
NEUTRAL OLT User Manual

P/N: NEUTRAL-E08/NEUTRAL-E04

Software version: epon_firmware_I_V2.2.0_Rel

Version	Date	Description
V1.0	2017.07.07	First Version
V1.1	2018.03.15	Add WebGUI
V1.2	2018.06.05	Follow the latest functions
V2.2.0	2019.07.18	Add functions:route,loid,link aggregation,ACL/QOS,loop detect

Contents

NEUTRAL OLT User Manual.....	- 1 -
P/N: NTUTRAL-E08/NEUTRAL-E04.....	- 1 -
Contents.....	- 4 -
1 Local and remote management and configuration management.....	- 8 -
1.1 Console interface.....	- 8 -
1.1.1 Essential information.....	- 8 -
1.1.2 Software operation method.....	- 9 -
1.2 NMS outbound management interface.....	- 12 -
1.3 Inbound management interface.....	- 14 -
2 Manage Configurations.....	- 19 -
2.1 configuration the equipment system information.....	- 19 -
2.2 Add route default gateway.....	- 20 -
2.3 Modify time.....	- 20 -
2.3.1 Change timezone.....	- 20 -
2.3.2 Setting time:.....	- 21 -
2.4 User management.....	- 22 -
2.4.1 User display.....	- 22 -
2.4.2 User add.....	- 22 -
2.4.3 Delete a user.....	- 23 -
2.4.4 Save user informations.....	- 23 -

2.4.5	Change the user's password.....	- 24 -
2.5	Olt config management.....	- 24 -
2.5.1	Export olt.config.....	- 24 -
2.5.2	Import olt.config.....	- 24 -
2.6	Services.....	- 24 -
2.6.1	SNMP Trap.....	- 24 -
2.6.2	SNMP Community.....	- 24 -
2.6.3	SSH.....	- 25 -
3	PON configuration management.....	- 26 -
3.1	PON port ONU registration and certification.....	- 26 -
3.2	DBA Bandwidth allocation.....	- 29 -
3.3	ONU Upgrade.....	- 30 -
4	ONU UNI configuration.....	- 33 -
4.1	VLAN Model introduction.....	- 33 -
4.2	ONU UNI interface configuration management.....	- 37 -
5	Switching side configuration management.....	- 39 -
5.1	VLAN configuration management.....	- 39 -
5.1.1	VLAN interface.....	- 39 -
5.1.2	INTERFACE vlan configuration.....	- 41 -
5.2	MAC Address management and configuration.....	- 43 -
5.2.1	DISPLAY mac address table.....	- 43 -

5.2.2	CONFIGURE mac address table.....	- 44 -
5.3	Port configuration management.....	- 44 -
5.3.1	Basic configuration.....	- 44 -
5.3.2	Broadcast/Multicast/Unicast storm control configuration...	- 44 -
5.3.3	Port rate limit and traffic shaping configuration.....	- 46 -
5.3.4	Port statistic.....	- 47 -
5.3.5	Port mirror.....	- 49 -
5.3.6	Loop detection.....	- 50 -
5.4	spanning-tree.....	- 53 -
5.4.1	Network demand.....	- 53 -
5.4.2	Configuring steps.....	- 53 -
5.5	IGMP.....	- 55 -
5.5.1	Network demand.....	- 55 -
5.5.2	Configuring steps.....	- 55 -
6	ACL/QOS.....	- 64 -
6.1	Timerange.....	- 64 -
6.2	ACL Management.....	- 64 -
6.3	Packet Filter.....	- 66 -
6.4	QOS.....	- 66 -
7	Route.....	- 69 -
7.1	Route Management.....	- 69 -

7.2	ARP Table.....	- 70 -
8	Link Aggregation.....	- 71 -
8.1	Create Link Aggregation.....	- 71 -
8.2	Display Link Aggregation.....	- 72 -
8.3	Port Selection Criteria.....	- 72 -
8.4	Remove Link Aggregation.....	- 72 -
9	SYSTEM UPDATE.....	75
10	WebGUI management support.....	76
11	Abbreviation terminology.....	77

1 Local and remote management and configuration management

This device provides a command line mode (CLI) local and remote management of equipment.

EPON OLT provides 4 types of equipment management interface

- ✧ Console interface
- ✧ WebGUI (Document-EPON OLT WebGUI UserManual.doc)
- ✧ NMS outbound management interface
- ✧ Inbound management interface

1.1 Console interface

1.1.1 Essential information

The console port connect directly to customized serial line (pictured) and operating the user command line of OLT device.

【The serial line is provided by our company】



【Notice】

The default serial port baud rate is 9600bps.

1.1.2 Software operation method

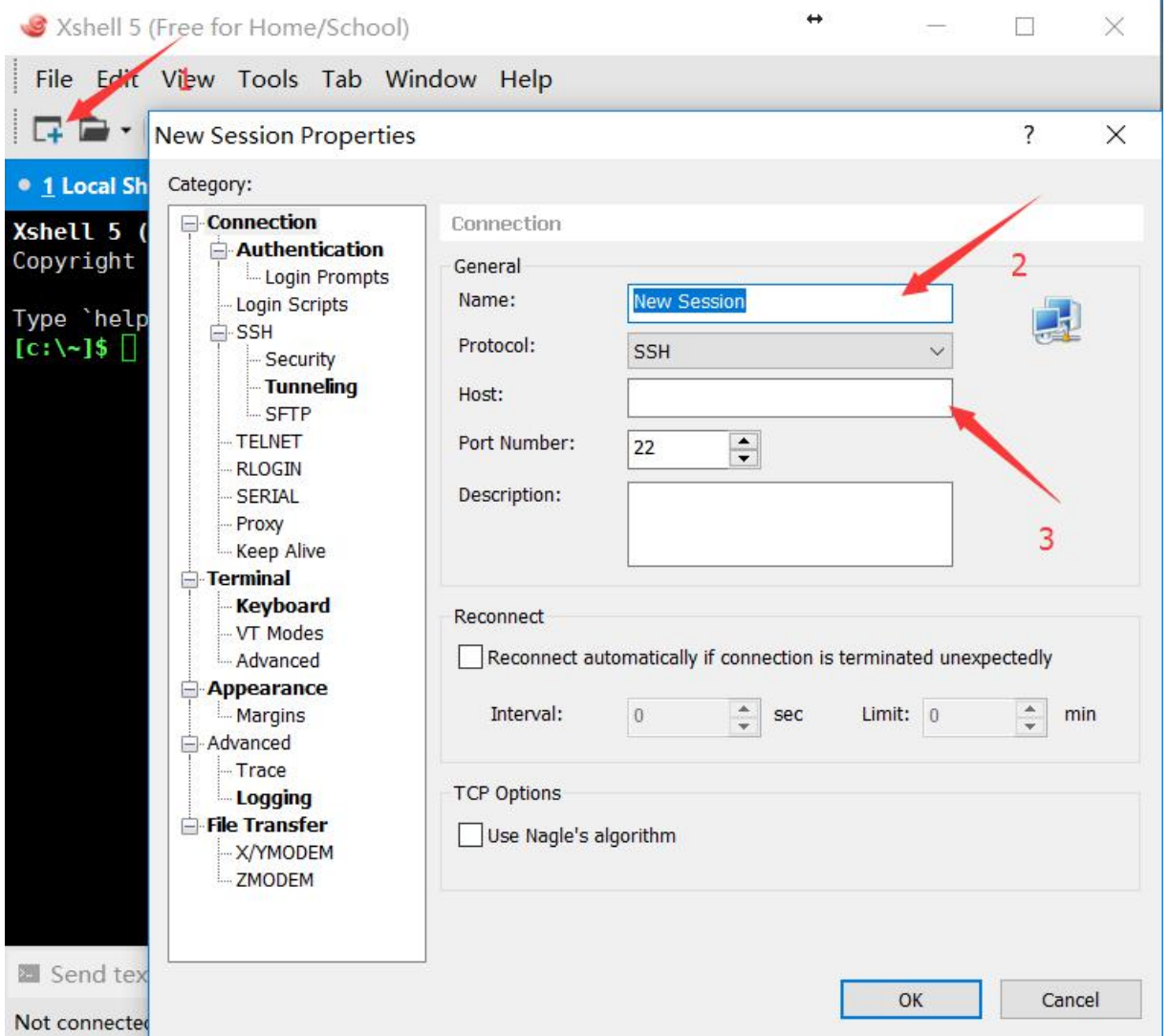
Open a serial port tool, such as xshell

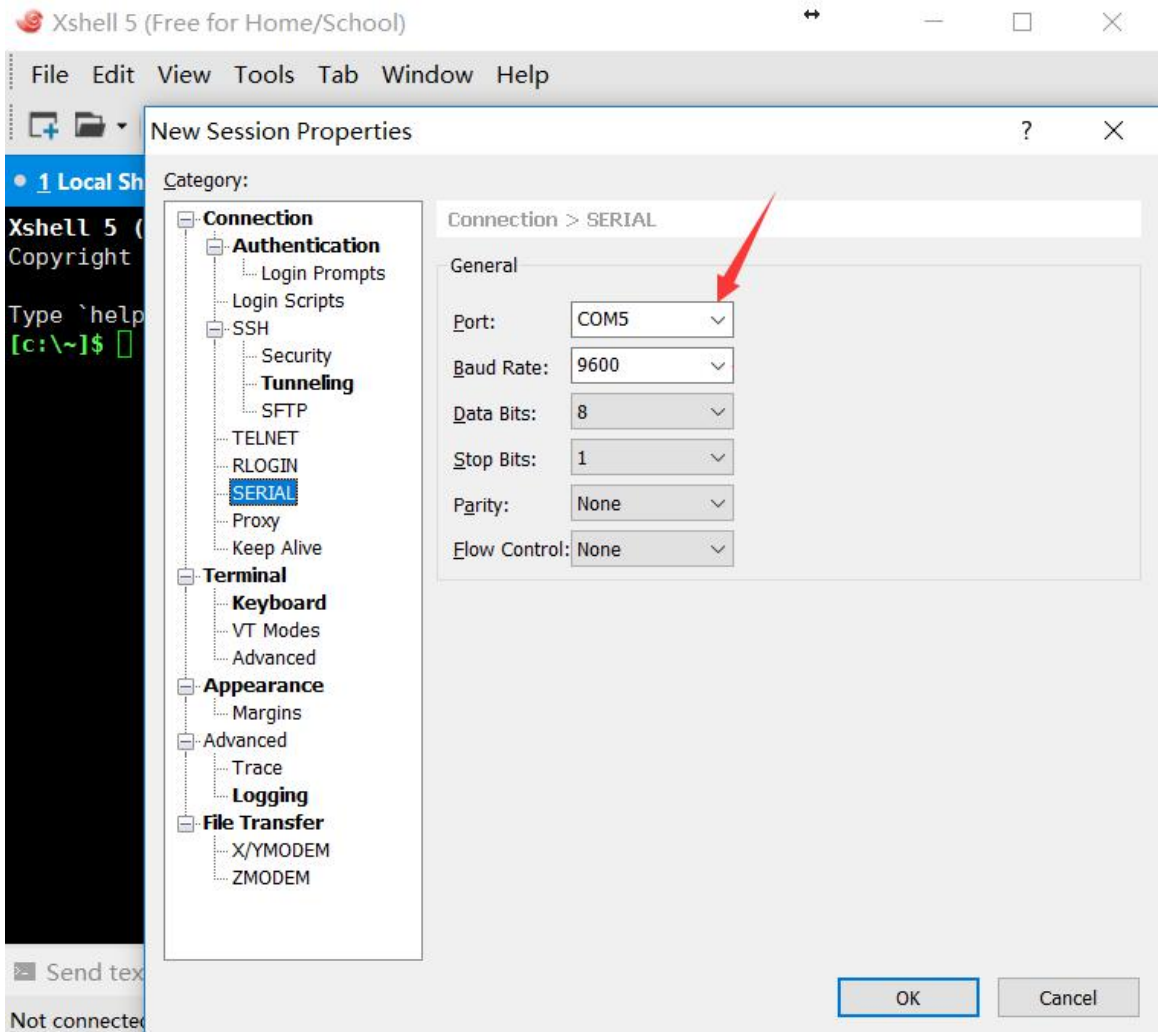
New-built a serial port link, and open it. Here are the steps:

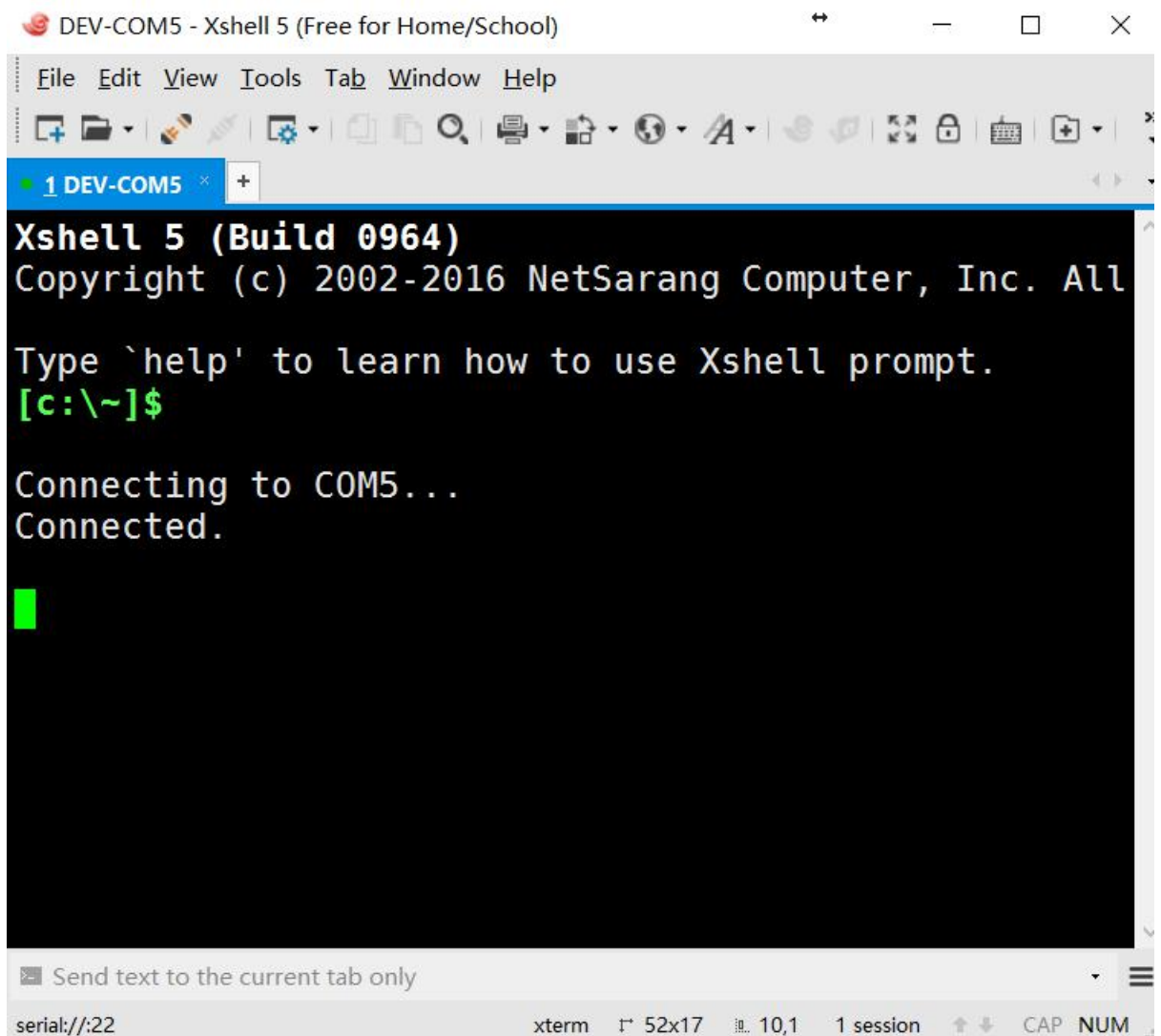
【Notice】

User name: root

Password: admin



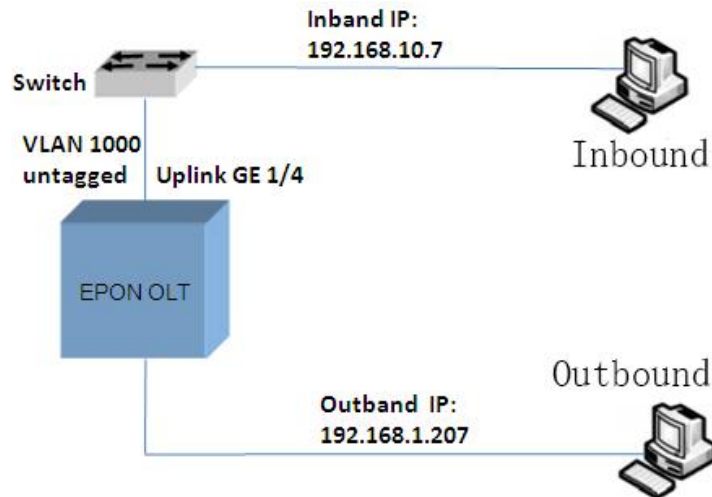




1.2 NMS outbound management interface

The one end of the two RJ-45 ports on crossover network cable is connected to the nearest switch or network reachable switch, the other end is connected to the OLT.

Configuration management network diagram:



OLT administrator IP address is defaulted as 192.168.100.1. You can configure the inbound IP or modify the IP address of the PC to ensure the route access to PC is up to the network of OLT IP network management.

```

username:root
password:

OLT> enable

OLT# configure

OLT(config)# interface manage

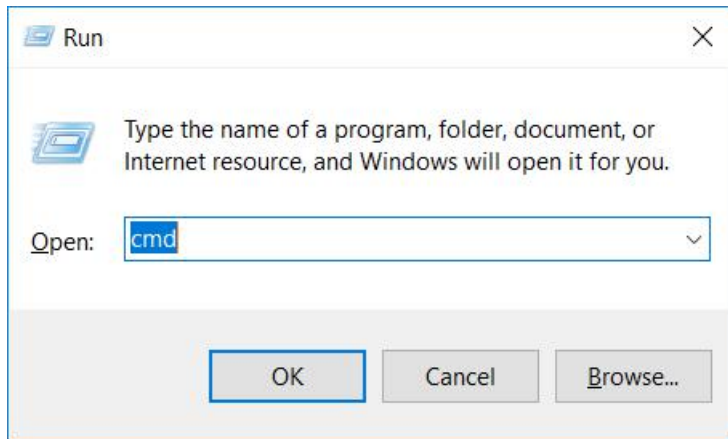
OLT(config-manage)# ifconfig
Description : For Outbound management
The Maximum Transmit Unit is 1500 bytes
Internet Address is 192.168.100.1, netmask 255.255.255.0
Hardware address is 38:3A:21:20:32:F1
  Recive 130 packets, 12151 bytes
  Transmit 2 packets, 168 bytes

OLT(config-manage)# █

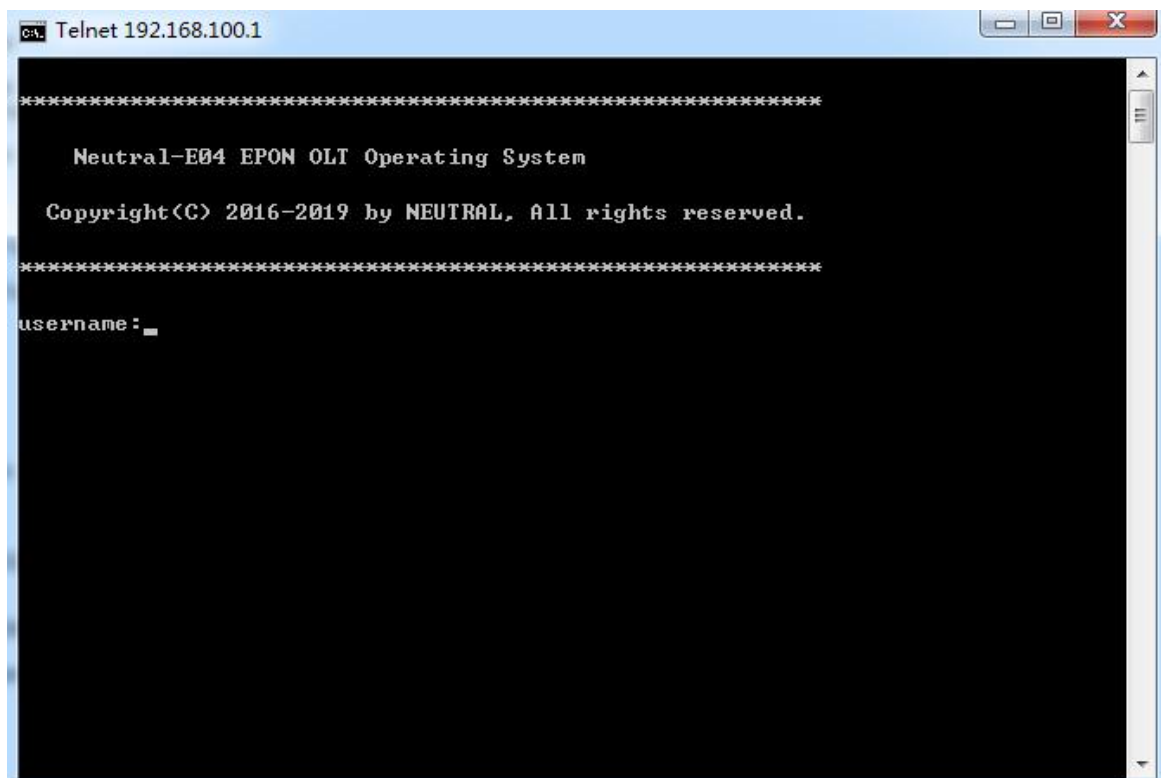
```

You can through the telnet remote access to OLT after configuring the IP address.

Opening windows operation window, input cmd:



Then telnet 192.168.100.1, and input username and password to enter the control command line [CLI] interface.



1.3 Inbound management interface

This OLT device can support inbound management configuration through uplink port(ge) or PON port following connected ONU. It needs configuration the IP address, subnet mask, and VLAN.

The relevant configuration routine:

```
OLT(config)# vlan standard 100

OLT(config-vlan-100)# interface vlanif 100

OLT(config-vlanif-100)# ifconfig 192.168.10.1 netmask 255.255.255.0

OLT(config-vlanif-100)# ifconfig

Description : For Inbound management

The Maximum Transmit Unit is 1500 bytes

Internet Address is 192.168.10.1, netmask 255.255.255.0

Hardware address is 38:3A:21:20:32:F2

Recive 0 packets, 0 bytes

Transmit 0 packets, 0 bytes

OLT(config-vlanif-100)# exit
```

```
OLT(config)# interface ge 1

OLT(config-ge-1)# vlan mode access

OLT(config-ge-1)# vlan access 100

OLT(config)# ping 192.168.10.175

PING 192.168.10.175 (192.168.10.175): 56 data bytes

64 bytes from 192.168.10.175: seq=0 ttl=64 time=1.509 ms

64 bytes from 192.168.10.175: seq=1 ttl=64 time=0.705 ms

64 bytes from 192.168.10.175: seq=2 ttl=64 time=0.648 ms

64 bytes from 192.168.10.175: seq=3 ttl=64 time=0.982 ms

--- 192.168.10.175 ping statistics ---
```

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max = 0.648/0.961/1.509 ms

OLT(config)#

1.4 WEB port

1.4.1 display WEB port

OLT(config)# web-port

HTTP Port : 80

HTTPS Port : 443

OLT(config)#

1.4.2 WEB port configuration

OLT(config)# web-port http 500

OLT(config)# web-port https 1000

OLT(config)# web-port

HTTP Port : 500

HTTPS Port : 1000

OLT(config)#

2 Manage Configurations

Manage Configurations contain the system name, save configuration, system configuration etc.

2.1 configuration the equipment system information

1. Configure system name:

```
OLT(config)# hostname NEUTRAL-E08
```

```
OLT(config)#
```

2. Store system configuration:

```
OLT(config)# save
```

```
OLT configuration saved successfully
```

3. System configuration

```
OLT(config)# interface manage
```

```
OLT(config-manage)#
```

4. Check the alarm history record

```
OLT(config-manage)# alarm-history
```

5. Configuring and viewing outbound management IP

```
OLT(config-manage)# ifconfig
```

6. Default OLT to factory config

```
OLT(config-manage)# erase config-file
```

7. Get the board informations

```
OLT(config-manage)# board
```

Copyright 2000-2017 Neutral-E04 Technology, et al.

Software Version : Neutral-E04_I_V1.1.0_Rel
Bootrom Version : Neutral-E04-bl-version-v1.0
Hardware Version : Neutral-E04-hw-version-v2.0
Base Mac Address : 38:3a:21:f0:00:3a
Build time : 2018/06/05 15:37:12
Ftp Server Host : 192.168.100.100
Ftp Name : 123
Ftp Password : 123
OLT(config-manage)#

2.2 Add route default gateway

```
OLT(config)# route default gw 192.168.1.1
```

2.3 Modify time

2.3.1 Change timezone

1. You need follow the command 'timezone utc+ 11:00' to checkout your city

```
OLT(config)# timezone utc+ 11:00
```

Find similar item ,list below:

--Using the location string to config--

```
Antarctica/Macquarie(UTC+11:00)
```

Asia/Anadyr(UTC+11:00)

Asia/Kamchatka(UTC+11:00)

Asia/Magadan(UTC+11:00)

Pacific/Efate(UTC+11:00)

Pacific/Guadalcanal(UTC+11:00)

Pacific/Kosrae(UTC+11:00)

Pacific/Norfolk(UTC+11:30)

Pacific/Noumea(UTC+11:00)

Pacific/Ponape(UTC+11:00)

2. OLT(config)# timezone "Pacific/Ponape"

3. Show the state

OLT(config)# show timezone

The current time zone: Pacific/Ponape(+11:00)

OLT(config)#

2.3.2 Setting time:

OLT(config)# time 2018/06/05-15:51:00

OLT(config)# time

System current time: 2018-06-05 15:51:01+08:00

System running time : 0 day 0 hour 13 minute 28 second

System boot time : Tue Jun 5 15:37:33 2018

OLT(config)#

2.4 User management

2.4.1 User display

OLT(config)# show user

```
-----  
Name   Level  Status  Reenter Append Info  
-----  
root   Super  online   1 Super User  
-----
```

Notice:

There is no limit to how many times a user can login again.

2.4.2 User add

OLT(config)# user add test test123 admin reenter 4

OLT(config)# show user

```
-----  
Name   Level  Status  Reenter Append Info  
-----  
root   Super  online   1 Super User  
-----
```

test Admin offline 4

OLT(config)#

If some user close browser or close browser's pages, the login status will save 5mins, means timeout is 5mins

Now, you can force a user to go offline

OLT(config)# user offline test

The user test have been offline

Info: Force user test offline success!

OLT(config)#

2.4.3 Delete a user

OLT(config)# user delete test

Info: Delete user test success!

OLT(config)#

Default the user account informations

OLT(config)# user default

2.4.4 Save user informations

OLT(config)# user save

2.4.5 Change the user's password

Change your own password

```
OLT(config)# user password test123
```

Change other user's password(You need login by root)

```
OLT(config)# user password test test123
```

2.5 Olt config management

Input ftp server ip(may be your pc ip), you can export the olt.config to ftp server shared dir or import olt.config from ftp server shared dir to the olt.

2.5.1 Export olt.config

```
OLT(config-manage)# config push 192.168.100.10/1
```

2.5.2 Import olt.config

```
OLT(config-manage)# config pull 192.168.100.10/1
```

2.6 Services

2.6.1 SNMP Trap

Here, you can setting the SNMP Trap configurations

Notice:The serverip must be an inbound or outbound address that exists

```
OLT(config)# snmp trap-cfg serverip 192.168.100.100 public
```

2.6.2 SNMP Community

Config snmp read community

```
OLT(config)# snmp community-cfg read public
```

Config snmp write community

OLT(config)# snmp community-cfg write private

2.6.3 SSH

By default, the ssh service will not start up, you need start it manual

Open the ssh service:

OLT(config)# ssh-server start

Stop the ssh service:

OLT(config)# ssh-server stop

3 PON configuration management

3.1 PON port ONU registration and certification

1. ONU authentication type and mode configuration

It supports two certification methods of PON port at present, manual and automatic authentication . As long as the fiber splitter access to OLT's PON port, ONU can automatically authorize and it will be online , while manual authentication need to configure the relevant command to make the ONU online.

ONU authentication mode: support MAC authentication, hybrid authentication and loid authentication.

Check ONU authentication mode command:

```
OLT (config-epon-1)# onu-authorize
```

```
PON-PORT AUTH-MODE AUTH-TYPE
```

```
pon1 mac auto
```

【Notice】

- (1)、 OLT defaults automatic registration and authentication at present
- (2)、 Defauting mac authentication mode

2. ONU support the black and white list .

3. Manually bind a ONU to a ONU ID

```
OLT (config-epon-1)# bind-onu mac 00:12:34:45:56:05
```

OLT (config-epon-1)# show onu-info all

PON/ONU	Mac-Address	Status	Auth-State	Config-State	Reg-time
ONU-TYPE					

1/1	00:12:34:45:56:05	Initial	TRUE	FALSE	1969/12/31 20:00:00
-----	-------------------	---------	------	-------	---------------------

OLT (config-epon-1)#

【Notice】 :

The system will automatically assign the unused ID to the ONU if not specify ONU ID

After you bind a onu, you need confirm it(authorize)

OLT (config-epon-1)# onu confirm onu-id 1

Manually bind a ONU to a blacklist, and once bound to a blacklist, the system will block ONU registration online.

OLT (config-epon-1)# blacklist add mac 00:00:00:11:11:11

OLT (config-epon-1)# show blacklist onu-info all

PON/ONU	Mac Address	Try REG Count
---------	-------------	---------------

```
1/1 00:00:00:11:11:11 0
```

```
OLT (config-epon-1)#
```

4. loid authentication

1-> Configure the ONU authentication mode first.

```
OLT(config)# interface epon 1
```

```
OLT(config-epon-1)# onu-authorize mode loid
```

```
OLT(config-epon-1)#
```

2-> Once configured ONU authentication mode, the ONU should display that loid does not exist, and the ONU's loid can be viewed.

```
OLT(config-epon-1)#
OLT(config-epon-1)#
[2019/07/20 12:44:38] Info: PON 2 PON link down and all onu will be offline
[2019/07/20 12:44:47] Info: PON 1 PON link up
[2019/07/20 12:44:50] Info: ONU 1/1 d8:42:ac:d9:af:0f ONU authorization fail, Reason:LOID NOT EXISTS
```

```
OLT(config-epon-1)#
```

```
OLT(config-epon-1)#
```

```
OLT(config-epon-1)# show onu-info onu-id 1
```

```
-----
PON ID           : 1
ONU ID           : 1
ONU Name         : ONU01/01
Authrize mode    : loid
Authrize state   : FALSE
Status           : Auth-Fail
ONU type         : lge
ONU RTT          : 14
Mac address      : d8:42:ac:d9:af:0f
LOID             : d842acd9af0f
Password         : 1111
Upgrade Type     :
CTC Version      : 3.0
ONU description  :
ONU vendor       : PHIC
ONU model        : 1001-8032
ONU sw(hw) version : V1.0.3(V1.0)
ONU Device Type  : SFU
ONU GE ports     : 1
-----
```

```
OLT(config-epon-1)#
```

3-> Added loid authentication, and then ONU registration online

```
OLT(config-epon-1)# loid add d842acd9af0f
```

```
OLT(config-epon-1)#
```

```
[2019/07/20 14:08:22] Info: ONU 1/1 d8:42:ac:d9:af:0f ONU authorization success
```

```
[2019/07/20 14:08:24] Info: ONU 1/1 d8:42:ac:d9:af:0f ONU link up
```

```
OLT(config-epon-1)#
```

3.2 DBA Bandwidth allocation

DBAs supports 5 types of bandwidth allocation

	Fixed	Assure	Max
Type1	√		
Type2		√	
Type3		√	√
Type4			√
Type5	√	√	√

Relevant Configuration command:

Configuring ONU ID 1 DBA bandwidth type as Type1,bandwidth is 10M:

```
OLT(config-epon-4)# sla-up 1 type1 fix 10000
```

Configuring ONU ID 1 DBA bandwidth type as Type2,guarantee bandwidth is 100M:

```
OLT(config-epon-4)# sla-up 1 type2 assure 100000
```

Configuring ONU ID 1 DBA bandwidth type as Type3, guarantee bandwidth is 100M, maximum bandwidth is 1000M:

```
OLT(config-epon-4)# sla-up 1 type3 assure 100000 max 1000000
```

Configuring ONU ID 1 DBA bandwidth type as Type4, maximum bandwidth is 1000M:

```
OLT(config-epon-4)# sla-up 1 type4 max 100000
```

Configuring ONU ID 1 DBA bandwidth type Type5, fixed bandwidth is 10M, guaranteed bandwidth is 100M, the maximum bandwidth is 1000M:

```
OLT(config-epon-4)# sla-up 1 type5 fix 10000 assure 100000 max 1000000
```

【Notice】

The maximum bandwidth of one PON port is 1G.

3.3 ONU Upgrade

1. add onu upgrade type

```
OLT(config)# onu-upgrade type add test
```

```
OLT(config)# show onu-upgrade type
```

2. load upgrade file to olt (need open ftp or tftp server in pc and put the upgrade file first)

```
OLT(config)# onu-upgrade load tftp 192.168.100.10 relimg-1.tar
```

```
OLT(config)# show onu-upgrade file
```

```
--w---x--T 1 root root 3543040 Aug 1 11:35 /tmp/onu_upgrade.img
```

3. onu upgrade only one (in pon node)

```
OLT(config-epon-1)# onu-upgrade onu-id 1
```

onu upgrade more (in pon node, need bind onu upgrade type)

OLT(config-epon-1)# bind-onu upgrade-type test onu-list 1,2

OLT(config-epon-1)# show onu-info all

OLT(config-epon-1)# onu-upgrade all-pon-port upgrade-type test

4 ONU UNI configuration

4.1 VLAN Model introduction

ONU Ethernet port supports the following 4 kinds of VLAN mode:

1. VLAN pass-through

This mode is suitable for those the client's home gateway or switch provided by operators, whose VLAN TAG is reliable. In this mode, the ONU will receive upload Ethernet frame without any processing of the Ethernet frame (regardless of whether the Ethernet frame with VLAN tag or not) and transparently forward to OLT, for download Ethernet frame forwarding mode is also transparent.

Table 5- 1 ONU processing mode in VLAN transmission mode

Direction	Whether Ethernet packets has Tag	Processing Mode
Upload	With VLAN tag	Pass-through
	W/O VLAN Tag	
Download	With VLAN tag	
	W/O VLAN Tag	

2. VLAN mode tag

This mode is suitable for the client's home gateway or switch VLAN tag is not to be trusted. In order to realize the management and control of VLAN entered the network service, the operators need to add a network layer VLAN tag for them.

Table 5- 2 ONU Processing mode in VLAN tag model

Direction	Whether Ethernet packets has Tag	Processing Mode
Upload	With VLAN tag	Discard
	W/O VLAN Tag	Adding new VLAN Tag and retransmission

Downlo ad	With VLAN tag	Transmission to the corresponding uni port according to VID and remove tag。
	W/O VLAN Tag	Discard

3. VLAN mode Translation

VLAN translation refers to the 1:1 conversion between the input VLAN and the output VLAN.

In this mode, ONU will change the upload Ethernet frame VLAN TAG (the VID may not be the only use, could be with other users using the same VID in the same system) to the network side only VLAN tag, and perform the reverse operation in the download direction. When the ONU support VLAN translation, the VLAN translation function should support Ether type value is 0x8100, optional support other Ether type values.

Table 5- 3 ONU ProceSSION mode in VLAN conversion mode

Directio n	Whether Ethernet packets has Tag	Processing Mode
Upload	With VLAN tag	Changing the VID to corresponding VID (output VID) according to the table then retransmission if the original TAG VID has corresponding entry (Equal to the VID input) in the corresponding port of the VLAN translation list, or else discard it.
	W/O VLAN Tag	Marking the untagged packet as default VLAN then retransmission.

Download	With VLAN tag	Changing the VID to corresponding VID(input VID) according to the table then retransmission if the original TAG VID has corresponding entry (Equal to the VID input) in the corresponding port of the VLAN translation list, or else discard it. Stripping tag and retransmission if the original TAG VID is default VID
	W/O VLAN Tag	Discard

4. VLAN mode Trunk

The ONU user side interface supports VLAN trunk function. By setting the ONU UNI port "VLAN allows" list to control whether forwarding message.

Table 5- 4 ONU Procession mode in VLAN Trunk model

Direction	Whether Ethernet packets has Tag	Processing Mode
Upload	Has VLAN tag	Up forwarding the message if its VLAN belongs to "permit VLAN" of the port, or else discard it.
	No VLAN Tag	Retransmission the packet after mark the untagged as default VLAN
Download	Has VLAN tag	Down forward the message if its VLAN belongs to "permit VLAN" of the port, or else discard it. Stripping VLAN tag and down forward it if the VLAN ID of the message is "default VID"
	No VLAN Tag	Discard

Configure ONU UNI VLAN transparent

The system configuration is defaulted in, if the original configuration of the other mode to change the transmission mode, configuration commands are as follows:

```
OLT (config-ONU-4:1)# port-vlan 1 mode transparent
```

Configure ONU UNI VLAN tag

Taking configuration ONU 1/1/2 first UNI port as example ONU1/1/2 example

Taking configuration of ONU 1/1/2 the first UNI port as example to explain ONU UNI VLAN marking configuration. The ONU 1/1/2 first port connected with the user's PC, user's data should be added VLAN 100 after enter into the ONU. Configuration commands as follows:

```
OLT (config-ONU-4:1)# port-vlan 1 mode tag 100 pri 0
```

Configure ONU UNI VLAN Trunk

Taking configuration of ONU 1/1/2 the first UNI port as example to explain ONU UNI VLAN trunk configuration. The ONU 1/1/2 first port connected to the AP Router, the router IP management data should not only be added VLAN 100 after enter into the ONU, but also pass through two businesses VLAN 2100 and 2101. Configuration commands are as follows:

Firstly configure the user port VLAN mode for trunk and PVID is 100, it has not yet come into effect at this moment.

```
OLT(config-ONU-4/1)# port-vlan 1 mode trunk 100 pri 1
```

Add trunk VLAN table

OLT(config-ONU-4/1)# port-vlan 1 trunk add 2100,2101

Configure ONU UNI VLAN Translation

1. Configuration mode for vlan translation, and interface pvid as 101

OLT(config-ONU-4/2)# port-vlan 1 mode translation 101 pri 1

2. Configuration vlan translation table

OLT(config-ONU-4/2)# port-vlan 1 translation add oldvlan 101 newvlan 102 pri 0

4.2 ONU UNI interface configuration management

1. Interface rate-limiting configuration

The port speed is divided into two kinds, the entrance and exit rate-limiting.

Configuration routines:

Configuration UNI port exit rate-limiting

OLT(config-ONU-4/2)# port-rate-limit 1 egress cir 1000 pir 100000

2. Enable port loop detection

OLT(config-ONU-4/2)# port-loop-detect 1 enable

3. Closing UNI interface

OLT(config-ONU-4/2)# port-shutdown 1

Opening UNI interface

OLT(config-ONU-4/2)# no port-shutdown 1

4. Enable port self-adaption

OLT(config-onu-4/2)# port-auto-neg 1 enable

5. fec switch

OLT(config-onu-4/2)# fec-mode mode enable

6. Port flow control

OLT(config-onu-4/2)# port-flow-control 1 enable

7. Check interface status

OLT(config-onu-4/2)# show onu-link-staus

5 Switching side configuration management

5.1 VLAN configuration management

VLAN (virtual local area network) is a kind of technology dividing logistically the LAN device into networks so as to realize the virtual work group. All the Et1000 VLAN are based on the port and all the GE interfaces are the VLAN1 member.

The same VLAN can have both tagged ports and untagged ports.

OLT supports three mode of port vlan mode: access /trunk /hybrid

Access: OLT one port only support one access vlan, it will be PVID;

Trunk: OLT can support a vlan list, and default it's PVID;

Hybrid: it can free specify.

5.1.1 VLAN interface

1.Create a VLAN command:

```
OLT(config)# vlan standard <1-4094>
```

Take setting up VLAN 2000 as example to show the operating steps.The VLAN 2000 interface members are uplink port GE1 and PON port PON 1, both of them act as tagged interface accede to VLAN. The configuration command as following:

```
OLT(config)# vlan standard 2000
```

```
OLT(config-vlan-2000)# port ge 1 tagged
```

```
OLT(config-vlan-2000)# port epon 1 tagged
```

```
OLT(config-vlan-2000)# show vlan
```

Attribute	Value
-----------	-------

VLAN ID	: 2000
---------	--------

Tagged Ports	: PON01,GE01
--------------	--------------

Untagged Ports	:
----------------	---

OLT(config-vlan-2000)#

Delet VLAN member port command:

OLT(config-vlan-2000)# no port epon 1

Delet VLAN command:

OLT(config-vlan-2000)# no vlan 2000

2.Create batch VLAN command:

OLT(config)# vlan standard <1-4094> <1-4094>

Take setting up VLAN 1000-2000 as example to show the operating steps.The VLAN 1000-2000 interface members are uplink port GE1 and PON port PON 1, both of them act as tagged interface accede to VLAN. The configuration command as following:

OLT(config)# vlan standard 1000 2000

```
OLT(config-vlan-<1000-2000>)#port ge 1 tagged
```

```
OLT(config-vlan-<1000-2000>)# port epon 1 tagged
```

Delet VLAN member port command:

```
OLT(config-vlan-<1000-2000>)# no port epon 1
```

Delet VLAN command:

```
OLT(config-vlan-<1000-2000>)# no vlan 2000
```

【Notice】

Above adding several interface to VLAN command can only be used when the interface mode is hybrid, this method cannot be used if in the other model .

If a VLAN is the management of VLAN, the configuration method is configuration after entering a port as a management interface node. This method was stated at the 1.3 section , here will not description no longer.

5.1.2 INTERFACE vlan configuration

As the 5.1 section is described, it can configure VLAN under VLAN interface mode in port hybrid mode, this section explains what port mode, and how to configure.

Interface VLAN is divided into three kinds: access、trunk、 hybrid

Configuration routines:

1. Set up VLAN

```
OLT(config)# vlan standard 2000
```

2. Configure Port Mode

OLT(config)# interface ge 1 #Enter the port node

OLT(config-ge-1)# vlan mode access

3. Configure VLAN

OLT(config-ge-1)# vlan access 2000

OLT(config-ge-1)# show vlan

Port vlan configuration:

Port type : access

Port default vlan : 2000

Tagged vlan :

Untagged vlan :

200

OLT(config-ge-1)#

4. The default port VLAN configuration (PVID):

OLT(config-ge-1)# port default-vlan 1000

5. Configure VLAN Qinq

VLAN Qinq shares resources with VLAN translate and can be configured with a total of 1024.

VLAN Qinq configuration VLAN 100 plus outer VLAN 200:

OLT(config-epon-1)# vlan qinq 100 200

VLAN QinQ configuration vlan 100-110 range plus outer VLAN 200:

```
OLT(config-epon-1)# vlan qinq batch 100 110 200
```

VLAN QinQ configuration show:

```
OLT(config-epon-1)# show vlan qinq
```

6. Configure VLAN translate

VLAN QinQ shares resources with VLAN translate and can be configured with a total of 1024.

VLAN translate configuration VLAN 100 to VLAN 200:

```
OLT(config-epon-1)# vlan translation 100 200
```

VLAN translate configuration show:

```
OLT(config-epon-1)# show vlan translation
```

5.2 MAC Address management and configuration

5.2.1 DISPLAY mac address table

Display all mac address:

```
OLT(config)# show mac-address all
```

Display the black hole MAC address table:

```
OLT(config)# show mac-address black-hole
```

Display the studied dynamic MAC address table:

```
OLT(config)# show mac-address dynamic
```

Displays the static MAC address table:

```
OLT(config)# show mac-address static
```

5.2.2 CONFIGURE mac address table

1. Configure MAC address aging time

```
OLT(config)# mac address-table age 100
```

2. Clear the MAC address table

```
OLT(config)# mac address-table flush all
```

3. Add a static MAC address table

```
OLT(config)# mac address-table static 00:11:22:33:44:55 vlan 100 port ge  
1
```

4. Add an MAC address to the black hole MAC address table, the source MAC address is 00:12:21:12:12:12, VLAN is 10 of the packets will be discarded.

```
OLT(config)# mac address-table black-hole 00:12:21:12:12:12 vlan 10
```

5.3 Port configuration management

5.3.1 Basic configuration

Port duplex mode attribute set:

```
OLT(config)# interface ge 2
```

```
OLT(config-ge-2)# port auto-negotiation enable duplex full
```

5.3.2 Broadcast/Multicast/Unicast storm control configuration

Limits the size of the broadcast traffic that the current port is allowed to receive:

OLT(config)# interface ge 1

OLT(config-ge-1)# port storm-control broadcast pps 1000

OLT(config-ge-1)# show storm-control

Port GE01 storm control:

Bulticast pps: 1000

Multicast pps: 0

Unicast pps: 0

Limits the size of the multicast traffic that the current port is allowed to receive:

OLT(config-ge-1)# port storm-control multicast pps 100

OLT(config-ge-1)# show storm-control

Port GE01 storm control:

Bulticast pps: 1000

Multicast pps: 100

Unicast pps: 0

Limits the size of the unkown unicast traffic that the current port is allowed to receive:

OLT(config-ge-1)# port storm-control unicast pps 10000

OLT(config-ge-1)# show storm-control

Port GE01 storm control:

Bulticast pps: 1000

Multicast pps: 100

Unicast pps: 10000

5.3.3 Port rate limit and traffic shaping configuration

```
OLT(config)# interface ge 1
```

```
OLT(config-ge-1)#
```

Confiure port egress rate limit:

```
OLT(config-ge-1)# port rate-limit egress 100
```

```
OLT(config-ge-1)# show ingress-rate
```

```
OLT(config-ge-1)# show state
```

Attribute	Value
-----------	-------

Port Name	: GE01
-----------	--------

Port State	: Enabled
------------	-----------

Link speed	: Auto-negotiation(- MBps -)
------------	------------------------------

Flow ctrl	: ON
-----------	------

MTU	: 1518
-----	--------

Link status	: DOWN
-------------	--------

Port traffic shaping:

Egress rate : 128 kbps

Ingress rate : 0 kbps

Port vlan configuration:

Port type : hybrid

Port default vlan : 1

Tagged vlan :

Untagged vlan :

OLT(config-ge-1)#

Cancel port rate limit:

OLT(config-ge-1)# no port rate-limit egress

5.3.4 Port statistic

OLT(config-ge-1)# show statistic

Rx rate (kbps): 0 Tx rate (kbps): 0

RX octets	: 0
RX frames	: 0
RX unicast frames	: 0
RX broadcast frames	: 0
RX multicast frames	: 0
RX discard frames	: 0
RX error frames	: 0
RX oversize frames	: 0
RX frames 64 octets	: 0
RX frames 65 to 127 octets	: 0
RX frames 128 to 255 octets	: 0
RX frames 256 to 511 octets	: 0
RX frames 512 to 1023 octets	: 0
RX frames 1024 to 1518 octets	: 0
TX octets	: 0
TX frames	: 0
TX unicast frames	: 0
TX broadcast frames	: 0
TX multicast frames	: 0
TX discard frames	: 0

```
TX error frames          : 0
TX oversize frames       : 0
TX frames 64 octets      : 0
TX frames 65 to 127 octets : 0
TX frames 128 to 255 octets : 0
TX frames 256 to 511 octets : 0
TX frames 512 to 1023 octets : 0
TX frames 1024 to 1518 octets : 0
```

```
OLT(config-ge-1)#
```

5.3.5 Port mirror

1. choose the port to mirror

```
OLT(config)# interface ge 1
```

2. choose the destination port

```
OLT(config-ge-1)# mirror dst-port ge 2 all
```

5.3.6 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.

1. PON Loop Detection

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 vlans 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 Detect Parameters Configuration

(1) Disable PON loop detection (the default is enable) :

```
OLT(config)# loop-detect pon disable
```

(2) Configure PON loop detection packet sending interval of 10 seconds (3-3600 seconds, default 5 seconds):

```
OLT(config)# loop-detect pon packet-send interval 10
```

(3) Configure PON loop detection recovery mode to be manual (default is automatic recovery) :

```
OLT(config)# loop-detect pon recover-mode manual
```

(4) PON loop detection recover manual:

```
OLT(config)# loop-detect pon recover manual
```

(5) Configure PON loop detection automatic recovery time of 50 seconds (3-3600 seconds, default 30 seconds):

```
OLT(config)# loop-detect pon recover-time 50
```

3. Uplink Loop Detection

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.

4. Uplink Loop Detect Parameters Configuration

(1) Disable Uplink loop detection (the default is enable) :

```
OLT(config)# loop-detect uplink disable
```

(2) Configure Uplink loop detection packet sending interval of 10 seconds (3-3600 seconds, default 5 seconds):

```
OLT(config)# loop-detect uplink packet-send interval 10
```

(3) Configure Uplink loop detection recovery mode to be manual (default is automatic recovery) :

```
OLT(config)# loop-detect uplink recover-mode manual
```

(4) Uplink loop detection recover manual:

```
OLT(config)# loop-detect uplink recover manual
```

(5) Configure Uplink loop detection automatic recovery time of 50 seconds (3-3600 seconds, default 30 seconds):

```
OLT(config)# loop-detect uplink recover-time 50
```

5.4 spanning-tree

5.4.1 Network demand

- ✧ ONU is 1:1, uplink port is ge3; Enable global RSTP.
- ✧ Configure the corresponding functions on global and uplink port .

5.4.2 Configuring steps

1. Enable the global RSTP function

OLT(config)# spanning-tree enable

2. Configure the device Bridge priority for is 4096

```
OLT(config)# spanning-tree priority 4096
```

Configure the device Forward Delay timer is 20s (Explain: The value of max-age is associated with hello and forward-delaymax-age,the specific relationship is : $2 * (\text{forward-delay} - 1) \geq \text{max-age} \geq 2 * (\text{hello} + 1)$), it will prompt the conflict configuration if several configuration does not meet this relationship.

```
OLT(config)# spanning-tree timer forward-delay 20
```

4. Configuration the device Hello timer value 5s

```
OLT(config)#spanning-tree timer hello 5
```

5. Configuration the device max-age timer value is 18s

```
OLT(config)#spanning-tree timer max-age 18
```

6. Configuration the device uplink port RSTP spending is 200000

```
OLT(config-ge-3)#spanning-tree cost 20000
```

7. Setting the device uplink port as boundary port

```
OLT(config-ge-3)#spanning-tree edged-port enable
```

8. Activating or closing equipment the point-to-point mode on of uplink port

OLT(config-ge-3)#spanning-tree point-to-point auto

OLT(config-ge-3)#spanning-tree point-to-point force-true

OLT(config-ge-3)#spanning-tree point-to-point force-false

9. Setting the device uplink port priority

OLT(config-ge-3)#spanning-tree port-priority 144

5.5 IGMP

5.5.1 Network demand

✧ ONU is 2/1,multicast VLAN is 100,router port is ge1; global mode to set IGMP mode.

✧ Configure the corresponding functions on global,multicast vlan and ONU .

5.5.2 Configuring steps

1. IGMP mode have three status:disable,snooping and proxy,default mode is disable.

eg:configure IGMP mode to snooping

OLT(config)#igmp mode snooping

2. igmp 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.

eg:fast leave enable

OLT(config)# igmp fast-leave enable

3. Igmp upstream protocol packets policy.When the policy is discard,Only programmes in the library of multicast programmes (see section 6) shall be effective;When the policy is pass, programs outside the program library can also take effect.Default is pass.

eg:igmp upstream protocol packets policy discard

OLT(config)# igmp protocol-packets policy discard

4. Configure the snooping mode parameters(Only configured in igmp mode for snooping):

(1).igmp group member 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.

eg:Configure igmp group member aging time with 200 seconds

OLT(config)# igmp snooping group-aging-time 200

5. Configure the proxy mode parameters(Only configured in igmp mode for proxy)

(1).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.

eg:Configure general query interval with 100 seconds

```
OLT(config)# igmp proxy gen-query-interval 100
```

(2).General query max 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.

eg:Configure general query max response time with 20 seconds

```
OLT(config)# igmp proxy gen-response-time 20
```

(3). robustness:This command 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.

eg:Configure robustness with 3

```
OLT(config)# igmp proxy robustness 3
```

(4).specific 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.

eg:Configure specific query interval with 2000 milliseconds

OLT(config)# igmp proxy sp-query-interval 2000

(5). specific query times: 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.

eg: Configure specific query times with 3

OLT(config)# igmp proxy sp-query-number 3

(6). specific query max response time: 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.

eg: Configure specific query max response time with 1000 milliseconds

OLT(config)# igmp proxy sp-response-time 1000

(7). 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.

eg: Configure query source with 192.168.1.1

OLT(config)# igmp proxy src-ip 192.168.1.1

(8). 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 in-band address.

eg: Configure query source MAC with 00:01:02:03:04:05

```
OLT(config)# igmp proxy src-mac 00:01:02:03:04:05
```

attention:The default aging time of multicast members in proxy mode is:
general query interval (125s)* robustness (2)+ general query maximum
response time (10s) = 260 seconds

6. Static multicast table entries:Statically added table entries are not limited by the aging time of member group aging.

eg:Add a static multicast table entry

```
OLT(config)# igmp static ip 224.1.1.1 ge 2 vlan 100
```

7. Multicast VLAN configuration

(1). Multicast unknown policy:If the multicast stream carries multicast unknown for a particular purpose, it is configured for transparent. Multicast unknown with no special purpose takes up bandwidth and is typically configured to be discarded, default is transparent.

eg:Configure Multicast unknown policy witch discard

```
OLT(multicast-vlan-100)# igmp multicast-unknown policy discard
```

(2).Multicast programs:Add the program library, users can switch to the multicast VLAN program channel.

eg:Add a program 224.1.1.1

```
OLT(multicast-vlan-100)# igmp program ip 224.1.1.1
```

eg:Add batch program 224.1.1.1-234.1.1.1

OLT(multicast-vlan-100)# igmp program ip batch 224.1.1.1 234.1.1.1

(3).Multicast router port:Routing port is a channel that connects to a multicast server and can only be configured with uplink port.

eg:Add a router port ge1

OLT(multicast-vlan-100)# igmp router-port ge 1

8. Show igmp Configuration

(1).show igmp config

OLT(config)# show igmp config

(2).show igmp entries

show igmp entries all:

OLT(config)# show igmp entry all

show igmp entries for dynamic:

OLT(config)# show igmp entry dynamic

show igmp entries for static:

OLT(config)# show igmp entry static

show igmp entry for multicast IP 224.1.1.1:

OLT(config)# show igmp entry multi-ip 224.1.1.1

show igmp entries for multicast vlan 100:

OLT(config)# show igmp entry vlan 100

9.show multicast vlan configuration

show multicast vlan configuration all:

OLT(config)# show multicast-vlan all

show multicast vlan configuration for vlan 100:

OLT(config)# show multicast-vlan 100

or:

OLT(multicast-vlan-100)# show multicast-vlan

10.ONU multicast configuration

(1).ONU multicast mode:default is igmp snooping mode,optional CTC controlled multicast mode.

eg:Configure ONU 2/1 multicast mode with ctc

OLT(config-ONU-2/1)# multicast mode ctc

show ONU 2/1 multicast mode:

OLT(config-ONU-2/1)# show multicast mode

(2).ONU fast leave:default is disable

eg:Configure ONU 2/1 fast leave enable

OLT(config-ONU-2/1)# multicast fast-leave-admin state enable

show ONU 2/1 multicast fast leave state:

OLT(config-onu-2/1)# show multicast fast-leave-state

(3).ONU multicast group num max:Only if the ONU multicast mode is configurable as igmp-snooping, the configuration will revert to the default value when the ONU multicast mode switches from igmp-snooping to another mode.The default is 64.

eg:Configure ONU 2/1:1 multicast group num max with 32

OLT(config-onu-2/1)# multicast 1 group-num_max 32

show ONU 2/1:1 multicast group num max:

OLT(config-onu-2/1)# show multicast 1 group-num-max

(4).ONU multicast vlan: 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 vlans.

eg:ONU 2/1:1 add multicast vlan 100

OLT(config-onu-2/1)# multicast 1 multicast-vlan 100

ONU 2/1:1 delete multicast vlan 100:

OLT(config-onu-2/1)# no multicast 1 multicast-vlan 100

ONU 2/1:1 clear multicast VLAN:

OLT(config-onu-2/1)# multicast 1 multicast-vlan clear

show ONU 2/1:1 multicast VLAN configuration:

OLT(config-onu-2/1)# show multicast 1 multicast-vlan

(5).ONU multicast tag mode: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. Up to 8 group translation can be configured.The default mode is untag.

eg:Configure ONU 2/1:1 with tag mode

```
OLT(config-onu-2/1)# multicast 1 tagmode tag
```

Configure ONU 2/1:1 multicast tagmode translate with VLAN 100 to 200(Up to 8 group translation):

```
OLT(config-onu-2/1)# multicast 1 tagmode translate 100 200
```

show ONU multicast tag mode:

```
OLT(config-onu-2/1)# show multicast 1 tagmode
```

6 ACL/QOS

6.1 Timerange

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

```
OLT(config)# time-range test 9:00 to 18:00 mon
```

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.

```
OLT(config)# time-range test from 9:00 2019/4/29 to 18:00 2019/4/29
```

2. Delete Time-range

You can delete one by one or delete all

```
OLT(config)# no time-range
```

```
NAME Time-range name
```

```
all Delete all
```

```
OLT(config)# no time-range test
```

```
OLT(config)#
```

6.2 ACL Management

Use this configuration to create an access control list when you need to filter specific packets through matching rules.

1. Basic ACL(2000-2999): 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.

```
OLT(config)# acl 2000
```

```
ACL 2000 create successful
```

```
OLT(acl-basic-2000)#
```

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

```
OLT(acl-basic-2000)# rule 1 deny source any
```

2. Advanced ACL(3000-4999): 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.

```
OLT(config)# acl 3000
```

```
ACL 3000 create successful
```

```
OLT(acl-adv-3000)#
```

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

```
OLT(acl-adv-3000)# rule 1 deny udp src-port 5000 time-range test
```

3. Link ACL(5000-5999): 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.

```
OLT(config)# acl 5000
```

```
ACL 5000 create successful
```

```
OLT(acl-link-5000)#
```

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

```
OLT(acl-link-5000)# rule 1 deny vlan 100
```

6.3 Packet Filter

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.

```
OLT(config)# packet-filter inbound 2000 port ge 4
```

6.4 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.

OLT(config)# show queue-scheduler

Queue scheduler mode : SP

Queue	Scheduler Mode	WRR Weight
-------	----------------	------------

0	SP	-
---	----	---

1	SP	-
---	----	---

2	SP	-
---	----	---

3	SP	-
---	----	---

4	SP	-
---	----	---

5	SP	-
---	----	---

6	SP	-
---	----	---

7	SP	-
---	----	---

Queue map:

Priority Queue

0	0
---	---

1	1
---	---

2	2
---	---

3 3

4 4

5 5

6 6

7 7

OLT(config)#

1. You can sets the mapping of prioritie and queue:

```
OLT(config)# qos cosq-map cos0 1 cos1 1 cos2 2 cos3 3 cos4 4 cos5 5 cos6  
6 cos7 7
```

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

```
OLT(config)# qos queue-scheduler wrr 10 20 30 40 0 0 0 0
```

7 Route

7.1 Route Management

1. Open route status:

```
OLT(config)# ip route enable
```

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

2. Add static route:

```
OLT(config)# ip route-static dest-ip 192.168.200.12 netmask  
255.255.255.0 next-hop 192.168.100.1
```

3. Display route static:

When next-hop is reachable,will learn the next-hop gateway ARP,the status will become reachable.OLT(config)#

```
OLT(config)# show route-table
```

```
IP Route:enable
```

```
-----  
Destination/Mask  Next-Hop      Interface  Protocol  Preference  Status  
-----  
192.168.200.0/24  192.168.100.1  VlanIf1   Static    2           Reachable  
192.168.100.0/24  192.168.100.2  VlanIf1   Direct    1           Reachable  
-----
```

```
OLT(config)#
```

```
OLT(config)# show arp-table
```

IP Address	MAC Address	Port	VLAN
------------	-------------	------	------

192.168.100.1	38:3a:21:f0:01:01	PON01	1
---------------	-------------------	-------	---

OLT(config)#

7.2 ARP Table

OLT(config)# show arp-table

IP Address	MAC Address	Port	VLAN
------------	-------------	------	------

192.168.100.1	38:3a:21:f0:01:01	PON01	1
---------------	-------------------	-------	---

OLT(config)#

8 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.

8.1 Create Link Aggregation

Attention:

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;

```
OLT(config)# link-aggregation group 1 member add ge 1-3
```

8.2 Display Link Aggregation

After successful creation, the member ports to join the link aggregation group can be viewed.

```
OLT(config)# show link-aggregation group
```

```
-----
```

```
Link Aggregation Group:1
```

```
Member Port: GE01,GE02,GE03
```

```
Load Balance Mode: Src MAC
```

```
-----
```

```
OLT(config)#
```

8.3 Port 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.

```
OLT(config)# link-aggregation group 1 load-balance src-ip
```

8.4 Remove Link Aggregation

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

```
OLT(config)# link-aggregation group 1 member delete ge 1-3
```

9 SYSTEM UPDATE

System support single image file update.

Update system or firmware.

Enter manage node:

```
OLT(config)# interface manage
```

Configur ftp username and password

```
OLT(config-manage)# ftp-client 123 123
```

2. Update system image:

```
OLT(config-manage)# update system 192.168.100.10 system.img
```

Update firmware image:

```
OLT(config-manage)# update firmware 192.168.100.10 firmware.img
```

10 WebGUI management support

See document EPON-OLT WebGUI UserManual.doc



语言: 简体中文 English | 固件版本号: Neutral-E04_V2.1.2_Rel | MAC地址: 38 3a 21 10 01 64

11 Abbreviation terminology

Abbreviation	English Explanation	Chinese Explanation
AES	Advanced Encryption Standard	高级加密标准
ARP	Address Resolution Protocol	地址解析协议
CATV	Cable Television	有线电视
CLI	Command Line Interface	命令行接口
MCSB	Main Control and Switching Board	控制与交换板卡
DBA	Dynamic Bandwidth Allocation	动态带宽分配
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DMA	Destination MAC address	目的 MAC 地址
DSCP	Differentiated Services Code Point	区分服务代码点
DTE	Data Terminal Equipment	数据终端设备
EMS	Element Management System	网元管理系统
FCAPS	Fault, Configuration, Accounting, Performance and Security management	故障、配置、统计、性能和安全
FTTB	Fiber To The Building	光纤到大楼
FTTC	Fiber to the Curb	光纤到路边
FTTH	Fiber To The Home	光纤到户
GE	Gigabit Ethernet	千兆以太网
GEM	GPON Encapsulation Method	GPON 封装模式
GPON	Gigabit-Capable Passive Optical Network	千兆无源光网络
ICMP	Internet Control Message Protocol	Internet 控制消息协议
LAG	Link Aggregation Group	链路汇聚组
MAC	Medium Access Control	介质访问控制
MDU	Multi Dwelling Units	多住户单元
MGCP	Media Gateway Control Protocol	媒体网关控制协议

Abbreviation	English Explanation	Chinese Explanation
MIB	Management Information Base	管理信息库
MTBF	Mean Time Between Failures	平均故障间隔时间
MTTR	Mean Time to Repair	平均修复时间
NE	Network Element	网元
OAM	Operation, Administration and Maintenance	操作、管理和维护
ODN	Optical Distribution Network	光分配网络
OLT	Optical Line Terminal	光线路终端
OMCI	ONU Management and Control Interface	ONU 管理控制接口
ONT	Optical Network Terminal	光网络终端
ONU	Optical Network Unit	光网络单元
PDU	Protocol Data Unit	协议数据单元
PIR	Peak Information Rate	峰值比特率
PMD	Physical Medium Dependent	物理介质相关
PON	Passive Optical Network	无源光网络
POTS	Plain Ordinary Telephone Service	普通常规电话业务
PVID	Port based VLAN ID	基于端口的 VLAN 号
PVST	Per-VLAN (Rapid) Spanning Tree	基于 VLAN 的生成树
QoS	Quality of Service	服务质量
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
RTT	Round Trip Time	环路时间
SCB	Single Copy Broadcast	单拷贝广播
SFU	Single Family Unit	单家庭单元
SLA	Service Level Agreement	服务等级协议
SMA	Source MAC Address	源 MAC 地址
SMB	Small to Medium Business	中小型企业
SMF	Single-mode Fiber	单模光纤
SNI	Service Node Interface	业务节点接口
SNMP	Simple Network Management Protocol	简单网络管理协议

Abbreviation	English Explanation	Chinese Explanation
STP	Spanning Tree Protocol	生成树协议
SVI	Switch Virtual Interface	交换虚拟接口
TC	Transmission Convergence	传输汇聚
T-CONT	Transmission Container	传输容器
TDM	Time Division Multiplex	时分复用
TOS	Type Of Service	业务类型
UNI	User Network Interface	用户侧接口
VLAN	Virtual Local Area Network	虚拟局域网
WRED	Weighted Random Early Detection	加权随机早期检测
WRR	Weighted Round Robin	加权轮询算法
XFP	10 Gigabit Small Form Factor Pluggable Module	10G 小型化可插拔光收发模块