EPON OLT Web User Manual

About Product

Product Name	Product Model	Product Software
EPON OLT	XE04/XE08/HE04/HE08/HE04L	epon_firmware_I_V3.0.8_Rel

Revision History

Version	Date	Editor	Description
V1.0	2018.06.05	Stephen.liu	First version for Web
V1.1	2018.08.08		Add some functions
V2.0	2019.04.29		Redesign Web and add some functions
V2.0.2	2019.05.27		Add loid & CTC3.0 support
V2.2.0	2019.07.18		Add link aggregation
V3.0.0	2019.05.05		
V3.0.1	2020.09.08	Lanbing	Adjustment document format and content

Content

1 OLT Login Setting.....1

1.1 Connect OLT with PC..... 1

1.2 Login WEB..... 2

1.3 WEB Home Page..... 3

2 Topology.....4

3 ONU Table..... 8

4 VLAN Configurations.....11

5 Advanced Setting.....13

5.1 Running Status..... 13

5.2 System Management..... 13

5.2.1 Device Management..... 13

5.2.2 Diagnose..... 14

5.2.3 Network Interface..... 14

5.2.4 Upgrade.....16

5.2.5 Time Setting.....17

5.2.6 Service.....17

5.2.7 Alarm..... 21

5.2.8 User Management.....22

5.3 PON Port..... 24

5.3.1 ONU Deny List.....24

5.3.2 Upstream Bandwidth..... 25

5.3.3 PON Setting..... 25

5.3.4 LOID List.....28

5.3.5 ONU Batch Upgrade.....29

5.3.6 Optical Diagnose..... 31

5.3.7 Batch Configuration.....32

5.4 ONU Device Management.....35

5.4.1 ONU Basic Info..... 35

5.4.2 ONU Port Config(Only support SFU).....38

5.4.3 ONU Multicast.....40

5.4.4 ONU Performance Statistics.....43

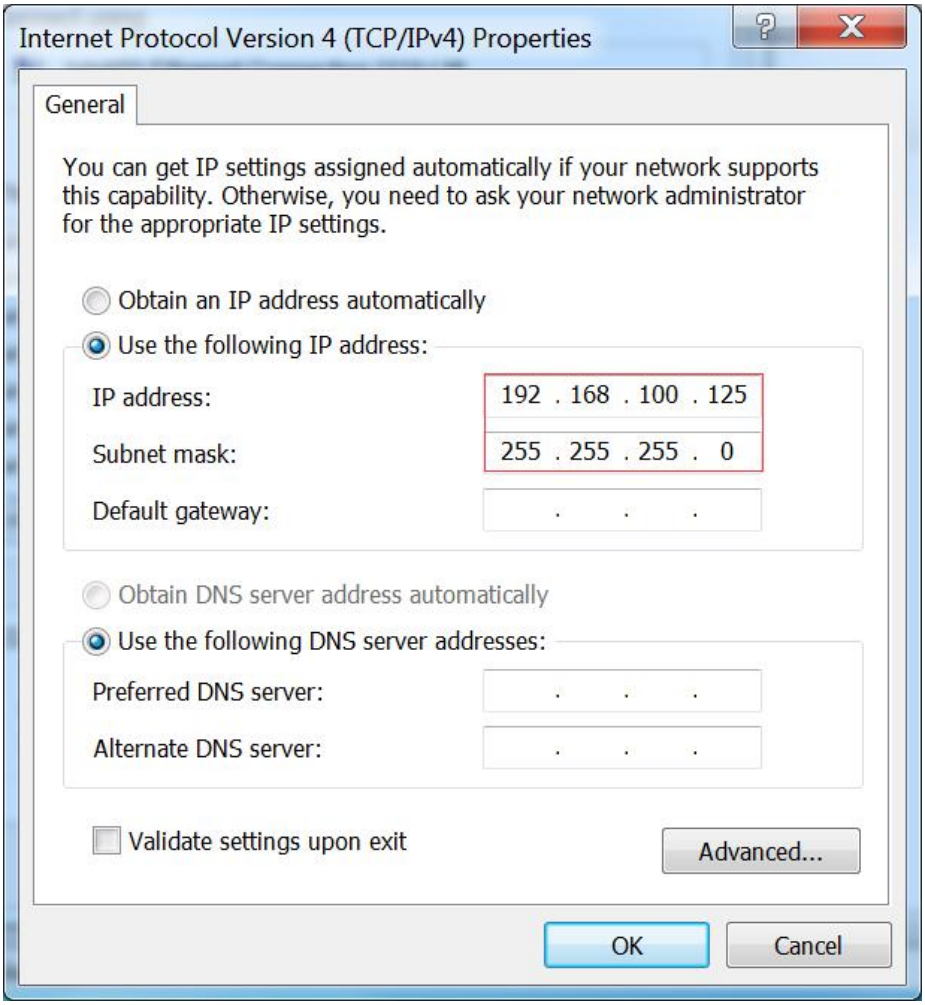
5.5 Port Management..... 45

5.5.1 Port Info....45
5.5.2 Performance....45
5.5.3 Port Config....46
5.5.4 Port VLAN Configuration....47
5.5.5 Loop Detection....49
5.5.6 Port Group....54
5.6 MAC Address Table....55
5.6.1 MAC Address Age Time....55
5.6.2 Add Static MAC Address....55
5.6.3 Add Blackhole MAC Address....56
5.6.4 Delete MAC Address....56
5.6.5 View MAC Address....57
5.7 Protocol....58
5.7.1 RSTP....58
5.7.2 IGMP....60
5.7.3 DHCP....68
5.7.4 MSTP....72
5.8 ACL/QOS....77
5.8.1 Time-range....77
5.8.2 ACL Management....79
5.8.3 Packet Filter....83
5.8.4 QOS....83
5.9 Route....85
5.9.1 Route Management....85
5.9.2 ARP Table....87
5.10 Link Aggregation....87
5.10.1 Create Link Aggregation....87
5.10.2 View Link Aggregation....89
5.10.3 Port Selection Criteria....89
5.10.4 Delete Link Aggregation....89
6 Shortcut....91
7 root....94

1 OLT Login Setting

1.1 Connect OLT with PC

Our company OLT default out-band management IP is **192.168.100.1/24**, and the in-band management IP is **192.168.99.1/24**. When connecting to the NMS port to manage OLT, Please set your PC IP to 192.168.100.X (X:1~254) . When connecting to the uplink port to manage OLT, Please set your PC IP to 192.168.99.X (X:1~254) . The following figure is an example of connecting the NMS port to configure the IP address:



After the setting is completed, you can ping to test connectivity, as shown below:

```
C:\Users\HSGQ001>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time=2ms TTL=64
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64
Reply from 192.168.100.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\HSGQ001>
```

1.2 Login WEB

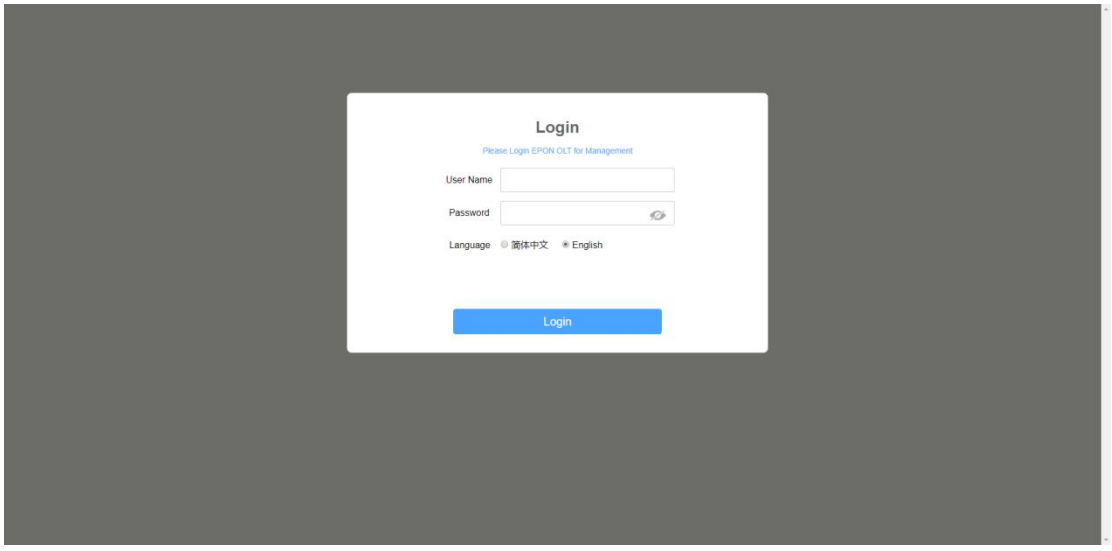
Please open the browser (now support firefox/chrome/IE 9 and up)

Input the OLT's management IP address

①192.168.100.1(Outbound IP address,connected to NMS port)

②192.168.99.1(Inbound IP address,connected to Uplink port)

Enter your user name and password, as shown below :



Note:

1. The default username **"root"** and password **"admin"** , the CLI is the same;
2. The same user can login to the WEB and the CLI at the same time;

3. The login timeout is 5mins, There's no any operations will be logout automatically after 5mins.

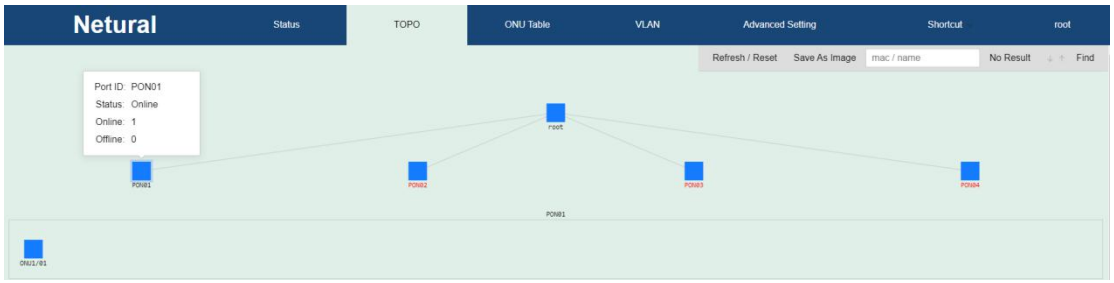
1.3 WEB Home Page

After logging in to the WEB, enter "**status** " option on the home page, and you can view the status information of the PON port and GE port . The PON port shows how many ONUs are registered, how many ONUs are online, and how many ONUs are offline; the uplink port shows the port status and link connection status. As shown below:

2 Topology

Enter the OLT WEB, click “**TOPO**” option, this page can overview the ONUs connected to the OLT, where the red font indicates the offline status, as shown below:

1. Move the mouse cursor to the PON icon,then it will automatically display the online state of the port,how many onus are online and how many onus are offline. As shown below:



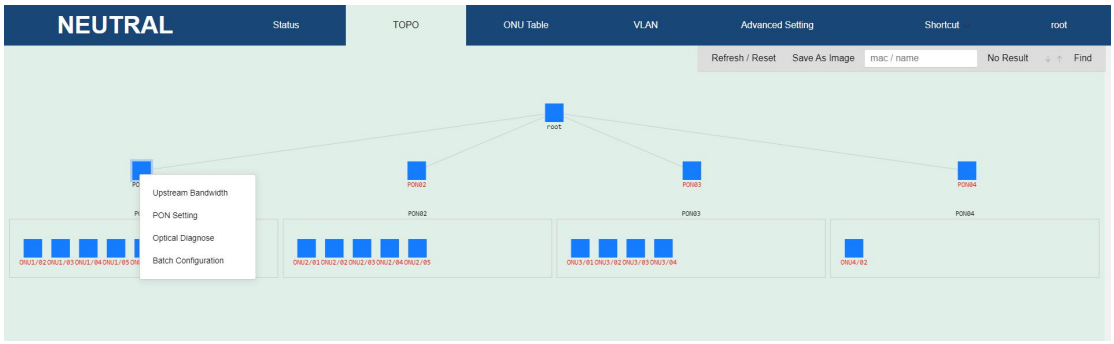
2. Right click the icon of PON port,you can quickly access to PON management including the following functions:

① Uplink bandwidth configuration

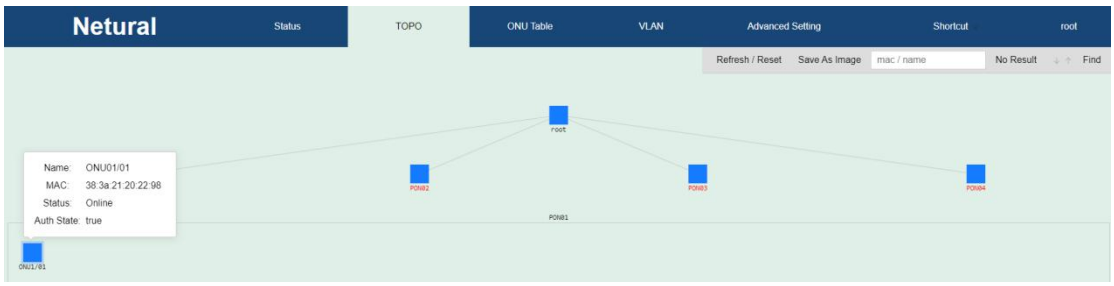
② PON settings

③ PON port optical diagnosis

④ Batch configuration



3. Move the mouse cursor to the ONU icon,then it will automatically display the name,MAC address,online state,authenticating state of the ONU. As shown below:

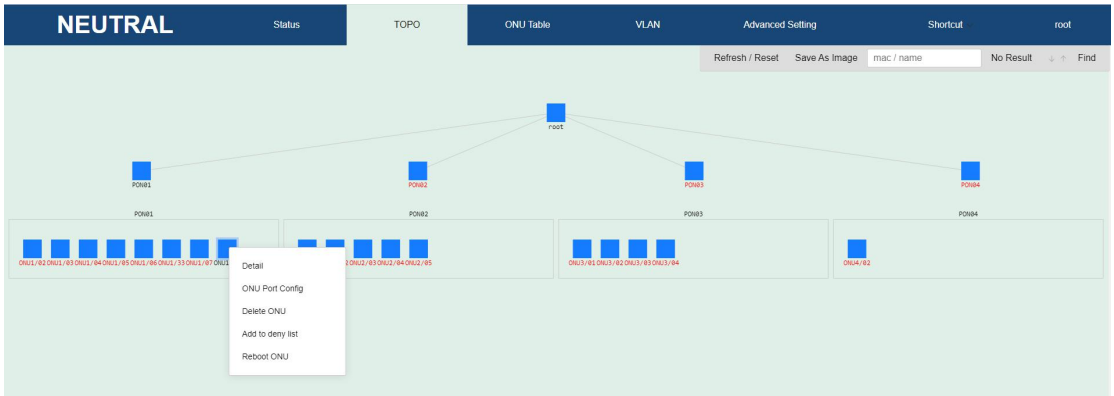


4. Right click the icon of ONU,you can quickly access to ONU management including the following functions:

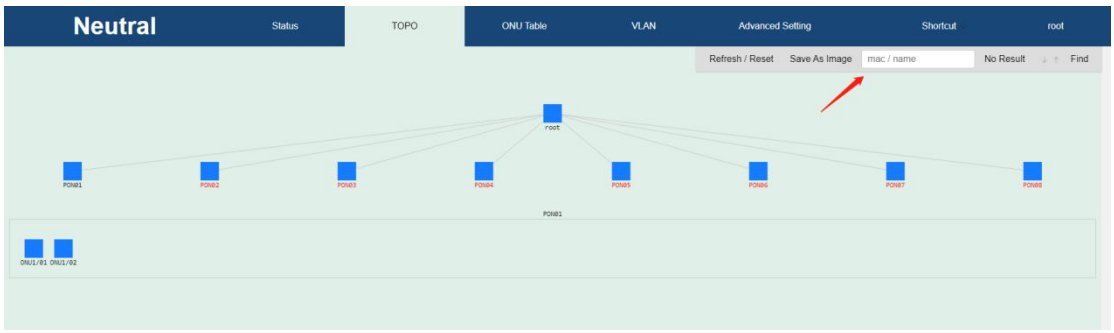
① Basic information

② Port configuration

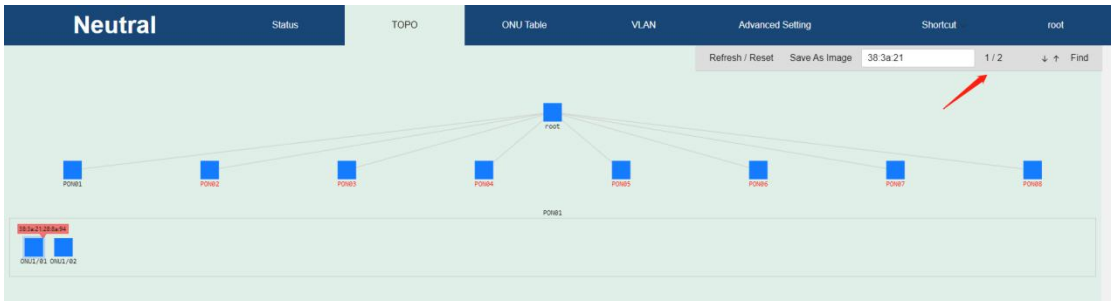
③ Delete ONU/Reset ONU/Add ONU to deny list

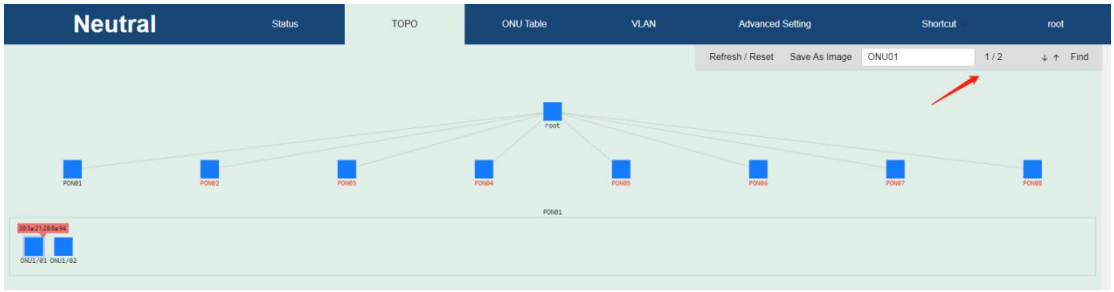


5. In the gray box in the upper right corner of the interface, you can quickly find the corresponding ONU by searching the ONU name or the ONU MAC address. As shown below:



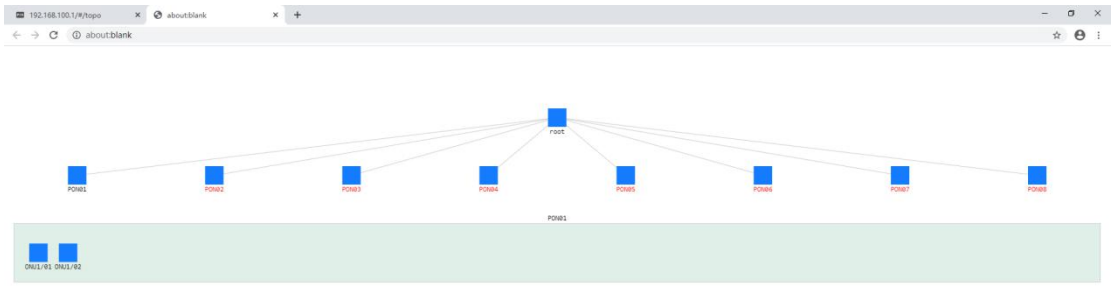
①You can input the MAC address or name of partial or full length at will, and the number of search results is shown as the following figure. Click the small black arrow up and down to quickly view the status of each ONU, and the corresponding ONU icon will blink five times automatically.





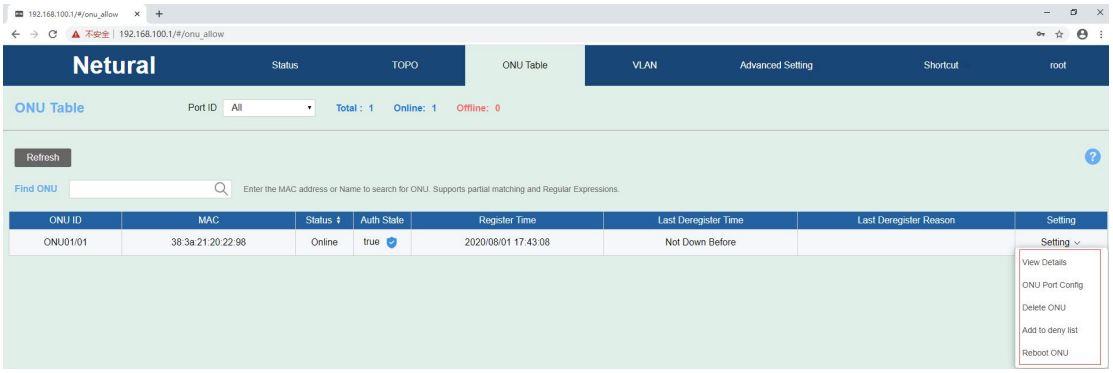
②The found ONU icon is surrounded by a layer of light blue. Click "**Refresh/Reset**" to reset the icon status.

③Click "**Save As Image**" to display the current topology status on the new label page of the browser. (the original topology interface cannot be operated by right clicking)

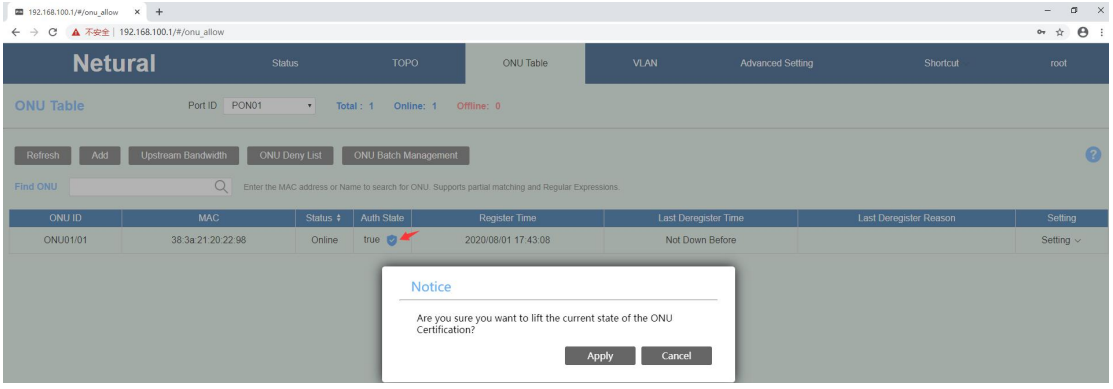

192.168.100.1/#/topo
about:blank
about:blank
root
PON01
PON02
PON03
PON04
PON05
PON06
PON07
PON08
PON01
ONU1/01
ONU1/02

3 ONU Table

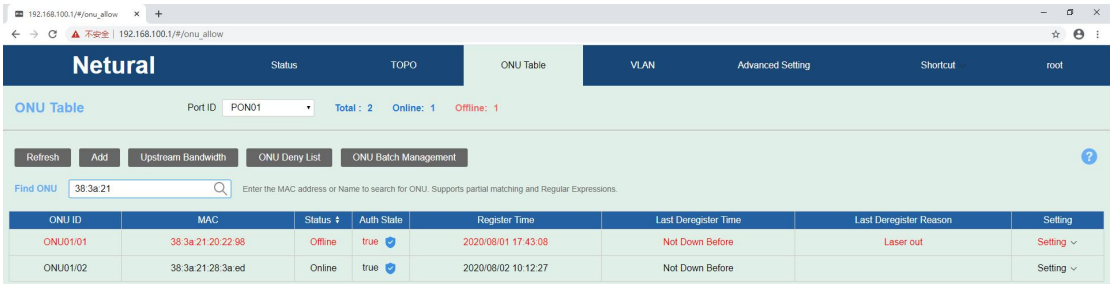
Enter the OLT WEB, click “**ONU Table**” option, you can view all ONU list information connected to the OLT in this page , the red font shows the offline ONU. Move the mouse to the "**Setting**" option to quickly access Advanced Setting -> ONU Device-> ONU Basic Info / ONU Port Config , Delete ONU, Add to deny list and Reboot ONU. As shown below:



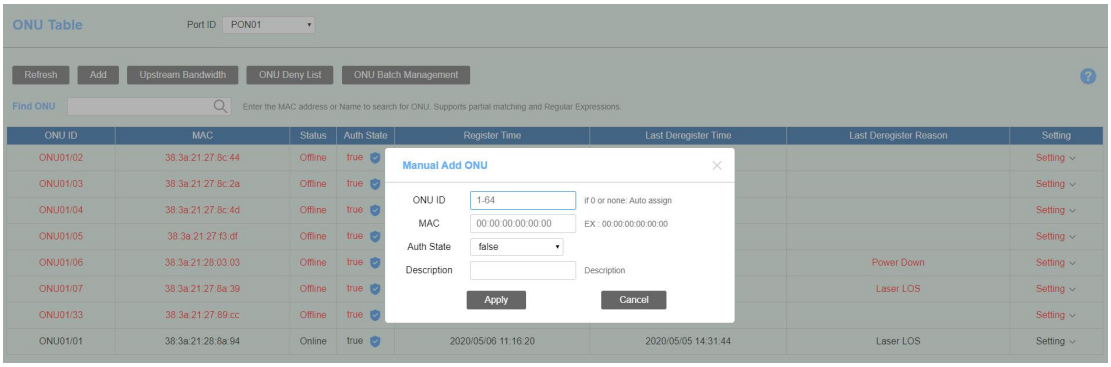
Left-click the blue icon next to the "**Auth State**" of the ONU, you can modify the current ONU authentication status, including "**true**" and "**false**". In generally, the normal registration needs to be set to true. As shown below:



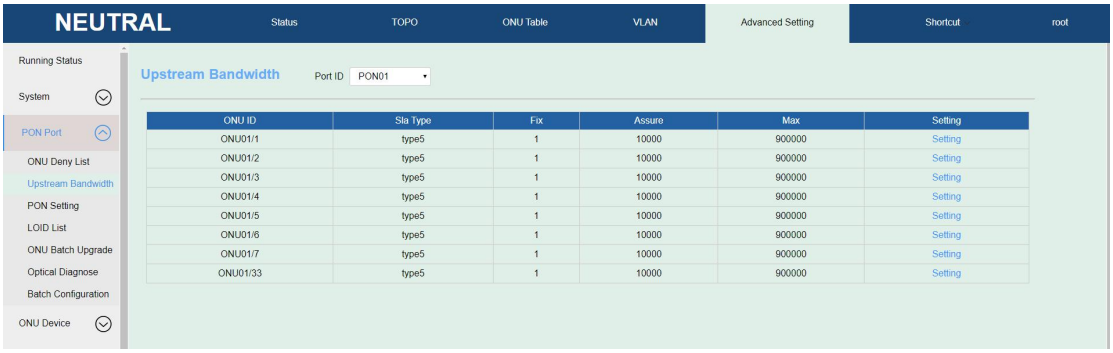
1. First choosing “**Port ID**”, then you can view all ONUs connected to the corresponding PON port. You can also enter the MAC address or name in the Find ONU option box to find a specific ONU, click the "Refresh" button to restore, as shown below:



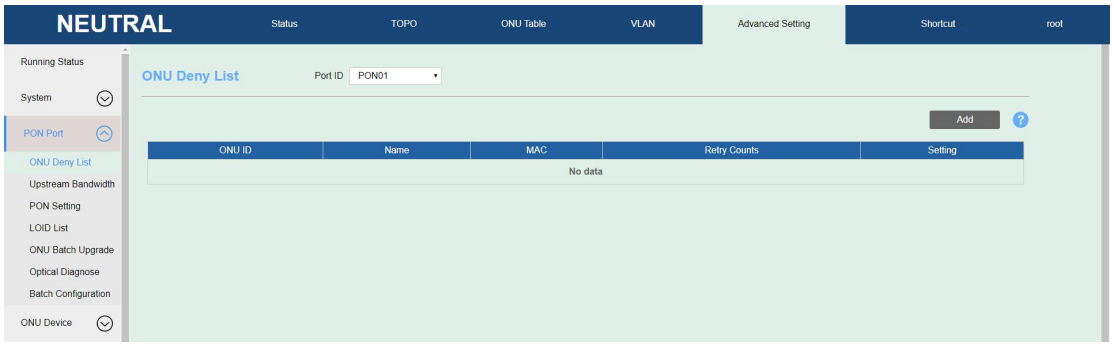
2. Choose **Port ID** -> **ADD,** You can specify the ONU ID or onu id is 0 will automatically distribution the ONU ID. As shown below:



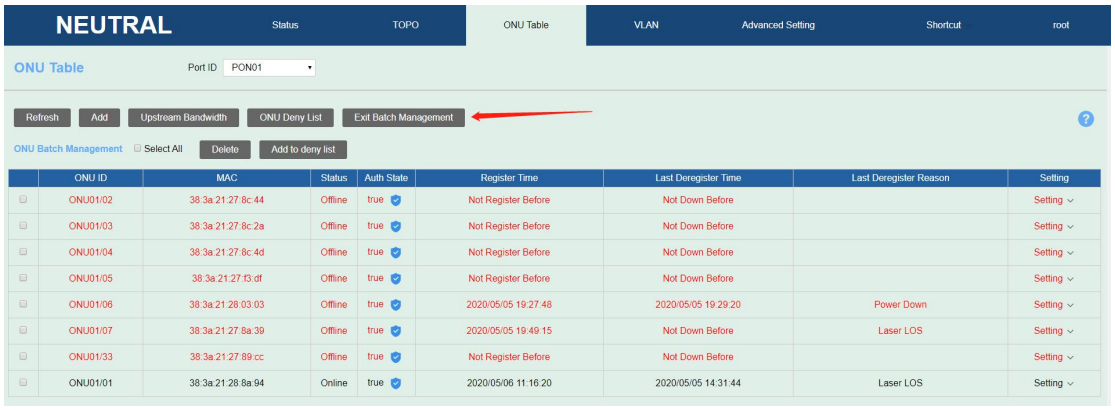
3. Choose **Port ID** -> **Upstream Bandwidth,** you can quickly enter ONU Upstream bandwidth configuration page. As shown below:



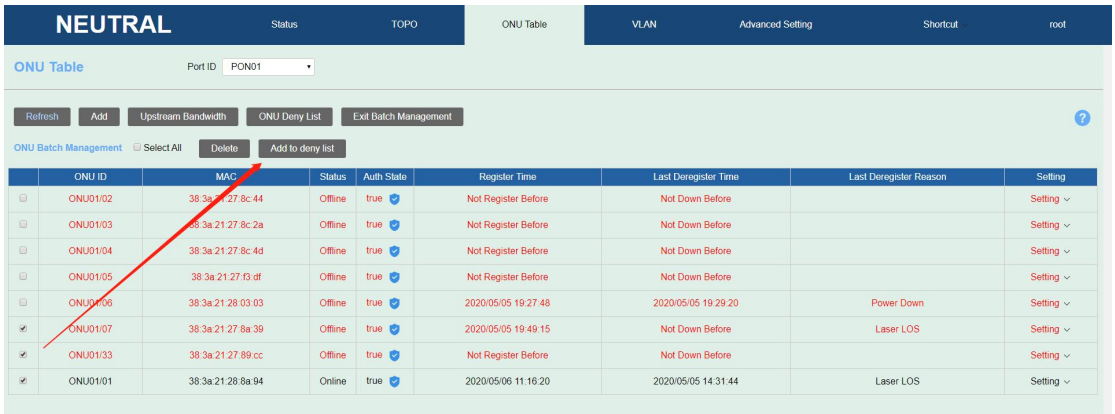
4. Choose **Port ID** -> **ONU Deny List,** you can quickly enter ONU Deny List page. As shown below:



5. Choose **Port ID -> ONU Batch Management ,** you can manage the batch of ONUs, including delete and add to deny list. As shown below:



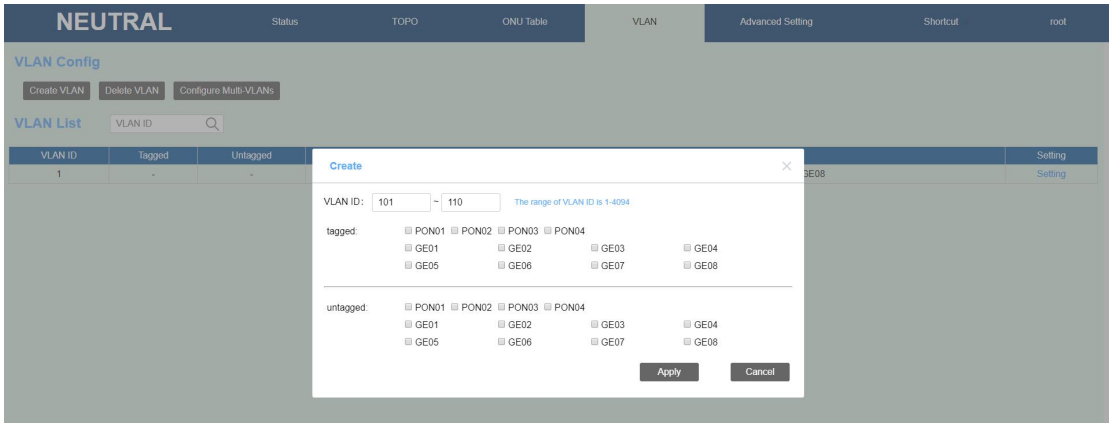
Choose multiple ONUs to operate:

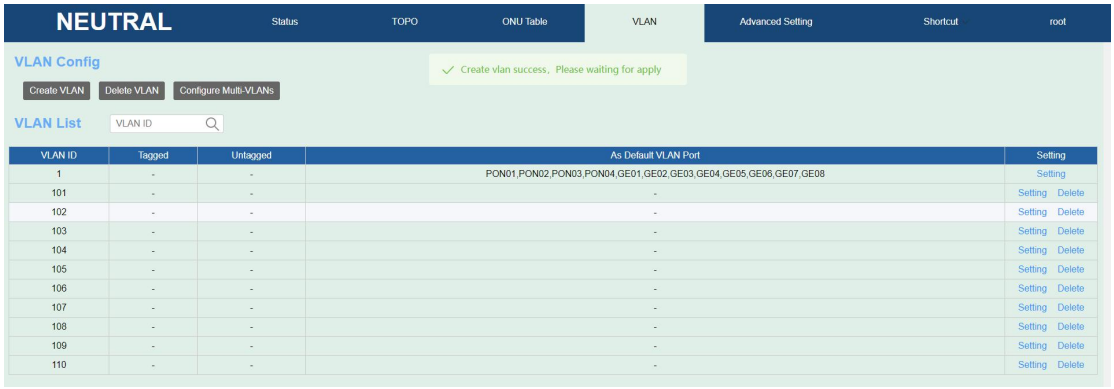


4 VLAN Configurations

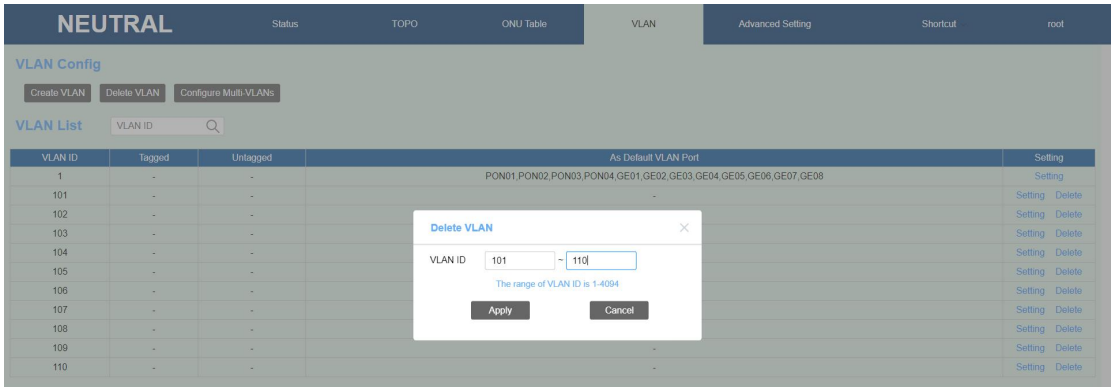
Enter the OLT WEB, click “**VLAN**” option, you can view the member ports of the created VLAN list, including tagged ports, untagged ports, and default VLAN ports. As shown below:

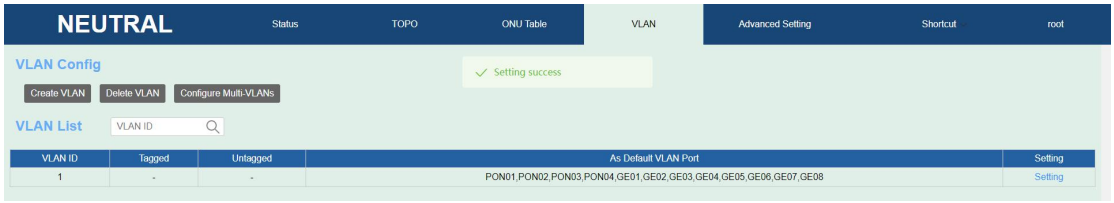
1. Choose **VLAN** -> **Create VLAN**, you enter VLAN ID and select both tagged port and untagged port. If you want to create a VLAN, just enter the same VLAN ID; if you want to create multiple consecutive VLANs, you can enter a valid VLAN ID range. As shown below:





2. Choose **VLAN** -> **Delete VLAN**, you can delete one VLAN or a valid VLAN ID range. As shown below:

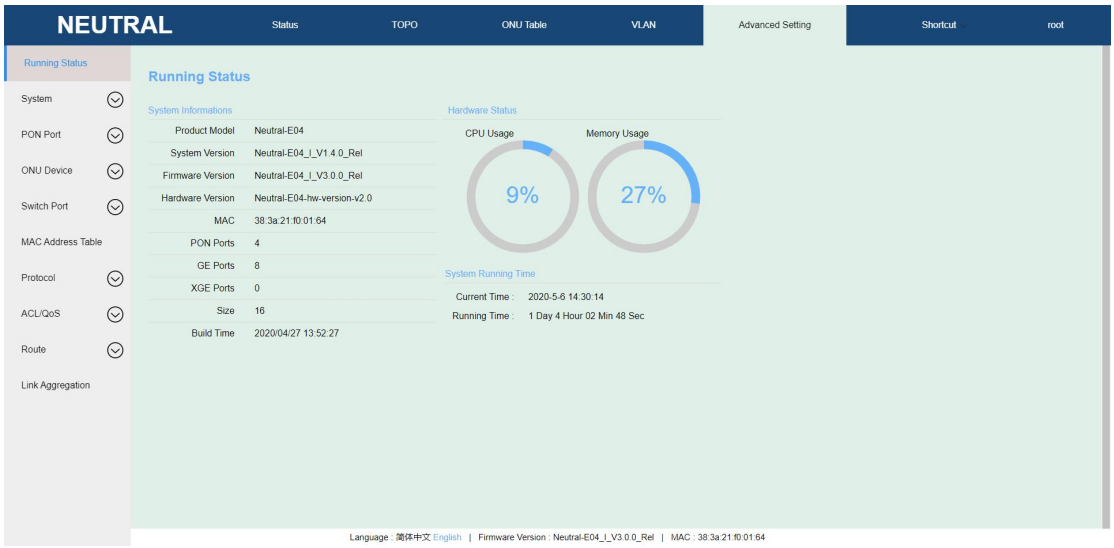




5 Advanced Setting

5.1 Running Status

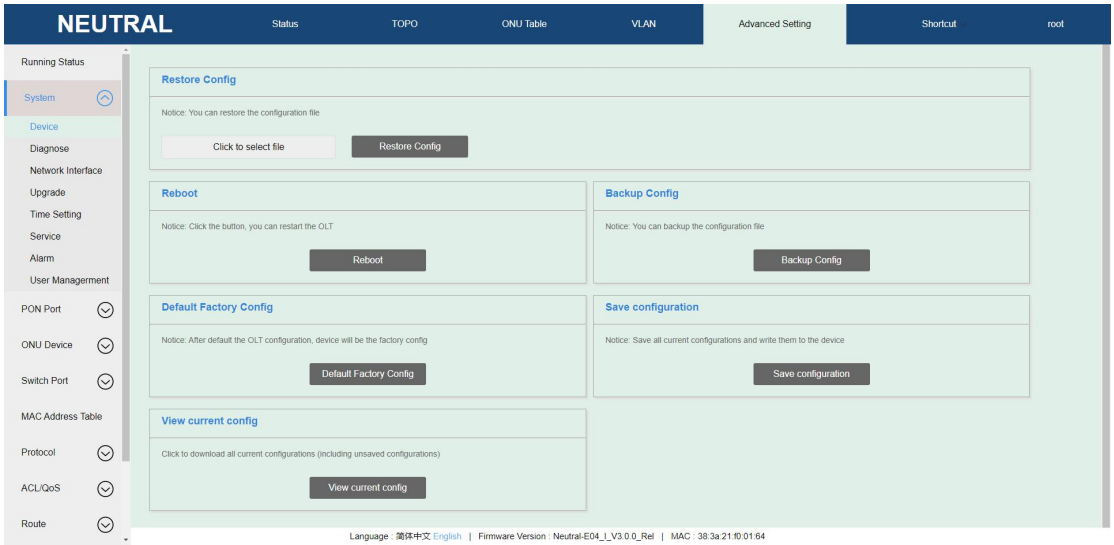
Choose **Advanced Setting** -> **Running Status**, you can view OLT system information, hardware status and system running time, as shown below:



5.2 System Management

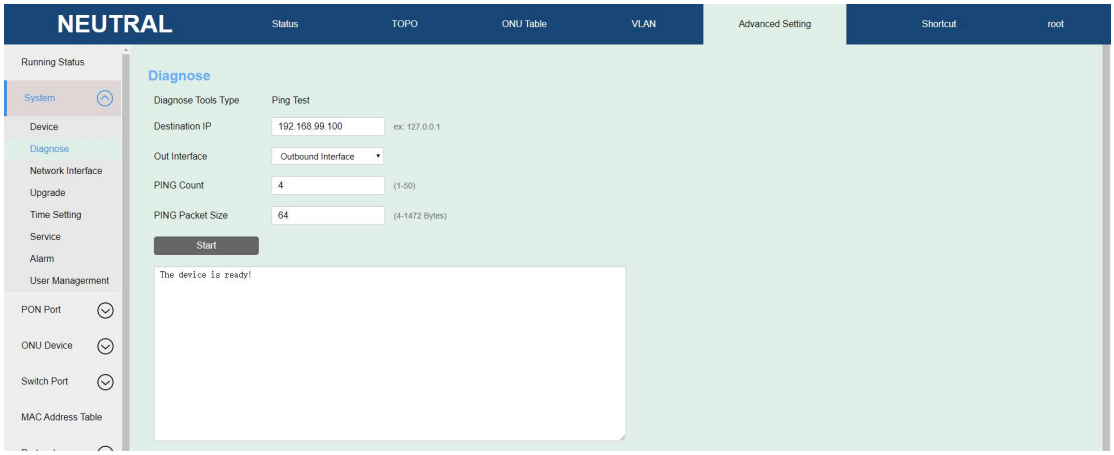
5.2.1 Device Management

Choose **Advanced Setting** -> **System** -> **Device**. On this page, you can view, save, backup and restore the OLT configuration, restart and initialize the OLT. As shown below:



5.2.2 Diagnose

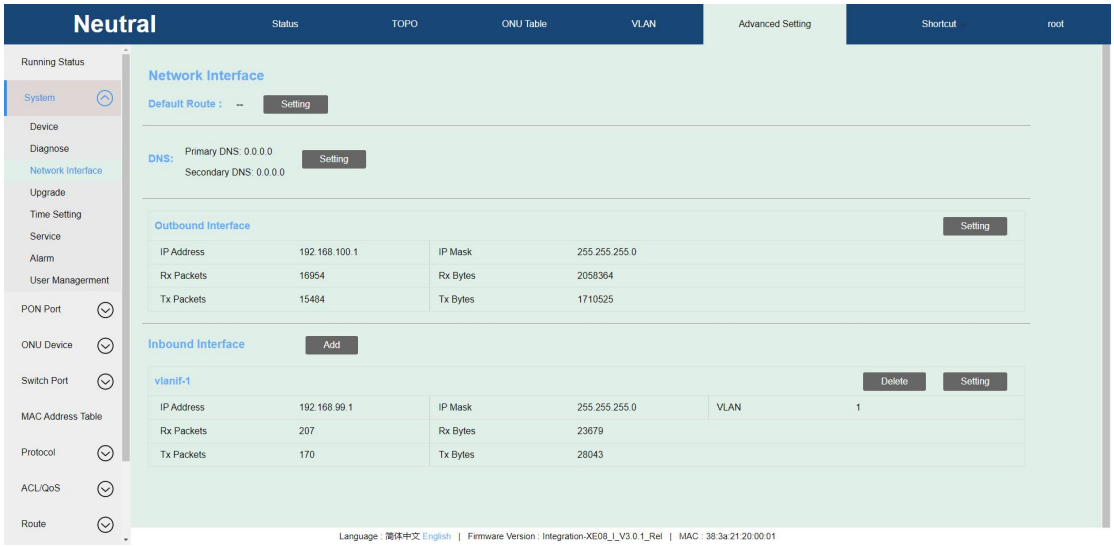
Choose **Advanced Setting** -> **System** -> **Diagnose**. On this page, you can ping diagnosis and check the link connection. As shown below:



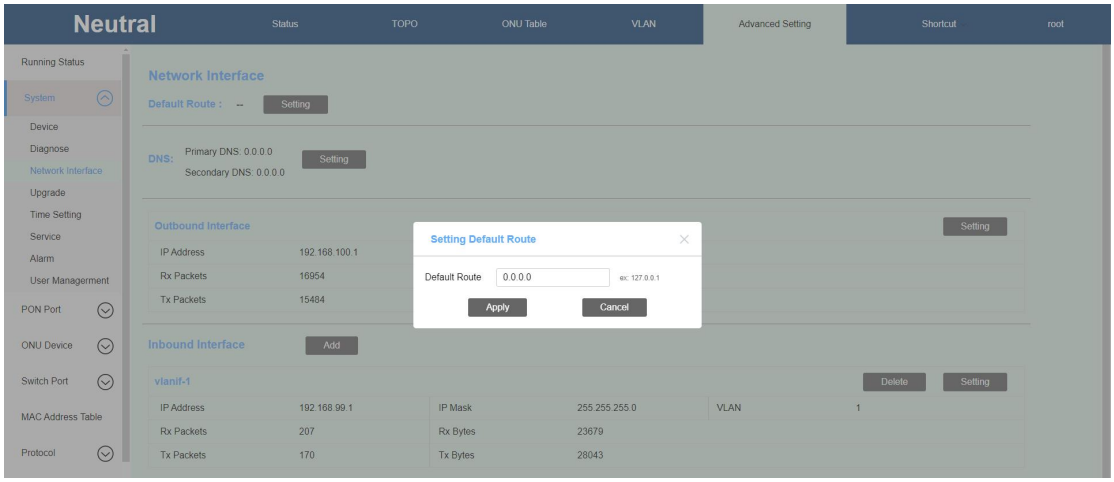
Note: Support ping domain name

5.2.3 Network Interface

Choose **Advanced Setting** -> **System** -> **Network Interface**. On this page, you can configure management port network parameters, including default route, DNS, in-band and out-of-band management interfaces. As shown below:

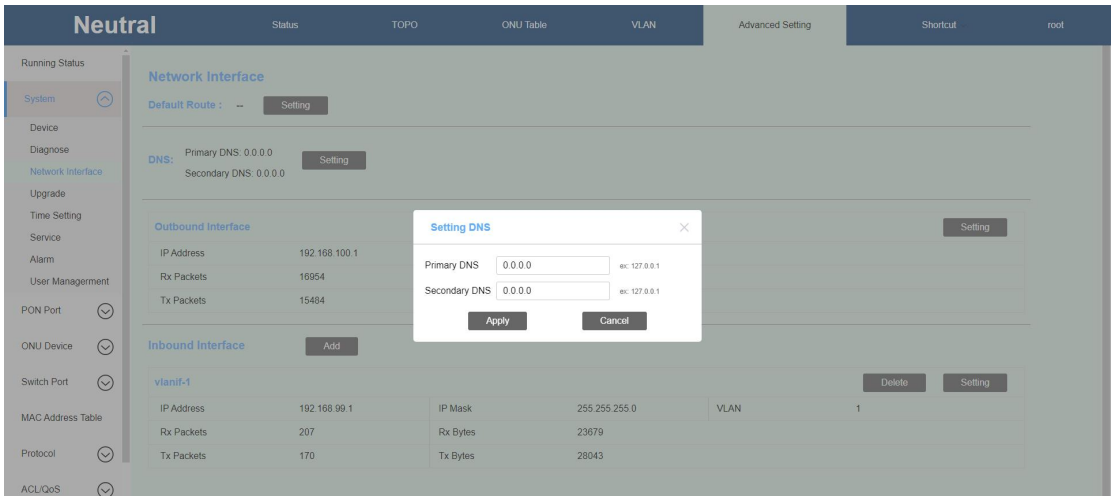


1. Configure default route

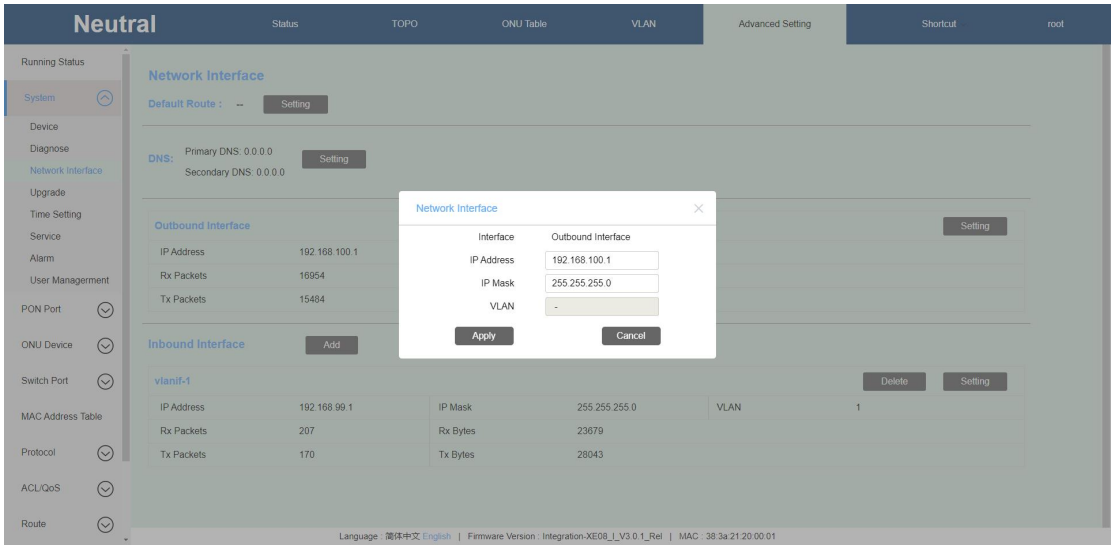


Note: It must exist the same network segment out-band and in-band management IP address.

2. Configure DNS

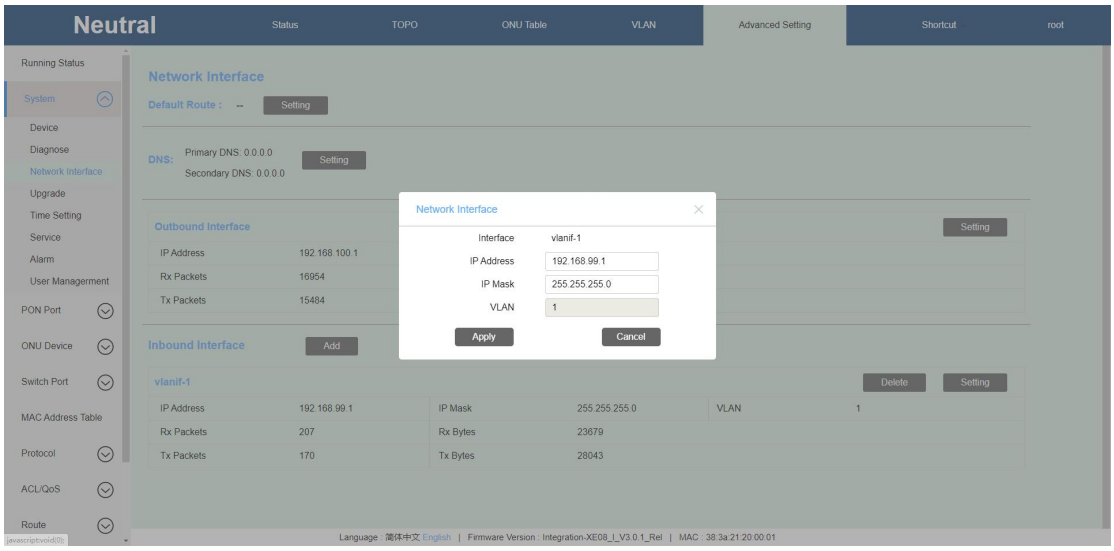


3. Configure out-band interface IP address



Note: Out-band management IP only can be modified, not added and deleted.

4. Add in-band interface IP address:



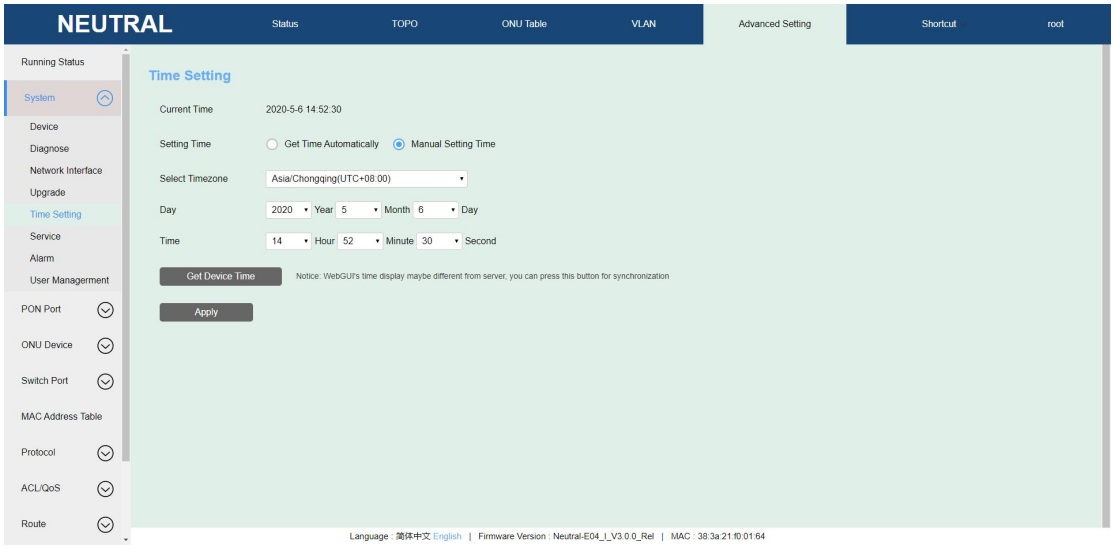
Note: Before you add it, you need create the corresponding vlan id.

5.2.4 Upgrade

Choose **Advanced Setting** -> **System** -> **Upgrade**. On this page, you can upgrade device Firmware(.img file), System(.img file) and Full Version(.zip). As shown below:

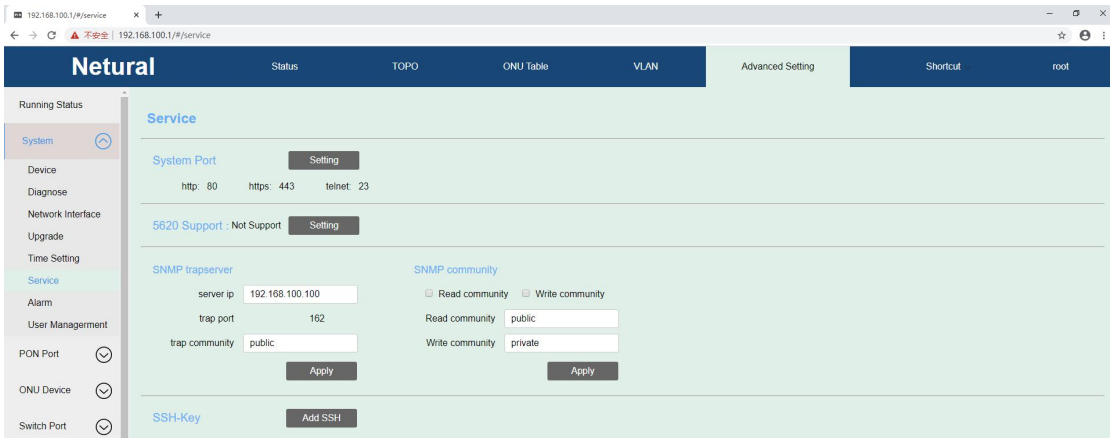
5.2.5 Time Setting

Choose **Advanced Setting** -> **System** -> **Time Setting** On this page, you can configure the OLT system time, including automatically get time and manually set time, as shown below:

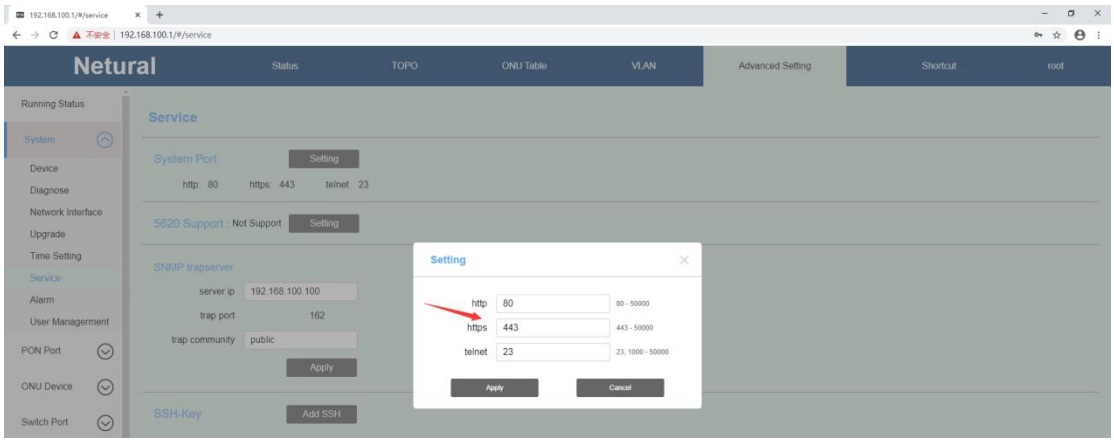


5.2.6 Service

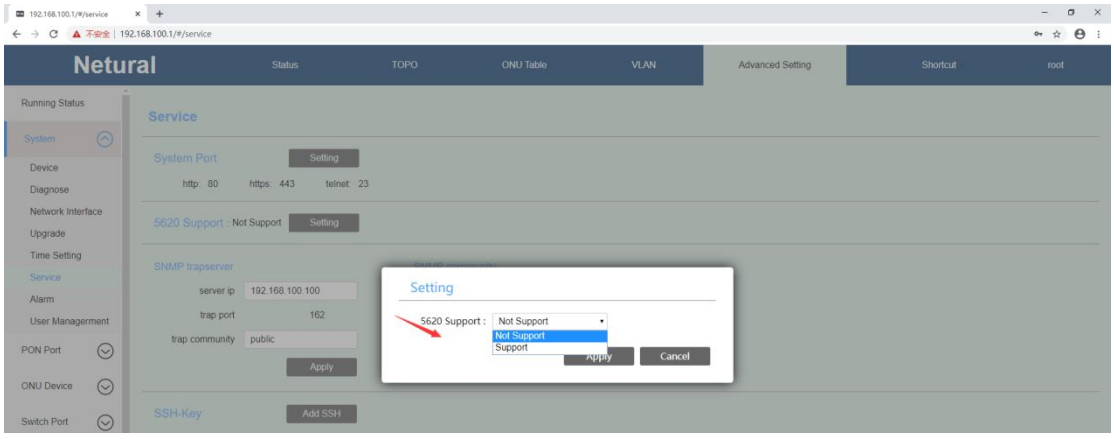
Choose **Advanced Setting** -> **System** -> **Service** On this page, you can configure system port , turning on or off 5620 function, snmp trap server, snmp community and SSH-Key. As shown below:



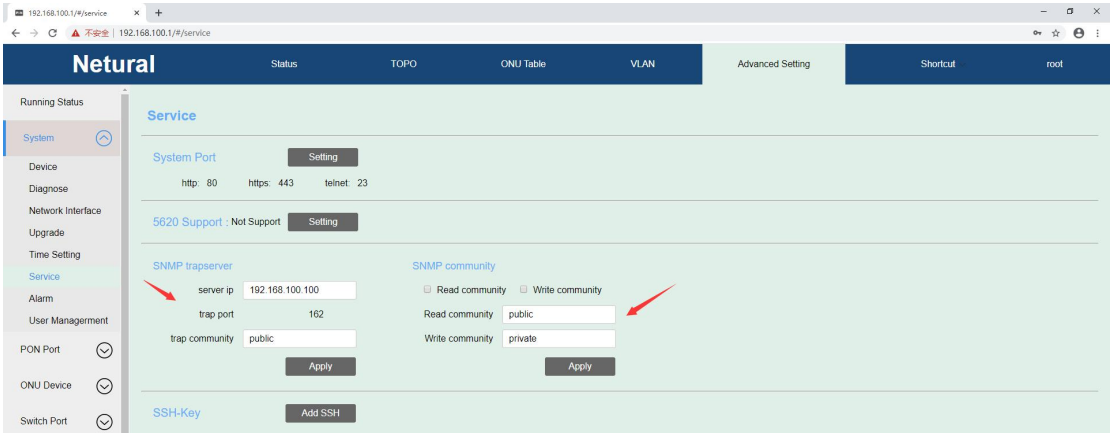
1. Configure the system port. This device supports modifying the default port number of the http/https/telnet services, as shown below:



2. Configure 5620 support. This function is developed for compatibility with Huawei ONU. When there is a problem with Huawei ONU, you can try to configure 5620 as "**Support**" , as shown below:



3. Configure SNMP parameters, including SNMP trap server parameters and read-write community parameters. The default trap server IP is 192.168.100.100, and you can modify it according to your own needs. After the parameters is completed, click the "**Apply**" button, as shown below:

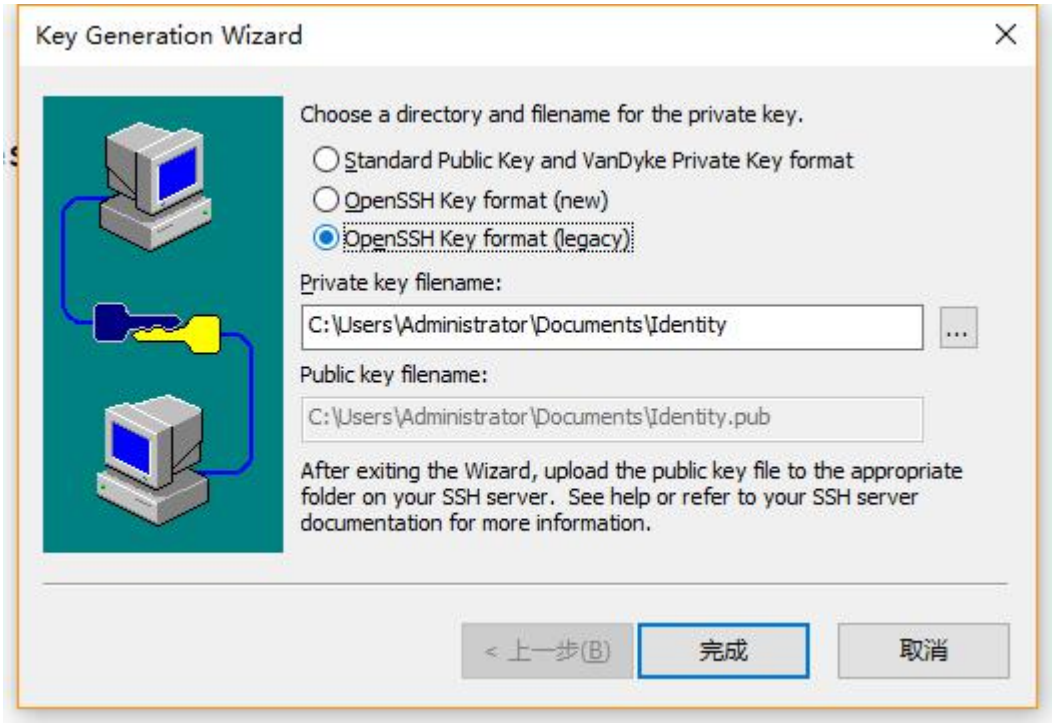


4. Configure SSH-Key for higher-level connections. You can log in to the CLI by SSH. The specific steps are as follows:

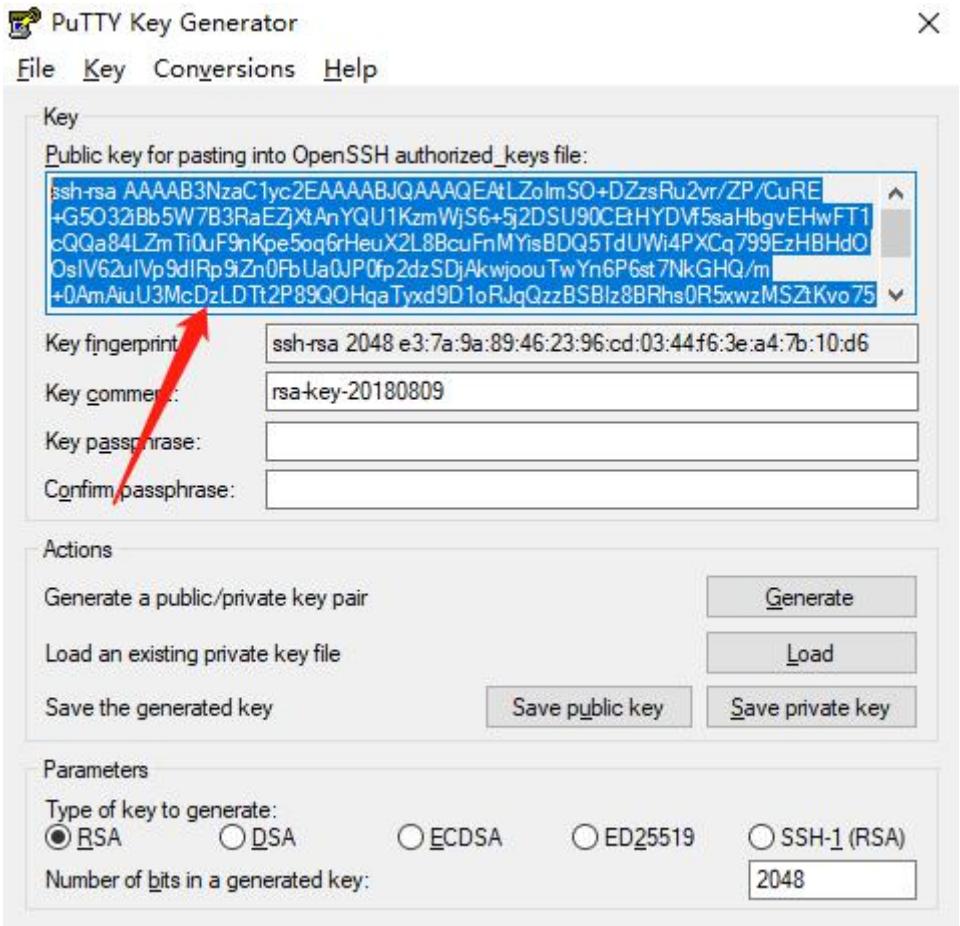
First, you need to add a public key to server.

Note: you need create a OPENSSH format public key, its type need by legacy,key type RSA.

Secure CRT like this:



Putty gen:



① Now, you need add the public key to OLT

② After done

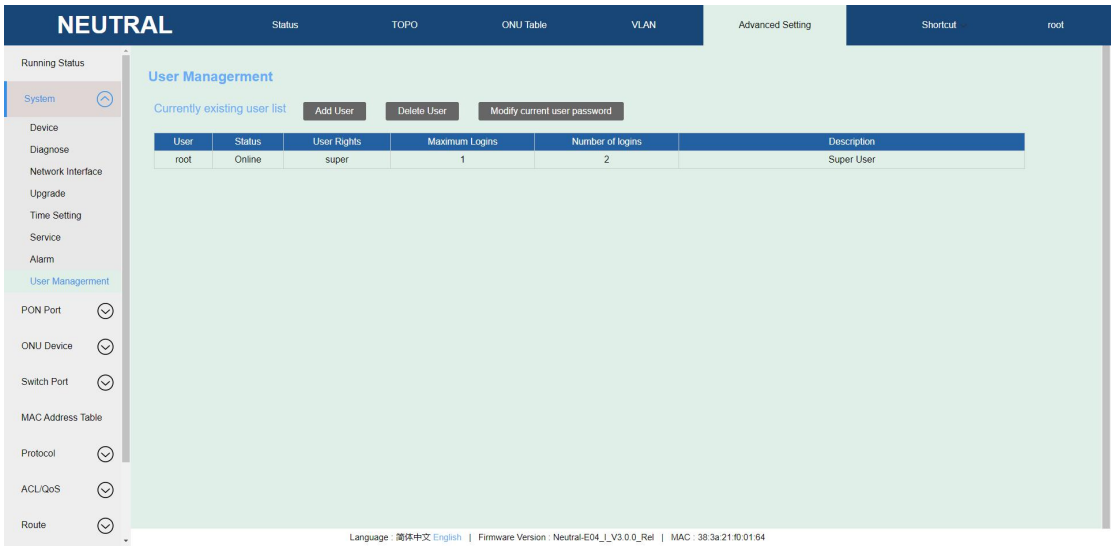
you can enter the username and password to login, it will be done.

5.2.7 Alarm

Choose **Advanced Setting** -> **System** -> **Alarm** On this page, you can view and download alarm information, enable and disable log record and download log. As shown below:

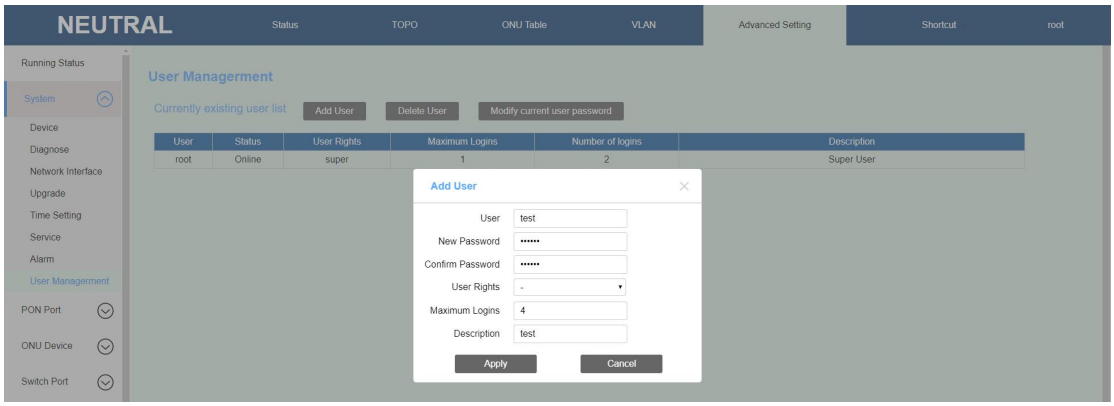
5.2.8 User Management

Choose **Advanced Setting** -> **System** -> **User Management** On this page, you can add, delete users, and modify user passwords, as shown below:

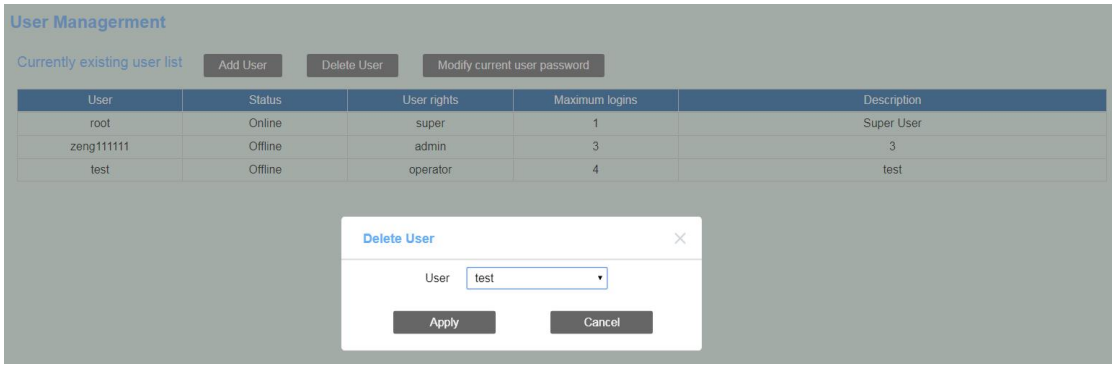


In user management menu, You can Add/Delete and modify user password

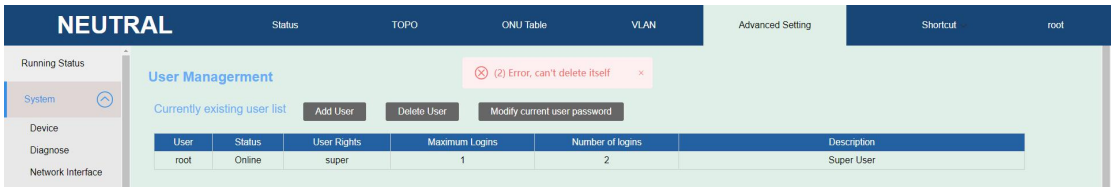
1. Add user



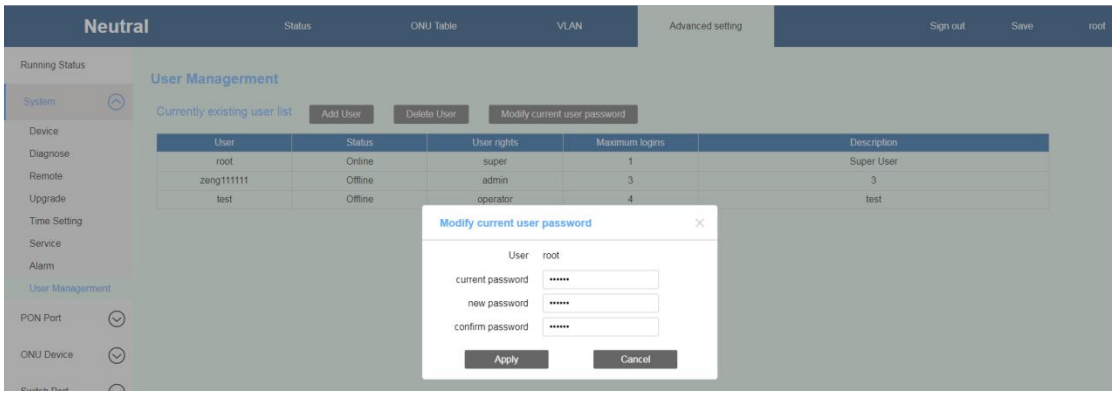
2. Add user



Note: The supper use can’t be deleted.



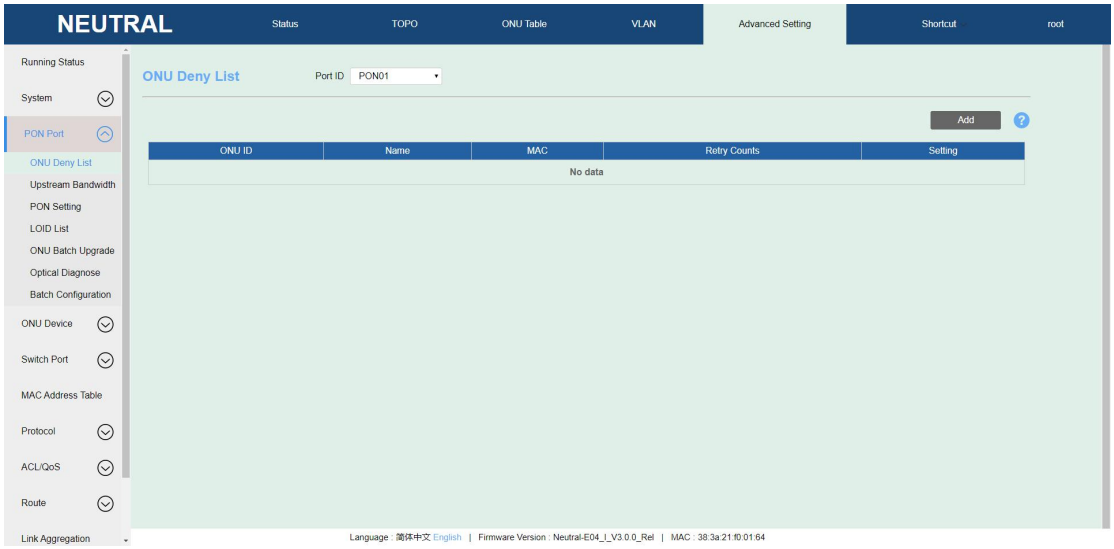
3. Modify user password, only can change your current login user password.



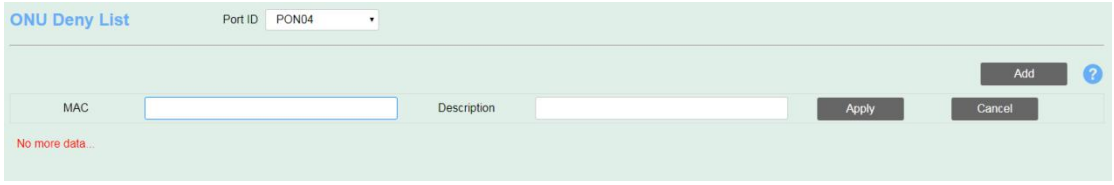
5.3 PON Port

5.3.1 ONU Deny List

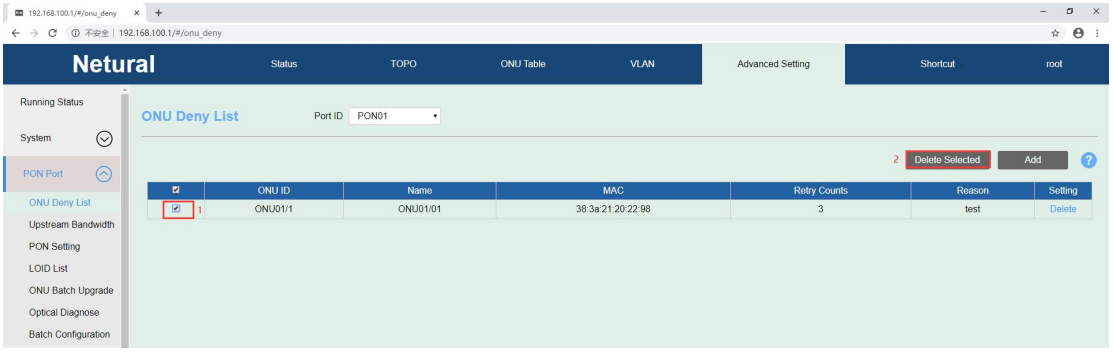
Select **Advanced Setting** -> **PON Port** -> **ONU Deny List**, enter this page, select the corresponding "**PON Port ID**", you can view the ONU deny list under the current PON port, as shown below:



1. Add ONU to deny list. Click "**Add**" button, enter ONU mac, as shown below:

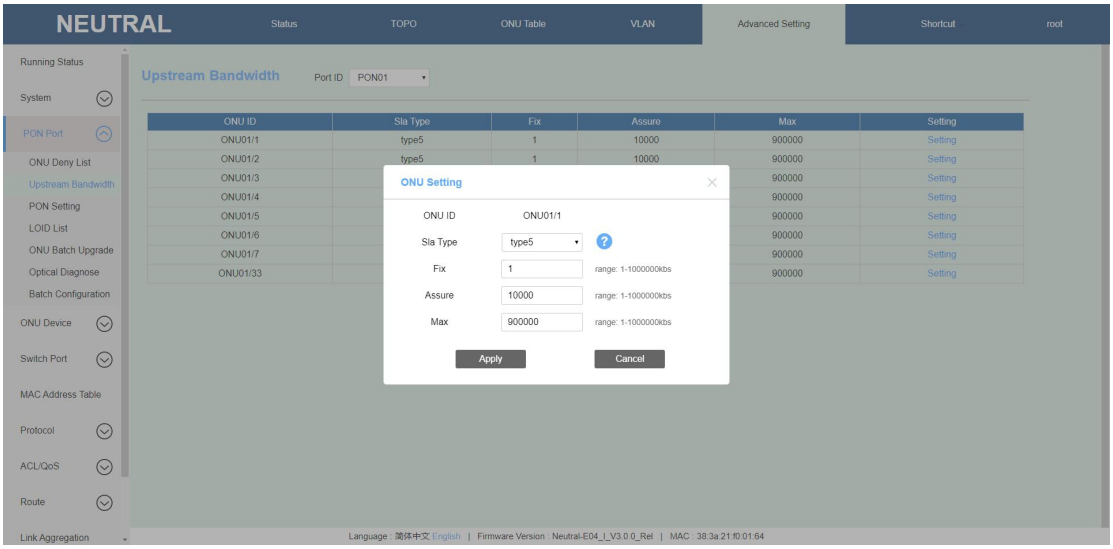


2. Delete ONU from deny list. First select ONU needed to be deleted, then click "**Delete Selected**", as shown below:



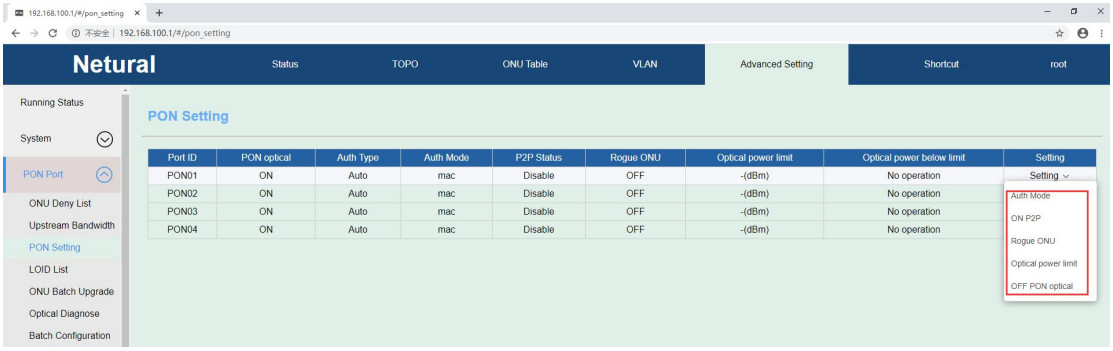
5.3.2 Upstream Bandwidth

Choose **Advanced Setting** -> **PON Port** -> **Upstream Bandwidth**, enter this page to configure ONU upstream bandwidth allocation rules, including 5 types, type1 (Fix bandwidth), type2 (Assure bandwidth), type3 (Assure bandwidth + Max bandwidth) , Type4 (Max bandwidth), type5 (Fixed bandwidth + Assure bandwidth + Max bandwidth), as shown below:



5.3.3 PON Setting

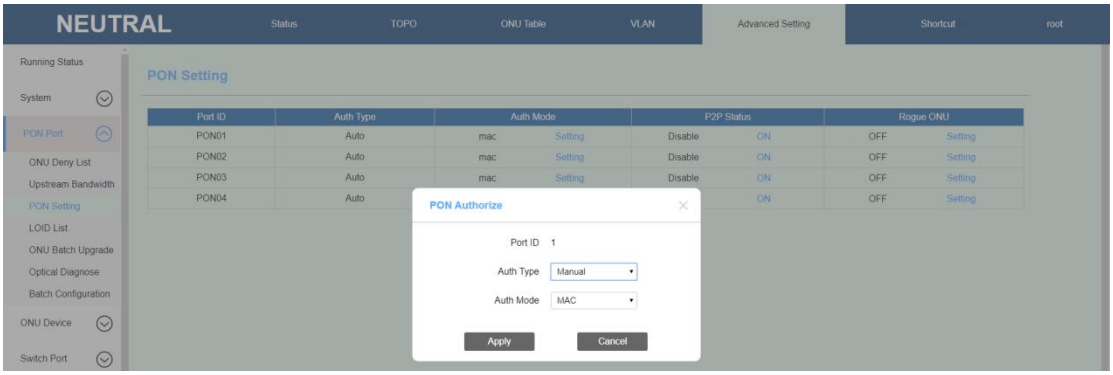
Choose **Advanced Setting** -> **PON Port** -> **PON Setting**, enter this page to set the pon port auth type, P2P function, rogue ONU detection function, optical limit power, and turning off and on the PON port. As shown below:



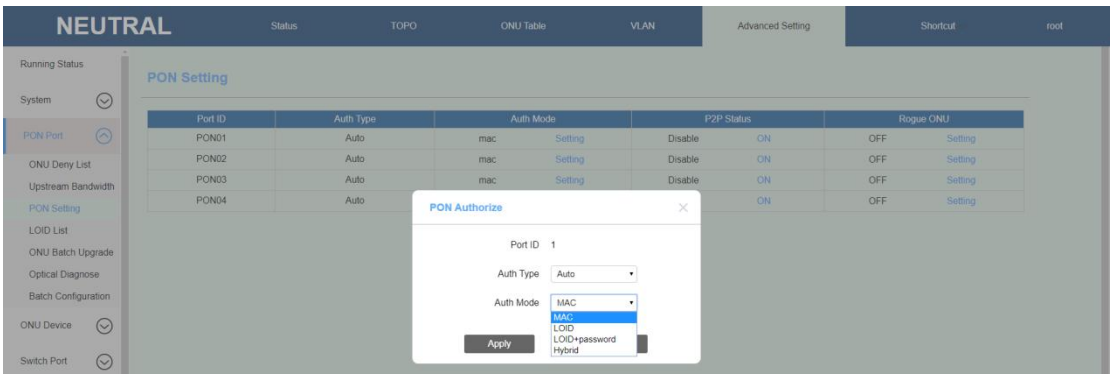
5.3.3.1 Auth Mode

Enter the PON setting page, move the mouse to the corresponding pon port "**Setting**" option, and select "**Auth Mode**" to set. Auth type includes “auto”and “manual” and auth modes include mac/loid/loid+password/hybrid, which can be set according to the actual application. As shown below:

Example 1: Set auth type to manual



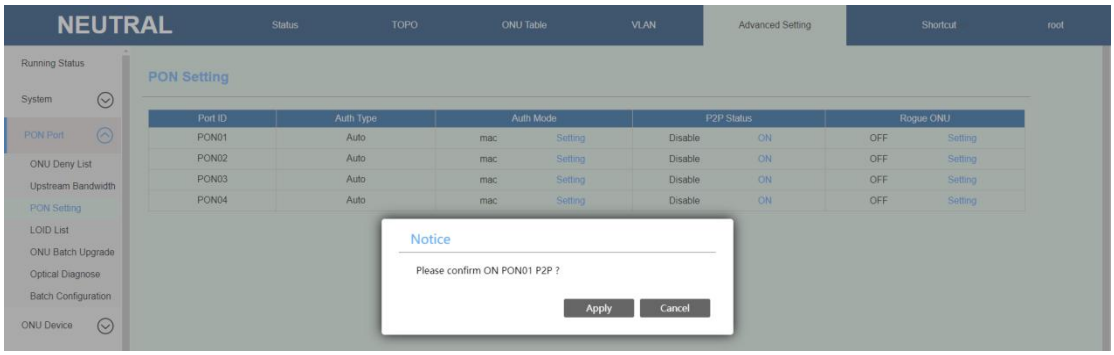
Example 2: Set auth mode to MAC



5.3.3.2 P2P

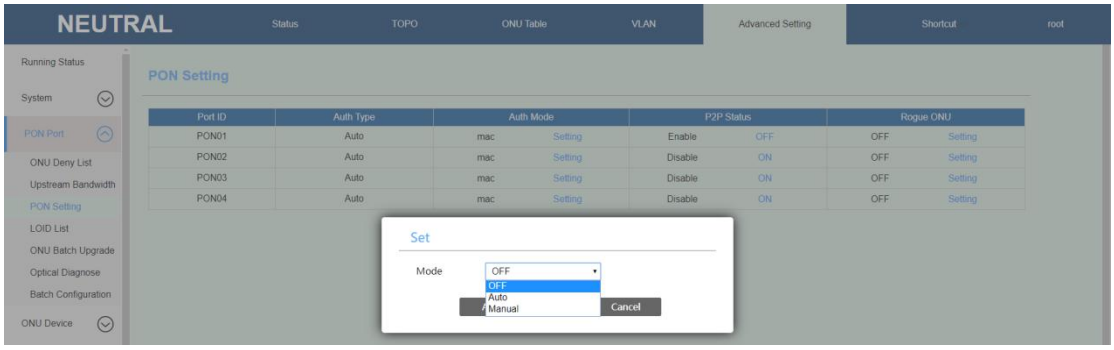
Enter the PON setting page, move the mouse to the corresponding pon port "**Setting**" option, and select "**ON/OFF P2P**" to set. The function is default off status. As shown below:

For example: Set P2P Status Enable



5.3.3.3 Rogue ONU detection

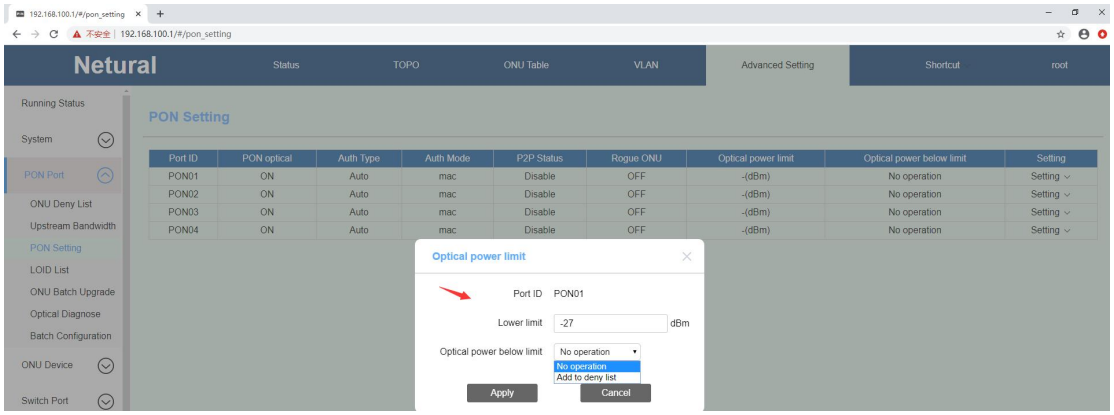
Enter the PON setting page, move the mouse to the corresponding pon port "**Setting**" option, and select "**Rogue ONU**" to set. Detect whether there is rogue ONU under PON port. Default status is off. As shown below:



5.3.3.4 Optical Power Limit

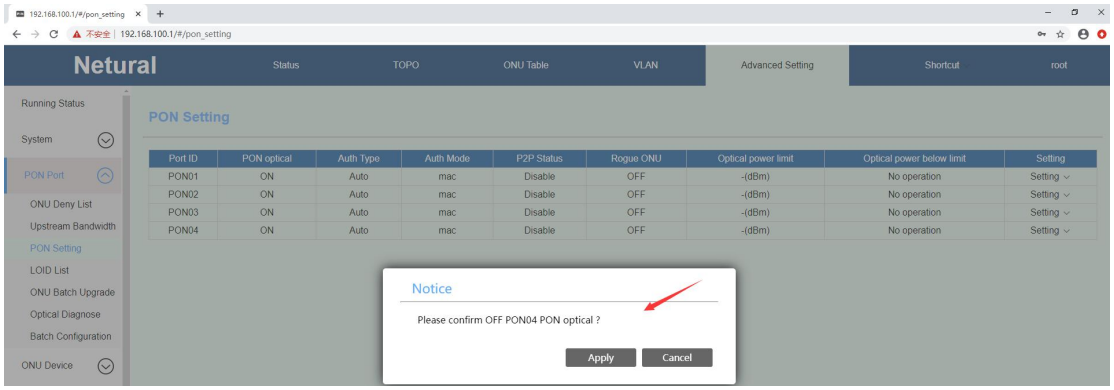
Enter the PON setting page, move the mouse to the corresponding pon port "**Setting**" option, and select "**Optical power limit**". This function can control the ONU to go online

by configuring the lower limit of the optical power. When the ONU power is lower than the configured threshold, the ONU can be added to the deny list. It is not configured by default and needs to be configured manually. As shown below:



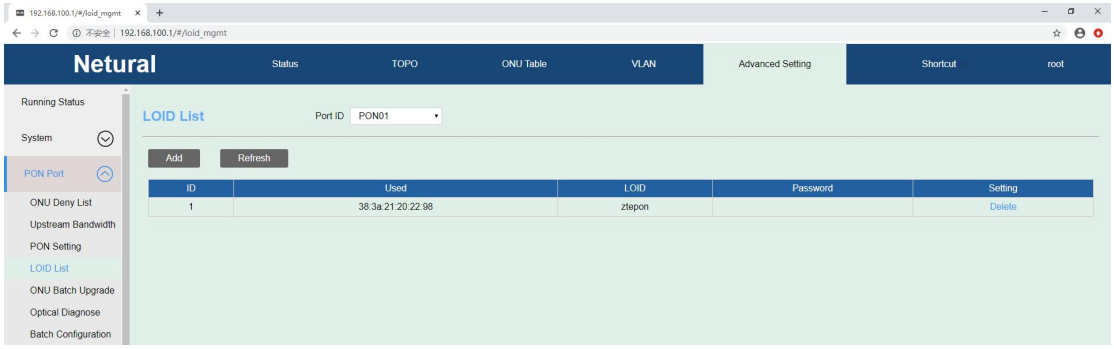
5.3.3.5 Turn on&off Port

Enter the PON setting page, move the mouse to the corresponding pon port "**Setting**" option, and select "**ON/OFF PON optical**" to turn on or off pon port. As shown below:

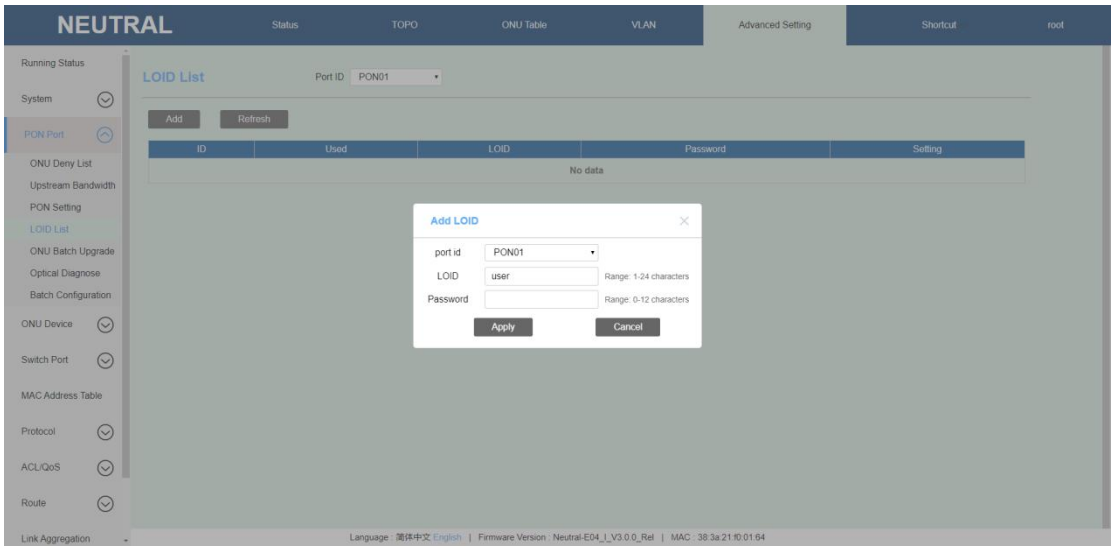


5.3.4 LOID List

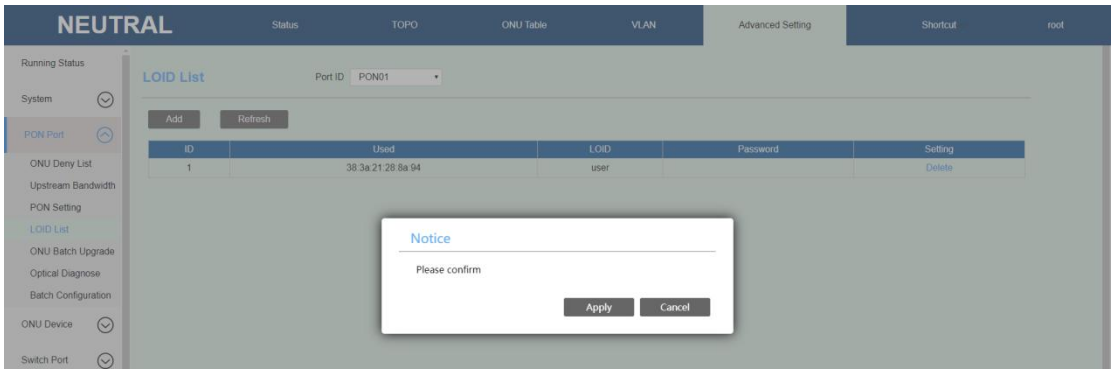
Choose **Advanced Setting** -> **PON Port** -> **LOID List**, enter this page, select the corresponding "**Port ID**", you can view the LOID allowed list under the current PON port, as shown below:



1. On the LOID list page, click the "**Add**" button to add the corresponding ONU to the LOID list, as shown below:

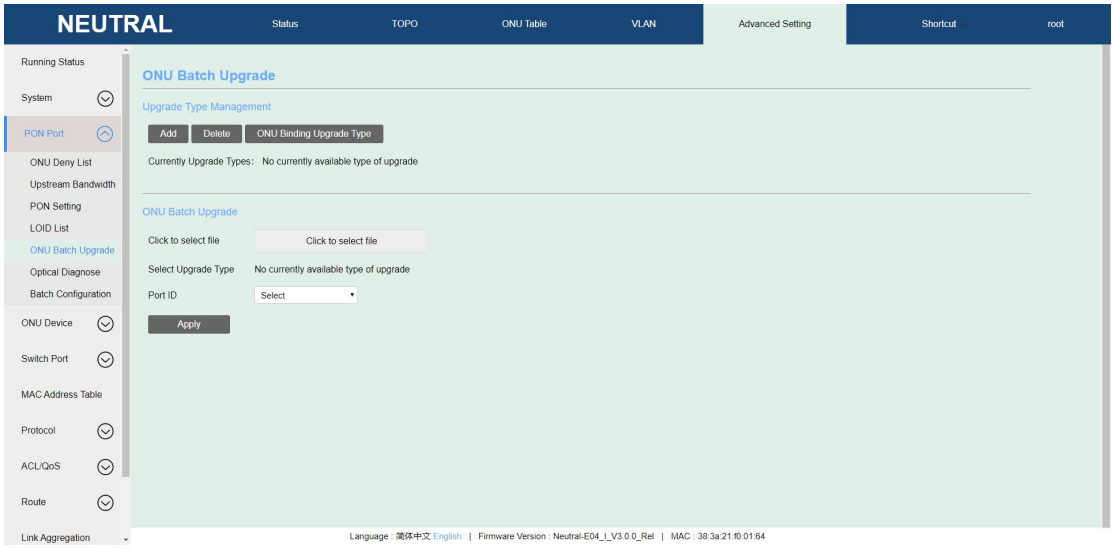


2. On the LOID list page, click the "**Delete**" button to remove the corresponding ONU from the LOID list, as shown below:

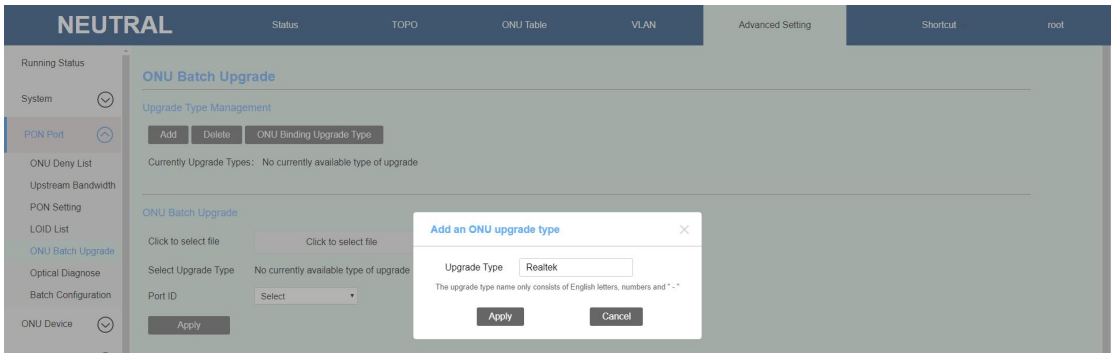


5.3.5 ONU Batch Upgrade

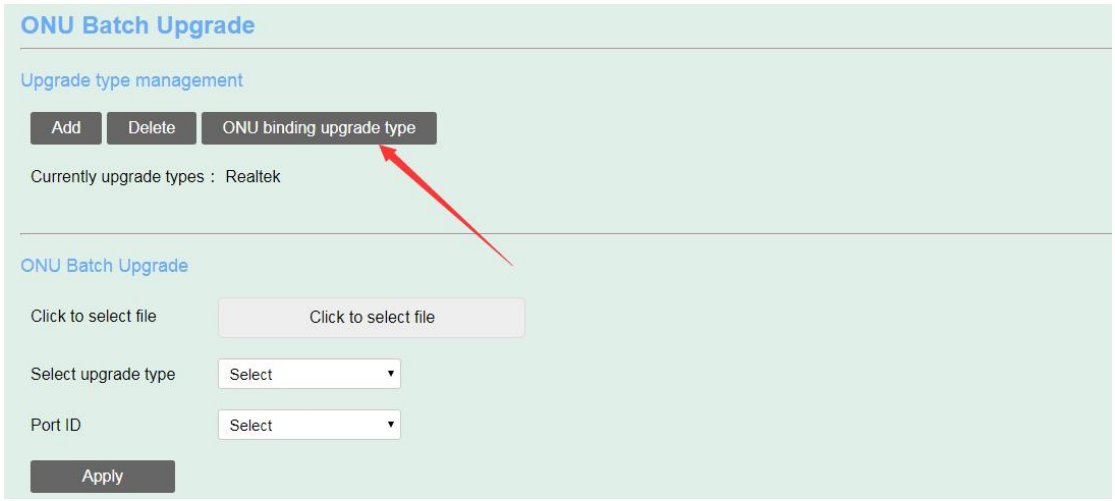
Choose **Advanced Setting** -> **PON Port** -> **ONU Batch Upgrade**, enter this page,you can upgrade the same type multiple ONUs at one time, as shown below:

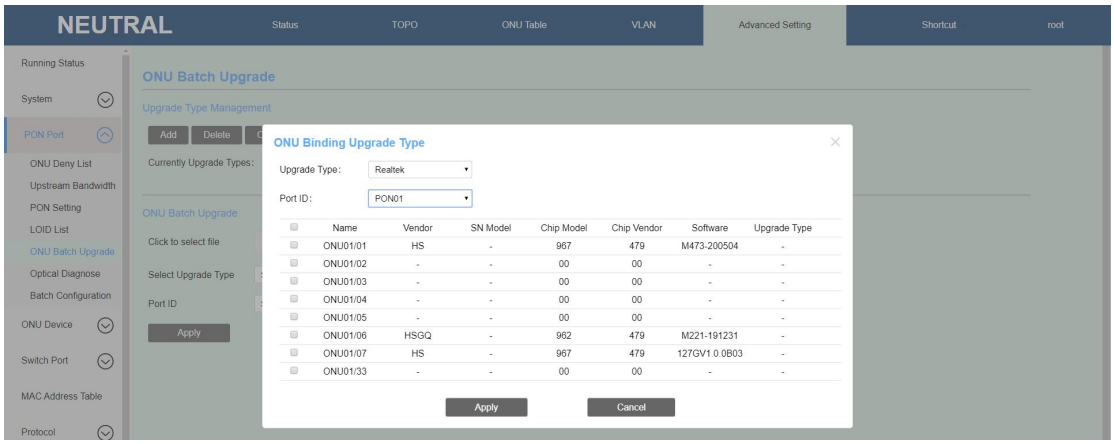


1. Click the "**Add**" button to manually configure the ONU upgrade type, as shown below:

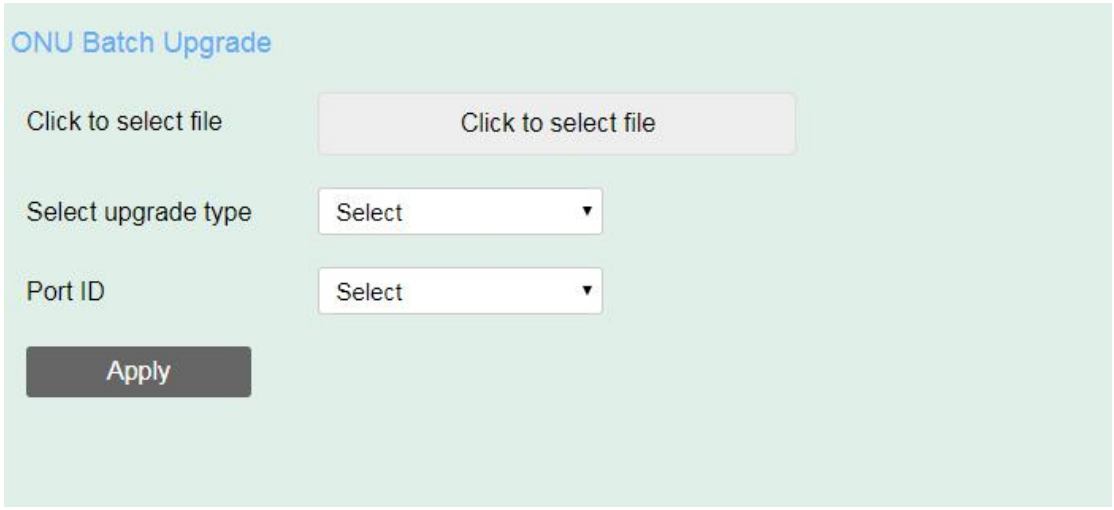


2. Click "**ONU Binding Upgrade Type**", select the corresponding upgrade type and the ONU that needs to be upgraded, as shown below:



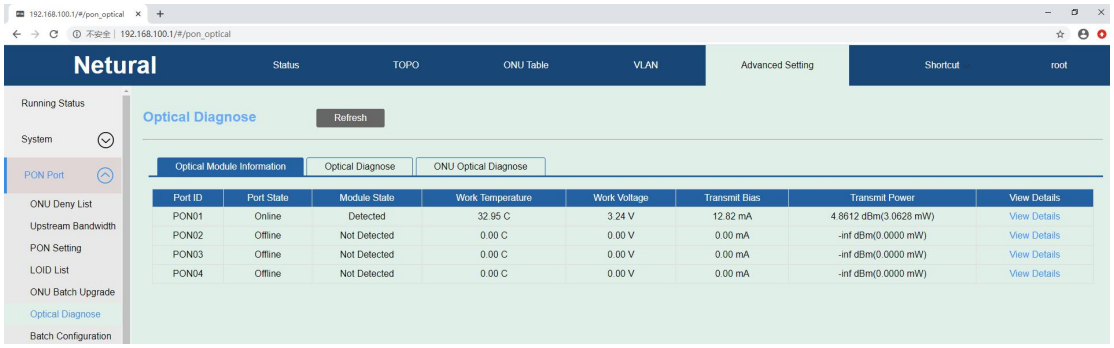


3. Select a file upgrade file and other select upgrade type, select which pon port you want to upgrade.Click "**Apply**", OLT will start to batch upgrade some ONUs.

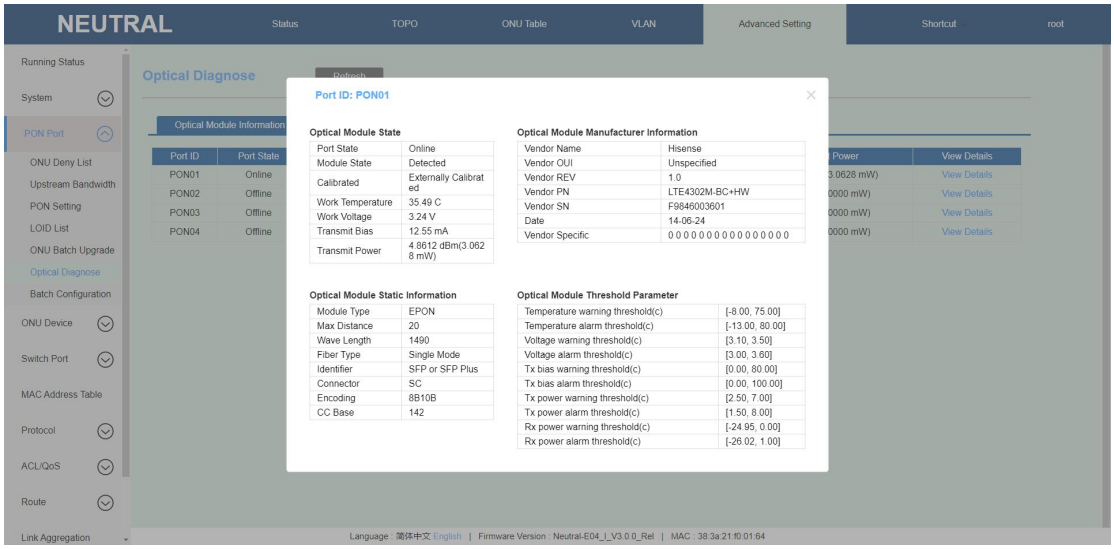


5.3.6 Optical Diagnose

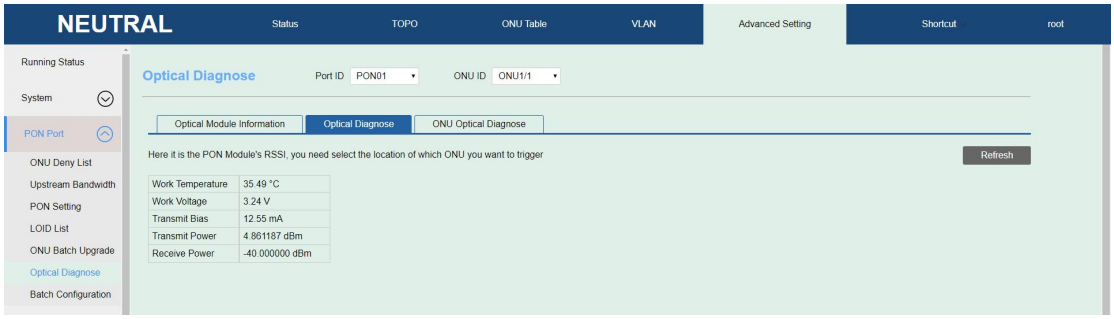
Choose **Advanced Setting** -> **PON Port** -> **Optical Diagnose**, enter this page,you can view optical module, PON optical and ONU optical information, as shown below:



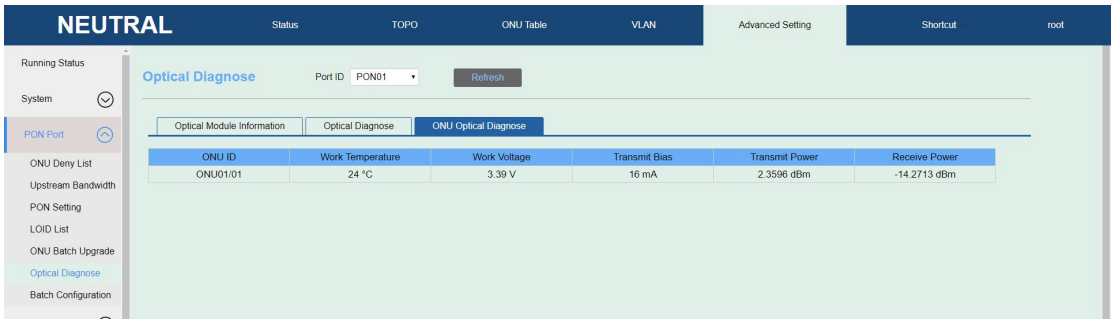
1. View details of optical module information



2. Read PON module's optical diagnose



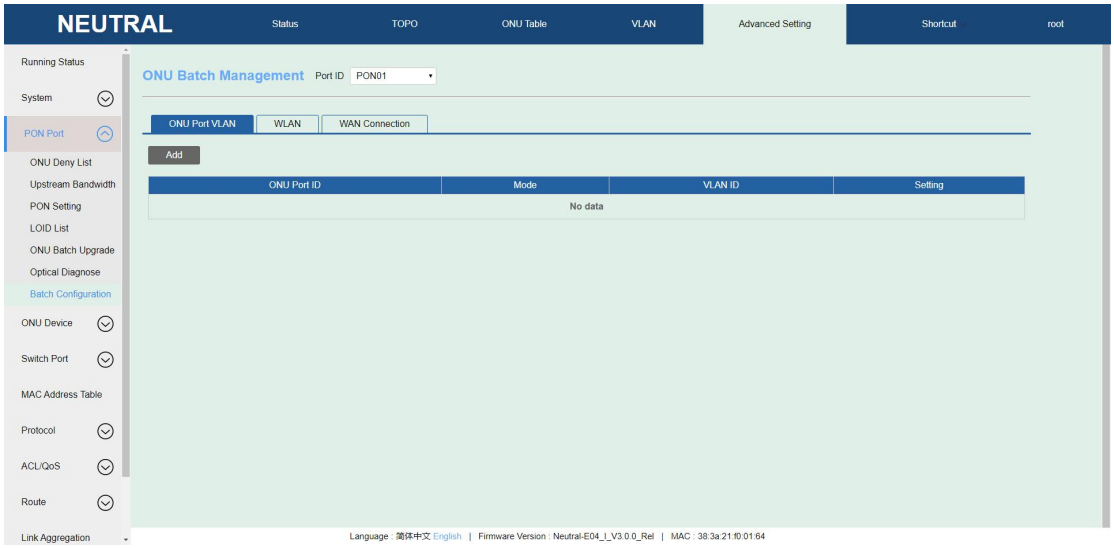
3. Read ONU optical diagnose,you must refresh first to update data



5.3.7 Batch Configuration

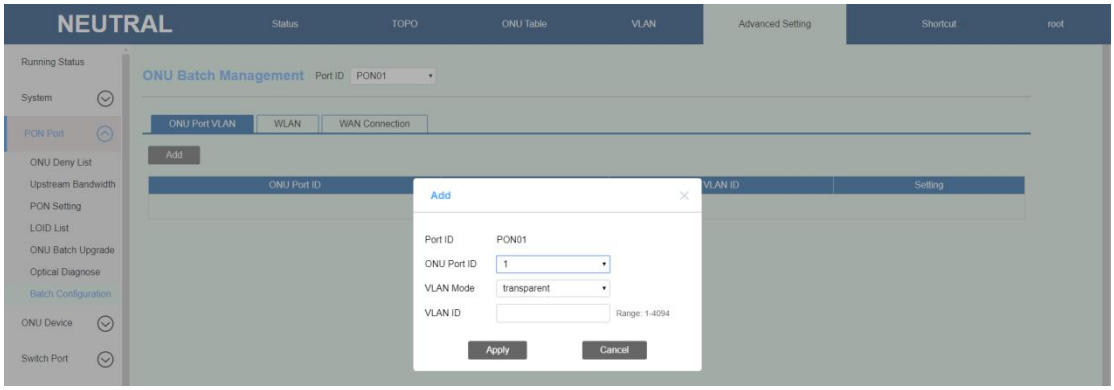
Choose **Advanced Setting** -> **PON Port** -> **Batch Configuration**, enter this page,you can configure ONU port VLAN,ONU WLAN,ONU WAN connection.

Note: ONU WLAN and WAN configuration is private protocol and only supports our company ONU.



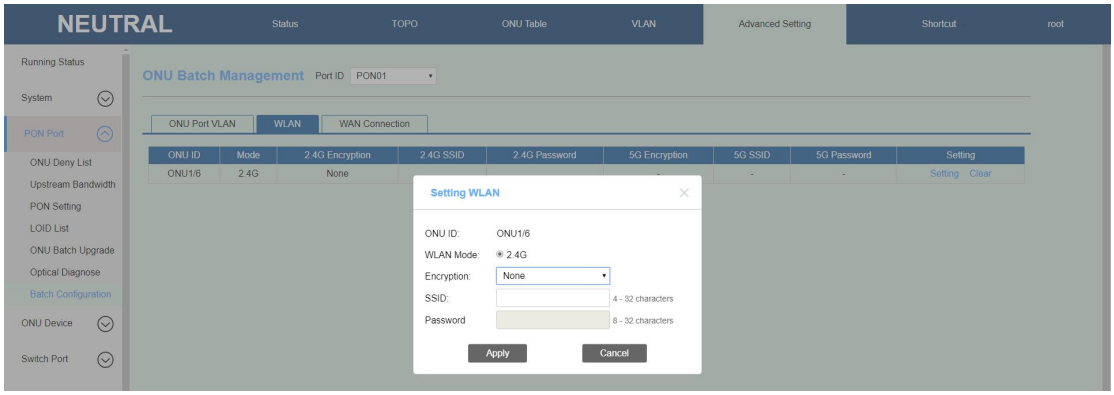
5.3.7.1 ONU Port VLAN(Only Support SFU)

Enter the ONU batch management page, choose **PON ID** -> **ONU Port VLAN**, and click the "**Add**" button to configure the ONU port VLAN. VLAN with up to 8 ONU port numbers can be configured, as shown below:



5.3.7.2 ONU WLAN(Only Support ONU with WIFI)

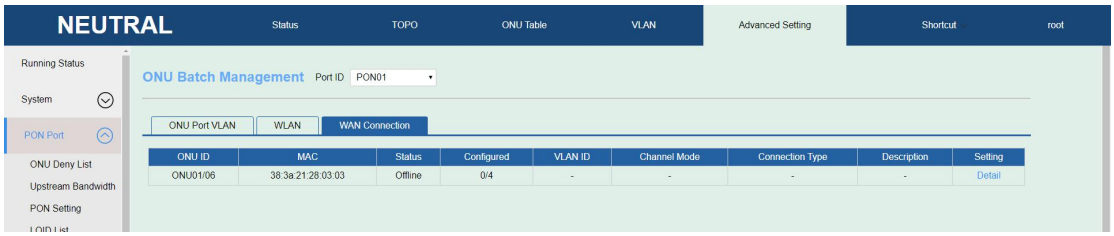
Enter the ONU batch management page, choose **PON ID** -> **WLAN**, You can modify the encryption method,SSID name and SSID password. As shown below:



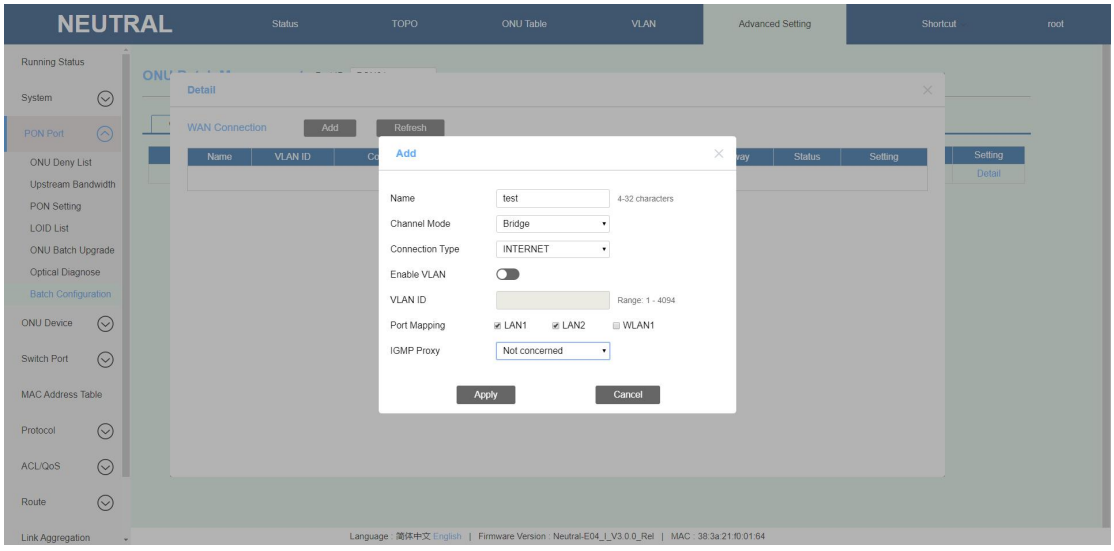
5.3.7.3 WAN Connection(Only Support HGU)

Enter the ONU batch management page, choose **PON ID** -> **WAN Connection**, You can view the created WAN connections and add new WAN connections.

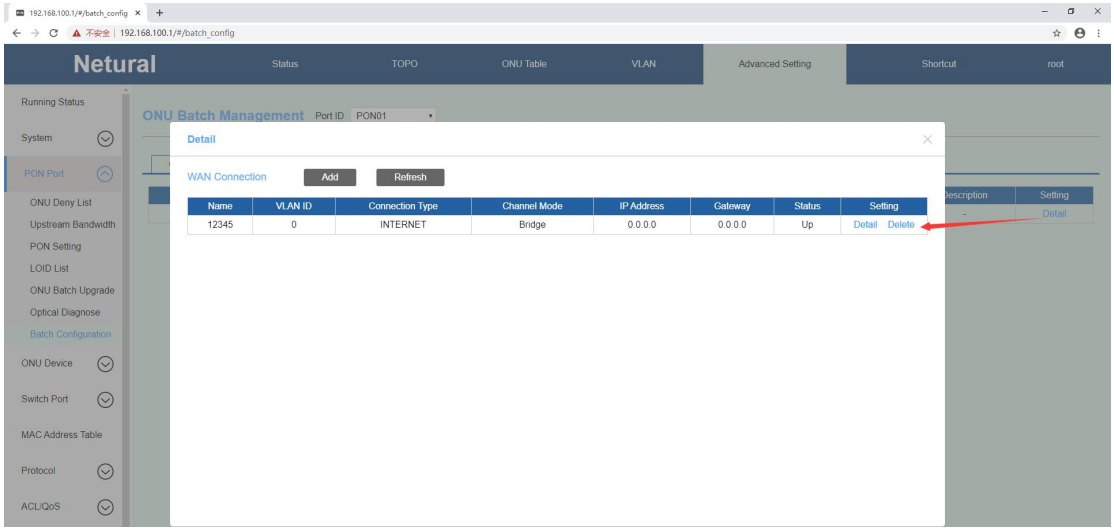
1. View ONU WAN connections. It shows the WAN connection status of all onus under the PON port.



2. Create ONU WAN connections. Select the "**Detail**" button to enter the WAN connection detail interface, then click the "**Add**" button to configure the WAN connection parameters on this interface,as shown below:



3. Delete ONU WAN connections. Select the "**Detail**" button to enter the WAN connection detail interface, then click the "**Delete**" button to remove the WAN connection on this interface,as shown below:

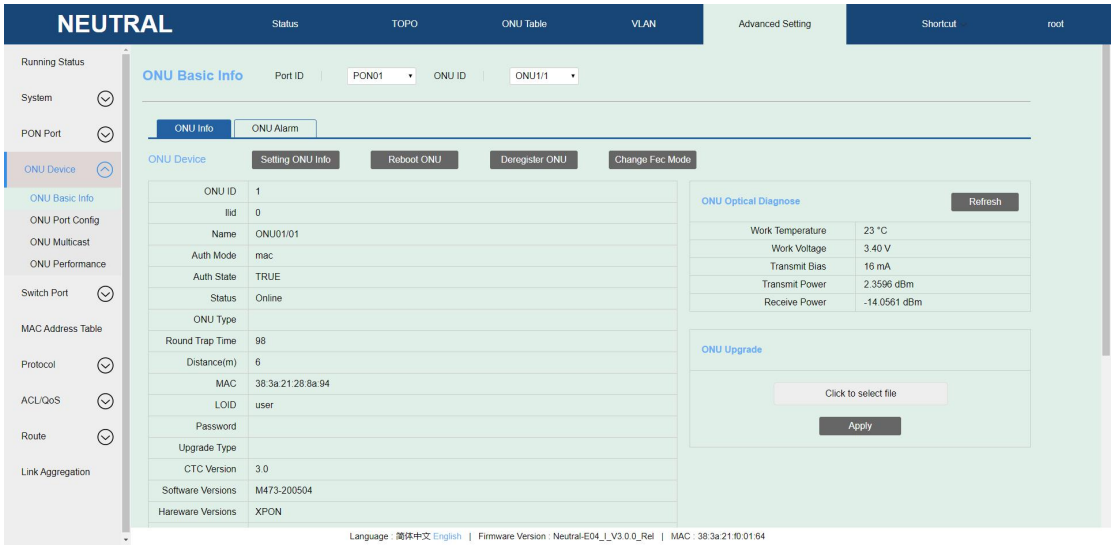


Note: If you delete the WAN connection you just added,wait for 30s.

5.4 ONU Device Management

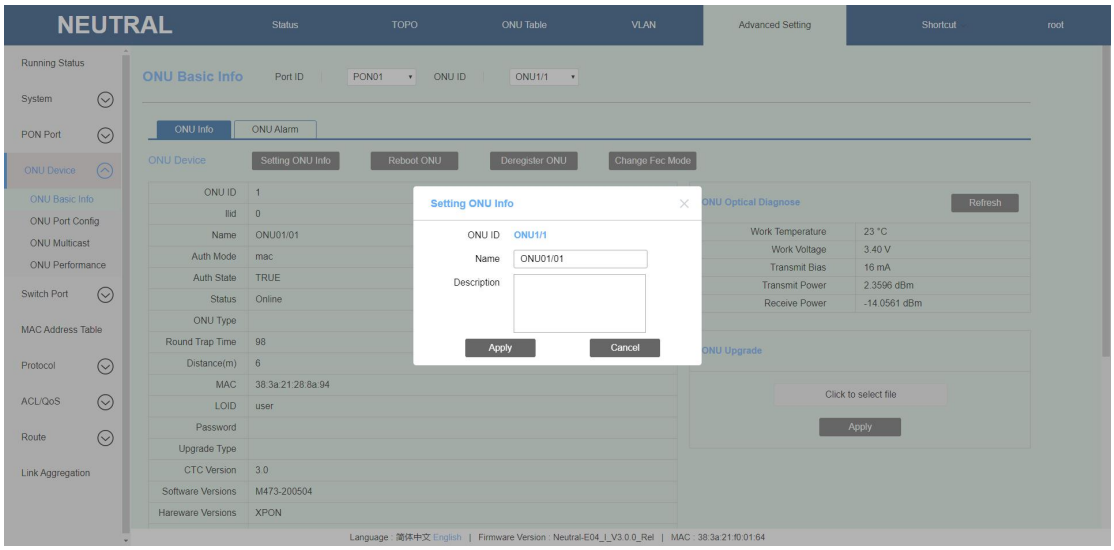
5.4.1 ONU Basic Info

Select **Advanced Setting** -> **ONU Device** -> **ONU Basic Info**, enter this page, you can view ONU basic information and configure ONU management and other settings, as shown below:



5.4.1.1 Configure ONU Info

Enter the ONU basic info page, select the corresponding ONU at the top, and click the "**Setting ONU Info**" button to configure the ONU name and description information. As shown below:

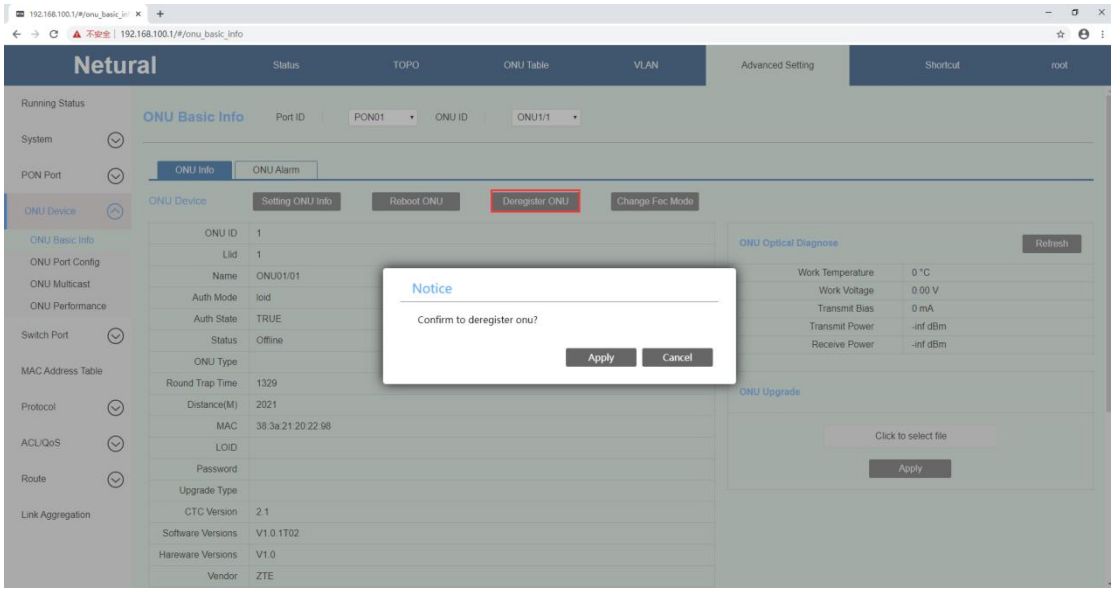


5.4.1.2 Reboot ONU

Enter the ONU basic info page, select the corresponding ONU at the top, and click the "**Reboot ONU**" button to restart ONU.

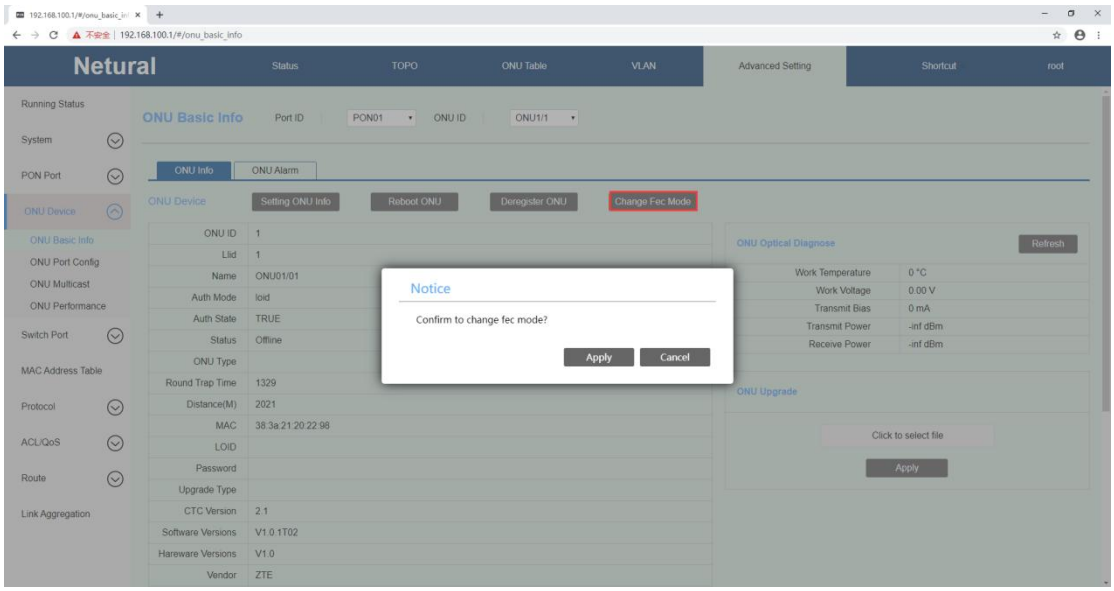
5.4.1.3 Deregister ONU

Enter the ONU basic info page, select the corresponding ONU at the top, and click the "**Deregister ONU**" button to let ONU offline. As shown below:



5.4.1.4 Turn on/off ONU Fec Mode

Enter the ONU basic info page, select the corresponding ONU at the top, and click the "**Change Fec Mode**" button to enable or disable this function. The default setting is disable. As shown below:

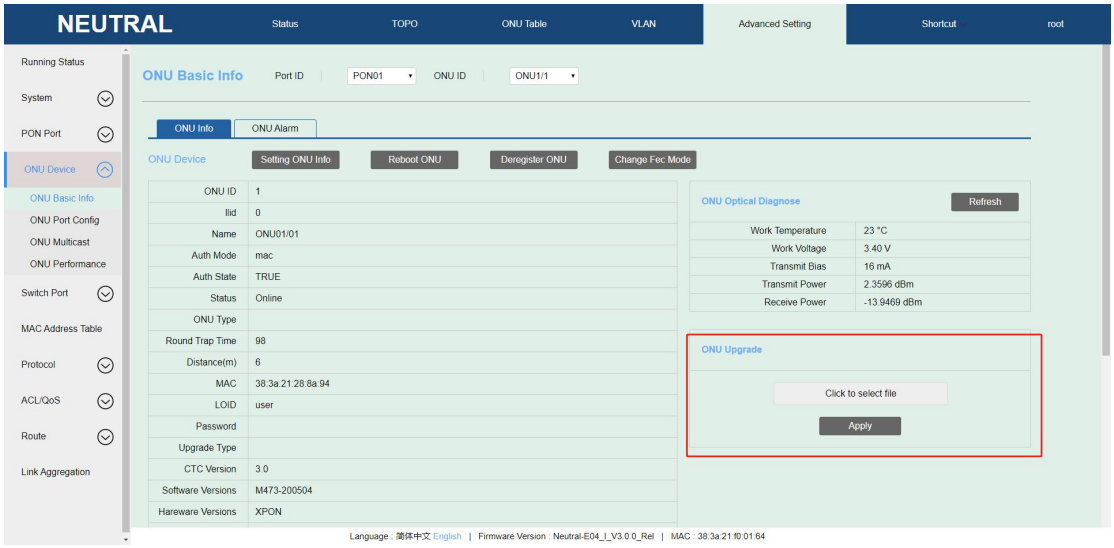


5.4.1.5 View ONU Optical Diagnose Information

Enter the ONU basic info page, select the corresponding ONU at the top, and click the ONU optical diagnose"**Refresh**" button to view ONU optical power information.

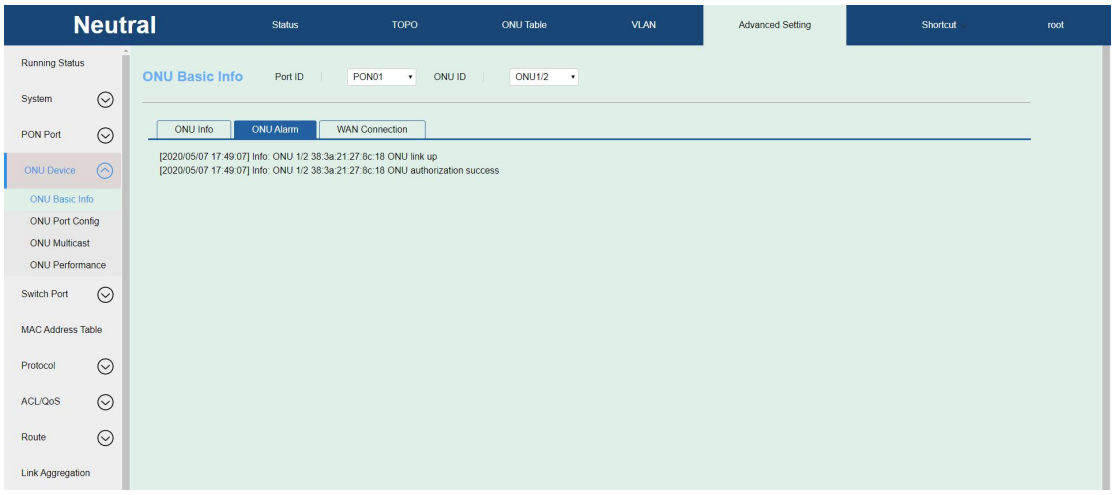
5.4.1.6 Upgrade ONU

Enter the ONU basic information page, select the corresponding ONU at the top, fist click the "**Click to select file**" button to upload the ONU upgrade file, and then click the "**Apply**" button, the ONU will enter the upgrade state. As shown below:



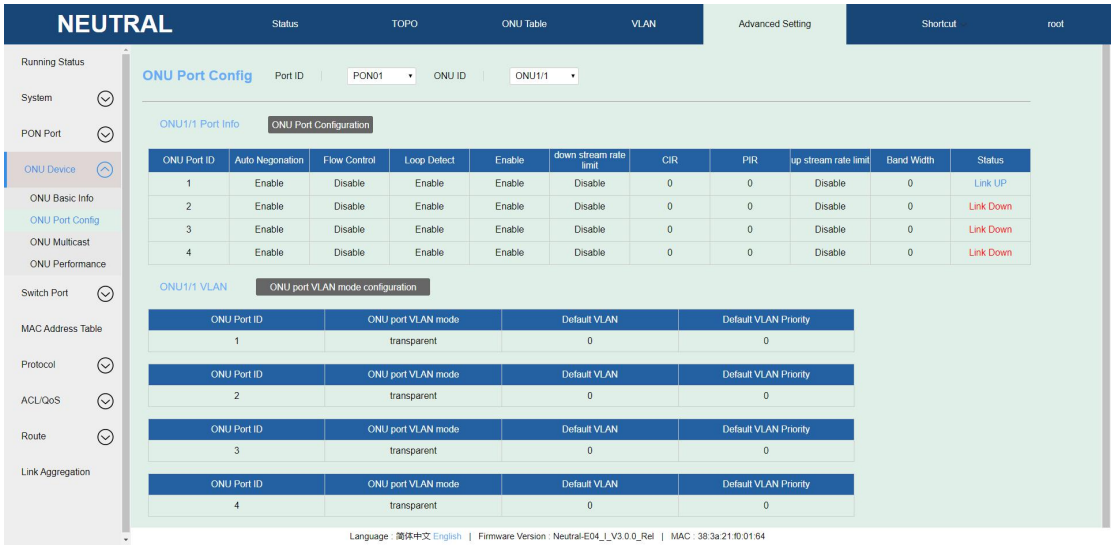
5.4.1.7 View ONU Alarm Information

Choose **Advanced Setting** -> **ONU Device** -> **ONU Basic Info**, enter this page, choose "**ONU Alarm**" you can view alarm information, as shown below:



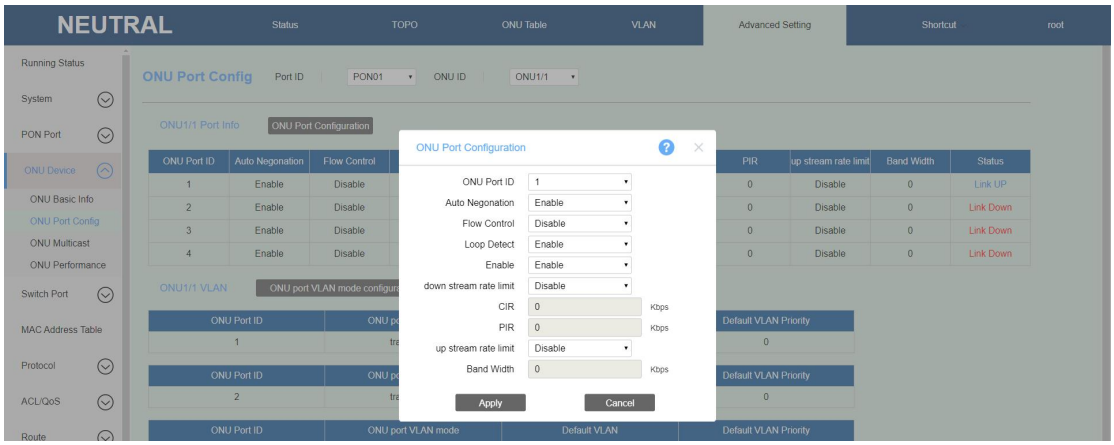
5.4.2 ONU Port Config(Only support SFU)

Select **Advanced Setting** -> **ONU Device** -> **ONU Port Config**, enter this page, you can configure ONU port basic functions and VLAN mode. As shown below:



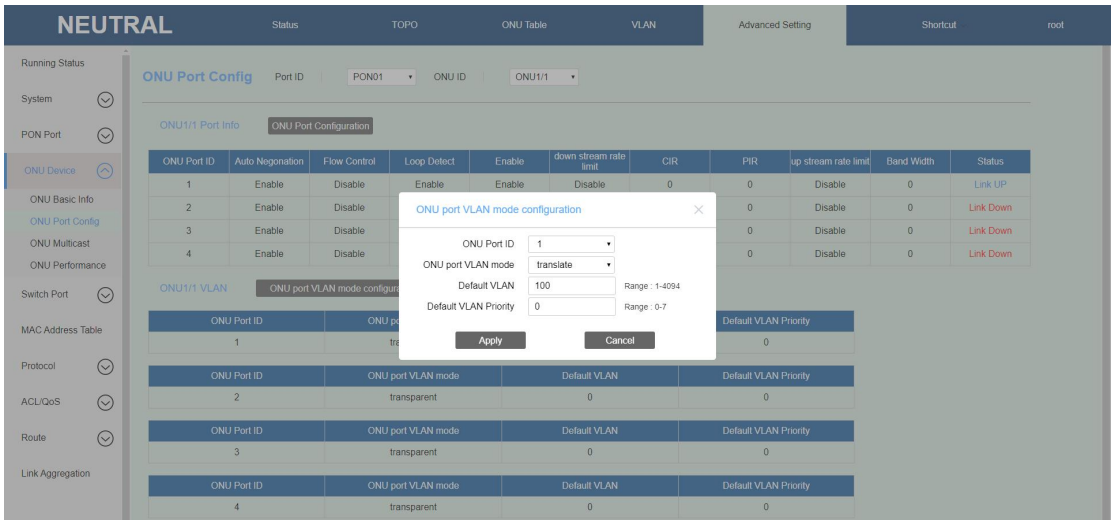
5.4.2.1 ONU Port Attribute Config

Enter the ONU port config page, select the corresponding ONU at the top, and click the "**ONU Port Configuration**" button to configure the ONU port attribute parameters, including port negonation, flow control, loop detect, port status, upstream and downstream limits speed, etc. As shown below:



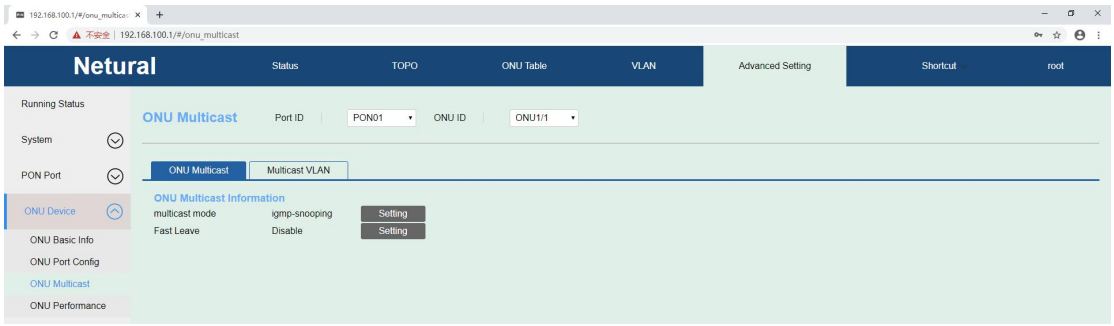
5.4.2.2 ONU Port VLAN Config

Enter the ONU port config page, select the corresponding ONU at the top, and click the "**ONU port VLAN mode configuration**" button to configure the ONU port VLAN mode, VLAN ID, VLAN priority. As shown below:



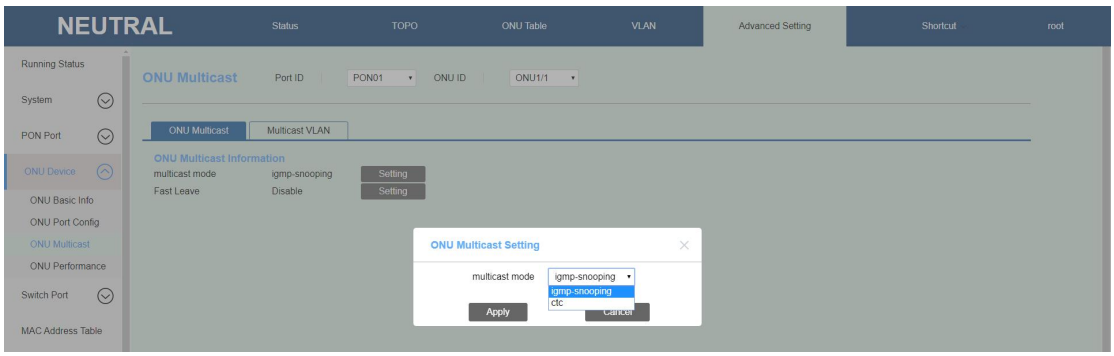
5.4.3 ONU Multicast

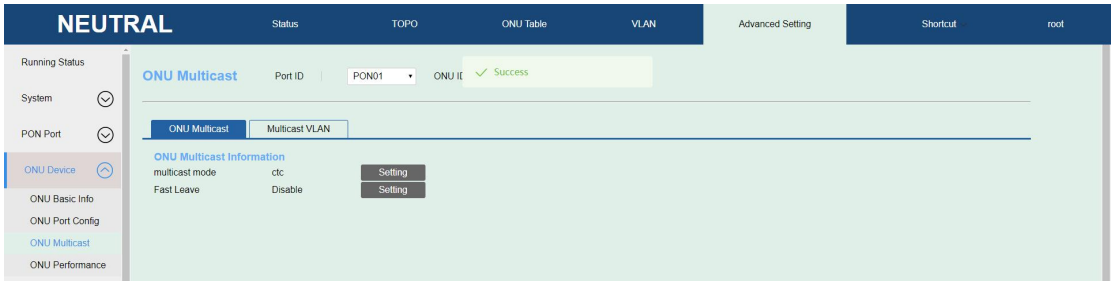
Select **Advanced Setting** -> **ONU Device** -> **ONU Multicast.** enter this page, you can configure ONU multicast function, including ONU multicast and multicast vlan. As shown below:



5.4.3.1 ONU Multicast Mode

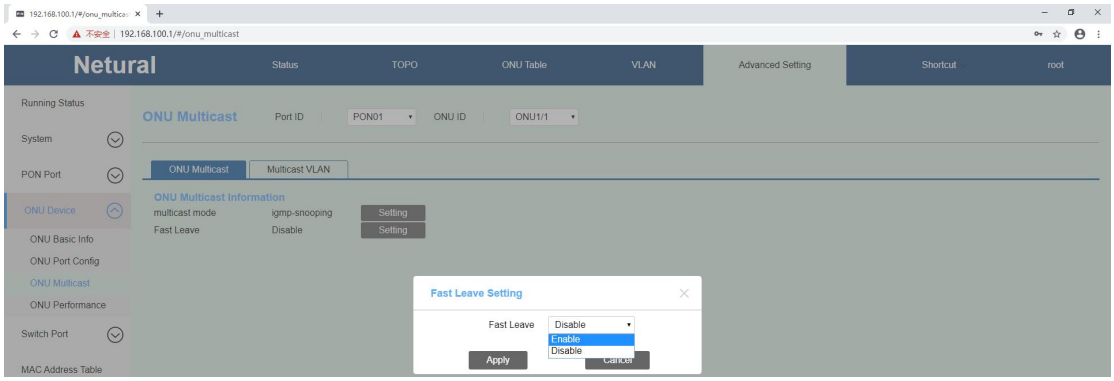
Enter the ONU multicast page, select the corresponding ONU at the top, and click multicast mode "**Setting**" button, as shown below:

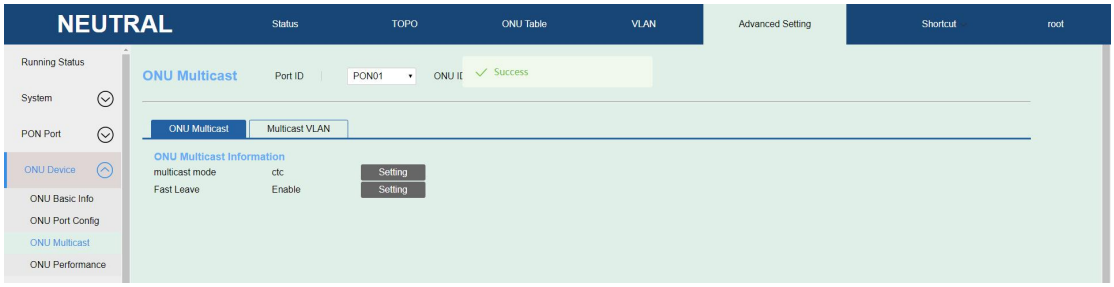




5.4.3.2 ONU Multicast Fast Leave

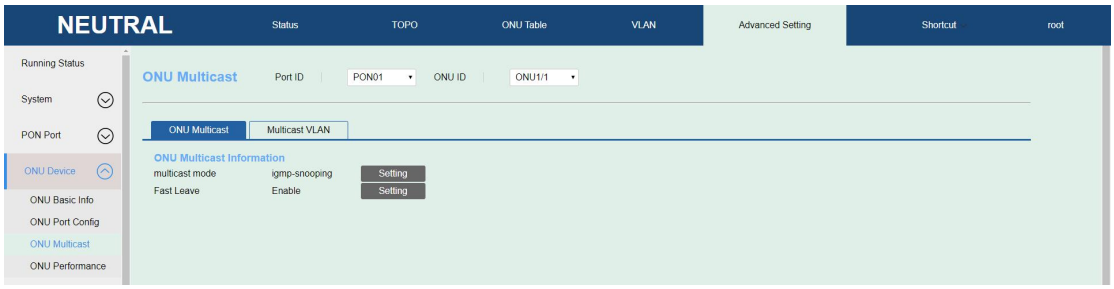
Enter the ONU multicast page, select the corresponding ONU at the top, and click fast leave "**Setting**" button, as shown below:

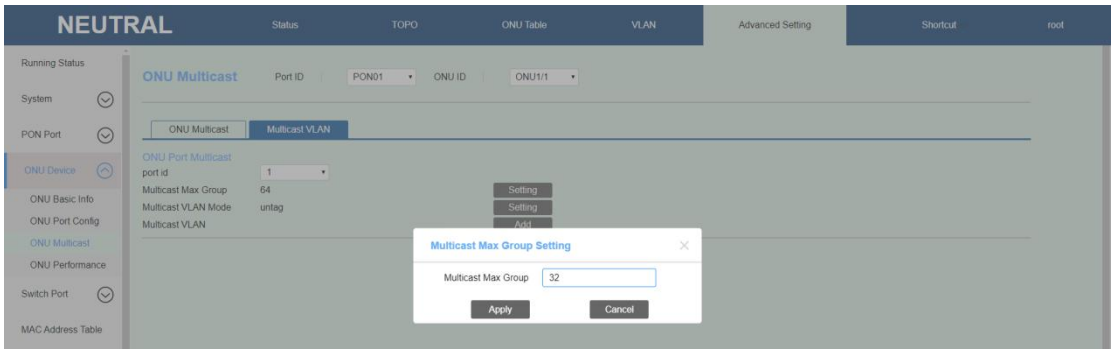


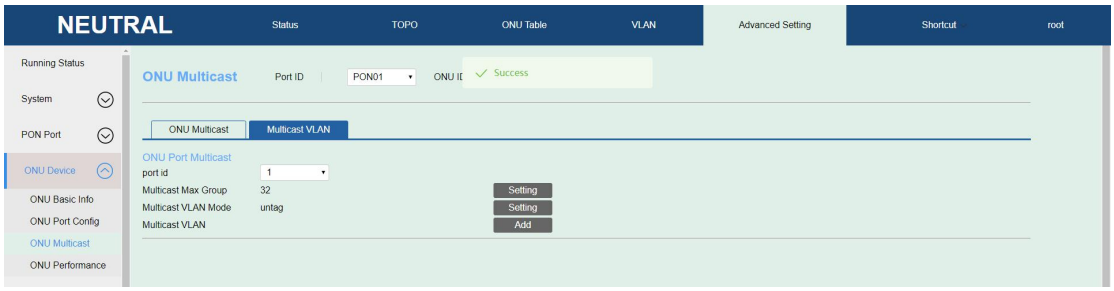


5.4.3.3 ONU Multicast Max Group

Enter the ONU multicast page, select the corresponding ONU at the top, click Multicast VALN -> Multicast Max Group setting, you can set this value. As shown below:



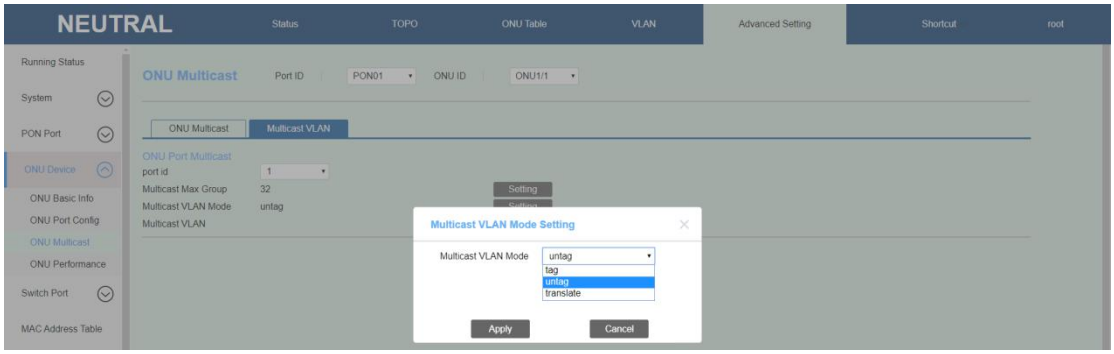




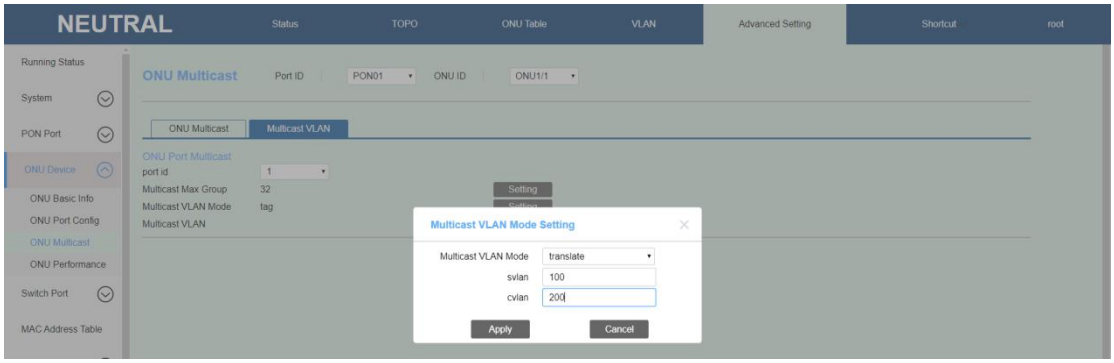
5.4.3.4 ONU Multicast VLAN Mode

Enter the ONU multicast page, select the corresponding ONU at the top, click Multicast VALN -> Multicast VLAN Mode Setting, you can set this value. this configuration determines whether the multicast streams forwarded by the ONU port has a VLAN tag. Untag is for stripping the tag, tag is for not stripping the tag, and translate is for converting the VLAN tag.

Example 1: configure multicast VLAN mode tag or untag.

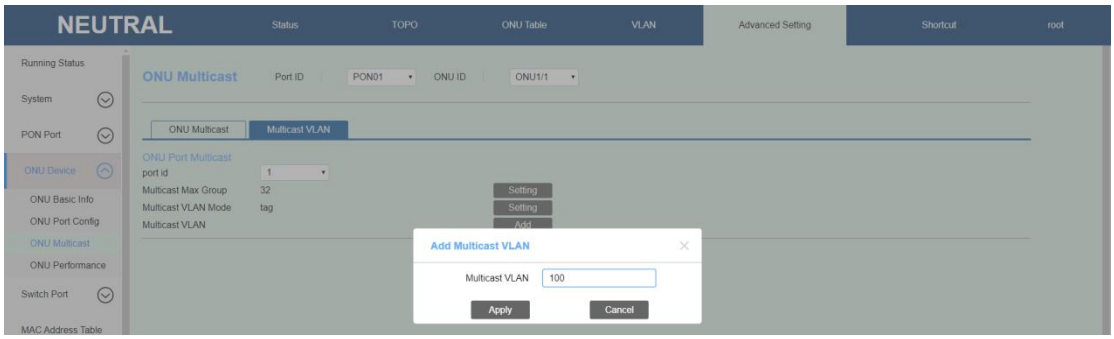


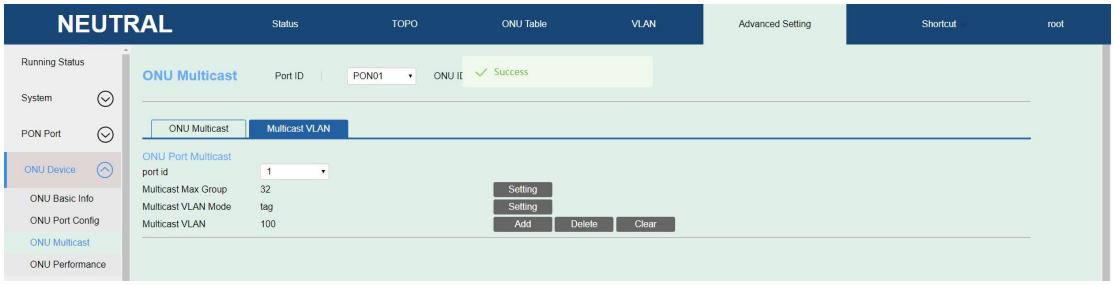
Example 2: Configure multicast VLAN mode translate ,up to 8 group translation can be configured(CTC standard definition, depending on ONU support).



5.4.3.5 ONU Multicast VLAN

Enter the ONU multicast page, select the corresponding ONU at the top, click Multicast VALN -> Multicast VLAN Add, you can set this value, as shown below:





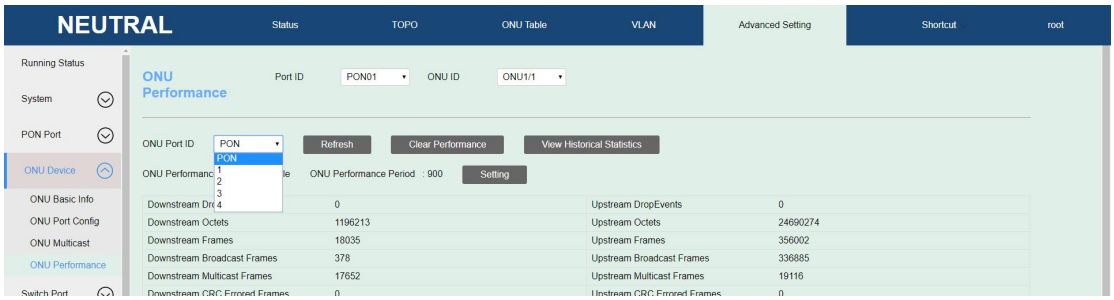
Note: Only if the ONU multicast mode is configurable as igmp-snooping,when the ONU multicast mode switches from igmp-snooping to another mode, the multicast VLAN will be cleared.Each port can be configured with up to 8 multicast vlan(CTC standard definition, depending on ONU support).

5.4.4 ONU Performance Statistics

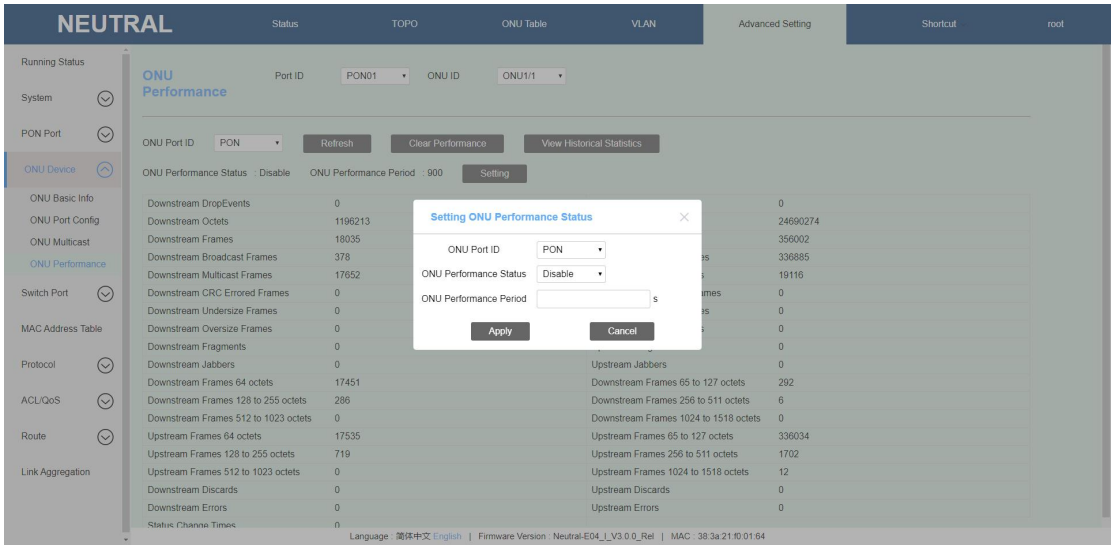
Select **Advanced Setting** -> **ONU Device** -> **ONU Performance Statistics.** enter this page, you can view,configure and clear ONU performance information.

1. Enter the ONU Performance page, select the corresponding ONU at the top, and click the "**Refresh**" button to view the current ONU port statistics, as shown below:

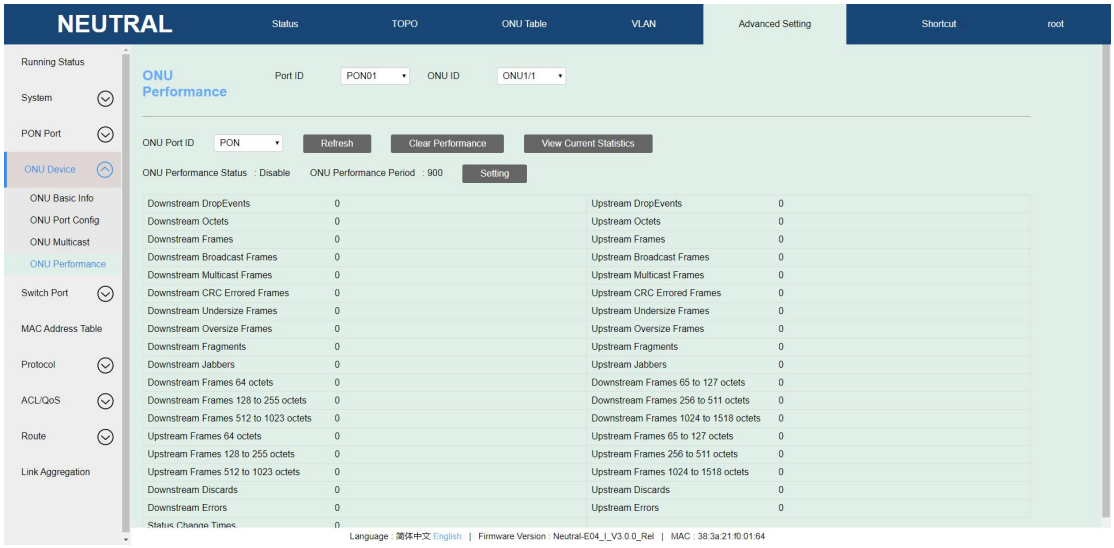
Also you will get the detail of PON & LAN port of ONU.Change the port to other. As show below:



2. Enter the ONU Performance page, select the corresponding ONU at the top, and click the "**Setting**" button to configure ONU port performance monitor state, as shown below:



3. Enter the ONU Performance page, select the corresponding ONU at the top, and click the "**View History Statistics**" button to get history performance monitor data, as shown below:



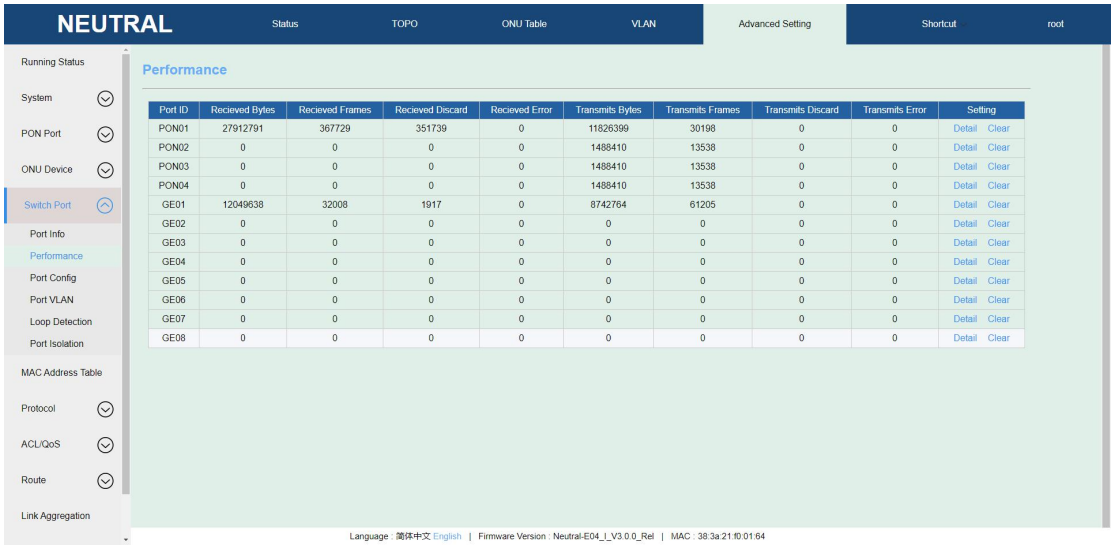
5.5 Port Management

5.5.1 Port Info

Choose **Advanced Setting** -> **Switch Port**-> **Port Info**, enter this page, you can view the OLT PON port and uplink port basic information, as shown below:

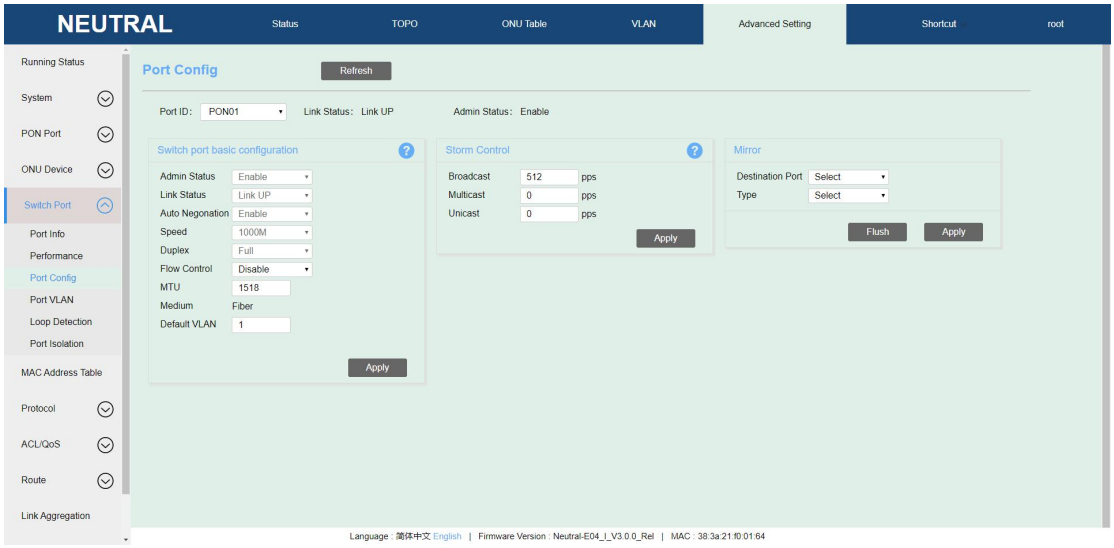
5.5.2 Performance

Choose **Advanced Setting** -> **Switch Port**-> **Performance**, enter this page, you can view and clear the OLT PON port and uplink port statistic information, as shown below:



5.5.3 Port Config

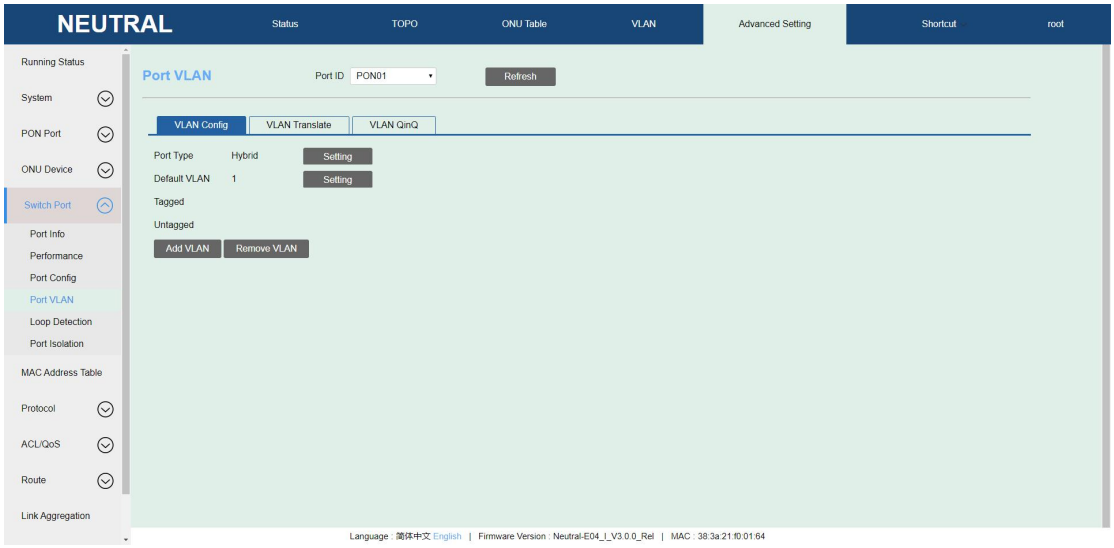
Choose **Advanced Setting** -> **Switch Port**-> **Port Config**, enter this page, you can first select the corresponding port at the top of the page, and then you can configure port parameters, including admin status, link status, auto negonation, speed, duplex mode, and MTU, default VLAN, port description, broadcast/multicast/unicas storm control and port mirroring functions. As shown below:



Note: The MTU default value is 1518, which can be configured according to the actual situation of the network. Broadcast/multicast/unicast storm control, with PPS as the unit, 0 means off storm suppression function.

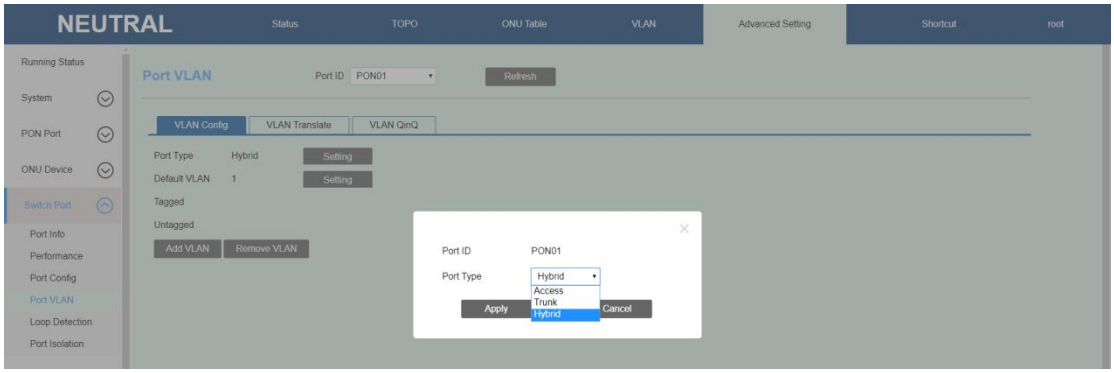
5.5.4 Port VLAN Configuration

Choose **Advanced Setting** -> **Switch Port**-> **Port VLAN**, enter this page, you can configure port VLAN parameter. As shown below:

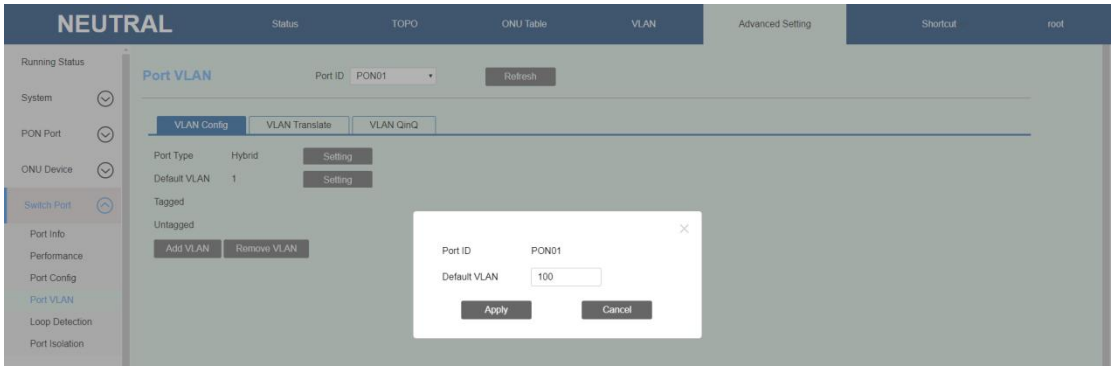


5.5.4.1 Port VLAN Config

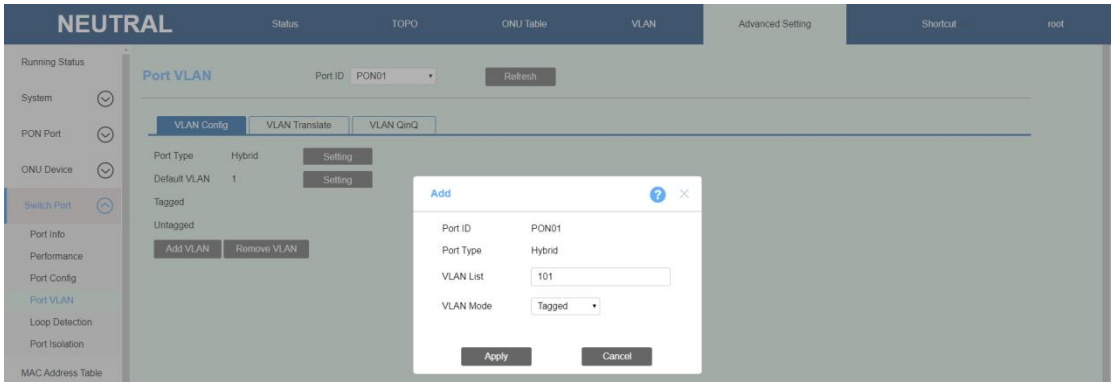
1. **Configure the port VLAN type:** enter the port VLAN page, select the interface to be set at the top, click the port type "**Setting**" button, you can configure the port VLAN to hybrid, access and trunk modes, as shown below:



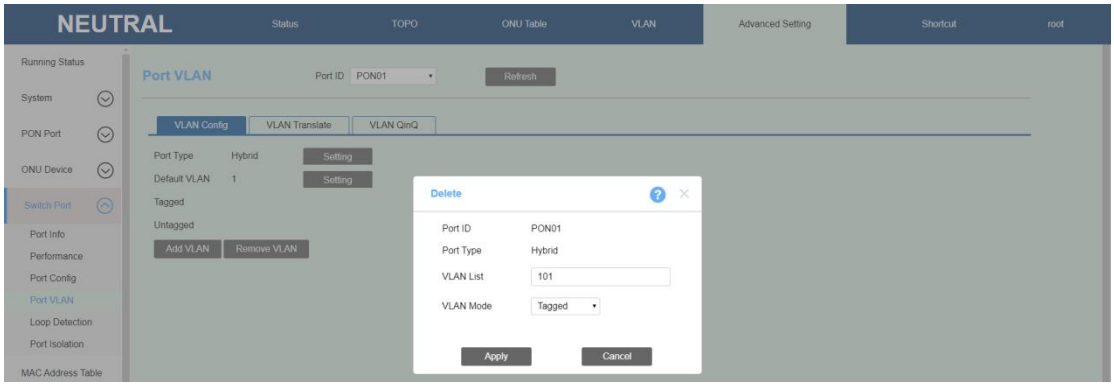
2. **Configure port default VLAN**: enter the port VLAN page, select the interface to be set at the top, click the default VLAN "**setting**" button, modify the default port VLAN here, and the port default VLAN is 1. As shown below:



3. **Add VLAN to this port:** enter the port VLAN page, select the interface to be set at the top, click the "**Add VLAN**" button, you can add VLAN to this port and select the vlan tag or untag mode, as shown below:

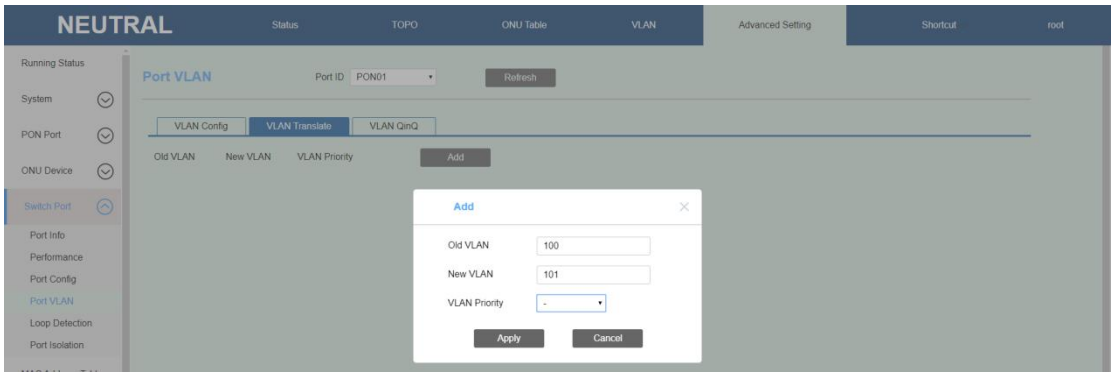


4. **Delete VLAN from this port:** enter the port VLAN page, select the interface to be set at the top, click the "**Remove VLAN**" button, you can delete VLAN from this port, as shown below:



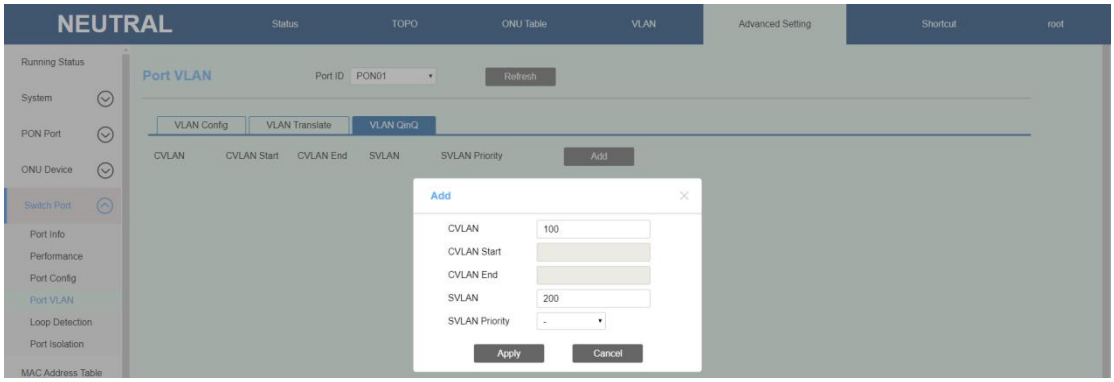
5.5.4.2 VLAN Translate

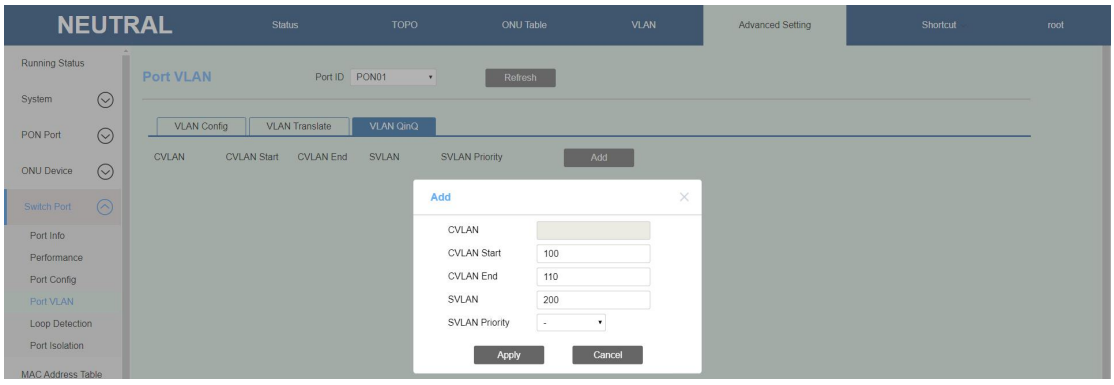
Enter the port VLAN page, select the interface to be set at the top, and then select VLAN translate, click the "**Add**" button below, you can create port translation, as shown below:



5.5.4.3 VLAN QinQ

Enter the port VLAN page, select the interface to be set at the top, and then select VLAN QinQ, click the "**Add**" button,here you can add the port QinQ, support the configuration of a single CVLAN, and also support the configuration of the CVLAN range, as shown below:



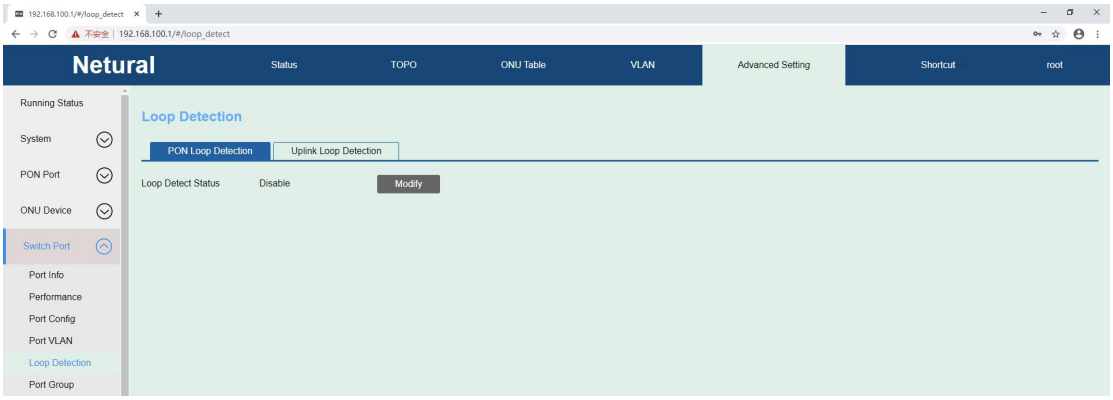


5.5.5 Loop Detection

This function is to process the loop that appears in the network to prevent the loop from affecting the services, and it is necessary to detect the user-side loop.After the user-side loop detection function is turned on, the system will automatically detect the user-side loop.

When the loop is detected, the occurrence of the loop will be stopped and an alarm will be issued.

Choose **Advanced Setting** -> **Switch Port**-> **Loop Detection** , enter this page, you can configure port loop detection function. As shown below:



5.5.5.1 PON Loop Detection

1. Introduction of PON loop detection function:

PON loop detection function is turned on by default. There are three conditions of loop detection processing:

(1) When a loop occurs on the same ONU port or connected device, the PON loop detection will not be triggered because the ONU port loop detection function is turned on by default.

(2) If loop occurs between different ONU in the same PON port, when the P2P function is turned off (by default), only ring alarm will be issued, and ONU will not be added to the blacklist.When the P2P function is turned on, an alarm is issued for the loop and an ONU of the loop is added to the blacklist.

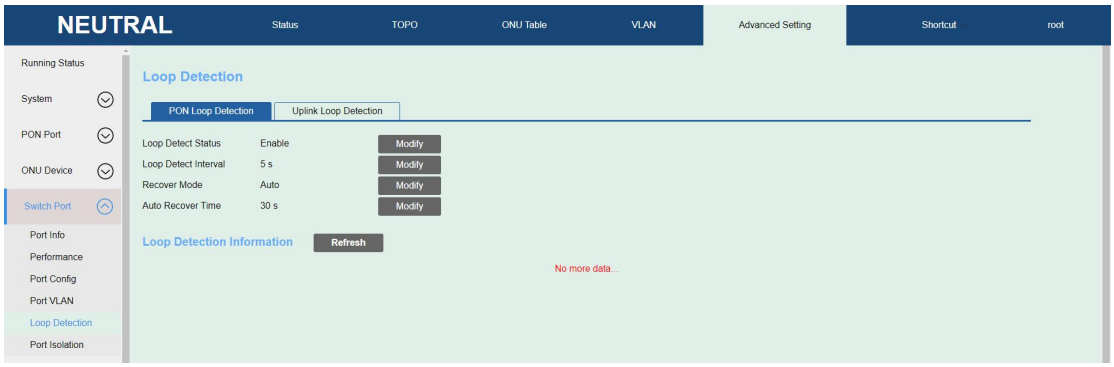
(3) When the PON port isolation function is turned on (by default), only ring alarm will be issued, and ONU will not be added to the blacklist.When the PON port isolation function is turned off and the default VLAN of the two PON ports are the same, the ring alarm will be issued and one of the ONU of the loop will be added to the blacklist.

Note:

1-> PON loop detects the blacklist ONU and saves the configuration without automatically removing the blacklist or in manual recovery mode. After reboot the device, the ONU will be permanently on the blacklist and the blacklist needs to be removed manually.

2-> In manual authentication mode, loop detection is added to the blacklist and manual authentication is required before re-online.

2. **PON loop detection parameter configuration:** enter the loop detection page, click the "**Modify**" button, here you can enable or disable the function, when configuring the enable status, you can modify the corresponding parameters, as shown below:



(1).Loop detect status:The default is the enable state. If the optional configuration disable, the PON loop detection function will not take effect after configuration.

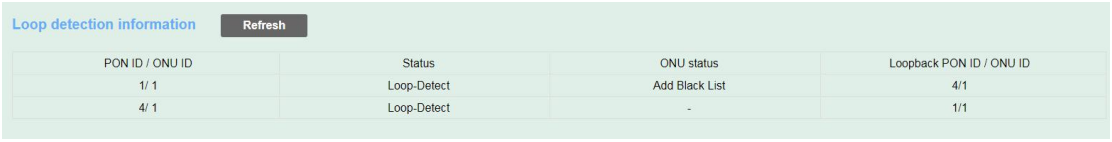
(2).Loop detect interval:This parameter is to configure the PON loop detection packet sending interval, and send a loop detection packet in 5 seconds by default.

(3). Loop detect recover mode:This parameter is to configure whether to automatically restore and remove the blacklist after the loop ONU is added to the blacklist. The default is automatic recovery mode, manual recovery mode is optional;

(4).Auto recover time: This parameter only takes effect when the loop detection recovery mode is Auto, and the default is automatic recovery for 30 seconds.

(5).Manual recover: This configuration is only available when the loop detects that the recovery mode is Manual, and ONU is removed from the blacklist.

3. Enter the loop detection page, where you can view the PON loop detection information, as shown below:



5.5.5.2 Uplink Loop Detection

1. Introduction of uplink loop detection function:

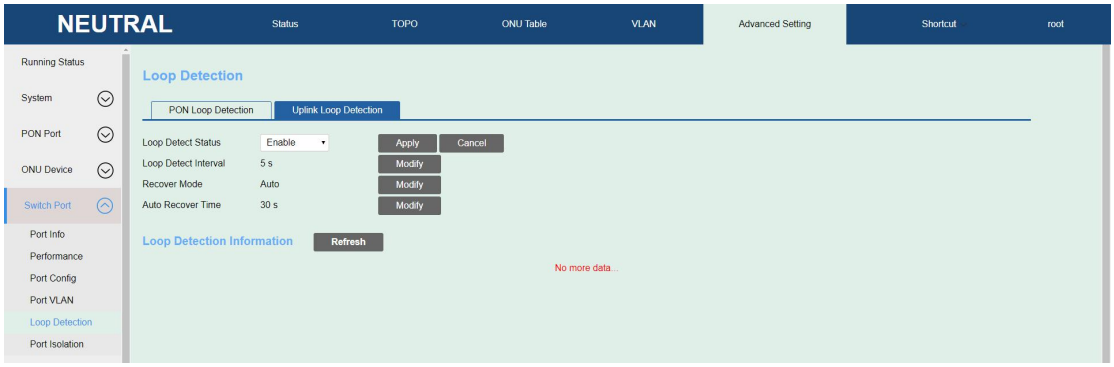
The loop detection function of the uplink port is turned on by default, and there are three conditions for loop detection processing:

(1). When the spanning tree protocol is enabled, the uplink loop detection does not take effect, and only when the spanning tree protocol is disabled will the uplink loop detection take effect.

(2). If a loop occurs with the same uplink port, directly link down the uplink port;

(3). When the default VLAN is different at the same time, the loop alarm occurs, and don’t link down the port.When the default VLAN is same, the loop alarm occurs and Link Down one of the ports.

2. **Configuration of uplink loop detection parameters**: enter the loop detection page, select the uplink loop detection, click "**Modify**" button, here you can enable or disable the function, when the enable status is configured, the corresponding parameters can be modified, as shown below:



(1).Loop detect status:The default is the enable state. If the optional configuration disable, the uplink loop detection function will not take effect after configuration.

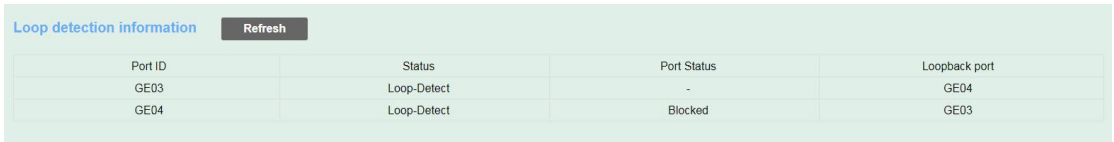
(2).Loop detect interval:This parameter is to configure the uplink loop detection packet sending interval, and send a loop detection packet in 5 seconds by default.

(3). Loop detect recover mode:This parameter is to configure whether to automatically restore the link down port to link up. The default is automatic recovery mode, manual recovery mode is optional;

(4).Auto recover time: This parameter only takes effect when the loop detection recovery mode is Auto, and the default is automatic recovery for 30 seconds.

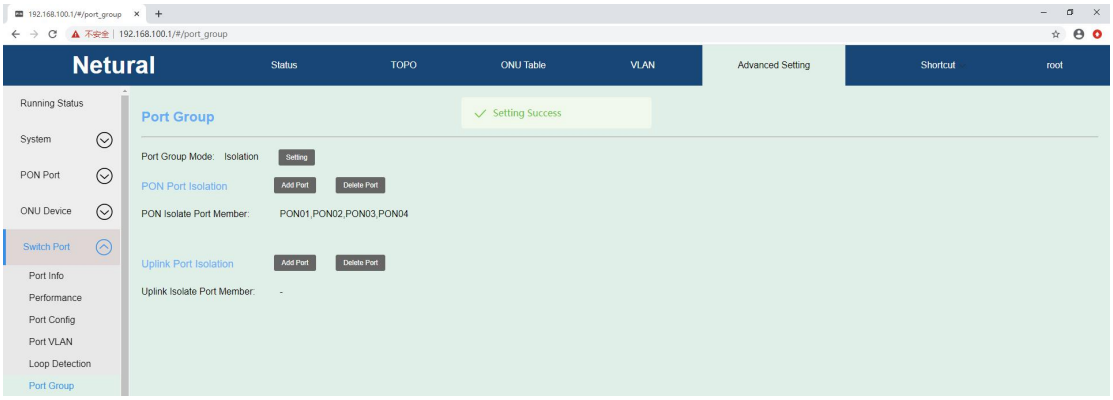
(5).Manual recover: This configuration is only available when the loop detects that the recovery mode is Manual, and the link down port will be link up.

3. Enter the loop detection page, select "uplink Loop Detection" here to view the uplink port loop detection information, as shown below:



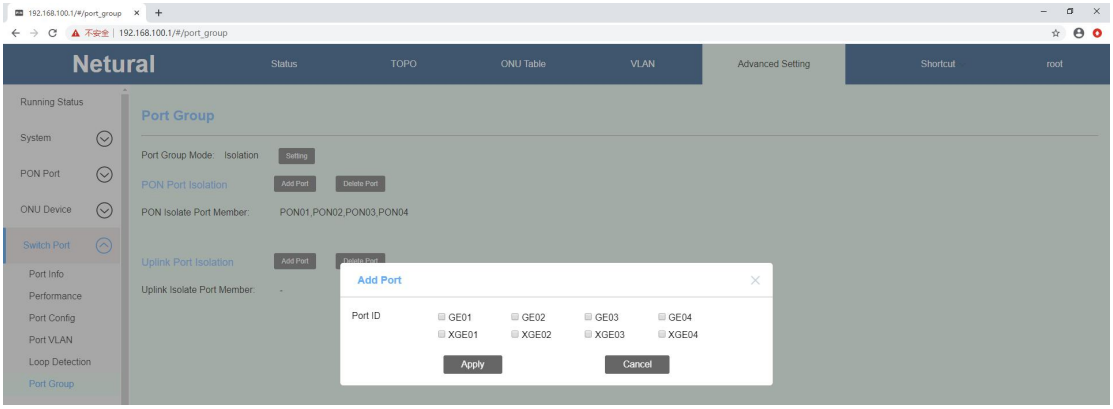
5.5.6 Port Group

Select **Advanced Setting** -> **Switch Port** -> **Port Group** to enter this page to configure port isolation and inter-working functions. As shown below:



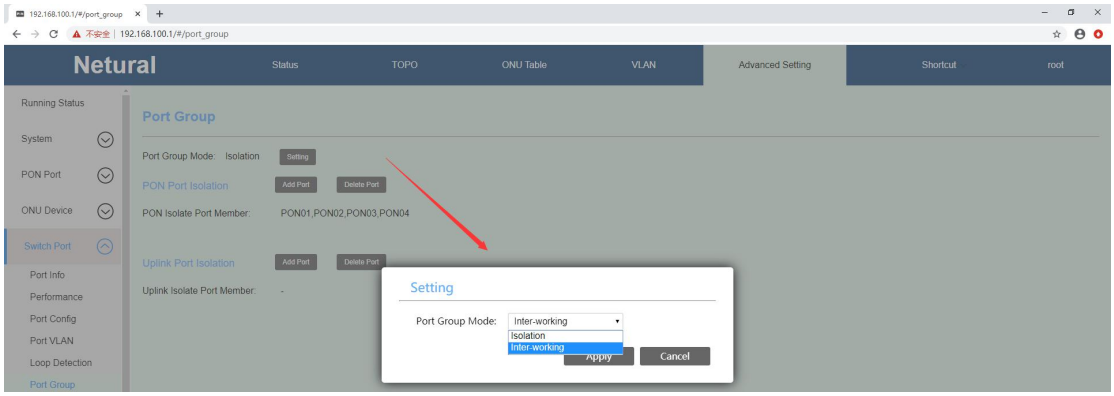
5.5.6.1 Port Isolation

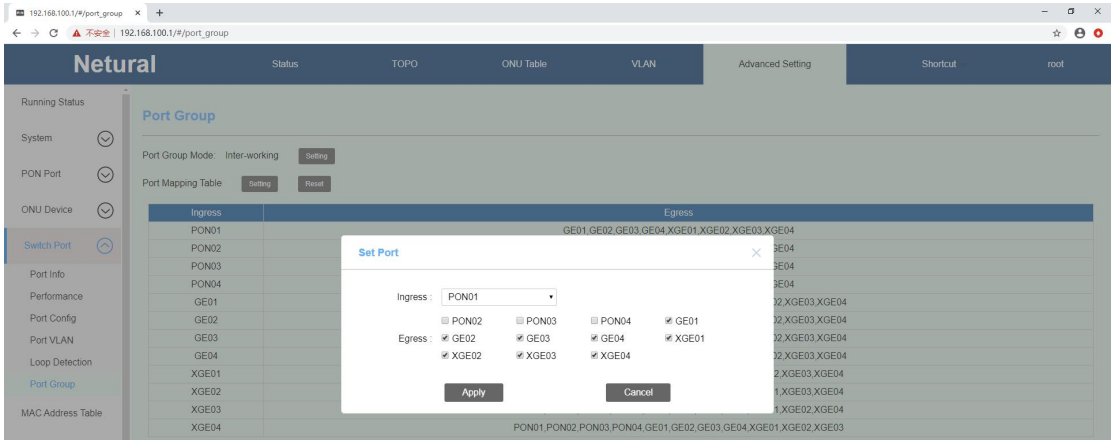
Enter the port group page, the current port group mode is isolation mode, you can click the "**Add Port**" and "**Delete Port**" buttons to configure port isolation. By default, PON port isolation is enabled and uplink port isolation is disabled. As shown below:



5.5.6.2 Port Inter-working

Enter the port group page, click the "**Setting**" button, select the inter-working mode. Enter the inter-working mode setting page, configure the inter-working group, first select the ingress port, and then select the egress port, the port group member ports can inter-communicate and isolate from the ports outside the group. As shown below:

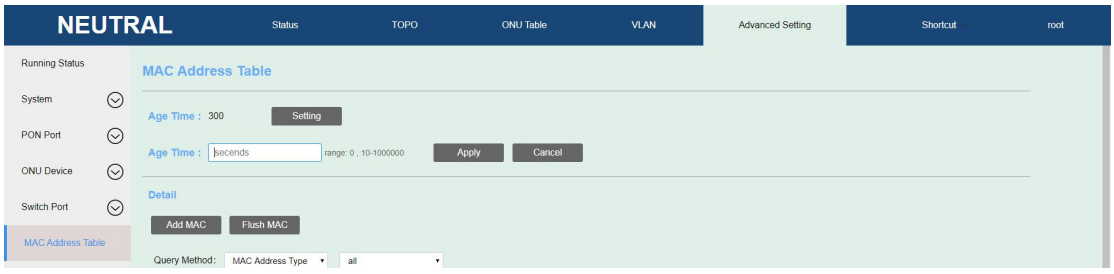




5.6 MAC Address Table

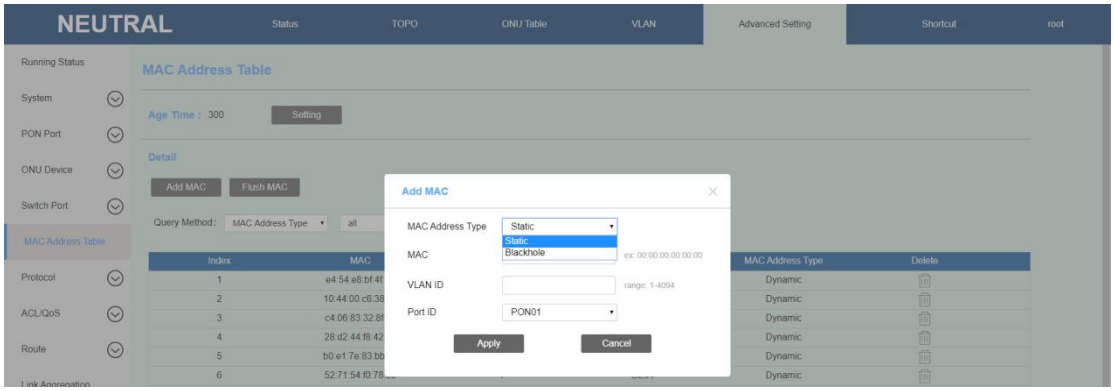
5.6.1 MAC Address Age Time

Choose **Advanced Setting** -> **MAC Address Table**, enter this page and click "**Setting**" button to modify the MAC address table age time. The default MAC address age time is 300S. As shown below:



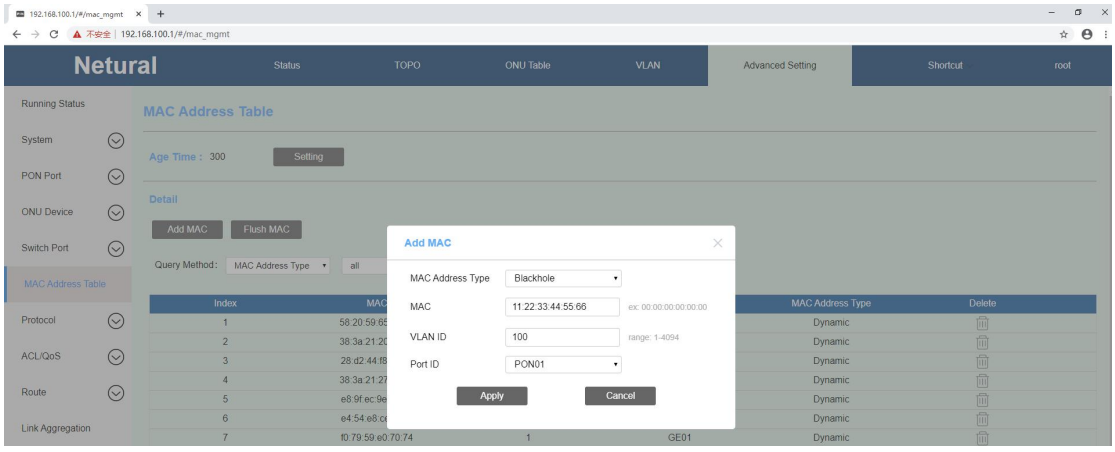
5.6.2 Add Static MAC Address

Choose **Advanced Setting** -> **MAC Address Table**, enter this page and click "**Add MAC**" button, and select the MAC address type as static MAC, as shown below:



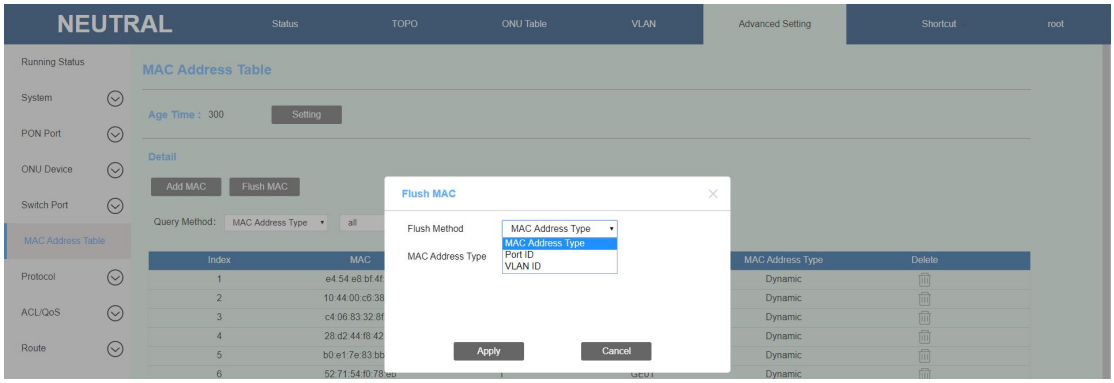
5.6.3 Add Blackhole MAC Address

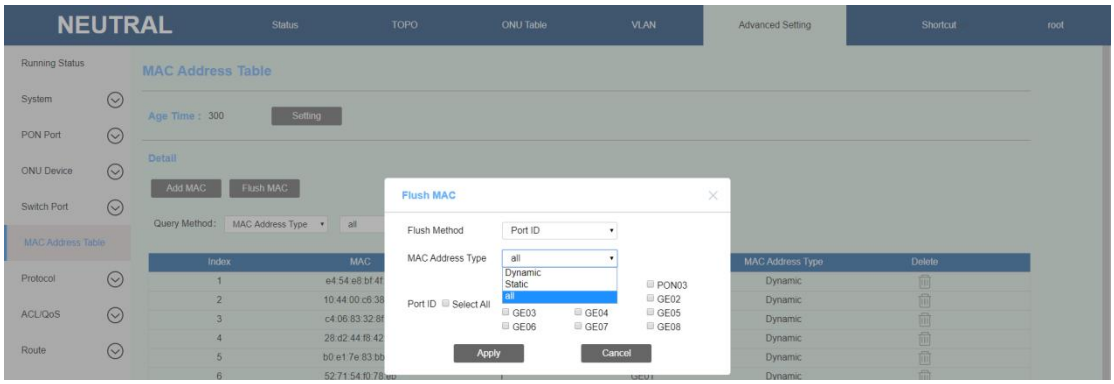
Choose **Advanced Setting** -> **MAC Address Table**, enter this page and click "**Add MAC**" button, and select the MAC address type as blackhole MAC, as shown below:

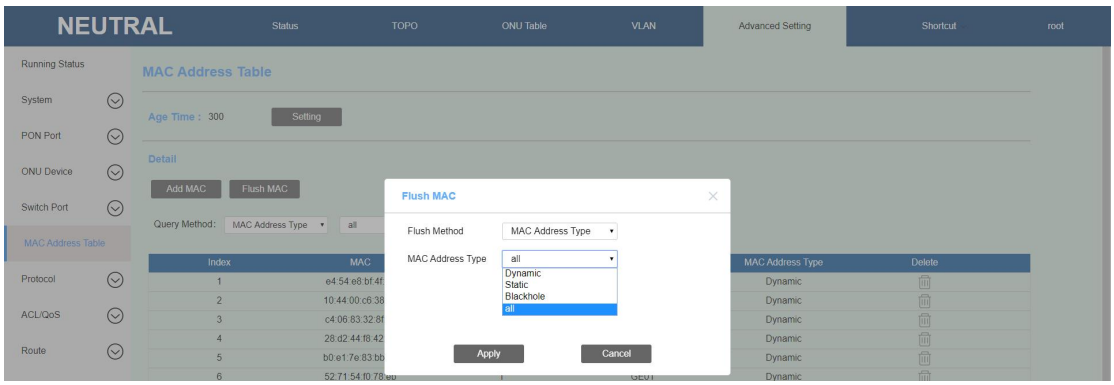


5.6.4 Delete MAC Address

Choose **Advanced Setting** -> **MAC Address Table**, enter this page and click "**Flush MAC**" button. In the pop-up option box, you can select the port number or VLAN ID to delete the corresponding MAC, as shown below:

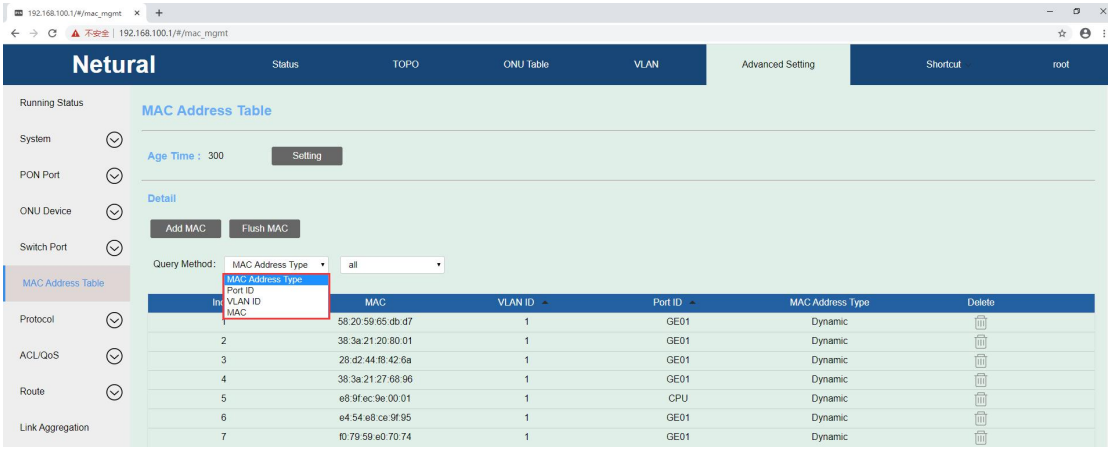






5.6.5 View MAC Address

Choose **Advanced Setting** -> **MAC Address Table**, enter this page and click "**Flush MAC**" button. In the pop-up option box, you can query the corresponding MAC address according to the MAC address type, port ID, VLAN ID, and MAC address, as shown below:

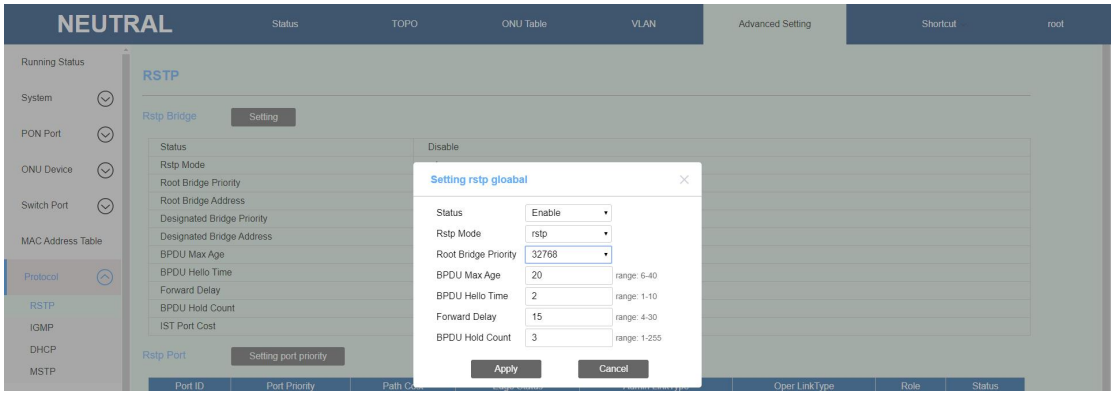


5.7 Protocol

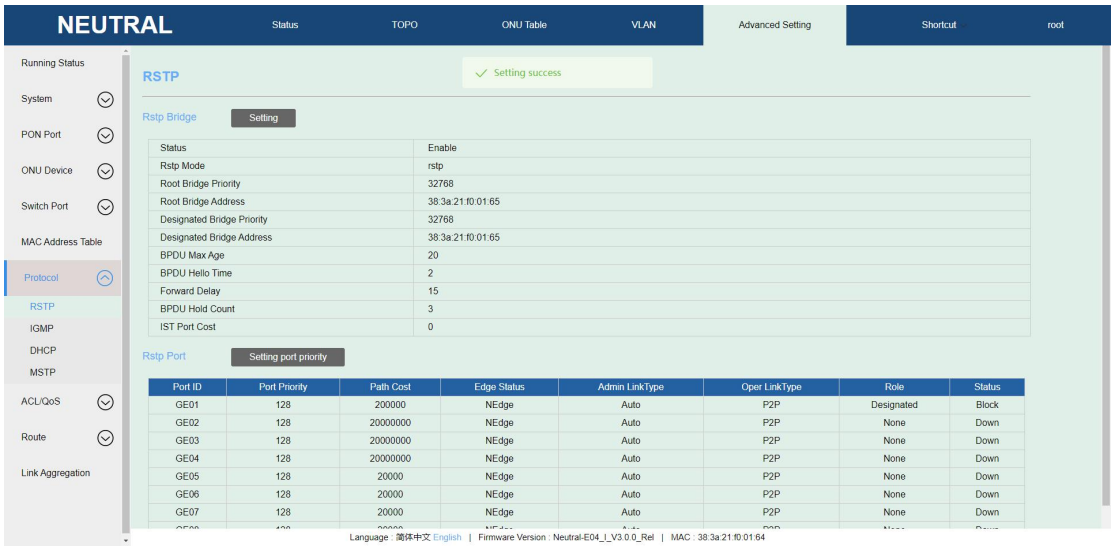
5.7.1 RSTP

Choose **Advanced Setting** -> **Protocol** -> **RSTP**, enter this page, you can view and configure RSTP protocol parameters, as shown below:

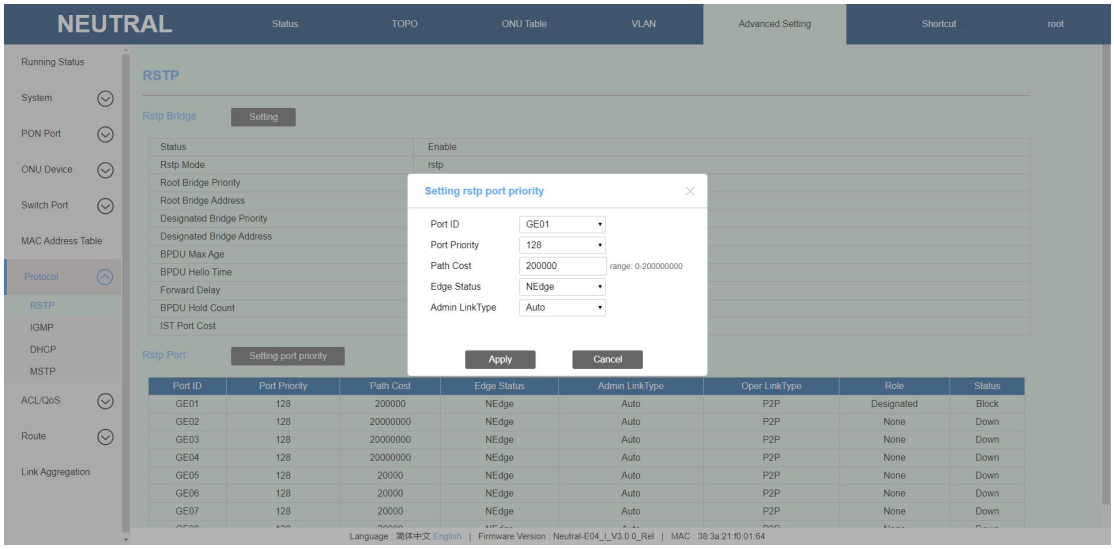
1. Set RSTP bridge parameters: Enter the RSTP page and click the "**Setting**" button to set RSTP global parameters, including RSTP status, mode, root bridge priority, etc., as shown below:



If setting successfully,you will get some result,it shows below:

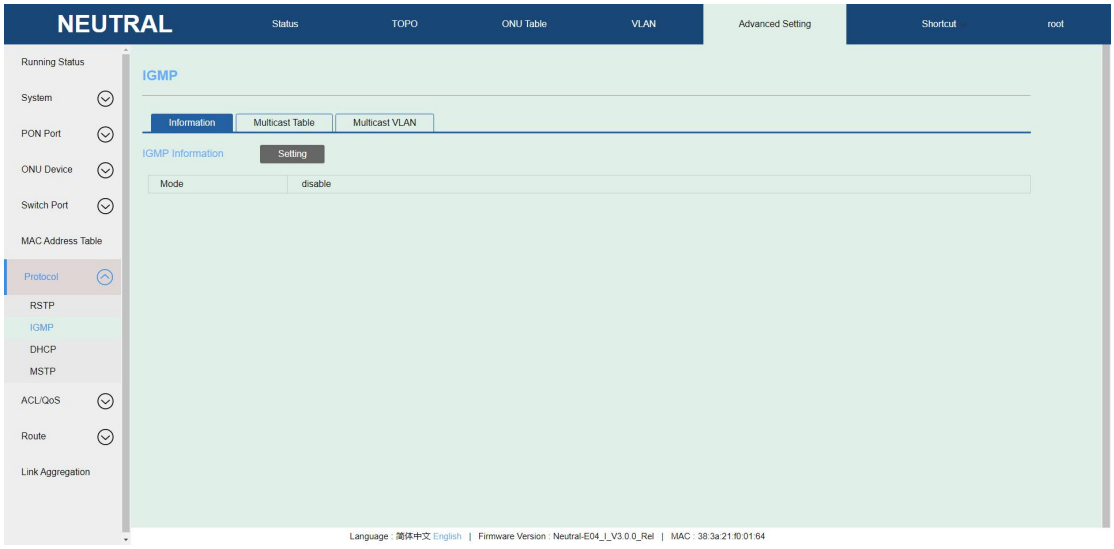


2. Set RSTP port parameters: Enter the RSTP page and click the "**Setting port priority**" button to set RSTP port parameters, including port priority, path cost, edge status and link type, as shown below:



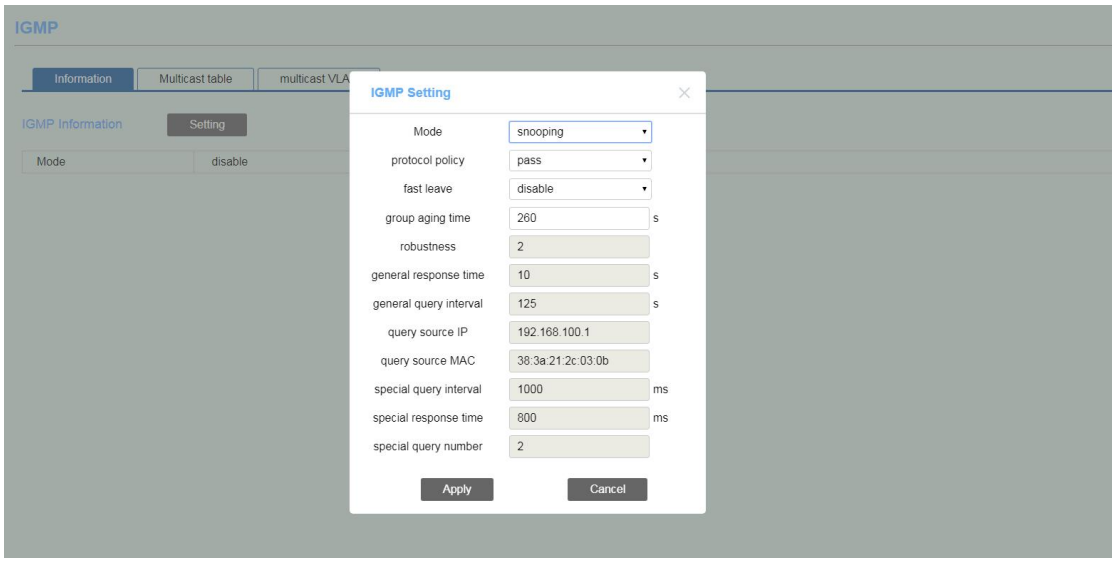
5.7.2 IGMP

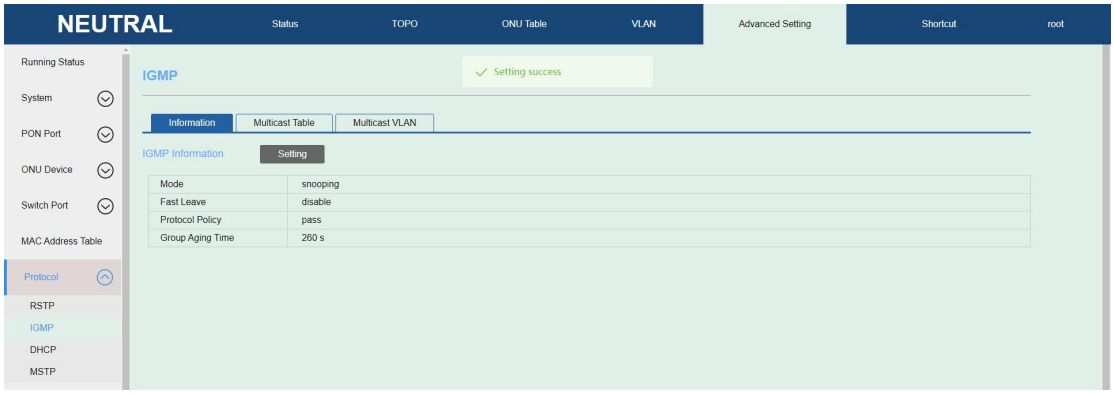
Select **Advanced Setting** -> **Protocol** -> **IGMP**, enter this page, you can view and set IGMP protocol parameters, the default mode is disable.



5.7.2.1 IGMP Snooping Mode

Enter the IGMP management page, click the "**setting**" button, and configure the IGMP mode as **Snooping** in the pop-up option box, as well as the protocol policy, fast leave and group aging time parameters. As shown below:





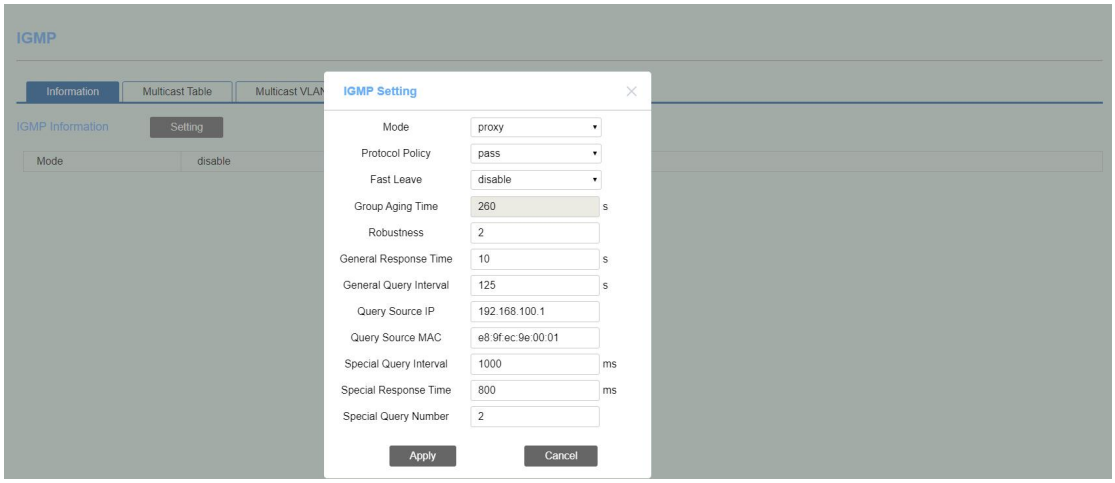
1> protocol policy: Whether IGMP protocol packets outside the multicast program are allowed to pass.

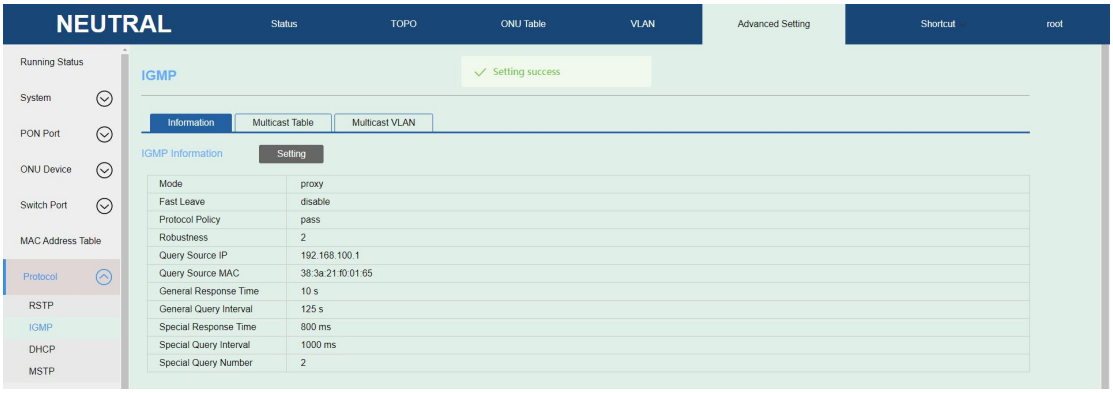
2> fast leave: When enabled fast leave, the device receives the IGMP leave packets and immediately disconnects the multicast service.When the device is not enabled fast leave, the multicast streams will be disconnected when the device fails to receive IGMP report packets within the maximum response time of general query or specific query.Default is not enabled.

3> group aging time: When the device does not receive IGMP report packets within the aging time, it is deemed that the user has gone offline and disconnected the user multicast service streams.The default is 260 seconds.

5.7.2.2 IGMP Proxy Mode

Enter the IGMP management page, click the "**setting**" button, and configure the IGMP mode as **Proxy** in the pop-up option box, as well as the protocol policy, quick leave, robustness, general response time, general query interval, query source IP and query source MAC address and other parameters. As shown below:





1> protocol policy: Same as above

2> fast leave: Same as above

3> robustness: This configuration can be used when the user wants to adjust the robustness coefficients, depending on the stability of the network.After setting, the system uses the robustness coefficient to confirm the aging time of the multicast user.The robustness coefficient is set to enhance the robustness of the system, which directly affects the aging time of multicast users and also affects the number of times to send generic group query messages.If a subnet may lose packets, the robustness factor should be added to ensure the stability of multicast users.The default is 2.

4> general response time: When the general query packet is sent, all online users will respond to the report packets within the response time, which is 10 seconds by default.

5> general query interval: When the device is in proxy mode, the device will send a general query packet at each general query interval.The default is 125 seconds.

6> query source IP: Configure the general query packet sent to the user side by the multicast router or the source IP address of a specific query packet, default is 192.168.100.1.

7> query source MAC: Configure the general query packet sent to the user side by the multicast router or the source MAC address of a specific query packet,default is device inbound address.

8> special query interval: For a specific program in accordance with the command to set the interval of send a specific set of queries to confirm that whether the user is watching the show, not received the report user feedback message, that the user is not in watching the show, the system is no longer sent to the user, the program

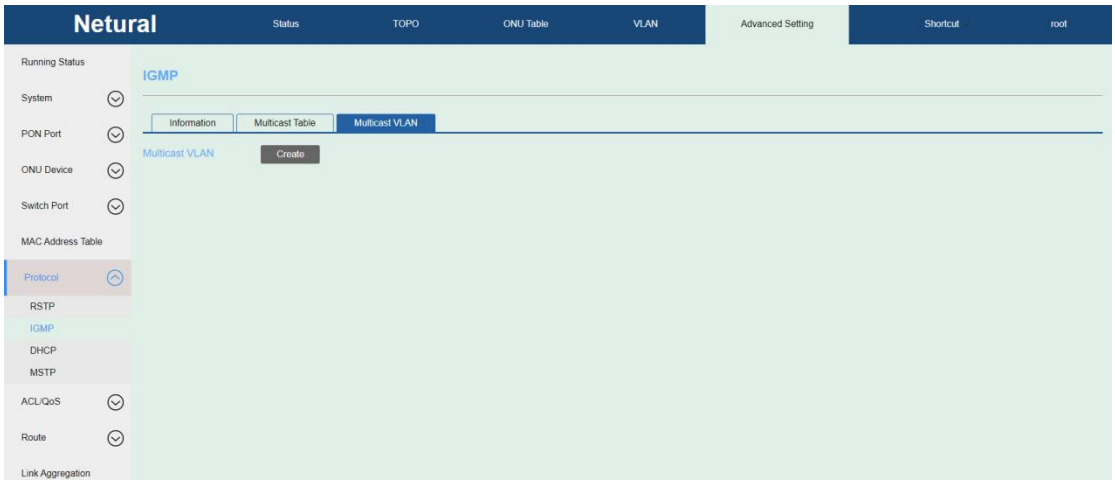
flow to avoid users do not have television still receive multicast flows and the waste of bandwidth.The default is 1000 milliseconds.

9> special response time: A specific set of queries is sent N times for a particular program (N is set by this command) to confirm that the user is watching the program, default is 2 times.

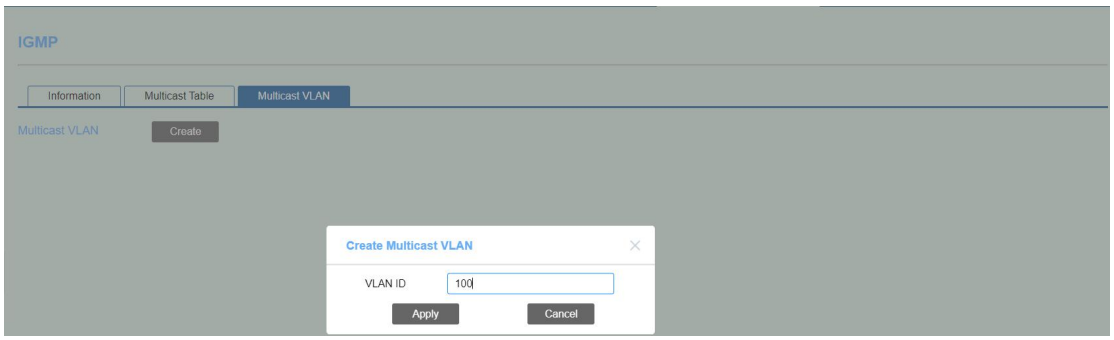
10>special query number: After a specific query packets are sent, all online users will respond to the report packets within the response time, which is 800 milliseconds by default.

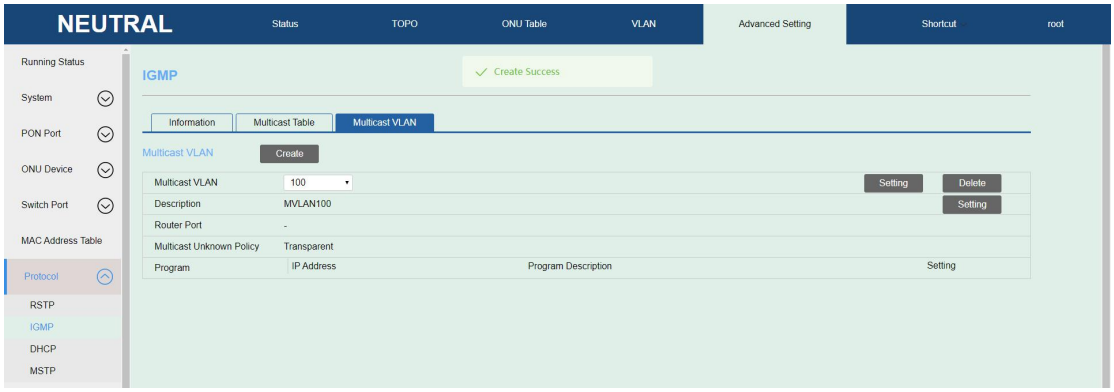
5.7.2.3 Multicast VLAN

Enter the IGMP page and select the "**Multicast VLAN**" option to view and configure the multicast VLAN related parameters .

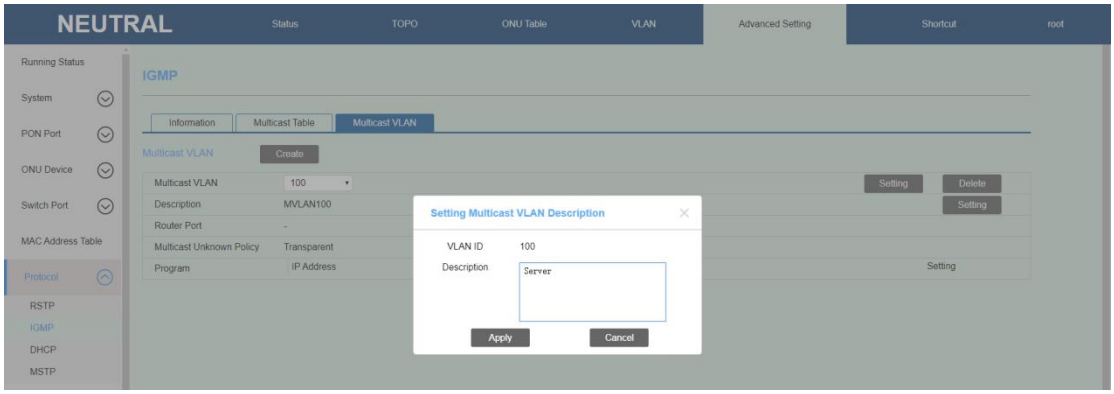


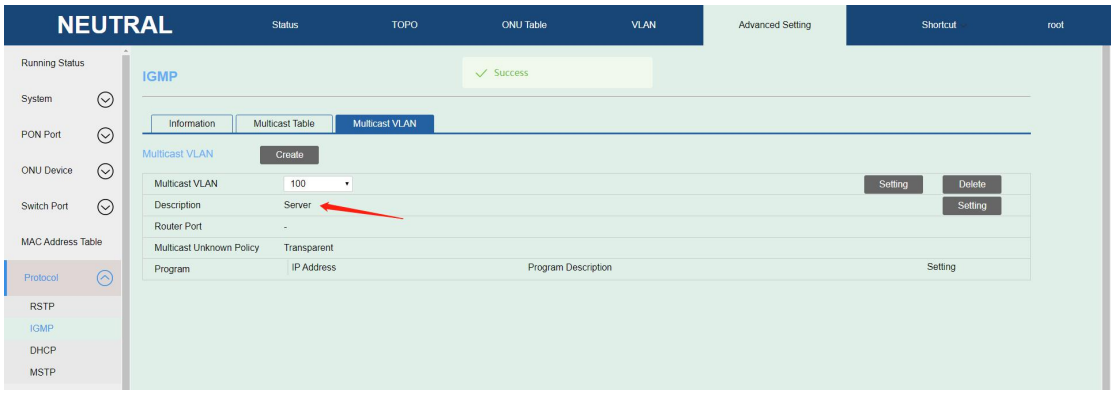
1. Click the "**Create**" button to add a multicast VLAN. The VLAN must exist to be successfully created. As shown below:



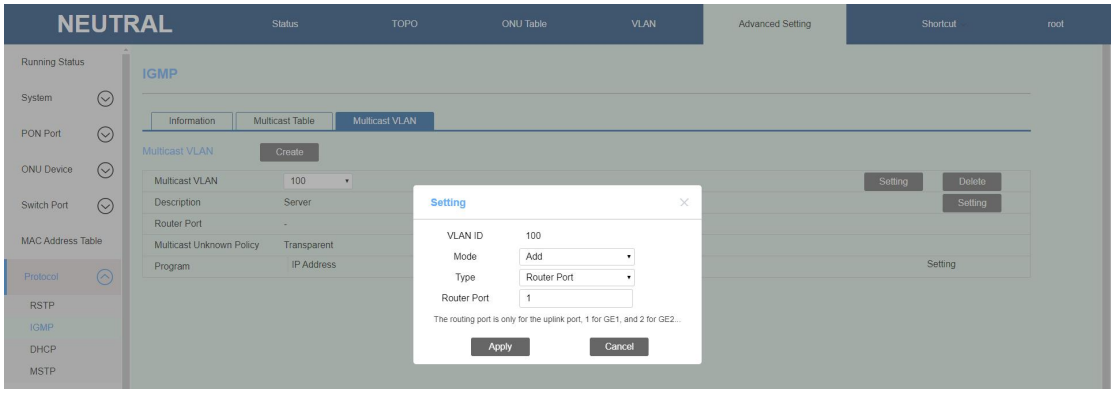


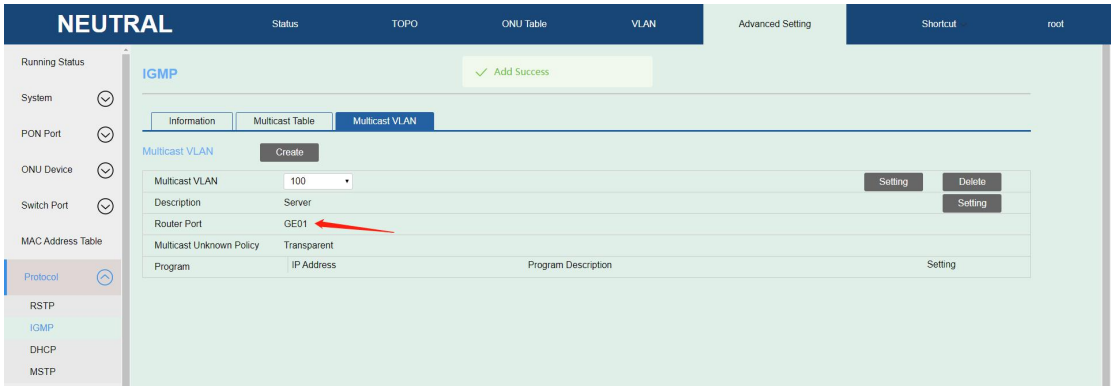
2. Configure the multicast VLAN description information, as shown below:



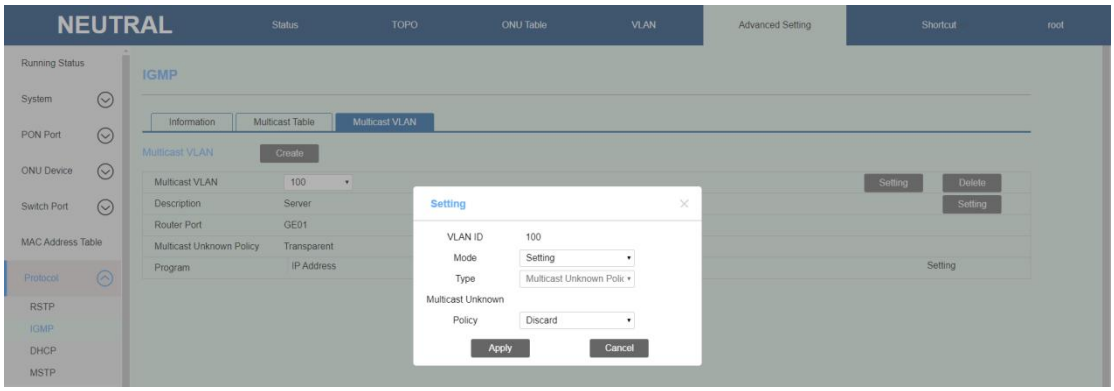


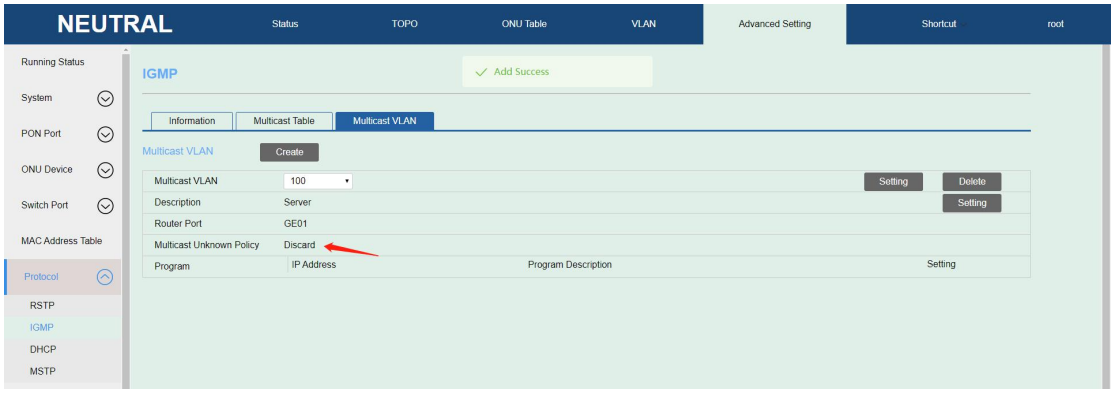
3. Configure IGMP router port.The IGMP router port is uplink ports, to connect IGMP program servers.



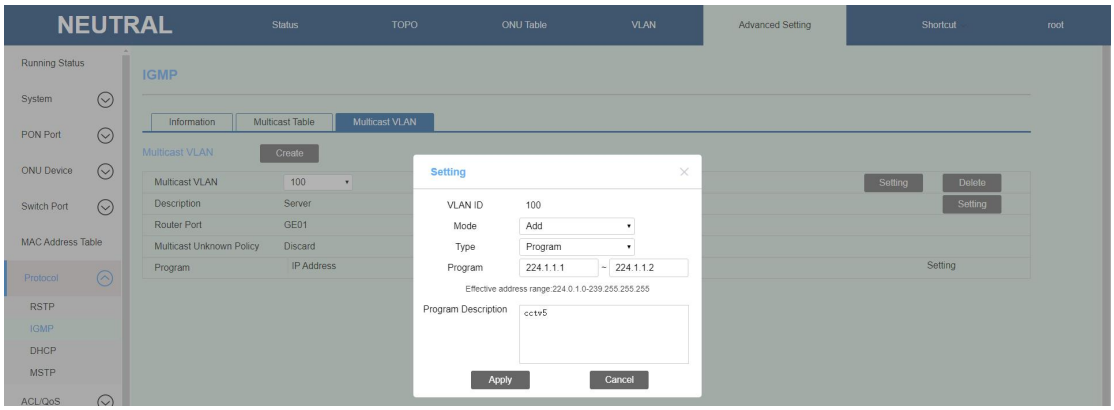


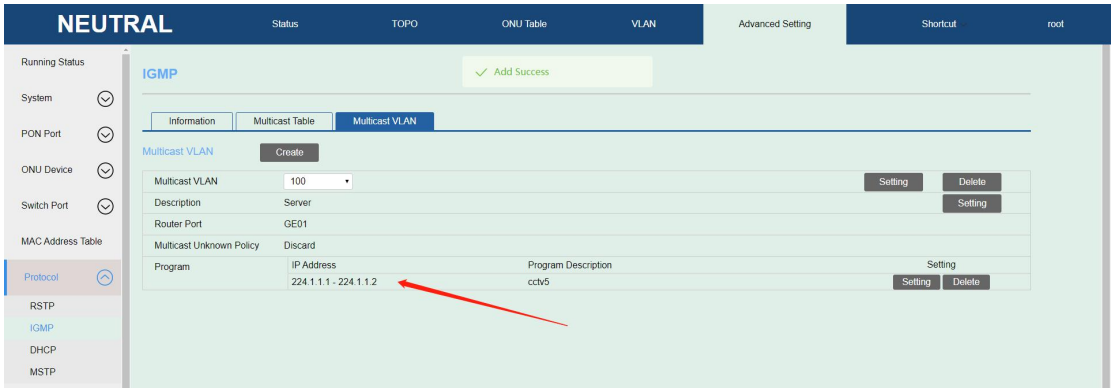
4. Configure multicast unknown policy. Configure the suppression strategy for unknown multicast traffic.If the business flow hosts unknown multicast for a specific purpose, it is configured for pass through.Unknown multicast with no special purpose consumes bandwidth and is typically configured to be discarded.





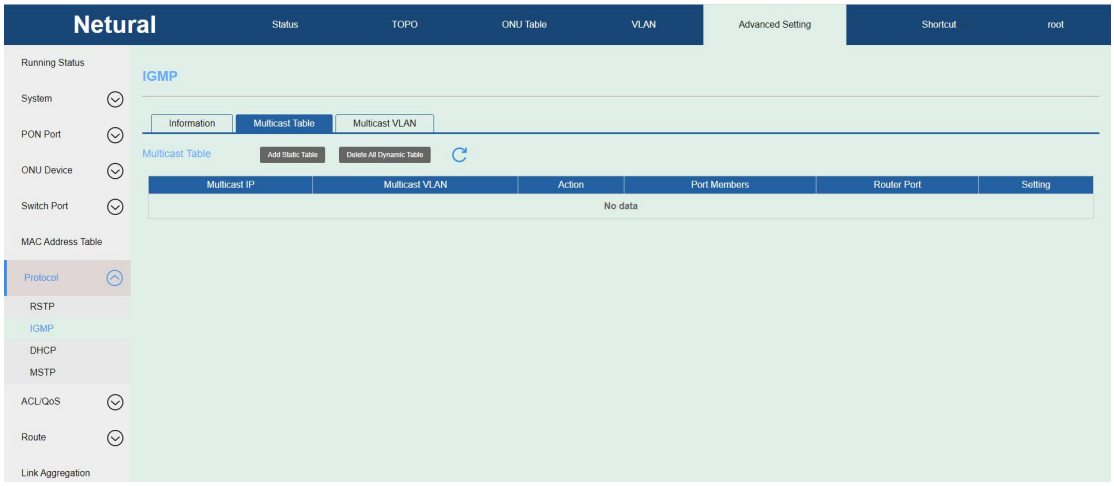
5. Configure IGMP program. Add the program library, users can switch to the multicast VLAN program channel.



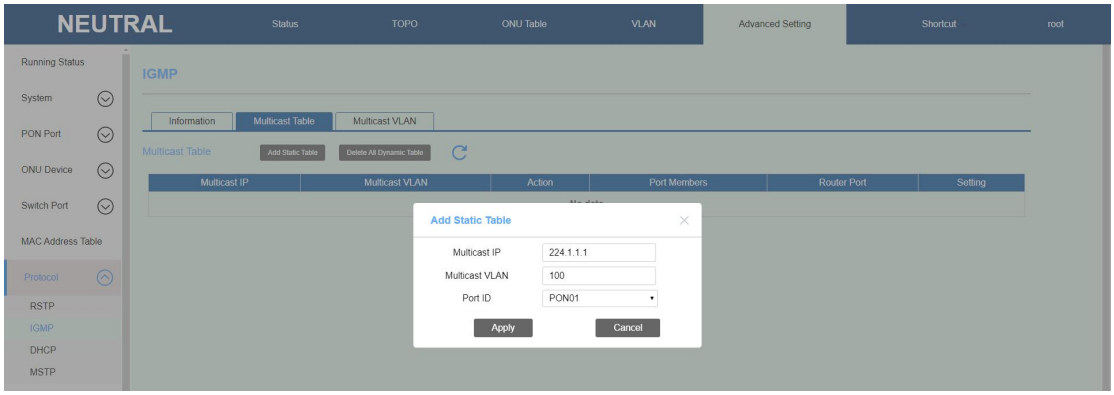


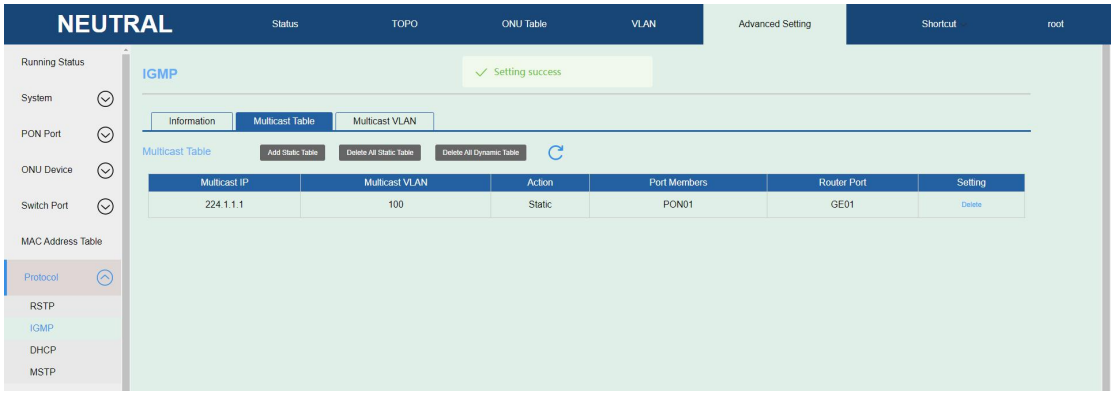
5.7.2.4 Multicast Table

Enter the IGMP page and select the "**Multicast Table**" option to view and configure the multicast table related parameters.

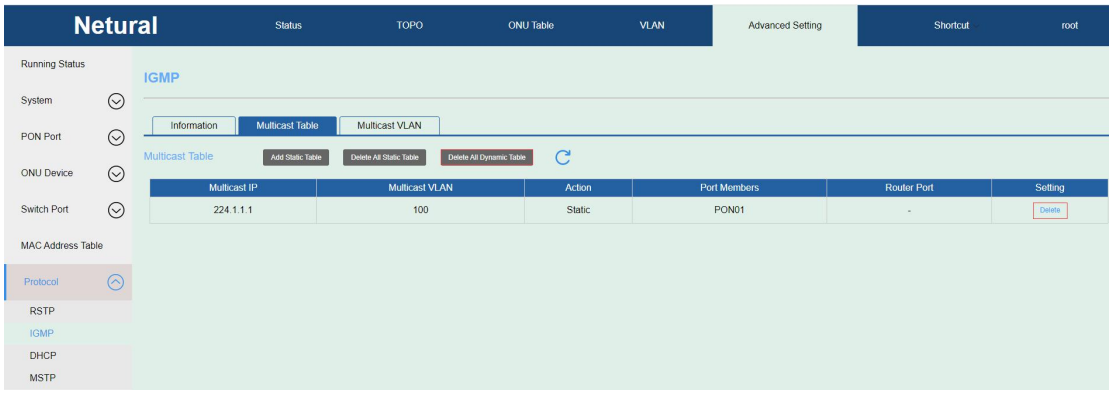


1. Configure static multicast table, click "**Add Static Table**" as shown below:





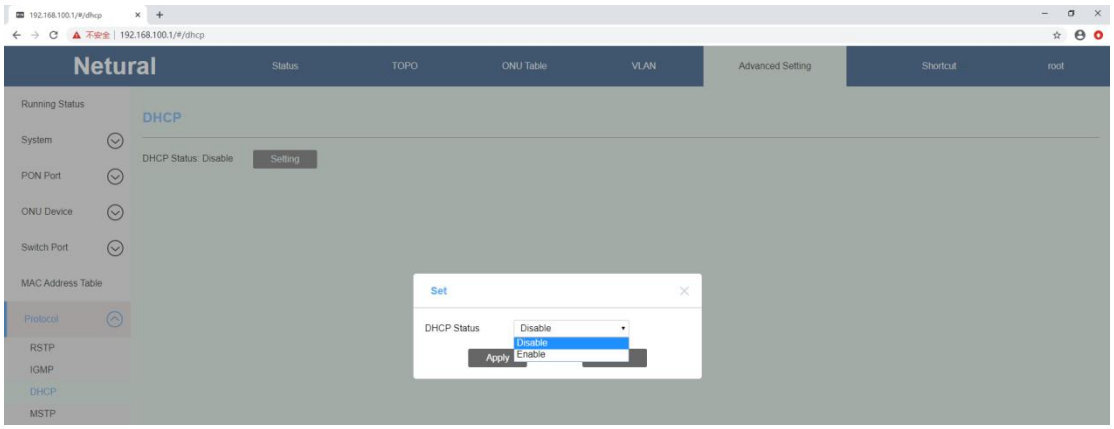
2. Delete Multicast table,as shown below:



Note: there are static multicast table items and dynamic multicast table,static multicast table do not aging.

5.7.3 DHCP

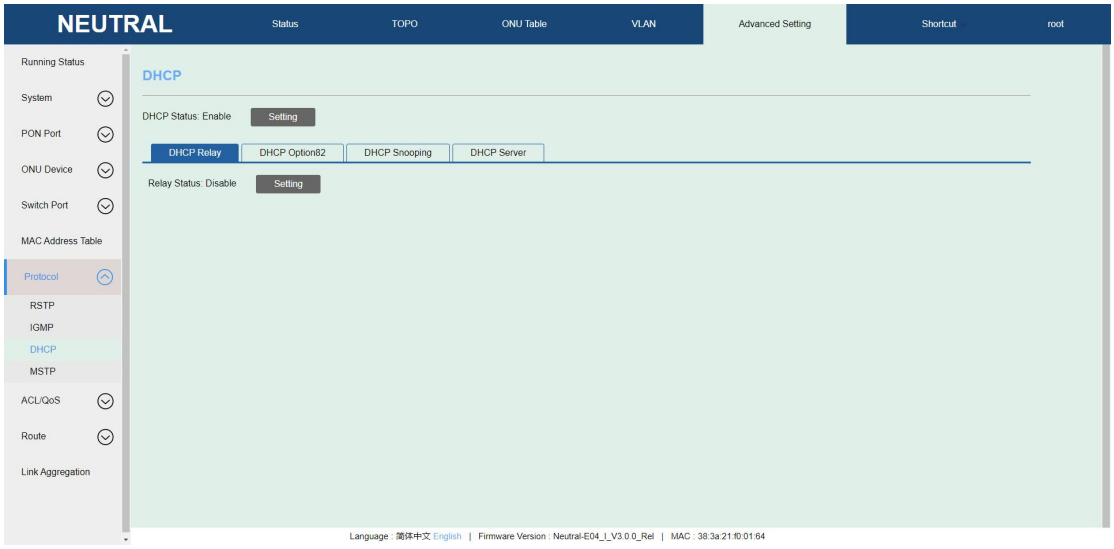
Select **Advanced Setting** -> **Protocol** -> **DHCP**, enter this page, click the "**Setting**" button to enable DHCP, and then you can configure the DHCP function parameters. This device supports the configuration of DHCP Snooping function, DHCP Relay function, DHCP Option82 function and DCHP Server function. As shown below:



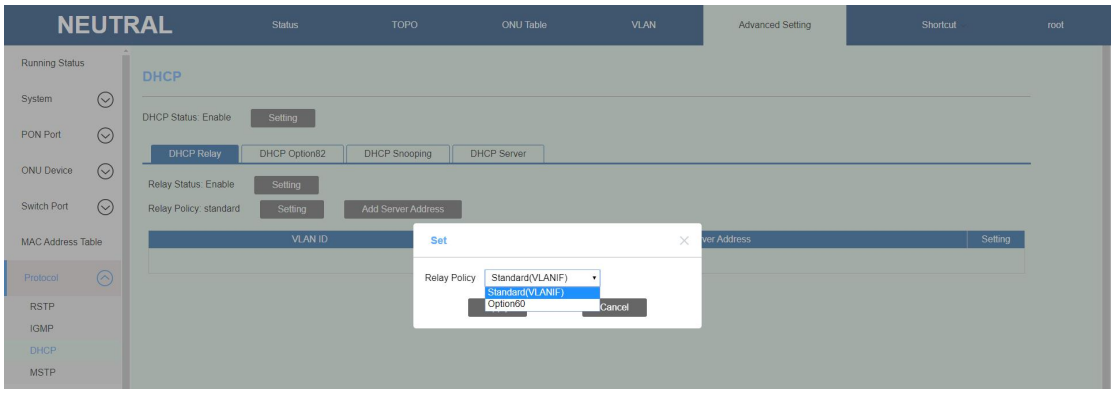
5.7.3.1 DHCP Relay

It works in three layers,which enables the request message of DHCP client to be sent to the specified DHCP server.Default status is disable.

Tips: Before enable the DHCP relay function,you need to ensure that the DHCP function is enabled and the IP route function is also enabled.Besides,to enable the configuration of related functions of the DHCP relay,you need to ensure that the DHCP relay function is enabled.



1. Configure DHCP Relay policy. Click the "**Setting**" button of the relay policy, and in the pop-up option box, you can select standard policy (default policy) or Option60 policy. As shown below:



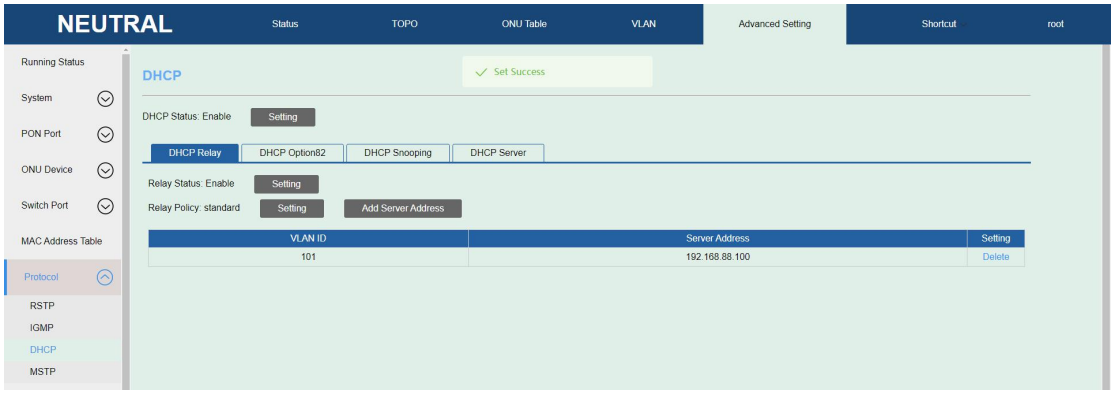
There are two strategies for DHCP relay:

(1)Standard policy(default policy):Finding DHCP server address baesd on VLAN.

(2)Option60 policy:Finding server address according to the option60 region value carried by the DHCP client.

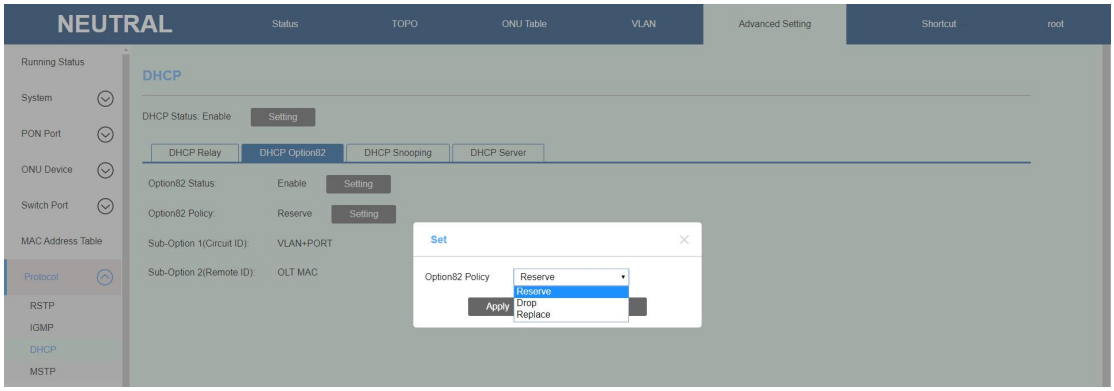
Tips: Switching policy will clear the server table established by another policy.

2. Click "**Add Server Address**" to add the corresponding server address in the pop-up option box. The device supports a maximum of 32 server tables, as shown below:



5.7.3.2 DHCP Option82

In order to enhance the security of DHCP server and improve the IP address configuration policy,a DHCP option is proposed.Default status is disable.



There are three strategies for DHCP Option82:

1) Reserving policy(default policy):If the client sends a request message without option82 information, OLT will bring option82 information. If the client sends it with option82 information, OLT will not process the direct forwarding server.

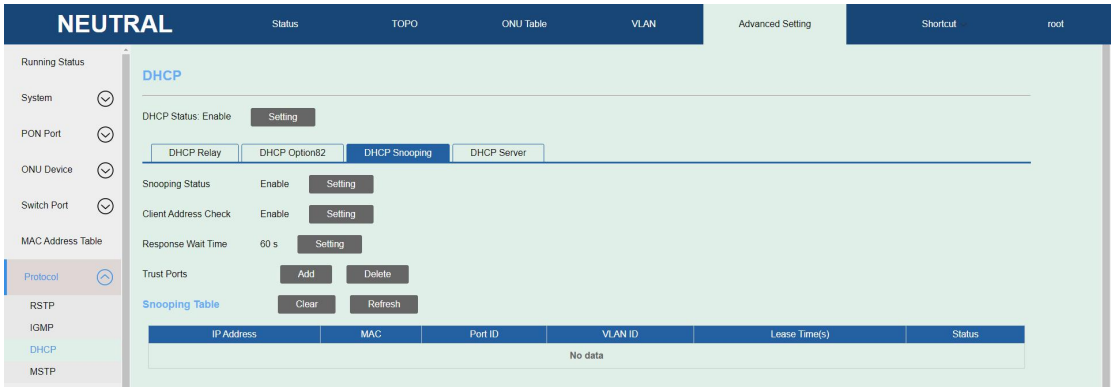
2) Dropping strategy: The client sends the request message without option82 information, and the OLT does not process the direct forwarding server. If the client sends the message with option82 information, the OLT strips the option82 information and forwards it to the server.

3) Replacement strategy: If the request message sent by the client does not contain option82 information, OLT will not process the direct forwarding server. If the message sent by the client contains option82 information, OLT will replace the option82 information and then forward the server.

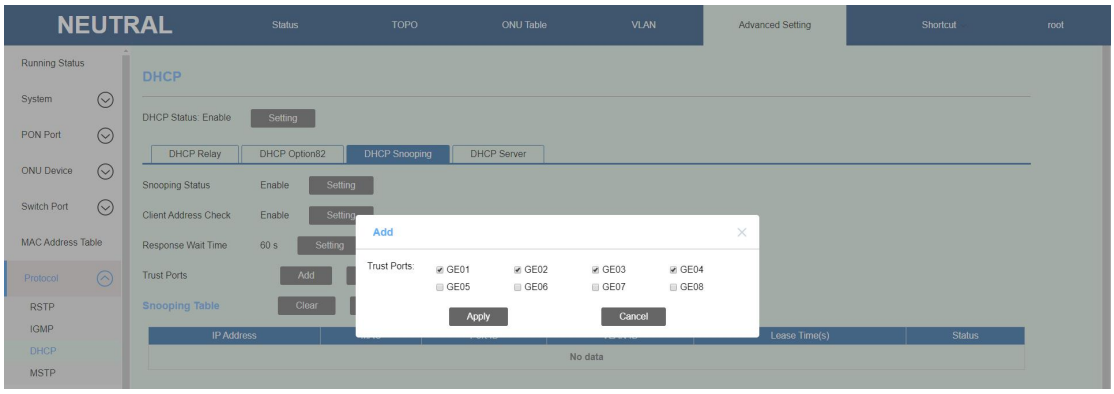
5.7.3.3 DHCP Snooping

The DHCP snooping function records the user's IP / MAC information by monitoring the message interaction between the DHCP client and the server. Default status is disable.

Tip: To open the DHCP snooping function, you need to ensure that the DHCP function is turned on.To open the DHCP snooping related function configuration, you need to ensure that the DHCP snooping function is turned on.



Add trust ports

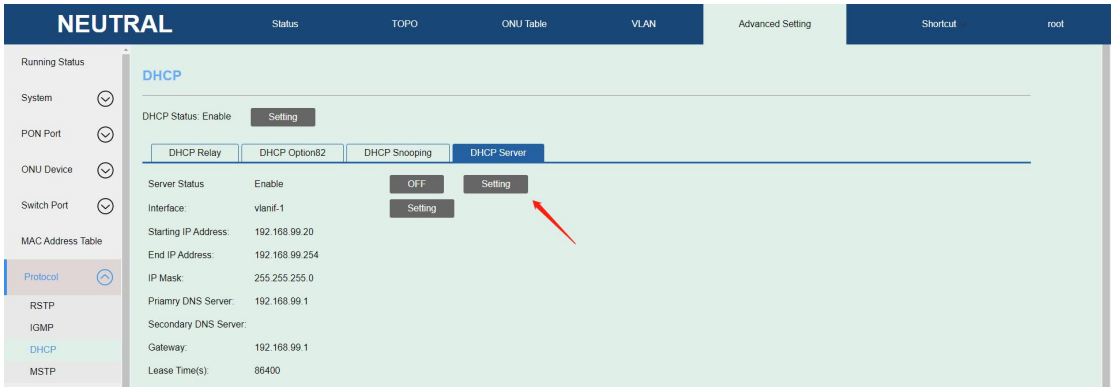


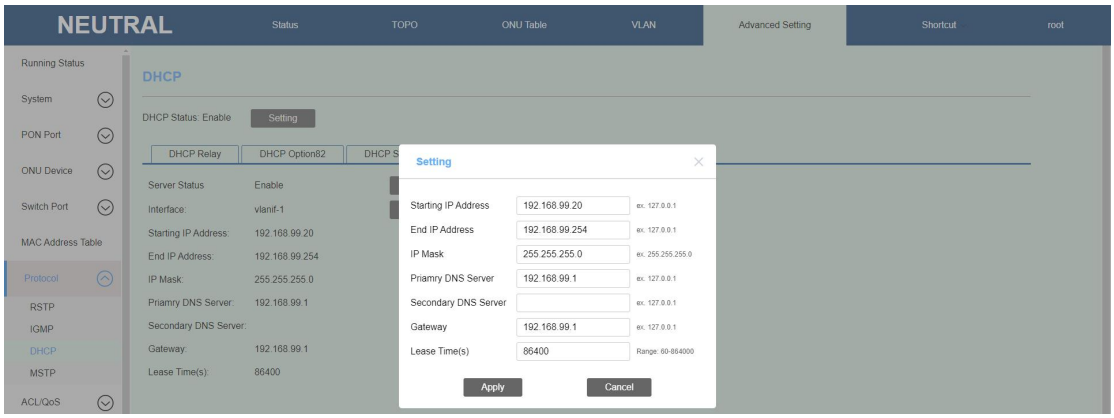
This configuration is only available for the upper interface. The trust port allows to receive all DHCP messages, and the non trust port does not allow to receive DHCP response messages. All ports are not trusted by default.

5.7.3.4 DHCP server

Default status is disable.Please turn off the function of DHCP relay, DHCP option82 and DHCP snooping before opening.

After enabling, you can start to configure the DHCP server. The default is in band management network segment, and the interface is the logical port vlanif-1.

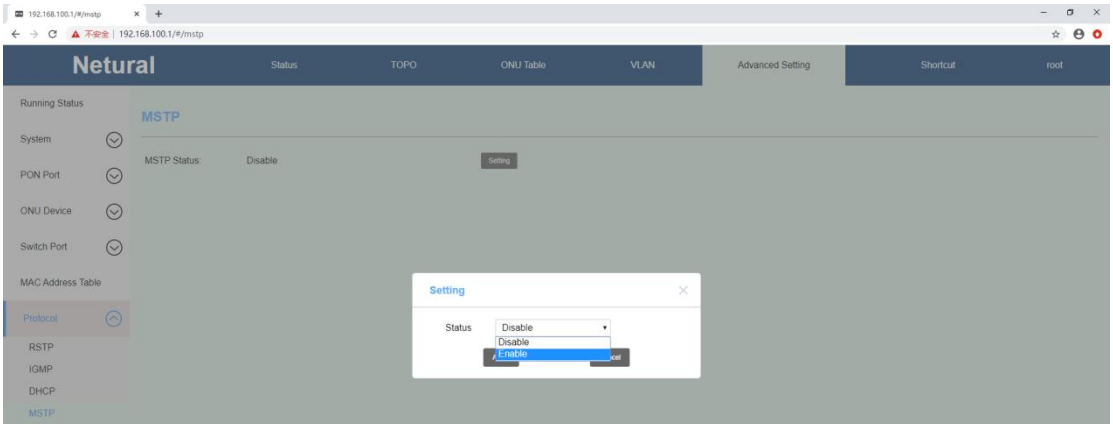


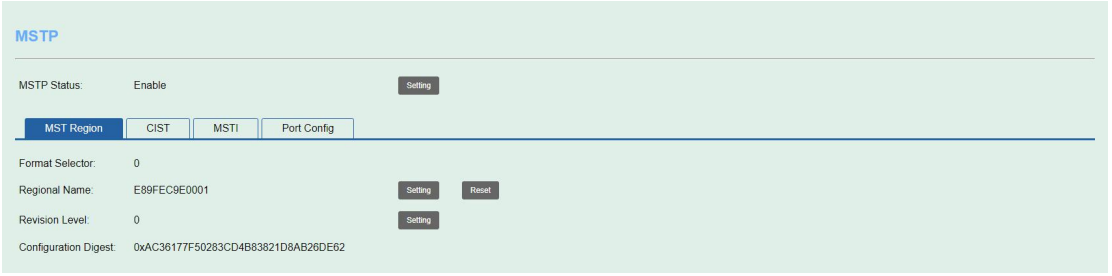


5.7.4 MSTP

MSTP is compatible with STP and RSTP, which can not only converge rapidly, but also make the traffic of different VLAN forward along their own paths, thus providing a better load sharing mechanism for redundant links. Through MSTP, a switching network is divided into multiple regions, each region forms multiple spanning trees, and the spanning trees are independent of each other. Each spanning tree is called MSTI (multiple spanning tree instance), and each region is called MST region (multiple spanning tree region).Default status is disable.

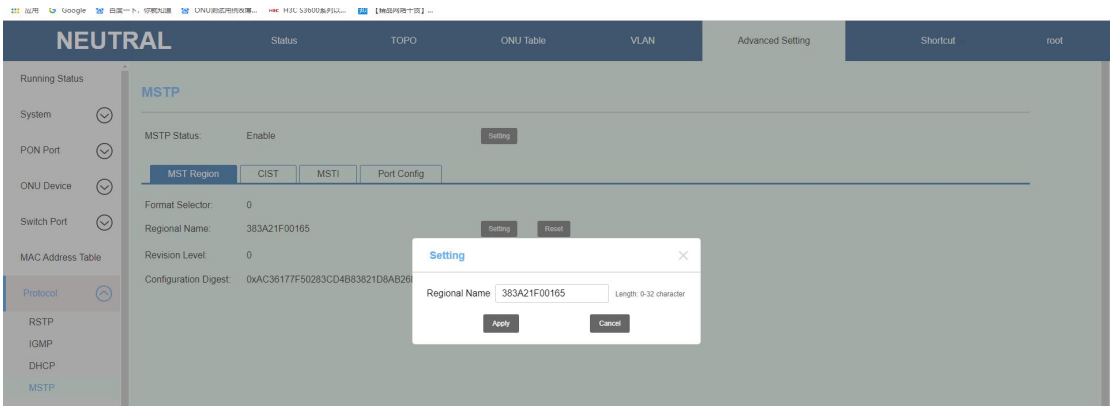
Choose **Advanced Setting** -> **Protocol** -> **MSTP**, enter this page, click the "**Setting**" button to enable MSTP, and then you can configure the MSTP parameters. As shown below:



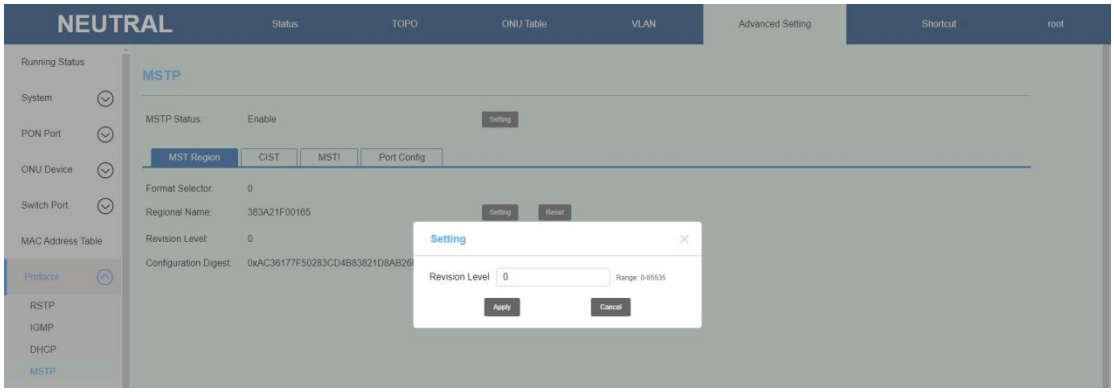


5.7.4.1 MST Region

It is composed of multiple devices in the switching network and the network segments between them. A LAN can have multiple MST regions. Each MST region is directly or indirectly connected. Multiple devices can be divided into the same MST region by MSTP configuration command.



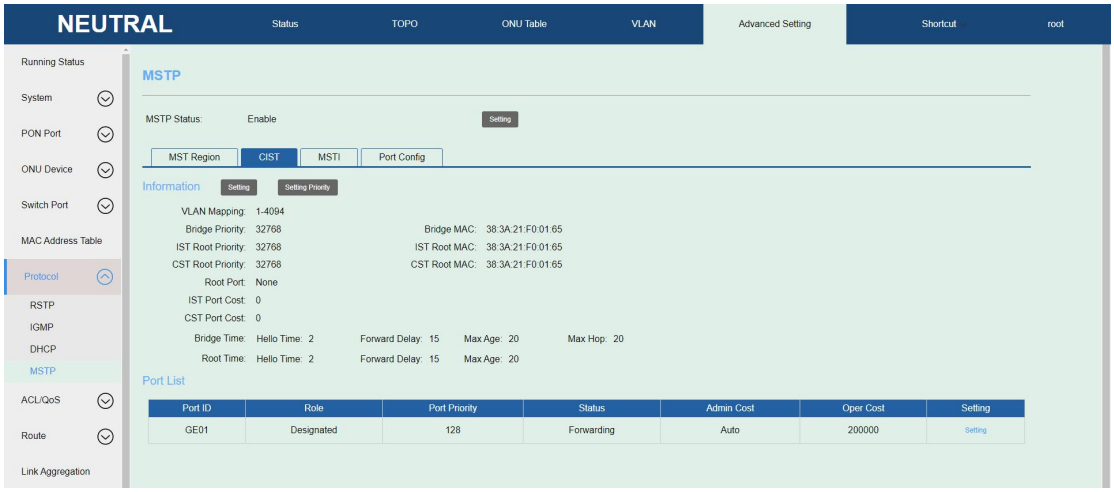
The configurable length of the region name is 0-32 bits, and it will be restored to system MAC after reset.



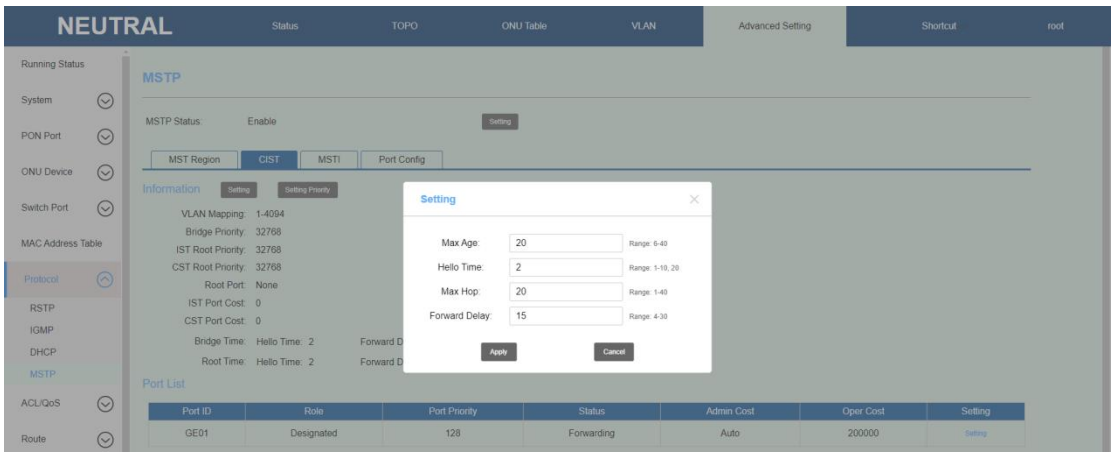
The configurable range of the modified version is 0-65535.

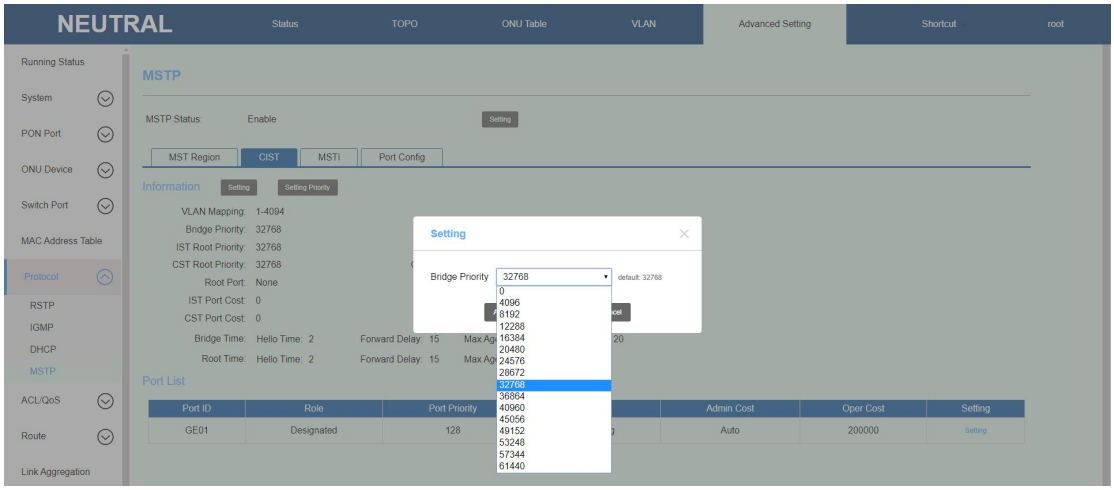
5.7.4.2 CIST

MSTP generates IST (a spanning tree in each MST region) through calculation in each MST region. At the same time, MSTP treats each MST region as a single switching device, and generates CST (a spanning tree connecting all MST regions in the switching network) between MST regions through calculation. CIST is a single spanning tree connecting all devices in a switching network, which is composed of IST and CST. VLAN mapping table is an attribute of MST region. It describes the mapping relationship between VLAN and MSTI. The default value is 1-4094.



Configuration interface and priority





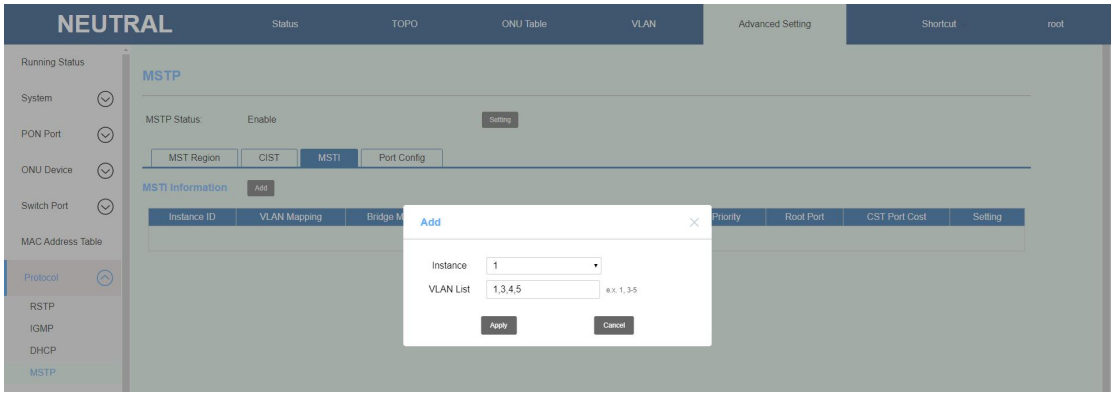
5.7.4.3 MSTI

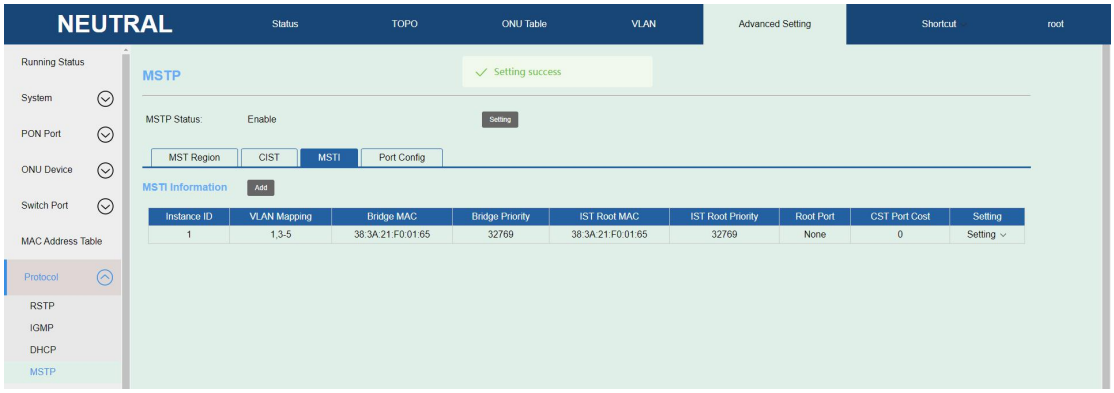
In one MST region, multiple spanning trees can be generated through MSTP, and each spanning tree is independent of each other, with the following characteristics:

1) Each MSTI computes its own spanning tree independently and does not interfere with each other.
2) The calculation method of the spanning tree of each MSTI is basically the same as that of STP.
3) Each MSTI spanning tree can have different roots and different topology.
4) Each MSTI sends BPDU in its own spanning tree.
5) The topology of each MSTI is determined by command configuration.
6) The spanning tree parameters of each port on different MSTI can be different.
7) The role and status of each port on different MSTI can be different.
8) In the network running MSTP protocol, a VLAN message will be forwarded along the following path:

① Within the MST region, forward along its corresponding MSTI.

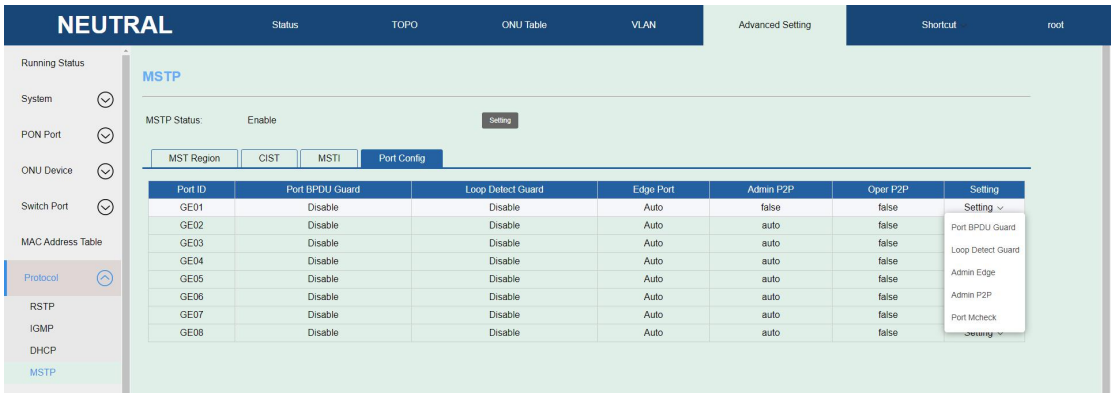
② Between MST regions, forward along CST.

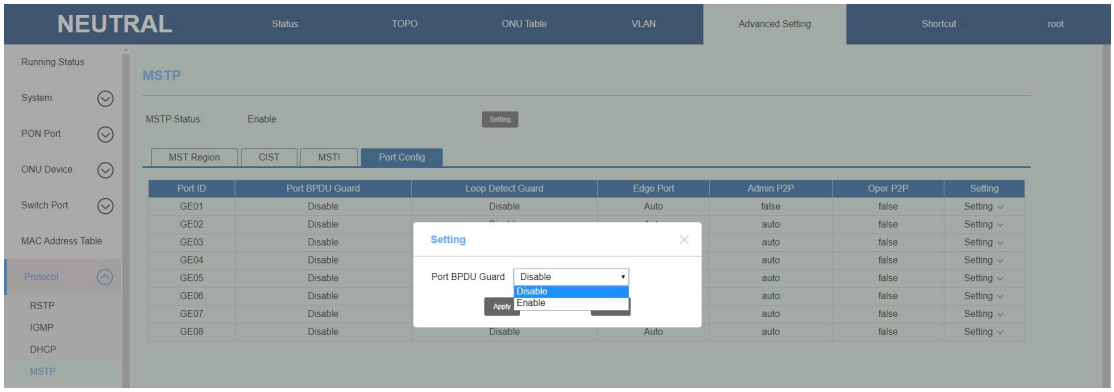




5.7.4.4 Port Configuration

You can switch of BPDU protection, loop protection, edge port and P2P functions of each Ge port quickly.





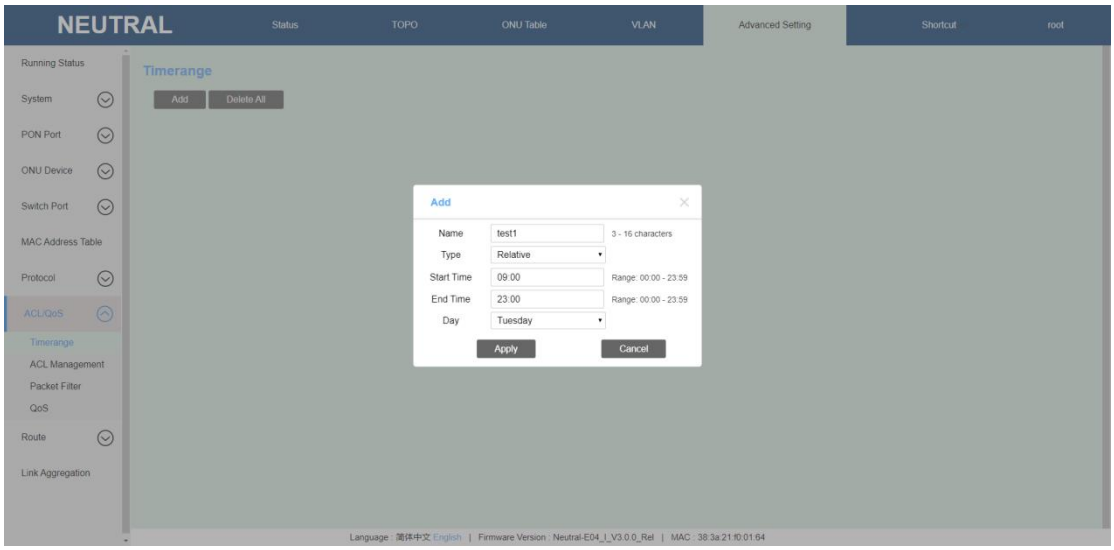
5.8 ACL/QOS

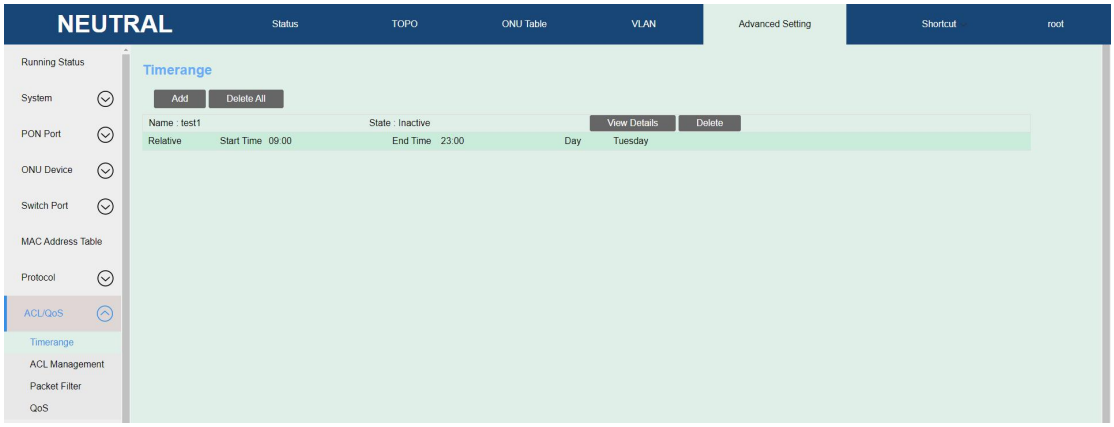
5.8.1 Time-range

It is used to specify a time period for the ACL rule to take effect.Once the configuration is executed successfully, the ACL rule can be created to specify the effective time by referring to the time period name, and the ACL rule is only valid for the effective time period.

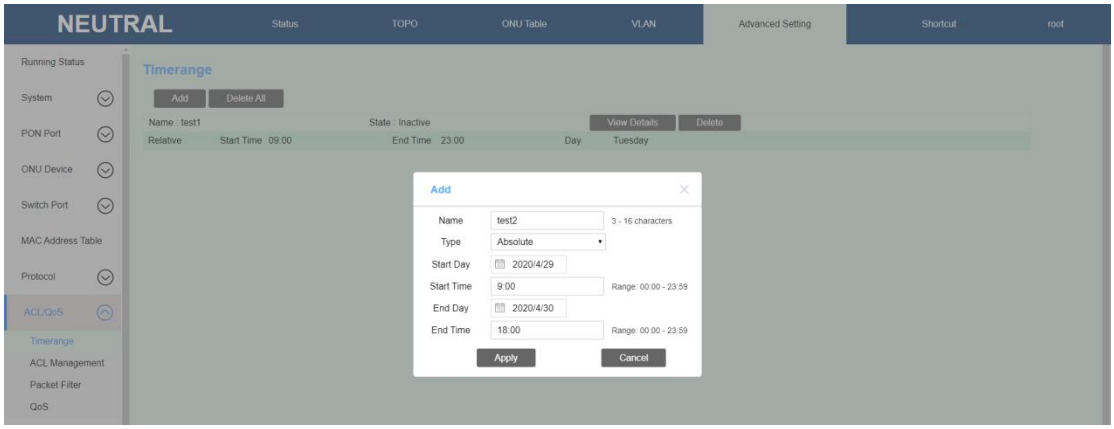
1. Add time-range

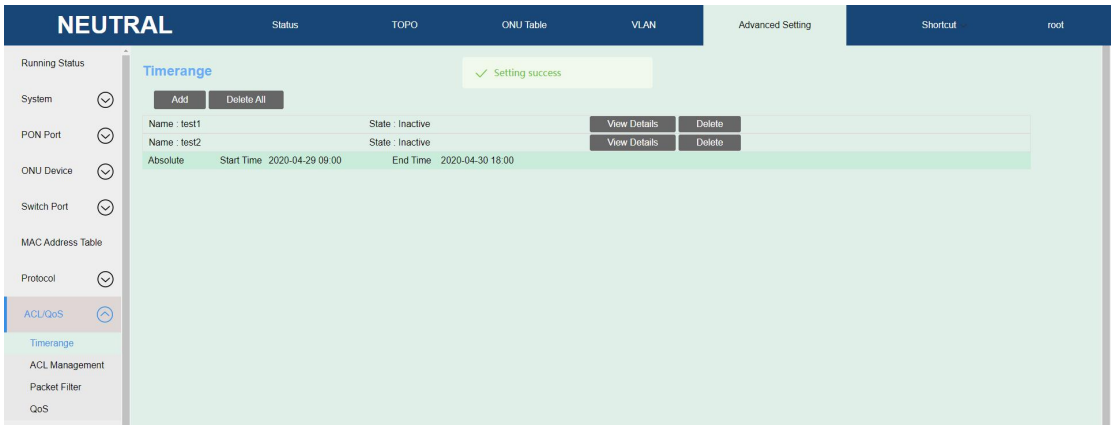
    1> Relative time: A periodic time, for example, Monday from 09:00 to 18:00





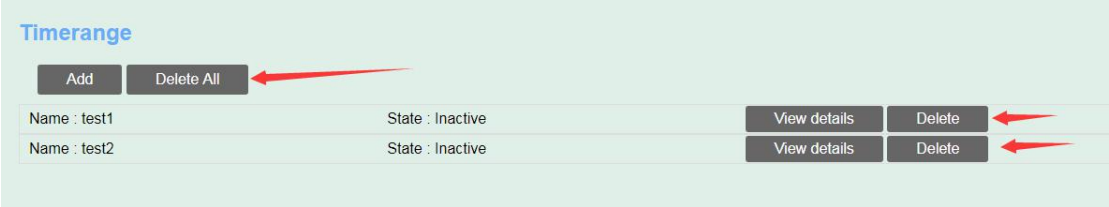
2> Absolute time: From a specific time to a specific time, such as 9:00 on April 29, 2019 to 18:00 on April 29, 2019.





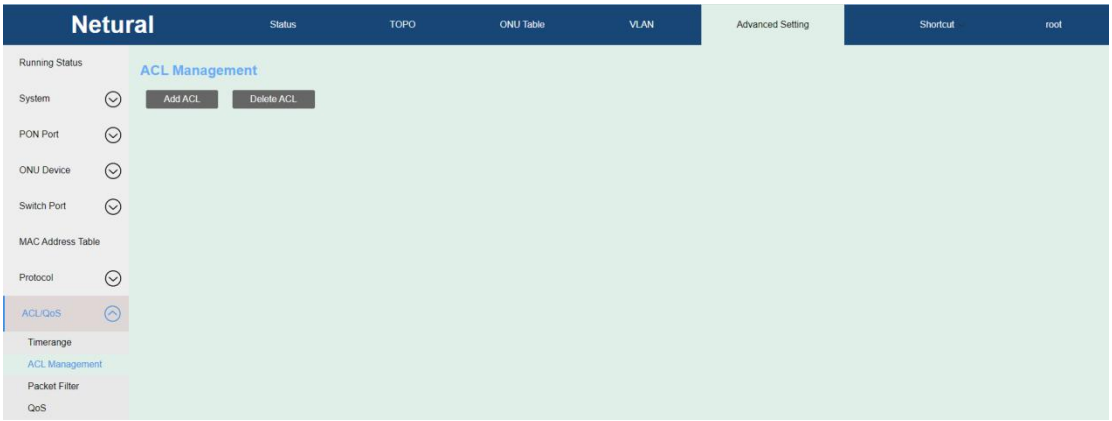
2. Delete Time-range

You can delete one by one or delete all, as shown below:



5.8.2 ACL Management

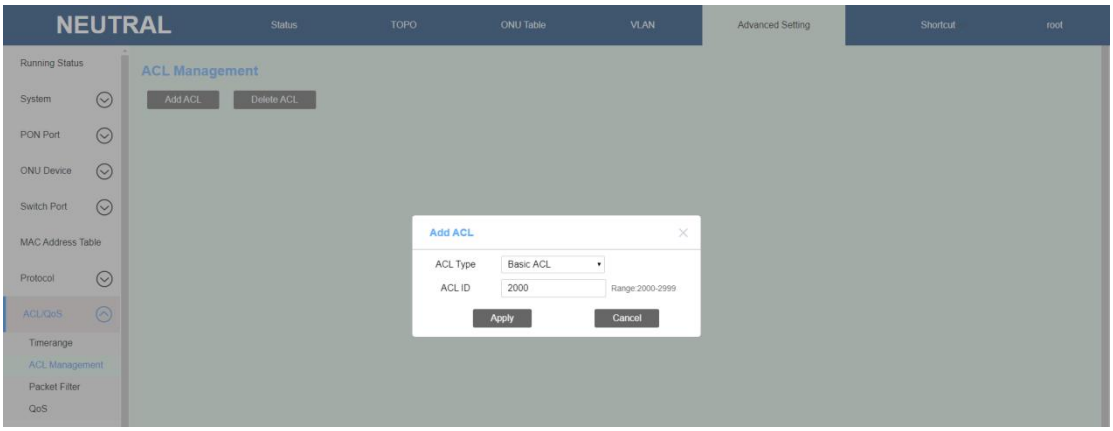
Use this configuration to create an access control list when you need to filter specific packets through matching rules. Select **Advanced Setting** -> **ACL/QOS** -> **ACL Management**, enter this page, you can configure ACL rules, as shown below:



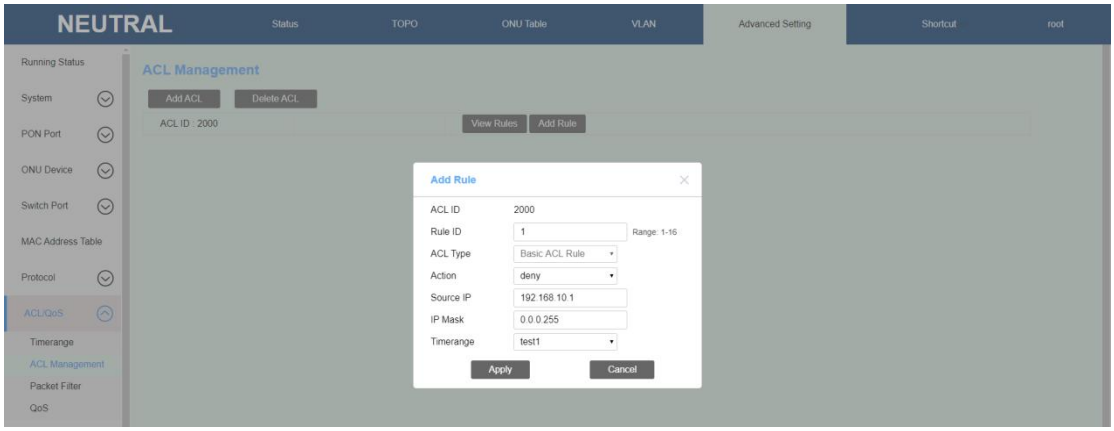
5.8.2.1 Basic ACL

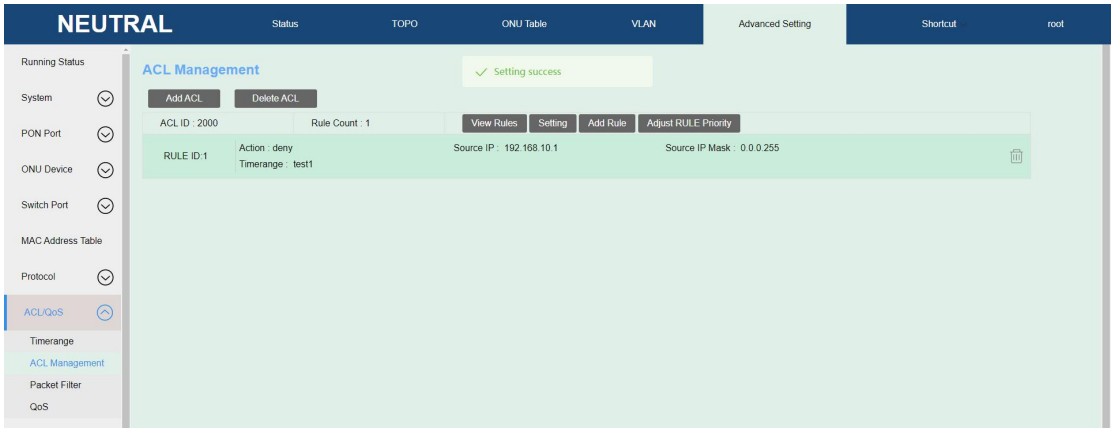
Use this configuration when ACL rules need to be made based on the IP address of the source of the message. After successful rule creation, packet-filter configuration reference rules can be used to filter packets.

1. Create basic ACL, the ID range is 2000-2999. As shown below:



2. Add rule:You can select time range take effect within the specified time or not select time range for immediate effect.

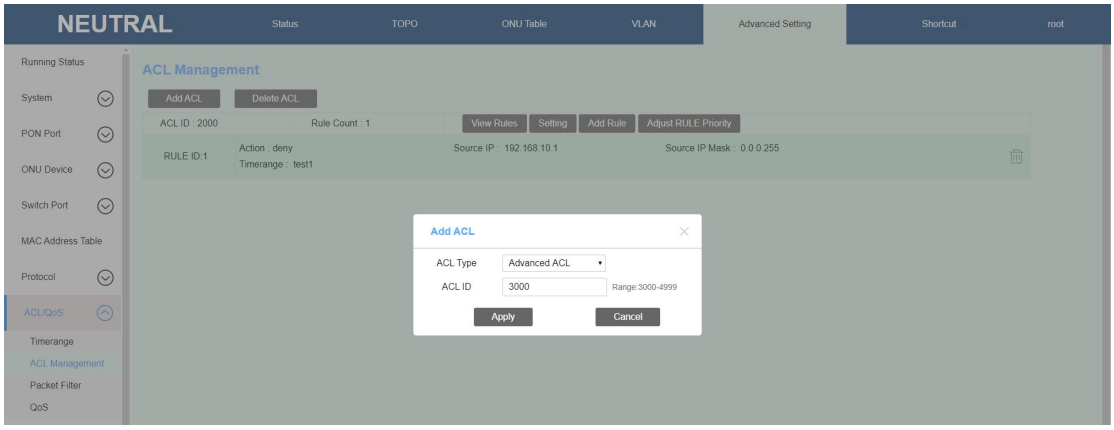




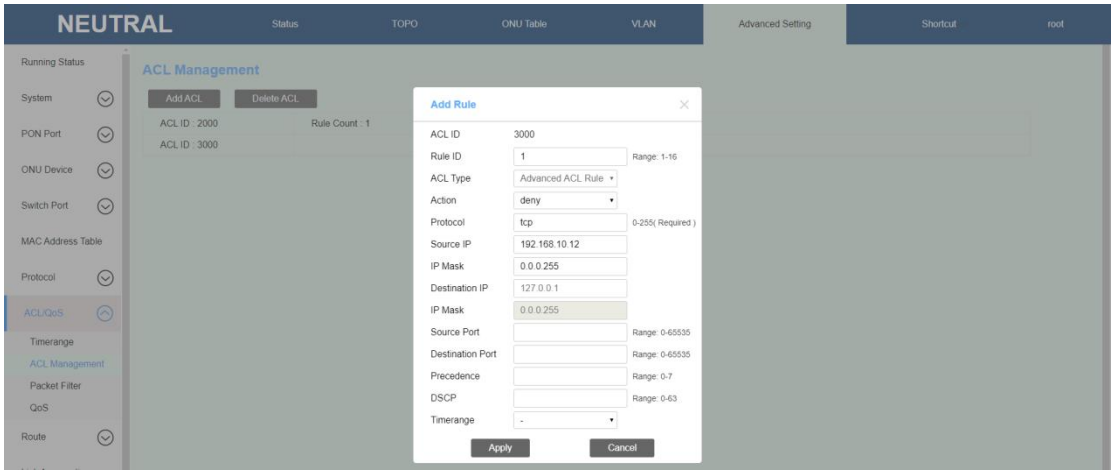
5.8.2.2 Advanced ACL

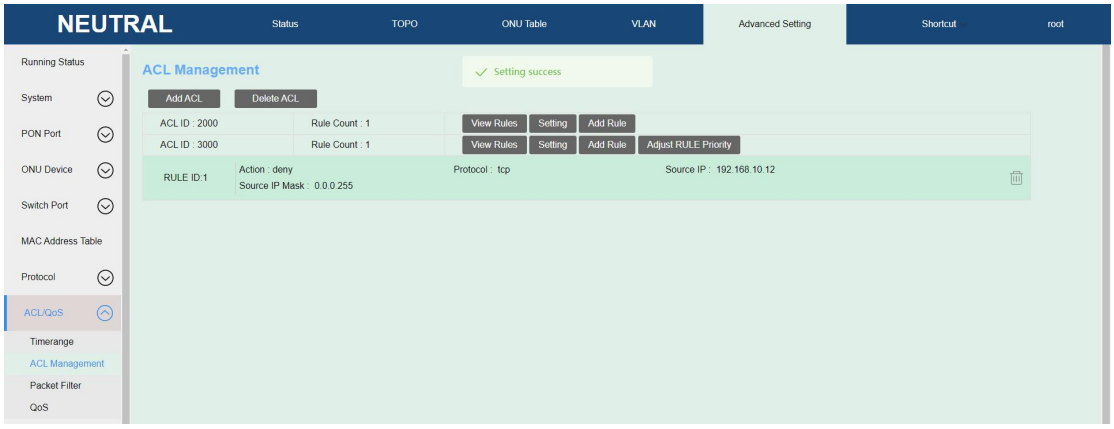
This configuration is used when matching rules need to be made based on the packet's source address information, destination address information, the protocol type hosted by the IP, and the characteristics of the protocol. After successful rule creation, packet-filter configuration reference rules can be used to filter packets.

1. Create Advanced ACL, the ID range is 3000-4999. As shown below:



2. Add Rule: You can select time range take effect within the specified time or not select time range for immediate effect.



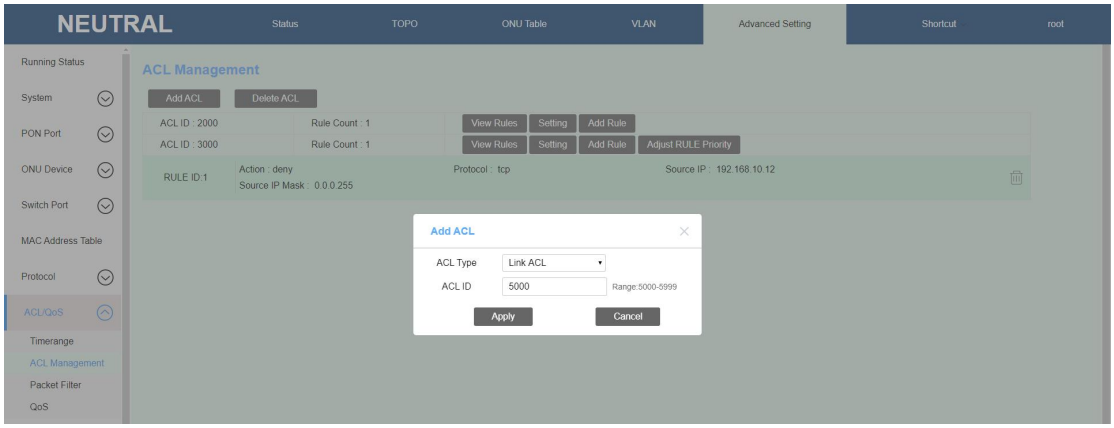


5.8.2.3 Link ACL

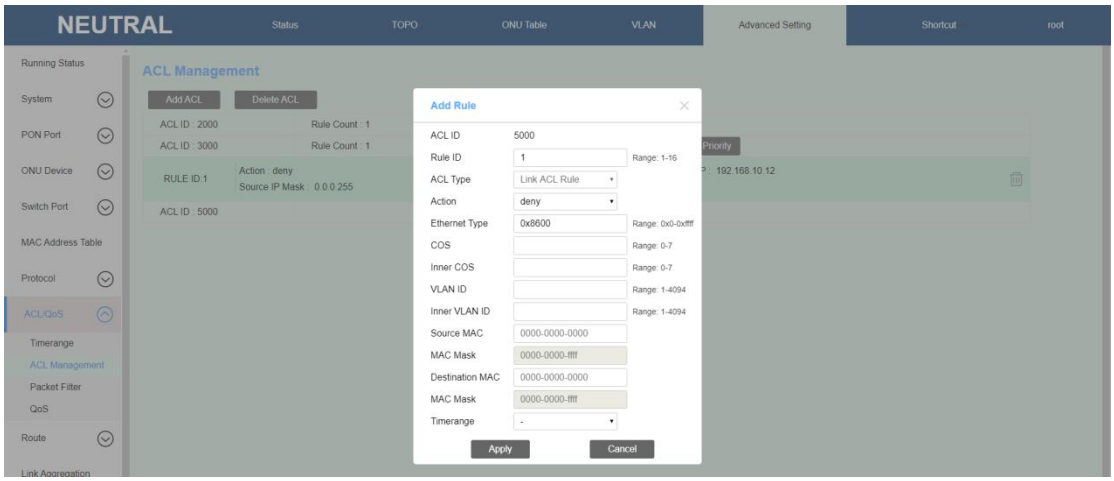
This configuration is used when ACL rules need to be formulated based on link-layer information such as the source MAC address of the message, the source VLAN ID, the

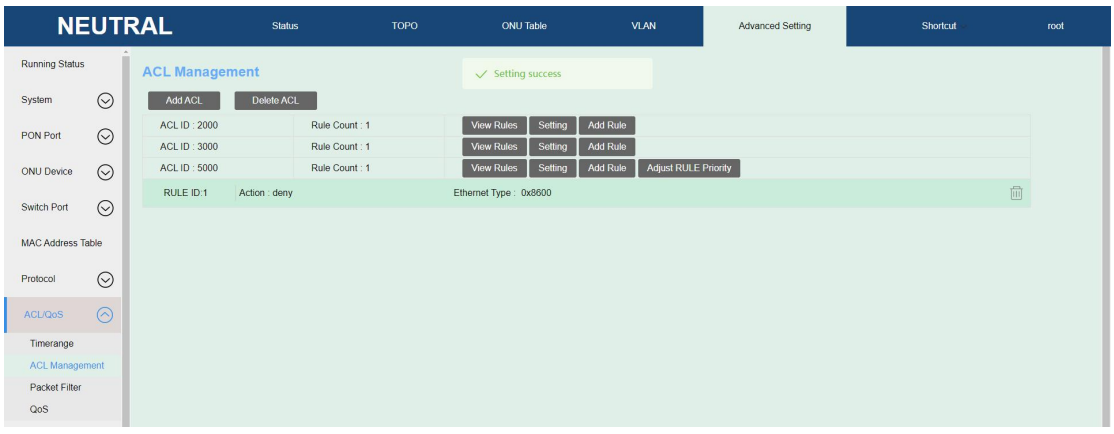
layer 2 protocol type, and the destination MAC address. After successful rule creation, packet-filter configuration reference rules can be used to filter packets.

1. Create link ACL, the ID range is 5000-5999. As shown below:



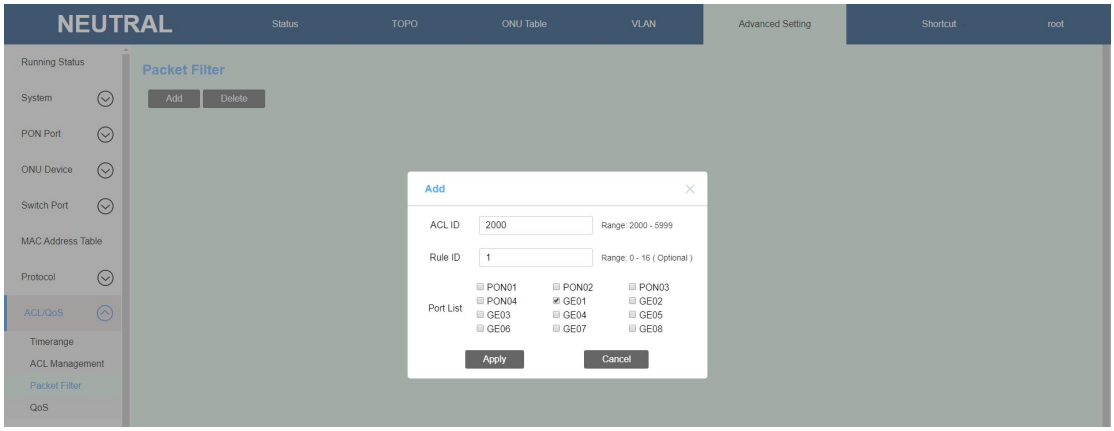
2. Add Rule: You can select time range take effect within the specified time or not select time range for immediate effect.

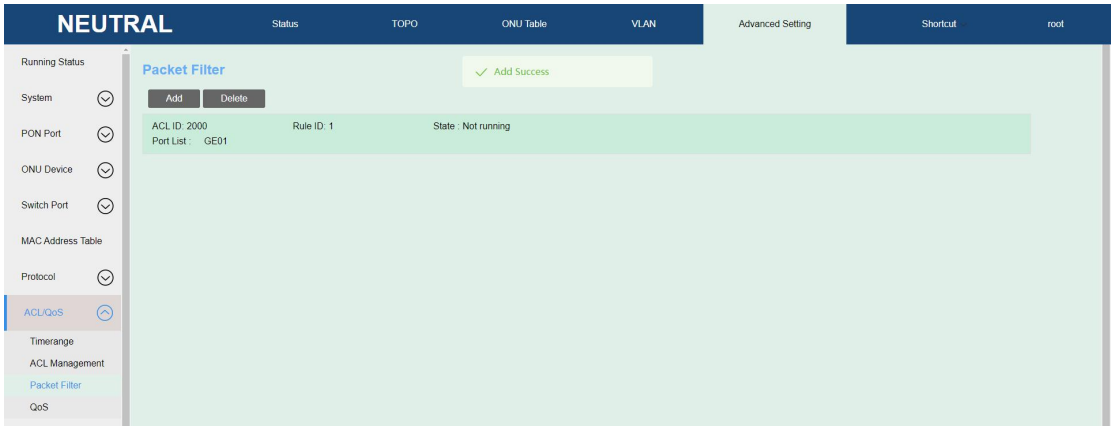




5.8.3 Packet Filter

It is used to configure and enable ACL filtering rules for a specified port. Use this configuration when you need to filter port traffic using ACL rules. Choose **Advanced Setting** -> **ACL/QOS** -> **Packet Filter**, enter this page, you can apply ACL rules to specific ports, as shown below:

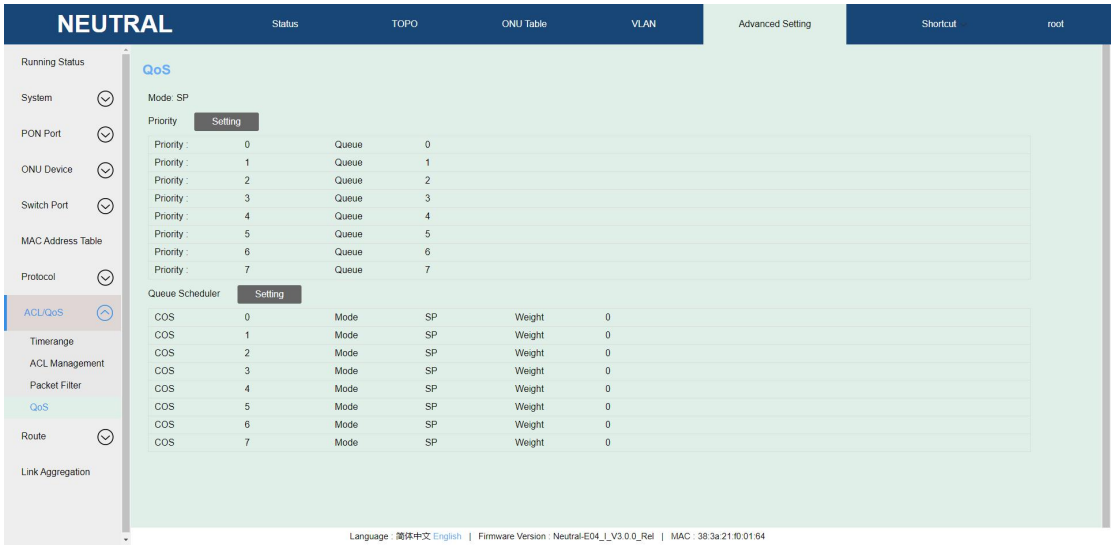




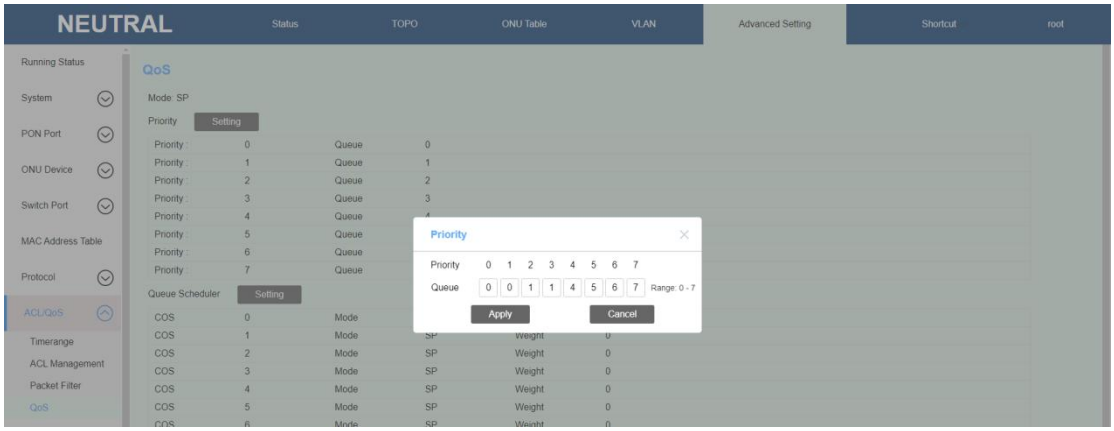
5.8.4 QOS

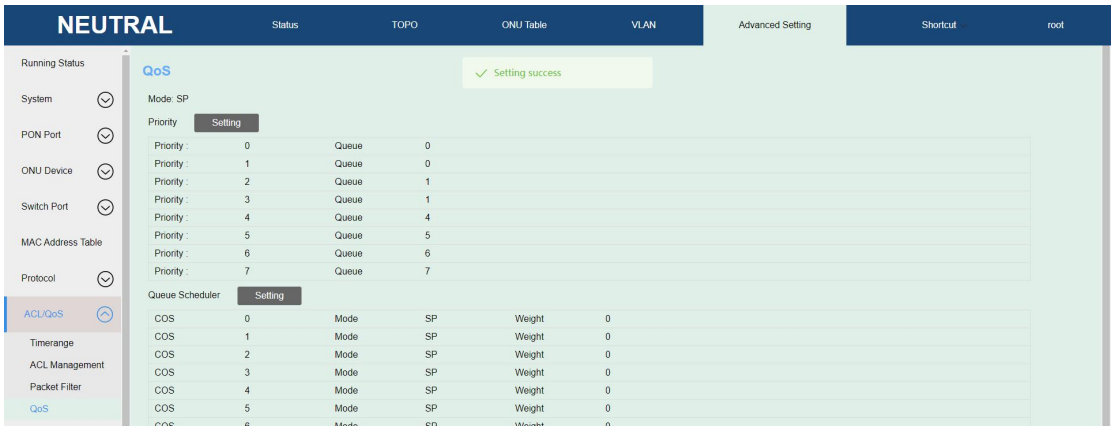
Configure the queue scheduling mode for the system.Queue scheduling is to divide the messages that need to be sent from the same port into multiple queues and schedule them between queues to decide which queue's messages should be sent first and which queue's messages should be sent later.This configuration is used when the user needs to select different queue scheduling modes according to the degree of importance of the service to ensure that QoS guarantee can be provided for the important service in case of network congestion.

Choose **Advanced Setting** -> **ACL/QOS** ->**QoS**, enter this page, you can configure QoS parameters, as shown below:

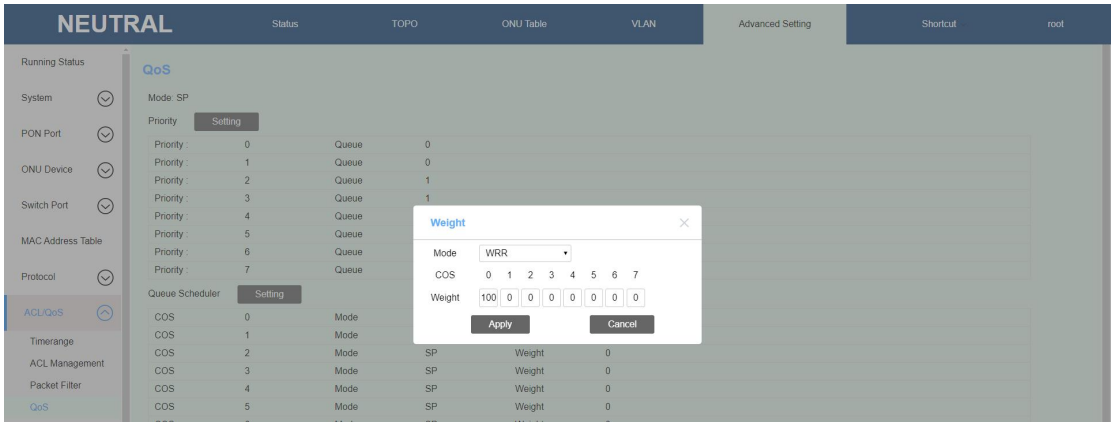


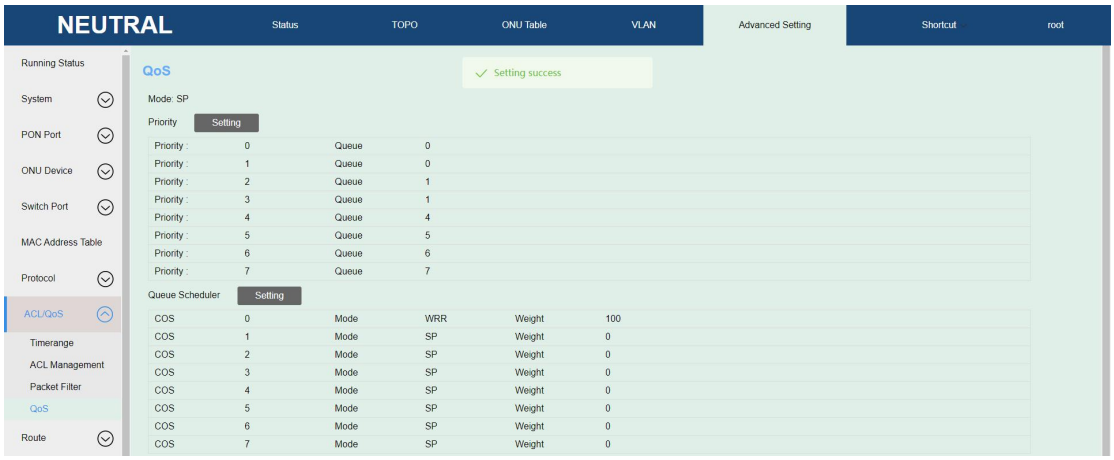
1. You can sets the mapping of priority and queue, as shown below:





2. You can set Queue scheduler.If you select WRR mode, all weight plus must be 100 or zero. as shown below:

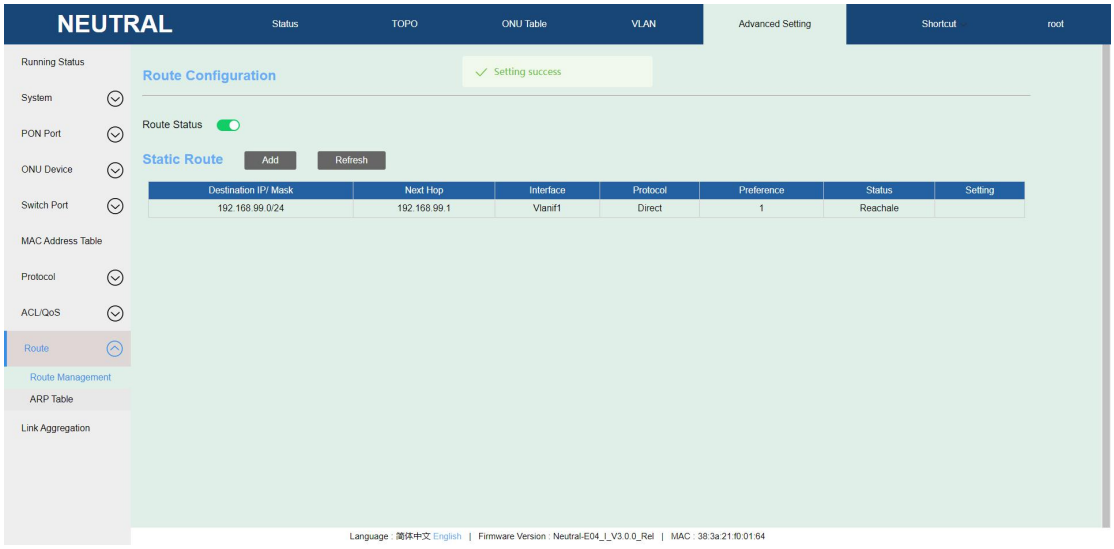




5.9 Route

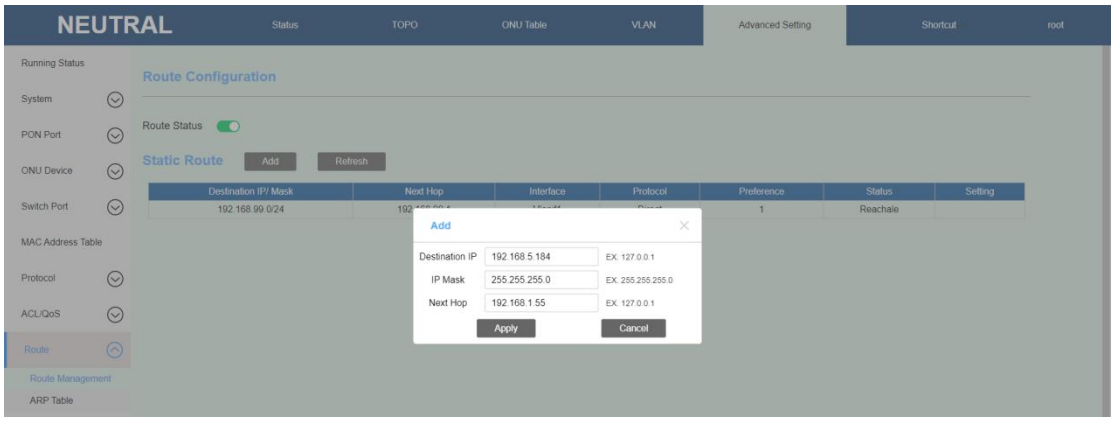
5.9.1 Route Management

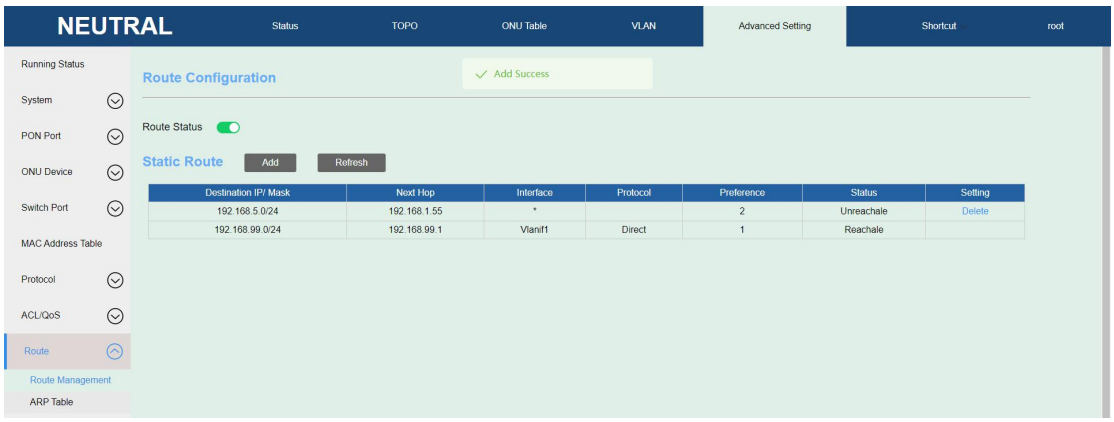
1. Choose **Advanced Setting** -> **Route** -> **Route Managemen**t, enter this page, you can start route management. By default, this function is disabled. To configure static route, you need to turn on the routing switch first. As shown below:



Note: When you close route status,all the static route entry and arp entry will clear.

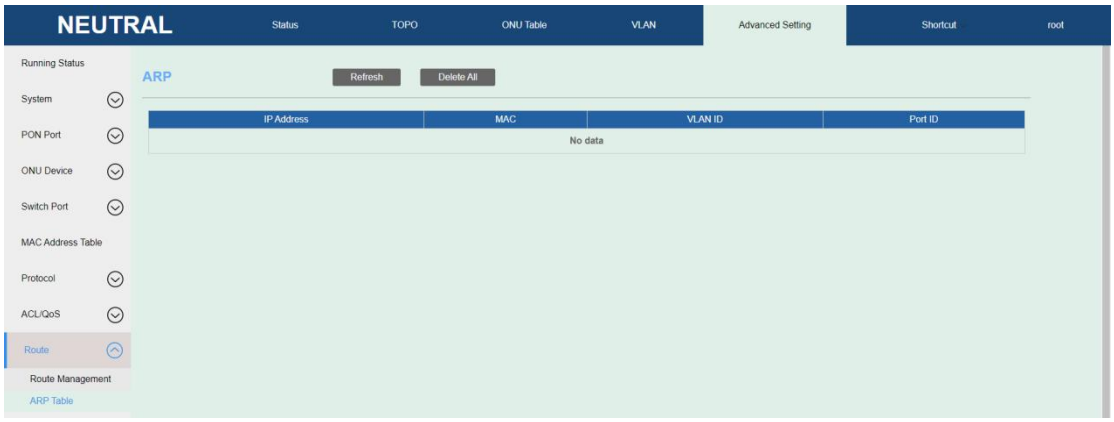
2. After turning on the route switch, click the "**Add**" button to add a static routing entry. When next-hop is reachable,will learn the next-hop gateway ARP,the status will become reachable. As shown below:





5.9.2 ARP Table

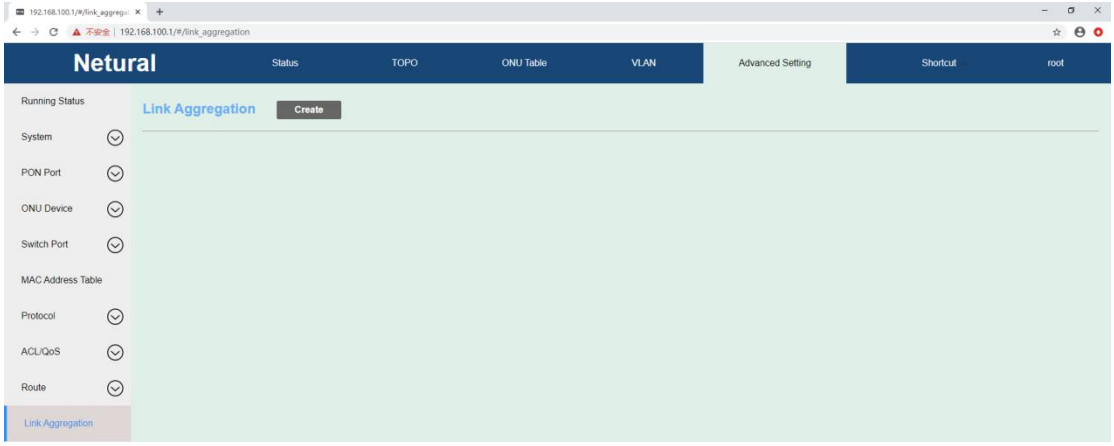
Choose **Advanced Setting** -> **Route** -> **ARP Table** , enter this page, you can view and delete ARP entries, as shown below:



5.10 Link Aggregation

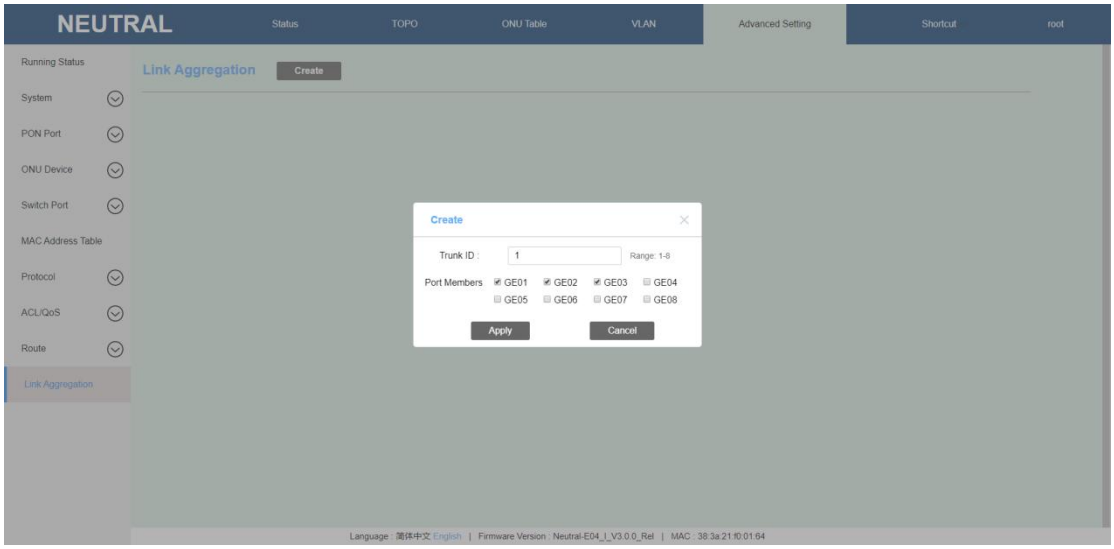
Link aggregation is the binding of multiple connected ports of the same type into one logical port, which can increase the bandwidth of the connected ports without upgrading the hardware, and effectively improve the reliability between links through the link backup mechanism.

Choose **Advanced Setting** -> **Link Aggregation**, enter this page to configure link aggregation function parameters, as shown below:



5.10.1Create Link Aggregation

Enter the link aggregation page, click the "**Create**" button, input the group ID and select port members in the pop-up option box, as shown below:



Note:

1) One port cannot join multiple aggregation groups at the same time;

2) Spanning tree protocol: the port joining the aggregation group will be treated as a logical port for protocol operation;

3) Uplink loop detection: when the port joins the aggregation group, the port loop detection does not take effect;

4) Port attributes: the port attributes of members joining the aggregation group must be consistent: speed, port type, MTU, port rate limit and storm control;When the aggregation group member port property is configured, the members of the group are bound together for configuration.

5) VLAN attribute: the port VLAN configuration of members joining the aggregation group must be consistent: PVID and port VLAN;When the aggregation group member VLAN is configured, the members of the group are bound together for configuration.

6) Port mirroring destination port cannot join the aggregation group as a member of the aggregation group, and the port joining the aggregation group cannot become the mirroring destination port;

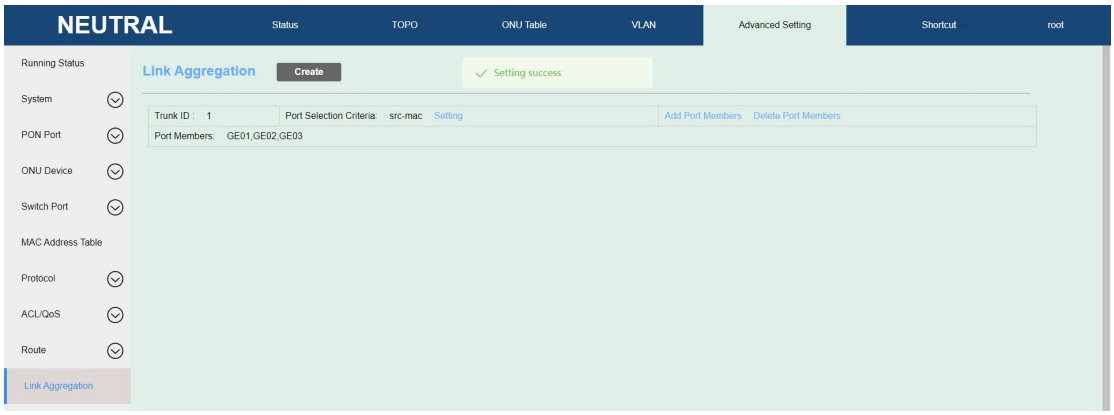
7) A port configured with a static MAC address cannot join an aggregation group as a member;

8) Ports configured with ACL rules cannot join an aggregation group as a member;

9) The multicast VLAN routing port configured cannot be added to the aggregation group as a member of the aggregation group;

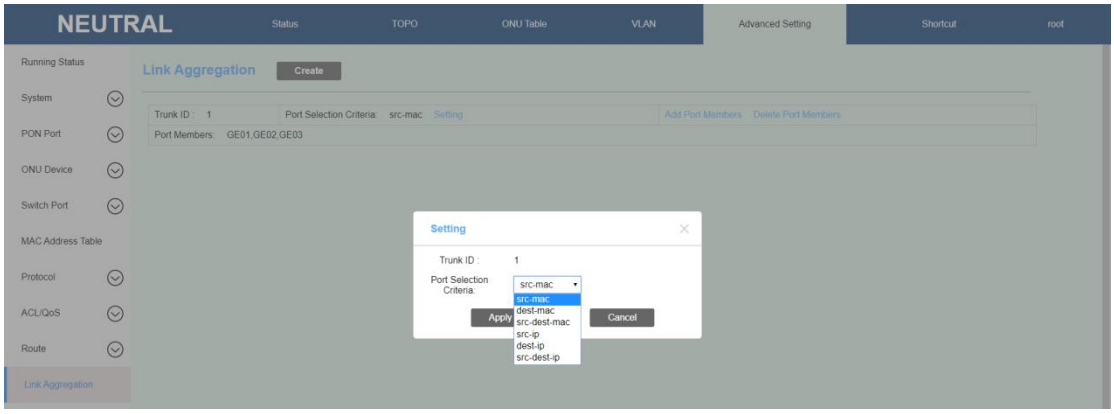
5.10.2View Link Aggregation

After successful creation, the member ports to join the link aggregation group can be viewed, and link aggregation group members can be added and deleted within the aggregation group. As shown below:



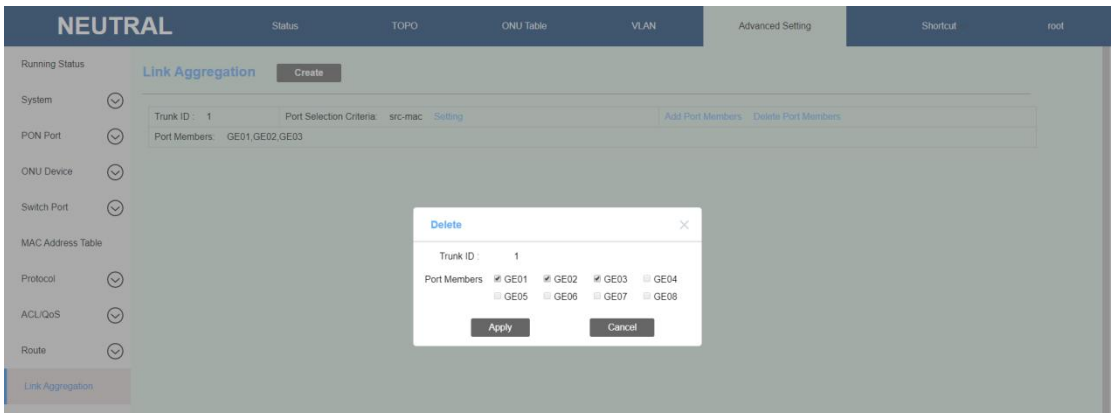
5.10.3Port Selection Criteria

The default load balancing routing algorithm is based on src-mac for hashing, and other routing algorithms can be configured according to requirements. As shown below:



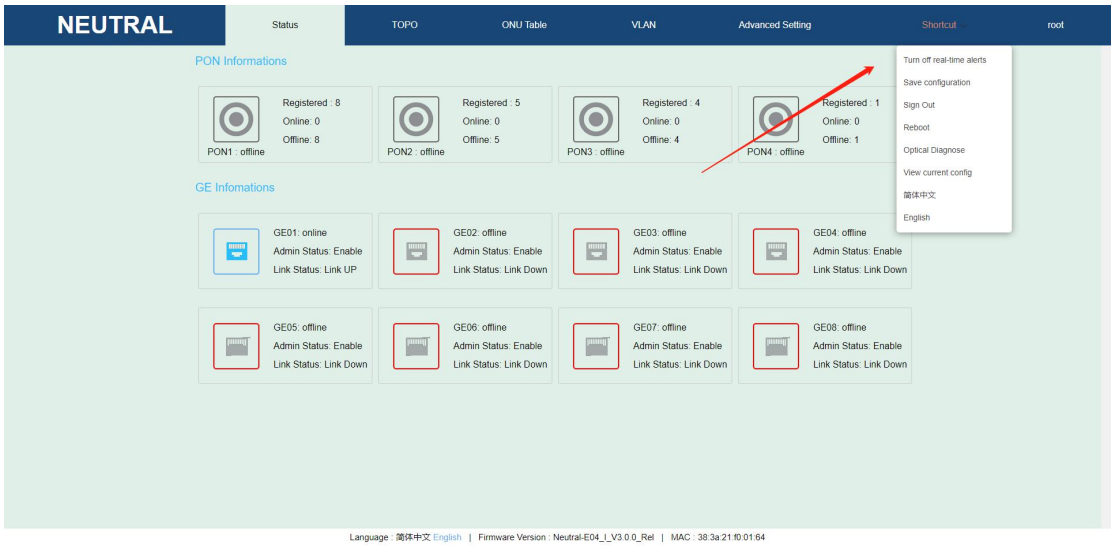
5.10.4Delete Link Aggregation

When link aggregation needs to be removed, all members of the link aggregation group are deleted, and the aggregation group is removed. As shown below:

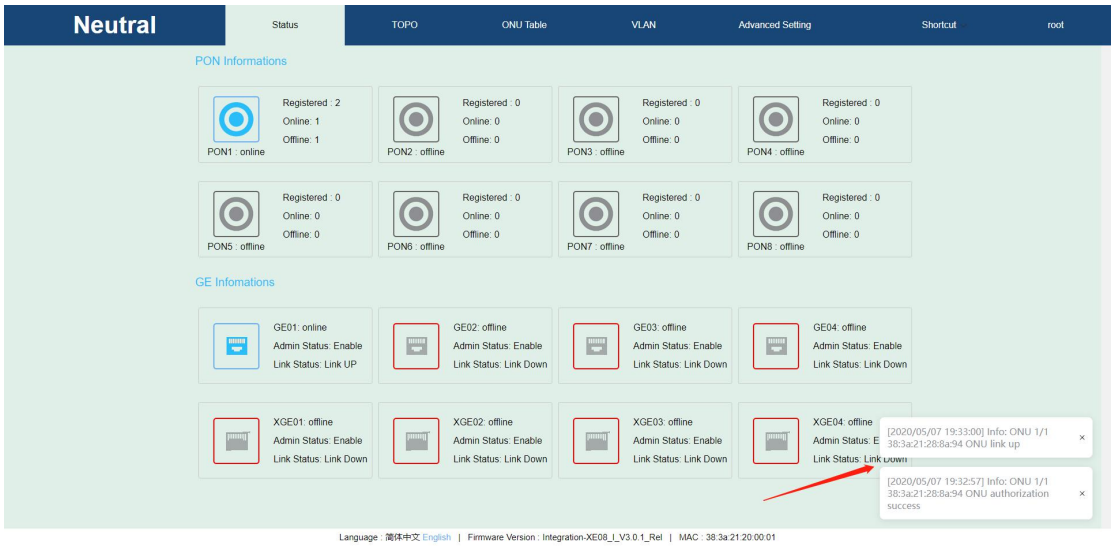

NEUTRAL
Status
TOPO
ONU Table
VLAN
Advanced Setting
Shortcut
root
Running Status
System
PON Port
ONU Device
Switch Port
MAC Address Table
Protocol
ACL/QoS
Route
Link Aggregation
Link Aggregation
Create
Trunk ID : 1
Port Selection Criteria: src-mac
Setting
Add Port Members
Delete Port Members
Port Members: GE01,GE02,GE03
Delete
Trunk ID : 1
Port Members
GE01
GE02
GE03
GE04
GE05
GE06
GE07
GE08
Apply
Cancel

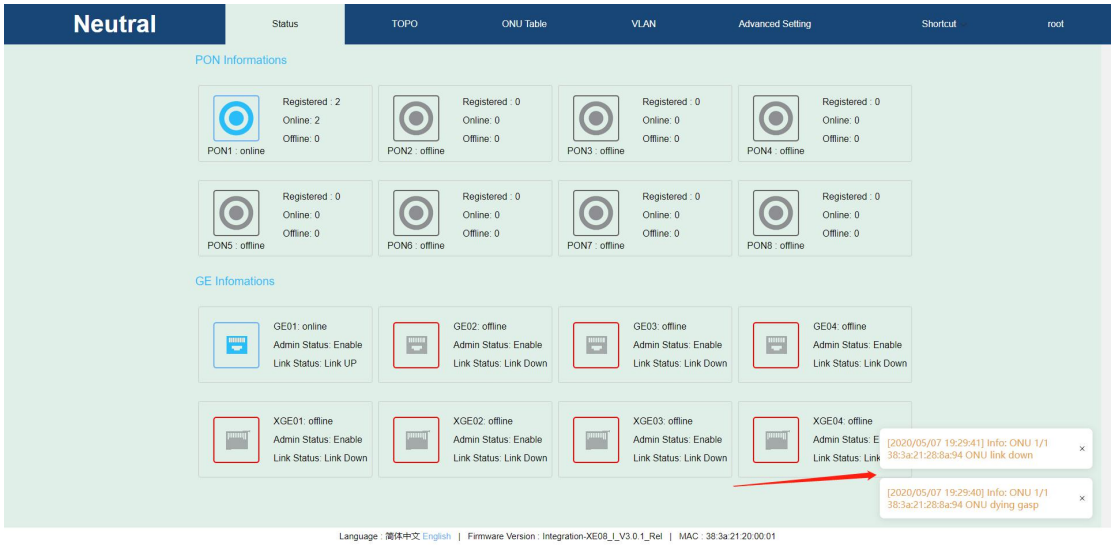
6 Shortcut

Enter OLT WEB, move the mouse to the "**Shortcut**" option, you can quickly use some common functions, including turn off / on real-time alters, saving configuration, sign out, reboot, optical diagnosis, viewing current configuration, simplified Chinese and English settings Features. As shown below:



1. Choose **Shortcut -> Turn off /on real-time alters**, you can close or open the real-time alarm information that automatically pops up in the lower right corner of the page. As shown below:



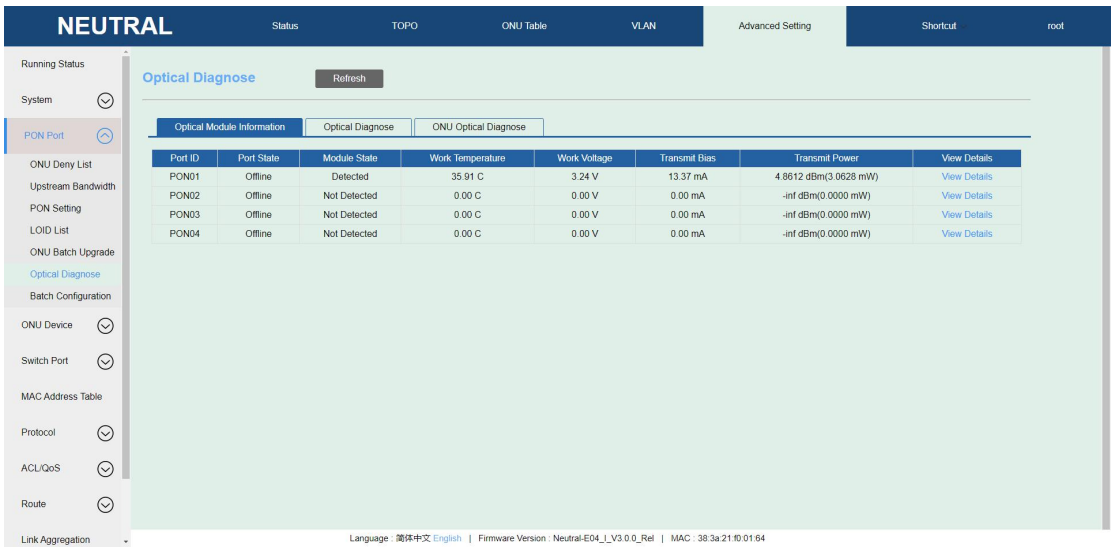


2. Choose **Shortcut** -> **Saving configuration**, you can save all modified configuration.

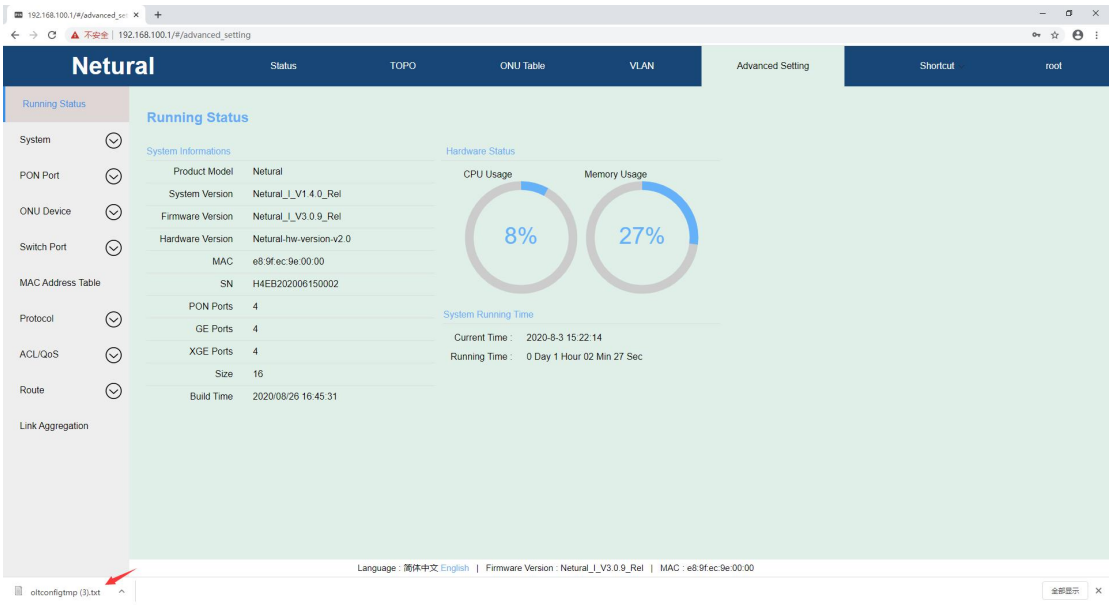
3. Choose **Shortcut** -> **Sign Out**, you can exit the current login interface to the login interface.

4. Choose **Shortcut** -> **Reboot**, you can restart device right now.

5. Choose **Shortcut** -> **Optical Diagnosis**, you can quickly access to PON port -> Optical diagnosis. As shown below:



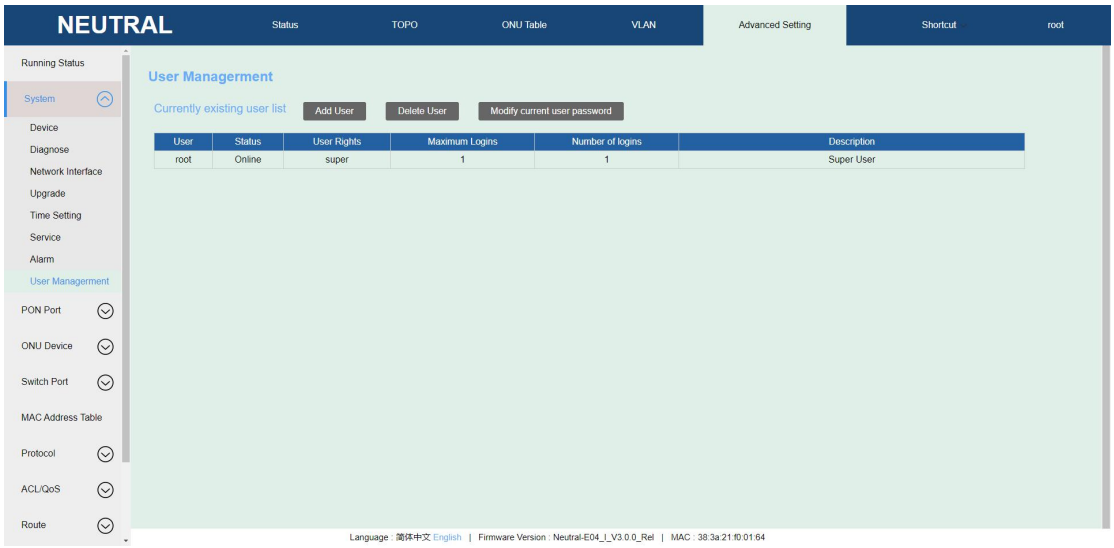
6. Choose **Shortcut** -> **View current config** , you can export OLT current configuration into file, the default file name is oltconfigtmp.txt. As shown below:



7. Choose **Shortcut -> Simplified Chinese & English**, you can switch page language.

7 root

Enter OLT WEB, the upper right corner of the page is the currently logged-in user name, click on the user name, you can jump to the System -> User Management page, if you are currently logged in with the system default user name **root/admin**, the upper right corner of the page displays " **root**". As shown below:



*******************Thank you for using our company products!*******************