Bridgestone P4 SA User Guide

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

Revision History

Rev	**Date**	**Description**	**Version**
V1.0	2022/7/7	Initial Release V 1.0	DG5605@2209062255
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

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

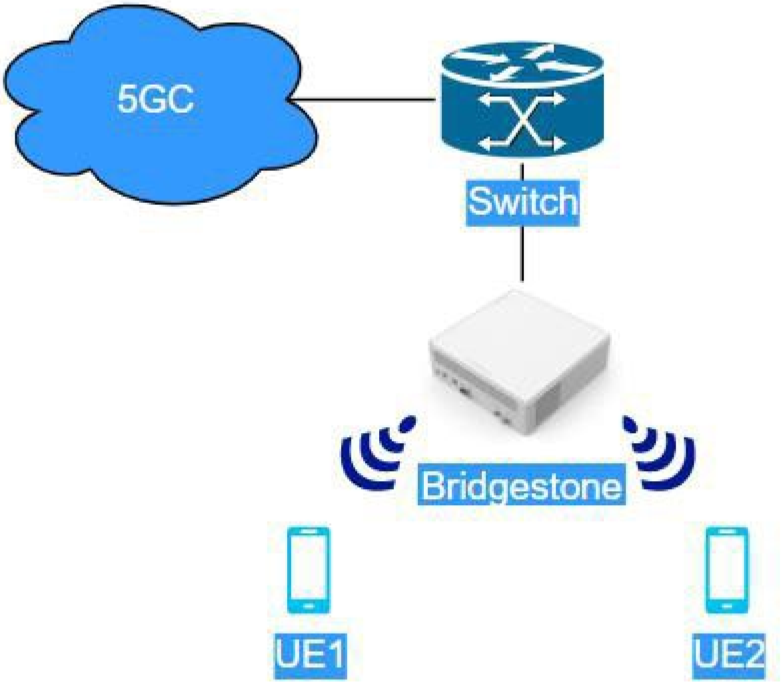
Bridgestone has 6 ports: DC, ETH1, ETH2, SFP, 1PPS, GPS. The function for them shows as below table.

Port	Description
DC	Power port
ETH2	WAN port
ETH1	LAN port (console port)
SFP	Reserved
1PPS	Export 1PPS signal
GPS	Connect to GPS antenna, use for GPS sync

2. Network Topology

2.1. Common Network

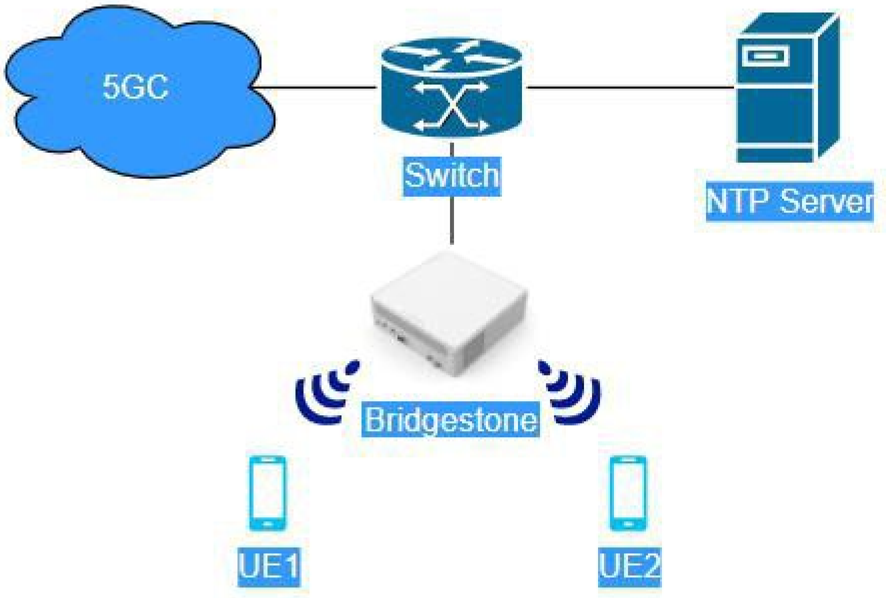
This topology includes 5GC, SmallCell, switch and UEs, shows as below figure.



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.



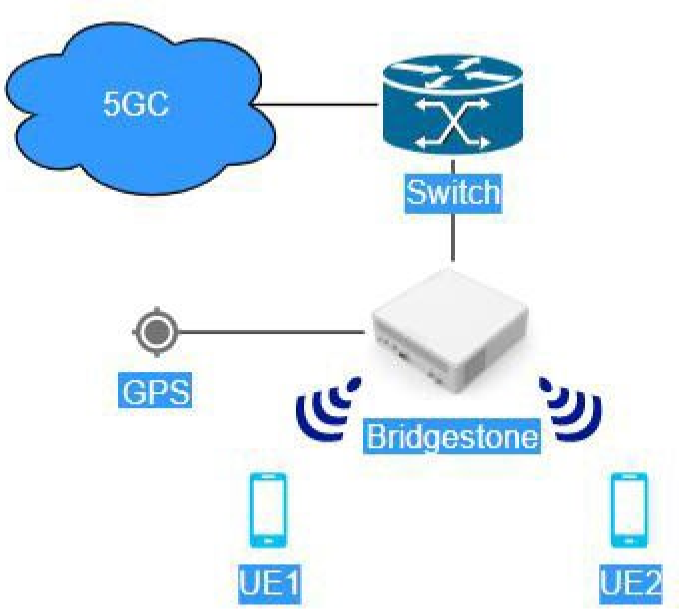
Using this topology need to enable WAN progress, NTP progress and NR progress. Please refer to chapter 4 "Basic Setting", 5.1 "NTP Server Setting" and 5.2.1 "Free Running" to configure Bridgestone.

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

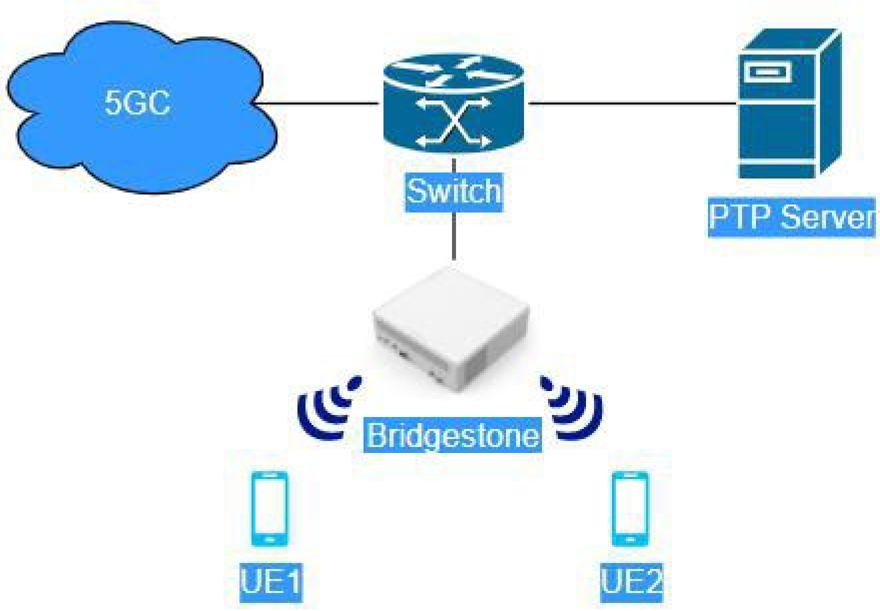
This topology includes 5GC, SmallCell, GPS, switch and UEs, shows as below figure.



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.

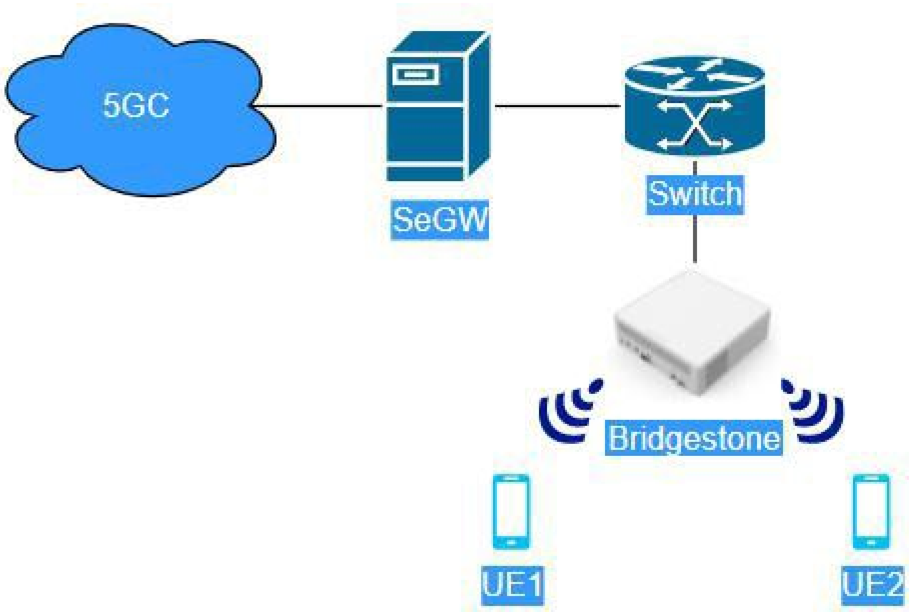


Using this topology need to enable WAN progress, GPS_SYNC progress and NR progress.

Please refer to chapter 4 “Basic Setting” and 5.2.3 "PTP Sync" to configure Bridgestone..

2.4. Add SeGW

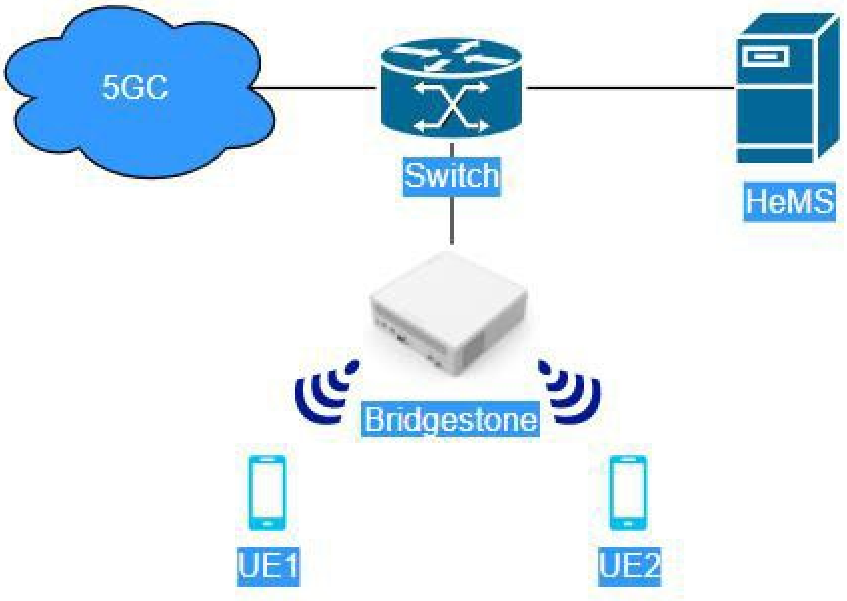
This topology includes 5GC, SmallCell, SeGW, switch and UEs, shows as below figure.



Using this topology need to enable WAN progress, S_SEGW 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

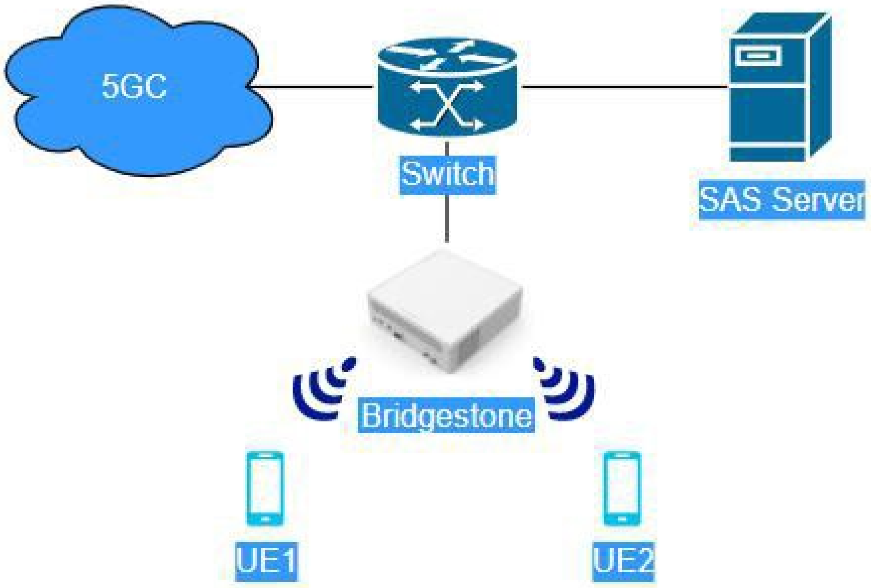
This topology includes 5GC, SmallCell, HeMS, switch and UEs, shows as below figure.



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.

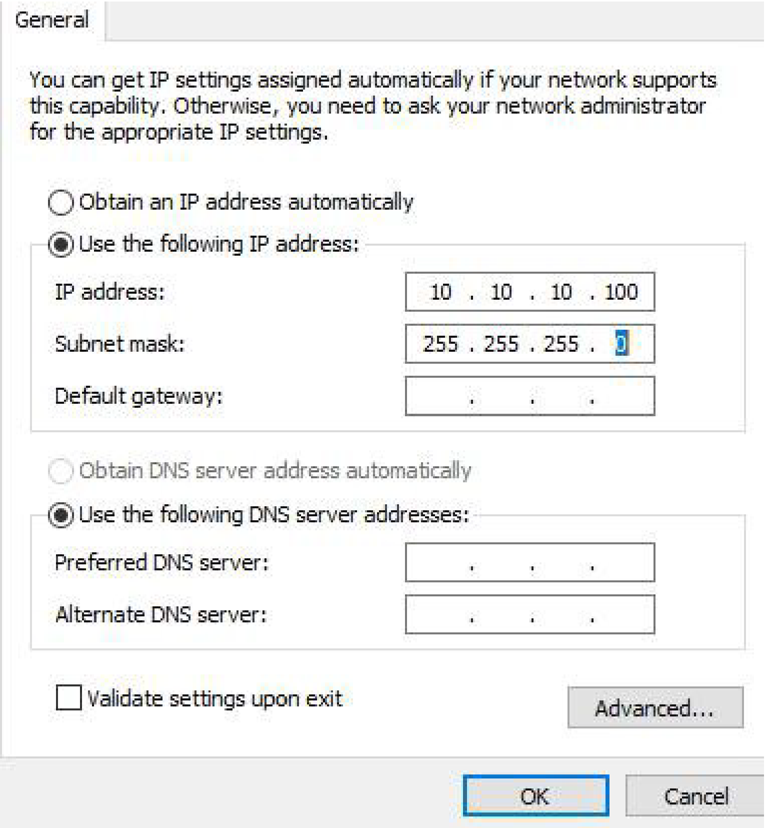
3. How to Access Bridgestone

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.



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

- LTE2(WAN) port for access

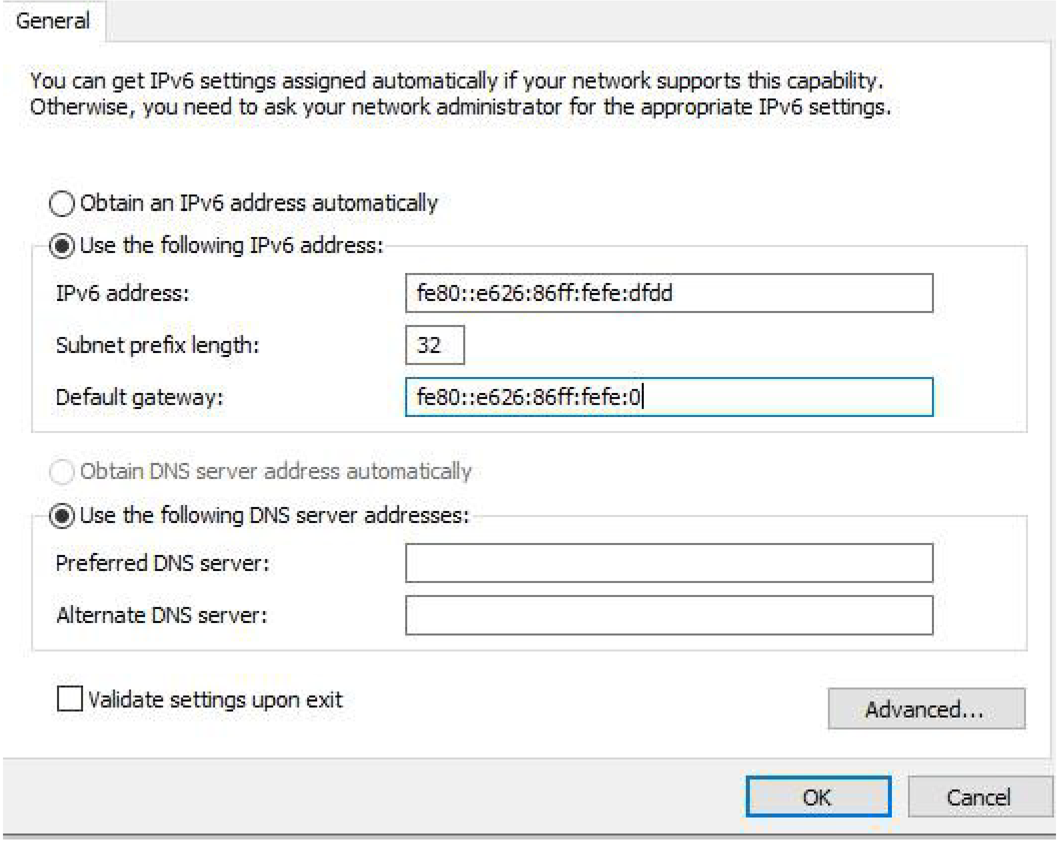
  The access address by using WAN port is WAN IPv4 address or the IPv6 link-local address of Bridgestone. IPv6 link-local can be calculated from MAC address, for example:

  MAC: E42686FD6A60, IPv6: fe80::e626:86ff:fefd:6a60

  MAC: E42686FD6A63, IPv6: fe80::e626:86ff:fefd:6a63

  MAC: E42686FD6A66, IPv6: fe80::e626:86ff:fefd:6a60

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.



You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: fe80::e626:86ff:fefe:dfdd

Subnet prefix length: 32

Default gateway: fe80::e626:86ff:fefe:0

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

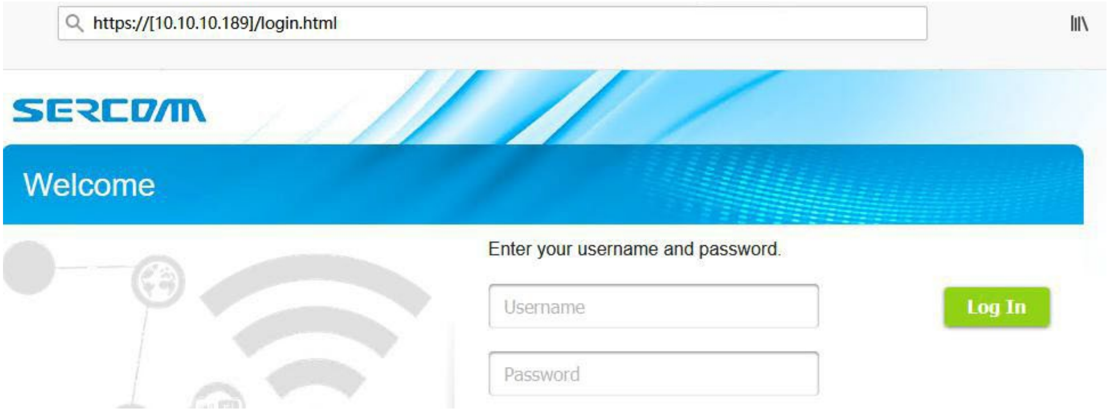
Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

3.1. Web GUI Login

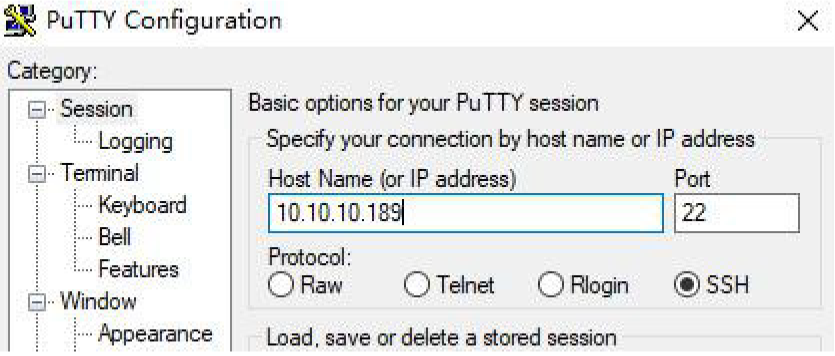
You can login the Bridgestone GUI on the browser by the URL: https://10.10.10.189 or https://WAN IPv4 address or https://[Bridgestone IPv6 link-local address] (which depends on what accessing mode you used). Also the account/password can be got form Sercomm.



https://[10.10.10.189]/login.html

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.



Host Name (or IP address): 10.10.10.189

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

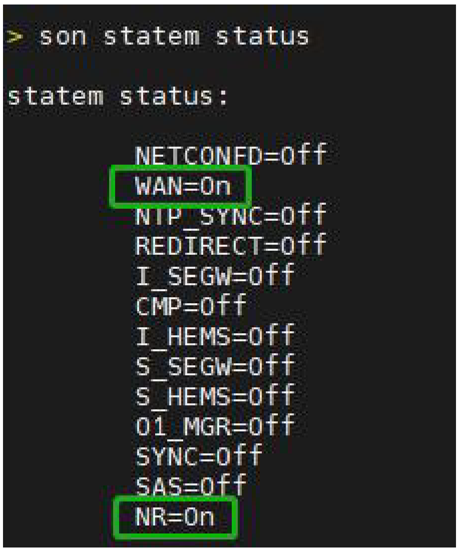
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Basic options for your PuTTY session
Specify your connection by host name or IP address
Load, save or delete a stored session

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.



```
> son statem status

statem status:

        NETCONFD=Off
        WAN=On
        NTP_SYNC=Off
        REDIRECT=Off
        I_SEGW=Off
        CMP=Off
        I_HEMS=Off
        S_SEGW=Off
        S_HEMS=Off
        01_MGR=Off
        SYNC=Off
        SAS=Off
        NR=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

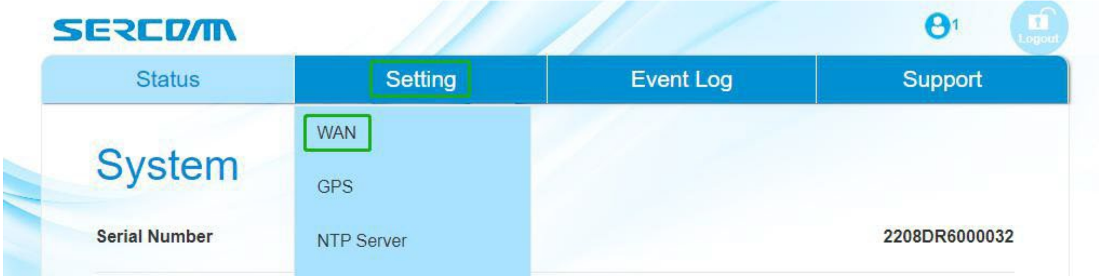
Bridgestone support 2 WAN mode.

- DHCP: Base on RFC 2131.

- Static IP: User can set a IP address, subnet mask, default gateway, and DNS server manually.

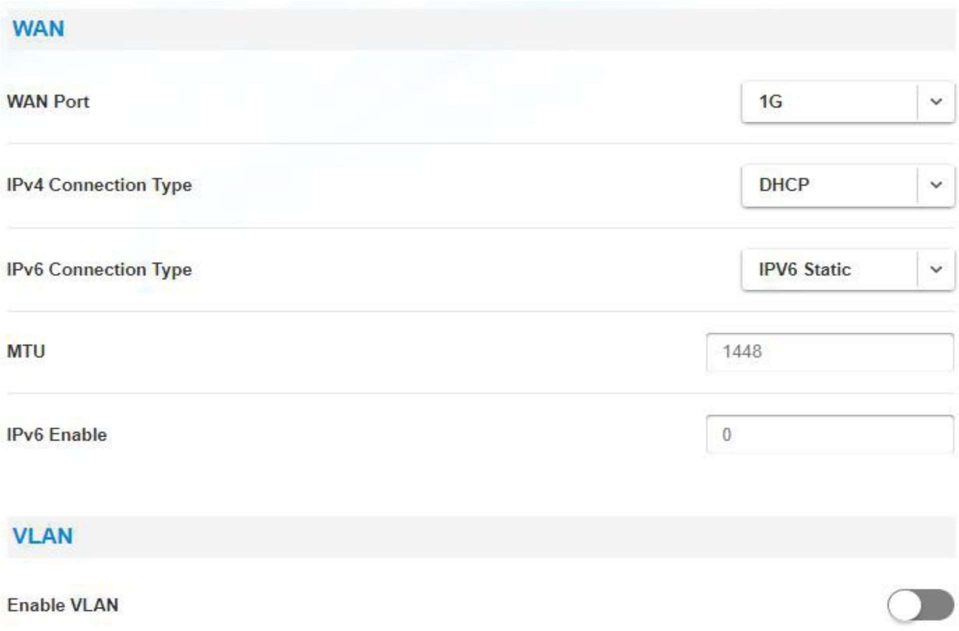
4.1.1. Configuration

Please go through “Setting” -> “WAN” to configuring.



Serial Number 2208DR6000032

(1) The default setting for Bridgestone is DHCP and non VLAN.



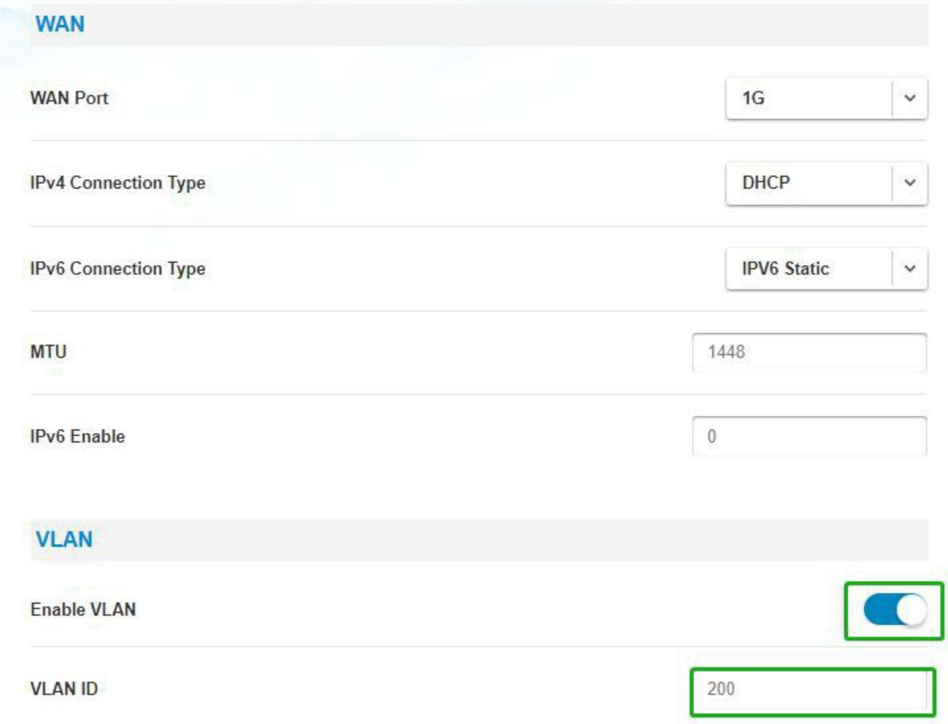
WAN

WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 Static
MTU	1448
IPv6 Enable	0

VLAN

Enable VLAN	○

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



WAN

WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 Static
MTU	1448
IPv6 Enable	0

VLAN

Enable VLAN	●
VLAN ID	200

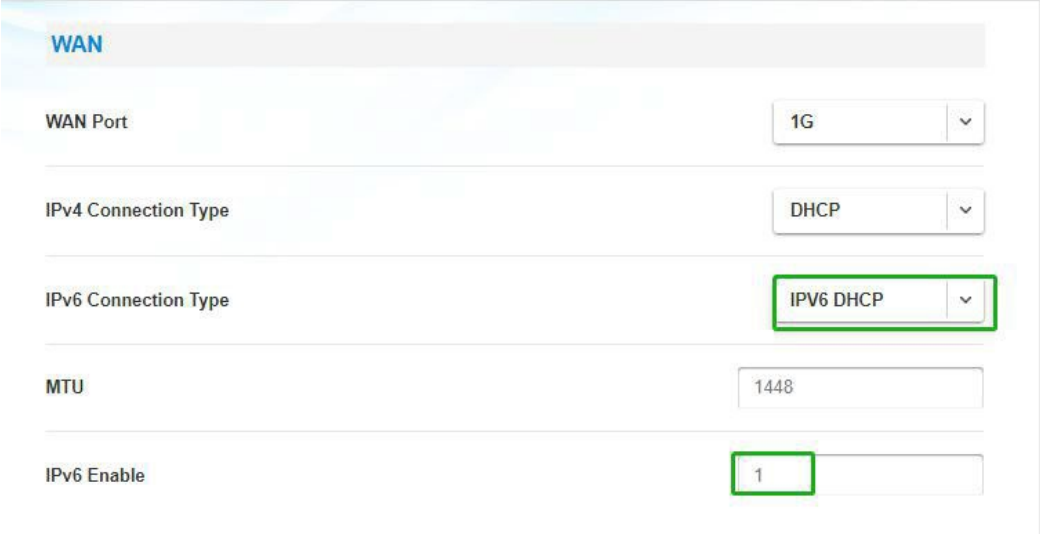
4.1.1.2. DHCP IPv6

(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.

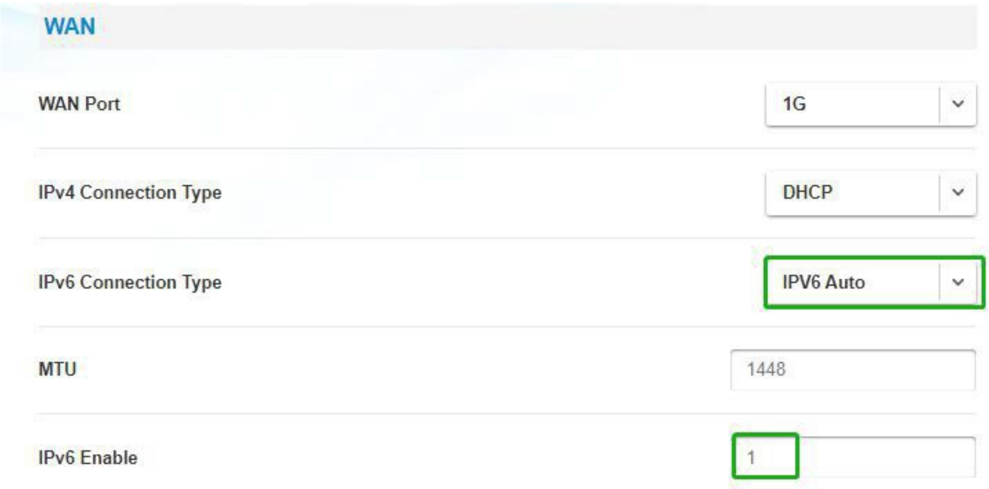
* IPv6 DHCP corresponds Stateful IPv6

* IPv6 Auto corresponds Stateless IPv6



WAN

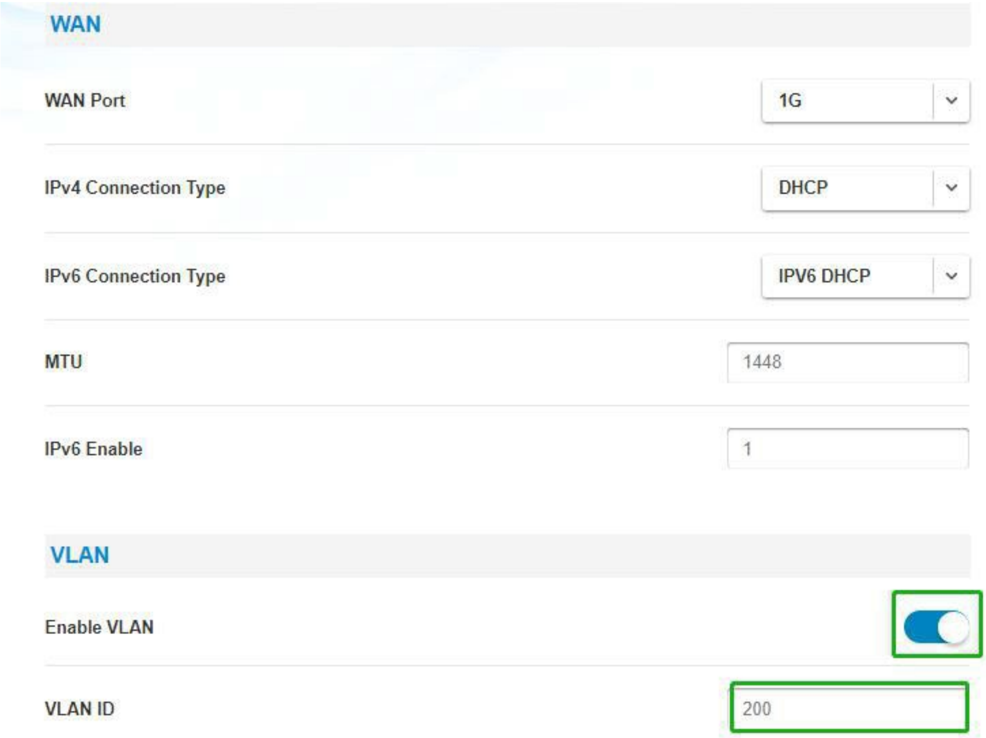
WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 DHCP
MTU	1448
IPv6 Enable	1



WAN

WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 Auto
MTU	1448
IPv6 Enable	1

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



WAN

WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 DHCP
MTU	1448
IPv6 Enable	1

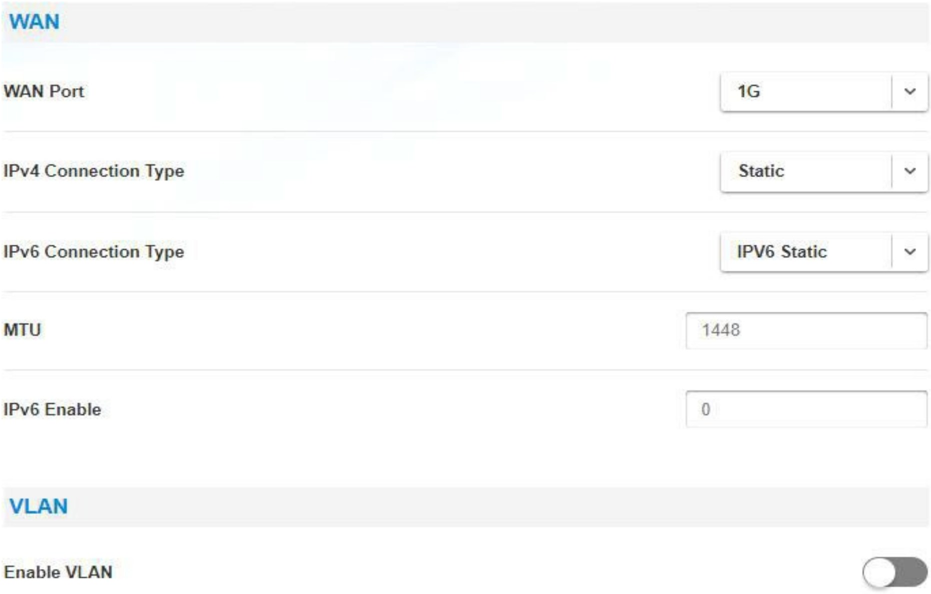
VLAN

Enable VLAN	●
VLAN ID	200

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.

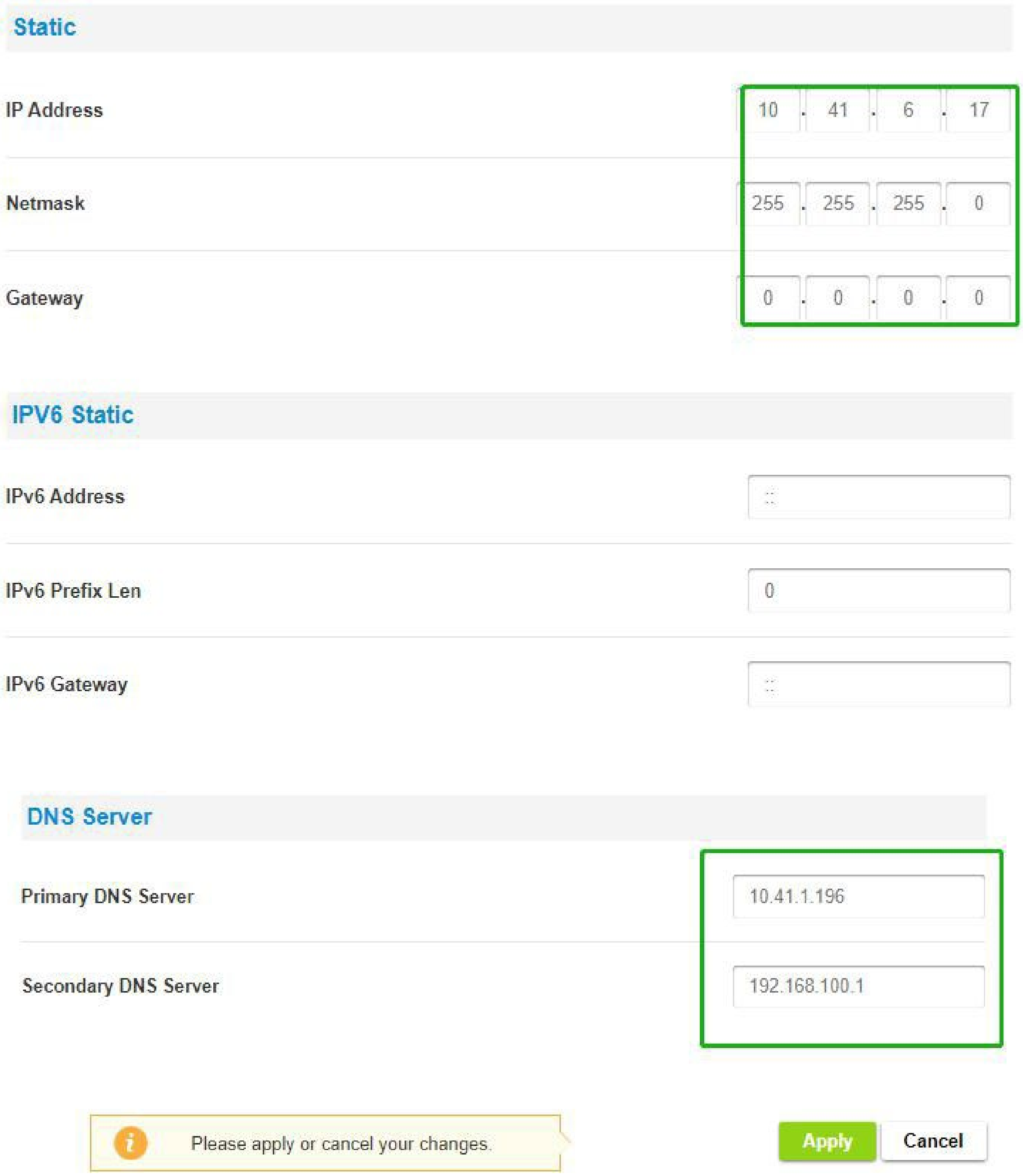


WAN

WAN Port	1G
IPv4 Connection Type	Static
IPv6 Connection Type	IPV6 Static
MTU	1448
IPv6 Enable	0

VLAN

Enable VLAN	○



Static

IP Address	10 . 41 . 6 . 17
Netmask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0

IPV6 Static

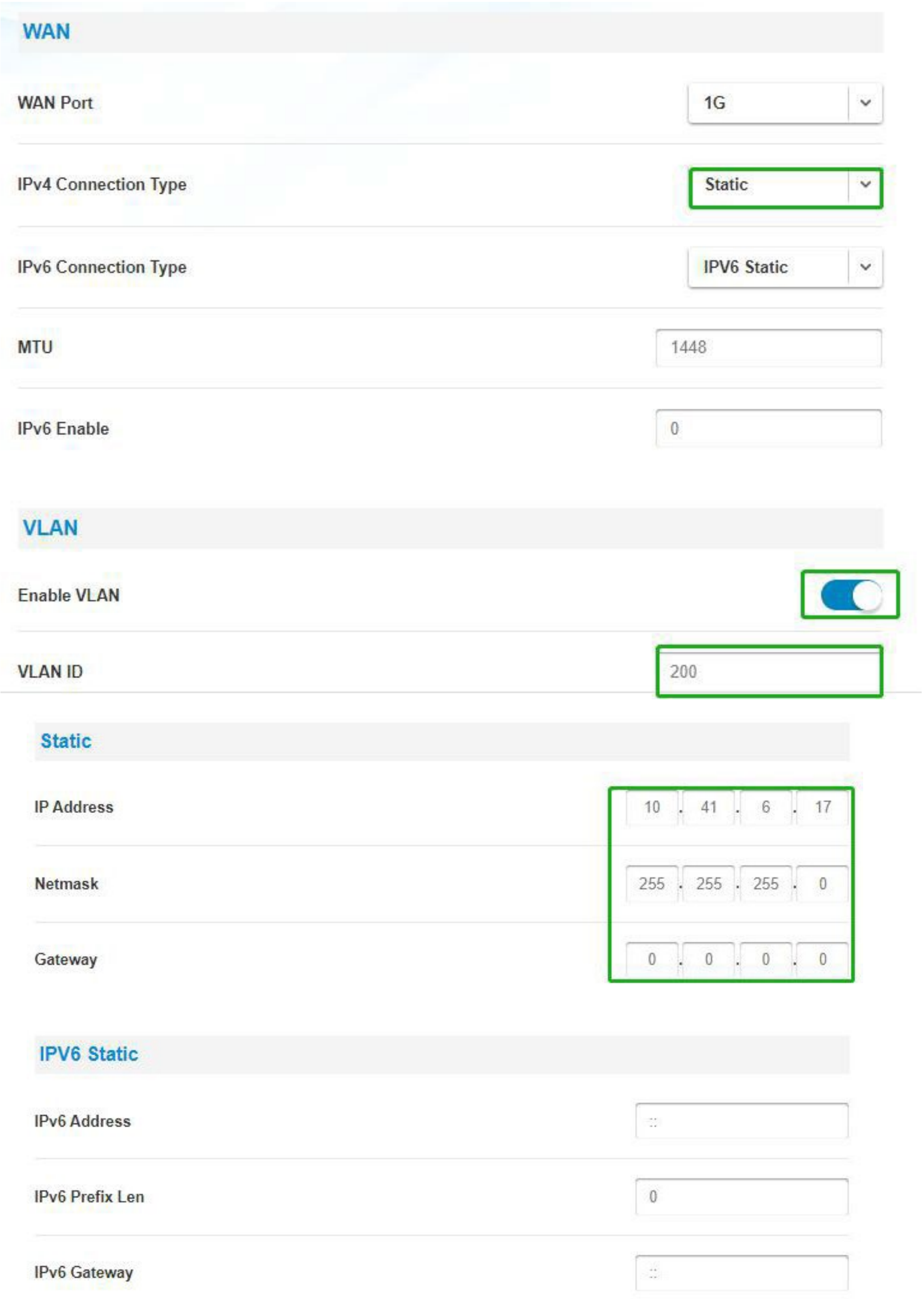
IPv6 Address	::
IPv6 Prefix Len	0
IPv6 Gateway	::

DNS Server

Primary DNS Server	10.41.1.196
Secondary DNS Server	192.168.100.1

Please apply or cancel your changes.

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



WAN

WAN Port	1G
IPv4 Connection Type	Static
IPv6 Connection Type	IPV6 Static
MTU	1448
IPv6 Enable	0

VLAN

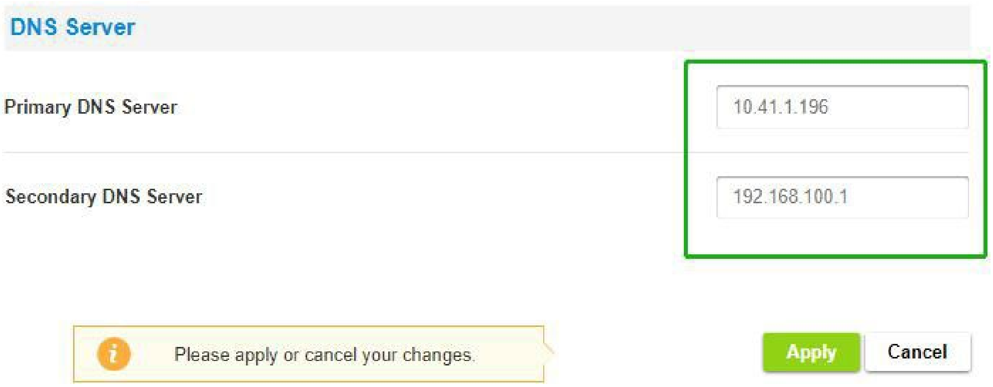
Enable VLAN	●
VLAN ID	200

Static

IP Address	10 . 41 . 6 . 17
Netmask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0

IPV6 Static

IPv6 Address	::
IPv6 Prefix Len	0
IPv6 Gateway	::



DNS Server

Primary DNS Server: 10.41.1.196

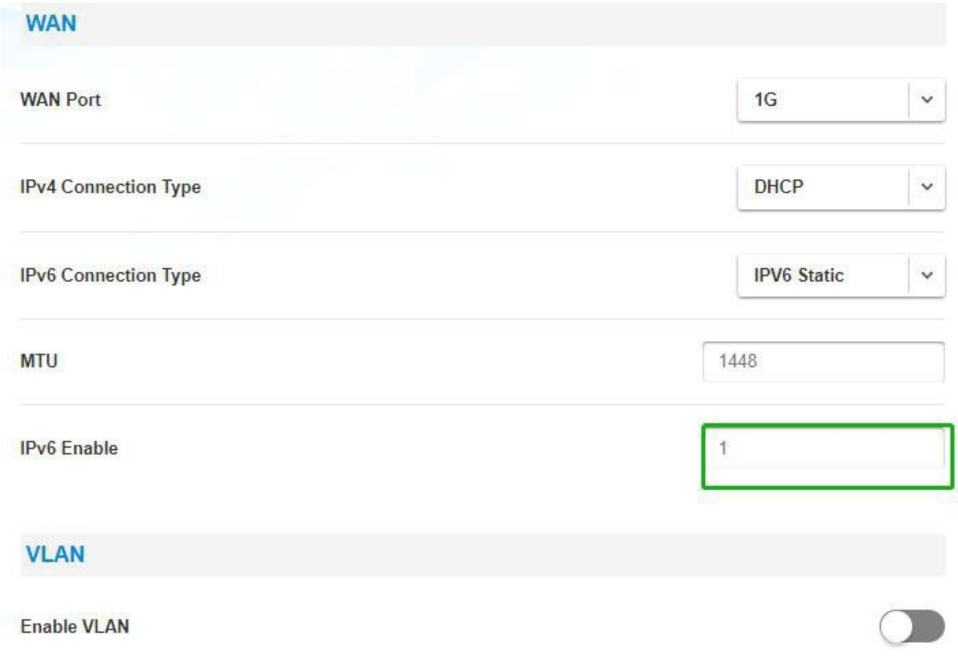
Secondary DNS Server: 192.168.100.1

Please apply or cancel your changes.

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.



WAN

WAN Port: 1G

IPv4 Connection Type: DHCP

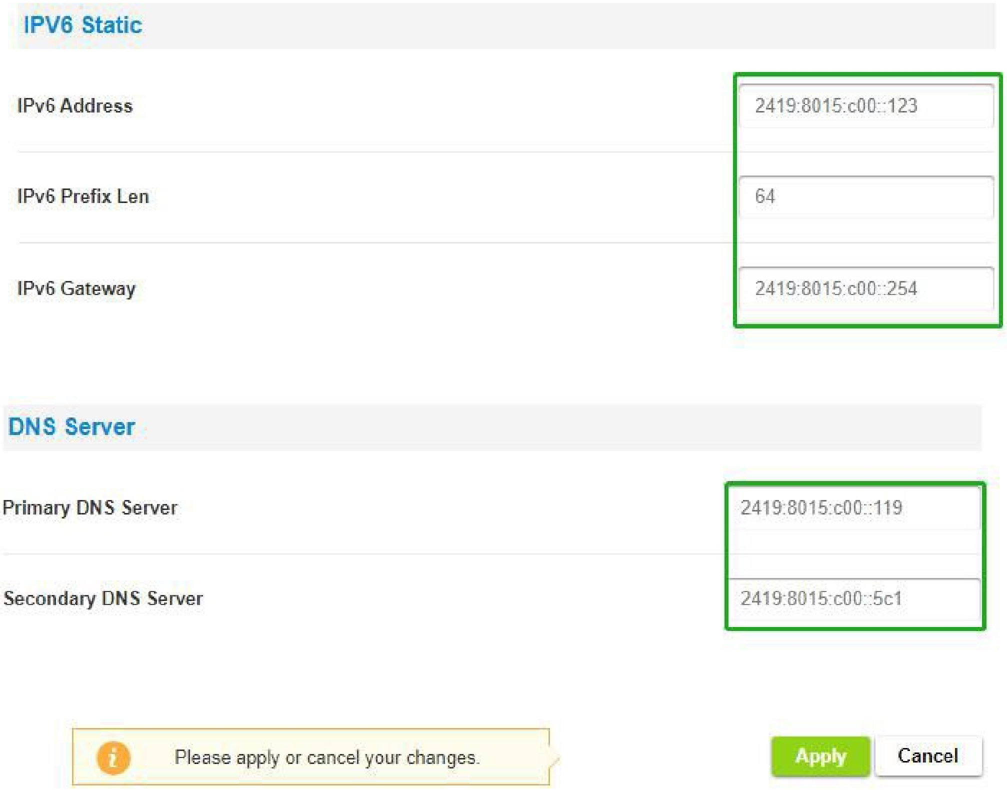
IPv6 Connection Type: IPV6 Static

MTU: 1448

IPv6 Enable: 1

VLAN

Enable VLAN



IPV6 Static

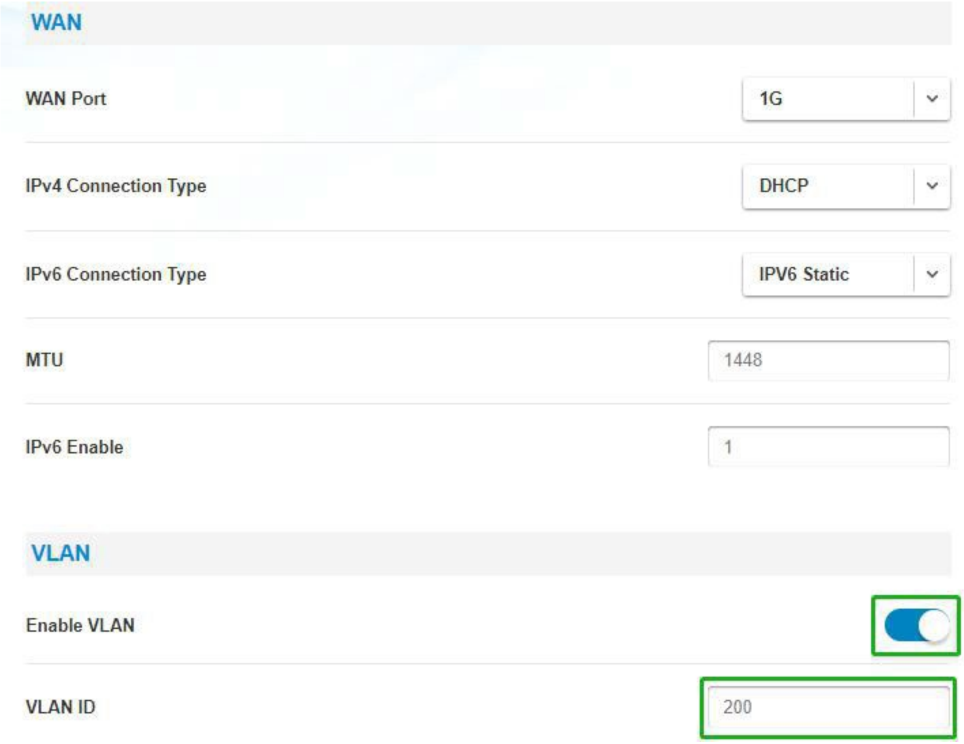
IPv6 Address	2419:8015:c00::123
IPv6 Prefix Len	64
IPv6 Gateway	2419:8015:c00::254

DNS Server

Primary DNS Server	2419:8015:c00::119
Secondary DNS Server	2419:8015:c00::5c1

Please apply or cancel your changes.

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

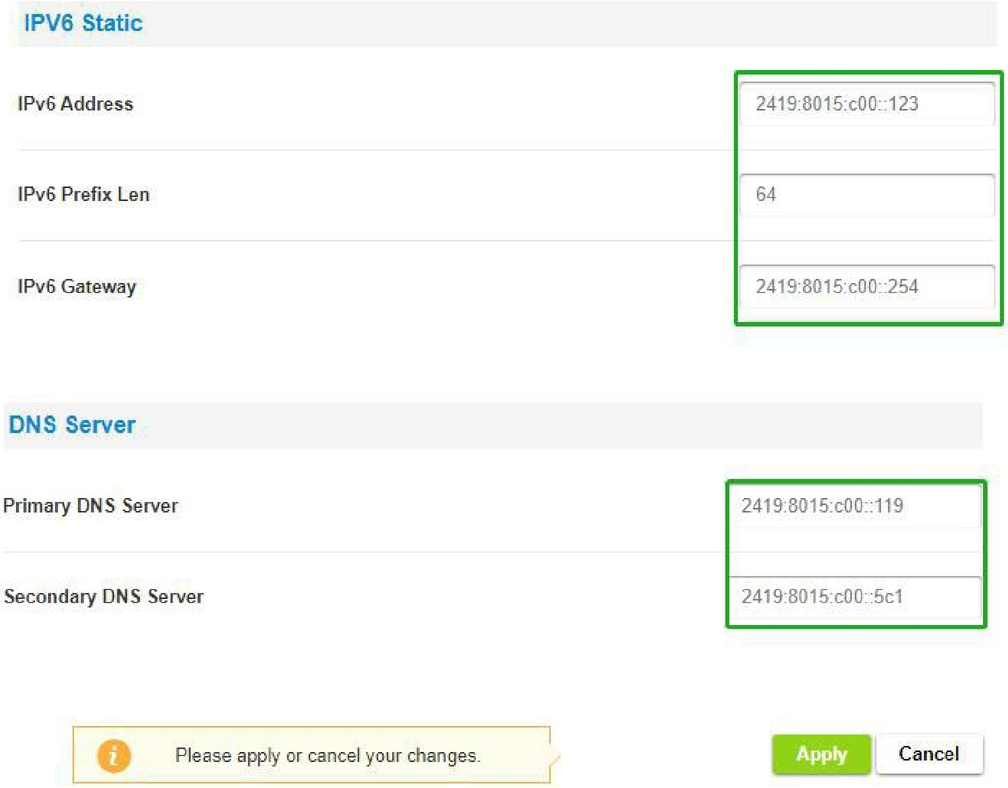


WAN

WAN Port	1G
IPv4 Connection Type	DHCP
IPv6 Connection Type	IPV6 Static
MTU	1448
IPv6 Enable	1

VLAN

Enable VLAN	●
VLAN ID	200



IPV6 Static

IPv6 Address: 2419:8015:c00::123

IPv6 Prefix Len: 64

IPv6 Gateway: 2419:8015:c00::254

DNS Server

Primary DNS Server: 2419:8015:c00::119

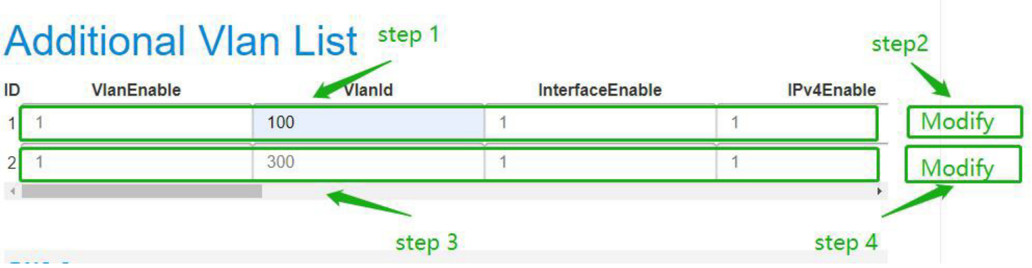
Secondary DNS Server: 2419:8015:c00::5c1

Please apply or cancel your changes.

4.1.1.5. Additional Multi-Vlan

(1) . Multi-Vlan with DHCP IPv4

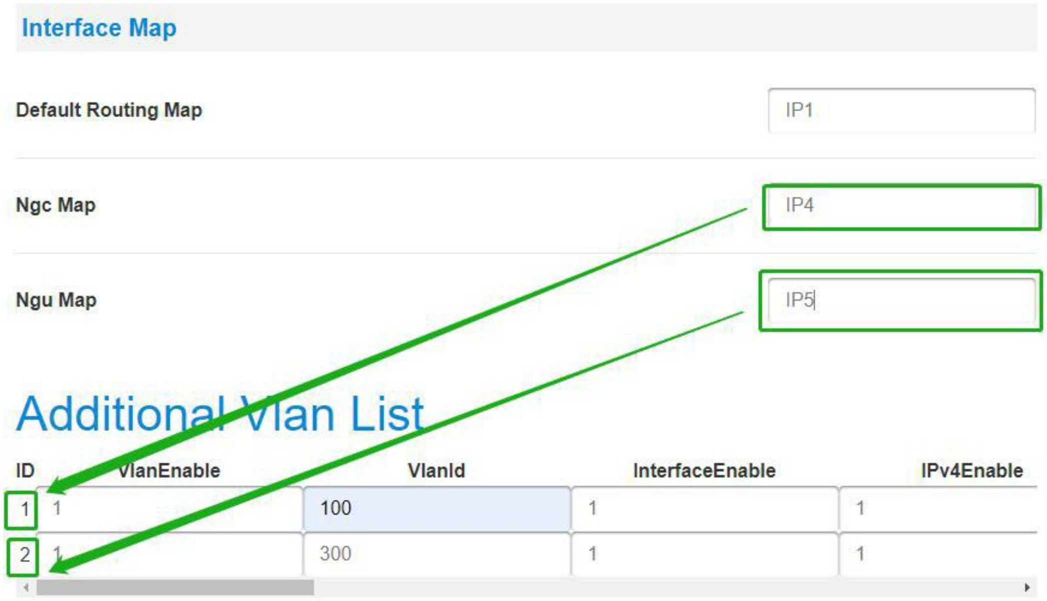
If you want configure multi-vlan, please configure the default VLAN by following instructions in 4.1.1.1(2), then you can set Additional Vlan List, VlanEnable, VlanId, InterfaceEnable, IPv4Enable and set modify to save configure



Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	1
2	1	300	1	1

After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List



Interface Map

Default Routing Map	IP1
Ngc Map	IP4
Ngu Map	IP5

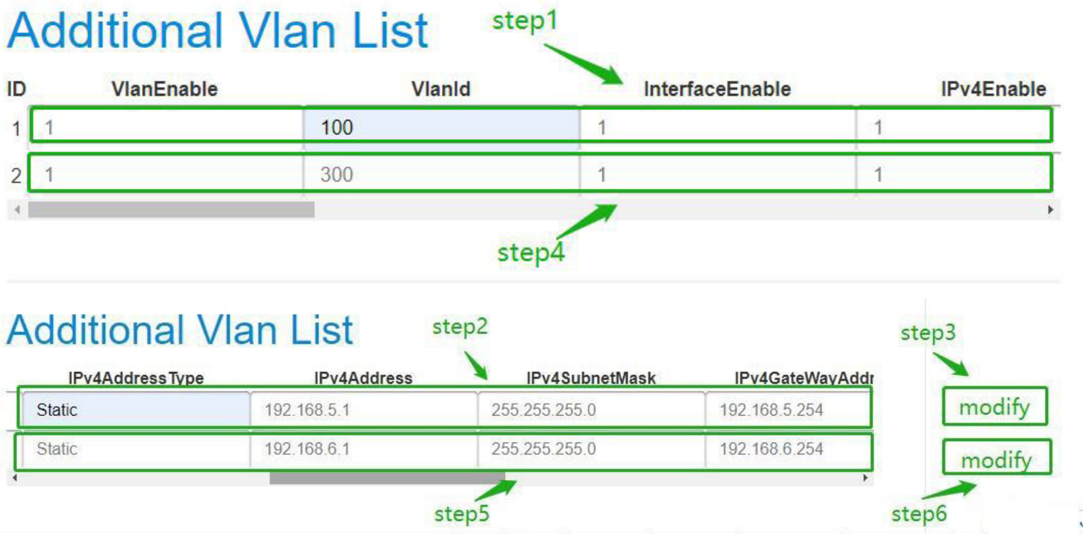
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	1
2	1	300	1	1

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

(2) . Multi-Vlan with Static IPv4

If you want 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



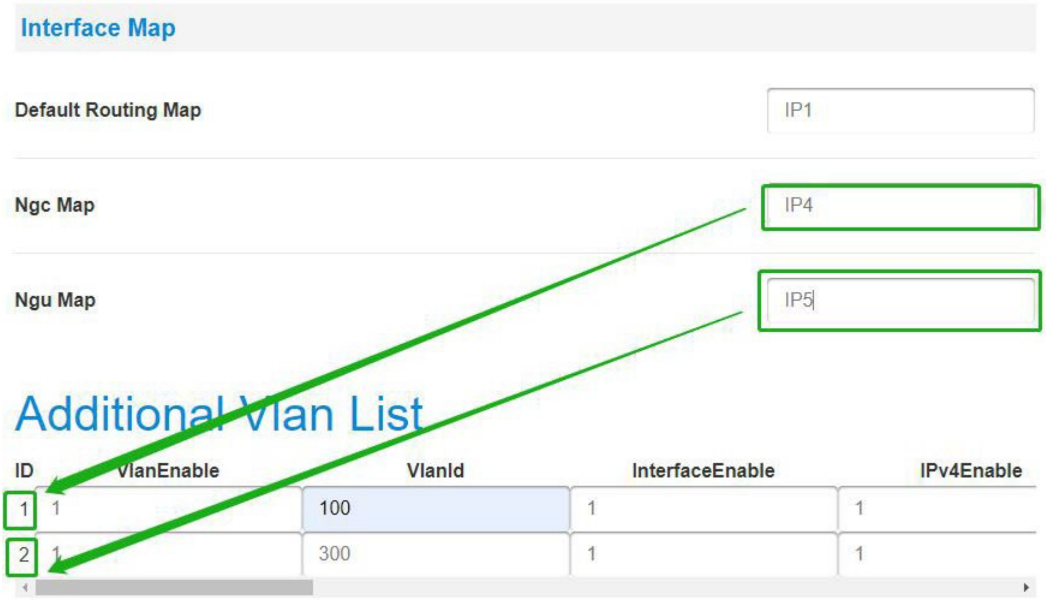
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	1
2	1	300	1	1

Additional Vlan List

IPv4AddressType	IPv4Address	IPv4SubnetMask	IPv4GateWayAddr	
Static	192.168.5.1	255.255.255.0	192.168.5.254	modify
Static	192.168.6.1	255.255.255.0	192.168.6.254	modify

After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List



Interface Map

Default Routing Map: IP1

Ngc Map: IP4

Ngu Map: IP5

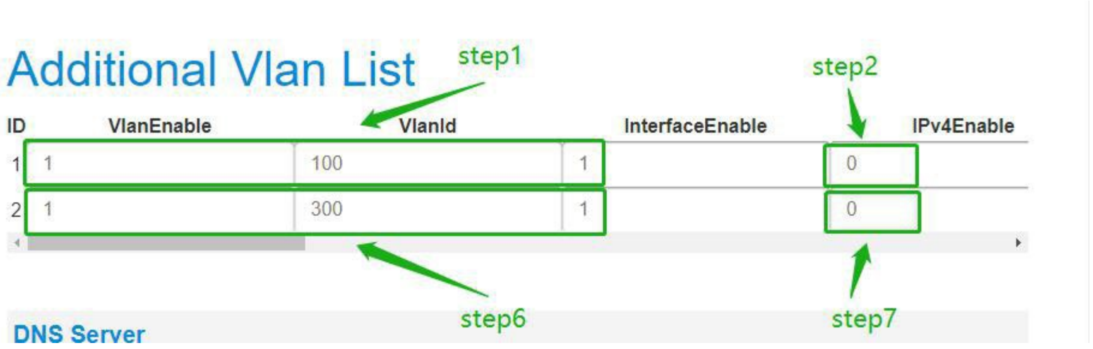
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	1
2	1	300	1	1

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

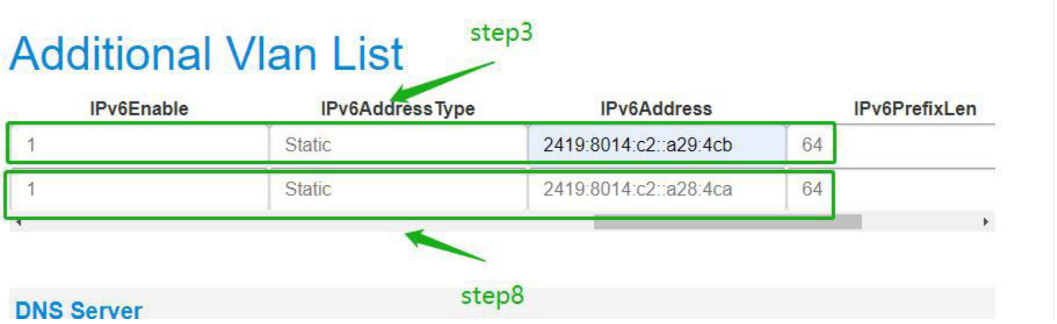
(3) . Multi-Vlan with Static IPv6

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



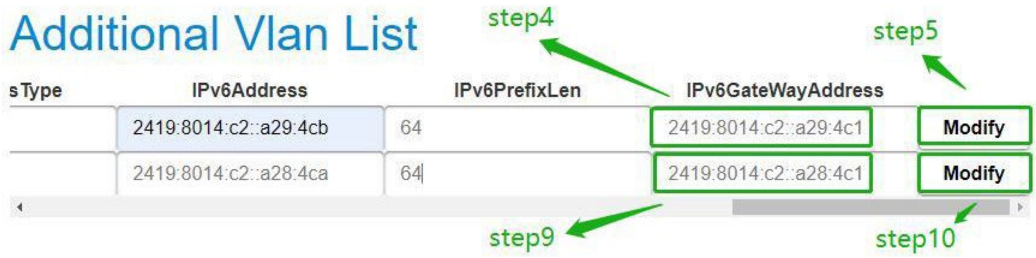
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	0
2	1	300	1	0



Additional Vlan List

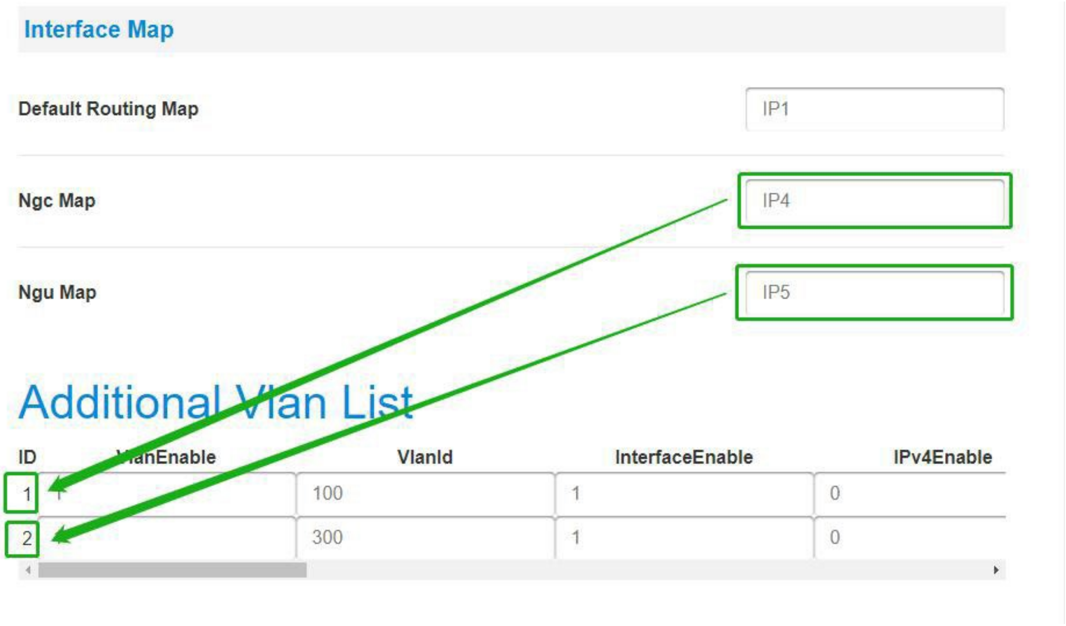
IPv6Enable	IPv6AddressType	IPv6Address	IPv6PrefixLen
1	Static	2419:8014:c2::a29:4cb	64
1	Static	2419:8014:c2::a28:4ca	64



Additional Vlan List

sType	IPv6Address	IPv6PrefixLen	IPv6GateWayAddress	
	2419:8014:c2::a29:4cb	64	2419:8014:c2::a29:4c1	Modify
	2419:8014:c2::a28:4ca	64	2419:8014:c2::a28:4c1	Modify

After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List



Interface Map

Default Routing Map	IP1
Ngc Map	IP4
Ngu Map	IP5

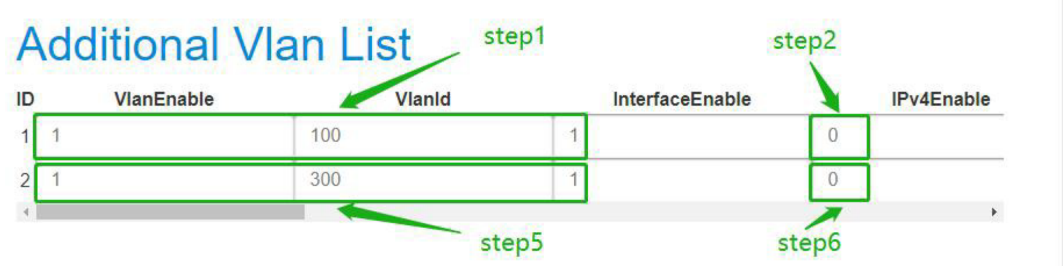
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1		100	1	0
2		300	1	0

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

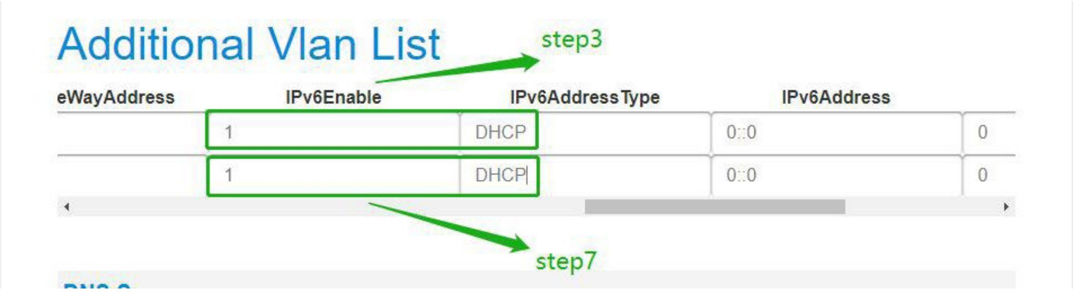
(4) . Multi-Vlan with DHCP IPv6

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 (Only DHCP and AUTO can be configured,DHCP corresponds to Stateful ipv6;AUTO corresponds to Stateles ipv6), set modify to save configure



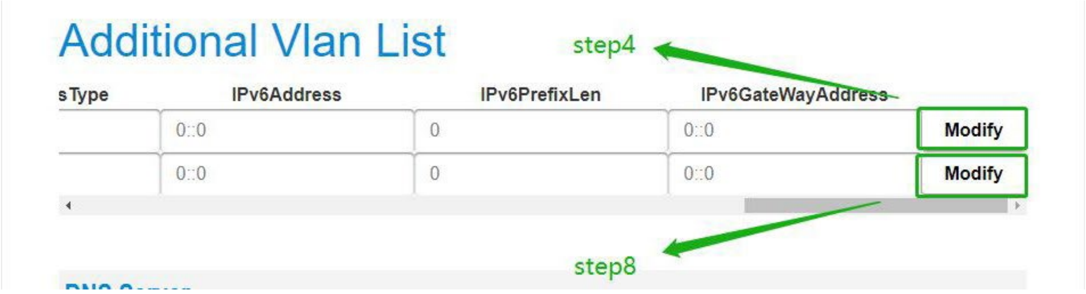
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	0
2	1	300	1	0



Additional Vlan List

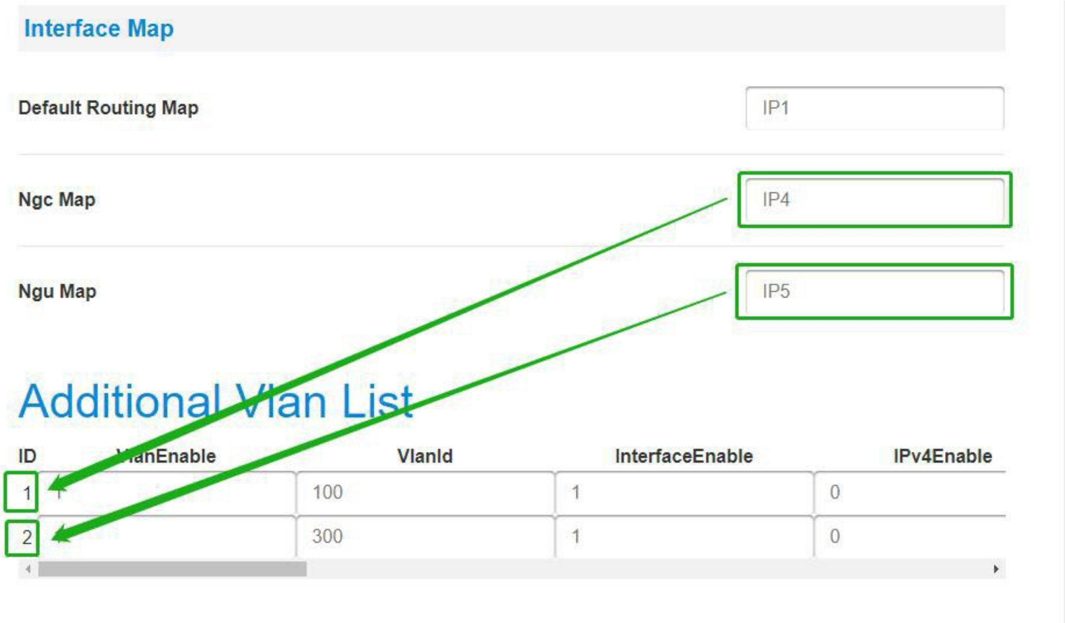
eWayAddress	IPv6Enable	IPv6AddressType	IPv6Address	
	1	DHCP	0::0	0
	1	DHCP	0::0	0



Additional Vlan List

sType	IPv6Address	IPv6PrefixLen	IPv6GateWayAddress	
	0::0	0	0::0	Modify
	0::0	0	0::0	Modify

After the additional VLANList is configured, configure NGC/NGU Map to correspond to ID1/2 in the Additional Vlan List



Interface Map

Default Routing Map	IP1
Ngc Map	IP4
Ngu Map	IP5

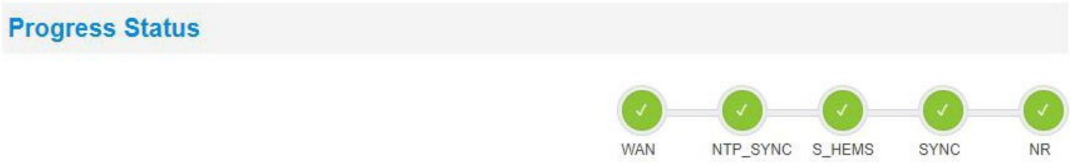
Additional Vlan List

ID	VlanEnable	VlanId	InterfaceEnable	IPv4Enable
1	1	100	1	0
2		300	1	0

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.

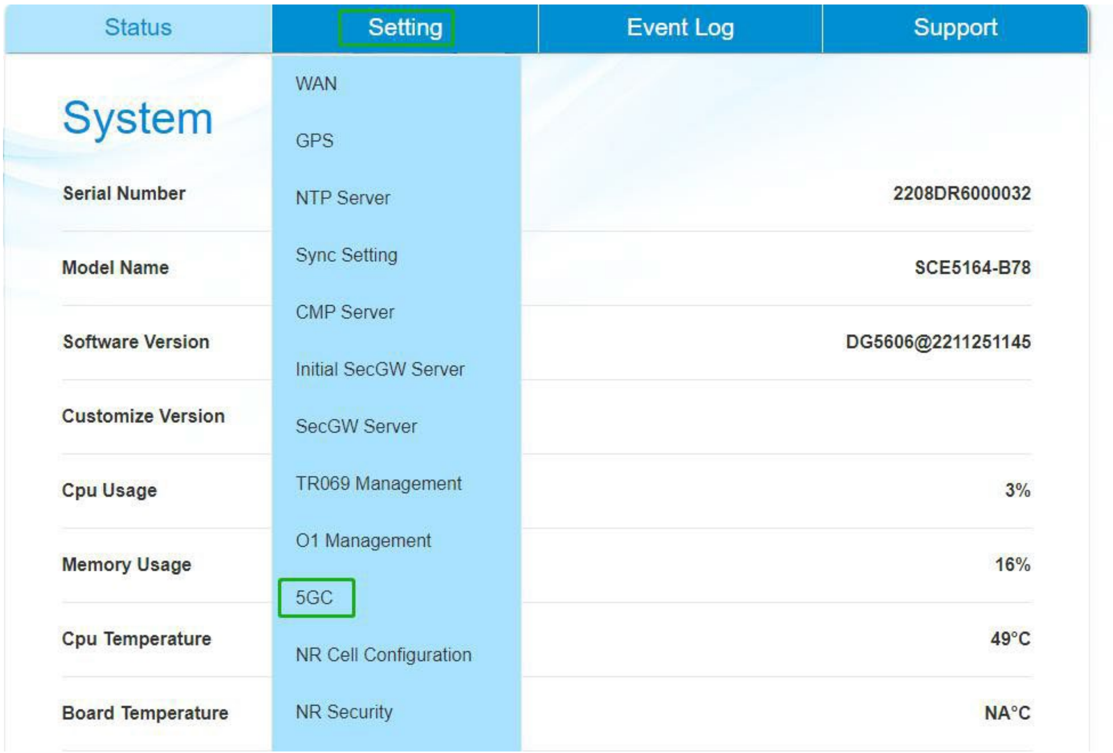


If WAN is not green, please follow below steps to check it.

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

4.2. 5GC Setting

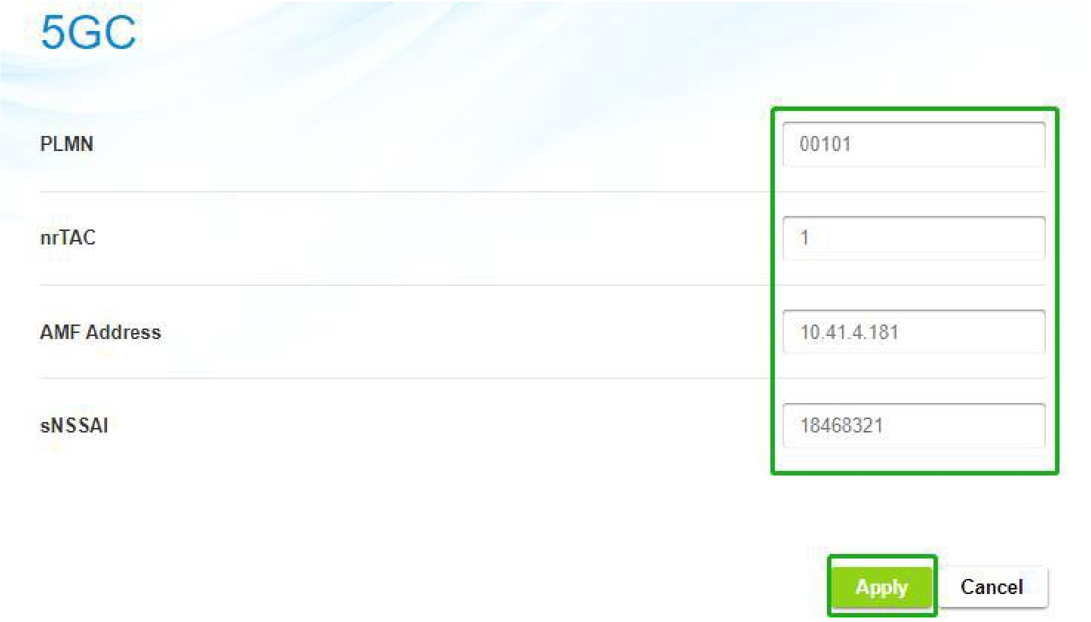
Please go through “Setting” -> “5GC” to configuring.



System

Serial Number	2208DR6000032
Model Name	SCE5164-B78
Software Version	DG5606@2211251145
Customize Version	
Cpu Usage	3%
Memory Usage	16%
Cpu Temperature	49°C
Board Temperature	NA°C

In this page, you need to set PLMN, TAC, AMF address and sNSSAI.



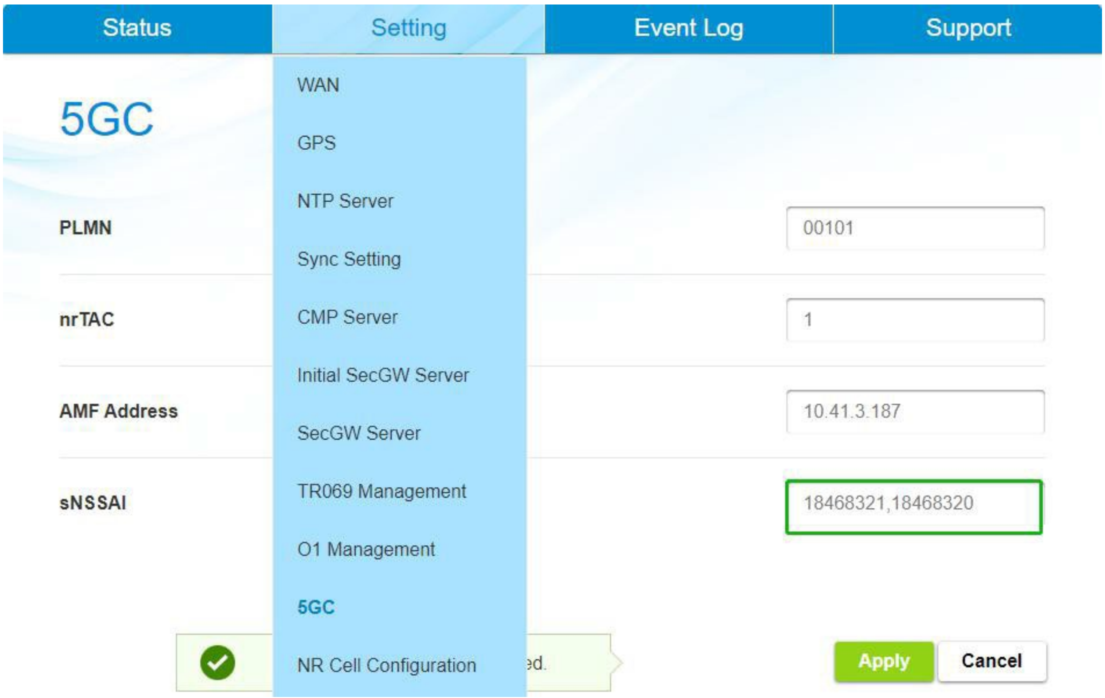
5GC

PLMN: 00101

nrTAC: 1

AMF Address: 10.41.4.181

sNSSAI: 18468321



5GC

PLMN: 00101

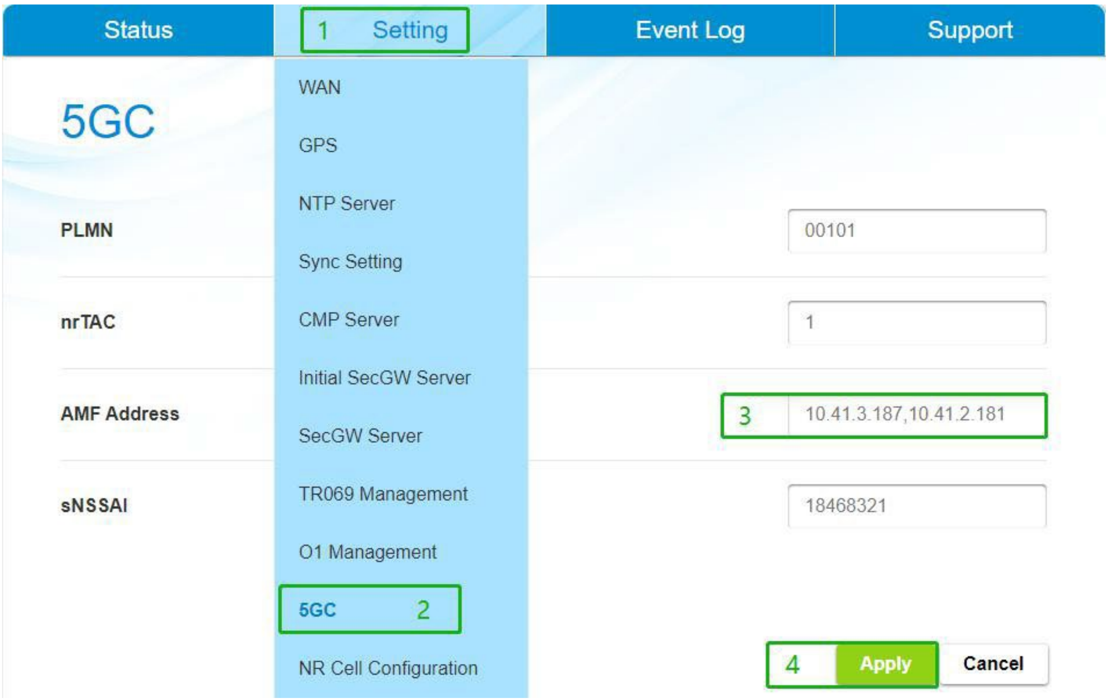
nrTAC: 1

AMF Address: 10.41.3.187

sNSSAI: 18468321,18468320

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.



5GC

PLMN: 00101

nrTAC: 1

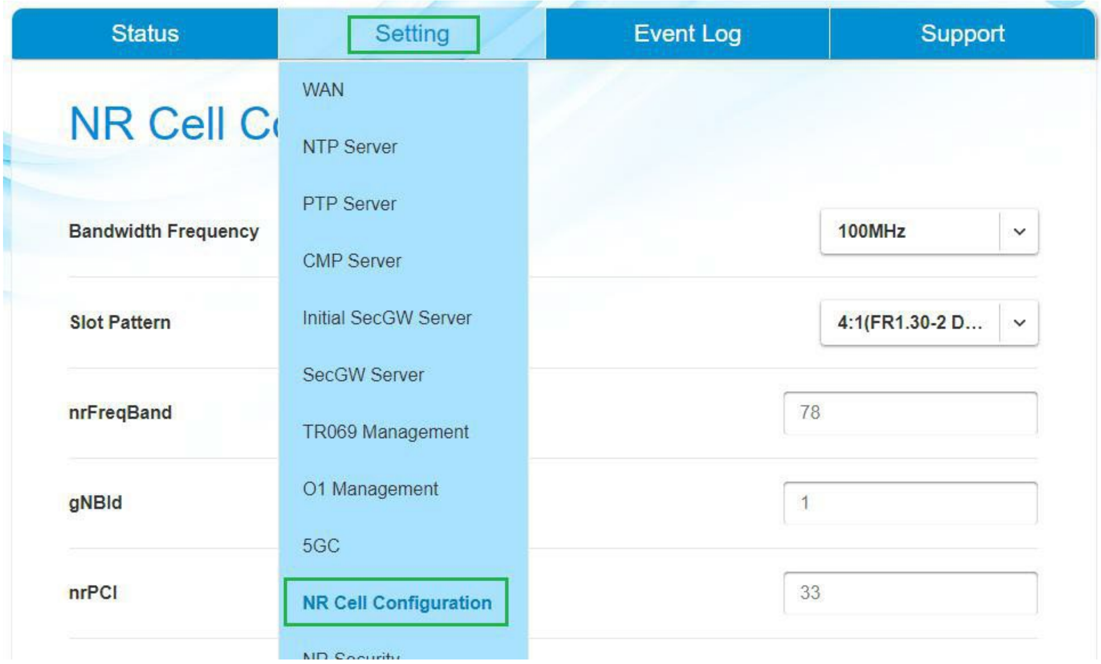
AMF Address: 10.41.3.187,10.41.2.181

sNSSAI: 18468321

Tips. PLMN, TAC and sNSSAI are decimal. sNSSAI is composed of sST and sD, for example: sST is 0x01, sD is 0x000001, 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.



Bandwidth Frequency: 100MHz

Slot Pattern: 4:1(FR1.30-2 D...

nrFreqBand: 78

gNBId: 1

nrPCI: 33

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

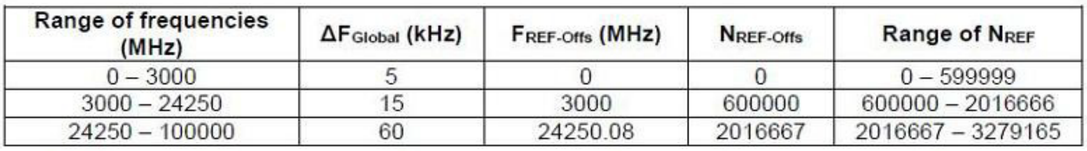
$N0 = (\text{StartFreq} - 3000 + 7.92) / 1.44$

$N = \text{RoundUptoInter}(N0)$

$\text{SSBFreq} = (3000 + N * 1.44) * 1000$

Utilize the below formula to calculate the SSBArfcn from SSBFreq

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



Range of frequencies (MHz)	ΔF_{Global} (kHz)	$F_{REF-Offs}$ (MHz)	$N_{REF-Offs}$	Range of N_{REF}
0 – 3000	5	0	0	0 – 599999
3000 – 24250	15	3000	600000	600000 – 2016666
24250 – 100000	60	24250.08	2016667	2016667 – 3279165

$\text{SSBArfcn} = (\text{SSBFreq} - \text{F\_REF\_OFFS})/\Delta\text{F\_Global} + \text{N\_REF\_OFFS}$

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

Then

$N0 = (3500-3000+7.92)/1.44=352.7$

$N = \text{RoundUptoInter}(352.7) = 353$

SSBFreq = (3000 + 353 * 1.44) * 1000 = 3508320

The SSBFreq 3508320kHz is between 3000~24250MHz, so:

SSBArfcn = (3508320-3000000)/15+600000 = 633888

Notice:

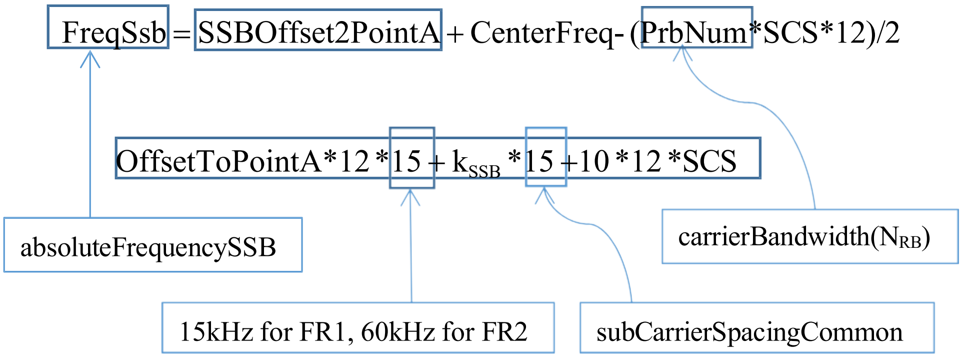
The start Freq is united by MHz.

The SSBFreq is unitied by kHz.

4.3.1.2. Calculate Center Arfcn

Calculate centerFreq then calculate the CenterArfcncorresponding to the centerfreq as known as dlEarfcn.

CenterFreq and FreqSsb must match below formula:



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

OffsetToPointA*12 *15 + k_{SSB} *15 +10 *12 *SCS

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

Tips: the unit for frequency is kHz, k_{SSB} 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:

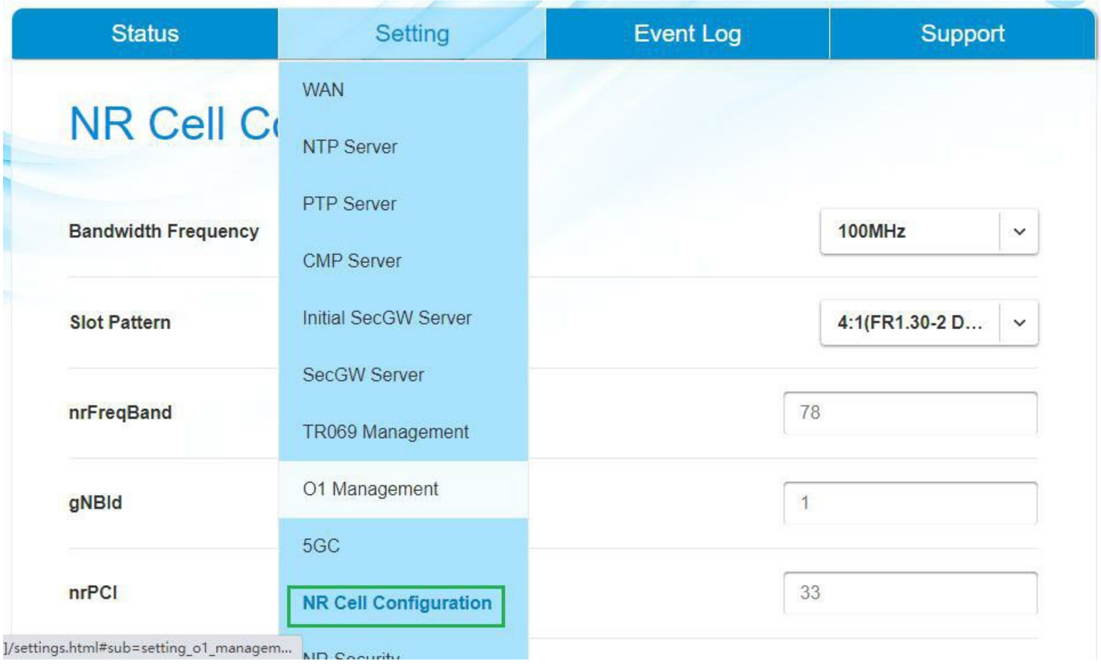
FreqSsb is 3708480, bandwidth is 100MHz, OffsetToPointA is 24 PRBs (default value), SCS is 30 kHz. Following the formula, CenterFreq = 3708480 - 24*12*15 - 0*15 - 10*12*30 + (273*30*12)/2 = 3749700 kHz.

The CenterFreq 3749700kHz is between 3000~24250MHz, so:

CenterArfcn = (3749700-3000000)/15+600000 = 649980

4.3.1.3. Configuration

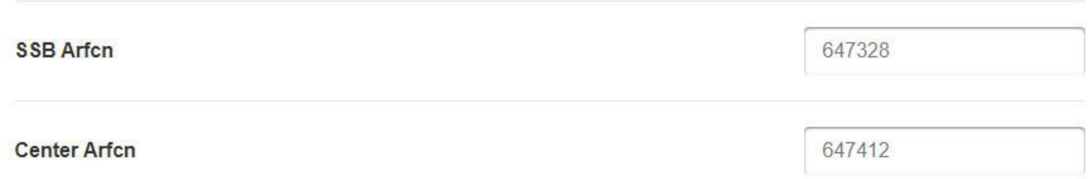
Login WebGUI, go through “Setting” -> “NR Cell”.



Bandwidth Frequency	100MHz
Slot Pattern	4:1(FR1.30-2 D...
nrFreqBand	78
gNBId	1
nrPCI	33

4.3.1.3.1. Using Default OffsetToPointA (24 PRBs)

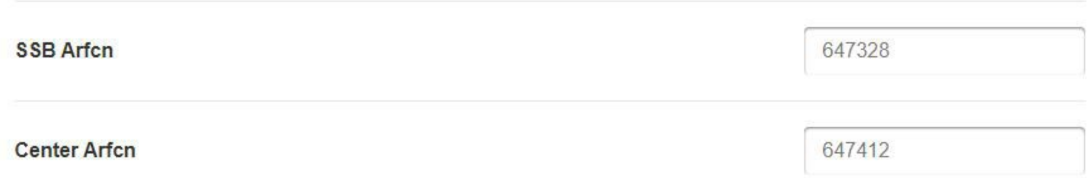
- ➢ Configure SSB Arfcn, Center Arfcn;
- ➢ Click apply;
- ➢ Reboot



SSB Arfcn	647328
Center Arfcn	647412

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



SSB Arfcn	647328
Center Arfcn	647412

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.

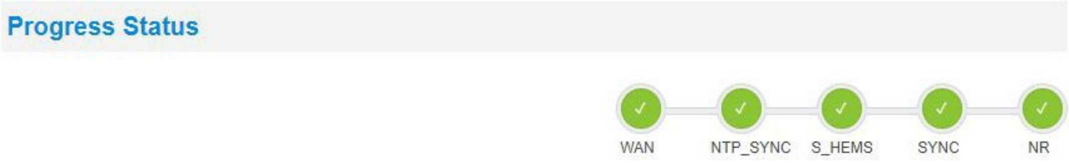
5. Advance Setting

5.1. NTP Server Setting

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

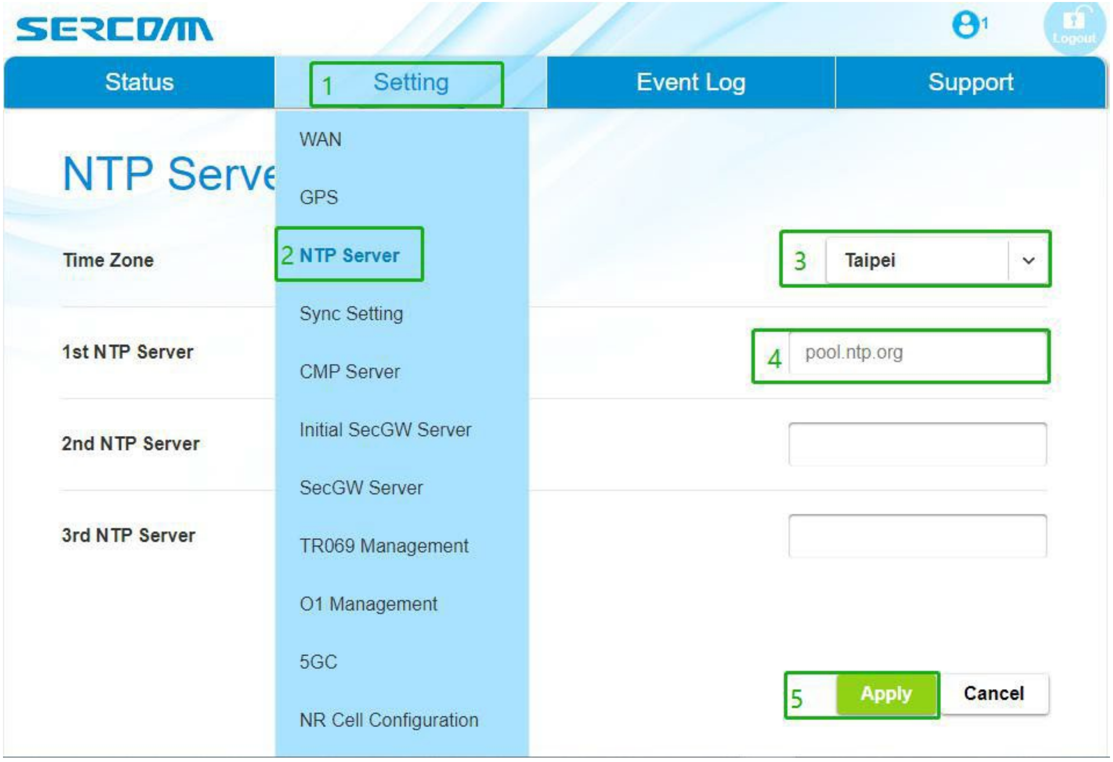
son statem on NTP_SYNC

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



5.1.1. Configuration

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



NTP Serve

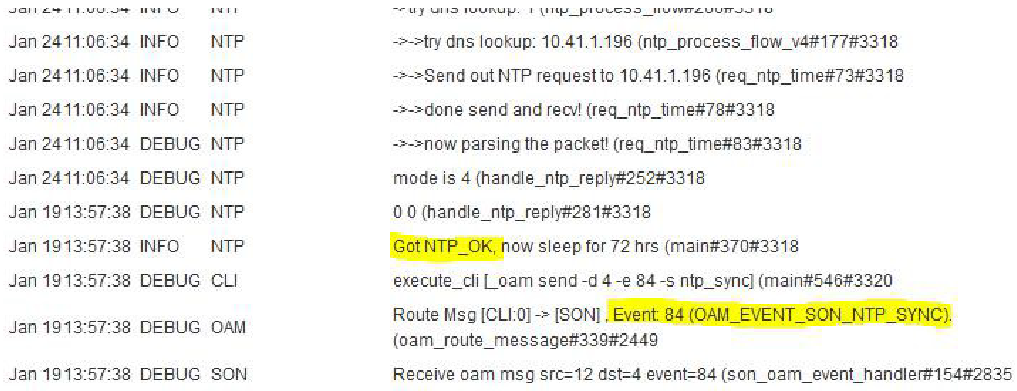
Time Zone: Taipei

1st NTP Server: pool.ntp.org

2nd NTP Server:

3rd NTP Server:

5.1.2. Success Log



```
Jan 24 11:06:34  INFO    NTP     ->->try dns lookup: 1 (ntp_process_flow#206#3318
Jan 24 11:06:34  INFO    NTP     ->->try dns lookup: 10.41.1.196 (ntp_process_flow_v4#177#3318
Jan 24 11:06:34  INFO    NTP     ->->Send out NTP request to 10.41.1.196 (req_ntp_time#73#3318
Jan 24 11:06:34  INFO    NTP     ->->done send and recv! (req_ntp_time#78#3318
Jan 24 11:06:34  DEBUG   NTP     ->->now parsing the packet! (req_ntp_time#83#3318
Jan 24 11:06:34  DEBUG   NTP     mode is 4 (handle_ntp_reply#252#3318
Jan 19 13:57:38  DEBUG   NTP     0 0 (handle_ntp_reply#281#3318
Jan 19 13:57:38  INFO    NTP     Got NTP_OK, now sleep for 72 hrs (main#370#3318
Jan 19 13:57:38  DEBUG   CLI     execute_cli [_oam send -d 4 -e 84 -s ntp_sync] (main#546#3320
                                 Route Msg [CLI:0] -> [SON] , Event: 84 (OAM_EVENT_SON_NTP_SYNC).
Jan 19 13:57:38  DEBUG   OAM     (oam_route_message#339#2449
Jan 19 13:57:38  DEBUG   SON     Receive oam msg src=12 dst=4 event=84 (son_oam_event_handler#154#2835
```

5.1.3. Trouble Shooting

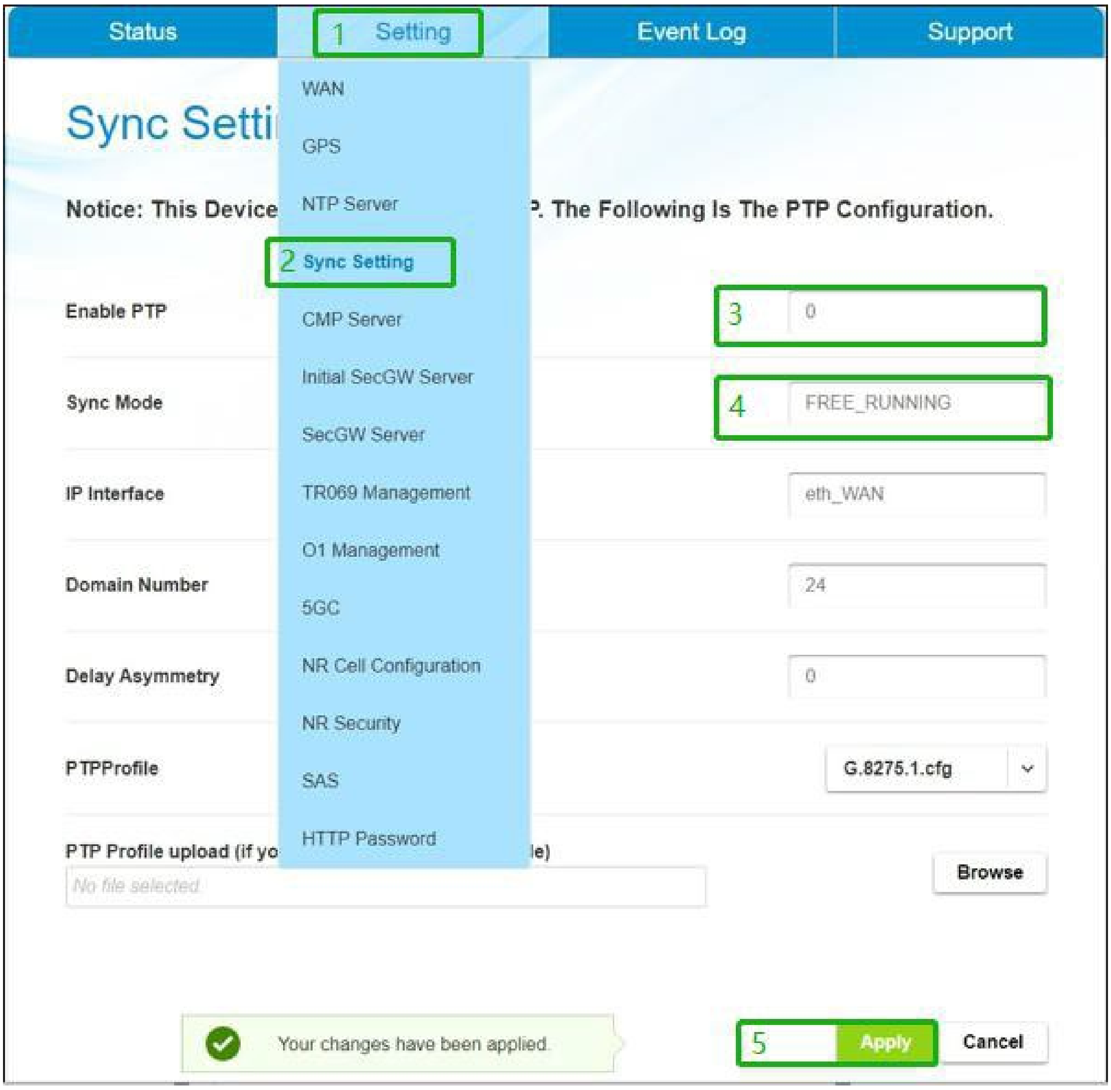
- Check NTP server working fine;
- Check NTP server address is correct;
- Check Bridgestone can connect to NTP server.

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



Sync Setti

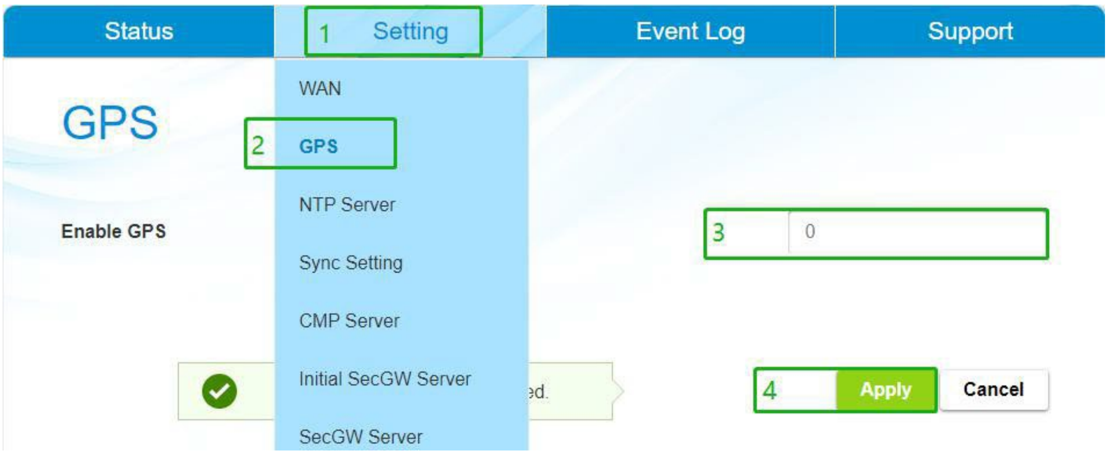
Notice: This Device P. The Following Is The PTP Configuration.

Enable PTP	0
Sync Mode	FREE_RUNNING
IP Interface	eth_WAN
Domain Number	24
Delay Asymmetry	0
PTPProfile	G.8275.1.cfg

PTP Profile upload (if yo le)

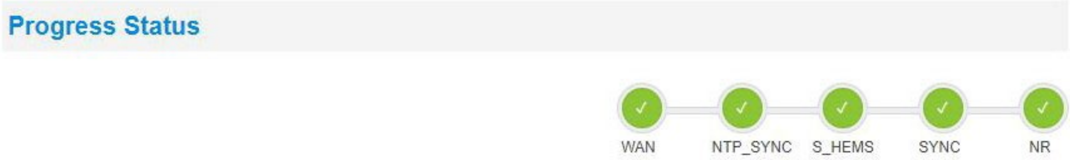
No file selected

Your changes have been applied.



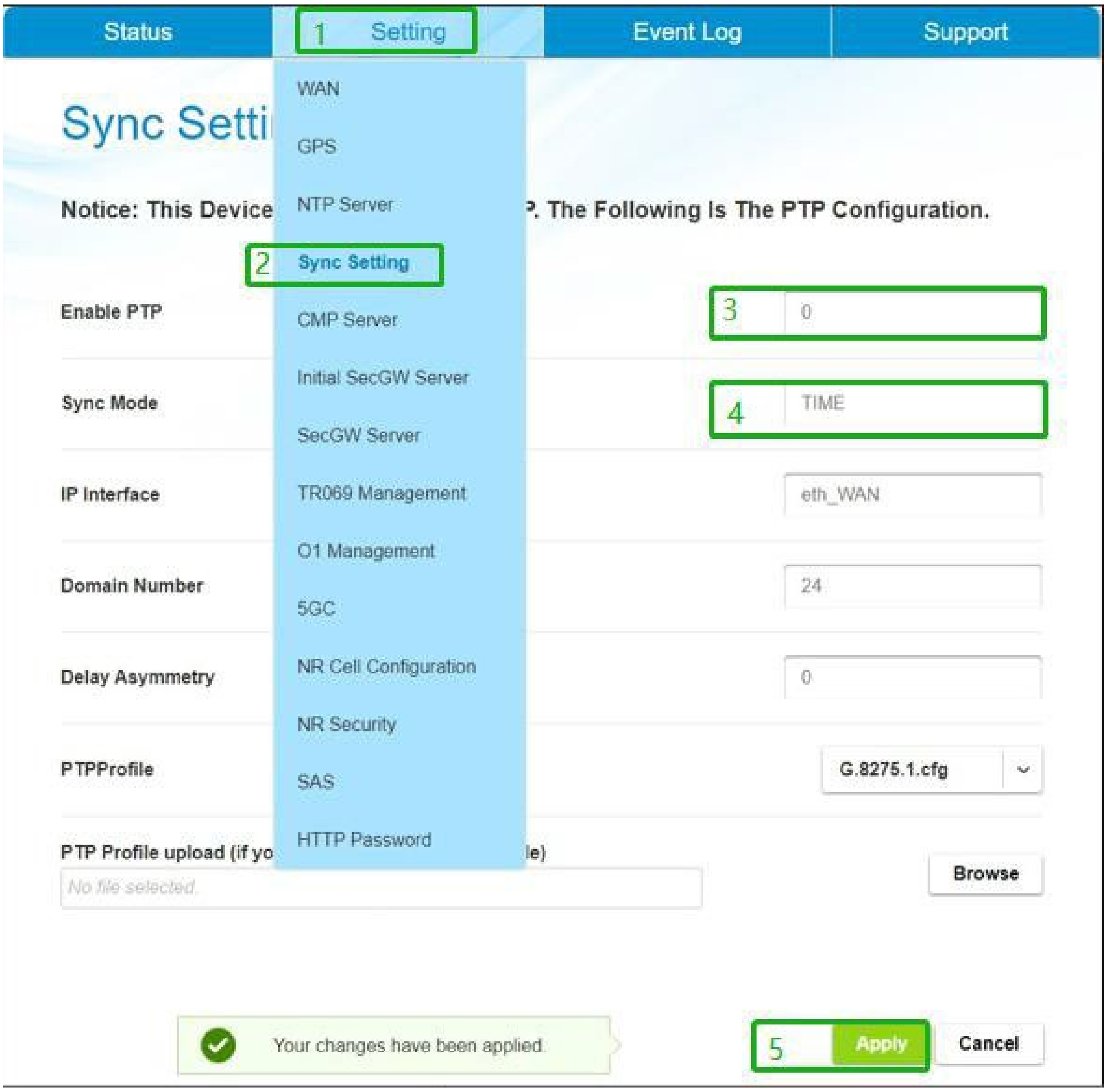
5.2.2. Sync

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



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 Setti

Notice: This Device ... . The Following Is The PTP Configuration.

Enable PTP: 0

Sync Mode: TIME

IP Interface: eth_WAN

Domain Number: 24

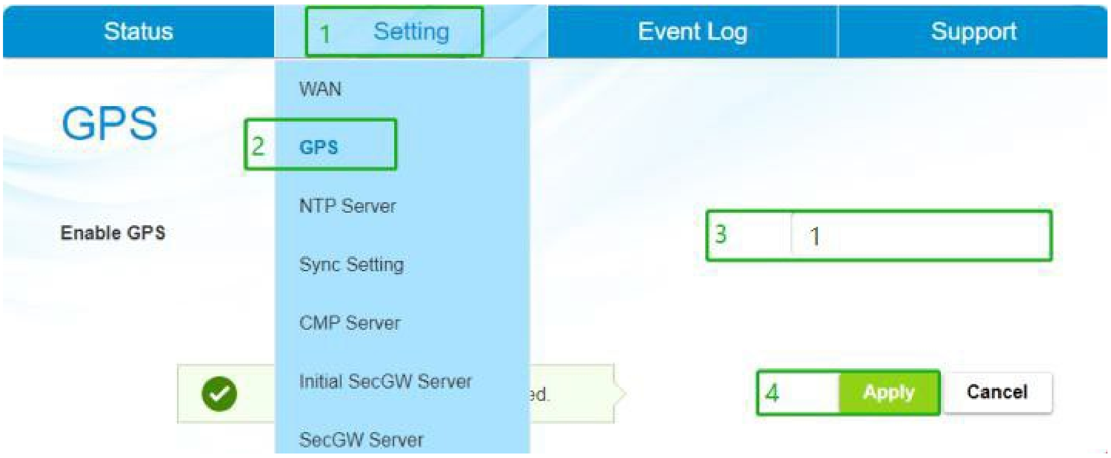
Delay Asymmetry: 0

PTPProfile: G.8275.1.cfg

PTP Profile upload (if yo ... le)

No file selected

Your changes have been applied.



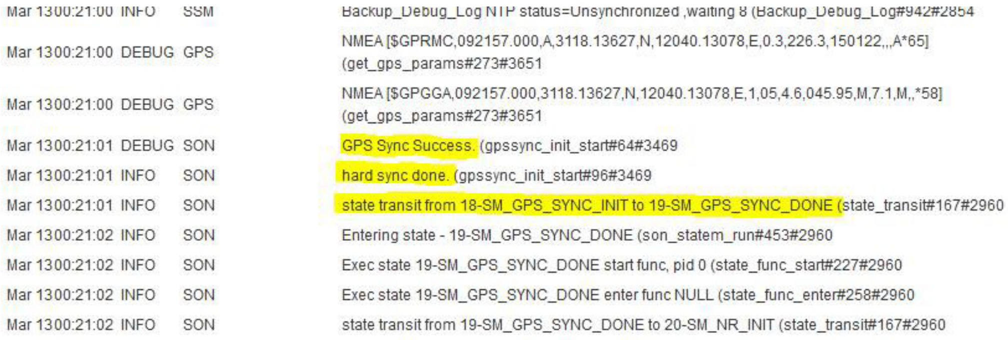
GPS

Enable GPS: 1

...ed.

5.2.2.2. Success Log

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



```
Mar 1300:21:00  INFO   SSM    Backup_Debug_Log NTP status=Unsynchronized ,waiting 8 (Backup_Debug_Log#942#2854
Mar 1300:21:00  DEBUG  GPS    NMEA [$GPRMC,092157.000,A,3118.13627,N,12040.13078,E,0.3,226.3,150122,,,A*65]
                              (get_gps_params#273#3651
Mar 1300:21:00  DEBUG  GPS    NMEA [$GPGGA,092157.000,3118.13627,N,12040.13078,E,1,05,4.6,045.95,M,7.1,M,,*58]
                              (get_gps_params#273#3651
Mar 1300:21:01  DEBUG  SON    GPS Sync Success. (gpssync_init_start#64#3469
Mar 1300:21:01  INFO   SON    hard sync done. (gpssync_init_start#96#3469
Mar 1300:21:01  INFO   SON    state transit from 18-SM_GPS_SYNC_INIT to 19-SM_GPS_SYNC_DONE (state_transit#167#2960
Mar 1300:21:02  INFO   SON    Entering state - 19-SM_GPS_SYNC_DONE (son_statem_run#453#2960
Mar 1300:21:02  INFO   SON    Exec state 19-SM_GPS_SYNC_DONE start func, pid 0 (state_func_start#227#2960
Mar 1300:21:02  INFO   SON    Exec state 19-SM_GPS_SYNC_DONE enter func NULL (state_func_enter#258#2960
Mar 1300:21:02  INFO   SON    state transit from 19-SM_GPS_SYNC_DONE to 20-SM_NR_INIT (state_transit#167#2960
```

5.2.2.3. Trouble Shooting

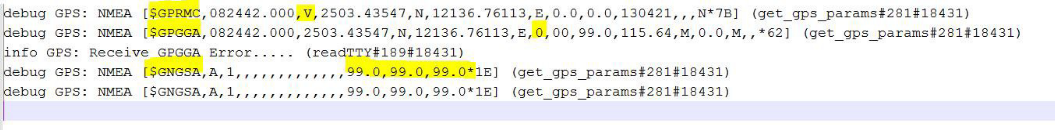
- GPS sync failed

Check NMEA message log.

GPRMC: A:GPS fix,V:Not Fixed.

GPGGA: 0=invalid; 1=GPS fix; 2=Diff. GPS fix

GNGSA: 99.0 mean not fix



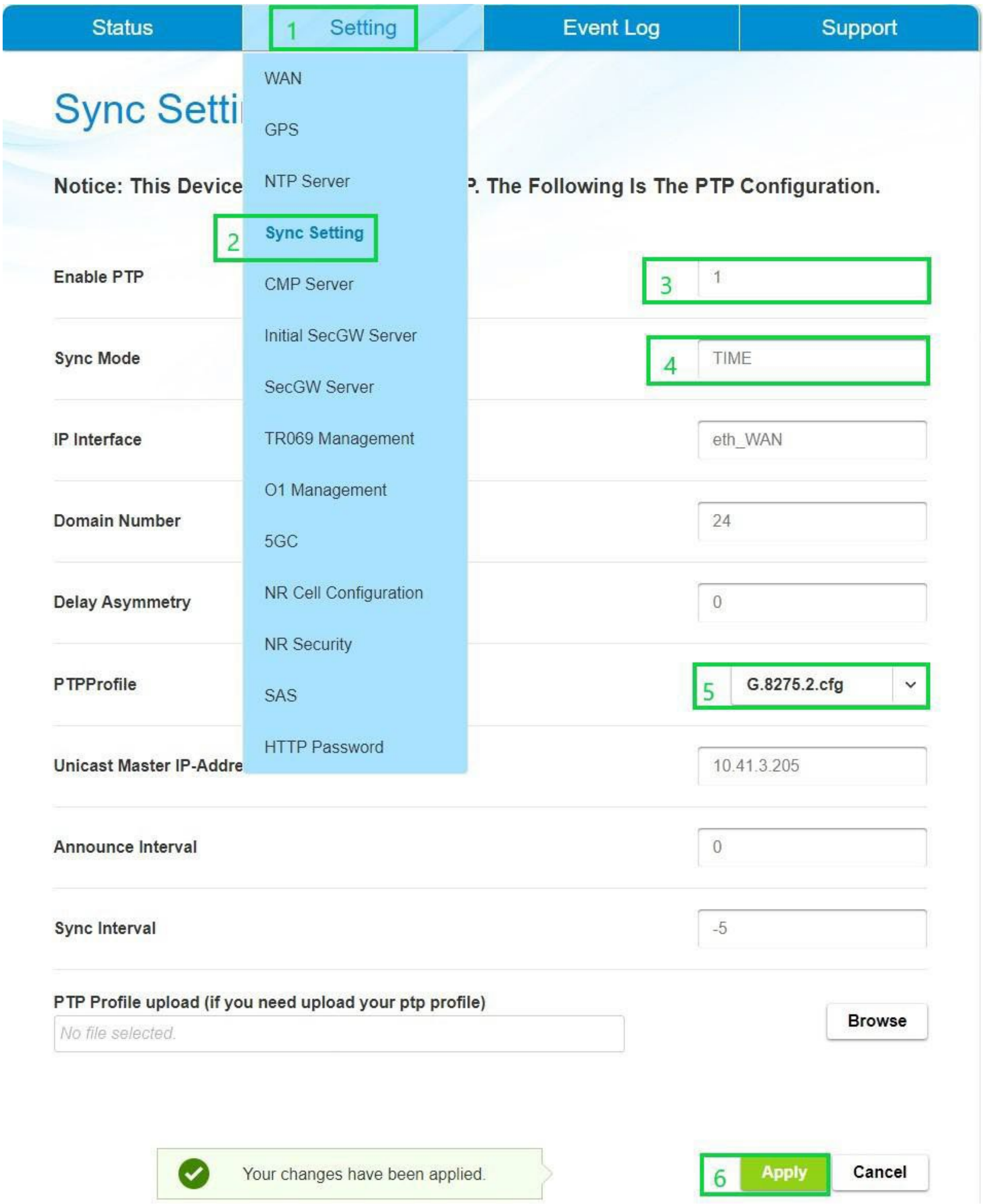
```
debug GPS: NMEA [$GPRMC,082442.000,V,2503.43547,N,12136.76113,E,0.0,0.0,130421,,,N*7B] (get_gps_params#281#18431)
debug GPS: NMEA [$GPGGA,082442.000,2503.43547,N,12136.76113,E,0,00,99.0,115.64,M,0.0,M,,*62] (get_gps_params#281#18431)
info GPS: Receive GPGGA Error..... (readTTY#189#18431)
debug GPS: NMEA [$GNGSA,A,1,,,,,,,,,,,,,99.0,99.0,99.0*1E] (get_gps_params#281#18431)
debug GPS: NMEA [$GNGSA,A,1,,,,,,,,,,,,,99.0,99.0,99.0*1E] (get_gps_params#281#18431)
```

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



Sync Setti

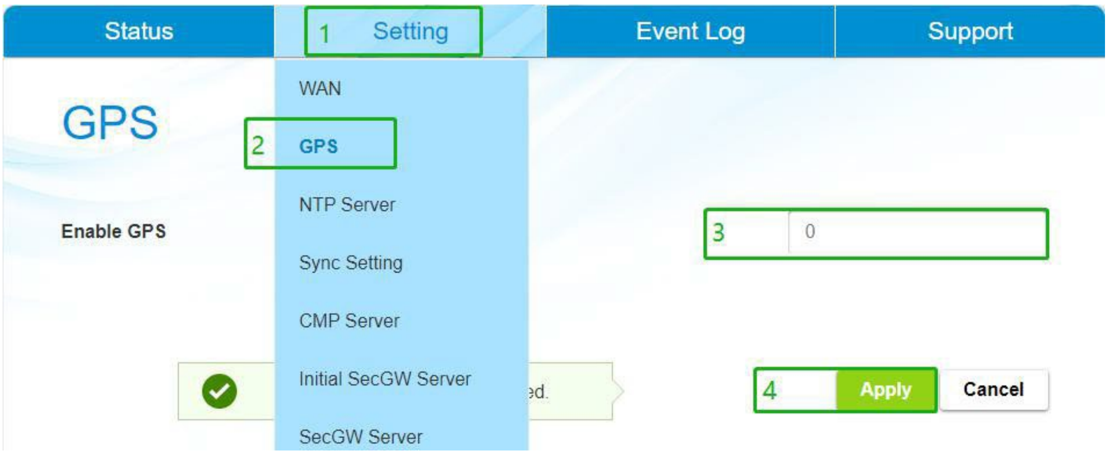
Notice: This Device … P. The Following Is The PTP Configuration.

Enable PTP	1
Sync Mode	TIME
IP Interface	eth_WAN
Domain Number	24
Delay Asymmetry	0
PTPProfile	G.8275.2.cfg
Unicast Master IP-Addre	10.41.3.205
Announce Interval	0
Sync Interval	-5

PTP Profile upload (if you need upload your ptp profile)

No file selected.

Your changes have been applied.



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.

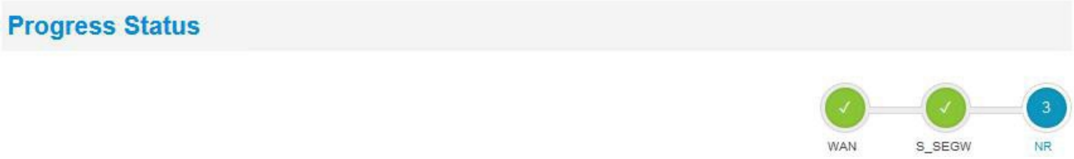
5.2.3.2. Trouble Shooting

- 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.

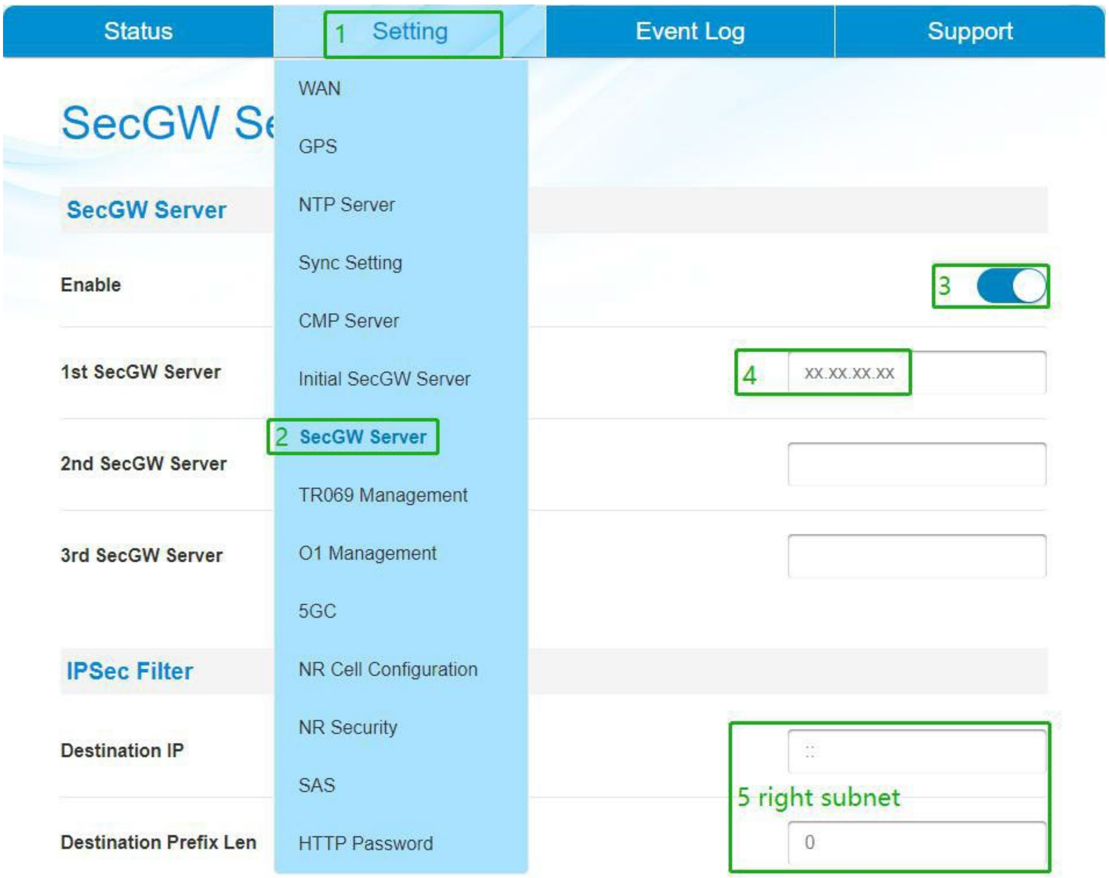


5.3.1. PSK Authentication

5.3.1.1. Configuration

- Follow below figure to configure PSK authentication;

- Reboot.



SecGW Se

SecGW Server

Enable

1st SecGW Server xx.xx.xx.xx

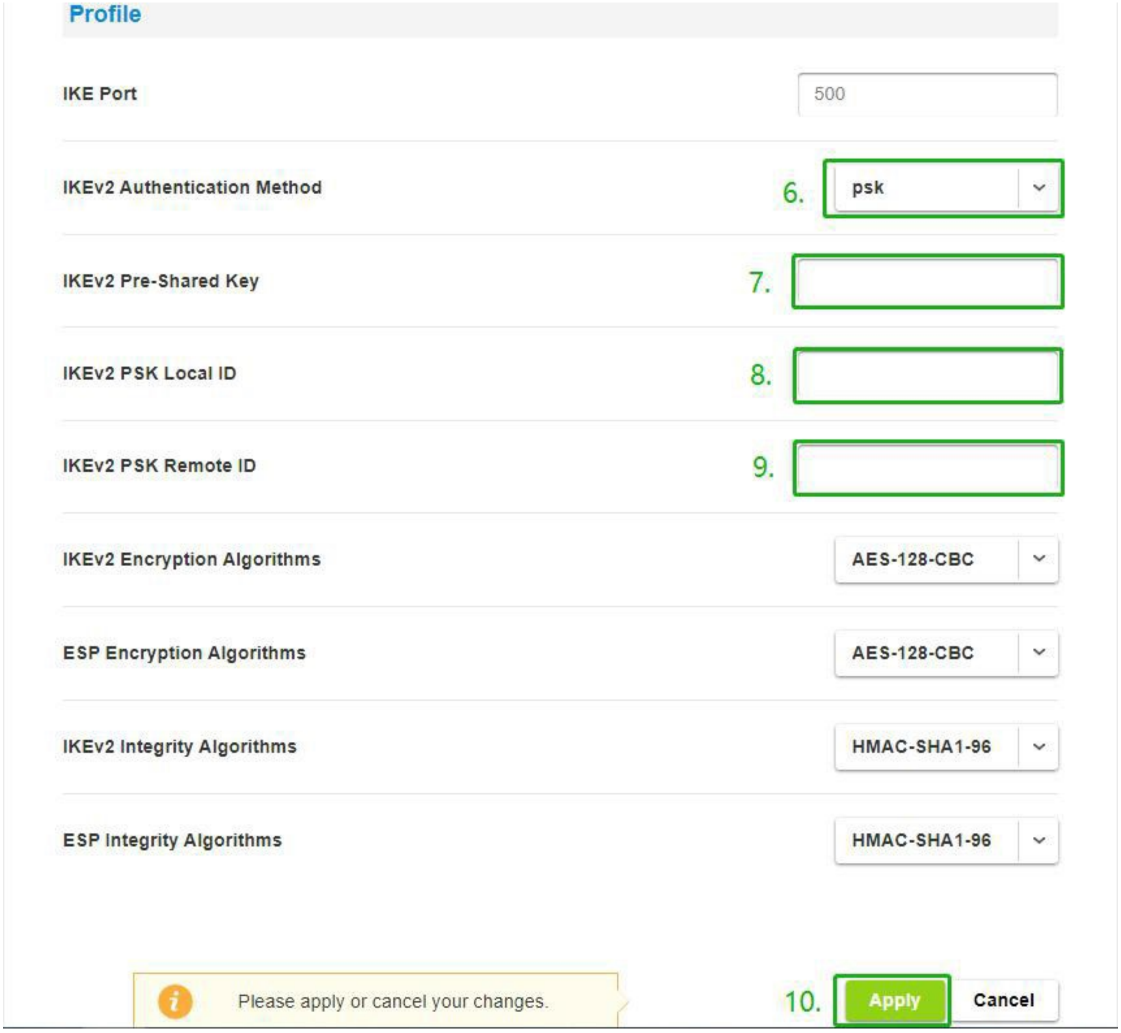
2nd SecGW Server

3rd SecGW Server

IPSec Filter

Destination IP ::

Destination Prefix Len 0



Profile

IKE Port: 500

IKEv2 Authentication Method: 6. psk

IKEv2 Pre-Shared Key: 7.

IKEv2 PSK Local ID: 8.

IKEv2 PSK Remote ID: 9.

IKEv2 Encryption Algorithms: AES-128-CBC

ESP Encryption Algorithms: AES-128-CBC

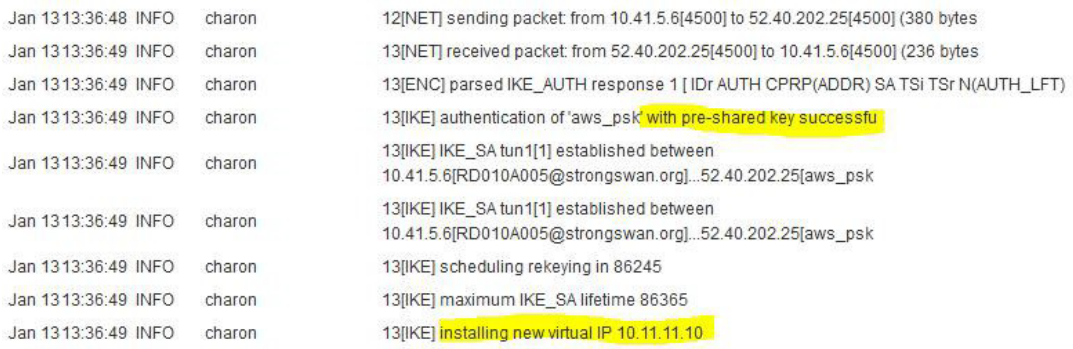
IKEv2 Integrity Algorithms: HMAC-SHA1-96

ESP Integrity Algorithms: HMAC-SHA1-96

Please apply or cancel your changes.

10. Apply | Cancel

5.3.1.2. Success Logs



```
Jan 13 13:36:48  INFO   charon    12[NET] sending packet: from 10.41.5.6[4500] to 52.40.202.25[4500] (380 bytes
Jan 13 13:36:49  INFO   charon    13[NET] received packet: from 52.40.202.25[4500] to 10.41.5.6[4500] (236 bytes
Jan 13 13:36:49  INFO   charon    13[ENC] parsed IKE_AUTH response 1 [ IDr AUTH CPRP(ADDR) SA TSi TSr N(AUTH_LFT)
Jan 13 13:36:49  INFO   charon    13[IKE] authentication of 'aws_psk' with pre-shared key successfu
                                  13[IKE] IKE_SA tun1[1] established between
Jan 13 13:36:49  INFO   charon    10.41.5.6[RD010A005@strongswan.org]...52.40.202.25[aws_psk
                                  13[IKE] IKE_SA tun1[1] established between
Jan 13 13:36:49  INFO   charon    10.41.5.6[RD010A005@strongswan.org]...52.40.202.25[aws_psk
Jan 13 13:36:49  INFO   charon    13[IKE] scheduling rekeying in 86245
Jan 13 13:36:49  INFO   charon    13[IKE] maximum IKE_SA lifetime 86365
Jan 13 13:36:49  INFO   charon    13[IKE] installing new virtual IP 10.11.11.10
```

5.3.1.3. Trouble Shooting

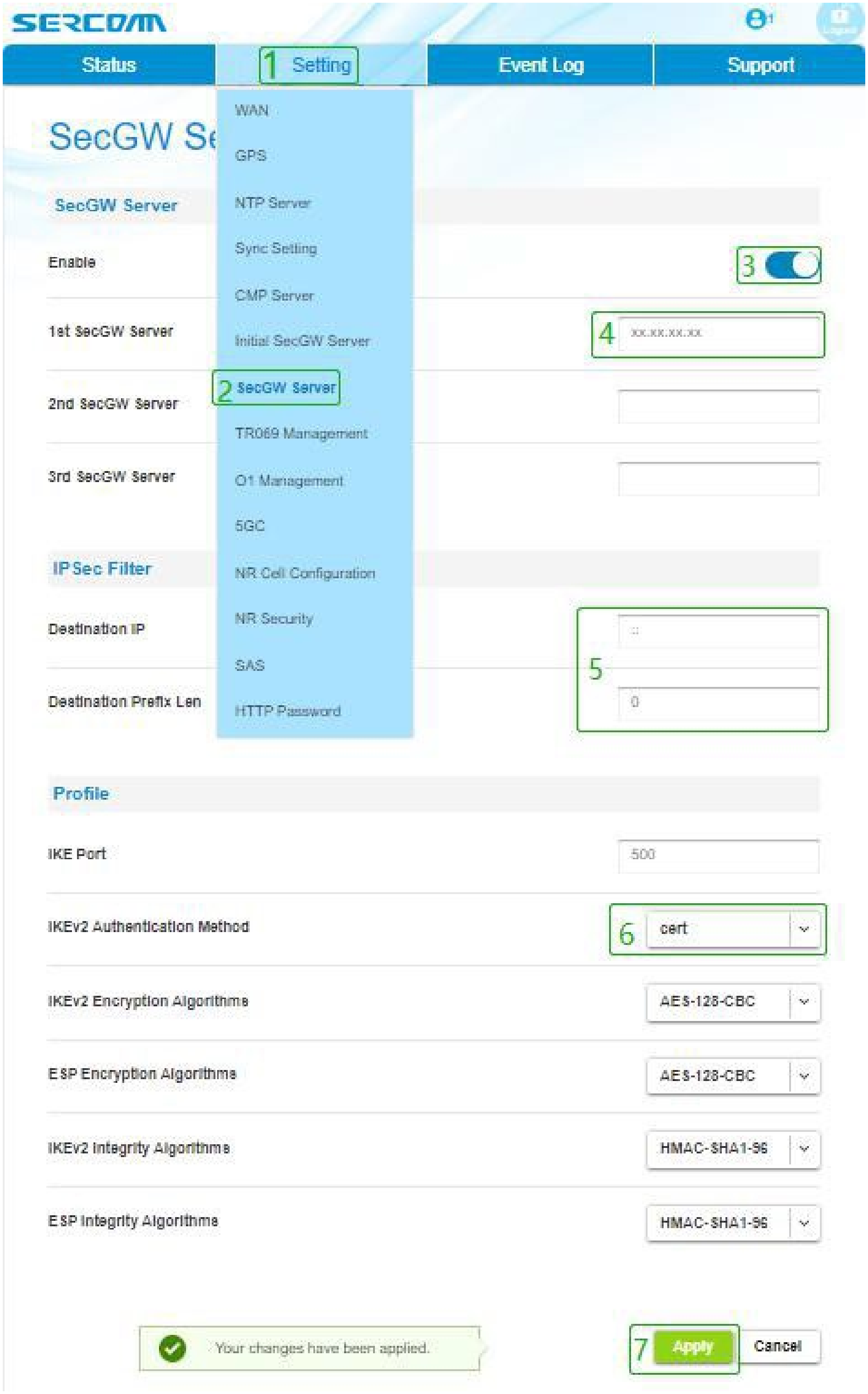
Check the parameters for PSK authentication were correct, and the SecGW should be reachable, also the log file shall show which step of IKEv2 was failed.

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.



SecGW Se

SecGW Server

Enable

1st SecGW Server xx.xx.xx.xx

2nd SecGW Server

3rd SecGW Server

IPSec Filter

Destination IP ::

Destination Prefix Len 0

Profile

IKE Port 500

IKEv2 Authentication Method cert

IKEv2 Encryption Algorithms AES-128-CBC

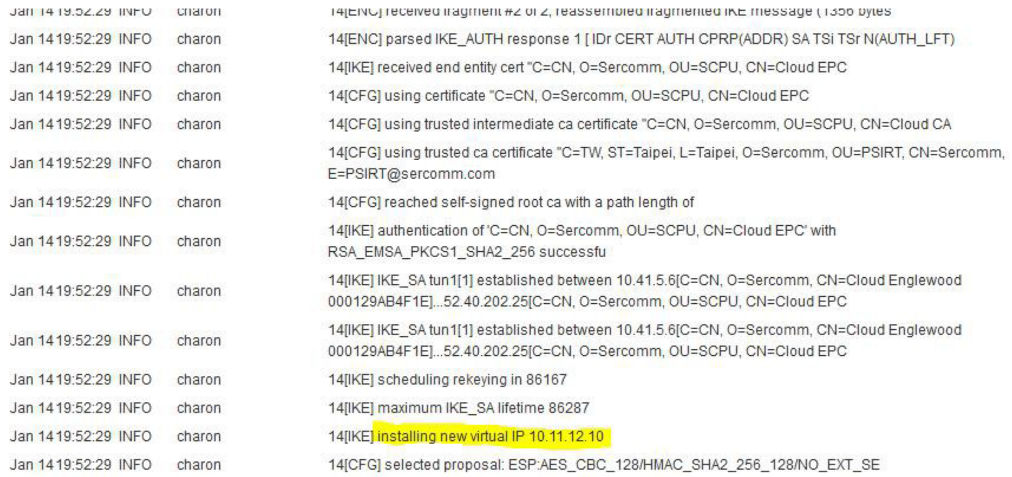
ESP Encryption Algorithms AES-128-CBC

IKEv2 Integrity Algorithms HMAC-SHA1-96

ESP Integrity Algorithms HMAC-SHA1-96

Your changes have been applied.

5.3.2.2. Success Logs



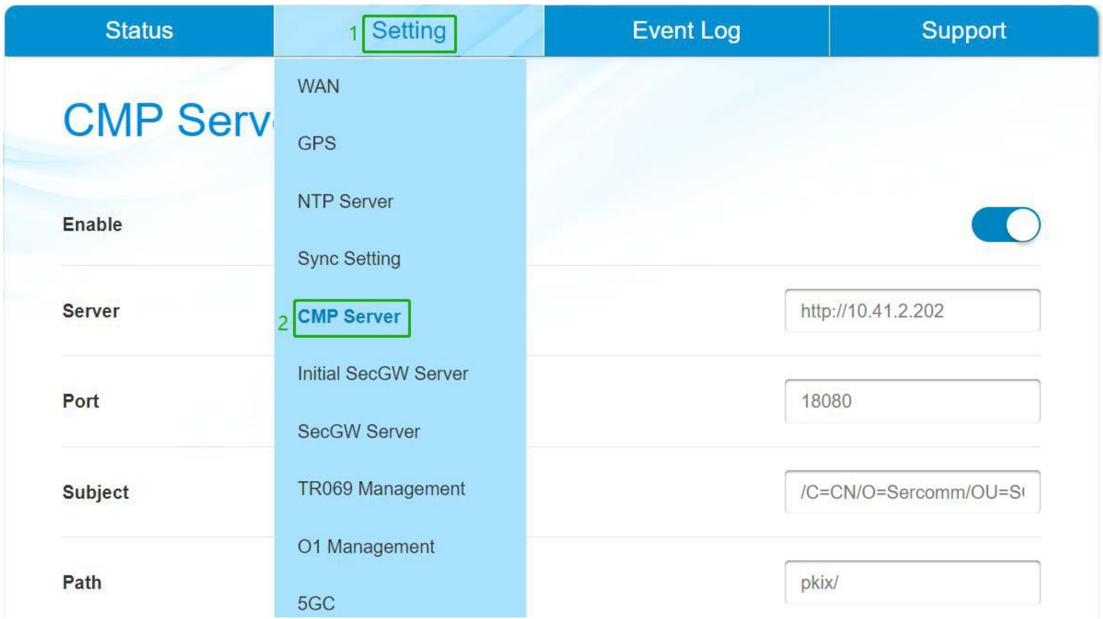
```
Jan 14 19:52:29  INFO    charon        14[ENC] received fragment #2 of 2, reassembled fragmented IKE message (1356 bytes
Jan 1419:52:29  INFO    charon        14[ENC] parsed IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR) SA TSi TSr N(AUTH_LFT)
Jan 1419:52:29  INFO    charon        14[IKE] received end entity cert "C=CN, O=Sercomm, OU=SCPU, CN=Cloud EPC
Jan 1419:52:29  INFO    charon        14[CFG] using certificate "C=CN, O=Sercomm, OU=SCPU, CN=Cloud EPC
Jan 1419:52:29  INFO    charon        14[CFG] using trusted intermediate ca certificate "C=CN, O=Sercomm, OU=SCPU, CN=Cloud CA
Jan 1419:52:29  INFO    charon        14[CFG] using trusted ca certificate "C=TW, ST=Taipei, L=Taipei, O=Sercomm, OU=PSIRT, CN=Sercomm,
                                      E=PSIRT@sercomm.com
Jan 1419:52:29  INFO    charon        14[CFG] reached self-signed root ca with a path length of
Jan 1419:52:29  INFO    charon        14[IKE] authentication of 'C=CN, O=Sercomm, OU=SCPU, CN=Cloud EPC' with
                                      RSA_EMSA_PKCS1_SHA2_256 successfu
Jan 1419:52:29  INFO    charon        14[IKE] IKE_SA tun1[1] established between 10.41.5.6[C=CN, O=Sercomm, CN=Cloud Englewood
                                      000129AB4F1E]...52.40.202.25[C=CN, O=Sercomm, OU=SCPU, CN=Cloud EPC
Jan 1419:52:29  INFO    charon        14[IKE] IKE_SA tun1[1] established between 10.41.5.6[C=CN, O=Sercomm, CN=Cloud Englewood
                                      000129AB4F1E]...52.40.202.25[C=CN, O=Sercomm, OU=SCPU, CN=Cloud EPC
Jan 1419:52:29  INFO    charon        14[IKE] scheduling rekeying in 86167
Jan 1419:52:29  INFO    charon        14[IKE] maximum IKE_SA lifetime 86287
Jan 1419:52:29  INFO    charon        14[IKE] installing new virtual IP 10.11.12.10
Jan 1419:52:29  INFO    charon        14[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SE
```

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.



CMP Serv

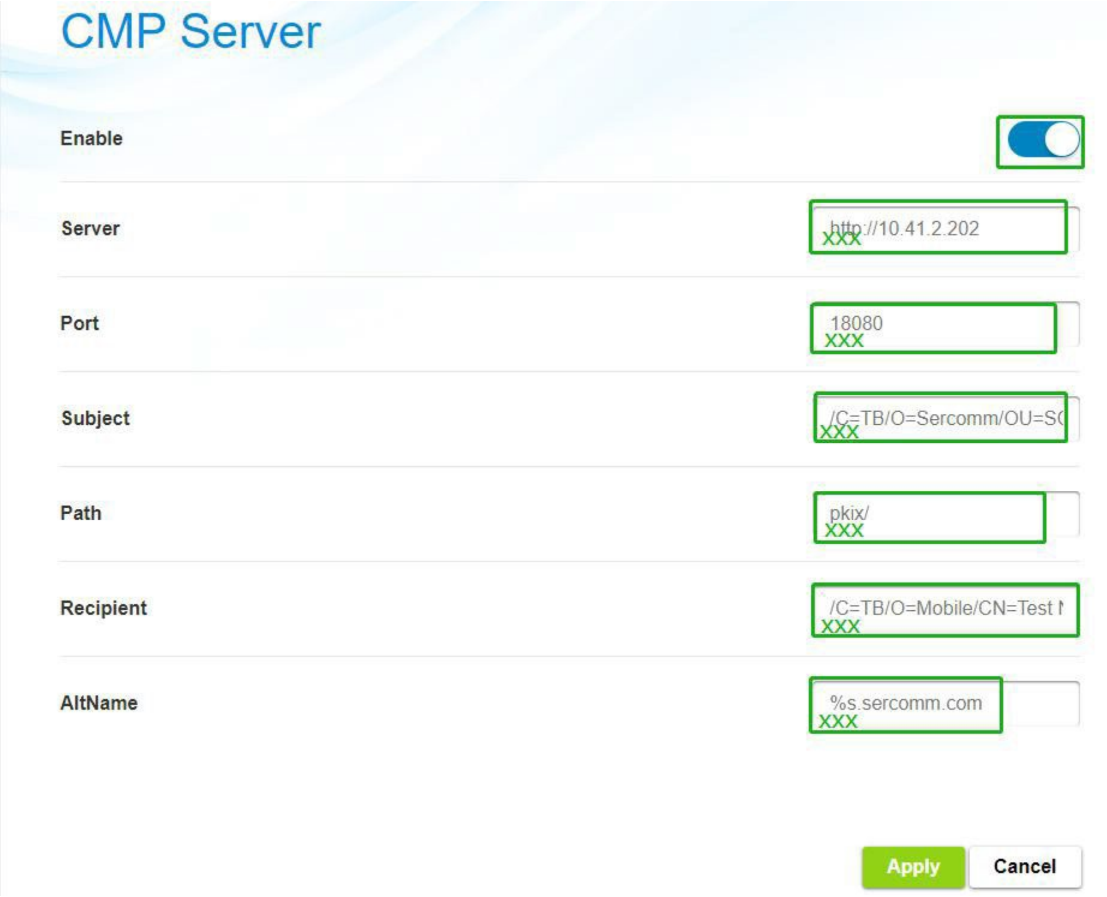
Enable

Server http://10.41.2.202

Port 18080

Subject /C=CN/O=Sercomm/OU=S(

Path pkix/



CMP Server

Enable

Server http://10.41.2.202 XXX

Port 18080 XXX

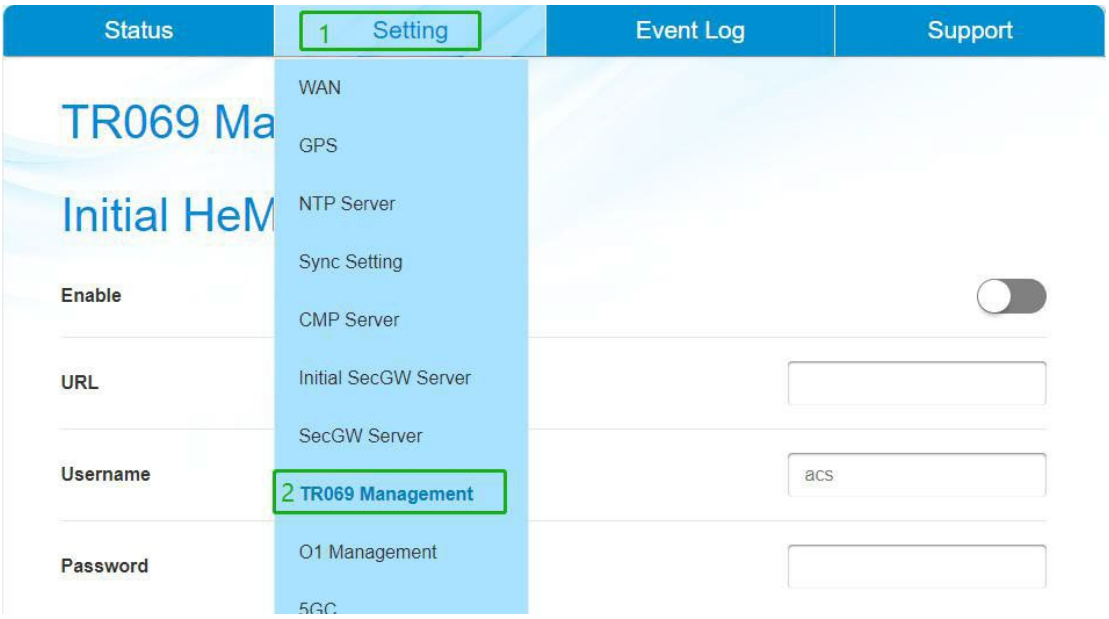
Subject /C=TB/O=Sercomm/OU=S(XXX

Path pkix/ XXX

Recipient /C=TB/O=Mobile/CN=Test I XXX

AltName %s.sercomm.com XXX

5.5. HeMS Server Setting



TR069 Ma

Initial HeM

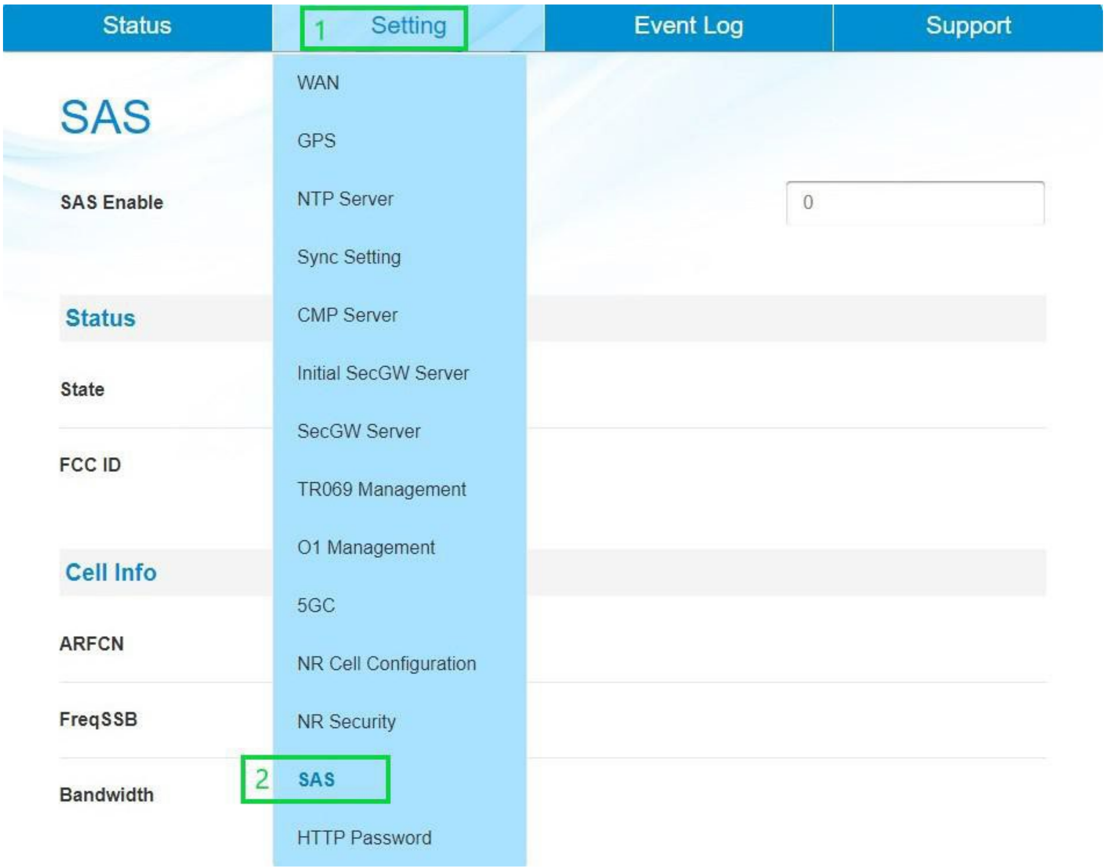
Enable

URL

Username acs

Password

5.6. SAS Setting



SAS

SAS Enable 0

Status

State

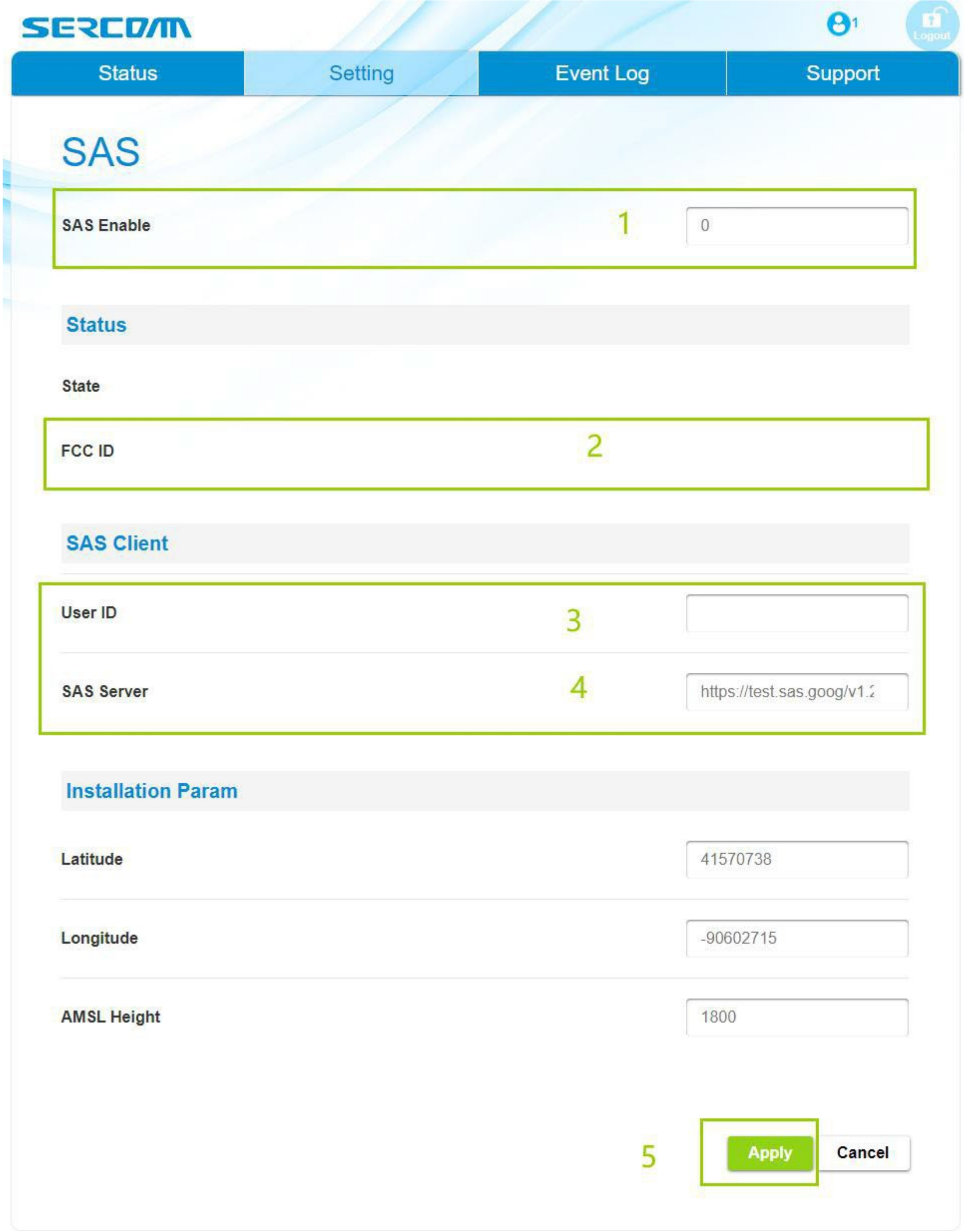
FCC ID

Cell Info

ARFCN

FreqSSB

Bandwidth



SAS

SAS Enable: 0

Status

State

FCC ID

SAS Client

User ID

SAS Server: https://test.sas.goog/v1.2

Installation Param

Latitude: 41570738

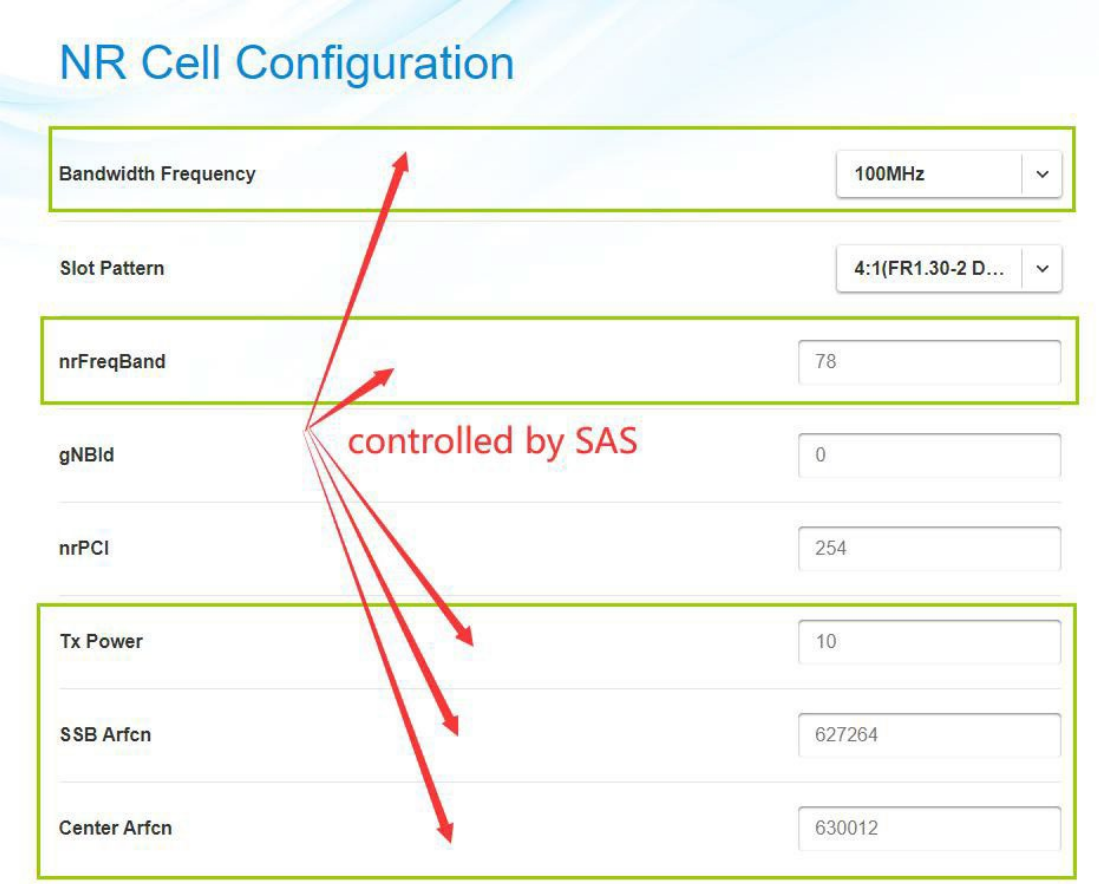
Longitude: -90602715

AMSL Height: 1800

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.



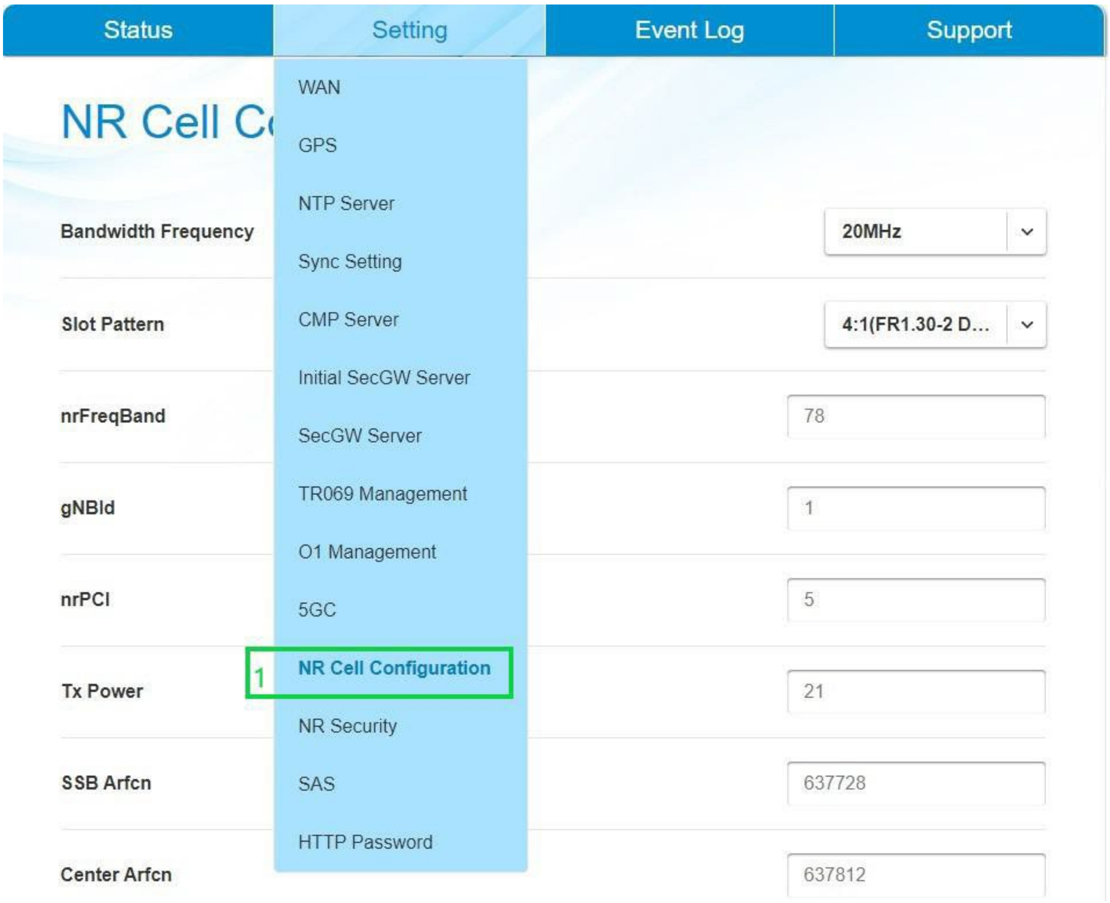
NR Cell Configuration

Bandwidth Frequency	100MHz
Slot Pattern	4:1(FR1.30-2 D…
nrFreqBand	78
gNBId	0
nrPCI	254
Tx Power	10
SSB Arfcn	627264
Center Arfcn	630012

Notice： When enable SAS,Bandwidth Frequency, nrFreqBand,TX Power,SSB Arfcn adn Center Arfcn at NR Cell Configuration page wil 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 DDDSUUUUDD).

5.7. Intra HO Setting



NR Cell C

Bandwidth Frequency 20MHz

Slot Pattern 4:1(FR1.30-2 D...

nrFreqBand 78

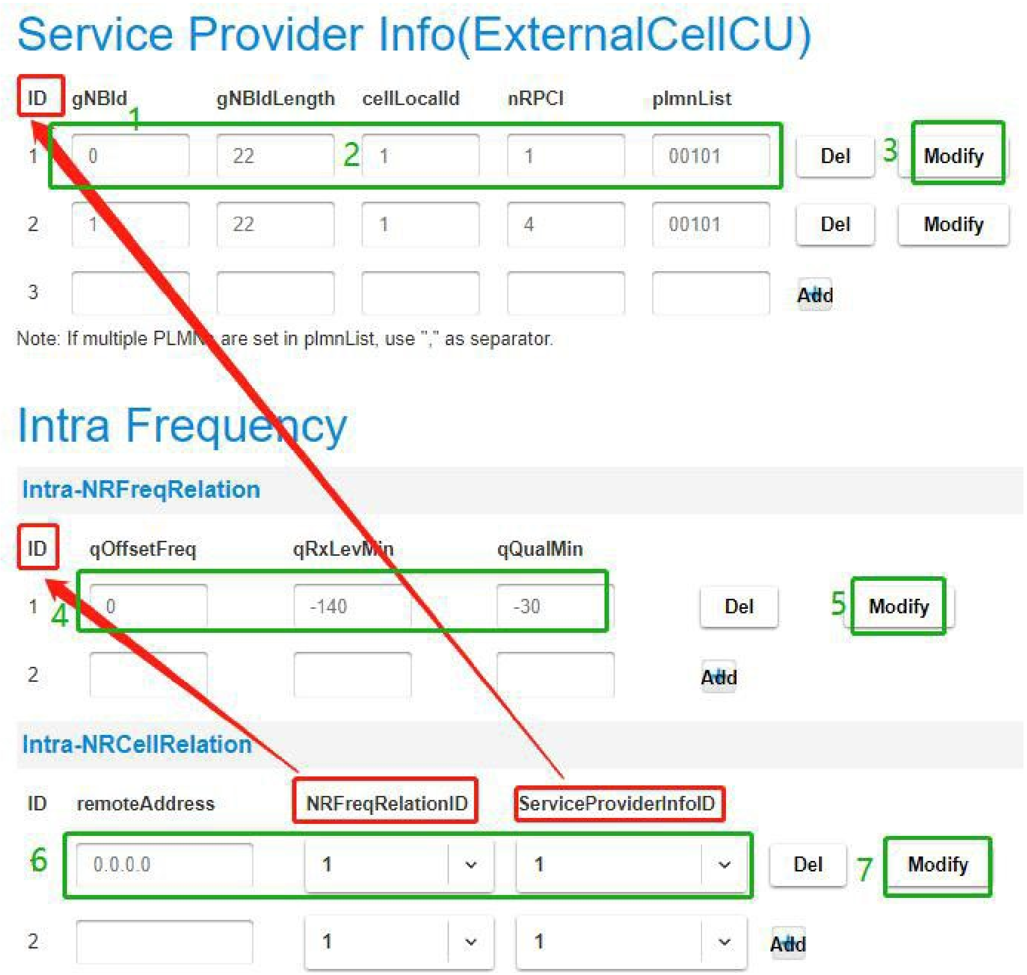
gNBId 1

nrPCI 5

Tx Power 21

SSB Arfcn 637728

Center Arfcn 637812



Service Provider Info(ExternalCellCU)

ID	gNBId	gNBIdLength	cellLocalId	nRPCI	plmnList		
1	0	22	1	1	00101	Del	Modify
2	1	22	1	4	00101	Del	Modify
3						Add	

Note: If multiple PLMNs are set in plmnList, use "," as separator.

Intra Frequency

Intra-NRFreqRelation

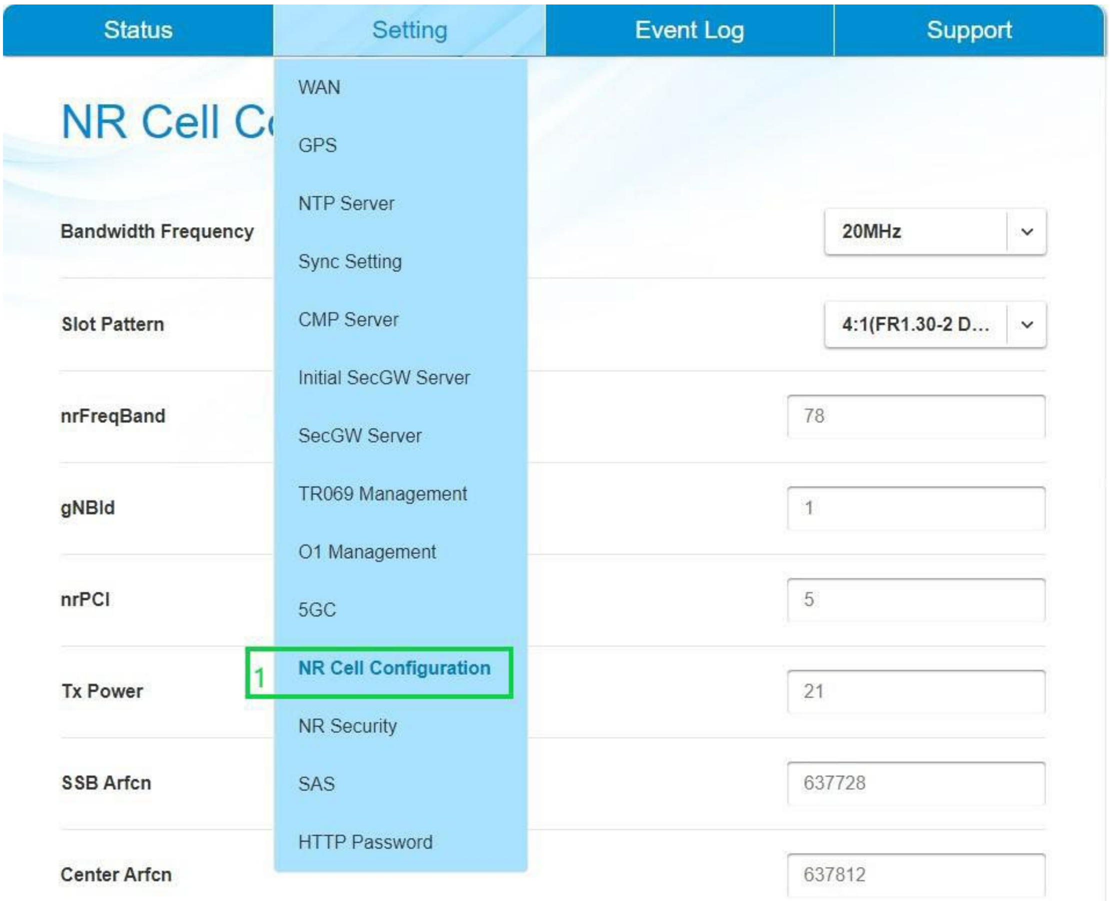
ID	qOffsetFreq	qRxLevMin	qQualMin		
1	0	-140	-30	Del	Modify
2				Add	

Intra-NRCellRelation

ID	remoteAddress	NRFreqRelationID	ServiceProviderInfoID		
	0.0.0.0	1	1	Del	Modify
2		1	1	Add	

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



Bandwidth Frequency: 20MHz

Slot Pattern: 4:1(FR1.30-2 D...

nrFreqBand: 78

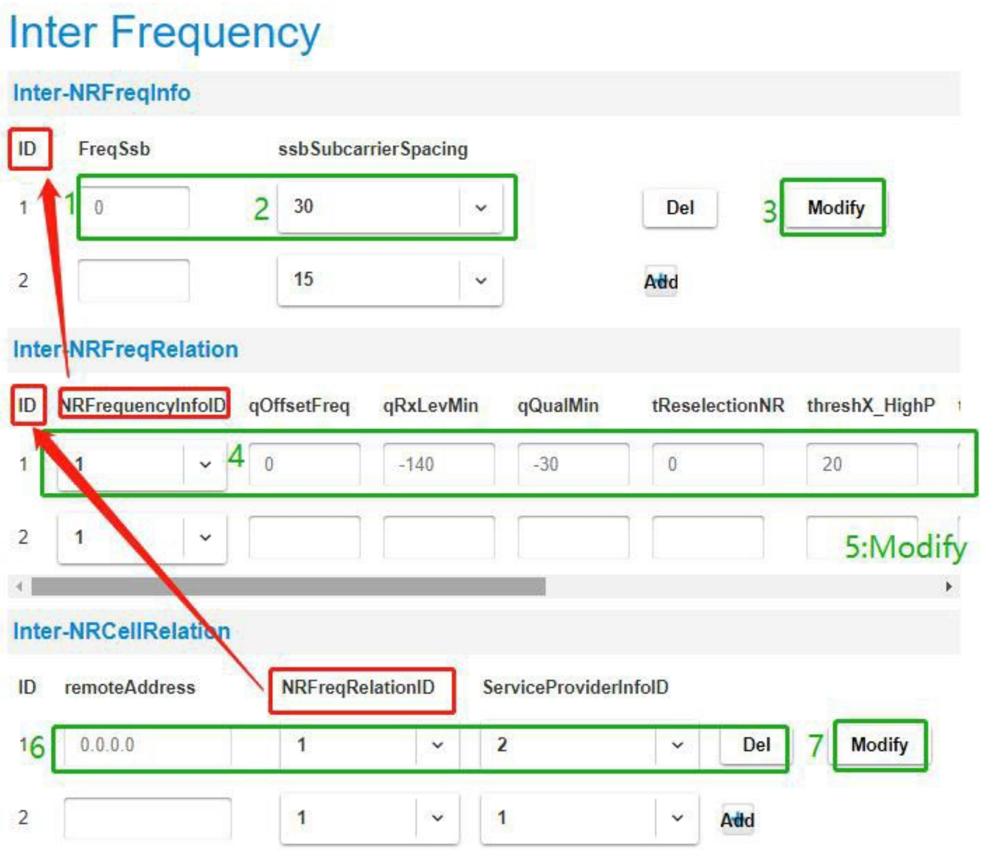
gNBId: 1

nrPCI: 5

Tx Power: 21

SSB Arfcn: 637728

Center Arfcn: 637812



Inter Frequency

Inter-NRFreqInfo

ID	FreqSsb	ssbSubcarrierSpacing		
1	0	30	Del	Modify
2		15	Add	

Inter-NRFreqRelation

ID	NRFrequencyInfoID	qOffsetFreq	qRxLevMin	qQualMin	tReselectionNR	threshX_HighP
1	1	0	-140	-30	0	20
2	1					

Inter-NRCellRelation

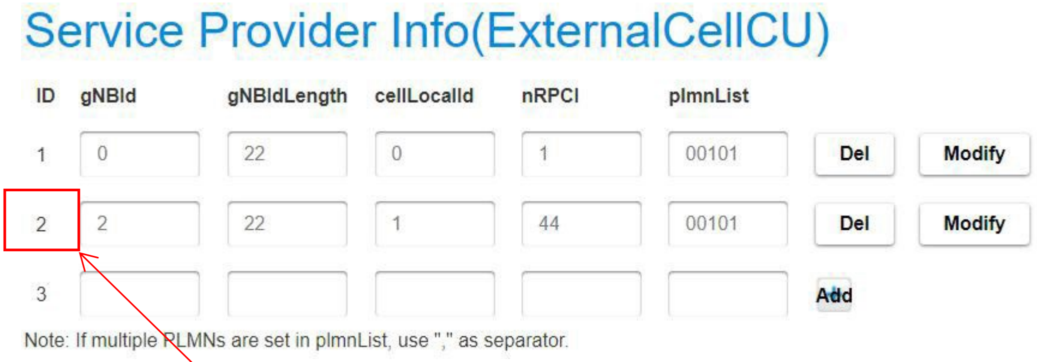
ID	remoteAddress	NRFreqRelationID	ServiceProviderInfoID		
1	0.0.0.0	1	2	Del	Modify
2		1	1	Add	

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.



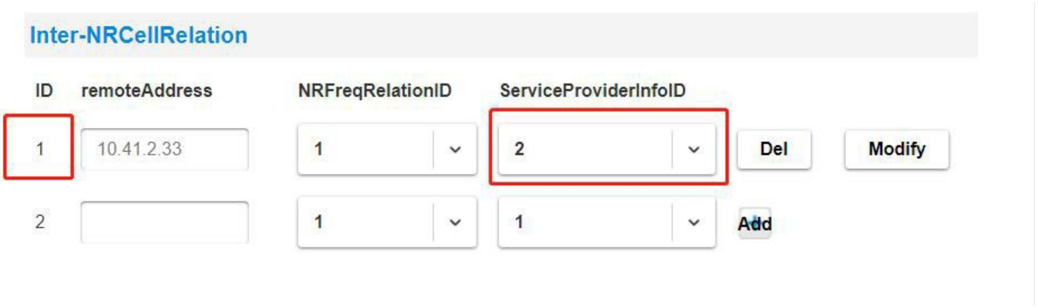
Service Provider Info(ExternalCellCU)

ID	gNBId	gNBIdLength	cellLocalId	nRPCI	plmnList		
1	0	22	0	1	00101	Del	Modify
2	2	22	1	44	00101	Del	Modify
3						Add	

Note: If multiple PLMNs are set in plmnList, use "," as separator.

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:



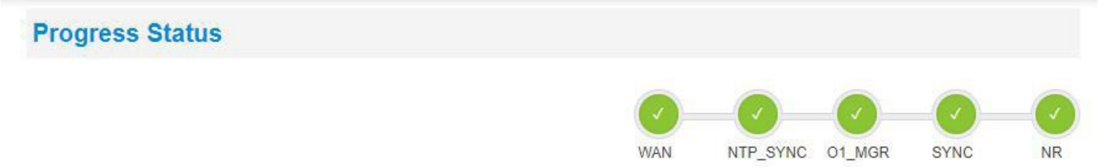
Inter-NRCellRelation

ID	remoteAddress	NRFreqRelationID	ServiceProviderInfoID		
1	10.41.2.33	1	2	Del	Modify
2		1	1	Add	

5.10. O1 Management Setting

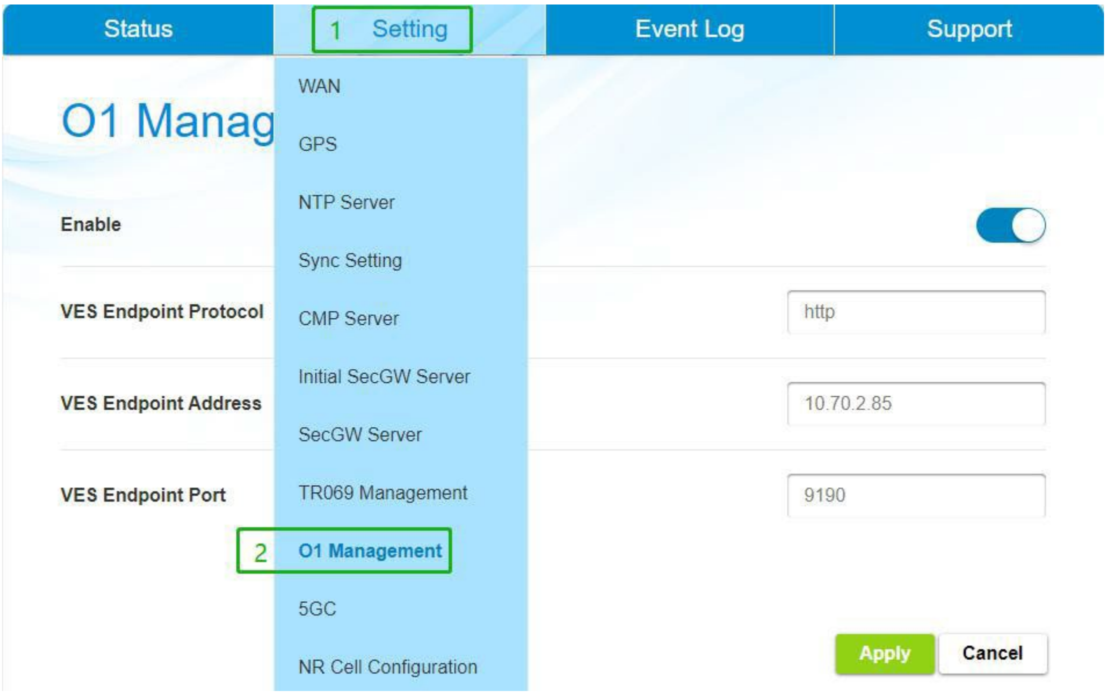
The O1 Management feature is following the O-RAN.WG10.O1-Interface.0-v06.00 specification. Trace Management Services and Cloudified NF Registration Management Service are not supported yet.

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



Progress Status

5.10.1. Configuration



O1 Manag

Enable: ON

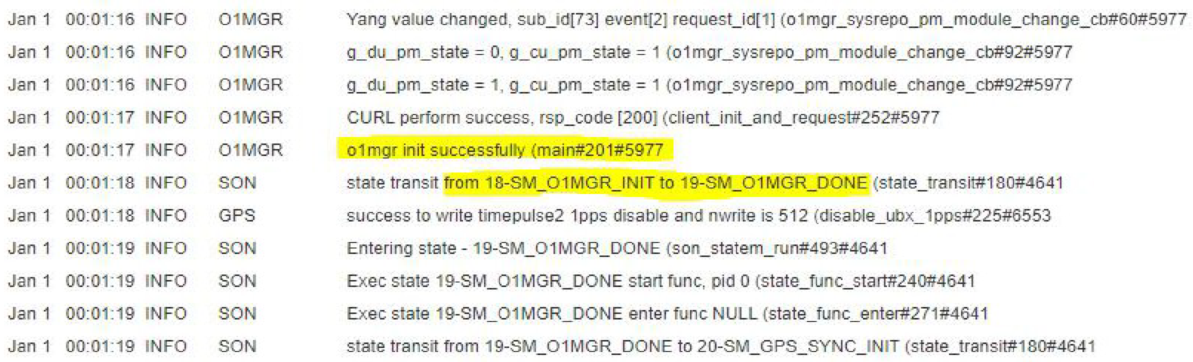
VES Endpoint Protocol: http

VES Endpoint Address: 10.70.2.85

VES Endpoint Port: 9190

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    O1MGR        Yang value changed, sub_id[73] event[2] request_id[1] (o1mgr_sysrepo_pm_module_change_cb#60#5977
Jan 1   00:01:16  INFO    O1MGR        g_du_pm_state = 0, g_cu_pm_state = 1 (o1mgr_sysrepo_pm_module_change_cb#92#5977
Jan 1   00:01:16  INFO    O1MGR        g_du_pm_state = 1, g_cu_pm_state = 1 (o1mgr_sysrepo_pm_module_change_cb#92#5977
Jan 1   00:01:17  INFO    O1MGR        CURL perform success, rsp_code [200] (client_init_and_request#252#5977
Jan 1   00:01:17  INFO    O1MGR        o1mgr init successfully (main#201#5977
Jan 1   00:01:18  INFO    SON          state transit from 18-SM_O1MGR_INIT to 19-SM_O1MGR_DONE (state_transit#180#4641
Jan 1   00:01:18  INFO    GPS          success to write timepulse2 1pps disable and nwrite is 512 (disable_ubx_1pps#225#6553
Jan 1   00:01:19  INFO    SON          Entering state - 19-SM_O1MGR_DONE (son_statem_run#493#4641
Jan 1   00:01:19  INFO    SON          Exec state 19-SM_O1MGR_DONE start func, pid 0 (state_func_start#240#4641
Jan 1   00:01:19  INFO    SON          Exec state 19-SM_O1MGR_DONE enter func NULL (state_func_enter#271#4641
Jan 1   00:01:19  INFO    SON          state transit from 19-SM_O1MGR_DONE to 20-SM_GPS_SYNC_INIT (state_transit#180#4641
```

5.10.3. Trouble Shooting

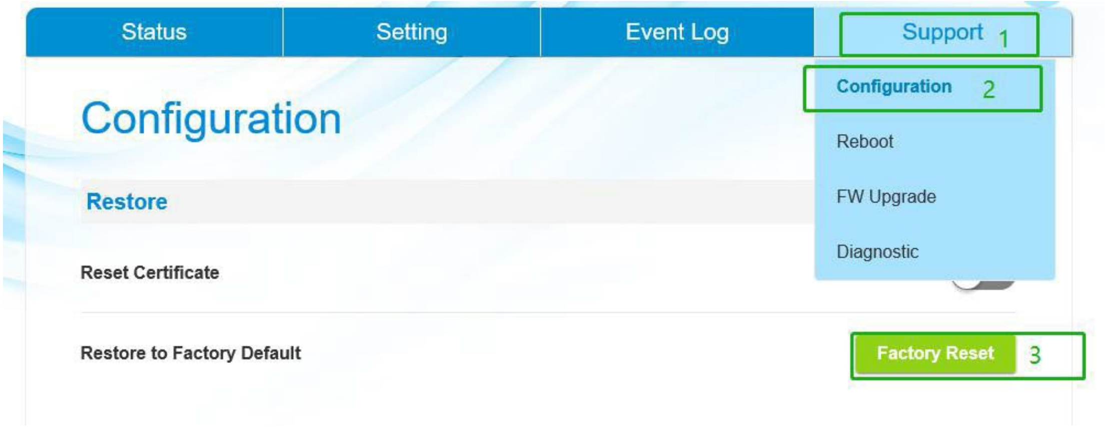
- Check O1 management server can support VES PNF registration procedure,otherwise

PnP will failure and system block in this stage.

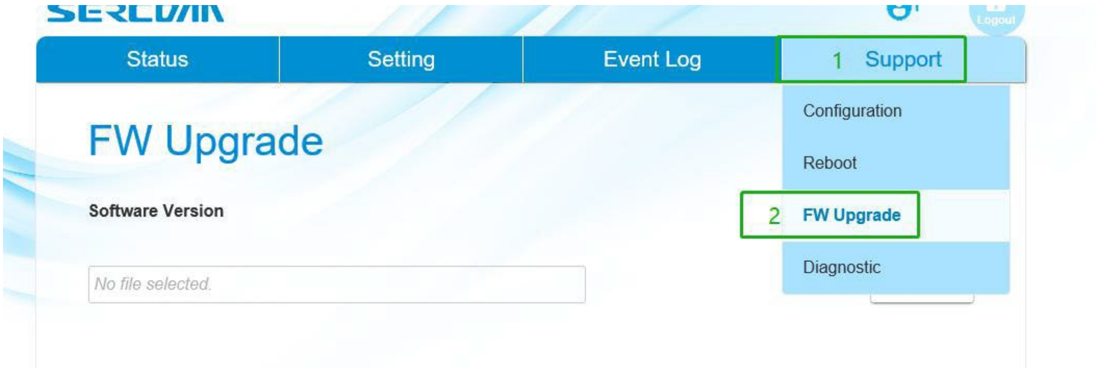
- Check the O1 management server IP address and port is correct
- Check the http or https protocol is supported in o1 management server side
- Check the device information(csn) is registered in the o1 management server side

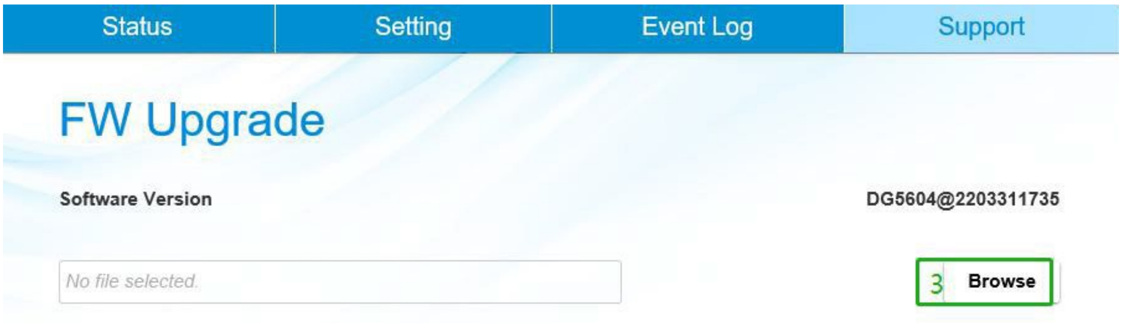
6. Firmware and Configuration Management

6.1. Factory Reset



6.2. FW Upgrade

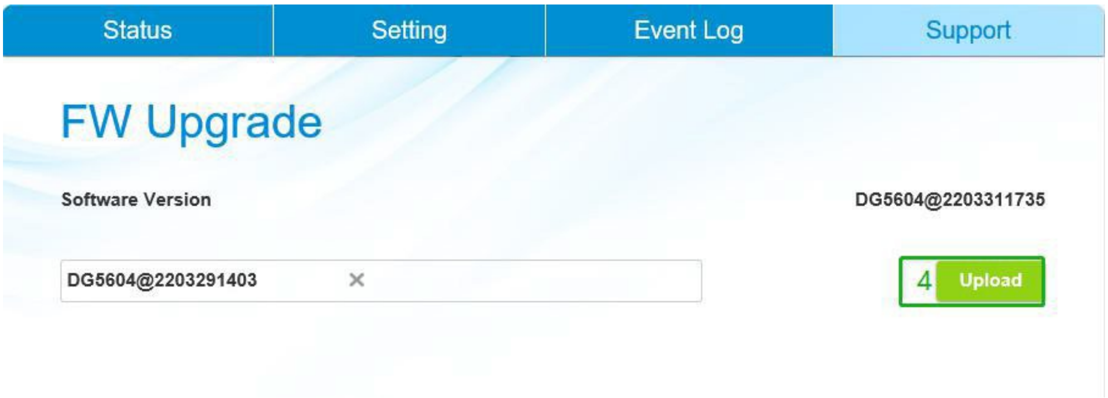




FW Upgrade

Software Version DG5604@2203311735

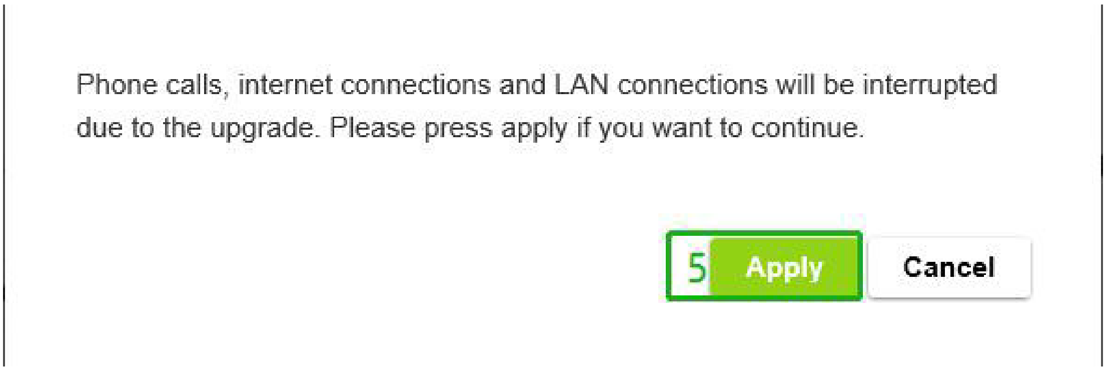
No file selected.



FW Upgrade

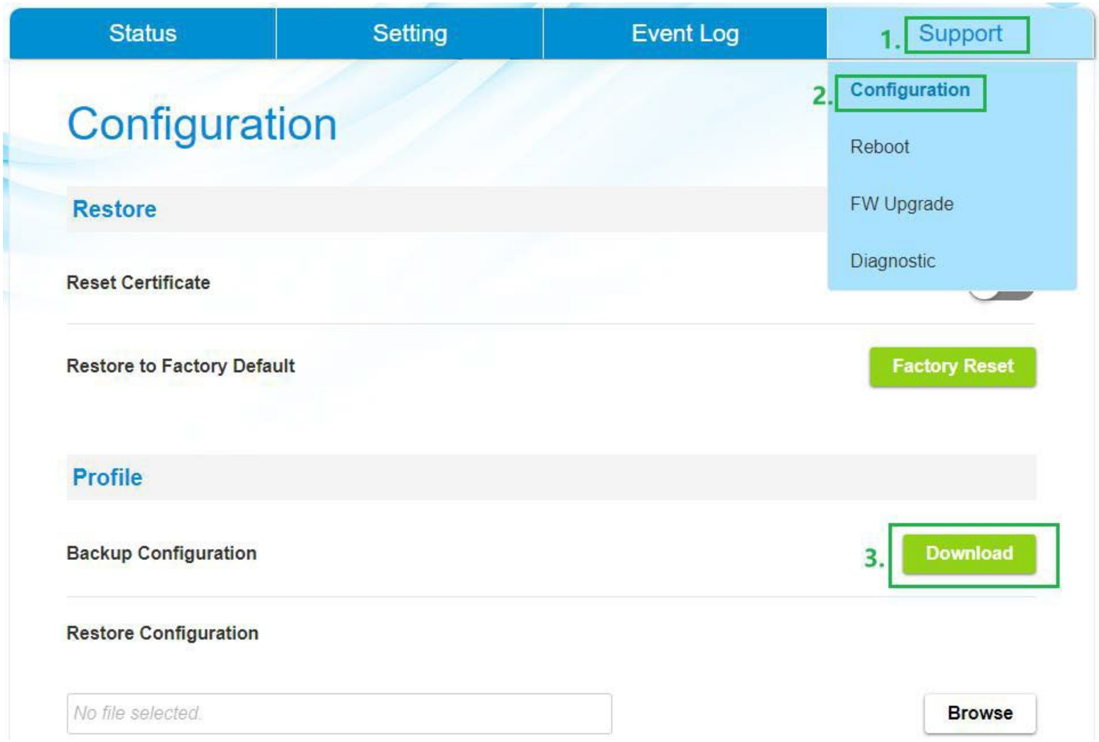
Software Version DG5604@2203311735

DG5604@2203291403 ×



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

6.3. Backup Configuration



Configuration

Restore

Reset Certificate

Restore to Factory Default

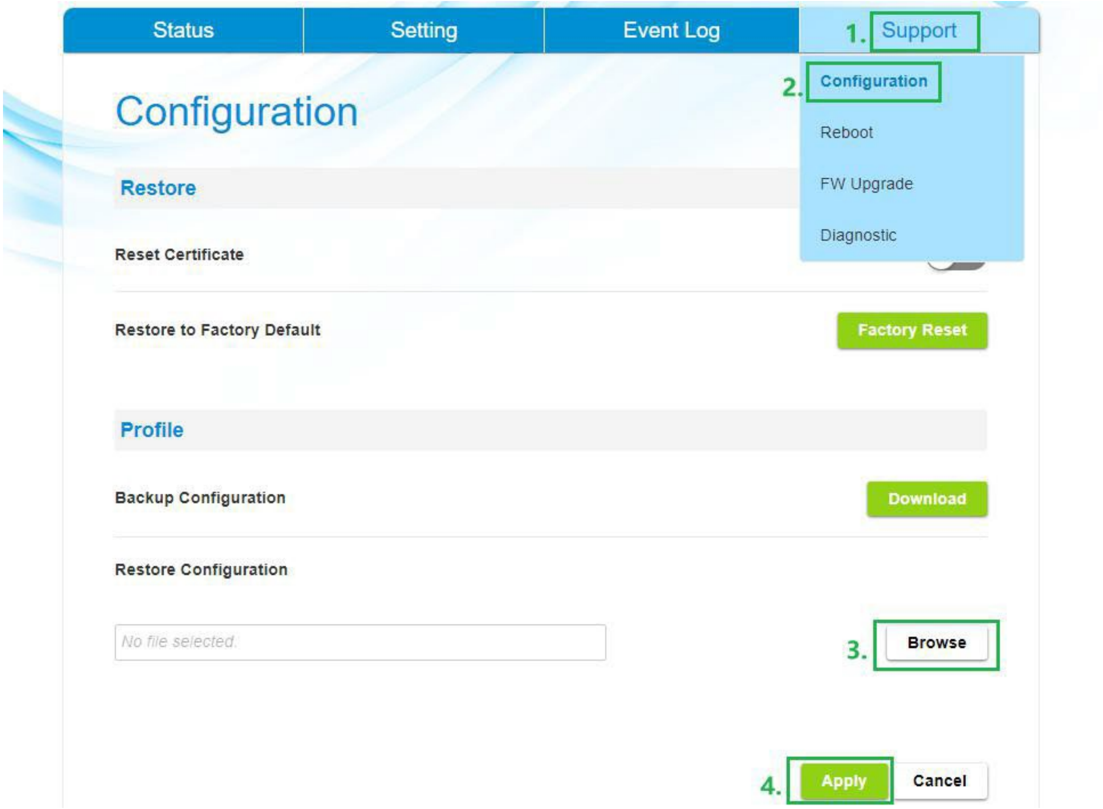
Profile

Backup Configuration

Restore Configuration

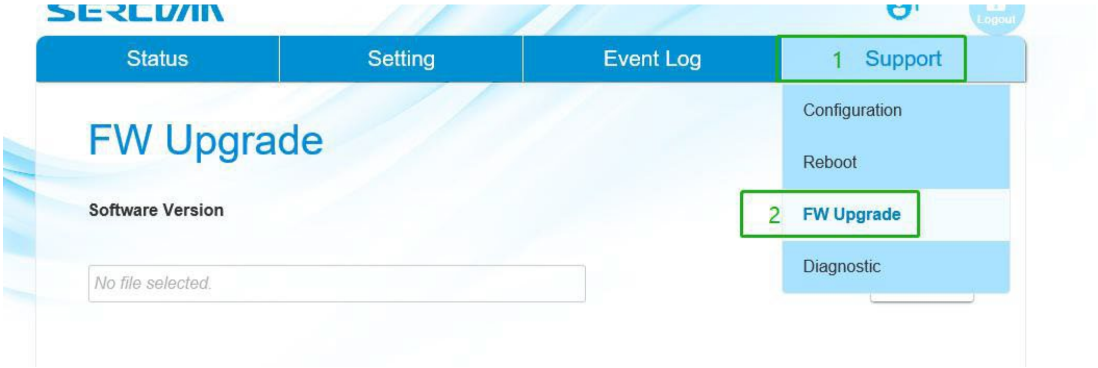
No file selected.

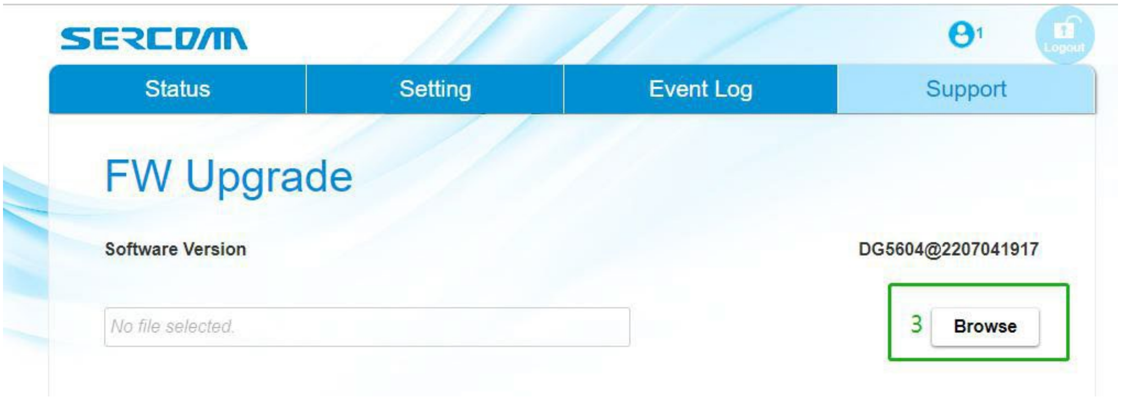
6.4. Restore Configuration



6.5. Customize Upgrade

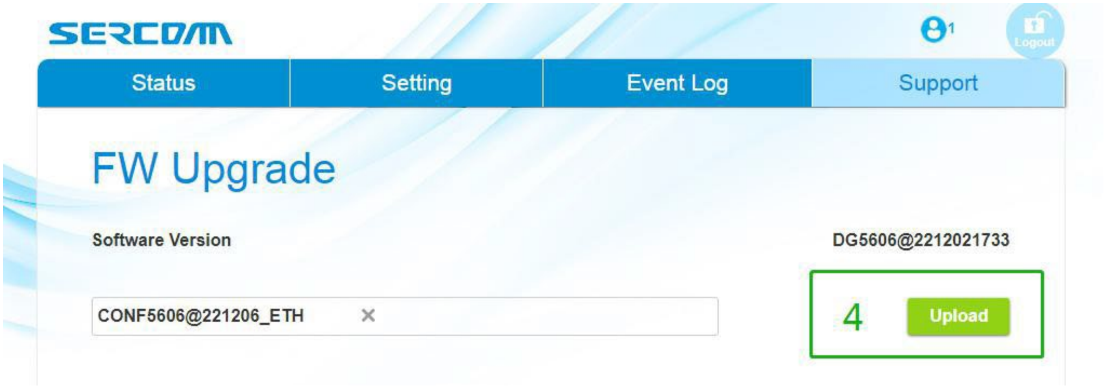
➢ Customize file upgrade from web page(same as FW upgrade)





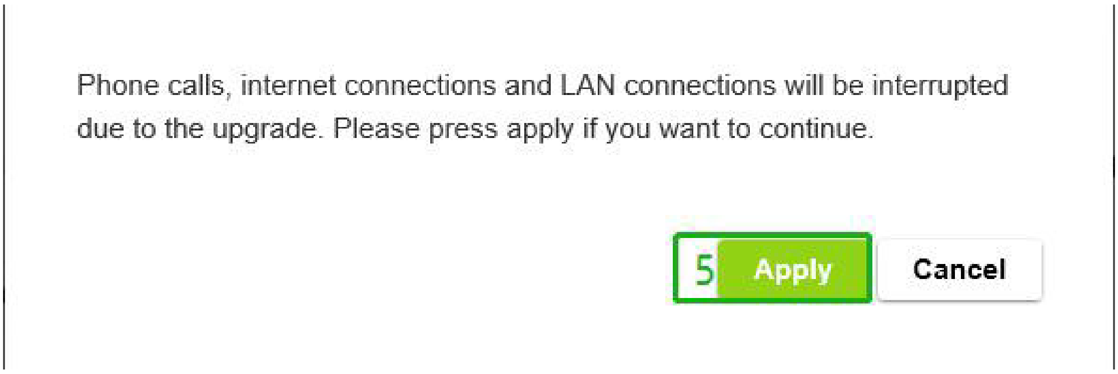
Software Version DG5604@2207041917

No file selected.



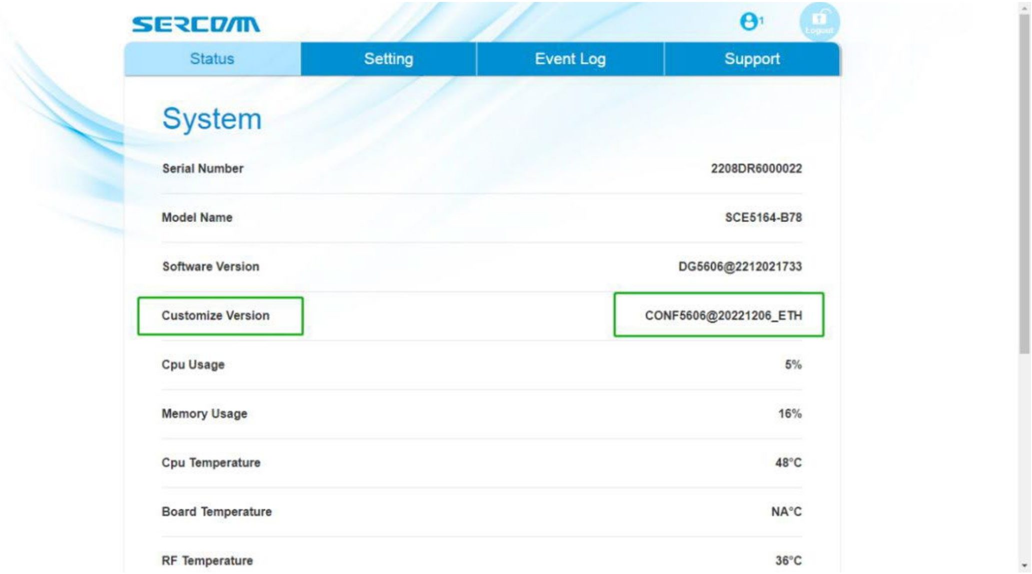
Software Version DG5606@2212021733

CONF5606@221206_ETH ×



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

- 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

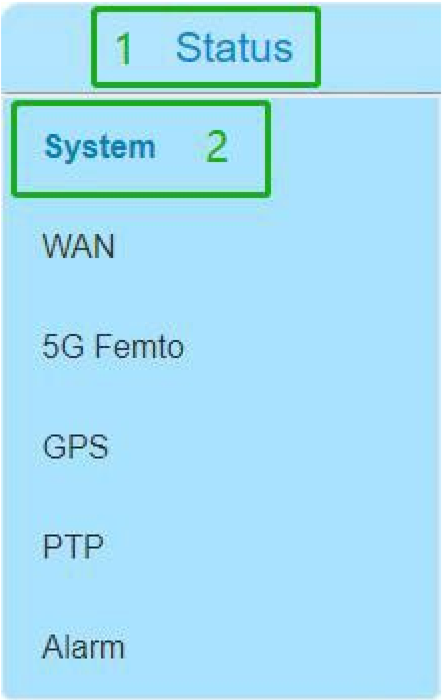


System

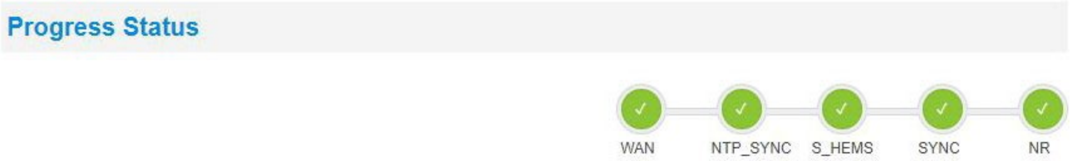
Serial Number	2208DR6000022
Model Name	SCE5164-B78
Software Version	DG5606@2212021733
Customize Version	CONF5606@20221206_ETH
Cpu Usage	5%
Memory Usage	16%
Cpu Temperature	48°C
Board Temperature	NA°C
RF Temperature	36°C

7. Status Indicators

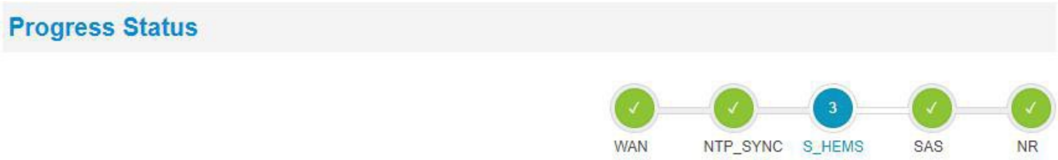
7.1. from GUI



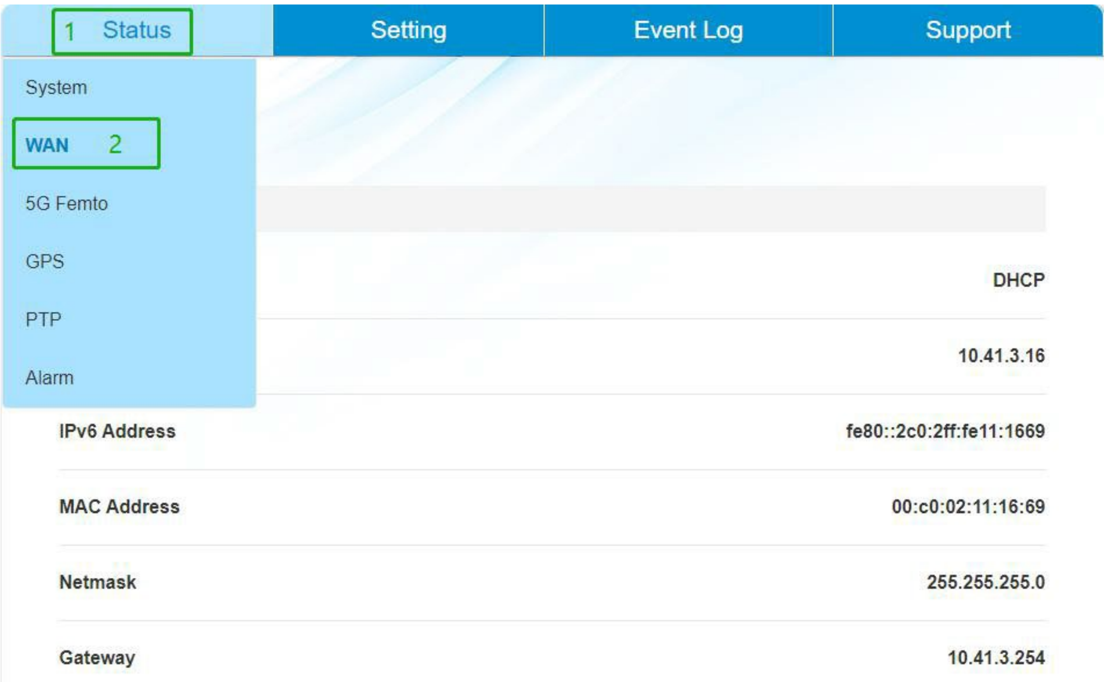
Customize Version


Progress Status

7.1.1. Status


Progress Status

7.1.2. WAN

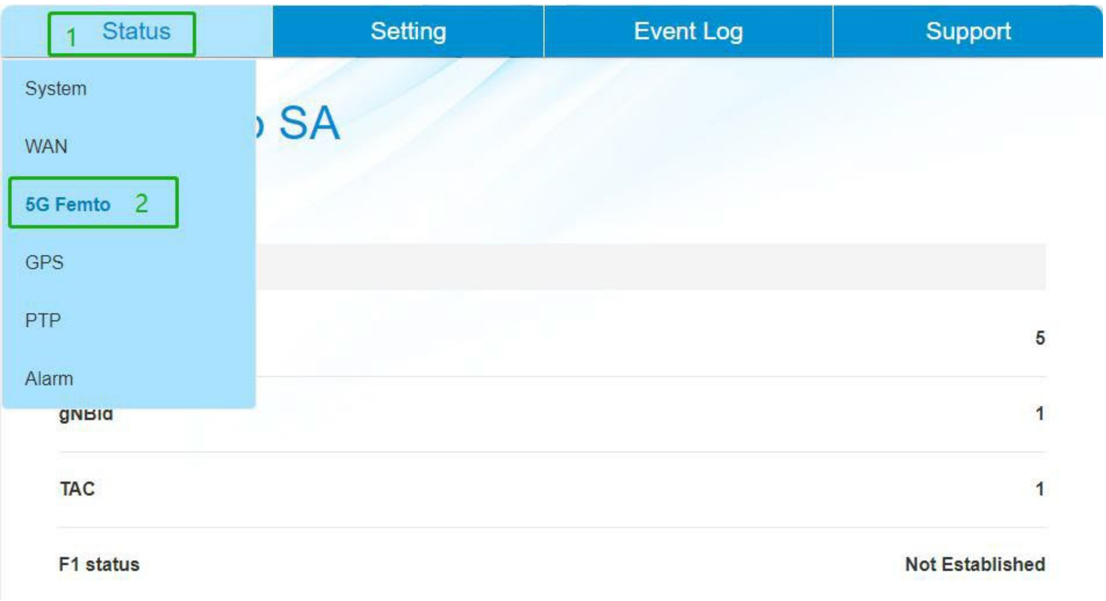


DHCP

10.41.3.16

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



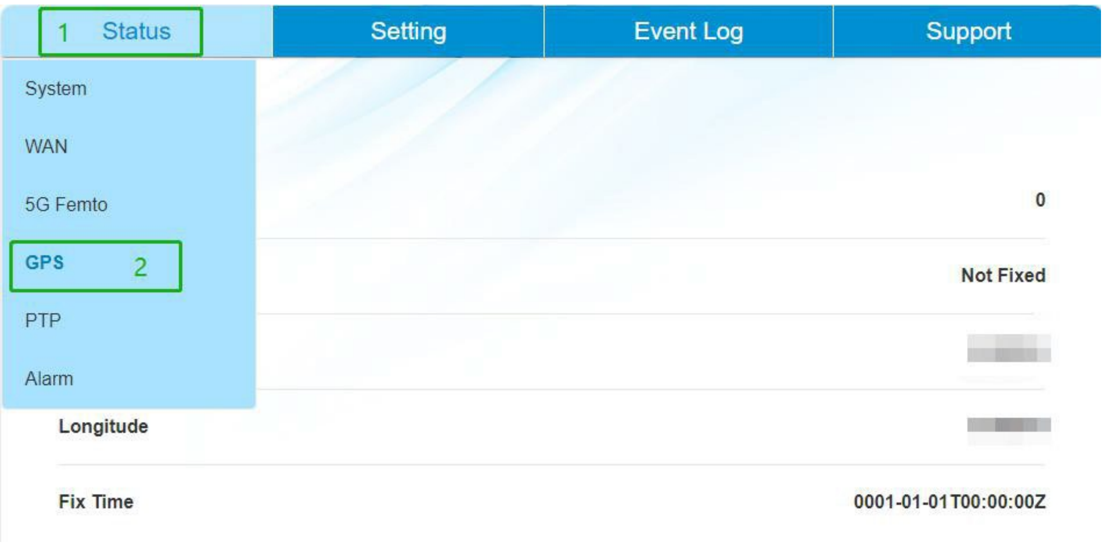
5

gNBid 1

TAC 1

F1 status Not Established

7.1.4. GPS



0

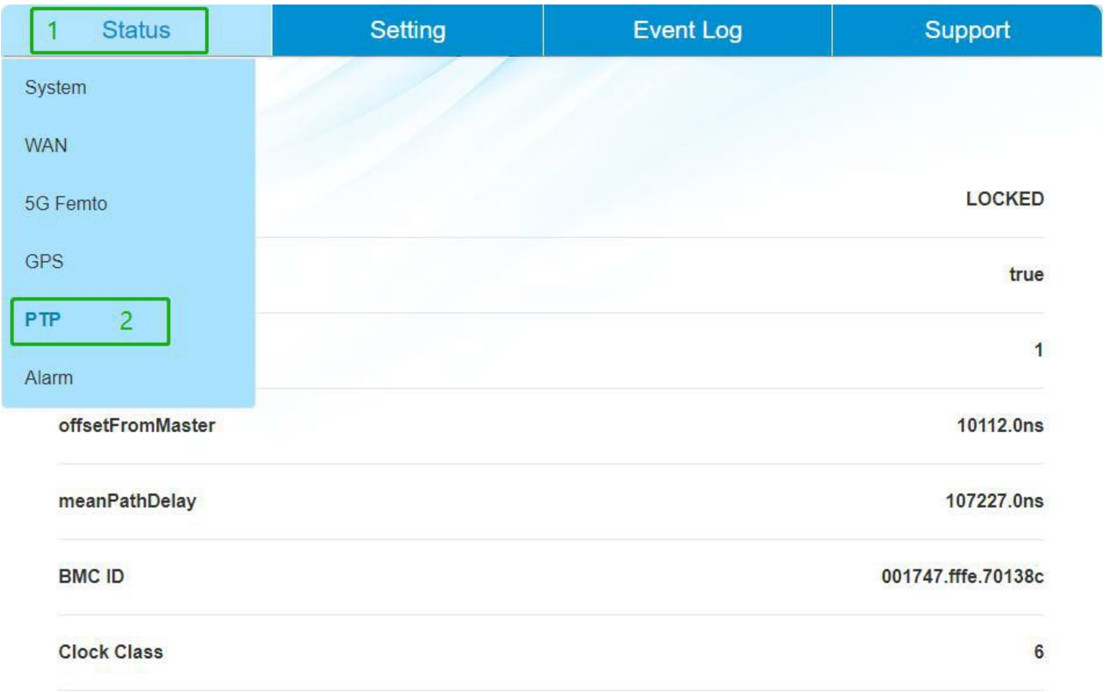
Not Fixed

[redacted]

Longitude [redacted]

Fix Time 0001-01-01T00:00:00Z

7.1.5. PTP



LOCKED

true

1

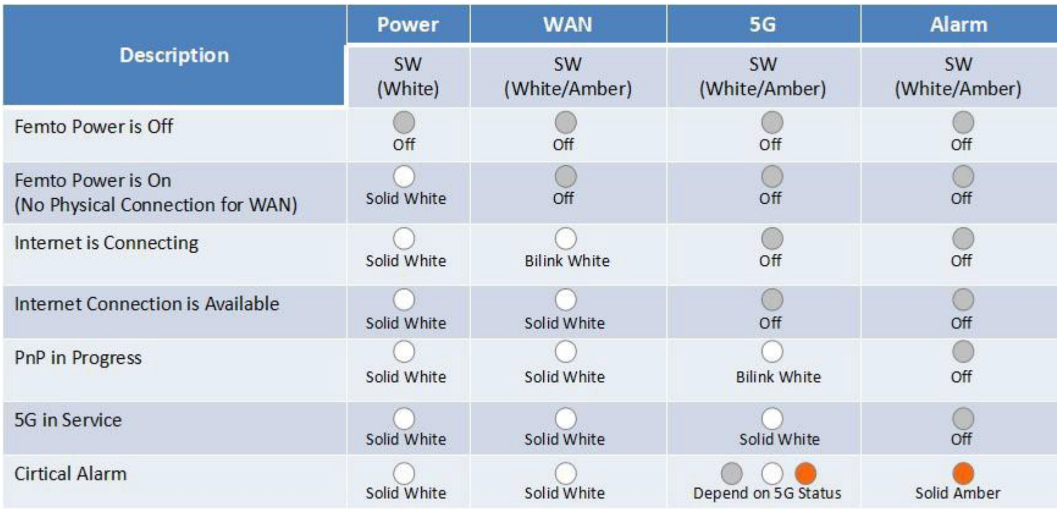
offsetFromMaster 10112.0ns

meanPathDelay 107227.0ns

BMC ID 001747.fffe.70138c

Clock Class 6

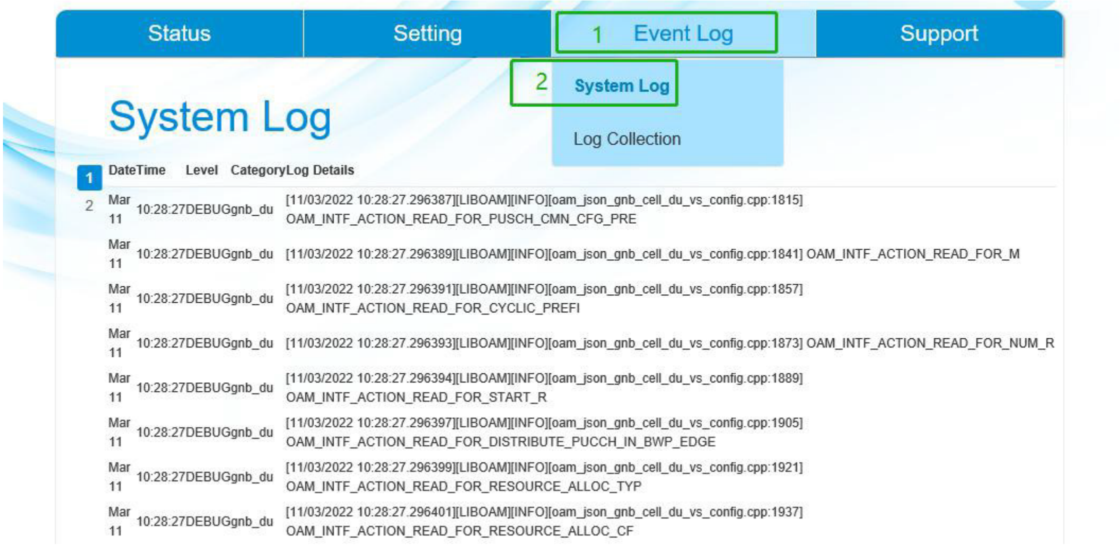
7.2. LED Indicators



Description	Power	WAN	5G	Alarm
	SW (White)	SW (White/Amber)	SW (White/Amber)	SW (White/Amber)
Femto Power is Off	Off	Off	Off	Off
Femto Power is On (No Physical Connection for WAN)	Solid White	Off	Off	Off
Internet is Connecting	Solid White	Bilink White	Off	Off
Internet Connection is Available	Solid White	Solid White	Off	Off
PnP in Progress	Solid White	Solid White	Bilink White	Off
5G in Service	Solid White	Solid White	Solid White	Off
Cirtical Alarm	Solid White	Solid White	Depend on 5G Status	Solid Amber

8. Logs

8.1. System Log Display



```
DateTime     Level   CategoryLog Details
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296387][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1815]
                         OAM_INTF_ACTION_READ_FOR_PUSCH_CMN_CFG_PRE
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296389][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1841] OAM_INTF_ACTION_READ_FOR_M
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296391][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1857]
                         OAM_INTF_ACTION_READ_FOR_CYCLIC_PREFI
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296393][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1873] OAM_INTF_ACTION_READ_FOR_NUM_R
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296394][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1889]
                         OAM_INTF_ACTION_READ_FOR_START_R
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296397][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1905]
                         OAM_INTF_ACTION_READ_FOR_DISTRIBUTE_PUCCH_IN_BWP_EDGE
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296399][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1921]
                         OAM_INTF_ACTION_READ_FOR_RESOURCE_ALLOC_TYP
Mar
11  10:28:27DEBUGgnb_du  [11/03/2022 10:28:27.296401][LIBOAM][INFO][oam_json_gnb_cell_du_vs_config.cpp:1937]
                         OAM_INTF_ACTION_READ_FOR_RESOURCE_ALLOC_CF
```

8.2. CU DU Log Setting

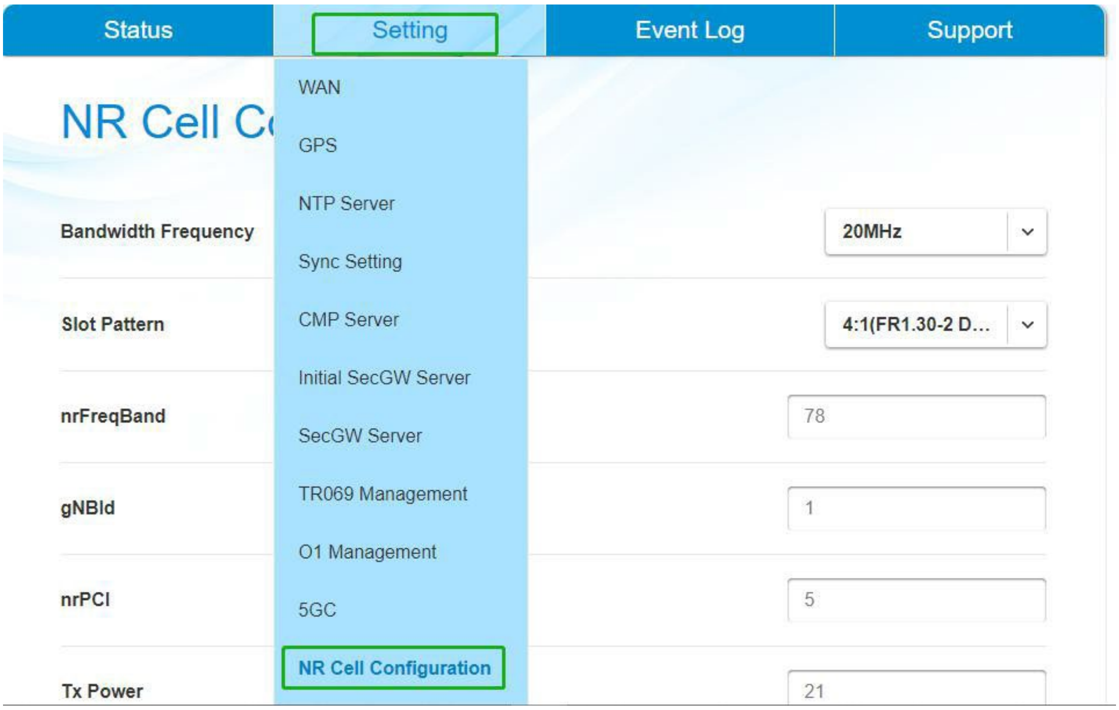
➢ Configure CU and DU log level, usually the default values are used, but when debugging certain issues it may be necessary to modify the level of certain modules, the corresponding content can be got from Sercomm. Three simple configurations are listed below:

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.

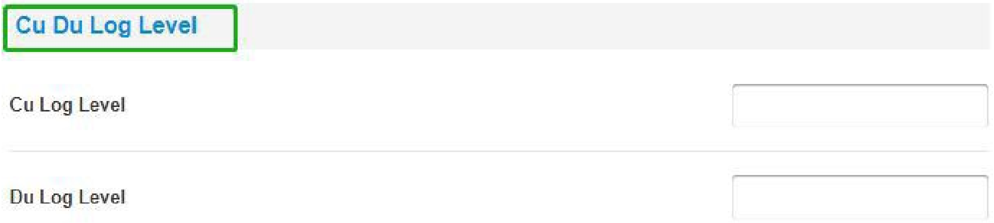
➢ Click apply;

➢ Requires reboot to take effect.



NR Cell C

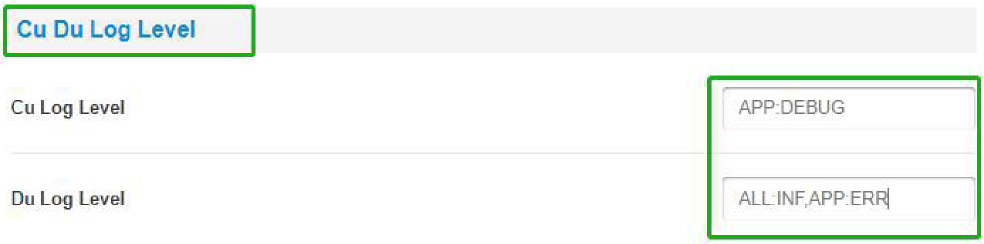
Bandwidth Frequency	20MHz
Slot Pattern	4:1(FR1.30-2 D...
nrFreqBand	78
gNBId	1
nrPCI	5
Tx Power	21



Cu Du Log Level

Cu Log Level	
Du Log Level	

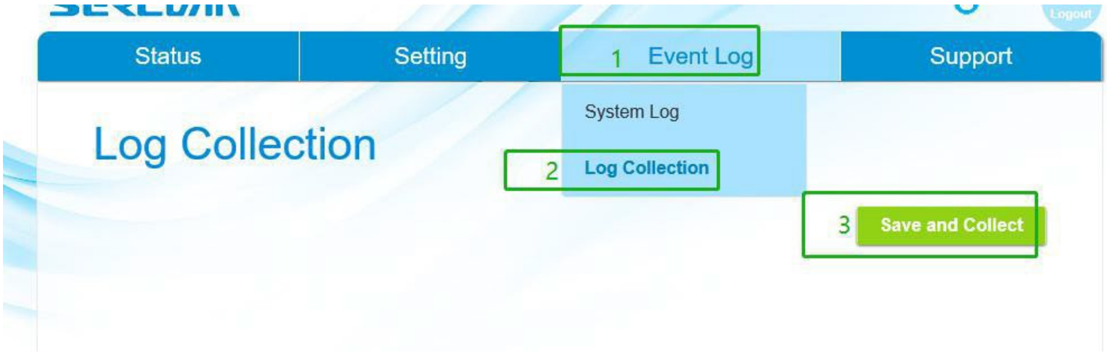
➢ The configuration example is as follows:



Cu Du Log Level

Cu Log Level	APP:DEBUG
Du Log Level	ALL:INF,APP:ERR

8.3. Log Collection



9. CLI Support List

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

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

sc_femto	1: ping 2: ip 3: ls 4: traceroute 5: date	1: show dev info 2: oam get 3: oam get_list 4: oam get_rw 5: oam get_rw_all 6: oam display 7: son statem status 8: show gps status 9: show ipsec key 10: quit 11: passwd 12: sc_yang_cli

9.1. Show Help

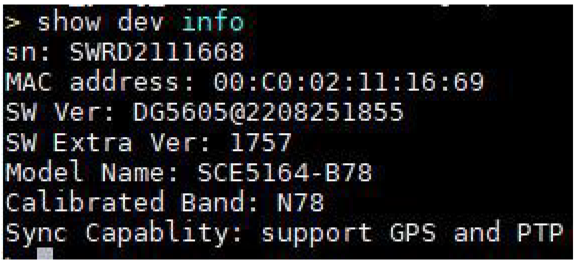
Step 1: use sc_femto or operator account to login ssh

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.

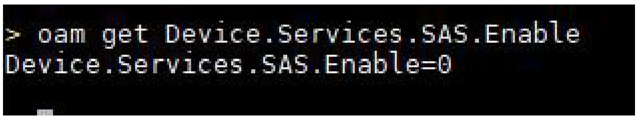


```
> show dev info
sn: SWRD2111668
MAC address: 00:C0:02:11:16:69
SW Ver: DG5605@2208251855
SW Extra Ver: 1757
Model Name: SCE5164-B78
Calibrated Band: N78
Sync Capablity: support GPS and PTP
```

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 et the value of parameters

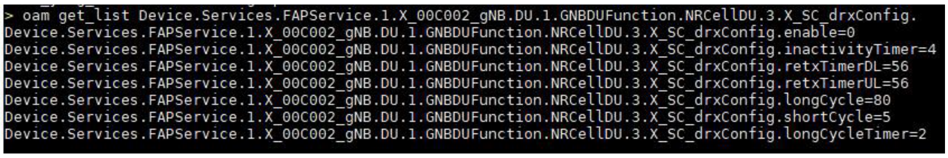


```
> oam get Device.Services.SAS.Enable
Device.Services.SAS.Enable=0
```

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

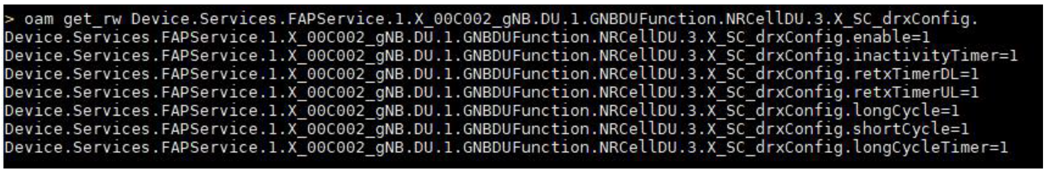


```
> oam get_list Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.enable=0
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.inactivityTimer=4
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.retxTimerDL=56
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.retxTimerUL=56
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.longCycle=80
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.shortCycle=5
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.longCycleTimer=2
```

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

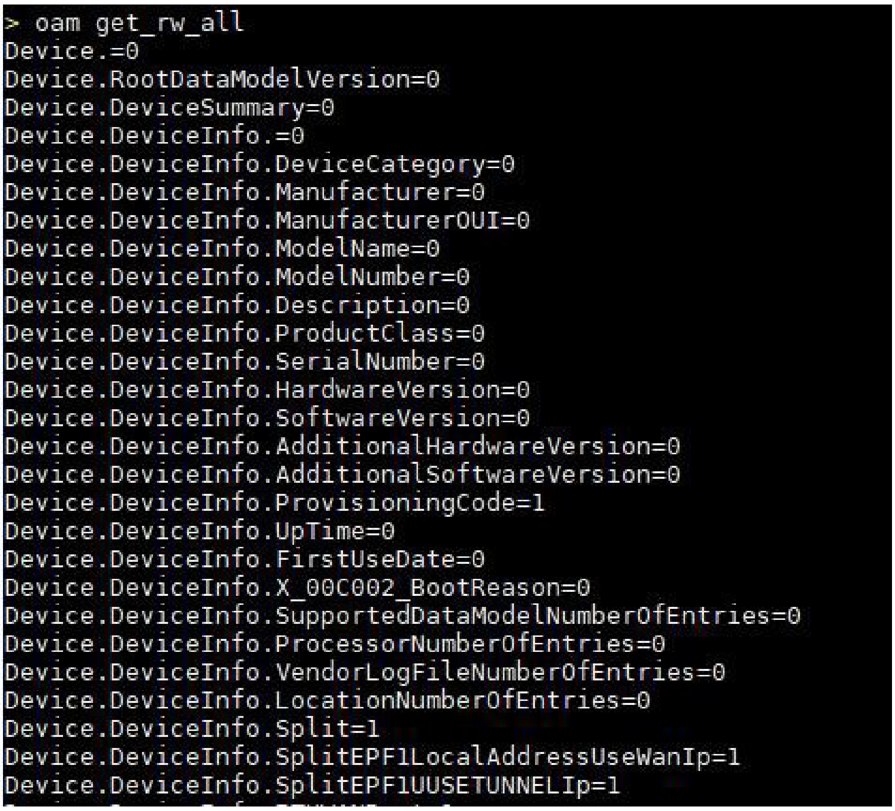


```
> oam get_rw Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.enable=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.inactivityTimer=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.retxTimerDL=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.retxTimerUL=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.longCycle=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.shortCycle=1
Device.Services.FAPService.1.X_00C002_gNB.DU.1.GNBDUFunction.NRCellDU.3.X_SC_drxConfig.longCycleTimer=1
```

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.

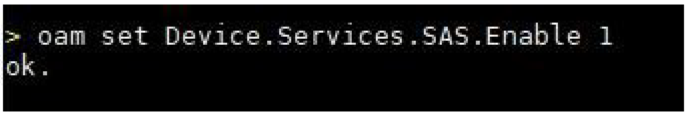


```
> oam get_rw_all
Device.=0
Device.RootDataModelVersion=0
Device.DeviceSummary=0
Device.DeviceInfo.=0
Device.DeviceInfo.DeviceCategory=0
Device.DeviceInfo.Manufacturer=0
Device.DeviceInfo.ManufacturerOUI=0
Device.DeviceInfo.ModelName=0
Device.DeviceInfo.ModelNumber=0
Device.DeviceInfo.Description=0
Device.DeviceInfo.ProductClass=0
Device.DeviceInfo.SerialNumber=0
Device.DeviceInfo.HardwareVersion=0
Device.DeviceInfo.SoftwareVersion=0
Device.DeviceInfo.AdditionalHardwareVersion=0
Device.DeviceInfo.AdditionalSoftwareVersion=0
Device.DeviceInfo.ProvisioningCode=1
Device.DeviceInfo.UpTime=0
Device.DeviceInfo.FirstUseDate=0
Device.DeviceInfo.X_00C002_BootReason=0
Device.DeviceInfo.SupportedDataModelNumberOfEntries=0
Device.DeviceInfo.ProcessorNumberOfEntries=0
Device.DeviceInfo.VendorLogFileNumberOfEntries=0
Device.DeviceInfo.LocationNumberOfEntries=0
Device.DeviceInfo.Split=1
Device.DeviceInfo.SplitEPF1LocalAddressUseWanIp=1
Device.DeviceInfo.SplitEPF1UUSETUNNELIp=1
```

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

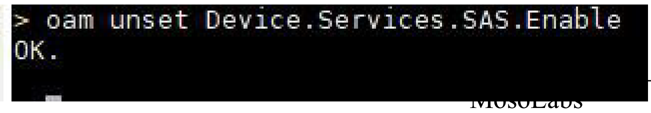


```
> oam set Device.Services.SAS.Enable 1
ok.
```

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.

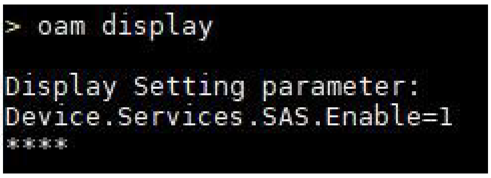


```
> oam unset Device.Services.SAS.Enable
OK.
```

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

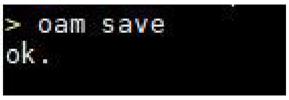


```
> oam display

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.

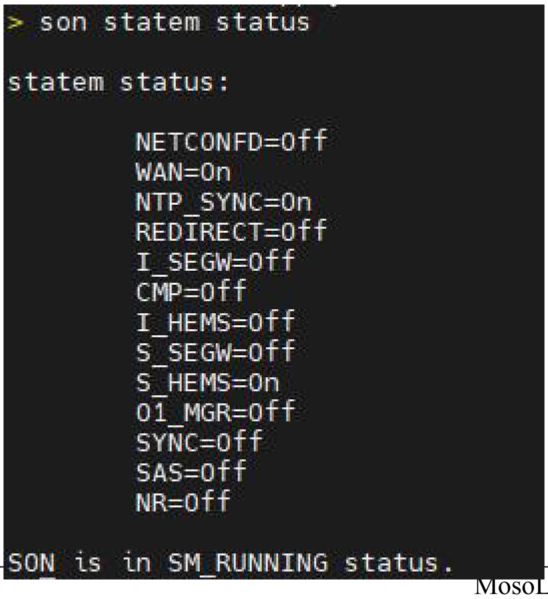


```
> oam save
ok.
```

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

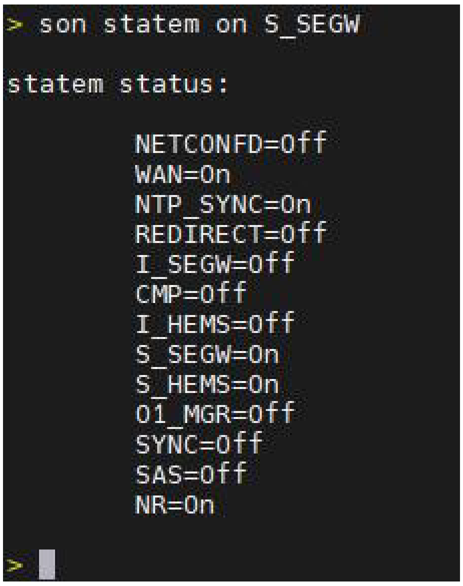


```
> son statem status

statem status:

        NETCONFD=Off
        WAN=On
        NTP_SYNC=On
        REDIRECT=Off
        I_SEGW=Off
        CMP=Off
        I_HEMS=Off
        S_SEGW=Off
        S_HEMS=On
        O1_MGR=Off
        SYNC=Off
        SAS=Off
        NR=Off

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.

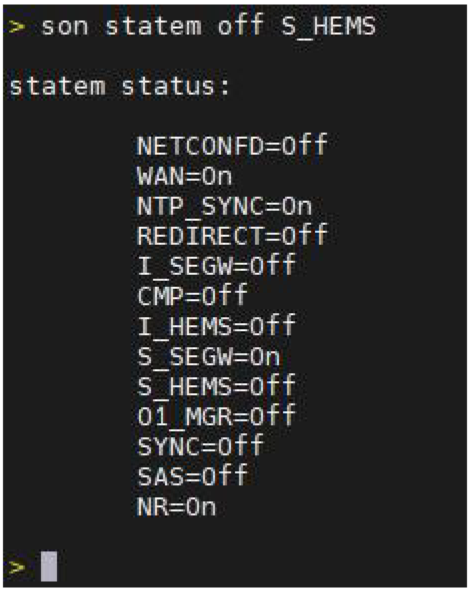


```
> son statem on S_SEGW

statem status:

        NETCONFD=Off
        WAN=On
        NTP_SYNC=On
        REDIRECT=Off
        I_SEGW=Off
        CMP=Off
        I_HEMS=Off
        S_SEGW=On
        S_HEMS=On
        O1_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.

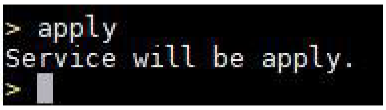


```
> son statem off S_HEMS

statem status:

        NETCONFD=Off
        WAN=On
        NTP_SYNC=On
        REDIRECT=Off
        I_SEGW=Off
        CMP=Off
        I_HEMS=Off
        S_SEGW=On
        S_HEMS=Off
        O1_MGR=Off
        SYNC=Off
        SAS=Off
        NR=On

> 
```

9.14. Apply All Parameter Changes

Step 1: use operator account to login ssh

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

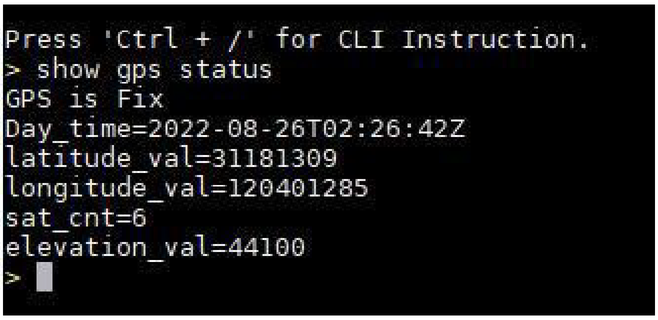


```
> apply
Service will be apply.
> 
```

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.

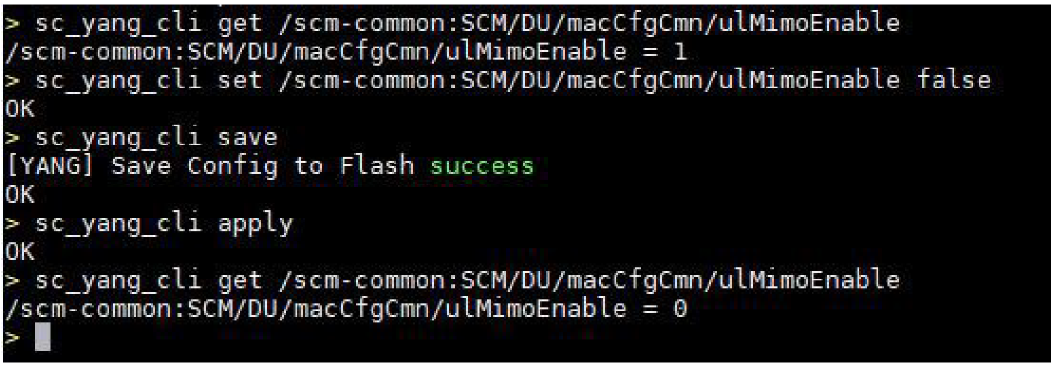


```
Press 'Ctrl + /' for CLI Instruction.
> show gps status
GPS is Fix
Day_time=2022-08-26T02:26:42Z
latitude_val=31181309
longitude_val=120401285
sat_cnt=6
elevation_val=44100
> 
```

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

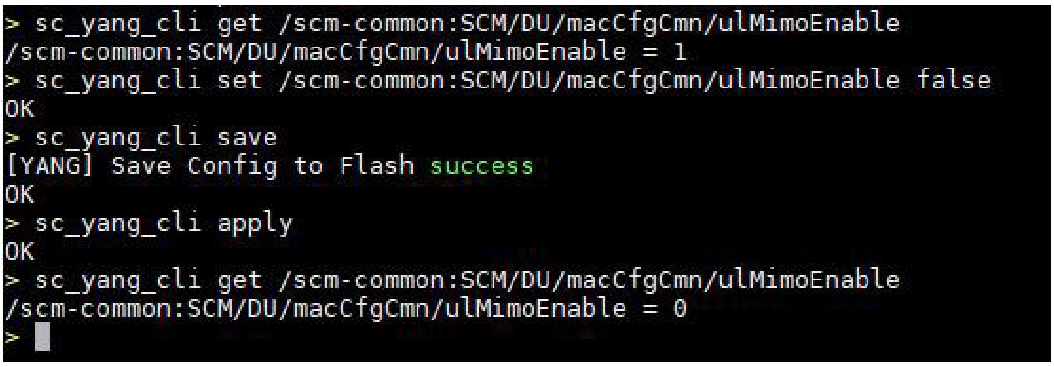


```
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
/scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 1
> sc_yang_cli set /scm-common:SCM/DU/macCfgCmn/ulMimoEnable false
OK
> sc_yang_cli save
[YANG] Save Config to Flash success
OK
> sc_yang_cli apply
OK
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
/scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 0
> 
```

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

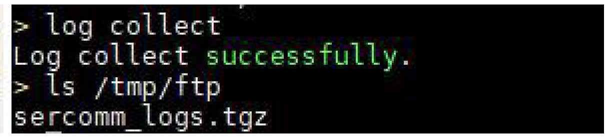


```
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
/scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 1
> sc_yang_cli set /scm-common:SCM/DU/macCfgCmn/ulMimoEnable false
OK
> sc_yang_cli save
[YANG] Save Config to Flash success
OK
> sc_yang_cli apply
OK
> sc_yang_cli get /scm-common:SCM/DU/macCfgCmn/ulMimoEnable
/scm-common:SCM/DU/macCfgCmn/ulMimoEnable = 0
> 
```

9.18. Support Download Log

Step 1: use sc_femto or operator account to login ssh

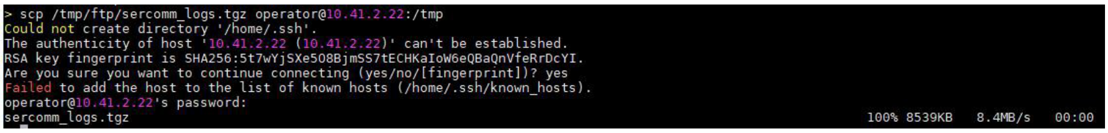
Step 2: use command “log collect” to package log file



```
> log collect
Log collect successfully.
> ls /tmp/ftp
sercomm_logs.tgz
```

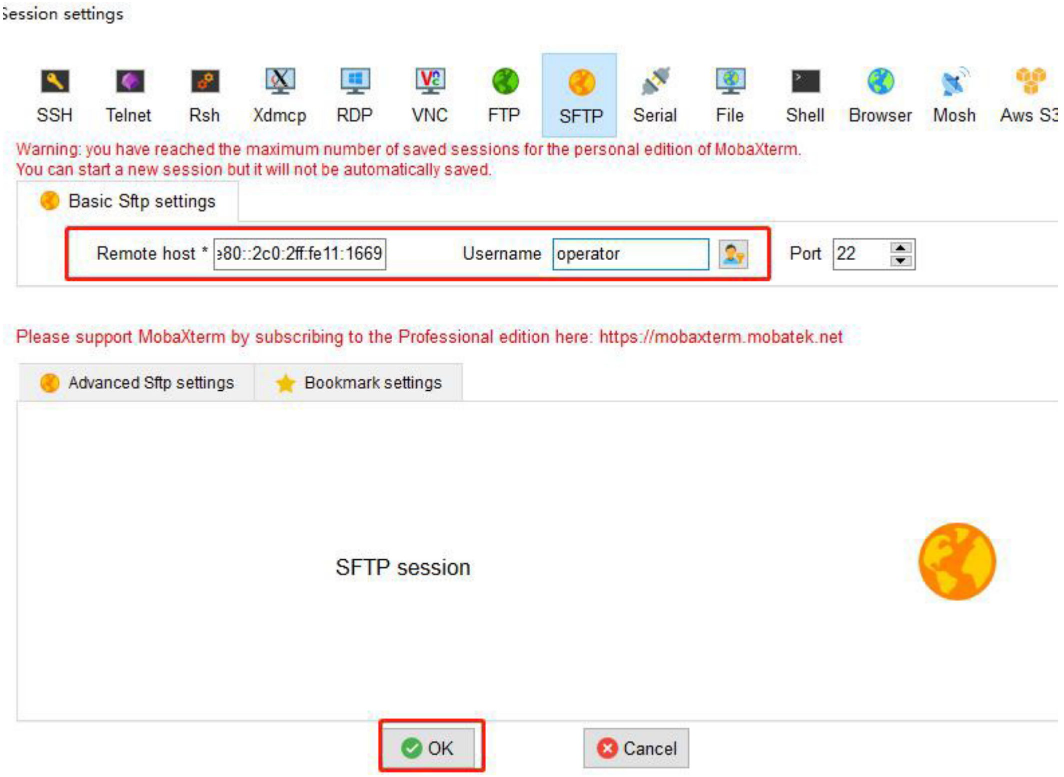
Step 3: download log and the logs are stored in /tmp/ftp/sercomm_logs.tgz

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



```
> scp /tmp/ftp/sercomm_logs.tgz operator@10.41.2.22:/tmp
Could not create directory '/home/.ssh'.
The authenticity of host '10.41.2.22 (10.41.2.22)' can't be established.
RSA key fingerprint is SHA256:5t7wYjSXe508BjmSS7tECHKaIoW6eQBaQnVfeRrDcYI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/.ssh/known_hosts).
operator@10.41.2.22's password:
sercomm_logs.tgz                                                                    100% 8539KB   8.4MB/s   00:00
```

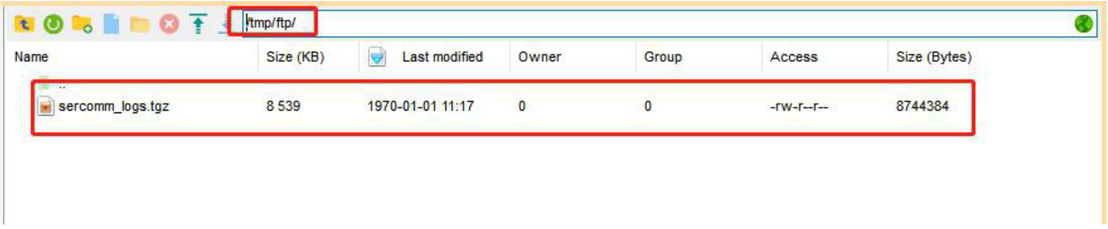
Method two: use sftp to download the log file



Warning: you have reached the maximum number of saved sessions for the personal edition of MobaXterm.
You can start a new session but it will not be automatically saved.

Remote host * ︰e80::2c0:2ff:fe11:1669   Username operator   Port 22

Please support MobaXterm by subscribing to the Professional edition here: https://mobaxterm.mobatek.net



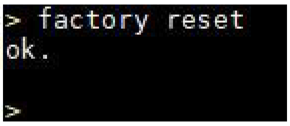
/tmp/ftp/

Name	Size (KB)	Last modified	Owner	Group	Access	Size (Bytes)
..						
sercomm_logs.tgz	8 539	1970-01-01 11:17	0	0	-rw-r--r--	8744384

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
```

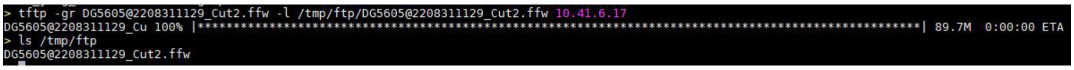
9.21. Support Firmware Version Upgrade

Step 1: use operator account to login ssh

Step 2: upload the firmware version file to /tmp/ftp

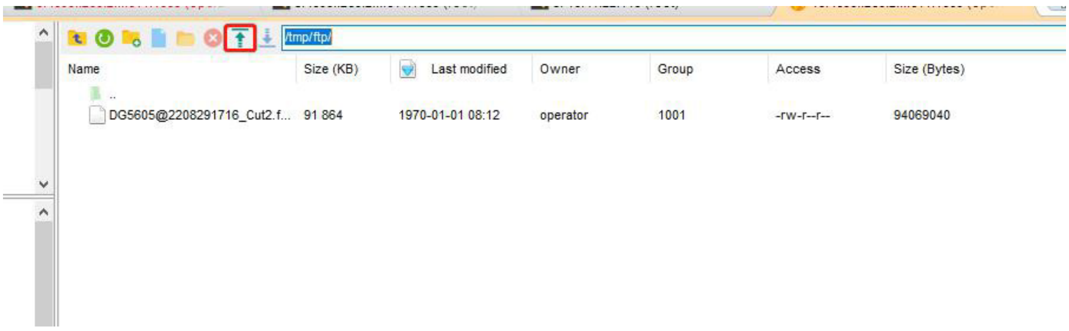
Step 3: use command “upgrade_cli -f /tmp/ftp/[FW_Name]”to upgrade the version

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



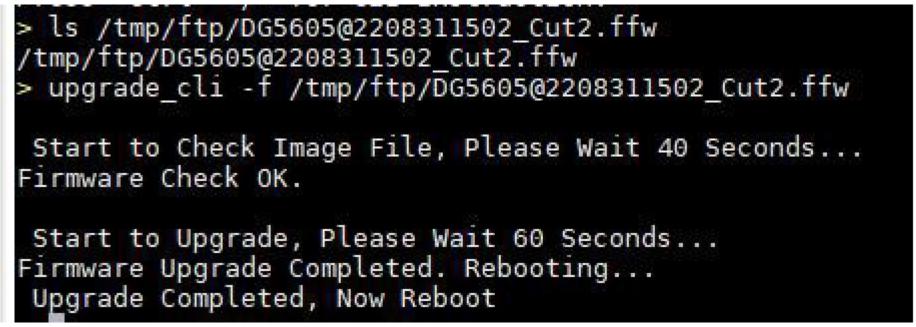
```
> tftp -gr DG5605@2208311129_Cut2.ffw -l /tmp/ftp/DG5605@2208311129_Cut2.ffw 10.41.6.17
DG5605@2208311129_Cu 100% |*****************************************************************************************************| 89.7M  0:00:00 ETA
> ls /tmp/ftp
DG5605@2208311129_Cut2.ffw
```

Method two: use sftp to upload the firmware version file:



/tmp/ftp/

Name	Size (KB)	Last modified	Owner	Group	Access	Size (Bytes)
..						
DG5605@2208291716_Cut2.f...	91 864	1970-01-01 08:12	operator	1001	-rw-r--r--	94069040



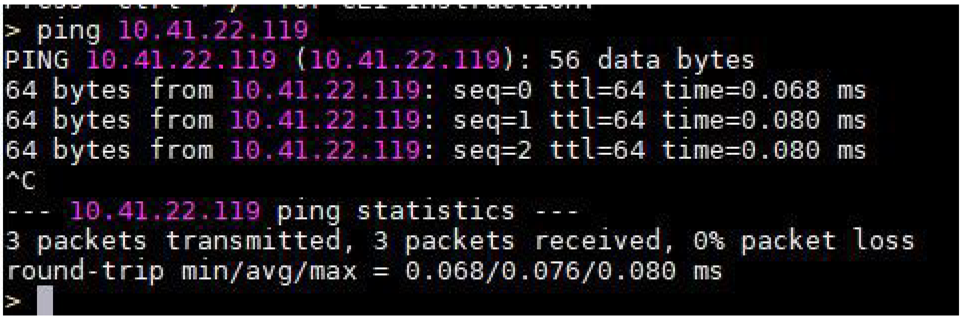
```
> ls /tmp/ftp/DG5605@2208311502_Cut2.ffw
/tmp/ftp/DG5605@2208311502_Cut2.ffw
> upgrade_cli -f /tmp/ftp/DG5605@2208311502_Cut2.ffw

 Start to Check Image File, Please Wait 40 Seconds...
Firmware Check OK.

 Start to Upgrade, Please Wait 60 Seconds...
Firmware Upgrade Completed. Rebooting...
 Upgrade Completed, Now Reboot
```

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.

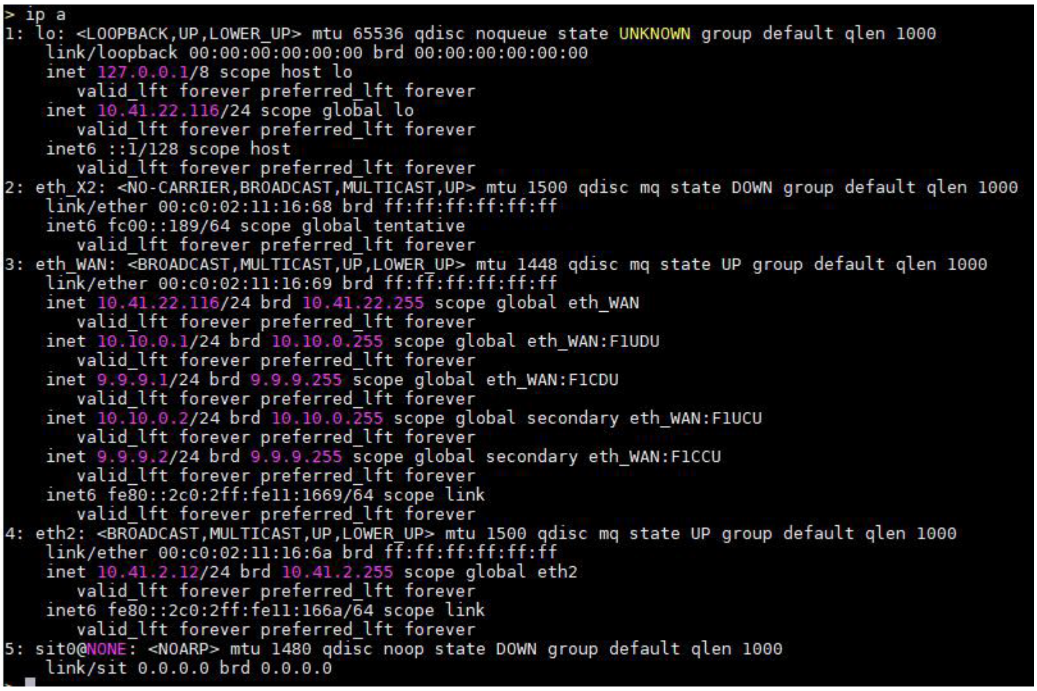


```
> ping 10.41.22.119
PING 10.41.22.119 (10.41.22.119): 56 data bytes
64 bytes from 10.41.22.119: seq=0 ttl=64 time=0.068 ms
64 bytes from 10.41.22.119: seq=1 ttl=64 time=0.080 ms
64 bytes from 10.41.22.119: seq=2 ttl=64 time=0.080 ms
^C
--- 10.41.22.119 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.068/0.076/0.080 ms
>
```

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.

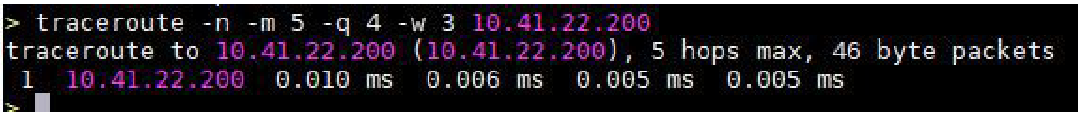


```
> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.41.22.116/24 scope global lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth_X2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 00:c0:02:11:16:68 brd ff:ff:ff:ff:ff:ff
    inet6 fc00::189/64 scope global tentative
       valid_lft forever preferred_lft forever
3: eth_WAN: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1448 qdisc mq state UP group default qlen 1000
    link/ether 00:c0:02:11:16:69 brd ff:ff:ff:ff:ff:ff
    inet 10.41.22.116/24 brd 10.41.22.255 scope global eth_WAN
       valid_lft forever preferred_lft forever
    inet 10.10.0.1/24 brd 10.10.0.255 scope global eth_WAN:F1UDU
       valid_lft forever preferred_lft forever
    inet 9.9.9.1/24 brd 9.9.9.255 scope global eth_WAN:F1CDU
       valid_lft forever preferred_lft forever
    inet 10.10.0.2/24 brd 10.10.0.255 scope global secondary eth_WAN:F1UCU
       valid_lft forever preferred_lft forever
    inet 9.9.9.2/24 brd 9.9.9.255 scope global secondary eth_WAN:F1CCU
       valid_lft forever preferred_lft forever
    inet6 fe80::2c0:2ff:fe11:1669/64 scope link
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:c0:02:11:16:6a brd ff:ff:ff:ff:ff:ff
    inet 10.41.2.12/24 brd 10.41.2.255 scope global eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::2c0:2ff:fe11:166a/64 scope link
       valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
> 
```

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.

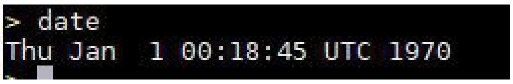


```
> traceroute -n -m 5 -q 4 -w 3 10.41.22.200
traceroute to 10.41.22.200 (10.41.22.200), 5 hops max, 46 byte packets
 1  10.41.22.200  0.010 ms  0.006 ms  0.005 ms  0.005 ms
> 
```

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

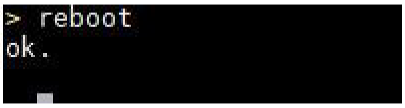


```
> date
Thu Jan  1 00:18:45 UTC 1970
> 
```

9.26. Support reboot command

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

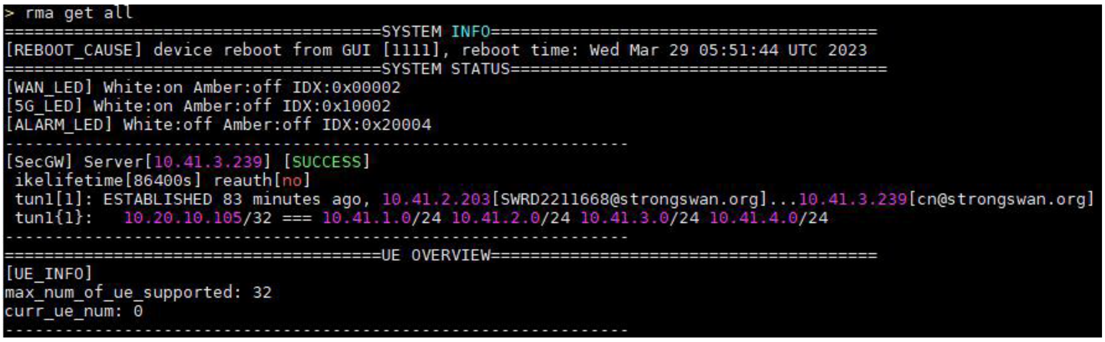
Step 1: use sc_femto or operator account to login ssh

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

SYSTEM INFO		
Reboot_Cause	The cause of last reboot, refer to section 9.27.2.	
SYSTEM STATUS		
LED	Show the state of lte led, and the corresponding pattern. Refer to section 9.27.3 for pattern mapping.	
SecGW	IPSec Status	IPSec connection status
	SecGW Server	Security gateway FQDN or IP address.
	IPSec Tunnel	Refer to section 9.27.4 for detailed explanation.

UE OVERVIEW

UE_INFO	Show the real time numbers of UE attached and the max numbers of supported UEs

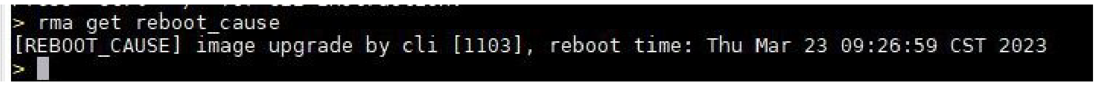


```
> rma get all
======================================SYSTEM INFO========================================
[REBOOT_CAUSE] device reboot from GUI [1111], reboot time: Wed Mar 29 05:51:44 UTC 2023
======================================SYSTEM STATUS======================================
[WAN_LED] White:on Amber:off IDX:0x00002
[5G_LED] White:on Amber:off IDX:0x10002
[ALARM_LED] White:off Amber:off IDX:0x20004
---------------------------------------------------------------
[SecGW] Server[10.41.3.239] [SUCCESS]
 ikelifetime[86400s] reauth[no]
 tun1[1]: ESTABLISHED 83 minutes ago, 10.41.2.203[SWRD2211668@strongswan.org]...10.41.3.239[cn@strongswan.org]
 tun1{1}:   10.20.10.105/32 === 10.41.1.0/24 10.41.2.0/24 10.41.3.0/24 10.41.4.0/24
---------------------------------------------------------------
======================================UE OVERVIEW========================================
[UE_INFO]
max_num_of_ue_supported: 32
curr_ue_num: 0
---------------------------------------------------------------
```

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



```
> rma get reboot_cause
[REBOOT_CAUSE] image upgrade by cli [1103], reboot time: Thu Mar 23 09:26:59 CST 2023
>
```

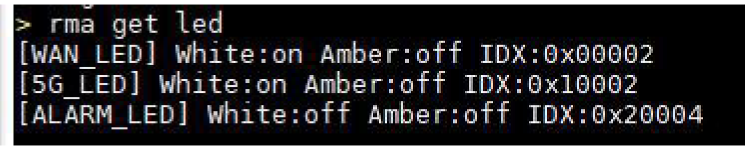
Reboot Detail	Description
1101	remote image upgrade by HEMS
1102	remote image upgrade by O1MGR
1103	image upgrade by cli
1104	image upgrade by GUI
1105	factory reset
1109	device reboot from HEMS
1110	device reboot from O1MGR
1111	device reboot from GUI
1112	system monitor check process crash

1120	set customer by CLI
1123	config restore by GUI
1124	device overheat
1125	CPU overload
1128	tti fail
1130	Cel1 auto reboot after it not active for 30min
1131	wan ip disconnected
1133	DU crash make the gnb reboot
1134	CU crash make the gnb reboot
1135	image upgrade by CLI
1201	Power down make last reboot
1401~1404	unidentified-failure

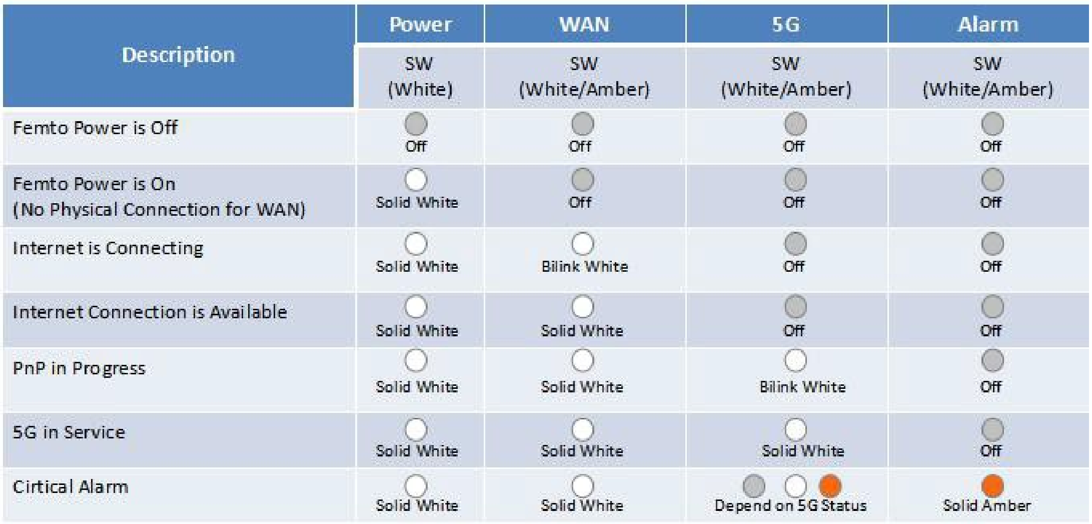
9.27.3 rma get led

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
```



Description	Power	WAN	5G	Alarm
	SW (White)	SW (White/Amber)	SW (White/Amber)	SW (White/Amber)
Femto Power is Off	Off	Off	Off	Off
Femto Power is On (No Physical Connection for WAN)	Solid White	Off	Off	Off
Internet is Connecting	Solid White	Bilink White	Off	Off
Internet Connection is Available	Solid White	Solid White	Off	Off
PnP in Progress	Solid White	Solid White	Bilink White	Off
5G in Service	Solid White	Solid White	Solid White	Off
Cirtical Alarm	Solid White	Solid White	Depend on 5G Status	Solid Amber

9.27.4 rma get secgw

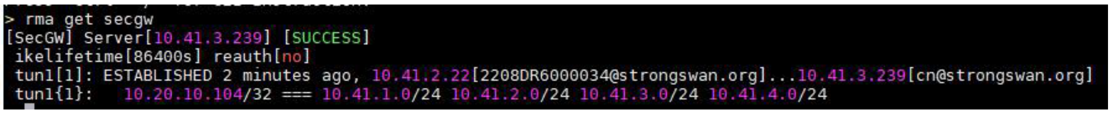
Step 1: use sc_femto or operator account to login ssh

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.

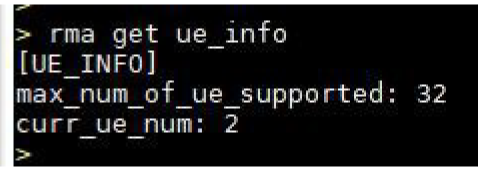


```
> rma get secgw
[SecGW] Server[10.41.3.239] [SUCCESS]
 ikelifetime[86400s] reauth[no]
 tun1[1]: ESTABLISHED 2 minutes ago, 10.41.2.22[2208DR6000034@strongswan.org]...10.41.3.239[cn@strongswan.org]
 tun1{1}:   10.20.10.104/32 === 10.41.1.0/24 10.41.2.0/24 10.41.3.0/24 10.41.4.0/24
```

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 .

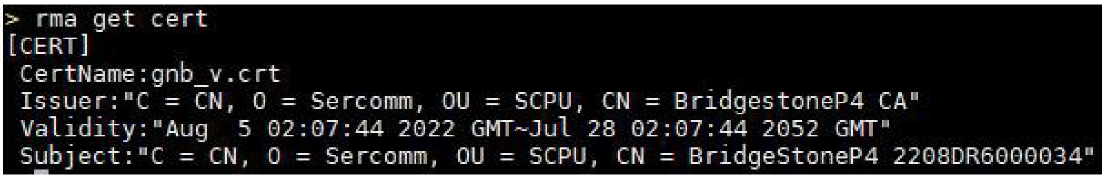


```
> rma get ue_info
[UE_INFO]
max_num_of_ue_supported: 32
curr_ue_num: 2
>
```

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 certificates.

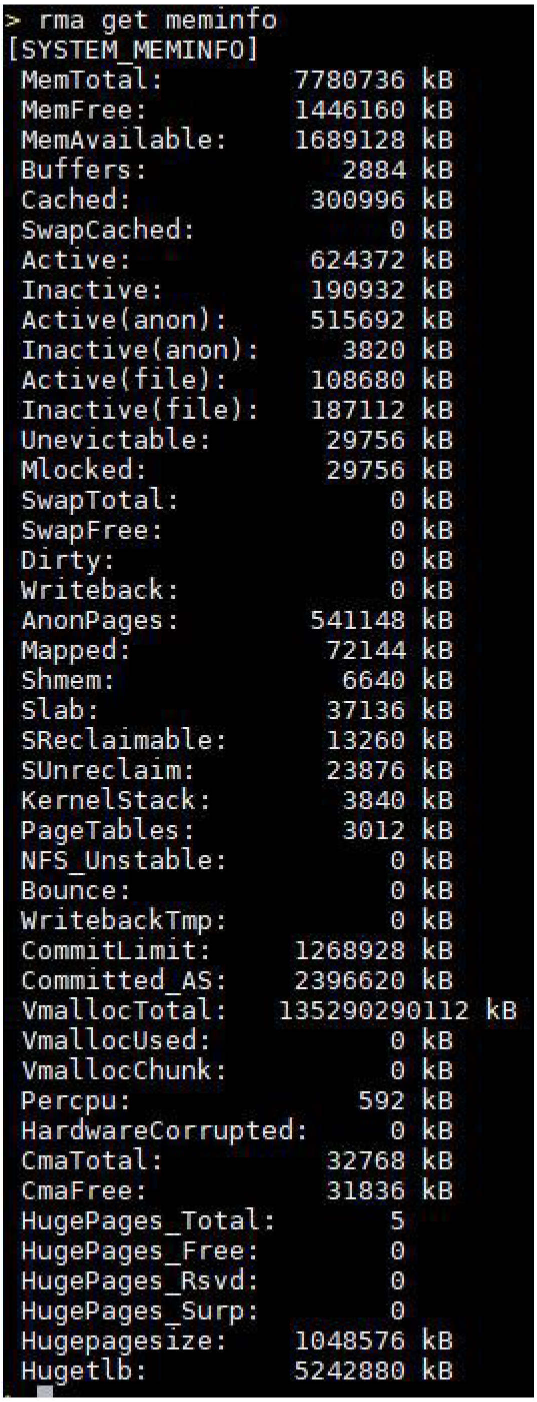


```
> rma get cert
[CERT]
 CertName:gnb_v.crt
 Issuer:"C = CN, O = Sercomm, OU = SCPU, CN = BridgestoneP4 CA"
 Validity:"Aug  5 02:07:44 2022 GMT~Jul 28 02:07:44 2052 GMT"
 Subject:"C = CN, O = Sercomm, OU = SCPU, CN = BridgeStoneP4 2208DR6000034"
```

9.27.7 rma get meminfo

Step 1: use sc_femto or operator account to login ssh

Step 2: use command “rma get meminfo” to get cert memory information.

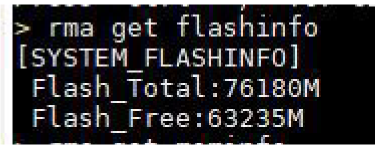


```
> rma get meminfo
[SYSTEM_MEMINFO]
 MemTotal:          7780736 kB
 MemFree:           1446160 kB
 MemAvailable:      1689128 kB
 Buffers:              2884 kB
 Cached:             300996 kB
 SwapCached:              0 kB
 Active:             624372 kB
 Inactive:           190932 kB
 Active(anon):       515692 kB
 Inactive(anon):       3820 kB
 Active(file):       108680 kB
 Inactive(file):     187112 kB
 Unevictable:         29756 kB
 Mlocked:             29756 kB
 SwapTotal:               0 kB
 SwapFree:                0 kB
 Dirty:                   0 kB
 Writeback:               0 kB
 AnonPages:          541148 kB
 Mapped:              72144 kB
 Shmem:                6640 kB
 Slab:                37136 kB
 SReclaimable:        13260 kB
 SUnreclaim:          23876 kB
 KernelStack:          3840 kB
 PageTables:           3012 kB
 NFS_Unstable:            0 kB
 Bounce:                  0 kB
 WritebackTmp:            0 kB
 CommitLimit:       1268928 kB
 Committed_AS:      2396620 kB
 VmallocTotal:    135290290112 kB
 VmallocUsed:             0 kB
 VmallocChunk:            0 kB
 Percpu:                592 kB
 HardwareCorrupted:       0 kB
 CmaTotal:            32768 kB
 CmaFree:             31836 kB
 HugePages_Total:         5
 HugePages_Free:          0
 HugePages_Rsvd:          0
 HugePages_Surp:          0
 Hugepagesize:      1048576 kB
 Hugetlb:           5242880 kB
```

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

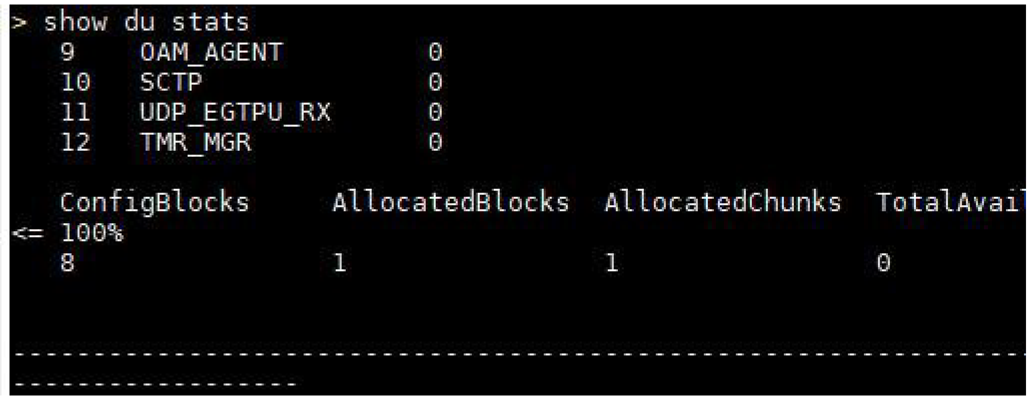


```
> rma get flashinfo
[SYSTEM_FLASHINFO]
 Flash_Total:76180M
 Flash_Free:63235M
```

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

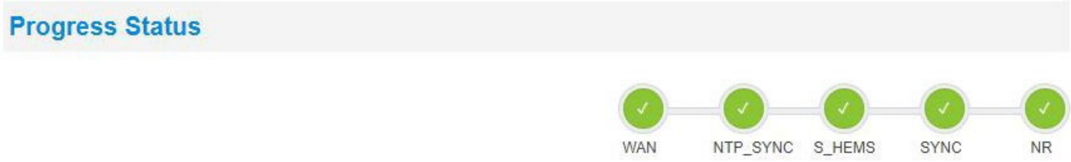


```
> show du stats
   9    OAM_AGENT          0
   10   SCTP               0
   11   UDP_EGTPU_RX       0
   12   TMR_MGR            0

   ConfigBlocks     AllocatedBlocks  AllocatedChunks  TotalAvai
<= 100%
   8                1                1                0


-----------------------------------------------------------------
------------------
```

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