

T&W

catalog

| | |
|---|----|
| 3、 Quick start | 4 |
| 3.2Log in to the web client | 4 |
| 3.2.1Set up client computers..... | 4 |
| 3.2.2Log in to the web maintenance page..... | 5 |
| 3.3Quick initial configuration | 5 |
| 4、 Common configuration | 8 |
| 4.1Configure network interface | 8 |
| 4.1.1Configure WAN interface..... | 8 |
| 4.1.2Configure VLAN..... | 10 |
| 4.1.3Configure LAN interface..... | 10 |
| 4.1.4Configure IPv4 routing..... | 10 |
| 4.2Configure IPSec | 12 |
| 4.2.1Set PSK..... | 12 |
| 4.2.2Configure virtual SIM card..... | 14 |
| 4.2.3Configure certificate..... | 15 |
| 4.2.4Configure profile..... | 17 |
| 4.2.5Enable IPSec..... | 23 |
| 4.2.6View IPSec status..... | 24 |
| 4.3Configure base station parameters | 25 |
| 4.3.1Set encryption and integrity protection algorithm..... | 25 |
| 4.3.2Configure network management connection..... | 26 |
| 4.3.3Configure base station synchronization parameters..... | 27 |
| 4.3.4Configure NTP service..... | 35 |
| 4.4Configure LTE parameters | 36 |
| 4.4.1Configure neighborhood parameters..... | 36 |
| 4.4.2Configure mobility parameters..... | 45 |
| 4.2.3 SONRelated configuration | 51 |
| 4.5Configure system parameters | 54 |
| 4.5.1Software version upgrade..... | 54 |
| 4.5.2System file backup | 55 |
| 4.6Restart base station | 56 |

3、 Quick start

3.2 Log in to the web client

Requirements for client computer browser are as followsTable 3-1.

| project | requirements |
|----------------------|--|
| The CPU | Intel Core above 2GHz |
| memory | More than 2 g RAM |
| The hard disk | Not less than 100 MB of available space |
| The operating system | <ul style="list-style-type: none">• Microsoft: Windows XP, Windows Vista, or Windows7• Mac: MacOS x 10.5 or above |
| Display resolution | Above 1024*768 pixels |
| The browser | Chrome 6 or later |

surface3-1Client environment requirements

3.2.1 Set up client computers

Before logging into the Web client, firstly set the IP address of the client computer and ensure that the client computer is connected to the base station. Take Windows 7 as an example.

1. Click start > control panel, and in the pop-up window click network and Internet.
2. Click view network status and tasks, and in the window that pops up, click local connections.
3. In the pop-up local connection status dialog box, click properties to pop up local connection properties.
4. Select Internet protocol version (TCP/IPv4), click properties, and the pop-up window looks like figure 3-2.

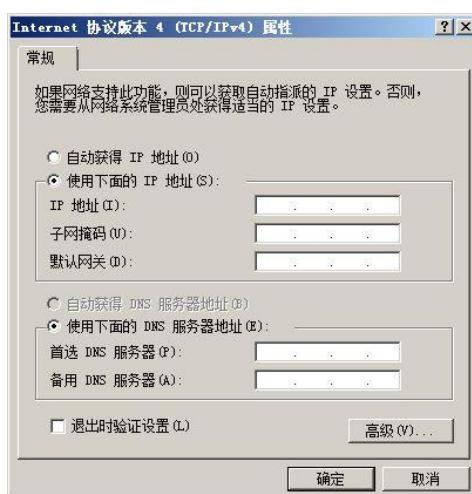


Figure 3-2 setting the client IP address

5. Select the IP address below.
6. Enter the IP address, subnet mask, and default gateway, and click ok.
 - IP address: 192.168. 0. XXX: (the recommended value of XXX is 102~199)
 - Subnet mask: 255.255.255.0
 - Default gateway: not required
7. Perform ping 192.168.0.101 in the command line window to check whether the network is connected between the client computer and the device.

3.2.2Log in to the web maintenance page

1. 1. Enter https://192.168.0.101 in the browser address bar and click "sing in" to open the Web client login page, as shown in figure 14.

User name: admin

Password: Pico @ 2018

192.168.0.101 is the initial IP address of the interface.



chart3-3Log in to the base station web page

3.3Quick initial configuration

Rapid configuration is to configure the cell parameters of the base station, including the working mode of the base station, cell identification, working frequency band, frequency point, etc., which needs to be set according to network planning data.

Select "management-> Cell" in the navigation bar to set basic parameters of the base station, as shown in figure 3-4.

Information Management

Cell

| | | | |
|------------------|--|--------------|---|
| AdminState: | <input checked="" type="checkbox"/> Enable | EnbType: | <input type="radio"/> MACRO ENB <input checked="" type="radio"/> HOME ENB |
| Duplex Mode: | <input checked="" type="radio"/> FDD <input type="radio"/> TDD | TAC: | 27007 |
| SecGWServer: | 61.132.154.86 | Standalone: | <input type="checkbox"/> Enable |
| S1SigLinkServer: | 7.191.1.192 | S1Status: | Success |
| S1RetryMaxNum: | 10 | AssocStatus: | Active |

PLMNID **Cell1**

| | |
|--------------------|---|
| Primary PLMNID No: | 1 |
| PLMNID1: | <input checked="" type="checkbox"/> Enable 46011 |
| PLMNID2: | <input type="checkbox"/> Enable |
| PLMNID3: | <input type="checkbox"/> Enable |
| PLMNID4: | <input type="checkbox"/> Enable |
| PLMNID5: | <input type="checkbox"/> Enable |
| PLMNID6: | <input type="checkbox"/> Enable |

Submit

Information Management

Cell

| | | | |
|------------------|--|--------------|---|
| AdminState: | <input checked="" type="checkbox"/> Enable | EnbType: | <input type="radio"/> MACRO ENB <input checked="" type="radio"/> HOME ENB |
| Duplex Mode: | <input checked="" type="radio"/> FDD <input type="radio"/> TDD | TAC: | 27007 |
| SecGWServer: | 61.132.154.86 | Standalone: | <input type="checkbox"/> Enable |
| S1SigLinkServer: | 7.191.1.192 | S1Status: | Success |
| S1RetryMaxNum: | 0 | AssocStatus: | Active |

PLMNID **Cell1**

| | | | |
|-----------------------|--|--------------------------|--|
| CellIdentity: | 42121095 | OpState: | true |
| UeNumber: | 2 | VolteUeNumber: | 0 |
| CandidateARFCNList: | 1850 | CandidatePCIList: | 0..503 |
| EARFCNDL: | 1850 | EARFCNUL: | 19850 |
| FreqBandIndicator: | 3 | PhyCellID: | 95 |
| DL Bandwidth: | 100 | UL Bandwidth: | 100 |
| ReferenceSignalPower: | -8 | PAGain: | 0 |
| SubFrameAssignment: | 2 | SpecialSubframePatterns: | 7 |
| AntennaPortsCount: | <input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 4 | RxAntennaPortsCount: | <input type="radio"/> 1 <input checked="" type="radio"/> 2 <input type="radio"/> 4 |

Submit

chart3-4Set basic parameters of base station quickly

The basic parameters are described in table 3-2.

| The parameter name | instructions |
|-----------------------------|--|
| AdminState | Cell state control switch.(check enable when all basic parameters are configured) <ul style="list-style-type: none"> • Check Enable: protocol stack to set up cell, base station RF work; • Uncheck Enable: protocol stack delete cell, base station RF shutdown; |
| EnbType | ENB type, MARCO and HOME |
| Duplex Mode | Duplex mode, default is FDD |
| TAC | Set the tracking area code where the base station is located to define the sending range of paging messages.TAC is Assigned by the operator. Value range: 0~65535 |
| PLMN ID | PLMN ID of cell ownership |
| S1SigLinkServer | The IP address of MME. It should be consistent with the IP address of MME on the core network side. <ul style="list-style-type: none"> • Support to configure up to 32 MME addresses; • Multiple MME addresses are separated by English commas |
| CellIdentity | The Cell ID. <ul style="list-style-type: none"> • When the eNB type is MARCO, it is the same as the eNB ID (20bits); • When the eNB type is HOME, it is the value of eNB ID moved 8bits to the left and Cell ID and operation, that is, eNB ID*256+Cell ID (28bits); |
| OpState | Cell working status. <ul style="list-style-type: none"> • When the cell is successfully established and the RF works, the state is "true"; • The Opstate is False when Adminstate is not enabled or the cell is not successfully established. |
| CandidateARFCNList | Absolute frequency point list.(multiple frequency points are separated by English commas) <ul style="list-style-type: none"> • If only one frequency point is configured, the base station use this frequency point to establish the cell; • If multiple frequency points are configured, the base station selects frequency points according to SON's self-configuration function and establishes the cell. |
| CandidatePCIList | PCI list.(multiple PCI is separated by English commas) <ul style="list-style-type: none"> • If only one PCI is configured, the base station will use this PCI to establish cell. • If multiple PCI is configured, the base station selects PCI according to SON's PCI self-configuration function and establishes the cell |
| EARFCNDLInUse | The actual uplink and downlink absolute frequency points used by the base station |
| FreqBandIndicator | The frequency band in which the base station operates |
| PhyCellIDInuse | The PCI that Base station actually uses |
| DL Bandwidth / UL Bandwidth | The number of PRBS of the bandwidth (the uplink and downlink bandwidth should be the same) <ul style="list-style-type: none"> • The 5MHz bandwidth is 25 • The 10MHz bandwidth is 50 • The 15MHz bandwidth is 75 • The 20MHz bandwidth is 100 |
| ReferenceSignal Power | Reference signal power.(maximum value is -10) <ul style="list-style-type: none"> • For a single rf port, the actual output power is ReferenceSignalPower+31 with dBm unit, such as -10+31=21dBm |
| PAGain | PA gain value, the integrated base station is set to "0" |
| AntennaPortsCount | Number of base station antennas, usually configured as "2" (MIMO) |
| RxAntennaPortsCount | The number of antennas a base station USES for receiving, usually configured as "2" (MIMO) |

Table 3-2 quick setting parameter description

1. After setting basic base station parameters in table 1-2, click "Submit" to Submit.



Note: some parameter changes (such as bandwidth, etc.) will cause the base station to restart, just wait for the restart to complete.

2. After basic parameter configuration is submitted, check "Enable" of "AdminState"

4、 Common configuration

4.1 Configure network interface

The network interface configuration interface of base station equipment is shown in the figure below.

Select "management network IP" in the navigation bar to enter the network interface configuration page.

| Address Type | IPv4 | | IPv6 | | Other | | |
|--------------|---------------|---------------|----------|--------------|----------|-------------------|------|
| | IP | Mask | IP | Mask | Ethernet | Mac address | MTU |
| DHCP | 10.98.100.218 | 255.255.255.0 | Disabled | /64 | eth0 | D8:37:BE:20:00:10 | 1500 |
| Static | 192.168.8.248 | 255.255.255.0 | Disabled | 4001::119/64 | eth1 | D8:37:BE:00:00:01 | 1500 |

Figure 4-1 network interface configuration

4.1.1 Configure WAN interface

WAN interface is the external communication interface of the base station. It is mainly used to connect the base station with external devices, such as OMC, Mme, gateway and other devices. It supports the configuration of multiple VLANs to connect with different devices.

Select "management-> Network"->IP in the navigation bar and WAN interface configuration is shown in Figure 4-2.

chart4-2Configure WAN interface address

The WAN port parameters are described in table 4-1, Table 4-2 and table 4-3.

| Parameter name | explain |
|------------------|---|
| The Address Type | The mode for WAN interface to obtain IPv4 address. Support: <ul style="list-style-type: none">DHCP: dynamically obtaining IP address, no other parameters need to be configured;Static: IP address and mask need to be configured;Disabled: closes the function of WAN port IPv4 protocol. It is not recommended to select. |
| IPv4 address | The IPv4 address of the WAN interface. <ul style="list-style-type: none">In DHCP mode, it is allocated by DHCP server.Static mode requires manual configuration; |
| Mask | IPv4 subnet mask for the WAN interface. <ul style="list-style-type: none">In DHCP mode, it is allocated by DHCP server.Static mode requires manual configuration; |

surface4-1 IPv4 parameter description of WAN interface

| Parameter name | explain |
|----------------|--|
| Origin | WAN interface to get IPv6 address. Support: <ul style="list-style-type: none">DCHPv6: dynamically obtain IP address, no need to configure other parameters;Static mode: IPv6 address and mask need to be configured;Disabled: turns off IPv6 protocol function of WAN port (turns off IPv6 protocol by default); |
| IPv6 address | IPv6 address and mask of WAN interface. <ul style="list-style-type: none">In DCHPv6 mode, it is assigned by DCHPv6 server.Static mode requires manual configuration; |

Table 4-2 IPv6 parameter description of WAN interface

| Parameter name | explain |
|----------------|------------------------------|
| Mac address | MAC address of WAN interface |
| MTU | MTU size of WAN interface |

Table 4-3 description of other common parameters of WAN interface

4.1.2 Configure VLAN

Refer to Figure 4-2 for VLAN configuration interface and table 4-4 for parameter description.

| Parameter name | explain |
|----------------|----------------------|
| Enable | VLAN function switch |
| VLAN ID | VLAN ID |

surface4-4 VLAN parameter description

4.1.3 Configure LAN interface

LAN interface is the local maintenance interface of the base station, which is mainly used for the local maintenance and configuration of the base station.

The default IP address for the LAN interface is 192.168.8.248, which is usually left as the default configuration.

4.1.4 Configure IPv4 routing

Select “management-> Network->Route” in the navigation bar to enter the route configuration view.

- Click “add” to add a routing instance, as shown in Figure 4-3.

| IPv4Forwarding | | | | | | | IPv6Forwarding | | | | |
|----------------|---------|------------|-----------------|------------------|--------------------|----------|----------------|----------|------------------|----------|----------|
| Enable | Status | Route Type | Dest IP Address | Dest Subnet Mask | Gateway IP Address | Ethernet | Enable | Status | Dest IPv6 Prefix | Next Hop | Ethernet |
| Enabled | Enabled | Default | 0.0.0.0 | 0.0.0.0 | 10.98.100.253 | eth0 | Disabled | Disabled | | | |

chart4-3Add route

- Configure routing entries

1) Add a default route, as shown in Figure 4-4.

The screenshot shows a web-based management interface for network configuration. On the left, a sidebar lists various management categories like Information, Management, Cell, Debug, Factory, and HeMS, with 'Network' selected. The main panel is titled 'Management -- Network' and contains instructions: 'You can add/delete/change the dns manually.' and 'All the network configures will be effective after rebooting.' Below this is a section titled 'Router information:' with two tables: 'IPv4Forwarding' and 'IPv6Forwarding'. The 'IPv4Forwarding' table has rows for Router ID (NEW), Enable (checked), StaticRoute (unchecked), DestIPAddress (0.0.0.0), DestSubnetMask (0.0.0.0), GatewayIPAddress (192.168.3.1), Ethernet (eth0), and Origin (Static). The 'IPv6Forwarding' table has rows for Enable (unchecked), DestIPPrefix (4001::118/64), NextHop (4001::118), Ethernet (none), and Origin (Static). At the bottom are 'Submit' and 'Back' buttons.

Figure 4-4 add default route

2) Add network segment route, as shown in Figure 4-5.

This screenshot is identical to Figure 4-4, showing the 'Management -- Network' configuration page. The sidebar shows 'Network' is selected. The main panel has the same instructions and 'Router information:' section with 'IPv4Forwarding' and 'IPv6Forwarding' tables. In the 'IPv4Forwarding' table, the 'Enable' checkbox is checked, while in the 'IPv6Forwarding' table, the 'Enable' checkbox is unchecked. The other fields in both tables are identical to Figure 4-4.

Figure 4-5 add segment route

Description of main route configuration parameters, as shown in table 4-5.

| Parameter classification | Parameter name | explain |
|--------------------------|------------------|---|
| IPv4 routing parameters | The Enable | Route item switches. Check to enable, check to not enable. |
| | The StaticRoute | Check this if the configured route is network segment route; If the configured route is the default route, this item is not checked; |
| | DestIPAddress | Destination IP address. |
| | DestSubnetMask | The subnet mask for the destination IP address. |
| | GatewayIPAddress | Gateway IP address to destination IP address. |
| | Ethernet | Select "eth0" |
| IPv6 Routing parameters | Enable | Route entry switch. Tick to enable and uncheck to disable. |
| | DestIPPrefix | Destination IPv6 network segment. |
| | NextHop | Next hop address. |
| | Ethernet | Configure the network interface where the route is located, WAN port is eth0 |

surface4-5Description of main route configuration parameters

4.2 Configure IPSec

Enb-f02004 supports EAP-AKA, certificate and PSK authentication modes. The configuration methods of the three modes are described below.

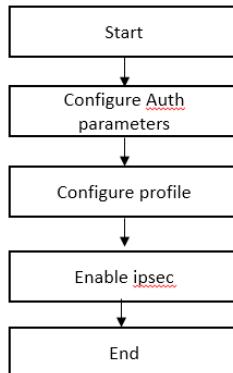


Figure 4-6 IPSec configuration flow

4.2.1 Set PSK

Web page path: "management -> security -> PSK"

1. Click "add" to add PSK, or select and click "Edit" to edit PSK.

The screenshot shows a web-based management interface titled "Management -- PSK". On the left, there is a vertical navigation menu with various options like Information, Management, Cell, Debug, Factory, HeMS, Network, Performance, Security, IPsec, Certificate, PSK (which is selected and highlighted in blue), vSIM, File transmission, Synchronization, Upgrade, Access Control, and Data Model. The main content area is titled "Management -- PSK" and contains a table with the following data:

| | ID | Enable | Encoding | PreSharedKey | In use |
|-----------------------|----|--------|----------|--------------|--------|
| <input type="radio"/> | 1 | Y | ASCII | ***** | IP sec |

Below the table are three buttons: "Edit", "Add", and "Delete".

Figure 4-7 adding or modifying PSK

2. Select the encoding method of PSK, enter the key value, such as 123456, and then click "submit" to submit.

The screenshot shows a "Management -- PSK detail" configuration page. The left sidebar has the same navigation menu as Figure 4-7. The main area has a title "Management -- PSK detail" and contains the following form fields:

| | |
|-----------------|--|
| ID: | 1 |
| Enable/Disable: | <input checked="" type="checkbox"/> Enable |
| Encoding: | ASCII ▾ |
| PreSharedKey: | ***** |

At the bottom are two buttons: "Submit" and "Back".

Figure 4-8 configure PSK

3. After submitting the configuration, you can view the PSK information through the web, as shown in Figure 4-9.

The screenshot shows a web-based management interface for a device. On the left, there is a vertical navigation menu with various options like Information, Management, Cell, Debug, Factory, HeMS, Network, Performance, Security, IPsec, Certificate, PSK (which is selected and highlighted in blue), eSIM, and File transmission. The main content area is titled "Management -- PSK". It contains a table with the following data:

| | ID | Enable | Encoding | PreSharedKey | In use |
|----------------------------------|----|--------|----------|--------------|--------|
| | | | | | IP sec |
| <input checked="" type="radio"/> | 1 | Y | ASCII | ***** | Y |

Below the table are three buttons: Edit, Add, and Delete.

Figure 4-9 view PSK information on the web

4.2.2 Configure virtual SIM card

Web page path: management->Security->Vsims

1. Click Add to add the virtual SIM configuration, or select and click Edit to edit the vSIM configuration.

The screenshot shows a web-based management interface for a device. On the left, there is a vertical navigation menu with various options like Information, Management, Cell, Debug, Factory, HeMS, Network, Performance, Security, IPsec, Certificate, PSK, vSIM (which is selected and highlighted in blue), File transmission, Synchronization, Upgrade, Access Control, and Data Model. The main content area is titled "Management -- vSIM". It contains a table with the following data:

| | ID | Enable | Encoding | Key | Opc | In use |
|----------------------------------|----|--------|----------|-----|-----|--------|
| | | | | | | IP sec |
| <input checked="" type="radio"/> | 1 | Y | Hex | | | |

Below the table are three buttons: Edit, Add, and Delete.

Figure 4-10 adding or modifying virtual USIM

2. Enable virtual SIM configuration, select encoding mode, input key and OPC value, and then click "submit" to submit.

The screenshot shows a web-based management interface for a virtual SIM (vSIM) in a system named T&W. The left sidebar contains a tree-like navigation menu with categories like Information, Management, Cell, Debug, Factory, HeMS, Network, Performance, Security, IPsec, Certificate, PSK, and vSIM. The vSIM node is expanded, showing sub-options: File transmission, Synchronization, Upgrade, Access Control, and Data Model. The main content area is titled "Management -- vSIM detail". It displays several configuration parameters in a table format:

| | |
|-----------------|--|
| ID: | 1 |
| Enable/Disable: | <input checked="" type="checkbox"/> Enable |
| Encoding: | Hex |
| Key: | 01020304050607080102030405060708 |
| OPc: | 01020304050607080102030405060708 |

At the bottom of the main panel are two buttons: "Submit" and "Back".

Figure 4-11 configuring virtual SIM parameters

4.2.3 Configure certificate

There are two ways to import certificates: through the web interface and through the network management.

1. Import the certificate through the web, as shown in Figure 3-11.

- Select CA Cert, click browse, and select the corresponding certificate file (usually in PEM format)



be careful:

It is not supported to put multiple CA certificates into one certificate file; If there are multiple CA certificates, you need to import them multiple times.

- Select "client cert", click "Browse", and select the corresponding certificate file (usually in p12 format); If the pkcs12 file has a decompression password, you need to enter the corresponding password.

Figure 4-12 web import certificate

2. Import the certificate through the network management.

The NMS can download the certificate through the download method. The download file types are "x d837be clcert" (client certificate p12 / PFX) and "x d837be cacert" (CA certificate). D837be is the manufacturer oui. Pay attention to replacement when different manufacturers have different versions.

3. After the certificate is imported, you can view the relevant information of the certificate through the web page.

Management -- Certificate Maintenance

Allows only the updating or deletion of expired certificates.

Updates or uploads a certificate that has the same issuer and serial number.

The system automatically reboots after a certificate is changed or updated.

Certificate List:

| ID | Enable | Type | Issuer | Detail | In use |
|----|-----------------------|------|---|---|--------|
| 1 | <input type="radio"/> | Y | Client C=CN,CN=CMCA Internal Server CA_2048 | SerialNumber : 012325BC Subject : C=CN,O=CMCC,CN=F068650AD676@AP.datangmobile.cn SubjectAlt : critical Valid period: 2020-12-28 8:14:32 - 2030-12-28 8:14:32 Last Modify : 2021-5-8 1:18:15 | |

Enable **Delete**

Figure 4-13 viewing certificate information on the web

4.2.4 Configure profile

4.2.4.1 Add or modify profile

Web page path: management -> security -> IPSec -> profile

Click Add to add or edit to modify the profile configuration.

4.2.4.2 Setting profile parameters

For PSK, certificate and USIM, except for different authentication mode parameters, other parameters can be configured in public. Please refer to the following details.

T&W

Information
 Management
 Cell
 Debug
 Factory
 HeMS
 Network
 Performance
 Security
IPsec
 Certificate
 PSK
 vSIM
 File transmission
 Synchronization
 Upgrade
 Access Control
 Data Model

Management -- IPsec Profile

| | | |
|--------------------------------|--|----------------|
| Enable: | <input checked="" type="checkbox"/> Enable | |
| RemoteEndpoints: | 61.132.154.86 | |
| LocalId: | 2295033000E | |
| RemoteId: | psk@comba.c | |
| EAPIdentity: | | |
| SubnetIPType: | same to SecGW ▼ | |
| LocalSubnet: | 0.0.0.0/0 | |
| RemoteSubnet: | 0.0.0.0/0 | |
| IKEv2: | EncryptionAlgorithms: | AES-CBC ▼ |
| | IntegrityAlgorithms: | HMAC-SHA1-96 ▼ |
| | DiffieHellmanGroupTransforms: | MODP-1024 ▼ |
| ESP: | EncryptionAlgorithms: | AES-CBC ▼ |
| | IntegrityAlgorithms: | HMAC-SHA1-96 ▼ |
| | DiffieHellmanGroupTransforms: | MODP-1024 ▼ |
| Rekey: | <input checked="" type="checkbox"/> Enable | |
| Reauth: | <input type="checkbox"/> Enable | |
| IKEv2SATimeLimit: | 7200 | |
| ChildSATimeLimit: | 3600 | |
| MarginTime: | 300 | |
| IKEv2DeadPeerDetectionTimeout: | 30 | |
| IKEv2DeadPeerDetectionAction: | None ▼ | |

IKEv2AuthMethod : PSK ▼

| ID | Enable | Encoding | PreSharedKey | In use |
|----|-------------------------------------|----------|--------------|----------------------------------|
| 1 | <input checked="" type="checkbox"/> | 0 | ***** | <input checked="" type="radio"/> |

Figure 4-14 web configuration profile

(1) Profile common parameter description

The profile common parameters are described as follows:

```

Device. IPsec. Profile. {i}. X_D837BE_Mode = tunnel (default)

Device. IPsec. Profile. {i}. X_D837BE_Interface = Device. IP. Interface. 1. (used to specify the enabling IPSec network port.

The default is WAN portIP. Interface.1. )

Device. IPsec. Profile{1}. Remoteendpoints = 10.98.100.192 (fill in the security gateway address)

Device. IPsec. Profile. {i}. X_D837BE_LocalId = *@lte. strongswan. org (base station ID (left ID))

Device. IPsec. Profile. {i}. X_D837BE_Remoteld = secgw. femto. cn (security gateway ID (right ID))

Device. IPsec. Profile. {i}. X_D837BE_Eapidentity = 0 + IMSI (15 IMSI of ESIM, specific filling requirements need to be confirmed with security gateway maintenance personnel)

Device. IPsec. Profile. {i}. X_D837BE_Subnetiptype = 0 (0: virtual address IP type is consistent with real address, 4: apply for IPv4 virtual address, 6: apply for IPv6 virtual address)
  
```

```
Device. IPsec. Profile. {i}. X_D837BE_Localsubnet = 0.0.0.0/0 (specify local TS policy, but general security gateway will ignore it)

Device. IPsec. Profile. {i}. X_D837BE_Remotesubnet = 0.0.0.0/0 (specify remote TS policy, fill in according to network planning)

Device. IPsec. Profile{I}. Ikev2allowedcryptionalgorithms = aes-cbc (encryption algorithm of Ike, multiple choices)

Device. IPsec. Profile{I}. Espallowedcryptionalgorithms = aes-cbc

Device. IPsec. Profile{I}. Ikev2allowedpseudorandomfunctions = hmac-sha1 (random number algorithm of Ike, multiple choice)

Device. IPsec. Profile{I}. Ikev2allowedintegrity algorithms = hmac-sha1-96

Device. IPsec. Profile{I}. Espallowedintegrity algorithms = hmac-sha1-96

Device. IPsec. Profile{I}. Ikev2alloweddiffiehellmangrouptransforms = modp-1024

Device. IPsec. Profile. {i}. X_D837BE_Espalloweddiffiehellmangrouptransforms = none

Device. IPsec. Profile{I}. Ikev2deadpeerdetectiontimeout = 30

Device. IPsec. Profile. {I}. Antireplaywindowsize = 32 (anti replay parameter, max. 64)

Device. IPsec. Profile. {i}. X_D837BE_Strictcrlpolicy = no (do not perform CRL check)

Device. IPsec. Profile. {i}. X_D837BE_Rekey = 1 (rekey function switch)

Device. IPsec. Profile. {i}. X_D837BE_Reauth = 0 (reauth function switch, reauth turns off automatically when rekey function is turned off)

Device. IPsec. Profile. {I}. Ikev2satimelimit = 7200 (IKE SA life cycle)

Device. IPsec. Profile{I}. Childsattrafficlimit = 5368709120 (bytes allowed in ESP life cycle, 5g bytes by default)

Device. IPsec. Profile. {I}. Childsatimelimit = 3600 (ESP SA life cycle)
```

(2) PSK authentication mode, profile configuration

When PSK authentication is used, the PSK for authentication needs to be configured in the profile. As shown in Figure 4-15.

| | | |
|-------------------|--------------------------------|--|
| Information | LocalId: | 2295033000E |
| Management | RemoteId: | psk@comba.c |
| Cell | EAPIdentity: | |
| Debug | SubnetIPType: | same to SecGW ▾ |
| Factory | LocalSubnet: | 0.0.0.0/0 |
| HeMS | RemoteSubnet: | 0.0.0.0/0 |
| Network | EncryptionAlgorithms: | AES-CBC ▾ |
| Performance | IntegrityAlgorithms: | HMAC-SHA1-96 ▾ |
| Security | DiffieHellmanGroupTransforms: | MODP-1024 ▾ |
| IPsec | EncryptionAlgorithms: | AES-CBC ▾ |
| Certificate | IntegrityAlgorithms: | HMAC-SHA1-96 ▾ |
| PSK | DiffieHellmanGroupTransforms: | NONE ▾ |
| eSIM | Rekey: | <input checked="" type="checkbox"/> Enable |
| File transmission | Reauth: | <input type="checkbox"/> Enable |
| Synchronization | IKEv2SATimeLimit: | 7200 |
| Upgrade | ChildSATimeLimit: | 3600 |
| Access Control | MarginTime: | 300 |
| Data Model | IKEv2DeadPeerDetectionTimeout: | 30 |
| | IKEv2DeadPeerDetectionAction: | None ▾ |

IKEv2AuthMethod : PSK

| ID | Enable | Encoding | PreSharedKey | In use |
|----|--------|----------|--------------|--------|
| 1 | Y | 0 | ***** | * |

IKEv2PeerAuthMethod: PSK

| ID | Enable | Encoding | PreSharedKey | In use |
|----|--------|----------|--------------|--------|
| 1 | Y | 0 | ***** | ○ |

Submit **Back**

Figure 4-15 select PSK

(3) Virtual SIM authentication mode, profile configuration

When the virtual USIM authentication mode is adopted, the virtual vSIM for authentication needs to be configured in the profile. As shown in the figure.

| Information Management Cell Debug Factory HeMS Network Performance Security IPsec Certificate PSK eSIM File transmission Synchronization Upgrade Access Control Data Model | <p>LocalId: 2295033000E</p> <p>RemoteId: psk@comba.c</p> <p>EAPIdentity: <input type="text"/></p> <p>SubnetIPType: same to SecGW <input type="button" value="▼"/></p> <p>LocalSubnet: 0.0.0.0/0</p> <p>RemoteSubnet: 0.0.0.0/0</p> <p>IKEv2:</p> <p>EncryptionAlgorithms: AES-CBC <input type="button" value="▼"/></p> <p>IntegrityAlgorithms: HMAC-SHA1-96 <input type="button" value="▼"/></p> <p>DiffieHellmanGroupTransforms: MODP-1024 <input type="button" value="▼"/></p> <p>ESP:</p> <p>EncryptionAlgorithms: AES-CBC <input type="button" value="▼"/></p> <p>IntegrityAlgorithms: HMAC-SHA1-96 <input type="button" value="▼"/></p> <p>DiffieHellmanGroupTransforms: NONE <input type="button" value="▼"/></p> <p>Rekey: <input checked="" type="checkbox"/> Enable</p> <p>Reauth: <input type="checkbox"/> Enable</p> <p>IKEv2SATimeLimit: 7200</p> <p>ChildSATimeLimit: 3600</p> <p>MarginTime: 300</p> <p>IKEv2DeadPeerDetectionTimeout: 30</p> <p>IKEv2DeadPeerDetectionAction: None <input type="button" value="▼"/></p> <p>IKEv2AuthMethod : PSK <input type="button" value="▼"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ID</th> <th>Enable</th> <th>Encoding</th> <th>PreSharedKey</th> <th>In use</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>0</td> <td>*****</td> <td>*</td> </tr> </tbody> </table> <p>IKEv2PeerAuthMethod: PSK <input type="button" value="▼"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>ID</th> <th>Enable</th> <th>Encoding</th> <th>PreSharedKey</th> <th>In use</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Y</td> <td>0</td> <td>*****</td> <td>○</td> </tr> </tbody> </table> <p style="text-align: center;"><input type="button" value="Submit"/> <input type="button" value="Back"/></p> | ID | Enable | Encoding | PreSharedKey | In use | 1 | Y | 0 | ***** | * | ID | Enable | Encoding | PreSharedKey | In use | 1 | Y | 0 | ***** | ○ |
|--|--|----------|--------------|----------|--------------|--------|---|---|---|-------|---|----|--------|----------|--------------|--------|---|---|---|-------|---|
| ID | Enable | Encoding | PreSharedKey | In use | | | | | | | | | | | | | | | | | |
| 1 | Y | 0 | ***** | * | | | | | | | | | | | | | | | | | |
| ID | Enable | Encoding | PreSharedKey | In use | | | | | | | | | | | | | | | | | |
| 1 | Y | 0 | ***** | ○ | | | | | | | | | | | | | | | | | |

Figure 4-16 selecting virtual SIM

(4) Certificate authentication method, profile configuration

T&W

| Information Management Alarm Information Debug Factory Upgrade HeMS Network Security IPSec Certificate PSK vSIM File transmission Data Model | ESP: IntegrityAlgorithms: HMAC-SHA1-96 DiffieHellmanGroupTransforms: NONE Rekey: <input checked="" type="checkbox"/> Enable Reauth: <input type="checkbox"/> Enable IKEv2SATimeLimit: 7200 ChildSATimeLimit: 3600 MarginTime: 300 IKEv2DeadPeerDetectionTimeout: 30 IKEv2DeadPeerDetectionAction: None | | | | | | | | | | |
|---|---|---|-------------------------------------|-----------------------|--------------|--------|--------|---|-------------------------------------|-------|-----------------------|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| IKEv2AuthMethod: Certificate | | | | | | | | | | | |
| <table border="1"><thead><tr><th>ID</th><th>Type</th><th>Issuer</th><th>In use</th></tr></thead><tbody><tr><td>1</td><td>Client</td><td>C = CN,O = China Telecom Guangdong Academy,CN = Guangdong Academy SubCA</td><td><input checked="" type="checkbox"/></td></tr></tbody></table> | | ID | Type | Issuer | In use | 1 | Client | C = CN,O = China Telecom Guangdong Academy,CN = Guangdong Academy SubCA | <input checked="" type="checkbox"/> | | |
| ID | Type | Issuer | In use | | | | | | | | |
| 1 | Client | C = CN,O = China Telecom Guangdong Academy,CN = Guangdong Academy SubCA | <input checked="" type="checkbox"/> | | | | | | | | |
| IKEv2PeerAuthMethod: PSK | | | | | | | | | | | |
| <table border="1"><thead><tr><th>ID</th><th>Enable</th><th>Encoding</th><th>PreSharedKey</th><th>In use</th></tr></thead><tbody><tr><td>1</td><td>Y</td><td>0</td><td>*****</td><td><input type="radio"/></td></tr></tbody></table> | | ID | Enable | Encoding | PreSharedKey | In use | 1 | Y | 0 | ***** | <input type="radio"/> |
| ID | Enable | Encoding | PreSharedKey | In use | | | | | | | |
| 1 | Y | 0 | ***** | <input type="radio"/> | | | | | | | |
| Submit Back | | | | | | | | | | | |

Figure 4-17 selecting certificates

(5) View profile configuration information

After the profile configuration is completed, you can view and confirm the profile configuration information through the web page, as shown in the figure.

T&W

| Information Management Cell Debug Factory HeMS Network Performance Security IPsec Certificate PSK vSIM File transmission Synchronization Upgrade Access Control Data Model | <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td colspan="2"></td><td>LocalId: 2295033000E</td></tr> <tr><td colspan="2"></td><td>RemoteId: psk@comba.c</td></tr> <tr><td colspan="2"></td><td>EAPIdentity:</td></tr> <tr><td colspan="2"></td><td>SubnetIPType: same to SecGW ▼</td></tr> <tr><td colspan="2"></td><td>LocalSubnet: 0.0.0.0/0</td></tr> <tr><td colspan="2"></td><td>RemoteSubnet: 0.0.0.0/0</td></tr> <tr><td colspan="2" style="text-align: right;">IKEv2:</td><td>EncryptionAlgorithms: AES-CBC ▼</td></tr> <tr><td colspan="2"></td><td>IntegrityAlgorithms: HMAC-SHA1-96 ▼</td></tr> <tr><td colspan="2"></td><td>DiffieHellmanGroupTransforms: MODP-1024 ▼</td></tr> <tr><td colspan="2" style="text-align: right;">ESP:</td><td>EncryptionAlgorithms: AES-CBC ▼</td></tr> <tr><td colspan="2"></td><td>IntegrityAlgorithms: HMAC-SHA1-96 ▼</td></tr> <tr><td colspan="2"></td><td>DiffieHellmanGroupTransforms: MODP-1024 ▼</td></tr> <tr><td colspan="2"></td><td>Rekey: <input checked="" type="checkbox"/> Enable</td></tr> <tr><td colspan="2"></td><td>Reauth: <input type="checkbox"/> Enable</td></tr> <tr><td colspan="2"></td><td>IKEv2SATimeLimit: 7200</td></tr> <tr><td colspan="2"></td><td>ChildSATimeLimit: 3600</td></tr> <tr><td colspan="2"></td><td>MarginTime: 300</td></tr> <tr><td colspan="2"></td><td>IKEv2DeadPeerDetectionTimeout: 30</td></tr> <tr><td colspan="2"></td><td>IKEv2DeadPeerDetectionAction: None ▼</td></tr> <tr><td colspan="3" style="text-align: center; padding-top: 10px;"> IKEv2AuthMethod: eSIM ▼ </td></tr> <tr> <td colspan="3" style="text-align: center; padding-top: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>eSIMKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>1</td><td>01020304050607080102030405060708</td><td><input checked="" type="radio"/></td></tr> </tbody> </table> </td></tr> <tr><td colspan="3" style="text-align: center; padding-top: 10px;"> IKEv2PeerAuthMethod: PSK ▼ </td></tr> <tr> <td colspan="3" style="text-align: center; padding-top: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>PreSharedKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>0</td><td>*****</td><td><input type="radio"/></td></tr> </tbody> </table> </td></tr> <tr> <td colspan="3" style="text-align: center; padding-top: 10px;"> Submit Back </td></tr> </table> | | | LocalId: 2295033000E | | | RemoteId: psk@comba.c | | | EAPIdentity: | | | SubnetIPType: same to SecGW ▼ | | | LocalSubnet: 0.0.0.0/0 | | | RemoteSubnet: 0.0.0.0/0 | IKEv2: | | EncryptionAlgorithms: AES-CBC ▼ | | | IntegrityAlgorithms: HMAC-SHA1-96 ▼ | | | DiffieHellmanGroupTransforms: MODP-1024 ▼ | ESP: | | EncryptionAlgorithms: AES-CBC ▼ | | | IntegrityAlgorithms: HMAC-SHA1-96 ▼ | | | DiffieHellmanGroupTransforms: MODP-1024 ▼ | | | Rekey: <input checked="" type="checkbox"/> Enable | | | Reauth: <input type="checkbox"/> Enable | | | IKEv2SATimeLimit: 7200 | | | ChildSATimeLimit: 3600 | | | MarginTime: 300 | | | IKEv2DeadPeerDetectionTimeout: 30 | | | IKEv2DeadPeerDetectionAction: None ▼ | IKEv2AuthMethod: eSIM ▼ | | | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>eSIMKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>1</td><td>01020304050607080102030405060708</td><td><input checked="" type="radio"/></td></tr> </tbody> </table> | | | ID | Enable | Encoding | eSIMKey | In use | 1 | Y | 1 | 01020304050607080102030405060708 | <input checked="" type="radio"/> | IKEv2PeerAuthMethod: PSK ▼ | | | <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>PreSharedKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>0</td><td>*****</td><td><input type="radio"/></td></tr> </tbody> </table> | | | ID | Enable | Encoding | PreSharedKey | In use | 1 | Y | 0 | ***** | <input type="radio"/> | Submit Back | | |
|---|--|---|----------------------------------|----------------------------------|----------|--------------|-----------------------|---|---|--------------|----------------------------------|----------------------------------|-------------------------------|--|--|------------------------|--|--|-------------------------|--------|--|---------------------------------|--|--|-------------------------------------|--|--|---|------|--|---------------------------------|--|--|-------------------------------------|--|--|---|--|--|---|--|--|---|--|--|------------------------|--|--|------------------------|--|--|-----------------|--|--|-----------------------------------|--|--|--------------------------------------|--|--|--|---|--|--|----|--------|----------|---------|--------|---|---|---|----------------------------------|----------------------------------|-----------------------------------|--|--|--|--|--|----|--------|----------|--------------|--------|---|---|---|-------|-----------------------|---|--|--|
| | | LocalId: 2295033000E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | RemoteId: psk@comba.c | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | EAPIdentity: | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | SubnetIPType: same to SecGW ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | LocalSubnet: 0.0.0.0/0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | RemoteSubnet: 0.0.0.0/0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IKEv2: | | EncryptionAlgorithms: AES-CBC ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | IntegrityAlgorithms: HMAC-SHA1-96 ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | DiffieHellmanGroupTransforms: MODP-1024 ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ESP: | | EncryptionAlgorithms: AES-CBC ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | IntegrityAlgorithms: HMAC-SHA1-96 ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | DiffieHellmanGroupTransforms: MODP-1024 ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | Rekey: <input checked="" type="checkbox"/> Enable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | Reauth: <input type="checkbox"/> Enable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | IKEv2SATimeLimit: 7200 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | ChildSATimeLimit: 3600 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | MarginTime: 300 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | IKEv2DeadPeerDetectionTimeout: 30 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | IKEv2DeadPeerDetectionAction: None ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IKEv2AuthMethod: eSIM ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>eSIMKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>1</td><td>01020304050607080102030405060708</td><td><input checked="" type="radio"/></td></tr> </tbody> </table> | | | ID | Enable | Encoding | eSIMKey | In use | 1 | Y | 1 | 01020304050607080102030405060708 | <input checked="" type="radio"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ID | Enable | Encoding | eSIMKey | In use | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Y | 1 | 01020304050607080102030405060708 | <input checked="" type="radio"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| IKEv2PeerAuthMethod: PSK ▼ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr><th>ID</th><th>Enable</th><th>Encoding</th><th>PreSharedKey</th><th>In use</th></tr> </thead> <tbody> <tr><td>1</td><td>Y</td><td>0</td><td>*****</td><td><input type="radio"/></td></tr> </tbody> </table> | | | ID | Enable | Encoding | PreSharedKey | In use | 1 | Y | 0 | ***** | <input type="radio"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ID | Enable | Encoding | PreSharedKey | In use | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Y | 0 | ***** | <input type="radio"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Submit Back | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 4-18 viewing profile information

4.2.5 Enable IPSec

After completing the relevant configuration in the above chapters, enable IPSec. Check the corresponding authentication method and click enable to enable IPSec function.



note:

After clicking "enable", the button will switch to "disable", indicating that the current status is already enabled, and clicking again will perform the disable operation.

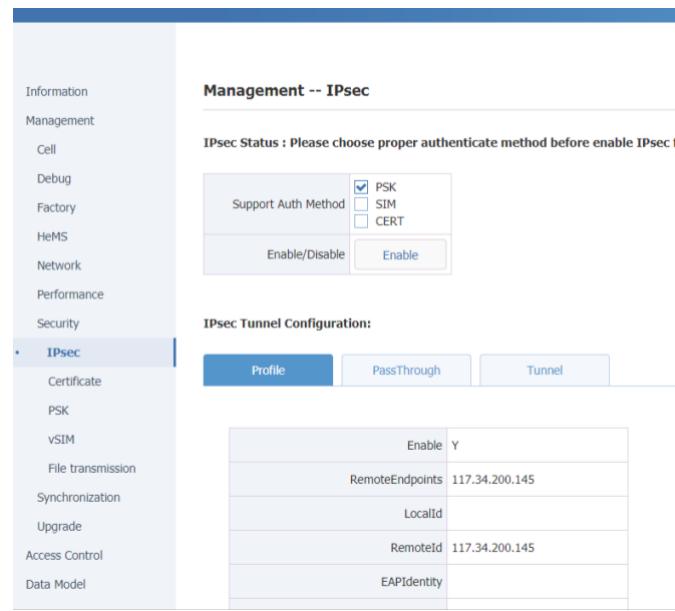


Figure 4-19 enabling IPSec

4.2.6 View IPSec status

After the base station and the security gateway successfully establish a security tunnel, you can view the IPSec tunnel status in the page **Management → IPsec → Tunnel**. As shown in the figure below.

| T&W | | | | | | | | | | | | | | | | | |
|--|---|------------------------------|---|------------------------------|-------------------------------|---|----------------------|-----------------------|--------------|----|---------------|---------------|------------|------------|------------------|---|----------------------|
| Management -- IPsec | | | | | | | | | | | | | | | | | |
| IPsec Status : Please choose proper authenticate method before enable IPsec function. | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Support Auth Method</th> <th><input checked="" type="checkbox"/> PSK</th> <th><input type="checkbox"/> SIM</th> <th><input type="checkbox"/> CERT</th> </tr> </thead> <tbody> <tr> <td>Enable/Disable</td> <td>Enable</td> <td>Disable</td> <td></td> </tr> </tbody> </table> | | Support Auth Method | <input checked="" type="checkbox"/> PSK | <input type="checkbox"/> SIM | <input type="checkbox"/> CERT | Enable/Disable | Enable | Disable | | | | | | | | | |
| Support Auth Method | <input checked="" type="checkbox"/> PSK | <input type="checkbox"/> SIM | <input type="checkbox"/> CERT | | | | | | | | | | | | | | |
| Enable/Disable | Enable | Disable | | | | | | | | | | | | | | | |
| IPsec Tunnel Configuration: <table border="1"> <thead> <tr> <th>Profile</th> <th>PassThrough</th> <th>Tunnel</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> | | Profile | PassThrough | Tunnel | | | | | | | | | | | | | |
| Profile | PassThrough | Tunnel | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| <table border="1"> <thead> <tr> <th>Status</th> <th>LocalAddress</th> <th>RemoteAddress</th> <th>InboundSPI</th> <th>OutboundSPI</th> <th>LocalTrafficSelector</th> <th>RemoteTrafficSelector</th> <th>CreationTime</th> </tr> </thead> <tbody> <tr> <td>Up</td> <td>134.84.128.16</td> <td>61.132.154.86</td> <td>0xc856f3f5</td> <td>0xc92be99d</td> <td>134.84.128.16/32</td> <td>7.191.0.0/16 10.0.0.0/8 36.60.0.0/16 134.64.248.0/24 134.84.0.0/16</td> <td>2019-11-14T06:04:24Z</td> </tr> </tbody> </table> | | Status | LocalAddress | RemoteAddress | InboundSPI | OutboundSPI | LocalTrafficSelector | RemoteTrafficSelector | CreationTime | Up | 134.84.128.16 | 61.132.154.86 | 0xc856f3f5 | 0xc92be99d | 134.84.128.16/32 | 7.191.0.0/16 10.0.0.0/8 36.60.0.0/16 134.64.248.0/24 134.84.0.0/16 | 2019-11-14T06:04:24Z |
| Status | LocalAddress | RemoteAddress | InboundSPI | OutboundSPI | LocalTrafficSelector | RemoteTrafficSelector | CreationTime | | | | | | | | | | |
| Up | 134.84.128.16 | 61.132.154.86 | 0xc856f3f5 | 0xc92be99d | 134.84.128.16/32 | 7.191.0.0/16 10.0.0.0/8 36.60.0.0/16 134.64.248.0/24 134.84.0.0/16 | 2019-11-14T06:04:24Z | | | | | | | | | | |

Figure 4-20 viewing IPSec tunnel status

4.3 Configure base station parameters

4.3.1 Set encryption and integrity protection algorithm

Set the data encryption and integrity protection algorithm of PDCP sublayer.

1. Select "data model" and "device" in the navigation bar
2. Enter "" to enter the configuration page, as shown in Figure 4-21. *Device.Services.FAPService.1.CellConfig.LTE.EPC*.
3. *AllowedCipheringAlgorithmList*



The following security parameters usually do not need to be modified, just keep the default value!

The screenshot shows the T&W configuration interface. The left sidebar has a tree view with nodes like Information, Management, Access Control, Data Model, DB export, DB import, Device (selected), and Internal. The main area has a title 'DataModel -- Device' and a search bar. Below it is a table with two columns: 'DB tree' and 'Device.Services.FAPService.1.CellConfig.LTE.EPC.'. The 'DB tree' column shows a hierarchical structure of device services, with 'EPC' being the selected node under 'LTE'. The 'Device.Services.FAPService.1.CellConfig.LTE.EPC.' column contains configuration fields:

| | | |
|---|--|---------------------------|
| AllowedCipheringAlgorithmList | 128-EEA1,128-EEA2,128-EEA3,EEAO | string(256) |
| AllowedIntegrityProtectionAlgorithmList | 128-EIA1,128-EIA2,128-EIA3,EIAO | string(256) |
| TAC | 27007 | unsignedInt([0:65535]) |
| EAID | 0 | unsignedInt([0:16777216]) |
| X_D837BE_PLMNMatchS1Enable | <input checked="" type="checkbox"/> Enable | boolean |
| MaxPLMNLListEntries | 16 | unsignedInt |
| MaxQoSEntries | 256 | unsignedInt |
| Device.Services.FAPService.1.CellConfig.LTE.EPC.PLMNLList.(). | | |
| Device.Services.FAPService.1.CellConfig.LTE.EPC.QoS.(). | | |

At the bottom are 'submit' and 'drop' buttons.

Figure 4-21 setting encryption and integrity protection algorithm

4. Safety parameter description is shown in table 4-6.

| Parameter name | explain |
|---|--|
| AllowedCipheringAlgorithmList | Encryption algorithm. Value range: <ul style="list-style-type: none">• 128-EEA1, 128-EEA2, 128-EEA3, EEA0• Configurable, separated by commas The default value is 128-eeal |
| AllowedIntegrityProtectionAlgorithmList | Integrity protection algorithm. Value range: <ul style="list-style-type: none">• 128-EIA1, 128-EIA2, 128-EIA3, EIA0• Configurable, separated by commas |

| Parameter name | explain |
|----------------|-------------------------------|
| | The default value is 128-eial |

Table 4 -6Safety parameter description

4.3.2Configure network management connection

Select "management-> HeMS" in the navigation bar, as shown in Figure 4-22.

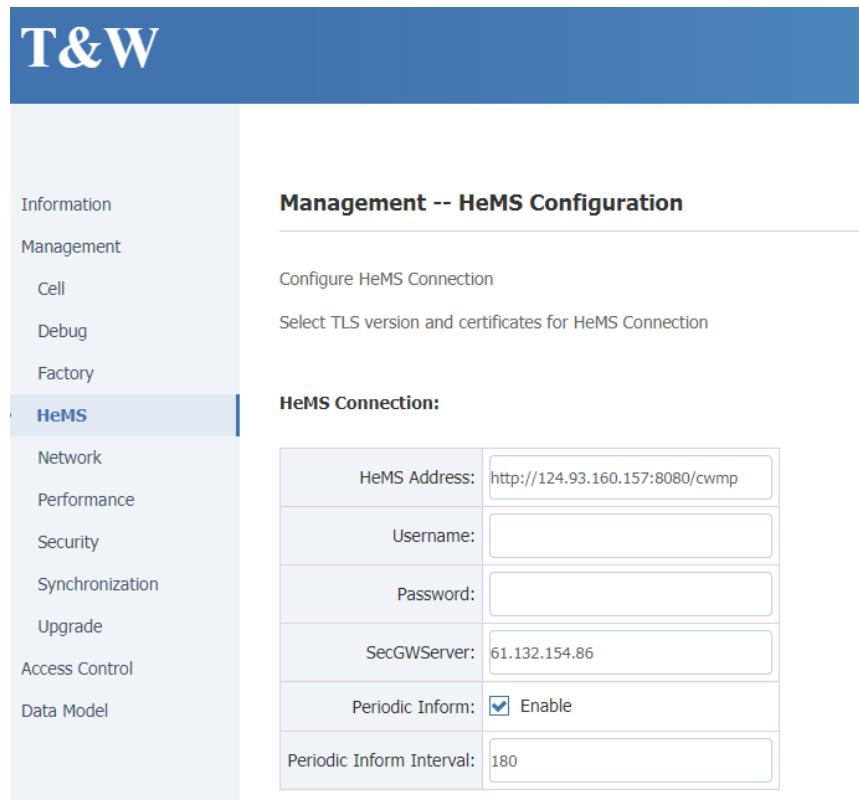


chart4-22Configure network management

Network management parameters are shown in table 3-9.

| Parameter name | explain |
|----------------|--|
| HeMS Address | Network management address of Picchi station, such as http://135.224.42.2:8080/itmscpe/inform |
| Username | User name of network management, fill in as required. |
| Password | Network management password, fill in as required. |
| SecGWServer | Security gateway address. According to the actual network deployment, this item needs to be filled in when the security gateway needs to be connected before connecting to the network management. |

Table 4-7 network management parameter description

4.3.3 Configure base station synchronization parameters

4G small base station supports 3 synchronization modes, IEEE1588 air port and GPS. When the synchronization mode switching function is turned on, the base station can switch between synchronization modes.

The screenshot shows a web-based configuration interface for a base station. On the left, a sidebar lists various management categories: Information, Management, Security, ACS, Cell, Performance, Synchronization (which is selected and highlighted in red), Network, Fault, Debug, Upgrade, Factory, Access Control, and Data Model. At the top right, there are tabs for Synchronization (selected), GPS, PTP/ACR, Sniffer, and NTP/Time. Below the tabs is a section titled "Sync Setting:" containing a table with the following data:

| | |
|------------------------|---------------------------------|
| CurrentSyncMode | Freedom |
| SyncStatus | Undefined |
| SuccessTime | 0001-01-01T00:00:00Z |
| SyncSwitchEnable | <input type="checkbox"/> Enable |
| SyncMode1 | Freedom ▾ |
| SyncMode2 | Freedom ▾ |
| SyncMode3 | Freedom ▾ |
| SyncFailureHandling | Ignored ▾ |
| TimingCorrectionOffset | 0 |

At the bottom of the table is a "Submit" button.

Figure 4-23 synchronization mode interface



note:

- At present, syncmode1 is only used for synchronization mode setting, while syncmode2 and syncmode3 are not used temporarily.
- Air port synchronization can only synchronize frequency, not time. It needs to be used with NTP function.

1. The corresponding parameters of synchronization mode are shown in table

| Synchronization mode | explain |
|-------------------------|---|
| Freedom | Free mode, i.e. no synchronization |
| IEEE1588 V2 | IEEE1588 uses accurate time stamp to calculate time and frequency offset through IEEE1588 message transmitted between master and slave devices, so as to achieve frequency and time synchronization between master and slave. And the accuracy can reach microsecond level. IEEE1588 V2 supports frequency synchronization and time synchronization. |
| IEEE1588 ACR | 1588acr (adaptive clock recovery) refers to the master device supporting IEEE 1588v2 that encapsulates the clock information of local system into 1588v2 message and transmits it to the slave device of the opposite through the third party network. The slave device obtains the time stamp from the 1588v2 message and recovers the clock to achieve the frequency synchronization of the devices at both sides of PSN (packet switched network). |
| Sniffer synchronization | By receiving the reference signal of macro cell to calculate the time deviation between macro cell and itself so as to |

| Synchronization mode | explain |
|----------------------|--|
| | calibrate the timing and achieve the purpose of synchronization with macro cell. |
| GPS/RGPS | The base station needs external GPS antenna |

Table 4 -8Synchronization mode

2. Synchronization configuration parameters are shown in table 4-9.

| parameter | explain |
|---------------------|--|
| SyncSwitchEnable | Synchronous source switch. Off by default. |
| SyncFailureHandling | How to deal with synchronization failure in BTS <ul style="list-style-type: none"> • Ignore by default: ignore synchronization failure; • Restart: if the synchronization fails, the cell will be deleted and retried; • Reboot: if the synchronization fails, the BTS will be restarted and retried; |

Table 4-9 synchronization mode parameters

4.3.3.1GPS synchronization

1. The base station needs external GPS antenna.
2. Set the synchronization mode to "GPS";
3. Configure frame migration according the operter plan, as shown in figure 4-24 and the calculation method of frame migration is shown in table4-10.

| CurrentSyncMode | Freedom |
|------------------------|--|
| SyncStatus | Undefined |
| SuccessTime | 0001-01-01T00:00:00Z |
| SyncSwitchEnable | <input checked="" type="checkbox"/> Enable |
| SyncMode1 | GPS |
| SyncMode2 | Freedom |
| SyncMode3 | Freedom |
| SyncFailureHandling | Ignored |
| TimingCorrectionOffset | 0 |

Figure 4-24GPS synchronization configuration-

Table 4-10 frame migration parameter description-

| The parameter name | instructions |
|------------------------|--|
| TimingCorrectionOffset | Time synchronization frame offset, Chip(1/30.72us), valid for GNSS and IEEE1588V2.If the macro station is 700us ahead of the GPS frame header, then the frame offset should be $700 \times 30.72 = 21504$. (the macro station here is of the same frequency band) |

4. After parameter configuration is completed, click "Submit";
5. Restart base station and perform GPS synchronization.
6. After the base station restarts, query the GPS synchronization status, as shown in the figure below.

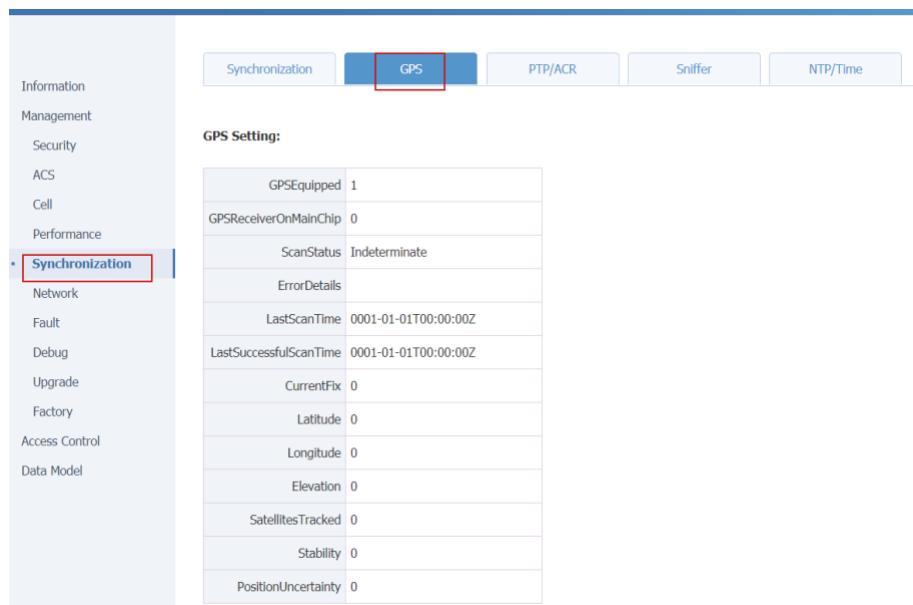


Figure 4-25 GPS synchronization status-

4.3.3.2 Configure IEEE1588 V2 synchronization

1. There are 1588 clock synchronization signals in the network environment of the base station.
2. 1588 PTPv2 is divided into two modes: multicast and unicast. The configuration of multicast mode is shown in figure 4-26.
 - Select "Ethernet" for Transport;
 - Role select "Slave";

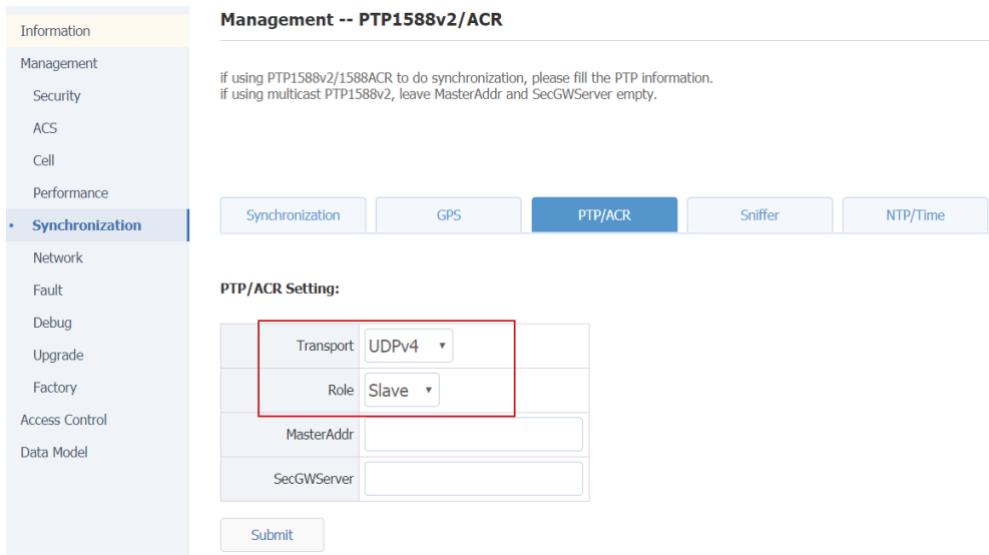


Figure 4-26 IEEE1588 V2 layer 2 multicast mode

3. IEEE1588 V2 unicast mode configuration, as shown in Figure 4-21.

- Select "Ethernet" for transport;
- Role select "slave";
- Master addr fills in IP address of master clock;
- In the PTP over IPSec scenario, you need to specify the security gateway address. Secgwserver fills in the security gateway IP address.

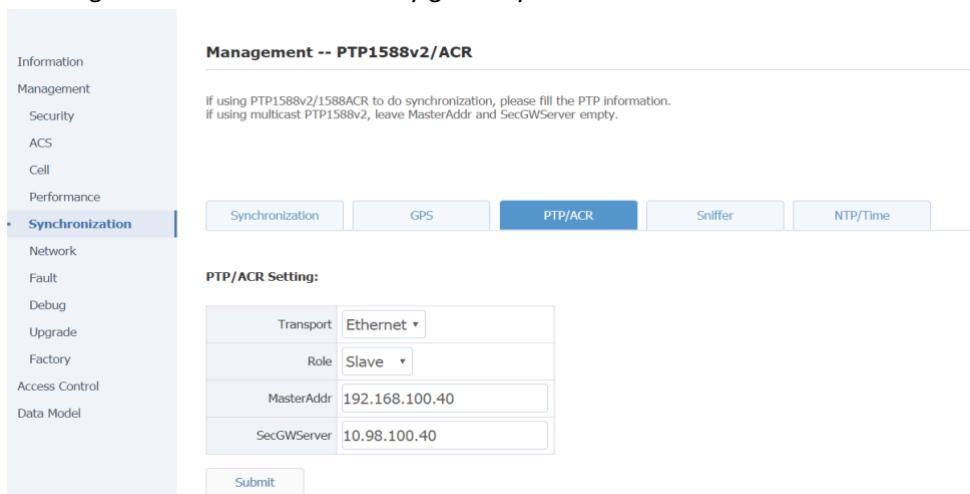


Figure 4-21 IEEE1588 layer V2 three unicast mode

4. Configure frame offset. See the table below for the value of frame offset.

| Parameter name | explain |
|------------------------|--|
| TimingCorrectionOffset | Time synchronization frame offset, in chip (1 / 30.72us), is effective for GNSS and ieee1588v2 modes. If the macro station is 700us ahead of the GPS frame head, then the frame offset should be |

| Parameter name | explain |
|----------------|--|
| | $700 * 30.72 = 21504$. (the macro station here is of the same frequency band) |

Table 4 -10Frame offset parameter description

5. After setting the above synchronization parameters, set the synchronization mode to "ptp1588", and click "submit" to submit;



After modifying the synchronization mode, the base station takes effect by restarting to performs synchronization.

T&W

| CurrentSyncMode | Sniffer |
|------------------------|---------------------------------|
| SyncStatus | Success |
| SuccessTime | 2019-11-13T09:18:25.174Z |
| SyncSwitchEnable | <input type="checkbox"/> Enable |
| SyncMode1 | PTP1588 |
| SyncMode2 | Freedom |
| SyncMode3 | Freedom |
| SyncFailureHandling | Ignored |
| TimingCorrectionOffset | 0 |

Figure 4-27 1588 ptpp2 synchronization configuration

6. After the base station is restarted, check the synchronization status.

4.3.3.3 Configure IEEE1588 ACR synchronization

- IEEE1588 ACR synchronization parameter settings are shown in Figure 4-28.
 - Transport select "udpv4";
 - Role select "slave";
 - Master addr fills in 1588 ACR server address;
 - In the PTP over IPSec scenario, you need to specify the security gateway address. Secgwserver fills in the security gateway IP address.

Information
Management
Security
ACS
Cell
Performance

Synchronization

Network
Fault
Debug
Upgrade
Factory
Access Control
Data Model

Management -- PTP1588v2/ACR

if using PTP1588v2/1588ACR to do synchronization, please fill the PTP information.
if using multicast PTP1588v2, leave MasterAddr and SecGWServer empty.

| | | | | |
|-----------------|-----|---------|---------|----------|
| Synchronization | GPS | PTP/ACR | Sniffer | NTP/Time |
|-----------------|-----|---------|---------|----------|

PTP/ACR Setting:

| | |
|---------------|---------|
| Transport | UDPV4 ▾ |
| Role | Slave ▾ |
| MasterAddr | |
| SecGWServer | |
| Submit | |

Figure 4-28 IEEE1588 ACR synchronization parameter setting

- Set the synchronization mode to 1588 ACR, and click "submit" to submit, as shown in Figure 4-29;



After modifying the synchronization mode, the base station takes effect by restarting to performs synchronization.

Information
Management
Security
ACS
Cell
Performance

Synchronization

Network
Fault
Debug
Upgrade
Factory
Access Control
Data Model

you can choose the sync mode here.
if you choose ptp1588 or gps, then ntp disabled.

| | | | | |
|-----------------|-----|---------|---------|----------|
| Synchronization | GPS | PTP/ACR | Sniffer | NTP/Time |
|-----------------|-----|---------|---------|----------|

Sync Setting:

| | |
|------------------------|---------------------------------|
| CurrentSyncMode | Freedom |
| SyncStatus | Undefined |
| SuccessTime | 0001-01-01T00:00:00Z |
| SyncSwitchEnable | <input type="checkbox"/> Enable |
| SyncMode1 | 1588ACR ▾ |
| SyncMode2 | Freedom ▾ |
| SyncMode3 | Freedom ▾ |
| SyncFailureHandling | Ignored ▾ |
| TimingCorrectionOffset | 0 |
| Submit | |

Figure 4-29 IEEE1588 ACR synchronization mode setting

4.3.3.4 Set air port synchronization

- Configure the frequency point of air port synchronization, as shown in Figure 4-30.

Management -- Sniffer

if using Sniffer to do synchronization, please fill the Sniffer information here.
Since Sniffer only adjust the frequency, better add one NTP server to fix system time.

Sniffer Setting:

| | |
|--------------------|---------------------------------|
| CheckRSPEnable | <input type="checkbox"/> Enable |
| CheckBWEnable | <input type="checkbox"/> Enable |
| EARFCNDDLList | 100,1825 |
| DonorBWThreshold | 50 |
| DonorRSPTThreshold | 9 |
| SuccessRatType | Eutran |
| SuccessArfcn | 100 |
| SuccessPci | 394 |

Submit

Figure 4-30 setting the sniffer synchronization frequency point

- Set the synchronization mode to "sniffer", and click "submit" to submit;

Management -- Sync Mode

you can choose the sync mode here.
if you choose ptp1588 or gps, then ntp disabled.

Sync Setting:

| | |
|------------------------|---------------------------------|
| CurrentSyncMode | Sniffer |
| SyncStatus | Success |
| SuccessTime | 2019-11-13T09:18:25.174Z |
| SyncSwitchEnable | <input type="checkbox"/> Enable |
| SyncMode1 | Sniffer |
| SyncMode2 | Freedom |
| SyncMode3 | Freedom |
| SyncFailureHandling | Ignored |
| TimingCorrectionOffset | 0 |

Submit

Figure 4-31 sniffer synchronization configuration

⚠ note:

After modifying the synchronization mode, the base station takes effect by restarting to performs synchronization.

3. After the base station is restarted, check the air port synchronization status, as shown in Figure 4-32.

The screenshot shows a web-based management interface titled "Management -- Sync Mode". On the left, there is a sidebar with various navigation options: Information, Management, Cell, Debug, Factory, HeMS, Network, Performance, Security, Synchronization (which is currently selected), Upgrade, Access Control, and Data Model. The main content area has a heading "Management -- Sync Mode" and a note: "you can choose the sync mode here. if you choose ptpt1588 or gps, then ntp disabled." Below this is a horizontal navigation bar with tabs: Synchronization (selected), GPS, PTP/ACR, Sniffer, and NTP/Time. A table titled "Sync Setting:" contains the following data:

| CurrentSyncMode | Sniffer |
|------------------------|---------------------------------|
| SyncStatus | Success |
| SuccessTime | 2019-11-13T09:18:25.174Z |
| SyncSwitchEnable | <input type="checkbox"/> Enable |
| SyncMode1 | Sniffer ▾ |
| SyncMode2 | Freedom ▾ |
| SyncMode3 | Freedom ▾ |
| SyncFailureHandling | Ignored ▾ |
| TimingCorrectionOffset | 0 |

At the bottom of the form is a "Submit" button.

Figure 4-32 air port synchronization status query

4. When the sniffer synchronization mode is selected, not all the scanned base stations can be used as synchronization targets, Device.Services.FAPService.1.X_D837BE_SON.CNM.DonorRSPTresholdThe minimum threshold that can be used as the reference signal power of the synchronization target cell is defined. The default value is 9, as shown in Figure 4-33. See table 4-11 for parameter description.

| Parameter name | Value range | explain |
|--------------------|-------------|---|
| DonorRSPTThreshold | [-60:50] | The minimum threshold that can be used as the reference signal power of the synchronization target cell. The default value is 9, which generally corresponds to the reference signal power of the macro station. If you want to use the small base station as the synchronization target, you should set this parameter as the reference signal power of the corresponding small base station, which is generally negative. |

Figure 4-33 power threshold of synchronous target reference signal

| Parameter name | Value range | explain |
|--------------------|-------------|---|
| DonorRSPTThreshold | [-60:50] | The minimum threshold that can be used as the reference signal power of the synchronization target cell. The default value is 9, which generally corresponds to the reference signal power of the macro station. If you want to use the small base station as the synchronization target, you should set this parameter as the reference signal power of the corresponding small base station, which is generally negative. |

surface4-11Synchronous target reference power description

4.3.3.5Free mode

1. Set the synchronization mode to "freedom";
2. In free mode, the base station will not synchronize with any synchronous source, only rely on its own crystal oscillator to ensure frequency offset.

4.3.4Configure NTP service

Select "management synchronization" in the navigation bar to enter the NTP / time setting page, as shown in Figure 4-34 below.

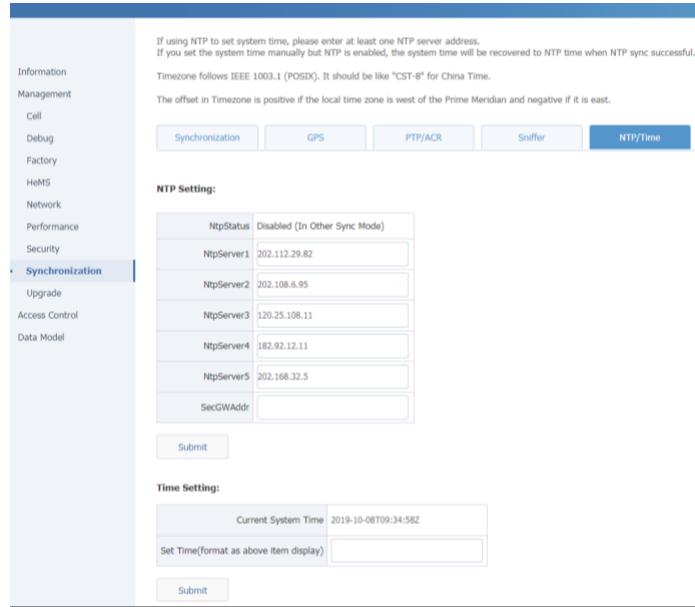


Figure 4-34 NTP configuration

Configure NTP server parameters, as shown in 4-12.

| Parameter name | explain |
|----------------|---|
| NTP Server | The domain name or IP address of the NTP server.(multiple can be configured at the same time) |

surface4-12 NTP server parameter description

4.4 Configure LTE parameters

4.4.1 Configure neighborhood parameters

4.4.1.1 Neighbor cell is found by air port listening mode

The base station has the self discovery and self configuration functions of the intra frequency neighborhood, inter frequency neighborhood and inter system neighborhood based on air port listening. It supports the self discovery and self configuration functions of the measurement frequency points based on air port listening.

1. Enable neighborhood self-discovery and frequency point self-measurement functions based on air port interception, as shown in Figure 4-35.

Data model path:

Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam.SnifferForANREnable

Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam.SnifferForMeasurementEnable

T&W

| Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam. | | | |
|--|--|----------------------|--|
| LTESnifferChannelList | | string(64[0:65535]) | |
| GERANSnifferEnable | <input type="checkbox"/> Enable | boolean | |
| GERANSnifferChannelList | | string(256[0:65535]) | |
| UTRANSnifferEnable | <input type="checkbox"/> Enable | boolean | |
| UTRANSnifferChannelList | | string(256[0:65535]) | |
| MROEnable | <input checked="" type="checkbox"/> Enable | boolean | |
| X_D837BE_MROInterFreqEnable | <input checked="" type="checkbox"/> Enable | boolean | |
| SHEnable | <input checked="" type="checkbox"/> Enable | boolean | |
| SyncMode | Sniffer | string | |
| X_D837BE_PeriodicSnifferInterval | 0 | unsignedInt | |
| X_D837BE_SnifferForANREnable | <input checked="" type="checkbox"/> Enable | boolean | |
| X_D837BE_SnifferForMeasurementEnable | <input checked="" type="checkbox"/> Enable | boolean | |
| X_D837BE_LTESnifferRSRPTresholdForANR | -95 | int([-140:-44]) | |

Figure 4-35 function switch of neighbor self discovery and frequency point self measurement based on air port listening

Parameter description is shown in table 4-13.

| Parameter name | explain |
|-----------------------------|---|
| SnifferForANREnable | Neighborhood self-discovery function switch based on air port interception. (default enable) |
| SnifferForMeasurementEnable | Frequency point self-measurement function switch based on air port interception. (default enable) |

Table 4-13 parameter description

(1) Add LTE neighbor by air port listening

- 1) Sets the LTE band or frequency point .

Information
Management
Access Control
Data Model
DB export
DB import
Device
Internal

DataModel -- Device

Root Path: Device.

DB tree

- Device
 - Services
 - FAPService
 - FAPService.1
 - Capabilities
 - FAPControl
 - AccessMgmt
 - CellConfig
 - REM
 - UMTS
 - WCDMA
 - X_D837BE_TDSCDMA
 - GSM
 - LTE
 - Cell
 - CarrierMeas
 - Transport
 - X_D837BE_L2Para
 - X_D837BE_X2
 - X_D837BE_HEX0
 - X_D837BE_PTP
 - X_D837BE_RF

Device.Services.FAPService.1.REM.LTE.

| | | |
|-------------------------|--|----------------------|
| InServiceHandling | Immediate | string |
| ScanOnBoot | <input checked="" type="checkbox"/> Enable | boolean |
| ScanPeriodically | <input type="checkbox"/> Enable | boolean |
| PeriodicInterval | 0 | unsignedInt |
| PeriodicTime | 0001-01-01T00:00:00Z | dateTime |
| REMLMNLList | | string(32) |
| REMBandList | | string(32) |
| EUTRACarrierARFCNDLList | 1750 | string(64[0:262143]) |
| ScanTimeout | 0 | unsignedInt |
| ScanStatus | Indeterminate | string |
| ErrorDetails | NULL | string |
| LastScanTime | 0001-01-01T00:00:00Z | dateTime |

Figure 4-36 setting listen LTE enable switch

Information
Management
Access Control
Data Model
DB export
DB import
Device
Internal

DataModel -- Device

Root Path: Device.

DB tree

- Device
 - Services
 - FAPControl
 - LTE
 - SelfConfig
 - SONConfigParam
 - Gateway
 - X2IpAddrMapInfo
 - AccessMgmt
 - CellConfig
 - REM
 - UMTS
 - WCDMA
 - X_D837BE_TDSCDMA
 - GSM
 - LTE
 - Cell
 - CarrierMeas
 - Transport
 - X_D837BE_L2Para
 - X_D837BE_X2
 - X_D837BE_HEX0
 - X_D837BE_PTP
 - X_D837BE_RF
 - X_D837BE_TCFS

Device.Services.FAPService.1.REM.LTE.

| | | |
|-------------------------|--|----------------------|
| InServiceHandling | Immediate | string |
| ScanOnBoot | <input checked="" type="checkbox"/> Enable | boolean |
| ScanPeriodically | <input type="checkbox"/> Enable | boolean |
| PeriodicInterval | 0 | unsignedInt |
| PeriodicTime | 0001-01-01T00:00:00Z | dateTime |
| REMLMNLList | | string(32) |
| REMBandList | | string(32) |
| EUTRACarrierARFCNDLList | 100,1825 | string(64[0:262143]) |
| ScanTimeout | 0 | unsignedInt |
| ScanStatus | Indeterminate | string |
| ErrorDetails | NULL | string |
| LastScanTime | 0001-01-01T00:00:00Z | dateTime |

Figure 4-37 setting LTE frequency points for listening

| Parameter name | explain |
|------------------------|---|
| ScanOnBoot | function switch, |
| LTESnifferFreqBandList | Scanning frequency points, common frequency points include: 1850, 1825, 100 |

| Parameter name | explain |
|-----------------------|---|
| LTESnifferChannelList | Frequency band scanned. Full band scanning will take a long time so it need to be configured as required. |

surface4-14 configuration description of LTE adjacent area scanning parameters

2) Check the scanning results of air port listening, as shown in figure 4-38.

Data model path: Device.Services.FAPService.1.REM.LTE.Cell

The screenshot shows the Data Model -- Device interface. On the left, there's a sidebar with options like Information, Management, Access Control, Data Model, DB export, DB import, and a selected 'Device' option. Below that is an 'Internal' link. The main area has a 'Root Path: Device.' input field with 'search' and 'clear' buttons. To the right is a 'DB tree' pane and a configuration pane for 'Device.Services.FAPService.1.REM.LTE.Cell.1.RF'. The DB tree shows a hierarchy: Device > Services > FAPService > FAPService.1 > Capabilities, FAPControl, AccessMgmt, CellConfig, REM, UMTS, WCDMA, X_D837BE_TDSCDMA, GSM, LTE, Cell, Cell.1, RF, BCCH. A red box highlights the 'LTE' node under 'Cell'. The configuration pane for 'Device.Services.FAPService.1.REM.LTE.Cell.1.RF' contains fields for EUTRACarrierARFCN (100), PhyCellID (402), RSRP (-64), RSRQ (0), and RSSI (0). There are 'submit' and 'drop' buttons at the bottom.

Figure 4-38 viewing the scanning results of air port listening

3) View the neighbor cells added by air port listening.

The neighbor cells discovered through the air port listening mode will be added to the neighbor relationship table of the base station.

Data model path:

Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborListInUse.



note:

Some of the scanned LTE cells are not added to the neighbor relationship table of the base station due to weak RSRP of the scanned LTE cells. You can add these cells to the neighbor relationship table by properly adjusting the threshold (LTESnifferRSRPThresholdForANR), see table 4-15.

Data model path:

Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam.

LTESnifferRSRPThresholdForANR

| Parameter name | Value range | explain |
|-------------------------------|-------------|---|
| LTESnifferRSRPThresholdForANR | [-140:-44] | The RPSR threshold that LTE adjacent cell scanned can be used as neighbor |

cell . The default value is - 95, which can be adjusted according to the actual environment.

surface4-15Whether the LTE neighbor listening is the neighbor of the base station

(2) Add GSM neighbor cell by air port listening mode

1) Enable GSM air port listening function

2) Set parameters for GSM listening

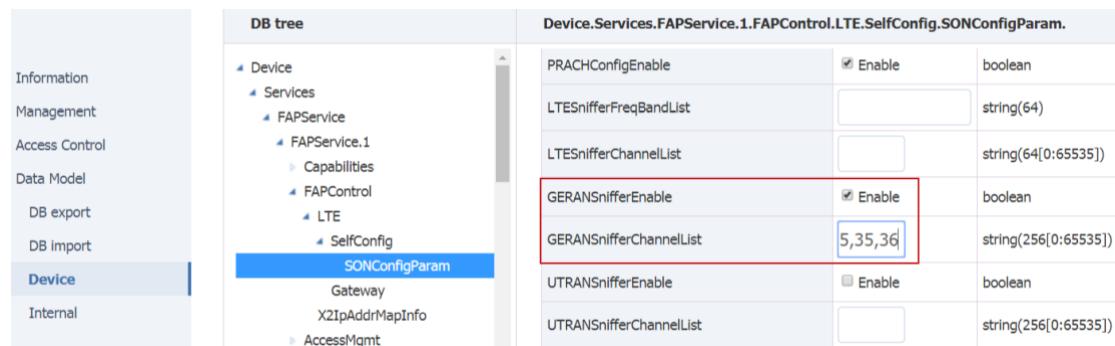


Figure 4-39 setting the GSM frequency point for listening

| Parameter name | explain |
|---|--|
| Device.Services.FAPService.1.REM.UMTS.GSM. ScanOnBoot | GSM air port listening switch.0: disable; 1: enabled |
| Device.Services.FAPService.1.REM.UMTS.GSM.REMPLMNList | Enter the operators PLMN, and the BTS will filter the scanned neighbor cell and only keep neighbor cell which PLMN belonging to the remplmnlist. |
| Device.Services.FAPService.1.REM.UMTS.GSM.REMBandList | Generally, the scanned GSM frequency band does not need to be scanned, so this item can be left blank. |
| Device.Services.FAPService.1.REM.UMTS.GSM. ARFCNList | GSM frequency point scanned. |

Table 4 -16 configuration description of GSM adjacent area scanning parameters

3) Check the scan results of GSM cell, as shown in figure 4-40.

Data model path:Device.Services.FAPService.1.REM.UMTS.GSM.Cell.

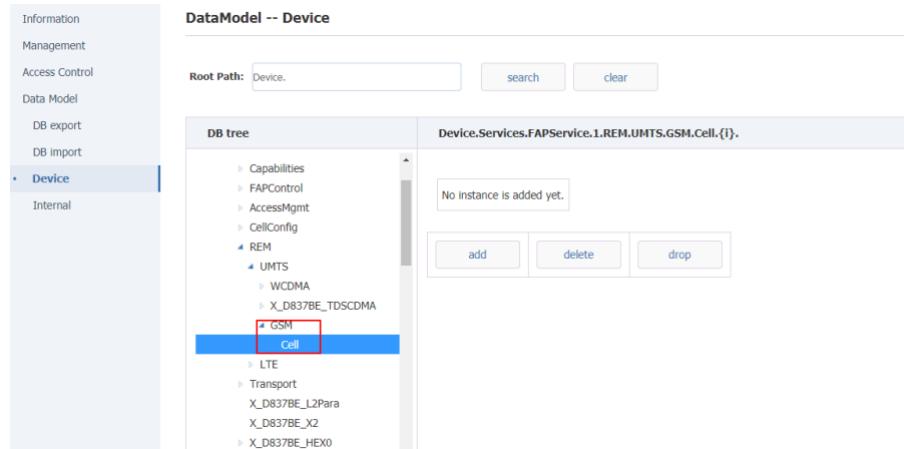


Figure 4-40gsm cell scan results

4) Add GSM neighbor through air port listening.

The neighbor discovered through the air port listening mode will be added to the neighbor list of the base station.

Data model path:

Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborListInUse.InterRACTCell.GSM.



note:

Some scanned cells are not added to the GSM neighborhood table of the base station due to weak RSSI of the scanned cells. In this case, these cells can be added to the neighborhood table by properly adjusting the threshold value, as shown in table 4-17.

Data model path:

Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam.GERANSnifferRSSIThresholdForANR

| Parameter name | Value range | explain |
|---------------------------------|-------------|--|
| GERANSnifferRSSIThresholdForANR | [-110:48] | The RSSI threshold that GSM adjacent cell scanned can be used as neighbor cell . The default value is - 95, which can be adjusted according to the actual environment. |

surface4-17 The threshold that BS add a scanned cell to the neighbor list

4.4.1.2Manually configure adjacent area

When you manually configure the neighbor cell, you need to configure the candidate neighbor cell list and enable the corresponding neighbor cell; the

enabled neighbor cell information will be added to the neighbor cell relationship table of the base station as an effective neighbor cell.

1. Manual configuration of neighborhood is achieved by setting the list of neighborhood.

Data model path:

`Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList`.

2. The enabled neighbor in the neighbor list will be added to the neighbor relationship table of the base station.

Data model path:

`Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborListInUse`.

(1) Manually configure LTE neighborhood

- 1) Manually configure the neighbor list;

Data model path:

`Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList`.

Figure 4-41 manually adding LTE neighborhood

- 2) After setting the LTE neighbor information, select "submit" to submit;

- 3) See table 4-18 for main parameters.

| Parameter name | explain |
|----------------|--|
| The Enable | Adjacent enable switch 0: invalid neighborhood;1: effective neighborhood |
| Alias | Keep the default |
| MustInclude | Whether to include the neighbor table switch 0: not added to neighborhood relational table;1: is added to the neighborhood relationship table |
| PLMNID | Adjacent regions PLMN ID |

| Parameter name | explain |
|----------------------------------|--|
| CID | Neighborhood community ID, <ul style="list-style-type: none">• When the neighborhood type is Home, the length is 28 bits• When the neighborhood type is Marco, the length is 20 bits (that is, eNodeB ID) |
| EUTRACarrierARFCN | Neighborhood absolute frequency |
| PhyCellID | Adjacent regions PCI |
| QOffset | Neighborhood migration, Idle mode cell re - selection, the larger the easier to re - selection to this cell |
| The CIO | Neighborhood offset, connection mode cell switching, the larger the easier to switch to this cell |
| RSTxPower | Reference signal power of adjacent region |
| Blacklisted | Turns off by default. If enabled, this neighborhood will not be a switching target for UE |
| TAC | Adjacent regions TAC |
| EnbType | 0: macro station, 1: small station |
| X_18396E_NoRemove | Disabled by default. If enabled, this neighborhood will not be automatically removed from the InUse list |
| X_18396E_NoX2 | Default off. <ul style="list-style-type: none">• If enabled, the base station will not establish an X2 connection with this neighborhood |
| X_18396E_NoX2HO | Default off. <ul style="list-style-type: none">• If enabled, the base station will not be switched with the adjacent area via the X2 interface |
| X_18396E_AccessMode | Neighborhood Access mode, default is Open Access |
| X_18396E_CSGID | CSG ID of adjacent area, default does not need to be filled in |
| X_18396E_BlacklistedSIB | This is turned off by default, corresponding to BlackCellList in SIB4 or 5 |
| X_18396E_AntennaPortsCount | Number of adjacent antenna ports |
| X_18396E_DLBandwidth | Adjacent downlink bandwidth |
| X_18396E_SubFrameAssignment | Neighborhood sub-frame ratio |
| X_18396E_SpecialSubframePatterns | Neighborhood special subframe mode |

surface4-18 LTE adjacent area parameter configuration description

(2) Manual configuration of 3G adjacent area

1) Manual configuration of 3G neighbor list

Data model path:

Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.InterRATCell.UMTS.

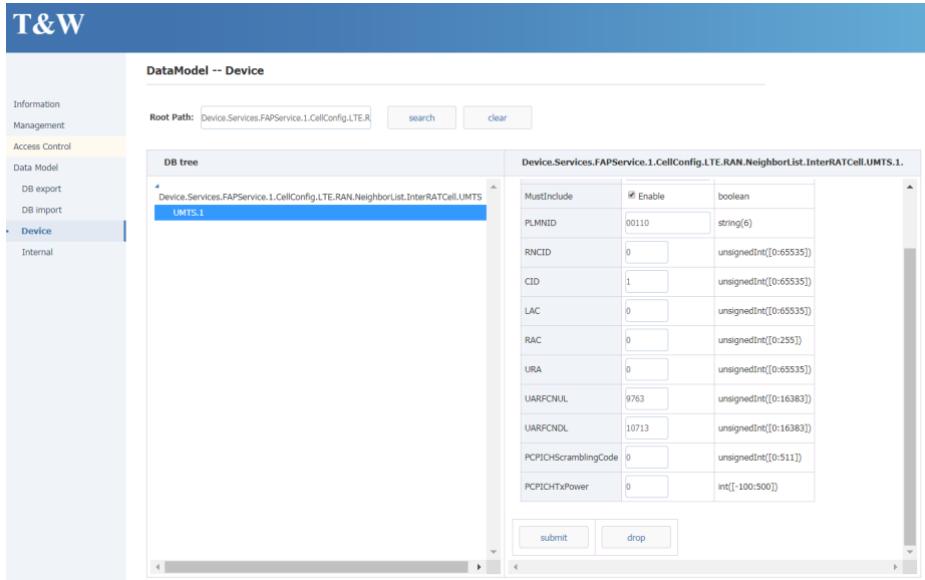


Figure 4-42 add 3G neighbor manually

2) Select "submit" to submit after setting 3G neighborhood information;

3) See table 4-19 below for the description of main parameters.

| Parameter name | explain |
|----------------------|--|
| Enable | Item enable switch, enable required |
| Alias | Keep default |
| MustInclude | Mandatory include switch, enable required |
| PLMNID | Adjacent PLMN ID |
| RNCID | Neighbor RNC ID |
| Parameter name | explain |
| CID | Neighborhood C-ID |
| LAC | Lac of adjacent area |
| RAC | Adjacent area RAC |
| URA | Neighborhood URA |
| UARFCNUL | Uplink frequency point |
| UARFCNDL | Downlink frequency point |
| PCPICHScramblingCode | Scrambling code |
| PCPICHTxPower | Pcpich transmit power, multiplied by 0.1 is the actual value, in dBm |

surface4-19 UMTS adjacent area parameter configuration description

(3) Manually configure GSM neighborhood

1) Manual configuration of GSM neighbor list

Data model path:

Device.Services.FAPService.1.CellConfig.LTE.RAN.NeighborList.InterRATCell.GSM.

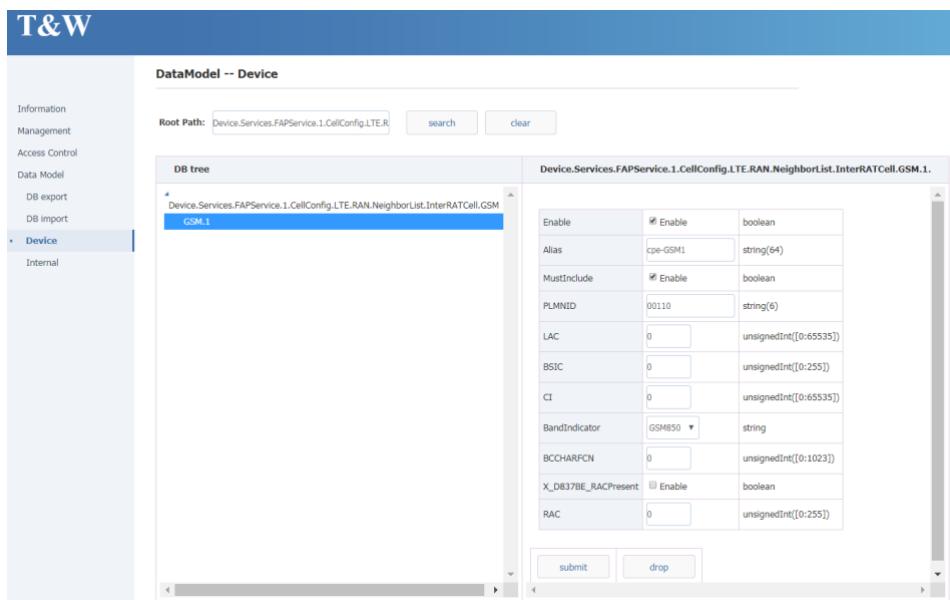


Figure 4-43 manual addition of GSM neighborhood

2) Select "submit" to submit after setting the adjacent area information of GSM;

3) See table 4-20 for main parameters.

| Parameter name | explain |
|----------------|---|
| Enable | Item enable switch, enable required |
| Alias | Keep default |
| MustInclude | Mandatory include switch, enable required |
| PLMNID | Adjacent PLMN ID |
| LAC | Lac of adjacent area |
| BSIC | Bit 7:6 - not used ("00") Bit 5:3 - NCC (PLMN Color Code) Bit 2:0 - BCC (BS color code) |
| CI | Cell ID of adjacent area |
| BandIndicator | Adjacent band indication |
| Parameter name | explain |
| BCCHARFCN | Adjacent frequency point |
| RAC | Adjacent area RAC |

surface4-20 GSM adjacent area parameter configuration description

4.4.2 Configure mobility parameters

1. The base station handover decision mainly uses the following events:

A1 event: indicates that the signal quality of the service community is higher than a certain threshold. When UE reports this event, the base station stops the measurement of different frequency/different system;

A2 event: indicates that the signal quality of the service community is below a certain threshold. When UE reports this event, the base station starts the measurement of different frequency/different system.

A3 event: indicates that the quality of the same frequency/different frequency neighborhood is higher than that of the service community. When UE reports this event, the base station initiates the same frequency/different frequency switching request.

B1 event: indicates that the quality of the neighboring area of the different system is higher than a certain threshold. When UE reports this event, the base station starts the eSRVCC switching request based on the uplinking service quality.

B2 event: it means that the quality of the service community is below a certain threshold and the quality of the neighboring area of the different system is above a certain threshold. When UE reports this event, the base station initiates the overcover-based eSRVCC switching request.

2. The data model configuration item corresponding to the above events is:

Device. Services. FAPService. 1. CellConfig. LTE. RAN. Mobility. ConnMode. EUTRA.
A1MeasureCtrl

Device. Services. FAPService. 1. CellConfig. LTE. RAN. Mobility. ConnMode. EUTRA.
A2MeasureCtrl

Device. Services. FAPService. 1. CellConfig. LTE. RAN. Mobility. ConnMode. EUTRA.
A3MeasureCtrl

Device. Services. FAPService. 1. CellConfig. LTE. RAN. Mobility. ConnMode. IRAT.
B1MeasureCtrl

Device. Services. FAPService. 1. CellConfig. LTE. RAN. Mobility. ConnMode. IRAT.
B2MeasureCtrl

Date model path:

Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.A1MeasureCtrl
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.A2MeasureCtrl
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.A3MeasureCtrl
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.IRAT.B1MeasureCtrl
Device.Services.FAPService.1.CellConfig.LTE.RAN.Mobility.ConnMode.IRAT.B2MeasureCtrl

4.4.2.1 Start inter frequency / inter system measurement

1. The measurement of the different frequency / different system is triggered by the A2 event, as shown in figure 4-44. There are 11 groups of A2 events in total, which need to be focused on 1 to 7, which are respectively used in different scenarios:

A2measurerctr1: different frequency measurement
A2measurectrl. 2: 3G measurement (LTE data service exists)
A2measurectrl.3: 2G measurement (LTE data service exists)
A2measurectrl. 4: 3G blind handover

- A2measurectrl.5: 2G blind handover
A2measurectrl.6: 3G measurement (LTE voice service exists)
A2measurectrl.7: 2G measurement (LTE voice service exists)

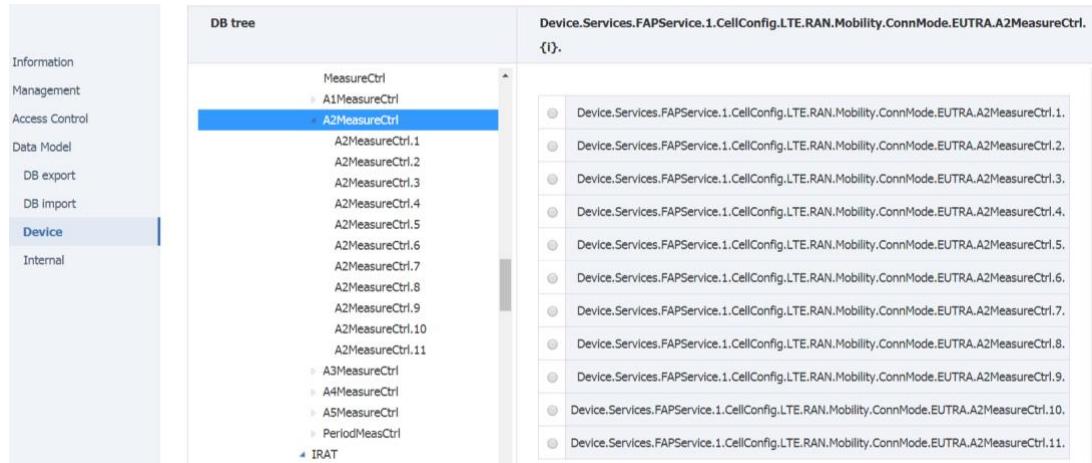


Figure 4-44 A2 event

2. Regarding the parameter configuration of A2 event, take the common inter frequency measurement scenario as an example.

A2 event will be triggered when UE's measurement results of primary plot are less than a2thresholdrsrp-hysteresis (both are actual converted values, as shown in figure 4-45, 45-140-2*0.5=-96 dBm) and are maintained longer than TimeToTrigger, and report continuously with ReportInterval.**Error! Reference source not found.** See table 311 for parameter description.

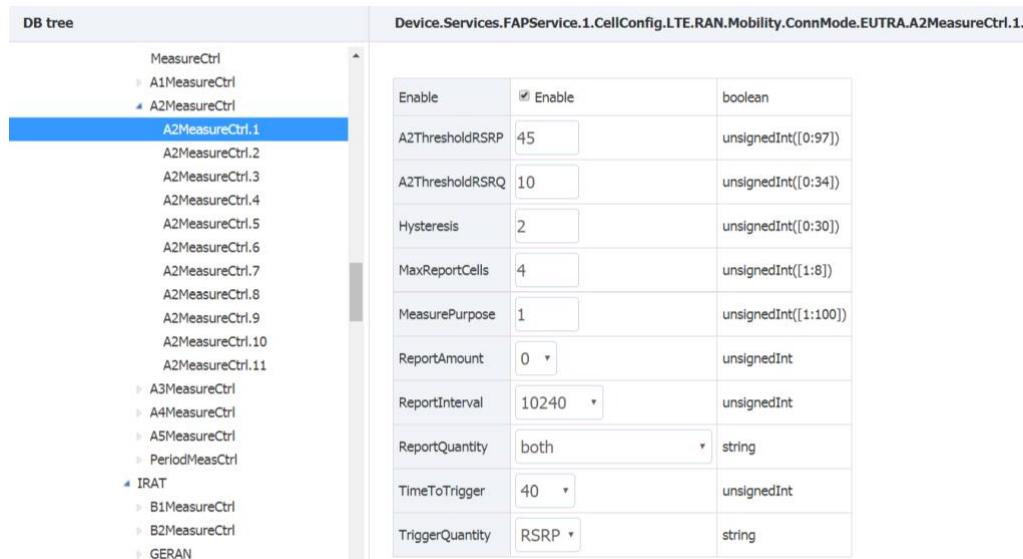


Figure 4-45 A2 event parameters

| Parameter name | explain |
|----------------|---------|
| The Enable | |

| | |
|-----------------|--|
| A2ThresholdRSRP | A2 RSRP trigger threshold, after subtracting 140, is the actual value (in dBm) |
| A2ThresholdRSRQ | |
| Hysteresis | Trigger hysteresis, multiplied by 0.5, is the actual value (in unit dB) |
| MaxReportCells | |
| MeasurePurpose | |
| ReportAmount | Number of reports, 0 is infinite |
| ReportInterval | Report interval, unit ms |
| ReportQuantity | Report the amount |
| Parameter name | explain |
| TimeToTrigger | Trigger time , unit ms |
| TriggerQuantity | Trigger quantity, rsrp by default |

surface4-21 A2 event configuration description

4.4.2.2 Stop the measurement of inter frequency / intra system

1. The BTS stops the measurement of inter frequency / inter system by triggering A1 event, as shown in Figure 4-46. There are 11 groups of A1 events in total, which need to be focused on 1 to 5, respectively for different scenarios:

A1measurectrl. 1: inter frequency measurement
 A1measurectrl. 2: 3G measurement (LTE data service exists)
 A1measurectrl.3: 2G measurement (LTE data service exists)
 A1measurectrl.4: 3G measurement (with LTE voice service)
 A1measurectrl.5: 2G measurement (LTE voice service exists)

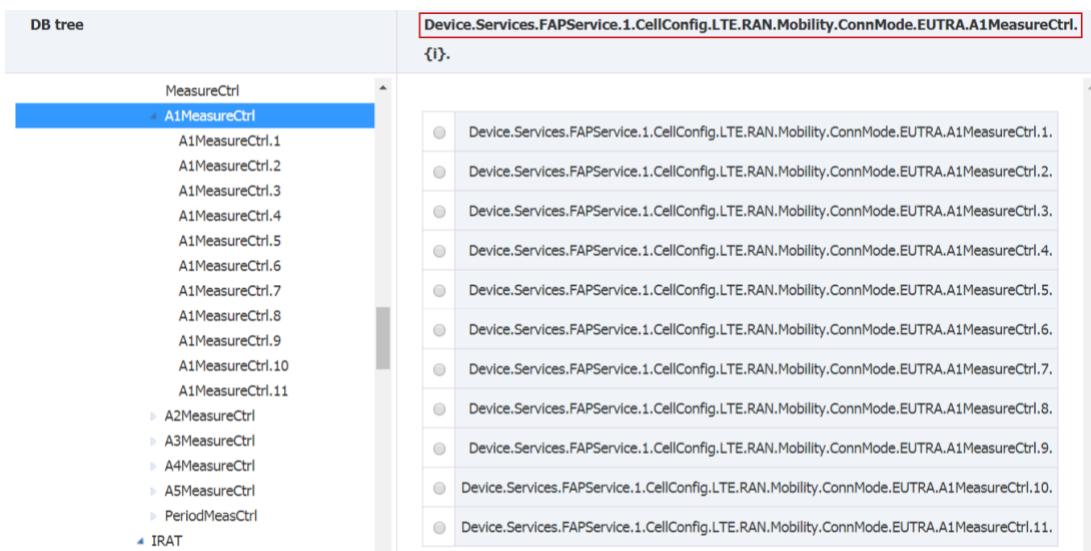


Figure 4-46 event A1

2. For the parameter configuration of A1 event, take the commonly used scene of inter frequency measurement as an example.

When the measurement result of UE to the server cell is greater than A1 thresholdrsrp + hysteresis (both are converted actual values, take figure 4-47 as an example, $55 - 140 + 2 * 0.5 = -84$ dBm), and the maintain time is greater than timetotrigger, A1 event will be triggered, and the A1 report will be continuously reported at the interval of reportinterval. See table 4-22 for parameter description.

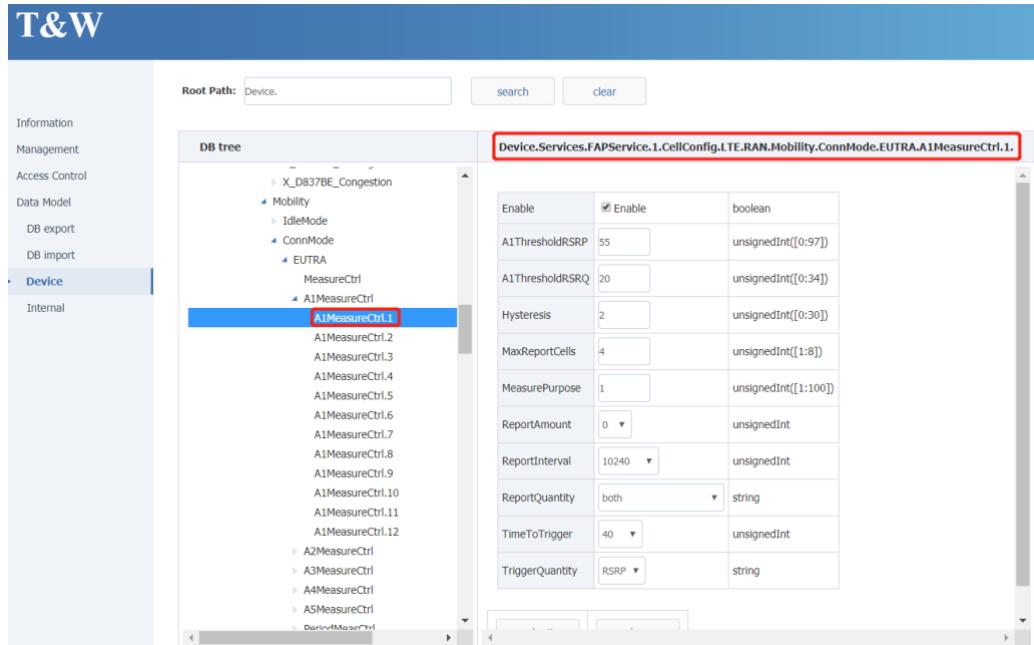


Figure 4-47 A1 event parameters

| Parameter name | explain |
|-----------------|--|
| The Enable | |
| A1ThresholdRSRP | A1 RSRP trigger threshold, which is the actual value (in dBm) after subtraction of 140 |
| A1ThresholdRSRQ | |
| Hysteresis | Trigger hysteresis, multiplied by 0.5, is the actual value (in unit dB) |
| MaxReportCells | |
| MeasurePurpose | |
| ReportAmount | Number of reports, 0 is infinite |
| ReportInterval | Report interval, in ms |
| ReportQuantity | Report the amount |
| TimeToTrigger | Trigger time in ms |
| TriggerQuantity | Trigger, default to RSRP |

表 4-22 A1 事件配置说明

 note:

Note: `a2thresholdrsrp-hysteresis` should be lower than `a1thresholdrsrp-hysteresis`, otherwise UE will repeatedly report A1, A2 events. .

4.4.2.3LTE intra/inter frequency handover

1. LTE same-frequency/different-frequency switching is triggered by A3 events. As shown in figure 4-48, there are two groups of configurations of A3 events, which are used in different scenarios:

A3MeasureCtrl.1: measurement of same frequency

A3MeasureCtrl.2: measurement of different frequencies

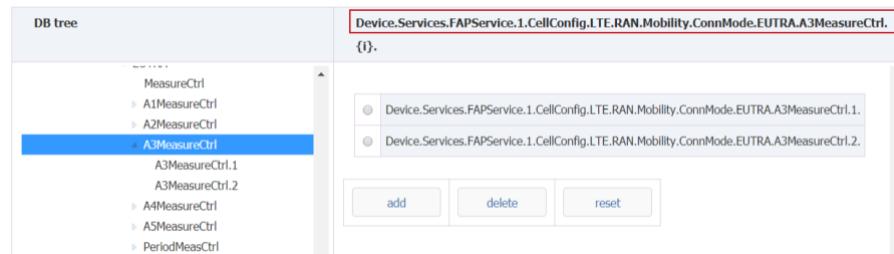


Figure 4-48 A3 event

2. The trigger condition of A3 is: where Mn and Mp are the measurement results of UE on adjacent area and main area respectively, Ofn and Ofp are frequency offset of adjacent area and main area respectively (default is 0), Ocn and Ocp are offset of adjacent area and main area respectively (default is 0), Off is A3Offset, Hys is Hysteresis. $Mn + Ofn + Ocn - Hys > Mp + Ofp + Ocp + Off$ Therefore, when the measurement results of UE on the adjacent area are larger than A3Offset + Hysteresis when compared with the main plot (both are actual values after conversion, as shown in FIG. 4-43, $4*0.5+2*0.5=3\text{dB}$) and the maintenance time is longer than TimeToTrigger, A3 events will be triggered and report continuously with ReportInterval as interval.**Error! Reference source not found.** See table 313 for parameter description.

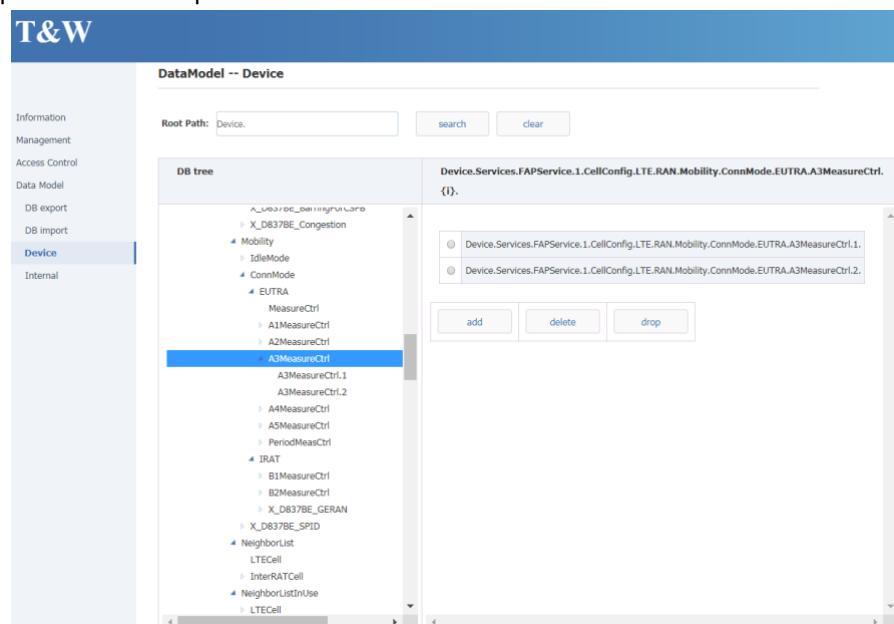


Figure 4-49 A3 event parameters

| 参数名称 | 说明 |
|----------------|---|
| The Enable | |
| A3Offset | A3 offset, multiplied by 0.5, is the actual value (in dB). |
| Hysteresis | Trigger hysteresis, multiplied by 0.5, is the actual value (in unit dB) |
| MaxReportCells | |
| MeasurePurpose | |
| ReportAmount | Number of reports, 0 is infinite |
| ReportOnLeave | |
| ReportInterval | Report interval, in ms |
| ReportQuantity | Report the amount |
| TimeToTrigger | Trigger time in ms |

table4-23 A3 event

4.2.3 SONRelated configuration

The son function parameters are located in the following nodes:

Device.Services.FAPService.1.FAPControl.LTE.SelfConfig.SONConfigParam.

Please refer to table 4-24 for parameter descriptions.

| Parameter name | Value range | explain |
|--------------------------|--|--|
| SONSysMode | Distributed Centralized | Son system mode |
| SONWorkMode | Free Control | Son mode setting |
| PCIOptEnable | - | PCI self optimization algorithm switch |
| PCIReconfigWaitTime | - | PCI reset wait timer |
| CandidateARFCNList | 64[0:262143] | List of candidate frequency points |
| CandidatePCIList | 64[0:503] | Candidate PCI list |
| ANREnable | - | Anr algorithm main switch |
| ANRInterFreqEnable | - | E-utran different frequency ANR algorithm switch |
| ANRGERANEnable | - | Geran different system ANR algorithm switch |
| ANRUTRANEnable | - | UTRAN differentsystem ANR algorithm switch |
| ARFCNEnable | - | Frequency point self configuration algorithm switch |
| MaxLTENeighbourCellNum | - | Maximum number of LTE neighbors |
| MaxUTRANNeighbourCellNum | - | Maximum number of UTRAN neighbors |
| MaxGRANNeighbourCellNum | - | Maximum number of Gen neighbors |
| ReSynCellEnable | - | Resynchronize cell enable switch |
| PowerEnable | - | Power self configuration algorithm switch |
| RootSeqConfigEnable | - | Root sequence self configuration switch |
| PRACHConfigEnable | - | PRACH index self configuration switch |
| LTESnifferFreqBandList | 64 | LTE listening band list |
| LTESnifferChannelList | 64 | LTE listening frequency list |
| GERANSnifferEnable | - | GERAN listen enable |
| GERANSnifferChannelList | 256 | GERAN listen channel number list |
| UTRANSnifferEnable | - | UTRAN listening enable |
| UTRANSnifferChannelList | 256 | UTRAN listening channel number list |
| MROEnable | - | Neighborhood robust optimization function switch |
| SHEnable | - | Self healing function switch |
| SyncMode | GNSS IEEE1588V2 Sniffer Freedom | Clock synchronization mode, this parameter is read-only permission |
| PeriodicSnifferInterval | - | Cycle listening interval, 0 means cycle listening is off |

| | | |
|---|------------|--|
| SnifferForANREnable | - | Neighborhood self-discovery function switch based on air port interception. (default enable) |
| SnifferForMeasurementEnable | - | Frequency point self-measurement function switch based on air port interception. (default enable) |
| LTESnifferRSRPThresholdForANR | [-140:-44] | The RPSR threshold that LTE adjacent cell scanned can be used as neighbor cell . The default value is - 95, which can be adjusted according to the actual environment. |
| LTESnifferRSRPThresholdForMeasurement | [-140:-44] | The LTE neighbor scanned can be used as the rsrp threshold of the measurement object |
| UTRANSnifferRSCPThresholdForANR | [-120:-25] | The scanned UTRAN neighborhood can be used as the RSCP threshold of the base station neighborhood |
| UTRANSnifferRSCPThresholdForMeasurement | [-120:-25] | The scanned UTRAN neighborhood can be used as the RSCP threshold of the base station measurement object |
| GERANSnifferRSSIThresholdForANR | [-110:48] | The scanned adjacent area of the gen can be used as the RSSI threshold of the adjacent area of the base station |
| GERANSnifferRSSIThresholdForMeasurement | [-110:48] | The scanned adjacent area of the gen can be used as the RSSI threshold of the base station measurement object |
| MLBEnable | - | Mobile load balancing switch |
| MLBTimerLength | - | Mobile load balancing timer duration |
| MLBThreshold | [0:100] | Mobility load balancing threshold, in% |
| MLBUEProtectTimerLength | - | Mobile load balancing UE protection timer duration |
| MLBUEHysteresisOffset | [0:30] | Mobility load balancing UE hysteresis offset |

| | | |
|----------------------|---------|---|
| ReduceRspTimerLength | [1:255] | When a cell is deleted, the timer duration of the cell reference signal power is reduced. The purpose is to reduce the power of cell reference signal and let UE switch out. This function is not used at present |
| ReduceRspTimes | [0:255] | Number of times to reduce cell reference power, 0 means disabled |
| ReduceRspStep | [1:255] | Step to reduce cell reference power, DB |

surface4-24 son parameter configuration description



note:
In general, these parameters do not need to be changed. Please keep the default value except for the parameters related to neighbor listening.

4.5Configure system parameters

4.5.1Software version upgrade

Select "management" upgrade in the navigation bar to enter the version upgrade page, as shown in figure 4-50.

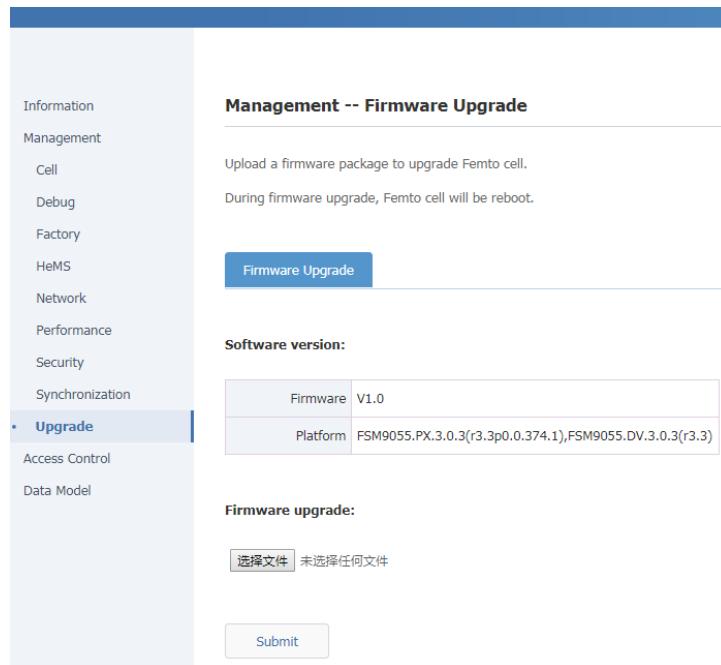


chart4-50Version upgrade

Software upgrade steps:

1. Click Select file, select upgrade file and upload to base station.
2. Click submit to upgrade.

3. The base station is restarted and upgraded, waiting for about 3-5min. After the upgrade is successful, the page will prompt accordingly.
4. The upgraded version can be confirmed through the "information" page.

4.5.2 System file backup

4.5.2.1 Import / export profile

1. Select "data model" in the navigation bar to enter the DB import / export page, as shown in figure 4-51

| Current DB Files | |
|------------------|--------|
| Device.xml | Export |
| Internal.xml | Export |
| SON_DM.xml | Export |

Figure 4-51 profile export and import

2. Export / import is used to export and import configuration files.

4.5.2.2 Export log file

1. Select "management debug" in the navigation bar to enter the log operation interface, as shown in figure 4-52.

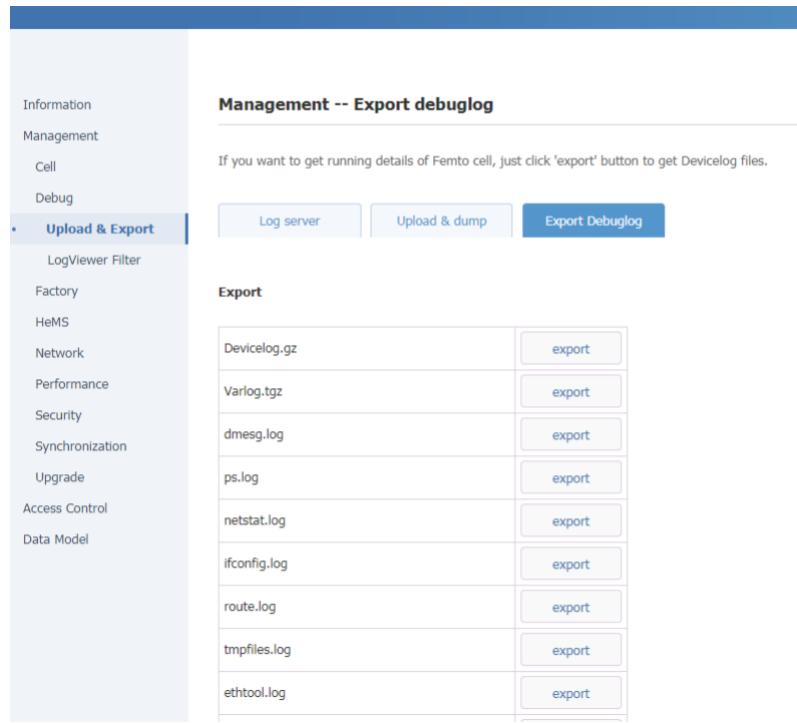


Figure 4-52 export log file

2. Select the log you want to export, and click export.
3. Select the save path in the pop-up download dialog box to save the log file locally.

4.6 Restart base station

1. In the navigation bar, select "management->factory".
2. Click "reboot" to restart the base station.
3. It usually takes 3-5 minutes for the base station to restart.

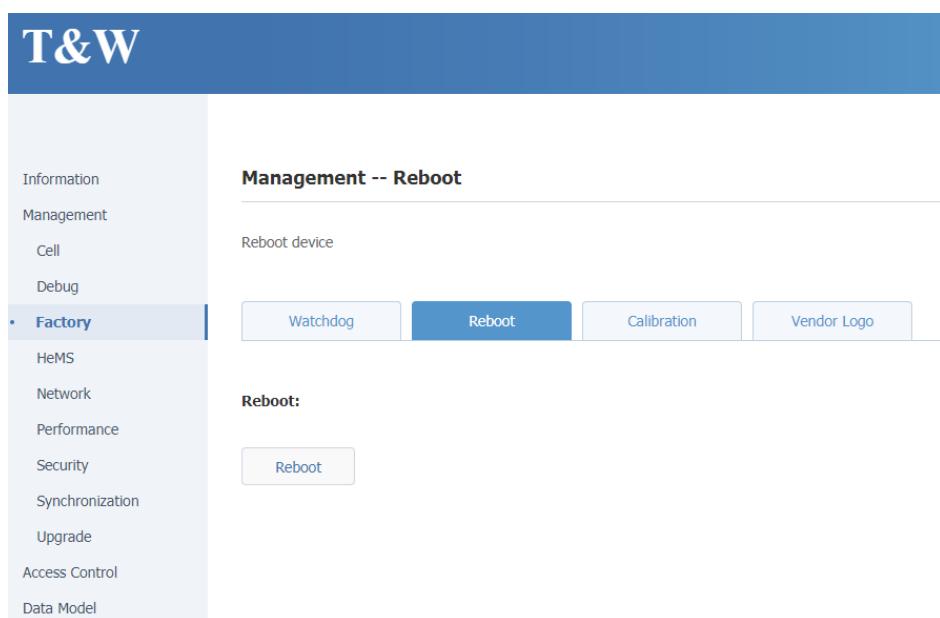


Figure 4-53 device restart