16/24 口 PoE 交换机

WEB 配置手册

V1.0.0

浙江大华技术股份有限公司

法律声明

版权声明

© 2017 浙江大华技术股份有限公司。版权所有。

在未经浙江大华技术股份有限公司（下称“大华”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。

本文档描述的产品中，可能包含大华及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- 、、、是浙江大华技术股份有限公司的商标或注册商标。
- HDMI 标识、HDMI 和 High-Definition Multimedia Interface 是 HDMI Licensing LLC 的商标或注册商标。本产品已经获得 HDMI Licensing LLC 授权使用 HDMI 技术。
- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

更新与修改

为增强本产品的安全性、以及为您提供更好的用户体验，大华可能会通过软件自动更新方式对本产品进行改进，但大华无需提前通知且不承担任何责任。

大华保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。产品部分功能在更新前后可能存在细微差异。

前言

概述

本文档详细描述了 16 口和 24 口 PoE 交换机的安装、配置和使用。

本说明书适用于以下产品型号：

产品型号
DH-S1500C-16ET2GF-APWR
DH-S1500C-24ET2GF-APWR

符号约定

在本文中可能出现下列标志，它们所代表的含义如下：

符号	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

重要安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。



注意

- 请在设备布控后及时修改用户的默认密码，以免被人盗用。
- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或安装在稳定的场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上不能放置装满液体的物品，防止液体流入设备。
- 请安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请勿随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。



警告

- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用。
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 IEC60950-1 符合 Limited Power Source（受限制电源）的额定电压供电，具体供电要求以设备标签为准。
- 请将 I 类结构的产品连接到带保护接地连接的电网电源输出插座上。
- 如果使用电源插头或器具耦合器等作为断开装置，请保持断开装置可以方便的操作。

特别声明

- 产品请以实物为准，说明书仅供参考。
- 说明书和程序将根据产品实时更新，如有升级不再另行通知。
- 如果不按照说明中的指导操作，因此造成的损失由使用方承担。
- 说明书可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。

目录

法律声明 ..... **I**
前言 ..... **II**
重要安全须知 ..... **III**
1 产品概述 **1**
1.1 产品简介 1
1.2 产品特性 1
2 设备结构 **2**
2.1 DH-PFS4218-16ET-240 结构图 2
2.1.1 前面板 2
2.1.2 后面板 2
2.2 DH-PFS4226-24ET-360 结构图 3
3 登录交换机 **4**
3.1 登录交换机 4
3.2 WEB 界面介绍 4
3.2.1 端口信息显示区 5
3.2.2 导航栏区 5
3.2.3 配置显示区 6
4 系统配置 **7**
4.1 系统配置 7
4.1.1 系统信息 7
4.1.2 系统时间 7
4.1.3 CPU 使用率 8
4.2 网络配置 8
4.3 DHCP 9
4.3.1 IP 地址动态获取过程 10
4.3.2 DHCP 报文格式 11
4.4 软件升级 12
4.5 密码修改 13
4.6 恢复出厂配置 13
4.7 系统重启 14
4.8 日志信息 14
5 端口管理 **16**
5.1 端口配置 16
5.2 端口镜像 17
5.3 端口流量统计 19
5.4 端口限速 20
5.5 广播风暴控制 22
5.6 远距离传输 24
6 设备管理 **26**
6.1 环网 26
6.1.1 生成树定义 26

6.1.2 生成树的基本概念 26
6.1.3 生成树设置 28
6.1.4 STP 端口设置 29
6.2 VLAN 配置 29
6.2.1 VLAN 定义 29
6.2.2 VLAN 作用 29
6.2.3 基于接口的划分 VLAN 30
6.3 链路聚合 32
6.3.1 静态聚合模式 32
6.3.2 LACP 模式 33
6.4 QoS 设置 35
6.4.1 网络拥塞 35
6.4.2 拥塞解决办法 36
6.4.3 队列调度 36
6.4.4 优先级模式 36
6.4.5 基于 Port/802.1p/DSCP 的 QoS 37
6.4.6 基于 TCP/UDP 端口号 39
6.5 安全 42
6.5.1 MAC 地址表 42
6.5.2 端口 MAC 绑定 42
6.5.3 端口 MAC 过滤 43
6.6 SNMP 设置 44
6.6.1 SNMP 的协议版本 45
6.6.2 SNMP 系统配置 45
6.7 802.1x 49
6.7.1 802.1x 的组网结构 49
6.7.2 802.1x 认证受控/非受控端口 50
6.7.3 802.1x 认证的触发方式 50
6.7.4 端口的授权状态 51
6.8 IGMP Snooping 52
6.8.1 IGMP Snooping 原理 52
6.8.2 IGMP Snooping 配置 53
7 PoE 54
7.1 PoE 设置 54
7.2 PoE 事件统计 56
7.3 绿色节能 PoE 56

1 产品概述

1.1 产品简介

16 口和 24 口 PoE（Power over Ethernet，以太网供电，又称远程供电）交换机为二层工业交换机，支持网管和 PoE 功能，通过光纤进行远距离传输。可广泛应用于安防监控、网络管理等场合。

1.2 产品特性

- 二层工业级交换机。
- 支持 2 个千兆光电自适应 Combo 口。
- 支持 16/24 个 10/100M 自适应 RJ45 端口。
- 支持 1 个 Console 接口。
- 符合 IEEE802.3、IEEE802.3u、IEEE802.3ab/z 和 IEEE802.3X 标准。
- 符合 802.1Q Standard VLAN(Access/Thunk/Hybrid)标准。
- 所有端口自动适应 MDI/MDIX 模式。
- MAC（Media Access Control，媒体访问控制）自动学习与老化，MAC 地址列表容量为 4K。
- IEEE802.3X 全双工流控与 Backpressure 半双工流控。
- 支持 AC 100V～240 V 供电。
- 符合 IEEE802.3af、 IEEE802.3at 标准，端口 1 和端口 2 支持 Hi-PoE 60W。
- 支持 PoE 功耗管理。
- 支持 SNMP（Simple Network Management Protocol，简单网络管理协议）V1/V2/V3 网管。
- 支持 STP（Spanning Tree Protocol，生成树协议）/RSTP（Rapid Spanning Tree Protocol，快速生成树协议）环网协议。
- 支持手动聚合和静态 LACP（link Aggregation Control Protocol，链路聚合控制协议）。
- 支持多对一镜像。
- 支持端口 MAC 绑定。
- 支持在线升级和日志管理。
- 支持 WEB 界面管理。

2 设备结构

2.1 DH-PFS4218-16ET-240 结构图

2.1.1 前面板

图2-1 前面板

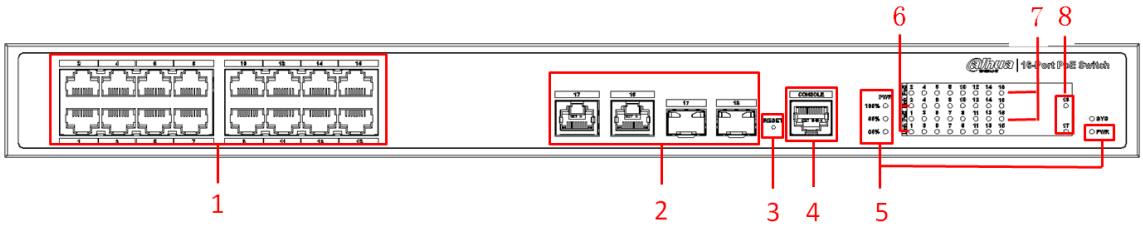


表2-1 前面板说明

序号	名称	说明
1	RJ45 端口	16 个以太网口，支持 10/100M 自适应。
2	COMBO 口	2 个以太网口，支持 10/100/1000M 自适应，2 个光口支持 1000M。
3	复位键	长按该按钮执行复位操作，并恢复默认配置。
4	CONSOLE	设备调试串口。
5	POWER 实时显示	当前 PoE 功耗显示和电源指示灯。
6	电口指示灯	电口状态实时显示。
7	PoE 指示灯	PoE 状态实时显示。
8	光电口指示灯	光电口状态实时显示。

2.1.2 后面板

设备后面板接口如图 2-2 所示，详细说明请参见表 2-2。

图2-2 后面板

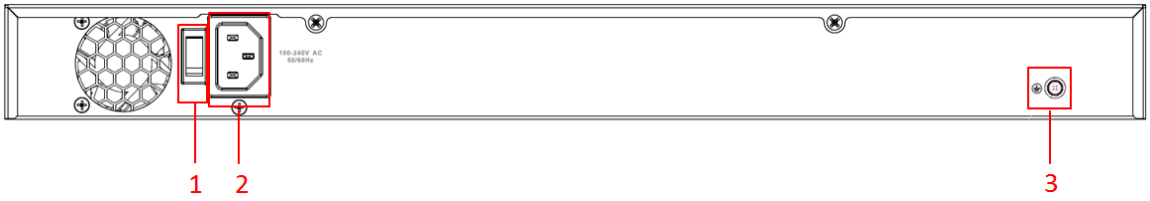


表2-2 后面板说明

序号	名称	说明
1	电源开关	控制设备上/下电。
2	电源接口	支持 AC 100V～240V。

序号	名称	说明
3	接地螺钉	接地。

2.2 DH-PFS4226-24ET-360 结构图

图2-3 前面板

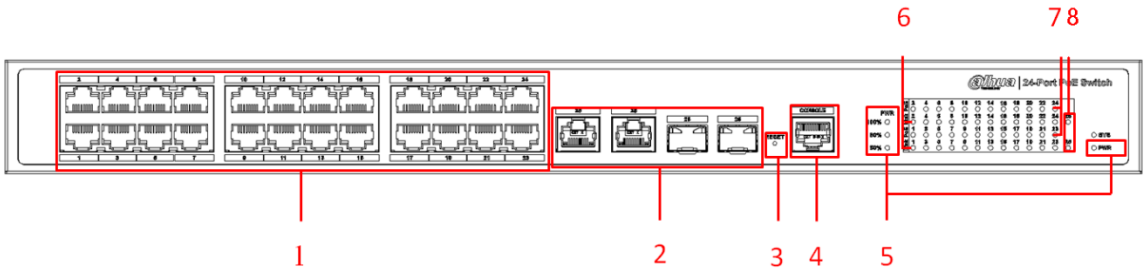


表2-3 前面板说明

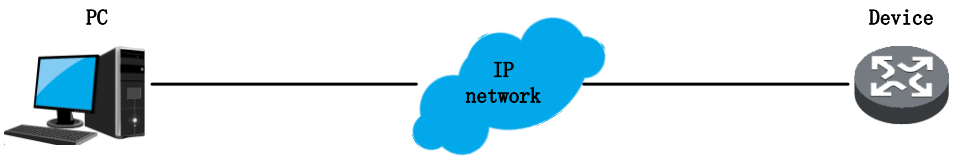
序号	名称	说明
1	RJ45 端口	24 个以太网口，支持 10/100M 自适应。
2	COMBO 口	2 个以太网口，支持 10/100/1000M 自适应，2 个光口支持 1000M。
3	复位键	长按该按钮执行复位操作。
4	CONSOLE	设备调试串口。
5	POWER 实时显示	当前 PoE 功耗显示和电源指示灯。
6	以太网口指示灯	以太网口状态实时显示。
7	PoE 指示灯	PoE 状态实时显示。
8	光电口指示灯	光电口状态实时显示。

3 登录交换机

3.1 登录交换机

设备组网如图 3-1 所示，配置交换机之前需要先登录交换机，用户通过 WEB 网管，可以在图形界面下非常直观地管理和维护交换机（即图中 Device）。

图3-1 设备组网



通过浏览器访问交换机，请确保交换机运行的主程序文件支持 WEB 访问，且您的计算机已经连接到交换机所在的网络。如果是第一次使用交换机，无需额外配置，您已经可以使用 WEB 访问。

步骤1　修改您 PC 的 IP 地址为“192.168.1.50”，子网掩码为“255.255.255.0”。

步骤2　打开浏览器，在地址栏中输入交换机的默认地址“192.168.1.110”。

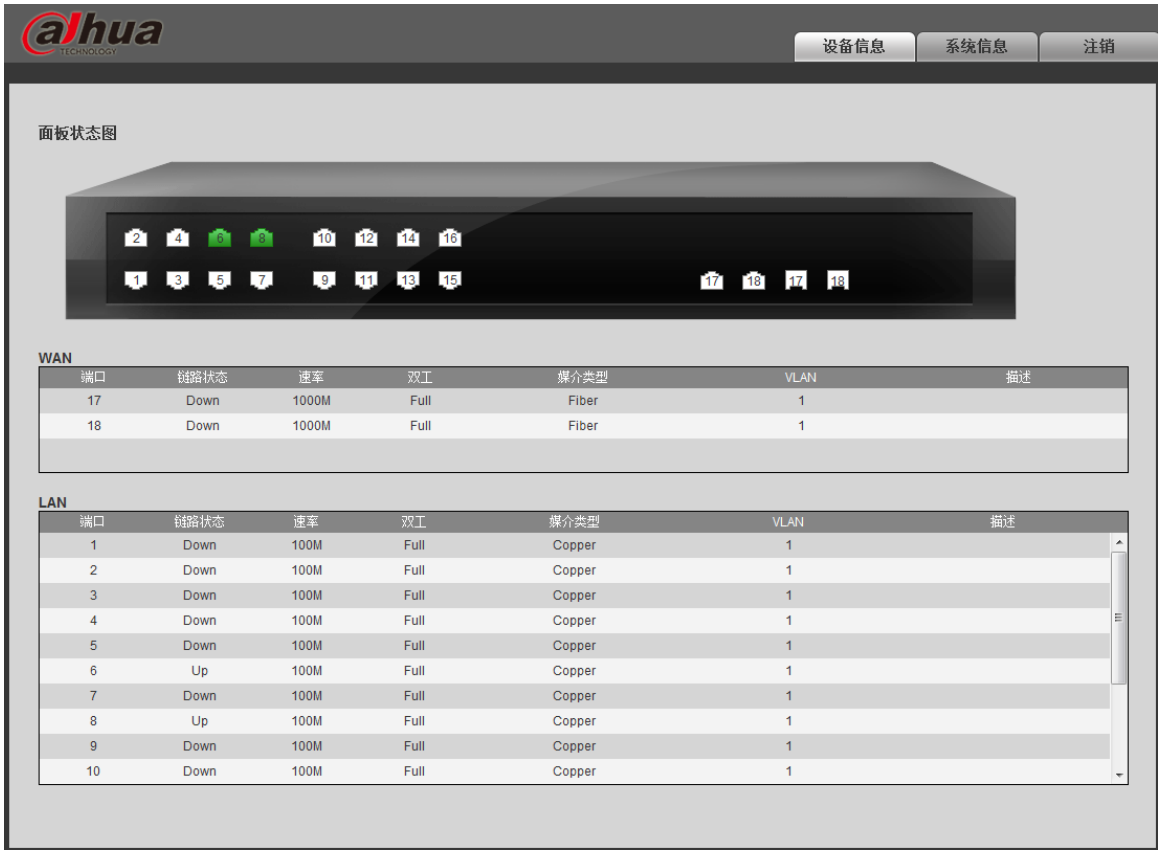
步骤3　在登录验证对话框中输入用户名和密码，初始的用户名为“admin”，密码为“admin”，请区分字母的大小写。登录后，为了安全起见，系统强制要求您修改密码。

若登录成功，浏览器中会显示交换机的设备信息界面。

3.2 WEB 界面介绍

设备正常登录后，直接进入设备信息界面，如图 3-2 所示。

图3-2 WEB 界面

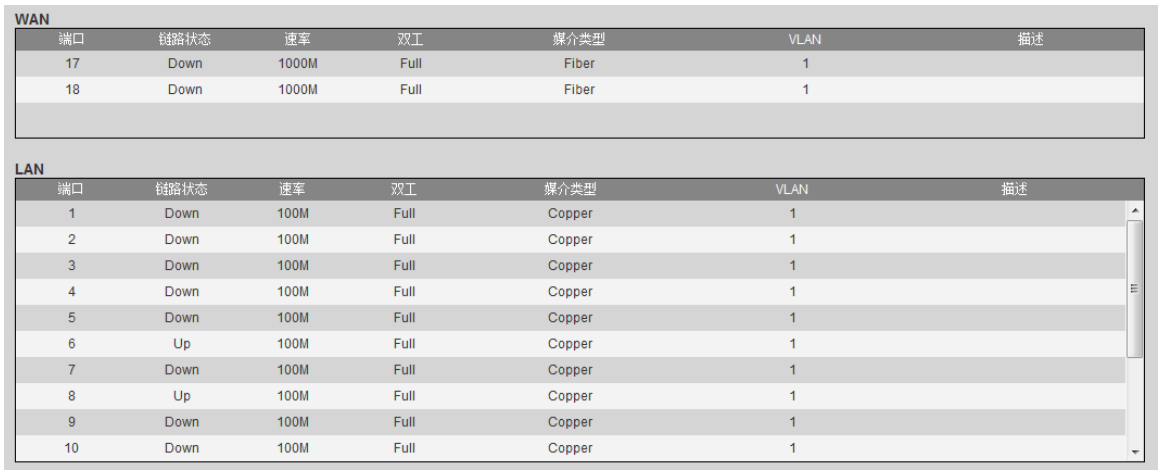


3.2.1 端口信息显示区

端口显示区可以显示端口当前的链路状态、端口速率、双工模式等信息。

如图 3-3 所示，端口信息显示区包括 WAN 端口状态显示和 LAN 端口状态显示。

图3-3 端口信息显示区



3.2.2 导航栏区

如图 3-4 所示为导航栏的内容。单击“系统信息”，系统显示“系统信息”界面，左侧的导航如图 3-5 所示，以列表的形式显示，并按类别分组。

图3-4 导航栏



图3-5 导航列表



3.2.3 配置显示区

如图 3-6 所示（图为举例），配置显示区显示从导航栏中选中的内容，配置区提供查看和修改等配置操作。

下面将通过四个章节来介绍四大配置模块：系统配置、端口管理、设备管理和 PoE。

图3-6 配置显示区示意图



4 系统配置

4.1 系统配置

4.1.1 系统信息

您可以查询设备的型号、MAC 地址和软件版本。

选择“系统信息 > 系统配置 > 系统信息 > 系统信息”。

系统显示“系统信息”界面，如图 4-1 所示。

图4-1 系统信息



4.1.2 系统时间

您可以查询和设置设备运行的当前时间和时区，也可以从 PC 上同步时间到设备。

步骤1 选择“系统信息 > 系统配置 > 系统信息 > 系统时间”。

系统显示“系统时间”界面，如图 4-2 所示。

图4-2 系统时间



步骤2　设置系统时间和时区。

- 单击“同步 PC”。
- 单击“保存”。

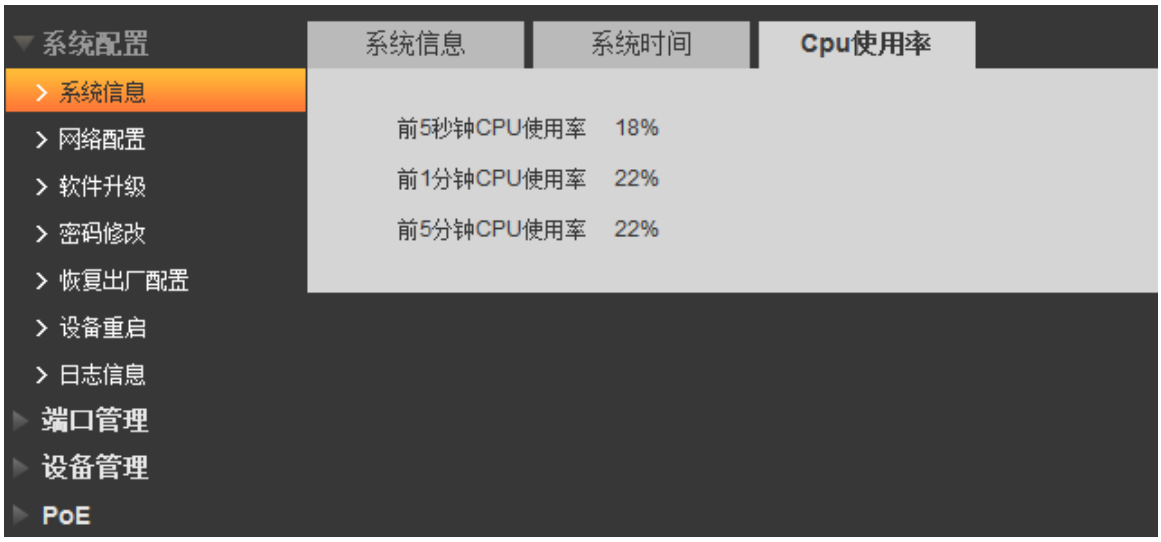
4.1.3 CPU 使用率

您可以查询设备运行过程中 CPU 的占用率。

选择“系统信息 > 系统配置 > 系统信息 > CPU 使用率”。

系统显示“CPU 使用率”界面，如图 4-3 所示。

图4-3 CPU 使用率



4.2 网络配置

在 IP 网络中通信，每个主机都需要拥有一个 IP 地址。

IP 地址是在 Internet 上使用的 32 位地址，由网络号和主机号两部分组成。IP 地址的网络号字段用来标识一个网络，主机号字段用来标识网络中的具体某台网络设备。对这些设备而言，无论实际所处的物理位置如何，只要它们的网络号相同，它们就处在同一个网络中。

您可以查看设备的 IP 地址、子网掩码、默认网关和 MAC 地址等。

步骤1　选择“系统信息 > 系统配置 > 网络配置 > IPV4”。

系统显示“IPV4”界面，如图 4-4 所示。

图4-4 IPV4



步骤2　设置参数，请参见表 4-1。

表4-1 IPV4

参数	说明
模式	包括“静态”和“DHCP”。如果选择了“静态”，则需要设置交换机的 IP 地址、子网掩码和 MAC 地址；如果选择了“DHCP”，则自动获取 IP。
IP 地址	设置交换机的 IP 地址，默认 IP 地址是“192.168.1.110”。
子网掩码	注意 请不要随意修改交换机的子网掩码，如修改不当，会出现无法登录交换机的情况。 设置交换机的子网掩码。
默认网关	设置交换机的默认网关。
MAC 地址	显示交换机的物理地址，不可修改。

步骤3　单击“保存”。

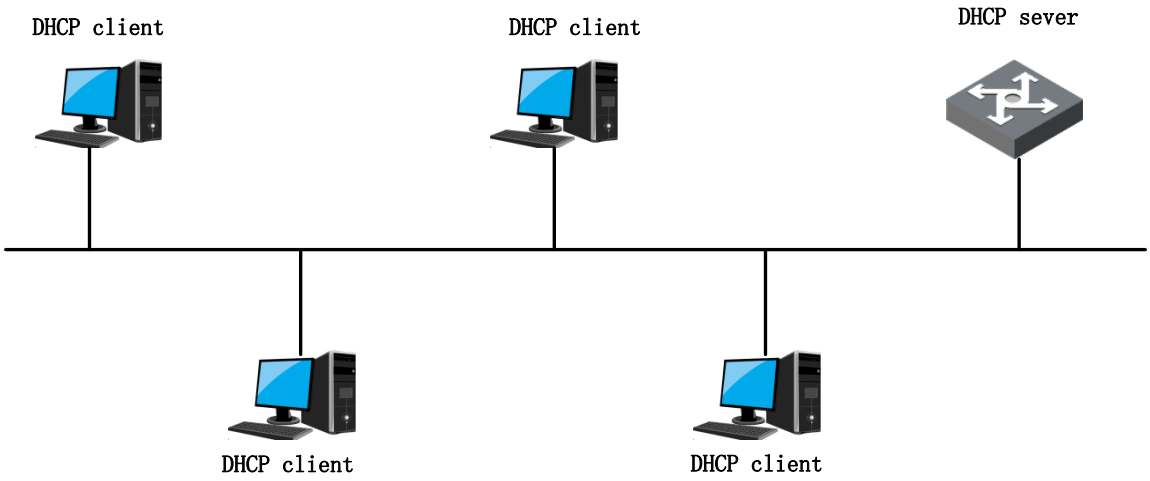
4.3 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态地分配 IP 地址等网络配置参数。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

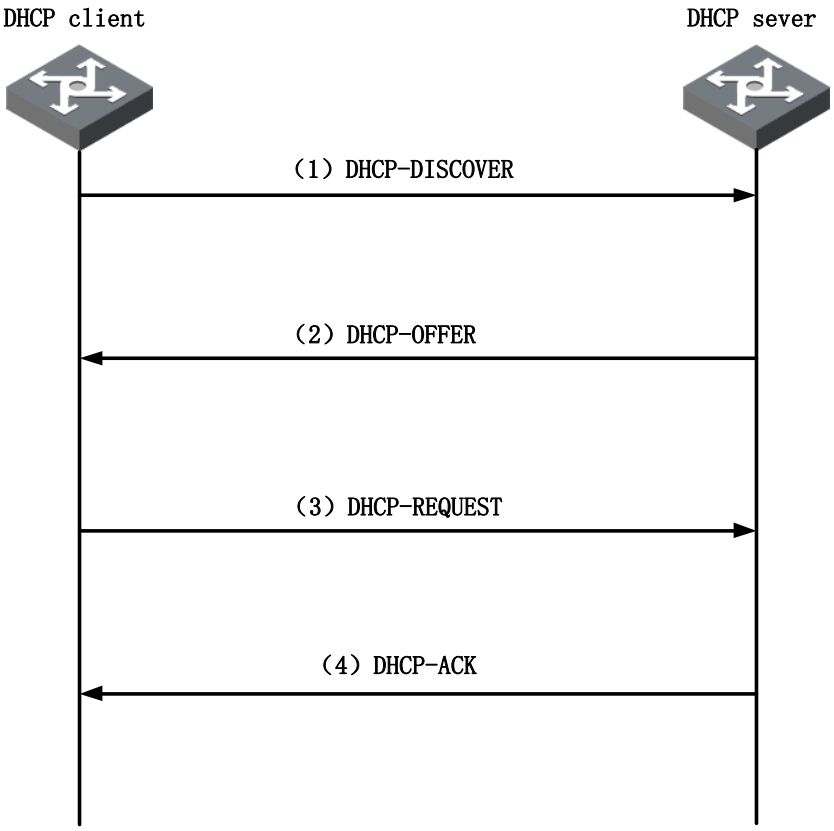
在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如下图 4-5 所示。

图4-5 DHCP 典型应用



4.3.1 IP 地址动态获取过程

图4-6 IP 地址动态获取过程



如图 4-6 所示 DHCP 客户端从 DHCP 服务器动态获取 IP 地址，主要通过四个阶段进行：

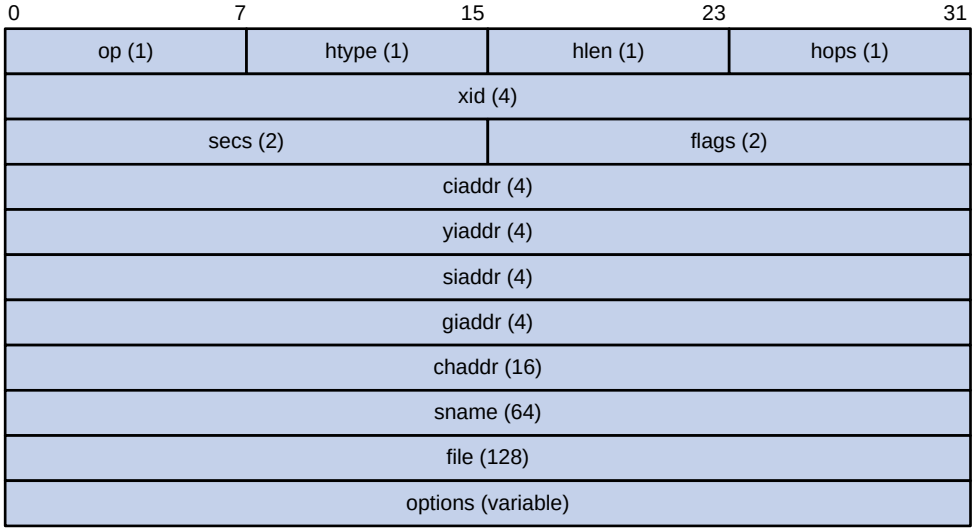
1. 发现阶段，即DHCP客户端寻找DHCP服务器的阶段。客户端以广播方式发送DHCP-DISCOVER报文。
2. 提供阶段，即DHCP服务器提供IP地址的阶段。DHCP服务器接收到客户端的DHCP-DISCOVER报文后，根据IP地址分配的优先次序选出一个IP地址，与其他参数一起通过DHCP-OFFER报文发送给客户端。DHCP-OFFER报文的发送方式由DHCP-DISCOVER报文中的flag字段决定。

3. 选择阶段，即DHCP客户端选择IP地址的阶段。如果有多台DHCP服务器向该客户端发来DHCP-OFFER报文，客户端只接受第一个收到的DHCP-OFFER报文，然后以广播方式发送DHCP-REQUEST报文，该报文中包含DHCP服务器在DHCP-OFFER报文中分配的IP地址，其它DHCP服务器中本次未分配出的IP地址仍可分配给其他客户端。
4. 确认阶段，即DHCP服务器确认IP地址的阶段。DHCP服务器收到DHCP客户端发来的DHCP-REQUEST报文后，只有DHCP客户端选择的服务器会进行如下操作：如果确认将地址分配给该客户端，则返回DHCP-ACK报文；否则返回DHCP-NAK报文，表明地址不能分配给该客户端。

4.3.2 DHCP 报文格式

DHCP 有 8 种类型的报文，每种报文的格式相同，只是某些字段的取值不同。DHCP 报文格式基于 BOOTP 的报文格式，具体格式如下图 4-7 所示（括号中的数字表示该字段所占的字节）。

图4-7 DHCP 报文格式



各字段的解释如下：

- op：报文的操作类型，分为请求报文和响应报文，1 为请求报文；2 为响应报文。具体的报文类型在 option 字段中标识。
- htype、hlen：DHCP 客户端的硬件地址类型及长度。
- hops：DHCP 报文经过的 DHCP 中继的数目。DHCP 请求报文每经过一个 DHCP 中继，该字段就会增加 1。
- xid：客户端发起一次请求时选择的随机数，用来标识一次地址请求过程。
- secs：DHCP 客户端开始 DHCP 请求后所经过的时间。目前没有使用，固定为 0。
- flags：第一个比特为广播响应标识位，用来标识 DHCP 服务器响应报文是采用单播还是广播方式发送，0 表示采用单播方式，1 表示采用广播方式。其余比特保留不用。
- ciaddr：DHCP 客户端的 IP 地址。
- yiaddr：DHCP 服务器分配给客户端的 IP 地址。
- siaddr：DHCP 客户端获取 IP 地址等信息的服务器 IP 地址。
- giaddr：DHCP 客户端发出请求报文后经过的第一个 DHCP 中继的 IP 地址。
- chaddr：DHCP 客户端的硬件地址。
- sname：DHCP 客户端获取 IP 地址等信息的服务器名称。
- file：DHCP 服务器为 DHCP 客户端指定的启动配置文件名称及路径信息。
- option：可选变长选项字段，包含报文的类型、有效租期、DNS 服务器的 IP 地址、WINS 服务器的 IP 地址等配置信息。

配置举例

组网需求

配置交换机为 DHCP 客户端，自动获取交换机管理 IP 地址。

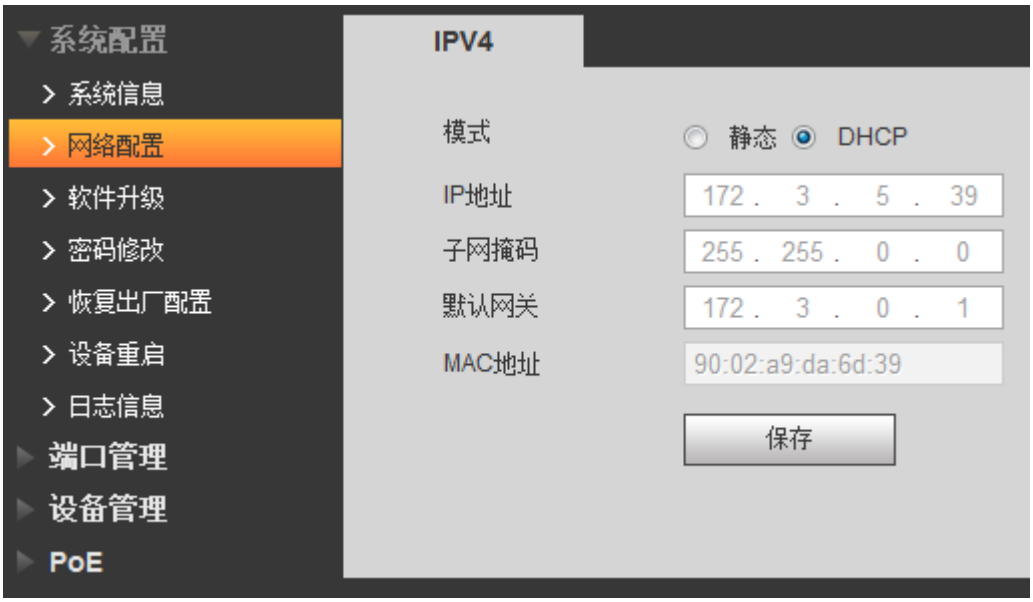
配置步骤

步骤1　选择“系统信息 > 系统配置 > 网络配置 > IPV4”。

系统显示“IPV4”界面，如图 4-4 所示。

步骤2　选择“模式”为“DHCP”，如图 4-8 所示。

图4-8 网络配置



步骤3　单击“保存”。

4.4 软件升级

本界面提供交换机通过 WEB 方式升级系统文件功能。您可以在大华网站下载最新版本的系统文件。

步骤1　选择“系统信息 > 系统配置 > 软件升级 > 固件升级”。

系统显示“固件升级”界面，如图 4-9 所示。

图4-9 软件升级



步骤2　单击“浏览文件”选择正确的升级文件。

步骤3　单击“升级”。

4.5 密码修改

您可以在本界面修改用户登录密码，用户名为 admin 不可修改，出厂原始密码为 admin。

步骤1　选择“系统信息 > 系统配置 > 密码修改 > 修改密码”。

系统显示“修改密码”界面，如图 4-10 所示。

图4-10 密码修改



步骤2　输入“旧密码”、“新密码”和“确认密码”。

步骤3　单击“保存”。

4.6 恢复出厂配置

当需要将交换机配置还原到最初的系统默认值时，可选择恢复出厂配置功能。除交换机管理 IP 外，其他信息均会恢复为出厂设置。

步骤1　选择“系统信息 > 系统配置 > 恢复出厂配置 > 恢复默认”。

系统显示“恢复默认”界面，如图 4-11 所示。

图4-11 恢复出厂配置



步骤2　单击“恢复默认”。

4.7 系统重启

在设备重启之前，需要对配置进行保存，否则，重启之后所有配置都会丢失。在设备重启之后，您需要重新登录设备 WEB 界面。

步骤1　选择“系统信息 > 系统配置 > 设备重启”。

系统显示“设备重启”界面，如图 4-12 所示。

图4-12 设备重启



步骤2　单击“重启设备”。

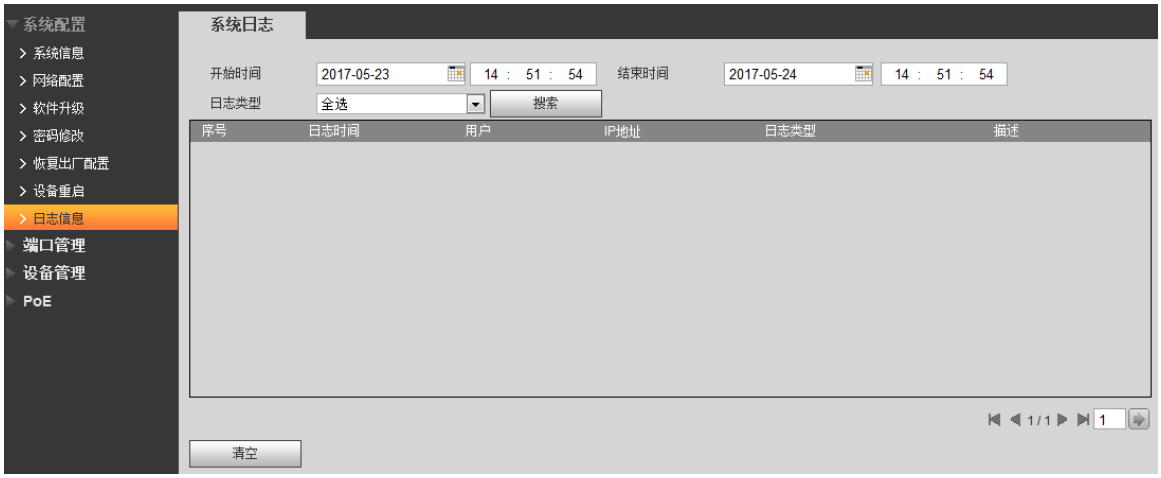
4.8 日志信息

您可以查看设备运行过程中的一些系统日志信息，方便维护人员分析问题。

步骤1　选择“系统信息 > 系统配置 > 日志信息 > 系统日志”。

系统显示“系统日志”界面，如图 4-13 所示。

图4-13 日志信息



步骤2　设置“开始时间”和“结束时间”，并设置要查找的时间段。

步骤3　选择日志类型，包括“全选”、“错误”、“警告”和“信息”。

步骤4　单击“搜索”。

说明

单击“清空”，可清空所有日志内容。

5 端口管理

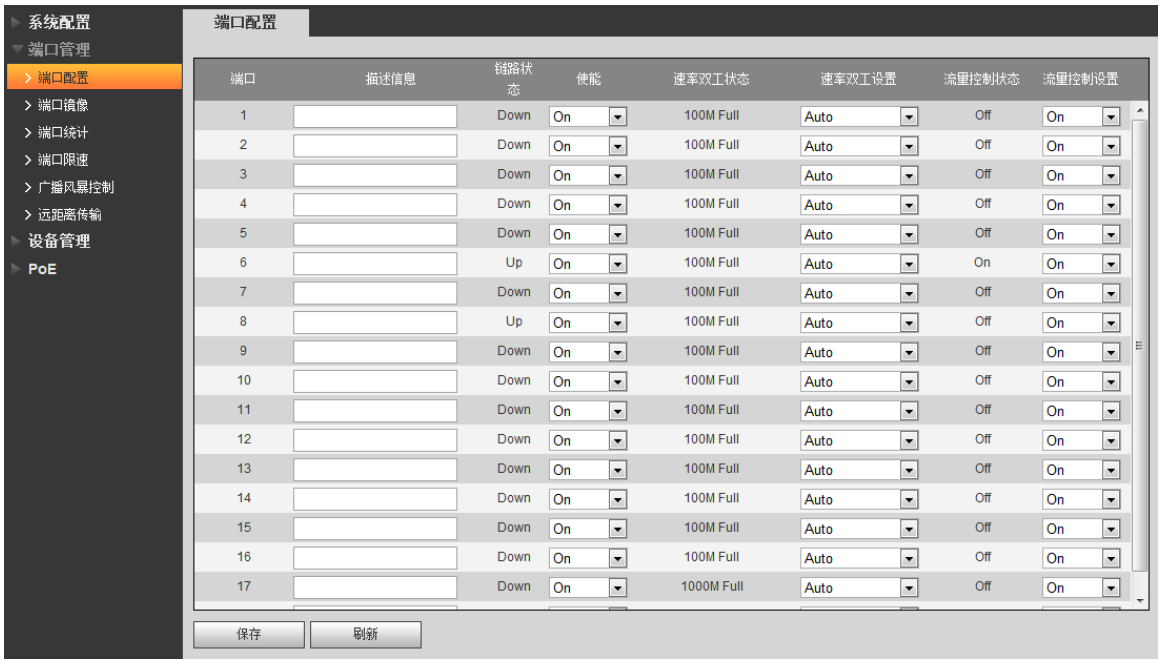
5.1 端口配置

您可以配置交换机端口相关的各项基本参数。端口基本参数将直接影响端口的工作方式，请结合实际需求情况进行配置。

步骤1　选择“系统信息 > 端口管理 > 端口配置”。

系统显示“端口配置”界面，如图 5-1 所示。

图5-1 端口配置



步骤2　设置参数，请参见表 5-1。

表5-1 端口配置说明

参数	说明
端口	显示交换机的端口号。
描述信息	为端口添加描述信息。
链路状态	显示链路状态。
使能	配置端口状态。 ● On：配置链路为使能状态。 ● Off：配置链路为非使能状态。
速率双工状态	显示端口当前的速率状态。

参数	说明
速率双工设置	配置端口速率双工方式。 ● 电口 ◇ Auto（默认值）：自协商模式 ◇ 10M FULL：10M 全双工 ◇ 10M HALF：10M 半双工 ◇ 100M FULL：100M 全双工 ◇ 100M HALF：100M 半双工 ◇ 1000M FULL：1000M 全双工 ● 光口 1000M-X：1000M 全双工，光口强制千兆全双工模式，只能适应光口强制千兆。 说明 更改端口速率双工方式，会直接影响到的端口的通信，请谨慎修改。
流量控制状态	显示交换机端口流量控制状态。
流量控制设置	配置交换机端口流控功能（默认开启）。 ● On：表示启用端口流控功能。 ● Off：表示未启用端口流控功能。 说明 “电口”可开启端口流控，同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。

步骤3　单击“保存”。

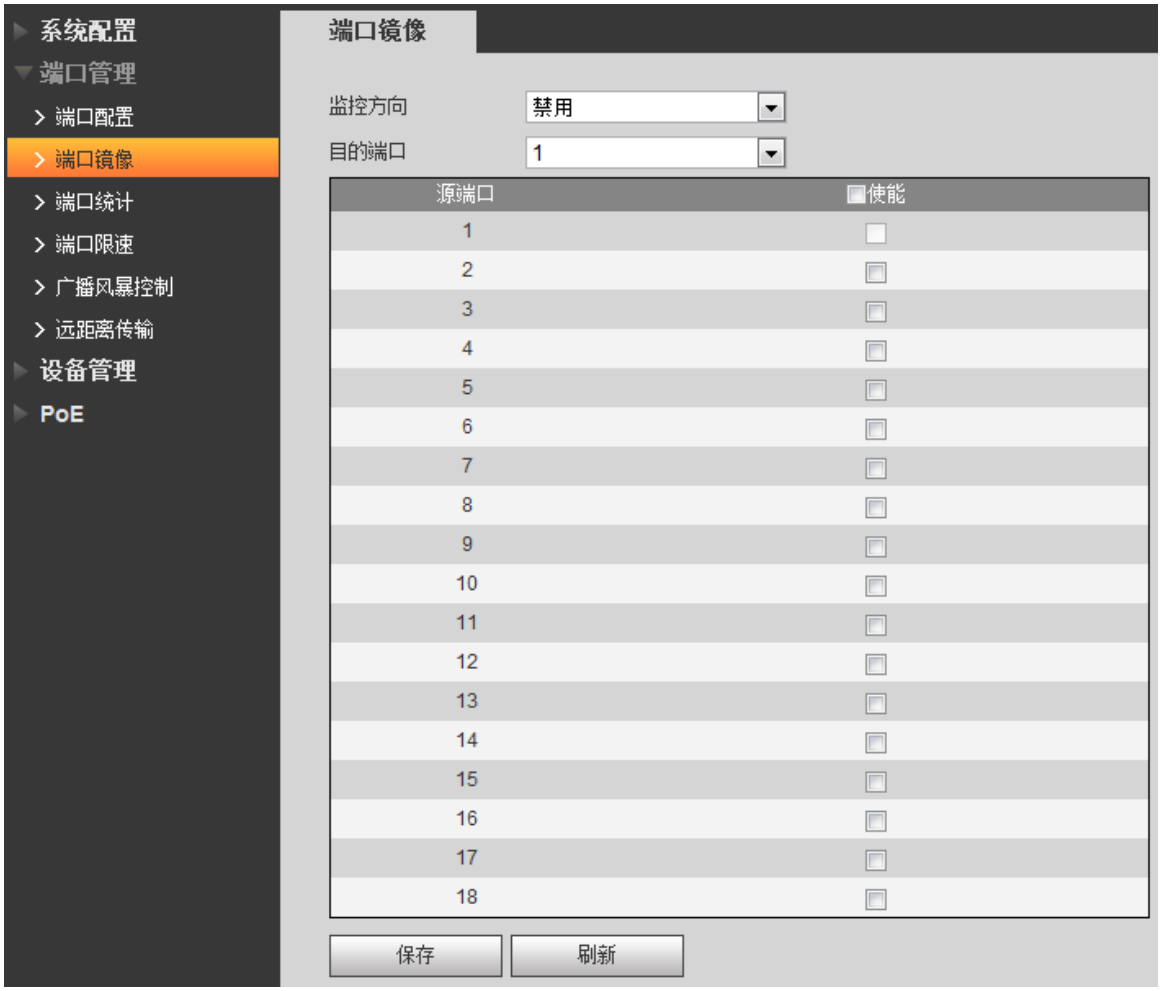
5.2 端口镜像

端口镜像也叫端口监控。端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（镜像源端口）的数据包复制到一个特定的端口（镜像目的端口），在镜像目的端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

步骤1　选择“系统信息 > 端口管理 > 端口镜像”。

系统显示“端口镜像”界面，如图 5-2 所示。

图5-2 端口镜像



步骤2　设置参数，请参见表 5-2。

表5-2 端口镜像参数说明

参数	说明
监控方向	设置监控方向，包括如下： ● 禁用：表示未开启被监控功能。 ● 出方向：表示输出监控。 ● 入方向：表示输入监控。 ● 双向：表示输入/输出都受监控。
目的端口	监控端口，只能选择一个，默认禁用。
源端口	被监控口，可以选择一个或者多个。
使能	选择复选框，开启该功能。

步骤3　单击“保存”。

配置举例

组网需求

开启端口镜像功能，使得端口 1 可以监控端口 2 和端口 3 的报文。

配置步骤

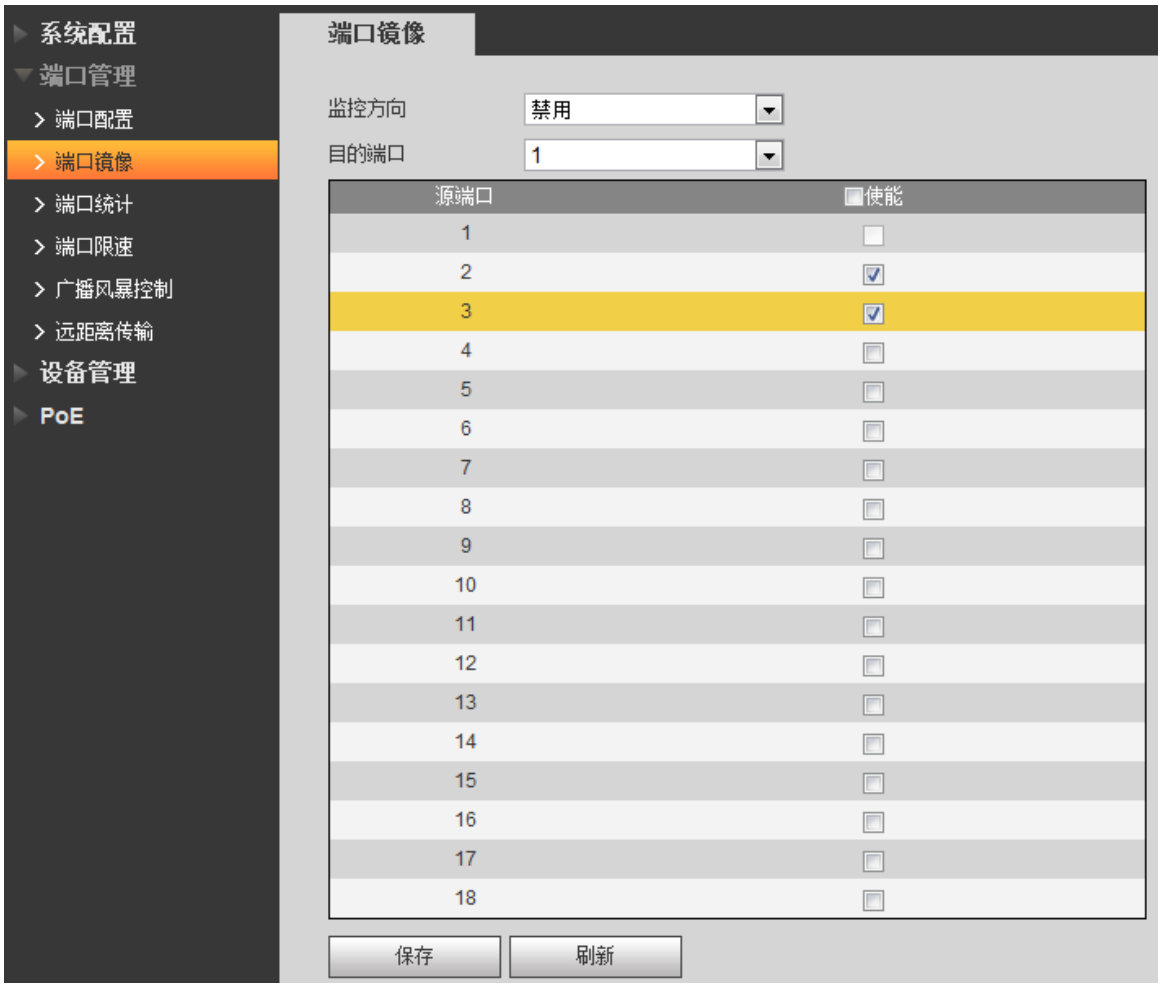
步骤1　使能镜像功能，并选择要监控的数据流。

步骤2　选择源端口。

步骤3　选择目的端口，配置结果如图 5-3 所示。

步骤4　单击“保存”。

图5-3 配置端口镜像



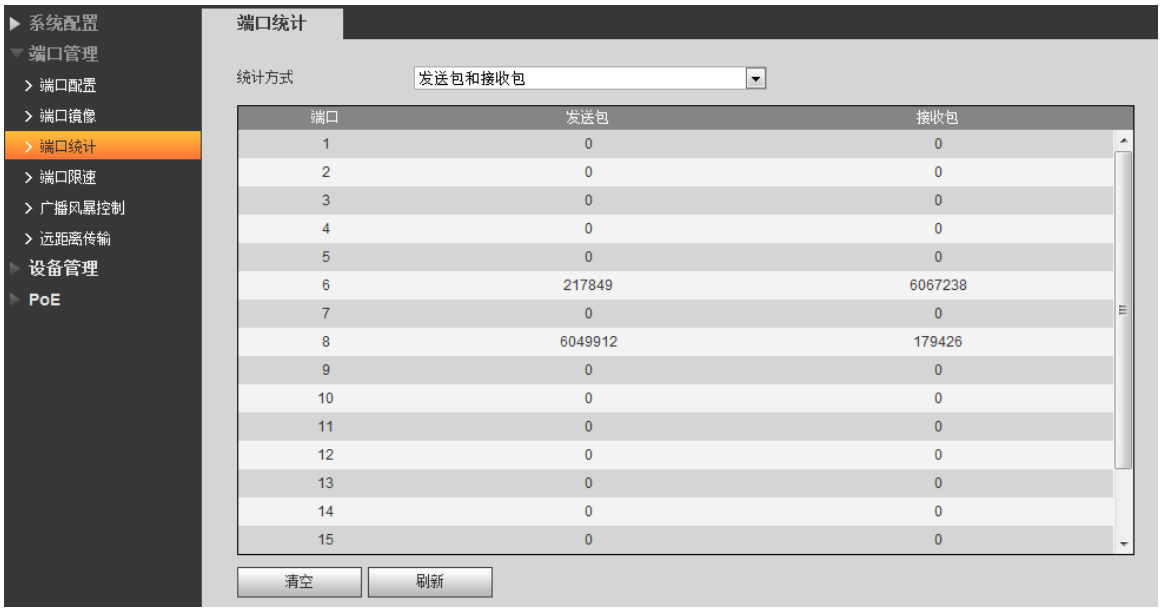
5.3 端口流量统计

您可以查看每个端口发送/接收的包数量，冲突统计和发送包的数量，丢包和接收数据包的数量，CRC 错误包和接收数据包数量。当端口的错误报文数过多则说明该端口的工作状态很差，需要检查端口所连的线缆或者对端设备是否存在问题。

步骤1　选择“系统信息 > 端口管理 > 端口统计”。

系统显示“端口统计”界面，如图 5-4 所示。

图5-4 端口统计



步骤2　选择“统计方式”，立刻生效。

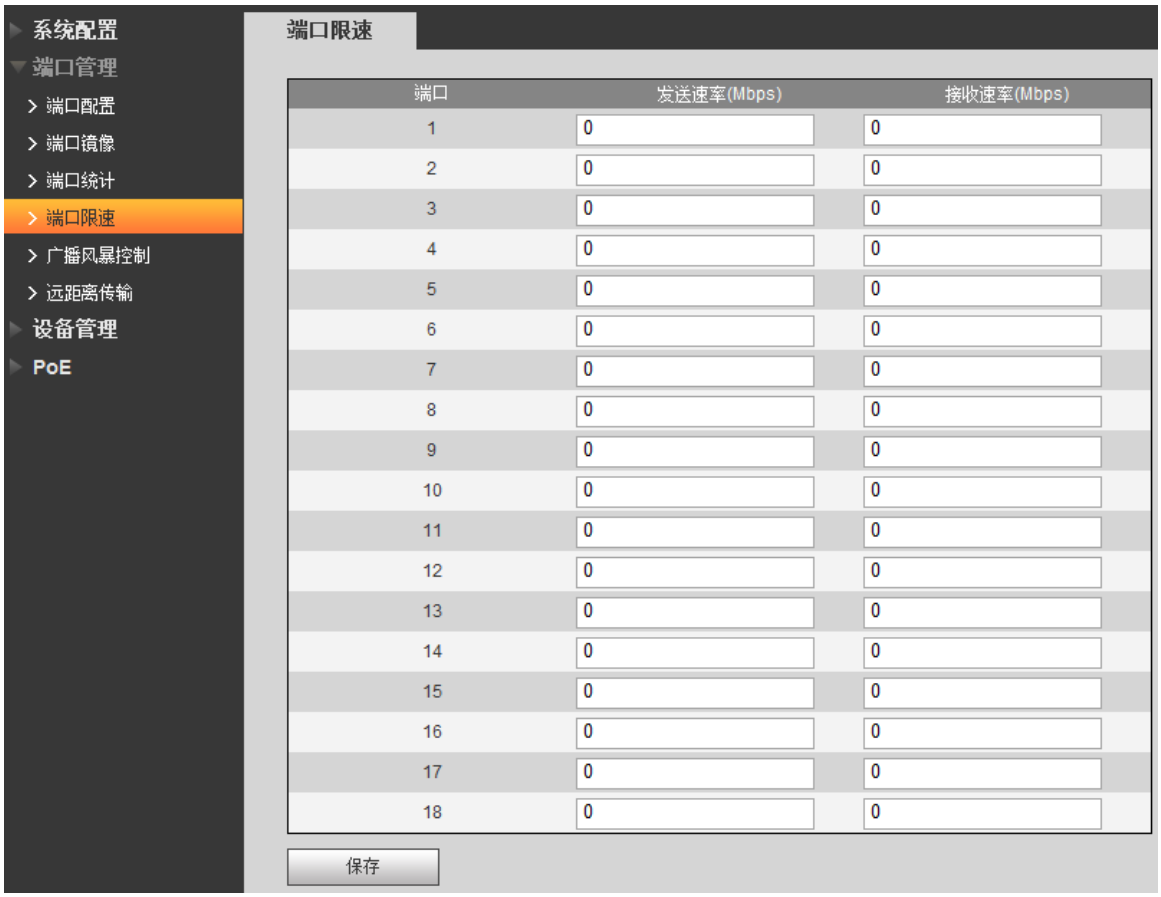
5.4 端口限速

您可以配置端口的限速策略，限制数据包进出端口的交换量的速率。

步骤1　选择“系统信息 > 端口管理 > 端口限速”。

系统显示“端口限速”界面，如图 5-5 所示。

图5-5 端口限速



步骤2　设置参数，请参见表 5-3。

表5-3 端口限速参数说明

参数	说明
端口	显示端口列表。
发送速率	配置端口发送数据包的速率，可配置速率为 0Mbps～63Mbps，默认为 0，不限速。
接收速率	配置端口接收数据包的速率，可配置速率为 0Mbps～63Mbps，默认为 0，不限速。

步骤3　单击“保存”。

配置举例

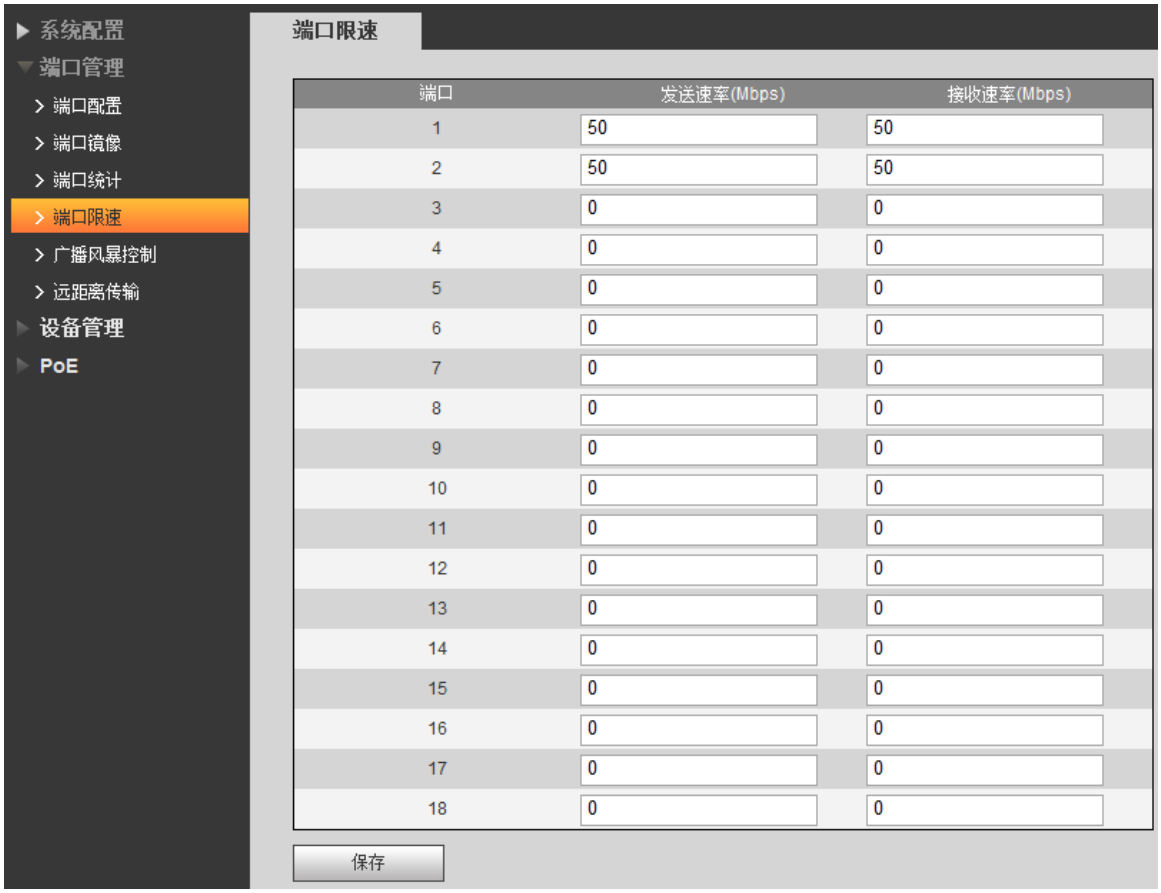
组网需求

配置端口 1 和端口 2 的限速功能，使其单端口速率在 50Mbps 以下。

配置步骤

步骤1　设置要限制端口 1 和 2 的收发速率均为“50”，如图 5-6 所示。

图5-6 配置端口限速



步骤2　单击“保存”。

5.5 广播风暴控制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

步骤1　选择“系统信息 > 端口管理 > 广播风暴控制”。

系统显示“广播风暴控制”界面，如图 5-7 所示。

图5-7 广播风暴控制



步骤2　设置阈值，阈值是指单端口一定时间内可通过的广播包数量。

步骤3　单击“保存”。

配置举例

组网需求

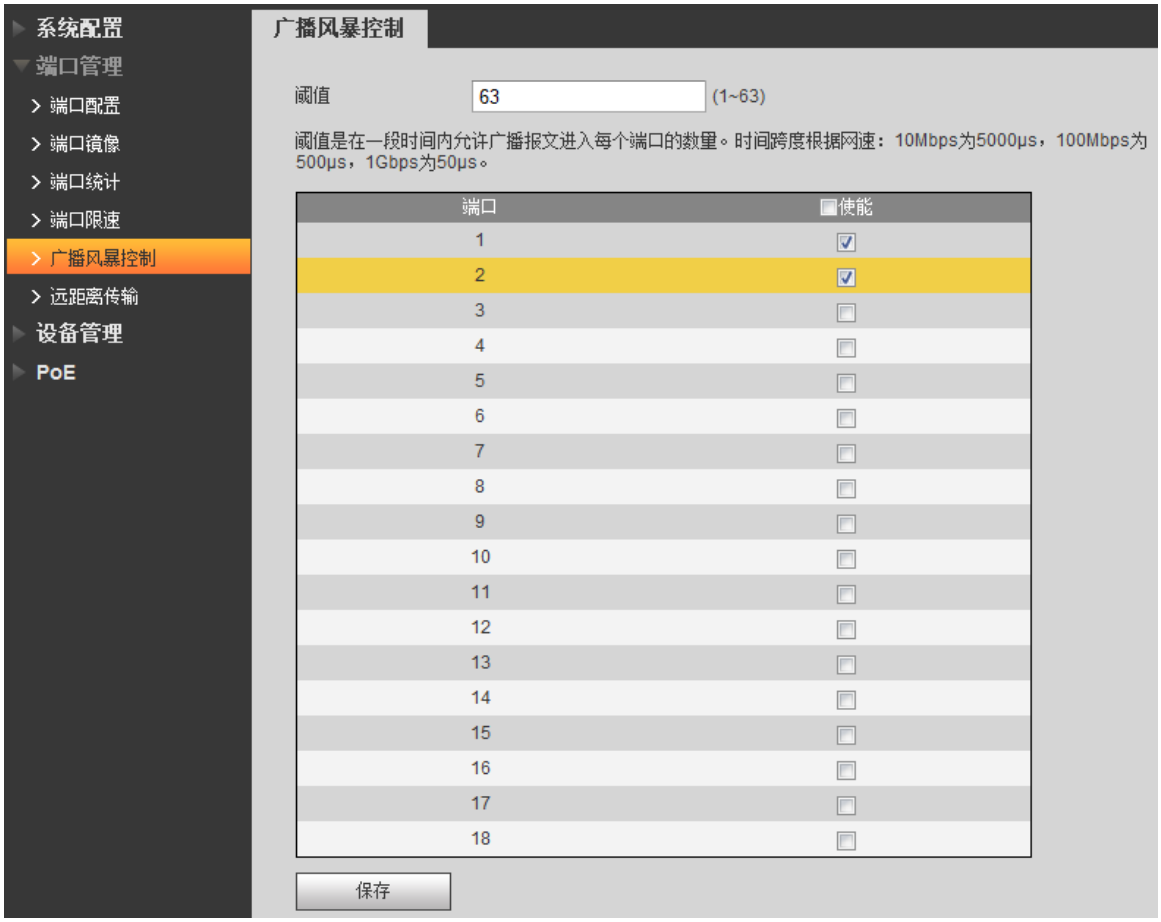
开启全端口多播风暴抑制功能，防止因产生环路导致设备无法转发正常数据报文，并设置单端口一定时间内可通过的广播包数量为 63。

配置步骤

步骤1　设置“阈值”为“63”，如图 5-8 所示。

步骤2　选择需要配置的端口。

图5-8 配置广播风暴控制



步骤3　单击“保存”。

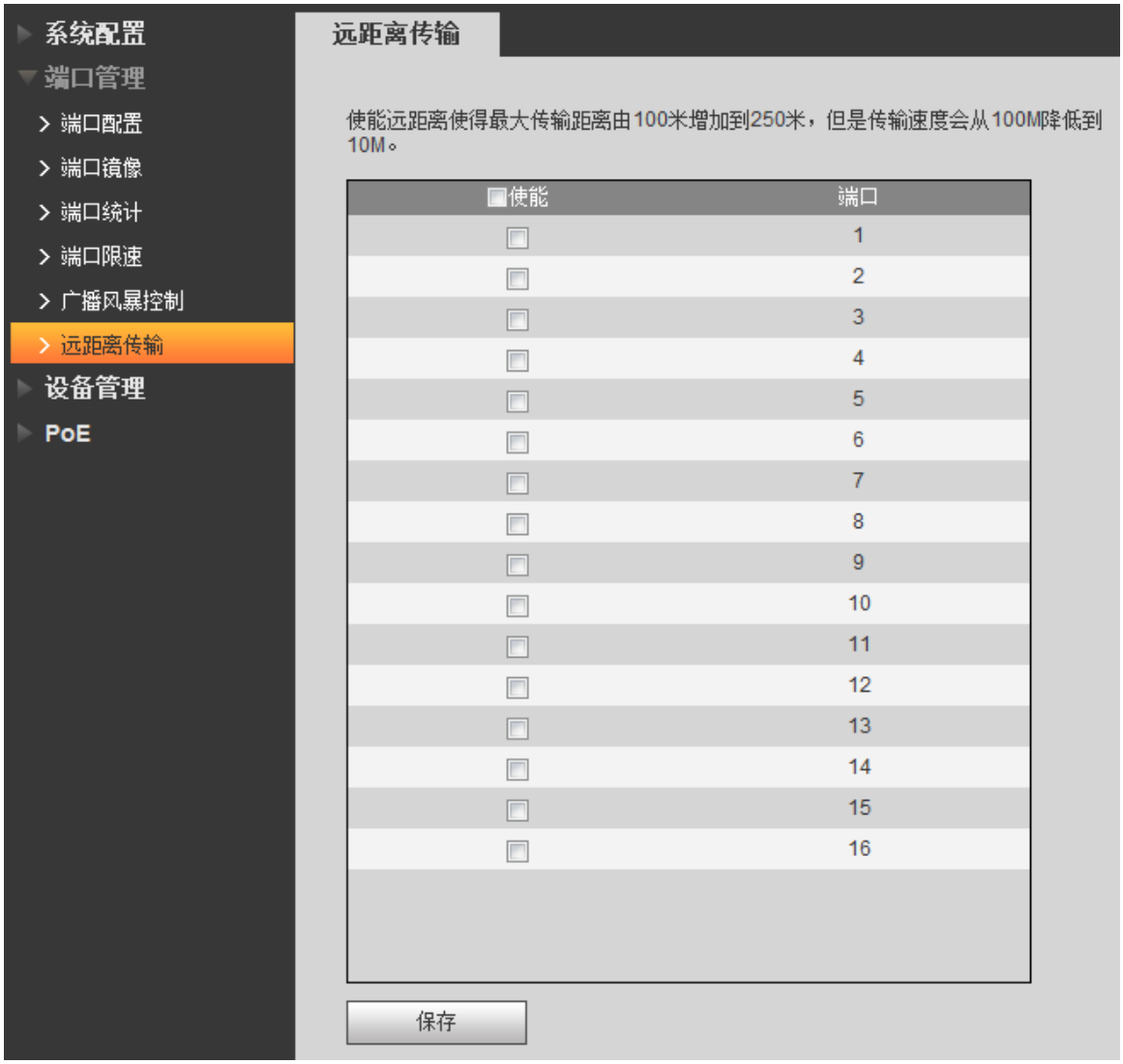
5.6 远距离传输

您可以选择需要的端口开启远距离传输模式，传输标准由原来的标准以太网模式 100 米可以传输 100M 速率，变为远距离模式 200 米可以传输 10M 速率。

步骤1　选择“系统信息 > 端口管理 > 远距离传输”。

系统显示“远距离传输”界面，如图 5-9 所示。

图5-9 远距离传输



步骤2　单击“保存”。

6 设备管理

6.1 环网

6.1.1 生成树定义

STP 协议的基本思想十分简单。自然界中生长的树是不会出现环路的，如果网络也能够像一棵树一样生长就不会出现环路。于是，STP 协议中定义了根桥（Root Bridge）、根端口（Root Port）、指定端口（Designated Port）、路径开销（Path Cost）等概念，目的就在于通过构造一棵树的方法达到裁剪冗余环路的目的，同时实现链路备份和路径最优化。用于构造这棵树的算法称为生成树算法（Spanning Tree Algorithm）。

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，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。STP 即是通过在设备之间传递 BPDU 来确定网络的拓扑结构。

BPDU 格式及字段说明要实现生成树的功能，交换机之间传递 BPDU 报文实现信息交互，所有支持 STP 协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。标准生成树的 BPDU 帧格式及字段说明如图 6-1 所示。

图6-1 BPDU 帧格式

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

- Protocol Identifier：协议标识。
- Version：协议版本。
- Message Type：BPDU 类型。
- Flag：标志位。
- Root ID：根桥 ID，由两字节的优先级和 6 字节 MAC 地址构成。
- Root Path Cost：根路径开销。
- Bridge ID：桥 ID，表示发送 BPDU 的桥的 ID，由 2 字节优先级和 6 字节 MAC 地址构成。
- Port ID：端口 ID，标识发出 BPDU 的端口。
- Message Age：BPDU 生存时间。
- Max Age：当前 BPDU 的老化时间，即端口保存 BPDU 的最长时间。
- Hello Time：根桥发送 BPDU 的周期。
- Forward Delay：表示在拓扑改变后，交换机在发送数据包前维持在监听和学习状态的时间。

6.1.2 生成树的基本概念

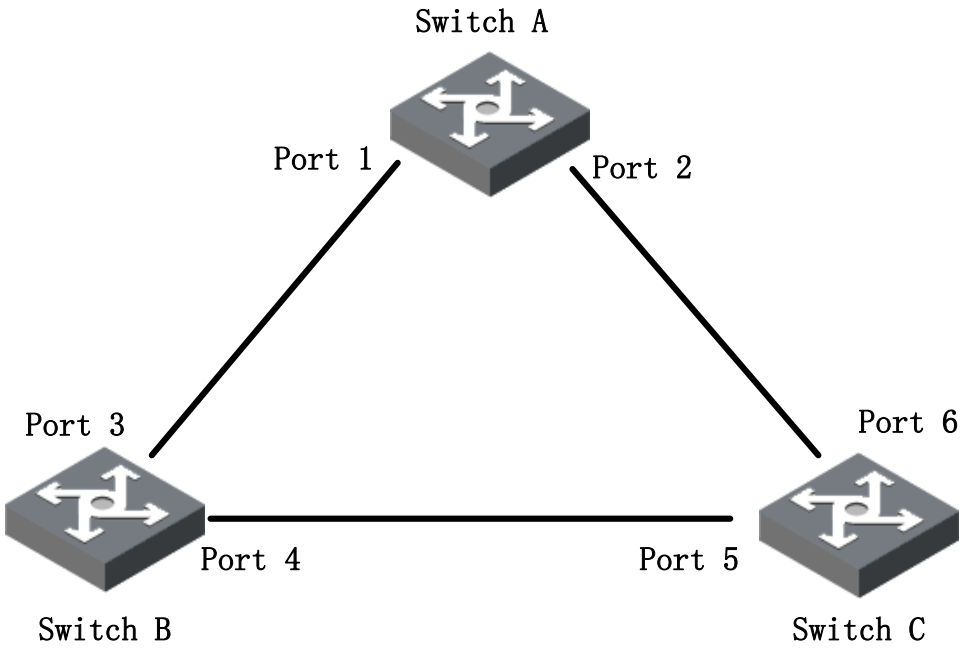
- 桥 ID（Bridge Identifier）：桥 ID 是桥的优先级和其 MAC 地址的综合数值，其中桥优先级是一个可以设定的参数。桥 ID 越低，则桥的优先级越高，这样可以增加其成为根桥的可能性。

- 根桥（Root Bridge）：具有最小桥 ID 的交换机是根桥。请将环路中所有交换机当中最好的一台设置为根桥交换机，以保证能够提供最好的网络性能和可靠性。
- 指定桥（Designated Bridge）：在每个网段中，到根桥的路径开销最低的桥将成为指定桥，数据包将通过它转发到该网段。当所有的交换机具有相同的根路径开销时，具有最低的桥 ID 的交换机会被选为指定桥。
- 根路径开销（Root Path Cost）：两个网桥间路径上所有的路径开销之和。根桥的根路径开销是零。
- 桥优先级（Bridge Priority）：是一个用户可以设定的参数，数值范围从 0 到 61440。设定的值越小，优先级越高。交换机的桥优先级越高，才越有可能成为根桥。
- 根端口（Root Port）：非根桥的交换机上离根桥最近的端口，负责与根桥进行通信，这个端口到根桥的路径开销最低。当多个端口具有相同的到根桥的路径开销时，具有最高端口优先级的端口会成为根端口。
- 指定端口（Designated Port）：指定桥上向本交换机转发数据的端口。
- 端口优先级（Port Priority）：数值范围从 0 到 240，且必须是 16 的整数倍。端口优先级值越小，表示优先级越高，才越有可能成为根端口。
- 路径开销（Path Cost）：STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

生成树基本概念的组网示意图如图 6-2 所示。交换机 A、B、C 三者顺次相连，经 STP 计算过后，交换机 A 被选为根桥，端口 2 和端口 6 之间的线路被阻塞。

- 桥：交换机 A 为整个网络的根桥；交换机 B 是交换机 C 的指定桥。
- 端口：端口 3 和端口 5 分别为交换机 B 和交换机 C 的根端口；端口 1 和端口 4 分别为交换机 A 和交换机 B 的指定端口；端口 6 为交换机 C 的阻塞端口。

图6-2 生成树组网示意图



STP 定时器

- 联络时间（Hello Time）

数值范围从 1 秒到 10 秒。是指根桥向其它所有交换机发出 BPDU 数据包的时间间隔，用于交换

机检测链路是否存在故障。

- 老化时间（Max Age）

数值范围从 6 秒到 40 秒。如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。

- 传输时延（Forward Delay）

数值范围从 4 秒到 30 秒。是指交换机的端口状态迁移所用的时间。

当网络故障引发生成树重新计算时，生成树的结构将发生相应的变化。但是重新计算得到的新配置消息无法立刻传遍整个网络，如果端口状态立刻迁移的话，可能会产生暂时性的环路。为此，生成树协议采用了一种状态迁移的机制，新的根端口和指定端口开始数据转发之前要经过 2 倍的传输时延，这个延时保证了新的配置消息已经传遍整个网络。

说明

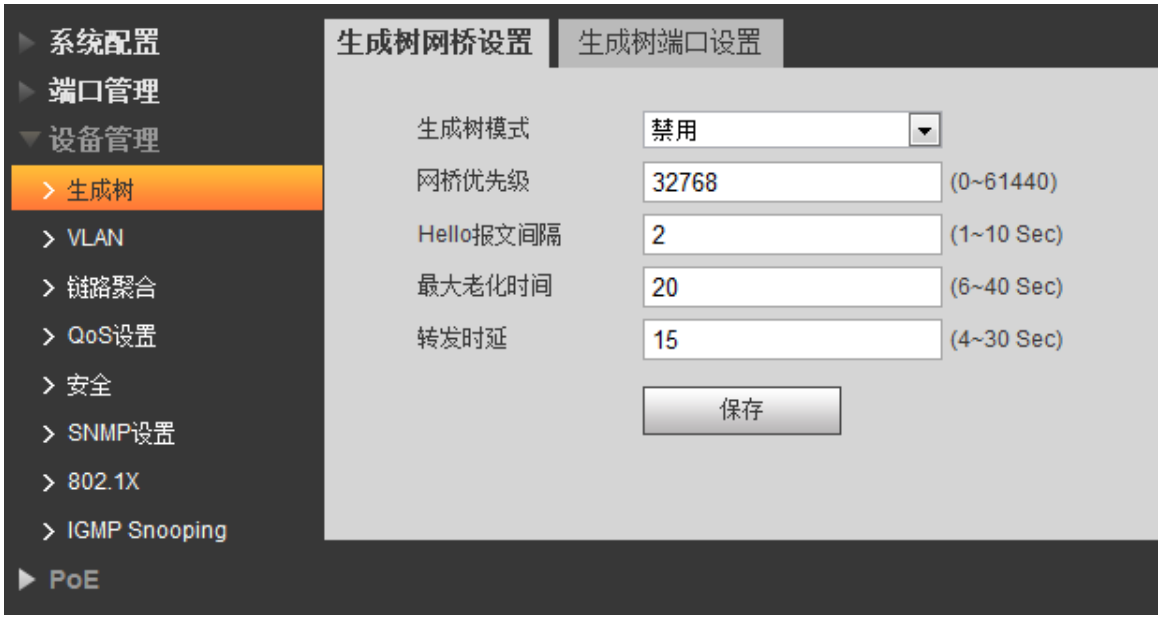
在拓扑稳定状态，只有根端口和指定端口转发数据，其它的端口都处于阻塞状态，它们只接收 BPDU 报文而不转发数据。

6.1.3 生成树设置

步骤1　选择“系统信息 > 设备管理 > 生成树 > 生成树网桥设置”。

系统显示“生成树网桥设置”界面，如图 6-3 所示。

图6-3 生成树网桥设置



步骤2　设置参数，请参见表 6-1。

表6-1 生成树网桥设置参数说明

参数	说明
生成树模式	设置生成树模式，包括禁用、STP 和 RSTP。
网桥优先级	设置桥优先级。
Hello 报文间隔	设置根桥发送 BPDU 的周期。
最大老化时间	设置当前 BPDU 的老化时间。
转发延时	设置拓扑变化后，桥维持监听和学习状态的时间。

步骤3　单击“保存”。

6.1.4 STP 端口设置

步骤1　选择“系统信息 > 设备管理 > 生成树 > 生成树端口设置”。

系统显示“生成树端口设置”界面，如图 6-4 所示。

图6-4 生成树端口设置



步骤2　设置参数，请参见表 6-2。

表6-2 生成树端口设置参数说明

参数	说明
端口号	选择您想要配置的端口。
优先级	配置端口优先级，必须为 16 的倍数。
根路径开销	配置当前选择端口到达根桥的路径开销，设置为 0 时为默认路径开销。

步骤3　单击“保存”。

6.2 VLAN 配置

6.2.1 VLAN 定义

在逻辑上将一个局域网 LAN 划分成多个子集，每个子集形成各自的广播域，即虚拟局域网 VLAN。简单地说，VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。

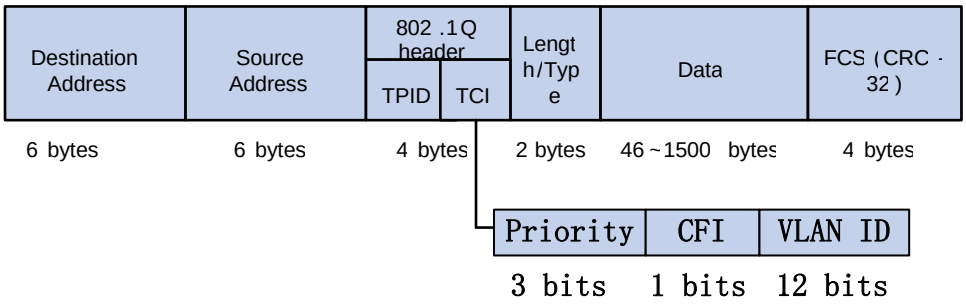
6.2.2 VLAN 作用

- 提高网络性能。将广播包限制在 VLAN 内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。
- 增强网络安全。不同 VLAN 的设备不能互相访问，不同 VLAN 的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

6.2.3 基于接口的划分 VLAN

在交换机处理的报文中会涉及到 tag 和 untag 的报文。标签的位置在如图 6-5 中蓝色位置。

图6-5 标签的位置



untag 就是普通的 ethernet 报文，普通 PC 机的网卡是可以识别这样的报文进行通讯。

tag 报文结构的变化是在源 MAC 地址和目的 MAC 地址之后，加上了 4bytes 的 vlan 信息，也就是 vlan tag 头，上图中的蓝色部分；一般来说这样的报文普通 PC 机的网卡是不能识别的，交换机就是凭借这 vlan tag 头信息来区分属于哪个 VLAN 的，使得不同 VLAN 之间不能通信，但是有时候又需要不同 VLAN 之间进行通信，所以就有了不同的端口类型来使得不同 vlan 之间可以通信。

端口类型

端口类型包括 Access 类型、Trunk 类型和 Hybrid 类型三种。

Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口。

Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口。

Hybrid 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

接口配置了链路类型和缺省 VLAN 后对收发报文的处理方法如表 6-3 所示。

表6-3 对收发报文的处理方法

端口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	对发送报文的处理
Access	接收该报文，并打上缺省 VLAN 的 Tag。	当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文。当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。	去掉 Tag，发送该报文。

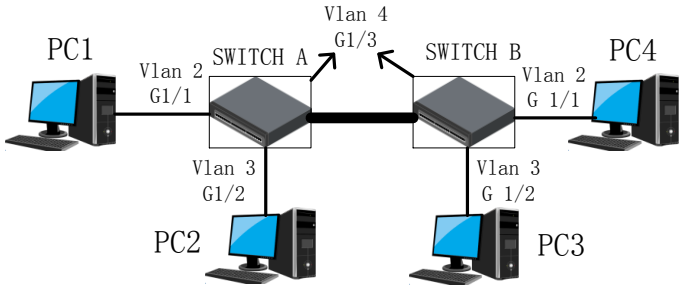
端口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	对发送报文的处理
Trunk	打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文并打上缺省 VLAN 的 Tag。 打上缺省的 VLAN ID，当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收 该报文。 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 与缺省 VLAN ID 相同时，且是该接口允许通过的 VLAN ID 时：去掉 Tag， 发送该报文。 当 VLAN ID 与缺省 VLAN ID 不同时，且是该接口允许通过的 VLAN ID 时：保持原有 Tag，发送该报文。
Hybrid			当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。 可以通过 port hybrid untagged/tagged vlan 设置发送时是否携带 Tag。

配置举例

组网需求

如图 6-6 所示，PC1 和 PC4 属于一个部门，PC2 和 PC3 属于一个部门，部门之内可以互相通信，部门之间不能通信。

图6-6 VLAN 组网



硬件连接

- PC1 连 SWITCH A 端口 G1/1，PC2 连 SWITCH A 端口 G1/2。
- PC3 连 SWITCH B 端口 G1/2，属于 vlan3，PC4 连 SWITCH B 端口 G1/1，属于 vlan2。
- SWITCH A 和 SWITCH B 由各自端口 G1/3 相连。

配置步骤

SWITCH A：端口 G1/1 属于 Vlan2，配置成 Access 口，G1/2 属于 Vlan3，配置成 Access 口，G1/3 配置成 trunk 口，属于 Vlan4，允许 Vlan2，3，4 通过。

步骤1　选择“系统信息 > 设备管理 > VLAN > 端口 VLAN 设置”。

系统显示“端口 VLAN 设置”界面，如图 6-7 所示。

步骤2　端口 1 的“端口类型”、“端口所属 VLAN”分别设置为“Access”和“2”。

步骤3　端口 2 的“端口类型”、“端口所属 VLAN”分别设置为“Access”和“3”。

步骤4　端口 3 的“端口类型”、“端口所属 VLAN”、“出接口打 tag”和“允许 VLAN”分别设置

为“Trunk”、“4”、“Untag Port VLAN”和“1”。

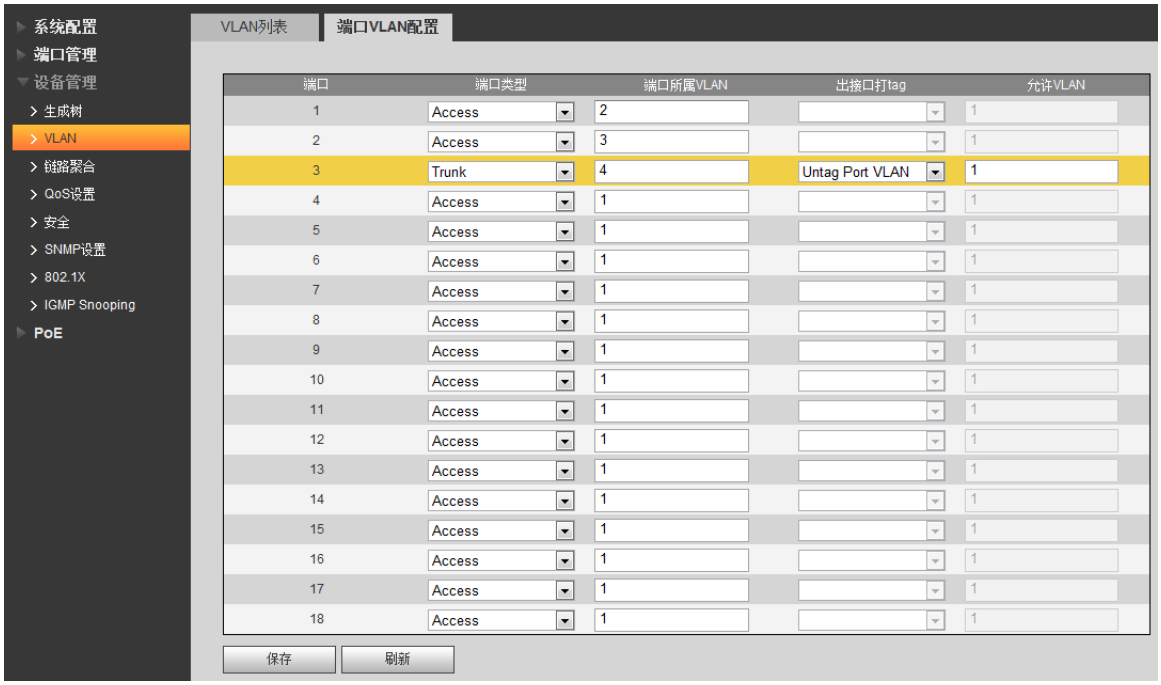
步骤5　单击“保存”。

SWITCH B：端口 G1/1 属于 Vlan2，配置成 Access 口，G1/2 属于 Vlan3 ，配置成 Access 口，G1/3 配置成 trunk 口，属于 Vlan4，允许 Vlan2，3，4 通过。

SWITCH B 的配置同 SWITCH A 一样，不再赘述。

配置结果如图 6-7 所示。

图6-7 端口 VLAN 配置



6.3 链路聚合

链路聚合是将交换机的多个物理端口形成一个逻辑端口，属于同一汇聚组内的多条链路可视为一条更大带宽逻辑链路。

链路聚合可以实现通信流量在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了链路的可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、VLAN、端口属性、MAC 地址学习、镜像、802.1x、MAC 过滤等。

说明

不建议用于链路汇聚的端口，进行端口及高级功能方面的配置。

链路聚合分为静态聚合和 LACP，与交换机链路聚合的对端设备一般是交换机、网卡。

6.3.1 静态聚合模式

静态聚合模式允许在聚合组中手工加入多个成员接口，所有的接口均处于转发状态，分担负载的流量。聚合组的创建、成员接口的加入都需要手工配置完成，没有 LACP 协议报文的参与。

步骤1　选择“系统信息 > 设备管理 > 链路聚合”。

系统显示“链路聚合”界面，如图 6-8 所示。

图6-8 链路聚合



步骤2　设置链路聚合模式，请参见表 6-4。

表6-4 链路聚合模式

链路聚合模式	说明
源 MAC	基于报文的源 MAC 地址进行链路聚合计算
目的 MAC	基于报文的目的 MAC 地址进行链路聚合计算
源 MAC 和目的 MAC	基于报文的源和目的 MAC 地址进行链路聚合计算

步骤3　单击“保存”。

步骤4　设置其他参数，请参见表 6-5。

表6-5 链路聚合参数说明

参数	说明
链路组 1、链路组 2、链路组 3	聚合组是一组以太网端口的集合，默认支持的聚合组数为 3 组不可修改，所有聚合组默认状态为非使能，端口成员默认为空。
成员端口	交换机默认创建了所有聚合组，端口成员为空，要为聚合组配置成员端口，首先使能聚合组，然后选择端口所在的聚合组，即可使能聚合功能。
状态	包括启用和禁用。
类型	包括 LACP 和静态。
操作 key	设置操作 key。
超时	包括长超时和短超时。
活动模式	包括被动和主动。

步骤5　单击“提交”。

6.3.2 LACP 模式

LACP 是基于 IEEE 802.3ad 标准用来实现链路动态汇聚与拆汇聚的协议。汇聚设备双方通过 LACPDU 报文交互汇聚信息，将匹配的链路汇聚在一起收发数据，汇聚组内端口的添加和删除是协议自动完成的，具有很高的灵活性并提供了负载均衡的能力。

启用端口的 LACP 功能后，该端口向对端通告本端的系统优先级、系统 MAC、端口优先级、端口号和操作 Key（由端口的物理属性、上层协议信息和管理 Key 决定）。

设备优先级高的一端将主导汇聚及拆汇聚，设备优先级由系统优先级和系统 MAC 决定，系统优先级值小的设备优先级高，系统优先级值相同时系统 MAC 较小的设备优先级高。设备优先级高

的一端将根据端口优先级、端口号以及操作 Key 选择汇聚端口，操作 Key 相同的端口才能被选入同一个汇聚组，同一个汇聚组内端口优先级值小的端口会被优先选择，当端口优先级相同的时候，端口号小的会被优先选择。双方交互汇聚信息后被选择的端口将汇聚在一起收发数据。

LACP 协议的配置参数主要包括：端口 LACP 功能使能、键值、活跃（主动/被动模式）、超时配置。

只有开启 LACP 协议的端口才会进行 LACP 协商，从而有可能形成汇聚链路。密钥是协商的基础，具有相同密钥的端口才能协商组成一个汇聚链路。协商模式“active | passive”，当选择“active”，设备会主动发起汇聚协商；当选择“passive”，设备被动接受其他设备发起的汇聚协商。两台设备互联，至少有一端或两端需设置成“active”模式才能协商成功。

- 键值：同一汇聚组的成员，需配置相同的操作 Key，范围 1～65535。
- 活跃：默认 Active 可选项为 Active 和 Passive，参与动态汇聚的设备一端要选配 Active 模式，另一端要配置 Passive 模式。
- 超时：默认 Long Timeout，可选项为 Long Timeout 和 Short Timeout，分别表示长超时和短超时。

配置举例

组网需求

因单千兆链路上行存在隐患，所以需求通过链路聚合功能实现链路备份，实现双千兆链路上行。

配置步骤

步骤1　选择“系统信息 > 设备管理 > 链路聚合”。
　　系统显示“链路聚合”界面，如图 6-8 所示。

步骤2　选择链路组 3，选择成员端口 p17 和成员端口 p18。

步骤3　选择“类型”为“LACP”。

步骤4　选择“活动模式”为“主动”。

步骤5　单击“提交”应用配置。

步骤6　选择链路聚合模式为“源 MAC 和目的 MAC”，配置结果如图 6-9 所示。
　　聚合成功相应的端口下会显示为“ √ ”。

图6-9 链路聚合



6.4 QoS 设置

QoS（Quality of Service，服务质量）用于评估服务方满足客户服务需求的能力。在 Internet 中，QoS 所评估的就是网络转发分组的服务能力。

由于网络提供的服务是多样的，因此 QoS 的评估可以基于不同方面。通常所说的 QoS，是对分组转发过程中带宽、延迟、抖动、丢包率等指标进行评估。

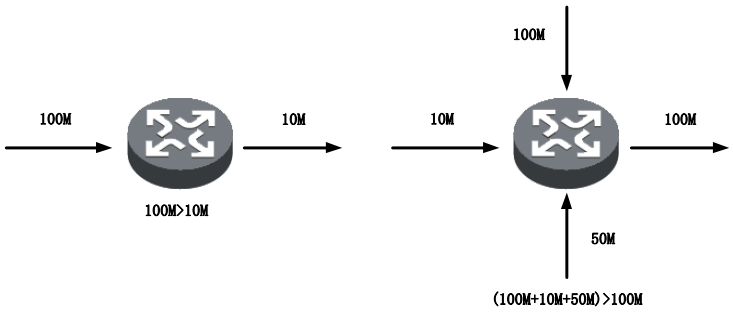
在传统的无 QoS 保障的 IP 网络中，设备无区别地对待所有的报文，设备处理报文采用的策略是 FIFO（First In First Out，先入先出），它依照报文到达时间的先后顺序分配转发所需要的资源。所有报文共享网络和设备的资源，至于得到资源的多少完全取决于报文到达的时间。这种服务策略称作 Best-Effort，它尽最大的努力将报文送到目的地，但对分组转发的延迟、抖动、丢包率等需求不提供任何承诺和保证。

传统的 Best-Effort 服务策略只适用于对带宽、延迟不敏感的 WWW、E-Mail 等业务。但是新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，还希望在转发过程中得到更好的服务，诸如为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量。所有这些都要求网络具备更为完善的服务能力。

6.4.1 网络拥塞

在复杂的 Internet 分组交换环境下，拥塞极为常见。以图 6-10 中的两种情况为例。

图6-10 网络拥塞



- 分组流从高速链路进入设备，由低速链路转发出去。
- 分组流从多个接口同时进入网络设备，由一个接口转发出去（多个接口的速率和大于出接口的速率）。

如果流量以线速到达，那么就会遭遇资源的瓶颈而导致拥塞。

不仅仅是链路带宽的瓶颈会导致拥塞，任何用于正常转发处理的资源的不足（如可分配的处理器时间、缓冲区、内存资源的不足）都会造成拥塞。此外，在某个时间内对所到达的流量控制不力，使之超出了可分配的网络资源，也是引发网络拥塞的一个因素。

拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和抖动，过高的延迟会引起报文重传。
- 拥塞使网络的有效吞吐率降低，造成网络资源的利用率降低。
- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。

可见，拥塞使流量不能及时获得资源是造成服务性能下降的源头。在分组交换以及多用户业务并存的复杂环境下，拥塞又是不可避免的，因此必须采用适当的方法来解决拥塞。

6.4.2 拥塞解决办法

增加网络带宽是解决资源不足的一个直接途径，然而网络带宽不可能无限制的增加，因此它并不能解决所有导致网络拥塞的问题。

解决网络拥塞问题的一个更有效的办法是在网络中增加流量控制和资源分配的功能，为有不同服务需求的业务提供有差别的服务，更合理地分配和使用资源。在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，从而减少拥塞发生的概率；在拥塞发生时，依据业务的性质及其需求权衡资源的分配，将拥塞的影响减到最小。

6.4.3 队列调度

对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

本产品支持两个等级的优先级队列，包括高优先级队列和低优先级队列。每个数据包的优先级设定基于以下四种方案：

1. 基于物理端口
2. 基于 802.1Q VLAN tag
3. 基于 IP 报文中的 TOS/DS 字段
4. 基于 TCP/UDP 端口

当多种 QoS 配置存在时，只要有一个优先级配置项被设置为高则此方案就会被放置在高优先级队列中进行转发。当多种同等级优先级存在时，则在同等级的优先级之间会以先入先出模式转发。

6.4.4 优先级模式

每个收到的报文会被映射到一个高优先级或者低优先级，报文的优先级配置分为三个模式。

步骤1　选择“系统信息 > 设备管理 > QoS 设置 > 优先级模式”。

系统显示“优先级模式”界面，如图 6-11 所示。

图6-11 优先级模式



步骤2　设置优先级模式，包括如下：

- 先进先出模式，设备会以先收到的报文先转发的方式处理，当 QoS 功能没有开启时，设备会以报文先进先出的模式工作。
- 严格优先级模式，设备会根据实际配置的高低优先级去转发报文。
- 权重轮循模式，通过修改权重等级来控制高优先级队列和低优先级队列中报文的转

发比重。

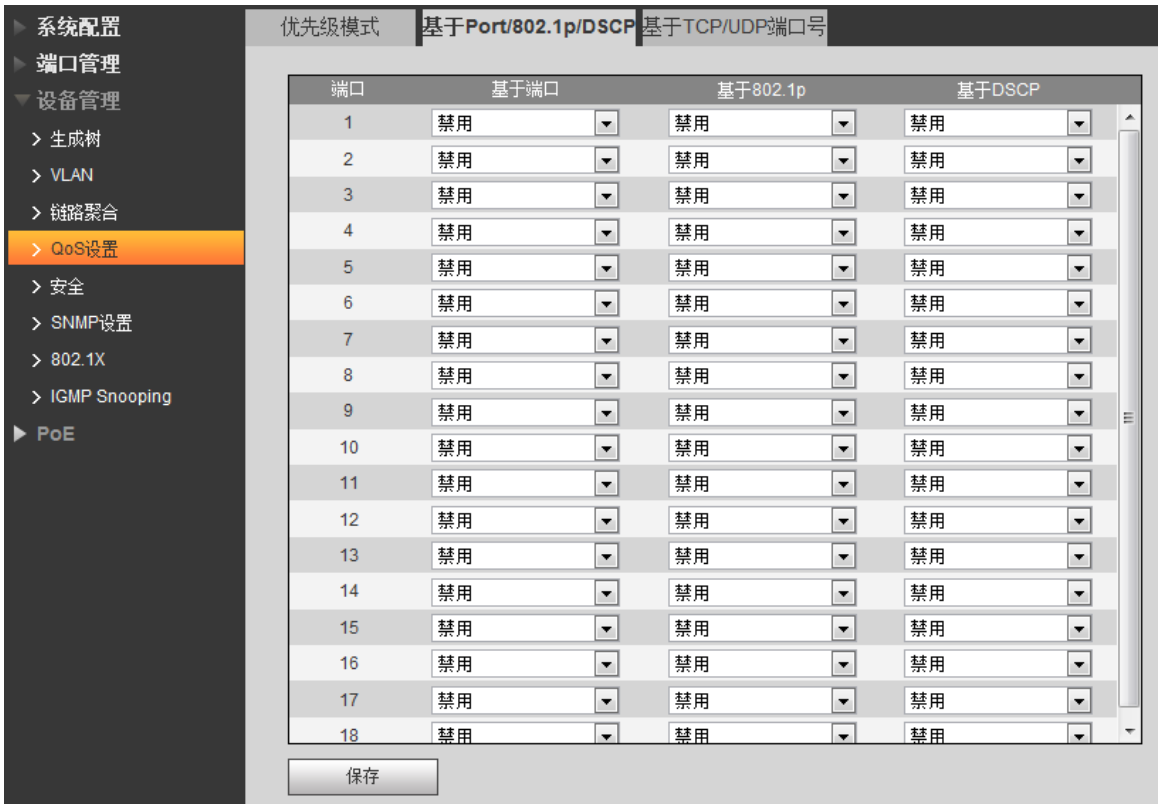
步骤3　单击“保存”。

6.4.5 基于 Port/802.1p/DSCP 的 QoS

选择“系统信息 > 设备管理 > QoS 设置 > 基于 Port/802.1p/DSCP”。

系统显示“基于 Port/802.1p/DSCP”界面，如图 6-12 所示。

图6-12 基于 Port/802.1p/DSCP



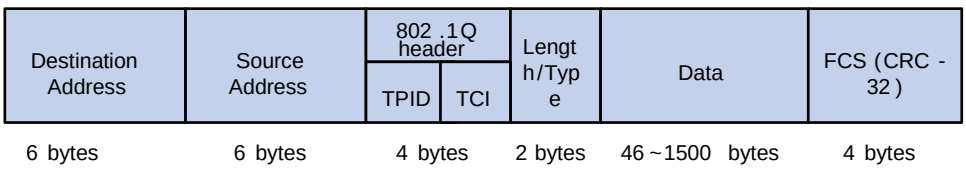
基于 Port

当端口（Port）被设置为高优先级，则收到的报文会被放置到高优先级队列。每个端口都可以被设置为高优先级。

基于 802.1p

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。

图6-13 802.1Q 标签头



如图 6-13 所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID（Tag Protocol Identifier，标签协议标识符）和 2 个字节的 TCI（Tag Control Information，标签控制信息），TPID 取值为 0x8100。

图 6-14 显示了 802.1Q 标签头的详细内容，Priority 字段就是 802.1p 优先级。之所以称此优先级为 802.1p 优先级，是因为有关这些优先级的应用是在 802.1p 规范中被详细定义的。

图6-14 802.1Q 标签头详细内容

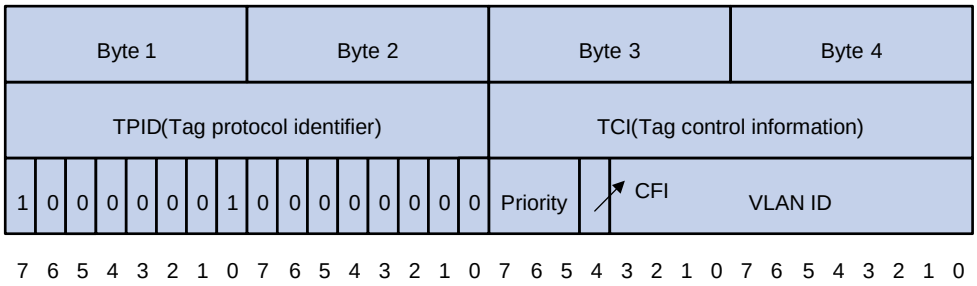
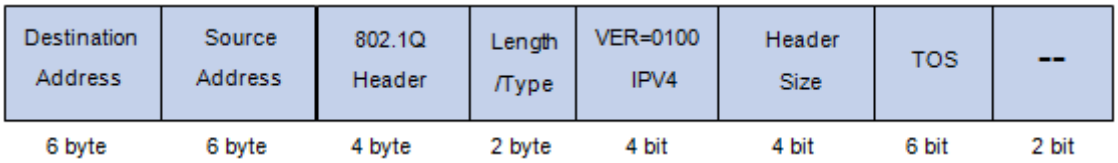


表6-6 802.1p 优先级说明

优先级队列	802.1p 优先级（十进制）	802.1p 优先级（二进制）	关键字
低优先级队列	0	000	best-effort
	1	001	background
	2	010	spare
	3	011	excellent-effort
高优先级队列	4	100	controlled-load
	5	101	video
	6	110	voice
	7	111	network-management

基于 DSCP

图6-15 ToS



如图 6-15 所示，IP 报文头的 ToS 字段有 8 个 bit，RFC 2474 中，重新定义了 IP 报文头部的 ToS 域，称之为 DS（Differentiated Services，差分服务）域，其中 DSCP 优先级用该域的前 6 位（0～5 位）表示，取值范围为 0～63，后 2 位（6、7 位）是保留位。

表6-7 IP 优先级说明

优先级队列	IP 优先级（十进制）	IP 优先级（二进制）	关键字
高优先级队列	46	101110	ef
	10	001010	af11
	18	010010	af21
	26	011010	af31
	34	100010	af41

优先级队列	IP 优先级（十进制）	IP 优先级（二进制）	关键字
	48	110000	cs6
	56	111000	cs7
低优先级队列	Others	xxxxxx	-

6.4.6 基于 TCP/UDP 端口号

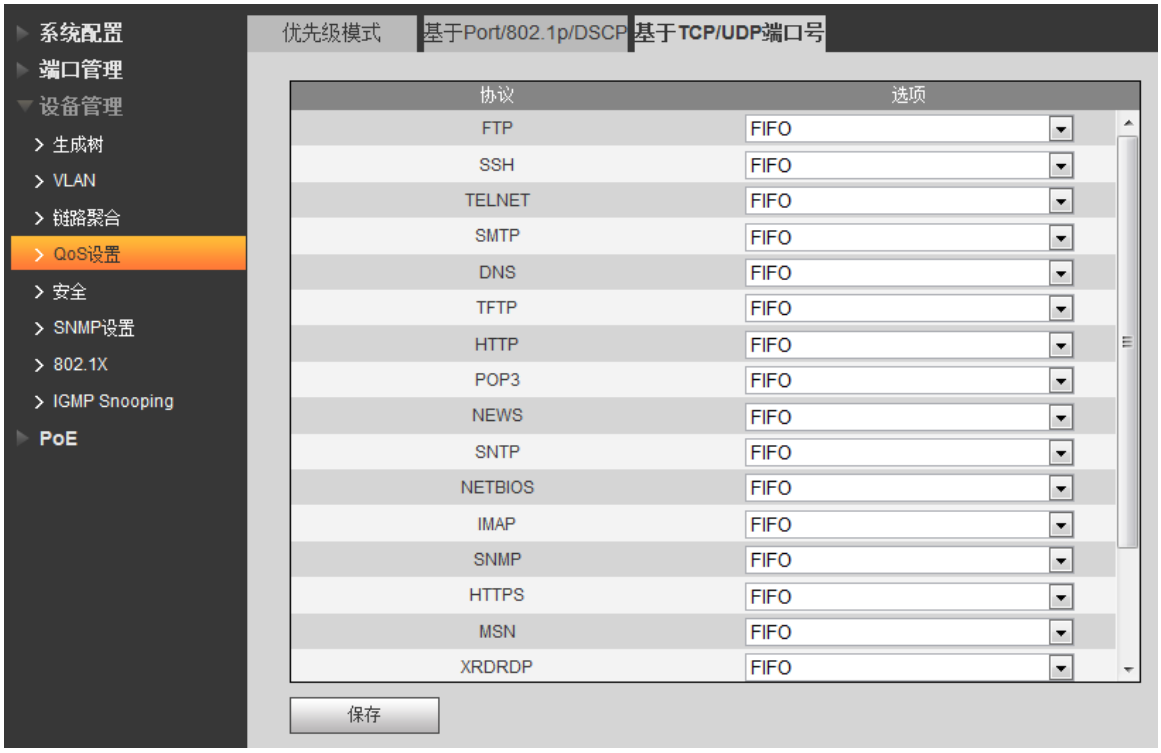
TCP 和 UDP 采用 16bit 的端口号来识别应用程序，服务器一般都是通过知名端口号来识别的。例如，FTP 服务器的 TCP 端口号都是 21，每个 Telnet 服务器的 TCP 端口号都是 23，每个 TFTP 服务器的 UDP 端口号都是 69。任何 TCP/IP 实现所提供的服务都用知名的 1-1023 之间的端口号。

本产品可以基于 TCP/UDP 端口对收到的报文进行处理，包括 FTP、SSH、TELNET、SMTP、DNS 等，您可以选择性的对报文进行设置高优先级、低优先级或者丢弃，默认为 FIFO（先入先出）模式。

选择“系统信息 > 设备管理 > QoS 设置 > 基于 TCP/UDP 端口号”。

系统显示“基于 TCP/UDP 端口号”界面，如图 6-16 所示。

图6-16 基于 TCP/UDP 端口号

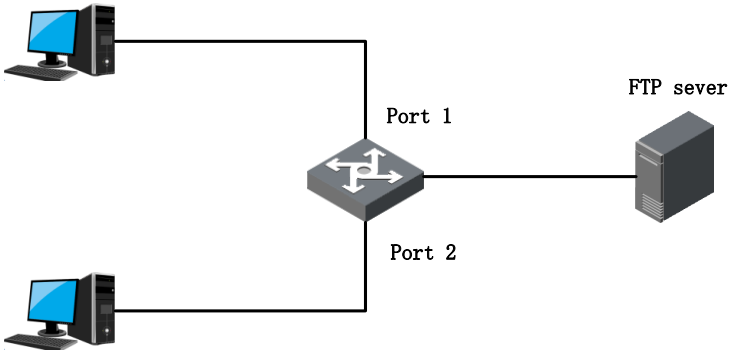


QoS 配置举例

组网需求

- 如图 6-17 所示，设备与 FTP 服务器（FTP Sever）相连，用户通过端口 1（Port1）和端口 2（Port2）接入设备。
- 要求正确配置 QoS 功能，使得端口 2（Port2）的优先级高于端口 1（Port1），并且禁止访问 FTP 服务器（FTP Sever）。

图6-17 设备与 FTP 服务器组网



配置步骤

步骤1　在“优先级”模式界面，配置设备为严格优先级模式。

1. 选择模式为“严格优先级”，如图 6-18 所示。
2. 单击“保存”。

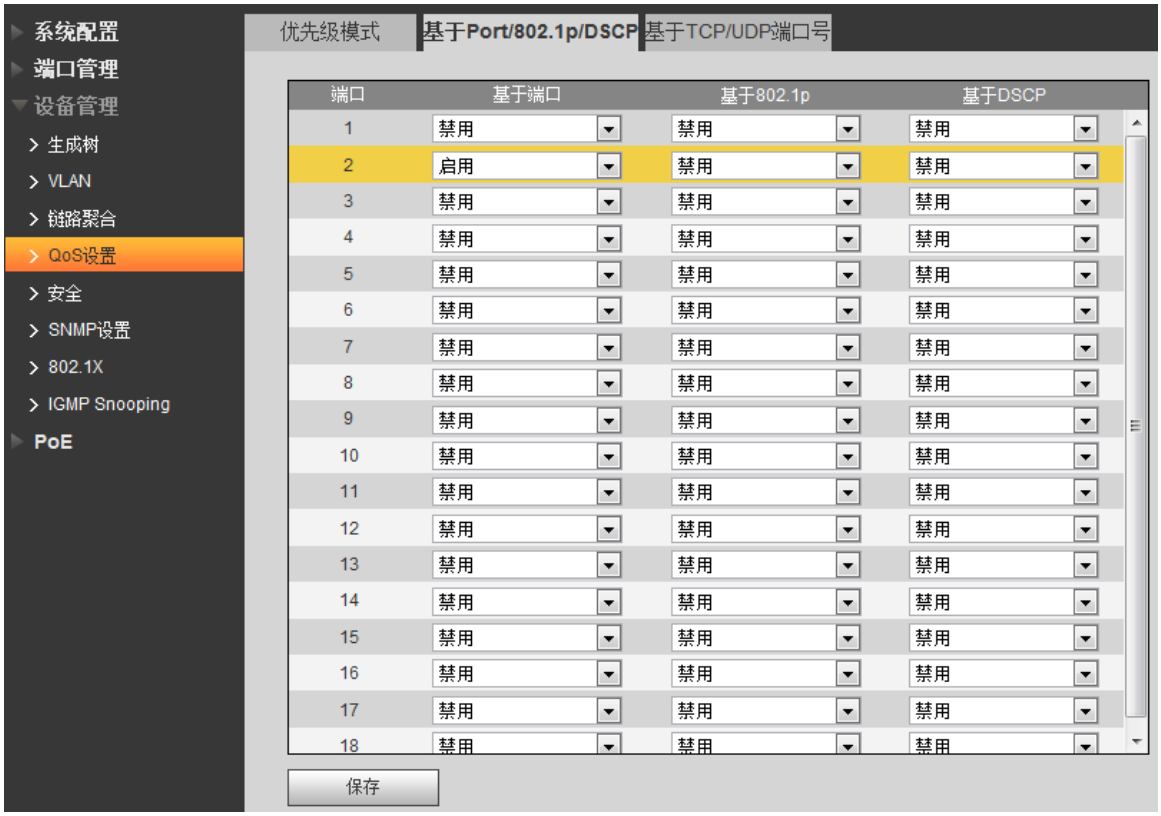
图6-18 配置设备优先级模式



步骤2　在“基于 Port/802.1p/DSCP”界面，配置端口 2 为高优先级。

1. 选择端口 2 的基于端口为“启用”，如图 6-19 所示。
2. 单击“保存”。

图6-19 配置端口优先级



步骤3 在“基于 TCP/UDP 端口号”界面，配置设备丢弃 FTP 数据包，限制用户访问 FTP Sever。

1. 选择对收到的 FTP 报文“Discard”，如图 6-20 所示。
2. 单击“保存”。

图6-20 丢弃 FTP 数据包



6.5 安全

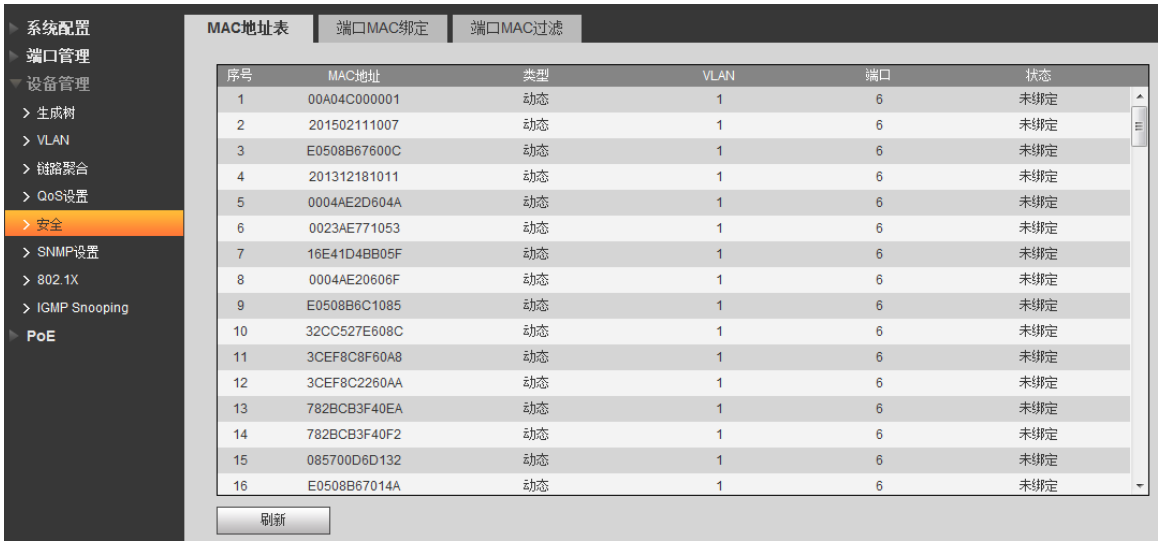
6.5.1 MAC 地址表

MAC 地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

选择“系统信息 > 设备管理 > 安全 > MAC 地址表”。

系统显示“MAC 地址表”界面，如图 6-21 所示。

图6-21 MAC 地址表



序号	MAC地址	类型	VLAN	端口	状态
1	00A04C000001	动态	1	6	未绑定
2	201502111007	动态	1	6	未绑定
3	E0508B67600C	动态	1	6	未绑定
4	201312181011	动态	1	6	未绑定
5	0004AE2D604A	动态	1	6	未绑定
6	0023AE771053	动态	1	6	未绑定
7	16E41D4BB05F	动态	1	6	未绑定
8	0004AE20606F	动态	1	6	未绑定
9	E0508B6C1085	动态	1	6	未绑定
10	32CC527E608C	动态	1	6	未绑定
11	3CEF8C8F60A8	动态	1	6	未绑定
12	3CEF8C2260AA	动态	1	6	未绑定
13	782BCB3F40EA	动态	1	6	未绑定
14	782BCB3F40F2	动态	1	6	未绑定
15	085700D6D132	动态	1	6	未绑定
16	E0508B67014A	动态	1	6	未绑定

6.5.2 端口 MAC 绑定

您可以选择当前已经连接的端口，配置端口 MAC 绑定功能，使得当前端口只能转发已经绑定 MAC 的设备。

选择“系统信息 > 设备管理 > 安全 > 端口 MAC 绑定”。

系统显示“端口 MAC 绑定”界面，如图 6-22 所示。

图6-22 端口 MAC 绑定



序号	MAC地址	类型	VLAN	端口	状态	绑定	去绑定
1	9002A909188D	动态	1	8	未绑定	绑定	去绑定
2	0200C183CBE6	动态	1	8	未绑定	绑定	去绑定

配置举例

组网需求

用户通过 WEB 网管设置端口 MAC 绑定，使得该端口只能给当前设备使用。

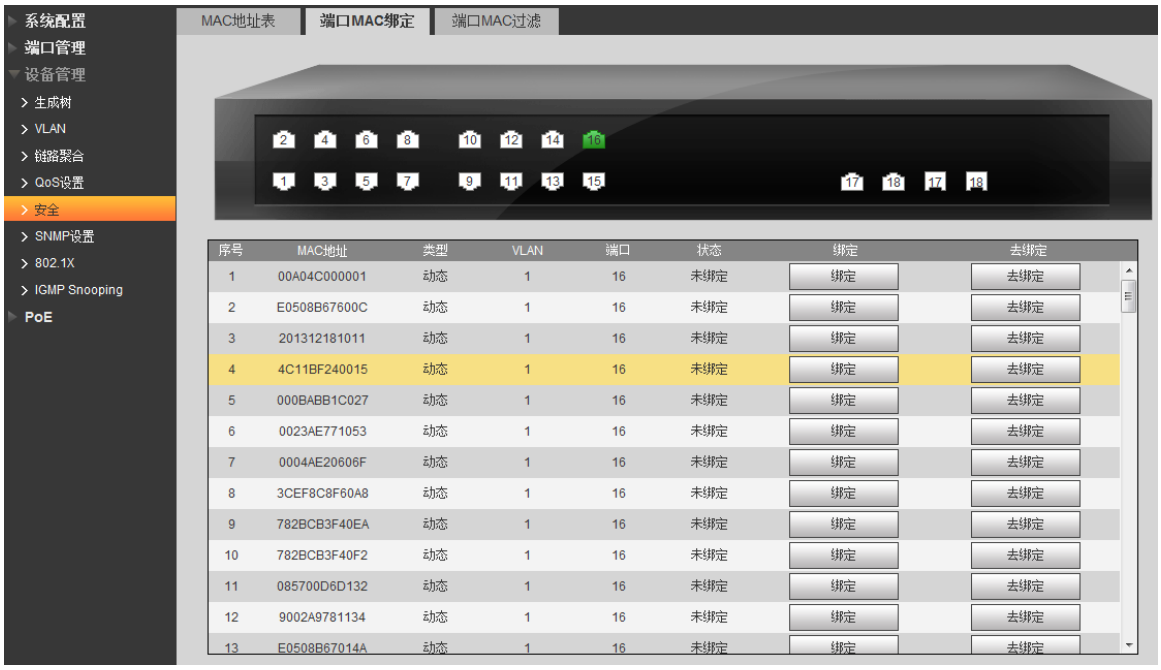
配置步骤

步骤1　选择“端口 MAC 绑定”页签。

步骤2　选择当前处于连接状态（绿色）的端口。

步骤3　单击“绑定”，如图 6-23 所示。

图6-23 端口 MAC 绑定



6.5.3 端口 MAC 过滤

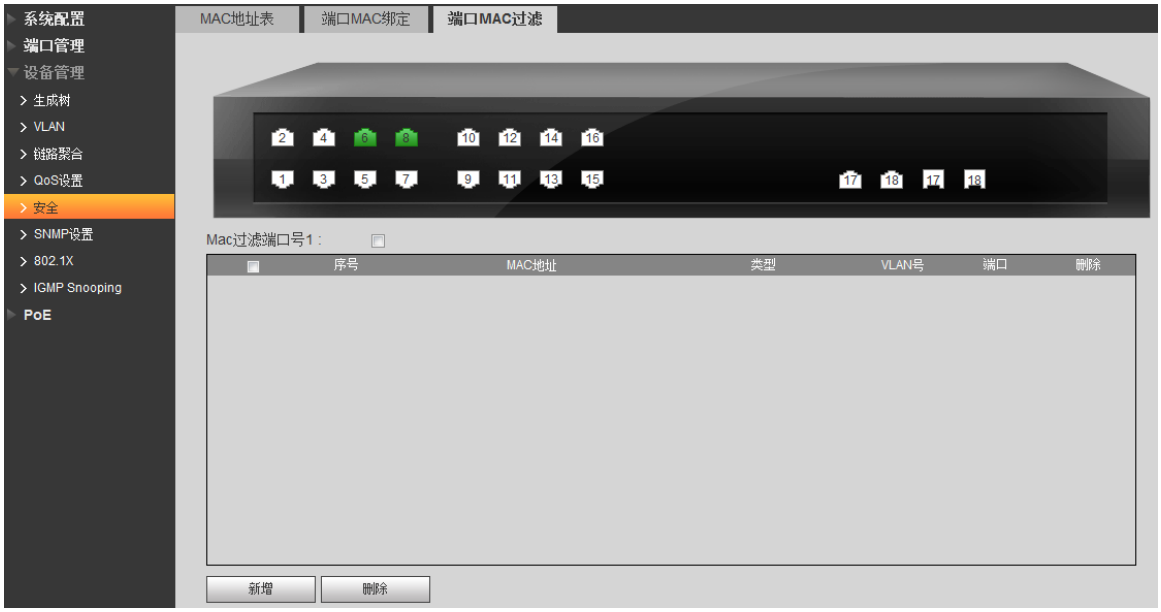
本功能用于限制端口下允许通过的 MAC 报文，可以防止仿冒用户的攻击。在端口上配置此功能后，当端口收到报文时，将检查报文的源 MAC 地址是否和允许通过的 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理。
- 如果不相同，则认为此报文非法，将其丢弃。

步骤1　选择“系统信息 > 设备管理 > 安全 > 端口 MAC 过滤”。

系统显示“端口 MAC 过滤”界面，如图 6-24 所示。

图6-24 端口 MAC 过滤



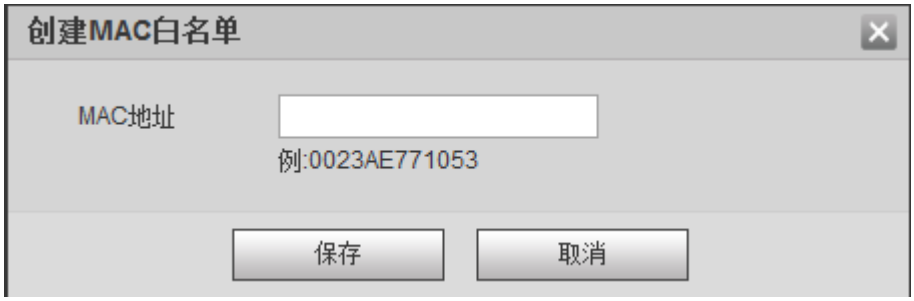
步骤2　选择当前处于连接状态（绿色）的端口。

步骤3　选择“MAC 过滤端口号 X”后的复选框，开启 MAC 过滤。

步骤4　单击“新增”。

系统显示“创建 MAC 白名单”界面，如图 6-25 所示。

图6-25 创建 MAC 白名单



步骤5　输入 MAC 地址。

步骤6　单击“保存”。

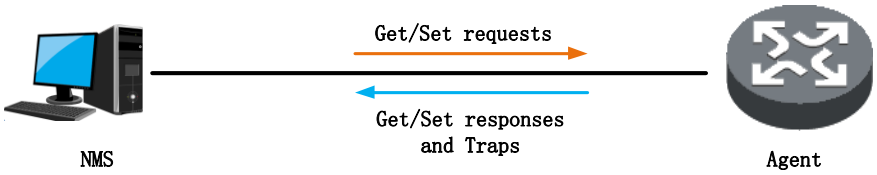
6.6 SNMP 设置

SNMP 网络包含 NMS 和 Agent 两种元素。

- NMS（Network Management System）是 SNMP 网络的管理者，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作。
- Agent 是 SNMP 网络的被管理者，负责接收、处理来自 NMS 的请求报文。在一些紧急情况下，如接口状态发生改变等，Agent 会主动向 NMS 发送告警信息。

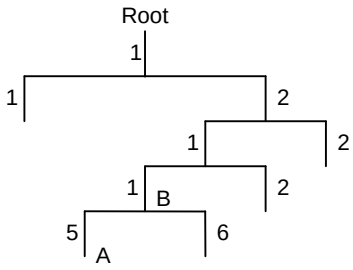
NMS 管理设备的时候，通常会对一些参数比较关注，比如接口状态、CPU 利用率等，这些参数的集合称为 MIB（Management Information Base，管理信息库）。这些参数在 MIB 中称为节点。MIB 定义了节点之间的层次关系以及对象的一系列属性，比如对象的名字、访问权限和数据类型等。每个 Agent 都有自己的 MIB。被管理设备都有自己的 MIB 文件，在 NMS 上编译这些 MIB 文件，就能生成该设备的 MIB。NMS 根据访问权限对 MIB 节点进行读/写操作，从而实现对 Agent 的管理。NMS 和 Agent 之间的关系如下图 6-26 所示。

图6-26 NMS 和 Agent 的关系



MIB 是按照树型结构组织的，它由很多个节点组成，每个节点表示被管理对象，被管理对象可以用从根开始的一串表示路径的数字唯一地识别，这串数字称为 OID（Object Identifier，对象标识符）”。如下图所示，被管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字就是被管理对象 B 的 OID。

图6-27 OID



SNMP 提供三种基本操作来实现 NMS 和 Agent 的交互：

- Get 操作：NMS 使用该操作查询 Agent MIB 中的一个或多个节点的值。
- Set 操作：NMS 使用该操作设置 Agent MIB 中的一个或多个节点的值。
- Trap 操作：Agent 使用该操作向 NMS 发送 Trap 信息。Agent 不要求 NMS 发送回应报文，NMS 也不会对 Trap 信息进行回应。SNMPv1、SNMPv2 和 SNMPv3 均支持 Trap 操作。

6.6.1 SNMP 的协议版本

目前 Agent 支持 SNMPv1、SNMPv2 和 SNMPv3 三个版本：

- SNMPv1 采用团体名（Community Name）认证机制。团体名类似于密码，用来限制 NMS 和 Agent 之间的通信。如果 NMS 设置的团体名和被管理设备上设置的团体名不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2 也采用团体名认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以设置鉴权和加密功能。鉴权用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能，可以为 NMS 和 Agent 之间的通信提供更高的安全性。

说明

NMS 和 Agent 成功建立连接的前提条件是 NMS 和 Agent 使用的 SNMP 版本必须相同。

6.6.2 SNMP 系统配置

本节对 SNMP 系统进行配置。

步骤1　选择“系统信息 > 设备管理 > SNMP”。

- 选择“SNMP”版本号为“SNMP v1”或“SNMP v2”，系统显示界面如图 6-28 所示。

- 选择“SNMP”版本号为“SNMP v3”，系统显示界面如图 6-29 所示。

图6-28 SNMP v1 和 SNMP v2

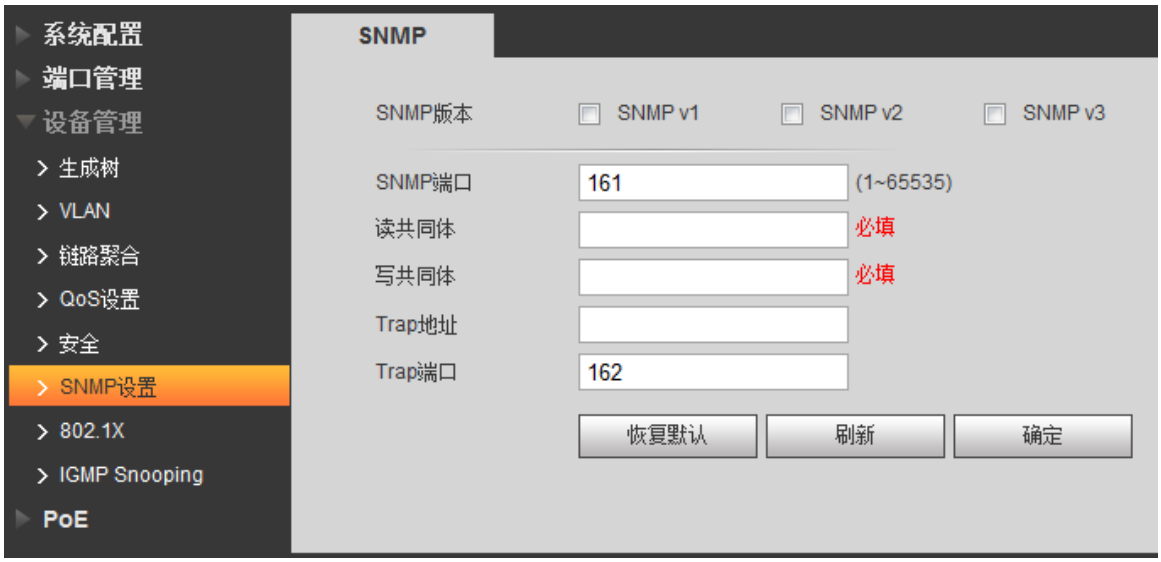
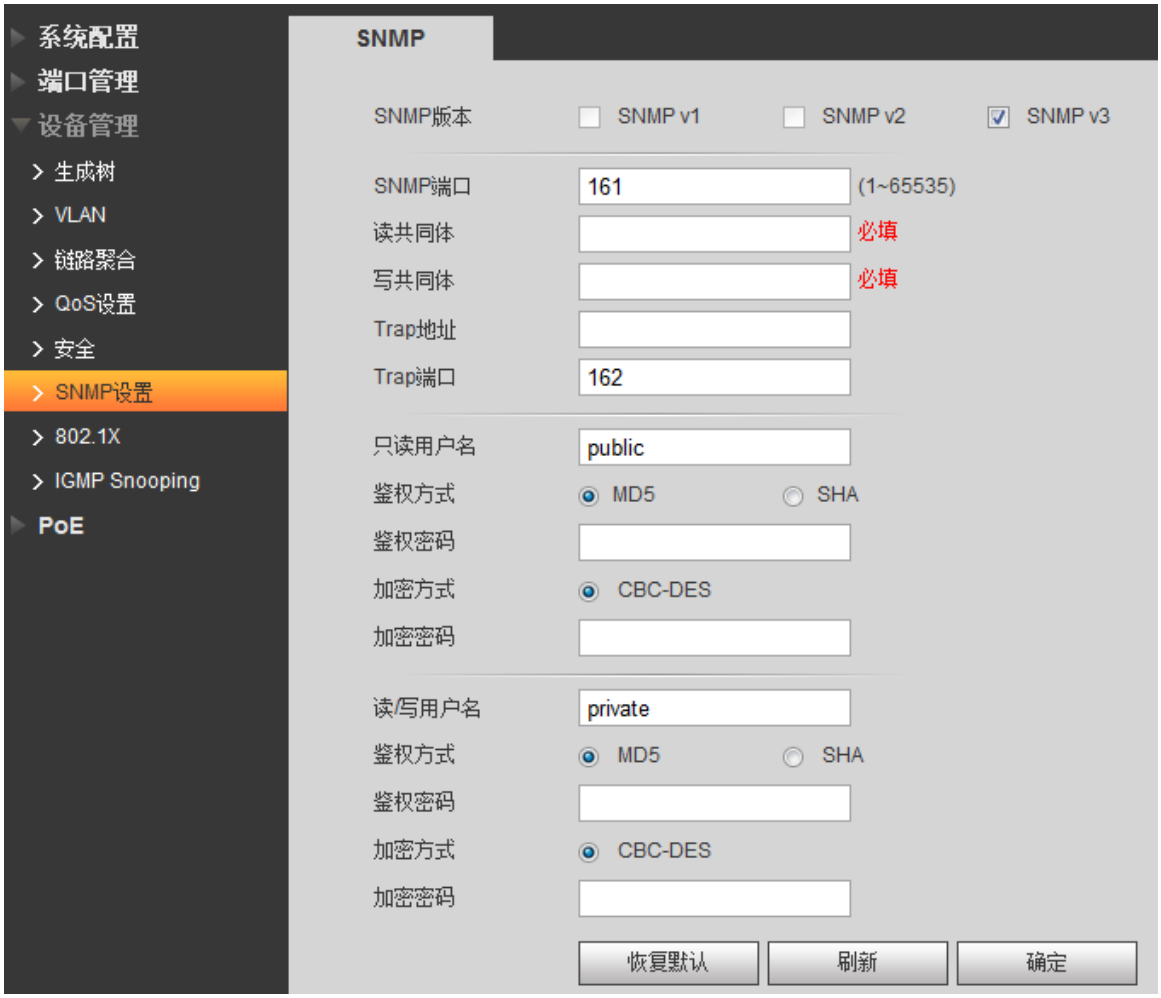


图6-29 SNMP v3



步骤2　设置参数，请参见表 6-8。

表6-8 SNMP 参数说明

参数	说明
读共同体	访问网管的共用体名称，权限为可读，缺省为 public。
写共同体	访问网管的共用体名称，权限为可写，缺省为 private。
Trap 地址	指定服务器的的 IP 地址。

参数	说明
Trap 端口	配置 Trap 的目的端口。
只读用户名	配置拥有只读权限的用户，仅 SNMP v3 有效。
鉴权方式	设置鉴权的方式，包括 MD5 和 SHA。
鉴权密码	配置鉴权密码。
加密方式	设置加密的模式，本产品仅支持 CBC-DES 方式。
加密密码	设置加密的密码。
读/写用户名	配置拥有可读可写权限的用户。

步骤3　单击“确定”。

SNMP v1/v2 配置举例

组网需求

如图 6-30 所示，NMS 与 Switch 相连。现要实现如下需求：

- NMS 通过 SNMPv1 或 SNMPv2 对 Switch 进行监控管理。
- Switch 在出现故障时能主动向 NMS 发送 Trap 报文。

图6-30 SNMP v1/v2 配置举例



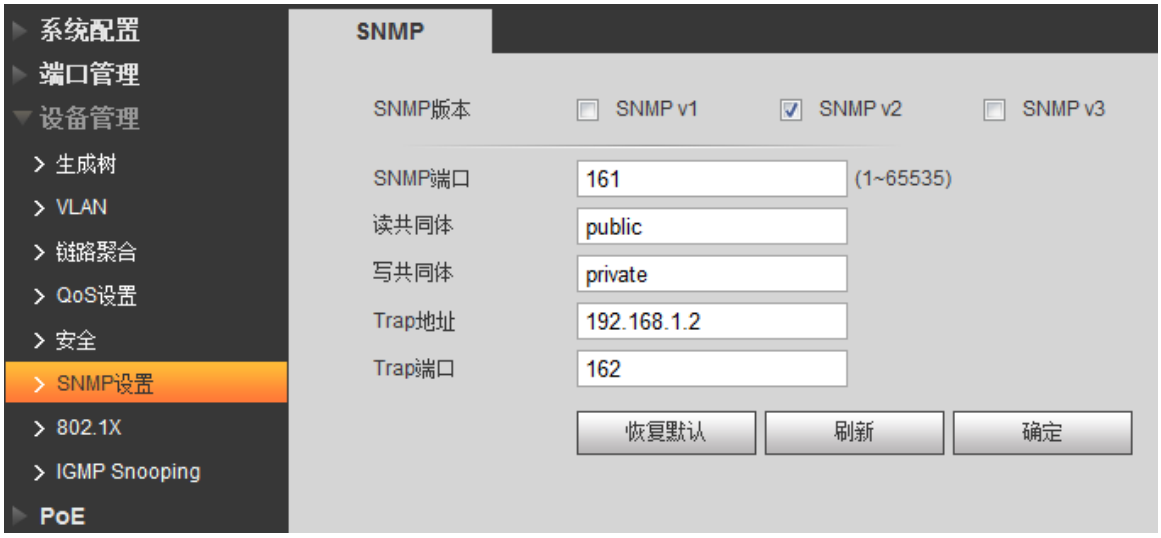
配置步骤

步骤1　选择“SNMP 版本”为“v2”。

步骤2　设置“SNMP 端口”为“161”。

步骤3　设置“读共同体”、“写共同体”、“Trap 地址”和“Trap 端口”分别为“public”、“private”、“192.168.1.2”和“162”，如图 6-31 所示。

图6-31 SNMP v2



步骤4　单击“确定”。

SNMP v3 配置举例

组网需求

如图 6-32 所示，NMS 与 Switch 相连。现要实现如下需求：

- NMS 通过 SNMP v3 对 Switch 的接口状态进行监控管理。
- Switch 在出现故障时能主动向 NMS 发送 Trap 报文。
- NMS 与 Agent 建立 SNMP 连接时需要认证，认证模式为 MD5，认证密码为 admin123。
- NMS 与 Agent 之间传输的 SNMP 报文需要加密，加密模式为 DES56，加密密码为 admin123。

图6-32 SNMP v3 配置举例



配置步骤

步骤1　选择“SNMP 版本”为“SNMP v3”。

步骤2　设置“SNMP 端口”为“161”。

步骤3　设置“读共同体”、“写共同体”和“Trap 地址”和“Trap 端口”分别为“public”、“private”、“192.168.1.2”和“162”。

步骤4　输入“只读用户名”为“user”。

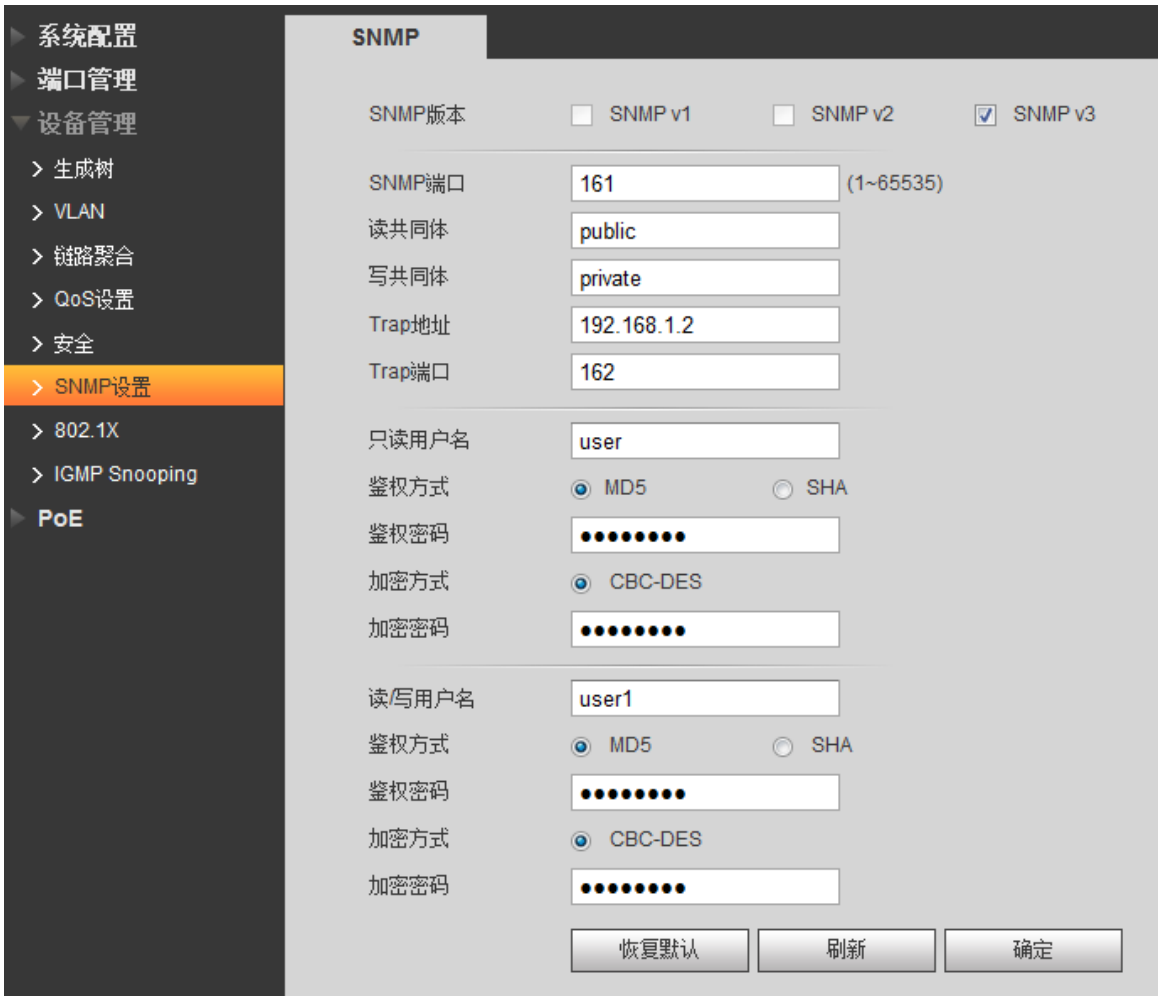
- 选择“鉴权方式”为“MD5”。
- 输入“鉴权密码”为“admin123”。
- 选择“加密方式”为“CBC-DES”。
- 输入“加密密码”为“admin123”。

步骤5　输入“读/写用户名”为“user1”。

- 选择“鉴权方式”为“MD5”。
- 输入“鉴权密码”为“admin123”。
- 选择“加密方式”为“CBC-DES”。
- 输入“加密密码”为“admin123”。

步骤6　单击“确定”，如图 6-33 所示。

图6-33 SNMP v3



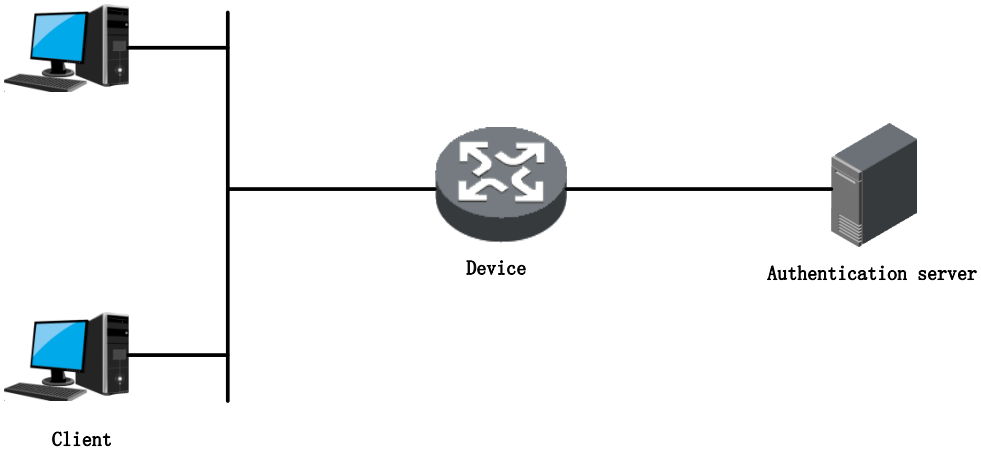
6.7 802.1x

IEEE 802.1x 是由 IEEE 指定的关于用户接入网络的认证标准，是一种基于端口的网络接入控制协议，所以具体的 802.1x 认证功能必须在设备端口上进行配置，对端口上接入的用户设备通过认证来控制对网络资源的访问。

6.7.1 802.1x 的组网结构

802.1x 系统中包括三个实体：Client、Device 和 Authentication server，如图 6-34 所示。

图6-34 802.1x 的组网结构



- 客户端（Client）是请求接入局域网的用户终端设备，它由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1x 认证的客户端软件。
- 设备端（Device）是局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口（物理端口或逻辑端口），并通过与服务器的交互来对所连接的客户端进行认证。
- 认证服务器（Authentication server）用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。在一些规模较小的网络环境中，认证服务器的角色也可以由设备端来代替，即由设备端对客户端进行本地认证、授权和计费。

6.7.2 802.1x 认证受控/非受控端口

设备端为客户端提供的接入局域网的端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

- 非受控端口始终处于双向连通状态，主要用来传递认证报文，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

6.7.3 802.1x 认证的触发方式

802.1X 的认证过程可以由客户端主动发起，也可以由设备端发起。

- 客户端主动触发方式
  - ◇ 组播触发：客户端主动向设备端发送认证请求报文来触发认证，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。
  - ◇ 广播触发：客户端主动向设备端发送认证请求报文来触发认证，该报文的目的地址为广播 MAC 地址。该方式可解决由于网络中有些设备不支持上述的组播报文，而造成设备端无法收到客户端认证请求的问题。
- 设备端主动触发方式

设备端主动触发方式用于支持不能主动发送认证请求报文的客户端，设备主动触发认证的方式分为以下两种：

◇ 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的请求报文来触发认证。

◇ 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的请求报文来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

6.7.4 端口的授权状态

通过配置端口的授权状态，可以控制端口上接入的用户是否需要经过认证来访问网络资源。端口支持以下三种授权状态：

- authorized-force：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- unauthorized-force：表示端口始终处于非授权状态，不允许用户进行认证。设备端不为通过该端口接入的客户端提供认证服务
- Port based 802.1x：表示端口初始状态为非授权状态，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。

配置举例

组网需求

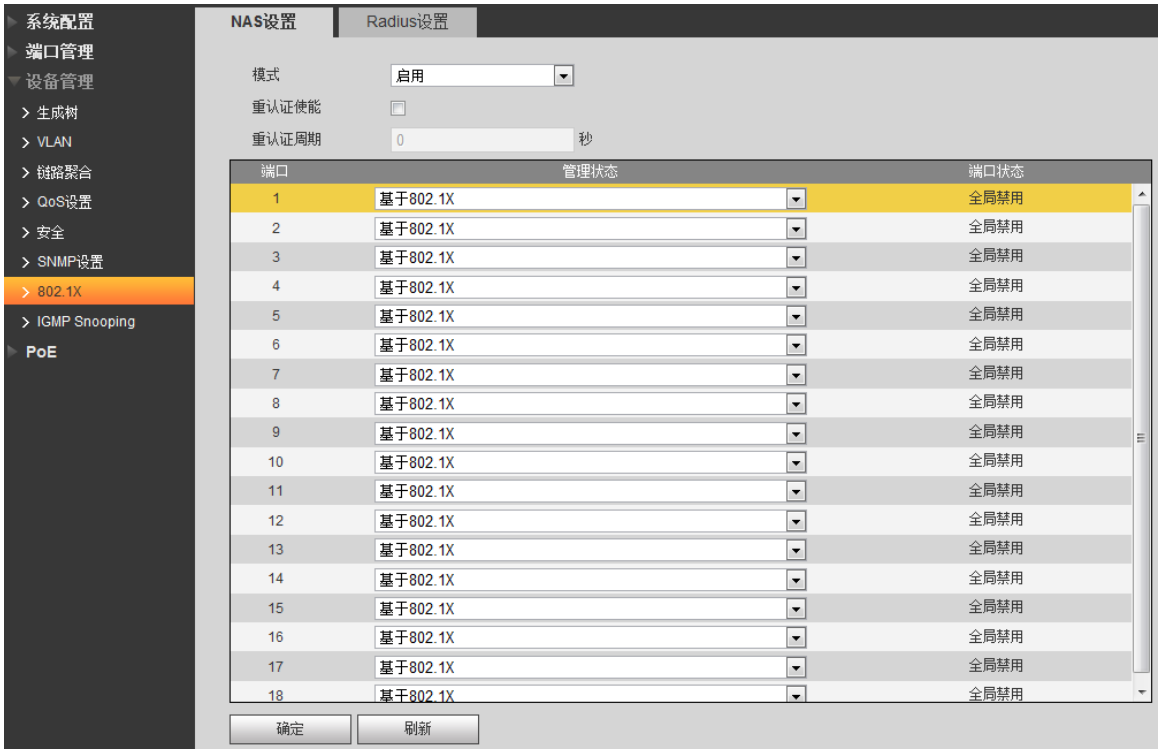
客户端 IP 为 192.168.1.1/24 网段，认证服务器 IP 为 192.168.1.100，要求设备所有端口接入时需要认证服务器认证。

配置步骤

步骤1　选择“系统信息 > 设备管理 > 802.1x > NAS 设置”。

系统显示“NAS 设置”界面，如图 6-35 所示。

图6-35 NAS 设置



步骤2　使能认证功能，全端口开启基于 802.1x 认证。

1. 选择“模式”为“启用”。
2. 选择所有端口的“管理状态”为“基于 802.1X”。

3. 单击“确定”。

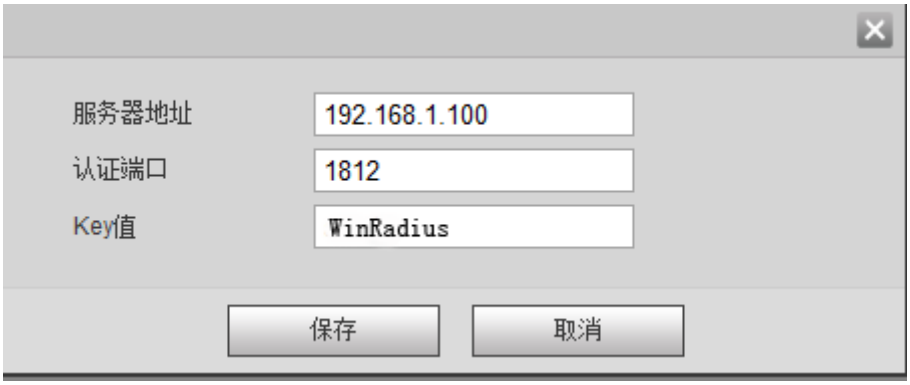
步骤3 配置认证服务器地址，如下图 6-36 所示。

图6-36 Radius 设置



1. 选择“Radius 设置”页签。
2. 输入“重传”为“3”。
3. 单击“新建服务器”，在弹出的对话框中，输入“服务器地址”为“192.168.1.100”，输入“认证端口”为“1812”，输入“Key 值”为“WinRadius”如图 6-37 所示。

图6-37 新建服务器



6.8 IGMP Snooping

IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）运行在二层设备上，通过侦听三层设备与主机之间的 IGMP 报文来生成二层组播转发表，从而管理和控制组播数据报文的转发，实现组播数据报文在二层的按需分发。

6.8.1 IGMP Snooping 原理

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

当二层设备没有运行 IGMP Snooping 时，组播数据在二层网络中被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层网络中被广播，而被组播给指定的接收者。

IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 减少了二层网络中的广播报文，节约了网络带宽。
- 增强了组播信息的安全性。

- 为实现对每台主机的单独计费带来了方便。

6.8.2 IGMP Snooping 配置

步骤1　选择“系统信息 > 设备管理 > IGMP Snooping”。

系统显示“IGMP Snooping”界面，如图 6-38 所示。

图6-38 IGMP Snooping



步骤2　设置 IGMP Snooping 的参数，如下：

- 组播侦听：启用或禁用 IGMP Snooping 功能。
- IGMP 离开报文：启用或禁用快速离开功能。

步骤3　单击“确定”。

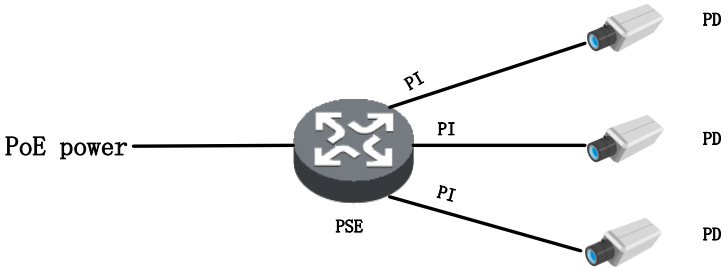
7 PoE

7.1 PoE 设置

PoE 是指设备通过以太网电口，利用双绞线对外接 PD（Powered Device，受电设备）进行远程供电。PoE 功能使得电源集中供电，备份方便，网络终端不需外接电源，只需要一根网线即可。符合 IEEE 802.3af 和 IEEE 802.3at 标准，使用全球统一的电源接口。可以用于 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头、数据采集等。

PoE 系统如图 7-1 所示，包括 PoE 电源、PSE（Power Sourcing Equipment，供电设备）、PI（Power Interface，电源接口）和 PD。

图7-1 PoE 系统



1. PoE 电源

PoE 电源为整个 PoE 系统供电。

2. PSE

PSE 是直接给 PD 供电的设备。PSE 分为内置（Endpoint）和外置（Midspan）两种：

- 内置指的是 PSE 集成在交换机/路由器内部。
- 外置指的是 PSE 与交换机/路由器相互独立。

PSE 支持的主要功能包括寻找、检测 PD，对 PD 分类，并向其供电，进行功率管理，检测与 PD 的连接是否断开等。

3. PI

PI 是指具备 PoE 供电能力的以太网接口，也称为 PoE 接口，包括 FE 和 GE 接口。

PoE 接口远程供电有两种模式：

- 信号线供电模式：PSE 使用 3/5 类双绞线中传输数据所用的线对（1、2、3、6）向 PD 传输数据的同时传输直流电。
- 空闲线供电模式：PSE 使用 3/5 类双绞线中没有用于数据传输的线对（4、5、7、8）向 PD 来传输直流电。

说明

选用哪种供电模式与 PD 的规格有关，选用的模式必须 PSE 和 PD 都支持，才能正常供电。如果 PSE 和 PD 支持的供电模式不同（比如 PSE 不支持空闲线供电式，PD 只支持空闲线供电），则需要转接才能给 PD 供电。

4. PD

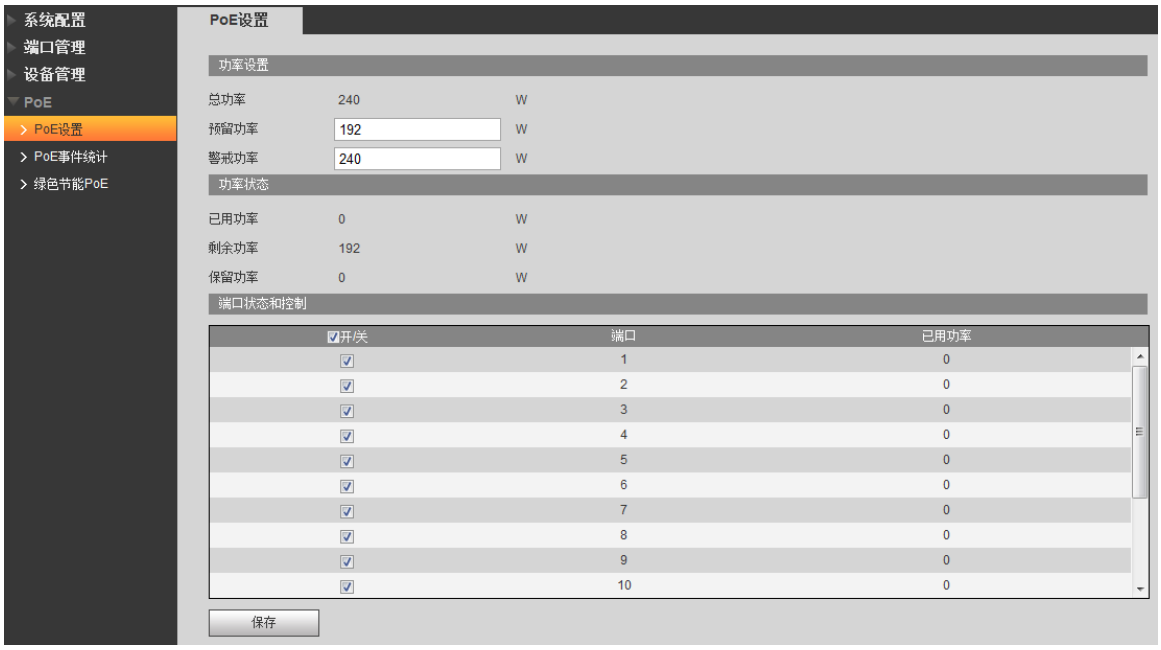
PD 是接受 PSE 供电的设备，如 IP 电话、无线 AP（Access Point，接入点）、便携设备充电器、刷卡机、网络摄像头等。

PD 设备在接受 PoE 电源供电的同时，可以连接其它电源，进行电源冗余备份。

步骤1　选择“系统信息 > PoE > PoE 设置”。

系统显示“PoE 设置”界面，如图 7-2 所示。

图7-2 PoE 设置



步骤2　设置参数，请参见表 7-1。

表7-1 PoE 端口设置

参数	说明
总功率	显示 PoE 的总功率。
预留功率	设置 PoE 的预留功率。
警戒功率	设置 PoE 的警戒功率。
选择端口	选择要进行 PoE 设置的端口。
端口状态和控制	开/关端口的 PoE 供电功能。 注意 PSE 功率过载，当 PSE 上已经获得供电的端口的最大功率之和大于 PSE 最大功率时，系统将认为 PSE 功率过载。 ● 当关闭 PoE 功能时，系统不会给 PoE 端口下挂的 PD 供电，也不会给 PD 预留功率。 ● 当开启 PoE 功能时，如果该 PoE 端口的加入不会导致 PSE 功率过载，则开启 PoE 功能；否则，不允许开启该 PoE 端口的 PoE 功能。 缺省情况下，接口的 PoE 供电功能处于关闭状态。

步骤3　单击“保存”。

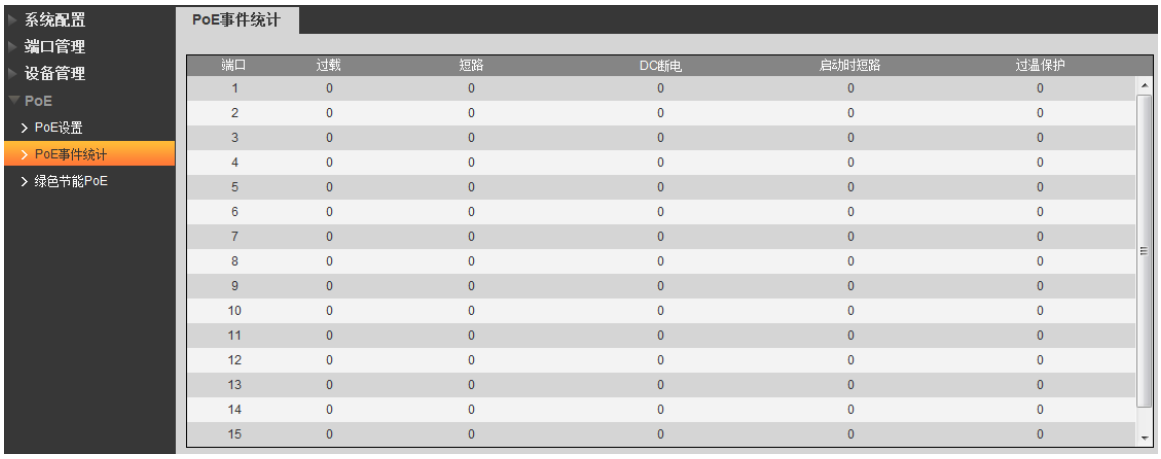
7.2 PoE 事件统计

此界面显示每个端口 PoE 功能的产生的事件统计，包括过载、短路、DC 断电、启动时短路和过温保护。

选择“系统信息 > PoE > PoE 事件统计”。

系统显示“PoE 事件统计”界面，如图 7-3 所示。

图7-3 PoE 事件统计



各参数含义请参见表 7-2。

表7-2 PoE 事件统计参数说明

参数	说明
过载	单个端口上电电流超过单端口输出电流限制。
短路	供电芯片开始对端口供电时发送端短路。
DC 断电	单端口供电断开。
启动时短路	供电芯片对外供电中受电电路短路。
过温保护	供电芯片因短路或其他原因导致芯片温度过高。

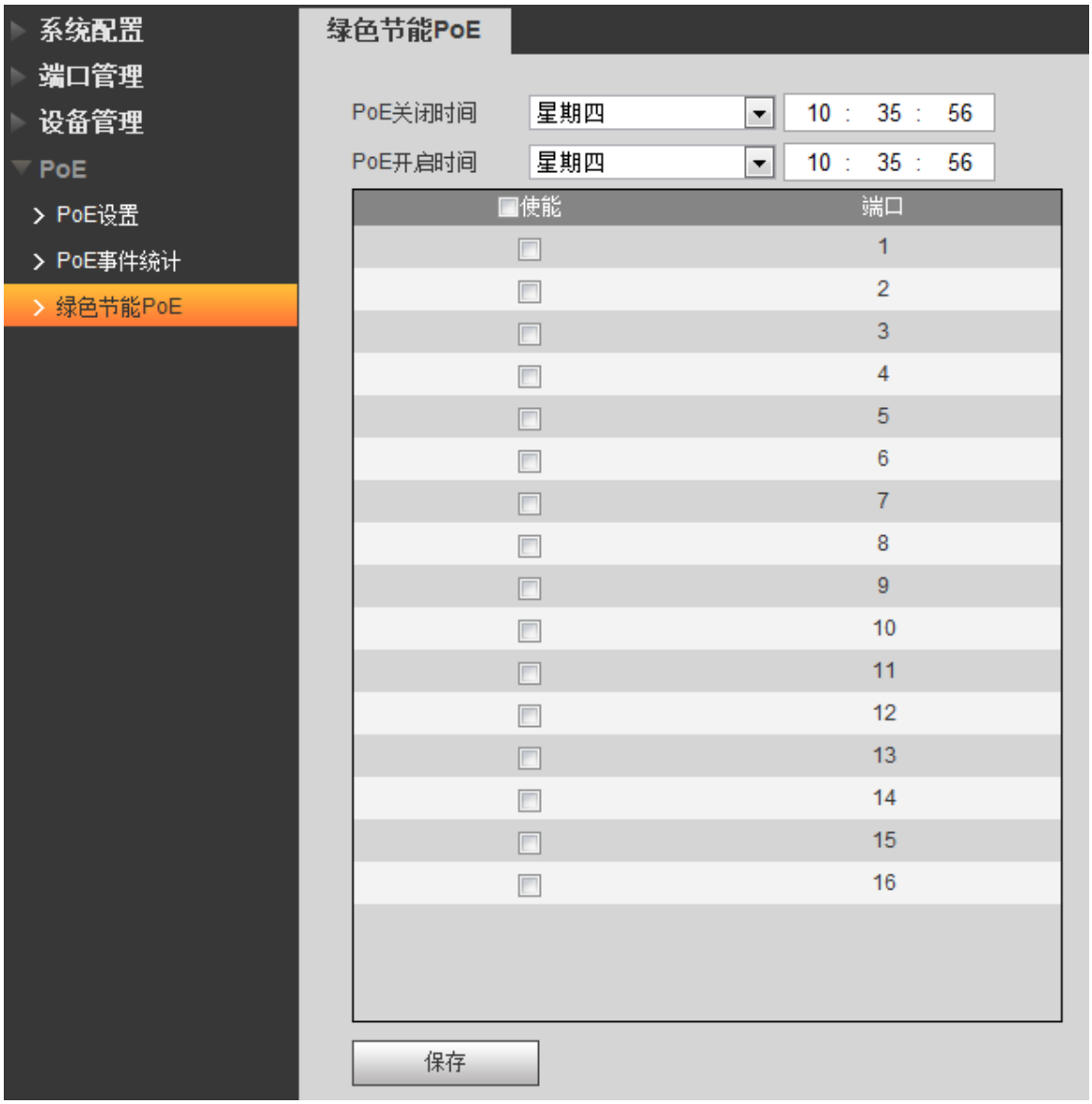
7.3 绿色节能 PoE

此界面是 PoE 省电功能配置项，您可以根据需要设置端口在每周的某天的某个时间段内 PoE 不供电，以达到设备节能的目的。当指定的时间范围结束时，端口会自动恢复正常。

选择“系统信息 > PoE > 绿色节能 PoE”。

系统显示“绿色节能 PoE”界面，如图 7-4 所示。

图7-4 绿色节能 PoE



配置举例

组网需求

配置端口 1～10 在每周六和周日掉电，并且在每周一上电。

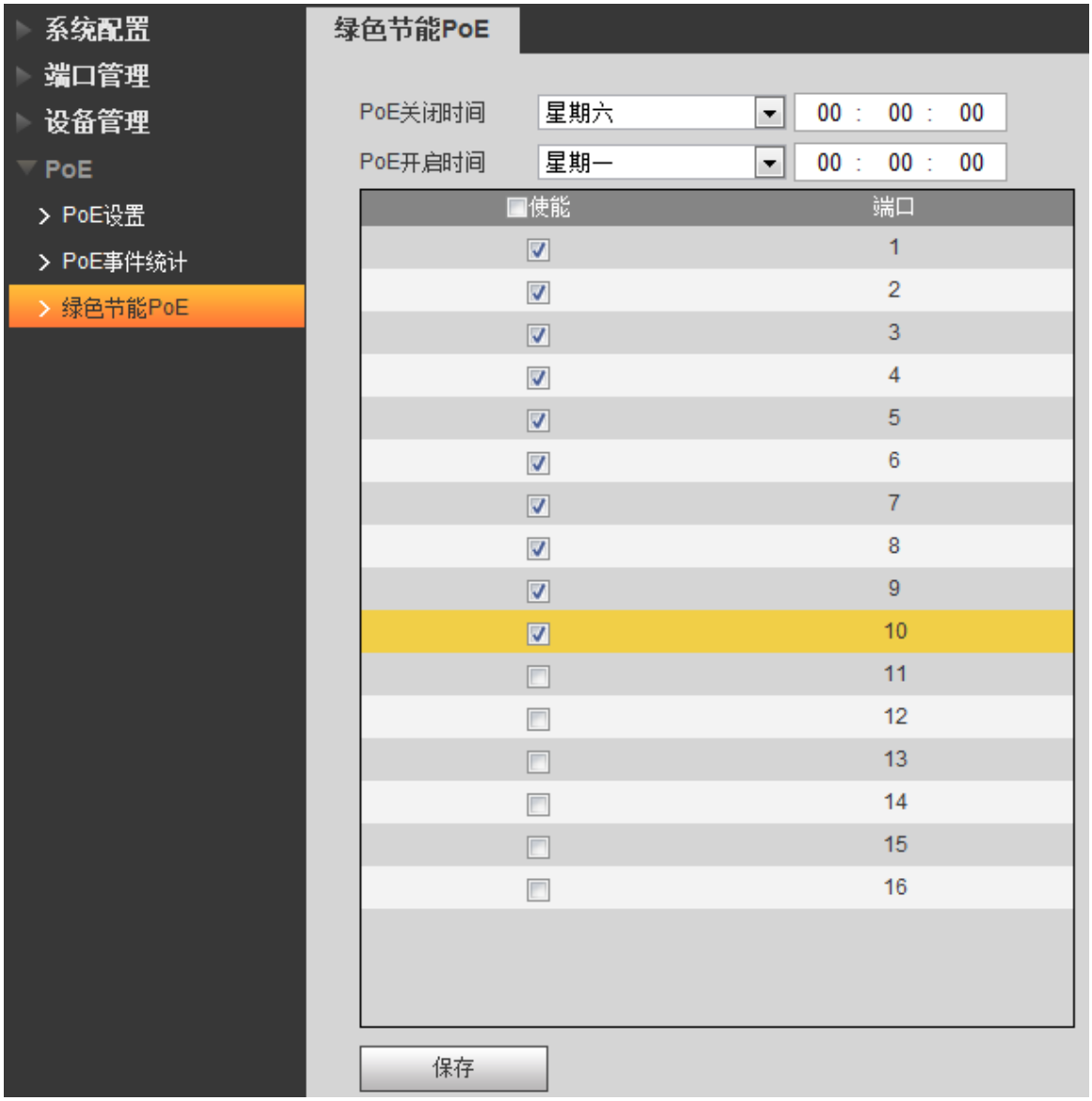
配置步骤

步骤 1　选择“PoE 关闭时间”和“PoE 开启时间”分别为“星期六”到“星期一”。

步骤 2　选择需要配置端口。

步骤 3　单击“保存”，具体配置结果如图 7-5 所示。

图7-5 绿色节能 PoE


系统配置
端口管理
设备管理
PoE
PoE设置
PoE事件统计
绿色节能PoE
绿色节能PoE
PoE关闭时间
星期六
00 : 00 : 00
PoE开启时间
星期一
00 : 00 : 00
使能
端口
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
保存

【社会的安全 我们的责任】

SOCIAL SECURITY IS OUR RESPONSIBILITY

浙江大华技术股份有限公司

地址：杭州市滨江区滨安路1187号

邮政编码：310053

客服热线：400-672-8166

公司网址：www.dahuatech.com