桢田管理型交换机

用户手册

手册版本: 2022-06-07-1.04

手册介绍

此用户手册为使用此型号交换机提供。手册包括交换机性能及功能。请在管理设备前阅读此手册。

适用对象

此手册适用于类似IT和网络技术的网络管理员。

安全注意事项

不要使产品离水太近，例如，在潮湿的地下室或游泳池.避免此产品处于电力风暴。闪电时可能发生电击的危险。

目录

第 1 部分: 产品介绍

1.1 产品特性

- 支持链路聚合
- 支持IEEE 802.1Q VLAN
- 支持速率限制，端口统计
- 支持端口镜像
- 支持QoS，提供严格优先，加权优先等
- 支持MAC地址绑定
- 支持环路检测，避免出现环路灾难
- 支持IGMP snooping
- 支持基于WEB管理
- 支持串口模式管理
- 支持基于WEB的固件升级
- 支持参数备份和恢复

1.2 技术规格

1.2.1 前面板

前面板有24个10/100M自适应UTP端口和4个1000M combo口和LED指示灯。24个端口支持10/100Mbps带宽连接设备，自动协商能力，并且有另外4个支持1000Mbps。每个端口相应有一个指示灯，LNK / ACT，1000Mbps指示灯。

CONSOLE口:波特率: 115200，数据位: 8 停止位: 1

指示灯：

LED	状态	功能
PWR	正常	电源启动
	关闭	电源关闭
10/100/1000M	正常	相应端口连接正常

	关闭	相应端口连接异常
LNK/ACT	闪烁	数据传输
	正常	相应端口连接正常

1.2.2 后面板

电源:电源适配器插座.

第 2 部分：安装设备

2.1 安装注意事项

确保设备放置的表面足够安全以防止它变得不稳定。确保电源输出端放置在离设备1.8m远。确保设备到电源用AC电源线安全连接。确保设备周围有良好的通风和散热环境。
不要在设备上放置重物。

2.2 桌面或搁板安装

将交换机底部向上放置在桌面上，在询问每个角上安装橡胶脚.翻转过来将交换机放置在桌面上。

2.3 机架安装

首先，在设备每边安装机架安装架，使用支撑螺丝钉，然后安装交换机到19寸机架上。

2.4 AC 电源

交换机可以使用AC供电100 到240V AC，50 到 60Hz。交换机内置供电系统可以为输入电压自动改变操作电压。电源连接口在交换机后面板。
电源线可以插到交换机后面板的插口上，另一端插到电源输出口上。

第 3 部分：登录到设备

您可以使用基于web的方式来配置以管理。 可以通过web浏览器配置，至少要有一台PC通过以太网线连接到。

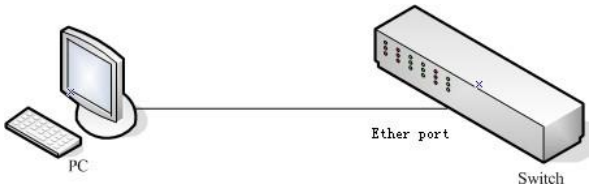


Figure 3-1

交换机默认IP地址为192.168.1.253，子网掩码为255.255.255.0.当要登录到交换机时，确认主机网卡的IP地址和交换机的在同一网段: 192.168.1. *** (1 <*** <255， *** 不等于1).参考以下步骤来设置:

3.1 配置您的电脑

可通过web页面来管理此管理型交换机.灵活和友好的界面使交换机管理成为容易的工作。WEB页面在不同的操作系统下可能显示有所不同。

3.1.1 Windows XP

按如下步骤配置您的电脑:

1.开始菜单—控制面板

Figure 3-1-1

2. 点击”网络和Internet连接”

Figure 3-1-2

3. 点击”网络连接”

Figure 3-1-3

4. 右键单击适配器图标并点击”属性”

Figure 3-1-4

5.双击“Internet协议(TCP/IP)”

Figure 3-1-5

6.使用如下IP地址:输入 192.168.1. *** (1 <*** <255， *** 不等于1，交换机默认IP为192.168.1.253)，子网掩码:255.255.255.0，默认网关和DNS服务器为可选不填，然后点击”确定”以关闭Internet协议(TCP/IP)属性窗口。

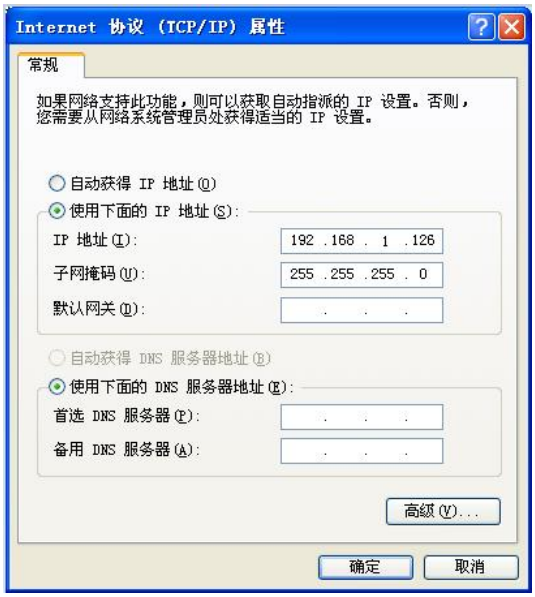


Figure 3-1-6

7.点击”确定”以关闭本地连接属性窗口

Figure 3-1-7

3.1.2 Windows 7/Windows Vista

按如下步骤配置您的电脑

1、开始菜单-控制面板

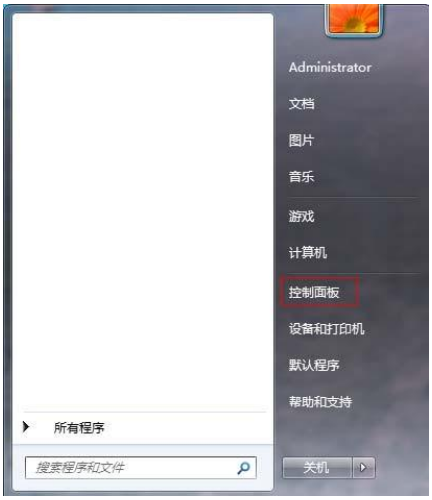


Figure 3-1-8

2、点击”网络和Internet ”

Figure 3-1-9

3、点击 ”更改适配器设置”

Figure 3-1-10

4. 右键单击适配器图标并选择”属性”

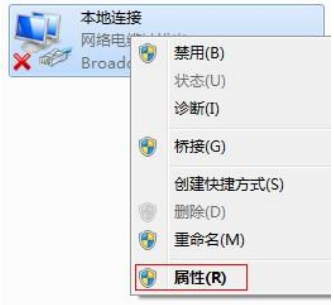


Figure 3-1-11

5.双击“Internet 协议版本4(TCP/IPv4)

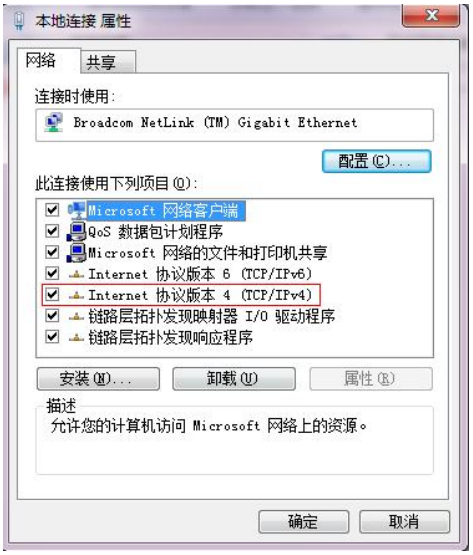


Figure 3-1-12

5、使用如下IP地址:输入 192.168.1. *** (1 <*** <255， *** 不等于1，交换机默认IP 为192.168.1.253)，子网掩码:255.255.255.0，默认网关和DNS服务器为可选不填，然后点击”确定”以关闭Internet协议(TCP/IP)属性窗口。

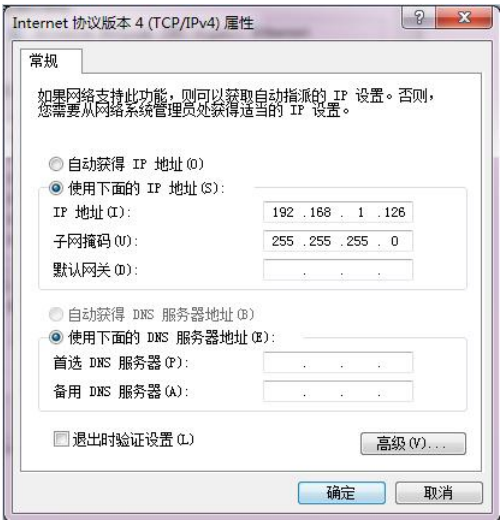


Figure 3-1-13

6、点击”确定”以关闭本地连接属性窗口

Figure 3-1-14

3.2 检查连接

在设置TCP/IP协议之后，您可以使用ping命令来检验PC主机是否能和交换机通信。需要执行ping命令检查，首先打开一个命令提示符窗口，然后执行ping命令的IP地址。进入命令行窗口，输入命令如：ping 192.168.1.253。

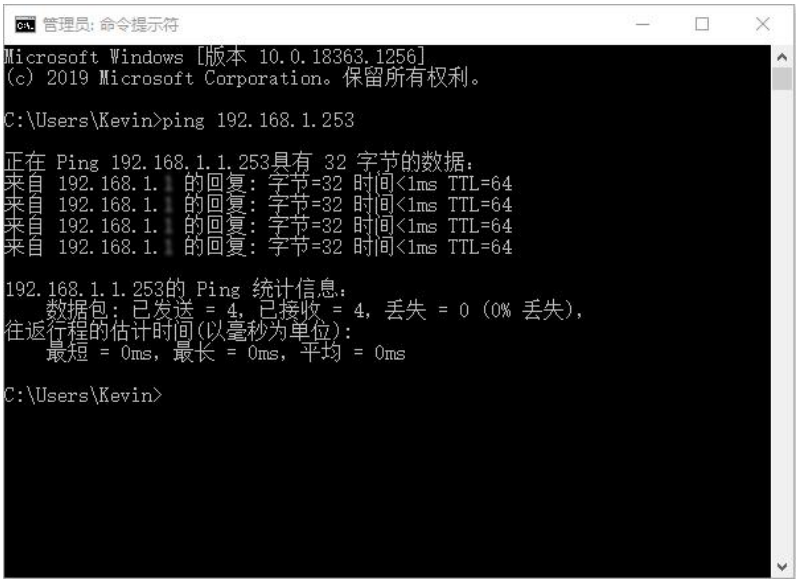


Figure 3-2-1

如命令行窗口返回如Figure 3-2-1，则表示PC和交换机之间的连接成功。

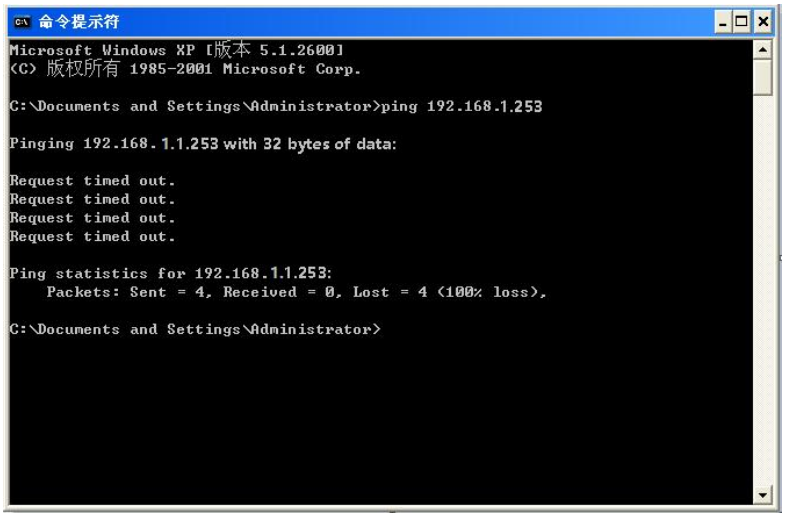


Figure 3-2-2

若PC到之间连接失败，命令行窗口将返回Figure 3-2-2内容。

请确保电脑网络设置正确且网线连接正常。

注意:
在进入上述命令之前，请使用双绞线连接到交换机端口和您PC的网卡。

3.3 登录到设备

1、 打开IE浏览器，在地址栏输入 http://192.168.1.253 并回车

Figure 3-3-1

2、在弹出窗口中输入用户名:admin，密码:admin，并点击”确定”

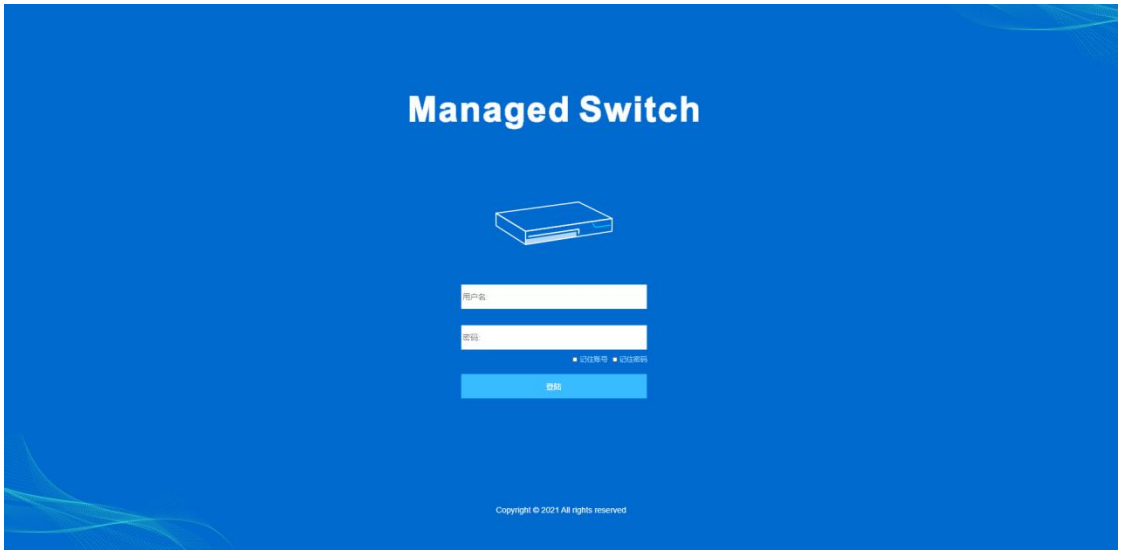


Figure 3-3-2

提示:

若您成功登录到交换机web页面，页面会实时刷新，以方便动态查看端口状态及其他信息。

3.4 功能概览

交换机具有丰富的特性，包括status，Network，port，VLAN，STP，Discovery，Multicast，Security，ACL，QoS，Diagnostics，Management设置，下一部分将为您介绍这些功能。

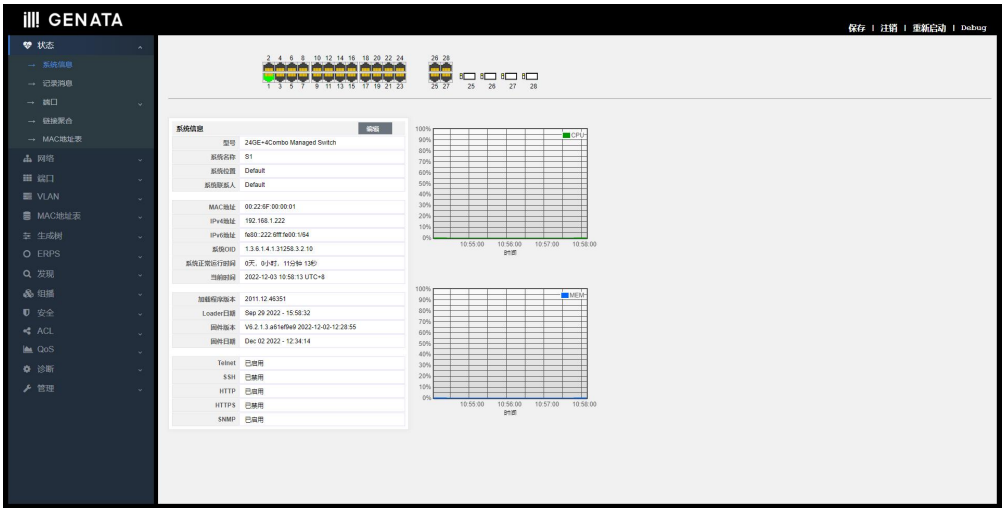


Figure 3-4-1

第 4 部分:系统

4.1 主页

在登录到交换机之后，可以看到如下图的主页.它包括三个部分:

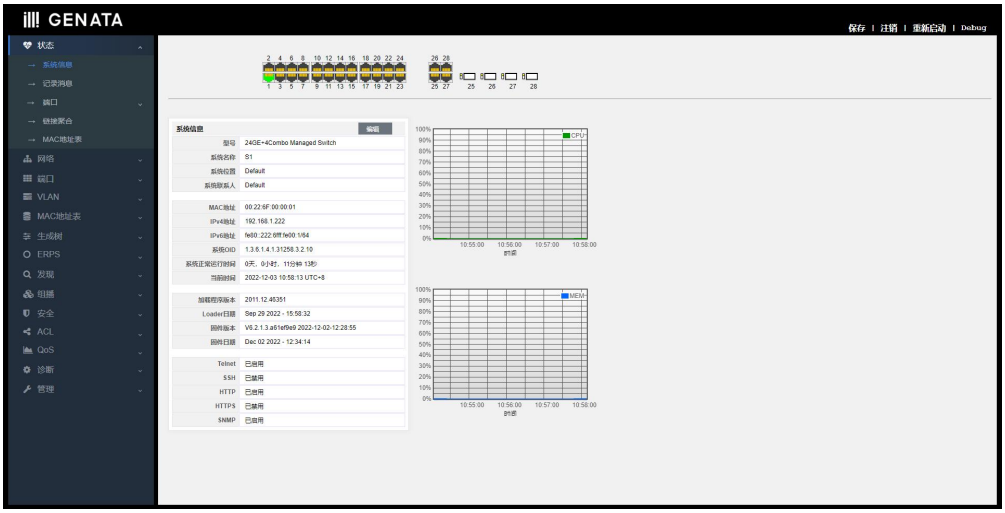


Figure 4-1-1

第"1"部分：在页面上方为端口Led指示器列表。提供了虚拟的端口提示。绿色标志表明端口连接，灰色图标明显端口没有连接。

第"2"部分：在页面左侧为菜单列表. 包含了12个主菜单.每个主菜单下有多个子菜单.点击菜单，将会出现子菜单和主窗口.

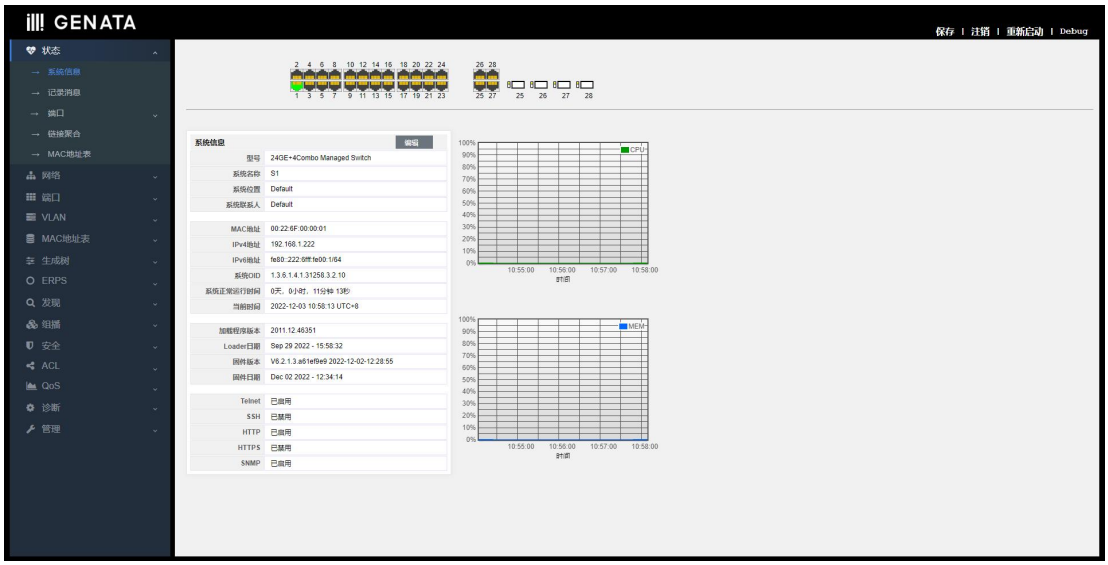
第3部分"：此页面的主要部分，显示配置页面。

4.2 Status

点击"Status" 出现如下所示交换机管理页面， 系统子菜单有一些基本信息，包括:系统信息，日志消息，端口管理，聚合，MAC地址表等。

Figure 4-2-1

Figure 4-2-2



系统信息菜单显示了系统的一些相关信息，如型号，系统名称，交换机MAC地址，IP地址，当前时间和CPU利息率。

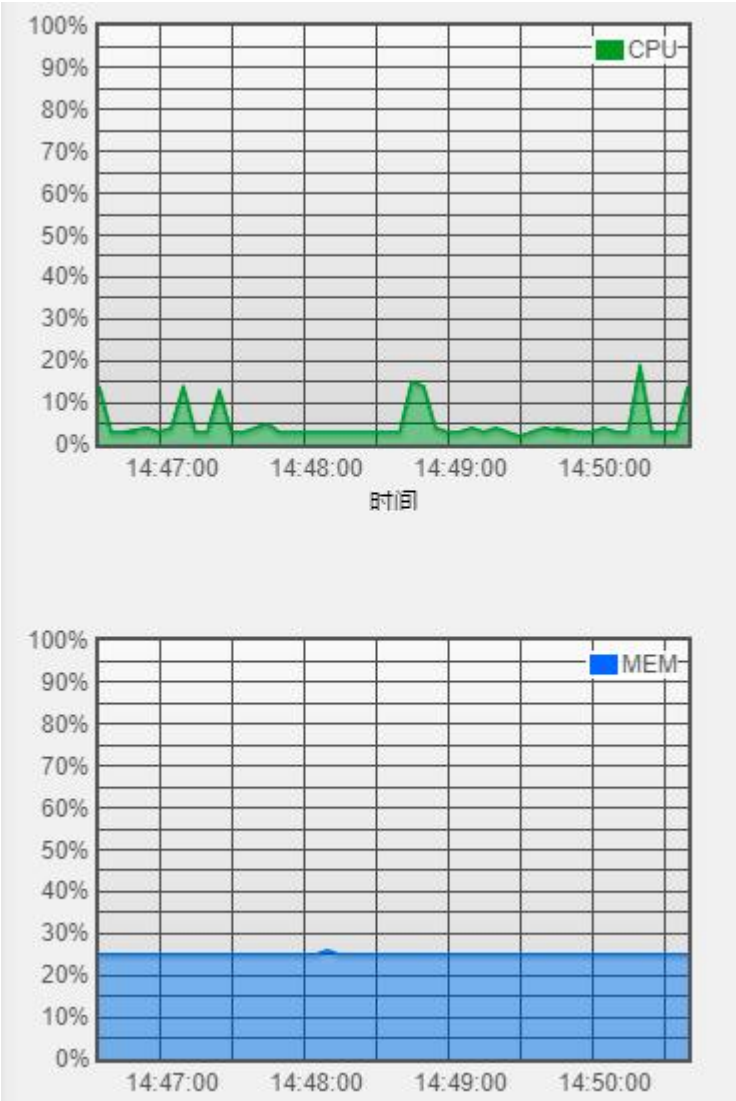


Figure 4-2-3

4.3 System information

在此页面上，可以看见访问web页面的端口号，您也可以看见交换机系统运行了多长时间。可以看见交换机当前的系统时间，开启了哪些服务：Telnet，SSH，HTTP，HTTPS，SNMP

最右边的第3部分界面就能看见，CPU和内存的实时利用率

4.4 Logging message

相关的信息都会记录到日志中，随时可以查看。不仅可以查看RAM里面的日志，还可以查看Flash里面的日志。

RAM：写到内存里面的日志信息，当交换机重启，RAM里面记录的日志信息就没有了。
Flash：写到Flash里面的日志信息，当交换机重启，Flash里面记录的日志信息依旧存在。

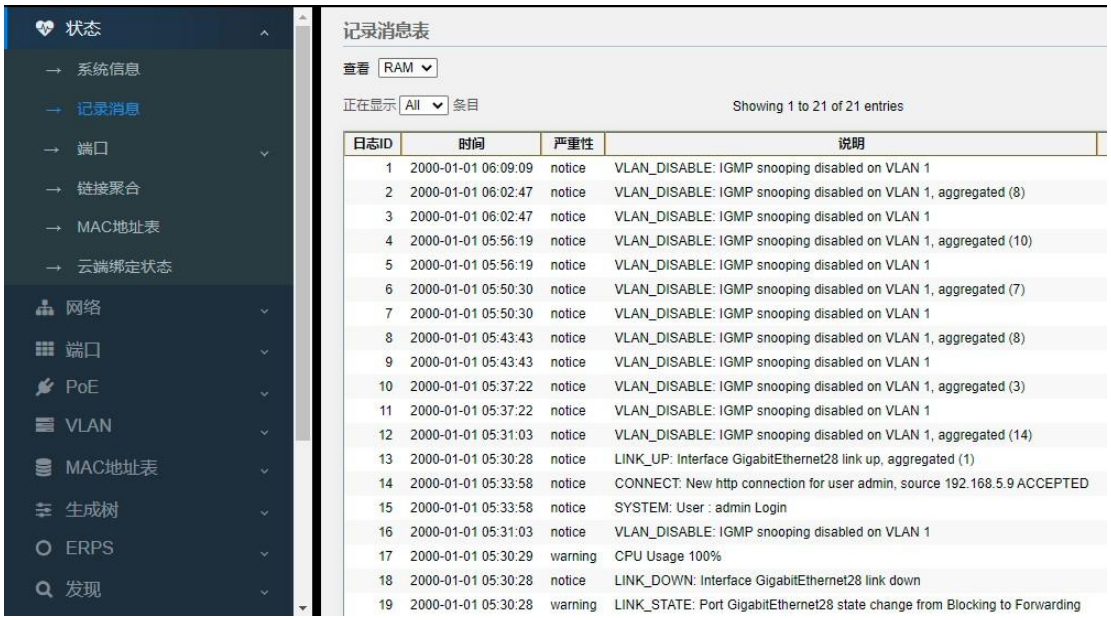


Figure 4-4-1

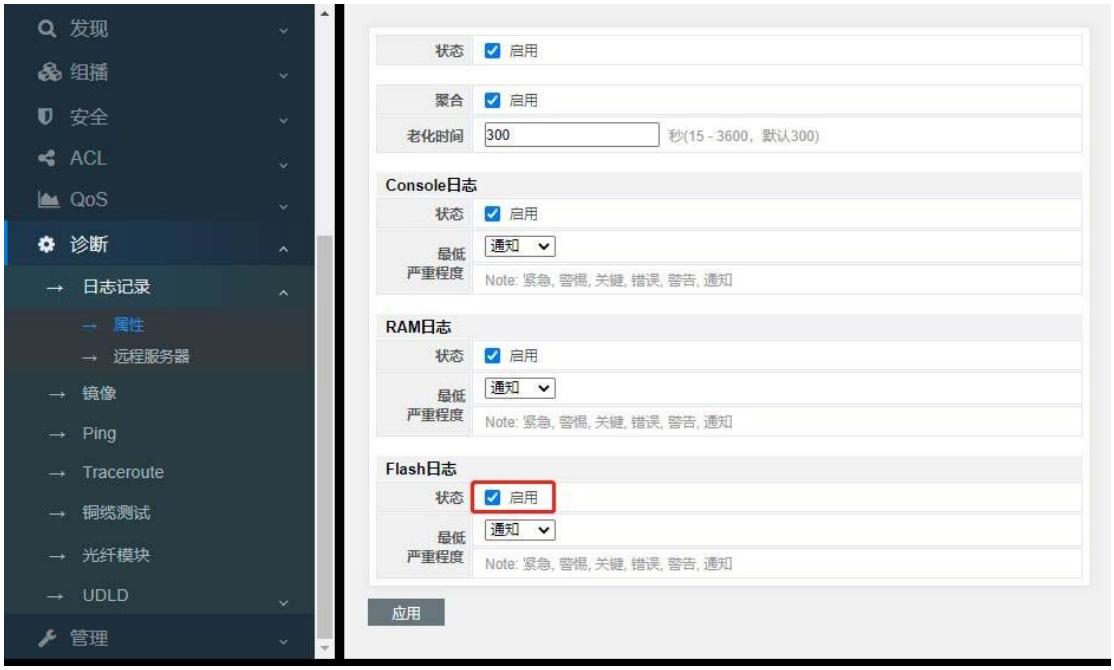
也还可以选择条目数，如果是All，就是选择一页显示所有条目数。
如果选择10，就表示一页显示10条日志信息条目，剩下的条目显示到后面的页面中，进行分页显示。

最后可以看见页面中，有一个搜索的输入框。可以输入“debug，info，notice……”进行分类显示。

Figure 4-4-2

注意：
如果希望日志保存到Flash里面，就需要在诊断菜单，日志记录中，把flash这个选项勾选上，才可以。

保存到Flash的好处是，即使交换机断电重启，以前的记录始终存在。如果保存到RAM里面，当交换机重启，之前的记录就没有了。



4.5 port

这个是查看端口的counter信息。

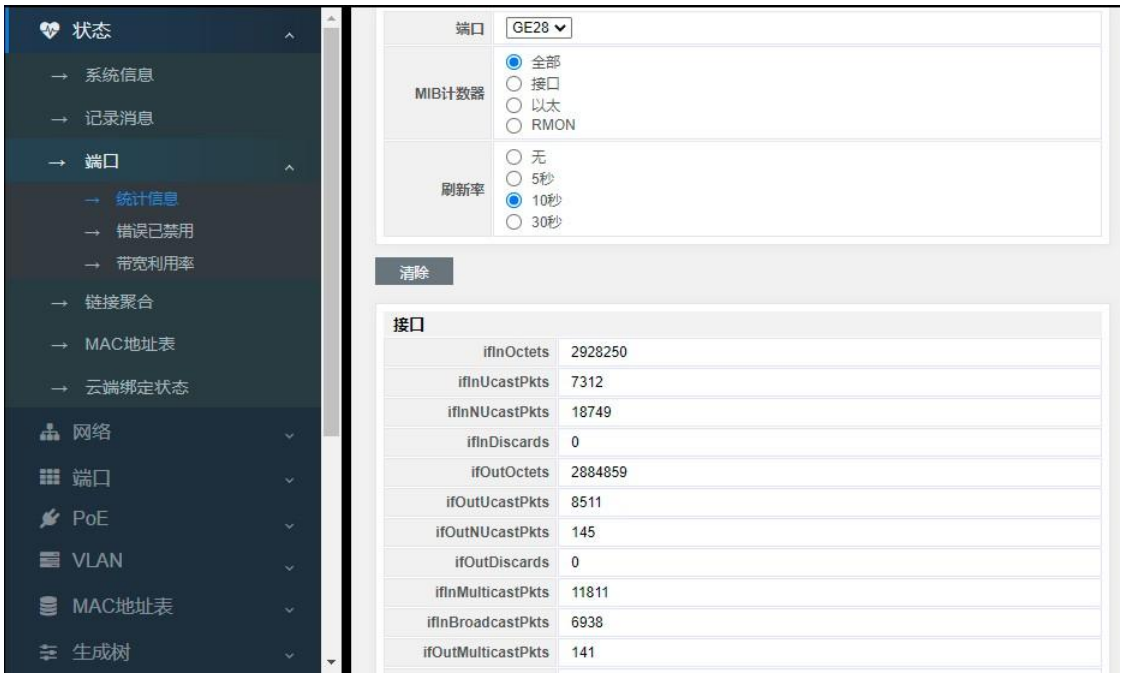


Figure 4-5-1

4.6 Link Aggregation

聚合组信息的显示：

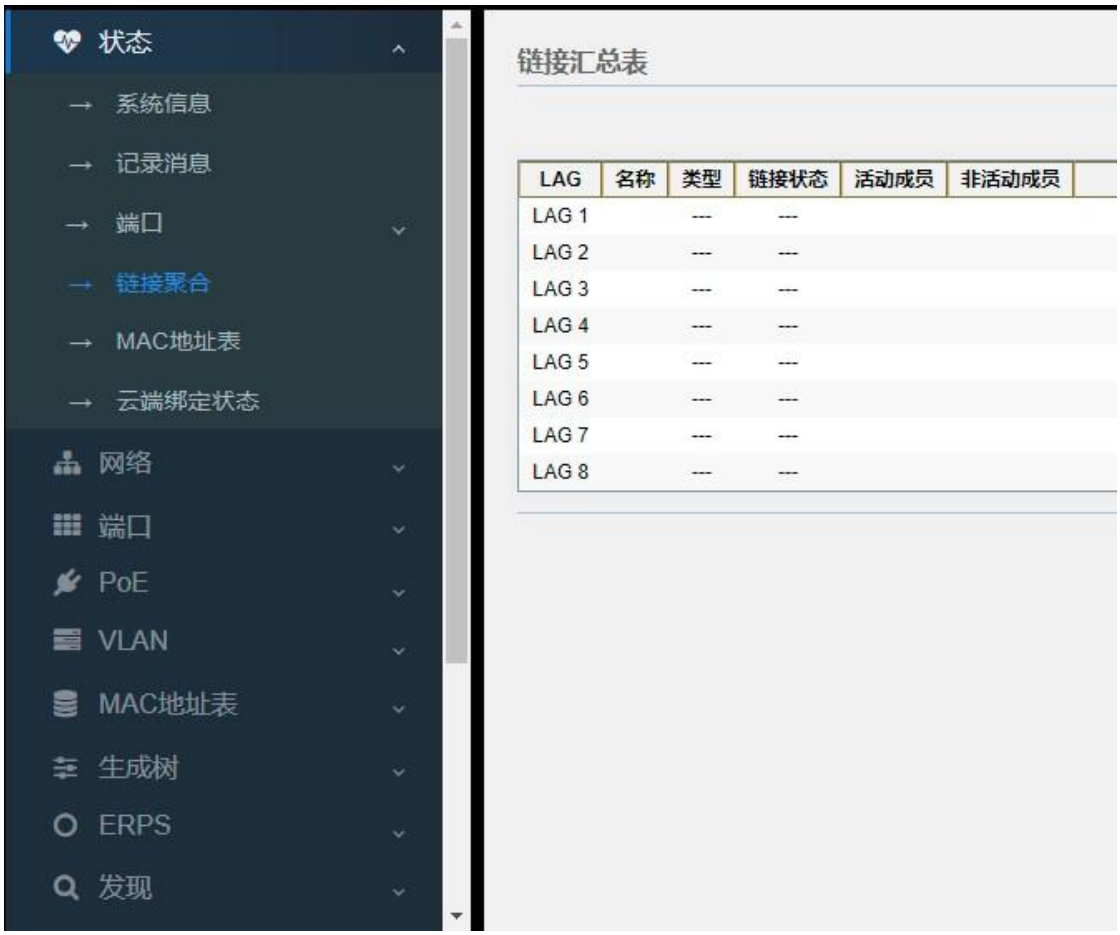


Figure 4-6-1

4.7 MAC Address Table

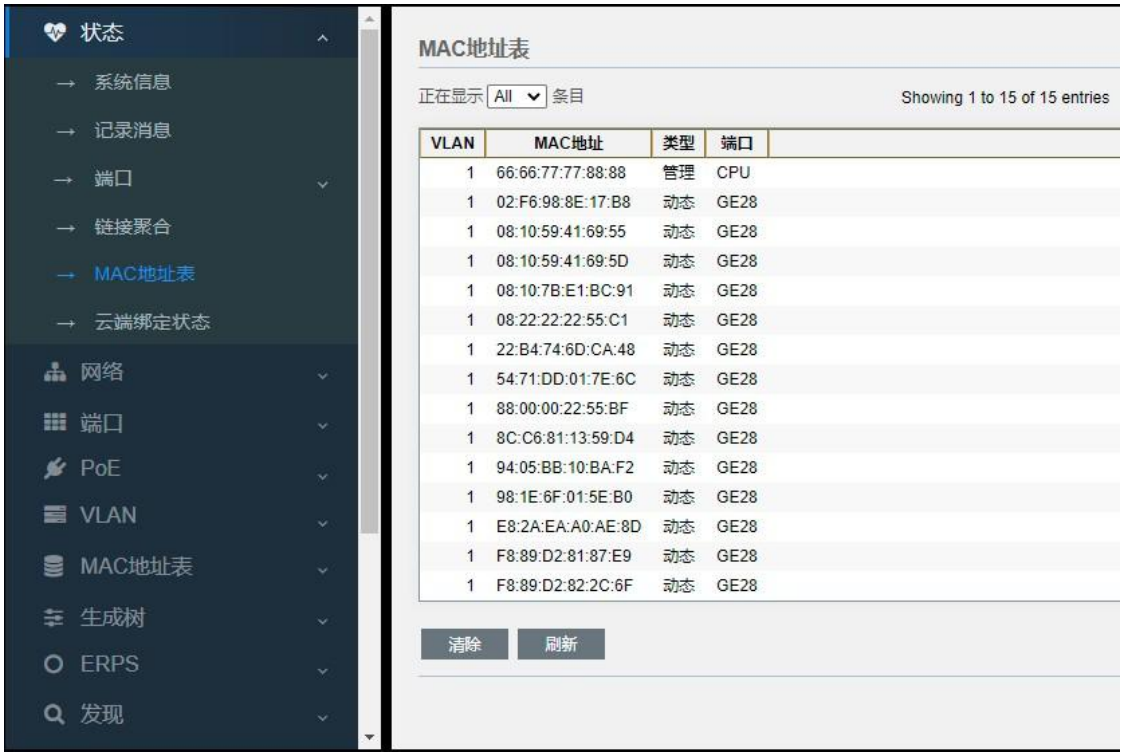


Figure 4-7-1

第 5 部分: Network

5.1 IP Address

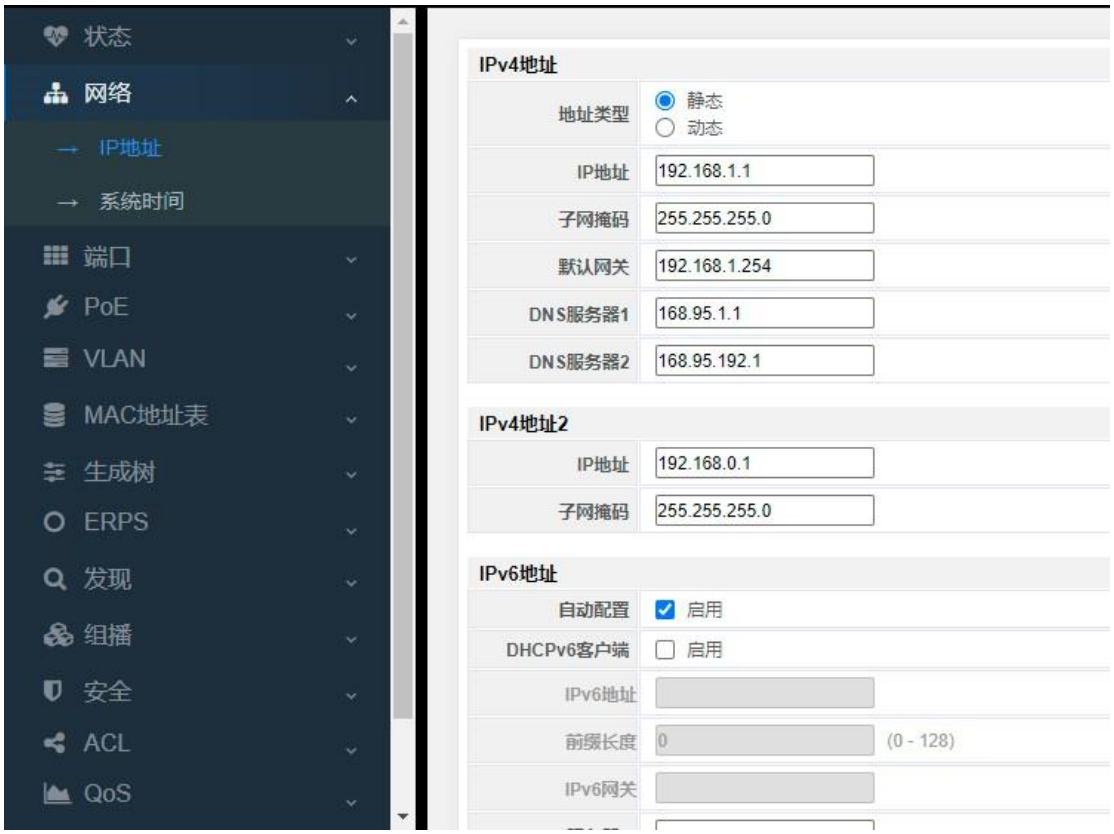


Figure 5-1-1

在这个页面中，您可以修改交换机的IPv4地址，子网掩码，网关及DNS Server。也可以配置DCHP获取IP地址。

同时也可以配置交换机的IPv6地址，不管是自动配置，还是DHCP获取，或是静态配置，都可以满足用户的需求。

5.2 System Time

Figure 5-2-1

交换机系统时间支持SNTP获取，也可以支持从访问交换机的电脑获取，还可以手动配置交换机系统时间。

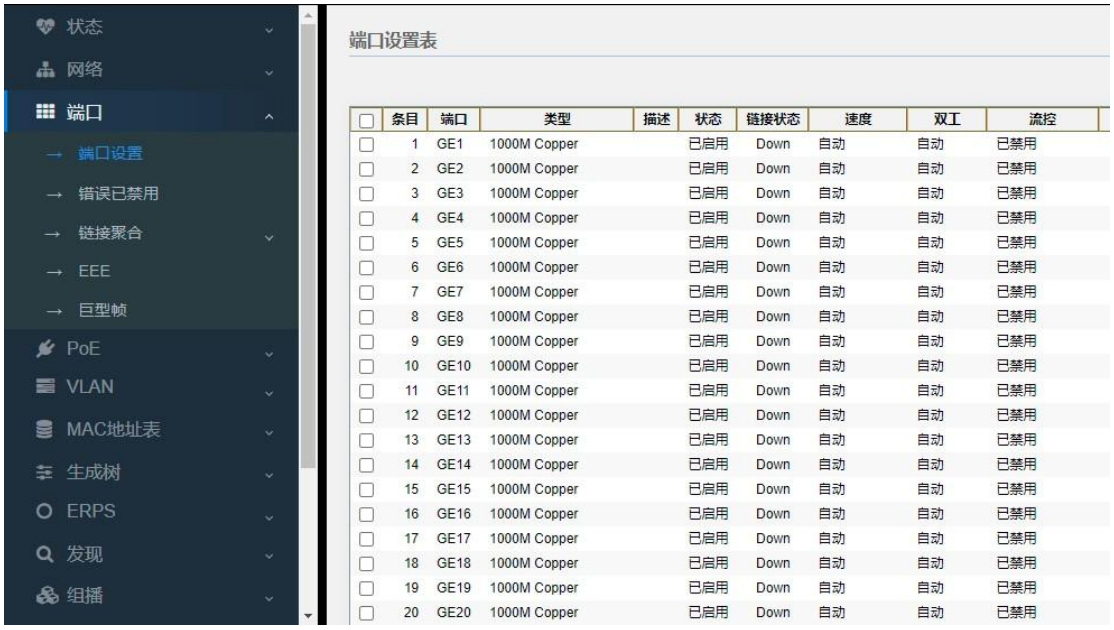
如果选择SNTP获取时间方式的话：

Figure 5-2-2

可以直接配置Time Server的IPv4的地址，port默认都是123，这样就可以了。

第 6 部分: Port

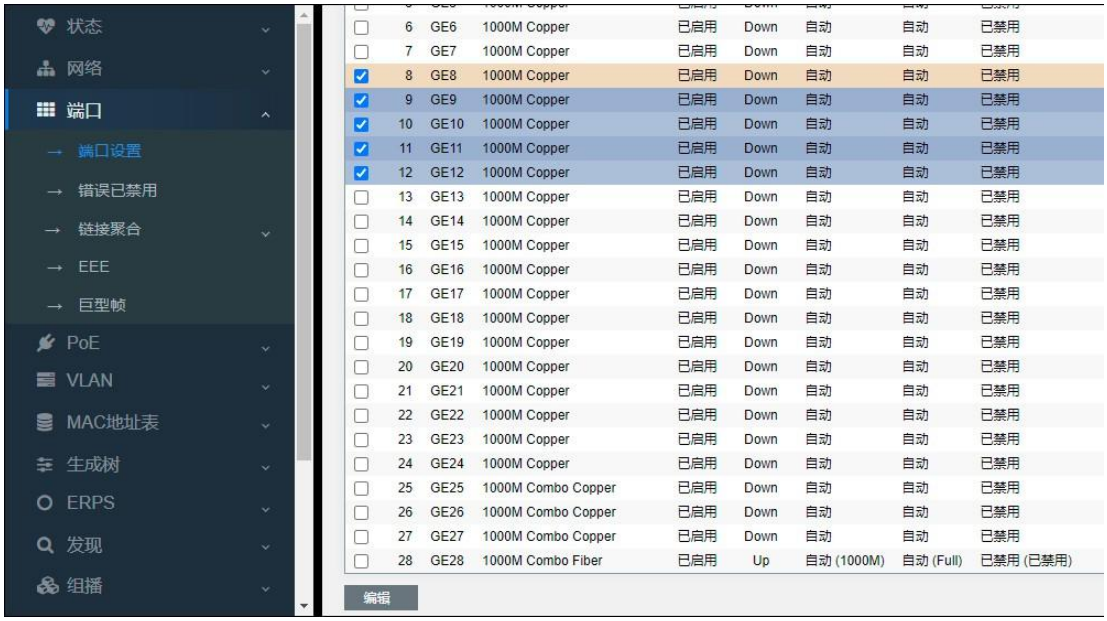
6.1 Port Setting



条目	端口	类型	描述	状态	链接状态	速度	双工	流控
1	GE1	1000M Copper		已启用	Down	自动	自动	已禁用
2	GE2	1000M Copper		已启用	Down	自动	自动	已禁用
3	GE3	1000M Copper		已启用	Down	自动	自动	已禁用
4	GE4	1000M Copper		已启用	Down	自动	自动	已禁用
5	GE5	1000M Copper		已启用	Down	自动	自动	已禁用
6	GE6	1000M Copper		已启用	Down	自动	自动	已禁用
7	GE7	1000M Copper		已启用	Down	自动	自动	已禁用
8	GE8	1000M Copper		已启用	Down	自动	自动	已禁用
9	GE9	1000M Copper		已启用	Down	自动	自动	已禁用
10	GE10	1000M Copper		已启用	Down	自动	自动	已禁用
11	GE11	1000M Copper		已启用	Down	自动	自动	已禁用
12	GE12	1000M Copper		已启用	Down	自动	自动	已禁用
13	GE13	1000M Copper		已启用	Down	自动	自动	已禁用
14	GE14	1000M Copper		已启用	Down	自动	自动	已禁用
15	GE15	1000M Copper		已启用	Down	自动	自动	已禁用
16	GE16	1000M Copper		已启用	Down	自动	自动	已禁用
17	GE17	1000M Copper		已启用	Down	自动	自动	已禁用
18	GE18	1000M Copper		已启用	Down	自动	自动	已禁用
19	GE19	1000M Copper		已启用	Down	自动	自动	已禁用
20	GE20	1000M Copper		已启用	Down	自动	自动	已禁用

Figure 6-1-1

1. 可以选择你需要配置的端口，例如：port 8-12



6	GE6	1000M Copper	已启用	Down	自动	自动	已禁用
7	GE7	1000M Copper	已启用	Down	自动	自动	已禁用
8	GE8	1000M Copper	已启用	Down	自动	自动	已禁用
9	GE9	1000M Copper	已启用	Down	自动	自动	已禁用
10	GE10	1000M Copper	已启用	Down	自动	自动	已禁用
11	GE11	1000M Copper	已启用	Down	自动	自动	已禁用
12	GE12	1000M Copper	已启用	Down	自动	自动	已禁用
13	GE13	1000M Copper	已启用	Down	自动	自动	已禁用
14	GE14	1000M Copper	已启用	Down	自动	自动	已禁用
15	GE15	1000M Copper	已启用	Down	自动	自动	已禁用
16	GE16	1000M Copper	已启用	Down	自动	自动	已禁用
17	GE17	1000M Copper	已启用	Down	自动	自动	已禁用
18	GE18	1000M Copper	已启用	Down	自动	自动	已禁用
19	GE19	1000M Copper	已启用	Down	自动	自动	已禁用
20	GE20	1000M Copper	已启用	Down	自动	自动	已禁用
21	GE21	1000M Copper	已启用	Down	自动	自动	已禁用
22	GE22	1000M Copper	已启用	Down	自动	自动	已禁用
23	GE23	1000M Copper	已启用	Down	自动	自动	已禁用
24	GE24	1000M Copper	已启用	Down	自动	自动	已禁用
25	GE25	1000M Combo Copper	已启用	Down	自动	自动	已禁用
26	GE26	1000M Combo Copper	已启用	Down	自动	自动	已禁用
27	GE27	1000M Combo Copper	已启用	Down	自动	自动	已禁用
28	GE28	1000M Combo Fiber	已启用	Up	自动 (1000M)	自动 (Full)	已禁用 (已禁用)

Figure 6-1-2

2. 然后点击左下角的"Edit" 按键。
3. 可以配置端口的管理状态、速度、双工、流控

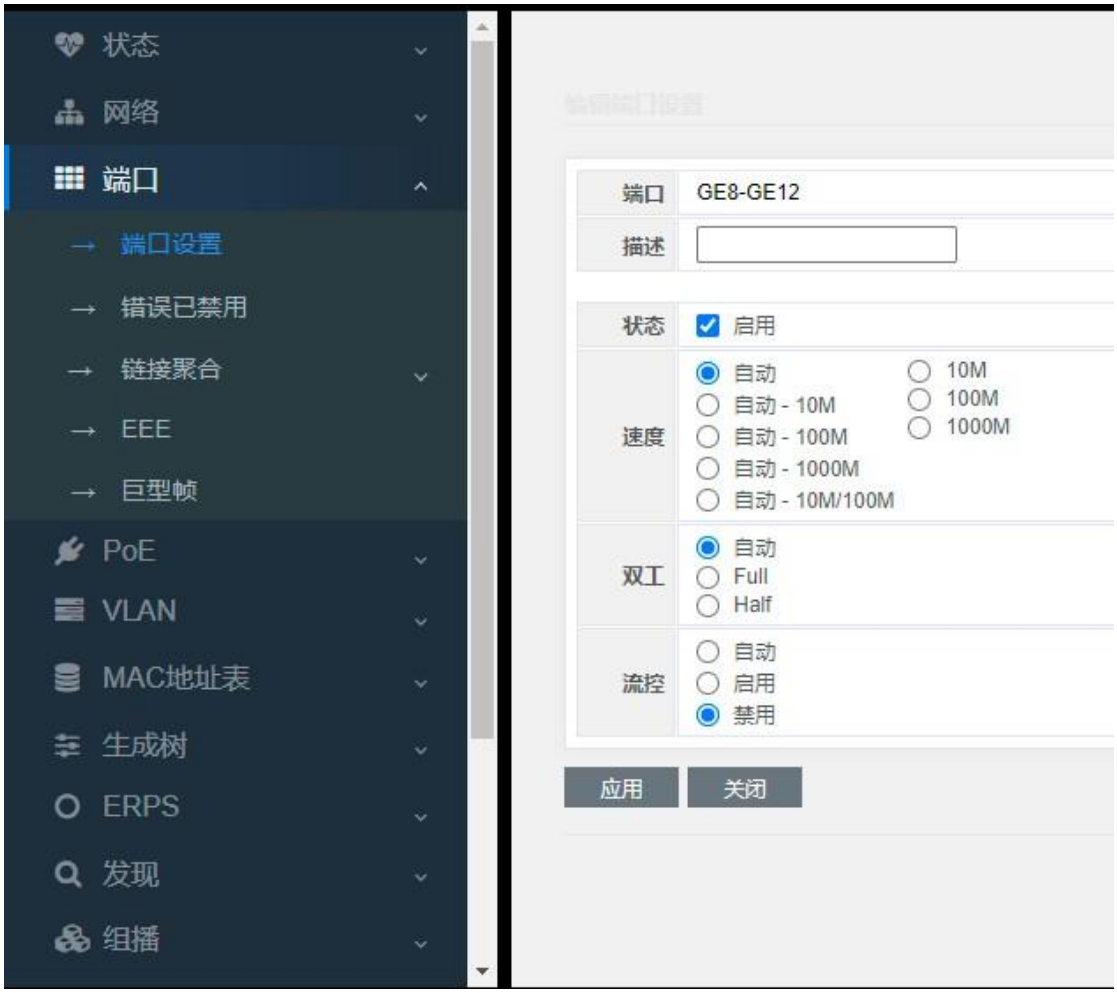


Figure 6-1-3

管理状态：Enable/Disable，开启表示端口可以正常使用，关闭表示端口不能使用。
速度：可以设置自动协商默认（5种），也可以设置强制模式（3种）
双工：自动模式，双工，半双工
流控：自动协商，开启，关闭

6.2 Error Disabled

关于接口处于err-disable的故障排查，故障症状： 线路不通，物理指示灯灭或者显示为橙色(不同平台指示灯状态不同)

Figure 6-2-2

从列表中，我们可以看出常见的原因有udld，bpduguard，port security以及loop等。
具体由什么原因导致当前接口err-disable可以查看。

系统在一段时间后试图恢复被置为err-disable的接口，这段时间缺省为300秒。
但是，如果引起err-disable的源没有根治，在恢复工作后，接口会再次被置为err-disable。
也可以调整err-disable的超时时间。

6.3 Link Aggregation

理解链路聚合

链路聚合在交换机，路由器和服务器之间提供容错高速的连接。您可以使用它在配线架和数据中心间增加带宽，并且您可以在网络中任何发生瓶颈的地方配置它。链路聚合通过重新分配负载通信在保持的链路上，为丢失的链路提供自动修复。如果一个链路断掉，链路聚合在聚合中无影响的从断掉的链路上重定向流量到保持的链路上。

每个链路聚合最多可以由8个适当配置过的以太接口组成。在链路聚合中的所有接口必须为相同速度且所有必须配置为2层接口。

链路聚合介绍

链路聚合可以将多个以太端口聚合在一起以形成一个逻辑聚合组。在层实体上，所有在一个聚合组的物理链路为一个逻辑链路。链路聚合被设计在一个聚合组中通过执行在成员端口间输出/输入负载分配以增加带宽。链路聚合组同样允许端口冗余提供连接可靠性。

LACP介绍

链路聚合控制协议 (LACP)设计以执行动态链路聚合和解聚合.这个协议基于IEEE802.3ad

且使用链路聚合控制协议数据单元(LACPDUs)和对点的启用LACP的端口组合，LACP通过LACPDUS通报端口的如下信息到它对端：系统优先级和MAC地址，端口优先级，端口号和操作key。
当收到信息，接入点将信息同在对点设备上的其他端口的信息相比较以决定端口能被聚合.用这种方式，两部分可以达成一致从动态聚合组添加/移除端口。
系统产生操作key。它被端口决定，如端口速度，双工模式，和基本配置。

- 在手动聚合组或静态聚合组选择的端口具有相同的操作key
- 在动态聚合组的成员端口具有相同的操作 key

交换LACP报文
主动和被动LACP模式都允许接口和对端口接口协商以决定它们是否可以基于如：接口速度，2层聚合，trunk状态和VLAN成员的标准成为一个聚合组。
当接口为不同的LACP模式，只要模式兼容，它们可以成为一个聚合组。例如：

- 在主动模式的接口可以同另一个在被动模式的接口成为一个聚合组。

在被动模式的接口不能和另一个也在被动模式下的接口成为一个聚合组，因为它们都不会开始LACP协商。
被添加为聚合端口在开启模式的端口强制和聚合组其他已经存在的开启模式的接口有相同的特征。

理解负载均衡和转发办法

链路聚合通过随机分配一个新链路新学到的MAC地址来平衡通过聚合中链路的流量负载。

以源MAC地址转发，到一个聚合口的被转发的报文基于进入报文的源MAC地址分布式地通过聚合组的端口。因此，以提供负载均衡的方式，从不同主机发出的报文使用聚合组中不同的端口，但从同一主机发出的报文使用聚合组中相同的端口。交换机学习MAC地址不改变。

以目的地址转发，被转发到聚合口的报文基于进入报文的目的MAC地址分布式地通过聚合组端口。因此，到相同目的的报文通过相同端口被转发，并且到不同目的的报文可能在聚合的不同端口被转发。

多个工作站连接到交换机，并且一个聚合口连接交换机到路由器。
交换机上使用的链路聚合上基于源的负载均衡确保交换机有效的使用路由器带宽，通过从工作站的物理连接分布通信。因为路由器是单MAC地址的设备，在链路聚合中使用基于目的的负载均衡通过物理连接有效的分布流量到工作站。

Figure 6-3-1

6.3.1 Group

配置静态聚合

Load Balance Alogorithm，负载均衡算法：

- MAC address（源MAC+目的MAC）
- IP-MAC address (源IP+目的IP+源MAC+目的MAC)

这个是聚合的选路算法，报文选择哪条线路，就是根据报文内容的address进行选路。

1. 选择聚合组（1-8），LAG 1~LAG 8
2. 点击Edit按键
3. 然后选择静态，将端口从左边的框添加到右边，以使端口加入聚合组。最多支持8个聚合组，且每个聚合组最多支持8个成员端口。

Figure 6-3-2

6.3.2 Port Setting

这个是设置聚合口的端口属性。

Figure 6-3-3

可以设置聚合口的速度、双工、流控。

Figure 6-3-4

6.3.3 LACP

可以设置 LACP 的 System Priority，也可以设置端口的 Port Priority。
默认已经配置了值，用户可以根据自己的需求进行修改。

Figure 6-3-5

6.4 EEE

Energy Efficient Ethernet，简称 EEE，即：节能高效以太网技术。作用是在网卡没有流量时自动降低功耗，只有网络使用率较高时，才会发挥最大功耗。

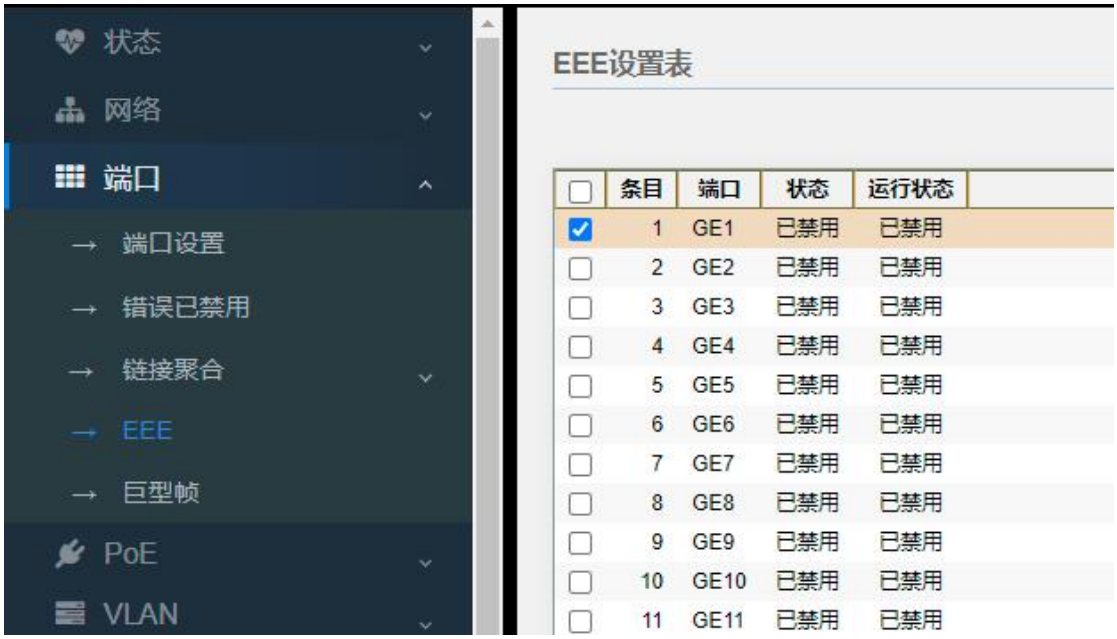


Figure 6-4

默认是端口关闭EEE的，如果需要这个功能，把端口开启就可以了。

注意：如果要使用这个功能，不仅本交换机的端口开启EEE功能，而且必须对端的端口也要开启，才能生效。

6.5 Jumbo Frame

Jumbo frame也称为巨型帧，是帧长大于1522字节的以太网帧。这是一种厂商标准的超长帧格式，专门为千兆以太网而设计。巨型帧的长度各厂商有所不同，从9000字节～64000字节不等。采用巨型帧能够令千兆以太网性能充分发挥，使数据传输效率提高50%～100%。在网络存储的应用环境中，巨型帧更具有非同寻常的意义。

Figure 6-5

只要开启了Jumbo Frame，是最大可以支持10K的。

第 7 部分: VLAN

7.1 VLAN

这儿主要说的是802.1Q-VLAN

VLAN 介绍

传统的以太网是广播网络，所有的主机在同一个广播域，并且通过集线器或交换机互相之间可以通信。集线器和交换机是基本的网络连接设备，只有有限的转发功能。

- 集线器是物理层连接设备，没有交换功能，它将收到的报文转发到除了收包外的所有端口。
- 交换机是可以依靠报文的MAC地址转发报文的链路层设备.交换机建立MAC地址表和端口的映射表，且只将已知MAC的流转发到一个端口。当交换机收到MAC不在交换机MAC地址表中的广播包或未知组播包，它将报文转发到除了收到报文的端口以外的所有端口。

以上设定可能导致如下网络问题

- 很大数量的广播包或未知单播包在网络中是可能存在的，会浪费网络资源。
- 一个主机收到很多目的不是这个主机自己的报文，导致潜在的严重的安全问题。
- 有关以上几点，网络中的某人能够监视广播包和单播包且得知他们在网络中的活跃性。那么他们可以试图访问网络上的其他资源，不管他们是否得到授权这样做。

以上的问题的解决是隔离广播域。传统方式是使用依照目的IP地址转发包的路由器且不转发链路层的广播包，路由器是昂贵的且只提供很少的端口，所以它们不能有效的分隔网络。因此，使用路由器隔离广播域有很多限制。

交换机的虚拟局域网(VLAN)技术得以发展以控制LAN内的广播。

一个VLAN可以跨越多个物理空间，这样可以激活处于不同的物理位置的一个VLAN内的主机。通过在一个物理LAN内创建VLAN， 您可以将LAN分隔成多个逻辑LAN，每个都有自己的广播域。 在相同VLAN内的主机用传统的以太方式通信，然而，在不同VLAN内的主机彼此之间不能直接通信，需要网络层设备，如路由器或三层交换机。

VLAN 优点

和传统以太技术相比较，VLAN技术具有如下好处：

- 限制广播域在单独的VLAN内。这可以节省带宽，改进网络效能。
- 提高网络安全。通过分配用户组到不同的VLAN，您可以在2层上隔离他们.要使不同VLAN间能够通信，需要路由器或3层交换机。
- 创建可变的虚拟工作组。相同工作组的用户可以被分配到相同的VLAN，不管他们的物理位置，网络建设和维护更容易和更具可变性。

7.1.1 Create VLAN

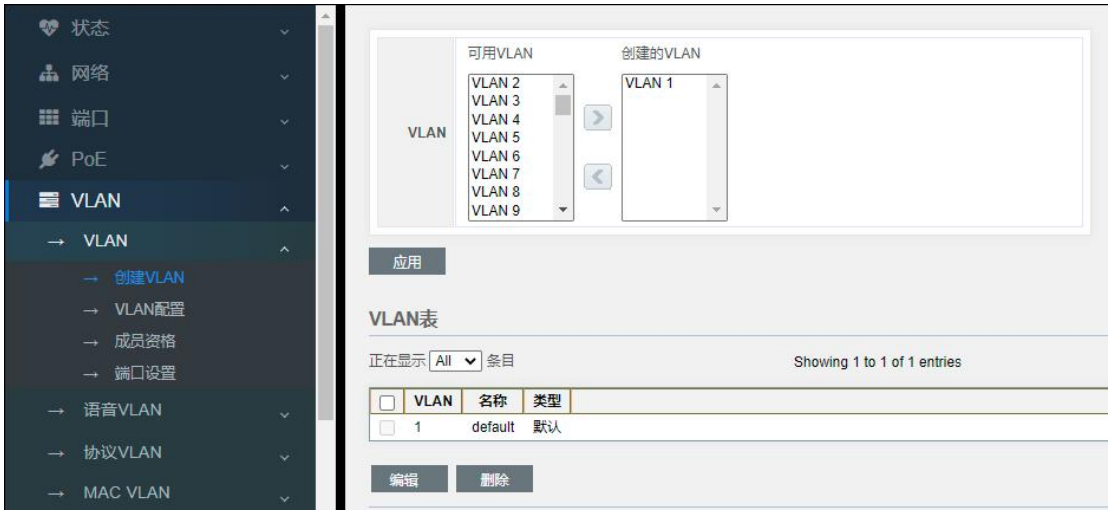


Figure 7-1-1

VLAN总数是1-4094，将VLAN号从左边的框添加到右边，默认已经加入了建立了VLAN 1。

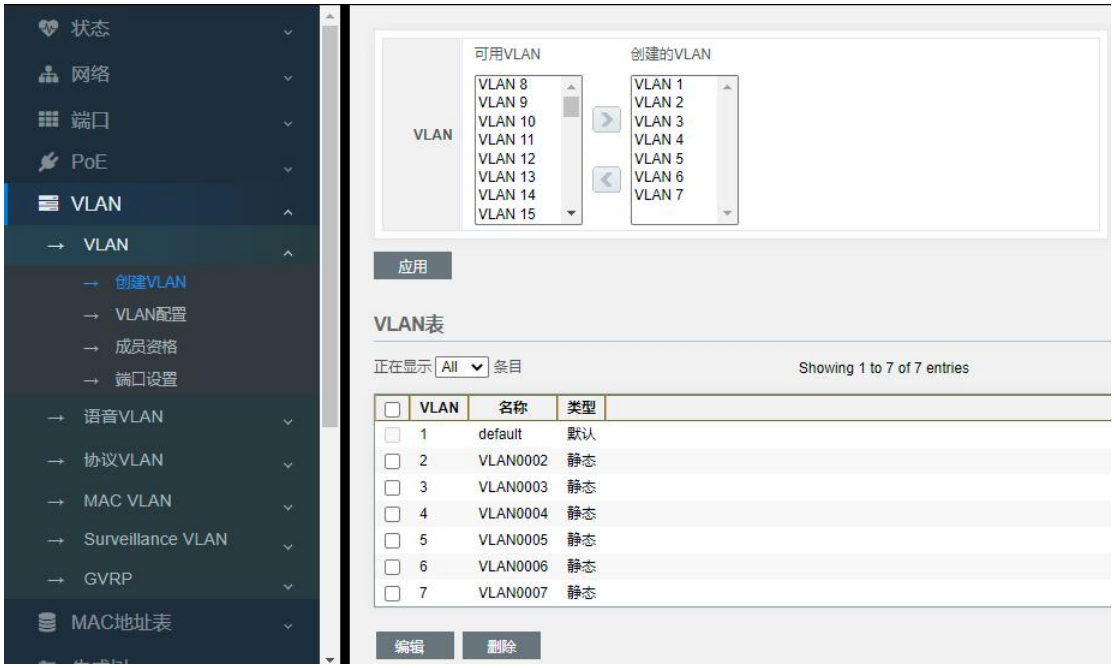


Figure 7-1-2

如上图，这样就添加了VLAN 2~7

7.1.2 VLAN Configuration

配置交换机的802.1Q_VLAN

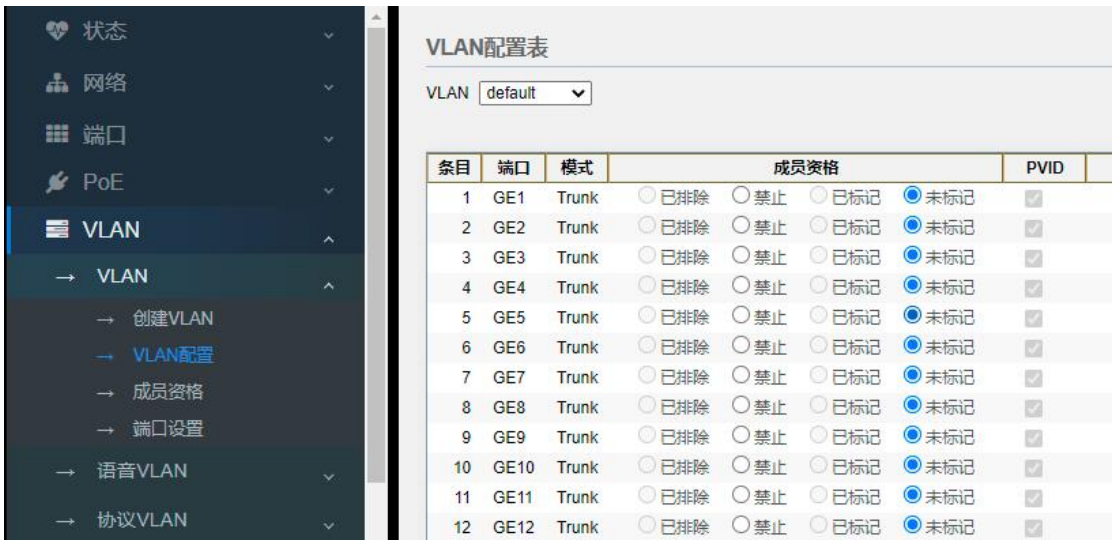


Figure 7-1-3

默认，default就是VLAN 1，可以看见，所有端口都属于VLAN 1，而且都是Untag，也都是PVID=1。

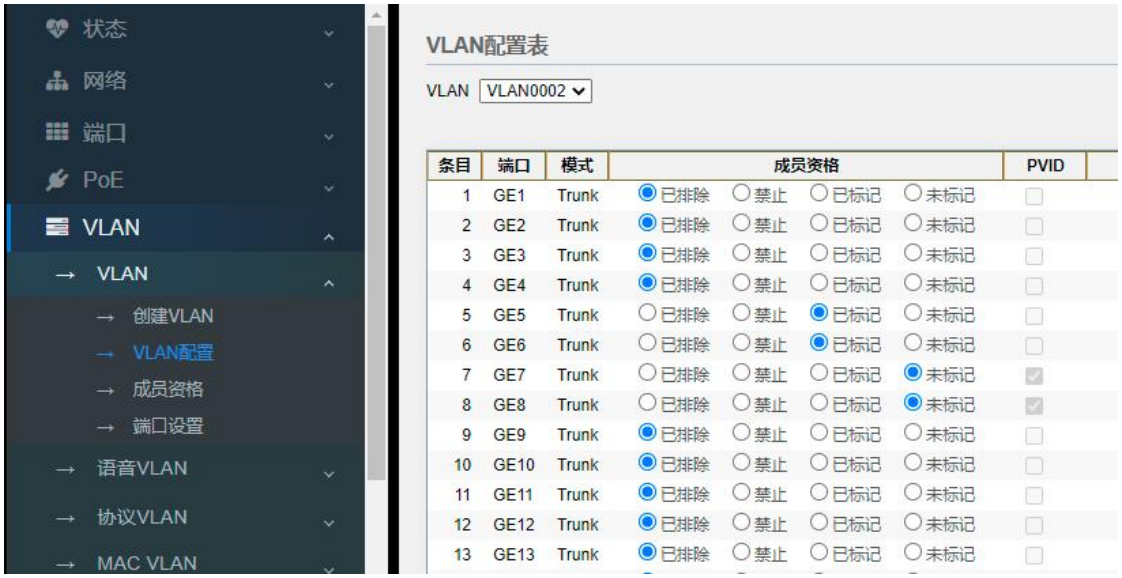
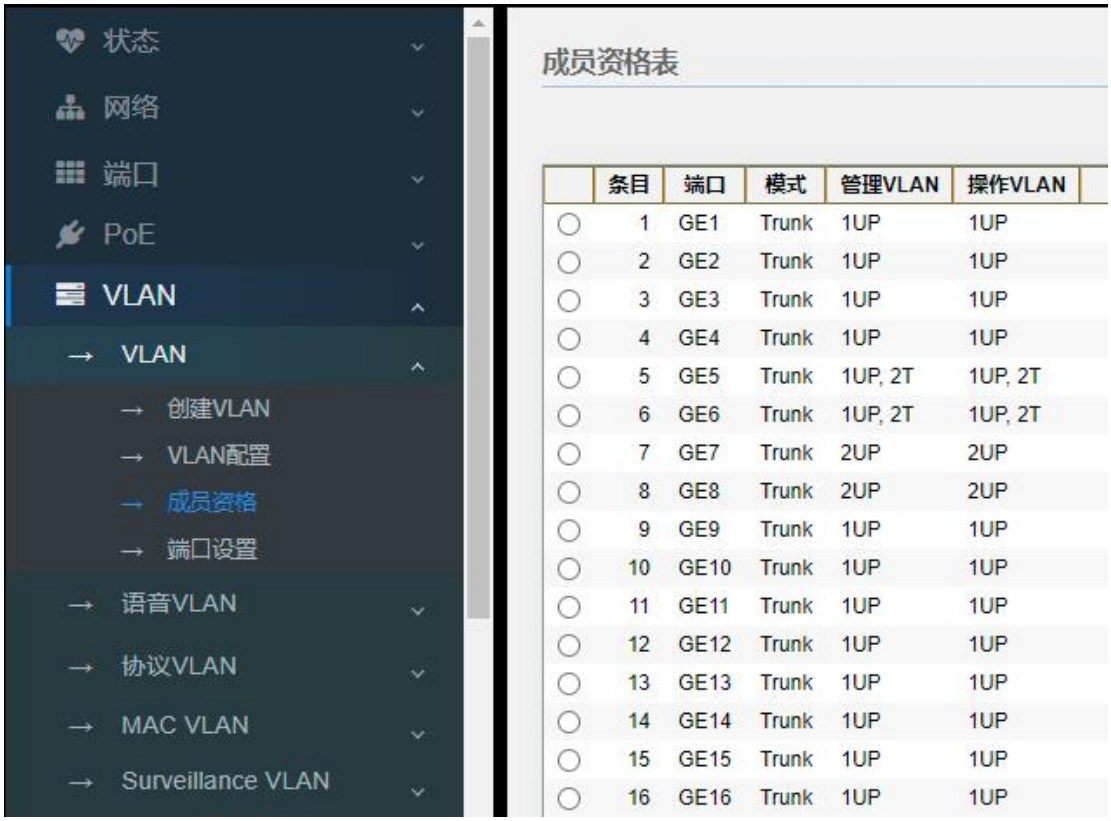


Figure 7-1-4

当选择VLAN 为VLAN 2的时候，默认是没有成员的，可以手动设置。
如上图所示，把5-6口加入VLAN 2的Tagged成员，把7-8口加入VLAN 2的Untagged成员，但是由于端口模式是Trunk，所以如果选择Untaged的时候，就自动把Pvid改成了2。

7.1.3 Membership

查看交换机的的 VLAN 配置



	条目	端口	模式	管理VLAN	操作VLAN
○	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP	1UP
○	3	GE3	Trunk	1UP	1UP
○	4	GE4	Trunk	1UP	1UP
○	5	GE5	Trunk	1UP, 2T	1UP, 2T
○	6	GE6	Trunk	1UP, 2T	1UP, 2T
○	7	GE7	Trunk	2UP	2UP
○	8	GE8	Trunk	2UP	2UP
○	9	GE9	Trunk	1UP	1UP
○	10	GE10	Trunk	1UP	1UP
○	11	GE11	Trunk	1UP	1UP
○	12	GE12	Trunk	1UP	1UP
○	13	GE13	Trunk	1UP	1UP
○	14	GE14	Trunk	1UP	1UP
○	15	GE15	Trunk	1UP	1UP
○	16	GE16	Trunk	1UP	1UP

Figure 7-1-4

如上图，UP就是Pvid值，T就是Tagged，U就是Untaged
GE1 口，Trunk模式，Pvid=1
GE5-6 口，Trunk模式，Pvid=1，Tag-vid=2
GE7-8 口，Trunk模式，Pvid=2

下一节我们来讲端口的VLAN模式

7.1.4 Port Setting

配置端口的模式，及对于入口检测功能，TPID功能的配置。

VLAN模式分3种：Access，Trunk，Hybird
Access：一般都是接终端设备（例如PC，摄像头，机顶盒……），直接设置Pvid就可以了
Trunk：一般是交换机和交换机之间相连的端口，一般是需要设置多个VLAN进行Tagged
Hybrid：称为混合模式，可以对于多个VLAN进行Tagged，也可以对另外多个VLAN进行Untagged

入口检测：
当端口是Hybrid链路的时候，在入口检测的地方，可以只让Tag报文通过，或是Untag报文通过，或是让所有报文通过。
TPID（Tag Protocol Identifier，标签协议标识）VLAN Tag中的一个字段，IEEE 802.1q协议

规定该字段的取值为0x8100。设备缺省采用协议规定的**TPID**值（0x8100），某些厂商将设备可识别的**TPID**值设置为0x9100或其他数值。

为了和这些设备兼容，设备提供了全局的VLAN-VPN报文**TPID**值可调功能，用户可以自行配置**TPID**值。VLAN-VPN Uplink端口在转发报文时会将报文外层VLAN Tag中的**TPID**值替换为用户设定值再进行发送，从而使发送到公网中的VLAN-VPN报文可以被其他厂商的设备识别。

所以这些参数都可以根据客户的需求来进行配置。

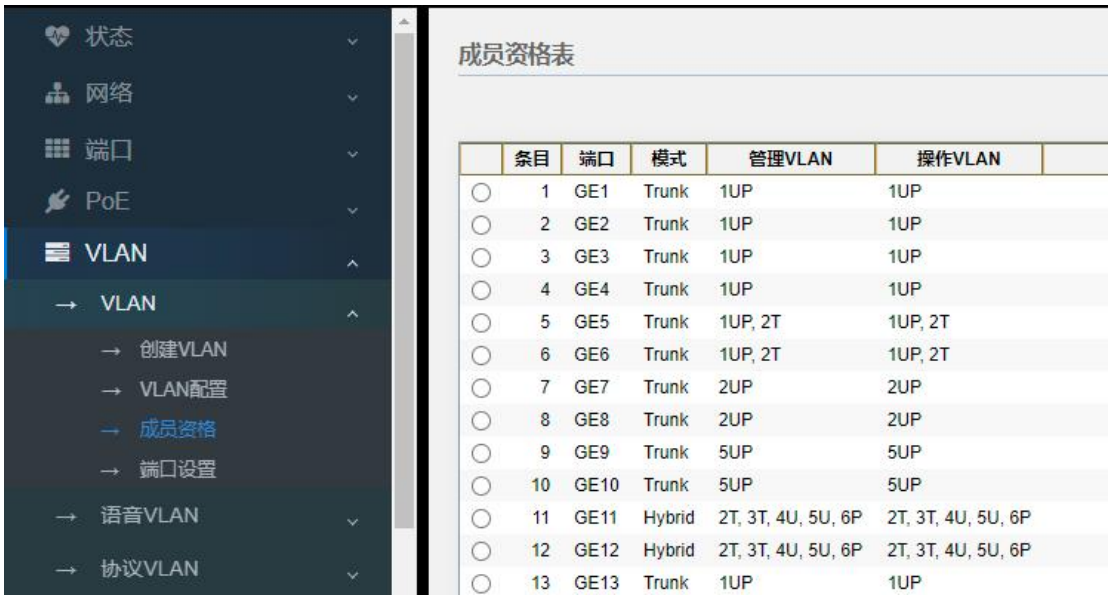
Figure 7-1-5

如上图所示，就把9-10口，同时设置为Access模式，并且PVID值改为5。

Figure 7-1-6

如上图所示，就把11-12口，同时设置为Hybrid模式，并且PVID值改为1，然后再进入成员资

格页面中，配置对于tag-vid=2，3，untag-vid=4，5。



	条目	端口	模式	管理VLAN	操作VLAN
○	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP	1UP
○	3	GE3	Trunk	1UP	1UP
○	4	GE4	Trunk	1UP	1UP
○	5	GE5	Trunk	1UP, 2T	1UP, 2T
○	6	GE6	Trunk	1UP, 2T	1UP, 2T
○	7	GE7	Trunk	2UP	2UP
○	8	GE8	Trunk	2UP	2UP
○	9	GE9	Trunk	5UP	5UP
○	10	GE10	Trunk	5UP	5UP
○	11	GE11	Hybrid	2T, 3T, 4U, 5U, 6P	2T, 3T, 4U, 5U, 6P
○	12	GE12	Hybrid	2T, 3T, 4U, 5U, 6P	2T, 3T, 4U, 5U, 6P
○	13	GE13	Trunk	1UP	1UP

Figure 7-1-7

可以看见，Gi 11-12，是hybrid模式，而且pvid=6，tag-vid=2，3，untag-vid=4，5

注意：
设置PVID值的时候，必须是之前添加了VLAN才能设置，7.1.1章节已经添加了VLAN2-7，所以，可以设置5。但是如果设置9的话，系统会报错，并且设置不成功。

正常情况下，入口检测过滤，一般都不用设置，TPID也不用设置，直接用默认就可以了。

注意：如果需要查看日志信息，可以到“Status-Logging Message”的页面下查看。

第 8 部分:MAC Address Table

MAC 地址简介

MAC 地址表简介

以太网交换机的主要功能是在数据链路层对报文进行转发，也就是根据报文的目的MAC地址将报文输出到相应的端口。MAC地址转发表是一张包含了MAC地址与转发端口对应关系的二层转发表，是以太网交换机实现二层报文快速转发的基础。MAC 地址转发表的表项中包含如下信息：

- 目的MAC 地址
- 端口所属的VLAN ID
- 本设备上的转发出端口编号

以太网交换机在转发报文时，根据MAC 地址表项信息，会采取以下两种转发方式：

- 单播方式：当MAC 地址转发表中包含与报文目的MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送。
- 广播方式：当交换机收到目的地址为全F 的报文，或MAC 地址转发表中没有包含对应报文目的MAC 地址的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。

MAC地址学习过程简介

MAC 地址转发表中的表项可以通过两种方式进行更新和维护：

- 手工配置方式
- MAC 地址学习方式

通常情况下，多数 MAC 地址表项都是通过 MAC 地址学习功能创建和维护的

MAC 地址转发表管理

MAC 地址转发表的老化机制

以太网交换机的MAC 地址转发表是有容量限制的，为了最大限度利用地址转发表资源，以太网交换机利用老化机制更新MAC 地址转发表，即：系统在动态创建某条表项的同时，开启老化定时器，如果在老化时间内没有再次收到来自该表项中的MAC 地址的报文，交换机就会把该MAC 地址表项删除。

MAC 地址表项的分类与特点

根据自身特点和配置方式等的不同，MAC 地址表项可以分为三类：

- 静态MAC 地址表项：也称为“永久地址”，由用户手工添加和删除，不会随着时间老化。对于一个设备变动较小的网络，手工添加静态地址表项可以减少网络中的广播流量。
- 动态MAC 地址表项：指可以按照用户配置的老化时间而老化掉的MAC 地址表项，交换机可以通过MAC 地址学习机制或通过用户手工建立的方式添加动态MAC 地址表项。
- 黑洞MAC 地址表项：也称过滤MAC地址表，由用户手工配置的一类特殊的MAC 地址，当交换机接收到源MAC 地址或目的MAC 地址为黑洞MAC 地址的报文时，会将该报文丢弃。

8.1 Dynamic Address

交换机自动学习到的MAC地址，表项如下图：

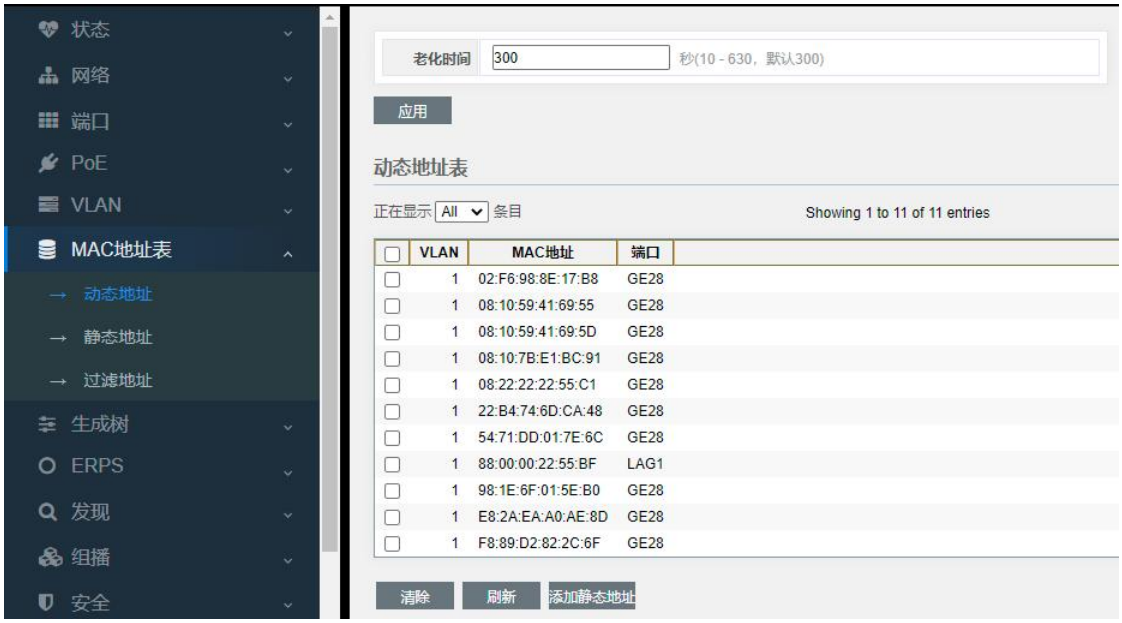


Figure 8-1-1

MAC地址: 端口自动学习到的MAC地址
端口: MAC地址学习到哪个端口上
VLAN ID(1-4094)： MAC地址学习到哪个VLAN上

8.2 Static Address

设置MAC 地址表项

管理员根据实际情况可以人工添加、修改或删除MAC 地址转发表中的表项。可以删除与某个端口相关的所有MAC 地址表项，也可以选择删除某类MAC 地址表项如动态表项、静态表项。

用户可以在页面中添加、删除静态 MAC 地址表项。也称为 MAC 地址绑定，MAC 地址和端口 VLAN 三者进行绑定。

Figure 8-2-1

举例：

手动添加静态MAC地址28:D2:44:80:B2:F0到GE 4口上

1. 点击“Add”，会弹出添加静态MAC地址的对话框
2. 输入需要绑定的MAC地址，VLAN号和端口号
3. 点击 “Apply”

Figure 8-2-2

添加完成后，如下图所示：

Figure 8-2-3

这样绑定配置后的效果是：

1. 这个MAC地址只能在GE 4口上才能通信，如果这个MAC是接在其他端口上，就收不到任何的目的地址是此MAC的报文。因为交换机收到目的地址是绑定的这个MAC地址后，只

会往绑定端口上转发。

2. 静态MAC地址配置后，原来此MAC存在在动态MAC的地址表项就被删除了。

8.3 MAC 地址过滤

本交换机如果设置了MAC地址过滤表项，那么报文中这个MAC地址不管是在源MAC或是目的MAC，只要交换机接收到此类报文，都会被丢弃。

举例：

手动添加过滤 MAC 地址 00:E0:4C:20:C1:C0

1. 点击“Add”，会弹出添加静态MAC地址的对话框
2. 输入需要绑定的MAC地址，VLAN号
3. 点击“Apply”

Figure 8-3-1

MAC地址: 输入需要拒绝的MAC地址

VLAN ID(1-4094): 输入被拒绝的MAC地址所在的VLAN

8.4 MAC 老化时间

用户可以调整动态 MAC 地址表项的老化时间。如果用户配置的老化时间过长，设备可能会保存许多过时的MAC 地址表项，从而耗尽MAC 地址表资源，导致设备无法根据网络的变化更新MAC 地址表。如果用户配置的老化时间太短，设备可能会删除有效的MAC 地址表项，可能导致设备广播大量的数据报文，影响设备的运行性能。所以用户需要根据实际情况，配置合适的老化时间来有效的实现MAC 地址老化功能。

figure 8-4-1

默认是 300 秒，如需要改变，输入老化时间值并点击“确定”

动态 MAC 地址表的老化时间作用于全部端口上，地址老化只对动态的（设备学习到的或者用户配置的动态的）MAC 地址表项起作用。

第 9 部分: Spanning Tree

9.1 STP 简介

9.1.1 STP 的用途

STP（Spanning Tree Protocol，生成树协议）是根据IEEE 协会制定的802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文造成的报文处理能力下降的问题发生。

STP 包含了两个含义，狭义的STP 是指IEEE 802.1D 中定义的STP 协议，广义的STP 是指包括

IEEE 802.1D 定义的STP 协议以及各种在它的基础上经过改进的生成树协议。

9.1.2 STP 的协议报文

STP 采用的协议报文是BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息。
STP 通过在设备之间传递BPDU 来确定网络的拓扑结构。BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。

BPDU 在STP 协议中分为两类：

- 配置BPDU（Configuration BPDU）：用来进行生成树计算和维护生成树拓扑的报文。
- TCN BPDU（Topology Change Notification BPDU）：当拓扑结构发生变化时，用来通知相

关设备网络拓扑结构发生变化的报文。

9.1.3 STP 的基本概念

(1) 根桥

树形的网络结构，必须要有树根，于是STP 引入了根桥（Root Bridge）的概念。

根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。

网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置BPDU，其他的设备对该配置BPDU进行转发，从而保证拓扑的稳定。

(2) 根端口

所谓根端口，是指一个非根桥的设备上离根桥最近的端口。根端口负责与根桥进行通信。非根桥设备上有且只有一个根端口。根桥上没有根端口。

(3) 指定桥与指定端口

指定桥与指定端口的含义，请参见表1-1的说明。

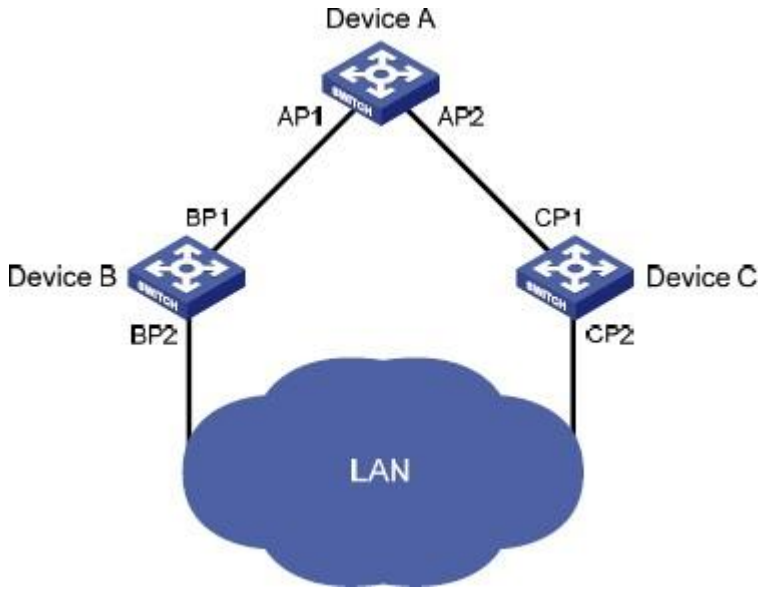
表1-1 指定桥与指定端口的含义

分类	指定桥	指定端口
对于一台设备而言	与本机直接相连并且负责向本机转发配置消息的设备	指定桥向本机转发配置消息的端口
对于一个局域网而言	负责向本网段转发配置消息的设备	指定桥向本网段转发配置消息的端口

指定桥与指定端口如图1-1所示，AP1、AP2、BP1、BP2、CP1、CP2 分别表示设备Device A、Device B、Device C的端口。

- Device A 通过端口AP1 向Device B 转发配置消息，则Device B 的指定桥就是Device A，指定端口就是Device A 的端口AP1；
- 与局域网LAN 相连的有两台设备：Device B 和Device C，如果Device B 负责向LAN转发配置消息，则LAN 的指定桥就是Device B，指定端口就是Device B 的BP2。

图1-1 指定桥与指定端口示意图



(4) 路径开销

路径开销是STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

9.1.4 STP 的基本原理

STP 通过在设备之间传递BPDU 来确定网络的拓扑结构。配置消息中包含了足够的信息来保证设备完成生成树的计算过程，其中包含的几个重要信息如下：

- 根桥ID：由根桥的优先级和MAC 地址组成；
- 根路径开销：到根桥的路径开销；
- 指定桥ID：由指定桥的优先级和MAC 地址组成；
- 指定端口ID：由指定端口的优先级和端口名称组成；
- 配置消息在网络中传播的生存期：Message Age；
- 配置消息在设备中能够保存的最大生存期：Max Age；
- 配置消息发送的周期：Hello Time；
- 端口状态迁移的延时：Forward Delay。

(1) STP 算法实现的具体过程

- 初始状态

各台设备的各个端口在初始时会生成以自己为根桥的配置消息，根路径开销为0，指定桥ID 为自身设备ID，指定端口为本端口。

- 最优配置消息的选择

各台设备都向外发送自己的配置消息，同时也会收到其他设备发送的配置消息。

最优配置消息的选择过程如表1-2所示。

表1-2 最优配置消息的选择过程

步骤	内容
1	每个端口收到配置消息后的处理过程如下： ● 当端口收到的配置消息比本端口配置消息的优先级低时，设备会将接收到的配置消息丢弃，对该端口的配置消息不作任何处理。 ● 当端口收到的配置消息比本端口配置消息的优先级高时，设备就用接收到的配置消息中的内容替换该端口的配置消息中的内容。
2	设备将所有端口的配置消息进行比较，选出最优的配置消息。

● 根桥的选择

网络初始化时，网络中所有的STP 设备都认为自己是“根桥”，根桥ID 为自身的设备ID。通过交换配置消息，设备之间比较根桥ID，网络中根桥ID 最小的设备被选为根桥。

● 根端口、指定端口的选择

根端口、指定端口的选择过程如表1-3所示。

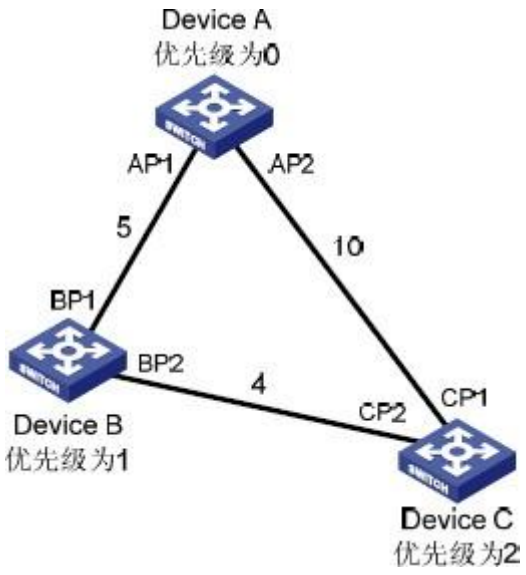
表1-3 根端口和指定端口的选择过程

步骤	内容
1	非根桥设备将接收最优配置消息的那个端口定为根端口
2	设备根据根端口的配置消息和根端口的路径开销，为每个端口计算一个指定端口配置消息： ● 根桥ID 替换为根端口的配置消息的根桥ID； ● 根路径开销替换为根端口配置消息的根路径开销加上根端口对应的路径开销； ● 指定桥ID 替换为自身设备的ID； ● 指定端口ID 替换为自身端口ID。
3	设备使用计算出来的配置消息和需要确定端口角色的端口上的配置消息进行比较，并根据比较结果进行不同的处理： ● 如果计算出来的配置消息优，则设备就将该端口定为指定端口，端口上的配置消息被计算出来的配置消息替换，并周期性向外发送； ● 如果端口上的配置消息优，则设备不更新该端口的配置消息并将此端口阻塞，此端口将不再转发数据，只接收但不发送配置消息。

一旦根桥、根端口、指定端口选举成功，则整个树形拓扑就建立完毕了。

下面结合例子说明STP算法实现的计算过程。具体的组网如图1-2所示，Device A的优先级为0，Device B的优先级为1，Device C的优先级为2，各个链路的路径开销分别为5、10、4。

图1-2 STP 算法计算过程组网图



- 各台设备的初始状态

各台设备的初始状态如表1-4所示。

表1-4 各台设备的初始状态

设备	端口名称	端口的配置消息
Device A	AP1	{0，0，0，AP1}
	AP2	{0，0，0，AP2}
Device B	BP1	{1，0，1，BP1}
	BP2	{1，0，1，BP2}
Device C	CP1	{2，0，2，CP1}
	CP2	{2，0，2，CP2}

- 各台设备的比较过程及结果

各台设备的比较过程及结果如表1-5所示。

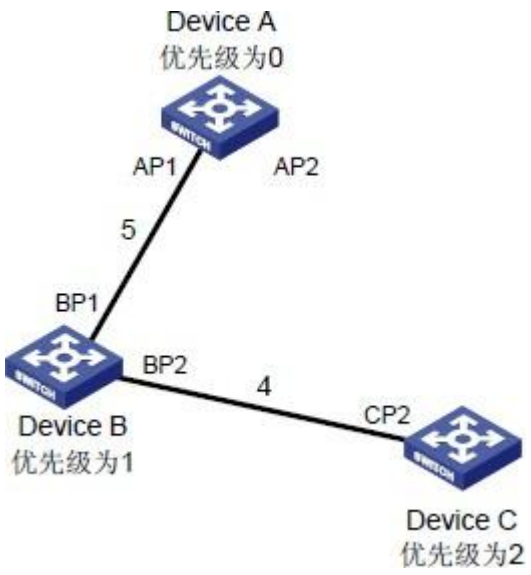
表1-5 各台设备的比较过程及结果

设备	比较过程	比较后端口的配置消息
Device A	● 端口AP1 收到Device B 的配置消息{1，0，1，BP1}，Device A 发现本端口的配置消息{0，0，0，AP1}优于接收到的配置消息，就把接收到的配置消息丢弃。 ● 端口AP2 收到Device C 的配置消息{2，0，2，CP1}，Device A 发现本端口的配置消息{0，0，0，AP2}优于接收到的配置消息，就把接收到的配置消息丢弃。 ● Device A 发现自己各个端口的配置消息中根桥和指定桥都是自己，则认为自己是根桥，各个端口的配置消息都不作任何修改，以后周期性的向外发送配置消息。	AP1：{0，0，0，AP1} AP2：{0，0，0，AP2}

Device B	● 端口BP1 收到来自Device A 的配置消息{0，0，0，AP1}，Device B 发现接收到的配置消息优于本端口的配置消息{1，0，1，BP1}，于是更新端口BP1的配置消息。 ● 端口BP2 收到来自Device C 的配置消息{2，0，2，CP2}，Device B 发现本端口的配置消息{1，0，1，BP2}优于接收到的配置消息，就把接收到的配置消息丢弃。	BP1：{0，0，0，AP1} BP2：{1，0，1，BP2}
	● Device B 对各个端口的配置消息进行比较，选出端口BP1 的配置消息为最优配置消息，然后将端口BP1 定为根端口，它的配置消息不作改变。 ● Device B 根据根端口BP1 的配置消息和根端口的路径开销5，为BP2 端口计算一个指定端口配置消息{0，5，1，BP2}。 ● Device B 使用计算出来的配置消息{0，5，1，BP2}和端口BP2 上的配置消息进行比较，比较的结果是计算出来的配置消息较优，则Device B 将端口BP2 定为指定端口，它的配置消息被计算出来的配置消息替换，并周期性向外发送。	根端口BP1： {0，0，0，AP1} 指定端口 BP2： {0，5，1，BP2}
Device C	● 端口CP1 收到来自Device A 的配置消息{0，0，0，AP2}，Device C 发现接收到的配置消息优于本端口的配置消息{2，0，2，CP1}，于是更新端口CP1的配置消息。 ● 端口CP2 收到来自Device B 端口BP2 更新前的配置消息{1，0，1，BP2}，Device C 发现接收到的配置消息优于本端口的配置消息{2，0，2，CP2}，于是更新端口CP2 的配置消息。	CP1：{0，0，0，AP2} CP2：{1，0，1，BP2}
	经过比较： ● 端口CP1 的配置消息被选为最优的配置消息，端口CP1 就被定为根端口，它的配置消息不作改变。 ● 将计算出来的指定端口配置消息{0，10，2，CP2}和端口CP2 的配置消息进行比较后，端口CP2 转为指定端口，它的配置消息被计算出来的配置消息替换。	根端口CP1： {0，0，0，AP2} 指定端口CP2： {0，10，2，CP2}
	● 接着端口CP2 会收到Device B 更新后的配置消息{0，5，1，BP2}，由于收到的配置消息比原配置消息优，则Device C 触发更新过程。 ● 同时端口CP1 收到Device A 周期性发送来的配置消息，比较后Device C 不会触发更新过程。	CP1：{0，0，0，AP2} CP2：{0，5，1，BP2}
	经过比较： ● 端口CP2 的根路径开销9（配置消息的根路径开销5+端口CP2 对应的路径开销4）小于端口CP1 的根路径开销10（配置消息的根路径开销0+端口CP1对应的路径开销10），所以端口CP2 的配置消息被选为最优的配置消息，端口CP2 就被定为根端口，它的配置消息就不作改变。 ● 将端口CP1 的配置消息和计算出来的指定端口配置消息比较后，端口CP1被阻塞，端口配置消息不变，同时不接收从Device A 转发的数据，直到新的情况触发生成树的计算，比如从Device B 到Device C 的链路down 掉。	阻塞端口CP1： {0，0，0，AP2} 根端口CP2： {0，5，1，BP2}

经过上表的比较过程，此时以Device A为根桥的生成树就确定下来了，形状如图1-3所示。

图1-3 计算得到的生成树



(2) STP 的配置消息传递机制

- 当网络初始化时，所有的设备都将自己作为根桥，生成以自己为根的配置消息，并以Hello Time为周期定时向外发送。
- 接收到配置消息的端口如果是根端口，且接收的配置消息比该端口的配置消息优，则设备将配置消息中携带的Message Age 按照一定的原则递增，并启动定时器为这条配置消息计时，同时将此配置消息从设备的指定端口转发出去。
- 如果指定端口收到的配置消息比本端口的配置消息优先级低时，会立刻发出自己的更好的配置消息进行回应。
- 如果某条路径发生故障，则这条路径上的根端口不会再收到新的配置消息，旧的配置消息将会因为超时而被丢弃，设备重新生成以自己为根的配置消息并向外发送，从而引发生成树的重新计算，得到一条新的通路替代发生故障的链路，恢复网络连通性。

不过，重新计算得到的新配置消息不会立刻就传遍整个网络，因此旧的根端口和指定端口由于没有发现网络拓扑变化，将仍按原来的路径继续转发数据。如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。

(3) STP 定时器

STP 计算中，需要使用三个重要的时间参数：Forward Delay、Hello Time 和Max Age。

- Forward Delay 为设备状态迁移的延迟时间。链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新配置消息无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的环路。为此，STP 采用了一种状态迁移的机制，新选出的根端口和指定端口要经过2 倍的Forward Delay延时后才能进入转发状态，这个延时保证了新的配置消息已经传遍整个网络。
- Hello Time 用于设备检测链路是否存在故障。设备每隔Hello Time 时间会向周围的设备发送hello 报文，以确认链路是否存在故障。
- Max Age 是用来判断配置消息在设备内保存时间是否“过时”的参数，设备会将过时的配置消息丢弃。

9.2 MSTP 简介

9.2.1 MSTP 产生的背景

(1) STP、RSTP 存在的不足

STP 不能快速迁移，即使是在点对点链路或边缘端口（边缘端口指的是该端口直接与用户终端相连，而没有连接到其它设备或共享网段上），也必须等待2 倍的Forward Delay 的时间延迟，端口才能迁移到转发状态。

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是STP 协议的优化版。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

- RSTP 中，根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。
- RSTP 中，指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

RSTP 可以快速收敛，但是和STP 一样存在以下缺陷：局域网内所有网桥共享一棵生成树，不能按VLAN 阻塞冗余链路，所有VLAN 的报文都沿着一棵生成树进行转发。

(2) MSTP 的特点

MSTP（Multiple Spanning Tree Protocol，多生成树协议）可以弥补STP 和RSTP 的缺陷，它既可以快速收敛，也能使不同VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。关于VLAN 的介绍，请参见“接入分册”中的“VLAN 配置”。

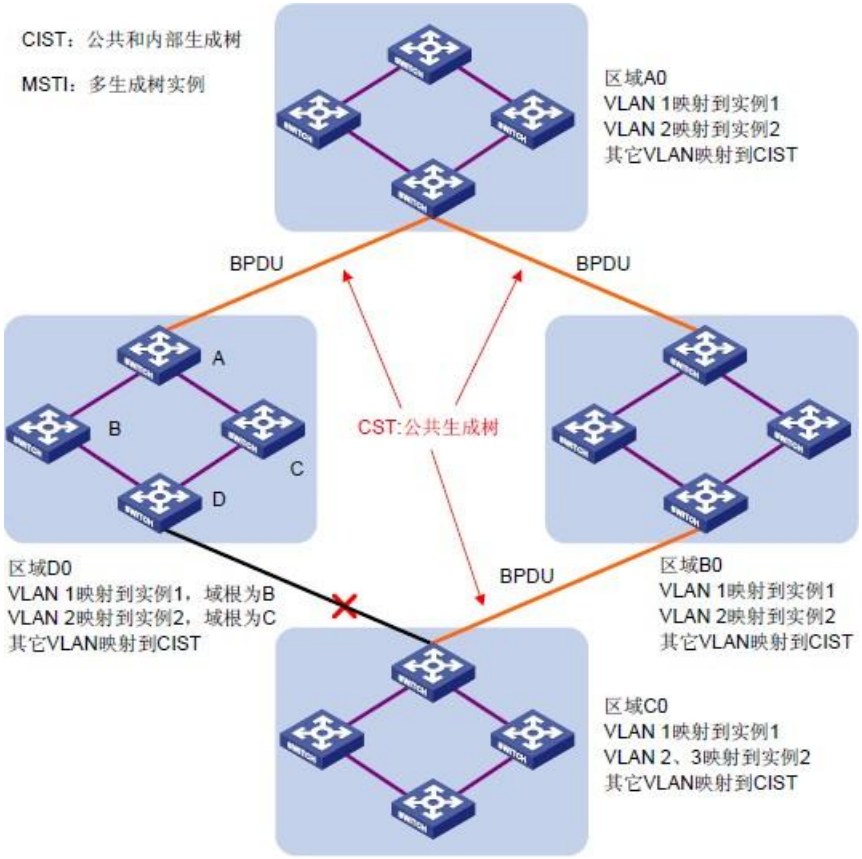
MSTP 的特点如下：

- MSTP 设置VLAN 映射表（即VLAN 和生成树的对应关系表），把VLAN 和生成树联系起来。通过增加“实例”（将多个VLAN 整合到一个集合中）这个概念，将多个VLAN 捆绑到一个实例中，以节省通信开销和资源占用率。
- 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。
- MSTP 将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现VLAN 数据的负载分担。
- MSTP 兼容STP 和RSTP。

9.2.2 MSTP 的基本概念

在图1-4中的每台设备都运行MSTP。下面将结合图形解释MSTP的一些基本概念。

图1-4 MSTP 的基本概念示意图



(1) MST 域

MST 域（Multiple Spanning Tree Regions，多生成树域）是由交换网络中的多台设备以及它们之间的网段所构成。这些设备具有下列特点：

- 都启动了MSTP；
- 具有相同的域名；
- 具有相同的VLAN 到生成树实例映射配置；
- 具有相同的MSTP 修订级别配置；
- 这些设备之间在物理上有链路连通。

例如图1-4中的区域A0，域内所有设备都有相同的MST域配置：

- 域名相同；
- VLAN 与生成树实例的映射关系相同（VLAN 1 映射到生成树实例1，VLAN 2 映射到生成树实例2，其余VLAN 映射到CIST。其中，CIST 即指生成树实例0）；
- 相同的MSTP 修订级别（此配置在图中没有体现）。

一个交换网络可以存在多个MST 域。用户可以通过MSTP 配置命令把多台设备划分在同一个MST域内。

(2) VLAN 映射表

VLAN 映射表是MST 域的一个属性，用来描述VLAN 和生成树实例的映射关系。
例如图1-4中，域A0 的VLAN映射表就是：VLAN 1 映射到生成树实例1，VLAN 2 映射到生成树实例2，其余VLAN映射到CIST。MSTP就是根据VLAN映射表来实现负载分担的。

(3) IST
IST（Internal Spanning Tree，内部生成树）是MST 域内的一棵生成树。
IST 和CST（Common Spanning Tree，公共生成树）共同构成整个交换网络的生成树CIST（Common and Internal Spanning Tree，公共和内部生成树）。IST 是CIST 在MST 域内的片段。
例如图1-4中CIST在每个MST域内都有一个片段，这个片段就是各个域内的IST。

(4) CST
CST 是连接交换网络内所有MST 域的单生成树。如果把每个MST 域看作是一个“设备”，CST就是这些“设备”通过STP 协议、RSTP 协议计算生成的一棵生成树。

例如图1-4中红色线条描绘的就是CST。

(5) CIST
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。
例如图1-4中，每个MST域内的IST加上MST域间的CST就构成整个网络的CIST。

(6) 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。每棵生成树都称为一个MSTI（Multiple Spanning Tree Instance，多生成树实例）。

例如图1-4中，每个域内可以存在多棵生成树，每棵生成树和相应的VLAN对应。这些生成树就被称为MSTI。

(7) 域根
MST 域内IST 和MSTI 的根桥就是域根。MST 域内各棵生成树的拓扑不同，域根也可能不同。

例如图1-4中，区域D0 中，生成树实例1 的域根为设备B，生成树实例2 的域根为设备C。

(8) 总根
总根（Common Root Bridge）是指CIST 的根桥。
例如图1-4中，总根为区域A0 内的某台设备。

(9) 域边界端口
域边界端口是指位于MST 域的边缘，用于连接不同MST 域、MST 域和运行STP 的区域、MST 域和运行RSTP 的区域的端口。

例如图1-4中，如果区域A0 的一台设备和区域D0 的一台设备的第一个端口相连，整个交

换网络的总根位于A0 内，则区域D0 中这台设备上的第一个端口就是区域D0 的域边界端口。域边界端口在生成树实例上的角色与CIST 的角色保持一致，但是Master 端口除外，Master 端口在CIST 上的角色为ROOT 端口，但是在其他实例上的角色才为Master 端口。

(10) 端口角色

在MSTP 的计算过程中，端口角色主要有根端口、指定端口、Master 端口、Alternate 端口、Backup端口等。

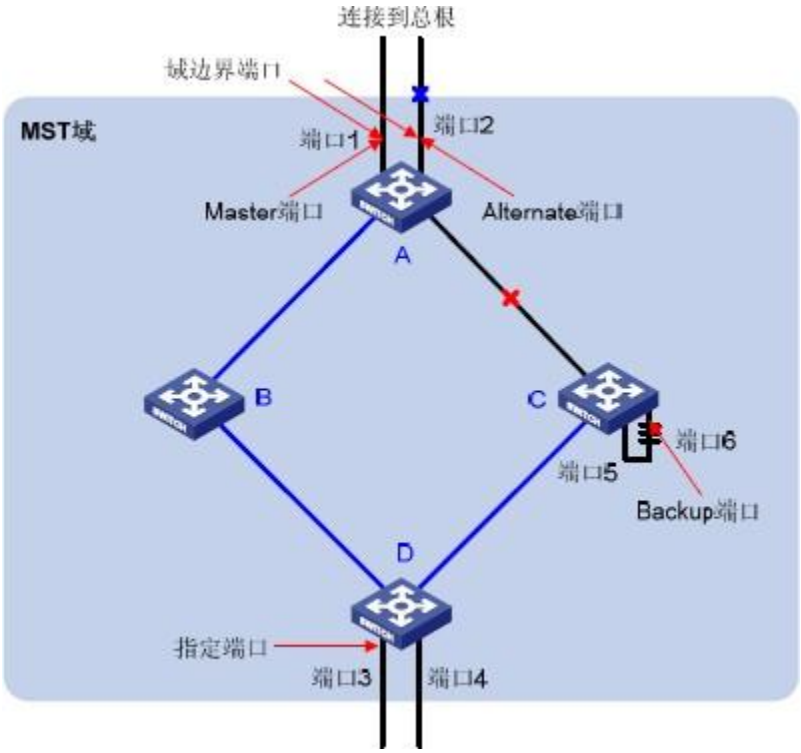
- 根端口：负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master 端口：连接MST 域到总根的端口，位于整个域到总根的最短路径上。从CST 上看，Master 端口就是域的“根端口”（把域看作是一个节点）。Master 端口在IST/CIST 上的角色是根端口，在其它各个实例上的角色都是Master 端口。
- Alternate 端口：根端口和Master 端口的备份端口。当根端口或Master 端口被阻塞后，Alternate端口将成为新的根端口或Master 端口。
- Backup 端口：指定端口的备份端口。当指定端口被阻塞后，Backup 端口就会快速转换为新的指定端口，并无时延的转发数据。当开启了MSTP 的同一台设备的两个端口互相连接时就存在一个环路，此时设备会将其中一个端口阻塞，Backup 端口是被阻塞的那个端口。

端口在不同的生成树实例中可以担任不同的角色。

请参考图1-5理解上述概念。图中：

- 设备A、B、C、D 构成一个MST 域。
- 设备A 的端口1、端口2 向总根方向连接。
- 设备C 的端口5、端口6 构成了环路。
- 设备D 的端口3、端口4 向下连接其他的MST 域。

图1-5 端口角色示意图



(11) 端口状态

MSTP 中，根据端口是否学习MAC 地址和是否转发用户流量，可将端口状态划分为以下三种：

- Forwarding 状态：学习MAC 地址，转发用户流量；
- Learning 状态：学习MAC 地址，不转发用户流量；
- Discarding 状态：不学习MAC 地址，不转发用户流量。

端口状态和端口角色是没有必然联系的，表1-6给出了各种端口角色能够具有的端口状态（“√”表示此端口角色能够具有此端口状态；“--”表示此端口角色不能具有此端口状态）。

表1-6 各种端口角色具有的端口状态

端口角色 端口状态	根端口/Master 端口	指定端口	Alternate 端口	Backup 端口
Forwarding	√	√	--	--
Learning	√	√	--	--
Discarding	√	√	√	√

9.2.3 MSTP 的基本原理

MSTP 将整个二层网络划分为多个MST 域，各个域之间通过计算生成CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。其中实例0 被称为

IST，其他的多生成树实例为MSTI。MSTP 同STP 一样，使用配置消息进行生成树的计算，只是配置消息中携带的是设备上MSTP 的配置信息。

(1) CIST 生成树的计算
通过比较配置消息后，在整个网络中选择一个优先级最高的设备作为CIST 的根桥。在每个MST 域内MSTP 通过计算生成IST；同时MSTP 将每个MST 域作为单台设备对待，通过计算在域间生成CST。CST 和IST 构成了整个网络的CIST。

(2) MSTI 的计算
在MST域内，MSTP根据VLAN和生成树实例的映射关系，针对不同的VLAN生成不同的生成树实例。每棵生成树独立进行计算，计算过程与STP计算生成树的过程类似，请参见“1.1.1 4. STP的基本原理”。

MSTP 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。

9.2.4 MSTP 在设备上的实现

MSTP 同时兼容STP、RSTP。STP、RSTP 两种协议报文都可以被运行MSTP 的设备识别并应用于生成树计算。

设备除了提供MSTP 的基本功能外，还从用户的角度出发，提供了许多便于管理的特殊功能，如下所示：
- 根桥保持；
- 根桥备份；
- 根保护功能；
- BPDU 保护功能；
- 环路保护功能；
- 防止TC-BPDU 报文攻击功能。

9.3 协议规范

相关的协议规范有：
- IEEE 802.1D：Spanning Tree Protocol
- IEEE 802.1w：Rapid Spanning Tree Protocol
- IEEE 802.1s：Multiple Spanning Tree Protocol

9.4 Property

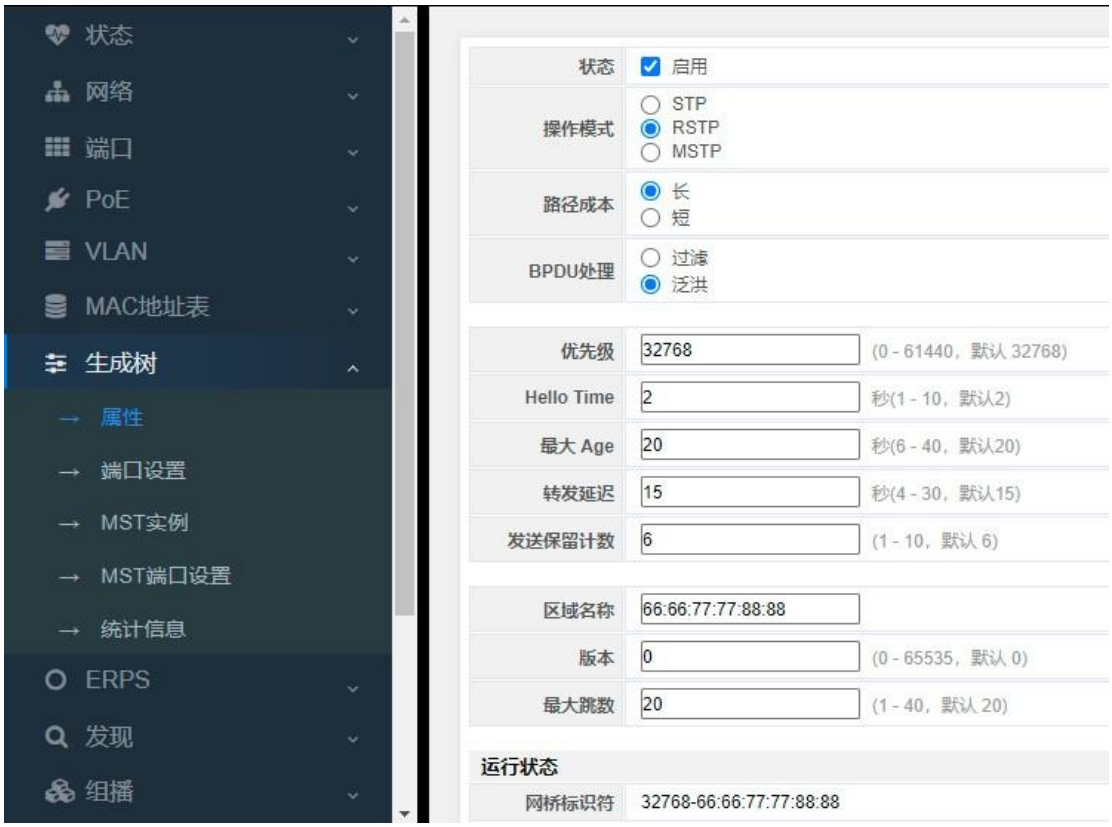


figure 9-4-1

State：Enable（交换机全局的Spanning Tree配置，勾选的话为开启，未勾选为关闭）
Operation Mode：STP/RSTP/MSTP （三种模式的选择）
Path Cost：Long/Short （取值范围为短整型（short：1～65535）（long：1～200000000））
BPDU Handling：Filtering/Flooding (对BPDU报文过滤处理或是泛洪处理)
Priority：配置交换机的优先级，取值范围为0到61440，按4096的倍数递增，缺省值为32768。
Hello Time：配置交换机定时发送 BPDU 报文的时间间隔。缺省值为 2 秒。
Max-Age Time：配置 BPDU 报文消息生存的最长时间。缺省值为 20 秒。
Forward-Delay Time：配置端口状态改变的时间间隔。缺省值为 15 秒。
Tx-Hold-Count：配置每秒种最多发送的BPDU个数，缺省值为3个。

9.5 Port Setting

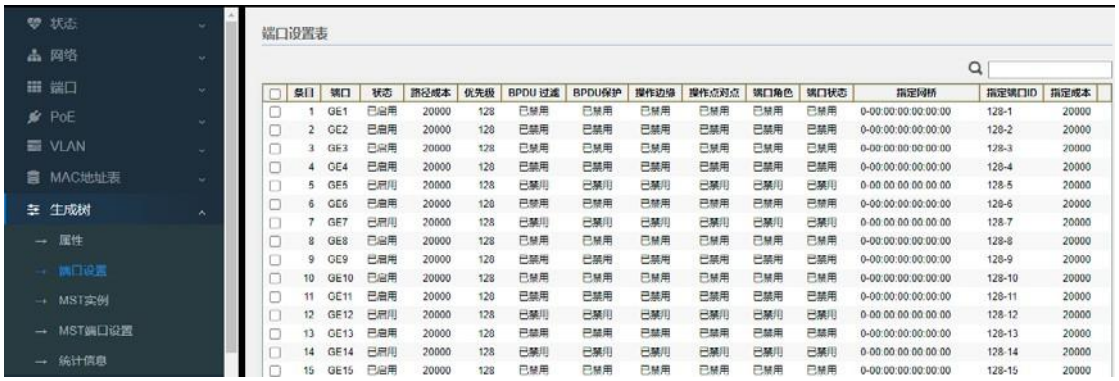


figure 9-5-1

State：Enable（交换机端口的Spanning Tree配置，勾选的话为开启，未勾选为关闭）
Path Cost：Long/Short （取值范围为短整型（short：1～65535）（long：1～200000000））
Priority：配置交换机端口的优先级，取值范围为0到240。
Edge Port：配置为边缘端口的端口在 UP 的时候就可以直接将端口的状态变为 forwading 状态
BPDU Filter：端口上配置 BPDU 过滤后，该接口上将不再发送和接收 BPDU 报文。
BPDU Guard：端口上配置 BPDU Guard 后，一旦在某指定接口接收到本不应存在的 BPDU 包，直接将该接口断掉，使其呈现为软关闭 err-disabled 状态。相较于过滤，该方法防护手段更加强硬。
Point-to-Point：端口半双工是 share 类型模式，全双工是 point-to-point 类型，只有在 point-to-point 链路上才能实现快速转换。也可以强制设置 Enable/Disable 来决定端口的连接是不是“point-to-point”。

9.6 MST Instance

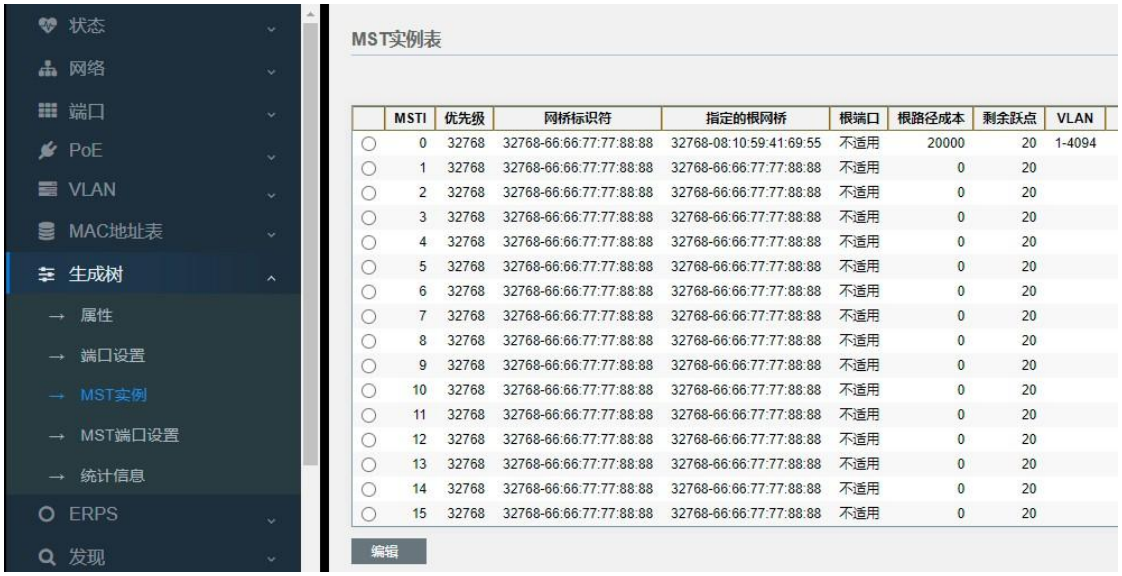


figure 9-6-1

在MST域内， MSTP根据VLAN和生成树实例的映射关系， 针对不同的VLAN生成不同的生成树实例。每棵生成树独立进行计算，计算过程与STP计算生成树的过程类似。总共有16个实例。

MSTI的0的实例，默认是配置了VLAN1-4094
例如要配置MSTI的1的实例，就需要配置哪些VLAN在这个域内。

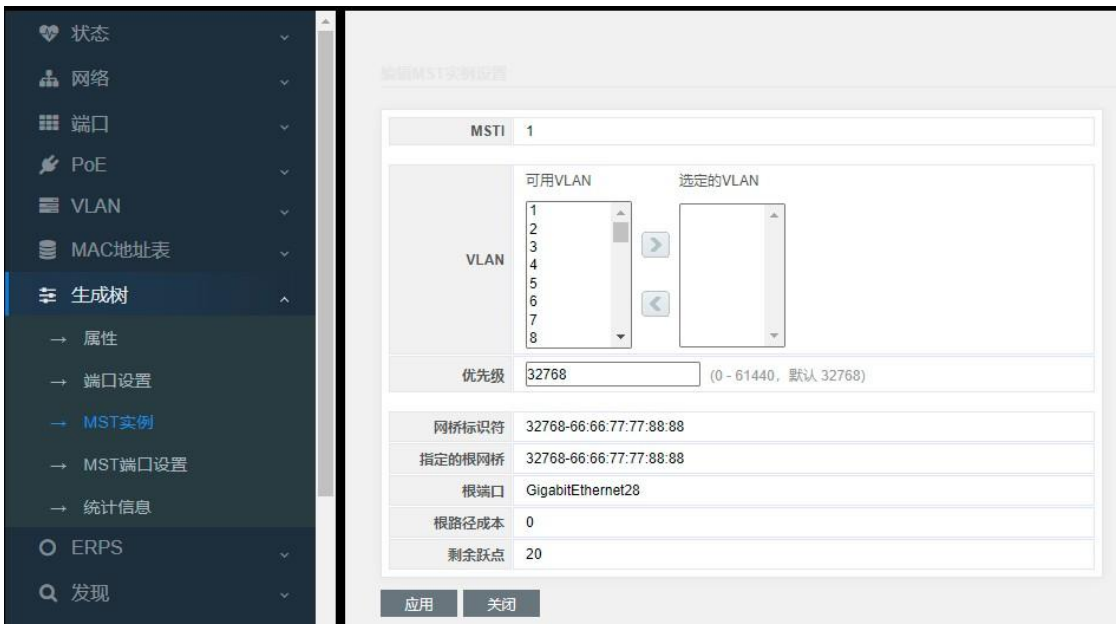


figure 9-6-2

9.7 MST Port Setting

有环路情况时，MSTP在选择一个接口放入转发状态时需要用到端口的优先级。您可以给要优先选择的端口指定较高的优先级值（低数值），给要备用选择的端口低优先级值（高数值）。如果所有端口都相同的优先级值，MSTP选择端口号小的为转发端口并阻断其他接口。

条目	端口	路径成本	优先级	端口角色	端口状态	模式	类型	指定网桥	指定端口ID	指定成本	剩余跃点
1	GE1	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-1	20000	20
2	GE2	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-2	20000	20
3	GE3	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-3	20000	20
4	GE4	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-4	20000	20
5	GE5	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-5	20000	20
6	GE6	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-6	20000	20
7	GE7	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-7	20000	20
8	GE8	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-8	20000	20
9	GE9	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-9	20000	20
10	GE10	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-10	20000	20
11	GE11	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-11	20000	20
12	GE12	20000	128	已禁用	已禁用	RSTP	边界	0-00:00:00:00:00:00	128-12	20000	20

figure 9-7-1

可以设置端口的Path Cost和Priority，也可以采用默认值。

9.8 Statistics

条目	端口	接收BPDU			传输BPDU		
		配置	TCN	MSTP	配置	TCN	MSTP
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0

figure 9-8-1

主要统计交换机接收和发送生成树的报文数量。

第 12 部分: Security

12.4 Management Access

12.4.1 Management VLAN

管理VLAN的意思就是，端口所在的VLAN，才能和交换机的cpu通信，才能管理交换机系统。默认就是VLAN1的成员端口可以管理交换机。

Figure 12-4-1

可以根据用户需求，任意选择VLAN几可以管理交换机系统，前提是，选择的VLAN是需要先被建立的。

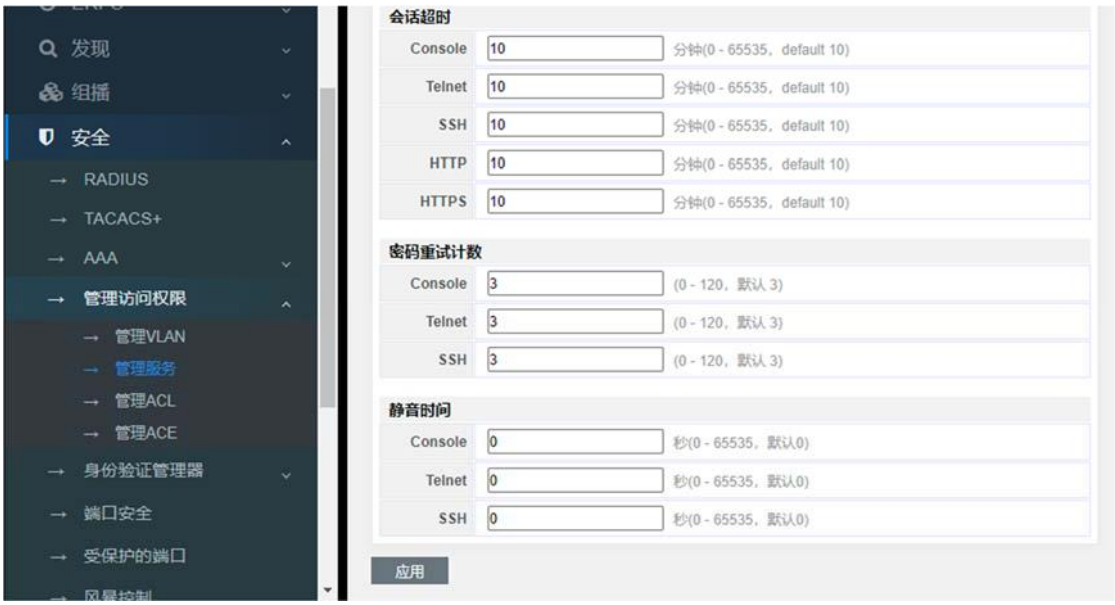
举例：

1. 先在VLAN中，把VLAN添加了，例如VLAN100
2. 把端口5加入到VLAN100
3. 把管理VLAN设置成VLAN100
4. 把pc连接到5口，这样pc就可以管理交换机了。

12.4.2 Management Service

Figure 12-4-2

Management Service：管理服务，可以根据用户的需要，选择支持哪些对于交换机的管理。
默认，只是开启了HTTP和SNMP的服务。
如果还需要Tlenet，SSH，HTTPS服务，需要手动开启。



Session Timeout：会话超时时间，例如登陆网页后，10秒钟没有任何操作，系统会自动退出网页。需要用户重新输入用户名，密码登陆才可以继续管理交换机。

如果觉得时间太短，可以根据自己的需求，改这个时间。

Password Retry Count：密码重试次数，如果输错密码超过设置的次数，就会让用户等待一段时间后，再重新输入密码，以防暴力破解。

12.10 Dynamic ARP Inspection

Dynamic ARP Inspection 功能介绍
用户可以通过配置 Dynamic ARP Inspection 功能，简称DAI。对于合法用户的ARP 报文进行正常转发，否则丢弃。DAI包含两个功能：用户合法性检查功能和ARP 报文有效性检查功能。
1. 用户合法性检查
用户合法性检查是根据 ARP 报文中源IP 地址和源MAC 地址检查用户是否是所属VLAN 所在端口上的合法用户，包括基于DHCP Snooping 安全表项的检查、基于802.1X 安全表项的检查和基于静态IP 和MAC 绑定表项的检查。用户可以任意选择使能哪些功能，各功能可以共存。
(1) 基于DHCP Snooping 安全表项的检查。主要针对仿冒用户的攻击。对于ARP 非信任

端口，打开DHCP Snooping 安全表项检查模式且所属VLAN 使能了DAI 功能，从该端口上接收的ARP 报文需进行DHCP Snooping 安全表项检查。如果查找到对应的表项，并且均与表项记录一致（IP 地址，MAC 地址，端口索引，VLAN ID 等）则检查通过，否则如果参数不一致或者没有查找到对应的表项，则认为是攻击报文，检查不通过。对于信任端口，不进行DHCP Snooping 安全表项检查。对于没有使能DAI 的VLAN，即使在ARP 非信任端口上，也不进行DHCP Snooping 安全表项检查。

(2)对于ARP 非信任端口，打开802.1X安全表项检查模式且所属VLAN 使能了DAI功能，从该端口上接收的ARP 报文需进行802.1X 安全表项检查。对于源IP 地址＋源MAC 地址＋端口索引＋VLAN ID 都一致或源IP地址不存在但源MAC 地址为OUI MAC 地址的情况，认为是合法报文检查通过；否则认为是攻击报文进行丢弃处理。

(3) 基于静态IP 和MAC 绑定表项的检查。主要针对仿冒网关的攻击。不论对于ARP 非信任端口，还是信任端口，只要打开静态IP 和MAC 绑定表项检查模式且所属VLAN 使能了DAI 功能后，从该端口上送的ARP 报文需进行基于静态IP 和MAC 绑定表项检查。对于源IP 存在绑定关系但是MAC 地址不符的ARP 报文，设备认为是非法报文进行丢弃处理；对于源IP 不存在绑定关系和源IP 存在绑定关系且MAC 地址相符的ARP 报文，设备认为是合法报文，检查通过。

2. ARP 报文有效性检查

对于 ARP 信任端口，不进行报文有效性检查；对于ARP 非信任端口，需要根据配置对MAC 地址和IP 地址不合法的报文进行过滤。可以选择配置源MAC 地址、目的MAC 地址或IP 地址检查模式。

(1) 对于源MAC地址的检查模式，会检查ARP 报文中的源MAC地址和以太网报文头中的源MAC地址是否一致，一致认为有效，否则丢弃；

(2) 对于目的MAC 地址的检查模式（只针对ARP 应答报文），会检查ARP 应答报文中的目的MAC 地址是否为全0 或者全1，是否和以太网报文头中的目的MAC 地址一致。全0、全1、不一致的报文都是无效的，无效的报文需要被丢弃；

(3) 对于IP 地址检查模式，会检查ARP 报文中的源IP 和目的IP 地址，全0、全1、或者组播IP地址都是不合法的，需要丢弃。对于ARP 应答报文，源IP 和目的IP 地址都进行检查；对于ARP 请求报文，只检查源IP 地址。

12.10.1 Property

Figure 12-10-1

如果要配置DAI，并且让功能生效：

1. 勾选enable按键
2. 把相关的VLAN加入到Selected VLAN中
3. 点击Apply，使之生效

Figure 12-10-2

如图12-10-2所示

就是开启了DAI的功能，并且在VLAN1下是生效的。

Figure 12-10-3

配置端口的属性：

Trust：信任端口，不做ARP报文的有效性检查。

Source MAC Address：启用源MAC地址的检查模式。

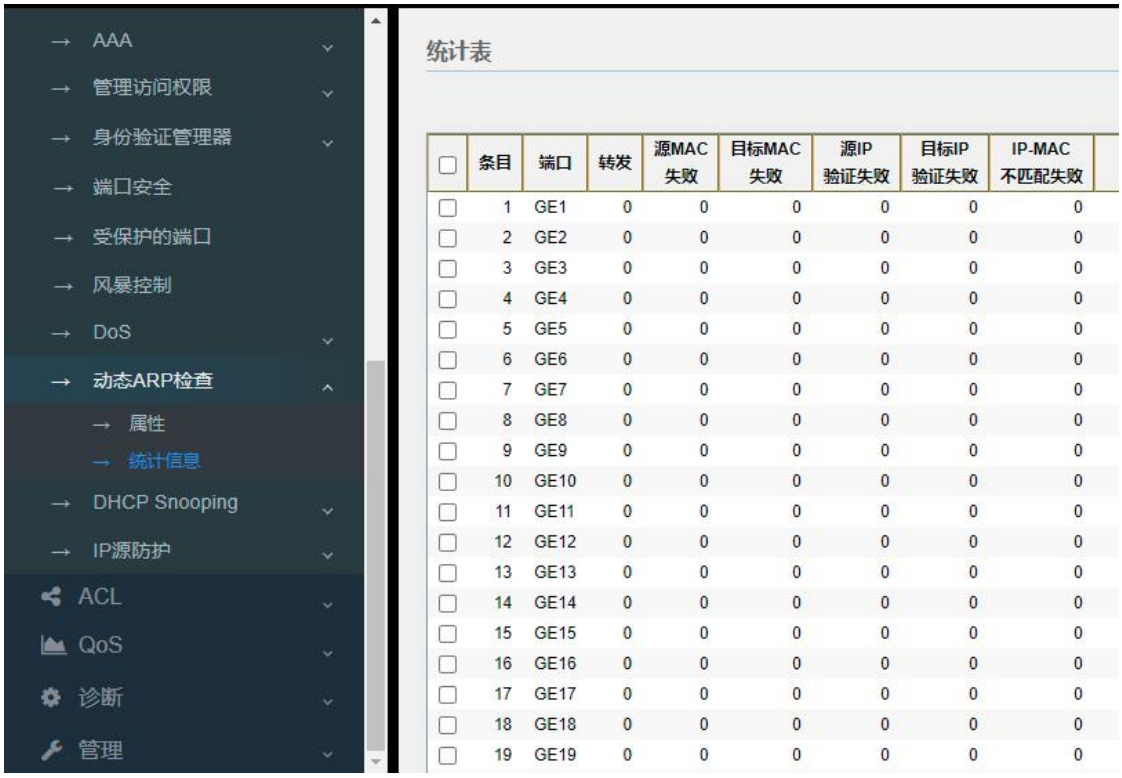
Destination MAC Address：启用目的MAC地址的检查模式。

IP Address：启用IP地址检查模式。

Rate Limit：对于此端口下的ARP报文进行限速。

如图12-10-3所示

12.10.2 Statistics



条目	端口	转发	源MAC失败	目标MAC失败	源IP验证失败	目标IP验证失败	IP-MAC不匹配失败
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0
14	GE14	0	0	0	0	0	0
15	GE15	0	0	0	0	0	0
16	GE16	0	0	0	0	0	0
17	GE17	0	0	0	0	0	0
18	GE18	0	0	0	0	0	0
19	GE19	0	0	0	0	0	0

Figure 12-10-4

端口的ARP报文相关的次数统计。包括转发的统计，验证的统计。
如图12-10-4所示

12.11 DHCP Snooping

DHCP Snooping 简介
DHCP Snooping 作用：
DHCP Snooping 是DHCP 的一种安全特性，具有如下功能：
(1) 记录DHCP 客户端IP 地址与MAC 地址的对应关系；
(2) 保证客户端从合法的服务器获取IP 地址。

1. 记录DHCP 客户端IP 地址与MAC 地址的对应关系
出于安全性的考虑，网络管理员可能需要记录用户上网时所用的 IP 地址，确认用户从DHCP 服务器获取的IP 地址和用户主机MAC 地址的对应关系。DHCP Snooping 可以实现该功能。DHCP Snooping 通过监听DHCP-REQUEST和信任端口收到的DHCP-ACK广播报文，记录DHCP客户端的MAC 地址以及获取到的IP 地址。管理员可以网页上查看DHCP 客户端获取的IP 地址信息。

2. 保证客户端从合法的服务器获取IP 地址
在网络中如果有私自架设的 DHCP 服务器，则可能导致用户得到错误的IP 地址。为了使用户能通过合法的DHCP 服务器获取IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文，从而保证了DHCP 客户端能够从DHCP 服务器获取IP 地址。
- 不信任端口接收到 DHCP 服务器响应的DHCP-ACK 和DHCP-OFFER 报文后，丢弃该报文，从而防止了DHCP 客户端获得错误的IP 地址。

信任端口的典型应用环境
1. 与DHCP 服务器直接或间接相连
与 DHCP 服务器直接或间接相连的端口需要配置为信任端口，以便DHCP Snooping 设备正常转发DHCP 服务器的应答报文，保证DHCP 客户端能够从合法的DHCP 服务器获取IP 地址。

如图 12-11-1 所示，Switch B 的接口 Ethernet1/0/1 与 DHCP 服务器 Switch A 相连，接口Ethernet1/0/1 需要配置为信任端口，使其能够转发 DHCP 服务器 Switch A 回复的应答报文。

图12-11-1 与DHCP 服务器直接或间接相连

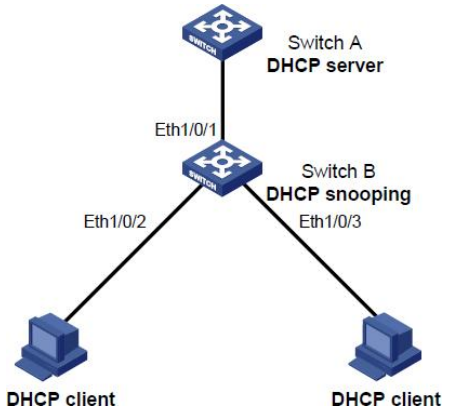


Figure 12-11-1

2. DHCP Snooping 级联网络

在多个 DHCP Snooping 设备级联的网络中，与其他DHCP Snooping 设备相连的端口需要配置为信任端口。

在这种网络环境中，为了节省系统资源，不需要每台DHCP Snooping 设备都记录所有DHCP 客户端的IP 地址和MAC 地址绑定，只需在与客户端直接相连的DHCP Snooping 设备上记录绑定信息。

通过将间接与DHCP 客户端相连的信任端口配置为不记录IP 地址和MAC 地址绑定，可以实现该功能。如果DHCP 客户端发送的请求报文从此类信任端口到达DHCP Snooping 设备，DHCPSnooping 设备不会记录客户端IP 地址和MAC 地址的绑定。

如 图12-11-2所示，Switch A、Switch B和Switch C作为DHCP Snooping设备，Switch A的接口Ethernet1/0/2 、Ethernet1/0/3 ， Switch B 的接口Ethernet1/0/1 、Ethernet1/0/2和Switch C的Ethernet1/0/2、Ethernet1/0/3、Ethernet1/0/4 配置为信任端口；为了避免在所有设备上都记录DHCP客户端IP地址和MAC地址的绑定，可以将Switch A的接口Ethernet1/0/3 、Switch B的接口Ethernet1/0/1 和Switch C的Ethernet1/0/3、Ethernet1/0/4配置为不记录绑定信息的信任端口。

图12-11-2 DHCP Snooping 级联组网图

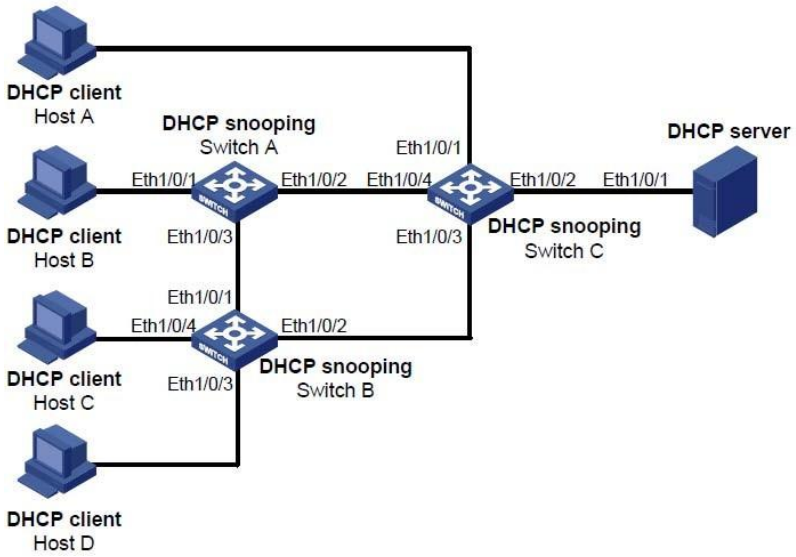


Figure 12-11-2

DHCP Snooping 支持Option 82 功能
Option 82 记录了DHCP客户端的位置信息。管理员可以利用该选项定位DHCP客户端，实现对客户端的安全和计费等控制。
如果DHCP Snooping支持Option 82 功能，则当设备接收到DHCP请求报文后，将根据报文中是否包含Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给DHCP服务器。

当设备接收到 DHCP 服务器的响应报文时，如果报文中含有Option 82，则删除Option 82，并转发给DHCP 客户端；如果报文中不含有Option 82，则直接转发。

12.11.1 Property

Figure 12-11-3

如果要配置DHCP Snooping，并且让功能生效：
1. 勾选enable按键
2. 把相关的VLAN加入到Selected VLAN中
3. 点击Apply，使之生效

Figure 12-11-4

如图12-11-4所示

就是开启了DHCP Snooping功能，并且在VLAN1下是生效的。

Figure 12-11-5

配置端口的属性：

Trust：信任端口，DHCP-ACK 和DHCP-OFFER报文不做有效性检查。

Verify Chaddr：启用IP+MAC+Port+VLAN有效性检查。

Rate Limit：对于此端口下的DHCP报文进行限速。

如图12-11-5所示

Figure 12-11-6

例如，如图所示：

1口接DHCP Server设备，所以需要开启Trust

7口接PC设备，开启Verify Chaddr，会进行报文有效性检查，并且限速100pps

这样DHCP Snooping生效，保证了网络使用的安全性。

如图12-11-6所示

12.11.2 Statistics

条目	端口	转发	Chaddr 检查丢弃	不信任端口丢弃	不信任端口带Option82丢弃	无效的丢弃
1	GE1	0	0	0	0	0
2	GE2	0	0	0	0	0
3	GE3	0	0	0	0	0
4	GE4	0	0	0	0	0
5	GE5	0	0	0	0	0
6	GE6	0	0	0	0	0
7	GE7	0	0	0	0	0
8	GE8	0	0	0	0	0
9	GE9	0	0	0	0	0
10	GE10	0	0	0	0	0
11	GE11	0	0	0	0	0
12	GE12	0	0	0	0	0
13	GE13	0	0	0	0	0
14	GE14	0	0	0	0	0
15	GE15	0	0	0	0	0
16	GE16	0	0	0	0	0
17	GE17	0	0	0	0	0
18	GE18	0	0	0	0	0

Figure 12-11-7

端口的DHCP报文相关的次数统计。包括转发的统计，丢弃的统计。
如图12-11-7所示

12.11.3 Option82 Property

Option 82 称为中继代理信息选项，该选项记录了DHCP 客户端的位置信息。DHCP 中继或DHCPSnooping设备接收到DHCP客户端发送给DHCP服务器的请求报文后，在该报文中添加Option 82，并转发给DHCP 服务器。

管理员可以从 Option 82 中获得DHCP 客户端的位置信息，以便定位DHCP 客户端，实现对客户端的安全和计费等控制。支持Option 82 的服务器还可以根据该选项的信息制定IP 地址和其他参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含255 个子选项。若定义了Option 82，则至少要定义一个子选项。目前设备只支持两个子选项：sub-option 1（Circuit ID，电路ID 子选项）和sub-option 2（Remote ID，远程ID 子选项）。

由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。
设备上，可以通过两种方式配置 Option 82 的内容：

- 用户自定义方式：用户手工指定 Option 82 的内容；
- 非用户自定义方式：采用默认的 normal 模式或verbose 模式填充Option 82。

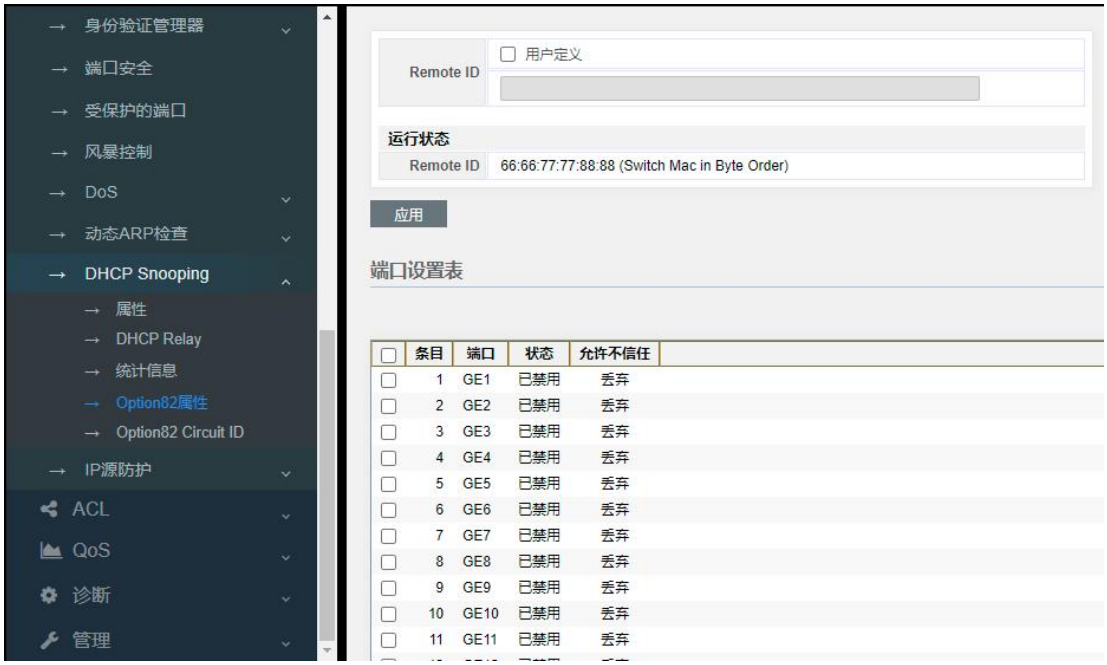


Figure 12-11-8

Remote ID可以自定义，也可以采用默认，默认就是交换机的MAC地址作为Remote ID。
如图12-11-7所示

Figure 12-11-9

收到的报文中带有 Option 82，处理策略有3种：Drop、Keep、Replace

Drop：丢弃报文

Keep：保持报文中的Option 82不变并进行转发

Replace：采用填充Option82方式，替换报文中原有的Option 82并进行转发

如图12-11-8所示

12.11.4 Option82 Circuit ID

Figure 12-11-10

配置Circuit ID，点击Add，如图12-11-9所示

Figure 12-11-11

需要选择端口号，VLAN号，手动添加Circuit ID就可以了。

12.12 IP Source Guard

IP Source Guard 简介

通过 IP Source Guard 绑定功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，提高了端口的安全性。端口接收到报文后查找IP Source Guard 绑定表项，如果报文中的特征项与绑定表项中记录的特征项匹配，则端口转发该报文，否则做丢弃处理。

IP Source Guard 支持的报文特征项包括：源IP 地址、源MAC 地址。并且，可支持端口与如下特征项的组合（下文简称绑定表项）：

- IP
- IP＋MAC

该特性提供两种触发绑定的机制：一种是通过手工配置方式提供绑定表项，称为静态绑定；另外一种由DHCP Snooping 提供绑定表项，称为动态绑定。而且，绑定是针对端口的，一个端口被绑定后，仅该端口被限制，其他端口不受该绑定影响。

12.12.1 Port Setting

Figure 12-12-1

Figure 12-12-2

配置IP Source Guard的端口属性，选择端口号，开启，然后选择报文特征项IP或是选择IP-MAC。建议选择IP-MAC，安全性更高一些。

12.12.2 IMPV Binding

Figure 12-12-2

查看DHCP获取的地址，同时也可以手动添加绑定条目。

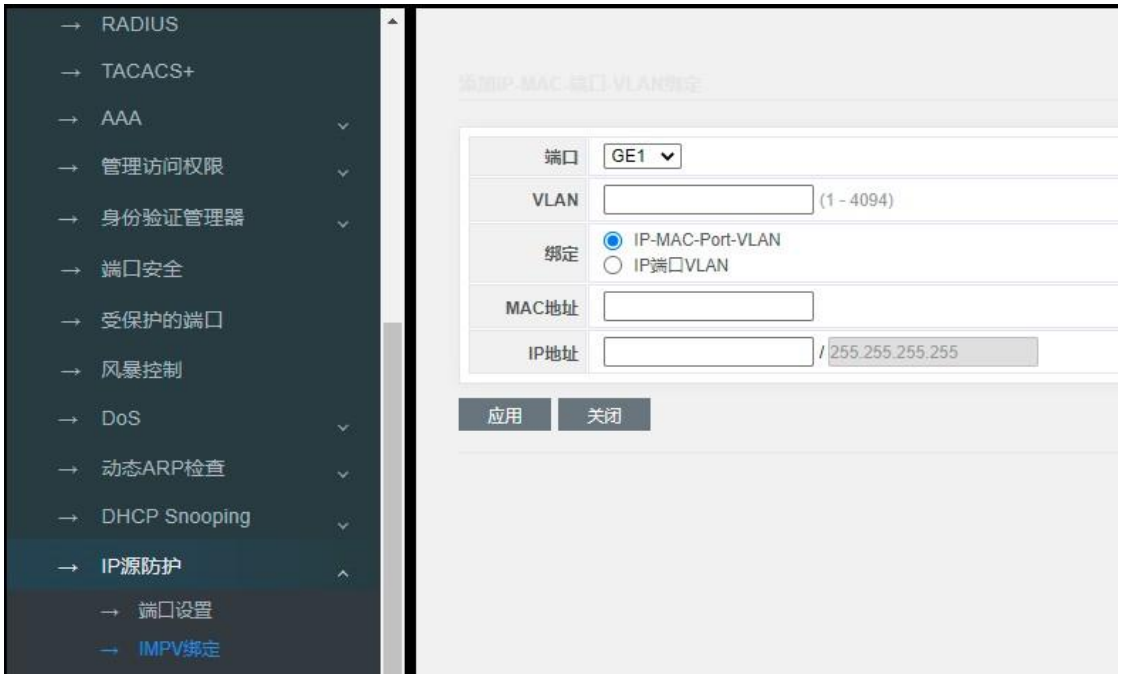


Figure 12-12-3

添加绑定条目，需要选择端口，VLAN号，绑定的模式，然后填写绑定的MAC地址和IP地址。

12.12.3 Save Database

Figure 12-12-4

保存的就是IMPV Binding的数据，可以选择不保存，也可以选择保存到flash中或是通过TFTP保存到服务器中。

第 15 部分: Diagnostics

15.1 Logging

15.1.1 Property

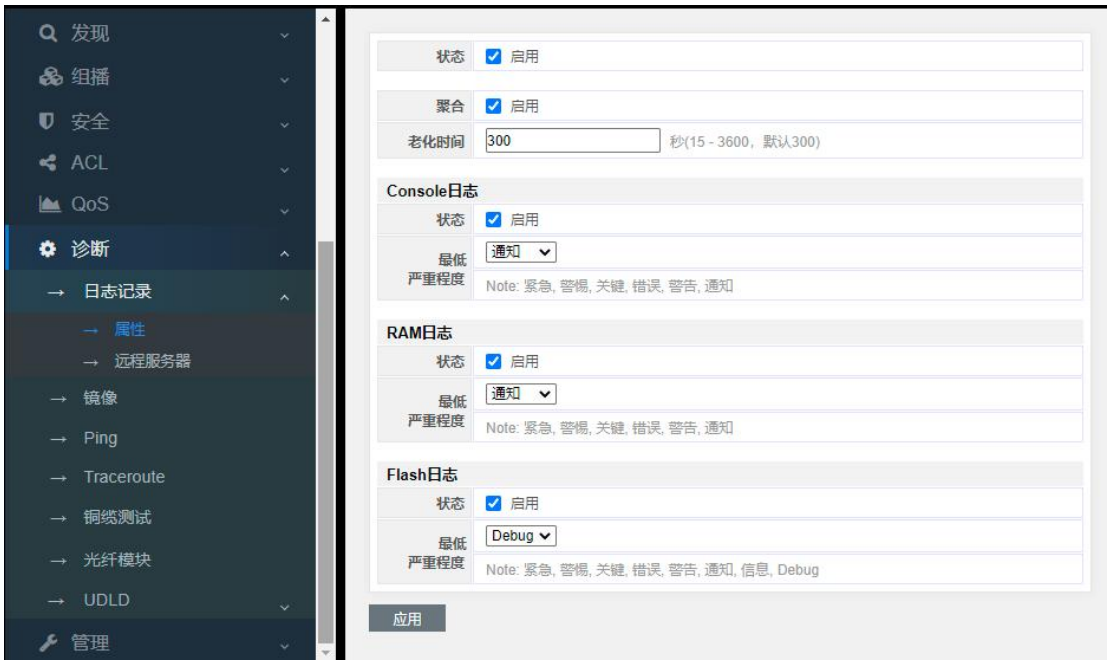


Figure 15-1-1

State：日志记录的信息，开启/关闭
Aggregation：日志信息的条目是否合并显示，开启/关闭
Aging Time：多长时间更新日志信息，默认是300秒

Console Logging：把日志信息显示在串口上
RAM Logging：把日志信息显示在RAM上
Flash Logging：把日志信息显示在Flash上
Minimum Severity：日志级别，分为8种: Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug

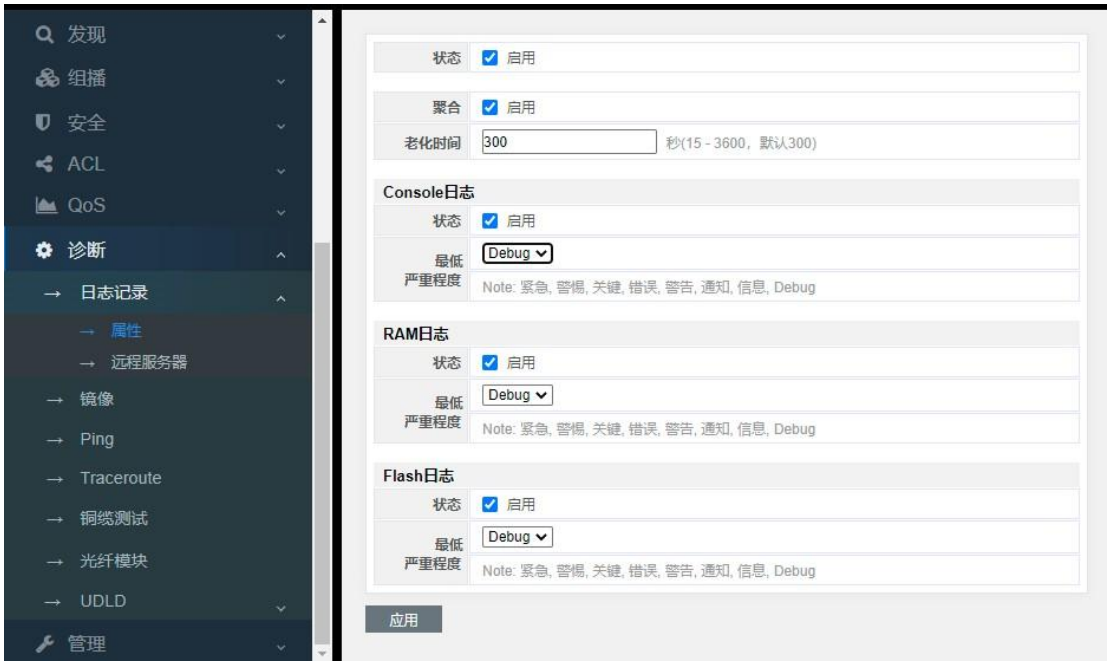


Figure 15-1-2

这样配置把日志的显示，比较全面的覆盖了，可以参考。

15.2 Mirroring

镜像的话，一共支持4个镜像会话。

流量捕获设置:
捕获状态: 设置端口镜像功能的开启/关闭状态
捕获端口: 选择捕获端口，即把被捕获的端口报文镜像到此端口
被捕获端口：此端口的进入的报文，或是出去的报文，或是进出的全部报文都可以进行捕获

Figure 15-2-1

选择一个镜像会话，点击“Edit”

Figure 15-2-2

State：需要勾选Enable

Monitor Port：选择把哪些端口的报文镜像到这个端口上

注意，勾选“Send or Receive Normal Packet”，是为了配置完成后，这个端口连接的PC，可以管控交换机。如果不勾选，那么此端口将不能访问、管控交换机了。

Ingress Port：进入此端口的报文

Egress Port：从此端口出去的报文

如上图示例：
把GE2口的入口报文镜像到GE15口
把GE3口的出口报文镜像到GE15口
把GE5口的进、出报文镜像到GE15口

Figure 15-2-3

查看镜像配置的具体情况。

15.3 Ping

PING （Packet Internet Groper），因特网包探索器，用于测试网络连接量的程序。Ping是工作在 TCP/IP网络体系结构中应用层的一个服务命令， 主要是向特定的目的主机发送 ICMP Echo 请求报文，测试目的站是否可达及了解其有关状态 。

ping用于确定本地主机是否能与另一台主机成功交换(发送与接收)数据包，再根据返回的信息，就可以推断TCP/IP参数是否设置正确，以及运行是否正常、网络是否通畅等

Figure 15-3-1

Address Type：Hostname，IPv4，IPv6
Service Address：这需要输入要ping的目的地址
Count：这个是连续ping多少个报文，默认是4个，也可以手动输入ping多少个报文。

Ping Result
Status：成功或是失败
Transmit Packet：发送了多少个ping报文
Receive Packet：接收了多少个ping报文
Packet Lost：通过发送，接收的报文的数据，统计出报文丢失的百分比。

15.4 Traceroute

Traceroute命令利用ICMP 协议定位终端设备和目标终端设备之间的所有路由器。TTL 值可以反映数据包经过的路由器或网关的数量，通过操纵独立ICMP 呼叫报文的TTL 值和观察该报文被抛弃的返回信息，traceroute命令能够遍历到数据包传输路径上的所有路由器。

程序利用增加存活时间（TTL）值来实现其功能。每当数据包经过一个路由器，其存活时间就会减1。当其存活时间是0时，主机便取消数据包，并传送一个ICMP TTL数据包给原数据包的发出者。
程序发出的首3个数据包TTL值是1，之后3个是2，如此类推，它便得到一连串数据包路径。注意IP不保证每个数据包走的路径都一样。

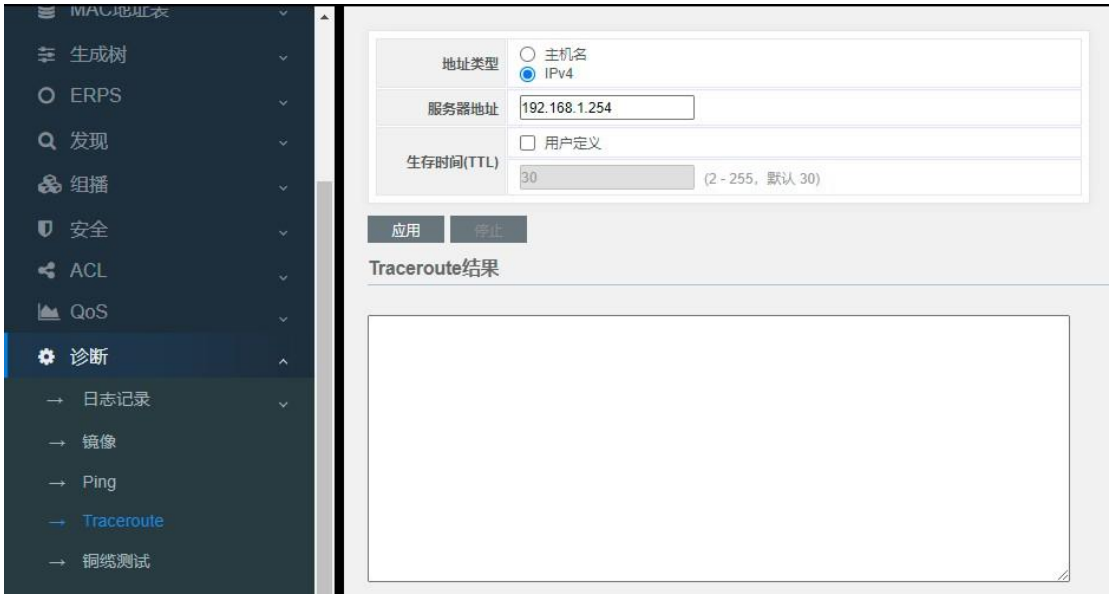


Figure 15-4-1

15.5 Copper Test

这就是 VCT 的功能，VCT 是（Virtual Cable Test）的英文缩写，它是网络通信设备中常见的一个功能。

VCT 是利用TDR(Time Domain Reflectometry-时域反射测试)来检测网络线缆的物理状态。

TDR 检测原理类似于雷达，它工作方式是通过主动向导线发射一个脉冲信号并检测所发送的脉冲信号的反射结果来检测电缆故障。当发送的脉冲信号通过电缆的末端或电缆的故障点时，就会引起部分或全部的脉冲能量被反射回来到达原来的发送源，VCT 技术根据测量脉冲信号在导线中的传输获得信号到达故障点或返回的时间，然后根据公式将相应时间换算为距离值。通过 VCT 可以检测电缆状态、故障距离是否极性交换、插入信号衰减、返回信号衰减等。

用户可以使能 VCT 特性对以太网电口连接电缆进行检测，开启系统对以太网电口连接电缆的检测功能。检测内容包括电缆的接收方向和发送方向是否存在短路、开路现象，同时可以检测出故障线缆的位置。

Figure 15-5-1

只需要选择端口，点击“Copper Test”按键就可以了。
当网线没有联通，是断开的，就会有测试结果，显示Length，就表示在多少米的地方是断开的。误差大概1米左右，所以对于网线故障，可以用此功能进行排查。

第 16 部分: Management

16.1 User Account

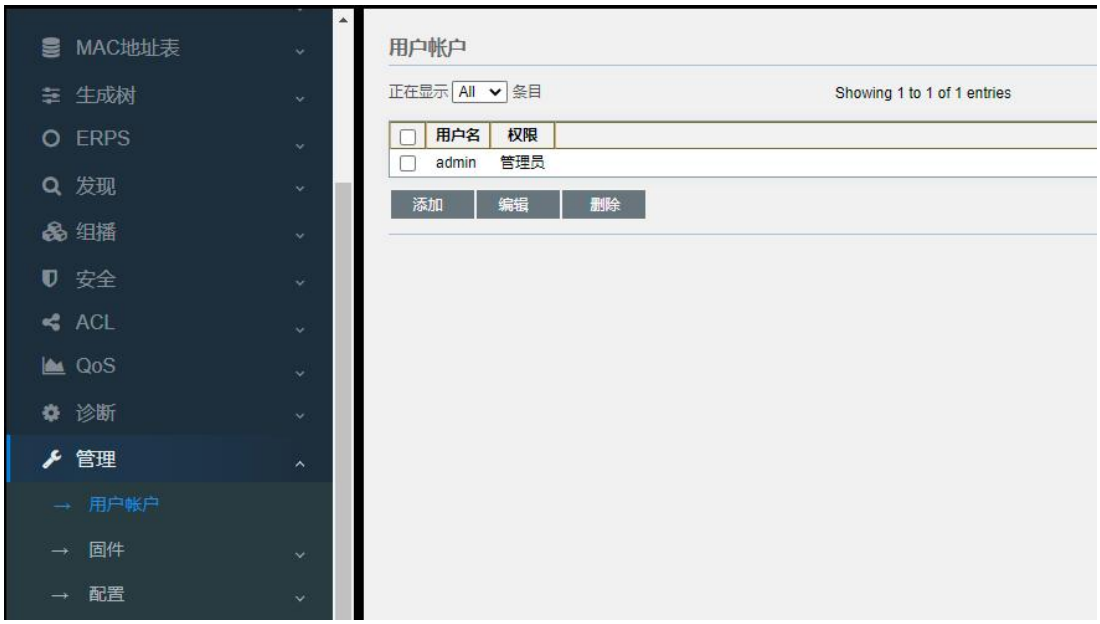


Figure 16-1-1

添加用户的话，点击Add按键

Figure 16-1-2

输入用户名，密码，确认密码就可以了。

级别分为Admin和User
Admin就是可以管理交换机系统所有功能
User就只能管理交换机几个功能。如下图所示：

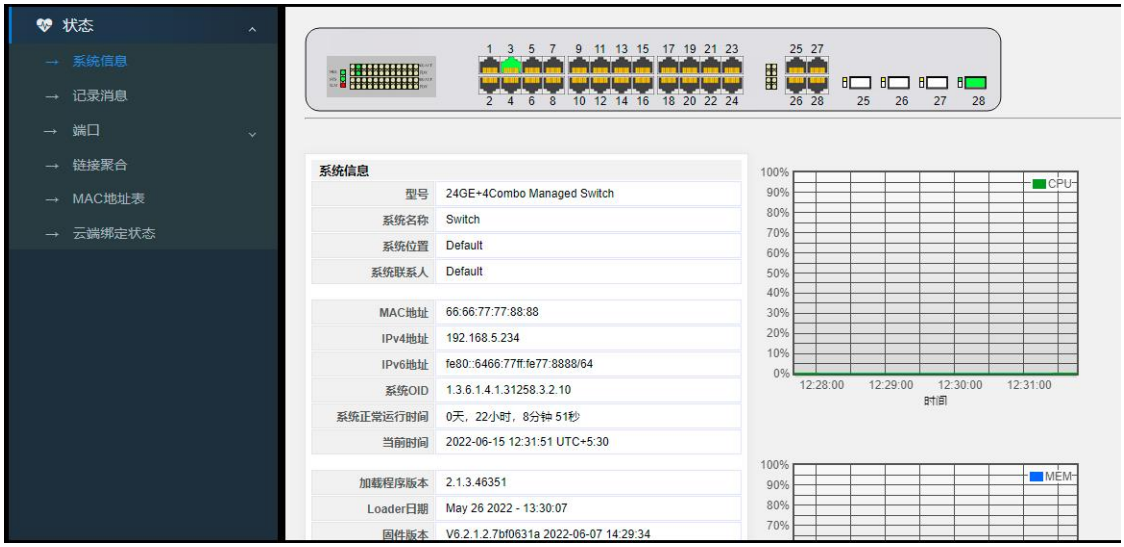


Figure 16-1-3

16.2 Firmware

16.2.1 Upgrade/Backup

可以升级和备份软件系统。可以选择通过TFTP和HTTP方式进行。

如果升级，可以选择Upgrade，HTTP方式，然后选择系统升级文件，点击Apply就可以了。

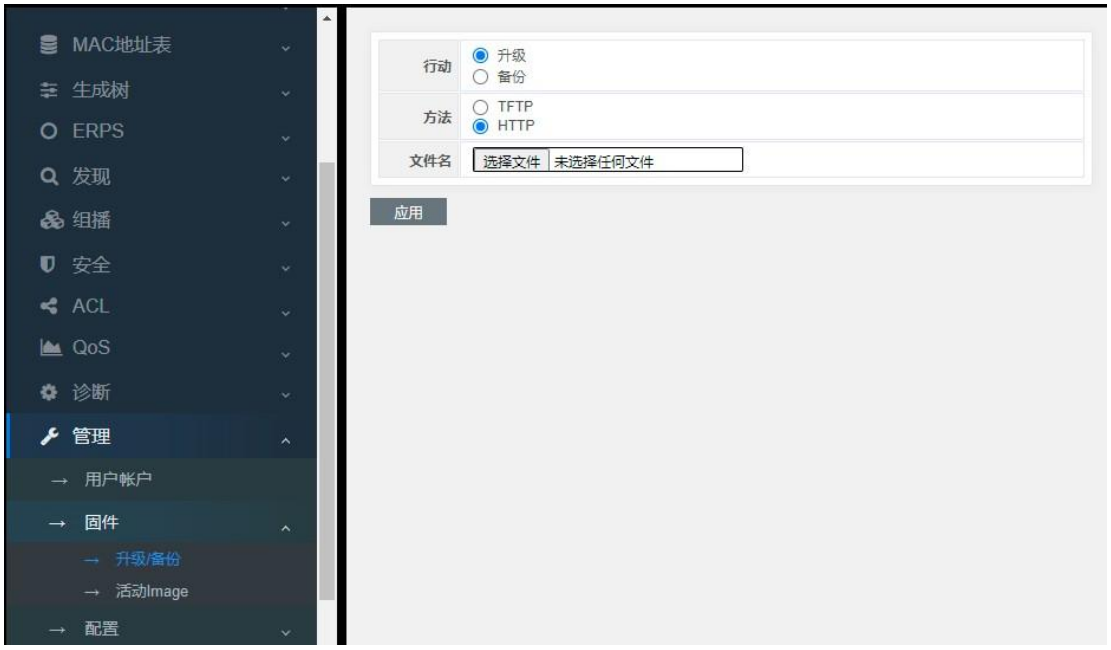


Figure 16-2-1

升级完成后，会弹出如下图信息，点击OK键就可以了。

Figure 16-2-2

然后就会显示如下信息。

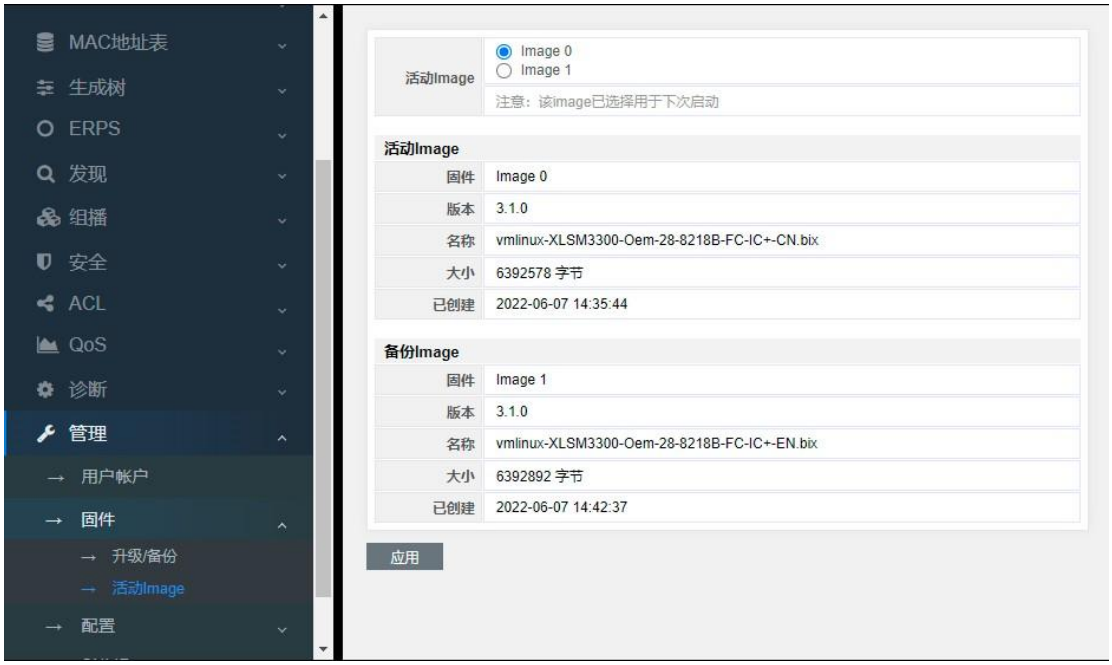


Figure 16-2-3

升级完成后，可以看见，我们刚刚用的vmlinux-XLSM3300-Oem-28-8218B-FC-IC+-EN.bix这个升级文件，对应的也就是升级的Image1。所以现在需要在Active Image选项上选择Image1，然后点击Apply，这样就完成了升级，然后点击Reboot按键就可以了。

注意，交换机是一个双img系统，当前如果是在操作Image0，那么升级的就是Image1；反之如果是操作Image1，那么升级的就是Image0。

16.3 Configuration

16.3.1 Upgrade/Backup

导入参数/导入参数

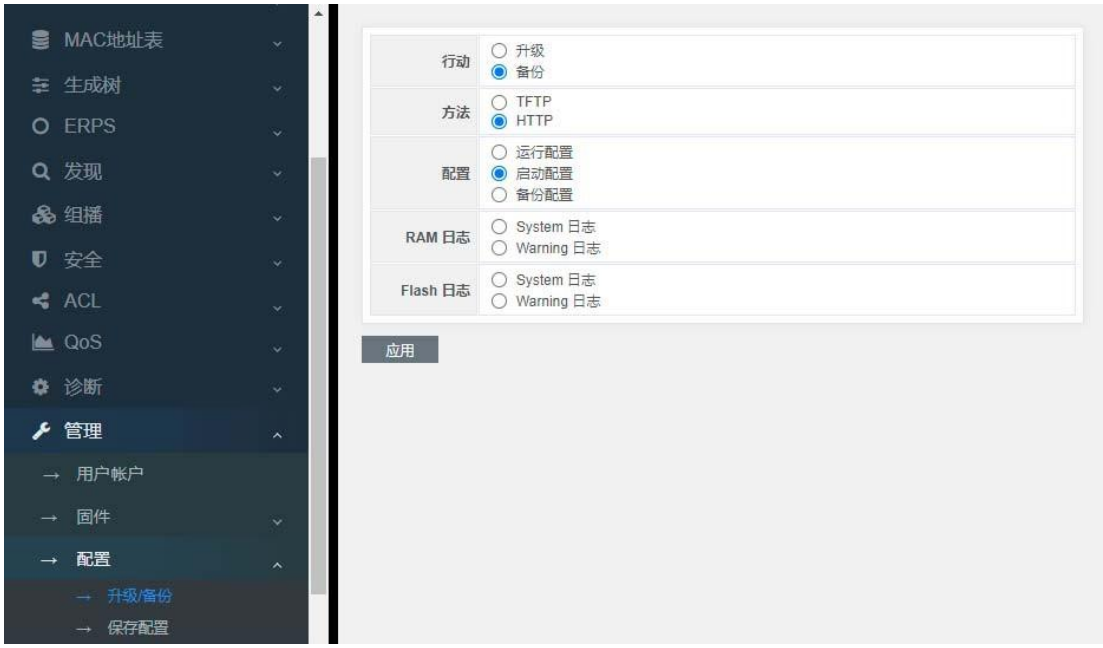


Figure 16-3-1

Action：
Upgrade升级参数，也就是导入参数
Backup备份参数，也就是导出参数

Method：TFTP/HTTP

Configuration：
Running Configuration：正在运行的参数
Startup Configuration：启动加载的参数
Backup Configuration：备份的参数

注意：
当导入参数的时候，请选择Startup configuration。然后点击重启，就可以完成参数的导入了。

当导出参数的时候, 请选择Running Configuration，就表示是当前运行的参数，选择startup configuration，就表示是保存后的参数。

16.3.2 Save Configuration

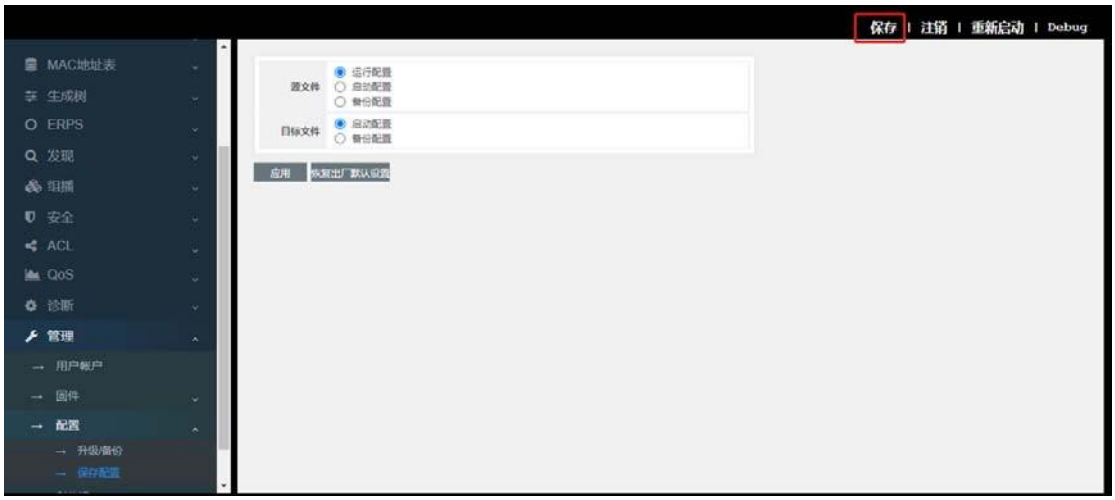


Figure 16-3-2

保存参数，是根据源文件复制到目的文件，这个比较麻烦，可以用一个最简单的方式。
那就是选择右上角的Save按键，这样就可以了。

同时这个界面中，也有恢复缺省参数的按键：“Restore Factory Default”
点击这个按键，会弹出确认的界面

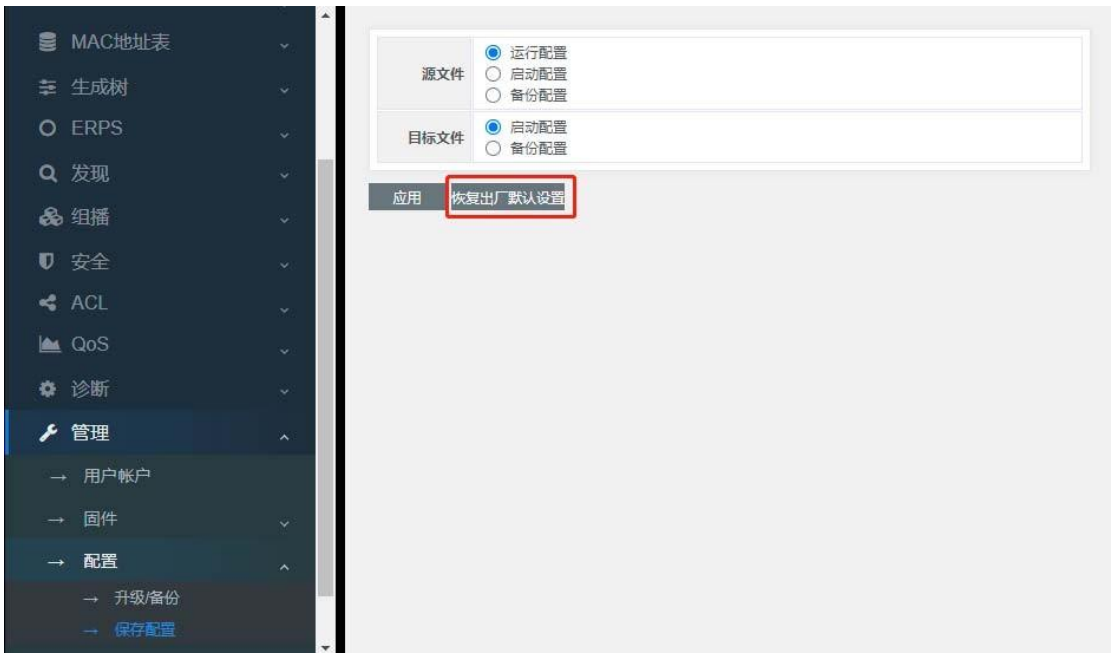


Figure 16-3-3

点击“OK”按键就可以了，然后点击Reboot，就完成了恢复缺省参数。

第 17 部分: FAQ

17.1 连接状态指示灯显示不正常(连接错误)

查看链路端连接到PC网卡或其他以太接口；
检查链路接入点是否生锈或损坏；
使用WEB检查此端口连接配置(双工，速度)，确保配置和链路另一端一样。
注意: 如果双工和速度都为强制设置，一个链路的配置必须和另一个匹配，否则不能建立连接。

17.2 连接状态指示灯显示正常但不能通信

当发生时，请按如下步骤操作：
使用WEB页面(进入”端口配置”)来检查是否端口停止，如果端口停止请启用端口。
使用WEB页面检查端口是否被VLAN隔离，和其他端口比较，当在同一VLAN的端口应设为access才能彼此同信。

17.3 不能登录到交换机

请按如下步骤检查交换机：
检查交换机是否上电；
检查连接失败，用”ping”检查交换机回应，如果没有回应，检查PC和交换机的IP地址配置是否正确;依照HTTP连接的返回信息来找出问题的原因。

检查IP地址设置
请按如下步骤检查交换机：
1) 检查PC的IP地址，子网掩码是否配置正确，请在命令行窗口输入”ipconfig”并回车以查看PC的IP地址配置。
2) 检查交换机的IP地址，子网掩码和默认网关是否为正确配置。
3) 检查交换机的IP地址是否被其他设备占用。

检查登录账户
当通过WEB登录时，如果交换机连续请求用户输入帐户和密码，这可能是提醒帐户不存在或密码无效。

17.4 交换机启动失败

如果交换机通过console口不能成功启动，请按如下步骤操作：
1) 检查串口号是否错误，通常为COM1和COM2；
2) 确保软件配置如下：115200bPS，8数据位，1停止位，并且无奇偶检验和数据流控制。
3) 检查PC的串口是否正常：您可以使用鼠标检测串口是否失败。
4) 确保没有其他程序使用此串口：在windows操作系统中，任何串口不能同时被1个以上的程序使用。

17.5 电源失效

检查电源指示灯，如果指示灯不亮，电源连接可能损坏，请确保电源供应正常，并检查交换机和电源间的连接是否为稳定并可靠的。