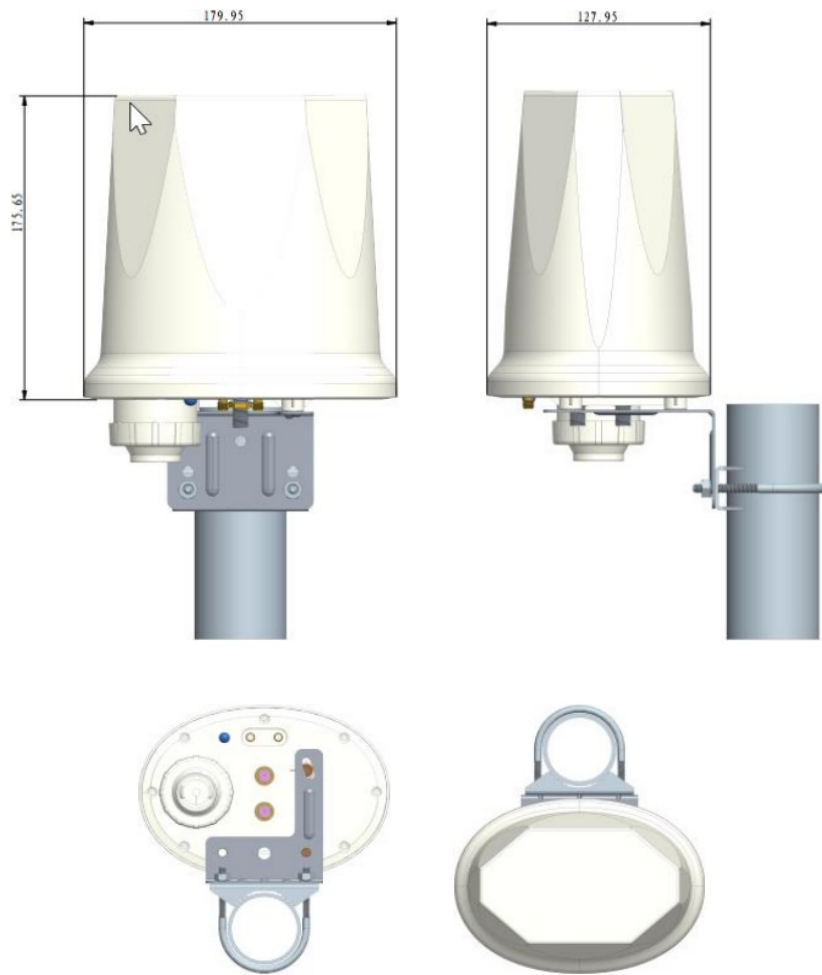


Asiatelco PW550 ATEL 5G CPE Indoor Fixed Wireless Access Router User Manual

Contents

- 1 ATEL 5G CPE User Manual**
 - 1.1 1. About this Manual**
 - 1.2 2. Router Interfaces**
 - 1.3 3. Configuring the Router**
 - 1.3.1 3.1 Login**
 - 1.3.2 3.2 Dashboard**
 - 1.3.3 3.3 Status**
 - 1.3.3.1 3.3.1 WAN Status**
 - 1.3.3.2 3.3.3 Cellular Status**
 - 1.3.3.3 3.3.4 Network Status**
 - CA**
 - 1.3.3.4 3.3.5 Software**
 - 1.3.3.5 3.3.6 Device List**
 - 1.3.3.6 3.3.7 Statistics**
 - 1.3.4 3.4 Settings**
 - 1.3.4.1 3.4.1 Basic**
 - 1.3.4.2 3.4.3 VPN**
 - 1.3.4.3 3.4.4 Security**
 - 1.3.4.4 3.4.5 Adanced**
 - 1.3.4.5 3.4.6 Cellular Settings**
 - 1.3.4.6 3.5 SMS**
 - 1.4 Glossary**
- 2 Documents / Resources**
 - 2.1 References**
- 3 Related Posts**

**ATEL 5G CPE
User Manual**



1. About this Manual

The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice. FCC ID: XYO-PW550

2. Router Interfaces

The Router has been designed to be placed on a desktop. All of the cables exit from the front of the Router for better organization and utility. The LED indicators are easily visible on the top of the Router to provide you with information about network activity and status:

- LED

LED	Bar	Color	SINR
Tri-color LED	Signal Level 5	purple	SINR>18dBm
	Signal Level 4	Blue	SINR:12~18dBm
	Signal Level 3	Green	SINR:6~12dBm
	Signal Level 2	Yellow	SINR:2~6 dBm
	Signal Level 1	Red	SINR<2 dBm
	Error	Red Blinking	No SIM, No signal
	Off		No Signal
Note		Blinking	On 1.5S, Off 1.5S
		All LED Blinking	While SW is updating

- **RJ-45 Switch**

This switch allows CPE to connect with your computer via RJ-45 ports. If you want to land into internet, the switch must be in RJ-45 port.

- **Power**

20V, 1.5A (depends on Router power consumption)

Note:

Adapter shall be installed near the equipment and shall be easily accessible.

3. Configuring the Router

The basic settings in WebGUI consist of four main parts named Home, Diagnostics, Settings, LTE. You can login to WebGUI as follows, and configure the settings according to your requirements.

Connect the PC to Router using the CAT-5 Ethernet cable. Use any one of the four Ethernet ports on the CPE. Power on the device and waiting for about 40 seconds until the device finished initializing. Please ensure that USIM card has been inserted into USIM slot in Router.

3.1 Login

Open your Web browser and enter 192.168.0.1 in the address bar;

Login window will popup;

When prompted for User name and password, enter the following username and password.

Username/Password: admin/on label

3.2 Dashboard

After successful login, the following screen will appear and you will see four main menus on the top bar of the WebGUI.

The bars in the middle indicate the received signal level and USIM icon displays the status of USIM. Click “help”, Click “Logout”, the screen will turn to login window.

From this page, you can also know Network status, WAN Info, LAN Info, Data Traffic and Device&SIM Info.

UNICOM

NR5G-SA

English ▾

Logout

Dashboard	Status	Settings	SMS
-----------	--------	----------	-----

Network

Connection Status: Connected

Band: n78

PCI: 142

RSRP: -102 dBm

RSRQ: -5 dB

SINR: 6 dB

WAN Info

IP: 0.0.0.0

Netmask: 255.255.255.0

Gateway: 0.0.0.0

ISP DNS: 0.0.0.0

MAC Addr: E6:60:6E:23:5A:1C

LAN Info

IP: 10.66.4.244

Netmask: 255.255.255.248

MAC Addr: E6:60:6E:23:5A:1C

DHCP Range: 192.168.0.2 - 192.168.0.254

Connect Devices: 1

Data Traffic

Received Traffic* (DL): 0 MB

Sent Traffic* (UL): 0 MB

Total Traffic* (DL+UL): 0 MB

Session Time: 00:10:28

Up Time: 00:11:22

*traffic since last reset, restart or reconnection of the device

Reset

Device & SIM Info

Router Version: CPE5_PW550_N0_00_v0.0.1

Module Version: 81103.7000.00.06.01.28

UICCID: 89860919023101021205

IMSI: 460018111340397

IMEI: 863867028241378

SN: 23456789

Model Name: WB550

3.3 Status

On this page, you can see WAN Status, LAN Status, LTE Status, Software, Device List and Statistics.

WAN Status	WAN Status
WiFi LAN Status	WAN Mode Cellular WAN
Cellular Status	Cellular Information
Network Status CA	Cellular IP Address Unknown
Software	Cellular Primary DNS 112.65.184.255
Device List	Cellular Secondary DNS 210.22.84.3
WLAN Device List	IPV6 WAN Information
Statistics	IPV6 WAN IP Address 2408:840d:9121:5043:1766:ea71:5c36:96e2

3.3.1 WAN Status

From the WAN Status, you can see WAN IP Address, WAN Primary DNS and WAN Secondary DNS information.

WAN Status	
WAN Mode	Cellular WAN
Cellular Information	
Cellular IP Address	Unknown
Cellular Primary DNS	112.65.184.255
Cellular Secondary DNS	210.22.84.3
IPv6 WAN Information	
IPv6 WAN IP Address	2408:840d:9121:5043:1766:ea71:5c36:96e2

3.3.3 Cellular Status

Clicking on the “LTE Status”, you can see the LTE information i.e. Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, PCI, Cell ID and Band.

Cellular Status	
Connection Status	Connected
USIM Status	Ready
IMEI	863867028241378
IMSI	460018111340397
RSRP	-96 dBm
RSRQ	-1 dB
RSSI	-69 dBm
SINR	9 dB
PCI	142
Band	n78
NCI	5AE291002
NCGI	460015AE291002
NARFCN	627264
gNodeB ID	5AE291002
DL BLER	3
UL BLER	1
DL MCS	0

3.3.4 Network Status CA

From this page, you can know the network status of the device.

Network Status CA							
Index	Band	PCI	EARFCN	Bandwidth	MIMO	Modulation	RSRP
PCC	n78	142	627264	100MHz	3/2	16QAM	-95

3.3.5 Software

From this page, you can know the IDU software version and the LTE software version.

Software	
Software Version	CPE5_PW550_N0_00_v0.0.1
Module Version	81103.7000.00.06.01.28

3.3.6 Device List

From this page, you can know the users' information, include hostname, MAC address, IP address and expires time.

Device List				
Hostname	MAC Address	IP Address	Type	Expires
zhfei-pc Host	2C:16:DB:AB:DA:13	192.168.0.152	Ethernet	23:38:16
<button>Refresh</button>				

3.3.7 Statistics

From this page, you can know the users' information, include hostname, MAC address, IP address and expires time.

Statistics				
	Download		Upload	
Cellular Speed	0 Kb/s		0 Kb/s	
Cellular	Duration	Downloaded	Uploaded	Total Used Data
Current Session	00:00:00	0 MB	0 MB	0 MB
Total	16:04:53	2 MB	1 MB	3 MB
The amounts of data is approximate. For more information please contact your network operator.				
<button>Clear</button>				

3.4 Settings

The settings menu consists of three main menus named Basic Settings, Advanced Settings and System Settings.

3.4.1 Basic

3.4.1.1 Management

The default password is admin, you can enter 1~32 characters for 2 times as your new password. Then you would logout automatically and you should login to the system by the new password. And you can click the "Restore" button to load default to the factory setting and click the "Reboot" button to reboot the device.

Device Settings	
Username	admin
Current Password	<input type="text"/> (32 characters max.)
New Password:	<input type="text"/> (32 characters max.)
Repeat Password	<input type="text"/> (32 characters max.)
<input type="button" value="Apply"/> <input type="button" value="Clear"/>	
Factory Reset	
Click button to restore default settings	<input type="button" value="Restore"/>
Device Reboot	
Click button to reboot the device	<input type="button" value="Reboot"/>

3.4.1.2 LAN Settings

Clicking on the “LAN Settings” tab will take you to the “LAN Settings” header page. On this page, all settings for the internal LAN setup of the CPE router can be viewed and changed.

LAN Settings	
IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP	<input type="text" value="Enabled"/> ▼
Start IP Address	<input type="text" value="192.168.0.2"/>
End IP Address	<input type="text" value="192.168.0.254"/>
Lease Time	<input type="text" value="86400"/>
Static IP 1	MAC: <input type="text"/> IP: <input type="text"/>
Static IP 2	MAC: <input type="text"/> IP: <input type="text"/>
Static IP 3	MAC: <input type="text"/> IP: <input type="text"/>
Static IP 4	MAC: <input type="text"/> IP: <input type="text"/>
Static IP 5	MAC: <input type="text"/> IP: <input type="text"/>
Static IP 6	MAC: <input type="text"/> IP: <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Clear"/>	

- **IP Address** – Enter the IP address of your router (factory default: 192.168.0.1).
- **Subnet Mask** – An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **DHCP** – Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server

within your network or else you must configure the address of your PC manually.

- **Start IP Address** – Specify an IP address for the DHCP server to start with when assigning IP address. The default start address is 192.168.0.2.
- **End IP Address** – Specify an IP address for the DHCP Server to end with when assigning IP address. The default end address is 192.168.0.254.
- **Lease Time** – The Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time in minutes and the user will be “leased” this dynamic IP address. After the time is up, the user will be assigned a new dynamic IP address automatically.
- **Static IP** – IP/MAC binding function, the system will assign a fixed IP address to the MAC according to the rules.



Note:

1. If you change the IP Address of LAN, you must use the new IP address to login to the CPE router.
2. If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will change at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

3.4.1.3 Software Upgrade

On this page, you can upgrade the current Router version and LTE Version from the local PC. 180s is needed to complete the whole upgrade process, and then the device will reboot automatically.

Software Upgrade	
Router Upgrade:	<input type="button" value="选择文件"/> 未选择任何文件
<input type="button" value="Apply"/>	

3.4.1.4 Remote Upgrade

After the device detects the new router and LTE version from Web server, the device will upgrade the new version automatically, or the device will upgrade the new version after you click the “Upgrade” button.

Device Remote Upgrade	
Upgrade Status	Waiting for network connection
Remote Upgrade	<input type="button" value="Enabled"/> ▼
Upgrade Address (IP or URL)	<input type="text" value="192.168.0.152"/>
Upgrade Mode	<input type="button" value="Manual"/> ▼
Manual	<input type="button" value="Check"/> <input type="button" value="Upgrade"/>
<input type="button" value="Apply"/>	

3.4.1.5 Automatic Reboot

On this page, you can set automatic restarts at one time per day, weekly, or monthly.

Automatic Reboot Settings	
Automatic Reboot	Disabled ▼
<input type="button" value="Apply"/>	

3.4.1.6 Install the device

1. Gather tools and materials
2. Install SIM cards
3. Install the PoE cable
4. Select a location
5. Secure the device to the wall

3.4.1.7 Testing the connection

1. Check the LED on the device
2. Open the APP and BT on your smart phone
3. Connect the BT between smart phone and WB550
4. Follow APP instruction to complete setting and testing

3.4.3 VPN

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet). VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol, PPTP, IPSec, L2TP and GRE.

PPTP VPN	
Basic	Enable <input type="button" value="Enable ▼"/>
WiFi	
VPN	Mode <input type="button" value="Client ▼"/>
PPTP VPN	Server Address <input type="text"/>
IPSec VPN	Account <input type="text"/>
L2TP VPN	Password <input type="text"/>
GRE VPN	
Security	Get online through VPN <input type="button" value="Disable ▼"/>
Advanced	Client Connection Status Disconnected
Cellular Settings	<input type="button" value="Apply"/>

Note: VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to “pass through” the router.

3.4.4 Security

46011 NR5G-SA English ▾ Logout

Dashboard
Status
Settings
SMS

Basic

WiFi

Security

MAC Filtering

IP/Port Filtering

Port Forwarding

Virtual Server

VPN Passthrough

DMZ

Parental Control

Advanced

Cellular Settings

MAC Filtering Settings

MAC Filtering
Disabled ▾

Default policy - the device that don't match any rule would be:
Allow ▾

Mac Filtering Schedule

Schedule
Disabled ▾

3.4.4.1 MAC Filtering

This function is a powerful security feature that allows you to specify which wireless client users are not allowed to surf the Internet.

MAC Filtering Settings

MAC Filtering
Disabled ▾

Default policy - the device that don't match any rule would be:
Allow ▾

The default MAC filtering setting is disabled, so you should enable it before you begin to configure the filter. Then click the “Add New” button, you can configure the rules you like.

Default Policy: The packets that don't match with any rules would be “Allow/Deny”. If you choose the “Allow” button here, the MAC address that you add would be dropped. Otherwise, only the MAC addresses on the rule table can be accepted.

The new rules will be shown on the rule table, here you can delete the rules that you have selected and add new rules sequentially. The maximum rule count is 10.

MAC Address Rule Table

ID	MAC Address	Action				
1	38:65:82:43:31:1D	-	-	-	-	Drop
Others would be accepted						-

(Note: maximum rule count is 10)

3.4.4.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users to login the router device.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Then clicking the “Add New” button, you can configure the settings you like (Figure 4-4-2-2-3).

Default Policy: The packets that don't match with any rules would be “Dropped/Accepted”. If you choose “Dropped” here, the action of the new rule would be “Accept”. Otherwise, the action turns to be “Drop” and the

packet that don't match with any rules would be accepted.

IP/Port Filtering Settings

IP/Port Filtering Disabled

Default policy - the IP/port that doesn't match any rule would be: Dropped

Apply

Rule Table

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	
1	<input type="checkbox"/>	8.8.8.8	192.168.0.180	All	-	-	Drop

Others would be accepted

Apply Delete Add New (Note: maximum rule count is 10)

- **Dest IP Address** – The IP address of a website that you want to filter (Such as google 74.125.128.106).
- **Source IP Address** – The IP address of PC. (Such as 192.168.0.2).
- **Protocol**- TCP, UDP, ICMP
- **Dest Port Range**- To restrict Internet access to the single user, you can set a fixed value, such as 21-21.
- **Source Port Range**- 1~65535
- **Action**- Accept, Drop

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 10.

3.4.4.3 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” header page. Clicking on the “Add New” button, you can configure IP address, port range to achieve the port forwarding purpose.

Port Forwarding Rule Table

ID	IP Address	Port Range	Protocol	Interface
----	------------	------------	----------	-----------

☐ Select All (Note: maximum rule count is 20)

Edit Delete Add New

Port Forwarding Settings

IP Address 192.168.0.2

Port Range 5100 - 5200

Protocol TCP&UDP

Apply Back

- **IP Address**- The IP address of the PC running the service application;
- **Port Range**- You can enter a range of service port or set a fixed value;
- **Protocol**- UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the “Add New” button here. The maximum rule count is 20.

Port Forwarding Rule Table

ID	IP Address	Port Range	Protocol	Interface
1 <input type="checkbox"/>	192.168.0.152	1 - 200	TCP + UDP	Both

☐ Select All
 (Note: maximum rule count is 20)

Edit

Delete

Add New

3.4.4.4 Virtual Server

Clicking on the header of the “Virtual Server” button will take you to the “Virtual Server” header page (Figure 4-4-2-5-1). It is a feature that similar to port forwarding, clicking on the “Add New” button, you can configure IP address, public port, private port and protocol to achieve the virtual server function.

Virtual Server Rule Table					
ID	IP Address	Public Port	Private Port	Protocol	Interface
1	<input type="checkbox"/>	192.168.0.152	1 - 200	TCP + UDP	Both
<input type="checkbox"/> Select All (Note: maximum rule count is 20)					
<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/>					

Virtual Server Settings	
IP Address	<input type="text" value="192.168.0.4"/>
Public Port	<input type="text" value="5100"/>
Private Port	<input type="text" value="5200"/>
Protocol	<div> <div>TCP&UDP</div> <div> <div>TCP&UDP</div> <div>TCP</div> <div>UDP</div> </div> </div>
<input type="button" value="Apply"/> <input type="button" value="Back"/>	

- **IP Address-** The IP address of the PC running the service application;
- **Public Port-** The port of server-side;
- **Private Port-** The port of client-side, it can be same with the public port;
- **Protocol-** UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the “Add New” button here. The maximum rule count is 20.

Virtual Server Rule Table

ID	IP Address	Public Port	Private Port	Protocol	Interface
1 <input type="checkbox"/>	192.168.0.152	1	200	TCP + UDP	Both
<input type="checkbox"/> Select All (Note: maximum rule count is 20)					
<div>EditDeleteAdd New</div>					

3.4.4.5 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol, PPTP, L2TP and IPSec.

VPN Passthrough	
L2TP Passthrough	Enable ▾
IPSec Passthrough	Enable ▾
PPTP Passthrough	Enable ▾
<input type="button" value="Apply"/>	

Note: VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to “pass through” the router.

3.4.4.6 Demilitarized Zone

From this page, you can configure a De-militarized Zone (DMZ) to separate internal network and Internet.

- **DMZ IP Address-** The IP address of your PC. (such as 192.168.0.3)

DMZ Settings	
DMZ	Disabled ▾
DMZ IP Address	<input type="text"/>
<input type="button" value="Apply"/>	

DMZ Settings	
DMZ	Enabled ▾
DMZ IP Address	192.168.0.3
<input type="button" value="Apply"/>	

3.4.4.7 Parental Control

The rules added to the rule tables will determine, when access to the Internet or website will be Denied. Internet or website access will be automatically blocked in the defined time.

Parental Control

Parental Control

Enabled ▾

Apply

The rules added to the rule tables will determine, when access to the Internet or website will be Denied. Internet or website access will be automatically blocked in the defined time.

Time Rule Table

No.	Rule Name	Mac Address	Device Name	Defined Time
<input type="checkbox"/> Select All <div>(Note: maximum rule count is 20)</div>				
<div>Delete</div> <div>Edit</div> <div>Add New</div>				

Website Rule Table

No.	Rule Name	Mac Address	Device Name	Website/Content	Defined Time
<input type="checkbox"/> Select All <div>(Note: maximum rule count is 20)</div>					
<div>Delete</div> <div>Edit</div> <div>Add New</div>					

3.4.5 Advanced

3.4.5.1 Diagnostic

On this page, you can see “Ping” and Traceroute. Ping: you can ping IP address and domain name. Traceroute: you can traceroute IP address and domain name

Diagnostic Tool

Choose Operation :

☒ Ping
☐ Traceroute

Host :

Send

3.4.5.2 Dynamic DNS

The dynamic DNS function is disabled in default, you can choose the dynamic DNS provider to configure the DDNS settings.

DDNS Settings	
DDNS Status	Disabled
Dynamic DNS Provider	Disabled ▼
User Name	Disabled
Password	www.no-ip.com
Domain Name	www.dyndns.org
	www.zoneedit.com
	www.freedns.afraid.org
<input type="button" value="Apply"/>	

3.4.5.3 Backup&Restore

Clicking the “Backup” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.

Backup Settings	
<input type="checkbox"/> Need password to backup	<input type="text"/> (32 characters max.)
Backup device configuration	<input type="button" value="Backup"/>
Restore Settings	
<input type="checkbox"/> Need password to restore	<input type="text"/> (32 characters max.)
Restore device configuration from file	<input type="button" value="选择文件"/> 未选择任何文件
	<input type="button" value="Restore"/>

3.4.5.4 Network Management

Clicking on the header of the “System Settings” tab will take you to the “System Security Settings” page. From this page, you can configure the system security settings to protect the device itself from the external attacking.

Network Management		
Remote management (http)	Disabled ▼	(e.g. http://ip_address:port)
Remote management (https)	Disabled ▼	(e.g. https://ip_address:port)
HTTP Login(WebUI Management)	Enabled ▼	
HTTPS Login(WebUI Management)	Enabled ▼	
Respond to PING on WAN	Disabled ▼	
Respond to PING on LAN	Enabled ▼	
<input type="button" value="Apply"/>		

- **Remote management(http)**

You can access to the router via HTTP IP address and achieve the remote control function when the remote management feature is enabled.

- **Remote management(https)**

You can access to the router via HTTPS IP address and achieve the remote control function when the remote management feature is enabled.

- **Respond to PING on WAN**

It is allowed to ping on WAN in default, you can disable it here.

- **Respond to PING on LAN**

It is allowed to ping on LAN in default, you can disable it here.

- **HTTP Login(WebUI Management)**

This function allows the users to login the system by the http protocol method.

- **HTTPS Login(WebUI Management)**

This function allows the users to login the system by the https protocol method.

3.4.5.5 NTP

From this page, you can set the Current Time, Time Zone, NTP Server and NTP synchronization. When the device obtains the WAN IP, the current time will synchronize with the NTP server automatically.

NTP Settings	
Current Time	<input type="text" value="Mon, 31 Oct 2022, 23:22:13"/> <input type="button" value="Sync with host"/>
Time Zone:	<input type="text" value="(GMT-08:00) Pacific Time"/> ▼
NTP Server	<input type="text" value="time.nist.gov"/> e.g.:time.stdtime.gov.tw time.nist.gov ntp0.broad.mit.edu
Interval synchronization (hours of range 1 - 300)	<input type="text" value="24"/>
<input type="button" value="Apply"/>	

3.4.5.6 WAN Settings

From this page, you can set the wan's connection mode such as Cellular WAN, Load Balancing, Failover, ETH WAN or IP Passthrough.

Internet Connection	
Mode	<input type="text" value="Cellular WAN"/> ▼
Only Cellular WAN, all ethernet ports work as a LAN.	
<input type="button" value="Apply"/>	

3.4.6 Cellular Settings

3.4.6.1 Network

On this page, you can choose network mode, "Auto", "4G Only" and "5G Only". "Auto" mode is default mode.

Network		
Band selection	Auto ▼	
4G Band		
<input checked="" type="checkbox"/> B2	<input checked="" type="checkbox"/> B4	<input checked="" type="checkbox"/> B5
<input checked="" type="checkbox"/> B7	<input checked="" type="checkbox"/> B12	<input checked="" type="checkbox"/> B13
<input checked="" type="checkbox"/> B14	<input checked="" type="checkbox"/> B17	<input checked="" type="checkbox"/> B25
<input checked="" type="checkbox"/> B26	<input checked="" type="checkbox"/> B29	<input checked="" type="checkbox"/> B30
<input checked="" type="checkbox"/> B41	<input checked="" type="checkbox"/> B46	<input checked="" type="checkbox"/> B48
<input checked="" type="checkbox"/> B66	<input checked="" type="checkbox"/> B71	
5G Band		
<input checked="" type="checkbox"/> n2	<input checked="" type="checkbox"/> n5	<input checked="" type="checkbox"/> n7
<input checked="" type="checkbox"/> n12	<input checked="" type="checkbox"/> n14	<input checked="" type="checkbox"/> n25
<input checked="" type="checkbox"/> n30	<input checked="" type="checkbox"/> n41	<input checked="" type="checkbox"/> n48
<input checked="" type="checkbox"/> n66	<input checked="" type="checkbox"/> n71	<input checked="" type="checkbox"/> n77
<input checked="" type="checkbox"/> n78		
<input type="checkbox"/> Select ALL		
<input type="button" value="Apply"/>		

3.4.6.2 APN Settings

The default APN mode is automatic and APN is NULL, if you want to configure the LTE APN, you should choose the manual mode, then you can configure the APN settings by clicking on the “Add New” button.

APN Settings	
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Host Name	▼
Profile Name	Auto
APN	Auto
Authentication	None ▼
User Name	
Password	
<input type="button" value="Set as default"/>	

From the “Host Name” option, you can choose the APN that you had configured, then click “Set as default” to make it take effect.

APN Settings	
Mode	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Host Name	<input type="text" value="Add New"/> <input type="button" value="Cancel"/>
Profile Name	<input type="text" value="test"/>
APN	<input type="text" value="cmnet"/>
Authentication	<input type="text" value="None"/>
User Name	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Save"/>	

APN Settings	
Mode	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Host Name	<input type="text" value="test"/> <input type="button" value="Add New"/>
Profile Name	<input type="text" value="test"/>
APN	<input type="text" value="cmnet"/>
Authentication	<input type="text" value="None"/>
User Name	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Set as default"/> <input type="button" value="Save"/> <input type="button" value="Delete"/>	

3.4.6.3 Network Watchdog

Clicking on the header of the “Ping Watchdog” tab will take you to the “Ping Watchdog” page. From this page, you can configure “Ping Watchdog” feature.

Network Watchdog Settings	
Network ping	<input type="text" value="Enabled"/>
URL or IP adress to ping no.1:	<input type="text" value="8.8.8.8"/>
URL or IP adress to ping no.2:	<input type="text" value="8.8.8.8"/>
URL or IP adress to ping no.3:	<input type="text" value="8.8.4.4"/>
<input type="button" value="Apply"/>	

3.4.6.4 IP Passthrough

From this page, you can set Bridge mode, the menu is Enable/Disable.

IP Passthrough

IP Passthrough (Bridge) Enabled ▾

Apply

3.4.6.5 PCI Lock

On this page, you can lock or unlock the PCI and Earfcn connected to the LTE.

PCI Lock Status

Locked Status Disabled ▾

Apply

PCI Lock

Name	Cellular	EARFCN	PCI
Locked Value	5G ▾	<input type="text"/>	<input type="text"/>
Lock			

Serving Cell List

No	Cellular	EARFCN	PCI	Band	Bandwith	RSRP	RSRQ	SINR
----	----------	--------	-----	------	----------	------	------	------

Neighbour Cell List

No	Cellular	EARFCN	PCI	RSRP	RSRQ	SINR
----	----------	--------	-----	------	------	------

Lock Refresh




White List

No	Cellular	EARFCN	PCI
----	----------	--------	-----

Unlock

3.5 SMS

There are 3 function on this page, they are inbox, outbox and drafts. You can send and receive the SMS on this page.

46011 NR5G-SA    English ▾ Logout

Dashboard	Status	Settings	SMS
-----------	--------	----------	-----

Inbox 0/0

Outbox 2

Drafts 2

Inbox

New Message Delete

<input type="checkbox"/>	Sender	Content	Date
--------------------------	--------	---------	------

⏪ ⏩ 1 ⏪ ⏩ 1/1 GO

FCC Regulations

ATEL 5G CPE complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, under Part 15 of

the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used by the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF exposure compliance requirements, this grant applies to only Mobile Configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.


Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Glossary

Term	Definition
zhfei	V.1.0

11/01/22

Documents / Resources

	Asiateco PW550 ATEL 5G CPE Indoor Fixed Wireless Access Router [pdf] User Manual PW550 ATEL 5G CPE Indoor Fixed Wireless Access Router, PW550, ATEL 5G CPE Indoor Fixed Wireless Access Router, Indoor Fixed Wireless Access Router, Fixed Wireless Access Router, Wireless Access Router, Access Router, Router
---	---

References

- [User Manual](#)