XGS-PON ONT STICK
User Manual

Contents

1. Product introduction

1.1 Summary

EN-XGSFPP-OMAC-V2 SFP+ SFU is an integrated SFP+ ONT, complying with the
ITU-T G.9807.1 standard for 10-Gigabit-Capable Symmetric Passive Optical Network (XGS-PON). This transceiver provides a pluggable SC/APC SFP+ compliant interface to upgrade existing devices for FTTx services. EN-XGSFPP-OMAC-V2 can also support IEEE1588v2, and Y.1731 for mobile backhaul application.

EN-XGSFPP-OMAC-V2 is best suited for FTTH residential, mobile backhaul and network switch/router/MDU applications.

1.2 Highlights

❖ Bi-directional 9.953Gbps Upstream/9.953Gbps Downstream
❖ Compliant with ITU-T G.9807
❖ SFP package with SC/APC
❖ Support Digital Diagnostic Monitoring interface
❖ 1270nm Burst mode transmitter, and 1577nm Continuous Mode Receiver
❖ Single + 3.3V Power Supply
❖ ROHS-6/6 compliant
❖ Case Operation Temperature Ranges: Industrial: 0-70℃
❖ Laser Class 1 Product which comply with the Requirements of IEC 60825-1 and IEC60825-2
❖ Dying Gasp

1.3 Specifications

1.3.1 General

Model	EN-XGSFPP-OMAC-V2
ONT Type	XGSPON SFP+ SFU
Main SoC	Max Linear PRX126
Uplink	XGSPON
Downlink	10G SFI, 1000BaseX, 2500BaseX
Operating Temperature	C-Temp (0-70C), case temperatures

2. Installation

Figure 2-1

2.1 Connect to the switch

a) Plug the stick into the correct port of the switch.

b) Once you plug the stick in the switch, make sure the switch's Link LED for the SFP is on, meaning the switch recognizes the stick and properly powered up the stick.
c) Create a VLAN configuration on the SFP port and where you PC is connected, and make both ports untagged with the proper PVID
d) Plug the fiber from the splitter into the ONU stick
e) Make sure the ONU stick gets registered to the OLT

3. Configuration
3.1 Firmware upgrade with Tibit OLT
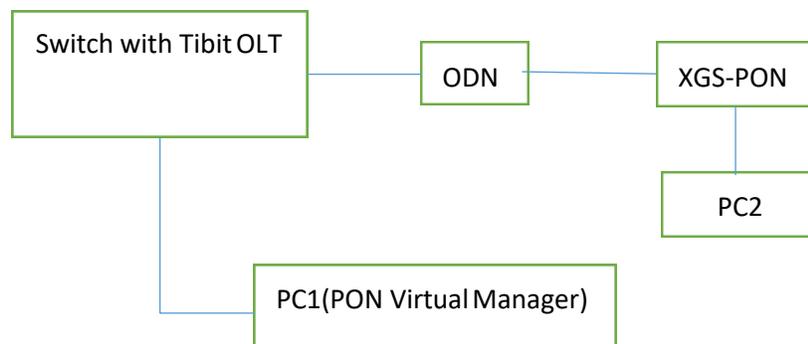
Figure 3.1

Working with the Tibit PON Manager, the firmware could be upgraded from the manager itself. The scenario is shown in Figure 3.1

To prepare, the firmware to be upgraded should be copied to the Tibit PON manager Virtual Machine.

1. Login the PON manager with your username and password
2. Run Browser: Open web browser with local address: 127.0.0.1
3. As shown in Figure 3.1-1, Global Config -> Files -> ONU firmware-> Upload from "sf_shared" (This is thefolder where the new firmware version is stored).
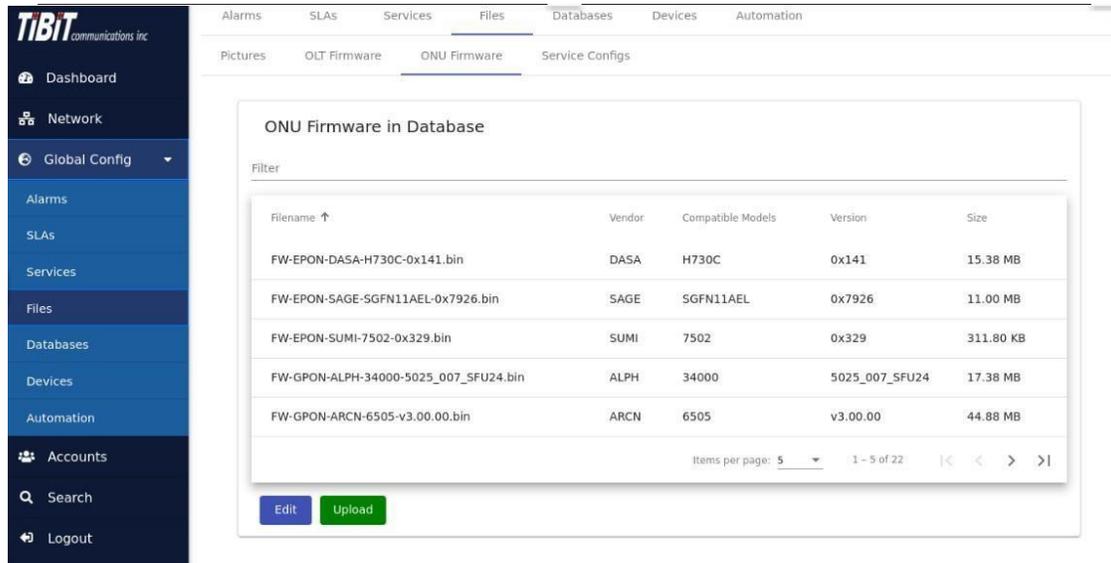
Figure 3.1-1
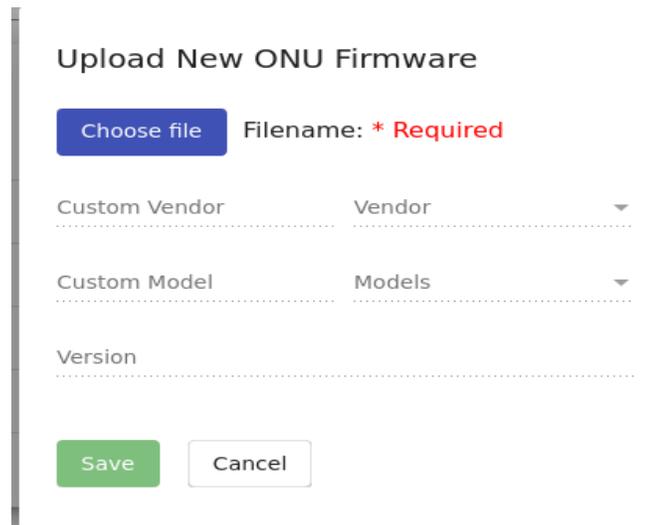
Figure 3.1-2

Click "Upload", as shown in Figure 3.1-2, then click "Choose file" to choose the right firmware version for upgrade.

Then fill in the information about the vendor (AZRS) and model number (WAS W110 for this example) and Version (the same with the version number from the file), click "Save"

4. As shown in Figure3.1-3, Go back to Network -> Topology to locate where the ONU is, then go to -> Firmware. Click "Edit"

mmary   Identification   Firmware   Services   P

ONU Firmware

Bank Pointer:	1
Bank 0:	
File:	
Version:	V1.0.06
Bank 1:	
File:	V1.0.08_20230215113636_WAS_110.img
Version:	V1.0.008
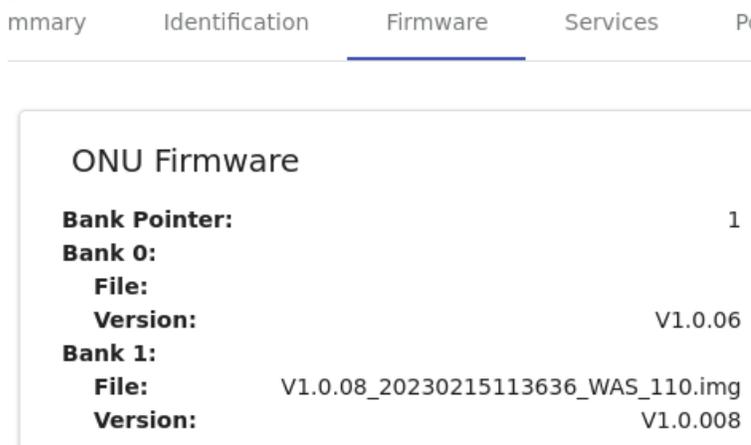
Figure 3.1-3

Since usually we firstly upgrade the backup bank, we configure the "bank pointer" to "State 1". As shown in Figure 3.1-4, it means that the current active running version is bank 1. What we are going to upgrade is bank 0. Click "Save". The ONU will be rebooted.

Summary   Identification   Firmware   Services   Ports

ONU Firmware

Bank Pointer
   State: 0

Config
0

Bank 0
   State Version: V1.0.06

Config Version
(W110i) V1.0.008
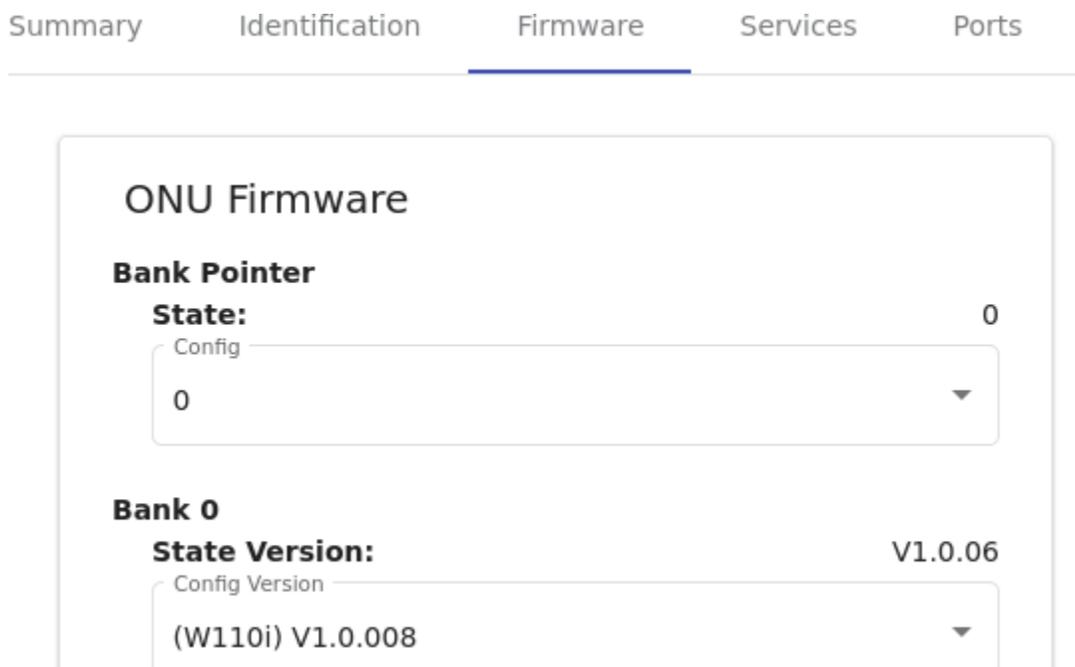
Figure 3.1-4

5. After the ONU works normally again, go back to Network -> Topology to locate where the ONU is, then go to -> Firmware. Click "Edit", as shown from Figure 3.1-4, click the State Version from Bank 0 and choose the version to be upgraded, then Click "Save". The upgrade process should begin.

6. Go Back to Network -> Topology, locate where the OLT is, then choose Firmware -> ONU firmware tocheck the upgrade status. When the status shows "Success", it means that the upgrade process has been successful. It is shown from Figure 3.1-5

AZRS00007358	0	V1.1.026_20220810145535_052C.img	Success

Figure 3.1-5

7. After the upgrade process, in order to run the newly upgraded firmware, we need to go back to Network -> Topology to locate where the ONU is. As shown in Figure 3.1-6, Go to -> Firmware, click"Edit", configure "Bank Pointer" to be "0" and "Save". When the ONU restarts, the newly upgraded firmware can be run on the ONU.

ONU Firmware

Bank Pointer
State: 1
Config

0

Bank 0
State Version: V1.0.11
Config Version

(Installed) V1.0.11

Bank 1
State Version: V1.0.08
Config Version

(W110i) V1.0.008

Figure 3.1-6

8. ONU Inventory

In order to keep the ONU's configuration when the ONU is offline, we need to the change ONU inventory.

Go to Topology and locate where the OLT is. Choose "Edit" and add the device to inventory then save the configuration.

Figure 3.1.7-1

3.2 Login

The device can be configured by the web interface. The following steps will enable you to login:

1. Conform to section "2. Installation" to install.

2. The device management default IP address is 192.168.11.1 since many switches uses 192.168.1.1 as the default IP address, which would be a conflict.

3. Open your web browser, type the device IP in the address bar.

4. Entry of the username and password will be prompted. Enter the default login username and password.

By default, there are one user level for management: the administrator account. The administrator account's username is "admin", and the password is "QsCg@7249#5281".

The administrator account is able to access and modify all the settings of the device.
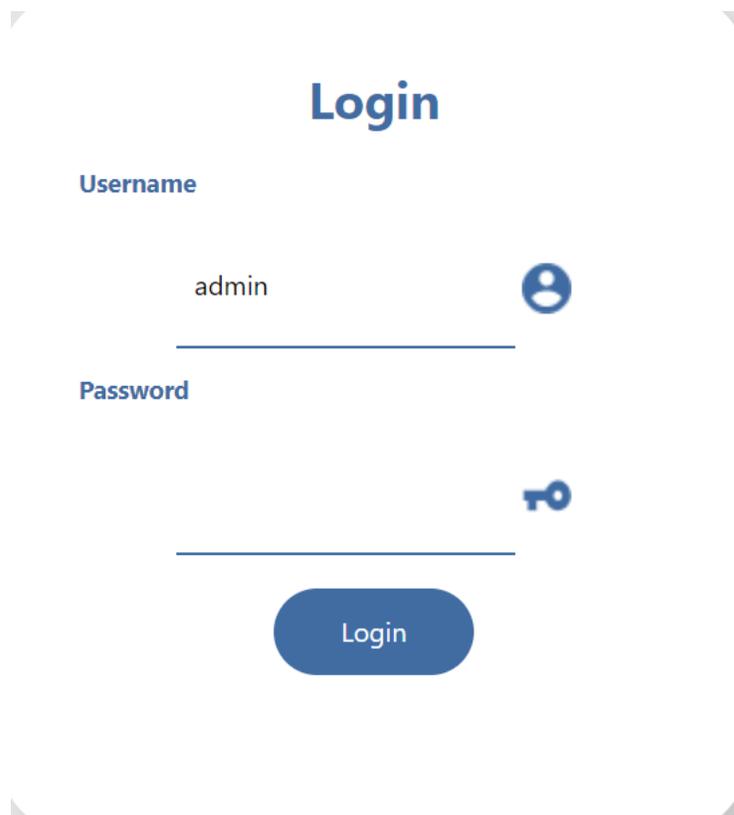
3.3 Status

The "Status" Tab page shows the main information for the device and the PON link connection status with the performance statistics as shown from Figure 3.3-1 and Figure3.3-2
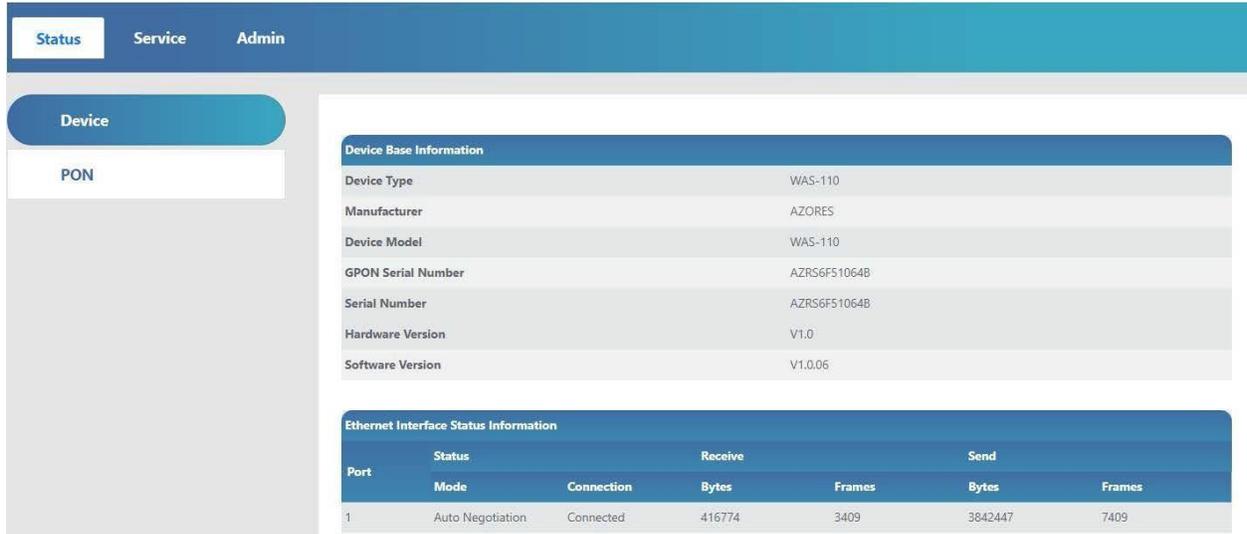
Figure 3.3-1
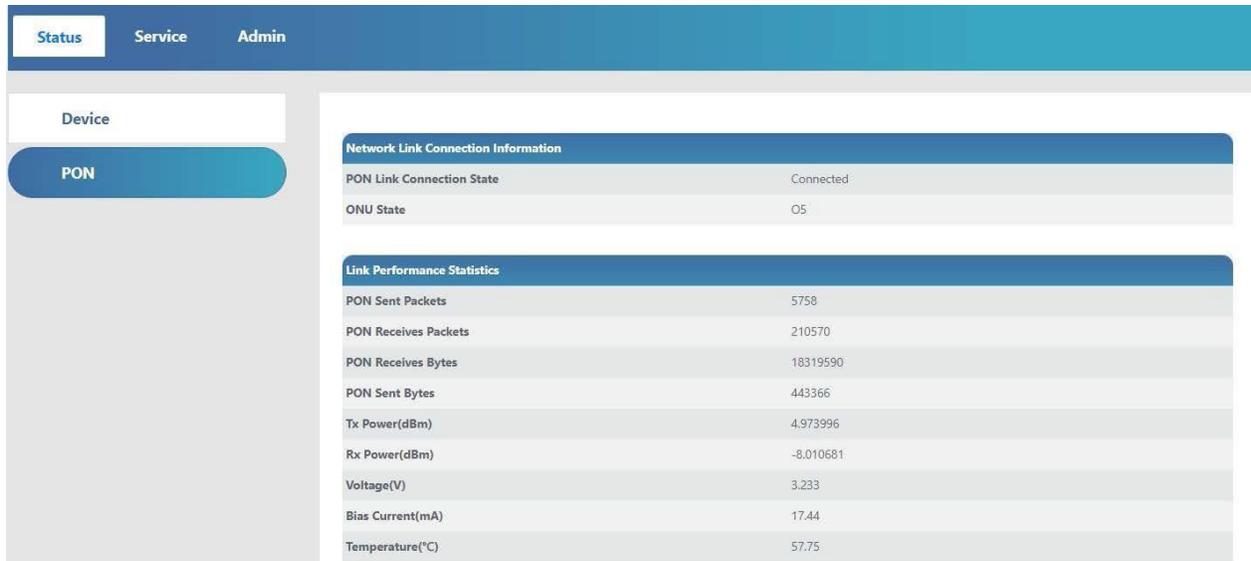
Figure 3.3-2

3.4 Service

3.4.1 Remote Access

This page is to enable/disable the interface to manage the device, like TELNET, HTTP, HTTPS and SSH based on your application scenarios and requirements.
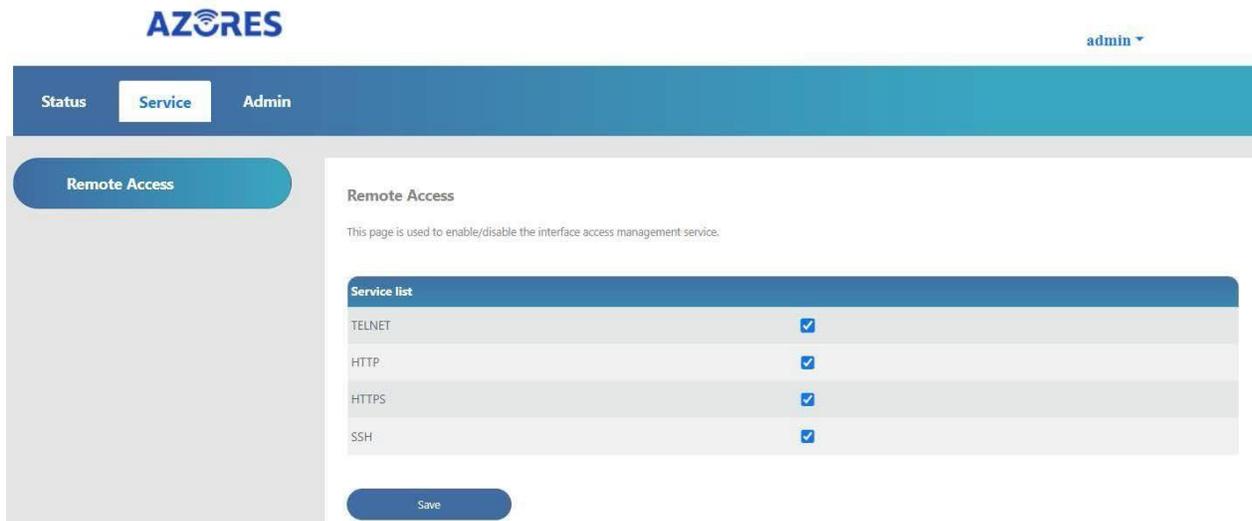
Figure 3.4.1

3.5 Admin

3.5.1 GPON Setting

This shows the registration ID and the serial number. We do not recommend changing them.
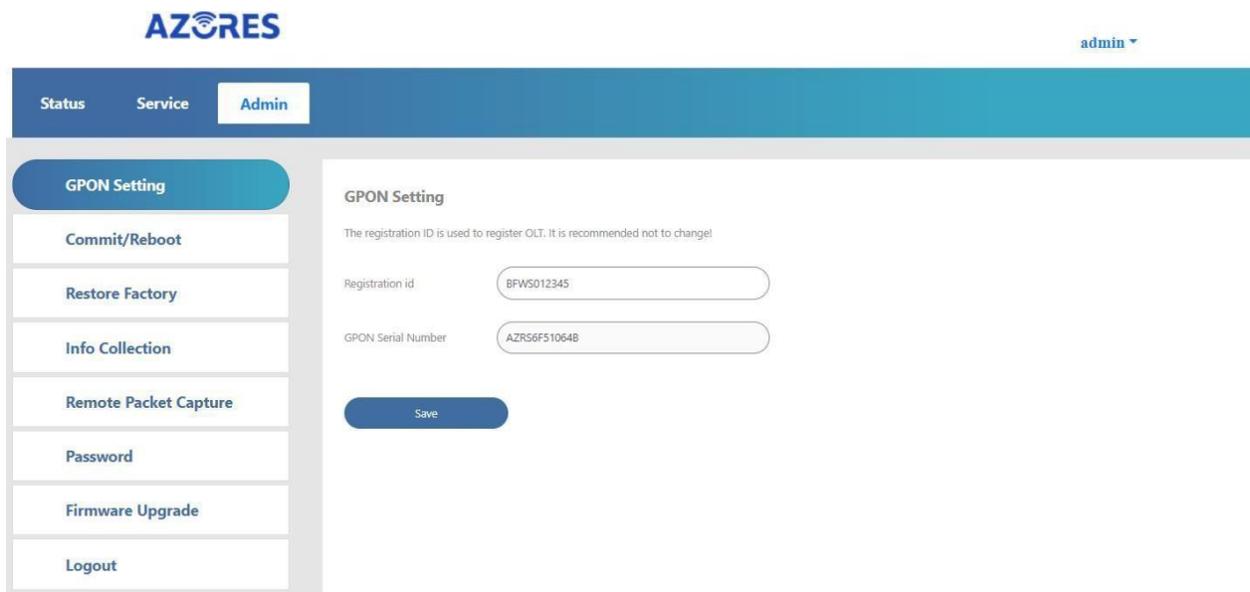
Figure 3.5.1

3.5.2 Commit and Reboot

- Press the "Commit and Reboot" button and the device will be rebooted.

Commit and Reboot

Click the button below to reboot your system.

Commit and Reboot
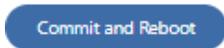
Figure 3.5.2

3.5.3 Backup/Restore

- Press the "Backup" button, a file with current device settings will be downloaded and stored.
- Press the "Choose File" button and select the data file then press the "Update" button, the device configuration will be updated, and this could be used when you need to replace the settings with the current one fromthe device.
- Press the "Restore Factory" button, then the device will be restored with the default configuration when it is right out of the factory. The whole process of restore factory will take several minutes.

Backup/Restore

Tip: You can backup and update settings on this page

Backup Settings: Backup

Update Settings: Choose File   No file chosen   Update

Restore Factory

Click the button below to restore the router to the factory settings.

Restore Factory

Figure 3.5.3

3.5.4 Information Collection

You could collect and download the logs and status related information from the device. This is helpful for us to do the debugging when you have issues using our device.
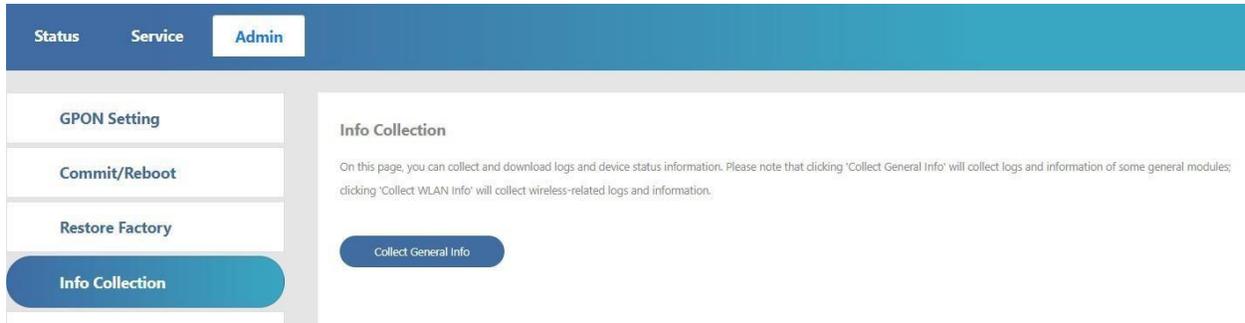
Figure 3.5.4

3.5.5 Remote Packet Capture

This tab page is to enable/disable the remote packet capture services. The port we use is 2002.
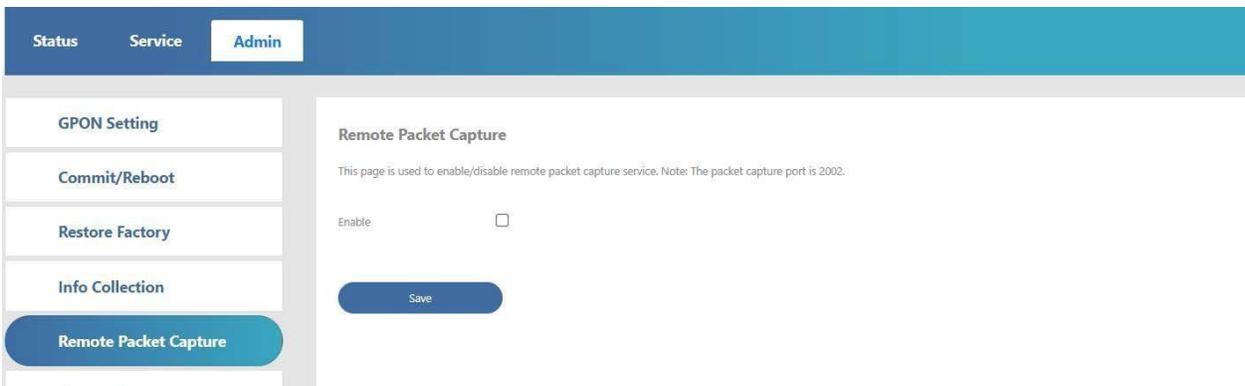
Figure 3.5.5

3.5.6 Password

This page allows the administrator to modify the password.
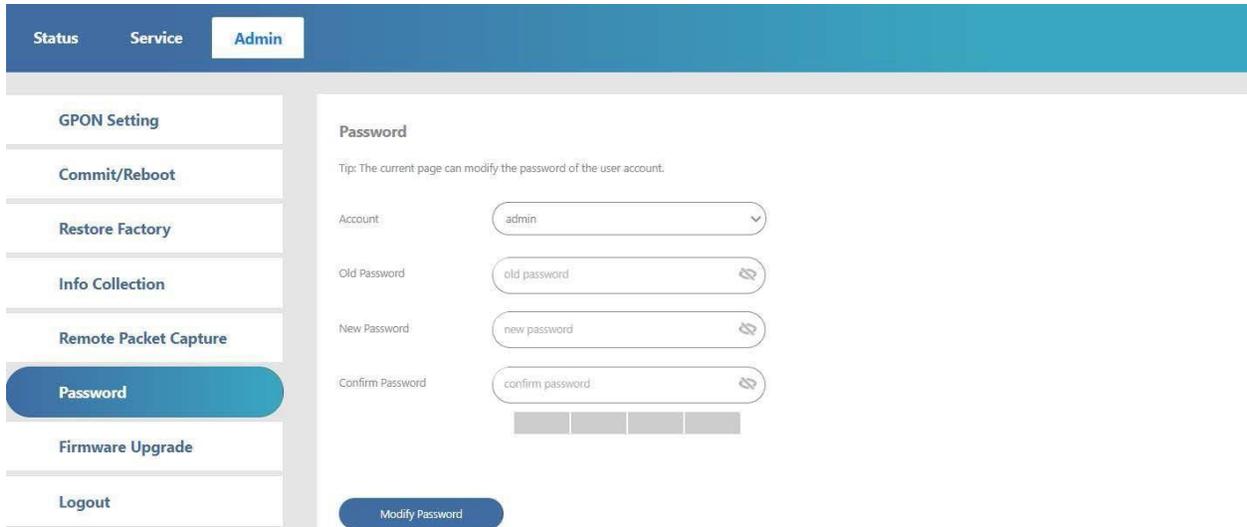
Figure 3.5.6

3.5.7 Firmware Upgrade

Press the "Choose File" button and select the firmware file to be upgraded, then press the "Upgrade" button, the device will be upgraded and you can also check the upgrade process.

Figure 3.5.7

3.5.8 Log Out

Press the "Logout" button and the user will logout this web page and return to the login page.

4. Safety

To ensure the optimum performance of the devices without damaging the equipment or endangering yourself and other users, please make sure to follow all safety precautions.

1. Please read the installation instructions in this Quick Start Guide thoroughly before you set up the devices!
2. Avoid using the devices in dusty or damp places and places where there is a risk of explosion.
3. Do not expose the devices to humidity (e.g., in a bathroom). Risk of electric shock!