万兆强三层核心交换机

Web 配置手册

（适用于 **US5500-16F8C4TF**）

1 登录 WEB 界面

1.1 WEB 浏览的系统需求

使用此系列交换机，系统应该满足如下条件。

硬件与软件	系统需求
CPU	奔腾 586 以上
内存	128MB 以上
分辨率	1024x768 以上
颜色	256 色以上
浏览器	Internet Explorer 8.0 以上/Firefox/Google Chrome/Opera 等
操作系统	● Windows XP ● Windows Vista ● Windows 7 ● Windows 8 ● Linux ● Unix

1.2 登录 WEB 配置界面

要登录到此系列交换机的 WEB 配置界面，用户需确认如下条件：

- 已经对交换机进行了IP 配置，缺省情况下，交换机VLAN1的接口IP地址是192.168.255.1。
- 用户保证自己本地PC（管理主机）的网卡的IP是192.168.255.*的网段。
- 用户保证自己本地PC的网线接在1-24之间任意一个端口。
- 已将一台安装有Web浏览器的主机连接到网络上，并且主机能够PING通交换机。

登录 WEB 配置界面的操作步骤如下：

步骤 1 运行计算机浏览器。

步骤 2 在浏览器的地址栏中输入交换机的地址“http://192.168.255.1”，按回车键。

步骤 3 如图 2-1 所示，在登录窗口中输入用户名和密码（默认用户名和密码均为 admin），单击“确定”。

图 2-1 WEB 界面登录窗口

成功登录后，您可以根据需要配置 WEB 界面相关参数及信息。

2 系统状态

2.1 系统信息

【功能说明】

在“系统信息”页面，您可以查看设备型号、硬件版本号、固件版本号、设备序列号等信息。

【操作路径】

系统状态>系统信息

【界面说明】

图 2-1 系统信息界面

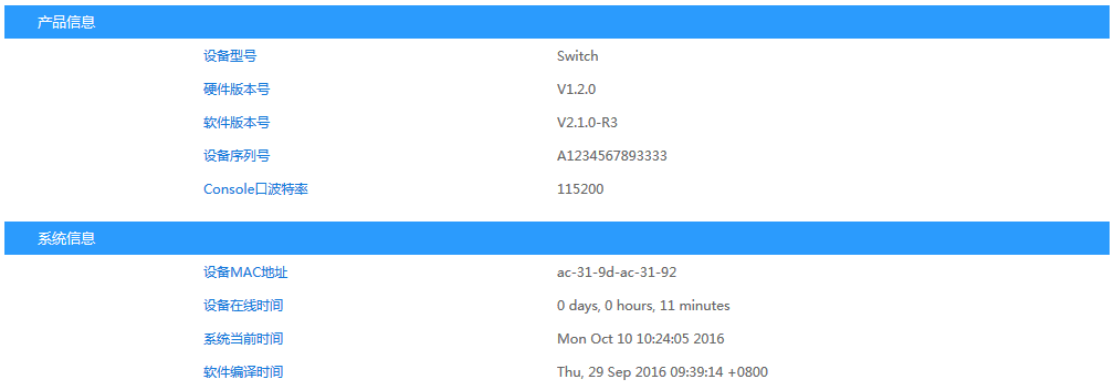


表 2-1 系统信息界面主要元素

界面元素	说明
设备类型	显示交换机的产品型号。
硬件版本号	显示交换机当前使用的硬件版本号。
软件版本号	显示交换机当前使用的软件版本号。
设备序列号	显示交换机的序列号。

串口波特率	显示交换机使用 Console 管理时的波特率。
界面元素	**说明**
设备 MAC 地址	显示交换机的 MAC 地址。
设备在线时间	显示交换机启动到现在的时间。
系统当前时间	显示系统的当前时间。
软件编译时间	显示软件的编译时间。

2.2 日志信息

【功能说明】

在“日志信息”页面，您可以查看并下载系统日志。

【操作路径】

系统状态 > 日志信息

【界面说明】

图 2-1-1 查看日志界面

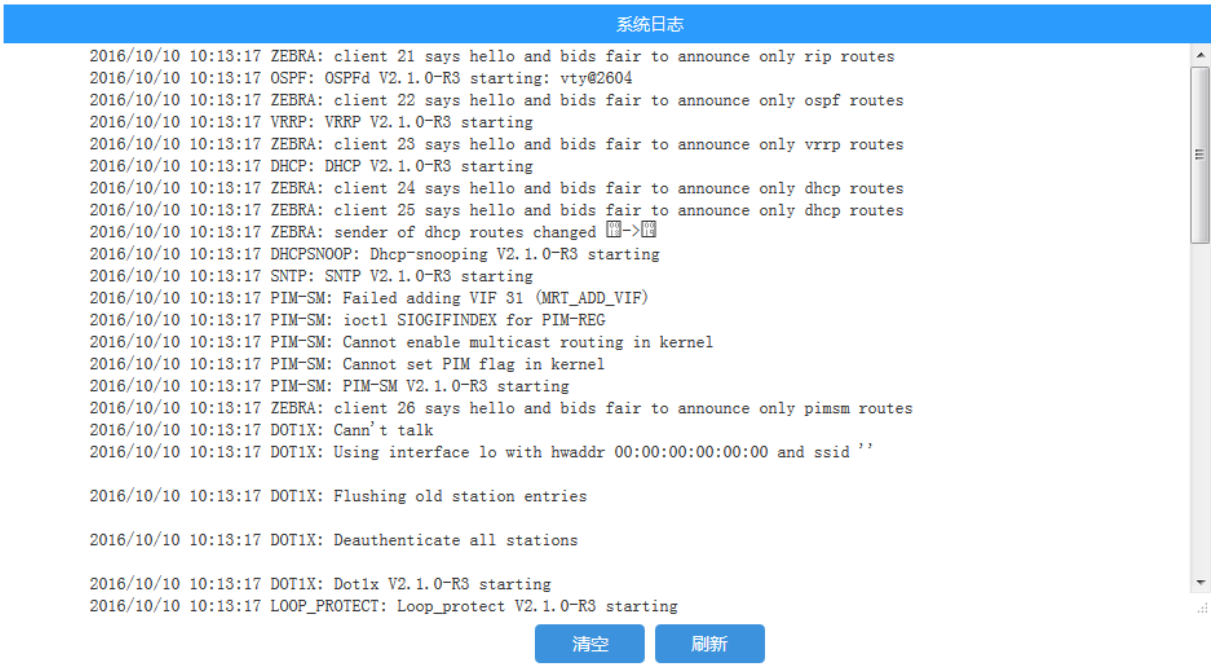


表 2-2-1 查看日志界面主要元素

界面元素	说明
系统日志	显示当前操作的信息。
清空	单击“清空”，可以清空当前系统日志。
刷新	单击“刷新”，可以刷新当前系统日志。

图 2-2-2 日志下载界面

表 2-2-2 日志下载界面主要元素

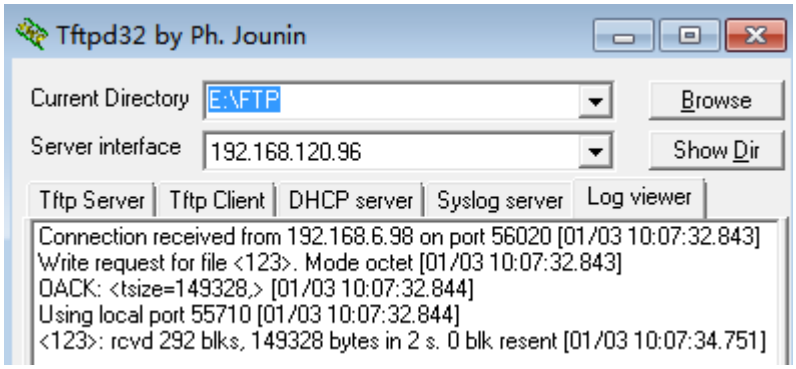
界面元素	说明
TFTP 服务器地址	输入服务器的 IP 地址。
文件名	输入日志文件在服务器上的保存名称。
下载	单击“下载”，可以将系统日志上传到服务器。

【示例】

1. 打开 tftp32 软件；

2. 在日志下载页面输入 tftp 服务器地址 192.168.120.96 和文件名；

3. 点击“下载”按钮。如下图：



2.3 端口统计

【功能说明】

在“端口统计”页面，您可以查看端口概要统计和端口详细统计相关信息。

【操作路径】

系统状态 > 端口统计

【界面说明】

图 2-3-1 端口概要统计界面

端口名称	数据包		字节		过滤
	接收	发送	接收	发送	接收
G1	16479	26597979	1308273	1812611243	1617
G2	26592335	143	1810989493	9696	26583364
G3	0	0	0	0	0
G4	0	0	0	0	0
G5	0	0	0	0	0
G6	0	0	0	0	0
G7	0	0	0	0	0
G8	0	0	0	0	0

表 2-3-1 端口概要统计界面主要元素

界面元素	说明
端口名称	显示端口名称。
数据包	显示发送和接收数据包数。
字节	显示发送和接收字节数。
过滤	显示接收方向过滤包数。

图 2-3-2 端口详细统计界面

表 2-3-2 端口详细统计界面主要元素

界面元素	说明
端口	单击“端口”下拉列表框，可选择任意一个端口来查看该端口的详细统计信息。
刷新	单击“刷新”，可刷新端口详细统计信息。
清空	单击“清空”，可清空端口详细统计信息。
接收总数	显示端口接收报文数、字节数等相关信息。
发送总数	显示端口发送报文数、字节数等相关信息。
接收报文大小分类统计	显示接收 64~9216 字节大小报文数的统计信息。
发送报文大小分类统计	显示发送 64~9216 字节大小报文数的统计信息。

2.4 Lacp 状态

【功能说明】

在“LACP 状态”页面，您可以查看 LACP 系统状态信息。

【操作路径】

系统状态> lacp 状态

【界面说明】

图 2-4 LACP 状态界面

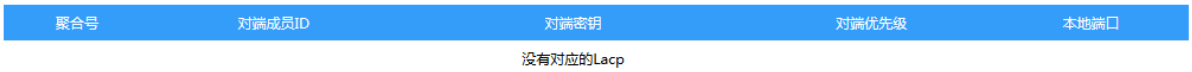


表 2-4 LACP 状态界面主要元素

界面元素	说明
聚合号	显示设置的聚合组 ID。
对端成员 ID	显示对端设备的聚合组成员 ID。
对端密钥	显示对端设备的聚合成员密钥。
对端优先级	显示对端设备聚合成员优先级。
本地端口	显示加入聚合组的该设备端口号。

2.5 查看路由

【功能说明】

在“查看路由”页面，您可以查看路由相关信息。

【操作路径】

系统状态 >查看路由

【界面说明】

图 2-5 查看路由界面

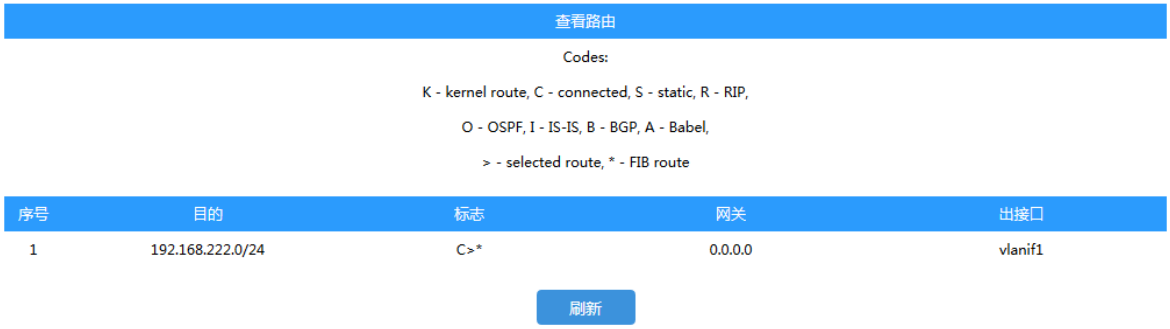


表 2-5 查看路由界面主要元素

界面元素	说明
序号	显示一条路由的序号。
目的	显示目的地址。
标志	显示连接状态。
网关	显示网关（下一跳）。
出接口	显示三层接口名称。

2.6 ERPS-Ring 状态

【功能说明】

在“ERPS-Ring 状态”页面，您可以查看 ERPS 状态信息。

【操作路径】

系统状态> erps-ring 状态

【界面说明】

图 2-6 ERPS-Ring 状态界面

端口	行动	传输报文	端口状态	Loop
G1	丢弃报文	禁止	Down	-
G2	丢弃报文	禁止	Down	-
G3	丢弃报文	禁止	Down	-
G4	丢弃报文	禁止	Down	-
G5	丢弃报文	禁止	Down	-
G6	丢弃报文	禁止	Down	-
G7	丢弃报文	禁止	Down	-
G8	丢弃报文	禁止	Down	-
G9	丢弃报文	禁止	Down	-
G10	丢弃报文	禁止	Down	-
G11	丢弃报文	禁止	Down	-
G12	丢弃报文	禁止	Down	-
G13	丢弃报文	禁止	Down	-
G14	丢弃报文	禁止	Down	-
G15	丢弃报文	禁止	Down	-

表 2-6 ERPS-Ring 状态界面主要元素

界面元素	说明
端口	显示交换机对应端口号。
行动	显示端口执行的动作。
传输报文	显示端口允许或禁止传输报文。
端口状态	显示端口状态是“up”还是“down”。
Loop 状态	显示端口 Loop 信息。

2.7 电源状态

【功能说明】

在“电源状态”页面，您可以查看电源供电状态信息。

【操作路径】

系统状态>电源状态

【界面说明】

图 2-7 电源状态界面

表 2-7 电源状态界面主要元素说明

界面元素	说明
电源 1	显示电源 1 的工作状态
电源 2	显示电源 2 的工作状态

3 系统设置

3.1 IP 配置

【功能说明】

在“IP 配置”页面可配置交换机的管理 IP 地址。

【操作路径】

系统设置 >ip 配置

【界面说明】

图 3-1 IP 配置界面

表 3-1 IP 配置界面主要元素

界面元素	说明
IP 地址	可以修改管理员 IP 地址。

3.2 用户配置

【功能说明】

在“用户配置”页面，您可以配置登录交换机 WEB 界面的用户名、密码和权限。

【操作路径】

系统设置 > 用户配置

【界面说明】

图 3-2 用户配置界面

表 3-2 用户配置界面主要元素

界面元素	说明
用户名	可以配置登录交换机 WEB 界面的用户名。
密码	可以配置登录交换机 WEB 界面的密码。
权限	可以配置登录交换机 WEB 界面的权限。 1.guest，2.admin。
修改	单击“修改”，可修改您配置的用户信息。
删除	单击“删除”，可删除您配置的用户信息。

3.3 时间设置

【功能说明】

在“时间设置”页面，您可以配置 NTP 服务器地址，使交换机系统时间与服务器同步。也可以手工配置当前时间。

【操作路径】

系统设置 > 时间设置

【界面说明】

图 3-3-1 NTP 配置界面

表 3-3-1 NTP 界面主要元素

界面元素	说明
模式	功能开启或者关闭。
使能	选择“使能”，表示开启 NTP 功能。
禁用	选择“禁用”，表示关闭 NTP 功能。
对时间隔	交换机与 NTP 服务器通信的时间间隔。
时区	下拉列表可以选择时区。
服务器	可以最多配置五个 NTP 服务器的地址。

图 3-3-2 本地时间配置界面

表 3-3-2 本地时间配置界面主要元素

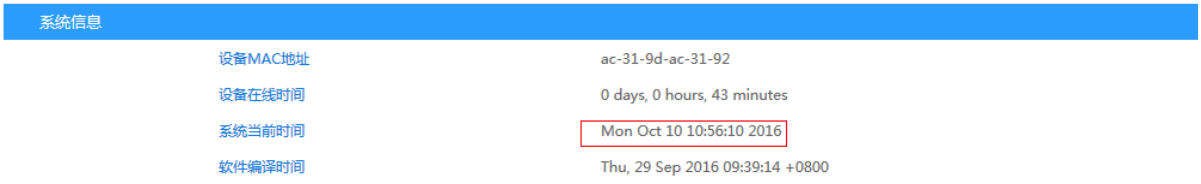
界面元素	说明
时间日期	设置本地时间和日期

【示例】

1. 使能 NTP 服务器，时间间隔默认 300s,时区设置为 00:00 伦敦时间，添加 NTP server：202.120.2.101。

2. 设置一条路由。如下图：

3. 在系统信息中可以看到时间变为伦敦时间。如图：



注意：如果时间没有改变：

1. 请确认交换机是否有联网（路由是否为通路）；2. 请重启交换机。

3.4 云管理配置

【功能说明】

在“云管理配置”页面，您可以配置云管理密钥，使交换机可以通过云盒子进行管理。

【操作路径】

系统设置 > 云管理配置

【界面说明】

图 3-4-1 云管理配置页面

表 3-4-1 云管理配置界面主要元素

界面元素	说明
云管理 key	配置 key 值和云盒子端相同，云盒子可以管理交换机。 默认为 admin。

4 端口配置

4.1 端口配置

【功能说明】

在“端口配置”页面，您可以启用或禁用端口，设置端口速率和流控，或查看所有端口的基本信息。

【操作路径】

端口配置 > 端口配置

【界面说明】

图 4-1 端口配置界面

端口名称	端口描述	状态	介质	速率双工配置	速率	双工模式	流控配置	流控状态	使能
*	-	-	-	<>	-	-		-	
G1		DOWN	RJ45	自协商	1G	AUTO			
G2		DOWN	RJ45	自协商	1G	AUTO			
G3		DOWN	RJ45	自协商	1G	AUTO			
G4		DOWN	RJ45	自协商	1G	AUTO			
G5		DOWN	RJ45	自协商	1G	AUTO			
G6		DOWN	RJ45	自协商	1G	AUTO			
G7		DOWN	RJ45	自协商	1G	AUTO			
G8		DOWN	RJ45	自协商	1G	AUTO			
G9		DOWN	RJ45	自协商	1G	AUTO			
G10		DOWN	RJ45	自协商	1G	AUTO			
G11		DOWN	RJ45	自协商	1G	AUTO			
G12		DOWN	RJ45	自协商	1G	AUTO			
G13		DOWN	RJ45	自协商	1G	AUTO			
G14		DOWN	RJ45	自协商	1G	AUTO			
G15		DOWN	RJ45	自协商	1G	AUTO			
G16		DOWN	RJ45	自协商	1G	AUTO			

表 4-1 端口配置界面主要元素

界面元素	说明
端口	显示端口名称。

端口描述	配置端口描述信息（只能包含数字、大小写字母和下划线）。
状态	显示端口状态。
介质	显示端口可以使用的介质类型。
速率、双工模式配置	配置端口速率，双工模式。
速率	显示端口速率。
双工模式	显示端口是否支持双工模式。
流控配置	选中“流控配置”复选框，则启用端口流控功能。
流控状态	显示端口流控状态。（“ ✕ 红色叉号”状态表示端口流控功能未启用或端口当前未发生流控，“ ✓ ”状态表示端口流控正在生效，可以正常发送或者接收 pause 帧）
端口使能	选中“使能”复选框，则启用相对应的端口。默认启用。

【示例】

端口 1 和端口 2 分别描述为 T1,T2,选择速率为 100M 全双工和 1000M 全双工,开启流控。如下图：

端口名称	端口描述	状态	介质	速率双工配置	速率	双工模式	流控配置	流控状态	使能
*	-	-	-	<>	-	-	☐	-	☑
G1	T1	DOWN	RJ45	百兆全双工	1G	AUTO	☐	✕	☑
G2	T2	DOWN	RJ45	强制千兆	1G	AUTO	☐	✕	☑
G3		DOWN	RJ45	自协商	1G	AUTO	☐	✕	☑
G4		DOWN	RJ45	自协商	1G	AUTO	☐	✕	☑
G5		DOWN	RJ45	自协商	1G	AUTO	☐	✕	☑
G6		DOWN	RJ45	自协商	1G	AUTO	☐	✕	☑

4.2 端口限速

【功能说明】

在“端口限速”页面，您可以配置所有端口出入速率。

【操作路径】

端口配置 > 端口限速

【界面说明】

图 4-2 端口限速界面

端口	入口速率(kbps) (0-10000000之间的整数)	出口速率(kbps) (0-10000000之间的整数)
*	0	0
G1	0	0
G2	0	0
G3	0	0
G4	0	0
G5	0	0
G6	0	0
G7	0	0
G8	0	0
G9	0	0

表 4-2 端口限速界面主要元素

界面元素	说明
端口	显示端口名称。
入口速率	配置相应端口出口速率。
出口速率	配置相应端口入口速率。

【示例】

在端口限速配置页面设置端口 1 的出口速率为 100Kbps；入口速率为 200Kbps。如图：

端口	入口速率(kbps) (0-10000000之间的整数)	出口速率(kbps) (0-10000000之间的整数)
*	0	0
G1	100	200
G2	100	200
G3	0	0
G4	0	0
G5	0	0

4.3 端口镜像

【功能说明】

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。

【操作路径】

端口配置 > 端口镜像

【界面说明】

图 4-3 端口镜像界面

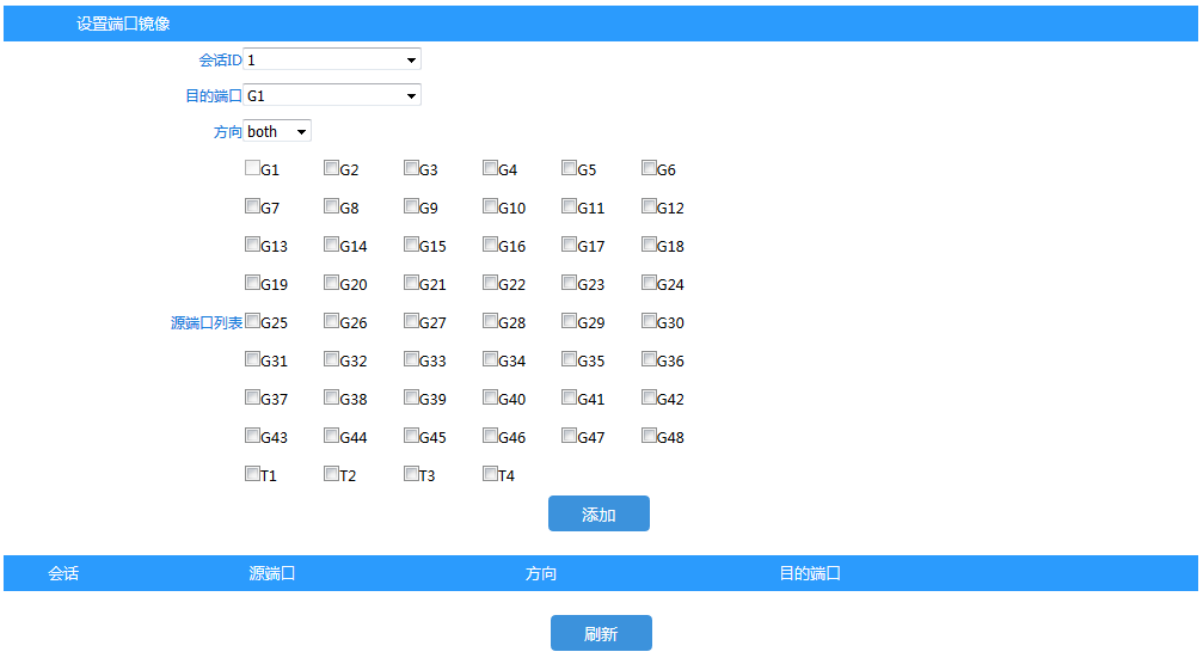
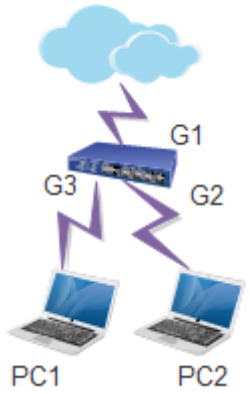


表 4-3 端口镜像界面主要元素

界面元素	说明
会话 ID	选择镜像会话的 ID，最多配置 4 个，取值范围为 1-4。
目的端口	选择镜像的目的端口，只能选一个。
方向	选择监听流入或流出、即流入又流出镜像源端口的数据流，包括 egress、ingress 和 both 三个选项。 egress：表示监听交换机端口收到的数据包。 ingress：表示监听交换机端口发送的数据包。 both：表示监听发送和接收的数据包。
界面元素	**说明**
源端口列表	勾选镜像源端口，可多选。

【示例】



会话	源端口	方向	目的端口	
1	G2	both	G1	删除

刷新

1. 设置源端口为 G1，目的端口为 G2，在 G2 抓包，可以抓到 G1 相关的数据包。

4.4 端口聚合

【功能说明】

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、ERPS 配置、loop Protect 配置、镜像、802.1x、IP 过滤、Mac 过滤、端口隔离等。

提示：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动态聚合（LACP），与交换机链路聚合的对端设备一般是交换机、网卡。

4.4.1 静态聚合

【功能说明】

静态聚合，需用户手动配置，不允许系统自动添加或删除聚合组中的端口，静态聚合配置逻辑简单，易于理解和使用。

【操作路径】

端口配置 >端口聚合

【界面说明】

图 4-4-1 聚合界面

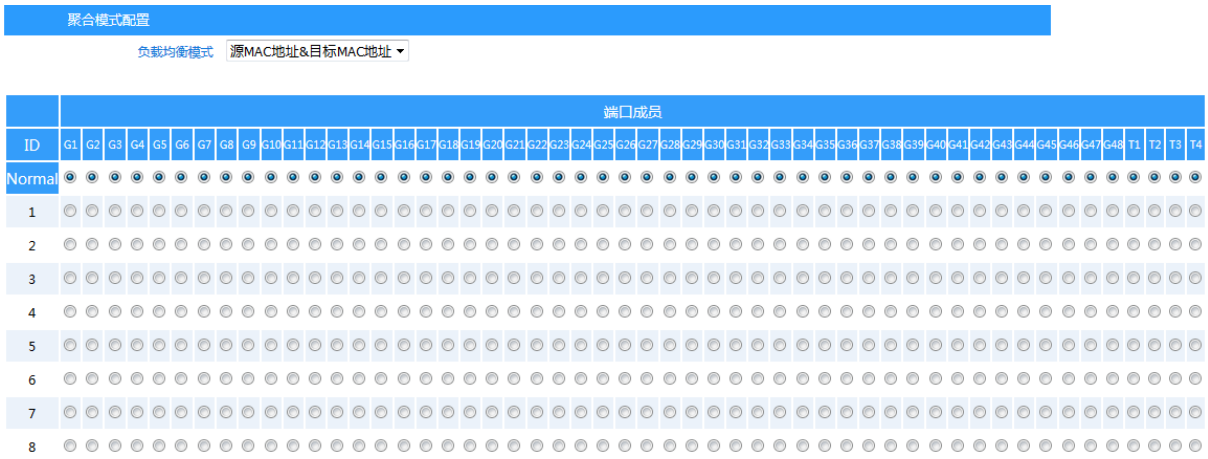


表 4-4-1 聚合界面主要元素

界面元素	说明
负载均衡模式	选择数据流的负载均衡模式。有以下三种： 1. Source MAC 2. Destination MAC 3. SMAC&DMAC
端口成员	选择需要汇聚成组的端口。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，点选端口到对应的聚合组，即可实现端口加入汇聚组。

特别提示：

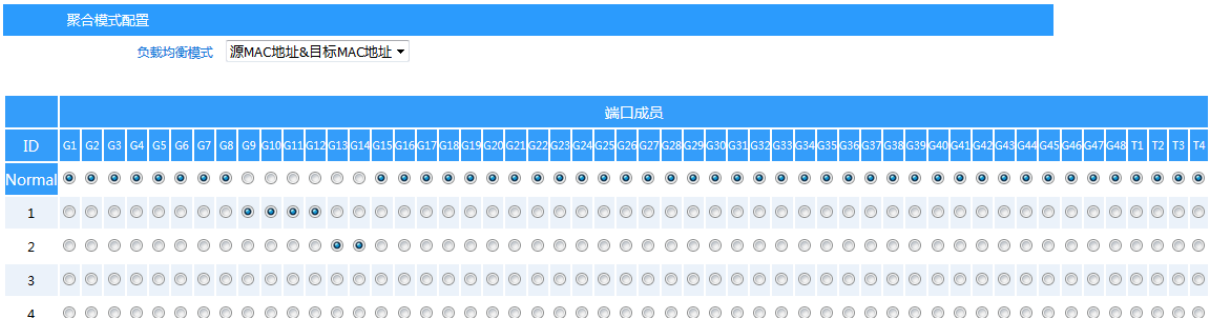
（1）同一端口静态汇聚不能与动态 LACP 汇聚同时配置；

（2）聚合组成员端口请保持配置方面的一致性；

（3）聚合组成员端口数目为 2-8 个。

【示例】

负载均衡模式选择 SMAC&DMAC，端口 9，10，11，12 添加到聚合组 1，端口 13，14 添加到聚合组 2。如下图：



4.4.2 LACP 配置

【功能说明】

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）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。

LACP 协议的配置参数主要包括：端口 LACP 功能使能、键值、端口角色（主动/被动模式）、端口优先级。

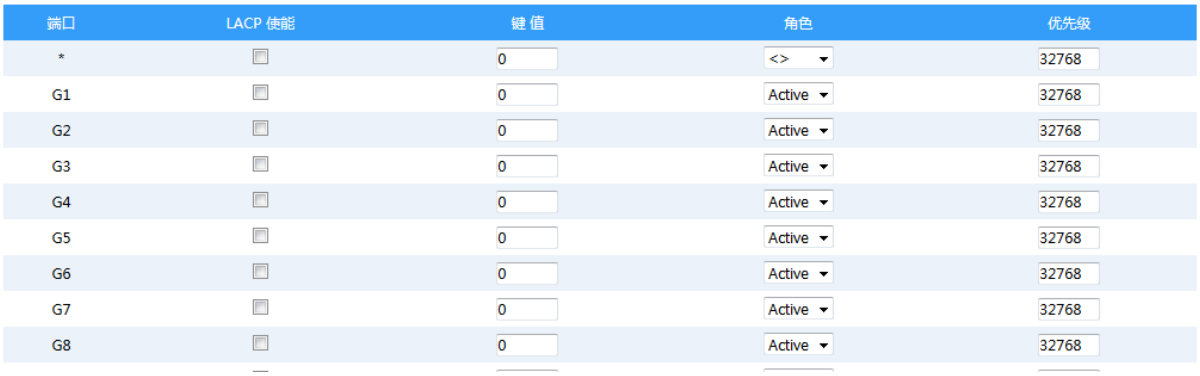
只有开启 LACP 协议的端口才会进行 LACP 协商，从而有可能形成汇聚链路。密钥是协商的基础，具有相同密钥的端口才能协商组成一个汇聚链路。协商模式“active/passive”，当选择“active”，设备会主动发起汇聚协商；当选择“passive”，设备被动接受其他设备发起的汇聚协商。两台设备互联，至少有一端或两端需设置成“active”模式才能协商成功。

【操作路径】

端口配置 > LACP 配置

【界面说明】

图 4-4-2 LACP 配置界面



端口	LACP 使能	键值	角色	优先级
*	☐	0	<>	32768
G1	☐	0	Active	32768
G2	☐	0	Active	32768
G3	☐	0	Active	32768
G4	☐	0	Active	32768
G5	☐	0	Active	32768
G6	☐	0	Active	32768
G7	☐	0	Active	32768
G8	☐	0	Active	32768

表 4-4-2 LACP 配置界面主要元素

界面元素	说明
端口	显示交换机端口号。
LACP 使能	启用或禁用 LACP 端口。
键值	同一汇聚组的成员，需配置相同的管理 Key（需手动配置，允许值范围 1-65535），默认为 0。
角色	配置端口角色信息。可选项为 Active 和 Passive，参与动态汇聚的设备一端要选择 Active 模式，另一端要选择 Passive 模式。默认为 passive。
优先级	配置 LACP 端口优先级。默认 32768。

5 高级配置

5.1 VLAN 配置

【功能说明】

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）技术的共享通讯介质。采用以太网技术构建的局域网，既是一个冲突域，又是一个广播域，当网络中主机数目较多时会导致冲突严重，广播泛滥、性能显著下降，甚至网络不可用等问题。通过在以太网中部署网桥或二层交换机，可以解决冲突严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN。处于同一 VLAN 的主机能直接互通，而处于不同 VLAN 的主机则不能直接互通。这样，广播报文被限制在同一个 VLAN 内，即每个 VLAN 是一个广播域。

VLAN 的优点如下：

1) 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。

2) 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。

3) 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。

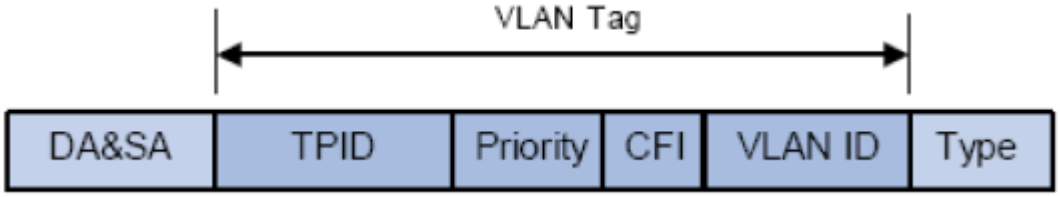
VLAN 划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机。

802.1Q VLAN

由于普通交换机工作在 OSI 模型的数据链路层，若要交换机能够识别不同 VLAN 的数据包，只能对数据包的数据链路层封装进行 VLAN 识别。因此，VLAN 识别字段被添加到数据链路层封装中。

IEEE 802.1Q 协议为了标准化 VLAN 实现方案，对带有 VLAN 标识的数据包结构进行了统一规定。协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息， VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol

Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。 如下图所示：



1) TPID：用来表示本数据帧是带有 VLAN Tag 的数据。该字段长度为 16bit。协议规定的缺省取值为 0x8100。

2)优先级：用来表示数据包的传输优先级。

3) CFI：以太网交换机中，CFI 总被设置为 0。由于兼容特性，CFI 常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧 CFI 设置为 1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。

4) VLAN ID：用来标识该报文所属 VLAN 的编号。该字段长度为 12bit，取值范围为 0~4095。由于 0 和 4095 为保留值，通常不给用户使用，所以 VLAN ID 的取值范围一般为 1~4094。VLAN ID 简称 VID。

交换机利用 VLAN ID 来识别报文所属的 VLAN，当接收数据包不带 VLAN Tag 时，交换机会为该数据包封装带有接收端口默认 VLAN ID，将数据包在接收端口的缺省 VLAN 中进行传输。

本手册中，对包含 VLAN Tag 字段的数据包我们简称为 tag 帧，untag 帧指数据包中没有 VLAN Tag 字段的数据包，优先级 tag 帧指数据包中有 VLAN Tag 字段，但 VLAN ID 为 0 的数据包。

端口的三种链路类型 ：

在创建 802.1Q VLAN 时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

1)ACCESS：端口只能属于 1 个 VLAN，出口规则为 UNTAG，多为连接用户终端设备的端口。当 ACCESS 类型端口加入了其它 VLAN 时，则自动退出原有 VLAN。

2)TRUNK：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，常用于网络设备之间级连。在网络中 VLAN 经常跨接在不同交换机上，TRUNK 类型端口的默认出口规则为 TAG，在转发端口默认 VLAN 数据时去掉 VLAN 信息，转发其余 VLAN 数据时保持原有 VLAN 信息。

3)Hybrid：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于网络设备之间连接，也可以用于连接用户设备。Hbrid 类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

PVID 与 VLAN 数据包处理关系：

PVID（端口 VLAN ID），就是端口的缺省 VID。当交换机的端口接收到的报文不带 VLAN Tag 时，交换机会根据接收端口的 PVID 值为该报文插入 VLAN Tag，并进行转发。

当在局域网中划分 VLAN 时，PVID 是每个端口的一个重要参数，表示端口默认所属的 VLAN。它有两个用途：

1） 当端口收到 untag 报文时，将根据 PVID 为数据包插入 VLAN Tag。

2）PVID 指定了端口的默认广播域，即当端口接收到 UL 包或广播包的时候，交换机将这些数据包在该端口的默认 VLAN 内广播。

IEEE802.1Q VLAN 功能包括 VLAN 配置、VLAN 状态两个页面。

【操作路径】

高级配置> vlan 配置

【界面说明】

图 5-1-1 VLAN 配置界面

表 5-1-1 VLAN 配置界面主要元素

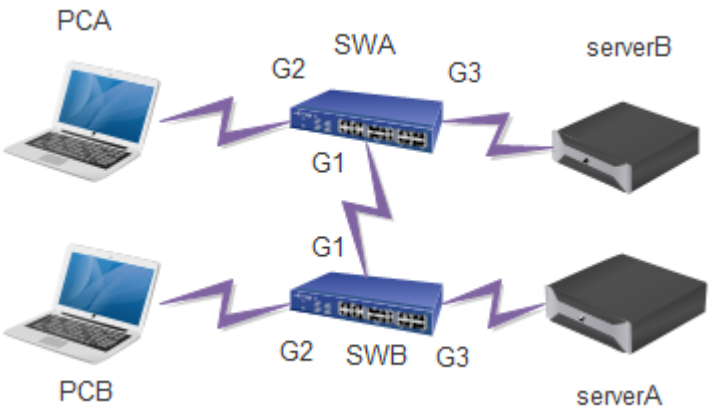
界面元素	说明
端口	显示端口名称。
模式	配置端口模式 Access/Trunk/Hybrid。
QinQ 使能	配置端口 QinQ 使能/去使能。
端口默认 VLAN	输入 ID 值，可设置端口 pvid 值。
UNTAG VLAN	配置 VLAN 出口标签 tag/untag。
VLAN 配置	输入 VLAN ID（1-4094），可以配置属于该端口的 VLAN。

图 5-1-2 VLAN 状态界面

表 5-1-2 VLAN 状态界面主要元素

界面元素	说明
端口成员	显示各个端口 VLAN 信息。

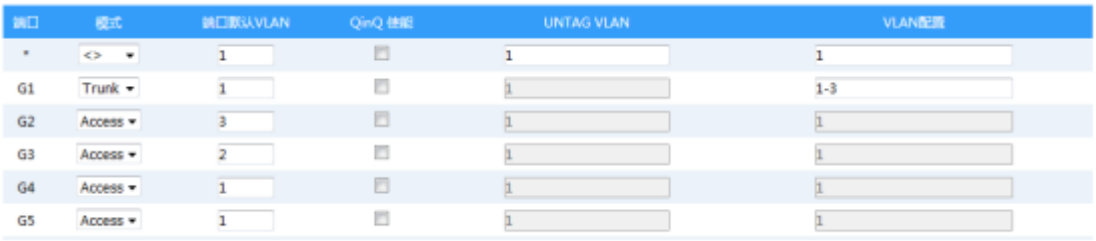
【示例】



组网需求：交换机 A 连接 PCA 和服务器 B，交换机 B 连接服务器 A 和计算机 B；计算机 A 和服务器 A 同属一个部门，计算机 B 和服务器 B 同属一个部门；两个部门以 VLAN 划分，互相之前不能通信。

Step1：配置交换机 A：端口 G3 加入 VLAN3 ，端口类型为 Access；端口 G2 添加到 VLAN2，端口类型为 Access；端口 G1 添加到 VLAN1-3，PVID 为 1，端口类型为 Trunk，添加 tag；配置如图示：

Step2：配置交换机 B：端口 G3 加入 VLAN2 ，端口类型为 Access；端口 G2 添加到 VLAN3，端口类型为 Access；端口 G1 添加到 VLAN1-3，PVID 为 1，端口类型为 Trunk，添加 tag；配置如图示：



5.2 QinQ 配置

【功能说明】

QinQ 技术（也称 Stacked VLAN 或 Double VLAN）是指将用户私网 VLAN 标签封装在公网 VLAN 标签中，使报文带着两层 VLAN 标签穿越运营商的骨干网络，在公网中只根据外层 VLAN 标签传播，私网 VLAN 标签被屏蔽，这样，不仅对数据流进行了区分，而且由于私网 VLAN 标签被透明传送，不同的用户 VLAN 标签可以重复使用，只需要外层 VLAN 标签的在公网上唯一即可，实际上也扩大了可利用的 VLAN 标签数量。

【操作路径】高级配置 > QinQ 配置

【界面说明】

图 5-2 QinQ 配置界面

表 5-2 QinQ 配置界面主要元素

界面元素	说明
OTPID	设置外层标签协议标识。默认 8100，可以设置成和其他设备兼容的 88a8 等 TPID

5.3 MAC 配置

【功能说明】

在“MAC 配置”页面，您可以配置 MAC 地址的老化时间，查看端口的 MAC 地址信息。

【操作路径】

高级配置 > mac 配置

【界面说明】

图 5-3 MAC 配置界面

表 5-3 MAC 配置界面主要元素

界面元素	说明
MAC 老化时间	设置 MAC 老化时间，取值范围为 10-1000000s。默认 300s。

5.4 ARP 配置

【功能说明】

在 ARP 配置页面，你可以配置 arp 老化时间或者静态绑定 IP+MAC，IP 或者 MAC 其中一个和绑定的条目中的 IP 或者 MAC 不同的，不能访问 CPU，但可以转发；IP+MAC 都不同或者都相同的则可以访问 CPU，也可转发。

【操作路径】

高级配置 > arp 配置

【界面说明】

图 5-1-1 查看 ARP 界面

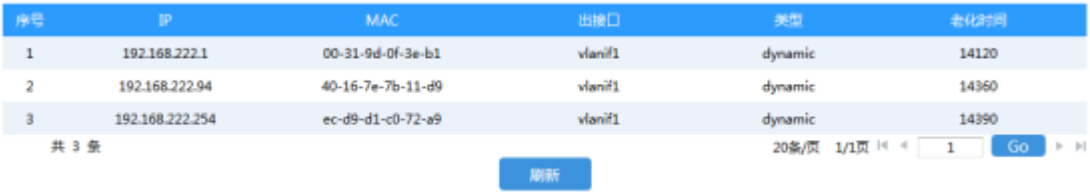


表 5-4-1 查看 ARP 配置界面主要元素

界面元素	说明
序号	显示条目序号。
IP	ARP 条目的 IP 地址。
MAC	ARP 条目的 MAC 地址。
出接口	显示绑定的虚接口。
类型	显示 arp 条目是动态还是静态。
老化时间	显示 Arp 老化时间，默认为 14400s。

图 5-2-2 静态 ARP 界面

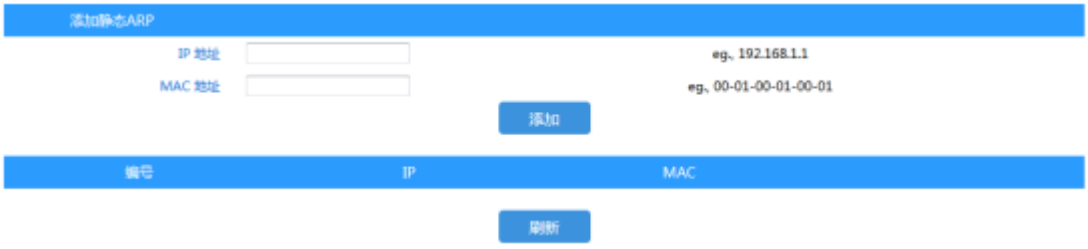


表 5-4-2 静态 ARP 界面主要元素

界面元素	说明
IP 地址	配置需要绑定的 IP 地址。
MAC 地址	配置 ARP 条目的 MAC 地址。

图 5-3-3 ARP 老化时间界面

表 5-4-3 ARP 老化时间界面主要元素

界面元素	说明
Interface	显示 ARP 老化时间对应的接口。
老化时间	配置 ARP 老化时间，默认 14400s。

【示例】

绑定 PCA 的 MAC 和 IP 后，PCA 可以 ping 通 SWB，也可以 ping 通 PCB。修改 PCA 的 IP 为非 192.168.6.96 后，则不能 ping 通 SWB，但可以访问 PCB。

5.5 MSTP 配置

【功能说明】

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

本设备生成树功能配置简单，使能生成树功能后选择相关协议（STP 或 RSTP）即可使用，多生成树 MSTP 也只需要使能后配置实例即可使用。

【操作路径】

高级配置 > mstp 配置

【界面说明】

图 5-5-1 全局配置界面

表 5-5-1 全局配置界面主要元素

界面元素	说明
使能	勾选则启用生成树，否则不启用。
模式	选择生成树协议模式，可选 stp、rstp 和 mstp。
最大老化时间	老化时间，数值范围为 6-40 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。 默认 20 秒。
有效时间	联络时间，数值范围为 1-10 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。默认 2 秒。

转发延迟时间	传输时延，数值范围为 4-30 秒，是指交换机的端口状态迁移所用的时间。默认 15 秒。
最大跳数	最大跳数，数值范围为 1-40，默认 20 跳。

图 5-4-2 域配置界面

表 5-1-2 域配置界面主要元素

界面元素	说明
修订级别	配置修订号，默认为 0。（范围：0-65535）
域名	配置域名，默认为设备 MAC 地址，最大长度为 31 位。

图 5-5-3 实例配置界面

MSTI 是 MST 域的一个属性，用来描述 VLAN 和生成树实例的映射关系。可以按需要将 VLAN 分配至不同的实例，每个实例就是一个“VLAN 组”，不受其它实例和公共生成树的影响。

表 5-2-3 实例配置界面主要元素

界面元素	说明
实例 ID	设置实例编号。
Vlan 映射	设置 Vlan 映射。

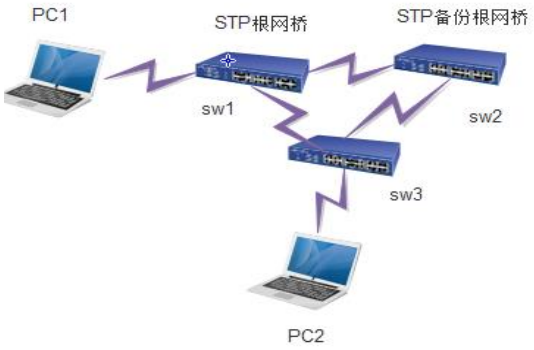
实例优先级	设置实例优先级 默认为 8，范围 0-15

图 5-5-4 端口状态界面

表 5-5-4 端口状态界面主要元素

界面元素	说明
实例 ID	选择实例 ID。
实例号	显示实例编号。
端口	显示各实例对应的端口号。
角色	显示端口角色信息。
状态	显示端口状态信息。

【示例】



1. SW1，SW2，SW3 使能 STP，SW1 选举为根网桥，SW2 为备份根网桥；

2. 当 SW3 与根网桥直连线路中断时，STP 能迅速切换，不影响网络通信。

5.6 IGMP 侦听

【功能说明】

IGMP 侦听是 Internet Groupmanagement Protocol 侦听（网际组播管理协议探测）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。运行 IGMP 侦听 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。

在“IGMP 侦听配置”页面，您可以进行全局配置，静态组播配置。

【操作路径】

高级配置>igmp 侦听

【界面说明】

图 5-6-1 igmp 侦听界面

表 5-6-1 igmp 侦听界面主要元素

界面元素	说明
使能	选择“使能”启用 IGMP 侦听功能，选择“禁用”则禁用 IGMP 侦听功能。
老化时间	配置主机老化时间，范围 200-1000s，默认 260s。
端口	显示端口信息。
快速离开	配置端口快速离开功能。

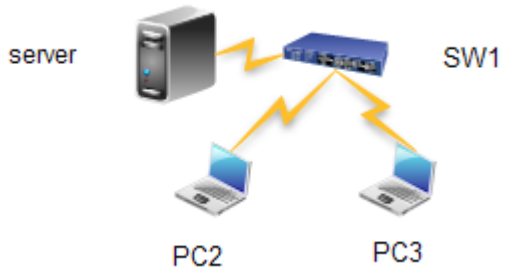
图 5-6-2 静态组播界面

表 5-6-2 静态组播界面主要元素

界面元素	说明
Vlan ID	填写 VLAN ID，范围 1-4094。
组播地址	填写静态绑定的组播 IP 地址。
端口列表	选择组播组成员端口。

静态绑定指组播源只能被限定的个别端口接收，没有绑定的端口不能接收。非静态绑定的组播源可以在绑定端口接收。

【示例】



server 为组播源 239.2.2.2，SW1 的端口 1 和端口 2 加入组播组。PC2 和 PC3 直连

端口 1、端口 2。

PC2 和 PC3 可以收到组播流。没加入组播组的端口不能收到组播流。

5.7 DHCP Server

【功能说明】

在“DHCP 服务器 ”页面，您可以进行地址池配置和静态绑定配置。

【操作路径】

高级配置 > dhcp 服务器

【界面说明】

图5-7-1 全局配置界面

表5-7-1 DHCP Server界面主要元素

界面元素	说明
使能	开启或禁用 DHCP 功能

图5-7-2 DHCP Leases配置界面

表5-7-2 DHCP leases配置界面主要元素

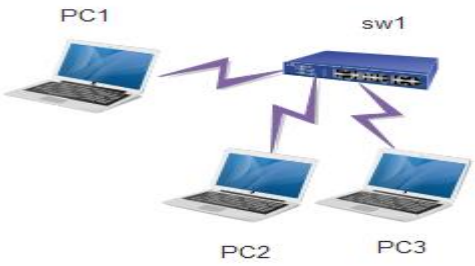
界面元素	说明
Pool name	填写 dhcp 地址池的名字。
起始 IP 地址	填写 DHCP 地址池的开始地址
结束 IP 地址	填写 DHCP 地址池的结束地址
Lease time	填写地址的租赁时间。
Default gateway	填写客户端默认网关，这个将作为服务器分配给客户端的默认网关参数。默认网关的 IP 地址必须与 DHCP 客户端的 IP 地址在同一网络。
主 DNS 服务器	填写主 DNS Server 地址
备 DNS 服务器	填写备 DNS 服务器地址
域名	填写服务器域名
接口	选择绑定的三层接口

图5-7-3 DHCP static leases配置界面

表5-7-3 DHCP static leases界面主要元素

界面元素	说明
DHCP 池	选择 DHCP 地址池。
IP 地址	填写要绑定的 IP 地址。
MAC 地址	填写要绑定的 MAC 地址。

【示例】



如上图，SW1 配置 DHCP server pool，PC1，PC2，PC3 自动获取地址，可以从 DHCP server pool 获取到地址。

注意：地址池和接口 IP 在同一网段。

5.8 DHCP Relay

【功能说明】

如果 DHCP 客户机与 DHCP 服务器在同一个物理网段，则客户机可以正确地获得动态分配的 ip 地址。如果不在同一个物理网段，则需要 DHCP Relay Agent(中继代理)。用 DHCP Relay 代理可以去掉在每个物理的网段都要有 DHCP 服务器的必要,它可以传递消息到不在同一个物理子网的 DHCP 服务器，也可以将服务器的消息传回给不在同一个物理子网的 DHCP 客户机。

【操作路径】

高级配置 > dhcp relay

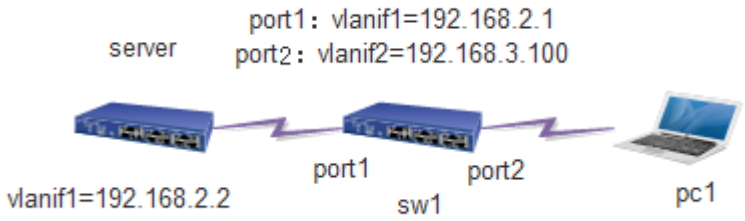
【界面说明】

图5-8 DHCP relay界面

表 5-8 DHCP relay 界面主要元素

界面元素	说明
接口	选择对应的三层接口。
Dhcp 服务器地址	配置服务器 IP 地址。

【示例】



配置 server：

1. 使能 dhcp(注：此使能按钮不是 DHCP server 使能，而是 DHCP 全局使能。在 SW1 上也必须开启)

2. 设置地址池 1。如下：

3. 在 server 上设置静态路由，如下：

配置 SW1：

1. 在 sw1 上使能 dhcp；

2. 配置 3 层接口：vlanif1=192.168.2.1；vlanif2=192.168.3.100

3. 配置 relay：在 vlanif2 下配置地址 192.168.2.2

4. 设置 SW1 的端口 2 的 pvid=2，连接 PC1。

5. PC1 自动获取 IP=192.168.3.3

5.9 DHCP 侦听

【功能说明】

DHCP 侦听 是 DHCP 的一种安全特性，具有如下功能：

1. 保证客户端从合法的服务器获取 IP 地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP 侦听 安全机制允许将端口设置为信任端口和不信任端口：

a. 信任端口正常转发接收到的 DHCP 报文。

b. 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP 侦听设备上指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系

DHCP 侦听 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCPSnooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现：

ARP Detection（ARP 检测）：根据 DHCP 侦听 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。

IP 源保护（IP 源保护）：通过动态获取 DHCP 侦听 表项对端口转发的报文进行过滤，防止非法报文通过该端口。

【操作路径】

高级配置 > dhcp 侦听

【界面说明】

图 5-9-1 全局配置界面

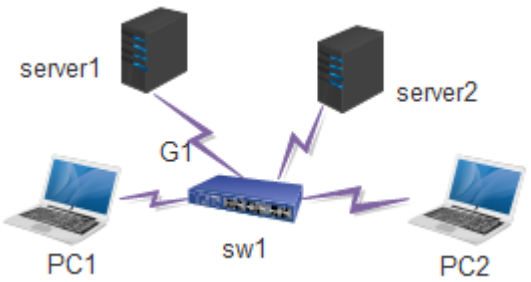
表 5-9-1 全局配置界面主要元素

界面元素	说明

侦听模式	禁用或启用 DHCP 侦听功能
端口	显示端口信息
模式	配置端口模式，可选信任、不信任。

图 5-9-2 DHCP 动态表界面

【示例】



交换机端口 G1 级联 server1，交换机下面所接 PC 均要从此服务器获取地址；交换机其它端口可能接有具有 DHCP 服务器功能的设备，通过配置，使得交换机下面的 PC 只能获取到 G1 端口所连接的 server1 分配的地址。

使能 DHCP 侦听全局开关，除 G1 口配置信任模式外，其它端口均配置非信任模式，配置如下图示：

5.10 QoS 配置

【功能说明】

QoS(Quality of Service，服务质量)指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是用来解决网络延迟和阻塞等问题的一种技术。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。

【操作路径】

高级配置> QoS 配置

【界面说明】

图 5-10-1 端口优先级页面

表 5-10-1 端口优先级界面主要元素

界面元素	说明
端口	显示端口号
优先级标记	选择优先级重标记类型。 1 Cos,2 dscp,3 all （选择 all 时，生效的是 dscp，dscp 优先级高于 cos）。
默认 cos	配置默认优先级。默认为 0（0-7）。值越大，优先级越高。
信任优先级	配置信任优先级，勾选表示信任数据包的优先级，不勾选表示信任可配置的默认 cos

图 5-10-2 802.1P 优先级页面

表 5-10-2 802.1P 优先级界面主要元素

界面元素	说明
Cos 优先级	显示 cos 优先级(0-7)
队列	选择 cos 优先级对应的 queue(0-7),默认 cos 优先级（0-7）和队列（0-7）一一对应。

图 5-10-3 DSCP 优先级页面

表 5-10-3 DSCP 优先级界面主要元素

界面元素	说明
Cos 优先级	显示 cos 优先级(0-7)
DSCP 优先级	选择 cos 优先级对应的 DSCP 优先级(0-63)做映射。默认 DSCP 优先级 0-7 对应 cos 优先级 0,DSCP 优先级 8-15 对应 cos 优先级 1，以此类推，DSCP 优先级 56-63 对应 cos 优先级 1。

图 5-10-4 调度配置页面

表 5-10-4 调度配置界面主要元素

界面元素	说明
调度模式	选择调度策略 SP 或者 WRR
队列	显示队列序号
权重	配置权重，WRR 时可以配置，SP 时权重为固定值。
占宽比	显示权重对应的占款比，改变队列权重大小，该队列占宽比也会变化。

5.11 VRRP

【功能说明】

VRRP 是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负

责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。是一种 LAN 接入设备备份协议。一个局域网络内的所有主机都设置缺省网关，这样主机发出的目的地址不在本网段的报文将被通过缺省网关发往三层交换机，从而实现了主机和外部网络的通信。

VRRP 是一种路由容错协议，也可以叫做备份路由协议。一个局域网络内的所有主机都设置缺省路由，当网内主机发出的目的地址不在本网段时，报文将被通过缺省路由发往外部路由器，从而实现了主机与外部网络的通信。当缺省路由器 down 掉（即端口关闭）之后，内部主机将无法与外部通信，如果路由器设置了 VRRP 时，那么这时，虚拟路由将启用备份路由器，从而实现全网通信。

【操作路径】

高级配置> vrrp

【界面说明】

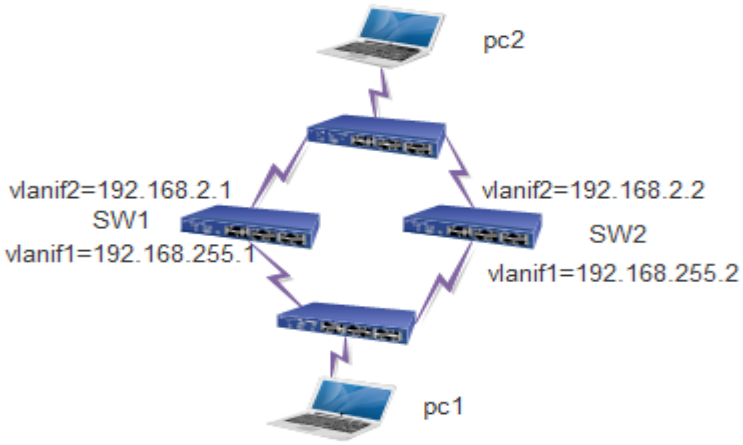
图 5-11 VRRP 页面

表 5-11 端口优先级 界面主要元素

界面元素	说明
接口	选择接口
虚拟路由器 ID	配置虚拟路由 ID 范围是 1-255
虚拟 IP	配置虚拟 IP。
通告时间间隔	配置通告间隔时间 范围是 1-10s。
优先级	配置优先级 默认是 100，范围是 1-254。

抢占	配置“抢占”模式。
抢占延迟	配置“抢占时延”范围是 1-1000s。

【示例】



SW1 配置：vlan1=192.168.255.1,vlan2=192.168.2.1

Vlan1 的虚拟 ID=100，虚拟 IP=192.168.255.100，其他默认。

Vlan2 的虚拟 ID=200，虚拟 IP=192.168.2.100,其他默认。

接口	使能	状态	IP 模式	MAC	IPv4		
vlanif1	☑	UP	static	ac-31-9d-ac-31-92	192.168.255.1/24	修改	删除
vlanif2	☑	DOWN	static	ac-31-9d-ac-31-92	192.168.2.1/24	修改	删除

接口	虚拟路由器ID	虚拟IP	状态	通告时间间隔	基本优先级	有效优先级	抢占	抢占延迟	
vlanif2	200	192.168.2.100	INIT	1	100	0	enable	0	删除
vlanif1	100	192.168.255.100	BACKUP	1	100	100	enable	0	删除

SW2 配置：vlan1=192.168.255.2,vlan2=192.168.2.2

Vlan1 的虚拟 ID=100，虚拟 IP=192.168.255.100，优先级设置为 50，其他默认。

Vlan2 的虚拟 ID=200，虚拟 IP=192.168.2.100，优先级设置为 50，其他默认。

接口	使能	状态	IP 模式	MAC	IPv4		
vlanif1	☑	UP	static	ac-31-9d-ac-31-92	192.168.255.2/24	修改	删除
vlanif2	☑	DOWN	static	ac-31-9d-ac-31-92	192.168.2.2/24	修改	删除

接口	虚拟路由器ID	虚拟IP	状态	通告时间间隔	基本优先级	有效优先级	抢占	抢占延迟	
vlanif2	200	192.168.2.100	INIT	1	50	0	enable	0	删除
vlanif1	100	192.168.255.100	BACKUP	1	50	100	enable	0	删除

PC1：IP=192.168.255.5　默认网关=192.168.255.100

PC2：IP=192.168.2.5 默认网关=192.168.2.100

说明：

因为我们的设备还未支持路由选择协议，所以需要两边都做 vrrp 的组网方式才可。并且，vrrp 的主备倒换功能要想完美的使用，还需要 bfd 等链路检测协议配合使用，这些协议我们暂且还不支持，所以，主备倒换功能，仅模拟某台设备断电的情况。

6 路由配置

6.1 接口配置

【功能说明】

在“接口配置”页面，您可以配置接口参数。

【操作路径】

路由配置 > 接口配置

【界面说明】

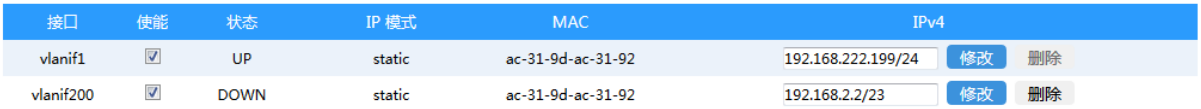
图 6-1 接口配置页面

表 6-1 接口配置界面主要元素

界面元素	说明
接口名称	设置三层接口名称，格式为 vlanifX(X 的范围 1-4094)。
使能	勾选则启用三层接口功能，不勾选则禁用三层接口功能。默认启用。
IPV4 地址	设置 IP 地址和掩码位数。
修改	修改 IP 后，点击 modify 按钮后 IP 修改成功。

【示例】

如图:设置 interface name 为 vlanif200,IP 设置为 192.168.2.2/23。



6.2 静态路由

【功能说明】

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

【操作路径】

路由配置〉静态路由

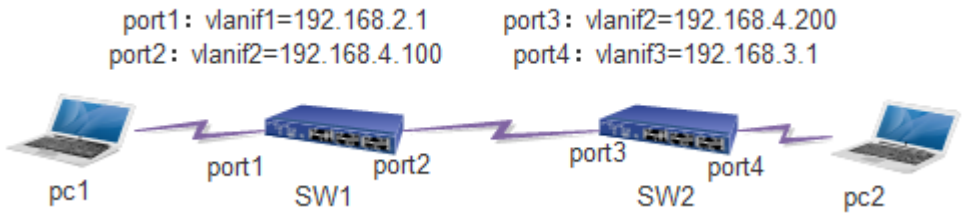
【界面说明】

图 6-2 静态路由页面

表 6-2 静态路由界面主要元素

界面元素	说明
网络地址	填写目的网络地址。
网关（下一跳）	填写下一跳的地址。
距离	填写管理距离，默认为 1，范围是 1-255。

【示例】



1.设置 PC 的 IP 和网关：

PC1：ip=192.168.2.100，gateway=192.168.2.1

PC2：ip=192.168.3.100，gateway=192.168.3.1

2.设置 SW 的 3 层接口 IP 和端口的 PVID：

Sw1：端口 1 属于 vlanif1,端口 2 属于 vlanif2,端口默认 access 模式。

vlanif1=192.168.2.1，vlanif2=192.168.4.100，端口 2 的 pvid=2

Sw2：端口 3 属于 vlanif2，端口 4 属于 vlanif3，端口默认 access 模式。

vlanif3=192.168.3.1，vlanif2=192.168.4.200，端口 3 的 pvid=2，端口 4 的 pvid=3

3.设置 SW 的静态路由：

SW1：如下图：

编号	目的	子网掩码	网关	距离	
1	192.168.3.0	24	192.168.4.200	1	删除

SW2：如下图：

编号	目的	子网掩码	网关	距离	
1	192.168.2.0	24	192.168.4.100	1	删除

4.PC1 和 PC2 互 ping，双方可以相互通信。

6.3 OSPF 配置

【功能说明】

OSPF 英文全称 Open Shortest Path First（开放式最短路径优先）。它是一种链路状态路由协议，使用基于带宽的度量值。OSPF 采用 SPF 算法计算路由，从算法上保证了无路由环路，通过邻居关系维护路由，避免了定期更新对带宽的消耗。OSPF 路由更新效率高，网络收敛快，适用于大中型网络。在“OSPF”页面，您可以配置 OSPF 参数。

【操作路径】

路由配置 >ospf 配置

【界面说明】

图 6-3-1 OSPF 全局配置页面

表 6-3-1 OSPF 全局配置界面主要元素

界面元素	说明
OSPF 使能	勾选则启用 ospf，不勾选则禁用 ospf。
路由器 ID	填写路由器 ID 号。
默认分发	使能/去使能默认分发。
度量类型	选择开销类型，默认为 2。
度量	设置引入外部路由时的开销（范围：0-16777214）
默认距离	填写 ospf 的默认开销值（范围：0-16777214）
接口默认被动	使能/去使能被动接口
延迟	填写节流 SPF 定时器延时时间，默认 200ms,(范围 1-600000ms)
初始保持时间	Initial hold time (msec) between consecutive SPF calculations,默认 1000ms,(范围 1-600000ms)
最大保持时间	Maximum hold time (msec)，默认 10000ms,(范围 1-600000ms)
重发布	选择重发布的路由类型。 1.Connect,2.static,3.rip

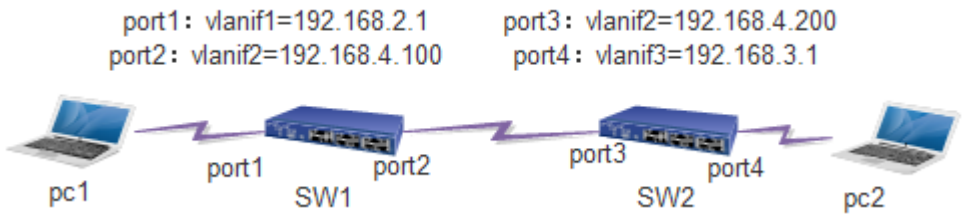
图 6-3-2 OSPF 网络界面

表 6-3-2 OSPF 网络界面主要元素

界面元素	说明
网络	填写路由网段地址和掩码。
区域	填写区域信息。
OSPF 网络	显示路由网段信息。
interface	显示接口名称。
网络	选择 ospf 的类型： **Point-to-point**：Hello 报文发送到组播地址 224.0.0.5，邻居可以自动发现，不选举 DR/BDR，默认 Hello 计时器为 10 秒、Dead 计时器为 40 秒。 **Broadcast**:Hello 报文发送到组播地址 224.0.0.5，邻居可以自动发现，选举 DR/BDR，默认 Hello 计时器为 10 秒、Dead 计时器为 40 秒。 **Non-broadcast**：Hello 报文是用单播来发送，邻居需要手工指定，不选举 DR/BDR，默认 Hello 计时器为 30 秒、Dead 计时器为 120 秒。 **Point-to-multipoint**：Hello 报文是发送到组播地址 224.0.0.5，邻居可以自动发现不选举 DR/BDR，默认 Hello 计时器为 30 秒、Dead 计时器为 120 秒。

开销	接口开销，默认为 10。
有效间隔	发送 hello 报文的间隔，默认为 10s。
失效间隔	路由器发出的 Hello 数据包没有被邻居看到而宣称此 OSPF 路由器已消失（关闭）所需要等待的秒数。默认为 40s。
优先级	接口优先级，默认为 1，范围（0-255）。
认证类型	基于区域的认证类型：1.无认证；2.简单口令认证；3.MD5 认证。默认无认证。
验证字符串	填写认证 key 值。

【示例】



1.使能 SW1 和 SW2 的 ospf 功能。

2.设置 PC 的 IP 和网关：

PC1：ip=192.168.2.100，gateway=192.168.2.1

PC2：ip=192.168.3.100，gateway=192.168.3.1

3.设置 SW 的 3 层接口 IP 和端口的 pvid：

Sw1：端口 1 属于 vlanif1,端口 2 属于 vlanif2,端口默认 access 模式。

vlanif1=192.168.2.1，vlanif2=192.168.4.100，端口 2 的 pvid=2

Sw2：端口 3 属于 vlanif2，端口 4 属于 vlanif3，端口默认 access 模式。

vlanif3=192.168.3.1，vlanif2=192.168.4.200，端口 3 的 pvid=2，端口 4 的 pvid=3

4.分别在 SW1 和 SW2 设置 ospf network

Sw1：router id=1.1.1.1

network 192.168.2.0/24 area 0，network 192.168.4.0/24 area 0

Sw2：router id=2.2.2.2

network 192.168.3.0/24 area 0，network 192.168.4.0/24 area 0

7 网络安全

7.1 防攻击配置

【功能说明】

在“防攻击”页面，您可以启用或禁用忽略 ping 包功能，启用或禁用防范 SYN DOS 攻击，设置 CPU 接收数据包阀值。

【操作路径】

网络安全> 防攻击

【界面说明】

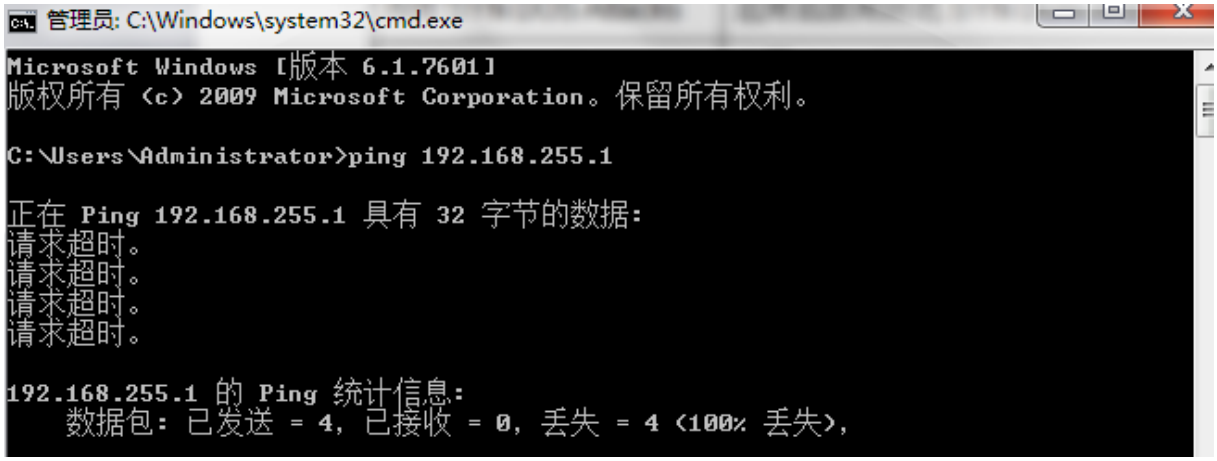
图 7-1 防攻击界面

表 7-1 防攻击主要元素

界面元素	说明
忽略 ping 包	启用或禁用忽略 ping 包功能。
CPU 接收数据包阀值	设置 CPU 接收数据包阀值。

【示例】

开启禁 ping 之后，PC 不能 ping 通交换机，交换机 IP 地址为 192.168.255.1



设置 CPU 伐值之后，每秒只能有 1000 个包上交换机的 CPU，如：ARP 报文。

7.2 MAC 绑定

【功能说明】

在“MAC 绑定”页面，您可以将端口和 MAC 地址绑定起来。MAC 和端口绑定后，该 MAC 的设备只能在该端口通信，不能在其他端口通信，其他 MAC 的设备在该端口通信没有影响。

【操作路径】

网络安全> mac 绑定

【界面说明】

图 7-2 MAC 绑定界面

表 7-2 MAC 绑定界面主要元素

界面元素	说明

MAC	输入需要绑定的 MAC 地址。
Vlan ID	输入 Vlan ID。
端口	选择需要绑定的端口号。

【示例】

配置 MAC 为 68-f7-28-f8-d4-01，VLANID=2（G2 端口的 PVID 设置为 2），端口=G2。主机 PC 不在 G2 不能与外界进行通讯，其它的 PC 在这个端口下，可以进行正常通讯。

7.3 ARP 绑定

【功能说明】

在“ARP 绑定”页面，您可以查看交换机 ARP 信息、配置静态 ARP 的 IP 地址和 MAC 地址、你可以通过扫描端口 arp。

【操作路径】

网络安全> arp 绑定

【界面说明】

图 7-3-1 ARP 全局界面

表 7-3-1　ARP 全局界面主要元素

界面元素	说明
ARP 使能	开启 ARP 绑定功能。

图 7-3-2 ARP 绑定界面

表 7-3-2 ARP 绑定界面主要元素

界面元素	说明
端口	选择绑定 ARP 的端口。
IP 地址	输入静态 ARP 表的 IP 地址。
MAC 地址	输入静态 ARP 表的 MAC 地址。

图 7-3-3　ARP 扫描界面

注：该功能只能在 web 实现，命令行不能实现。

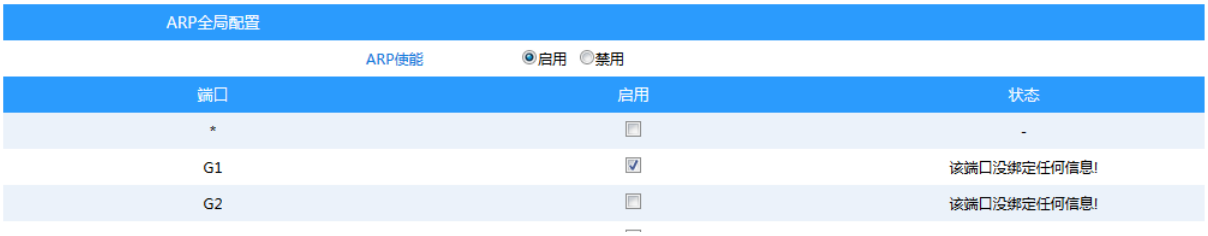
表 7-3-3　ARP 扫描界面主要元素

界面元素	说明

起始地址	输入查询起始地址。
结束地址	输入查询结束地址。

【示例 1】ARP 扫描:

1.使能 ARP 绑定功能，使能 G1 端口。



2.输入需要扫描的开始地址和结束地址，点击扫描，如下图:

3.选择需要绑定的 IP+MAC，点击绑定。可以在 arp 绑定表页面看到扫描的条目已经被静态绑定。

【示例 2】 ARP 绑定:

使能 ARP 绑定，使能端口 G2。

在 G2 口上添加地址 192.168.1.1，MAC：68-f7-28-f8-d4-61，除绑定的 MAC 的相关终端，其他 MAC 相关终端不能通过该端口通信。

7.4 ACL 配置

【功能说明】

ACL，Access Control List，访问控制列表。ACL 是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，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，根据预先设定的操作（允许/禁止通过、限速、重定向、关闭端口等）来进行相应的处理。在“ACL 配置”页面，您可以对数据包的 L2-L4 层的协议字段进行匹配。通过定义时间段可以设置 ACL 规则的生效时间，配置 MAC ACL 和 IP ACL 可以对匹配了 ACL 规则的数据包进行处理。

【操作路径】

网络安全> acl 配置

【界面说明】

图 7-4-1 ACL GROUP 界面

表 7-4-1 ACL GROUP 界面主要元素

界面元素	说明
端口	显示交换机的所有端口。
MAC 访问列表 ID	配置相应端口执行 MAC ACL 组号的匹配规则。
IP 访问列表 ID	配置相应端口执行 IP ACL 组号的匹配规则。

图 7-4-2 MAC ACL 配置界面

表 7-4-2 MAC ACL 配置主要元素

界面元素	说明
组 ID	输入需要配置的 ACL 组号，取值范围为 1-99。
规则 ID	输入规则号，取值范围为 1-127。

行动	选择交换机对满足匹配规则的数据包的处理方式，deny 为丢弃数据包，permit 为转发数据包。
源 MAC 地址	输入规则包含的源 MAC 地址信息。
源 MAC 地址掩码	输入规则包含的源 MAC 地址掩码信息。
目的 MAC 地址	输入规则包含的目的 MAC 地址信息。
目的 MAC 地址掩码	输入规则包含的目的 MAC 地址掩码信息。
VLAN ID	输入规则包含的 VLAN 信息。
COS（802.1p 优先级）	输入规则包含的优先级信息。
以太网类型	输入规则包含的以太网类型。
以太网类型掩码	输入规则包含的以太网类型掩码。

图7-4-3 MAC ACL 表项界面截图

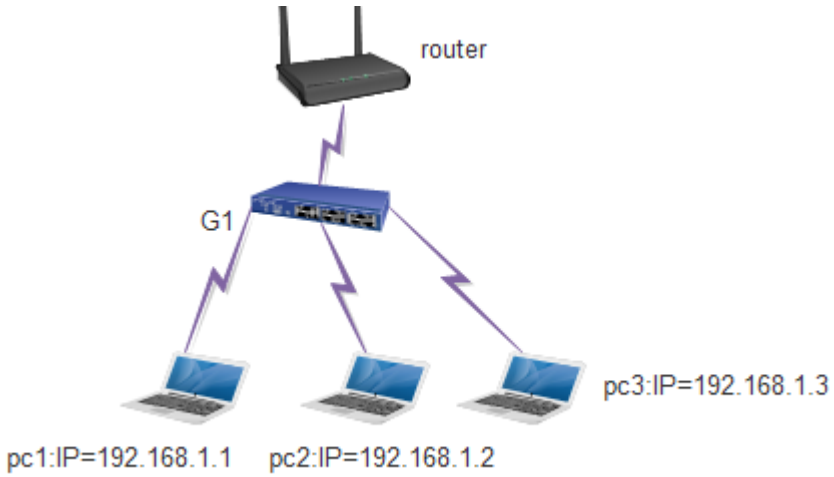
图 7-4-4 IP ACL 配置界面

表 7-4-4　IP ACL 配置主要元素

界面元素	说明
组 ID	输入需要配置的 ACL 组号，取值范围为 100-999。
规则 ID	输入规则号，取值范围为 1-127。
行动	选择交换机对满足匹配规则的数据包的处理方式，deny 为丢弃数据包，permit 为转发数据包。
协议	选择交换机数据传输规则。
源 IP 地址	输入源 IP 地址信息。
源 IP 地址掩码	输入源 IP 地址的掩码，掩码置 1 表示严格匹配。
源端口	输入 TCP/UDP 源端口号。
目的 IP 地址	输入目的 IP 地址信息。
目的 IP 地址掩码	输入目的 IP 地址的掩码，掩码置 1 表示严格匹配。
目的端口	输入 TCP/UDP 目的端口号。
TCP 标志	选择“TCP 标志”。
优先级过滤	选择过滤的优先级。

图 7-4-5 IP ACL table 界面

【示例】



配置 ip rule

组ID	100	范围100-999
规则ID	1 1个组可配置多条acl规则.	范围1-127
行动	拒绝	rule动作
协议	任意	协议类型
源IP	任意 用户定义	
源IP值	192.168.1.1	格式：192.168.0.1
源IP掩码	0.0.0.255	格式：0.0.0.255 (0 代表匹配，bit=1 代表不匹配.)
源端口	任意 用户定义	
源端口值		(范围:0-65535)
目的IP	任意 用户定义	
目的IP值	192.168.1.3	格式：192.168.0.1
目的IP掩码	0.0.0.255	格式：0.0.0.255 (0 代表匹配，bit=1 代表不匹配.)
目的端口	任意 用户定义	
目的端口		(范围:0-65535)

设置组号 100，条目为 1，行为拒绝通过所有协议，源为 192.168.1.1 到目的 192.168.1.3 的报文。

端口	MAC访问列表ID	IP访问列表ID
G1	0	100
G2	0	0
G3	0	0
G4	0	0
G5	0	0
G6	0	0
G7	0	0

在需要开启 G1 端口上设置相应的 ACL 的组（100）保存，即可生效，192.168.1.1 能和 192.168.1.2 通讯不能和 192.168.1.3 通讯。

7.5 802.1X 配置

【功能说明】

802.1X 协议是 IEEE802 LAN/WAN 委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

【操作路径】

网络安全> 802.1X 配置

【界面说明】

在“全局配置”页面，您可以启用或禁用 802.1x 认证功能相关参数。

图 7-5-1 全局配置界面

表 7-5-1 全局配置主要元素

界面元素	说明
模式	使能/去使能 802.1X。
更新	使能/去使能认证更新。
认证更新间隔	认证更新时间间隔设置。默认 3600s。（范围 1-65535s）
静默	使能/去使能静默定时器。
静默定时器	配置静默定时器周期时间。默认 60s。（范围 1-65535s）
保持时间	配置认证保持时间。默认 300s。（范围 1-65535s）

图 7-5-2 端口配置界

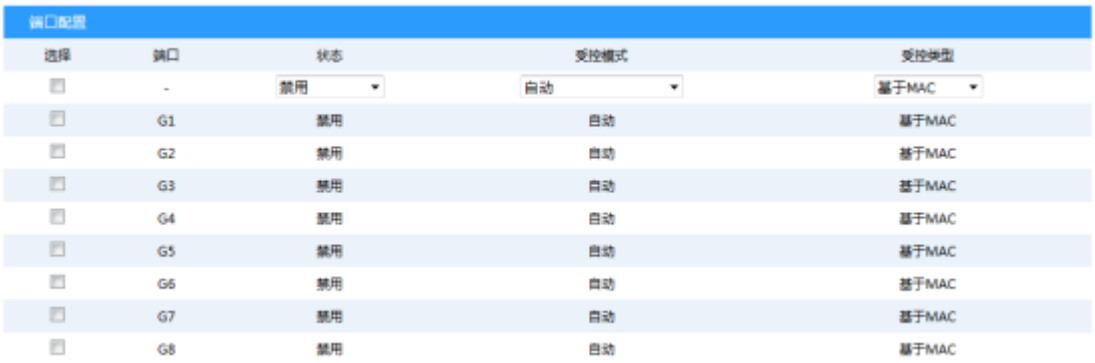


表 7-5-2 端口配置界面主要元素

界面元素	说明
选择	选择端口。
端口	选择开启 802.1X 的端口。
状态	选择是否开启 802.1X。
受控模式	选择认证方式，自动，强制认证通过和强制认证不通过。
受控类型	选择基于通过认证的类型，端口或者 MAC。

【示例】

802.1X 是 AAA 的一个模块，配置举例在 AAA 中共同实现。

7.6 AAA

【功能说明】

AAA 是认证（Authentication）、授权（Authorization）和计费（Accounting）的简称，是网络安全中进行访问控制的一种安全管理机制，提供认证、授权和计费三种安全服务。

AAA 提供的安全服务具体是指：

首先，认证部分提供了对用户的认证。整个认证通常是采用用户输入用户名与密码来进行权限审核。认证的原理是每个用户都有一个唯一的权限获得标准。由 AAA 服务器将用户的标准同数据库中每个用户的标准一一核对。如果符合，那么对用户认证通过。如果不符合，则拒绝提供网络连接。

其次，用户要通过授权来获得操作相应任务的权限。比如，登录系统后，用户可能会执行一些命令来进行操作。这时，授权过程会检测用户是否拥有执行这些命令的权限。

简单而言，授权过程是一系列强迫策略的组合，包括：确定活动的种类或质量、资源或者用户被允许的服务有哪些。授权过程发生在认证上下文中，一旦用户通过了认证，他们也就被授予了相应的权限。

最后，计费这一过程将会计算用户在连接过程中消耗的资源数目。这些资源包括连接时间或者用户在连接过程中的收发流量等等。可以根据连接过程的统计日志、用户信息、授权控制、账单、趋势分析、资源利用以及容量计划活动来执行计费过程。

【操作路径】

网络安全> AAA

【界面说明】

图 7-6-1 Radius 配置界面

表 7-6-1 Radius 配置界面主要元素

界面元素	说明
认证配置	
使能	选择认证方式。
主 IP	输入主 radius 服务器的地址。
从 IP	输入从 radius 服务器的地址。
认证端口	输入认证端口。
认证密钥	输入交换机与服务器共享的密码。
计费配置	
使能	开启计费。

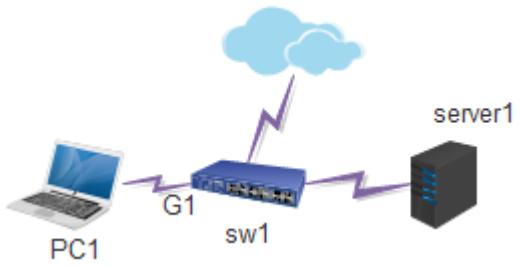
实时计费	开启实时计费。
实时计费时间	设置服务器更新数据时间。
主 IP	填写主计费服务器地址。
从 IP	填写从计费服务器地址。
计费端口	显示计费端口号。
计费密钥	输入交换机与服务器共享的密码。

图 7-6-2 本地账号界面

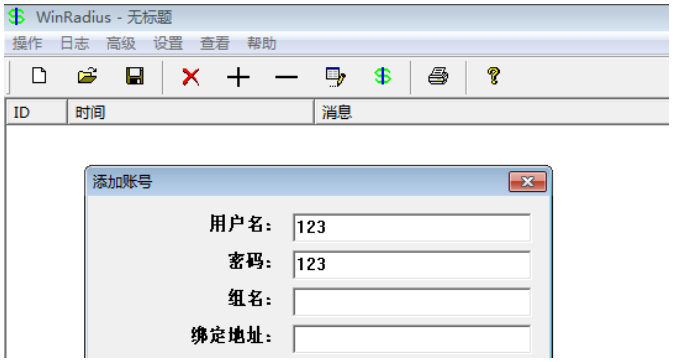
表 7-6-2 本地账号界面主要元素

界面元素	说明
用户名	设置本地认证帐号。
密码	设置本地认证密码。
端口	设置帐号在哪个端口登录。
MAC	设置帐号绑定的 MAC 地址。

【示例】



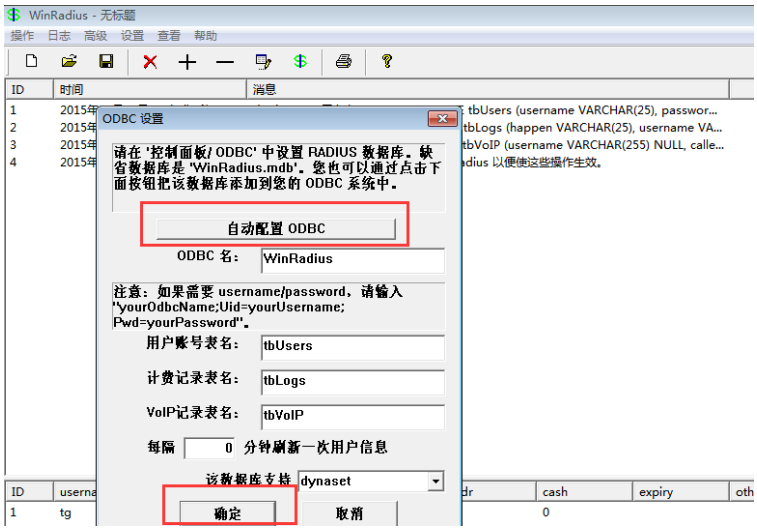
1.配置 server1=192.168.2.96。打开 winradius，在操作--->添加帐号菜单添加帐号和密码；



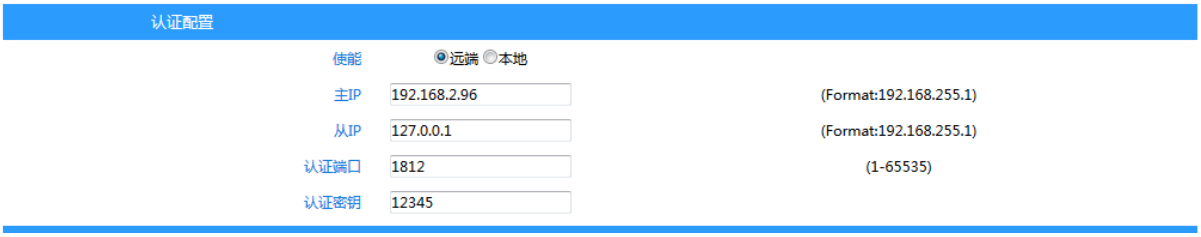
在高级中选择创建 radius 表来创建 raidus，并重启 radius。

在设置--->系统设置中设置 NAS 密钥 12345

打开设置--->数据库设置，点击“自动配置 ODBC”，点击确认。关闭 WinRadius，重新打开。



2. 在 sw1 上设置 AAA 参数。使能 remote radius 功能，primary IP=192.168.2.96，Auth key=12345 和 NAS 密钥一致。其他默认。



使能 802.1X 功能。配置端口 G1 使能，control type 为基于端口。

PC1 打开 802.1X 认证功能。启用 MD5 值认证。

拔插 PC1 直连 G1 口的网线，客户端弹出认证登陆界面，输入用户名，密码，认证通过之后可以正常访问网络。

计费：

a. 以上配置不变，使能计费功能，primary ip =192.168.2.96, accounting key=12345, 其他默认。

如下所示：

b. 重新认证登陆后，Radius 开始计时。

本地认证：

a. 使能本地认证，在本地认证页面设置账户如下：

b. 用户名密码都为 123，绑定端口 G1 和 MAC（MAC 为终端 PC1 的 MAC）

c. 使能 802.1X 功能。配置端口 G1 使能，受控类型为基于端口。

d. 插拔网线后可以重新认证登陆。

7.7 端口隔离

【功能说明】

在“端口隔离”页面，您可以配置端口的相互隔离。

【操作路径】

网络安全> 端口隔离

【界面说明】

图 7-7　端口隔离界面

端口名称	端口隔离	端口名称	端口隔离
G1	☐	G2	☐
G3	☐	G4	☐
G5	☐	G6	☐
G7	☐	G8	☐
G9	☐	G10	☐
G11	☐	G12	☐
G13	☐	G14	☐
G15	☐	G16	☐
G17	☐	G18	☐

表 7-7　端口隔离界面主要元素

界面元素	说明
端口	显示各个端口号。
端口隔离	勾选相应“端口隔离”复选框，表示相应端口将被隔离。

【示例】

端口名称	端口隔离	端口名称	端口隔离
G1	☑	G2	☑
G3	☐	G4	☐
G5	☐	G6	☐
G7	☐	G8	☐
G9	☐	G10	☐
G11	☐	G12	☐

开启端口隔离的两个端口不能进行通讯，隔离端口与其他端口通讯正常。

7.8 风暴抑制

【功能说明】

在“风暴抑制”页面，您可以配置各个端口的广播包、组播包和未知单播包的速率，达到端口抑制功能。

【操作路径】

网络安全> 风暴抑制

【界面说明】

图 7-8 风暴抑制界面

表 7-8 风暴抑制界面主要元素

界面元素	说明
端口	显示各个端口号。
广播	配置相应端口的广播抑制速率。单位：pps
组播	配置相应端口的组播抑制速率。单位：pps
未知单播	配置相应端口的未知单播抑制速率。单位：pps

【示例】

端口	广播（pps）(0-10000000之间的整数)	组播（pps）(0-10000000之间的整数)	未知单播（pps）(0-10000000之间的整数)
*	0	0	0
G1	1000	0	0
G2	0	0	0
G3	0	0	0
G4	0	0	0
G5	0	0	0
G6	0	0	0

在 G1 口上做广播限速广播限速 1000 个包每秒。

A	B	C	D
Name	192.168.2.127:01.07	192.168.2.127:01.08	192.168.2.127:01.0
Link State	Link Up	Link Up	Link Up
Line Speed	1000 Mbps	1000 Mbps	1000 Mbps
Duplex Mode	Full	Full	Full
Frames Sent	407,217,625	0	0
Frames Sent Rate	1,488,095	0	0
Valid Frames Received	106	273,755	273,748
Valid Frames Received Rate	0	1,000	1,000
Bytes Sent	26,061,928,000	0	0
Bytes Sent Rate	95,238,050	0	0

07 对应的是 G1，08 对应的是 G2，09 对应 G3，G2 口是对照端口，先用 07 发送广播包 G3 口收到的广播包为 1000 个每秒。

A	B	C	D
Name	192.168.2.127:01.07	192.168.2.127:01.08	192.168.2.127:01.0
Link State	Link Up	Link Up	Link Up
Line Speed	1000 Mbps	1000 Mbps	1000 Mbps
Duplex Mode	Full	Full	Full
Frames Sent	0	16,613,287	0
Frames Sent Rate	0	1,488,094	0
Valid Frames Received	16,618,797	4	16,616,024
Valid Frames Received Rate	1,488,091	0	1,488,091
Bytes Sent	0	1,063,250,368	0
Bytes Sent Rate	0	95,238,048	0

在用 G2 口发广播包，G3 口收到的广播包为 1488095。

7.9 ERPS-Ring 配置

【功能说明】

环路保护功能功能方面类似 STP，但环路保护没有 IEEE 标准，属于私有协议，配置使用简单，对于简单的环网拓扑和普通网络业务，在线路备份方面的优势也很明显。在“ERPS-Ring 配置”页面，您可以启用或禁用 ERPS-Ring 功能，添加多个 ERPS-Ring 并设置相关参数。

【操作路径】

网络安全> erps-ring 配置

【界面说明】

图 7-9 ERPS-Ring 全局配置界面

表 7-9 ERPS-Ring 配置界面主要元素

界面元素	说明
使能	启用或禁用 ERPS-Ring 功能。
传输时间	配置传输时间。默认 500ms，范围 500-5000ms
端口	显示交换机端口号。
使能	勾选“使能”复选框，表示启用相应端口。
行为	选择相应端口的行为。默认丢弃报文。
主检测模式	选择相应端口的主检测模式，disable 关闭主检测模式，使能开启主监测模式。

【示例】

所有交换机开启 ERPS-Ring。其中一台开启主监测模式，两个口都要开启。

在其中一台交换机上，在系统状态下的 ERPS-Ring 状态可以查看到如下图情况，有一个端口是被堵塞了。

端口	行动	传输报文	端口状态	Loop
G1	丢弃报文	允许	Up	-
G2	丢弃报文	允许	Disabled	Loop
G3	丢弃报文	禁止	Down	-
G4	丢弃报文	禁止	Down	-
G5	丢弃报文	禁止	Down	-
G6	丢弃报文	禁止	Down	-
G7	丢弃报文	禁止	Down	-
G8	丢弃报文	禁止	Down	-
G9	丢弃报文	禁止	Down	-

7.10 ERPS-E 配置

【功能说明】

ERPS（Ethernet Ring Protection Switching）：以太网多环保护技术，协议标准为 ITU-TG.8032 多环标准 。ERPS 追求更高性能、更加安全是网络永远的发展方向，以太环网技术成为二层网络中重要的冗余保护手段。

在二层网络中，对于网络可靠性一般采用 STP 协议，还有上节提到的环路保护协议，STP 协议是由 IEEE 开发的一种标准的环网保护协议，已得到广泛应用，但实际应用中受到网络大小的限制，收敛时间受网络拓扑影响。STP 一般收敛时间为秒级，网络直径较大时收敛时间更长，采用 RSTP/MSTP 虽然可以减少收敛时间，达到毫秒级，但是对于 3G/NGN 语音等高服务质量要求的业务仍然不能满足要求。为更大缩短收敛时间，消除网络尺寸的影响，ERPS 协议应运而生。

ERPS 是一个专门应用于以太网环的链路层协议，它在以太网环中能够防止数据环路引起的广播风暴；当以太网环上一条链路断开时，能迅速启用备份链路以恢复环网上各个节点之间的通信。和 STP 协议相比，ERPS 协议具有拓扑收敛速度快（低于 20ms）和

收敛时间与环网上节点数无关的特点。环路保护功能功能方面类似 STP、erps，但环路保护没有 IEEE 标准，属于私有协议，配置使用简单，收敛时间也是秒级，对于简单的环网拓扑和普通网络业务，在线路备份方面的优势也很明显。

【操作路径】

网络安全>erps-e 配置

【界面说明】

图 7-10-1 ERPS-E settings 界面

表 7-10-1 ERPS-E settings 界面主要元素

界面元素	说明
使能 ERPS-E	启用或禁用 ERPS-E 功能。

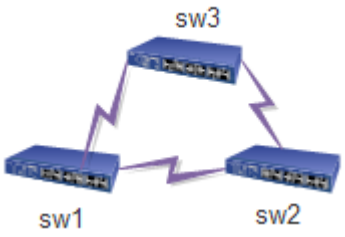
图 7-10-2 节点配置界面

表 7-10-2 Node settings 界面主要元素

界面元素	说明
使能 ERPS-E	启用或禁用 ERPS-E 功能。
ERPS ID	ERPS 域标识，用整数表示，范围是 1-24。

角色	选择节点角色。1.master，2.transit。
主端口	选择主端口。
从端口	选择从端口。
控制 vlan id	配置控制 vlan ID，范围 1-4094，默认 3001。
Wtr 定时器	配置 wtr-time 定时器的时间，范围 1-12m，默认 1m。
Guard 定时器	配置 Guard time 定时器的时间，范围 100-2000ms，默认 500ms。

【示例】



启用 ERPS-E 功能；

配置 ERPS ID=1，Role=master，main 端口=G19，secondary 端口=G20，其他默认。

7.11 IP 源保护

【功能说明】

通过 IP 源保护功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了端口的安全性。在“IP 源保护”配置页面，您可以启用或禁用 IP 源保护功能。

【操作路径】

网络安全>IP 源保护

【界面说明】

图 7-11-1 IP 源保护界面

表 7-11-1 全局配置界面主要元素

界面元素	说明
模式	启用或禁用全局 IP 源保护功能。
端口	显示端口号。
模式	启用或禁用端口的 IP 源保护功能。
动态客户端最大数量	允许通过的动态客户端最大数量，可选 0、1、2、无限制。
端口绑定数	显示当前绑定数量。

图7-11-2 动态表界面

注：该功能只能在 web 实现，命令行不能实现。

表 7-11-2 动态表界面主要元素

界面元素	说明
Search	搜索相应的动态表条目。
Dynamic To Static	将动态表条目转为静态表条目。

图7-11-3 静态表界面

表 7-11-3 静态表界面主要元素

界面元素	说明
端口	选择要绑定的端口。
Vlan ID	填写端口所属的 Vlan。
IP 地址	填写要绑定的终端 IP 地址。
子网掩码	填写要绑定的终端子网掩码。
MAC 地址	填写要绑定的终端 MAC 地址。

【示例】

开启 IP 源保护功能，选择需要开启源保护的端口，并且选择绑定的数量。

在 G1 口上绑定 VLAN2，IP 地址是 192.168.222.231，MAC 是 68-f7-28-f8-d4-61 的 PC。这个 PC 只能在 G1 口才能进行通讯，不在 G1 端口则不能通讯，别的 PC 在这个端口不能进行正常通讯。


IP源保护静态表
端口
G1
Vlan ID
2
IP 地址
192.168.222.231
例如:192.168.1.1
子网掩码
255.255.255.255
例如:255.255.0.0
MAC 地址
68-f7-28-f8-d4-61
例如：01-02-03-04-05-06
添加
删除
序号
端口
VLAN ID
IP 地址
子网掩码
MAC 地址
-
-
-
-
-
G1
2
192.168.222.231
255.255.255.255
68-f7-28-f8-d4-61
删除
共 1 条
20条/页
1/1页
1
Go
一键删除

8 网络管理

8.1 HTTP 配置

【功能说明】

在“HTTP 配置”页面，您可以启用或关闭 HTTP 和 HTTPS 功能。

【操作路径】

网络管理 > HTTP 配置

【界面说明】

图 8-1 HTTP 配置界面

表 8-1 HTTP 配置界面主要元素

界面元素	说明
HTTP	勾选“启用”复选框，则表示开启 http 功能。 可通过“http://192.168.255.1”登录交换机 WEB 页面，否则无法通过 http 登录。
HTTPS	勾选“启用”复选框，则表示开启 https 功能。 可通过“https://192.168.255.1”登录交换机 WEB 页面，否则无法通过 https 登录。

8.2 SNMP 配置

【功能说明】

SNMP 是目前 UDP/IP 网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。

SNMP 网络元素分为 NMS 和 Agent 两种：

NMS（Network Management Station）是运行 SNMP 客户端程序的工作站，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 是驻留在设备上的一个进程，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 也会通知 NMS。

NMS 是 SNMP 网络的管理者，Agent 是 SNMP 网络的被管理者。NMS 和 Agent 之间通过 SNMP 协议来交互管理信息。

SNMP 提供四种基本操作：

Get 操作：NMS 使用该操作查询 Agent 的一个或多个对象的值。

Set 操作：NMS 使用该操作重新设置 Agent 数据库（MIB，Management Information Base）中的一个或多个对象的值。

Trap 操作：Agent 使用该操作向 NMS 发送报警信息。

Inform 操作：NMS 使用该操作向其他 NMS 发送报警信息。

SNMP 的协议版本：

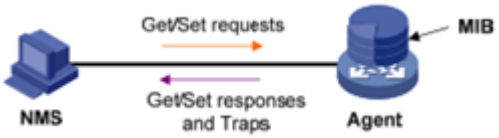
目前，设备的 SNMP Agent 支持 SNMP v2c 版本，兼容 SNMP v1 版本。

SNMP v1 采用团体名（Community Name）认证。团体名用来定义 SNMP NMS 和 SNMP Agent 的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP NMS 对 SNMP Agent 的访问。

SNMP v2c 也采用团体名认证。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：它提供了更多的操作类型（GetBulk 和 InformRequest）；它支持更多的数据类型（Counter64 等）；它提供了更丰富的错误代码，能够更细致地区分错误。

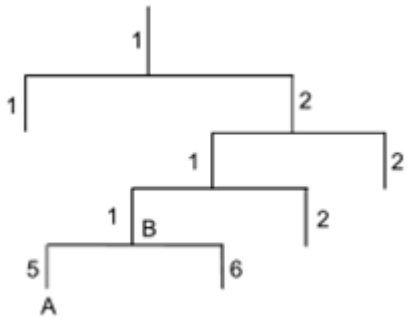
MIB 简介：

任何一个被管理的资源都表示成一个对象，称为被管理的对象。MIB（Management Information Base，管理信息库）是被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 Agent 都有自己的 MIB。NMS 根据权限可以对 MIB 中的对象进行读/写操作。NMS、Agent 和 MIB 之间的关系如下图所示：



MIB 是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别（OID）。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，这串数字是被管理对象的 OID（Object Identifier，对象标识符）。



【操作路径】

网络管理 > SNMP 配置

【界面说明】

图 8-2 SNMP 配置界面

表 8-2 SNMP 界面主要元素

界面元素	说明
Snmp 系统配置	
模式	SNMP 使能/去使能。
版本	SNMP 支持的版本 V1，V2C。
Read community	访问网管的共用体名称，权限为可读，缺省为 public。
Write community	访问网管的共用体名称，权限为可写，缺省为 private。
Trap 配置	

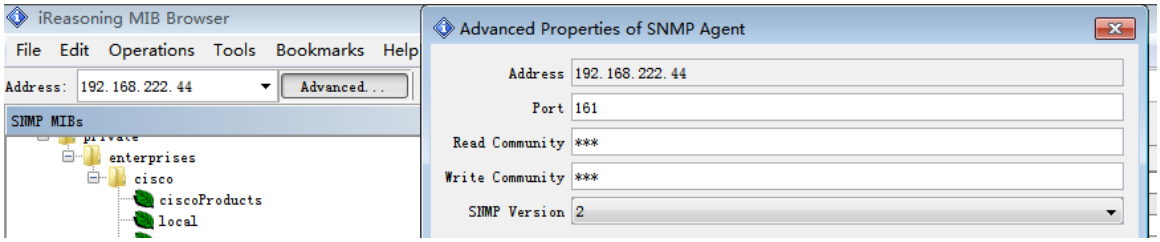
Mode	Trap 使能/去使能。
Trapv1 Receiver	填写 SNMPV1 版本陷阱接收地址。
Trapv2 Receiver	填写 SNMPV2 版本陷阱接收地址。

【配置说明】

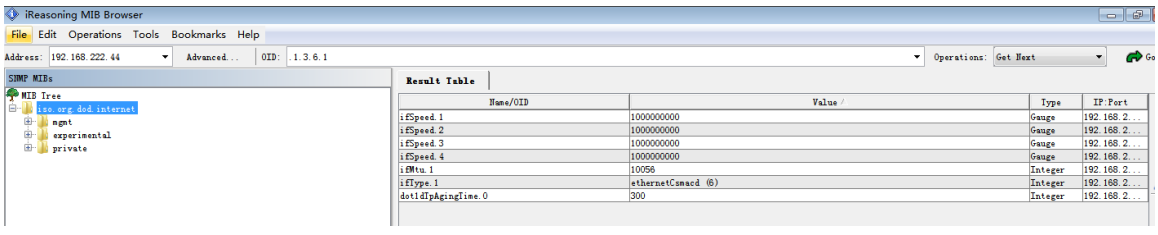
1. SNMP 配置使能，版本默认 V1，V2C，读写设置均填写 111；
2. 使能 trap，在 trapv1 中输入 192.168.222.96(管理系统端的 ip，我们的 trap 目前只有 coldstart,linkup,linkdown 三种，只需配置 trapv1 即可)，点击保存。

配置参考结果如下图：

3. SNMP 使用 MIBbrowser，加载相应的 mib，填写被管理设备 IP，读写设置，版本号。如下图：



4. 如下图，右键单击 iso.org.dod.internet,点击 work,在信息显示页面就会显示相关信息。



9 系统维护

9.1 重启

【功能说明】

在“重新启动”页面，您可以重新启动交换机。

【操作路径】

系统维护 > 重新启动

【界面说明】

图 9-1 重启设备界面

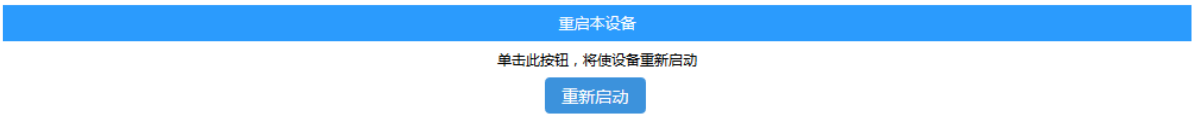


表 9-1 重启设备界面主要元素

界面元素	说明
重新启动	单击“重新启动”，即可重新启动交换机。

9.2 恢复出厂配置

【功能说明】

在“恢复出厂”页面，您可以将交换机恢复出厂配置。

【操作路径】

系统维护 >恢复出厂

【界面说明】

图 9-2 恢复出厂界面

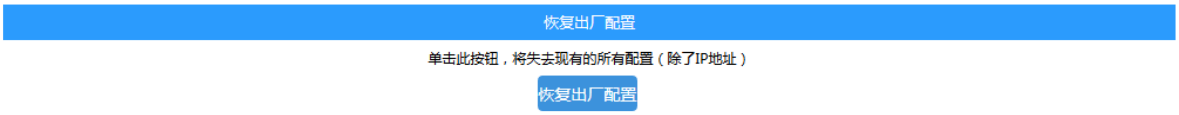


表 9-2 恢复出厂界面主要元素

界面元素	说明
恢复出厂配置	单击“恢复出厂配置”按钮，即可将交换机恢复出厂配置。

除 IP 地址以外，其他均可恢复出厂配置。
交换机前面板有 RESET 键，您只需用针状物长按 5 秒即可恢复出厂配置。

9.3 在线升级

【功能说明】

在“在线升级”页面，您可以实现交换机软件在线升级功能。

【操作路径】

系统维护 >在线升级

【界面说明】

图 9-3 在线升级界面

表 9-3 在线升级界面主要元素

界面元素	说明
升级文件路径	单击“选择文件”，选择您准备好的软件升级文件，单击“上传”，即可实现交换机软件在线升级。

软件升级过程中，请不要点击或配置交换机的其它 WEB 页面，更不要重启交换机；否则会导致软件升级失败，造成交换机系统崩溃等现象。

9.4 配置管理

【功能说明】

在“配置管理”页面，您可以下载交换机当前配置文件，也可以上传已有配置到交换机。

【操作路径】

系统维护 >配置管理

【界面说明】

图 9-4-1 配置管理界面

表 9-4-1 配置 管理界面主要元素

界面元素	说明
文件路径	单击“下载”，即可下载交换机当前配置文件。 单击“选择文件”，选择您准备好的配置文件，单击“上传”，即可上传已有配置到交换机。

配置文件上传过程中，请不要点击或配置交换机的其它 WEB 页面，更不要重启交换机；否则会导致配置文件上传失败，造成交换机系统崩溃等现象。

图 9-4-2 查看启动配置界面

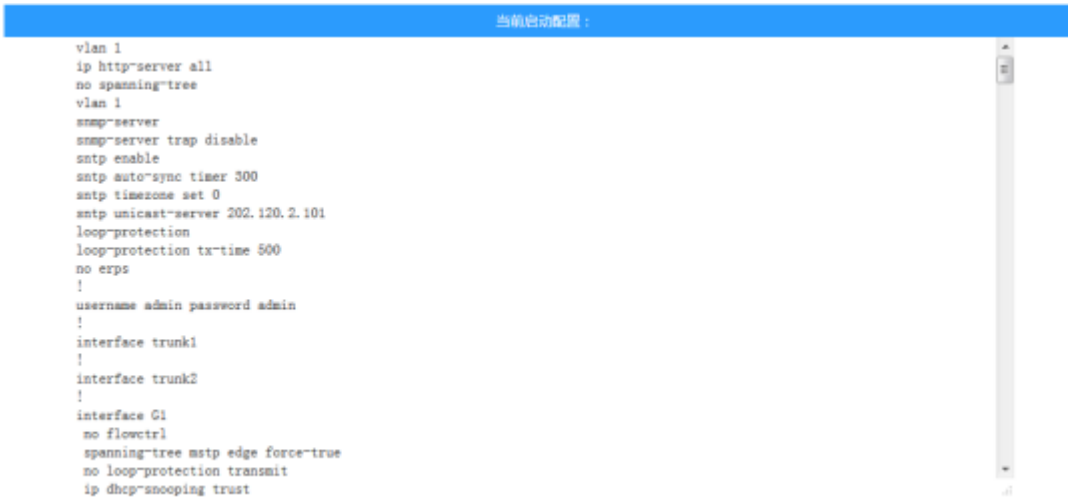


表 9-4-2 查看启动配置界面主要元素

界面元素	说明
当前启动配置	显示交换机当前启动配置信息。

9.5 Ping 测试

【功能说明】

Ping 诊断和普通计算机上的 ping 命令一样，都是用来检测网络中两个节点之间的链路是否连通。两者区别在于，两台普通计算机之间的 ping 命令是为了检测物理链路连接是否正常，而交换机的 ping 检测功能是为了方便网络管理员检测局域网中的网络设备是否已经断开连接，定位网络故障。

【操作路径】

系统维护 > ping 测试

【界面说明】

图 9-5 ping 测试界面

表 9-5 ping 测试界面主要元素

界面元素	说明
IP 地址	输入 IP 地址

10 常见故障诊断

表 10-1 常见故障诊断列表说明

故障现象	可能的故障原因	解决方法
通电后所有指示灯均不亮	电源连接错误或供电不正常	检查电源线和插座
LINK 指示灯不亮	● 网线损坏或连接不牢 ● 网线类型错误或网线过长，超出允许范围	更换网线
网络能通，但传输速度变慢，有丢包现象	交换机与网络终端以太网口工作模式不匹配	设置以太网口工作模式使其匹配或将其设为自适应工作模式
在某一口可通，将网线换到其他口时则不通	将网线换到其他网口时，如果此端口所连接的设备没有发送数据，交换机将学不到新地址，因此此端口会暂时不通	120 秒后交换机的地址会自动更新，此现象会自动消失；或者从此网口发送数据也会使交换机立即更新其地址表
所有 ACT 指示灯闪烁，网络速率变慢	广播风暴	● 检查网络连接是否成环路，合理配置网络 ● 检查是否有站点发送大量的广播包
正常工作一段时间后停止工作	● 电源不正常 ● 交换机过热	● 检查电源是否有接触不良，电压过低或过高 ● 检查周围环境，通风孔是否畅通，交换机风扇是否工作正常