Bridgestone P4 SA User Guide

Version: v1.9
Date: 2023/04/03

Copyright © 2022 Mosolabs. All Rights Reserved. Mosolabs reserves the right to make changes to this document without notice. Mosolabs makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose. Mosolabs assumes no liability arising out of the application or use of any product or circuit. Mosolabs specifically disclaims all liability, including without limitation consequential or incidental damages; neither does it convey any license under its patent rights, nor the rights of others.
<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>2022/7/7</td>
<td>Initial Release V 1.0</td>
<td>DG5605@2209062255</td>
</tr>
</tbody>
</table>
| V1.1 | 2022/7/29| 1. Add backup & restore configuration setting  
2. Add O1 management setting  
3. Add inter-frequency HO setting  
4. Add customize upgrade setting | DG5605@2209062255 |
| V1.2 | 2022/8/3 | 1. Add IPv6 static setting&Replace CenterFreq with Arfcn                  | DG5605@2209062255 |
| V1.3 | 2022/9/6 | 1. Add CLI support                                                           | DG5605@2209281146 |
| V1.4 | 2022/10/10| 1. Support log download by CLI  
2. Add multi-vlan setting  
3. Add CU DU log setting | DG5606@2210281802 |
| V1.5 | 2022/12/1| 1. Sync enable setting update  
2. Update use SSB Arfcn instead of FreqSsb                          | DG5606@2212021733 |
| V1.6 | 2022/12/5| 1. SecGW server setting update                                             | DG5606@2212021733 |
| V1.7 | 2022/12/30| 1. Add multi-amf address on 5GC Page  
2. Add PTP Page to Status Page                                         | DG5606@2301112306 |
| V1.8 | 2023/03/08| 1. Update the snapshots for intra and inter neighbor cells in chapter 5.6 &5.7 | DG5606@2303062212 |
| V1.9 | 2023/03/29|                                                                              |                  |
Index

1. Device Descriptions .......................................................................................................................... 6
   1.1. Basic Descriptions .......................................................................................................................... 6
   1.2. Port Descriptions .......................................................................................................................... 6

2. Network Topology ................................................................................................................................... 7
   2.1. Common Network .......................................................................................................................... 7
   2.2. Add NTP Server ............................................................................................................................... 7
   2.3. Add Synchronization Source ......................................................................................................... 8
       2.3.1. GPS Sync ................................................................................................................................. 8
       2.3.2. PTP Sync ................................................................................................................................. 9
   2.4. Add SeGW ..................................................................................................................................... 10
   2.5. Add HeMS .................................................................................................................................. 10
   2.6. Add SAS Server ............................................................................................................................ 11

3. How to Access Bridgestone .................................................................................................................. 12
   3.1. Web GUI Login ............................................................................................................................... 13
   3.2. CLI ................................................................................................................................................ 14
   3.3. Trouble Shooting ........................................................................................................................... 14

4. Basic Setting ......................................................................................................................................... 14
   4.1. WAN Setting .................................................................................................................................. 15
       4.1.1. Configuration ........................................................................................................................... 15
       4.1.2. Trouble Shooting .................................................................................................................... 27
   4.2. 5GC Setting .................................................................................................................................. 28
   4.3. NR Cell Setting ............................................................................................................................... 30
       4.3.1. Center Arfcn and SSB Arfcn Setting ....................................................................................... 31
   4.4. Trouble Shooting ........................................................................................................................... 34

5. Advance Setting .................................................................................................................................... 34
   5.1. NTP Server Setting .......................................................................................................................... 34
       5.1.1. Configuration ........................................................................................................................... 34
       5.1.2. Success Log .............................................................................................................................. 35
       5.1.3. Trouble Shooting .................................................................................................................... 35
   5.2. Sync Type Setting ............................................................................................................................ 36
       5.2.1. Free Running ............................................................................................................................ 36
       5.2.2. Sync ....................................................................................................................................... 37
       5.2.3. PTP Sync .................................................................................................................................. 39
   5.3. SecGW Server Setting ...................................................................................................................... 41
       5.3.1. PSK Authentication .................................................................................................................. 41
       5.3.2. Cert Authentication ............................................................................................................... 44
   5.4. CMPv2 Server Setting ..................................................................................................................... 46
   5.5. HeMS Server Setting ....................................................................................................................... 47
9.15. Show GPS Sync Status ................................................................................................... 74
9.16. Show OAM(YANG) parameters .................................................................................. 75
9.17. Set OAM(YANG) parameters .................................................................................... 75
9.18. Support Download Log ............................................................................................. 75
9.19. Support Factory Default .......................................................................................... 77
9.20. Support Quit .............................................................................................................. 77
9.21. Support Firmware Version Upgrade ......................................................................... 77
9.22. Support ping command ............................................................................................ 78
9.23. Support ip command ................................................................................................. 78
9.24. Support traceroute command .................................................................................... 79
9.25. Support date command ............................................................................................ 79
9.27. Support rma command ............................................................................................. 80
   9.27.1 rma get all ........................................................................................................... 80
   9.27.2 rma get reboot_cause ....................................................................................... 81
   9.27.3 rma get led .......................................................................................................... 82
   9.27.4 rma get secgw ..................................................................................................... 83
   9.27.5 rma get ue_info .................................................................................................. 83
   9.27.6 rma get cert ......................................................................................................... 83
   9.27.7 rma get meminfo ............................................................................................... 84
   9.27.8 rma get flashinfo ............................................................................................... 85
9.28. Support show du stats command ............................................................................. 86
10. Diagnostic ...................................................................................................................... 86
   10.1. Cell Setup ............................................................................................................... 86
   10.2. Common Issues ....................................................................................................... 86
1. Device Descriptions

1.1. Basic Descriptions

Bridgestone supports n78/n48 SA mode.

Tips. n48 depends on the calibration, please follow the device spec.

1.2. Port Descriptions

Bridgestone has 6 ports: DC, ETH1, ETH2, SFP, 1PPS, GPS. The function for them shows as below table.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC</td>
<td>Power port</td>
</tr>
<tr>
<td>ETH2</td>
<td>WAN port</td>
</tr>
<tr>
<td>ETH1</td>
<td>LAN port (console port)</td>
</tr>
<tr>
<td>SFP</td>
<td>Reserved</td>
</tr>
<tr>
<td>1PPS</td>
<td>Export 1PPS signal</td>
</tr>
<tr>
<td>GPS</td>
<td>Connect to GPS antenna, use for GPS sync</td>
</tr>
</tbody>
</table>
2. Network Topology

2.1. Common Network

This topology includes 5GC, SmallCell, switch and UEs, shows as below figure.

Using this topology only need to enable WAN progress and NR progress. Please refer to chapter 4 “Basic Setting” and chapter 5.2.1 “Free Running” to configure Bridgestone.

2.2. Add NTP Server

This topology includes 5GC, SmallCell, NTP Server, switch and UEs, shows as below figure.
Using this topology need to enable WAN progress, NTP progress and NR progress. Please refer to chapter 4 “Basic Setting”, 5.1 “NTP Server Setting” and 5.2.1 “Free Running” to configure Bridgestone.

2.3. Add Synchronization Source

Currently, Bridgestone P4V2 only support one of them (GPS sync or PTP sync). Which one to be used, please follow the spec.

2.3.1. GPS Sync

This topology includes 5GC, SmallCell, GPS, switch and UEs, shows as below figure.
Using this topology need to enable WAN progress, GPS_SYNC progress and NR progress. Please refer to chapter 4 “Basic Setting” and 5.2.2 "GPS Sync" to configure Bridgestone.

2.3.2. PTP Sync

This topology includes 5GC, SmallCell, PTP server, switch and UEs, shows as below figure.

Using this topology need to enable WAN progress, GPS_SYNC progress and NR progress.
Please refer to chapter 4 “Basic Setting” and 5.2.3 "PTP Sync" to configure Bridgestone.
2.4. Add SeGW

This topology includes 5GC, SmallCell, SeGW, switch and UEs, shows as below figure.

Using this topology need to enable WAN progress, SSEGW progress and NR progress. Please refer to chapter 4 “Basic Setting”, 5.2.1 “Free Running” and 5.3 “SecGW Server Setting” to configure Bridgestone.

2.5. Add HeMS

This topology includes 5GC, SmallCell, HeMS, switch and UEs, shows as below figure.
Using this topology need to enable WAN progress, S_HEMS progress and NR progress. Please refer to chapter 4 “Basic Setting”, 5.2.1 “Free Running” and 5.4 “HeMS Server Setting” to configure Bridgestone.

2.6. Add SAS Server

This topology includes 5GC, SmallCell, SAS Server, switch and UEs, shows as below figure.
Using this topology need to enable WAN progress and NR progress. Please refer to chapter 4 “Basic Setting”, 5.2.1 “Free Running” and 5.6 “SAS Setting” to configure Bridgestone.

3. How to Access Bridgestone

Bridgestone supports using ETH1/ETH2 port for local access.

- ETH1(LAN) port for local access
  The access address by using LAN port is 10.10.10.189.
  Connecting laptop to LAN port and using static IPv4 address (10.10.10.xxx) for laptop, then laptop can visit 10.10.10.189 to access Bridgestone.

- LTE2(WAN) port for access
  The access address by using WAN port is WAN IPv4 address or the IPv6 link-local address of Bridgestone. IPv6 link-local can be calculated from MAC address, for example:
  
<table>
<thead>
<tr>
<th>MAC</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>E42686FD6A60</td>
<td>fe80::e626:86ff:fed6:6a60</td>
</tr>
<tr>
<td>E42686FD6A63</td>
<td>fe80::e626:86ff:fed6:6a63</td>
</tr>
<tr>
<td>E42686FD6A66</td>
<td>fe80::e626:86ff:fed6:6a60</td>
</tr>
</tbody>
</table>
Laptop and WAN port are connected to the same router, laptop uses the address.
(Allocated by router or configured static IPv6 address) on the same network segment
as Bridgestone WAN IPv4 address or the IPv6 link-local address. Then the laptop can
visit Bridgestone WAN IPv4 address or Bridgestone IPv6 link-local address to access
Bridgestone.

3.1. Web GUI Login

You can login the Bridgestone GUI on the browser by the URL: https://10.10.10.189 or
https://WAN IPv4 address or https://[Bridgestone IPv6 link-local address] (which depends on what
accessing mode you used). Also the account/password can be got form Sercomm.
3.2. CLI

Bridgestone also support sending command via CLI. Please SSH the Bridgestone by the IP: 10.10.10.189 or WAN IPv4 address or Bridgestone IPv6 link-local address (which depends on what accessing mode you used). The account/password can reference to chapter 3.1.

3.3. Trouble Shooting

Please check your laptop IP address setting, also please check the connection between your laptop and Bridgestone. Make sure all of them are correct.

4. Basic Setting

Before setting, please make sure only WAN progress and NR progress are on.
Please follow below method to confirm it.

- Enter CLI;
- Send “son statem status” to check provision progress status;
- Send “son statem off xxx” to disable unneeded provision progress, for example “son statem off S_SEGW” to disable S_SEGW progress;
- apply

4.1. WAN Setting

Bridgestone support 2 WAN mode.
- DHCP: Base on RFC 2131.
- Static IP: User can set a IP address, subnet mask, default gateway, and DNS server manually.

4.1.1. Configuration

Please go through “Setting” -> “WAN” to configuring.
(1) The default setting for Bridgestone is DHCP and non VLAN.

(2) If you need to enable VLAN, please enable VLAN and apply.
4.1.1.2. DHCP IPv6

(1) If you need to configure DHCPv6, please change “IPv6 Connection Type” to “IPv6 DHCP” or “IPv6 Auto”, then you need set IPv6 Enable to “1”. The default setting for Bridgestone is non VLAN.

After configuring all the parameters, please click apply and reboot Bridgestone.

* IPv6 DHCP corresponds Stateful IPv6
* IPv6 Auto corresponds Stateless IPv6

(2) If you need to enable VLAN, please enable VLAN and apply.
4.1.1.3. Static IPv4

(1) Please change “IPv4 Connection Type” to “Static”, then you can set IP address, subnet mask, default gateway, and DNS server manually. The default setting for Bridgestone is non VLAN.

After configuring all the parameters, please click apply and reboot Bridgestone.
(2) If you need to enable VLAN, please enable VLAN and apply. After configuring all the parameters, please click apply and reboot Bridgestone.
### WAN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Port</td>
<td>1G</td>
</tr>
<tr>
<td>IPv4 Connection Type</td>
<td>Static</td>
</tr>
<tr>
<td>IPv6 Connection Type</td>
<td>IPv6 Static</td>
</tr>
<tr>
<td>MTU</td>
<td>1448</td>
</tr>
<tr>
<td>IPv6 Enable</td>
<td>0</td>
</tr>
</tbody>
</table>

### VLAN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable VLAN</td>
<td></td>
</tr>
<tr>
<td>VLAN ID</td>
<td>200</td>
</tr>
</tbody>
</table>

#### Static

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.41.6.17</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

#### IPv6 Static

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td></td>
</tr>
<tr>
<td>IPv6 Prefix Len</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Gateway</td>
<td></td>
</tr>
</tbody>
</table>
4.1.1.4. Static IPv6

(1) Please change “IPv6 Enable” to “1”, then you can set IPv6 address, IPv6 Prefix Len, IPv6 Gateway and DNS server manually. The default setting for Bridgestone is non VLAN.

After configuring all the parameters, please click apply and reboot Bridgestone.
(2) If you need to enable VLAN, please enable VLAN and apply. After configuring all the parameters, please click apply and reboot Bridgestone.
4.1.1.5. Additional Multi-Vlan

(1) Multi-Vlan with DHCP IPv4

If you want to configure multi-vlan, please configure the default VLAN by following the instructions in 4.1.1.1(2), then you can set Additional Vlan List, VlanEnable, VlanId, InterfaceEnable, IPv4Enable and set modify to save the configuration.

After the additional VLAN list is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List.
After configuring all the parameters, please click apply and reboot Bridgestone

(2) Multi-Vlan with Static IPv4

If you want to configure multi-vlan, please configure the default VLAN by following instructions in 4.1.1.2(2), then you can set Additional Vlan List, VlanEnable, VlanId, InterfaceEnable, IPv4Enable, IPv4AddressType, IPv4Address, IPv4SubnetMask, IPv4GateWayAddress and set modify to save configure.

After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List.
After configuring all the parameters, please click apply and reboot Bridgestone

(3) Multi-Vlan with Static IPv6

If you want configure multi-vlan, please configure the default VLAN by following instructions in 4.1.1.3(2), then you can set Additional Vlan List, VlanEnable, VlanId, InterfaceEnable, IPv6Enable, IPv6AddressType, IPv6Address, IPv6PrefixLen, IPv6GateWayAddress and set modify to save configure
After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List

After configuring all the parameters, please click apply and reboot Bridgestone

(4) Multi-Vlan with DHCP IPv6

If you want to configure multi-vlan, please configure the default VLAN by following instructions in 4.1.1.3(2), then you can set Additional Vlan List, VlanEnable, VlanId, InterfaceEnable, IPv6Enable, IPv6AddressType (Only DHCP and AUTO can be configured, DHCP corresponds to Stateful ipv6; AUTO corresponds to Stateless ipv6), set modify to save configure
After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List

After configuring all the parameters, please click apply and reboot Bridgestone

4.1.2. Trouble Shooting

WAN will show green in “Status -> System” page if WAN was connect.
If WAN is not green, please follow below steps to check it.

- Check WAN link light is on;
- Check WAN setting parameters;
- Check DHCP server is working (if using DHCP mode);

4.2. 5GC Setting

Please go through “Setting” -> “5GC” to configuring.

In this page, you need to set PLMN, TAC, AMF address and sNSSAI.
AMF Address can be IPv6 address from this release, but you need configure IPSec first and IPSec tunnel IP is ipv6 address, please refer to IPSec section of "5.3.SecGW Server Setting" for IPSec configuration.

AMF Address can be set to multiple IPs, and each ip need be separated by ",". Do not put a space after "," , this will make the setting not work.
Tips. PLMN, TAC and sNSSAI are decimal. sNSSAI is composed of sST and sD, for example: sST is 0x01, sD is 0x0000001, then sNSSAI is 0x01000001, we must convert 0x01000001 to 16777217, so the value of sNSSAI is 16777217. A total of up to 8 sNSSAI can be configured, and each sNSSAI need be separated by ",".

4.3. NR Cell Setting

Please go through “Setting” -> “NR Cell Configuration” to configuring.
In this page, you can set bandwidth, slot pattern, NR band, gNB ID, PCI, Tx power, absolute Center ARFCN and absolute SSB ARFCN. Please note, NR band must follow device spec.

4.3.1. Center Arfcn and SSB Arfcn Setting

4.3.1.1. Calculate SSB Arfcn

Utilize the below formula to calculate the SSBFreq

\[ N_0 = \frac{(\text{StartFreq} - 3000 + 7.92)}{1.44} \]

\[ N = \text{RoundUptoInter}(N_0) \]

\[ \text{SSBFreq} = (3000 + N \times 1.44) \times 1000 \]

Utilize the below formula to calculate the SSBArfcn from SSBFreq

\[ \text{SSBArfcn} = \frac{(\text{SSBFreq} - \text{F\_REF\_OFFS})}{\Delta F_{\text{Global}}} + \text{N\_REF\_OFFS} \]

**Table 5.4.2.1-1: NR-ARFCN parameters for the global frequency raster**

<table>
<thead>
<tr>
<th>Range of frequencies (MHz)</th>
<th>( \Delta F_{\text{Global}} ) (kHz)</th>
<th>( F_{\text{REF-OFHS}} ) (MHz)</th>
<th>( N_{\text{REF-OFHS}} )</th>
<th>Range of N_{\text{REF}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – 3000</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0 – 599999</td>
</tr>
<tr>
<td>3000 – 24250</td>
<td>15</td>
<td>3000</td>
<td>6000000</td>
<td>600000 – 2016666</td>
</tr>
<tr>
<td>24250 – 100000</td>
<td>60</td>
<td>24250.08</td>
<td>2016667</td>
<td>2016667 – 3279165</td>
</tr>
</tbody>
</table>

**SSBArfcn = (SSBFreq - F\_REF\_OFFS)/\( \Delta F_{\text{Global}} \) + N\_REF\_OFFS**

Take example, there is a Freq range 3500-3600 be used to bring up a sub6 cell, Then

\[ N_0 = \frac{(3500-3000 + 7.92)}{1.44} = 352.7 \]

\[ N = \text{RoundUptoInter}(352.7) = 353 \]
SSBFreq = (3000 + 353 * 1.44) * 1000 = 3508320

The SSBFreq 3508320kHz is between 3000–24250MHz, so:
SSBArfcn = (3508320-3000000)/15+600000 = 633888

Notice:
The start Freq is united by MHz.
The SSBFreq is united by kHz.

4.3.1.2. Calculate Center Arfcn

Calculate centerFreq then calculate the CenterArfcn corresponding to the centerfreq as known as dlEarfcn.

CenterFreq and FreqSsb must match below formula:

FreqSsb = SSBOffset2PointA + CenterFreq - (PrbNum*SCS*12)/2

OffsetToPointA*12 + kSSB * 15 + 10 * 12 * SCS

absoluteFrequencySSB

carrierBandwidth(NRB)

15kHz for FR1, 60kHz for FR2

subCarrierSpacingCommon

FreqSsb - SSBOffset2PointA ≧ lower edge of the carrier, and FreqSsb+10*12*SCS ≧ upper edge of the carrier.

Tips: the unit for frequency is kHz, kSSB is 0 (can not be changed), OffsetToPointA must be an even number.

Utilize the below formula to calculate the CenterArfcn from CenterFreq
CenterArfcn = (CenterFreq - F_REF_OFFS)/ΔF_Global + N_REF_OFFS

For example:
FreqSsb is 3708480, bandwidth is 100MHz, OffsetToPointA is 24 PRBs (default value), SCS is 30 kHz. Following the formula, CenterFreq = 3708480 - 24*12*15 - 0*15 - 10*12*30 + (273*30*12)/2 = 3749700 kHz.
The CenterFreq 3749700kHz is between 3000–24250MHz, so:
CenterArfcn = (3749700-3000000)/15+600000 = 649980

4.3.1.3. Configuration

Login WebGUI, go through “Setting” -> “NR Cell”.
4.3.1.3.1. Using Default OffsetToPointA (24 PRBs)

- Configure SSB Arfcn, Center Arfcn;
- Click apply;
- Reboot

<table>
<thead>
<tr>
<th>SSB Arfcn</th>
<th>647028</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center Arfcn</td>
<td>647412</td>
</tr>
</tbody>
</table>

4.3.1.3.2. Using Other OffsetToPointA

- Configure SSB Arfcn and Center Arfcn; OffsetToPointA must be an even number and meet 3GPP definition.
- Click apply;
- Reboot

<table>
<thead>
<tr>
<th>SSB Arfcn</th>
<th>647028</th>
</tr>
</thead>
<tbody>
<tr>
<td>Center Arfcn</td>
<td>647412</td>
</tr>
</tbody>
</table>
Suggesting you to use default OffsetToPointA since it is easy to configure and hard to make mistake.

4.4. Trouble Shooting

You will find NR shows green in “Status -> System” page when NR cell bring up. If not, please check below information:

- Bridgestone WAN works fine;
- Bridgestone 5GC parameters are correct;
- Bridgestone NR Cell parameters are correct;
- AMF is reachable;
- 5GC works fine.

5. Advance Setting

5.1. NTP Server Setting

If sync progress is disabled, please enter CLI and use bellow command to enable sync progress.

```plaintext
son statement NTP_SYNC
```

The NTP_SYNC which is in “Status -> System” page will show green when NTP sync success.

![Progress Status](image)

5.1.1. Configuration

- Go through “Setting” -> “NTP Server”, choose “Time Zone” and input NTP server;
- Click “Apply”;
- Reboot.
5.1.2. Success Log

- Try dns lookup: 10.41.1.196 (ntp_process_flow_v2#177#3318)
- Send out NTP request to 10.41.1.196 (req_nip_time#179#3318)
- done send and rec(l(req_nip_time#178#3318)
- now parsing the packet! (req_nip_time#179#3318)
- mode is 4 (handle_nip_reply#252#3318)
- 0 0 (handle_nip_reply#291#3318)
- Got NTP_OK now sleep for 72 hrs (main#370#3318)
- execute ds [cam_send_d 4 -e 4 -v ntp_sync] (main#548#3320)
- Route msg (CLI) -> [SON_EVENT_SON_NIP_074C1]
  (cam_route_message#539#2449)
- Receive cam msg src=12 dst=4 events=4 (son_event_son_handler#154#2835)

5.1.3. Trouble Shooting

- Check NTP server working fine;
- Check NTP server address is correct;
- Check Bridgestone can connect to NTP server.
5.2. Sync Type Setting

5.2.1. Free Running

5.2.1.1. Configuration

- Go through “Setting” -> “Sync Setting”, modify “Enable PTP” to 0.
- Go through “Setting” -> “Sync Setting”, modify “Sync Mode” to FREE_RUNNING.
- Click “Apply”.
- Go through “Setting” -> “GPS”, modify “Enable GPS” to 0.
- Click “Apply”.
- Reboot
5.2.2. Sync

SYNC will show green in “Status -> System” page if sync success.

Progress Status

5.2.2.1. Configuration

- Go through “Setting” -> “Sync Setting”, modify “Enable PTP” to 0, “Sync Mode” to TIME.
- Click “Apply”.
- Go through “Setting” -> “GPS”, modify “Enable GPS” to 1.
- Click “Apply”.
- Reboot
## Sync Setting

**Notice:** This Device is a precision timing device. The following is the PTP configuration.

### Settings
- **Enable PTP:**
  - CMP Server
  - Intel SecGW Server
  - SecGW Server

- **Sync Mode:**
  - TR069 Management
  - O1 Management

- **IP Interface:**
  - eth0 WAN

- **Domain Number:**
  - 24

- **Delay Asymmetry:**
  - NR Cell Configuration
  - NR Security

- **PTP Profile:**
  - SAS
  - G.8275.1 cfg

- **HTTP Password:**
  - No file selected.

- **PTP Profile uploaded (if you selected a file):**
  - No file selected.

- **Your changes have been applied:**
  - Apply
  - Cancel

---

## GPS

### Settings
- **Enable GPS:**
  - NTP Server
  - Sync: Setting
  - CMP Server
  - Initial SecGW Server
  - SecGW Server

- **Status:**
  - Apply
  - Cancel

---

MosoLabs
5.2.2.2. Success Log

You will find “GPS Sync Success” form “Event Log -> System Log”.

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1300</td>
<td>INFO SON</td>
<td>GPS Sync Success (gpssync.ini) state: #483450</td>
</tr>
<tr>
<td>1200</td>
<td>INFO SON</td>
<td>state transition from 19-SM_GPS_SYNC_INIT to 19-SM_GPS_SYNC DONE (state_trans#16792959)</td>
</tr>
<tr>
<td>1100</td>
<td>INFO SON</td>
<td>Exec state 19-SM_GPS_SYNC_DONE startfunc: psd 0 (stateᐠ�opsy�佥#22792950)</td>
</tr>
<tr>
<td>1000</td>
<td>INFO SON</td>
<td>Exec state 19-SM_GPS_SYNCDONE enterfunc: NULL (stateposix#250#2950)</td>
</tr>
</tbody>
</table>

5.2.2.3. Trouble Shooting

- GPS sync failed
  - Check NMEA message log.
  - GPGGA: 0=invalid; 1=GPS fix; 2=Diff. GPS fix
  - GNGSA: 99.0 mean not fix

Check the device can receive GPS signal.

5.2.3. PTP Sync

5.2.3.1. Configuration

- Go through “Setting” -> “Sync Setting”, modify “Enable PTP” to 1, “PTPProfile” to G.8275.1.cfg or G.8275.2.cfg, “Sync Mode” to TIME.
- Click “Apply”.
- Go through “Setting” -> “GPS”, modify “Enable GPS” to 0.
- Click “Apply”.
- Reboot
Tips: If “PTPProfile” configure to G.8275.2.cfg, you need configure “Unicast Master IP-Address” to your PTP server. If there are more parameters need to configure than on the “Sync Setting” page, you can use “PTP Profile upload” function to load a PTP profile, you need send your request to Sercomm for generate initial PTP profile.

5.2.3.2. Trouble Shooting

- Check PTP server working fine;
- Check Bridgestone parameters of PTP server are correct.

5.3. SecGW Server Setting

Bridgestone connects to the core network through internet which may be encountered malicious attack, the signals and data between Bridgestone and core network shall be well protected, IPSec tunnel provides a transparent protection for privacy and integrity.

The S_SEGW which is in “Status -> System” page will show green when the IPSec tunnel established.

5.3.1. PSK Authentication

5.3.1.1. Configuration

- Follow below figure to configure PSK authentication;
- Reboot.
5.3.1.2. Success Logs

Jan 13 13:36:48 INFO charon 12[NET] sending packet: from 10.41.5.6:4500 to 52.49.202.254:4500 (388 bytes)
Jan 13 13:36:49 INFO charon 13[NET] received packet: from 52.49.202.254:4500 to 10.41.5.6:4500 (236 bytes)
Jan 13 13:36:49 INFO charon 13[ENC] parsed IKE_AUTH response 1 (DY AUTH CFRP ADDR SA TS TSN AUTH LIFT)
Jan 13 13:36:49 INFO charon 13[KE] authentication of "aws_psk" with pre-shared key successful
Jan 13 13:36:49 INFO charon 13[KE] IKE_SA_tunnel(1) established between 10.41.5.6:[60109896@strongswan.org]:52.49.202.254[aws_psk]
Jan 13 13:36:49 INFO charon 13[KE] IKE_SA_tunnel(1) established between 10.41.5.6:[60109896@strongswan.org]:52.49.202.254[aws_psk]
Jan 13 13:36:49 INFO charon 13[KE] scheduling rekeying in 86245
Jan 13 13:36:49 INFO charon 13[KE] maximum IKE_SA lifetime 86300

MosoLabs
44
5.3.1.3. Trouble Shooting

Check the parameters for PSK authentication were correct, and the SecGW should be reachable, also the log file shall show which step of IKEv2 was failed.

5.3.2. Cert Authentication

Make sure the certs have been assigned.

5.3.2.1. Configuration

- Follow below figure to configure Cert authentication;
- Send command “oam set Device.IPsec.Profile.1.X_00C002_IKEv2LocalID leftid” by CLI;
- Send command “oam set Device.IPsec.Profile.1.X_00C002_IKEv2RemoteID rightid” by CLI;
- Reboot.
5.3.2.2. Success Logs

Check the parameters for cert authentication were correct, and the SecGW should be reachable, also the log file shall show which step of IKEv2 was failed.

5.3.2.3. Trouble Shooting

Check the parameters for cert authentication were correct, and the SecGW should be reachable, also the log file shall show which step of IKEv2 was failed.

5.4. CMPv2 Server Setting

Please go through “Setting” -> “CMP Server” to configuring.
5.5. HeMS Server Setting
5.6. SAS Setting
When enabling SAS, ensure that the device has an available FCC ID and certificate, and fill in the user ID and SAS server address before saving and restarting.

You can get more detailed information from the sas user manual.docx.

Notice: When GPS is enabled, the device will use the location information provided by the GPS. When GPS is not enabled, the device will use the installation param in this page.
Notice: When enable SAS, Bandwidth Frequency, nrFreqBand, TX Power, SSB Arfcn and Center Arfcn at NR Cell Configuration page will be controlled by SAS.

The Slot Pattern on the NR Cell Configuration page supports two configurations: 8:2 (FR1.30-4 DDDSUUDDDD), 6:4 (CBRSA_1 DDDSUUDDDD).
5.7. Intra HO Setting
Make sure that NRFreqRelationID equals 1 and choose the matching ServiceProviderInfoID, and when you have made all the settings you need, the last step is reboot.
5.8. Inter-frequency Reselection Setting
The FreqSsb in Inter Frequency should be filled absArfcnSsb.
Make sure that choose the matching NRFrequencyInfoID, NRFreqRelationID and ServiceProviderInfoID (related content see above), and when you have made all the settings you need, the last step is reboot.

5.9. Inter-frequency HO Setting

As the same as reselection setting to config neighbour info. The only thing we need to concern is service provider info. It contains critical neighbour info.

When we config service provider info, we need to know the ID “1” “2” “3” have
connection with intra rat and inter rat. If we config one intra neighbour rat, the rat id is “1”. But if we config one intra rat and one inter rat, the intra rat id is “1” and the inter rat id is “2”.

For example:

5.10. O1 Management Setting

The O1 Management feature is following the O-RAN.WG10.O1-Interface.0-v06.00 specification. Trace Management Services and Cloudified NF Registration Management Service are not supported yet.

The O1_MGR which is in “Status -> System” page will show green when O1 Management Server is connected success.
5.10.1. Configuration

Enable the O1 Management and fill the protocol/address/port, click “Apply” and then reboot.

5.10.2. Success Log

Jan 1 00:01:16 INFO 01MOR Yang value changed, sub_id[73] event[2] request_id[1] {lo1mgr_sysrepo_pm_module_change_cbl=6245977
Jan 1 00:01:16 INFO 01MOR q_du_pm_state = 0, q_cu_pm_state = 1 {lo1mgr_sysrepo_pm_module_change_cbl=6245977
Jan 1 00:01:16 INFO 01MOR q_du_pm_state = 1, q_cu_pm_state = 1 {lo1mgr_sysrepo_pm_module_change_cbl=6245977
Jan 1 00:01:17 INFO 01MOR CURL perform success, rsp_code [200] {client_init_and_request=#2525977
Jan 1 00:01:17 INFO 01MOR o1mgr init successfully (main=2014977
Jan 1 00:01:18 INFO 01MOR state transit from 19-SM_01MOR_INIT to 19-SM_01MOR_DONE (state_transit#100#4641
Jan 1 00:01:18 INFO OF5 success to write timespase2 1ps disable and nwrite is 512 (disable Ub) 1ps=2525653
Jan 1 00:01:19 INFO 01MOR entering state - 19-SM_01MOR_DONE (son_statem_run#493#4641
Jan 1 00:01:19 INFO 01MOR exec state 19-SM_01MOR_DONE start func pid 0 (state_func_start#240#4641
Jan 1 00:01:19 INFO 01MOR exec state 19-SM_01MOR_DONE enter func NULL (state_func_enter#271#4641
Jan 1 00:01:19 INFO 01MOR state transit from 19-SM_01MOR_DONE to 20-SM_OF5_SYNC_INIT (state_transit#100#4641

5.10.3. Trouble Shooting

- Check O1 management server can support VES PNF registration procedure, otherwise
PnP will fail and system block in this stage.

- Check the O1 management server IP address and port is correct
- Check the http or https protocol is supported in o1 management server side
- Check the device information(csn) is registered in the o1 management server side

6. Firmware and Configuration Management

6.1. Factory Reset

6.2. FW Upgrade
Phone calls, internet connections and LAN connections will be interrupted due to the upgrade. Please press apply if you want to continue.

Apply   Cancel
6.3. Backup Configuration
6.4. Restore Configuration

6.5. Customize Upgrade

- Customize file upgrade from web page (same as FW upgrade)
gNB will automatically restart when customized file upgrade is complete. After device bootup, please login the web “state” page to check the customized version to ensure the upgrade is successfully
7. Status Indicators

7.1. from GUI
7.1.1. Status

7.1.2. WAN

<table>
<thead>
<tr>
<th>1 Status</th>
<th>Setting</th>
<th>Event Log</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WAN 2</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5G Femto</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PTP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Address: fe80::2c0:2ff:fe11:1669

MAC Address: 00:c0:02:11:16:69

Netmask: 255.255.255.0

Gateway: 10.41.3.254
7.1.3. 5G Femto

7.1.4. GPS
7.1.5. PTP

![PTP Status Screen]

7.2. LED Indicators

<table>
<thead>
<tr>
<th>Description</th>
<th>Power</th>
<th>WAN</th>
<th>5G</th>
<th>Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Femto Power is Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Femto Power is On (No Physical Connection for WAN)</td>
<td>Solid White</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Internet is Connecting</td>
<td>Solid White</td>
<td>Blink White</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Internet Connection is Available</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>PHP In Progress</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Blink White</td>
<td>Off</td>
</tr>
<tr>
<td>5G in Service</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Off</td>
</tr>
<tr>
<td>Critical Alarm</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Solid White</td>
<td>Solid Amber</td>
</tr>
</tbody>
</table>
8. Logs

8.1. System Log Display

8.2. CU DU Log Setting

- Configure CU and DU log level, usually the default values are used, but when debugging certain issues it may be necessary to modify the level of certain modules, the corresponding content can be got from Sercomm. Three simple configurations are listed below:
  1. ALL:INF
  2. APP:INF
  3. ALL:INF, COMMON:DEBUG, APP:ERR

Tips: There are far more than these three configurations that can be configured, and you can choose the ones you need to configure.

- Click apply;
- Requires reboot to take effect.
The configuration example is as follows:

<table>
<thead>
<tr>
<th>Cu Du Log Level</th>
<th>Cu Log Level</th>
<th>Du Log Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>APP:DEBUG</td>
<td>ALL:INFO,APP:ERR</td>
</tr>
</tbody>
</table>
8.3. Log Collection

9. CLI Support List

Sercomm Bridgestone project provide essential standard Linux and Sercomm private commands.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Linux standard Commands</th>
<th>Sercomm private commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>1: ping</td>
<td>1: show dev info</td>
</tr>
<tr>
<td></td>
<td>2: ip</td>
<td>2: oam get</td>
</tr>
<tr>
<td></td>
<td>3: ls</td>
<td>3: oam get_list</td>
</tr>
<tr>
<td></td>
<td>4: scp</td>
<td>4: oam get_rw</td>
</tr>
<tr>
<td></td>
<td>5: tftp</td>
<td>5: oam get_rw_all</td>
</tr>
<tr>
<td></td>
<td>6: traceroute</td>
<td>6: oam set</td>
</tr>
<tr>
<td></td>
<td>7: date</td>
<td>7: oam unset</td>
</tr>
<tr>
<td></td>
<td>8: reboot</td>
<td>8: oam display</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9: oam save</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10: son statem status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11: son statem on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12: son statem off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13: show gps status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14: show ipsec key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15: upgrade_cli</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16: apply</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17: factory reset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18: quit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>19: passwd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20: sc_yang_cli</td>
</tr>
</tbody>
</table>
### 9.1. Show Help

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: Press `Ctrl` + `/` to show help of command.

### 9.2. Show Device Information

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: use command “show dev info” to show the device information.

```
> show dev info
sn: SWRD2111668
MAC address: 00:C0:02:11:16:89
Sw Ver: DG560S@2208251855
Sw Extra Ver: 1757
Model Name: SCE5164-B78
Calibrated Band: N78
Sync Capability: support GPS and PTP
```

### 9.3. Show OAM Parameters

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: exec command “oam get [OAM_Parameters]” to get the value of parameters

```
> oam get Device.Services.SAS.Enable
Device.Services.SAS.Enable=0
```
9.4. Show OAM Parameters List

Step 1: use sc_femto or operator account to login ssh
Step 2: use command "oam get_list [OAM_Parameters]" to get the value of list

9.5. Show Read Write Access of OAM Parameters

Step 1: use sc_femto or operator account to login ssh
Step 2: use command "oam get_rw [OAM_Parameters]" to get the read write access of parameters

9.6. Show Read Write Access of All OAM Parameters

Step 1: use sc_femto or operator account to login ssh,
Step 2: use command "oam get_rw_all" to get the read write access of all parameters.
9.7. Set OAM Parameters

Step 1: use operator account to login ssh,

Step 2: use command “oam set [OAM_Parameters]” to modify the value of OAM parameters

```
> oam set Device.Services.SAS.Enable 1
ok.
```

9.8. Unset OAM Parameters

Step 1: use operator account to login ssh,

Step 2: use command “oam unset [OAM_Parameters]” to unset the value of parameter which is not applied.

```
> oam unset Device.Services.SAS.Enable
ok.
```
9.9. Show OAM Parameters Not Applied

Step 1: use `sc_femto` or `operator` account to login ssh.

Step 2: use command "oam display" to display parameters which are set but not applied

```
> oam display
Display Setting parameter:
Device.Services.SAS.Enable=1
****
```

9.10. Save OAM Configuration

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: use command "oam save" to save OAM configuration.

```
> oam save
ok.
```

9.11. Show Provision Status

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: use command "son statem status" to show provision status

```
> son statem status
statem status:
    NETCONF=0ff
    WAN=On
    NTP_SYNC=0n
    REDIRECT=0ff
    I_SEGW=0ff
    CMP=0ff
    I_HEMS=0ff
    S_SEGW=0ff
    S_HEMS=0n
    01_MGR=0ff
    SYNC=0ff
    SAS=0ff
    NR=0ff

SON is in SM RUNNING status.
```
9.12. Turn On The Chosen States in Provision Flow

Step 1: use operator account to login ssh

Step 2: use command "son statem on [Feature_Name]" to turn on the chosen states in provision flow.

```
$ son statem on S_SEGW
statem status:

NETCONFd=off
WAN=on
NTP SYNC=on
REDIRECT=off
I_SEGW=off
CNP=off
I_HEMS=off
S_SEGW=on
S_HEMS=on
DI_MGR=off
SYNC=off
SAS=off
NR=on
```

9.13. Turn Off The Chosen States in Provision Flow

Step 1: use operator account to login ssh

Step 2: use command "son statem off [Feature_Name]" to turn off the chosen states in provision flow.
9.14. Apply All Parameter Changes

Step 1: use operator account to login ssh

Step 2: use command “apply” to apply all parameter changes

> apply
Service will be apply.

9.15. Show GPS Sync Status

Step 1: use sc_femto or operator account to login ssh

Step 2: use command "show gps status" to show GPS status.
9.16. Show OAM(YANG) parameters

   Step 1: use `sc_femto` or `operator` account to login ssh
   
   Step 2: use command "sc_yang_cli get [YANG_xpath]" to show the value of the yang parameter

```
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
> sc_yang_cli set /scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 1
> sc_yang_cli save
[YANG] Save Config to Flash success
> sc_yang_cli apply
OK
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
> sc_yang_cli save
[YANG] Save Config to Flash success
> sc_yang_cli apply
OK
```

9.17. Set OAM(YANG) parameters

   Step 1: use `operator` account to login ssh
   
   Step 2: use command "sc_yang_cli [get/set/save] [YANG_xpath]" to set the value of the yang parameter

```
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
> sc_yang_cli set /scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 1
> sc_yang_cli save
[YANG] Save Config to Flash success
> sc_yang_cli apply
OK
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
> sc_yang_cli save
[YANG] Save Config to Flash success
> sc_yang_cli apply
OK
```

9.18. Support Download Log

   Step 1: use `sc_femto` or `operator` account to login ssh
   
   Step 2: use command "log collect" to package log file
Step 3: download log and the logs are stored in /tmp/ftp/sercomm_logs.tgz

**Method one:** use `scp` to download the log file (only for operator)

**Method two:** use `sftp` to download the log file
9.19. Support Factory Default

Step 1: use operator account to login ssh
Step 2: use command "factory reset" to factory default.

```
> factory reset
ok.
>
```

9.20. Support Quit

Step 1: use sc_femto or operator account to login ssh,
Step 2: use command "quit" to disconnect the ssh connection.

```
> quit
```

9.21. Support Firmware Version Upgrade

Step 1: use operator account to login ssh
Step 2: upload the firmware version file to /tmp/ftp
Step 3: use command "upgrade_cli -f /tmp/ftp/[FW_Name]" to upgrade the version

**Method one:** use tftp to upload the firmware version file:

**Method two:** use sftp to upload the firmware version file:
9.22. Support ping command

Step 1: use operator to login ssh

Step 2: use command “ping <ip address>” to check endpoint is reachable or not. ping also provide some parameter, and you can exec combine parameter to test the network.

9.23. Support ip command

Step 1: use sc_femto or operator to login ssh

Step 2: use command “ip a” to check network status.
9.24. Support traceroute command

Step 1: use operator to login ssh

Step 2: use command “traceroute -n -m 5 -q 4 -w 3 <ip address>” to locate all routers between your computer and the target computer.

9.25. Support date command

Step 1: use sc_femto or operator account to login ssh

Step 2: use command “date” to show the system time


Step 1: use operator account to login ssh
Step 2: use command “reboot” to reboot the device

> reboot
ok.

9.27. Support rma command

9.27.1 rma get all

Step 1: use sc_femto or operator account to login ssh

Step 2: use command “rma get all” to show the DU information about system info/system status/ue overview.

<table>
<thead>
<tr>
<th>SYSTEM INFO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot_Cause</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SYSTEM STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED</td>
</tr>
<tr>
<td>SecGW</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
9.27.2  rma get reboot_cause

Step 1: use sc_femto or operator account to login ssh

Step 2: use command "rma get reboot_cause" to show last reboot cause
<table>
<thead>
<tr>
<th>Reboot Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1101</td>
<td>remote image upgrade by HEMS</td>
</tr>
<tr>
<td>1102</td>
<td>remote image upgrade by O1MGR</td>
</tr>
<tr>
<td>1103</td>
<td>image upgrade by cli</td>
</tr>
<tr>
<td>1104</td>
<td>image upgrade by GUI</td>
</tr>
<tr>
<td>1105</td>
<td>factory reset</td>
</tr>
<tr>
<td>1109</td>
<td>device reboot from HEMS</td>
</tr>
<tr>
<td>1110</td>
<td>device reboot from O1MGR</td>
</tr>
<tr>
<td>1111</td>
<td>device reboot from GUI</td>
</tr>
<tr>
<td>1112</td>
<td>system monitor check process crash</td>
</tr>
<tr>
<td></td>
<td>Event Description</td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
</tr>
<tr>
<td>1120</td>
<td>set customer by CLI</td>
</tr>
<tr>
<td>1123</td>
<td>config restore by GUI</td>
</tr>
<tr>
<td>1124</td>
<td>device overheat</td>
</tr>
<tr>
<td>1125</td>
<td>CPU overload</td>
</tr>
<tr>
<td>1128</td>
<td>tti fail</td>
</tr>
<tr>
<td>1130</td>
<td>Cell auto reboot after it not active for 30min</td>
</tr>
<tr>
<td>1131</td>
<td>WAN IP disconnected</td>
</tr>
<tr>
<td>1133</td>
<td>DU crash make the gnb reboot</td>
</tr>
<tr>
<td>1134</td>
<td>CU crash make the gnb reboot</td>
</tr>
<tr>
<td>1135</td>
<td>image upgrade by CLI</td>
</tr>
<tr>
<td>1201</td>
<td>Power down make last reboot</td>
</tr>
<tr>
<td>1401~1404</td>
<td>unidentified-failure</td>
</tr>
</tbody>
</table>

9.27.3  rma get led

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: use command “rma get led” to show led status

```
> rma get led
[WAN LED] White:on Amber:off IDX:0x00002
[5G LED] White:on Amber:off IDX:0x10002
[ALARM LED] White:off Amber:off IDX:0x20004
```
9.27.4  rma get secgw

   Step 1: use sc_femto or operator account to login ssh

   Step 2: use command “rma get secgw” to show secgw address and ipsec information

Server: SecGW IP address.

Lifetime/Reauth: The configuration of lifetime/reauth.

tun1xxx: The uptime since ipsec established, and the inner ip of ipsec tunnel.

9.27.5  rma get ue_info

   Step 1: use sc_femto or operator account to login ssh

   Step 2: use command “rma get ue_info” to show the real time numbers of UE attached and the max numbers of supported UEs.

9.27.6  rma get cert

   Step 1: use sc_femto or operator account to login ssh

   Step 2: use command “rma get cert” to get cert info. Preferred display of operator
Step 2: use command "rma get meminfo" to get cert memory information.
9.27.8  rma get flashinfo

    Step 1: use sc_femto or operator account to login ssh

    Step 2: use command “rma get flashinfo” to get flash information
9.28. Support show du stats command

Step 1: use `sc_femto` or `operator` account to login ssh

Step 2: use command “show du stats” to get du stats

10. Diagnostic

10.1. Cell Setup

The NR which is in “Status -> System” page will show green when cell is up.

10.2. Common Issues

TBD