轻网管交换机

HR310S-4T2XT

Web 管理手册

版本：V1.0

目录

修订记录

日期	版本	描述
2024-12-27	V 1.0	第一版

1 前言

1.1 目标读者

本手册适用于负责安装、配置或维护网络的安装人员和系统管理员。本手册假定您了解所有网络使用的传输和管理协议。

本手册也假定您熟知与组网有关的网络设备、协议和接口的专业术语、理论原理、实践技能以及特定专业知识。同时您还必须有图形用户界面、命令行界面、简单网络管理协议和 Web 浏览器的工作经验。

1.2 本书约定

本手册采用以下约定方式。

GUI 约定	描述
说明	操作内容的描述，进行必要的补充和说明。
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。

2 登录 Web 页面

2.1 登录 Web 网管客户端

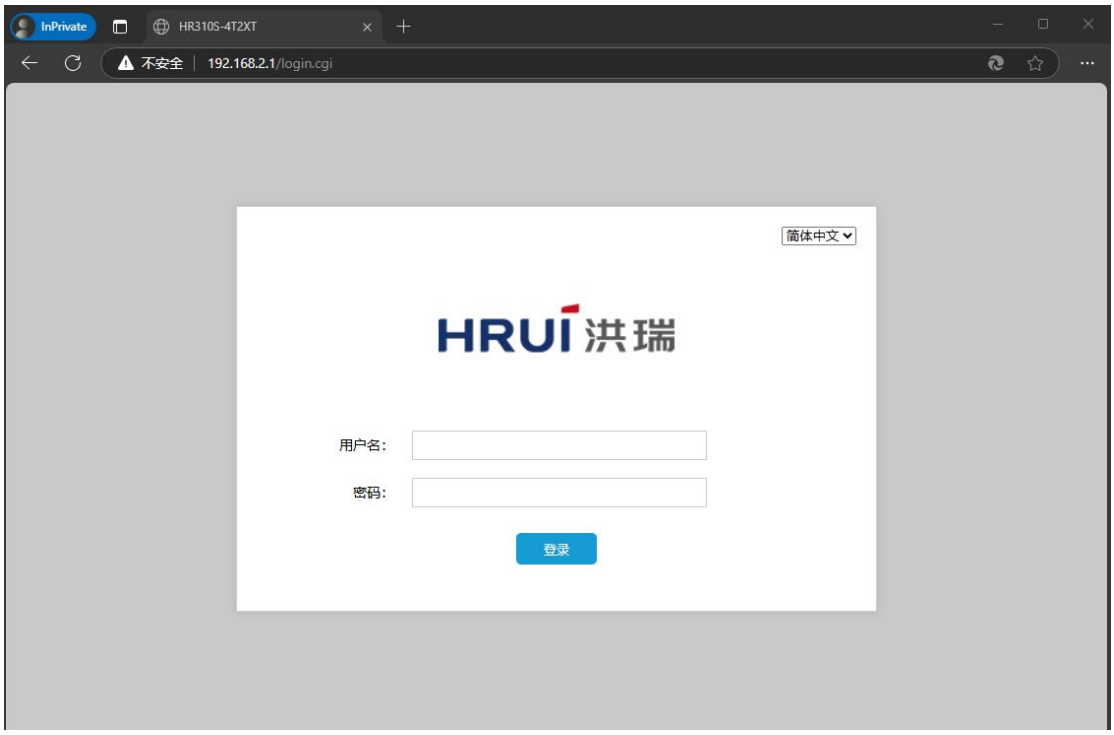
用户可通过打开 Web 浏览器，输入交换机缺省地址：**http://192.168.2.1**，按 Enter 键。

说明:

设备支持浏览器：IE9.0 以上，Chrome23.0 以上，Firefox20.0 以上

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 **192.168.2.x**（x 代表 1~254，除 1），子网掩码设置为 **255.255.255.0**， 但 PC 的 IP 不可与交换机相同， 即不能为 **192.168.2.1**。

此时出现登录窗口，如下图所示。输入缺省用户名: **admin** 和密码: **admin**。单击<登录>按钮，将看到交换机系统信息。



2.2 客户端界面组成

Web 网管系统的典型操作界面的介绍，如下图所示。

2.3 Web 界面导航树

Web 网管的菜单主要提供系统、配置、安全、诊断、工具等菜单项。每个菜单选项下又有子菜单。详细导航树的信息如下:

菜单项	子菜单	二级子菜单	说明
首页	系统信息		显示端口状态与产品信息
交换机监控	MAC 地址表		查看 MAC 地址信息
	端口统计		查看端口统计
交换机设置	端口设置		配置查看设备所有端口信息
	端口镜像		配置查看端口镜像
	端口隔离		配置查看端口隔离
	端口限速		配置查看端口速率限制
	端口汇聚		配置查看链路聚合
	静态 MAC		配置查看静态 MAC 信息
VLAN 设置	VLAN	VLAN 设置	配置查看 VLAN
		端口 VLAN	配置端口 VID 允许接受帧类型
环路设置	环路协议		配置查看环路检测
	STP 全局		配置查看生成树全局信息
	STP 端口		配置查看生成树端口信息
QoS	端口到列队		配置查看端口队列
	列队权重		配置查看列队权重
高级设置	DHCP 侦听		配置查看 DHCP 侦听
	风暴控制		配置查看风暴抑制信息
	IGMP 设置		配置查看 IGMP Snooping
	巨型帧		配置查看端口 Jumbo 帧

系统管理	IP 设置		配置查看当前设备的管理 IP 地址
	登录设置		配置查看设备用户信息
	设置重启		重启系统
	保存配置		保存配置
	备份与恢复配置		更新升级设配置文件
	系统升级		更新升级设备软件版本
	恢复出厂设置		重置系统

3 首页

3.1 系统信息

根据所连接的交换机，能够非常直观地显示出该款交换机前面板上各端口的信息与产品信息，其显示内容包括：产品型号，版本，MAC 地址等等。

操作步骤：

1. 单击导航树中的“首页”菜单，进入系统信息查看界面，如下图所示：

4 交换机监控

4.1 MAC 地址表

操作步骤：

1. 单击导航栏中“交换机监控 > MAC 地址表”菜单，进入 MAC 地址表页面：

MAC地址表

搜索

MAC 地址	类型	端口	VLAN ID
00:0E:C6:3C:2F:4C	动态	1	1

共 2 条　当前显示 1-10 条,　每页 10 条　<<　<　1　>　>>　1 /1页　跳转

2. 在该页，可以查看 MAC 地址表信息，为适应网络的变化，MAC 地址表需要不断更新。MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，到达生存周期仍得不到刷新的表项将被删除，这个生存周期被称作老化时间。如果在到达生存周期前记录被刷新，则该表项的老化时间重新计算。

MAC地址表

00:E0:C4:00:00:00　搜索

MAC 地址	类型	端口	VLAN ID
00:E0:C4:00:00:00	静态	1	1

共 1 条　当前显示 1-10 条,　每页 10 条　<<　<　1　>　>>　1 /1页　跳转

注意：MAC 查找显示等待过程会与设备中断通信

4.2 端口统计

查询端口统计信息

操作步骤：

1. 单击导航栏中“交换机监控 > 端口统计”菜单，进入端口配置页面：

端口统计

端口	状态	连接状态	发送数据包数	接收数据包数	发送字节数	接收字节数
端口 1	开启	断开	0	0	0	0
端口 2	开启	断开	0	0	0	0
端口 3	开启	断开	0	0	0	0
端口 4	开启	连接	0	0	0	0
端口 5	开启	断开	0	0	0	0
端口 6	开启	断开	0	0	0	0

清空

5 交换机设置

5.1 端口设置

查询和配置以太网端口

操作步骤:

1. 单击导航树中的“交换机设置 > 端口设置”菜单，进入界面，如下图所示:

端口列表

端口	开关	双工模式		协商速率		流量控制
		配置属性	实际状态	配置属性	实际状态	
端口 1	开启	自动	半双工	自动	10M	关闭
端口 2	开启	自动	半双工	自动	10M	关闭
端口 3	开启	自动	半双工	自动	10M	关闭
端口 4	开启	自动	全双工	自动	1000M	关闭
端口 5	开启	自动	半双工	自动	10M	关闭
端口 6	开启	自动	半双工	自动	10M	关闭

界面信息含义如下表所示。

配置项	说明
状态	端口开关
速度/双工	端口速率
流控	流控开关

5.2 端口镜像

端口镜像是把交换机被镜像端口的报文复制到监控端口；监控端口通常会接入数据检测设备，用户利用这些设备分析被镜像端口接收到的报文，进行网络监控和故障排除。

1. 单击导航树中的“交换机设置 >端口镜像”菜单，进入界面，如下图所示：

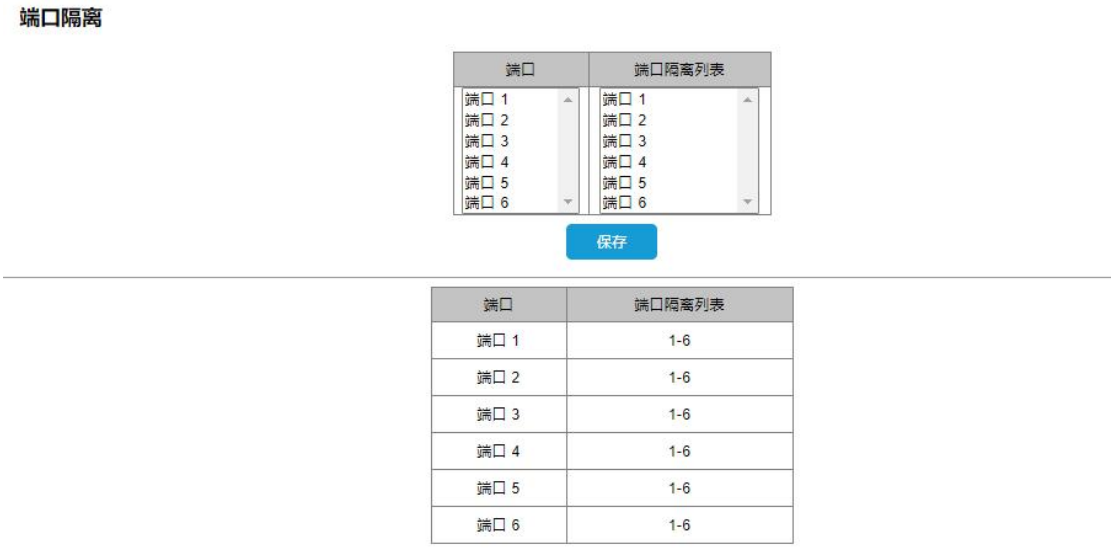
界面信息含义如下表所示。

配置项	说明
镜像方向	使能或去使能端口镜像，支持入方向，出方向和双方向
监控端口	只能选择一个普通物理端口，不包括链路聚合端口和源端口。
被监控端口列表	镜像源端口列表

5.3 端口隔离

端口流量之间有时不需要互相通信，但是广播、组播等报文会泛洪到各个端口之间，此时可以通过端口隔离功能来实现端口与端口之间的报文隔离。

1. 单击导航树中的“交换机设置 > 端口隔离”菜单，进入界面，如下图所示：



界面信息含义如下表所示。

配置项	说明

端口	端口列表
端口隔离列表	对应端口报文允许转发到哪个端口

5.4 端口限速

配置接口限速就是限制物理接口向外发送数据的速率。在流量从接口发出前，在接口的出方向上配置限速，对流出的所有报文流量进行控制。

1. 单击导航树中的“交换机设置 > 端口限速”菜单，进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
端口	端口列表
类型	入口\出口
状态	使能或去使能端口限制
速率	速率限制值，范围:1 到 2500 M/1 到 10000M

5.5 端口汇聚

链路聚合（Link Aggregation）是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽和可靠性的一种方法。

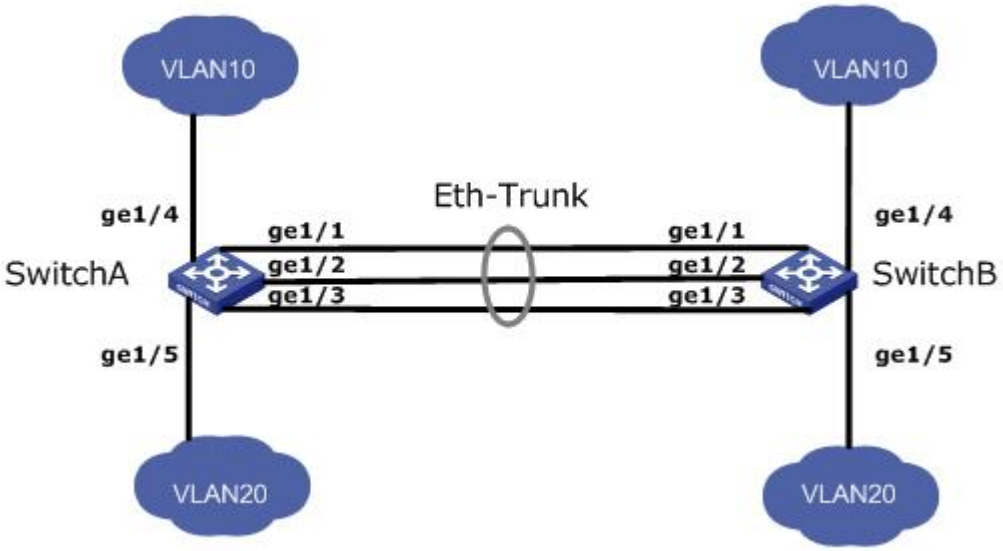
静态链路聚合组 LAG（Link Aggregation Group）是指将若干条以太链路捆绑在一起所形成的逻辑链路，简写为 Eth-Trunk。

随着网络规模不断扩大，用户对链路的带宽和可靠性提出越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。

采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻

辑接口，实现增加链路带宽的目的。链路聚合的备份机制能有效提高可靠性，同时，还可以实现流量在不同物理链路上的负载分担。

如下图所示，SwitchA 与 SwitchB 之间通过三条以太网物理链路相连，将这三条链路捆绑在一起，就成为了一条 Eth-Trunk 逻辑链路，这条逻辑链路的带宽等于原先三条以太网物理链路的带宽总和，从而达到了增加链路带宽的目的；同时，这三条以太网物理链路相互备份，有效地提高了链路的可靠性。



在有以下需求时，可通过配置链路聚合实现：

- 当两台交换机设备之间通过一条链路连接带宽不够时。
- 当两台交换机设备之间通过一条链路连接可靠性不满足要求时。

根据是否启用链路聚合控制协议 LACP，链路聚合分为静态模式和 LACP 模式。静态模式下，Eth-Trunk 的建立、成员接口的加入由手工配置，没有链路聚合控制协议的参与。该模式下所有活动链路都参与数据的转发，平均分担流量，因此称为负载分担模式。如果某条活动链路故障，链路聚合组自动在剩余的活动链路中平均分担流量。当需要在两个直连设备间提供一个较大的链路带宽而设备又不支持 LACP 协议时，可以使用静态模式。

操作步骤：

1. 单击导航树中的“交换机配置 > 端口汇聚”菜单，进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
聚合号	聚合组 ID，最大支持 2 组
端口号	聚合组成员端口，最大支持 4 个成员

LACP（链路聚合控制协议）基于 IEEE 802.3ad 标准，对链路进行动态聚合和分解。它通过 LACPDU（链路聚合控制协议数据单元）与相对的网络设备交换信息。

端口使用 LACP 后，将通过发送 LACPDU 向对方网络设备通知系统优先级、系统 MAC、端口优先级和端口号以及操作密钥。对方设备接收到这些信息后，会将其与其他端口保存的信息进行比较，从而就端口参与或退出动态聚合达成一致。

动态 LACP 聚合由系统自动创建或删除，即内部端口可以自行添加或删除。只有连接到具有相同速率、双工和基本配置的同一设备的端口才能聚合。

添加动态链接聚合的说明:

1. 点击导航栏中的“交换机配置>端口汇聚”，选择 LAG ID 和 LACP 模式，“编辑”如下:

2. 点击“交换机配置>端口汇聚”选择 LACP，选择两个端口添加为一个 LACP 组

界面信息含义如下表

配置项	说明
类型	静态模式：当需要增加两台设备之间的带宽或可靠性，而两台设备中有一台不支持 LACP 协议时，可在设备上创建静态链路聚合，并加入多个成员接口增加设备间的带宽及可靠性。 LACP 模式：在动态 LACP 模式下两设备间的链路具有冗余备份的能力，当部分链路故障时使用备份链路替代故障链路，保持数据传输的不中断。
系统优先级	LACP 确定两台设备之间选择主动、被动模式时根据优先级决策
端口优先级	LACP 在确定动态聚合组成员模式，根据系统优先级高的设备端口优先级来确定。
超时时间	决定 LACP 协议报文发送的频率

说明:

改变 Eth-Trunk 工作模式前请首先确保该 Eth-Trunk 中没有加入任何成员接口，否则无法修改 Eth-Trunk 的工作模式。本端和对端配置的工作模式应保持一致。

5.6 静态 MAC

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：

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

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端口发送。
- 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。

静态表项由用户手工配置，并下发到各接口板，表项不老化。

1. 单击导航树中的“交换机设置 > 静态 MAC”菜单进入界面，如下图所示：

界面信息含义如下表所示。

静态MAC

MAC	VLAN ID	端口
FF:FF:FF:FF:FF:FF (MAC格式：FF:FF:FF:FF:FF:FF)	VLAN 1	端口 1

添加MAC

选择	MAC 地址	VLAN ID	端口
☐	00:E0:C4:00:00:00	1	1

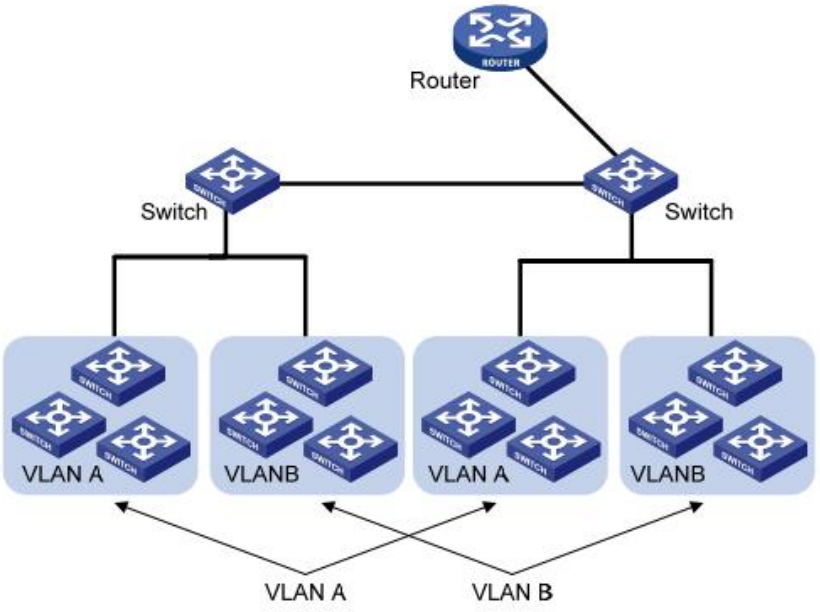
删除

配置项	说明
MAC 地址	MAC 地址 e.g.: HH:HH:HH:HH:HH:HH
VLAN ID	指定的 VLAN
端口	静态 MAC 绑定端口列表

6 VLAN 设置

6.1 VLAN

VLAN 的组成不受物理位置的限制，因此同一 VLAN 内的主机也无须放置在同一物理空间里。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。

此管理型交换机支持 802.1Q VLAN、基于端口的 VLAN。在缺省配置时，VLAN 为 802.1Q VLAN 模式。

6.1.1 VLAN 设置

该设置页面功能可以添加 VLAN

操作步骤：

1. 单击导航树中的“VLAN 设置 > VLAN 设置> ”菜单，进入界面，如下图所示：

6.1.2 端口 VLAN

该设置页面功能可以选中 Access 和 Trunk 端口类型

操作步骤：

1. 单击导航树中的“VLAN 设置 > 端口 VLAN ”菜单，进入界面，如下图所示：

VLAN端口

端口	端口类型	Access VLAN	Native VLAN	允许VLAN
选择端口	Access	VLAN 1	VLAN 1	选择VLAN

保存

端口	端口类型	Access VLAN	Native VLAN	允许VLAN
端口 1	Trunk	-	1	1
端口 2	Trunk	-	1	1
端口 3	Trunk	-	1	1
端口 4	Trunk	-	1	1
端口 5	Trunk	-	1	1
端口 6	Trunk	-	1	1

界面信息含义如下表所示。

配置项	说明
VLAN	端口的默认 VLAN
Native VLAN	设置端口的 PVID

7 环路设置

7.1 环路检测/环路避免

设备通过发送环路检测报文并检测其是否返回本设备（不要求收、发端口为同一端口）以确认是否存在环路。若某端口收到了由本设备发出的环路检测报文，就认定该端口所在链路存在环路。当网络中出现环路时，对应的端口 LED 灯将会闪烁告警（启用环路避免时会阻塞环路），以便给网络管理员释放该端口存在环路情况

操作步骤：

1. 单击导航树中的“环路设置 > 环路协议”菜单，进入界面，如下图所示：

环路协议设置

界面信息含义如下表所示。

配置项	说明
环路协议	关闭、环路检测、生成树

7.2 STP 全局

快速生成树协议（RSTP） 用于在局域网中消除数据链路层物理环路，其核心是快速生成树算法。RSTP 完全向下兼容 STP 协议，除了和传统的 STP 协议一样具有避免回路、动态管理冗余链路的功能外，RSTP 极大的缩短了拓扑收敛时间，在理想的网络拓扑规模下，所有交换设备均支持 RSTP 协议且配置得当时，拓扑发生变化（链路 UP/DOWN）后恢复稳定的时间可以控制在秒级。RSTP 的主要功能可以归纳如下：

1、 发现并生成局域网的一个最佳树型拓扑结构；

2、 发现拓扑故障并随之进行恢复，自动更新网络拓扑结构，启用备份链路，同时保持最佳树型结构；

操作步骤：

1. 单击导航树中的“环路设置 > STP 全局”菜单，进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
版本	配置查看 STP 模式
最大老化时间	配置查看最大老化时间
欢迎时间	配置查看欢迎时间
转发延时	配置查看转发延时时间

7.3 STP 端口

操作步骤：

1. 单击导航树中的“ 环路设置 > STP 端口”菜单，进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
路径开销	配置查看端口路径开销
优先级	配置查看端口优先级
点到点	配置查看 P2P
边缘	配置查看边缘端口

8 QoS

QoS（Quality of Service）用于评估服务方满足客户服务需求的能力，在 Internet 中，QoS 用于评估网络传送分组的服务能力。由于网络提供的服务是多样的，因此可以基于不同方面进行评估。通常所说的 QoS，是对分组投递过程中可为带宽、时延、时延抖动、丢包率等核心需求提供支持的服务能力的评估。带宽，又可称为吞吐量，表示一定时间内业务流的平均速率，单位通常是 Kbit/s。时延，表示业务流穿过网络时需要的平均时间。对于网络中的一个设备来说，一般将时延的需求理解为几种等级。例如分为两种时延等级，通过优先队列的调度方法使得高优先级的业务尽可能快地获得服务，而低优先级的业务则需要等待没有高优先级业务时才能获得服务。时延抖动，表示业务流穿过网络的时间的变化。丢包率，表示业务流在传送过程中的丢失比率。由于现代的传输系统具有很高的可靠性，信息的丢失往往发生在网络出现拥塞时。最常见的情况是队列溢出导致分组丢失。在传统的 IP 网络中，所有的报文都被无区别的等同对待，每个网络设备对所有的报 文均采用先入先出的策略进行处理，尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。

网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求。例如 VoIP 和视频等时延敏感业务对报文的传输时延提出了较高要求。如果报文传送延时太长，将是用户所不能接受的。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的业务类型，进而为之提供相应的服务。

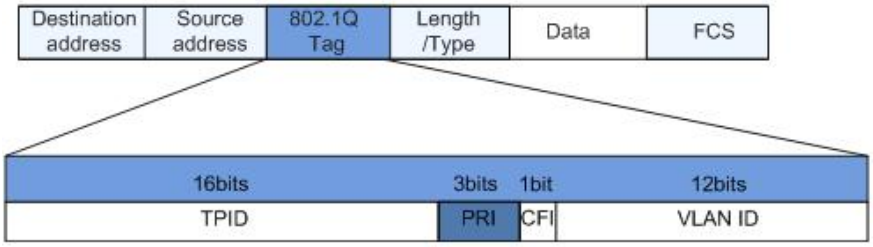
传统 IP 网络的尽力服务不可能识别和区分出网络中的各种业务类型，而具备业务类型的区分能力正是为不同的业务提供差异化服务的前提，所以传统网络的尽力服务模式已不能满足应用的需要。QoS 技术的出现便致力于解决这个问题。QoS 可以对网络流量进行调控，避免并管理网络拥塞，减少报文丢包率。同时支持为用户提供专用带宽，为不同业务提供不同的服务质量等，完善了网络的服务能力。

不同的报文使用不同的 QoS 优先级，例如 VLAN 报文使用 802.1p，或称 CoS（Class of Service）字段，IP 报文使用 DSCP。当报文经过不同网络时，为了保持报文的优先级，需要在连接不同网络的网关处配置这些优先级字段的映射关系。

VLAN 帧头中的 802.1p 优先级

通常二层设备之间交互 VLAN 帧。根据 IEEE 802.1Q 定义，VLAN 帧头中的 PRI 字段（即 802.1p 优先级），或称 CoS（Class of Service）字段，标识了服务质量需求。

VLAN 帧中的 802.1p 优先级

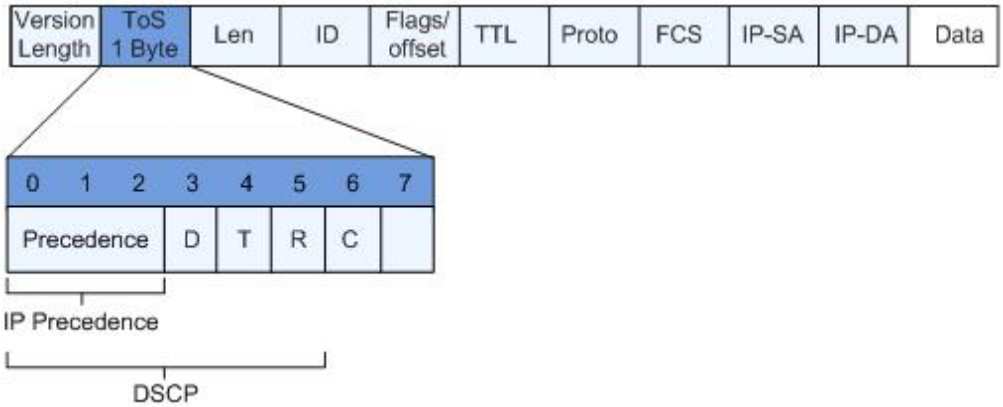


在 802.1Q 头部中包含 3 比特长的 PRI 字段。PRI 字段定义了 8 种业务优先级 CoS，按照优先级从高到低顺序取值为 7、6、……、1 和 0。

IP Precedence/DSCP 字段

根据 RFC791 定义，IP 报文头 ToS（Type of Service）域由 8 个比特组成，其中 3 个比特的 Precedence 字段标识了 IP 报文的优先级，Precedence 在报文中的位置如图所示。

IP Precedence/DSCP 字段



比特 0 ~ 2 表示 Precedence 字段，代表报文传输的 8 个优先级，按照优先级从高到低顺序取值为 7、6、……、1 和 0。最高优先级是 7 或 6，经常是为路由选择或更新网络控制通信保留的，用户级应用仅能使用 0 级 ~ 5 级。除了 Precedence 字段外，ToS 域中还包括 D、T、R 三个比特：D 比特表示延迟要求（Delay，0 代表正常延迟，1 代表低延迟）。T 比特表示吞吐量（Throughput，0 代表正常吞吐量，1 代表高吞吐量）。R 比特表示可靠性（Reliability，0 代表正常可靠性，1 代表高可靠性）。ToS 域中的比特 6 和 7 保留。

RFC1349 重新定义了 IP 报文中的 ToS 域，增加了 C 比特，表示传输开销（Monetary Cost）。之后，IETF DiffServ 工作组在 RFC2474 中将 IPv4 报文头 ToS 域中的比特 0 ~ 5 重新定义为 DSCP，并将 ToS 域改名为 DS（Differentiated Service）字节。DSCP 在报文中的位置如上图

所示。DS 字段的前 6 位（0 位～5 位）用作区分服务代码点 DSCP（DS Code Point），高 2 位(6 位、7 位)是保留位。DS 字段的低 3 位(0 位～2 位)是类选择代码点 CSCP(Class Selector Code Point），相同的 CSCP 值代表一类 DSCP。DS 节点根据 DSCP 的值选择相应的 PHB（Per-Hop Behavior）。

8.1 端口到队列

为数据帧的不同标记设置处理优先级

操作步骤:

1. 单击导航树中的“QOS 设置 > 端口到队列”菜单，进入界面，如下图所示:

界面信息含义如下表所示。

配置项	说明
队列	范围 1-8

8.2 队列权重

权重为严格优先级时相当于 SP，权重为 1-15 的值时相当于 WRR（加权循环调度算法）

操作步骤:

1. 单击导航树中的“QOS 设置 > 队列权重”菜单，进入界面，如下图所示:

队列权重

队列	权重
1	严格优先级
2	严格优先级
3	严格优先级
4	严格优先级
5	严格优先级
6	严格优先级
7	严格优先级
8	严格优先级

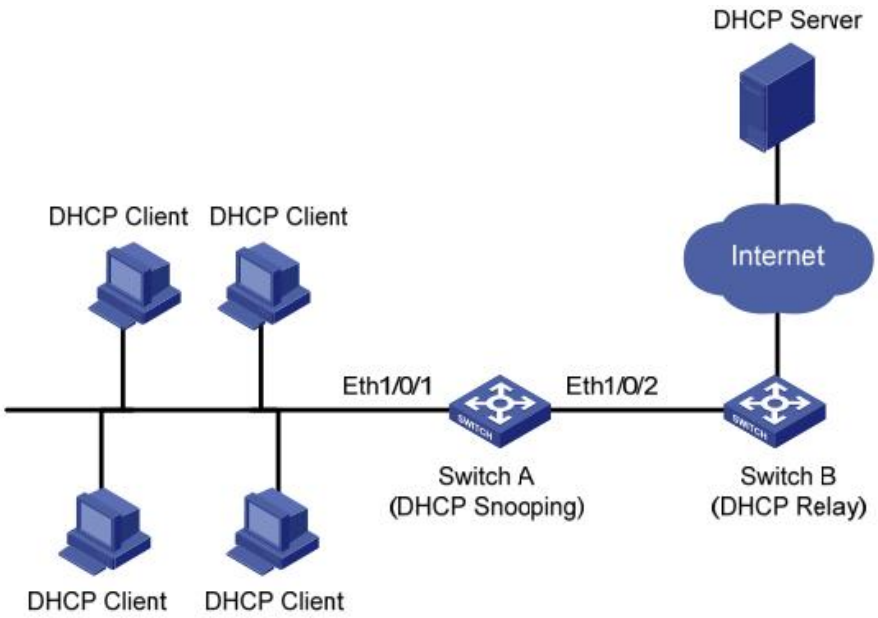
界面信息含义如下表所示。

配置项	说明
权重	默认为严格优先级，权重范围 1-15

9 高级设置

9.1 DHCP 侦听

出于安全性的考虑，网络管理员可能需要记录用户上网时所用的 IP 地址，确认用户从 DHCP 服务器获取的 IP 地址和用户主机的 MAC 地址的对应关系。交换机可以通过运行在网络层的 DHCP 中继的安全功能记录用户的 IP 地址信息。交换机可以通过运行在数据链路层的 DHCP Snooping 功能监听 DHCP 报文，记录用户的 IP 地址信息。另外，在网络中如果有私自架设的 DHCP 服务器，将可能导致用户得到错误的 IP 地址。为了使用户能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口与不信任端口。信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的 DHCP 报文正常转发，从而保证了 DHCP 客户端获取正确的 IP 地址。不信任端口是不与合法的 DHCP 服务器连接的端口。如果从不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文则会丢弃，从而防止了 DHCP 客户端获得错误的 IP 地址。



DHCP Snooping 典型组网

DHCP Snooping 通过以下两种方法来获得用户从 DHCP 服务器获取的 IP 地址和用户 MAC 地址信息：

- 监听 DHCP-REQUEST 报文
- 监听 DHCP-ACK 报文

启用 DHCP snooping

操作步骤：

1. 单击导航树中的“高级设置 > DHCP 侦听”菜单，进入 DHCP snooping 配置界面。

界面含义说明如下表

配置项	说明
状态	开启与关闭 DHCP snooping
端口	配置 DHCP snooping 的端口号
信任	该端口是否为信任端口

9.2 风暴控制

风暴控制按以下形式来防止广播、未知组播以及未知单播报文产生广播风暴。设备支持

对接口下的这三类报文分别按包速率进行风暴控制。在一个检测时间间隔内，设备监控接口下接收的三类报文的平均速率并和配置的最大阈值相比较，当报文速率大于配置的最大阈值时，设备会对该接口进行风暴控制，执行配置好的风暴控制动作。

当设备某个二层以太接口收到广播、组播或未知单播报文时，如果根据报文的目的 MAC 地址设备不能明确报文的出接口，设备会向同一 VLAN（Virtual Local Area Network）内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。

引入风暴抑制特性，可以控制这三类报文流量，防范广播风暴。

操作步骤：

1. 单击导航树中的“高级设置 > 风暴控制”菜单进入界面，如下图所示：

界面信息含义如下表所示。

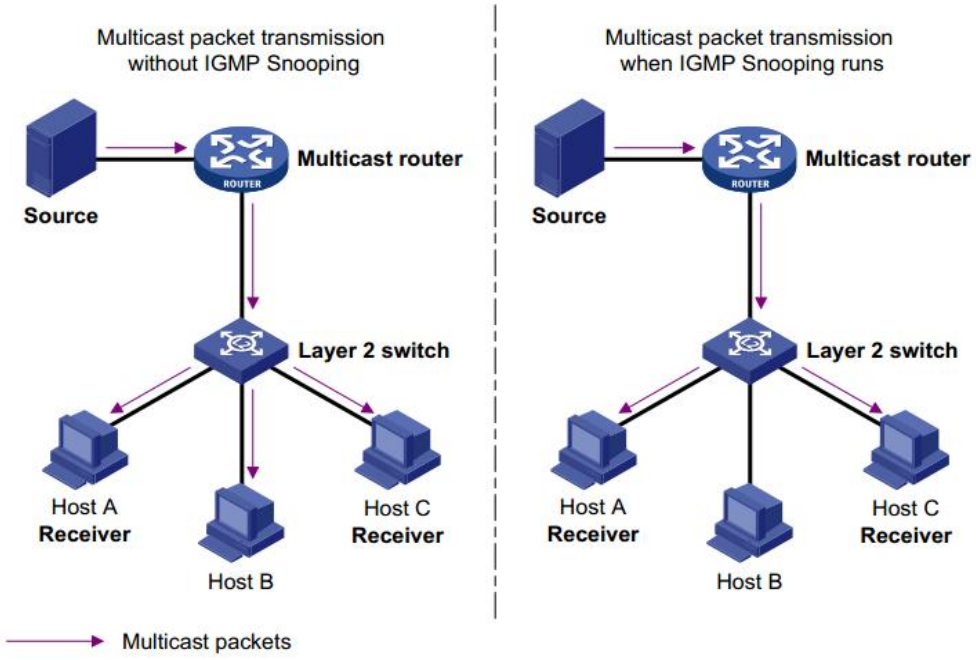
配置项	说明
风暴类型	广播、已知组播、未知单播、未知组播
端口	端口列表
状态	使能/去使能
速度	风暴抑制值

9.3 IGMP 设置

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。

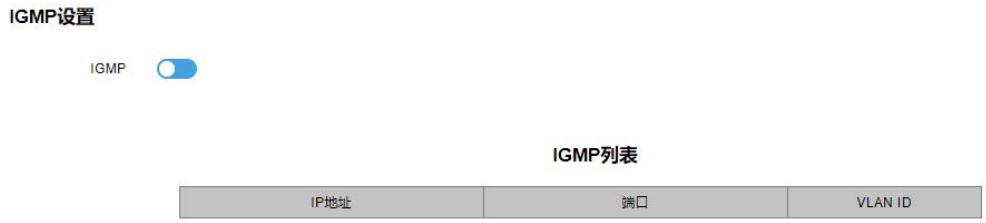
运行 IGMP 侦听的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

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。



操作步骤：

1. 单击导航树中的“高级配置 > IGMP 设置”菜单，进入界面，如下图所示：



界面信息含义如下表所示。

配置项	说明
打开	使能或去使能 IGMP Snooping
显示 IGMP 表	查询 IGMP 组信息

9.4 巨型帧

设置端口最大 MTU

操作步骤：

1. 单击导航树中的“高级设置 > 巨型帧”菜单进入界面，如下图所示：

界面信息含义如下表所示。

配置项	说明
巨型帧设置	设置端口 MTU

10 系统管理

10.1 IP 设置

配置和查看设备的管理 IP 地址。

操作步骤:

1. 单击导航树中的“系统管理 > IP 设置”菜单，进入 IP 设置界面，如下图所示:

界面信息含义如下表所示。

配置项	说明
DHCP 设置	Enable: 使能 DHCP 获取 Disable: 去使能 DHCP 获取
IP 地址	管理 IP 地址
子网掩码	IP 地址掩码
网关	IP 地址的网关

10.2 登录设置

用户可以检查和修改交换机的当前用户名、密码

操作步骤:

1. 单击导航树中的“系统管理 > 登录设置”菜单，进入界面，如下图所示:

界面信息含义如下表所示。

配置项	说明
用户名	账户名称
新密码	账户密码
新密码	账户密码重新输入

10.3 设备重启

操作步骤:

1. 单击导航树中的“系统管理 > 设备重启”菜单进入界面，如下图所示:

10.4 保存配置

保存配置

操作步骤:

1. 单击导航树中的“系统管理 > 保存配置”菜单进入界面，如下图所示:

10.5 备份与恢复配置

系统配置文件的升级和备份

操作步骤:

1. 单击导航树中的“系统管理 > 备份与恢复配置”菜单进入界面，如下图所示:

界面信息含义如下表所示。

配置项	说明
备份	备份配置文件
恢复	上传配置文件

注: 上传配置后需重启生效

10.6 系统升级

系统版本固件的升级，点击升级后会进入升级模式，跳转升级页面后选择固件在线升级

操作步骤：

1. 单击导航树中的“系统管理 > 系统升级”菜单进入界面，如下图所示：

注意：点击确定以后，升级过程中请勿断电，停留在升级页面等待约 1 分钟升级完成

10.7 恢复出厂设置

系统将恢复出厂配置

操作步骤：

1. 单击导航树中的“系统管理 > 恢复出厂设置”菜单进入界面，如下图所示：