



导轨式 i6xx 系列 工业以太网交换机 用户手册

2013 年 05 月 27 日

版本: V 1.2

深圳市金恒威通信技术有限公司

<http://www.inmax.com.cn>

Copyright © 深圳市金恒威通信技术有限公司 版权所有

本档包含专有信息，受版权保护。未经深圳市金恒威通信技术有限公司事先书面许可，不得以任何形式或电子、机械、磁学、光学、化学和人工等其它方式复制、传播、转录本文件的任何部分，也不得将任何部分储存于检索系统中或翻译成任何语言。

免责声明

深圳市金恒威通信技术有限公司专利或专利权不作任何暗示或其它方式授权。深圳市金恒威通信技术有限公司对本档以及本档中描述的产品不作任何暗示或其它方式的保证。本档所提供的信息从发布之日起被认为是准确可靠的。深圳市金恒威通信技术有限公司不承担本档中的任何错误之责任。此外，深圳市金恒威通信技术有限公司不承担任何本档使用或本档信息被滥用以及因使用本档可能引起的任何专利侵权责任。本档的信息和在本档中的产品规格可能会随时变更，恕不另行通知。

目 录

1 前言	1-1
1.1 各类标志.....	1-1
1.2 产品介绍.....	1-1
1.2.1 产品简介.....	1-1
1.2.2 面板介绍.....	1-2
1.2.3 端口介绍.....	1-4
1.2.4 指示灯介绍.....	1-4
1.2.5 缺省配置.....	1-5
1.2.6 登录 Web 页面.....	1-6
1.2.7 工业交换机 WEB 管理概述.....	1-6
第 2 章 系统信息	2-1
第 3 章 高级配置	3-1
第 4 章 端口管理	4-1
4.1 端口配置.....	4-1
4.2 端口链路聚合.....	4-2
4.2.1 设置链路聚合组.....	4-2
4.2.2 LACP 端口配置.....	4-3
4.2.3 链路汇聚基本配置.....	4-4
4.2.4 LACP 状态配置.....	4-5
4.3 端口带宽.....	4-5
4.4 端口镜像.....	4-6
第 5 章 VLAN 设置	5-1
5.1 VLAN 高级功能.....	5-1
5.2 基于端口 VLAN.....	5-2
5.3 802.1Q VLAN.....	5-2
5.3.1 802.1Q VLAN 设置.....	5-3
5.3.2 802.1Q 端口成员配置.....	5-4
5.3.3 802.1Q 端口配置.....	5-5
5.4 GARP.....	5-6
5.4.1 GARP 设置.....	5-6
5.4.2 GVRP 设置.....	5-7
5.4.3 GMRP 设置.....	5-8
第 6 章 QoS 服务质量	6-1
6.1 QoS 配置.....	6-1
6.1.1 优先级.....	6-1
6.1.2 端口 QoS 设置.....	6-1
6.2 调度模式.....	6-2
6.3 发送队列.....	6-2
6.4 DSCP 映射.....	6-3

第 7 章 转发	7-1
7.1 单播 MAC 地址.....	7-1
7.1.1 MAC 地址配置.....	7-1
7.1.2 动态单播 MAC 地址.....	7-2
7.2 组播 MAC 地址.....	7-2
7.3 IGMP 侦听.....	7-4
7.3.1 IGMP 侦听.....	7-5
7.3.2 路由端口.....	7-6
7.3.3 全局参数.....	7-7
第 8 章 安全设置	8-1
8.1 安全配置.....	8-1
8.2 端口授权.....	8-1
8.2.1 802.1X 端口.....	8-2
8.2.2 802.1X 系数参数.....	8-3
8.3 MAC 认证.....	8-4
8.3.1 端口配置.....	8-4
8.3.2 MAC 授权系统参数配置.....	8-5
8.3.3 授权信息.....	8-5
8.4 风暴控制.....	8-6
第 9 章 LLDP	9-1
9.1 LLDP 管理.....	9-1
9.1.1 端口 LLDP 配置.....	9-1
9.1.2 TLVs 配置.....	9-3
9.1.3 LLDP 参数配置.....	9-4
9.2 邻端信息.....	9-5
9.3 LLDP 统计信息.....	9-5
第 10 章 统计信息	10-1
10.1 端口状态.....	10-1
10.2 端口统计.....	10-1
10.3 VLAN 列表.....	10-2
10.4 MAC 地址表.....	10-2
10.4.1 单播 MAC 地址列表.....	10-2
10.4.2 多播 MAC 地址列表.....	10-3
10.5 IGMP 侦听器.....	10-3
10.6 链路汇聚.....	10-3
10.6.1 手工聚合组.....	10-3
10.6.2 静态聚合组.....	10-3
10.6.3 LACP 聚合组.....	10-3
10.7 INMAX RING 环状态.....	10-4
第 11 章 生成树	11-1
11.1 生成树 (STP)	11-2
11.1.1 STP 设置.....	11-2
11.1.2 STP 桥信息.....	11-3
11.1.3 STP 端口属性.....	11-4
11.2 快速生成树 (RSTP)	11-5

第 12 章 INMAX RING 配置	12-1
12.1 INMAX RING 环.....	12-2
12.2 INMAX RING 耦合.....	12-3
12.3 INMAX RING 定时器.....	12-4
第 13 章 SNMP 管理	13-1
13.1 SNMP 账户.....	13-1
13.1.1 SNMP 团体.....	13-1
13.1.2 SNMP 用户.....	13-2
13.2 SNMP 陷阱.....	13-3
13.2.1 全局陷阱设置.....	13-3
13.2.2 陷阱主机 IP.....	13-4
13.2.3 陷阱端口.....	13-4
第 14 章 RMON	14-1
14.1 统计.....	14-1
14.2 历史.....	14-2
14.2.1 历史记录控制.....	14-2
14.2.2 历史记录列表.....	14-3
14.3 告警.....	14-3
14.4 事件.....	14-5
14.4.1 事件.....	14-5
14.4.2 事件日志.....	14-6
第 15 章 精准时间 PTP	15-1
15.1 PTP 系统配置.....	15-1
15.2 PTP 端口设置.....	15-2
15.3 PTP 状态信息.....	15-2
第 16 章 管理配置	16-1
16.1 语言.....	16-1
16.2 IP 配置.....	16-1
16.3 SNTP (简单网络时间协议).....	16-1
16.4 SMTP (简单邮件传输协议).....	16-2
16.5 邮件告警.....	16-2
16.5.1 系统事件.....	16-2
16.5.2 端口事件.....	16-3
16.6 中继告警.....	16-4
16.6.1 系统事件.....	16-4
16.6.2 端口事件.....	16-4
16.7 系统日志.....	16-5
16.8 PING 测试.....	16-6
16.9 账户.....	16-6
16.10 TFTP 服务.....	16-7
16.10.1 更新 Firmware.....	16-7
16.10.2 备份配置.....	16-7
16.10.3 重载配置.....	16-7
16.11 重启.....	16-8
16.12 复位.....	16-8

16.13 保存.....	16-9
第 17 章 退出.....	17-1
附录 A 订购信息.....	A-错误！未定义书签。
附录 B 可用的 MIB.....	B-错误！未定义书签。
附录 C 兼容 SFP 模块信息.....	C-错误！未定义书签。

修订记录

日期	版本	描述
2013-03-04	V1.0	首次发布
2013-04-26	V1.1	增加 IEEE 1588 PTP
2013-5-27	V1.2	增加 GMRP 功能

1 前言

本手册适用于工业交换机 InMax 6XX 系列。

1.1 各类标志

本手册采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 说明	操作内容的描述，进行必要的补充和说明。

图形界面格式约定

格 式	意 义
黑体字	网络管理页关键词用黑体字
斜体字	标签页名称用斜体字
[]	带方括号“[]”表示窗口名、菜单名、子菜单名和域名，如“弹出[新建用户]窗口”。
< >	带尖括号“< >”表示按钮名，如“单击<确定> 按钮”。

1.2 产品介绍

1.2.1 产品简介

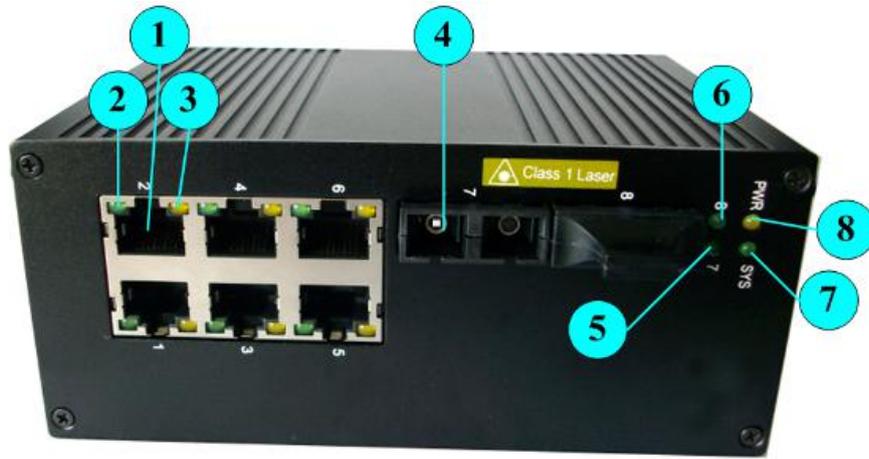
导轨式 6XX 系列工业交换机是新一代管理型工业以太网交换机。该系列交换机专门为满足灵活多变的工业应用需求而设计，提供一种高性价比工业以太网通讯解决方案。产品具有高的可用性、可靠性、安全性来确保关键数据的传输。并且该交换机提供强大的管理功能，可通过 Web、CLI 和 SNMP 管理。导轨式 6XX 系列工业交换机还提供冗余电源支持，支持宽范围的直流电源输入。在结构方面，充分考虑工业安装需求，使用 DIN 导轨式安装或壁挂式安装。

金恒威环网协议（inmax Ring）是深圳金恒威通信技术有限公司的专利技术，专门为工业应用而设计开发的。它提供 20 毫秒内自动恢复功能，用户可通过管理界面指定任意端口（普通以太网端口或聚合端口）进行组环，以提供更快的恢复速度和更高的通信带宽。

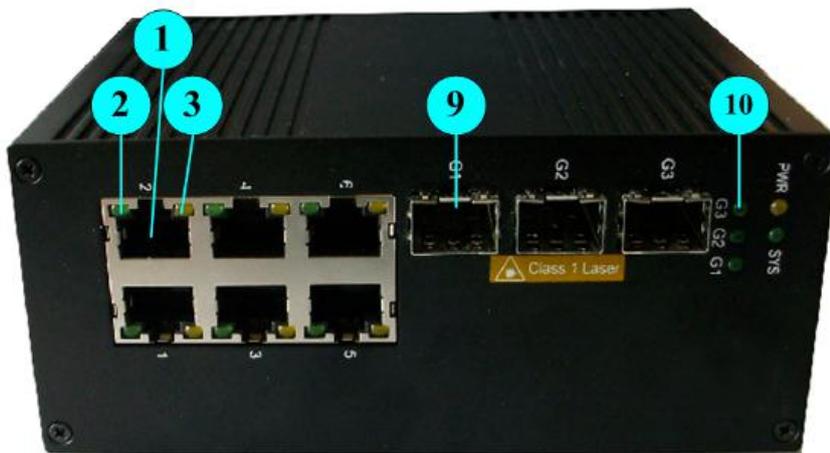
1.2.2 面板介绍

前面板示意图

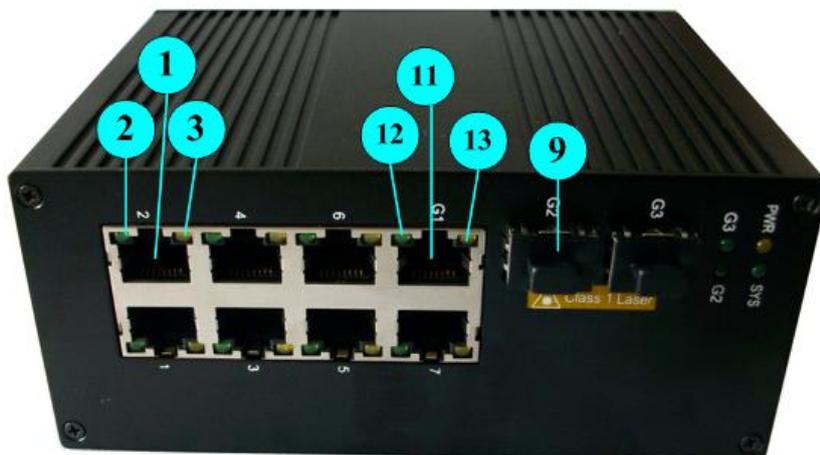
i608A、P608A



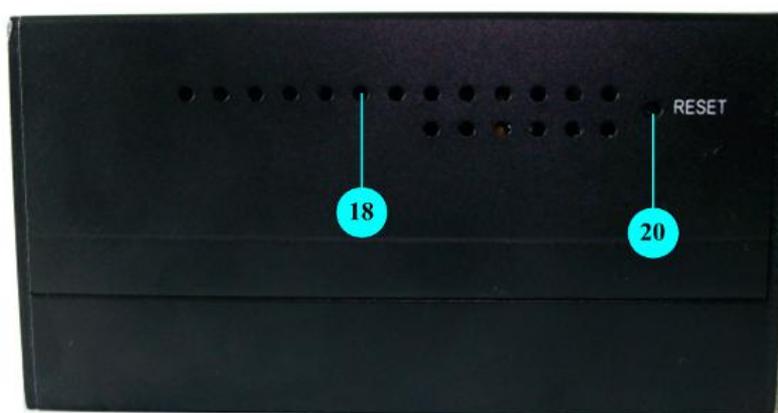
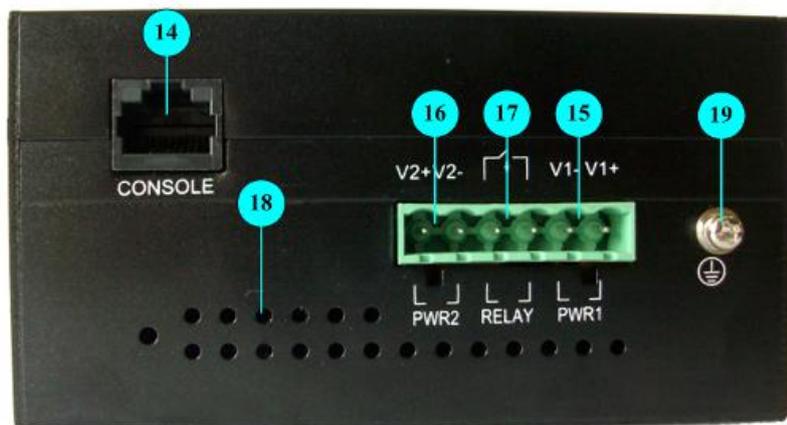
i609A、P609A



i610A、P610A



侧视图



后视图



(1) 10/100BaseTX 自适应以太网端口	(2) (3) 10/100BaseTX 自适应以太网端口状态指示灯
(4) 100Base FX 双纤光口	(5) (6) 1000Base-X 双纤光口状态指示灯 (绿色)
(7) 系统状态指示灯	(8) 电源状态指示灯

(9) 1000Base-X SFP 口	(10) 1000Base-X SFP 口状态指示灯
(11) 10/100/1000BaseTX 自适应以太网端口	(12) (13) 10/100BaseTX 自适应以太网端口状态指示灯
(14) Console 口	(15) 电源 1 (PWR 1)
(16) 电源 2 (PWR 2)	(17) 中继连接线 (RELAY) 继电器的默认状态用 open。
(18) 散热孔	(19) 接地螺钉
(20) 复位键 (RESET)	(21) 导轨

1.2.3 端口介绍

型号	以太网端口数	Console 口	电源接口
i608	6X10/100BaseTX 端口+ 2X100BaseFX 端口	1个 RS232	2个 24V DC
i609	6 X10/100BaseTX 端口+ 3X1000BaseX SFP 插槽		
i610	7X10/100BaseTX 端口+1X10/100/1000BaseTX 端口 + 2X1000BaseX SFP 插槽		

1.2.4 指示灯介绍

10/100BaseTX 端口

端口指示灯状态	说明
绿灯	绿灯亮—端口工作在 100Mbps 绿灯不亮—端口工作在 10Mbps
黄灯	黄灯亮并闪烁—LINK UP 状态, 正在收发数据包 黄灯亮- 不闪烁--端口 Link Up 黄灯不亮- 端口 Link down

10/100/1000BaseTX 自适应以太网端口

端口指示灯状态	说明
绿灯	绿灯亮—端口 Link Up 绿灯不亮—端口 Link Down

黄灯	黄灯闪烁—正在收发数据包 黄灯不亮—没有收发数据包
----	------------------------------

100BaseFX 端口/1000BaseX SFP 插槽

端口指示灯状态	说明
绿灯	绿灯亮并闪烁—端口 Link Up, 正在收发数据包 绿灯亮—端口 Link Up 绿灯不亮—端口 Link Down

其他指示灯

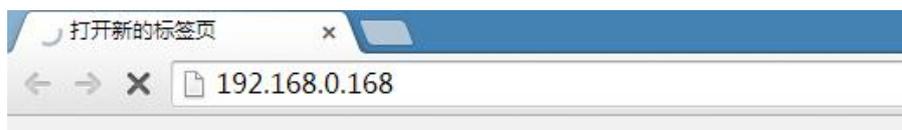
端口模式指示灯状态	说明
电源指示灯 (PWR)	黄灯亮—电源开启 黄灯不亮—未上电
系统指示灯	绿灯亮—系统启动完成 绿灯不亮—系统启动未完成

1.2.5 缺省配置

用户级别	用户名	密码	权限
Administrator (管理员)	superuser	123	可执行交换机所有操作
User (用户)	manager	123	除以下操作外的其他操作都可执行： <ul style="list-style-type: none"> ● 创建或删除账号； ● 恢复缺省配置； ● 利用 TFTP 服务进行软件升级、备份和恢复配置。
Visitor(访客)	guest	(none)	可使用因特网诊断命令，如 ping 命令以维护设备，以及“show”命令，但以下“show”命令除外：“show user”、“show snmp community”、“show snmp traps-host”和“show snmp user”。 备注：Visitor 只可通过串口访问交换机。

1.2.6 登录 Web 页面

可通过打开 Web 浏览器，输入交换机缺省地址：<http://192.168.0.168>，按 **Enter** 键。



 说明：

登录交换机时，应使 PC 的 IP 网段与交换机网段一致。首次登录时，设置 PC 的 IP 地址为 192.168.0.x (x 代表 1~254)，子网掩码设置为 255.255.255.0，但 PC IP 不可与交换机相同，即不能为 192.168.0.253。

此时出现登录窗口，如下图所示。输入缺省用户名和密码（参考本手册 [1.2.5 缺省配置](#)）。点击<确定>按钮，将看到交换机系统信息。如选中“记住我的密码”，下次登录时将无需输入密码。



如需在首次登录交换机时修改其 IP 地址，可用 RS232 串口线连接 PC 与交换机或通过 telnet 登录交换机进行修改，具体请参考《导轨式 6XX 系列工业交换机 命令手册 V1.0》。

1.2.7 工业交换机 WEB 管理概述

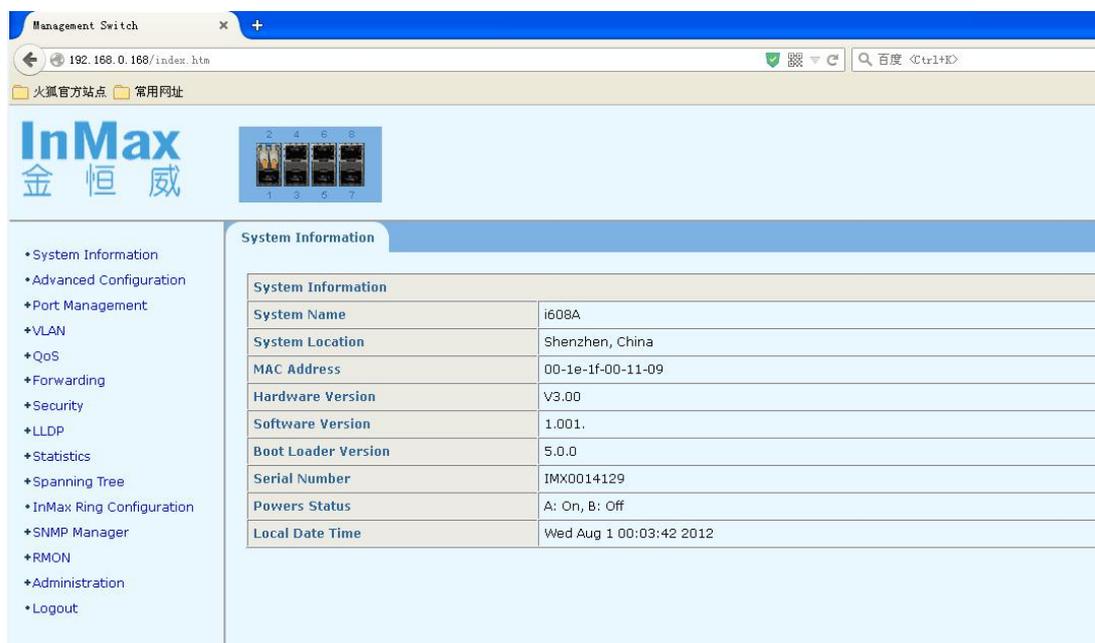
本手册主要通过 WEB 页面来介绍导轨式 6XX 系列工业交换机管理功能，包括如下内容：

菜单名	功能简介
系统信息	显示设备系统信息
高级配置	全局开启或关闭一些主要的功能
端口管理	端口配置、端口带宽和端口镜像的配置

VLAN	配置基于端口的 VLAN 和 802.1Q VLAN
QoS 服务质量	配置 QoS、调度模式、发送队列和 DSCP 映射
转发	单播 MAC 地址和多播 MAC 地址的配置以及 IGMP Snooping 配置
安全设置	设置 Radius 服务器、配置端口授权、MAC 认证和风暴控制
LLDP	配置端口 LLDP 和邻居信息，查看 LLDP 统计信息
统计信息	包括设备端口状态、VLAN 列表、MAC 地址列表、IGMP 侦听器、链路聚合组合 inmax Ring 环状态统计
生成树	配置生成树（STP）和快速生成树（RSTP）
inmax Ring 配置	配置 inmax Ring 环、耦合和定时器
SNMP 管理	配置 SNMP 账户和陷阱
RMON	配置 RMON 事件、告警和历史，查看 RMON 统计
管理配置	可设置设备系统语言、IP、SNTP、SMTP、邮件告警、中继告警，查看系统日志，进行 Ping 测试，添加、修改或删除新账户，通过 TFTP 服务器更新系统软件、备份配置文件和重载配置文件，可重启系统、复位和保存配置。
退出	退出 Web 页面

第 2 章 系统信息

系统信息，即为交换机基本信息，如下图所示：



通过 SNMP 软件可以给每个工业交换机配置相应的系统名字和系统位置，以方便管理。

📖 说明：

本手册以 i608A 或 i610A 为例。

第 3 章 高级配置

该页用来全局启用/禁用协议如 IGMP 侦听、GVRP、STP、LACP、LLDP、802.1X、inmax Ring、PTP 和 Modbus，如下图所示：

全局协议配置	
系统高级配置	
IGMP 侦听	关闭
GVRP	关闭
STP	快速生成树(RSTP)
LACP	关闭
LLDP	关闭
802.1x	关闭
Fi Ring	关闭
PTP	关闭
Modbus	关闭
提交	

第 4 章 端口管理

该菜单下可配置端口、端口链路聚合、端口带宽和端口镜像。

4.1 端口配置

首先选择要进行配置的端口。可配置设备所有端口的状态、协商、速率/双工、流控，MAC 地址学习功能和 MDI/MDIX。



注意：

- 只有启用端口，才可以配置其协商、速率/双工、流控，MAC 地址学习功能和 MDI/MDIX。
 - 只有把协商配置成强制模式，才可配置速率/双工。
-

状态：	是否启用该端口。
协商：	如选择自协商，将为一个网段的两个端之间交换配置信息提供机制，自动选择具有最高性能的运行模式；如选择强制，则需手动配置速率/双工。
速率/双工：	有四个选项：10M 半双工、10M 全双工、100M 半双工、100M 全双工。
流控：	流量控制通过限制与导轨式 6XX 交换系列相连的终端站或终端段的流量，避免帧损失。可开启/关闭流量控制功能。如关闭，则端口将全速运行。
MAC 地址学习功能：	交换机是根据报文的目的 MAC 地址对报文进行转发的，因此交换机维护了一种记录 MAC 地址与端口对应关系的转发表来指导交换机进行转发，这个表称为 MAC 地址转发表。交换机将接收到的报文的源 MAC 地址以及接收端口记录到该表中，供后续报文转发使用，这个记录过程称为 MAC 地址的学习过程。
MDI/MDIX：	有三个选项：自动、MDI、MDIX。

各端口配置完成后点击<提交>按钮，其配置结果将显示在页面下方。

端口配置

端口	状态	协商	速率/双工	流控	MAC地址学习	MDI/MDIX
Ethernet0/1	开启	自协商	10M 半双工	关闭	开启	自动

端口状态

端口	状态	链路状态	协商	速率/双工配置	实际的速率/双工	流控配置	实际流控	MAC地址学习	MDI/MDIX配置	实际MDI/MDIX
Ethernet0/1	开启	断开	自协商	-	-	关闭	-	开启	自动	MDI
Ethernet0/2	开启	断开	自协商	-	-	关闭	-	开启	自动	MDIX
Ethernet0/3	开启	断开	自协商	-	-	关闭	-	开启	自动	MDIX
Ethernet0/4	开启	连接	自协商	-	100M 全双工	关闭	关闭	开启	自动	MDI
Ethernet0/5	开启	断开	自协商	-	-	关闭	-	开启	自动	MDIX
Ethernet0/6	开启	断开	自协商	-	-	关闭	-	开启	自动	MDIX
Ethernet0/7	开启	断开	强制	100M 全双工	-	关闭	-	开启	自动	-
Ethernet0/8	开启	断开	强制	100M 全双工	-	关闭	-	开启	自动	-

4.2 端口链路聚合

链路聚合是将两个或更多数据信道结合成单个信道,该信道以单个更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备。

端口有 3 种聚合模式：手工、静态和动态。

4.2.1 设置链路聚合组

导轨式 6XX 系列工业交换机支持多达 13 个链路聚合组。

设置链路聚合组有如下技术优势：

- 带宽增加--带宽相当于聚合组的端口的带宽总和。如下图所示的 Trunk1 的带宽达到了 300M（端口 1~3 的带宽之和）。
- 增加冗余--只要组内不是所有的端口都 down 掉，两个交换机之间仍然可以继续通信。
- 负载均衡--流量可以在聚合组内的端口上自动进行负载均衡。

注意：

- 如在高级配置内未开启 LACP 链路聚合控制协议(Link Aggregation Control Protocol)，则只能手工配置端口链路聚合；
- 如要进行静态端口链路聚合的配置，需先在高级配置内开启 LACP 功能。
- 链路聚合组端口必须在同一 VLAN 里。
- 链路聚合组端口的 GVRP、单播、组播、inmax Ring 以及 VLAN 配置必须相同。

配置步骤：

步骤 1 选择聚合 ID，共有 T1 ~ T13，13 个聚合组。

步骤 2 给所选聚合组命名。

步骤 3 选择聚合类型。

手工：手工聚合组只能手工设置或删除，LACP 可以处于禁用状态。

静态：静态聚合组只能手动设置或删除，任何一个静态 LACP 聚合组端口应使该端口链路聚合控制协议（LACP）处于启用状态。当一个静态 LACP 聚合组被（手动）删除时，该聚合组中的处于“启用”状态的所有端口将自动产生一个或多个动态 LACP 聚合组。

步骤 4 选择聚合组成员端口。

链路聚合设置								
聚合 ID	17							
聚合组名字	Trunk7							
聚合类型	静态							
端口	Ethernet0/							
	1	2	3	4	5	6	7	8
端口成员	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
<input type="button" value="提交"/>								

步骤 5 点击<提交>，链路聚合信息将显示在页面下方。

链路聚合信息				
聚合 ID	聚合组名字	聚合类型	端口列表	删除
T2	Trunk2	手工	Ethernet0/1,3	<input type="button" value="删除"/>
T7	Trunk7	静态	Ethernet0/7-8	<input type="button" value="删除"/>

4.2.2 LACP 端口配置

该功能提供动态配置链路汇聚组。[4.2.1](#) 中已配置了两组链路汇聚组，包含端口 1、3、7、8，端口 2、4、5、6 可配置为 LACP 动态端口。

动态 LACP 聚合是一种系统自动创建或删除的汇聚，动态汇聚组内端口的添加和删除是 LACP 协议自动完成的。只有基本配置相同、速率和双工属性相同、连接到同一个设备、并且对端端口也满足以上条件时，端口才能被动态汇聚在一起。

LACP 的协商过程

在收到对端的 LACP 报文后，选取系统 ID（请参考 [3.2.3](#)）优先级比较高的系统。对端收到更新后的 LACP 报文后，也会把相应的端口设置成聚合状态。

基本汇聚设置	
LACP系统优先级(1-65535)	<input type="text" value="1"/>
<input type="button" value="提交"/>	

4.2.4 LACP 状态配置

LACP 动态汇聚端口可设成主动状态和被动状态。

- **主动**：使端口处于主动协商状态，在该状态下，端口通过发送 LACP 数据包开始与其他端口进行协商。
- **被动**：将端口置于被动协商状态，在该状态下，端口会响应其接收到的 LACP 数据包，但不会开始 LACP 数据包协商。该设置最大程度地减少了 LACP 数据包的传输。

有一个或两个主动 LACP 端口的链路可进行动态 LACP 聚合。两方都是被动端口的链路将不进行动态 LACP 聚合，因为这两个端口都在等候对端设备的 LACP 协议数据包。

 说明：

该设备上处于主动状态的动态汇聚端口可与对端处于主动和被动状态的端口协商汇聚，但该设备上处于被动状态的动态汇聚端口只能与对端处于主动状态的端口协商汇聚。

LACP 状态设置		Ethernet0/							
端口		1	2	3	4	5	6	7	8
LACP 状态	被动	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>				
	主动	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>					
<input type="button" value="提交"/>									

4.3 端口带宽

设置每个端口的出端口速率限制，即对端口发送报文的速率进行限制。

端口：配置速率限制端口。

出端口限速：配置该端口所需的发送速率。选择“关闭”表示该端口无出口速率限制，这意味着在该端口上，发送数据将全速运行。

完成配置后，单击<提交>，使其生效。页面下方列出各端口的速率限制。

端口	出端口限速
Ethernet0/1	关闭
提交	

速率限制列表

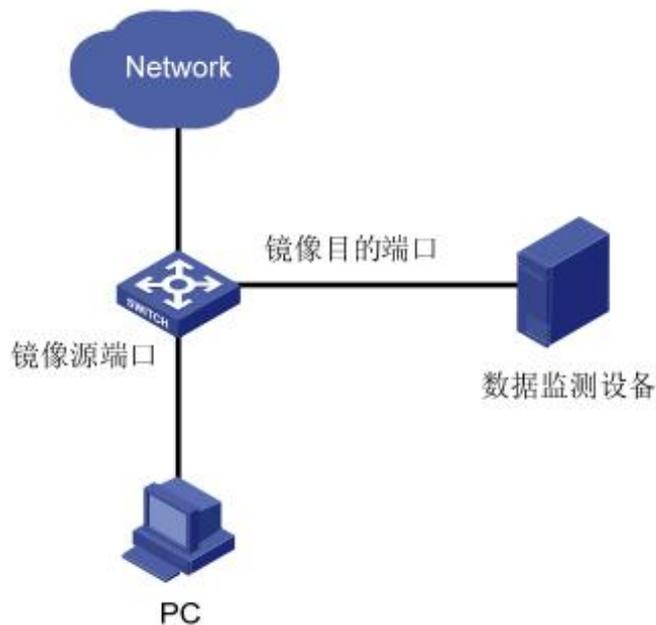
端口	出端口限速	端口	出端口限速
Ethernet0/1	关闭	Ethernet0/2	关闭
Ethernet0/3	关闭	Ethernet0/4	关闭
Ethernet0/5	关闭	Ethernet0/6	关闭
Ethernet0/7	关闭	Ethernet0/8	关闭

说明：上图灰色部分表示该端口为聚合端口，不可配置限速功能。

 注意：开启限速的端口不能是链路汇聚的端口。

4.4 端口镜像

端口镜像是把交换机指定端口的报文复制给管理端口；其中被复制的端口称为镜像端口，复制的端口称为管理端口。管理端口会接入数据检测设备，用户利用这些设备分析管理端口接收到的报文，进行网络监控和故障排除。如下图所示：



配置步骤:

步骤 1 开启/关闭镜像状态。

步骤 2 如开启了端口镜像状态，在管理端口一行选择一个端口作为管理端口。

 注意:

- 管理端口不能是链路汇聚端口;
- 只能选择一个端口作为管理端口;

步骤 3 其他端口都是镜像端口，

可配置成“不镜像”：即该端口的任何报文都不被镜像。

“镜像入端口”：即该端口的任何接收报文都被镜像到管理端口。

“镜像出端口”：即该端口的任何发送报文都被镜像到管理端口。

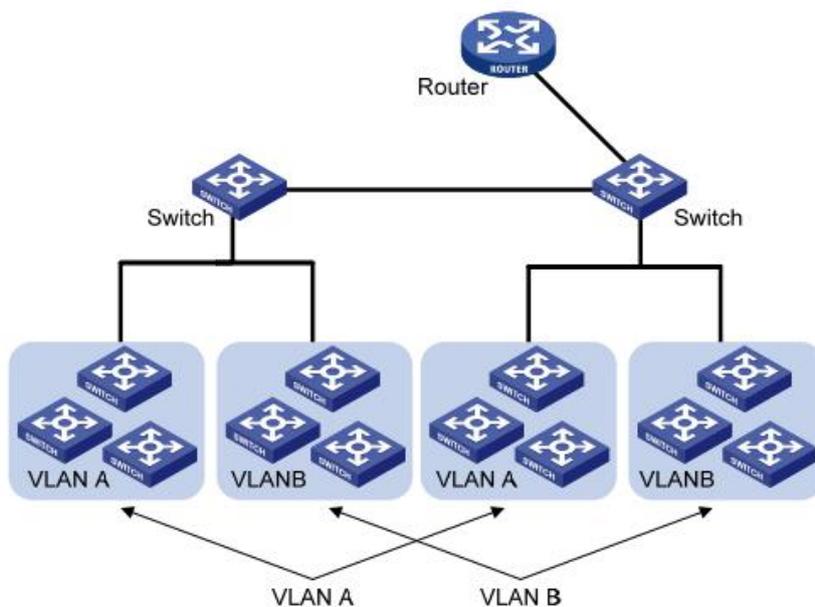
“镜像出入端口”：即该端口的任何接收和发送报文都被镜像到管理端口。

步骤 4 点击<提交>生效。

端口镜像配置								
镜像状态	<input type="text" value="开启"/>							
端口	Ethernet0/							
	1	2	3	4	5	6	7	8
管理端口	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
不镜像	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
镜像入端口	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
镜像出端口	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>				
镜像出入端口	<input type="radio"/>	<input checked="" type="radio"/>						
<input type="button" value="提交"/>								

第 5 章 VLAN 设置

VLAN 的组成不受物理位置的限制，因此同一 VLAN 内的主机也无须放在同一物理空间里。如下图所示，VLAN 把一个物理上的 LAN 划分成多个逻辑上的 LAN，每个 VLAN 是一个广播域。VLAN 内的主机间通过传统的以太网通信方式即可进行报文的交互，而处在不同 VLAN 内的主机之间如果需要通信，则必须通过路由器或三层交换机等网络层设备才能够实现。



与传统以太网相比，VLAN 具有如下的优点：

- 控制广播域的范围：局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了 LAN 的安全性：由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 灵活创建虚拟工作组：使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。

目前导轨式 6XX 系列工业交换机支持基于端口的 VLAN 和 802.1Q VLAN。

5.1 VLAN 高级功能

可在此选择关闭交换机的 VLAN 功能，或选择配置交换机基于端口的 VLAN 或 802.1Q VLAN。点击<提交>生效。



5.2 基于端口 VLAN

基于端口的 VLAN 是最简单的一种 VLAN 划分方法。用户可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

基于端口的 VLAN 具有实现简单、易于管理的优点，适用于连接位置比较固定的用户。



注意：

在 VLAN 高级功能页选择“基于端口 VLAN”，才可配置基于端口的 VLAN。

配置举例：

如下图所示，配置了 VLAN ID 为 1，端口成员为端口 6 和聚合组 T2，表示与交换机端口 6 相连的设备和与 T1 聚合端口相连的设备处于同一 VLAN 内，相互之间可互相通信，但不可与其他 VLAN 内的成员通信。

另还配置了 VLAN 2，其 VLAN ID 为 2，成员端口为端口 5、6 和 T7，即表示与其相连的设备处于同一个 VLAN 内，互相可以互相通信，但不可与其他 VLAN 内设备通信。

配置的 VLAN 可修改其名称和成员端口，也可删除。

基于端口VLAN 设置						
VLAN ID	<input type="text" value="1"/>					
VLAN 名称	<input type="text"/>					
端口	Ethernet0/				TRUNK	
	2	4	5	6	T2	T7
成员端口	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="创建"/>						
VLAN 列表						
VLAN ID	VLAN 名称	端口			修改	删除
1	vlan 1	Ethernet0/6,T2			<input type="button" value="修改"/>	<input type="button" value="删除"/>
2	vlan 2	Ethernet0/5-6,T7			<input type="button" value="修改"/>	<input type="button" value="删除"/>

5.3 802.1Q VLAN

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。

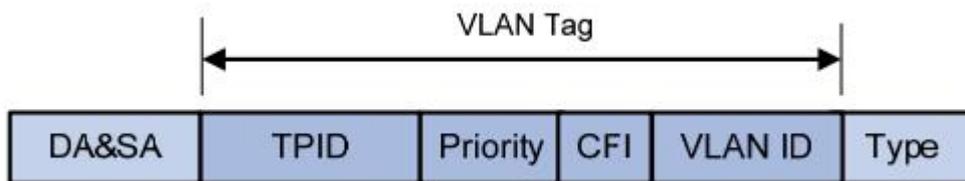
IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案，对带有 VLAN 标识的报文结构进行了统一规定。

传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如下图所示。



其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。

IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。



如上图所示，VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

- TPID 用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。
- Priority 表示报文的 802.1P 优先级，长度为 3bit。
- CFI 字段标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1bit，取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装，缺省取值为 0。
- VLAN ID 标识该报文所属 VLAN 的编号，长度为 12bit，取值范围为 0~4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1~4094。

网络设备利用 VLAN ID 来识别报文所属的 VLAN，根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 值，来对报文进行处理。

 说明：配置 802.1Q VLAN 前，请在 VLAN 高级功能页选择“802.1Q VLAN”。

5.3.1 802.1Q VLAN 设置

用户可以新建一个带有特定 VID 和 VLAN 名称的 VLAN 组。可以创建多达 252 个 VLAN 组，同时每个 VLAN 组的 ID 号范围为 1 到 4094。

有一个带有 VLAN 标识符（VID）为 1 的缺省 VLAN 组 default，每个端口在缺省情况下都是该组的成员；在某端口从该组中被删除之前，它一直是该组的成员。

页面下方列出所有现有的 VLAN 组，以及每个 VLAN 组的信息。用户可以修改或删除现有的 VLAN 组。

 **注意：**不允许删除 VID 号为 1 的 VLAN 组。

802.1Q VLAN 设置				
VID	<input type="text" value="1"/>			
VLAN 名称	<input type="text"/>			
<input type="button" value="创建"/>				
VLAN 列表				
VID	VLAN 类型	VLAN 名称	修改	删除
1	静态	Default	-	-
2	静态	VLAN 2	<input type="button" value="修改"/>	<input type="button" value="删除"/>

5.3.2 802.1Q 端口成员配置

配置一个 VLAN 组的端口成员关系。对于该 VLAN 组，每个端口可被配置为一个特定成员：

Tag: 表示该端口是 VLAN 组的一个 tagged 成员。端口转发的所有数据包均带标签。数据包包含 VLAN 信息。

Untag: 表示该端口是 VLAN 组的一个 untagged 成员。端口转发的数据包不带标签。

排除: 非 VLAN 组的端口。但是，端口可通过 GVRP 动态地被添加到该 VLAN 组中。

禁止: 即使开启了 GVRP 功能，仍不允许端口被添加到 VLAN 组中。

802.1Q VLAN 配置								
VID	<input type="text" value="2"/>							
VLAN 名称	<input type="text" value="vlan 2"/>							
端口	Ethernet0/							
	1	2	3	4	5	6	7	8
Tag	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untag	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
排除	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
禁止	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="button" value="提交"/>								

5.3.3 802.1Q 端口配置

PVID: 当交换机端口接收到的报文不带有 VLAN Tag 时，交换机会自动为该报文分配一个 VID，这个 VID 就是端口的默认 VLAN ID，简称 PVID。每个端口只能有一个端口 VLAN ID (PVID)。当不带标签的以太网数据包到达端口时，它将被打上 PVID VID 标签。每个端口的缺省 PVID 为 1。

端口 VLAN 模式: 从该下拉列表中，可以选择**混合**（默认）、**访问**和**主干**三种模式。这三种端口在加入 VLAN 和对报文进行转发时会进行不同的处理。

- **访问模式:** 端口只能属于 1 个 VLAN，一般用于交换机与终端用户之间的连接。一个访问端口只能归属于一个 VLAN 组；在发送数据时，标签被删除（即 Untagged）。
- **主干模式:** 端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间的连接。一个主干端口可以归属于多个 VLAN 组，但只允许在一个 VLAN 组里被配置为 Untag。除了发出的数据包所在的 VLAN 里所带的 VID 与 PVID 相同的情况外，所有的数据包均带标签。
- **混合模式:** 混合端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。混合端口类似于主干端口，不同的是它可以使用户灵活配置每个端口为 Tag 或 Untag。

帧类型: 选择端口接收以太网数据包的方式。当选择“**全部接收**”时，端口接收所有入口数据包。而选择“**仅接受 Tag**”时，端口只接收带标签的数据包，不带标签的数据包将被丢弃。

VLAN 接收过滤: 通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤。如果端口开启了该功能，接收的报文所在的 VLAN ID 不在该端口中，即该端口没有加入到相应的 VLAN 中，报文会被马上丢弃。

端口	PVID	端口VLAN模式	帧类型	VLAN接收过滤
Ethernet0/2	1	访问	全部接收	关闭
<input type="button" value="提交"/>				

端口状态

端口	PVID	端口VLAN模式	帧类型	VLAN接收过滤
Ethernet0/2	1	访问	接受所有	开启
Ethernet0/4	1	访问	接受所有	开启
Ethernet0/5	2	混合	接受所有	开启
Ethernet0/6	1	主干	接受所有	开启
T2	1	混合	接受所有	开启
T7	2	混合	接受所有	开启

5.4 GARP

 说明：请先在[高级配置](#)里开启 GVRP。

5.4.1 GARP 设置

GARP（Generic Attribute Registration Protocol）即通用属性注册协议。GARP 提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息（如 VLAN、组播信息等）。GARP 本身不作为一个实体存在于设备中，遵循 GARP 协议的应用实体称为 GARP 应用。当 GARP 应用实体存在于设备的某个端口上时，该端口对应于一个 GARP 应用实体。

GARP 成员之间的信息交互借助于消息的传递来完成，主要有三类消息起作用，分别为加入消息、离开消息和全部离开消息。

- 当一个 GARP 应用实体希望其它设备注册自己的属性信息时，它将对外发送加入消息；当收到其它实体的加入消息或本设备静态配置了某些属性，需要其它 GARP 应用实体进行注册时，它也会向外发送加入消息。
- 当一个 GARP 应用实体希望其它交换机注销自己的某属性信息时，它将对外发送离开消息；当收到其它实体的离开消息注销某些属性或静态注销了某些属性后，它也会向外发送离开消息。
- 每个 GARP 应用实体启动后，将同时启动全部离开计时器，当该计时器超时后 GARP 应用实体将对外发送全部离开消息，全部离开消息用来注销所有的属性，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。

离开消息、全部离开消息与加入消息配合确保属性的注销或重新注册。

通过消息交互，所有待注册的属性信息可以传播到同一局域网内开启了 GARP 功能的所有设备上。

GARP 消息发送的时间间隔是通过计时器来实现的，用于控制 GARP 消息的发送周期：

- **加入计时器：**GARP 应用实体可以通过将每个加入消息向外发送两次来保证消息的可靠传输，在第一次发送的加入消息没有得到回复的时候，GARP 应用实体会第二次发送加入消息。两次加入消息发送之间的时间间隔用加入计时器来控制。取值范围为 10-2147483640 毫秒，必须为 10 的正整数倍，缺省值为 200 毫秒。
- **离开计时器：**当一个 GARP 应用实体希望注销某属性信息时，将对外发送离开消息，接收到该消息的 GARP 应用实体启动离开计时器，如果在该计时器超时之前没有收到加入消息，则注销该属性信息。取值范围为 30-2147483640 毫秒，必须为 10 的正整数倍，缺省值为 600 毫秒。
- **全部离开计时器：**每个 GARP 应用实体启动后，将同时启动全部离开计时器，当该计时器超时后，GARP 应用实体将对外发送全部离开消息，以使其它 GARP 应用实体重新注册本实体上所有的属性信息。随后再启动全部离开计时器，开始新一轮循环。取值范围为 40-2147483640 毫秒，必须为 10 的正整数倍，缺省值为 1000 毫秒。

GARP 定时器设置	
加入计时器(10-2147483640)	<input type="text" value="200"/> 毫秒(10的倍数)
离开计时器(30-2147483640)	<input type="text" value="600"/> 毫秒(10的倍数)
全部离开计时器(40-2147483640)	<input type="text" value="10000"/> 毫秒(10的倍数)
<input type="button" value="提交"/>	

5.4.2 GVRP 设置

GVRP (GARP VLAN Registration Protocol, GARP VLAN 注册协议) 是 GARP 的一种应用。它基于 GARP 的工作机制, 用来维护设备中的 VLAN 动态注册信息, 并传播该信息到其它交换机。

设备启动 GVRP 特性后, 能够接收来自其它设备的 VLAN 注册信息, 并动态更新本地的 VLAN 注册信息, 包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个端口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播, 以使同一局域网内所有设备的 VLAN 信息达成一致。GVRP 传播的 VLAN 注册信息既包括本地手工配置的 VLAN 静态注册信息, 也包括来自其它设备的 VLAN 动态注册信息。

GVRP 的端口注册类型有三种: 正常、固定和禁止, 各类型描述如下。

- **正常类型:** 允许该端口动态注册、注销 VLAN, 传播动态 VLAN 以及静态 VLAN 信息。
- **固定类型:** 禁止该端口动态注册、注销 VLAN, 只传播静态 VLAN 信息, 不传播动态 VLAN 信息。该端口只允许静态 VLAN 通过, 即只对其它 GARP 成员传播静态 VLAN 信息。
- **禁止类型:** 禁止该端口动态注册、注销 VLAN。该端口只允许缺省 VLAN (即 VLAN1) 通过, 即只对其他 GARP 成员传播 VLAN1 的信息。

配置步骤:

选择配置端口, 开启或关闭其 GVRP 状态, 设置其端口 GVRP 注册类型, 点击<提交>, 其配置结果将显示在页面下方。



注意:

- 如果端口已经在 inmax Ring 里配置了, 则该端口不能开启 GVRP 功能;
- 配置 GVRP 的端口类型必须为主干端口。

端口	GVRP状态	GVRP注册类型
Ethernet0/2	关闭	正常
提交		
GVRP 端口属性		
端口	GVRP状态	GVRP注册类型
Ethernet0/2	关闭	正常
Ethernet0/4	关闭	正常
Ethernet0/5	关闭	正常
Ethernet0/6	关闭	正常
T1	开启	固定
T2	关闭	正常

5.4.3 GMRP 设置

GMRP 是基于 GARP 协议的一种具体的应用。它利用了 GARP 协议的工作机制维护交换机中的多播 MAC 表信息，从而避免多播报文被广播而浪费网络资源的情形。所有支持 GMRP 特性的交换机能够接收来自其他交换机的多播 MAC 地址注册信息，并动态更新本地的多播 MAC 地址注册信息，包括当前哪些端口下存在这些多播 MAC 地址等信息。同时所有支持 GMRP 特性的交换机能够将本地的多播 MAC 地址注册信息向其他交换机传播。

配置步骤如下：

- 1、开启全局 GMRP 功能
- 2、选择特定的设置端口
- 3、启用或关闭端口的 GMRP 功能

GARP		GVRP		GMRP	
Port		GMRP			
Ethernet0/1		Disabled			
Apply					
GMRP Attribute type					
Port		GMRP			
Ethernet0/1		Disabled			
Ethernet0/2		Enabled			
Ethernet0/3		Disabled			
Ethernet0/4		Disabled			
Ethernet0/5		Disabled			
Ethernet0/6		Disabled			
Ethernet1/1		Disabled			
Ethernet1/2		Disabled			

第 6 章 QoS 服务质量

QoS (Quality of Service, 服务质量), 在 Internet 中, QoS 所评估的就是网络转发分组的服务能力。由于网络提供的服务是多样的, 因此对 QoS 的评估可以基于不同方面。通常所说的 QoS, 是对分组转发过程中为延迟、抖动、丢包率等核心需求提供支持的服务能力的评估。

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

随着计算机网络的高速发展, 越来越多的网络接入 Internet。Internet 无论从规模、覆盖范围和用户数量上都拓展得非常快。越来越多的用户使用 Internet 作为数据传输的平台, 开展各种应用, 比如远程教学、远程医疗、可视电话、电视会议、视频点播等这些新业务有一个共同特点, 即对带宽、延迟、抖动等传输性能有着特殊的需求。新业务的不断涌现对 IP 网络的服务能力提出了更高的要求, 用户已不再满足于能够简单地将报文送达目的地, 而是还希望在转发过程中得到更好的服务, 诸如支持为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级。所有这些, 都要求网络应当具备更为完善的服务能力。

6.1 QoS 配置

6.1.1 优先级

可选择开启或关闭 (缺省) 该设备的优先级, 点击<提交>生效。

6.1.2 端口 QoS 设置

可设置该设备各端口的 QoS 配置。

802.1P: 802.1P 是 IEEE 802.1Q (VLAN 标签技术) 标准的扩充协议, 它们协同工作。IEEE 802.1Q 标准定义了为以太网 MAC 帧添加的标签。VLAN 标签有两部分: VLAN ID (12 比特) 和优先级 (3 比特)。IEEE 802.1Q VLAN 标准中没有定义和使用优先级字段, 而 802.1P 中则定义了该字段。

端口优先级: 共八个优先级 0-7, 对应 802.1P 的优先级。

DSCP: 是否开启 DSCP 优先级。

配置结果将显示在页面下方的端口优先级列表中。

端口	802.1p	端口优先级	DSCP
Ethernet0/2	关闭	0	关闭
提交			

端口优先级列表

端口	802.1p	端口优先级	DSCP	端口	802.1p	端口优先级	DSCP
Ethernet0/2	关闭	0	关闭	Ethernet0/4	关闭	0	关闭
Ethernet0/5	关闭	0	关闭	Ethernet0/6	关闭	0	关闭
T1	关闭	0	关闭	T2	关闭	0	关闭

6.2 调度模式

该页面设置队列调度算法及相关参数。当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。导轨式 6XX 系列以太网工业交换机支持的队列调度算法有**严格优先级**和**加权轮询（8:4:2:1）**。

严格优先级：队列实行严格的优先调度算法，SP 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。

加权轮询（8:4:2:1）：加权循环调度算法。加权循环调度算法 WRR（Weighted Round Robin）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。加权循环（WRR）提供所有业务队列服务，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。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。其工作原理是 WRR 队列调度将每个端口分为多个输出队列，队列之间轮流调度，保证每个队列都得到一定的服务时间，WRR 可为每个队列配置一个加权值（依次为 w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 50、30、10、10（依次对应 w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 10Mbit/s 带宽，避免了采用 SP 模式时低优先级队列中的报文可能长时间得不到服务的缺点。WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间，如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

6.3 发送队列

当缺省的 802.1p 优先级和本地优先级的映射关系不能满足用户需求时，用户可以修改 802.1p 优先级到本地优先级的映射关系，从而实现 802.1p 优先级和出端口队列之间映射关系的改变，将不同优先级的报文放入相应的出端口队列进行调度。

下表列出缺省的 802.1p 优先级到本地优先级的映射。

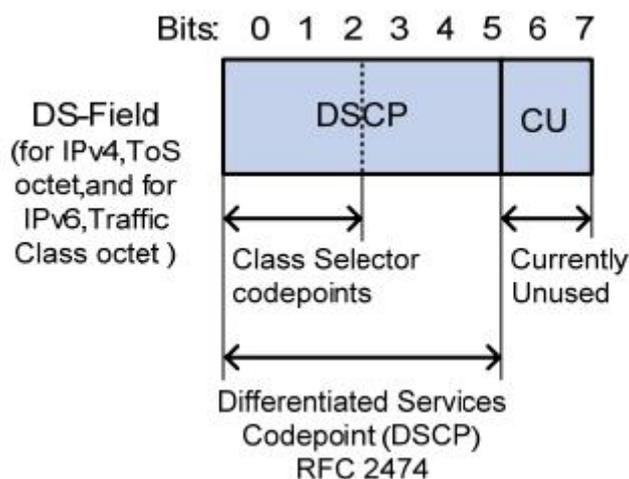
802.1p priority	Local precedence
0	Q0
1	Q0
2	Q1
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

用户可按照具体的需求更改优先级队列。单击<Apply>生效。如无需进行更改，直接单击<Apply>。

发送队列设置								
优先级	0	1	2	3	4	5	6	7
发送队列	<input checked="" type="radio"/> Q0	<input checked="" type="radio"/> Q0	<input type="radio"/> Q0	<input type="radio"/> Q0	<input type="radio"/> Q0	<input type="radio"/> Q0	<input type="radio"/> Q0	<input type="radio"/> Q0
	<input type="radio"/> Q1	<input type="radio"/> Q1	<input checked="" type="radio"/> Q1	<input checked="" type="radio"/> Q1	<input type="radio"/> Q1	<input type="radio"/> Q1	<input type="radio"/> Q1	<input type="radio"/> Q1
	<input type="radio"/> Q2	<input type="radio"/> Q2	<input type="radio"/> Q2	<input type="radio"/> Q2	<input checked="" type="radio"/> Q2	<input checked="" type="radio"/> Q2	<input type="radio"/> Q2	<input type="radio"/> Q2
	<input type="radio"/> Q3	<input checked="" type="radio"/> Q3	<input checked="" type="radio"/> Q3					
<input type="button" value="提交"/>								

6.4 DSCP 映射

DSCP (Differentiated Services CodePoint, 差分服务编码点) 优先级取值范围为 0~63。RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域，其中 DSCP (Differentiated Services CodePoint, 差分服务编码点) 优先级用该域的前 6 个 bit(0~5bit) 表示，取值范围为 0~63，后 2 个 bit (6、7bit) 是保留位，如下图所示：



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

第 7 章 转发

导轨式 6XX 系列工业交换机转发机制有单播地址转发和组播地址转发，下面分别介绍。

7.1 单播 MAC 地址

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

MAC 地址转发表的表项中包含如下信息：

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

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

单播方式：当**MAC 地址转发表**中包含与报文目的**MAC 地址**对应的表项时，交换机直接将报文从该表项中的转发出口发送。

广播方式：当交换机收到目的地址为全 F 的报文，或**MAC 地址转发表**中没有包含对应报文目的**MAC 地址**的表项时，交换机将采取广播方式将报文向除接收端口外的所有端口转发。

单播地址配置针对的是单播方式。

7.1.1 MAC 地址配置

可设置从某端口发送包含单播目的**MAC 地址**的数据包及学习**MAC 地址**的方式。

步骤 1 从 VID 下拉列表中选择 VID。

步骤 2 输入需要转发的单播**MAC 地址**，地址格式为：**xx-xx-xx-xx-xx-xx**。

步骤 3 在端口下拉列表中选择转发端口。



注意：该端口必须包含在该 VLAN 中。

步骤 4 在类型下拉列表中选择静态、动态或黑洞。

静态：将**MAC 地址**绑定到一个端口。

动态：使一个端口临时学习一个**MAC 地址**。

黑洞：使一个端口不学习这个**MAC 地址**。

配置完成的**MAC 地址**项列表将显示在页面下方。可单击<修改>和<删除>按钮进行修改或删除。动态**MAC 地址**同时也将显示在**动态单播 MAC 地址**页中。

转发表			
VLAN ID	单播MAC地址 [xx-xx-xx-xx-xx-xx]	端口	类型
1	<input type="text"/>	Ethernet0/1	静态
<input type="button" value="提交"/>			

MAC地址表					
VLAN ID	单播MAC地址	端口	类型	修改	删除
1	00-11-11-22-11-22	Ethernet0/5	动态	<input type="button" value="修改"/>	<input type="button" value="删除"/>
2	00-33-33-33-33-33	Ethernet0/5	静态	<input type="button" value="修改"/>	<input type="button" value="删除"/>
1	00-45-45-45-45-45	Ethernet0/6	黑洞	<input type="button" value="修改"/>	<input type="button" value="删除"/>

7.1.2 动态单播 MAC 地址

该页显示交换机端口动态学习到的 MAC 地址以及手动添加的动态 MAC 地址。可手动删除。如老化时间超时，会自动更新该列表。该设备固定缺省老化时间为 300 秒，不可修改。

VLAN ID	单播MAC地址	端口	类型	删除
1	00-11-11-22-11-22	Ethernet0/5	动态	<input type="button" value="删除"/>
1	4c-1f-cc-11-da-c5	Ethernet0/2	动态	<input type="button" value="删除"/>
1	50-e5-49-e4-44-f7	Ethernet0/4	动态	<input type="button" value="删除"/>

7.2 组播 MAC 地址

相比单播来说，组播的优点在于：

- 不论接收者有多少，相同的组播数据流在每一条链路上最多仅有一份。
- 使用组播方式传递信息，用户数量的增加不会显著增加网络的负载。

相比广播来说，组播的优点在于：

- 组播数据流仅会发送到要求数据的接收者。
- 不会造成网络资源的浪费，合理的利用带宽。

以太网传输单播 IP 报文的时候，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播报文时，传输目标不再是一个具体的接收者，而是一个成员不确定的组，所以需要组播 MAC 地址作为目的地址。

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，能够节约大量网络带宽、降低网络负载。

组播功能主要有以下的应用：

- 多媒体、流媒体的应用，如：网络电视、网络电台、实时视/音频会议。

- 培训、联合作业场合的通信，如：远程教育。
- 数据仓库、金融应用（股票）等。
- 任何“点到多点”的数据发布应用。

组播的优点：

- 提高效率：降低网络流量，减轻服务器和 CPU 负荷。
- 优化性能：减少冗余流量。分布式应用：使多点应用成为可能。

在组播方式的信息传输过程中，网络中各部分的角色如下：

- 信息的发送者称为“组播源”
- 所有的接收者都是“组播组成员”
- 由所有接收者构成一个“组播组”，组播组不受地域的限制



注意：

- 组播源不一定属于组播组，也就是说其本身不一定是组播数据的接收者；
- 一个组播源可以同时向多个组播组发送数据，而多个组播源也可以同时向一个组播组发送数据。

为了更好地理解，可以将组播方式的信息传输过程类比于电视节目的传送过程，如下表所示：

步骤	电视节目的传送过程	组播方式的信息传输过程
1	电视台 S 通过频道 G 传送电视节目	组播源 S 向组播组 G 发送组播数据
2	用户 U 将电视机的频道调至频道 G	接收者 U 加入组播组 G
3	用户 U 能够收看到由电视台 S 通过频道 G 传送的电视节目了	接收者 U 能够收到由组播源 S 发往组播组 G 的组播数据了
4	用户 U 关闭电视机	接收者 U 离开组播组 G

可设置从某几个端口发送包含多播目的 MAC 地址的数据包。配置后列表将显示在页面下方。如下所示，VLAN 1 中端口 2 可给组播 MAC 地址 01-52-65-11-32-34 发送数据包，VLAN 2 中端口 5 可给组播 MAC 地址 01-ac-2b-4e-32-55 发送数据包。

静态组播转发表									
VLAN ID	1								
组播MAC地址	<input type="text"/> [xx-xx-xx-xx-xx-xx]								
端口	Ethernet0/								
	1	2	3	4	5	6	7	8	
成员	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="button" value="提交"/>									
静态组播MAC地址表									
VLAN ID	组播MAC地址	成员端口						修改	删除
1	01-52-65-11-32-34	Ethernet0/2						<input type="button" value="修改"/>	<input type="button" value="删除"/>
2	01-ac-2b-4e-32-55	Ethernet0/5						<input type="button" value="修改"/>	<input type="button" value="删除"/>

 注意：链路聚合端口不可配置组播 MAC 地址。

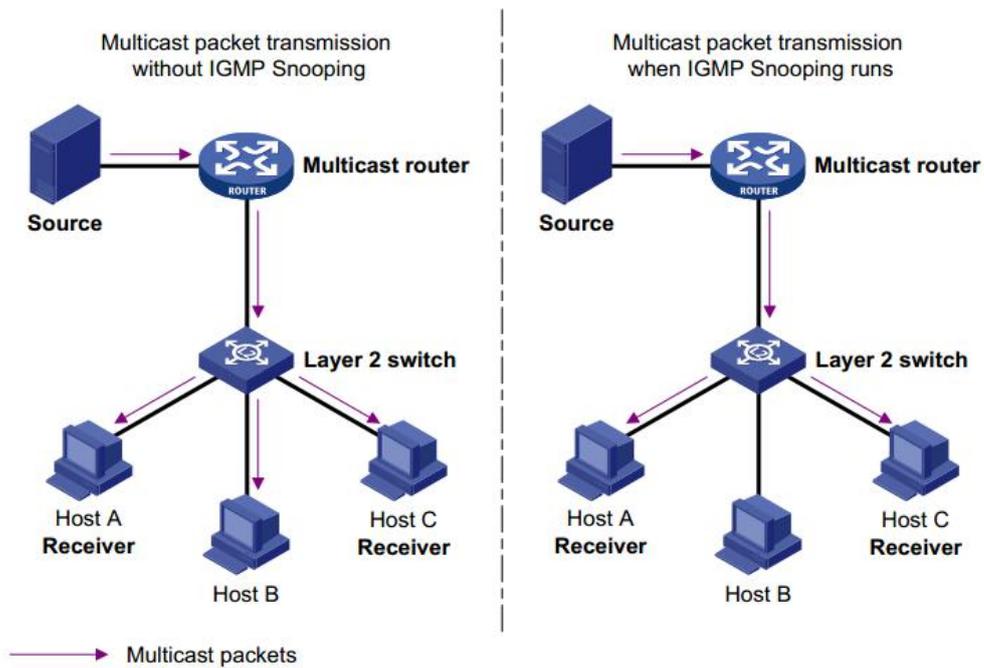
7.3 IGMP 侦听

 说明：应先在[高级配置](#)里开启 IGMP 侦听才可设置转发的 IGMP 侦听。

IGMP 侦听（Internet Group Management Protocol Snooping）是运行在二层设备上的组播约束机制，用于管理和控制组播组。

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

如下图所示，当二层设备没有运行 IGMP 侦听时，组播数据在二层被广播；当二层设备运行了 IGMP 侦听后，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，但是未知组播数据仍然会在二层广播。



7.3.1 IGMP 侦听

随着组播应用的不断深入，IGMPv3 协议应用得越来越多，它增加了组播源过滤功能，使接收者不仅可以指定要加入的组播组，还能明确要求接收从某特定组播源发出的组播信息。

配置步骤：

步骤 1 确定组播组所在的 VLAN ID。VLAN 名称不可在此修改。

步骤 2 选择开启或关闭 IGMP 侦听。如开启，选择 IGMP 版本：版本 2 或版本 3。

IGMP 版本 1： 主机可以加入组播组。没有离开信息（leave messages）。路由器使用基于超时的机制去发现其成员不关注的组。

IGMP 版本 2： 该协议包含了离开信息，允许迅速向路由协议报告组成员终止情况，这对高带宽组播组或易变型组播组成员而言是非常重要的。

IGMP 版本 3： 与以上两种协议相比，该协议的主要改动为：允许主机指定它要接收通信流量的主机对象。来自网络中其它主机的流量是被隔离的。IGMP 版本 3 也支持主机阻止那些来自于非要求的主机发送的网络数据包。

VLAN ID	VLAN名称	状态
1	Default	版本2
提交		

IGMP 侦听状态列表将显示在页面下方。

IGMP侦听状态列表

VLAN ID	VLAN名称	状态
1	Default	版本2
2	VLAN 2	版本3

7.3.2 路由端口

如果某端口所连接的主机需要固定接收某个组播组播数据，可以配置该端口静态加入该组播组，成为静态成员端口。交换机可以通过该端口接收路由器发来的 IGMP 报文。

路由端口：交换机上靠近三层组播设备（即 IGMP 查询器）一侧的端口。交换机将本设备上的所有路由端口都记录在路由器端口列表中。

在各 VLAN 里，静态配置交换机的路由端口，即接收 igmp query 报文的端口。



注意：配置的路由端口必须为该 VLAN 的成员端口。可参考 [4 VLAN 设置](#)。

静态路由端口配置								
VLAN ID	1							
VLAN 名称	Default							
端口	Ethernet0/							
	1	2	3	4	5	6	7	8
路由端口	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
提交								
静态路由端口列表								
VLAN ID	VLAN名称	路由端口						
1	Default	Ethernet0/2,4						
2	VLAN 2	Ethernet0/5						

7.3.3 全局参数

设置 IGMP 侦听全局参数。其参数说明如下：

主机端口老化时间：当一个端口加入某组播组时，交换机为该端口启动一个定时器，其超时时间为主机端口老化时间。超时后，交换机将该端口从组播组的转发表中删除。该值取值范围为 200-1000 秒，缺省值为 260 秒。

路由端口老化时间：交换机为其上的每个路由器端口都启动一个定时器，其超时时间为路由端口老化时间。超时后，交换机将该端口从路由器端口列表中删除。该值取值范围为 1-1000 秒，缺省值为 105 秒。

IGMP 查询器：IGMP 查询器定期向本地网段内的所有主机与路由器发送 IGMP 通用查询报文，以查询该网段有哪些组播组的成员。缺省情况下，IGMP 查询器为关闭。

查询发送间隔：IGMP 查询器发送 IGMP 通用查询报文的时间间隔。超时后，交换机将端口从组播组中删除。该值取值范围为 1-300 秒，缺省值为 125 秒。

最大响应时间：IGMP 通用查询报文的最大响应时间。超时后，交换机将端口从组播组中删除。该值取值范围为 1-25 秒，缺省值为 10 秒。

快速离开：启动快速删除功能后，交换机从某端口收到离开某组播组的 IGMP 离开报文时，直接将端口从组播组中删除。当端口下只有一个用户时，快速删除可以节省带宽。

IGMP 侦听全局参数配置	
主机端口老化时间(200-1000)	260 秒
路由端口老化时间(1-1000)	105 秒
IGMP 查询器	关闭
查询发送间隔(1-255)	125 秒
最大响应时间(1-25)	10 秒
快速离开	开启
<input type="button" value="提交"/>	

第 8 章 安全设置

主要包括 802.1X 配置、MAC 认证和广播风暴配置。

802.1x 简介：IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

8.1 安全配置

 说明：请先在[高级配置](#)里开启 802.1x。

认证服务器是为设备端提供认证服务的实体。认证服务器用于实现用户的认证、授权和计费，通常为 RADIUS 服务器。该服务器可以存储用户的相关信息，例如用户的账号、密码以及用户所属的 VLAN、优先级以及用户的访问控制列表等。

设置 Radius 配置，包括认证 RADIUS 服务器 IP、认证端口号、认证共享密钥、计费 RADIUS 服务器、计费端口和计费共享密钥。

Radius 配置	
认证RADIUS服务器IP	<input type="text" value="192.168.0.234"/>
认证端口号(0-65535)	<input type="text" value="1812"/>
认证共享密钥	<input type="text" value="admin"/>
计费RADIUS服务器IP	<input type="text" value="192.168.0.234"/>
计费端口(0-65535)	<input type="text" value="1813"/>
计费共享密钥	<input type="text" value="admin"/>
<input type="button" value="提交"/>	

8.2 端口授权

IEEE 802.1x 认证系统利用 EAP（Extensible Authentication Protocol，可扩展认证协议）协议，在客户端和认证服务器之间交换认证信息。当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端 PAE 根据 RADIUS 服务器的指示（Accept

或 Reject) 决定受控端口的授权/非授权状态。

 说明：请先在[高级配置](#)里开启 802.1x。

802.1x 的认证过程：

- 当用户有上网需求时打开 802.1x 客户端，输入已经申请、登记过的用户名和口令，发起连接请求（EAPoL-Start 报文）。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。
- 交换机收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。
- 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（EAP-Response/Identity 报文）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（RADIUS Access-Request 报文）送给 RADIUS 服务器进行处理。
- RADIUS 服务器收到交换机转发的用户名信息后，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，同时也将此加密字通过 RADIUS Access-Challenge 报文传送给交换机，由交换机传给客户端程序。
- 客户端程序收到由交换机传来的加密字（EAP-Request/MD5 Challenge 报文）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，生成 EAP-Response/MD5 Challenge 报文），并通过交换机传给 RADIUS 服务器。
- RADIUS 服务器将加密后的口令信息（RADIUS Access-Request 报文）和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，反馈认证成功通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。
- 交换机将端口状态改为授权状态，允许用户通过该端口访问网络。
- 客户端也可以发送 EAPoL-Logoff 报文给交换机，主动终止已认证状态，交换机将端口状态从授权状态改变成未授权状态。

8.2.1 802.1X 端口

配置步骤：

步骤 1 确定需要配置的交换机端口



注意：配置授权的端口不能是链路聚合端口。

步骤 2 确定开启或关闭端口的 802.1X 管理功能

步骤 3 如开启 802.1X 管理，可继续配置端口管理模式为：自动、强制授权或强制不授权。

自动：需要通过身份认证，如通过了就授权访问，没通过则不授权。

强制授权：无需授权即可访问。

强制不授权：无论是否认证都不可访问。

步骤 4 确定开启或关闭端口重新认证

重新认证： 802.1X 重认证是通过定时器或报文触发，对已经认证成功的用户进行一次重新认证。通过启用 802.1X 重认证功能，交换机可以定时检测用户的连接状况。当发现接入用户在一定时间内未响应重认证报文，则切断与该用户的连接。若用户希望再次连接，则必须通过客户端软件重新发起 802.1x 认证。

步骤 5 确定开启或关闭端口 Guest VLAN 功能

Guest VLAN： Guest VLAN 功能用来允许未认证用户访问某些特定资源。在实际应用中，如果用户在没有安装 802.1X 客户端的情况下，需要访问某些资源；或者在用户未认证的情况下升级 802.1X 客户端，这些情况可以通过开启 Guest VLAN 功能来解决。

Guest VLAN 的功能开启后：

- 交换机将在所有开启 802.1X 功能的端口发送触发认证报文（EAP-Request/Identity），如果达到最大发送次数后，仍有端口尚未返回响应报文，则交换机将该端口加入到 Guest VLAN 中；
- 之后属于该 Guest VLAN 中的用户访问该 Guest VLAN 中的资源时，不需要进行 802.1X 认证，但访问外部的资源时仍需要进行认证。

端口	802.1x 管理	端口控制	重新认证	Guest VLAN
Ethernet0/5	开启	强制不授权	开启	开启
<input type="button" value="提交"/>				

802.1x 端口状态列表

端口	802.1x 状态	端口控制	重认证	Guest VLAN	端口状态
Ethernet0/1	关闭	强制授权	开启	关闭	连接断开
Ethernet0/2	关闭	强制授权	开启	关闭	已授权
Ethernet0/3	关闭	强制授权	开启	关闭	连接断开
Ethernet0/4	关闭	强制授权	开启	关闭	已授权
Ethernet0/5	开启	强制不授权	开启	开启	连接断开
Ethernet0/6	开启	强制授权	开启	开启	连接断开
Ethernet0/7	关闭	强制授权	开启	关闭	连接断开
Ethernet0/8	关闭	强制授权	开启	关闭	连接断开

8.2.2 802.1X 系数参数

802.1X 认证过程中会启动多个定时器以控制接入用户、交换机以及 RADIUS 服务器之间进行合理、有序的交互。802.1X 的定时器主要有以下几种：

静默定时器： 对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设

置)后,用户可以再重新发起认证,在静默期间,交换机不进行该用户的 802.1X 认证相关处理。取值范围为 1~65535 秒,缺省值为 60 秒。

传送超时定时器: 以下两种情况交换机启动传送超时定时器: 其一是在客户端主动发起认证的情况下,当交换机向客户端发送单播 Request/Identity 请求报文后,交换机启动该定时器,若在该定时器设置的时长内,交换机没有收到客户端的响应,则交换机将重发认证请求报文; 其二是为了对不支持主动发起认证的 802.1X 客户端进行认证,交换机会在启动 802.1X 功能的端口不停地发送组播 Request/Identity 报文,发送的间隔为传送超时定时器。取值范围为 1~65535 秒,缺省值为 30 秒。

握手定时器: 此定时器是在用户认证成功后启动的,交换机以此间隔为周期发送握手请求报文,以定期检测用户的在线情况。如果重试一定次数后仍然没有收到客户端的响应报文,就认为用户已经下线。用户可以使用 dot1x retry 命令配置最大发送次数。取值范围为 1~300 秒,缺省值为 30 秒。

服务端超时定时器: 若在该定时器设置的时长内,RADIUS 服务器未成功响应,交换机将向 RADIUS 服务器重发认证请求报文。取值范围为 1~300 秒,缺省值为 30 秒。

最大验证请求数: 为检测用户的在线情况,认为用户已经下线前交换机发送握手请求的最大次数。取值范围为 1~10 次,缺省值为 2 次。

重认证定时器: 每隔该定时器设置的时长,交换机会定期发起 802.1X 重认证。取值范围为 60~ 7200 秒,缺省值为 60 秒。

Guest VLAN: 缺省情况下, Guest VLAN 处于关闭状态。

8.3 MAC 认证



说明: 请先在[高级配置](#)里开启 MAC 认证。

MAC 地址认证是一种基于端口和 MAC 地址对用户访问网络的权限进行控制的认证方法,它不需要用户安装任何客户端认证软件。交换机在首次检测到用户的 MAC 地址以后,即启动对该用户的认证操作。认证过程中,也不需要用户手动输入用户名或者密码。

8.3.1 端口配置

配置交换机各端口的 MAC 认证功能: 开启或关闭。端口状态列表将显示在页面下方。

端口	MAC认证
Ethernet0/1	关闭
提交	

端口状态列表

端口	MAC认证	端口	MAC认证
Ethernet0/1	关闭	Ethernet0/2	关闭
Ethernet0/3	关闭	Ethernet0/4	关闭
Ethernet0/5	关闭	Ethernet0/6	关闭
Ethernet0/7	开启	Ethernet0/8	开启

 注意：链路聚合端口不可配置 MAC 认证。

8.3.2 MAC 授权系统参数配置

MAC 地址认证过程受以下定时器的控制：

- **离线检测时间：**用来设置交换机检查用户是否已经下线的时间间隔。当检测到用户下线后，交换机立即通知 RADIUS 服务器，停止对该用户的计费。取值范围为 1~65535 秒，缺省为 300 秒。
- **静默时间：**用来设置用户认证失败以后，该用户需要等待的时间间隔。在静默期间，交换机不处理该用户的认证功能，静默之后交换机再重新对用户发起认证。取值范围为 1~3600 秒，缺省为 60 秒。
- **服务器超时时间：**用来设置交换机同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果服务器超时时间超过设置值，则此次认证失败。取值范围为 1~65535 秒，缺省为 100 秒。

8.3.3 授权信息

该页面显示 MAC 地址认证 MAC 地址状态信息，包括 VLAN ID、MAC 地址、认证端口和认证状态。

端口配置		MAC授权系统参数配置	授权信息
VLAN ID	MAC 地址	认证端口	认证状态
1	00-0a-e4-43-8f-2a	Ethernet0/5	静默

8.4 风暴控制

当网络中有大量的广播/组播/未知单播流量通过以太网端口时，会在端口上产生流量风暴，可能导致网络的拥塞。在接口上配置了广播/组播/未知单播风暴抑制功能后，当接口上的广播/组播/未知单播流量超过用户设置的抑制阈值时，系统会丢弃超出流量限制的报文，从而使接口的广播/组播/未知单播流量降低到限定范围内，保证网络业务的正常运行。

用户可以通过配置风暴控制，限制交换机上允许通过的广播/组播/未知单播流量的大小。

如在**风暴类型**下拉菜单中选择“无”，则表示关闭风暴控制功能；

对于未知目的的单播有两种处理模式：丢弃或转发。

对于广播和未知组播，均默认为转发模式。

风暴控制设置	
风暴类型	广播
速率	2000 Kbps
未知目的单播模式	转发
提交	

第 9 章 LLDP

📖说明：请先在[高级配置](#)里开启 LLDP 功能。

目前，网络设备的种类日益繁多且各自的配置错综复杂，为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。

LLDP (Link Layer Discovery Protocol, 链路层发现协议) 就是在这样的背景下产生的, 它提供了一种标准的链路层发现方式, 可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV (Type/Length/Value, 类型/长度/值), 并封装在 LLDPDU (Link Layer Discovery Protocol Data Unit, 链路层发现协议数据单元) 中发布给与自己直连的邻居, 邻居收到这些信息后将其以标准 MIB (Management Information Base, 管理信息库) 的形式保存起来, 以供网络管理系统查询及判断链路的通信状况。

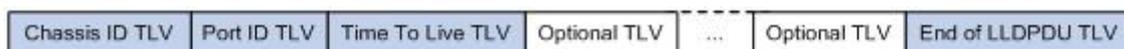
9.1 LLDP 管理

9.1.1 端口 LLDP 配置

配置端口 LLDP 状态 ---- 选择要配置的端口, 开启或关闭 LLDP 开关, 确定 LLDP 状态为关闭、接收和发送、只发送或只接收, 并选择封装类型为 Ethernet II 或 SNAP。

LLDPDU 就是封装在 LLDP 报文数据部分的数据单元。在组成 LLDPDU 之前, 设备先将本地信息封装成 TLV 格式, 再由若干个 TLV 组合成一个 LLDPDU 封装在 LLDP 报文的数据部分进行传送。

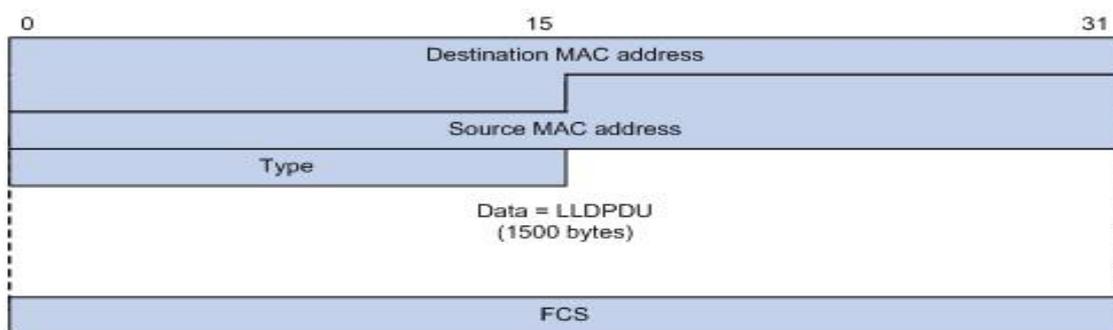
LLDPDU 的封装格式



每个 LLDPDU 共可携带 28 种 TLV, 其中深蓝色的 Chasis ID TLV、Port ID TLV、TTL TLV 和 End of LLDPDU TLV 这四种是必须携带的, 其余的 TLV 则为可选携带。

封装有 LLDPDU 的报文称为 LLDP 报文, 其封装格式有两种: Ethernet II 和 SNAP (Subnetwork Access Protocol, 子网访问协议)。

(1) Ethernet II 格式封装的 LLDP 报文



上图是以 Ethernet II 格式封装的 LLDP 报文, 其中各字段的含义如下:

Destination MAC address：目的 MAC 地址，为固定的组播 MAC 地址 0x0180-C200-000E。

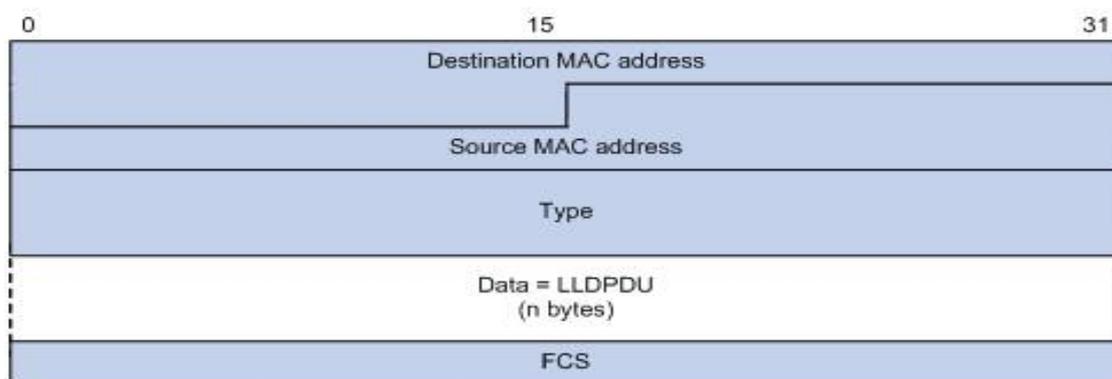
Source MAC address: 源 MAC 地址，为端口 MAC 地址。

Type: 报文类型，为 0x88CC。

Data: 数据内容，为 LLDPDU。

FCS: 帧检验序列，用来对报文进行校验。

(2) SNAP 格式封装的 LLDP 报文



上图是以 SNAP 格式封装的 LLDP 报文，其中各字段的含义如下：

Destination MAC address：目的 MAC 地址，为固定的组播 MAC 地址 0x0180-C200-000E。

Source MAC address: 源 MAC 地址，为端口 MAC 地址。

Type: 报文类型，为 0xAAAA-0300-0000-88CC。

Data: 数据内容，为 LLDPDU。

FCS: 帧检验序列，用来对报文进行校验。

LLDP 有以下四种工作模式

关闭: 既不发送也不接收 LLDP 报文。

接收和发送: 既发送也接收 LLDP 报文。

只发送: 只发送不接收 LLDP 报文。

只接收: 只接收不发送 LLDP 报文。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时，延迟一段时间再执行初始化操作。

LLDP 报文的发送机制

当端口工作在接收和发送/只发送模式时，设备会周期性地向邻居设备发送 LLDP 报文。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，每发送一个 LLDP 报文后都需延迟一段时间后再继续发送下一个报文。

当设备的工作模式由关闭/只接收切换为接收和发送/只发送，或者发现了新的邻居设备（即收到一个新的 LLDP 报文且本地尚未保存发送该报文设备的信息）时，该设备将自动启用快速发送机制，即将 LLDP 报文的发送周期缩短为 1 秒，并连续发送指定数量的 LLDP 报文后再恢复为正常的发送周期。

LLDP 报文的接收机制

当端口工作在接收和发送/只接收模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 LLDP 报文中携带的 TTL（Time To Live，生存时间）值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

端口	LLDP 开关	LLDP 状态	封装类型
Ethernet0/1	开启	关闭	Ethernet II
<input type="button" value="提交"/>			

端口LLDP状态列表

端口	LLDP 开关	LLDP 状态	封装类型	端口	LLDP 开关	LLDP 状态	封装类型
Ethernet0/1	打开	关闭	Ethernet II	Ethernet0/2	打开	关闭	Ethernet II
Ethernet0/3	打开	关闭	Ethernet II	Ethernet0/4	打开	接收和发送	SNAP
Ethernet0/5	打开	关闭	Ethernet II	Ethernet0/6	打开	只接收	Ethernet II
Ethernet0/7	打开	关闭	Ethernet II	Ethernet0/8	打开	关闭	Ethernet II



注意：配置 LLDP 状态的端口不能是聚合端口成员。

9.1.2 TLVs 配置

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。

选择以下内容是否包含在 LLDPDU 中：

- 端口描述** 接口识别信息，包括制造商名称、产品名称、接口硬件和软件版本。
 - 系统名称** 识别设备由网管指定的名称。
 - 系统描述** 设备的文字说明。该项通常包括系统的硬件类型、软件操作系统、和网络软件的全称和版本识别。
 - 系统能力** 识别设备的能力和基本功能（如中继器、网桥、无线局域网、接入点、路由器、电话、DOCSIS 电缆设备和站点等）。
 - 管理地址** 识别设备的 IP 地址或 MAC 地址。
- 这些信息只能在邻端设备查看。

链路层发现协议传输TLVs配置	
端口描述	<input checked="" type="checkbox"/>
系统名称	<input type="checkbox"/>
系统描述	<input checked="" type="checkbox"/>
系统能力	<input checked="" type="checkbox"/>
管理地址	<input checked="" type="checkbox"/>
Apply	

9.1.3 LLDP 参数配置

LLDP 报文所携 Time To Live TLV 中 TTL 的值用来设置邻居信息在本地设备上的老化时间，由于 $TTL = \text{Min}(65535, (TTL \text{ 乘数} \times \text{发送 LLDP 报文的时间间隔}))$ ，即取 65535 与 $(TTL \text{ 乘数} \times \text{发送 LLDP 报文的时间间隔})$ 中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。



注意：

发送 LLDP 报文的时间间隔和延迟时间都应小于 TTL，否则将导致当前设备的信息在邻居设备上老化后仍无法收到当前设备发送的 LLDP 报文。

发送间隔	发送 LLDP 数据包的时间间隔。范围是 5 到 32768 秒，缺省值是 30 秒。
发送持续	TTL 倍数。LLDPDU 中 TLV TTL 用来设置邻居设备的老化时间。由于 $TLV \text{ TTL} = TTL \text{ 倍数} \times \text{发送间隔}$ ，因此邻居设备的老化时间应通过发送持续倍数做调整。该值范围是 2 到 10，缺省值为 4。
发送延时	发送连续 LLDP 数据包的延迟时间。当端口参数改变时，交换机将延迟发送延时发送数据包。范围是 1 到 8192，缺省值为 2。
重初始化	当 LLDP Status 模式改变时，端口将初始化协议状态设备；交换机将需等候重初始化，才能开始下一次初始化。该值范围是 1 到 10 秒，缺省值为 2。
快速计数	快速发送数据包的次数。它的范围是 1 到 10，缺省值为 3。

LLDP 参数配置	
发送间隔 (5-32768)	<input type="text" value="30"/> 秒
发送持续 (2-10)	<input type="text" value="4"/>
发送延时 (1-8192)	<input type="text" value="2"/> 秒
重初始化 (1-10)	<input type="text" value="2"/> 秒
快速计数 (1-10)	<input type="text" value="3"/>
发送延时值不能大于 0.25倍 发送间隔值	
<input type="button" value="Apply"/>	

9.2 邻端信息

该页面显示 LLDP 邻端交换机的信息：接受对端信息的本地端口、设备 ID、远端端口 ID、系统名称、端口描述、系统能力和管理地址。

LLDP 邻端						
本地端口	设备 Id	远端端口 Id	系统名称	端口描述	系统能力	管理地址
Ethernet0/2	00-1e-6e-00-12-34(MAC-address)	2(local)	IDS-508	Ethernet0/2	Bridge (+)	192.168.110.18 (IPv4)

9.3 LLDP 统计信息

该页显示每个以太网端口上的发送帧数、接收帧数、接收错误帧数、丢弃帧数、TLVs 丢弃数、TLVs 为识别数、Org.TLVs 丢弃数和超时数据包数的统计信息。

端口	发送帧数	接收帧数	接收错误帧数	丢弃帧数	TLVs 丢弃	TLVs 未识别	Org.TLVs 丢弃	超时
Ethernet0/1	0	0	0	0	0	0	0	0
Ethernet0/2	0	0	0	0	0	0	0	0
Ethernet0/3	0	0	0	0	0	0	0	0
Ethernet0/4	12	0	0	0	0	0	0	0
Ethernet0/5	0	0	0	0	0	0	0	0
Ethernet0/6	0	0	0	0	0	0	0	0
Ethernet0/7	0	0	0	0	0	0	0	0
Ethernet0/8	0	0	0	0	0	0	0	0

第 10 章 统计信息

该页显示交换各统计信息，包括端口状态、端口统计、VLAN 列表、MAC 地址表、IGMP 侦听表、链路汇聚、inmax Ring 环状态信息。

10.1 端口状态

此页面显示交换机每个以太网端口的端口状态、链路状态、协商、速率与双工、流控、MAC 地址学习和 MDI/MDIX 状态。

端口	端口状态	链路状态	协商	速率和双工	流控	MAC 地址学习	MDI/MDIX
Ethernet0/1	开启	断开	自协商	-	-	开启	MDIX
Ethernet0/2	开启	连接	自协商	100M 全双工	关闭	开启	MDI
Ethernet0/3	开启	断开	自协商	-	-	开启	MDI
Ethernet0/4	开启	连接	自协商	100M 全双工	关闭	开启	MDIX
Ethernet0/5	开启	断开	自协商	-	-	开启	MDIX
Ethernet0/6	开启	断开	自协商	-	-	开启	MDIX
Ethernet0/7	开启	断开	强制	-	-	开启	-
Ethernet0/8	开启	断开	强制	-	-	开启	-

10.2 端口统计

此页面显示每个以太网端口的发送好报文数、发送坏报文数、接受好报文数、接受坏报文数、发送 FCS 错误报文数、碰撞报文数和丢弃报文数。

发送好报文数 端口上发送的正常报文总数，包括正在发送的正常数据帧和正常终止报文。

发送坏报文数 发送的错误报文总数。

接受好报文数 端口上接收的正常报文总数，包括正在接收的正常报文和正常终止报文。

接受坏报文数 接收的错误报文总数。

发送 FCS 错误报文数 端口上发送的错误 FCS（Frame Check (Checking) Sequence）报文数。

碰撞报文数 被检测到碰撞的数据报文数。

丢弃报文数 由于种种原因造成的丢弃报文数。

端口	发送好报文数	发送坏报文数	接受好报文数	接受坏报文数	发送FCS错误报文数	碰撞报文数	丢弃报文数
Ethernet0/1	0	0	0	0	0	0	0
Ethernet0/2	38972	0	57996	0	0	0	0
Ethernet0/3	0	0	0	0	0	0	0
Ethernet0/4	63024	0	42386	0	0	0	0
Ethernet0/5	0	0	0	0	0	0	0
Ethernet0/6	0	0	0	0	0	0	0
Ethernet0/7	0	0	0	0	0	0	0
Ethernet0/8	0	0	0	0	0	0	0

[复位](#)

10.3 VLAN 列表

此页面显示所有 VLAN 列表，包括 VLAN ID、名称、类型、Tagged 端口、Untagged 端口和禁止端口。Type 为 Static 或 Dynamic。Tagged 端口包括所有发送标签数据包的端口。Untagged 端口包括所有发送不带标签数据包的端口。禁止端口包括所有不能添加到 VLAN 组的端口。

VLAN ID	名称	类型	Tagged端口	Untagged端口	禁止端口
1	Default	静态	Ethernet0/2,4	Ethernet0/6,T7	Ethernet0/5
2	vlan 2	静态	Ethernet0/5	T7	-

10.4 MAC 地址表

10.4.1 单播 MAC 地址列表

此网页显示 MAC 地址表中单播 MAC 地址表项信息，包括 VLAN ID、单播 MAC 地址、端口和类型。类型分为动态、静态和黑洞。

VLAN ID	单播MAC 地址	端口	类型
1	00-1e-6e-00-58-33	Ethernet0/2	动态
1	00-1e-6e-00-98-65	CPU	静态
1	4c-1f-cc-11-da-c5	Ethernet0/2	动态
1	50-e5-49-e4-44-f7	Ethernet0/4	动态
1	6c-f0-49-cc-53-7e	Ethernet0/2	动态
2	00-1e-6e-00-98-65	CPU	静态

10.4.2 多播 MAC 地址列表

此网页显示 MAC 地址表中静态多播 MAC 地址表项信息，包括 VLAN ID、多播 MAC 地址、成员端口和类型。

VLAN ID	多播MAC 地址	成员端口	类型
1	01-00-50-00-00-00	Ethernet0/3-4	静态

10.5 IGMP 侦听器

此网页显示 IGMP 侦听器播组信息，包括 VLAN ID、组播组、MAC 地址和成员端口。

VLAN ID	组播组	MAC地址	成员端口
1	239.255.255.250	01-00-5e-7f-ff-fa	Ethernet0/2,4
1	229.38.76.218	01-00-5e-26-4c-da	Ethernet0/2

10.6 链路汇聚

10.6.1 手工聚合组

显示手动聚合组信息，包括集合组 ID、聚合组名称、类型和端口列表；类型固定为手动。

聚合组ID	聚合组名字	类型	端口列表
T2	Trunk2	手工	Ethernet0/1,3

10.6.2 静态聚合组

显示静态聚合组信息，包括集合组 ID、聚合组名称、类型和端口列表；类型固定为静态。

聚合组ID	聚合组名字	类型	端口列表
T7	Trunk7	静态	Ethernet0/7-8

10.6.3 LACP 聚合组

显示动态 LACP 聚合组信息，包括 Actor 与 Partner 的 Priority 和 MAC。它还显示成员端口的 Key、priority 和 Active 状态。

手工聚合组		静态聚合组		LACP 聚合组		
聚合组ID	8					
Actor				对端		
优先级	1			1		
MAC	00-1e-6e-00-12-89			00-1e-6e-00-12-34		
端口	密钥	优先级	激活状态	端口	密钥	优先级
Ethernet0/4	512	1	Selected	3	512	1

10.7 inmax Ring 环状态

该页面显示 inmax Ring 状态信息，包括链路状态和端口状态等，如下图所示：

环ID	状态	环节点	链路状态	主端口状态	备用端口状态	耦合模式	耦合链路状态	耦合主端口状态	耦合备用端口状态
环1	开启	传输节点	断开	传输	连接断开	双归	断开	传输	连接断开
环2	关闭	传输节点	未配置	连接断开	连接断开	双归	未配置	-	-

第 11 章 生成树

 说明：生成树默认全局模式为 RSTP 模式。

1. STP 的用途

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 协会制定的 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互报文发现网络中的环路，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，避免主机由于重复接收相同的报文造成的报文处理能力下降的问题发生。

STP 包含了两个含义，狭义的 STP 是指 IEEE 802.1D 中定义的 STP 协议，广义的 STP 是指包括 IEEE 802.1D 定义的 STP 协议以及各种在它的基础上经过改进的生成树协议。

2. STP 的协议报文

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

3. STP 的基本概念

(1) 根桥

树形的网络结构，必须要有树根，于是 STP 引入了根桥（Root Bridge）的概念。根桥在全网中只有一个，而且根桥会根据网络拓扑的变化而改变，因此根桥并不是固定的。网络收敛后，根桥会按照一定的时间间隔产生并向外发送配置 BPDU，其他的设备对该配置 BPDU 进行转发，从而保证拓扑的稳定。

(2) 根端口

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

(3) 指定桥与指定端口

指定桥与指定端口的含义，请参见下表的说明。

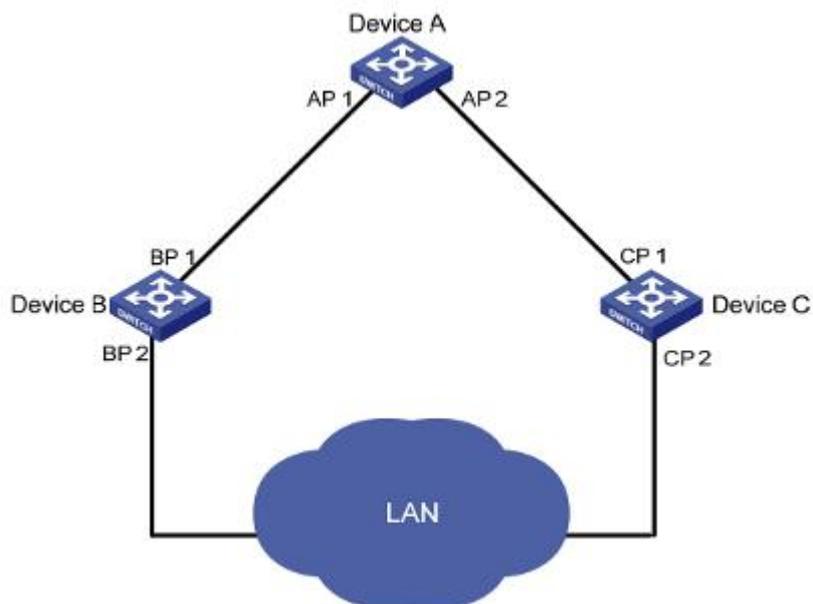
分类	指定桥	指定端口
对于一台设备而言	与交换机直接相连并且负责向交换机转发 BPDU 报文的设备	指定桥向本机转发 BPDU 报文的端口
对于一个局域网而言	负责向本网段转发 BPDU 报文的设备	指定桥向本网段转发 BPDU 报文的端口

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

- Device A 通过端口 AP1 向 Device B 转发配置消息，则 Device B 的指定桥就是

Device A，指定端口就是 Device A 的端口 AP1；

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



(4) 桥 ID

桥 ID 由 8 个字节组成，其中前 2 个字节为设备的桥优先级，后 6 个字节为设备的 MAC 地址。

(5) 路径开销

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

11.1 生成树 (STP)

 说明：STP 默认设置为快速生成树 (RSTP)。

11.1.1 STP 设置

设置交换机的 STP 配置，需要考虑以下几个因素：

优先级：设置交换机生成树的优先级。此值的范围为 0 到 65535，缺省值为 32768。设置值越小，其优先级越高。

联络时间：指 BPDU 的发送间隔，用于交换机检测链路是否存在故障。此值的范围为 1 到 10 秒，缺省值为 2 秒。

根桥定时向外发送配置 BPDU 报文，以维持现有生成树的稳定。如果在指定时间内交换机没有收到 BPDU 数据包，由于 BPDU 数据包超时，则生成树将被重新计算。当交换机

成为根桥时，它将定时在联络时间所配置的时间间隔内发送 BPDU，而其他非根桥交换机采用联络时间所指定的时间间隔。

交换机每隔联络时间会向周围的交换机发送联络报文，以确认链路是否存在故障。

最长老化时间:即 BPDU 的保留时间，是用来判断配置消息在交换机内保存时间是否“过时”的参数，交换机会将过时的配置消息丢弃。取值范围为 6 到 40 秒，缺省值为 20 秒。

STP 能够检测链路故障并使冗余链路自动恢复到转发状态。在 CIST 协议内，交换机使用最长老化时间参数以判断收到的配置 BPDU 是否超时。如果端口收到的配置 BPDU 超时，则生成树将被重新计算。

传输延迟:为交换机状态迁移的延迟时间。

链路故障会引发网络重新进行生成树的计算，生成树的结构将发生相应的变化。不过重新计算得到的新配置消息无法立刻传遍整个网络，如果新选出的根端口和指定端口立刻就开始数据转发的话，可能会造成暂时性的路径回环。

为此，生成树协议采用了一种状态迁移的机制，根端口和指定端口重新开始数据转发之前要经历一个中间状态，中间状态经过 2 倍的 Forward Delay 的延时后才能进入 Forwarding 状态，这个延时保证了新的配置消息已经传遍整个网络。

快速发包检测: 启用/禁用快速发包检测功能，默认为禁用。

为防止出现临时环路，当端口从丢弃变为转发状态时，它将经历一个中间状态，并等候一个特定时间，以便与远程交换机的状态转换同步。这种状态转换时间是由根桥上所配置的转发延迟决定。根桥上配置的转发延迟适用于所有非根桥场合。

至于三个与时间相关的参数的配置（即联络时间，传输延迟和最长老化时间），为防止频繁的网络抖动，必须满足下面公式的要求。

$$2 \times (\text{传输延迟} - 1 \text{ 秒}) \geq \text{最长老化时间}$$

$$\text{最长老化时间} \geq 2 \times (\text{联络时间} + 1 \text{ 秒})$$

桥配置	
优先级(0-65535)	<input type="text" value="32768"/>
联络时间(1-10)	<input type="text" value="2"/> 秒
最长老化时间(6-40)	<input type="text" value="20"/> 秒
传输延迟(4-30)	<input type="text" value="15"/> 秒
快速发包检测	<input type="button" value="关闭"/>
<input type="button" value="提交"/>	

11.1.2 STP 桥信息

该页显示交换机的桥信息。

当交换机启动时，会假定自己就是根网桥，并在发出的所有 BPDU 中将根网桥 ID 设置为本地网桥 ID。若收到具有较低根网桥 ID 的 BPDU，该交换机就会将该 BPDU 中根网桥 ID 所标示的交换机当做根网桥。然后，这台交换机便开始在其发送的 BPDU 中使用那个根网桥。

此页面显示指定桥的基本信息，包括桥 ID、根桥 ID、根端口和根路径开销。

桥 ID：此交换机 ID。每台网桥都有一个网桥 ID。网桥 ID 由网桥优先级和网桥的 MAC 地址组成。网桥优先级是一个可配置的两字节字段，缺省值为 **32768**。网桥的 ID 值越低，越有可能成为根网桥。

根桥 ID：根网桥 ID。根网桥 ID 同样由两个字段组成：根网桥优先级和根网桥 MAC 地址。缺省情况下，根网桥优先级被配置为 **32786**。若根网桥优先级相同，则使用较低的根网桥 MAC 地址来打破僵局。

根端口：根端口就是在交换机上距离根网桥最近的端口。在根网桥上没有根端口只有指定端口。

根路径开销：交换机到根桥的路径开销。因为网桥和网桥之间是以“接力”的形式来转发 BPDUs 的，因此，通过将初始的路径开销加上每台网桥的端口优先级，来确定根网桥路径开销。

指定桥	
桥 ID	32768:00-1e-6e-00-ff-88
根桥 ID	32768:00-1e-6e-00-ff-88
根端口	0
根路径开销	0

11.1.3 STP 端口属性

该页可配置交换机各端口的 STP 属性。

STP 状态：开启或关闭指定端口的 STP 功能。

快速转换端口：是一种 STP 特性，该特性能让交换机绕过所有其他的生成树状态，直接跳转至转发状态。快速转换端口只能在不连交换机的端口上启用。生成树将一个正常的端口置为转发状态时，要耗时 **30** 秒，这会导致某些使用 DHCP 的系统超时，从而无法获取 IP 地址。在端口上启用速端口特性就能规避这个问题。

根保护：在缺省配置时，该功能被禁用。

由于配置错误或遭恶意攻击，网络根桥可收到比根桥优先级更高的配置 BPDUs 数据包，这将导致新的根桥被选用从而使网络拓扑结构发生抖动。在这种情况下，本应沿着高速链路传输的数据流可能被引到低速链路上。此问题可通过启用根保护功能予以解决。启用根保护功能的端口只能作为指定端口使用。当这种类型的端口接收优先级较高的配置 BPDUs 时，更确切的说，当它成为一个非指定端口时，它将转变成丢弃状态并停止转发数据包（即它好像与链路断开连接）。

路径开销：设置一个指定端口的路径开销。此值范围是 **1** 至 **200000000**，缺省值是 **55**。也可使其自动配置。

优先级：设置一个指定端口的优先级。取值范围为 **0** 到 **255**，缺省值是 **128**。

该标签页的底部列出交换机所有端口的 STP 属性。

端口	STP状态	快速转换端口	根保护	路径开销	优先级
Ethernet0/1	关闭	关闭	关闭	55 自动 <input type="checkbox"/>	128
提交					

端口属性

端口	STP状态	快速转换端口	根保护	端口状态	端口角色	路径开销	优先级	指定桥ID	指定端口ID	指定路径开销
Ethernet0/1	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet0/2	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet0/3	开启	开启	开启	阻塞	关闭	-	128	32768:001e6e00ff88	128:3	0
Ethernet0/4	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet0/5	开启	关闭	开启	阻塞	关闭	55	128	32768:001e6e00ff88	128:5	0
Ethernet0/6	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet1/1	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet1/2	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0
Ethernet1/3	关闭	关闭	关闭	阻塞	关闭	55	128	0:000000000000	0:0	0

11.2 快速生成树（RSTP）

 说明：请先在高级设置里开启快速生成树（RSTP）。STP 参数亦有效。

RSTP 由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

点对点：是两台交换机之间直接连接的链路。如启用，表示连接到当前以太网端口的链路为点对点类型，将使该端口迅速处于转发状态。

协议迁移：为了向后兼容 802.1d 交换机，RSTP 有选择地基于每个端口发送 802.1D 配置 BPDU 或 TCN BPDU 信息。可启用或禁用协议转移。如该端口启用了 RSTP，而对端连接的端口启用的是 STP 时，该端口的发送的 BPDU 报文将自动的由 RSTP 报文转为 STP 报文。

当一个端口初始化时，启动迁移延迟定时器（指定发送 RSTP BPDU 的最短时间），同时发送 RSTP BPDU。当此定时器处于启用状态，交换机将处理端口上收到的所有 BPDU，同时忽略协议类型。

当端口迁移延迟定时器失效后，如果交换机收到 802.1d BPDU，它认为它与 802.1d 交换机相连并且开始只使用 802.1d BPDU。但是，如果 RSTP 交换机正在端口上使用 802.1d BPDU 并在定时器失效后仍然收到 RSTP BPDU，它将重新启动定时器，同时在端口上开始使用 RSTP BPDUs。

边缘端口：选择“是”，配置指定的以太网端口为边缘端口，将加速该端口的转发速度。在缺省情况下，所有以太网端口为非边缘端口。

边缘端口是直接和用户终端相连的端口，而不是连接到另一个交换机或网段。边缘端口可以快速切换到转发状态，因为在边缘端口上，网络拓扑结构的变化不产生环路。通过把一个端口设置成边缘端口可以使其迅速切换到转发状态。建议把直接连接到用户终端的以太网端口配置成边缘端口。

通常情况下，因为端口未连接到另一个交换机，配置 BPDU 不能到达边缘端口，但是当 BPDU 保护功能在边缘端口上被禁用时，恶意用户故意发送的配置 BPDU 可以到达该端口。如果边缘端口收到 BPDU，它将变为一个非边缘端口。



注意：inmax Ring 和 STP 不能同时设置。

端口	点对点	协议迁移	边缘端口
Ethernet0/2	开启	开启	否
提交			

端口属性

端口	生成树模式	端口状态	端口角色	点对点	协议迁移	边缘端口
Ethernet0/2	RSTP	阻塞	关闭	开启	开启	否
Ethernet0/4	RSTP	阻塞	关闭	开启	开启	否
Ethernet0/5	RSTP	阻塞	关闭	开启	开启	否
Ethernet0/6	RSTP	阻塞	关闭	开启	开启	否
T1	RSTP	阻塞	关闭	开启	开启	否
T2	RSTP	阻塞	关闭	开启	开启	否

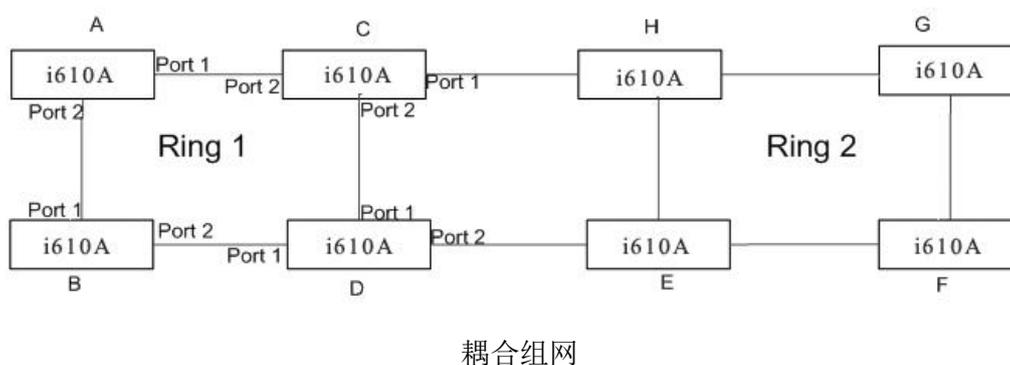
第 12 章 inmax Ring 配置

 说明：请先在[高级配置](#)里开启 inmax Ring，不能同时开启 STP。

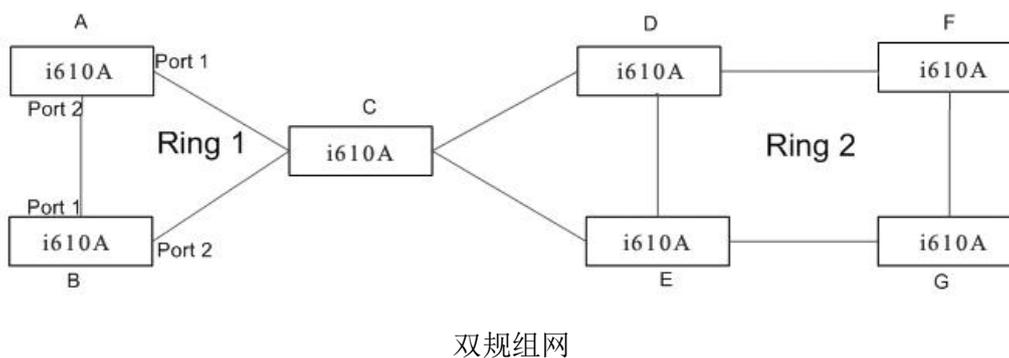
inmax Ring（金恒威环网保护）是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。

目前，解决二层网络环路问题的技术有 STP 和 inmax Ring。STP 应用比较成熟，但收敛时间在秒级。inmax Ring 是专门应用于以太网环的链路层协议，具有比 STP 更快的收敛速度。并且 inmax Ring 的收敛时间与环网上节点数无关，可应用于网络直径较大的网络。

inmax Ring 组网示意图如下：



耦合组网



双规组网

具有相同 ring ID 和相同控制 VLAN，并且相互连通的设备构成一个 inmax Ring 域。一个 inmax Ring 域具有 inmax Ring 主环、控制 VLAN、主节点、传输节点、主端口和副端口、公共端口和边缘端口等要素。

如上图所示，有两个 ring 域，ring 1 和 ring 2，他们同时又可以通过耦合和双归组网。组网时，ring 1 和 ring 2 要交替配置，这样可以组成更多的环网。

在 inmax Ring 协议中，最多允许有 2 级环网，每级都有环 ID。交换机可以是环网的一个节点。

12.1 inmax Ring 环

此页面对 inmax Ring 环配置进行设置：环 ID、环状态、控制 VLAN、保护 VLAN、快速检测状态、节点模式、主端口和备用端口。

环 ID：确定此交换机是属于哪个环的成员。在 inmax Ring 协议上，有 2 级环网。

环状态：启用/禁用指定交换机环。

 **说明：**一个交换机只能在一个环网上被启用。

控制 VLAN：在 inmax Ring 环上用于传输 inmax Ring 协议包的 VLAN。

保护 VLAN：用于传输数据包，当环网上一个 VLAN 被创建时，该 VLAN 如果不是控制 VLAN，则必须配置为保护 VLAN。

快速检测状态：在启用状态时，inmax Ring 将使用**快速握手超时定时器**和**快速环断开超时定时器**而非**握手超时定时器**和**环断开超时定时器**来定期发送数据包，以检测环网连接状态。

节点模式：inmax Ring 环网上每个交换机就是一个节点。有两种类型的节点：主节点和传输节点。主节点从它的主端口定期发送 HELLO（健康检测）数据包；传输节点依次在环网上传输此数据包。若主节点的备用端口收到由自身发送的 HELLO 数据包，这表明已完成组网。否则，HELLO 数据包无法到达其自身，且主节点会认为环网上出现了链路故障。

传输节点负责监测它们所直接连接的 inmax Ring 链路状态，并把链路变化情况通知主节点。



注意：一个环网应该有且只能有一个主节点。

主节点和传输节点分别有两个端口接入 inmax Ring 环，其中一个为主端口，另一个为备用端口。端口的角色由用户的配置决定。

主端口：主节点通过主端口发送 inmax Ring 数据包。

备用端口：主节点使用备用端口接收 inmax Ring 数据包。堵塞备用端口以阻止洪泛，在链路发生故障时解除阻塞。

主节点的主端口和备用端口在功能上有所区别：

- 主节点的主端口用来发送环路探测报文，备用端口用来接收环路探测报文。
- 当 inmax Ring 环处于健康状态时，主节点的备用端口在逻辑上阻塞数据 VLAN，只允许控制 VLAN 的报文通过。
- 当 inmax Ring 环处于断裂状态时，主节点的备用端口将解除数据 VLAN 的阻塞状态，转发数据 VLAN 的报文。

传输节点的主/备用端口具有相同功能，都用于 inmax Ring 环上协议报文和数据报文的传输。

如 11 章图所示，Device A 为 Ring1 的主节点，Port 1 和 Port 2 为其在 Ring1 上的主端口与备用端口。Device B、Device C 和 Device D 为 Ring 1 的传输节点，它们的 Port 1 和 Port 2 分别为各自节点在 Ring 1 上的主端口和备用端口。

此页面底部列出每个环网（共 2 个环网）配置。



注意：开启了生成树的端口不能再开启 inmax Ring 主端口或备用端口。

环ID	环1
环状态	关闭
控制VLAN	4091
保护VLAN	1 (e.g:2-3,5)
快速检测状态	关闭
节点模式	主节点
主端口	Ethernet0/1
备用端口	Ethernet0/6
提交	

环列表

环ID	环状态	控制VLAN	保护VLAN	快速检测	节点模式	主端口	备用端口
环1	关闭	4091	1	关闭	主节点	Ethernet0/1	Ethernet0/6
环2	关闭	4092	1	关闭	主节点	Ethernet0/2	Ethernet0/4

12.2 inmax Ring 耦合

此页面对 inmax Ring 耦合配置进行设置：环、耦合状态、耦合模式、耦合主端口和耦合备用端口。

环：与耦合功能有关的环 ID。

耦合状态：启用或禁用所选环的耦合功能。要启用此功能，必须启用相关环网。



耦合模式：有 4 种耦合模式：双归、主耦合、备用耦合和辅助耦合。耦合主端口和耦合备用端口在不同模式下所扮演的端口角色是不一样的。在双规模式下，有主耦合端口和耦合备用端口。在主耦合和辅助耦合模式下，只有 1 个主端口。在备用模式下只有 1 个耦合备用端口。

耦合主端口：指定连接到其它环网上的端口，用于环网之间的连接。此端口通常设置为转发状态。

耦合备用端口：指定连接到其它环网上的端口，用于备份。当耦合主端口断开，此端口阻塞解除。

耦合模式配置规则：

1. 两个直接连接的环不可有相同的环 ID。
2. 在一个环网内，只有一个交换机可设置为主耦合，而另一个交换机则设置成备用耦合。
3. 在同一级环内可以将多个交换机设置成双归模式。

此页面的下面部分列出两个耦合环网的配置。



注意：

- 耦合主端口不能和环的主端口或备用端口一样。
- 开启了生成树的端口不能配置成耦合主端口。

Fi Ring耦合设置				
环	环 1			
耦合状态	关闭			
耦合模式	双归			
耦合主端口	Ethernet0/3			
耦合备用端口	Ethernet0/8			
提交				
耦合环列表				
环ID	耦合状态	耦合模式	耦合主端口	耦合备用端口
环1	关闭	双归	Ethernet0/3	Ethernet0/8
环2	关闭	双归	-	-

12.3 inmax Ring 定时器

此页面对 inmax Ring 定时器配置进行设置：握手超时定时器、环断开超时定时器、快速握手超时定时器和快速环断开超时定时器。

握手超时定时器：主节点从主端口发送握手报文的周期。取值范围为 1 到 10 秒，缺省值为 1 秒。

环断开超时定时器：主节点从主端口发送握手报文到副端口收到该报文的最大时延。在环断开定时器超时前，如果主节点在副端口上接收到自己从主端口发出的握手报文，主节点认为环网处于健康状态；否则，主节点认为环网处于断裂状态。取值范围为 3 至 30 秒，缺省值为 3 秒。

快速握手超时定时器：和握手超时定时器定义相同，如果开启快速检测机制，则握手超时定时器的值为此设置的值。取值范围为 10 至 500 毫秒，缺省值为 10 毫秒。

快速环断开超时定时器：和环断开超时定时器定义相同，如果开启快速检测机制，则环断开超时定时器的值为此设置的值。取值范围为 30 至 1500 毫秒，缺省值为 30 毫秒。

这些定时器用于主节点。当握手超时定时器超时，主节点将发出握手数据包。若环断开超时定时器超时，这表明环网上出现链路故障。

当设置这些参数时，应遵循下列规则：

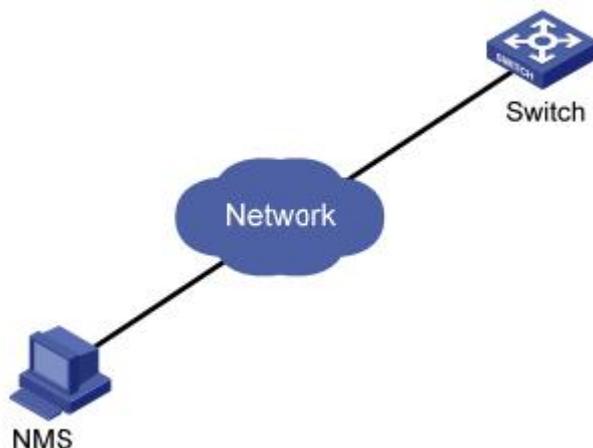
3*握手超时定时器 ≤ 环断开超时定时器 和

3*快速握手超时定时器 ≤ 快速环断开超时定时器。

Fi Ring定时器设置	
握手超时定时器(1-10)	<input type="text" value="1"/> 秒
环断开超时定时器(3-30)	<input type="text" value="3"/> 秒
快速握手超时定时器(10-500)	<input type="text" value="10"/> 毫秒
快速环断开超时定时器(30-1500)	<input type="text" value="30"/> 毫秒
<input type="button" value="提交"/>	

第 13 章 SNMP 管理

用户可通过 NMS（Network Management Station，网管工作站）登录到交换机上，通过交换机上的 Agent 模块对交换机进行管理、配置，如下图所示。NMS 和 Agent 之间运行的协议为 SNMP（Simple Network Management Protocol，简单网络管理协议）。SNMP 是使用 TCP/IP 协议族对互联网上的设备进行管理的一个框架，它提供一组基本的操作来监视和维护互联网。



SNMP 具有以下优势：

- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务分别与设备物理特性和下层的联网技术相对独立，从而实现对不同厂商设备的管理，特别适合在小型、快速和低成本的环境中使用。

SNMP 网络元素分为 NMS 和 Agent 两种。

- NMS（Network Management Station，网络管理站）是运行 SNMP 客户端程序的工作站，能够提供非常友好的人机交互界面，方便网络管理员完成绝大多数的网络管理工作。
- Agent 是驻留在设备上的一个进程，负责接收、处理来自 NMS 的请求报文。在一些紧急情况下，如接口状态发生改变等，Agent 也会通知 NMS。

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

13.1 SNMP 账户

配置管理 SNMP 的用户名和密码。

13.1.1 SNMP 团体

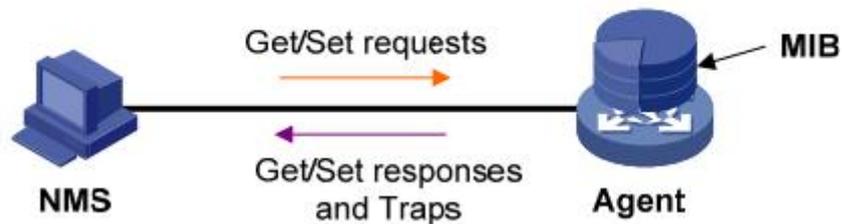
在该标签页中，可设置 SNMP 版本（“v1”和“v2c”）、团体名和访问模式（只读和读写）。

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

- SNMP v1 采用团体名（Community Name）认证。团体名用来定义 SNMP NMS 和 SNMP Agent 的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP NMS 对 SNMP Agent 的访问。
- SNMP v2c 也采用团体名认证。它在兼容 SNMP v1 的同时又扩充了 SNMP v1 的功能：它提供了更多的操作类型（GetBulk 和 InformRequest）；它支持更多的数据类型（Counter64 等）；它提供了更丰富的错误代码，能够更细致地区分错误。

团体名： 登陆要访问的 agent 的用户名。

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



页面下方将显示团体列表，每个团体名可被删除。

SNMP 版本	v2c		
团体名	<input type="text"/>		
访问模式	读写		
提交			
团体列表			
SNMP版本	团体名	访问模式	删除
v1	public	只读	删除
v1	Lemon	只读	删除
v2c	sky	读写	删除

13.1.2 SNMP 用户

SNMP v3 提供了基于用户的安全模型（USM，User-Based Security Model）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP NMS 和 SNMP Agent 之间的通信提供更高的安全性。

NMS 和 Agent 的 SNMP 版本匹配，是它们之间成功互访的前提条件。Agent 可以同时配置多个版本，与不同的 NMS 交互采用不同的版本。

在该标签页中，可创建一个 SNMP v3 用户，设置 USM（基于用户的安全模式）用户名、权限、是否启用 SNMP V3 加密，如启用，还可设置验证算术、证密码、私人算术和私人密码。

- **USM 用户：** USM（User-based Security Model）用户名，3 到 16 个字符的字符串。
- **访问模式：** 指定已创建用户对系统的只读权限或读写权限。
- **SNMP V3 封装：** SNMP V3 安全加密方式。如 SNMP V3 封装不被选择，验证和加密都将无需执行。
- **授权算法：** 确定验证所用的安全模式。
- **MD5：** 使用 HMAC MD5 算术作为验证模式。
- **SHA：** 使用 HMAC SHA 算术作为验证模式，比 MD5 更安全。
- **授权密码：** 验证密码，在纯文本中为 9 到 15 个字符的字符串；在加密文本中，如启用了 MD5 算术，为 32 位十六进制字符；在加密文本中，如启用了 SHA 算术，为 40 位十六进制字符。
- **私有算法：** 确定加密的安全模式。
- **DES：** 确定加密协议为数据加密标准（DES）。
- **AES：** 确定加密协议为高级加密标准（AES），比 DES 更安全。
- **私有密码：** 加密密码，在纯文本中为 9 到 15 个字符的字符串；在加密文本中，如启用了 MD5 算术，为 32 位十六进制字符；在加密文本中，如启用了 SHA 算术，为 40 位十六进制字符。

页面底部列出了所有现有的 SNMP v3 USM 用户，包括 SNMP 版本、USM 用户和访问模式。USM 用户可删除。

USM 用户	访问模式	SNMP V3 封装	授权算法	授权密码	私有算法	私有密码
<input type="text"/>	读写	<input type="checkbox"/>	MD5	<input type="text"/>	无	<input type="text"/>
<input type="button" value="提交"/>						
用户列表						
SNMP 版本	USM用户	访问模式	删除			
v3	Monica	读写	<input type="button" value="删除"/>			

13.2 SNMP 陷阱

Agent 使用 SNMP 陷阱操作向 NMS 发送报警信息。

13.2.1 全局陷阱设置

全局开启或关闭陷阱功能。

全局陷阱配置	
陷阱	<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px;">开启 ▼</div> <div style="margin-left: 5px;"> <div style="border: 1px solid black; padding: 2px;">关闭</div> <div style="border: 1px solid black; padding: 2px;">开启</div> </div> </div>
<input type="button" value="提交"/>	

13.2.2 陷阱主机 IP

设置接收 Agent 发送的陷阱的 NMS IP 地址。页面下方将显示当前陷阱用户。

增加陷阱主机 IP							
主机 IP	<input type="text"/>						
<input type="button" value="提交"/>							
当前陷阱用户							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">序号</th> <th style="width: 70%;">主机 IP</th> <th style="width: 20%;">删除</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">192.168.10.136</td> <td style="text-align: center;"> <input type="button" value="删除"/> </td> </tr> </tbody> </table>		序号	主机 IP	删除	1	192.168.10.136	<input type="button" value="删除"/>
序号	主机 IP	删除					
1	192.168.10.136	<input type="button" value="删除"/>					

13.2.3 陷阱端口

设置交换机发送陷阱的端口。陷阱内容指端口上 linkup 和 linkdown 的情况。指定端口，选择开启或关闭陷阱功能，点击<提交>，页面下方将列出交换机端口陷阱情况。缺省情况下，端口陷阱功能为开启。

端口陷阱设置																					
端口	<div style="border: 1px solid black; padding: 2px;">Ethernet0/1 ▼</div>																				
陷阱	<div style="border: 1px solid black; padding: 2px;">开启 ▼</div>																				
<input type="button" value="提交"/>																					
端口陷阱状态																					
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">端口</th> <th style="width: 25%;">陷阱</th> <th style="width: 25%;">端口</th> <th style="width: 25%;">陷阱</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Ethernet0/1</td> <td style="text-align: center;">开启</td> <td style="text-align: center;">Ethernet0/2</td> <td style="text-align: center;">开启</td> </tr> <tr> <td style="text-align: center;">Ethernet0/3</td> <td style="text-align: center;">开启</td> <td style="text-align: center;">Ethernet0/4</td> <td style="text-align: center;">关闭</td> </tr> <tr> <td style="text-align: center;">Ethernet0/5</td> <td style="text-align: center;">开启</td> <td style="text-align: center;">Ethernet0/6</td> <td style="text-align: center;">关闭</td> </tr> <tr> <td style="text-align: center;">Ethernet0/7</td> <td style="text-align: center;">开启</td> <td style="text-align: center;">Ethernet0/8</td> <td style="text-align: center;">开启</td> </tr> </tbody> </table>		端口	陷阱	端口	陷阱	Ethernet0/1	开启	Ethernet0/2	开启	Ethernet0/3	开启	Ethernet0/4	关闭	Ethernet0/5	开启	Ethernet0/6	关闭	Ethernet0/7	开启	Ethernet0/8	开启
端口	陷阱	端口	陷阱																		
Ethernet0/1	开启	Ethernet0/2	开启																		
Ethernet0/3	开启	Ethernet0/4	关闭																		
Ethernet0/5	开启	Ethernet0/6	关闭																		
Ethernet0/7	开启	Ethernet0/8	开启																		

第 14 章 RMON

RMON (Remote Monitoring, 远程网络监视) 的实现完全基于 SNMP 体系结构, 它与现存的 SNMP 框架相兼容, 不需对该协议进行任何修改。RMON 使 SNMP 更有效、更积极主动地监测远程网络设备, 为监控子网的运行提供了一种高效的手段。RMON 能够减少网管站同代理间的通讯流量, 达到简便而有力地管理大型互连网络的目的。

14.1 统计

利用 RMON 统计管理功能, 可以监视端口的使用情况。统计信息包括收发字节、收发包、广播包、组播包、CRC 校验错误报文数、过小 (或超大) 的数据报文数、碎片、无用信息、网络冲突数、各种字节帧、和丢弃事件等。

在指定接口下创建统计表项成功后, 统计组就对当前接口的报文数进行统计, 它统计的结果是一个连续的累加值。

统计收发字节: 从网络上收到的和向网络发送的字节数据总数, 包括坏数据包。它不包括帧位, 但包括帧校验序列 (FCS) 字节。

统计收发包: 接收到的和发送的数据包总数, 包括坏数据包、广播数据包和组播数据包。

广播包: 接收到的指向广播地址的好数据包总数, 但不包括组播数据包。

组播包: 接收到的指向组播地址的好数据包总数, 但不包括指向广播地址的数据包。

CRC 校验错误: 接收到的长度为 64 到 1518 位 (含两者) 字节 (不含帧位, 但包括 FCS 字节) 同时含有整数位字节的坏 FCS (FCS Error) 或者非整数位字节的坏 FCS (Alignment Error) 的数据包总数。

过小包: 接收到的长度小于 64 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数。

超长包: 接收到的长度大于 1518 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数。

碎片: 接收到的长度小于 64 位字节 (不含帧位, 但包括 FCS 字节), 同时含有整数位字节的坏 FCS (FCS Error) 或者非整数位字节的坏 FCS (Alignment Error) 的数据包总数。

无用信息: 接收到的长度大于 1518 位字节 (不含帧位, 但包括 FCS 字节), 同时含有整字节的坏 FCS (FCS Error) 或者非整字节的坏 FCS (Alignment Error) 的数据包总数。

碰撞: 该以太网段上冲突总数的最佳估值。

64 字节帧: 接收到长度为 64 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数, 包括坏数据包。

65~127 字节帧: 接收到的长度为 65 到 127 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数, 包括坏数据包。

128~255 字节帧: 接收到的长度为 128 到 255 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数, 包括坏数据包。

256~511 字节帧: 接收到的长度为 256 到 511 位字节 (不含帧位, 但包括 FCS 字节) 的数据包总数, 包括坏数据包。

512~1023 字节帧：接收到的长度为 512 到 1023 位字节（不含帧位，但包括 FCS 字节）的数据包总数，包括坏数据包。

1024~1510 字节帧：接收到的长度为 1024 到 1518 位字节（不含帧位，但包括 FCS 字节）的数据包总数，包括坏数据包。

丢弃事件：由于缺乏足够信息而发生丢包的事件总数。

每个以太网端口所有统计信息均可复位。

14.2 历史

14.2.1 历史记录控制

历史组是按周期对端口的使用情况进行统计，并将统计结果存储在历史记录表中以便以后查看。统计数据包括带宽利用率、错误包数和总包数等。

在指定接口下创建历史表项成功后，统计组就对当前接口的报文数按周期进行统计，它统计的结果是一个周期内端口收发报文的情况。

此页面设置历史记录控制表项。

端口：收集统计的以太网端口。

所有者：配置此表项的实体以使用分配给它的资源。

采样间隔：每组数据采样的时间间隔（秒）。此间隔设置范围在 1 至 3600 秒（1 小时）之间。

保留的采样数目：离散采样保存的总数。在该配置的时间间隔内，数据应保存在与历史记录表项有关的部分特定介质表中。

配置完成后点击<创建>，页面下方将出现 RMON 历史控制表，各控制索引可被删除。

RMON 历史					
端口	Ethernet0/1 ▾				
所有者	<input type="text"/>				
采样间隔(s)	<input type="text"/>				
保留的采样数目(s)	<input type="text"/>				
<input type="button" value="创建"/>					
RMON 历史控制列表					
历史控制索引	端口	所有者	采样间隔(s)	保留的采样数目(s)	删除
1	Ethernet0/1	ddd	30	10	<input type="button" value="删除"/>
2	Ethernet0/2	hjh	5	4	<input type="button" value="删除"/>

14.2.2 历史记录列表

在此页面上，选择历史检索，以显示相关统计情况。

此网页的底部列出有关参数统计信息。以历史索引 3 为例说明，从历史记录控制中可得知，其每隔 3 秒采样一次，每次最多显示 10 条采样，只显示最新的采样。

RMON 历史												
历史索引	3											
所有者	333											
RMON历史纪录列表												
索引	丢弃事件	接受字节	接受包	广播包	组播包	CRC校验错误	过小包	超长包	碎片	无用信息	碰撞	使用率
189	0	0	0	0	0	0	0	0	0	0	0	0
190	0	0	0	0	0	0	0	0	0	0	0	0
191	0	1022	12	0	0	0	0	0	0	0	0	0
192	0	0	0	0	0	0	0	0	0	0	0	0
193	0	0	0	0	0	0	0	0	0	0	0	0
194	0	125	1	0	0	0	0	0	0	0	0	0
195	0	0	0	0	0	0	0	0	0	0	0	0
196	0	93	1	0	0	0	0	0	0	0	0	0
197	0	0	0	0	0	0	0	0	0	0	0	0
198	0	551	3	0	0	0	0	0	0	0	0	0

14.3 告警

RMON 告警管理可对指定的告警变量（如端口的统计数据）进行监视。被监视的告警变量的采样值大于或等于上限阈值时，触发一次上限告警事件；被监视的告警变量的采样值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

用户定义了告警表项后，系统对告警表项的处理如下：

- (1) 对所定义的告警变量按照定义的时间间隔进行采样。
- (2) 将采样值和设定的阈值进行比较，越过阈值就触发相应事件。

配置步骤：

步骤 1 选择收集统计情况的以太网端口。

步骤 2 选择计数器名。

步骤 3 选择采样类型：绝对值和增量。对于采样已选定变量和计算它与阈值大小的方法是：如果采样类型是绝对值，则在采样间隔的末端，已选定变量值将直接与阈值比较；如果采样类型是增量，则将当前值减去最后一个采样的已选定变量值，并将该差值与阈值比较。

步骤 4 填写上升阈值，取值范围为 1~2147483640；选择上升事件，事件在 [14.4](#) 事件中设置好。

上升阈值：采样统计的上升阈值。若当前采样值大于或等于该阈值，并且上一次采样值低于此阈值时，则会引发单一事件。在该表项生效后如果第一个采样值大于或等于此阈值，同时相关启动告警等于上升告警或上升和下降告警，也可以引发单一事件。当一个上升事件发生后，其他类似事件将不会产生，直到采样值达到或低于此阈值为止。

上升事件：当上升阈值被超越时所使用的表项索引。由该索引特定值所确定的表项与事件表项对象所确定的索引值相同。

步骤 5 填写下降阈值，取值范围为 1~2147483640；选择下降事件，事件在 [14.4](#) 事件中设置好。

下降阈值：采样统计的下降阈值。若当前采样值小于或等于此阈值，并且上一次采样值大于此阈值时，则会引发单一事件。在该表项生效后如果第一个采样值小于或等于此阈值，同时相关启动告警等于下降告警或上升和下降告警，也可以引发单一事件。当一个下降事件发生后，其他类似事件将不会产生，直到采样值高于此阈值并达到上升阈值为止。

下降事件：当下降阈值被超越时所使用的表项索引。由该索引特定值所确定的表项与事件表项对象所确定的索引值相同。

步骤 6 选择启动告警类型：上升告警、下降告警、上升和下降告警。

启动告警：当该表项第一次设置有效时发送的报警。在该表项生效后如果第一个采样值大于或等于上升告警，同时启动告警等于上升告警或上升和下降告警，则会引发单一上升报警。而在该表项生效后若第一个采样值小于或等于下降阈值，同时启动告警等于下降告警或上升和下降告警，则会引发单一下降报警。

步骤 7 设置数据采样并与上升和下降阈值比较的时间间隔（秒）。

步骤 8 配置此表项的实体，以使用分配给它的资源。

步骤 9 点击<创建>，页面下方将出现 RMON 告警列表。

RMON 告警	
端口	Ethernet0/1
计数器名	In Octets
采样类型	绝对值
上升阈值	
上升事件	1
下降阈值	
下降事件	1
启动告警	上升告警
采样间隔(s)	
所有者	
<input type="button" value="创建"/>	

RMON 告警列表

索引	端口	计数器名	采样类型	上升阈值	上升事件	下降阈值	下降事件	启动告警	采样间隔	所有者	删除
1	Ethernet0/2	InOctets	绝对值	5	1	1	1	上升告警	3	gfd	删除
2	Ethernet0/4	InOctets	绝对值	5	2	1	2	上升和下降告警	5	ghh	删除
3	Ethernet0/2	InOctets	绝对值	6	1	1	1	上升和下降告警	2	dsf	删除
4	Ethernet0/2	InOctets	绝对值	6	1	1	1	上升和下降告警	2	guj	删除

14.4 事件

事件组用来定义事件索引号及事件的处理方式。事件组定义的事件主要用在告警组配置项和扩展告警组配置项中。当监控对象达到告警条件时，必然会触发事件，事件有如下几种处理方式：

- 不做任何处理
- 将事件相关信息记录在事件日志表中
- 向网管站发送 Trap 消息
- 将事件相关信息记录在事件日志表中并向网管站发送 Trap 消息

14.4.1 事件

配置步骤如下：

步骤 1 指定团体，陷阱被发送到的团体。

步骤 2 添加说明文字。

步骤 3 选择事件类型：无、日志、陷阱、日志和陷阱。如选择无，关闭告警功能；如选择日志，其结果将显示在事件日志中。如选择陷阱，交换机将发送陷阱信息给指定陷阱主机，可参考 [13.2.2](#)；如选择日志和陷阱，则同时在事件日志中显示并发送陷阱信息给指定陷阱主机。

步骤 4 指定所有者，在 log 事件中便于管理。

步骤 5 点击<创建>，页面下方将显示配置的 RMON 事件实体。

RMON 事件					
团体	<input type="text"/>				
说明	<input type="text"/>				
类型	无 <input type="button" value="v"/>				
所有者	<input type="text"/>				
<input type="button" value="创建"/>					
RMON 事件实体					
索引	团体	说明	类型	所有者	删除
1	kkk	kkk123	日志和陷阱	sea	<input type="button" value="删除"/>
2	tht	tht123	日志和陷阱	road	<input type="button" value="删除"/>

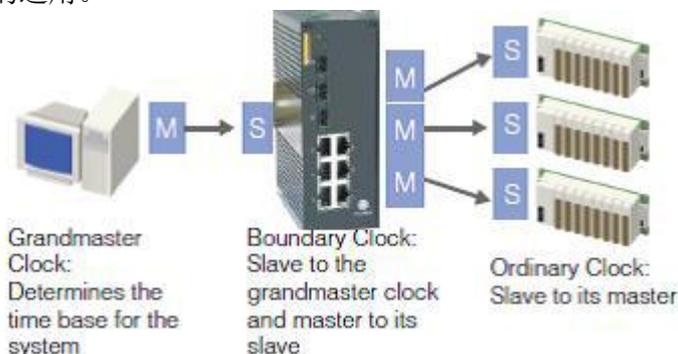
14.4.2 事件日志

此页面显示事件中设置的 RMON 事件日志类型，日志表项的信息，包括事件索引、日志索引、日志时间和日志说明。

事件索引	日志索引	日志时间	日志说明
1	1	Sep 03 09:33:26 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.2.0,Absolute,Falling,Actual Val:0,Thresh.Set:1,Interval(sec):2
1	2	Sep 03 09:33:27 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.2.0,Absolute,Rising,Actual Val:64,Thresh.Set:5,Interval(sec):3
1	3	Sep 03 09:33:27 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.2.0,Absolute,Rising,Actual Val:64,Thresh.Set:6,Interval(sec):2
2	4	Sep 03 09:33:29 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.4.0,Absolute,Rising,Actual Val:256,Thresh.Set:5,Interval(sec):5
1	5	Sep 03 09:37:17 2012	MIB Var:1.3.6.1.2.1.2.2.1.10.2.0,Absolute,Rising,Actual Val:19411,Thresh.Set:6,Interval(sec):2

第 15 章 精准时间 PTP

IEEE 1588 颁布于 2002 年，通过硬件和软件将网络设备（客户机）的内时钟与主控机的主时钟实现同步，满足分布式网络的精准时间同步需求，提供同步建立时间小于 10 μ s 的运用。



金恒威支持 PTP 的交换机通过软件实现时钟同步，具体配置如下面所介绍。

说明：如需对 PTP 进行配置，请先在[高级配置](#)里全局开启 PTP。

15.1 PTP 系统配置

时钟模型：设置交换机的时钟模型，有以下四种类型可选，默认为 V2 P2P TC。

V2 P2P TC 点到点 IEEE 1588 v2 透明时钟

V2 E2E TC 端到端 IEEE 1588 v2 透明时钟

V2 P2P BC 点到点 IEEE 1588 v2 边界时钟

V2 E2E BC 端到端 IEEE 1588 v2 边界时钟

一步时钟：开启/关闭一步时钟，默认为关闭状态，即两步方法。

Sync 报文间隔：设置同步报文时间间隔，可选 128ms, 256ms, 512ms, 1s, 2s, 4s, 8s 或 16s，默认为 1s。

Announce 报文间隔(秒)：设置通知报文时间间隔，时间单位为秒，可选 1, 2, 4, 8 或 16，默认为 2。

Announce 报文接收超时定时器(秒)：设置通知报文接收超时定时器，时间单位为秒，可选 2~10 间任一数值，默认为 3。

Delay Req 报文间隔(秒)：设置最小延迟请求报文间隔。时间单位为秒，可选 0~5 间任一数值，默认为 3。

域号：PTP 消息的子域名(IEEE 1588-2002)或域地址(IEEE 1588-2008)，可选 0~3 间任一数值，默认为 0。

优先权 1：设置第一优先级值，可设为 0~255 间任一数值，0 为最高优先级，255 为最低优先级，默认为 128。

优先权 2：设置第二优先级值，可设为 0~255 间任一数值，0 为最高优先级，255 为最低优先级，默认为 128。

时钟类：主时钟派发的时间或频率的可追溯性。可设为 0~255 间任一数值，默认为 248。

时标：可选 PTP 或 ARB，默认为 PTP。

PTP 时标：在正常操作中，日期就是 PTP 日期，时标是连续的。时间单位是 SI（国际单位制）秒。

ARB 时标：在正常操作中，日期由管理程序设定，并且可以重设。在管理程序间调用，时标是连续的。在整个时间内，管理程序的其它调用采用非连续时间。

59 秒跳跃：当前 UTC 天的最后一分钟包括 59s，如果日期不是 PTP，可选“关闭”，默认设为“关闭”。

61 秒跳跃：当前 UTC 天的最后一分钟包括 61s，如果日期不是 PTP，可选“关闭”，默认设为“关闭”。

开启 UTC 位移：如果当前 UTC 位移已知是正确的，初始化该值为“开启”，否则设为“关闭”，默认设为“关闭”。

UTC 位移：已知的 UTC 位移大，单位为秒。

The screenshot shows the 'PTP 系统配置' (PTP System Configuration) page. It contains a form with the following fields and values:

时钟模式	v2 P2P TC
一步时钟	关闭
Sync 报文间隔	1s
Announce 报文间隔(s)	2
Announce 报文接收超时定时器(s)	3
Delay Req 报文间隔(s)	3
域号	0
优先级 1	128
优先级 2	128
时钟类	248
时标	PTP
59 秒跳跃	关闭
61 秒跳跃	关闭
开启 UTC 位移	关闭
UTC 位移	0

An 'Apply' button is located at the bottom right of the form.

15.2 PTP 端口设置

将每个端口的 PTP 功能设置为开启/关闭状态。

该页下方将会列出各个端口当前是处于开启/关闭 PTP 状态，以及各个端口角色。

The screenshot shows the 'PTP 端口' (PTP Port) configuration page. It includes a form to set the status of a specific port and a table listing all ports.

Form fields:

- 端口: Ethernet0/1
- 状态: 关闭

PTP Port List Table:

端口	PTP 状态	端口角色
Ethernet0/1	关闭	无
Ethernet0/2	关闭	无
Ethernet0/3	关闭	无
Ethernet0/4	关闭	无
Ethernet0/5	关闭	无
Ethernet0/6	关闭	无
Ethernet0/7	关闭	无
Ethernet1/1	关闭	无
Ethernet1/2	关闭	无
Ethernet1/3	关闭	无

15.3 PTP 状态信息

显示当前 IEEE 1588 PTP 状态信息。

PTP 系统配置		PTP 端口		PTP 状态信息	
PTP 信息					
偏移主时钟的位移 (nsec)		0			
平均路径延迟 (nsec)		0			
移除步骤		0			
父时钟ID		00000000000000000000			
主时钟ID		0000000000000000			
主时钟时间类		248			
主时钟时间精度		0			
优先级 1		128			
优先级 2		128			
开启当前UTC位移		0			
当前UTC位移		0			
59秒跳跃		0			
61秒跳跃		0			
时标		1			
时钟源		0			

第 16 章 管理配置

本节概述了交换机管理和维护功能，包括：语言、IP 配置、SNTP、SMTP、邮件告警、中继告警、系统日志、Ping 测试、账户、TFTP 服务、重启、复位和保存。

16.1 语言

有两种语言可供选择：中文和英文，点击<提交>即可生效，页面将返回至系统信息页。

16.2 IP 配置

交换机支持 DHCP 和静态 IP 两种获取 IP 地址的方式。如开启 DHCP 客户端，交换机通过 DHCP 服务器自动获取 IP 地址，以实现网络资源的动态配置。或通过指定 IP 地址，子网掩码和网关来使用静态 IP，点击<提交>保存设置。绑定静态 IP 后将要求用新的 IP 地址重新登录。

DHCP客户端	<input checked="" type="checkbox"/> 开启
IP 地址	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="117"/> . <input type="text" value="241"/>
子网掩码	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
网关	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="117"/> . <input type="text" value="1"/>
<input type="button" value="提交"/>	

16.3 SNTP（简单网络时间协议）

在大型的网络中，如果依靠管理员手工配置来修改网络中各台设备的系统时间，不但工作量巨大，而且也不能保证时间的精确性。NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，并提供较高的时间同步精度。

NTP 时间同步过程中需要进行复杂的时钟优选运算，时间同步速度较慢，并且占用较多的系统资源。SNTP（Simple NTP，简单 NTP）简化了 NTP 的时间同步算法，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 SNTP 来实现时间同步。

SNTP 既提供了客户端功能也提供服务器端功能。

如果交换机作为 SNTP 服务器端，交换机作为 SNTP 服务器使用，其他交换机的时间可以同步到该交换机。设置该交换机系统时间年、月、日、时、分和秒，让其他交换机都同步到该交换机设置的时间。

如果交换机作为 SNTP 客户端，可以通过 SNTP 服务器获取同步时间来设置该交换机的

时间。填写 SNTP 服务器 IP 地址，格式为 xxx.xxx.xxx.xxx。

响应时间：交换机从 SNTP 服务器中获取响应的的时间间隔（秒），取值范围为 1~59 秒，缺省值为 5 秒。

时区偏移：格林威治标准时间（GMT）和本地时间的时差。

时分偏移：格林威治标准时间（GMT）和本地时间的分钟偏差。

SNTP设置					
SNTP模式	服务端				
SNTP服务器IP地址	<input type="text" value="xxx.xxx.xxx.xxx"/>				
最大响应时间(秒)	<input type="text" value="5"/>				
时区偏移	GMT				
时分偏移(分钟)	<input type="text" value="0"/>				
年	<input type="text" value="2012"/>	月	<input type="text" value="12"/>	日	<input type="text" value="7"/>
时	<input type="text" value="11"/>	分	<input type="text" value="20"/>	秒	<input type="text" value="38"/>
<input type="button" value="提交"/>					

16.4 SMTP（简单邮件传输协议）

当邮件告警中设置的事件发生时，交换机将发送电子邮件到一个目标邮件地址。

目的邮件：接收事件信息的电子邮件地址。

SMTP 服务器 IP 地址：SMTP 服务器的 IP 地址。

SMTP 账户名字：SMTP 服务器上源电子邮件帐号。

SMTP 账户密码：源电子邮件帐户的密码。

点击 <提交>，并点击<测试>按钮，以检查配置是否正确。如果正确，将会提示“测试成功”，目标邮箱也将收到电子邮件。

16.5 邮件告警

该页设置触发电子邮件的事件，包括系统事件和端口事件。

16.5.1 系统事件

该页设置以下系统事件，当事件发生时，点击<提交>以触发电子邮件发送。

设备冷启动：冷启动，第一次上电启动交换机。

设备热启动：热启动，在没有关掉电源情况下重新启动交换机。



Web 授权失败：由于用户名或密码不正确，登录交换机失败。

inmax Ring 环状态改变：inmax Ring 链路状态改变，例如 inmax Ring 端口关闭。

RMON 事件日志：详情见本手册 [14](#)。

邮件告警设置	
设备冷启动	<input type="button" value="关闭"/>
设备热启动	<input type="button" value="开启"/>
Web授权失败	<input type="button" value="开启"/>
Fi Ring环状态改变	<input type="button" value="关闭"/>
RMON事件日志	<input type="button" value="关闭"/>
<input type="button" value="提交"/>	

16.5.2 端口事件

该页设置以下端口事件，当事件发生时，启用事件以触发电子邮件发送。

端口：选择用于事件配置的端口。

告警类型：如启用，事件有三种报警类型：**链路连接**、**链路断开**以及**链路连接和断开**。

<input type="button" value="关闭"/>
<input type="button" value="链路连接"/>
<input type="button" value="链路断开"/>
<input type="button" value="链路连接和断开"/>

流量过载：在**流量统计时间**期间，端口流量超过**流量阈值**。

流量阈值：端口流量阈值（用端口速率百分比表示）。

流量统计时间：计算端口流量的统计持续时间。

 说明：

流量过载、**流量阈值**和**流量统计时间**是相互关联的。当启用**流量过载**时，**流量阈值**设置值应介于 1%和 99%之间，同时**流量统计时间**不得少于 10 秒。

页面下方列出所有的端口事件。

端口	告警类型	流量过载	流量阈值(%)	流量统计时间(s)
Ethernet0/1	链路断开	关闭	100	9
<input type="button" value="提交"/>				
端口事件状态				
端口	告警类型	流量过载	流量阈值(%)	流量统计时间(s)
Ethernet0/1	链路断开	关闭	100	9
Ethernet0/2	链路连接和断开	开启	50	20
Ethernet0/3	关闭	关闭	0	0
Ethernet0/4	关闭	关闭	0	0
Ethernet0/5	关闭	关闭	0	0
Ethernet0/6	关闭	关闭	0	0
Ethernet0/7	关闭	关闭	0	0
Ethernet0/8	关闭	关闭	0	0

16.6 中继告警

该页设置中继报警事件，包括系统事件及端口事件。当有事件出现时，外部设备的继电器输出将被闭合，例如，告警指示灯将发挥作用。

16.6.1 系统事件

该页是对系统事件报警配置进行设置，包括电源 A 掉电、电源 B 掉电和 inmax Ring 环断开。

电源 A 掉电： 电源 A 故障。

电源 B 掉电： 电源 B 故障。

inmax Ring 环断开： inmax Ring 链路状态断开。

中继告警设置	
电源A掉电	关闭
电源B掉电	关闭
Ring环断开	关闭
<input type="button" value="提交"/>	

16.6.2 端口事件

该页是对端口事件告警配置进行设置，包括端口、告警类型、流量过载、流量阈值和流量统计时间。

端口： 选择用于事件配置的端口。

告警类型：事件有三种报警类型：**链路连接、链路断开以及链路连接和断开。**

流量过载：在**流量统计时间**期间，端口流量超过**流量阈值**。

流量阈值：端口流量阈值（用端口速度百分比表示）。

流量统计时间：计算端口流量的统计持续时间。

📖说明：

流量过载、流量阈值和流量统计时间是相互关联的。当启用**流量过载**时，**流量阈值**设置值应介于 1 和 99 之间，同时**流量统计时间**不得少于 10 秒。

页面下方列出所有的端口事件。

端口	告警类型	流量过载	流量阈值(%)	流量统计时间(s)
Ethernet0/1	链路连接和断开	关闭	52	13
<input type="button" value="提交"/>				

端口事件状态

端口	告警类型	流量过载	流量阈值(%)	流量统计时间(s)
Ethernet0/1	链路连接和断开	关闭	52	13
Ethernet0/2	链路断开	开启	44	40
Ethernet0/3	链路连接	关闭	44	52
Ethernet0/4	关闭	关闭	0	0
Ethernet0/5	关闭	关闭	0	0
Ethernet0/6	关闭	关闭	0	0
Ethernet0/7	关闭	关闭	0	0
Ethernet0/8	关闭	关闭	0	0

16.7 系统日志

该页显示系统日志。每页显示 50 个日志。点击<前一页>或<下一页>可显示更多日志。点击<清除>，所有系统日志均可被清除。

日志索引	日志描述
1	2012/8/1 00:09:32 192.168.114.248 logins the system via WEB UI!
2	2012/8/1 00:09:23 192.168.114.248 has logout the system via WEB UI!
3	2012/8/1 00:03:24 192.168.114.248 logins the system via WEB UI!
4	2012/8/1 00:01:52 Someone logins the system via Serial Port, level 3.
5	2012/8/1 00:00:00 Starting system!
6	2012/8/1 00:45:08 192.168.117.242 has logout the system via WEB UI!
7	2012/8/1 00:36:20 192.168.114.248 has logout the system via WEB UI!
8	2012/8/1 00:29:12 192.168.114.248 logins the system via WEB UI!
9	2012/8/1 00:28:55 192.168.117.242 logins the system via WEB UI!
10	2012/8/1 00:20:23 192.168.0.30 has logout the system via WEB UI!
11	2012/8/1 00:07:39 192.168.0.30 logins the system via WEB UI!
12	2012/8/1 00:01:03 Someone logins the system via Serial Port, level 3.

16.8 Ping 测试

该页可通过 Ping IP 地址来检查交换机和某设备之间的连接情况。在 ping 文本框内填入要 ping 的 IP 地址，如不能 ping 成功，则会提示“此 IP 地址 ping 不通”；如能 Ping 成功，将提示“此 IP 地址可以 ping 通”。

Ping 测试

ping	<input style="width: 90%;" type="text" value="192.155.233.12"/>
<input type="button" value="提交"/>	

此IP地址ping不通.

此IP地址可以ping通.

16.9 账户

可以添加新帐户，并为指定的新帐户设置用户名、密码和访问权限。

用户名：用户名，为 3 到 16 个字符的字符串。

密码：密码，为 1 到 16 个字符的字符串。

访问权限：选择用户或管理员。用户级权限不能添加删除账户、不能使用 tftp 服务和不能使用复位功能，管理员可查看也可修改交换机的任何配置。

页面下方列出所有帐户，包括用户名和访问权限。可在此页面修改和删除帐户。



注意：如只有一个管理员用户，该用户不能删除；如有多个管理员用户，则可删除，但至少要保留一个管理员用户。

增加账户	
用户名	<input type="text"/>
密码	<input type="password"/>
确认密码	<input type="password"/>
访问权限	用户 <input type="button" value="v"/>
<input type="button" value="提交"/>	

用户列表

序号	用户名	访问权限	修改	删除
1	manager	用户	<input type="button" value="修改"/>	<input type="button" value="删除"/>
2	superuser	管理员	<input type="button" value="修改"/>	<input type="button" value="删除"/>
3	park	用户	<input type="button" value="修改"/>	<input type="button" value="删除"/>

16.10 TFTP 服务

TFTP（Trivial File Transfer Protocol，简单文件传输协议）使用方便，在连接过程中不需要认证控制，适用于客户端和服务器之间不需要复杂交互的环境。

16.10.1 更新 Firmware

该功能用于软件升级。设置交换机更新软件的 TFTP 服务器 IP 地址和 Firmware 名字。单击<提交>按钮升级交换机软件之前，请确认交换机已连接到 TFTP 服务器上。

Firmware更新	
TFTP服务器IP地址	<input type="text" value="192.168.10.23"/>
Firmware名字	<input type="text" value="508"/>
<input type="button" value="提交"/>	

16.10.2 备份配置

设置交换机备份配置的 TFTP 服务器 IP 地址和文件名。再单击<提交>按钮上传带有指定文件名的交换机配置文件到 TFTP 服务器之前，请确认交换机已连接到 TFTP 服务器上。

16.10.3 重载配置

设置交换机重载配置的 TFTP 服务器 IP 地址和文件名。首先，保证交换机连接到 TFTP 服务器中；然后，单击<提交>按钮，交换机将下载该指定文件名的文件，并将其作为配置文件。



注意：当升级软件、上传或下载配置文件时，不要关闭电源。

16.11 重启

在该页面，有两个按钮，一个是<保存并重启>，另一个是<不保存重启>。

保存并重启：保存当前的配置，然后重新启动。

不保存重启：直接重新启动，同时不保存当前配置。所有的新配置可能会丢失。

如果你不保存当前配置，所有的新配置将会丢失。

请确认在重启前是否要保存当前配置？

保存并重启

不保存重启

16.12 复位

该页面有两个标签页，一个是复位，另一个是恢复出厂值。

复位：除了 IP 地址和用户帐户，交换机将恢复出厂默认值。

恢复出厂值：交换机将被复位成出厂默认设置，包括 IP 地址和用户账号。

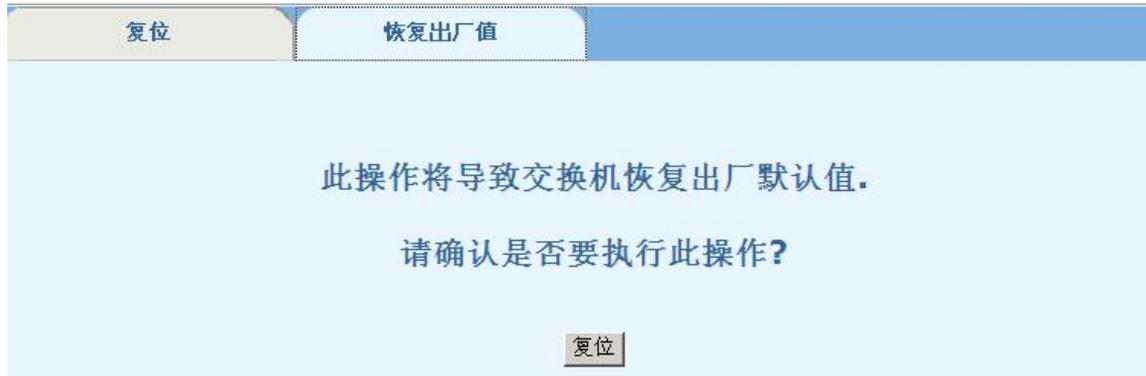
复位

恢复出厂值

除了 IP 地址和用户帐户，此操作将恢复交换机出厂默认值。

请确认是否要复位交换机出厂配置？

复位



16.13 保存

该页保存当前配置。

第 17 章 退出

单击左边菜单上的[退出]，点击<确定>退出交换机 Web 页面。