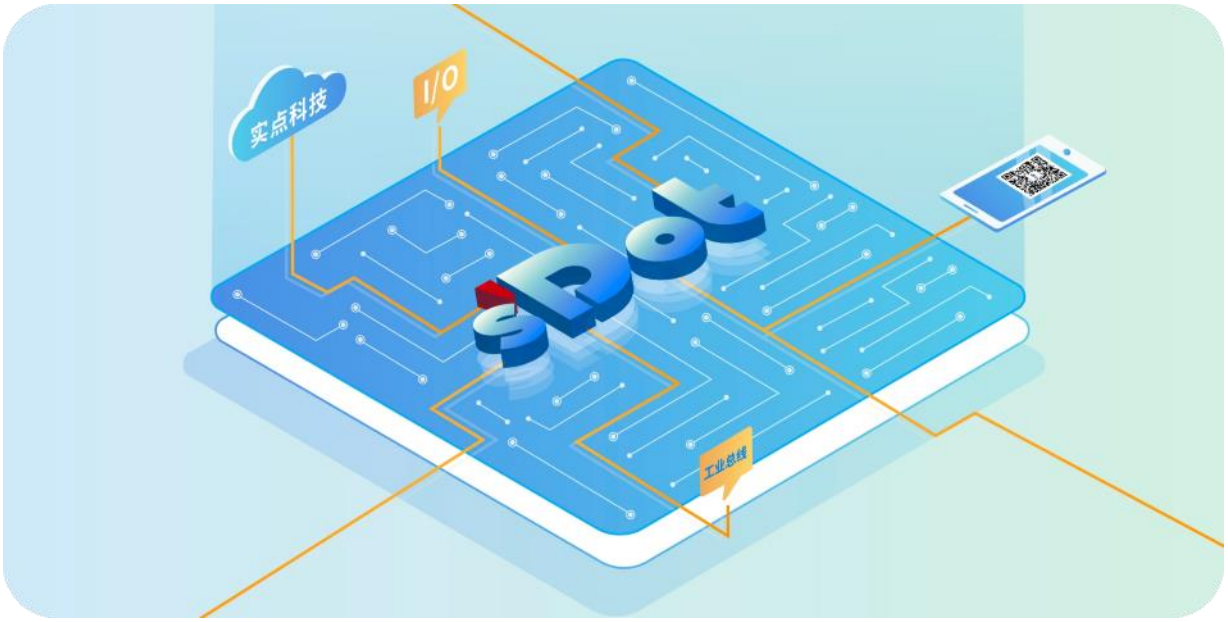



# 全二层管理环网交换机软件使用手册

南京实点电子科技有限公司

**商标声明**

sDot 和其它实点商标均为南京实点电子科技有限公司的商标。

本文档提及的其它所有商标或注册商标，由各自的所有人拥有。

**注意**

您购买的产品、服务或特性等应受实点公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，实点公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

南京实点电子科技有限公司
地址：江苏省南京市江宁区隐龙路 9-1 号 40 栋
邮编：211106
电话：4007788929
网址：http://www.solidotech.com

# 目录

# 第一章 配置准备

本章对配置准备进行详细的描述，主要包括以下内容：

- WEB 登陆界面
- WEB 配置界面
- 当前设置信息

## 1.1 WEB 登录界面

系统的缺省 IP 是 192.168.1.6。在登陆之前，请确保以下几点：

- 管理PC的IP地址与交换机IP地址在同一网段内，否则无法访问交换机管理IP地址
- 设确保PC与交换机连接的端口为非聚合端口
- WEB浏览器为IE8以上版本

**登录步骤**

1. 在 PC 上打开浏览器。

2. 在地址栏中输入设备 IP 地址（默认为 192.168.1.6），按回车进入 Web 登录界面，如图 1.1。

2. 在 Web 登录界面输入用户名和密码。

3. 在 Web 登录界面选择界面语言。

4. 单击<登录>，进入 WEB 配置界面。

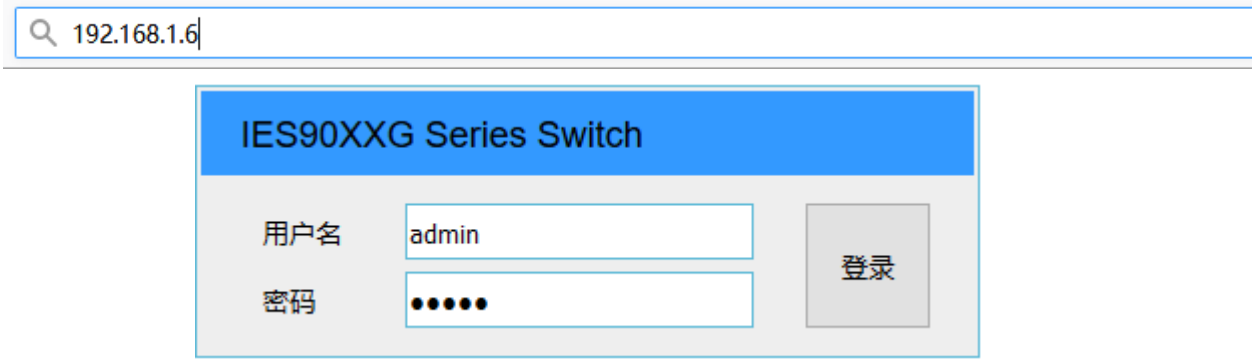



**图 1.1 设备 Web 登录界面**

Web 登录界面说明，见表 1.1。

**表 1.1 Web 登录界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |

| | |
|---|---|
| 用户名 | 输入需要登录的用户名，系统默认用户名为：admin |
| 密码 | 输入需要登录的用户的登录密码，系统默认用户的密码为：admin |
| 语言 | 界面语言显示方式：<br>● Auto：根据系统语言自动选择显示方式（默认）；<br>● Chinese：选择中文显示方式；<br>● English：选择英文显示方式。<br>注：目前只支持中文和英文两种语言 |

# 1.2 WEB 配置界面

## 1.2.1 WEB 配置界面组成

Web 配置界面的组成，如图 1.2。

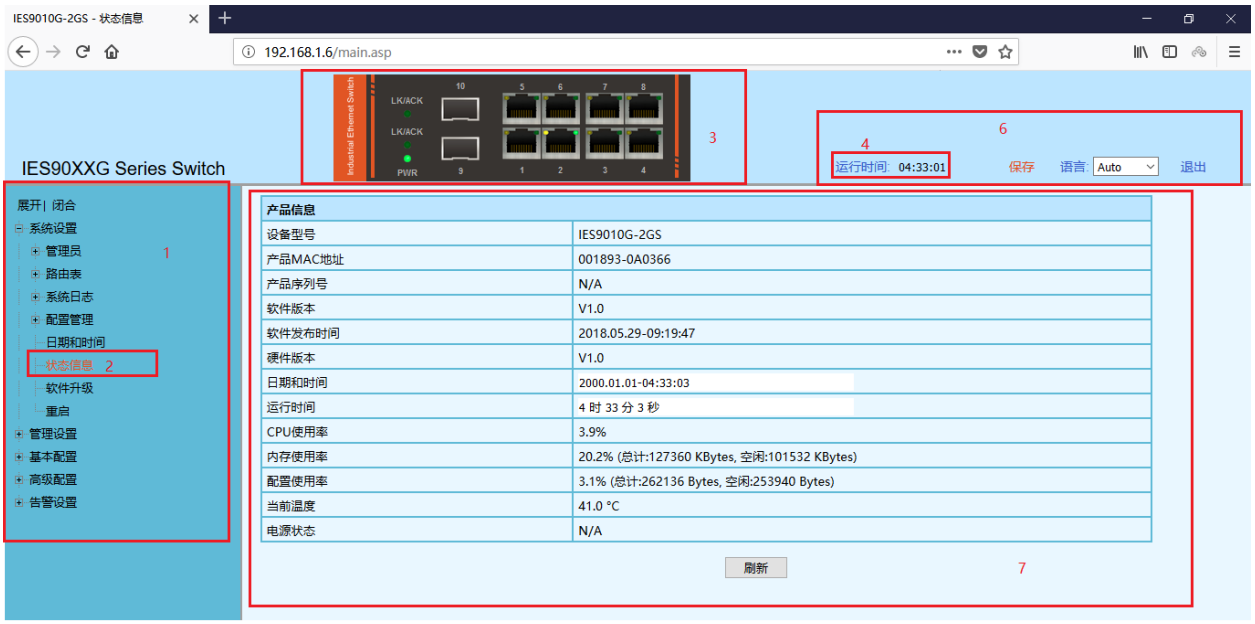



**图 1.2 设备 Web 配置界面**

1.导航栏 2.选中的页面 3.设备面板 4.设备运行时间

5.当前设备型号 6.常用功能 7.当前配置页面

Web 配置界面各个部分说明，如表 1.2

| 配置界面 | 说明 |
|---|---|
| 导航栏 | 即菜单栏，可在这找到并跳转到任意一个已实现的配置页面。 |
| 选中的页面 | 当前配置页面在导航栏中的位置。 |

| | |
|---|---|
| 设备面板 | 显示设备上各个接口的启用和连接状态。 |
| 设备运行时间 | 显示设备上电后的运行时间。 |
| 当前设备型号 | 显示当前设备的型号。 |
| 常用功能 | ● 多语言：可选择界面语言显示方式；<br>● 保存：将当前配置保存到配置文件中（颜色不变表示没有需要保存的配置，颜色闪烁表示有需要保存的配置）；<br>● 退出：退出Web配置界面； |
| 当前配置页面 | 当前要配置的主页面。 |

**表 1.2 Web 配置界面说明**

### 1.2.2 设备面板

通过设备面板图可以查看到设备各个接口的启用和连接状态，如图 1.3。

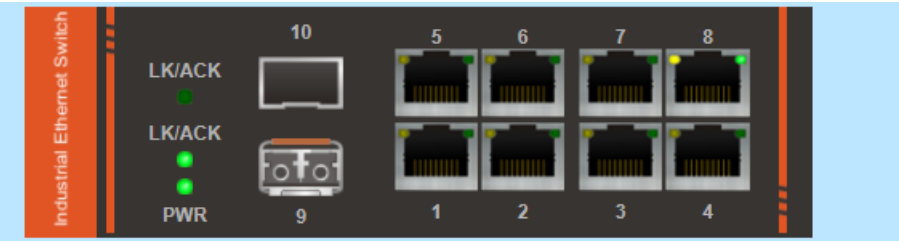



**图 1.3 设备面板图**

设备面板图上接口说明，见表 1.3。

**表 1.3 设备面板接口说明**

| 接口 | 说明 |
|---|---|
|  | Copper接口，已启用、已连接。 |
|  | Copper接口，已启用、未连接。 |
|  | Fiber接口，已启用、已连接。 |
|  | Fiber接口，已启用、未连接。 |

### 1.2.3 常用按钮

设备配置界面的常用按钮说明，见表 1.4。

**表 1.4 设备配置界面的按钮说明**

| 按钮 | 说明 |
| --- | --- |
| 展开 | 展开按钮，展开导航栏所有页面或展开所有端口信息。 |
| 闭合 | 闭合按钮，收起导航栏所有页面或收起所有端口信息。 |
| 应用 | 应用按钮，配置应用到系统中。 |
| 刷新 | 刷新按钮，刷新当前界面的信息。 |
| 添加 | 添加按钮，新添加当前页面中的一个项目。 |
| 修改 | 修改按钮，修改当前页面中选中的一个项目。 |
| 删除 | 删除按钮，删除当前页面中选中的一个项目。 |
| 上一页 | 上一页按钮，返回到上一个页面。 |
| 下一页 | 下一页按钮，进入到下一个页面。 |
| 跳转到 | 跳转到按钮，跳转到指定页面。 |
| 首页 | 首页按钮，跳转到第一个页面。 |
| 尾页 | 尾页按钮，跳转到最后一个页面。 |
| 应用 | 应用按钮，当前配置应用到系统中。 |
| 取消 | 取消按钮，取消当前配置。 |
| 清除 | 清除按钮，清除指定端口显示信息。 |
| 保存 | 保存按钮，保存系统配置信息。 |
| 退出 | 退出按钮，退出当前界面，重新回到登录界面。 |

### 1.2.4 保存配置

1．当前配置完成后，点击[应用]，配置应用到系统中。保存在内存中而并不是真正保存到配置文件中。如果未按[保存]，则设备掉电或重启后，上次保存配置操作之后的配置将会丢失。

2．当前所有配置完成后，请单击[保存]。保存到配置文件中的配置，在设备掉电或重

启后不会丢失。

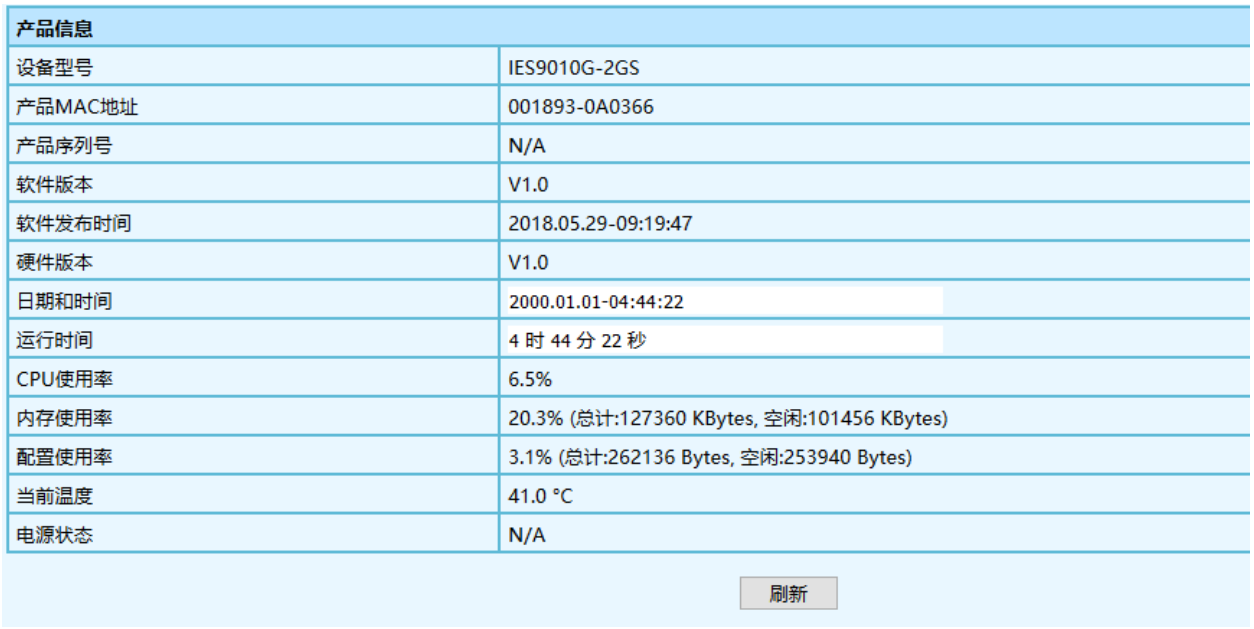
### 1.2.5 退出 Web 配置界面

1. 当在 Web 界面完成配置后，请先按[保存]，以免配置丢失。然后单击[退出]可退出 Web 配置界面。
2. 直接关闭浏览器无法退出 Web 配置界面。下次登录时如果用户未超时将直接进入 Web 配置界面。

## 1.3 当前设备信息

**配置步骤**

在[产品信息]界面中显示了当前设备的基本信息和设备系统的运行状态信息，如图 1.4 所示。



| 产品信息 | |
|---|---|
| 设备型号 | IES9010G-2GS |
| 产品MAC地址 | 001893-0A0366 |
| 产品序列号 | N/A |
| 软件版本 | V1.0 |
| 软件发布时间 | 2018.05.29-09:19:47 |
| 硬件版本 | V1.0 |
| 日期和时间 | 2000.01.01-04:44:22 |
| 运行时间 | 4 时 44 分 22 秒 |
| CPU使用率 | 6.5% |
| 内存使用率 | 20.3% (总计:127360 KBytes, 空闲:101456 KBytes) |
| 配置使用率 | 3.1% (总计:262136 Bytes, 空闲:253940 Bytes) |
| 当前温度 | 41.0 °C |
| 电源状态 | N/A |

刷新

图 1.4 产品信息界面

**配置项说明**

[状态信息]界面的设备信息说明。

表 1.4 [产品信息]界面的信息说明

| 配置项 | 说明 |
|---|---|
| 设备型号 | 当前设备型号，如IES9010G-2GS。 |
| 设备MAC地址 | 当前设备MAC地址。 |

| | |
|---|---|
| 产品系列号 | 当前设备的产品系列号。 |
| 软件版本 | 当前设备运行的软件版本。 |
| 软件发布时间 | 当前设备运行的软件的发布时间。 |
| 硬件版本 | 当前设备的硬件版本。 |
| 日期和时间 | 当前设备系统的时间 |
| 运行时间 | 当前设备系统的运行时间。 |
| CPU使用率 | 当前设备系统的CPU使用率。 |
| 内存使用率 | 当前设备系统的内存使用率。 |
| 配置使用率 | 当前设备系统的配置空间占用率。 |

# 第二章 端口

本章对端口配置进行详细的描述，主要包括以下内容：

- 端口配置
- 端口统计

## 2.1 端口配置

### 配置步骤

1．在导航栏中选择[基本配置/端口/状态和设置]，进入[状态和设置]界面。

2．[状态和设置]界面（如图 2.1）显示了每个端口的运行状态与配置信息。

| | 运行状态 | | | | 管理状态 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 端口 | 连接状态 | 端口类型 | 速率 | 双工模式 | 管理状态 | 速率 | 双工模式 | 流控 | 设置 |
| GE/1 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/2 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/3 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/4 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/5 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/6 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/7 | ✖ | 电口 | 10M | 半双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/8 | ✔ | 电口 | 100M | 全双工 | 开启 | 自动 | 自动 | 关闭 | 修改 |
| GE/9 | ✔ | 光口 | 1000M | 全双工 | 开启 | Fiber-Auto | 全双工 | 关闭 | 修改 |
| GE/10 | ✖ | 光口 | 10M | 半双工 | 开启 | Fiber-Auto | 全双工 | 关闭 | 修改 |

刷新

**图 2.1 端口状态和设置界面**

**表 2.1 [端口配置]界面的配置项说明**

| 值 | 描述 |
|---|---|
| 端口 | 端口的名称序号 |
| 连接状态 | ✔ 表示端口目前处于连接的状态<br>✖ 表示端口目前处于断开或未连接的状态 |
| 端口类型 | 当前端口的类型，电口(Copper)或者光口(Fiber) |
| 速率 | 端口当前工作的速率，未连接的端口始终显示为10M |
| 双工模式 | 端口当前的工作的双工模式，未连接的端口始终显示为半双工 |

3．如需修改某个端口的配置，只需单击界面中对应条目右侧的[修改]按钮，进入修改

界面后（如图 2.2），修改相应的配置项。单击[应用]按钮完成修改，单击[取消]按钮取消修改。


**图 2.2 端口配置界面**

### 管理状态-配置项说明

[设置]界面的配置项说明。

**表 2.2 [设置]界面的配置项说明**

| 值 | 值域 | 描述 |
|---|---|---|
| 管理状态 | 关闭<br>开启<br>缺省值：开启 | 对端口进行关闭/开启。关闭状态下连接/断开状态均为link down；开启状态下连接状态为link up。 |
| 速率和双工模式 | 10M half<br>10M full<br>100M half<br>100M full<br>1000M<br>自动<br>缺省值：自协商 | 可配置端口的双工和速率，如：10M/100M/1000M/自动等带宽，半双工模式下只允许一个方向的通信，全双工模式下可同时两个方向通信。 |
| 流控 | 关闭<br>开启<br>缺省值：关闭 | 二层端口流控功能，开启后可以有效的防止网络拥塞。流控是点对点的功能，采用puase帧的方式实现，当PVRP系统端口开启时，对端端口也必须开启。 |

## 2.2 端口统计

### 配置步骤

1.在导航栏中选择[基本配置/端口/统计信息],进入端口[统计信息]界面(如图 2.3)。

2.[统计信息]界面显示了每个端口的统计信息。可通过单击端口条目左侧的‘▲’标志展开相应端口的统计信息，单击右侧的清除的按钮可清除该端口的统计信息。

3. 单击[刷新]按钮对所有端口的统计信息进行更新。单击[清除全部]按钮可以清除所有端口的统计信息。


**图 2.3 端口统计信息界面**

具体端口统计信息类型介绍如下图：

**表 2.2 端口统计信息类型**

| 统计信息类型 | 说明 |
|---|---|
| Rx/Tx Bytes | 接收/发送报文总字节数量 |
| Rx/Tx Packets | 接收/发送报文总数据包 |
| Rx/Tx Unicast Packets | 接收/发送单播报文总数据包 |
| Rx/Tx Multicast Packets | 接收/发送组播报文总数据包 |
| Rx/Tx Broadcast Packets | 接收/发送广播报文总数据包 |
| Rx/Tx Discards Packets | 接收/发送废弃报文总数据包 |
| Rx/Tx Pause Packets | 接收/发送流控报文总数据包 |
| Drop Events | 丢弃报文(间隔时间抽样) |
| FCS Errors | FCS错误包 |
| Fragments | 碎片包（小于64字节的） |

# 第三章 转发表

本章对转发表进行详细的描述，主要包括以下内容：

- 基础配置
- 转发表
- 删除

## 3.1 基础配置

### 3.1.1 老化配置

老化配置包括老化时间配置和端口快速老化配置，老化时间是一个影响交换机学习进程的参数。从一个地址记录加入地址表以后开始计时，如果在老化时间内各端口未收到源地址为该 MAC 地址的帧，那么，这些地址将从动态转发地址表中被删除。静态 MAC 地址表不受地址老化时间影响。端口快速老化是在端口 Link Down 之后此端口学习到的动态 MAC 地址全部被清掉。

**配置步骤**

1．在导航栏中选择[基本配置/转发表/配置/老化设置]，进入[老化设置]界面。

2．在转发表[老化设置]界面中可以查看转发表的老化时间的相关配置信息。

3．如需修改转发表的老化时间配置，可在老化时间配置框中修改相应配置，然后单击<应用>，如图 3.1。

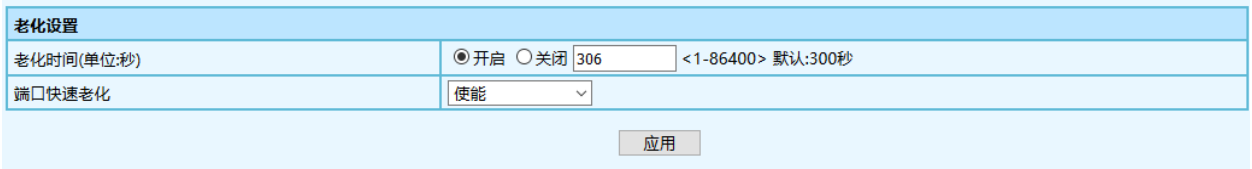



**图 3.1 老化时间配置界面**

**配置项说明**

转发表[老化时间]界面的配置项说明。

**表 3.1 转发表[老化时间]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 老化时间 | 转发表的老化时间，可通过单选按钮进行配置。<br>• 开启：开启老化时间，范围为1-86400，默认为300，单位为秒。 |

| | |
|---|---|
| | • 关闭：转发表永不老化，但系统复位会清空动态的转发表项。<br>注：默认开启，值为300秒。 |
| 端口快速老化 | • 使能：端口Link Down之后学习到的动态MAC地址立即被清掉。<br>• 禁止：端口Link Down之后需要等待上面的老化时间过后才会清掉MAC地址。<br>注：默认使能 |

### 3.1.2 静态 MAC

单播是主机之间“一对一”的通讯模式，当 MAC 地址转发表中包含与报文目的 MAC 地址对应的表项时，交换机直接将报文从该表项中的转发出端口发送。单播 MAC 地址提供配置目的 MAC 地址与端口一一对应的功能，手动配置静态 MAC 地址表。配置某一端口与某一 MAC 地址对应后，目的地址为该 MAC 地址的报文只能从所对应的端口转发，而不进行广播。

**配置步骤**

1. 在导航栏中选择[基本配置/转发表/配置/静态 MAC]，进入[静态 MAC]配置界面。

2. 在转发表[静态 MAC]界面中可以查看转发表的静态 MAC 相关配置信息，如图 3.2。

3. 如需添加新的静态 MAC，单击<添加>，进入[静态 MAC]配置界面，填写相应的配置项，单击<应用>，完成添加。如配置项填写有误，会有相应的提示。

4. 如需修改静态 MAC，勾选相应的静态 MAC，单击<修改>，进入[静态 MAC]界面，修改相应的配置项，单击<应用>，完成修改。如配置项填写有误，会有相应的提示。

5. 如需删除静态 MAC，勾选相应的静态 MAC，单击<删除>，删除静态 MAC。

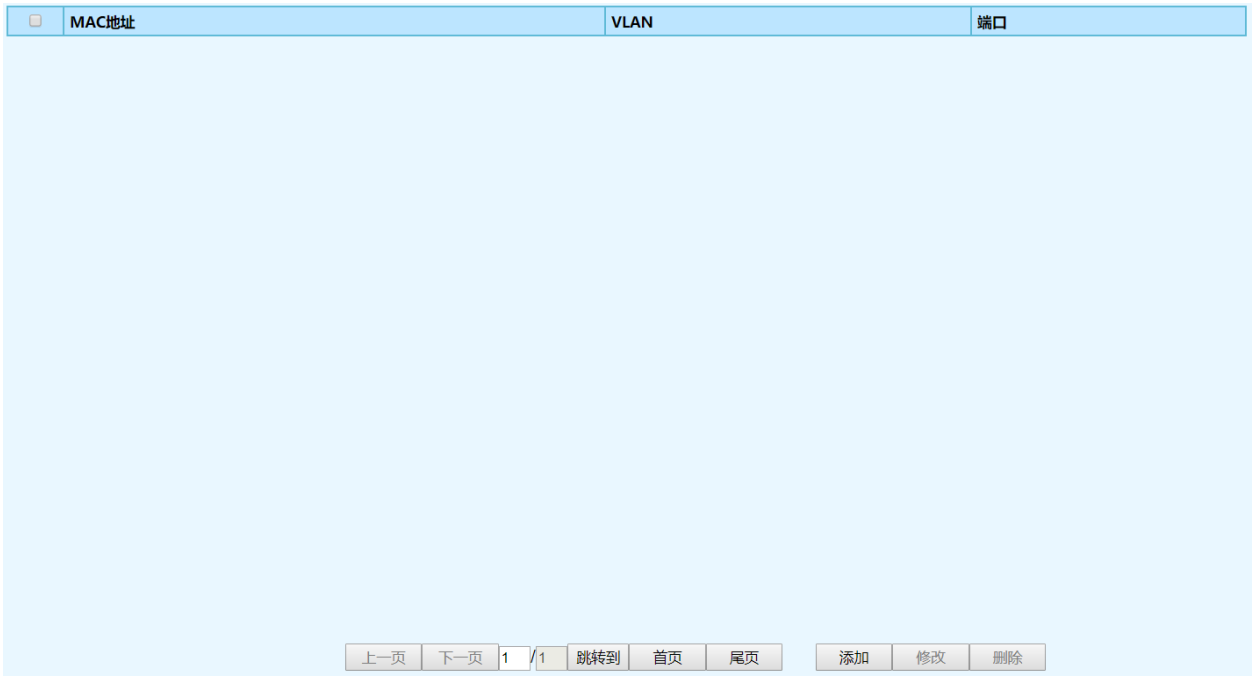



图 3.2 静态 MAC 显示界面

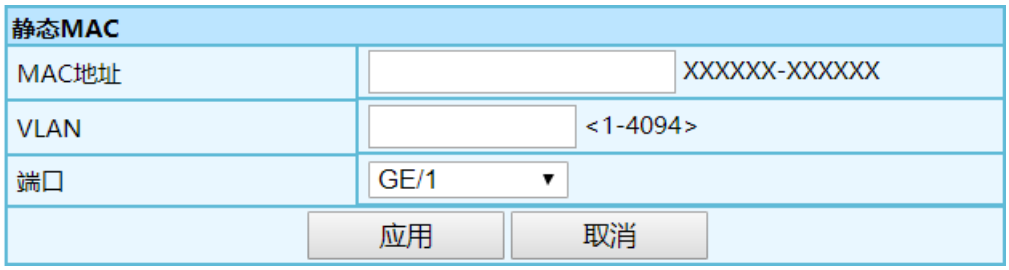



图 3.2 静态 MAC 配置界面

### 配置项说明

转发表[静态 MAC]界面的配置项说明。

表 3.2 转发表[静态 MAC]界面的配置项说明

| 配置项 | 说明 |
|---|---|
| MAC地址 | 有效的单播MAC地址，格式XXXXXX-XXXXXX。 |
| VLAN | 有效的VLAN ID，范围为1-4094。 |
| 端口 | 端口，可选择指定端口。 |

## 3.1.3 端口学习能力

本设备每个端口都具有一定的学习能力，缺省使能学习能力，根据不同的芯片方案，而端口学习能力的数目决定了端口学习 MAC 地址的总数目，IES9000 系列设备缺省情况下

为 8192 条，每个产品根据能力的不同，具体见每个产品系列的规格书为准，建议在非未必要的情况下，不需修改此功能配置。

设备的 MAC 地址学习为独立 VLAN 学习，IVL（Independent VLAN Learning，独立 VLAN 学习）：交换机为每个 VLAN 维护独立的 MAC 地址转发表。由某个 VLAN 内的端口接收的报文，其源 MAC 地址只被记录到该 VLAN 的 MAC 地址转发表中，且报文的转发只以该表中的信息作为依据。

## 配置步骤

1. 在导航栏中选择[基本配置/转发表/配置/端口学习能力]，进入[端口学习能力]界面。

2. 在转发表[端口学习能力]界面中可以查看转发表的端口学习能力相关配置信息。

3. 如需修改端口学习能力配置，单击对应端口显示栏后的<修改>按钮，进入端口配置界面，如图 3.3。

4. 选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。


**图 3.3 端口学习能力配置界面**

## 配置项说明

转发表[端口学习能力]界面的配置项说明。

**表 3.3 转发表[端口学习能力]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称，当前选择修改的端口号 |
| 学习 | 端口学习的功能配置。可通过单选按钮进行配置。<br>• 开启：开启端口学习能力。如：IES9000系列范围为1-8192；<br>• 关闭：关闭端口学习能力。<br>注：默认为开启，值为8192。 |

**注：地址学习数量是所有端口共享的。**

## 3.2 转发表

以太网交换机在转发数据前必须知道它的每一个端口所连接的主机的 MAC 地址，构建出一个 MAC 地址表。 当交换机从某个端口收到数据帧后， 读取数据帧中封装的目的地 MAC 地址信息，然后查阅事先构建的 MAC 地址表，找出和目的地地址相对应的端口，从该端口把数据转发出去，其他端口则不受影响，这样避免了与其它端口上的数据发生碰撞。因此构建 MAC 地址表是交换机的首要工作，也是基本工作原理。

**配置步骤**

1. 在导航栏中选择[基本配置/转发表/转发表]，进入[转发表]界面。
2. 在[转发表]界面中可以查看转发表信息，如图 3.4。

| 序号 | MAC地址 | VLAN | 端口 | 类型 |
|---|---|---|---|---|
| 1 | 000A0C-0B2925 | 1 | GE/9 | dynamic |
| 2 | 000BAB-A9FF3F | 1 | GE/9 | dynamic |
| 3 | 000C29-F4930F | 1 | GE/9 | dynamic |
| 4 | 001517-F8D948 | 1 | GE/9 | dynamic |
| 5 | 00C0F6-502029 | 1 | GE/9 | dynamic |
| 6 | 00E04C-360CD3 | 1 | GE/9 | dynamic |
| 7 | 00E04C-360FE5 | 1 | GE/9 | dynamic |
| 8 | 00E04C-373329 | 1 | GE/9 | dynamic |
| 9 | 00E04C-4D21DF | 1 | GE/9 | dynamic |
| 10 | 08606E-91785E | 1 | GE/9 | dynamic |
| 11 | 1C1B0D-02D300 | 1 | GE/9 | dynamic |
| 12 | 201A06-BD004A | 1 | GE/9 | dynamic |
| 13 | 206A8A-2FC48F | 1 | GE/9 | dynamic |
| 14 | 244C07-331764 | 1 | GE/9 | dynamic |
| 15 | 28D244-5571E7 | 1 | GE/9 | dynamic |
| 16 | 2CD141-A00417 | 1 | GE/9 | dynamic |
| 17 | 2CD141-A0050F | 1 | GE/9 | dynamic |

上一页 下一页 1 /3 跳转到 首页 尾页 删除 刷新

**图 3.4 转发表界面**

3. 如需删除转发条目，勾选中相应的转发条目或全部选中，然后单击<删除>，即可删除发条目。

## 3.3 删除

**配置步骤**

1. 在导航栏中选择[基本配置/转发表/删除]，进入[删除]界面。
2. 如需批量删除转发表的相关条目，可在 MAC 地址删除栏中选择相应的删除条件，然

后单击<应用>，如图 3.5。

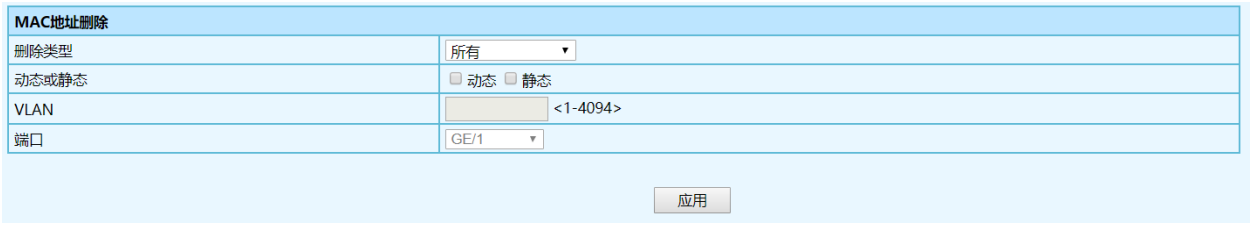



**图 3.5 转发表删除界面**

## 配置项说明

转发表[删除]界面的配置项说明。

**表 3.4 转发表[删除]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 删除类型 | 选择删除操作的类型。<br>• 所有：删除所有转发表条目。<br>• VLAN：指定VLAN ID值来删除转发表条目。<br>• 端口：指定端口号来删除转发表条目。 |
| 动态或静态 | 选择删除类型动态类型或静态类型：<br>• 动态：删除通过学习的动态转发表条目。<br>• 静态：删除手动添加的静态转发表条目。 |
| VLAN | 删除指定VLAN的转发表条目，范围为1-4094。 |
| 端口 | 删除指定端口的转发表条目。 |

# 第四章 VLAN

本章对 VLAN 进行详细的描述，主要包括以下内容：

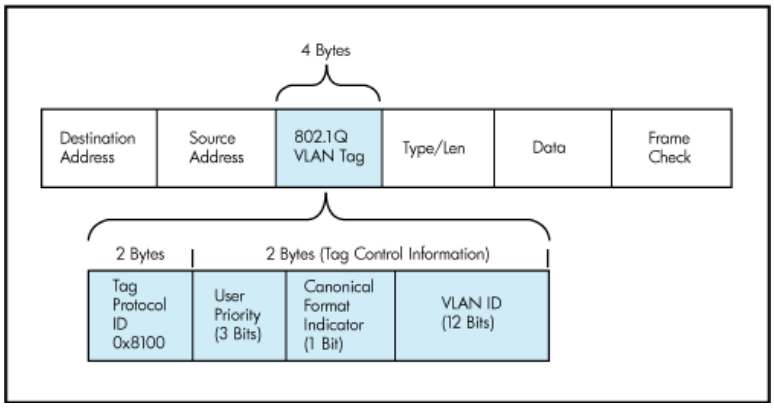
- VLAN 概述
- VLAN 优点
- VID 概念
- PVID
- 端口处理报文方式
- 基础配置
- VLAN 端口配置

## 4.1 VLAN 概述

VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”。VLAN 是一种将局域网设备从逻辑上划分成一个个网络，从而实现将一个大的物理网络分隔成多个虚拟工作组数据交换技术。这些设备和用户不受物理位置的限制，可以根据功能、部门及应用等因素设定为一个群组，使它们之间通信像在同一个物理分段中。

VLAN 技术的出现，使得管理员根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 内。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少广播域、简化网络管理、提高网络的可靠性。

VLAN 数据包格式：



## 4.2 VLAN 优点

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它的优点如下：

●广播风暴防范

限制网络上的广播，将网络划分为多个 VLAN 可减少参与广播风暴的设备数量。VLAN 分段可以防止广播风暴波及整个网络。

●安全性

增强局域网的安全性，含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。

●性能提高

将第二层平面网络划分为多个逻辑工作组（广播域）可以减少网络上不必要的流量扩散并提高性能。

●增加网络连接的灵活性

借助 VLAN 技术，能将不同地点、不同物理网络、不同用户组合在一起，形成一个虚拟的网络环境，就像使用本地 LAN 一样方便、灵活、有效。

## 4.3 VID 概念

VID，即交换机收到数据帧的 VLAN 标识号。 交换机根据收到数据帧的 VLAN 标识（VID）将它们分类，无标号的为一类，标号相同的为一类。交换机根据 VID 来决定转发或者丢弃一个数据包，同时启用了 VLAN 的交换机也可以配置一个 VID 给一个无标记帧或者贴了优先级标记的帧。 如果一个数据帧没有标记 VID，启用了 VLAN 的交换机将会配置一个 VID 给它，并把这个 VID 插到它的帧头中。交换机通过这个过程来处理包的转发，来填写数据帧的 VLAN 或者优先级信息的标记字段。管理员可以设置优先级别来选择 VLAN 类型，选择 VID 值。

## 4.4 PVID

PVID 为 Port-base VLAN ID，也就是端口的虚拟局域网 ID 号，关系到端口收发数据帧时的 VLAN Tag 标记。PVID 是在划分 VLAN 时候每个端口都有的属性。交换机上的端口分为三种，一种是接入层端口直连设备的，叫做 Access(接入端口)；一种是交换机和交换机之

间的端口负责汇聚的叫做 Trunk(中级)，还有一种是 Access 与 Trunk 混合的模式，叫做 Hybrid。具体这三种端口处理报文下面说明。

## 4.5 端口处理报文方式

用户根据不同的需求，需要对不同的端口进行 VLAN 类型和 VLAN LIST 进行配置，下面表 4.1 简单说明各类型对报文不同的处理方式：

**表 4.1 三种 VLAN 类型端口处理报文方式**

| VLAN 端口类型 | 入口报文的处理 | 出口报文的处理 |
|---|---|---|
| Access 端口 | 1.收到一个报文；<br>2.判断是否有 VLAN 标签：如果没有转到第 3 步，否则转到第 4 步；<br>3.打上端口的 PVID，并进行交换转发；<br>4.丢弃报文 | 1.判断是否有 VLAN 标签：如果有转到第 2 步，否则转到第 3 步；<br>2.判断 VALN 的标签是否跟端的 PVID 一样，一样则剥掉标签转发，否则丢弃<br>3.丢弃报文 |
| Trunk 端口 | 1.收到一个报文；<br>2.判断是否有 VLAN 标签：如果没有则转到第 3 步， 否则转到第 4 步；<br>3.打上端口的 PVID， 该 VLAN 的 PVID 在端口 tag 表里则进行交换转发，否则丢弃；<br>4.判断该VLAN 的PVID 是否存在端口的 tag 表里：如果是则转发，否则丢弃 | 1.比较端口的 PVID 和将要发送报文的 VLAN 标签；<br>2.如果两者相同则转到第 3 步，否则转到第 4 步；<br>3.判断标签是否在端口 tag 表里，如果在剥离 VLAN 标签，再发送，否则丢弃；<br>4. 判断标签是否在端口 tag 表里，如果在直接发送，否则丢弃 |
| Hybrid 端口 | 1.收到一个报文；<br>2.判断是否有 VLAN 标签：如果没有则转到第 3 步， 否则转到第 4 步；<br>3.打上端口的 PVID， 该 PVID 在端口 tag 或 untag 表里则进行交换转发，否则丢弃；<br>4.判断该报文的VID 是否存在端口的 tag 或 untag 表里：如果是则转发，否则丢弃 | 1.判断是否有 VLAN 标签：如果有转到第 2 步，否则转到第 3 步；<br>2.判断标签是否在端口 tag 或 untag 表里，如果在 untag 表则剥离 VLAN 标签，再发送，如果在 tag 表里，判断标签是否跟端口 PVID 一样，一样剥离标签转发，不一样直接转发，不在 tag 或者 untag 表里报文被丢弃；<br>3.丢弃报文 |

## 4.6 基础配置

**配置步骤**

1．在导航栏中选择[基本设置/VLAN/基本设置]，进入 VLAN[基本设置]界面。

2．在[基本设置]界面中可以查看各个 VLAN 的相关配置信息。

- 如需查找某 VLAN ID 的信息，在下拉框中选择 VLAN ID 所在范围，在输入框中输入

指定的 VLAN ID，单击<查找>。

3．如需添加、修改或删除 VLAN，单击<设置>，在设置界面的<VLAN 列表>框中输入要添加、修改或删除的 VLAN，再选择添加、修改或删除，单击<应用>，完成设置，修改选项只能修改 VLAN 名称，如图 4.2。


**图 4.2 VLAN 基本设置界面**

## 配置项说明

VLAN[基本设置]的相关界面的配置项说明。

**表 4.2 VLAN[基本设置]界面的配置项说明**

| 配置项 | 说明 |
|---|---|
| 查找 | 用来搜索某个VLAN ID信息<br>1．在区间选择框中选择要查找的VLAN所在的区间；<br>2．在输入框中输入特定VLANID，如 11，则显示框中的VLAN号为11的信息条变黄；<br>3．如无该VLAN， 则提示相应信息； |
| 置顶 | 显示第一页的VLAN信息 |
| 置底 | 显示最后一页的VLAN信息 |

**表 4.2 VLAN[基本设置]的设置界面的配置项说明**

| 配置项 | 说明 |
|---|---|
| VLAN列表框 | 用来输入需要设置的VLAN列表，支持多VLAN批量输入，如：“ 1,2,3,4-10”； |
| 添加 | 用来添加在VLAN列表框中输入的VLAN，VLAN1为默认VLAN，已经存在，无需创建； |
| 删除 | 用来删除在VLAN列表框中输入的VLAN，VLAN1为默认VLAN，不能删除； |
| 修改 | 用来修改在VLAN列表框中输入的VLAN，目前支持修改VLAN名称，新的名称需要在名称框中输入。 |

# 4.7 VLAN 端口配置

## 配置步骤

1．在导航栏中选择[基本配置/VLAN/端口设置]，进入 VLAN[端口设置]界面。

2．在[端口设置]界面中可以查看各个端口的 VLAN 相关配置信息。

3．如需修改某个端口的 VLAN 配置，单击对应端口显示栏后的<修改>按钮，进入端口设置界面，如图 4.2。

4．选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。

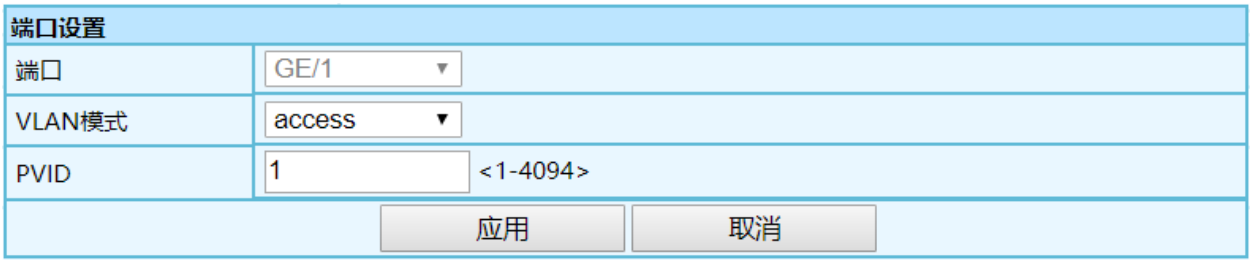



图 4.2 VLAN 端口设置界面

## 配置项说明

VLAN[端口设置]的相关界面的配置项说明。

表 4.3 VLAN[端口设置]界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 修改 | 修改对应端口的VLAN配置信息； |
| 刷新 | 刷新所有端口的VLAN配置信息； |

**表 4.4 VLAN[端口设置]的修改界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息； |
| VLAN模式 | 端口VLAN模式：<br>● access：access模式；<br>● trunk：trunk模式；<br>● hybrid：hybrid模式； |
| PVID | 端口PVID； |
| Tagged VLAN | 端口允许通过的VLAN列表，支持多VLAN批量输入，如：“ 1,2,3,4-10”；<br>添加：添加输入的VLAN为端口的tagged VLAN；<br>删除：将输入的VLAN从端口的tagged VLAN中删除；<br>替换：将端口原来的tagged VLAN替换为输入的VLAN；<br>所有已创建的VLAN：将所有已创建的VLAN作为端口的tagged VLAN，即使是后来创建的VLAN，也会自动加入该端口的tagged VLAN。 |
| Untagged VLAN | 端口untagged VLAN列表，支持多VLAN批量输入，如：“ 1,2,3,4-10”；<br>添加：添加输入的VLAN为端口的untagged VLAN；<br>删除：将输入的VLAN从端口的untagged VLAN中删除；<br>替换：将端口原来的untagged VLAN替换为输入的VLAN； |

# 第五章 QoS

本章对 QoS 进行详细的描述，主要包括以下内容：

- QoS 概述
- 功能简介
- 拥塞管理
- 策略分类
- 调度方式
- 优先级映射配置
- QoS 端口配置

## 5.1 QoS 概述

QoS（Quality of Service，服务质量）是用各种手段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 能确保重要业务量和关键应用不受延迟或丢弃，同时保证网络的高效运行。

## 5.2 功能简介

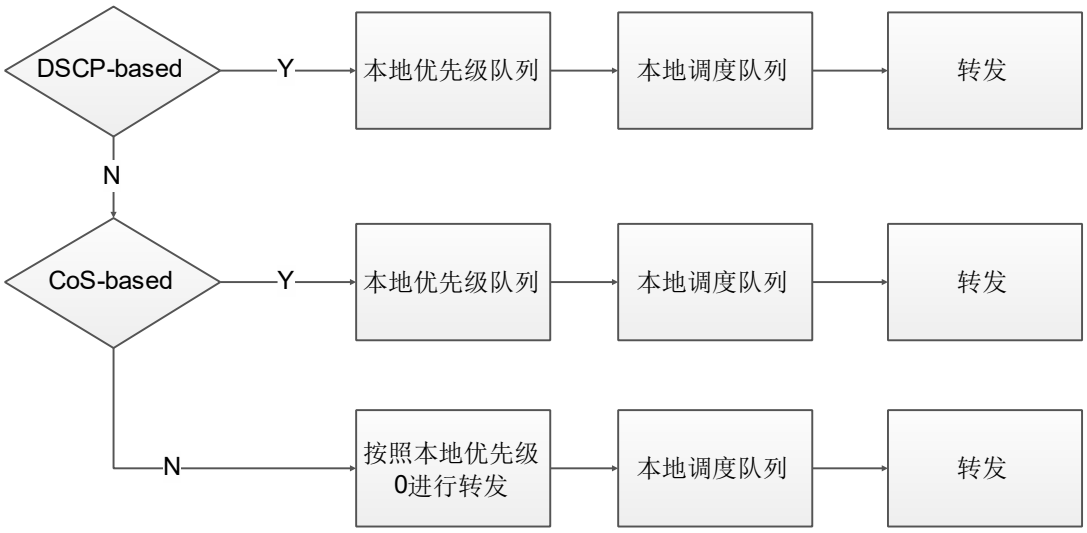
当网络发生拥塞的时候，所有的数据流都有可能被丢弃；为满足用户对不同应用不同服务质量的要求，就需要网络能根据用户的要求分配和调度资源，对不同的数据流提供不同的服务质量：对实时性强且重要的数据报文优先处理；对于实时性不强的普通数据报文，提供较低的处理优先级，网络拥塞时甚至丢弃。支持 QoS 功能的设备，能够提供传输品质服务；针对某种类别的数据流，可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。配置了 QoS 的网络环境，增加了网络性能的可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

## 5.3 拥塞管理

当出现拥塞时，在未启动 QoS 的情况下，交换机的各个端口中的各个队列对待所有的数据都是一视同仁，在一个端口中使用的策略都是：FIFO（先进先出），在此且说明 QoS 的作用是在出站口上的，在现实情况下，不同数据的重要性是由用户自身的需求产生，所以就得将不同的数据分配到不同的输出队列，也就是 QoS 的内部 DSCP，QoS 其实也就是当发生拥塞时，对不同数据进行管理。

## 5.4 策略分类

启动 QoS 后，交换机会对不同的数据流进行区别对待，那么分类的依据是什么？对数据包进行分类的时候，对于三层数据和二次数据的分类依据一样吗？而分类的依据是系统默认还是可以人为设置的？




对于交换机的内部而言，其 QoS 主要进行分类依据就是 DSCP(此为交换机内部分类依据，后面一律用内部 DSCP)。由上图可以看出对于网络数据流的分类分为 DSCP 和 COS，且当一个报文同时具备 DSCP 和 COS 两种分类依据时，只考虑 DSCP 的分类依据。

## 5.5 调度方式

拥塞管理是指网络在发生拥塞时，如何进行管理和控制。处理的方法是使用队列技术。将所有要从一个接口发出的报文进入多个队列，按照各个队列的优先级进行处理。不同的队列算法用来解决不同的问题，并产生不同的效果。常用的队列技术有FIFO、PQ、CQ、CB、WFQ、WRR、SP等，下面将主要对WFQ、WRR、SP进行逐一介绍。

### 5.5.1 SP(Strict Priority)-严格优先级

原理：对不同的队列设置不同的优先级，优先级高的队列享有绝对优先低，只要优先级高的队列有数据包存在，优先调度优先级高的队列进行转发。

### 5.5.2 WRR(Weighted Round Robin)-加权循环调度算法

加权循环(WRR)所有业务队列服务，并且将优先权分配给较高优先级队列。在大多数情况下，相对低优先级，WRR 将首先处理高优先级，但是当高优先级业务很多时，较低优先级的业务并没有被完全阻塞。加权循环调度算法 WRR 是一种较强的队列调度算法,它能够有效地区分队列中所有的业务。对于所有的业务流在排队等待调度的队列,WRR 是根据每个队列配置的权值与所有的业务流在排队等待调度的队列的权值总和的比来平等地分配带宽。因此，在处理多个用户的高优先等级的业务时,WRR 确保每个用户都不会过度地占用网络带宽。而且 WRR 算法容易在硬件中实现。所以 WRR 算法能够实现带宽分享的公平性、恶意流的隔离能力和带宽的利用率等性能指标

### 5.5.3 WFQ(Weighted Fair Queuing)-加权公平排队

加权公平排队(WFQ)是一种拥塞管理算法，该算法识别对话（以数据流的形式）、分开属于各个对话的分组，并确保传输容量被这些独立的对话公平地分享。WFQ 是在发生拥塞时稳定网络运行的一种自动的方法,它能提高处理性能并减少分组的重发(几乎和 WRR 的调度一样，唯一的不同它是综合包数量及字节数调度)。

## 5.6 优先级映射配置

### 5.6.1 802.1p 优先级(CoS)

**配置步骤**

1．在导航栏中选择[基本配置/QOS/优先级映射/802.1p 优先级]，进入 QOS[802.1p 优先级映射]界面。

2．在 QOS[802.1p 优先级映射]界面中可以查看 802.1p 优先级到本地优先级的映射关系。

3．如需修改映射关系，单击<修改>按钮，再在相应的下拉列表框中为对应的 802.1p 优先级选择映射的本地优先级，如图 5.1。

| 802.1p 优先级映射 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 802.1p优先级 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 本地优先级 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

修改

图 5.1 QOS 802.1p 优先级映射设置界面

### 配置项说明

QOS[802.1p 优先级]的相关界面的配置项说明。

表 5.1 QOS[802.1p 优先级]界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 修改 | 修改802.1p优先级到本地优先级的映射关系。 |

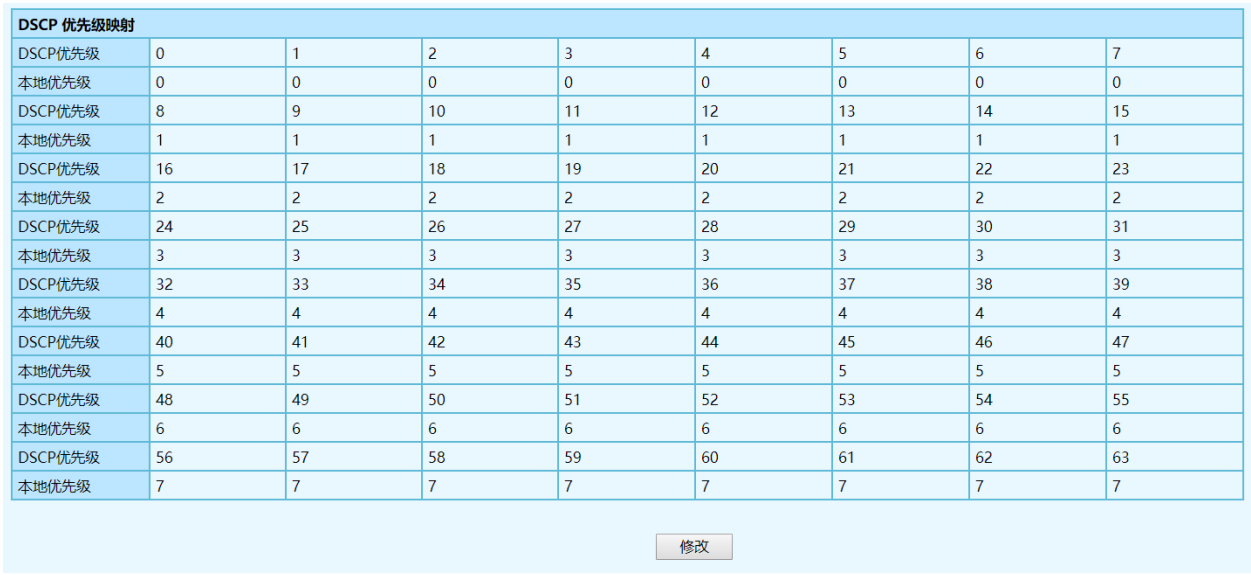
## 5.6.2 DSCP 优先级

### 配置步骤

1．在导航栏中选择[基本配置/QOS/优先级映射/DSCP 优先级]，进入 QOS[DSCP 优先级映射]界面。

2．在 QOS[DSCP 优先级映射]界面中可以查看 DSCP 优先级到本地优先级的映射关系。

3．如需修改映射关系，单击<修改>按钮，再在相应的下拉列表框中为对应的 DSCP 优先级选择映射的本地优先级，如图 5.2。



| DSCP 优先级映射 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| DSCP优先级 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 本地优先级 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| DSCP优先级 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 本地优先级 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| DSCP优先级 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 本地优先级 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| DSCP优先级 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 本地优先级 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| DSCP优先级 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 本地优先级 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| DSCP优先级 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| 本地优先级 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| DSCP优先级 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 |
| 本地优先级 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| DSCP优先级 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| 本地优先级 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |

修改

图 5.2 QOS DSCP 优先级映射设置界面

### 配置项说明

QOS[DSCP 优先级]的相关界面的配置项说明。

表 5.2 QOS[DSCP 优先级]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 修改 | 修改DSCP优先级到本地优先级的映射关系。 |

### 5.6.3 本地优先级

### 配置步骤

1．在导航栏中选择[基本配置/QOS/优先级映射/本地优先级]，进入 QOS[本地优先级映射]界面。

2．在 QOS[本地优先级映射]界面中可以查看本地优先级到出口队列的映射关系。

3．如需修改映射关系，单击<修改>按钮，再在相应的下拉列表框中为对应的本地优先级选择映射的出口队列，如图 5.3。

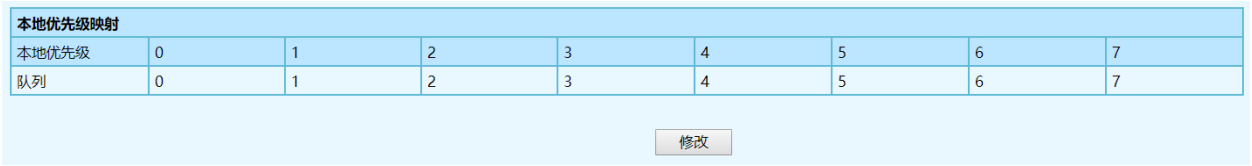



图 5.3 QOS 本地优先级映射设置界面

### 配置项说明

QOS[本地优先级]的相关界面的配置项说明。

表 5.3 QOS[本地优先级]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 修改 | 修改本地优先级到出口队列的映射关系。 |

## 5.7 QOS 端口配置

### 5.7.1 端口优先级设置

### 配置步骤

1．在导航栏中选择[基本配置/QOS/端口/端口优先级]，进入 QOS[端口优先级]界面。

2．在 QOS[端口优先级]界面中可以查看端口的 QOS 相关配置。

3．如需修改某个端口的 QOS 配置，单击对应端口显示栏后的<修改>按钮，进入端口设

置界面，如图 5.4。

4．选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。


图 5.4 QOS 端口设置界面

## 配置项说明

QOS[端口优先级]的相关界面的配置项说明。

表 5.4 QOS[端口优先级]配置界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 修改 | 修改端口的QOS相关配置。 |

表 5.5 QOS[端口优先级]的修改界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息； |
| 默认优先级 | 端口默认优先级，范围为<0-7>； |
| QOS策略 | 端口的QOS策略：<br>● NONE：表示没有策略，端口默认情况下没有策略；<br>● COS：COS优先级策略；<br>● DSCP：DSCP优先级策略；<br>● COS-DSCP：COS-DSCP优先级策略。 |
| 调度模式 | QOS调度策略：<br>● SP：严格优先级调度策略；<br>● WRR：加权平均调度策略；<br>● WFQ：加权公平队列调度策略。 |
| 权重 | 若选择的调度模式为WRR或WFQ，则需要配置每个队列的权重，共8个队列，所以需 |

| | |
|---|---|
| | 设置8个权重，所有队列的权重和必须为127。 |

### 5.7.2 端口限速

#### 配置步骤

1．在导航栏中选择[基本配置/QOS/端口/端口限速]，进入 QOS[端口限速]界面。

2．在 QOS[端口限速]界面中可以查看端口的限速相关配置。

3．如需修改端口的限速配置，单击对应端口显示栏后的<修改>按钮，进入端口限速设置界面，如图 5.5。

4．选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。

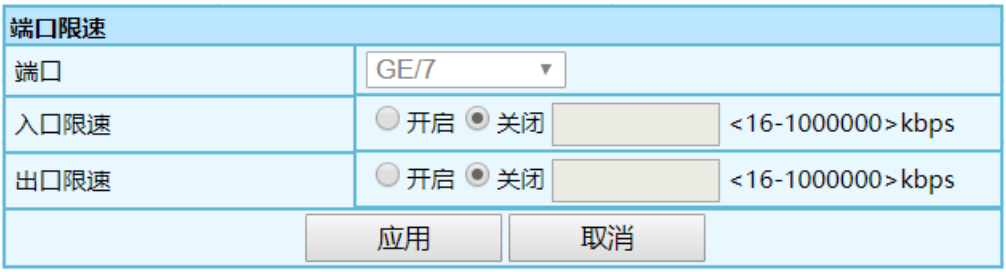



图 5.5 QOS 端口限速设置界面

#### 配置项说明

QOS[DSCP 优先级]的相关界面的配置项说明。

表 5.6 QOS[端口限速]界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 修改 | 修改端口限速的相关配置。 |

表 5.7 QOS[端口限速]的修改界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 端口 | 端口名称信息； |
| 入口限速 | 设置端口的入口限速：<br>● 开启：开启端口的入口限速，限速取值范围为<16-1000000>；<br>● 关闭：关闭端口的入口限速； |
| 入口限速 | 设置端口的出口限速：<br>● 开启：开启端口的出口限速，限速取值范围为<16-1000000>； |

| | |
|---|---|
| | ● 关闭：关闭端口的出口限速； |

# 第六章 ACL

本章对 ACL 进行详细的描述，主要包括以下内容：

- ACL 概述
- 工作原理
- ACL 组设置
- ACL 规则

## 6.1 ACL 概述

访问控制列表（Access Control List，ACL） 是路由器和交换机接口的指令列表，用来控制端口进出的数据包。配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。信息点间通信和内外网络的通信都是企业网络中必不可少的业务需求，为了保证内网的安全性，需要通过安全策略来保障非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。简而言之，ACL 可以过滤网络中的数据报文，是控制访问的一种网络技术手段。

## 6.2 工作原理

以单一端口说明，一个端口执行哪条 ACL，这需要按照列表中的条件语句执行顺序来判断。如果一个数据包的报头跟表中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

数据包只有在跟第一个判断条件不匹配时，它才被交给 ACL 中的下一个条件判断语句进行比较。如果匹配（假设为允许发送），则不管后面的语句，数据都会立即发送到目的接口。如果所有的 ACL 判断语句都检测完毕，仍没有匹配的语句出口，则该数据包将视为正常转发。

## 6.3 ACL 组设置

**配置步骤**

1. 在导航栏中选择[高级配置/ACL/ACL 组设置]，进入 ACL 组界面。
2. 在[ACL 组设置]界面可以看到已经添加的 ACL 组信息，如图 6.1 所示。


图 6.1 ACL 组信息

3. 如需添加 ACL 组，单击<添加>，进入[ACL 组设置]界面，如图 6.2 所示。序号一栏中为该组分配一个序号（0-3999），组名称一栏中为该组设置一个名称，名称不可重复。绑定到端口一栏中，选择该组要绑定的端口，不绑定到端口该组不能使用。相应的配置项填写完毕后，单击<应用>，完成配置。


图 6.2 ACL 组设置界面

4. 如需修改 ACL 组配置，勾选某条 ACL 组后单击<修改>，进入[ACL 组设置]界面。填写应的配置项，单击<应用>，完成配置。

5. 如需删除 ACL 组配置，勾选某条 ACL 组后单击<删除>，删除配置。

**配置项说明**

**表 6.1 ACL 组配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 序号 | ACL组索引，范围<0-3999>,分为4个匹配组L2， L3/L4，Source L2/L3/L4, Destination L2/L3/L4,其中各匹配组支持的匹配项如下：<br>L2：源MAC，目的MAC，以太网类型，VLAN，IP协议，范围0-999<br>L3/L4:VLAN，源IP，目的IP，源IP端口，目的IP端口，IP协议，范围1000-1999<br>Source<br>L2/L3/L4:源MAC，以太网类型，VLAN，源IP，源IP端口，IP协议，范围2000-2999<br>Destination<br>L2/L3/L4:目的MAC，以太网类型，VLAN，目的IP，目的IP端口，IP协议，范围3000-3999 |
| ACL组名称 | ACL的名称，字符串格式，必须为ASCII码A-Z,a-z,0-9,_，不超过32个字符，名称不允许重复 |
| 绑定到端口 | ACL应用到某个或某些端口，绑定端口ACL才会生效 |

# 6.4 ACL 规则

## 6.4.1 ACL 规则设置

**配置步骤**

1．在导航栏中选择[高级配置/ACL/ACL 规则设置]，进入 ACL 规则查看界面，如图 6.3 所示。

2．在[ACL 规则设置]界面选择区间一栏中，第一个下拉列表选择组的区间，第二下拉列表选择该组区间内具体的一个组。接下来的两行分别显示选择的组名和该组绑定的端口。表格中显示了，该组已经配置的 ACL 规则。单击过滤规则栏中的⊞图标可以展开查看过滤规则的具体内容，展开后图标由⊞变成⊟。


图 6.3 ACL 规则查看界面

3．如需添加 ACL 规则，单击<添加>，进入[ACL 规则设置]界面。其中过滤规则一项，可以通过下拉列表选择不同的过滤项，然后会自动出现相应的过滤项供用户填写。也可以通过右侧的<删除>按钮，删除相应的过滤项。相应的配置项填写完毕后，单击<应用>，完成配置。

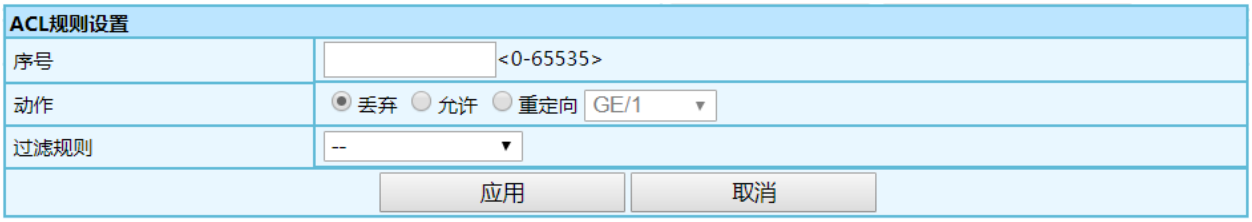



图 6.4 ACL 规则设置界面

4．如需修改 ACL 规则，勾选某条 ACL 后单击<修改>，进入[ACL 规则设置]界面。填写应的配置项，单击<应用>，完成配置。

5．如需删除 ACL 规则，勾选某条 ACL 后单击<删除>，删除配置。

## 配置项说明

表 6.1 ACL 规则项说明

| 配置项 | 说明 |
| --- | --- |
| 序号 | ACL规则索引， |
| 动作 | 当报文符合过滤规则的时候，采取的动作，包括<br>● 允许<br>● 丢弃<br>● 重定向到指定端口 |

| | |
|---|---|
| 过滤规则 | ACL的过滤规则，包括：<br>● 源MAC，支持掩码<br>● 目的MAC，支持掩码<br>● 源IP地址，支持掩码<br>● 目的IP地址，支持掩码<br>● 源IP端口<br>● 目的IP端口<br>● IP协议<br>● 以太网类型，支持掩码<br>● VLAN<br>支持掩码的过滤项，可以通过设置掩码，该过滤项可以实现按某个范围进行过滤。 |

**表 6.2 匹配项说明**

| 配置项 | 说明 |
|---|---|
| 源MAC | 源MAC地址，格式xxxxxx-xxxxxx，支持掩码，默认掩码ffffff-ffffff |
| 目的MAC | 目的MAC地址，格式xxxxxx-xxxxxx，支持掩码，默认掩码ffffff-ffffff |
| 源IP地址 | 源IP地址，格式点分十进制，支持掩码，默认掩码255.255.255.255 |
| 目的IP地址 | 目的IP地址，格式点分十进制，支持掩码，默认掩码255.255.255.255 |
| 源IP端口 | IP报文中源端口，整数形式，范围1~65535 |
| 目的IP端口 | IP报文中目的端口，整数形式，范围1~65535 |
| IP协议 | IP报文中的协议，目前仅支持TCP，UDP，ICMP，IGMP |
| 以太网类型 | 以太网协议类型，16进制形式，支持掩码，默认掩码ffff |

**注：匹配掩码为 1 时，则匹配，为 0 时则不匹配。**

# 第七章 STP

本章对 STP 进行详细的描述，主要包括以下内容：

- STP 概述
- RSTP 概述
- STP 和 RSTP 介绍
- 桥配置
- 映射配置
- 优先级配置
- CIST 端口配置
- MSTI 端口配置
- 桥状态
- 端口状态
- 统计信息

## 7.1 STP 概述

STP（Spanning Tree Protocol，生成树协议）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。

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

BPDU 格式及字段说明要实现生成树的功能，交换机之间传递 BPDU 报文实现信息交互，所有支持 STP 协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。标准生成树的 BPDU 帧格式及字段说明：Stp 端口配置本页对 stp 端口进行配置，包括以下设置（如下图）

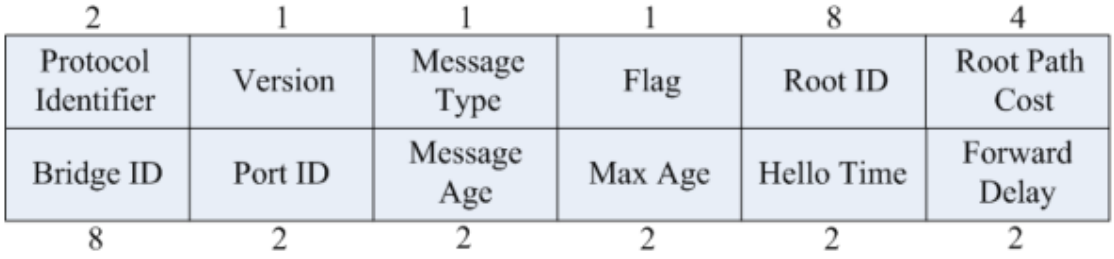



**图 7.1 标准生成树的 BPDU 帧格式**

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

## 7.2 RSTP 概述

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的 STP，它大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。RSTP 的端口状态实现快速迁移的前提如下：

根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。

指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

## 7.3 STP 和 RSTP 介绍

RSTP(802.1w)为 802.1ad 发展而来，其目的为了解决 STP 收敛时间较长的问题，下面

为 RSTP 与 STP 的介绍：

**表 7.1 STP/RSTP 介绍**

| | STP | RSTP |
|---|---|---|
| 技术介绍 | 基于OSI网络模型的数据链路层(第二层)通讯协定，用作确保一个无回圈的区域网络环境。通过有选择性地阻塞冗余链路来达到消除网路二层环路的目的，同时具备链路的备份功能，又称扩展树协议。 | RSTP是从STP发展过来的，其实现基本思想一致，但它更进一步的处理了网络临时失去连通性的问题。 |
| 相同点 | 1.整个交换网络只有一棵生成树，拓扑收敛受网路拓扑规模影响；<br>2.网络的连通性受网络结构对称性影响；<br>3.链路阻塞链路不承载任何流量。 | |
| 不同点 | 1.不能快速迁移，需要等待2倍forward delay时间延时；<br>2.在点对点或边缘端口，需要等待2倍delay时间延时；<br>3.边缘端口需要等待2倍delay时间延时。 | 1.能够快速迁移，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延地进入转发状态；<br>2.指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态；<br>3.直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。 |

## 7.4 桥配置

### 配置步骤

1. 在导航栏中选择[高级配置/STP/桥配置]，进入 STP[桥配置]界面。

2. 在[桥配置]界面中可以进行桥配置。

3. 如需修改相关配置，可直接在对应配置项的配置栏中输入需要配置的值，如图 7.2。

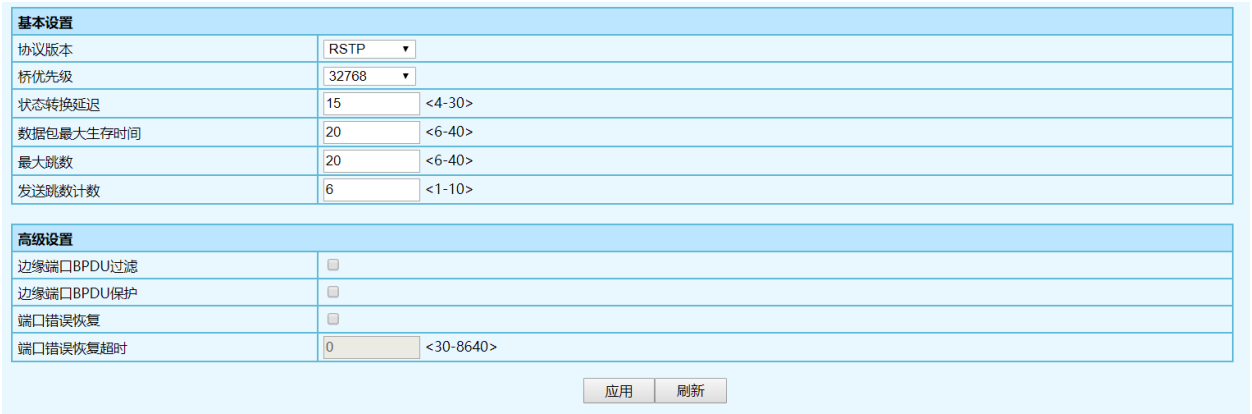



**图 7.2 STP 桥配置界面**

### 配置项说明

STP[桥配置]的相关界面的配置项说明。

**表 7.2 STP[桥配置]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 协议版本 | 协议版本包括mstp、rstp、stp三个版本 |
| 桥优先级 | 桥优先级的大小决定了本设备是否能够被选作生成树的树根，桥优先级范围为0-61440，缺省情况下，桥优先级为32768 |
| 状态转换延迟 | 状态迁移的延迟时间，延时范围为4-30s，缺省情况下，延时时间为15s |
| 数据包发送间隔 | 稳定状态下，STP协议报文发送的时间间隔 |
| 数据包最大生存时间 | 用来判断配置消息在交换机内保存时间是否“过时”的参数，老化时间范围为6-40s，缺省情况下，老化时间为20s |
| 最大跳数 | 决定bpdu的传递范围，跳数范围为6-40，缺省情况下，跳数为20 |
| 发送跳数计数 | 计数发送跳数，计数范围为1-10，缺省情况下，计数为6 |
| 边缘端口BPDU过滤 | bpdu<br>过滤将能够防止交换机在启用了边缘端口特性的端口上发送BPDU给主机，缺省关闭 |
| 边缘端口BPDU保护 | bpdu<br>防护使具备边缘端口特性的端口在接收到BPDU时进入err-disable状态来避免桥接环路 |
| 端口错误恢复 | 对err-disable状态的端口开启恢复功能，勾选为开启，缺省不勾选为关闭 |
| 端口错误恢复超时 | 超时时间后重新启动这个端口 |

## 7.5 映射配置

### 配置步骤

1．在导航栏中选择[高级配置/STP/映射配置]，进入 STP[映射配置]界面。

2．在[映射配置]界面中可以进行映射配置。

3．如需修改相关配置，可直接在对应配置项的配置栏中输入需要配置的值，如图 7.3。

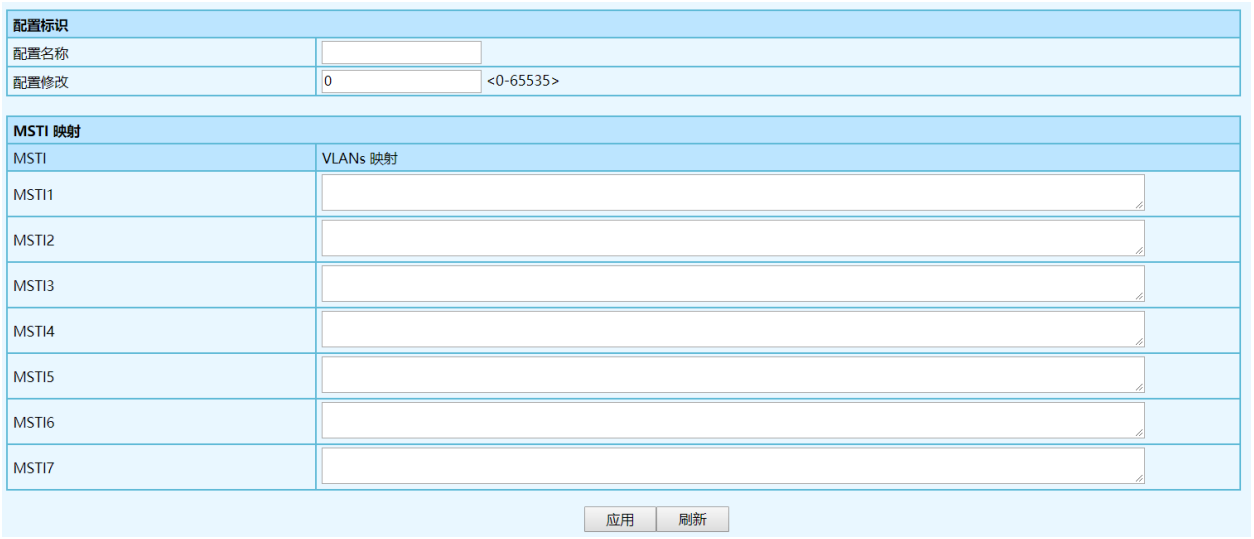



**图 7.3 映射配置界面**

### 配置项说明

STP[映射配置]的相关界面的配置项说明。

**表 7.3 STP[映射配置]界面的配置项说明**

| 配置项 | 说明 |
|---|---|
| 配置名称 | 配置的名称，mac地址标识 |
| 配置修改 | 修改范围为0-65535，缺省情况下，值为0 |
| 映射表 | 使用逗号分开，VLAN范围为1-4096，比如2-5,7,9等 |

## 7.6 优先级配置

### 配置步骤

1．在导航栏中选择[高级配置/STP/优先级配置]，进入 STP[MSTI 优先级配置]显示界面。

2．在[MSTI 优先级配置]界面中可以可以进行映射配置。

3．如需修改相关配置，可直接在对应配置项的配置栏中输入需要配置的值，如图 7.4。

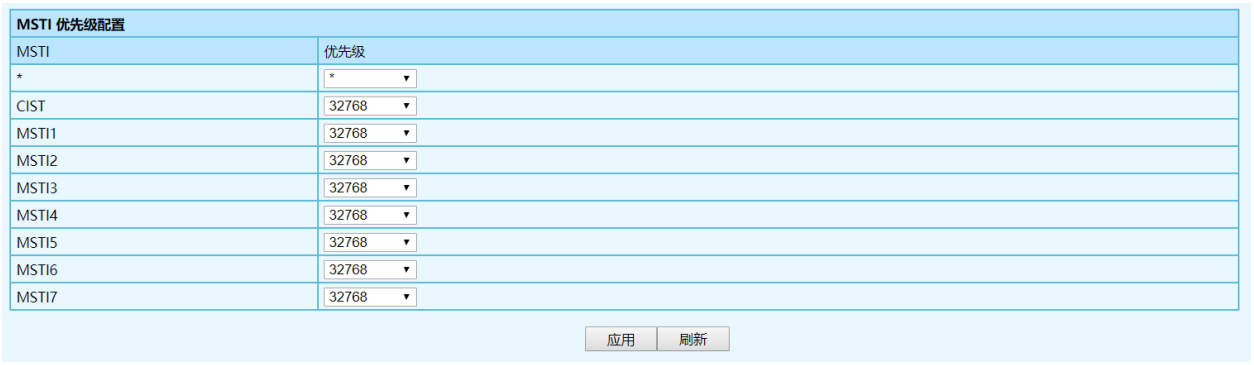



图 7.4 MSTI 优先级配置界面

### 配置项说明

STP[MSTI 优先级配置]的相关界面的配置项说明。

表 7.4 STP[MSTI 优先级配置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 优先级 | 桥优先级的大小决定了本设备是否能够被选作生成树的树根，桥优先级范围为0-61440，缺省情况下，桥优先级为32768 |

## 7.7 CIST 端口配置

### 配置步骤

1. 在导航栏中选择[高级配置/STP/CIST 端口配置]，进入 STP[CIST 端口配置]显示界面。

2. 在[CIST 端口配置]界面中可以可以进行 CIST 的端口配置。

3. 如需修改相关配置，可直接在对应配置项的配置栏中输入需要配置的值，如图 7.5。


**图 7.5 CIST 端口配置界面**

## 配置项说明

STP[CIST 端口配置]的相关界面的配置项说明。

**表 7.5 CIST 端口配置界面**

| 配置项 | 说明 |
|---|---|
| 端口 | 显示交换机端口号 |
| STP 使能 | 勾选端表示使能端口stp功能，不勾选则为未使能，缺省为关闭 |
| 路径开销 | STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构，auto自动协商的，specific手动设置，缺省为自动 |
| 优先级 | 端口优先级改变时，STP 会重新计算端口的角色并进行状态迁移，端口的优先级的值只能是16的倍数，配置范围是0-240,缺省配置128 |
| 管理边缘 | 边缘端口有或者无，缺省为无 |
| 自动边缘 | 勾选端表示使能边缘端口自动识别，不勾选则为未使能，缺省为开启 |
| 角色 | 勾选端表示使能角色，不勾选则为未使能，缺省为关闭 |
| TCN | 勾选端表示使能角TCN，不勾选则为未使能，缺省为关闭 |
| BPDU防护 | bpdu |

| | |
|---|---|
| | guard使具备边缘端口特性的端口在接收到BPDU时进入err-disable状态来避免桥接环路，bpdu<br>filter将能够防止交换机在启用了边缘端口特性的端口上发送BPDU给主机，缺省关闭 |
| 点对点 | 端口相连的链路类型，Force<br>true：点到点链路,如果端口运行于全双工模式则为点对点链路类型，Force<br>false：共享链路,如果运行于半双工模式则为共享链路类型Auto：设置端口自动建立链路，缺省端口自动建立链路。现在交换机之间一般为点对点链路类型 |

## 7.8 MSTI 端口配置

**配置步骤**

1. 在导航栏中选择[高级配置/STP/MSTI 端口配置]，进入 STP[MSTI 端口配置]显示界面。

2. 在[MSTI 端口配置]界面中可以可以进行 MSTI 的端口配置。

3. 如需修改相关配置，可直接在对应配置项的配置栏中输入需要配置的值，如图 7.6。

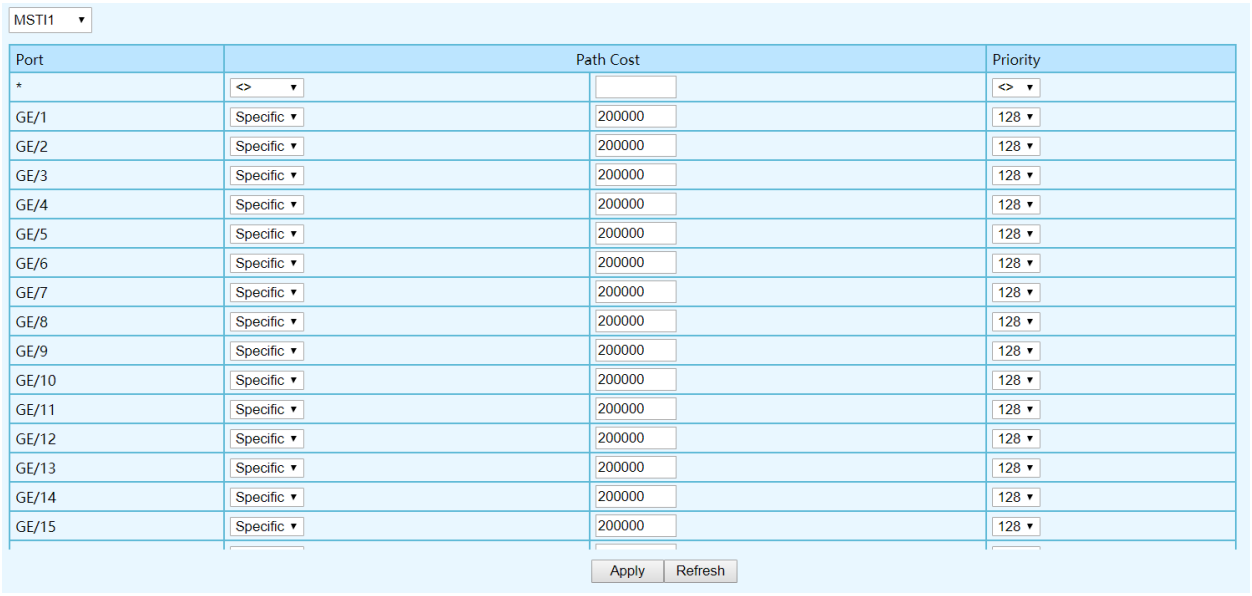



**图 7.6 MSTI 端口配置界面**

### 配置项说明

STP[MSTI 端口配置]的相关界面的配置项说明。

**表 7.6 MSTI 端口配置界面**

| 配置项 | 说明 |
| --- | --- |
| 端口 | 显示交换机端口号 |
| 路径开销 | STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构，auto自动协商的，specific手动设置，缺省为自动 |
| 优先级 | 端口优先级改变时，STP 会重新计算端口的角色并进行状态迁移，端口的优先级的值只能是16的倍数，配置范围是0-240,缺省配置128 |

## 7.9 桥状态

### 配置步骤

1. 在导航栏中选择[高级配置/STP/桥状态]，进入 STP[桥状态]显示界面。
2. 在[桥状态]界面中可以查看 STP 的当前的桥状态信息，如图 7.7。
3. 单击[刷新]，可显示最新的桥状态信息。


**图 7.7 STP 桥状态显示界面**

单击 MSTI 列的名称，比如此处的蓝色文字带下划线的“CIST”，可以查看该桥的详细状态信息。

| STP 桥详细状态 | |
|---|---|
| 桥实例 | CIST |
| 网桥ID | 32768.00-18-93-0A-97-CD |
| 根桥ID | 0.00-18-93-0A-97-CD |
| 根端口 | - |
| 根路径开销 | 0 |
| 区域根 | 0.00-18-93-0A-97-CD |
| Int. Path Cost | 0 |
| Max Hops | 20 |
| 拓扑标志 | 稳定的 |
| 拓扑修改个数 | 0 |
| 拓扑最后修改时间 | - |

| CIST Ports & Aggregations State | | | | | | | |
|---|---|---|---|---|---|---|---|
| 端口 | 角色 | 状态 | 优先级 | 路径开销 | 边缘 | 点对点 | 正常运行时间 |

刷新 返回

图 7.8 STP 详细桥状态显示界面

# 7.10 端口状态

## 配置步骤

1. 在导航栏中选择[高级配置/STP/端口状态]，进入 STP[端口状态]显示界面。
2. 在[端口状态]界面中可以查看 STP 的当前的端口状态信息，如图 7.7。
3. 单击[刷新]，可显示最新的端口状态信息。

| 端口 | CIST 角色 | CIST 状态 | 正常运行时间 |
|---|---|---|---|
| GE/1 | Disabled | Discarding | - |
| GE/2 | Disabled | Discarding | - |
| GE/3 | Disabled | Discarding | - |
| GE/4 | Disabled | Discarding | - |
| GE/5 | Disabled | Discarding | - |
| GE/6 | Disabled | Discarding | - |
| GE/7 | Disabled | Discarding | - |
| GE/8 | Disabled | Discarding | - |
| GE/9 | Disabled | Discarding | - |
| GE/10 | Disabled | Discarding | - |
| GE/11 | Disabled | Discarding | - |
| GE/12 | Disabled | Discarding | - |
| GE/13 | Disabled | Discarding | - |
| GE/14 | Disabled | Discarding | - |
| GE/15 | Disabled | Discarding | - |
| GE/16 | Disabled | Discarding | - |
| GE/17 | Disabled | Discarding | - |
| GE/18 | Disabled | Discarding | - |
| GE/19 | Disabled | Discarding | - |

刷新

图 7.9 STP 端口状态显示界面

# 7.11 统计信息

## 配置步骤

1．在导航栏中选择[高级配置/STP/统计信息]，进入 STP[统计信息]显示界面。

2．在[统计信息]界面中可以查看 STP 的当前的端口统计信息，如图 7.7。

3．单击[刷新]，可显示最新的端口统计信息。

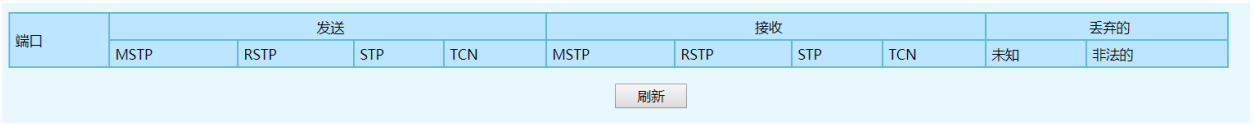



**图 7.10 STP 端口统计显示界面**

# 第八章 ERPS

本章对 ERPS 进行详细的描述，主要包括以下内容：

- ERPS 概述
- ERPS 技术介绍
- ERPS 工作原理
- 全局配置
- 环网信息

## 8.1 ERPS 概述

ERPS(Ethernet Ring Protection Switching，以太环网保护切换协议)是 ITU 开发的一种环网保护协议，也称 G.8032。它是一个专门应用于以太环网的链路层协议。它在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。ERPS 协议提供了一种快速以太环网保护机制，能够在环网发生故障时，快速地恢复网络传输，从而保障交换机在环网拓扑的情况下高可用性、高可靠性。

## 8.2 ERPS 技术介绍

### 8.2.1 ERPS 环

ERPS 环以最小化环为原则，每个环必须为最小的环，分为主环和子环：主环是封闭的环；子环是非封闭的环或封闭的环；都需要通过命令进行配置。

每个 ERPS 环(不论是主环还是子环)都有五种状态：

(1)Idle 状态：环网每条物理链路都是连通时的状态；

(2)Protection 状态：环网中某条或多条物理链路断开时的状态；

(3)Manual switch 状态：手工改变环的状态；

(4)Forced switch 状态：强制改变环的状态；

(5)Pending 状态：悬而未决的中间状态。

### 8.2.2 ERPS 节点

加入 ERPS 环的二层交换设备称之为节点。每个节点不能多于两个端口加入同一个 ERPS 环，一个端口为 RPL 端口，另一个端口为普通环端口。

对于全局而言，节点的角色分为下列两种：(1)相交节点：在相交 ERPS 环中，同时属于多个环的节点被称为相交节点；(2)非相交节点：在相交 ERPS 环中，只属于某个 ERPS 环的节点被称为非相交节点。

ERPS 协议中规定的节点模式主要有 RPL owner 节点、RPL neighbour 节点和普通环节点三种类型：

(1)RPL owner 节点：一个 ERPS 环只有一个 RPL owner 节点，由用户配置决定，通过阻塞 RPL 端口来防止 ERPS 环中产生环路，当 RPL owner 节点收到故障报文得知 ERPS 环上其他节点或链路故障时，会自动放开 RPL 端口，此端口恢复流量的接收和发送，保证流量不会中断；

(2) RPL neighbour 节点：与 RPL owner 节点的 RPL 端口直接相连的节点，正常情况下，RPL owner 节点的 RPL 端口和 RPL neighbour 节点的 RPL 端口都会被阻塞，以防止环路产生。当 ERPS 环出现故障时，RPL owner 节点的 RPL 端口和 RPL neighbour 节点的 RPL 端口都会被放开；

(3) 普通环节点：在 ERPS 环中，除 RPL owner 节点和 RPL neighbour 节点以外的节点都是普通环节点，普通环节点的 RPL 端口和普通环端口没有区别，普通环节点的环端口负责监测自己直连的 ERPS 协议的链路状态，并把链路状态的变化消息及时通知其他节点；

### 8.2.3 链路与通道

(1)RPL（Ring Protection Link，环保护链路）：每个 ERPS 环都有且仅有一条 RPL，即 RPL owner 节点的 RPL 端口所在链路。当以太环处于 Idle 状态时，RPL 链路处于阻塞状态，不转发数据报文，以避免形成环路；

(2)子环链路：在相交环当中，归属于子环，由子环控制的链路；

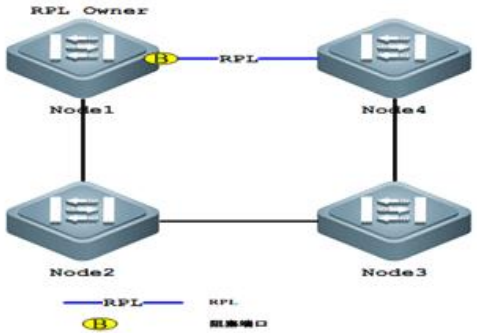
(3)RAPS（Ring Auto Protection Switch）virtual channel：在相交环中，相交节点间，用于传输子环协议报文，但不属于子环的通路被称为子环的 RAPS 虚拟通道。

### 8.2.4 ERPS VLAN

ERPS 中有两种类型的 VLAN：(1)RAPS VLAN：用来传递 ERPS 协议报文,设备上接入 ERPS 环的端口都属于 RAPS VLAN，且只有接入 ERP 环的端口可加入此 VLAN。不同环的 RAPS VLAN 必须不同。RAPS VLAN 的接口上不允许配置 IP 地址；(2)数据 VLAN：与 RAPS VLAN 相对，数据 VLAN 用来传输数据报文，数据 VLAN 中既可包含 ERP 环端口，也可包含非 ERP 环端口。

## 8.3 ERPS 工作原理

### 8.3.1 正常状态

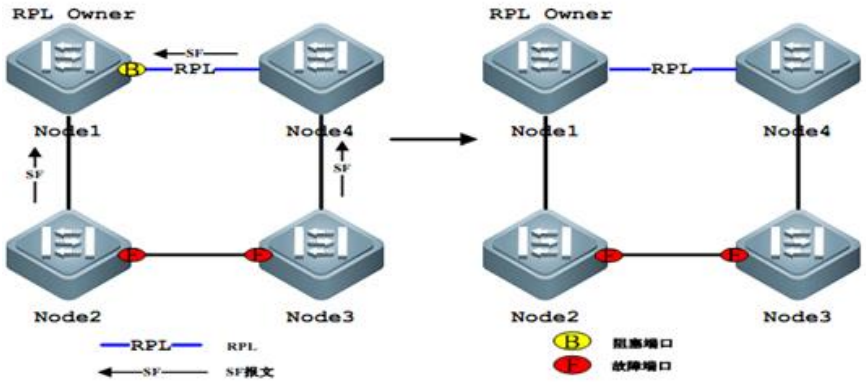



(1)所有的节点在物理拓扑上以环的方式连接；

(2)环路保护协议通过阻塞 RPL 链路，确保不会成环。如图上图所示，Node1 和 Node4 间的链路为 RPL 链路；

(3)对相邻节点间的每条链路进行故障检测。

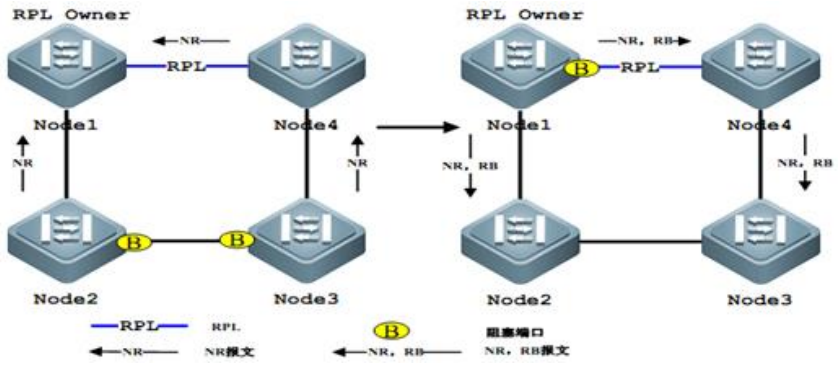
### 8.3.2 链路故障



(1)与故障链路相临的节点对故障链路进行阻塞,并使用 RAPS(SF)消息向环上的其他节点报告故障,如图上图所示,假设 Node2,Node3 间链路故障,则 Node2 和 Node3 等待 holdoff 计时器超时后，会阻塞故障链路，分别向环网上各个节点发送 RAPS(SF)消息;

(2)RAPS(SF)消息触发 RPL 拥有节点打开 RPL 端口。RAPS(SF)消息还触发所有的节点更新各自 MAC 表项，然后节点进入保护状态。

### 8.3.3 链路恢复




(1)当故障恢复时，故障相邻的节点继续保持阻塞状态，并发送 RAPS(NR)消息，表示没有本地故障;

(2)guard 计时器耗尽后，RPL Owner 节点收到第一个 RAPS(NR)消息后，开始启动 WTR 定时器;

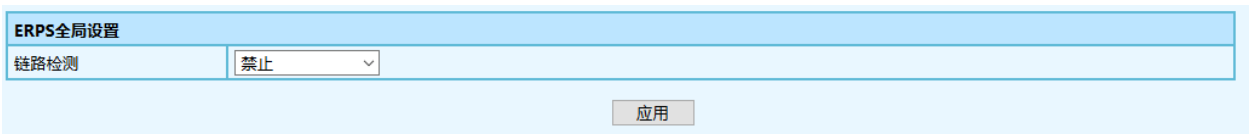
(3)当 WTR 定时器耗尽后，RPL Owner 节点阻塞 RPL，并发送 RAPS(NR,RB)消息;

(4)其他节点收到这个消息后，更新各自 MAC 表项，发送 RAPS(NR)消息的那个节点停止周期性发送消息，并打开原先阻塞的端口。环网又恢复到了最初的正常状态。

## 8.4 环设置

### 配置步骤

1.ERPS 全局设置




这是一种靠发包的机制来检测链路是否正常的方法，如果是光口做为环端口的话，这里建议把它“禁止”掉。如果是电端口做为环端口，分以下两种情况决定是否开启：

(1) 对切换时间要求很高，这时要把这一功能打开，虽然切换时间提高了，但是带来的弊端就是这种发包机制会占用带宽。

(2) 对切换时间要求不是很高的情况，建议这一功能禁止。

2.在导航栏中选择[高级配置/ERPS/全局设置]，进入 ERPS[全局设置]界面(如图 8.1)。

| 环ID | 环类型 | 节点类型 | 协议VLAN | 所属主环 | 东向端口 | 西向端口 | 返回模式 | 子环虚拟信道 | WTR定时器 | Guard定时器 | HoldOff定时器 | 倒换方式 | 设置 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 主环 | transfer | 1 | N/A | GE/1 | GE/3 | revertive | with | 1 | 500 | 0 | N/A | 修改 删除 倒换 |

**图 8.1 ERPS 环配置界面**

3. ERPS[全局配置]界面显示了当前创建的所有环信息。

4. 单击[添加]按钮，进入环创建界面(如图 8.2)后，输入有效的配置参数，单击[应用]提交修改。单击[取消]放弃修改。

| Ring Adding | |
|---|---|
| 环ID | <1-255> |
| 环类型 | 主环 |
| 节点类型 | transfer |
| 协议VLAN | <1-4094> |
| 东向端口 | GE/1 |
| 西向端口 | GE/1 |
| RPL 端口 | none |
| 所属主环 | none |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 |

**图 8.2 ERPS 环创建界面**

5. 单击[修改]按钮，进入环信息修改界面，如图 8.3。


**图 8.3 ERPS 环修改界面**

6. 单击[倒换]按钮，进入环流量倒换配置界面，如图 8.4。

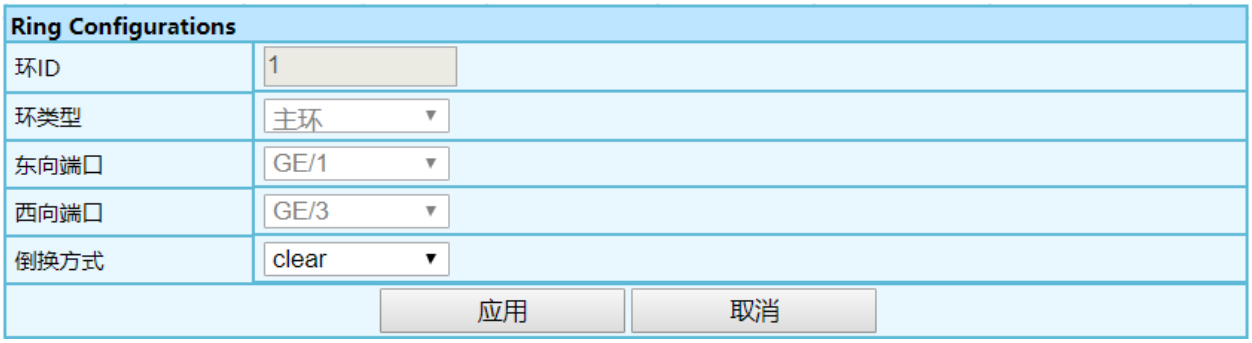



**图 8.4 ERPS 流量倒换配置界面**

另外做下说明，环倒换分为 FS（强制倒换）和 MS（手工倒换），倒换实际的操作就是将倒换指定的端口设置成 block 状态，然后清除转发表，这样，相对于这个端口而言，流量的方向就倒换了；其次 ERPS 的操作是有先后次序的，当存在优先次序高的事件时，优先次序低的就不会被相应，优先次序如图 8.5，据图可知，clear 操作的优先级是最高的，不管目前有何种事件发生，只要执行 clear 操作，都会清除掉当前的倒换配置；FS 操作次之；SF 表示的是故障，local SF 表示本地故障，R-APS(SF)表示的是收到别的地方传来的故障，SF 优先级高于 SF（包括 local SF 和 R-APS(SF)），所以即使当前系统处于故障状态，如果下发 FS 操作，系统依然会相应病执行；MS 在 SF 和 R-APS(MS)（R-APS(MS)表示的是别的设备执行了 MS 操作）之后，所以，如果系统在故障状态，或者环中别的设备执行了 MS 操作，当前新下发的 MS 操作不会被执行。后面几个事件是状态机事件，此处不必追究。

| Request/state and status | Type | Priority |
|---|---|---|
| Clear | local | highest |
| FS | local | \| |
| R-APS (FS) | remote | \| |
| local SF [a)] | local | \| |
| local clear SF | local | \| |
| R-APS (SF) | remote | \| |
| R-APS (MS) | remote | \| |
| MS | local | \| |
| WTR Expires | local | \| |
| WTR Running | local | \| |
| WTB Expires | local | \| |
| WTB Running | local | \| |
| R-APS (NR, RB) | remote | \| |
| R-APS (NR) | remote | lowest |
| [a)] If an Ethernet ring node is in the Forced switch state, local SF is ignored. | | |

图 8.5 ERPS 流量倒换配置界面

7. 单击[删除]按钮，删除对应的环。

## 配置项说明

ERPS[全局配置]相关界面的配置项说明。

表 8.1 ERPS[全局配置]环界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 环ID | 需要创建的环ID |
| 环类型 | 选择需要创建的环的类型 |
| 节点类型 | 本节点在环中的角色 |
| 协议VLAN | 所创建的环的ERPS协议VLAN |
| 东向端口 | 本节点上所创建环的一个环端口 |
| 西向端口 | 本节点上所创建环的另一个环端口 |
| RPL端口 | 如果节点类型为RPL-OWNER或者RPL-NEIGHBOUR时，需选择RPL端口 |
| 所属主环 | 当所创建的环为子环，且本节点为相交节点时，需指定所属于的主环 |

| | |
|---|---|
| 子环虚拟信道 | 主环中传输子环协议信息的通路 |
| WTR定时器 | 配置WTR定时器的值 |
| Guard定时器 | 配置guard定时器的值 |
| HoldOff定时器 | 配置holdOff定时器的值 |

**表 8.2 ERPS[全局配置]环修改界面的配置项说明**

| 配置项 | 说明 |
|---|---|
| 环ID | 需要修改的环ID |
| 环类型 | 需要修改的环的类型 |
| 子环虚拟信道 | 主环中传输子环协议信息的通路 |
| WTR定时器 | 配置WTR定时器的值 |
| Guard定时器 | 配置guard定时器的值 |
| HoldOff定时器 | 配置holdOff定时器的值 |

**表 8.3 ERPS[全局配置]流量倒换界面的配置项说明**

| 配置项 | 说明 |
|---|---|
| 环ID | 需要修改的环ID |
| 环类型 | 需要修改的环的类型 |
| 东向端口 | 本节点上所创建环的一个环端口 |
| 西向端口 | 本节点上所创建环的另一个环端口 |
| 倒换方式 | 流量倒换方式 |

## 8.5 环网信息

### 配置步骤

1. 在导航栏中选择[高级配置/ERPS/环网信息]，进入 ERPS[环网信息]显示界面。
2. 在[环网信息]界面中可以查看 ERPS 的当前运行信息，如图 8.5。
2. 单击[刷新]，可显示最新的运行信息。

展开 | 闭合

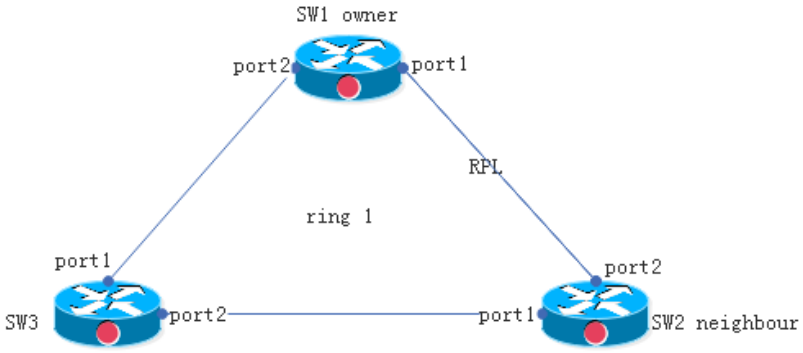
| 环ID:1 | | | | | |
|---|---|---|---|---|---|
| 环类型 | 主环 | 节点类型 | transfer | 协议VLAN | 1 |
| 返回模式 | revertive | FSM状态 | protection | 子环虚拟信道 | with |
| 东向端口 | GE/1/blocking | 西向端口 | GE/3/blocking | 所属主环 | N/A |
| Guard定时器 | 500毫秒 | HoldOff定时器 | 0毫秒 | WTB定时器 | 5000毫秒 |
| WTR定时器 | 1分钟 | 强制倒换 | 禁止 | 手工倒换 | 禁止 |

刷新

图 8.5 ERPS 信息显示界面

# 8.6 配置实例

## 8.6.1 单环配置实例




按如图拓扑，首先，配置 vlan，所有环端口都需要允许协议 VLAN 通过，VLAN 配置不再赘述，环配置如下：

SW1 web 配置如图：

| Ring Adding | | |
|---|---|---|
| 环ID | 1 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | rpl-owner | |
| 协议VLAN | 1 | <1-4094> |
| 东向端口 | GE/1 | |
| 西向端口 | GE/2 | |
| RPL 端口 | 东向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

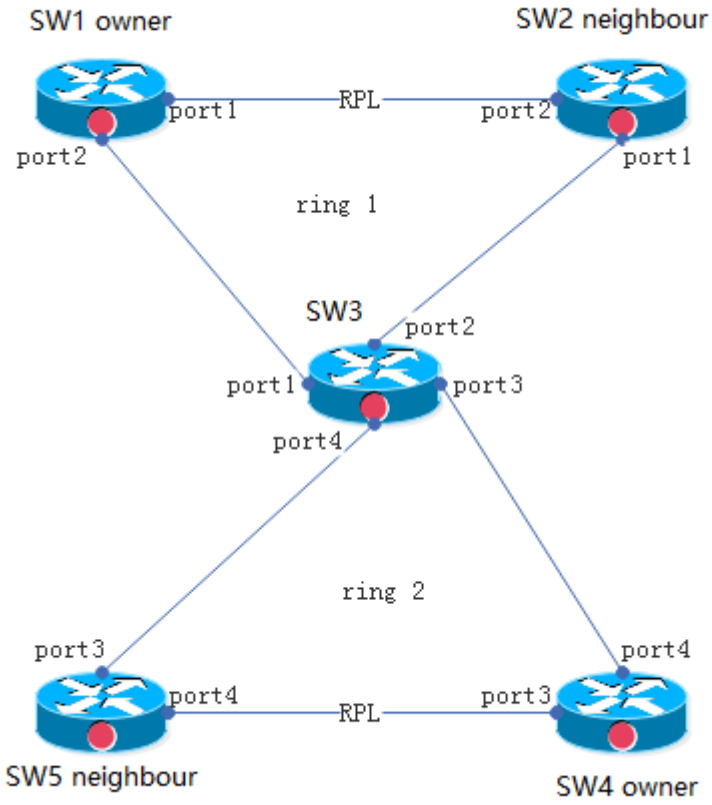
SW2 web 配置如图：

| Ring Adding | |
|---|---|
| 环ID | 1 <1-255> |
| 环类型 | 主环 |
| 节点类型 | rpl-neighbou |
| 协议VLAN | 1 <1-4094> |
| 东向端口 | GE/1 |
| 西向端口 | GE/2 |
| RPL 端口 | 西向端口 |
| 所属主环 | none |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 |

SW3 web 配置如图：

| Ring Adding | |
|---|---|
| 环ID | 1 <1-255> |
| 环类型 | 主环 |
| 节点类型 | transfer |
| 协议VLAN | 1 <1-4094> |
| 东向端口 | GE/1 |
| 西向端口 | GE/2 |
| RPL 端口 | none |
| 所属主环 | none |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 |

### 8.6.2 相切环配置实例




按如图拓扑，先配置 VLAN，对应的环的端口需要允许相应的环的协议 VLAN 通过，VLAN 配置不再赘述，相切环配置如下：

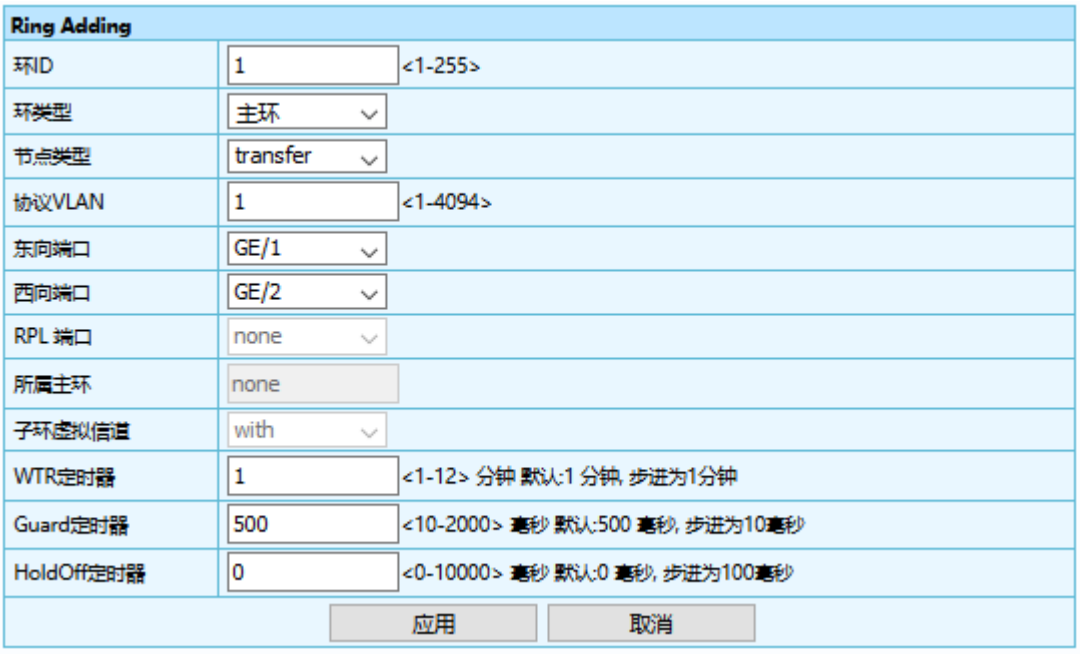
SW1 web 配置如图：

| Ring Adding | |
|---|---|
| 环ID | 1 <1-255> |
| 环类型 | 主环 |
| 节点类型 | rpl-owner |
| 协议VLAN | 1 <1-4094> |
| 东向端口 | GE/1 |
| 西向端口 | GE/2 |
| RPL 端口 | 东向端口 |
| 所属主环 | none |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 取消 | |

SW2 web 配置如图：


SW3 web 配置如图：

创建环 1：




创建环 2：

| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | transfer | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | GE/3 | |
| 西向端口 | GE/4 | |
| RPL 端口 | none | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW4 web 配置如图：

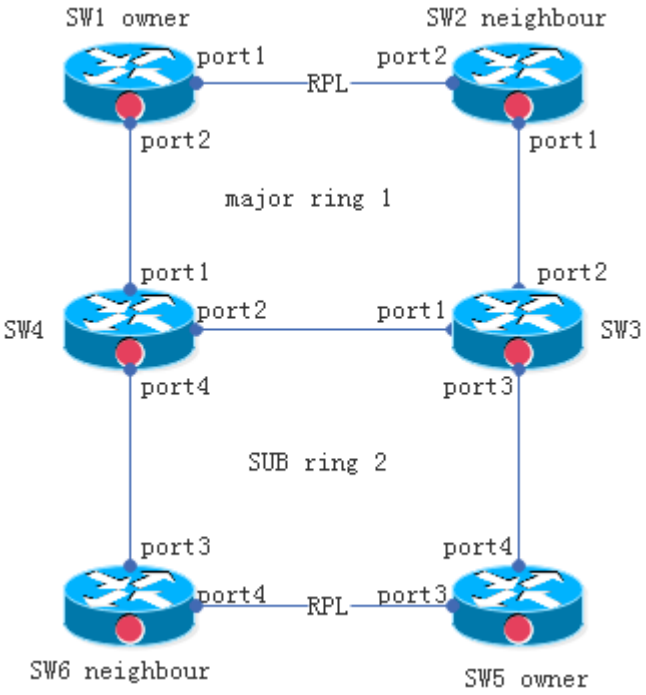
| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | rpl-owner | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | GE/3 | |
| 西向端口 | GE/4 | |
| RPL 端口 | 东向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW5 web 配置如图：

| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | rpl-neighbou | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | GE/3 | |
| 西向端口 | GE/4 | |
| RPL 端口 | 西向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

### 8.6.3 相交环配置实例

如下图拓扑，首先配置 VLAN，对应的环的端口需要允许相应的协议 VLAN 通过，同时，主环的环端口还需要允许子环的协议 VLAN 通过，VLAN 配置不再赘述，相交环配置如下：




SW1 web 配置如图；

| Ring Adding | | |
|---|---|---|
| 环ID | 1 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | rpl-owner | |
| 协议VLAN | 1 | <1-4094> |
| 东向端口 | GE/1 | |
| 西向端口 | GE/2 | |
| RPL 端口 | 东向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW2 web 配置如图；

| Ring Adding | | |
|---|---|---|
| 环ID | 1 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | rpl-neighbou | |
| 协议VLAN | 1 | <1-4094> |
| 东向端口 | GE/1 | |
| 西向端口 | GE/2 | |
| RPL 端口 | 西向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW3 web 配置如图；

创建主环 1：

| Ring Adding | | |
|---|---|---|
| 环ID | 1 | <1-255> |
| 环类型 | 主环 | |
| 节点类型 | transfer | |
| 协议VLAN | 1 | <1-4094> |
| 东向端口 | GE/1 | |
| 西向端口 | GE/2 | |
| RPL 端口 | none | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

创建子环 2：

| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 子环 | |
| 节点类型 | transfer | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | none | |
| 西向端口 | GE/3 | |
| RPL 端口 | none | |
| 所属主环 | 1 | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW4 web 配置如图；

创建主环 1：

| Ring Adding | |
|---|---|
| 环ID | 1 <1-255> |
| 环类型 | 主环 |
| 节点类型 | transfer |
| 协议VLAN | 1 <1-4094> |
| 东向端口 | GE/1 |
| 西向端口 | GE/2 |
| RPL 端口 | none |
| 所属主环 | none |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 取消 | |

创建子环 2：

| Ring Adding | |
|---|---|
| 环ID | 2 <1-255> |
| 环类型 | 子环 |
| 节点类型 | transfer |
| 协议VLAN | 2 <1-4094> |
| 东向端口 | none |
| 西向端口 | GE/4 |
| RPL 端口 | none |
| 所属主环 | 1 |
| 子环虚拟信道 | with |
| WTR定时器 | 1 <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 取消 | |

SW5 web 配置如图；

创建子环 2：

| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 子环 | |
| 节点类型 | rpl-owner | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | GE/3 | |
| 西向端口 | GE/4 | |
| RPL 端口 | 东向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

SW6 web 配置如图；

创建子环 2：

| Ring Adding | | |
|---|---|---|
| 环ID | 2 | <1-255> |
| 环类型 | 子环 | |
| 节点类型 | rpl-neighbou | |
| 协议VLAN | 2 | <1-4094> |
| 东向端口 | GE/3 | |
| 西向端口 | GE/4 | |
| RPL 端口 | 西向端口 | |
| 所属主环 | none | |
| 子环虚拟信道 | with | |
| WTR定时器 | 1 | <1-12> 分钟 默认:1 分钟, 步进为1分钟 |
| Guard定时器 | 500 | <10-2000> 毫秒 默认:500 毫秒, 步进为10毫秒 |
| HoldOff定时器 | 0 | <0-10000> 毫秒 默认:0 毫秒, 步进为100毫秒 |
| 应用 | 取消 | |

# 第九章 LLDP

本章对 LLDP 进行详细的描述，主要包括以下内容：

- LLDP 概述
- LLDP 技术介绍
- LLDP 配置

## 9.1 LLDP 概述

LLDP 是一个用于信息通告和获取的协议，但是需要注意的一点是，LLDP 发送的信息通告不需要确认,不能发送一个请求来请求获取某些信息,也就是说 LLDP 是一个单向的协议，只有主动通告一种工作方式，无需确认，不能查询、请求（比如像 ARP 协议那样请求某个 IP 的 MAC 地址）

## 9.2 LLDP 技术介绍

LLDP 主要完成如下工作：

- 初始化并维护本地 MIB 库中的信息
- 从本地 MIB 库中提取信息，并将信息封装到 LLDP 帧中。LLDP 帧的发送有两种触发方式，一是定时器到期触发，一是设备状态发生了变化触发。
- 识别并处理接收到的 LLDPDU 帧
- 维护远端设备 LLDP MIB 信息库
- 当本地或远端设备 MIB 信息库中有信息发生变化时，发出通告事件

## 9.3 LLDP 配置

### 9.3.1 LLDP 全局设置

**配置步骤**

1. 在导航栏中选择[管理设置/LLDP/全局设置]，进入 LLDP[全局设置]界面。
2. 在 LLDP[全局设置]界面中可以查看 LLDP 的全局配置，如图 9.1。
3. 如需修改 LLDP 的全局配置，在 LLDP 全局配置框中修改相应配置，然后单击<应用>。


图 9.1 LLDP 全局设置

### 配置项说明

LLDP[全局配置]的相关界面的配置项说明。

表 9.1 LLDP[全局配置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| LLDP使能状态 | LLDP全局使能开关。<br>● 开启：使能LLDP功能；<br>● 关闭：关闭LLDP功能。<br>注意：默认关闭。 |
| 发送周期 | LLDP发送周期，范围为0-32768，默认值为30。 |
| 邻居老化系数 | LLDP邻居老化系数，范围为2-10，默认值为4。 |
| 重启延时时间 | LLDP重启延时时间，范围为1-10，默认值为2。 |
| 告警周期 | LLDP告警周期，范围为5-3600，默认值为30。 |
| 发送信用量 | LLDP发送信用量，范围为1-100，默认值为5。 |
| 快速发送周期 | LLDP快速发送周期，范围为1-3600，默认值为1。 |
| 快速发送数量 | 设置LLDP快速发送数量，范围为1-8，默认值为4。 |

## 9.3.2 LLDP 端口配置

### 配置步骤

1. 在导航栏中选择[管理设置/LLDP/端口配置]，进入 LLDP[端口配置]界面。
2. 在 LLDP[端口配置]界面中可以查看 LLDP 的端口相关配置。
3. 在 LLDP[端口配置]界面中目的地址一栏，在这可选择

0180C2-00000E,0180C2-000003，0180C2-000000 中任意一个目的地址对应的所有端口的 LLDP 配置，如图 9.2。

3．如需修改某个目的地址的某个端口的 LLDP 配置，在选择目的地址后单击对应端口显示栏后的<修改>按钮，进入端口配置界面，如图 9.3。

4．选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。


图 9.2 LLDP 目的地址选择界面


图 9.3 LLDP 端口配置界面

## 配置项说明

LLDP[端口配置]的相关界面的配置项说明。

表 9.2 LLDP[端口配置]界面配置项说明

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息。 |
| 目的地址 | LLDP目的地址（0180C2-00000E、0180C2-000003、0180C2-000000）。 |

| | |
|---|---|
| 管理状态 | 端口的LLDP状态：<br>● 只发送：只开启端口的LLDP的发送功能。<br>● 只接受：只开启端口的LLDP的接受功能。<br>● 发送和接受：开启端口的LLDP的发送和接受功能。<br>● 禁止：关闭端口的LLDP的发送和接受功能。<br>注：端口默认为禁止。 |
| 发送周期 | 端口的发送周期：<br>● 默认：发送周期采用全局配置的发送周期。<br>● 设置：设置发送周期，范围5-32768。<br>注：端口默认为默认状态。 |
| 邻居老化系数 | 端口的邻居老化系数：<br>● 默认：邻居老化系数采用全局配置的邻居老化系数。<br>● 设置：设置邻居老化系数，范围2-10。<br>注：端口默认为默认状态。 |
| 重启延时时间 | 端口的重启延时时间：<br>● 默认：重启延时时间采用全局配置的重启延时时间。<br>● 设置：设置重启延时时间，范围1-10。<br>注：端口默认为默认状态。 |
| 告警周期 | 端口的告警周期：<br>● 默认：告警周期采用全局配置的告警周期。<br>● 设置：设置告警周期，范围5-3600。<br>注：端口默认为默认状态。 |
| 发送信用量 | 端口的发送信用量：<br>● 默认：发送信用量采用全局配置的发送信用量。<br>● 设置：设置发送信用量，范围1-100。<br>注：端口默认为默认状态。 |
| 快速发送周期 | 端口的快速发送周期：<br>● 默认：快速发送周期采用全局配置的快速发送周期。<br>● 设置：设置快速发送周期，范围1-3600。 |

| | |
|---|---|
| | 注：端口默认为默认状态。 |
| 快速发送数量 | 端口的快速发送数量：<br>● 默认：快速发送数量采用全局配置的快速发送数量。<br>● 设置：设置快速发送数量，范围1-8。<br>注：端口默认为默认状态。 |
| 告警使能 | 端口的告警使能：<br>● 使能：开启端口的LLDP的告警功能。<br>● 禁止：关闭端口的LLDP的告警功能。<br>注：默认为禁止。 |
| TLVs发送使能 | 支持选择端口描述、系统名称、系统描述、系统能力一种或多种TLVs发送使能内容。 |

# 第十章 802.1X

本章对 802.1x 进行详细的描述，主要包括以下内容：

- 802.1x 概述
- 802.1x 技术介绍
- 802.1x 工作原理
- 认证服务器
- 全局设置
- 端口配置
- 用户认证信息

## 10.1 802.1x 概述

802.1x 协议是基于 Client/Server 的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口(access port)访问 LAN/WLAN。在获得交换机或 LAN 提供的各种业务之前，802.1x 对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1x 只允许 EAPoL（基于局域网的扩展认证协议）数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

## 10.2 802.1x 技术介绍

基于以太网端口认证的 802.1x 协议有如下特点：IEEE802.1x 协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有效降低建网成本；借用了在 RAS 系统中常用的 EAP（扩展认证协议），可以提供良好的扩展性和适应性，实现对传统 PPP 认证架构的兼容；802.1x 的认证体系结构中采用了"可控端口"和"不可控端口"的逻辑功能，从而可以实现业务与认证的分离，由 RADIUS 和交换机利用不可控的逻辑端口共同完成对用户的认证与控制，业务报文直接承载在正常的二层报文上通过可控端口进行交换，通过认证之后的数据包是无需封装的纯数据包；可以使用现有的后台认证系统降低部署的成本，并有丰富的业务支持；可以映射不同的用户认证等级到不同的 VLAN；可以使交换端口和无线 LAN 具有安全的认证接入功能。

## 10.3 802.1x 工作原理

1.当用户有上网需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

2.交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名送上来。

3.客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

4.认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

5.客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理（此种加密算法通常是不可逆的），并通过交换机传给认证服务器。

6.认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的指令，允许用户的业务流通过端口访问网络。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，只允许认证信息数据通过而不允许业务数据通过。

# 10.4 认证服务器

## 配置步骤

1. 在导航栏中选择[高级配置/802.1X/认证服务器]，进入[认证服务器设置]界面。
2. 在认证服务器设置界面中可以查看认证服务器的配置信息。
3. 如需修改认证服务器配置，可在认证服务器配置框中修改相应配置，然后单击<应用>，如图 10.1 所示。


图 10.1 认证服务器配置界面

## 配置项说明

表 10.1 802.1X 认证服务器配置项说明

| 配置项 | 说明 |
|---|---|
| 主机 | Radius认证服务器的IP，IPv4，点分十进制格式 |
| 端口号 | Radius认证服务器的的端口号，范围<1-65535>，默认为1812 |
| 共享密钥 | 必须与Radius服务器一致，否则无法通过认证。字符串格式，且只能包含字母，数字，下划线，长度不超过20 |

# 10.5 全局设置

## 配置步骤

1. 在导航栏中选择[高级配置/802.1X/全局配置]，进入[全局配置]界面。
2. 在全局界面中可以查看全局配置信息。
3. 如需修改全局配置，可在全局配置框中修改相应配置，然后单击<应用>，如图 10.2。


图 10.2 全局配置界面

## 配置项说明

表 10.2 802.1X 全局配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | • 禁止：禁止全局802.1X<br>• 使能：使能全局802.1X |
| 重认证 | • 禁止：禁止重认证功能<br>• 使能：使能重认证功能 |
| 静默功能 | • 禁止：禁止静默功能<br>• 使能：使能静默功能 |
| 认证方法 | • EAP<br>• PAP<br>• CHAP |
| 请求报文发送超时定时器 | 整数1-120，默认30 |
| 客户端超时定时器 | 整数1-120，默认30 |
| 服务器超时定时器 | 整数1-120，默认30 |
| 重认证定时器 | 整数60-7200，默认3600 |
| 静默定时器 | 整数10-3600，默认60 |

## 10.6 端口配置

### 配置步骤

1．在导航栏中选择[高级配置/802.1X/端口配置]，进入[端口配置]界面。

2．[端口配置]界面，可以查看每个端口的配置信息，如图 10.3 所示，显示了每个端口当前的 802.1X 配置信息。

| 端口 | 管理状态 | 接口控制模式 | 接口认证模式 | 最大支持主机数 | 设置 |
|---|---|---|---|---|---|
| GE/1 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/2 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/3 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/4 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/5 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/6 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/7 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/8 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/9 | 禁止 | 自动 | PortBased | 8 | 修改 |
| GE/10 | 禁止 | 自动 | PortBased | 8 | 修改 |

图 10.3 802.1X 端口配置信息

3. 如需修改某个端口的配置，只需单击界面中对应条目右侧的[修改]按钮，进入修改界面，如图 10.4 所示。修改相应的配置项。单击[应用]按钮完成修改，单击[取消]按钮取消修改。


图 10.4 802.1X 端口配置界面

注意事项：802.1X 端口配置更改接口认证模式时，会导致该端口下所有已认证通过的用户全部下线，需要重新认证才能访问网络。

**配置项说明**

表 10.3 802.1X 端口配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | • 禁止：禁止端口802.1X<br>• 使能：使能端口802.1X |
| 接口控制模式 | • 自动：认证前无法访问网络，认证通过后可以访问网络<br>• 强制授权：始终可以访问网络<br>• 强制非授权：始终无法访问网络 |
| 接口认证模式 | 基于端口：一个用户通过认证后，该端口下的所有用户都可以访问网络<br>基于MAC:所有用户都需要单独认证通过后才能访问网络 |
| 最大支持主机数 | 端口支持的最大认证主机数目，超过该数后无法认证。整数1-8，默认8 |

## 10.7 用户认证信息

**配置步骤**

1. 在导航栏中选择[高级配置/802.1X/用户认证信息]，进入[用户认证信息]界面。

2. 单击左上角的<展开>可以展开所有端口当前的用户认证信息,单击<闭合>可以闭合所有端口的用户认证信息。单击⊞图标可以展开相应端口的用户认证信息，单击⊟图标可以闭合相应端口的用户认证信息。

3. 在该界面可以查看到用户的认证信息包括：用户名，客户端 MAC 地址，认证通过的时间。

4. 单击下方的<刷新>可以刷新当前的用户认证信息。

# 第十一章 环路检测

本章对环路检测进行详细的描述，主要包括以下内容：

- 环路检测概述
- 环路检测技术介绍
- 全局配置
- 端口配置

## 11.1 环路检测概述

网络连接或配置的错误容易导致二层网络中出现转发环路，使设备对广播、组播以及未知单播等报文重复发送，造成网络资源的浪费甚至网络瘫痪，于是环路检测孕育而生，专门为了有效的防止环路，确保了网络的稳定与安全。

## 11.2 环路检测技术介绍

为了能够及时发现二层网络中的环路，以避免对整个网络造成严重影响，需要提供一种监测机制，使网络中出现环路时能及时通知用户检查网络连接和配置情况，并能够自动关闭出问题的端口以消除环路，这种机制就是环路监测机制。

当网络中出现环路时，环路监测机制通过打印日志信息(log)和发送告警信息(trap)以通知用户，同时还可根据用户事先的配置来选择是否关闭出现环路的端口。

## 11.3 全局配置

**配置步骤**

1. 在导航栏中选择[高级配置/环路检测/全局配置]，进入[全局配置]界面。
2. 在全局配置界面中可以查看全局配置信息。
3. 如需修改全局配置，可在认全局配置框中修改相应配置，然后单击<应用>，如图11.1 所示。

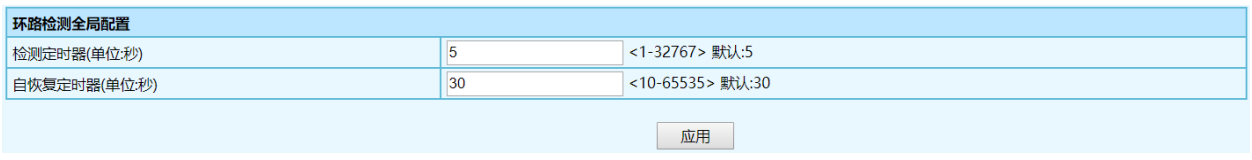



**图 11.1 环路检测全局配置界面**

**配置项说明**

表 11.1 环路检测全局配置项说明

| 配置项 | 说明 |
| --- | --- |
| 检测定时器 | 环路检测报文发送周期，范围<1-32767>，默认5 |
| 自恢复定时器 | 端口自动恢复周期，范围<10-65535>，必须不小于2倍检测定时器 |

## 11.4 端口配置

**配置步骤**

1. 在导航栏中选择[高级配置/环路检测/端口配置]，进入[端口配置]页面。

2. 在端口配置页面中可以看到所有端口的环路检测配置信息和运行状态，如图 11.2 所示。

3. 如需修改某个端口的配置，只需单击页面中对应条目右侧的[修改]按钮，进入修改界面，如图 11.3 所示。修改相应的配置项。单击[应用]按钮完成修改，单击[取消]按钮取消修改。

4. 某个端口出现环路按指定的动作关闭或者阻塞端口后，如果想立即恢复可以点击页面中对应条目右侧的<立即恢复>按钮恢复端口。

| 端口 | 管理状态 | 恢复模式 | 执行操作 | 端口状态 | 设置 |
| --- | --- | --- | --- | --- | --- |
| GE/1 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/2 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/3 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/4 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/5 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/6 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/7 | 禁止 | 自动 | 关闭 | 断开 | 修改 立即恢复 |
| GE/8 | 禁止 | 自动 | 关闭 | 连接 | 修改 立即恢复 |
| GE/9 | 禁止 | 自动 | 关闭 | 连接 | 修改 立即恢复 |
| GE/10 | 禁止 | 自动 | 关闭 | 连接 | 修改 立即恢复 |

图 11.2 环路检测端口配置和运行状态查看界面


图 11.3 环路检测端口配置界面

## 配置项说明

**表 11.2 环路检测端口配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | • 禁止：禁止环路检测功能<br>• 使能：使能环路检测功能 |
| 恢复模式 | • 自动：出现环路以后，端口关闭或者阻塞，端口自动恢复<br>• 手动：出现环路以后，端口关闭或者阻塞，需要手动恢复端口 |
| 执行操作 | • 关闭：出现环路后，端口关闭<br>• 阻塞：出现环路后，端口阻塞 |

# 第十二章 组播管理

本章对组播管理进行详细的描述，主要包括以下内容：

- 组播概述
- IGMP Snooping
- 组播表

## 12.1 组播概述

### 12.1.1 产生背景

传统的 IP 通信有两种方式：一种是在源主机与目的主机之间点对点的通信，即单播；另一种是在源主机与同一网段中所有其它主机之间点对多点的通信，即广播。如果要将信息发送给多个主机而非所有主机，若采用广播方式实现，不仅会将信息发送给不需要的主机而浪费带宽，也不能实现跨网段发送；若采用单播方式实现，重复的 IP 包不仅会占用大量带宽，也会增加源主机的负载。所以，传统的单播和广播通信方式不能有效地解决单点发送、多点接收的问题。

组播是指在 IP 网络中将数据包以尽力传送的形式发送到某个确定的节点集合（即组播组），其基本思想是：源主机（即组播源）只发送一份数据，其目的地址为组播组地址；组播组中的所有接收者都可收到同样的数据拷贝，并且只有组播组内的主机可以接收该数据，而其它主机则不能收到。

### 12.1.2 技术优点

组播技术有效地解决了单点发送、多点接收的问题，实现了 IP 网络中点到多点的高效数据传送，能够大量节约网络带宽、降低网络负载。作为一种与单播和广播并列的通信方式，组播的意义不仅在于此。更重要的是，可以利用网络的组播特性方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等互联网的信息服务领域。

### 12.1.3 IP 组播地址到链路层的映射

由于本设备为二层设备，故只讨论数据链路层协议的组播实现。

IANA 将 MAC 地址范围 01:00:5E:00:00:00～01:00:5E:7F:FF:FF 分配给组播使用，这就要求将 28 位的 IP 组播地址空间映射到 23 位的组播 MAC 地址空间中，具体的映射方法是将组播地址中的低 23 位放入 MAC 地址的低 23 位。

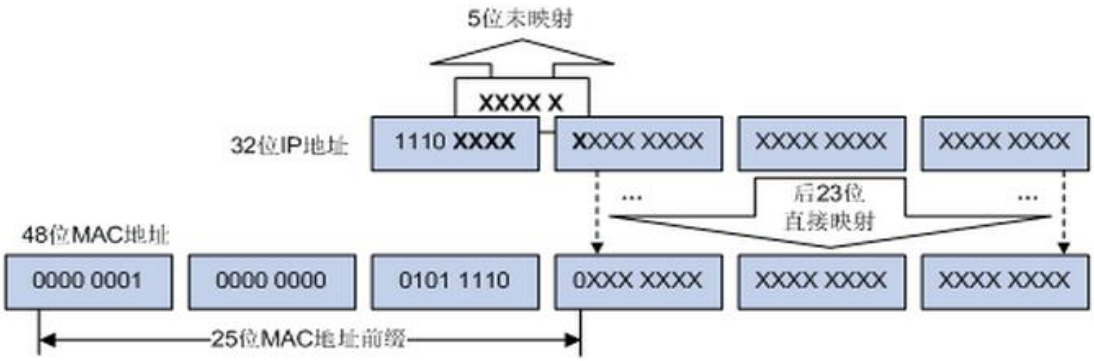



**图 12.1 IP 组播地址到组播 MAC 地址的映射**

由于 IP 组播地址的后 28 位中只有 23 位被映射到组播 MAC 地址，这样会有 32 个 IP 组播地址映射到同一组播 MAC 地址上。

### 12.1.4 IGMP

IGMP 运行于主机和与主机直连的路由器之间，其实现的功能是双向的：一方面，主机通过 IGMP 通知路由器希望接收某个特定组播组的信息；另一方面，路由器通过 IGMP 周期性地查询局域网内的组播组成员是否处于活动状态，实现所连网段组成员关系的收集与维护。通过 IGMP，在路由器中记录的信息是某个组播组是否在本地有组成员，而不是组播组与主机之间的对应关系。

**表 12.1 IGMP 版本说明**

| IGMP版本 | 版本特点 |
|---|---|
| IGMPv1(RFC 1112) | 定义了基本的组成员查询和报告过程 |
| IGMPv2(RFC 2236) | 在IGMPv1的基础上添加了组成员快速离开的机制等 |
| IGMPv3(RFC 3376) | 增加的主要功能是成员可以指定接收或拒绝来自某些组播源的报文，以实现对SSM模型的支持 |

IGMPv2 为目前主要使用版本。

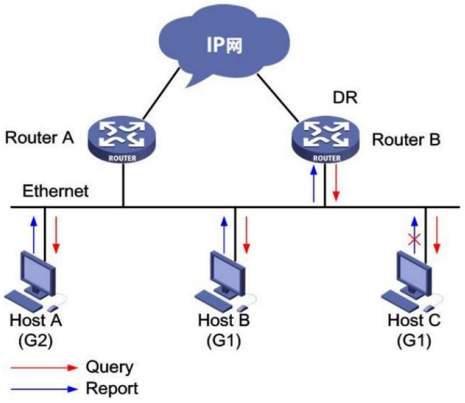



**图 12.2 IGMPv2 工作原理**

当同一个网段内有多个 IGMP 路由器时，IGMPv2 通过查询器选举机制从中选举出唯一的查询器。查询器周期性地发送普遍组查询消息进行成员关系查询，主机通过发送报告消息来响应查询。而作为组成员的路由器，其行为也与普通主机一样，响应其它路由器的查询。

当主机要加入组播组时，不必等待查询消息，而是主动发送报告消息；当主机要离开组播组时，也会主动发送离开组消息，查询器收到离开组消息后，会发送特定组查询消息来确定该组的所有组成员是否都已离开。

通过上述机制，在路由器里建立起一张表，其中记录了路由器各接口所对应子网上都有哪些组的成员。当路由器收到发往组 G 的组播数据后，只向那些有 G 的成员的接口转发该数据。至于组播数据在路由器之间如何转发则由组播路由协议决定，而不是 IGMP 的功能。

### 12.1.5 IGMP 版本

**IGMP V1 工作机制**

IGMP V1 主要基于查询和响应机制来完成对组播组成员的管理。当一个网段内有多台组播路由器时，由于它们都能从主机那里收到 IGMP 成员关系报告报文（Membership ReportMessage），因此只需要其中一台路由器发送 IGMP 查询报文（Query Message）就足够了。这就需要有一个查询器（Querier）的选举机制来确定由哪台路由器作为 IGMP 查询器。对于 IGMP V1 来说，由组播路由协议（如 PIM）选举出唯一的组播信息转发者 DR（Designated Router，指定路由器）作为 IGMP 查询器。IGMP V1 没有专门定义离开组播组的报文。当运行 IGMP V1 的主机离开某组播组时，将不会向其要离开的组播组发送报告报文。当网段中不再存在该组播组的成员后，IGMP 路由器将收不到任何发往该组播组的报告报文，于是 IGMP 路由器在一段时间之后便删除该组播组所对应的组播转发项。

**IGMP V2 的改进**

与 IGMP V1 相比，IGMP V2 增加了查询器选举机制和离开组机制。

**（1）查询器选举机制**

在 IGMP V1 中，当某共享网段上存在多个组播路由器时，由组播路由协议（如 PIM）选举的指定路由器充当查询器。在 IGMP V2 中，增加了独立的查询器选举机制，其选举过程如下：

①所有 IGMP V2 路由器在初始时都认为自己是查询器，并向本地网段内的所有主机和路由器发送 IGMP 普遍组查询（General Query）报文（目的地址为:224.0.0.1）；

②本地网段中的其它 IGMP V2 路由器在收到该报文后， 将报文的源 IP 地址与自己的接口地址作比较。通过比较，IP 地址最小的路由器将成为查询器，其它路由器成为非查询器（Non-Querier）；

③所有非查询器上都会启动一个定时器（即其它查询器存在时间定时器 Other QuerierPresent Timer）。在该定时器超时前，如果收到了来自查询器的 IGMP 查询报文，则重置该定时器；否则，就认为原查询器失效，并发起新的查询器选举过程。

**（2）离开组机制**

在 IGMP V1 中，主机离开组播组时不会向组播路由器发出任何通知，导致组播路由器只能依靠组播组成员查询的响应超时来获知组播组成员的离开。而在 IGMP V2 中，当一个主机离开某组播组时：

①该主机向本地网段内的所有组播路由器（目的地址为 224.0.0.2）发送离开组（LeaveGroup）报文；

② 当查询器收到该报文后；向该主机所声明要离开的那个组播组发送特定组查询（Group-Specific Query）报文（目的地址字段和组地址字段均填充为所要查询的组播组地址）；

③如果该网段内还有该组播组的其它成员，则这些成员在收到特定组查询报文后，会在该报文中所设定的最大响应时间（Max Response Time）内发送成员关系报告报文；

④如果在最大响应时间内收到了该组播组其它成员发送的成员关系报告报文，查询器就会继续维护该组播组的成员关系；否则，查询器将认为该网段内已无该组播组的成员，于是不再维护这个组播组的成员关系。

# 12.2 IGMP snooping

## 12.2.1 IGMP Snooping 介绍

igmp Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束的机制，用于管理和控制组播组。

### 12.2.2 IGMP Snooping 技术介绍

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

IGMP Snooping 和 IGMP 协议一样，两者都用于组播组的管理和控制，它们都使用 IGMP 报文。IGMP 协议运行在网络层，而 IGMP Snooping 则运行在链路层，当二层以太网交换机收到主机和路由器之间传递的 IGMP 报文时，IGMP Snooping 分析 IGMP 报文所带的信息，在二层建立和维护 MAC 表，以后从路由器下发的组播报文就根据 MAC 表进行转发。IGMP Snooping 只有在收到某一端口的 IGMP 离开报文或者某一端口的老化时间定时器超时的时候才会主动向端口发 IGMP 特定组查询报文，除此之外，它不会向端口发任何 IGMP 报文。

IGMP Snooping，就是监听 IGMP 协议包，提取相应的信息，形成组播成员关系表，然后对组播业务按照组成员关系进行转发，保证组成员收到正确的的组播业务，而其余主机无法收到。

IGMP Snooping 相对于路由器和主机是透明的，它仅仅监听两者之间的 IGMP 报文，来建立自己的组播成员关系表。

### 12.2.3 全局设置

#### 配置步骤

1. 在导航栏中选择[高级配置/IGMP snooping/全局设置]，进入 [全局设置]界面。
2. 在 IGMP snooping[全局设置]界面中可以查看 IGMP snooping 的全局配置信息。
3. 如需修改 IGMP snooping 的全局配置，可在配置框中修改相应配置，然后单击<应用>，如图 12.3。


图 12.3 IGMP snooping 全局设置界面

### 配置项说明

IGMP snooping[全局设置]界面的配置项说明。

**表 12.3 IGMP snooping[全局设置]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | 选择IGMP Snooping的全局使能状态：<br>• 使能：使能IGMP snooping功能；<br>• 禁止：关闭IGMP snooping功能。<br>注：默认禁止。 |
| 绑定的VLAN | 绑定的VLAN列表。 |
| 添加或删除VLAN | 选择对VLAN的操作，并输入要添加或删除的VLAN列表：<br>• 添加：添加VLAN，格式如：1-10,13,15-4094；<br>• 删除：删除VLAN，格式如：1-10,13,15-4094。 |
| 路由端口老化时间 | 有效的路由端口老化时间，范围为30-300，默认为105，单位为秒。 |
| 主机端口老化时间 | 有效的主机端口老化时间，范围为60-600，默认为260，单位为秒。 |

## 12.2.4 VLAN 设置

### 配置步骤

1. 在导航栏中选择[高级配置/IGMP snooping/VLAN 设置]，进入到[VLAN 设置]界面，如图 12.4。


**图 12.4 IGMP snooping VLAN 设置界面**

2. IGMP snooping[VLAN 设置]界面展示了 IGMP Snooping 的所有绑定的 VLAN 配置信息。

3. 修改单个绑定 VLAN 配置信息。进入[VLAN 设置]界面后，单击将要修改的条目右侧的<修改>按键，进入修改界面，如图 12.5。输入有效的配置参数，单击<应用>提交修改。单击<取消>放弃修改。


图 12.5 IGMP snooping VLAN 配置修改界面

4. 批量绑定 VLAN 配置信息。进入[VLAN 设置]界面后，单击页面底部的[批量配置]按键，进入[VLAN 批量配置]界面，如图 12.6。输入有效的配置参数，单击<应用>提交修改。单击<取消>放弃修改。

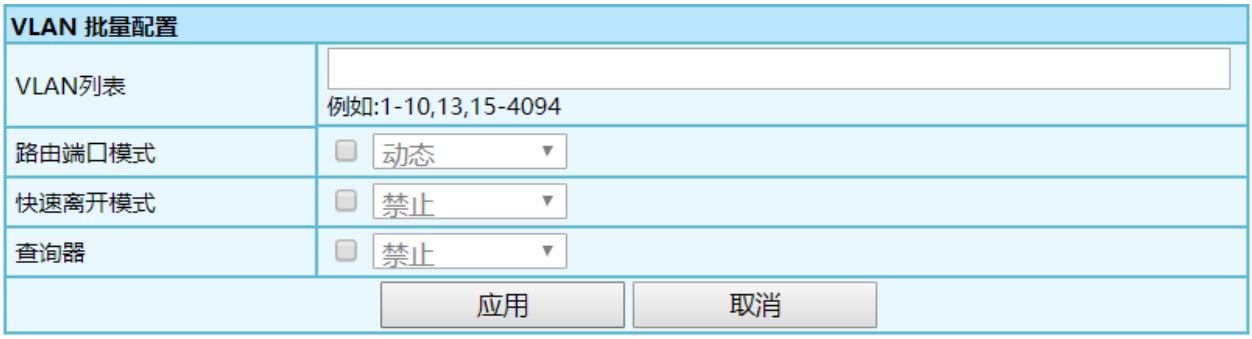



图 12.6 IGMP snooping VLAN 批量配置界面

### 配置项说明

IGMP snooping[VLAN 设置]界面的配置项说明。

**表 12.4 IGMP snooping[VLAN 设置]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| VLAN | 正在配置的VLAN。 |
| 路由端口模式 | 选择该VLAN下的路由端口的模式。通过下拉框进行修改。<br>• 动态<br>• 静态<br>--如果选择静态路由端口模式，还需要继续选择具体的路由端口，可通过复选按钮进行选择。 |
| 快速离开模式 | 选择是否使能该VLAN下的快速离开模式。通过下拉框进行修改。<br>• 禁止<br>• 使能 |
| 查询器 | 选择是否使能该VLAN下的查询器功能。通过下拉框进行修改。<br>• 禁止<br>• 使能<br>--如果使能了查询器，则需要设置相应的查询器间隔和查询源IP。 |
| 查询间隔 | 查询器的查询间隔时间范围为30-120，单位为秒。 |
| 查询器源IP地址 | 设置查询器发出的查询报文的源IP地址，有效的单播地址，如“192.168.1.11”，<br>“0.0.0.0”也可。 |

## 12.2.5 IP 组

### 配置步骤

1. 在导航栏中选择[高级配置/IGMP snooping/IP 组]，进入[IP 组]界面，如图 12.7。

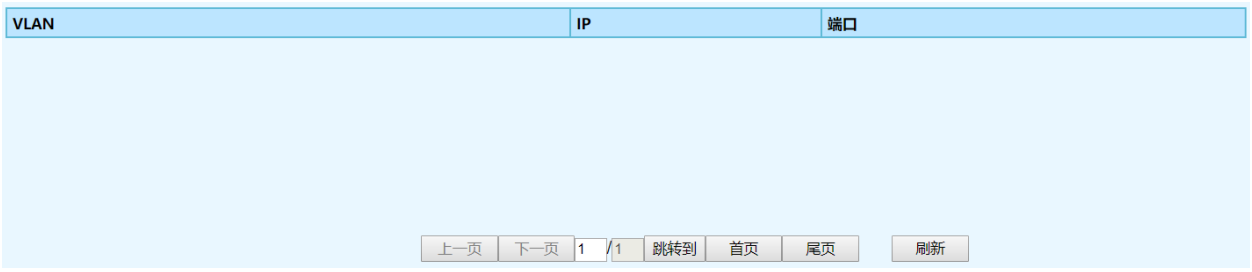


图 12.7 IGMP snooping IP 组界面

2. IGMP snooping[IP 组]界面展示了 IGMP Snooping 所维护的 IP 组信息，单击[刷新]按钮即可刷新。

### 12.2.6 MAC 组

#### 配置步骤

1. 在导航栏中选择[高级配置/IGMP snooping/MAC 组]，进入[MAC 组]界面，如图 12.8。

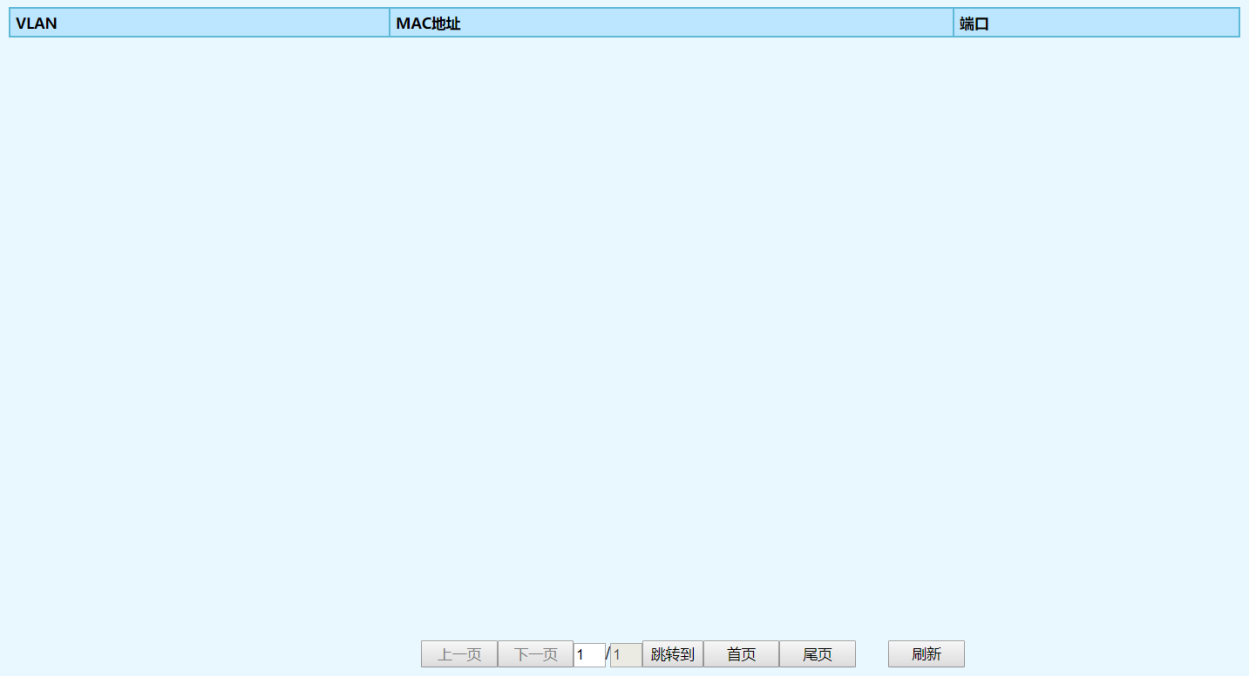



图 12.8 IGMP snooping MAC 组界面

2. IGMP snooping[MAC 组]界面展示了 IGMP Snooping 所维护的 MAC 组信息，单击[刷新]按钮即可刷新。

# 第十三章 安全配置

本章对安全配置进行详细的描述，主要包括以下内容：

- 风暴过滤
- 端口镜像
- 端口隔离

## 13.1 风暴过滤

### 13.1.1 广播风暴

所谓广播风暴，简单的讲，当广播数据充斥网络无法处理，并占用大量的网络宽带，导致正常业务不能运行，甚至彻底瘫痪，这就发生了“广播风暴”。一个数据帧被传输到本地网段(由广播域定义)上的每个节点就是广播；由于网络拓扑的设计和连接问题，或其他原因导致广播在网段内大量复制，传播数据帧，导致网络特性下降或网络瘫痪，这就是广播风暴。

### 13.1.2 风暴过滤介绍

交换机专用术语。网络上的广播帧（由于被转发）数量急剧增加而影响正常的网络通讯的反常现象，广播风暴会占用相当可观的网络带宽，造成整个网络无法正常工作。广播风暴控制是允许端口对网络上出现的广播风暴进行过滤。开启广播风暴控制后，当端口收到的广播帧累计到预定门限值时，端口将自动丢弃收到的广播帧。当未启用该功能或广播帧未累计到门限时，广播帧将被正常广播到交换机的其它端口。而本设备风暴过滤的对象分别为广播/未知单播/未知组播三种，对于三种报文的操作和工作原理均一样。

### 13.1.3 风暴过滤设置

**配置步骤**

1. 在导航栏中选择[基本配置/风暴过滤]，进入[风暴过滤]配置界面，如图 13.1 所示。

| 端口 | 广播报文 | 阈值(kbps) | 未知单播报文 | 阈值(kbps) | 未知组播报文 | 阈值(kbps) | 设置 |
|---|---|---|---|---|---|---|---|
| GE/1 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/2 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/3 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/4 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/5 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/6 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/7 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/8 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/9 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |
| GE/10 | 开启 | 64 | 关闭 | N/A | 关闭 | N/A | 修改 |

图 13.1 风暴过滤界面

2．[风暴过滤]界面显示了每个端口的广播风暴过滤的配置信息。

3．修改端口风暴过滤配置信息。单击要修改的条目右侧的[修改]按钮，进入[风暴过滤]修改界面，如图 13.2 所示。输入有效的配置参数，单击[应用]提交修改。单击[取消]放弃修改。


图 13.2 风暴过滤修改界面

## 配置项说明

表 13.1 风暴过滤配置项说明

| 配置项 | 说明 |
|---|---|
| 端口 | 修改配置的端口 |
| 广播报文 | 选择是否开启对广播报文的速率抑制。可通过单选按钮进行选择。<br>• 开启<br>--如果选择开启，则要输入相应的速率抑制值，<16-1000000>，步进为16，单位为kbps<br>• 关闭 |
| 未知单播报文 | 选择是否开启对未知单播报文的速率抑制。可通过单选按钮进行选择。<br>• 开启 --如果选择开启，则要输入相应的速率抑制值，<16-1000000>，步进为16，单位为kbps<br>• 关闭 |
| 未知组播报文 | 选择是否开启对未知组播报文的速率抑制。可通过单选按钮进行选择。<br>• 开启 --如果选择开启，则要输入相应的速率抑制值，<16-1000000>，步进为16，单位为kbps<br>• 关闭 |

## 13.2 端口镜像

### 13.2.1 端口镜像介绍

端口镜像（port Mirroring）功能通过在交换机或路由器上，将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”，在不严重影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。在企业中用镜像功能，可以很好地对企业内部的网络数据进行监控管理，在网络出故障的时候，可以快速地定位故障。

### 13.2.2 端口镜像技术介绍

镜像的功能简单地说就是将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析、流量备份等，监控端口一般直接与监控主机等相连。

监视到进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据，如网吧需提供此功能把数据发往公安部门审查。而企业出于信息安全、保护公司机密的需要，也迫切需要网络中有一个端口能提供这种实时监控功能。在企业中用端口镜像功能，可以很好的对企业内部的网络数据进行监控管理，在网络出现故障的时候，可以做到很好地故障定位。

(备注：交换机把某一个端口接收或发送的数据帧完全相同的复制给另一个端口；其中被复制的端口称为镜像源端口，复制的端口称为镜像目的端口)

### 13.2.3 端口镜像设置

**配置步骤**

1. 在导航栏中选择[基本配置/端口镜像]，进入[端口镜像]配置界面，如图 13.3 所示。

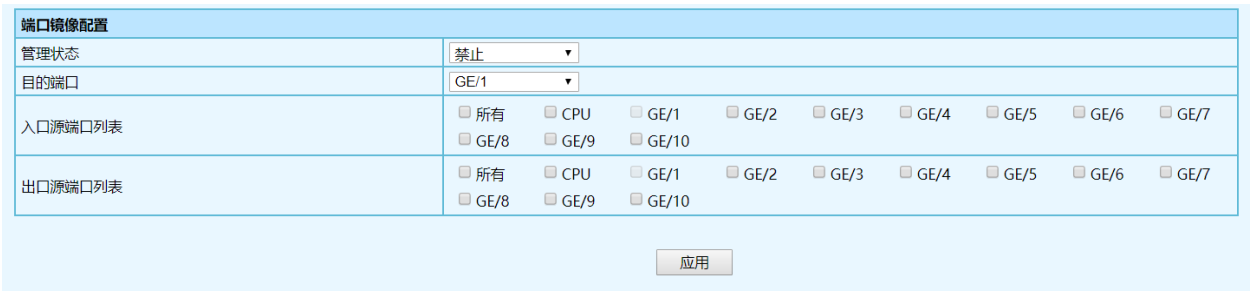



**图 13.3 端口镜像配置界面**

2. 修改端口镜像配置信息。通过下拉选择禁止或使能镜像，选择镜像目的端口，勾选入口端口和出口端口，入口或出口不能包含目的端口，单击[应用]提交修改。

**配置项说明**

**表 13.2 端口镜像配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | 选择是否使能端口镜像功能 |
| 目的端口 | 选择端口镜像的目的端口，可通过下拉框进行选择。 |
| 入口源端口列表 | 选择入口方向的源端口列表。可通过复选按钮进行选择。（源端口列表不能包含目的端口） |
| 出口源端口列表 | 选择出口方向的源端口列表。可通过复选按钮进行选择。（源端口列表不能包含目的端口） |

## 13.3 端口隔离

### 13.3.1 端口隔离介绍

端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，即可实现隔离组内端口之间二层数据通信的隔离。端口隔离功能为用户提供了更安全、更灵活、更便捷的组网方案。

### 13.3.2 端口隔离设置

**配置步骤**

1. 在导航栏中选择[基本配置/端口隔离]，进入[端口隔离]配置界面，如图 13.4 所示。

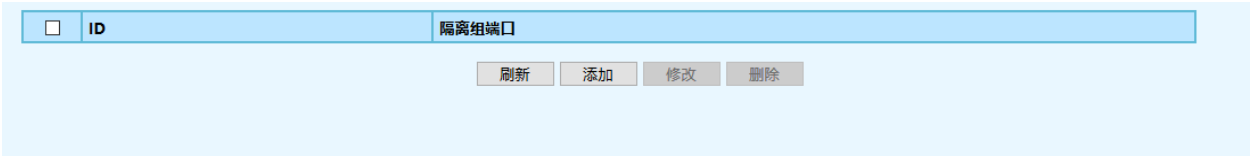



**图 13.4 端口隔离配置界面**

2. 点击图 13.4 中的“添加”按钮，添加一个新的端口隔离组，如图 13.5 所示。

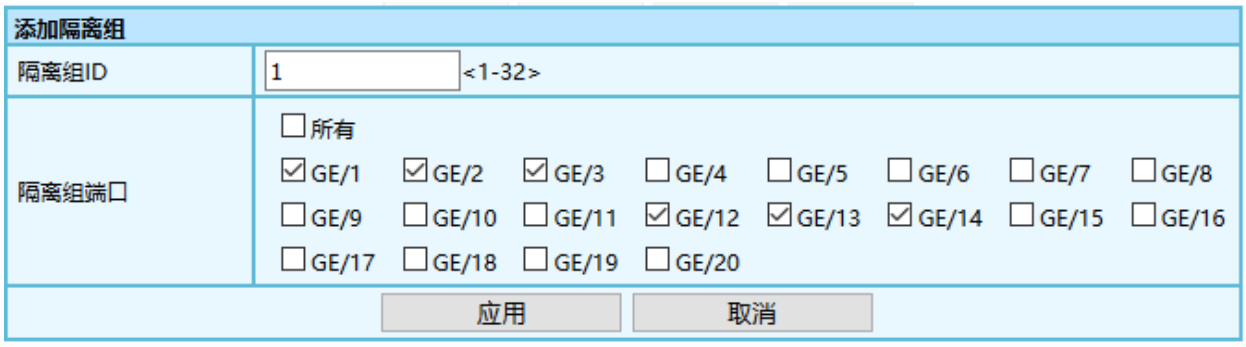



**图 13.5 端口隔离添加界面**

3. 配置结果如图 13.6 所示。

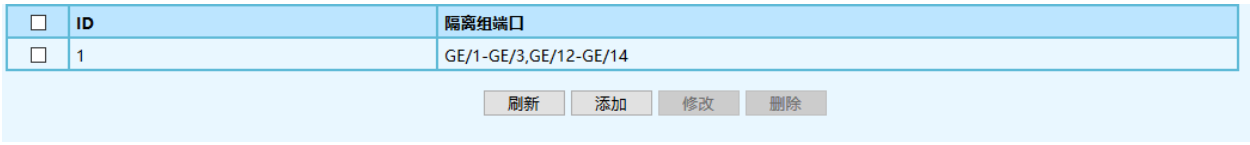



**图 13.6 端口隔离配置界面**

在端口隔离组 1 内，GE/1、GE/2、GE/3、GE/12、GE/13、GE/14 端口实现了相互隔离，但是与隔离组外其它端口可以通信。

# 第十四章 可靠性配置

本章对可靠性配置进行详细的描述，主要包括以下内容：

- 链路聚合
- 链路聚合工作模式
- 链路聚合设置

## 14.1 链路聚合

### 14.1.1 链路聚合介绍

链路聚合（Link Aggregation）是指将一组物理端口捆绑在一起作为一个逻辑接口来增加带宽的一种方法。通过两台设备之间建立链路聚合组（Link Aggregation Group），可以提供更高的通讯带宽和更高的可靠性，而这种提高不需要硬件的升级，并且还为两台设备的通讯提供了冗余保护。

链路聚合可以通过手工方式配置，由用户配置聚合组号和端口成员。在手工配置聚合组时，不会考虑到对端设备的汇聚信息，而将本端设备的端口进行汇聚，可能会出现一端汇聚端口和另一端汇聚端口不一致的错误配置，从而形成环路。基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议，为交换数据的设备提供一种标准的协商方式，LACP 根据设备端口的配置（既速率 双工 基本配置 管理 KEY）形成聚合链路并启动聚合链路收发数据。聚合链路形成后，LACP 负责维护链路状态，在聚合条件发生变化时，自动调整或者解散链路聚合，从而使两端设备对端口加入或者退出某个动态汇聚组达成一致。

## 14.2 链路聚合工作模式

本设备支持三种聚合方式，分别是手工聚合、静态聚合、动态聚合，各聚合方式如下：

### 14.2.1 手工聚合

手工负载分担模式链路聚合是应用比较广泛的一种链路聚合，大多数运营级网络设备均支持该特性，当需要在两个直连设备间提供一个较大的链路带宽而对端设备又不支持 LACP 协议时，可以使用手工负载分担模式。

### 14.2.2 静态聚合

静态 LACP 模式链路聚合是一种利用 LACP 协议进行参数协商选取活动链路的聚合模式。该模式由 LACP 协议确定聚合组中的活动和非活动链路，又称为 M：N 模式，即 M 条活动链路与 N 条备份链路的模式。这种模式提供了更高的链路可靠性，并且可以在 M 条链路中实现不同方式的负载均衡。静态聚合组是有手工创建的。

### 14.2.3 动态聚合

动态汇聚和静态汇聚原理类似，只是动态汇聚中所有端口都是通过协议确定，而不是像静态汇聚通过协议在指定端口中确定汇聚相关端口。聚合组的形成不需要手工干预，由协议自动生成。

### 14.2.4 负载分担

链路聚合功能工作过程中，发送报文会根据一定的负载分担算法将不同的报文从不同的端口进行传输，系统目前支持基于源 MAC 地址/目的 MAC 地址/源 IP 地址/目的 IP 地址/源端口/源 IP 端口/目的 IP 端口共七种负载分担算法,用户仅需要选择对应的负分担算法，具体算法由底层决定。

# 14.3 链路聚合设置

## 14.3.1 链路聚合全局设置

### 配置步骤

1．在导航栏中选择[高级配置/链路聚合/全局设置]，进入链路聚合[全局设置]界面。

2．在链路聚合全局设置界面中可以查看链路聚合的全局配置。

3.如需修改链路聚合的全局配置,可在 LACP 配置框中修改相应配置,然后单击<应用>,如图 14.1。


图 14.1 LACP 全局设置

4．如需添加聚合组，单击<设置>，如图 14.2，单击<应用>生效，如配置项填写有误，会有相应的提示。

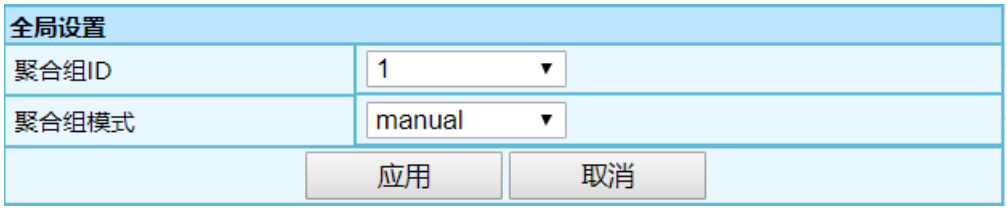



图 14.2 聚合组添加

## 配置项说明

链路聚合[全局配置]的相关界面的配置项说明。

**表 14.1 链路聚合[全局配置]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | 链路聚合全局使能开关。<br>● 开启：使能链路聚合功能；<br>● 关闭：关闭链路聚合功能。 |
| 系统优先级 | 设置链路聚合系统优先级，范围为0-65535，默认值为32768。优先级值越小则越优。 |
| 负载分担算法 | 系统支持根据报文中的源端口、源MAC、目的MAC、源IP、目的IP、源IP端口、目的IP端口中的一种或多种计算负载端口； |
| 设置 | 先在聚合组的显示栏前的选中框中选中需要修改配置的聚合组，然后单击<设置>，即可对相应聚合组配置进行修改。 |

**表 14.2 链路聚合[全局配置]的设置界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 聚合组ID | 聚合组ID信息； |
| 聚合组模式 | 设置聚合组的模式：<br>● manual：手工模式，该模式下，聚合组成员端口的加入由手工配置完成，且端口LACP协议处于关闭状态；<br>● static：静态模式，该模式下，聚合组成员端口的加入由手工配置完成，但端口的LACP协议处于开启状态。 |
| 最小链路数 | 配置聚合组的最少活动端口数，范围为<0-8>，且值不能大于最大链路数。 |
| 最大链路数 | 配置聚合组的最多活动端口数，范围为<0-8>，且值不能小于最小链路数。 |
| 成员端口列表 | 配置聚合组的成员端口。 |

### 14.3.2 链路聚合端口设置

**配置步骤**

1．在导航栏中选择[高级配置/链路聚合/端口配置]，进入链路聚合[端口配置]界面，如图 14.3。

2．在链路聚合[端口配置]界面中可以查看端口的链路聚合相关配置。

3．如需修改端口的链路聚合配置，单击对应端口显示栏后的<修改>按钮，进入端口配置界面，如图 14.4。

4．选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。

| 端口 | 聚合组ID | 优先级 | 管理Key | LACP端口模式 | LACP使能状态 | 设置 |
|---|---|---|---|---|---|---|
| GE/1 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/2 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/3 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/4 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/5 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/6 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/7 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/8 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/9 | 0 | 32768 | 0 | Active | 禁止 | 修改 |
| GE/10 | 0 | 32768 | 0 | Active | 禁止 | 修改 |

图 14.3 链路聚合端口信息界面

| 端口配置 | | |
|---|---|---|
| 端口 | GE/4 | |
| 聚合组ID | 0 | <0-8> 删除:0 |
| 优先级 | 32768 | <0-65535> 默认:32768 |
| 管理Key | 0 | <0-65535> 默认:0 |
| LACP端口模式 | Active | |
| LACP使能状态 | 禁止 | |
| 应用 | 取消 | |

图 14.4 链路聚合端口配置界面

## 配置项说明

链路聚合[端口配置]的相关界面的配置项说明。

**表 14.3 链路聚合[端口配置]界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 修改 | 修改端口的链路聚合相关配置。 |

**表 14.4 链路聚合[端口配置]的修改界面的配置项说明**

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息； |
| 聚合组ID | 表示端口所在聚合组的ID。 |
| 优先级 | 端口的链路聚合优先级，范围为<0-65535>，默认值为32768。优先级值越小则越优。 |
| LACP端口模式 | 端口在LACP协议中的主从模式：<br>● active：主动模式，该模式下，端口使能LACP协议后会主动发送协议报文。<br>● passive：被动模式，该模式下，端口不会主动发送协议报文，而只有当收到协议报文时才会发送。<br>注：端口默认为active模式。 |
| LACP超时模式 | 端口在LACP协议中的超时模式：<br>● fast：快速超时模式，该模式下，超时时间为1s。<br>● slow：慢速超时模式，该模式下，超时时间为30s。<br>注：端口默认为slow模式。 |
| LACP使能状态 | 端口的LACP使能状态：<br>● 使能：开启端口的LACP。<br>● 禁止：关闭端口的LACP。<br>注：端口默认为禁止状态。 |

### 14.3.3 链路聚合信息

#### 配置步骤

1. 在导航栏中选择[高级配置/链路聚合/聚合信息]，进入链路聚合[聚合信息]界面。
2. 在链路聚合[聚合信息]界面中可以查看所有端口的链路聚合相关信息，如图 14.4。
3. 单击<刷新>，查看各端口的最新聚合信息。

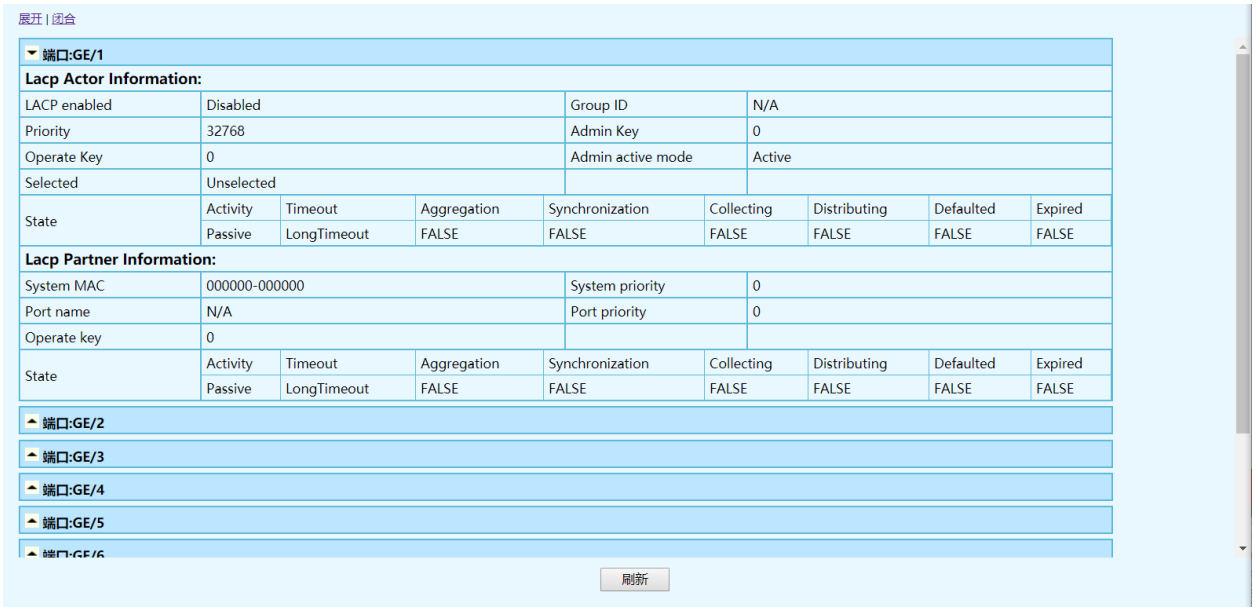



图 14.5 端口聚合信息

# 第十五章 SNMP

本章对 SNMP 进行详细的描述，主要包括以下内容：

- SNMP 概述
- SNMP 技术介绍
- 基础配置
- Trap 设置

## 15.1 SNMP 概述

简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资源对象。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。该协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的 internet 协议簇的一部分。SNMP 的目标是管理互联网 Internet 上众多厂家生产的软硬件平台，因此 SNMP 受 Internet 标准网络管理框架的影响也很大。SNMP 已经出到第三个版本的协议。

## 15.2 SNMP 技术介绍

SNMP 是基于 TCP/IP 协议族的网络管理标准，是一种在 IP 网络中管理网络节点（如服务器、工作站、路由器、交换机等）的标准协议。SNMP 能够使网络管理员提高网络管理效能，及时发现并解决网络问题以及规划网络的增长。网络管理员还可以通过 SNMP 接收网络节点的通知消息以及告警事件报告等来获知网络出现的问题。

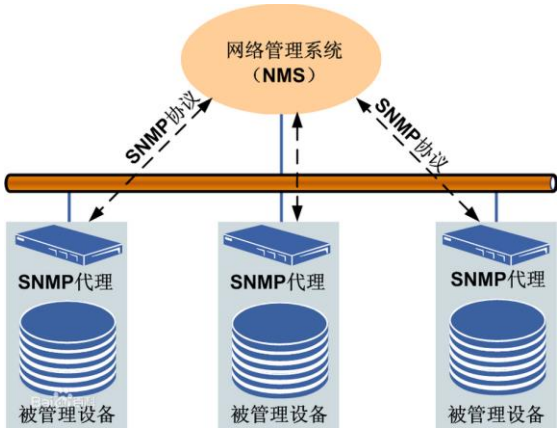



图 15.1 SNMP 管理网络拓扑组成

SNMP 管理的网络主要由三部分组成：

1. 被管理的设备

2. SNMP 代理

3. 网络管理系统（NMS）

它们之间的关系如图 15.1 所示：

1. 网络中被管理的每一个设备都存在一个标准的管理信息库（MIB）用于收集并储存管理信息。通过 SNMP 协议，NMS 能获取这些信息。被管理设备，又称为网络单元或网络节点，可以是支持 SNMP 协议的路由器、交换机、服务器或者主机等。

2. SNMP 代理是被管理设备上的一个网络管理软件模块，拥有本地设备的相关管理信息，并用于将它们转换成与 SNMP 兼容的格式，传递给 NMS。

3. NMS 运行应用程序来实现监控被管理设备的功能。另外，NMS 还为网络管理提供大量的处理程序及必须的储存资源。

## 15.3 基础配置

### 配置步骤

1. 在导航栏中选择[管理设置/SNMP/V1/V2 配置]，进入 SNMP[基本配置]界面。

2. 在 SNMP[基本配置]界面中可以查看当前 SNMP 的基本配置。

3. 如需修改基本配置，可在配置框中修改相应配置，然后单击<应用>生效，如图 15.1。

4. 如需添加团体字，单击<添加>后就会增加一个团体字，设置团体字名称和类型。系统最多支持 8 个团体字，其中第 1 和第 2 个是系统默认的，所以最多还可以添加 6 个团体字。单击<应用>生效。

5. 如需删除团体字，单击相应条目右侧的<删除>（其中第 1 个和第 2 个是系统默认的，不能被删除），单击<应用>生效。


图 15.2 SNMP 基本配置界面

### 配置项说明

表 15.2 SNMP 基本配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | SNMP全局使能状态：<br>● 使能：开启SNMP功能。<br>● 禁止：关闭SNMP功能。<br>注：默认为开启。 |
| SNMP端口 | SNMP端口，取值范围为<1-65535>，默认值为161。 |
| 系统名称 | 系统名称，可输入除空格外任意合法字符，最大长度为255。 |
| 系统位置信息 | 系统位置信息，可输入除空格外任意合法字符，最大长度为255。 |
| 系统联系信息 | 系统联系信息，可输入除空格外任意合法字符，最大长度为255。 |
| 团体字 | SNMP团体字：<br>● 名称：可输入除空格外任意合法字符，最大长度为127。<br>● 类型：只读、读写。<br>注：系统最多支持8个团体字，最少必须要两个团体字，系统默认的两个团体字只能修改团体字名，不能更改类型，不能删除；单击<添加>可添加团体字，添加的团体字可以修改名称，可以更改类型，可以删除。 |

## 15.4 trap 设置

### 配置步骤

1．在导航栏中选择[管理设置/SNMP/Trap 设置]，进入 SNMP[Trap 设置]界面。

2．在 SNMP[Trap 设置]界面中可以查看当前 SNMP 的 Trap 配置。

3．如需修改 Trap 设置，可在配置框中修改相应配置，然后单击<应用>，如图 15.3 所示。

4. 如需添加 Trap 服务器，单击<添加>后就会 Trap 服务器条目。系统最多支持 4 组 Trap 服务器，其中第 1 组是系统默认存在的，不能被删除，所以最多还可以添加 3 组 Trap 服务器，单击<应用>生效。

5. 如需删除 Trap 服务器，单击相应条目右侧的<删除>（其中第 1 组是系统默认的，不能被删除），单击<应用>生效。

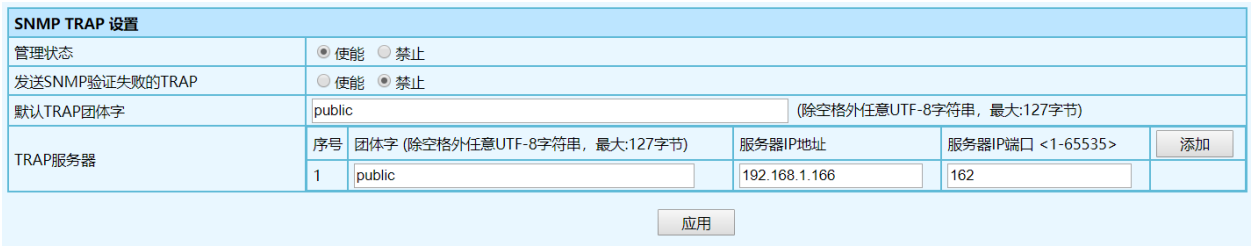



图 15.3 SNMP trap 设置界面

## 配置项说明

表 15.3 SNMP[trap 设置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | trap全局使能状态：<br>● 使能：开启trap功能。<br>● 禁止：关闭trap功能。<br>注：默认为开启。 |
| TRAP版本 | trap版本，支持v1和v2c。 |
| 发送SNMP验证失败的TRAP | 使能或关闭发送SNMP验证失败的TRAP：<br>● 使能：使能发送SNMP验证失败的TRAP。<br>● 禁止：关闭发送SNMP验证失败的TRAP。<br>注：默认为禁止。 |
| 默认trap团体字 | 默认的trap团体字，可输入除空格外任意合法字符，最大长度为127。 |
| trap服务器 | 设置trap服务器：<br>● 团体字：可输入除空格外任意合法字符，最大长度为127。<br>● 服务器IP地址：trap服务器的IP地址， IPv4，点分十进制格式。<br>● 服务器IP端口：trap服务器的IP端口， 范围<1-65535>，默认162。<br>注：系统最多支持4个服务器，单击<添加>按钮进行添加，系统默认服务器的序号为1 ，团体字为public，IP地址为192.168.1.200，IP端口为162；默认服务器不能删除，添加的服务器可删除。 |

# 第十六章 IP 接口

本章对 IP 接口进行详细的描述，主要包括以下内容：

- IP 地址
- DHCP 客户端配置

## 16.1 IP 地址

### 16.1.1 IP 地址介绍

IP 全称为 Internet Protocol Address，译为互联网协议地址，是 IP Address 的缩写。IP 地址是 IP 协议提供的一种统一的地址格式，它为互联网上的每一个网络和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。

IP 地址由两部分组成：网络地址(Net-id)、主机地址(Host-id)

网络地址具有区分不同网络的作用，主机地址用于区分一个网络内不同的主机。

IP 地址共分类为五类，详细如下表：

| IP地址类型 | IP地址范围 | 相关说明 |
| --- | --- | --- |
| A类 | 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，对应于当前主机<br>127．0．0．1到127．255．255．255用于回路测试，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 |
| B类 | 128.0.0.0-191.255.255.255 | - |
| C类 | 192.0.0.0-223.255.255.255 | 适用于小规模的局域网络，每个网络最多只能包含254台计算机 |
| D类 | 224.0.0.0-239.255.255.255 | 该网段地址为多播地址，即组播地址 |
| E类 | 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 |

部分特殊 IP 地址具有特殊作用而保留起来，用户配置 IP 接口时不可设置为主机地址：

1.每一个字节都为 0 的地址(“0.0.0.0”)对应于当前主机；

2. IP 地址中的每一个自己都为 1 的 IP 地址(“255.255.255.255”)是当前子网的广播地址；

3.IP 地址中凡是以“11110”开头的 E 类 IP 地址都保留用于将来和实验使用；

4.IP 地址中不能以十进制“127”作为开头，改地址中数字 127.0.0.1 到 127.255.255.255 用于回路测试，如：127.0.0.1 可以代表本机 IP 地址，用“http://127.0.0.1”就可以测试本机中的 Web 服务器；

5.网络 ID 的第一个 8 位组也不能全置为“0”，全“0”表示地址；

6.在 IP 网络中，相同的网络的地址可以直接通信，不同网络的地址不能直接通信。

### 16.1.2 基础配置

**配置步骤**

1．在导航栏中选择[管理设置/IP 接口/设置]，进入 IP 接口[设置]界面。

2．在 IP 接口[设置]界面中可以查看当前所有 IP 接口及其相关配置信息，如图 16.1。

3．如需添加新的 IP 接口，单击<添加>，然后填写相关配置，单击<应用>即可，如图 16.2。

4．如需修改某个 IP 接口，先勾选相应的 IP 接口，单击<修改>，然后修改相关的配置，单击<应用>即可，IP 接口设置界面如图 16.2。

5．如需删除某个 IP 接口，先勾选相应的 IP 接口，单击<删除>。


图 16.1 IP 接口查看界面


图 16.2 IP 接口设置界面

### 配置项说明

IP 接口基本设置的相关界面的配置项说明。

表 16.1 IP 接口[设置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 静态IP地址 | 静态IPv4地址，格式点分十进制，每个接口的IPv4地址不能再同一网段。 |
| 掩码 | IPv4地址的掩码。 |
| VLAN | 指定IP接口绑定的VLAN。 |

## 16.2 DHCP 客户端配置

**备注：**DHCP 相关功能内容在 17 章 DHCP 中有详细介绍。

### 配置步骤

1. 在导航栏中选择[管理设置/IP 接口/DHCP 客户端]，进入[DHCP 客户端]界面。

2. 在[DHCP 客户端]界面中可以查看 DHCP 客户端当前的配置信息和 DHCP 客户端状态。


图 16.3 DHCP 客户端配置界面

### 配置项说明

DHCP 客户端配置的相关界面的配置项说明。

表 16.2 [DHCP 客户端]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | 使能或禁止DHCP客户端：<br>● 使能：使能DHCP客户端；<br>● 禁止：禁止DHCP客户端；<br>注：默认为禁止。 |
| 重新获取 | DHCP客户端重新获取配置。 |
| 释放 | DHCP客户端释放当前配置。 |

# 第十七章 DHCP

本章对 DHCP 进行详细的描述，主要包括以下内容：

- DHCP Snooping
- DHCP 服务器端

## 17.1 DHCP Snooping

### 17.1.1 DHCP Snooping 介绍

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不信任的 DHCP 信息，这些信息是来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租约期、VLAN-ID 接口等信息。

### 17.1.2 DHCP Snooping 具体作用

●dhcp snooping 的主要作用就是隔绝非法的 dhcp server，通过配置信任端口对合法的 dhcp server 发送的报文进行正常接收并转发 dhcp offer 报文，对于非信任端口接收到的 dhcp offer 报文直接丢弃。

●与交换机 DAI 的配合，防止 ARP 病毒的传播。

●建立和维护一张 dhcp-snooping 的绑定表，这张表一是通过 dhcp ack 包中的 ip 和 mac 地址生成的，二是可以手工指定。这张表是后续 DAI（dynamic arp inspect）和 IPSource Guard 基础。这两种类似的技术，是通过这张表来判定 ip 或者 mac 地址是否合法，来限制用户连接到网络的。

●通过建立信任端口和非信任端口，对非法 DHCP 服务器进行隔离，信任端口正常转发 DHCO 数据包，非信任端口收到的服务器响应的 DHCP offer 和 DHCPACK 后，做丢包处理，不进行转发。

### 17.1.3 DHCP Snooping 技术介绍

DHCP 监听将交换机端口划分为两类：

●非信任端口：通常为连接终端设备的端口，如 PC，网络打印机等

●信任端口：连接合法 DHCP 服务器的端口或者连接汇聚交换机的上行端口

通过开启 DHCP 监听特性，交换机限制用户端口（非信任端口）只能够发送 DHCP 请求，丢弃来自用户端口的所有其它 DHCP 报文，例如 DHCP Offer 报文等。而且，并非所有来自用户端口的 DHCP 请求都被允许通过，交换机还会比较 DHCP 请求报文的（报文头里的）源 MAC 地址和（报文内容里的）DHCP 客户机的硬件地址（即 CHADDR 字段），只有这两者相同的请求报文才会被转发，否则将被丢弃。这样就防止了 DHCP 耗竭攻击。

信任端口可以接收所有的 DHCP 报文。通过只将交换机连接到合法 DHCP 服务器的端口设置为信任端口，其他端口设置为非信任端口，就可以防止用户伪造 DHCP 服务器来攻击网络。DHCP 监听特性还可以对端口的 DHCP 报文进行限速。通过在每个非信任端口下进行限速，将可以阻止合法 DHCP 请求报文的广播攻击。

DHCP 监听还有一个非常重要的作用就是建立一张 DHCP 监听绑定表（DHCP Snooping Binding）。一旦一个连接在非信任端口的客户端获得一个合法的 DHCP Offer，交换机就会自动在 DHCP 监听绑定表里添加一个绑定条目，内容包括了该非信任端口的客户端 IP 地址、MAC 地址、端口号、VLAN 编号、租期等信息。

### 17.1.4 option82

当 DHCP 服务器和客户端不在同一个子网内时，客户端要想从 DHCP 服务器上分配到 IP 地址，就必须由 DHCP 中继代理（DHCP Relay Agent）来转发 DHCP 请求包。DHCP 中继代理将客户端的 DHCP 报文转发到 DHCP 服务器之前，可以插入一些选项信息，以便 DHCP 服务器能更精确的得知客户端的信息，从而能更灵活的按相应的策略分配 IP 地址和其他参数。这个选项被称为：DHCP relay agent information option（中继代理信息选项），选项号为 82，故又称为 option 82，相关标准文档为 RFC3046。

Option 82 是对 DHCP 选项的扩展应用。选项 82 只是一种应用扩展，是否携带选项 82 并不会影响 DHCP 原有的应用。另外还要看 DHCP 服务器是否支持选项 82。不支持选项 82 的 DHCP 服务器接收到插入了选项 82 的报文，或者支持选项 82 的 DHCP 服务器接收到了没有插入选项 82 的报文，这两种情况都不会对原有的基本的 DHCP 服务造成影响。要想支持选项 82 带来的扩展应用，则 DHCP 服务器本身必须支持选项 82 以及收到的 DHCP 报文必须被插入选项 82 信息。

### 17.1.5 全局设置

#### 配置步骤

1. 在导航栏中选择[管理设置/DHCP snooping/全局设置]，进入 DHCP snooping[全局设置]界面。

2. 在 DHCP snooping[全局设置]界面中可以查看 DHCP snooping 的全局配置信息。

3. 如需修改 DHCP snooping 的全局配置，可在 DHCP snooping 全局配置框中修改相应配置，然后单击<应用>，如图 17.1。

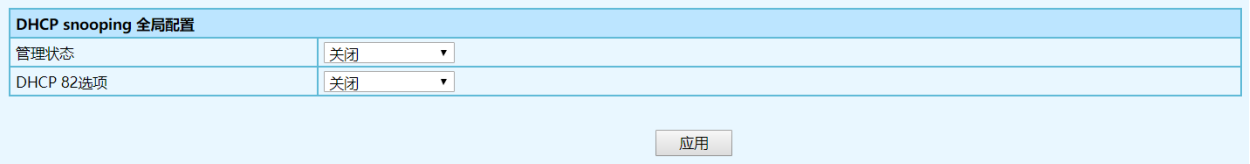



图 17.1 DHCP snooping 全局设置界面

#### 配置项说明

DHCP snooping [全局设置]的相关界面的配置项说明。

表 17.1 DHCP snooping[全局设置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | DHCP snooping全局使能开关:<br>● 开启：使能DHCP snooping功能；<br>● 关闭：关闭DHCP snooping功能。<br>注：默认为关闭。 |

### 17.1.6 端口设置

#### 配置步骤

1. 在导航栏中选择[管理设置/DHCP snooping/端口设置]，进入 DHCP snooping[端口设置]界面。

2. 在 DHCP snooping[端口设置]界面中可以查看 DHCP snooping 的端口配置。

3. 如需修改某个端口的 DHCP snooping 配置，单击对应端口显示栏后的<修改>按钮，进入端口配置界面，如图 17.2。

4. 选择或填写需要修改的配置项，单击<应用>生效，如配置项填写有误，会有相应的提示。


图 17.2 DHCP snooping 端口设置界面

### 配置项说明

DHCP snooping[端口设置]的相关界面的配置项说明。

表 17.2 DHCP snooping[端口设置]的修改界面的配置项说明

| 配置项 | 说明 |
|---|---|
| 端口 | 端口名称信息。 |
| 信任 | 端口的信任：<br>● 是：设置端口为信任端口；<br>● 否：设置端口为非信任端口。<br>注：端口默认为否。 |
| 代理电路ID | 设置端口的代理电路ID，默认采用全局的代理电路ID。 |
| 代理远程ID | 设置端口的代理远程ID，默认采用全局的代理远程ID。 |

## 17.1.7 绑定表

### 配置步骤

1. 在导航栏中选择[管理设置/DHCP snooping/绑定表]，进入 DHCP snooping[绑定表]界面。

2. 在 DHCP snooping[绑定表]界面中可以查看所有的绑定表相关信息，如图 17.3。

3. 单击<刷新>，更新查看所有的 DHCP snooping 绑定表信息。

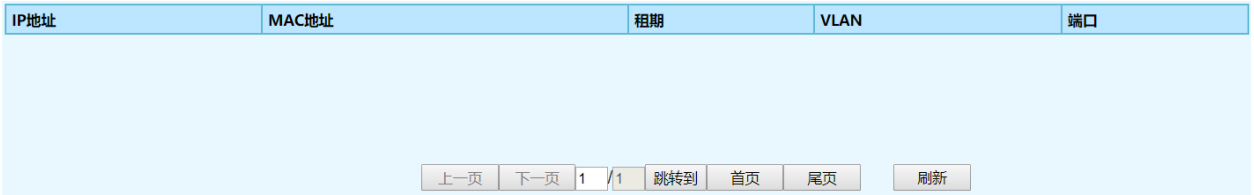



图 17.3 DHCP snooping 绑定表界面

# 第十八章 管理员

本章对管理员进行详细的描述，主要包括以下内容：

- 用户管理
- 在线用户
- 登录超时设置

## 18.1 用户管理

**配置步骤**

1．在导航栏中选择[系统设置/管理员/管理员]，进入[管理员]界面。

2．在[管理员]界面中可以查看当前的用户配置信息，如图 18.1。

3．如需添加新用户，单击<添加>，进入管理员配置界面，填写相应的配置项，单击<应用>完成添加用户，添加用户界面如图 18.2。

4．如需修改用户信息，先勾选相应的用户，然后单击<修改>，进入用户配置修改界面，修改相应的配置项。单击<应用>，完成配置修改，修改用户界面如图 18.3。

5．如需删除用户，先勾选相应的用户，单击<删除>，删除该用户。

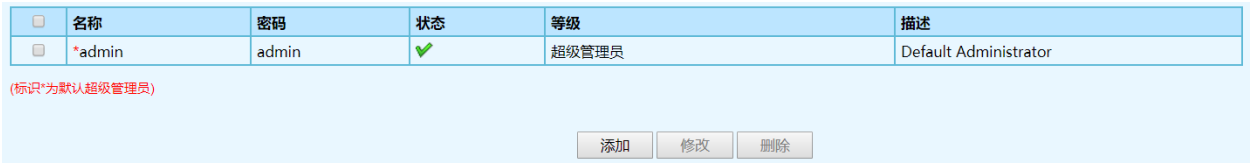



图 18.1 管理员界面


图 18.2 添加用户界面

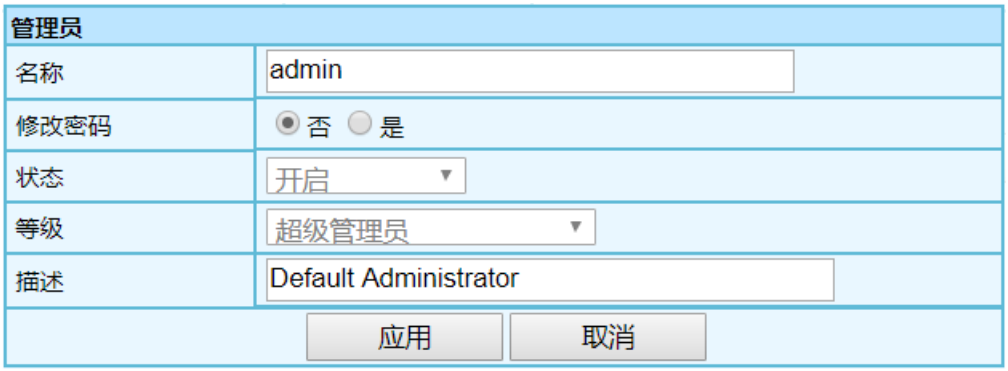



图 18.3 修改用户界面

## 配置项说明

表 18.1 [管理员]界面配置项说明

| 配置项 | 说明 |
| --- | --- |
| 用户名 | 用户名信息。 |
| 密码 | 用户密码。 |
| 状态 | 用户激活状态：<br>● ✔：激活<br>● ✖：未激活<br>默认情况下，新增用户为激活状态。 |
| 等级 | 用户等级，包括：超级管理员，高级管理员，初级管理员，访客用户。 |
| 描述 | 用户描述信息。 |

表 18.2 [用户管理]界面添加用户配置项说明

| 配置项 | 说明 |
| --- | --- |
| 用户名 | 用户的用户名信息，字符串形式，有效字符A-Z,a-z,0-9, _ ，长度1-32个字节。 |
| 密码 | 用户登录设备的密码，字符串形式，任意可打印的ASCII字符，长度1-16个字节。 |
| 确认密码 | 重新输入登录密码进行确认。 |
| 等级 | 设定用户的等级，包括：<br>● 超级管理员<br>● 高级管理员<br>● 初级管理员<br>● 访客用户 |

| | |
|---|---|
| | 注：默认为访客用户。 |
| 状态 | 用户激活状态，包括<br>● 开启：激活<br>● 关闭：未激活<br>注：默认为开启。 |
| 描述 | 用户描述信息，任意可打印的ASCII字符，长度1-128字节。 |

**表 18.3 [用户管理]界面修改用户配置项说明**

| 配置项 | 说明 |
|---|---|
| 用户名 | 用户的用户名信息，字符串形式，有效字符A-Z,a-z,0-9, _ ，长度1-32个字节。 |
| 旧密码 | 用户当前登录Web界面的密码。 |
| 密码 | 用户设置的新密码，字符串形式，任意可打印的ASCII字符，长度1-16个字节。 |
| 确认密码 | 重新输入用户设置的新密码，对密码进行确认。 |
| 等级 | 设定用户的等级，包括：<br>● 超级管理员<br>● 高级管理员<br>● 初级管理员<br>● 访客用户 |
| 状态 | 用户激活状态，包括开启和关闭。 |
| 描述 | 用户描述信息，任意可打印的ASCII字符，长度1-128字节。 |

## 注意事项

设备默认存在一个用户名为 admin 的超级管理员，该用户不能被删除，用户等级也不能被更改。除了该用户外，最多还可以添加 15 个用户。

# 18.2 在线用户

## 配置步骤

1. 在导航栏中选择[系统设置/管理员/在线用户]，进入[在线用户]界面。
2. 在[在线用户]界面中，可以查看当前登录设备的用户信息。


图 18.4 在线用户信息界面

## 配置项说明

表 18.4 [在线用户]界面配置项说明

| 配置项 | 说明 |
|---|---|
| 用户名 | 用户名信息。 |
| 等级 | 用户等级，包括：超级管理员，高级管理员，初级管理员，访客用户。 |
| 描述 | 用户描述信息。 |
| 登录方式 | 用户登录设备的方式，包括web，console，telnet。 |
| 登录IP地址 | 用户登录设备的客户端IP地址，console方式登录除外。 |
| 登录时间 | 用户登录设备的时间。 |

# 18.3 登录超时设置

## 配置步骤

1．在导航栏中选择[系统设置/管理员/管理设置]，进入[登录超时设置]界面。

2．在[登录超时设置]界面中，可以查看登录超时的相关设置信息。

3．如需修改登录超时时间，填写相应登录方式的超时时间，单击<应用>，完成配置修改，如图 18.5。

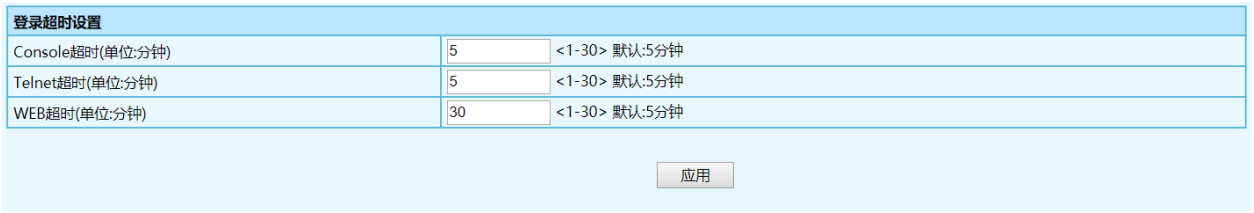



**图 18.5 登录超时设置界面**

## 配置项说明

**表 18.5 [登录超时设置]界面配置项说明**

| 配置项 | 说明 |
|---|---|
| Console超时 | 通过console口登录设备的超时时间，范围为1-30，默认值为5，单位为分钟。 |
| Telnet超时 | 通过telnet方式登录设备的超时时间，范围为1-30，默认值为5，单位为分钟。 |
| Web超时 | 通过web方式登录设备的超时时间，范围为1-30，默认值为5，单位为分钟。 |

## 注意事项

设置不同登录方式的超时时间，本次设置后，要下次登录才生效。

# 第十九章 系统配置

本章对系统配置进行详细的描述，主要包括以下内容：

- 系统日志
- 配置管理
- 日期与时间
- 软件升级
- 软件重启

设备配置完成后，需要将配置信息保存到设备中，新保存的配置信息将覆盖原有的配置信息。配置完成后，如果不进行保存操作，设备重启后会丢失新的配置，继续执行原有的配置。

设备出现故障时，可根据实际情况，通过重启设备来尝试解决故障。使用该界面可以实现对系统的配置管理，包括擦除配置、保存配置、重启设备等。用户还可以根据自己的需要查看和配置相应的系统启动管理。

## 19.1 系统日志

### 19.1.1 设置

**配置步骤**

1．在导航栏中选择[系统设置/系统日志/设置]，进入系统日志[设置]界面。

4． 在系统日志[设置]界面中，可以查看当前系统日志配置信息，如图 19.1 所示。

5． 如需修改系统日志配置，在系统日志设置框中设置相应的配置，单击<应用>，即可完成配置，如图 19.1。

6． 如需添加远程日志服务器，则单击<添加>，在弹出的远程日志服务器[设置]界面，填写相应的配置项，单击<应用>完成配置，最多可添加 4 组远程服务器。

7． 如需修改远程日志服务器，先勾选相应的远程日志服务器，然后单击<修改>，进入远程日志服务器[设置]界面，修改相应的配置项，单击<应用>，完成配置修改。

8． 如需删除远程日志服务器，先勾选相应的远程日志服务器，单击<删除>，

删除远程日志服务器。


**图 19.1 系统日志设置**


**图 19.2 远程日志服务器设置**

## 配置项说明

**表 19.1 系统日志[设置]界面配置项说明**

| 配置项 | 说明 |
|---|---|
| 管理状态 | 系统日志功能状态，包括：<br>● 使能<br>● 禁止<br>注：默认为使能。 |
| 输出到控制台 | 系统日志输出到控制台状态，包括<br>● 开启<br>● 关闭<br>注：默认为关闭。 |
| 输出到本地缓存 | 系统日志输出到本地缓存状态，包括<br>● 开启<br>● 关闭<br>注：默认为开启。 |
| 输出到远程主机 | 系统日志输出到远程日志服务器 |

| | |
|---|---|
| 等级 | 系统日志级别，根据严重程度分为8个等级<br>● EMERG ：级别0，系统不可以使用<br>● ALERT ：级别1，需要立即处理<br>● CRIT ：级别2，严重状态<br>● ERR ：级别3，错误状态<br>● WARNNING ：级别4，警告状态<br>● NOTICE ：级别5，正常但是很重要的状态<br>● INFO ：级别6，通告事件<br>● DEBUG ：级别7，调试信息<br>注：默认为INFO。 |

**表 19.2 远程日志服务器[设置]界面配置项说明**

| 配置项 | 说明 |
|---|---|
| 主机IP地址 | 远程日志主机IP地址，点分十进制格式，有效的主机IP地址，最多可以添加4组。 |
| 主机IP端口 | 远程日志主机的端口，范围514,1024-65534，默认为514。 |
| 等级 | 系统日志级别，根据严重程度分为8个等级<br>● EMERG ：级别0，系统不可以使用<br>● ALERT ：级别1，需要立即处理<br>● CRIT ：级别2，严重状态<br>● ERR ：级别3，错误状态<br>● WARNNING ：级别4，警告状态<br>● NOTICE ：级别5，正常但是很重要的状态<br>● INFO ：级别6，通告事件<br>● DEBUG ：级别7，调试信息<br>注：默认为INFO |

## 注意事项

日志级别数值越小，级别越高。只有级别等于或大于设定级别的日志才会被输出。例如：设置输出到控制台的日志级别为 5(NOTICE)，则只有级别为 0~5 的日志才会被输出到控制台。

### 19.1.2 查看

#### 配置步骤

1. 在导航栏中选择[系统设置/系统日志/查看]，进入系统日志[查看]界面。
2. 在系统日志[查看]界面中，可以查看系统日志的内容，如图 19.3 所示。

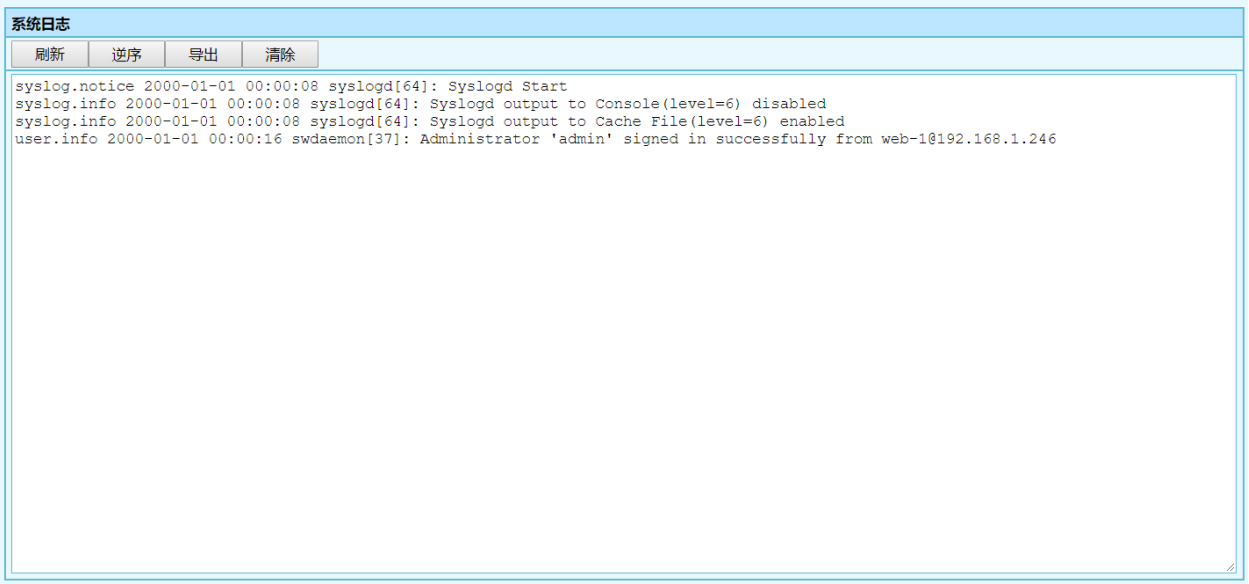



图 19.3 查看系统日志内容

#### 配置说明

表 19.3 系统日志[查看]界面配置项说明

| 配置项 | 说明 |
| --- | --- |
| 刷新 | 刷新系统日志内容。 |
| 顺序 | 按时间顺序由旧到新显示，默认为顺序显示。 |
| 逆序 | 按时间顺序由新到旧显示。 |
| 导出 | 导出系统日志的内容。 |
| 清除 | 清空系统日志的内容。 |

## 19.2 配置管理

### 19.2.1 配置查看

#### 配置步骤

1. 在导航栏中选择[系统设置/配置管理/查看]，进入配置[查看]界面。
2. 在配置[查看]界面中，可以查看运行配置和启动配置。

### 配置说明

表 19.4 配置管理[查看]界面配置说明

| 配置项 | 说明 |
| --- | --- |
| 运行配置 | 查看系统运行配置文件，文本风格。 |
| 启动配置 | 查看系统启动配置文件，文本风格。 |
| 重新加载 | 重新加载运行或启动配置文件。 |

## 19.2.2 配置导入

### 配置步骤

1．在导航栏中选择[系统设置/配置管理/导入]，进入配置管理[导入]界面，配置管理[导入]界面如图 19.4 所示。

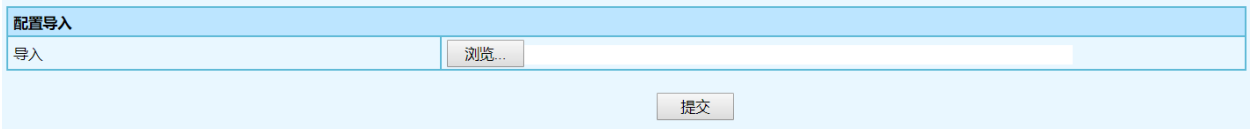



图 19.4 配置管理导入界面

2．在配置管理[导入]界面中，可单击<浏览>，选择要导入的配置文件，单击<提交>，开始导入。

## 19.2.3 配置导出

### 配置步骤

1．在导航栏中选择[系统设置/配置管理/导出]，进入配置管理[导出]界面，配置管理[导出]界面如图 19.5 所示。

2．导出配置分为启动配置和运行配置。在相应的项目单击<导出>，弹出“文件保存”对话框（不同的浏览器可能有所不同，这里以 IE11 浏览器为例），点击<保存>即可导出相应的配置文件到本地。


图 19.5 配置导出界面

### 19.2.4 恢复出厂配置

#### 配置步骤

1．在导航栏中选择[系统设置/配置管理/恢复出厂配置]，进入[恢复出厂配置]界面，[恢复出厂配置]界面如图 19.6 所示。

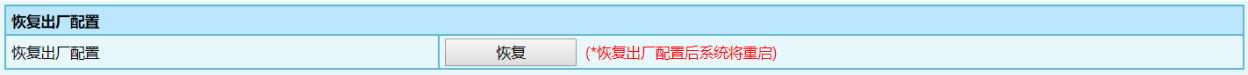



图 19.6 恢复出厂设置界面

2．单击<恢复>，在弹出的确认对话框中，单击<确定>恢复到出厂配置，单击<取消>取消恢复出厂配置。成功恢复出厂设置后，系统会自动重启以生效出厂配置，如图 19.7。

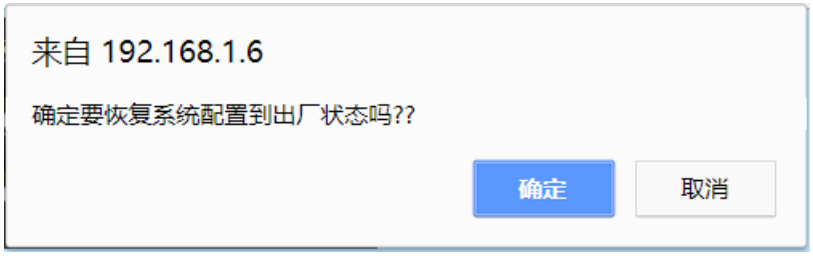



图 19.7 恢复出厂配置确认对话框

## 19.3 日期和时间

#### 配置步骤

1． 在导航栏中选择[系统设置/日期和时间]，进入系统设置[日期和时间]界面。系统时间可以手动设定，也可以通过 SNTP 客服端自动同步系统时间。

2． [日期和时间]界面可查看系统时间和相关的日期和时间配置信息。

3．手动设定系统时间。SNTP 客户端必须禁止才能设置系统时间。在<时区>栏中选择相应的时区，<时间设定>栏中设置欲设置的系统时间。单击<应用>完成系统时间设定，如图 19.8。

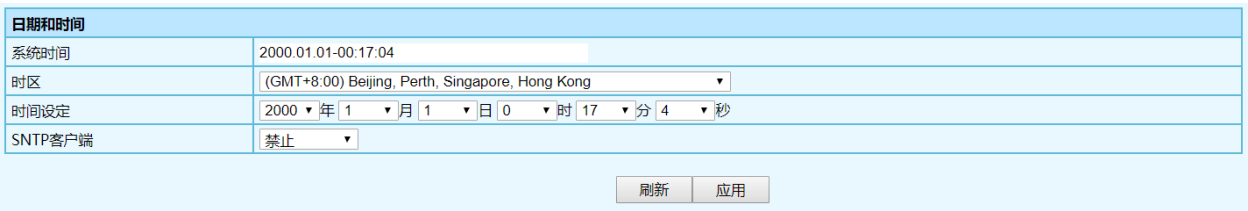



图 19.8 手动设置系统时间界面

4．通过 SNTP 客户端自动同步系统时间。首先要使能 SNTP 客户端，才能设置 SNTP 客户端。SNTP 客户端时间同步模式分为单播，组播，广播三种，这三种模式是可以复选的，但是必须至少选择一种模式。当单播模式被选择时，还必须设定授时服务器的 IP 地址(默认为 8.8.8.8)和同步间隔(默认 1440 分钟)。<立即同步>按钮，SNTP 客户端立即请求时间同步。否则按设定的同步间隔同步一次。单击<应用>，完成 SNTP 客户端时间同步设置，如图 19.9。


**图 19.9 SNTP 客户端设置界面**

## 配置项说明

**表 19.5 [日期和时间]界面配置项说明**

| 配置项 | 说明 |
|---|---|
| 系统时间 | 显示实际生效的系统时间。 |
| 时区 | 系统时区设定，从下拉列表中可选择任意一个时区。 |
| 时间设定 | 在禁止SNTP客户端后可设置，年份范围为1970-2037，其他与常用设置一致。 |
| SNTP客户端 | SNTP客户端有两种状态：<br>● 使能：使能SNTP客户端<br>● 禁止：禁止SNTP客户端<br>注：默认为禁止。 |
| 同步模式 | SNTP客户端同步模式分为：<br>● 单播模式：默认IP为8.8.8.8；间隔范围为10-43200，默值1440，单位分。<br>● 组播模式<br>● 广播模式<br>这三种模式是可以多选的，但是必须至少选择一种 |
| IP | SNTP授时服务器的IP地址，仅针对单播模式 |
| 间隔 | SNTP客户端时间同步间隔，仅针对单播模式 |
| 立即同步 | SNTP客户端立即同步时间，仅针对单播模式 |

## 19.4 软件升级

### 配置步骤

1．在导航栏中选择[系统设置/软件升级]，进入[软件升级]界面，如图 19.10 所示。

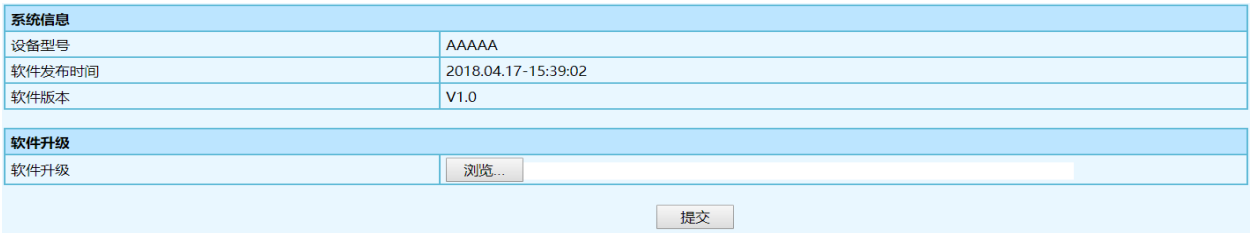



图 19.10 软件升级界面

2．在[软件升级]界面中，可单击<浏览>，选择要导入的升级文件（升级文件一般有.ub 和 .urk 两种，标记为 b 表示带 BOOT 文件，标记为 r 表示带文件系统的文件，标记为 k 表示带内核的文件），单击<提交>，系统开始上传升级文件，上传完毕后，等待升级完成后，设备会自动重启以更新软件。

**注：软件升级过程中请确保设备通电到升级完成。**

## 19.5 软件重启

### 配置步骤

1．在导航栏中选择[系统设置/重启]，进入[重启]界面，[重启]界面如图 19.11 所示。


图 19.11 重启界面

2．单击<重启>按钮，弹出“确定重启”对话框。单击<确定>按钮，重启设备，弹出重启进度条。单击<取消>按钮，取消重启设备，确认框如图 19.12，重启进度如图 19.13。

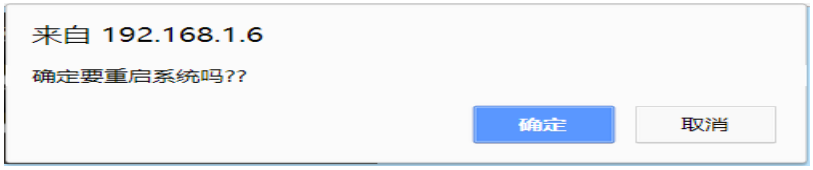



图 19.12 重启确认框


图 19.13 重启进度条

# 第二十章 GMRP

本章对 GMRP 进行详细的描述，主要包括以下内容：

- GMRP 概述
- GMRP 技术介绍
- GMRP 配置

## 20.1 GMRP 概述

GMRP（garp multicast registration protocol，garp 组播注册协议）是基于 GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一个组播注册协议，用于注册和注销组播属性。

## 20.2 GMRP 技术介绍

GMRP 协议是一个动态二层组播注册协议,所有支持 GMRP 的交换机都能够接收来自其他交换机的组播注册信息，并动态更新本地的组播注册信息，同时也能将本地的组播注册信息向其他交换机传播。这种信息交换机制，确保了同一交换网内所有支持 GMRP 的设备维护的组播信息的一致性。

当一台主机想要加入某个组播组时，它将发出 GMRP 加入消息。交换机将接到 GMRP 加入消息的端口加入到该组播组中,并在接收端口所在的 VLAN 中广播该 GMRP 加入消息,VLAN 中的组播源就可以知晓组播成员的存在。当组播源向组播组发送组播报文时，交换机就只把组播报文转发给与该组播组成员相连的端口，从而实现了在 vlan 内的二层组播。

交换机会周期性发送 GMRP 查询，如果主机想留在组播组中，它就会响应 GMRP 查询，在该情况下，交换机没有任何操作；如果主机不想留在组播组中，它既可以发送一个 leave 信息也可以不响应周期性 GMRP 查询。一旦交换机在计时器（leave all timer）设定期间收到主机 leave 信息或没有收到响应信息，它便从组播组中删除该主机。

那么为什么需要二层组播协议呢？与 IGMP 协议一样，如果我们在自己的局域网内成立一个组播组，可能我们的局域网包含了很多交换机。如果这些交换机没有实现二层组播协议的话，那么某个组员给其他组员发送数据包时，交换机就会将该数据包向所有的端口广播。因为交换机不知道哪个端口有人加入了该组播组，唯一的解决办法就是管理员配置交换机，只有这样才能将这种广播转发数据包的发送方式限制住。而组播本身是动态的，所

以通过这种靠管理员的配置来实现组播的方式是不现实的。因此，就需要有一个二层组播协议来动态管理组员。

### 20.2.1 GMRP 消息类型

**1.Join 消息**

当一个 GMRP 应用实体希望其它设备注册自己的属性信息时，它将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GMRP 应用实体进行注册时，它也会向外发送 Join 消息。

**2.Leave 消息**

当一个 GMRP 应用实体希望其它设备注销自己的属性信息时，它将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性后，它也会向外发送 Leave 消息。

**3.LeaveAll 消息**

每个应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后应用实体将对外发送 LeaveAll 消息。

LeaveAll 消息用来注销所有的属性，以使其它应用实体重新注册本实体上所有的属性信息，以此来周期性地清除网络中的垃圾属性（例如某个属性已经被删除，但由于设备突然断电，并没有发送 Leave 消息来通知其他实体注销此属性）。

### 20.2.2 GMRP 定时器

**1.Join 定时器**

Join 定时器是用来控制 Join 消息的发送的。

为了保证 Join 消息能够可靠的传输到其它应用实体，发送第一个 Join 消息后将等待一个 Join 定时器的时间间隔，如果在一个 Join 定时器时间内收到 JoinIn 消息，则不发送第二个 Join 消息；如果没收到，则再发送一个 Join 消息。

**2.Hold 定时器**

Hold 定时器是用来控制 Join 消息和 Leave 消息的发送的。

当在应用实体上配置属性或应用实体接收到消息时不会立刻将该消息传播到其它设备，而是在等待一个 Hold 定时器后再发送消息，设备将此 Hold 定时器时间段内接收到的消息尽可能封装成最少数量的报文，这样可以减少报文的发送量。如果没有 Hold 定时器的

话，每来一个消息就发送一个，造成网络上报文量太大，既不利于网络的稳定，也不利于充分利用每个报文的数据容量。Hold 定时器的值要小于等于 Join 定时器值的一半。

**3.Leave 定时器**

Leave 定时器是用来控制属性注销的。

每个应用实体接收到 Leave 或 LeaveAll 消息后会启动 Leave 定时器，如果在 Leave 定时器超时之前没有接收到该属性的 Join 消息，属性才会被注销。这是因为网络中如果有一个实体因为不存在某个属性而发送了 Leave 消息,并不代表所有的实体都不存在该属性了，因此不能立刻注销属性，而是要等待其他实体的消息。例如，某个属性在网络中有两个源，分别在应用实体 A 和 B 上，其他应用实体通过协议注册了该属性。当把此属性从应用实体 A 上删除的时候，实体 A 发送 Leave 消息，由于实体 B 上还存在该属性源，在接收到 Leave 消息之后，会发送 Join 消息，以表示它还有该属性。其他应用实体如果收到了应用实体 B 发送的 Join 消息，则该属性仍然被保留，不会被注销。只有当其它应用实体等待两个 Join 定时器以上仍没有收到该属性的 Join 消息时，才能认为网络中确实没有该属性了，所以这就要求 Leave 定时器的值大于 2 倍 Join 定时器的值。

**4.LeaveAll 定时器**

每个 GMRP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GMRP 应用实体将对外发送 LeaveAll 消息，随后再启动 LeaveAll 定时器，开始新的一轮循环。

接收到 LeaveAll 消息的实体将重新启动所有的定时器，包括 LeaveAll 定时器。在自己的 LeaveAll 定时器重新超时之后才会再次发送 LeaveAll 消息，这样就避免了短时间内发送多个 LeaveAll 消息。

一次 LeaveAll 事件相当于全网所有属性的一次 Leave。由于 LeaveAll 影响范围很广，所以建议 LeaveAll 定时器的值不能太小，至少应该大于 Leave 定时器的值。

每个设备只在全局维护一个 LeaveAll 定时器。

## 20.3 GMRP 配置

### 20.3.1 GMRP 全局设置

**配置步骤**

1．在导航栏中选择[GMRP/GMRP 配置]，进入 GMRP 配置界面。

2．在[GMRP 全局设置]界面中可以查看 GMRP 的全局配置，如图 20.1。

3. 如需修改 GMRP 的全局配置，在 GMRP 全局配置框中修改相应配置，然后单击<应用>。


图 20.1 GMRP 全局设置

### 配置项说明

[GMRP 全局设置]的相关界面的配置项说明。

表 20.1 [GMRP 全局设置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | GMRP全局使能开关。<br>● 使能：使能GMRP功能；<br>● 禁止：关闭GMRP功能。<br>注意：默认关闭。 |
| Hold Time | Hold 定时器周期，范围为100-32760(ms)，默认值为100ms；<br>注意hold time*2 <= join time。 |
| Join Time | Join定时器周期，范围为100-32760(ms)，默认值为200ms；<br>注意join time*2<=leave time。 |
| Leave Time | Leave定时器周期，范围为100-32760(ms)，默认值为600ms；<br>注意leave time<=leaveall time |
| Leaveall Time | Leaveall定时器周期，范围为100-32760(ms)，默认值为10000ms；<br>注意leaveall time>=leave time |

## 20.3.2 GMRP 端口配置

### 配置步骤

1. 在导航栏中选择[GMRP/GMRP 配置]，进入 GMRP 配置界面。
2. 在[GMRP 端口设置]界面中可以查看 GMRP 的端口配置，如图 20.2。
3. 如需修改 GMRP 的端口配置，单击指定端口后面的修改按钮，进入 GMRP 端口配置修

改界面，如图 20.3，,配置好后，然后单击<应用>。

| 端口 | GMRP端口模式 | 设置 |
| --- | --- | --- |
| GE/1 | Forbidden | 修改 |
| GE/2 | Forbidden | 修改 |
| GE/3 | Forbidden | 修改 |
| GE/4 | Forbidden | 修改 |
| GE/5 | Forbidden | 修改 |
| GE/6 | Forbidden | 修改 |
| GE/7 | Forbidden | 修改 |
| GE/8 | Forbidden | 修改 |
| GE/9 | Forbidden | 修改 |
| GE/10 | Forbidden | 修改 |

图 20.2 GMRP 端口配置查看界面


图 20.3 GMRP 端口配置修改界面

## 配置项说明

GMRP[端口配置]的相关界面的配置项说明。

表 20.2 GMRP[端口配置]界面配置项说明

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息。 |
| VLAN模式 | 端口的GMRP模式，默认为Forbidden。 |

# 第二十一章 GVRP

本章对 GVRP 进行详细的描述，主要包括以下内容：

- GVRP 概述
- GVRP 技术介绍
- GVRP 配置

## 21.1 GVRP 概述

同 GMRP，GVRP（GARP VLAN Registration Protocol，GARP VLAN 注册协议）是基于 GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一个 VLAN 注册协议，用于注册和注销 VLAN 属性。

## 21.2 GVRP 技术介绍

GVRP 用来维护交换机中的 VLAN 动态注册信息并传播该信息到其它的交换机中。所有支持 GVRP 特性的交换机能够接收来自其它交换机 VLAN 注册信息,并动态更新本地的 VLAN 信息。包括当前存在的 VLAN，VLAN 有哪些成员等信息。

### 20.2.1 GVRP 消息类型

**1.Join 消息**

当一个 GVRP 应用实体希望其它设备注册自己的属性信息时，它将对外发送 Join 消息；当收到其它实体的 Join 消息或本设备静态配置了某些属性，需要其它 GVRP 应用实体进行注册时，它也会向外发送 Join 消息。

**2.Leave 消息**

当一个 GVRP 应用实体希望其它设备注销自己的属性信息时,它将对外发送 Leave 消息；当收到其它实体的 Leave 消息注销某些属性或静态注销了某些属性后，它也会向外发送 Leave 消息。

**3.LeaveAll 消息**

每个应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后应用实体将对外发送 LeaveAll 消息。

LeaveAll 消息用来注销所有的属性，以使其它应用实体重新注册本实体上所有的属性

信息，以此来周期性地清除网络中的垃圾属性（例如某个属性已经被删除，但由于设备突然断电，并没有发送 Leave 消息来通知其他实体注销此属性）。

### 21.2.2 GVRP 定时器

**1.Join 定时器**

Join 定时器是用来控制 Join 消息的发送的。

为了保证 Join 消息能够可靠的传输到其它应用实体，发送第一个 Join 消息后将等待一个 Join 定时器的时间间隔，如果在一个 Join 定时器时间内收到 JoinIn 消息，则不发送第二个 Join 消息；如果没收到，则再发送一个 Join 消息。

**2.Hold 定时器**

Hold 定时器是用来控制 Join 消息和 Leave 消息的发送的。

当在应用实体上配置属性或应用实体接收到消息时不会立刻将该消息传播到其它设备，而是在等待一个 Hold 定时器后再发送消息，设备将此 Hold 定时器时间段内接收到的消息尽可能封装成最少数量的报文，这样可以减少报文的发送量。如果没有 Hold 定时器的话，每来一个消息就发送一个，造成网络上报文量太大，既不利于网络的稳定，也不利于充分利用每个报文的数据容量。Hold 定时器的值要小于等于 Join 定时器值的一半。

**3.Leave 定时器**

Leave 定时器是用来控制属性注销的。

每个应用实体接收到 Leave 或 LeaveAll 消息后会启动 Leave 定时器，如果在 Leave 定时器超时之前没有接收到该属性的 Join 消息，属性才会被注销。这是因为网络中如果有一个实体因为不存在某个属性而发送了 Leave 消息,并不代表所有的实体都不存在该属性了，因此不能立刻注销属性，而是要等待其他实体的消息。例如，某个属性在网络中有两个源，分别在应用实体 A 和 B 上，其他应用实体通过协议注册了该属性。当把此属性从应用实体 A 上删除的时候，实体 A 发送 Leave 消息，由于实体 B 上还存在该属性源，在接收到 Leave 消息之后，会发送 Join 消息，以表示它还有该属性。其他应用实体如果收到了应用实体 B 发送的 Join 消息，则该属性仍然被保留，不会被注销。只有当其它应用实体等待两个 Join 定时器以上仍没有收到该属性的 Join 消息时，才能认为网络中确实没有该属性了，所以这就要求 Leave 定时器的值大于 2 倍 Join 定时器的值。

**4.LeaveAll 定时器**

每个 GVRP 应用实体启动后，将同时启动 LeaveAll 定时器，当该定时器超时后 GVRP 应

用实体将对外发送 LeaveAll 消息，随后再启动 LeaveAll 定时器，开始新的一轮循环。

接收到 LeaveAll 消息的实体将重新启动所有的定时器，包括 LeaveAll 定时器。在自己的 LeaveAll 定时器重新超时之后才会再次发送 LeaveAll 消息，这样就避免了短时间内发送多个 LeaveAll 消息。

一次 LeaveAll 事件相当于全网所有属性的一次 Leave。由于 LeaveAll 影响范围很广，所以建议 LeaveAll 定时器的值不能太小，至少应该大于 Leave 定时器的值。

每个设备只在全局维护一个 LeaveAll 定时器。

## 21.3 GVRP 配置

### 21.3.1 GVRP 全局设置

#### 配置步骤

1. 在导航栏中选择[GVRP/GVRP 配置]，进入 GVRP 配置界面。
2. 在[GVRP 全局设置]界面中可以查看 GVRP 的全局配置，如图 20.1。
3. 如需修改 GVRP 的全局配置，在 GVRP 全局配置框中修改相应配置，然后单击<应用>。


图 21.1 GVRP 全局设置

#### 配置项说明

[GVRP 全局设置]的相关界面的配置项说明。

表 21.1 [GVRP 全局设置]界面的配置项说明

| 配置项 | 说明 |
| --- | --- |
| 管理状态 | GVRP全局使能开关。<br>● 使能：使能GMRP功能；<br>● 禁止：关闭GMRP功能。<br>注意：默认关闭。 |
| Hold Time | Hold 定时器周期，范围为100-32760(ms)，默认值为100ms； |

| | |
|---|---|
| | 注意hold time*2 <= join time。 |
| Join Time | Join定时器周期，范围为100-32760(ms)，默认值为200ms；<br>注意join time*2<=leave time。 |
| Leave Time | Leave定时器周期，范围为100-32760(ms)，默认值为600ms；<br>注意leave time<=leaveall time |
| Leaveall Time | Leaveall定时器周期，范围为100-32760(ms)，默认值为10000ms；<br>注意leaveall time>=leave time |

### 21.3.2 GVRP 端口配置

#### 配置步骤

1．在导航栏中选择[GVRP/GVRP 配置]，进入 GVRP 配置界面。

2．在[GVRP 端口设置]界面中可以查看 GVRP 的端口配置，如图 21.2。

3．如需修改 GVRP 的端口配置，单击指定端口后面的修改按钮，进入 GVRP 端口配置修改界面，如图 21.3，,配置好后，然后单击<应用>。

| 端口 | GVRP端口模式 | 设置 |
|---|---|---|
| GE/1 | Forbidden | 修改 |
| GE/2 | Forbidden | 修改 |
| GE/3 | Forbidden | 修改 |
| GE/4 | Forbidden | 修改 |
| GE/5 | Forbidden | 修改 |
| GE/6 | Forbidden | 修改 |
| GE/7 | Forbidden | 修改 |
| GE/8 | Forbidden | 修改 |
| GE/9 | Forbidden | 修改 |
| GE/10 | Forbidden | 修改 |

图 21.2 GVRP 端口配置查看界面


图 21.3 GVRP 端口配置修改界面

#### 配置项说明

GVRP[端口配置]的相关界面的配置项说明。

表 21.2 GVRP[端口配置]界面配置项说明

| 配置项 | 说明 |
| --- | --- |
| 端口 | 端口名称信息。 |
| VLAN模式 | 端口的GVRP模式，默认为Forbidden。 |

# 第二十二章 PoE

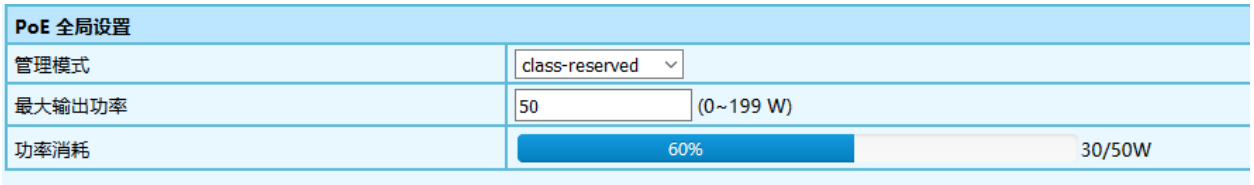
## 22.1 概述

PoE全称为Power Over Ethernet，是指通过10BASE-T、100BASE-TX、1000BASE-T以太网网络供电，其可靠供电的距离最长为100米。通过这种方式，可以有效的解决IP电话、无线AP、便携设备充电器、刷卡机、摄像头、数据采集等终端的集中式电源供电，对于这些终端而言不再需要考虑其室内电源系统布线的问题，在接入网络的同时就可以实现对设备的供电。在通用性方面，目前的PoE供电也有了统一的标准，只要遵循已经发布的802.3af标准和802.3at标准，就可以解决不同厂家设备之间的适配性的问题。按照标准定义，PoE供电系统包含两种设备PSE和PD，对于PSE设备的定义如下：
PSE(power-sourcing equipment)，主要是用来给其它设备进行供电的设备。对于PD设备定义如下：
PD(Powered Device)是在PoE供电系统中用来受电的设备，主要是指一些我线的AP设备或者一些IP PHONE设备以及部分小功率的SOHU类交换机等。

## 22.2 配置管理

通过 PSE 供电系统可以为 PD 设备提供智能的电源管理，包括功率分配、设备功率分级、使能/禁止端口供电等。

### 22.2.1 PoE 全局配置




- 管理模式

  (1) Class-reserved

  (2) Class-consump

  (3) Allocated-reserved

  (4) Allocated-consump

  Class ：按 PD 的分级来分配相对应的功率，如下图所示：

| | Class 0 | Class 1 | Class 2 | Class 3 | Class 4 |
|---|---|---|---|---|---|
| 功率 | 15.4W | 4.0W | 7.0W | 15.4W | 30.0W |

  Allocated: 不考虑 PD 的级别，直接分配一定的功率值给 PD，并且这个功率值是

可以设置的。如果是使能 PoE，功率的最大值是 15.4W，如果使能 PoE+，功率的最大值是 30.0W。

Reserved: 按分配给 PD 的功率来计算系统总的功率。

Consump：按 PD 当前所消耗的功率来计算系统总的功率

- 最大输出功率

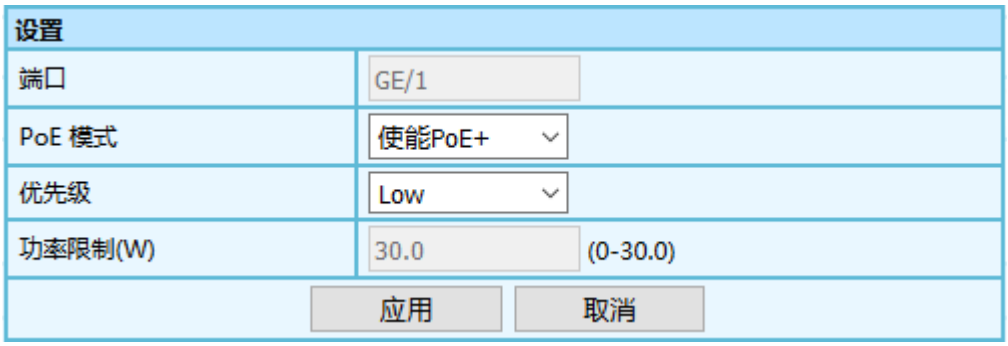
  PSE 系统当前最大的输出总功率。

- 功率消耗百分比

  所有 PD 的消耗功率总和占最大输出总功率的百分比。

### 22.2.2 PoE 端口配置

| | 运行状态 | | | | | | 管理状态 | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 端口 | 状态 | 电流(mA) | 功率(W) | 请求功率(W) | 分配功率(W) | PD Class | PoE 模式 | 优先级 | 功率限制(W) | 设置 |
| GE/1 | PoE turned OFF - Power budget exceeded | 0 | 0 | 30 | 0 | Class 4 | 使能PoE+ | Low | 30 | 修改 |
| GE/2 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |
| GE/3 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |
| GE/4 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |
| GE/5 | PoE turned ON | 327 | 15.5 | 30 | 30 | Class 4 | 使能PoE+ | High | 30 | 修改 |
| GE/6 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |
| GE/7 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |
| GE/8 | No PD Detected | 0 | 0 | 0 | 0 | 未知 | 使能PoE+ | Low | 30 | 修改 |




端口的配置项包括：

(1) 端口模式：使能 PoE+，使能 PoE 和 禁止。

(2) 端口优先级：Low，High 和 Critical，默认为 Low。在 PD 设备消耗的功率大于 PSE 能够提供的总功率时，保证关键设备能够优先供电的手段。当 PSE 设备的供电功率不足时，如果不同端口优先级相同时，按照端口号进行优先排序，端口号小的端口优先得到供电保证。

(3) 端口功率限制：端口的最大输出功率。当管理模式为 Allocated 时，此值才生效。

端口的当前状态项包括：

(1) PoE 端口状态

(2) PD 设备的电流

(3) PD 设备的功率

(4) PD 设备的请求功率

(5) PD 设备的分配功率

(6) PD 设备的分级