

SLC-120XOGA SERIES ENGINEER GUIDE

SEOWON INTECH

V 1.1.3

2019.01.25

1.	INTRODUCTION TO THE PRODUCT	4
1.1.	PC CONFIGURATION (WINDOWS 7)	4
1.2.	HOW TO CHECK YOUR IP ADDRESS	6
2.	BUILD-IN WEB SERVER ACCESS	8
3.	SETUP ON THE WEB PAGE	9
3.1.	DASHBOARD	9
3.2.	CONNECTION MODE	11
3.3.	STATUS	12
3.3.1.	LTE	12
3.3.2.	NETWORK	17
3.3.3.	DEVICE DETAILS	19
3.3.4.	DEVICE PERFORMANCE	20
3.4.	SETTINGS	22
3.4.1.	LTE	22
3.4.1.1.	CELL SELECTION	22
3.4.1.2.	CELL LOCK	24
3.4.1.3.	PCI CELL LOCK	25
3.4.1.4.	SIM MANAGEMENT	26
3.4.1.5.	DEFAULT PDN	27
3.4.1.6.	MULTIPLE PDN	28
3.4.1.7.	INTERNET MTU	29
3.4.1.8.	IPv6 SETTINGS	30
3.4.1.9.	CBSD SETTINGS	31
3.4.2.	NETWORK	34
3.4.2.1.	SWITCH	34
3.4.2.2.	DHCP SERVER	36
3.4.2.3.	DMZ	38
3.4.2.4.	PORT FORWARDING	39
3.4.2.5.	PORT TRIGGERING	40
3.4.2.6.	VPN CONFIGURATION	42
3.4.2.7.	VPN PASSTHROUGH	45
3.4.2.8.	UPNP	46
3.4.2.9.	QoS	47
3.4.2.10.	DDNS	49
3.4.3.	FIREWALL	51
3.4.3.1.	BASIC	51
3.4.3.2.	FILTER SETUP	52
3.4.3.3.	ACCESS CONTROL	56
3.4.3.4.	IP-MAC BINDING	59
3.4.4.	USER MANAGEMENT	61
3.4.4.1.	ACCOUNT	61
3.4.4.2.	LANGUAGE	62
3.4.4.3.	RESTORE DEFAULT	63
3.4.4.4.	REBOOT	64
3.4.4.5.	TR-069 SETTINGS	65
3.4.4.6.	DATE AND TIME	66
3.4.4.7.	FOTA	67
3.4.4.8.	SNMP	68
3.4.4.9.	REMOTE MANAGEMENT	69
3.4.5.	FIRMWARE MANAGEMENT	70
3.4.5.1.	SOFTWARE	70
3.4.6.	MONITORING	71
3.4.6.1.	IPERF	71
3.4.6.2.	DIAGNOSTIC	72
3.4.6.3.	LOG	74

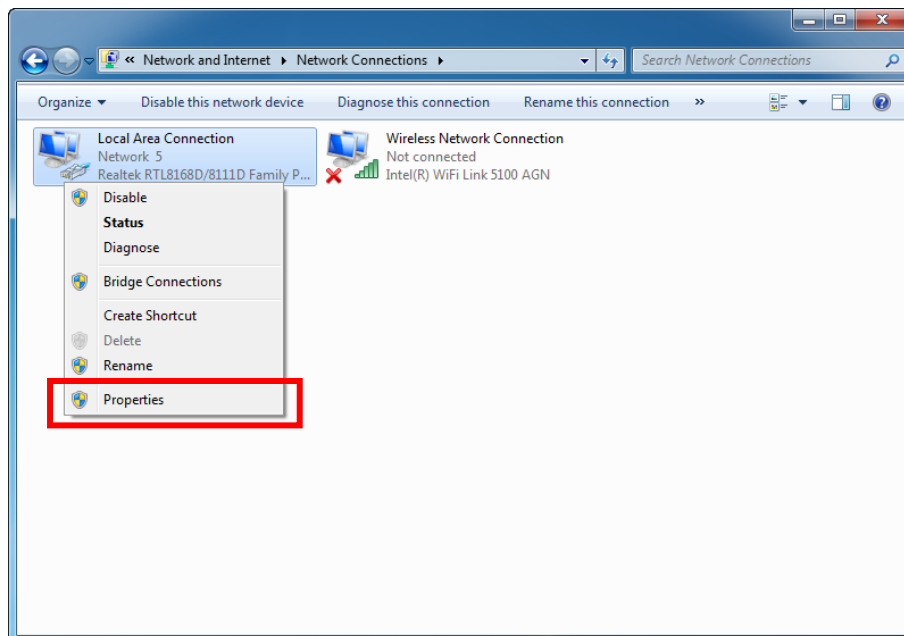
4. THE DEFAULT SETTING FOR THE SLC-1200GA CPE.....	76
ACRONYMS	78

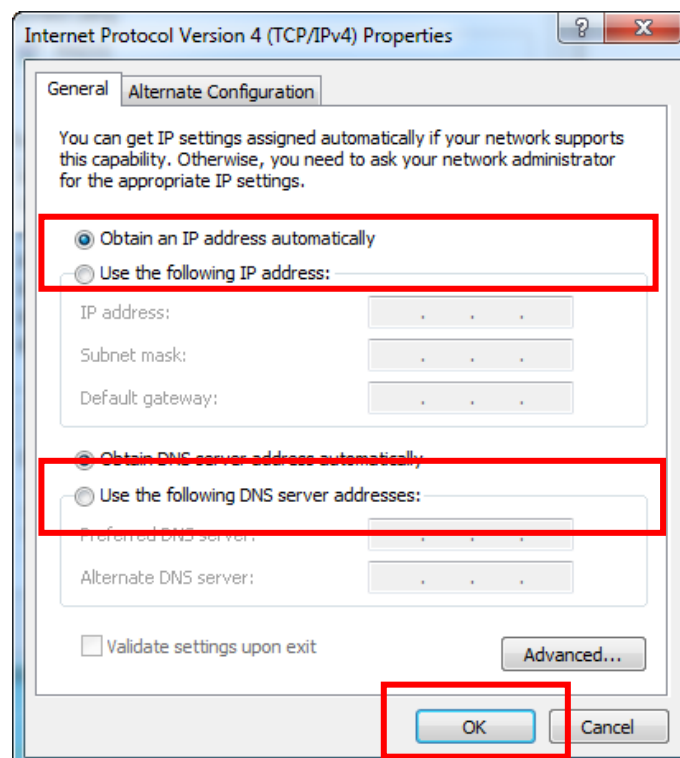
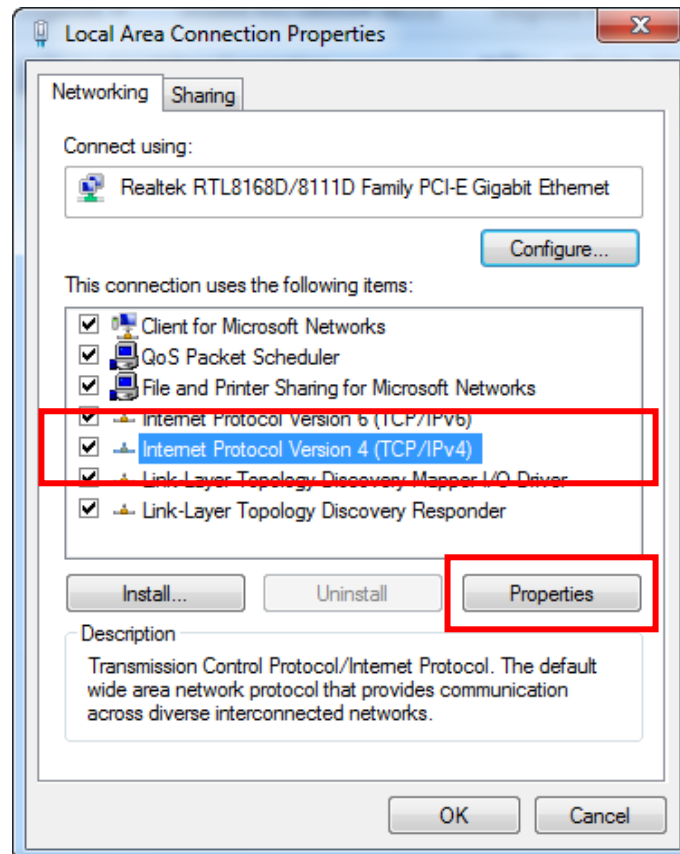
1. Introduction to the Product

1.1. PC Configuration (Windows 7)

Most computers already have the TCP/IP configuration enabled. For your computer to support CPE, please verify that the IP address and DNS settings are automatically generated in the Local Area connection of your Internet Protocol (TCP/IP) properties.

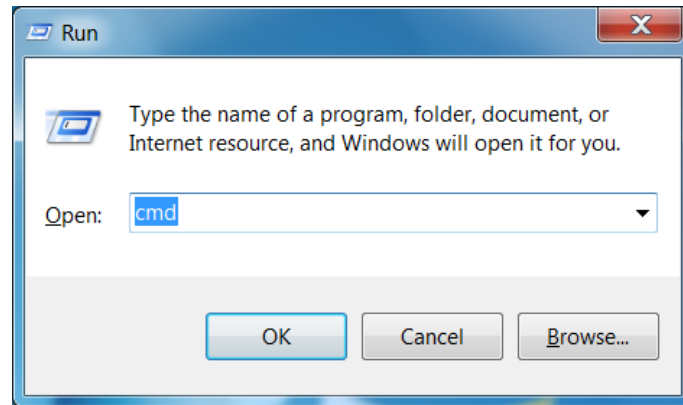
- In a Windows environment :
- Click “**Start**” button >> Click “**Control Panel**”>> Click “**Network and Internet Connection**”>> Click “**Network Connection**”>> Right-click “**Local Area Connection**”and Select “**Properties**”>> Select “**Internet Protocol 4(TCP/IPv4)**” and click “**Properties**”>> Select “**obtain an IP address automatically**” and “**obtain DNS server address automatically**”>> Click “**OK**”.





1.2. How To Check your IP address

Open the Command Prompt window by clicking the “**Start**” button and selecting “**Run**”. Enter “cmd”, and click the “OK” button.



<Run cmd>

- When the Command Prompt window opens , enter the “ipconfig” command to verify the IP address , Subnet mask , and Gateway , which are automatically assigned to PC

[Note] PCs connected to Device will receive own assigned IP address.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>_
```

<Verify IP address>

```
C:\Users\Steve_Kim>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=8ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

If the host can reach the device using the ping command, the device has successfully attached.

[Note] If an IP address is not assigned, check the following, and then restart the PC and check whether an IP address is assigned.

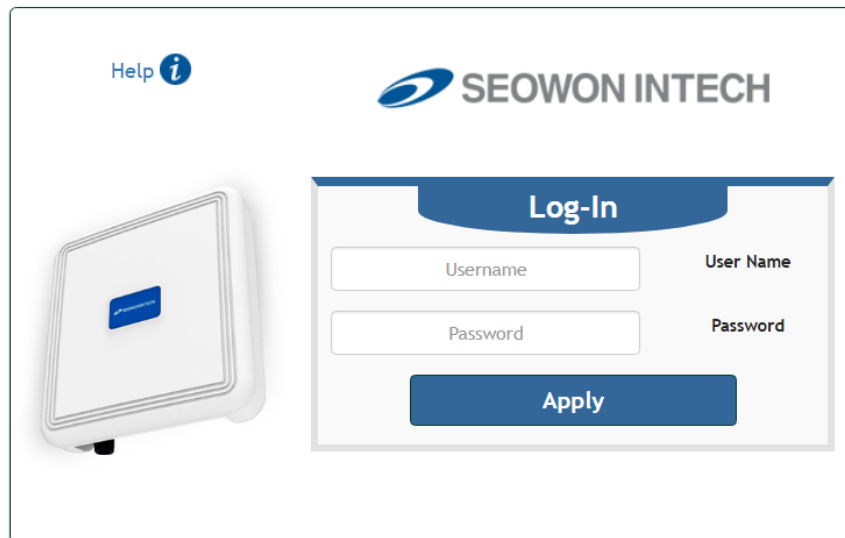
- ✓ LAN cable connection between PC and Device.
- ✓ Check TCP/IP setup details

2. Build-in Web Server Access

The Web Browser allows you to manage the Device and to view.

In the Address Bar:

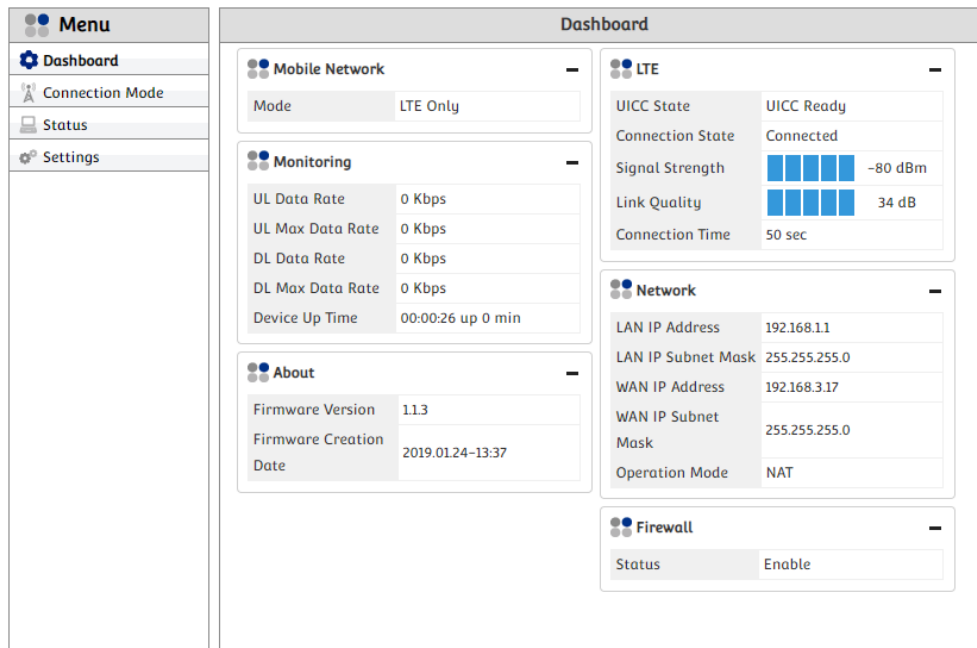
- Type <http://192.168.1.1> and press ENTER to access the login screen.
- When the login screen appears, it prompts you for a password.
- Default engineer ID and password are “**system / system**”
- You can change the password after logged in (Passwords are case-sensitive).



[Note] The Web Interface can be accessed by entering <http://192.168.1.1> in the Address Bar, regardless of the network connection status. When there is no input for 1 hour after your login to the Web Interface, you will be automatically logged out.

3. Setup on the web page

3.1. Dashboard



“Dashboard” shows overall status of CPE’s functionality. A user can see LTE connection status, transferred Data rate, LAN and WAN IP address assigned, and Firmware version information at a glance.

- Mobile Network
 - ✓ Mode : Currently supported Radio Access Technology
 - ✓ Operator : Manufacturer of CPE
- LTE
 - ✓ UICC state : Status of USIM card inserted
 - ✓ Connection State : Connection status on LTE network
 - ✓ PDN Type : IPv4 / Plv6
- Monitoring
 - ✓ UL Data Rate : Current Uplink Data Rate
 - ✓ UL Max Data Rate : Maximum Uplink Data Rate reached
 - ✓ DL Data Rate : Current Downlink Data Rate
 - ✓ DL Max Data Rate : Maximum Downlink Data Rate reached
 - ✓ Device Up Time : Time elapsed after CPE turned on
- Network
 - ✓ LAN IP Address : IP address assigned by LAN DHCP Server
 - ✓ LAN IP Subnet Mask : Subnet Mask address assigned by LAN DHCP Server
 - ✓ WAN IP Address : WAN (LTE) IP address assigned to CPE

- ✓ WAN IP Subnet Mask : WAN (LTE) Subnet Mask address assigned to CPE
- ✓ Operation Mode : Switch mode status. NAT / Bridge
- About
 - ✓ Firmware Version : Version of current firmware
 - ✓ Firmware Creation Date : The time when Firmware made
- Firewall
 - ✓ Status : Enable / Disable status of Firewall

3.2. Connection Mode

Menu	
Dashboard	
Connection Mode	
Status	
Settings	

Connection Mode

Operation
Auto-connect: Auto ▼ Apply

Connect Manager
Status: Connected
Action: Connect Disconnect

- Operation
 - ✓ Auto-connect : A user can select LTE registration time after CPE's boot-up. "Auto" means CPE tries to attach LTE network just after boot-up. "Manual" means CPE will not try to attach LTE network until a user clicks "Connect" in the "Connect Manager" menu.
- Connect Manager
 - ✓ A user can "CONNECT" or "DISCONNECT" LTE connectivity by this menu.

3.3. Status

3.3.1. LTE

Menu	LTE Status			
	LTE Information			
	LTE Status			
	LTE Statistics			
LTE	LTE Information			
	FW Ver	0.3.2.21	CM Ver	3.7.18.2
	SDK Ver	0.64.13.0	Driver Ver	1.0.2.2
	IMEI	352470060006193	IMSI	001010000000023
Settings				

This table shows LTE software version information, device ID and USIM ID.

- FW Ver : Modem firmware version
- CM Ver : LTE Connection Manager version
- SDK Ver : SDK version
- Driver Ver : LTE Driver version
- IMEI : International Mobile Equipment Identity
- IMSI : International Mobile Subscriber Identity of inserted USIM

Menu		LTE Status			
Dashboard		LTE Information			
Connection Mode		LTE Status			
Status		LTE Statistics			
LTE		LTE Status			
Network		UICC State			
Device Details		UICC Ready			
Device Performance		Connection			
Settings		Connected			
		Band			
		42			
		APN Name			
		PDN Type			
		IPv4 & IPv6			
		IP v4 Address			
		192.168.3.17			
		IP v6 Address			
		2600:0:0:0:0:05:345			
		PLMN Search			
		Success			
		MCC			
		001			
		PLMN Selected			
		00101			
		MNC			
		01			
		Cell Global ID			
		0xdcd8602 (231572994)			
		EMM State			
		Registered [EMM-REGISTERED]			
		eNodeB ID			
		0xdcd86 (904582)			
		Cell ID			
		0x2 (2)			
		Current UL T/P			
		0 Kbps			
		Service Cell State			
		RRC CONNECTED			
		CQI			
		15			
		Transmission Mode			
		TM [4]			
		Auto Refresh			
		<input type="checkbox"/>			
		Current CA			
		2 CA			
		Current Uplink CA			
		2 CA			
		Primary Cell			
		Physical CELL ID			
		0x3c (60)			
		TX power			
		-34.8 dB			
		RSSI			
		-57.4/-54.1 dBm			
		RSRP			
		-83.3/-80.1 dBm			

All LTE information like Radio Frequency, Throughput, IP address, and Connection status are displayed in this page. Also, if the device is connected by multiple antennas, "Secondary Cell" information will be displayed.

- UICC State : Universal Integrated Circuit Card, status of inserted USIM card
- Connection : LTE connection status (Connected / Not Connected)
- PDN Type : Connected Packet Data Network type
- Band : Camped LTE Frequency Band
- IP v4 Address : IP v4 Address from network
- IP v6 Address: IP v6 Address from network
- PLMN Search: Searching or Registration status of Public Land Mobile Network
- MCC : Mobile Country Code
- PLMN Selected : Network Identifier of camped network
- MNC : Mobile Network Code
- Cell Global ID : E-UTRAN Cell Identifier. eNodeB ID + Cell ID
- EMM state : EPS Mobility Management (One of NAS function) status
- eNodeB ID : eNodeB ID
- Cell ID : Cell ID
- UL EARFCN : Uplink Evolved-UTRA Absolute Radio Frequency Channel Number
- UL Freq. : Uplink Frequency that matched to UL EARFCN [MHz]
- Current UL T/P : Current Uplink Throughput [Kbps]
- Current DL T/P : Current Downlink Throughput [Kbps]

- UL MCS : Modulation and Coding Scheme used in Uplink
20(1) : MCS index (The number of allocated Resource Block)
- TX power : Transmission Power [dB]
- Service Cell state : RRC (Radio Resource Control) state
- CQI : Channel Quality Indicator
- Transfer Mode : Transmission Mode
- Auto Refresh : If checked, all LTE Status values are renewed by every second
- Current CA : Carrier Aggregation Status. Non-CA / 2CA / 4CA

Menu

Dashboard

Connection Mode

Status

LTE

Network

Device Details

Device Performance

Settings

LTE Status

LTE Information

LTE Status

LTE Statistics

LTE Statistics

Rx packets1Tx packets632

Rx bytes88Tx bytes44354

CQI Statistics

APERIODIC

Mode	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
MODE1-2	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE2-0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE2-2	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE3-0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE3-1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0

PERIODIC

Mode	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
MODE1-0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE1-1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	5,5
MODE2-0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
MODE2-1	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0

You can see how many Packets and Bytes are exchanged through LTE network from power-on of the device.

Also, CQI (Channel Quality Indicator) Report Statistics is displayed as tables, arranged by CQI Index and Transmission Mode, and by Aperiodic and Periodic reporting.

- Rx Packets : The number of received packets
- Tx Packets : The number of sent packets
- Rx Bytes : The size of received Bytes
- Tx Bytes : The size of sent Bytes
- CQI Index : 1 – 16
- MODE1-2 : Transmission Mode that is decided by the combination of CQI and PMI (Precoding Matrix Indicator)
- APERIODIC : CQI is transmitted periodically with a certain interval specified by higher layer message
- PERIODIC : CQI is transmitted by a special trigger
- CW0,CW1 : CQI reporting counts through Code Word 0, Code Word 1

3.3.2. Network

Menu

Dashboard

Connection Mode

Status

LTE

Network

Device Details

Device Performance

Settings

Network Information

WAN

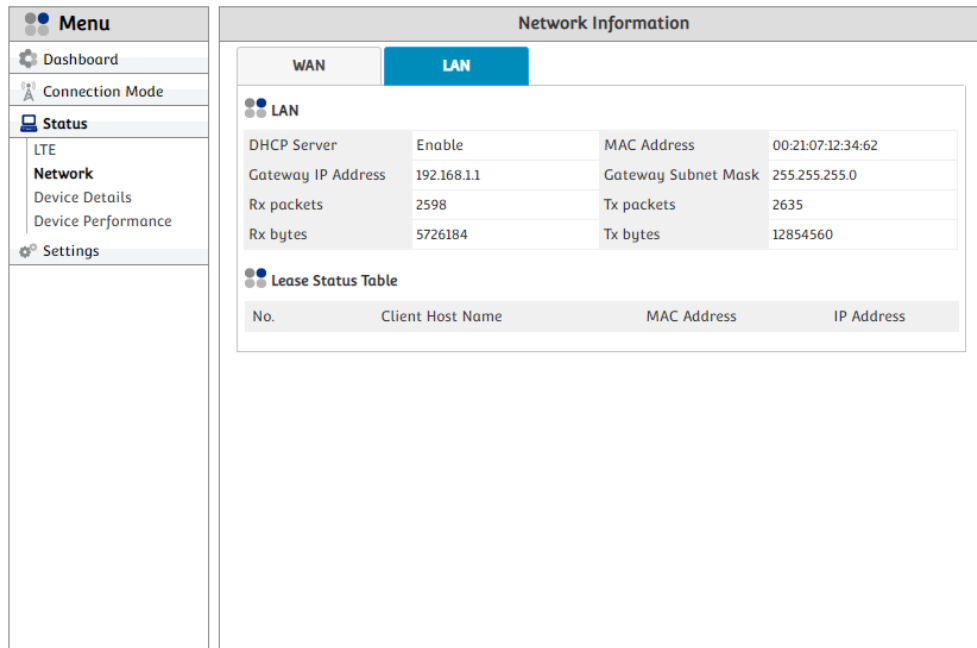
LAN

WAN

WAN IP Address	192.168.3.17	WAN IP Subnet Mask	255.255.255.0
WAN IP Default Gateway	192.168.3.238		
Primary DNS	168.126.63.1	Secondary DNS	168.126.63.2

This page shows IP address of WAN(LTE network) side.

- WAN
 - ✓ WAN IP Address : WAN(LTE) IP address assigned to CPE
 - ✓ WAN IP Subnet Mask : WAN(LTE) Subnet Mask address assigned to CPE
 - ✓ WAN IP Default Gateway : WAN(LTE) Default Gateway address assigned to CPE
(All packets (except its destination IP address is inside LTE network) are delivered to the Default Gateway)
 - ✓ Primary DNS : First DNS address assigned to CPE
 - ✓ Secondary DNS : Second DNS address assigned to CPE



LAN(Ethernet)Information is displayed in the menu.

- LAN

- ✓ DHCP Server : LAN DHCP Server status (Enable / Disable)
- ✓ MAC Address : LAN(Ethernet) MAC (Media Access Control) address
- ✓ Gateway IP Address : Gateway IP address assigned by LAN DHCP Server
- ✓ Gateway Subnet Mask : Subnet Mask address assigned by LAN DHCP Server
- ✓ Rx Packets : The number of all packets received through LAN connection
- ✓ Tx Packets : The number of all packets sent through LAN connection
- ✓ Rx bytes : Sum of all packets received through LAN connection [bytes]
- ✓ Tx bytes : Sum of all packets sent through LAN connection [bytes]
- ✓ Lease Status Table : The list of all the device which are connected by LAN and assigned IP, Subnet Mask, and Default Gateway Address by CPE

3.3.3. Device Details

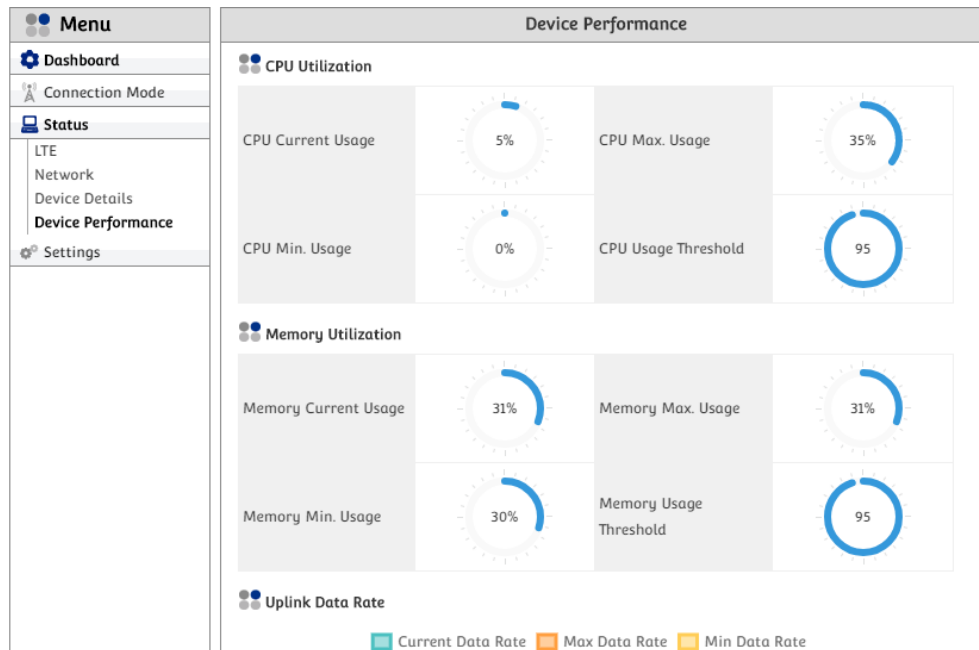
Menu	Device Details			
Dashboard				
Connection Mode				
Status				
LTE				
Network				
Device Details				
Device Performance				
Settings				

Device Details			
Device Time			
Current Local Time	2015-01-01 00:21:52	Time Server	ntp1.caLnet
Synchronize With PC	Out of sync	Time Zone	Pacific Time (US and Canada)
Daylight Saving Time	Enable		
Device Information			
ODM	Seowonintech co., LTD.	Product Name	SLC-120T42OGA
OUI	00:21:07	Serial Number	SEOWONXX130T03-0000001
Firmware Version	1.1.3	Firmware Creation Date	2019.01.24-13:37
Hardware Version	1.0	Last reboot cause	Abnormal Reboot by Electrical Power Off or Defect Device

This page shows the device and time information.

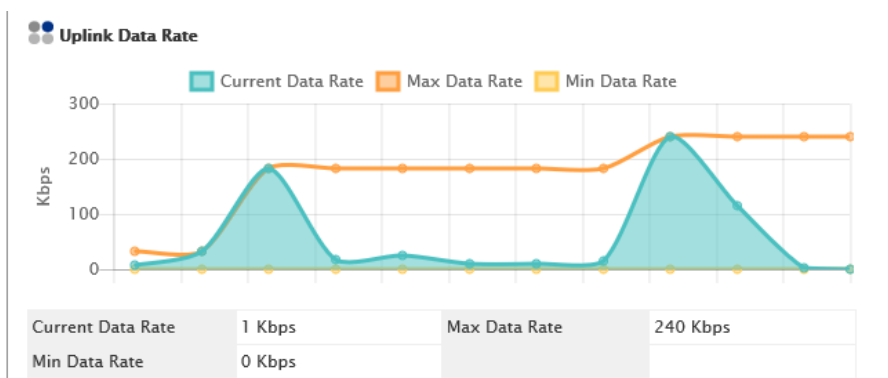
- Current Local Time : Current time where CPE is located
- Time Server : Server address that CPE synchronize its time
- Synchronize With PC : Time synchronization status between connected PC and CPE
- Time Zone : Standard time of CPE
- Daylight Saving Time : Daylight Saving Time (Summer Time) status (Enable / Disable)
- ODM : Original Development Manufacturing of CPE
- Product Name : Model name
- OUI : Organizationally Unique Identifier. Uniquely identifies a vendor, manufacturer
- Serial Number : Uniquely assigned to every CPE by manufacturer
- Firmware Version : Version of current firmware
- Firmware Creation Data : The time when Firmware made
- Hardware Version : Hardware Version.

3.3.4. Device Performance

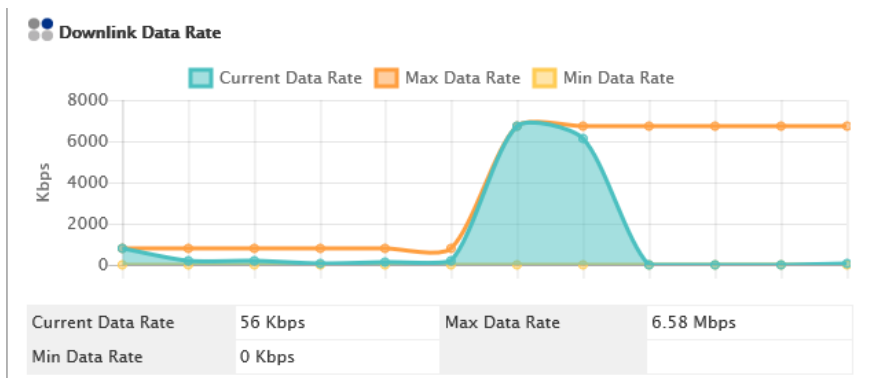


Several statistics relative to Device performance, is shown.

- CPU Current Usage : CPU currently used
- CPU Max. Usage : CPU Maximum used
- CPU Min. Usage : CPU Minimum used
- CPU Usage Threshold : Maximum CPU can be used
- Memory Current Usage : Memory currently used
- Memory Max. Usage : Memory Maximum used
- Memory Min. Usage : Memory Minimum used
- Memory Usage Threshold : Maximum Memory can be used



- Current Data Rate : Current Uplink Data Rate
- Max Data Rate : Maximum Uplink Data Rate reached
- Min Date Rate : Minimum Uplink Data Rate reached



- Current Data Rate : Current Downlink Data Rate
- Max Data Rate : Maximum Downlink Data Rate reached
- Min Date Rate : Minimum Downlink Data Rate reached

System Information

Firewall	Enable
Device Up Time	00:41:49 up 42 min

- Firewall : Firewall status (Enable / Disable)
- Device Up Time : Time elapsed after CPE turned on

3.4. Settings

3.4.1. LTE

3.4.1.1. Cell Selection

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
 - LTE**
 - Cell Selection**
 - Cell Lock
 - PCI Cell Lock
 - SIM Management
 - Default PDN
 - Multiple PDN
 - Internet MTU
 - IPv6 Settings
 - Network
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring

Cell Selection

Band Selection

Mode: Full Band

Status: 42,43,48

Band Selection: ☒ Band-42 ☒ Band-43 ☒ Band-48

PLMN Selection: Auto

Apply

Cell Selection Option

Power Scan Option: ☒ First Detected Cell ☐ Strongest Cell(Power On) ☐ Strongest Cell(Always)

Apply

Cell Selection provides two main functions: Band Selection and Cell Selection Option.

By default setting in Band Selection, the device will search full LTE band supported and select PLMN automatically. With this menu, you can specify LTE band and PLMN that are needed as per uses.

Cell Selection

Band Selection

Mode: Full Band

Status: 42,43,48

Band Selection: ☒ Band-42 ☒ Band-43 ☒ Band-48

PLMN Selection: Manual

Apply

Manual PLMN selection

Current MCC/MNC: Clear

Search

Cell Selection

Band Selection

Mode: Frequency

Status: 42,43,48

Band Selection: ☒ Band-42 ☒ Band-43 ☒ Band-48

Channel Plan

Count: 1

Band: 42 EARFCN: Freq.: MHz

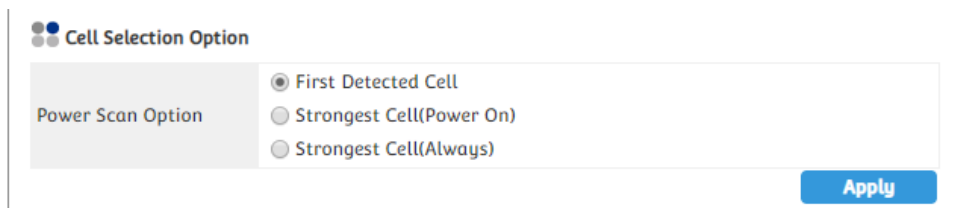
Apply

- Select “Settings” → “LTE” → “Cell Selection” from the menu.

- You can change the mode “Full Band” or “Frequency” and set EARFCN manually.
- You can see the status of band and change the band.
- You can change the “PLMN selection”.
- You can set MCC and MNC manually if you select “Manual” in “PLMN Selection” list.
- Finish setup by clicking the “Apply” button.

By default setting in Cell Selection Option, in the idle mode, the cell reselection operates according to 3GPP standard 36.304. When the idle state is changed in the connected state, the cell selection preferentially selects the Serving Cell according to 3GPP standard 36.300.

The criterion for determining the strongest cell is RSRP(Reference Signal Received Power) information.



The screenshot displays the 'Cell Selection Option' configuration screen. On the left, there is a 'Power Scan Option' label. To its right, three radio button options are listed: 'First Detected Cell' (which is selected), 'Strongest Cell(Power On)', and 'Strongest Cell(Always)'. At the bottom right of the configuration area, there is a blue 'Apply' button.

- First Detected Cell
: Cell Selection and Cell Reselection operate according to 3GPP standard.
- Strongest Cell(Power On)
: When the device is powered on, the cell selection will camp on the cell with the strongest Cell.
- Strongest Cell(Always)
: When the device is powered on and entered idle state during operation, the Cell Selection with the strongest Cell is camped on.

3.4.1.2. Cell Lock

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
 - LTE**
 - Cell Selection
 - Cell Lock**
 - PCI Cell Lock
 - SIM Management
 - Default PDN
 - Multiple PDN
 - Internet MTU
 - IPv6 Settings
 - Network
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring

Cell Lock

Search Cell

Check	Index	DL EARFCN	PCI	RSRP(dBm)	RSRQ(dB)	SINR(dB)
<input checked="" type="checkbox"/>	1	42690	0x3c (60)	-85.3/-80.4	-5.9/-6.0	31.4/33.7
<input type="checkbox"/>	2	42888	0x3c (60)	-89.2/-95.7	-6.2/-6.1	31.8/29.2

Cell Lock List

Check	DL EARFCN	PCI
-------	-----------	-----

If you want the device to camp on specific cell except others, you can use this menu. The device will only try to camp on the cell in the “Cell Lock List” if there is any item.

- Select “Settings” → “LTE” → “Cell Lock” from the menu.
- You can add current the cell to Cell Lock List or delete the cell to unlock from the list.
- You can manually add the cell by clicking “Add+” button.
- Finish setup by clicking the “Apply” button.

3.4.1.3. PCI Cell Lock

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
 - LTE**
 - Cell Selection
 - Cell Lock
 - PCI Cell Lock**
 - SIM Management
 - Default PDN
 - Multiple PDN
 - Internet MTU
 - IPv6 Settings
 - Network
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring

PCI Cell Lock

Search Cell

Check	Index	DL EARFCN	PCI	RSRP(dBm)	RSRQ(dB)	SINR(dB)
<input checked="" type="checkbox"/>	1	42690	0x3c (60)	-85.0/-81.1	-5.9/-6.2	31.5/33.2
<input type="checkbox"/>	2	42888	0x3c (60)	-89.6/-96.5	-6.1/-6.1	31.6/28.7

PCI Cell Lock List

Check	PCI
<input type="checkbox"/>	

If you want the device to camp on specific cell except others, you can use this menu. The device will only try to camp on the cell in the “PCI Cell Lock List” if there is any item.

PCI Cell Lock can be set up to 32 lists.

- Select “Settings” → “LTE” → “PCI Cell Lock” from the menu.
- You can add current the cell to PCI Cell Lock List or delete the cell to unlock from the list.
- You can manually add the cell by clicking “Add+” button.
- Finish setup by clicking the “Apply” button.

3.4.1.4. SIM Management

SIM Management	
PIN Information	
PIN Status	PIN DISABLED
RETRIES PIN	3
RETRIES PUK	10
<button>Refresh</button>	
PIN Management	
PIN Code	<input type="text"/>
<button>Verify</button> <button>Enable</button> <button>Disable</button>	
PIN Change	
PIN Code	<input type="text"/>
New PIN Code	<input type="text"/>
Confirm New PIN Code	<input type="text"/>
<button>Change</button>	
PIN Unblock	
PUK Code	<input type="text"/>
New PIN Code	<input type="text"/>
<button>Unblock</button>	
SIM Card Restriction	

For giving higher security of using LTE, SIM (Subscriber Identification Module) can have PIN (Personal Identification Number) verification procedure. You can enable or disable SIM functionality by PIN and PUK (PIN Unblock Key).

- Select “Settings” → “LTE” → “SIM Management” from the menu.
- You can see the current status of SIM.
- Only the button operation is enabled to match the current status.
 - ✓ If your SIM card is locked, PIN Status shows “PIN ENABLED NOT VERIFIED”.
 - ✓ Then you should enter the PIN code and click the “Verify” button.
 - ✓ After success unlock PIN then you can attached the LTE network.
 - ✓ You can set new PIN code by unblocking with PUK code.
 - ✓ If you failed to unblock PIN, you never use this SIM card.
 - ✓ You can set IMSI Prefix (MCC/MNC) for SIM card restriction.
00101 : 001 = MCC, 01 = MNC
 - ✓ Finish setup by clicking the “Apply” button.
 - ✓ PIN is 4 digit numbers, PUK is 8 digit numbers and IMSI prefix is 5 digit numbers.

3.4.1.5. Default PDN

The screenshot displays the 'Default PDN' configuration page. On the left is a 'Menu' sidebar with the following items: Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management, Firmware Management, and Monitoring. The 'LTE' section is expanded, showing sub-items: Cell Selection, Cell Lock, PCI Cell Lock, SIM Management, Default PDN, Multiple PDN, Internet MTU, and IPv6 Settings. The 'Default PDN' sub-item is selected. The main content area is titled 'Default PDN' and contains a 'Default PDN Connection' section. This section has five input fields: 'APN Name' (text box), 'Authentication Type' (dropdown menu with 'PAP' selected), 'Username' (text box), 'Password' (text box), and 'PDN Type' (dropdown menu with 'IPv4v6' selected). An 'Apply' button is located at the bottom right of the form.

A certain network requires the device to specify “APN (Access Point Name)”, “Authentication Type”, and “PDN Type” for Default PDN (Packet Data Network) Connection. If these parameters are not correct, the device can’t access to LTE network.

- Select “Settings” → “LTE” → “Default PDN” from the menu.
- You can set the PDN parameters such as APN Name, Authentication Type, Username, Password and PDN Type (IPv4, IPv6, IPv4v6).
- Put data in the box and click “Apply” button.

3.4.1.6. Multiple PDN

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
 - LTE**
 - Cell Selection
 - Cell Lock
 - PCI Cell Lock
 - SIM Management
 - Default PDN
 - Multiple PDN**
 - Internet MTU
 - IPv6 Settings
 - Network
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring

Multiple PDN

PDN Configure

PDN cid: 2
PDN Label: ims
APN Name:
Authentication Type: NONE
PDN Type: IPv4v6
Enable: ☐

Apply **Cancel**

PDN Configure

	Cid	PDN Label	PDN Type	APN Name	Auth Type	Username	Enable
<input checked="" type="radio"/>	2	ims	IPv4v6		NONE		Off
<input type="radio"/>	3	admin	IPv4		NONE		Off
<input type="radio"/>	4	app	IPv4		NONE		Off

By default, the device is set as Default PDN (Packet Data Network) for LTE registration and PDN Connectivity. But if network requires Multiple PDN for using “internet”, “IMS (IP Multimedia Subsystem)” or any other purpose, you should set and enable Multiple PDN function by this menu.

- Select “Settings” → “LTE” → “Multiple PDN” from the menu.
- You can set the multiple PDN parameters for IMS, admin, and App services.
- Select “Cid”, check “Enable”, put data in the box, and then click “Apply” button.

3.4.1.7. Internet MTU

The screenshot shows a web interface for configuring the Internet MTU. On the left is a 'Menu' sidebar with options: Dashboard, Connection Mode, Status, Settings, LTE, Cell Selection, Cell Lock, PCI Cell Lock, SIM Management, Default PDN, Multiple PDN, Internet MTU (highlighted), IPv6 Settings, Network, Firewall, User Management, Firmware Management, and Monitoring. The main content area is titled 'Internet MTU' and contains the text: 'This page display the maximum number of bytes in the packets transmitted over the internet port.' Below this is a section 'Internet MTU Settings' with a label 'Internet MTU' and a text input field containing '1500'. To the right of the input field is a note: '(The default is 1500, do not change unless necessary.)'. An 'Apply' button is located at the bottom right of the settings section.

In case that LTE network requires the device to limit MTU (Maximum Transmission Unit) size, you can set in this menu. Change of MTU size is usually for IP packet management between LTE network entities. Normally, the default value, 1500 is used without any problem.

- Select “Settings” → “LTE” → “Internet MTU” from the menu.
- You can change the internet MTU size [Bytes].
- Put data in the box and then click “Apply” button.

3.4.1.8. IPv6 Settings

Menu	
Dashboard	
Connection Mode	
Status	
Settings	
LTE	
Cell Selection	
Cell Lock	
PCI Cell Lock	
SIM Management	
Default PDN	
Multiple PDN	
Internet MTU	
IPv6 Settings	
Network	
Firewall	
User Management	
Firmware Management	
Monitoring	

IPv6 Settings	
IPv6 Setup	
IPv6 Enable	Enable
DHCPv6 Address Settings	
DHCPv6 Autoconfiguration Mode	Stateful
Select DHCPv6 Prefix	Manual
IPv6 Prefix	2600:1010:b005:2bc7 ::/64
Gateway IPv6 Address	2600:1010:b005:2bc7 ::0001
Start IPv6 Address	2600:1010:b005:2bc7 ::0129
End IPv6 Address	2600:1010:b005:2bc7 ::0255
DNS Server Address Mode	Auto
Apply	

The device supports IPv6 and can be enabled or disabled by the menu. You can use IPv6 by its own purpose with DHCPv6 Auto-configuration – Stateless mode. IPv6 address is automatically assigned to its connected device. Or if you want to set IPv6 address manually (like DHCPv4), you can change the mode from Stateless to Stateful and set IPv6 Prefix, Gateway IPv6 address, and Start/End IPv6 address. Also, you can set DNS (Domain Name System) Server IPv6 Address manually.

- Select “Settings” → “LTE” → “IPv6 Setup” from the menu.
- You can enable or disable IPv6 function by selecting the list.
- You can set DHCPv6 Auto-configuration Mode by selecting the list.
- You can set DNS server address mode to “Auto” or “Manual”.
- After selecting the each mode, put in the data to all boxes.
- Finish setup by clicking the “Apply” button

3.4.1.9. CBSD Settings

The screenshot displays the 'CBSD Settings' web interface. On the left, a sidebar menu shows 'Settings' selected, with 'LTE' expanded to show 'CBSD Settings' as the active option. The main content area is titled 'CBSD' and features four tabs: 'Enable' (active), 'Registration', 'Spectrum Inquiry', and 'Grant'. Under the 'Enable' tab, the 'CBSD' section includes 'CBSD Enable' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected) and 'Select Category' (a dropdown menu showing 'Category B'). Below this is the 'CBSD Status' section, which includes 'CPI Enable' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), a 'Status' field, and 'CBSD ID'. There are also fields for 'Grant1 ID', 'Grant2 ID', 'Grant3 ID', and 'Grant4 ID'. An 'Apply' button is located at the bottom right of the form.

The CBSD Setting page is shown only when the following two conditions are satisfied.

- Band-48 item should be checked in Band Selection section of LTE-Cell Selection.
- You must log in as the engineer account ID and PASSWORD when you login the WEB GUI (**root / gksrmf28**)

The device supports CBSD and can be enabled or disabled by the menu. The Citizens Broadband Radio Service Device (CBSD) function is used to connect with SAS Server to use CBRS.

- Select “Settings” → “LTE” → “CBSD Setup” from the menu.
- You can enable or disable CBSD function.
- You can set the Registration item, Spectrum Inquiry item and Grant item.
- Finish setup by clicking the “Apply” button.

- CBSD should be changed to Enable in order to use it because Default value is Disable.
- Items to check for initial setup
 - Sas URL, User ID, Category, Latitude, Longitude

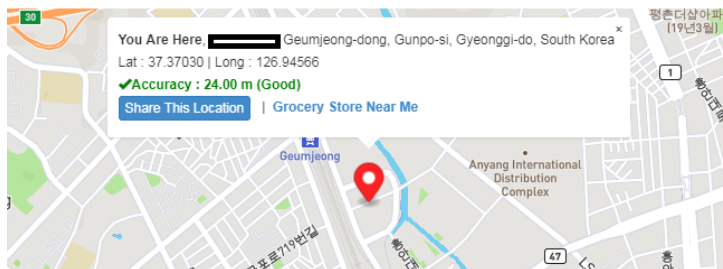
- Latitude, Longitude setting method

Information received from an LTE network does not have latitude and longitude.

Therefore, these values can not be set automatically.

You need to check and set latitude and longitude information yourself.

Go to the site : <https://mycurrentlocation.net/>



Latitude	37.37030
Longitude	126.94566
Altitude	
Accuracy	24.00
Location Name	Geumjeong-dong, Gunpo-si, Gyeonggi-do, South Korea

- CBSD device category classification.

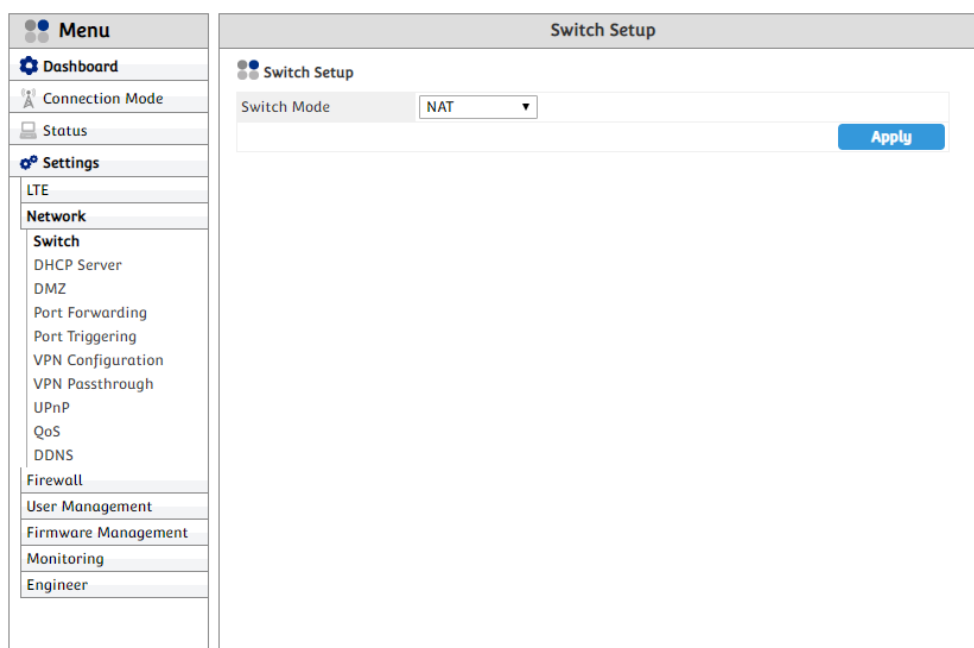
CBSD Type	Maximum EIRP (dBm/10 MHz)	Maximum EIRP (dBm/MHz)	Antenna Height (Meter)
Category A	30 dBm or 1 watt	20 dBm	< 6 meters
Category B	47 dBm or 50 Watt	37 dBm	> 6 meters
End User Device (EUD)	23 dBm or 200 mili Watt	NA	NA

- SLC-1200GA : Available in Category B, Category A and EUD mode.

- You can use the max power limit by selecting the Category of the device.
 - If EUD is selected in the select category menu, CBSD does not work and the device operates below 23dBm.

3.4.2. Network

3.4.2.1. Switch



- There are two kinds of mode in Switch Setup - “NAT” and “Bridge”.
 - ✓ Default PDN support both NAT and Bridge and other PDNs support NAT only. So if change Switch Mode then will apply to Default PDN.
 - ✓ NAT (Network Address Translation) is translation function between Private IP and Public IP address. If one user tries to send its data packets with 192.168.1.2 which is private IP address to outer network, then NAT will change that private IP address to public IP address like 119.200.124.81, which make that packets be regarded as Public IP packets. On the contrary, when packets from outer side come to CPE, NAT should decide which Private IP address to deliver. By this method, only Public IP address is used and known to outer network. So, local network inside CPE are protected.
 - ✓ Bridge mode ‘bridges’ Host LTE network and Guest LAN network. By this, guest device is directly networked to LTE, which binds two networks as one and work like one network. This “Bridge” means Guest network operates as same level as Host network.
 - ✗ On Bridge mode, CPE can’t use Network functions.
 - ✗ For using TR-069, activate “admin PDN” in “Settings”→“LTE”→“Multiple PDN”. If LTE registration is ok with admin PDN, then a user can use TR-069 function.
- How to change “Switch mode”
 - ✓ Goes to “Settings” → “Network” → “Switch” menu

- ✓ Select "NAT" or "Bridge" in Switch Mode menu
- ✓ Click "Apply button". Applied Switch mode is activated after re-boot.

3.4.2.2. DHCP Server

DHCP Server Settings

Enable DHCP Server:

Gateway IP Address: 192 . 168 . 1 . 1

Gateway Subnet Mask: 255 . 255 . 255 . 0

Starting IP Address: 192 . 168 . 1 . 2

Number of users: 253

From ISP: ☒

Primary DNS:

Secondary DNS: Optional

Tertiary DNS: Optional

DHCP Lease Time: 3600 seconds

Lease Reservation Table

Add		Del		Searched List		Add
Select	Host Name	MAC Address	IP Address	Enable	Select	IP/MAC Address
<input type="checkbox"/>					<input type="checkbox"/>	192.168.1.101 / 08:9E:01:DE:9E:43

Up to 10 rules can be set

DHCP(Dynamic Host Configuration Protocol) Server assigns network configurations like IP address, Subnet Mask, and Default Gateway, to connected client devices automatically.

DHCP Server manages complicated IP address in efficient way and adapts to insufficient IP address. You can assign same IP address to a specific device through Lease Reservation Table. For this purpose, MAC address of that device is needed. DHCP Server manages connected clients by MAC address so, user can add or delete in easy way.

- How to set “DHCP Server” settings
 - ✓ Goes to “Settings” → “Network” → “DHCP Server”
 - ✓ Select “On” in Enable DHCP Server menu
 - ✓ Set Gateway IP address
 - ✓ Set Gateway Subnet Mask address
 - ✓ Set “Starting IP Address”. If there are values in “Starting IP Address”, then “Number of users” will be changed automatically. “Number of users” can be set from 1 to 253.
 - ✓ In case of “From ISP” is checked, DHCP Server assigns DNS address from ISP (Internet Service Provider) to its connected devices through LAN connection. If “From ISP” is not checked, those devices will have DNS addresses which are set manually.
 - ✓ You can set “DHCP Lease Time”. DHCP Lease Time is time limit of IP address, which is assigned dynamically from DHCP Server to DHCP client. If that time is expired, new dynamic IP address will be assigned to DHCP client automatically. DHCP Lease Time can have the value between 300 ~ 86400 seconds and 3600 seconds by default.
 - ✓ When IP/MAC Address is enlisted in “Lease Reservation Table”, DHCP Server assigns

specific IP address to that MAC address matched. In “Searched List”, you can see IP/MAC address of the devices that are assigned IP address by DHCP Server. If you select one item and “Add”, then that item will be enlisted on “Lease Reservation Table”. The enlisted item can be edited or removed by user.

- ✓ If all settings are ready, then select “Apply button”.The changes will be operated after re-boot.

3.4.2.3. DMZ

The screenshot displays the DMZ configuration interface. On the left, a 'Menu' sidebar lists various system settings, with 'DMZ' highlighted under the 'Network' section. The main panel, titled 'DMZ', contains the following configuration options:

- Enable DMZ:** Two radio buttons, 'Enable' and 'Disable'. 'Disable' is selected.
- Redirect ICMP To The Host:** Two radio buttons, 'Enable' and 'Disable'. 'Disable' is selected.
- Exclude Web Server Port:** Two radio buttons, 'Enable' and 'Disable'. 'Enable' is selected.
- Private LAN IP Address:** Four input fields containing the values 192, 168, 1, and 2, representing the IP address 192.168.1.2.

An 'Apply' button is located at the bottom right of the configuration area.

- DMZ(Demilitarized Zone) function makes local network connected PC be opened to internet, and that will make bidirectional communication between internal host and external host without any restriction. DMZ enabled host is all port opened condition. So, if you want to use specific application programs like IP camera and Database management software but don't know which port to open, then you can set that PC as DMZ host.

Warning! DMZ is proper function when a user doesn't have information which port to be opened. But that DMZ host is entirely open to internet environment, which may bring potential security problem. If DMZ function is not necessary, please disable DMZ.

- How to use "DMZ"
 - ✓ Goes to "Settings" → "Network" → "DMZ"
 - ✓ Check "Enable" in Enable DMZ item
 - ✓ Input IP address that want to open all ports, in "Private LAN IP Address"
 - ✓ Even in DMZ mode, there are two exceptional configurations.
 - If you want to let ICMP packet to be delivered to DMZ host, please enable "Redirect ICMP to the host"
 - If you want to exclude Web Server Port of the device, please enable "Exclude Web Server Port"
 - ✓ If all settings are ready, then select "Apply button". The changes will be operated after re-boot.

3.4.2.4. Port Forwarding

Menu

- Dashboard
- Connection Mode
- Status
- Settings
 - LTE
 - Network**
 - Switch
 - DHCP Server
 - DMZ
 - Port Forwarding**
 - Port Triggering
 - VPN Configuration
 - VPN Passthrough
 - UPnP
 - QoS
 - DDNS
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring
 - Engineer

Port Forwarding

Name: [View Existing Application](#)

Protocol:

Start Port:

End Port: (Blank or Start Port-65535)

Destination IP: . . .

Destination Port: (Blank or 1-65535)

[Save](#) [Cancel](#)

Port Forwarding List

No.	Name	Start Port	End Port	Protocol	IP Address	Destination Port	
1	FTP	21	21	BOTH	192.168.1.100	21	Edit Del

Up to 10 rules can be set

- Select “Settings” → “Network” → “Port Forwarding” from the menu.
- What is “Port Forwarding”?
 - ✓ One of NAT(Network Address Translation) function. “Port Forwarding” opens specific port and make communication available through that opened port. This function is used in case that external host wants to activate a service for the host in internal network. When packets arrive from external network, those are managed by destination IP address, port and the rule that a user sets, and are matched to specific host. Communication between internal host and external network with specific port, is available through this way.
- Configure Port Forwarding Setting.
 - ✓ Input “Name”. You can reference it with click “View Existing Application”, which shows the application name that is generally used.
 - ✓ Select one of the listed Protocols (BOTH, TCP, UDP).
 - ✓ Enter Start port, End Port, Destination IP address and Destination Port.
 - ✓ For example, if you want to use one PC connected to this CPE as FTP server, you can configure as set on the picture above. 192.168.1.100 is IP address of that connected PC. You can find IP address of connected PC (or other network device) in that PC’s network configuration.
 - ✓ You can change the range of the external port by change of “Start port ~ End port”.
 - ✓ “Destination IP” and “Destination Port” are for the PC (or network device) connected to CPE.
 - ✓ Click the “Add” button when you finished.
 - ✓ You can change the data by clicking “Edit” or “Del” button in the list.

3.4.2.5. Port Triggering

Menu

- Dashboard
- Connection Mode
- Status
- Settings
 - LTE
 - Network
 - Switch
 - DHCP Server
 - DMZ
 - Port Forwarding
 - Port Triggering**
 - VPN Configuration
 - VPN Passthrough
 - UPnP
 - QoS
 - DDNS
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring
 - Engineer

Port Triggering

Port Trigger Settings Table

Name	IRC	Port Type	RANGE
Trigger Protocol	ALL	Trigger Port	6660 - 7000
Open Protocol	ALL	Open Port	113 - 113

Save **Cancel**

Port Trigger List

No.	Name	Trigger Protocol	Trigger Port(s)	Open Protocol	Open Port(s)	Edit	Del
			StartPort	EndPort	StartPort	EndPort	
1	IRC	all	6660	7000	all	113	113

Edit **Del**

Up to 10 rules can be set

- Select “Settings” → “Network” → “Port Triggering” from the menu.
- What is “Port Triggering”?
 - ✓ Port Triggering is automated version of Port Forwarding. “Port Forwarding” forwards its packet to fixed IP address and port that a user sets, but “Port Triggering” forwards received packets to pre-defined Triggering port range of local network that client is belonged to.
 - ✓ Application programs like FTP and IRC (Internet Relay Chat) use several ports when it responses. If one session is opened and starts to send, additional ports open operation for receiving packets, can be done by “Port Triggering”.
- Configure Port Triggering
 - ✓ Input “Name” item according to purpose
 - ✓ Select “Port Type” that apply to Port Range
 - ✓ Set “Trigger Protocol” and “Trigger Port”. These items are for the client in the local network (LAN).
 - ✓ “Open Protocol” and “Open Port” is for external (WAN) port that will be used in Triggering.
 - ✓ Click the “Add” button when you finished.
 - ✓ You can change the data by clicking “Edit” or “Del” button in the list.
- Port Triggering Example

One of application that uses Port Triggering is IRC (Internet Relay Chat). IRC authenticates user by IDENT protocol through port 113, generally. When client PC tries to connect to IRC server, it uses port 6667 (or port range 6660 ~ 7000) for connection request message. In response to this, IRC

server send identification message through port 6667 and port 113 additionally. So, port 113 must be opened to client PC. If user sets as picture above, then CPE will open port 113 automatically and deliver packets through that, when it detects session over port 6667 is started.

3.4.2.6. VPN Configuration

- Input GRE (Generic Routing Encapsulation) configuration items and “Add” to “GRE Configuration List”. Click “Apply button” will bring re-boot of CPE. GRE VPN (Virtual Private Network) will be operated after that.
- GRE Tunnel can have 5 items maximum.
- Tunnel Destination IP Address : External IP address of CPE (LTE IP)
- GRE Interface IP Address : GRE Interface Private IP Address of CPE
- GRE Interface Remote IP Address : WAN IP Address of remote device
- Remote Private IP Address : GRE Interface Private IP Address of remote device
- Key value can have the range of 0~4294967295.

Menu	
Dashboard	
Connection Mode	
Status	
Settings	
LTE	
Network	
Switch	
DHCP Server	
DMZ	
Port Forwarding	
Port Triggering	
VPN Configuration	
VPN Passthrough	
UPnP	
QoS	
DDNS	
Firewall	
User Management	
Firmware Management	
Monitoring	
Engineer	

VPN Configuration	
VPN Configuration Settings	
VPN	L2TP
L2TP Mode	
Server Address	
Server Address(Private)	Enable
Private Server Address	
Username	
Password	
Pre Shared Key	
Connect Mode	Keep Alive
Redial Period	Seconds
<div>Apply</div> <div>Cancel</div>	

- Input L2TP (Layer 2 Tunneling Protocol) configuration items. Click “Apply button” will bring re-boot of CPE and then L2TP VPN is operated after that.
- If “Private Server Address” is needed for L2TP VPN connection, then enable “Ser Address(Private)” and input “Private Server Address” after that.
- “Connect Mode” has two options - Keep Alive / Manual.
- “Keep Alive” attempts to connect periodically by the time defined in “Redial Period”. “Manual” attempts only one time at the boot-up.

Menu	
Dashboard	
Connection Mode	
Status	
Settings	
LTE	
Network	
Switch	
DHCP Server	
DMZ	
Port Forwarding	
Port Triggering	
VPN Configuration	
VPN Passthrough	
UPnP	
QoS	
DDNS	
Firewall	
User Management	
Firmware Management	
Monitoring	
Engineer	

VPN Configuration	
VPN Configuration Settings	
VPN	PPTP
PPTP Mode	
User MPPE	Disable
Server Address	
Username	
Password	
Connect Mode	Keep Alive
Redial Period	Seconds
<div>Apply</div> <div>Cancel</div>	

- Input PPTP (Point-to-Point Tunneling Protocol) configuration items. Click “Apply button” will bring re-boot of CPE and then PPTP VPN is operated after that.
- User can use “User MPPE (Microsoft Point-to-Point Encryption)” by selection of Enable/Disable.
- “Connect Mode” has two options - Keep Alive / Manual.
- “Keep Alive” attempts to connect periodically by the time defined in “Redial Period”. “Manual” attempts only one time at the boot-up.

3.4.2.7. VPN Passthrough

The screenshot displays the 'VPN Passthrough' configuration page. On the left, a 'Menu' sidebar lists various system settings, with 'Settings' and 'Network' highlighted. The main content area, titled 'VPN Passthrough', shows the 'VPN Pass Through Settings' section. It includes a 'VPN Service' dropdown menu, two checked checkboxes for 'PPTP Service' and 'L2TP/IPSEC Service', and an 'Apply' button.

- Select “Settings” → “Network” → “VPN Pass through” from the menu.
- The device supports 2 types of service: PPTP Service, L2TP/IPSEC Service.
- Select the type(s) of VPN pass through to use with the checkboxes.
- Finish setup by clicking the “Apply” button.

3.4.2.8. UPnP

The screenshot displays the UPnP configuration page. On the left, a sidebar menu shows the navigation path: Menu > Settings > Network > UPnP. The main content area is titled 'Universal Plug & Play'. It features a section for 'UPnP Enable/Disable' with radio buttons for 'Enable' (selected) and 'Disable', followed by an 'Apply' button. Below this is a 'Client List' section with a table header: No., Client Program, Protocol, External Port, IP Address, and Internal Port. A 'Refresh' button is located at the bottom right of the table.

- Select “Settings” → “Network” → “UPnP” from the menu.
- What is “UPnP(universal plug and play)”?
 - ✓ The interface standard for home appliances for access of home network. This is expanded version of “Plug and Play” which was originally adopted in Windows Operating System. Those devices that support UPnP can recognize each other in the network connected, without any configuration change.
- Select whether or not to enable the Universal Plug & Play function.
 - ✓ If this function is enabled, CPE will provide internet gateway device and port mapping protocol services to the UPnP supported clients. This function also allows the client in the LAN network to request ‘re-assign new port’, and gives compatibility with peer-to-peer software that is connected to ‘Xbox Live and PlayStation Network included online services’, messaging application programs, and game consoles. You can check current UPnP clients in the “Client List”.
- Finish setup by clicking the “Apply” button.

3.4.2.9. QoS

Menu

- Dashboard
- Connection Mode
- Status
- Settings
 - LTE
 - Network**
 - Switch
 - DHCP Server
 - DMZ
 - Port Forwarding
 - Port Triggering
 - VPN Configuration
 - VPN Passthrough
 - UPnP
 - QoS**
 - DDNS
 - Firewall
 - User Management
 - Firmware Management
 - Monitoring
 - Engineer

QoS

QoS Setup

QoS Enable/Disable: ☐ Disable ☒ Enable

Download(kbps):

Setting QoS on device might be mandatory for access control and usage tracking, but suffering a performance hit is strictly optional.

QoS Rule Setup

QoS Mode: Add Cancel

QoS List

Download(WAN -> LAN)

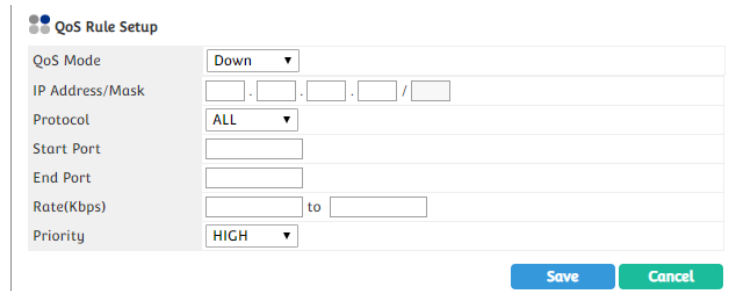
No.	IP Address/Mask	Protocol	Port	Rate(Kbps)	Priority
Up to 10 rules can be set					

Apply

QoS(Quality of Service) is used for maximize its usage of limited bandwidth, and optimize its load. This function can allocate minimum or maximum bandwidth to those PCs connected. So, in case that one PC occupies too much bandwidth load, QoS can control that PC's bandwidth and minimize its influence to others for seamless internet environment.

- How to set "QoS",

- ✓ Goes to "Settings" → "Network" → "QoS"
- ✓ If you want to limit total Upload and Download speed, you need to set "Upload(kbps)" and "Download(kbps)" in the "QoS Setup" menu. Upload and Download can be changed by the selection menu in the "QoS Rule Setup" and "QoS Mode".
Warning! The sum of each IP address' Uploader Download speed can't be more than the total Upload and Download speed.
- ✓ You can configure Upload and Download speed separately by each IP address.
- ✓ At first, select Upload or Download in the "QoS Rule Setup" and "QoS Mode" menu.
- ✓ After that click "Add button". Then additional configuration menu will be displayed as below image for setting up items differently by IP address.



QoS Rule Setup

QoS Mode: Down

IP Address/Mask: . . . /

Protocol: ALL

Start Port:

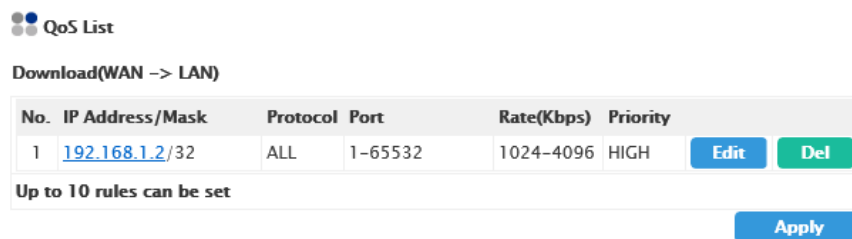
End Port:

Rate(Kbps): to

Priority: HIGH

Save Cancel

- ✓ Input "IP Address/Mask".
- ✓ You can select "ALL / TCP / UDP" in the "Protocol" menu as per uses.
- ✓ Input "Start Port" and "End Port". Full port range is "1~65532".
- ✓ Now you must define "Upload" and "Download" speed range in the "Rate(kbps)" menu.
- ✓ Each IP address can have "Priority" which is one of "HIGH/MEDIUM/LOW". "HIGH" is highest priority than other IP address.
- ✓ After setting up all items in the menu, you can click "Save" for saving all values. If all values are valid, then one item will be showed on "QoS List".



QoS List

Download(WAN -> LAN)

No.	IP Address/Mask	Protocol	Port	Rate(Kbps)	Priority	
1	192.168.1.2/32	ALL	1-65532	1024-4096	HIGH	Edit Del

Up to 10 rules can be set

Apply

- ✓ Saved item can be edited or deleted by the "QoS List" menu.
- ✓ Maximum 10 items can be saved.

3.4.2.10. DDNS

The screenshot shows the DDNS configuration page. On the left, the 'Menu' sidebar has 'Settings' expanded, with 'Network' and then 'DDNS' selected. The main content area is titled 'DDNS' and contains a 'Dynamic DNS' section. In this section, 'DDNS Enable' has radio buttons for 'Enable' (selected) and 'Disable'. Below this is the 'DDNS Setting' section with several input fields: 'Service' (a dropdown menu showing 'dyndns.org'), 'Hostname' (text input 'hostname'), 'Username' (text input 'username'), 'Password' (text input 'password'), 'Check for change IP every' (text input '300'), 'Check-time unit' (dropdown menu showing 'seconds'), 'Force update every' (text input '80'), and 'Force-Time unit' (dropdown menu showing 'minutes'). An 'Apply' button is located at the bottom right of the settings area.

- Select “Settings” → “Network” → “DDNS” from the menu.
- What is “DDNS(Dynamic DNS)”?
 - ✓ DNS(Domain Name Server) is updated real time base. Usually, it is used when clients have assigned IP address dynamically. Even though IP address is changed, domain name is same on DDNS as user sets. So, it can be accessed to the client from outside the network in convenient way.
- Set the DDNS environment
 - ✓ If you want to set the DDNS, check “Enable” in the checkbox to enter necessary inputs.
 - ✓ For activation of DDNS operation, an account is needed that is given by DDNS service provider. This DDNS account is provided by the contract between DDNS service provider and user, not by the CPE manufacturer. (DDNS service account can be charged by the service provider based on its service policy.)
 - ✓ Select DDNS service provider that provides DDNS account in “Service” menu.
 - ✓ If your DDNS service provider is not listed in “Service” menu, then select “Custom URL” menu and input its URL address manually.

This is a close-up of the 'Service' dropdown menu. The dropdown is open, showing 'Custom URL' as the selected option. Below the dropdown, there is a text input field labeled 'Custom update-URL' which contains the text 'seowon.com'.

- ✓ “Hostname” is unique address that given by the DDNS service provider. (This can be different by DDNS service provider. So, you can check this with DDNS service provider or you can use “Service” and “Custom URL” instead.)
- ✓ “Username” and “Password” are account information given by DDNS service provider.

- ✓ “Check for change IP every” and “Check-time unit” are checking time period of DDNS IP change.
- ✓ Current DDNS configurations are updated unconditionally at the time of “Force update every” and “Force-Time unit”.
- ✓ After entering all the necessary information for DDNS setting, finally, click the “Apply” button to finish setting.

3.4.3. Firewall

3.4.3.1. Basic

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
- LTE
- Network
- Firewall**
- Basic
- Filter Setup
- Access Control
- IP-MAC Binding
- User Management
- Firmware Management
- Monitoring
- Engineer

Firewall

Firewall Setup

Firewall Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow Ping From WAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow HTTP login from WAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow HTTPS login from WAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Multicast Filter	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

SIP ALG Settings

The modem supports the SIP ALG function. The SIP application can run and communicate with other internet application.

Enable SIP ALG	<input type="checkbox"/>
SIP port	5060

Apply

- Network security configuration can be managed in “Firewall” menu. Network security policy like ‘access block of unauthorized network devices’ can be operated safely.
 - ✓ Allow Ping From WAN
If enabled, ICMP (Internet Control Message Protocol) packets from external WAN is blocked, so IP address will not be opened to outside.
 - ✓ Allow HTTP login from WAN
If enabled, remote management access from external WAN is allowed. Management access by LAN is always available, regardless of this option.
 - ✓ Multicast Filter
If enabled, Multicast traffic from external WAN is blocked for protection of internal devices.
- SIP (Session Initiation Protocol) ALG (Application Level Gateway) function is used for blocking communication between SIP application and other internet-connected applications.
- For basic firewall configuration,
 - ✓ Goes to “Settings”->“Firewall”->“Basic”
 - ✓ Select “Enable” in the “Firewall Setup” ->“Firewall Enable/Disable” menu.
 - ✓ Click “Apply button” for saving the configuration.
- For SIP ALG configuration,
 - ✓ Click check box in the “SIP ALG Settings”->“Enable SIP ALG” menu.
 - ✓ Input SIP port which range is 1 ~ 65534.
 - ✓ Click “Apply button”. Changed configurations will be operated after re-boot.

3.4.3.2. Filter Setup

- With “Filter Setup”, user can block packet transaction between internal LAN connected client and WAN. Also specific network service can be blocked. By the rules of packet filtering that a user set, internal network can be protected from outside and internet usage can be limited for kids.
Warning! Network filter is operated based on time set on CPE. A user must check currently operated time in the menu “Settings” ->“User Management” ->“Date and Time”.
- “Filter Setup” supports 3 types of filter. You can select one of them in the “Select Filter” menu. Maximum 10 items for each filter are available.
 - ✓ IP Filter / URL Filter / MAC Filter

- For network filter configuration,
 - ✓ Goes to “Settings” ->“Firewall” ->“Filter Setup”
- For using “URL Filter”,

- ✓ Select “Enable” in the “Filter Setup” ->“URL Filter Enable” menu.
 - ✓ Click “Apply button”. Changed configurations will be operated after re-boot.
Warning! If URL Filter is enabled, network performance will be lowered. If you don’t use this function, disable URL Filter.
- For “IP Filter” configuration,
 - ✓ Select “IP Filter” in the “Select Filter” menu.

- ✓ Click “Add button” for additional configurations as below.

Select Filter	IP Filter ▼
Policy	DROP ▼
Name	<input type="text"/>
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Start Port	<input type="text"/>
End Port	<input type="text"/>
Protocol	BOTH ▼
Blocked Day	<input checked="" type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Blocked Time	<input checked="" type="checkbox"/> 24 Hours <input type="text"/> HH : <input type="text"/> MM To <input type="text"/> HH : <input type="text"/> MM
Enable	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- ✓ “Policy” menu only has “DROP” option.
- ✓ Input proper name on “Name” menu.
- ✓ Input “Source IP” and “Destination IP Address” that want to apply.
- ✓ Input “Start Port” and “End Port”.
- ✓ Select one of “BOTH/TCP/UDP” in the “Protocol” menu.
- ✓ You can select a day or days of a week that filter activated. If “Every Day” is selected, filter will be operated everyday.
- ✓ Input “Blocked Time”. Filter will be activated during the time set in the day of “Blocked Day”. If “24 Hours” is checked, filter is work on the day selected in “Blocked Day”.
- ✓ If both “Every Day” and “24 Hours” are checked, then filter will be operated every day regardless of what is checked in the day.
- ✓ After checking “Enable” check box, click “Save button”, then changed configurations will be saved.
- ✓ If “Enable” check box is not checked and “Save” after that, filter will not be operated even though filter configurations are saved.
- ✓ “Cancel button” will initiate all configurations.
- For “URL Filter” configuration,
 - ✓ Select “URL Filter” in the “Select Filter” menu.
 - ✓ Click “Add button” for additional configurations as below.

Select Filter	URL Filter ▼
Policy	DROP ▼
Name	<input type="text"/>
URL Address	<input type="text"/>
Blocked Day	<input checked="" type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Blocked Time	<input checked="" type="checkbox"/> 24 Hours <input type="text"/> HH : <input type="text"/> MM To <input type="text"/> HH : <input type="text"/> MM
Enable	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- ✓ “Policy” menu only has “DROP” option.
- ✓ Input proper name on “Name” menu.
- ✓ Input URL address that want to block. Those sites that include the URL address input can’t

be accessed. If you want to block specific site, then input accurate address in the “URL Address” menu.

- ✓ “Blocked Day / Blocked Time / Enable” menu work same as described in “IP Filter” configuration.
- ✓ After input all configurations and click “Save button” for saving user change. “Cancel button” click will initiate all changes up to that point, and then need to input from the beginning.
- For “MAC Filter” configuration,
 - ✓ Select “MAC Filter” in the “Select Filter” menu.
 - ✓ Click “Add button” for additional configurations as below.

- ✓ “Policy” menu only has “DROP” option.
- ✓ Input proper name on “Name” menu.
- ✓ Click “View Existing Device” for checking currently connected devices and select one of them if needed.

Existing device list			
No.	Device Name	IP Address	MAC Address
1	Unknown	192.168.1.101	08:9e:01:de:9e:43

- ✓ If a user clicks “Select button”, “Device Name / MAC Address” is input automatically in the menu.
- ✓ “Blocked Day / Blocked Time / Enable” menu work same as described in “IP Filter” configuration.
- ✓ After input all configurations and click “Save button” for saving user change. “Cancel button” click will initiate all changes up to that point, and then need to input from the beginning.

- All filter rules saved are displayed by each filter in the “Filter List”. If a user selects filter type in “Select Filter” menu, different filter rules saved will be listed.

Filter List

No.	Policy	Name	MAC Address	Protocol	Status		
1	DROP	Unknown	08:9E:01:DE:9E:43	BOTH	y		<button>Edit</button> <button>Del</button>

Up to 10 filter can be set

- If you want to edit saved filter,
 - ✓ Select one filter type to change in the “Select Filter” menu.

- ✓ Click “Edit button” to edit among the “Filter List” items.
- ✓ Then additional configuration window will be showed like “Add button” click in the “Select Filter”. Those configurations have the value from the one user selects, so user can change and save after that.
- ✓ If a user doesn’t want to edit, then click “Cancel button”.
- If you want to delete saved filter,
 - ✓ Select one filter type to delete in the “Select Filter” menu.
 - ✓ Click “Del button” in the “Filter List” will delete that filter immediately.

3.4.3.3. Access Control

Menu

- Dashboard
- Connection Mode
- Status
- Settings
 - LTE
 - Network
 - Firewall
 - Basic
 - Filter Setup
 - Access Control**
 - IP-MAC Binding
 - User Management
 - Firmware Management
 - Monitoring
 - Engineer

Access Control

Access Control Enable: ☐ Enable ☒ Disable

Default Access Mode: ☒ Black List ☐ White List

Black List

Up to 10 filter can be set

Device Name	MAC Address	Modify

Devices Online

Device Name	IP Address	MAC Address
Unknown	192.168.1.101	08:9E:01:DE:9E:43

“Access Control” function can control the device (PC, Smartphone, etc.) accessibility to CPE by management of “White List” that is list of access granted to CPE, and “Black List” that is blocked to access CPE. In case that “White List” is set, only those devices in the list can access to CPE. Otherwise, “Black List” is set, those devices can’t access to CPE. “White List” and “Black List” can’t be used at the same time. Only one “List” is available at one time.

- Access Control
 - ✓ Access Control Enable : Enable / Disable of Access Control function
 - ✓ Default Access Mode : List that need to apply (Black List / White List)
 - ✗ White List : Device list of access granted
 - Black List : Device list that is blocked
- Black List or White List
 - ✓ Enlisted devices will be showed by “Black List” or “White List”
 - ✓ “Add” : Add one device to the selected list in “Default Access Mode”
 - ✓ Delete checked : Delete selected devices in the list of “Default Access Mode”.
- Device Online
 - ✓ Device list of currently connected to CPE.
- Access Control Configuration
 - ✓ Goes to “Settings” -> “Firewall” -> “Access Control” menu.
 - ✓ Select “Enable” in the “Access Control Enable” menu.
 - ✓ Select one of “Black List” or “White List” in the “Default Access Mode” menu.
 - ✓ Click “Apply button” for apply changed configuration.

- Add a device to the List

- ✓ Click “Add button” and input “Device Name” and “MAC Address”.

- ✓ Or select one of devices in the “Devices Online” and Click “Add checked button”.

Devices Online Add checked

	Device Name	IP Address	MAC Address
<input checked="" type="checkbox"/>	Unknown	192.168.1.101	08:9E:01:DE:9E:43

- Delete a device in the List

- ✓ Click “Del button” at the end of the list information.

Black List

	Device Name	MAC Address	Modify
<input type="checkbox"/>	Unknown	08:9E:01:DE:9E:43	Edit Del

Up to 10 filter can be set

Add Delete checked

- ✓ Or check the check box at the first column of the list and click “Delete checked button”.

Black List

	Device Name	MAC Address	Modify
<input checked="" type="checkbox"/>	Unknown	08:9E:01:DE:9E:43	Edit Del

Up to 10 filter can be set

Add Delete checked

- White List Activation and Device Addition Example

- ✓ Select “Enable” in the “Access Control Enable” menu.
- ✓ Select “White List” in the “Default Access Mode” menu.
- ✓ Click “Apply button” for applying configuration changed.
- ✓ Click “Add button” for input “Device Name” and “MAC Address”.

Create a rule

✕

All form fields are required.

Device Name

MAC Address

Create a rule

Cancel

- ✓ Check added device is in the “White List”.

White List

<input type="checkbox"/>	Device Name	MAC Address	Modify	
<input type="checkbox"/>	Unknown	00:12:07:00:11:22	<div>Edit</div>	<div>Del</div>

Up to 10 filter can be set

Add

Delete checked

3.4.3.4. IP-MAC Binding

- Select “Settings” -> “Firewall” -> “IP-MAC Binding” in the menu.
- What is “IP-MAC Binding”?
 - ✓ IP-MAC Binding makes that specific IP address is assigned only to the client that has specific MAC address. This function will prevent unwanted device’s use of specific IP address which is defined for specific use.
 - ✓ Even if one network client assigns static IP address, CPE checks that IP address is registered in IP-MAC Binding List. Also even if it is registered, the client’s MAC address is checked that IP address and MAC address are matched or not. If MAC address is not matched one, that device’s network access is blocked.
- If you want to use the IP-MAC Binding function, check the “Enable” checkbox.
- Click “Add button” for new IP-MAC Binding rule. Or click “Bind button” that want to be add in the “ARP (Address Resolution Protocol) List”.

- When IP-MAC Binding configuration window is displayed, input IP address and MAC address. (In case that click “Bind button” in the “ARP List”, all configurations are already set automatically.) IP-MAC Binding is operated when “Status” is checked in “Enable”. If “Status” is set as “Disable”, then IP-MAC Binding is not functional even if “Bind List” has items. After all configurations are done, click “Save button” for saving configuration or click “Cancel button” for quit configuration.

- “ARP List” shows clients list of currently found in the network.
- Even though one item is deleted by “Del button” in the “ARP List”, that item can be displayed in the case that re-registration is done by ARP.

3.4.4. User Management

3.4.4.1. Account

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
- LTE
- Network
- Firewall
- User Management**
- Account**
- Language
- Restore Default
- Reboot
- TR-069 Settings
- Date and Time
- FOTA
- Remote Management
- Firmware Management
- Monitoring

Account

Account Management

Privilege: system

Username: system

Current Password:

New Password:

Confirm Password:

Apply

Customer Name

Customer Name:

Apply

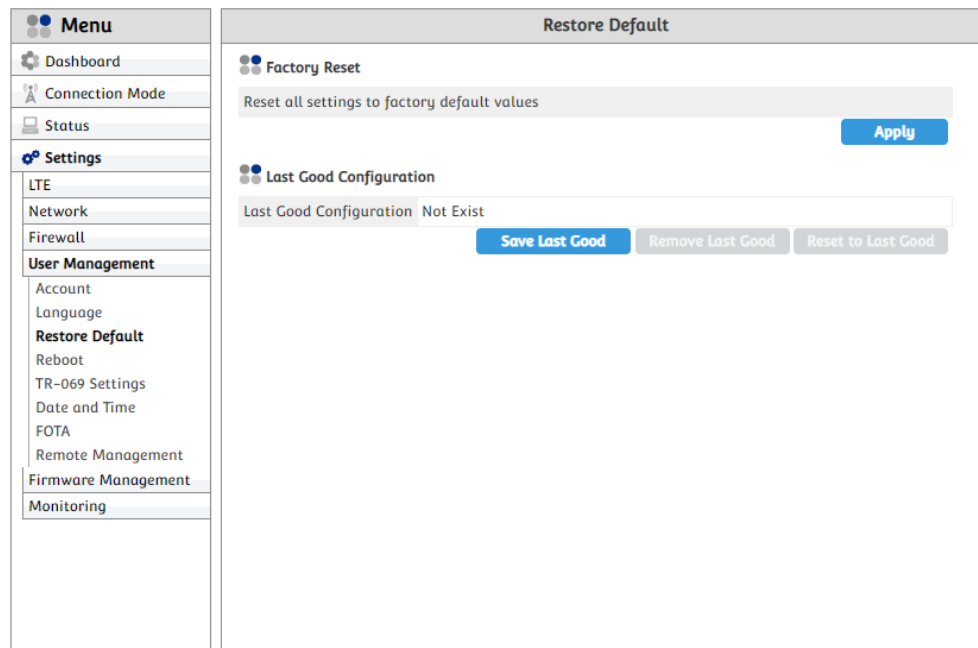
- If you want to change ID (account name), then select one of “Privilege” option, input “Username” and “Current Password”, and “Apply”.
- If you want to change Password, then selection one of “Privilege” option, input “Current Password” and “New Password / Confirm Password” to be changed, and “Apply”.

3.4.4.2. Language

The screenshot displays the SEOWONINTECH web interface. On the left is a vertical menu with the following items: Menu, Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management, Account, Language, Restore Default, Reboot, TR-069 Settings, Date and Time, FOTA, Remote Management, Firmware Management, and Monitoring. The 'Language' option is highlighted. The main content area is titled 'Language' and contains 'Language Settings'. It features a dropdown menu labeled 'Language' with 'English' selected, and a blue 'Apply' button to its right.

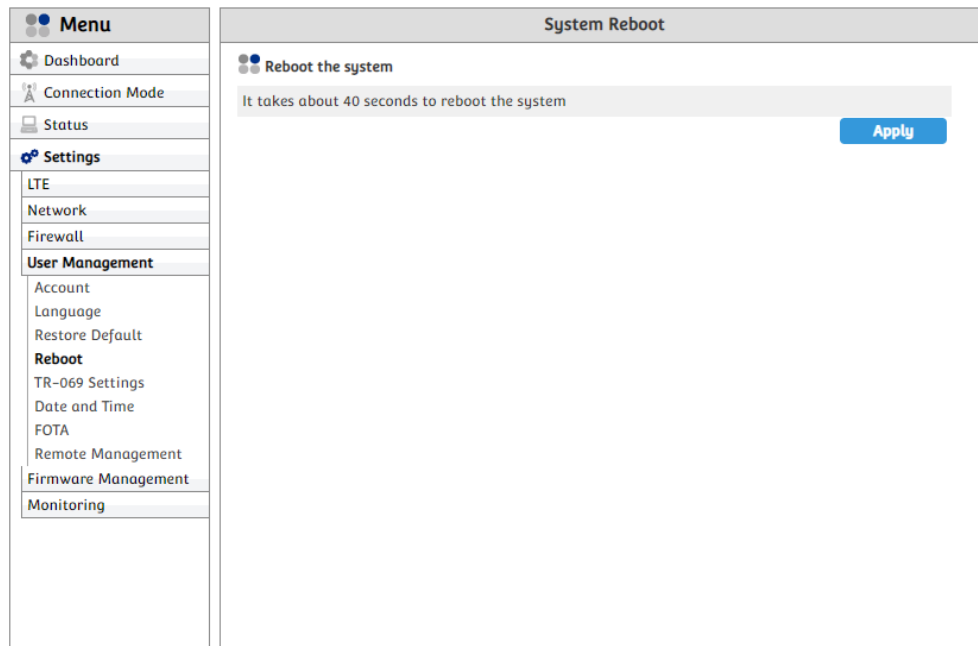
- Select “Language” needed and click “Apply button”.

3.4.4.3. Restore Default



- “Factory Reset” ->“Apply” will reset all the configurations changed by a user, to default values.
- If a user wants to save a configuration at a certain time, he/she can save it by click “Save Last Good” in “Last Good Configuration” menu. Even though some configurations are changed after that, a user can back to that point by click “Reset to Last Good”. If a user wants to delete it, then click “Remove Last Good”.

3.4.4.4. Reboot



- You can reboot the CPE by click “Apply button” in the System Reboot menu.

3.4.4.5. TR-069 Settings

Menu

- Dashboard
- Connection Mode
- Status
- Settings
 - LTE
 - Network
 - Firewall
 - User Management
 - Account
 - Language
 - Restore Default
 - Reboot
 - TR-069 Settings**
 - Date and Time
 - FOTA
 - Remote Management
 - Firmware Management
 - Monitoring

TR-069 Settings

CPE WAN Management Protocol(CWMP). It provides the communication between CPE and Auto Configuration Servers(ACS).

TR-069 Settings

TR-069 ☐ Enable ☒ Disable

Periodic Inform ☒ Enable ☐ Disable

Periodical Inform Interval

ACS Address

Username

Password

Connection Request Username

Connection Request Password

Apply

- Click the “Enable” button in the “TR-069” field to use TR-069 feature, or click the “Disable” button to disable it.
- Click the “Enable” button in the “Periodic Inform” field to enable Periodic Inform so it informs the user periodically about the connection setup, or click the “Disable” button to disable it.
- In the “Periodic Inform Interval” field, enter the time in seconds when the CPE reconnects to ACS periodically.
- In the “ACS Address” field, enter the ACS URL provided by the ISP with the format of “http://”
- In the “Username” field, enter the ACS username provided by the ISP.
- In the “Password” field, enter the password associated with the username.
- Enter the connection request username for the ACS to initiate the connection in the “Connection Request Username” field. This acts as the username for the ACS when a connection is initiated and the user is asked for security credentials.
- Enter the connection request password for the ACS in the “Connection Request Password” field. This acts as the password for the ACS when a connection is initiated and the user is asked for security credentials.
- Click "Apply" button to changes new configuration. Then CPE will be rebooted.

3.4.4.6. Date and Time

Menu

- Dashboard
- Connection Mode
- Status
- Settings**
- LTE
- Network
- Firewall
- User Management**
- Account
- Language
- Restore Default
- Reboot
- TR-069 Settings
- Date and Time**
- FOTA
- Remote Management
- Firmware Management
- Monitoring

Date and Time

Time Zone Setup

NTP Client
Enable/Disable: ☒ Enable ☐ Disable

Local Time: 2015-01-01 14:10:24

Time Server: my.pool.ntp.org

Time Zone Select: Seoul

Enable Daylight Saving: ☐

Start Date: First Sunday of April at 2 o'clock

End Date: Last Sunday of October at 2 o'clock

Apply

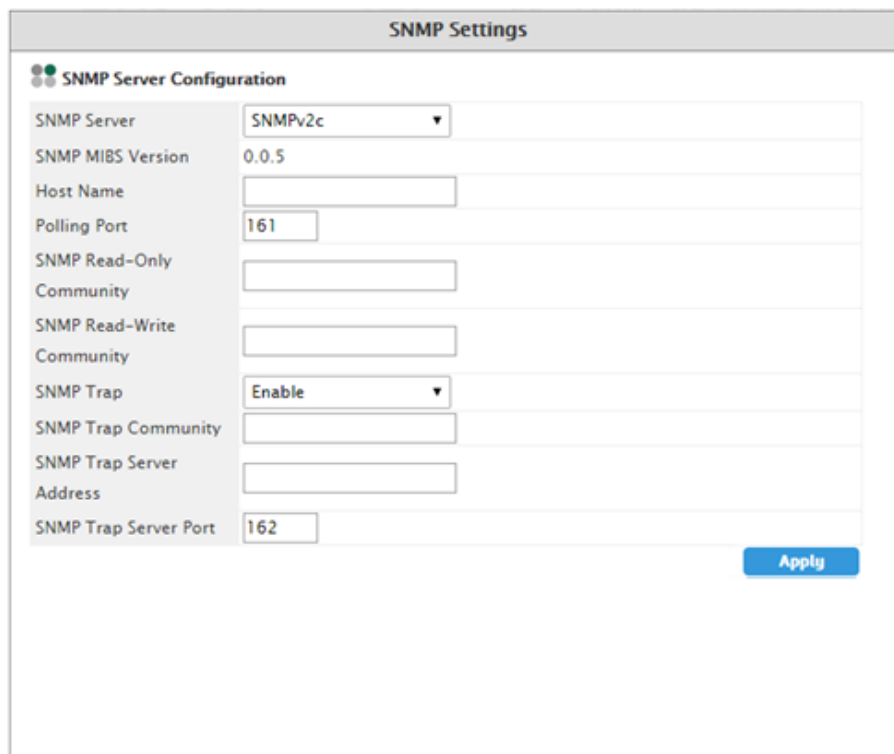
- If “NTP Client” enables and “Time Server” / “Time Zone Select” are properly configured, current time will be displayed in the “Local Time” menu.
- You can apply Daylight Saving time by checking “Enable Daylight Saving” and setting “Start Date” and “End Date”.

3.4.4.7. FOTA

The screenshot shows a web interface for FOTA Setup. On the left is a 'Menu' sidebar with options: Dashboard, Connection Mode, Status, Settings (highlighted), LTE, Network, Firewall, User Management (with sub-items: Account, Language, Restore Default, Reboot, TR-069 Settings, Date and Time), FOTA (highlighted), Remote Management, Firmware Management, and Monitoring. The main area is titled 'FOTA Setup' and contains a warning: 'If you setup this function, Firmware will be updated automatically.' Below this, the 'FOTA Setup' section has three radio buttons: 'Never check for updates', 'Check for update at device booting', and 'In the upgrade cycle' (which is selected). To the right of these are input fields for 'FOTA periodic timer' (Start/End: 00 To 24 hours, Period: 1 day) and 'FOTA randomization timer' (15 minutes). There is an 'Update Server URL' field with the value 'http://61.83.223.242/LTE/CHARTER/ODU' and a 'Check URL' button labeled 'Check FOTA server'. An 'Apply' button is at the bottom right.

- If “Never check for updates” is checked, FOTA (Firmware Over The Air) will not check its latest firmware on the FOTA server.
- If “Check for updates at device booting” is checked, FOTA will check “Update Server URL” and try to update every time CPE is boot-up.
- If “In the upgrade cycle” is checked, FOTA will check “Update Server URL” at the time set of the menu “FOTA periodic timer” and “FOTA randomization timer”.
 - ✓ Select a start time, end time, and period and start time must be less than end time.
 - ✓ FOTA periodic timer will be start when current time is between start and end time and start over after selected time period.
- Click “Check URL” ->“Check FOTA server” will bring immediate check for FOTA server.

3.4.4.8. SNMP



The image shows a web-based configuration window titled "SNMP Settings". Inside, there is a section labeled "SNMP Server Configuration" with a list of settings. The settings are as follows:

Setting	Value
SNMP Server	SNMPv2c
SNMP MIBS Version	0.0.5
Host Name	
Polling Port	161
SNMP Read-Only Community	
SNMP Read-Write Community	
SNMP Trap	Enable
SNMP Trap Community	
SNMP Trap Server Address	
SNMP Trap Server Port	162

An "Apply" button is located at the bottom right of the configuration area.

- Select "SNMPv2c" or "SNMPv3c" for using SNMP function.
- SNMP MIBS Version : It shows version of current SNMP MIBS.
- Host Name : Enter Host name.
- Polling Port : Enter Polling Port number. (Default value is 161)
- SNMP Read-Only Community : Enter community string for read only.
- SNMP Read-Write Community : Enter community string for read and write.
- SNMP Trap : Select "Enable" for using SNMP Trap function.
- SNMP Trap Community : Enter community string for SNMP Trap.
- SNMP Trap Server Address : Enter Server Address for SNMP Trap.
- SNMP Trap Server Port : Enter Trap Server Port number. (Default value is 161)

3.4.4.9. Remote Management

The screenshot shows a web interface for configuring Remote Management. On the left is a 'Menu' sidebar with options: Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management (Account, Language, Restore Default, Reboot, TR-069 Settings, Date and Time, FOTA), Remote Management (highlighted), Firmware Management, Monitoring, and Engineer. The main area is titled 'Remote Management' and contains two sections: 'HTTP Server' and 'HTTPS Server'. The 'HTTP Server' section has a 'Remote IP Address' text box and a 'Port Number' dropdown menu set to '80' with a note '(The default is 80)'. The 'HTTPS Server' section has an 'Enable' checkbox (unchecked) and a 'Port Number' dropdown menu set to '443' with a note '(The default is 443)'. An 'Apply' button is located at the bottom right of the configuration area.

- By default, all devices that connected to CPE can access to CPE's management web page. But by using "Remote Management", you can limit only one device to manage the CPE.
- Input IP address and Port number of the connected device.
- You can use this function though HTTPS server by checking "HTTPS Server Enable" option.

3.4.5. Firmware Management

3.4.5.1. Software

Software

Software Upgrade

Filename 1

Choose File

No file chosen

Filename 2

Choose File

No file chosen

Filename 3

Choose File

No file chosen

Filename 4

Choose File

No file chosen

Status

Please select the update package file

Device Software Version

1.0.3

Update

Configuration Backup

Configuration Export

Export

Configuration Import

Choose File

No file chosen

Import

- For software upgrade, you need to click “Choose File”, select firmware binary file and click “Update button”. New software will be applied after re-boot of CPE.
- You can extract all configurations that currently applied by click “Export button” in “Configuration Export” menu, to compressed file.
- If you want to apply ‘exported configuration file’ to CPE, then click “Choose File” in the “Configuration Import” menu, select ‘exported file’, and click “Import button”.

3.4.6. Monitoring

3.4.6.1. Iperf

The screenshot displays a web-based interface for the Performance Measurement Tool. On the left is a vertical menu with the following items: Menu, Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management, Firmware Management, Monitoring, Iperf, Diagnostic, Log, and Engineer. The 'Monitoring' section is expanded, showing 'Iperf' as the selected option. The main content area is titled 'Performance Measurement Tool' and contains the 'Iperf Settings' form. This form includes a 'Status' section with 'Start' and 'Stop' radio buttons, where 'Stop' is selected. Below this are fields for 'Last Measurement Date/Time', 'Server Address', 'Server Port' (set to 5001), 'Measurement Time' (set to 60) with a 'secs' unit, 'Protocol Type' (set to TCP), and 'Number of parallel client' (set to 1). A large, empty rectangular box is provided for the measurement results. At the bottom right of the form are two buttons: 'Refresh' and 'Execute'.

- Input all the items and check “Enable” in the status menu. If you click “Apply button”, then speed with connected Iperf server device will be displayed in the result box, and “Last Measurement Date/Time” will also be updated.
- If you want to see the result again, then click “Refresh button”.

3.4.6.2. Diagnostic

The screenshot shows a web interface for network diagnostics. On the left is a 'Menu' sidebar with options: Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management, Firmware Management, Monitoring, Iperf, Diagnostic (highlighted), Log, and Engineer. The main area is titled 'Diagnostic' and has two tabs: 'Ping' (active) and 'Trace router'. The 'Ping' tab contains a form with the following fields: 'IP Address (URL)' with the value '8.8.8.8', 'Ping Packet Size (Bytes)' with '56', 'Ping Timeout (sec)' with '30', and 'Ping Count' with a dropdown set to '4'. Below the form is a text area displaying the results of a ping test to 8.8.8.8, showing four successful packets with varying response times. At the bottom right of the text area is an 'Apply' button.

Field	Value
IP Address (URL)	8.8.8.8
Ping Packet Size (Bytes)	56
Ping Timeout (sec)	30
Ping Count	4

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=115 time=73.088 ms
64 bytes from 8.8.8.8: seq=1 ttl=115 time=81.267 ms
64 bytes from 8.8.8.8: seq=2 ttl=115 time=91.272 ms
64 bytes from 8.8.8.8: seq=3 ttl=115 time=81.486 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 73.088/81.778/91.272 ms

- Input IP address to test, Ping Packet Size, Ping Timeout, Ping Count and click “Apply button” for starting Ping test.

Menu

Dashboard
Connection Mode
Status
Settings
LTE
Network
Firewall
User Management
Firmware Management
Monitoring
Iperf
Diagnostic
Log

Diagnostic

Ping
Trace router

Trace router

IP Address (URL)
Set Maximum TTL(Max Hops) (Max Hops)
Set the number of queries at each TTL
Report IP Address Only

30

3

☐

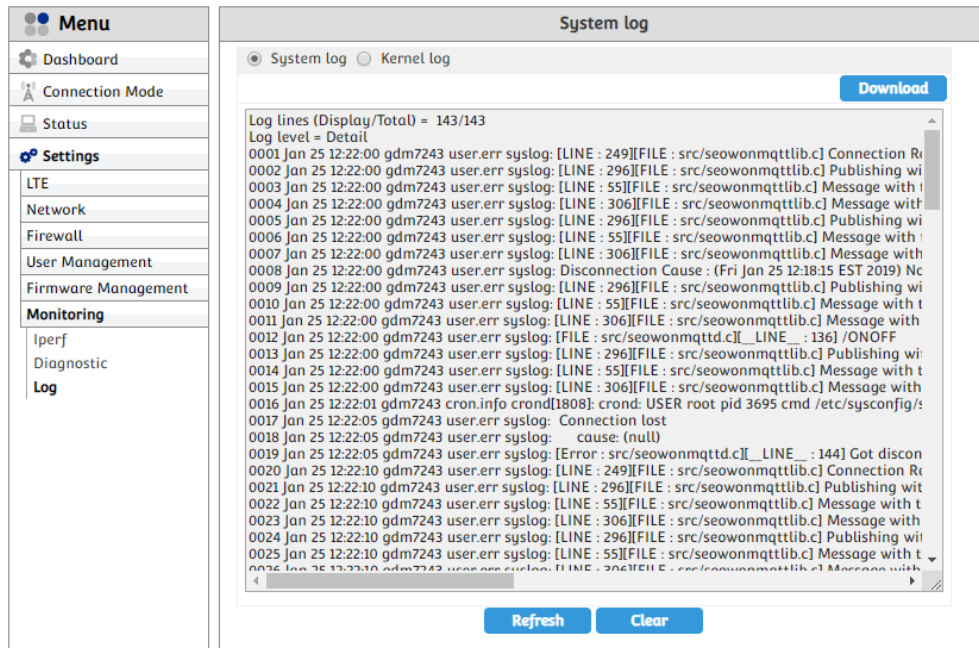
Apply

- Input IP address to trace.
- Input “Set Maximum TTL (Time To Live)”, “Set the number of queries at each TTL”. Those values are used for trace test and will be displayed in the result box
- If “Report IP Address Only” is checked, the result box will only show IP address data.

3.4.6.3. Log

The screenshot shows a web interface for configuring system logs. On the left is a 'Menu' sidebar with options: Dashboard, Connection Mode, Status, Settings, LTE, Network, Firewall, User Management, Firmware Management, Monitoring, Iperf, Diagnostic, and Log. The main area is titled 'System log' and contains two sections. The first section, 'System log Enable/Disable', has radio buttons for 'Disable' and 'Enable' (which is selected), and an 'Apply' button. The second section, 'View System Log', has radio buttons for 'System log' and 'Kernel log' (which is selected), and a 'Download' button. Below these are radio buttons for 'Detailed' (selected) and 'Simple'. A note states: 'Note: It could take a longer time to display detailed log'. The log content area is currently empty.

- System log will be displayed in case that “System log” is enabled, “System log” is checked in “View System log” menu, and user clicks “Refresh button” at the bottom of the page. “Clear button” will clear the system log displayed.
- You can download kernel log by click “Download button”



- Kernel log will be displayed in case that “System log” is enabled, “Kernel log” is checked in the “View System log” menu, and user clicks “Refresh button” at the bottom of the page log. Two options are available - Detailed and Simple. “Clear button” will clear the system log displayed.
- You can download kernel log by click “Download button”

4. The default setting for the SLC-1200GA CPE.

The table below shows the default settings of the SLC-1200GA CPE and can be changed by the installer.

Meaning of "Items requiring reset"

O : Parameters Applied After CPE Reset

X : Parameters that do not require a CPE reset

- : Parameter showing set value

Menu		Item	Default Value View	Items requiring reset
Settings	LTE	Basic (Only engineer account can be modified)	MMO Mode	Downlink MMO Mode 2-Layer (2-Layer/4-Layer) O
			Uplink CA Mode	Enable (enable/Disable) O
			Internal DM	Disable (enable/Disable) O
			Additional Commands	External DM Enable (enable/Disable) O
			UE Mode	Mode PS mode 2 O
			EMM Timer	T3402 12 / 1 minute O
			PSM Timer	T3411 5 / 2 seconds O
			Mode	Disable (enable/Disable) O
			T3324	5 / 2 seconds O
			T3412	1 / 10 hours O
		Cell Selection	Full Band	Full Band (Full Band / Frequency) O
			Status	42.43.48 -
			Band Selection	Band-42 (Checked) Band-43 (Checked) Band-48 (Checked) O
			PLMN Selection	Auto (Auto / Manual / From USIM) O
		Cell Lock	Search Cell	- O
			Cell Lock List	- O
		SIM Management	SIM Card Restriction	Unchecked O
		Default PDN	IMS Prefix	- O
			APN Name	- O
			Authentication Type	NONE O
		Multiple PDN	PDN Type	IPv4v6 (IPv4 Only / IPv6 Only / IPv4v6) O
			PDN cid	2 O
			APN Name	- O
			Authentication Type	NONE O
			PDN Type	IPv4v6 (IPv4 Only / IPv6 Only / IPv4v6) O
		Internet MTU	Enable	Unchecked O
			Internet MTU Settings	1500 O
		IPv6 Settings	IPv6 Enable	Enable (Enable / Disable) O
		CBS Settings (Only engineer account can be modified)	DHCPv6 Address Settings	DHCPv6 Autoconfiguration Mode Stateless (Stateless / Stateful) O
			Enable	CBSD Enable Enable (Enable / Disable) X
			Selected Category	Category B (EUD / Category A / Category B) X
			CPI Enable	Disable (Enable / Disable) X
			Sas URL	https://developer.s-c-02.federatedwireless.com/v1.2/ X
			Cert	etc/ssl/certs/TS.pem X
			User ID	IQmaM X
			F ID	V7MESL.C-120T420GA X
			Category	B X
			SupportedSpec	FFS X
			Longitude	-105 X
			HeightType	agl X
			Vertical	1.0 X
			Antazimuth	359 X
			Antgain	6 X
			Antbeamwidth	65 X
			Meascapability	- X
			Cert Password	123abcdelfg X
			Call Sign	callSign123 X
			Radiotech	E_UTRA X
			Latitude	39 X
			Height	8.0 X
			Horizontal	1.0 X
			Indoor	false X
			Antdowntilt	2 X
			Eirpcapability	30 X
			Antmodel	antennaModel123 X
			Meascapability2	- X
		Spectrum Inquiry	Inquired Low Freq	3500000000 X
			Inquired High Freq	3700000000 X
		Grant	GRANT AUTO	Enable (Enable / Disable) X
		Switch	Switch Mode	NAT (NAT / Bridge) O
			Switch Setup	Enable DHCP Server On O
		DHCP Server	Gateway IP Address	192.168.1.1 O
			Gateway Subnet Mask	255.255.255.0 O
			Start IP Address	192.168.1.2 O
			Number of users	253 O
			From ISP	Checked O
			DHCP Lease Time	3600 O
			Lease Reservation Table	Empty O
		DMZ	Enable DMZ	Disable (enable / Disable) O
			Redirect ICMP To The Host	Disable (enable / Disable) O
			Exclude Web Server Port	Enable (enable / Disable) O
			Private LAN IP Address	192.168.1.2 O
		Port Forwarding	Name	- X
			Protocol	Both (BOTH / TCP / UDP) X
			Start Port	- X
			End Port	- X
			Destination IP	- X
			Destination Port	- X
			Port Forwarding List	- X
		Port Triggering	Name	- X
			Port Type	RANGE (RANGE / SINGLE) X
			Trigger Protocol	ALL (ALL / TCP / UDP) X
			Trigger Port	- X
			Open Protocol	ALL (ALL / TCP / UDP) X
			Open Port	- X
		VPN Configuration	Port Trigger List	- O
			VPN Configuration Settings	VPN Disable (Disable / GRE / L2TP / PPTP) O
		VPN Passthrough	PPTP Service	Checked X
			L2TP/IPSEC Service	Checked X
		UPnP	Universal Plug & Play	UPnP Enable/Disable Enable (Enable / Disable) X
		QoS	QoS Setup	QoS Enable/Disable Disable (Enable / Disable) O
		DDNS	Dynamic DNS	DDNS Enable Disable (Enable / Disable) X

Settings	Firewall	Basic	Firewall Setup	Firewall Enable/Disable	Enable (Enable / Disable)	X
				Allow Ping From WAN	Enable (Enable / Disable)	X
				Allow HTTP login from WAN	Enable (Enable / Disable)	X
				Allow HTTPS login from WAN	Disable (Enable / Disable)	X
				Multicast Filter	Disable (Enable / Disable)	X
		SIP ALG Settings	SIP ALG Settings	Enable SIP ALG	UnChecked	O
				SIP port	5060	O
				URL Filter Enable	Disable (Enable / Disable)	O
		Filter Setup	Filter Setup	Select Filter	IP Filter (IP Filter / MAC Filter)	O
				Access Control Enable	Disable (Enable / Disable)	X
				Default Access Mode	Checked Black List	X
		Access Control	Access Control	Black List	-	-
				Devices Online	-	-
				Binding Setting	IP-MAC Binding Enable	Disable (Enable / Disable)
		IP-MAC Binding	IP-MAC Binding	Bind list	-	-
				ARP List	-	-
				Privilege	system (system / user)	X
	Account	Account Management	Username	system	X	
			Customer Name	system	X	
			Language	Language Setting	English	-
	Restore Default	Restore Default	Factory reset	-	O	
	Reboot	System Reboot	Last Good Configuration	-	-	
			Reboot the System	-	-	
			TR-069	Disable (Enable / Disable)	O	
	User Management	TR-069 Settings	TR-069 Settings	Periodic Inform	Enable (Enable / Disable)	O
				Periodical Inform Interval	300	O
				ACS Address	http://acs.seowonintech.co.kr/acsadmin/opseserver	O
				Username	-	O
				Password	-	O
				Connection Request Username	-	O
				Connection Request Password	-	O
				NTP Client Enable/Disable	Enable (Enable / Disable)	X
				Local Time	-	-
				Time Server	us.pool.ntp.org	X
		Date and Time	Time Zone Setup	Time Zone	Eastern Time (US and Canada)	X
				Enable Daylight Saving	Unchecked	X
				Start Date	First Sunday of April at 2 o'clock	X
				End Date	Last Sunday of October at 2 o'clock	X
				Never check for updates	Unchecked	O
				Check for update at device booting	Unchecked	O
		FOTA	FOTA Setup	In the upgrade cycle	Checked	O
				FOTA periodic timer Start / End	00 to 24	O
				FOTA periodic timer Periodic	1 day	O
				FOTA randomization timer	15 minutes	O
				Update Server URL	http://61.83.223.242/TE/SEOWON/ODU	O
				Check URL	-	-
		Remote Management	HTTP Server	Remote IP Address	-	O
				Port Number	80	O
			HTTPS Server	Enable	Unchecked	O
				Port Number	443	O
		Firmware Management	Software	Software Update	Filename 1	-
Monitoring		Iperf	Iperf Settings	Status	Stop (Start / Stop)	-
				Last Measurement Date/Time	-	-
				Server Address	-	-
				Server Port	5001	-
				Measurement Time	60	-
				Protocol Type	TCP (TCP / UDP)	-
				Number of parallel client	1	-
				IP Address (URL)	-	-
	Ping Packet Size (Bytes)			56	-	
	Ping Timeout (sec)			30	-	
	Diagnostic	Ping	Ping Count	4	-	
			IP Address (URL)	-	-	
			Set Maximum TTL(Max Hops) (Max Hops)	30	-	
			Set the number of queries at each TTL	3	-	
		Trace Router	Report IP Address Only	UnChecked	-	
			System log Enable/Disable	Disable (Enable / Disable)	O	
			Kernel Log (System log / Kernel log)	-	-	
			View System Log	Simple (Detailed / Simple)	-	

Acronyms

3GPP	3rd Generation Partnership Project
ACS	Auto Configuration Servers
ALG	Application Layer Gateway
APN	Access Point Name
ARP	Address Resolution Protocol
CA	Carrier Aggregation
CBRS	Citizens Broadband Radio Service
CBSD	Citizens Broadband radio Service Device
CID	Context Identification (Parameter)
CM	Connection Manager
CPE	Customer Premises Equipment or Customer Provided Equipment
CPI	Certified Professional Installer
CQI	Channel Quality Indicator
DDNS	Dynamic DNS(Domain Name System) Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
EIRP	Effective Isotropic Radiated Power
EMM	EPS Mobility Management
EPS	Evolved Packet System
EUD	End User Device
E-UTRA	Evolved Universal Terrestrial Radio Access
FOTA	Firmware Over The Air
FTP	File Transfer Protocol
FW	Firmware
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet Control Message Protocol
IDENT Protocol	Identification Protocol
IMEI	International Mobile Equipment Identity
IMS	IP(Internet Protocol) Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

IRC	Internet Relay Chat
ISP	Internet Service Provider
LAN	Local Area Network
LTE	Long-Term Evolution
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control Address
MCC	Mobile Country Code
MCS	Modulation Coding Scheme
MNC	Mobile Network Code
MPPE	Microsoft Point-to-Point Encryption
MTU	Maximum Transmission Unit
NAS	Non-Access Stratum
NAT	Network Address Translation
NTP	Network Time Protocol
ODM	Original Development Manufacturing
OUI	Organizationally Unique Identifier
PCI	Physical Cell Identity
PDN	Packet Data Network
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMI	Precoding Matrix Indicator
PPTP	Point-to-Point Tunneling Protocol
PUK	Personal Unlock Key
QoS	Quality of Service
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
SAS	Spectrum Access System
SDK	Software Development Kit
SIM	Subscriber Identity Module
SINR	Signal to Interference & Noise Ratio
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TM	Transmission Mode
TR-069	Technical report 069
TTL	Time To Live
UDP	User Datagram Protocol

UICC	Universal Integrated Circuit Card
UPnP	Universal Plug and Play
URL	Uniform Resource Locator
USIM	Universal Subscriber Identification Module
VPN	Virtual Private Network
WAN	Wide Area Network