WEB 管理手册

RG-S5750-S 系列交换机

RGOS 10.4(3b18)

文档版本号：V1.0

版权声明












免责声明

本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。锐捷网络保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。

本手册仅作为使用指导，锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前　言

版本说明

本手册对应的软件版本为：RGOS 10.4(3b18)

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷网络官方网站：http://www.ruijie.com.cn/
- 锐捷网络在线客服：http://webchat.ruijie.com.cn
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7×24 小时技术服务热线：4008-111-000
- 锐捷网络技术论坛：http://bbs.ruijie.com.cn/portal.php
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷网络技术支持与反馈信箱：4008111000@ruijie.com.cn

相关资料

手册名称	说明
产品 安装手册	本手册介绍了产品在功能和物理上的一些特性，提供了设备安装步骤、硬件故障排除、模块技术规格，以及电缆和连接器的规格和使用准则等。
产品 配置手册	本手册对产品支持的各网络协议及其实现原理进行了描述，并配有详细的配置实例。
产品 命令手册	本手册对产品支持的配置命令做了详细的描述。包括命令模式、参数说明和使用指南等，并配有具体的实例。

本书约定

1)　命令行格式约定

命令行格式意义如下：

粗体：命令行关键字（命令中保持不变必须照输的部分）采用加粗字体表示。

斜体：命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示

[ ] ：表示用[ ] 括起来的部分，在命令配置时是可选的。

{ x | y | ... }：表示从两个或多个选项中选取一个。

[x | y | ...]：表示从两个或多个选项中选取一个或者不选。

//：由双斜杠开始的行表示为注释行。

2) 各类标志

本书还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、警告、提醒操作中应注意的事项。

说明、提示、窍门、对操作内容的描述进行必要的补充。

对于产品的支持情况进行必要的补充。

3) 说明

- 本手册举例说明部分的端口类型同实际可能不符，实际操作中需要按照各产品所支持的端口类型进行配置。
- 本手册部分举例的显示信息中可能含有其它产品系列的内容（如产品型号、描述等），具体显示信息请以实际使用的设备信息为准。
- 本手册中涉及的路由器及路由器产品图标，代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

1 交换机 WEB 管理

1.1 WEB管理概述

WEB 管理通过使用浏览器如 IE 来管理网络设备，如交换机或路由器。

WEB 管理包括 WEB 服务器和 WEB 客户端两部分。WEB 服务器集成在设备上，用来接收和处理客户端发来的请求（读取 WEB 文件或执行命令请求），并把处理结果返回给客户端，WEB 客户端通常指网络浏览器，如 IE。

1.2 配置环境要求

1.2.1 客户端要求

- 网管使用 WEB 管理客户端的 WEB 浏览器登录到交换机 WEB 管理界面对交换机进行管理。客户端通常是指 PC，也可能是一些其它的移动终端设备，如笔记本电脑、IPAD 等
- 浏览器：支持 IE6.0、IE7.0、IE8.0 以及部分基于 IE 核心的浏览器，如傲游 maxthon 等。使用其它浏览器登录 WEB 管理时，可能出现乱码或格式错误等异常
- 分辨率：建议分辨率设置为 1024*768、1280*1024 及 1440*960，在其它分辨率下，页面字体和格式可能出现不对齐、不够美观等异常

1.2.2 服务器要求

- 交换机需要启动 WEB 服务
- 交换机需要配置 WEB 管理登录认证信息
- 交换机需要配置管理 IP 地址

1.3 启动WEB服务

WEB 服务缺省是关闭的，如果要开启 WEB 服务，详细配置过程请参考本文“WEB 管理典型配置举例”小节。

如果 WEB 配置用 Enable 方法进行认证，则认证时不要输入用户名直接输入 Enable 密码进行认证。

1.4 登陆WEB管理平台

缺省管理 IP 未配置，需要用户先配置好管理 IP 地址才可以登录 WEB 管理平台。

在浏览器地址栏中输入设备的管理 IP 地址，如：http://192.168.1.200,按回车后将进入如下面页：

图 1-1 初始页面

选择好语言类型后点击“登录”按钮，这时会弹出认证对话框，请在此对话框中输入用户名、密码。

图 1-2 登录认证对话框

认证成功后将进入 WEB 管理主页面，如下图：

图 1-3 WEB 管理平台主页面

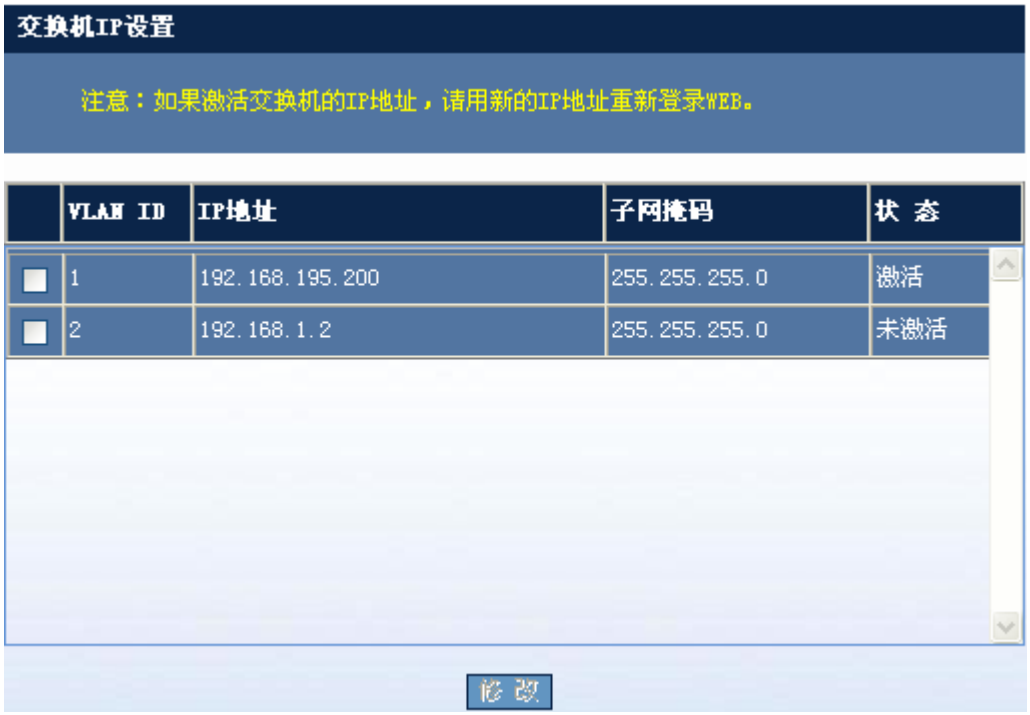
1.5 系统管理

1.5.1 交换机IP设置

通过菜单“交换机 IP 设置”使用该功能。

交换机 IP 设置页面：

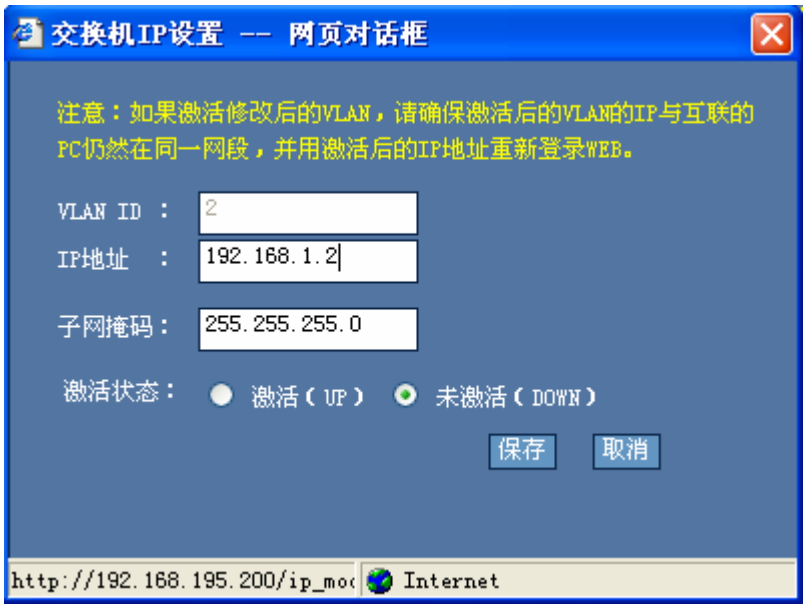
图 1-4 交换机 IP 设置



配置说明：

修改：如果要修改某个交换机 ip，请选中所对应的复选框，按“修改”按钮后，将弹出如下配置页面：

图 1-5 交换机 IP 修改



用户可以对 IP 地址，子网掩码等参数进行修改，修改完后请按“保存”按钮使配置生效。

1.5.2 VLAN管理

通过菜单项“VLAN 管理”使用该功能。

VLAN 管理页面设置页面：

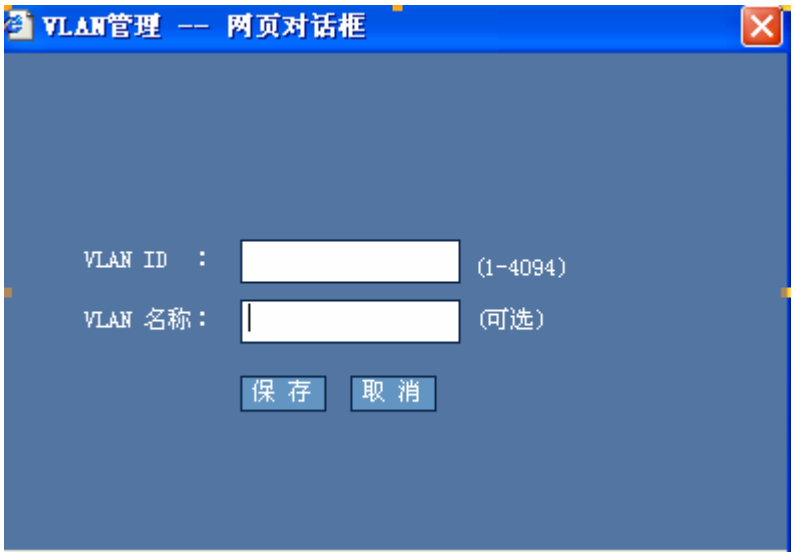
图 1-6 VLAN 管理

VLAN 管理页面

配置说明：进入该页面后，首先显示当前系统的 VLAN 信息。用户可以新建、删除、修改 VLAN，但默认 VLAN 不能被删除。

新建：点击“新建”按钮后，将弹出如下配置页面：

图 1-7 新建 VLAN

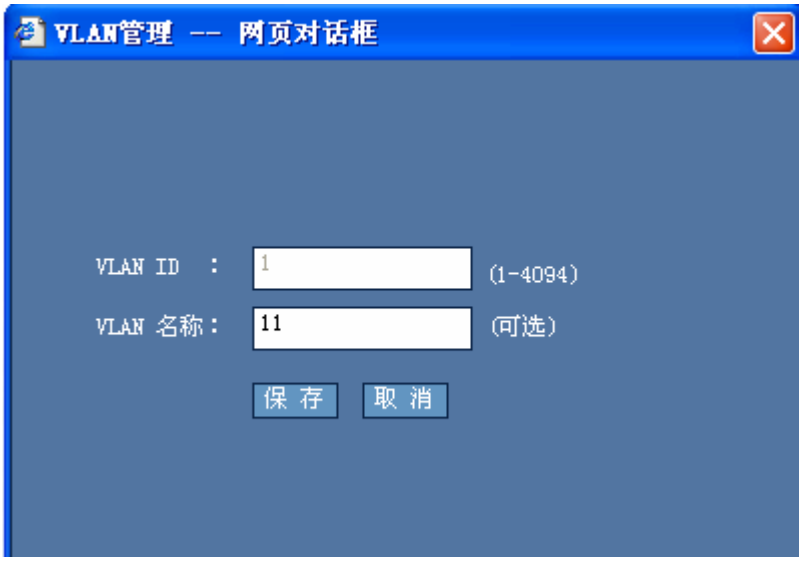


请输入 VLAN ID 和 VLAN 名称（可选）后按“保存”按钮使配置生效。配置成功后，新建的 VLAN 将显示在 VLAN 管理页面上。

删除：如果要删除指定的 VLAN，请选中相应的复选框后按“删除”按钮使配置生效。

修改：如果要修改已配置的 VLAN，只要选中所对应的复选框后按“修改”按钮，这时将弹出如下配置页面：

图 1-8 修改 VLAN



要修改的 VLAN 的信息将会显示在文本框中，这时对其修改后按“保存”按钮使配置生效。修改后的结果将显示在 VLAN 管理页面上。

指定 VLAN 页面

图 1-9 指定 VLAN

配置说明：

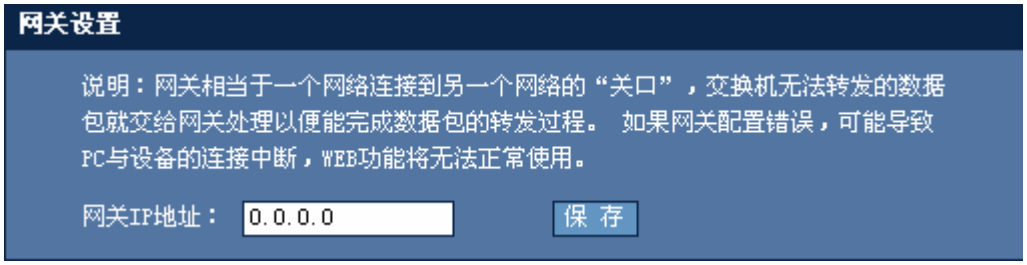
请指定所要设置的端口模式和 VLAN ID，当对所有端口都设置好后，请按“保存”按钮，使配置生效。

1.5.3 网关设置

通过菜单项“网关设置”使用该功能，该功能三层交换机不支持。

网关设置页面：

图 1-10 网关设置



配置说明：

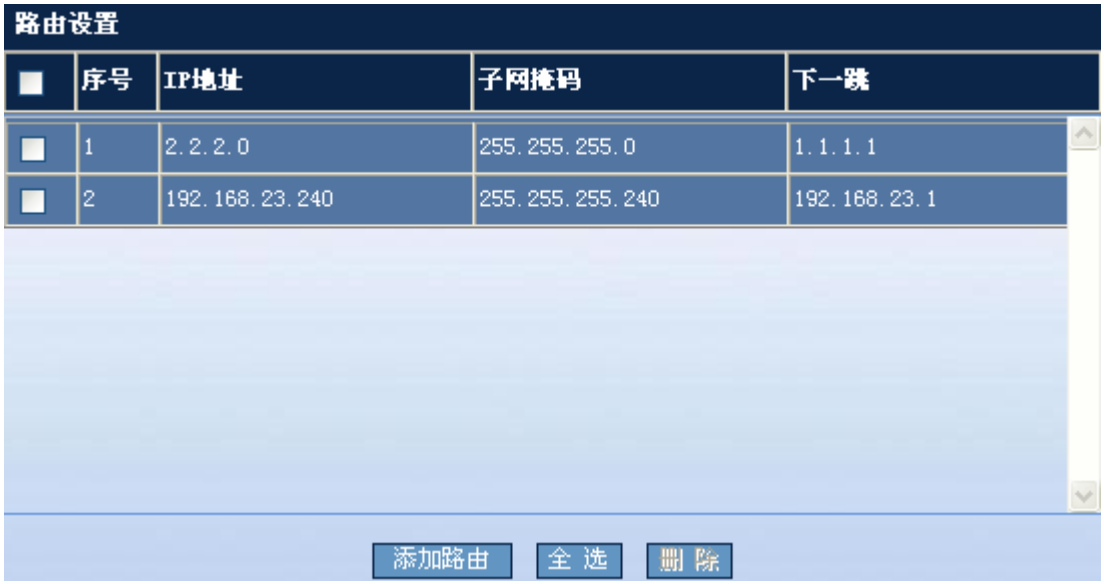
如果交换机已配置了网关，则打开该页面后，将会在文本框中显示已配置的网关地址，如果要设置新的网关 IP 地址，只要在文本框中输入新的网关 IP 地址后，按“保存”按钮使配置生效。

1.5.4 路由设置

通过菜单项“路由设置”使用该功能，该功能二层交换机不支持。

路由设置页面：

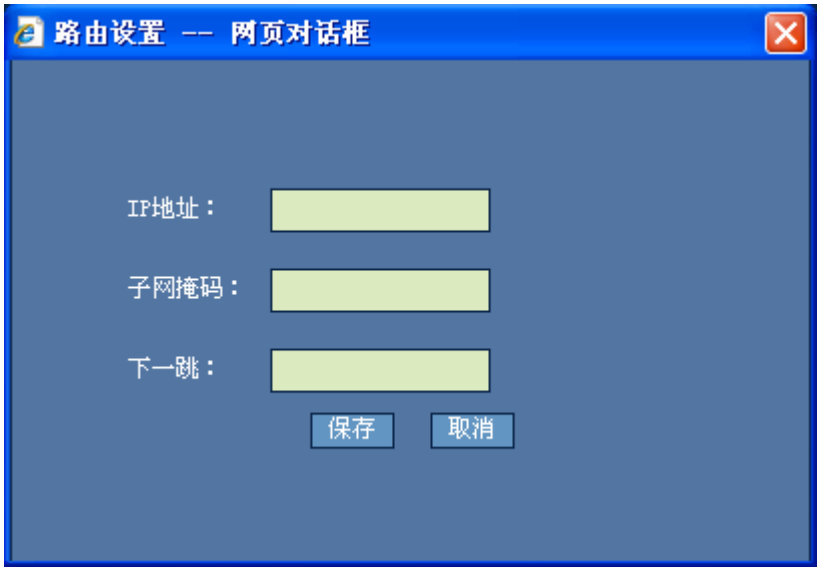
图 1-11 路由设置



配置说明：

添加路由：如果要添加路由，请点击“添加路由”按钮，将弹出如下配置页面：

图 1-12 添加路由



请输入 IP 地址、子网掩码和下一跳 后按“保存”按钮使配置生效。配置成功后，新加的用户将显示在路由设置页面上。

删除：请选中要删除的路由所对应的复选框，按“删除”按钮。这时所选中的路由项将被删除。

1.5.5 端口镜像

通过菜单项“端口镜像”使用该功能。

端口镜像设置页面：

图 1-13 端口镜像设置

配置说明：

请先选择监控端口，然后再选中要被监控的端口前面的复选框按“保存”按钮使配置生效，监控端口与被监控端口不能是同一个口。选择会话数序列号可以配置多个会话。按“删除端口监控”按钮，将删除端口监控配置。

1.5.6 端口限速

通过菜单项“端口限速”使用该功能。

端口限速设置的主要页面：

图 1-14 输入限速设置

输入限速

配置说明：

可以对端口输入速率以及瞬时速率进行限速。请在要限速的端口相应文本框中输入限速值，一次可以对多个端口进行设置，其中瞬时速率大小只能为 2 的 n 次方，设置好端口限速值后按“保存”按钮使配置生效。不限速的端口请保持相应的文本框为空。如果要取消所有端口的限速设置，请按“取消全部限速”按钮使配置生效。

输出限速

图 1-15 输出限速设置

配置说明：

同理可以对端口输出速率以及瞬时速率进行限速。设置好端口限速值后按“保存”按钮使配置生效。不限速的端口请保持相应的文本框为空。如果要取消所有端口的限速设置，请按“取消全部限速”按钮使配置生效。

1.5.7 聚合端口

通过菜单项“聚合端口”使用该功能。

聚合端口设置页面：

图 1-16 聚合端口设置

配置说明：

- 配置流量平衡算法

如果要配置流量平衡算法，请选择对应的算法选项后按“保存”按钮使配置生效。

- 配置聚合端口

如果要新建一个聚合端口，请按“新建”按钮，将弹出如下界面：

图 1-17 新建聚合端口

此时，请选择成员端口并指定聚合端口号后按“保存”按钮使配置生效，如果某个成员端口已是其它聚合端口成员，则该成员端口前的复选框将不能被选中。

- 删除聚合端口

如果要删除聚合端口，请选中相应聚合端口前面的复选框后，按“删除”按钮使配置生效。

1.5.8 端口设置

通过菜单项“端口设置”使用该功能。

端口设置页面：

图 1-18 端口设置

配置说明：

请选择要配置的端口后对其进行设置，配置好参数后按“保存”按钮使配置生效。如果选择的参数设备不支持，对应的参数设置将不生效。

1.5.9 DHCP中继

通过菜单项“DHCP 中继”使用该功能。

DHCP 中继设置页面：

图 1-19 DHCP 中继

配置说明：

- 开启/关闭 DHCP 中继

要开/关闭 DHCP 中继功能，请选中相应的单选按钮后，按“保存”按钮使配置生效。

- DHCP 服务器设置

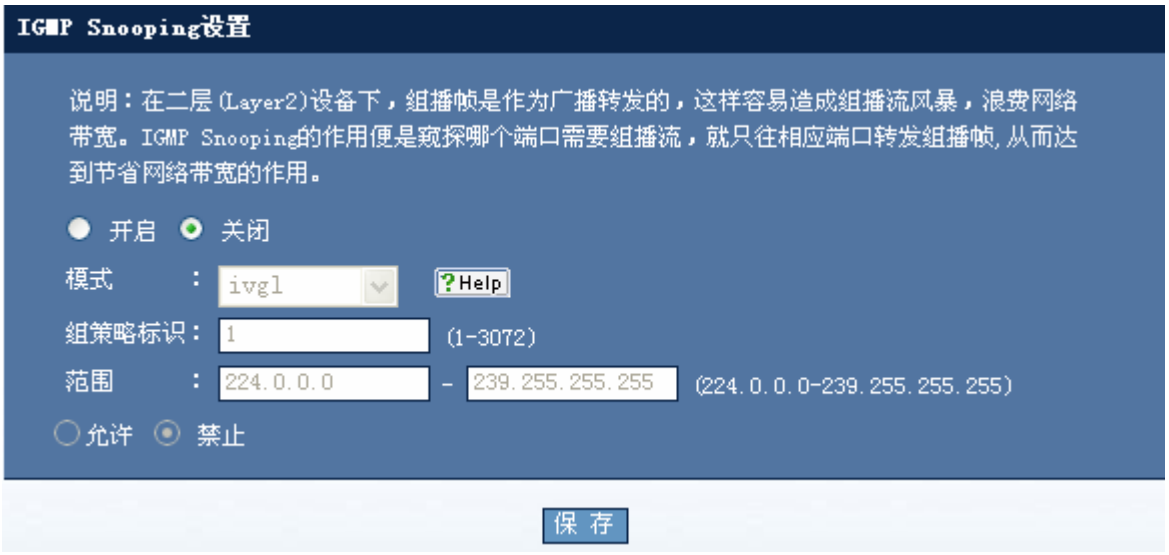
请设置好 DHCP 服务器地址后，按“保存”按钮使配置生效。配置成功后配置结果将显示在下表中。如果要删除 DHCP 服务器，请选中对应的复选框后按“删除”按钮使配置生效。

1.5.10 IGMP Snooping

通过菜单项“IGMP Snooping”使用该功能。

IGMP Snooping 设置页面：

图 1-20 IGMP Snooping 设置



配置说明：

如果要打开 IGMP Snooping 功能，请先选中“开启”单选按钮，这时模式下拉框变为可选状态，您可以从中选择 ivgl、svgl、ivgl-svgl 三中模式，如果选择了 svgl、ivgl-svgl 模式，才可以设置标识、IP 范围等参数。配置好参数后按“保存”按钮使配置生效。如果要关闭 IGMP Snooping 功能，请先选中“关闭”单选按钮按“保存”按钮使配置生效。

1.5.11 STP设置

通过菜单项“STP 设置”使用该功能。

STP 设置页面：

图 1-21 STP 设置

配置说明：

选中“开启 STP 功能”按“保存”按钮使配置生效。开启 STP 功能默认开启的是 MSTP，下面还可以对 MSTP 等进行配置保存 。端口设置，选择对应的端口设置为快速端口和开启 BPDU 过滤，点击“保存”按钮使配置生效。这里选中某端口，会动态显示该端口的配置情况。

配置了 MSTP 后，会将 MSTP 实例值和 VLAN 像是在实例-VLAN 对应表中，选中实例值前面的复选框后，按“删除”按钮，删除对应的实例-VLAN 配置。

1.5.12 SNMP管理

通过菜单项“SNMP 管理”使用该功能。

SNMP 管理页面：

图 1-22 SNMP 管理设置

配置说明：

如果开启 SNMP 管理功能，请选择“开启 SNMP”单选按钮，这时才可以设置团体名称、读写属性，设置好参数后，按“保存”按钮使配置生效。如果要关闭 SNMP 管理功能，请直接选择“关闭 SNMP”单选按钮后，按“保存”按钮使配置生效。如果要删除已配置的团体名称，请直接选中所要删除的表项所对应的复选框后按“删除”按钮使配置生效。

1.5.13 NFPP设置

通过菜单项“NFPP 设置”使用该功能。

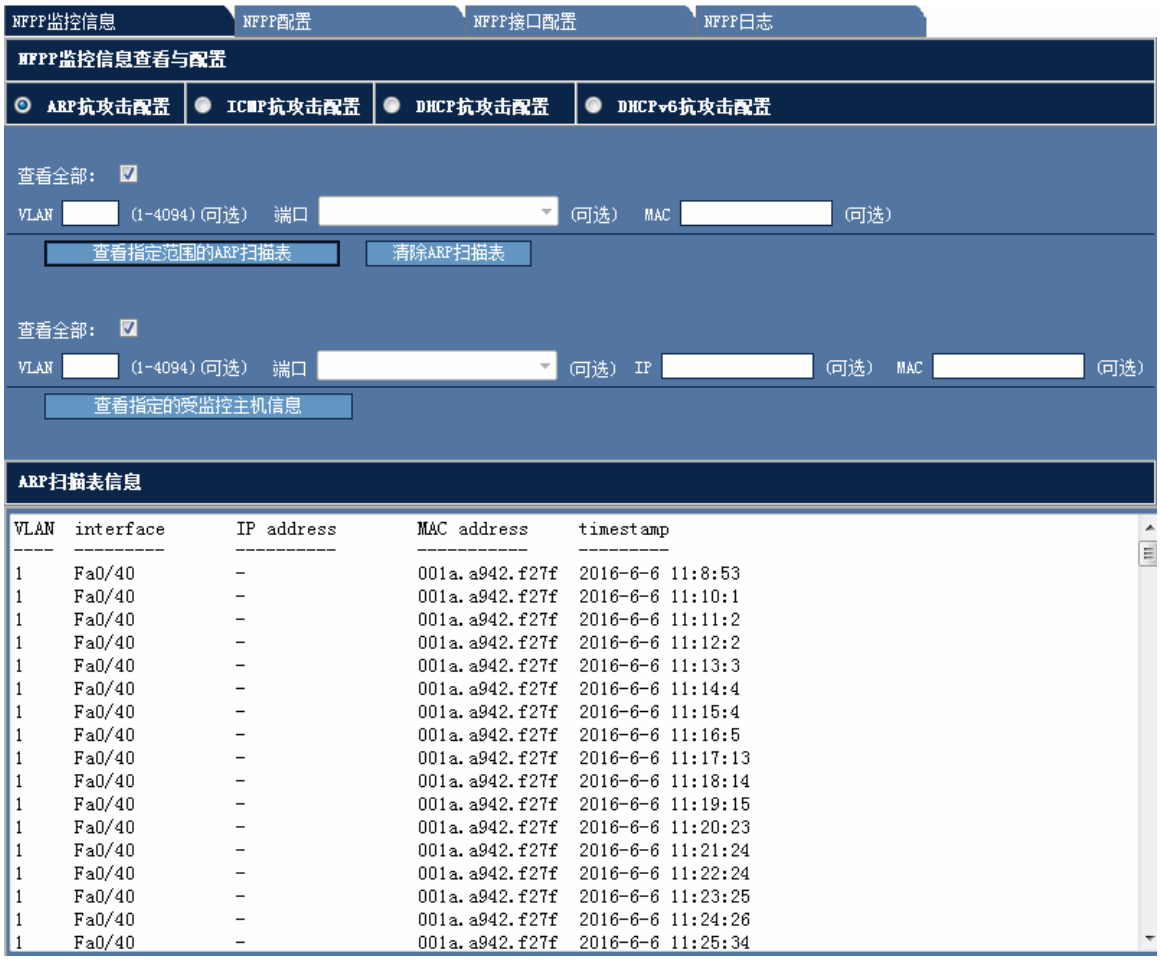
NFPP监控信息设置页面：

图 1-23 NFPP 监控信息

NFPP 监控信息

1) ARP 抗攻击配置

图 1-24 NFPP 监控信息—ARP 抗攻击配置



配置说明：

ARP 抗攻击配置监控信息显示界面如图所示，默认显示所有受监控主机的详细信息，点击“查看指定范围的 ARP 扫描表”则显示符合所填参数的 ARP 扫描结果，如图所示，不填或者勾选“查看全部”复选框则显示所有 ARP 扫描表信息。点击“清除 ARP 扫描表”按钮将 ARP 扫描表中的信息全部清除。点击“查看指定范围的受监控主机信息”则显示符合所填参数的受监控主机信息，不填或者勾选“查看全部”复选框则显示所有受监控主机信息。如果要删除某条主机信息，请选中对应的复选框后按“删除”按钮使配置生效。如果要删除所有主机信息，请按“全选”按钮后，选中所有主机，按“删除”按钮使配置生效。

2) ICMP 抗攻击配置

图 1-25 NFPP 监控信息—ICMP 抗攻击配置

配置说明：

ICMP 抗攻击配置监控信息界面默认显示所有受监控主机的详细信息，点击“查看不监控的信任主机”则显示符合所有不监控的信任主机信息，如图所示。输入 IP 地址和相应的掩码，点击“设置指定的信任主机”则将该范围内的所有主机加入到信任主机列表中。点击“查看指定范围的受监控主机信息”则显示符合所填参数的受监控主机信息，不填或者勾选“查看全部”复选框则显示所有受监控主机信息。

3) DHCP 抗攻击配置

图 1-26 NFPP 监控信息—DHCP 抗攻击配置

配置说明：

DHCP 抗攻击配置监控信息显示界面如图所示，默认显示所有受监控主机的详细信息，点击“查看指定范围的受监控主机信息”则显示符合所填参数的受监控主机信息，不填或者勾选“查看全部”复选框则显示所有受监控主机信息。

4) DHCPv6 抗攻击配置

图 1-27 NFPP 监控信息—DHCPv6 抗攻击配置

配置说明：

DHCPv6 抗攻击配置监控信息显示界面如图所示，默认显示所有受监控主机的详细信息，点击“查看指定范围的受监控主机信息”则显示符合所填参数的受监控主机信息，不填或者勾选“查看全部”复选框则显示所有受监控主机信息。

NFPP配置

图 1-28 NFPP 监控信息

1) CPU 保护配置

图 1-29 CPU 保护配置

配置说明：

CPU 保护配置，显示当前各类报文的占用带宽和报文所占比例的信息，点击“修改”，弹出如图所示的配置窗口，填好相应参数后点击“保存”按钮使配置生效，结果将显示在界面上，参数不填则配置为默认，参数不修改则保持当前配置不变。

2) NFPP 配置

图 1-30 NFPP 配置

配置说明：

NFPP 配置，显示当前各协议的基本配置信息，点击对应列的末行“恢复默认”则将该协议的 NFPP 置为默认配置，点击表格下方的“恢复默认”将把所有协议的 NFPP 置为默认配置。点击“修改”按钮将弹出如图所示的配置窗口，选择对应的协议，填好相应参数后点击“保存”按钮使配置生效，结果将显示在界面上，参数不填则配置为默认，参数不修改则保持当前配置不变。

NFPP接口配置

1) ARP 抗攻击配置

图 1-31 NFPP 监控信息—NFPP 接口 ARP 配置

配置说明：

ARP 抗攻击接口 NFPP 配置界面如图所示，选择需要配置的接口，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。

2) ICMP 抗攻击配置

图 1-32 NFPP 监控信息—NFPP 接口 ICMP 配置

配置说明：

ICMP 抗攻击接口 NFPP 配置界面如图所示，选择需要配置的接口，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。

3) DHCP 抗攻击配置

图 1-33 NFPP 监控信息—NFPP 接口 DHCP 配置

配置说明：

DHCP 抗攻击接口 NFPP 配置界面如图所示，选择需要配置的接口，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。

4) DHCPv6 抗攻击配置

图 1-34 NFPP 监控信息—NFPP 接口 DHCPv6 配置

配置说明：

DHCPv6 抗攻击接口 NFPP 配置界面如图所示，选择需要配置的接口，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。

5) ND 抗攻击配置

图 1-35 NFPP 监控信息—NFPP 接口 ND 配置

配置说明：

ND 抗攻击接口 NFPP 配置界面如图所示，选择需要配置的接口，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。

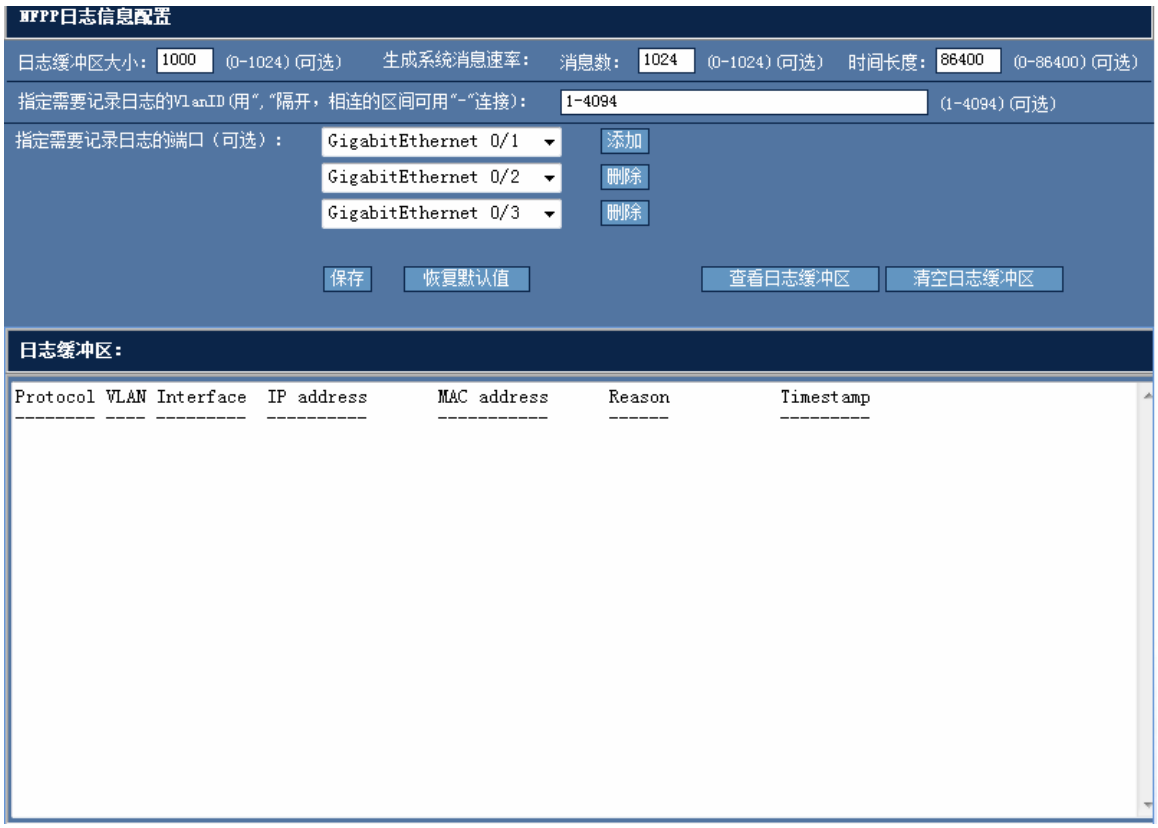
NFPP日志

图 1-36 NFPP 日志信息配置

配置说明：

NFPP 日志信息配置界面如图所示，填好相应的配置参数，选择需要记录日志的接口后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果将显示在下方的表格中，参数不填则配置为默认值。点击“查看日志缓冲区”将在配置界面下方弹出一个显示当前缓冲数据的窗口，如下图所示，点击“清空日志缓冲区”删除所有缓冲的日志信息，并关闭缓冲区窗口。

图 1-37 日志缓冲区



1.6 安全

1.6.1 防网关ARP欺骗

通过菜单项“防网关 ARP 欺骗”使用该功能。

防网关 ARP 欺骗页面：

图 1-38 防网关 ARP 欺骗

配置说明：

请选中要配置的端口，在输入网关地址后按“保存”按钮使配置生效，一个端口可配置多个网关地址，如果要删除所配置的网关，请选中要删除的网关地址所对应的复选框，按“删除”按钮使配置生效。

1.6.2 防ARP欺骗

通过菜单项“防 ARP 欺骗”使用该功能。

防 ARP 欺骗设置页面：

图 1-39 防 ARP 欺骗设置

配置说明：

■ 端口/MAC/IP 绑定

如果要配置端口/MAC/IP 绑定，请选中要配置的端口，并配置好 IP 和 MAC 后，按“保存”按钮使配置生效，如果选中的端口有学到 MAC 地址，则将会在端口自动学习到的地址文本框中显示出来，如上图所示，当选中 GigabitEthernet 0/15 口后，文本框中将列出该端口所学习到的 MAC 地址。

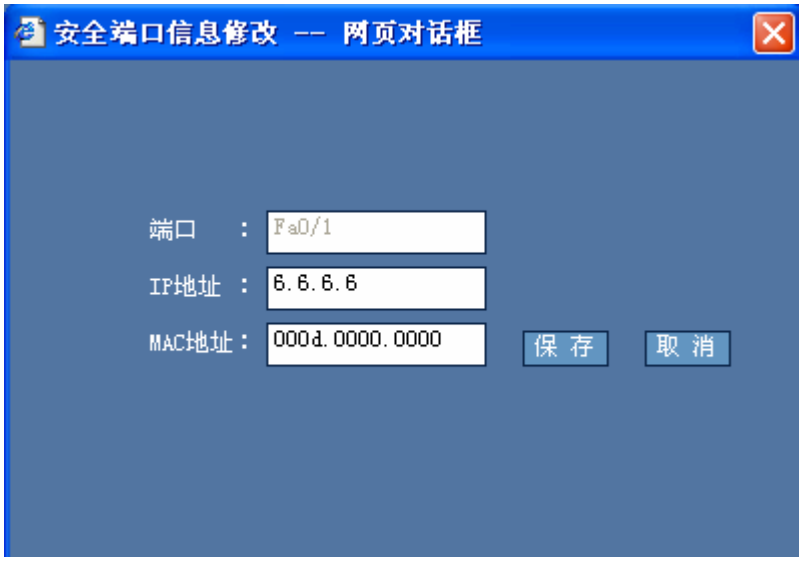
■ 端口安全功能设置

选中所要配置的端口后，如果该端口开启了端口安全功能，则开启端口安全功能的单选按钮将会选中，反之则选中关闭端口安全功能单选按钮。如果开启了端口安全功能，则将会在下表中显示安全端口信息。

■ 修改安全端口信息

如果要修改端口安全信息，请选中要修改的端口所对应的复选框后按“修改”按钮，将弹出安全端口修改设置界面，如下图：

图 1-40 修改安全端口



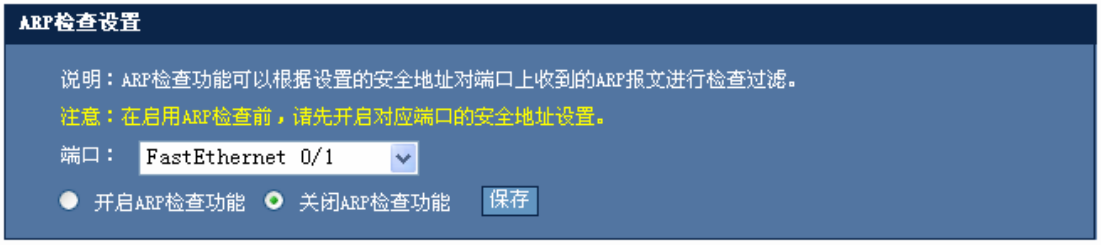
修改好相关参数后按“保存”按钮使配置生效，如果端口类型为动态，则修改后端口类型将转换为静态。

1.6.3 APR检查设置

通过菜单项“ARP 检查设置”使用该功能。

ARP 检查设置页面：

图 1-41 ARP 检查设置



配置说明：

如果选中的端口已开启该功能，则“开启 ARP 检查功能”单选按钮将被选中，否则默认都选中“关闭 ARP 检查功能”单选按钮。

1.6.4 ACL

通过菜单项“ACL”使用该功能。

ACL 设置页面：

图 1-42 ACL 设置

显示 ACL 信息

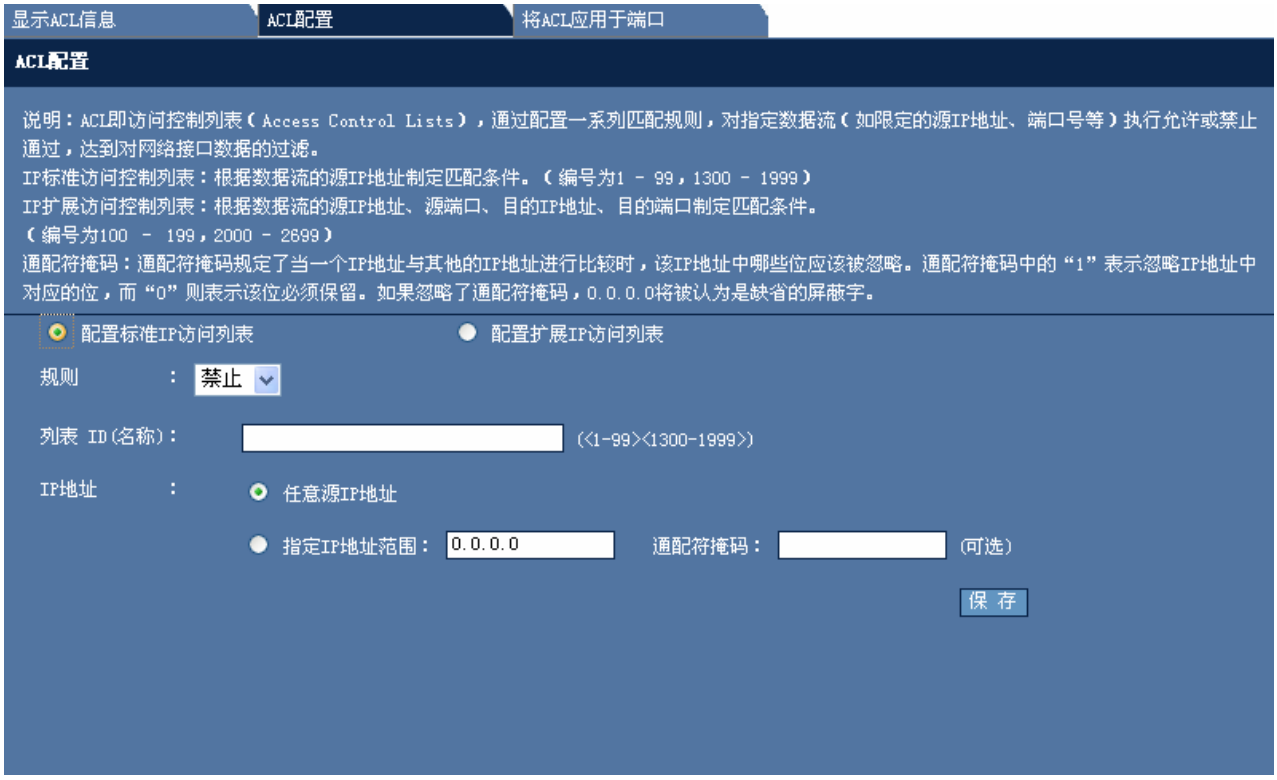
配置说明：

ACL 信息显示界面如图所示，如果要查看指定 ACL 的详细信息，请从 ACL 列表框中选中该条 ACL 后，便会在表格中显示出该 ACL 的所有 ACE。如果要删除某条 ACE，请选中对应的复选框后按“删除”按钮使配置生效。如果要删除整条 ACL，请按“全选”按钮后，选中所有 ACE，按“删除”按钮使配置生效。

ACL 配置

如果要配置标准 IP 访问列表，请点击“配置标准 IP 访问列表”单选按钮，下图为配置标准 IP 访问列表界面：

图 1-43 配置标准 IP 访问列表



配置说明：

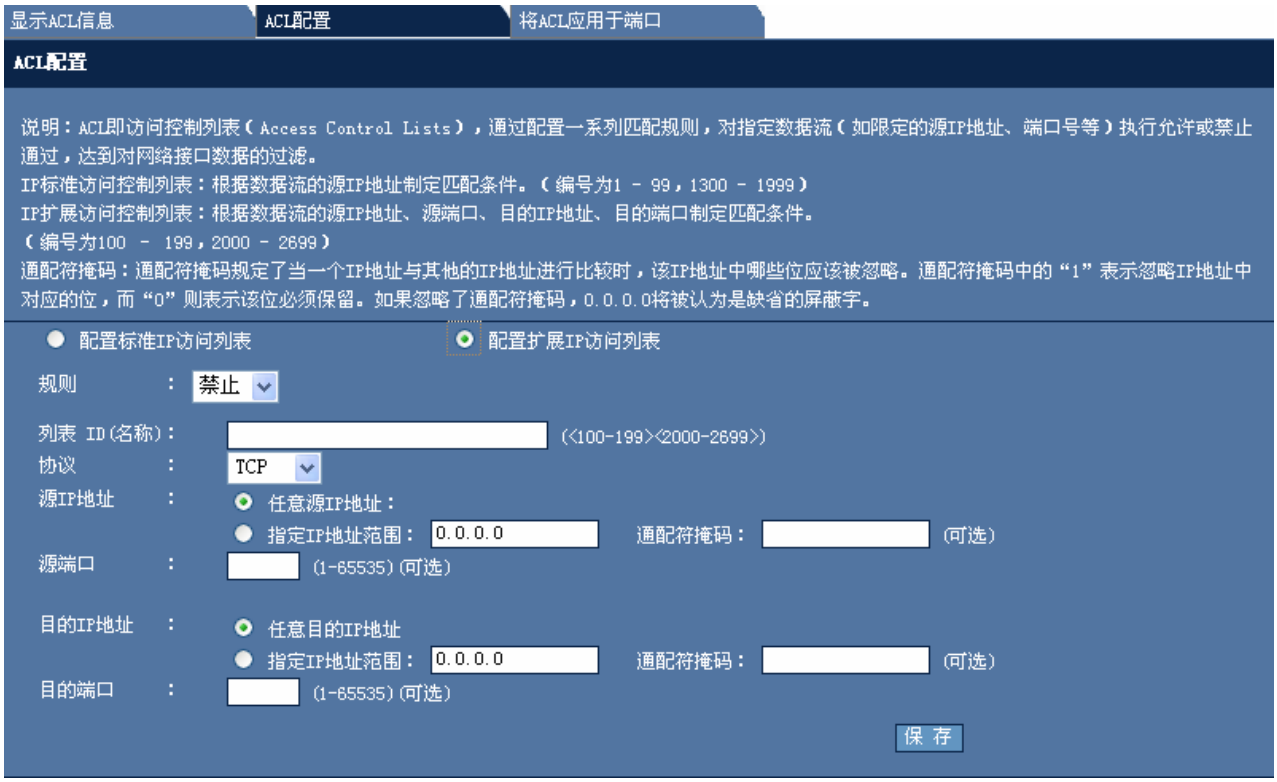
规则：请从下接列表中选择过滤规则，只有“禁止”和“允许”两种规则。

列表 ID（名称）：请输入标准访问列表号，也可以输入标准访问列表的名称。

IP 地址：如果选择指定 IP 地址范围,请输入正确的 IP 地址，通配符掩码文本框如果不需要，可以不填，配置好后按“保存”按钮使配置生效。

如果要配置扩展 IP 访问列表，请点击“配置扩展 IP 访问列表”单选按钮，下图为配置扩展 IP 访问列表：

图 1-44 配置扩展 IP 访问列表



配置说明：

规则：请从下接列表中选择过滤规则，只有“禁止”和“允许”两种规则。

列表 ID（名称）：请输入扩展访问列表号，也可以输入扩展访问列表的名称。

协议：该选项支持 TCP、UDP、IP、ICMP

源 IP 地址：你可以选择任意源 IP 地址或指定 IP 地址范围，通配符为可选配置。

源端口：可选配置。

目的 IP 地址：你可以选择任意源 IP 地址或指定 IP 地址范围，通配符为可选配置

目的端口：可选配置。

配置好参数后，请按“保存”按钮使配置生效。

将 ACL 应用于端口

图 1-45 将 ACL 应用于接口

配置说明：

端口：请选择要配置的端口。

ACL 列表：请选择要应用于该端口的 ACL。

配置好参数后按“保存”按钮使配置生效。

如果要删除对应端口的配置，请选中要删除的表项后按“删除”按钮使配置生效。

如果要配置与 PC 所连的端口，请确认该 ACL 是否会影响 PC 与设备的交互。如果配置错误，将无法继续使用 WEB 来管理设备。

1.6.5 IP Source Guard

IP Source Guard 概述

IP Source Guard 功能维护一个 IP 源地址数据库，通过将数据库中的用户信息[VLAN、MAC、IP、PORT]设置为硬件过滤表项，只允许对应的用户使用网络。

IP Source Guard 功能的应用是和 DHCP Snooping 结合起来的。DHCP Snooping 维护一个用户 IP 的数据库，并将该数据提供给 IP Source Guard 功能进行过滤，从而限制只有通过 DHCP 获取 IP 的用户才能够使用网络，这样就阻止了用户随意设置静态 IP。

基于接口的 IP Source Guard 仅仅在 DHCP Snooping 控制范围内的非信任口上生效，在其他信任口或者非 DHCP Snooping 控制范围内的接口上配置该功能，功能将不生效。

通过菜单项“IP Source Guard”使用该功能。

IP Source Guard 设置页面：

图 1-46 IP Source Guard 设置

接口配置

配置说明：

接口：选择要开启 IP Source Guard 功能的接口。

如果要设置过滤类型为：IP+MAC，请勾选“基于 IP+MAC 的过滤功能(可选)”

用户绑定

配置静态的 IP 源地址绑定用户

配置说明：

MAC 地址：用户 MAC 地址

VLAN：使用的 VLAN ID

IP 地址：用户 IP 地址

接口：选择关联的接口。

图 1-47 用户绑定

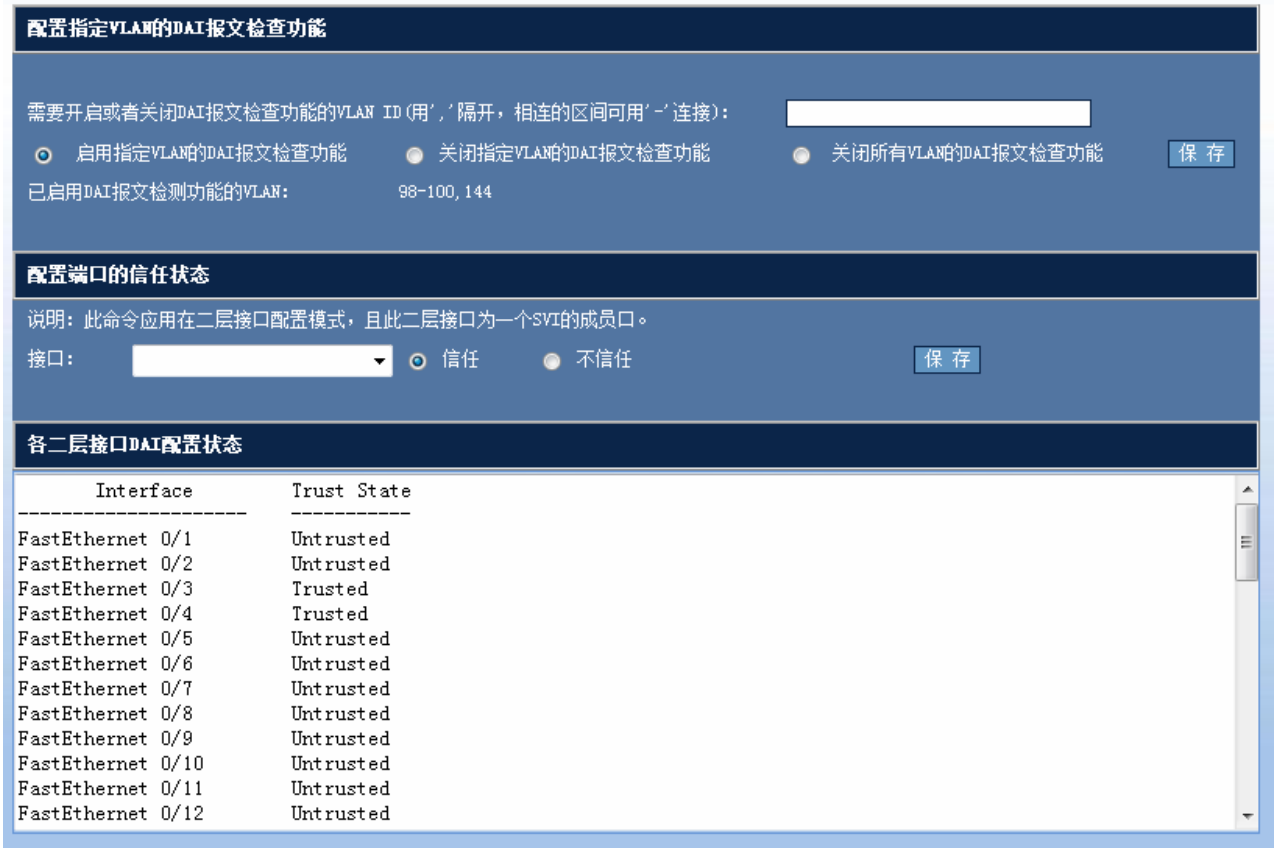
1.6.6 DAI

DAI 的全称是 Dynamic ARP Inspection（动态 ARP 检测）。即对接收到的 ARP 报文进行合法性检查，丢弃不合法的 arp 报文。

通过菜单项“DAI”使用该功能。

DAI 设置页面：

图 1-48 DAI 设置



■ 配置指定 VLAN 的 DAI 功能

缺省情况下，所有 VLAN 的 DAI 报文检查功能是关闭的。

比如未启用 VLAN 100 的 DAI 报文检查功能，vlan-id 为 100 的 ARP 报文会跳过 DAI 相关的安全检查。

配置说明：

在“需要开启或者关闭 DAI 报文检查功能的 VLAN ID”文本框中输入需要设置的 VLAN 列表。然后选择启用或关闭指定 VLAN 的 DAI 报文检查功能单选框，或者选择关闭所有 VLAN 的 DAI 报文检查功能，最后点击“保存”。

保存后页面上会显示已经启用 DAI 报文检查功能的 VLAN。

■ 配置端口信任状态

基于设备上每一个端口的信任状态，对 ARP 报文作出相应的检查，从受信任端口接收到的报文将跳过 DAI 检查，被认为是合法的 ARP 报文； 而从非信任端口接收到的 ARP 报文，将严格执行 DAI 检查。

在一个典型的网络配置中，应该将连接到网络设备的二层端口设置为受信任端口，连接到主机设备的二层端口设置为非信任端口。

配置说明：

在接口下拉框中选择一个接口，点击“信任”或“不信任”，然后点击“保存”按钮。

在“各二层接口 DAI 配置状态”文本框中显示配置结构。

1.6.7 GSN

通过菜单项“GSN”使用该功能。

GSN 页面：

图 1-49 GSN 设置

配置说明：

- 打开关闭 GSN 功能

点击打开 GSN 前的单选框开启 GSN，点击关闭 GSN 前的单选框关闭 GSN。

- 同 SMP server 之间的通讯

同 SMP server 之间的通讯支持 v1（默认），v2，v3 三种模式，输入 Community 或 User 值后点击“保存”后即可开启。点击“关闭”按钮即可关闭。

- 应用于端口

配置好 GSN 后即可将 GSN 应用于端口，配置方法是选择端口后点击“保存”按钮，配置的结果将在下面的表格中显示。要删除配置时先选择相应配置前的复选框，再点击表格下方的“删除”按钮。

1.6.8 CPP配置

通过菜单项“CPP 配置”使用该功能。

CPP 配置页面：

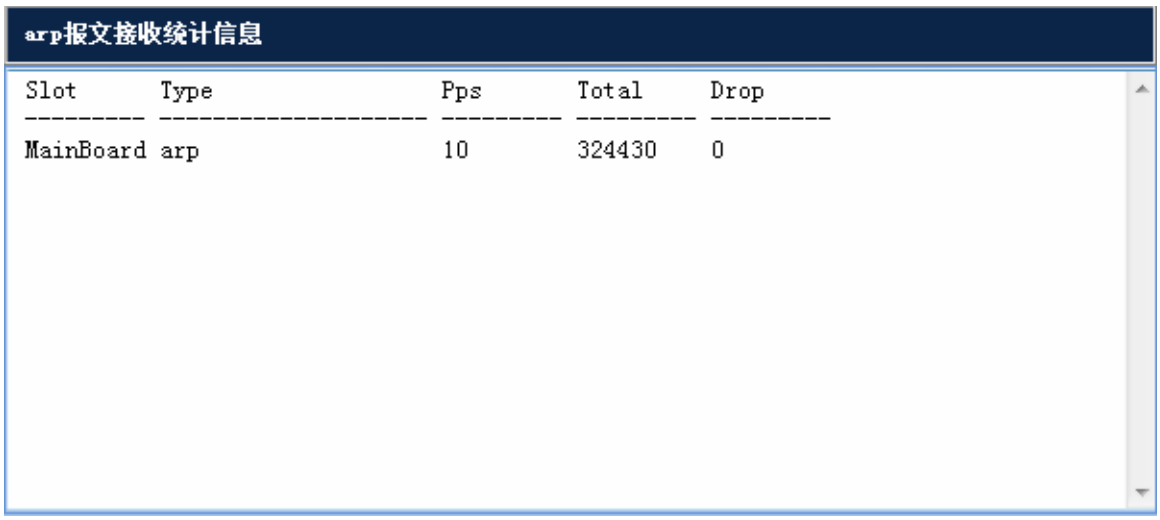
图 1-50 CPP 配置

配置说明：

选择需要修改的报文类型，“恢复默认配置”按钮将把该类型对应的带宽和优先级置为默认值，填写带宽，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。选择优先级，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。

点击“查看指定报文接收统计信息”将显示如下图所示的信息：

图 1-51 指定报文接收统计

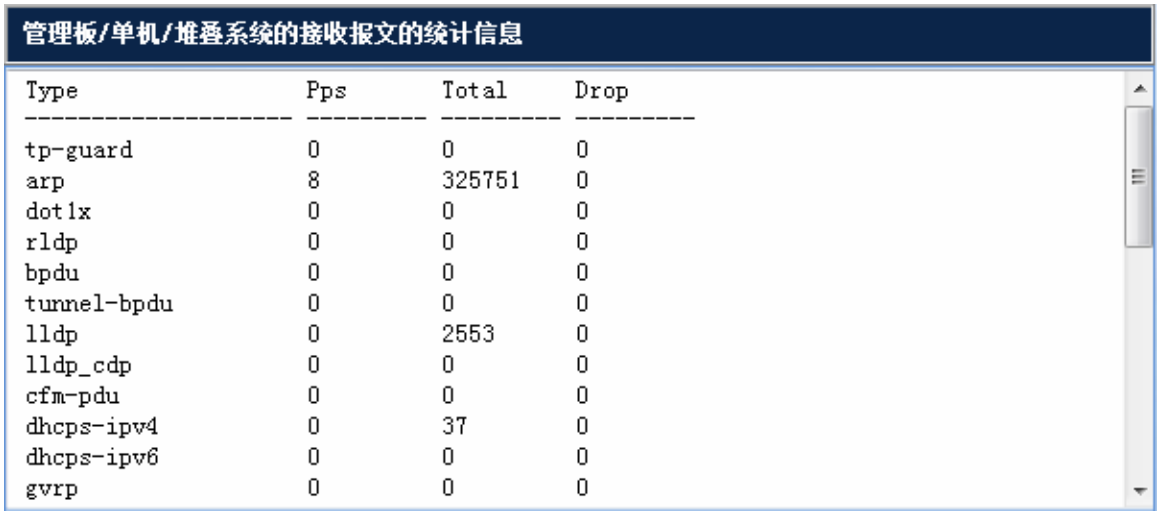


点击“查看配置信息”将显示所有报文的带宽和优先级信息，如下图所示：

图 1-52 报文的带宽和优先级信息

点击查看管理板/单机/堆叠系统的接收报文的统计信息后的“查看”将显示管理板/单机/堆叠系统的接收报文的统计信息，如下图所示：

图 1-53 管理板/单机/堆叠系统的接收报文的统计信息



输入显卡号，点击“查看”将显示接收报文的统计信息。

1.6.9 RADIUS配置

通过菜单项“RADIUS 配置”使用该功能。

RADIUS 配置页面：

图 1-54 RADIUS 服务器配置

RADIUS 服务器

配置说明：

上半部分为 AAA 相关配置，只有在开启 AAA 功能的情况下，RADIUS 服务器才能进行正确的配置。点击 AAA new-model 后面的“开启”按钮 AAA 功能打开，选择密钥模式，输入密钥，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。记帐计费更新功能、IP 授权模式后面的单选框选中时配置生效，选择 IP 授权模式，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。

在 RADIUS 服务器输入框中输入服务器的 IP 地址，填写认证和记账端口号，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。不填写端口号则使用默认值。

RADIUS 服务器组配置

图 1-55 RADIUS 服务器组配置

配置说明：

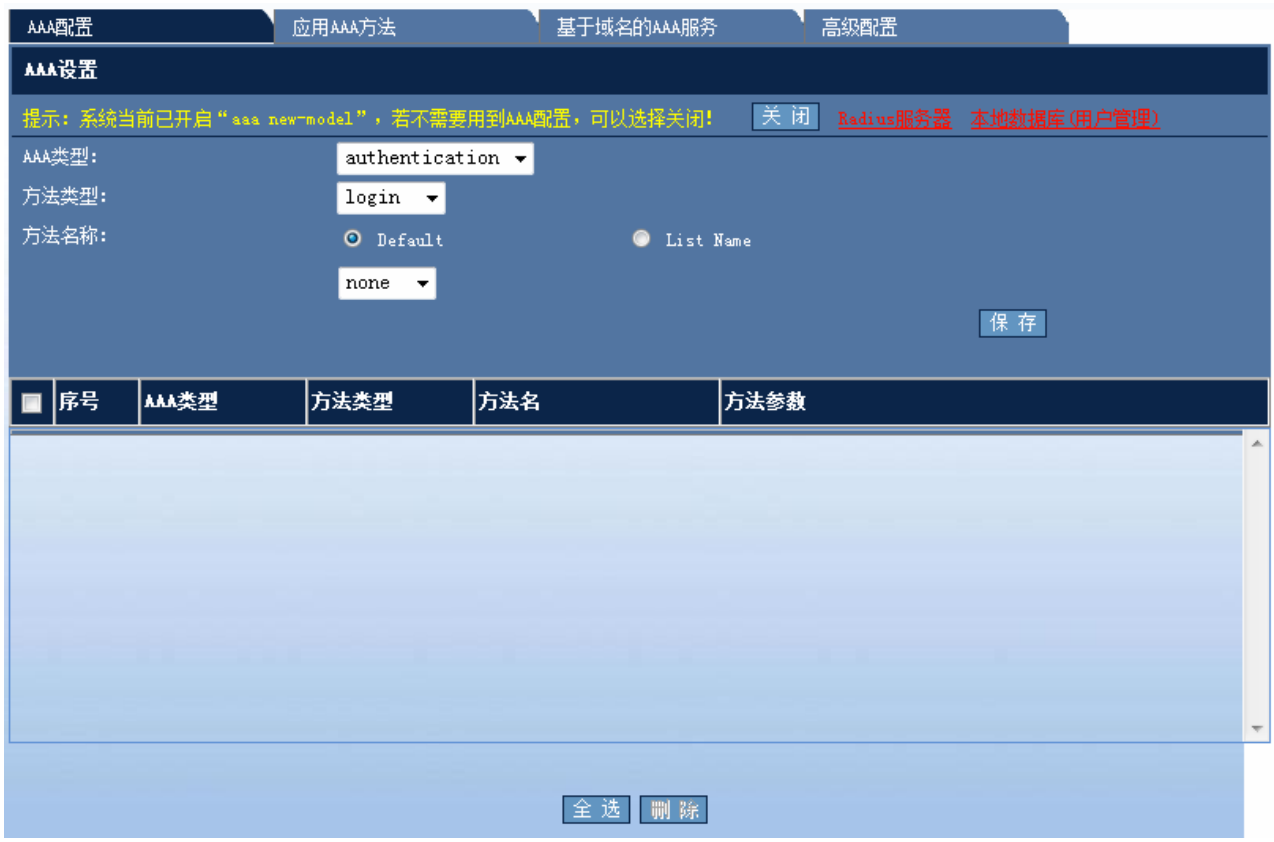
输入要新建或者修改的服务器组名，输入需要加入改组的 RADIUS 服务器 IP 地址，填写该服务器对应的端口号，点击下方的“保存”按钮使配置生效，成功后会弹出配置成功提示框，结果显示在下面的文本框中，不填写端口号则使用默认值。在 Radius 服务器组管理后面的下拉框中选择需要删除的服务器组，点击“删除”按钮将把相应的服务器组删除。

1.6.10 AAA设置

通过菜单项“AAA 配置”使用该功能。

AAA 设置页面：

图 1-56 AAA 配置



AAA 配置

配置说明：

AAA 类型中可以选择 authentication，authorization，accounting 三种类型，方法类型根据 AAA 类型的不同有 login，enable，ppp，dot1x 及 exec，command，network 两种方法类型。方法名称可以选择默认或选择 List Name 自定义，认证方法参数分为 local，group 等多种认证方法，选择相应方法后点击“保存”按钮后将下下面表格中显示配置结果。

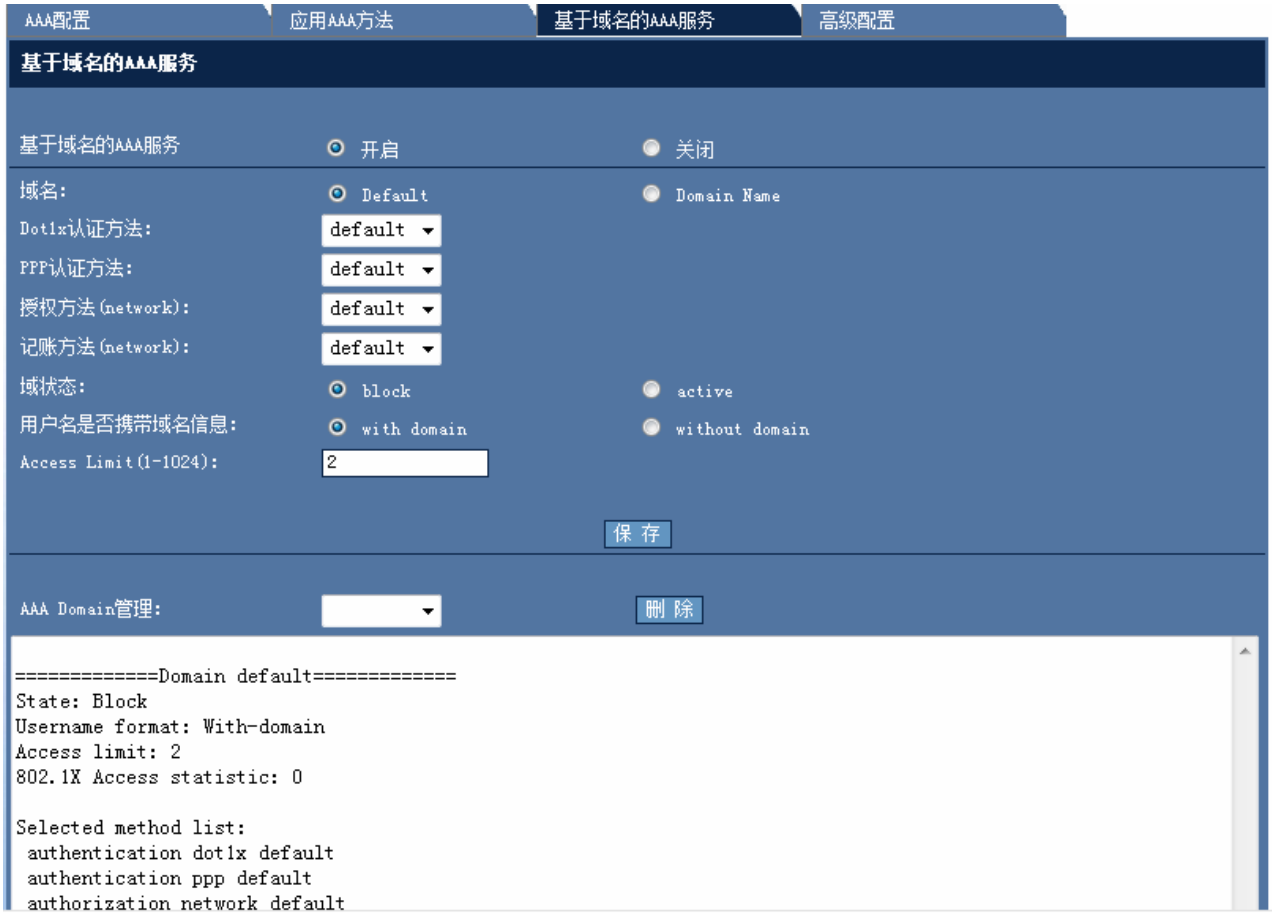
应用 AAA 方法

图 1-57 应用 AAA 方法

配置完 AAA 后即可应用 AAA 方法。选择相应方法后，设置好相应线路参数点击“保存”后即可。点击“查看”按钮可查看相应配置，点击“恢复默认”后即可恢复系统默认设置。

配置基于域名的 AAA 服务

图 1-58 基于域名的 AAA 服务

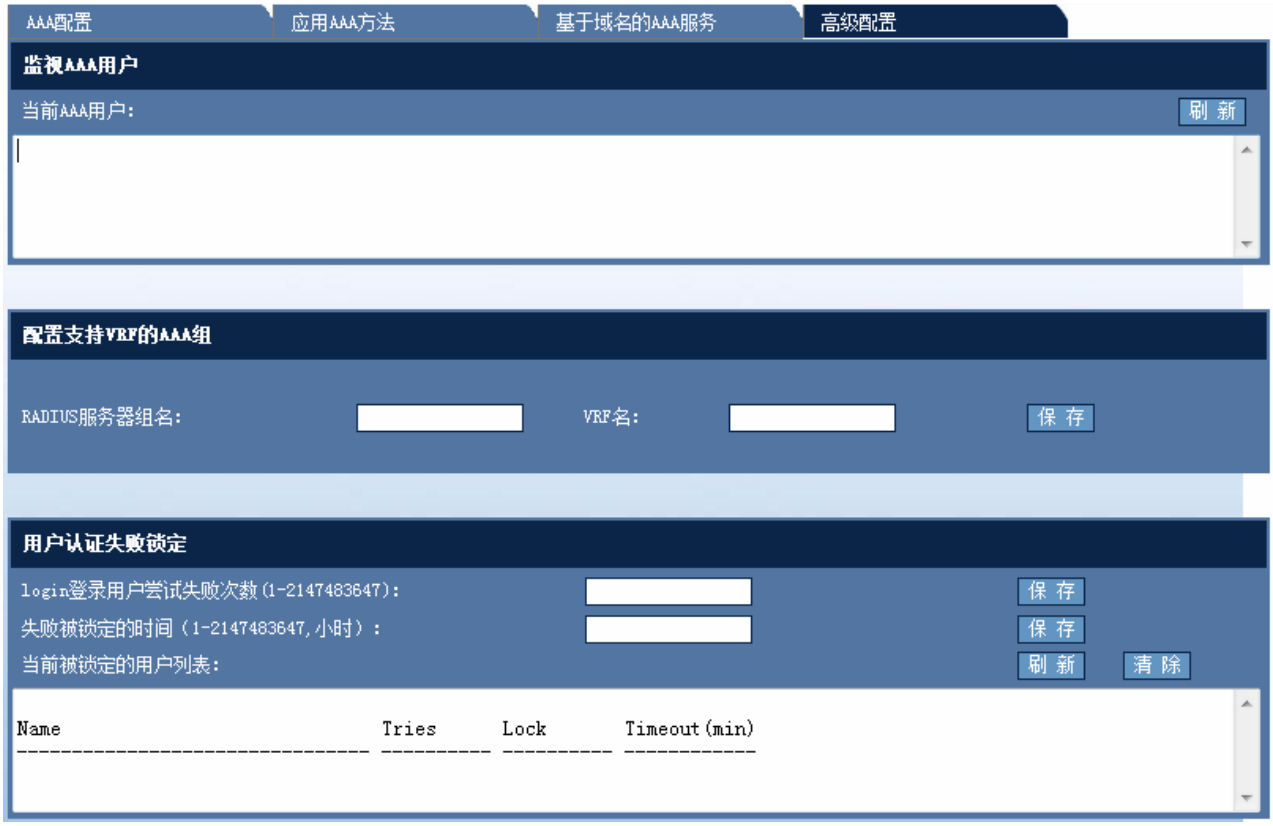


首先开启基于域名的 AAA 服务，选择域名及 Dot1x 认证方法，PPP 认证方法，授权方法(network)，记账方法(network)，域状态，用户名是否携带域名信息，Access Limit 等信息后点击“保存”按钮，配置好的信息将在下面文本框中显示。

要删除配置时，在 AAA Domain 管理下拉框中选择相应配置，点击右边的“删除”按钮即可。

高级配置

图 1-59 AAA 高级配置



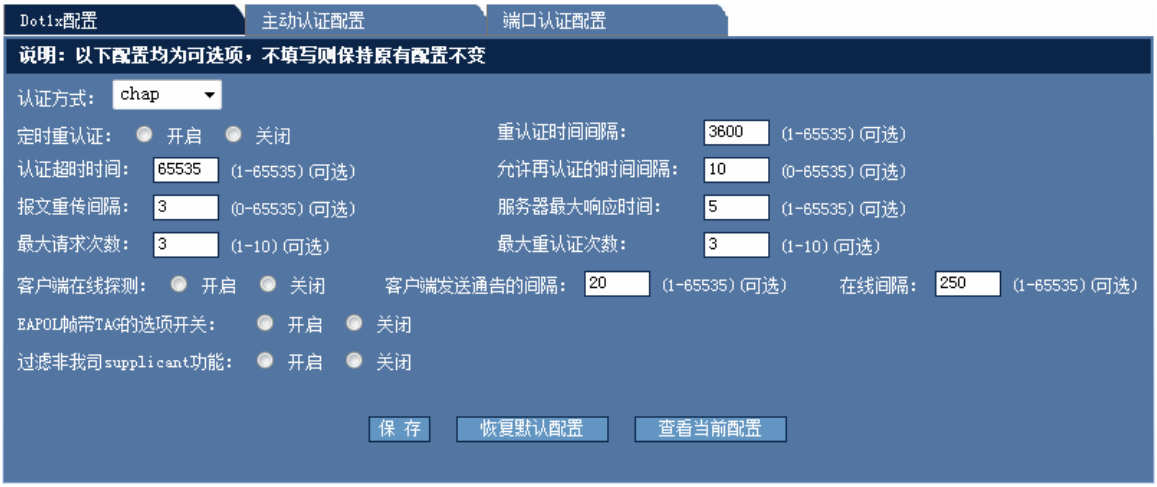
AAA 高级配置可以查看监视 AAA 用户，配置支持 VRF 的 AAA 组及用户失败锁定信息。

1.6.11 Dot1x配置

通过菜单项“Dot1x 配置”使用该功能。

Dot1x 配置页面：

图 1-60 Dot1x 配置



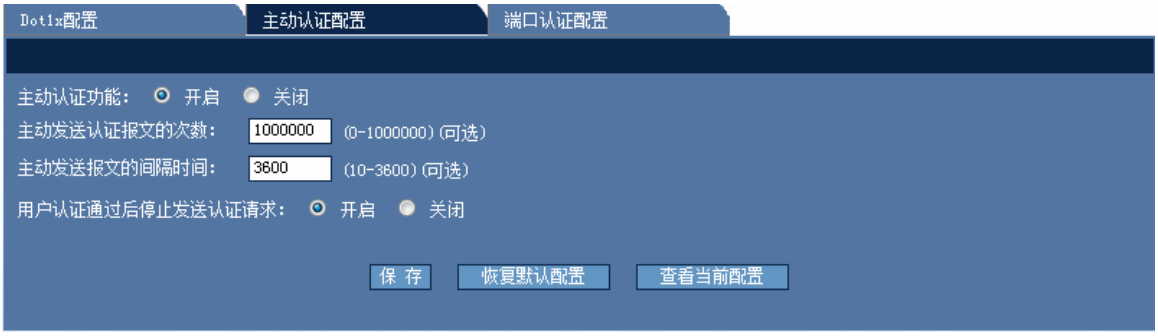
Dot1x 配置

配置说明：

Dot1x 配置界面如图所示，选择认证参数，填好相应的配置参数后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，点击“恢复默认配置”所有参数值恢复为默认，点击“查看当前配置”所有参数为当前的配置值。

主动认证配置

图 1-61 主动认证配置



配置说明：

主动认证配置界面如图所示，选择功能的“开启”或“关闭”单选按钮，填好相应的配置参数，选择是否在用户认证通过后停止发送认证请求，然后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，点击“恢复默认配置”所有参数值恢复为默认，点击“查看当前配置”所有参数为当前的配置值。

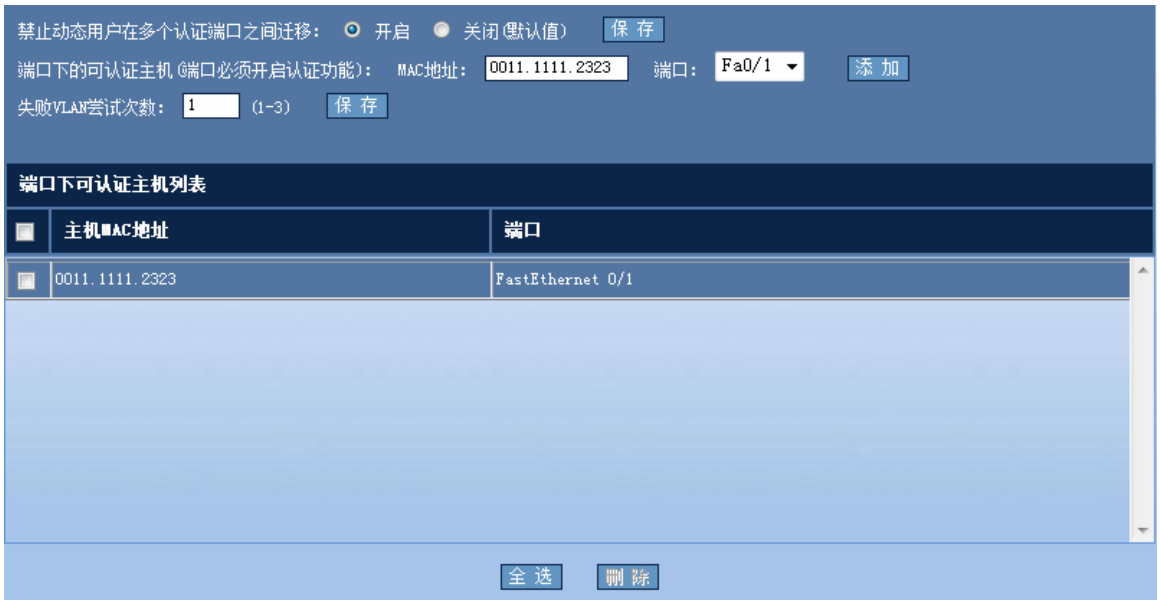
端口认证配置

图 1-62 端口认证配置 1

配置说明：

端口认证配置界面如图所示，上半部分为基于接口来配置 Dot1x 功能，选择各项功能的开关按钮，填好相应的配置参数，然后点击“保存”按钮使配置生效，成功后会弹出配置成功提示框，点击“恢复默认”则该接口下的所有参数值恢复为默认，点击“查看当前配置”所有参数显示为当前接口的配置值。

图 1-63 端口认证配置 2



如上图所示，选择是否开启禁止用户在多个认证端口之间迁移功能，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。当某个端口开启 802.1x 认证功能时，则可基于该端口配置可认证主机，输入 MAC 地址，选择相应的端口，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框，成功后结果将显示在下方的表格中。填写失败 VLAN 尝试次数，点击后面的“保存”按钮使配置生效，成功后会弹出配置成功提示框。

1.6.12 智能绑定

通过菜单项“智能绑定”使用该功能。

智能绑定页面：

图 1-64 智能绑定

配置说明：

智能绑定即将 IP 地址和 MAC 地址进行绑定

- 可以通用输入 IP 地址，点击查找后获取 MAC 地址，当找到 MAC 地址后点击“绑定”按钮，配置的结果在下面表格中显示。
- 可通过 ARP 表查看 IP 及 MAC 对应信息，然后点击表格中的“绑定”按钮进行绑定。

图 1-65 通过 ARP 表进行智能绑定

1.6.13 WEB认证设置

通过菜单项“web 认证设置”使用该功能。

web 认证设置：

图 1-66 web 认证设置

基本设置

配置说明：

web 认证可以设置重定向的 IP 地址，认证页面 URL， 重定向端口， 未认证用户的最大 HTTP 会话数(0-255，可选)及维持重定向连接的超时时间，设备与认证服务器之间的通信密钥，团体名称，发送 Web 认证消息的目的主机 IP，SNMP-Inform 消息使用的团体字符串,线用户信息的更新时间间隔,基于流量来检测用户是否下线、Vlan List 等。其中重定向端口默认为 80。保存后即可应用。

免认证资源

图 1-67 免认证资源

设定好 IP 地址及子网掩码后点击保存，即可设置免认证资源。要删除配置则在表格中选择相应配置后点击“删除”按钮。

免认证用户

图 1-68 免认证用户

设定好 IP 地址，子网掩码，及端口后点击“保存”，即可设置免认证资源。其中端口为可选选项。要删除配置则在表格中选择相应配置后点击“删除”按钮。

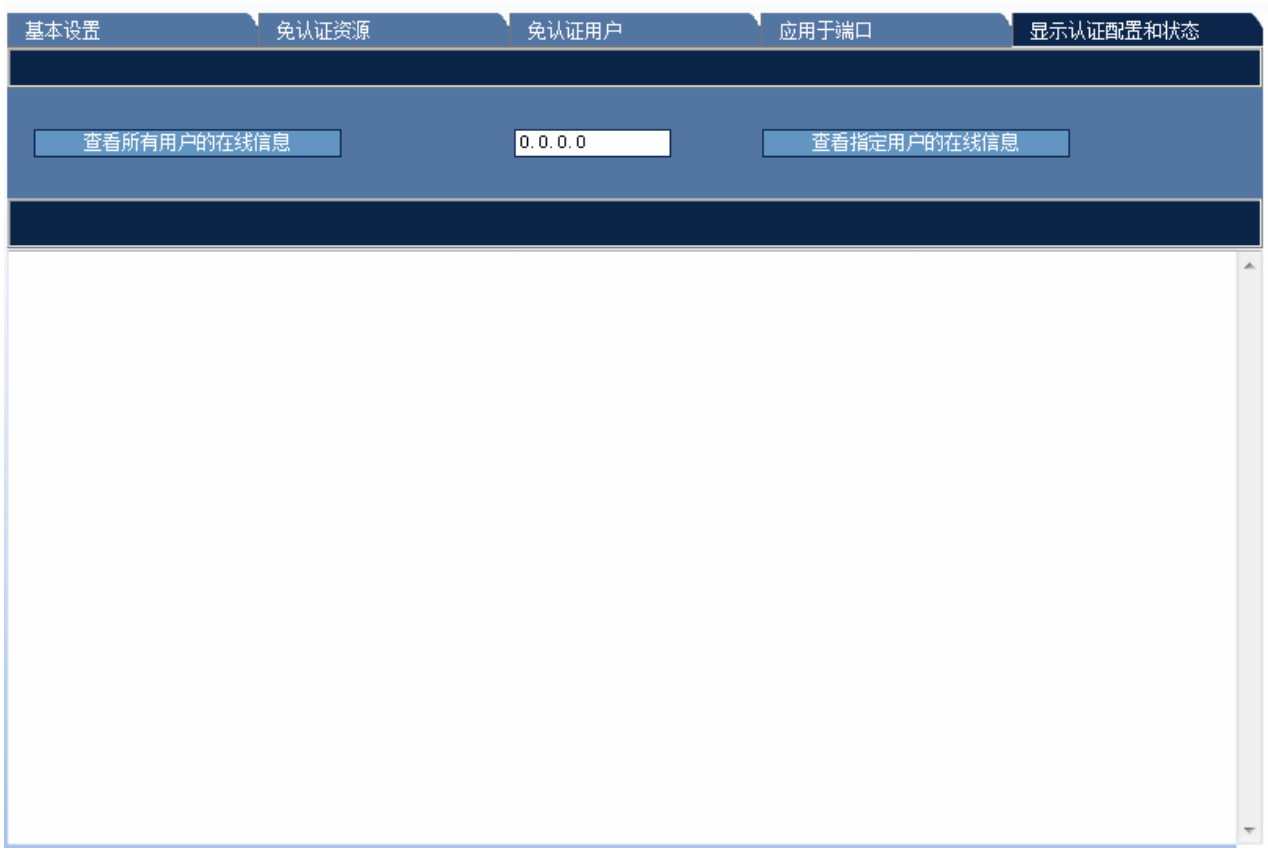
应用于端口

图 1-69 应用于端口

选择相应端口后点击“保存”。要删除配置则在表格中选择相应配置后点击“删除”按钮。

显示认证配置和状态

图 1-70 认证配置和状态



提供查看所有用户的在线信息和通过 IP 地址查看指定用户的在线信息。

1.6.14 DHCP Snooping

通过菜单项“DHCP Snooping”使用该功能。

DHCP Snooping 设置页面：

图 1-71 DHCP Snooping 设置

配置说明：

- DHCP Snooping 设置

要开启 DHCP Snooping 功能或 DHCP Snooping 源 MAC 检查功能，请选中相应的单选按钮后按“保存”使配置生效。

- DHCP Snooping 信任端口设置

请选择要设置为信任端口的端口后按“保存”按钮使配置生效，配置成功后将在下表显示配置信息。如果要删除信任端口，请选中相应的复选框后按“删除”按钮使配置生效。

1.7 QOS

1.7.1 分类设置

通过菜单项“分类设置”使用该功能。以下是分类设置的主要页面：

图 1-72 分类设置

配置说明：

设置好类名和 ACL 后按“保存”按钮使配置生效。配置成功后，将在下表中显示出配置信息。如果要删除已配置的类，请选中该类所对应的复选框后按“删除”按钮使配置生效。

1.7.2 策略设置

通过菜单项“策略设置”使用该功能。

策略设置页面：

图 1-73 策略设置

配置说明：

策略名字：配置策略名字。

分类列表：列出已设置的分类名称，如果列表为空，则说明没有设置分类，请先到分类设置页面进行分类设置。

带宽：请输入指定范围内的带宽值。

突发流量：请输入指定范围内的值，请按页面上的提示输入。

带宽超限部分指定处理动作：如果指定 DSCP 优先级，请输入指定范围内的数字。

设置好参数后按“保存”按钮使配置生效。

如果要删除设置好的策略，请从策略列表中选中该策略后，将会在表格中显示该策略的详细信息，选中要删除的表项后按“删除”按钮使配置生效。如果要一同删除策略名，只要全选后按“删除”按钮使配置生效。

1.7.3 流设置

通过菜单项“流设置”使用该功能。

流设置页面：

图 1-74 流设置

配置说明：

端口：请选择要配置的端口。

策略列表：请选择要应用于该端口的策略，如果列表为空，请先设置策略。

限速方向：请选择限速方向。

设置好参数后按“保存”按钮使配置生效。如果要删除端口的配置，请选中要删除的表项所对应的复选框后按“删除”按钮使配置生效。

1.7.4 风暴控制

通过菜单项“风暴控制”使用该功能。

风暴控制页面：

图 1-75 风暴控制

配置说明：

选择端口及相应的风暴类型，选择控制方式及设定好控制力度后点击“保存”按钮即可。配置结果将在下面表格中显示。如果要删除端口的配置，请选中要删除的表项所对应的复选框后按“删除”按钮。

1.7.5 端口安全

通过菜单项“端口安全”使用该功能。

端口安全页面：

图 1-76 端口安全

基本设置

配置说明

选择相应端口，设定好安全地址的最大个数，安全地址老化时间，Static，雇用 Sticky Mac 地址学习功能及处理违例方式后，点击“保存”按钮后即可。配置结果在下面表格中显示。若配置为系统默认配置，表格中将不显示。如果要删除端口的配置，请选中要删除的表项所对应的复选框后按“删除”按钮使配置生效。

安全地址

图 1-77 安全地址

配置安全地址时，先选择相应端口，设定安全地址类型及 Mac 地址，VLAN ID 等信息后点击“保存”按钮。配置结果将在下面表格中显示。要删除配置则在表格中选择相应配置后点击“删除”按钮。

安全地址绑定

图 1-78 安全地址绑定

安全地址绑定配置时，先选择相应端口，设置相应 IP 地址，若启用将 MAC 及 Vlan 进行绑定到安全端口，则还需要设置 Mac 地址及 VLAN ID 信息，点击“保存”按钮。配置结果将在下面表格中显示。要删除配置则在表格中选择相应配置后点击“删除”按钮。

1.8 系统状态

1.8.1 系统信息

通过菜单项“系统信息”使用该功能。

系统信息页面：

图 1-79 系统信息

系统信息	
设备型号：	S2924G
主机名 ：	Ruijie
软件版本：	RGOS 10.2(4), Release(55222),Web Version:10.2.55222
硬件版本：	1.0
MAC地址 ：	00d0f8f80fc4

1.8.2 当前配置

通过菜单项“当前配置”使用该功能。

当前配置页面：

图 1-80 当前配置

当前配置

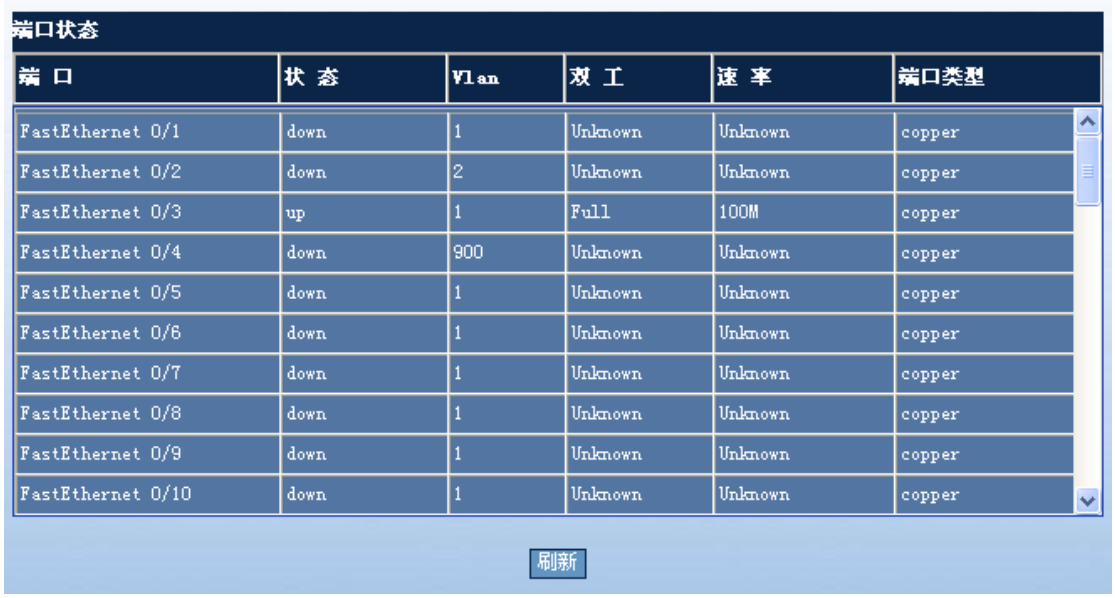
```
Building configuration...
Current configuration : 12931 bytes

!
version RGNOS 10.2.00(3), Release(30355)(Tue Mar 11 19:23:04     2008 -
23195A44470348C)
!
!
!
vlan 1
 name vlan1
!
vlan 2
!
vlan 3
!
vlan 4
!
vlan 5
!
vlan 6
!
vlan 7
!
```

1.8.3 端口状态

通过菜单项“端口状态”使用该功能。

端口状态页面：

图 1-81 端口状态


端口状态

端 口	状 态	Vlan	双 工	速 率	端口类型
FastEthernet 0/1	down	1	Unknown	Unknown	copper
FastEthernet 0/2	down	2	Unknown	Unknown	copper
FastEthernet 0/3	up	1	Full	100M	copper
FastEthernet 0/4	down	900	Unknown	Unknown	copper
FastEthernet 0/5	down	1	Unknown	Unknown	copper
FastEthernet 0/6	down	1	Unknown	Unknown	copper
FastEthernet 0/7	down	1	Unknown	Unknown	copper
FastEthernet 0/8	down	1	Unknown	Unknown	copper
FastEthernet 0/9	down	1	Unknown	Unknown	copper
FastEthernet 0/10	down	1	Unknown	Unknown	copper

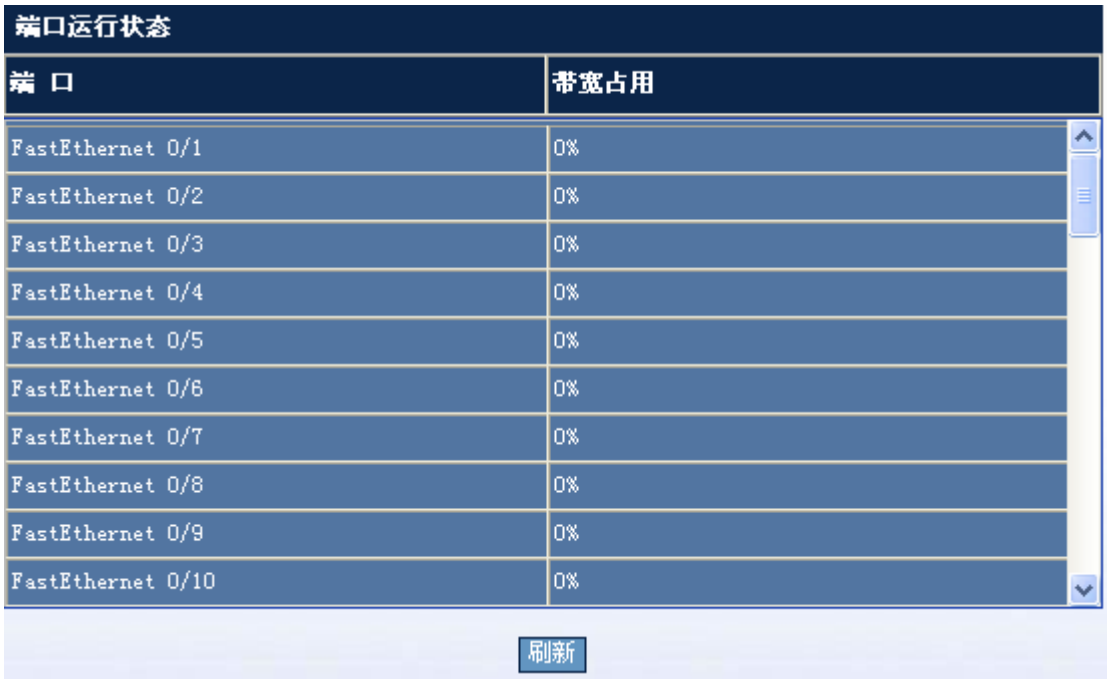
刷新

1.8.4 端口运行状态

通过菜单项“端口运行状态”使用该功能。

端口运行状态页面：

图 1-82 端口运行状态


端口运行状态

端 口	带宽占用
FastEthernet 0/1	0%
FastEthernet 0/2	0%
FastEthernet 0/3	0%
FastEthernet 0/4	0%
FastEthernet 0/5	0%
FastEthernet 0/6	0%
FastEthernet 0/7	0%
FastEthernet 0/8	0%
FastEthernet 0/9	0%
FastEthernet 0/10	0%

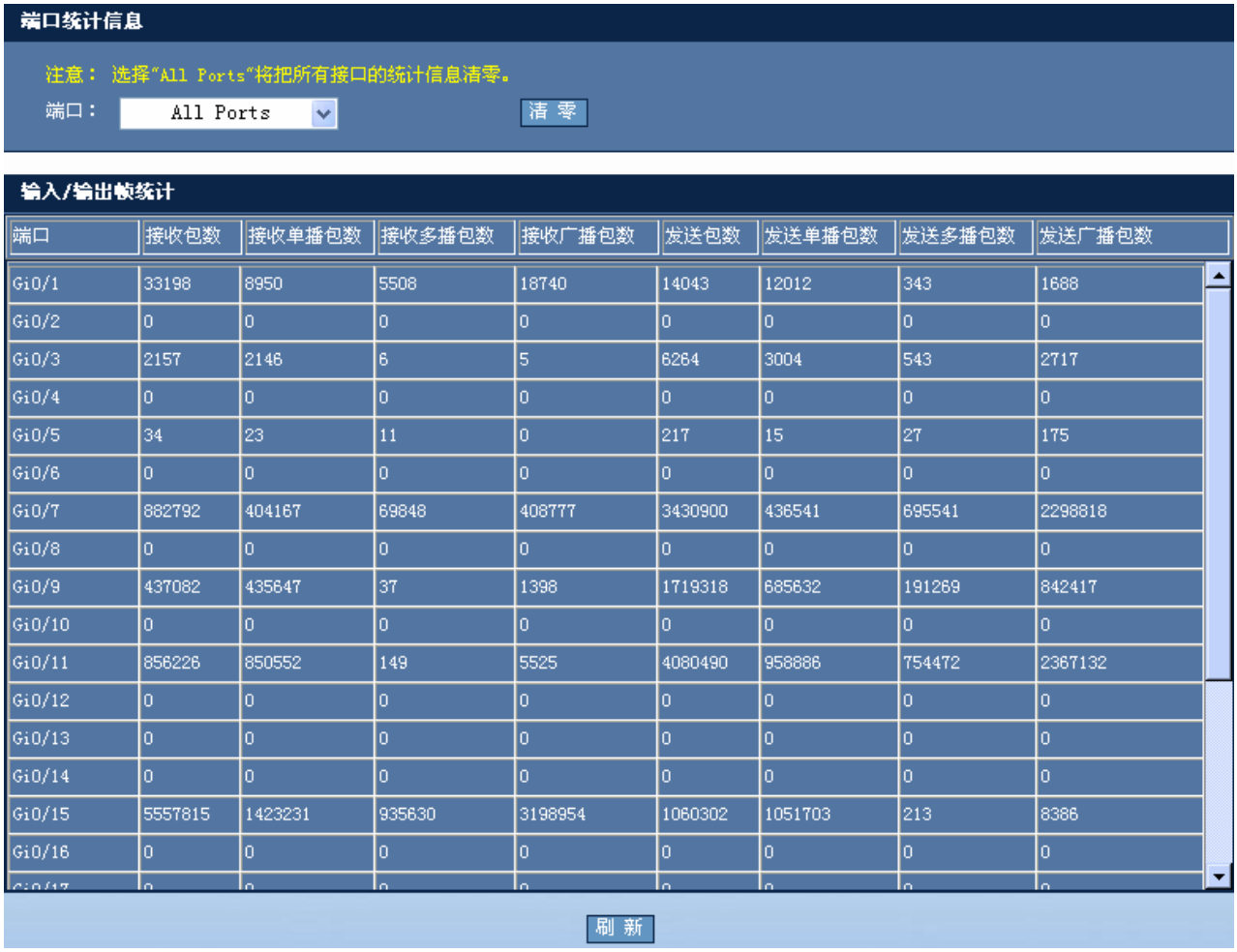
刷新

1.8.5 端口统计信息

通过菜单项“端口统计信息”使用该功能。

端口统计信息页面：

图 1-83 端口统计信息



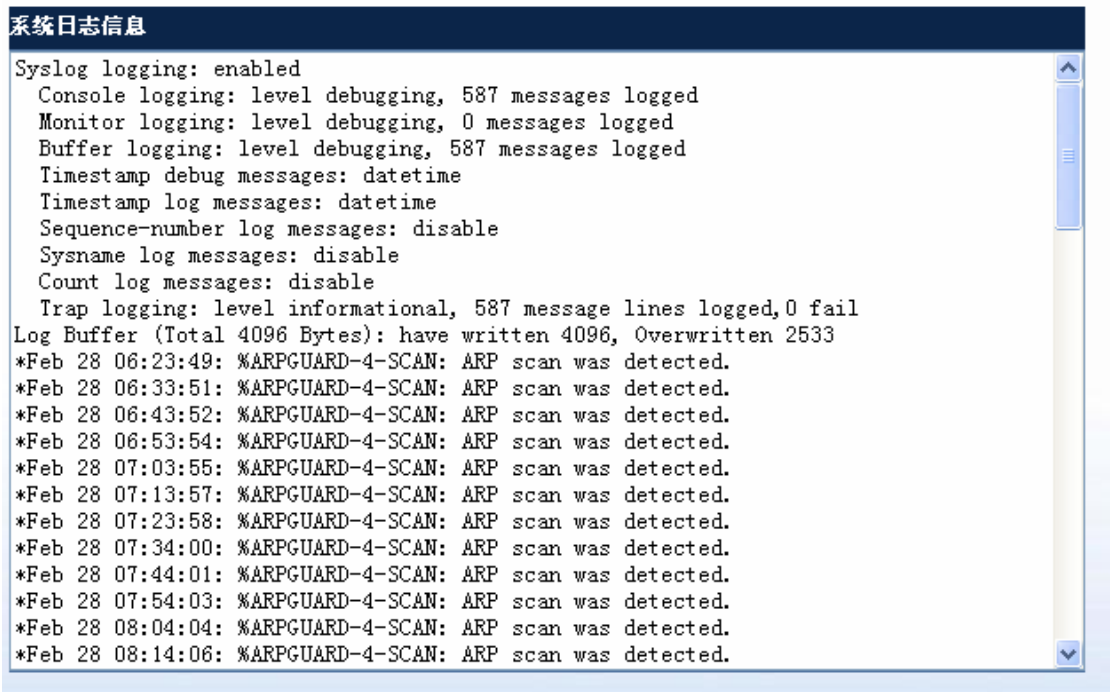
端口	接收包数	接收单播包数	接收多播包数	接收广播包数	发送包数	发送单播包数	发送多播包数	发送广播包数
Gi0/1	33198	8950	5508	18740	14043	12012	343	1688
Gi0/2	0	0	0	0	0	0	0	0
Gi0/3	2157	2146	6	5	6264	3004	543	2717
Gi0/4	0	0	0	0	0	0	0	0
Gi0/5	34	23	11	0	217	15	27	175
Gi0/6	0	0	0	0	0	0	0	0
Gi0/7	882792	404167	69848	408777	3430900	436541	695541	2298818
Gi0/8	0	0	0	0	0	0	0	0
Gi0/9	437082	435647	37	1398	1719318	685632	191269	842417
Gi0/10	0	0	0	0	0	0	0	0
Gi0/11	856226	850552	149	5525	4080490	958886	754472	2367132
Gi0/12	0	0	0	0	0	0	0	0
Gi0/13	0	0	0	0	0	0	0	0
Gi0/14	0	0	0	0	0	0	0	0
Gi0/15	5557815	1423231	935630	3198954	1060302	1051703	213	8386
Gi0/16	0	0	0	0	0	0	0	0

1.8.6 日志信息显示

通过菜单项“日志信息显示”使用该功能。

系统日志信息页面：

图 1-84 系统日志信息显示



1.9 系统维护

1.9.1 Ping

通过菜单项“Ping”使用该功能。

Ping 页面：

图 1-85 Ping

配置说明：

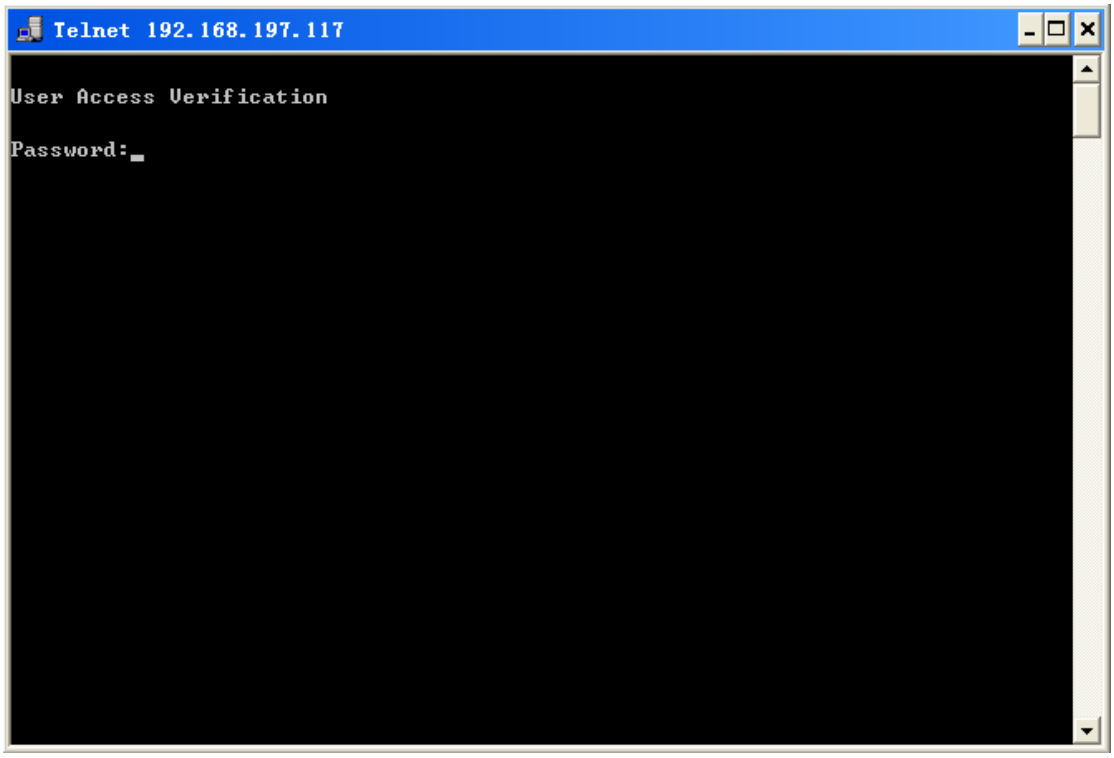
请在文本框中输入 IP 地址后，按“开始”按钮，如果 IP 地址不通，页面将等到 Ping 超时后才能响应。

1.9.2 Telnet

通过菜单项“Telnet”使用该功能。

Telnet 页面：

图 1-86 Telnet



配置说明：

直接点击菜单项“Telnet”后，将直接启用 Telnet 功能。如果 PC 未开启 Telnet 服务，请先开启 PC 的 Telnet 服务。

1.9.3 用户管理

通过菜单项“用户管理”使用该功能。

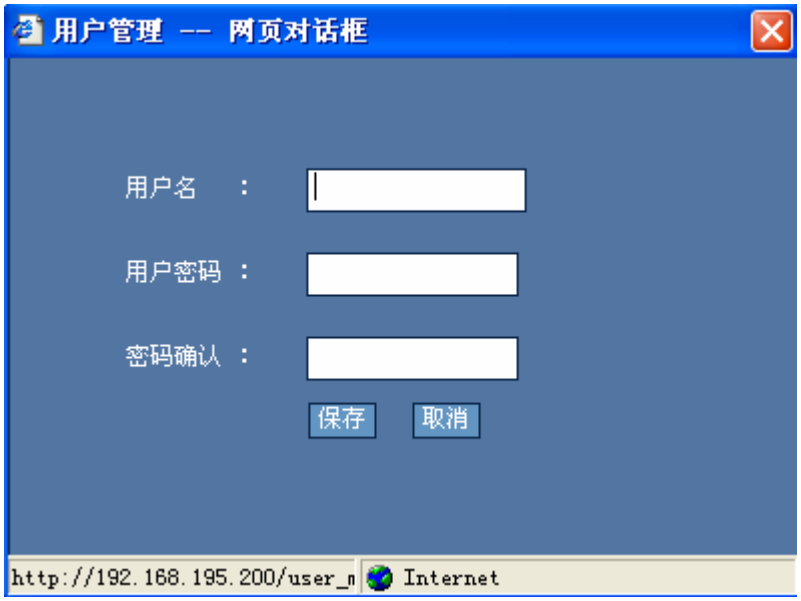
用户管理页面：

图 1-87 用户管理

配置说明：

添加用户：如果要新加用户，请点击“添加用户”按钮，将弹出如下配置页面：

图 1-88 添加用户

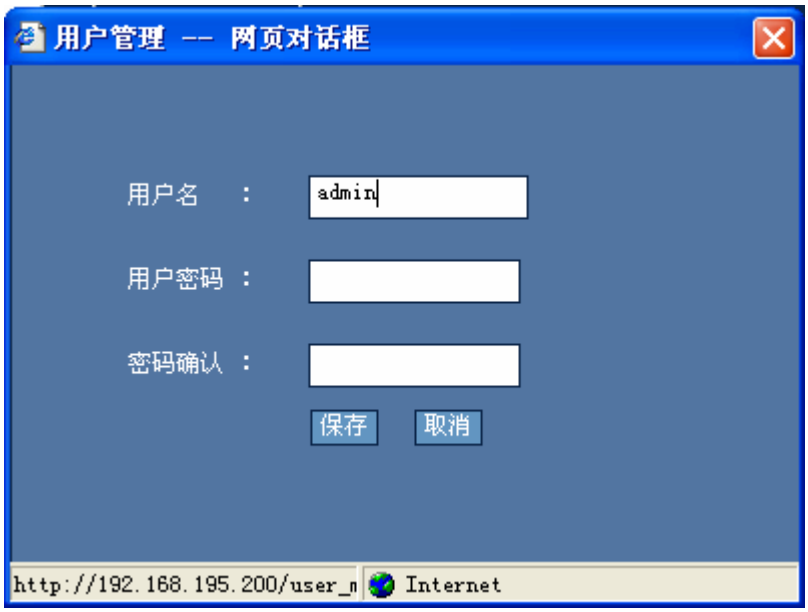


请输入用户名 和密码后按“保存”按钮使配置生效。配置成功后，新加的用户将显示在用户管理页面上。

删除：请选中要删除的用户所对应的复选框，按“删除”按钮。这时所选中的用户将被删除。

修改：请选中要修改的用户所对应的复选框，按“修改”按钮，将弹出如下配置页面：

图 1-89 修改用户



请输入用户名和密码后按“保存”按钮使配置生效。配置成功后，修改后的用户将显示在用户管理页面上。

如果删除、修改的用户名是系统登录时使用的用户名，则将会弹出认证对话框，这时请用其它用户名或修改后的用户名重新认证。如果当前系统中只有一个用户名，则将不允许删除。

1.9.4 密码设置

通过菜单项“密码设置”使用该功能。

密码设置页面：

图 1-90 密码设置

配置说明：

- 修改 Enable 口令

如果要修改 Enable 口令，请输入新口令后按“保存”按钮，使配置生效。这时将弹出：

图 1-91 登录验证对话框

请用新口令重新登录。

- 修改 Telnet 登录口令

如果要修改 Telnet 口令，请输入新口令后按“保存”按钮，使配置生效。

1.9.5 导入/导出配置

通过菜单项“导入/导出配置”使用该功能。

导入/导出配置页面：

图 1-92 导入/导出配置

配置说明：

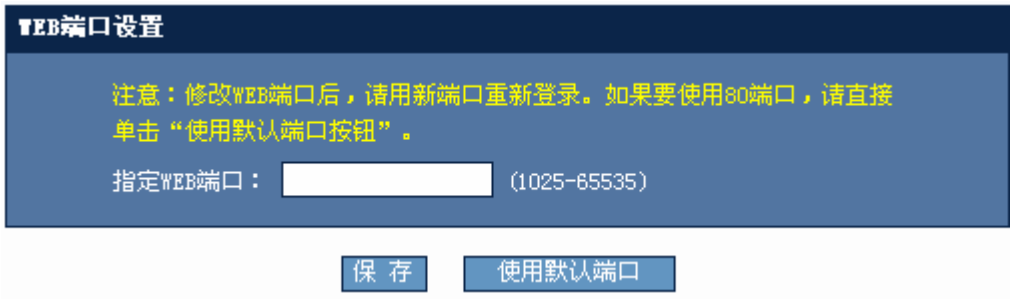
要导入、导出交换机上的 config.text 文件，请先输入 TFTP 服务器的 IP 和 TFTP 服务器上的文件名后，按“导入”按钮使设备上 config.text 文件保存到 TFTP 服务器上，按“导出”按钮使 TFTP 服务器上的指定文件保存到设备上。

1.9.6 设置WEB端口

通过菜单项“WEB 端口设置”使用该功能。

WEB 端口设置页面：

图 1-93 WEB 端口设置



配置说明：

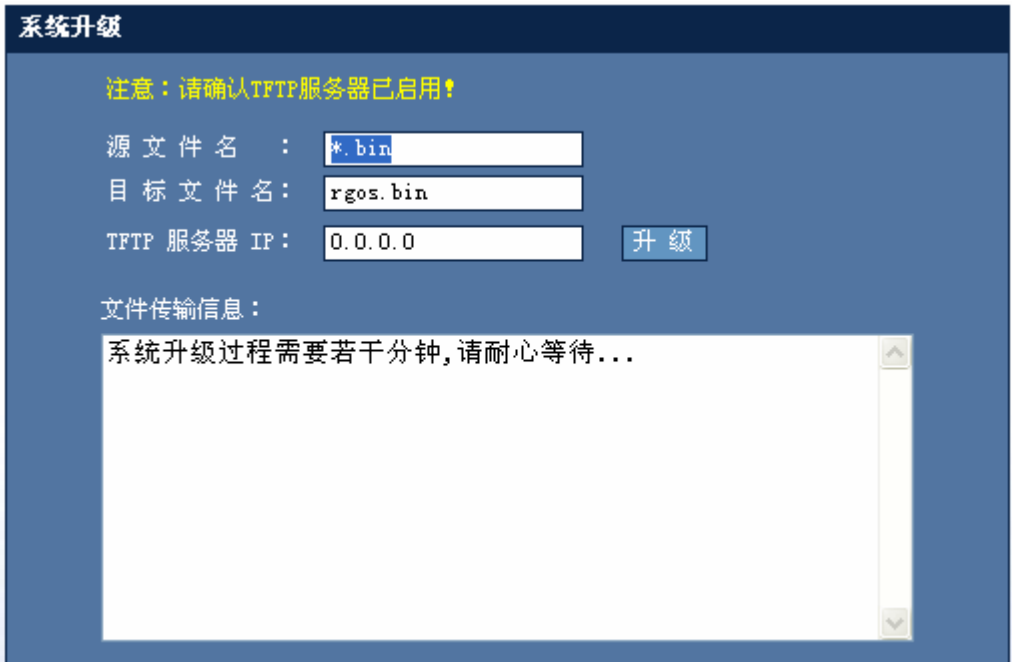
请输入合法范围内的端口后，按“保存”按钮使配置生效。端口设置完后请用新端口重新登录设备。如设新端口为 8080，设备 IP 地址为：192.168.1.1 则要用 http://192.168.1.1:8080 登录设备。如果要恢复为默认端口，请按“使用默认端口”按钮后，用 http://192.168.1.1 重新登录。

1.9.7 系统升级

通过菜单项“系统升统”使用该功能。

系统升统页面：

图 1-94 系统升统



配置说明：

要升级系统，请确认已打开了 TFTP 服务器。源文件名为 TFTP 服务器上要升级的文件，目标文件名为升级到设备上后要命名的文件名，输入 TFTP 服务器的 IP 地址后按“升级”按钮使配置生效。

1.9.8 退出系统

通过菜单项“退出系统”使用该功能。

配置说明：

当点击菜单项的“退出系统”后，将关闭浏览器窗口。

1.10 WEB管理典型配置举例

配置要点

WEB 管理在打开 WEB 服务后，默认就已配置 enable 方法进行认证。

配置步骤

WEB 管理支持 Local 方法或 Enable 方法进行登录认证，只有认证通过了，用户才可以进入 WEB 管理页面，进行 WEB 配置。

- 用 Local 方法进行登录认证

详细配置如下：

进入 config 模式

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

打开 WEB 服务

```
Ruijie(config)#enable service web-server
```

配置 WEB 管理登录认证方法为 Local 方法

```
Ruijie(config)#ip http authentication local
```

配置本地用户名（必须为 15 级用户）和密码

```
Ruijie(config)#username admin password admin
Ruijie(config)#username admin privilege 15
```

配置设备管理 IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

- 用 Enable 方法进行登录认证

详细配置如下：

进入 config 模式

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

打开 WEB 服务

```
Ruijie(config)#enable service web-server
```

配置 WEB 管理登录认证方法为 Enable 方法（该命令配置后不显示）

```
Ruijie(config)#ip http authentication enable
```

配置 Enable 密码

```
Ruijie(config)#enable password admin
```

配置设备管理 IP

```
Ruijie(config)#interface vlan 1
Ruijie(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

显示验证

- 用 Local 方法进行登录认证

```
Ruijie(config)#show running-config
Building configuration...
Current configuration : 2014 bytes
!
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009 -ngcf32)
vlan 1
username admin password admin      //WEB 管理认证用户名与密码
username admin privilege 15          //WEB 管理用户必须是 15 级用户
no service password-encryption
ip http authentication local           //WEB 管理用 local 方法进行认证
!
enable service web-server           //开启 WEB 服务
!
!
interface VLAN 1
 ip address 192.168.100.1 255.255.255.0   //设备管理 IP
 no shutdown
!
!
line con 0
line vty 0 4
 login
!
!
end
```

- 用 Enable 方法进行登录认证

```
Ruijie(config)#show running-config
Building configuration...
Current configuration : 2014 bytes
!
version RGOS 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009 -ngcf32)
vlan 1
no service password-encryption
!
enable password admin             //WEB 管理 Enable 认证密码
enable service web-server           //开启 WEB 服务
!
!
interface VLAN 1
 ip address 192.168.100.1 255.255.255.0   //设备管理 IP
```

```
 no shutdown
!
!
line con 0
line vty 0 4
 login
!
!
end
```