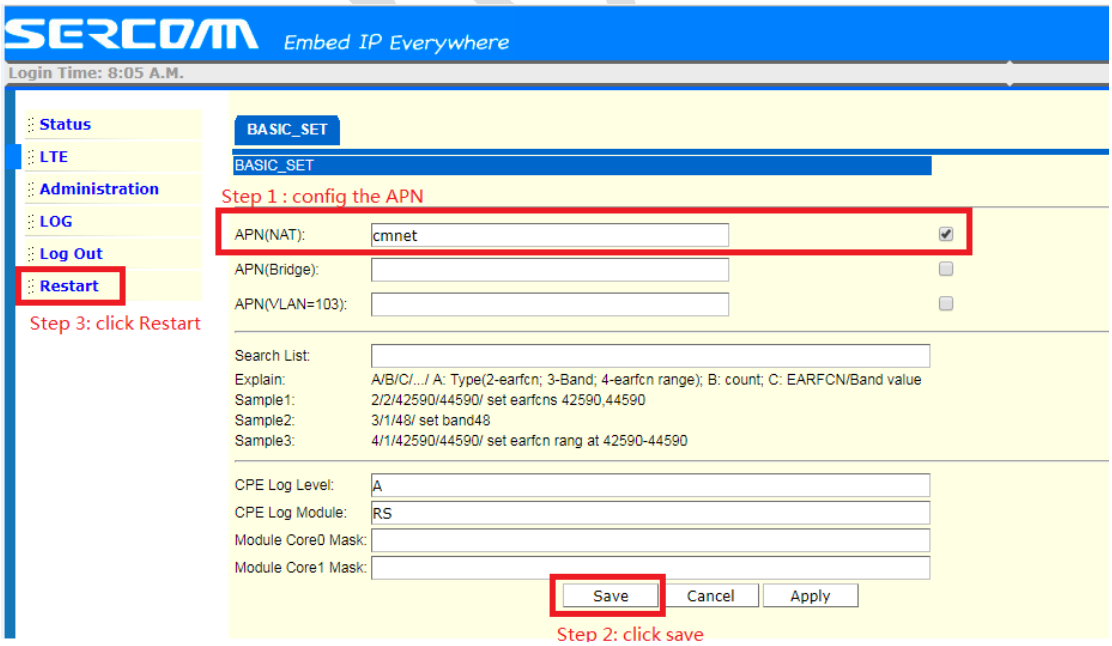


Fig2-1 Configure APN Name

注意：

1. 本系统支持多 PDN 设定，不同的 PDN 工作在不同的网络分享模式，请勿修改当前的 PDN 启用参数，以免设备无法正常提供服务。

Notice: CPE supports multiple PDN, each PDN works in different mode, double confirm current network mode and only enables related PDN to protect CPE not in service .

2. 各种 APN 的使用场景说明

a) APN(NAT) -- 接在其后的主机通过 DHCP 获取私有 IP，CPE 为所有接在其后的主机通过 NAT 技术提供共享上网服务，支持多主机接入。

Notice: CPE works as NAT mode.

b) APN(Bridge) -- 接在其后的主机通过 DHCP 获取“合法 IP”，CPE 作为 Bridge 将主机的以太网络和 LTE 网络对接，主机独享并完全拥有该“合法 IP”。

i. 仅识别每次上电后的第一台接入的主机，一旦识别成功（成功获取 IP），将不再为其他接入主机提供服务，如果需要更换接入主机，则需要在跟还完主机之后重启设备。

Notice: CPE works as Bridge mode. There is only connected PC can get IP, To change the other PC, CPE needs to restart.

ii. 仅当 CPE 在该 APN 上成功获取到 IP 之后，接在其后的主机才能够获取到 IP。

Notice: CPE works as Bridge mode. Connected PC cannot get IP until APN’s PDN connection be established successfully.

c) APN(VLAN=103) -- 接在其后的主机通过 vlan 方式独占该 APN 上的 IP 资源，vlan id=103；IP 需要通过手动方式绑定到接入主机上。

Notice: CPE works as Bridge mode and the interface between CPE and connected PC is VLAN, and VLAN ID is 103.

d) 以上三种 APN 可以混合使用，混合使用的时候，需要注意以下几点：

Notice: These three APN can be used at the same time, but there are some condition needs to meet.

i. 多个 APN 同时使用的时候，只允许一个 APN 的 APN Name 为空，其余不允

Notice: One of three APN name can be empty if there are more than 1 APN used.

ii. APN(NAT) +APN(Bridge)混合使用的时候，CPE 的 APN(NAT)用于 CPE 自身网络访问之需求，接入 CPE 按照 b)规则执行。

Notice: When NAT and Bridge used at the same time, the APN of NAT is used for CPE itself, Bridge APN follow b) rule to work.

2.2.修改锁频信息

Configure Search List

（1）PC 需要 fix IP:10.10.2.2，不要指定网关地址；

Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（1）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；

Open your web browser and visit device.

（3）请进入【LTE】页面，按照 fig 2-2 配置：

Click [LTE] on the left menu, the method is shown in fig2-2:

Search List：　　设置优选频点，如何设置，页面上有说明
Refer to examples on GUI.

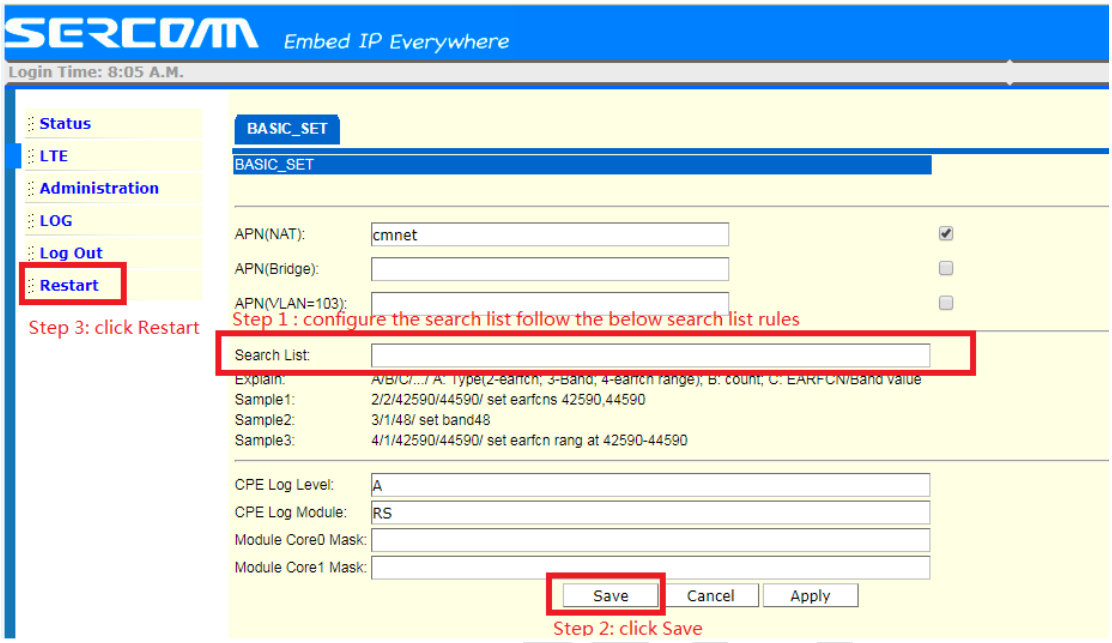


Fig 2-2 Configure Search List

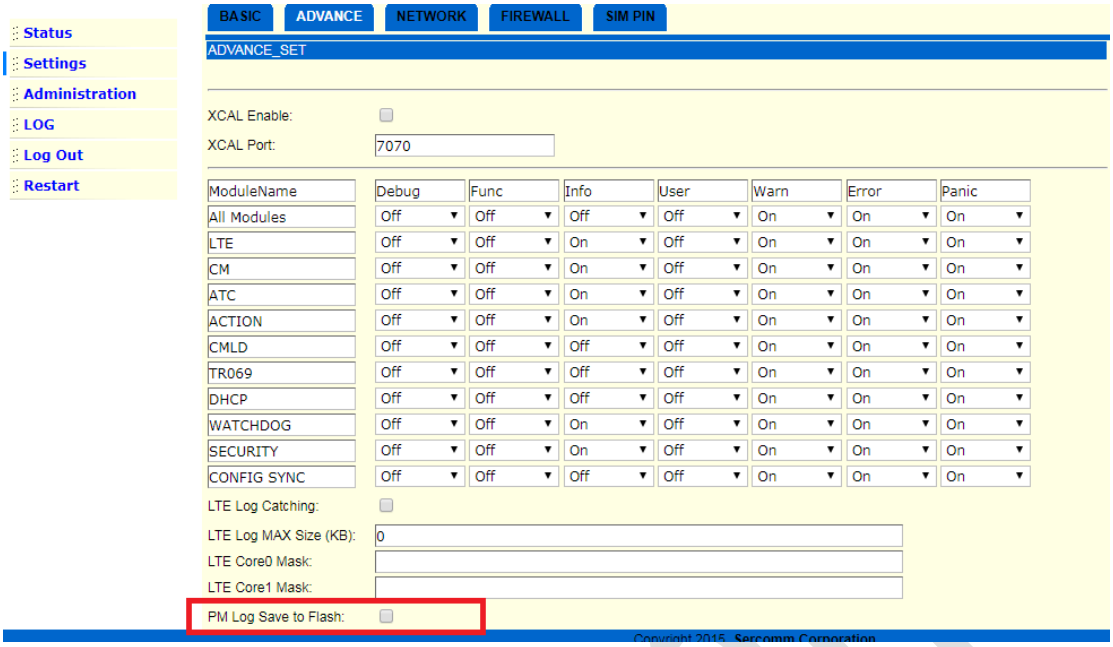
2.3.将 log 存入 Flash

Save PM log into Flash

（1）PC 需要 fix IP:10.10.2.2，不要指定网关地址；
Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；
Open your web browser and visit device.

（3）进入【Settings】→【ADVANCE】页面，选中 PM log save to Flash.
Click [Settings] on the left menu, get into the ADVAANCE page, click on PM log save to Flash.



2.4.开启/关闭 Host_cm

Host_cm Enable/Disable

（1）PC 需要 fix IP:10.10.2.2，不要指定网关地址；

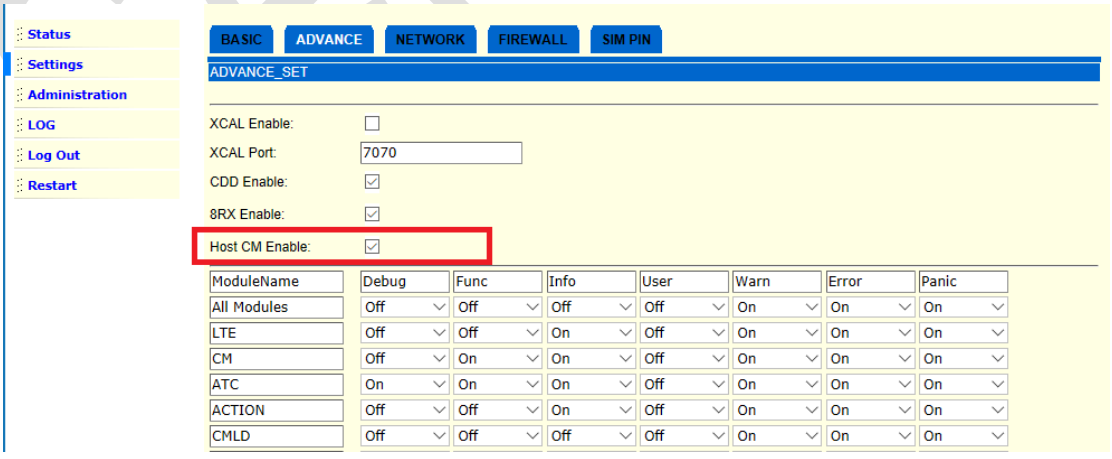
Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；

Open your web browser and visit device.

（3）进入【Settings】→【ADVANCE】页面，选中 Host CM Enable.

Click [Settings] on the left menu, get into the ADVAANCE page, click on Host CM Enable.



2.5.恢复出厂设置

Factory Default

（1）PC 需要 fix IP:10.10.2.2/24，不要指定网关地址；
Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；
Open your web browser and visit device .

（3）请进入【Administration】页面，按照 fig 2-3 配置：
Click [Administration] on the left menu, steps are shown in fig2-3 :

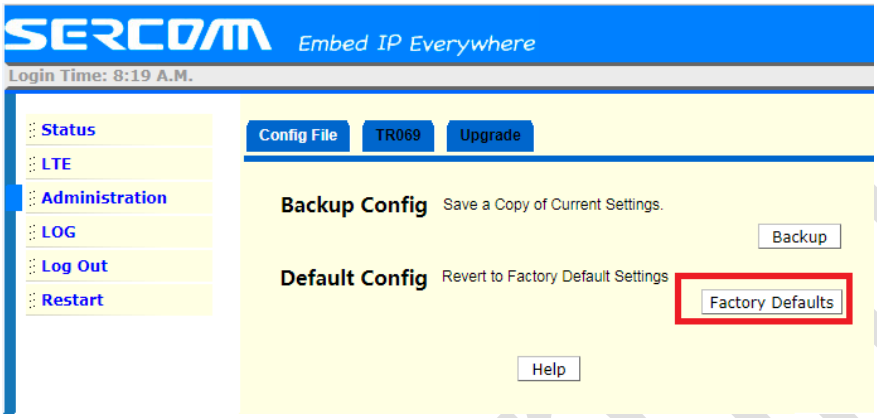


Fig 2-3 Factory Default

2.6.配置工作频段

Configure working band

(1) PC 需要 fix IP:10.10.2.2/24，不要指定网关地址；
Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

(2) 通过 telnet 访问 CPE：telnet 10.10.2.254，用户名/密码：root/gct
Telnet 10.10.2.254 username:root password:gct

(3) 通过下述方法，进入 DM 模式：
Follow below steps to make CPE enter DM mode

1) 在 shell 模式下，输入 lted_cli，出现 lted_client_init_ex success
Under shell, input “led_cli”, and it will show “lted_client_init_ex success”

2) 按回车键会出现 DM> 即进入 DM 模式
Press return(or Enter) on the keyboard, if it shows “DM>”, meas CPE is under DM mode

3) 如果没有出现 DM>，请输入 arm1log 2
If it doesn’t show “DM>”, please input “arm1log 2”

4) 如果出现大量的日志，请输入 q 0
If it show out too much log, please input “q 0” under DM mode.

(4) 输入 nvm bcfgr 49 0，查看当前 CPE 的工作频段
Input “nvm bcfgr 49 0”, and it will show current support band list.

(5) 输入 nvm bcfgw 49 0 48，设置 CPE 的工作频段为 48
Input “nvm bcfgw 49 0 48”, to set that support band list is 48 in CPE.

(6) 保持当前配置，nvm bcfgsv 1
Input “nvm bcfgsv 1” to save current configure.

(7) 重启 CPE，kern reboot

Input “kern reboot” to reboot CPE.

完整示例如下：

Following is a detailed example:

1. telnet 10.10.2.254, root/gct
2. #lted_cli
3. DM>nvm bcfgr 49 0
4. DM>nvm bcfgw 49 0 48
5. DM>nvm bcfgsv 1
6. DM>kern reboot

2.7 SAS 相关参数配置

SAS parameter configure

（1）PC 需要 fix IP:10.10.2.2/24，不要指定网关地址；

Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）PC 通过浏览器访问 HTTPS://10.10.2.254（用户名:admin; 密码:admin）；

Open your web browser and visit device .

（3）点击【Settings】，再点击【SAS】，请参考 fig 2-4：

Click [Settings] on the left menu, then click [SAS] on the top menu, which is shown in fig2-4 :

（4）对相关参数进行配置，以及上传相关证书；

Configure parameters and upload certificates

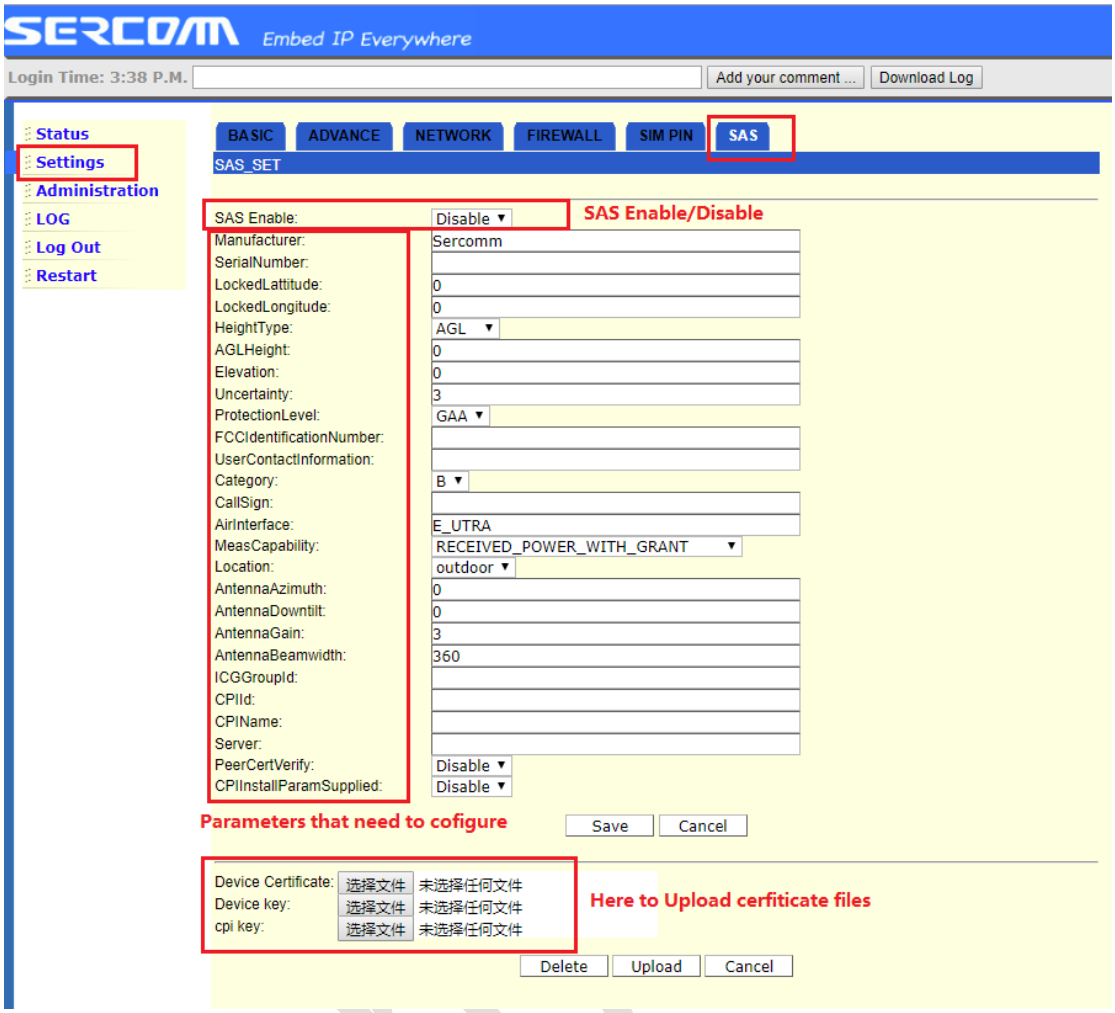


Fig 2-4 SAS parameter configure

3.CPE 升级

CPE Upgrade

3.1.CPE 升级方法

CPE Upgrade Method

（2）（1）PC 需要 fix IP: 10.10.2.2，不要指定网关地址；

Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）登录到 CPE 的页面: HTTPS://10.10.2.254 (用户名: admin 密码: admin);

Open your web browser and visit device .

（3）点击 Administration 按钮;

Click the Administration.

（4）点击 Upgrade 按钮;

Click the Upgrade.

（5）选择要升级的文件(例如: SERCOMM_CPE_101A.bin);

Choose the file you want to upgrade (e.g: SERCOMM_CPE_101A.bin).

（6）点击 Upload 按钮升级.

Click the Upload button to upgrade.

Fig 3-1 CPE Upgrade

3.2.ARM1 升级方法

CPE ARM1 Upgrade Method

（1）PC 需要 fix IP: 10.10.2.2，不要指定网关地址；

Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）登录到 CPE 的页面: HTTP://10.10.2.254:8080;

Open your web browser and visit device .

（3）点击 System 按钮;

Click the System.

（4）点击 Firmware Update 按钮;

Click the Firmware Update.

（5）选择要升级的文件(例如: tk.gz);

Choose the file you want to upgrade (e.g: tk.gz).

（6）选择 RAW Format;

Choose RAW Format.

（7）点击 Update 按钮升级.

Click the Update button to upgrade.

4.获取 CPE 日志

Get CPE Logs

4.1.通过页面查看 CPE 日志

Check CPE Logs by GUI

页面查看 CPE 的日志方法：
Steps to check logs as follow:

（3）PC 需要 fix IP:10.10.2.2，不要指定网关地址；
Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）页面登陆到 CPE，地址：HTTPS://10.10.2.254（用户名：admin 密码：admin）；
Open your web browser and visit device .

（3）点击页面左侧 LOG 按钮；
Click [LOG] on the left menu, as shown in fig4-1.

（4）在 LOG 页面中包含五个子页面，分别显示不同类型的 LOG：
There are five sub pages, each shows different kind of CPE logs.

LOG	CPE 的运行日志 Includes running logs such as attach procedure
STATUS	显示 CPE 连接状态 Includes CPE connection status
PM	周期性统计信息，主要包括 CPE 信号强度，流量统计等 Periodic Monitor Logs such as signal strength and flow statistics
NAS	显示 NAS 信令 NAS signaling during attach
RRC	显示 RRC 信令 RRC signaling during attach

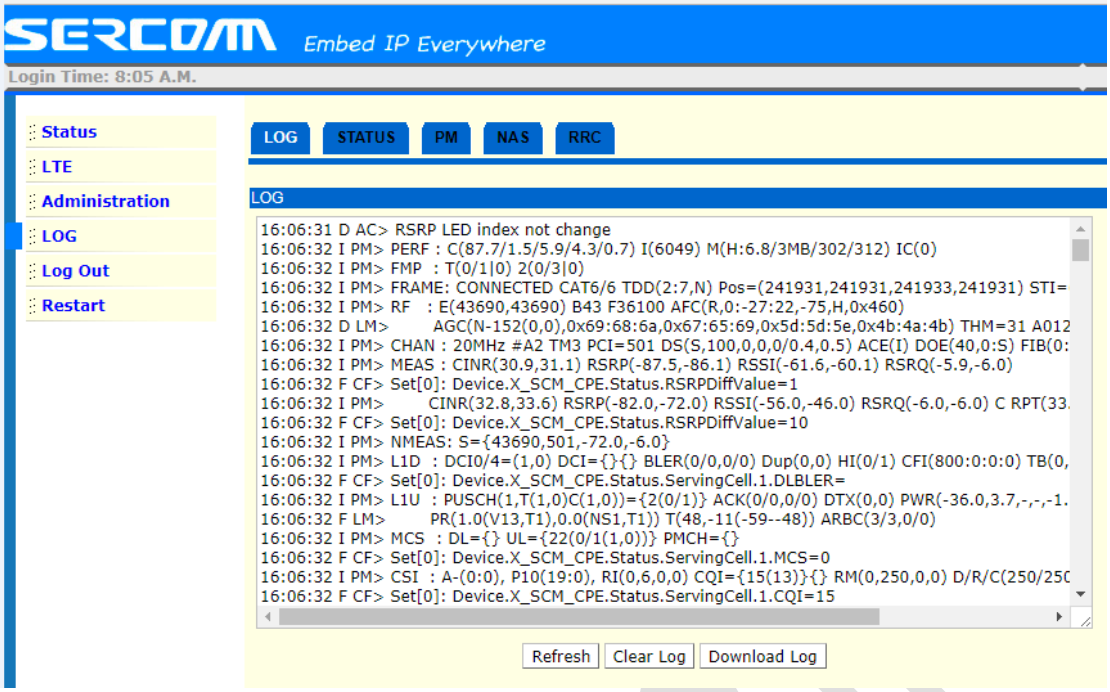


Fig 4-1 CPE Logs

4.2.通过页面下载 CPE 全部日志

Download CPE logs by GUI

（4）（1）PC 需要 fix IP: 10.10.2.2，不要指定网关地址；

Fix 10.10.2.2/24 to PC , no Gateway address be assigned .

（2）登录到 CPE 的页面: HTTPS://10.10.2.254 (用户名: admin 密码: admin);

Open your web browser and visit device .

（3）点击 LOG 按钮;

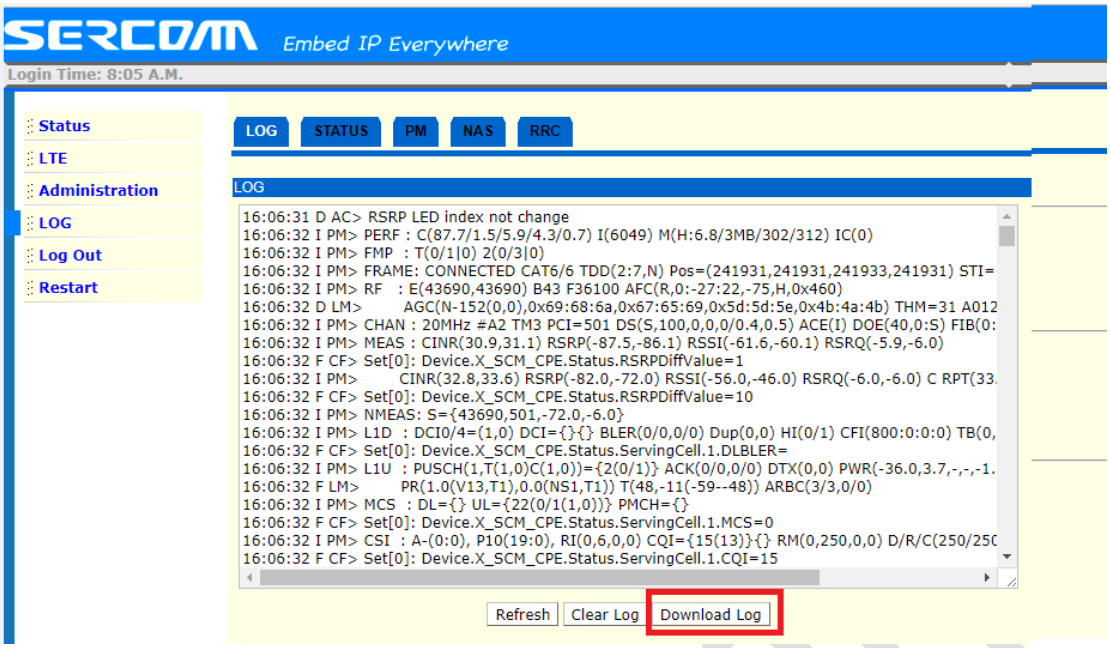
Click the Administration.

（4）点击 Download Log 按钮下载日志;

Click the Download Log to download log.

（5）运行批处理文件解压解密日志，生成日志。

Run win_unpackage.bat on Windows OS to generate unzip logs.



Fix 4-2 Download CPE Logs

5.故障定位与处理

Troubleshooting and Handling

本章主要阐述如何对 CPE 进行故障处理，可以从两个方面对 CPE 进行故障问题定位，分别是通过 LTE 连接状态定位问题和通过日志分析定位问题。

This chapter mainly described how to troubleshooting, we can get the suspicious point from LTE connection status and log analysis .

5.1.LTE 连接状态分析

Check LTE Connection Status

当 CPE 发生上线故障时，可以通过获取健康节点的值来分析 CPE 上线故障，1.3 章节中获取的 Status Cause 就是该节点的值，健康节点可以显示的过程定义如下：

When CPE attach failed, you can get the reason why CPE attach failed through HealthCheck value which illustrated in chapter 1.3, the value of the HealthCheck is defined as follows:

i. InitialModule
ii. USIMChecking
iii. ConfigChecking
iv. Detaching
v. NetworkSearching
vi. Attaching
vii. PDNActiving
viii. Established

当某个过程正常完成时，会在该过程名称后面加上 Success 的标示，如果该过程出错，则在该过程名称后面加上出错原因。以下三个小节分别对容易出错的三个过程（USIMChecking、NetworkSearching、Attaching）进行了错误分析。

When a process is normally complete, “success” will be added to tail of the that step , else a error cause will be added . The following three chapters define the detail of the possible error in in step USIMChecking, NetworkSearching, and Attaching.

5.1.1 USIM Checking 错误分析

USIM Checking Error analysis

该小节主要是对 USIM 的检查，如果检查不通过，则会产生 CME Error。CME Error 的定义参考附录 C.

The section is primarily check USIM, and CME Error is generated if the check fail. Please refer to the appendix C about the definition of CME Error..

5.1.2 Network Searching 错误分析

Network Searching Error

扫网失败，失败的原因主要有以下两类，其他的根据提供的错误码直接参考附录 A：

The are two mainly cases which may cause the network searching failure , and please get the right reason by searching the error code in appendix A .:

A.设置了主辅频点，但是设定频点的小区在环境中并不存在。

A. A frequency is set but any cell in such frequency be broadcast nearby in the environment.

这个问题需要检查是否配置主辅频点，若有设置，请确定设置的主辅频点环境中是否存在。

In this case , please double confirm you've set with a right frequency .

B.周围并没有可用的小区存在，导致扫描不到网络。

No cell available nearby , which causes network searching failed.

5.1.3 Attaching 错误分析

Attach Error

目前将 PDN 激活的过程合并到 Attach 的过程，因此这个过程出现故障的原因主要为 Attach 失败和 PDN Active 失败。

The procedure of the PDN activation can be separated into two steps : network attach and PDN active, the failure cause of this sub-procedure can be found by searching error code in appendix B .

（1）Attach 失败（结果定义参考附录 B）：

Attach failure (reference appendix B) :

Attach 失败比较常见的原因就是被 MME 拒绝接入。这种情况一般都是扫到并尝试驻留的小区没有注册过设备使用的 USIM 卡，这种情况在 Cause 的结果中显示 EMM 值为 129。另外一种情况是，要驻留的小区状态出现异常，或者信号出现异常，导致 RRC 不能正常建立成功，这种情况在 Cause 的结果中显示 EMM 值为 138.

The most familiar attach failure is reject by MME. A unregistered USIM could be the main reason , in this case , you can see error code “EMM 129”. Another familiar case is something wrong with the Cell which CPE is trying to attach , the error code is “EMM 138”.

（2）PDN Active 失败

PDN Active failure

该种情况主要分析 EMS 的 cause，可以参考 3GPP TS 24.301 Annex B.

Could refer to Annex B (it is copied from 3GPP TS24.301)

5.2.LTE 无线质量分析

CPE Wireless Quality

CPE 出现丢包率高、速率上不去等问题时，往往是因为无线质量导致。LTE 无线质量可根据 PM 日志来进行分析，PM 日志获取方法可以参考第 4.2 章节，fig 5-1 反应了一个完整周期的 PM 日志。后续的 3 个小节简单描述了如何通过一个完整 PM 周期的日志获取需要

的信息。

Bad radio quality can cause the high drop rate , low data rate etc. We can get the radio quality of the environment by analysis PM log. You can refer to chapter 4.2 to get PM log, and as shown in fig 5-1 is a full cycle of PM logs. The following three chapter simply describe how to get KPI information through a full PM cycle.

```
06:38:49 I PM> PERF : C(74.7/1.2/9.9/12.7/1.4) I(6859) M(H:25.4/5MB/423/458) IC(0)
06:38:49 I PM> FMP  : T(0/3|0) P(0/1|0) 2(0/43|0)
06:38:49 I PM> FRAME: CONNECTED CAT6 FDD(N) Pos=(479865,479865) STI=2170
06:38:49 I PM> RF   : E(200,18200) B1 F21300 AGC(N,0x7e:7c:7f,0x6b:69:6c) AFC(R,0:-45:27,-98,H,0x450) THM=119
06:38:49 I PM> CHAN : 10MHz #A2 TM3 PCI=123 DS(S,300,0,0,0/0.9,0.9) ACE(A) DOE(180,0:S) FIB(0:0) CS(9:9)
06:38:49 I PM> MEAS : CINR(6.0,9.7) RSRP(-94.2,-84.4) RSSI(-67.1,-58.0) RSRQ(-10.1,-9.4) C     2
06:38:49 I PM> NMEAS: {1250,138,-83.5,-7.5} {200,123,-84.0,-9.5}
06:38:49 I PM> L1D  : DCI0/4=(599,0) DCI={2A(0/6)}{} BLER(0/6,0/0) Dup(0,0) HI(0/599) CFI(2777:223:0:0) TB(0,0) DRX(0:0:0) TP=1K
06:38:49 I PM>        Layer-Map={1C1L=6,1C2L=0,2C2L=0,2C3L=0,2C4L=0}, ARBC={21/0}                                    4
06:38:49 I PM> L1U  : PUSCH(599,T(599,0)C(599,0))={0(0/299),5(0/300)} ACK(0/0,0/0) DTX(0,0) PWR(-29.0,-16.9,-,-,-19.9) TP=179K
06:38:49 I PM> MCS  : DL={9(0/1),11(0/1),12(0/4)} UL={22(0/599(599,0))} PMCH={}
06:38:49 I PM> CSI  : RM(0,0,3000,0) A30(0), P10(600), D/R/C(2571/3000/3000) PRE(2400/3000)
06:38:49 I PM>        RI(38,0,0,0) PMI={}{}{} CQI={11(48),12(514)}{}
06:38:49 I PM> TP   : PHY(1K:179K) MAC(1K:179K) RLC(270:270) PDCP(252:258) DIM(5:252)) IPC(252:0/252)  6
06:38:49 I PM> MAC  : [S] PDU=D{6},U{599(599,0,0,599)}
06:38:49 I PM>        [CE] D{PAD(0/6)},U{PHR(3)(0:62,),BSR(0/6/593)(0,0,0,0),SR(0/1),PAD(0/599)},I{0,0,0}
06:38:49 I PM> RLC  : [3] PDU=D{A3/0,C3},U{A0/3,C3},I{O(0,0),E(0),R(0,0)},STATE=D{905,905},U{1010,1010}
06:38:49 I PM> PDCP : [3:5] PDU=D{3/3,0},U{0/3/3/0,0},I{W(0,0),T(0)},STATE=D{65,3438,3437},U{63,2186}
06:38:49 I PM> DP   : RLC=D0{DC0,AF0,UF0} IPC=D{F0,M0,T3},U{A0,M0,T3}
06:38:49 I PM> CIP  : S=3 DL(3,1) UL(3,1) DI(118,118,118) DO(118,118,118) UI(14,14,14) UO(14,14,14) B(0,0)
06:38:49 I PM> [SCC]FRAME: CC1 ACT=0 FDD(N) Pos=(479869,479869) STI=2170
06:38:49 I PM> [SCC]RF   : E(1250,65535) B3 F18100 AGC(N,0x6a:6a:6b,0x73:72:73)
06:38:49 I PM> [SCC]CHAN : 10MHz #A2 TM3 PCI=138 DS(S,300,0,0,0/1.0,1.1) ACE(A) DOE(70,0:S) FIB(0:0) CS(9:9)
06:38:49 I PM> [SCC]MEAS : CINR(13.7,9.8) RSRP(-83.7,-88.1) RSSI(-59.4,-63.3) RSRQ(-7.3,-7.8) C     3
06:38:49 I PM> [SCC]L1D  : DCI0/4=(0,0) DCI={}{} BLER(0/0,0/0) Dup(0,0) HI(0/0) CFI(0:0:0:0) TB(0,0) DRX(0:0:0) TP=0
06:38:49 I PM> [SCC]       Layer-Map={1C1L=0,1C2L=0,2C2L=0,2C3L=0,2C4L=0}, ARBC={0/0}                                5
06:38:49 I PM> [SCC]L1U  : PUSCH(0,T(0,0)C(0,0))={} ACK(0/0,0/0) DTX(0,0) PWR(-,-,-,-,-) TP=0
06:38:49 I PM> [SCC]MCS  : DL={} UL={} PMCH={}
06:38:49 I PM> [SCC]CSI  : A30(0), P10(0), D/R/C(0/0/0) PRE(0/0) RI(0,0,0,0) PMI={}{}{}
06:38:49 I PM> [SCC]       CQI={}{}
```

1

Fig 5-1 a full cycle of PM logs

5.2.1 CPE 信号强度分析

CPE Signal Strength

在 fig 5-1 标记为 2 和 3 的红色框中，分别可以看到小区的信号强度各个指标（CINR,RSRP,RSSI）的具体数值，括号中有两个数值表示 CPE 有两根天线，两个值分别与两根天线相对应，其中包含“[SCC]”字样的为辅载波小区信号强度，各个指标的参考数值如下所示：

Marked with “2” and “3” in the red area in fig5-1, we can see the values of CINR, RSRP and RSSI, in parentheses, there are two value meas CPE has two antennas, two values correspond to two antennas respectively, "[SCC]" meas secondary carrier , the various indicators of reference values as shown below:

CINR - 这里的 CINR 等效于 SINR，一般要求 CINR 需要大于 17dB，如果低于 17dB，则可能会导致上下行的误码率偏高，致使传输效率降低，如传输速率达不到预期目标，丢包率严重等现象。

CINR - the CINR equivalent SINR, CINR needs more than 17 db, if less than 17 db, maybe lead to CPE UL/DL BLER rising, resulting in reduced the transmission efficiency, such as transmission is lowly or packet loss is .highly.

RSRP - 建议值是大于-95dBm，RSRP 用于指示小区的有效功率情况，相对较弱的小区信号不利于空口的传输效率。所以如果信号低于预期值，则建议排查环境.

RSRP - the recommended value is greater than -95dbm, RSRP is used to indicate the effective power of the eNodeB, and the relatively weak signals are bad for the transmission in air. So if the signal is below the expected value, please check the environment.

- 确保设备的天线对准了宏基站

- make sure the antenna is aligned with the Cell

- 确认设备到宏基站之间尽量是无阻挡，特别是没有金属遮挡，必要的时候需要调整设备位置，确保设备满足的 RSRP 满足要求。

- confirm there is no barrier between the device and Cell, especially no metal barrier. To ensure the device meet the RSRP requirements , adjusting the location is necessary sometimes .

- 确认设备到宏基站之间的距离是合理的，以手机用户为例，如果在该位置处放置手机，手机能够正常上网以及通话正常。

- confirm a reasonable distance between the device and Cell, you can simply determine by a commercial mobile phone, if mobile phone works well at that place , it means the distance should be reasonable.

RSSI - 建议值是 -75dBm 到 -55dBm ，反映的是当前环境下该频点上的总信号强度。。

RSSI - the recommended value is -75dBm to -55dBm .

在我们的实践过程中，RSRP 和 RSSI 这两个指标往往是需要结合起来分析的，有一种比较简单的做法是，我们可以引入误码率进行二次分析，正常情况下上行或下行的误码率不应该长期占据在协议规定的极限位置 10%，从实验室的调测数据来看，通过调整设备角度，设备和基站距离，基站发射强度等是可以有效控制误码率的，建议误码率需要能够降低到 5%以内，误码率的查看可以参考 5.2.2 小节 CPE 误码率分析。

Most of time ,RSRP and RSSI are often taken into analysis together , but it seems not a easy work, there is a simple way we can follow, analyze the BLER . UL BLER or DL BLER should not be occupied for a long time in the degree of the maximum value - 10%, our experiences show that antenna angle, distance , TX power of cell can take effect to the BLER . The recommended value of BLER less than 5%. You can refer to chapter 5.2.2 to analyze BLER..

5.2.2 CPE 误码率分析

CPE BLER

在 fig 5-1 标记为 4 和 5 的红色小框中，可以对误码率进行统计，“[SCC]”字样表示辅载波频点信息，其中 BLER 指示下行误码率，HI 指示上行误码率。BLER 和 HI 格式如下：

Label “4” and “5” in the red area in fig 3-1, you can get BLER information, "[SCC]" meas secondary carrier, BLER shows download BLER, HI shows upload BLER. The BLER and HI formats are as follows:

BLER (P1 / P2, P3 / P4)　HI (P5 / P6)

BLER (P1 / P2, P3 / P4)　HI (P5 / P6)

P1: CW0 信道上的坏块数

P1: the number of bad blocks on the CW0 channel

P2: CW0 信道上总的码块数
P2: the total number of blocks on the CW0 channel

P3: CW1 信道上的坏块数
P3: the number of bad blocks on the CW1 channel

P4: CW1 信道上总的码块数
P4: the total number of blocks on the CW1 channel

P5: 上行信道上的坏块数
P5: the number of bad blocks on the upload channel

P6: 上行信道上总的码块数
P6: the total number of blocks on the upload channel

上行误码率和下行误码率的计算方法如下：
The calculation of DL BLER and UL BLER as follows:

下行误码率: (P1 + P3)/(P2 + P4) * 100%
DL BLER: (P1 + P3)/(P2 + P4) * 100%

上行误码率：P5 / P6 * 100%
UL BLER: P5 / P6 * 100%

5.2.3 CPE RI 分析

对速率影响比较大的除了信号质量，还有 RI 值，在支持 MINO 的环境下，如果 RI 值一直无法超过 1 的话，那么设备实际上是工作在 single 模式下，这个时候其能够提供的速率将会受到明显的限制（最高为理论速率的一半）。

5.2.4 CPE 流量分析

CPE Throughput

在 fig 5-1 标记为 6 的红色小框中，可以对不同分层的流量进行统计，日志格式如下：
Label “6” in the red area in fig 3-1, you can count the traffic flows of different layers, and the log format is as follows:

PHY/MAC/RLC/PDCP/IPC(P1,P2)
PHY/MAC/RLC/PDCP/IPC(P1,P2)

P1：下行速率
P1：download throughput

P2：上行速率
P2：upload throughput

5.2.5 CPE 指标趋势分析

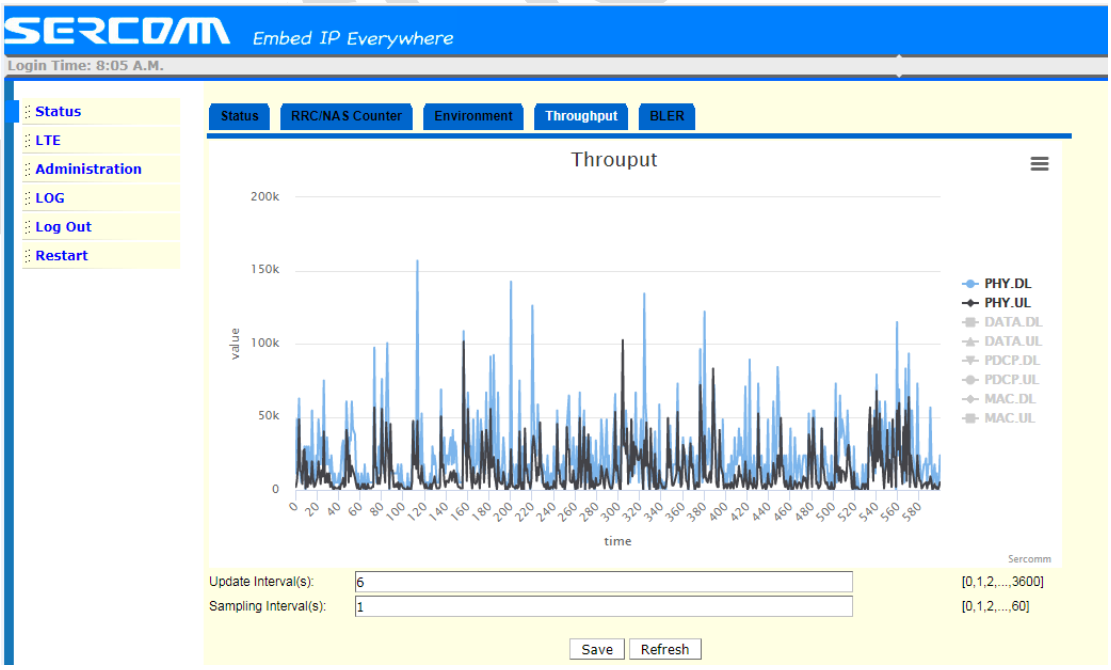
CPE 近端提供各种无线指标的趋势透视图，使用者可以通过这些趋势图结合自己的经

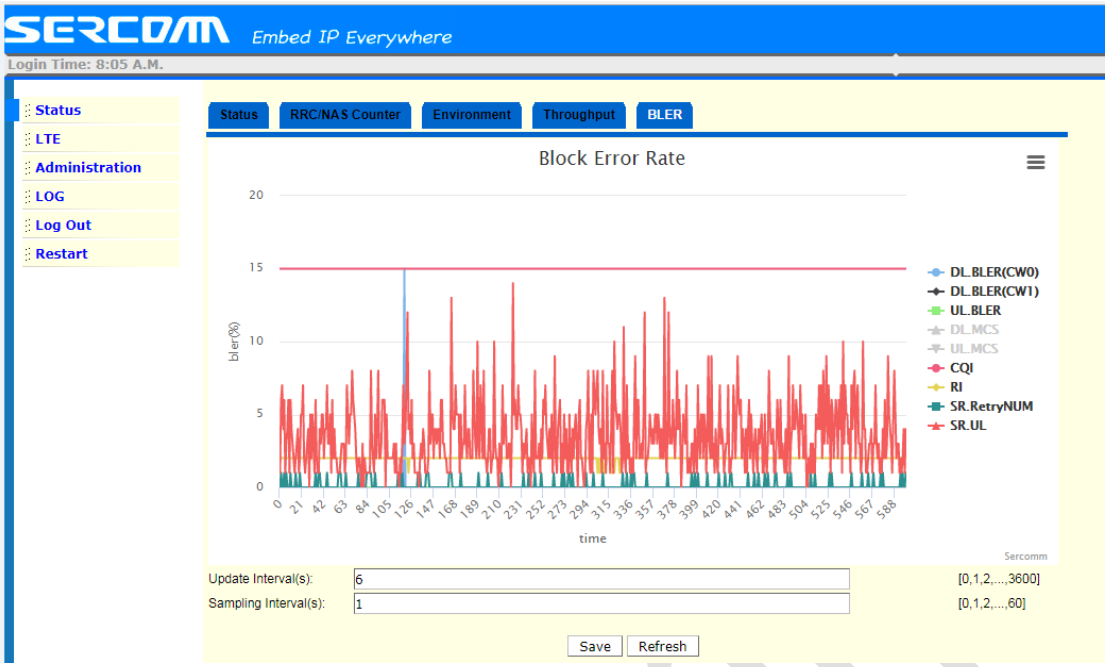
验经一步的定位当下环境中可能存在的问题。

该设备提供三类趋势分析，分别是无线环境（environment），流量（throughput）以及误码率（BLER）

在使用近端指标趋势分析的时候，需要先配置更新周期以及采样周期。一般更新周期设定为 6 即可，采样周期设备为 1 或者 3。

Web page in CPE supports LTE signal related parameters for connection quality analysis. They can be found from Status/Environment, Throughput, and BLER





5.3.LTE 信令分析

LTE signaling

5.3.1 NAS 信令分析

NAS signaling

在 info 日志中可以看到 CPE 的 NAS 信令，可以根据关键词“LM> TYPE: ”对 NAS 信令进行检索，fig 5-2 为一份 info 日志检索出来的 NAS 信令：

In the info log , the NAS signaling of CPE is placed, according to the keywords "LM > TYPE:" to you can retrieve the NAS signaling, figure 5-2 is the NAS signaling retrieved from Info log:

```
07:58:18 I LM>      TYPE: EMM_ATTACH_REQUEST
07:58:19 I LM>      TYPE: EMM_AUTHENTICATION_REQUEST
07:58:19 I LM>      TYPE: EMM_AUTHENTICATION_RESPONSE
07:58:19 I LM>      TYPE: EMM_SECURITY_MODE_COMMAND
07:58:19 I LM>      TYPE: EMM_SECURITY_MODE_COMPLETE
15:59:00 I LM>      TYPE: EMM_ATTACH_ACCEPT
15:59:00 I LM>      TYPE: EMM_ATTACH_COMPLETE
```

Fig 5-2 NAS signaling

当在 NAS 信令中看到异常（比如出现 FAIL 字样、REJECT 字样等），则需要查看该信令打印时间点附近的 info 日志，判断发生异常的原因，假如 info 日志不足以确定异常发生的原因，需要将 log 级别开到 debug 级别。

When negative keyword (such as FAIL, REJECT, etc.) presents in the log , you will need to

analyze the signaling in the context of the issue point to find out the cause of the exception, if the info log is not sufficient to find out the cause of the exception occurs, will need to set log to debug level.

RRC 信令主要有以下过程：

The RRC signaling mainly has the following procedures:

（1）Attach 流程

The Attach process

EMM_ATTACH_REQUEST
EMM_ATTACH_ACCEPT
EMM_ATTACH_COMPLETE
EMM_ATTACH_REJECT

（2）业务请求流程

Business request process

EMM_SERVICE_REQUEST
EMM_SERVICE_REJECT

5.3.2 RRC 信令分析

RRC signaling

在 info 日志中可以看到 CPE 的 RRC 信令，可以根据关键词“LM> message c1 ：”对 RRC 信令进行检索，fig 5-3 为一份 info 日志检索出来的部分 RRC 信令：

In the info log can see RRC signaling of CPE, you can according to the keywords "LM > message c1:" to retrieve the RRC signaling, figure 5-3 is the part RRC signaling retrieved from info log

```
07:58:18 I LM>   message c1 : rrcConnectionRequest :
07:58:18 I LM>   message c1 : rrcConnectionSetup :
07:58:19 I LM>   message c1 : rrcConnectionSetupComplete :
15:59:00 I LM>   message c1 : securityModeCommand :
15:59:00 I LM>   message c1 : securityModeComplete :
15:59:00 I LM>   message c1 : rrcConnectionReconfiguration :
15:59:00 I LM>   message c1 : rrcConnectionReconfigurationComplete :
15:59:00 I LM>   message c1 : rrcConnectionReconfiguration :
15:59:00 I LM>   message c1 : rrcConnectionReconfigurationComplete :
16:32:14 I LM>   message c1 : rrcConnectionRelease :
```

Fig 5-3 RRC signaling

当在 RRC 信令中看到异常（比如出现 fail 字样、reject 字样等），则需要查看该信令打印时间点附近的 info 日志，判断发生异常的原因，假如 info 日志不足以确定异常发生的原因，需要将 log 级别开到 debug 级别。

When see anomalies in RRC signaling (such as fail, reject, etc.), you will need to analyze the signaling in the context of the problem point to find out the cause of the exception, if the info log is not sufficient to find out the cause of the exception occurs, you will need to set log to debug level.

RRC 信令主要有以下过程：

The RRC signaling mainly has the following procedures:

（1）RRC 建立流程

RRC Establishment Process

rrcConnectionRequest

rrcConnectionSetup

rrcConnectionSetupComplete

（2）RRC 重配流程

RRC Reconfiguration Process

rrcConnectionReconfiguration

rrcConnectionReconfigurationComplete

（3）RRC 重建流程

RRC Reestablishment Process

rrcConnectionReestablishmentRequest

rrcConnectionReestablishment

rrcConnectionReestablishmentComplete

rrcConnectionReestablishmentReject

高级维护

Advanced Management

6.测试

Test

6.1.iperf 下行测试

iperf download test

（1）PC 通过 dhcp 的方式获取 IP （假设拿到了 10.10.2.10 的 IP）；
The PC gets the IP via DHCP (assuming the IP is 10.10.2.10).

（2）telnet/console 的方式登录 10.10.2.254；
Telnet to 10.10.2.254.

（3）执行 iptables -t nat -I PREROUTING -i lte0pdn0 ! -p icmp -j DNAT --to 10.10.2.10；
Perform iptables -t nat -I PREROUTING -i lte0pdn0 ! -p icmp -j DNAT --to 10.10.2.10.

（4）执行 iptables -A FORWARD -d 10.10.2.10 -j ACCEPT；
Perform iptables -A FORWARD -d 10.10.2.10 -j ACCEPT.

（5）在 PC 上运行 iperf -s -u -i 1 （iperf UDP server）；
Run the iperf-s-u-i 1 (iperf UDP server) on the PC.

（6）SSH 到 PGW 并运行 iperf -c 192.168.200.2 -u -b 100M -i 1 -t 9999 (192.168.200.2 为 lte0pdn0 上的 IP，可以在 10.10.2.254 上使用 ifconfig 命令查看)。
SSH to the PGW and run the iperf-c 192.168.200.2-u-b 100M - I 1-t 9999 (IP on lte0pdn0, available on 10.10.2.254);

测试方法

1. SSL test

1.1 cpe 与 femto 板间测试

Femto 连接 HeMs，cpe IP: 11.11.111.18，femto IP: 11.11.111.17

1.1.1 SSL CML Agent

（一）Get Parameter

获取参数值有两种，分别是 femto 板子内通过 femto_cli 获得，和网管获取。

TestMethod	femto_cli　get Device.X_SCM_CPE.Status.Hardware.IMEI
Test Result	成功获取 IMEI

TestMethod	1.在网管上找到设备 ID，右击选择 configuration 2.在 Device Method 一栏，进入 GetParameterValues 页面，在页面的右侧输入所要获取的参数节点名 Device.X_SCM_CPE.Status.Hardware.IMEI， 点击 GetParameterValues，获取 value 值
Test Result	成功获取 IMEI 从日志可以看到，获取 value 值流程为： Get_permission -> get_datatype -> get_attr -> get

（二）Set Parameter

配置参数值有两种，分别是 femto 板子内通过 femto_cli 配置，和网管配置。

Method　1	femto_cli　set　Device.X_SCM_CPE.Status.Hardware.IMEI=aaaa
Test Result	成功设值 IMEI set 流程：writable check -> TR069_set
备注	femto_cli 执行 set 时，只有 cpe 侧节点 permission 为 5 的才能设值成功； femto_cli 执行 sset 时，对 cpe 侧任何节点都能设值成功；

Method 2	1.在网管上找到设备 ID,右击选择 configuration 2.在 Device Method 一栏，进入 SetParameterValues 页面，在页面的右侧点击 edit，输入所要获取的参数节点名及 value 值（如 Device.X_SCM_CPE.ModuleConfigMgmt.PLMN.SecEARFCN.4.SecondaryEARFCN），页面最下面点击 SetParameterValues
Test Result	设值成功 从日志可以看到，set 流程为： Get_permission(permission 为 5 才会被设值) -> get_attr -> get(检查当前设的值与原来的值是否一样，如果一样则不去 set) -> TR069_set

（三）ValueChange

TestMethod	1.cmld_client　set　Device.X_SCm_CPE.Status.UpgradeState=1 2.在网管上找到设备 ID，右击选择 configuration 3.进入 Alarm -> Device Current Alarm，等待一会即可看到 alarm
Test Result	在 Device Current Alarm 页面看到 20007 告警

（四）Traversing the tree

网管爬树有两种，一是点击 Download Datamodel 进行爬树，二是

点击 GetParameterNames 进行爬树

Method 1	在 Device Method 一栏，点击 Download Datamodel -> confirm
Method 2	在 Device Method 一栏，选择 GetParameterNames，在右侧的 paramter path 输入 Device.后点击 GetParameterNames
Test Result	返回 download success

1.1.2 SSL File Agent

（一）Download/Upload Config

① Upload Config to Femto

TestMethod	1.在网管上找到设备 ID，右击选择 configuration 2.在 Device Method 一栏，进入 Upload CFG File 页面，在页面的右侧点击 Upload，等待一段时间后 refresh 页面
Test Result	可以在当前页面看到获取的 configuration file，文件名为 device id

② Download Config to CPE

TestMethod	1.找到设备 ID，右击选择 configuration 2.在 Device Method 一栏，进入 Device Upgrade 页面，在页面右侧的 file type 选择 configuration file，选择 restore 的配置文件，点击 upgrade ※为了确保 restore 成功，可以先修改节点的值保存后再进行第二步
Test Result	Restore config 成功，板子重启

（二）Upload log

日志上传分为网管主动要 cpe 日志和 cpe 日志满了后触发 valuechange 上传日志，但发 valuechange 给 femto 后，femto 会通知 HeMs 来取日志，但最终 HeMs 是否来取日志则由 HeMs 决定，因此，cpe 日志满了只是发一条 valuechange 而不管最终日志是否被上传到网管。

HeMs get cpe log	1.在网管上找到设备 ID，右击选择 configuration 2.在 Device Method 一栏，进入 Upload Log File 页面，如果立刻上传日志，则点击 Upload now，等待一段时间后 refresh 页面；如果需要周期性上传，则在当前页面上配置完周期后，点击 start periocdic 即可
Cpe logfull	Cmld_client set Device.X_SCM_CPE.ActionMgmt.LogFull=1
Test Result	网管上看到名为 Log_XXX_cpe_XXX.zip 文件

（三）FW Upgrade

HeMs get cpe log	1.在网管上找到设备 ID，右击选择 configuration 2.在 Device Method 一栏，进入 Device Upgrade 页面，在页面右侧的 file type 选择 upgrade file，选择升级的 MultiPkg(或 single cpe fw)文件包，点击 Upgrade
Test Result	升级成功，板子重启

1.2 cpe 板内自测

测试准备：

如果与 ssl 相关的可执行程序被修改过，把新编译的测试程序放在/tmp/ftp 下，用到的可执行文件为：

cmld_client, cmld, libcml_api.so, (cml 相关)

act_mod, （valuechange 模块）

ssl_agent, ssl_test, libscm_ssl.so （ssl_agent 模块）

测试 ssl 通道，运行脚本 start_ssl.sh，脚本内容为：

```
LD_LIBRARY_PATH=. ./cmld /tmp/nv/nvram.xml &
LD_LIBRARY_PATH=. ./act_mod &
LD_LIBRARY_PATH=. ./ssl_agent -f /etc/.ssl_certs/ca.cert -s /etc/.ssl_certs/server.cert -k /etc/.ssl_certs/server.key -c /etc/.ssl_certs/client.cert -l /etc/.ssl_certs/client.key -m -g -d
```

127.0.0.1 -p 8888 &

※ 如果 cmld 及 act_mod 没有被修改过且进程存在，则不需要再重新起该进程。

在起 ssl_agent 时，client 与 server 可使用同一个证书，即-c -l 参数可带可不带。

下面附上各个参数的含义，如下：

```
printf("Usage: [OPTION] -c <Certificate> -k <PrivateKey>\n\n");
printf("\t-f <CA>          \tSpecify CA path and filename\n");
printf("\t-s <Certificate>\tSpecify certificate file of server\n");
printf("\t-k <PrivateKey> \tSpecify private key file of server\n");
printf("\t-c <Certificate>\tSpecify certificate file of client\n");
printf("\t-l <PrivateKey> \tSpecify private key file of client\n");
printf("\t-m               \tVerify client certificate, need CA and client certificate, privatekey if enable this option\n");
printf("\t-g               \tEnable recv file service\n");
printf("\t-h               \tHelp\n");
```

ssl 成功建立后，进行接下来的测试，如果 ssl 连接成功，日志如下：

16:40:57 I SSLAGNT> Conection from 127.0.0.1:dbae

16:40:58 D SSLAGNT> Peer Info: /C=CN/ST=JiangSu/O=Sercomm/OU=Sercomm/CN=Client

16:40:58 D SSLAGNT> Peer Info: /C=CN/ST=JiangSu/O=Sercomm/OU=Sercomm/CN=Server

16:40:58DSSLAGNT>Peer Issuer:/C=CN/ST=JiangSu/L=SuZhou/O=Sercomm/OU=Sercomm/CN=CA

16:40:58 I SSLAGNT> Conected to server 127.0.0.1:22b8, after 0times

16:40:58DSSLAGNT>Peer Issuer:/C=CN/ST=JiangSu/L=SuZhou/O=Sercomm/OU=Sercomm/CN=CA

通过 wireshark 抓包得到 ssl 建立握手连接过程：

No.	Time	Source	Destination	Protocol	Length	Info
18	6.813195168	127.0.0.1	127.0.0.1	TLSv1.2	371	Client Hello
20	6.816130656	127.0.0.1	127.0.0.1	TLSv1.2	2062	Server Hello, Certificate, Certificate Request, Server Hello Done
22	6.843849126	127.0.0.1	127.0.0.1	TLSv1.2	2535	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
24	6.867785213	127.0.0.1	127.0.0.1	TLSv1.2	1236	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

1.2.1 SSL CML Agent

（一）Get Parameter

TestMethod	cmld_client get Device.X_SCM_CPE.Status.Hardware.IMEI -s
Test Result	成功获取 IMEI

（二）Set Parameter

TestMethod	cmld_client set Device.X_SCM_CPE.Status.Hardware.IMEI=aaa -s
Test Result	成功设置 IMEI 为 aaa

（三） ValueChange

TestMethod	cmld_client set Device.X_SCm_CPE.Status.UpgradeState=1 -s
Test Result	成功发送 20007(FW upgrade failure)告警到 ssl peer

1.2.2 SSL File Agent

ssl_test help:

```
printf("Usage: [OPTION] -d <DestIP> -e <Action> -c <Certificate> -k <PrivateKey> -f <File>\n\n");
printf("\t-d <DestIP>     \tSpecify remote server\n");
printf("\t-e <action>     \tSpecify action, 0-Upload FW, 1-Download Cfg, 2-Upload Cfg, 3-Download Log, 4-Security Log, 5-Running Log, 6-Debug Log\n");
printf("\t-f <File>       \tSpecify filename to send or store\n");
printf("\t-a <CA>         \tSpecify CA path and filename\n");
printf("\t-c <Certificate>\tSpecify certificate file of client\n");
printf("\t-l <PrivateKey> \tSpecify private key file of client\n");
printf("\t-h              \tHelp\n");
```

（一）Fw Upgrade

TestMethod	./ssl_test -d 127.0.0.1 -a /etc/.ssl_certs/ca.cert -c /etc/.ssl_certs/client.cert -l /etc/.ssl_certs/client.key -f /tmp/ftp/*.bin -e 0
Test Result	tail -f /var/cgitest 查看升级日志，升级成功

（二）Download Config to CPE

TestMethod	./ssl_test -d 127.0.0.1 -a /etc/.ssl_certs/ca.cert

	-c /etc/.ssl_certs/client.cert -l /etc/.ssl_certs/client.key -f /tmp/ftp/cpe_cfg.zip -e 2
Test Result	在/tmp/ftp 路径下存在配置文件 cpe_cfg.zip

（三）Upload Config to Femto

TestMethod	./ssl_test -d 127.0.0.1 -a /etc/.ssl_certs/ca.cert -c /etc/.ssl_certs/client.cert -l /etc/.ssl_certs/client.key -f /tmp/ftp/cpe_cfg.zip -e 1
Test Result	在/tmp/ftp 路径下存在配置文件 cpe_cfg.zip

（四）Upload log

TestMethod	LD_LIBRARY_PATH=. ./ssl_test -d 127.0.0.1 -a /etc/.ssl_certs/ca.cert -c /etc/.ssl_certs/client.cert -l /etc/.ssl_certs/client.key -f /tmp/ftp/log.zip -e 3
Test Result	在/tmp/ftp 路径下存在日志文件 log.zip

2. SAS Test

2.1. 升级 FW、恢复厂设置以及 SAS 配置

升级 FW 请参考 3.1 节“CPE 升级方法”。

恢复出厂设置请参考 2.5 节“恢复出厂设置”。

SAS 配置请参考 2.7 节“SAS 相关参数配置”，通过页面进行配置。

2.2. 如何登入到板子里面

可通过 SSH 的方式登入到板子里面，相关信息如下：

protocol: SSH2

Hostname: 10.10.2.254

username: root

password: sercomm.cd1

2.3. SAS 怎么测

与不同的 SAS Server 进行测试时，使用的测试用例不同，但测试方法基本相同，具体可参考开发手册中 SAS 部分的内容。关于 SAS 测试的详细步骤及内容，可参考相关测试用例文档（可以从 SAS 开发组的同事获得）。

2.4. 查看 sasd 的 log

查看 sasd 的 log 有两种方式：通过访问 GUI，通过页面下载或者登入到板子里，通过命令进行查看。

关于如何通过页面下载 log，可参考 4.2.节“通过页面下载 CPE 全部日志”。

如果需要动态查看日志，可以登入到板子里，并通过以下命令查看：

```
tail -f /var/log/messages | grep ‘sas’ -i
```

2.5. sasd 的 log 分析

由于对 sasd 的 log 的分析，还没有具体的文档或资料，所以如果在进行 SAS 测试时遇到了问题，可以请 SAS 的开发组的同事帮忙分析。

2.6. 通过命令行对 SAS 相关参数进行设置

对 SAS 相关参数的配置有两种方法：通过 GUI 进行配置或者登入到板子里面，通过命令的方式进行设置。

通过 GUI 进行配置的方法，可参考 2.7 节“SAS 相关参数配置”。

登入到板子里面，在命令行中可使用 cmld_client 命令进行设置或查看。

2.4.1. 查看 sasd 相关参数的值

查看当前所有 sasd 参数的值，可使用以下命令：

```
cmld_client show | grep 'sas' -i
```

2.4.2. SAS 调试阶段/SAS IoT

a) 设置 sasd 的 Register 状态和 State 状态

```
cmld_client set Device.X_SCM_CPE.SAS.Registered=0
cmld_client set Device.X_SCM_CPE.SAS.State="Unknown"
```

b) 改变 eirpCapability 的值

通过如下命令增加或减小 MaxTxPower 的值:

```
cmld_client set Device.X_SCM_CPE.ModuleConfigMgmt.MaxTxPower=20
```

附录

Appendix

附录 A：PLMN Search 结果定义

Appendix A: PLMN Search Result

Result	Cause	Display String
0	LAPI_PLMN_SELECT_RESULT_SUCCESS	Success
1	LAPI_PLMN_SELECT_RESULT_FAILURE	NoNetwork
2	LAPI_PLMN_SELECT_RESULT_ABORTED	InternalError
3	LAPI_PLMN_SELECT_RESULT_INVALID_USIM	InvalidUSIM
4	LAPI_PLMN_SELECT_RESULT_ALREADY_IN_PROGRESS	InProgress
5	LAPI_MISMATCH_FREQ_BAND	FreqBandMisatch
6	LAPI_FREQ_LIST_NOT_EXIST	FreqListNotFind
7	LAPI_PLMN_BAND_INVALID_PARAMETER	FreqError

附录 B：ATTACH Response 结果定义

Appendix B: ATTACH Response Result

regResult	regResultOrg	
0 : LAPI_REG_RESULT_SUCCESS	0 :LAPI_REG_RESULT_SUCCESS	Success
1:ATT_FAIL_SERVICE_NOT_ALLOWED_UNTIL_POWER_CYCLE_OR_UICC_REPLACE	3: Illegal UE 6: Illegal ME 7: EPS services not allowed 8: EPS services and non-EPS services not allowed	ServiceLimit-NeedCycle（3GPP EMM Cause:）
2:ATT_FAIL_SERVICE_NOT_ALLOWED_CURRENT_PLMN	11: PLMN not allowed 14: EPS services not allowed in this PLMN	ServiceLimit（3GPP EMM Cause:）
3:ATT_FAIL_SERVICE_IS_LIMITED	12: Tracking area not allowed 13: Roaming not allowed in this tracking area 15: No suitable cells in this tracking area	ServiceLimit-ParametersMismatch（3GPP EMM Cause:）
4: ATT_FAIL_AUTO_RETRY_AFTER_T3402	When the attach attempt counter is equal to 5.	T3402Timeout（3GPP EMMCause：151）
5:ATT_FAIL_OTHERS	All of other cases	Others（3GPP EMM Cause:）

附录 C：CMEError

Appendix C: CMEError

Refer to 3GPP 24.007:section9.2

Numeric	Text
0	phone failure
1	no connection to phone
2	phone-adaptor link reserved
3	peration not allowed
4	operation not supported
5	PH-SIM PIN required
6	PH-FSIM PIN required
7	PH-FSIM PUK required
10	SIM not inserted (See NOTE 1)
11	SIM PIN required
12	SIM PUK required
13	SIM failure (See NOTE 1)
14	SIM busy (See NOTE 1)
15	SIM wrong (See NOTE 1)
16	incorrect password
17	SIM PIN2 required
18	SIM PUK2 required
20	memory full
21	invalid index
22	not found
23	memory failure
24	text string too long
25	invalid characters in text string
26	dial string too long
27	invalid characters in dial string
30	no network service
31	network timeout
32	network not allowed - emergency calls only
40	network personalization PIN required
41	network personalization PUK required
42	network subset personalization PIN required
43	network subset personalization PUK required
44	service provider personalization PIN required
45	service provider personalization PUK required
46	corporate personalization PIN required
47	corporate personalization PUK required
48	hidden key required (See NOTE 2)

49	EAP method not supported
50	Incorrect parameters
51	command implemented but currently disabled
52	command aborted by user
53	not attached to network due to MT functionality restrictions
54	modem not allowed - MT restricted to emergency calls only
55	operation not allowed because of MT functionality restrictions
56	fixed dial number only allowed - called number is not a fixed dial number (refer 3GPP TS 22.101 [147])
57	temporarily out of service due to other MT usage
58	language/alphabet not supported
59	unexpected data value
60	system failure
61	data missing
62	call barred
63	message waiting indication subscription failure
100	unknown
103	illegal MS
106	illegal ME
107	GPRS not allowed
111	PLMN not allowed
112	location area not allowed
113	roaming not allowed in this location area
127	missing or unknown apn
132	service option not supported
133	request service option not subscribed
134	service option temporary out of order
148	unspecified GPRS error
149	PDP authentication fail
150	invalid mobile class
171	last PDN disconnection not allowed
240	PLMN search already progress
241	EPS service not allowed
242	EPS service and non EPS service not allowed
243	APN verification fail
244	Network reject
245	already in progress

NOTE 1: This error code is also applicable to UICC.

NOTE 2: This key is required when accessing hidden phonebook entries.

附录 D：ESM Cause

Appendix D: ESM Cause

附录 E：EMM Cause

Result	Cause
8	ESM_OPERATOR_DETERMINED_BARRING
22	ESM_INSUFFICIENT_RESOURCES
23	ESM_UNKNOWN_OR_MISSING_APN
28	ESM_UNKNOWN_PDN_TYPE
29	ESM_USER_AUTHENTICATION_FAILED
30	ESM_REQUEST_REJECTED_BY_SGWORPGW
31	ESM_REQUEST_REJECTED_UNSPECIFIED
32	ESM_SERVICE_OPTION_NOT_SUPPORTED
33	ESM_REQUESTED_SERVICE_OPTION_NOT_SUBSCRIBED
34	ESM_SERVICE_OPTION_TEMPORARILY_OUT_OF_ORDER
35	ESM_PTI_ALREADY_IN_USE
36	ESM_REGULAR_DEACTIVATION
37	ESM_EPS_QOS_NOT_ACCEPTED
38	ESM_NETWORK_FAILURE
39	ESM_REACTIVATION_REQ
40	ESM_FEATURE_NOT_SUPPORTED
41	ESM_SEMANTIC_ERROR_IN_TFT_OPERATION
42	ESM_SYNTACTICAL_ERROR_IN_TFT_OPERATION
43	ESM_INVALID_EPS_BEARER_ID
44	ESM_SEMANTIC_ERROR_IN_PACKET_FILTERS
45	ESM_SYNTACTICAL_ERRORS_IN_PACKET_FILTERS
46	ESM_EPS_BEARER_WITHOUT_TFT_ALREADY_ACTIVATED
47	ESM_PTI_MISMATCH
49	ESM_LAST_PDN_DISCONNECTION_NOT_ALLOWED
50	ESM_PDN_TYPE_IPV4_ONLY_ALLOWED
51	ESM_PDN_TYPE_IPV6_ONLY_ALLOWED
52	ESM_SINGLE_ADDRESS_BEARERS_ONLY_ALLOWED
53	ESM_ESM_INFORMATION_NOT_RECEIVED
54	ESM_PDN_CONNECTION_DOES_NOT_EXIST
55	ESM_MULTIPLE_PDN_CONNECTIONS_FOR_A_GIVEN_APN_NOT_ALLOWED
56	ESM_COLLISION_WITH_NETWORK_INITIATED_REQUEST
59	ESM_UNSUPPORTED_QCI_VALUE
60	ESM_BEARER_HANDLING_NOT_SUPPORTED
81	ESM_INVALID_PTI_VALUE
95	ESM_SEMANTICALLY_INCORRECT_MESSAGE
96	ESM_INVALID_MANDATORY_INFORMATION
97	ESM_MESSAGE_TYPE_NON_EXISTENT_OR_NOT_INPLEMENTED
98	ESM_MESSAGE_TYPE_NOT_COMPATIBLE_WITH_THE_PROTOCOL_STATE
99	ESM_INFORMATION_ELEMENT_NON_EXISTENT_OR_NOT_IMPLEMENTED
100	ESM_CONDITIOINAL_IE_ERROR
101	ESM_MESSAGE_NOT_COMPATIBLE_WITH_THE_PROTOCOL_STATE
111	ESM_PROTOCOL_ERROR_UNSPECIFIED
112	ESM_APN_RESTRICTION_VALUE_INCOMPATIBLE_WITH_ACTIVE_EPS_BEARER_CONTEXT

Appendix E: EMM Cause

Original REGISTRATION RESULT
0 : LAPI_REG_RESULT_SUCCESS
/* 3GPP EMM Cause */
2 : LAPI_REG_RESULT_REJECT_2_IMSI_UNKNOWN_IN_HSS
3 : LAPI_REG_RESULT_REJECT_3_ILLEGAL_UE
5: LAPI_REG_RESULT_REJECT_5_IMEI_NOT_ACCEPTED
6 : LAPI_REG_RESULT_REJECT_6_ILLEGAL_ME
7 :LAPI_REG_RESULT_REJECT_7_EPS_SERVICES_NOT_ALLOWED
8 :LAPI_REG_RESULT_REJECT_8_EPS_AND_NON_EPS_SERVICES_NOT_ALLOWED
9 : LAPI_REG_RESULT_REJECT_9_UE_ID_CANNOT_BE_DERIVED
10 : LAPI_REG_RESULT_REJECT_10_IMPLICITLY_DETACHED
11 : LAPI_REG_RESULT_REJECT_11_PLMN_NOT_ALLOWED
12 : LAPI_REG_RESULT_REJECT_12_TA_NOT_ALLOWED
13 :LAPI_REG_RESULT_REJECT_13_ROAMING_NOT_ALLOWED_IN_THIS_TA
14 :LAPI_REG_RESULT_REJECT_14_EPS_SERVICES_NOT_ALLOWED_IN_THIS_PLMN
15 :LAPI_REG_RESULT_REJECT_15_NO_SUITABLE_CELLS_IN_THIS_TA
16 :LAPI_REG_RESULT_REJECT_16_MSC_TEMPORARILY_NOT_REACHABLE
17 : LAPI_REG_RESULT_REJECT_17_NETWORK_FAILURE
18 :LAPI_REG_RESULT_REJECT_18_CS_DOMAIN_NOT_AVAILABLE
19 : LAPI_REG_RESULT_REJECT_19_ESM_FAILURE
20 : LAPI_REG_RESULT_REJECT_20_MAC_FAILURE
21 : LAPI_REG_RESULT_REJECT_21_SYNCH_FAILURE
22 : LAPI_REG_RESULT_REJECT_22_CONGESTION
23 :LAPI_REG_RESULT_REJECT_23_UE_SEC_CAPABILITIES_MISMATCH
24 :LAPI_REG_RESULT_REJECT_24_SECURITY_MODE_REJECTED_UNSPECIFIED
25 :LAPI_REG_RESULT_REJECT_25_NOT_AUTHORIZED_FOR_THIS_CSG
26 :LAPI_REG_RESULT_REJECT_26_NON_EPS_AUTHENTICATION_UNACCEPTABLE
39 :LAPI_REG_RESULT_REJECT_39_CS_DOMAIN_TEMPORARILY_NOT_AVAILABLE
40 :LAPI_REG_RESULT_REJECT_40_NO_EPS_BEARER_CONTEXT
95 :LAPI_REG_RESULT_REJECT_95_SEMANTICALLY_INCORRECT_MESSAGE
96 :LAPI_REG_RESULT_REJECT_96_INVALID_MANDATORY_INFORMATION
97 :LAPI_REG_RESULT_REJECT_97_MESSAGE_TYPE_NON_EXISTENT_OR_NOT_IMPLEMENTED
98 :LAPI_REG_RESULT_REJECT_98_MESSAGE_TYPE_NOT_COMPATIBLE_WITH_PROTOCOL_STATE
99 :LAPI_REG_RESULT_REJECT_99_INFORMATION_ELEMENT_NON_EXISTENT_OR_NOT_IMPLEMENTED,
100 : LAPI_REG_RESULT_REJECT_100_CONDITIONAL_IE_ERROR
101 :LAPI_REG_RESULT_REJECT_101_MESSAGE_NOT_COMPATIBLE_WITH_PROTOCOL_STATE
111 :LAPI_REG_RESULT_REJECT_111_PROTOCOL_ERROR_UNSPECIFIED

/* defined registration cause */
128 : LAPI_REG_RESULT_FAILURE_NO_USIM
129 : LAPI_REG_RESULT_FAILURE_INVALID_USIM
130 :LAPI_REG_RESULT_FAILURE_NETWORK_INIT_DETACH_TRIGGERED
131 :LAPI_REG_RESULT_FAILURE_DEFALULT_BEARER_SETUP_FAILURE
132 : LAPI_REG_RESULT_FAILURE_MAX_ATTACH_ATTEPT
133 : LAPI_REG_RESULT_ATTACH_IS_ALREADY_IN_PROGRESS
134 :LAPI_REG_RESULT_FAILURE_PDNCONNECT_APN_VERIFICATION_FAIL
137 :LAPI_REG_RESULT_FAILURE_START_USIM_REFRESH_MODE_4_5_6
138 : LAPI_REG_RESULT_FAILURE_LOWER_LAYER_FAIL
139 :LAPI_REG_RESULT_FAILURE_UE_INIT_DETACH_TRIGGERED
140 : LAPI_REG_RESULT_FAILURE_P_CSCF_MISSING
141 : LAPI_REG_RESULT_FAILURE_T3402_RUNNING
142: LAPI_REG_RESULT_FAILURE_MO_DATA_BARRING
143:LAPI_REG_RESULT_FAILURE_NOT_ALLOW_LIMITED_IMS_EMERGENCY
144: LAPI_REG_RESULT_LIMITED_SERVICE_ONLY
256 : LAPI_REG_RESULT_NO_AVAILABLE_CELL
150：LAPI_REG_RESULT_T3410_Timeout
151：LAPI_REG_RESULT_T3420_Timeout
152：LAPI_REG_RESULT_T3430_Timeout
153：LAPI_REG_RESULT_T3418_Timeout
154：LAPI_REG_RESULT_T3417_Timeout
155：LAPI_REG_RESULT_T3411_Timeout
156：LAPI_REG_IMS_NI_DEREG_IND
157：LAPI_REG_RESULT_T3442_Timeout
0xFFFF:LAPI_REG_RESULT_OTHER_FAILURE

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 47cm between the radiator & your body.

Professional installation instruction

1. Installation personal
This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location
The product shall be installed at a location where the radiating antenna can be kept 47cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. Installation procedure
Please refer to user’s manual for the detail.

4. Warning
Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.