Web配置

目录

第 1 章　配置准备

1.1　HTTP协议配置

交换机除了通过命令行，snmp 协议进行配置以外，也支持通过 Web 浏览器进行交换机配置。交换机支持 HTTP 服务端口的配置，异常报文超时时间配置等等。

1.1.1　选择提示信息语言

目前为止，交换机支持 2 种配置语言，英语和中文，可以通过以下配置命令来进行切换。

命令	目的
[no] ip http language { english}	将 web 配置提示语言设置为(英语)

1.1.2　配置 HTTP 服务端口

一般而言，HTTP 服务端口默认是 80，用户可以通过直接输入 ip 地址的方式来访问交换机，但交换机也支持用户更改服务端口，一旦更改了服务端口以后，访问交换机需要通过 ip 地址加上端口的方式。例如配置 ip 地址为 192.168.1.3，服务端口为 1234，则 http 的访问地址就应该改为 http://192.168.1.3:1234。建议不要使用其他公共协议使用的端口，以免防造成访问冲突，例如：ftp-20，telnet-23，dns-53，snmp-161，由于很多协议使用的端口号不方便记忆，所以建议使用 1024 以后的端口号。

命令	目的
ip http port { *portNumber* }	配置 HTTP 服务端口

1.1.3　开启 HTTP 服务

交换机支持对 HTTP 访问的控制，只有在开启 HTTP 服务时，交换机和 PC 才有 HTTP 协议交互，当关闭 HTTP 服务时，HTTP 协议交互就停止。

命令	目的
ip http server	开启 HTTP 服务

1.1.4　配置 HTTP 访问模式

交换机除了支持通过 HTTP 访问交换机的方式以外，也支持 HTTPS 的访问方式，通过以下命令可以将访问模式设置为 HTTP。

命令	目的
ip http http-access enable	配置 HTTP 访问模式

1.1.5 配置 Web 页面中最大显示的 Vlan 条目数

交换机支持最大 vlan 为 4094 个，但很多时候 web 上不一定要显示全部 vlan 信息，只要显示出部分 vlan 信息即可，即用户关心的 vlan 信息即可，用户可以通过以下命令设置最大的 vlan，web 上只会显示出从 1 到设定的最大 vlan 条目信息，默认最大 vlan 是 100。

命令	目的
ip http web max-vlan { *max-vlan* }	配置 Web 页面中最大显示的 Vlan 条目数

1.1.6 配置 Web 页面中最大显示的组播条目数

交换机支持最大组播条目为 100 条，用户可以通过以下命令设置最大的组播条目，web 上只会显示出从 1 到设定的最大组播条目信息，默认组播条目数是 15。

命令	目的
ip http web igmp-groups { *igmp-groups* }	Web 页面中最大显示的组播条目数

1.2 HTTPS协议配置

为了增加通信的安全性，除了 HTTP 协议，交换机也支持 HTTPS 协议。HTTPS 是以安全为目标的 HTTP 通道，在 HTTP 下加入 SSL 层。

1.2.1 配置 HTTPS 访问方式

通过以下命令可以将访问模式设置为 HTTPS。

命令	目的
ip http ssl-access enable	配置 HTTPS 访问模式

1.2.2 配置 HTTPS 服务端口

和 HTTP 服务端口类似，HTTPS 也有默认的服务端口 443，用户可以通过命令更改其服务端口，同样建议使用 1024 以后的端口，以防止和其他协议的端口号冲突。

参数	说明
ip http secure-port {*portNumber*}	配置 HTTPS 服务端口

第 2 章　访问交换机

2.1　通过HTTP访问交换机

通过 Web 浏览器访问交换机，请确保您所使用的浏览器能够符合以下几点要求：

- HTML 版本 4.0
- HTTP 版本 1.1
- JavaScript™版本 1.5

此外，请确保交换机运行的主程序文件支持 Web 访问，且您的计算机已经连接到交换机所在的网络。

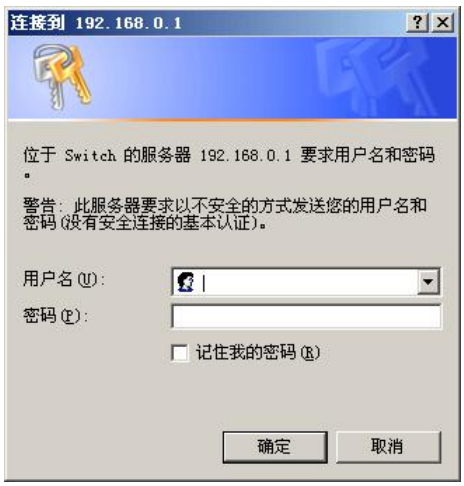
2.1.1　初次访问交换机

如果是第一次使用交换机，无需额外配置，您已经可以使用 Web 访问：

1、修改您计算机网络适配器的 IP 地址为“192.168.0.2”，子网掩码为“255.255.255.0”。

2、打开 Web 浏览器，在地址栏中输入“192.168.0.1”。注意“192.168.0.1”是交换机的缺省管理地址。

3、如果使用的是 Internet Explorer 浏览器，可以看到类似下图的对话框。在身份验证对话框中输入用户名和密码，初始的用户名和密码均为“admin”，请注意区分字母的大小写。



4、若认证成功，浏览器中会显示交换机的系统信息页。

2.1.2　升级到支持 Web 的版本

如果您的交换机是在使用中升级到支持 Web 访问的版本，且交换机中已经保存了配置文件，则此时无法直接使用 Web 访问。请按照下面的步骤启动交换机的 Web 功能。

1、使用随机附送的线缆连接到交换机的 Console 口，或者通过计算机 Telnet 到交换机的管理地址。

2、通过命令行进入交换机的全局配置模式，此时命令行提示符应该类似“Switch_config#”。

3、若交换机尚未配置管理地址，请创建 VLAN 接口，并配置 IP 地址。

4、在全局配置模式下，输入命令“**ip http server**”，启动 Web 服务。

5、通过命令“**username**”设置登录交换机的用户名和密码。该命令的使用请参见用户手册的“安全配置”部分。

完成上述步骤之后，便可在 Web 浏览器中输入交换机的地址对其进行访问。

6、输入命令“**write**”，将当前配置保存到配置文件。

2.2 通过安全的连接访问交换机

通过普通的 HTTP 访问交换机，Web 浏览器与交换机之间的数据不会经过加密。您可以选择通过基于安全套接字层（Secure Sockets Layer）的安全的连接来访问设备，以加密这些数据。

如果希望使用安全的连接访问交换机，请按照以下步骤操作：

1、使用随机附送的线缆连接到交换机的 Console 口，或者通过计算机 Telnet 到交换机的管理地址。

2、通过命令行进入交换机的全局配置模式，此时命令行提示符应该类似“Switch_config#”。

3、若交换机尚未配置管理地址，请创建 VLAN 接口，并配置 IP 地址。

4、在全局配置模式下，输入命令“**ip http server**”，启动 Web 服务。

5、通过命令“**username**”设置登录交换机的用户名和密码。该命令的使用请参见用户手册的“安全配置”部分。

6、输入命令“**ip http ssl-access enable**”，以开启交换机的安全连接访问。

7、输入命令“**no ip http http-access enable**”，禁止通过非安全连接访问交换机。

8、输入命令“**write**”，将当前配置保存到配置文件。

9、在与交换机相连的 PC 上打开 Web 浏览器，在地址栏中输入“https://192.168.0.1”（192.168.0.1 代表交换机的管理 IP 地址）后回车，此时便可通过安全的连接访问交换机。

2.3 Web界面介绍

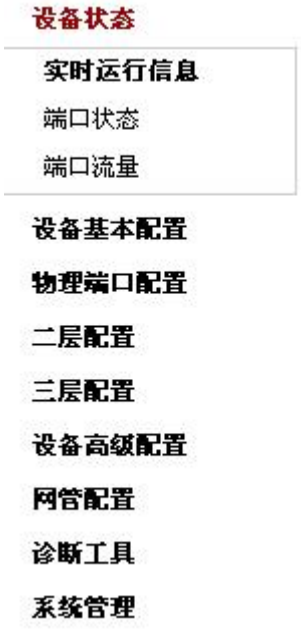
登录后的 Web 主页面分为顶部控制栏、导航栏、配置区和底部控制栏等部分。

2.3.1 顶部控制栏

全部保存	将当前的配置写入设备的配置文件存储。相当于在命令行执行“**write**”。 通过Web所作的配置生效后不会被立即写入配置文件，若不执行“全部保存”，设备重启后未保存的配置将会丢失。
English	切换界面语言为英文。
中文	切换界面语言为中文。
退出	从当前的登录状态退出。 点击“退出”之后，如果继续使用Web功能需要重新输入用户名和密码。

在您对设备进行了配置之后，顶部控制栏的左侧会显示上一步操作的结果。如果显示出错信息，请检查您的配置，并在稍后重试。

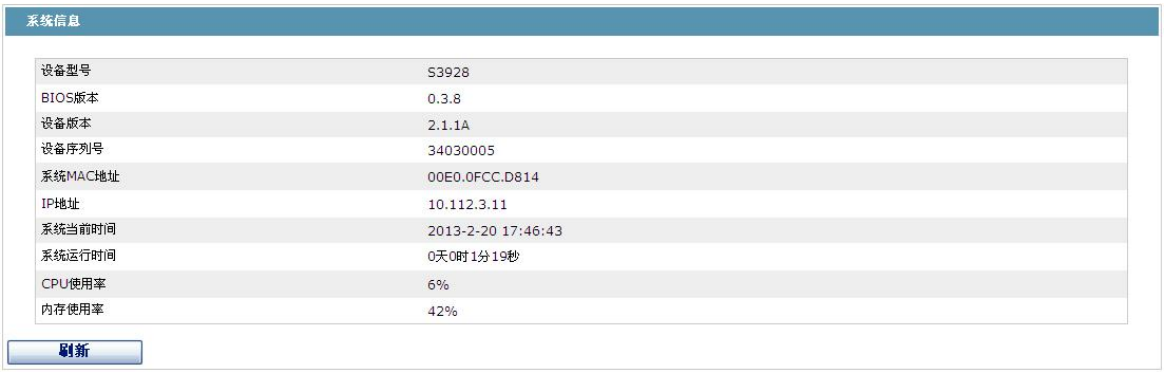
2.3.2 导航栏



导航栏控制配置区中显示的内容。导航栏的内容以列表的形式显示，并按类别分组。缺省情况下列表定位在“实时运行信息”。如需进行某项配置，请先点击组名，待列表展开后点击子项。比如，如果需要查看当前的端口流量，请先点击“设备状态”，然后点击“端口流量”。

请注意：
受限用户只能查看设备状态，不能修改设备配置。如果以受限用户权限登录 Web，除“设备状态”之外的组将不会显示。

2.3.3 配置显示区



配置显示区显示设备的状态信息和配置。通过点击导航栏的列表项可以改变该区域的内容。

2.3.4 配置区

配置区显示从导航栏中选中的内容。配置区总是会包含一个或多个按钮，它们的作用列举如下。

刷新	刷新当前配置区显示的内容。
应用	将配置的修改应用到设备。 应用配置的过程并不会将配置保存到设备的配置文件，如需保存请点击顶部控制栏的“全部保存”按钮。
重填	放弃对表单的修改。表单内容将会被复位。
新建	创建新的列表条目。比如新建VLAN条目、新建用户等。
删除	删除列表条目。
返回	返回上一级配置页面。

第 3 章　设备基本配置

3.1　设备名配置

在导航栏依次点击“设备基本配置”、“设备名配置”，打开配置页面如下图。

设备名称将被显示在登录对话框中。

设备缺省的名称为“Switch”，在文本框中输入新的名称，点击“应用”后对其进行修改。

3.2　时间管理

在导航栏依次点击“设备基本配置”、“时间管理”，进入时间管理页面。

点击“刷新”按钮，刷新显示设备的时钟。

在“时区选择”右侧的下拉框中选择设备所处的时区。选择“手工设置时间”，可以手动修改设备的时间。选择“网络时间同步”，可以为设备指定 3 个 SNTP 服务器，并设置时间同步的间隔。

第 4 章　物理端口配置

4.1　端口描述配置

在导航栏依次点击“物理端口配置”、“端口描述配置”，打开配置页面如下图。

端口	端口描述
G0/1	

在页面上可以修改端口的描述信息，最大可输入 120 个字符。 暂不支持 VLAN 端口的端口描述信息配置。

4.2　端口属性配置

在导航栏依次点击“物理端口配置”、“端口属性配置”，打开配置页面如下图。

端口	状态	速度	双工	流控	介质
G0/1	使能	自动	自动	关闭	自动

在页面上可以修改端口的使能状态、速率、双工模式以及流控状态。

请注意：
修改端口的速率或双工模式之后可能会造成端口链路状态切换，影响网络通信。

4.3 端口限速

在导航栏依次点击“物理端口配置”、“端口限速”，打开配置页面如下图。

通过该页面设置端口的接收和发送速率限制。缺省情况下所有端口均未限速。接收速率和发送速率可以按照百分比来配置，也可以按照交换机的指定单位来配置。

4.4 端口镜像

在导航栏依次点击“物理端口配置”、“端口镜像”，进入镜像配置页面。

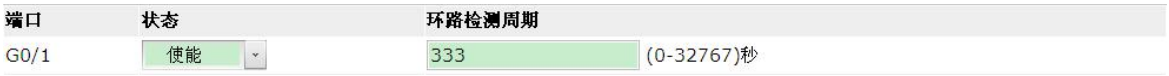
在“镜像端口”右侧的下拉框中选择一个端口作为镜像的目的端口。

通过点击复选框，选择镜像的源端口。

RX	端口收到的报文会被镜像到目的端口。
TX	端口发送的报文会被镜像到目的端口。
RX & TX	同时对端口接收和发送的报文进行镜像。

4.5 端口环路检测

在导航栏依次点击“物理端口配置”、“端口环路检测”，进入端口环路检测页面。



在“端口环路检测”页面中，可以配置端口环路检测的周期。

4.6 端口安全

4.6.1 IP 端口绑定配置

在导航栏依次点击“物理端口配置”、“端口安全”、点击页面上面的“IP 绑定”，进入 IP 端口绑定配置页面。

点击详细可以对各个物理端口进行源 IP 地址的绑定，以限定允许访问该端口的 IP 地址。

4.6.2 MAC 端口绑定配置

在导航栏依次点击“物理端口配置”、“端口安全”、点击页面上面的“MAC 绑定”，进入 MAC 端口绑定配置页面。

端口名称	详细
G0/1	详细

点击详细可以对各个物理端口进行源 MAC 地址的绑定，以限定允许访问该端口的 MAC 地址。

	序号	地址	操作
☐	1	1234.1234.1234	修改
☐	2	1234.1234.1235	修改

4.6.3 静态 MAC 过滤模式配置

在导航栏依次点击“物理端口配置”、“端口安全”、点击页面上面的“静态 MAC 过滤模式”，进入静态 MAC 过滤模式配置页面。

端口名称	端口模式	静态MAC过滤模式
G0/1	Access	未使能

通过该页面可以配置静态 MAC 过滤模式。缺省情况下，静态 MAC 过滤模式都未使能。静态 MAC 过滤模式不能配置在 Trunk 模式下的端口上。

4.6.4 静态 MAC 过滤条目

在导航栏依次点击“物理端口配置”、“端口安全”、“静态 MAC 过滤条目”，静态 MAC 过滤条目配置页面。

端口名称	详细
G0/1	详细

点击详细可以对各个物理端口进行源 MAC 地址的绑定，根据设置的静态 MAC 过滤模式，以限定允许或拒绝访问该端口的 MAC 地址。

	序号	过滤模式	MAC地址	操作
☐	0	未使能	0001.0002.0003	修改

4.6.5 动态 MAC 过滤模式配置

在导航栏依次点击“物理端口配置”、“端口安全”、点击页面上面的“动态 MAC 过滤模式”，进入动态 MAC 过滤模式配置页面。

端口名称	动态MAC过滤模式	最大地址数
G0/1	未使能	1 (1-4095)

通过该页面可以配置动态 MAC 过滤模式和所能允许的最大地址数。缺省情况下，动态 MAC 过滤模式都未使能，且最大地址数为 1。

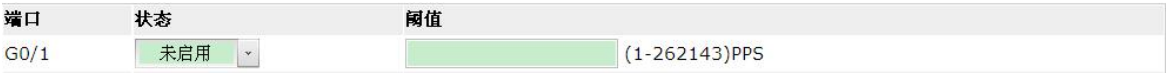
4.7 风暴控制

在导航栏依次点击“物理端口配置”、“风暴控制”，进入广播风暴控制、多播风暴控制和未知单播风暴控制配置页面。

4.7.1 广播风暴控制

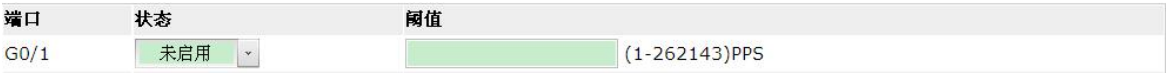
通过“状态”一列的下拉框控制端口是否启用广播风暴控制。在“阈值”一列中输入端口处理广播报文的阈值，每个端口都给出了阈值的合法范围。

4.7.2 多播风暴控制



通过“状态”一列的下拉框控制端口是否启用多播风暴控制。在“阈值”一列中输入端口处理多播报文的阈值，每个端口都给出了阈值的合法范围。

4.7.3 未知单播风暴控制



通过“状态”一列的下拉框控制端口是否启用未知单播风暴控制。在“阈值”一列中输入端口处理未知单播报文的阈值，每个端口都给出了阈值的合法范围。

第 5 章　二层配置

5.1　VLAN配置

5.1.1　VLAN 列表

在导航栏依次点击“二层配置”、“VLAN 配置”，进入 VLAN 列表视图。

	VLAN ID	VLAN 名称	操作
☐	1	Default	修改
☐	2	2	修改

VLAN 列表会按照从小到大的顺序列出当前设备中已经存在的 VLAN 条目。在条目较多的情况下，通过“上一页”、“下一页”、“搜索”等功能查找所需配置的 VLAN。

点击“新建”按钮，创建一个新的 VLAN。

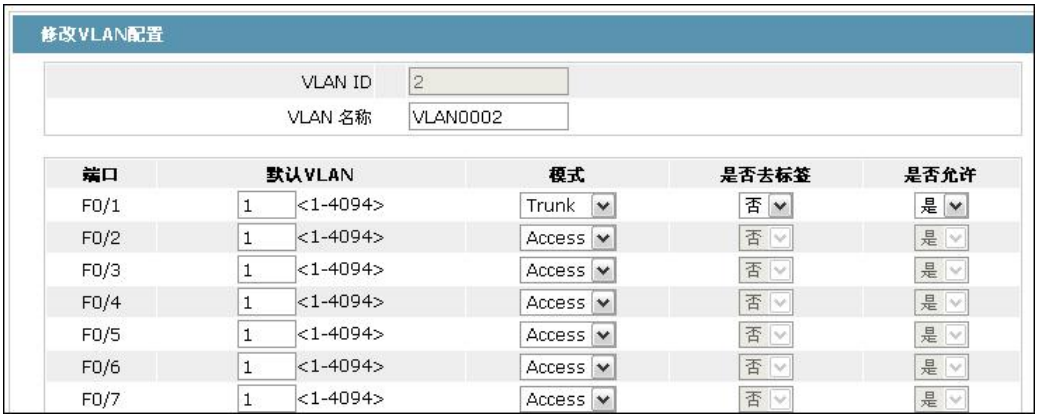
点击 VLAN 条目后的“操作”选项，可以修改 VLAN 的名称以及该 VLAN 中的端口属性。

选中条目前的复选框，然后点击“删除”按钮，可以删除选中的 VLAN。

请注意：
缺省配置下，VLAN 列表最多可以显示的条目数为 100。如需通过 Web 配置更多的 VLAN。请通过 Console 口或 Telnet 登录到交换机，进入全局配置模式，然后使用“**ip http web max-vlan**”命令修改最多显示的 VLAN 数目。

5.1.2 VLAN 配置

点击 VLAN 列表的“新建”按钮或“修改”选项，均可以进入 VLAN 配置页面，此页面用于创建新的 VLAN 或修改现有 VLAN 的属性。



如果是创建新的 VLAN，需要填写 VLAN ID，VLAN 名称可以为空。

通过端口列表，可以设置每个端口的缺省 VLAN，VLAN 模式（Trunk 或 Access），是否允许当前 VLAN 的报文进入，以及作为出口时对当前 VLAN 是否执行去标签。

请注意：
Trunk 模式的端口作为出口时，缺省情况下仅对自己的缺省 VLAN 执行去标签。

5.2 GVRP配置

5.2.1 GVRP 全局属性配置

在导航栏依次点击“二层配置”、“GVRP 配置”，进入 GVRP 全局属性配置页面。

用户可以配置开启或者关闭全局 GVRP 协议，并且可以设置动态 vlan 是否仅在注册端口生效。

5.2.2 GVRP 端口属性配置

在导航栏依次点击“二层配置”、“GVRP 配置”、 “GVRP 端口配置”进入 GVRP 端口属性配置页面。

GVRP 端口配置可以对端口进行启动或关闭 GVRP 协议的操作。

5.3 LLDP配置

5.3.1 LLDP 全局属性配置

在导航栏依次点击“二层配置”、“LLDP 配置”，进入 LLDP 全局属性配置页面。

用户可以选择开启 LLDP 协议，或者关闭该协议。当用户选择关闭 LLDP 协议时，用户将无法对设备端口进行 LLDP 协议配置。

HoldTime 表示 LLDP 的发送报文 ttl 值，默认为 120s。

Reinit 表示 LLDP 连续报文发送的延迟时间，默认为 2s。

5.3.2 LLDP 端口属性配置

在导航栏依次点击“二层配置”、“LLDP 配置”、 “LLDP 端口配置”进入 LLDP 端口属性配置页面。

LLDP 端口配置可以对端口进行启动或关闭接收、发送 LLDP 报文的功能。

5.4 STP配置

5.4.1 STP 状态信息

在导航栏依次点击“二层配置”、“STP 配置”，进入 STP 状态信息和根桥 STP 配置显示和本地 STP 属性配置页面。

其中，根桥 STP 配置和 STP 端口状态信息为只读。

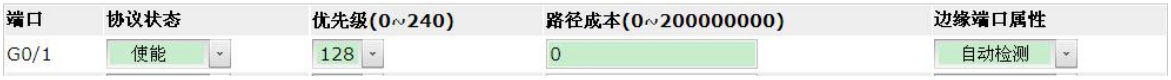
本地 STP 配置中，通过“协议类型”右侧的下拉框可以改变当前运行的生成树协议模式，支持的模式包括 STP，RSTP 和不使能 STP。

优先级和时间参数需要对不同的模式分别配置。

请注意：
改变 STP 模式可能会造成网络中断。

5.4.2 STP 端口属性配置

点击页面上的“STP 端口信息配置”选项卡，进入 STP 端口属性配置页面。



端口属性的配置与全局的 STP 模式无关。比如，如果配置端口协议状态为“不使能”，然后又改变了 STP 模式，端口在新的模式中同样不会参与协议运行。

端口的路径成本缺省值为 0，表示路径成本根据端口的速率自动计算，如果需要修改路径成本，请输入 0 以外的值。

5.5 IGMP-Snooping配置

5.5.1 IGMP-Snooping 配置

在导航栏依次点击“二层配置”、“IGMP Snooping”，进入 IGMP-Snooping 配置页面。

通过该页面可以配置交换机是否转发未知组播、是否使能 IGMP-Snooping、以及是否作为 IGMP 的 Querier。

5.5.2 IGMP-Snooping VLAN 列表

在导航栏依次点击“二层配置”、“IGMP Snooping”、“IGMP Snooping VLAN 列表”，进入 IGMP-Snooping VLAN 页面。

点击新建，可以新建 IGMP-Snooping Vlan 配置，通过 Web 每个 IGMP-Snooping VLAN 最多可以配置 8 个物理端口。点击删除可以删除选中的 IGMP-Snooping Vlan，点击修改可以对 IGMP-Snooping Vlan 的成员端口，运行状态和 Immediate-leave 进行修改。

当新建 IGMP-Snooping Vlan 时，VLAN ID 可修改，当修改 IGMP-Snooping Vlan 时，VLAN ID 不可修改。

用户可以通过“>>”和“<<”按钮来删除路由端口和添加路由端口。

5.5.3 静态组播地址

在页面上方点击“静态组播地址”选项卡，进入静态组播地址配置页面。

该页面显示了 IGMP-Snooping 配置的，当前网络中存在的静态组播组，以及每个组中成员所在的端口集合。

点击“刷新”按钮刷新列表的内容。

5.5.4 组播成员列表

在页面上方点击“组播成员列表”选项卡，进入组播成员列表页面。

该页面显示了 IGMP-Snooping 统计的，当前网络中存在的组播组，以及每个组中成员所在的端口集合。

点击“刷新”按钮刷新列表的内容。

请注意：
缺省配置下，组播成员列表最多显示的条目数为 15。可以通过“**ip http web igmp-groups**”全局配置命令修改此限制，该命令需要通过 Console 口或 Telnet 登录设备后配置。

5.6 静态ARP配置

在导航栏依次点击“二层配置”、“静态 ARP 配置”，进入静态 ARP 配置页面。

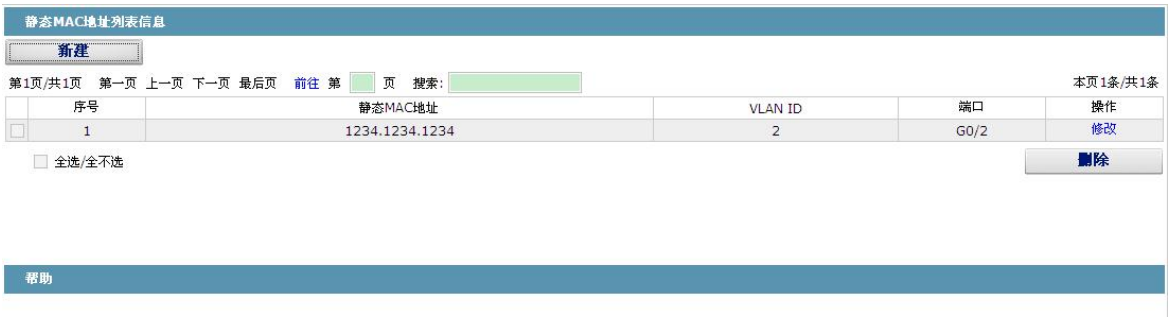
点击新建可以添加 ARP 表项，在配置 ARP 表项时，需要指定 VLAN 接口。

点击修改可以修改当前条目的 ARP 表项。

点击删除可以删除选中的 ARP 表项。

5.7 静态MAC地址配置

在导航栏依次点击“二层配置”、“静态 MAC 地址配置”，进入静态 MAC 地址配置页面。



点击新建可以为指定端口配置静态 MAC 地址和 VLAN，单播 MAC 地址只能配置一个端口，多播 MAC 地址可以配置多个端口。

点击修改可以对已配置的静态 MAC 地址做修改。

点击删除可以删除选中的静态 MAC 地址表项。

图 20：静态 MAC 地址配置

5.8 DDM配置

在导航栏依次点击“二层配置”、“DDM 配置”，进入 DDM 配置页面。

5.9 链路聚合配置

5.9.1 端口聚合配置

在导航栏依次点击“二层配置”、“链路聚合配置”，进入聚合配置页面。

点击新建，可以新建聚合组，通过 Web 可以最多配置 32 个聚合组，每个组最多可以配置 8 个物理端口加入聚合。点击删除可以删除选中的聚合组，点击修改可以对聚合端口的成员端口和聚合模式进行修改。

当新建聚合组时，聚合组可选，当修改聚合组时，聚合组不可选。

当聚合端口存在成员端口时，用户可以选择聚合模式 Static，LACP Active 和 LACP Passive。

用户可以通过“>>”和“<<”按钮来删除聚合组成员端口和添加聚合组成员端口。

5.9.2 链路聚合负载均衡配置

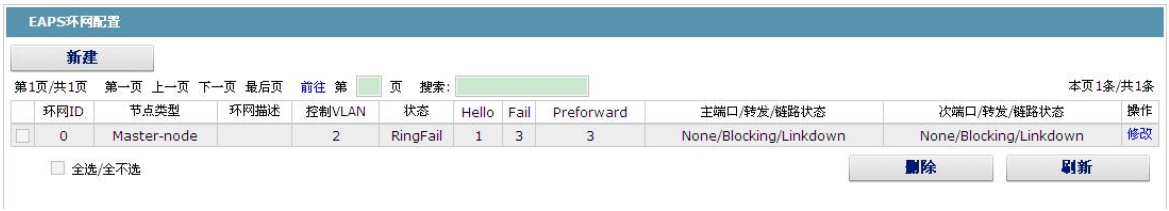
链路聚合负载均衡有些机型支持基于聚合组的负载均衡模式配置，有的不支持，但可以在全局配置模式下设置。

用户可以为不同的聚合组设置不同的聚合模式。

5.10 环网保护配置

5.10.1 EAPS 环网列表

在导航栏依次点击“二层配置”、“环网保护配置”，进入 EAPS 环网列表页面。



列表中显示了当前已经配置的 EAPS 环网，包括环网状态、端口的转发状态和链路状态。

点击“新建”创建新的 EAPS 环网。

点击表项右侧的“修改”选项，对环网的时间参数进行配置。

请注意：
1、系统支持的 EAPS 环网数目为 8 个。
2、一个环网已经配置之后，其端口、节点类型和控制 Vlan 将无法修改。如果需要调整环网的端口、类型或控制 Vlan，请将环网删除后重新建立。

5.10.2 EAPS 环网配置

通过点击 EAPS 环网列表的“新建”按钮，或环网条目右侧的“修改”选项，进入 EAPS 环网配置页面。

请注意：
如果是对环网进行修改，则页面上节点类型、控制 VLAN、主端口和次端口将不可修改。

在“环网 ID”右侧的下拉框中选择一个作为环网的标识。注意同一环网上所有设备的环网 ID 必须一致。

“节点类型”右侧的下拉框用于选择节点的类型。请注意，一个环网上只能够配置一个主节点。

在“控制 VLAN”右侧的文本框中输入 1-4094 范围内的一个值作为控制 VLAN 号。在新建环网时，控制 VLAN 也会被自动创建。请注意，如果指定控制 VLAN 为 1，且用于管理设备的 VLAN 也是 1，会造成设备无法访问。此外，请避免输入的 VLAN 与其它环网的控制 VLAN 冲突。

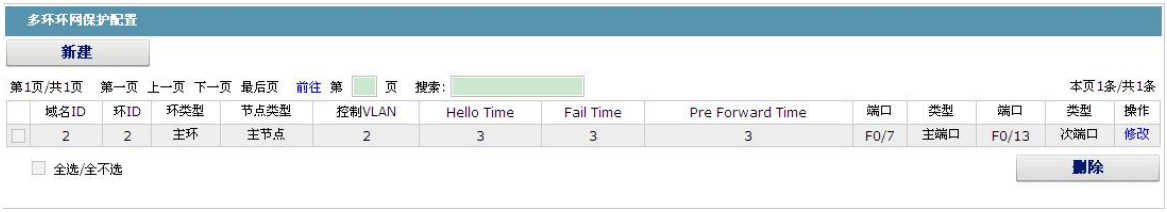
在“主端口”和“次端口”右侧的下拉框中各选择一个端口作为环网端口。若选择的节点类型为传输节点（Transit-Node），则两个端口都会被自动设置为传输端口。

点击“应用”以完成 EAPS 环网配置，“重填”将表单恢复为初始状态，“返回”返回 EAPS 环网列表页面。

5.11 MEAPS多环环网保护协议配置

5.11.1 MEAPS 环网列表

在导航栏依次点击“二层配置”、“多环环网保护配置”，进入 MEAPS 环网列表页面。



列表中显示了当前已经配置的 MEAPS 环网，包括域名 ID，环 ID，环类型，节点类型，控制 VLAN，Hello Time，Fail Time，Pre Forward Time 以及环上的主端口和次端口。

点击“新建”创建新的 MEAPS 环网。

点击表项右侧的“修改”选项，对环网的时间参数以及主次端口进行配置。

请注意：
1、系统支持的 MEAPS 域数目为 4 个（0-3）。
2、一个域内支持的环的个数是 8 个（0-7）
2、一个 MEAPS 已经配置之后，其域名 ID、环 ID、环类型、节点类型和控制 Vlan 将无法修改。如果需要调整，请将环网删除后重新建立。

5.11.2 MEAPS 环网配置

在 MEAPS 环网列表页面点击“新建”按钮，或者点击条目右侧的“修改”选项，进入 MEAPS 配置页面。

请注意：
如果是对已经存在的 MEAPS 环网进行配置，页面中的域名 ID、环 ID、环类型、节点类型和控制 Vlan 不可修改。

主环中只能配置主节点和传输节点。

子环中可以配置主节点、传输节点、边缘节点和辅助边缘节点。

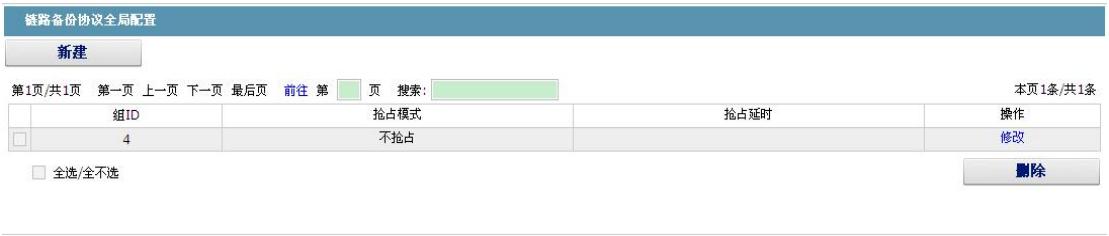
主节点和传输节点只能存在于一个环中，边缘节点和辅助边缘节点可以同时存在于多个环中。

在“主端口”和“次端口”右侧的下拉框中各选择一个端口作为环网端口，也可以选择 None。

5.12 链路备份协议配置

5.12.1 链路备份协议全局配置

在导航栏依次点击“二层配置”、“链路备份协议配置”，然后点击页面上方的“链路备份协议全局配置” 选项卡，进入链路备份协议全局配置页面。



页面中列出了当前已配置的链路备份组，包括其抢占模式和抢占延时。

点击“新建”创建新的链路备份组。

点击条目右侧的“修改”选项，对链路备份组的抢占模式和抢占延时参数进行配置。

请注意：
1、系统支持的链路备份组数目为 8 个。
2、链路备份组的抢占模式决定了主端口和备份端口选择转发报文的策略。

5.12.2 链路备份协议端口配置

在导航栏依次点击“二层配置”、“链路备份协议配置”，然后点击页面上方的“链路备份协议端口配置” 选项卡，进入链路备份协议端口配置页面。

页面中列出了当前已加入备份链路组的成员端口，以及成员端口的端口属性，MMU 属性和负载均衡 vlan，MMU 发送方可以通过发送 MMU 报文给接收方，来触发接收方快速更新 mac 地址表。

点击条目右侧的“修改”选项，对端口进行链路备份协议配置。

对于已经配置了主端口的链路备份组，不能再配置其他端口作为该链路备份组的主端口。同样，对于已经配置了备份端口的链路备份组，不能再配置其他端口作为该链路备份组的备份端口。

5.13 DHCP Snooping配置

5.13.1 DHCP Snooping 全局属性配置

在导航栏依次点击“二层配置”、“DHCP Snooping 配置”，进入 DHCP Snooping 全局配置页面。

开启全局 DHCP Snooping 协议，交换机侦听所有 DHCP 报文，形成相应的绑定关系。如果客户端是在配置该命令之前通过此交换机获取地址，则交换机不能添加相应的绑定关系。

当交换机配置保存重新启动之后，原来配置的接口绑定关系会丢失，这时，接口上没有绑定关系，启动IP 源地址监测功能后，交换机拒绝转发所有IP报文。配置了接口绑定关系备份的TFTP服务器之后，绑定关系会通过TFTP协议备份到服务器，在交换机重启后，自动到TFTP服务器下载绑定表，以保证网络正常工作。

配置备份接口绑定关系时，在TFTP服务器上保存的文件名。这样，不同的交换机可以将自己的接口绑定关系表备份到同一台TFTP服务器。

接口的MAC地址和IP地址的绑定关系表是动态变化的，需要在一定的时间间隔之后，检查绑定是否有更新，如果有更新（添加或者删除绑定条目）则进行重新备份。默认时间间隔为30分钟。

5.13.2 DHCP Snooping VLAN 属性配置

在导航栏依次点击“二层配置”、“DHCP Snooping 配置”，“DHCP Snooping VLAN 列表”，进入 DHCP Snooping VLAN 配置页面。

在VLAN上启动DHCP Snooping功能，则对属于整个VLAN的所有非信任物理端口收到的DHCP报文进行合法化检查。对于VLAN内的非信任物理端口收到的DHCP 响应报文将丢弃，防止用户非法伪造或者误配的DHCP服务器提供地址分配；对于非信任端口的DHCP 请求报文，如果报文发送MAC地址和报文内的硬件地址字段不匹配，认为是用户故意伪造的用于DHCP DOS（拒绝服务）的攻击报文，交换机也将丢弃。

在属于某个VLAN的所有物理端口进行ARP动态监测，如果该接口收到的ARP报文的源MAC和源IP地址不满足接口上配置的MAC和IP地址绑定关系，则拒绝处理该报文。接口上配置的绑定关系可以是DHCP动态绑定的，也可以是手工配置的。如果物理接口上没有配置任何MAC和IP地址绑定，则交换机拒绝转发所有ARP报文。

启动IP源地址监测的VLAN，属于该VLAN的所有物理端口收到的IP报文的源MAC和源IP地址不满足接口上配置的MAC和IP地址绑定关系，则该报文被拒绝处理。接口上配置的绑定关系可以是DHCP动态绑定的，也可以是手工配置的。如果此物理接口上没有配置任何MAC和IP地址绑定，则交换机拒绝转发所有该接口收到的IP报文。

5.13.3 DHCP Snooping 端口属性配置

在导航栏依次点击“二层配置”、“DHCP Snooping 配置”、 “DHCP Snooping 端口配置”进入 DHCP Snooping 端口属性配置页面。

配置接口为DHCP信任接口，则该接口收到的DHCP报文不进行检查。

对于ARP监测信任接口，不启动ARP监测功能。接口默认为非信任接口。

对于IP源地址信任接口，不启动源地址检查功能。

5.13.4 DHCP Snooping 手工配置接口绑定

在导航栏依次点击“二层配置”、“DHCP Snooping 配置”、 “DHCP Snooping 手工配置接口绑定列表”进入 DHCP Snooping 手工配置接口绑定列表页面。

对于不使用DHCP获取地址的主机，在交换机接口上可以手工配置添加绑定条目以使主机正常访问网络。使用该命令的no命令可以删除绑定条目。

手工配置的绑定条目比动态配置的绑定条目优先级要高，如果配置条目的MAC地址与动态配置条目的MAC地址相同，则手工配置的更新动态配置条目。接口绑定条目以MAC地址为唯一索引。

点击新建，用户可以创建 DHCP Snooping 手工配置接口绑定条目。

5.14 MTU配置

在导航栏依次点击“二层配置”、“MTU 配置”，进入 MTU 配置页面。

用户可以在指定范围内，设定最大传输单元 MTU 大小。

5.15 PDP配置

5.15.1 PDP 全局属性配置

在导航栏依次点击“二层配置”、“PDP 配置”，进入 PDP 全局属性配置页面。

用户可以选择开启 PDP 协议，或者关闭该协议。当用户选择关闭 PDP 协议时，用户将无法对设备端口进行 PDP 协议配置。

HoldTime 表示如果没有接收到其他 PDP 分组，路由器在丢弃接收到的信息之前将要保存的时间量。

5.15.2 PDP 端口属性配置

在导航栏依次点击“二层配置”、“PDP 配置”、 “PDP 端口配置”进入 PDP 端口属性配置页面。

在全局开启 PDP 协议的前提下，PDP 端口配置可以对端口进行启动或关闭 PDP 协议的操作。

第 6 章　三层配置

6.1　VLAN接口配置

在导航栏依次点击“三层配置”、“VLAN 接口及 IP 地址配置”，进入 VLAN 接口配置页面。

点击“新建”，可以新增一个 VLAN 接口配置。点击“删除”，可以删除该 VLAN 接口。点击“修改”，可以进入到相应的 VLAN 接口配置页面，进行相应的设置。

点击“新建”，VLAN 接口名可以修改；点击“修改”，VLAN 接口名不可修改。

请注意：
配置 VLAN 接口辅助 IP 之前，必须先配置主 IP。

6.2 静态路由配置

在导航栏依次点击“三层配置”、“静态路由配置”，进入静态路由配置页面。

点击新建可以添加静态路由表项。

点击修改可以修改当前条目的静态路由表项。

点击删除可以删除选中的静态路由表项。

6.3 OSPF路由配置

6.3.1 OSPF 进程配置

在导航栏依次点击“三层配置”、“OSPF 路由配置”，进入 OSPF 进程页面。

在配置 OSPF 路由条目之前，必须先创建 OSPF 进程，否则无法配置。在 OSPF 进程页面，可以新建 OSPF 进程，也可以删除 OSPF 进程。

点击新建即可进入创建 OSPF 进程页面。

6.3.2 OSPF 路由条目配置

在导航栏依次点击“三层配置”、“OSPF 路由配置”，选择 OSPF 路由条目 tab 页，进入 OSPF 路由条目页面。

输入已创建的 OSPF 进程号，点击应用，即可进入指定的的 OSPF 进程路由条目页面。

点击新建，即可新建指定进程的 OSPF 路由条目。

其中，Area 支持整数和 IP 地址形式。

6.4 IGMP代理配置

6.4.1 IGMP 代理的开启和关闭

在导航栏依次点击“三层配置”、“IGMP 代理”，选择开启 IGMP 代理 tab 页，进入开启 IGMP 代理页面。

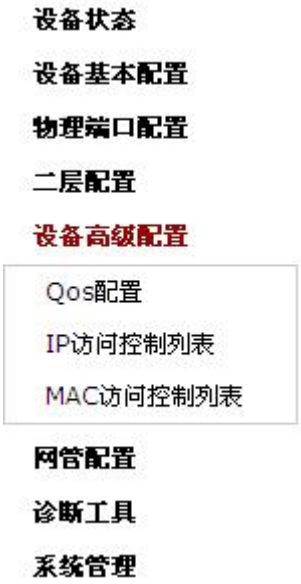
开启或者关闭 IGMP 代理之前，必须先开启 IGMP Snooping 功能，否则，按钮是灰显的，无法配置。可以点击二层配置，IGMP Snooping 进行配置。

6.4.2 配置 IGMP 代理

在导航栏依次点击“三层配置”、“IGMP 代理”，选择配置 IGMP 代理 tab 页，进入 IGMP 代理列表页面。

点击新建，即可新建 IGMP 代理条目。

第 7 章　设备高级配置



7.1　QoS配置

7.1.1　QoS 接口配置

在导航栏依次点击“设备高级配置”、“QoS 配置”，然后点击页面上方的“QoS 接口配置”选项卡，进入接口的 QoS 参数配置页面。

通过端口名称右侧的下拉框设置端口的 CoS 值。端口缺省的 CoS 均为 0，表示最低优先级。CoS7 为最高优先级。

7.1.2　QoS 全局配置

在导航栏依次点击“设备高级配置”、“QoS 配置”，然后点击页面上方的“QoS 全局配置”选项卡，进入接口的 QoS 参数配置页面。

在 WRR 优先级队列调度模式下，用户可以设置 QoS 队列的权重比，总共有 8 个队列，队列 1 为最低优先级，队列 8 为最高优先级。

7.2 MAC访问控制列表

7.2.1 MAC 访问控制列表名配置

在导航栏依次点击“设备高级配置”、“MAC 访问控制列表”，然后点击页面上方的“MAC 访问控制列表配置”，进入 MAC 访问控制列表配置页面。

点击“新建”，可以新增一个 MAC 访问控制列表名。点击“删除”，可以删除该访问控制列表。

7.2.2 MAC 访问控制列表规则配置

点击“修改”，可以进入到相应的 MAC 访问控制列表，进行相应的规则设置。

点击“新建”，可以新增一个 MAC 访问控制列表规则。点击“删除”，可以删除该访问控制列表规则。点击“修改”，可以进入到相应的 MAC 访问控制列表规则，进行相应的修改。

7.2.3 MAC 访问控制列表应用

在导航栏依次点击“设备高级配置”、“MAC 访问控制列表”，然后点击页面上方的“MAC 访问控制列表应用”，进入 MAC 访问控制列表应用页面。

7.3 IP访问控制列表

7.3.1 IP 访问控制列表名配置

在导航栏依次点击“设备高级配置”、“IP 访问控制列表”，然后点击页面上方的“IP 访问控制列表配置”，进入 IP 访问控制列表配置页面。

点击“新建”，可以新增一个 IP 访问控制列表名。点击“删除”，可以删除该访问控制列表。

点击“修改”，可以进入到相应的 IP 访问控制列表，进行相应的规则设置。

7.3.2 IP 访问控制列表规则配置

- 访问控制列表属性为“standard”

点击“新建”，可以新增一个 IP 访问控制列表规则。点击“删除”，可以删除该访问控制列表规则。点击“修改”，可以进入到相应的 IP 访问控制列表规则，进行相应的修改。

- 访问控制列表属性为“extended”

点击“新建”，可以新增一个 IP 访问控制列表规则。点击“删除”，可以删除该访问控制列表规则。点击“修改”，可以进入到相应的 IP 访问控制列表规则，进行相应的修改。

7.3.3 IP 访问控制列表应用

在导航栏依次点击“设备高级配置”、“IP 访问控制列表”，然后点击页面上方的“IP 访问控制列表应用”，进入 IP 访问控制列表应用页面。

第 8 章　网管配置

8.1　SNMP配置

在导航栏依次点击“网管配置”、“SNMP 配置”，进入 SNMP Community 管理和 SNMP Host 管理页面。

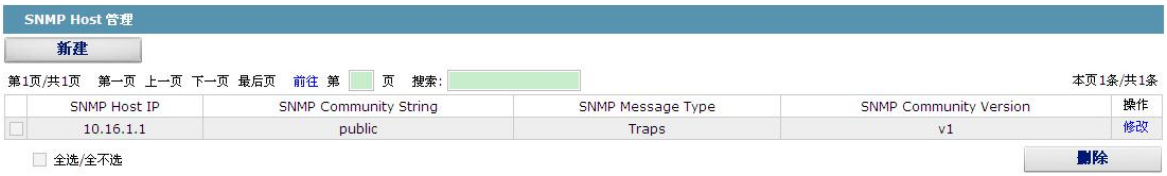
8.1.1　SNMP Community 管理

通过 SNMP Community 管理页面，用户可以了解 SNMP Community 的相关配置信息。

用户可以新建、修改、删除 SNMP Community 信息，点击新建或者修改，可以切换到 SNMP Community 相关信息的配置页面。

在 SNMP Community 的配置页面，用户可以输入 SNMP Community 名，可以选择 SNMP Community 属性，属性包括只读和读写。

8.1.2 SNMP Host 管理



通过 SNMP Host 管理页面，用户可以了解 SNMP Host 的相关配置信息。

用户可以新建、修改、删除 SNMP Host 信息，点击新建或者修改，可以切换到 SNMP Host 相关信息的配置页面。

在 SNMP Host 的配置页面，用户可以输入 SNMP Host IP，SNMP Community，SNMP Message Type 和 SNMP Community Version，其中，SNMP Message Type 包括 Traps 和 Informs，对于 v1 版本，SNMP Message Type 不支持 Informs 类型。

8.2 RMON

8.2.1 RMON 统计信息配置

在导航栏依次点击“网管配置”、“RMON” 、“ RMON 统计”、“新建”，进入 RMON 统计信息设置界面。

设置一个物理端口，作为监控数据信息的接收端。

索引用来标识一个具体应用接口，当索引与之前设置的应用接口的索引相同时，先前的配置将被取代。

目前监控统计信息能够通过 show rmon statistics 在命令行获得，web 暂不支持。

8.2.2 RMON 历史信息配置

在导航栏依次点击“网管配置”、“RMON”、“ RMON 历史”、“新建”，进入 RMON 历史信息设置界面。

设置一个物理端口，作为监控数据信息的接收端。

索引用来标识一个具体应用接口，当索引与之前设置的应用接口的索引相同时，先前的配置将被取代。

采样数目表示需要保留的表项条目，默认为 50 条。

采样间隔为每两次获取统计数据的间隔时间，默认值为 1800 秒。

目前监控历史信息能够通过 show rmon history 在命令行获得，web 暂不支持。

8.2.3 RMON 告警信息配置

在导航栏依次点击“网管配置”、“RMON”、“ RMON 告警”、“新建”，进入 RMON 告警信息设置界面。

索引用来标识一个具体告警配置信息，当索引与之前设置的应用的索引相同时，先前的配置将被取代；

MIB 节点与 OID 所对应；

报警类型使用 absolute 来直接监测 MIB 对象的取值；报警类型使用 delta 来监测两次取样之间 MIB 对象值的变化。

当监控的 MIB 对象到达或超过上升阈值时，将触发上升事件索引所对应的事件；

当监控的 MIB 对象到达或超过下降阈值时，将触发下降事件索引所对应的事件；

8.2.4 RMON 事件配置

在导航栏依次点击“网管配置”、“RMON”、“ RMON 事件”、“新建”，进入 RMON 事件设置界面。

索引与 RMON 告警信息配置中所设置的上升事件索引和下降事件索引相对应，即当监控的 MIB 对象超过阈值时所触发的事件；

拥有者用来描述该事件的一些描述性信息；

启用 log 表示该事件被引发时在 log 表中增加一条信息；

启用 trap 表示该事件被引发时产生一条 trap。

第 9 章　诊断工具

9.1　Ping

9.1.1　Ping

在导航栏依次点击“诊断工具”、“Ping”，便可进入 Ping 页面。

Ping 用于测试交换机与其它设备是否连通。

如果需要进行 Ping 测试，请在“目的地址”右侧的文本框中输入一个 IP 地址，比如，您计算机的 IP 地址，然后点击“PING”按钮。如果交换机与您输入的地址是连通的，设备可以很快返回测试结果；如果无法连通，设备返回结果的时间会稍长。

“源 IP 地址”用于设置设备发送的 Ping 报文中携带的源 IP 地址。

“PING 包大小”用于设置设备发送的 Ping 报文的长度。

第 10 章　系统管理

10.1　用户管理

10.1.1　用户列表

在导航栏依次点击“系统管理”、“用户管理”，进入用户列表页面。

点击“新建”按钮创建新的用户。

点击用户列表项右侧的“修改“选项，对用户的权限和登录密码进行修改。

请注意：

1、请确保系统中至少存在一个“系统管理员”权限的用户，以确保能够通过 Web 管理设备。
2、“受限用户”权限的用户，只能查看设备状态，不能进行配置修改。

10.1.2 创建新用户

在用户列表页面点击“新建”按钮，进入用户创建页面。

在“用户名”后的文本框中输入新用户的名称，请注意用户只能为字母、数字和除?\"&#和空格以外的字符。

在“密码”后的文本框中输入用户登录设备的密码，并在“确认密码”后的文本框中再次输入密码以确认。

10.1.3 用户组管理

点击用户组管理 Tab 页，进入用户组管理页面。

点击“新建”按钮创建新的用户组。

点击“删除”按钮删除用户组。

新建的用户组名必须是没有创建过的。而密码规则名，认证规则名和授权规则名必须是已经创建的，否则，新建用户组无法成功。关于密码规则，认证规则和授权规则的配置在其他 3 个 tab 页操作。

10.1.4 密码规则管理

点击密码规则管理 Tab 页，进入密码规则管理页面。

点击“新建”按钮创建新的密码规则。

点击“删除”按钮删除密码规则。

在密码规则中，设置一些密码的规则，其中包括密码是否可以与用户名相同，是否必须包含数字，是否必须包含小写字母，是否必须包含大写字母，是否必须包含特殊字符，最小长度是多少，以及有效期是多少。

当规则创建以后，将其运用于用户管理，当设置的密码不满足密码规则时，用户状态为用户密码无效，而只有在设置的密码满足密码规则时，用户状态才会是用户正常使用中。

10.1.5 认证规则管理

点击认证规则管理 Tab 页，进入认证规则管理页面。

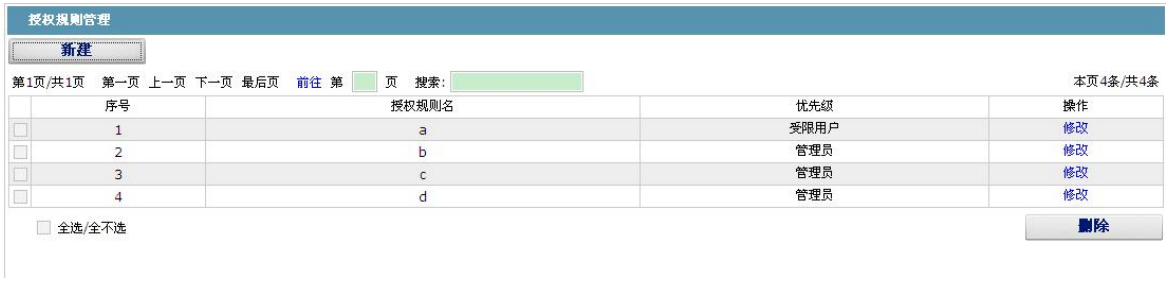
点击“新建”按钮创建新的认证规则。

点击“删除”按钮删除认证规则。

其中，最大重试次数和重试周期可以都配置，也可以都不配置，但必须同时配置或同时不配置。

10.1.6 授权规则管理

点击授权规则管理 Tab 页，进入授权规则管理页面。



点击“新建”按钮创建新的授权规则。

点击“删除”按钮删除授权规则。

用户运用不同的授权，其权限是管理员还是受限用户，就是由授权规则决定的，如果授权规则是管理员，那么运用该规则的用户就具有管理员权限，如果授权规则是受限用户，那么运用该规则的用户就是受限用户，受限用户对许多 web 操作都是无法进行的，他只具有查询的功能。

10.2 日志管理

在导航栏依次点击“系统管理”、“日志管理”，进入设备日志管理页面。

“启用日志服务器”，设备将把日志信息发送到指定的服务器，请输入服务器地址并选择发送到服务器的日志等级，“7-debugging”为最低等级的日志信息。

“启用日志缓冲区”，设备将把日志信息记录到内存中。可以通过 Console 口或 Telnet 登录设备，然后执行“show log”命令查看设备保存的日志。保存在内存中的日志信息将在设备重启后丢失。请输入用于保存日志的内存缓冲区大小，并选择缓存日志的等级。

10.3 配置文件管理

在导航栏依次点击“系统管理”、“配置导入导出”，便可进入配置文件管理页面。

10.3.1 导出配置

您可以将设备当前的配置文件导出，保存在计算机的磁盘或移动存储设备中作为备份。

如需导出配置文件，请点击“导出”按钮，然后在弹出的下载对话框中选择“保存”。

配置文件的缺省名称为“startup-config”，建议您将其修改为好记的名称。

10.3.2 导入配置

您可以将保存在计算机上的配置文件导入到设备，并替换当前正在使用的配置文件。比如，通过导入备份的配置文件，您可以将设备恢复到之前某一时刻的配置。

请注意：
1、请确保导入的配置文件具有合法的格式，不合法的配置文件可能导致设备无法正常启动。
2、如果导入过程出现错误，请稍候重试，或者点击页面顶部控制区的“全部保存”按钮，让设备使用当前的配置重新建立配置文件，以避免出现不完整的文件而导致设备不正常。
3、配置文件导入完成后，如果需要立即应用导入的配置，请直接重启设备，而**不要**点击“全部保存”。

10.4 设备软件管理

在导航栏依次点击“系统管理”、“软件升级”，进入设备软件管理页面。

10.4.1 备份系统软件

页面中会显示当前正在运行的软件版本。如需备份系统，请点击“备份系统软件”，然后浏览器会弹出文件下载对话框，请选择“保存”，将系统文件保存到您的计算机磁盘、移动存储设备或网络中的其它位置。

请注意：
系统文件的缺省名称为“Switch.bin”，建议在备份时将其修改为易于识别和查找的名称。

10.4.2 升级系统软件

请注意：
1、请确保您升级的系统文件与设备类型是匹配的，不匹配的系统文件会导致设备无法正常启动。
2、升级系统文件可能需要 1 至 2 分钟，点击“升级”按钮并确认之后，文件将被上传到设备，请耐心等候。
3、升级过程如果出现错误，请勿对设备执行重启或断电操作，否则可能造成设备无法启动。请稍候重新尝试升级。
4、升级完成之后，请保存配置之后重启设备，以运行新的系统。

升级系统软件通常用于解决已知的问题或者完善特定的功能，如果您的设备运行正常，则无需频繁升级系统软件。

如需升级系统，请先在“升级系统软件”右侧的文本框中输入新的系统文件的完整路径，或者点击“浏览”按钮，在您的计算机上选择新的系统文件，然后点击“升级”。

10.5 恢复出厂配置

在导航栏依次点击“系统管理”、“恢复出厂配置”，进入恢复出厂配置页面。

请注意：
1、恢复出厂配置，设备将使用出厂配置替换当前的配置文件，并在您重启设备之后生效。
2、在重启之前，设备仍然工作在当前的配置状态，此时如果点击顶部控制栏的“全部保存”按钮，设备会使用当前的配置再次覆盖配置文件。恢复出厂配置将不会生效。
3、设备重启完成，出厂配置生效后，设备的 Web 访问会自动启动，管理地址（Interface Vlan 1 的地址）为 192.168.0.1/255.255.255.0，登录用户名和密码均为“admin”。

如果需要恢复设备的出厂配置，请点击“恢复”按钮，并等待完成之后重启设备。

10.6 重新启动

在导航栏依次点击“系统管理”、“重新启动”，便可进入重启设备页面。

如需重启设备，请先确保对设备配置的修改已经保存，然后点击“重新启动设备”按钮。