Moso Canopy 4G Indoor Radios
Model: SCE4255W

Configuration Guide

Table of Contents

INTRODUCTION **3**

ACCESS DEVICE **3**

ETHERNET LAN CONNECTION 3
DEVICE WAN CONNECTION 3
ACCESS WEB 5
RESET BUTTON 6
DEVICE STATUS CHECK 7

FIRMWARE AND CONFIGURATION FILE MANAGEMENT **9**

FIRMWARE SWITCH 9
FIRMWARE UPGRADE 9
CONFIGURATION FILE MANAGEMENT 10
FACTORY RESET 11

DEVICE FUNCTIONS CONFIGURATION **11**

CONFIGURE DEVICE'S NETWORK 11
BRING UP S1 WITH MME 13
MOSO CANOPY OUTPUT POWER 17
ADD ONE NEIGHBOR CELL 19
GPS SYNC 20
1588 SYNC 22
IPSEC CONFIGURATION 24
MULTIPLE IPSEC CONFIGURATION 27
MODIFY EVENTS THRESHOLD 29
CONFIGURE SAS 30
SETUP FOR S1 OR X2 HANDOVER 37
SON CONFIGURATION 40
MULTIPLE SOURCE IP CONFIGURATION 41
SPLIT C/U PLANE FOR MOCN 43
CMP CONFIGURATION 45
KPI CONFIGURATION 46
DSCP CONFIGURATION 47
IPV6 CONFIGURATION 47
MOSO CANOPY NL SYN CONFIGURATION 48
VOLTA OTA SYN CONFIGURATION 49
ANR CONFIGURATION 51

EPC CONFIGURATION **52**

CONNECT TO MOSOLABS' CLOUD EPC 52

LOG MANAGEMENT **54**

VIEW LOG FROM GUI 54
GET TXT LOG 54
GET LOG.ZIP 55
CLEAR LOG 55

TCPDUMP CAPTURE PROCEDURE **56**

TCPDUMP CAPTURE PROCEDURE ON GUI 56
ABBREVIATIONS 57

Introduction

This document provides the user guide for Moso Canopy 4G Indoor radio devices ("Moso Canopy"), including accessing key features such as: firmware management, configuration file management, basic functions configuration, and EPC configuration.

Notes: After modifying settings, the user should reboot device.

Access Device

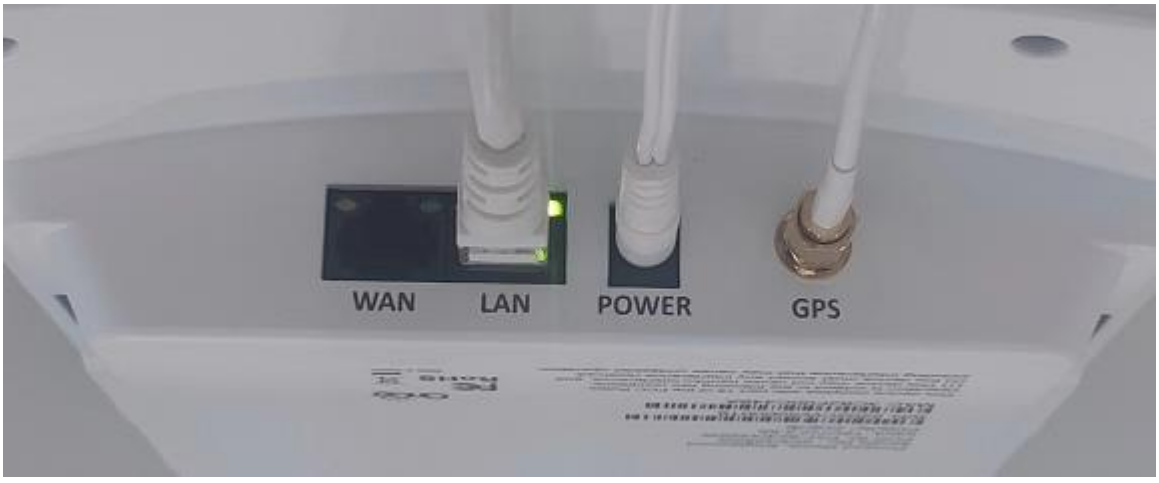
Ethernet LAN Connection

This section provides details of LAN connection between the Moso Canopy and the PC if the Moso Canopy supports the Ethernet LAN port.

Step 1. Connect PC's Ethernet interface to the LAN port of the Moso Canopy with an RJ45 cable.

Step 2. Power on the Moso Canopy device.

Step 3. Check if the PC gets the dynamic IP address: 11.11.11.xx.

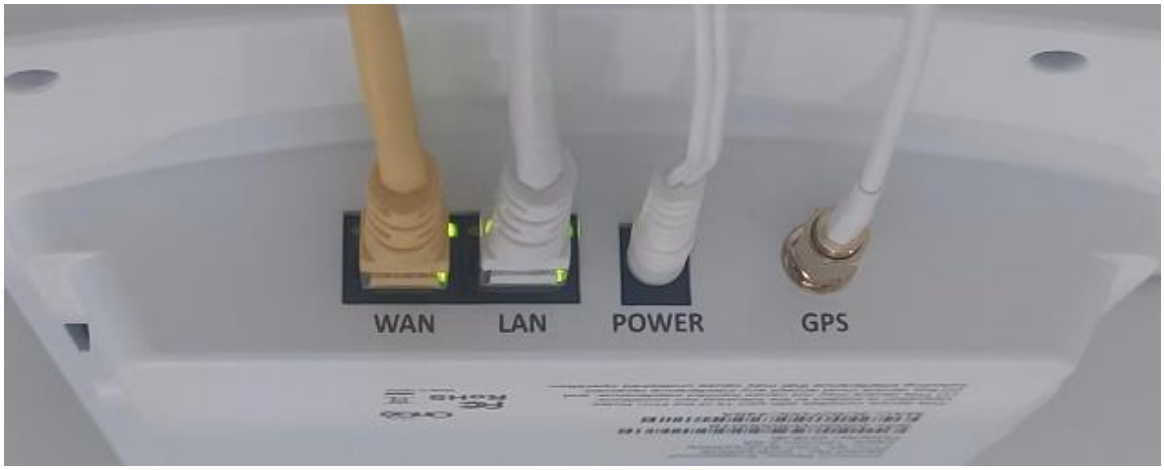


Device WAN Connection

This section provides details of WAN connection of the Moso Canopy after the PC is connected to the Moso Canopy via Ethernet interface and has a dynamic IP address.

Notes: If device has more than ONE physical WAN interface, please just select one WAN interface to use.

Step 1. Use an RJ45 cable to connect the WAN port of the Moso Canopy to a Router which is connected to Internet or Intranet.



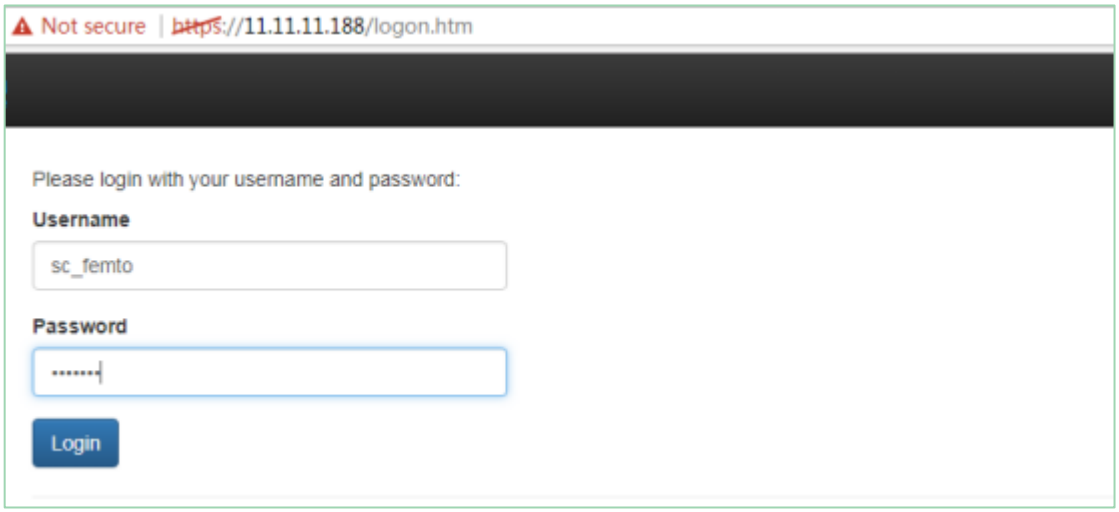
Step 2. The WAN port of the Moso Canopy will be able to get one dynamic IP if the router supports DHCP server. Or refer to “Configure Device’s Network” section to setup the WAN port of the Moso Canopy.

Access Web

This section provides details of accessing the web GUI of the Moso Canopy.

After the PC connect to the Moso Canopy with Ethernet LAN interface, open a web browser on the PC and visit https://11.11.11.188 and input username and password, and then click "Login" button.

Please get the general account from MosoLabs team.

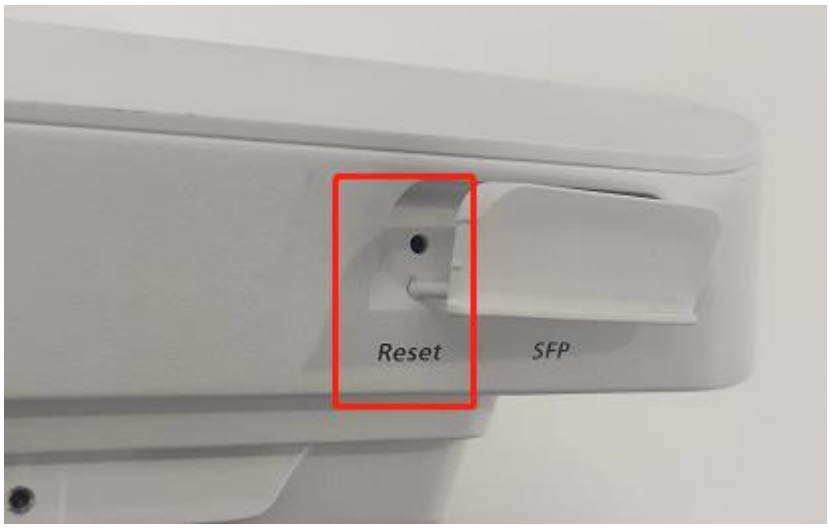


For testing purposes, the Moso Canopy opens the remote login function temporarily, to determine the IP of the Moso Canopy's WAN port and to find a PC on the WAN side of the Moso Canopy. Open a web browser on the PC and type the URL https://wan_ip_address and input username and password, and then click "Login" button.

The remote login function will be disabled in the formal shipment firmware.

Reset Button

This section provides details of factory default by pressing “reset” button.

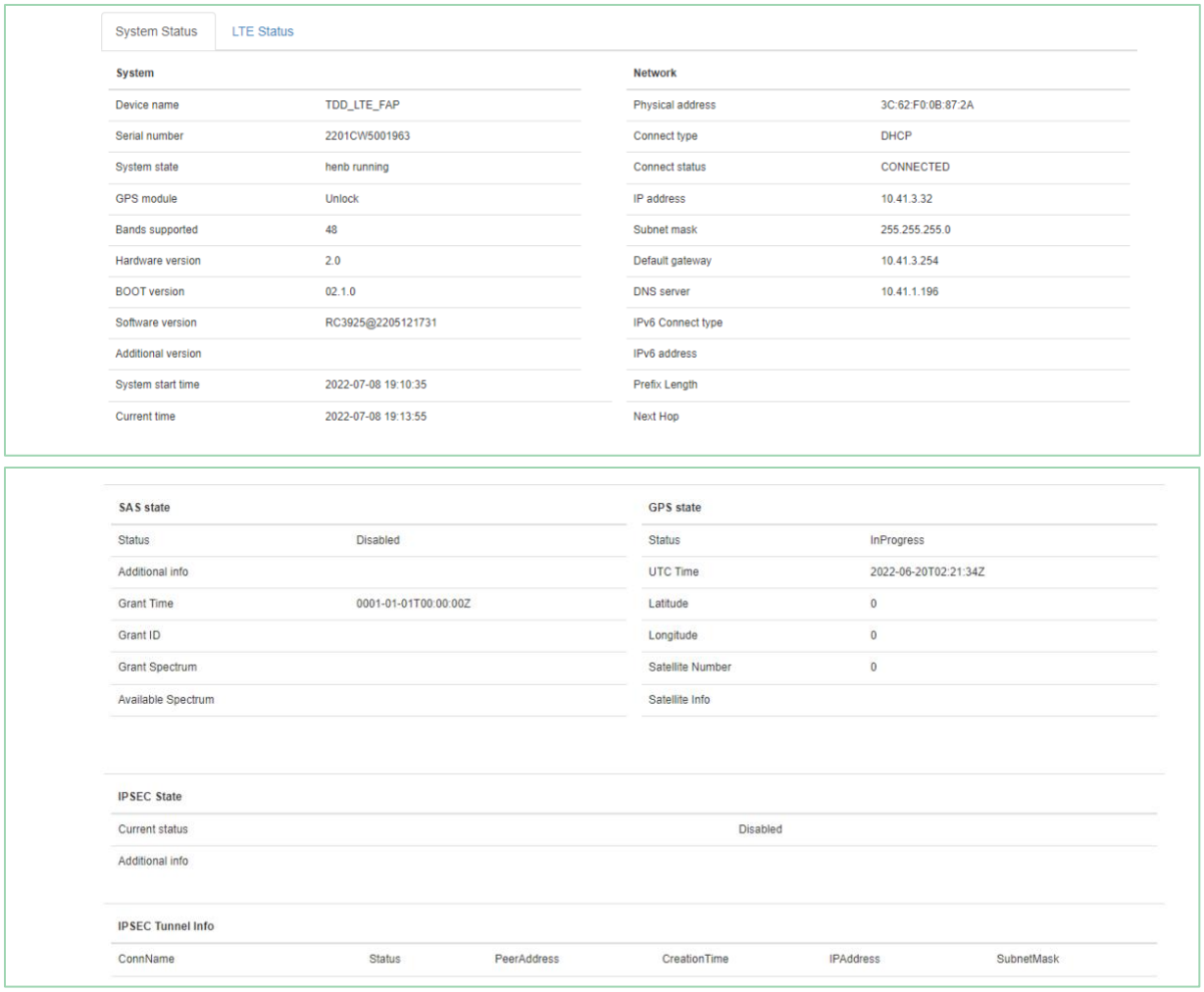


Press and hold the “reset” button for more than 10 seconds and release it to force the device to factory default. In this process, all LEDs will shut down, then the PWR LED will flash which means the device is rebooting. This takes 2-3 minutes.

Device Status Check

This section provides details of how to check the basic status of Moso Canopy device.

Visit "State" page under "State" group to check the system status and network status, SAS state, GPS state, IPSEC state of Moso Canopy device, this page is the default one after login.



System Status | LTE Status

System		Network	
Device name	TDD_LTE_FAP	Physical address	3C:62:F0:0B:87:2A
Serial number	2201CW5001963	Connect type	DHCP
System state	henb running	Connect status	CONNECTED
GPS module	Unlock	IP address	10.41.3.32
Bands supported	48	Subnet mask	255.255.255.0
Hardware version	2.0	Default gateway	10.41.3.254
BOOT version	02.1.0	DNS server	10.41.1.196
Software version	RC3925@2205121731	IPv6 Connect type	
Additional version		IPv6 address	
System start time	2022-07-08 19:10:35	Prefix Length	
Current time	2022-07-08 19:13:55	Next Hop	

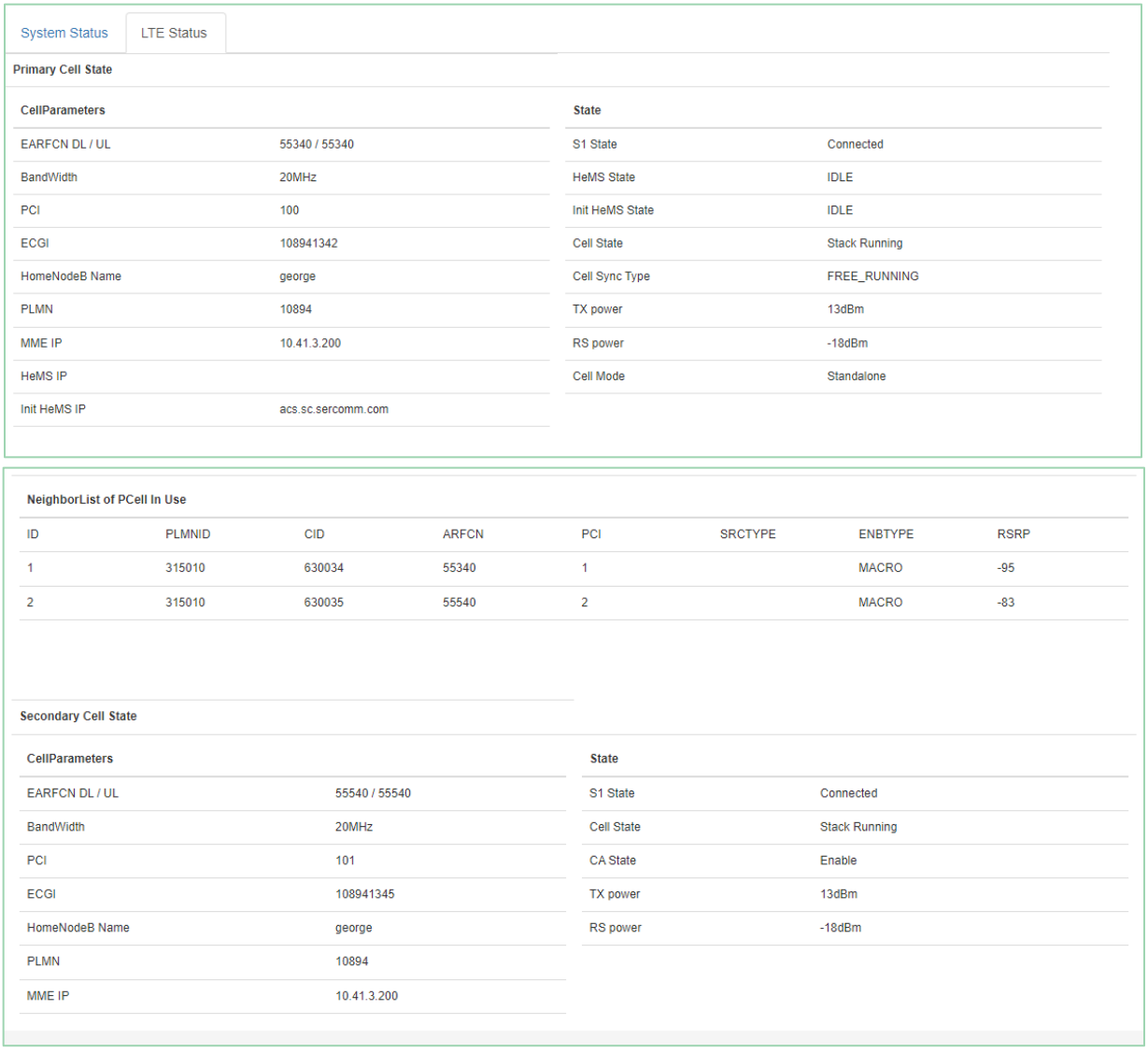
SAS state		GPS state	
Status	Disabled	Status	InProgress
Additional info		UTC Time	2022-06-20T02:21:34Z
Grant Time	0001-01-01T00:00:00Z	Latitude	0
Grant ID		Longitude	0
Grant Spectrum		Satellite Number	0
Available Spectrum		Satellite Info	

IPSEC State	
Current status	Disabled
Additional info	

IPSEC Tunnel Info

ConnName	Status	PeerAddress	CreationTime	IPAddress	SubnetMask

Visit "LTE State" page under "State" group to check the cell parameters and 2nd cell state, neighbor list of Moso Canopy device.



System Status | LTE Status

Primary Cell State

CellParameters		State	
EARFCN DL / UL	55340 / 55340	S1 State	Connected
BandWidth	20MHz	HeMS State	IDLE
PCI	100	Init HeMS State	IDLE
ECGI	108941342	Cell State	Stack Running
HomeNodeB Name	george	Cell Sync Type	FREE_RUNNING
PLMN	10894	TX power	13dBm
MME IP	10.41.3.200	RS power	-18dBm
HeMS IP		Cell Mode	Standalone
Init HeMS IP	acs.sc.sercomm.com		

NeighborList of PCell In Use

ID	PLMNID	CID	ARFCN	PCI	SRCTYPE	ENBTYPE	RSRP
1	315010	630034	55340	1		MACRO	-95
2	315010	630035	55540	2		MACRO	-83

Secondary Cell State

CellParameters		State	
EARFCN DL / UL	55540 / 55540	S1 State	Connected
BandWidth	20MHz	Cell State	Stack Running
PCI	101	CA State	Enable
ECGI	108941345	TX power	13dBm
HomeNodeB Name	george	RS power	-18dBm
PLMN	10894		
MME IP	10.41.3.200		

The "Cell State" has a total of 11 statuses as follows:

Starting L1

Starting Stack

Setup S1

S1 Connected

Stack Running

Pending

Down

PowerDown

L1 Finished

L1 Failed

None

Firmware and Configuration File Management

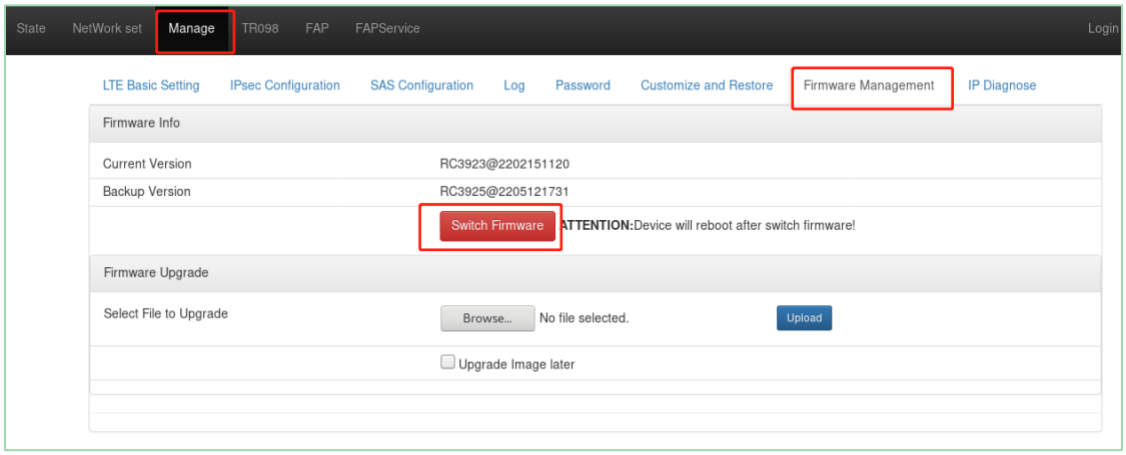
Firmware Switch

This section provides details of how to switch the firmware for the Moso Canopy device.

The Moso Canopy supports dual firmware images. You can use this function as following steps.

Step 1. Visit "Firmware Management" page under "Manage" group.

Step 2. Check the current version and backup version, click "Switch Firmware" button if the backup version is needed. The Moso Canopy will perform a reboot automatically after switching. This takes about 3 minutes.



Step 3. Visit "Firmware Management" page under "Manage" group to check firmware version again.

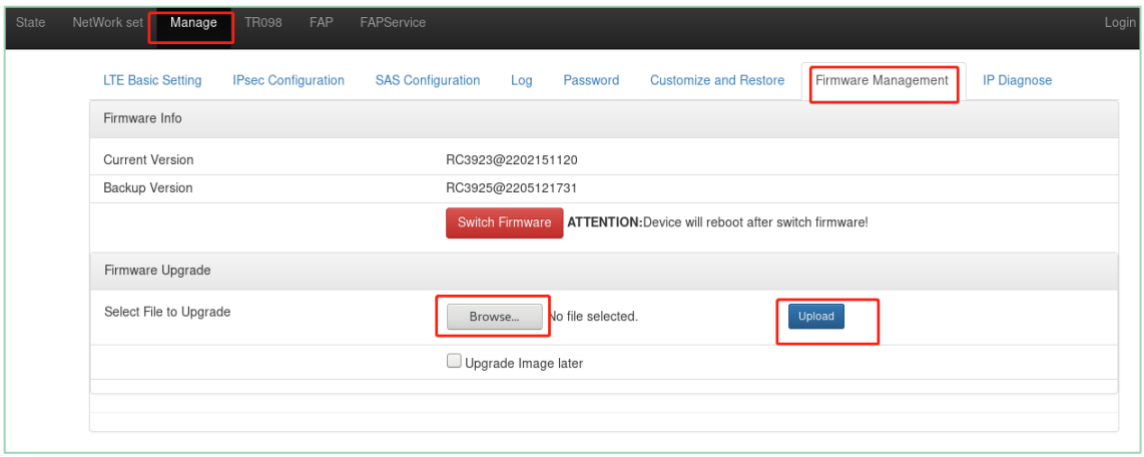
Firmware Upgrade

This chapter provides details of upgrading the firmware onto the Moso Canopy device.

Step 1. Get the new firmware from MosoLabs and store it in the local disk.

Step 2. Visit "Firmware Management" page under "Manage" group.

Step 3. Click "Select a File" button and select the new firmware restored on the local disk.



Step 4. Click "Upload" button and start the firmware upgrading, the Moso Canopy will perform a reboot automatically after upgrading. This will take 4 to 6 minutes.

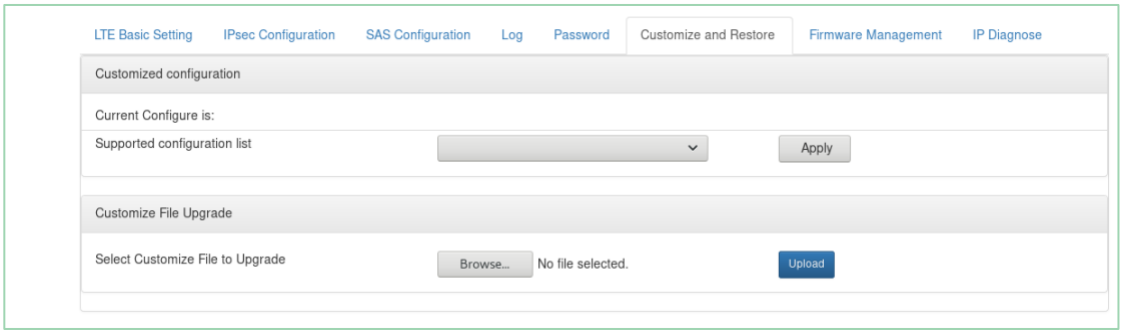
Configuration File Management

This section provides details of management of the Moso Canopy's configuration file.

Visit "Customize and Restore" page under "Manage" group.

Function 1. Choose customized file. Select a configuration file from "Supported configuration list" and click the "Apply" button. The Moso Canopy will reboot automatically after applying the new configuration. This will take 3 to 5 minutes.

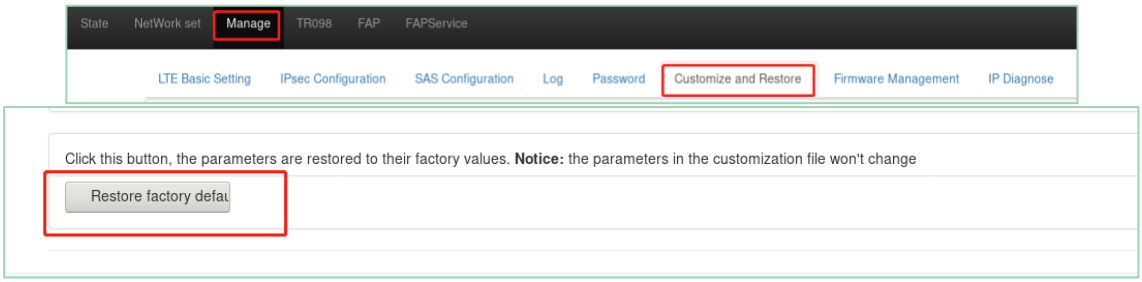
Function 2. Upgrade customized file. Click "Select a File" button and select a customized configuration file stored locally and click "Upload" button and start the configuration upgrade. The Moso Canopy will reboot automatically after upgrading. This will take 3-5 minutes. The customized configuration can be obtained from MosoLabs.



Factory Reset

This section provides how to factory reset on the webGUI.

Visit "Customize and Restore" page under "Manage" group.



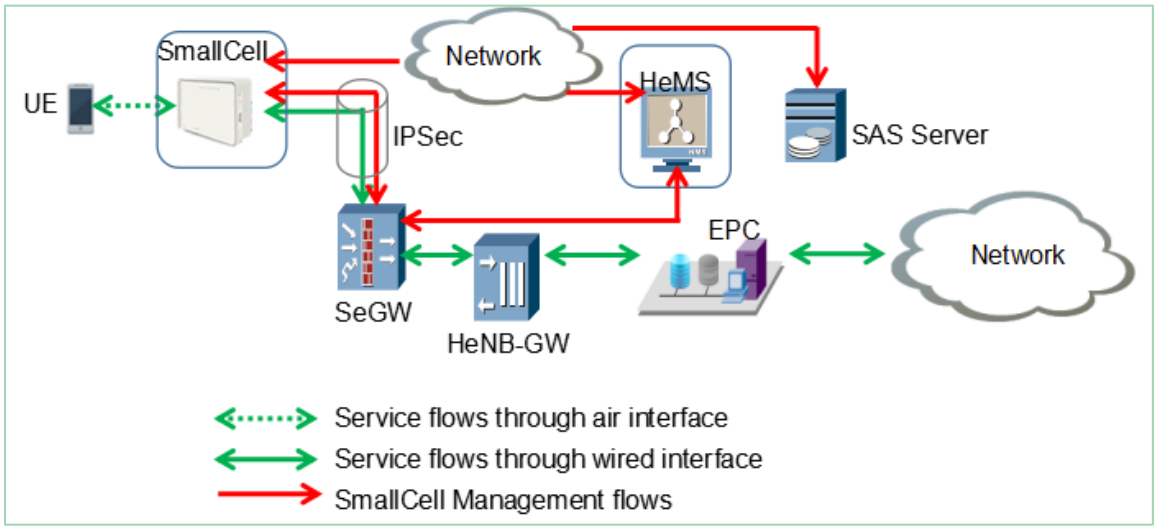
Click "Restore factory default" button to use factory values. The Moso Canopy will reboot automatically after restoring default values. This will take 2-3 minutes.

Device Functions Configuration

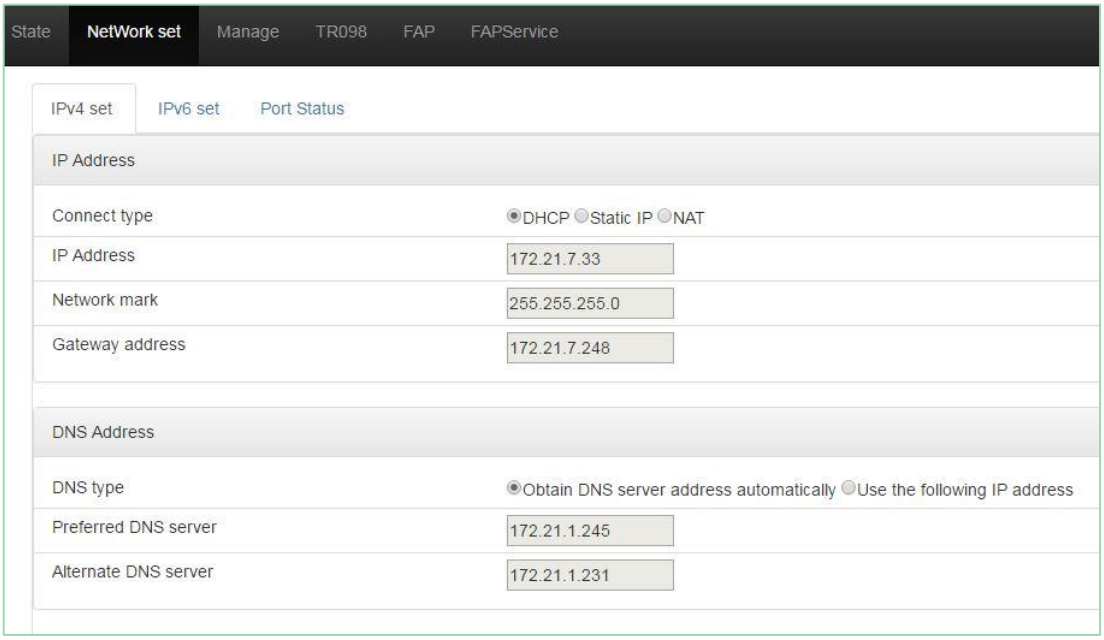
Configure Device's Network

This section provides details of configuration of the Moso Canopy's WAN IP address.

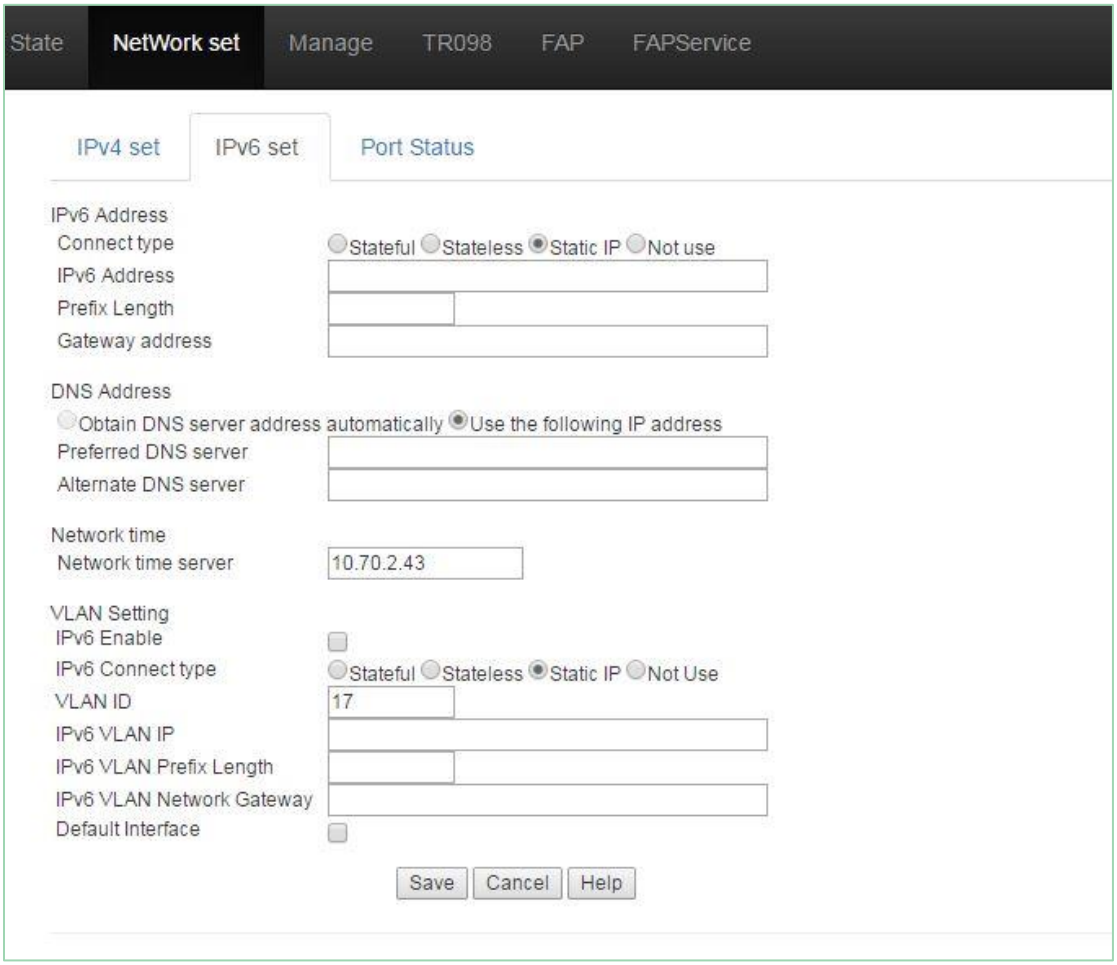
The following figure is a reference to the Network Architecture and useful for the setup the test environment.



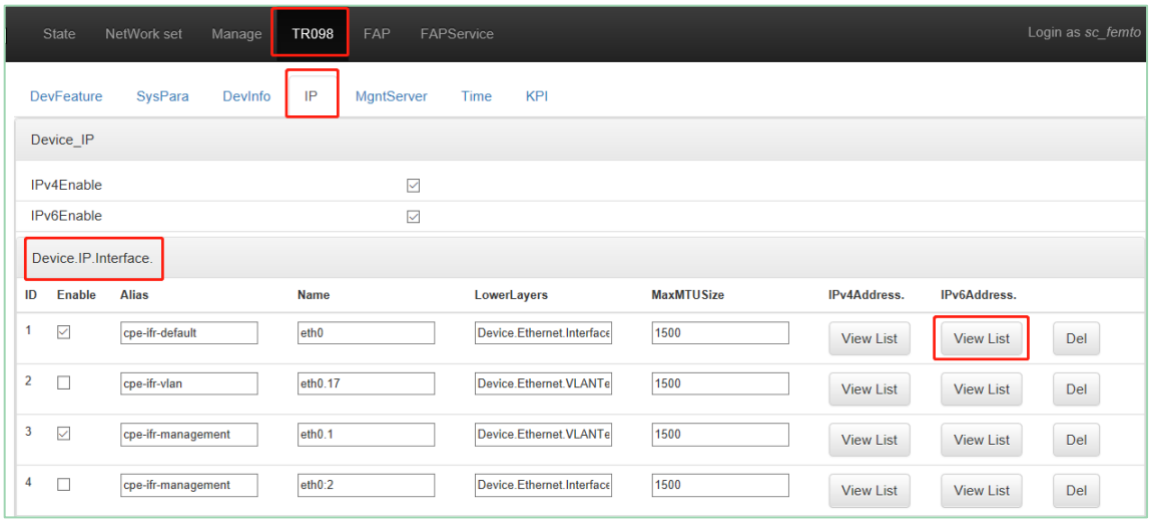
1. Visit "IPv4 Set" page under "Network set" group and configure the WAN IPv4 address of the Moso Canopy device. The default IPv4 connection type of the Moso Canopy device is "DHCP" which means the Moso Canopy's WAN is a DHCP client. The Moso Canopy will get the dynamic IP from DHCP server in the network.

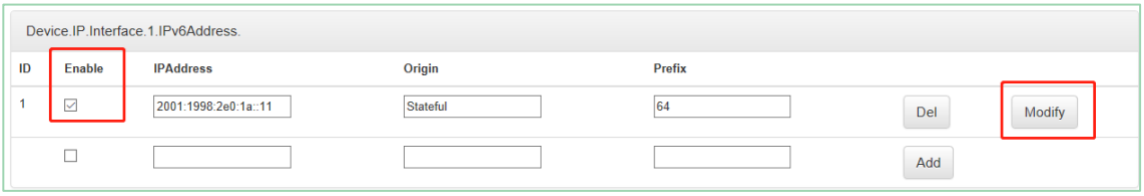


2. Visit "IPv6 Set" page under "Network set" group and configure the WAN IPv6 address of the Moso Canopy device.



3. Visit "IP" page under "TR098" group. Click Device.IP.Interface
   The first IPv6Address View List button, then it will open another page. Please enable Device.IP.Interface.1.IPv6Address and click Modify button to save it to flash.



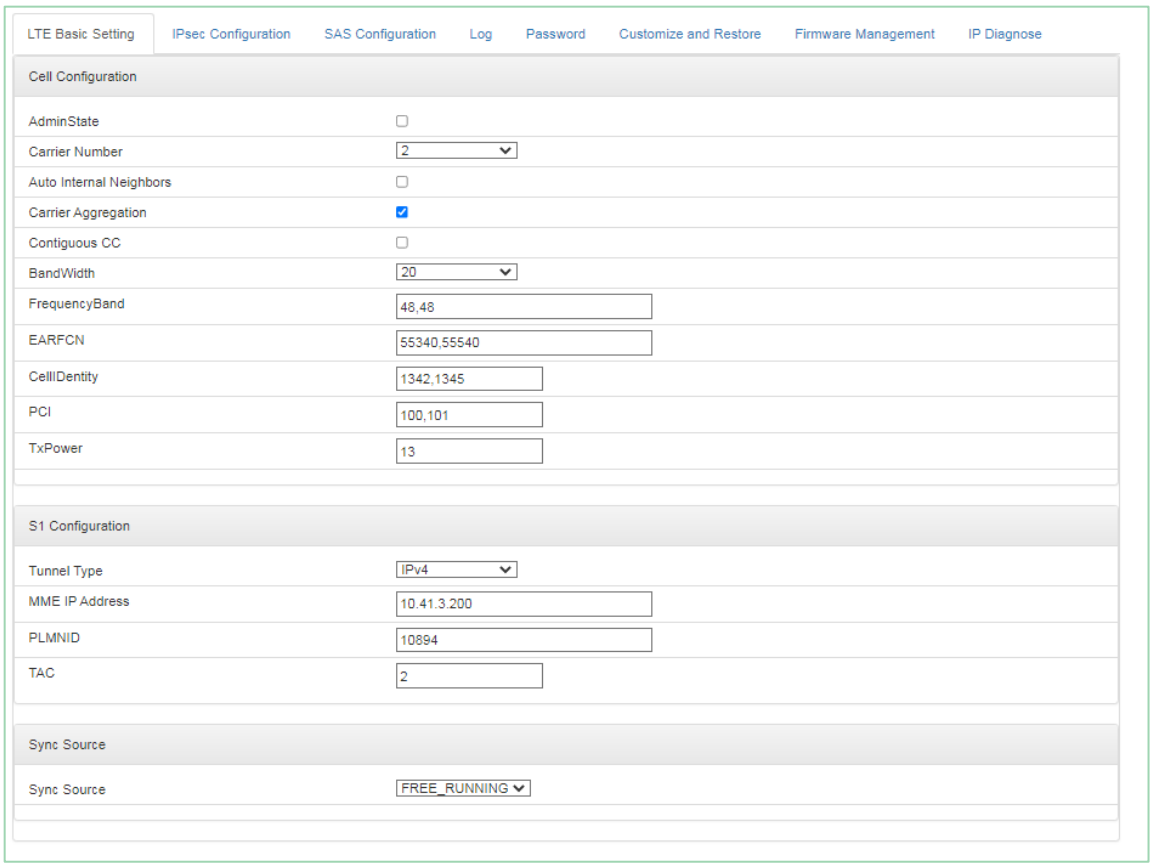


4. Visit "IP" page under "TR098" group and enable ForwardingPolicy of IPv6.Click IPv6Forwarding. View List button, then it will open another page. Please set ForwardingPolicy to 1 and then click Modify button to save it to flash.

Bring up S1 with MME

This section provides details of the configuration of Moso Canopy's S1, which can support the CA function.

1. Visit "LTE Basic Setting" page under "Manage" group to set Cell parameters.



AdminState: enable or disable Moso Canopy
Carrier Number: number of carriers which will be enabled.
Auto Internal Neighbors:
Carrier Aggregation: enable or disable Carrier Aggregation
Contiguous CC: contiguous component carrier
Bandwidth: each carrier bandwidth
FrequencyBand: frequency band indicator, need to input 2 parameters for CA mode.
EARFCN: EUTRA-Frequency, need to input 2 parameters if CA mode.
CellIdentity: Cell Identity, need to input 2 parameters if CA mode.
PCI: Moso Canopy's phycellid list, need to input 2 parameters if CA mode.
TxPower: the output power of each path and the unit is dB, follow below formula to calculate EIRP of Moso Canopy
Moso Canopy EIRP = TxPower + 3*CarrierNumber + AntennaGain

Tunnel Type: The type of tunnel,such as IPv4,IPSEC
MME IP Address: IP of MME
PLMNID: PLMN of Moso Canopy
TAC: TAC of Moso Canopy

Sync Source:The sync type,default is FREE_RUNNING

Notes: If you configured Carrier Number to 2, means you enabled 2 cells. In this case, you should be aware of that our eNB must be set to macro cell and work in the mode of Intra- eNB with two cells. So CellIdentity should be set two values, and these two values use the same eNB-Id and different cell ids. For macro mode of eNBType, you should configure PCI to ensure their values are out the range of Moso Canopy PCI.

Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.AdminState
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_RRMConfig.X_000E8F_Cell_Number
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_RRMConfig.X_000E8F_CA_Enable
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_RRMConfig.X_000E8F_CELL_Freq_Contiguous
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.DLBandwidth
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.ULBandwidth
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.FreqBandIndicator
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.EARFCNDL
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.EARFCNUL
Device.Services.FAPService.1.CellConfig.LTE.RAN.Common.CellIdentity
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.PhyCellID
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.X_000E8F_TxPowerConfig
Device.IP.X_000E8F_IPTypeInTunnel
Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkServerList
Device.Services.FAPService.1.FAPControl.LTE.Gateway.S1SigLinkPort
Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList.1.PLMNID
Device.Services.FAPService.1.REM.LTE.Cell.1.BCCH.TAC
Device.Services.FAPService.1.REM.X_000E8F_tfcsManagerConfig.primSrc

2. Config Multi-MME

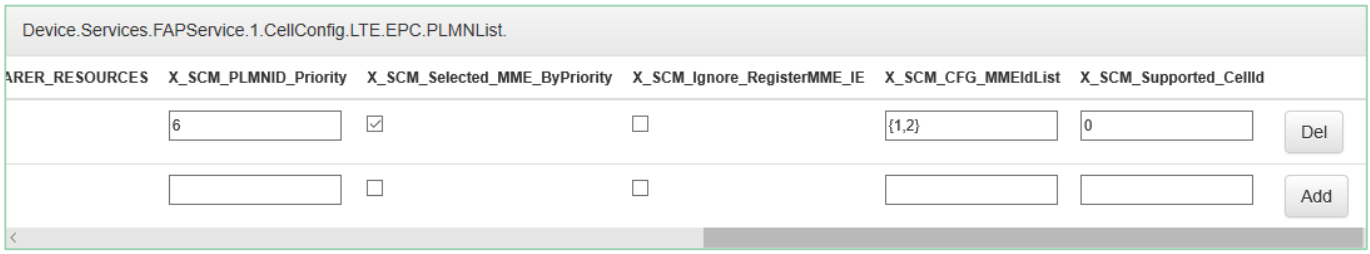
Visit "FAPControl" page under "FAPService" group to find "S1SigLinkServerList" and fill.

S1SigLinkServerList:{{mmeId1,noOfIp,mmeIp1,mmeIp2,...},{mmeId2,noOfIp,mmeIp1,mmeIp2,...},...}. Configure this parameter in the data format as above, with the meaning of each parameter from left to right: MME ID, number of MME IP, and each MME IP address.

Ex.: {{1,1,172.21.143.206},{2,1,172.21.143.220}}.Represents a total of two MMEs configured with MMEID of 1 and 2, and each MME has only one IP, 172.21.143.206 and 172.21.143.220, respectively.

3. Config Multi-MME with one PLMNID

Visit "CellConfig" page under "FAPService" group to find "Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList" and fill in "X_000E8F_CFG_MMEIdList" parameter.

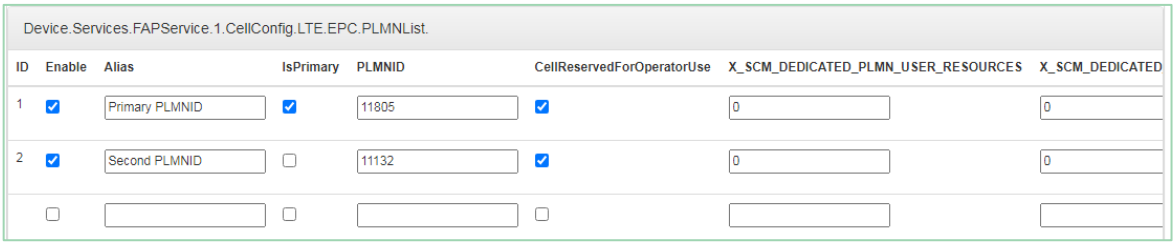


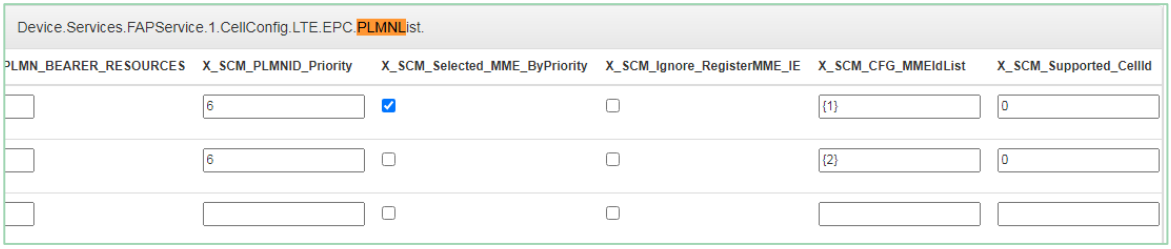
X_000E8F_CFG_MMEIdList:Data format is {mmeId1,mmeId2,...}.The MME to which the PLMNID belongs is described in the form of MMEID. The configuration order determines the priority of the MME to the PLMN. Each parameter represents the MMEID of the MME configured by the PLMNID. Such as {2,1}, MME ID 2 represents MME 172.21.143.220 in S1SigLinkServerList, so MME ID 2 has more priority than MME ID 1.

X_000E8F_Ignore_RegisterMME_IE: Indicate if according to the RegisterMME_IE to decide which MME to be used. The IE will be in RRCConnectionCompelete message, and it is an optional IE. If there is no RegisterMME_IE, then will select MME according to parameter X_000E8F_CFG_MMEIdList.

4. MOCN configuration

Firstly, configure the Multi-MME as description in “Config Multi-MME” above, then configure the Multi-PLMN, visit "CellConfig" page under "FAPService" group to add a ID for "Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNList" and fill the configuration as below:

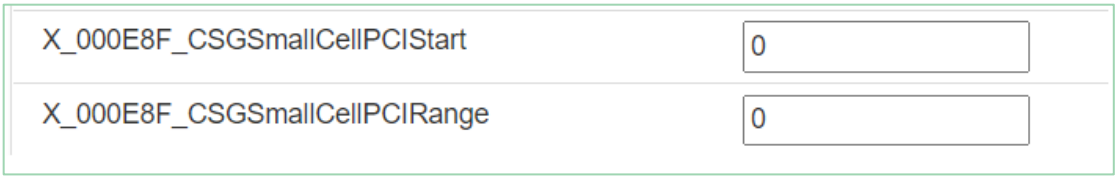




Ex.：{1} in X_000E8F_CFG_MMEIdList represents 172.21.143.206 configured in 4.3.2 and {2} represents 172.21.143.220. Cell with PLMNID 11805 will connect to MME ID 1, and cell with 11132 will connect to MME ID 2.

5. eNodeB Type Configuration

Visit "FAPControl" page under "FAPService" group to find "FAPService_FAPControl_LTE_X_000E8F_RRMConfig" Object and below parameter.



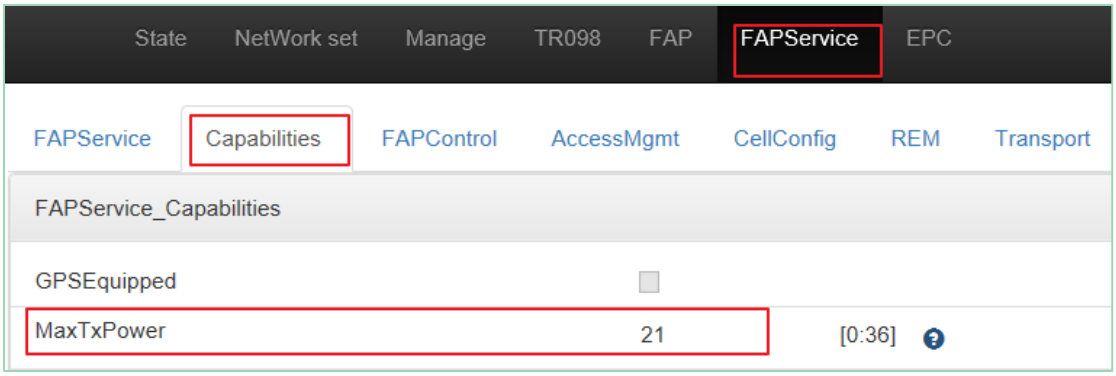
X_000E8F_CSGSmallCellPCIStart: Start PCI for Moso Canopy

X_000E8F_CSGSmallCellPCIRange: The range of PCI for small cell, these two parameters define the range of PCI for small cell, the rest of PCI is used for macro cell.

6. Visit "FAPControl" page under "FAPService" group to enable S1 "AdminState", then click "Save" button in the end of the page and reboot the Moso Canopy device, then S1 will be work.

Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.AdminState

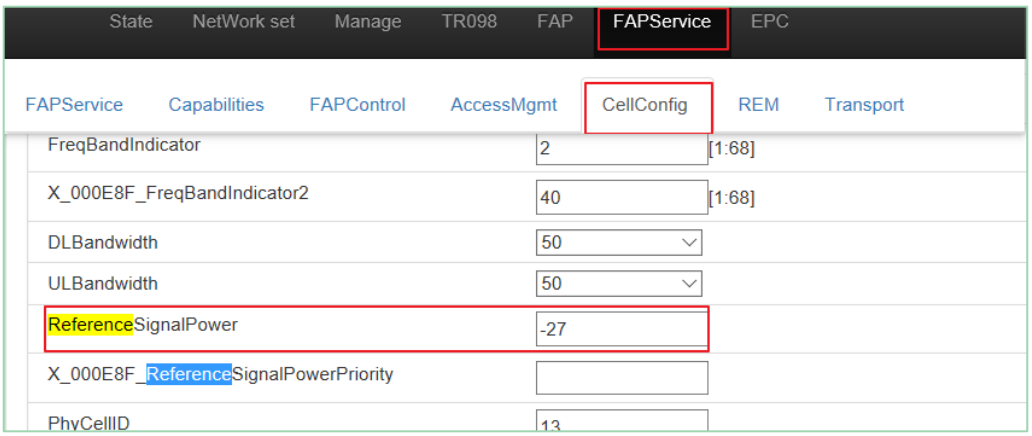
7. Visit "Capabilities" page under "FAPService" group and check the MaxTxPower which the Moso Canopy device hardware supports. Make sure value of TxPower is smaller than Moso Canopy capability.



Moso Canopy Output Power

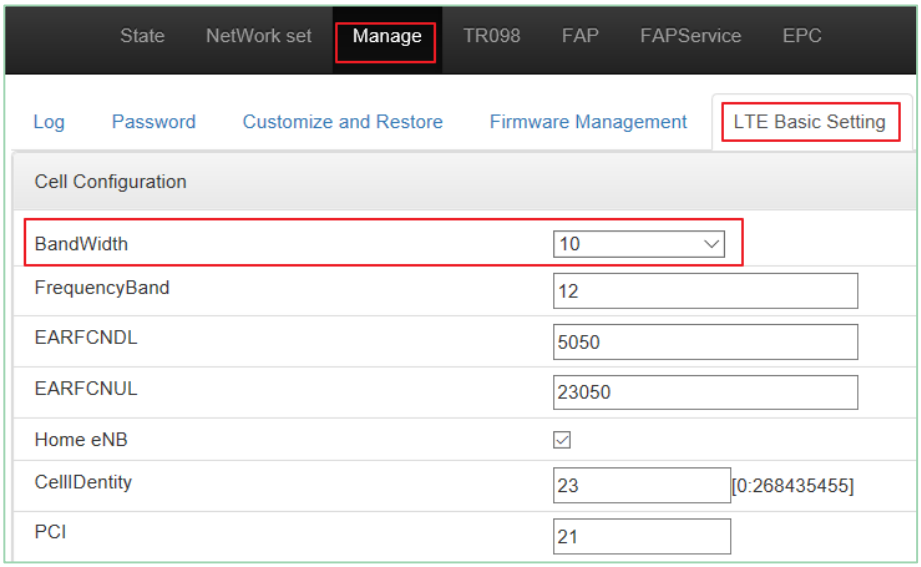
This section provides details of configuration of Moso Canopy's output power. Bring up S1.

1. Visit "CellConfig" page under "FAPService" group and set ReferenceSignalPower, it's in dBm with a range between -60 and 50.



Data Model Nodes Table
Device.Services.FAPService.1.CellConfig.LTE.RAN.RF.ReferenceSignalPower

2. Visit "LTE Basic Settings" page under "Manage" group and select the bandwidth.



3. Follow the below formula to calculate the TxPower

TxPower = ReferenceSignalPower + 28, if Bandwidth = 10MHz.

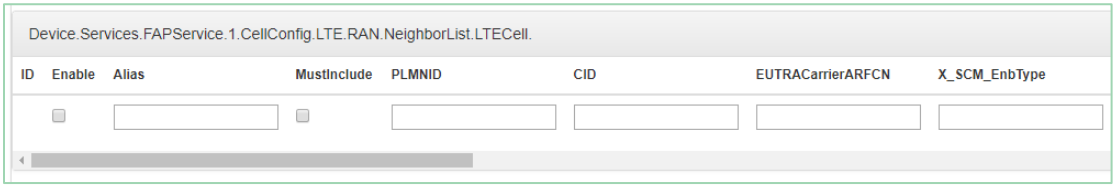
TxPower = ReferenceSignalPower + 31, if Bandwidth = 20MHz.

The calculated TxPower will be announced to the UE in packets sent from the small cell device to UE, then the UE will use that value from the Moso Canopy device to perform the communication preparation.

Add one Neighbor Cell

This section provides details of the configuration of Moso Canopy's neighbor cell list.

1. Visit "CellConfig" page under "FAPService" group and find "Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell" table to add a neighbor cell or additional devices.



Cell Configure page (Neighbor cell list)

Enable: enable option of this item.
Alias: the alias name for this neighbor cell list.
MustInclude: enable it if this neighbor cell always exists.
PLMNID: PLMN of neighbor cell.
CID: CID of neighbor cell.
EUTRACarrierARFCN: EARFCN DL of neighbor cell.
X_000E8F_EnbType: 0 if neighbor cell is Macrocell, 1 for Home Moso Canopy.
X_000E8F_EnbAddr: input it if X2 interface will be needed
X_000E8F_TAC: TAC of neighbor cell.
X_000E8F_TrgrX2: enable this if the X2 interfaceis needed.
X_000E8F_AccessMode: Access mode of neighbor cell, set it to1(Open Mode) normally
X_000E8F_CSGID: CSD ID of neighbor cell. Leave it blank if it is open mode.
PhyCellID: PCI of neighbor cell.
QOffset: QOffset of neighbor cell. Leave it blank for normal priority neighbor cell.
CIO: CIO of neighbor cell. Leave it blank for normal priority neighbor cell.
RSTxPower: RS power of neighbor cell. Leave it blank if not knowing this value.
Blacklisted: enable it if putting this neighbor cell to black list of HO.
TAC/EnbType: not modify it.

Data Model Nodes Table
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.Enable
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.Alias
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.MustInclude
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.PLMNID
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.CID
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.EUTRACarrierARFCN
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_EnbType
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_EnbAddr

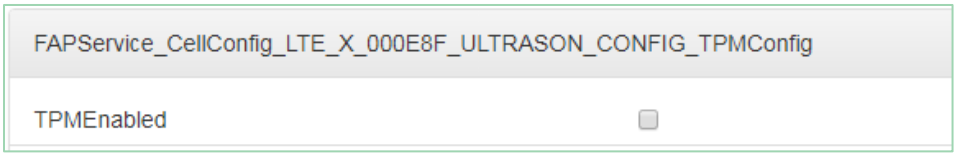
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_TAC
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_TrgrX2
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_AccessMode
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.X_000E8F_CSGID
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.PhyCellID
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.QOffset
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.CIO
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.RSTxPower
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.Blacklisted
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.TAC (Same as ".X_000E8F_TAC")
Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.EnbType (Same as ".X_000E8F_EnbType")

2. Click "Add" Button in the end of a new neighbor cell. And click "Modify" button in the end of an existing neighbor cell if some parameters will need to be modified. Click "Save" button in the end of the page.

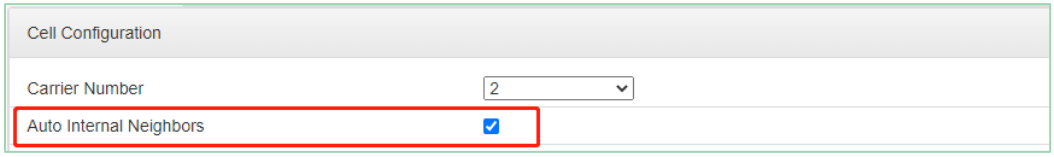
3. Reboot the Moso Canopy device.

4. Notes:

- If you add neighbor cell by the above method, you have better to disable TPM function first. Visit "CellConfig" page under "FAPService" group and find "FAPService_CellConfig_LTE_X_000E8F_ULTRASON_CONFIG_TPMConfig" object to disable TPMEnabled as below:



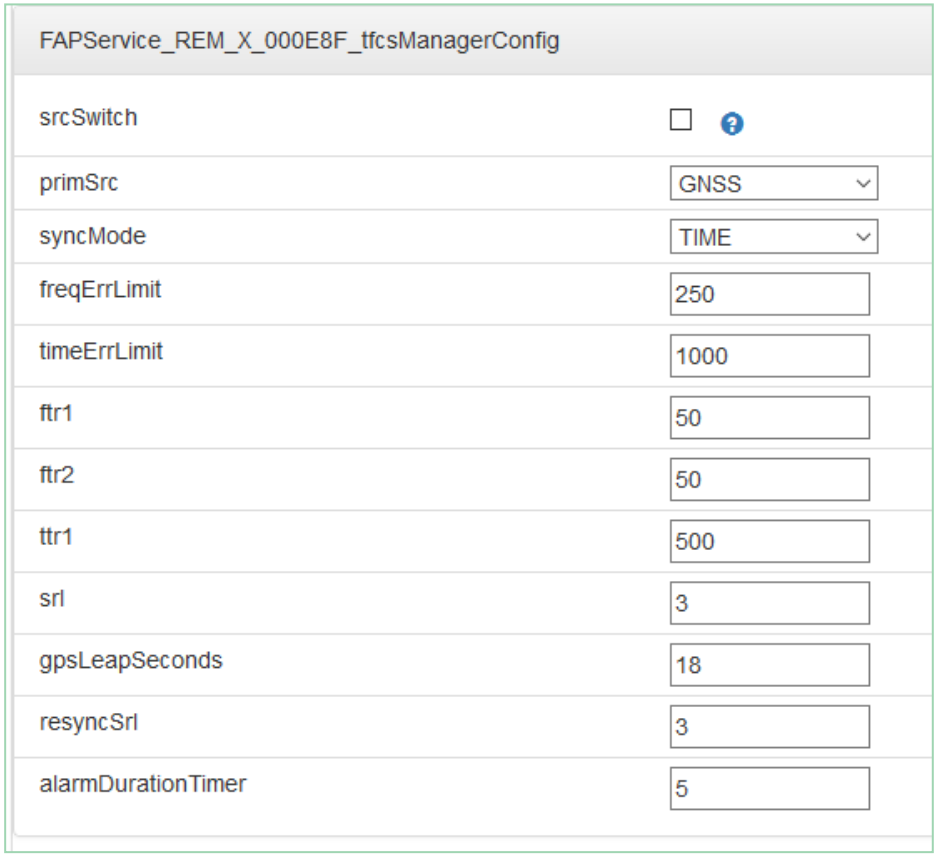
- If you configured two carriers as described in “Moso Canopy Output Power” section. If you want to add neighbors for internal cells, please visit "LTE Basic Setting" page under "Manage" group and find "Cell Configuration" object to enable "Auto Internal Neighbors" as below:



GPS Sync

This section provides details of the configuration of GPS.

1. Visit "REM" page under "FAPService" group and find "FAPService_REM_X_000E8F_tfcsManagerConfig" table. Select "GNSS" for primSrc item, then the GPS module will function after powering on the Moso Canopy device.



2. Reboot the Moso Canopy device and visit "LTEState" page under "State" group to check the status of GPS sync.

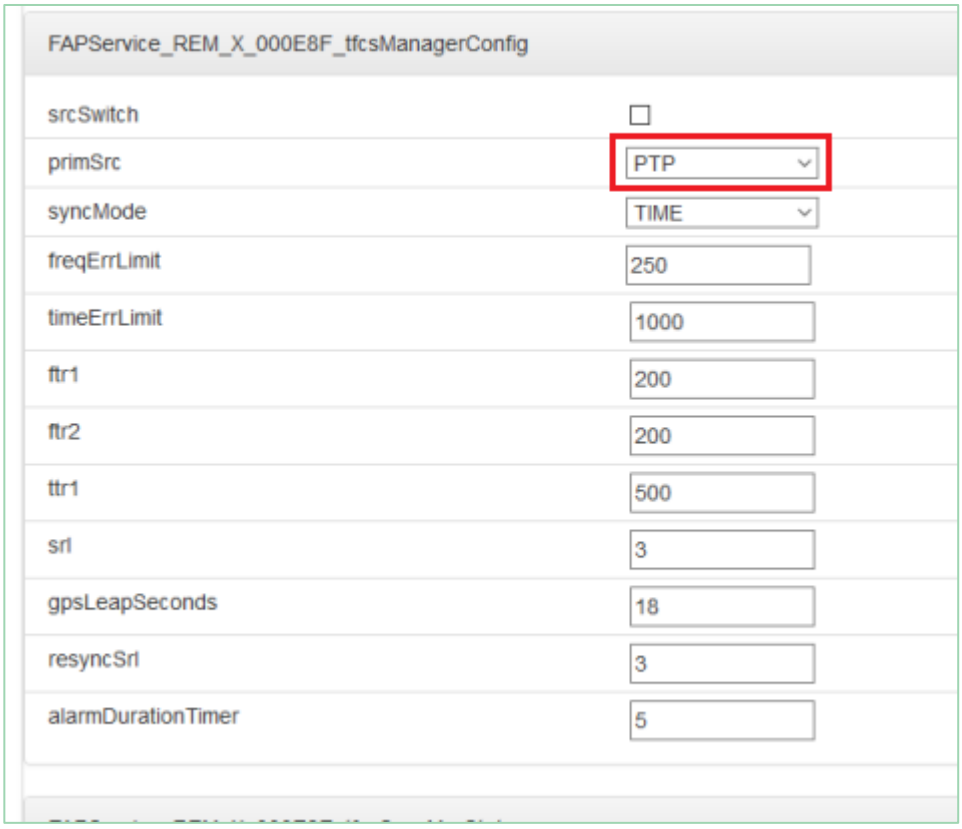
The Moso Canopy device starts to do GPS Sync. It will take a couple of minutes to run GPS Sync function. After it's completed, the "LTE State" page shows GPS Sync.

Data Model Nodes Table
Device.Services.FAPService.1.REM.X_000E8F_tfcsManagerConfig.primSrc

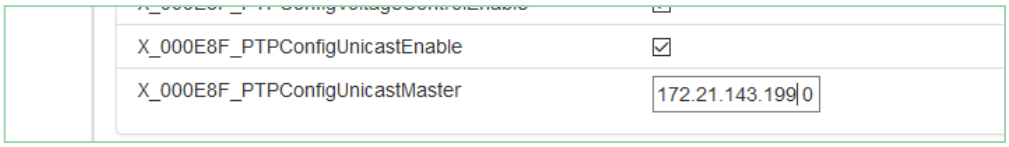
1588 Sync

This section provides details of configuration of 1588.

1. Visit "REM" page under "FAPService" group and find "FAPService_REM_X_000E8F_tfcsManagerConfig" table, Select "PTP" for primSrc.



2. Visit "REM" page and find "X_000E8F_PTP_Cfg" table to modify PTP parameters of 1588.



The following 3 parameters will need to be modified:

X_000E8F_PTPConfigUnicastEnable: If selected, enable Unicast mode, otherwise use Multicast mode. Default is Multicast.

X_000E8F_PTPConfigUnicastMaster: If unicast mode is enabled, configure PTP master related parameters. The format is as below:

<address><priority><log_sync_interval><log_delay_req_interval>

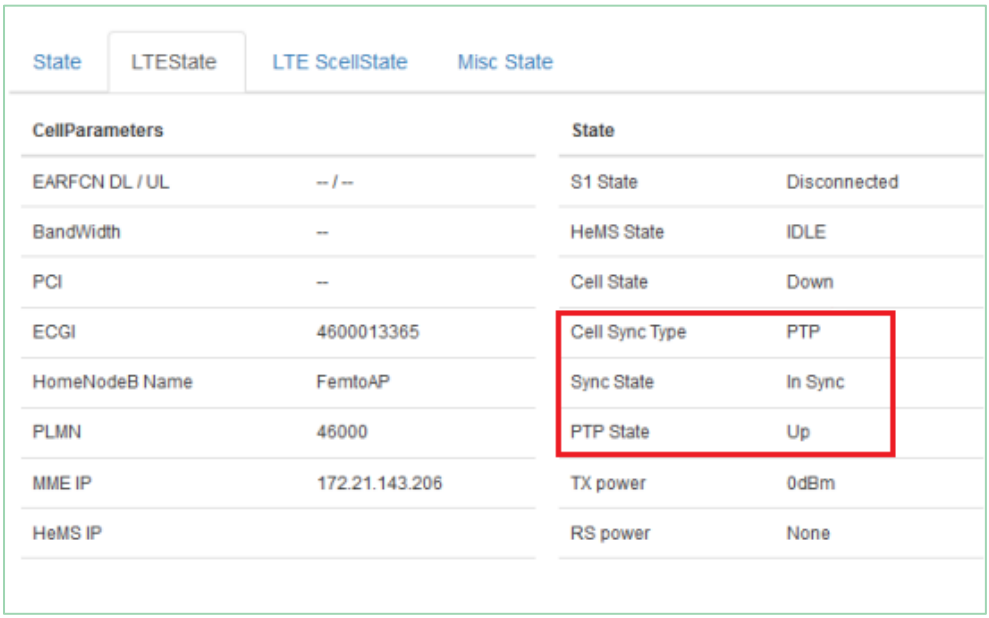
<address>: PTP master IP address

<priority>: 0

<log_sync_interval>: 0

<log_delay_req_interval>: 0

3. Reboot the Moso Canopy device and visit "LTEState" page under "State" group to check the status of 1588 sync. The following screen will be shown when sync is OK.



Data Model Nodes Table
Device.Services.FAPService.1.REM.X_000E8F_tfcsManagerConfig.primSrc
Device.Services.FAPService.1.REM.LTE.X_000E8F_PTP_Cfg.*

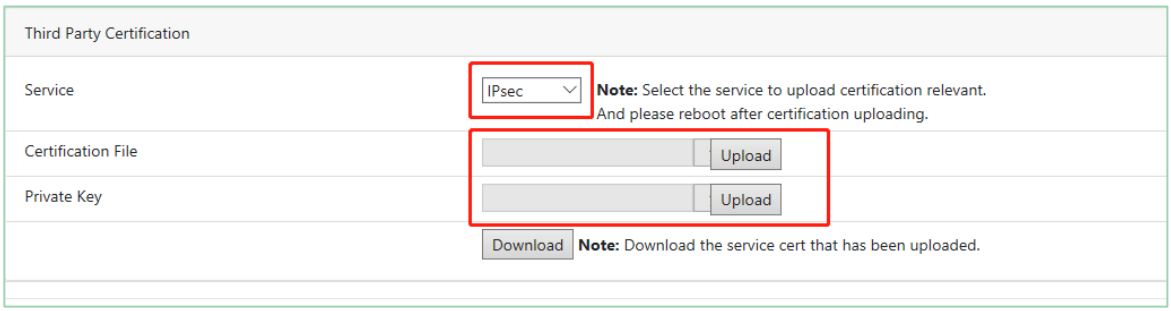
IPsec Configuration

This section provides details of the configuration of IPSec in 2 modes.

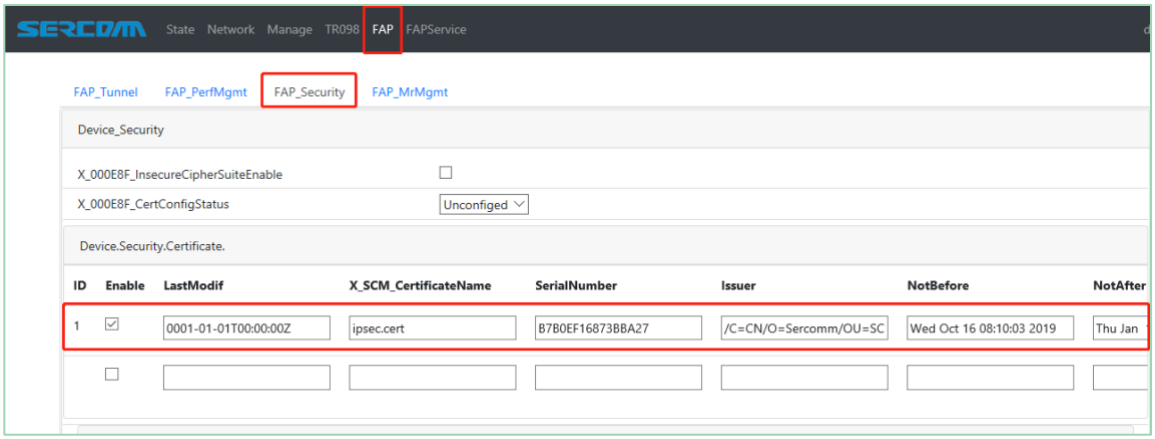
Please refer to section “Multiple IPSec Configuration” for multiple IPSec configuration.

Steps are as follows.

1. IPsec Cert Assign
   a) IPsec cert should have two files: cert.pem and key file. We need assign the cert to our device. they can upload by GUI.
   b) Open Web Page, then go to https://11.11.11.188:/cert_mgt.htm (Notice: This is a hidden page, you need go to it manually).
   c) Select "Third Party Certification Service" as IPsec and select "Certification File" to local cert file.
   d) Click "Upload" to Assign cert file.
   e) Select "Third Party Certification Service" as IPsec and select "Private Key" to local key file.
   f) Click "Upload" to Assign key file.



   g) Reboot Device and check the "Device.Security Certificate." list in below picture (FAP->FAP_Security). It will add a new cert. Check the "Subject" value to validate the cert.



2. Modify the IPSec Configuration

a) Enter Manage->IPsec Configuration, Modify the value as follows (cert mode):

Enable: Turn on the IPsec if IPsec functionality is required. This should be verified.

UseForCWMP: Check this field if CWMP should use IPsec tunnel

IPsec Mode: There are 4 IPsec modes,PSK\CERT\AKA\CUSTOM. The required CERT is chosen here.

Certificate Subject: Cert subject

SecGW Server: SecGWServer's IP Address

SecGW ID: The id of SecGW, use %any when unsure

Subnet: The right subnet that IPsec use for S1 connection and/or CWMP (Don't configure to 0.0.0.0/0, otherwise the DUT will not be accessible)

InnerIP: The IP in IPsec tunnel, left blank to auto obtain IP from SecGW(This will appear when IPSec Mode is set to PSK)

For example: Enable: √

IPsec Mode: CERT

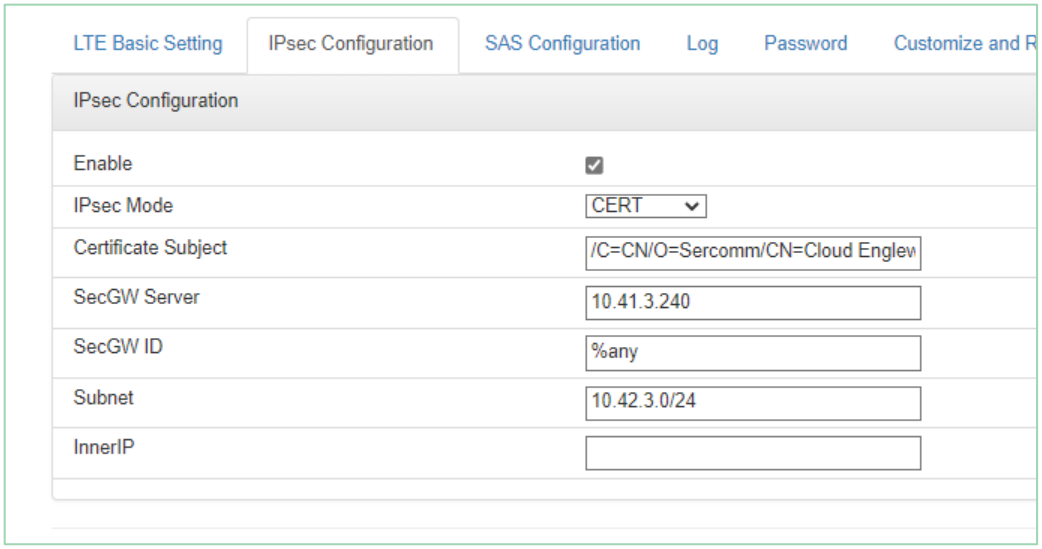
Certificate Subject: XXX

SecGW Server: 10.41.3.240

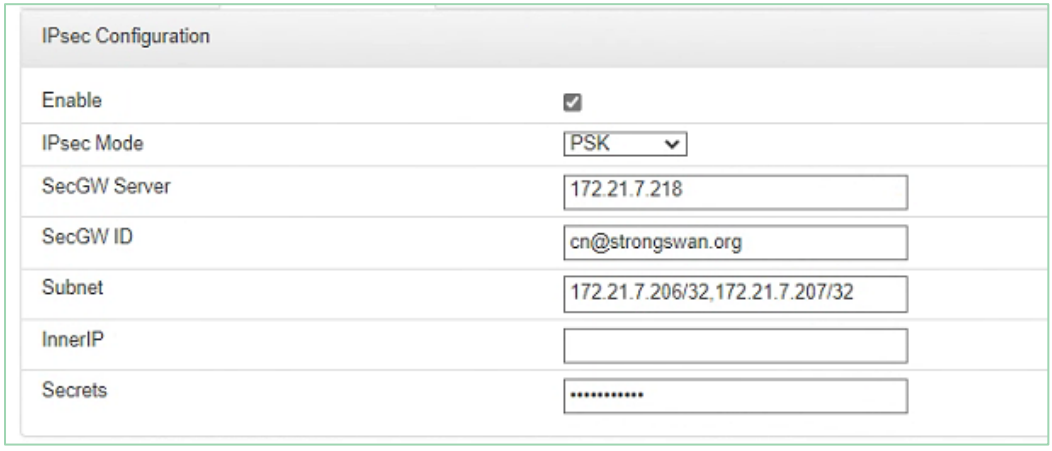
SecGW ID: %any

Subnet: 10.42.3.0/24

b) Then click on the Save button.

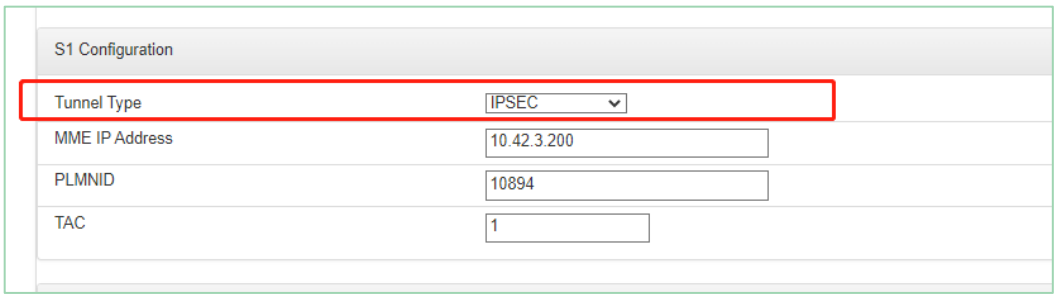


If you want to set IPSec mode to PSK, you can refer to below configuration.



3. Modify the Tunnel type

a) Enter Manage->LTE Basic Setting->S1 Configuration, Modify the value as follows:
Tunnel Type: IPSEC

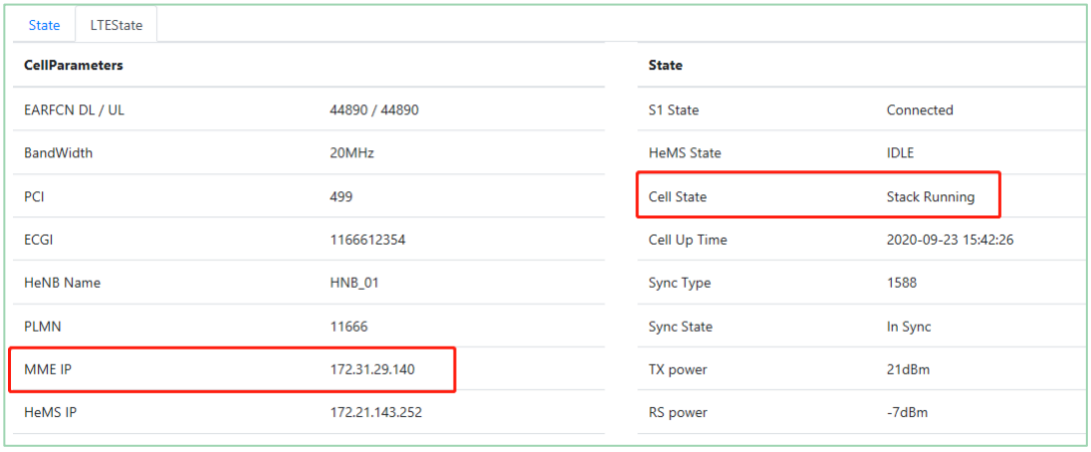


b) Then click on the Save button.
c) Please make sure you've configured other cell parameters properly following < How To Bring Up S1 With MME> manual, especially you need to change the default CellIdentity.
d) When everything is done, reboot the device and you are good to go.

(Tips: it may take a while for IPsec connect, please wait).

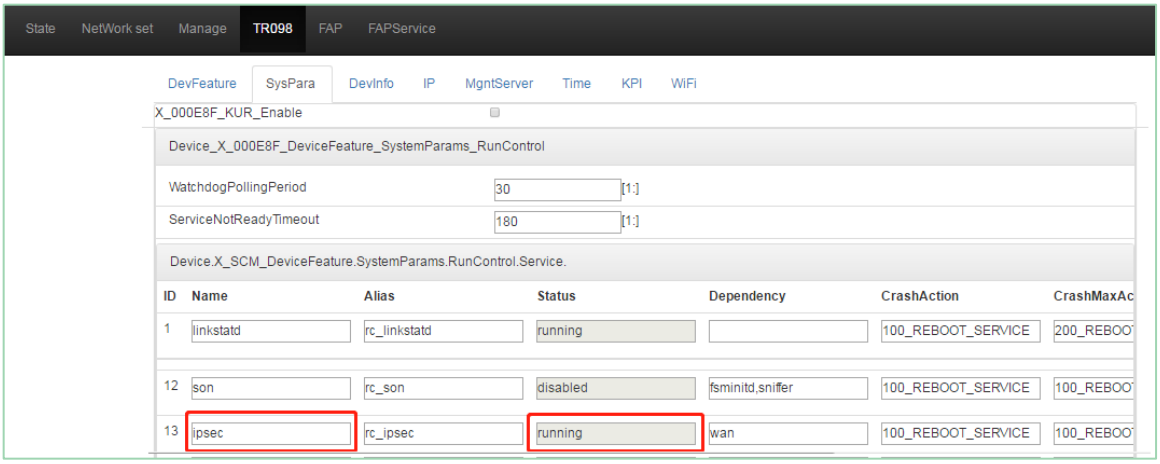
4. Check IPSec Status

You can view Cell status in LTE_status.htm webpage, if Cell is up, the status will be "Stack Running".



You can view IPsec status in TR098->SysPara->

Device.X_000E8F_DeviceFeature.SystemParams.RunControl.Service. If the IPsec is up, the status will be "running".



Besides, you can visit rma_support page(https://11.11.11.188/rma_support.htm) to check IPSec status, the web page will show that status is OK if IPSec is established successfully.

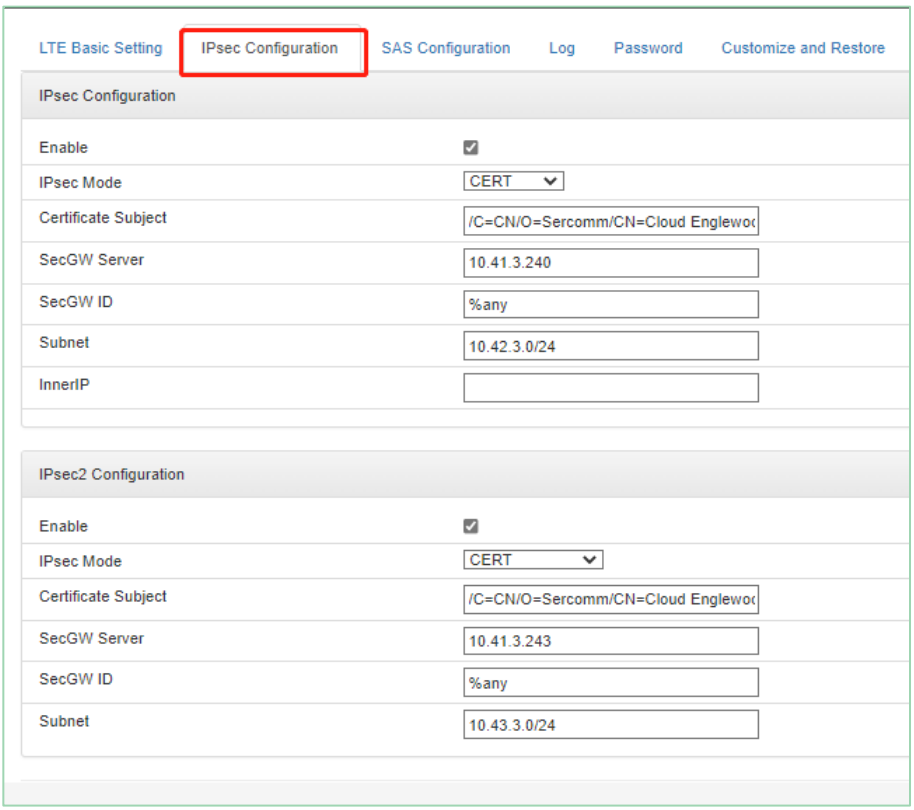
Data Model Nodes Table
Device.FAP.Tunnel.CryptoProfile.1.Enable
Device.FAP.Tunnel.UseForCWMP
Device.FAP.Tunnel.CryptoProfile.1.AuthMethod
Device.Services.FAPService.1.FAPControl.LTE.Gateway.SecGWServer1
Device.Security.X_000E8F_IPsec.X_000E8F_Ipsecconf.X_000E8F_Connection.1.X_000E8F_Rightid
Device.Security.X_000E8F_IPsec.X_000E8F_Ipsecconf.X_000E8F_Connection.1.X_000E8F_Rightsubnet
Device.Security.X_000E8F_IPsec.X_000E8F_Ipsecconf.X_000E8F_Connection.1.X_000E8F_Leftsubnet
Device.Security.X_000E8F_IPsec.X_000E8F_Ipsecsecrets.X_000E8F_Entries.1.X_000E8F_Secret

Multiple IPSec Configuration

This section provides details of the configuration of the Multiple IPSec tunnels, the qty can be 1 or 2. And the section “IPSec Configuration” only provides details of the configuration of one IPSec tunnel.

The Multiple IPSec is to set up two IPSec at the same time. And each IPSec has a different purpose, for example, the first IPSec is used to connect the first MME, and the second IPSec is used to connect the second MME.

1. Visit "Manage" page under "IPsec Configuration" group to configure the two IPsec tunnels.



Enable: to check it

IPsec Mode: choose CERT, because the second tunnel only support CERT mode now.

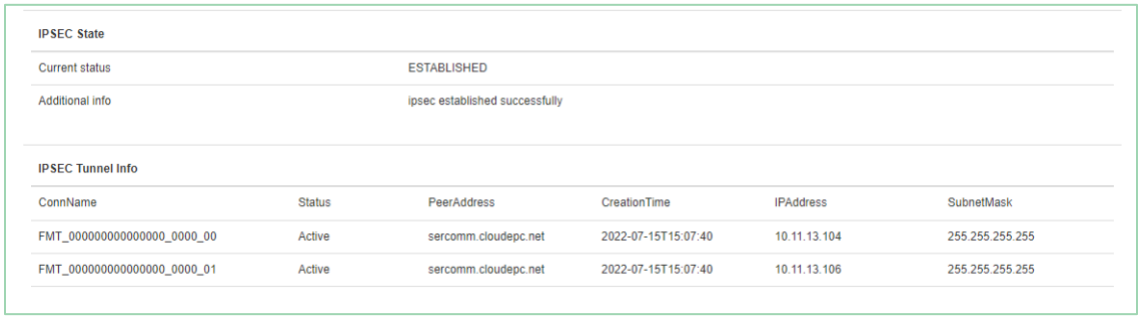
Certificate Subject: The cert subject of devices which can refer to page FAP->FAP_Security->Device.Security.Certificate.{i}.Subject

SecGW Server: server address

SecGW ID: rightid in ipsec.conf section

Subnet: rightsubnet in ipsec.conf section

2. Visit "State" -> "System Status" page to check IPSec status. The page will be shown in the following figure if the configuration is correct.

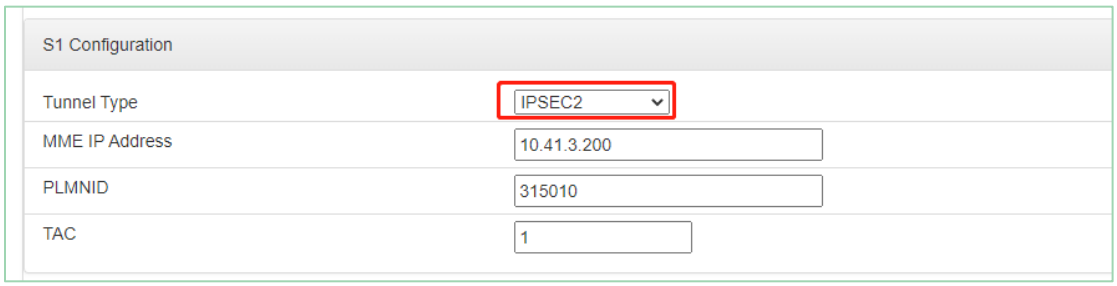


System Status Page

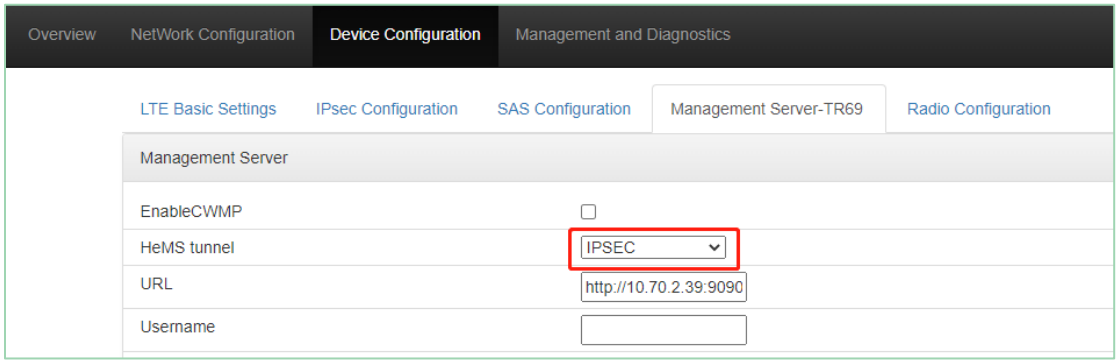
The 1st ConnName is configured with FMT_000000000000000_0000_00.

The 2nd ConnName is configured with FMT_000000000000000_0000_01.

3. Visit "Manage"->"LTE Basic Setting" to configure the tunnel of S1 connection.



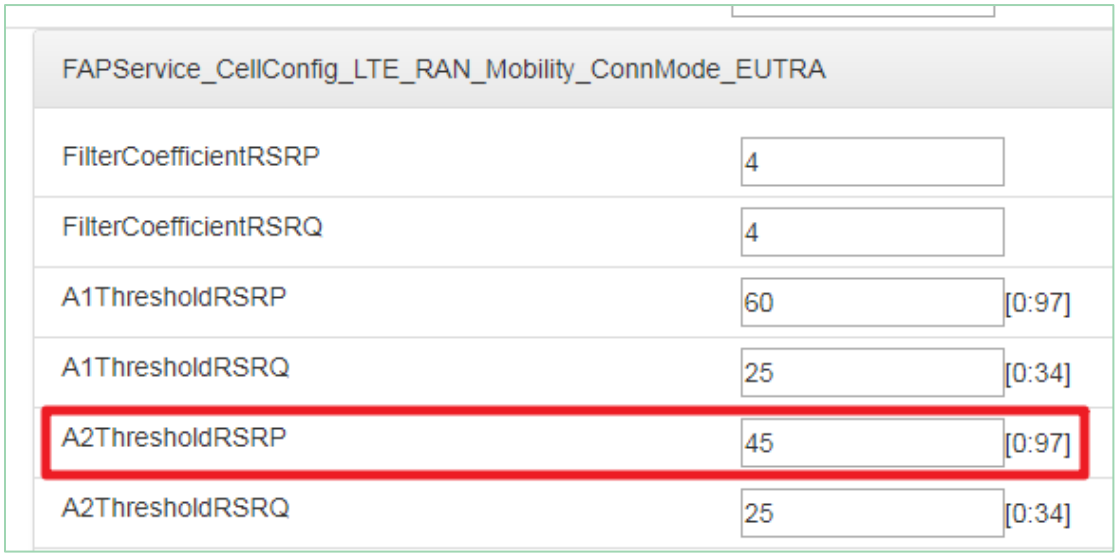
Visit "Device Configuration"->"Management Server-TR69" to configure the tunnel of cwmp. (This page is available to account operator.)



Modify Events Threshold

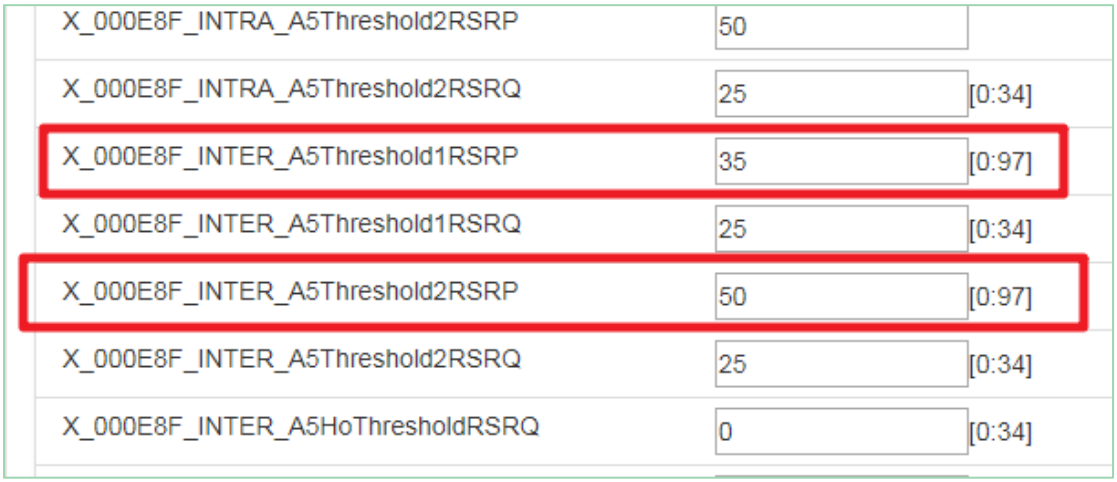
This section provides details of the configuration of A2 threshold and A5 threshold.

1. Visit "CellConfig" page under "FAPService" group to find "FAPService_CellConfig_LTE_RAN_Mobility_ConnMode_EUTRA" table to set A2ThresholdRSRP



2. In same page and same table, set X_000E8F_INTER_A5Threshold1RSRP and X_000E8F_INTER_A5Threshold2RSRP

The real threshold value will be the configuration value minus 140dBm, for example. A5 threshold1 will be -90dBm as 50-140 = -90



Data Model Nodes Table
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.A2ThresholdRSRP
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.X_000E8F_INTER_A5Threshold1RSRP
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.X_000E8F_INTER_A5Threshold2RSRP

Configure SAS

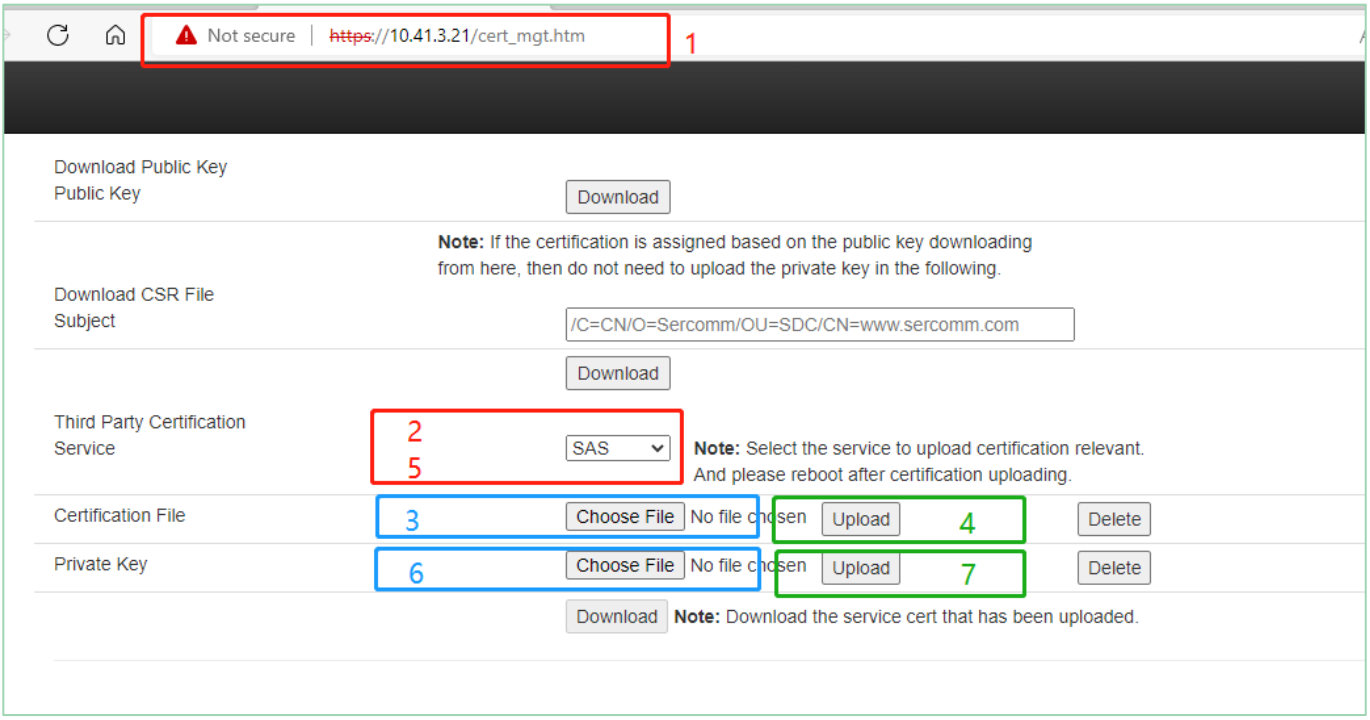
This section provides details of the configuration of SAS function.

1. SAS Cert Assign

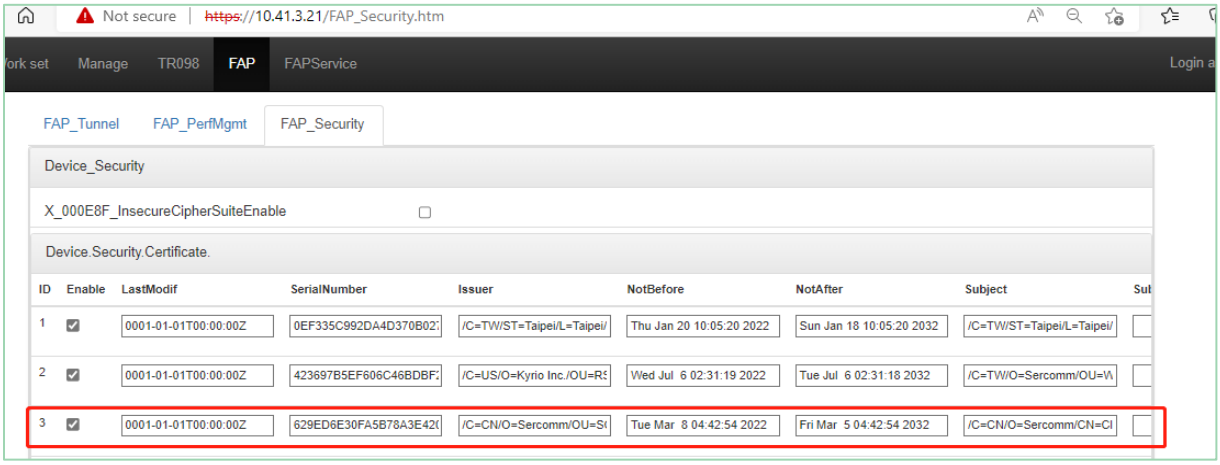
This section provides details of the assignment of the certificate files. These certificate files can be used to work with SAS or IPSec. IPSec cert assign steps are the same as SAS. By default, SAS and IPsec certificates should be assigned in manufacturing, and just jump to step (8). If you want to use your certificate, follow below steps.

SAS cert should have two file: cert.pem and key file. We need assign the cert to our device. they can upload by GUI.

1) Open Web Page Like below: 11.11.11.188 is the device IP. This page is hide page, so you should fill the whole address.(/cert_mgt.htm cannot be omitted)
2) Select "Third Party Certification Service" as SAS .
3) select "Certification File" to local cert file.
4) Click "Upload" to Assign cert file.
5) Select "Third Party Certification Service" as SAS.
6) Select "Private Key" to local key file.
7) Click "Upload" to Assign key file.

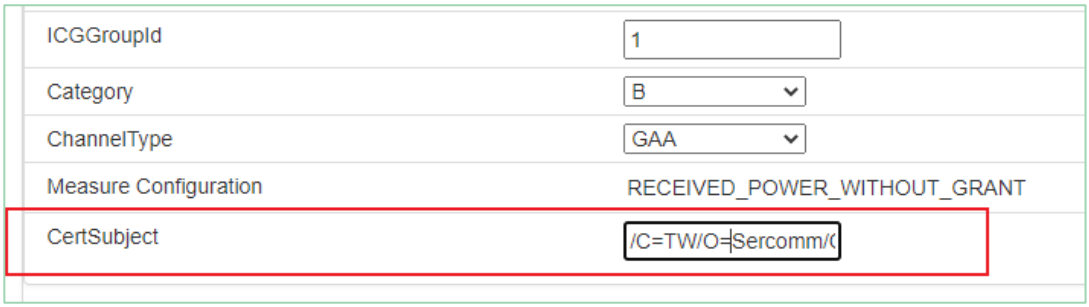


8) Reboot Device and check the "Device.Security Certificate." list in below picture. It will add a new cert. Check the "Subject" value to validate the cert.



9) Configure the "CertSubject" item in table

SAS Configuration of Manage->SAS Configuration page with the Subject value see from above setup. See the below Picture.

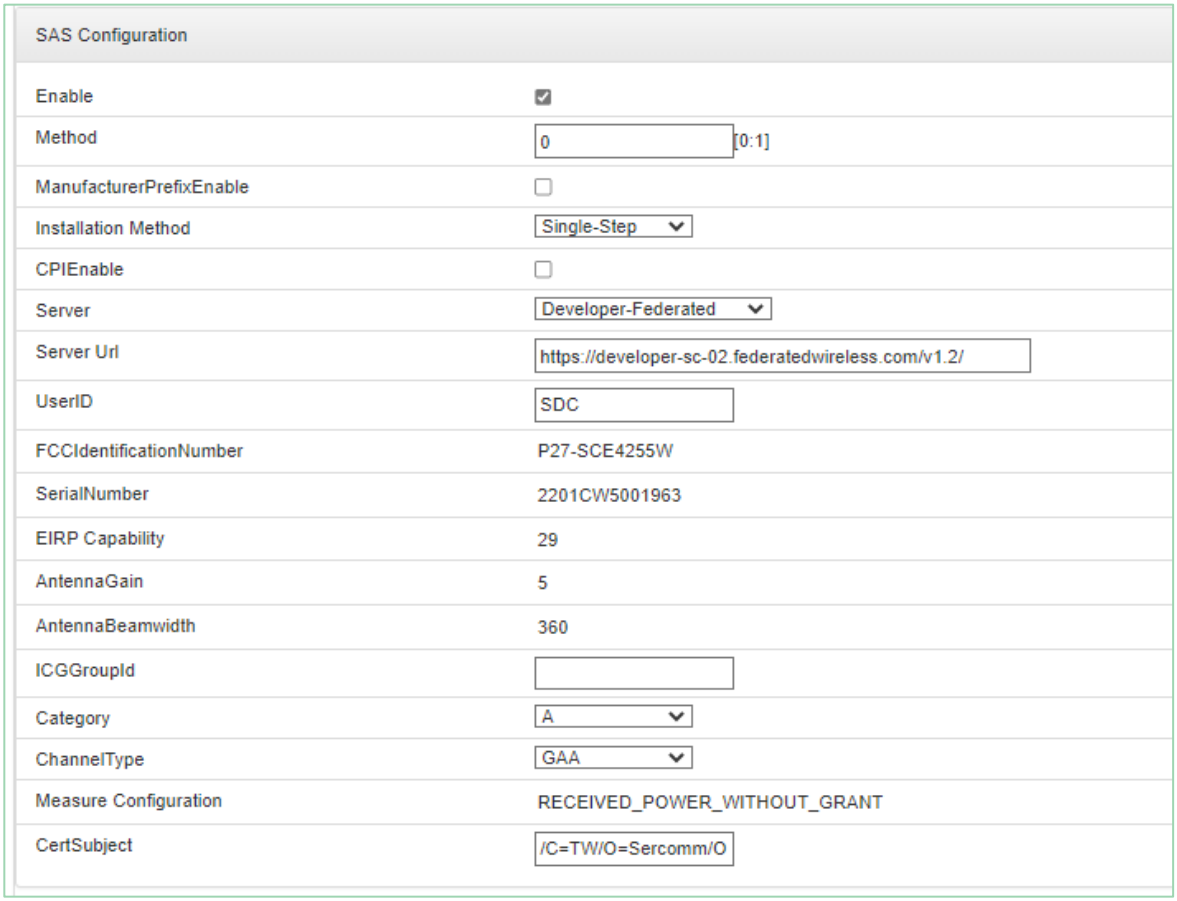


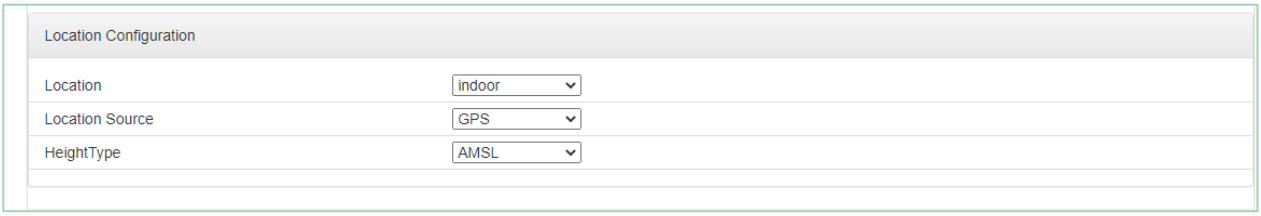
2. Visit "SAS Configuration" page under "Manage" group to configure the SAS function and manually input Location if GPS can't work.

Single step (CPI disable):

SAS OAM Configuration

Parameter	value
SAS Enable	Enable
Method(support from FF3922)	0
ManufacturerPrefixEnable(Only the Google platform may need to be enabled)	Disable
Installation Method	Single-step
CPI Enable	Disable
Server	https://developer-sc-02.federatedwireless.com/v1.2/[sample]
UserID	SDC[sample]
ICGGroupId	1
Category	A
ChannelType	GAA
CertSubject	/C=TW/O=Sercomm/OU=WInnForum CBSD Certificate/CN=P27-SCE4255W:%s
Location	indoor
Location Source	GPS
HeightType	AMSL



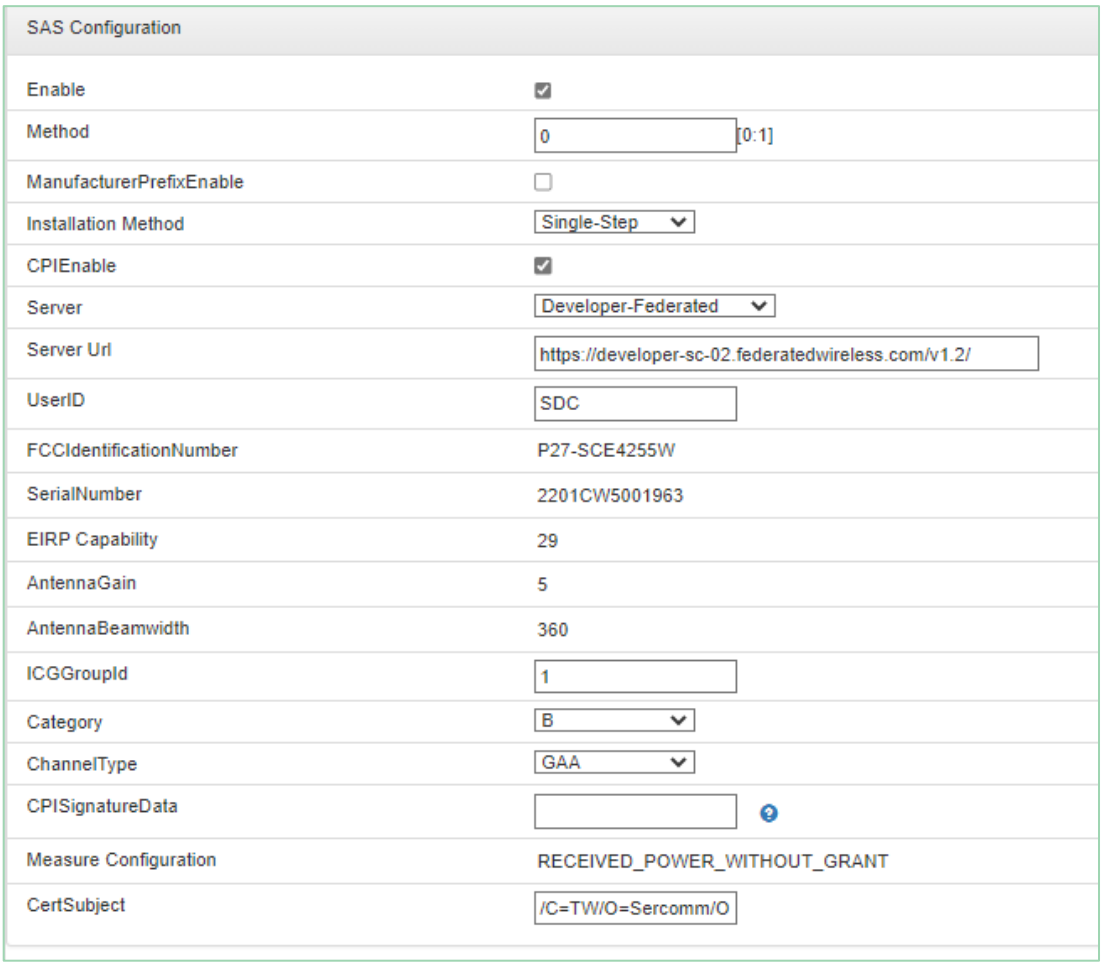


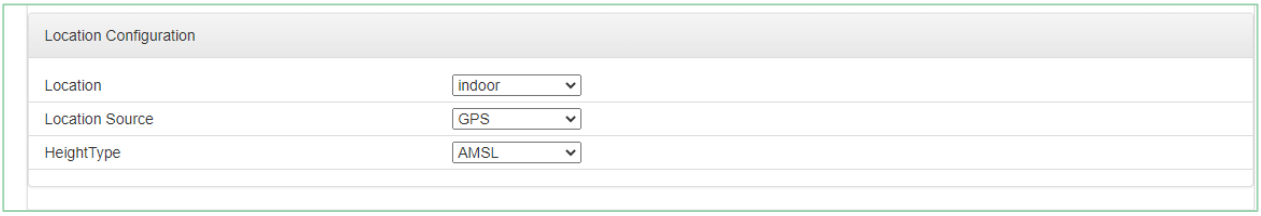
Single step (CPI enable):

SAS OAM Configuration

Parameter	value
SAS Enable	Enable
Method (support from FF3922)	0
ManufacturerPrefixEnable (Only the Google platform needs to be enabled)	Disable
Installation Method	Single-step
CPI Enable	Enable
Server	https://developer-sc-02.federatedwireless.com/v1.2/[sample]
UserID	SDC[sample]

ICGGroupId	1
Category	B
ChannelType	GAA
CPISignatureData	ABCD[sample]
CertSubject	/C=TW/O=Sercomm/OU=WInnForum CBSD Certificate/CN=P27-SCE4255W:%s
Location	indoor
Location Source	GPS
HeightType	AMSL

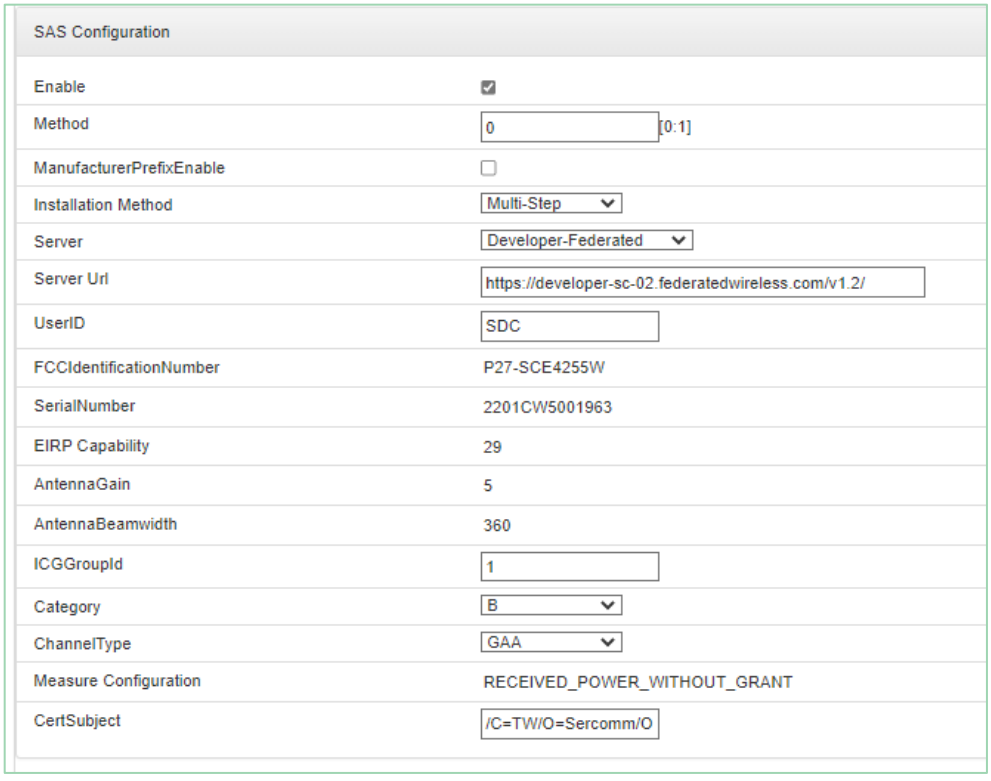


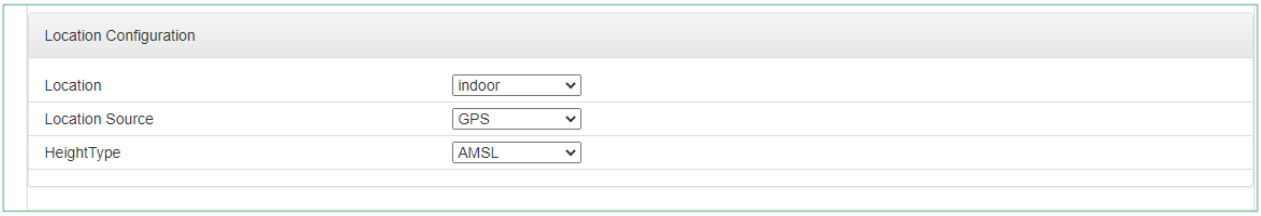


Multi step:

SAS OAM Configuration

Parameter	value
SAS Enable	Enable
Method (support from FF3922)	0
ManufacturerPrefixEnable (Only the Google platform needs to be enabled)	Disable
Installation Method	Multi-step
Server	https://developer-sc-02.federatedwireless.com/v1.2/[sample]
UserID	SDC[sample]
ICGGroupId	1
Category	B
ChannelType	GAA
CertSubject	/C=TW/O=Sercomm/OU=WInnForum CBSD Certificate/CN=P27-SCE4255W:%s
Location	indoor
Location Source	GPS
HeightType	AMSL





Enable: Turn on the SAS function, the Moso Canopy will use the EARFCNDL/UL set in "LTE Basic Setting" page to query spectrum for enable S1.

Method: SAS method 0: SAS Client 1: SAS Domain proxy

ManufacturerPrefixEnable: Enable or disable CBSD serial number with manufacturer's name.

Installation Method: Single-Step Registration refers to the Registration procedure where the REG-Conditional parameters are included in the "RegistrationRequest Object". Multi-Step Registration refers to the Registration procedure in which the "REG-Conditional" parameters are preloaded into the SAS UUT prior to initiating the CBSD Registration Procedure and excluded from the CBSD Registration Request Message

CPIEnable: Enable or disable CBSD registration with CPI data.

Server: SAS server

Server URL: SAS server URL

UserID: Required by CFR 96.39(c). User contact information can be inferred from a registered User ID to which the CBSD Reqistration is tied.

ICGGroupId: ICG Group ID

Category: If an indoor device, configure Category to be "A"; if an outdoor device, configure Category to be "B".

ChannelType: PAL or GAA. Instead of having it in the registration, providing protection level in grant request allows more flexible operation of CBSD. For PAL use, a PAL ID and authentication credential must be presented for access.

CertSubject: The Distinguished Name (DN) of the entity associated with the Public Key; i.e., the Subject field in an X.509 certificate, see [RFC5280].

Location: Indoor or Outdoor device

Location Source: Manual Input or GPS

Latitude: manually input Latitude. Value equal to latitude multiply 1 million.

Longitude: manually input Longitude. Value equal to longitude multiply 1 million.

HeightType: The value should be "AGL" or "AMSL". AGL height is measured relative to the ground level. AMSL height is measured relative to the mean sea level.

Elevation: manually input Elevation

Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.Enable
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.Method
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.ManufacturerPrefixEnable
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.CPIEnable
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.Server

Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.UserContactInformation
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.ICGGroupId
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.Category
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.ProtectionLevel
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.CertSubject
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.Location
Device.FAP.GPS.LockedLatitude
Device.FAP.GPS.LockedLongitude
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SAS.HeightType
Device.FAP.GPS.X_000E8F_Elevation

Setup for S1 or X2 Handover

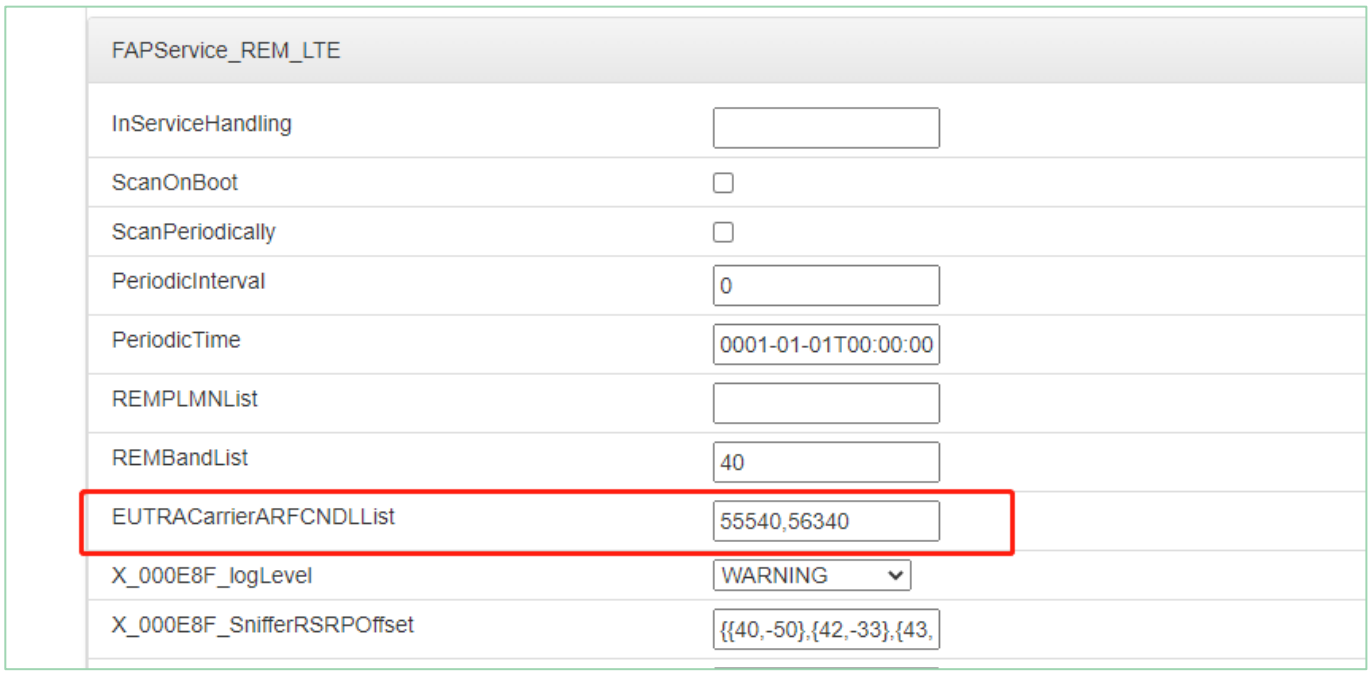
This section provides details of the configuration of S1 or X1 handover function.

1. Visit "REM" page under "FAPService" group to enable "X_000E8F_X2InterfaceConfig" if X2 Handover is needed, otherwise S1 Handover will work.

Data Model Nodes Table
Device.Services.FAPService.1.REM.LTE.X_000E8F_X2InterfaceConfig

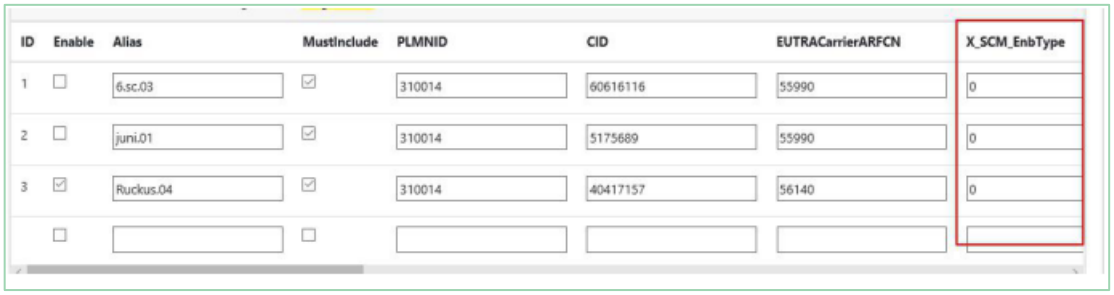
2. Refer to “Add One Neighbor Cell” section to manually add Neighbor Cell.

3. Visit "REM" page under "FAPService" group to find "FAPService_REM_LTE" table to set "EUTRACarrierARFCNDLList". This is needed to set ANR frequency. This list is comma-separated (maximum length 256) of strings and each entry is a EARFCN in the DL direction to measure.



Data Model Nodes Table
Device.Services.FAPService.1.REM.LTE.EUTRACarrierARFCNDLList

4. The eNB type of neighbor cell must be set correctly. Otherwise Handovers will fail. When adding neighbor cell manually, X_000E8F_EnbType needs to be set for each neighbor cell entry: 0 means Macro eNB and 1 means Home eNB.



The PCI range of different type eNB will need to be configured if using ANR to add neighbor cell. Visit "FAPControl" page under "FAPService" group to configure X_000E8F_CSGSmallCellPCIStart and X_000E8F_CSGSmallCellPCIRange. In the following figure, PCI range of Home eNB is from 485 to 503 (both 485 and 503 are included).

Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_RRMConfig.X_000E8F_CSGSmallCellPCIStart
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_RRMConfig.X_000E8F_CSGSmallCellPCIRange

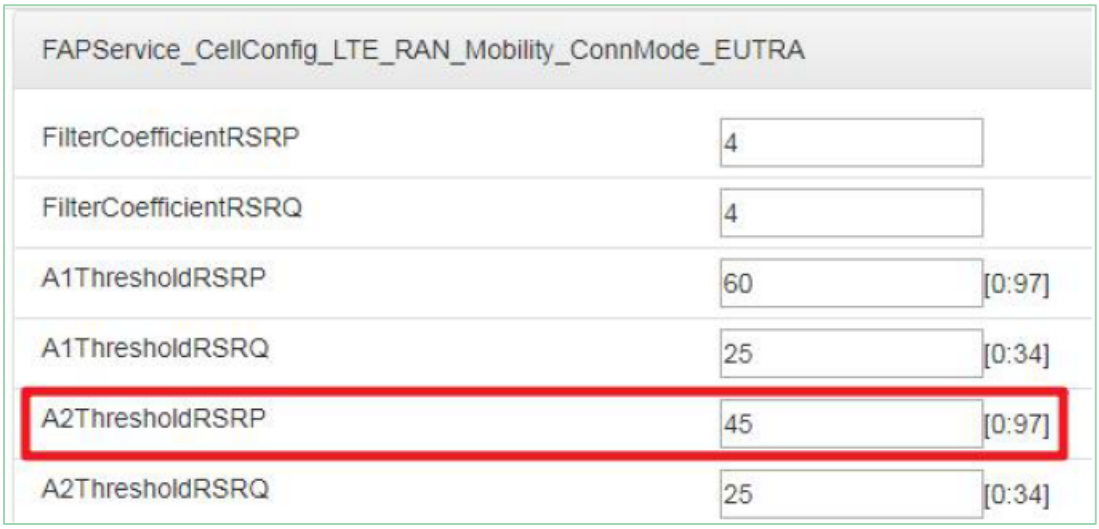
5. Visit "CellConfig" page under "FAPService" group to find "FAPService_CellConfig_LTE_RAN_Mobility_ConnMode_EUTRA" table to set Intra-frequency handover parameter "A3Offset"

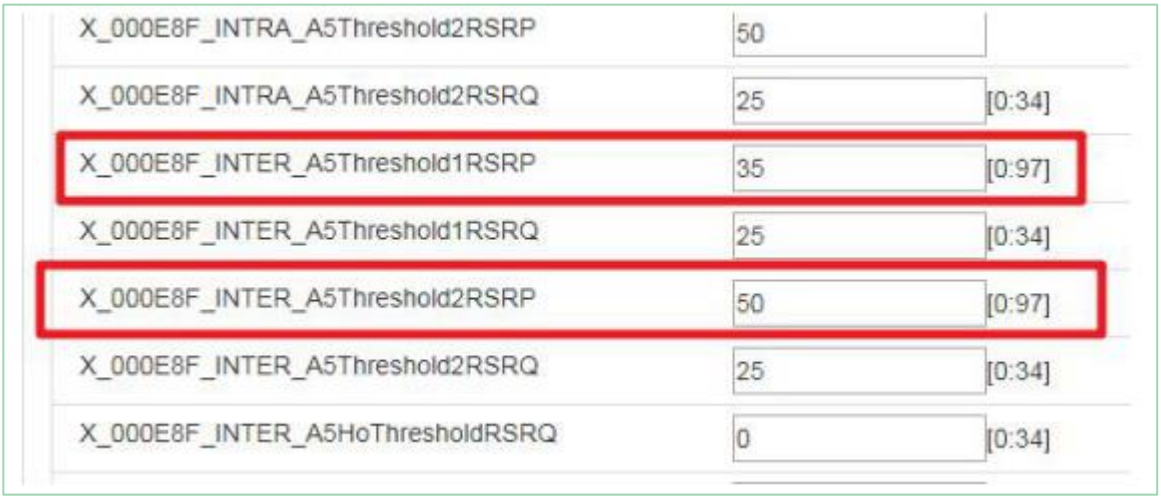
Data Model Nodes Table
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.A3Offset

6. Visit "CellConfig" page under "FAPService" group to find "FAPService_CellConfig_LTE_RAN_Mobility_ConnMode_EUTRA" table to set Inter-frequency handover parameters "A2ThresholdRSRP", "X_000E8F_INTER_A5Threshold1RSRP" and "X_000E8F_INTER_A5Threshold2RSRP".

The real value equals to (configuration value - 140)dBm. Ex. A5 threshold1 is 35-140=-105dBm.

The A1Threshold couldn't be less than A2Threshold.





SON Configuration

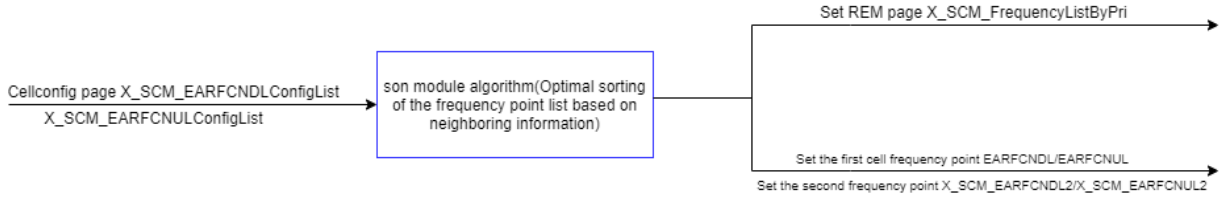
This section provides details of the configuration of the SON function.

The SON function depends on the sniffer feature. The "Sniffer" will need to be enabled first. The SON function works when the configured EARFCN and PCI value are greater than cell number.

The system supports EARFCN and PCI self-configuration functions. If SON function are enabled, it will automatically selects the best frequency and PCI from the configured frequency list and PCI list according to the current environment of the cell.

EARFCN self-optimization:

If the Son function is enabled, Son will continue to configure the frequency point after the page is set：

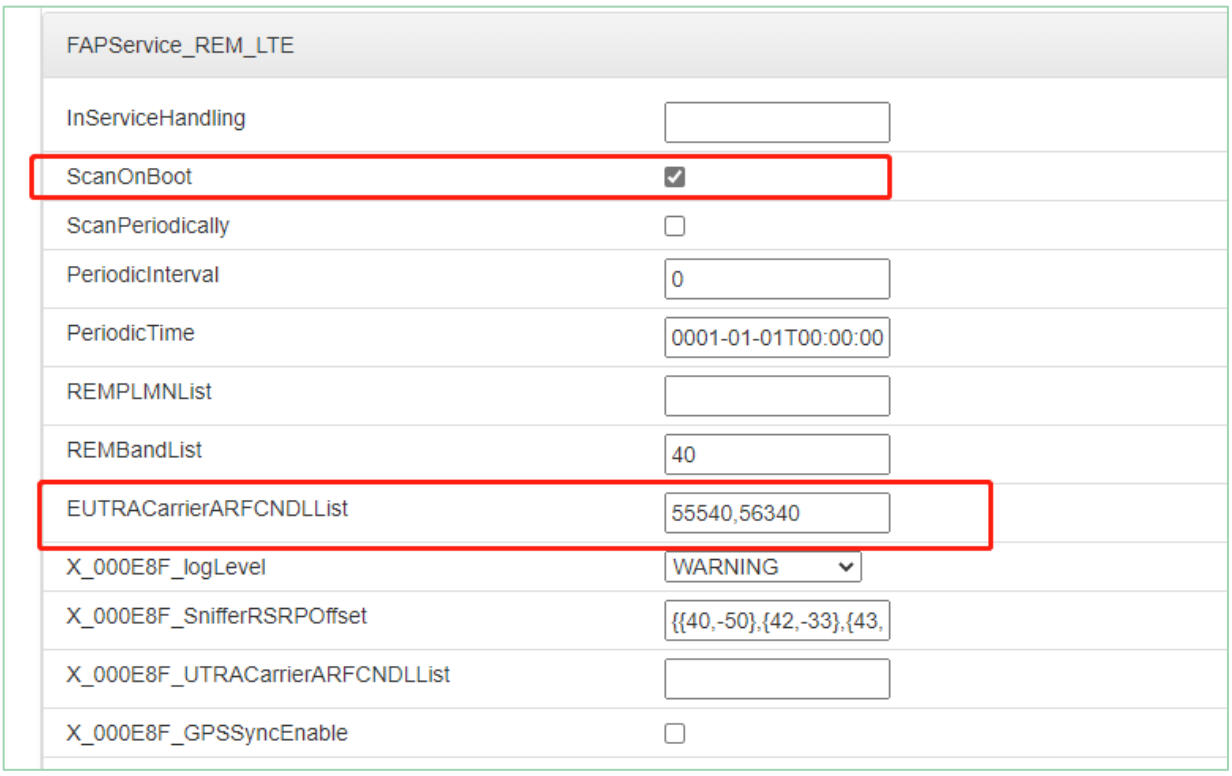


PCI self-optimization:

(1) The PCI of the cells is selected in order from the PCI List.

(2) Starting from the first PCI in PCI List, compare the dl Earfcn and new Pci of the cell with the neighbor cell. When the frequency of the cell is consistent with the neighbor cell, compare whether the new PCI and the PCI of the neighboring cell have a modulus (Mod3, Mod6, Mod30) conflict or whether they are the same; secondly, check whether the dl Earfcn and new PCI of the cell are consistent with the neighbor cell of the neighbor cell. If the detection fails, select the next one in the PCI List, the method is as step two.

1. Visit "REM" page under "FAPService" group and Setting "ScanOnBoot" and "EUTRACarrierARFCNDLList"under "FAPService_REM_LTE". EUTRACarrierARFCNDLList should be Comma-separated EARFCNs list which needs to be scanned before cell is UP.



Data Model Nodes Table
Device.Services.FAPService.1.REM.LTE.ScanOnBoot
Device.Services.FAPService.1.REM.LTE.EUTRACarrierARFCNDLList

2. Visit "FAPSON" page under "FAPService" group to enable "X_000E8F_SonEnable".

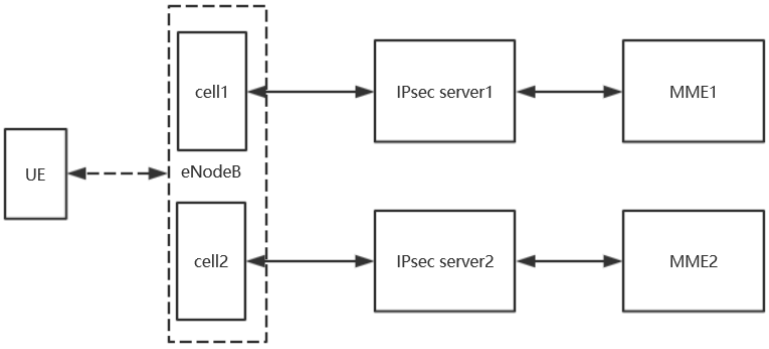
Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_SON.X_000E8F_SonEnable

Multiple Source IP Configuration

This section provides details of the configuration of the Multiple Source IP.

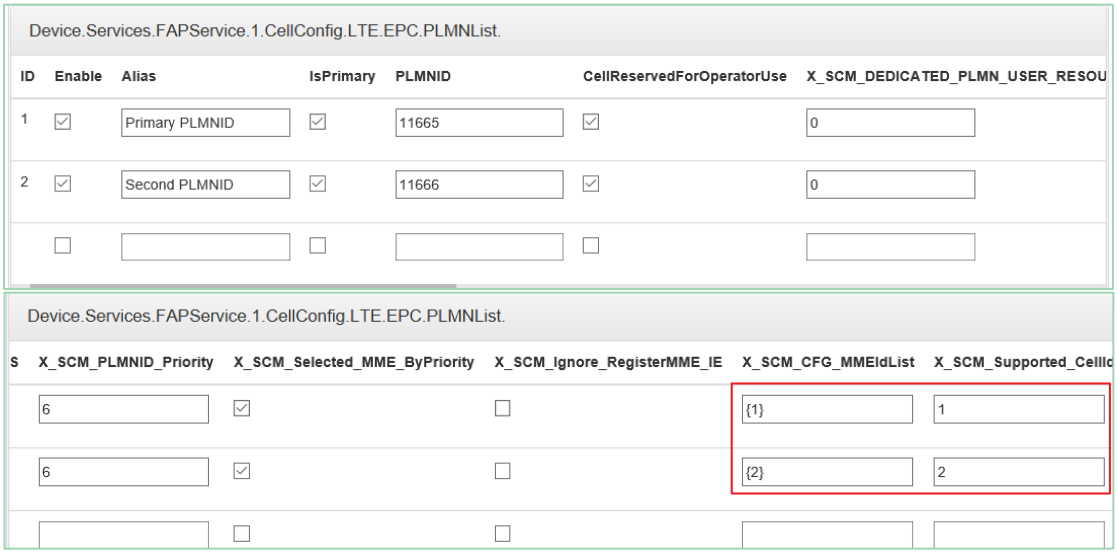
The WAN of the Moso Canopy will get the dynamic IP address from the DHCP Server and the Moso Canopy will also get multiple IP addresses in IPSec tunnels from multiple IPSec server after the multiple IPSec function was configured (in section “Multiple IPSec Configuration”), then by referring this chapter, the administrator will be able to use these IP addresses in IPSec tunnels to setup the multiple MME.

Of course, the administrator can still keep the WAN IP addresses of Moso Canopy to setup the multiple MME.



1. Visit "FAPControl"page under "FAPService"group to configure two MME address.

2. Visit "Cellconfig" page under "FAPService" group to configure two PLMMID.

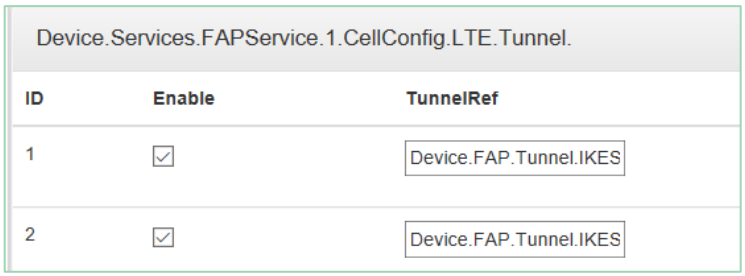


In the red block diagram of above figure, the first cell uses the first MME and IPSec and the second cell uses the second MME and IPSec.

3. Visit "LTE Basic Setting" page under "Manage" group to set carrier number.

4. Visit "LTE Basic Setting" page under "Manage" group to set Tunnel type to be IPSec.

5. Visit "Cellconfig" page under "FAP_Service" group to add a Tunnel.

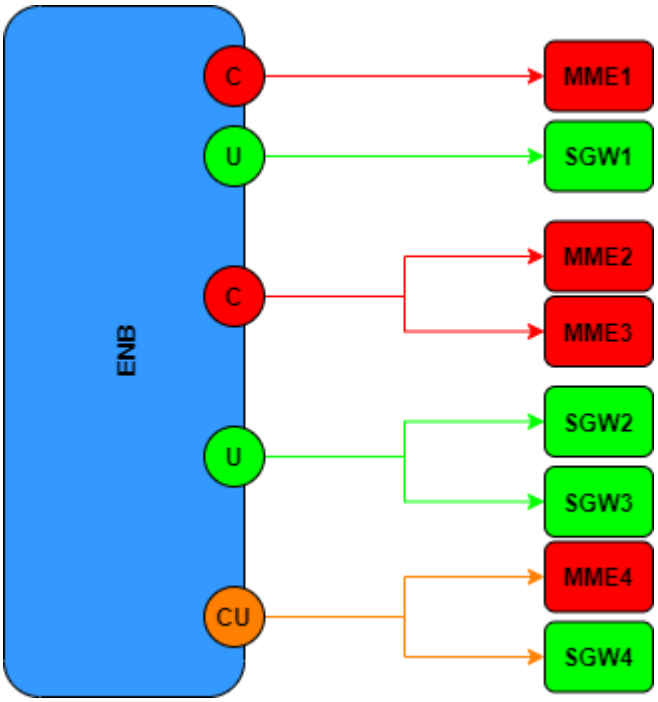


TunnelRef: set 1st one to Device.FAP.Tunnel.IKESA.1 and set 2nd one to Device.FAP.Tunnel.IKESA.2.

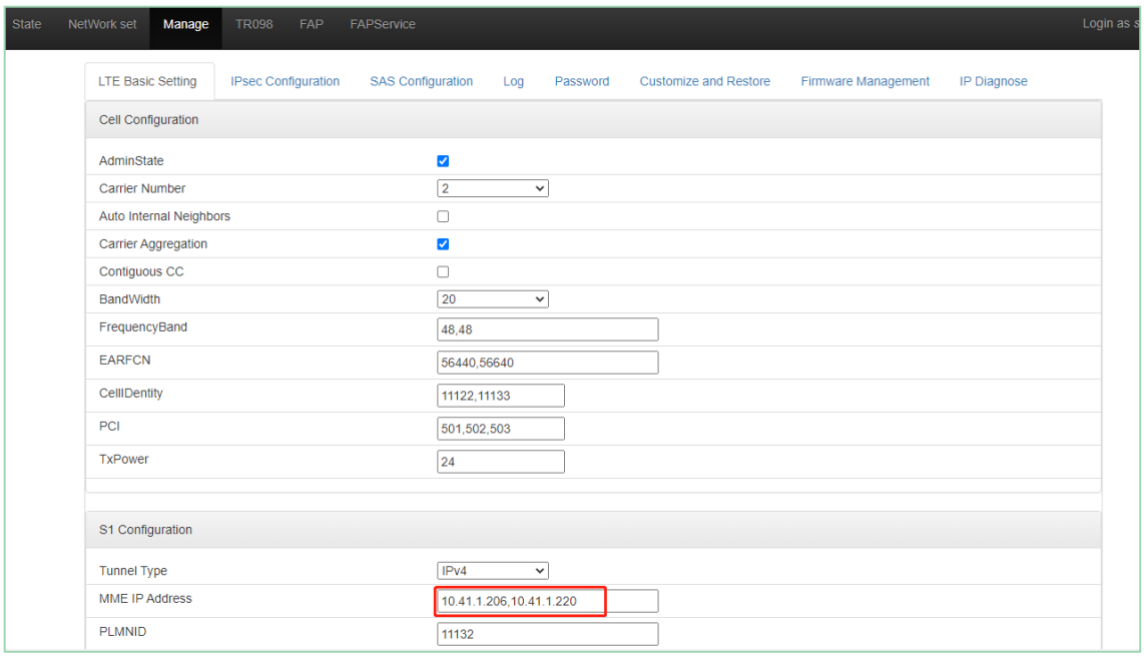
Split C/U Plane for MoCN

This section introduces how to split the control plane and user plane by using different IP address.

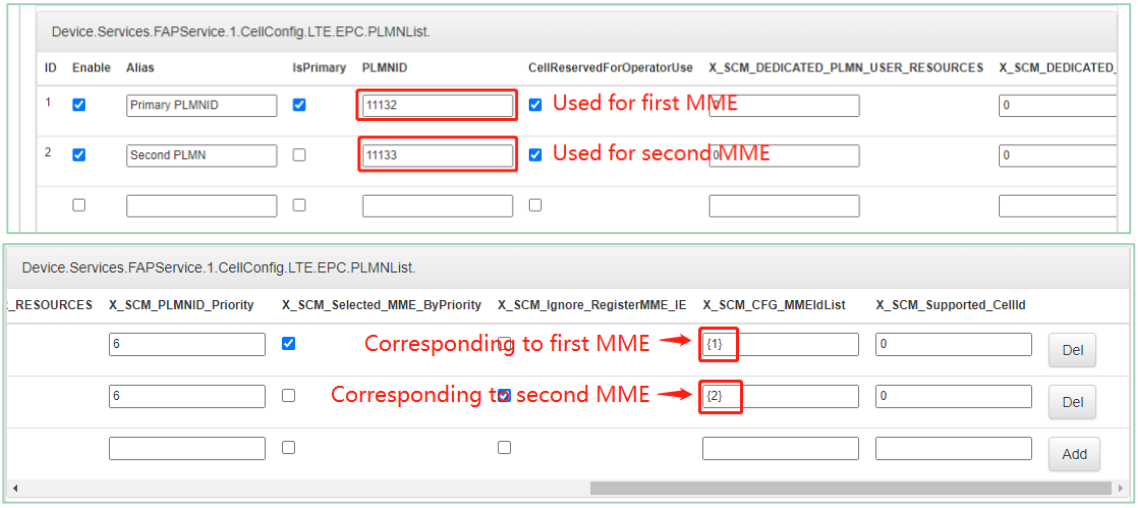
The eNB can be configured to different interface IP to make control plane connect to different MMEs and make user plane connect to different SGWs.



1. Visit Manage->LTE Basic Setting page to add Multi MME IP address.

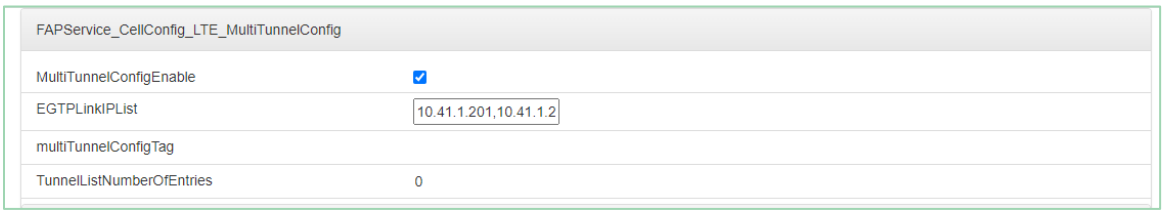


2. Visit FAPService->CellConfig page to configure the PLMN according to different MMEs.



For explanation of nodes, please refer to section “Bring up S1 with MME.”

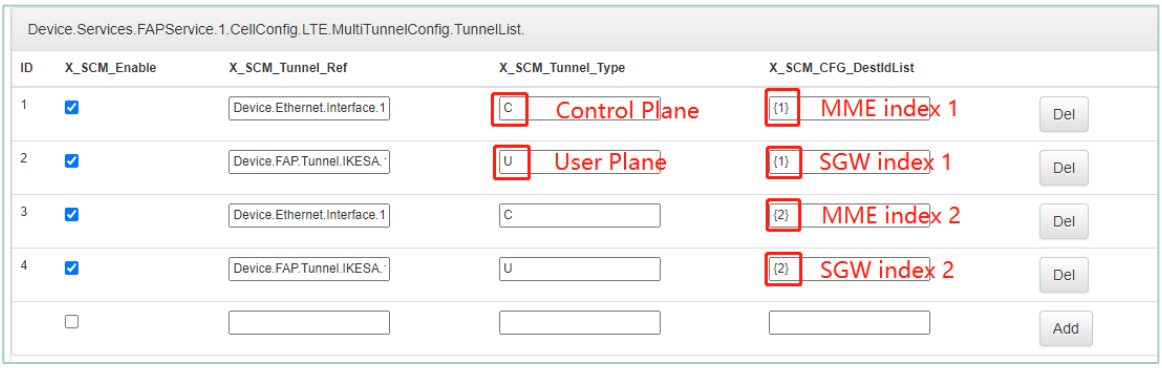
3. Visit FAPService->CellConfig page to configure the SGW IP (such as 10.41.3.201,10.41.1.207) and then to enable the function.



MultiTunnelConfigEnable: enable the function.

EGTPLinkIPList: SGW IP configure List.

4. Visit FAPService->CellConfig page to configure the tunnel list



X_000E8F_Enable: enable the tunnel list.

X_000E8F_Tunnel_Ref: the corresponding interface IP. For example, “Device.Ethernet.Interface.1.” means the data will go out of the IPsec tunnel and “Device.FAP.Tunnel.IKESA.2.” means the data will go through the IPsec tunnel.

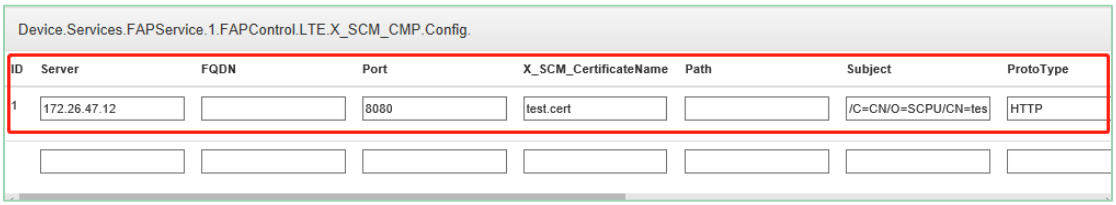
X_000E8F_Tunnel_Type: indicate the tunnel list is used for control plane or user plane. “C” means control and “U” means user plane.

X_000E8F_CFG_DestList: index of corresponding MME or SGW. If the X_000E8F_Tunnel_Type is “C” which means it is an index of MME, otherwise is SGW.

CMP Configuration

The section provides details of CMP configuration.

1. First, the device must have the factory certificate and private key, and the root certificate has been placed on the CMP server.
2. Visit "FAPControl" page under "FAPService" group to set CMP configuration



Server: CMPv2 server IP address

Port: CMPv2 server service port

X_000E8F_CertificateName: Name of new certificate which request from CMP server (Suffix must be. Cert or. PEM or. Der) and name should be unique.

Path: CMPv2 server service path . eg. ejbca/publicweb/cmp

Subject: subject of new client certification

ProtoType: The protocol type of customer for theCMPv2, HTTP or HTTPS

Recipient: subject of the CMPv2 server certification, used to verify the CMPv2 server

CertEncodeMethod: CMPv2 the cert encode method (Optional, or fill in "V_ASN1_APP_CHOOSE"(default))

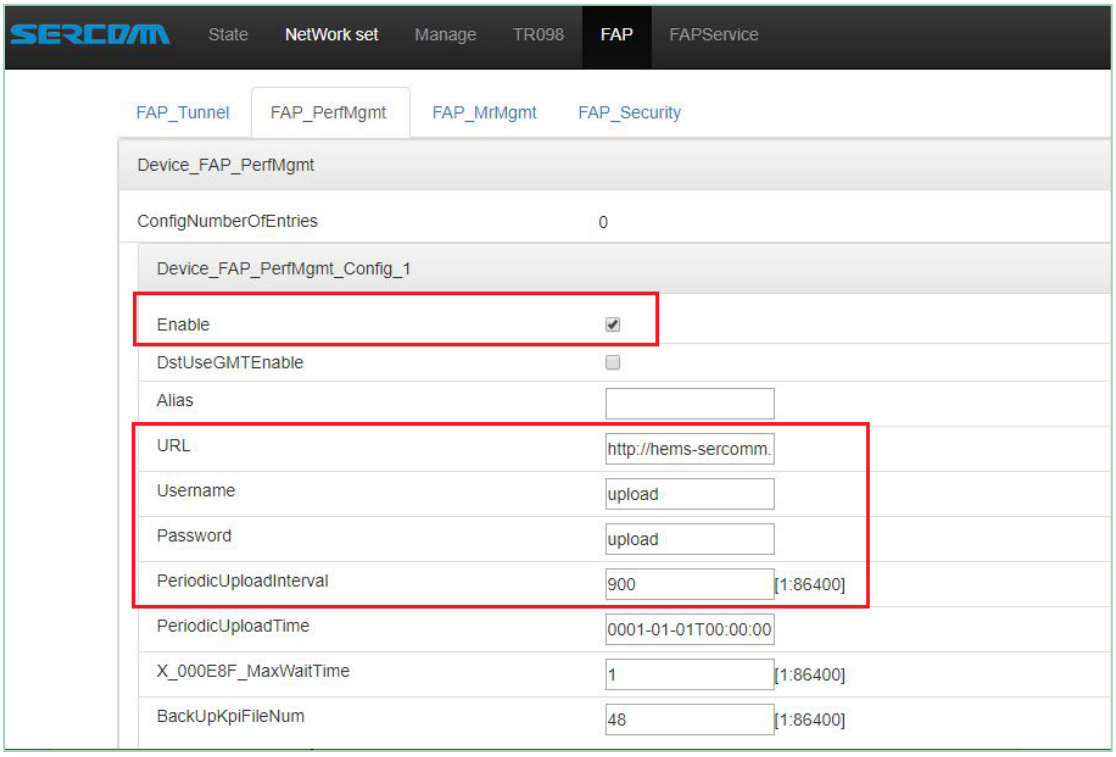
AltName: CMPv2 process needs to have an Alternative Name

Data Model Nodes Table
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.Server
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.Port
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.X_000E8F_CertificateName
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.Path
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.Subject
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.Recipient
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.CertEncodeMethod
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.AltName
Device.Services.FAPService.1.FAPControl.LTE.X_000E8F_CMP.Config.{i}.ProtoType

KPI Configuration

This section provides details of the configuration of KPI.

1. Visit "FAP_PerfMgmt" page under "FAP" group to the "Device.Security Certificate."



Enable: the KPI statistics function is turned on or off.
URL: URL is the address of file server for the XML file of KPI statistics upload.

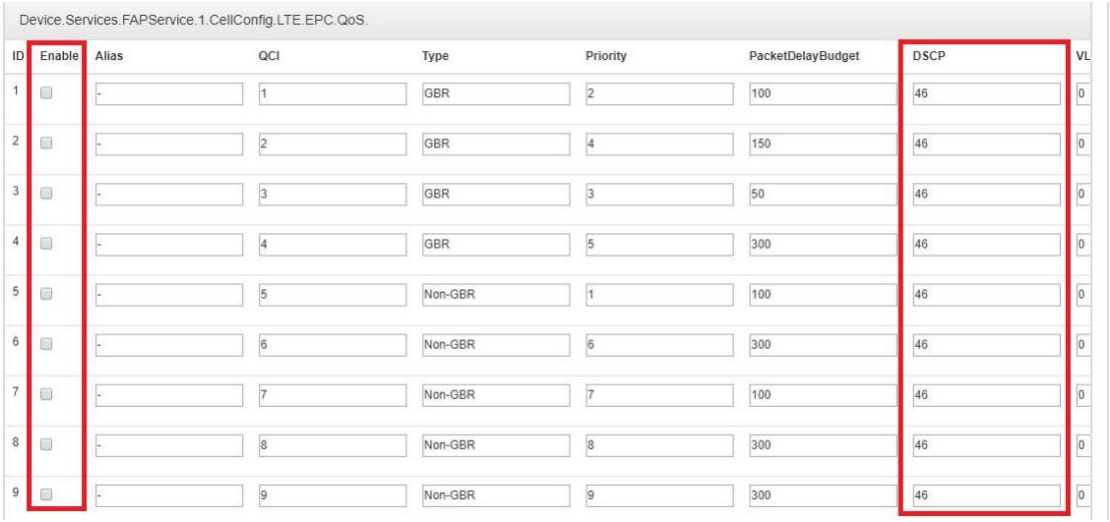
Username, Password: Username and password used by the device to authenticate the file server. If authentication is not used, it is set to an empty string.

PeriodicUploadInterval: The duration in seconds of the interval for which the device MUST create a Performance File. If Enable is true, try uploading the file to the URL and delete the local file.

DSCP Configuration

This section provides details of the configuration of DSCP of outgoing GTP packet.

Visit "CellConfig" page under "FAPService" group to "Device.Services.FAPService.1.CellConfig.LTE.EPC.QoS."



Device.Services.FAPService.1.CellConfig.LTE.EPC.QoS.

ID	Enable	Alias	QCI	Type	Priority	PacketDelayBudget	DSCP	VL
1	☐	-	1	GBR	2	100	46	0
2	☐	-	2	GBR	4	150	46	0
3	☐	-	3	GBR	3	50	46	0
4	☐	-	4	GBR	5	300	46	0
5	☐	-	5	Non-GBR	1	100	46	0
6	☐	-	6	Non-GBR	6	300	46	0
7	☐	-	7	Non-GBR	7	100	46	0
8	☐	-	8	Non-GBR	8	300	46	0
9	☐	-	9	Non-GBR	9	300	46	0

Enable: modify DSCP feature is turned on or off of corresponding QCI number

DSCP: specific DSCP number

NOTE: You need to click Modify button at the end of this line after you modify and then you need to click Save button at the bottom of this page.

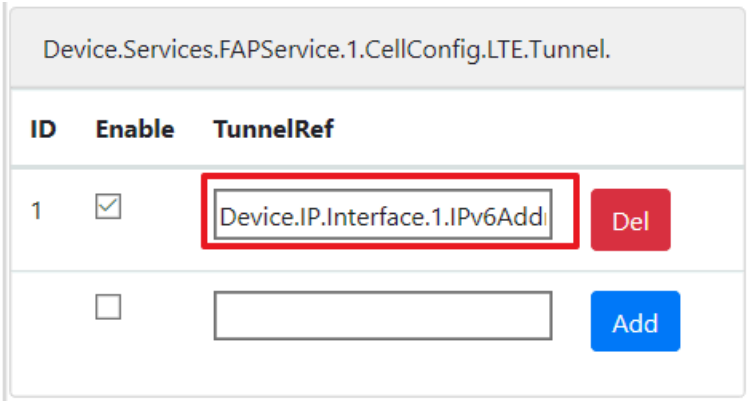
IPv6 Configuration

1. Please follow directions in section “Configure Device’s Network” to make device support IPv6.
2. IPv6 MME

If your MME IP address type is IPv6. You may need to modify TunnelRef of LTE tunnel too. Please visit "CellConfig" page under "FAPService" group and set tunnel reference to be Device.IP.Interface.1.IPv6Address.1.. Normally, you just need to modify "4" to "6".

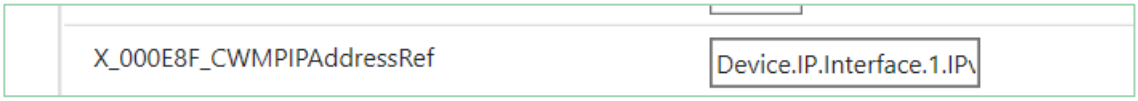
But if your MME IP address type is IPv4, you may need to check this config and make sure it is IPv4.

NOTE: Our default value is IPv4.



3. IPv6 EMS

Similar to MME, if your EMS IP address type is IPv6, you may need to modify EMS tunnel type too. Please visit "MgntServer" page under TR098 group. Please set X_000E8F_CWMPIPAddressRef following MME tunnel rules.

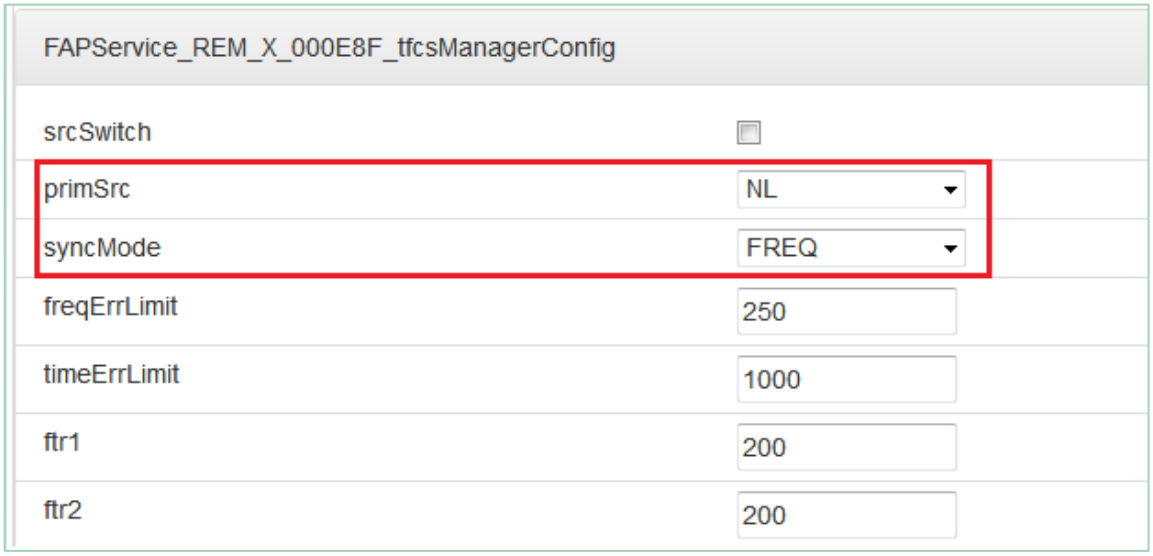


Moso Canopy NL Syn Configuration

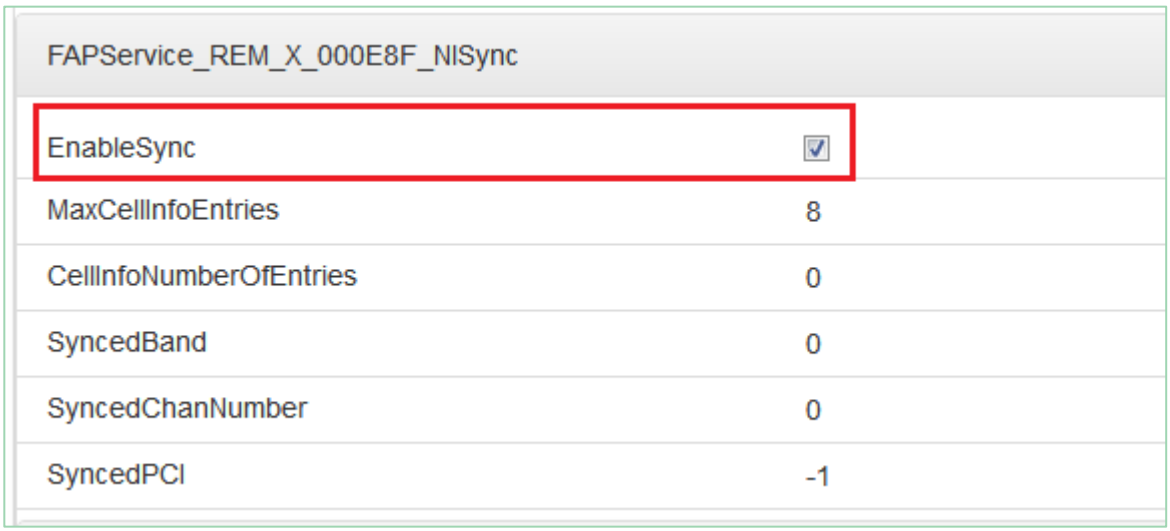
This section provides details of the configuration of the NL sync.

Visit "REM" page under "FAPService" group:

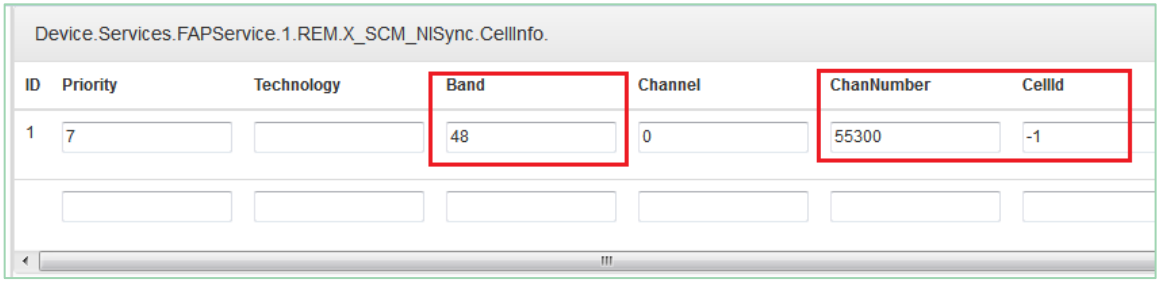
1. Under "FAPService_REM_X_000E8F_tfcsManagerConfig", set primSrc to be NL, and syncMode to be FREQ or PHASE.



2. Under "FAPService_REM_X_000E8F_NlSync", enable EnableSync.



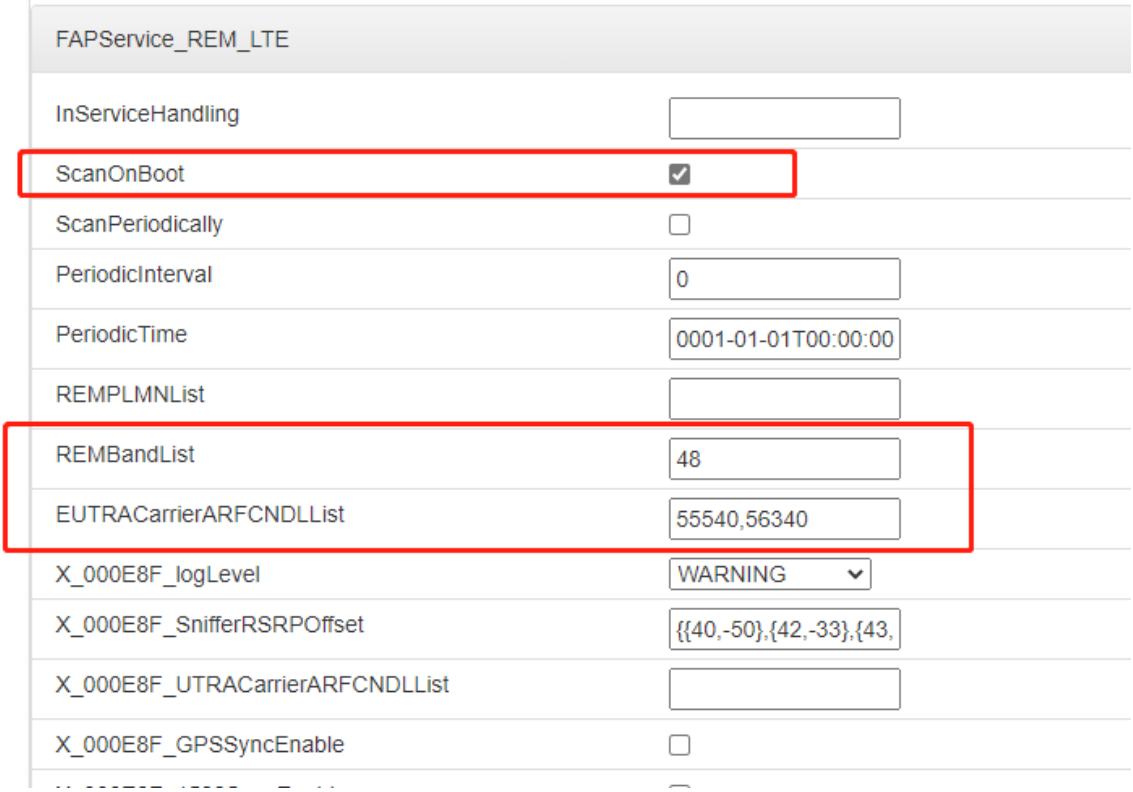
3. Under "Device.Services.FAPService.1.REM.X_000E8F_NISync.CellInfo", add an entry to set the sync source cell information. Set the right "Band" info, "ChanNumber" means the earfcn , and "CellId means the PhyCellID(PCI)". Setting "CellId" to be "-1" means that it will synchronize with all cells at this earfcn.



Volta OTA Syn Configuration

Visit "REM" page under "FAPService" group:

1. Enable ScanOnBoot. Enabled means to open the Sniffer function, disabled means to close the sniffer function. Then change REMBandlist and EUTRACarrierARFCNDLList. EUTRACarrierARFCNDLList is the frequency point of the configured sweep frequency.



Change PrivateAlgCtrl bit0 to 1， because it means to turn on the synchronization function, on the contrary,bit0 =0 means to turn off the synchronization function.

Restart the cell, then you can see the following information.

State	
S1 State	Connected
HeMS State	Connected
Cell State	Stack Running
Cell Up Time	2020-07-30 17:59:01
Sync Type	OTA
Sync State	In Sync
Sync PCI	49
Sync Earfcn	45090
TX power	21dBm
RS power	-7dBm

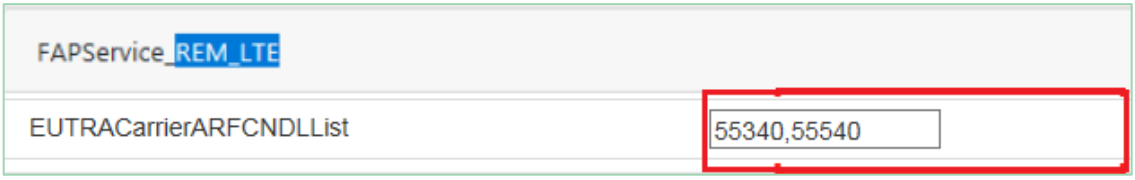
ANR Configuration

1. Enable ANR

Enter FAPService->FAPControl page, configure enable parameter:

AnrReportConfigValue: Enable or disable ANR feature. 0 means disable ANR and is default value, 3 means enable ANR.

Enter FAPService->REM page, configure EARFCN list:



EUTRACarrierARFCNDLList: This is a comma-separated list and means which EARFCN numbers will be configured into UE for ANR measurement.

2. PCI Range Configuration

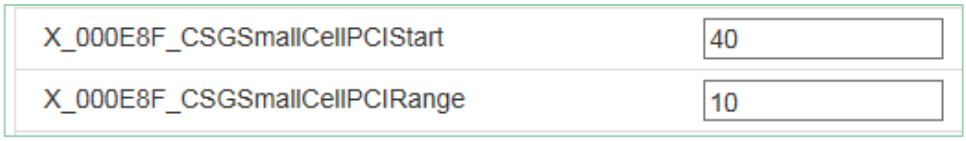
According to above ANR configurations, UE will try to measure specific EARFCN and find existed neighbor cells. If measured, UE will report ECGI info of the neighbor cell to serving cell. But serving cell cannot know whether reported neighbor cell is macro or home cell. So our eNodeB uses the specific configuration to pre-assign small cell PCI range. If neighbor cell's PCI is in the range of small cell, neighbor cell is home type. If neighbor cell's PCI is out of range of small cell, neighbor cell is macro type.

So for serving eNodeB and neighbor eNodeB, they should keep the same configuration for small cell PCI range. Small cell PCI range configuration should be set in FAPService->FAPControl:

Default value for CSGSmallCellPCIStart and CSGSmallCellPCIRange is 0, means all PCIs are used for macro cell.

For example:

If your server eNodeB is enabled ANR and Small cell PCI range is configured as below, then your neighbor eNodeB should also set the same configuration for small cell range, which means PCI in the range of 40~49 is used for home cell and the other PCIs are used for macro cell.



There will be 4 alternative configuration groups for two carrier disabled case:

1) Neighbor cell PCI is configured into home type, such as 45 and serving cell is configured into home type, such as 47, then serving cell will add this neighbor cell into home cell by ANR;
2) Neighbor cell PCI is configured into home type, such as 45 and serving cell is configured into macro type, such as 55, then serving cell will add this neighbor cell into home cell by ANR;
3) Neighbor cell PCI is configured into macro type, such as 55 and serving cell is configured into home type, such as 47, then serving cell will add this neighbor cell into macro cell by ANR;
4) Neighbor cell PCI is configured into macro type, such as 55 and serving cell is configured into macro type, such as 56, then serving cell will add this neighbor cell into macro cell by ANR;

There will be 2 alternative configuration groups for two carrier enabled case since our device only supports macro mode in the case of two carrier enabled.

1) Neighbor cell PCI is configured into macro type, such as 55,56 and serving cell is macro type, such as 65,66, then serving cell will add this neighbor cell into macro cell by ANR;
2) Neighbor cell (other vendor product) PCI is configured into home type, such as 45 and serving cell is macro type, such as 65,66, then serving cell will add this neighbor cell into home cell by ANR.

EPC Configuration

Connect to MosoLabs' Cloud EPC

This section provides details of the configuration of the MosoLabs' Cloud EPC.

MosoLabs' Cloud EPC function should be used only after the discussion with the MosoLab team.

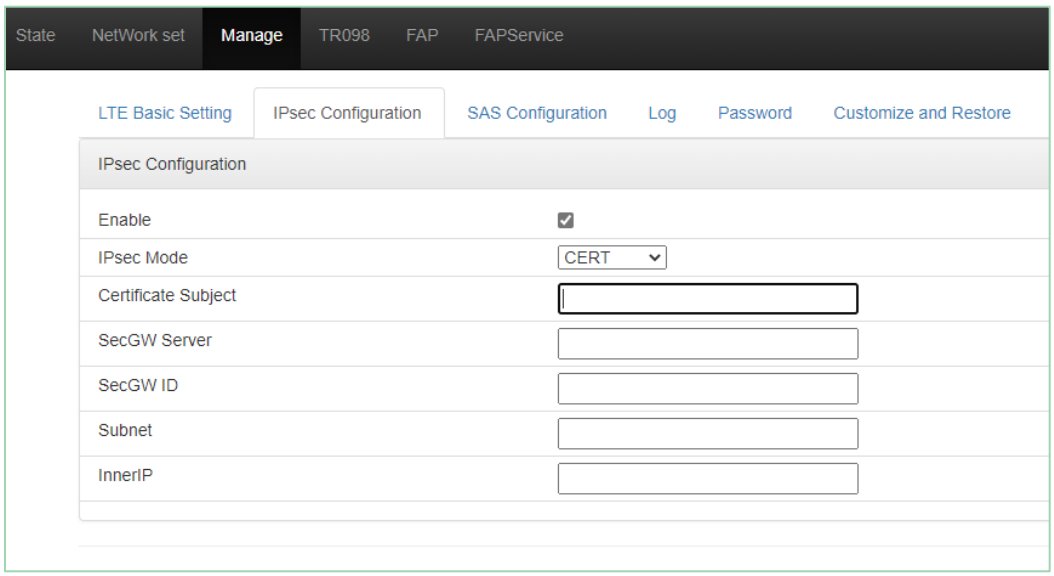
1. Visit "IPSec" page under "Manage" group to set IPSec with certification mode, MosoLabs' Cloud EPC parameters are as below:

IPsec Mode: CERT

SecGW Server: Get From MosoLab

SecGW ID: Get From MosoLab

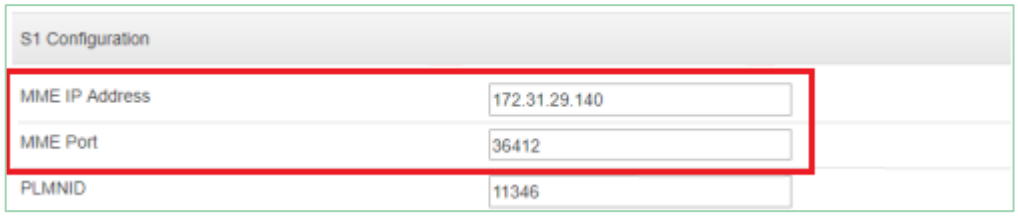
Subnet: Get From MosoLab



2. Visit "LTE Basic Setting" page under "Manage" group to set S1 configuration as below parameters. Refer to section “Bring up S1 with MME” to set correct Cell Configuration. Reboot the Moso Canopy device.

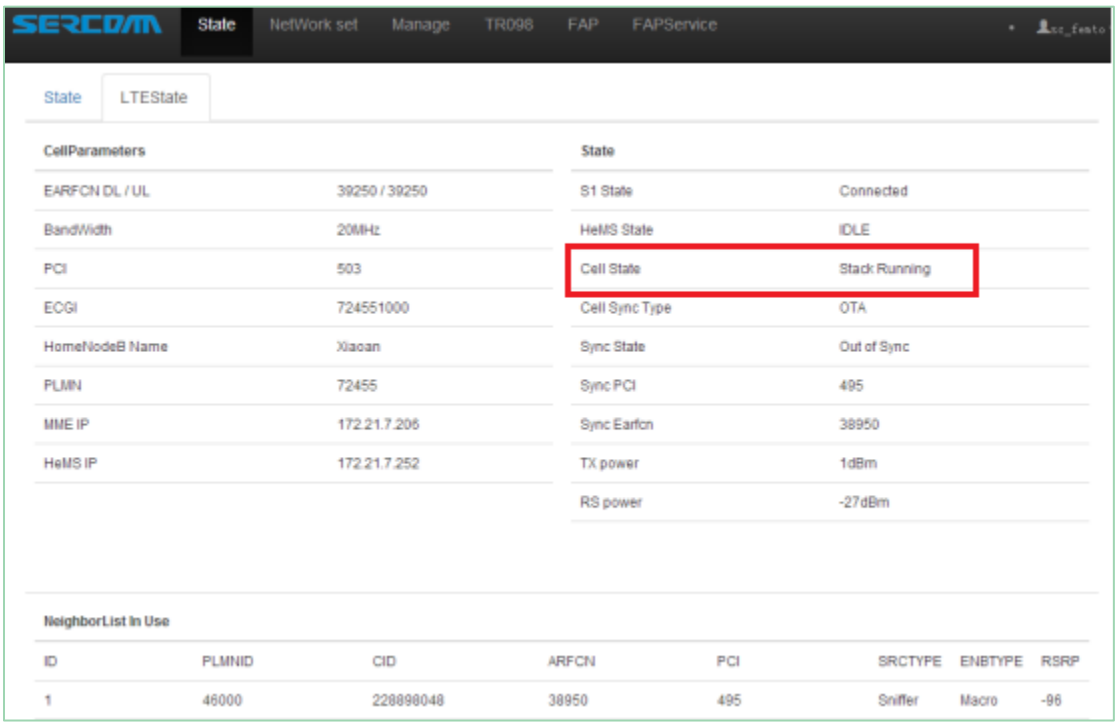
MME IP Address: 172.31.29.140

MME Port: 36412



3. Refer to “IPsec Configuration” section to check IPsec status after rebooting. The status should indicate OK.

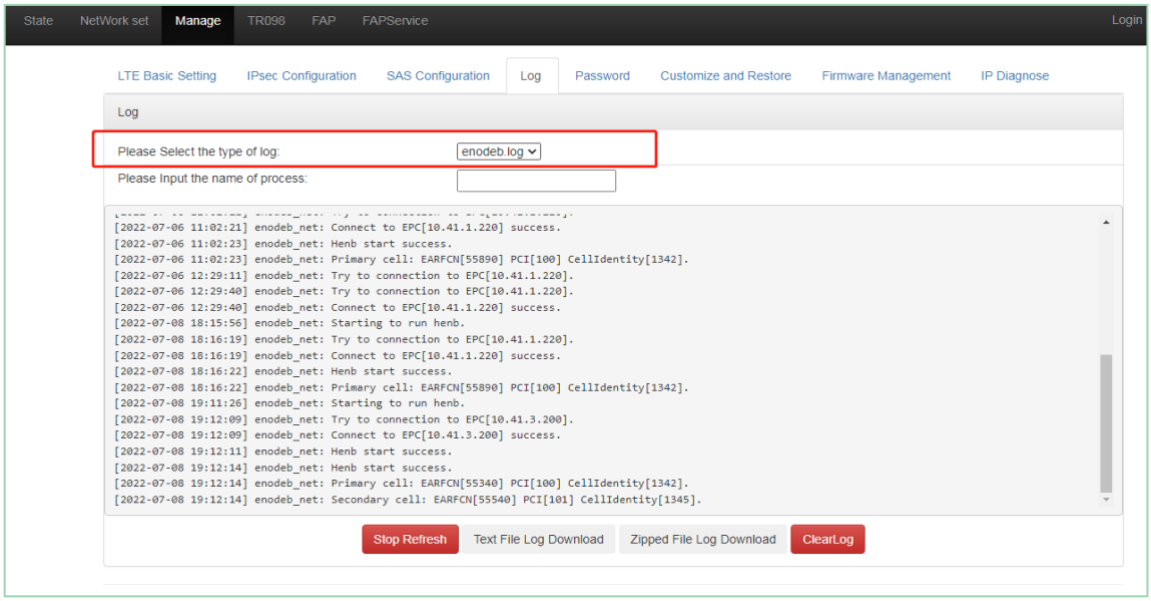
4. Visit "LTEState" page under "State" group to check "Cell State". The status should be "Stack Running"



Log Management

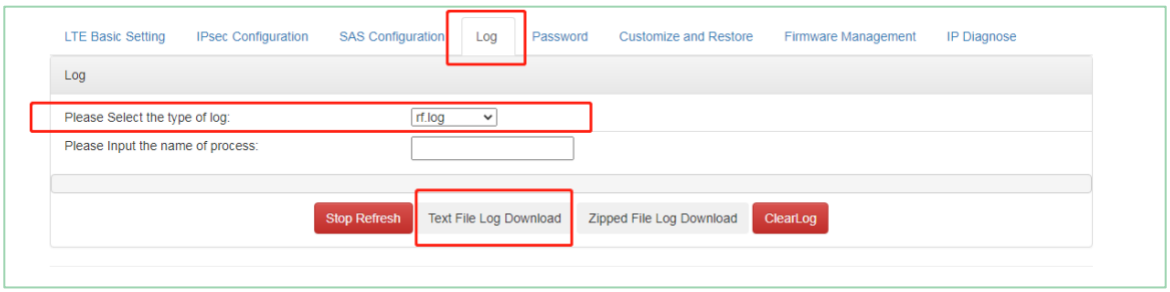
View Log from GUI

Visit "Manage" page under "Log" group to click "LogDownload" button, then you can Select the type of log and view it. Etc. It will show you enodeb log after you select "enodeb.log"



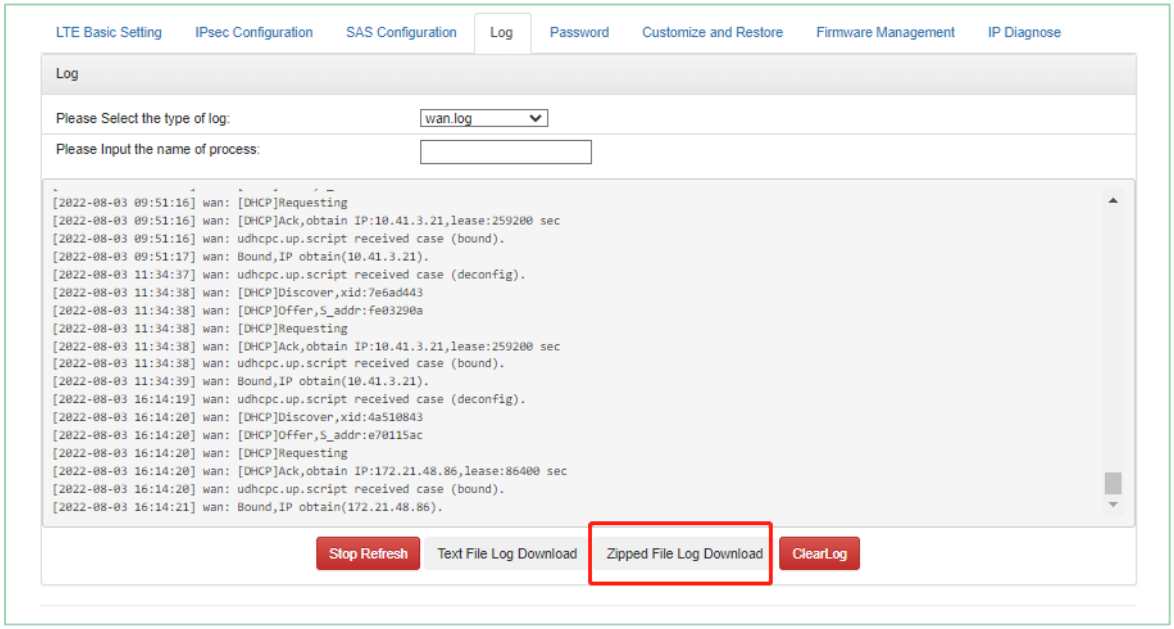
Get txt Log

Visit "Manage" page under "Log" group. Select the type of log and then click "Text File Log Download" button. Then you can get txt log you want.



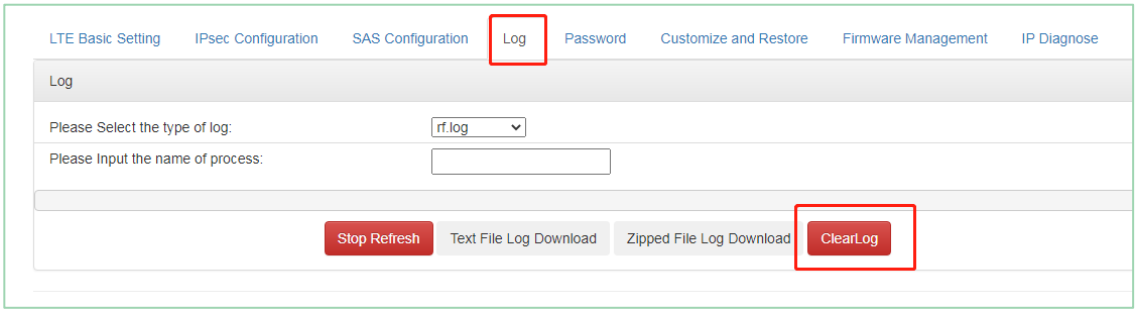
Get log.zip

Visit "Manage" page under "Log" group to click "Zipped File Log Download" button, then you can get log.zip. Normally, you may need to click "ClearLog" button to clear old log before testing.



Clear Log

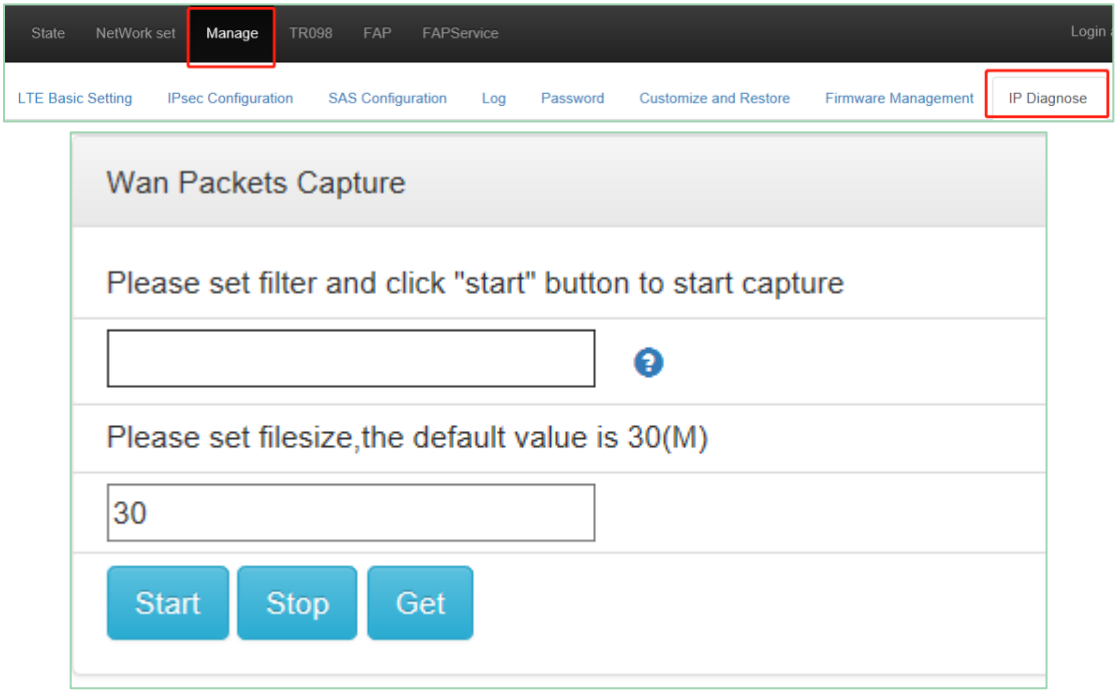
Normally, you may need to click "ClearLog" button to clear old log before testing.



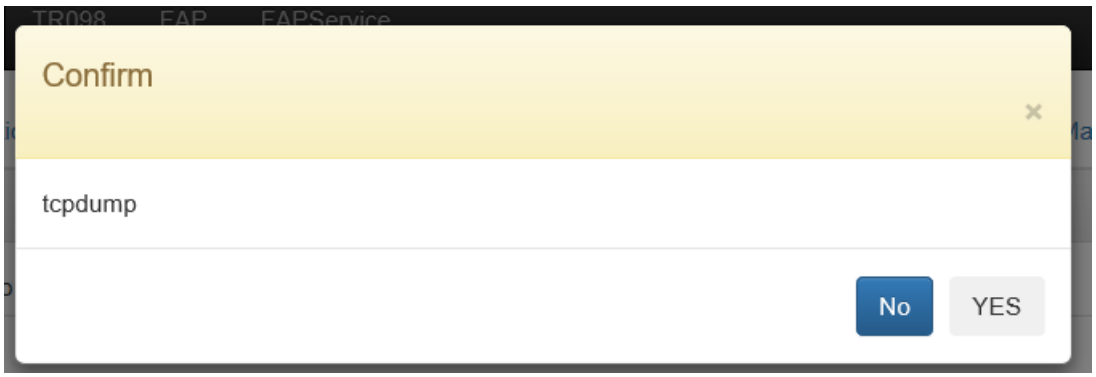
Tcpdump Capture Procedure

Tcpdump Capture Procedure on GUI

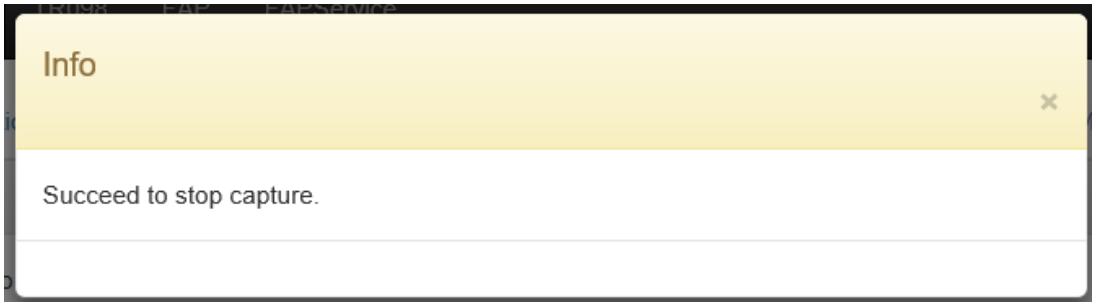
Select the IP Diagnose on the Manage page, input the tcpdump filter condition in the first text box (tcpdump is the default value for capturing all packets if you don't input anything), and the second text box can set the maximum size of the pcap file where the capture results are stored. It will automatically stop capturing packets when that value is reached (30M by default).



Click Start and the following prompt will appear. After confirming the tcpdump command is correct, click Yes button to Start capturing packets. If the command is incorrect, you can click No and re-input the command.



Click Stop to stop the tcpdump capture.



Click the Get Button. It will prompt to download the relevant compressed file, and you can choose your own path to download and unzip it. After that, you can open it with Wireshark to view the captured content.

Abbreviations

Abbreviation	Full Characteristics
1xRTT	CDMA2000 1x Radio Transmission Technology
3GPP	3rd Generation Partnership Project
ABS	Almost Blank Subframe
ADR	Average Data Rate
AIS	Alarm Indication Signal
AM	Acknowledged Mode
AMBR	Aggregate Maximum Bit Rate
ANR	Automatic neighbor Relation
ARP	Allocation and Retention Priority
AS	Access Stratum
AWGN	Additive White Gaussian Noise
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
BFD	Bidirectional Forwarding Detection
BLER	Block Error Rate
BSR	Buffer Status Report
CA	Carrier Aggregation
CC	Chase-Combing
CCCH	Common Control Channel
CCE	Channel Control Element
CCO	Cell Change Order

Abbreviation	Full Characteristics
CCO	Coverage and Capacity Optimization
CDT/MR	Call Detail Trace / Measurement Report
CESoPSN	Circuit Emulation Service over Packet Switched Network
CGI	Cell Global Identifier
CLSM	Close-Loop Spatial Multiplexing
CMC	Connection Mobility Control
COC	Cell Outage Compensation
CoMP	Coordinated Multipoint Tx/Rx
COS	Class of Service
CQI	Channel Quality Indicator
CS	Certification Server
CSFB	CS Fallback
CTS	Call Trace System
C-RNTI	Cell Radio Networks Temporary Identifier
DCCH	Dedicated Control Channel
DCI	Downlink Control Information
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DL	Downlink
DL-SCH	DL Dedicated Channel
DRX	Discontinuous Reception
DSCP	Differentiated Services Code Point
DTCH	Dedicated Traffic Channel
DTX	Discontinuous Transmission
EMBMS	Evolved Multimedia Broadcast and Multicast Service
SmallCell	E-UTRAN NodeB
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
ECN	Explicit Congestion Notification
EPC	Evolved Packet Core

Abbreviation	Full Characteristics
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
E-UTRAN	Evolved UTRAN
ETWS	Earthquake and Tsunami Warning System
EVC	Ethernet Virtual Connection
FDD	Frequency Division Duplex
FE	Fast Ethernet
FFR	Fractional Frequency Reuse
FTP	File Transfer Protocol
GCI	Global Cell ID
GE	Gigabit Ethernet
GERAN	GSM EDGE Radio Access Network
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile communication
GBR	Guaranteed Bit Rate
GPS	Global Positioning System
GTP	GPRS Tunneling Protocol
GUMMEI	Globally Unique MME Identifier
HARQ	Hybrid Automatic Repeat Request
HeNB	Home E-UTRAN NodeB
Het-Net	Heterogeneous Network
HII	High Interference Indicator
HSDPA	High Speed Downlink Packet Access
HRPD	CDMA2000 High Rate Packet Data
HTTP	HyperText Transfer Protocol
ICIC	Inter-Cell Interference Coordination
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMS	Inventory Management Server
IP	Internet Protocol
IPsec	Internet Protocol Security

Abbreviation	Full Characteristics
IP-CAN	IP Connectivity Access Network
IP-SM-GW	IP-Short-Message-Gateway
IR	Incremental-Redundancy
ITU	International Telecommunication Union
LAA	Licensed Assisted Access
LB	Load Balancing
LDAP	Lightweight Directory Access Protocol
LMT	Local Maintenance Terminal
LTE	Long Term Evolution
MAC	Medium Access Control
MBMS	Multimedia Broadcast Multicast Service
MBR	Maximum Bit Rate
MCCH	MBMS point-to-multipoint Control Channel
MCH	Multicast Channel
MIB	Master Information Block
MIMO	Multiple Input Multiple Output
MLB	Mobility Load Balancing
MME	Mobility Management Entity
MPLS	Multi-Protocol Label Switching
MTCH	MBMS point-to-multipoint Traffic Channel
NACC	Network Assisted Cell Change
NAS	Non-Access Stratum
NCL	Neighbor Cell List
NE	Net Element
NRT	Neighbor Relation Table
O&M	Operation & Maintenance
OAM	Operation Administration Maintenance
OFDM	Orthogonal Frequency Division Multiplexing
OI	Overload Indicator
OLSM	Open-Loop Spatial Multiplexing
OMC	Operation and Maintenance Center

Abbreviation	Full Characteristics
PBCH	Physical broadcast channel
PBR	Prioritised Bit Rate
PCCH	Paging Control Channel
PCH	Paging Channel
PCFICH	Physical control format indicator channel
PCI	Physical Cell Identity
PDB	Packet Delay Budget
PDCCH	Physical downlink control channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical downlink shared channel
PE	Provider Edge
PER	Packet Error Rate
PHB	Per-Hop Behavior
PKI	Public Key Infrastructure
PHICH	Physical Hybrid ARQ Indicator Channel
PLMN	Public Land Mobile Network
PMCH	Physical multicast channel
PQ	Priority Queueing
PRACH	Physical random access channel
PRB	Physical Resource Block
PTP	Precision Time Protocol
PUCCH	Physical uplink control channel
PUSCH	Physical uplink shared channel
PWE	Pseudo Wire Emulate
QCI	QoS Class Identifier
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
RADIUS	Remote Authentication Dial In User Service
RAT	Radio Access Technology
RBC	Radio Bearer Control

Abbreviation	Full Characteristics
RDI	Remote Defect Indication
RF	Radio Frequency
RLC	Radio Link Control
RNTP	Relative Narrowband Transmit Power
RO	RACH Optimization
ROHC	Robust Header Compression
RS	Reference Signal
RSRP	Reference Signal Received Power
RRC	Radio Resource Control
RRM	Radio Resource Management
RTP	Real-time Transport Protocol
RV	Redundancy Version
SAE	System Architecture Evolution
SAP	Service Access Point
SDH	Synchronous Digital Hierarchy
SDR	Software Defined Radio
SFR	Soft Frequency Reuse
SHA	Secure Hash Algorithm
S-GW	Serving Gateway
SINR	Signal Interference Noise Ratio
SIB	System Information Block
SM	Short Message
SON	Self Organizing Network
SONET	Synchronous Optical Network
SPS	Semi-Persistent Scheduling
SRVCC	Single Radio Voice Call Continuity
SSR	Setup Success Rate
SU-MIMO	Single-User Multi Input and Multi Output
SW	Software
TA	Tracking Area
TAU	Tracking Area Update

Abbreviation	Full Characteristics
TBS	Transport Block Size
TCP	Transport Control Protocol
TTI	Transmission Time Interval
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
UL-SCH	UL Dedicated Channel
UTRAN	Universal Terrestrial Radio Access Network
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
VoIP	Voice over IP