

# EPON OLT WEB 管理用户手册

软件版本: epon\_firmware\_I\_V3.0.0\_Rel



# 目录

1 系统描述 .....	1
1.1 描述 .....	1
1.2 登录 .....	1
1.3 登录状态 .....	1
2 TOPO 图 .....	3
3 ONU 列表 .....	6
4 VLAN 管理 .....	9
5 高级设置 .....	11
5.1 运行状态 .....	11
5.2 系统管理 .....	11
5.2.1 设备管理 .....	11
5.2.2 诊断工具 .....	12
5.2.3 网络接口 .....	13
5.2.4 升级管理 .....	14
5.2.5 时间管理 .....	14
5.2.6 服务(SSH/SNMP) .....	15
5.2.7 告警列表 .....	18
5.2.8 用户管理 .....	18
5.3 PON 管理 .....	20
5.3.1 ONU 阻止列表 .....	20
5.3.2 上行带宽配置 .....	20
5.3.3 PON 设置 .....	21
5.3.4 LOID 允许列表 .....	23
5.3.5 ONU 批量升级 .....	24
5.3.6 PON 光诊断 .....	26
5.3.7 批量配置 .....	27
5.4 ONU 管理 .....	29
5.4.1 ONU 基本信息 .....	29

5.4.2 ONU 端口配置 .....	31
5.4.3 ONU 组播管理 .....	32
5.4.4 ONU 统计信息 .....	37
5.5 端口管理 .....	38
5.5.1 端口信息 .....	38
5.5.2 端口统计信息 .....	38
5.5.3 端口配置 .....	39
5.5.4 端口 VLAN .....	39
5.5.5 环路检测 .....	43
5.5.6 端口隔离 .....	47
5.6 MAC 地址管理 .....	47
5.7 协议管理 .....	50
5.7.1 RSTP .....	50
5.7.2 IGMP .....	52
5.7.3DHCP .....	57
5.7.4MSTP .....	61
5.8 ACL/QOS .....	65
5.8.1 时间范围 .....	65
5.8.2 ACL 管理 .....	67
5.8.3 包过滤 (Packet Filter) .....	70
5.8.4 QOS .....	71
5.9 路由 .....	72
5.9.1 路由管理 .....	72
5.9.2 ARP 表 .....	73
5.10 链路聚合 .....	73
1. 创建链路聚合 .....	73
2. 查看链路聚合 .....	74
3. 负载均衡选路算法 .....	74
4. 删除链路聚合 .....	75
6 快捷访问 .....	76

7root.....78

# 1 系统描述

## 1.1 描述

通过 OLT 带外口连接网络。OLT 的缺省带外管理地址是 192.168.100.1，请把电脑网段设置成跟带内想同网段 192.168.100.XXX(例如：192.168.100.100)，设置后才能通过带外管理 OLT。

## 1.2 登录

请打开浏览器（目前支持 firefox/chrome/IE 9 以及更高级版本）

输入 OLT 的 IP 地址：

- ①192.168.100.1（带外管理地址，接 NMS 口）
- ②192.168.99.1（带内管理地址，接上联口）

如下图所示，语言选择中文，并输入用户名和密码登录：



说明：

1. 默认的用户名是超级账户 root，用户密码是 admin，跟登录命令行是相同的；
2. 同一用户可以同时登录网页和命令行；
3. 页面超时退出是五分钟，如果在五分钟内没有任何操作，页面会自动退出；
4. 可以通过命令行设置默认中文语言“web-lang zh”。

## 1.3 登录状态

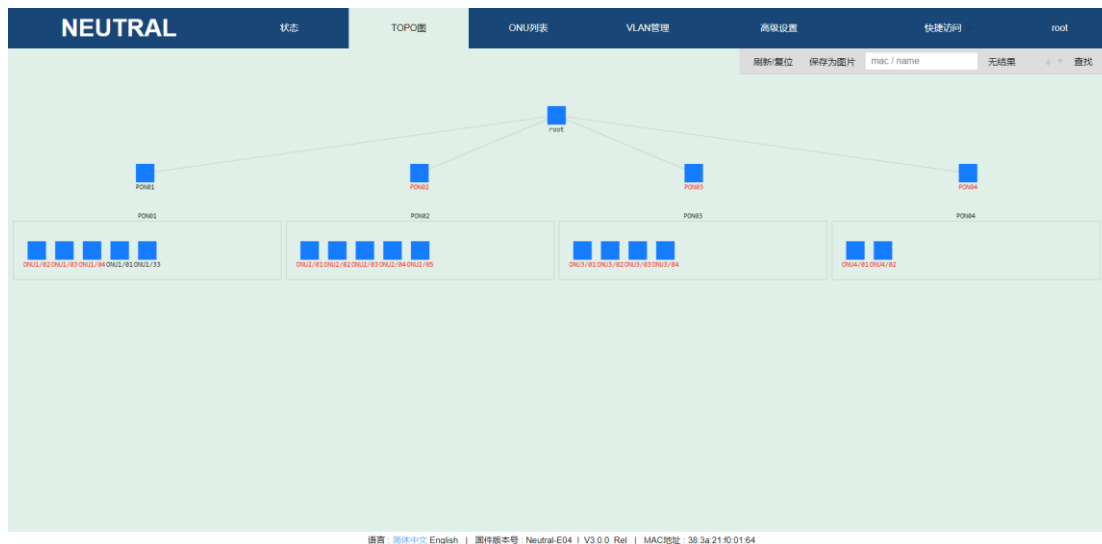
登录页面以后，可以看到如下页面：



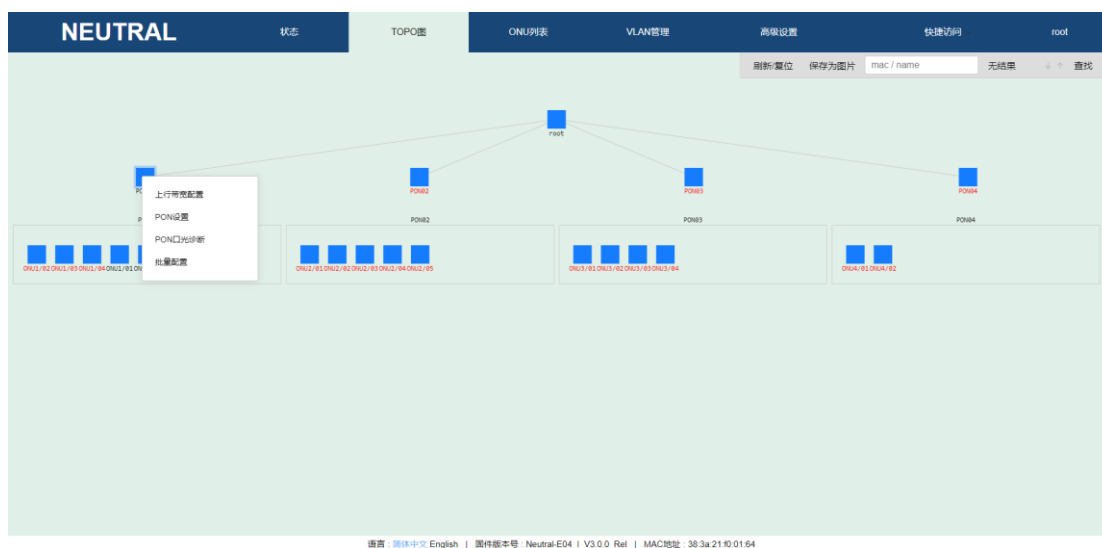
PON 口和上联口的状态展示在这里。PON 口将展示多少个 ONU 注册、多少个 ONU 在线和多少个 ONU 离线；上联口信息将展示端口管理状态以及链路连接状态，一目了然。

## 2 TOPO 图

下图展示了 PON 口的状态：（红色字体表示离线状态）

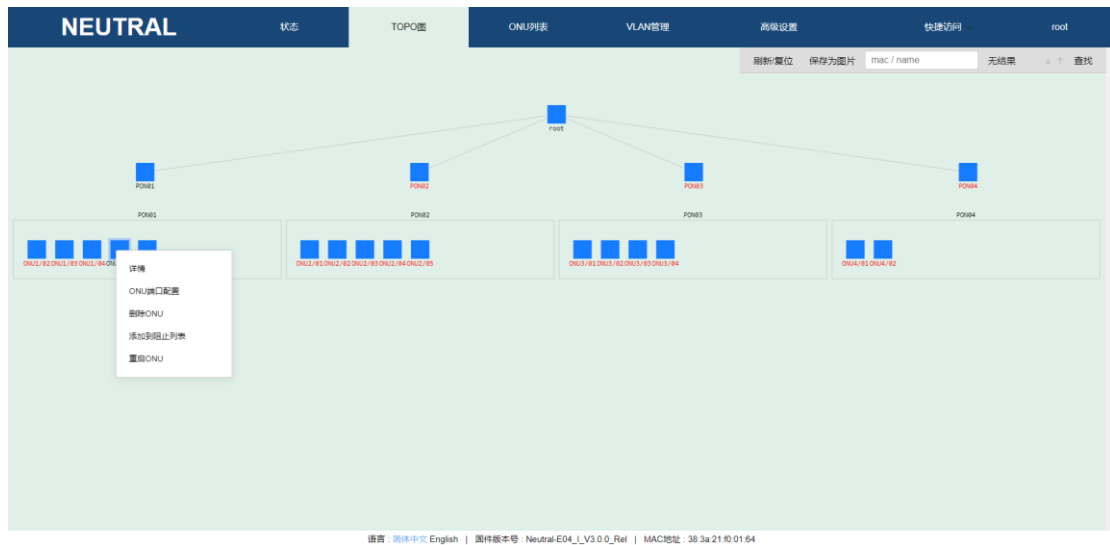


1. 鼠标右键点击 PON 口图标，可快捷访问高级设置——PON 管理——上行带宽配置、PON 设置、PON 口光诊断、批量配置。

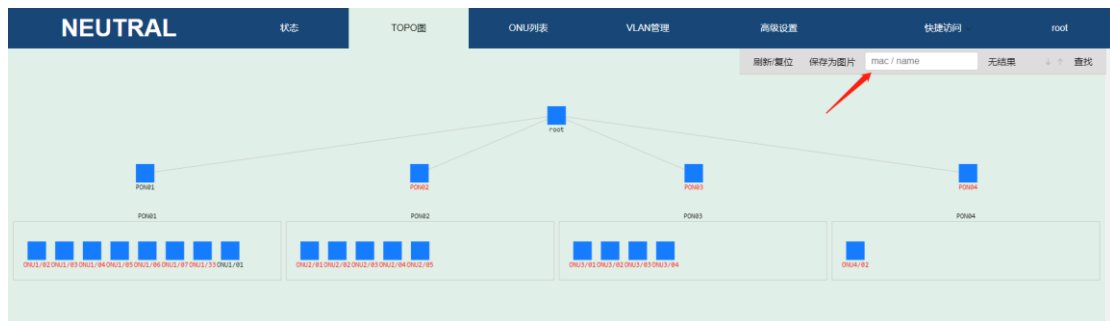


2. 鼠标右键点击 ONU 图标，可快捷访问高级设置——ONU 管理——基本信息、端口配置以及删除 ONU、重启 ONU 或者添加 ONU 到阻拦列表。





3. 鼠标光标移至 PON 图标，自动展示该端口在线情况、多少个 ONU 在线、多少个 ONU 离线。
4. 鼠标光标移至 ONU 图标，自动展示该台 ONU 的名称、MAC 地址、在线状态、认证状态。
5. 在界面右上角的灰色框通过搜索 ONU 名称或 ONU MAC 地址可以快速查找相应 ONU。



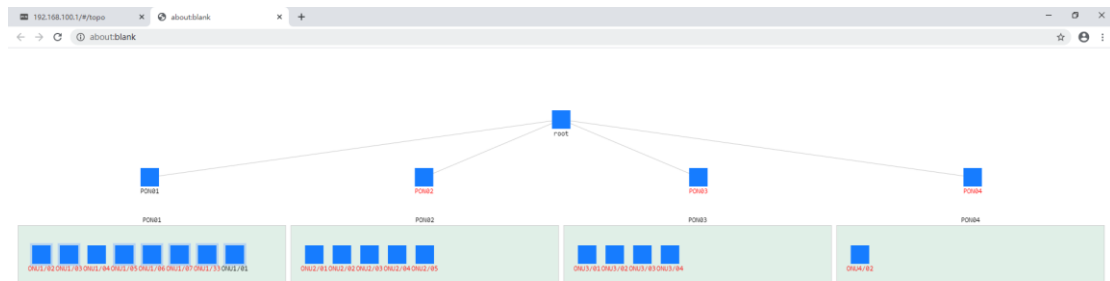
①可以任意输入部分或完整长度的 MAC 地址或名称，搜索结果数目显示如下图，通过点击上下黑色小箭头快速查看各个 ONU 的状态，同时对应的 ONU 图标自动闪烁五次。





②查找到的 ONU 图标外围包裹一层淡蓝色，点击刷新/复位重置图标状态。

③通过点击保存为图片，将当前拓扑图状态显示在浏览器新的标签页面。（原拓扑图界面不能右键操作）

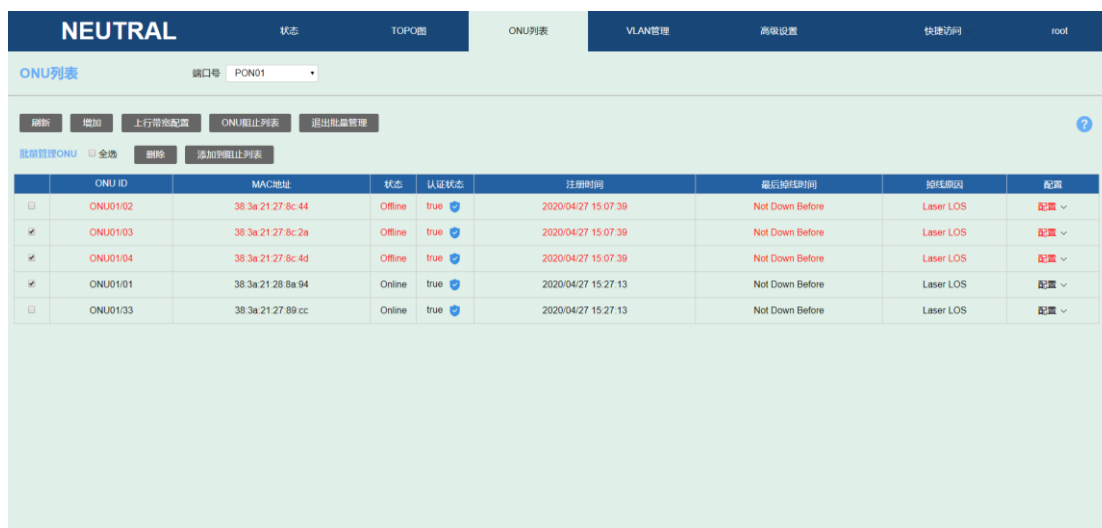


### 3 ONU 列表

①切换 PON ID 获取不同 PON 口的 ONU 列表

②红色字体展示的是离线 ONU

③最后掉线时间和掉线原因



1. 增加一个 ONU，可以指定 ONU ID 或者 ONU ID 为 0 自动分配 ONU ID



2. 点击上行带宽配置会进入到 PON 管理——上行带宽配置页面



### 3. 点击 ONU 阻止列表会进入到 PON 管理——ONU 阻止列表页面



### 4. 可以批量管理 ONU，可以删除 ONU 或者添加 ONU 到阻止列表 当点击批量管理 ONU 会出现以下界面：



可以勾选多个 ONU 同时操作

ONU列表 端口号 PON01

刷新 增加 上行带宽配置 ONU阻止列表 退出批量管理

批量管理ONU  全选 删除 添加到阻止列表

	ONU ID	MAC地址	状态	认证状态	注册时间	最后掉线时间	掉线原因	配置
<input type="checkbox"/>	ONU0102	38 3a 21 27 8c 44	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
<input checked="" type="checkbox"/>	ONU0103	38 3a 21 27 8c 2a	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
<input checked="" type="checkbox"/>	ONU0104	38 3a 21 27 8c 4d	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
<input checked="" type="checkbox"/>	ONU0101	38 3a 21 28 8a 94	Online	true	2020/04/27 17:50:00	Not Down Before	Laser LOS	配置
<input type="checkbox"/>	ONU0133	38 3a 21 27 89 cc	Online	true	2020/04/27 17:50:04	2020/04/27 17:38:21	Laser LOS	配置

5. 鼠标光标移至配置自动展示以下界面：

ONU列表 端口号 PON01

刷新 增加 上行带宽配置 ONU阻止列表 批量管理ONU

查找 ONU  输入MAC地址或名称搜索ONU，支持部分匹配和正则表达式

ONU ID	MAC地址	状态	认证状态	注册时间	最后掉线时间	掉线原因	配置
ONU0102	38 3a 21 27 8c 44	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
ONU0103	38 3a 21 27 8c 2a	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
ONU0104	38 3a 21 27 8c 4d	Offline	true	2020/04/27 15:07:39	Not Down Before	Laser LOS	配置
ONU0101	38 3a 21 28 8a 94	Online	true	2020/04/28 10:18:41	Not Down Before	Power Down	配置
ONU0133	38 3a 21 27 89 cc	Online	true	2020/04/28 10:18:39	2020/04/28 10:16:10	Power Down	配置

详情

ONU端口配置

删除ONU

添加到阻止列表

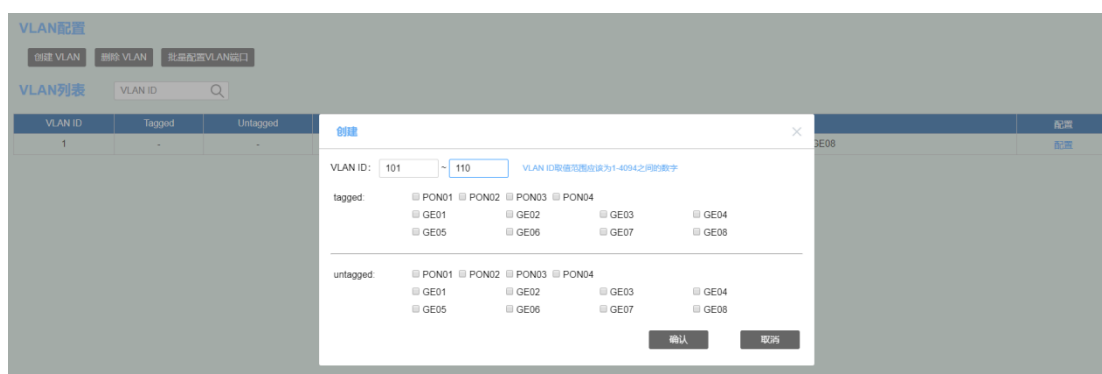
重置ONU

## 4 VLAN 管理

下图 VLAN 管理展示了 VLAN 列表的成员端口包括带标签端口（tagged），不带标签端口（untagged）和作为缺省 VLAN 端口。



1. 创建 VLAN: 输入 VLAN ID, 选择带标签(tagged port)或不带标签(untagged port)。如果想要创建一个 VLAN, 输入相同的 VLAN ID 即可; 若要创建连续的多个 VLAN, 可以输入一个有效的 VLAN ID 范围。



2. 删除 VLAN 也是一样, 可以选择删除单个或者删除连续的 VLAN ID

**VLAN配置**

创建 VLAN 删除 VLAN 批量配置VLAN端口

**VLAN列表**

VLAN ID	Tagged	Untagged	As Default VLAN Port	配置
1	-	-	PON01, PON02, PON03, PON04, GE01, GE02, GE03, GE04, GE05, GE06, GE07, GE08	<a href="#">配置</a>
101	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
102	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
103	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
104	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
105	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
106	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
107	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
108	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
109	-	-	-	<a href="#">配置</a> <a href="#">删除</a>
110	-	-	-	<a href="#">配置</a> <a href="#">删除</a>

**删除 VLAN** X

VLAN ID  -

VLAN ID取值范围应该为1-4094之间的数字

**VLAN配置**

✓ 设置成功

创建 VLAN 删除 VLAN 批量配置VLAN端口

**VLAN列表**

VLAN ID	Tagged	Untagged	As Default VLAN Port	配置
1	-	-	PON01, PON02, PON03, PON04, GE01, GE02, GE03, GE04, GE05, GE06, GE07, GE08	<a href="#">配置</a>

## 5 高级设置

### 5.1 运行状态

下图展示了本台 OLT 的系统信息、硬件状态、系统运行时间



### 5.2 系统管理

#### 5.2.1 设备管理

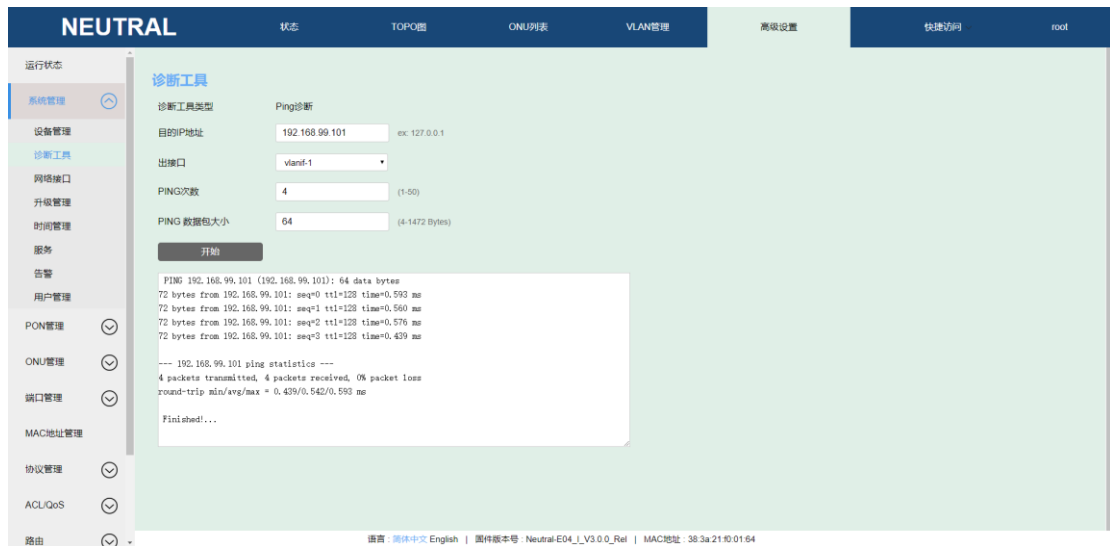
1. 重启 OLT
2. 备份 OLT 配置
3. 导入 OLT 配置
4. 恢复出厂设置
5. 保存配置
6. 查看当前配置（导出 txt 配置文件）



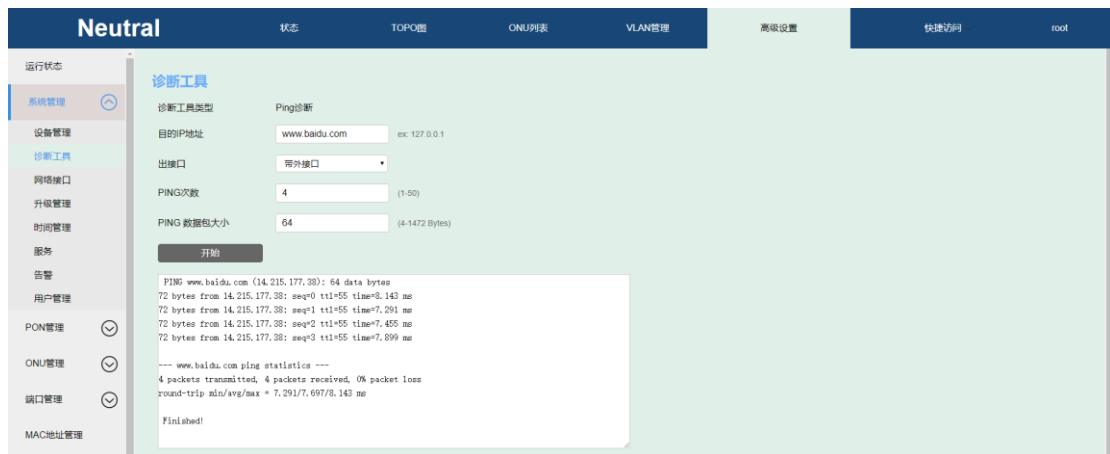


## 5.2.2 诊断工具

设备支持 ping 诊断，检查链路连接情况。



支持 ping 域名



## 5.2.3 网络接口

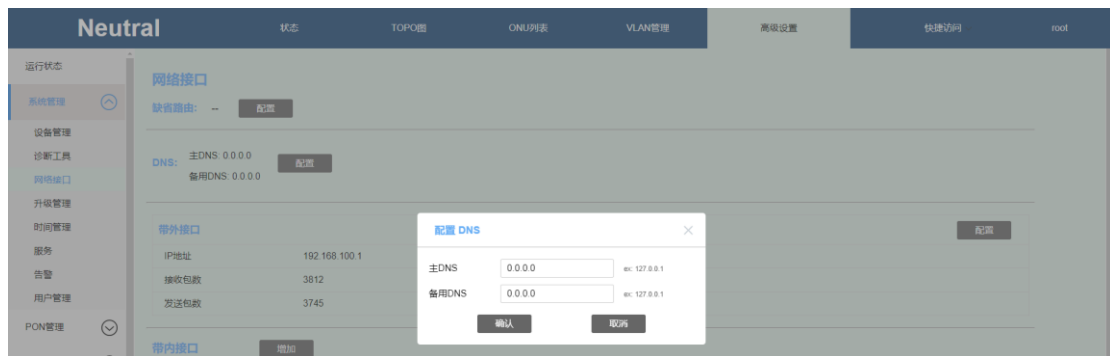
默认的远程管理接口是带外口（NMS 口）和带内口（上联口）



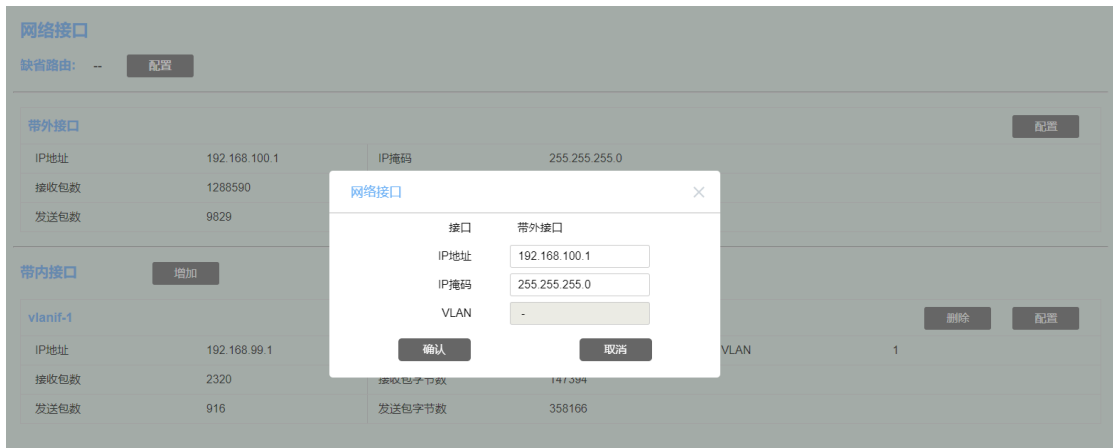
### 1. 配置默认路由（配置缺省路由必须存在带内或者带外存在的网段）



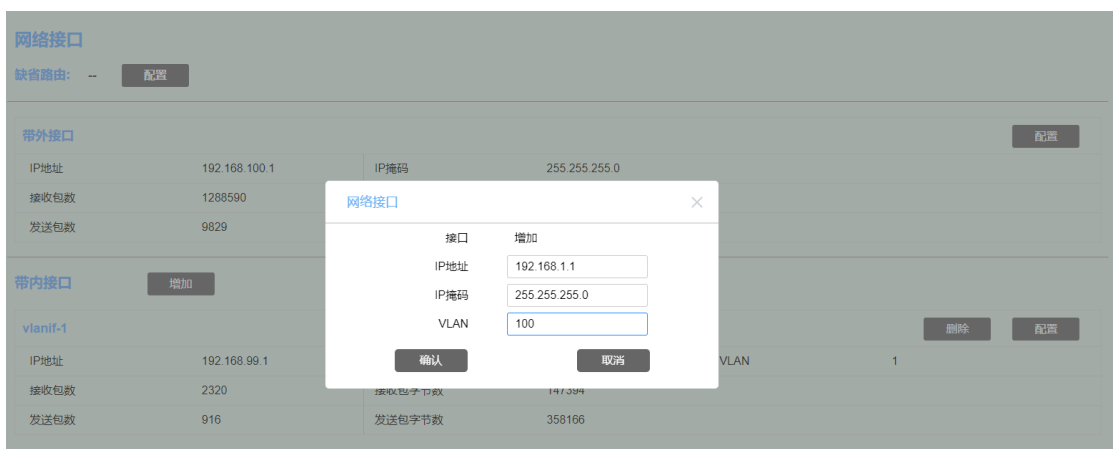
### 2. DNS



### 3. 配置带外管理 IP 地址



#### 4. 带内管理（在增加带内管理前，要先创建相应的 VLAN）



### 5.2.4 升级管理

可以通过该配置升级固件（firmware/img 文件）、系统（system/img 文件）和全版本（upgrade/压缩包文件）。



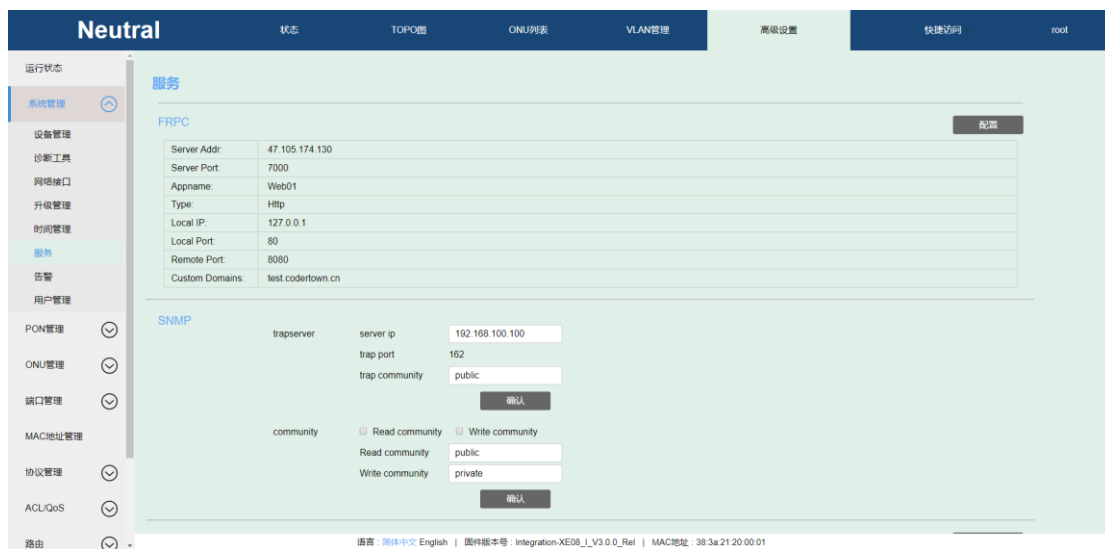
### 5.2.5 时间管理

1. 配置时区
2. 配置 OLT 系统时间



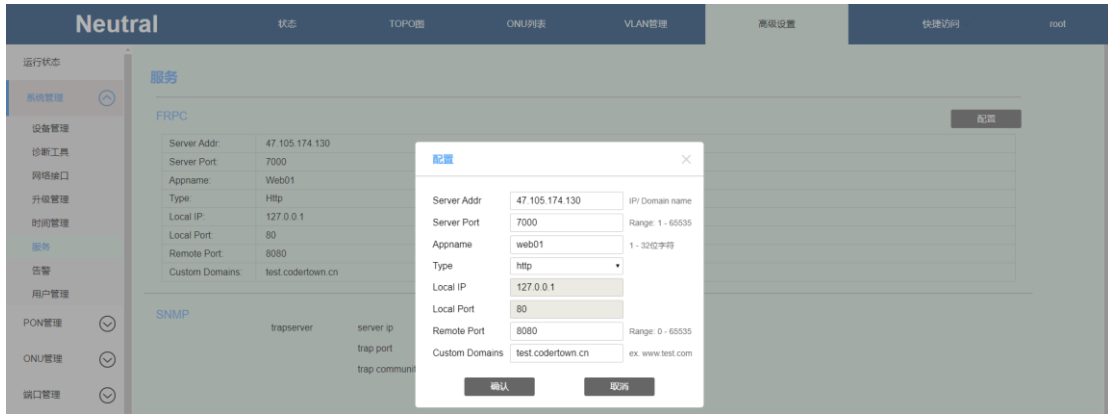
## 5.2.6 服务(SSH/SNMP)

如果想要更高安全级别的连接，可以通过 SSH 登录命令行：



### 1. FRPC

FRP 是一个可用于内网穿透的高性能的反向代理应用，本设备支持配置成 FRP 客户端，用户可以自建服务器来进行远程管理。类型仅支持 http 协议。



## 2. SNMP 配置

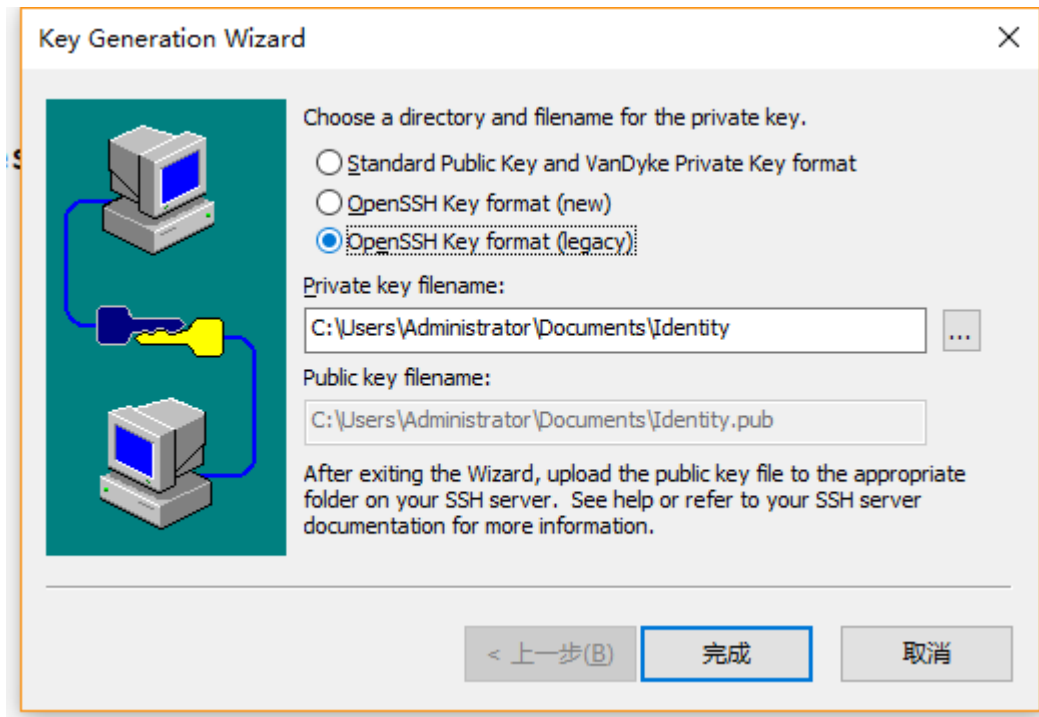
设置支持配置 trap server 和 community

## 3. SH Access

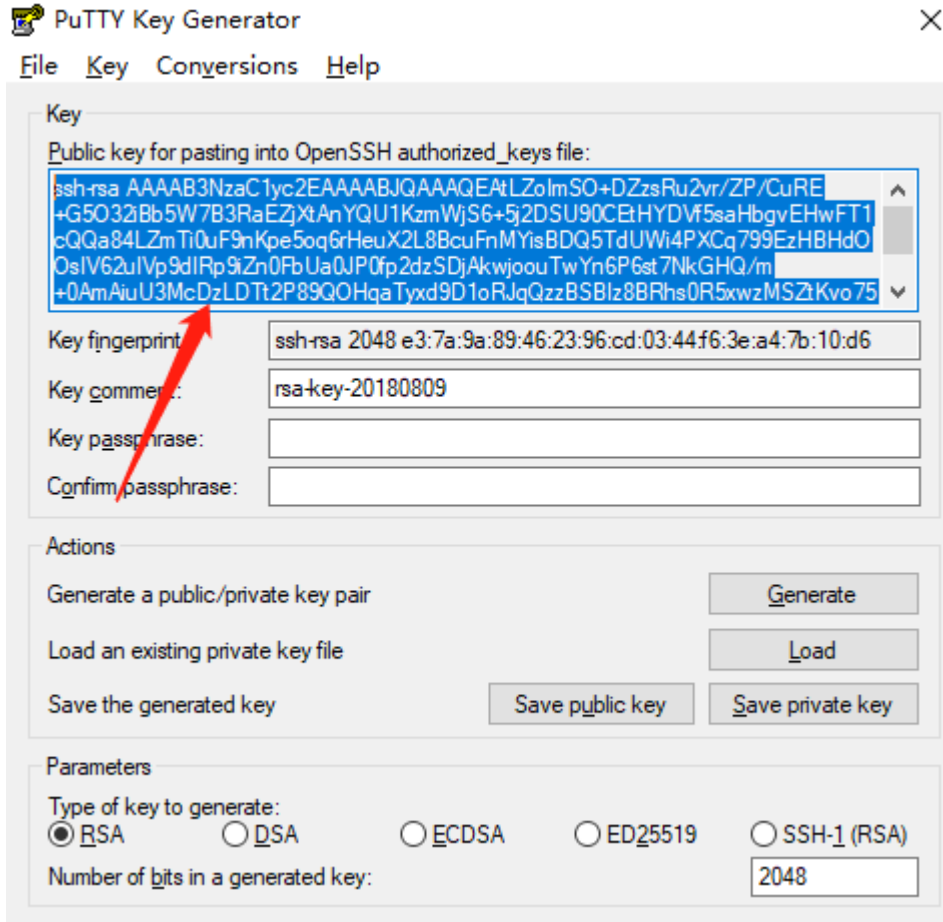
首先，您需要向服务器添加一个公钥。

**注意：**您需要创建一个 OPENSSH 格式的公钥，它的类型需要按 legacy、密钥类型 RSA 创建。

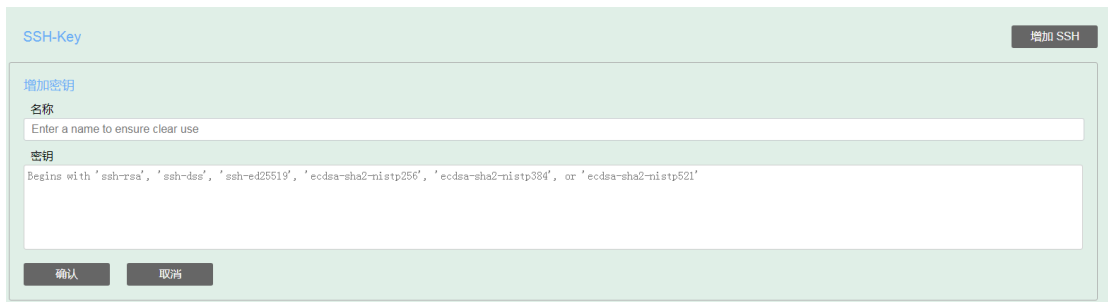
SecureCRT:



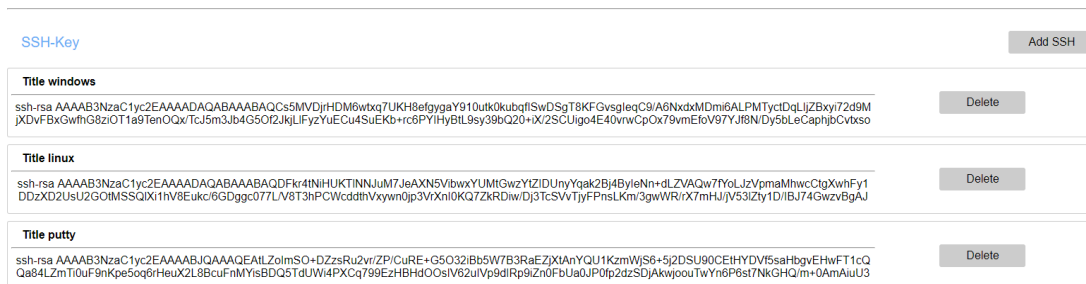
Puttygen 密钥生成器:



①把上面的公钥填进 OLT



②完成增加



现在可以通过用户名密码登录了。

## 5.2.7 告警列表

告警信息

[2020/04/27 18:59:31] Info: GE 4 Uplink port link down  
[2020/04/27 18:58:21] Info: GE 4 Uplink port link up  
[2020/04/27 18:51:39] Info: GE 1 Uplink port link up  
[2020/04/27 18:51:15] Info: GE 1 Uplink port link down  
[2020/04/27 18:01:27] Info: GE 1 Uplink port link up  
[2020/04/27 18:00:13] Info: GE 1 Uplink port link down  
[2020/04/27 17:55:50] Info: GE 4 Uplink port link down  
[2020/04/27 17:54:14] Info: GE 4 Uplink port link up  
[2020/04/27 17:50:04] Info: ONU 1/33 38.3a.21.27.89 cc ONU link up  
[2020/04/27 17:50:01] Info: ONU 1/33 38.3a.21.27.89 cc ONU authorization success  
[2020/04/27 17:50:00] Info: ONU 1/1 38.3a.21.28.8a.94 ONU link up  
[2020/04/27 17:49:57] Info: ONU 1/1 38.3a.21.28.8a.94 ONU authorization success  
[2020/04/27 17:47:24] Info: GE 2 Uplink port link down  
[2020/04/27 17:46:56] Info: GE 1 Uplink port link up  
[2020/04/27 17:46:47] Info: GE 2 Uplink port link up  
[2020/04/27 17:46:43] Info: GE 1 Uplink port link down  
[2020/04/27 17:45:28] Info: GE 1 Uplink port link up  
[2020/04/27 17:45:25] Info: GE 1 Uplink port link down  
[2020/04/27 17:45:11] Info: GE 1 Uplink port link up  
[2020/04/27 17:45:06] Info: GE 2 Uplink port link down  
[2020/04/27 17:45:01] Info: GE 1 Uplink port link down  
[2020/04/27 17:44:41] Info: GE 1 Uplink port link up  
[2020/04/27 17:43:51] Info: GE 1 Uplink port link down  
[2020/04/27 17:40:12] Info: GE 2 Uplink port link up  
[2020/04/27 17:38:21] Info: ONU 1/33 38.3a.21.27.89 cc ONU link down  
[2020/04/27 15:27:13] Info: ONU 1/1 38.3a.21.27.89 cc ONU link up  
[2020/04/27 15:27:13] Info: ONU 1/1 38.3a.21.28.8a.94 ONU link up

语言: 简体中文 English | 固件版本号: Neutral-ED4\_L\_V3.0.0\_Rel | MAC地址: 38.3a.21.01.64

## 5.2.8 用户管理

用户管理

当前已有用户列表

用户	状态	用户权限	最大登录次数	已登录次数	描述信息
root	在线	super	1	1	Super User

语言: 简体中文 English | 固件版本号: Neutral-ED4\_L\_V3.0.0\_Rel | MAC地址: 38.3a.21.01.64

在用户管理菜单，可以增加、删除用户、修改用户密码

增加用户：



超级用户（root）不能删除



修改用户密码，只能修改自己登录账户的密码。





## 删除指定用户

用户管理

当前已有用户列表 增加用户 删除用户 修改当前用户密码

用户	状态	用户权限	最大登录次数	描述信息
root	在线	super	1	Super User
zeng111111	离线	admin	3	3
test	离线	operator	3	test

删除用户

用户

确认 取消

用户管理

当前已有用户列表 增加用户 删除用户 修改当前用户密码

✓ 删除成功

用户	状态	用户权限	最大登录次数	描述信息
root	在线	super	1	Super User
zeng111111	离线	admin	3	3

## 5.3 PON 管理

### 5.3.1 ONU 阻止列表

NEUTRAL

状态 TOPO图 ONU列表 VLAN管理 高级设置 快速访问 root

运行状态

系统管理

PON管理

ONU阻止列表

上行带宽配置

PON设置

LOID允许列表

ONU批量升级

PON口光诊断

批量配置

ONU管理

端口管理

MAC地址管理

协议管理

ACL/QoS

路由

ONU阻止列表 端口号: PON01

增加

ONU ID	名称	MAC地址	重复次数	配置
No data				

语言: 简体中文 English | 固件版本号: Neutral-ED4\_V3.0.0\_Rel | MAC地址: 38 3a 21 01 64

### 增加 onu 到阻止列表

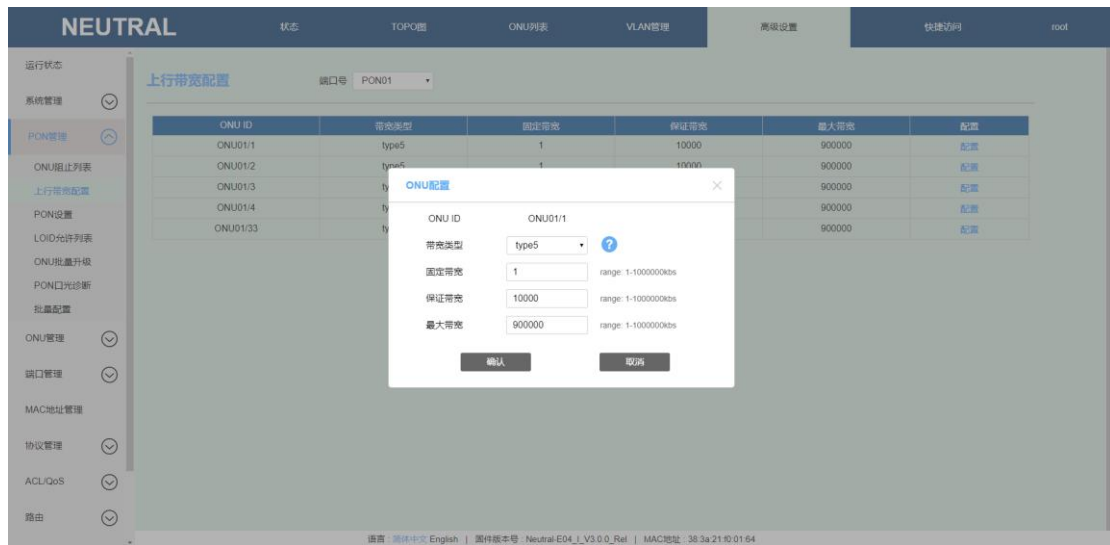
ONU阻止列表 端口号: PON01

增加

MAC地址  描述信息  确认 取消

ONU ID	名称	MAC地址	重复次数	配置
No data				

### 5.3.2 上行带宽配置



### 5.3.3 PON 设置

#### 5.3.3.1 PON 鉴权

该功能可以配置 PON 口的鉴权类型和认证模式



修改类型为手动添加



修改认证模式，可支持 MAC,LOID,LOID+PASSWORD,Hybrid



### 5.3.3.2 P2P

该配置可以设置 P2P 是否开启。如果启用 P2P，则 PON 中的 ONU 可以相互通信。默认状态为禁用



### 5.3.3.3 流氓 ONU 检测

检测 PON 口下是否存在流氓 ONU，缺省情况下不打开

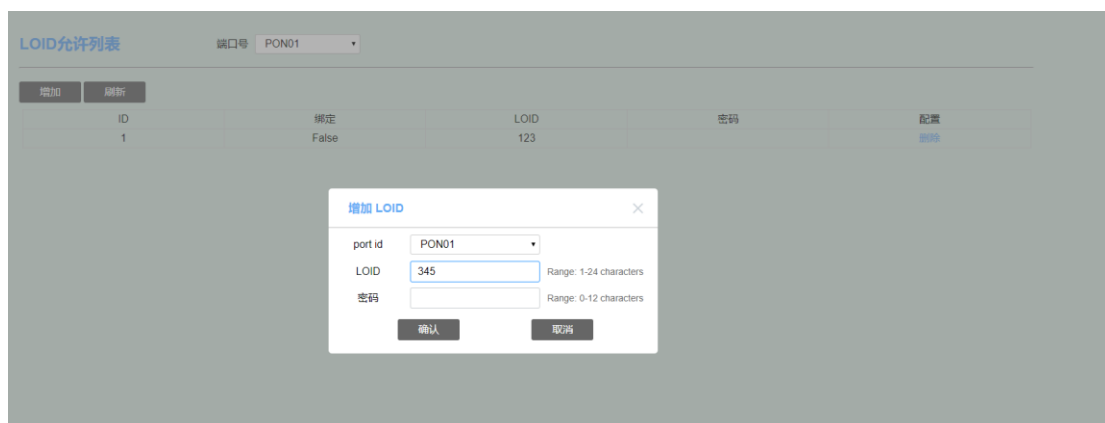


改为手动检测



### 5.3.4 LOID 允许列表

增加 LOID



删除 LOID

LOID允许列表 端口号: PON01

增加 刷新

ID	绑定	LOID	密码	配置
1	False	123		删除
2	False	345		删除

### 5.3.5 ONU 批量升级



在当前配置里面，若要升级 ONU 镜像，要先配置 ONU 升级类型



接下来需要绑定 ONU 类型



选择需要升级的 ONU

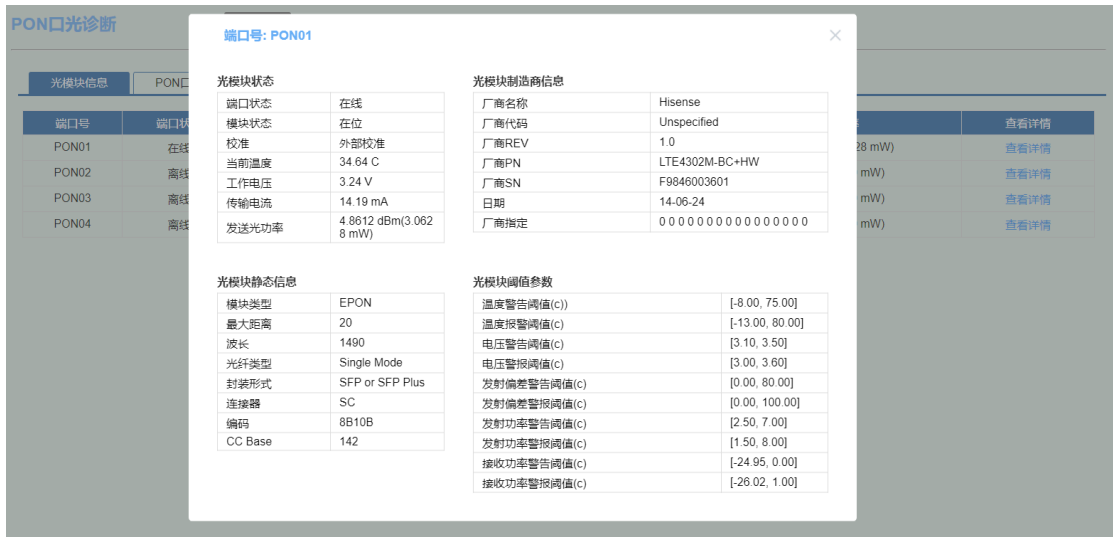


接下来，选择升级文件、升级类型和你想要升级的 PON 口，点击确认，OLT 就会开始批量升级指定的 ONU。

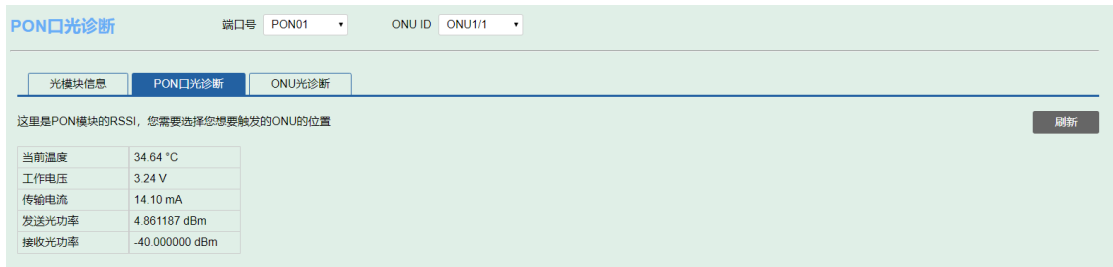


### 5.3.6 PON 光诊断

#### 1. 光模块信息查看



#### 2. 读取 PON 口光模块光诊断信息



#### 3. 读取 ONU 光诊断信息，需要先手动刷新获取 ONU 光功率数据

PON口光诊断 端口号 PON01 刷新

光模块信息 PON口光诊断 ONU光诊断

ONU ID	当前温度	工作电压	传输电流	发送光功率	接收光功率
ONU01/01	20 °C	3.40 V	15 mA	2.3289 dBm	-8.5886 dBm
ONU01/33	38 °C	3.36 V	17 mA	2.3877 dBm	-6.2342 dBm

### 5.3.7 批量配置

支持配置 ONU 端口 VLAN、ONU WLAN、ONU WAN 连接

**注意：**该配置为私有协议，仅支持本司 ONU！

NEUTRAL 状态 TOPO图 ONU列表 VLAN管理 高级设置 快速访问 root

运行状态 系统管理 PON管理 ONU阻止列表 上行带宽配置 PON设置 LOID允许列表 ONU批量升级 PON口光诊断 批量配置 ONU管理 端口管理 MAC地址管理 协议管理 ACL/DoS 路由

批量管理ONU 端口号 PON01

ONU端口VLAN WLAN WAN连接

增加

ONU端口号	模式	VLAN ID	配置
No data			

语言: 简体中文 English | 固件版本号: Neutral-E04\_L\_V3.0.0\_Rel | MAC地址: 38-3a-21-01-01-64

#### 1. ONU 端口 VLAN

最多支持配置 8 个 ONU 端口号的 VLAN

批量管理ONU 端口号 PON01 设置成功

ONU端口VLAN WLAN WAN连接

增加

ONU端口号	模式	VLAN ID	配置
1	transparent	100	清除
2	transparent	101	清除
3	transparent	102	清除
4	transparent	103	清除

#### 2. ONU WLAN，可修改加密方式、SSID 名称、SSID 密码

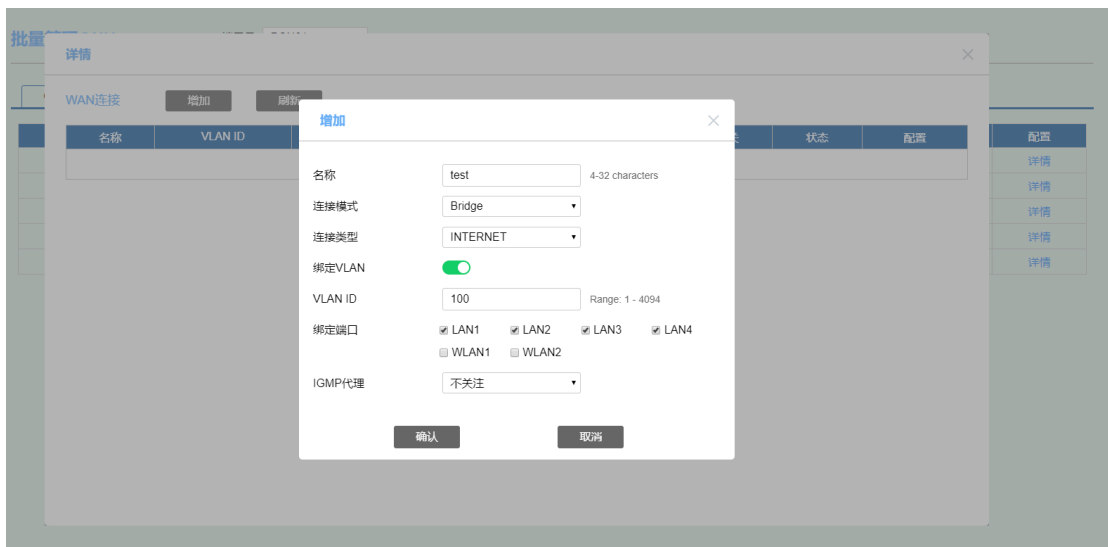




### 3. WAN 连接，展示了 PON 口下所有 ONU 的 wan 连接状态



### 添加 WAN 连接



若删除刚添加的 WAN 连接，需等待 30s



## 5.4 ONU 管理

### 5.4.1 ONU 基本信息



如上图，可以完成以下操作：

1. 设置 ONU 基本信息、ONU 名称和 ONU 描述信息。

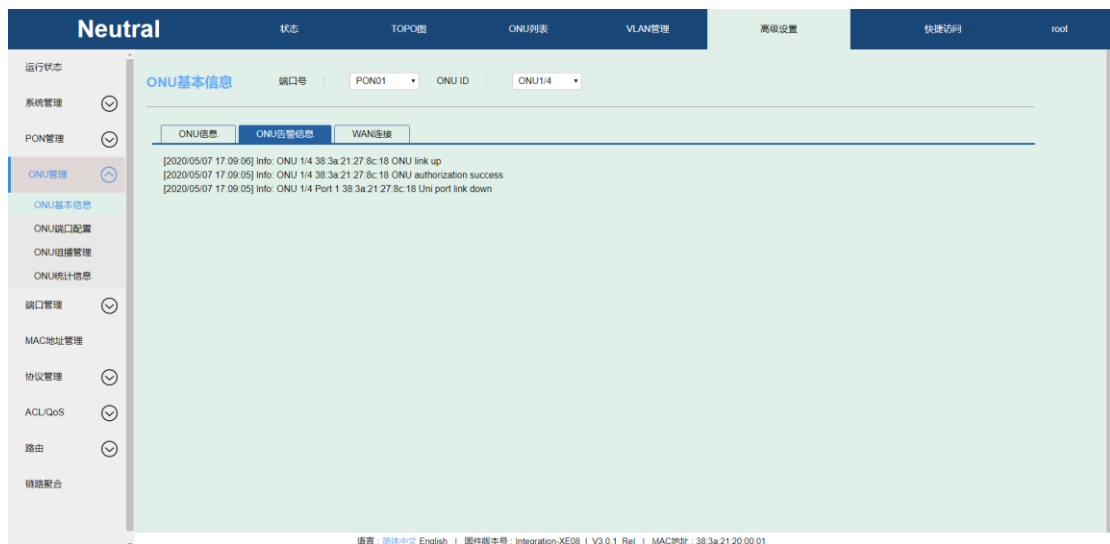


2. 重启 ONU
3. 解注册 ONU
4. 更改 fec mode
5. 刷新 ONU 光诊断数据
6. ONU 升级管理

如下操作，选择升级文件并点击确认，该 ONU 就会进入升级状态

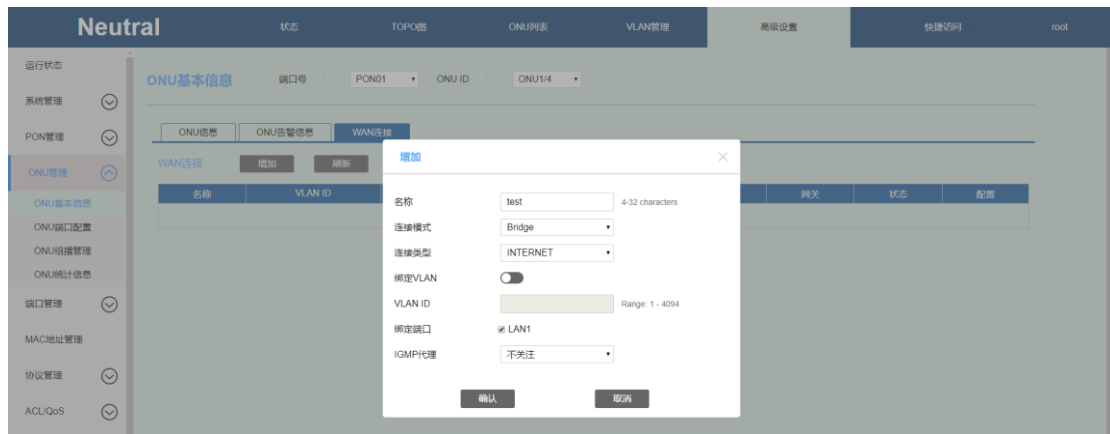


## 7. 查看 ONU 告警信息



## 8. 单页 WAN 链接配置

**注意：**该配置为私有协议，仅支持本司 ONU！



## 5.4.2 ONU 端口配置



1. 可以根据端口号和 ONU ID 选择想要配置的 ONU
2. 如下所示可以配置 ONU 的基本功能

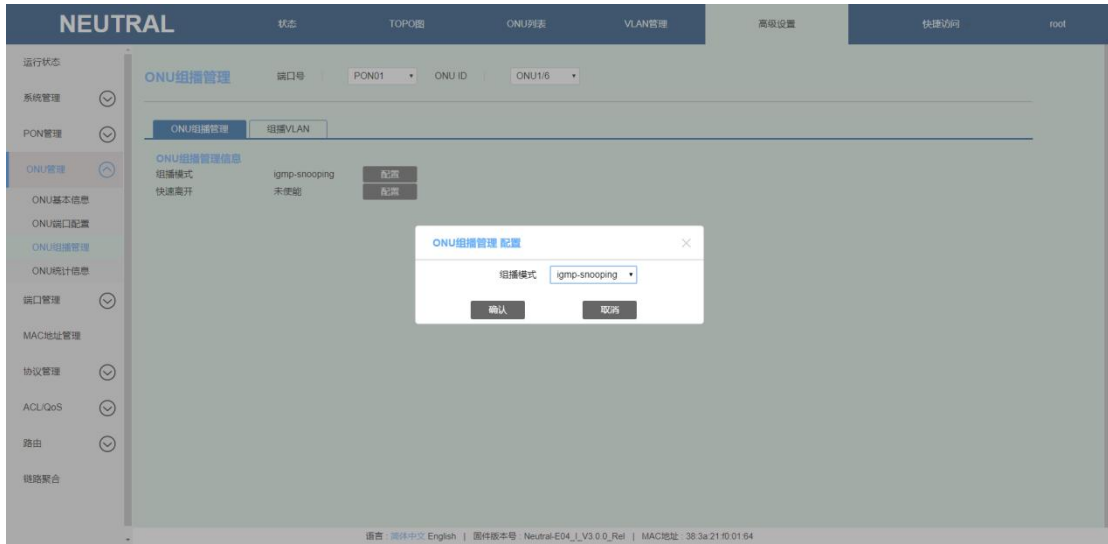


### 3. 配置端口 VLAN

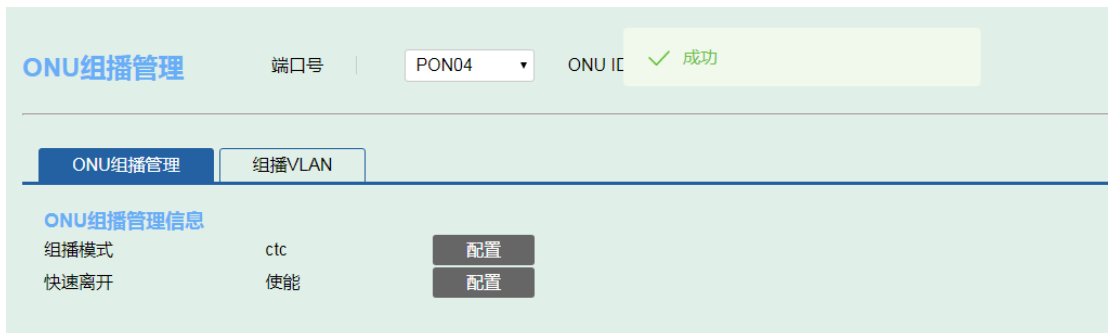


## 5.4.3 ONU 组播管理

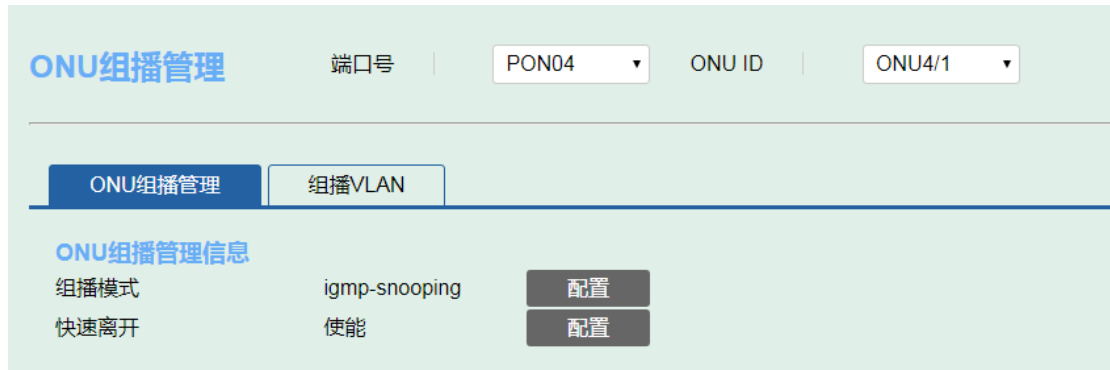
### 1. 配置 ONU 组播模式



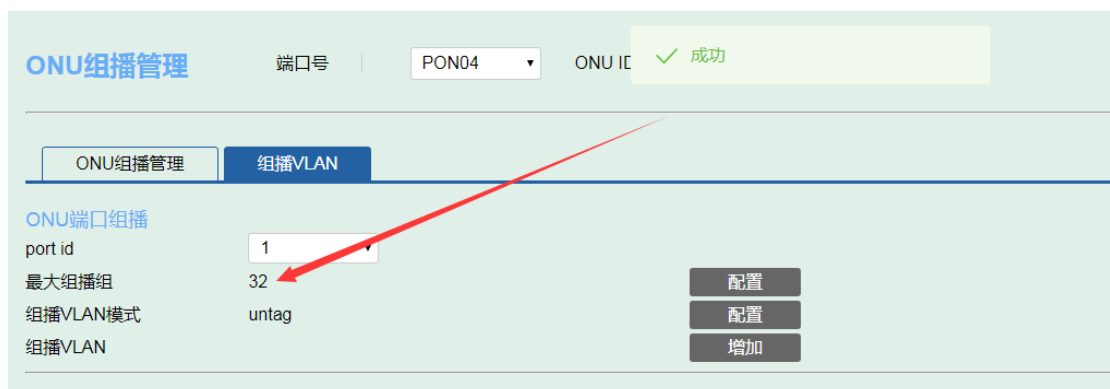
## 2. 配置 ONU 组播快速离开



3. 配置 ONU 最大组播组：仅在 ONU 组播模式为 igmp-snooping 可配置，当 ONU 组播模式从 igmp-snooping 切换为其他模式时，配置将会恢复缺省值，缺省为 64。首先需要检查 ONU 组播模式为 igmp-snooping 模式：

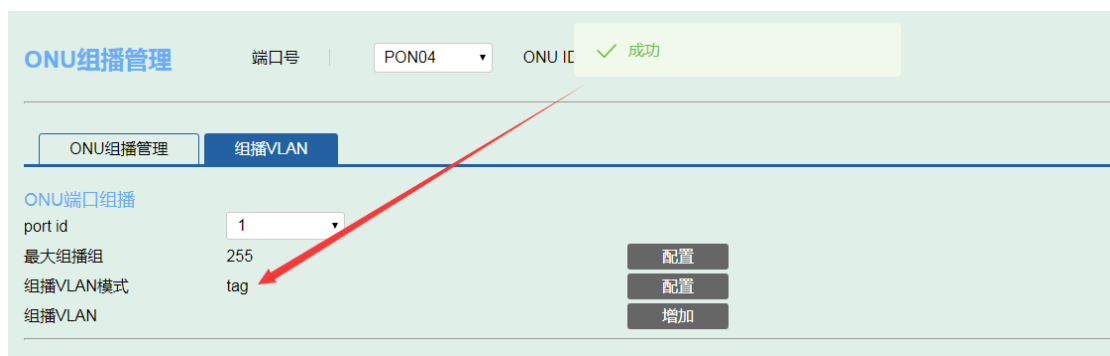


接下来就可以配置 ONU 最大组播组数，最大值 255（CTC 标准定义最大值，具体得看 ONU 支持）



4. 配置组播 VLAN 模式：该配置决定 ONU 端口转发出去的组播业务流是否带 VLAN 标签，untag 为剥除标签，tag 为不剥除标签，translate 为转换 VLAN 标签，最多可以配置 8 组转换。缺省模式为 untag。

配置 ONU 组播 VLAN 模式为 tag 或 untag:



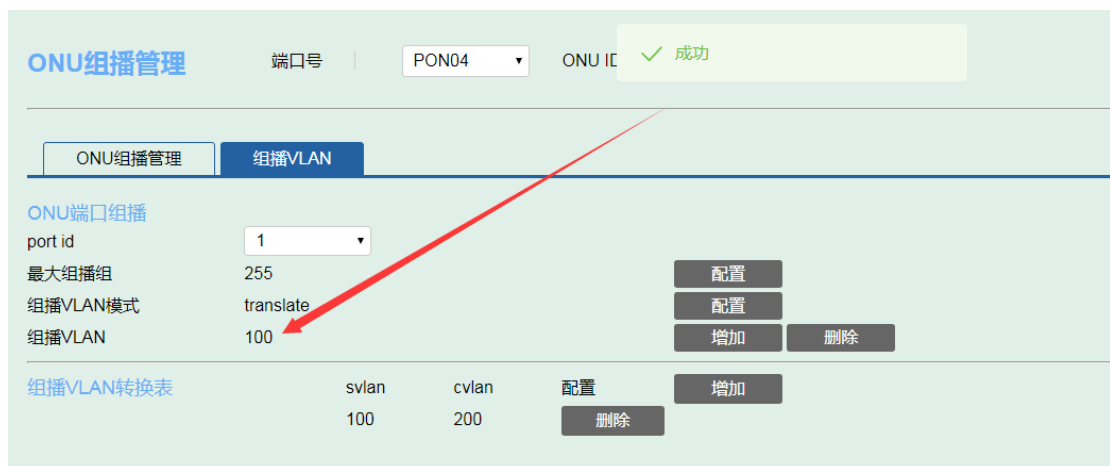
配置 ONU 组播 VLAN 为切换模式，最多支持 8 组 VLAN 转换（CTC 标准定义最大值，具体得看 ONU 支持）







5. 配置 ONU 组播 VLAN。仅在 ONU 组播模式为 igmp-snooping 可配置，当 ONU 组播模式从 igmp-snooping 切换为其他模式时，组播 VLAN 将会清零。每个端口最多可以配 8 个组播 VLAN（CTC 标准定义最大值，具体得看 ONU 支持）。



## 5.4.4 ONU 统计信息

**ONU统计信息** 端口号: PON01 ONU ID: ONU1/6

ONU端口号: PON 刷新 清除统计信息 查看历史统计信息

ONU端口统计状态: 未使能 ONU端口统计周期: 900 配置

下行丢弃事件数	0	上行丢弃事件数	0
下行字节数	1017601	上行字节数	668380
下行报文数	15379	上行报文数	10051
下行广播报文数	179	上行广播报文数	0
下行组播报文数	15199	上行组播报文数	10051
下行CRC错误报文数	0	上行CRC错误报文数	0
下行超短报文数	0	上行超短报文数	0
下行超长报文数	0	上行超长报文数	0
下行Fragment数	0	上行Fragment数	0
下行Jabber数	0	上行Jabber数	0
下行长度为64字节报文数	14876	下行长度为65-127字节的报文数	333
下行长度为128-255字节的报文数	168	下行长度为256-511字节的报文数	2
下行长度为512-1023字节的报文数	0	下行长度为1024-1518字节的报文数	0
上行长度为64字节报文数	9928	上行长度为65-127字节的报文数	25
上行长度为128-255字节的报文数	15	上行长度为256-511字节的报文数	83
上行长度为512-1023字节的报文数	0	上行长度为1024-1518字节的报文数	0
上行丢弃报文数	0	上行丢弃报文数	0
下行错误报文数	0	上行错误报文数	0
端口状态变化次数	0		

语言: 简体中文 English | 固件版本号: Neutral-E04\_L\_V3.0.0\_Rel | MAC地址: 38 3a 21 01 01 64

### 设置 PON 和 LAN 口的统计状态

**ONU统计信息** 端口号: PON01 ONU ID: ONU1/1

ONU端口号: PON 刷新 清除统计信息 查看当前统计信息

ONU端口统计状态: 使能 ONU端口统计周期: 300 配置

**配置ONU端口统计状态**

ONU端口号: PON

ONU端口统计状态: 使能

ONU端口统计周期:  s

确认 取消

下行丢弃事件数	0	上行丢弃事件数	0
下行字节数	19520	上行字节数	22988
下行报文数	305	上行报文数	310
下行广播报文数	0	上行广播报文数	0
下行组播报文数	305	上行组播报文数	0
下行CRC错误报文数	0	上行CRC错误报文数	0
下行超短报文数	0	上行超短报文数	0
下行超长报文数	0	上行超长报文数	0
下行Fragment数	0	上行Fragment数	0
下行Jabber数	0	上行Jabber数	0
下行长度为64字节报文数	305	下行长度为65-127字节的报文数	0
下行长度为128-255字节的报文数	0	下行长度为256-511字节的报文数	0
下行长度为512-1023字节的报文数	0	下行长度为1024-1518字节的报文数	0
上行长度为64字节报文数	0	上行长度为65-127字节的报文数	303
上行长度为128-255字节的报文数	0	上行长度为256-511字节的报文数	7

### 查看当前端口历史统计状态

ONU统计信息 端口号 PON01 ONU ID ONU16

ONU端口号 PON 刷新 清除统计信息 查看当前统计信息

ONU端口统计状态: 未使能 ONU端口统计周期: 900 配置

下行丢弃事件数	0	上行丢弃事件数	0
下行字节数	1032651	上行字节数	670498
下行报文数	15608	上行报文数	10203
下行广播报文数	181	上行广播报文数	0
下行组播报文数	15426	上行组播报文数	10203
下行CRC错误报文数	0	上行CRC错误报文数	0
下行超短报文数	0	上行超短报文数	0
下行超长报文数	0	上行超长报文数	0
下行Fragment数	0	上行Fragment数	0
下行Jabber数	0	上行Jabber数	0
下行长度为64字节报文数	15099	下行长度为65~127字节的报文数	337
下行长度为128~255字节的报文数	170	下行长度为256~511字节的报文数	2
下行长度为512~1023字节的报文数	0	下行长度为1024~1518字节的报文数	0
上行长度为64字节报文数	10075	上行长度为65~127字节的报文数	25
上行长度为128~255字节的报文数	15	上行长度为256~511字节的报文数	88
上行长度为512~1023字节的报文数	0	上行长度为1024~1518字节的报文数	0
下行丢弃报文数	0	上行丢弃报文数	0
下行错误报文数	0	上行错误报文数	0
端口状态变化次数	0		

## 5.5 端口管理

### 5.5.1 端口信息

NEUTRAL 状态 TOPO图 ONU列表 VLAN管理 高级设置 快速访问 root

运行状态

系统管理

PON管理

ONU管理

端口管理

端口信息

统计信息

端口配置

端口VLAN

环路检测

端口隔离

MAC地址管理

协议管理

ACL/CoS

路由

链路聚合

#### 端口信息

端口号	管理状态	链路状态	自协商	速率	双工	流控	最大传输单元	端口媒介	缺省VLAN	配置
PON01	Enable	连接	Enable	1000M	full	Disable	1518	Fiber	1	配置
PON02	Enable	未连接	Enable	1000M	full	Disable	1518	Fiber	1	配置
PON03	Enable	未连接	Enable	1000M	full	Disable	1518	Fiber	1	配置
PON04	Enable	未连接	Enable	1000M	full	Disable	1518	Fiber	1	配置
GE01	Enable	连接	Enable	100M	full	Disable	1518	Copper	1	配置
GE02	Enable	未连接	Enable	auto	half	Enable	1518	Copper	1	配置
GE03	Enable	未连接	Enable	auto	half	Enable	1518	Copper	1	配置
GE04	Enable	未连接	Enable	auto	half	Enable	1518	Copper	1	配置
GE05	Enable	未连接	Disable	1000M	full	Enable	1518	Fiber	1	配置
GE06	Enable	未连接	Disable	1000M	full	Enable	1518	Fiber	1	配置
GE07	Enable	未连接	Disable	1000M	full	Enable	1518	Fiber	1	配置
GE08	Enable	未连接	Disable	1000M	full	Enable	1518	Fiber	1	配置

语言: 简体中文 English | 固件版本号: Neutral-ED4\_U\_V3.0.0\_Rel | MAC地址: 38-3a-21-01-01-64

### 5.5.2 端口统计信息

NEUTRAL 状态 TOPO图 ONU列表 VLAN管理 高级设置 快速访问 root

运行状态

系统管理

PON管理

ONU管理

端口管理

端口信息

统计信息

端口配置

端口VLAN

环路检测

端口隔离

MAC地址管理

协议管理

ACL/QoS

路由

链路聚合

### 统计信息

端口号	接收字节数	接收帧数	接收丢弃帧	接收错误帧	发送字节数	发送帧数	发送丢弃帧	发送错误帧	配置
PON01	1093031	8852	6170	0	3681567	48350	0	0	详情 清除
PON02	314	3	1	0	3489668	47412	0	0	详情 清除
PON03	1408	20	2	0	3489668	47412	0	0	详情 清除
PON04	3358	34	0	0	3400434	47415	0	0	详情 清除
GE01	3754474	47120	427	0	6574123	86588	0	0	详情 清除
GE02	373140	2398	54	0	368557	1305	0	0	详情 清除
GE03	0	0	0	0	0	0	0	0	详情 清除
GE04	143027	1197	433	0	341425	796	0	0	详情 清除
GE05	0	0	0	0	0	0	0	0	详情 清除
GE06	0	0	0	0	0	0	0	0	详情 清除
GE07	0	0	0	0	0	0	0	0	详情 清除
GE08	0	0	0	0	0	0	0	0	详情 清除

语言: 简体中文 English | 固件版本号: Neutral-ED4\_V3.0.0\_Rel | MAC地址: 38 3a 21 f0 01 64

### 5.5.3 端口配置

NEUTRAL 状态 TOPO图 ONU列表 VLAN管理 高级设置 快速访问 root

运行状态

系统管理

PON管理

ONU管理

端口管理

端口信息

统计信息

端口配置

端口VLAN

环路检测

端口隔离

MAC地址管理

协议管理

ACL/QoS

路由

链路聚合

### 端口配置

刷新

端口号: PON01 链路状态: 连接 管理状态: 使能

#### 交换端口基本配置

管理状态: 使能

链路状态: 连接

自适应: 使能

速率: 1000M

双工: 全双工

流控: 未使能

最大传输单元: 1518

端口媒介: Fiber

缺省VLAN: 1

确认

#### 风暴抑制

广播: 512 pps

组播: 0 pps

单播: 0 pps

确认

#### 端口镜像

目的端口: 请选择

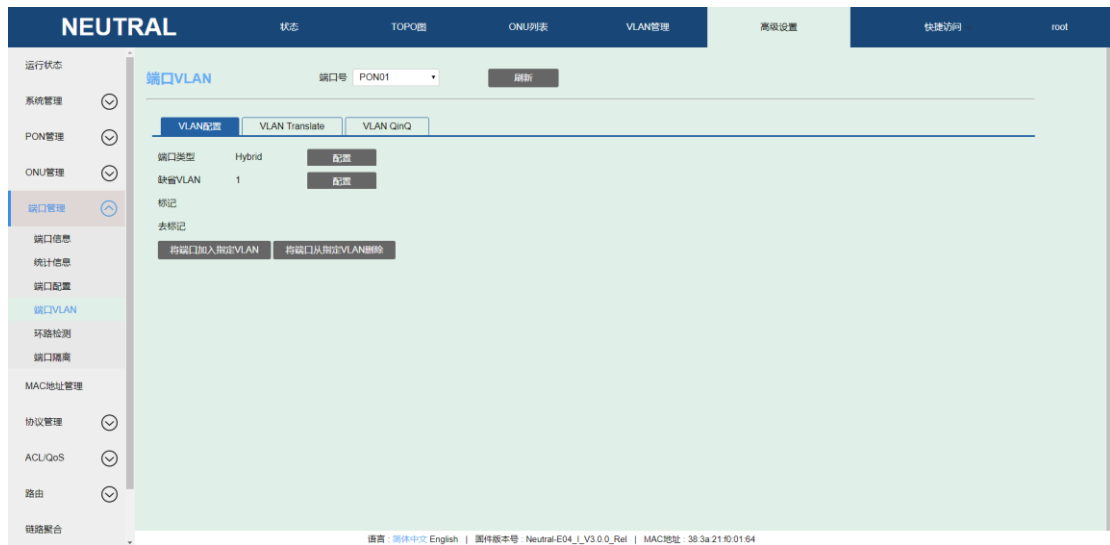
类型: 请选择

清除 确认

语言: 简体中文 English | 固件版本号: Neutral-ED4\_V3.0.0\_Rel | MAC地址: 38 3a 21 f0 01 64

- 1.可以切换端口号获取不同端口信息
- 2.配置端口基本信息，例如：配置 MTU 或者缺省
- 3.配置风暴抑制，以 PPS 为单位，可以配置广播、组播和单播风暴抑制，0 表示关闭风暴抑制功能
- 4.端口镜像功能

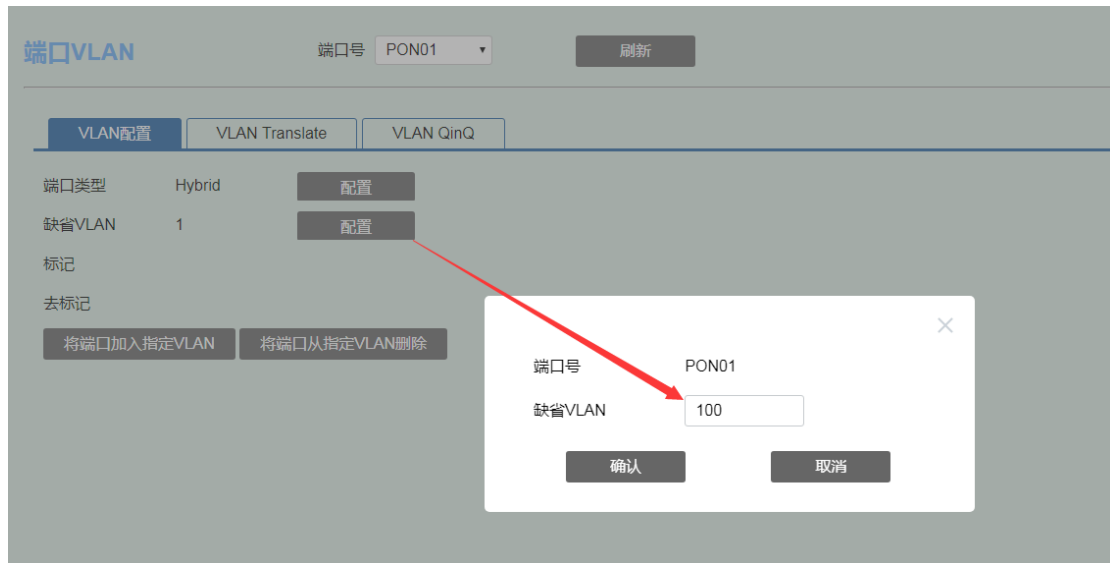
### 5.5.4 端口 VLAN



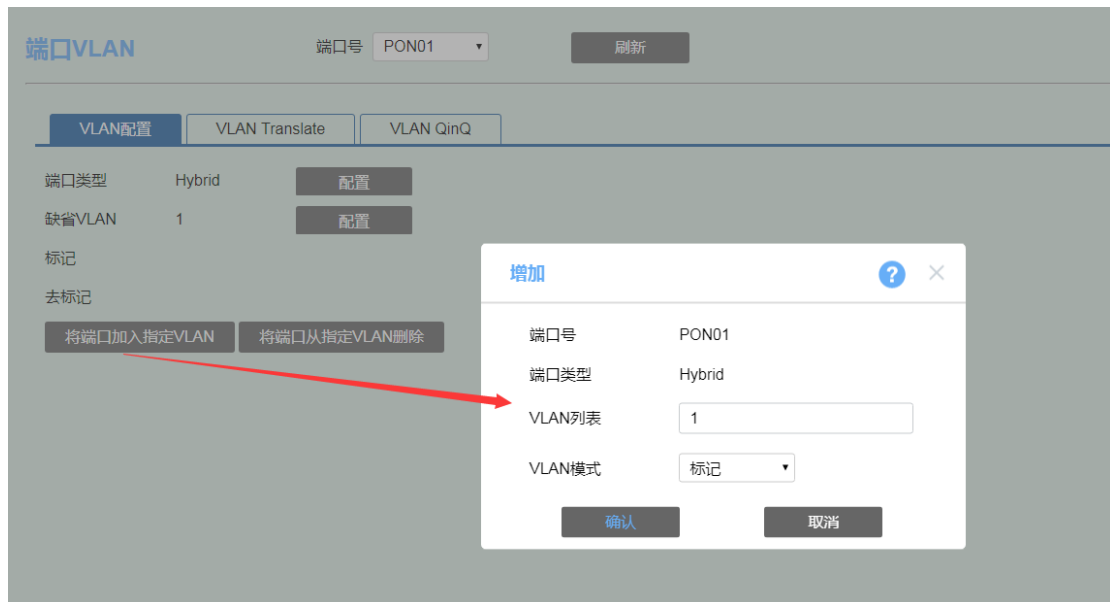
## 1. 设置端口 VLAN 类型



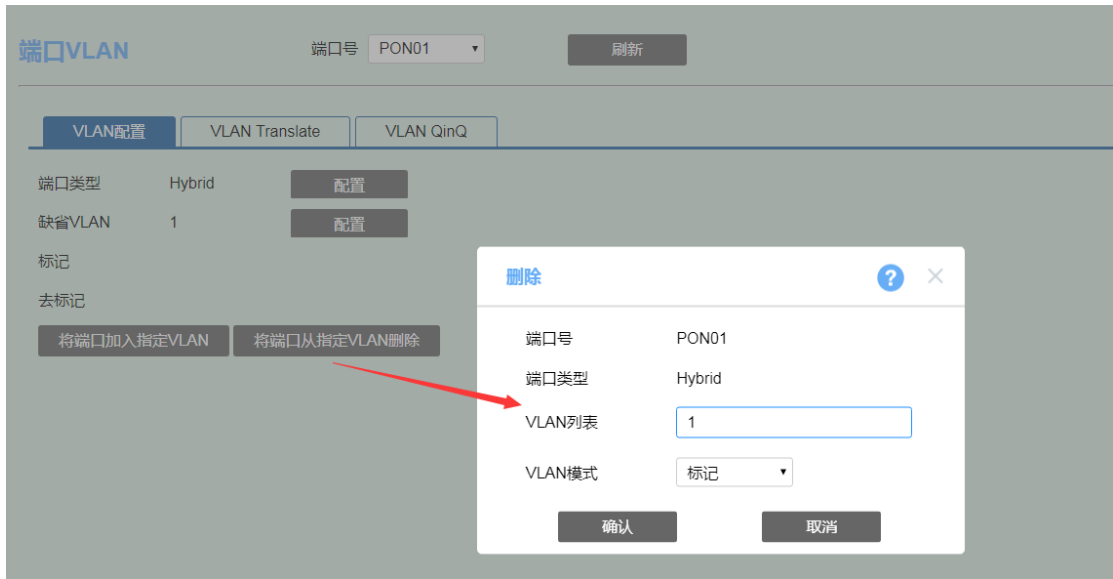
在这里可以配置端口 VLAN 为 hybrid、access 和 trunk 模式，接下来还可以配置端口缺省 VLAN



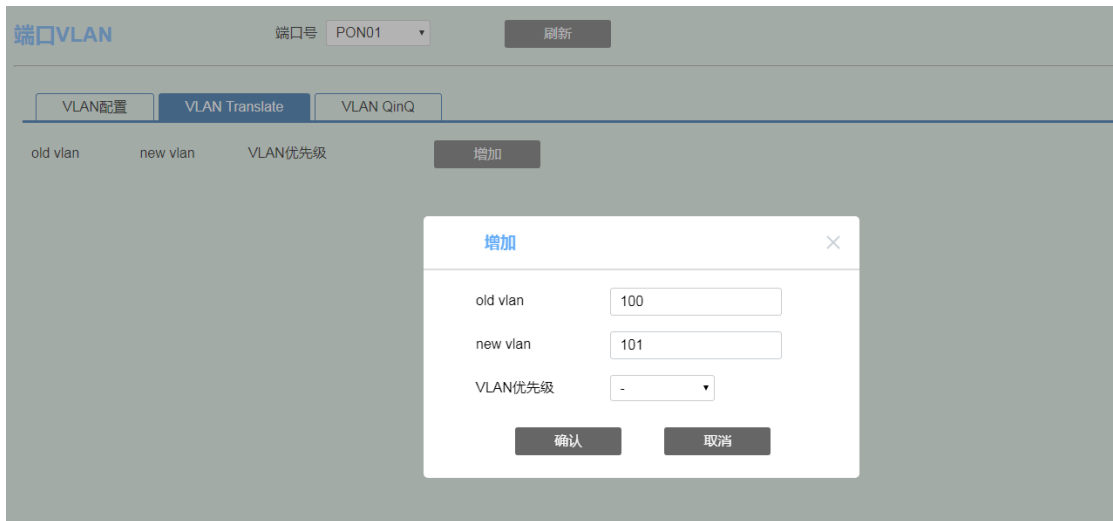
2. 可以在这个端口增加 VLAN 和选择 vlan 的标记或者去标志模式。



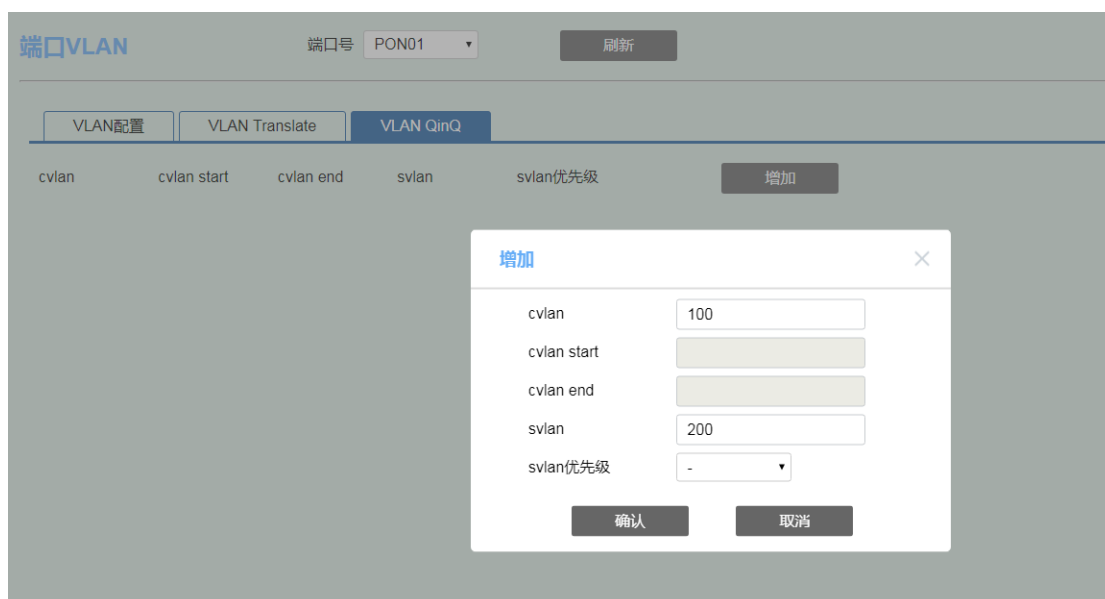
当然，也可以删除端口 VLAN



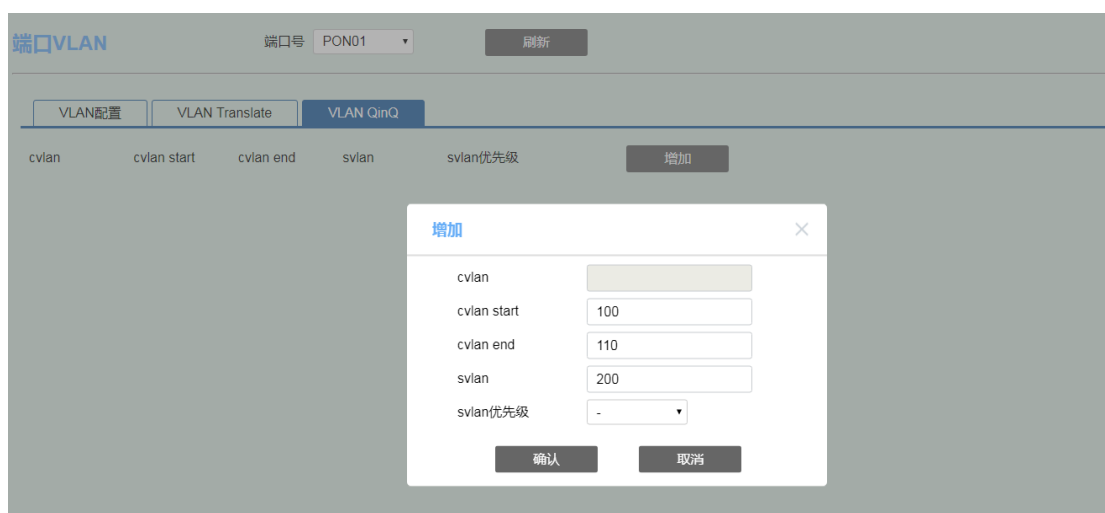
### 3. 增加端口 VLAN 转换



### 4. 增加端口 QinQ



也支持配置 CVLAN 范围:



### 5.5.5 环路检测

此功能为了对组网中出现的环路进行处理，以防止环路对业务造成影响，需要对用户侧环路进行检测。打开用户侧环路检测功能后，系统对用户侧环路进行自动检测，当检测到环路会制止环路的发生以及发出告警。

#### 5.5.5.1 PON 环路检测

##### 1. PON 环路检测功能介绍:

PON 环路检测功能默认打开，环路检测处理条件有以下三种情况:

(1)当同一个 ONU 端口或下联设备发生环路，因 ONU 端口环路检测功能默认是打开的，不触发 PON 环路检测。



(2)同一个 PON 口下不同 ONU 之间发生环路,当 P2P 功能关闭时(缺省情况下关闭),只发出环路告警,不把 ONU 加入黑名单;当 P2P 功能打开时,发出环路告警同时将发生环路的一个 ONU 加入黑名单。

(3)不同 PON 口下的 ONU 发生环路,当 PON 端口隔离功能打开时(缺省情况下打),只发出环路告警,不把 ONU 加入黑名单;当 PON 端口隔离功能关闭且发生环路的两个 PON 口的缺省 VLAN 相同时,发出环路告警同时将发生环路的一个 ONU 加入黑名单。

**注意:**

1->PON 环路检测加入黑名单的 ONU,在没有自动移除黑名单或手动恢复模式下进行配置保存,重启设备后该 ONU 会永久在黑名单,需要手动移除黑名单。

2->手动认证模式下环路检测加入黑名单后需要手动认证才能重新上线。

## 2. PON 环路检测参数配置

环路检测		
PON环路检测		
环路检测状态	使能	修改
环路检测间隔	5 s	修改
环路检测恢复模式	Auto	修改
自动恢复时间	30 s	修改

(1)环路检测状态: 缺省是未使能状态,可选配置使能,配置后 PON 环路检测功能生效;

(2)环路检测间隔: 该参数是配置 PON 环路检测报文发出间隔,缺省情况下 5 秒发一个环路检测报文;

(3)环路检测恢复模式: 该参数是配置当环路发生 ONU 被加入黑名单后是否自动恢复移除黑名单,缺省是自动恢复模式,可选手动恢复模式;

(4)自动恢复时间: 该参数仅在环路检测恢复模式为 Auto 时生效,默认 30 秒自动恢复;

(5)手动恢复：该配置仅在环路检测恢复模式为 Manual 时可配，配置后 ONU 会从黑名单移除。

### 环路检测

PON环路检测
上联口环路检测

环路检测状态	使能	修改
环路检测间隔	5 s	修改
环路检测恢复模式	Manual	修改
手动恢复		确认
自动恢复时间	30 s	修改

### 3.PON 环路检测信息查看

环路检测信息 刷新

PON ID / ONU ID	状态	ONU状态	回环 PON ID / ONU ID
1/ 1	Loop-Detect	-	4/1
4/ 1	Loop-Detect	Add Black List	1/1

#### 5.5.5.2 上联口环路检测

##### 1.上联口环路检测功能介绍：

上联口环路检测功能默认打开，环路检测处理条件有以下三种情况：

(1)当使能生成树协议，上联口环路检测不生效，只有在生成树协议关闭的情况下上联口环路检测才会生效；

(2)同一个上联口发生环路，直接 Link Down 该上联端口；

(3)不同上联口发生环路，当 PVID 不同时，发生环路告警，不 Link Down 端口；当 PVID 相同时，发生环路告警同时 Link Down 其中一个端口。

##### 2.上联口环路检测参数配置

## 环路检测

PON环路检测

上联口环路检测

环路检测状态	使能	修改
环路检测间隔	5 s	修改
环路检测恢复模式	Auto	修改
自动恢复时间	30 s	修改

(1)环路检测状态：缺省是使能状态，可选配置未使能，配置后上联口环路检测功能不生效；

(2)环路检测间隔：该参数是配置上联口环路检测报文发出间隔，缺省情况下 5 秒发一个环路检测报文；

(3)环路检测恢复模式：该参数是配置当环路发生端口被 Link Down 后是否自动恢复 Link Up，缺省是自动恢复模式，可选手动恢复模式；

(4)自动恢复时间：该参数仅在环路检测恢复模式为 Auto 时生效，默认 30 秒自动恢复；

(5)手动恢复：该配置仅在环路检测恢复模式为 Manual 时可配，配置后 Link Down 端口会 Link Up。

## 环路检测

PON环路检测

上联口环路检测

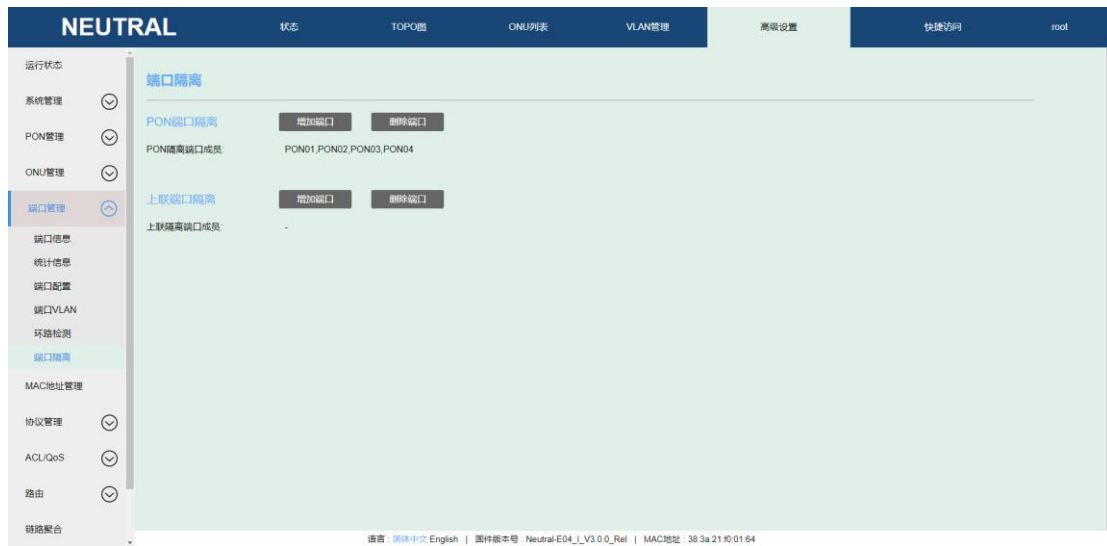
环路检测状态	使能	修改
环路检测间隔	5 s	修改
环路检测恢复模式	Manual	修改
手动恢复		确认
自动恢复时间	30 s	修改

### 3.上联口环路检测信息查看

端口号	状态	端口状态	回环端口
GE03	Loop-Detect	-	GE04
GE04	Loop-Detect	Blocked	GE03

## 5.5.6 端口隔离

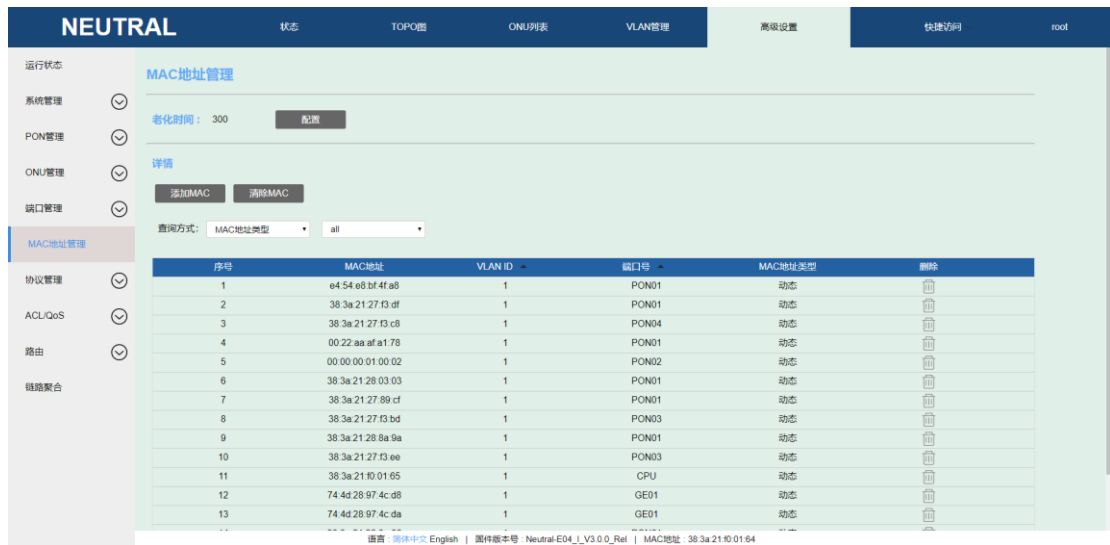
缺省情况下 PON 端口隔离打开，上联端口端口隔离关闭



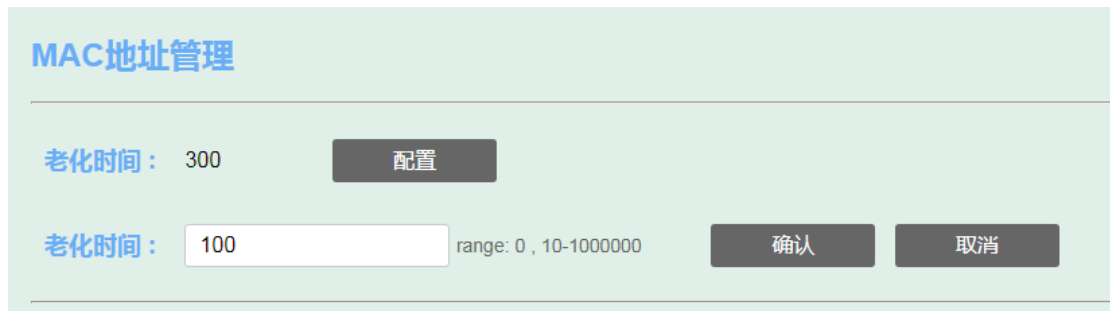
可以增加或删除相互通信的端口 ID



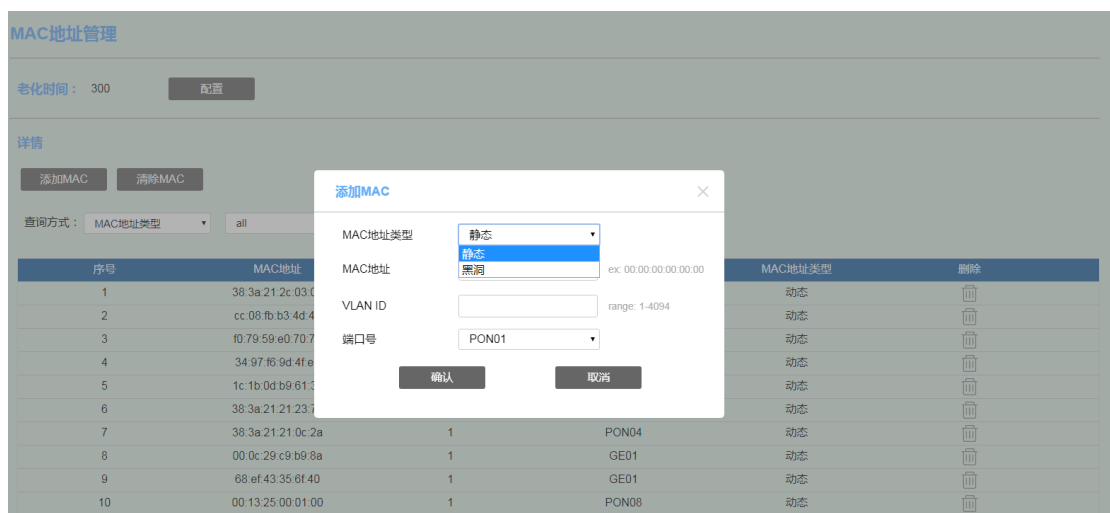
## 5.6 MAC 地址管理



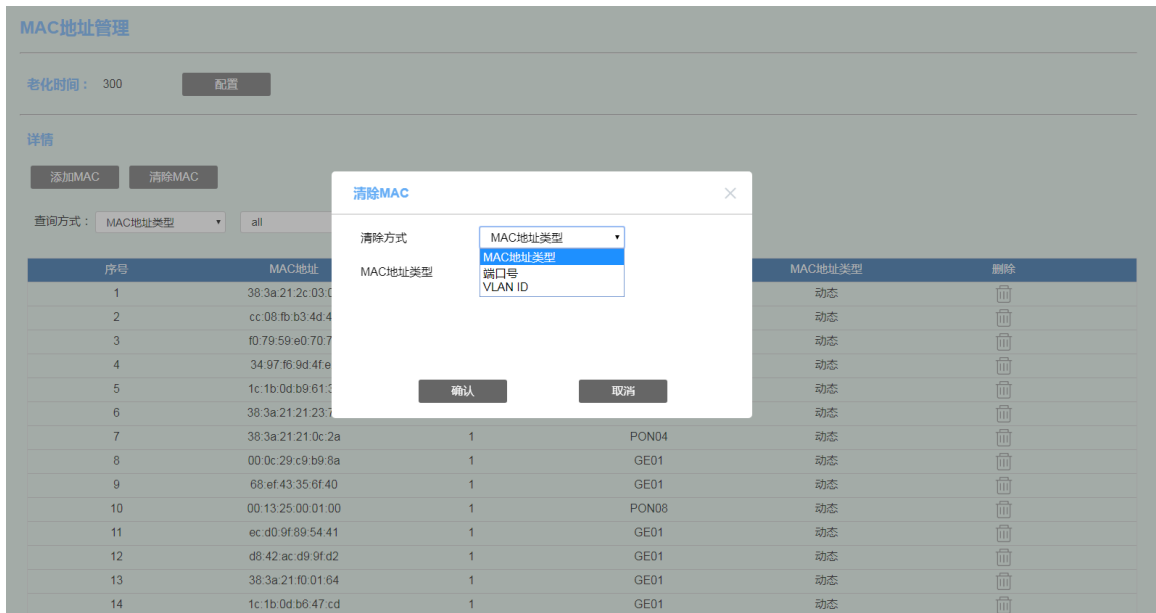
### 1. 配置 MAC 地址老化时间



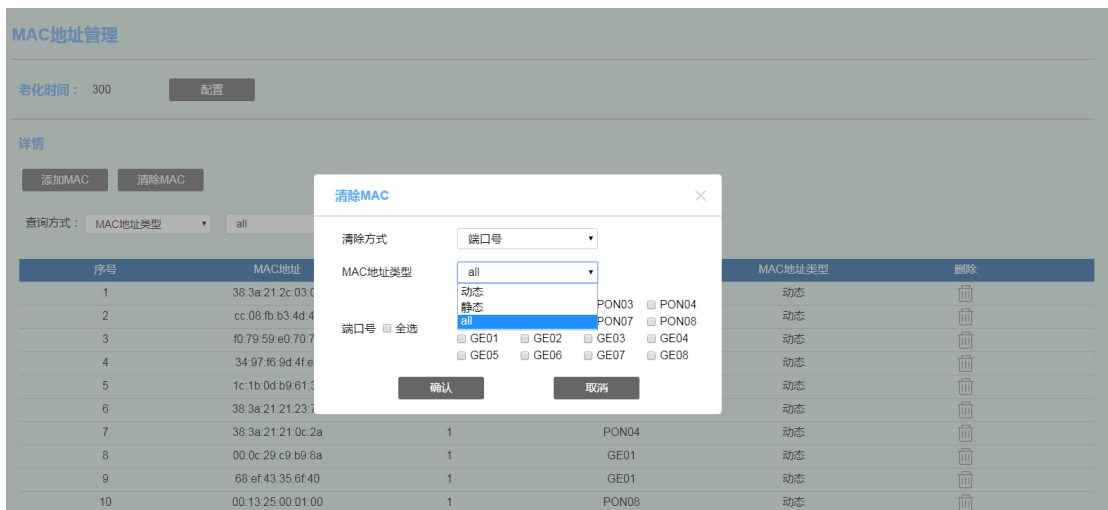
### 2. 增加 MAC 地址（可以选择增加静态或者黑洞 MAC 地址）



### 3. 清除 MAC 地址



可以选择根据端口号删除:



也可以根据 VLAN ID 清除



## 4. MAC 地址查询

可以根据 MAC 地址类型、端口号、VLAN ID、MAC 地址查询：

The screenshot shows the 'MAC地址管理' (MAC Address Management) interface. At the top, there is a '老化时间' (Aging Time) set to 300 and a '配置' (Configure) button. Below this, there are '添加MAC' (Add MAC) and '清除MAC' (Clear MAC) buttons. A search section includes '查询方式' (Search Method) with a dropdown menu currently showing 'MAC地址类型' (MAC Address Type) selected, and another dropdown set to 'all'. Below the search is a table with columns: 'VLAN ID', 'MAC地址', 'VLAN ID', '端口号' (Port Number), 'MAC地址类型', and '删除' (Delete). The table contains 8 rows of data.

VLAN ID	MAC地址	VLAN ID	端口号	MAC地址类型	删除
	e4 54 e8 bf 4f a8	1	PON01	动态	
2	38 3a 21 27 f3 df	1	PON01	动态	
3	38 3a 21 27 f3 c8	1	PON04	动态	
4	00 22 aa af a1 78	1	PON01	动态	
5	00 00 00 01 00 02	1	PON02	动态	
6	38 3a 21 28 03 03	1	PON01	动态	
7	38 3a 21 27 89 cf	1	PON01	动态	
8	38 3a 21 27 f3 bd	1	PON03	动态	

## 5.7 协议管理

### 5.7.1 RSTP

The screenshot shows the 'RSTP' configuration page in the NEUTRAL system. The top navigation bar includes 'NEUTRAL', '状态' (Status), 'TOPO图' (Topology), 'ONU列表' (ONU List), 'VLAN管理' (VLAN Management), '高级设置' (Advanced Settings), '快速访问' (Quick Access), and 'root'. The left sidebar shows a navigation menu with '协议管理' (Protocol Management) selected, and sub-items for 'RSTP', 'IGMP', 'DHCP', and 'MSTP'. The main content area is titled 'RSTP' and has a '配置' (Configure) button. It is divided into two sections: 'rstp桥信息' (RSTP Bridge Information) and 'rstp端口信息' (RSTP Port Information). The bridge information table shows parameters like '状态' (Status: 未使能), '模式' (Mode: rstp), '根桥优先级' (Root Bridge Priority: 32768), '根桥地址' (Root Bridge Address: 38 3a 21 f0 01 65), '指定桥优先级' (Designated Bridge Priority: 32768), '指定桥地址' (Designated Bridge Address: 38 3a 21 f0 01 65), 'BPDU最大生存期' (Max BPDU Age: 20), 'BPDU发送周期' (BPDU Tx Interval: 2), '端口状态延时' (Port State Delay: 15), 'BPDU限制速率' (BPDU Rate Limit: 3), and '总根端口开销' (Total Root Port Cost: 0). The port information table has columns for '端口号' (Port Number), '端口优先级' (Port Priority), '路径开销' (Path Cost), '边缘端口' (Edge Port), '链路管理状态' (Link Management State), '链路运行状态' (Link Operational State), '角色' (Role), and '状态' (Status). The table lists ports GE01 through GE07.

端口号	端口优先级	路径开销	边缘端口	链路管理状态	链路运行状态	角色	状态
GE01	0	0	NEdge	P2P	Shared	None	Down
GE02	0	0	NEdge	P2P	Shared	None	Down
GE03	0	0	NEdge	P2P	Shared	None	Down
GE04	0	0	NEdge	P2P	Shared	None	Down
GE05	0	0	NEdge	P2P	Shared	None	Down
GE06	0	0	NEdge	P2P	Shared	None	Down
GE07	0	0	NEdge	P2P	Shared	None	Down

设置 RSTP 桥信息：

RSTP

rstp桥信息 配置

状态	未使能
模式	rstp
根桥优先级	
根桥地址	
指定桥优先级	
指定桥地址	
BPDU最大生存期	
BPDU发送周期	
端口状态延时	
BPDU限制速率	
根桥路径开销	

设置rstp全局信息

状态:

模式:

根桥优先级:

BPDU最大生存期:  range: 6-40

BPDU发送周期:  range: 1-10

端口状态延时:  range: 4-30

BPDU限制速率:  range: 1-255

确认 取消

rstp端口信息 设置端口优先级

端口号	优先级	链路运行状态	角色
GE01	0	NEdge	P2P
		Shared	None

设置成功后，可以看到以下配置结果：

RSTP ✓ 设置成功

rstp桥信息 配置

状态	使能
模式	rstp
根桥优先级	32768
根桥地址	38:3a:21:f0:01:65
指定桥优先级	32768
指定桥地址	38:3a:21:f0:01:65
BPDU最大生存期	20
BPDU发送周期	2
端口状态延时	15
BPDU限制速率	3
总根端口开销	0

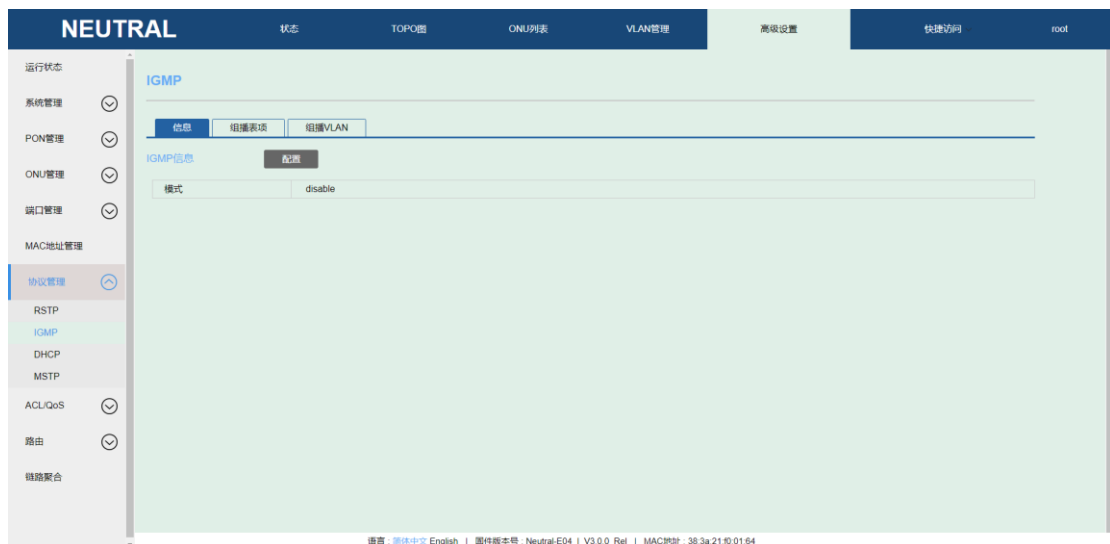
端口配置：





## 5.7.2 IGMP

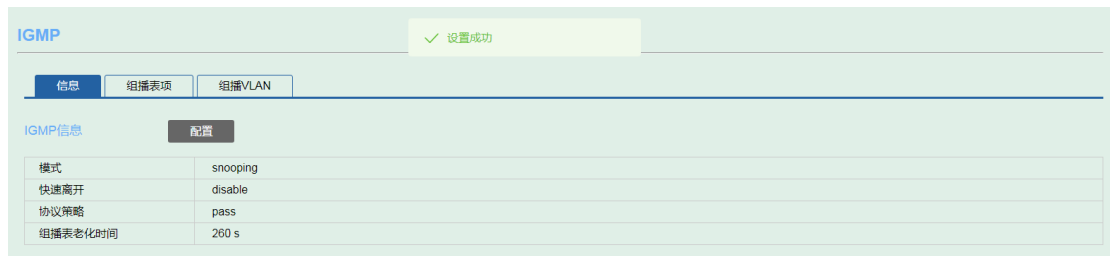
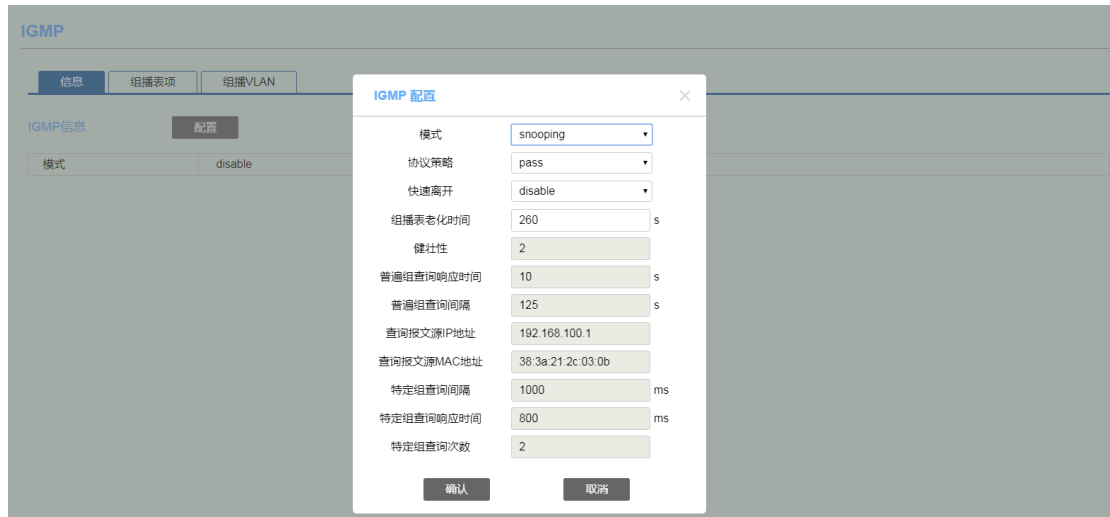
### 1. IGMP 配置，缺省为 disable 模式



### 2. 配置 IGMP snooping 参数:

snooping 模式可以配置以下参数:

- 1> 协议策略: 在组播节目库以外的组播协议报文能否通过的策略, 缺省情况下为 pass。
- 2> 快速离开: 当使能快速离开, 设备收到 igmp 离开报文会马上断开组播业务; 当未使能快速离开, 当设备在普遍组查询最大响应时间/特定组查询最大响应时间内没收到 igmp 加组报文, 才会断开组播业务流。缺省为未使能。
- 3> 组播成员老化时间: 当设备在老化时间内没有收到 igmp 加组报文, 就认为该用户已经下线, 断开该用户组播业务流。缺省为 260 秒。



### 3. 配置 IGMP proxy 参数

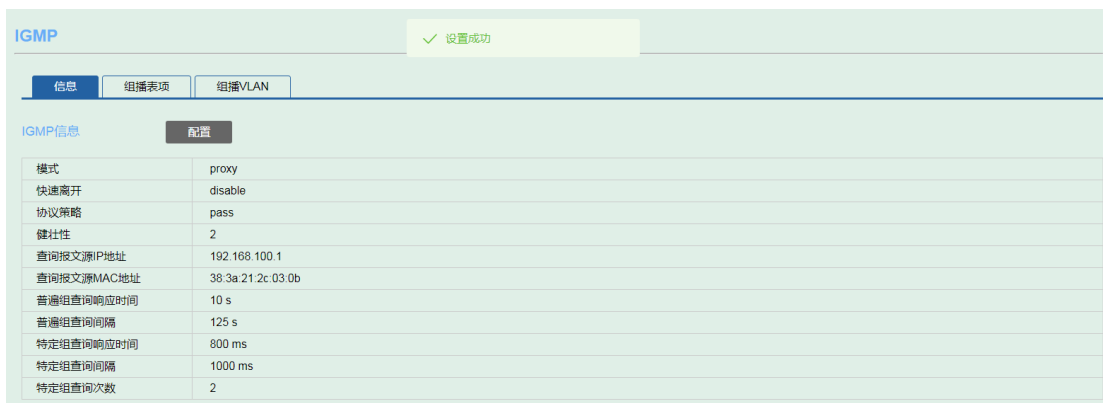
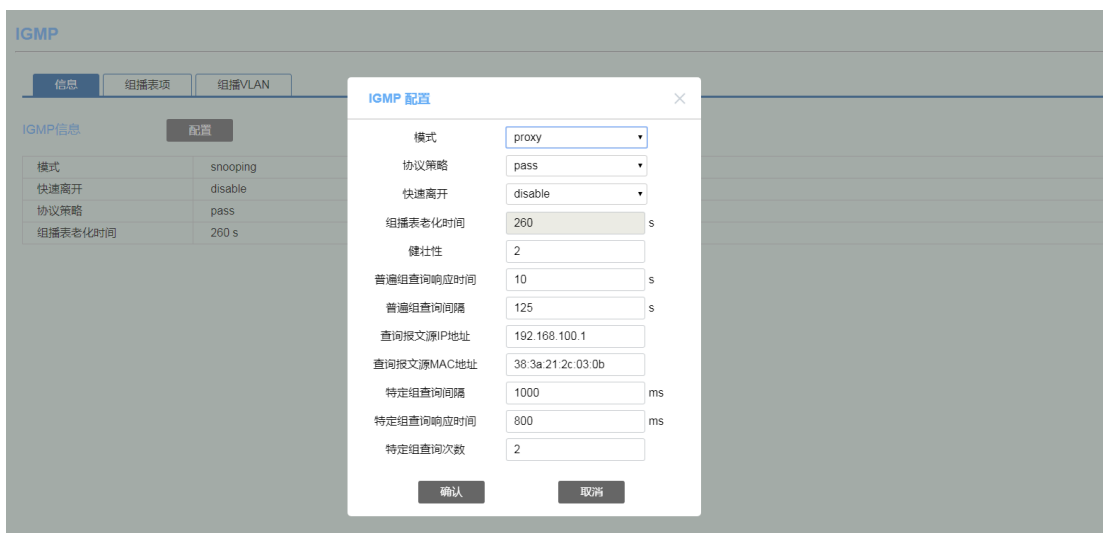
proxy 模式可以配置以下参数：

- 1> 协议策略：同上
- 2> 快速离开：同上
- 3> 健壮性系数：根据网络的稳定性情况变化，用户希望调整健壮性系数时，可使用此命令。设置后，系统使用该健壮性系数以确认组播用户的老化时间。健壮性系数为增强系统的健壮性而设置的系数，它直接影响组播用户的老化时间长短，也影响发送通用组查询报文的次数。如果一个子网可能会丢包，应该增加健壮性系数，以保证组播用户的稳定性。缺省为 2。
- 4> 普遍组查询最大响应时间：通用组查询报文发出后，在响应时间内所有在线用户都会回应 report 报文，缺省下为 10 秒。
- 5> 普遍组查询间隔：当设备处于 proxy 模式，设备会在每个通用组查询间隔时间发送一个通用组查询报文。缺省为 125 秒。
- 6> 查询报文源 IP 地址：配置组播路由器向用户侧发送的通用组查询报文或者特定组查询报文的源 IP 地址，缺省为 192.168.100.1。
- 7> 查询报文源 MAC 地址：配置组播路由器向用户侧发送的通用组查询报文或者特定组查询报文的源 MAC 地址，缺省为设备带内地址。
- 8> 特定组查询间隔：针对某一特定的节目按照此命令设置的间隔发送特定组查询来确认用户是否正在收看该节目，没有收到用户反馈的 report 报文，就认为用

户没有在收看这个节目，系统不再发送该节目流给用户，避免用户没有收看节目却仍然收到组播流而浪费了带宽。缺省为 1000 毫秒。

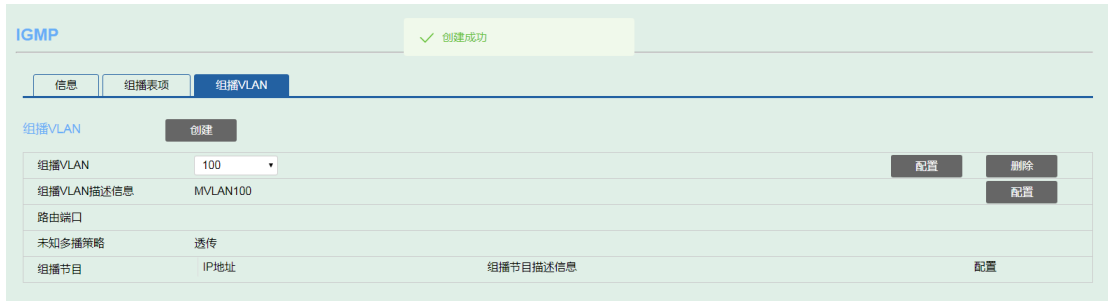
9> 特定组查询次数：针对某一特定的节目通过发送 N 次（N 通过此命令设置）特定组查询来确认用户是否正在收看该节目，缺省为 2 次。

10> 特定组查询最大响应时间：特定组查询报文发出后，在响应时间内所有在线用户都会回应 report 报文，缺省下为 800 毫秒。



#### 4. 配置组播 VLAN 100，VLAN 必须存在才能创建成功。





5. 配置组播 VLAN 100 描述信息



6. 配置组播路由端口

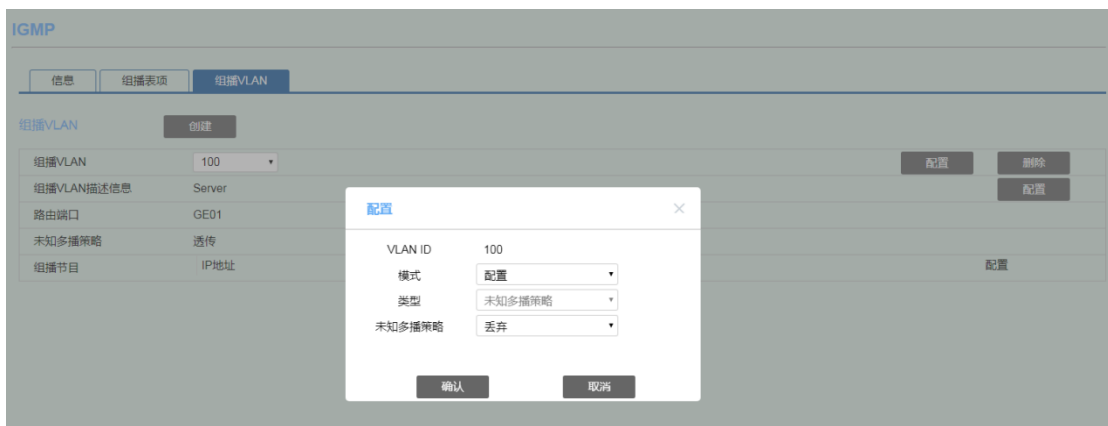
IGMP 路由端口只能是上联端口，连接组播服务器的。





## 7. 配置未知多播策略

未知多播业务流的抑制策略：如果业务流承载特定用途的未知多播，则配置为透传。没有特殊用途的未知多播会占用带宽，一般配置为丢弃，缺省为透传。



## 8. 配置组播节目库

增加组播节目库，用户可以切换到该组播 VLAN 节目频道。



## 9. 配置组播静态表项



10. 静态组播表项是不会被老化的，只能手动删除

11. 删除动态表项



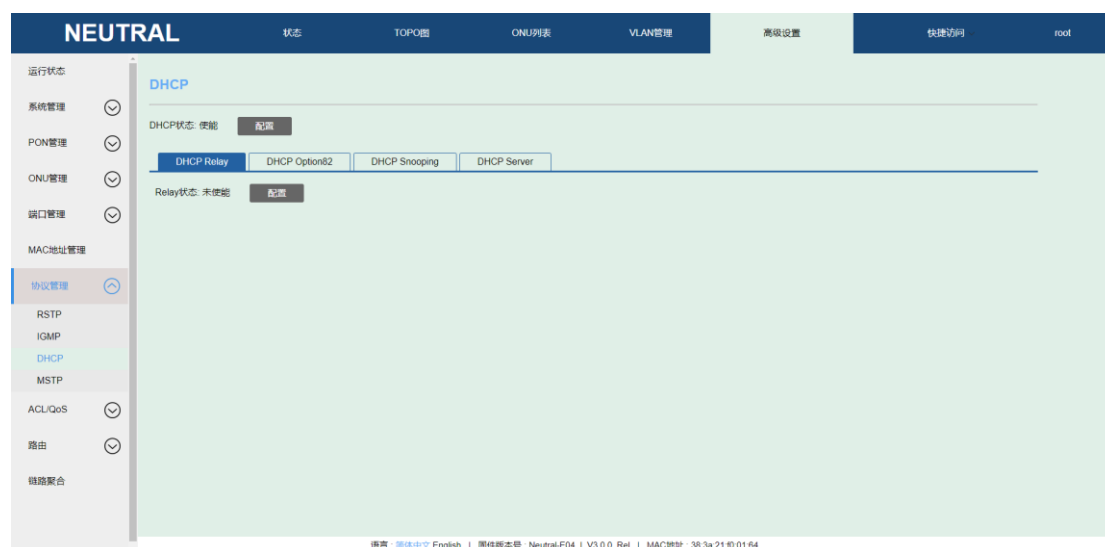
## 5.7.3DHCP

本设备支持配置 DHCP Snooping 功能、DHCP Relay 功能、DHCP Option82 功能和 DHCP Server 功能

## 1. DHCP Relay

DHCP Relay 功能是工作在三层,可以使 DHCP 客户端的请求报文发送到指定的 DHCP 服务器。缺省未使能。

**提示:** 打开 DHCP Relay 功能需要确保 DHCP 功能已经开启且路由功能(ip route enable)也是开启的; 打开 DHCP Relay 相关功能配置需要确保 DHCP Relay 功能已经开启。

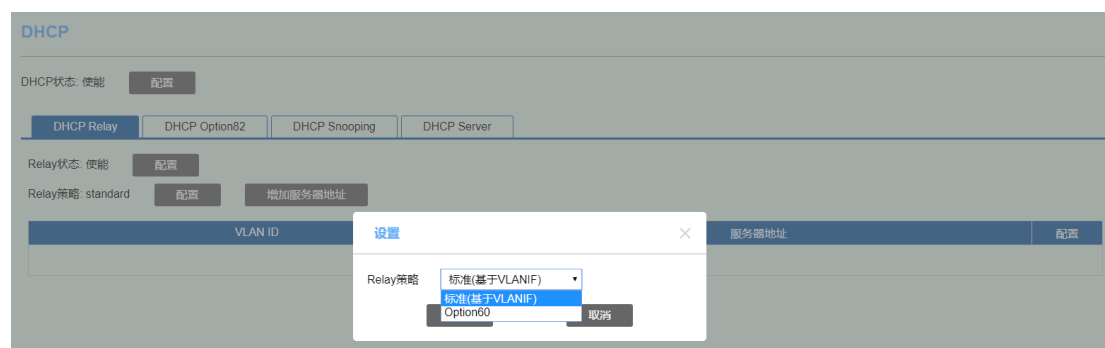


DHCP Relay 有两种策略:

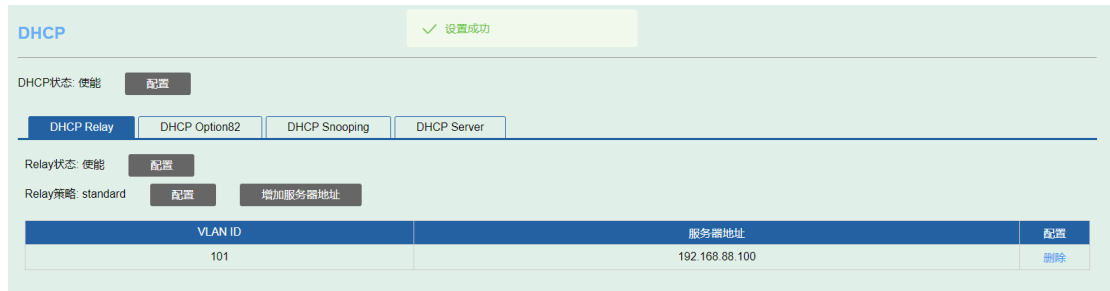
(1)Standard 策略(默认策略): 根据 VLAN 找到 DHCP 服务器地址;

(2)Option60 策略: 根据 DHCP 客户端携带的 Option60 域值找到服务器地址。

**提示:** 切换策略会把另一个策略建立的服务器表清除。



增加服务器地址 (系统最大支持配置 32 个服务器表)



## 2. DHCP Option82

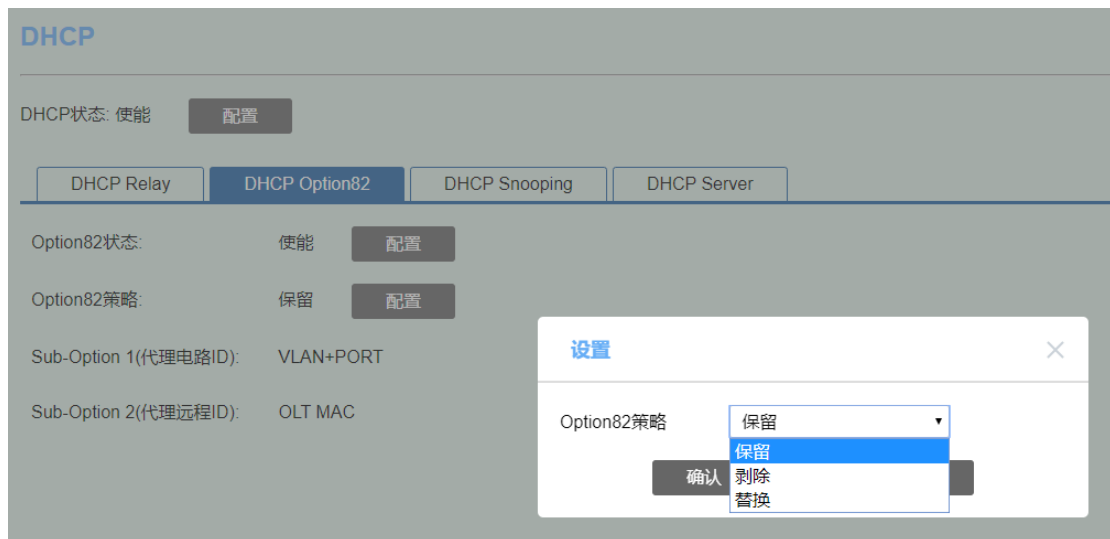
为了增强 DHCP 服务器的安全性，改善 IP 地址配置策略而提出的一种 DHCP 选项。缺省未使能。

支持三种策略：

(1)保留策略(默认策略)：客户端发上来的请求报文不带 Option82 信息 OLT 会带上 Option82 信息，客户端发上来是带 Option82 信息，则 OLT 不处理直接转发服务器。

(2)剥除策略：客户端发上来的请求报文不带 Option82 信息 OLT 不处理直接转发服务器，客户端发上来是带 Option82 信息，则 OLT 剥除 Option82 信息再转发服务器。

(3)替换策略：客户端发上来的请求报文不带 Option82 信息 OLT 不处理直接转发服务器，客户端发上来是带 Option82 信息，则 OLT 替换 Option82 信息再转发服务器。

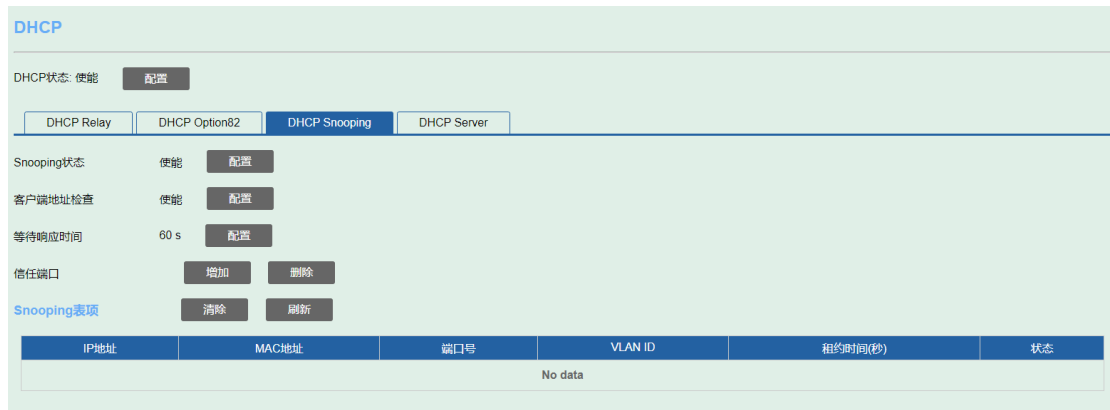


## 3. DHCP Snooping

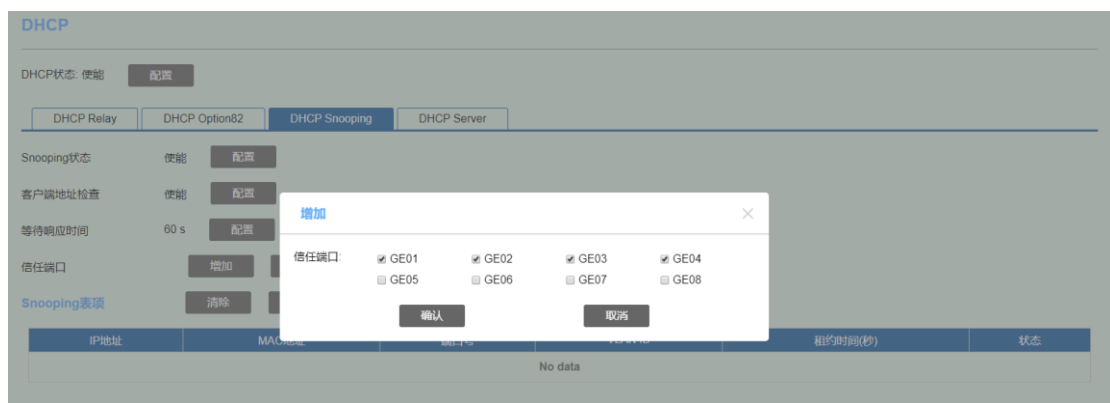
DHCP Snooping 功能通过监听 DHCP 客户端与服务器之间的报文交互，从而记录用户 IP/MAC 信息。缺省未使能。

**提示：**打开 DHCP Snooping 功能需要确保 DHCP 功能已经开启，打开 DHCP Snooping 相关功能配置需要确保 DHCP Snooping 功能已经开启。





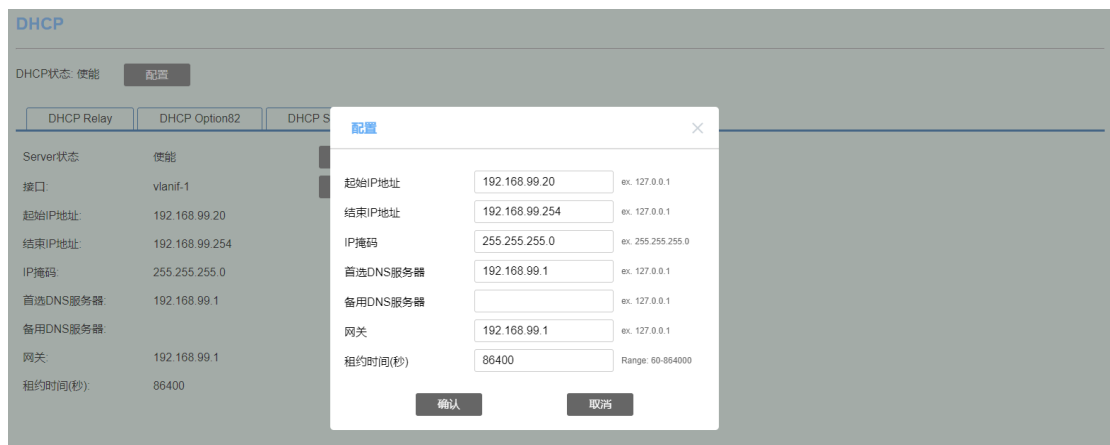
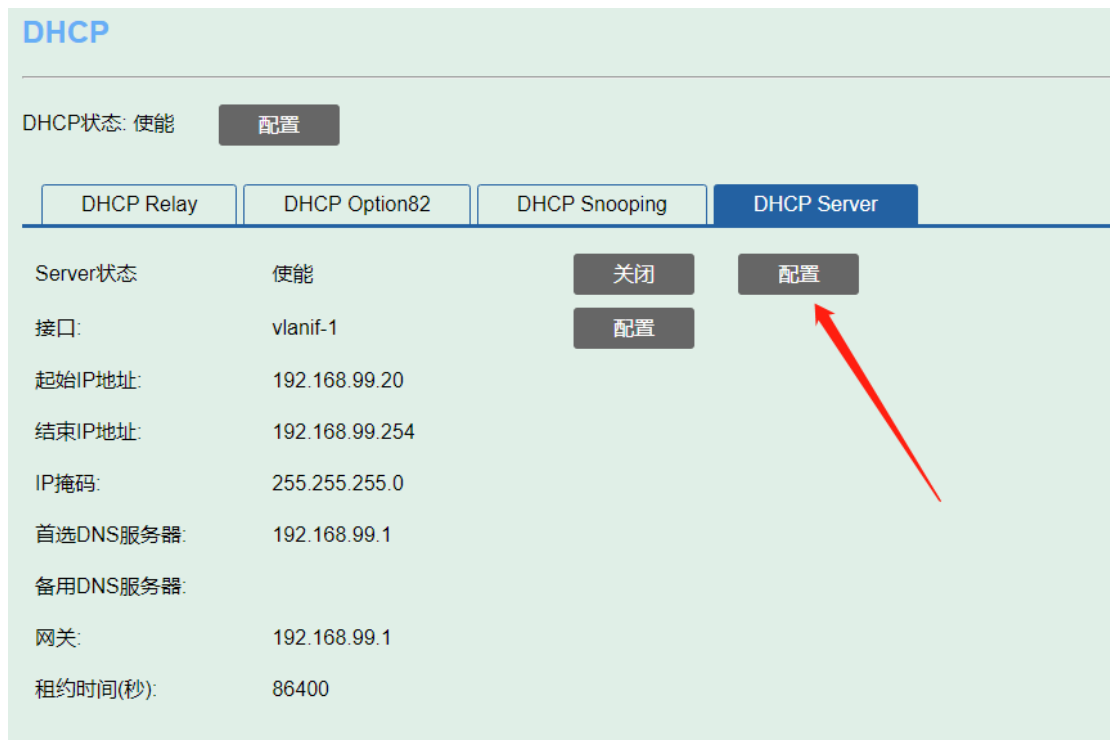
## 添加信任端口



该配置仅限上联口可配，信任端口允许接收所有的 DHCP 报文，非信任端口不允许接收 DHCP 响应报文。默认所有端口为非信任端口。

## 4. DHCP Server

缺省未使能，开启前需关闭 DHCP Relay、DHCP Option82、DHCP Snooping 功能。开启后，开始配置 DHCP 服务器，默认为带内管理网段，接口为逻辑端口 vlanif-1

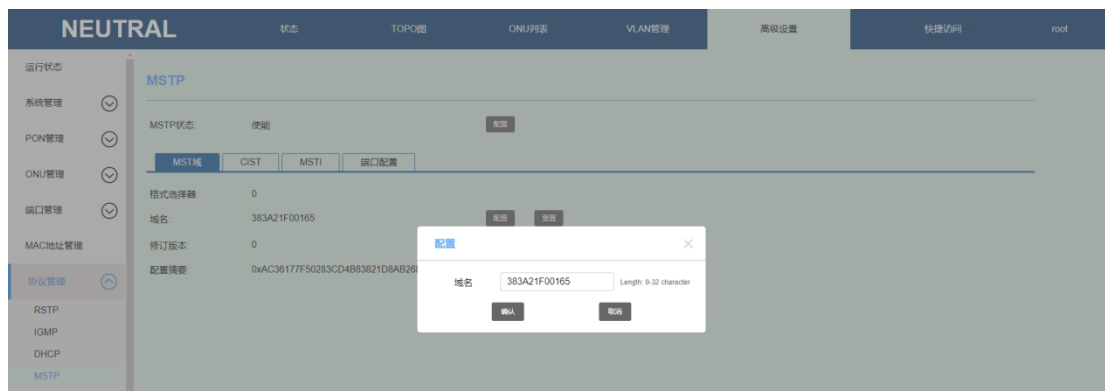


## 5.7.4 MSTP

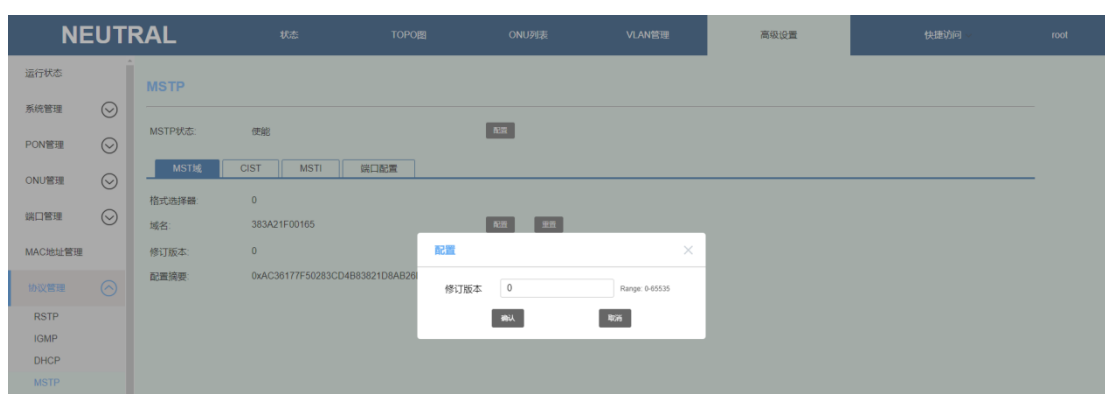
MSTP 兼容 STP 和 RSTP，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余的链路提供了更好的负载分担机制。通过 MSTP 把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。每棵生成树叫做一个多生成树实例 MSTI(Multiple Spanning Tree Instance)，每个域叫做一个 MST 域(MST Region:Multiple Spanning Tree Region)。缺省状态未使能。

### 1. MST 域

由交换网络中的多台设备以及它们之间的网段所构成，一个局域网可以存在多个 MST 域，各 MST 域之间在物理上直接或间接相连，可以通过 MSTP 配置命令把多台设备划分在同一个 MST 域内。



域名可配置长度为 0-32 位，重置后恢复为 383A21F00165。



修改版本可配置范围为 0-65535

## 2. CIST

在每个 MST 域内 MSTP 通过计算生成 IST（各 MST 域内的一棵生成树），同时 MSTP 将每个 MST 域作为单台交换设备对待，通过计算在 MST 域间生成 CST（连接交换网络内所有 MST 域的一棵生成树），CIST 是连接一个交换网络内所有设备的单生成树，由 IST 和 CST 共同构成。VLAN 映射表是 MST 域的属性，它描述了 VLAN 和 MSTI 之间的映射关系，默认为 1-4094。

**MSTP**

MSTP状态: 使能 配置

MST域 CIST MSTI 端口配置

信息 配置 配置优先级

VLAN映射表: 1-4094  
 本桥优先级: 32768 本桥MAC: 38:3A:21:F0:01:65  
 总根桥优先级: 32768 总根桥MAC: 38:3A:21:F0:01:65  
 域根桥优先级: 32768 域根桥MAC: 38:3A:21:F0:01:65  
 根端口: None  
 总根端口开销: 0  
 域根端口开销: 0

本桥时间: Hello时间: 2 转发时延: 15 最大老化时间: 20 最大跳数: 20  
 根桥时间: Hello时间: 2 转发时延: 15 最大老化时间: 20

端口列表

端口号	角色	端口优先级	状态	配置开销	运行开销	配置
GE01	Designated	128	Forwarding	Auto	200000	<a href="#">配置</a>

### 配置界面及优先级

**MSTP**

MSTP状态: 使能 配置

MST域 CIST MSTI 端口配置

信息 配置 配置优先级

VLAN映射表: 1-4094  
 本桥优先级: 32768  
 总根桥优先级: 32768  
 域根桥优先级: 32768  
 根端口: None  
 总根端口开销: 0  
 域根端口开销: 0

本桥时间: Hello时间: 2 转发时延: 15 最大老化时间: 20 最大跳数: 20  
 根桥时间: Hello时间: 2 转发时延: 15 最大老化时间: 20

**配置** ✕

最大老化时间:  Range: 6-40

Hello时间:  Range: 1-10, 20

最大跳数:  Range: 1-40

转发时延:  Range: 4-30

确认 取消



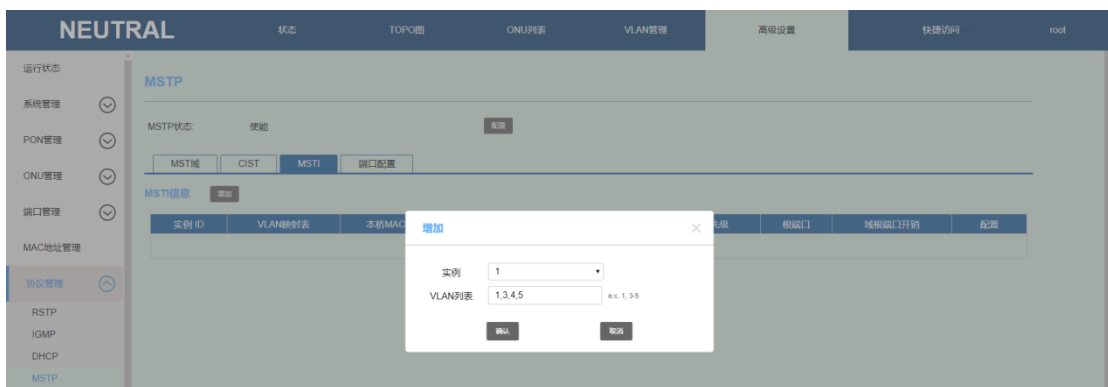
### 3. MSTI

一个 MST 域内可以通过 MSTP 生成多棵生成树，各棵生成树之间彼此独立，有以下特点：

- ①每个 MSTI 独立计算自己的生成树，互不干扰
- ②每个 MSTI 的生成树计算方法与 STP 基本相同
- ③每个 MSTI 的生成树可以有不同的根，不同的拓扑
- ④每个 MSTI 在自己的生成树内发送 BPDU
- ⑤每个 MSTI 的拓扑通过命令配置决定
- ⑥每个端口在不同 MSTI 上的生成树参数可以不同
- ⑦每个端口在不同 MSTI 上的角色、状态可以不同
- ⑧在运行 MSTP 协议的网络中，一个 VLAN 报文将沿着如下路径进行转发：

在 MST 域内，沿着其对应的 MSTI 转发。

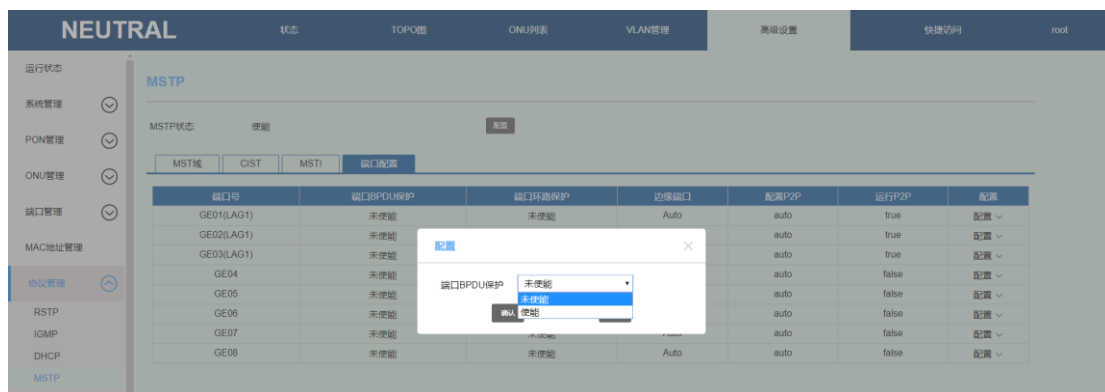
在 MST 域间，沿着 CST 转发。





#### 4. 端口配置

可快速切换每个 GE 口的 BPDU 保护、环路保护、Edge 端口、P2P 功能



## 5.8 ACL/QOS

### 5.8.1 时间范围

1. 用于指定 ACL 规则的生效时间段。配置成功后，在创建 ACL 规则时可以通过引用时间段名称来指定生效时间，ACL 规则仅在生效时间段内有效。
2. 增加 time-range
  - 1> 相对时间：周期性时间，例如，每周二 09: 00 至 23: 00。



2> 绝对时间：从具体某一点时间到另外某点时间，例如 2020 年 4 月 29 日 9: 00 至 2020 年 4 月 29 日 18: 00。



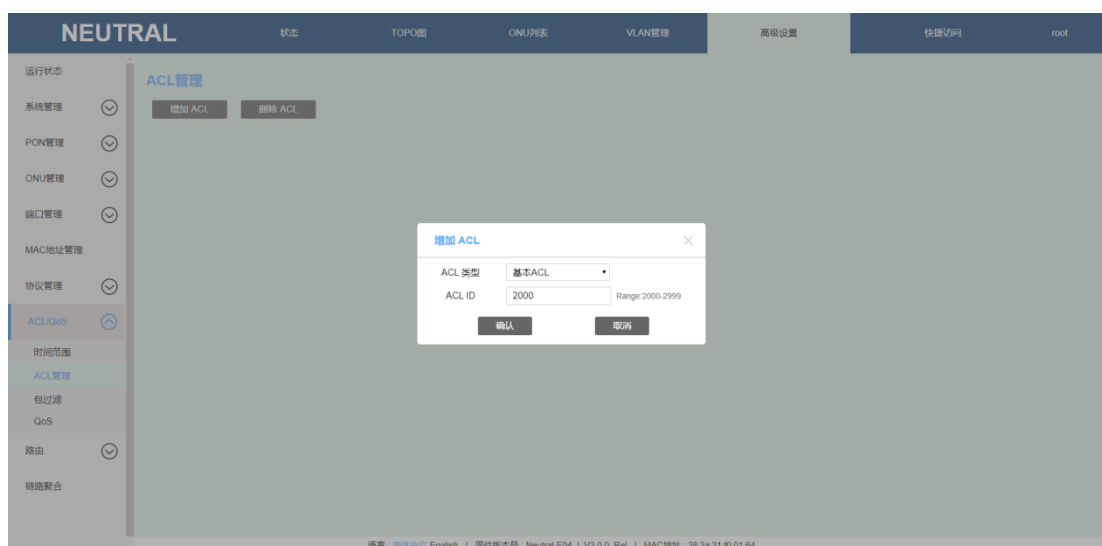
### 3. 删除 Time-range



## 5.8.2 ACL 管理

当需要通过匹配规则对特定的数据报文进行过滤时，使用此配置创建 ACL（访问控制列表）。

1. 基本 ACL(2000-2999): 当需要根据报文的源 IP 地址制定 ACL 规则时，使用此配置。成功创建规则后，可以使用 `packet-filter` 命令引用规则对报文进行过滤。

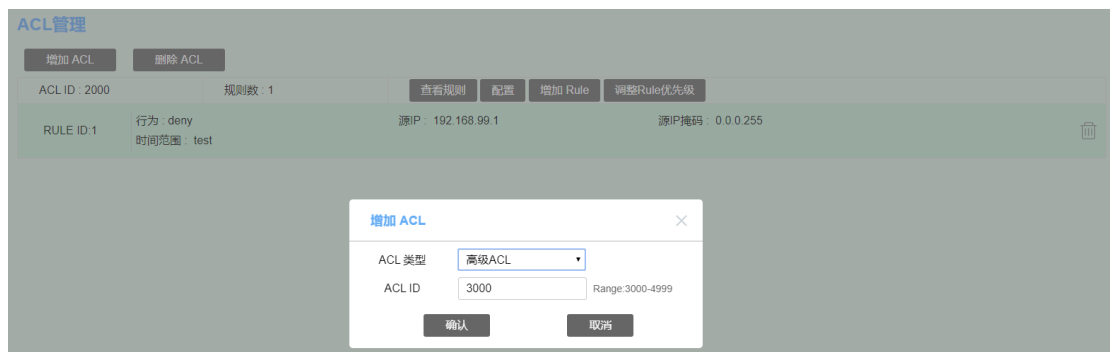


增加规则：可以选择 `time-range` 在指定的时间内生效或者不使用 `time-range` 立即生效。





- 高级 ACL(3000-4999): 当需要根据数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性制定匹配规则时, 使用此配置。成功创建规则后, 可以使用 `packet-filter` 命令引用规则对报文进行过滤。



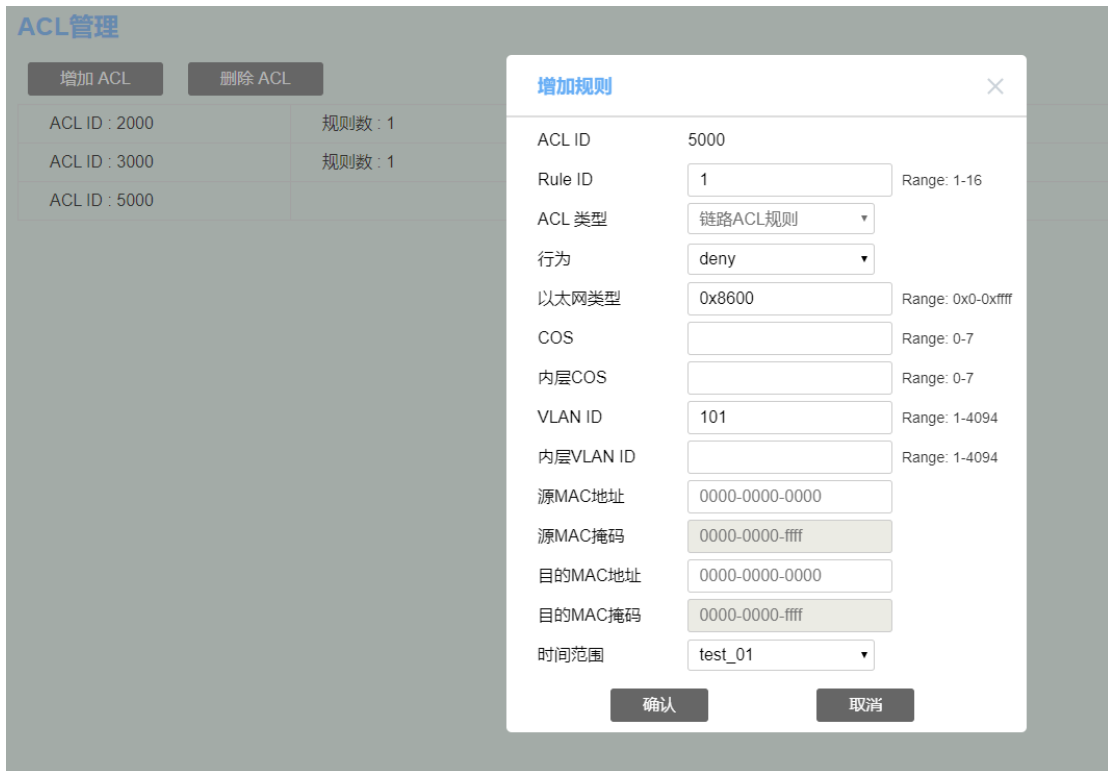
增加规则: 可以选择 `time-range` 在指定的时间内生效或者不使用 `time-range` 立即生效。



3. 链路 ACL(5000-5999): 当需要根据报文的源 MAC 地址、源 VLAN ID、二层协议类型、目的 MAC 地址等链路层信息制定 ACL 规则时, 使用此配置。成功创建 ACL 规则后, 可以使用 `packet-filter` 命令引用 ACL 规则对报文进行过滤。



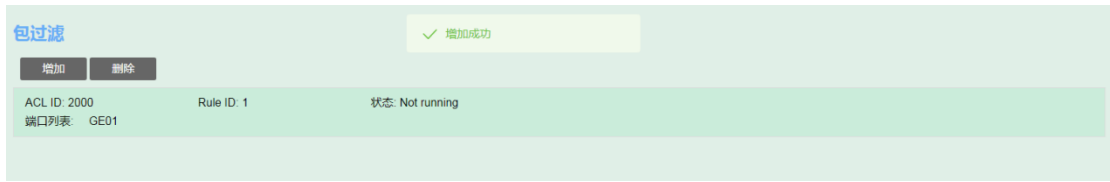
增加规则: 可以选择 `time-range` 在指定的时间内生效或者不使用 `time-range` 立即生效。



### 5.8.3 包过滤 (Packet Filter)

用于为指定端口配置 ACL 过滤规则，并使之生效。当需要使用 ACL 规则对端口流量进行过滤时，使用此配置。





## 5.8.4 QoS

用于配置系统的队列调度模式。队列调度，就是将需要从同一个端口发送出去的报文划分到多个队列中，在队列与队列之间进行调度，以决定哪个队列的报文先发送，哪个队列的报文后发送。当用户需要根据业务的重要程度选择不同的队列调度模式，以确保在网络出现拥塞时仍能为重要业务提供 QoS 保证时，使用此配置。设备支持 8 个队列。



### 1. 设置优先级和队列的映射关系





2. 设置队列调度：如果选择 WRR 模式，所有权重相加必须等于 100 或 0



队列调度程序 **配置**

COS	0	模式	WRR	权重	100
COS	1	模式	SP	权重	0
COS	2	模式	SP	权重	0
COS	3	模式	SP	权重	0
COS	4	模式	SP	权重	0
COS	5	模式	SP	权重	0
COS	6	模式	SP	权重	0
COS	7	模式	SP	权重	0

## 5.9 路由

### 5.9.1 路由管理

1. 打开路由开关:

路由状态

静态路由

目的IP掩码	下一跳	接口	协议	优先级	状态	配置
192.168.1.0/24	192.168.1.9	Vlanif100	Direct	1	Reachable	
192.168.2.0/24	192.168.2.8	Vlanif101	Direct	1	Reachable	
192.168.3.0/24	192.168.3.8	Vlanif200	Direct	1	Reachable	

**提示：**当关闭路由开关，所有静态路由配置以及 ARP 表项都会被清除。

## 2. 静态路由：

路由状态

静态路由

目的IP掩码	下一跳	接口	协议	优先级	状态	配置
192.168.1.0/24	192.168.1.9			1	Reachable	
192.168.2.0/24	192.168.2.8			1	Reachable	
192.168.3.0/24	192.168.3.8			1	Reachable	

**增加**

目的IP:  EX: 127.0.0.1

IP掩码:  EX: 255.255.255.0

下一跳:  EX: 127.0.0.1

当下一条是可达的情况，会主动学习到下一跳网关的 ARP，该静态路由的状态就会变成可达状态。

路由配置 ✓ 增加成功

路由状态

静态路由

目的IP掩码	下一跳	接口	协议	优先级	状态	配置
192.168.5.0/24	192.168.1.8	*		2	Unreachable	<a href="#">删除</a>
192.168.3.0/24	192.168.1.9	*		2	Unreachable	<a href="#">删除</a>
192.168.99.0/24	192.168.99.1	Vlanif1	Direct	1	Reachable	

## 5.9.2 ARP 表

ARP

IP地址	MAC地址	VLAN ID	端口号
192.168.5.184	f0:79:59:e0:70:74	200	GE03

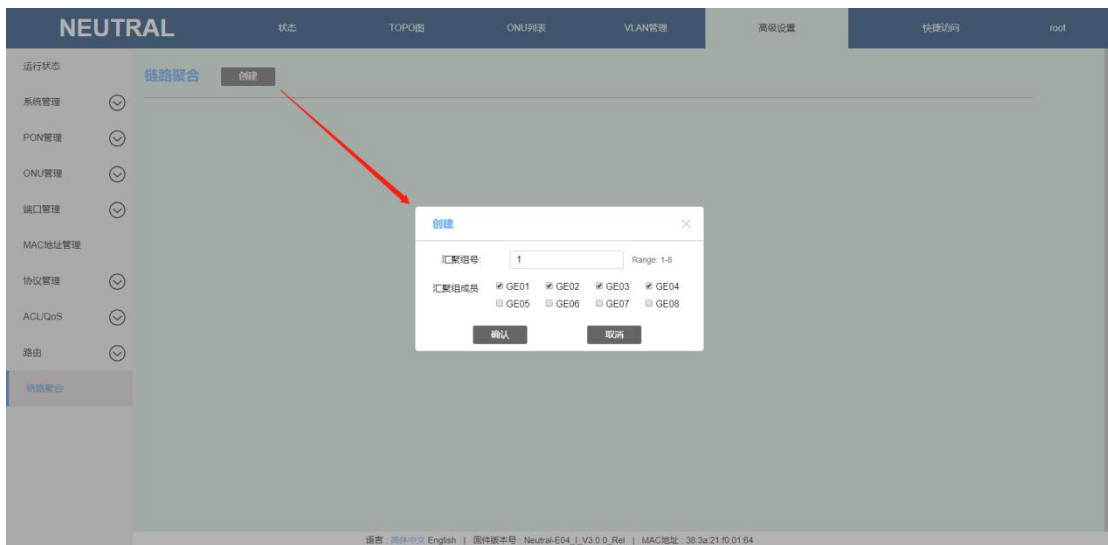
## 5.10 链路聚合

链路聚合是多个同类型的上联端口捆绑为一个逻辑端口，在不升级硬件的情况下，达到增大上联端口带宽的目的，并且通过链路备份机制，有效提升链路之间的可靠性。

### 1. 创建链路聚合

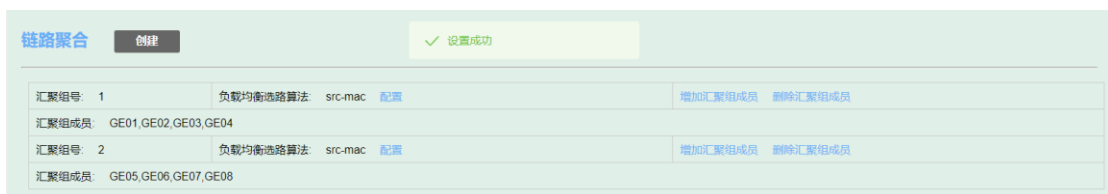
**提示：**

- ①一个端口不能同时加入多个汇聚组；
- ②生成树协议：加入汇聚组的端口会当成一个逻辑端口进行协议运算；
- ③上联口环路检测：当端口加入汇聚组，该端口环路检测不生效；
- ④上联端口属性：加入汇聚组的成员端口属性必须一致：速率、端口类型、MTU、端口限速、风暴控制；配置汇聚组成员端口属性时，组内成员绑定在一起配置；
- ⑤VLAN 属性：加入汇聚组的成员端口 VLAN 配置必须一致：PVID、端口 VLAN；配置汇聚组成员 VLAN 时，组内成员绑定在一起配置；
- ⑥端口镜像目的端口不能作为聚合组成员加入聚合组，同时加入聚合组的端口不能成为镜像目的端口；
- ⑦配置了静态 MAC 地址的端口不能作为聚合组成员加入聚合组；
- ⑧配置了 ACL 规则的端口不能作为聚合组成员加入聚合组；
- ⑨配置了组播 VLAN 路由端口不能作为聚合组成员加入聚合组；



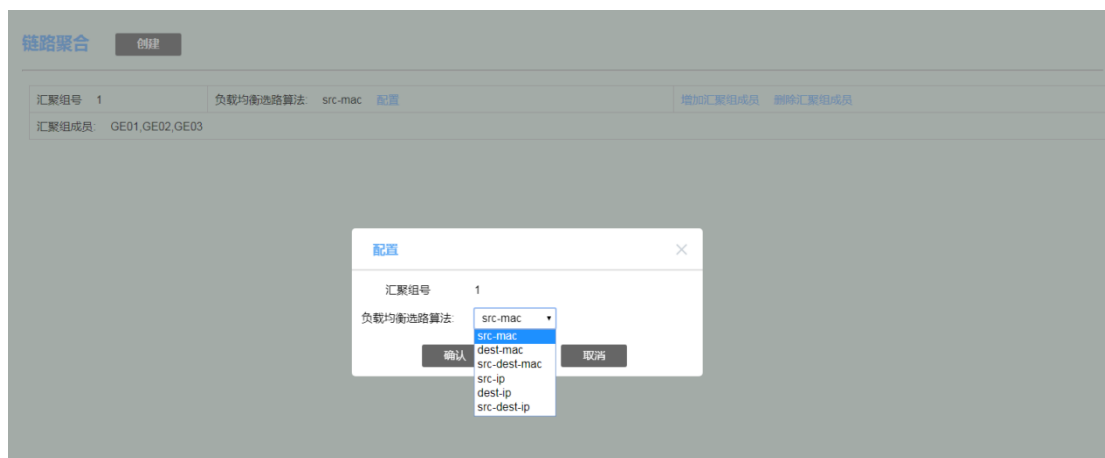
## 2. 查看链路聚合

创建成功后，可以查看到加入汇聚组的成员端口，并且可以在该汇聚组内增加和删除汇聚组成员。



## 3. 负载均衡选路算法

负载均衡选路算法默认是基于 src-mac 进行哈希计算，可配根据需求配置其他选路算法。



#### 4. 删除链路聚合

当需要删除链路聚合，把汇聚组内成员全部删除，该汇聚组就被删除。



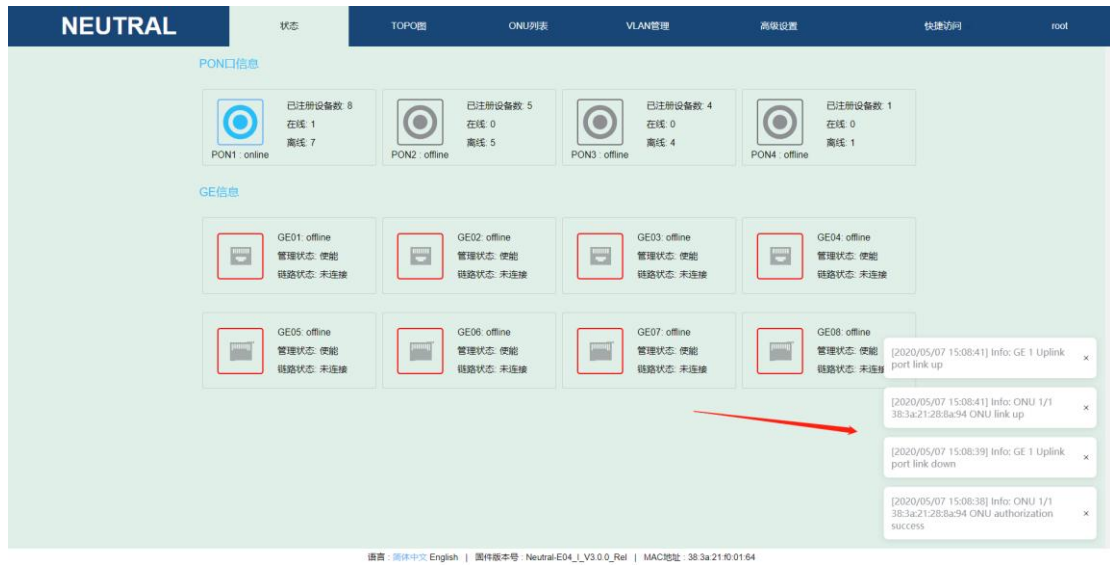


## 6 快捷访问

登陆页面成功后鼠标光标移至快捷访问自动展示如下功能：



1. 关闭实时告警：关闭页面右下角自动弹出的实时告警信息





2. 保存配置: 保存当前访问 OLT 所修改后的所有配置信息
3. 退出登录
4. 重启
5. PON 口光诊断: 快速访问 PON 管理——PON 口光诊断



6. 查看当前配置: 导出当前 OLT 的配置文件, 文件名 olconfigtmp.txt
7. 简体中文&English: 切换页面语言

# 7root

点击右上角 root 后进入系统管理——用户管理

The screenshot displays the NEUTRAL system management interface. The top navigation bar includes 'NEUTRAL', '状态', 'TOPO图', 'ONU列表', 'VLAN管理', '高级设置', '快速访问', and 'root'. The left sidebar lists various system management functions such as '运行状态', '系统管理', '设备管理', '诊断工具', '网络接口', '升级管理', '时间管理', '服务', '告警', 'PON管理', 'ONU管理', '端口管理', 'MAC地址管理', '协议管理', 'ACLUoS', and '路由'. The main content area is titled '用户管理' and shows a table of current users. The table has columns for '用户', '状态', '用户权限', '最大登录次数', '已登录次数', and '描述信息'. A single user 'root' is listed with status '在线', permissions 'super', a maximum of 1 login, 2 current logins, and the description 'Super User'. Below the table are buttons for '增加用户', '删除用户', and '修改当前用户密码'. At the bottom of the interface, there is a footer with language options and system version information: '语言: 简体中文 | English | 固件版本号: Neutral-E04\_L\_V3.0.0\_Rel | MAC地址: 38 3a 21 01 01 64'.

用户	状态	用户权限	最大登录次数	已登录次数	描述信息
root	在线	super	1	2	Super User

谢谢!