ZXR10 ZSR
智能集成多业务路由器
用户手册WEB GUI分册

产品版本：2.8.11

中兴通讯股份有限公司
地址：深圳市高新技术产业园科技南路中兴通讯大厦
邮编：518057
电话：(86) 755 26770800 800-830-1118
传真：(86) 755 26770801
技术支持网站：http://support.zte.com.cn
电子邮件：800@zte.com.cn

法律声明

修订历史

Revision No.	Revision Date	Revision Reason
R1.0	20081225	ZXR10 ZSR(V2.8.11)第一次发布

资料编号：sjzl20086545

发布日期：20081225

目录

前言

手册说明

本手册为《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（WEB GUI分册）》，适用于ZXR10 ZSR（V2.8.11）智能集成多业务路由器。ZXR10 ZSR的配套手册有：

- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器安装手册》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器硬件手册》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（基本配置分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（二层协议分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（路由分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（MPLS分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（安全分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（WEB GUI分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（IPv6分册）》
- 《ZXR10 ZSR（V2.8.11）智能集成多业务路由器用户手册（VOIP分册）》
- 《ZXR10 路由器/以太网交换机命令手册（命令索引分册）》
- 《ZXR10 路由器/以太网交换机命令手册（系统管理分册）》
- 《ZXR10 路由器/以太网交换机命令手册（功能体系分册一）》
- 《ZXR10 路由器/以太网交换机命令手册（功能体系分册二）》
- 《ZXR10 路由器/以太网交换机命令手册（功能体系分册三）》
- 《ZXR10 路由器/以太网交换机命令手册（功能体系分册四）》
- 《ZXR10 路由器/以太网交换机命令手册（协议栈分册一）》
- 《ZXR10 路由器/以太网交换机命令手册（协议栈分册二）》
- 《ZXR10 路由器/以太网交换机命令手册（协议栈分册三）》
- 《ZXR10 路由器/以太网交换机信息手册》

ZXR10 ZSR（V2.8.11）智能集成多业务路由器支持的命令是基于统一平台ZXROS V4.8.01版本。

内容介绍

章名	概要
第1章 WEB GUI简介	本章主要介绍了WEB GUI的功能、使用方法以及注意事项。
第2章 系统维护	本章主要介绍系统基本信息、帐号、系统时间、告警日志、端口镜像、配置保存、和重新启动。
第3章 端口管理	本章介绍端口管理，主要内容有：配置实现二层以太端口与三层以太端口的二三层切换，配置二层以太端口、三层以太端口和三层VLAN子接口的端口基本属性，以及查看以上三种接口的接口状态信息。
第4章 基本配置	本章介绍对多用途接口进行基本属性的配置，包括WAN配置、LAN配置、DHCP配置、E1配置和MPPP配置。WAN端口是接入广域网的端口，而LAN端口是接入局域网的端口。
第5章 VLAN管理	本章主要介绍了ZXR10 ZSR路由器中的VLAN的配置以及在VLAN中添加和删除pvidport、tagport和untagport端口的操作。
第6章 NAT配置	本章主要介绍NAT功能，通过配置私网地址/端口和公网地址/端口的对应关系，从而实现私网和公网的互相访问。
第7章 静态路由	本章主要介绍如何查看已经配置过的静态路由，添加新的静态路由和删除静态路由。
第8章 流过滤器配置	本章主要介绍了标准流过滤器和扩展流过滤器的规则以及配置方法。
第9章 QoS配置	本章主要介绍PQ和CAR的配置方法。
第10章 VPN配置	本章主要介绍L2TP VPN和IPSEC VPN的配置方法。其中L2TP VPN根据业务类型分为LAC业务和LNS业务属性配置。
第11章 防火墙配置	本章主要介绍防火墙一些常用业务的配置方法

1 WEB GUI简介

本章包含如下主题：

1.1 软件简介

WEB GUI是利用WEB浏览器软件通过HTTP协议对路由器进行配置管理，代替以往在超级终端模式下繁琐的命令行配置方式，从而使用户对路由器的配置管理更加实用、简单，实现控制系统和使用设备所提供的功能的作用。

使用前的操作步骤：

1. 打开超级终端，在全局配置模式下输入命令web enable，开启WEB GUI功能；
2. 配置用户名；
3. 在WEB浏览器地址栏输入用户配置的业务口地址，如http://192.168.0.1/；
4. 进入登录页面，依据提示框输入路由器已存在的用户名和密码，便可进入路由器WEB配置界面完成相关配置。

1.2 注意事项

- WEB GUI不支持IPv6地址的配置和显示。
- WEB GUI不支持一些特殊字符，比如：\、“”、‘’、？、空格的输入和显示。
- 如果一段时间（十分钟左右）不操作页面，再进行操作时会弹出一个超时页面，如图1−1所示。数秒后，会自动跳转到登录页面，用户只要重新输入用户名和密码再次登录即可使用。

图1-1 超时页面


Error Infomation
Time out or bad request!
This page will jump to login page in three seconds ..
login

2 系统维护

本章包含如下主题：

2.1 查看系统基本信息

步骤

1. 进入路由器WEB配置界面。
2. 选择导航栏菜单[**系统维护→系统基本信息**]，进入**系统基本信息**界面，如图2−1所示。

图2-1 系统基本信息界面

界面说明：

- 设备型号：当前设备的类型
- 版本号：版本编号
- 编译时间：版本编译时间
- 系统运行时间：系统运行时间

--步骤结束--

2.2 用户帐号设置

选择导航栏菜单[**系统维护→帐号**]，进入**用户显示**界面，如图2-2所示。

图2-2 用户显示界面

2.2.1 添加用户帐号

步骤

1. 单击图2-2界面上的**添加新用户**按钮，进入**用户添加**界面，如图2-3所示。

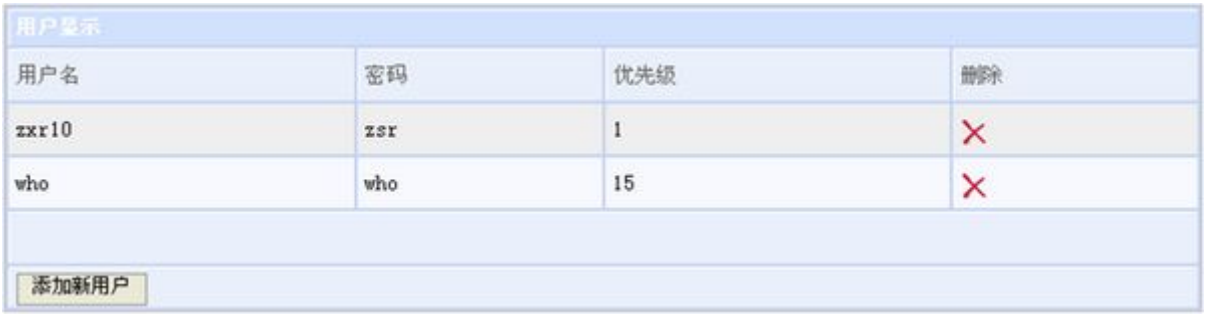
图2-3 用户添加界面

界面说明：

- 用户名：1~32个字符，一般是由数字、字母、下划线组成，不能包含中文字符。
- 用户管理权限：用户优先级。
- 密码：3~32个字符，一般是由数字、字母、下划线组成，不能包含中文字符。
- 确认密码：必须与密码相同。

2. 配置成功后，单击**应用**按钮，返回**用户显示**界面，如图2-4所示。

图2-4 用户显示界面



NOTE **说明：**

当用户账号条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

2.2.2 删除用户帐号

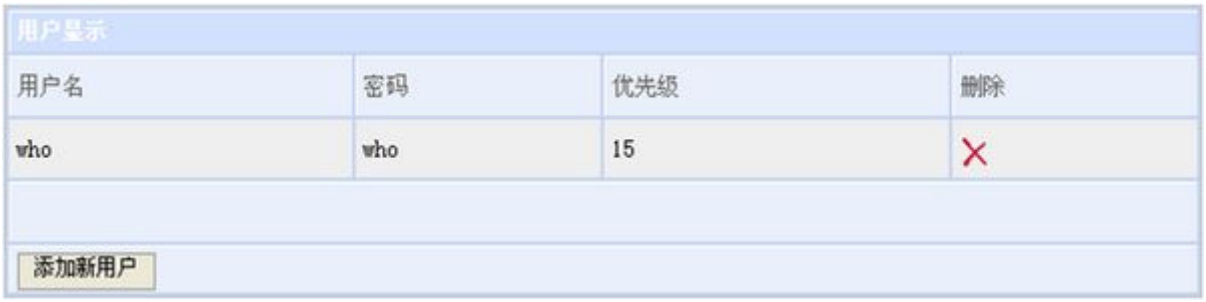
步骤

1. 单击**用户显示**界面图2-4中的**删除**按钮，会出现**确认删除用户**对话框（以zxr10为例），如图2-5所示。

图2-5 用户帐号删除提示界面

2. 单击**确定**按钮，删除成功后，返回**用户显示**界面，如图2-6所示。

图2-6 用户删除后显示界面



--步骤结束--

2.3 系统时间设置

选择导航栏菜单[**系统维护→系统时间**]，进入**时间显示**界面，如图2-7所示。

图2-7 系统时间显示界面

2.3.1 自动设置时间

步骤

1. 单击**时间显示**界面图2-7上的**设置**按钮，弹出**时间设置**界面，如图2-8所示。

图2-8 系统时间设置界面

2. 选中**电脑当前时间**前的单选框，单击**应用**按钮，应用成功后，返回**时间显示**界面，如图2-9所示。

图2-9 系统时间显示界面

--步骤结束--

2.3.2 手动设置时间

步骤

1. 进入**时间设置**界面图2-8
2. 在**时间设置**界面中，选中**手动设置时间**前的单选框，显示**手动设置时间**界面，设置完成后，单击**应用**按钮，返回**时间显示**界面，如图2-10所示。

图2-10 手动设置时间界面

界面说明：

- 日期设置：单击**选择日期**按钮，选择需要设置的日期。
- 时：范围0~23，24小时制。
- 分：范围0~59。
- 秒：范围0~59。

--步骤结束--

2.4 告警日志设置

告警日志用于查看路由器上发生的告警信息及接口状态变化。日志信息为我们对路由器进行日常维护提供了方便。

选择导航栏菜单[**系统维护→告警日志**]，进入**告警日志设置**界面，如图2-11所示。

图2-11 告警日志设置界面

界面说明：

- Syslog发送源端口：范围0~65535，默认值为514。
- Syslog发送目的端口：范围0~65535，默认值为514。

2.4.1 设置告警日志

步骤

1. 启用日志开关

   在**告警日志设置**界面图2-11中，选中**启用**前的单选框，会弹出**确认启用日志开关**对话框，如图2-12所示。

图2-12 确认启用日志开关对话框

若要禁用告警日志，选中**告警日志设置**界面中**禁用**前的单选框即可。

2. 配置Syslog源IP地址

在**Syslog源IP地址**中输入地址，单击**应用**按钮，配置成功。若单击**删除**按钮，则文本框置空，删除成功。如图2-13所示。

图2-13 Syslog源IP地址配置界面

--步骤结束--

2.4.2 配置Syslog服务器

步骤

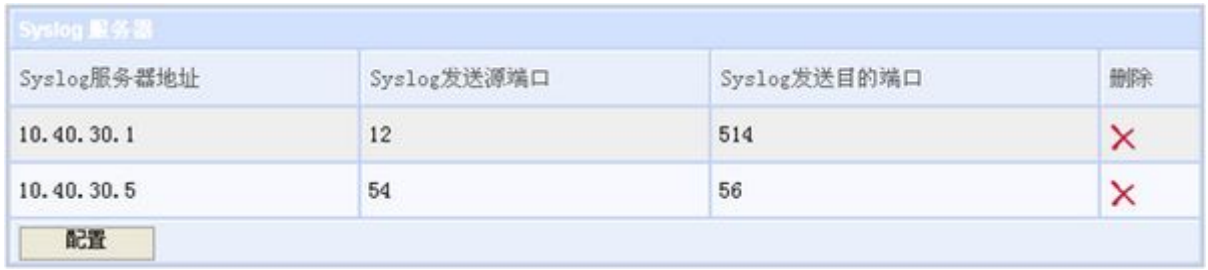
1. 配置Syslog服务器

a. 单击**告警日志设置**界面图2-11中**Syslog服务器**区域框中的界面中的**配置**按钮，进入**Syslog服务器设置**界面，如图2-14所示。

图2-14 Syslog服务器配置界面

b. 配置完成后，单击**应用**按钮，返回**Syslog服务器显示**界面，如图2-15所示。

图2-15 Syslog服务器显示界面



2. 删除Syslog服务器

单击图2-15界面中的**删除**按钮，会弹出对话框，单击**确认**按钮即可删除Syslog服务器，如图2-16所示。

图2-16 Syslog服务器删除后显示界面

--步骤结束--

2.5 配置端口镜像

相关信息

端口镜像是指将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析。被监控流量所在端口称为源端口，监控端口称为目的端口，目的端口直接与网络分析器相连。

步骤

1. 选择导航栏菜单[**系统维护→端口镜像**]，进入**端口镜像显示**界面，如图2-17所示。

图2-17 端口镜像显示界面

界面说明：

- 会话号：范围1~64。
- 镜像方式：目前只支持“Mirror”方式。
- 镜像方向：有三种，分别为“TX”（源端口出方向）、“RX”（源端口入方向）和“BOTH”（源端口出方向和入方向）。

2. 在图2-17界面的**端口镜像**区域框中，选中**打开**前的单选框，会弹出**镜像开关打开确认**界面，如图2-18所示。

图2-18 镜像开关打开确认界面

3. 单击**确定**按钮即可打开端口镜像。

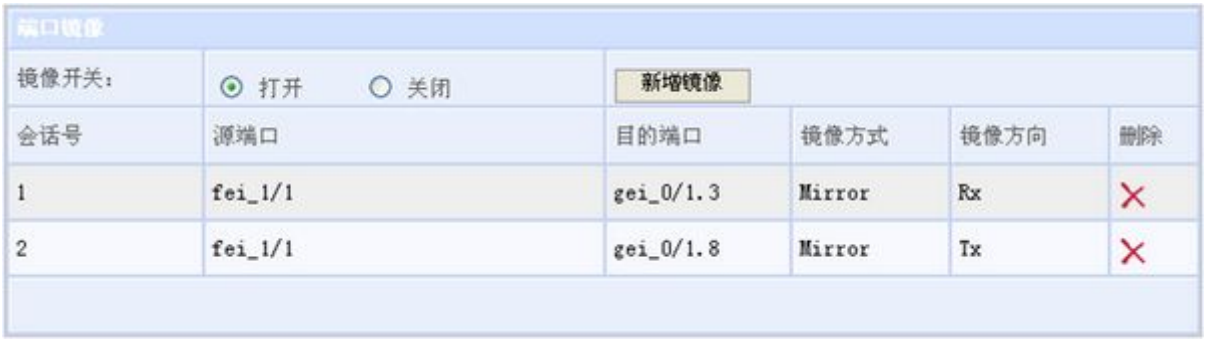
若要关闭端口镜像，可以选中**端口镜像**区域框中**关闭**前的单选框。

4. 配置端口镜像

单击图2-18中的**新增镜像**按钮，进入**端口镜像配置**界面，如图2-19所示。配置完成后，单击**应用**按钮，返回**端口镜像显示**界面，如图2-20所示。

图2-19 端口镜像配置界面

图2-20 端口镜像显示界面



NOTE **说明：**

当端口镜像条目超过64条时，将采用分页显示，每页最多显示64个条目。

5. 删除端口镜像

单击图2-20界面中的**删除**按钮，会弹出对话框，单击**确认**按钮即可删除端口镜像，如图2-21所示。

图2-21 端口镜像删除后显示界面

--步骤结束--

2.6 保存配置

步骤

1. 选择导航栏菜单[**系统维护→配置保存**]，进入**配置保存**界面，如图2-22所示。

图2-22 配置保存界面

2. 在图2-22界面中，单击**配置保存**按钮，弹出**配置保存成功**界面，保存成功，如图2-23所示。

图2-23 配置保存成功界面

--步骤结束--

2.7 重新启动设备

步骤

1. 选择导航栏菜单[**系统维护→重新启动**]，进入**系统重启**界面，如图2-24所示。

图2-24 系统重启界面

2. 选中**重启设备并保存当前配置**前的单选框，可以重新启动设备并保存配置。

若选中**重启设备但不保存当前配置**前的单选框，则可以重新启动设备，但不保存当前配置。

--步骤结束--

3 端口管理

本章包含如下主题：

3.1 二层以太端口配置

选择导航栏菜单[**端口管理→二层以太端口**]，进入**二层以太端口显示**界面，如图3-1所示。

图3-1 二层以太端口显示界面

界面说明：

- 端口速率：显示端口的配置速率，取值为“10M”、“100M”、“1000M”。
- 双工模式：分为“Full”（全双工）或“Half”（半双工）。

- 广播抑制：端口对广播报文的速率限制，速率范围百兆口（1~100）Mbps，千兆口（1~1000）Mbps。
- 组播抑制：端口对组播报文的速率限制，速率范围百兆口（1~100）Mbps，千兆口（1~1000）Mbps。
- 交换模式：有三种链路类型，“Access”、“Hybrid”和“Trunk”。
- 配置：点击表内的按钮，可以对该端口的基本属性进行配置。
- 统计：点击表内的按钮，可以查看该接口的统计信息。

3.1.1 配置端口二层到三层切换

步骤

1. 在**二层以太端口显示**界面图3-1的**请选择槽位号**下拉列表框中，选择需要转换的槽位号。
2. 单击**应用**按钮，可以完成二层到三层的切换，如图3-2所示。

图3-2 端口二层到三层切换配置界面

NOTE **说明：**

当机架类型为ZXR10 1809时，仅支持在端口模式下切换至三层，需进入端口配置进行配置；其他类型机架仅支持在全局配置模式下整个槽位切换至三层。

--步骤结束--

3.1.2 配置二层以太端口

步骤

1. 在**二层以太端口显示**界面图3-1中，点击端口所对应的**配置**按钮，进入该端口对应的配置界面，如图3-3所示。

图3-3 二层以太端口基本配置界面

界面说明：

- 端口描述：描述该端口的实际用途等信息。
- 管理状态：接口的管理状态是否可用，“UP”表示可用，“DOWN”表示不可用。
- 交换模式：根据需要可以选择配置三种链路类型，“Access”、“Hybrid”和“Trunk”。
- 广播抑止：端口对广播报文的限制速率，可配范围为，百兆口（1~100）Mbps，千兆口（1~1000）Mbps。
- 组播抑止：端口对组播报文的限制速率，可配范围为，百兆口（1~100）Mbps，千兆口（1~1000）Mbps。
- 自动协商：选择“Enable”为自动协商，“Disable”为非自动协商，自动协商时不能够配置端口速率。

- 双工工作模式：配置端口的双工模式，可以选择“Full”（全双工）或“Half”（半双工）。
- 端口速率：配置端口的速率，值可以选择“10M”、“100M”、“1000M”。

2. 配置完端口属性后，单击图3-3中的**应用**按钮，配置字段生效，并返回到**二层以太端口配置状态**界面；

   若单击**返回**按钮，则立即返回到**二层以太端口配置状态**界面，并且已经填写的属性字段将不会生效。

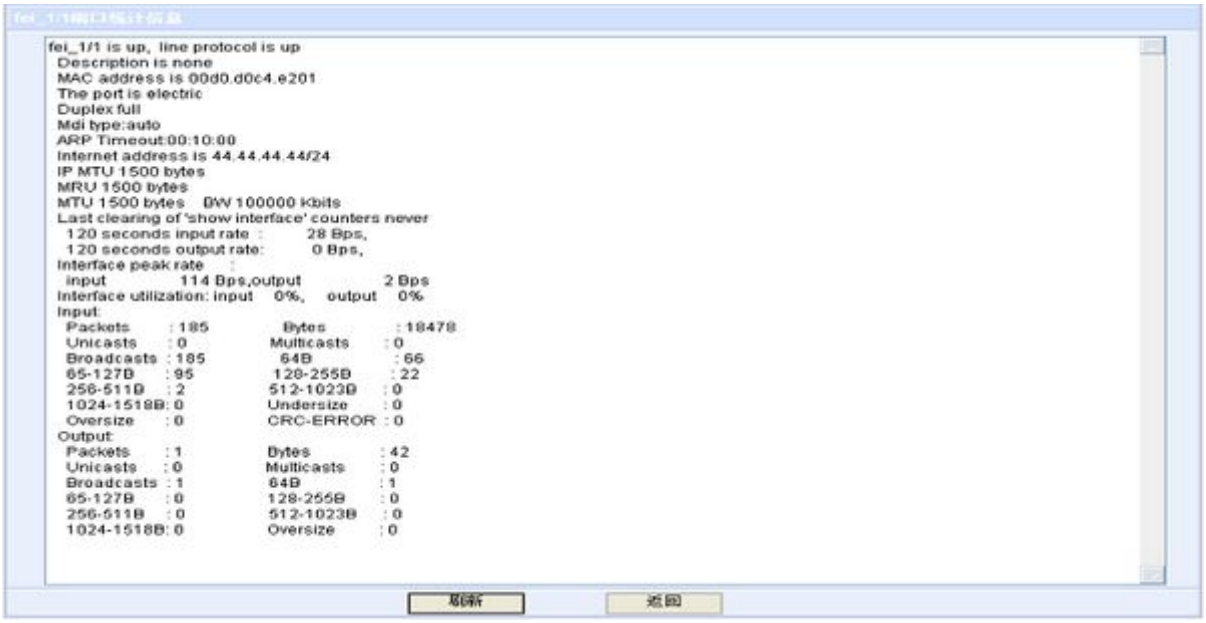
--步骤结束--

3.1.3 查看二层以太端口统计信息

步骤

1. 在**二层以太端口显示**界面图3-1中，点击端口所对应的**统计**按钮，进入该端口对应的统计信息界面，如图3-4所示。

图3-4 二层以太端口统计信息界面



该端口统计信息主要包含：接口的物理状态和协议状态、接口速率、协商模式、双工工作模式、接口的MTU值和收发包的速率及数目。

2. 单击**刷新**按钮，获得最新的接口统计信息；

   若单击**返回**按钮，则可以返回到**二层以太端口显示**界面。

--步骤结束--

3.2 三层以太端口配置

选择导航栏菜单[**端口管理→三层以太端口**]，进入**三层以太端口显示**界面，如图3-5所示。

图3-5 三层以太端口显示界面

界面说明：

- 请选择槽位号：在下拉列表框中选择需要将三层切换到二层的槽位号。
- 端口：对应端口的名称。
- 接口属性：显示该接口的属性信息，值为“Null”、“WAN”、“LAN”。
- 管理状态：接口的管理状态是否可用，“UP”表示可用，“DOWN”表示不可用。
- IP地址：该接口的IP地址。
- 端口速率：显示端口的配置速率，值为“10M”、“100M”、“1000M”。
- 双工模式：分为“Full”（全双工）或“Half”（半双工）。
- 最大传输单元：即MTU，该接口所能传输的最大报文长度。
- 自动协商：显示该接口的协商模式，值为“enable”表示自动协商，值为“disable”表示非自动协商。
- MAC地址：显示该接口的MAC地址。
- 配置：点击表内的按钮，对该端口进行相关属性配置。
- 创建子接口：点击表内的按钮，可以在该实接口下创建子接口。
- 统计：点击表内的按钮，可以查看该接口的统计信息。

3.2.1 配置端口三层到二层切换

步骤

1. 在**三层以太端口显示**界面图3-5的**请选择槽位号**下拉列表框中，选择需要转换的槽位号。
2. 单击**应用**按钮，可以完成三层到二层的切换，如图3-6所示。

图3-6 端口三层到二层切换配置图

NOTE **说明：**

当机架类型为ZXR10 1809时，仅支持在端口模式下切换至二层，需进入端口配置进行配置；其他类型机架仅支持在全局配置模式下整个槽位切换至二层。

--步骤结束--

3.2.2 配置三层以太端口

步骤

1. 在**三层以太端口显示**界面图3-5中，点击端口所对应的**配置**按钮，进入该端口对应的配置界面，如图3-7所示。

图3-7 三层以太端口基本配置图

界面说明：

- 端口描述：描述该端口的用途。
- 接口属性：配置该接口的属性信息，可选值为“Null”、“WAN”、“LAN”。
- 管理状态：接口的管理状态是否可用，“UP”表示可用，“DOWN”表示不可用。
- 最大传输单元：配置该接口所能传输的最大报文长度，配置范围为（128~1500）bytes。
- 自动协商：选择“Enable”为自动协商，“Disable”为非自动协商，自动协商时不能够配置端口速率。
- 双工工作模式：配置端口的双工模式，可以选择“Full”（全双工）或“Half”（半双工）。
- 端口速率：配置端口的速率，值可以选择“10M”、“100M”、“1000M”。

2. 配置完端口属性后，单击图3-7中的**应用**按钮，配置字段生效，并返回到**三层以太端口显示**界面；

若单击**返回**按钮，则立即返回到**三层以太端口显示**界面，并且已经填写的属性字段将不会生效。

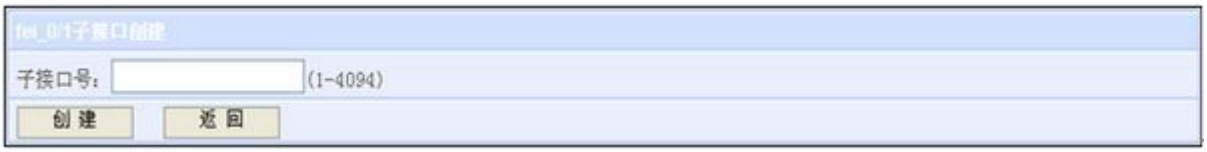
--步骤结束--

3.2.3 配置子接口

步骤

1. 在**三层以太端口显示**界面图3-5中，点击端口所对应的**创建子接口**按钮，进入创建子接口的配置界面。如图3-8所示。

图3-8 三层以太端口创建子接口配置图



2. 在**子接口号**输入框中输入要创建的子接口的接口号，子接口号范围为1~4094。
3. 单击**创建**按钮，进入**三层VLAN子接口配置**界面，如图3-9所示。

图3-9 三层以太端口子接口配置界面

界面说明：

- 端口描述：描述VLAN子接口的信息，描述字符最多为100个非中文字符，不能含有字符“\”。
- 接口属性：可选值为“Null”、“LAN”、“WAN”。
- 管理状态：接口的管理状态是否可用，“UP”表示可用，“DOWN”表示不可用。

- Vlan ID：该子接口的Vlan ID号，范围为1~4096。
- 最大传输单元：该子接口所能传输的最大报文长度，范围为128~1500bytes。

4. 完成子接口属性配置后，单击按钮，则进入**三层VLAN子接口状态**界面，如图3-10所示。

图3-10 三层VLAN子接口状态界面

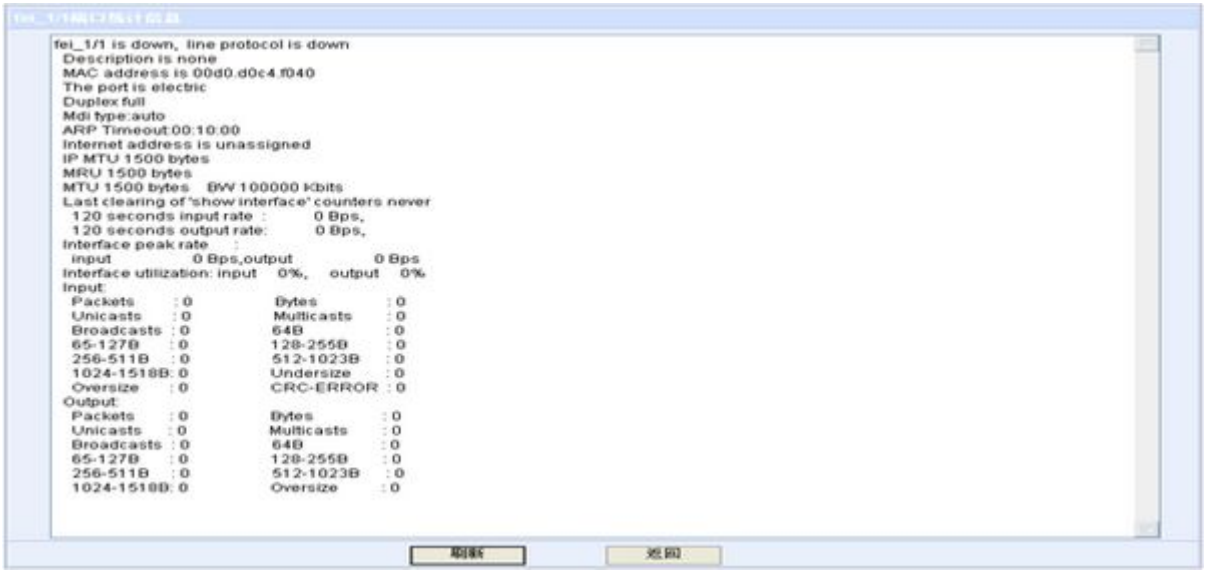
--步骤结束--

3.2.4 查看三层以太端口统计信息

步骤

1. 在**三层以太端口显示**界面图3-5中，点击端口所对应的**统计**按钮，进入该端口对应的统计信息界面，如图3-11所示。

图3-11 端口统计信息图



该端口统计信息主要包含：接口的物理状态和协议状态、接口速率、协商模式、双工工作模式、接口的MAC地址、接口的MTU值、收发包的速率及数目。

2. 单击**刷新**按钮，获得最新的接口统计信息；

若单击**返回**按钮，则可以返回到**三层以太端口显示**界面。

--步骤结束--

3.3 三层VLAN子接口配置

选择导航栏菜单[**端口管理→三层VLAN子接口**]，进入**三层VLAN子接口显示**界面，如图3-12所示。

图3-12 三层VLAN子接口显示界面

界面说明：

- 端口名：对应端口的名称。
- 接口属性：显示该接口的属性信息，值为“Null”、“WAN”、“LAN”。
- 管理状态：接口的管理状态是否可用，“UP”表示可用，“DOWN”表示不可用。
- IP地址：该接口的IP地址。
- 最大传输单元：即MTU，该接口所能传输的最大报文长度。
- Vlan ID：显示该子接口的VlanID号。
- 配置：点击表内的按钮，对该端口进行相关属性配置。
- 删除：点击表内的按钮，可以删除该子接口。
- 统计：点击表内的按钮，可以查看该接口的统计信息。

3.3.1 配置三层VLAN子接口

步骤

1. 在**三层VLAN子接口显示**界面图3-12中，点击相应端口（以fei_0/1.1为例）所对应的**配置**按钮，进入**三层VLAN子接口配置**界面，如图3-13所示。

图3-13 三层VLAN子接口配置界面

2. 在**三层VLAN子接口配置**界面的各输入框中输入相应参数。例如在**Vlan ID**输入框中输入**100**。
3. 单击**应用**按钮，使配置的子接口属性生效，配置完成返回界面如图3-14所示。

图3-14 三层VLAN子接口配置返回显示界面

端口名	接口属性	管理状态	IP 地址	最大传输单元	Vlan ID	配置	删除	统计
fei_0/1.1	NULL	up	--	1500	100			
fei_0/1.2	NULL	up	--	1500	--			
gei_0/3.2	NULL	up	--	1500	--			

--步骤结束--

3.3.2 删除三层VLAN子接口

步骤

1. 在**三层VLAN子接口显示**界面图3-12中，点击该子接口所对应的**删除**按钮（以fei_0/1.1为例），弹出**确认删除端口**对话框，如图3-15所示。

图3-15 三层VLAN子接口删除确认对话框

2. 若确定删除该子接口，单击**确定**按钮；若不删除该子接口，则单击**取消**按钮。
3. 子接口删除成功，返回到**三层VLAN子接口显示**界面，如图3-16所示，可以看到子接口fei_0/1.1已经被删除。

图3-16 三层VLAN子接口删除成功界面

三层Vlan子接口显示

端口名	接口属性	管理状态	IP 地址	最大传输单元	Vlan ID	配置	删除	统计
fei_0/1.2	NULL	up	--	1500	--			
gei_0/3.2	NULL	up	--	1500	--			

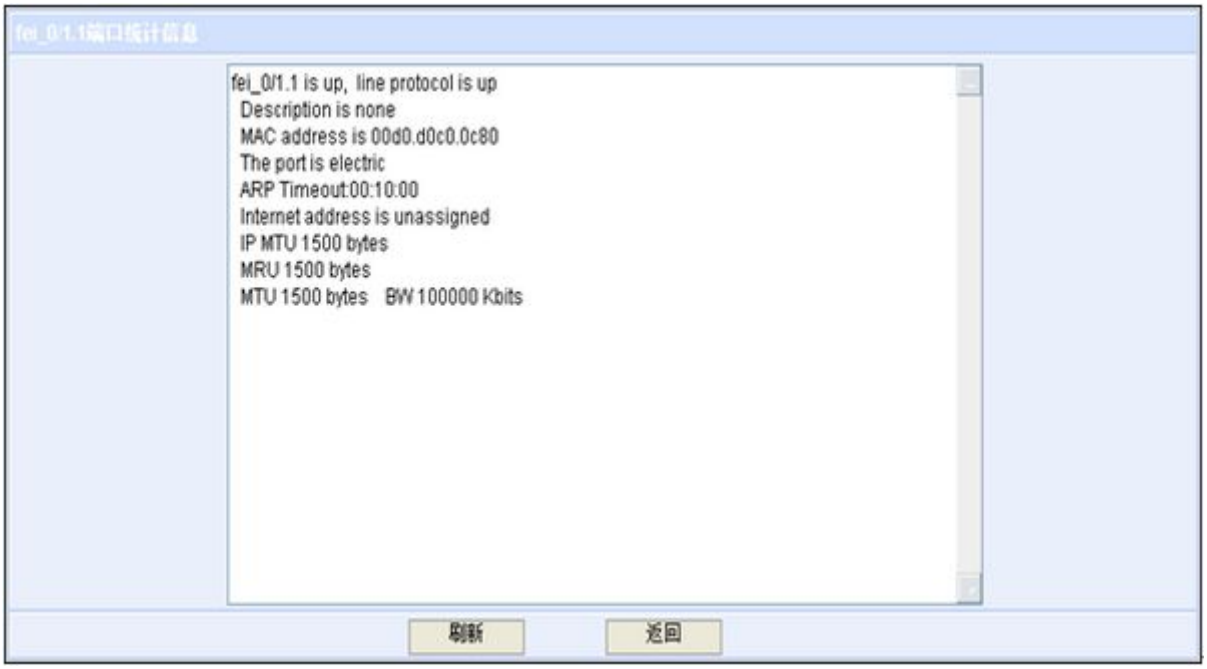
--步骤结束--

3.3.3 查看三层VLAN子接口统计信息

步骤

1. 在**三层VLAN子接口显示**界面图3-12中，点击子接口所对应的**统计**按钮，进入该子接口对应的统计信息界面，如图3-17所示。

图3-17 三层VLAN子接口统计信息图



该接口统计信息主要包含：接口的物理状态和协议状态、接口速率、协商模式、双工工作模式、接口的MAC地址和接口的MTU值。

2. 单击**刷新**按钮，获得最新的接口统计信息；

   若单击**返回**按钮，则可以返回到**三层VLAN子接口显示**界面。

--步骤结束--

4 基本配置

本章包含如下主题：

4.1 配置WAN

步骤

1. 选择导航栏菜单[**基本配置→WAN配置**]，进入**WAN显示配置**界面，如图4-1所示。

图4-1 WAN显示配置界面

界面说明：

- WAN端口：配置为WAN类型的物理端口的端口号。
- 地址：该端口的IP地址。
- 地址掩码：端口配置的IP地址掩码。
- 地址获取方式：端口IP地址的获取方式，显示为“手动设置”或“动态获取”。
- ADSL拨号：表示该端口是否启用ADSL拨号，显示为“ON”或“OFF”。
- 配置：点击对应的按钮，可以添加或更改接口的配置。

2. 点击端口所对应的**配置**按钮，会弹出**端口配置**界面，首先选择该端口的线路类型，如图4-2所示。

图4-2 线路类型选择

- 在**线路类型选择**区域框中，选中**以太网（静态IP）**前的单选框，进入以太网（静态IP）配置，具体请参见4.1.1 配置以太网静态IP地址。
- 在**线路类型选择**区域框中，选中**以太网（动态IP）**前的单选框，进入以太网（动态IP）配置，具体请参见4.1.2 配置以太网动态IP地址。
- 在**线路类型选择**区域框中，选中**ADSL（PPPoE）**前的单选框，进入ADSL配置，具体请参见4.1.3 配置ADSL。

NOTE **说明：**

需先在端口管理中配置接口属性为WAN，才能进行WAN配置。

--步骤结束--

4.1.1 配置以太网静态IP地址

步骤

1. 在**端口配置**界面的**线路类型选择**区域框中，选中**以太网（静态IP）**前的单选框。如图4-3所示。

图4-3 以太网静态IP地址配置界面

2. 在**IP地址**输入框中输入该端口的IP地址。
3. 在**子网掩码**输入框中输入网段对应的子网掩码。
4. 单击**应用**按钮，字段配置生效，跳转到**WAN显示配置**界面，属性更新；

   若单击**返回**按钮，则字段配置不生效，界面跳转到**WAN显示配置**界面，如图4-1所示；

   在静态IP地址已经配置生效的情况下，单击**删除**按钮，该端口的静态IP地址会被删除，并跳转到**WAN显示配置**界面。

   --步骤结束--

4.1.2 配置以太网动态IP地址

步骤

1. 在**端口配置**界面的**线路类型选择**区域框中，选中**以太网（动态IP）**前的单选框。如图4-4所示。

图4-4 以太网动态IP地址配置界面

2. 单击**应用**按钮，端口获取IP地址的方式设置为“动态获取”，并跳转到**WAN显示配置**界面；

   若单击**返回**按钮，则端口保持原有的IP地址获取方式不变，并跳转到**WAN显示配置**界面。

   --步骤结束--

4.1.3 配置ADSL

步骤

1. 在**端口配置**界面的**线路类型选择**区域框中，选中**ADSL（PPPoE）**前的单选框。如图4-5所示。

图4-5 ADSL配置界面

界面说明：

- 用户名：ADSL拨号帐号的用户名。
- 密码：ADSL拨号帐号的密码。
- 空闲时间：在时间段内，如果没有数据传输，则自动断开拨号连接。
- 拨号方式：可以选择为“永久在线”或“按需”。

2. 单击**应用**按钮，字段配置生效，界面跳转到**WAN显示配置**界面，端口属性更新；

   若单击**返回**按钮，则字段配置不生效，界面跳转到**WAN显示配置**界面；

在ADSL配置生效的情况下，单击**删除**按钮，所配置的内容将被删除，并跳转到**WAN显示配置**界面。

--步骤结束--

4.2 配置LAN

步骤

1. 选择导航栏菜单[**基本配置→LAN配置**]，进入**LAN显示配置**界面，如图4-6所示。

图4-6 LAN端口显示配置界面

2. 点击端口对应的**配置**按钮，进入**LAN端口配置**界面，如图4-7所示。

图4-7 LAN端口配置界面

3. 配置静态IP地址，具体请参见4.1.1 配置以太网静态IP地址；

   配置动态IP地址，具体请参见4.1.2 配置以太网动态IP地址。

NOTE **说明：** 需先在端口管理中配置接口属性为LAN，才能进行LAN配置。

--步骤结束--

4.3 配置DHCP

步骤

1. 选择导航栏菜单[**基本配置→DHCP配置**]，进入**DHCP显示配置**界面，如图4-8所示。

图4-8 DHCP显示配置界面

界面说明：

- DHCP开关：通过单选按钮选择DHCP功能的启用和关闭。
- DNS主服务器：DHCP服务器返回给用户的主DNS服务器地址。
- DNS辅服务器：DHCP服务器返回给用户的备用DNS服务器地址。
- 端口名：配置DHCP的端口号。
- 端口类型：该端口上启用的DHCP类型，值为“server”或“relay”。
- 查看：点击对应的按钮可以查看该端口下的DHCP配置信息。

2. 配置DNS主服务器地址和DNS辅服务器地址（可选）。
3. 单击**应用**按钮，DNS服务器字段配置生效。

   在DNS服务器已经配置生效的情况下，单击**删除**按钮，DNS服务器地址会被清空。

   --步骤结束--

4.3.1 配置DHCP服务器

步骤

1. 在图4-8**DHCP显示配置**界面中，单击按**新增**钮进入**DHCP服务器添加**界面，如图4-9所示。

图4-9 DHCP服务器添加界面

界面说明：

- 接口名：启用DHCP功能的接口。
- DHCP类型：根据环境需要可选为“服务器”或“中继器”。
- DHCP网关地址：DHCP服务器负责分配地址的接口的IP地址。
- DHCP地址池起始地址：DHCP服务器分配地址的起始IP地址。
- DHCP地址池截止地址：DHCP服务器分配地址的截止IP地址。
- DHCP地址池掩码：划定DHCP分配地址的有效范围。

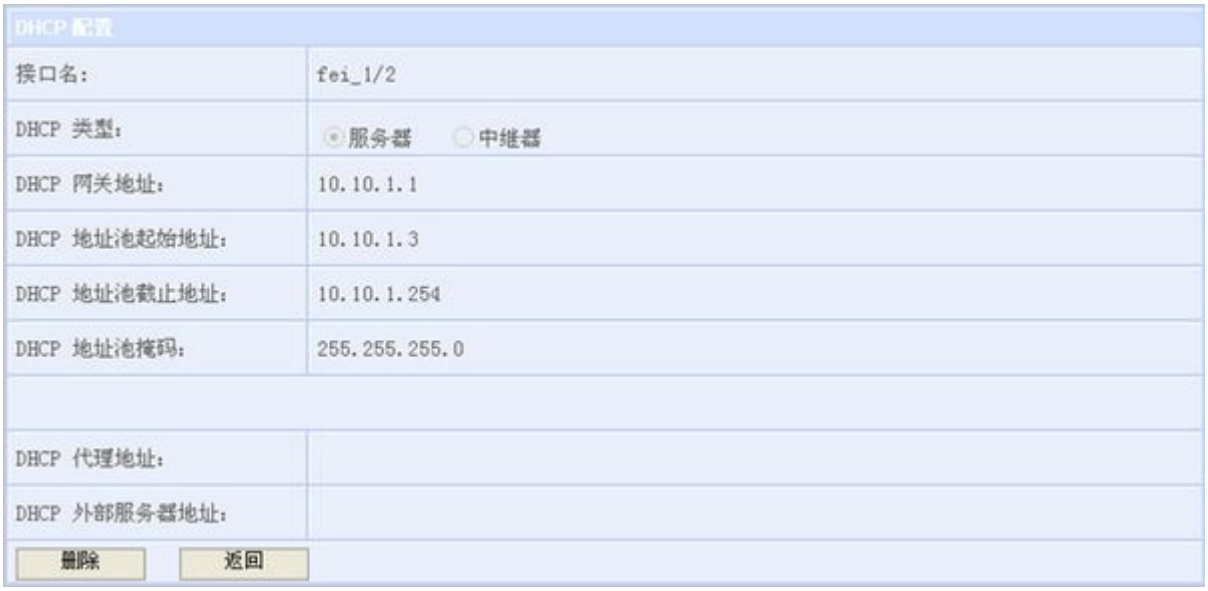
2. 在**DHCP类型**区域框中，选中**服务器**前的单选框击，开始填写DHCP服务器对应的配置字段。
3. 单击**应用**按钮，字段配置生效，**DHCP显示配置**界面内容更新，如图4-10所示；

   若单击**返回**按钮，则字段配置不生效，返回到**DHCP显示配置**界面，如图4-8所示。

图4-10 DHCP服务器完成添加界面

4. 单击图4-10中对应的**查看**按钮，可以看到DHCP服务器配置的详细信息，如图4-11所示。

图4-11 DHCP服务器配置具体信息界面



5. 在图4-11中单击**返回**按钮，可以返回到**DHCP显示配置**界面；

若单击**删除**按钮，则删除DHCP服务器配置，并返回到**DHCP显示配置**界面。

--步骤结束--

4.3.2 配置DHCP中继器

步骤

1. 在图4-8所示的**DHCP显示配置**界面中，单击**新增**按钮进入**DHCP服务器添加**界面，如图4-12所示。

图4-12 DHCP中继器配置界面

界面说明：

- 接口名：启用DHCP功能的接口。
- DHCP代理地址：接入代理的IP地址。
- DHCP外部服务器地址：DHCP外部服务器的IP地址。

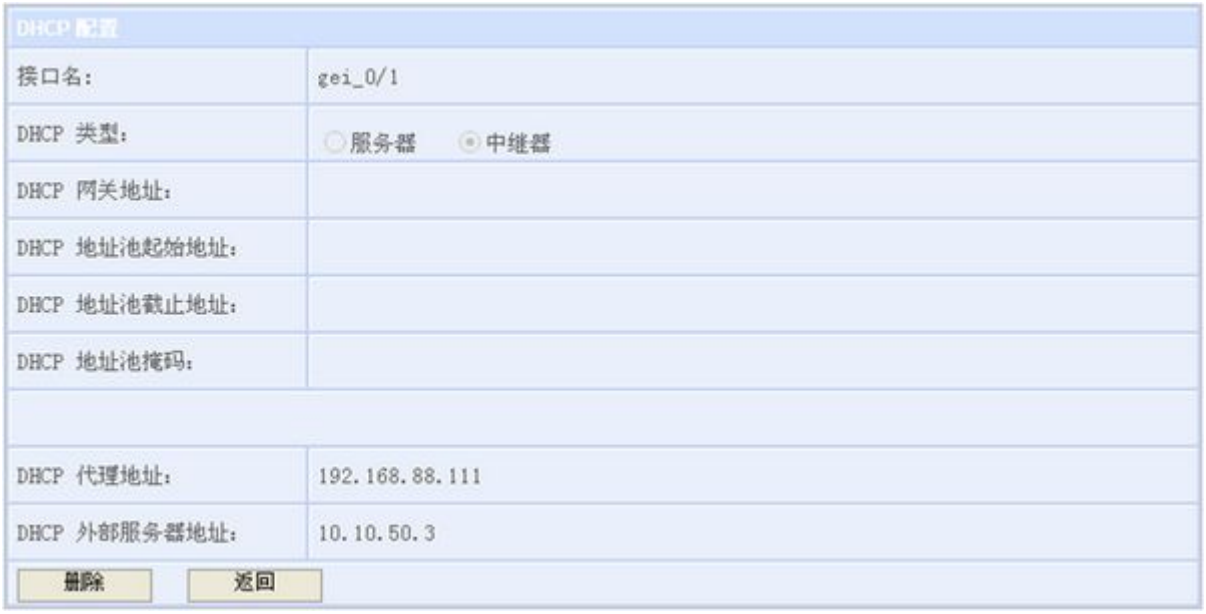
2. 在**DHCP类型**区域框中，选中**中继器**前的单选框，开始填写DHCP中继器对应的配置字段。
3. 单击**应用**按钮，字段配置生效，**DHCP显示配置**界面内容更新，如图4-13；

   若单击**返回**按钮，则字段配置不生效，返回到**DHCP显示配置**界面。

图4-13 DHCP中继器完成添加界面

4. 单击图4-13中对应的**查看**按钮，可以看到DHCP中继器配置的具体信息，如图4-14所示。

图4-14 DHCP中继器配置具体信息界面



5. 单击**返回**按钮，可以返回到**DHCP显示配置**界面；

若单击**删除**按钮，则删除DHCP中继器配置，并返回到**DHCP显示配置**界面。

--步骤结束--

4.4 配置E1

步骤

1. 选择导航栏菜单[**基本配置→E1配置**]，进入**E1信息显示配置**界面，如图4-15所示。

图4-15 E1信息显示配置界面

界面说明：

- 接口名：当前设备中E1接口的接口号。
- 帧方式：配置的成帧模式，值为“成帧”（frame）和“非成帧”（unframe）。
- IDLE-CODE：空闲码的码值。
- 时隙：该接口绑定的时隙范围。
- 配置：点击对应的按钮进入E1接口配置。

2. 点击E1接口所对应的**配置**按钮，可以进入**E1接口配置**界面，如图4-16所示。

图4-16 E1接口配置界面

界面说明：

- 帧方式选择：有两种选择，“frame”或是“unframe”。若选择为“frame”则需要选择时隙复选框；若选择为“unframe”则不可以选择时隙。
- 时隙选择：有31个时隙可供选择。

3. 配置E1接口属性后，单击**应用**按钮，字段配置生效，**E1信息显示配置**界面内容更新，如图4-17所示；

   若单击**返回**按钮，则字段配置不生效，返回到**E1信息显示配置**界面，如图4-15所示。

图4-17 E1信息配置添加完成界面

--步骤结束--

4.5 配置MPPP

步骤

1. 选择导航栏菜单[**基本配置→MPPP配置**]，进入**MPPP信息显示配置**界面，如图4-18所示。

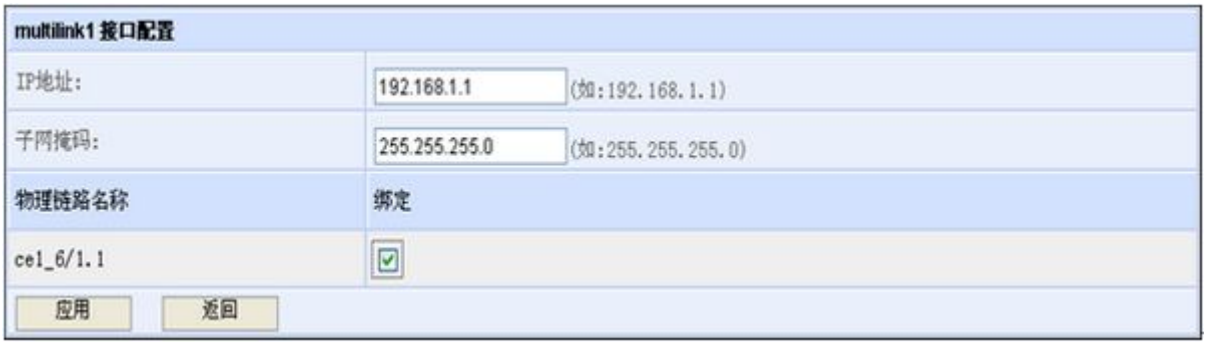
图4-18 MPPP信息显示配置界面

2. 在**multilink接口**输入框中输入multilink端口号（范围为1~64）。
3. 单击**配置**按钮，可以在**MPPP配置信息列表**显示框中看到新添加的multilink端口，如图4-19所示。

图4-19 MPPP信息显示配置界面

4. 在**MPPP配置信息列表**显示框中，点击multilink端口对应的**配置**按钮  ，进入**MPPP接口配置**界面进行参数配置，如图4-20所示。

图4-20 MPPP接口配置界面



5. 配置完multilink端口后，单击**应用**按钮，字段配置生效，**MPPP信息显示配置**界面内容更新，如图4-21所示；

   若单击**返回**按钮，则字段配置不生效，返回到**MPPP信息显示配置**界面，如图4-19所示。

图4-21 MPPP接口配置完成界面

6. 在图4-21所示界面中，点击该MPPP接口对应的**删除**按钮，弹出**确认删除端口**对话框，如图4-22所示。

7. 确定删除该MPPP接口，单击**确定**按钮；

   若不删除该接口，则单击**取消**按钮。

图4-22 MPPP接口配置完成界面

8. MPPP接口删除成功，返回到**MPPP信息显示配置**界面，如图4-23所示，可以看到MPPP接口multilink1已经被删除。

图4-23 MPPP接口删除完成界面

--步骤结束--

5 VLAN管理

本章包含如下主题：

5.1 配置VLAN

步骤

1. 选择导航栏菜单[**VLAN管理→VLAN管理**]，进入**VLAN管理配置**界面，如图5-1所示。

图5-1 VLAN管理配置界面1

NOTE **说明：**

当系统中存在二层接口板时，系统默认创建Vlan 1且所有的二层接口都默认属于Vlan 1；如果没有二层接口板，不创建VLAN。

2. 在**VLAN管理**界面的**Vlan ID**输入框中输入Vlan ID。
3. 单击**配置**按钮，创建VLAN，并进入**Vlan信息配置**界面。

4. 在**Vlan信息**配置界面中，选中**端口添加**前的单选框，如图5-2所示。

图5-2 Vlan信息配置界面

5. 单击**配置**按钮，完成端口添加操作。

6. 在**VLAN管理配置**界面图5-1的**Vlan ID**输入框中输入Vlan ID后，单击**删除**按钮可以删除Vlan；

   或者在**VLAN管理配置**界面中在要删除的VlanId后点击**删除**按钮，也可删除相应的VLAN。

   删除VLAN2后的界面如图5-3所示。

图5-3 VLAN管理配置界面2

NOTE **说明：**

VlanId 1是系统默认的VlanId，不能被删除。

Vlan ID下接口数为零时，该Vlan ID才能被删除。

--步骤结束--

5.2 VLAN端口配置

在图5-3界面中，点击**配置**按钮 对Vlan的端口进行配置。通过选中端口类型前的单选框，可以对相应的VLAN进行添加或删除端口的操作，如图5-4和图5-5所示。

图5-4 VLAN端口添加界面

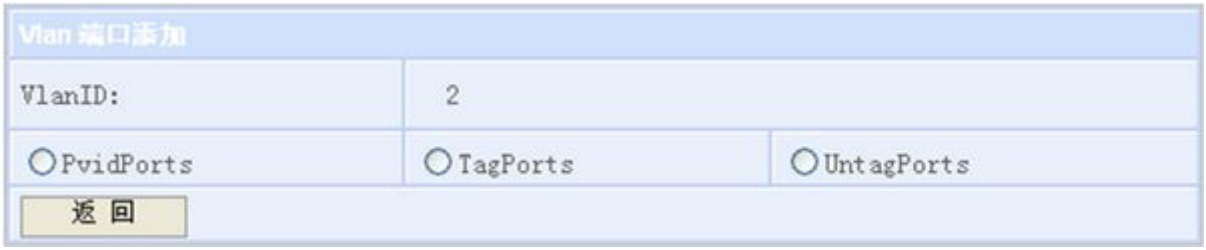
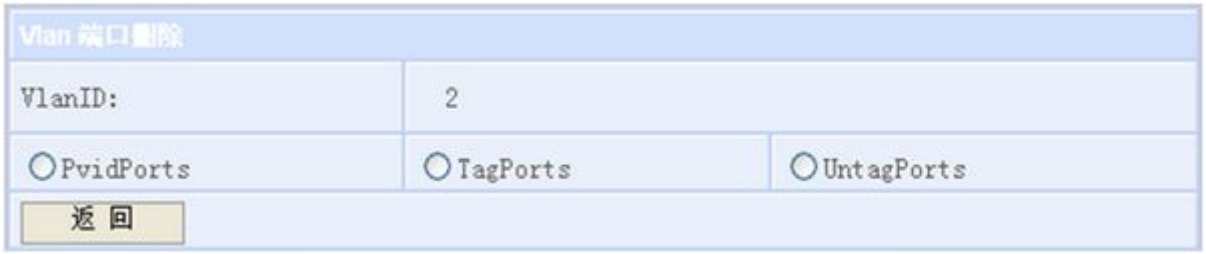


图5-5 VLAN端口删除界面



5.2.1 Pvid端口配置

5.2.1.1 添加Pvid端口

步骤

1. 在**VLAN端口添加**界面图5-4的**Vlan端口添加**区域框中，选中**PvidPorts**前的单选框，进入**PvidPort端口添加**界面，如图5-6所示。

图5-6 PvidPort端口添加界面1

2. 选中要添加的端口后，点击按钮 ，如图5-7所示。

图5-7 PvidPort端口添加界面2

3. 单击**应用**按钮后，完成配置。如图5-8所示，可以将接口fei_1/1添加到VLAN 2中。

图5-8 添加PvidPort端口后显示界面

NOTE **说明：**

同一个二层接口只能作为一个VLAN的PvidPort。

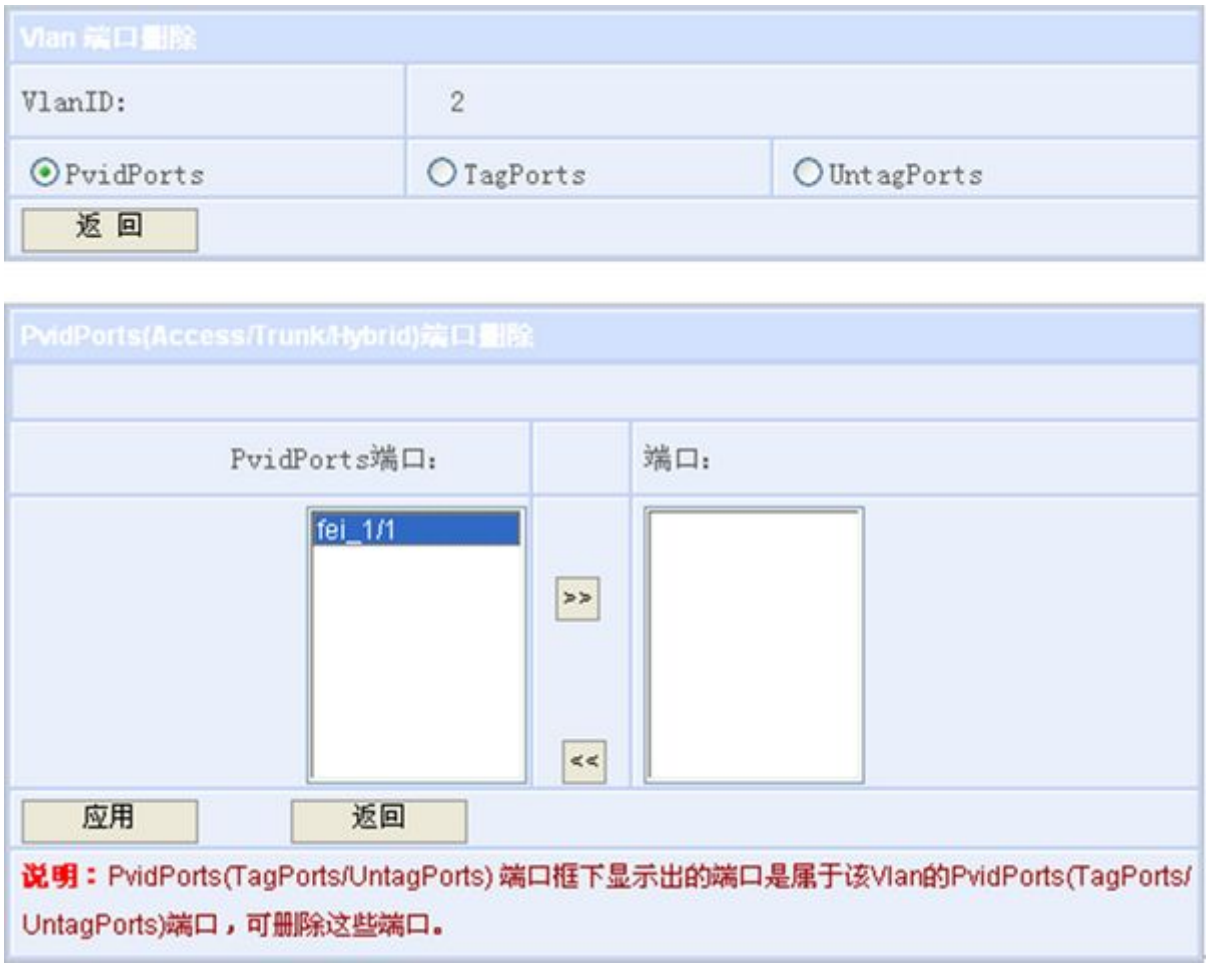
--步骤结束--

5.2.1.2 删除Pvid端口

步骤

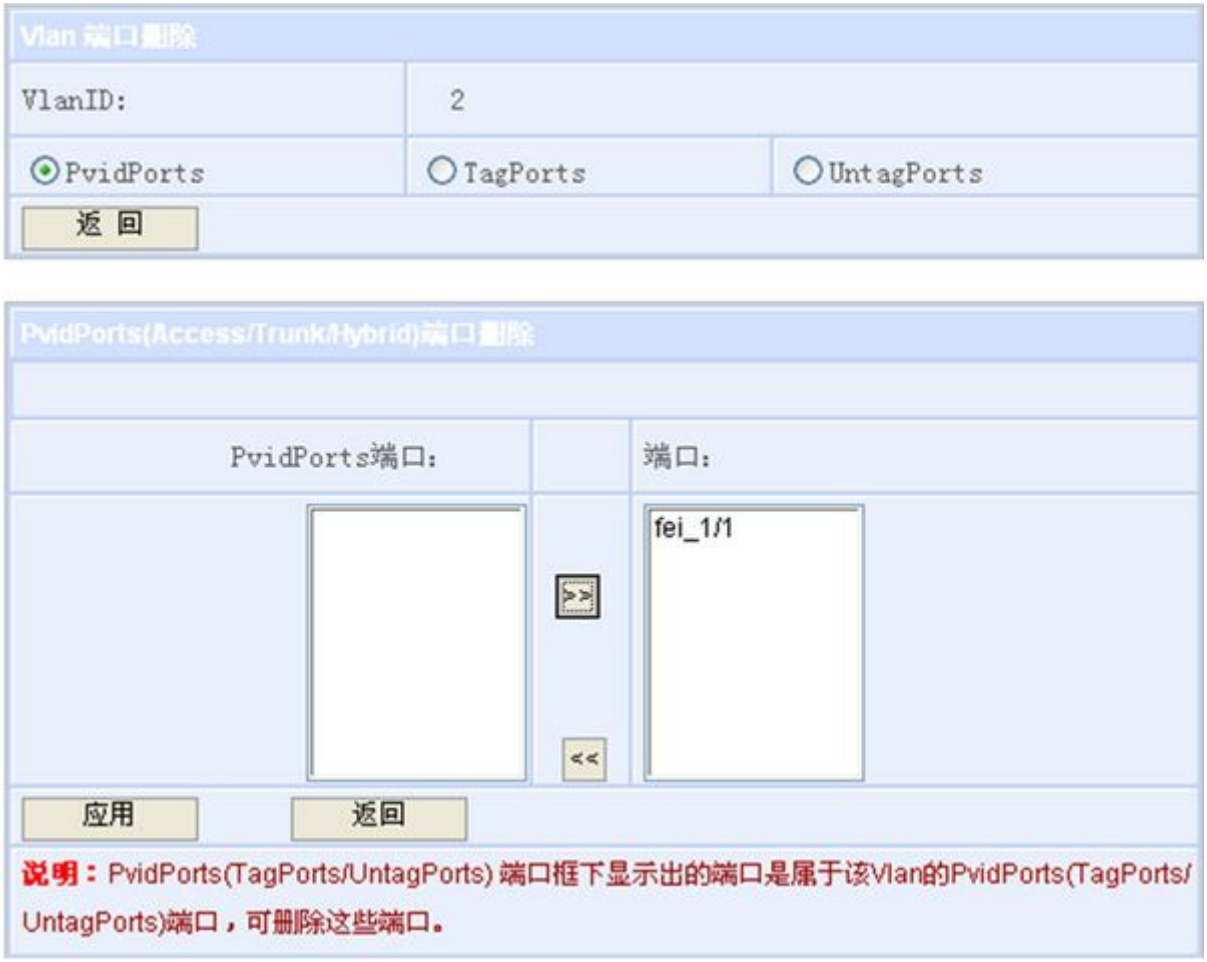
1. 在**VLAN端口删除**界面图5-4的**Vlan端口删除**区域框中，选中**PvidPorts**前的单选框，进入**PvidPort端口删除**界面，如图5-9所示。

图5-9 PvidPort端口删除界面



2. 选中要删除的端口后，点击“>>”按钮，如图5-10所示。

图5-10 PvidPort端口删除界面



3. 单击**应用**按钮后，完成配置。如图5-11所示，可以将接口fei_1/1从VLAN 2的PvidPort端口中删除。

图5-11 删除VLAN中的PvidPort端口后显示界面

--步骤结束--

5.2.2 Tag端口配置

5.2.2.1 添加Tag端口

步骤

1. 在**VLAN端口添加**界面图5-4的**Vlan端口添加**区域框中，选中**TagPorts**前的单选框，进入**TagPort端口添加**界面，如图5-12所示。

图5-12 TagPort端口添加界面

NOTE **说明：**

只有二层接口的交换模式为Truck和Hybrid时才能加入到TagPort端口中。

2. 选中要添加的端口后，点击“**>>**”按钮，如图5-13所示。

图5-13 TagPort端口添加界面

3. 单击**应用**按钮后，完成配置。如图5-14所示，可以将接口fei_1/5添加到VLAN 2中。

图5-14 添加TagPort端口后显示界面

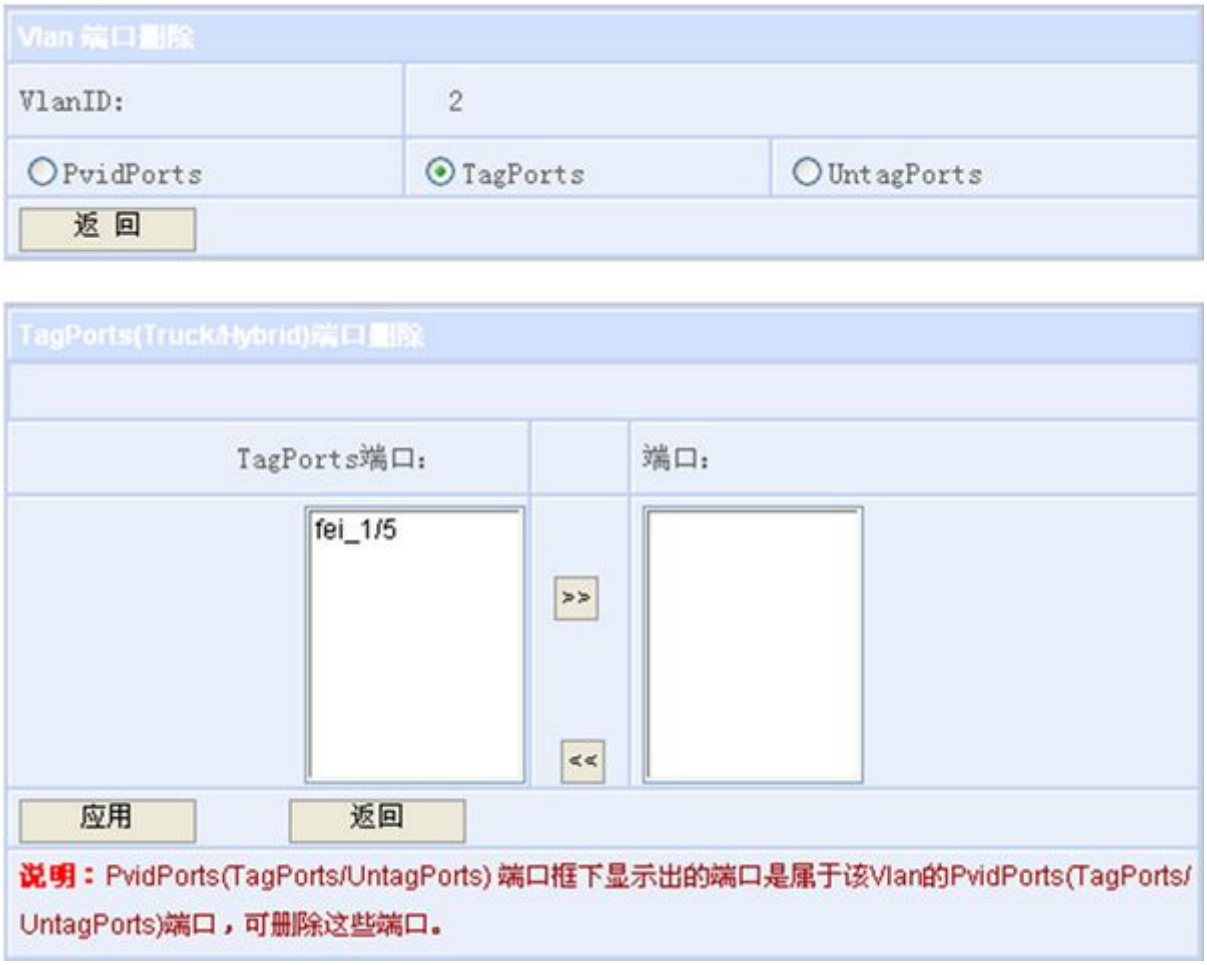
--步骤结束--

5.2.2.2 删除Tag端口

步骤

1. 在**VLAN端口删除**界面图5-5的**Vlan端口删除**区域框中，选中**TagPorts**前的单选框，进入**TagPort端口删除**界面，如图5-15所示。

图5-15 TagPort端口删除界面



2. 选中要删除的端口后，点击“>>”按钮，如图5-16所示。

图5-16 TagPort端口删除界面

3. 单击**应用**按钮后，完成配置。如图5-17所示，可以将接口fei_1/5从VLAN 2的TagPort端口中删除。

图5-17 删除VLAN中的TagPort端口后显示界面

--步骤结束--

5.2.3 Untag端口配置

5.2.3.1 添加Untag端口

步骤

1. 在**VLAN端口添加**界面图5-4的**Vlan端口添加**区域框中，选中**UntagPorts**前的单选框，进入**UntagPort端口添加**界面，如图5-18所示。

图5-18 UntagPort端口添加界面

NOTE **说明：**

只有二层接口的交换模式为Hybrid时才能加入到UntagPort端口中。

2. 选中要添加的端口后，点击“>>”按钮，如图5-19示。

图5-19 UntagPort端口添加界面

3. 单击**应用**按钮后，完成配置。如图5-20所示，可以将接口fei_1/7添加到VLAN 2中。

图5-20 添加UntagPort端口后显示界面

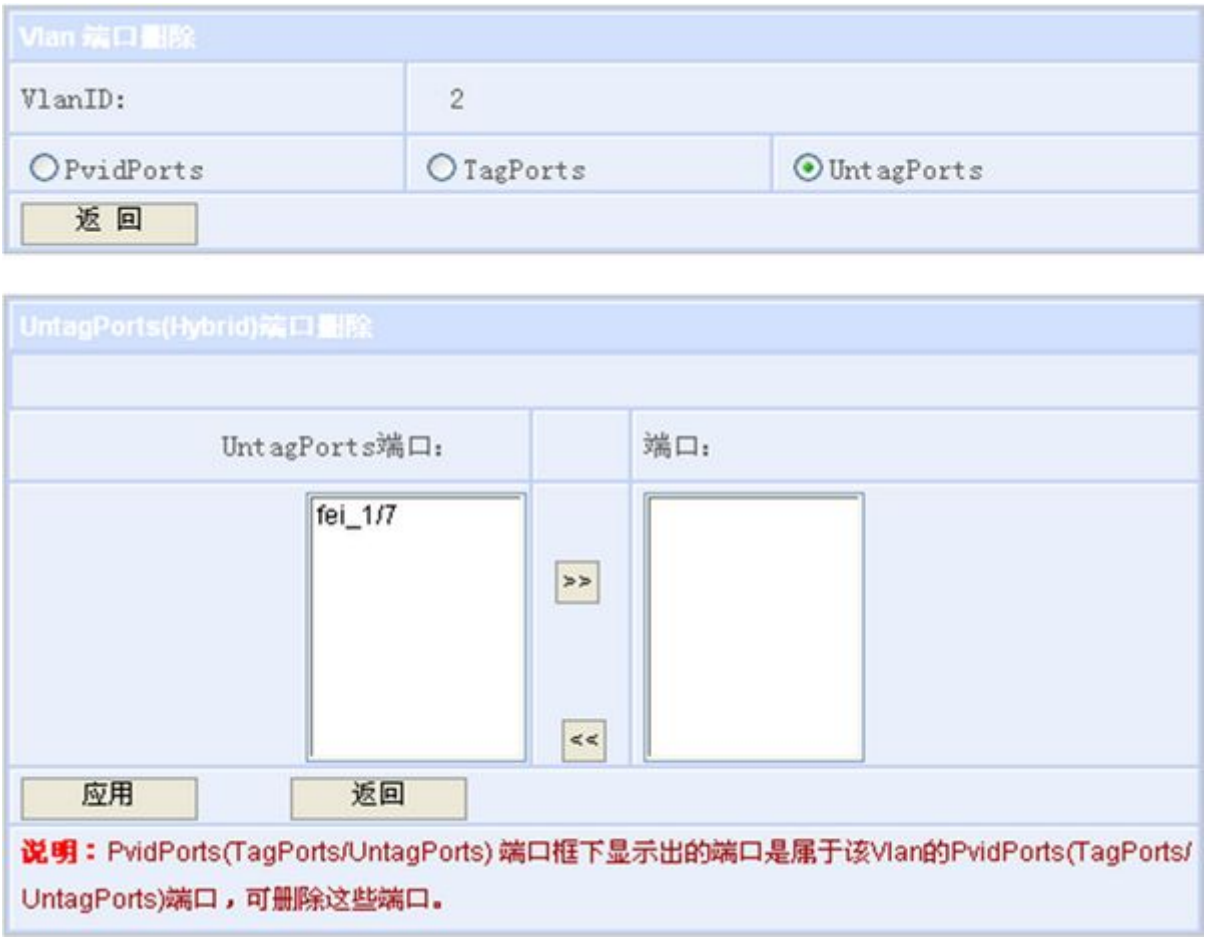
--步骤结束--

5.2.3.2 删除Untag端口

步骤

1. 在**VLAN端口删除**界面图5-5的**Vlan端口删除**区域框中，选中**UntagPorts**前的单选框，进入**UntagPort端口删除**界面，如图5-21所示。

图5-21 添加UntagPort端口后显示界面



2. 选中要删除的端口后，点击“>>”按钮，如图5-22所示。

图5-22 UntagPort端口删除界面

3. 单击**应用**按钮后，完成配置。如图5-23所示，可以将接口fei_1/7从VLAN 2的UntagPort端口中删除。

图5-23 删除VLAN中的UntagPort端口后显示界面

--步骤结束--

6 NAT配置

本章包含如下主题：

6.1 NAT基本配置

选择导航栏菜单[**NAT→基本配置**]，进入**NAT基本配置**界面，如图6-1所示。

图6-1 NAT基本配置界面

6.1.1 启用NAT

步骤

1. 在**NAT基本配置**界面图6-1的**NAT配置**区域框中，选中**启用**前的单选框，如图6-2所示。

图6-2 启用NAT功能单选框

2. 选中**启用**后，弹出**确认打开NAT配置**对话框，如图6-3所示。

图6-3 确认打开NAT配置对话框

3. 单击**确定**按钮，启用NAT配置功能，进入**NAT配置**界面，如图6-4所示。

图6-4 NAT配置界面

--步骤结束--

6.1.2 关闭NAT

步骤

1. 在**NAT基本配置**界面图6-1的**NAT配置**区域框中，选中**关闭**前的单选框，如图6-5所示。

图6-5 关闭NAT功能单选框

2. 选中**关闭**后，弹出**确认关闭NAT配置**对话框，如图6-6所示。

图6-6 确认关闭NAT配置对话框

--步骤结束--

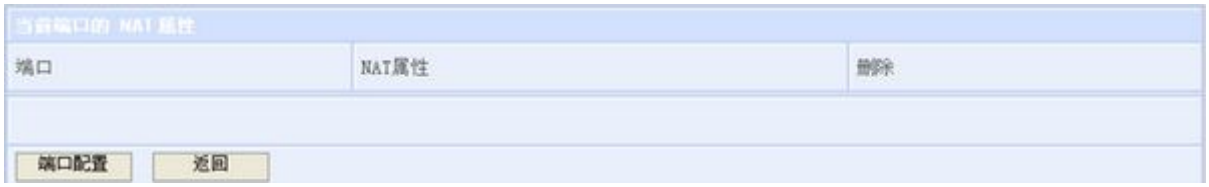
6.2 配置NAT端口

步骤

1. 单击**NAT配置**界面图6-4中的**端口配置**按钮，进入**端口配置按钮**界面，如图6-7和图6-8所示。

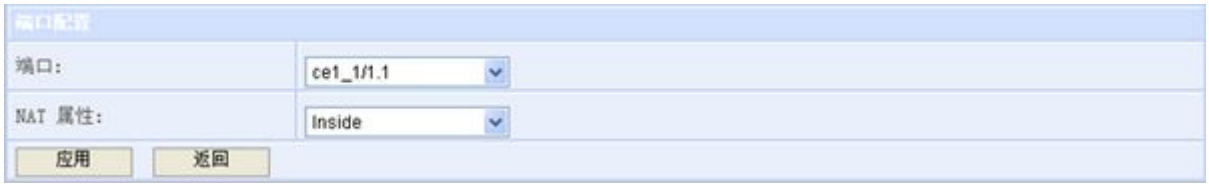
图6-7 端口配置按钮

图6-8 端口配置按钮界面



2. 单击图6-8中**端口配置**按钮，进入**端口配置**界面，如图6-9所示。

图6-9 端口配置界面



3. 配置相应的NAT inside和outside端口，单击**应用**按钮，完成配置，并进入**当前端口的NAT属性**界面，如图6-10所示。

图6-10 当前端口的NAT属性界面

NOTE **说明：**

- NAT inside接口是连接私网的接口。
- NAT outside接口是连接公网的接口。
- NAT配置中，必须配置NAT inside和outside接口。

--步骤结束--

6.3 NAT规则配置

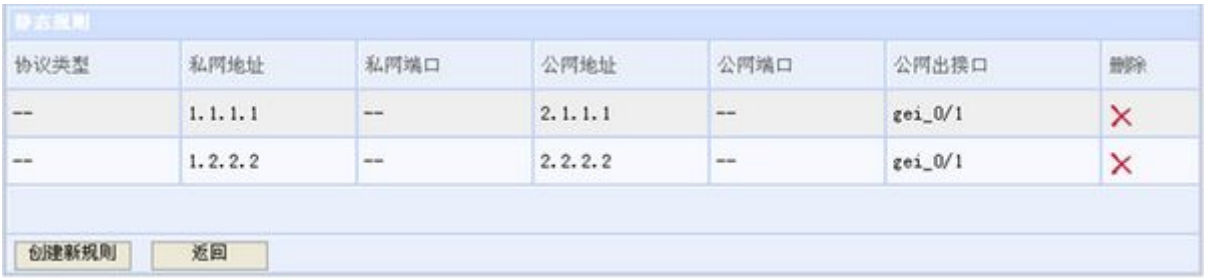
6.3.1 配置NAT静态规则

步骤

1. 单击图6-4所示**NAT配置**界面中**静态规则**按钮，进入**静态规则**界面，如图6-11和图6-12所示。

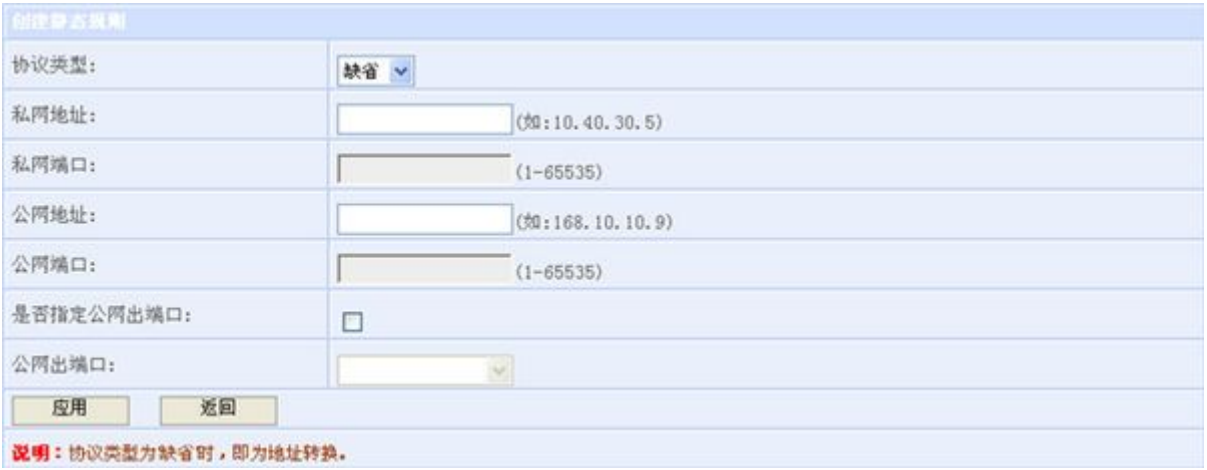
图6-11 静态规则按钮

图6-12 静态规则界面



2. 单击**创建新规则**按钮，进入**创建静态规则**界面，如图6-13所示。

图6-13 创建静态规则界面

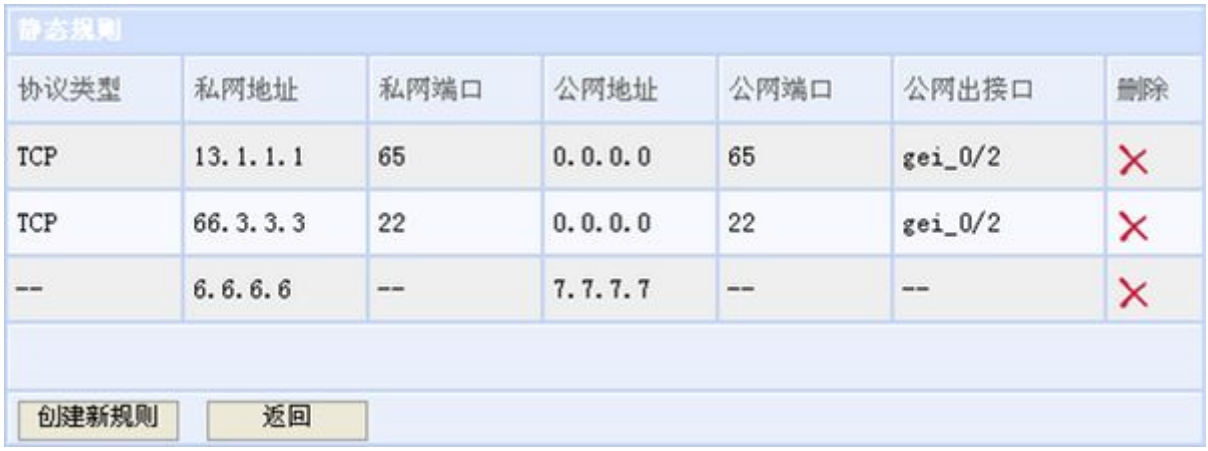


界面说明：

- 协议类型：有3种选择协议类型，分别是“缺省”、“TCP”和“UDP”。
- 私网地址：私网的IP地址。
- 私网端口：当选择协议类型为TCP或UDP时，可以指定一个空闲端口与私网地址配对。
- 公网地址：注意这个地址不是要访问的公网的地址，而是将私网IP地址映射后的公网地址。
- 公网端口：当选择协议类型为TCP或UDP时，可以指定一个已使用地址的空闲端口，用地址和端口的配对来替代私网数据包中的相应地址和端口。
- 是否指定公网出端口：只有选择此选项，公网出端口才可以配置，否则不可以配置。
- 公网出端口：可以配置多个NAT的outside接口，只有和公网出端口一样的outside接口才能正常访问公网，否则报文将被丢弃。

3. 配置完成后，单击**应用**按钮，进入**静态规则配置完成**界面，如图6-14所示。

图6-14 静态规则配置成功的界面



NOTE **说明：**

静态规则和动态规则的配置是可选择，无论是动态还是静态都是可以独立生效的，不需要同时配置。

4. 点击**静态规则**界面中的**删除**按钮，可以删除已配置的静态规则。

--步骤结束--

6.3.2 配置NAT动态规则

步骤

1. 单击图6-4所示**NAT配置**界面中**动态规则**按钮，进入**动态规则**界面，如图6-15和图6-16所示。

图6-15 动态规则按钮

图6-16 动态规则界面

2. 单击**创建新规则**按钮，进入**创建动态规则**界面，如图6-17所示。

图6-17 动态规则配置界面

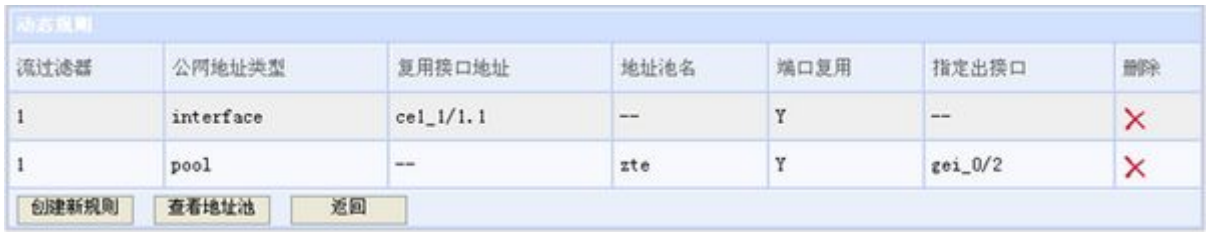
界面说明：

- 流过滤器：即访问控制列表（ACL），用于过滤报文。
- 公网地址类型：有“interface”和“pool”两种选项。若选择“interface”，则把公网地址指定为复用接口地址；若选择“pool”，则从地址池中选择空闲的IP地址作为映射私网地址的公网地址，当映射关系解除后可以释放该IP地址，再次映射给其他私网地址。
- 复用接口地址：当公网地址类型选择interface时，此选项可配置。
- 地址池名：当公网地址类型选择pool时，选择对应的配置的地址池，该地址的配置见6.3.3 配置NAT地址池。
- 端口复用：有“yes”和“no”两个选项，选择“yes”代表启用端口复用，选择“no”不启用。

  启用端口复用后，映射关系就会变为（私网IP+端口）对应(公网IP+端口)，否则映射关系为（私网IP）对应（公网IP）。
- 指定出接口：可选项，如果选择，那么只有NAT的outside接口和指定的出接口报文才可以通过。

3. 配置完成后，单击**应用**按钮，进入**动态规则配置完成**界面，如图6-18所示。

图6-18 动态规则界面



4. 点击**动态规则**界面中的**删除**按钮，可以删除已配置的动态规则。

--步骤结束--

6.3.3 配置NAT地址池

步骤

1. 单击图6-4所示**NAT配置**界面中**动态规则**按钮，进入**动态规则**界面，如图6-19和图6-20所示。

图6-19 动态规则按钮

图6-20 动态规则界面

2. 单击**查看地址池**按钮，进入**NAT地址池查看**界面，如图6-21所示。

图6-21 NAT地址池查看界面

3. 单击**配置地址池**按钮，进入**NAT地址池配置**界面，如图6-22所示。

图6-22 地址池配置界面

4. 配置完成后，单击**应用**按钮，进入**NAT地址池配置完成**界面，如图6-23所示。

图6-23 完成配置界面

5. 点击**NAT地址池配置完成**界面中的**删除**按钮，可以删除已配置的NAT地址池。

--步骤结束--

6.3.4 配置用户限制规则

相关信息

用户限制规则是用户配置某种规则来限制公网地址的最大映射数量。

步骤

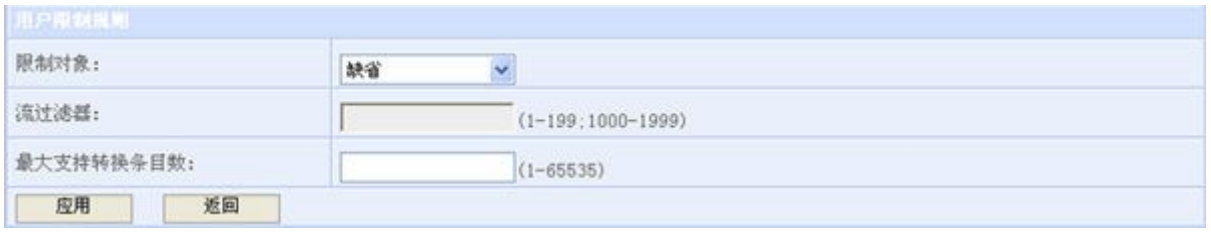
1. 单击图6-4所示**NAT配置**界面中**用户限制规则**按钮，进入**用户限制规则**界面，如图6-24和图6-25所示。

图6-24 用户限制规则按钮

图6-25 用户限制规则界面

2. 单击**添加新规则**按钮，进入**新规则添加**界面，如图6-26所示。

图6-26 新规则添加界面



界面说明：

- 限制对象：有“缺省”和“流过滤器”两种。选择“缺省”是对所有流进行检查，看是否达到最大支持转换条目数，达到了要丢弃流；选择“流过滤器”是对能通过流过滤器的流进行检查，看是否达到最大支持转换条目数，达到了要丢弃流。
- 最大支持转换条目数：公网地址允许映射成私网地址的最大个数。

--步骤结束--

6.3.5 配置NAT日志

步骤

1. 在**NAT配置**界面图6-4的**基本配置框**区域中，配置NAT日志各参数，界面如图6-27所示。

图6-27 NAT日志界面

界面说明：

- 日志ftp服务器地址：保存日志服务器ftp的IP地址。
- 日志ftp服务器用户名：保存日志服务器ftp的用户名。
- 日志ftp服务器用户密码：保存日志服务器ftp的密码。
- 日志文件名：保存日志信息的文件的名称。
- 日志文件保存周期：取值范围为1~10天。
- 日志文件保存时间：保存周期开始当天的几点几分几秒。

2. 配置完成后，单击**应用**按钮，当前页面会显示配置信息；

   若单击**删除FTP配置**按钮，则页面显示的配置信息被清空。

--步骤结束--

6.3.6 配置NAT最大转换条目

步骤

1. 在图6-4所示**NAT配置**界面的**NAT配置**区域框中，选中**关闭**前的单选框，进入**NAT最大转换条目数配置**界面，如图6-28和图6-29所示。

图6-28 NAT关闭按钮

图6-29 NAT最大转换条目数配置

2. 在**最大转换条目数**下拉列表框中选择路由器支持的最大转换数量，可以选择“32”K、“64”K、“128”K、“256”K、“512”K或“1024”K。

--步骤结束--

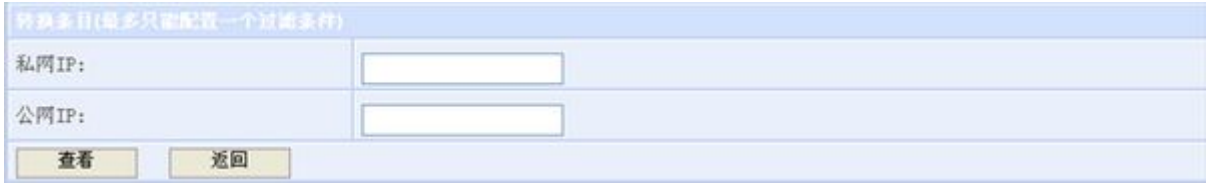
6.3.7 查看NAT转换条目

步骤

1. 单击图6-4所示**NAT配置**界面中**转换条目**按钮，进入**转换条目查看**界面，如图6-30和图6-31所示。

图6-30 转换条目按钮

图6-31 转换条目查看界面



界面说明：

- 私网IP：输入私网IP，查询当前输入IP和公网IP的映射关系。
- 公网IP：输入公网IP，查询当前输入IP和私网IP的映射关系。

  查看时，只能选择输入私网IP或者公网IP中的一个进行查看，不能两个同时查看。

2. 输入IP地址，单击**查看**按钮，查看指定IP的NAT转换条目。

   若不输入IP地址，单击**查看**按钮，则此时查看的是所有的映射关系。

--步骤结束--

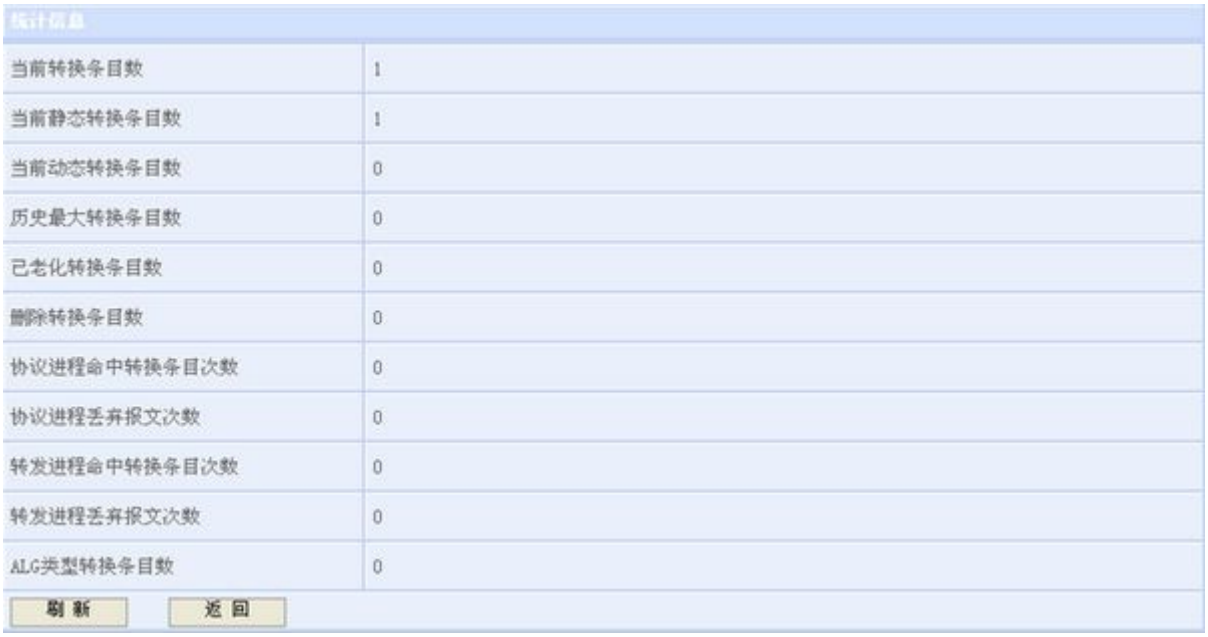
6.3.8 查看NAT统计信息

步骤

1. 单击图6-4所示**NAT配置**界面中**统计信息**按钮，进入**统计信息查看**界面，如图6-32和图6-33所示。

图6-32 统计信息按钮

图6-33 统计信息查看界面



2. 在**统计信息查看**界面中，单击**刷新**按钮可以更新当前的统计信息。

--步骤结束--

7 静态路由配置

本章包含如下主题：

7.1 添加静态路由

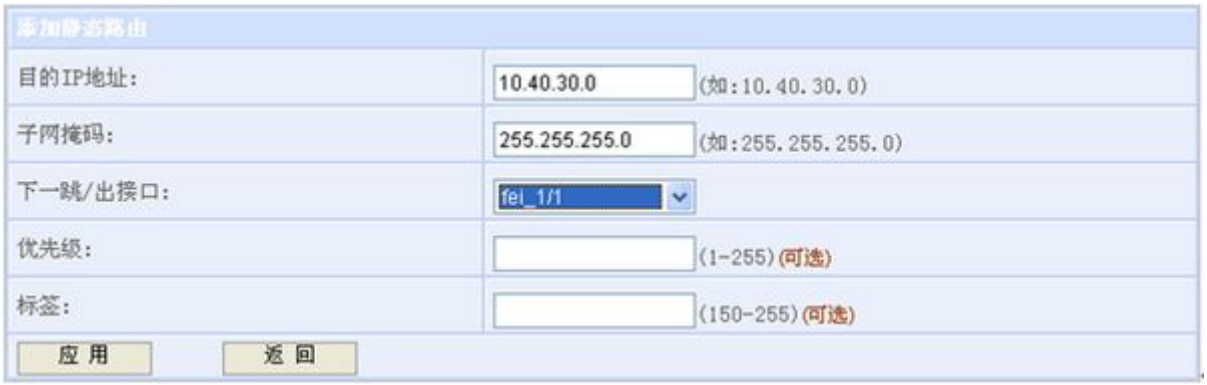
步骤

1. 选择导航栏菜单[**静态路由→静态路由**]，进入**静态路由显示配置**界面，如图7−1所示。

图7−1 静态路由显示配置界面

2. 单击**添加新路由**按钮，进入**添加静态路由**界面，如图7−2所示。

图7-2 添加静态路由界面



界面说明：

- 下一跳/出接口：可以指定路由下一跳地址或者指定路由出接口。
- 优先级：可选字段，设定指定路由的优先级，数值越小优先级越高。
- 标签：到同一个目的网络的静态路由不能具有相同的标签值。

3. 配置完成后，单击**应用**按钮，配置字段生效，并返回到**静态路由添加完成**界面，可以看到新添加的路由信息已经显示，如图7-3所示；

   若单击**返回**按钮，则返回到**静态路由显示配置**界面，如图7-1所示，并且已经填写的属性字段将不会生效。

图7-3 静态路由添加完成界面

NOTE **说明：**

默认路由也可以在此配置。

--步骤结束--

7.2 删除静态路由

步骤

1. 选择导航栏菜单[**静态路由→静态路由**]，进入**静态路由显示配置**界面，如图7-1所示。
2. 单击静态路由条目对应的**删除**按钮，弹出**确认删除静态路由**对话框，如图7-4所示。确定删除该静态路由，单击**确定**按钮；不删除该静态路由，单击**取消**按钮。

图7-4 确认删除静态路由对话框

NOTE **说明：**

仅能删除Owner字段显示为“static”的路由条目。

3. 静态路由删除成功，返回到**静态路由显示配置**界面。

--步骤结束--

8 流过滤器配置

本章包含如下主题：

8.1 流过滤器简介

流过滤器也就是常说的ACL，实现对策略路由和特殊流量的控制。

一个过滤器中可以包含一条或多条特定类型的IP数据报规则，每条规则告诉路由器对于与规则中所指定的选择标准相匹配的分组是准许还是拒绝通过。每个被定义的过滤器都有一个用以识别的过滤器名，WEB GUI中只支持数字型，如100。

过滤器分为标准过滤器和扩展过滤器两种方式。标准过滤器的名称范围为1~99和1000~1499，扩展过滤器的名称范围为100~199和1500~1999。

过滤器规则中的选择标准描述了分组的特性。我们可以定义一个基于源地址过滤的过滤器，也可以定义一个基于源和目的的特定流的过滤器。

通常使用下列规则来定义一个过滤器语句：源IP地址、目的IP地址、源端口号、目的端口号、协议类型。这些选择标准被指定为过滤器规则的域。在标准过滤器中仅对源地址进行定义，而在扩展过滤器中可以对源地址、目的地址、源端口号、目的端口号和协议号进行定义。

8.2 标准流过滤器配置

8.2.1 添加标准流过滤器

步骤

1. 选择导航栏菜单[**流过滤器→流过滤器配置**]，进入**流过滤器显示**界面，如图8-1所示。

图8-1 流过滤器显示界面

2. 单击**流过滤器添加**按钮，进入**流过滤器添加**界面，如图8-2所示。

图8-2 标准流过滤器添加界面

3. 在**流过滤器名**输入框中输入标准流过滤器号，单击**应用**按钮，添加成功，并返回**流过滤器显示**界面，如图8-3所示。

图8-3 标准流过滤器显示界面

NOTE **说明：**

当流过滤器条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

8.2.2 标准流过滤器规则配置

8.2.2.1 添加标准流过滤器规则

步骤

1. 单击**流过滤器显示**界面中图8-3的**配置**按钮，进入**标准流过滤器规则显示**界面，如图8-4所示。

图8-4 标准流过滤器规则显示界面

2. 在**添加新rule**输入框中输入规则号，单击**添加**按钮，进入**标准流过滤器规则添加**界面，如图8-5所示。

图8-5 标准流过滤器规则添加界面

界面说明：

- 是否允许通过：有“permit”和“deny”两种属性，分别表示允许通过和不允许通过。
- 源IP地址类型：可以选择“任意”或者“指定”这两种方式。
- 源IP地址：返回值与地址反掩码有关。
- 地址反掩码：反掩码格式。
- 日志：有“选中”和“不选中”两种选择，“选中”表示打开日志，“不选中”表示关闭日志。

3. 标准流过滤器规则添加成功后，返回**标准流过滤器规则显示**界面，如图8-6所示。

图8-6 标准流过滤器规则显示界面

NOTE **说明：**

当扩展流过滤器规则条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

8.2.2.2 修改标准流过滤器规则

步骤

1. 单击**标准流过滤器规则显示**界面图8-3中相应条目后的**配置**按钮，进入**标准流过滤器规则修改**界面，如图8-7所示。

图8-7 标准流过滤器规则修改界面

2. 修改完成后，单击**确定**按钮，修改成功，返回**标准流过滤器规则显示**界面，如图8-8所示。

图8-8 标准流过滤器规则显示界面

--步骤结束--

8.2.2.3 删除标准流过滤器规则

步骤

1. 单击**标准流过滤器规则显示**界面图8-8中的**删除**按钮，弹出**确认删除规则**对话框，如图8-9所示。

图8-9 确认删除规则对话框

2. 单击**确定**按钮，即执行删除操作。

--步骤结束--

8.2.2.4 修改标准流过滤器规则顺序

步骤

1. 单击**标准流过滤器规则显示**界面图8-8中的**修改rule顺序**按钮，进入**标准流过滤器规则修改**界面，如图8-10所示。

图8-10 标准流过滤器规则修改界面

2. 把要修改顺序的两个规则号分别输入图中两个输入框中，同时可以选择调整到之前或者之后的位置。单击**应用**按钮，完成修改，如图8-11所示。修改效果可以与图8-8对照。

图8-11 标准流过滤器规则顺序修改显示界面

NOTE **说明：**

数据包转发是按照流过滤器的规则顺序来匹配的，用户可以通过修改规则顺序来实现不同的转发需求。

--步骤结束--

8.2.3 删除标准流过滤器

步骤

1. 单击**标准流过滤器显示**界面图8-3中相应条目后的**删除**按钮，弹出**确认删除流过滤器**对话框，如图8-12所示。

图8-12 确认删除流过滤器对话框

2. 单击**确定**按钮，执行删除操作。

--步骤结束--

8.3 扩展流过滤器配置

8.3.1 添加扩展流过滤器

步骤

1. 选择导航栏菜单[**流过滤器→流过滤器配置**]，进入**流过滤器显示**界面，如图8-13所示。

图8-13 流过滤器显示界面

2. 单击**流过滤器添加**按钮，进入**流过滤器添加**界面，如图8-14所示。

图8-14 扩展流过滤器添加界面

3. 在**流过滤器名**输入框中输入扩展流过滤器号，单击**应用**按钮，添加成功，并返回**流过滤器显示**界面，如图8-15所示。

图8-15 扩展流过滤器显示界面

NOTE **说明：**

当流过滤器条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

8.3.2 扩展流过滤器规则配置

8.3.2.1 添加扩展流过滤器规则

步骤

1. 单击**扩展流过滤器显示**界面图8-15中相应条目后的**配置**按钮，进入**扩展流过滤器规则显示**界面，如图8-16示。

图8-16 扩展流过滤器规则显示界面

2. 在**添加新rule**输入框中输入规则号，单击**添加**按钮，进入**扩展流过滤器规则添加**界面，如图8-17所示。

图8-17 扩展流过滤器规则添加界面

界面说明：

- 是否允许通过：有“permit”和“deny”两个属性，分别表示允许通过和不允许通过。
- 协议类型：有“tcp”、“udp”、“ospf”、“pim”、“vrrp”、“icmp”、“gre”九种类型，必须在下拉列表框中选择一种。
- 源IP地址类型：可以选择“任意”或者“指定”这两种方式。
- 源IP地址：返回值与地址反掩码有关。
- 地址反掩码：反掩码格式。
- 目的IP地址类型：可以选择“任意”或者“指定”这两种方式。
- 目的IP地址：返回值与地址反掩码有关。
- 地址反掩码：反掩码格式。
- 日志：有“选中”和“不选中”两种选择，“选中”表示打开日志，“不选中”表示关闭日志。

3. 扩展流过滤器规则添加成功后，返回**扩展流过滤器规则显示**界面，如图8-18所示。

图8-18 扩展流过滤器规则显示界面

NOTE **说明：**

当扩展流过滤器规则条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

8.3.2.2 修改扩展流过滤器规则

步骤

1. 单击**扩展流过滤器规则显示**界面中相应条目后的**配置**按钮，进入**扩展流过滤器规则修改**界面，如图8-19所示。

图8-19 扩展流过滤器规则修改界面

2. 修改完成后，单击**确定**按钮，修改成功，返回**扩展流过滤器规则显示**界面，如图8-20所示。

图8-20 扩展流过滤器规则显示界面

--步骤结束--

8.3.2.3 删除扩展流过滤器规则

步骤

1. 单击**扩展流过滤器规则显示**界面图8-20中的**删除**按钮，弹出**确认删除规则**对话框，如图8-21所示。

图8-21 确认删除规则对话框

2. 单击**确定**按钮，即执行删除操作。

--步骤结束--

8.3.2.4 修改扩展流过滤器规则顺序

步骤

1. 单击**扩展流过滤器规则显示**界面图8-20中的**修改rule顺序**按钮，进入**扩展流过滤器规则修改**界面，如图8-22所示。

图8-22 扩展流过滤器规则修改界面

2. 把要修改顺序的两个规则号分别输入图中两个输入框中，同时可以选择调整到之前或者之后的位置。单击**应用**按钮，完成修改，如图8-23所示。修改效果可以与图8-20对照。

图8-23 扩展流过滤器规则顺序修改显示界面

--步骤结束--

8.3.3 删除扩展流过滤器

步骤

1. 单击**扩展流过滤器显示**界面图8-15中相应条目后的**删除**按钮，弹出**确认删除流过滤器**对话框，如图8-24所示。

图8-24 确认删除流过滤器对话框

2. 单击**确定**按钮，执行删除操作。

--步骤结束--

8.4 流过滤器绑定接口配置

8.4.1 添加流过滤器绑定接口

步骤

1. 选择导航栏菜单[**流过滤器→流过滤器运用**]，进入**流过滤器绑定接口显示**界面，如图8-25所示。

图8-25 流过滤器绑定接口显示界面

2. 单击**流过滤器绑定接口显示**界面**配置**按钮，进入**流过滤器绑定接口添加**界面，如图8-26所示。

图8-26 流过滤器绑定接口添加界面

界面说明：

- 接口名：当前可以绑定的接口，用下拉框列表显示。
- 流过滤器名：范围“1~199”和“1000~1999”。

- 方向：有“in”和“out”两种属性，“in”表示在入接口对数据流进行过滤，“out”表示在出接口对数据流进行过滤。

3. 添加完成后，单击**应用**按钮，进入**流过滤器绑定接口显示**界面，如图8-27所示。

图8-27 流过滤器绑定接口显示界面

NOTE **说明：**

当绑定接口的流过滤器条目超过64条时，将采用分页显示，每页最多显示64个条目。

4. 点击相应条目后的**配置**按钮，界面会根据流过滤器名分别进入**标准流过滤器规则显示**界面（流过滤器名为1~99或1000~1499）或者**扩展流过滤器规则显示**界面（流过滤器名为100-199或1500-1999）。

   后续配置请参照8.2.2.1 添加标准流过滤器规则和8.3.2.1 添加扩展流过滤器规则扩展流过滤器规则，此处不再赘述。

--步骤结束--

8.4.2 删除流过滤器绑定接口

步骤

1. 点击**流过滤器绑定接口显示**界面图8-27相应条目后的**删除**按钮。弹出**确认删除接口与该流过滤器的绑定**对话框，如图8-28所示。

图8-28 确认删除接口与该流过滤器的绑定对话框

2. 单击**确定**按钮，执行接口与流过滤器的解绑定操作。

--步骤结束--

9 QoS配置

本章包含如下主题：

9.1 启用QoS

步骤

1. 选择导航栏菜单[**QoS→QoS**]，进入**QoS配置**界面，如图9-1所示。

图9-1 QoS配置界面

2. 在**QoS开关**区域框中，选中**打开**前的单选框，弹出**确认打开QoS**对话框，如图9-2所示。

图9-2 确认打开QoS对话框

3. 若单击**确定**按钮，则服务器执行打开命令，界面开关状态选中为**打开**项，如图9-3所示；

   若单击**取消**按钮，则不进行任何操作。

图9-3 QoS开关打开状态界面

4. 在**QoS开关**区域框中，选中**关闭**前的单选框即可将开关置为关闭状态。

说明：

QoS功能关闭后，系统中与QoS相关的配置全部删除。

--步骤结束--

9.2 PQ功能配置

9.2.1 绑定PQ策略接口

步骤

1. 打开QoS功能，在**QoS开关打开状态**界面图9-3中单击**PQ**区域框后的**配置**按钮，进入**PQ队列端口绑定**界面，如图9-4所示。

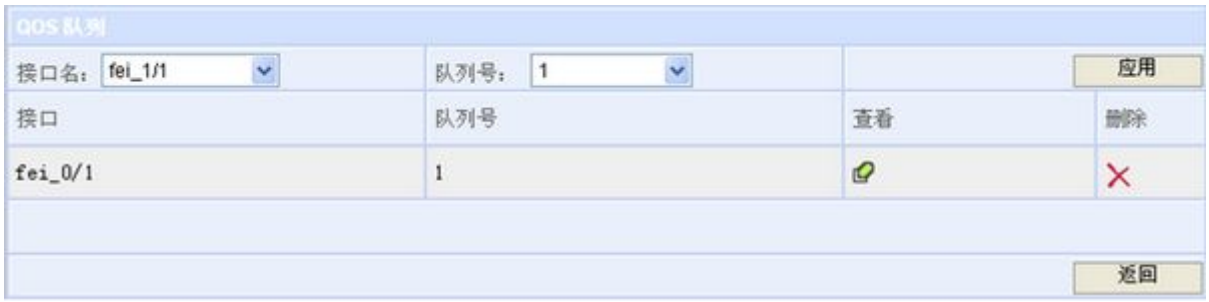
图9-4 PQ队列端口绑定界面

界面说明：

- 接口名：需要绑定PQ策略的接口。
- 队列号：PQ队列号。
- 查看：查看PQ队列号中的策略。
- 删除：删除配置的条目。

2. 配置完成后，单击**应用**按钮，将PQ的队列号绑定到对应的端口中，显示界面如图9-5所示。

图9-5 PQ队列与接口绑定关系显示界面



3. 在图9-5中点击相应端口名后的**删除**按钮，即可解除PQ的队列号与对应端口的绑定关系。

--步骤结束--

9.2.2 修改PQ缺省队列

步骤

1. 在**PQ队列与接口绑定关系显示**界面图9-5中，单击**查看**按钮，进入对应的**QoS队列显示**界面，如图9-6所示。

图9-6 QoS队列显示界面

2. 单击**配置**按钮进入**QoS队列配置**界面，如图9-7所示。

图9-7 QoS队列配置界面

界面说明：

- 入队分类队型：选择“缺省队列”。
- 子队列属性：可以选择“high”、“medium”、“normal”和“low”。

3. 单击**应用**按钮修改缺省队列，修改后显示界面如图9-8所示。

图9-8 修改缺省队列后显示界面

4. 在**修改缺省队列显示**界面图9-8中单击**删除**按钮，即可恢复缺省队列配置，如图9-9所示。

图9-9 删除缺省队列配置后显示界面

NOTE **说明：**

当数据包没有可用队列匹配时，便匹配PQ的默认队列。

--步骤结束--

9.2.3 配置基于入接口的PQ策略

步骤

1. 在**PQ队列与接口绑定关系显示**界面图9-5中，单击**查看**按钮，进入对应的**QoS队列显示**界面，如图9-6所示。
2. 单击**配置**按钮进入**QoS队列配置**界面，如图9-10所示。

图9-10 QoS队列配置界面

3. 在**入队分类队型**下拉列表框中选择**入接口**，配置基于入接口的PQ队列。
4. 单击**应用**按钮，完成配置，如图9-11所示。

图9-11 基于入接口的PQ策略配置后显示界面

5. 在图9-11所示界面中，点击相应入接口条目后的**删除**按钮，即可删除所配置的策略，删除后的显示界面如图9-12所示。

图9-12 删除基于入接口的PQ策略配置显示界面

--步骤结束--

9.2.4 配置基于流过滤器的PQ策略

步骤

1. 在**PQ队列与接口绑定关系显示**界面图9-5中，单击**查看**按钮，进入对应的**QoS队列显示**界面，如图9-6所示。
2. 单击**配置**按钮进入**QoS队列配置**界面，如图9-13所示。

图9-13 QoS队列配置界面

3. 在**入队分类队型**下拉列表框中选择**流分类**，配置基于流过滤器的PQ队列。
4. 单击**应用**按钮，完成配置，如图9-14所示。

图9-14 基于流分类的PQ策略配置后显示界面

5. 在图9-14所示界面中，点击相应流过滤器条目后的**删除**按钮，即可删除所配置的策略，删除后的显示界面如图9-15所示。

图9-15 删除基于流分类的PQ策略配置后显示界面

--步骤结束--

9.3 CAR功能配置

9.3.1 配置基于接口的CAR策略

步骤

1. 打开QoS功能，在**QoS开关打开状态**界面图9-3中单击**CAR**区域框后的**配置**按钮，进入**CAR配置信息显示**界面，如图9-16所示。

图9-16 CAR配置信息显示界面

界面说明：

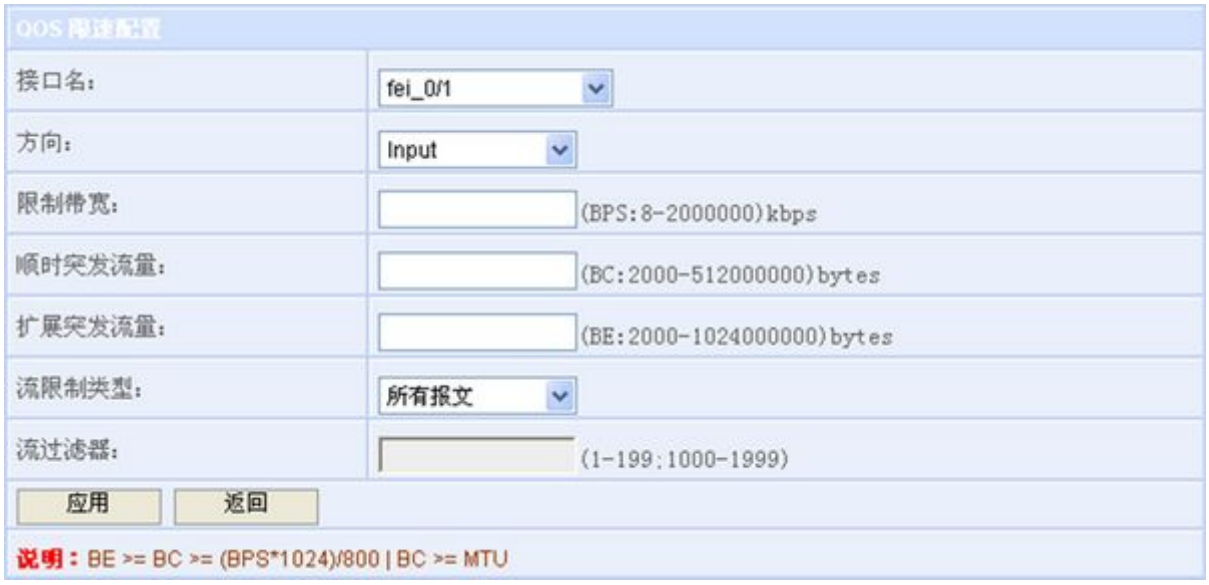
- 限速接口：需要配置CAR接口。
- 方向：CAR策略对流过接口的input或output方向的流量限速。
- 限制带宽：允许通过的流的平均速度。
- 顺时突发流量：一些流量超出限制速率之前一个突发的最大值。
- 扩展突发流量：所有流量超出限制速率之前突发的最大值。

NOTE **说明：**

CAR策略中当发送的流的流速小于限制带宽时通过，当大于限制带宽时，发送流的流速是限制带宽，超过的部分将被丢弃。

2. 单击**新增限速**按钮，进入**CAR配置**面，如图9-17所示。

图9-17 CAR配置界面



3. 在**流限制类型**下拉列表框中选择**所有报文**并填入其它相关参数，如图9-18所示。

图9-18 基于接口的CAR配置界面

4. 单击**应用**按钮，完成配置，显示界面如图9-19所示。

图9-19 CAR配置信息显示界面

5. 在图9-19所示界面中，点击相应流接口条目后的**删除**按钮，即可删除接口中绑定的CAR策略，删除后的显示界面如图9-20所示。

图9-20 删除条目后CAR显示界面

--步骤结束--

9.3.2 配置基于流过滤器的CAR策略

步骤

1. 打开QoS功能，在**QoS开关打开状态**界面图9-3中单击中**CAR**区域框后的**配置**按钮，进入**CAR配置信息显示**界面，如图9-16所示。
2. 单击**新增限速**按钮，进入**CAR配置**界面，如图9-17所示。
3. 在**流限制类型**下拉列表框中选择**指定流**，并填入其它相关参数，如图9-21所示。

图9-21 基于流过滤器的CAR配置界面

4. 单击**应用**按钮，完成配置，显示界面如图9-22所示。

图9-22 CAR配置信息显示界面

5. 在图9-22所示界面中，点击相应流过滤器条目后的**删除**按钮，即可删除接口中绑定的CAR策略，删除后的显示界面如图9-23所示。

图9-23 删除条目后CAR显示界面

--步骤结束--

10 VPN配置

本章包含如下主题：

10.1 L2TP VPN配置

10.1.1 启用L2TP VPN

步骤

1. 选择导航栏菜单[**VPN→L2TP**]，进入**L2TP VPN配置**界面，如图10−1所示。

图10-1 L2TP VPN配置界面

2. 在**启用L2TP**区域框中，选中**打开**前的单选框，弹出**确认打开L2TP**话框，如图10−2所示。

图10-2 确认打开L2TP对话框

3. 若单击**确定**按钮，则执行当前操作；若单击**取消**按钮则不改变原开关状态。

   单击**确定**按钮后，返回界面如图10-3所示。

图10-3 L2TP开关打开状态界面

4. 在**启用L2TP**区域框中，选中**关闭**前的单选框，可以将L2TP开关置为关闭状态。

NOTE **说明：**

L2TP开关默认是关闭状态，在配置LAC和LNS业务之前都需要打开L2TP开关。

--步骤结束--

10.1.2 LAC业务配置

10.1.2.1 配置LAC业务

步骤

1. 单击**L2TP VPN配置**界面图10-1中的**LAC配置**按钮，进入**LAC业务配置**界面，如图10-4所示。

图10-4 LAC业务配置界面

界面说明：

- LAC域名：LAC业务路由器中配置的用户数据库的用户组名，例如：zte.com.cn。
- 用户名：用户组下的用户名。
- 用户密码：用户名对应的用户密钥。
- LAC端口名：LAC业务路由器中和用户相连的下行用户接入侧端口。
- LAC端口认证方式：下行用户接入侧端口认证方式，有“PAP”和“CHAP”两种方式。
- 隧道对端地址：L2TP隧道的对端地址。

- 隧道源地址：L2TP隧道的源地址。
- 本地隧道名：L2TP本地隧道名，缺省为主机的hostname。
- 启用L2TP隧道认证：LAC和LNS之间的L2TP隧道认证，缺省是启用。
- 隧道认证密码：L2TP隧道认证密码。
- 隐藏L2TP敏感属性：选择是否隐藏L2TP敏感属性，缺省是不隐藏。

2. 输入相应的参数后，单击**应用**按钮完成配置，并返回**LAC业务配置显示**界面，配置成功的参数将显示在对应的输入框内，如图图10-5所示。

图10-5 LAC业务配置显示界面

--步骤结束--

10.1.2.2 修改LAC业务

步骤

1. 在**LAC业务配置显示**界面图10-5中，按需求修改各输入框中的参数。

比如将原先“启用L2TP隧道认证”状态置为不启用，可以不勾选**启用L2TP隧道认证**后的复选框。

2. 单击**应用**按钮，完成修改操作。修改后的配置如图10-6所示。

图10-6 LAC业务配置显示界面

--步骤结束--

10.1.2.3 删除LAC业务

步骤

1. 在**LAC业务配置显示**界面图10-5中单击**删除业务**按钮，弹出对话框。
2. 单击**确认**按钮即可删除LAC业务当前所有配置，删除后界面如图10-7所示。

图10-7 LAC业务配置删除后界面

NOTE **说明：**

LAC业务只支持一个VPDNGroup，组名为“webDefaultGroup”。

--步骤结束--

10.1.3 LNS业务配置

10.1.3.1 配置LNS业务

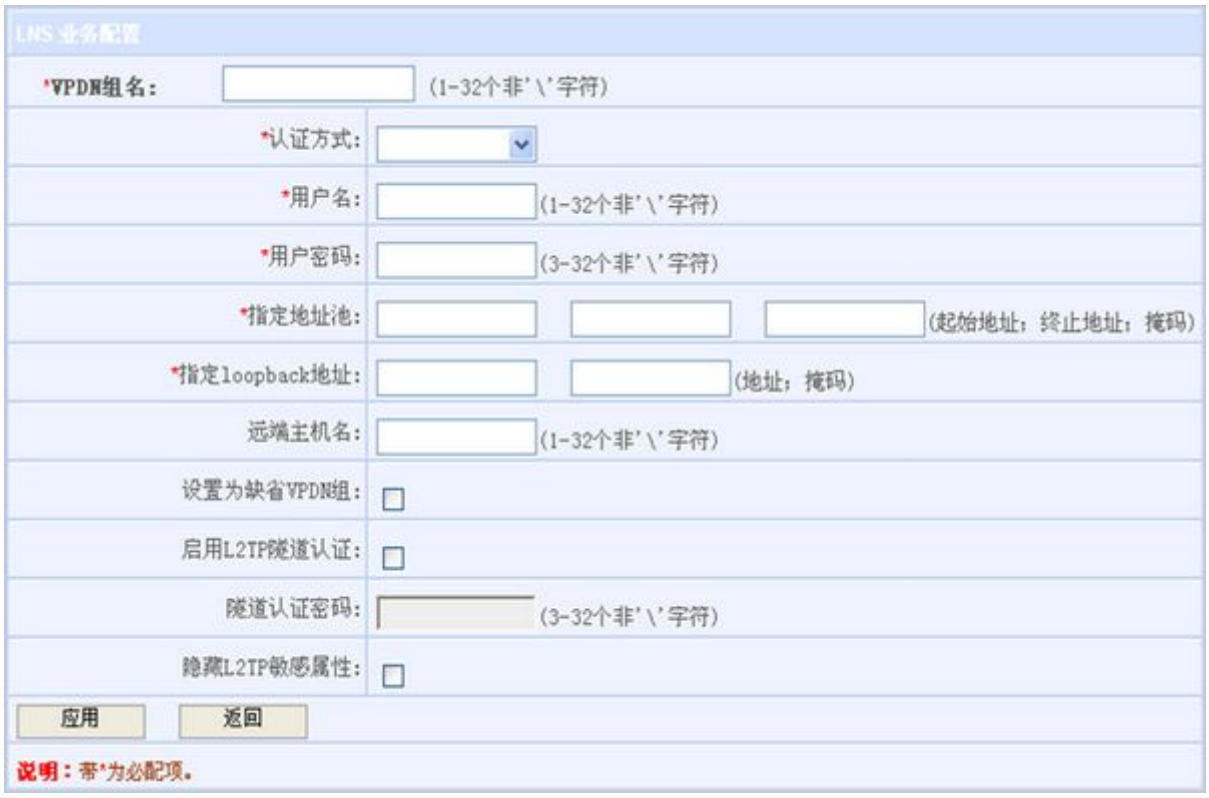
步骤

1. 单击**L2TP VPN配置**界面图10-1中的**LNS配置**按钮，进入**VPDN信息列表**界面，该界面主要是显示VPDN组以及和该VPDN组相关联的一些配置信息，如图10-8所示。

图10-8 VPDN信息列表界面1

2. 单击**VPDN信息列表**界面中的**新增VPDN组**按钮，进入详细信息配置界面，如图10-9所示。

图10-9 LNS业务配置界面



界面说明：

- VPDN组名：本地的VPDN组名。
- 认证方式：分为“PAP”和“CHAP”两种，和对端认证方式匹配使用。
- 用户名：PAP或者CHAP认证方式的用户名。
- 用户密码：PAP或者CHAP认证方式的用户密码。
- 指定地址池：配置LNS业务该VPDN组使用的地址池，分配地址给对方使用。
- 指定loopback地址：配置LNS业务该VPDN组使用的loopback地址。

- 远端主机名：隧道远端主机名，和对端匹配使用。
- 设置为缺省VPDN组：设置为缺省，当用户查找不到相应的VPDN组时，就匹配该VPDN组。默认是不设置为缺省，且系统只有一个缺省的VPDN组。
- 启用L2TP隧道认证：LNS和LAC之间的L2TP隧道认证，缺省是启用。
- 隧道认证密码：L2TP隧道认证密码。
- 隐藏L2TP敏感属性：L2TP敏感属性，缺省是不隐藏。

3. 输入相应的参数后，单击**应用**按钮完成配置，并返回**VPDN信息列表**界面，配置成功的条目信息将显示在列表内，如图10-10所示。

图10-10 VPDN信息列表界面2

NOTE **说明：**

VPDN组超过64条的话，将采用分页显示，每页最多显示64个条目。

4. **VPDN信息列表**界面中主要显示VPDN组名以及相关的基本配置信息，若要查看具体的配置信息，可以点击**VPDN信息列表**界面中的**编辑**按钮 进入**LNS业务配置信息显示**界面，如图10-11所示。

图10-11 LNS业务配置信息显示界面

--步骤结束--

10.1.3.2 修改LNS业务

步骤

1. 在**LNS业务配置显示**界面图10-11中，按需求修改各输入框中的参数。

   比如将原先“启用L2TP隧道认证”的状态置为不启用，即可不勾选**启用L2TP隧道认证**后的复选框。

2. 单击**应用**按钮，完成修改操作。修改后的配置如图10-12所示。

图10-12 LNS业务配置信息显示界面

--步骤结束--

10.1.3.3 删除LNS业务

步骤

1. 在**VPDN信息列表**界面图10-10中，点击对应VPDN条目（如［group1］）后的**删除**按钮，弹出确认对话框。
2. 单击**确认**按钮，即可删除当前VPDN组以及组关联的所有配置信息，删除后的界面如图图10-13所示。

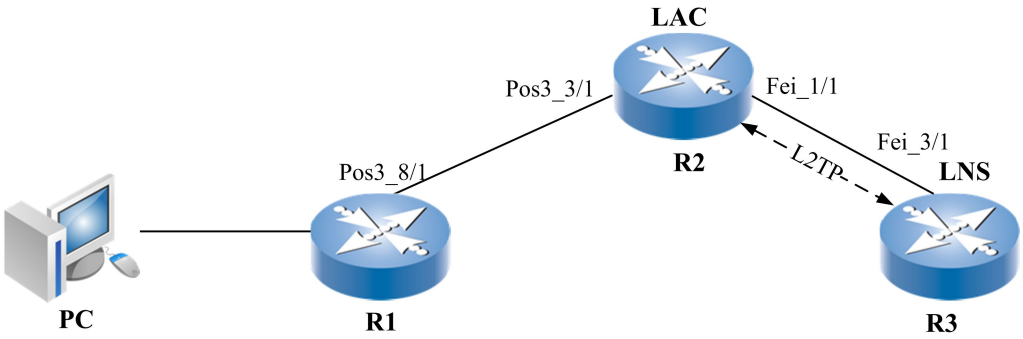
图10-13 LNS业务配置列表显示界面

--步骤结束--

10.1.4 L2TP VPN组网配置实例

图10-14为L2TP隧道免认证测试的组网实例。

图10-14 L2TP隧道免认证的组网拓扑图



1. R1的配置

   R1的pos3_8/1接口配置PAP认证方式，用户名和密码均为zte。

   该路由器不使用WEB GUI配置，此处不加描述。

2. R2（LAC）的配置

   配置要求如下：

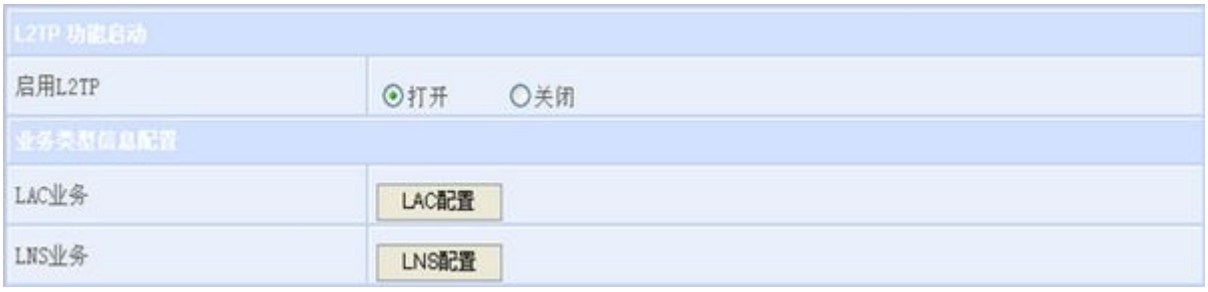
   - 使能vpdn（启用L2TP开关）。
   - 配置域名group1，用户名zte，用户密码zte。
   - 配置组名为“webDefaultGroup”的本地vpdnGroup。
   - 组“webDefaultGroup”下设置隧道对端地址为192.1.1.1。
   - 组“webDefaultGroup”下设置隧道本端地址为192.1.1.2。
   - 组“webDefaultGroup”下设置本地隧道名（主机名）为zte。
   - 组“webDefaultGroup”不启用L2TP隧道认证。
   - pos3_3/1（LAC端口）配置pap认证方式。
   - fei_1/1接口配置IP地址为192.1.1.2（接口地址在WEB GUI的**基本配置**模块中配置，此处不加描述）。

   a. 选择导航栏菜单[**VPN→L2TP**]，进入**L2TP VPN配置**界面，如图10-15所示。

图10-15 L2TP VPN配置主界面

b. 在**启用L2TP**区域框中，选中**打开**前的单选框，启用L2TP后的界面如图10-16所示。

图10-16 L2TP 开关启用显示界面



c. 单击**LAC业务**区域框中的**LAC配置**按钮进入配置界面，依据R2的配置要求在各输入框中输入相应参数，如图10-17所示。

图10-17 LAC业务配置界面

d. 单击**应用**按钮，完成R2（LAC）的配置。

3. R3（LNS）的配置

配置要求如下：

- 使能vpdn（启用L2TP开关）。
- 配置组名为“1”的本地vpdnGroup。
- 组“1”下设置服务类型为lns。
- 组“1”不启用L2TP隧道认证。
- 组“1”下设置远端主机名为zte。
- 组“1”绑定virtual-template接口（隐藏操作）。
- 该virtual-template接口下设置pap认证方式，用户名和密码均为zte。
- 该virtual-template接口下指定地址池191.1.1.1/24~191.1.1.253/24。

- 该virtual-template接口下指定loopback地址191.1.1.254/24。
- fei_3/1接口配置IP地址为192.1.1.2（接口地址在WEB GUI的**基本配置**模块中配置，此处不加描述）。

配置过程：

a. 同R2的配置，选择导航栏菜单[**VPN→L2TP**]，进入**L2TP VPN配置**界面，如图10-15所示。

b. 在**启用L2TP**区域框中，选中**打开**的单选框，启用L2TP后的界面如图10-16所示。

c. 单击图10-16界面**LNS业务**区域框中的**LNS配置**按钮进入配置界面，依据R3的配置要求在各输入框中输入相应参数，如图10-18所示。

图10-18 LNS业务配置界面

4. 单击**应用**按钮，完成R3（LNS）的配置。

10.2 IPSEC VPN配置

10.2.1 启用IPSEC VPN

步骤

1. 选择导航栏菜单[**VPN→IPSEC**]，进入**IPSEC VPN配置**界面，如图10-19所示。

图10-19 IPSEC VPN配置主界面

该界面主要包含了IPSEC功能开关设置显示、加密方式设置显示、IKE信息配置链接、接口启用策略状态查看和策略配置链接。

2. 在**启用IPSEC**区域框中，选中**打开**前的单选框，弹出**确认打开IPSEC**对话框，如图10-20所示。

图10-20 确认打开IPSEC对话框

3. 若单击**确定**按钮，则执行当前操作；若单击**取消**按钮则不改变原开关状态。

   单击**确定**按钮后，返回界面如图10-21所示。

图10-21 IPSEC开关打开状态界面

4. 在**启用IPSEC**区域框中，选中**关闭**前的单选框，可以将IPSEC开关置为关闭状态。

NOTE **说明：**

IPSEC开关状态默认是关闭的。

--步骤结束--

10.2.2 选择IPSEC加密方式

步骤

1. 在**IPSEC业务配置**界面图10-21的**加密方式**下拉列表框中选择一种加密方式，如图10-22所示。

图10-22 加密方式选择状态界面

2. 在弹出的是**确认设置的加密方式**对话框中，单击**确认**按钮，完成选择。

   例如，当前选择**cpu-security-core**加密方式，返回**IPSEC业务配置**面并且显示当前配置，如图10-23所示。

图10-23 加密方式显示界面

NOTE **说明：**

加密方式有三种，分别是“software”、“mndec-card”和“cpu-security-core”，缺省情况是“software”。

其中“cpu-security-core”是嵌入在CPU中的一种硬件加密方式，而“mndec-card”是使用一种扩展硬件加密卡的加密方式。

--步骤结束--

10.2.3 IKE信息配置

在**IPSEC业务配置**面图10-21中，单击**IKE信息配置**区域框中的**配置**按钮，进入**ISAKMP信息配置显示**界面，如图10-24所示。

图10-24 ISAKMP信息配置显示界面

该界面主要包括IKE的标识、NAT穿透、DPD使能的配置显示和ISAKMP预共享密钥列表、协商类型列表、策略信息列表显示以及各新增列表配置的链接。

10.2.3.1 配置IKE标识

步骤

1. 在**ISAKMP信息显示**界面图10-24中的**IKE标识**下拉列表框中选择一种方式。
2. 单击**应用**按钮完成配置，如图10-25所示。

图10-25 IKE标识配置显示界面

NOTE **说明：**

IKE标识有两种选择方式：address和hostname，缺省为address方式。

--步骤结束--

10.2.3.2 配置NAT穿透

步骤

1. 在**ISAKMP信息显示**界面图10-24中，选中**启用NAT穿透**后的复选框（缺省为不启用）。
2. 单击**应用**按钮即启用NAT穿透功能，如图10-26所示。

图10-26 NAT穿透启用显示界面

3. 若不选中**启用NAT穿透**后的复选框，单击**应用**按钮则可以恢复缺省值。

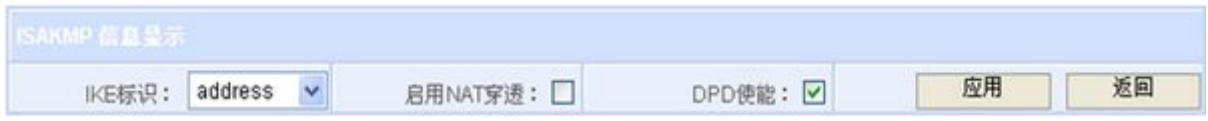
--步骤结束--

10.2.3.3 配置DPD使能

步骤

1. 在**ISAKMP信息显示**界面图10-24中，选中**DPD使能**后的复选框（缺省为不使能）。
2. 单击**应用**按钮即使能DPD功能，如图10-27所示。

图10-27 DPD使能显示界面



3. 若不选中**DPD使能**后的复选框，单击**应用**按钮则可以恢复缺省值。

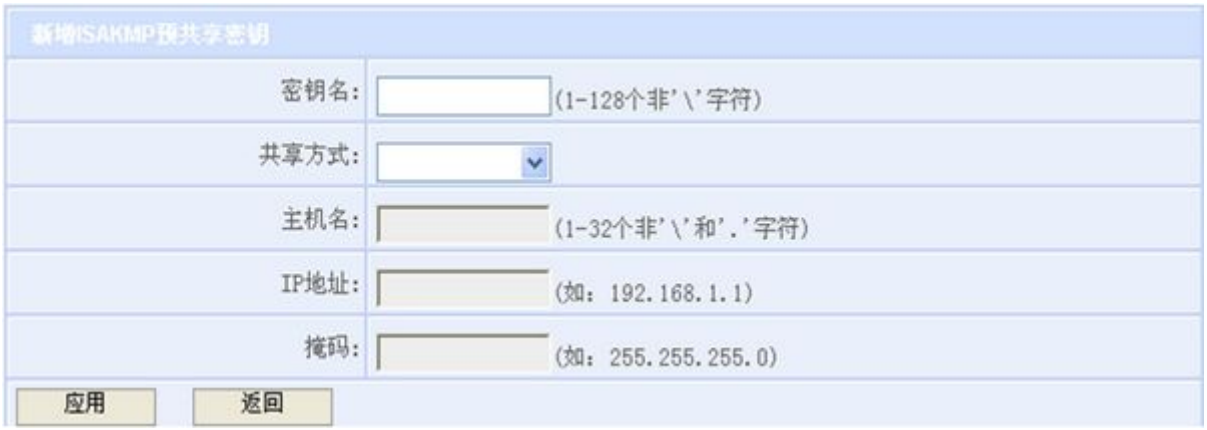
--步骤结束--

10.2.3.4 配置ISAKMP预共享密钥

步骤

1. 单击**ISAKMP信息显示**界面图10-24中的**新增密钥**按钮，进入**新增密钥配置**界面，如图10-28所示。

图10-28 新增密钥配置界面

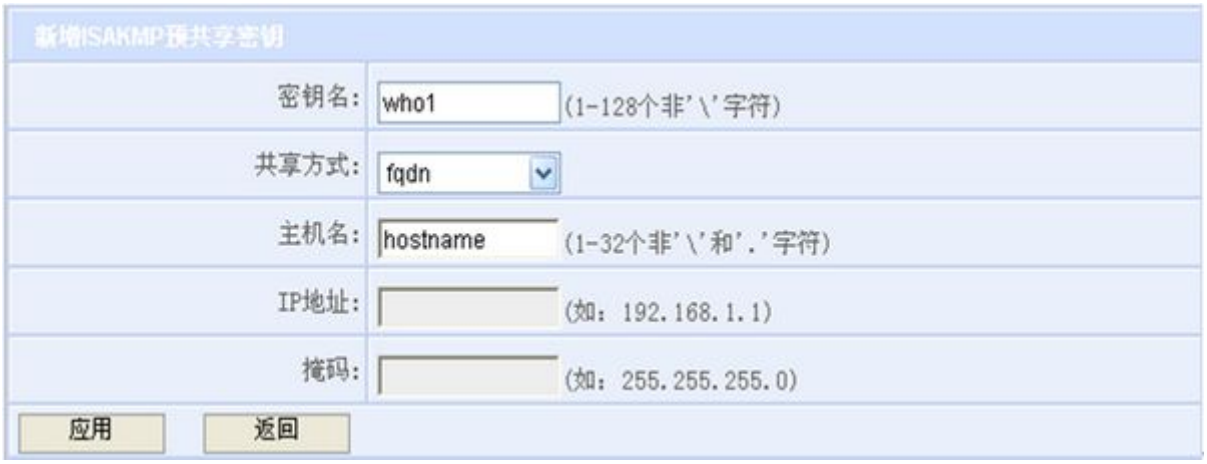


界面说明：

- 密钥名：预共享密钥名。
- 共享方式：分为“fqdn”、“address”两种。
- 主机名：选择“fqdn”方式时，需要填写主机名。
- IP地址：选择“address”方式时，需要填写IP地址。
- 掩码：IP地址的掩码。

2. 配置参数
   - 若在**共享方式**下拉列表框中选择**fqdn**方式，不需要配置IP地址和掩码（对应文本框变为灰色），在**密钥名**和**主机名**输入框中输入参数，如图10-29所示。

图10-29 新增密钥配置界面



- 若在**共享方式**下拉列表框中选择**address**方式，不需要配置主机名（对应文本框变为灰色），在**密钥名**、**IP地址**和**掩码**入框中输入参数即可，如图10-30所示。

图10-30 新增密钥配置界面

3. 配置参数完成后，单击**应用**按钮，返回到如图10-31所示界面，进行信息显示。

图10-31 预共享密钥显示界面1

4. 如果要删除列表，可在图10-31显示列表中点击**删除**按钮，会弹出对话框，单击**确认**按钮即可删除对应条目信息。如删除密钥名为**who1**的条目，可点击该条目后的按钮，完成操作后，返回界面如图10-32所示。

图10-32 预共享密钥显示界面2

--步骤结束--

10.2.3.5 配置ISAKMP协商类型

步骤

1. 单击**ISAKMP信息配置显示**界面图10-24中的**新增模式**按钮，进入**新增协商类型配置**界面，如图10-33所示。

图10-33 新增协商类型配置界面1

界面说明：

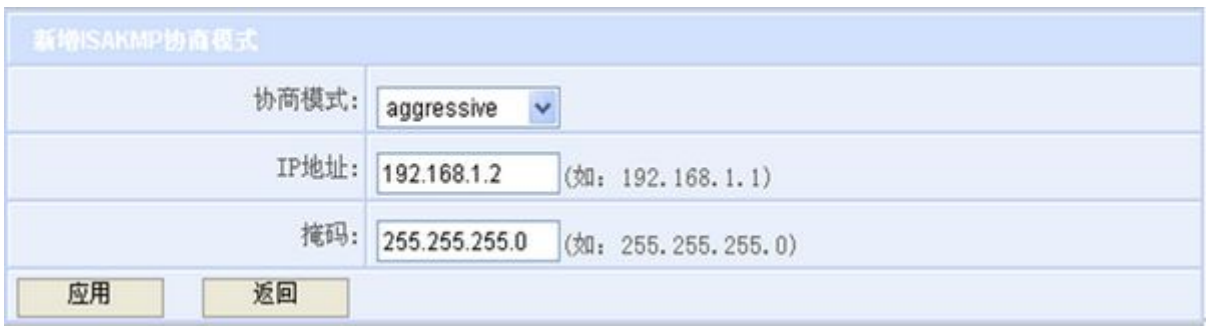
- 协商模式：分为“main”和“aggressive”两种，缺省是“main”交换模式。
- IP地址：协商配置的IP地址。
- 掩码：IP地址的掩码。

2. 在**协商模式**下拉列表框中选择一种协商模式。
3. 在**IP地址**和**掩码**输入框中输入参数。

   选择**main**交换模式的配置完成界面如图10-34所示，选择**aggressive**交换模式的配置完成界面如图10-35所示。

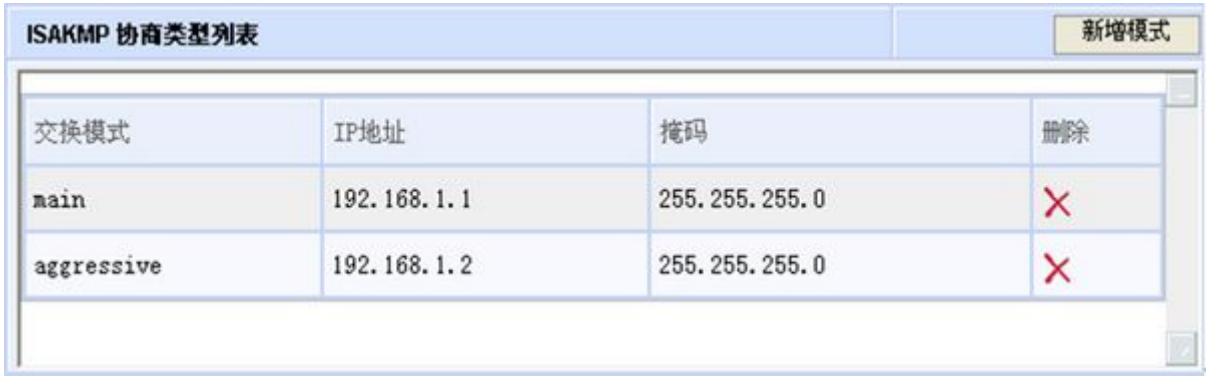
图10-34 新增协商类型配置界面2

图10-35 新增协商类型配置界面3



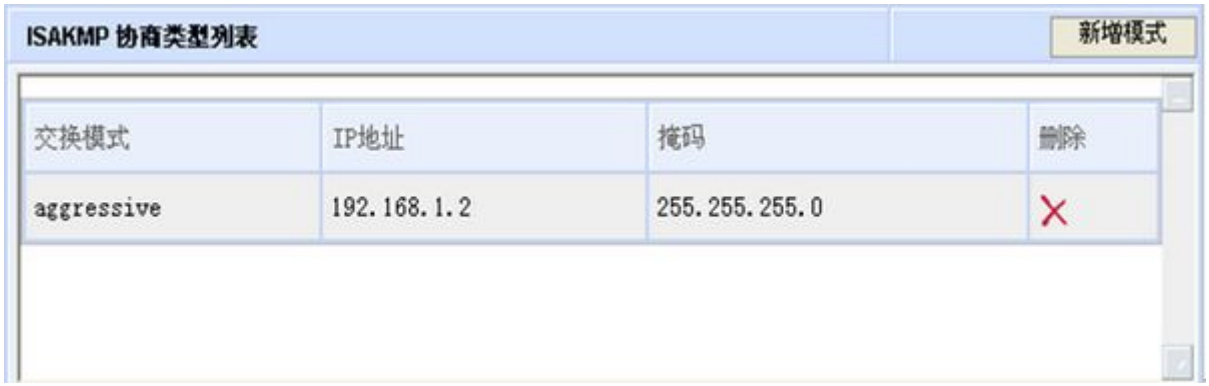
4. 配置参数完成后，单击**应用**按钮，返回到如图10-36所示界面，进行信息显示。

图10-36 协商类型显示界面



5. 如果要删除列表，可在图10-36显示列表中点击**删除**按钮，会弹出对话框，单击**确认**按钮即可删除对应条目信息。如删除IP地址为**192.168.1.1**，交换模式为**main**的条目，可点击该条目后的按钮，完成操作后，返回界面如图10-37所示。

图10-37 协商类型显示界面



--步骤结束--

10.2.3.6 配置ISAKMP策略信息

步骤

1. 单击**ISAKMP信息配置显示**界面图10-24中的**新增策略**按钮，进入**新增策略信息配置**界面，如图10-38所示。

图10-38 新增策略信息配置界面1

界面说明：

- ISAKMP策略号：范围1~10000。
- 策略加密算法：分为“3des”、“des”和“aes-128”三种，缺省为“3des”。
- 策略HASH算法：分为“md5”和“sha1”两种，缺省为“sha1”。
- 策略DH交换群：分为“group 1”（MODP群768位）和“group 2”（MODP群1024位），缺省为“group 1”。

2. 在各输入框中输入相应参数，如图10-39所示。

图10-39 新增策略信息配置界面2

3. 配置参数完成后，单击**应用**按钮，返回到如图10-40所示界面，进行信息显示。

图10-40 策略信息显示界面

4. 如果要删除列表，可在图10-40显示列表中点击**删除**按钮，会弹出对话框，单击**确认**按钮即可删除对应条目信息。如删除策略号为**1**的条目，可点击该条目后的按钮，完成操作后，返回界面如图10-41所示。

图10-41 策略信息显示界面

--步骤结束--

10.2.4 配置IPSEC策略

步骤

1. 选择导航栏菜单[**VPN→IPSEC**]，进入**IPSEC VPN配置**界面，如图10-42所示。

图10-42 IPSEC VPN配置主界面

界面说明：

策略启用列表标记为“Y”表示接口已经启用IPSEC策略，标记为“N”表示没有启用策略。

2. 选择需要配置策略的接口。
3. 点击该接口后相应的**策略配置**按钮，并进入**IPSEC策略配置**界面，如图10-43所示。

图10-43 IPSEC策略配置主界面

NOTE **说明:**

配置IPSEC策略之前，需要先配置策略指定的转码集。转码集可以配置多个，但策略只能指定其中一个转码集名。

--步骤结束--

10.2.4.1 配置转码集

步骤

1. 在**IPSEC策略配置**界面图10-43的**新增转码集配置**区域框中，输入要配置的各相应参数，如图10-44所示。

图10-44 新增转码集配置界面

界面说明：

- 转码集名：用字符串表示，长度不能超过18个字符。
- 封装模式：分为“tunnel”和“transport”两种模式，缺省为“tunnel”模式。
- 认证方式：分为“ah-md5-hmac”、“ah-sha-hmac”、“esp-md5-hmac”和“esp- sha -hmac”四种方式。
- 加密算法：分为“esp-3des”、“esp-des”、“esp-aes-128”和“esp-null”四种算法。

2. 完成配置后，单击**应用**按钮，返回**转码集信息显示**界面显示配置的条目，如图10-45所示。

图10-45 转码集信息显示界面

3. 如果要删除转码集配置，可在图10-45**转码集信息显示**界面中点击**删除**按钮，会弹出对话框，单击**确认**按钮即可删除对应条目信息。如删除转码集名为**set1**的条目，可点击该条目后的按钮，完成操作后，返回界面如图10-46所示。

图10-46 转码集信息显示界面

--步骤结束--

10.2.4.2 配置IPSEC策略信息

相关信息

IPSEC策略信息的配置分为两种情况：

- 不启用动态安全策略；
- 启用动态安全策略。

如果不启用动态安全策略，需要指定对端地址或者主机名；如果启用动态安全策略，则不需要指定对端地址或者主机名。

步骤

1. 在**IPSEC策略配置**界面图10-43的**接口xx IPSEC策略信息配置**区域框中，输入要配置的各相应参数（不启用动态安全策略），如图10-47所示。

图10-47 IPSEC策略配置主界面

2. 完成配置后，单击**应用**按钮，可将配置生效的信息显示在各输入框中，如图10-48所示。

图10-48 IPSEC策略信息显示界面

此时**IPSEC策略配置**界面中的**删除策略**按钮不再是灰色的，说明对应接口下已经应用了IPSEC策略。

同时返回**IPSEC VPN配置**主界面可以看到接口**fei_1/1**对应条目后的**策略启用**状态变为**Y**，说明该接口已经应用策略，如图10-49所示。

图10-49 IPSEC策略应用显示界面

3. 配置完策略信息后，可在**IPSEC策略信息显示**界面图10-48中修改输入框内的参数进行配置修改操作。

   如要将**指定流过滤器**的**100**修改为**1999**，则可直接在对应输入框内进行修改，修改后单击**应用**按钮即可，如图10-50所示。

图10-50 IPSEC策略信息配置界面

4. 若要删除策略，必须当接口应用了IPSEC策略信息，即显示界面上的**删除策略**按钮不再是灰色的情况下进行删除。

   此时，可单击**删除策略**按钮将接口下配置的策略信息删除。删除后各输入框内的参数被清空，**删除策略**按钮自动变为灰色，如图10-51所示。

图10-51 IPSEC策略信息显示界面

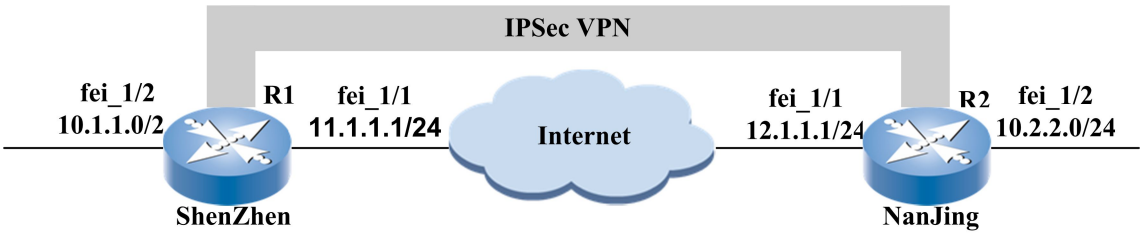
--步骤结束--

10.2.5 IPSEC VPN组网配置实例

10.2.5.1 IKE协商配置实例

图10-52为IKE协商（两端为固定公网IP）的组网实例。

图10-52 IKE协商（两端为固定公网IP）组网拓扑图



R1（Shenzhen）的配置要求如下：

- 开启ISAKMP，开启IPSec（界面上合并为一个开关控制）。
- 配置感兴趣流号101：permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255（该配置在**流过滤器**模块中配置）。
- 配置ISAKMP预共享密钥名zxr10，共享方式address，IP地址12.1.1.1/32。
- 配置ISAKMP策略信息，策略号为10（要和对方匹配）。
- 协商预共享方式pre-share（缺省），加密算法3des，HASH算法sha1，DH交换群group 2（要和对方匹配）。
- 配置转码集名set1：加密算法esp-3des，认证方式esp-sha-hmac（要和对方匹配）。
- 配置IPSEC策略名webCryptoName1（自动生成）：策略顺序号1（缺省），策略类型isakmp（缺省），匹配感兴趣流101，匹配对端地址12.1.1.1，指定转码集set1。
- 接口fei_1/1启用IPSEC策略（隐藏操作）。
- 接口fei_1/1配置地址11.1.1.1/24（该配置在**基本配置**模块中配置）。
- 接口fei_1/2配置地址10.1.1.1/24（该配置在**基本配置**模块中配置）。
- 配置静态路由ip route 0.0.0.0 0.0.0.0 11.1.1.2（该配置在**静态路由**模块中配置）。

R2（Nanjing）的配置要求如下：

- 开启ISAKMP，开启IPSec（界面上合并为一个开关控制）。
- 配置感兴趣流号101：permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255（该配置在**流过滤器**模块中配置）。
- 配置ISAKMP预共享密钥名zxr10，共享方式address，IP地址11.1.1.1/32。
- 配置ISAKMP策略信息，策略号10（要和对方匹配）。

- 协商预共享方式pre-share（缺省），加密算法3des，HASH算法sha，DH交换群group 2。
- 配置转码集名set1：加密算法esp-3des，认证方式esp-sha-hmac。
- 配置IPSEC策略名webCryptoName1(自动生成)：策略顺序号1(缺省)，策略类型isakmp(缺省)，匹配感兴趣流101，匹配对端地址11.1.1.1，指定转码集set1。
- 接口fei_1/1启用IPSEC策略（隐藏操作）。
- 接口fei_1/1配置地址12.1.1.1/24（该配置在**基本配置**模块中配置）。
- 接口fei_1/2配置地址10.2.2.1/24（该配置在**基本配置**模块中配置）。
- 配置静态路由ip route 0.0.0.0 0.0.0.0 12.1.1.2（该配置在**静态路由**模块中配置）。

R1的配置过程：

1. 启用IPSEC vpn功能开关

   a. 选择导航栏菜单[**VPN→IPSEC**]，进入**IPSEC VPN配置**界面，如图10-53所示。

图10-53 IPSEC VPN配置主界面

b. 在**启用IPSEC**区域栏中，选中**打开**前的单选框，启用IPSEC功能开关（同时开启ISAKMP），启用后的界面如图10-54所示。

图10-54 IPSEC开关启用显示界面

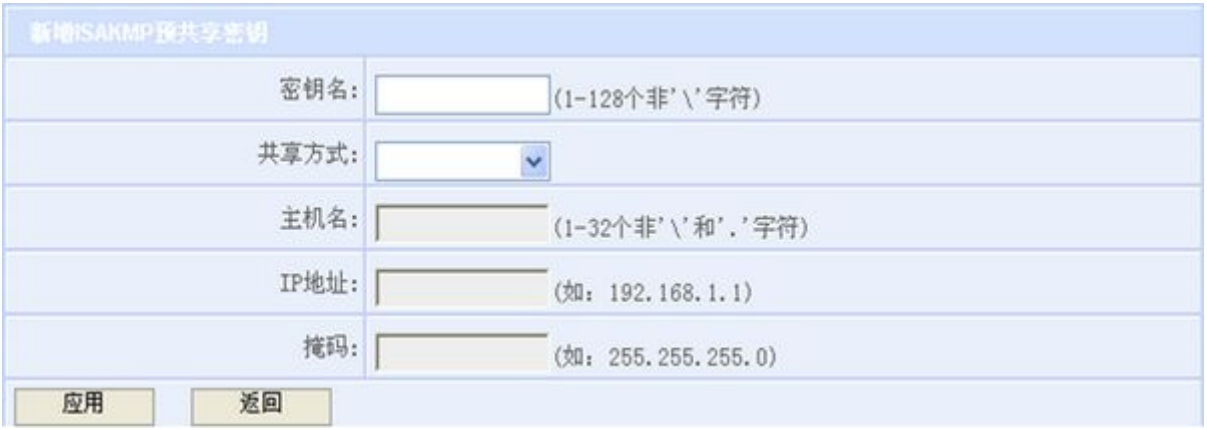
2. 配置ISAKMP预共享密钥

a. 单击**IKE信息配置**区域栏中的**配置**按钮，进入**ISAKMP信息配置显示**界面，如图10-55所示。

图10-55 ISAKMP信息配置显示界面

b. 单击**新增密钥**按钮，进入**新增密钥配置**界面，如图10-56所示。

图10-56 新增密钥配置界面



c. 在**密钥名**输入框中输入**zxr10**

d. 在**共享方式**下拉列表框中选择**address**

e. 在**IP地址**输入框中输入**12.1.1.1**

f. 在**掩码**输入框中输入**255.255.255.255**

g. 单击**应用**按钮，完成ISAKMP预共享密钥配置，界面如图10-57所示。

图10-57 IKE预共享密钥配置界面

3. 配置ISAKMP策略信息

a. 单击**ISAKMP信息配置显示**界面图10-55中的**新增策略**按钮，进入**新增策略信息配置**界面，如图10-58所示。

图10-58 新增策略信息配置界面

b. 在**ISAKMP策略号**输入框中输**10**

c. 在**策略加密算法**下拉列表框中选择**3des**。

d. 在**策略HASH算法**下拉列表框中选择**sha1**。

e. 在**策略DH交换群**下拉列表框中选择**2**，界面如图10-59所示。

图10-59 ISAKMP策略信息配置界面

f. 单击**应用**按钮，完成ISAKMP策略信息配置，返回界面如图10-60所示。

图10-60 ISAKMP信息显示界面

4. 配置转码集

a. 在**IPSEC VPN配置**界面图10-53中选择要配置的接口**fei_1/1**，点击该接口后相应的**策略配置**按钮，并进入**IPSEC策略配置**界面，如图10-61所示。

图10-61 IPSEC策略配置主界面

b. 在**新增转码集配置**区域框中的**转码集**输入框中输入**set1**

c. 在**封装模式**下拉列表框中选择**tunnel**

d. 在**认证方式**下拉列表框中选择**esp-sha-hmac**

e. 在**加密算法**下拉列表框中选择**esp-3des**，界面如图10-62所示

图10-62 新增转码集配置界面

f. 完成配置后，单击**应用**按钮，返回**转码集信息显示**界面显示配置的条目，如图10-63所示。

图10-63 转码集信息显示界面

5. 配置IPSEC策略信息

a. 在**IPSEC策略配置**界面图10-61的**接口fei_1/1 IPSEC策略信息配置**区域框的**指定流过滤器**输入框中输入**101**

b. 在**指定转码集名**下拉列表框中选择**set1**

c. 在**指定对端地址或主机名**下拉列表框中选择**ipaddress**

d. 在**地址**输入框中输入**12.1.1.1**，界面如图10-64所示。

图10-64 IPSEC策略配置界面

e. 单击**应用**按钮，完成IPSEC配置，此时配置的策略自动对接口fei_1/1生效。

配置完成后返回**IPSEC VPN配置**界面，可以看到接口**fei_1/1**的**策略启用**状态显示为**Y**，表示该接口已经启用IPSEC策略，如图10-65所示。

图10-65 IPSEC策略应用状态显示界面

IPSEC业务应用

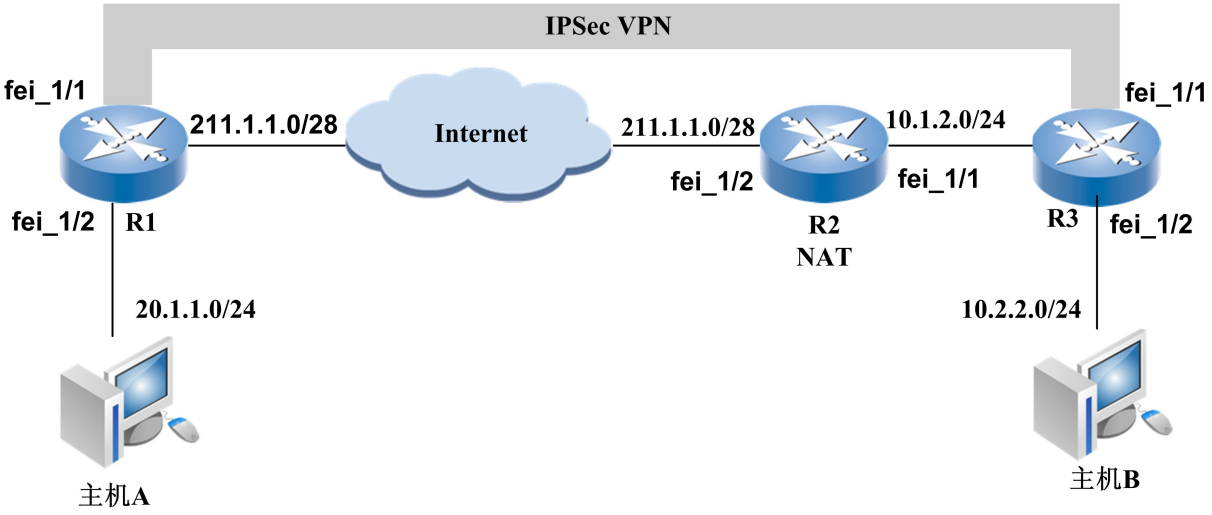
接口名	策略启用	策略配置
fei_1/1	Y	
gei_0/1	N	
gei_0/1.1	N	

R2的配置同R1，此处不加描述。

10.2.5.2 IKE穿越NAT配置实例

图10-66为IKE穿越NAT的组网实例。R3作为发起者发起IPSec协商，NAT设备(R2)的FEI_1/1接口作为NAT inside，FEI_1/2作为NAT outside。R1作为IPSec响应者。

图10-66 IKE穿越NAT组网拓扑图



R1的配置要求如下：

- 开启ISAKMP，开启IPSec（界面上合并为一个开关控制）。
- 使能NAT穿越。
- 配置感兴趣流号101：permit ip 20.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255（该配置在**流过滤器**模块中配置）。
- 配置ISAKMP预共享密钥名zxr10，共享方式fqdn，主机名nanjing。
- 配置ISAKMP策略信息，策略号为10（要和对方匹配）。
- 协商预共享方式pre-share（缺省），加密算法3des，HASH算法sha1，DH交换群group 2（要和对方匹配）。
- 配置转码集名set1：加密算法esp-3des，认证方式esp-sha-hmac（要和对方匹配）。
- 配置动态IPSEC策略名webCryptoName1（自动生成）：策略顺序号1（缺省），策略类型isakmp（缺省），匹配感兴趣流101，指定转码集set1，动态策略webCryptoName1绑定到静态策略webCryptoName1里（隐藏操作）。
- 接口fei_1/1启用IPSEC策略（隐藏操作）。
- 接口fei_1/1配置地址211.1.1.1/28（该配置在**基本配置**模块中配置）。
- 接口fei_1/2配置地址20.1.1.1/24（该配置在**基本配置**模块中配置）。
- 配置静态路由ip route 0.0.0.0 0.0.0.0 211.1.1.2（该配置在**静态路由**模块中配置）。

R2（NAT网关）的配置要求如下：

- 开启NAT功能（该配置在**NAT**模块中配置）。
- 接口fei_1/1配置为NAT的inside接口，接口fei_1/2配置为NAT的outside接口（该配置在**NAT**模块中配置）。

- 接口fei_1/1配置地址为10.1.2.2/24（该配置在**基本配置**模块中配置）。
- 接口fei_1/2配置地址为211.1.1.2/28（该配置在**基本配置**模块中配置）。

R3（IPSEC发起者）的配置要求如下：

- 开启ISAKMP，开启IPSec（界面上合并为一个开关控制）。
- 使能NAT穿越。
- 配置感兴趣流号101：permit ip 10.2.2.0 0.0.0.255 20.1.1.0 0.0.0.255（该配置在**流过滤器**模块中配置）。
- 配置ISAKMP预共享密钥名zxr10，共享方式address，IP地址211.1.1.1/32。
- 配置ISAKMP策略信息，策略号为10（要和对方匹配）。
- 协商预共享方式pre-share（缺省），加密算法3des，HASH算法sha1，DH交换群group 2（要和对方匹配）。
- 配置IKE阶段1j协商模式aggressive，IP地址211.1.1.1/32。
- 配置IKE标识hostname方式。
- 配置转码集名set1：加密算法esp-3des，认证方式esp-sha-hmac（要和对方匹配）。
- 配置IPSEC策略名webCryptoName1（自动生成）：策略顺序号1（缺省），策略类型isakmp（缺省），匹配感兴趣流101，匹配对端地址211.1.1.1，指定转码集set1。
- 接口fei_1/1启用IPSEC策略（隐藏操作）。
- 接口fei_1/1配置地址10.1.2.1/24（该配置在**基本配置**模块中配置）。
- 接口fei_1/2配置地址10.2.2.1/24（该配置在**基本配置**模块中配置）。
- 配置静态路由ip route 0.0.0.0 0.0.0.0 10.1.2.2（该配置在**静态路由**模块中配置）。

R1的配置过程：

1. 启用IPSEC VPN功能开关

   a. 选择导航栏菜单[**VPN→IPSEC**]，进入**IPSEC VPN配置**界面，如图10-67所示。

图10-67 IPSEC VPN配置主界面

b. 在**启用IPSEC**区域栏中，选中**打开**前的单选框，启用IPSEC功能开关（同时开启ISAKMP），启用后的界面如图10-68所示。

图10-68 IPSEC开关启用显示界面

2. 使能NAT穿越

a. 单击**IKE信息配置**区域栏中的**配置**按钮，进入**ISAKMP信息配置显示**界面，如图10-69所示。

图10-69 ISAKMP信息配置显示界面

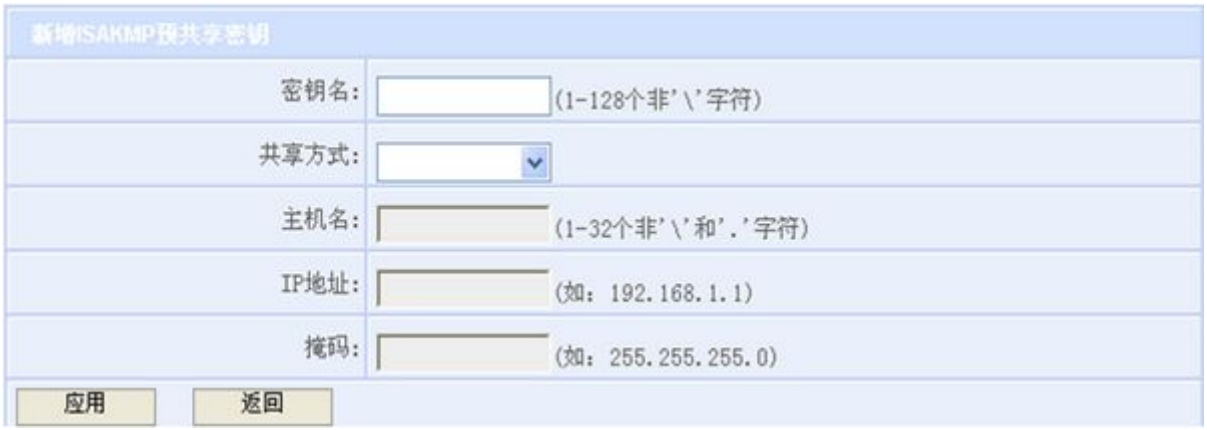
b. 在**ISAKMP信息显示**区域栏中，选中**启用NAT穿透**后的复选框即可使能NAT穿越功能，使能后的界面如图10-70所示。

图10-70 NAT穿越使能显示界面

3. 配置ISAKMP预共享密钥

a. 单击**ISAKMP信息配置显示**界面图10-69中的**新增密钥**按钮，进入**新增密钥配置**界面，如图10-71所示。

图10-71 新增密钥配置界面



b. 在**密钥名**输入框中输入**zxr10**

c. 在**共享方式**下拉列表框中选择**fqdn**

d. 在**主机名**输入框中输入**nanjing**

e. 单击**应用**按钮，完成ISAKMP预共享密钥配置，界面如图10-72所示。

图10-72 IKE预共享密钥配置界面

4. 配置ISAKMP策略信息

a. 单击**ISAKMP信息配置显示**界面图10-69中的**新增策略**按钮，进入**新增策略信息配置**界面，如图10-73所示。

图10-73 新增策略信息配置界面

b. 在**ISAKMP策略号**输入框中输入**10**

c. 在**策略加密算法**下拉列表框中选择**3des**

d. 在**策略HASH算法**下拉列表框中选择**sha1**

e. 在**策略DH交换群**下拉列表框中选择**2**，界面如图10-74所示

图10-74 ISAKMP策略信息配置界面

f. 单击**应用**按钮，完成ISAKMP策略信息配置，返回界面如图10-75所示。

图10-75 ISAKMP信息显示界面

5. 配置转码集

a. 在**IPSEC VPN配置**界面图10-67中选择要配置的接口**fei_1/1**，点击该接口后相应的**策略配置**按钮，并进入**IPSEC策略配置**界面，如图10-76所示。

图10-76 IPSEC策略配置主界面

b. 在**新增转码集配置**区域框中的**转码集**输入框中输入**set1**

c. 在**封装模式**下拉列表框中选择**tunnel**

d. 在**认证方式**下拉列表框中选择**esp-sha-hmac**

e. 在**加密算法**下拉列表框中选择**esp-3des**，界面如图10-77所示

图10-77 新增转码集配置界面

f. 完成配置后，单击**应用**按钮，返回**转码集信息显示**界面显示配置的条目，如所图10-78示。

图10-78 转码集信息显示界面

6. 转码集信息显示界面

a. 在**IPSEC策略配置**界面图10-76的**接口fei_1/1 IPSEC策略信息配置**区域框中，选中**启用动态安全策略**后面的复选框。

b. 在**指定流过滤器**输入框中输入**101**

c. 在**指定转码集名**下拉列表框中选择**set1**，界面如图10-79所示。

图10-79 IPSEC策略配置界面

d. 单击**应用**按钮，完成IPSEC配置，此时配置的策略自动对接口fei_1/1生效。

配置完成后返回**IPSEC VPN配置**界面，可以看到接口**fei_1/1**的**策略启用**状态显示为**Y**，表示该接口已经启用IPSEC策略，如图10-80所示。

图10-80 IPSEC策略应用状态显示界面

IPSEC业务应用

接口名	策略启用	策略配置
fei_1/1	Y	
gei_0/1	N	
gei_0/1.1	N	

R2的配置同R1，此处不加描述，R3以及其他相关配置略。

11 防火墙配置

本章包含如下主题：

11.1 防火墙业务简介

防火墙业务按照应用范围分为：防火墙全局业务和防火墙接口业务。

全局业务配置主要有：MAC过滤全局策略设置、黑名单业务全局开关设置、防DOS攻击防欺骗和异常包检测业务全局开关设置、P2P限流业务。

接口业务配置主要有：即时通讯拦截业务设置、MAC过滤业务设置、黑名单业务设置、防ARP欺骗业务设置、防DOS防欺骗和异常包检测业务设置、WEB过滤业务设置。

按照业务类型分为：P2P限流业务、即时通讯拦截业务、MAC过滤业务、黑名单业务、防ARP欺骗业务、WEB过滤业务、防DOS攻击防欺骗和异常包检测业务。

下面对各种业务分别进行介绍。

1. P2P限流业务

   实现对P2P数据流的会话数限制以及速度限制。P2P限流业务针对所有数据流进行限制，它保证来自某一个源地址的会话数不能超过用户设定的最大单元会话数（即发自某源地址的最大连接数）。若会话数超过最大单元会话数，则触发对这个源地址的所有已建立会话的流量限制。

2. 即时通讯拦截业务

   主要分为QQ拦截和MSN拦截。当收到一个数据包时，查看访问的服务器地址在路由器中是否已经设置，如设置则数据包就被拦截。

3. MAC过滤业务

   根据以太网帧头中的源MAC地址与配置的过滤MAC地址进行比较，若比较结果匹配，则报文根据策略执行操作，从而达到控制二层数据帧的目的，这样可以降低非法报文的处理时间。

4. 黑名单业务

通过限制访问用户的源IP地址进行过滤，如果收到数据包的源地址不在黑名单范围内，则包被放行；如果在黑名单范围内，系统会将包丢弃，并且提供日志。

5. 防ARP欺骗业务

该模块主要分为三部分，分别为接口下设置ARP-keepAlive开关、ARP扫描和MAC-IP绑定业务。

ARP欺骗业务即正常通信的主机A和B之间，收到来自C的伪装成A或B的ARP更新报文，从而A或B认 C是与之通信的对方，从而直接将通信内容发给C，C就可以窃取A和B之间的通信内容。通过接口下设置ARP-keepAlive开关、ARP扫描和MAC-IP绑定业务可以防止ARP欺骗的攻击。

- ARP-keepAlive开关

  在以太接口下添加ARP KEEPALIVE 功能。

  默认情况下路由器就会以1次/秒的速度向内网广播免费ARP报文（免费ARP报文是一种特殊的ARP报文，该报文中携带的发送者IP地址和目标IP地址都是本机IP地址，发送者MAC地址是本机MAC地址，目标MAC地址是广播地址），如果ARP攻击软件发送的ARP欺骗包的速度比路由器发送的慢，那么主机就不会受到ARP攻击的影响。默认情况下是关闭此功能。

- MAC-IP绑定业务

  根据用户的配置，在特定的IP地址和MAC地址之间形成关联关系。对于声称从这个IP地址发送的报文，如果其MAC地址不是指定关系对中的地址，将予以丢弃，这是避免IP地址假冒攻击的一种方式。

- ARP扫描

  ARP扫描功能，可以一次性的将学习到的地址进行IP+MAC绑定或者进行ARP固化。

6. WEB过滤业务

对企业网应用来说，基于HTTP的WEB访问占据企业流量的大部分。因此对WEB访问进行有效管理是企业网用户考虑的重要议题。针对这种状况，我们实现WEB过滤功能，方便用户对企业内部员工的WEB访问进行有效管理。

WEB过滤业务主要提供以下功能：

- 实现URL过滤，有效过滤非健康网站、含有病毒的网站等。
- 实现URL参数过滤，对get、put、post等WEB请求进行有效管理。
- 对java applet、exe、zip、ActiveX控件小程序的有效阻止，防止病毒、木马程序的引入。

- 对WEB过滤进行有效的日志管理。
- 对某些特殊的用户可以不进行WEB过滤。

7. 防DOS攻击防欺骗和异常包检测业务

- 异常包检测

  网络攻击者可以通过精心设计封包来执行侦查或发起拒绝服务（DoS）攻击。有时网络管理者不太清楚此类封包的意图，但由于封包是精心设计的，这就暗示它会被用到某些类型的阴险用途中。此时可以通过配置SCREEN规则丢弃此类报文，从而起到保护网络用户的功能。

- 攻击防范（DDOS攻击等）

  DoS（Denial Of Service，拒绝服务）攻击的目的是用极大量的虚拟信息流耗尽目标受害者的资源，使受害者被迫全力处理虚假信息流，而无法处理合法信息流。攻击的目标可以是路由器本身、ZXR10 ZSR所控制访问的网络资源或者个别主机的特定硬件平台或操作系统（OS），因此可以通过配置SCREEN组的规则丢弃相应的数据报，起到保护网络用户的功能。

- 防欺骗

  每个攻击者执行攻击前通常都需要收集信息，因此可以将收集信息的尝试作为攻击的前兆，通过配置安全防范SCREEN组的规则来丢弃相应的数据报，起到保护网络用户的功能。

11.2 防火墙全局业务配置

选择导航栏菜单[**防火墙→防火墙业务**]，进入**防火墙业务配置**界面，如图11-1所示。

图11-1 防火墙业务配置主界面

本界面主要分为防火墙全局业务配置和防火墙接口业务配置链接，全局业务配置主要包括策略设置、开关设置和P2P限流业务设置。

11.2.1 配置MAC过滤策略

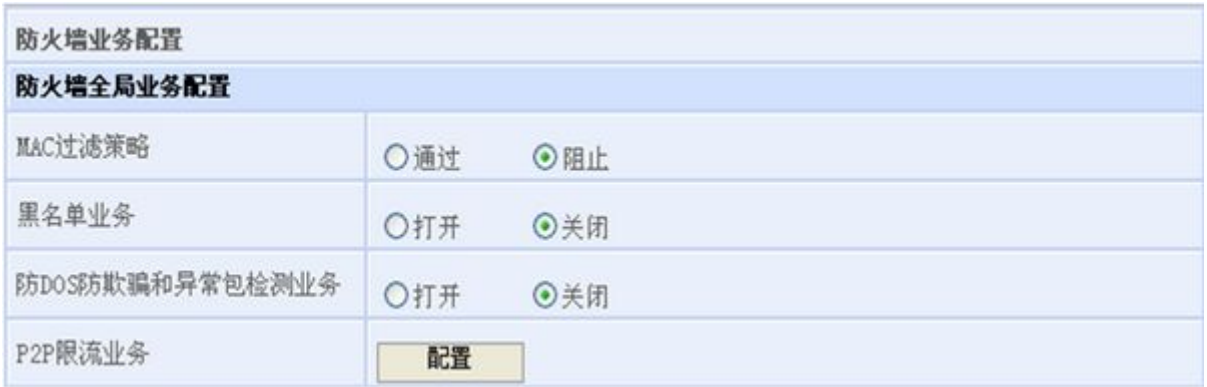
步骤

1. 进入**防火墙业务配置**界面，如图11-1所示。
2. 在**防火墙全局业务配置**区域框的**MAC过滤策略**区域栏中，选中**通过**前的单选框，则当前MAC过滤全局业务策略为通过状态，也是缺省状态。
3. 若要阻止MAC过滤策略，则在**MAC过滤策略**区域框中，选中**阻止**前的单选框，并弹出确认对话框，如图11-2所示。

图11-2 确认对话框

4. 若单击**确定**按钮则执行当前操作，若单击**取消**按钮则不改变原策略状态。单击**确定**按钮后返回显示界面，如图11-3所示。

图11-3 防火墙MAC过滤全局业务策略状态显示



NOTE **说明：**

防火墙MAC过滤全局策略生效优先级比MAC过滤接口策略低。如果数据包流经的接口设置了对应该数据包的策略，则执行接口下的策略，并且不再查询全局策略；如果接口上没有设置对应该数据包的策略，则执行全局策略，全局策略是针对所有数据包的。

--步骤结束--

11.2.2 启用黑名单业务

步骤

1. 在**防火墙全局业务配置**区域框的**黑名单业务**区域栏中，选中**打开**前的单选框，并弹出确认对话框，如图11-4所示。

图11-4 确认打开黑名单业务对话框

2. 单击**确定**按钮，打开黑名单业务；若单击**取消**按钮，则不改变原开关状态。

   单击**确定**按钮后返回显示界面如图11-5所示。

图11-5 防火墙黑名单业务全局开关状态显示

3. 若要关闭黑名单业务，可以在**黑名单业务**区域框中，选中**关闭**前的单选框，则黑名单业务全局开关恢复为关闭状态，也是缺省状态。

NOTE **说明：**

只有防火墙黑名单业务全局开关处于开启状态时，才能配置接口下的黑名单业务。同时在关闭黑名单业务全局开关之前，要先删除所有接口下的黑名单业务配置。

--步骤结束--

11.2.3 启用防DOS防欺骗和异常包检测业务

步骤

1. 在**防火墙全局业务配置**区域框的**防DOS防欺骗和异常包检测业务**区域栏中，选中**打开**前的单选框，并弹出确认对话框，如图11-6所示。

图11-6 确认对话框

2. 单击**确定**按钮，打开防DOS防欺骗和异常包检测业务；若单击**取消**按钮，则不改变原开关状态。

   单击**确定**按钮后返回显示界面如图11-7所示。

图11-7 防火墙防DOS攻击全局开关状态显示

3. 若要关闭防DOS防欺骗和异常包检测业务，可以在**防DOS防欺骗和异常包检测业务**区域框中，选中**关闭**前的单选框，在弹出的对话框中单击**确定**按钮，则防DOS防欺骗和异常包检测业务全局开关恢复为关闭状态，也是缺省状态。

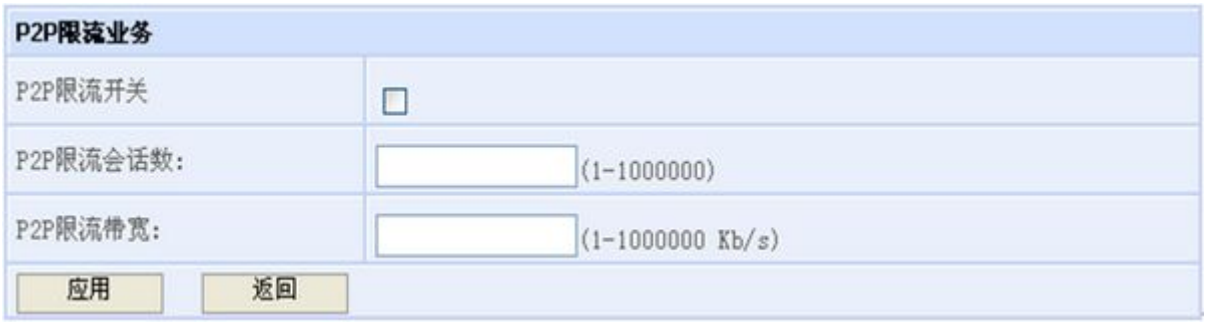
--步骤结束--

11.2.4 配置P2P限流业务

步骤

1. 在**防火墙业务配置**界面图11-1的**防火墙全局业务配置**区域框中，点击**P2P限流业务**区域栏后的**配置**按钮，进入**P2P限流业务配置**界面，如图11-8所示。

图11-8 P2P限流业务配置界面

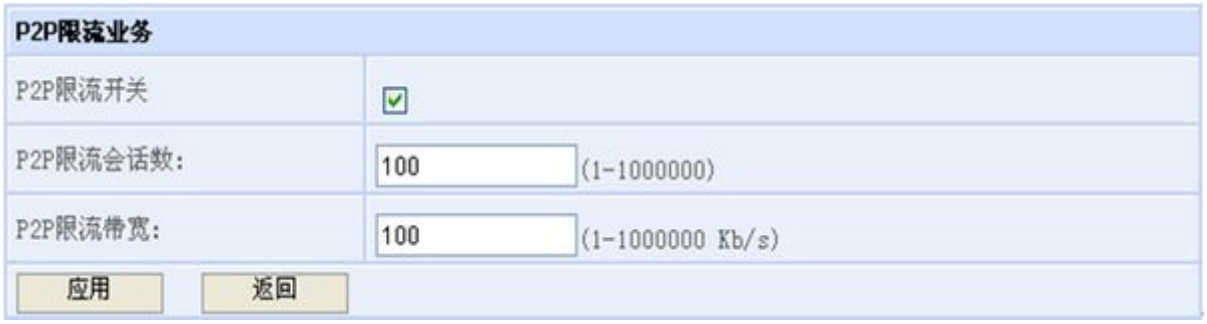


界面说明：

- P2P限流开关：缺省关闭。
- P2P限流会话数：范围1~1000000。
- P2P限流带宽：范围1 ~ 1000000Kb/s。

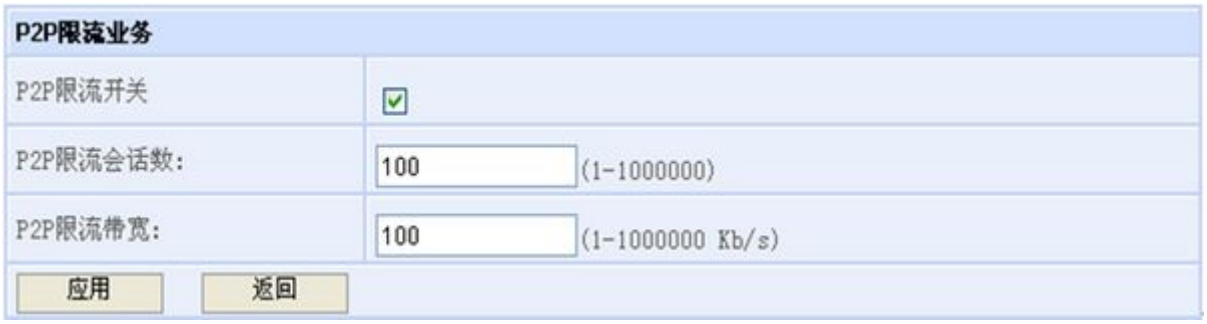
2. 在**P2P限流业务**界面中输入各相应参数，如图11-9所示。

图11-9 P2P限流业务配置界面



3. 单击**应用**按钮完成配置，并返回**P2P限流业务**界面，并且把配置生效的参数显示在输入框内，如图11-10所示。

图11-10 P2P限流业务配置显示界面

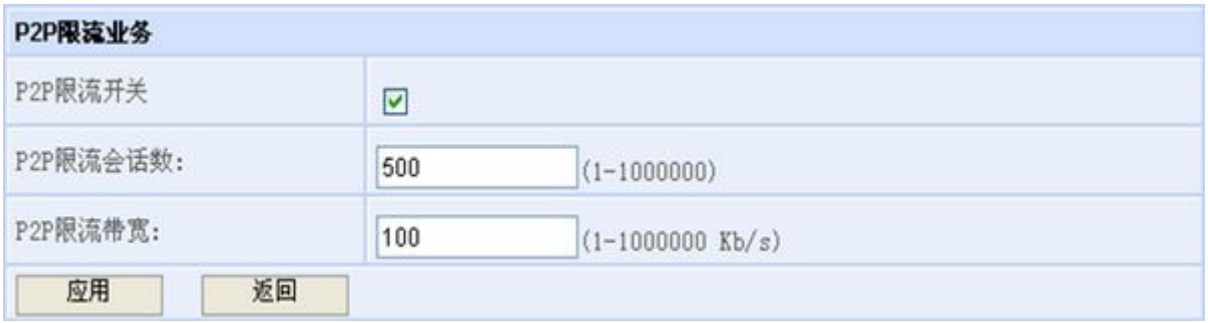


4. 在**P2P限流业务**界面图11-10中重新填入新的参数可执行修改操作。

   例如修改会话数“100”为“500”，此时只需要在**P2P限流会话数**输入框内输入**500**

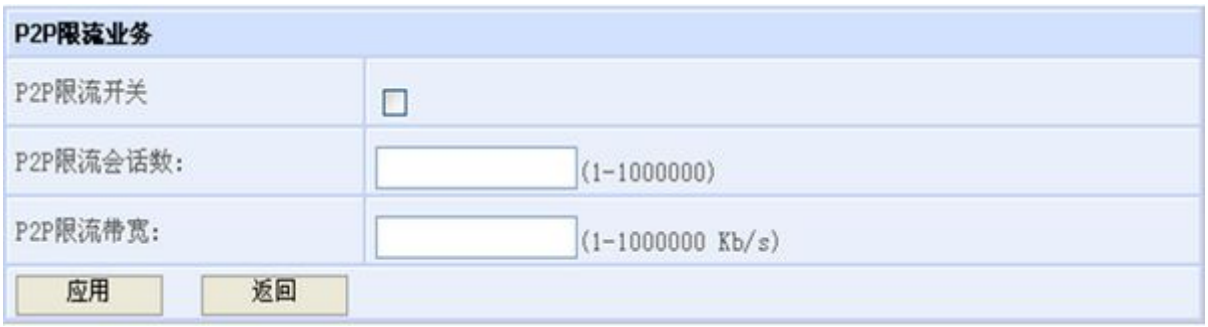
5. 修改完成后，单击**应用**按钮即可，生效的界面如图11-11所示。

图11-11 P2P限流业务配置显示界面



6. 在**P2P限流业务**界面图11-11中，不勾选**P2P限流开关**后的复选框，单击**应用**按钮即可删除P2P限流业务。生效的界面如图11-12所示。

图11-12 P2P限流业务配置显示界面



--步骤结束--

11.3 配置防火墙接口业务

步骤

1. 选择导航栏菜单[**防火墙→防火墙业务**]，进入**防火墙业务配置**界面，如图11-13所示。

图11-13 防火墙业务配置主界面

2. 在**防火墙接口业务配置**区域框的**接口名**下拉列表框中选择要启用业务的接口。
3. 单击**配置**按钮进入**接口***防火墙业务配置**界面，如图11-14所示。

图11-14 防火墙接口业务配置选择界面

4. 选择需要配置的业务，单击对应的**配置**按钮即可进入该业务的配置界面。

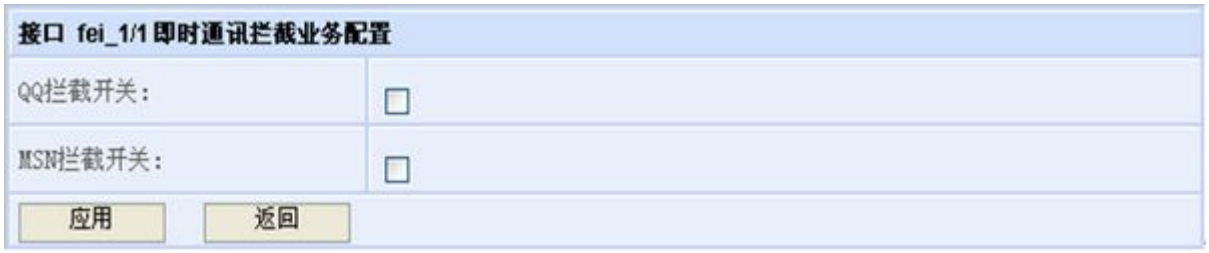
--步骤结束--

11.3.1 配置即时通讯拦截业务

步骤

1. 在**接口***防火墙业务配置**界面图11-14中，单击**即时通讯拦截业务**区域栏后的**配置**按钮，进入**接口***即时通讯拦截业务配置**界面，如图11-15所示。

图11-15 接口即时通讯拦截业务配置界面

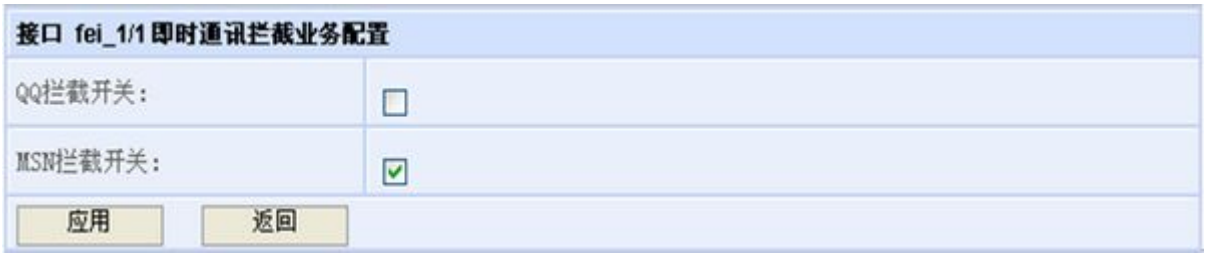


即时通讯拦截业务配置主要分为QQ拦截开关和MSN拦截开关配置，缺省状态都是不开启的

2. 若要开启即时通讯拦截业务，只需选中相应即时工具后的复选框即可。

   例如，要开启MSN拦截开关，需选中**MSN拦截开关**后面的复选框，单击**应用**按钮完成配置。如图11-16所示。

图11-16 接口即时通讯拦截业务配置界面



--步骤结束--

11.3.2 MAC过滤业务配置

在**接口***防火墙业务配置**界面图11-14中，单击**MAC过滤业务**区域栏后的**配置**按钮，进入**接口***MAC过滤业务**界面，如图11-17所示。

图11-17 接口MAC过滤业务界面

该配置界面主要包含了接口下MAC过滤开关设置、MAC过滤条目新增、显示、编辑和删除操作。

11.3.2.1 启用MAC过滤

步骤

1. 在**接口***MAC过滤业务**界面图11-17的**过滤开关**区域栏中，选中**打开**前的单选框，弹出确认对话框，如图11-18所示。

   图11-18 确认打开MAC过滤对话框

2. 单击**确定**按钮，打开MAC过滤开关；若单击**取消**按钮则不改变原开关状态。

   单击**确定**按钮后返回界面如图11-19所示。

图11-19 MAC过滤开关配置显示界面

3. 若要关闭MAC过滤开关，则在**过滤开关**区域栏中，选中**关闭**前的单选框并且单击**确定**按钮，则MAC过滤开关恢复为关闭状态。

NOTE **说明：**

只有接口下MAC过滤处于打开状态，转发时才会查询接口下设置的策略，否则直接查询全局MAC过滤策略。

--步骤结束--

11.3.2.2 配置MAC过滤条目

步骤

1. 进入**接口***MAC过滤业务**界面，如图11-17所示。
2. 在**新增MAC过滤条目**区域框的**MAC地址**输入框中输入要配置的MAC地址。
3. 在**过滤方式**下拉列表框中选择相应的过滤方式（permit或者deny），界面如图11-20所示。

图11-20 MAC过滤条目新增配置界面

4. 单击**应用**按钮完成新增条目配置，配置生效的条目将在**MAC过滤条目信息显示**区域栏中显示出来，如图11-21所示。

图11-21 MAC过滤条目配置显示界面

NOTE **说明：**

当MAC过滤条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

11.3.2.3 修改MAC过滤条目

步骤

1. 在**MAC过滤条目配置显示**界面的**MAC过滤条目信息显示**区域栏中，点击相应MAC地址条目后的**编辑**按钮，系统会将当前条目信息填入**新增MAC过滤条目**区域栏的输入框中。

   此时，MAC地址变为灰色，修改操作只能对**过滤方式**进行修改，如图11-22所示。

图11-22 MAC过滤条目配置修改界面

2. 在**过滤方式**下拉列表框中选择**deny**。
3. 单击**应用**按钮完成修改配置操作。修改后的显示界面如图11-23所示。

图11-23 MAC过滤条目配置修改后显示界面

--步骤结束--

11.3.2.4 删除MAC过滤条目

步骤

1. 在**MAC过滤条目配置显示**界面的**MAC过滤条目信息显示**区域栏中，点击对应条目后的**删除**按钮，会弹出确认对话框中。

2. 单击**确定**按钮，即可以将当前条目删除。删除后的条目不会在**MAC过滤条目信息显示**区域栏中显示。

   如删除“MAC地址”为“1111.1111.1111”的条目，删除后的界面显示如图11-24所示。

图11-24 MAC过滤条目配置修改后显示界面

--步骤结束--

11.3.3 黑名单业务配置

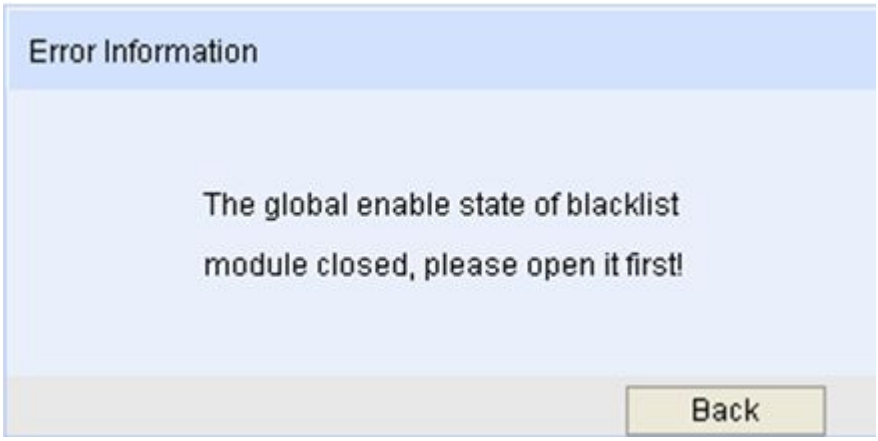
在**接口防火墙业务配置**界面图11-14中，单击**黑名单业务**区域栏后的**配置**按钮，进入**接口黑名单业务配置**界面，如图11-25所示。

图11-25 黑名单业务配置界面

该配置界面主要包含了接口下黑名单日志开关设置、黑名单条目新增、显示和删除操作。

在进入**接口黑名单业务配置**界面之前，如果出现信息提示如图11-26所示，说明黑名单的全局业务开关没有打开。此时，需要单击信息提示界面中的**Back**按钮，返回到**防火墙业务配置**界面图11-1，将黑名单业务全局开关打开，再进行接口下的黑名单业务配置。

图11-26 黑名单业务配置错误界面



11.3.3.1 启用黑名单业务

步骤

1. 在**接口黑名单业务配置**界面图11-25的**日志开关**区域栏中，选中**打开**前的单选框，弹出**确认打开日志**对话框，如图11-27所示。

图11-27 确认打开日志对话框

2. 单击**确定**按钮，打开黑名单日志开关；若单击**取消**按钮则不改变原开关状态。

   单击**确定**按钮后返回界面如图11-28所示。

图11-28 黑名单接口下日志开关显示界面

3. 若要关闭黑名单日志开关，则在**日志开关**区域栏中，选中**关闭**前的单选框，在弹出的对话框中单击**确定**按钮，则日志开关恢复为关闭状态。

   --步骤结束--

11.3.3.2 配置黑名单条目

步骤

1. 进入**接口黑名单业务配置**界面，如图11-25所示。
2. 在**新增黑名单条目**区域框的**IP地址**输入框中输入要配置的IP地址。
3. 在**掩码**输入框中输入掩码（掩码长度至少为24位），界面如图11-29所示。

图11-29 黑名单条目新增配置界面

4. 单击**应用**按钮完成新增黑名单条目配置，配置生效的条目将在**黑名单条目信息显示**区域栏中显示出来，如图11-30所示。

图11-30 黑名单条目配置显示界面

NOTE **说明：**

当黑名单条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

11.3.3.3 删除黑名单条目

步骤

1. 在**黑名单条目配置显示**界面的**黑名单条目信息显示**区域栏中，点击对应条目后的**删除**按钮，在弹出的对话框中单击**确定**按钮，即可将当前条目删除。删除后的条目不会在**黑名单配置信息显示**区域栏中显示。

   如删除“IP地址”为“192.168.1.0”的条目，删除后的界面显示如图11-31所示。

图11-31 黑名单条目配置显示界面

NOTE **说明：**

图11-30界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务是指将该接口下的黑名单业务当前所有配置（包括日志和配置的黑名单条目）都删除，所以请慎重使用。

--步骤结束--

11.3.4 防ARP欺骗业务配置

在**接口防火墙业务配置**界面图11-14中，单击**防ARP欺骗业务**区域栏后的**配置**按钮，进入**接口防ARP欺骗业务**界面，如图11-32所示。

图11-32 接口防ARP欺骗业务界面

该界面主要包含了接口下ARP-keepAlive开关设置、ARP扫描功能按钮、MAC-IP绑定条目的配置、显示和删除。

11.3.4.1 启用ARP-keepAlive

步骤

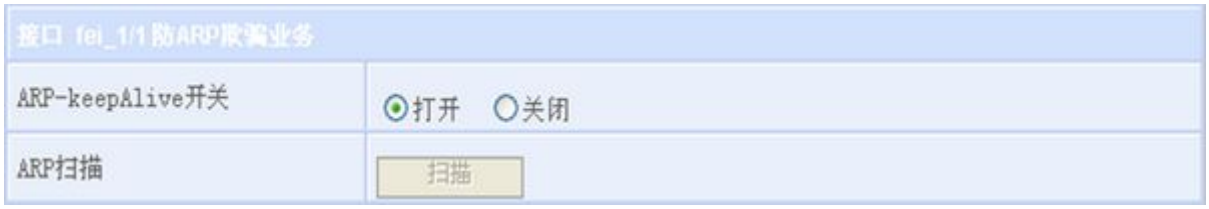
1. 在**扫描接口防ARP欺骗业务**界面图11-32的**ARP-keepAlive开关**区域栏中，选中**打开**前的单选框，弹出**确认打开ARP-keepAlive**对话框，如图11-33所示。

图11-33 确认打开ARP-keepAlive对话框

2. 单击**确定**按钮，打开ARP-keepAlive开关；若单击**取消**按钮则不改变原开关状态。

   单击**确定**按钮后返回界面如图11-34所示。

图11-34 防ARP欺骗业务ARP-keepAlive开关显示界面



3. 若要关闭ARP-keepAlive开关，则在**ARP-keepAlive开关**区域栏中，选中**关闭**前的单选框并且单击**确定**按钮，则ARP-keepAlive开关恢复为关闭状态。
4. 单击**接口防ARP欺骗业务**界面图11-34的**ARP扫描**区域栏后的**扫描**按钮，系统立即执行扫描功能，并将扫描到的条目显示在**MAC-IP绑定条目信息显示**区域栏中。

NOTE **说明：**

只有当接口下已经存在MAC-IP绑定条目时才可以点击**扫描**按钮，否则按钮处于灰色状态，禁止使用。

--步骤结束--

11.3.4.2 配置MAC-IP绑定条目

步骤

1. 进入**接口防ARP欺骗业务**界面，如图11-32所示。
2. 在**新增MAC-IP绑定条目**区域框的**IP地址**输入框中输入要配置的IP地址。
3. 在**MAC地址**输入框中输入相应的MAC地址，界面如图11-35所示。

图11-35 MAC-IP绑定条目新增配置界面

4. 单击**应用**按钮完成新增MAC-IP绑定条目配置，配置生效的条目将在**MAC-IP绑定条目信息显示**区域栏中显示出来，如图11-36所示。

图11-36 MAC-IP绑定条目配置显示界面

NOTE **说明：**

当MAC-IP绑定条目超过64条时，将采用分页显示，每页最多显示64个条目。

--步骤结束--

11.3.4.3 删除MAC-IP绑定条目

步骤

1. 在**MAC-IP绑定条目配置显示**界面的**MAC-IP绑定条目信息显示**区域栏中，点击对应条目后的**删除**按钮 ，弹出确认对话框。
2. 单击**确定**按钮，即可将当前条目删除。删除后的条目不会在**MAC-IP绑定条目信息显示**区域栏中显示。

   如删除“IP地址”为“192.168.1.1”的条目，删除后的界面显示如图11-37所示。

图11-37 MAC-IP绑定条目显示界面

NOTE **说明：**

图11-36界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务是指将该接口下的防ARP欺骗业务当前所有配置都删除掉（包括ARP-keepAlive开关和所有MAC-IP绑定条目），所以请慎重使用。

--步骤结束--

11.3.5 防DOS防欺骗和异常包检测业务配置

在**接口防火墙业务配置**界面图11-14中，单击**防DOS防欺骗和异常包检测业务**区域栏后的**配置**按钮，进入**防DOS防欺骗和异常包检测业务配置**界面，如图11-38所示。

图11-38 防DOS防欺骗和异常包检测业务配置界面

该配置界面主要包含了接口下防DOS攻击、防欺骗和异常包检测三个子业务的配置。

1. 防DOS攻击业务包含：
   - 防LAND攻击；
   - 防WinNuke攻击；
   - 防TearDrop攻击；
   - 防Ping-of-death攻击；
   - 防ICMP泛滥攻击；
   - 防UDP泛滥攻击。
2. 防欺骗业务包含：
   - IP欺骗检测；
   - SYN/FIN的TCP包检测；
   - FIN_noACK的TCP包检测；
   - 未设置标志的TCP包检测；
   - IP地址扫描检测；

- 端口扫描检测；
- IP选项网络侦察。

3. 异常包检测业务包含：
   - 坏的IP选项检测；
   - 未知协议包检测；
   - IP碎片包检测；
   - SYN碎片包检测；
   - ICMP碎片包检测
   - 大的ICMP数据包检测。

11.3.5.1 配置防DOS防欺骗和异常包检测业务

步骤

1. 在**防DOS防欺骗和异常包检测业务配置**界面图11-38中选择需要配置的业务，选中对应业务前面的复选框，如图11-39所示。

图11-39 防DOS防欺骗和异常包检测业务配置界面

NOTE **说明：**

配置带有阀值参数的业务时，如果不手动输入参数，服务器将默认取缺省参数。

2. 单击**应用**按钮完成配置，并返回**防DOS防欺骗和异常包检测业务配置显示**界面，此时配置生效的业务会显示在该界面上，如图11-40所示。

图11-40 防DOS防欺骗和异常包检测业务配置显示界面1

NOTE **说明：**

此时可以再次选择界面上的其他业务进行新增业务配置。

--步骤结束--

11.3.5.2 修改防DOS防欺骗和异常包检测业务

步骤

1. 在**防DOS防欺骗和异常包检测业务配置显示**界面图11-40中，按需求修改各输入框中的参数。

例如修改端口扫描业务的扫描阀值，只需要在**防欺骗业务配置**区域框内**端口扫描检测**一栏的**扫描阀值**输入框中重新输入参数。

2. 修改完成后，单击**应用** 按钮。

修改**端口扫描检测**的扫描阀值**100**为**500**后的界面如图11-41所示。

图11-41 防DOS防欺骗和异常包检测业务配置修改界面

--步骤结束--

11.3.5.3 删除防DOS防欺骗和异常包检测业务

步骤

1. 在**防DOS防欺骗和异常包检测业务配置显示**界面图11-40中，不选中要删除条目前面的复选框。
2. 单击**应用**按钮即可完成业务删除操作。

如删除端口扫描业务后的界面显示如图11-42所示。

图11-42 防DOS防欺骗和异常包检测业务配置显示界面2

NOTE **说明：**

图11-42界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务是指将该接口下的防DOS防欺骗和异常包检测业务当前所有配置都删除掉，所以请慎重使用。

--步骤结束--

11.3.6 WEB过滤业务配置

在**接口防火墙业务配置**界面图11-14中，点击**WEB过滤业务**后面的下拉列表框，可以看到有**网页地址过滤业务**、**网站IP地址过滤业务**、**网页参数过滤业务**和**小程序阻断业务**四个子业务选择提示，如图11-43所示。

图11-43 WEB过滤业务子业务选择界面

11.3.6.1 配置网页地址过滤业务

步骤

1. 在**WEB过滤业务子业务选择**界面图11-43的**WEB过滤业务**下拉列表框中选择**网页地址过滤业务**，进入**网页地址过滤业务配置**界面，如图11-44所示。

图11-44 网页地址过滤业务配置界面

界面说明：

- 日志开关：缺省是“关闭”状态。
- 缺省过滤动作：当匹配不到关键字时，则执行缺省过滤动作，缺省是“通过”状态。
- 关键字：网页地址过滤业务匹配的关键字。
- 过滤动作：匹配关键字的过滤动作，有“permit”和“block”两种方式。

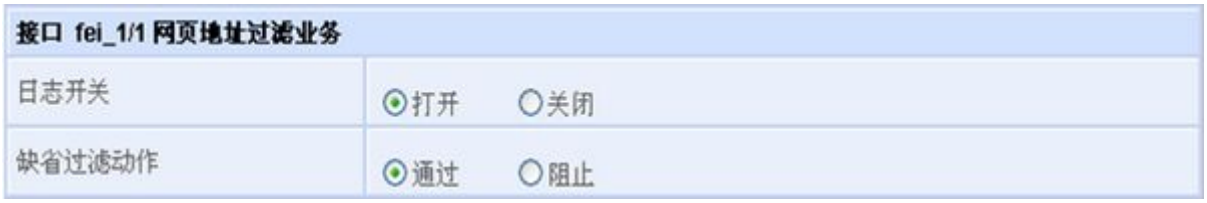
2. 启用网页地址过滤业务日志

a. 在**网页地址过滤业务配置**界面图11-44的**日志开关**区域栏中，选中**打开**前的单选框，弹出确认对话框，如图11-45所示。

图11-45 确认打开日志开关对话框

b. 单击**确定**按钮，打开日志开关；若单击**取消**按钮，打开日志开关；若单击**确定**按钮后返回界面如图11-46所示。

图11-46 网页地址过滤业务日志开关显示界面



c. 若要关闭日志开关，则在**日志开关**区域栏中，选中**关闭**前的单选框并且单击**确定**按钮，则日志开关恢复为关闭状态。

3. 配置网页地址过滤业务缺省过滤动作

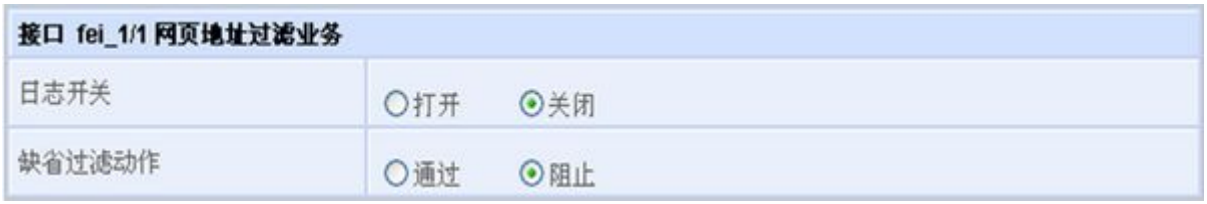
a. 在**网页地址过滤业务配置**界面图11-44的**缺省过滤动作**区域栏中，选中**阻止**前的单选框，弹出确认对话框，如图11-47所示。

图11-47 确认缺省过滤动作设置为阻止对话框

b. 若单击**确定**按钮则执行当前操作，缺省过滤动作变为阻止；若单击**取消**按钮则不改变原策略状态。

单击**确定**按钮后返回界面如图11-48所示。

图11-48 网页地址过滤业务缺省过滤动作显示界面



c. 若要设置缺省过滤动作为通过，则在**缺省过滤动作**区域栏中，选中**通过**前的单选框并且单击**确定**按钮，则过滤动作恢复为通过状态。

4. 配置网页地址过滤条目

a. 进入**网页地址过滤业务配置**界面，如图11-44所示。

b. 在**新增网页地址过滤条目**区域框的**关键字**输入框中输入要配置的关键字（关键字为1~31个非‘\’字符）。

c. 在**过滤动作**下拉列表框中选择相应的过滤动作，界面如图11-49所示。

图11-49 网页地址过滤业务过滤条目配置界面

NOTE **说明：**

在进行网页地址过滤时，如果访问的网页地址匹配到设置的条目时，执行该条目设置的过滤动作，如果查找不到条目，则执行缺省过滤动作设置的策略。

d. 单击**应用**按钮完成网页地址过滤条目配置，配置生效的条目将在**网页地址过滤条目信息显示**区域栏中显示出来，如图11-50所示。

图11-50 网页地址过滤业务过滤条目配置显示界面

NOTE **说明：**

当过滤条目超过64条时，将采用分页显示，每页最多显示64个条目

5. 修改网页地址过滤条目

在**网页地址过滤条目信息显示**区域框中，点击要修改的条目后面的在**网页地址过滤条目信息显示**区域框中，点击要修改的条目后面的**编辑**按钮，可以对已经存在的条目进行过滤动作修改。

例如要修改关键字“zte.com.cn”的过滤动作“block”为“permit”，操作步骤如下：

a. 在**网页地址过滤条目信息显示**区域框中，点击**关键字**为**zte.com.cn**条目后面的**编辑**按钮，系统会将当前条目信息填入**新增网页地址过滤条目**区域框的输入框中。

此时，**关键字**一栏变为灰色，修改操作只能对**过滤动作**进行修改，如图11-51所示。

图11-51 网页地址过滤业务过滤条目配置界面

b. 在**过滤动作**下拉列表框中选择**permit**，单击**应用**按钮即可完成修改操作。修改后的界面显示如图11-52所示。

图11-52 网页地址过滤业务过滤条目修改界面

6. 网页地址过滤业务过滤条目修改界面

在**网页地址过滤业务过滤条目显示**界面的**网页地址过滤条目信息显示**区域栏中，点击对应条目后的**删除**按钮，可以将当前条目删除。删除后的条目不会在**MAC-IP绑定条目信息显示**区域栏中显示。

如删除“关键字”为“zte.com.cn”的过滤条目，删除后的界面显示如图11-53所示。

图11-53 网页地址过滤业务过滤条目删除界面

NOTE **说明：**

图11-53界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务是指将该接口下的网页地址过滤业务当前所有配置都删除掉（包括恢复日志开关和缺省过滤动作状态），所以请慎重使用。

--步骤结束--

11.3.6.2 配置网站IP地址过滤业务

相关信息

在**WEB过滤业务子业务选择**界面图11-43的**WEB过滤业务**下拉列表框中选择**网站IP地址过滤业务**，进入**网站IP地址过滤业务配置**界面，如图11-54所示。

图11-54 网站IP地址过滤业务配置界面

步骤

1. 启用网站IP地址过滤业务日志

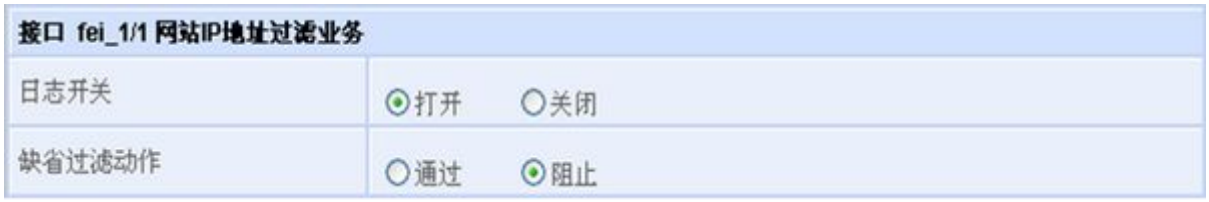
   a. 在**网站IP地址过滤业务配置**界面图11-54的**日志开关**区域栏中，选中**打开**前的单选框，弹出确认对话框，如图11-55所示。

图11-55 确认打开日志开关对话框

b. 单击**确定**按钮，打开日志开关；若单击**取消**按钮则不改变原开关状态。

单击**确定**按钮后返回界面如图11-56所示。

图11-56 网站IP地址过滤业务日志开关显示界面



c. 若要关闭日志开关，则在**日志开关**区域栏中，选中**关闭**前的单选框并且单击**确定**按钮，则日志开关恢复为关闭状态。

2. 配置网站IP地址过滤业务缺省过滤动作

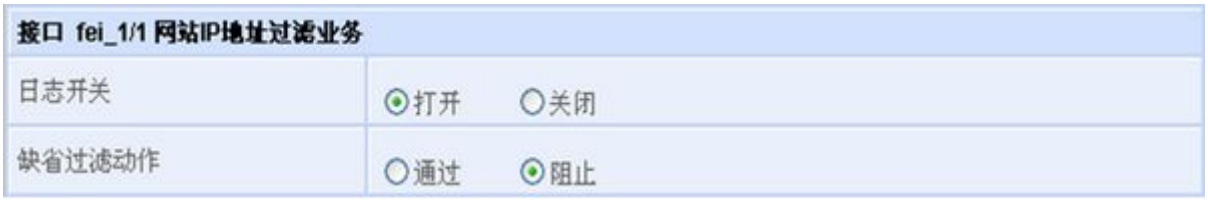
a. 在**网页地址过滤业务配置**界面图11-54的**缺省过滤动作**区域栏中，选中**阻止**前的单选框，弹出确认对话框，如图11-57所示。

图11-57 确认缺省过滤动作设置为阻止对话框

b. 若单击**确定**按钮则执行当前操作，缺省过滤动作变为阻止；若单击**取消**按钮则不改变原策略状态。

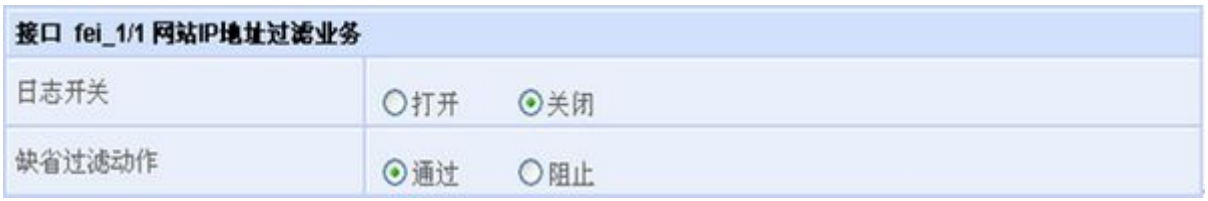
单击**确定**按钮后返回界面如图11-58所示。

图11-58 网站IP地址过滤业务缺省过滤动作显示界面1



c. 若要设置缺省过滤动作为通过，则在**缺省过滤动作**区域栏中，选中**通过**前的单选框并且单击**确定**按钮，则过滤动作恢复为通过状态，如图11-59所示。

图11-59 网站IP地址过滤业务缺省过滤动作显示界面2



3. 配置网站IP地址匹配的流过滤器

a. 进入**网站IP地址过滤业务配置**界面，如图11-54所示。

b. 在**设置网站IP地址匹配的流过滤器**区域框的**流过滤器**输入框中输入流过滤器号（流过滤器号取值范围为1~99、1000~1499）。

c. 单击**应用**按钮完成配置，配置生效后的界面如图11-60所示。

图11-60 网站IP地址过滤业务设置流过滤器配置界面

4. 修改网站IP地址匹配的流过滤器

如果需要修改匹配的流过滤器，只需要重新输入流过滤器号并单击**应用**按钮即可。

例如修改流过滤器号“99”为“1000”，操作步骤如下：

a. 在**设置网站IP地址匹配的流过滤器**区域框的**流过滤器**输入框中输入**1000**

b. 单击**应用**按钮完成修改操作，修改操作后的界面如图11-61所示。

图11-61 网站IP地址过滤业务设置流过滤器修改界面

5. 删除网站IP地址匹配的流过滤器

如果要删除匹配的流过滤器，只需要在**流过滤器**输入框内将参数置空，单击**应用**按钮即可完成删除操作，删除后的界面如图11-62所示。

图11-62 网站IP地址过滤业务设置流过滤器删除界面

NOTE **说明：**

图11-62界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务是指将将该接口下的网站IP地址过滤业务当前所有配置都删除掉（包括恢复日志开关和缺省过滤动作状态），所以请慎重使用。

--步骤结束--

11.3.6.3 配置网页参数过滤业务

相关信息

在**WEB过滤业务子业务选择**界面图11-43的**WEB过滤业务**下拉列表框中选择**网页参数过滤业务**，进入**网页参数过滤业务配置**界面，如图11-63所示。

图11-63 网页参数过滤业务配置界面1

步骤

1. 配置网页参数过滤业务

   网页参数过滤业务配置界面主要包含了日志开关和关键字选择配置，用户可以根据需要选择配置。

   例如设置日志开关为打开，关键字选择“get”和“put”的操作步骤如下：

   a. 选中**日志开关**后面的复选框。

   b. 在**关键字选择**区域栏中，选中**get**和**put**前面的复选框。 操作界面如图11-64所示。

图11-64 网页参数过滤业务配置界面2

   c. 单击**应用**按钮完成配置操作，配置生效后界面如图11-65所示。

图11-65 网页参数过滤业务配置显示界面

2. 删除网页参数过滤业务

例如要删除网页参数过滤业务配置中关键字“get”的操作步骤如下：

a. 在**关键字选择**区域栏中，不选中**get**前面的复选框。

b. 单击**应用**按钮即可删除该业务，界面如图11-66所示。

图11-66 网页参数过滤业务配置删除界面

NOTE **说明：**

图11-66界面上的[删除业务]按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

[删除业务]意思是将该接口下的网页参数过滤业务当前所有配置都删除掉，所以请慎重使用。

--步骤结束--

11.3.6.4 配置小程序阻断业务

相关信息

在**WEB过滤业务子业务选择**界面图11-43的**WEB过滤业务**下拉列表框中选择**小程序阻断业务**，进入**小程序阻断业务配置**界面，如图11-67所示。

图11-67 小程序阻断业务配置界面

步骤

1. 配置日志开关、ActiveX阻断开关和JavaApplet阻断开关

   按照下列步骤进行配置日志开关、ActiveX阻断开关和JavaApplet阻断开关操作。

   a. 在**小程序阻断业务配置**界面中，选中**日志开关**、**ActiveX阻断开关**、**JavaApplet阻断开关**后面的单选框。

   b. 单击**应用**按钮完成配置，配置生效后的界面如图11-68所示。

图11-68 小程序阻断业务配置开关显示界面

c. 若将开关置为关闭状态，只要不选中**日志开关**、**ActiveX阻断开关**、**JavaApplet阻断开关**后面的单选框即可。

2. 配置JavaApplet阻断扩展参数名

a. 进入**小程序阻断业务配置**界面中，如图11-67所示。

b. 在**新增JavaApplet阻断扩展参数名**域栏的**JavaApplet阻断扩展参数名**输入框中输入参数名（扩展参数名为1~31个非‘\’字符）。

操作界面如图11-69所示。

图11-69 小程序阻断业务配置扩展参数名显示界面

c. 单击**应用**按钮完成新增参数名配置，配置生效后条目将显示在**JavaApplet阻断扩展参数名信息显示**区域栏中，界面如图11-70所示。

图11-70 小程序阻断业务配置参数名生效显示界面

NOTE **说明：**

只有当JavaApplet阻断开关处于打开状态时，才可以进行新增JavaApplet阻断扩展参数名配置。

3. 删除JavaApplet阻断扩展参数名

在**JavaApplet阻断扩展参数名信息显示**区域栏中点击相应参数名后的**删除**按钮，可以对已经存在的条目进行删除操作。

例如删除参数名“aaa”的条目，删除后的界面显示如图11-71所示。

图11-71 小程序阻断业务配置删除显示界面

NOTE **说明：**

图11-71界面上的**删除业务**按钮只有当前接口下已经配置了该业务时才可以使用，否则处于灰色状态，禁止使用。

删除业务意思是将该接口下的小程序阻断业务当前所有配置都删除掉（包括恢复日志开关、ActiveX阻断开关和JavaApplet阻断开关），所以请慎重使用。

--步骤结束--

图目录

缩略语

DHCP – Dynamic Host Configuration Protocol，动态主机配置协议

IP – Internet Protocol，网际协议

LAN – Local Area Network，局域网

MAC – Media Access Control，介质访问控制

NAT – Network Address Translation，网络地址转换

VLAN – Virtual Local Area Network，虚拟局域网

WAN – Wide Area Network，广域网