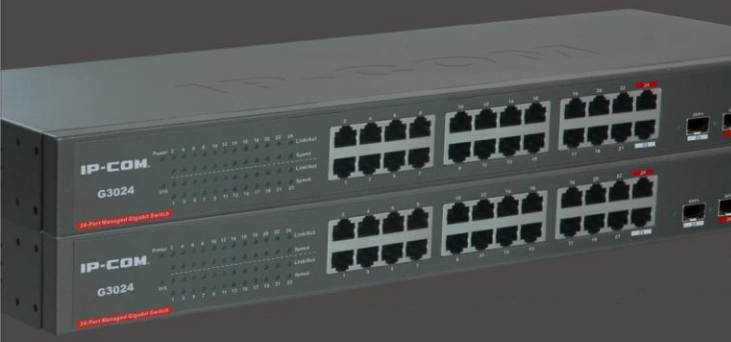
IP-COM™

说明书



24口全千兆网管型交换机

www.ip-com.com.cn

G3024

V1.0

版 权 声 明

IP-COM™是深圳市联科通网络技术有限公司注册商标。这里提及的其它产品和产品名称均是他们所属公司的商标或注册商标。本产品的所有部分（包括配件和软件），其版权属于深圳市联科通网络技术有限公司所有，在未经过深圳市联科通网络技术有限公司许可的情况下，不得任意拷贝、抄袭、仿制或翻译。

本手册中的所有图片和产品规格参数仅供参考，随着软件或硬件的升级会略有差异，如有变更，恕不另行通知，如需了解更多产品信息，请浏览我们公司的网站：http://www.ip-com.com.cn。

温馨提示：

在本交换机的配套光盘中,分别提供了中英文电子档 web 调试说明书和命令行调试的说明书(通过 Telnet 和 Console 口调试)。为了方便客户操作，还提供这本 web 调试的纸质档说明书。

目　　录

第一章 产品介绍.....1
1.1 端口特性.....1
1.2 功能及性能特点.....1
1.3 管理方式.....2
1.4 物品清单.....3
1.5 产品安装.....4
1.5.1 安装注意事项.....4
1.5.2 桌面或平面安装.....4
1.5.3 机架安装.....5
1.5.4 交换机的供电.....6
1.5.4.1 交流电源插座.....6
1.5.4.2 交流电源线连接.....6
1.6 外观描述.....7
1.6.1 前面板.....7
1.6.2 后面板.....7
1.6.3 侧面板.....8
1.6.4 LED 指示灯.....8
第二章 交换机的连接.....10
2.1 交换机连接到终端设备.....10
2.2 交换机连接到交换机或者路由器.....10

第三章 交换机的登录 11
3.1 通过 Web 登录 11
3.2 通过 Console 口登录 12
3.3 通过 Telnet 登录 14
第四章 交换机的配置 16
4.1 系统配置界面 16
4.1.1 IP 地址简介 17
4.1.2 系统信息设置界面 19
4.1.3 IP 和时间设置界面 20
4.1.4 系统用户设置界面 21
4.1.5 省电模式设置界面 22
4.2 端口设置界面 22
4.3 端口汇聚设置界面 25
4.3.1 端口汇聚概述 25
4.3.2 端口汇聚对端口配置的要求 26
4.3.3 端口汇聚的特点 27
4.3.4 端口汇聚配置和显示界面 28
4.3.4.1 静态汇聚设置 28
4.3.4.2 LACP 设置 29
4.4 生成树设置界面 31
4.4.1 生成树简介 31
4.4.2 快速生成树简介 31

4.4.3 生成树系统配置界面 33
4.4.4 生成树端口配置界面 34
4.5 802.1x 设置界面 36
4.5.1 802.1x 简介 36
4.5.2 802.1x 配置界面 36
4.6 IGMP 侦听 40
4.6.1 IGMP 侦听的概述 40
4.6.2 IGMP 侦听的原理 40
4.6.3 IGMP 侦听的工作机制 41
4.6.4 IGMP 侦听配置界面 42
4.7 链路层发现协议 44
4.7.1 链路层发现协议概述 44
4.7.2 链路层发现协议配置界面 44
4.8 MAC 地址表配置界面 46
4.8.1 老化设置 46
4.8.2 MAC 地址表学习 47
4.8.3 静态 MAC 地址表设置 47
4.9 虚拟局域网 48
4.9.1 虚拟局域网概述 48
4.9.2 VLAN 的优点 49
4.9.3 VLAN 的划分 50
4.9.4 VLAN 成员配置界面 51

4.9.5 VLAN 的端口配置界面 52
4.10 服务质量 54
4.10.1 QoS 概述 54
4.10.2 常用优先级 54
4.10.3 调度方式 56
4.10.4 QoS 配置 57
4.10.4.1 设置向导界面 57
4.10.4.2 端口设置界面 59
4.10.4.3 QoS 控制列表设置界面： 60
4.10.4.4 速率限制配置界面 63
4.10.4.5 风暴控制配置界面 64
4.11 访问控制列表 65
4.11.1 访问控制列表概述 65
4.11.2 ACL 配置 65
4.11.2.1 ACL 配置向导界面 65
4.11.2.2 ACL 端口配置界面 73
4.11.2.3 ACL 速率限制配置界面 74
4.11.2.4 ACL 控制列表配置界面 75
4.12 端口镜像 87
4.12.1 镜像概述 87
4.12.2 镜像配置界面 88
4.13 简单网络管理协议 89

4.13.1 简单网络管理协议概述.....89
4.13.2 简单网络管理协议配置界面.....90
第五章 交换机的监控.....92
5.1 系统监控.....92
5.1.1 系统信息.....92
5.1.2 系统日志信息.....93
5.1.3 具体的系统日志信息.....94
5.2 端口监控.....95
5.2.1 端口整体统计信息.....95
5.2.2 QoS 的队列统计信息.....96
5.2.3 端口统计信息.....97
5.3 LACP 监控.....99
5.3.1 LACP 系统信息.....99
5.3.2 LACP 端口状态信息.....100
5.3.3 LACP 端口统计信息.....101
5.4 生成树监控.....102
5.4.1 生成树桥状态信息.....102
5.4.2 生成树端口状态.....103
5.4.3 生成树端口统计状态.....104
5.5 802.1x 监控.....105
5.5.1 端口状态.....105
5.5.2 802.1x 端口统计.....105

5.6 IGMP Snooping 监控.....108
5.7 LLDP 监控 110
5.7.1 LLDP 邻居信息 110
5.7.2 LLDP 端口统计 111
5.8 MAC 地址表监控.....112
第六章 交换机的诊断.....114
6.1 ICMP Ping.....114
6.2 VeriPHY 115
第七章 交换机的维护.....116
7.1 系统重启 116
7.2 恢复出厂值.....116
7.3 软件升级 117
7.4 配置文件的上传.....118
7.5 配置文件的下载.....118
7.6 系统日志文件的下载 119
第八章 附 录.....120
8.1 技术参数 120
8.2 专业术语概述.....123
8.3 技术支持 119

第一章　产品介绍

G3024 是一款全千兆网管型交换机。它的功能非常强大，提供 WEB、Telnet、串口、SNMP V1 和 SNMP V2c 全方位管理方式，提供 2 个千兆共享 SFP 光纤接口。集高度的灵活性和完善的网管功能于一体，可为企业、高档网吧、行业用户等提供理想的接入方案。

其产品特性主要包括以下几个部分：

1.1 端口特性

- 提供 24 个高性能的 1000BASE-T 端口，自动以 10/100/1000Mbps 速率连接骨干网、服务器或网络终端。
- 提供 2 个千兆共享 SFP 接口，可以用光纤连接其它交换机、服务器或网络终端。
- 提供一个 RS-232 控制口，通过一条配置电缆就可以与控制终端连接，从而达到管理交换机的目的。

1.2 功能及性能特点

- 支持存储转发架构
- 支持高达 48Gbps 的背板带宽
- 每个端口的转发速率可达 1488095pps（包的大小为 64 字节）
- 支持 8K 的 MAC 地址表

- 支持巨型帧的转发
- 支持 DSCP 和 802.1p 优先级，每个端口提供 4 个优先级转发队列
- 支持 1~4094 的 802.1Q VLAN 功能，最大可同时支持 64 组 VLAN
- 支持 IGMP V1 和 V2 功能
- 支持基于端口的 802.1x 认证功能
- 支持全双工 802.3x 流控和半双工背压流控
- 支持 ACL（访问控制列表）功能
- 支持 QoS（服务质量）功能
- 支持生成树协议。包括 802.1d（Spanning Tree）和 802.1w（Rapid Spanning Tree）协议
- 支持链路汇聚功能，包括静态链路汇聚和 LACP，最多可支持 12 个 Trunk 组，每组最多可支持 16 个端口成员
- 支持链路层邻居发现协议——LLDP(Link Layer Discovery Protocol)
- 支持端口镜像功能
- 支持多播、广播和未知单播的风暴控制功能
- 支持 CLI 中的 TFTP 和 Web 中的 HTTP 软件升级方式
- 支持系统日志
- 支持 CLI、Web、Telnet、SNMP V1 和 SNMP V2c 管理功能

1.3 管理方式

- 支持 RS-232 Console 口管理，只需一根串口线连接到管理终端即可实现管理
- 支持 SNMP V1 和 SNMP V2c 网络管理
- SNMP 管理范围

- ✧ RFC1213：system、interface、ip、icmp、tcp、udp 和 snmp
- ✧ EtherLike-MIB：dot3StatsTable
- ✧ Bridge-MIB：dot1Base
- ✧ IF-MIB：ifXTable

- ➢ 支持 Web 管理
- ➢ 支持远程 Telnet 管理，最大可同时支持 5 个用户登录
- ➢ 支持 CLI 命令行管理

1.4 物品清单

- ➢ G3024 全千兆网管型交换机 1 台
- ➢ 4 个橡胶脚垫、1 对 L 型支架（包括 8 颗配套螺丝）
- ➢ 1 条 AC 电源线
- ➢ 一根串口线
- ➢ 一根网线
- ➢ 一本说明书
- ➢ 1 张光盘
- ➢ 1 张保修卡（包括合格证）

1.5 产品安装

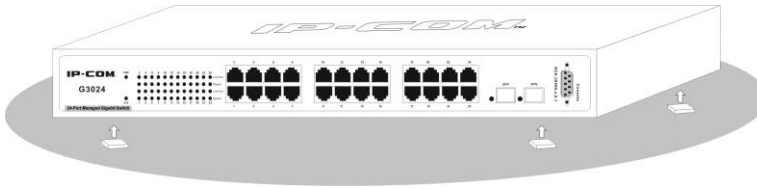
1.5.1 安装注意事项

为避免使用不当造成设备损坏及对人身的伤害，请遵从以下的注意事项：

- 请不要将交换机放在不稳定的箱子或桌子上，万一跌落，会对交换机造成严重损害。
- 交换机要在正确的电压下才能正常工作，请确认工作电压同交换机所标示的电压相符。
- 为减少受电击的危险，建议接地。在交换机工作时不要打开外壳，即使在不带电的情况下，也不要随意打开交换机机壳。
- 确认交换机的入风口及通风口处留有空间，以利于交换机机箱的散热。
- 确认机柜及工作台足够牢固，能够支撑交换机及其安装附件的重量。

1.5.2 桌面或平面安装

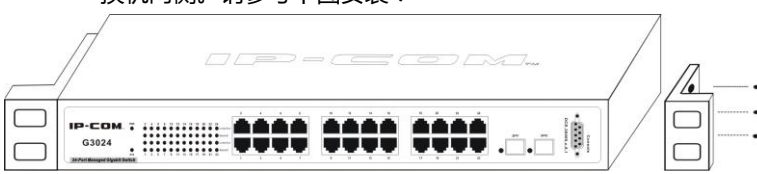
很多情况下，用户并不具备 19 英寸标准机柜，此时，人们经常用到的方法就是将交换机放置在干净的工作台上使用，此种操作比较简单，首先将附件中 4 个塑料脚垫安装在交换机底部对应的位置，防止交换机在放置的桌面或其它水平面上滑动，减轻外来的震荡力。另外，在使用时还要保持周围环境的良好通风。请参考下图安装：



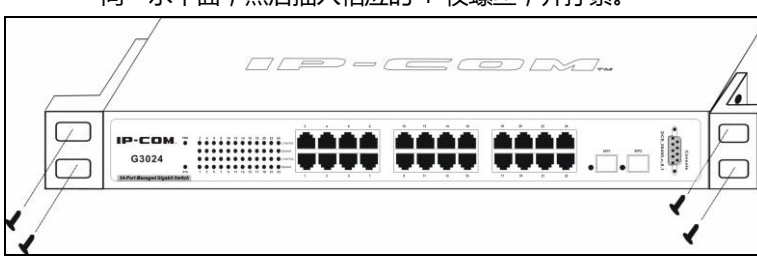
1.5.3 机架安装

安装交换机到 19 英寸机柜

- 用 1 号十字头螺丝刀和随机附带的 8 枚螺丝将脚铁架固定在交换机两侧。请参考下图安装：



- 将安装在交换机上脚铁架的上下槽对准机架上的螺孔并保持在同一水平面，然后插入相应的 4 枚螺丝，并拧紧。



说明：

为了安全，请在安装交换机之前认真阅读安装程序。

1.5.4 交换机的供电

G3024 交换机使用 AC 100-240V 50/60Hz 电源，建议按照如下方式连接：

1.5.4.1 交流电源插座

建议使用有中性点接头的单相三线电源插座，或多功能计算机电源插座。电源的中性点要可靠接地。

1.5.4.2 交流电源线连接

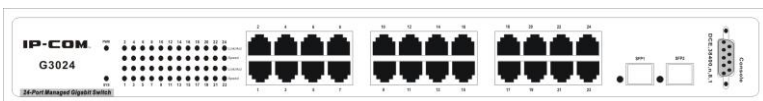
第一步：将交换机的电源线一端插到交换机机箱后面板的电源插座上，另一端插到外部的供电交流电源插座上。

第二步：检查交换机前面板的电源指示灯是否变亮，灯亮则表示电源连接正常。

1.6 外观描述

1.6.1 前面板

G3024 的前面板由 24 个 10/100/1000MbpsRJ-45 端口、2 个千兆共享 SFP 光纤接口、1 个 RS-232 Console 口、24 组 100/1000Mbps 双色指示灯和 Link/Act 指示灯、2 个共享 SFP 光纤接口的 Link/Act 指示灯、1 个 Power 指示灯、1 个系统（SYS）灯组成，请参考下图：



前面板示意图

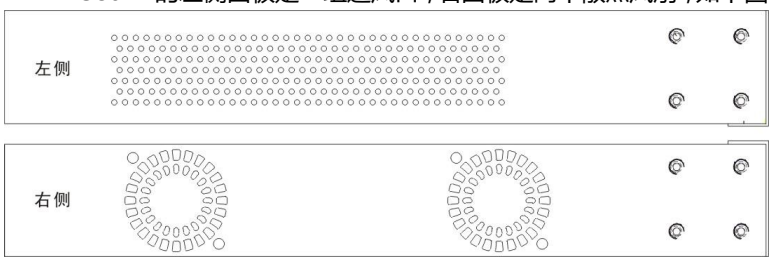
1.6.2 后面板

G3024 的后面板由一个 AC 电源接口及其标识组成，如下图：

后面板示意图

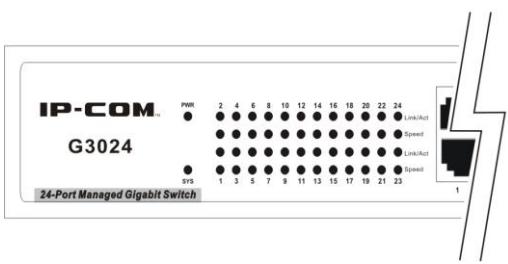
1.6.3 侧面板

G3024 的左侧面板是一组通风口，右面板是两个散热风扇，如下图



侧面板示意图

1.6.4 LED 指示灯



指示灯示意图

G3024 的指示灯包括 24 组 100/1000Mbps 指示灯和 Link/Act 指示灯、1 个 Power 指示灯和 1 个系统（SYS）灯组成，这些绿色的 LED 指示灯用于工作状态的监控和故障显示，下表针对每种类型的指示灯做出解释:

LED 指示灯	状态	描述
POWER	常亮	表示交换机正常加电
	熄灭	表示交换机没有加电或加电不正常，请检查电源是否正常接入
SYS	常亮	表示交换机运行正常
	熄灭	表示交换机没有运行或运行不正常
	闪烁	表示系统正在升级
Link/Act	常亮	表示该端口正常连接
	熄灭	表示该端口无连接或连接不正常，请检查是否正常连接
	闪烁	表示该端口在接收或传送数据
Speed	绿色	表示该端口以千兆速率连接
	橙色	表示该端口以百兆速率连接
	熄灭	表示该端口没有连接或者以十兆速率连接

第二章 交换机的连接

2.1 交换机连接到终端设备

PC 或其它终端设备可以通过 5 类或超 5 类屏蔽(STP)或非屏蔽(UTP)线缆连接到 G3024 交换机，因为交换机提供了自动识别平行/交叉线的功能，因此，PC 或其它终端设备不需要区分平行/交叉线即可连接交换机的任意一个端口。

2.2 交换机连接到交换机或者路由器

与 PC 或其它终端设备连接方式类似，因为交换机提供了自动识别平行/交叉线功能，使用 5 类或超 5 类屏蔽(STP)或非屏蔽(UTP)平行/交叉线都可以方便地从 G3024 交换机的任意端口级联到其它交换机任意端口。

第三章 交换机的登录

3.1 通过 Web 登录

登录到 G3024 的 Web 界面的方法：

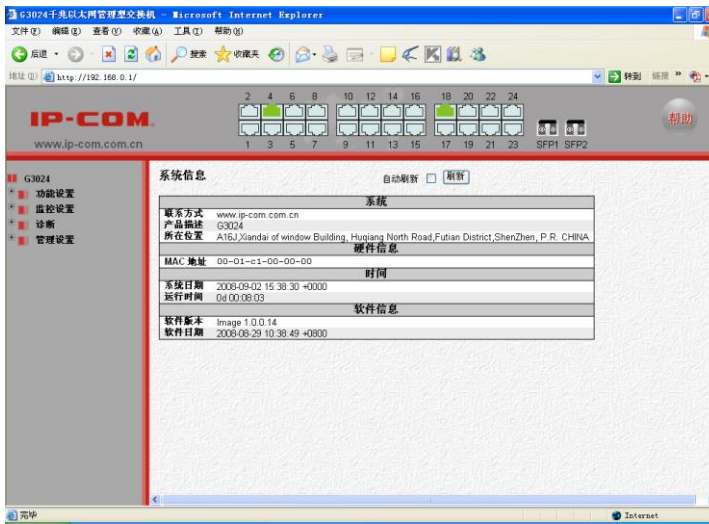
由于 G3024 提供 WEB 的管理方式，所以可以通过手动配置计算机的 IP 地址登录到交换机。交换机的默认参数如下表所示：

参数	默认值
默认 IP 地址	192.168.0.1
默认用户名	admin（管理用户）/user（普通用户）
默认密码	admin（管理用户）/user（普通用户）

在默认情况下，手动配置 IP 地址登录到交换机的管理界面步骤如下：

1. 用网线的一端连接交换机，一端连接计算机网卡；
2. 接通交换机的电源；
3. 手动设置计算机的 IP 地址属于 192.168.0.xxx 网段，如：192.168.0.100（xxx 为 2～254）；
4. 打开浏览器，在地址栏输入 http://192.168.0.1 并回车，会出现交换机的登录页面，如下图所示：

5. 在登录页面的对话框中输入用户名和密码，点击“确定”按钮即可登录到交换机配置界面。如下图：



3.2 通过 Console 口登录

第一步：将计算机（或终端）的串口通过配置电缆与以太网交换机的串口连接。

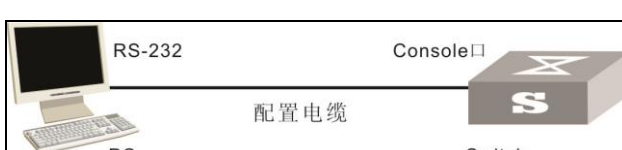


图3-1 串口的连接

第二步：在PC机上运行终端仿真程序（如Windows 3.X的Terminal

或Windows 9X/Windows 2000/Windows XP的超级终端等，以下配置以Windows XP为例），选择与交换机相连的串口，设置终端通信参数：传输速率为115200bit/s、8位数据位、1位停止位、无校验和无流控。

图3-2 新建连接

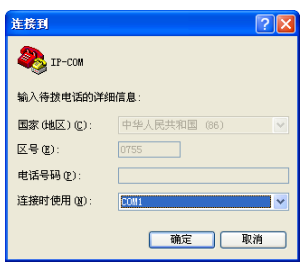


图3-3 连接端口设置

图3-4 通讯端口参数设置

第三步：给交换机上电，终端上显示设备自检信息，出现LOG的信息后，输入用户名和密码（系统默认为admin/admin），之后将出现命令行提示符（如>），如图2-5所示。

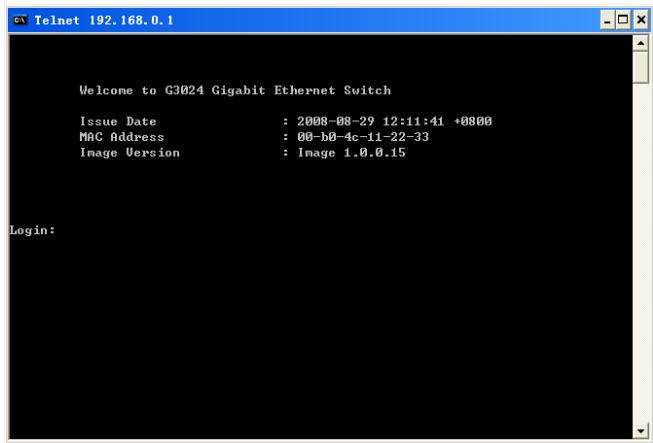
```
        ************************************************************
        *                                                          *
        *          IP-COM G3024 BOOTROM Version 1.0.0              *
        *                                                          *
        ************************************************************
        IP-COM is the registered trade mark of Shenzhen IP-COM
        Network Technology Co., Ltd.
        Creation date            : 01:22:41, Sep  9 2008
        Memory Size              : 64 M

Press Ctrl-C to enter Boot Menu ...
auto-booting...


        Welcome to G3024 Gigabit Ethernet Switch

        Issue Date                : 2008-08-29 12:11:41 +0800
        MAC Address               : 00-aa-bb-cc-dd-00
        Image Version             : Image 1.0.0.15



Login:
```

图3-5 交换机配置界面

3.3 通过Telnet登录

以 Window XP 为例，点击计算机的“开始”按钮，选择“运行”，如下图所示:

在打开的输入栏中输入 telnet 192.168.0.1。回车后就可以进入 telnet 界面，如下图所示：(输入用户名和密码即可进入和 CLI 相同的管理界面)



温馨提示:

通过 Telnet 和 Console 口调试的具体方法，请参照光盘中的命令行部分电子档说明书。

第四章 交换机的配置

本章介绍交换机各种功能在 Web 界面的配置方法，使用户能够轻松使用和管理交换机。

在 Web 管理界面中分以下 13 个模块介绍 G3024 的各个功能：

- 系统设置
- 端口设置
- 端口汇聚设置
- 生成树设置
- 802.1x 设置
- IGMP 侦听
- LLDP
- MAC 地址表
- VLAN 设置
- QoS 设置
- ACL
- 端口镜像
- SNMP

4.1 系统配置界面

G3024 的系统配置主要分以下四个方面：信息、IP&时间、用户管理和省电模式。

4.1.1 IP 地址简介

1. IP 地址的分类和表示：

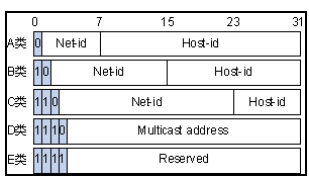
连接到 Internet 上的设备接口必须有一个全球唯一的 IP 地址。IP 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 192.168.0.1。

IP 地址由两部分组成：

A、网络号码字段（Net-id）：用于区分不同的网络。网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。

B、机号码字段（主机-id）：用于区分一个网络内的不同主机。

为了方便管理及组网，IP 地址被分成五类，如下图所示，其中蓝色部分为类别字段。



上述五类 IP 地址的地址范围如下表所示。目前大量使用的 IP 地址属于 A、B、C 三类。

地址类型	地址范围	说明
A	0.0.0.0 ~ 127.255.255.255	IP 地址 0.0.0.0 仅用于主机在系统启动时进行临时通信，并且永远不是有效目的地址 127.0.0.0 网段的地址都保留作回路测试，发送到这个地址的分组不会输出到链路上，它们被当作输入分组在内部进行处理

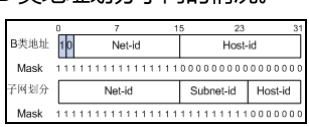
地址类型	地址范围	说明
B	128.0.0.0 ~ 191.255.255.255	
C	192.0.0.0 ~ 223.255.255.255	
D	224.0.0.0 ~ 239.255.255.255	组播地址
E	240.0.0.0 ~ 255.255.255.255	255.255.255.255 用于广播地址，其他地址保留今后使用

2. 子网和掩码

随着 Internet 的快速发展，IP 地址已近枯竭。为了充分利用已有的 IP 地址，可以使用子网掩码将网络划分为更小的部分（即子网）。通过从主机号码字段部分划出一些比特位作为子网号码字段，能够将一个网络划分为多个子网。子网号码字段的长度由子网掩码确定。

子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成，通常采用点分十进制方式表示。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。

下图所示是一个 B 类地址划分子网的情况。



多划分出一个子网号码字段会浪费一些 IP 地址。例如，一个 B 类地址可以容纳 65534（216-2，去掉全 1 的广播地址和全 0 的网段地址）个主机号码。但划分出 9 比特长的子网字段后，最多可有 512

（29）个子网，每个子网有 7 比特的主机号码，即每个子网最多可有 126（27-2，去掉全 1 的广播地址和全 0 的网段地址）个主机号码。因此主机号码的总数是 512*126=64512 个，比不划分子网时要少 1022 个。

若不进行子网划分，则子网掩码为默认值，此时子网掩码中“1”的长度就是网络号码的长度，即 A、B、C 类 IP 地址对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

4.1.2 系统信息设置界面

请点击导航栏的“G3024→功能设置→系统设置→信息 ”，即可进入系统信息配置界面，如下图：

本页面中提供了交换机的系统信息。包括以下三个方面：

1. 交换机联系方式

本栏目填写的内容是对管理该节点的联系人的文本描述，以及如何联系该人的信息。可允许的字符串长为 0～255 个 NVT ASCII 字符（32-126）。

2. 系统名

本栏目填写的内容是对该管理节点分配的管理名。系统名是由字母（A-Z，a-z）和数字（0-9），减号（-）组成。在名中，不能有空格或留空的字符出现。第一个字符必须是一个字母字符。第一个和最后一

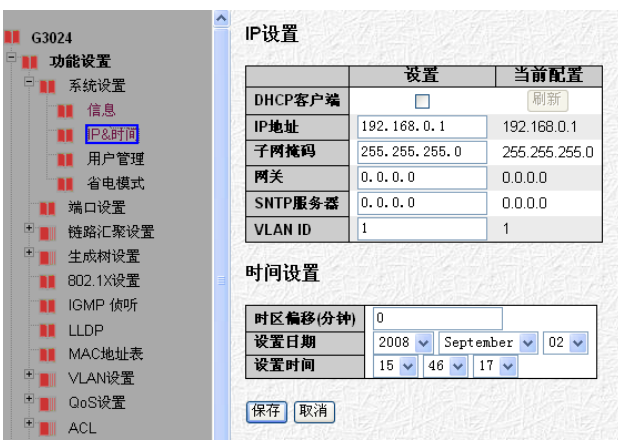
个字符不可以是减号字符。可允许的字符长为 0~255。

3. 系统位置

本栏目填写的内容是本节点的物理位置（比如：电话橱，三楼）。可允许的字符串长为 0～255 个 NVT ASCII 字符（32-126）。

4.1.3 IP&时间设置界面

请点击导航栏的“G3024→功能设置→系统设置→IP&时间”，即可进入 IP 和时间配置界面，如下图：



在本页面对可管理交换机的 IP 信息进行设置。

“**设置**”栏用于查看或改变 IP 的设置。

“**当前配置**”栏用于显示激活的 IP 设置。

DHCP 客户端

点击该方框可启用 DHCP 客户端。如果 DHCP 启用失败或设置的 IP 地址显示为 0，则 DHCP 会重试分配 IP 地址。如果 DHCP 启用失败

或设置的 IP 地址显示的不是为 0，则 DHCP 将不会分配 IP 地址并将使用已有的 IP 设置。

IP 地址：设置交换机的 IP 地址。

子网掩码：设置交换机的子网掩码。

网关：设置网关的 IP 地址。

SNTP 服务器：设置 SNTP 服务器的 IP 地址。

VLAN ID：提供可管理 VLAN 的 ID。可用范围为：1～4094。

时间偏移(分钟)：提供相关于 UTC/GMT 的时区偏移。偏移按照 GMT 东区的分钟形式给予。有效范围为-720 到 720 分钟。

4.1.4 系统用户设置界面

请点击导航栏的“G3024→功能设置→系统设置→用户管理”，即可进入系统用户配置界面，如下图：

点击“添加”即可进入用户名和密码配置界面，如下图：

本页面可用于设置访问 Web 页面或 CLI 登录的系统密码。

用户名：登录管理界面需要输入的用户名。长度为 32 位，由字母、

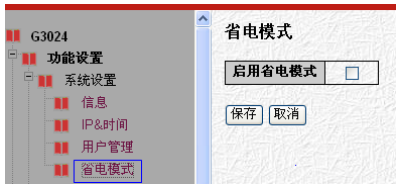
数字和下划线组成，且必须一字母开头。

新密码：系统的新密码。最多可设置 32 个 NVT ASCII 字符(32-126)。

确认新密码：新密码需要输入两次，以防输入错误。

4.1.5 省电模式设置界面

请点击导航栏“G3024→功能设置→系统设置→省电模式”，即可进入省电模式配置界面，如下图：



省电模式用于节省系统的能源消耗，当启用省电模式后，没有连接设备的端口的能耗几乎为零，这样可以大大降低系统的能源消耗。但启用省电模式可能会影响系统的驱动距离。当端口连接的距离大于 80m 时，建议不要启用省电模式功能。系统默认该功能为禁用状态。

4.2 端口设置界面

请点击导航栏的“G3024→功能设置→端口”，即可进入端口配置界面，如下图：

本页面可用于显示和设置端口状态。其参数描述如下：

端口：表示交换机的逻辑端口号。

链接：图示显示端口当前链接状态。绿色表示已链接上，红色表示未链接。

链接速度/当前配置：显示端口当前的链接速度、双工和链接状态。

链接速度/设置：对给定的交换端口选择可用的链接速度。在下拉菜单中选择相应的选项即可设置端口的速率和双工状态，系统默认为自适应状态。各状态描述如下：

禁用——表示禁用该端口。

Auto——表示选择最高速度与相连接的设备匹配。

1GbpsFDX——表示将该端口强制到 1000M 全双工状态。

100MbpsFDX——表示将该端口强制到 100M 全双工状态。

100M bpsHDX——表示将该端口强制到 100M 半双工状态。

10M bpsFDX——表示将该端口强制到 10M 全双工状态。

10M bpsHDX——表示将该端口强制到 10M 半双工状态。

流控：当端口选择了“auto”，该项表示将流控容量广播到其相连接的

设备上。如果选择的是固定的速度，则表示正在使用的速度。

勾选设置栏可运行流控。其设置与“设置链接速度”有关。

最大帧：输入交换端口可允许的最大帧大小，包括 FCS。可允许的范围为 1518～9600 字节。

过分冲突模式：设置端口传送冲突行为。其参数描述如下：

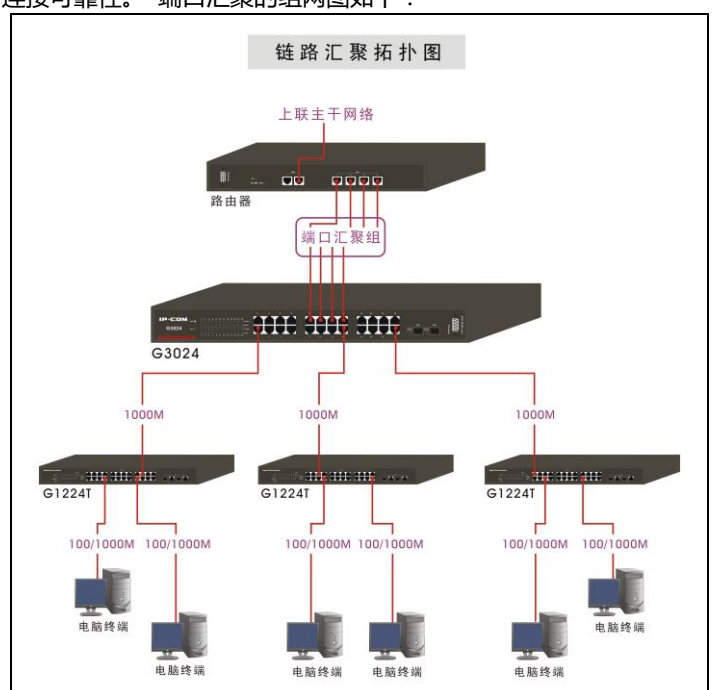
丢弃：在 16 个冲突（默认）后丢弃帧。

重启：在 16 个冲突后重启 backoff 算法。

4.3 端口汇聚设置界面

4.3.1 端口汇聚概述

端口汇聚是将多个以太网端口汇聚在一起形成一个逻辑上的汇聚组，使用汇聚服务的上层实体把同一汇聚组内的多条物理链路视为一条逻辑链路。端口汇聚可以实现出/入负荷在汇聚组中各个成员端口之间分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。 端口汇聚的组网图如下：



端口汇聚的示意图

4.3.2 端口汇聚对端口配置的要求

在同一个汇聚组中，能进行出/入负荷分担的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、VLAN、端口属性等相关配置。

STP 配置一致，包括：

端口的 STP 开启/关闭、

与端口相连的链路属性（如点对点或非点对点）、

STP 优先级、

STP 开销、

是否为边缘端口等。

QoS 配置一致，包括：

缺省队列

Tag 优先级

QCL ID

入口方向速率限制（开关）

入口方向速率

入口方向速率限制（开关）

入口方向速率

模式

权重

VLAN 配置一致，包括：

端口上允许通过的 VLAN。

VLAN 端口配置，包括:

Aware

PVID

帧类型

进入过滤

端口属性配置一致，包括：

端口的速率、双工模式、 自动协商。

4.3.3 端口汇聚的特点

1. **增加带宽：**

   交换机把Trunk组中的所有端口都类似当作一个端口来对待。在Trunk组中，传输的数据总是将有效的数据传输至目的端口，这样可以使传输的数据流保持相同的顺序。端口汇聚允许几个端口聚合在一起传输数据时作为同一条链路。这使传输的带宽相当于几个单端口传输的带宽总和。

2. **链路备份：**

   在Trunk中，当单个链路出现故障时，系统会自动执行负载共享功能，从而把相应的数据转发到Trunk中的其他链路上。从交换机整体上，STP（生成树协议）将端口汇聚当作单一链路看待。从端口的角度来看，STP会应用在主端口的参数上，计算端口开销并决定端口汇聚的状态。如果在交换机上设置了两个冗余Trunk组，STP会对其中的一个Trunk进行逻辑上的阻塞。 同样，STP也会对单个端口的冗余链路进行逻辑上的阻塞。

说明：

1. G3024最多提供了12个Trunk组，每组支持2—16个端口。
2. 对于开启了802.1x的端口，不能加入到汇聚组中。
3. 对于镜像目的端口，不能加入到汇聚组中。
4. 对于配置了静态 MAC 地址、组播 MAC 地址的端口，不能加入到汇聚组中。
5. 对于配置了 MAC 地址绑定的端口，不能加入到汇聚组中。

4.3.4 端口汇聚配置和显示界面

4.3.4.1 静态汇聚设置

请点击导航栏的“G3024→功能设置→链路汇聚设置→静态汇聚”，即可进入静态汇聚配置界面，如下图：

本页面用于设置端口汇聚的哈希模式和汇聚组。端口汇聚的哈希模式设置是针对全局的。

哈希模式主要分为以下 4 种，源 MAC 地址、目的 MAC 地址、IP 地址和 TCP/UDP 端口。使用时可以选择其中一种，也可以选择多种。

1. **源 MAC 地址**

   源 MAC 地址用来为数据帧计算目的端口。点击勾选可使用源 MAC 地址，否则禁用源 MAC 地址。默认为启用源 MAC 地址。

2. **目的 MAC 地址**

   目的 MAC 地址用来为数据帧计算目的端口。点击勾选可使用目的 MAC 地址，否则计算时不包含目的 MAC 地址。默认为不选择目的 MAC 地址。

3. **IP 地址**

   IP 地址用来为数据帧计算目的端口。点击勾选可使用 IP 地址，否则不选择 IP 地址。默认为不选择 IP 地址。

4. **TCP/UDP 端口号**

TCP/UDP 端口号用来为数据帧计算目的端口。“勾选”可使用端口号，否则不选择端口号。默认为不选择端口号。

汇聚组设置：

组 ID—表示包含在同一行中的群组 ID 设置。群组 ID 为“Normal”表示没有汇聚。每个端口只有一个组 ID 有效。

端口成员— 显示每组汇聚中的每个交换端口。选择一个单选按钮可在汇聚组中包含该端口，也可以点击该端口的“Normal”单选按钮使该端口从汇聚在中移除。默认情况下，没有任何端口属于任何汇聚组。

4.3.4.2 LACP 设置

请点击导航栏的“G3024→功能设置→链路汇聚设置→LACP”，即可进入 LACP 配置界面，如下图：

本页面可允许用户检查和设置 LACP 的端口设置。各参数的描述如下：

端口：交换机的端口号。

启用 LACP：是否在交换机端口上启用 LACP。当 2 个或更多的端口连接到同一设备时，LACP 将形成汇聚。每个交换机最多可形成 12 组端口汇聚。

密钥：由端口触发的密钥值，范围为 1 ~ 65535。“Auto”设置将设置物理连接速度对应合适的密钥值：10Mb = 1, 100Mb = 2, 1Gb = 3。选择“指定”设置时，用户可输入自定义的取值。端口具有相同的密钥值可加入到相同的汇聚组中，而不同密钥值的端口则不能加入同一汇聚组中。

角色：角色显示的是 LACP 活动状态。“主动方式”将在每秒钟发送 LACP 数据包，而“被动方式”将等待来自相连设备的 LACP 数据包。

4.4 生成树设置界面

4.4.1 生成树简介

STP（Spanning Tree Protocol，生成树协议）是用来避免链路环路产生的广播风暴，并提供链路冗余备份的协议。对以太网来说，两个设备间只能有一条活动的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。STP 协议就自动的完成这项工作。它能使一个局域网中的交换机起如下作用：

1. 发现并启动局域网的一个最佳的树型拓朴结构。
2. 发现故障并随之进行恢复，自动更新网络拓朴结构，使得在任何时候都选择了可能的最佳的树型结构。局域网的拓朴结构是根据管理员设置的一组网桥配置参数自动进行计算的。如果配置得当，使用这些参数能够生成最好的一棵拓朴树，得到最佳方案。

4.4.2 快速生成树简介

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）完全向下兼容 802.1d STP 协议，除了和传统的 STP 协议一样具有避免回路、提供冗余链路的功能外，最主要的特点就是“快速收敛”。如果一个局域网内的网桥都支持 RSTP 协议且管理员配置得当，一旦网络拓朴改变而要重新生成拓朴树只需要极短时间（传统的 STP 需要大约 50 秒，RSTP 只需要 1 秒左右）。

RSTP能快速的转变到转发状态，不再依赖计时器的设置。RSTP桥接对于其他RSTP桥接链接的反应非常敏感。端口无需等待拓扑的稳定。为了快速过渡，协议中引入了两种新的变量：边缘端口和点对点（P2P）端口。下面来介绍边缘端口和点对点端口：

1. 边缘端口

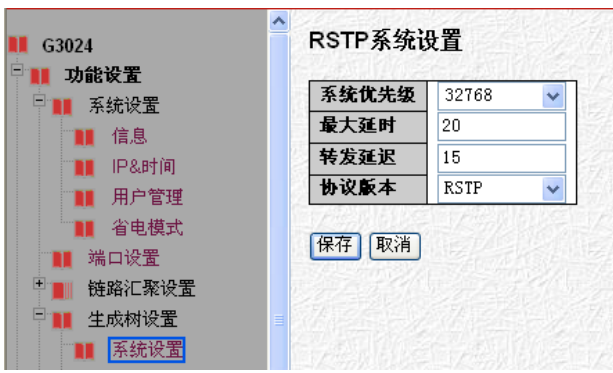
边缘端口是一个可以被设置的指定端口，可直接连接到无环路的网络端口。通常就是端口直接连接到单个工作站。指定为边缘端口可快速迁移到转发状态，而不需要经历监听和学习的状态。如果接收了一个BPDU数据包，边缘端口可立即丢失其状态，变成一个普通的生成树端口。

2. 点对点端口

点对点端口可以进行快速的迁移，可以连接到其他的桥接。在RSTP/MSTP下，所有在全双工模式下的端口被认为点对点端口，除非手动设置。在使用生成树的协议时，三种生成树之间的兼容性可以相互进行，并没有协议之间的冲突以及在使用中出现瘫痪问题。

4.4.3 生成树系统配置界面

请点击导航栏的“G3024→功能设置→生成树设置→系统设置”，即可进入生成树系统配置界面，如下图：



本页面可用于设置 RSTP 的系统设置。该设置用于所有 RSTP 的桥接实例。所有参数描述如下：

系统优先级：代表桥 ID 的优先级别。数值越小，代表优先级越高。

最大延时：根桥传输信息的最大存活时间。有效值为 6~200 秒。

转发延时：STP 桥从根和目的端口转变为转发状态的延迟时间（用于 STP 的兼容模式）。有效取值为 4～30 秒。

协议版本：版本分为 STP 兼容模式和 RSTP 模式。STP 兼容模式表示交换机工作在 STP 兼容模式下；RSTP 模式表示交换机工作在 RSTP 模式下。

说明：

1. Hello Time 不能设置，系统默认为 2s。
2. Hello时间不能长于最大延时。否则，设置发生错误。在设置上述参数时请参考下列公式。

最大延时 ≤ 2 x (转发延时 - 1秒)

最大延时≥ 2 x (Hello Time + 1秒)

4.4.4 生成树端口配置界面

请点击导航栏的“G3024→功能设置→生成树设置→端口设置”，即可进入生成树端口配置界面，如下图：

本页面用于查看和更改当前 RSTP 端口设置。其设置大多是针对汇聚和物理端口。各参数描述如下：

端口：RSTP 的逻辑端口号。

启用 RSTP：是否在交换机端口启用 RSTP。

路径开销：端口形成的路径开销。“自动”将设置与物理链路速度合适的路径开销，一般采用 802.1d 推荐的值。“指定”设置表示用户可以输入一个自定义的取值。路径开销用于建立网络的拓扑结构。例如，哪些端口用于转发，而哪些端口用于阻塞。百兆端口默认路径开销为 200000. 千兆端口默认路径开销为 20000。有效取值的范围为 1 ~ 200000000。

优先级：端口的优先级，用于控制有相同路径开销的端口优先级。数值越小，优先级越高。

边缘端口：判断端口是否直接连接到边缘设备。一旦在边缘端口上接收到任何 BPDU 数据包，则边缘的标记将取消。边缘端口切换到转发状态的速度要快。（仅针对物理端口，汇聚则永远是非边缘。）

P2P 端口：判断端口是否连接到共享局域网段。一般由其 auto 决定，或强制为 True 或 false。点到点的属性也影响转发状态的速度。非共享链路的切换速度更快。（仅针对物理端口，汇聚则总是强制点到点。）

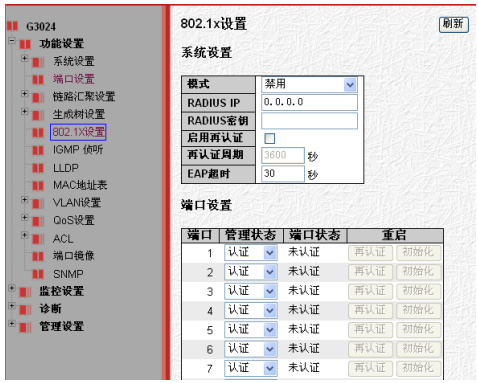
4.5 802.1x 设置界面

4.5.1 802.1x 简介

G3024 交换机提供基于端口的 802.1x 认证功能，提高网络的安全性。802.1x 提出基于数据链路层的认证模式，其认证系统由认证客户端、认证系统和认证服务器三部分组成。认证客户端指局域网所连接的一端的实体，它向认证系统发起请求，对其身份的合法性进行检验。认证系统是运行在认证用户端和网络设备上的实体；而认证服务器是向认证客户端提供具体认证服务的实体。其中，运行认证客户端网络设备上每个物理端口对应一个认证者实体，负责利用认证服务器对与该端口相连接的用户认证，并根据认证结果决定是否对该用户开放端口服务。认证客户端处于核心地位，使 802.1x 认证模式极具扩展性，可兼容多种认证方法。 802.1x 采用加密算法提高认证安全性。认证者和申请者间信息交互采用 RC4 加密算法，而认证者和认证服务器间的交互采用 MD5 加密算法或者 HMAC-MD5 加密算法。这些加密算法能够为认证信息提供较高的安全保证。同时协议本身已经考虑到将来的系统扩展，将安全强度更高的加密算法引入到 802.1x 系统中。

4.5.2 802.1x 配置界面

请点击导航栏的“G3024→功能设置→802.1x 设置”，即可进入 802.1x 配置界面，如下图：



本界面用于设置 IEEE 802.1x 系统配置和端口属性。IEEE802.1x 标准定义了基于端口的访问控制协议，要求用户首先提交认证证书以防止对网络的非授权访问。802.1x 的设置包含了两个部分：系统设置和端口设置。下面就分两部分对各个参数进行详细说明：

系统设置：

模式：表示在交换机中是否全局启用/禁用 802.1x 标准。

RADIUS IP：RADIUS 服务器的 IP 地址。

RADIUS 密钥：RADIUS 服务器和交换机间的密钥（长达 29 个字符）。

启用再认证：如果勾选，用户在经过一个再认证周期后需要重新认证。认证用于检测是否有新的用户接入交换机的端口。同时也是检测通过认证的客户端是否链接正常，此过程对用户透明。

再认证周期：已连接用户必须再认证周期时间（单位为秒）。只有在“启用再认证”中勾选，本参数才可激活。有效取值为：1～3600 秒。

EAP 超时：交换机在重新传送数据包之前，等待客户端反应的时间。

取值为：1～255 秒。系统默认为 30 秒。

说明：

本页面设置的服务器参数必须和服务器的实际参数相同，否则，802.1x 客户端的所有认证信息将不能传输到 RADIUS 认证服务器进行认证。

端口设置：本表格用于对当前交换机中的每个端口设置如下属性：

端口：表示端口 ID。不可更改。

管理状态：设置端口的认证模式，包括：

自动：要求 802.1x-aware 的客户端需要认证服务器的认证。不是 802.1x-aware 的客户端将拒绝访问。

认证：强制端口允许所有的客户端访问，包括 802.1x-aware 客户端和非 802.1x-aware 的客户端。

未认证：强制端口拒绝所有的客户端访问，包括 802.1x-aware 客户端和非 802.1x-aware 的客户端。

端口状态：表示端口所处的认证状态，包括：

禁用 802.1X: 表示全局禁用 802.1x 认证标准。

未连接：表示启用了 802.1x，但是端口未连接上。

认证：表示端口处于认证状态。这种情况一般表示，启用了 802.1x，端口已经连接上，管理状态为“自动”并且客户端需要认证，或管理状态为“认证”。

未认证：表示端口处于未认证状态。这种情况一般表示，启用了 802.1x，端口已经连接上，管理状态为“自动”，但是客户端未（或还没有）认证，或管理状态为“未认证”。

重启：在每行中有两个按钮。只有当启用了 802.1x，端口状态为“auto”时，两个按钮才可用。点击这两个按钮不会使页面中的其它设

置生效。

再认证：当端口的安静周期（等待周期）超时时，设置再认证的时间。

初始化：忽视端口的安静周期并立即启用再认证，而不管当前安静周期的状态。

设置再认证的原因：如果再认证失败，IEEE802.1x 标准将强制进**再认证**。 在**再认证**时，认证者（交换机）将处于安静状态，并不会再认证。来自客户端的数据包也将被丢弃，以防止蛮力攻击。

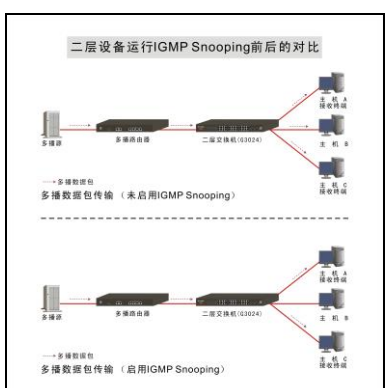
4.6 IGMP 侦听

4.6.1 IGMP 侦听的概述

IGMP Snooping（Internet Group Management Protocol Snooping，IGMP侦听）是运行在二层以太网交换机上的组播约束机制，用于管理和控制组播组。

4.6.2 IGMP 侦听的原理

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包。当二层设备没有运行 IGMP Snooping 时，组播数据包在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据包不会在二层被广播，而在二层被组播给指定的接收者，但是未知组播数据包仍然会在二层广播。 G3024 启用 IGMP Snooping 前后的对比：



4.6.3 IGMP 侦听的工作机制

运行了IGMP Snooping的交换机对不同IGMP报文处理，具体处理方式如下面的描述：

1. 组查询

IGMP查询器定期向本地网段内的所有主机与网络设备（例如：路由器）发送IGMP通用查询报文，以查询该网段有哪些组播组的成员。在收到IGMP通用查询报文时，交换机将其通过VLAN内除接收端口以外的其它所有端口转发出去，并对该报文的接收端口做处理（主要是端口老化定时器的重置和启动）。

2. 报告成员关系

以下情况，主机会向组播路由器发送IGMP成员关系报告报文：

当组播组的成员主机收到IGMP查询报文后，会回复IGMP成员关系报告报文。

如果主机要加入某个组播组，它会主动向组播路由器发送IGMP成员关系报告报文以声明加入该组播组。在收到IGMP成员关系报告报文时，交换机将其通过VLAN内的所有路由器端口转发出去，从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做相应处理（主要是端口老化定时器的重置和启动）。交换机不会将IGMP成员关系报告报文通过非路由器端口转发出去。

3. 离开组播组

运行IGMP V1的主机离开组播组时不会发送IGMP离开组报文，因此当其对应的成员端口的老化定时器超时后，交换机就会将该端口对应的转发表项从转发表中删除。

运行IGMP V2或IGMP V3的主机离开组播组时，会通过发送IGMP离开组报文，以通知组播路由器自己离开了某个组播组。

当从最后一个成员端口上收到IGMP离开组报文时，交换机会将该报文通过VLAN内的所有路由器端口转发出去，同时由于并不知道该报文的接收端口下是否还有该组播组的其它成员，所以交换机不会立刻把该端口对应的转发表项从转发表中删除，而是重置该成员端口的老化定时器。

当IGMP查询器收到IGMP离开组报文后，从中解析出主机要离开的组播组的地址，并通过接收端口向该组播组发送IGMP特定组查询报文。交换机在收到IGMP特定组查询报文后，将其通过VLAN内的所有路由器端口和该组播组的所有成员端口转发出去。

对于 IGMP 离开组报文的接收端口，交换机在该成员端口的老化时间内：如果从该端口收到了主机发送的响应该组播组的 IGMP 成员关系报告报文，则表示该端口下还有该组播组的成员，于是重置该成员端口的老化定时器；如果没有从该端口收到主机发送的响应该组播组的 IGMP 成员关系报告报文，则表示该端口下已没有该组播组的成员，则在该成员端口老化时间超时后，将转发表中该端口对应该组播组的转发表项删除。

4.6.4 IGMP 侦听配置界面

请点击导航栏的“G3024→功能设置→IGMP 侦听”，即可进入 IGMP 侦听配置界面，如下图：

本页面提供了 IGMP 侦听的相关设置信息。而且 IGMP 侦听中的大部分设置是针对全局的，各个参数的描述如下：

启用 IGMP 侦听：全局启用 IGMP 侦听。

启用未注册 IPMC 洪泛：使未注册的 IPMC 流量洪泛

VLAN ID：VLAN 组的编号。

启用 IGMP 侦听：基于每个 VLAN 启用 IGMP 侦听。

IGMP 查询：基于每个 VLAN 启用 IGMP 查询。

路由端口：路由端口是指接收从组播路由器发送来的 IGMP 数据包的端口。通常来说，该端口会连接到路由器或因特网。建立一个路由端口可使来自路由器的多播数据包传播到网络上，也可使来自网络上的多播信息（IGMP）能传播到路由器上。如果汇聚成员端口中的端口被选为路由端口，汇聚将由该路由端口来担任。

4.7 链路层发现协议

4.7.1 链路层发现协议概述

LLDP 是 IEEE 802.1ab 标准协议。链路层发现协议用于网络发现，并与网络中邻居设备使用 LLDP 数据帧交互信息。

4.7.2 链路层发现协议配置界面

请点击导航栏的“G3024→功能设置→LLDP”，即可进入链路层发现协议配置界面，如下图：

本页面可允许用户检查和设置当前 LLDP 的全局和端口设置。本页面分为两部分进行说明：

1. LLDP 参数：

Tx 间隔：交换机周期性的发送 LLDP 数据帧到相邻设备，用于更新网络的发现信息。每个 LLDP 数据帧之间的间隔是由 Tx 间隔

值决定。有效取值限制在 5～32768 秒。

Tx Hold：每个 LLDP 数据帧包含的信息有一个有效时长。LLDP 信息的有效时长是由 Tx Hold 乘以 Tx 间隔来计算的。有效取值限制在 2-10 倍。

Tx 延时：如果设置信息发生改变（如 IP 地址），将传送新的 LLDP 数据帧。但是 LLDP 数据帧间的时间将至少是 Tx 延迟的取值。Tx 延迟不能大于 1/4 的 Tx 间隔时间。有效值限制为 1～8192 秒。

Tx 重初始化：当某个端口禁用、LLDP 禁用或交换机重启，一个 LLDP 关闭数据帧将传送到相邻的单元，以告之 LLDP 信息不再有效。Tx 重初始化控制了关闭数据帧和新 LLDP 初始化间的时间。有效取值限制为 1-10 秒。

2. LLDP 端口设置：

端口：表示 LLDP 的逻辑端口号。

模式：供选择的 LLDP 模式，分为以下 4 种：

仅接收：交换机将不发出 LLDP 信息。但是需要解析来自相邻单元的 LLDP 信息。

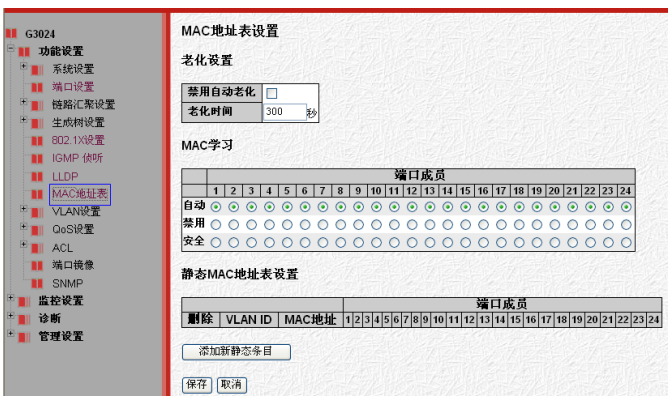
仅发送：交换机将丢弃来自相邻的 LLDP 信息，但自动发出 LLDP 信息。

禁用：交换机将不发出 LLDP 信息，并丢弃来自相邻的 LLDP 信息。

启用：交换机将发出 LLDP 信息，并解析从相邻接收的 LLDP 信息。

4.8 MAC 地址表配置界面

请点击导航栏的“G3024→功能设置→MAC 地址表”，即可进入 MAC 地址表配置界面，如下图：



在本页用于设置 MAC 地址表。在动态 MAC 地址表中为各 MAC 地址条目设置超时时间。在本页还可用于设置静态 MAC 地址表。分为以下 3 部分进行描述：

4.8.1 老化设置

默认情况下 动态 MAC 地址条目在 MAC 地址表中的老化时间为 300 秒。在老化时间后输入一个数值即可设置老化时间。可允许的取值范围为：10～1000000 秒。如需禁用动态条目的自动老化时间，请在“**禁用自动老化**”的方框内勾选。

4.8.2 MAC 地址表学习

基于下列参数可设置每个端口 MAC 地址学习：

自动：一旦有未知的源 MAC 数据帧接收到，对其进行自动学习。

禁用：不执行学习功能。

安全：只学习静态 MAC 地址条目。其它的数据帧将丢弃。

⚠ ***注意：***

在切换到安全学习模式前，请确定用于管理交换机的链路已添加至静态 MAC 地址表中。否则管理链路将失去，只能通过另外一个非安全端口或通过串口连接到交换机将其保存。

4.8.3 静态 MAC 地址表设置

在 MAC 地址列表中显示的是静态 MAC 地址条目。 静态 MAC 地址表可最多包含 64 个条目。最多 64 个条目针对整个交换机。本 MAC 地址表根据 VLAN ID 和 MAC 地址整理而成。各参数描述如下：

删除：勾选后可删除条目。勾选后该条目将在下一次保存时删除。

VLAN ID：MAC 地址条目对应的 VLAN ID 号。

MAC 地址：条目的 MAC 地址。

端口成员：打勾标记表示端口为条目的成员。需要修改该条目时，可选择打勾或不打勾。

添加新静态条目：点击“添加新静态条目”可添加新的条目至静态 MAC 地址表中。然后为新条目指定 VLAN ID、MAC 地址和端口成员。点击 “保存”即可完成设置。

4.9 虚拟局域网

4.9.1 虚拟局域网概述

VLAN (Virtual Local Area Network)，又称虚拟局域网，是一种通过将局域网内设备在逻辑上，而非物理上划分成一个个网段从而实现虚拟工作组的网络拓扑结构。IEEE于1999年颁布了用以标准化VLAN实现方案的802.1Q协议标准草案。

在物理上划分的局域网通常被定义为一个单独的广播域，主要使用Hub，网桥，或交换机等网络设备连接同一网段内的所有节点。虽然交换机具备根据报文的目的MAC地址进行转发的能力，但在收到广播报文或未知单播报文（报文的目的MAC地址不在交换机MAC地址表中）时，会向接收端口之外的所有端口转发。当网络中的主机收到大量并非以自身为目的地的报文时，这就给网络带来严重的安全隐患。解决以上网络问题的根本方法就是隔离广播域。传统的方法是使用路由器，因为路由器是依据目的IP地址对报文进行转发，不会转发链路层的广播报文。但是路由器的成本较高，而且端口较少，无法细致地划分网络，所以使用路由器隔离广播域有很大的局限性。为了解决以太网交换机在局域网中无法限制广播的问题，VLAN技术应运而生。通过VLAN，我们可以在局域网上将有共同需求的计算机工作站进行逻辑分组，分组间隔绝广播。组内的工作站位于同一个广播域，与物理位置无关，像连接在同一个网段上一样正常通信。由于广播包的隔绝，组间即VLAN间不能直接通信，必须经过路由器或其它三层转发设备转发。

4.9.2 VLAN 的优点

正是由于 VLAN 彼此内部的广播和单播流量都不会相互转发，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

1. **控制网络的广播风暴**

   采用 VLAN 技术，局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。

2. **减少设备投资**

   传统上通过路由器来隔离广播风暴的方法加大的管理控制的成本。VLAN的应用正是使成本控制成为可能。

3. **简化网络管理**

   使用VLAN可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。例如需要为完成某个项目建立一个工作组网络，其成员可能遍及全国或全世界，此时，网络管理员只需设置几条命令，就能在几分钟内建立该项目的VLAN网络，其成员使用VLAN网络，就像在本地使用局域网一样。

4. **确保网络安全**

   由于报文在数据链路层被VLAN划分的广播域所隔离，因此各个VLAN内的主机间不能直接通信，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。

4.9.3 VLAN 的划分

根据划分方式的不同，可以将 VLAN 分为不同类型，常用的几种划分方式如下：

1. **基于端口的 VLAN**

   基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。

2. **基于 MAC 地址的 VLAN**

   由于网卡分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划分于某个 VLAN。事实上，该类型的 VLAN 是一些 MAC 地址的集合。当设备移动时，VLAN 能够自动识别。网络管理需要管理和配置设备的 MAC 地址，显然当网络规模很大，设备很多时，会给管理带来难度。

3. **基于 IP 子网的 VLAN**

   基于 IP 子网的 VLAN 是指所有的流量根据源/目的 IP 子网进行分配。其中，局域网交换机允许一个子网扩展到多个局域网交换端口，甚至允许一个端口对应于多个子网。

4. **基于协议的 VLAN**

   基于协议的 VLAN 是指，在 VLAN 中，流量的传送根据协议来分配。不同的端口可以指定不同的协议类型。如 1 端口可以用来传送 IP 协议的数据包，而其他端口则可以传送其他协议类型的数据包。

   鉴于当前业内 VLAN 发展的趋势，考虑到各种 VLAN 划分方式的优缺点，为了最大程度上地满足用户在具体使用过程中需求，减轻用户在 VLAN 的具体使用和维护中的工作量，G3024 交换机采用根据端口来划分 VLAN 的方法。

4.9.4 VLAN 成员配置界面

请点击导航栏的“G3024→功能设置→VLAN 设置→VLAN 成员”，即可进入 VLAN 成员配置界面，如下图：

本页面用于监控和修改交换机的 VLAN 成员设置。最多可支持 64 组 VLAN 除了可在本页面中添加和删除 VLAN，同时还可以为每个 VLAN 组添加和删除 VLAN 端口成员，各参数描述如下：

删除：勾选该方框可删除 VLAN 条目。在保存时，该 VLAN 条目将在交换机中被删除。当前我们的 VLAN1 及成员是不可删除的。

VLAN ID ：表示交换机中的 VLAN 组的编号。

端口成员：每个 VLAN ID 会为每个端口显示一行方框，点击该方框，可将该端口包含在该 VLAN 中。默认情况下，VLAN 中没有端口成员。

添加 VLAN：点击“添加新 VLAN”，可添加一个新的 VLAN。在列表中将添加一个空行。可根据需要，对 VLAN 进行设置。VLAN ID 的有效值从 1 到 4094。点击“保存”后，将在选择的交换机单元中启用 VLAN。

4.9.5 VLAN 的端口配置界面

请点击导航栏的“G3024→功能设置→VLAN 设置→端口设置”，即可进入 VLAN 的端口配置界面，如下图：

本页面用于设置交换机的端口在 VLAN 中的状态。各参数描述如下：

端口：VLAN 的逻辑端口号。

VLAN Aware：点击方框可为该端口启用 VLAN awareness。参数可影响 VLAN 的入站过程。如果启用 VLAN awareness，端口接收的数据帧将会把 tag 标记去除掉。而且，这些含有 tag 的数据帧在标记中通过 VLAN ID 来划分。如果禁用 VLAN awareness， 所有的数据帧将将划分到端口 VLAN ID 中，并不会移除标记。默认情况下，VLAN awareness 是禁用的。

入站过滤：点击该方框可启用端口的入站过滤。该参数可影响 VLAN 的入站过程。如果启用了入站过滤，若数据包进入端口不是帧所映射的 VLAN 的成员，则丢弃数据包。默认情况下，入站过滤为禁用。

帧类型：决定端口是接收所有的数据帧，还是仅接收 tag 数据帧。该

参数会影响 VLAN 的入站过程。如果端口仅接收带有 tag 的数据帧，那么在端口接收了没有 tag 的数据帧将被抛弃。默认情况下，帧类型设置为“All”。

端口 VLAN/模式：设置端口的 VLAN 模式。可允许的取值为“None”和“指定”。该参数影响 VLAN 的入站和出站过程。

如果选择“None”，已划分 VLAN ID 的 VLAN 标记将插入端口发送的数据帧中。这种模式，通常用于在端口连接了 VLAN aware 交换机上。如果选择“指定”（默认值），端口的 VLAN ID 可进行如下设置。在端口接收的 untag 数据帧将划分到端口 VLAN ID 中。如果禁用了 VLAN awareness，端口接收的所有数据帧将将划分到端口 VLAN ID 中。如果端口发送了的数据帧中 VLAN ID 不同于端口 VLAN ID, VLAN ID 的 tag 将插入该数据帧中。

端口 VLAN/ID：设置端口 VLAN 的标识符。可允许的取值为 1～4094。默认值为 1。

4.10 服务质量

4.10.1 QoS 概述

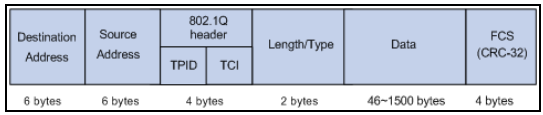
QoS(Quality of Service)，中文名为“服务质量”。它是指网络提供更高优先服务的一种能力，包括专用带宽、抖动控制和延迟（用于实时和交互式流量情形）、丢包率的改进以及不同 WAN 和 LAN 技术下的指定网络流量等，同时确保为每种流量提供的优先权不会阻碍其它流量的进程。

QoS 是网络的一种安全机制, 是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

4.10.2 常用优先级

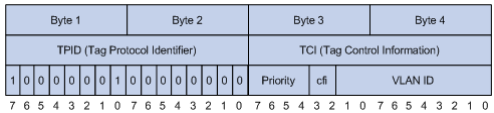
1. 802.1p 优先级

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。带有 802.1Q 标签的数据包才带有 802.1p 优先级，如下图所示，4 个位的 802.1Q 标签头包含了 2 个位的 TPID（Tag Protocol Identifier，标签协议标识，取值为 0x8100）和 2 个位的 TCI（Tag Control Information，标签控制信息）



带有 802.1Q 标签头的以太网帧

下图显示了 802.1Q 标签头的详细内容，TCI 中 Priority 字段就是 802.1p 优先级，也称为 COS 优先级。它由 3 个 bit 组成，取值范围为 0～7。

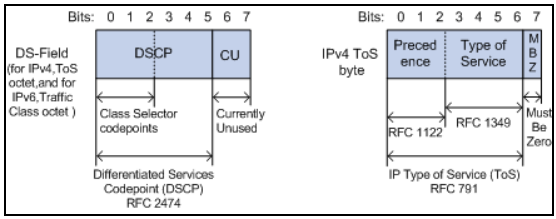


802.1Q 标签头

2. DSCP 优先级

在 IP 数据包的包头带有 DSCP 优先级，IP header 的 ToS 字段有 8 个 bit，其中：

前 3 个 bit 表示的是 IP 优先级，取值范围为 0～7；
第 3～6 这 4 个 bit 表示的是 ToS 优先级，取值范围为 0～15；
RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域，其中 DSCP（Differentiated Services Code point，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。



DS 域和 ToS 字节

4.10.3 调度方式

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。G3024 支持 SP（Strict-Priority，严格优先级队列）和 WFQ(Weighted Fair 队列，加权公平队列)调度。

1. 严格优先级队列

SP 队列调度算法是针对关键业务型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有 4 个输出队列为例 ,优先队列将端口的 4 个输出队列分成 4 类，依次为 High、Medium、Normal 和 Low 队列，它们的优先级依次降低。

在队列调度时，SP 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务（如 E-Mail）的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

2. 加权公平队列

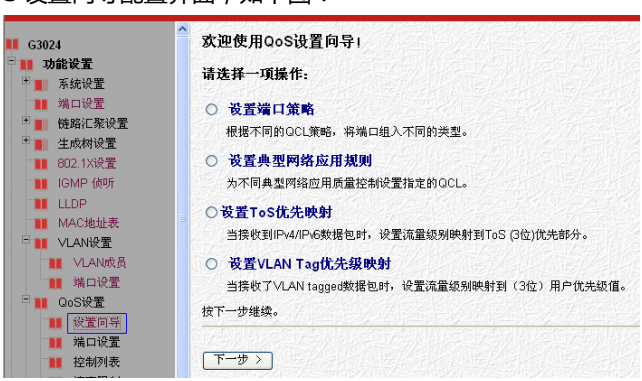
Weighted Fair 队列 ,加权公平队列。WFQ 将分组按照不同的业务流、不同的 IP 优先级，自动按照 HASH 算法，划分成不同的队列，在保证高优先级业务的同时，按照配置权重，将带宽公平地分给低优先级别的业务。G3024 在每个接口上最大支持 4 个队列，在此范围之内，

网络管理员可以配置队列的数目和相应权值。WFQ 的优点是对所有应用都能比较公平地提供服务质量，对于要求较高的业务可以通过设置权重保障优先级，能智能划分队列和调度，配置相对简单，对网络管理员要求相对较低；缺点是由于相对公平，对于 QOS 要求极高的应用，不能象 PQ 那样绝对保证，策略计算复杂，比较消耗系统处理能力。它适用于应用较复杂，并且应用相对公平的网络，如 Internet 网。

4.10.4 QoS 配置

4.10.4.1 设置向导界面

请点击导航栏的“G3024→功能设置→QoS 设置→设置向导” ,即可进入 QoS 设置向导配置界面，如下图：



本向导可帮助您快速设置 QCL，免除各参数的繁杂设置。根据向导配置方式分为以下 4 种：

1. 设置端口策略 ：

根据不同的 QCL 策略，将端口设置为不同的类型。各参数描述如下：

QCL ID：将匹配该 QCE 数据帧类型的数据帧配置到指定的 QCL。

端口成员：在每个 QCL ID 前每个端口有一个单选按钮。点击某单选按钮，即可将该端口包含在 QCL 成员中。

2. 安装典型网络应用规则

为不同典型网络应用质量控制设置指定的 QCL。各参数描述如下：

语音视频：表示将常用的服务器应用到指定的 QCE 中。常用的服务器有：QuickTime 4 Server、MSN Messenger Phone、Yahoo Messenger Phone、Napster 和 Real Audio 等。

游戏：表示将常用的游戏应用到指定 QCE。常用的游戏有：Blizzard Battlenet (Diablo2 and StarCraft)、Fighter Ace II、Quake2、Quake3 和 MSN Game Zone。

用户定义：表示将用户自定义的应用映射到指定的 QCE。用户定义有：

以太网类型：为该 QCE 设置以太网类型过滤。可用范围为：0x600~0xFFFF。

VLAN ID：为该 QCE 设置 VLAN ID 过滤。可用范围为：1~4094。

UDP/TCP 端口：为该 QCE 设置 UDP/TCP 端口过滤。可用范围为：0～65535。

DSCP：为该 QCE 设置 DSCP 过滤。可用范围为：0～63。

3. 设置 ToS 优先映射

当接收到了 IPv4/IPv6 数据包时，设置流量级别映射到 ToS 的优先部位。各参数描述如下：

QCL ID：选择这些 QCE 应用的 QCL ID。

ToS 优先级别 :选择应用到 QCE 的流量级别 :Low、Normal、Medium 或 High。

4. 设置 VLAN Tag 优先级映射

当接收了带 VLAN 标记数据包时，设置流量级别映射到用户优先级（3 位）。各参数描述如下：

QCL ID：选择这些 QCE 应用的 QCL ID。

VLAN 优先级别：选择应用到 QCE 的流量级别：Low、Normal、Medium 或 High。

4.10.4.2 端口设置界面

请点击导航栏的“G3024→功能设置→QoS 设置→端口设置”，即可进入 QoS 端口配置界面，如下图：

本页面用于对每个端口进行 QoS 设置。数据帧可以划分为 4 种不同的 QoS 级别：Low、Normal、Medium 和 High。分配到每个端口的 QoS

控制 QoS 的分类。一个 QCL 是由 12QCE 按照一定的顺序构成。每个 QCE 可用来划分数据帧到指定的 QoS 级别。而分类是以参数的设置为基础，如 VLAN ID、UDP/TCP 端口、IPv4/IPv6 DSCP 或 Tag 优先级。与任何 QCE 不相匹配的数据帧将被划分到默认 QoS 级别。各参数描述如下：

设置流量级别数：

设置流量级别数 1，2 或 4。默认为“4”。

队列级别：

端口: 设置的逻辑端口。

默认级别 :设置端口的默认 QoS 级。即在 QCL 中没有匹配任何 QCE 数据帧的 QoS 类。

QCL #：选择为端口使用的 QCL。

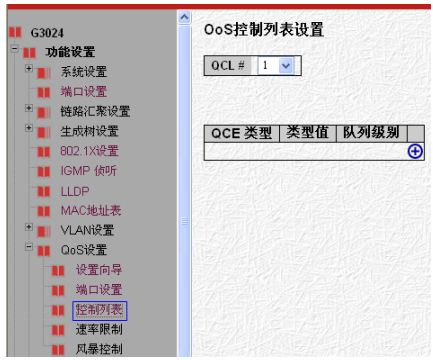
用户优先级：当添加标记了到 untagged 数据帧时，为该端口选择默认用户优先级。

列队模式：为该端口选择列队模式。

列队加权：如果列队模式为 “加权模式”，则可设置列队加权（Low:Normal:Medium:High）。

4.10.4.3 QoS 控制列表设置界面：

请点击导航栏的“G3024→功能设置→QoS 设置→控制列表” ,即可进入 QoS 控制列表配置界面，如下图：



本页面用于对每个端口进行 QoS 设置。数据帧可以划分为 4 种不同的 QoS 级别：Low、Normal、Medium 和 High。分配到每个端口的 QoS 控制 QoS 的分类。一个 QCL 是由 12QCE 按照一定的顺序构成。每个 QCE 可用来划分数据帧到指定的 QoS 级别。而分类是以参数的设置为基础，如 VLAN ID、UDP/TCP 端口、IPv4/IPv6 DSCP 或 Tag 优先级。与任何 QCE 不相匹配的数据帧将被划分到默认 QoS 级别。各参数描述如下：

QCL #：选择 QCL 可显示列出指定 QCL 的所有 QCE 列表。

QCE 类型：设置 QCE 处理的帧用来决定数据帧的 QoS 类别。支持的 QCE 类型有：

以太网类型: 以太网类型域。如果数据帧被标记，在标记头的后面将紧接的就是以太网类型。

VLAN ID：只有数据帧被打上了 VLAN 的标记才可用。

TCP/UDP 端口：IPv4 TCP/UDP 源和目的端口。

DSCP：IPv4 和 IPv6 的 DSCP。

ToS：IPv4 和 IPv6 包头在 ToS 字节中的三个优先位。

Tag 优先级：用户优先级。只有数据帧带有 VLAN 标记或优先标记才可用。

类型值：表示 QCE 类型的取值。

以太网类型：显示以太网类型值。

VLAN ID：显示 VLAN ID 的域。

TCP/UDP 端口范围：显示 TCP/UDP 端口范围的域。

DSCP：显示 IPv4/IPv6 DSCP 的值。

流量级别

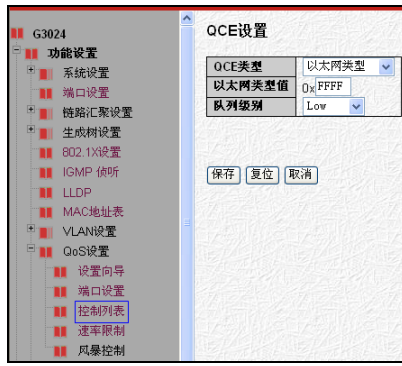
QCE 流量相关的 QoS 级别。

修改按钮

使用下列按钮可修改列表中的每个 QCE。

按钮	意义
+	在当前行插入一个新的 QCE。
e	编辑 QCE。
↑	**向上：**在列表中向上移动 QCE。
↓	在列表中向下移动 QCE。
x	删除 QCE。
+	最下端的“+”标记可在 QCL 列表的下端可添加一个新的条目。

添加和修改 QCE 时将进入以下配置界面：



4.10.4.4 速率限制配置界面

请点击导航栏的“G3024→功能设置→QoS 设置→速率限制” ,即可进入 QoS 速率限制配置界面，如下图：

在本页中为入口方向和出口方向设置交换端口的速率限制。各参数描述如下：

端口：设置的逻辑端口。

入口方向：启用或禁用端口的入口速率限制。默认值为“禁用”。

速率：为端口的入口方向设置速率。默认值为“500”。当单位为“kbps”时，取值范围限定在“500-1000000”；而单位为“Mbps”时，取值范围限定在“1-1000”。

速率：设置端口入口方向速率的单位。默认为“Kbps”。

出口方向：启用或禁用端口的出口速率限制。默认值为“禁用”。

速率：为端口的出口方向设置速率。默认值为“500”。当单位为“kbps”时，取值范围限定在“500-1000000”；而单位为“Mbps”时，取值范围限定在“1-1000”。

速率：设置端口出口方向速率的单位。默认为“Kbps”。

4.10.4.5 风暴控制配置界面

请点击导航栏的“G3024→功能设置→QoS 设置→风暴控制” ,即可进入 QoS 风暴控制配置界面，如下图：

本页面可设置交换机的广播风暴控制，包含了单播风暴速率控制、多播风暴速率控制和广播风暴速率控制。速率的算法是 2^n，n 少于或等于 15。速率的单位不是 pps 就是 kpps。所有的设置表示在整个交换机上对单播，多播或广播流量可允许数据包速率。各参数描述如下：

帧类型: 在行中应用帧类型的设置：单播、多播或广播。

状态：对选定的帧类型启用或禁用风暴控制。

速率(pps)：速率的单位是 pps。可设置的速率有：1、 2、 4、 8、 16、 32、 64、 128、 256、 512、 1K、 2K、 4K、 8K、 16K、 32K、 64K、 128K、 256K、 512K 和 1024K。其中 1kpps 实际上是 1002.1pps。

4.11 访问控制列表

4.11.1 访问控制列表概述

随着网络规模的扩大和流量的增加，对网络安全的控制和对带宽的分配成为网络管理的重要内容。通过对数据包进行过滤，可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。

ACL（Access Control List，访问控制列表）即通过配置对报文的匹配规则和处理操作来实现包过滤的功能。

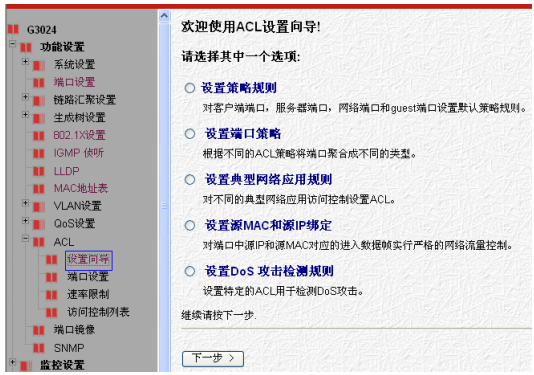
当交换机的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的策略允许或禁止相应的数据包通过。

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是目的 MAC 地址、源 MAC 地址、目的 IP 地址、源 IP 地址、协议以及端口号等。

4.11.2 ACL 配置

4.11.2.1 ACL 配置向导界面

请点击导航栏的“G3024→功能设置→ACL→设置向导”，即可进入 ACL 设置向导配置界面，如下图：

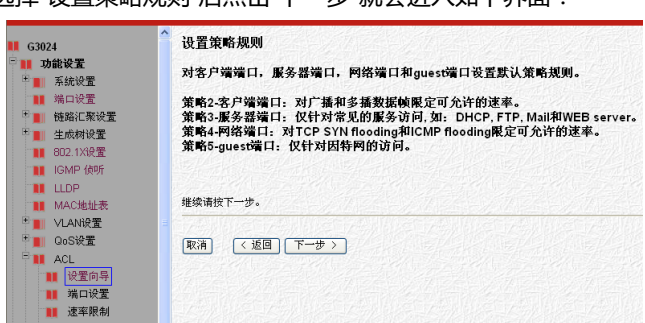


本向导可帮助您快速设置 ACL。分为 5 个类型进行设置：

1. 设置策略规则

对客户端端口，服务器端口，网络端口和 guest 端口设置默认策略规则。

选择“设置策略规则”后点击“下一步”就会进入如下界面：



点击“下一步”，系统就会自动生成以下 4 组策略：

对客户端端口、服务器端口、网络端口或 guest 端口设置默认策略规则。

策略 2-客户端端口：对广播和多播数据帧限定可允许的速率。

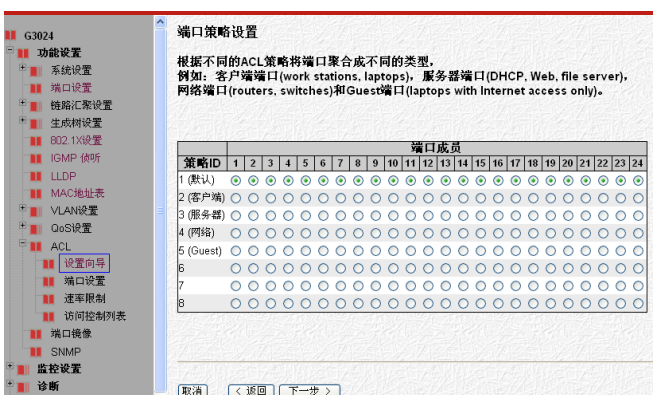
策略 3-服务器端口：仅针对常见的服务访问，如：DHCP、FTP、Mail 和 WEB server。

策略 4-网络端口：对 TCP SYN flooding 和 ICMP flooding 限定可允许的速率。

策略 5-guest 端口：仅针对因特网的访问。

2. 设置端口策略

根据不同的 ACL 策略将端口聚合成不同的类型。选择“设置端口策略”后点击“下一步”就会进入如下界面：



选择针对各种策略的端口后点击“下一步”即可完成该向导的设置。各参数描述如下：

策略 ID：给匹配该 ACE 类型的数据帧设置对应的策略。

端口成员：显示了一行对应每个端口的单选按钮。点击单选按钮可使该端口对应相应的策略。

3. 设置典型网络应用规则

对不同的典型网络应用访问控制设置 ACL。选择“设置典型网络应用

规则”后点击“下一步”就会进入如下界面：

对不同的典型网络应用访问控制设置 ACL。对各参数详细描述如下：

常见服务：

表示一些常见的服务应用到 ACL 中。常见的服务有：DHCP、DNS、FTP、HTTP、IMAP、NFS、POP3、SAMBA、SMTP、TELNET 和 TFTP。

即时通讯：表示即时通讯服务将应用到 ACL 中。常见的即时通讯平台有：Google Talk、MSN Messenger 和 Yahoo Messenger。

用户定义：表示用户定义将应用到 ACL 中。用户定义有：

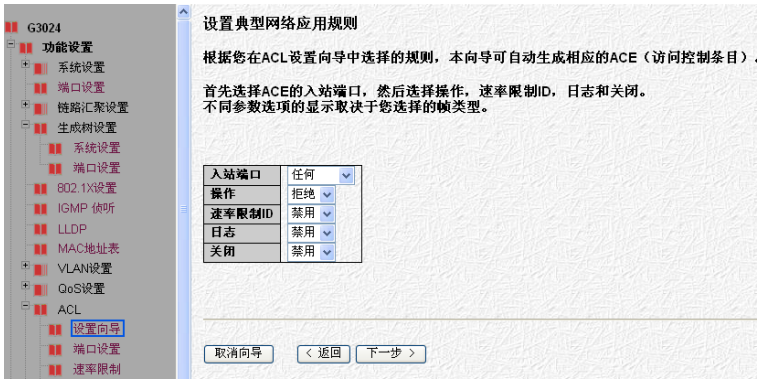
以太网类型：对 ACE 设置以太网类型过滤。范围为 :0x600~0xFFFF。

UDP 端口：对 ACE 设置 UDP 目的端口过滤。范围为：0～65535。

TCP 端口：对 ACE 设置 TCP 目的端口过滤。范围为：0～65535。

其它：表示将其他的应用运用到 ACE 中。其他的应用有：HTTPS、ICMP、Multicast IP Stream、NetBIOS、PING 请求、Ping 响应、SNMP 和 SNMP Traps。

根据应用设置好各参数后点击“下一步”，即可进入如下界面：



根据您在 ACL 设置向导中选择的规则，本向导可自动生成相应的 ACE（访问控制条目）。

首先选择 ACE 的入站端口，然后选择操作、速率限制 ID、日志和关闭。不同参数选项的显示取决于您选择的帧类型。各参数描述如下：

入站端口：选择 ACE 应用的入站端口。

所有：ACE 将应用在任何端口。

端口 n: ACE 应用到该端口号。n 表示交换机的端口号。

策略 n: ACE 应用到该策略。n 的范围为 1～8。

操作：设置数据帧帧符合 ACE。

允许：匹配该 ACE 的数据帧的行为获得允许。

拒绝：丢弃匹配该 ACE 的数据帧。

速率限制 ID：指定速率限制的基础单元数。可选范围为 1～15。“禁用”表示禁止操作速率限制。

日志：指定 ACE 的日志操作。取值如下：

启用: 对应的 ACE 帧将存储至系统日志中。

禁用：对应的 ACE 帧将不列入日志中。

请注意：系统日志内存的大小和日志比率有限。

关闭：设置 ACE 的端口关闭操作。取值为：

启用：如果有数据帧对应该 ACE，入站端口将禁用。

禁用：禁用 ACE 的端口关闭功能。

4. 设置源 MAC 和源 IP 绑定

对端口中源 IP 和源 MAC 对应的进入数据帧实行严格的网络流量控制。选择“设置源 MAC 和源 IP 绑定”后点击“下一步”就会进入如下界面：

对端口中源 IP 和源 MAC 对应的进入数据帧实行严格的网络流量控制。各参数描述如下：

端口：逻辑端口的设置。

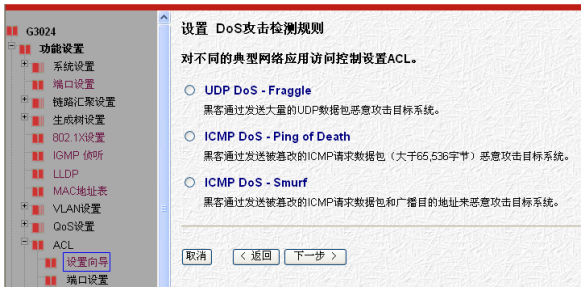
启用绑定：对逻辑端口启用或禁用源 IP 和源 MAC 的绑定。

源 MAC 地址：用于绑定的源 MAC 地址。

源 IP 地址：用于绑定的源 IP 地址。

5. 设置 DoS 攻击检测规则

设置特定的 ACL 用于检测 DoS 攻击。选择“设置 DoS 攻击检测规则”后点击“下一步”就会进入如下界面：



此界面用于对不同的典型网络应用访问控制设置 ACL。分为以下 3 种方式：

UDP DoS 攻击-Fraggle：

黑客通过发送大量的 UDP 数据包恶意攻击目标系统。当目标系统接受到这些数据包时，它会安排不同的应用在相应的目的端口前等候进入。当系统知道目的端口没有任何应用在等待时，它会生成一个 ICMP 数据包发送到伪造的源地址，告之发送的数据包没有到达目的端口。最后造成其他客户端发出的合理应用也无法到达目的端口，从而导致系统资源无法使用。

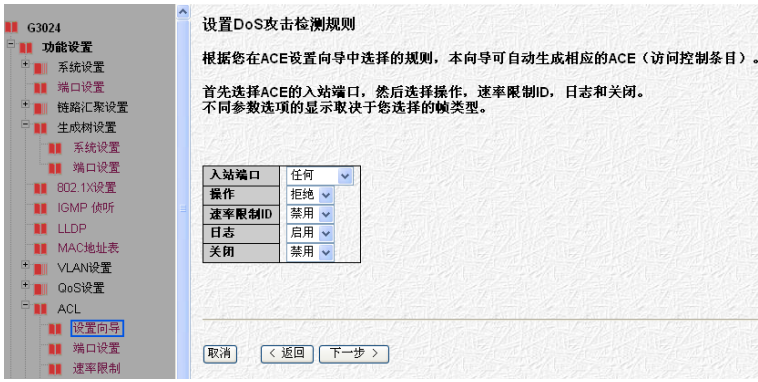
ICMP DoS 攻击-Ping of Death：

黑客通过发送被篡改的 ICMP 请求数据包（大于 65,536 字节）恶意攻击目标系统。一些目标系统由于不能处理这些已经超出最大 IP 包字节的数据包，而导致目标系统的死机，崩溃或重启。

ICMP DoS 攻击-Smurf：

黑客通过发送被篡改的 ICMP 请求数据包和广播目的地址来恶意攻击目标系统。接受到这些数据包后，所有主机会发送一个 ICMP 回应数据包到伪造的源地址。因此这会使目标主机生成大量数据流，而造成网络带宽的拥塞。

根据应用选择其中一种方式，点击“下一步”即可进入以下界面：



此介面用于设置 DoS 攻击检测规则。根据您在 ACL 设置向导中选择的规则，本向导可自动生成相应的 ACE（访问控制条目）。

首先选择 ACE 的入站端口，然后选择操作，速率限制 ID，日志和关闭。不同参数选项的显示取决于您选择的帧类型。各参数描述如下：

入站端口：选择 ACE 应用的入站端口。

所有：ACE 将应用在任何端口。

端口 n: ACE 应用到该端口号。n 表示交换机的端口号。

策略 n: ACE 应用到该策略。n 的范围为 1～8。

操作：设置数据帧帧符合 ACE。

允许：匹配该 ACE 的数据帧的行为获得允许。

拒绝：丢弃匹配该 ACE 的数据帧。

速率限制 ID：指定速率限制的基础单元数。可选范围为 1～15。“禁用”表示禁止操作速率限制。

日志：指定 ACE 的日志操作。取值如下：

启用: 对应的 ACE 帧将存储至系统日志中。

禁用：对应的 ACE 帧将不列入日志中。

请注意：系统日志内存的大小和日志比率有限。

关闭：设置 ACE 的端口关闭操作。取值为：

启用：如果有数据帧对应该 ACE，入站端口将禁用。

禁用：禁用 ACE 的端口关闭功能。

4.11.2.2 ACL 端口配置界面

请点击导航栏的“G3024→功能设置→ACL→端口设置”，即可进入 ACL 端口配置界面，如下图：

端口	策略ID	操作	速率阀ID	端口复制	日志	关闭	计数器
1	1	Permit	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	45
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	0
13	1	Permit	Disabled	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	Disabled	0
15	1	Permit	Disabled	Disabled	Disabled	Disabled	0
16	1	Permit	Disabled	Disabled	Disabled	Disabled	0
17	1	Permit	Disabled	Disabled	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	Disabled	Disabled	1833
19	1	Permit	Disabled	Disabled	Disabled	Disabled	0

对交换机的每个端口设置 ACL 参数。这些参数将会对端口接收的数据帧产生影响，除非该数据帧已对应指定的 ACE。各参数描述如下：

端口：逻辑端口的设置。

策略 ID：选择策略应用于该端口。可选范围为 1～8。默认值为 1。

操作：选择“允许”或“拒绝”转发。默认值为“允许”。

速率限制 ID：选择速率限制应用到该端口。可选范围为：“禁用”和 1~15。默认值为“禁用”。

端口复制：选择端口数据帧将被复制到哪个端口。可选范围为：“禁用”或某端口号。默认值为“禁用”。

日志：设置端口的日志操作。取值有：

启用: 端口接收的数据帧将存储至系统日志中。

禁用：端口接收的数据帧将不列入日志中。

默认值为“禁用”。请注意：系统日志内存的大小和日志比率有限。

关闭：设置端口的端口关闭操作。取值有：

启用: 如果端口接收到数据帧，端口将禁用。

禁用：禁用端口关闭。

默认值为“禁用”。

计数器：计算对应该 ACE 的数据帧数。

4.11.2.3 ACL 速率限制配置界面

请点击导航栏的“G3024→功能设置→ACL→速率限制”，即可进入 ACL 速率限制配置界面，如下图：

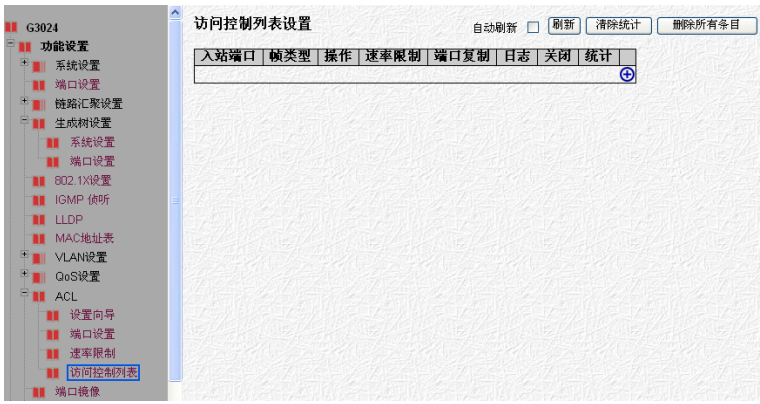
本界面用于交换机的 ACL 速率限制设置。各参数描述如下：

速率限制 ID：设置速率限制的编号。

速率(pps) :速率的单位为包每秒(pps)。可设置的速率有: 1、 2、 4、 8、 16、 32、 64、 128、 256、 512、 1K、 2K、 4K、 8K、 16K、 32K、 64K、 128K、 256K、 512K 或 1024K。

4.11.2.4 ACL 控制列表配置界面

请点击导航栏的“G3024→功能设置→ACL→访问控制列表”，即可进入 ACL 控制列表配置界面，如下图：



本界面显示的是由 ACE 组成的访问控制列表。每行都对已定义的 ACE 进行了描述。最多可设置 128 组 ACE。点击页面最下方的 “+”标识即可添加新的 ACE 至列表中。各参数描述如下：

入站端口：表示 ACE 的入站端口。取值有:

任何: 该 ACE 将对应任何的入站端口。

策略：该 ACE 将对应有特定策略的入站端口。

端口：该 ACE 将对应指定的入站端口。

帧类型：表示 ACE 的数据帧类型。取值有：

任何：该 ACE 将对应任何的数据帧。

以太网: 该 ACE 将对应 Ethernet Type 以太网类型数据帧。

ARP：该 ACE 将对应 ARP/RARP 帧。

IPv4：该 ACE 将对应所有的 IPv4 帧。

IPv4/ICMP：该 ACE 将对应 ICMP 协议中的 IPv4 帧。

IPv4/UDP: 该 ACE 将对应 UDP 协议中的 IPv4 帧。

IPv4/TCP：该 ACE 将对应 TCP 协议中的 IPv4 帧。

IPv4/Other :该 ACE 将对应 IPv4 帧，不包括 ICMP/UDP/TCP。

操作：表示 ACE 的转发操作。

允许：转发和学习对应 ACE 的帧。

拒绝：丢弃对应 ACE 的帧。

速率限制：表示 ACE 的速率限制数。可选范围为 1～15。如果显示为“禁用”，表示禁用速率限制的操作。

端口复制：表示 ACE 的端口复制操作。对应的 ACE 帧将复制到某端口号。可选值为“禁用”或某端口号。如果显示为“禁用”，表示禁用端口复制的操作。

日志：表示 ACE 的日志操作。取值有：

启用：对应的 ACE 帧将存储至系统日志中。

禁用：对应的 ACE 帧将不列入日志中。

请注意：系统日志内存的大小和日志比率有限。

关闭：表示 ACE 的端口关闭操作。取值有：

启用：如果有数据帧对应 ACE，入站端口将关闭。

禁用：禁用 ACE 的端口关闭。

计数器：计数器表示数据帧符合 ACE 的次数。

修改按钮 :使用下列按钮可对列表中所有 ACE (访问控制条目)进行修改：

“+”：在本行前插入一条新的 ACE。

“e”：编辑该 ACE 行。

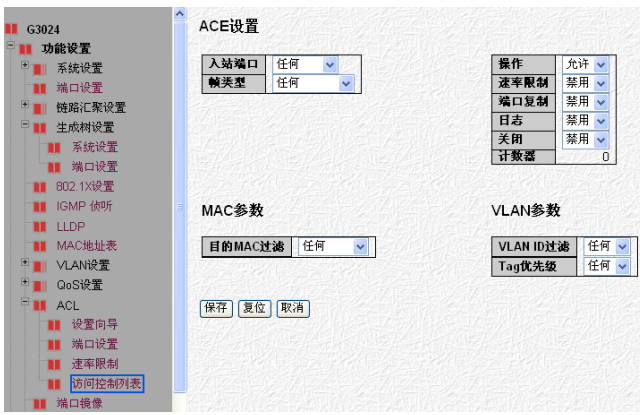
“↑”：向上移动。

“↓”：向下移动。

“×”：删除。

“+”：点击最下方的“+”标识可在 ACE 列表的下端添加新的条目。

点击最下方的“+”标识即可进入“访问控制条目设置界面”：



本界面用于描述如何设置 ACE（访问控制条目）。

ACE 条目由多个参数构成。根据您选择的帧类型，参数而有所变动。首先选择 ACE 的入站端口，然后选择帧类型。不同的参数选项取决于您选择的帧类型。

关于符合 ACE 的数据帧对应设置，定义如下：

入站端口：选择 ACE 应用的入站端口。

任何：该 ACE 应用到任何端口。

端口 n: 该 ACE 应用到某端口号。n 表示交换机的端口号。

策略 n: 该 ACE 应用到某策略。n 的范围为 1～8。

帧类型：为该 ACE 选择帧类型。

任何：任何帧可应用该 ACE。

以太网类型：仅以太网类型能应用到该 ACE。

ARP：仅 ARP 帧可应用到该 ACE。

IPv4: 仅 IPv4 帧可应用到该 ACE。

操作：指定数据帧符合该 ACE 的行为。

允许：符合该 ACE 的数据帧的行为获得允许。

拒绝：丢弃符合该 ACE 的数据帧。

速率限制：指定速率限制的基础单元数。可选范围为 1～15。“禁用”表示禁止操作速率限制。

端口复制：符合 ACE 的数据帧将被复制到指定的端口号。可选范围等同于交换机的端口范围。“禁用”表示禁用端口复制操作。

日志：指定 ACE 的日志操作。取值为：

启用: 对应的 ACE 帧将存储至系统日志中。

禁用：对应的 ACE 帧将不列入日志中。

请注意：系统日志内存的大小和日志比率有限。

关闭：指定 ACE 的端口关闭操作。取值为：

启用：如果有数据帧对应 ACE，入站端口将关闭。

禁用：禁用 ACE 的端口关闭。

计数器：计数器表示数据帧符合 ACE 的次数。

MAC 参数：

源 MAC 过滤（仅帧类型为以太网类型或 ARP 时，本参数才会显现。）指定用于该 ACE 的源 MAC 过滤。

任何：未指定源 MAC 过滤。（源 MAC 的过滤状态为“不用管”。）

指定：如果您需要对该 ACE 过滤某源 MAC 地址，请选择本参数，在其后的空间内可输入源 MAC 值。

源 MAC 值：在源 MAC 过滤中选择了“指定”后，您需要输入一个源 MAC 地址。正确的格式为：xx-xx-xx-xx-xx-xx. 符合该 ACE 的数据帧将对应这个源 MAC 值。

目的 MAC 过滤：为该 ACE 指定目的 MAC 地址过滤。

任何：未指定目的 MAC 过滤。（目的 MAC 的过滤状态为“不用管”。）

多播：帧必须为多播帧。

广播：帧必须为广播帧。

未知单播：帧必须为单播帧。

指定：如果您需要对该 ACE 过滤某目的 MAC 地址，请选择本参数，在其后的空间内可输入目的 MAC 值。

目的 MAC 值：在目的 MAC 过滤中选择了“指定”后，您需要输入一个目的 MAC 地址。正确的格式为：xx-xx-xx-xx-xx-xx. 符合该 ACE 的数据帧将对应这个目的 MAC 值。

VLAN 参数：

VLAN ID 过滤：为该 ACE 指定 VLAN ID 过滤。

任何：未指定 VLAN ID 过滤。（VLAN ID 的过滤状态为“不用管”。）

指定：如果您需要对该 ACE 过滤某 VLAN ID，请选择本参数，在其后的栏内输入 VLAN ID 值。

VLAN ID：在 VLAN ID 过滤中选择了“指定”后，您需要输入一个 VLAN ID 号。可选范围为 1～4094。符合该 ACE 的数据帧将对应这个 VLAN ID 号。

Tag 优先级：为该 ACE 指定标记优先级。符合该 ACE 的数据帧将对应本标记优先级。可选范围为 0～7。取值“任何”表示没有指定标记优先级 （标记优先级为“不用管”。）

ARP 参数：当选择帧类型为 ARP 时，即可对 ARP 参数进行设置。

ARP/RARP：为该 ACE 指定可用的 ARP/RARP OP 标记。

任何：未指定 ARP/RARP OP 标记。（OP 为“不用管”。）

ARP：帧必须设置 ARP/RARP OP 到 ARP 中。

RARP：帧必须设置 ARP/RARP OP 到 RARP 中。

其它：帧中含有未知 ARP/RARP OP 标记。

请求/响应：为该 ACE 指定可用的 ARP/RARP OP 标记。

任何：未指定 ARP/RARP OP 标记。（OP 为“不用管”。）

请求：数据帧必须有设置的 ARP 请求或 RARP 请求的 OP 标记。

响应：数据帧必须有 ARP 回复或 RARP 回复的 OP 标记。

发送方 IP 过滤：为该 ACE 指定发送方 IP 过滤。

任何：未指定发送方 IP 过滤。（发送方 IP 过滤为“不用管”。）

主机：设置主机为发送方 IP 过滤。请在源 IP 地址栏中指定发送方的 IP 地址。

网段：设置网络为发送方 IP 过滤。请在相应的栏目中指定发送方的 IP 地址和发送方的 IP 掩码。

发送方 IP 地址：在发送方 IP 过滤中选择了“**主机**”或“**网段**”后，您需要输入十进制式的发送方 IP 地址。

发送方掩码：在发送方 IP 过滤中选择了“**网段**”后，您需要输入十进制式的发送方 IP 掩码。

目的 IP 过滤：为选定的 ACE 指定目标 IP 过滤

任何：未指定目标 IP 过滤。（目标 IP 过滤为“不用管”。）

主机：设置主机为目标 IP 过滤。请在源 IP 地址栏中指定目标 IP 地址。

网段：设置网络为目标 IP 过滤。请在相应的栏目中指定目标 IP 地址和目标 IP 掩码。

目的 IP 地址：在目标 IP 过滤中选择了“主机”或“**网段**”后，您需要输入十进制式的目标 IP 地址。

发送方掩码：在目标 IP 过滤中选择了“**网段**”后，您需要输入十进制式的目标 IP 掩码。

ARP 源 MAC 匹配：根据发送方硬件地址栏（SHA）的设置，指定数据帧是否能执行符合操作。

0：ARP 数据帧中 SHA 不等同于源 MAC 地址。

1：ARP 数据帧中 SHA 等同于源 MAC 地址。

任何：可允许任何值。（“不用管”）。

RARP 目的 MAC 匹配：根据目标硬件地址栏（THA）的设置，指定数据帧是否能执行符合操作。

0：RARP 数据帧中 THA 不等同于源 MAC 地址。

1：RARP 数据帧中 THA 等同于源 MAC 地址。

任何：可允许任何值。（“不用管”）。

IP/Ethernet 长度：根据 ARP/RARP 硬件地址长度（HLN）和协议地址长度（PLN）的设置，指定数据帧是否能执行符合操作。

0：ARP/RARP 数据帧中，如果 HLN 为以太网（0x06），并且 PIN 为 IPv4 时， 不可匹配本条目。

1：ARP/RARP 数据帧中，如果 HLN 为以太网（0x06），并且 PIN 为 IPv4 时， 可匹配本条目。

任何：可允许任何值。（“不用管”）。

IP： 根据 ARP/RARP 硬件地址空间（HRD）设置，指定数据帧是否能执行符合操作。

0：ARP/RARP 数据帧中 HLD 等同于以太网中（1），则不可对应该条目。

1：ARP/RARP 数据帧中 HLD 等同于以太网中（1），则可对应该条目。

任何：可允许任何值。（“不用管”）。

以太网：根据 ARP/RARP 协议地址空间（PRO）设置，指定数据帧是否能执行符合操作。

0：ARP/RARP 数据帧中 PRO 等同于 IP（0x800），则不可对应该条目。

1: ARP/RARP 数据帧中 PRO 等同于 IP（0x800），则可对应该条目。

任何：可允许任何值。（“不用管”）

IP 参数：当选定帧类型为“IPv4”，可对 IP 参数进行设置。

IP 协议过滤：为该 ACE 指定 IP 协议过滤。

任何：未指定 IP 协议过滤（“不用管”）。

指定：如果您需要对该 ACE 过滤某 IP 协议，请选择本参数，在其后的栏内输入 IP 协议过滤。

ICMP：选择 ICMP 过滤 IPv4 ICMP 协议帧。其他栏用于定义 ICMP 参数。在其后的帮助文件中将对这些栏有进一步的解释。

UDP：选择 UDP 过滤 IPv4 UDP 协议帧。其他栏用于定义 UDP 参数。在其后的帮助文件中将对这些栏有进一步的解释。

TCP: 选择 TCP 过滤 IPv4 TCP 协议帧。其他栏用于定义 TCP 参数。在其后的帮助文件中将对这些栏有进一步的解释。

IP 协议值：当在 IP 协议值中选择了“指定”时，您需要输入一个数值。该数值的范围为 0～255。符合该 ACE 的数据帧将匹配该 IP 协议值。

IP TTL：为该 ACE 设置生存时间。

0：IPv4 数据帧中的生存时间大于 0 时，则不可以匹配该条目。

非 0：IPv4 数据帧中的生存时间大于 0 时，则可以匹配该条目。

任何：可允许任何值。（“不用管”）。

IP 碎片：为该 ACE 设置碎片偏移量，其中包含了在 IPv4 的数据帧中对多碎片（MF）比特和碎片偏移量（FRAG OFFSET）的设置。

否：IPv4 数据帧中，设置了 MF 比特或碎片偏移量大于 0，则不能对应该条目。

是：IPv4 数据帧中，设置了 MF 比特或碎片偏移量大于 0，则

可以对应该条目。

任何：可允许任何值。（“不用管”）。

IP 选项：为该 ACE 设置选项标记。

否：IPv4 数据帧中设置了选项标记，则不能对应该条目。

是：IPv4 数据帧中设置了选项标记，则可以对应该条目。

任何：可允许任何值。（“不用管”）。

源 IP 过滤：为该 ACE 设置源 IP 过滤。

任何: 未指定源 IP 过滤（源 IP 过滤为“不用管”）。

主机：对主机设置源 IP 过滤。在其后的源 IP 地址栏中，可指定源 IP 地址。

网段：对网络设置源 IP 过滤。在其后对应栏中，可指定源 IP 地址和源 IP 掩码。

源 IP 地址：在源 IP 过滤中选择了“主机”或“网段”后，您需要输入十进制式的源 IP 地址。

源 IP 掩码：在源 IP 过滤中选择了“网段”后，您需要输入十进制式的源 IP 掩码。

目的 IP 过滤：为该 ACE 设置目的 IP 过滤。

任何: 未指定目的 IP 过滤（目的 IP 过滤为“不用管”）。

主机：对主机设置目的 IP 过滤。在其后的目的 IP 地址栏中，可指定目的 IP 地址。

网段：对网络设置目的 IP 过滤。在其后对应栏中，可指定目的 IP 地址和目的 IP 掩码。

目的 IP 地址：在目的 IP 过滤中选择了“主机”或“网段”后，您需要输入十进制式的目的 IP 地址。

目的 IP 掩码：在目的 IP 过滤中选择了“网段”后，您需要输入十进制式的目的 IP 掩码。

ICMP 参数：

ICMP 类型过滤

任何：不设置 ICMP 过滤（ICMP 过滤状态为“不用管”）。

指定：如果需要为该 ACE 设置 ICMP 过滤，您可在其后栏内输入 ICMP 值。

ICMP 类型值：在 ICMP 过滤中选择“指定”，您需要输入一个 ICMP 值。取值范围为 0～255。符合该 ACE 的数据帧将对应该 ICMP 值。

ICMP 过滤：对该 ACE 设置 ICMP 代码过滤。

任何：不设置 ICMP 代码过滤（ICMP 代码过滤状态为“不用管”）。

指定：如果需要为该 ACE 设置 ICMP 代码过滤，您可在其后栏内输入 ICMP 代码值。

ICMP 码值：在 ICMP 代码过滤中选择“指定”，您需要输入一个 ICMP 代码值。取值范围为 0～255。 符合该 ACE 的数据帧将对应该 ICMP 代码值。

TCP/UDP 参数

源端口过滤：对该 ACE 设置 TCP/UDP 源过滤。

任何：不设置 TCP/UDP 源过滤（TCP/UDP 源过滤状态为“不用管”）。

指定：如果需要为该 ACE 设置 TCP/UDP 源过滤，请在其后栏内输入 TCP/UDP 源值。

范围：如果需要为该 ACE 设置 TCP/UDP 源范围过滤，请在其后栏内输入 TCP/UDP 源范围值。

源端口号：在 TCP/UDP 源过滤中选择“指定”，您需要输入一个 TCP/UDP 源值。取值范围为 0～65535。 符合该 ACE 的数据帧将对应该 TCP/UDP 源值。

源端口范围：在 TCP/UDP 源过滤中选择“范围”，您需要输入一个 TCP/UDP 源范围值。取值范围为 0～65535。 符合该 ACE 的数据帧将对应该 TCP/UDP 源范围值。

目的端口过滤：对该 ACE 设置 TCP/UDP 目的过滤。

任何：不设置 TCP/UDP 源过滤（TCP/UDP 源过滤状态为“不用管”）。

指定：如果需要为该 ACE 设置 TCP/UDP 源过滤，请在其后栏内输入 TCP/UDP 源值。

范围：如果需要为该 ACE 设置 TCP/UDP 源范围过滤，请在其后栏内输入 TCP/UDP 源范围值。

目的端口号：在 TCP/UDP 目的过滤中选择“指定”，您需要输入一个 TCP/UDP 目的值。取值范围为 0～65535。 符合该 ACE 的数据帧将对应该 TCP/UDP 目的值。

目的端口范围：在 TCP/UDP 目的过滤中选择“范围”，您需要输入一个 TCP/UDP 目的范围值。取值范围为 0～65535。 符合该 ACE 的数据帧将对应该 TCP/UDP 目的范围值。

TCP FIN：对该 ACE 设置“不再接受来自发送方的数据”（FIN）值。

0：对于已设置 FIN 值的 TCP 数据帧，不能对应该条目。

1：对于已设置 FIN 值的 TCP 数据帧，能对应该条目。

任何：任何：可允许任何值。（“不用管”）。

TCP SYN：对该 ACE 设置“同步序列号”（FIN）值。

0：对于已设置 SYN 值的 TCP 数据帧，不能对应该条目。

1：对于已设置 SYN 值的 TCP 数据帧，能对应该条目。

任何：任何：可允许任何值。（“不用管”）。

TCP PSH：对该 ACE 设置“Push 功能”（PSH）值。

0：对于已设置 PSH 值的 TCP 数据帧，不能对应该条目。

1：对于已设置 PSH 值的 TCP 数据帧，能对应该条目。

任何：任何：可允许任何值。（“不用管”）。

TCP ACK：对该 ACE 设置 ACK (Acknowledgment field significant) 值。

0：对于已设置 ACK 值的 TCP 数据帧，不能对应该条目。

1：对于已设置 ACK 值的 TCP 数据帧，能对应该条目。

任何：任何：可允许任何值。（“不用管”）。

TCP URG：对该 ACE 设置 URG (Urgent Pointer field significant)值。

0：对于已设置 URG 值的 TCP 数据帧，不能对应该条目。

1：对于已设置 URG 值的 TCP 数据帧，能对应该条目。

任何：可允许任何值。（“不用管”）。

以太网类型参数：选择帧类型为以太网类型，可对以太网类型参数进行设置。

以太网帧过滤：对该 ACE 设置以太网类型过滤。

任何：不设置以太网类型过滤（以太网类型过滤状态为“不用管”）。

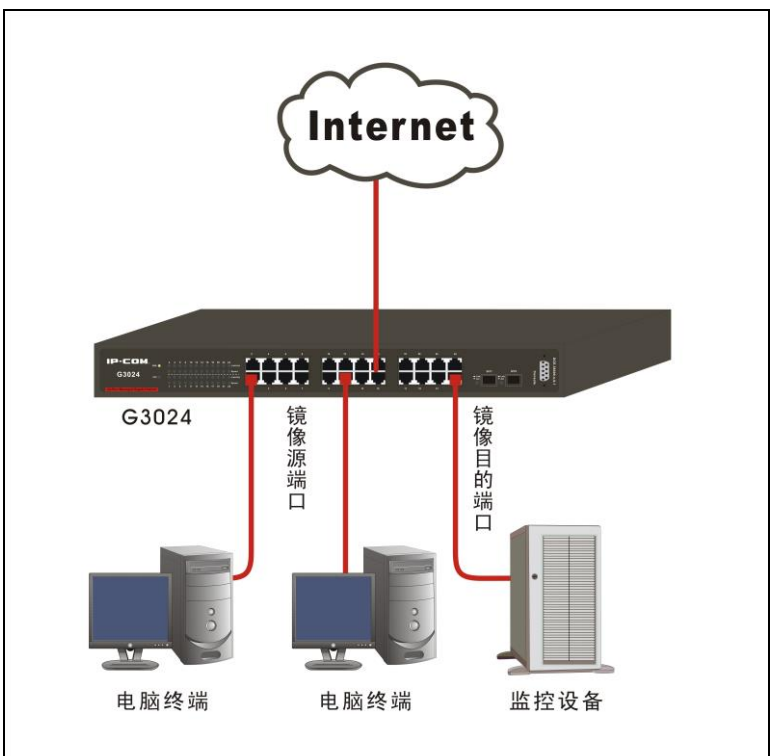
指定：如果需要为该 ACE 设置以太网类型过滤，请在其后栏内输入以太网类型值。

以太网类型值：在以太网类型过滤中选择“指定”，您需要输入一个以太网类型值。取值范围为 0x600～0xFFFF。 符合该 ACE 的数据帧将对应该以太网类型值。

4.12 端口镜像

4.12.1 镜像概述

镜像是将指定端口的报文复制到镜像端口，镜像端口会接入数据检测设备，用户利用数据检测设备分析镜像端口接收到的报文，进行网络监控和故障排除。镜像的示意图如下：



4.12.2 镜像配置界面

请点击导航栏的“G3024→功能设置→端口镜像”，即可进入镜像配置界面，如下图：

本页面用于设置端口镜像。为解决网络问题，将流量复制或镜像到一个镜像端口。 然后将该端口连接到数据帧分析仪以分析数据帧的流量。

复制到镜像端口的流量选择如下：

在某端口接收的所有数据帧（也被称为入站或源镜像）。

在某端口发送的所有数据帧（也被称为出站或目的镜像）。

镜像端口：来自启用了源或目的镜像端口的数据帧将镜像到该端口。

“禁用”表示禁用端口镜像。

被镜像端口设置：下列表格用于启用 Rx 和 Tx。

端口：逻辑端口设置。

模式：选择镜像模式。

仅 Rx：仅端口接收的数据帧将镜像到镜像端口。

仅 Tx：仅端口发送的数据帧将镜像到镜像端口。

禁用：接收和发送的数据帧都不做镜像处理。

启用：接收和发送的数据帧都将镜像到镜像端口。

说明：

如果用低速率端口来监控高速率端口时，就会产生数据包的丢失。即：如果流量为100Mbps端口被10Mbps端口监控，就会造成数据包丢失的问题。

4.13 简单网络管理协议

4.13.1 简单网络管理协议概述

SNMP（Simple Network Management Protocol）是专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机等）的一种标准协议，它是一种应用层协议。 SNMP 可以让网络管理员能够轻松的管理网络，发现并及时解决网络问题以及规划网络增长的未来不可缺少的协议。

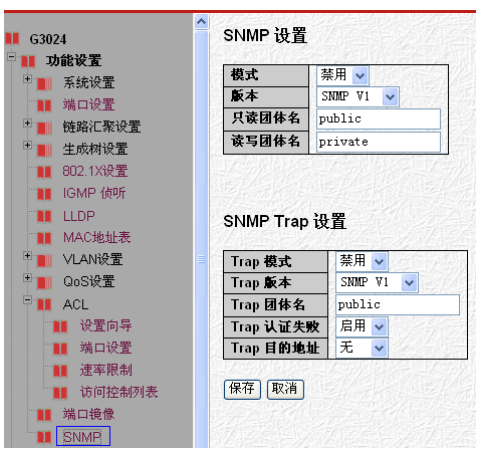
SNMP 最重要的思想就是要尽可能简单明了，以便及时有效的解决问题。SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP 可实现统计、配置和测试等功能。当网络出故障时，可实现各种差错检测和恢复功能。SNMP 启用的网络管理站可读取和修改路由器，交换机以及其他网络设备的设置。虽然 SNMP

是在 TCP/IP 基础上的网络管理协议，但也可扩展到其他类型的网络设备上。

支持 SNMP 的管理设备包括在本地设备运行的软件（代理软件）。SNMP 代理维持的一组定义的变量可用于管理设备。这些对象定义了管理信息库（MIB），在 MIB 库里提供了由 SNMP 代理控制的标准信息展示。SNMP 定义了 MIB 规格的格式和用于访问网络信息的协议。

4.13.2 简单网络管理协议配置界面

本交换机支持 SNMP V1 和 SNMP V2c 两种版本，请点击导航栏的“G3024→功能设置→SNMP”，即可进入简单网络管理协议配置界面，如下图：



本页面用于设置 SNMP。分为 SNMP 设置和 SNMP Trap 设置两部分。

1. SNMP 设置：

模式：表示 SNMP 模式操作。可能的模式有：

启用：启用 SNMP 模式操作。

禁用：禁用 SNMP 模式操作。

版本：表示 SNMP 支持的版本。可能的取值有：

SNMP V1：设置 SNMP 支持的版本为 1。

SNMP V2c: 设置 SNMP 支持的版本为 2c.

只读团体名：表示允许访问 SNMP 代理的团体读取访问字符串。可允许的字符串长为：0 ~ 255。可允许的字符串内容为 NVT ASCII 字符（32-126），但空格除外。

读写团体名：表示允许访问 SNMP 代理的团体写入访问字符串。可允许的字符串长为：0 ~ 255。可允许的字符串内容为 NVT ASCII 字符（32-126），但空格除外。

2. SNMP Trap 设置

Trap 模式：表示 SNMP Trap 模式操作。可能的模式有：

启用：启用 SNMP Trap 模式操作。

禁用：禁用 SNMP Trap 模式操作。

Trap 版本：表示 SNMP Trap 支持的版本。可能的取值有：

SNMP V1：设置 SNMP Trap 支持的版本为 1。

SNMP V2c: 设置 SNMP Trap 支持的版本为 2c。

Trap 团体名：当发送 SNMP trap 数据包时，用于表示团体访问字符串。可允许的字符串长为：0 ~ 255。可允许的字符串内容为 NVT ASCII 字符（32-126），但空格除外。

Trap 认证失败：表示 SNMP 实体允许生成认证失败 trap 信息。可能的模式有：

启用 d：启用 SNMP Trap 认证失败。

禁用：禁用 SNMP Trap 认证失败。

Trap 目的地址：表示 SNMP 的 trap 目的状态。可能的模式有：

无：表示没有 trap 目的地址。

指定：表示设置指定的 trap 目的地址。

Trap 目的地址：表示 SNMP Trap 目的地址。

第五章 交换机的监控

5.1 系统监控

5.1.1 系统信息

请点击导航栏的“G3024→监控设置→系统监控→系统信息”，即可进入系统信息监控界面，如下图：

本页面提供了交换机的系统信息。各个参数的信息如下：

联系方式:显示在设置→系统→信息→系统联系方式中设置系统的联系方式。

产品描述:显示在设置→系统→信息→系统名中设置系统名。

所在位置:显示在设置→系统→信息→系统位置中设置系统的位置。

MAC 地址:显示本交换机的 MAC 地址。

系统日期：当前系统的时区、系统时间和日期。如果可以，系统时间可从设置的 SNTP 服务器中获取。

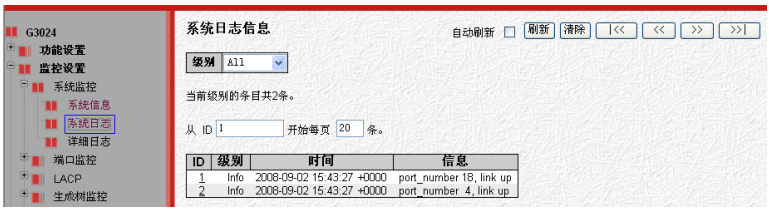
运行时间：设备处于运行状态的时间长度。

软件版本：交换机的软件版本号。

软件日期：交换机软件的生成日期。

5.1.2 系统日志信息

请点击导航栏的“G3024→监控设置→系统监控→系统日志”，即可进入系统日志监控界面，如下图：



本页面提供了交换机的系统日志信息。各参数信息描述如下：

ID：系统日志条目的 ID（大于等于 1）。

级别：系统日志条目的级别。支持的级别类型有：

Info：资讯级别

Warning：警告级别

Error：错误级别

All：所有级别

时间：系统日志条目的时间。

信息：系统日志条目的信息描述。

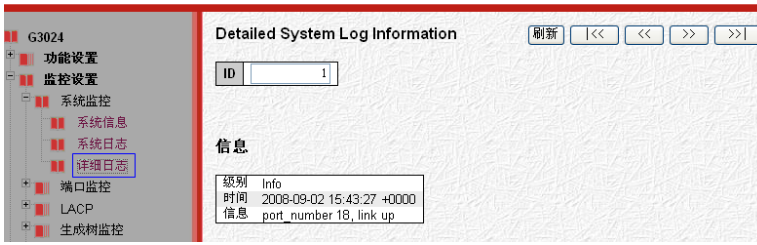
按钮：

自动刷新：勾选该方框可使页面在一定的间隔时间内自动更新。

刷新：更新系统日志，从当前条目 ID 开始。

5.1.3 具体的系统日志信息

请点击导航栏的“G3024→监控设置→系统监控→详细日志”，即可进入具体的系统信息监控界面，如下图：



本页面提供了交换机系统具体的日志信息。各参数信息描述如下：

ID：系统日志条目的 ID（大于等于 1）。

信息：系统日志条目的具体信息描述。

按钮：

刷新：更新系统日志条目到当前条目 ID。

|<<：更新系统日志条目到第一个可用的条目 ID。

<<：更新系统日志条目到前一个可用的条目 ID。

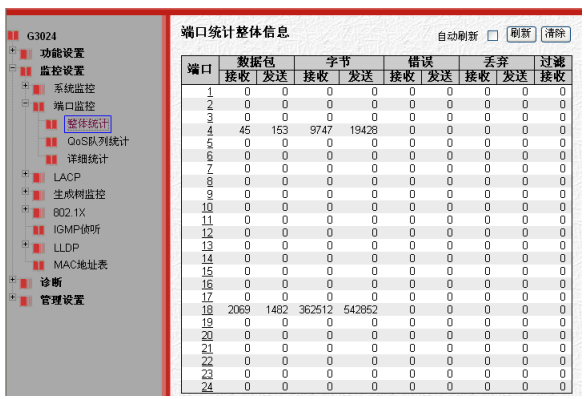
>>：更新系统日志条目到下一个可用的条目 ID。

>>|：更新系统日志条目到最后一个可用的条目 ID。

5.2 端口监控

5.2.1 端口整体统计信息

请点击导航栏的“G3024→监控设置→端口监控→整体统计”，即可进入端口整体统计信息监控界面，如下图：



端口	数据包		字节		错误		丢弃		过滤
	接收	发送	接收	发送	接收	发送	接收	发送	接收
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	45	153	9747	19428	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	2069	1482	362512	542852	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0

本页面提供了对所有交换端口的流量的整体情况。各参数信息描述如下：

端口：对逻辑端口的设置。

数据包：每个端口接收和发送的数据包。

字节：每个端口接收和发送的字节数。

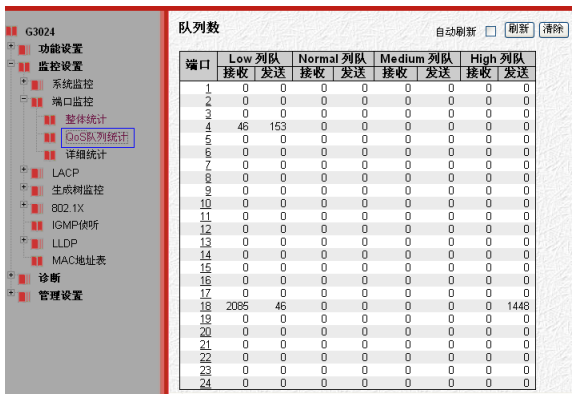
错误：接收的错误帧数和每个未完成传输的帧数。

丢弃：由于进站和出站的拥塞而丢弃的帧数。

过滤：在转发过程中过滤了接收到的帧数

5.2.2 QoS 的队列统计信息

请点击导航栏的“G3024→监控设置→端口监控→QoS 队列监控” ,即可进入 QoS 队列监控界面，如下图：



端口	Low 列队		Normal 列队		Medium 列队		High 列队	
	接收	发送	接收	发送	接收	发送	接收	发送
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	46	153	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	2085	46	0	0	0	0	0	1448
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

本页面对所有的交换端口提供了不同列队的统计。各参数信息描述如下：

端口：设置的逻辑端口。

Low 队列：每个端口有 4 个 QoS 列队和 strict 或 weighted 列队调度。这是最低优先级列队。

Normal 队列：4 个 QoS 列队中的 Normal 优先级列队，优先级比 Low 列队高。

Medium 队列：4 个 QoS 列队中的 Medium 优先级列队，优先级比 Normal 列队高。

High 队列：4 个 QoS 列队中优先级最高的列队。

接收/发送：每个端口接收和传送的数据包。

5.2.3 端口统计信息

请点击导航栏的“G3024→监控设置→端口监控→详细统计”，即可进入端口统计信息监控界面，如下图：

本页面对指定的交换端口提供了具体的流量统计信息。使用端口的选择方框可选择显示哪些交换端口的详细信息。本页面显示了接收和发送的总帧数，大小数和错误数。

接收和发送的总数量

RX and Tx Packets：接收和发送的数据包数。

Rx and Tx Octets：接收和发送的字节数。包括了 FCS，但不包括帧字节。

Rx and Tx Unicast：接收和发送的单播数。

Rx and Tx Multicast:接收和发送的多播数。

Rx and Tx Broadcast:接收和发送的广播数。

Rx and Tx Pause:在端口的接收和发送中含有 PAUSE 操作的 MAC 控制数据帧数。

接收和发送的字节数统计:接收和发送的数据包基于各自帧的大小来划分类别。

接收和发送的列队统计：每个输入和输出的列队中接受和发送的数据包数。

接收错误计数器

Rx Drops:因接收的缓存不够或出站拥塞而丢失的数据帧。

Rx CRC/Alignment:接收的数据帧中有 CRC 或 Alignment 错误的数。

Rx Undersize:接收的数据帧中含有效 CRC 的短帧数。

Rx Oversize :接收的数据帧中含有效 CRC 的长帧数。

Rx Fragments:接收的数据帧中含无效 CRC 的短帧数。

Rx Jabber :接收的数据帧中含无效 CRC 的长帧数。

Rx Filtered:在转发过程中过滤了接收到的帧数。

短帧指小于 64 字节的数据帧。

长针指大于为该端口设置的最大数据帧长度。

发送错误计数器

Tx Drops :由于输出缓存拥塞而丢弃的数据帧。

Tx Late/Exc. Coll. :由于过分冲突或后期冲突而丢弃的数据帧数。

按钮

刷新：点击可立即刷新页面。

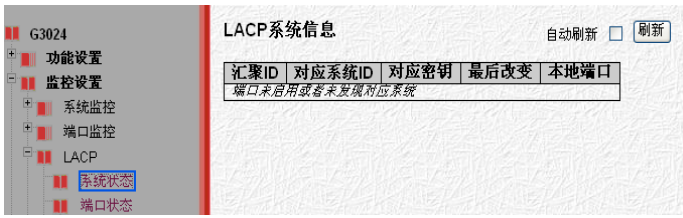
清除：清除计数器。

自动刷新：勾选该方框可使页面在一定的间隔时间内自动更新。

5.3 LACP 监控

5.3.1 LACP 系统信息

请点击导航栏的“G3024→监控设置→LACP→系统状态”，即可进入 LACP 系统信息监控界面，如下图：



本页面提供了所有 LACP 实例的整体信息。

汇聚 ID:与该汇聚实例相关的汇聚 ID。对于 LLAG，其 ID 显示为：isid:aggr-id；而对于 GLAG，其 ID 显示为: aggr-id。

对应系统 ID:汇聚对应系统 ID（MAC 地址）。

对应密钥:对应设备分配到该 ID 的密钥。

最后改变:汇聚改变的最后时间。

本地端口:显示本交换机中属于该汇聚的端口。

格式为：交换机 ID:端口号

5.3.2 LACP 端口状态信息

请点击导航栏的“G3024→监控设置→LACP→端口状态”，即可进入 LACP 端口状态信息监控界面，如下图：

端口	LACP	密钥	汇聚ID	对应系统ID	对应端口
1	否	-	-	-	-
2	否	-	-	-	-
3	否	-	-	-	-
4	否	-	-	-	-
5	否	-	-	-	-
6	否	-	-	-	-
7	否	-	-	-	-

本页面对所有端口提供了 LACP 状态的整体情况。

端口:交换机的端口号。

LACP: “是”表示启用了 LACP，端口处于已连接状态。

“否”表示 LACP 未启用或端口处于未连接状态。

密钥: 分配到端口的密钥。只有相同密钥值的端口才可以汇聚。

汇聚 ID:分配到汇聚组的汇聚 ID 号。ID1 和 ID2 属于 GLAG ,ID3 ~ ID14 属于 LLAG。

对应系统 ID:对应系统的 ID 号（MAC 地址）。

对应端口:连接本端口的对应端口号。

5.3.3 LACP 端口统计信息

请点击导航栏的“G3024→监控设置→LACP→端口统计”，即可进入 LACP 端口统计监控界面，如下图：

本页面对所有端口提供了 LACP 的统计信息。

端口：交换机的端口号。

发送 LACP：显示从每个端口发送出去的 LACP 数据帧量。

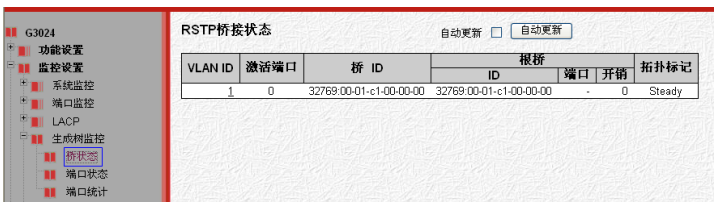
接收 LACP：显示每个端口接收的 LACP 数据帧量。

丢弃：显示每个端口已丢弃的未知和非法 LACP 数据帧数。

5.4 生成树监控

5.4.1 生成树桥状态信息

请点击导航栏的“G3024→监控设置→生成树监控→桥状态”，即可进入生成树桥状态监控界面，如下图：



本页面提供了所有 RSTP 桥接实例的整体信息。各个参数信息描述如下：

VLAN ID：与桥接实例相关的 VLAN ID。

激活端口：RSTP 桥接实例中交换机端口的激活数。

桥 ID：该桥接实例的桥 ID。

根桥：

ID：当前选择的根桥的桥 ID。

端口：当前分配到根端口的交换端口。

路径开销：根路径开销。在根桥上，根开销为零。对于其他的桥接，则是端口路径开销到根桥的总和。

拓扑标记：根桥路径的当前拓扑变换标记状态。

5.4.2 生成树端口状态

请点击导航栏的“G3024→监控设置→生成树监控→端口状态”，即可进入生成树端口状态监控界面，如下图：

端口	端口	状态	桥
1	Non-STP	Non-STP	-
2	Non-STP	Non-STP	-
3	Non-STP	Non-STP	-
4	Non-STP	Non-STP	-
5	Non-STP	Non-STP	-
6	Non-STP	Non-STP	-
7	Non-STP	Non-STP	-
8	Non-STP	Non-STP	-
9	Non-STP	Non-STP	-
10	Non-STP	Non-STP	-
11	Non-STP	Non-STP	-
12	Non-STP	Non-STP	-
13	Non-STP	Non-STP	-
14	Non-STP	Non-STP	-
15	Non-STP	Non-STP	-
16	Non-STP	Non-STP	-
17	Non-STP	Non-STP	-
18	Non-STP	Non-STP	-
19	Non-STP	Non-STP	-
20	Non-STP	Non-STP	-
21	Non-STP	Non-STP	-
22	Non-STP	Non-STP	-
23	Non-STP	Non-STP	-
24	Non-STP	Non-STP	-

在当前选择的交换机中，页面显示的是对物理端口的 RSTP 端口状态。各个参数描述如下：

端口：逻辑 RSTP 端口的交换机端口号。

角色：当前 RSTP 的端口角色。端口角色的取值有 :disabled Alternate Backup Root Designated Non-STP。

状态：当前 RSTP 的端口状态。端口状态的取值有：禁用、Blocking、Learning、listening、Forwarding 和 Non-STP。

5.4.3 生成树端口统计状态

请点击导航栏的“G3024→监控设置→生成树监控→端口统计”，即可进入生成树端口统计状态监控界面，如下图：

本页面显示的是在当前选择的交换机中物理端口的 RSTP 端口统计。各个参数描述如下：

端口：逻辑 RSTP 端口的交换机端口号。

RSTP：BPDU 在端口接收/传输的 RSTP 设置数。

STP：BPDU 在端口接收/传输的原始 RSTP 设置数。

TCN：BPDU 在端口接收/传输的（原始）拓扑改变通告数。

丢弃：

未知：在端口接收（和抛弃的）未知生成树 BPDU 数。

非法：在端口接收（和抛弃的）非法的生成树 BPDU 数。

5.5 802.1x 监控

5.5.1 端口状态

请点击导航栏的“G3024→监控设置→802.1x→端口状态”，即可进入 802.1x 端口状态监控界面，如下图：

本页面提供了交换机当前 IEEE802.1x 端口状态的整体情况。各参数信息描述如下：

端口：交换机的端口号。点击可导出该端口详细的 802.1x 统计信息。

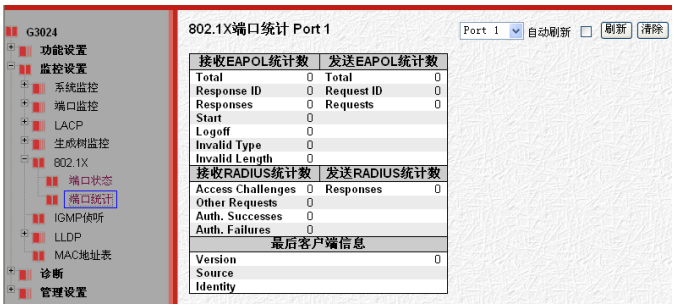
状态：端口的当前状态。不同状态的描述请参考 IEEE802.1x 端口状态部分。

最后源 MAC 地址：最后接收的 EAPOL 数据帧的源 MAC 地址。

最后 ID：最后接收的 Resp/ID EAPOL 数据帧的用户名(客户端身份)。

5.5.2 802.1x 端口统计

请点击导航栏的“G3024→监控设置→802.1x→端口统计”，即可进入 802.1x 端口统计监控界面，如下图：



本页面提供了交换机端口详细的 IEEE802.1x 统计信息。通过端口选择方框可选择端口的显示信息。本表格有三部分组成：

EAPOL 计数器

客户端数据帧计数器统计。包含了 7 个接收帧计数器和 3 个发送帧计数器。

方向	名字	IEEE 名	描述
Rx	Total	dot1xAuth EapolFramesRx	交换机接收的所有类型的有效 EAPOL 数据帧数。
Rx	Response ID	dot1xAuth EapolRespId FramesRx	交换机接收的有效 EAP Resp/ID 数据帧数。
Rx	Responses	dot1xAuth EapolResp FramesRx	交换机接收的有效 EAPOL 回复数据帧（不是 EAP Resp/ ID）数。
Rx	Start	dot1xAuth EapolStart FramesRx	交换机接收的有效 EAPOL 开始数据帧数。
Rx	Logoff	dot1xAuth EapolLogoff	交换机接收的有效 EAPOL logoff 数据帧数。

		FramesRx	
Rx	Invalid Type	dot1xAuth InvalidEapol FramesRx	未识别帧类型的交换机接收的 EAPOL 数据帧数。
Rx	Invalid Length	dot1xAuth EapLength ErrorFrames Rx	数据包主体长度无效的交换机中，接受的 EAPOL 数据帧数。
Tx	Total	dot1xAuth EapolFrame Tx	交换机发送的所有类型的有效 EAPOL 数据帧数。
Tx	请求 ID	dot1xAuth EapolReqId FramesTx	交换机发送的 EAP 初始请求数据帧数。
Tx	请求	dot1xAuth EapolReq FramesTx	交换机发送的有效 EAP 请求数据帧（不是初始请求数据帧）数。

RADIUS 计数器

RADIUS 服务器数据帧计数器统计。包含了 4 个接收帧计数器和 1 个发送帧计数器。

方向	名字	IEEE 名	描述
Rx	Access Challenges	dot1xAuthBackendAccess Challenges	客户端首次回复后，交换机从 RADIUS 服务器接收的首个请求次数。表示 RADIUS 服务器与交换机可以进行通讯。
Rx	Other 请求	dot1xAuthBackend Other Requests To	交换机发送 EAP 请求数据包至客户端的次数。表示 RADIUS 服务器选择了 EAP

		Supplicant	的方式。
Rx	Auth. Successes	dot1xAuthBackend Auth Successes	交换机接收到认证成功信息的次数。表示客户端已经成功的经过 RADIUS 服务器的认证。
Rx	Auth. Failures	dot1xAuthBackend AuthFails	交换机接收到认证失败信息的次数。表示客户端没有经过 RADIUS 服务器的认证。
Tx	Responses	dot1xAuthBackend Responses	交换机试图尝试首个客户端的回复数据包至 RADIUS 服务器的次数。表示交换机尝试与 RADIUS 服务器建立通讯。

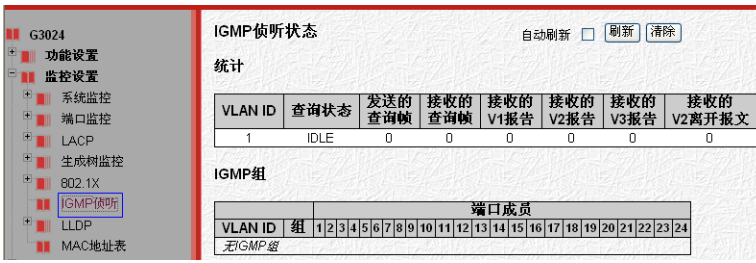
最后客户端信息

客户端最后一次尝试认证的信息。

名称	IEEE 名	描述
Version	dot1xAuthLastEapolFrameVersion	在当前接收的 EAPOL 数据帧中的协议版本号。
Source	dot1xAuthLastEapolFrameSource	在当前接收的 EAPOL 数据帧中的源 MAC 地址。
Identity	__	在当前接收的 Resp/ID EAPOL 数据帧中的用户名（客户端身份）。

5.6 IGMP Snooping 监控

请点击导航栏的“G3024→监控设置→IGMP 侦听”，即可进入 IGMP 监控界面，如下图：



本页面提供了 IGMP 侦听状态的相关信息。各参数信息描述如下：

VLAN ID：条目的 VLAN ID。

端口成员：条目成员的端口。

查询状态：显示查询状态是“激活”还是“空闲”。

发送的查询帧：已传输查询的数量。

接收的查询帧：已接收查询的数量。

接收的 V1 报告：已接收的 V1 报告数量。

接收的 V2 报告：已接收的 V2 报告数量。

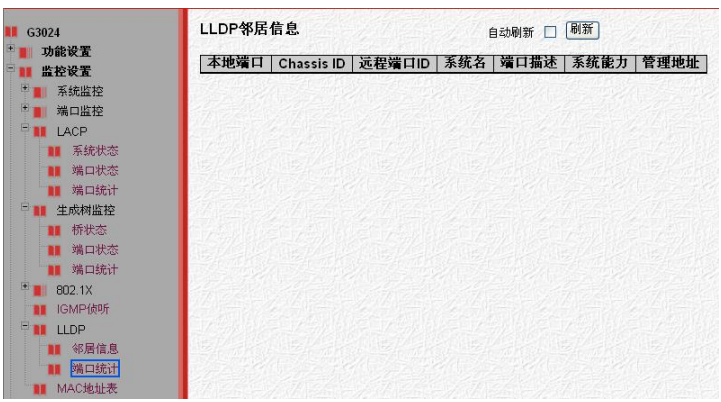
接收的 V3 报告：已接收的 V3 报告数量。

接收的 V2 离开报文：已接收的 V2 离开的报告数量。

5.7 LLDP 监控

5.7.1 LLDP 邻居信息

请点击导航栏的“G3024→监控设置→LLDP→邻居信息”，即可进入 LLDP 邻居信息监控界面，如下图：



本页面提供了 LLDP 邻居状态的整体信息。显示的列表中包含了 LLDP 邻居检测到的每个端口和下列参数：

本地端口：LLDP 数据帧接收的端口号。

Chassis ID：用于识别邻居的 LLDP 数据帧。

远程端口 ID：用于识别邻居端口。

系统名：由邻居单元广播的系统名。

端口描述：由邻居单元广播的端口描述。

系统能力：系统能力指邻居单元的能力。其能力有：

1. 其他
2. 中继

3. 桥接
4. 无线局域网接入点
5. 路由器
6. 电话
7. DOCSIS 有线设备
8. 仅站点模式
9. Reserved

当启用了某个能力时，在能力的后面有个（+）的标识。如果禁用了该能力，则在能力的后面有个（-）的标识。

管理地址：管理地址就是邻单元的地址，用于高层实体协助网络管理的发现。一般情况下，管理地址在这里显示的是邻单元的 IP 地址。

5.7.2 LLDP 端口统计

请点击导航栏的“G3024→监控设置→LLDP→端口统计”，即可进入 LLDP 邻居信息监控界面，如下图：

本地端口	Tx数据帧	Rx数据帧	Rx错误帧	丢弃帧	TLVs 丢弃	TLVs不可认	Org. 丢弃	老化
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0

本页面提供了 LLDP 流量的整体信息。本表格由端口和下列参数组成：

本地端口：LLDP 数据帧接收或发送的端口。

Tx 数据帧：在端口发出的 LLDP 数据帧数。

Rx 数据帧：在端口接收的 LLDP 数据帧数。

Rx 错误帧：已接收的 LLDP 数据帧中有某种的错误的数量。

丢弃帧：如果某个端口接收了 LLDP 数据帧，并且交换机的内部列表已经用完，则计算 LLDP 数据帧并将其丢弃。这种情况在 LLDP 标准里称为“Too Many Neighbors”。当底盘 ID 或远程端口 ID 已经不在列表中时，LLDP 的数据帧在列表中需要一个新的条目。当下列的一种情况发生时，条目将从列表中移除：端口未连接；接收了 LLDP 关闭数据帧；或条目已老化。

TLVs 丢弃：每个 LLDP 的数据帧中包含了多个信息，被称为 TLV（类型长度值）。如果 TLV 变形，则计算 LLDP 数据帧并将其丢弃。

未知 TLVs：构成良好的 TLV 数，但是其类型值不可知。

Org.丢弃：组织地 TLV 接收数量。

老化：每个 LLDP 数据帧中包含了 LLDP 信息的有效时间（老化时间）。如果在老化时间内没有接收到新的 LLDP 数据帧，LLDP 信息将被移除，并增加老化计数器。

5.8 MAC 地址表监控

请点击导航栏的“G3024→监控设置→MAC 地址表”，即可进入 MAC 地址表监控界面，如下图：

本页面中显示了 MAC 地址表中的条目。该表可容纳 8192 个条目，

由 VLAN ID 和 MAC 地址来划分。各个参数信息描述如下：

MAC 地址表

MAC 地址表中的每页最多可显示 999 个条目。默认显示为 20 个。也可以从“每页条目”输入栏内选择自定义的显示条目数。首次访问 MAC 地址时，Web 界面将会显示 MAC 地址表的头 20 个条目。根据 VLAN ID 和 MAC 地址大小，按照从低到高的顺序显示。

“起始 MAC 地址”和“VLAN”输入栏可允许用户选择 MAC 地址表的起始点。点击刷新按钮，MAC 地址表将显示“起始 MAC 地址”中输入的 MAC 地址，或与之最近的下一 MAC 地址表匹配。此外，一旦点击刷新按钮，两个输入栏将提取第一个条目的值，允许以同一个起始 MAC 地址显示并保持不断的刷新。

>>表示可使用当前 VLAN/MAC 地址对的最后条目作为下次查询的基础。当最后条目显示时，列表将显示文本“条目显示完毕”。使用“<<”按钮，表示开始从头显示。

MAC 地址表栏

类型：表示显示的是静态还是动态条目。

MAC 地址：条目的 MAC 地址。

VLAN：条目的 VLAN ID 号。

端口成员：条目成员的端口。

第六章 交换机的诊断

6.1 ICMP Ping

请点击导航栏的“G3024→诊断→Ping”，即可进入 ICMP Ping 界面，如下图：

本界面用于发送 ICMP 数据包来解决 IP 连接问题。

点击“开始”后，发出 5 个 ICMP 数据包。从下面的回复接收中我们可以看到其序列号和往返时间。在所有的数据包回复之前或发生超时，本页面可自动更新。

Ping 10.10.132.20

64 bytes from 10.10.132.20: icmp_seq=0, time=0ms

64 bytes from 10.10.132.20: icmp_seq=1, time=0ms

64 bytes from 10.10.132.20: icmp_seq=2, time=0ms

64 bytes from 10.10.132.20: icmp_seq=3, time=0ms

64 bytes from 10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

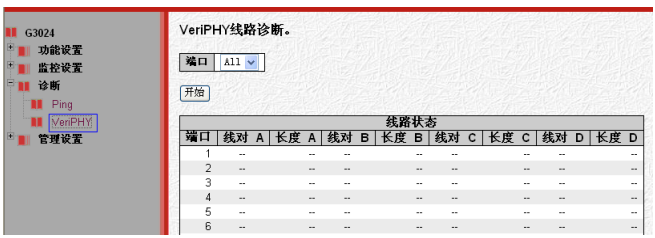
ICMP 数据包（已发出）属性设置：

IP 地址：目的 IP 地址。

Ping 包大小：ICMP 数据包有效载荷的大小。取值范围为：8~1400 位

6.2 VeriPHY

请点击导航栏的“G3024→诊断→VeriPHY” ,即可进入 VeriPHY 界面，如下图：



本页面用于运行 VeriPHY 线路诊断。

点击“开始”可运行诊断。大概要花费 5 秒钟。如果选择所有的端口，则需要大约 15 秒钟。完成后，页面会自动更新，在线路状态列表中可以看到线路诊断的结果。

⚠ ***注意：***

1. VeriPHY 精确度只限于 7 ~ 140 米的线路长度。在运行 VeriPHY 时，10/100Mbps 的端口将会处于断开连接状态。因此，在 10/100Mbps 管理端口上运行 VeriPHY 会造成交换机停止反映，直到 VeriPHY 运行完成。
2. 光纤端口不可检测

端口: 需要 VeriPHY 线路诊断的端口。

线路状态：

端口: 端口号。

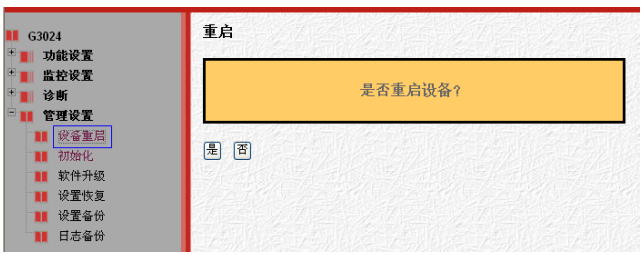
线对：线对的状态。

长度：线对的长度（米）。

第七章 交换机的维护

7.1 系统重启

请点击导航栏的“G3024→管理设置→设备重启”，即可进入交换机重启界面，如下图：



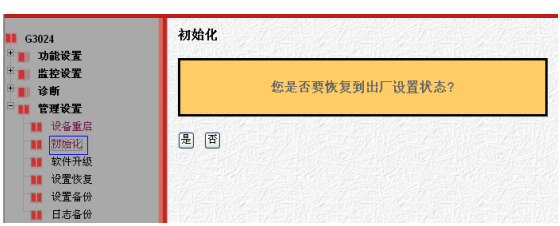
在本页您可以重启交换机。在重启后，系统将会正常的启动。

是：点击重启设备。

否：点击返回到系统信息界面而不会重启。

7.2 恢复出厂值

请点击导航栏的“G3024→管理设置→初始化”，即可进入恢复出厂值界面，如下图：



在本页面可复位交换机的设置，复位时只有 IP 设置保留，其它所有

的设置都恢复到出厂设置。因为新的设置可立即启用，因此没有必要重启。

是：点击可复位设置到出厂默认值。

否：点击可返回到系统信息页面，而不会复位系统设置。

7.3 软件升级

请点击导航栏的“G3024→管理设置→软件升级”，即可进入软件升级界面，如下图：

本页面用于软件的更新以控制交换机。点击“浏览”可定位软件映像的位置，然后点“上传”按钮即可。

在软件映像上传后，将跳出一页面告知软件更新正初始化。在数分钟后，软件更新完成，交换机将重启。

⚠ ***注意：***

在软件更新中，web 页面不能操作，“SYS”指示灯也以 10Hz 的频率闪烁。此时，请不要复位或切断电源，否则会使交换机造成损坏。

7.4 配置文件的上传

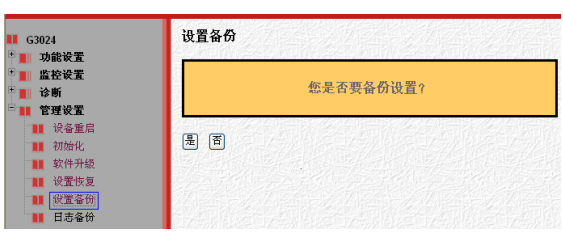
请点击导航栏的“G3024→管理设置→设置恢复”，即可进入配置文件的上传界面，如下图：

本页面用于将配置文件上传到交换机。点击“浏览”可定位软件映像的位置，然后点“上传”按钮即可。

在软件映像上传后，将跳出一页面告知配置更新正初始化。在数分钟后，配置更新完成。完成后需手动重启交换机，否则新上传的配置将不会生效。

7.5 配置文件的下载

请点击导航栏的“G3024→管理设置→设置备份”，即可进入配置文件的下载界面，如下图：



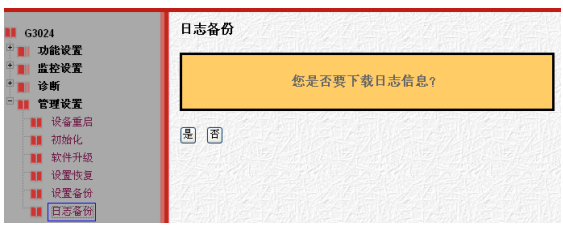
本页面用于将交换机的配置文件下载到电脑终端。

是：点击可将交换机的配置文件下载到电脑终端。

否：点击可返回到系统信息页面，而不会下载配置文件。

7.6 系统日志文件的下载

请点击导航栏的“G3024→管理设置→日志备份”，即可进入系统日志下载界面，如下图：



本页面用于将交换机的系统日志下载到电脑终端。

是：点击可将交换机的系统日志下载到电脑终端。

否：点击可返回到系统信息页面，而不会下载系统日志。

第八章 附 录

8.1 技术参数

一 般 特 性			
标准	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.3z 1000BASE-LX Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1d Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1Q VLAN IEEE 802.1p QoS IEE 802.1X Port Access Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3ad Link Aggregation Port Mirror IGMP Snooping Jumbo Frame 超长帧 （≥9Kbytes）		
协议	CSMA/CD Ethernet		
数据传输率	以太网： 10Mbps（半双工） 20Mbps（全双工）	快速以太网 100Mbps（半双工） 200Mbps（全双工）	千兆以太网 2000Mbps （全双工）

拓扑结构	星型
端口数量	24 个 10/100/1000Mbps RJ-45 端口 2 个千兆 SFP（mini GBIC）接口 1 个 RS-232 控制口
支持的 SFP（mini GBIC）	支持标准的 SFP 光纤模块： IEEE 802.3z 1000 BASE-LX IIEEE 802.3z 1000BASE-LH IEEE 802.3z 1000BASE-ZX IEEE 802.3z WDM 1000BASE-LX IEEE 802.3z WDM 1000BASE-LHX
电缆长度	
网络电缆	10Base-T： 3 类或 3 类以上 UTP(100 米) 100Base-TX：5 类 UTP (100 米) 1000Base-T：5 类或超 5 类 UTP（100 米）
光纤	1000Base-LX：单模光纤（10km） 1000Base-SX：多模光纤（550m） 1000Base-LHX：单模光纤（50km） 1000Base-ZX：单模光纤（80km）
性 能	
转发机制	存储转发
MAC 地址表	8K
数据包过滤/转发率	14880pps（10Mbps 线速）
	148800pps（100Mbps 线速）
	1488095pps（1000Mbps 线速）
MAC 地址学习	自动学习/老化

背板带宽	48Gbps
转发表老化时间	10-1000000s（默认 300s）
物 理 及 环 境 特 性	
AC 输入范围	AC100~240V 1.2A（Max） 50~60Hz（内置通用开关电源）
功耗	最大 50W
运行温度	0°C～40°C
存储温度	-40°C～70°C
工作湿度	10%～95% RH 无凝结
存储湿度	5%～95% RH 无凝结
风扇	2 个散热风扇
规格	441.5mm*206.6mm*44.4mm（19 英寸机架）
重量	2.97kg
认证	CCC、CE 和 RoHS

8.2 专业术语概述

ACE

ACE（Access Control Entry，访问控制条目)，它描述了对 ACE ID 相关的访问权限。在本交换机中，提供 3 种 ACE 帧类型（Ethernet Type, ARP 和 IPv4）和 2 个操作（允许和拒绝）。除了这些，ACE 还包含了许多具体而又不同的参数选项，用于各种不同的应用。

ACL

ACL（Access Control List，访问控制列表)，其访问控制条目可用来对单个用户或群组，设置允许或拒绝特定的流量对象，如某个过程或项目。每个流量对象包含了 ACL 的标识符。这些权限决定了特定的流量对象是否有访问权限。ACL 的应用相对比较复杂，比如，对不同的情况，ACE 需要分清优先次序。在网络中，ACL 会参照主机或服务器上可用的服务端口和网络服务单，上面列举了主机和服务器可允许或拒绝使用的服务。通常，可设置 ACL 来控制网络内的流量，从这个角度来说，ACL 相当于防火墙。

汇聚

使用多个平行端口增加单端口局限的链路速度，和增加更高可用的冗余。同时也叫端口汇聚，或链路汇聚。

ARP

ARP（Address Resolution Protocol，地址解析协议)，该协议用于转换 IP 地址到物理地址，如以太网地址。只有知道邻居的因特网地址，ARP 才可允许主机与其他的主机通讯。在使用 IP 之前，主机会发送一个 ARP 请求广播数据包，其中包含了欲到达目的系统的因特网地址。

自适应

自适应是两个不同设备间建立操作模式和速度设置以供链路共享的过程。

DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议)，该协议用于分配动态 IP 地址到网络中的设备。网络中的电脑（客户端）使用 DHCP 来获取 IP 地址和其他参数，例如默认网关，子网掩码和 DNS 服务器的 IP 地址。DHCP 服务器确保所有的 IP 地址是唯一的，比如，当第一个客户分配到了有效的 IP 地址（租期未过期），则该 IP 地址将不会再分配到第二个客户端上。因此，IP 地址池是由 DHCP 服务器，而不是由网管来管理。

DNS

DNS（Domain Name System，域名系统)，它存储和关联与域名的多种信息类型。更重要的是，DNS 将域名和电脑主机名转换成 IP 地址。比如，域名 www.example.com 可能转换成 192.168.0.1。

DoS

DoS（Denial of Service，拒绝服务)，在拒绝服务攻击中， 攻击者试图阻止合法用户访问信息或服务。攻击者通常瞄准网络站点或网络连接，以阻止网络用户访问邮件，网络站点，在线账户（银行等）或其他依赖受感染计算机的服务。

Dotted Decimal Notation

Dotted Decimal Notation 指使用十进制小数和圆点来分割字节来表示 IP 地址的一种方式。IPv4 的点十进制地址采用的格式为 x.y.z.w, 其中 x, y, z 和 w 是间于 0～255 的十进制数。

DSCP

DSCP 是由 Differentiated Services Code Point 首写字母而组成。它是 IP 包头的一个字段，由以太网的网络标准定义。可用来表示，在以太网的数据帧中，表示正在传输的协议。

Ethernet Type

Ethernet Type 是以太网 MAC 地址头部的一个字段，由以太网网络标准定义。用于显示传输以太网数据帧中的协议类型。

FTP

FTP（File Transfer Protocol，文件传输协议)，它是一种传输协议，结合参数控制协议（TCP）并提供文件的读写。同时也提供了目录服务和安全特征。

HTTP

HTTP（Hypertext Transfer Protocol，超文本传输协议)，这种协议用于在万维网传输或传送信息。HTTP 定义了信息采用的格式和传输方式，以及 Web 服务器和浏览器对不同需求应采取的操作。比如，当您在浏览器中输入一个 URL，实际上是发送了一个 HTTP 命令到 Web 服务器，Web 服务器收到该命令后发送所需的 Web 页面。控制万维网是如何工作的另一个主要标准是 HTML，它包含了 Web 页面是如何形成和显示的。任何 Web 服务器，除了 Web 页面文件，还包含了一个 HTTP daemon 后台程序。这个后台程序的设计就是等待 HTTP 的请求，然后在到达之后处理它们。Web 浏览器是一个 HTTP 的客户端，用于发送请求到服务器。通过在远程主机（默认为 80 端口）建立传输控制协议（TCP）连接到特定端口，HTTP 客户端可创建一个请求。则 HTTP 服务器会听取那个端口，并等待客户端发送的请求信息。

HTTPS

HTTPS（ Hypertext Transfer Protocol over Secure Socket Layer，超文本传输协议安全套接字层)，用于表示 HTTP 的安全连接。HTTPS 提供了认证和加密通讯，并大范围的使用在万维网上，用于安全敏感较高的通讯，如支付业务和法人登录。HTTPS 实际上就是使用 Netscape 的安全套接字层（SSL）作为子层放在常规的 HTTP 应用层下。（在其与低层（TCP/IP）的通信中， HTTPS 使用的是 443 端口，而不是 HTTP 的 80 端口。）SSL 使用 40 位的密钥用于 RC4 流加密算法，对商业交易保障了充分的安全系数。

ICMP

ICMP(Internet Control Message Protocol ,因特网控制信息协议)，该协议可生成错误回复，诊断或路由目的。ICMP 信息通常包含如路由困难或简单交互（时间戳或回复处理）的信息。比如，PING 命令就是使用 ICMP 来诊断网络的连接。

IEEE 802.1X

IEEE 802.1X 是基于端口的网络访问控制 IEEE 标准。它提供了连接 LAN 口的设备的认证，建立了点到点的连接，并在认证失败时，能阻止该端口的访问。通过 802.1X，访问所有的交换端口可以集中由一台服务器来控制。也就是说，认证用户可以使用相同的证书来认证网络中任何节点。

IGMP

IGMP（Internet Group Management Protocol，网络群组管理协议），它是一种通信协议用于管理网络协议多播群组会员资格。IP 主机和相邻的多播路由器使用 IGMP 来建立多播群组会员资格。如同用于单播连接的 ICMP，IGMP 也仅是 IP 多播规范中的一部分。

IGMP 也可用于在线视频和游戏，以允许资源更高效的使用。

IGMP Querier

路由器在特定链路上发送的 IGMP 询问信息。该路由器就叫做 Querier。

IMAP

IMAP（Internet Message Access Protocol，网络信息访问协议），这种协议对邮件客户端可从邮件服务器上重现邮件信息。IMAP 是 IMAP 客户端使用与服务器通信的一种协议。而 SMTP 是用于传送邮件到 IMAP 服务器的一种协议。当前网络信息访问协议的版本是 IMAP4，类似于邮局协议版本 3，但是它提供了额外的和更复杂的特性。比如，IMAP4 协议可以让您的邮件保留在服务器上，而不能将邮件下载至电脑上。如果您希望从服务器上删除信息，您需要在邮件客户端上生成本地文件夹，将信息复制到您的本地硬盘中，然后可从服务器上删除该信息。

IP

IP（Internet Protocol，网际协议），该协议用于在因特网网络中的数据通信。IP 是一个"最大努力"系统，意思就是说，没有数据包在网络上发送时，能保证在相同条件下到达目的地。与局域网或广域网相连的每个设备都有分配了一个网际协议地址。该 IP 地址用于在扩展网络上相连的其他设备中能唯一的标识该 IP 地址。

当前使用的网际协议版本为 IPv4，这种 32 位的 IP 地址可以允许超过四百万个唯一的地址。由于 Web 站点管理员在区间大量的使用地址，其数量在急剧的减少，但是一些主干地址还仍未使用。所以逐渐推行新的网际协议版本 IPv6，它是 128 位的 IP 地址。但是，IPv4 依然是大多数网络选择的协议。

IPMC

IPMC 是 IP MultiCast (IP 多播) 首写字母而组成。

LACP

LACP 是 IEEE 802.3ad 的标准协议。链路汇聚控制协议可以捆绑多个物理端口而形成一个单独的逻辑端口。

LLDP

LLDP 是 IEEE 802.1ab 标准协议。链路层发现协议用于网络发现，并与网络中邻居设备使用 LLDP 数据帧交互信息。

MAC Table

数据帧的转换是基于数据帧中的 DMAC 地址。交换机内建了一张表格，将 MAC 地址和交换端口作了一一对应。这样数据帧就知道从哪个端口转发。这个列表中包含了静态和动态条目。如果管理员需要在 DMAC 地址和交换机端口作静态映射，静态条目则由网络管理员来设置。

数据帧中也包含了 MAC 地址（SMAC 地址），显示就是发送数据帧设备的 MAC 地址。交换机根据 SMAC 地址自动更新 MAC 地址表和动态 MAC 地址。如果在一段老化时间后没有看到相应 SMAC 地址的数据帧，则动态条目将从 MAC 地址表中移除。

镜像

为了调试网络中的问题和监控网络流量，可设置交换机系统监控来自多个端口的数据帧到镜像端口。（镜像数据帧在此等同于复制数据帧。）入站（源）数据帧和出站（目的）数据帧都可以被镜像到镜像端口。

NetBIOS

NetBIOS（Network Basic Input/Output System，网络基本输入/输出系统)，它是一个可以在单独计算机上允许应用程序在局域网内通信的程序。不支持在广域网上使用。网络中每台计算机上都有 NetBIOS 分配的一个 NetBIOS 名和一个对应不同主机名的 IP 地址。而且 NetBIOS 还提供了会话和 OSI 模型中的传输服务。

NFS

NFS（Network File System，网络文件系统)，它允许主机在远程系统上分区并像在本地文件系统中使用它们。NFS 允许系统管理员在网络的中心位置上存储资源，这样认证过的用户就可以持续访问它们。也就是说，NFS 支持文件，打印机和其他资源在网络上共享。

PING

Ping 就是指在网络或因特网上发送一系列的数据包到指定的计算机上，以便从该计算机上得到回复。计算机在收到 ping 发出的数据包后，会回复该计算机。使用 Ping 的目的就是核实是否网络上或因特网上的某计算机是否存在或连接上。Ping 使用的是网络控制信息协议（ICMP）的数据包。从源计算机上上发出 Ping 请求数据包；从目的回应 Ping 回复数据包。

Policer

Policer 用来限定接收数据帧的带宽，位于入站列队的前面。

POP3

POP3（Post Office Protocol version 3，邮局协议版本 3)，该协议可对邮件用户从邮件服务器找回邮件信息。只要用户下载了邮件，POP3 就可以把邮件从服务器上删除。但是，有些执行可允许用户

或管理员来设置邮件保存一段时间。因此，POP 可以认为是“存储和转发”的服务。另外一个协议是网络信息访问协议 IMAP。IMAP 为用户提供了将邮件保留在服务器上的更多容量，并将它们组织在一起，放到服务器的文件夹中。IMAP 可以认为是远程文件服务器。POP 和 IMAP 应对的是邮件的接收，而并不会与 SMTP 混为一谈。您可以通过 SMTP 发送邮件，然后邮件处理员以接收者的身份接受该邮件。使用 POP 或 IMAP 来读取该邮件。IMAP4 和 POP3 是邮件重现的两个常见的网络标准协议。事实上，现代的邮件客户端和服务器通常都支持这两种协议。

私有 VLAN

在私有 VLAN 中，不允许端口之间的通信。VLAN 可以设置为私有 VLAN。

QCE

QCE（QoS Control Entry ，QoS 控制条目)，它描述的是有关于特定 QCE ID 的 QoS 级别。本设备中具有六种 QCE 帧类型：Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, 和标记优先级。针对单一应用，数据帧可以通过如下四种 QoS 级别来分类: "Low", "Normal", "Medium", 和"High"。

QCL

QCL（QoS Control List，QoS 控制列表) ，即 QCE 的控制列表，包含了去 QoS 控制条目。QoS 控制条目在特定的流量对象中可划分到一个 QoS 级别。每个可访问的流量对象包含了其 QCL 的标识符。

QoS

QoS（Quality of Service ，QoS 服务质量），其保证了单个应用程序间或协议间的带宽关系。在通信网络上，传输着多个应用程序和数据，包含了高质量的视频和对延迟很敏感的数据，如实时语音。因此，网络必须要提供安全和有保障的服务。实现所需要的服务质量成为了端到端商务解决方案的成功的秘诀。所以，通过有技巧的设置 QoS，即可管理网络资源。

RARP

RARP(Reverse Address Resolution Protocol，逆地址解析协议)，该协议用于从硬件地址获取 IP 地址，如以太网地址。RARP 是 ARP 协议的补充。

路由端口

路由端口是以太网交换机上的一个端口，用于引导交换机面向 3 层多播设备。

RSTP

1998 年，IEEE 的 802.1w 文件引入了 STP 的升级版：快速生成树协议，在拓扑发生改变后，它提供了更快的生成树收敛时间。标准 IEEE 802.1D-2004 整合了 RSTP 和 STP，同时向后兼容 STP。

SAMBA

Samba 是运行在如 UNIX 操作系统下的一个程序，它提供了 UNIX 和 Windows 间的无缝整合。Samba 可以充当 Windows IBM OS/2, 和其他 SMB 客户设备的文件和打印服务器。Samba 使用了 SMB（Server Message Block，服务信息块）协议和 CIFS（Common

Internet Files System，通用网络文件协议），这种协议是 Microsoft 正在开发的一种新的文件和打印共享协议。Samba 可以在运行在多个操作系统平台上，包括 Linux，常用的 Unix 平台，Open VMS 和 IBM OS/2。Samba 也可以在网络上注册进主浏览器中，这样在 Windows 的"网络邻居"的主机列表中显示。

Sharper

Sharper 可以限定发送数据帧的带宽，位于入站列队之后。

SMTP

SMTP（Simple Mail Transfer Protocol ，简单邮件传输协议），它是一种基于文本的协议，使用了传输控制协议（TCP）并在 FTP 文件传输服务上提供了邮件服务。

SNMP

SNMP（Simple Network Management Protocol ，简单网络管理协议），它是用于管理的 TCP/IP 协议中的一部分。SNMP 允许逆向网络对象加入网络管理架构。它启用网络管理系统接收 trap 信息或通告来了解网络中的问题。

SNTP

SNTP（Simple Network Time Protocol，简单网络时间协议) ，这种网络协议可同步计算机系统的时钟。SNTP 使用的是传输层的 UDP datagrams 报文。

STP

生成树是 OSI 的二层协议，对所有桥接的局域网，可确保无环路的拓扑结构。随着 RSTP 的出现，原 STP 协议逐渐作废。

Tag Priority

标记优先级是 802.1Q 数据帧中的一个 3 位字段，当中存储的是优先级别。

TCP

TCP（Transmission Control Protocol，传输控制协议)，它是一种通信协议，结合网际协议(IP)在计算机间交互信息。

TELNET

TELNET（TELetype NETwork），它是一种终端仿真协议，使用的是 TCP 协议并提供了在 TELNET 服务器和 TELNET 客户端间的虚拟连接。

TFTP

TFTP（Trivial File Transfer Protocol，简单文件传输协议），大家可以从它的名称上看出，它适合传送“简单”的文件。与 FTP 不同的是，它使用的是 UDP 的 69 端口，因此它可以穿越许多防火墙。不过它也有缺点，比如传送不可靠、没有密码验证等。虽然如此，它还是非常适合传送小型文件的。

ToS

ToS（Type of Service ，服务类型），是 3 个 bit，范围 0-7，同样可当作优先级标记，另外 5 个实际指示 Delay，Throughput，Reliability 等特性的 bit 位一般没有使用；现在为了更好的控制数据流分类，使用 DSCP（Differential Services Code Point），扩展了 ToS 的后三个 bit，因此，范围从 0-63。在实施 QoS 策略时，Cos 与 ToS 或 DSCP 之间通常要做映射机制。

UDP

UDP（User Datagram Protocol ，用户数据报协议），它是一种通信协议，结合网际协议(IP)在计算机间交互信息。

User Priority

User Priority (用户优先级) 是 802.1Q 数据帧中的一个 3 位字段，当中存储的是优先级别。

VLAN

虚拟局域网是交换端口间限定通信的一种方式。

VLAN ID

VLAN ID 是一个 12 位的字段，用于描述数据帧属于哪个 VLAN。

8.3 技术支持

如果您在使用的过程中遇到问题，有以下两种方法可获得公司的技术支持：

1. 欢迎登录我们公司的网站 **http://www.ip-com.com.cn**。在“客户服务”有一些常见问题的解决方案。在“下载中心”有最新的软件升级包下载。
2. 如果网站没有该问题的解决方案，或该方案不能解决你的问题，请拨打公司的售后服务电话请求支援。公司的技术支持的联系方式如下：

   客户服务 E-mail： ip-com@ip-com.com.cn
   全国客户服务电话：
   公司总部售后支持电话：0755 - 21101879
   北京：010 - 86812368

3. 服务时间：
   周一到周五 9：00 - 12：00 13：30 - 18：00
   周六 9：00 - 12：00

IP-COM™

出品厂商：深圳市联科通网络技术有限公司
地址:深圳市福田区华强北路现代之窗A16J
服务电话:0755-21101879
网址:http://www.ip-com.com.cn
电子邮箱:ip-com@ip-com.com.cn