



WEB 管理手册

RSR20-14E&F 系列路由器

RGOS 10.4(3b34)p3

文档版本号：V1.0

版权声明

锐捷网络©2016

锐捷网络版权所有，并保留对本手册及本声明的一切权利。

未得到锐捷网络的书面许可，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。



都是锐捷网络的注册商标，不得仿冒。

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(3b34)p3

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>。
- 锐捷网络远程技术支持中心：<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>
- 锐捷网络技术支持与反馈信箱：service@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 WEB管理

1.1 概述

1.1.1 简介

WEB 管理通过使用浏览器如 IE、Firefox、Chrome 等来管理网络设备，如路由器或交换机。主要用于简化设备配置，提升产品易用性。

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，并把处理结果返回给客户端，WEB 客户端通常指网页浏览器，如 IE、Firefox、Chrome 等。

1.1.2 基本概念

WEB 服务器

WEB服务器是指一种驻留在设备上的程序。当WEB浏览器（客户端）连到服务器上并请求文件时，服务器将处理该请求并将文件发送到该浏览器上，附带的信息会告诉浏览器如何查看该文件（即文件类型）。服务器使用HTTP（超文本传输协议）或HTTPS（TLS1.0，加密协议）进行信息交流。

WEB 客户端

WEB 客户端是一种能让用户与 WEB 服务器互动的一种软件，它拥有解释 WEB 服务器文件，并呈现文件内容的能力。WEB 客户端通常指网页浏览器，个人电脑上常见的网页浏览器包括微软 IE、火狐 Firefox、谷歌 Chrome 和苹果 Safari 等。

1.2 配置指南

1.2.1 配置环境

服务器要求

- 被配置设备需要启动 WEB 服务
- 被配置设备需要配置 WEB 管理登录用户认证信息
- 被配置设备需要配置管理 IP 地址

客户端要求

- WEB 网管使用 WEB 浏览器登录到设备，通过 WEB 管理界面对设备进行管理。

- 浏览器：支持微软 IE、火狐 Firefox、谷歌 Chrome 和苹果 Safari 以及部分基于 IE 内核的浏览器(如傲游 Maxton)。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：分辨率的设置需要根据 PC 显示器的大小来确定，普通的显示器建议分辨率设置为 1280*1024，而宽屏的显示器建议分辨率设置成 1440*900，此分辨率浏览 WEB 效果最佳，其它的分辨率可能会出现页面不对齐、不够美观等异常。

1.2.2 网络设置

缺省情况下,路由器的 WEB 服务功能是开启状态，设备管理接口是 GE0/0 接口，该接口的出厂 IP 为 192.168.1.1，子网掩码为 255.255.255.0，WEB 管理账户为：admin，密码为：admin。下文将以默认配置介绍网络设置的具体步骤（以 Windows XP 为例）：

WEB 缺省配置

功能特性	缺省值
WEB 服务器状态	开启
WEB 管理接口	GE0/0 或 VLAN1，管理 IP：192.168.1.1
WEB 管理账户	用户名：admin 密码：admin

步骤一：确认客户端 PC 和路由器已上电，使用网线将客户端 PC 网卡与路由器的 GE0/0 连接，若连接成功，则设备管理接口的状态指示灯会以橙色或绿色点亮，若指示灯没有点亮，则可能是网线或客户端 PC 网卡出现故障。

步骤二：设置客户端 PC 的 IP 地址，操作步骤如下：

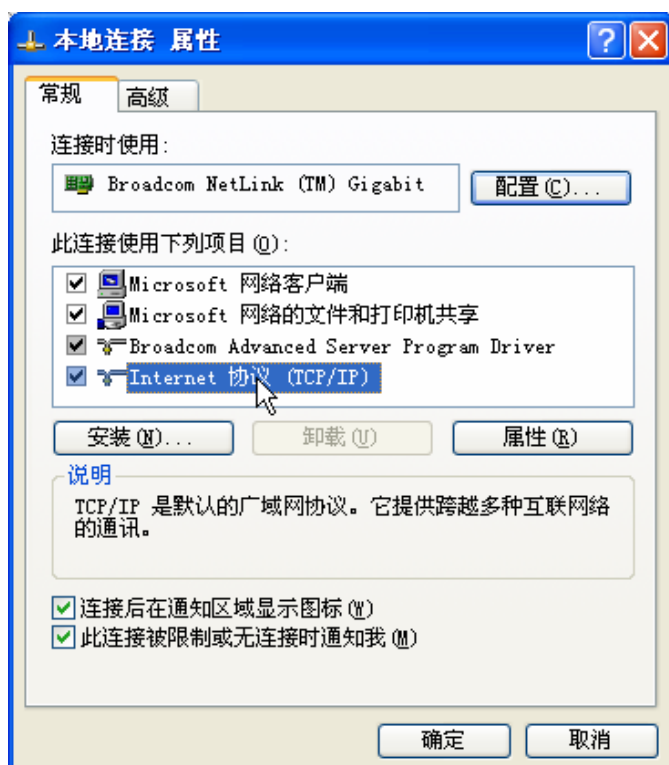
将鼠标移至 PC 的左下角点击“开始”->“控制面板”->“网络和 Internet 连接”->“网络连接”，如图：

图 1-1



鼠标右键单击“本地连接”，在弹出的上下文菜单中单击“属性”菜单，选中“Internet 协议 (TCP/IP)”，如图：

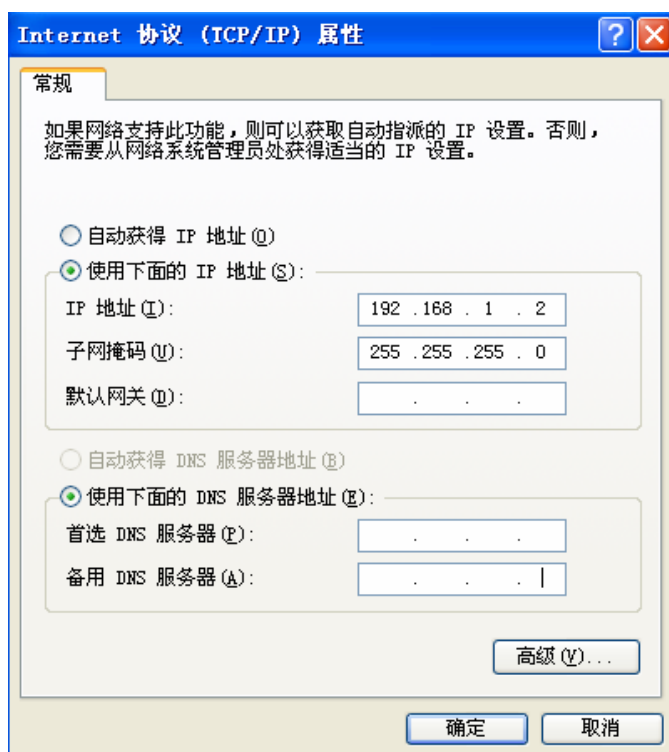
图 1-2



单击“属性”按键，设置客户端PC的IP地址。

在“Internet 协议 (TCP/IP) 属性”对话框中点选“使用下面的IP地址”。在“IP地址”中填入192.168.1.xxx (xxx的范围为2 ~ 254)，“子网掩码”中填入255.255.255.0。“默认网关”中填入192.168.1.1 (即路由器默认的IP地址) 如图：

图 1-3



⚡ 由于路由器的默认 IP 地址为 192.168.1.1，因此客户端 PC 的 IP 地址最后一位不能为 1，单击“确定”完成配置。

步骤三：测试客户端 PC 和路由器是否连通

将鼠标移至PC的左下角单击“开始”->“运行”->键入“cmd”->“确定”。

在命令提示符使用ping命令测试是否连通。执行：ping 192.168.1.1 如果显示：

图 1-4 连接成功

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 1-5 连接失败

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

✚ 若连接失败，你可以检查：

- ✚ 路由器面板上与客户端 PC 相连端口的指示灯是否亮起，指示灯未亮表示物理上的连接不正常，可以换一根网线。
- ✚ 检查上述 TCP/IP 设置是否正确。
- ✚ 检查路由器是否已经上电。

1.2.3 登录WEB网管

在设备 WEB 服务开启后，客户端就可以通过浏览器访问 WEB 网管系统。在第一次登录时，需要确认以下几点：

- 1) 路由器已正常加电启动，GE0/0 口已与客户端主机相连。
- 2) 客户端主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装 IE 7.0 以上版本浏览器或者其它兼容浏览器。
- 3) 客户端主机 IP 地址已设为与设备 GE0/0 口同一网段，即 192.168.1.xxx (xxx 为 2 至 254 之间的任意整数)，子网掩码为 255.255.255.0，默认网关为路由器管理地址 192.168.1.1。

打开IE浏览器，在地址栏输入http://192.168.1.1登录RSR路由器的WEB网管界面，如图 1-6

📖 为了获得更好的 WEB 效果，推荐使用 IE7.0 以上版本、Google Chrome、Apple Safari、Firefox3.0 等浏览器

图 1-6 登录界面



在此界面输入设备管理用户名和密码，出厂缺省值为 admin/admin。成功登录后将看到路由器 WEB 首页信息,如图 1-7

✈ 为了设备帐号安全，请在登录成功后修改出厂初始密码

图 1-7:系统首页



1.2.4 WEB界面简介

1.2.4.1 界面总览

RSR路由器WEB界面布局如下图 1-8所示

图 1-8 WEB界面区域划分



在图 1-8WEB界面区域划分中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域为配置管理区域，是设备配置管理的主要操作区域，常见的配置添加、删除、修改等操作都在这里进行。

1.3 功能设置

1.3.1 设备概览

设备概览界面主要显示当前设备基本信息，主要包括设备型号、硬件版本、软件版本、WEB 包版本、序列号、运行时间、系统时间、各槽位接口状态、内存、温度、CPU、USB、SD 卡等信息。

图 1-9



✈ 路由器设备有接入 USB 设备，或插入 SD 卡时，设备概览界面才会显示 USB、SD 图标，否则不会显示。

1.3.2 网络部署

通过网络部署，设备可以达到基本通信的目的，包括互联网的接入，局域网的部署。对互联网的接入包含多种方式，其中主要包括 ADSL 接入，DHCP 动态 IP 地址接入，固定公网 IP 地址接入，联通、移动、电信的 3G 网络接入，同步卡和 CE1 卡等网络接入方式。对局域网的部署，可以实现对局域网的主机进行动态 IP 地址分配，VLAN 隔离，以及 VLAN 间的互联互通。

1.3.2.1 广域网

固化以太网接口

通过固化以太网接口配置，可以实现基本数据转发，实现快速接入互联网。接入互联网的方式有 PPPOE(ADSL)拨号，DHCP 方式从运营商获取 IP 地址，或者以固定公网 IP 地址方式接入。具体接入方式请咨询网络服务供应商

PPPoE (ADSL) 拨号接入：PPPoE(ADSL)拨号方式接入，需要从运营商处获取帐号和密码。

DHCP 方式接入：直接选取 DHCP 方式接入即可，通过 DHCP 协议，以太网接口会自动从运营商处获取公网 IP 地址。

固定公网地址接入：固定公网地址接入，需要从运营商处获取接入的公网地址和默认网关地址

✈ PPPoE (ADSL) 拨号、DHCP、固定公网地址接入互联网需要手动指定默认路由和网络地址转换规则。

图 1-10

选择“静态 IP 地址”，即公网地址接入，直接依次输入公网 IP，网络掩码即可。选择“动态 IP 地址接入”，即 DHCP 方式接入，直接选择即可。选择“PPPoE(ADSL)”，即以 ADSL 方式接入，只要输入供应商提供的用户和密码即可。

广域网扩展接口

广域网扩展接口主要实现 SIC 系列 3G 卡实现联通、移动、电信的 3G 网络接入，以及同步卡、CE1 卡网络接入。该网页的线卡以槽位的形式显示，若槽位上无线卡设备，则该槽位显示“无插卡”，若线卡存在则显示相对应的线卡信息。当鼠标移动到图片上时，鼠标的图形会改变成手型（表示可点击），点击图标后，会出现相应的配置表单，完成不同端口的配置。

CE1 卡配置:CE1 卡分 E1 和 CE1 两种模式，默认情况下，工作模式是 E1 模式。选择 E1 模式，没有时隙和信道的划分，配置完成后，会生成一个同步子接口，网络带宽为 2M;选择 CE1 模式，时隙可以与信道进行自由的组合，因此信道的带宽大小由绑定时隙的数量有关，配置完成后，同步子接口的带宽为：时隙数量*64Kbytes。同步接口支持静态配置 IP、PPP 协商 IP 两种获取 IP 方式。

图 1-11

接口名称	IP 地址	子网掩码	接口状态	接口带宽	操作
Serial 4/0/0	0.0.0.0	0.0.0.0	未连接	2048 Kbits	编辑 删除

同步子接口创建成功以后，在接口数据表单的右侧点击“编辑”按钮，进行对同步子接口的配置。

图 1-12

同步接口配置

接口名称: Serial 4/0:0

获取IP方式: 协商 (PPP)

IP地址: * (例如: 192.168.0.1)

子网掩码: * (例如: 255.255.255.0)

链路封装协议: HDLC

保活时间间隔: 10 * (范围: 1-32767)

完成 取消

同步卡配置:同步接口默认情况下属于外网口,支持静态配置IP,PPP协商IP。其工作模式分为DTE(数据终端设备)和DCE(数据通信设备)两种模式,一般情况下,路由器扮演DTE角色,此时设备不提供时钟频率,只负责数据的发送或接收工作;而作为DCE角色时,则必须提供时钟频率,负责数据的传输工作。

图 1-13

固化以太网接口 广域网扩展接口 广域网SVI接口

槽位2 槽位3 槽位4 槽位5

无插卡 无插卡 CE1 同步串口

同步串口配置: Serial 5:0

获取IP方式: 静态IP地址

IP地址: * (例如: 192.168.0.1)

子网掩码: * (例如: 255.255.255.0)

工作模式: DTE

时钟频率: 64000

线路编码: 不归零 (NRZ)

发送时钟: 不生效

接收时钟: 不生效

链路封装协议: HDLC

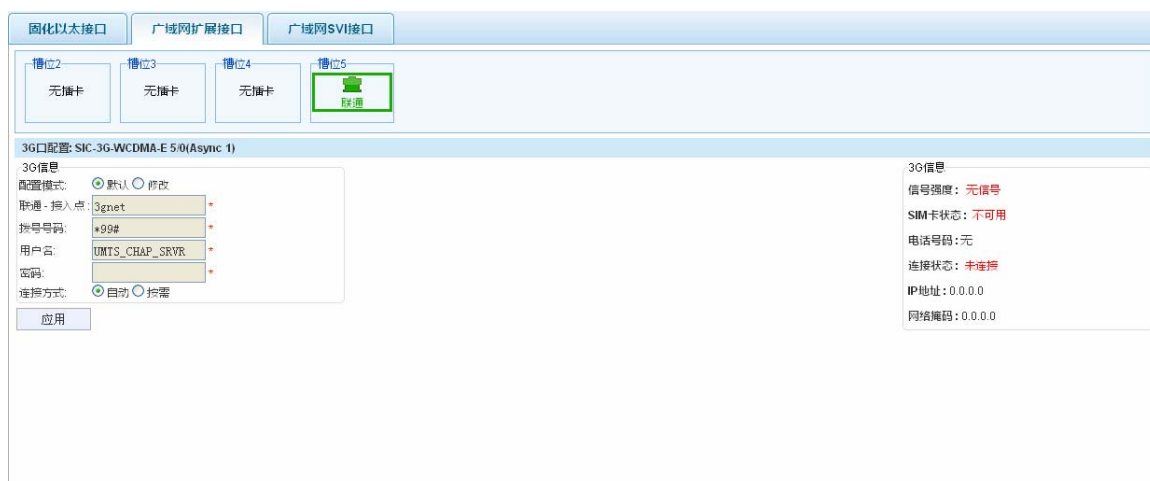
保活时间间隔: 10 * (范围: 1-32767)

应用 清除配置

PPP 协商: Point-to-Point Protocol(点到点协议),是为在同等单元之间传输数据包的链路层协议。在广域网中PPP是应用最广泛的协议之一,它的优点在于简单、具备用户验证能力、可以解决IP分配等。最常见的一种应用方式就是以太网上运行PPP来进行用户认证接入的方式称为PPPoE。

SIC-3G卡配置:3G卡默认情况下属于外网口,通过3G卡制式,自动识别所需要的参数,公共用户无需用户进行配置,直接点击“应用”即可拨号接入。如果对于专网用户可能需要修改默认参数,请使能修改即可配置。3G卡的拨号方式有,自动拨号和按需拨号,自动拨号,在保存配置后,3G卡会自动拨号连接互联网;按需拨号方式,需要有数据报文匹配按需拨号的规则时,才会触发拨号,这种方式常用于3G做备份链路的场景,可以节约3G费用。

图 1-14



SIC-3G 卡插入槽位后，就会在相应槽位显示接口。将会自动识别接入的运营商，并自动填写默认配置。路由器会自动生成一个 Async 接口与插槽上的 3G 卡对应。

3G 卡信息显示在右侧。

信号的强度：分为五个档次，信号强度依次降低，“非常好”，“好”，“一般”，“差”，“很差”。

SIM 卡状态：SIM 卡，即电话卡，如果没有插入可用的电话卡，那么 SIM 卡的状态是不可用的。

电话号码：是 SIM 卡对应电话号码。

连接状态：如果获取到了 IP 地址，那么说明连接成功。

IP 地址和网络掩码：地址和掩码是连接成功后从运营商处获取的。

移动 3G 默认参数：接入点：“CMNET”，帐号：“*99***1”，用户名：“PPPS” 密码为空；

联通 3G 默认参数：接入点：“3GNET”，帐号：“*99#”，用户名：“UMTS_CHAP_SRVR” 密码为空；

电信 3G 默认参数：接入点：为空，帐号：“#777”，用户名：“card” 密码：“card”；

广域网 SVI 接口

SVI 接口即交换虚拟接口（Switch Virtual Interface，简称 SVI）是一个虚拟三层接口，可以实现路由和桥接的功能。因此 SVI 接口也可以部署在广域网作为一种连接 Internet 公网接口。在获取 IP 地址的方式上与固化以太网接口一样，支持静态 IP 地址、DHCP（获取动态 IP 地址）、PPPoE 拨号。要创建 SVI 接口，必须先有相应 VLAN ID，可以通过“固化交换接口”配置相应 VLAN ID。

PPPoE（ADSL）拨号接入：PPPoE(ADSL)拨号方式接入，需要从运营商处获取帐号和密码。

DHCP 方式接入：直接选取 DHCP 方式接入即可，通过 DHCP 协议，SVI 接口会自动从运营商处获取公网 IP 地址。

固定公网地址接入：固定公网地址接入，需要从运营商处获取接入的公网地址和默认网关地址

PPPoE（ADSL）拨号、DHCP、固定公网地址接入互联网需要手动指定默认路由和网络地址转换规则。

图 1-15

固化以太网接口

广域网扩展接口

广域网SVI接口

SVI

V1

可选项

选中项

不可选项

设备接口配置-VLAN 1

获取IP方式: 静态IP地址

IP地址: 192.168.45.210 (网段: 192.168.0.45)

子网掩码: 255.255.255.0 (网段: 255.255.255.0)

接口描述: (范围: 1-32个字符)

应用 清除配置

选择“静态 IP 地址”，即公网地址接入，直接依次输入公网 IP，网络掩码即可。选择“动态 IP 地址接入”，即 DHCP 方式接入，直接选择即可。选择“PPPoE(ADSL)”，即以 ADSL 方式接入，只要输入供应商提供的用户和密码即可。

- 若 SVI 接口指定为广域网接口，则局域网 SVI 接口会自动隐藏该接口。
- 若 SVI 接口对应的 VLAN 没有与交换口绑定，则在清除配置时，VLAN 将会被删除，该网页中 SVI 图片将不存在。
- 广域网 SVI 接口根据 VLAN ID 的顺序排列，但最多只能显示 18 个 SVI 接口图标，剩余部分不会显示。

1.3.2.2 局域网

固化交换接口

根据内部局域网部署需要，可自定义交换接口模式和接口 VLAN ID，接上联设备的接口通常为 Trunk 模式，接 PC 客户端的接口通常为 Access 模式。

TRUNK 模式：允许多个 VLAN 通信，默认情况下，是允许所有 VLAN 通过此交换口，将数据转发到上联设备。指定该模式时，不会创建 VLAN，只设置交换口的允许通信的 VLAN 列表。

ACCESS 模式：只能输入一个允许通信的 VLAN，进出此接口的报文，VLAN 标识将会被剥离，通常用于连接客户端 PC。指定该模式时，同时会创建指定的允许 VLAN，该 VLAN 可以用于创建广域网或局域网的 SVI 接口。

图 1-16

固化交换接口

局域网SVI接口

Trunk交换口:

14187

131517

可选项

选中项

不可选项

接口名称	接口模式	接口状态	许可VLAN列表	操作
FastEthernet 1/1	TRUNK	未连接	ALL	编辑 默认配置
FastEthernet 1/2	TRUNK	未连接	ALL	编辑 默认配置
FastEthernet 1/3	ACCESS	未连接	1	编辑 默认配置
FastEthernet 1/4	ACCESS	未连接	1	编辑 默认配置
FastEthernet 1/5	ACCESS	未连接	1	编辑 默认配置
FastEthernet 1/6	ACCESS	已连接	1	编辑 默认配置
FastEthernet 1/7	ACCESS	已连接	1	编辑 默认配置
FastEthernet 1/8	ACCESS	未连接	1	编辑 默认配置
GigabitEthernet 1/0	TRUNK	未连接	ALL	编辑 默认配置

批量配置

首页 上一页 1 下一页 尾页 1 / 1 页

在配置 Trunk 交换口时，只需点击面板中的交换口图标，由白底色变成深蓝色即可，若要恢复 Access 模式，再点击一次恢复成白底色即可，为了方便操作，同时还提供了“批量配置”、“编辑”、“恢复配置”等功能。

批量配置：是指对一组相同模式的交换口设置允许 VLAN。点击“批量配置”按钮，选择需要设置的交换口、接口模式和输入允许 VLAN 即可，因此批量配置不会改变交换口原有的接口模式，若要修改只能通过固化交换接口主页去修改模式。

图 1-17 Access 模式

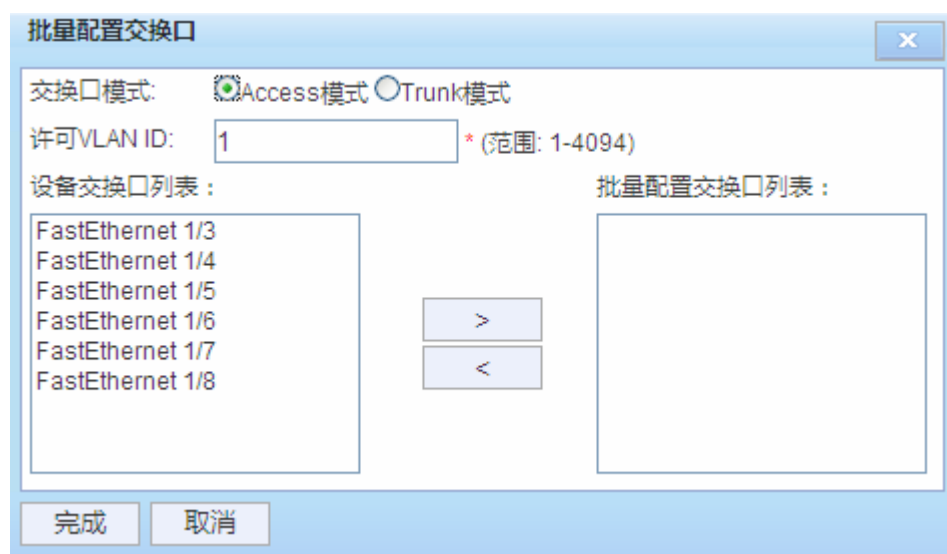
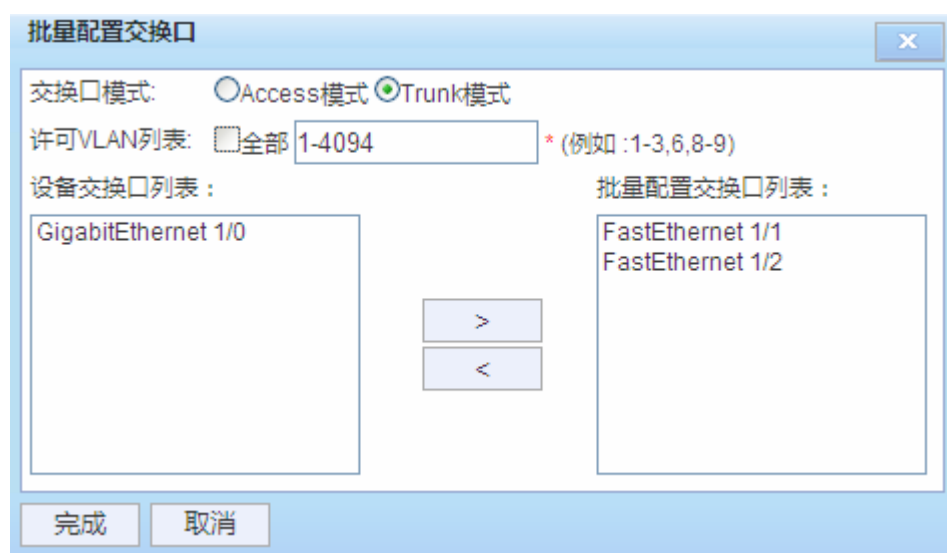


图 1-18 Trunk 模式

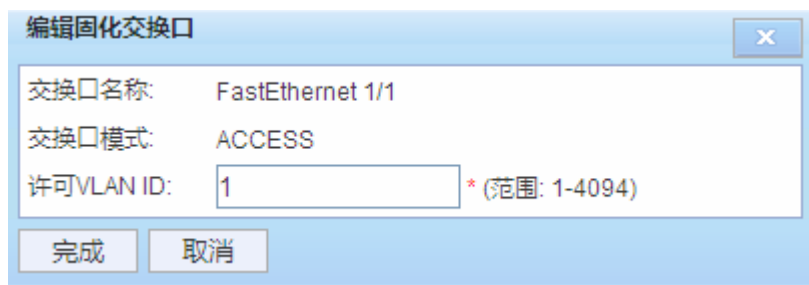


✚ 选择 Access 模式时，设备交换口列表只呈现 Access 模式的交换口，而 Trunk 模式的交换口不会呈现。

✚ 选择 Trunk 模式时，设备交换口列表只呈现 Trunk 模式的交换口，而 Access 模式的交换口不会呈现。

编辑：是指针对一个交换口设置允许 VLAN。点击“编辑”按钮，输入允许 VLAN 即可，若该交换口已设置过 VLAN，则会直接覆盖以前的 VLAN。

图 1-19

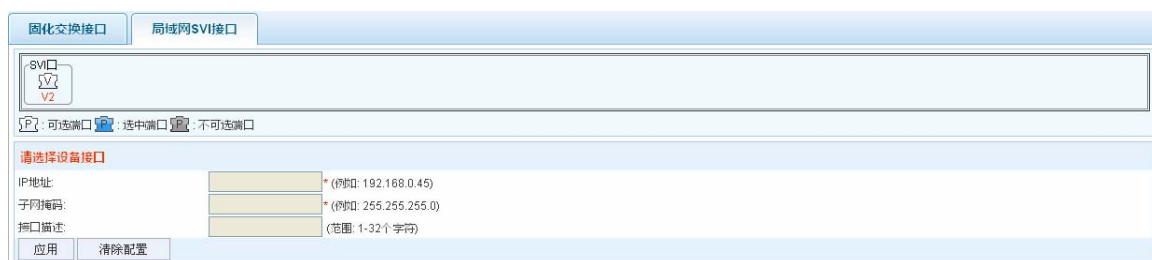


默认配置：是指恢复交换口的默认配置，在恢复配置的过程中，若 VLAN 没有被用于创建 SVI 接口，则会在此过程中被删除，因此会影响广域网 SVI 接口和局域网 SVI 接口面板接口呈现。

局域网 SVI 接口

通过 VLAN 管理实现不同 VLAN 间的通信。所有在同一个 IP 子网中的主机属于同一个 VLAN，VLAN 之间的通讯必须通过三层接口。为了实现不同 VLAN 之间的通信，可以创建 SVI 接口（Switch Virtual Interfaces，及交换虚拟接口）来进行 VLAN 之间的 IP 路由。达到不同 VLAN 间通信的目的。

图 1-20



局域网 SVI 接口只需要指定接口的 IP 地址和子网掩码即可。

- ⚡ 若 SVI 接口指定为局域网接口，则广域网 SVI 接口会自动隐藏该接口。
- ⚡ 若 SVI 接口对应的 VLAN 没有与交换口绑定，则在清除配置时，VLAN 将会被删除，该网页中 SVI 图片将不存在。
- ⚡ 局域网 SVI 接口根据 VLAN ID 的顺序排列，但最多只能显示 18 个 SVI 接口图标，剩余部分不会显示。

1.3.2.3 NAT配置

网络地址转换

通过网络地址转换（NAT），实现内网私有地址转换成合法的公网地址，实现互联网接入。NAT 英文全称是“Network Address Translation”，即“网络地址转换”，它允许一个整体机构以一个公用 IP 地址出现在 Internet 上。顾名思义，它是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。

图 1-21

网络地址转换

网络地址端口映射

网络地址转换: 即 NAT (Network Address Translation) , 是将IP 数据包头中的IP 地址转换为另一个IP 地址的过程。在实际应用中, 需要将内网IP地址转换成可以访问互联网的外网IP地址。

网络地址转换配置表单

外网接口:

☒Serial5/0☐Gi0/0☐Gi0/1☐Virt-P1☒VLAN1

内网接口:

☐Serial5/0☒Gi0/0☐Gi0/1☐Virt-P1☐VLAN1

应用

序号	外网接口	内网接口	报文转换统计	转换限制	操作
1	Serial5/0	Gi0/0	使用 0 次	详细清单	删除

网络地址转换只需要确定外网接口和内网接口, 就可以实现内网地址转换公网地址。转换后的地址也可以选择多个接口组建成公网地址池, 数据报文会在匹配的接口上进行转换, 达到在不同运营商接入情况下数据报文负载均衡的目的。


 转换后的地址通常选择为外网接口地址。因为在 PPPoE 拨号接入情况下, IP 由运营商动态分配。

图 1-22

限制转换清单

限制转换: 在默认情况下, 网络地址转换是允许所有内网IP地址转换成外网IP地址, 当需要限制某些内网地址进行地址转换时, 因此可以在本表单中指定限制转换的内网IP地址。

限制转换清单

内网地址:

*(限制转换的内网IP地址)

子网掩码:


*(限制转换的内网子网掩码)

应用

序号	内网地址	子网掩码	操作
无数据			

首页 上一页 下一页 尾页 0/0 页

完成 取消

 默认情况下, 允许所有的内网地址转换, 若需要限制某些内网地址转换时, 可以在此指定限制转换的内网地址。

网络地址端口映射

在路由器默认设置下, 广域网中的主机不能直接与局域网中的服务器进行通信。为了方便广域网的合法用户访问本地服务器, 同时又要保护局域网内部不受侵袭, 路由器提供了网络地址端口映射功能。首先, 它定义一条公网地址及端口映射到局域网中本地服务器的地址及端口规则, 然后设定的公网地址及端口收到数据后, 通过映射规则转发给局域网中的服务器, 这样就实现了局域网服务器对外提供服务的能力, 同时不影响局域网内部的网络安全。

图 1-23 端口映射

网络地址转换

网络地址端口映射

功能说明: 在路由器默认设置下, 广域网中的主机不能直接与局域网主机进行通信。为了方便广域网的合法用户访问本地主机, 又要保护局域网内部不受侵害, 路由器提供了网络地址端口映射功能。

网络地址端口映射表

映射类型:

端口映射

内网IP:

内网端口:

外网IP:

手工输入

外网接口:

请选择

外网端口:

协议类型:

TCP

应用

映射类型	内网IP	内网端口	外网IP	外网端口	协议类型	外网接口	操作
端口映射	192.168.46.23	8080	N/A	8083	tcp	GigabitEthernet 0/1	编辑 删除

新建

首页 上一页 1 下一页 尾页 1 / 1 页

映射类型：端口映射或整机映射。

服务协议：请根据需要选择 TCP 或 UDP。

外网 IP：广域网的 IP 地址。如果选择接口，则外网接口上所有的 IP 都会映射。

外网端口：广域网上的端口，取值范围为 1 至 65535。

内网 IP：要映射到外网的内网 IP，通常是您的服务器 IP 地址。

内网端口：要映射到外网的端口，取值范围为 1 至 65535。

图 1-24 整机映射

网络地址转换

网络地址端口映射

功能说明: 在路由器默认设置下, 广域网中的主机不能直接与局域网主机进行通信。为了方便广域网的合法用户访问本地主机, 又要保护局域网内部不受侵害, 路由器提供了网络地址端口映射功能。

网络地址端口映射表

映射类型:

整机映射

内网IP:

外网IP:

手工输入

外网接口:

请选择

应用

映射类型	内网IP	内网端口	外网IP	外网端口	协议类型	外网接口	操作
端口映射	192.168.46.23	8080	N/A	8083	tcp	GigabitEthernet 0/1	编辑 删除

新建

首页 上一页 1 下一页 尾页 1 / 1 页

外网 IP：广域网的 IP 地址。如果选择接口，则外网接口上所有的 IP 都会映射。

内网 IP：要映射到外网的内网 IP，通常是您的服务器 IP 地址。

1.3.2.4 DHCP 服务

动态主机设置协议 (Dynamic Host Configuration Protocol, DHCP) 是一个局域网的网络协议。DHCP 服务为局域网内主机提供动态 IP 地址分配功能。页面配置主要功能包括：DHCP 使能、动态分配 IP 地址、静态绑定 IP 地址、保留 IP 地址、客户端列表。

DHCP 使能

DHCP 使能，实现 DHCP 服务开启或关闭。

图 1-25

DHCP使能

动态分配IP地址

静态绑定IP地址

保留IP地址

客户端列表

关闭/开启DHCP服务

DHCP服务：

关闭

开启

应用

动态分配 IP 地址

动态分配 IP 地址，包括要分配的地址网段、客户端获取的网关和 DNS 地址等。要分配的地址网段和 LAN 侧的接口保持同一网段，否则可能地址分配不成功。

图 1-26

DHCP使能

动态分配IP地址

静态绑定IP地址

保留IP地址

客户端列表

动态分配IP地址配置表单

地址池名称:

*(由字母、数字或下划线组成)

客户端IP地址段:

-子网掩码:

网关地址:

首选DNS:

-备用DNS:

应用

地址池名称	客户端IP地址段	子网掩码	网关地址	首选DNS	备用DNS	操作
无数据						

首页 上一页 下一页 尾页 0/0 页

客户端地址段：分配给客户端使用的 IP 地址段，客户端会动态获取该范围的 IP 地址。

子网掩码：客户端地址子网所对应的掩码。

网关：输入网关地址，这里指设备的网关地址。

首选 DNS：为客户端分配的 DNS 服务器地址。

备用 DNS：为客户端分配的 DNS 服务器地址。

点击“应用”按钮完成 DHCP 服务器设置。

静态绑定 IP 地址

静态绑定 IP 地址，用于指定 MAC 地址的主机分配 IP 地址信息。

图 1-27

DHCP使能

动态分配IP地址

静态绑定IP地址

保留IP地址

客户端列表

静态绑定IP地址配置表单

客户端名称:

*(由字母、数字或下划线组成)

客户端IP地址:

-子网掩码:

客户端MAC地址:

*(例如: 0000.0000.0000)

网关地址:

-首选DNS:

应用

客户端名称	客户端IP地址	子网掩码	客户端MAC地址	网关	首选DNS	操作
无数据						

首页 上一页 下一页 尾页 0/0 页

客户端名称：为该客户端指定名称。

客户端 IP 地址：分配给客户端电脑的 IP。

子网掩码：分配给客户端 IP 对应的掩码。

客户端 MAC 地址：客户端电脑的 MAC 地址。

网关地址：输入网关地址，这里指客户端的网关地址。(非必填)

首先 DNS：客户端 DNS 服务器地址。(非必填)

✚ 如果增加重复的客户名称，原有的绑定记录将被新的记录取代。不同的 MAC 地址不能同时绑定到同一个 IP 地址。

保留 IP 地址

保留 IP 地址，用于对某个网段的 IP 地址或某个特定 IP 地址限制分配，保留的 IP 地址可能被用于网络部署中其它设备的 IP 地址设置。

图 1-28

DHCP使能	动态分配IP地址	静态绑定IP地址	保留IP地址	客户端列表
保留IP地址配置表单				
起始IP地址	192.168.1.2 *			
结束IP地址	192.168.45.20 *			
<input type="button" value="应用"/>				
起始IP地址	结束IP地址	操作		
192.168.1.2	192.168.45.20	编辑 删除		
首页 上一页 1 下一页 尾页 1 / 1 页				

起始 IP 地址：被保留的起始 IP 地址

结束 IP 地址：被保留的结束 IP 地址

📖 起始 IP 地址与结束 IP 地址相同时，是对特定的 IP 地址限制分配。

客户端列表

通过该功能可以查看当前已经分配的 IP 地址情况。

图 1-29

DHCP使能	动态分配IP地址	静态绑定IP地址	保留IP地址	客户端列表
地址分配列表				
已分配IP地址	MAC地址	地址租期		
192.168.45.210	0025.64c5.84d2	IDLE		
首页 上一页 1 下一页 尾页 1 / 1 页				

1.3.3 路由配置

1.3.3.1 静态路由

路由是选择一条最佳路径把数据从源地点传送到目的地点的行为。静态路由则是由网络管理员手动配置的一种特殊路由，具有简单、高效、可靠等优点。

静态路由不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

图 1-30

静态路由						
<p>路由优先级: 策略路由和普通IP路由都可以作为报文转发的依据。优先级是：策略路由 > 静态路由 > 默认路由。</p> <p>普通IP路由: 让到达目的网络的数据包，按照指定的路径传输。当设备不能学到一些目标网络的路由时，配置静态路由就会显得十分重要。给所有没有确切路由的数据包配置一个默认路由，是通常的做法。普通IP路由包括：静态路由和默认路由，其中默认路由的优先级是最低的。</p>						
静态路由信息						
筛选条件:	全部					
目的地址	下一跳地址	出接口	路由类型	管理距离	状态	操作
0.0.0.0/0	192.168.45.1		默认路由	1	激活	编辑 删除
新建路由						
首页 上一页 1 下一页 尾页 1 / 1 页						

➤ 静态路由规则


目的地址： 设定数据包需要到达的目的 IP 地址。

目的掩码： 设定目的 IP 地址的子网掩码。

下一跳地址： 指定一个 IP 地址，路由器下一步会将符合条件的数据包转发到该地址上。

出接口： 设定数据包发送出去的接口。

管理距离： 设定路由的优先级，路由的管理距离值越小则优先级越高，默认情况下管理距离值为“1”。

 目的地址与目的掩码同为 0.0.0.0 的路由为默认路由

 下一跳地址和出接口必须有一项被配置，或者两项都配置

图 1-31

新建路由

说明: 管理距离-N : N值越小越优先进行选路

路由类型:

☒默认路由☐静态路由

目的地址:

* (例如: 202.210.19.0)

目的掩码:

* (例如: 255.255.255.0)

出接口:

下一跳地址:

* (例如: 192.168.1.1)

管理距离:

(范围: 1-255)

完成

取消

1.3.3.2 策略路由

策略路由 (PBR : Policy-Based Routing) 提供了一种比基于目的地址进行路由转发更加灵活的数据包路由转发机制。策略路由可以根据 IP 报文源地址等信息灵活地进行路由选择。当网络接入多个运营商网络时，需要有选择性的进行报文转发，不同用户接入不同网络，这时策略路由是很好的选择。

图 1-32

策略路由

路由优先级: 策略路由和普通IP路由都可以作为报文转发的依据。优先级是：策略路由 > 静态路由 > 默认路由。

说明: 策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。

策略路由信息

策略应用接口	匹配策略	出口地址	下一跳地址	策略优先级	操作
Async 1	源地址: any, 目的地址: any	GigabitEthernet 0/0		1	编辑 删除

新建策略路由

首页 上一页 1 下一页 尾页 1 / 1 页

➤ 策略路由规则

策略应用接口：报文匹配策略有效的入接口。

策略优先级：策略组的策略路由规则优先级，数值越小优先级越高。

匹配报文：所匹配的数据报文源地址和目的地址。指定 IP 时，需要输入网络地址和子网掩码。

出接口：设定数据包发送出去的接口。

下一跳地址：指定一个 IP 地址，路由器下一步会将符合条件的数据包转发到该地址上。

 当普通 IP 路由和策略路由同时存在的情况下,优先使用策略路由转发。

图 1-33

19

新建策略路由

策略应用接口:Serial 4/0:1

策略优先级:*(0-65535, 数字越小优先级越高)

出接口:请选择

下一跳地址:*(例如: 192.168.50.1)

匹配策略

☐任意源IP

源地址:*(例如: 192.168.1.0)

子网掩码:*(例如: 255.255.255.0)

☐任意目的IP

目的地址:*(例如: 192.168.1.0)

子网掩码:*(例如: 255.255.255.0)

完成

取消

1.3.3.3 RIP路由

RIP(Routing information Protocol)是应用较早、使用较普遍的内部网关协议(Interior Gateway Protocol,简称IGP),是典型的距离向量(distance-vector)协议。RIP通过UDP报文来交换路由信息,报文每到一个路由器,将记录到达路由器的个数,该计数用来度量路由距离,由于从源到目的网间所要经过的路由器的数目最多为 15,因此它适用于小型同类网络。经常应用在政府机关单位这样的小型单位。

WEB 主要实现了 RIPv2,由于 RIP 协议通过关联网地址,使得在该网络地址范围内的接口参与 RIP 运行,因此 WEB 的配置方式是以接口关联网地址,实现 RIP 关联网地址配置,需要注意的是必须先设置接口的 IP 地址,再关联接口地址,否则接口无法运行 RIP 协议。

 先配置接口 IP 地址,再配置 RIP。

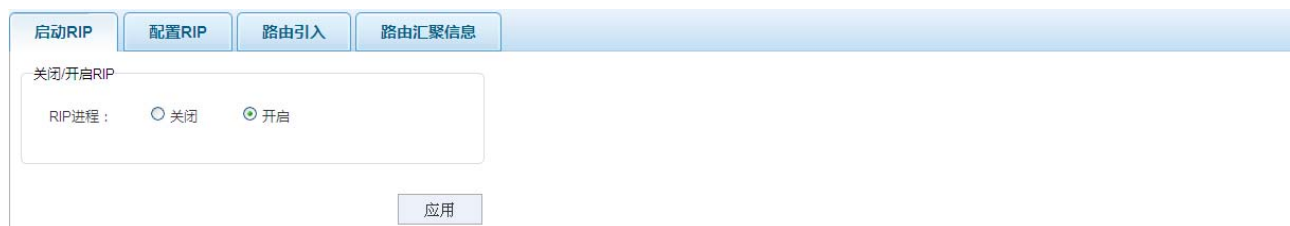
启动 RIP

启动:创建 RIP 进程

关闭:删除 RIP 进程,并删除进程相关的所有配置。

 关闭进程会删除进程相关的所有配置。

图 1-34



The interface shows the '启动RIP' (Start RIP) tab. It contains a section for '关闭/开启RIP' (Close/Start RIP) with a label 'RIP进程:' and two radio buttons: '关闭' (Close) and '开启' (Start). The '开启' button is selected. Below this is an '应用' (Apply) button.

配置 RIP

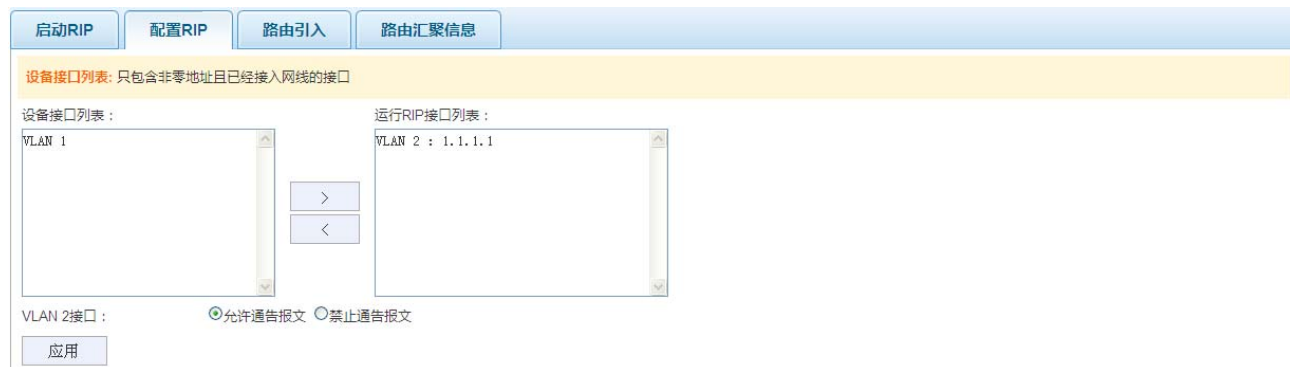
设备接口列表：包括固化以太网路由接口、同步接口（含子接口）、异步接口、VLAN 接口

运行 RIP 接口列表：通过接口获取接口地址，实现 RIP 网络地址关联

允许通告报文：允许接口向外通告本地路由。

禁止通告报文：禁止接口向外通告路由，该接口可以学习外部路由，但不能通告本地路由。

图 1-35



The interface shows the '配置RIP' (Configure RIP) tab. It features a yellow header bar with the text '设备接口列表: 只包含非零地址且已经接入网线的接口'. Below this are two list boxes: '设备接口列表:' containing 'VLAN 1' and '运行RIP接口列表:' containing 'VLAN 2 : 1.1.1.1'. Between the lists are '>' and '<' buttons. At the bottom, there is a label 'VLAN 2接口:' followed by two radio buttons: '允许通告报文' (Allow advertisement) and '禁止通告报文' (Prohibit advertisement). The '允许通告报文' button is selected. An '应用' (Apply) button is at the bottom left.

路由引入

路由引入是对内部网络的衍生，最常见的网络部署场景：运行 RIP 的小型网络与邻近的运行 OSPF 网络相连接，若小型网络需要与 OSPF 域内的网络通信，则必须在运行 RIP 的路由器上要引入 OSPF 域的路由。

引入路由类型：包含 ospf、connected、static。

指定引入路由的类型：确定需要引入路由的类型。

图 1-36

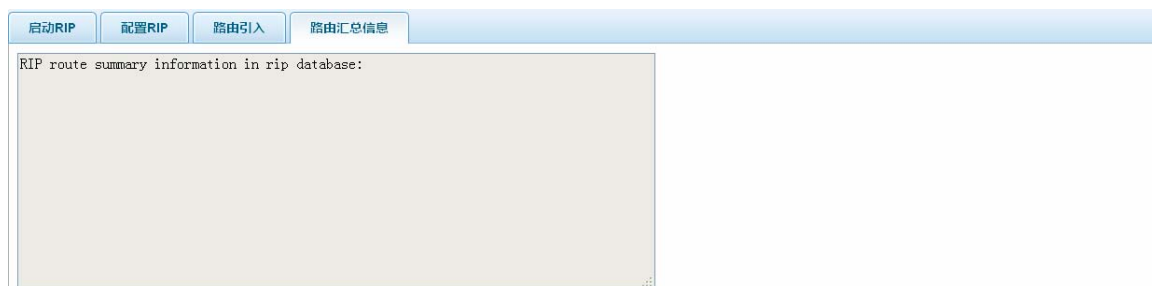


The interface shows the '路由引入' (Route Introduction) tab. It has a yellow header bar with the text '路由引入: 在一个路由协议中通告其它途径学习到的路由，其途径包括直连网络、静态路由或其它路由协议。'. Below this are two list boxes: '引入路由的类型:' containing 'ospf' and 'connected', and '指定引入路由的类型:' containing 'static'. Between the lists are '>' and '<' buttons. An '应用' (Apply) button is at the bottom left.

路由汇总信息

路由汇总功能默认是处于开启状态，如果有汇聚路由存在，在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模，该网页主要呈现路由汇聚之后的路由信息。

图 1-37



1.3.3.4 OSPF路由

OSPF (Open Shortest Path First , 开放式最短路径优先) 是一种内部网关协议(Interior Gateway Protocol,IGP),用于在同一个自治域 (Autonomous System) 中的路由器之间发布路由信息。它是一种连接状态协议,在链路状态广播数据时会同时将路由广播到某一自治域内的所有路由器设备，这有别于距离矢量协议(RIP)。OSPF 具有支持大型网络、路由收敛快、占用网络资源少等优点。经常应用在大型的企业网络环境。

由于 OSPF 协议通过网络地址划分区域，使得在该网络地址范围内的接口参与 OSPF 运行，因此 WEB 的配置方式是以接口关联网络地址，实现 OSPF 区域划分配置，需要注意的是必须先设置接口的 IP 地址，再关联接口地址，否则接口无法运行 OSPF 协议。

⚡ 划分区域时，区域 ID 与邻近的区域 ID 一致，且区域内的网络地址段必须在同一网段，否则 OSPF 运行无效。

启动 OSPF

启动：创建 ospf 进程，默认进程 ID 为 “1”。

关闭：删除进程，并删除进程相关的所有配置。

图 1-38



OSPF 区域划分

设备接口列表：包括固化以太路由接口、同步接口（含子接口）、异步接口、VLAN 接口

区域接口列表：通过接口获取接口地址，实现 OSPF 网络地址关联

指定区域编号：指定网络地址的区域。

图 1-39



OSPF 邻居管理

一般情况下，OSPF 运行的环境是在广播的网络环境中，因此 OSPF 部署完成之后，就可以实现区域之间的路由学习，但对于一个非广播的网络，OSPF 是无法实现路由学习，因此网络与网络之间也就无法通信。为了实现 OSPF 互联到非广播网络，OSPF 提供了邻居管理功能，通过手工增加邻居，实现广播与非广播网络之间的通信。

图 1-40



OSPF 路由引入

路由引入是对 OSPF 域内网络的衍生，最常见的网络部署场景：运行 OSPF 网络与邻近的运行 RIP 的小型网络连接，若 OSPF 域内的网络需要与运行 RIP 的小型网络通信，则必须在 OSPF 域引入运行 RIP 小型网络的路由。

引入路由类型：包含 rip、connected、static。

指定引入路由的类型：确定需要引入路由的类型。

图 1-41



OSPF 路由信息

路由汇聚功能默认是处于开启状态，如果有汇聚路由存在，在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小小路由表的规模，该网页主要呈现路由汇聚之后的路由信息。

图 1-42

OSPF进程配置

OSPF区域划分

OSPF邻居管理

OSPF路由引入

OSPF路由信息

OSPF route information:
OSPF link state database information:

1.3.4 虚拟专网

1.3.4.1 VPN配置

VPN 的英文全称是“Virtual Private Network”即“虚拟专用网络”。它并不是真实存在的物理链路，而是通过技术手段模拟出来的虚拟线路。互联网上的两个节点通过 VPN，可以建立一条虚拟的专用数据传输通道，在这个专用通道中相互传递资料不会被外界干扰或窃听。

VPDN 客户端

VPDN 客户端是指主动与远程 VPDN 服务器发起协商并建立隧道的路由器。目前 VPDN 客户端只支持 L2TP 隧道协议。

图 1-43

VPDN客户端

功能说明: VPDN客户端是指主动与远程VPDN服务器发起协商并建立隧道的路由器。目前VPDN客户端只支持L2TP隧道协议。
注意事项: 在配置VPDN客户端之前，先确认是否存在到VPDN服务器的路由。若不存在这样的路由，请在“路由配置”->“静态路由”创建路由。

VPDN客户端配置表单

服务器地址:

*(远程VPDN服务器的隧道地址)

隧道密码:

☐启用隧道认证

用户名:

*(由字母、数字或下划线组成)

密码:

*(由字母、数字或下划线组成)

备注:

应用

序号	本地隧道ID	服务器隧道ID	服务器地址	隧道当前状态	备注	操作
1	1	0	12.3.3.3	未连接		编辑 删除

服务器地址：远程 VPDN 服务器地址

隧道密码：隧道认证密码

用户名：用于认证的客户端帐号，由 VPDN 服务器提供。

密码：用于认证的客户端密码，由 VPDN 服务器提供。

备注：描述 VPN 连接说明性文字。

IPSec VPN

虽然 VPN 隧道能跨越 Internet 连接并访问公司网络，但是报文信息却裸露在复杂 Internet 的网络环境中，数据安全成为一个至关重要的问题，为防止数据信息泄露，达到数据秘密传送的目的，因此必须对数据报文进行加密。IPSec 协议作用在网

络层，它规定了一套安全体系架构，在IPSec实体之间实现数据保密性、完整性和数据验证服务。它可以为主机之间、子网之间、安全网关之间的一条和多条数据流提供保护。

图 1-44

组网模式：站点到站点（如分公司连接总公司），客户端到站点（出差人员连接到公司）。

预共享密钥：建立安全联盟时，自动协商交换的密钥，主要用于IPSec通信的认证。

对端地址：远程运行IPSec的路由器IP地址。

IKE策略：安全协议，封装安全载荷协议（DES、3DES、AES、SM1），报文认证头协议（SHA、MD5）。

变换集合：数据加密方式，主要包括ESP-DES、ESP-3DES、ESP-3DES ESP-SHA-HMAC、ESP-3DES ESP-MD5-HMAC、ESP-DES ESP-SHA-HMAC、ESP-DES ESP-MD5-HMAC等等。

加密接口：部署VPN隧道报文加密的接口，只要隧道报文通过该接口就能实现报文加密。

加密匹配规则：不是所有的报文都需要加密，因此加密匹配规则起到加密过滤的作用。

备注：IPSec VPN本地配置的说明性文字。

1.3.5 动态防火墙

1.3.5.1 攻击防御

攻击防御就是对需要进入控制层面处理的数据报文进行分类、过滤、限速，实现对数据报文的控制，防止攻击行为，从而达到保护控制层面关键资源的目的。

ARP攻击，是针对以太网地址解析协议（ARP）的一种攻击技术。此种攻击可让攻击者取得局域网上的数据封包甚至可篡改封包，且可让网络上特定计算机或所有计算机无法正常连接。

防ARP流量攻击：通过启用“防ARP流量攻击”可以对到达本地的ARP流量配置限速，设备每秒处理的ARP报文不超过10个，多余ARP报文将被过滤掉。

防DoS攻击：开启内外网常见的DoS攻击，很多的DoS/DDoS攻击都是采用假冒的源IP地址，通过开启此功能，限制其范围和降低攻击的机会

防本地流量攻击：防御SYN Flood等流量攻击。

端口过滤：过滤非法传输层报文。

WEB 访问端口：WEB 服务默认端口是 80，WEB 服务端口可以根据设备 WEB 网管安全需要，修改端口。

图 1-45



攻击防御

防ARP流量攻击: ☐ 开启防ARP流量攻击 (设备每秒处理的ARP报文不超过10个, 多余ARP报文将被过滤掉)

防DOS攻击: ☐ 开启防内外网DOS攻击

防本地流量攻击: ☐ 开启防本地管理流量和协议流量攻击

端口过滤: ☐ 开启过滤非法传输层报文

WEB访问端口: (默认: 80, 1025-65535)

1.3.5.2 防主机欺骗

防主机欺骗即是防 ARP 欺骗，通过 IP-MAC 的绑定关系，确认 IP 主机和 MAC 地址是可信赖的关系。IP-MAC 地址的绑定可以是手工静态绑定的，也可以是通过当前 ARP 表自动绑定的可信赖关系。通过这种 IP-MAC 地址绑定关系，不合法的报文将被丢弃，在静态 IP-MAC 绑定页面将有丢弃报文的统计信息。

图 1-46



静态IP-MAC绑定 **动态IP-MAC绑定**

静态IP-MAC表

序号	IP地址	MAC地址	类型	操作
1	1.1.1.1	00f0.a210.bf01	静态	

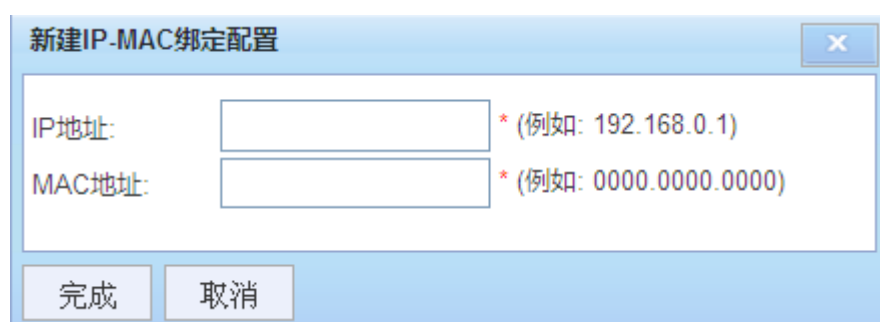
首页 上一页 **1** 下一页 尾页 1 / 1页

IP-MAC绑定丢包统计: 3 (packets)

IP 地址：与 MAC 地址被绑定的 IP 地址

MAC 地址：与 IP 地址被绑定的 MAC 地址

图 1-47



新建IP-MAC绑定配置

IP地址: * (例如: 192.168.0.1)

MAC地址: * (例如: 0000.0000.0000)

开启动态 IP-MAC 绑定会从当前 ARP 表项中绑定这种关系，如果关闭动态 IP-MAC 绑定，那么通过动态方式绑定的表项将会被清除。

通过“转静态 IP-MAC 绑定”可以将动态 IP-MAC 绑定方式转换为静态方式。

图 1-48

静态IP-MAC绑定

动态IP-MAC绑定

关闭/开启动态IP-MAC绑定

☐关闭动态IP-MAC绑定

☒开启动态IP-MAC绑定

应用

动态IP-MAC表

序号	IP地址	MAC地址	类型	操作
1	192.168.45.117	001a.a938.9602	动态	转静态IP-MAC绑定
2	192.168.45.39	0025.648f.e778	动态	转静态IP-MAC绑定
3	192.168.45.113	14fe.b5ed.425c	动态	转静态IP-MAC绑定
4	192.168.45.69	14fe.b5e1.0541	动态	转静态IP-MAC绑定
5	192.168.45.212	0023.ae67.d8b4	动态	转静态IP-MAC绑定
6	192.168.45.194	0025.649b.8c92	动态	转静态IP-MAC绑定
7	192.168.45.66	b8ac.6f24.670a	动态	转静态IP-MAC绑定
8	192.168.45.235	00d0.f822.33b7	动态	转静态IP-MAC绑定
9	192.168.45.8	0800.27dd.8217	动态	转静态IP-MAC绑定
10	192.168.45.217	bc30.5bcc.19ed	动态	转静态IP-MAC绑定

首页

上一页

[1]

[2]

[3]

[4]

[5]

下一页

尾页

1

/ 7 页

1.3.5.3 访问限制

访问限制功能是一种对用户上网行为、通信行为进行限制的功能。可以对用户基于 IP 地址和时间的访问限制。访问限制是针对局域网内的用户访问外网的限制。

限制规则只有在有效的时间段内才会被激活，未被激活的规则是无效规则，在报文匹配的时候，总是先从第一条规则依次匹配，如果报文匹配某条规则，那么报文就不会再匹配以后的规则。在配置了限制规则的情况下，将会在所有规则后隐含一条拒绝任何报文访问访问外网的规则。

访问限制是针对用户访问外网的限制

规则的生效时间段是对设备系统时间而言，设备时间不在生效时间段内，则规则处于未激活状态

图 1-49



访问策略：设置当前规则是允许访问还是禁止访问。

规则编号：策略规则编号，数值越小优先级越高，值域范围（1-2147483647）。

源地址和源地址掩码：设置要限制的源地址网段。

周期时间段：即规则生效的时间段，可以设置要生效的星期和当天生效的时间点。

- ✚ 数据报文的匹配规则总是从第一条规则开始，直到匹配到满足的规则为止，规则最后隐含一条拒绝所有报文的规则。
- ✚ 访问限制接口面板最多支持 18 个逻辑接口：主要包含同步口、异步口、Dialer 口和 Virtual-PPP 口。超过该数目的逻辑接口将不会显示，且无法配置访问限制业务。

图 1-50



1.3.6 资源保障

1.3.6.1 主机限速

主机限速的目的是防止某些用户或者应用占用过多的资源（比如带宽等）。另外，对于 icmp flood、和 udp flood 攻击，在其他防御手段都无效的情况下，流量限制是一个简单直接的方式。

 主机限速，确保在源地址网段内所有主机地址平均分配相同的带宽（即页面所设置的带宽）


 主机限速规则需要在生效的时间段内才能激活

图 1-51



接口名称：即生效的接口，设置通过选择上面的接口图标，选中的图标将会变成蓝色，同时填入输入框内。

源 IP 地址和掩码：要限制速度的网段，通过 IP 网段和掩码来确定。

上行带宽：该网段内每台主机的上行带宽。

下行带宽：该网段内每台主机的下行带宽。

周期时间段：即规则生效的时间段，可以设置要生效的星期和当天生效的时间点。


 主机限速接口面板最多支持 18 个逻辑接口：主要包含同步口、异步口、Dialer 口和 Virtual-PPP 口。超过该数目的逻辑接口将不会显示，且无法配置主机限速业务。

图 1-52

主机限速规则配置

接口名称: GigabitEthernet 0/1

源IP地址: * (例如: 192.168.0.1)

源IP地址掩码: * (例如: 255.255.0.0)

上行带宽: * (范围: 1-100000 kbps)

下行带宽: * (范围: 1-100000 kbps)

隐藏

周期时间段

☐ 星期一 ☐ 星期二 ☐ 星期三

☐ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期日

开始时间 : 结束时间 :

完成

取消

1.3.6.2 业务保障

业务保障简介

业务保障采用 HQoS 服务实现，传统的 QoS（Quality of Service，服务质量）通过对业务流分类，并通过针对业务流指定不同的处理策略，从而实现对业务的区分对待，保证业务传输的要求，如带宽要求、时延要求等；然而现有的用户接入网络比较复杂，特别是用户接入网络中存在大量不支持复杂 QoS 的接入设备（如二层交换机、各种转换器等），虽然用户接入网的出口设备能够最大限度的对传输业务进行 QoS 质量保证，但是无法实现针对用户、用户组/群等更为细致的质量保证。

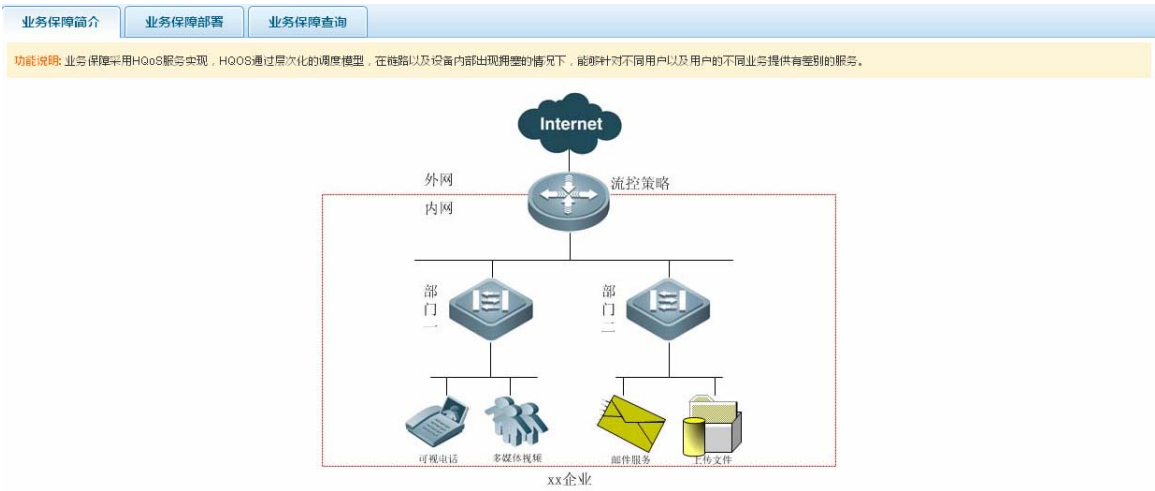
HQoS 即层次化 QoS，不同于以往的单层 QoS 主要针对业务进行保证服务，HQoS 可以将网络中的数据流按照用户业务+用户+楼道+居民区的多层面 QoS 质量服务，最低层的用户业务保证 QoS 可以实现单个用户多业务流之间的质量服务，然后次之的用户业务保证 QoS 可以实现楼道内多个用户之间的质量服务，以此类推楼道和社区都实现对应的 QoS 质量保证，HQoS 技术可以实现按照业务层次划分实现对应分层的 QoS 质量保证，可以实现数据聚合设备 QoS 技术的作用精度，提高整网用户服务质量。

“业务保障简介”页面的拓扑图为典型的企业机构应用场景，在场景应用中，出口总带宽有限的情况下，不同部门内部有不同的业务需要保障，一般情况下语音视频业务优先于一般上网业务。不同部门之间也需要按部门重要程度保障带宽。这个时候传统的 QoS 无法进行差异化的服务，那么 HQoS 解决了这个问题，对应用业务进行分层。企业出口一层，部门一层，下面的数据业务一层。

在企业总带宽一定的情况下，会议室可能因为重要会议而不能因为被其它部门抢占了带宽资源而视频会议卡死或断线，那么它将被设置更高的保证带宽，但是会议室因为用户个别非法用户下载电影而上其它部门业务无法开展，那么他将被限制最大带宽。对于部门下的员工来说，行政人员，需要经常电话沟通，那么在行政部带宽资源一定的情况下，那么保证其电

话业务畅通就显得更为重要，可以针对电话业务设置高优先级，电话业务的数据报文优先于其它业务进行处理，降低语音电话的时延，保障语音畅通。

图 1-53



业务保障部署

业务保障的部署将按照企业->部门->业务三层结构模型进行部署，他们的关系示意图如下图，每一个节点都有其带宽或者报文处理的优先级属性。根据企业的部署需要，适当调整各节点属性参数，就能满足不同部门，不同业务的优先级保障。最大限度利用企业出口带宽，节约企业成本。

图 1-54

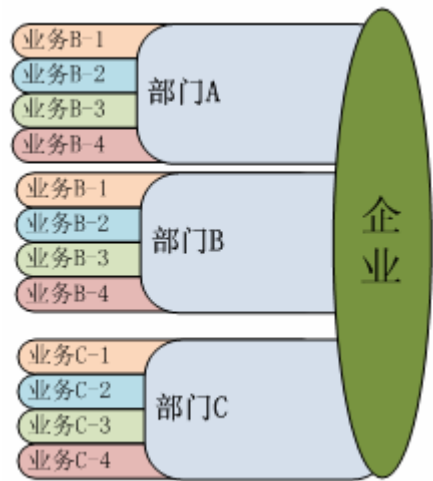


图 1-55

业务保障简介 业务保障部署 业务保障查询

操作提示: 请在<<拓扑结构>>栏选择目录对象。当鼠标移到目录节点时，字体变成淡蓝，鼠标形状变成手型时表示可点击，点击后会在表单尾部出现相应的功能按钮。

注意事项: 业务部署时，请确认部署接口为下联接口，下联接口主要负责业务报文的发送工作。

业务保障部署表单	最小带宽	最大带宽	业务优先级	操作
xx企业	N/A	1,000,000 kbps	N/A	编辑
部门一	5,000 kbps	10,000 kbps	N/A	编辑 删除
部门二	6,000 kbps	10,000 kbps	N/A	编辑 删除

xx企业:

业务保障部署，首先需要设置企业出口的总带宽，然后在企业节点下面新建部门，并为根据每个部门带宽需求的重要性进行保证带宽和最大带宽设置，常规情况下，重要的部门设置比较高的带宽，其他部门次之。比如领导办公室，通常会设置比较高的最大保证带宽和合理的最大带宽，保证领导们的带宽需求。然后再在部门节点下设置需要优先保护的業務。比如领导经常需要视频会议，电话会议，那么需要设置视频和电话业务为高优先级处理。

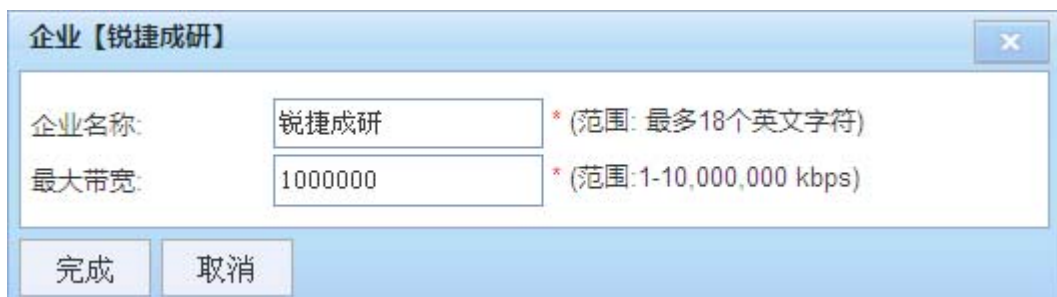
具体的操作如下：

1) 企业总带宽设置

默认情况下，总有一个企业节点存在，可以对企业节点改名，设置企业出口总带宽。具体可点击“编辑”

展开企业下的子节点，请点击  图标。

图 1-56



企业【锐捷成研】

企业名称:	<input type="text" value="锐捷成研"/>	* (范围: 最多18个英文字符)
最大带宽:	<input type="text" value="1000000"/>	* (范围: 1-10,000,000 kbps)

2) 部门带宽设置

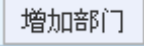
增加部门需要点击其要下挂的父节点，即企业节点，点击  按钮，增加部门，设置部门保证带宽和最大带宽，要调整部门带宽请点击“编辑”。



图 1-57



增加部门【锐捷成研】

部门名称:	<input type="text"/>	* (范围: 最多18个英文字符)
最小带宽:	<input type="text"/>	* (范围: 0-1,000,000 kbps)
最大带宽:	<input type="text"/>	* (范围: 1-1,000,000 kbps)


3) 业务设置

部门下业务的展开需要点击  图标，添加业务需要先点击其父节点，即部门节点，点击  业务按钮添加业务，修改业务请点击“编辑”。

对业务的设置首先需要进行业务区分，业务的分类是通过 DSCP 值，或者 ACL（即访问控制列表，通过协议号，源 IP，源端口，目的 IP，目的端口报文五元组信息来匹配数据报文的控制列表）来区分的，一条业务的识别，只要匹配规则中的任意一条规则来决定这条业务。

对匹配出来的业务数据流，需要设置相应的属性，比如业务的带宽，业务优先级。业务的优先级分为高优先级和低优先级，他们的优先级顺序是 高优先级>低优先级。对于一些实时通信类业务往往设置高优先级，比如语音、视频等。对于通信实时性要求不高的业务，往往设置较低的优先级，比如下载类业务，上网浏览业务。

业务部署完成之后，点击“编辑”，可以查看当前业务的部署情况，同时也可以查看当前业务部署接口上的其它业务，进入编辑业务配置菜单，若当前业务有部署，则接口的颜色为蓝色，将鼠标移至接口图标上，立即显示接口业务，并对当前业务用黄色标记；若没有部署则接口颜色为白色。

 业务的优先级顺序为：高优先级>低优先级。


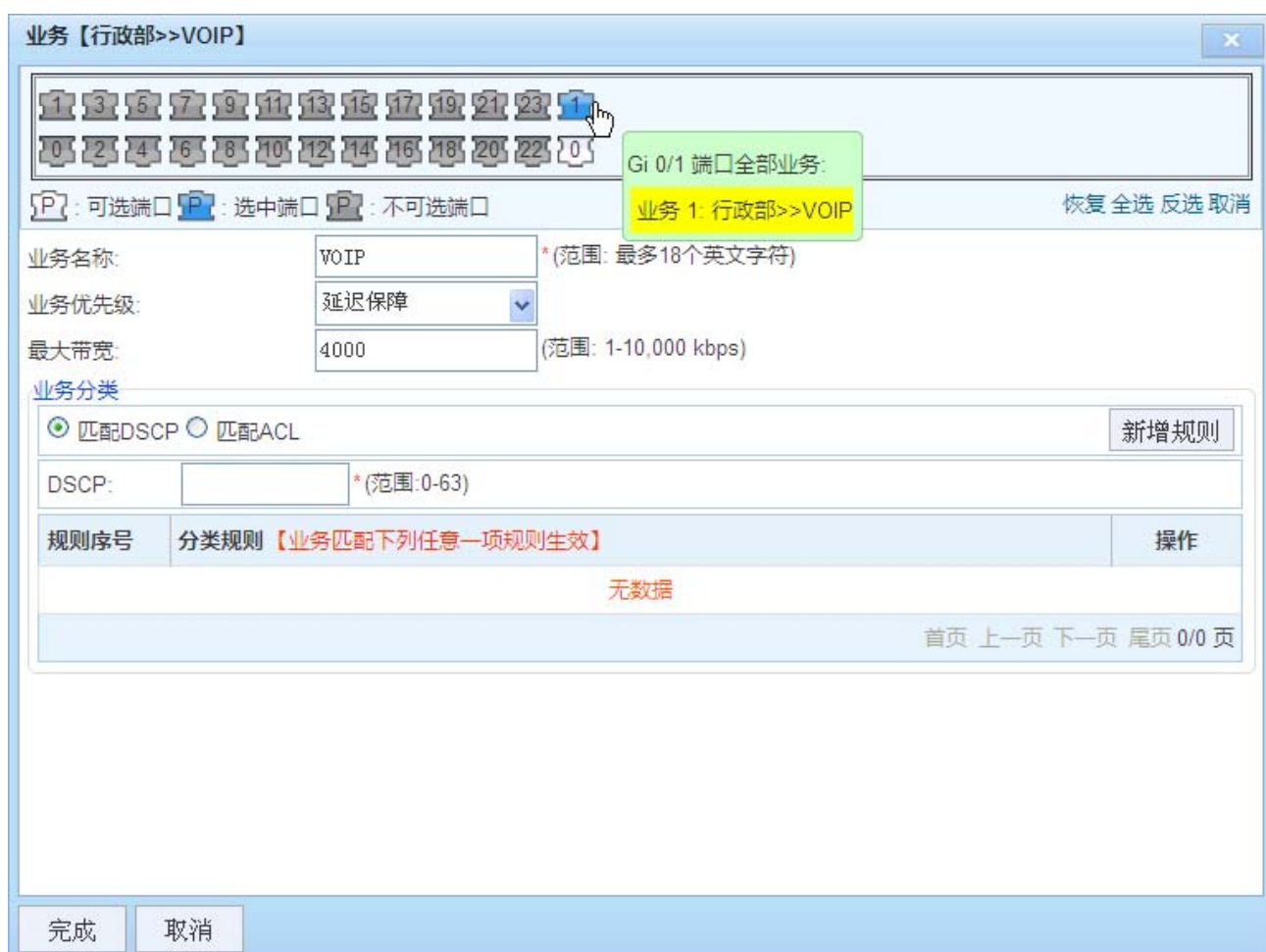
 业务分类即数据流的识别，通过规则来区分这条业务流。决定这条业务流的关系是“或”的关系

图 1-58



当选择匹配 ACL，再点击“新增规则”按钮弹出以下业务分类规则设置对话框。首先选择当前协议，然后进行报文五元组信息识别的设置。


 该网页接口面板最多支持 18 个逻辑接口：主要包含同步口、异步口、Dialer 口和 Virtual-PPP 口。超过该数目的逻辑接口将不会显示，且无法指定相关业务。

图 1-59

业务分类规则

TCP UDP IP ICMP

动作: ☒ 允许 ☐ 禁止

☐ 任意源 IP 地址

地址类型: 单 IP 地址 源 IP 地址: *

源端口范围(0-65535): -

☐ 任意目的 IP 地址

地址类型: 单 IP 地址 目的 IP 地址: *

目的端口范围(0-65535): -

完成 取消

业务保障策略默认应用在接口的入方向

DSCP：差分服务代码点（Differentiated Services Code Point），IETF 于 1998 年 12 月发布了 Diff-Serv（Differentiated Service）的 QoS 分类标准。它在每个数据包 IP 头部的服务类别 TOS 标识字节中，利用已使用的 6 比特和未使用的 2 比特字节，通过编码值来区分优先级

各参数的设置需要根据网络环境的实际情况进行调整，不断优化，否则业务保障将起不到很好的效果

业务保障查询

为了方便用户查阅接口业务部署，特提供了业务保障查询的功能，用户可以在本网页点击要查询接口，确认接口之后，接口上部署的业务立即显示在网页的下方，并提供了业务的名称、业务带宽、业务优先级、隶属部门名称、保障带宽和最大带宽等信息。

图 1-60

业务保障简介 业务保障部署 业务保障查询

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

可选端口 选中端口 不可选端口

接口 GigabitEthernet 0/1 应用业务表

业务名称	业务带宽	业务优先级	部门名称	最小带宽	最大带宽
VOIP	4,000 kbps	延迟保障	行政部	5,000 kbps	10,000 kbps

首页 上一页 1 下一页 尾页 1 / 1 页

该网页接口面板最多支持 18 个逻辑接口：主要包含同步口、异步口、Dialer 口和 Virtual-PPP 口。超过该数目的逻辑接口将不会显示，且无法查看隐藏接口业务部署。

1.3.7 系统维护

1.3.7.1 基本配置

在基本设置里，包含系统时间设置，SNMP 管理。

时间设置

通过该功能可以设置设备的当前时间，您也可以开启“自动与 Internet 时间服务器同步”时间，也就是设备的时间会始终保持跟互联网上的时间一致；不过这个功能依赖于是否配置了正确的 DNS 服务，如果您还未配置 DNS 服务器。请到“快捷配置”页面进行配置。

图 1-61

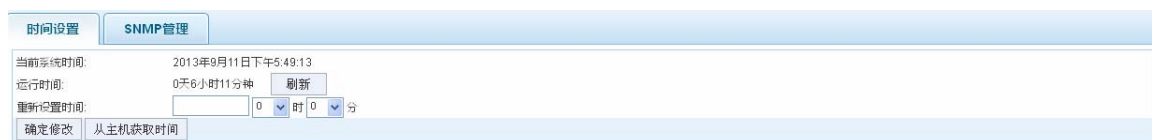


图 1-61 展示了设备的时间设置界面。界面顶部有两个标签页：“时间设置”和“SNMP管理”，当前选中的是“时间设置”。界面内容显示当前系统时间为 2013 年 9 月 11 日下午 5:49:13，运行时间为 0 天 6 小时 11 分钟，并有一个“刷新”按钮。下方有“重新设置时间”的输入框，显示为 0 时 0 分。底部有两个按钮：“确定修改”和“从主机获取时间”。

SNMP 管理

简单网络管理协议，配置 SNMP 管理员可轻松进行对网络上的节点进行监控和管理。主要针对远程专业的网管人员通过 SNMP 维护和管理设备。

SMNP 版本：目前设备支持 V2 和 V3 版本；下图是配置 V2 版本的示意。

图 1-62



图 1-62 展示了设备 SNMP 管理的 V2 版本配置界面。界面顶部有两个标签页：“时间设置”和“SNMP管理”，当前选中的是“SNMP管理”。界面内容显示“说辞：SNMP即简单网络管理协议，配置SNMP管理员可轻松进行对网络上的节点进行监控和管理。”。下方有“SNMP版本”选择，当前选中了“V2版本”，旁边有“V3版本”选项。下方有“SNMP口令”、“Trap口令”和“Trap接收主机”三个输入框，每个输入框右侧都有一个红色的星号。底部有两个按钮：“应用”和“清除设置”。

配置 SNMP V3 版本的示意图：

图 1-63



图 1-63 展示了设备 SNMP 管理的 V3 版本配置界面。界面顶部有两个标签页：“时间设置”和“SNMP管理”，当前选中的是“SNMP管理”。界面内容显示“说辞：SNMP即简单网络管理协议，配置SNMP管理员可轻松进行对网络上的节点进行监控和管理。”。下方有“SNMP版本”选择，当前选中了“V3版本”，旁边有“V2版本”选项。下方有“SNMP用户”、“加密密码”、“认证密码”、“Trap口令”和“Trap接收主机”五个输入框，每个输入框右侧都有一个红色的星号。底部有两个按钮：“应用”和“清除设置”。

SNMP V3 版本提高了安全性设置，需要添加 SNMP 用户的加密密码和认证密码。

1.3.7.2 权限管理

密码设置

WEB 管理员密码：修改当前登录管理员的密码，登出 WEB 系统之后，必须使用修改后的密码登录。

✚ 修改后的密码请务必牢记，以免下次登录时无法进入

图 1-64

管理员权限

该功能只有特权用户“admin”才拥有权限，其他用户登录 WEB 系统后，该功能不可见。特权用户可以在此页创建 WEB 管理员，并授权页面，新增的管理员可以登录 WEB 管理系统对设备进行日常维护或管理，但无法通过 Telnet 执行命令。

✚ 为了安全起见该功能页面有且只有 admin 用户可以查看并编辑。

图 1-65

用户名：这里可以任意输入您想要的管理员名称，推荐使用英文避免使用中文；例如：zhangs;

登录密码：是管理员登录设备 WEB 网管的密码；

授权页面：点击“编辑授权页面”会弹出对话框，您可以对该管理员指派管理的权限。如下图

图 1-66 admin 用户登入

管理员权限

说明：本页面添加的设备管理员可以登录Web管理系统对设备进行日常维护，但无法通过Telnet执行命令；保留用户manager和guest不能删除。

用户名： *

登录密码： *

授权页面：[编辑授权页面](#)

☐ 用户名
☐ guest
[删除选中](#)
[首页](#) [上一页](#) [\[1\]](#) [下一页](#)

编辑授权页面 [关闭]

- ☒ 所有页面
 - ☒ 设备概览
 - ☒ 基本配置
 - ☒ 虚拟专网
 - ☒ 动态防火墙
 - ☒ 资源保障
 - ☒ 系统维护

[确定](#)

操作	
	编辑

在 WEB 网管系统中，只有“Admin”用户才拥有该权限，该用户可以指派管理员以及授权管理员访问 WEB 的界面，而指派管理员登录到 WEB 网管系统，是没有指派其他管理员的能力，该网页会自动隐藏。

图 1-67 guest 用户登入

密码设置

说明：admin用户拥有配置和查看设备信息的所有权限。
提示：如果您设置了新的WEB登录密码，则在设置之后使用新密码重新登录。密码不能含有中文、全角字符、问号和空格。密码最长不能超过20字符。

修改WEB超级管理员密码

用户名：

新密码：

确认新密码：

[确定修改](#) [清空](#)

非特权用户登录 WEB 网管系统后，只能修改登录密码，没有指派管理员的能力。

1.3.7.3 软件升级

软件升级，可以升级设备主程序固件，同时也可以升级 WEB 软件包，它们通过文件名后缀自动识别所升级的软件。

本地升级：点击“浏览”按钮，选择你下载到本地电脑上的升级包文件。然后点击“开始升级”，界面会出现“正在升级”的进度条，此时请耐心等待，不能进行任何操作。大约等待 50 秒左右设备会提示升级成功，若升级软件主程序，必须在升级成功后，设备重启主程序方能生效，若升级 WEB 包文件，设备无需重启，直接刷新网页即可。

图 1-68

软件升级	
版本信息	
软件版本: RGOS 10.4(3b13) Release(159680) 硬件版本: 1.00	
说明: 软件升级可实现固件版本和WEB包的升级, 固件版本升级完成后须重启设备才能生效。	
软件升级	
<input type="text"/>	<input type="button" value="浏览..."/> <input type="button" value="开始升级"/>

- 您可以访问[锐捷网络官方网站](#)的"软件版本"来下载最新的升级文件到本地, 然后通过该页面升级到设备。升级过程中不能关闭或者刷新本页面, 直至出现升级成功的提示, 否则会导致升级失败。升级过程大约需要 50 秒左右的时间。
- 如果是升级软件主程序必须将文件后缀名指定为 "bin", 升级 WEB 包文件后缀名指定为 "upd", 请确认所升级的版本适用于该设备。
- 在升级过程中, 可能会遇到整理 flash 从而导致页面暂时没响应, 此时不能断电或者重启设备, 直到提示升级成功, 否则可能导致设备不能启动。

1.3.7.4 配置管理

保存配置

在各页面配置完成后, 并没有将配置写入配置文件, 所以为了配置不丢失, 需要在这里保存配置, 确保修改的配置在系统断电后不会丢失。

- 在保存过程中由于配置信息量大, 所以保存配置的过程需要一定的时间。

图 1-69

保存配置	配置导入与导出	恢复出厂设置
说明: 配置将被保存到设备中, 设备断电也不会丢失。 提示: 保存过程可能需要几分钟, 请耐心等待。		
<input type="button" value="保存设置"/>		

配置导入与导出

配置导入: 配置文件必须以 ".text" 为后缀名, 否则无法导入配置, 文件名可以随意, 只要符合本地命名规则即可, 但导入配置文件分为两种情况, 一种是导入 "config.text", 以此文件名的配置文件导入后, 设备重启后配置会生效。另一种则是其他的名称的配置文件, 导入到设备后, 只是作为配置的备份, 即使设备重启也不会生效。

配置导出: 配置导出除了可以查看当前配置之外, 另一个用途就是备份配置到本地, 出于安全考虑, 在完成设备配置之后, 都应该备份的配置文件。

- 导入 "config.text" 配置文件后必须重启设备后才能生效。
- 在导入的过程中, 不能关闭页面或刷新网页, 否则可能导入失败。

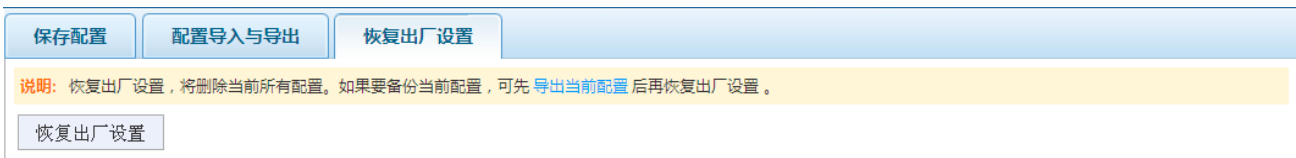
图 1-70



恢复出厂设置

恢复出厂设置将删除所有配置，在确认要恢复出厂设置前，最好先备份配置，以免配置丢失。恢复出厂设置系统将重启

图 1-71



1.3.7.5 设备重启

点击“立即重启设备”将使设备重新启动。重新启动需要2分钟左右的时间，该期间不要做其它任何操作。当设备重启成功后将自动登出到 WEB 系统，跳转到 WEB 认证界面。

图 1-72



1.3.7.6 日志信息

操作日志

操作日志记录 WEB 操作的记录，比如，用户登录、保存配置、导入配置等 WEB 操作的关键信息

图 1-73

操作日志		
系统日志		
提示：操作日志显示最多500条操作日志		
操作日志		
时间	操作员的ip	描述
2012-12-28 10:06:53	192.168.50.117	用户登录
2012-12-28 09:58:24	192.168.50.117	配置导入与导出页面，导出系统配置
2012-12-28 09:57:29	192.168.50.117	保存配置
2012-12-28 09:55:22	192.168.50.117	密码设置页面，修改telnet登陆密码
2012-12-27 18:05:21	192.168.50.117	保存配置
2012-12-27 18:02:41	192.168.50.117	时间设置页面，修改系统时间
2012-12-27 08:58:37	192.168.50.117	新建策略路由成功
2012-12-26 15:32:14	192.168.50.117	外网接口 GigabitEthernet 0/0 保存成功
2012-12-26 15:32:00	192.168.50.117	外网接口 GigabitEthernet 0/0 保存成功
2012-12-26 15:28:33	192.168.50.117	外网接口 GigabitEthernet 0/0 保存成功
首页 上一页 [1] [2] [3] 下一页 尾页 <input type="text" value="1"/> / 3页		

系统日志

系统日志记录设备软件系统的日志，日志的生成有系统决定，比如接口掉线、IP 冲突、遭受攻击等

图 1-74



1.3.7.7 通信检测

Ping 通信检测

通过 Ping 工具，检测本设备和目的地址是否数据可达。当出现 “!!!!” 表示数据是可达的，当出现 “.....” 表示数据包丢失，数据不可达。

“!” 代表一个可达的数据包，“.” 代表一个不可达的数据包，有几个符号代表有几个检测数据包

图 1-75



路由跟踪检测

通过 traceroute 路由跟踪工具，检测本设备到目的网络的路由是否可达。帮助网络管理人员定位网络故障。

图 1-76

PING通信检测

路由跟踪检测

说明: 您可以输入IP地址或者网站的域名, 通过TRACEROUTE进行路由跟踪检测, 您的主机到目的主机之间经过的路由信息将显示出来, 若要对某个域名进行路由跟踪检测, 请先在“快速配置”页面配置DNS服务器。

目的IP/域名:

< press Ctrl+C to break >

Tracing the route to 192.168.50.110

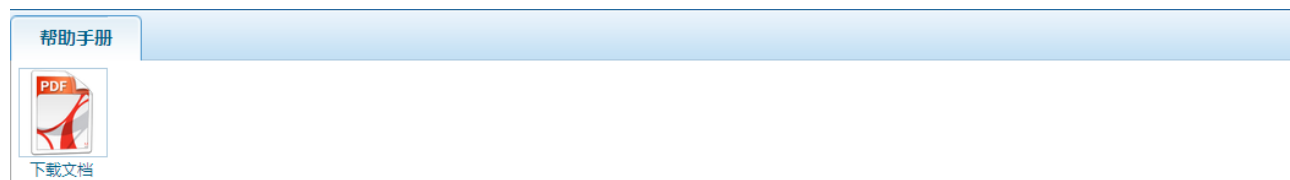
1 192.168.52.1 0 msec 0 msec 0 msec

2 192.168.50.110 10 msec 10 msec 10 msec

1.3.7.8 帮助手册

帮助手册是为用户提供的在线帮助手册, 指导用户配置和使用设备, 用户可以点击图标下载手册保存到私人电脑查阅。

图 1-77



1.4 技术支持

1.4.1 售后在线客服

我司为快捷的解决客户遇到的问题, 提供了售后“在线客服”交流平台, 客户只需在 WEB 系统上点击“在线客户”链接就可以与我们的售后服务人员交流, 为更好了解和帮助客户, 该平台能自动将设备型号以及软件版本反馈给售后平台, 同时在平台中, 为客户提供多种服务内容, 如: 在线留言、典型配置案例、常见问题搜索、软件下载、技术论坛, 文件传输等等。

图 1-78 WEB 登录界面



图 1-79 WEB 网管首页



图 1-80 售后服务平台



售后服务平台服务时间:周一至周五, 8:30-18:00, 若客户未在此时间登入, 可以在线留言。

售后服务平台若出现功能异常或是无法交流, 请使用技术支持服务电话: 4008-111-000。

售后服务平台是独立于 WEB 管理系统, 因此平台中出现操作异常与 WEB 管理系统无关。

1.4.2 售后技术支持

除了“在线客服”平台支持之外, 我司还提供了技术支持论坛 <http://support.ruijie.com.cn>, 以及技术支持服务电话: 4008-111-000。在WEB网管系统中, 这些信息显示在WEB界面的页脚, 客户可以点击链接或打服务电话进行咨询。

图 1-81 技术支持链接



1.5 异常处理

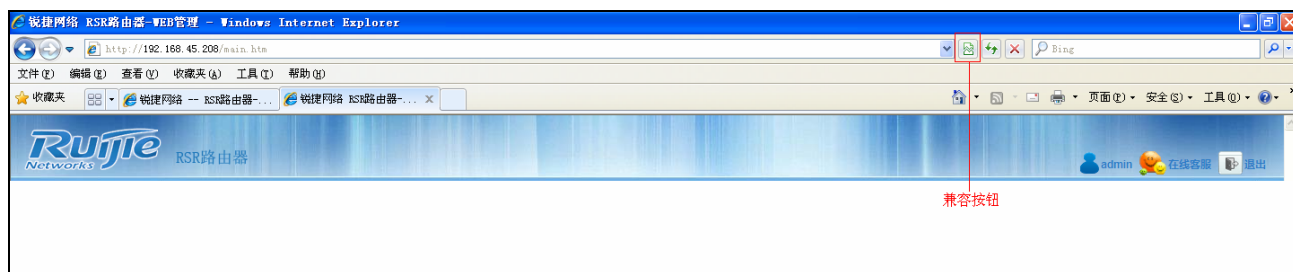
1.5.1 加载插件

加载插件这种情况一般很少出现，只有客户在刚安装浏览器之后，就访问 WEB 网管系统时有可能出现，一旦出现这样只需运行插件即可，无需担心插件带来的影响。

1.5.2 显示异常

由于浏览器版本更新的速度越来越频繁，这也给 WEB 带来了一系列的兼容性问题，特别是使用 IE 浏览器时，当网页显示出异常的时候，请点击兼容模式，能解决一些异常行为。

图 1-82 兼容模式



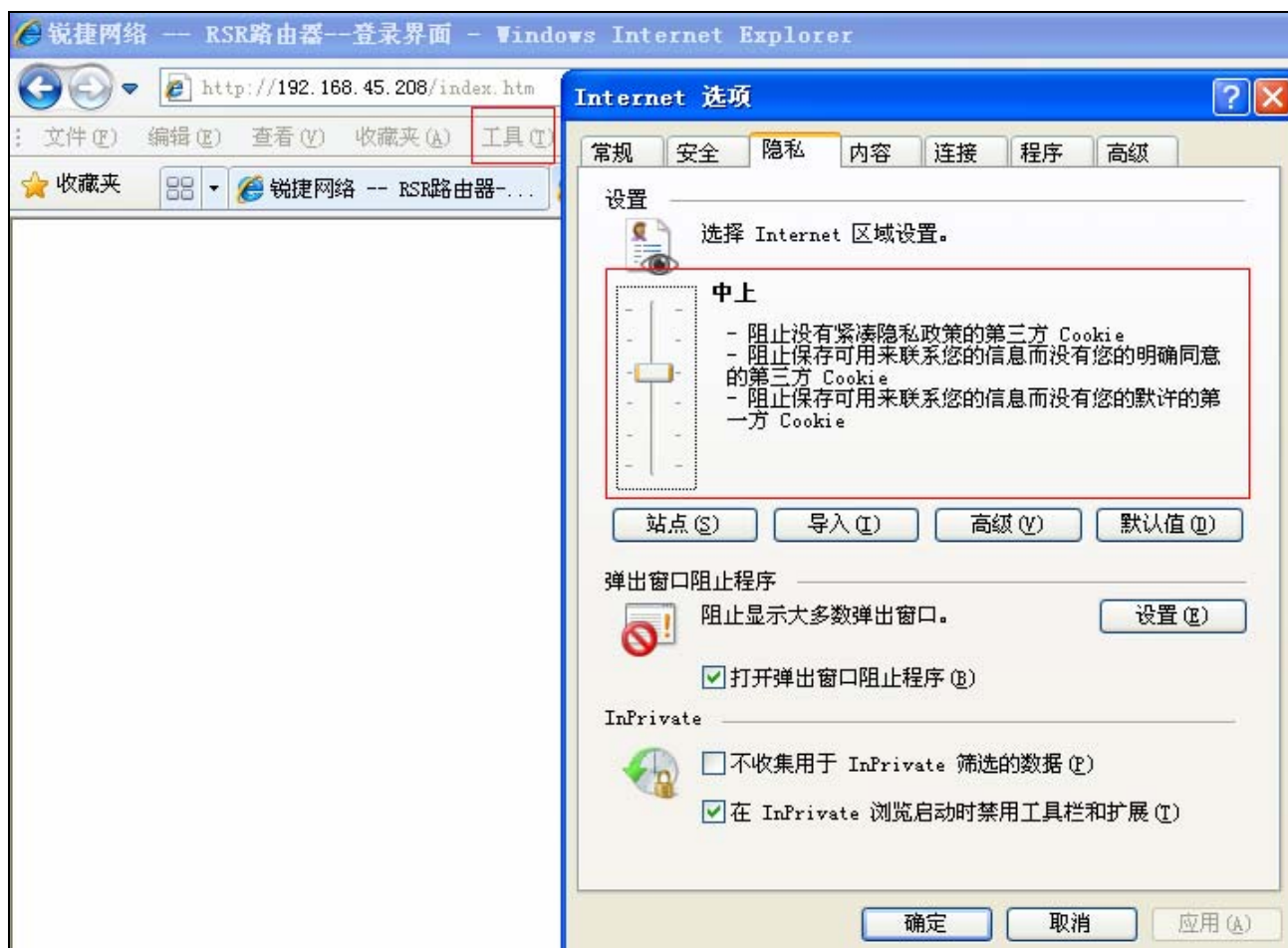
使用 IE9.0 或 IE10.0 访问 WEB 管理系统时，首页的 CPU 可能会异常，可以点击兼容模式，其它浏览无异常。

1.5.3 WEB认证失败

WEB 认证失败，一般情况下是用户输入的用户名或密码错误导致，因此请在登录 WEB 系统之后，一定要牢记修改密码。

，若在确认输入的用户名或密码无误的情况下，请检查浏览器的设置，下面以 IE 浏览器为例：

图 1-83 IE 设置



点击“工具”，选择“隐私”，在红色的区域中，选择中上或中上偏下即可，若设置成高级别，将无法登陆 WEB。

1.5.4 WEB无法访问

案例 1：若 PC 能正常 Ping 通设备，但又无法访问 WEB，请检查 WEB 服务是否开启。

图 1-84 WEB 服务状态

```
Ruijie(config)#show service
ssh-server      : disabled
telnet-server   : enabled
web-server      : disabled
web-server(https): disabled
snmp-agent      : enabled
```

“disabled”表示 WEB 服务未开启，需要使用命令“enable service web-server all”开启 WEB 服务。

案例 2：若 PC 不能 Ping 通设备，这时需要检查连接设备的接口指示灯，若接口的指示灯亮起，请检查 PC 与路由器的 IP 地址，若指示灯未亮起，则检查网线是否插好或更换网线。

案例 3：网页返回“404”，可能 WEB 包已经损坏，需要更新 WEB 包。

图 1-85 无网页



1.5.5 WEB超时登出

WEB 管理系统默认设置有系统超时登出时间，只要管理人员登入 WEB 管理系统之后，若在 10 分钟之内无任何操作，系统就会自动登出，若在 10 分钟之内有操作 WEB 行为，时间计数器会自动清零重新计时。

 超时时间默认为 10 分钟，不能手动修改。

1.5.6 逻辑接口异常

逻辑接口异常主要体现在逻辑接口过多时，只显示一部分逻辑接口，而另外一部分逻辑接口不能显示。这是因为 WEB 在设计面板时限制了逻辑接口的显示数目（最多显示 18 个逻辑接口），限制逻辑接口是按照真实的使用场景进行分析得出的结果。分布如下：

PPPoE：计划 4 个 Dialer 逻辑接口；

SVI 口（外网）：计划 2 个 SVI 接口；

VPN 拨号：计划 3-5 个 Virtual-PPP 逻辑接口；

3G、同步卡、E1：一台 RSR 系列路由器最多 6 个插槽，即 6 个逻辑接口；

为了避免这类问题发生，请按照实际的网络部署进行配置，减少冗余配置。