



海蜘蛛路由 V8 用户手册


海蜘蛛文档编写小组 <docs@hi-spider.com>

最后更新时间：2013-12-04 17:35 星期三

版权 © 2005-2013 版权所有 武汉海蜘蛛网络科技有限公司 (Hi-Spider Network Technology Co., Ltd. All rights reserved)

摘要

本手册对海蜘蛛路由系统的功能特性、配置方法等进行了详细的说明，关于安装方法请参考[\[安装指南\]](#)

您可以访问 [\[这里\]](#) 获取本手册的最新版本；为了方便在本地离线阅读，您可以 [下载pdf](#)  （推荐使用 Adobe Acrobat pro 7.0 以上版本来打开）

如果您发现本手册有错误之处，或您有何建议，请与作者联系，感谢您的支持！

目录

[I. 系统介绍](#)

[1. 系统介绍](#)

- [1.1. 产品概述](#)
- [1.2. 功能介绍](#)
- [1.3. 技术特性](#)

[II. 系统设置](#)

[2. 海蜘蛛路由首页](#)

[3. 系统设置](#)

- [3.1. 基本设置](#)
- [3.2. WEB 远程管理](#)
- [3.3. 控制台登录](#)
- [3.4. 报警设置](#)
- [3.5. 邮件设置](#)
- [3.6. 定时关机 & 重启](#)
- [3.7. 网卡驱动模块](#)
- [3.8. 启动菜单配置](#)
- [3.9. 磁盘分区管理](#)
- [3.10. 保存 & 重启](#)
- [3.11. 远程唤醒 \(WOL\)](#)

[III. 网络设置](#)

[4. 网络设置](#)

[4.1. DNS 参数](#)

[4.2. 动态域名解析](#)

[4.2.1. 配置动态域名解析](#)

[4.2.2. 动态域名解析相关问题](#)

[4.3. 静态路由](#)

[4.4. 多线负载及策略](#)

[4.4.1. 多线路策略简介](#)

[4.4.2. 两条相同网络运营商线路接入](#)

[4.4.3. 两条不同的网络运营商线路接入](#)

[4.4.4. 多条不同网络运营商线路接入](#)

[4.4.5. 两条电信+两条网通+一条铁通](#)

[4.4.6. 多线负载均衡](#)

[4.4.7. 不同ISP实现策略路由](#)

[4.5. 自定义策略](#)

[4.6. 自定义路由表](#)

[4.7. 虚拟局域网\(VLAN\)](#)

[4.7.1. 虚拟局域网简介](#)

[4.7.2. 路由上划分VLAN](#)

[4.8. 透明网桥](#)

[4.8.1. 透明网桥典型实例](#)

[4.8.2. 启用透明网桥](#)

[4.8.3. 透明网桥直接接外网](#)

[5. 快速接入互连网](#)

[5.1. 局域网 \(LAN\) 设置](#)

[5.2. 设置 DNS 参数](#)

[5.3. 设置广域网 \(WAN\)](#)

[6. 3G 无线接入设置](#)

[6.1. 3G 无线上网简介](#)

[6.2. 参数设置](#)

[6.3. 设置多线负载及策略](#)

[6.4. 支持的3G无线上网卡](#)

[IV. 防火墙](#)

[7. 基本安全设置](#)

[7.1. 普通模式](#)

[7.2. 高级应用](#)

[7.3. 特殊应用](#)

[8. 黑白名单](#)

[9. IP-MAC 绑定](#)

[9.1. IP与MAC地址绑定的作用](#)

[9.2. 启用IP与MAC绑定](#)

[10. DNS/IP过滤](#)

[10.1. 什么是DNS/IP过滤](#)

[10.2. 启用DNS/IP过滤](#)

[11. 网址/关键字过滤](#)

[11.1. 网址/关键字过滤的好处](#)

[11.2. 规则说明](#)

[11.3. 启用网址/关键字过滤](#)

[12. ACL 规则](#)

[13. 端口镜像](#)

[13.1. 端口镜像简介](#)

[13.2. 设置步骤](#)

[14. 端口映射](#)

[14.1. 端口映射简介](#)

[14.2. 启用端口映射](#)

[14.3. 端口映射不成功，如何找出问题原因](#)

[14.4. 端口443映射不成功的原因](#)

[15. DMZ主机](#)

[15.1. DMZ简介](#)

[15.2. DMZ主机设置](#)

[16. UPnP支持](#)

[16.1. UPnP简介](#)

[16.2. 启动UPnP服务](#)

[17. 一对一NAT](#)

[17.1. 一对一NAT简介](#)

[17.2. 启动一对一NAT服务](#)

[17.3. 一对一NAT与端口映射及DMZ的区别](#)

[18. No NAT](#)

[18.1. No NAT简介](#)

[18.2. 启动No NAT功能](#)

[V. 上网行为管理](#)

[19. 恶意网址拦截](#)

[19.1. 恶意网站简介](#)

[19.2. 自定义恶意网址](#)

[19.3. 拦截动作设定](#)

[20. URL 重定向](#)

[21. 推送网页通知](#)

[21.1. 通知内容的几种形式](#)

[21.2. 编写网页通知](#)

[21.2.1. 指定推送用户](#)

[21.2.2. 上传文件](#)

[21.2.3. 编写网页通知](#)

[22. 预定义对象](#)

[23. 对象分组管理](#)

[24. 应用协议过滤](#)

[25. 上网期限管理](#)

[26. 上网行为管理综合应用](#)

[26.1. 网络拓扑结构](#)

[26.2. 新建用户与分组](#)

[26.3. 新建时间与网址对象](#)

[26.4. 设置各组的应用协议控制](#)

[26.5. 仅允许收发Web邮件](#)

[26.6. 特征库的更新](#)

[VI. 服务应用](#)

[27. 用户账号管理](#)

[28. DHCP服务](#)

[28.1. DHCP简介](#)

[28.2. 启动服务器端DHCP服务](#)

[28.3. 客户端配置](#)

[29. DNS代理解析](#)

[29.1. 启用DNS代理解析](#)

[29.2. DNS重定向](#)

[29.3. DNS劫持](#)

[30. NTP时间服务器](#)

[31. 网络打印服务](#)

[31.1. 网络打印解决方案](#)

[31.2. 服务端设置](#)

[31.3. 客户端设置](#)

[32. 上网Web认证](#)

[32.1. 上网Web认证简介](#)

[32.2. Web认证设置](#)

[32.2.1. 参数设置](#)

[32.2.2. 认证页面设置](#)

[32.2.3. 在线用户管理](#)

[32.3. Web用户帐号管理](#)

[32.4. 自定义Web认证页面](#)

[33. 局域网PPPoE服务](#)

[33.1. 什么是局域网 PPPoE](#)

[33.2. PPPoE 服务端的设定](#)

[33.3. PPPoE 客户端设置\(Windows \)](#)

[33.4. PPPoE 拨号专线客户端](#)

[33.4.1. PPPoE 拨号专线设置](#)

[33.5. 与第三方计费系统对接](#)

[33.5.1. 与蓝海卓越计费系统对接](#)

[33.6. 测试 PPPoE 连接](#)

[33.7. 管理已拨号用户](#)

[33.8. 客户机无法访问Internet](#)

[34. 虚拟专用网\(VPN\) PPTP 服务](#)

[34.1. 什么是 PPTP VPN](#)

[34.2. PPTP VPN 典型解决方案](#)

[34.3. PPTP VPN 服务端的设定](#)

[34.4. 使用内网 PPTP VPN 服务器](#)

[34.5. PPTP VPN 客户端设置\(Windows\)](#)

[34.6. 测试 VPN 连接](#)

[34.7. 常见错误及问题](#)

[34.8. PPTP VPN 虚拟双线（借线）](#)

[34.8.1. 借线服务器端设置](#)

[34.8.2. 借线客户端的设置](#)

[34.9. 和Win Server建立PPTP VPN连接](#)

[35. 虚拟专用网\(VPN\) SSL服务](#)

[35.1. 什么是 SSL VPN](#)

[35.2. SSL VPN 典型解决方案](#)

[35.3. SSL VPN 服务端的设定](#)

[35.4. 使用内网 SSL VPN 服务器](#)

[35.5. SSL VPN 客户端设置\(Windows\)](#)

[35.6. 测试 VPN 连接](#)

[35.7. 常见错误及问题](#)

[35.8. 局域网互连\(路由模式\)](#)

[35.8.1. 服务器端设置](#)

[35.8.2. 客户端设置](#)

[35.8.3. 测试连接](#)

[35.9. 局域网互连（桥接模式）](#)

[35.9.1. 服务器端设置](#)

[35.9.2. 客户端设置](#)

[35.10. 路由 SSL VPN 互联导入证书](#)

[36. IP 隧道服务](#)

[36.1. 什么是 IP 隧道服务](#)

[36.2. IP 隧道服务的网络拓扑图](#)

[36.3. IP 隧道服务服务端的设定](#)

[36.4. IP 隧道服务客户端设置](#)

[36.5. 测试 IP 隧道连接](#)

[VII. 流量控制](#)

[37. 流量控制](#)

[37.1. 流控简介](#)

[37.2. 流量控制的设置步骤](#)

[37.3. 流量控制说明](#)

[37.3.1. 带宽使用模式](#)

[37.3.2. 限速设置说明](#)

[37.4. 针对 PPPoE 用户限速](#)

[38. 如何查看路由流量](#)

[38.1. SSH简介](#)

[38.2. 启动SSH远程登录服务](#)

[38.3. 利用Putty查看路由流量](#)

[VIII. 扩展模块](#)

[39. ha \(高可用性套件\) 模块](#)

[40. smsgw \(短信网关\) 模块](#)

[41. FTP 服务](#)

[41.1. 什么是 FTP 服务](#)

[41.2. FTP 服务器参数设置](#)

[41.3. FTP 账号管理](#)

[42. PXE 无盘服务](#)

[42.1. 什么是 PXE 无盘服务](#)

[42.2. PXE 无盘分组启动的典型解决方案](#)

[42.3. PXE 无盘分组启动的设置](#)

[42.4. 制作PXE的多重启动](#)

[43. 无线接入服务](#)

[43.1. 服务端设置](#)

[43.2. 客户端设置](#)

[43.3. 无线AP支持网卡列表](#)

[44. IPSec VPN 模块](#)

[44.1. 什么是 IPSec VPN](#)

[44.2. IPSec VPN 的典型解决方案](#)

[44.3. IPSec VPN 的设置](#)

[44.4. 测试 VPN 连接](#)

[44.5. 与其它设备建立IPSec VPN](#)

[44.5.1. 与天融信网络卫士防火墙建立IPSec VPN](#)

[45. 智能 QoS 模块](#)

[46. 安全流控模块](#)

[46.1. 安全流控简介](#)

[46.2. 安全流控配置](#)

[46.3. 安全流控的升级](#)

[46.4. 安全流控的部署](#)

[46.4.1. 万象2004版+易游有盘整合版安装部署](#)

[46.4.2. PUBWIN2007+易游有盘整合版安装部署](#)

[46.4.3. 顺网无盘安装部署](#)

[46.4.4. 易游无盘安装部署](#)

[46.4.5. 信佑无盘安装部署](#)

[47. 第四代流控](#)

[48. ipgeodbs \(IP地理位置数据库\) 模块](#)

[49. npnp 即插即用服务](#)

[IX. 解决方案](#)

[50. 企业三层交换网络解决方案](#)

[50.1. 路由上不划分VLAN](#)

[50.1.1. 路由器设置](#)

[50.1.2. 三层交换机设置](#)

[50.1.3. 常见问题及解答](#)

[51. 单WAN口通过交换机扩展接入多线路解决方案](#)

[51.1. 单WAN口通过交换机扩展接入多ADSL解决方案](#)

[51.1.1. 网络拓扑结构](#)

[51.1.2. 三层交换机上的配置](#)

[51.1.3. 路由上的配置](#)

[51.1.4. 采用支持VLAN的二层交换机](#)

[51.2. 单WAN口通过交换机扩展多个固定IP解决方案](#)

[51.2.1. 单WAN口通过交换机扩展接入同一ISP的多个固定IP](#)

[51.2.2. 单WAN口通过交换机扩展接入不同ISP的多个固定IP](#)

[52. 关于光纤接入的几种解决方案](#)

[52.1. 光纤接入绑定多个固定IP地址解决方案](#)

[52.1.1. 网络拓扑图](#)

[52.1.2. 路由器上的设置](#)

[52.2. 光纤接入绑定多个PPPoE账号解决方案](#)

[52.2.1. 网络拓扑图](#)

[52.2.2. 交换机设置](#)

[52.2.3. 路由器设置](#)

[53. 光纤接入无需交换机扩展多线路解决方案](#)

[53.1. 光纤接入绑定多个固定IP无交换机扩展解决方案](#)

[53.1.1. 网络拓扑图](#)

[53.1.2. 路由器上的设置](#)

[53.2. 光纤接入绑定多个PPPoE账号无交换机扩展解决方案](#)

[53.2.1. 网络拓扑图](#)

[53.2.2. 路由器设置](#)

[54. PPPoE认证+web认证+验证码的三重安全认证方案](#)

[54.1. PPPoE服务器模式简介](#)

[54.1.1. 三重安全认证的优点](#)

[54.1.2. 网络拓扑图](#)

[54.2. PPPoE拨号的设置](#)

[54.3. Web认证设置和验证码](#)

[55. 路由无线局域网解决方案](#)

[55.1. 路由无线局域网模式简介](#)

[55.2. 建立内网网段](#)

[55.3. 内网利用 PPPoE 服务上网](#)

[55.4. 内网利用 Web 认证上网](#)

[56. 主机电脑和手机平板设备分别认证解决方案](#)

[X. 常见问题](#)

[57. 路由不能上网相关初步分析思路图](#)

[58. 网络慢卡的初步分析排查思路图](#)

[59. 关于重新绑定网卡](#)

[59.1. LAN口之间重新绑定](#)

[59.2. LAN接口与WAN接口之间重新绑定](#)

[60. 关于CPU中断](#)

[60.1. 中断简介](#)

[60.2. 影响CPU中断频率的因素](#)

[61. 特征库升级不成功](#)

[62. 路由上突然很多功能都失效](#)

[63. 即时通讯监控里看不到qq号或qq不能被禁止登录](#)

[64. 怎样查看路由上过去的日志](#)

[65. 变路由为透明网桥后可用哪些功能](#)

[66. 路由自动重启或关机的原因](#)

[67. 路由上的优先级顺序](#)

[68. 网卡突然全部启动不了，控制台无IP信息](#)

[69. 客户机PPTPVPN拨号成功后无法访问对端内网](#)

[70. DNS检测失败的原因](#)

[71. 内网主机ping网址不通或掉包的原因](#)

[72. 内网用户限速不了](#)

[73. 某个网页打不开或出错](#)

[74. 网卡不能正常工作相关问题](#)

[75. 网页打开非常慢或者基本都打不开](#)

[76. 磁盘错误引起的问题](#)

[77. 内网主机无法上网，并且路由上ping不通网关](#)

[78. WAN口LAN口流量不对称](#)

[79. 内网ARP攻击检测与防护](#)





部分 I. 系统介绍

目录

[1. 系统介绍](#)

[1.1. 产品概述](#)

[1.2. 功能介绍](#)

[1.3. 技术特性](#)





第 1 章 系统介绍

目录

- [1.1. 产品概述](#)
- [1.2. 功能介绍](#)
- [1.3. 技术特性](#)

海蜘蛛路由系统（Hi-Spider Router）是一套运行于 x86-CPU 硬件架构（即普通PC机）上的路由系统。基于稳定的 GNU/Linux 2.6 系列内核开发。

1.1. 产品概述

秉承丰富的网络软件研发经验，海蜘蛛网络科技推出了稳定、高效、功能丰富的软路由系统——海蜘蛛路由系统（Hi-Spider Router）。该路由采用模块化的结构设计，结合行之有效的软件技术实现了快速、高效的路由策略，是企业、家庭、社区或网吧等场所的首选产品。

海蜘蛛网络科技针对中国互联网的特点，根据终端接入路由器的功能需要，设计和构建了一套专用 Linux 系统，并以此系统为基石，以用户需求为导向，逐步开发了路由系统的各个通用模块，以及针对有中国特色的网络环境所设计的一系列专用模块。整个系统模块化程度高，灵活性和可扩展性强，体积精减、运行效率高、安全性好、稳定性佳，并具有良好硬件兼容性。





1.2. 功能介绍

系统功能介绍

路由功能	防火墙功能	流量控制	VPN功能	上网管理功能
ADSL/DHCP 光纤接入	ICMP/SYN/UDP 攻击防御	上传/下载限速	PPTP VPN 服务	基于对象的管理 (IP/时间/端口/协议)
静态路由	UDP Flood/IP 碎片防御	共享或单机限速	SSL VPN 服务	对象分组管理
动态域名解析	DNS/域名/IP 过滤	源/目的IP 限速	L2TP VPN 服务	协议特征过滤
多线策略路由	网址 URL/关键字过滤	源/目的端口限速	PPTP/L2TP VPN 借线 (实现虚拟多线)	PPPoE 服务器
多线路负载均衡	防火墙黑白名单	按时段限速	SSL VPN 网间互联 (LAN-to-LAN)	PPPoE RADIUS 认证 (自定义同时拨入数)
带宽叠加	一对一 NAT	小包优先转发	IPsec VPN	上网 Web 认证
IP/端口分流	UpnP 即插即用	QoS 规则	VPN RADIUS 认证	上网期限管理
双 LAN 口支持	端口映射	P2P 下载/上传控制		上网到期提前通知
单网卡绑定 IP 地址	IP 与 MAC 绑定	PPTP VPN 限速		上网到期断网
单 WAN 绑定多 ADSL	DMZ 主机	SSL VPN 限速		定时发送网页通知
802.1Q VLAN 支持	反端口扫描	PPPoE 限速		禁止客户机使用二级路由上网
端口镜像/流量复制	攻击动态拦截			
自定义 LAN/WAN 口	ARP 攻击检测			
路由表在线更新	DNS 重定向			
DNS 缓存加速	反 DNS 劫持			
DHCP 功能	恶意网址过滤			
透明网桥				
短信网关				
路由冗余备份				
PXE 无盘服务				

表 1.1. 系统功能介绍

附加功能介绍

网络诊断工具	信息监测	系统日志	其他应用
PING 工具	系统运行状态	内网DNS查询日志（统计分析）	网络打印
路由跟踪工具	硬件信息	网卡流量统计分析（分钟/小时/年）	定时重启/关机/关机重开
子网计算工具	网络状态/负载信息	SYSLOG日志转发	远程唤醒
WHOIS IP 查询	PPP连接信息	用户上网访问日志	同吧QQ在线
IP属地查询	内网扫描信息	防火墙攻击日志	系统自动升级
域名诊断查询	NAT 会话信息	内核日志	恶意网址自动升级
MAC地址查询	内网流量实时监测		路由表自动升级
系统综合诊断	网卡实时流量图		协议特征自动升级
在线抓包分析	网卡历史流量图		

表 1.2. 附加功能介绍



1.3. 技术特性

- 支持光纤（静态/动态IP地址）、ADSL/PPPoE 等多种接入方式
- 支持静态路由、智能动态路由
- 支持策略路由、带宽叠加、多线路负载均衡
- 支持路由冗余备份
- 支持 SSL/PPTP/L2TP/IPsec VPN、支持 IPsec/GRE 隧道
- 支持 VLAN 网络环境
- 支持快速转发（小包优先），吞吐量最高可达 200Mbps，最多 210Kpps
- 支持流量控制与 QoS（包括客户端）
- 支持 UPnP、端口回流、DMZ 主机
- 支持局域网 PPPoE 服务器、RADIUS 认证
- 支持一个网卡绑定多个 IP 地址
- 支持每个外网网卡拨多个 ADSL 帐号
- 支持每个外网网卡绑定一个动态域名
- 支持 DHCP 服务
- 支持 PXE 无盘安装与启动
- 支持基于 IP 地址/网段、协议和端口的数据包过滤
- 支持基于站点、URL、关键字等应用层过滤
- 支持网络时间同步
- 支持 IP 和 MAC 绑定
- 支持 DNS 代理/缓存
- 支持动态域名解析





部分 II. 系统设置

目录

[2. 海蜘蛛路由首页](#)

[3. 系统设置](#)

- [3.1. 基本设置](#)
- [3.2. WEB 远程管理](#)
- [3.3. 控制台登录](#)
- [3.4. 报警设置](#)
- [3.5. 邮件设置](#)
- [3.6. 定时关机 & 重启](#)
- [3.7. 网卡驱动模块](#)
- [3.8. 启动菜单配置](#)
- [3.9. 磁盘分区管理](#)
- [3.10. 保存 & 重启](#)
- [3.11. 远程唤醒 \(WOL\)](#)



1.3. 技术特性



第 2 章 海蜘蛛路由首页



第 2 章 海蜘蛛路由首页

单击海蜘蛛路由左上方logo图标即可进入海蜘蛛路由首页界面。

以下图片显示的是各个接口的物理状态，如图：



图 2.1. 各接口状态

右边类似于冰糖葫芦的指示灯可以根据显示颜色来判断线路状况：

- 绿色表示线路畅通。
- 黄色表示线路不通，出现此种情况需检查WAN口设置。
- 粉红色表示没有开启线路检测。

提示

当启动多线路负载时才会出现指示灯，否则只显示此图标： 点击此图标即可查看对应网卡的流量图

接着显示的是系统状态：

主机名:	xywxedu.com
系统版本:	V8.0 Build20130319 (发布于 2013-03-19 09:52:51)
内核版本:	2.6.32.15 [多核] (编译于 2012-10-26 09:20:05)
运行时间:	29 分 22 秒 (启动于 2013-03-20 14:14:25)
会话数:	40, 在线用户: 2, 活动用户: 2, PPP用户: 2
平均负载:	1分钟前: 0.07, 5分钟前: 0.02, 15分钟前: 0.00
进程状态:	活动: 1, 睡眠: 111, 停止: 0, 僵死: 0

图 2.2. 系统状态

主机名是安装路由系统的计算机名称，系统版本是当前路由系统的版本号，内核版本包括当前系统内核的版本号和启动内核的种类，在线用户数是指用户在线半小时以上的主机数，活动用户指经过路由上网有流量的主机数，PPP用户指以PPPoE拨号方式连接到路由的主机数。当前Web登陆到路由的计算机数量，平均负载一般都为0.OX，下面的停止数和僵死数正常时都为0。

再下面是CPU的负载状态，此为双核CPU的运行情况：

CPU	用户	系统	IO等待	硬中断	软中断	中断频率	已使用	空闲
CPU-0	7.20%	1.40%	0.00%	0.00%	0.00%	27.00/s	8.60%	91.40%
CPU-1	2.32%	1.26%	0.00%	0.21%	0.00%	19.20/s	3.79%	96.21%
平均	4.82%	1.33%	0.00%	0.10%	0.00%	139.80/s	6.26%	93.74%

图 2.3. CPU 状态

最下面是内存的使用情况：

内存类型	使用百分比	%	已使用	剩余大小	总容量
物理内存	<div></div>	8.7%	179.89 MB	1893.59 MB	2073.48 MB
+ - 内核 + 应用程序	<div></div>	4.1%	83.52 MB		
+ - 缓冲	<div></div>	0.0%	0.20 MB		
+ - 缓存	<div></div>	4.6%	96.17 MB		

图 2.4. 内存状态



第 3 章 系统设置

目录

- [3.1. 基本设置](#)
- [3.2. WEB 远程管理](#)
- [3.3. 控制台登录](#)
- [3.4. 报警设置](#)
- [3.5. 邮件设置](#)
- [3.6. 定时关机 & 重启](#)
- [3.7. 网卡驱动模块](#)
- [3.8. 启动菜单配置](#)
- [3.9. 磁盘分区管理](#)
- [3.10. 保存 & 重启](#)
- [3.11. 远程唤醒 \(WOL\)](#)

3.1. 基本设置

基本设置分为系统全局参数设置和其他设置两部分。系统全局参数主要是设置系统界面语言、主机名、时区、时间等；其他设置主要设置用户备注信息、更新消息首页提醒和分页时每页显示的记录条数等。

界面语言：分为简体中文和英语，可根据自身习惯选择，选择后点击“保存设置”即可生效。

主机名：就是给路由系统取一个名字，只能由字母、数字、下划线、圆点及减号组成。

选择时区：根据所在的地区选择，如你所在的地区是马来西亚，则选择“（北京时间+08:00）北京、佩思、新加坡、香港、马来西亚”。

时间服务器：点击“校准”，系统会自动连接到时间服务器同步时间，常用时间服务器有 `time.nist.gov` `clock.via.net` `rdate.darkorb.net`。



注意

系统每隔24小时会自动校准时间。

系统全局参数...	
界面语言:	Simplified Chinese (简体中文) ▼
主机名:	hzz . example.com (只能由字母、数字、下划线、圆点及减号组成)
系统时区:	(北京时间+08:00) 北京、佩思、新加坡、香港、马来西亚 ▼
当前系统时间:	2010年03月24日 下午 15:59:07 星期三
客户机时间:	2010年03月24日 下午 15:58:58 星期三
设置日期:	2010 年 3 月 24 日
设置时间:	15 时 55 分 48 秒 修改
时间服务器:	rdate.darkorb.net 校准 同步日志

图 3.1. 全局参数设置

用户备注：此信息显示在浏览器标题中，可以随意设置。

是否在首页显示最新消息：勾选此项后，软件有更新，会在最新消息中显示，一般建议勾选。

分页时每页显示的记录条数：默认为12，用户可根据个人习惯来设置，范围为：8~30。

重定向上网首页，用于将内网用户主页统一，请根据需要自定义。

用户备注:	hispider (显示在浏览器标题中)
首页显示最新消息:	<input checked="" type="checkbox"/> 是 (如果软件有更新, 会在最新消息中显示) 更新
分页时每页显示的记录条数:	12 (8~100)
启用流量监测图形统计:	<input checked="" type="checkbox"/> 是 (统计当前和历史的网卡流量信息并以图形方式输出)
重定向客户上网首页:	<input type="checkbox"/> 是, 浏览网页空闲时间 60 s 重定向到 http://www.hao123.com (http://xx.yy.com)
内网流量监测最多显示的IP个数:	20 (10~1000)
NAT 会话最多显示的IP个数:	100 (10~1000)
NAT 会话中是否显示外网IP:	<input type="checkbox"/> 是

图 3.2. 其它设置

路由极速模式用于加快内网NAT转发：

启用路由转发极速模式：☒ 是, 生效时间段： (格式: HH:MM-HH:MM, 如 19:00-23:00)

保存设置

重置

图 3.3. 路由极速模式

这里表示每天的**10:00-17:00**启用极速模式。



警告

启用极速模式后上网日志、即时通讯监控、上网到期通知、各种提醒等、流量统计图、强制进行 IP/MAC 地址绑定、恶意网址拦截功能、网址过滤、强制用户通过PPPoE拨号上网、WEB认证、端口镜像等暂时失效！





3.2. WEB 远程管理

页面分为登录帐号、端口设置和安全策略三个窗口。

这里可以设置通过 **Web** 登录系统时的密码、端口、安全连接等，系统默认禁止从广域网登录，如需开启，请先修改管理员密码。

登录账号：分为管理员帐号、普通帐号和自定义账号。管理员帐号可以修改任何设置；普通帐号可以查看所有项目配置，不能修改；自定义账号可以自定义修改的项目配置权限。

在 登录账号 页面中，点击“登录账号管理”。

登录帐号	端口设置	安全策略
管理员帐号:	<input type="text" value="admin"/> (只能由字母、数字、下划线、圆点及减号组成)	
旧密码:	<input type="password"/> (密码长度 4-20 位, 建议使用8位以上密码)	
新密码:	<input type="password"/> (为空表示不修改)	
密码确认:	<input type="password"/>	
是否启用验证码:	<input type="checkbox"/> 启用	
<div>保存设置 重置 登录帐号管理</div>		

图 3.4. 登录帐号管理

点击“新增”，选择“自定义”，输入用户名test和密码，勾选“计划任务”，保存设置后就建立了一个自定义账号。

用户名:	<input type="text" value="test"/>
	<div>自定义</div>
	<div>系统设置</div>
	<div><input type="checkbox"/> 基本设置</div>
	<div><input type="checkbox"/> Web 远程管理</div>
	<div><input type="checkbox"/> 控制台登录</div>
	<div><input type="checkbox"/> 报警设置</div>
	<div><input checked="" type="checkbox"/> 计划任务</div>

图 3.5. 建立自定义账号

现在注销当前账户，用test账号登陆，就只能管理计划任务功能。



图 3.6. test账号登陆

系统设置

计划任务

计划任务

设置让系统在指定时间或按指定的计划执行任务，比如重启或关闭系统，当系统的经过长时间的工作后，建议重启使硬件(如网卡)进行复

定时重启...

启用定时重启功能:	<input checked="" type="checkbox"/> 是	2010-08-18 12:10 执行重启操作
定时任务执行方式:	一次性	
执行日期:	2010-08-18	
执行时间:	12:10	
星期:	<input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input type="checkbox"/> 工作日 <input type="checkbox"/> 全部	


定时关机...

启用定时关机功能:	<input type="checkbox"/> 是	
定时任务执行方式:	每天	
执行日期:		
执行时间:		
星期:	<input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input type="checkbox"/> 工作日 <input type="checkbox"/> 全部	
定时重新开机:	<input type="checkbox"/> 启用, 开机方式: <input checked="" type="radio"/> 延时等待: 0 小时 0 分钟 <input type="radio"/> 指定时间: <input type="text"/>	

保存设置 重置

端口设置：分为 WEB 管理端口、是否启用 SSL 连接加密和强制使用 SSL 连接加密。

WEB 管理端口：设置WEB 远程登录时的端口号，默认为 880，更改范围为：1~65535。修改之后，建议使用“端口测试”，看端口是否处于空闲状态，是否可用。

 注意

端口修改失败时，系统将在 15 秒内恢复管理端口到默认设置。

是否启用 SSL 连接加密：启用后，SSL 连接使用 443 端口。访问系统 Web 管理的 URL 地址为：<https://<IP 地址>端口号443>

强制使用 SSL 连接加密：适用于对安全性要求较高的场合，一般不用勾选。

登录帐号	端口设置	安全策略
WEB 管理端口： <input type="text" value="880"/> (范围: 1-65535) 运行中 (PID: 1846)		
是否启用 SSL 连接加密： <input checked="" type="checkbox"/> 启用 (SSL 连接使用 443 端口)		
强制使用 SSL 连接加密： <input type="checkbox"/> 启用 (适用于对安全性要求较高的场合)		

图 3.7. 端口设置

安全策略：设置是否允许外网 IP 访问 Web 远程管理，默认设置是禁止所有外网 IP 访问。

如果选择“只允许指定 IP 从外网登录执行远程管理（自定义）”，则需要在右边列表中添加允许远程管理的 IP 列表，每个 IP 地址或网段占一行。

登录帐号	端口设置	安全策略
<div>允许远程管理的IP列表, 每个IP地址或网段占一行</div> <div><input type="radio"/> 禁止所有外网IP访问 Web 远程管理 (默认)</div> <div><input type="radio"/> 允许所有外网IP访问 Web 远程管理</div> <div><input checked="" type="radio"/> 只允许指定IP从外网登录执行远程管理 (自定义)</div> <div><div>11. 22. 33. 44</div></div>		

图 3.8. 安全策略



3.3. 控制台登录

当您忘记 Web 管理密码或由于其他因素导致无法通过 Web 方式登录系统时，您还可以在本地控制台登录或通过串口连接进行一些应急性操作，比如修改 Web 登录密码、局域网接口IP地址等。

控制台登录用户名为 root，初始密码为 123456，建议修改为更复杂的密码。



注意

在路由上勾选允许通过串口登录。进入windows系统的超级终端：串口登录时选择 COM1 口，数据Bit为8，奇偶校验无，停止Bit为1，流量控制为无，每秒位数要和系统设置的数据传输波特率一致。

为了安全考虑，root 用户只允许通过控制台登录。

允许按 Ctrl-Alt-Del 组合键重启：勾选后，点击“保存设置”，无需登录，Ctrl-Alt-Del 即可快速重启系统。

请输入新密码：	<input type="password" value="•••••"/>	(密码长度 4-20 位, 建议使用8位以上密码)
允许通过串口登录：	<input checked="" type="checkbox"/> 是，数据传输波特率：	<input type="text" value="38400"/> 工作正常
允许按 Ctrl-Alt-Del 组合键重启：	<input checked="" type="checkbox"/> 是	(无需登录快速重启系统)
控制台登录时需要密码：	<input checked="" type="checkbox"/> 是	

图 3.9. 控制台登录

利用windows系统的超级终端串口登陆系统过程：

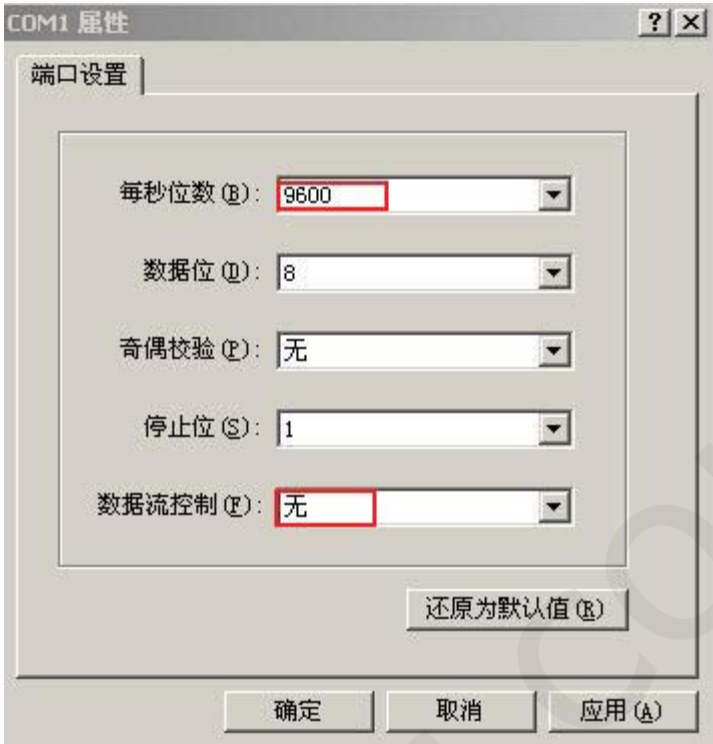
1. 串口登录海蜘蛛

- 连线：将海蜘蛛系统的串口与任一计算机的串口连接(在海蜘蛛系统和与其连接的PC上同时开启 允许串口通信)
- 开始->程序->附件->通讯->超级终端，打开终端连接图标，如下图所示：




连接名称任意





按回车键后输入用户名和密码：





注意

为了安全起见，此处密码不可见

输入用户名和密码后进入控制界面，如下图：

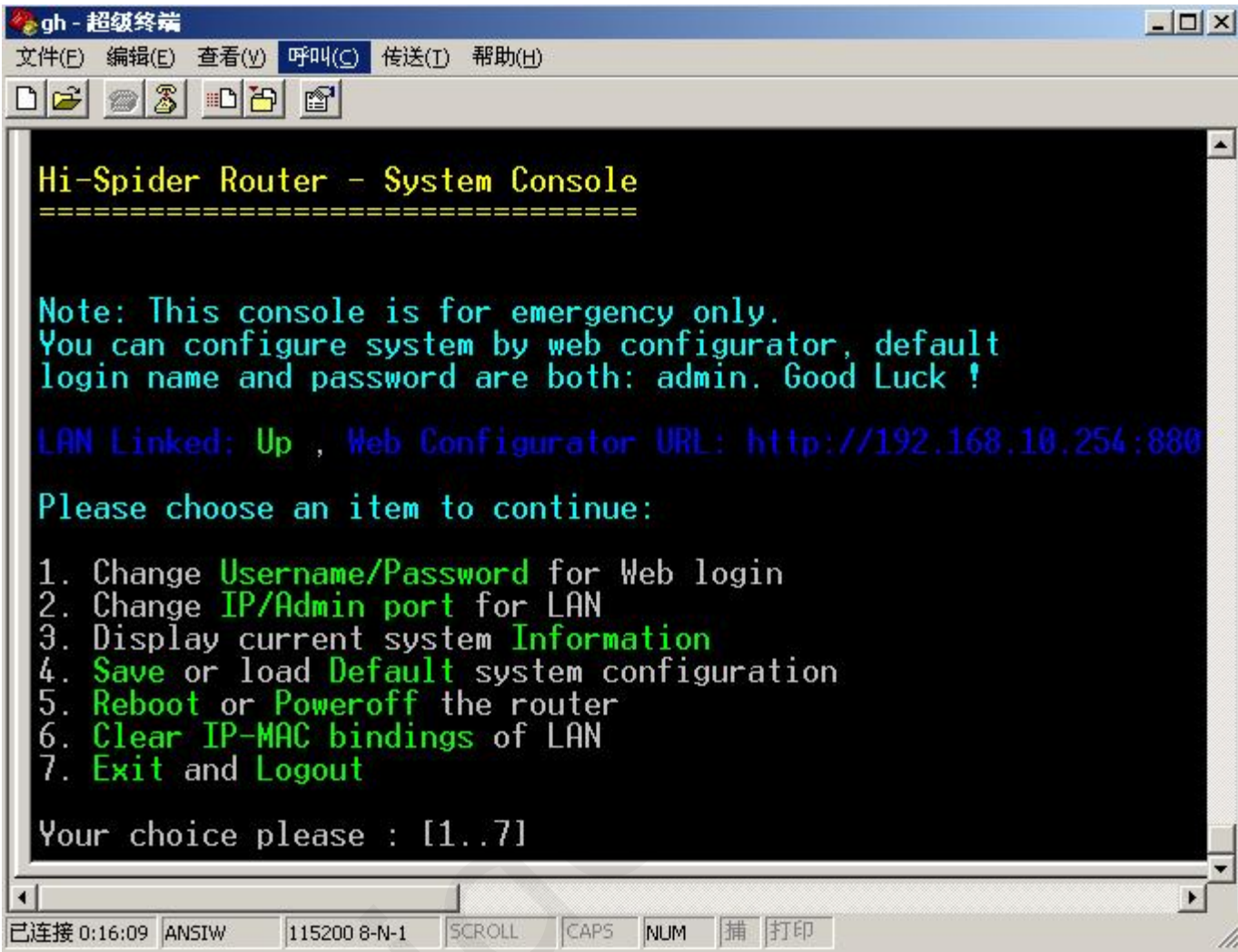


图 3.10. 控制台登录界面

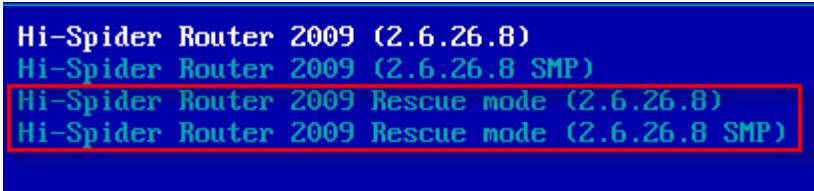
2. 常见问题及解决方法

- 如何防止其他用户登录控制台修改WEB管理密码？

进入海蜘蛛web管理页面->“系统设置”->“控制台登陆”，开启“控制台登陆时需要密码”并设置更为复杂的密码，这样就避免了任何人都可以进入畅通无阻的进入控制台并修改web管理密码。

- 控制台登录时需要密码，但密码忘记了，该怎么办？

在启动海蜘蛛系统进入以下画面时用光标选择救援模式即可恢复为控制台默认登陆密码：



提示

rescue表示救援，smp表示多核

这里第三行为单核救援模式，第四行为多核救援模式



3.2. WEB 远程管理



3.4. 报警设置

Hi-Spider.com



3.4. 报警设置

报警设置主要采用声音/蜂鸣器报警。

当检测到或受到攻击、运行负载过大或异常、磁盘出现故障等情况时，系统可以通过自我报警的方式表现出来，有助于管理人员及时发现并处理相关问题。

通过主板上的蜂鸣器（PC Speaker）来发出指定频率的声音，声音格式为一长一短，声音频率范围为 50Hz ~ 5000Hz。

关闭声音报警：关闭后系统检测到攻击或异常时将不会报警。

关闭系统启动完成声音提示：当系统启动完成时，您将会听到两次3短1长1短的鸣笛声（滴滴滴-滴---滴），关闭后系统启动完成后将不会发出声音提示。

声音/蜂鸣器报警...

通过主板上的蜂鸣器 (PC Speaker) 来发出指定频率的声音, 声音格式为一长一短. 声音频率范围为 50Hz ~ 5000Hz.

PC Speaker 硬件状态:	工作正常	
高音频率:	<input type="text" value="800"/>	Hz (默认为 800)
低音频率:	<input type="text" value="300"/>	Hz (默认为 300)
重复次数:	<input type="text" value="3"/>	(范围: 1~10, 默认为 3 次) 声音测试
关闭声音报警:	<input type="checkbox"/> (关闭后系统检测到攻击或异常时将不会报警)	
关闭系统启动完成声音提示:	<input type="checkbox"/> (关闭后系统启动完成时将不会发出声音提示)	

图 3.11. 报警设置





3.5. 邮件设置



提示
此功能为20120815以后版本支持

配置路由上发送邮件地址，这里支持各种常见的邮箱地址。具体各邮件配置如下图：

电子邮件通知...	
发信人邮箱帐户:	<input type="text" value="hispider_test@163.com"/> (test@example.com)
发信人登录验证名:	<input type="text" value="hispider_test"/> (一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)
发信人名字(姓名):	<input type="text" value="test"/>
发信人邮箱密码:	<input type="password" value="....."/>
SMTP 服务器地址:	<input type="text" value="smtp.163.com"/>
收信人E-mail地址(仅测试时需填写):	<input type="text" value="1554217016@qq.com"/> <input type="button" value="测试邮件"/>

图 3.12. 163 邮箱

电子邮件通知...	
发信人邮箱帐户:	<input type="text" value="hispider_test@126.com"/> (test@example.com)
发信人登录验证名:	<input type="text" value="hispider_test"/> (一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)
发信人名字(姓名):	<input type="text" value="test"/>
发信人邮箱密码:	<input type="password" value="....."/>
SMTP 服务器地址:	<input type="text" value="smtp.126.com"/>
收信人E-mail地址(仅测试时需填写):	<input type="text" value="1554217016@qq.com"/> <input type="button" value="测试邮件"/>

图 3.13. 126 邮箱

电子邮件通知...	
发信人邮箱帐户:	hispidr_test@sina.com (test@example.com)
发信人登录验证名:	hispidr_test (一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)
发信人名字(姓名):	test
发信人邮箱密码:
SMTP 服务器地址:	mail.sina.com
收信人E-mail地址(仅测试时需填写):	1554217016@qq.com 测试邮件

图 3.14. sina邮箱

电子邮件通知...	
发信人邮箱帐户:	hispidr_test@yahoo.com.cn (test@example.com)
发信人登录验证名:	hispidr_test (一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)
发信人名字(姓名):	test
发信人邮箱密码:
SMTP 服务器地址:	smtp.mail.yahoo.com.cn
收信人E-mail地址(仅测试时需填写):	1554217016@qq.com 测试邮件

图 3.15. yahoo邮箱

电子邮件通知...	
发信人邮箱帐户:	hispidr_test@sohu.com (test@example.com)
发信人登录验证名:	hispidr_test (一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)
发信人名字(姓名):	test
发信人邮箱密码:
SMTP 服务器地址:	mail.sohu.com
收信人E-mail地址(仅测试时需填写):	1554217016@qq.com 测试邮件

图 3.16. sohu邮箱

电子邮件通知...

发信人邮箱帐户:	<input type="text" value="1554217016@qq.com"/>	(test@example.com)
发信人登录验证名:	<input type="text" value="1554217016"/>	(一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)	
发信人名字(姓名):	<input type="text" value="test"/>	
发信人邮箱密码:	<input type="password" value="....."/>	
SMTP 服务器地址:	<input type="text" value="smtp.qq.com"/>	
收信人E-mail地址(仅测试时需填写):	<input type="text"/>	<input type="button" value="测试邮件"/>

图 3.17. qq邮箱

电子邮件通知...

发信人邮箱帐户:	<input type="text" value="hispidertest@gmail.com"/>	(test@example.com)
发信人登录验证名:	<input type="text" value="hispidertest"/>	(一般为帐户 @ 前面的部分, 有的为邮箱地址)
登录时启用 TLS 连接:	<input checked="" type="checkbox"/> (根据邮件系统而定, 如 Gmail 要求 TLS 连接)	
发信人名字(姓名):	<input type="text" value="test"/>	
发信人邮箱密码:	<input type="password" value="....."/>	
SMTP 服务器地址:	<input type="text" value="smtp.gmail.com"/>	
收信人E-mail地址(仅测试时需填写):	<input type="text"/>	<input type="button" value="测试邮件"/>


图 3.18. gmail邮箱

 重要

配置时需要确定各发送邮箱开启SMTP服务

正确配置后测试发送，可以在收件箱里看到如下信息：

邮件发送测试 ☆

发件人：**test** <root@hsrouter.example.com> 

(由 hispider_test@163.com 代发) ?

时 间：2012年8月16日(星期四) 上午9:21

收件人：**1554217016** <1554217016@qq.com>

恭喜您！您能看到这封邮件，表明邮件通知的相关设置一切正常！

图 3.19. 邮件测试

Hi-Spider.com



3.6. 定时关机 & 重启

设置让系统在指定时间或按指定的计划方式重新启动或关闭。当系统的经过长时间的工作后，建议重启使硬件(如网卡)进行复位。

• 定时重启


定时任务执行方式：有每天、每星期、每月、一次性四种方式。

执行方式设置为每天，设置执行时间，则每天该时间系统自动重启。

执行方式设置为每星期，则在星期栏中勾选相应的重启的星期数，再设置执行时间，点击“保存设置”即可在设置的时间自动重启。

执行方式设置为每月，选择执行日期和执行时间，系统则会在每月该日期的该时间自动重启。

执行方式设置为一次性，设置执行日期和执行时间，点击“保存设置”后，系统则会在设定的时间自动重启一次。



注意

点击时间选择图标右边的删除图标，可以清除所设定的时间或日期。

下图以每星期任务执行方式为例，设置每星期的工作日（周一至周五）早上 08:00 重启。






定时重启 ...	
启用定时重启功能:	<input checked="" type="checkbox"/> 是
定时任务执行方式:	每星期
执行日期:	  2009-05-01
执行时间:	  08:00
星期:	<input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input checked="" type="checkbox"/> 工作日 <input type="checkbox"/> 全部

图 3.20. 定时重启

• 定时关机

勾选启用定时关机功能，选择定时任务执行方式（每天、每星期、每月、一次性），选择相应设置即可，设置方式和定时重启类似。

定时重新开机：是指在关机后，等待一段时间再开机。



注意

在等待时间段内，出现停电或者断电现象，此设置就会失效。

下图以每天任务执行方式为例，设置每天关机时间为 18:10 ，重新开机时间为 08:00 。

启用定时关机功能:	<input checked="" type="checkbox"/> 是
定时任务执行方式:	每天 <input type="button" value="v"/>
执行日期:	<input type="button" value="日历"/> <input checked="" type="button" value="X"/> 2012-08-27
执行时间:	<input type="button" value="日历"/> <input checked="" type="button" value="X"/> 18:10
星期:	<input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input type="checkbox"/> 工作日 <input type="checkbox"/> 全部
定时重新开机:	<input checked="" type="checkbox"/> 启用， 开机方式: <input checked="" type="radio"/> 延时等待: <input type="text" value="13"/> 小时 <input type="text" value="50"/> 分钟 <input type="radio"/> 指定时间: <input type="button" value="日历"/> <input checked="" type="button" value="X"/> <input type="text"/>

图 3.21. 定时关机



3.5. 邮件设置



3.7. 网卡驱动模块



3.7. 网卡驱动模块

为了提高内核运行效率，网卡驱动以模块方式加载，默认情况下系统启动时会自动探测网卡型号并加载相应的驱动模块，如果少数网卡没有驱动成功，您可以手动指定此网卡的模块名。

只有当网卡没有驱动时才需要手动指定模块，一般不需要。

需要额外加载的网卡驱动模块列表（每个模块名占一行，以 # 开头的为注释行）。此模块名称需根据您的网卡型号来查询。

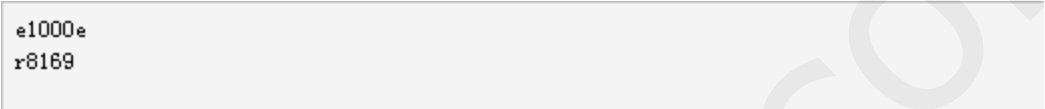


图 3.22. 网卡驱动模块

点击“保存设置”即可。





3.8. 启动菜单配置

设置启动菜单相关配置，比如默认启动的选项等。

默认要启动的内核：单核（Uniprocessor）和多核（SMP）。单核 CPU 用单核内核，多核 CPU 用多核内核。

启动菜单等待时间：单位是秒，设置为多长时间后自动启动默认菜单。

内核参数：禁止 USB、禁止 APIC、禁止本地 APIC。禁止 USB 是禁用内核的USB驱动，就相当于禁止了USB接口；禁止 APIC 是指禁用 APIC（高级可编程中断控制器）功能，这个一般不禁用，有助于解决网卡中断冲突问题；勾选内核禁用本地APIC后，即使 BIOS 设置里已经启用了，在这里也可以禁用掉。

对于下面的PCI模式和禁止SMP自动IRQ负载均衡仅用于特殊场合，一般不做修改



注意

修改“保存设置”后，需重启路由系统才能生效。

默认要启动的内核：	<div><input type="radio"/> i386 (适用于工控机/嵌入式系统/老式主板或CPU)</div> <div><input type="radio"/> 单核 (适用于大多数硬件场合)</div> <div><input checked="" type="radio"/> 多核 (适用于双核等多CPU场合)</div>
启动菜单等待时间：	<div><input type="text" value="1"/> s (多长时间后自动启动默认菜单)</div>
内核参数 (请勿随意修改)：	<div><input type="checkbox"/> 禁止USB</div> <div><input type="checkbox"/> 禁止APIC</div> <div><input type="checkbox"/> 禁止本地APIC</div> <div><input type="checkbox"/> 禁止HPET</div> <div><input type="checkbox"/> 禁止Intel_IOMMU</div> <div><input type="checkbox"/> 内核崩溃自动重启</div> <div><input type="checkbox"/> 禁止hda上的DMA</div> <div><input type="checkbox"/> 禁止hdb上的DMA</div> <div><input type="checkbox"/> 禁止hdc上的DMA</div> <div><input type="checkbox"/> 禁止hdd上的DMA</div> <div><input type="checkbox"/> 关闭超线程</div>
PCI 模式 (请勿随意修改)：	<div>自动 (默认) <input type="button" value="v"/></div>
禁止SMP自动IRQ负载均衡：	<div><input type="checkbox"/> 是 (一般不建议勾选)</div>

图 3.23. 启动参数配置



3.7. 网卡驱动模块



3.9. 磁盘分区管理

Hi-Spider.com



3.9. 磁盘分区管理

如果路由上安装了多块磁盘，或者单个磁盘空间有剩余。可以创建分区用来存储日志或做FTP服务等。

进入“系统设置”->“磁盘分区管理”，打开主界面：

磁盘分区管理

管理连接到系统的磁盘，对磁盘进行分区、格式化、挂载及卸载等操作。

sda - WDC WD5000AADS-0 [500.1 GB]

分区	大小	文件系统	使用率	已使用	剩余	挂载点	自动挂载	启用	HTTP 映射	映射目录	动作
/dev/sda1	100.0 GB	reiserfs	3%	2.6G	90.5G	/data/vm	✓	✗			卸载
/dev/sda2	300.0 GB	reiserfs	0%	32.4M	279.3G	/data/sda2.4937	✓	✓	✓	sda2.4937	卸载
/dev/sda3	100.1 GB	reiserfs	4%	3.7G	89.6G	/data/sda3	✓	✓	✓	sda3	卸载

* sdb - Fordisk SATA DOM [4.0 GB]

分区	大小	文件系统	使用率	已使用	剩余	挂载点	自动挂载	启用	HTTP 映射	映射目录	动作
/dev/sdb1	1.0 GB	reiserfs				系统分区	-	-	-		-
Free	2.9 GB										创建分区

图 3.24. 磁盘分区管理

点击下面的创建分区，填入需要分区的大小，文件系统一般选择Reiserfs，勾选开机自动挂载和启用 HTTP 下载映射，挂载点和映射名称可以任意，保存设置即可：

* sdb - Fordisk SATA DOM [4.0 GB]

分区	大小	文件系统	使用率	已使用	剩余	挂载点	自动挂载	启用	HTTP 映射	映射目录
/dev/sdb1	1.0 GB	reiserfs				系统分区	-	-	-	
Free	2.9 GB									
		大小:	1000 MB (最小512 MB, 0表示所有剩余空间)							
		文件系统:	<input checked="" type="radio"/> ReiserFS <input type="radio"/> XFS <input type="radio"/> Ext3 <input type="radio"/> FAT32 <input type="radio"/> NTFS <input type="radio"/> LVM							
		挂载点:	/data/ abc							
		开机自动挂载:	<input checked="" type="checkbox"/> 是							
		启用 HTTP 下载映射:	<input checked="" type="checkbox"/> 是, 映射名称: cba							
<div>保存设置 重置 取消</div>										

图 3.25. 创建磁盘分区

* sdb - Fordisk SATA DOM [4.0 GB]

分区	大小	文件系统	使用率	已使用	剩余	挂载点	自动挂载	启用	HTTP 映射	映射目录	动作
/dev/sdb1	1.0 GB	reiserfs				系统分区	-	-	-		-
/dev/sdb2	1.0 GB	reiserfs	3%	32.1M	932.7M	/data/abc	✓	✓	✓	cba	卸载
Free	1.9 GB										创建/删除分区前需卸载已挂载分区

图 3.26. 新分区

这样对于路由存储日志或者FTP等有此路径可以选择保存了

日志保存位置: 磁盘 /dev/sdb2 -- /data/abc

图 3.27. 选取路径



3.10. 保存 & 重启

1. 系统配置管理

由于系统在内存运行，您修改的配置信息也保存在内存中，重启后这些配置将会丢失。这就需要您定期将配置文件备份到磁盘。进入“系统设置”->“保存 & 重启”，在最近修改的文件配置后点击导出到您的计算机。如果您由于误操作或断电导致配置丢失，您可以通过“最近一次正确配置”恢复以前的备份设置，也可以通过上传您备份的配置信息来进行恢复。

单击表格最后面的“导出”按钮即可将当前配置文件导出，使用“浏览”、“上传”按钮即可导入系统配置文件。

ID	文件名	最后修改时间	备注	动作			
1	current	2010-09-01 08:44:26	当前使用的配置 (已写入磁盘, 无须保存)	-	-	🔍	导出
2	lastgood	2010-08-31 17:26:55	最后一次正确的配置	恢复	-	🔍	导出
3	default	0000-00-00 00:00:00	出厂设置	恢复	-	🔍	导出
4	main.conf.20100804150828	2010-08-04 15:03:53		恢复	🗑️	🔍	导出
5	main.conf.20100804112142	2010-08-04 11:17:15		恢复	🗑️	🔍	导出

当前配置另存为: 确定

发送当前配置文件到指定邮箱: 发送

是否自动发送配置文件到邮箱: ☒ 是 (当系统配置修改后自动发送到上述邮箱) 确定

是否自动保存配置到磁盘: ☒ 是 (当系统配置修改后或重启、关机前自动保存到磁盘, 推荐选上) 确定

上传并导入配置: 浏览... 上传

图 3.28. 系统配置管理

使用 当前配置另存为 功能可以将当前配置以不同的名字多次保存，例如这里将当前配置命名为 aa，确定后如下图所示：

ID	文件名	最后修改时间	备注	动作			
1	current	2009-08-26 08:45:35	当前使用的配置 (已写入磁盘, 无须保存)	-	-	🔍	导出
2	lastgood	2009-08-26 08:40:46	最后一次正确的配置	恢复	-	🔍	导出
3	default	0000-00-00 00:00:00	出厂设置	恢复	-	🔍	导出
4	main.conf.20090826090702	2009-08-26 09:07:02	aa	恢复	🗑️	🔍	导出
5	main.conf.20090826084046	2009-08-26 08:40:46	启用VLAN的配置	恢复	🗑️	🔍	导出

图 3.29. 重命名当前配置

您也可以通过 发送当前配置到指定邮箱 将配置保存到任意邮箱中。

当您修改了路由系统任何一处配置时，将会出现以下界面，单击“写入磁盘”即可保存当前配置，如图所示：

ID	文件名	最后修改时间	备注	动作			
1	current	2009-08-26 09:15:45	当前使用的配置 *已修改*	写入磁盘	-	-	🔍 导出

2. 电源管理

点击“重新启动”，可重新启动系统。

点击“关闭电源”，关闭系统，使系统停止工作。



图 3.30. 电源管理

3. 硬盘休眠

系统只在启动或保存设置时需要读取硬盘，大部分时间硬盘都处于空闲状态。为了减少硬盘的损耗或噪音，您可以设定让硬盘空闲时自动休眠。（注：仅对 IDE 硬盘有效，CF卡/DOM电子盘勿用）。启用休眠后，将不会在系统信息里显示硬盘温度。



图 3.31. 硬盘休眠

4. 系统负载监测

您可以设定系统在负载极其严重时（比如 CPU 占用率将近100%，路由接近死机的情况下），通过自动重启来进行自我恢复，而无需手工重启。（注：如果您的网络 DoS/DDoS 攻击比较频繁，建议关闭此选项，以免导致路由经常自动重启）。

负载监测触发条件：1分钟平均负载值 > 5分钟负载 > 15分钟负载。

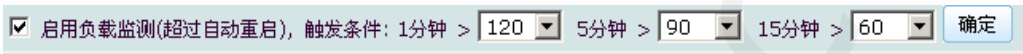


图 3.32. 系统负载监测

5. 断线自动重启

这里指WAN口在开启线路检测的情况下，如下图配置，10分钟内仍然断开就自动重启路由：



图 3.33. 断线自动重启

6. 无人上网自动关机

配置如下图，指从12点到20点这段时间有半小时以上路由上未检测到下面有用户经过路由上网就会自动关闭路由：



图 3.34. 无人上网自动关机

7. 无人上网自动关机后重新开机

这个配置是与上一项配合使用的，如下图所示，关闭后一小时会自动重新启动路由（电源需保持接上），或者手动指定任意开机时间：

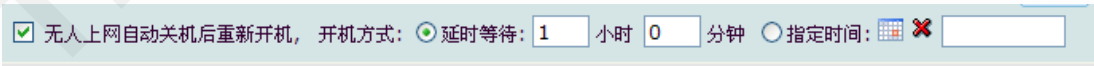


图 3.35. 自动关机后重新开机





3.11. 远程唤醒 (WOL)



小知识

远程唤醒技术 (WOL, Wake-on-LAN) 是由网卡配合其他软硬件, 可以通过局域网实现远程开机的一种技术。通过它我们可以在需要时远程控制计算机的开机, 它非常适合具有远程网络管理要求的环境。

远程唤醒需要网卡、主板、电源的支持和配合才能实现。

在路由主页面下进入“系统工具”->“远程唤醒”页面, 填入远程计算机的网卡 (MAC) 地址 和 远程计算机 IP 地址。

远程计算机的网卡 (MAC) 地址:	<input type="text" value="00-03-56-0c-20-b0"/>
远程计算机 IP 地址:	<input type="text" value="10.0.55.150"/> (可选, 默认为 255.255.255.255) <input type="button" value="唤醒"/>

图 3.36. 远程唤醒

预定义远程唤醒信息, 可以储存远程唤醒的计算机信息。每条记录占一行, 格式: MAC地址 IP地址 可选注释。

预定义远程唤醒信息, 每条记录占一行, 格式: MAC地址 IP地址 可选注释		
00-03-56-0c-20-b0	10.0.55.150	民航
00-09-6b-34-79-c4	192.168.1.3	yi

图 3.37. 预定义远程唤醒





部分 III. 网络设置

目录

[4. 网络设置](#)

[4.1. DNS 参数](#)

[4.2. 动态域名解析](#)

[4.2.1. 配置动态域名解析](#)

[4.2.2. 动态域名解析相关问题](#)

[4.3. 静态路由](#)

[4.4. 多线负载及策略](#)

[4.4.1. 多线路策略简介](#)

[4.4.2. 两条相同网络运营商线路接入](#)

[4.4.3. 两条不同的网络运营商线路接入](#)

[4.4.4. 多条不同网络运营商线路接入](#)

[4.4.5. 两条电信+两条网通+一条铁通](#)

[4.4.6. 多线负载均衡](#)

[4.4.7. 不同ISP实现策略路由](#)

[4.5. 自定义策略](#)

[4.6. 自定义路由表](#)

[4.7. 虚拟局域网\(VLAN\)](#)

[4.7.1. 虚拟局域网简介](#)

[4.7.2. 路由上划分VLAN](#)

[4.8. 透明网桥](#)

[4.8.1. 透明网桥典型实例](#)

[4.8.2. 启用透明网桥](#)

[4.8.3. 透明网桥直接接外网](#)

[5. 快速接入互连网](#)

[5.1. 局域网 \(LAN\) 设置](#)

[5.2. 设置 DNS 参数](#)

[5.3. 设置广域网 \(WAN\)](#)

[6. 3G无线接入设置](#)

[6.1. 3G无线上网简介](#)

[6.2. 参数设置](#)

[6.3. 设置多线负载及策略](#)

[6.4. 支持的3G无线上网卡](#)



3.11. 远程唤醒 (WOL)



第 4 章 网络设置

第 4 章 网络设置

目录

[4.1. DNS 参数](#)[4.2. 动态域名解析](#)[4.2.1. 配置动态域名解析](#)[4.2.2. 动态域名解析相关问题](#)[4.3. 静态路由](#)[4.4. 多线负载及策略](#)[4.4.1. 多线路策略简介](#)[4.4.2. 两条相同网络运营商线路接入](#)[4.4.3. 两条不同的网络运营商线路接入](#)[4.4.4. 多条不同网络运营商线路接入](#)[4.4.5. 两条电信+两条网通+一条铁通](#)[4.4.6. 多线负载均衡](#)[4.4.7. 不同ISP实现策略路由](#)[4.5. 自定义策略](#)[4.6. 自定义路由表](#)[4.7. 虚拟局域网\(VLAN\)](#)[4.7.1. 虚拟局域网简介](#)[4.7.2. 路由上划分VLAN](#)[4.8. 透明网桥](#)[4.8.1. 透明网桥典型实例](#)[4.8.2. 启用透明网桥](#)[4.8.3. 透明网桥直接接外网](#)

4.1. DNS 参数

设置用于域名解析（将域名解析成 IP 地址）的服务器地址。

DNS 获取方式：手动指定或自动获取。

选择“手动指定”，用户需输入运营商提供的“首选DNS”和“辅助DNS”，您还可以填入“可选DNS”服务器地址作为备用，以便在网络运营商提供的 DNS 服务器失效时能正常地提供 DNS 解析服务。

**注意**

请尽量使用网络运营商提供给您的 DNS 地址；PPPoE 或 DHCP 方式接入可设为“自动获取”。

如果您不知道本地网络运营商的 DNS ，可以在“主要省份城市 DNS 列表[版本： v1.0]”中查找。

DNS 的修改将影响到 PPPoE 拨号及 DHCP 的设置，提交后将自动更新相应设置。

DNS 获取方式:	手动指定	
首选 DNS:	202.103.44.150	运营商: 中国电信
辅助 DNS:	202.103.24.68	运营商: 中国电信
可选 DNS-1:	218.104.111.122	运营商: 中国联通
可选 DNS-2:	218.104.111.114	运营商: 中国联通
可选 DNS-3:		运营商: 中国电信
可选 DNS-4:		运营商: 中国电信

[DNS 代理解析](#)
[保存设置](#) [重置](#) [诊断](#) [诊断日志](#)

图 4.1. DNS 参数

点击下面的“诊断”按钮会有对应的诊断日志显示

[保存设置](#) [重置](#) [诊断](#) [诊断日志](#)

== 2012-12-14 09:25:57 ==
正在测试 DNS 服务器 202.103.44.150 ... 成功
正在测试 DNS 服务器 202.103.24.68 ... 成功
正在测试 DNS 服务器 218.104.111.122 ... 成功
正在测试 DNS 服务器 218.104.111.114 ... 成功

图 4.2. DNS 诊断





4.2. 动态域名解析

4.2.1. 配置动态域名解析

- 动态域名解析简介

动态域名解析(DDNS)就是实现固定域名到动态 IP 地址之间的解析，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态IP地址传送给位于服务商主机上的服务器程序，服务程序负责提供DNS服务并实现动态域名解析。



注意

动态域名解析仅适用于非静态IP（比如通过 DHCP 获取或 PPPoE 拨号分配），如果您拥有固定IP，无需使用此功能。

如果您使用 PPPoE 拨号连接到 Internet，PPPoE 拨号完后会自动更新域名信息。

- 启用动态域名解析功能

海蜘蛛路由支持多种动态域名服务商，如下图所示：



图 4.3. 域名服务商

这里支持的中文服务提供商有希网、金万维和花生壳，这里我们以申请花生壳域名为例：

1. IE url中输入 **www.oray.cn** 进入花生壳主页->单击免费注册->登录->免费域名申请，申请成功后在我的控制台的产品管理选项卡中的免费域名选项卡中将会显示新申请的域名，如下图所示：



图 4.4. 新申请的域名

2. web登录海蜘蛛路由->网络设置->动态域名解析->增加按钮，进入新增页面，输入新申请的域名、用户名和密码并选择线路，如下图所示：

☒ 启用动态域名解析功能

ID	服务提供商/动态域名	用户名/密码	线路	备注	激活	删除
1	<div>花生壳 (oray.net)</div> <div>asdfgdgfhfh.vicp.net</div>	<div>qq-shirly</div> <div>*****</div>	WAN-1 (eth0/ 218.36.24)		<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

提交修改

重置

更新域名

取消

更新日志

3. 单击更新域名->查看更新日志，如下图所示：

```
2009-07-27 10:26:01 正在更新花生壳域名 qq-shirly ...
2009/07/27 10:26:01.030| Init phservice2.oray.net with user qq-shirly/*****
2009/07/27 10:26:01.080| Init service OK!
2009/07/27 10:26:01.080| Soap invoke begun with url: /userinfo.asmx/GetMiscInfo
== 客户端IP: 218.36.24.34 与所选线路WAN-1端口IP相同
2009/07/27 10:26:01.268| ExecuteUpdate Connecting PhLinux3.Oray.Net.
2009/07/27 10:26:01.438| SEND AUTH REQUEST COMMAND...2009/07/27 10:26:01.438| OK.
2009/07/27 10:26:01.514| SERVER SIDE KEY "334 24z0RNGVNhBtSiKxLyINDw==" RECEIVED.
2009/07/27 10:26:01.514| SEND AUTH DATA...2009/07/27 10:26:01.514| OK
== 找到动态域名: asdfgdgfhfh.vicp.net
== 找到动态域名: qq-shirly.vicp.net
2009/07/27 10:26:02.066| SEND CNFM DATA...2009/07/27 10:26:02.066| OK
2009/07/27 10:26:02.172| ExecuteUpdate 250 Register successfully
2009/07/27 10:26:02.246| ExecuteUpdate 250 Register successfully
2009/07/27 10:26:02.246| 250 4243218 1277681478
2009/07/27 10:26:02.246| ExecuteUpdate nChatID:4243218, nStartID:1277681478
2009/07/27 10:26:02.246| SEND QUIT COMMAND...2009/07/27 10:26:02.246| OK.
== 域名信息更新成功！
```

可知此时客户端的WAN端口IP为 218.36.24.34，管理员可通过此IP或者 <http://asdfgdgfhfh.vicp.net> 从外网访问客户端。

4.2.2. 动态域名解析相关问题

1. 更改了动态域名解析后，日志显示更新成功，但访问域名还是原来的IP地址的原因。

这个有可能是DNS缓存问题，现在网络上的DNS服务器都是分布式的，这里涉及到缓存更新时间问题，您可以访问 [域名查询网站](#) 来查看缓存更新时间，在如下图位置输入您想要查询的域名：

图 4.5. 输入域名

这里查询的是海蜘蛛技术支持页面，这里的TTL为3600就是缓存更新时间：

host	ip	class	ttl
support.hi-spider.com	59.175.215.26	IN	3600

图 4.6. 缓存更新时间

也就是说我们这里更改了动态域名后要一个小时后访问这个域名才会指向正确的IP，每个动态域名提供商也有自己的缓存更新时间。此时间过后才会查询到新的域名IP。

2. 有时更改了动态域名解析后，日志显示更新成功，从外网访问域名正常，但从内网访问域名还是原来的IP地址的原因。

您从外网查询此域名时，与当地DNS服务器更新时间有关，如果从内网查询，还可能与路由设置的DNS缓存时间有关，如下图：

启用 DNS 域名解析服务：	<input checked="" type="checkbox"/> 是
强制使用 DNS 代理：	<input checked="" type="checkbox"/> 是 (DNS即插即用, 启用后客户机可任意配置DNS地址)
DNS查询记录缓存大小：	<input type="text" value="8192"/> (缓存DNS查询记录, 默认8192, 最大32768)
DNS缓存时间：	<input type="text" value="300"/> s (60~3600, 默认为 300)

图 4.7. DNS缓存时间

这里我们配置的是300秒，假设当地DNS服务器更新时间为120秒，从当地外网查询域名时会在120秒后更新，但通过此路由的内网主机查询域名时会300秒后才更新。





4.3. 静态路由

1. 静态路由简介

静态路由是指由网络管理员手工配置的路由表信息。通过配置静态路由，管理员可以人为地指定对某一网络访问时所经过的路径。在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

2. 配置静态路由

这里假设routerA与routerB直连，routerA的WAN口IP为218.36.24.34/29,LAN口IP为172.16.10.1/24; routerB的WAN口IP为218.36.24.35/29,LAN口IP为172.16.30.1/24

在routerA上配置静态路由如下图所示：

☒ 启用静态路由功能

ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	172.16.30.1/24	<input type="text"/> <input checked="" type="checkbox"/> 自动	WAN-1 (eth0/218.36.24.34)	1	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

[日志记录](#)

图 4.8. routerA上设置静态路由

☒ 启用静态路由功能

ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	172.16.10.1/24	<input type="text"/> <input checked="" type="checkbox"/> 自动	WAN-1 (eth0/218.36.24.35)	1	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

[日志记录](#)

图 4.9. routerB上设置静态路由



提示

目的网路即为用户所要访问的网络，出口网关即为路由器下一跳IP的地址。

3. 测试静态路由

在路由A下任意一主机ping路由器B下的任意一主机，如能ping通则路由由设置成功。

```
C:\Documents and Settings\Administrator>ping 172.16.30.33

Pinging 172.16.30.33 with 32 bytes of data:

Reply from 172.16.30.33: bytes=32 time=39ms TTL=126
Reply from 172.16.30.33: bytes=32 time=39ms TTL=126
Reply from 172.16.30.33: bytes=32 time=39ms TTL=126
Reply from 172.16.30.33: bytes=32 time=43ms TTL=126

Ping statistics for 172.16.30.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 43ms, Average = 40ms
```

图 4.10. 测试静态路由



4.2. 动态域名解析



4.4. 多线负载及策略



4.4. 多线负载及策略

4.4.1. 多线路策略简介

多线路接入是指路由器通过多条线路接入互联网，这些线路可能是相同或不同网络运营商提供的。这种情况下可能会出现两种问题：

- 多条同一网络运营商提供线路时，一条线路流量很大，而另外的线路没有流量，也就是说所有数据只走一条线路。
- 多条不同网络运营商提供线路时，访问某些网站时有时候很慢，有时候却很快。例如一条中国电信和一条中国网通线路接入时，访问位于中国电信的 [海蜘蛛网络科技有限公司](#) 网站时，有时候很快，有时候却很慢。这是因为您的访问请求有时候走了中国电信的线路，它们位于同一个网络中，所以速度会很快；但有时候访问请求会走中国网通的线路，它们位于不同的网络中，要走很多弯路才能到达我们的网站，所以速度会很慢。

针对以上两种问题，海蜘蛛路由系统提供了多线路负载均衡、带宽叠加、策略路由等多种解决方案。

下面将以四种情况为例来说明多线路的设置：

1. 两条相同网络运营商线路的叠加，例如：两条中国电信线路叠加或两条中国网通线路叠加。
2. 两条不同网络运营商线路的策略路由，例如：一条中国电信线路和一条中国网通线路的策略路由。
3. 多条不同网络运营商线路的策略路由，例如：一条中国电信、一条中国网通和一条中国铁通的策略路由。
4. 多条不同网络运营商线路的带宽叠加和策略路由，例如：两条中国电信线路带宽叠加、两条中国网通线路带宽叠加再和一条中国铁通线路做策略路由。

4.4.2. 两条相同网络运营商线路接入

以两条中国电信提供的线路接入为例，将这两条线路的带宽叠加起来以提供高速互联网接入。例如一条线路的带宽为 2M，另一条线路的带宽为 4M，叠加后就相当于有一条带宽为 6M 的高速互联网接入线路。

登录到 Web 远程管理设置，进入“网络设置”->“广域网（WAN）”，选择广域网接口 [WAN-1] 和 [WAN-2]，在“网卡位置”下拉框中分别选择要分配的网卡， 点击“绑定”即可。



图 4.11. 选择 广域网 接口

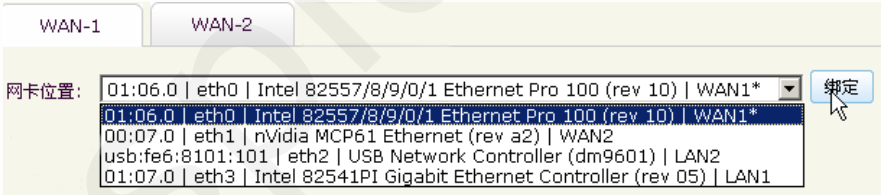


图 4.12. 绑定网卡

广域网接口设置可参照 [设置广域网（WAN）](#)。

以下设置，广域网 [WAN-1] 和 广域网 [WAN-2] 相同。

点击WAN口设置最下面的线路检测，进入此页面中编辑WAN口。

先勾选启用，选择“运营商”为 中国电信。

启用线路检测：用于探测是否掉线，及掉线后进行自动切换，一般勾选。

“线路探测模式”：推荐选择“PING+SYN 混合探测”，若在禁止 ping 的情况下，选择“SYN/TCP 外部探测”。

“SYN/TCP 探测对象”：依据选择的运营商进行相应的选择，一般填所属线路的本地网址。

编辑 wan1 ...

启用：☒ 是

运营商：

中国电信

(启用多线策略及负载时需要)

检测时间间隔：

10

 s (每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)

线路探测模式：

PING+SYN 混合探测 (推荐)

禁止ping通时选择 SYN/TCP外部探测

重复探测次数：

3

 (连续多少次探测不通才认为是掉线, 默认为2次)

PING/ICMP 探测对象： (为空表示网关, 延时不大于

0

 ms

选择当地的官方ISP地址

SYN/TCP 探测对象：

www.hbtelecom.com.cn

 端口：

80

 (默认为 80), 延时不大于

0

 ms

湖北省电信公司

线路工作时间： - (线路非24小时连通时才需设置, 如 08:00 表示上午8点)

调试模式运行：☐ 是 (一般不用开启)

测试模式运行：☐ 是 (掉线后不切换)

保存设置

重置

取消

图 4.13. 线路检测设置

设置好后，点击“保存设置”。

进入“网络设置”->“多线负载及策略”，勾选“启用多线负载及策略”。

在“线路设置”中可以看到刚才设置的 广域网 [WAN-1] 和 广域网 [WAN-2] 的摘要信息，把线路类型都设置为默认线路，将 WAN1 和 WAN2 的“激活”栏勾选，点击“保存设置”即可。

☒ 启用多线负载及策略

☐ 自动从服务器更新路由表 (最后更新时间: 2009-05-26 10:38:49)

[线路变化日志](#) [清除](#)

线路设置...

策略路由由工作模式：

正常模式、掉线自动切换

☐ 所有数据全部走策略线路 (仅用于VPN借线)

默认线路: 所有不符合策略的数据将全部走默认线路. 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条. 同一ISP应选择同一线路类型.

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth2/eth2/192.168.10.1/255.255.255.0	<div>默认线路</div>	<div>中国电信 (222 条 v2.4)</div>	<input checked="" type="checkbox"/> 是
WAN2	中国电信	eth3/eth3/192.168.10.1/255.255.255.0	<div>默认线路</div>	<div>中国电信 (222 条 v2.4)</div>	<input checked="" type="checkbox"/> 是

保存设置

重设

图 4.14. 启用多线负载及策略-O1

这样就完成了两条相同 ISP 线路的带宽叠加，实现了高速的互联网接入。

4.4.3. 两条不同的网络运营商线路接入

一条为中国电信提供的线路接入，另一条为中国网通提供的线路接入，在这两条线路之间做策略路由，以避免出现上网过慢的现象。即访问位于中国电信的网络资源时走中国电信的线路；访问位于中国通网的网络资源时走中国通网的线路。

登录 Web 远程管理，进入“网络设置”->“广域网 (WAN)”，选择广域网接口 [WAN-1] 和 [WAN-2]，在“网卡位置”下拉框中分别选择要分配的网卡，点击“绑定”按钮。参照[两条相同网络运营商线路接入](#)。

广域网接口设置可参照[设置广域网 \(WAN\)](#)。

在“线路检测设置”中选择运营商，广域网 [WAN-1] 选择“中国电信”，广域网 [WAN-2] 选择“中国联通/网通”。

以下设置，广域网 [WAN-1] 和 广域网 [WAN-2] 相似，参照[两条相同网络运营商线路接入](#)。

在WAN口设置里点击进入最下面的线路检测，进入线路检测页面，启用线路检测。

“线路探测模式”：推荐选择“PING+SYN 混合探测”，若在禁止 ping 的情况下，选择“SYN/TCP 外部探测”。

“SYN/TCP 探测对象”：依据选择的运营商进行相应的选择，一般填所属线路的本地网址。

重要

此时“此网关作为默认路由”选项 广域网 [WAN-1] 和 广域网 [WAN-2] 只需勾选一个。

此网关作为默认路由:	<input type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)

设置好后, 点击“保存设置”。

进入“网络设置”->“多线负载及策略”, 勾选“启用多线负载及策略”。

在“线路设置”中可以看到刚才设置的 广域网 [WAN-1] 和 广域网 [WAN-2] 的摘要信息, 在“线路类型”栏中分别选择不同的线路类型, 如: WAN1 选择“默认线路”, WAN2 选择“策略线路-1”。并勾选“激活”选项, 点击“保存设置”即可。

☒ 启用多线负载及策略

☐ 自动从服务器更新路由表 (最后更新时间: 2009-05-26 10:38:49)

[线路变化日志](#) [清除](#)

线路设置...

策略路由工作模式: 正常模式、掉线自动切换 ☐ 所有数据全部走策略线路 (仅用于VPN借线)

默认线路: 所有不符合策略的数据将全部走默认线路。策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路。默认线路和策略线路可以是一条或者多条, 同一ISP应选择同一线路类型。

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth2/eth2/192.168.10.1/255.255.255.0	默认线路	中国电信 (222 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN2	中国联通/网通	eth3/eth3/192.168.10.1/255.255.255.0	策略线路-1	中国联通/网通 (192 条 v2.4)	<input checked="" type="checkbox"/> 是

保存设置

重设

图 4.15. 启动多线负载及策略-02

注意

默认线路: 所有不符合策略的数据将全部走默认线路。

策略线路: 如果用户访问的 IP 在策略线路对应的网络运营商路由表中, 则走此线路。

默认线路和策略线路可以是一条或者多条, 同一网络运营商应选择同一线路类型。

这样就完成了两条不同 ISP 线路间的策略路由, 从而避免了出现访问某些网络资源很慢的情况。

4.4.4. 多条不同网络运营商线路接入

一条为中国电信提供的线路接入, 另一条为中国网通提供的线路接入, 还有一条中国铁通提供的线路接入, 在这三条线路之间做策略路由, 以避免出现上网过慢的现象。即访问位于中国电信的网络资源时走中国电信的线路; 访问位于中国网通的网路资源时走中国网通的线路; 访问位于中国铁通的网络资源时走中国铁通的线路。

登录 Web 远程管理, 进入“网络设置”-> “广域网 (WAN)”, 选择广域网接口 [WAN-1]、[WAN-2] 和 [WAN-3], 在“网卡位置”下拉框中分别选择要分配的网卡, 点击“绑定”按钮。参照[两条相同网络运营商线路接入](#)。

广域网接口设置可参照[设置广域网 \(WAN\)](#)。

在WAN口设置下进入“线路检测”设置页面中, 选择运营商。广域网 [WAN-1] 选择“中国电信”, 广域网 [WAN-2] 选择“中国联通/网通”, 广域网 [WAN-3] 选择“中国铁通”。

以下设置, 广域网 [WAN-1]、广域网 [WAN-2] 和 广域网 [WAN-3] 相似, 参照[两条相同网络运营商线路接入](#)和[两条不同网络运营商线路接入](#)。

进入线路检测页面, 启用线路检测: 用于探测是否掉线, 及掉线后进行自动切换, 一般勾选。

“线路探测模式”: 推荐选择“PING+SYN 混合探测”, 若在禁止 ping 的情况下, 选择“SYN/TCP 外部探测”。

“SYN/TCP 探测对象”: 依据选择的运营商进行相应的选择, 一般填所属线路的本地网址。

重要

此时“此网关作为默认路由”, 广域网 [WAN-1]、广域网 [WAN-2] 和 广域网 [WAN-3] 只需勾选一个。

此网关作为默认路由:

☐ 是 (一般选上, 如果有多条WAN线, 请只选一个)

开机自动启动:

☒ 是 (随系统启动, 一般选上)

设置好后, 点击“保存设置”。

进入“网络设置”->“多线负载及策略”, 勾选“启用多线负载及策略”。

在“线路设置”中可以看到刚才设置的 广域网 [WAN-1]、广域网 [WAN-2] 和 广域网 [WAN-3] 的摘要信息, 在“线路类型”栏中分别选择不同的线路类型, 如: WAN1 选择“默认线路”, WAN2 选择“策略线路-1”, WAN3 选择“策略线路-2”, 并勾选“激活”选项, 点击“保存设置”即可。

线路设置...

策略路由工作模式: 正常模式、掉线自动切换 ☐ 所有数据全部走策略线路 (仅用于VPN借线)

默认线路: 所有不符合策略的数据将全部走默认线路。策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路。默认线路和策略线路可以是一条或者多条, 同一ISP应选择同一线路类型。

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth2/eth2/192.168.10.1/255.255.255.0	默认线路	中国电信 (222 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN2	中国联通/网通	eth3/eth3/192.168.10.1/255.255.255.0	策略线路-1	中国联通/网通 (192 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN3	中国铁通	eth1/eth1/10.8.0.1/255.255.255.0	策略线路-2	自定义路由表-1 (0 条)	<input checked="" type="checkbox"/> 是

保存设置 重设 须在“路由表设置”中的“自定义路由表-1”下手动增加

图 4.16. 启动多线负载及策略-O3


若这里的中国铁通选择“自定义路由表-1”, 则需要下面“路由表设置”中的“自定义路由表-1”下手动增加路由表。

路由表设置...

自定义路由表-1 (682 条)

1.68.0.0/14
1.80.0.0/13
1.180.0.0/14
1.192.0.0/13
1.202.0.0/17
1.204.0.0/14
27.16.0.0/12
27.128.0.0/15
27.148.0.0/14
27.184.0.0/13
27.224.0.0/14
58.30.0.0/15

图 4.17. 手动增加路由表

 注意

手动添加路由表时, 需同时输入IP/子网掩码, 一排输入一个IP段, 否则无法添加成功。

您也可以设置IP或端口走指定的线路, 例如:

这里假设让内网所有 QQ 通信都走中国电信线路 (WAN-1), 可以在“自定义策略[按 IP/协议/端口]”处“新增规则”。

在“线路”下拉框中选择 WAN1; 在“协议类型”下拉框中选择“UDP” (QQ 默认是 UDP 通信); 在“源IP/网段”输入框中填写内网的网段, 如: 192.168.10.0/24; “源端口”输入框可以不填 (QQ客户端 和 QQ服务器 通信的时候, 客户端端口是随机的); “目的IP/网段”输入框可以不填 (QQ 有很多服务器, 统计较麻烦); 在“目的端口”输入框中填写 QQ服务器使用的端口, 通常是 8000; “优先级”输入框可随便填写 (这里填 1); “注释”输入框可以随便填写 (这里填 QQ); 勾选“激活”复选框, 点击“保存设置”即可。

自定义策略 [按IP/协议/端口] ...

ID	线路	源IP/网段	源端口	优先级	激活
	协议类型	目的IP/网段	目的端口	注释	删除
1	WAN1	192.168.10.0/24		1	<input checked="" type="checkbox"/> 是
	UDP		8000	QQ	

保存设置 新增规则 重设 应用

图 4.18. 自定义策略

这样多条不同 ISP 线路间的策略路由就设置好了，并且所有 QQ 聊天数据全部走中国电信 [WAN-1] 线路。

4.4.5. 两条电信+两条网通+一条铁通

两条中国电信提供的线路接入，两条中国网通提供的线路接入，还有一条中国铁通提供的线路接入。将两条中国电信线路带宽叠加（假设得到线路 A），将两条中国网通线路带宽叠加（假设得到线路 B），再在线路 A、B 和中国铁通线路之间做策略路由。这样既得到了高速的互联网接入，又避免了出现上网过慢的现象，即访问位于中国电信的网络资源时走 A 线路；访问位于中国网通的网路资源时走 B 线路；访问位于中国铁通的网络资源时走中国铁通的线路。

登录 Web 远程管理，进入“网络设置”->“广域网（WAN）”，选择广域网接口 [WAN-1]、[WAN-2]、[WAN-3]、[WAN-4] 和 [WAN-5]，在“网卡位置”下拉框中分别选择要分配的网卡，点击“绑定”按钮。参照[两条相同网络运营商线路接入](#)。

广域网接口设置可参照[设置广域网（WAN）](#)。

在WAN口设置下点击进入“线路检测”页面，选择相应的运营商，广域网 [WAN-1] 和 广域网 [WAN-2] 选择“中国电信”，广域网 [WAN-3] 和 广域网 [WAN-4] 选择“中国联通/网通”，广域网 [WAN-5] 选择“中国铁通”。

以下设置，广域网 [WAN-1]、广域网 [WAN-2]、广域网 [WAN-3]、广域网 [WAN-4] 和 广域网 [WAN-5] 相似，可分别参照[两条相同网络运营商线路接入](#)，[两条不同网络运营商线路接入](#)和[多条不同网络运营商线路接入](#)。

启用线路检测：用于探测是否掉线，及掉线后进行自动切换，一般勾选。

“线路探测模式”：推荐选择“PING+SYN 混合探测”，若在禁止 ping 的情况下，选择“SYN/TCP 外部探测”。

“SYN/TCP 探测对象”：依据选择的运营商进行相应的选择，一般填所属线路的本地网址。

☒ 启用多线负载及策略

☐ 自动从服务器更新路由表 (最后更新时间: 2009-05-26 10:38:49)

[线路变化日志](#) [清除](#)

线路设置...

策略路由工作模式: 正常模式、掉线自动切换 ☐ 所有数据全部走策略线路 (仅用于VPN借线)

默认线路: 所有不符合策略的数据将全部走默认线路, 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条, 同一ISP应选择同一线路类型.

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth0/eth0/192.168.10.1/255.255.255.0	默认线路	中国电信 (222 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN2	中国电信	eth2/eth2/10.8.0.1/255.255.255.0	默认线路	中国电信 (222 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN3	中国联通/网通	eth3/eth3/10.8.0.3/255.255.255.0	策略线路-1	中国联通/网通 (192 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN4	中国联通/网通	eth4/eth4/10.8.0.4/255.255.255.0	策略线路-1	中国联通/网通 (192 条 v2.4)	<input checked="" type="checkbox"/> 是
WAN5	中国铁通	eth5/eth5/10.8.0.5/255.255.255.0	策略线路-2	中国铁通 (7 条 v1.0)	<input checked="" type="checkbox"/> 是

保存设置

重设

图 4.19. 多线负载及策略-04

这样就完成了多条不同 ISP 线路间的叠加和策略路由。

4.4.6. 多线负载均衡

这里以电信的静态IP线路和PPPoE拨号线路为例实现负载均衡，具体设置如下：

1. “网络设置”->“广域网”，设置WAN1口相关属性，如下所示：

- 设置Internet接入方式为静态IP模式

Internet 接入方式: 以太网/静态IP (固定IP上网, 如光纤)

图 4.20. 静态IP模式

- 设置静态IP地址

MAC地址:	<input type="text" value="00-e0-4c-68-00-df"/>		
MAC地址克隆:	<input type="text"/>		
IP地址:	<input type="text" value="219.36.24.34"/>		
子网掩码:	<input type="text" value="255.255.255.248"/>	[此网段可容纳 6 台机器]	
网关:	<input type="text" value="219.36.24.33"/>		
绑定网关:	<input type="text"/>	<input type="button" value="绑定"/>	<input type="button" value="获取"/>
扩展 IP地址:	<div></div>		<div><input type="text" value="IP地址:"/> <input type="text" value="子网掩码:"/> <input type="button" value="增加"/> <input type="button" value="删除"/></div>
此网关作为默认路由:	<input checked="" type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)		
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)		

图 4.21. 设置静态IP

- 进入线路检测页面，如下图：

启用:	<input checked="" type="checkbox"/> 是		
运营商:	<input type="text" value="中国电信"/>	(启用多线策略及负载时需要)	
检测时间间隔:	<input type="text" value="10"/> s (每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)		
线路探测模式:	<input type="text" value="PING+SYN 混合探测 (推荐)"/>		
重复探测次数:	<input type="text" value="3"/> (连续多少次探测不通才认为是掉线, 默认为2次)		
PING/ICMP 探测对象:	<input type="text"/> (为空表示网关), 延时不大于 <input type="text" value="0"/> ms		
SYN/TCP 探测对象:	<input type="text" value="www.hbtelecom.com.cn"/>	端口: <input type="text" value="80"/>	(默认为 80), 延时不大于 <input type="text" value="0"/> ms <input type="text" value="湖北省电信公司"/>
线路工作时间:	<input type="text"/> - <input type="text"/> (线路非24小时连通时才需设置, 如 08:00 表示上午8点)		
调试模式运行:	<input type="checkbox"/> 是 (一般不用开启)		
测试模式运行:	<input type="checkbox"/> 是 (掉线后不切换)		

图 4.22. 线路检测设置

2. 设置WAN2口相关属性

- 设置Internet接入方式为ADSL/PPPoE拨号模式

Internet 接入方式:

图 4.23. 拨号模式

- PPPoE 拨号连接

MAC地址:	<input type="text" value="00-e0-4c-68-00-e0"/>		
MAC地址克隆:	<input type="text"/>		
PPPoE 拨号用户名:	<input type="text" value="123"/>		
PPPoE 密码:	<input type="text" value="....."/>		
发送 LCP(连接控制协议) 数据包间隔:	<input type="text" value="20"/> s (20~60, 如果频繁掉线, 请适当增大此值)		
多少个LCP请求未应答则断开连接:	<input type="text" value="3"/> (2~6, 如果频繁掉线, 请适当增大此值)		
此网关作为默认路由:	<input type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)		
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)		

图 4.24. 拨号连接设置

• 线路检测设置

启用:

☒ 是

运营商:

中国电信

(启用多线策略及负载时需要)

检测时间间隔:

10

s (每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)

线路探测模式:

PING+SYN 混合探测 (推荐)

重复探测次数:

3

(连续多少次探测不通才认为是掉线, 默认为2次)

PING/ICMP 探测对象:

(为空表示网关), 延时不大于 0 ms

SYN/TCP 探测对象:

www.hbtelecom.com.cn

端口: 80

(默认为 80), 延时不大于 0 ms

湖北省电信公司

线路工作时间:

-

(线路非24小时连通时才需设置, 如 08:00 表示上午8点)

调试模式运行:

☐ 是 (一般不用开启)

测试模式运行:

☐ 是 (掉线后不切换)

图 4.25. 线路检测设置

3. “网络设置”->“多线路负载及策略”, 启用多线路负载及策略, 如下图所示:

☒ 启用多线负载及策略

☒ 自动从服务器更新路由表 (最后修改时间: 2009-08-21 14:38:49)

[线路变化日志](#) [清除](#)

线路设置...

策略路由工作模式: 正常模式、掉线自动切换

默认线路: 所有不符合策略的数据将全部走默认线路. 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条. 同一ISP应选择同一线路类型.

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth1/eth1/219.36.24.34/255.255.255.224	默认线路	中国电信 (286 条 v3.0)	<input checked="" type="checkbox"/> 是
WAN2	中国电信	eth2/ppp0/10.8.0.4/255.255.255.255	默认线路	中国电信 (286 条 v3.0)	<input checked="" type="checkbox"/> 是


图 4.26. 多线路负载设置

4. 指定哪些网段的数据走哪条线, 实现负载均衡, 例如指定IP为172.16.1.10的PC机访问外网时走WAN1线路, 需如下设置:

自定义策略 [按IP/协议/端口]...

ID	线路	源IP/网段	源端口	优先级	状态/动作
	协议类型	目的IP/网段	目的端口	备注	-
1	WAN1	172.168.1.10		1	<input checked="" type="checkbox"/> 激活
	TCP+UDP			WAN1	<input type="checkbox"/> 掉线不切换

图 4.27. 自定义策略

 IP表示规则

表示单个IP: 172.16.1.10

表示多个不连续IP: 172.16.1.1,172.16.1.2

表示一段IP地址: 172.16.1.100-172.16.1.200

表示一个网段: 172.16.1.0/24

5. tracert测试

不设置自定义策略时用tracert检测数据包访问外网线路：

```
C:\Documents and Settings\Administrator.B4CD3B289DB04B4>tracert www.baidu.com

Tracing route to www.a.shifen.com [119.75.213.61]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  172.16.1.2
  2  <1 ms  <1 ms  <1 ms  softbank219036024033.bbtec.net  [219.36.24.33]
  3  16 ms  19 ms  23 ms  59.175.215.25
  4  1 ms  1 ms  1 ms  221.232.249.181
  5  <1 ms  <1 ms  <1 ms  221.232.249.113
  6  1 ms  1 ms  1 ms  221.232.254.97
  7  1 ms  1 ms  1 ms  59.175.246.41
  8  17 ms  18 ms  18 ms  202.97.34.161
  9  22 ms  21 ms  21 ms  220.181.16.62
 10  21 ms  21 ms  21 ms  220.181.17.118
 11  21 ms  21 ms  21 ms  119.75.213.61
```

图 4.28.

将IP地址为172.16.1.10的PC机改为走WAN1时的tracert路径图：

```
C:\Documents and Settings\Administrator.B4CD3B289DB04B4>tracert www.baidu.com

Tracing route to www.a.shifen.com [119.75.213.61]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  172.16.1.2
  2  <1 ms  <1 ms  <1 ms  softbank219036024033.bbtec.net  [219.36.24.33]
  3  16 ms  19 ms  23 ms  59.175.215.25
  4  1 ms  1 ms  1 ms  221.232.249.181
  5  <1 ms  <1 ms  <1 ms  221.232.249.113
  6  1 ms  1 ms  1 ms  221.232.254.97
  7  1 ms  1 ms  1 ms  59.175.246.41
  8  17 ms  18 ms  18 ms  202.97.34.161
  9  22 ms  21 ms  21 ms  220.181.16.62
 10  21 ms  21 ms  21 ms  220.181.17.118
 11  21 ms  21 ms  21 ms  119.75.213.61
```

图 4.29.

将IP地址为172.16.1.10的PC机改为走WAN2时的tracert路径图：

```
C:\Documents and Settings\Administrator.B4CD3B289DB04B4>tracert www.baidu.com

Tracing route to www.a.shifen.com [119.75.213.61]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  172.16.1.2
  2  <1 ms  4 ms  <1 ms  10.8.0.1
  3  26 ms  57 ms  27 ms  1.244.140.219.broad.wh.hb.dynamic.163data.com.cn
  4  26 ms  25 ms  25 ms  59.175.253.245
  5  26 ms  27 ms  27 ms  59.175.249.225
  6  25 ms  27 ms  27 ms  59.175.246.41
  7  44 ms  43 ms  41 ms  202.97.34.161
  8  60 ms  57 ms  57 ms  220.181.16.62
  9  58 ms  53 ms  55 ms  220.181.17.118
 10  43 ms  52 ms  43 ms  119.75.213.61
```

图 4.30.

由此可知默认情况下所有数据都走WAN1线路，自定义策略后实现指定IP走WAN2线路从而实现负载均衡。

4.4.7. 不同ISP实现策略路由

以电信和网通双静态IP为例实现策略路由。

环境描述：电信光纤一根：LAN口IP 172.16.1.2，WAN1口IP：219.36.24.34，GW：219.36.24.33；网通光纤一根：WAN2口IP：59.175.24.38，GW：59.175.24.33。

1. “网络设置”->“广域网”，设置WAN1口相关属性，如下所示：

- 设置Internet接入方式为静态IP模式

Internet 接入方式：

以太网/静态IP (固定IP上网, 如光纤)

图 4.31. 静态IP模式

- 设置静态IP地址

MAC地址:	<input type="text" value="00-e0-4c-68-00-df"/>		
MAC地址克隆:	<input type="text"/>		
IP地址:	<input type="text" value="219.36.24.34"/>		
子网掩码:	<input type="text" value="255.255.255.248"/>	[此网段可容纳 6 台机器]	
网关:	<input type="text" value="219.36.24.33"/>		
绑定网关:	<input type="text"/>	<input type="button" value="绑定"/>	<input type="button" value="获取"/>
扩展 IP地址:	<div><div></div><div><input type="text" value=""/> <input type="text" value=""/> <input type="button" value="增加"/> <input type="button" value="删除"/></div></div>		
此网关作为默认路由:	<input checked="" type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)		
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)		

图 4.32. 设置静态IP

- 进入线路检测页面, 如下图:

运营商:	<input type="text" value="中国电信"/>	(启用多线策略及负载时需要)
是否启用线路检测	<input checked="" type="checkbox"/> 启用 (用于探测是否掉线, 及掉线后进行自动切换) 运行中 (PID:5300)	
检测时间间隔:	<input type="text" value="10"/> s (每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)	
线路探测模式:	<input type="text" value="PING+SYN 混合探测 (推荐)"/>	
重复探测次数:	<input type="text" value="3"/> (连续多少次探测不通才认为是掉线, 默认为2次)	
PING/ICMP 探测对象:	<input type="text"/> (为空表示网关)	
SYN/TCP 探测对象:	<input type="text" value="www.hbtelecom.com.cn"/>	端口: <input type="text" value="80"/> (默认为 80)
调试模式运行:	<input type="checkbox"/> 是 (一般不用开启)	
测试模式运行:	<input type="checkbox"/> 是 (掉线后不切换)	

图 4.33. 设置线路检测

2. 设置WAN2口相关属性, 如下所示:

- 设置Internet接入方式为静态IP模式

Internet 接入方式:

图 4.34. 静态IP模式

- 设置静态IP地址

MAC地址:

00-e0-4c-68-00-e0

MAC地址克隆:

IP地址:

59.175.24.38

子网掩码:

255.255.255.248

[此网段可容纳 6 台机器]

网关:

59.175.24.33

绑定网关:

绑定

获取

扩展 IP地址:

IP地址:

子网掩码:

增加

删除

此网关作为默认路由:

☐ 是 (一般选上, 如果有多条WAN线, 请只选一个)

开机自动启动:

☒ 是 (随系统启动, 一般选上)

图 4.35. 设置静态IP

- 进入线路检测设置, 如下图:

运营商:

中国联通/网通

(启用多线策略及负载时需要)

是否启用线路检测

☒ 启用 (用于探测是否掉线, 及掉线后进行自动切换)

运行中 (PID:5222)

检测时间间隔:

10

s (每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)

线路探测模式:

PING+SYN 混合探测 (推荐)

重复探测次数:

3

(连续多少次探测不通才认为是掉线, 默认为2次)

PING/ICMP 探测对象:

(为空表示网关)

SYN/TCP 探测对象:

www.hb.chinaunicom.com

端口: 80

(默认为 80)

调试模式运行:

☐ 是 (一般不用开启)

测试模式运行:

☐ 是 (掉线后不切换)

图 4.36. 设置线路检测

- “网络设置”->“多线负载及策略”, 启用多线负载及策略, 设置线路类型及路由表, 如下图所示:

☒ 启用多线负载及策略

☒ 自动从服务器更新路由表 (最后修改时间: 2009-08-21 14:38:49)

[线路变化日志](#) [清除](#)

线路设置...

策略路由工作模式: 正常模式、掉线自动切换

默认线路: 所有不符合策略的数据将全部走默认线路. 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条. 同一ISP应选择同一线路类型.

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth1/eth1/219.36.24.34/255.255.255.248	默认线路	中国电信 (233 条 v2.5)	<input checked="" type="checkbox"/> 是
WAN2	中国联通/网通	eth2/eth2/59.175.24.38/255.255.255.248	策略线路	中国联通/网通 (199 条 v2.6)	<input checked="" type="checkbox"/> 是

图 4.37. 多线负载及策略设置

此时, 客户机访问电信的资源将会WAN1线路, 访问网通的资源将会走WAN2线路; 所有不符合策略的数据将全部走默认线路。

- 利用tracert测试

客户机访问电信网站时的tracert图:

```
C:\Documents and Settings\Administrator.B4CD3B289DB04B4>tracert www.hbtelecom.com.cn

Tracing route to www.hbtelecom.com.cn [58.53.193.41]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    172.16.1.2  客户机网关
  2  <1 ms    <1 ms    <1 ms    softbank219036024033.bbtec.net  [219.36.24.33]
  3  26 ms    26 ms    26 ms    1.244.140.219.broad.wh.hb.dynamic.163data.com.cn [219.140.244.1]
```

图 4.38. 访问电信

客户机访问网通网站时的tracert图：

```
C:\Documents and Settings\Administrator.B4CD3B289DB04B4>tracert www.hb.chinaunicom.com

Tracing route to www.hb.chinaunicom.com [211.91.133.60]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    172.16.1.2  客户机网关
  2  <1 ms    <1 ms    <1 ms    59.175.24.33  WAN2口网关
  3  28 ms    27 ms    29 ms    1.244.140.219.broad.wh.hb.dynamic.163data.com.cn [219.140.244.1]
```

图 4.39. 访问网通



4.3. 静态路由



4.5. 自定义策略



4.5. 自定义策略

进入“网络设置”->“多线路负载”->“自定义策略”，来自定义内网用户走线，这里的走线配置可以有多种方式：

线路：选择外网的线路，包括单WAN多拨的扩展线路，如WAN2.3

协议类型：一般都选择TCP+UDP

源IP/网段：一般都为内网的IP段，可以是单个的主机IP或者整个网段，支持PPPoE拨号主机或固定IP主机

目的IP/网段：一般都为外网IP段或者VPN对端网段

源端口：内网主机的端口号

目的端口：对端设备的端口号

优先级：数字越小权限越高，0最大

掉线不切换：配置固定走到外网，如果此配置的外网线路断开，那么此条配置在多线里并不切换到其它线路，继续保持断线状态。

自定义策略 [按IP/协议/端口]...

ID	线路	源IP/网段	源端口	优先级	状态/动作
	协议类型	目的IP/网段	目的端口	备注	-
1	WAN1	192.168.0.248		1	<input checked="" type="checkbox"/> 激活 <input type="checkbox"/> 删除
	TCP+UDP				<input type="checkbox"/> 掉线不切换

这条配置表示内网192.168.0.248这个主机，所有的数据流量仅走路由的WAN1线路

自定义策略 [按IP/协议/端口]...

ID	线路	源IP/网段	源端口	优先级	状态/动作
	协议类型	目的IP/网段	目的端口	备注	-
1	WAN2			2	<input checked="" type="checkbox"/> 激活 <input type="checkbox"/> 删除
	TCP+UDP		80,443		<input type="checkbox"/> 掉线不切换

这条配置表示内网所有主机在访问目的端口为80和443的外网主机时走WAN2线路，一般是http和https协议的Web网站

每次配置完毕后，必须要保存设置然后再点击应用才能生效



注意

各条配置的优先级最好不要一样，以避免配置冲突导致访问外网时出现线路切换而断线。





4.6. 自定义路由表

除了使用系统自定义的路由表以外，您同样可以根据需要自定义路由表。

- 1. 首先进入“网络设置”->“多线路负载”->“路由表设置”创建路由表，如图：

路由表设置...

自定义路由表-1 (1708 条)

1.48.0.0/15
1.68.0.0/14
1.80.0.0/13
1.92.0.0/15
1.94.0.0/15
1.116.0.0/14
1.192.0.0/13
1.202.0.0/15
1.204.0.0/14
14.104.0.0/13
27.16.0.0/12
27.128.0.0/15

说明

每条规则占一行

cnc => 中国电信；cnc => 中国联通/网通

edu => 教育网；gwb => 长城宽带

crt => 中国铁通；cmc => 中国移动

catv => 有线宽带；citic => 中信网络

- 2. 应用自定义路由表

在使用路由表的下拉列表框中选择自定义路由表-1，保存设置即可，如图：

线路名	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth1/eth1/214.36.24.34/255.255.255.248	默认线路	中国电信 (247 条 v2.6)	<input checked="" type="checkbox"/> 是
WAN2	中国电信	eth2/eth2/59.175.24.38/255.255.255.248	默认线路	中国电信 (247 条 v2.6)	<input checked="" type="checkbox"/> 是
WAN3	中国联通/网通	eth3/eth3/11.22.33.44/255.255.255.0	策略线路-1	自定义路由表-1 (1708 条)	<input checked="" type="checkbox"/> 是

此时，用户访问联通/网通、教育网以及220.11.22.0/24这个网络的资源将都会走WAN3线路。





4.7. 虚拟局域网(VLAN)

4.7.1. 虚拟局域网简介

• 虚拟局域网概念

VLAN（Virtual Local Area Network）即虚拟局域网，是一种通过将局域网内的设备逻辑地而不是物理地划分成一个个网段从而实现虚拟工作组的新兴技术。

• 虚拟局域网的优点

- 1. 限制广播域。广播域被限制在一个VLAN内，节省了带宽，提高了网络处理能力。
- 2. 增强局域网的安全性。不同VLAN内的报文在传输时是相互隔离的，即一个VLAN内的用户不能和其它VLAN内的用户直接通信，如果不同VLAN要进行通信，则需要通过路由器或三层交换机等网络设备。
- 3. 灵活构建虚拟工作组。用VLAN可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。
- 4. 可启用DHCP服务给不同的VLAN网段分配各自的IP地址池，对网络客户机自动分配IP地址，有效地防止网络上计算机配置地址的冲突。
- 5. 局域网内所有客户机都可采用PPPoE 拨号到网关通过网关的实现共享上网，用户只需设置拨号账户即可方便入网。

4.7.2. 路由上划分VLAN

有如下网络拓扑图：

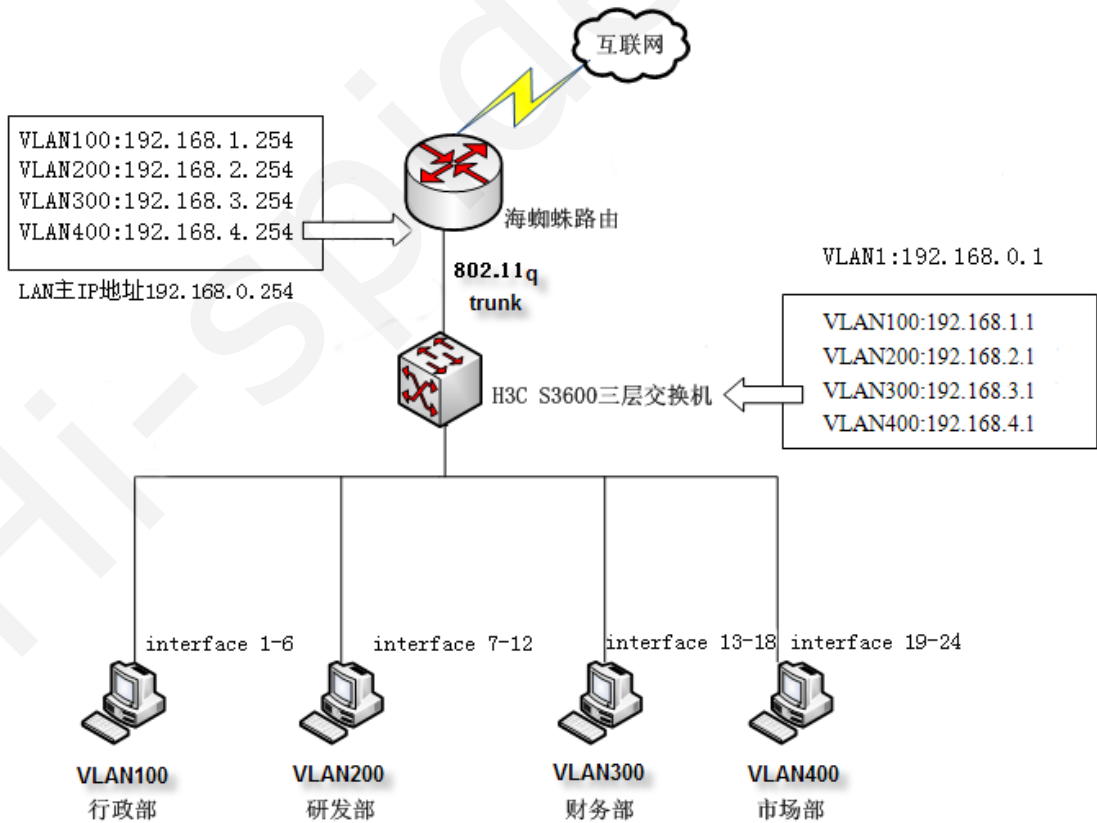


图 4.40. 某公司的网络拓扑图

中继接口使用 802.11q 封装，允许所有VLAN访问，在这种情况下，交换机上不需要设置默认路由。

4.7. 虚拟局域网(VLAN)

海蜘蛛路由的LAN口主IP地址为192.168.0.254，并建立了4个逻辑VLAN，和交换机上的VLAN相对应。

DHCP服务器对VLAN-1/2/3/4 提供IP分配，每个VLAN获取对应网段的地址，即：

- VLAN-1 下的机器获得 192.168.1.0/255.255.255.0 段的IP
- VLAN-2 下的机器获得 192.168.2.0/255.255.255.0 段的IP
- VLAN-3 下的机器获得 192.168.3.0/255.255.255.0 段的IP
- VLAN-4 下的机器获得 192.168.4.0/255.255.255.0 段的IP

4.7.2.1.1. 路由器设置

1. 划分vlan

“网络设置”->“VLAN 虚拟局域网”，新增VLAN网段，配置如下图所示：

☒ 启用 VLAN (虚拟局域网)功能

ID	VLAN_ID	IP地址	子网掩码	接口	备注	激活	编辑
1	100	192.168.1.254	255.255.255.0	lan1	1.0网段		
2	200	192.168.2.254	255.255.255.0	lan1	2.0网段		
3	300	192.168.3.254	255.255.255.0	lan1	3.0网段		
4	400	192.168.4.254	255.255.255.0	lan1	4.0网段		

[\[专家模式\]](#) [\[导出规则\]](#)

提交修改

重设

新增

查看状态

日志记录

图 4.41. VLAN网段配置

提示

这里VLAN_ID号必须大于1小于4096，VLAN_ID与交换机上划分的VLAN_ID号需一一对应。下面主机的网关指向路由各VLAN的子接口。

4.7.2.1.2. 交换机设置

```
      此为H3C S3600交换机的设置
DIS current-configuration
#
 sysname SystemTest
#
radius scheme system
#
domain system
#
local-user admin
 password simple admin
 service-type telnet
 level 3
local-user sxy
 password simple sxy
 service-type telnet
#
vlan 1
#
vlan 100
 description Test1
#
vlan 200
 description Test2
#
vlan 300
 description Test3
#
vlan 400
 description Test4
#
interface Vlan-interface1
```

4.7. 虚拟局域网(VLAN)

```
ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.3.1 255.255.255.0
#
interface Vlan-interface400
ip address 192.168.4.1 255.255.255.0
#
interface Aux1/0/0
#
interface Ethernet1/0/1
port access vlan 100
#
interface Ethernet1/0/2
port access vlan 100
#
interface Ethernet1/0/3
port access vlan 100
#
interface Ethernet1/0/4
port access vlan 100
#
interface Ethernet1/0/5
port access vlan 100
#
interface Ethernet1/0/6
port access vlan 100
#
interface Ethernet1/0/7
port access vlan 200
#
interface Ethernet1/0/8
port access vlan 200
#
interface Ethernet1/0/9
port access vlan 200
#
interface Ethernet1/0/10
port access vlan 200
#
interface Ethernet1/0/11
port access vlan 200
#
interface Ethernet1/0/12
port access vlan 200
#
interface Ethernet1/0/13
port access vlan 300
#
interface Ethernet1/0/14
port access vlan 300
#
interface Ethernet1/0/15
port access vlan 300
#
interface Ethernet1/0/16
port access vlan 300
#
interface Ethernet1/0/17
port access vlan 300
#
interface Ethernet1/0/18
port access vlan 300
#
interface Ethernet1/0/19
port access vlan 400
#
interface Ethernet1/0/20
```


4.7. 虚拟局域网(VLAN)

```
port access vlan 400
#
interface Ethernet1/0/21
port access vlan 400
#
interface Ethernet1/0/22
port access vlan 400
#
interface Ethernet1/0/23
port access vlan 400
#
interface Ethernet1/0/24
port link-type trunk
port trunk permit vlan 1 100 200 300 400
#
interface GigabitEthernet1/1/1
#
interface GigabitEthernet1/1/2
#
interface GigabitEthernet1/1/3
#
interface GigabitEthernet1/1/4
#
undo irf-fabric authentication-mode
#
interface NULL0
##
voice vlan mac-address 0001-e300-0000 mask ffff-ff00-0000
#
user-interface aux 0 7
user-interface vty 0
authentication-mode none
user privilege level 3
history-command max-size 20
idle-timeout 6 0
screen-length 30
protocol inbound telnet
user-interface vty 1 4
#
return
```

4.7.2.1.3. 测试

使用ping测试工具来测试VLAN划分后网络连接是否正常,这里以192.168.2.0网段为例

1. 检查客户机IP地址设置是否正确

☐ 自动获得 IP 地址 (I)

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

192 . 168 . 2 . 132

子网掩码 (U):

255 . 255 . 255 . 0

默认网关 (Q):

192 . 168 . 2 . 254

此为路由器上

VLAN200的网关

☐ 自动获得 DNS 服务器地址 (B)

☒ 使用下面的 DNS 服务器地址 (E):

首选 DNS 服务器 (E):

202 . 103 . 24 . 68

备用 DNS 服务器 (A):

图 4.42. 客户机IP地址实例

2. 客户机是否可以ping通网关

```
C:\Documents and Settings\Administrator>ping 192.168.2.254

Pinging 192.168.2.254 with 32 bytes of data:

Reply from 192.168.2.254: bytes=32 time<1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64
Reply from 192.168.2.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

图 4.43. 客户机ping网关

若ping的通，则VLAN配置成功；若ping不通网关，测试客户机是否可以ping通交换机VLAN接口IP地址

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=34ms TTL=255
Reply from 192.168.2.1: bytes=32 time=6ms TTL=255
Reply from 192.168.2.1: bytes=32 time=8ms TTL=255
Reply from 192.168.2.1: bytes=32 time=6ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 34ms, Average = 13ms
```

图 4.44. 客户机ping交换机vlan接口IP地址

这里一般都可以ping通，若ping不通，检查物理线路连接；若ping的通，测试是否可以ping通中继接口IP

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=13ms TTL=255
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time=7ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 13ms, Average = 7ms
```

图 4.45. 客户机ping中继接口IP地址

若ping不通，通过以下方法检测：

- 1.检查是否在交换机上配置了中继口以及中继口是否设置了允许所有VLAN通过
- 2.物理网络连接是否正确，路由与三层交换机之间不能存在其它硬件设配（集线器、网桥、交换机、路由器等等）
- 3. 默认情况下，路由允许各VLAN之间访问，下面以访问VLAN3网段为例

```
C:\Documents and Settings\Administrator>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=20ms TTL=255
Reply from 192.168.3.1: bytes=32 time=6ms TTL=255
Reply from 192.168.3.1: bytes=32 time=5ms TTL=255
Reply from 192.168.3.1: bytes=32 time=6ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 20ms, Average = 9ms
```

图 4.46. 客户机ping 交换机 VLAN3 接口的IP地址

```
C:\Documents and Settings\Administrator>ping 192.168.3.168

Pinging 192.168.3.168 with 32 bytes of data:

Reply from 192.168.3.168: bytes=32 time<1ms TTL=64
Reply from 192.168.3.168: bytes=32 time<1ms TTL=64
Reply from 192.168.3.168: bytes=32 time<1ms TTL=64
Reply from 192.168.3.168: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.168:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

图 4.47. 客户机ping VLAN3 网段中某一个客户机的IP地址

若不通，检测客户机是否开启了防火墙。



提示

在此种网络模式下，内网主机无论有没有配置本地IP地址，都可以直接PPPoE拨号穿透三层交换机到路由网关



4.6. 自定义路由表



4.8. 透明网桥



4.8. 透明网桥

4.8.1. 透明网桥典型实例

- 透明网桥简介

透明网桥工作在数据链路层，将两个LAN连起来，通过学习接收到数据包的MAC地址，在本地建立一个以MAC地址和网络接口对应的网桥表，并根据这张表来转发帧，可以看作是一个“低层的路由器”（但路由器工作在网络层，根据网络地址如IP地址进行转发）。

- 典型拓扑图

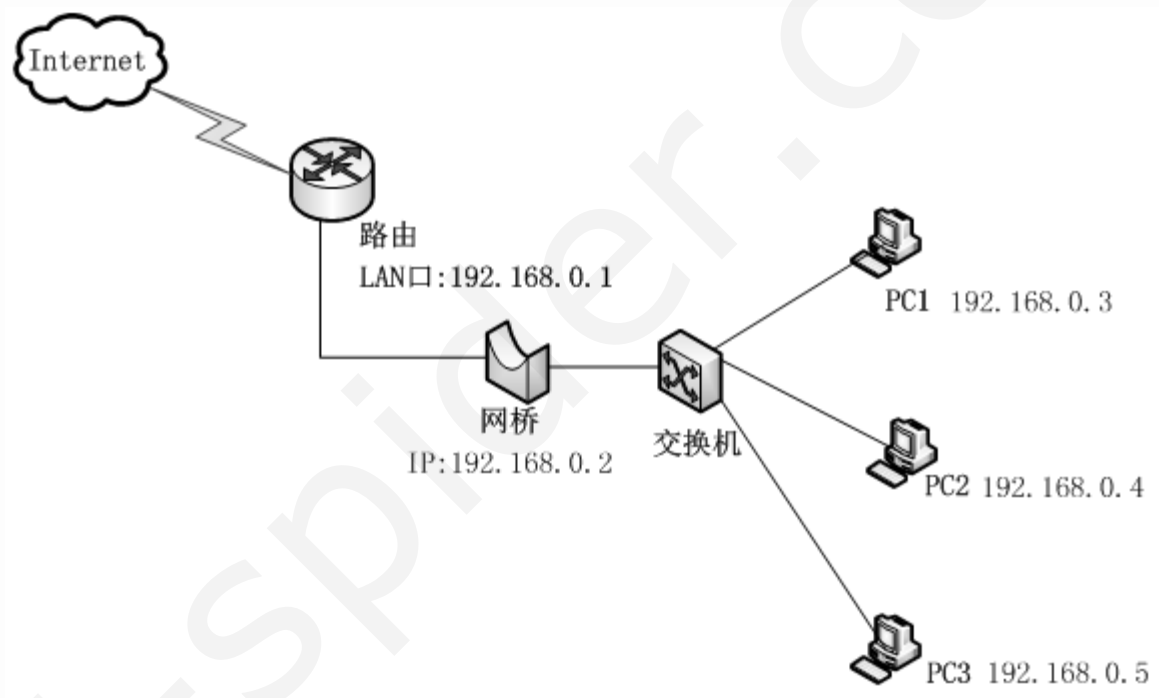


图 4.48. 透明网桥拓扑图

根据以上拓扑图可知，客户机IP和路由LAN口IP在同一网段，有没有网桥都不需要改变客户端IP地址，这也就是网桥对于客户机来说透明的原因了。交换机本来是可以直接与路由连接，中间多出一网桥的主要原因是交换机没有防火墙和流量控制这些功能，不能对客户机作一些限制操作，但是网桥可以。此种网络结构一般用于企业内部管理。

4.8.2. 启用透明网桥

Web登录海蜘蛛路由->“网络设置”->“透明网桥”设置页面，如下图所示：

☒ 启用透明网桥功能 (启用后 NAT 功能将不起作用)

MAC地址:			
MAC地址克隆:	<input type="text" value="00-30-18-d0-f4-c6"/>		
填透明网桥的 IP	IP地址:	<input type="text" value="192.168.0.2"/>	
	子网掩码:	<input type="text" value="255.255.255.0 (默认)"/>	[此网段可容纳 254 台机器]
扩展 IP 地址:	<div></div>		<div>IP地址: <input type="text"/></div> <div>子网掩码: <input type="text"/></div> <div>新增 删除</div>
	VLAN 网络地址:	<div></div>	
用于VLAN之间互访, 网络地址为VLAN网段的合集, 比如有 192.168.1.x - 192.168.5.x 5个VLAN, 则用 192.168.0.0/255.255.0.0 表示即可.			
填路由 IP	网关:	<input type="text" value="192.168.0.1"/>	
网桥出口 IP:	<input type="text"/> (一般不用填) 只有当网桥直接接外网且主IP为私有地址、扩展IP为公网地址时才需要设置		
网桥成员设备:	<input checked="" type="checkbox"/> LAN-1 (eth2/eth2/192.168.0.11/255.255.255.0)		
	<input checked="" type="checkbox"/> WAN-1 (eth0/eth0/220.249.XX.XX/255.255.255.224)		

图 4.49. 透明网桥设置

这里的IP地址填透明网桥自身的IP地址192.168.0.2，网关填路由的IP地址192.168.0.1。网桥成员设备勾选网桥两端连接的WAN口和LAN口。

重要

启用透明网桥功能后，NAT 功能将不起作用。

透明网桥的IP要和网关在同一网段。

启用或修改网桥设置后，需要等待约 20s 时间后才能重新访问到网桥，因为网桥有一个学习网络接口上接收到的数据包MAC地址的过程。

4.8.3. 透明网桥直接接外网

有时候我们需要将透明网桥直接连接外网，这时一般运营商会分给您一串公网IP地址，如这里是202.103.11.21-

202.103.11.23

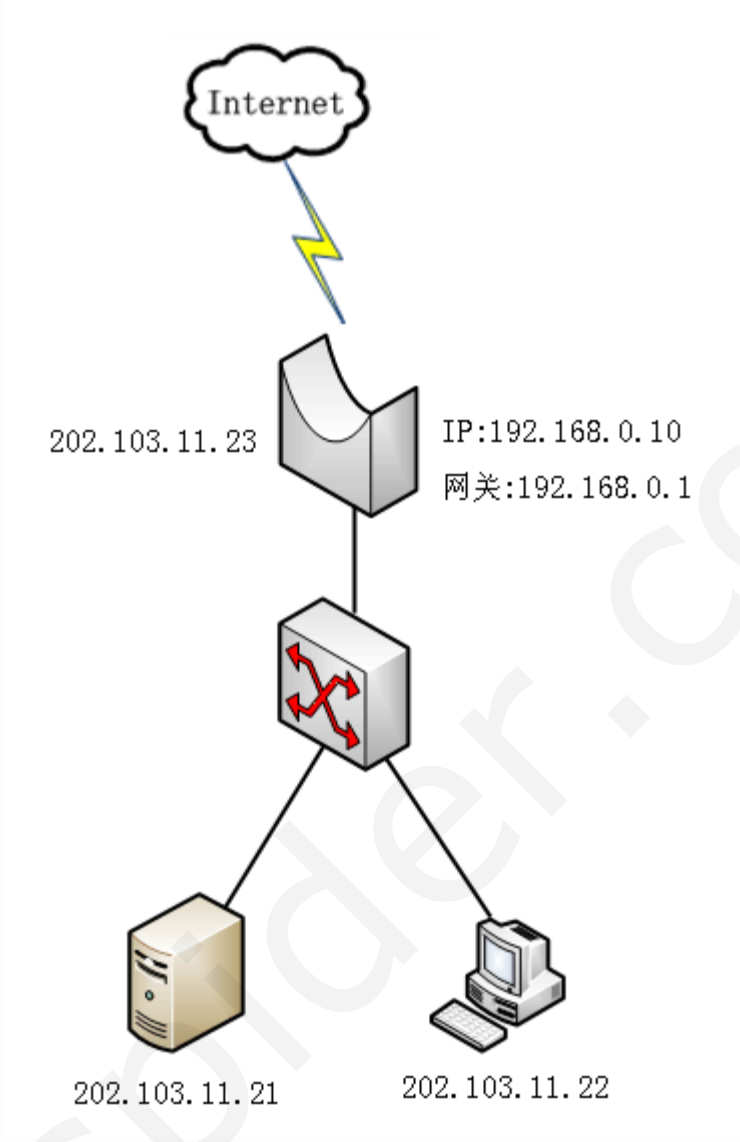


图 4.50. 网桥直接接外网

进入透明网桥设置页面，这里的IP地址填写此透明网桥的内网主IP地址，将运营商分配给您的IP地址和子网掩码填入扩展IP地址，下面的网桥出口IP地址填写此透明网桥的公网IP地址。

☒ 启用透明网桥功能 (启用后 NAT 功能将不起作用)

MAC地址:			
MAC地址克隆:	<input type="text" value="90-E6-BA-DC-27-A1"/>		
网桥IP地址	IP地址:	<input type="text" value="192.168.0.10"/>	
	子网掩码:	<input type="text" value="255.255.255.0 (默认)"/>	[此网段可容纳 254 台机器]
扩展 IP 地址:	<div><div>202.103.11.23 / 255.255.255.224 202.103.11.22 / 255.255.255.224 202.103.11.21 / 255.255.255.224</div><div>填写运营商分配的公网 IP地址和子网掩码</div></div>	IP地址:	<input type="text" value="202.103.11.23"/>
		子网掩码:	<input type="text" value="255.255.255.224"/> <input type="button" value="新增"/> <input type="button" value="删除"/>
VLAN 网络地址:	<div></div>	网络地址:	<input type="text"/>
		子网掩码:	<input type="text"/> <input type="button" value="新增"/> <input type="button" value="删除"/>
用于VLAN之间互访, 网络地址为VLAN网段的合集, 比如有 192.168.1.x - 192.168.5.x 5个VLAN, 则用 192.168.0.0/255.255.0.0 表示即可.			
出口IP为网桥连接外网的IP地址	网关:	<input type="text" value="192.168.0.1"/>	
	网桥出口 IP:	<input type="text" value="202.103.11.23"/> (一般不用填)	只有当网桥直接接外网且主IP为私有地址、扩展IP为公网地址时才需要设置

图 4.51. 网桥接外网设置

设置好后，此透明网桥会和外网运营商路由相连接，再由运营商路由来完成数据转发。



第 5 章 快速接入互连网

目录

[5.1. 局域网 \(LAN\) 设置](#)

[5.2. 设置 DNS 参数](#)

[5.3. 设置广域网 \(WAN\)](#)



注意

设置之前，请先确认网卡、局域网、广域网等已经正常连接好。

下面将以单线路接入为例来配置快速接入互连网。

5.1. 局域网 (LAN) 设置

海蜘蛛路由系统 (Hi-Spider Router) 默认的路由器 IP 地址为 192.168.0.1，用户可以直接采用路由器默认的 IP 地址作为局域网的网关地址。

此时客户端网络链接可以如下设置：

☒ 使用下面的 IP 地址(S):

IP 地址(I):	192 . 168 . 0 . 2
子网掩码(U):	255 . 255 . 255 . 0
默认网关(D):	192 . 168 . 0 . 1

图 5.1. 客户机IP设置

您同样可以根据以下方法修改IP地址或者加入扩展IP地址：

1. 修改局域网 IP 地址

可通过 控制台 和 Web远程管理 两个途径修改局域网IP地址：

- 通过控制台修改局域网IP

控制台修改 IP 可参考：安装指南 [2.8.2 修改LAN口 IP 地址](#)。

- 通过Web远程管理修改局域网IP

在客户机浏览器地址栏输入路由器局域网 IP 或扩展 IP 地址，如打开：<http://192.168.0.1:880> 后输入 admin:admin 登录到 Web 远程管理页面，进入“网络设置”->“局域网 (LAN)”，在“IP 地址”输入框中填入您要分配给路由器局域网接口的 IP 地址，并选择相应的“子网掩码”，点击“保存设置”即可。

2. 修改局域网扩展 IP 地址

登录到 Web 远程管理页面，进入“网络设置”->“局域网 (LAN)”，在“扩展 IP 地址”右侧“IP 地址”和“子网掩码”输入

框中填入您要添加的扩展 IP 地址和子网掩码， 点击“增加”->“保存设置”即可。

• 通过子网掩码扩展IP

例如：若一个局域网的计算机数量有500台，则可设置其网关IP为192.168.0.1，子网掩码为255.255.254.0，此时局域网中的计算机的IP地址为192.168.0.2-192.168.1.254之间。如图所示：

物理连接状态:	已连接, 速度: 100Mb/s (工作模式: 全双工)		
MAC地址:	<input type="text" value="00-13-46-77-8a-3f"/>		
MAC地址克隆:	<input type="text"/>		
IP地址:	<input type="text" value="192.168.0.1"/>		
子网掩码:	<input type="text" value="255.255.254.0"/>	<input type="button" value="v"/>	[此网段可容纳 510 台机器]
扩展 IP地址:	<div><div><div></div></div><div><div>IP地址:</div><div><input type="text"/></div></div><div><div>子网掩码:</div><div><input type="text"/></div></div><div><div>增加</div><div>删除</div></div></div>		

图 5.2. 子网掩码扩展IP

• 通过划分网段扩展IP

例如：同样一个局域网包含500台计算机，可设置网关IP为192.168.0.1，子网掩码为255.255.255.0，此网段中的IP地址为192.168.0.2-192.168.0.254之间。

设置扩展IP为192.168.1.1，子网掩码为255.255.255.0。此网段中的IP地址为192.168.1.2-192.168.1.254，如图所示：

物理连接状态:	已连接, 速度: 100Mb/s (工作模式: 全双工)		
MAC地址:	<input type="text" value="00-13-46-77-8a-3f"/>		
MAC地址克隆:	<input type="text"/>		
IP地址:	<input type="text" value="192.168.0.1"/>		
子网掩码:	<input type="text" value="255.255.255.0 (默认)"/>	<input type="button" value="v"/>	[此网段可容纳 254 台机器]
扩展 IP地址:	<div><div><div>192.168.1.1 / 255.255.255.0</div></div><div><div>IP地址:</div><div><input type="text" value="192.168.1.1"/></div></div><div><div>子网掩码:</div><div><input type="text" value="255.255.255.0"/></div></div><div><div>增加</div><div>删除</div></div></div>		

图 5.3. 划分网段扩展IP



提示

海蜘蛛路由系统（Hi-Spider Router）默认的 Web 远程管理端口为 880，帐户名和密码均为 admin。

用 Web 远程管理 方式修改了路由器的局域网 IP 地址后，需要在浏览器地址栏中输入新的 IP 地址重新登录。

以上两种方法都可以扩展IP地址，通过划分网段扩展IP多一个LAN访问地址。

3. 设置客户机网关

客户机的网关要设为路由器的局域网 IP 或扩展 IP 地址才能接入互连网，以 Windows 操作系统为例，鼠标左键单击“开始”->“设置”->“网络连接”，右键点击“本地连接”，选择“属性”-> “Internet 协议（TCP/IP）”->“属性”，修改“默认网关”为路由器的局域网 IP 或扩展 IP 地址，如：192.168.1.1

☐ 自动获得 IP 地址 (A)

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

192 . 168 . 1 . 2

子网掩码 (U):

255 . 255 . 255 . 0

默认网关 (Q):

192 . 168 . 1 . 1

图 5.4. 设置客户机网关



提示

此时客户机的IP地址可设置为192.168.1.2—192.168.1.254中的任意一个，局域网内每台计算机的IP地址都不能一样。

如果您的路由两个LAN口各直接连接二层交换机，在默认情况下两LAN之间的主机是可以互访的，如果要设置它们不能互访，需在 LAN 间互访 页面里禁用互访。

LAN-1

LAN-2

LAN 间互访

☒ 禁止 LAN-1 <--> LAN-2 之间相互访问

保存设置

重置

图 5.5. 禁止LAN间互访

提示



如果需要在此基础上设置某台主机允许访问另一局域网，只需将其主机的IP地址加入防火墙的白名单中，如图：

☒ 启用防火墙白名单功能

白名单列表（每条记录占一行）：[清空列表](#)

192.168.1.33



4.8. 透明网桥



5.2. 设置 DNS 参数

5.2. 设置 DNS参数



小知识

DNS即域名解析协议，实现域名与IP地址之间的转换。如我们上网时输入www.sina.com.cn 网址时，DNS会把它转换为计算机可识别的IP地址218.30.6.101（申请）

登录 Web 远程管理，进入“网络设置”->“DNS参数”。

DNS获取方式分为 手动指定 和 自动获取 两种。

若选择“手动指定”，用户需输入运营商提供的“首选DNS”和“辅助DNS”，点击“保存设置”即可，如下图所示：

DNS 获取方式:	<div>自动获取</div> <div>手动指定</div> <div>自动获取</div>	<div>一般手动指定静态IP</div> <div>自动获取动态IP</div>	
首选 DNS:	<input type="text" value="208.67.220.68"/>	运营商:	<div>中国电信</div>
辅助 DNS:	<input type="text" value="208.67.220.220"/>	运营商:	<div>中国联通/网通</div>
可选 DNS-1:	<input type="text"/>	运营商:	<div>中国电信</div>
可选 DNS-2:	<input type="text"/>	运营商:	<div>中国电信</div>
可选 DNS-3:	<input type="text"/>	运营商:	<div>中国电信</div>
可选 DNS-4:	<input type="text"/>	运营商:	<div>中国电信</div>
		<div>保存设置</div> <div>重设</div> <div>诊断</div> <div>诊断日志</div>	

图 5.6. 设置 DNS参数



提示

您可以填入“可选 DNS”服务器地址，以便在网络运营商提供的 DNS 服务器失效时域名能够正常解析。

若域名解析出现故障，可在dos环境下输入nslookup命令查看有关域名解析信息，这里我们以查看百度为例，如下图所示。

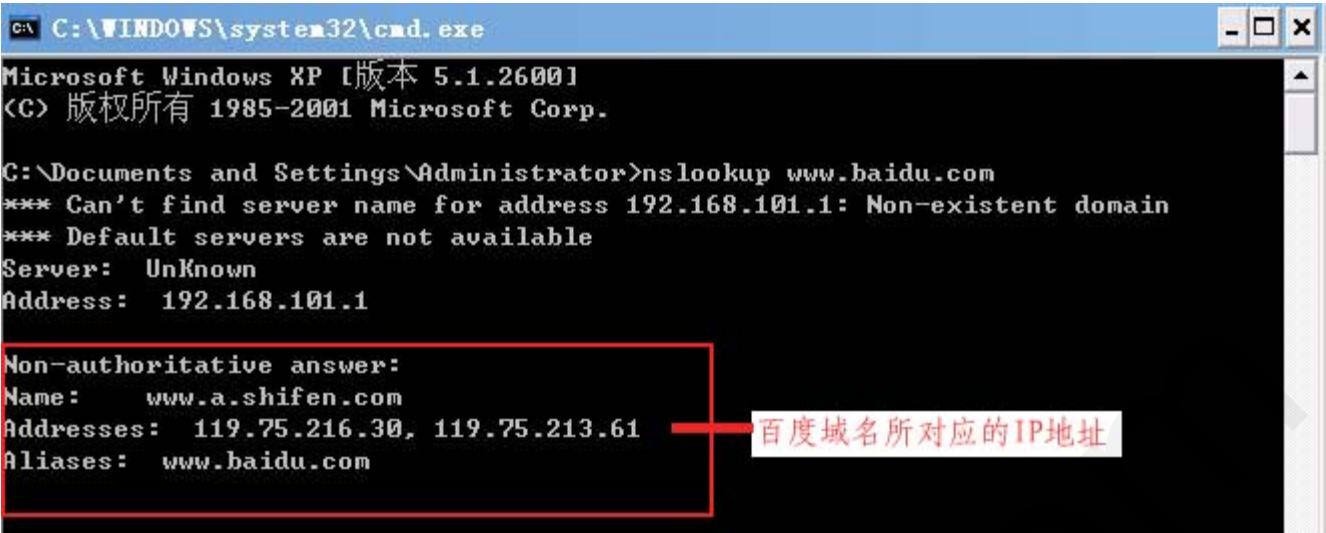


图 5.7. 查看百度IP地址



提示

这里我们可以在IE地址栏中输入address后的IP地址同样可以登录百度主页。





5.3. 设置广域网 (WAN)

广域网接入方式有三种：静态IP接入、动态IP接入、ADSL/PPPoE拨号上网

用户可以登录路由器，进入“网络设置”->“广域网 (WAN)”，在internet接入方式中选择适合自己的WAN接入方式，如图：

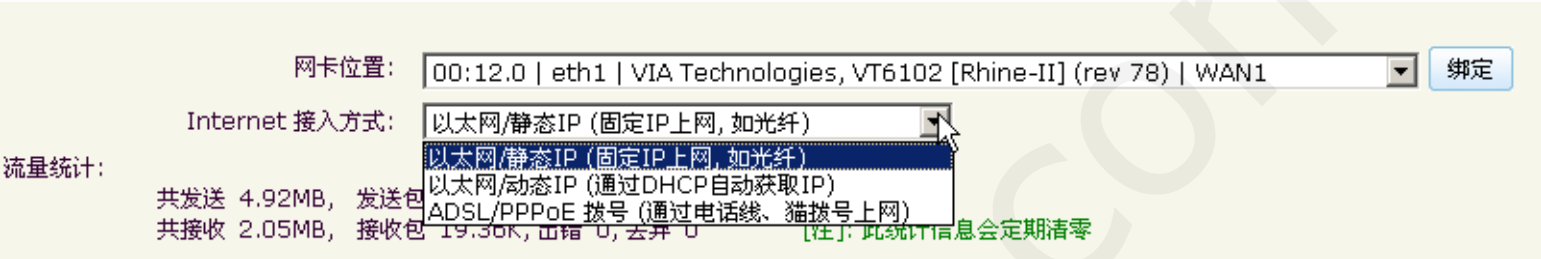


图 5.8. 选择 Internet 接入方式



小知识

静态IP：也叫固定IP，由网络运营商分配。

动态IP：由于IP地址资源短缺，通过 ADSL 拨号上网用户一般不具备固定的IP地址，而是由DHCP服务器自动分配的临时IP地址，用户每一次被分配的IP都不一样。

- 以太网/静态IP（固定IP上网，如光纤）

通过网络运营商分配的固定IP地址、子网掩码、网关等上网。此种接入方式一般用于网吧、大型公司。

选择“Internet 接入方式”为“以太网/静态IP”，在“IP 地址”，“子网掩码”和“网关”输入框中分别填入网络运营商分配给您的 IP 地址、子网掩码、网关。如下图：

IP地址:	<input type="text" value="192.168.100.9"/>
子网掩码:	<input type="text" value="255.255.255.0 (默认)"/> [此网段可容纳 254 台机器]
网关:	<input type="text" value="192.168.100.1"/>

图 5.9. 设置静态 IP 地址

- 以太网/动态IP（通过DHCP自动获取IP）

通过 DHCP 协议自动从网络运营商的 DHCP 服务器获得 IP 地址、子网掩码、网关等上网。

选择“Internet 接入方式”为“以太网/动态IP（通过DHCP自动获取IP）”即可。



小知识

DHCP：即动态主机配置协议，提供主机IP地址的动态租用配置、并将其他配置参数分发给合法网络客户端的 **TCP/IP** 服务协议。**DHCP** 提供了安全、可靠、简便的 **TCP/IP** 网络配置，能避免地址冲突，并且有助于保留网络上客户端 IP 地址的使用。**DHCP** 使用客户端/服务器模式，通过这种模式，**DHCP** 服务器集中维持网络上使用的 IP 地址的管理。然后，支持 **DHCP** 的客户端就可以向 **DHCP** 服务器请求和租用 IP 地址，以接入网络。

• ADSL/PPPoE拨号（通过电话线、猫拨号上网）

通过网络运营商提供的 **ADSL/PPPoE** 帐户名和密码拨号上网，目前普通家庭的宽带连接大都采用**ADSL**拨号上网。

选择“Internet 接入方式”为“**ADSL/PPPoE**拨号（通过电话线、猫拨号上网）”，在“**PPPoE** 拨号用户名”和“**PPPoE** 密码”输入框中分别填入网络运营商提供给您**的 ADSL** 帐户名和密码保存即可。

PPPoE 断线后会自动重新拨号，无需手动重拨。

PPPoE 拨号用户名：	<input type="text" value="test"/>	在此WAN口上捆绑多个帐号（已绑定 0，激活 0）
PPPoE 密码：	<input type="password" value="••••"/>	

图 5.10. ADSL/PPPoE拨号

WAN口带宽限速根据实际应用来调整，比如接入的是**10M**的**ADSL**，那么上行带宽**512Kbit**，下行带宽**10Mbit**，就按如下配置

带宽：	下行：	<input type="text" value="10"/>	<input type="text" value="Mbit"/>	， 上行：	<input type="text" value="512"/>	<input type="text" value="Kbit"/>	<input checked="" type="checkbox"/> 限制总下行	<input checked="" type="checkbox"/> 限制总上行	<input type="button" value="确定"/>
-----	-----	---------------------------------	-----------------------------------	-------	----------------------------------	-----------------------------------	---	---	-----------------------------------

图 5.11. WAN口限速

这里必须勾选后面的限制总上下行，点击后面的确定才有效，这里和路由上其它功能如流控**QOS**配合需配置准确。

MAC地址克隆用于运营商对用户这边的网卡绑定或者通过绑定**MAC**来限制私接路由：

MAC地址：	<input type="text" value="bc-ae-c5-ac-96-27"/>
MAC地址克隆：	<input type="text" value="b0-51-8e-00-ab-a5"/>


图 5.12. MAC地址克隆

广域网接口的其它设置：

运营商:	中国电信	(启用多线策略及负载时需要)
关闭网卡自动协商功能:	<input type="checkbox"/> 是	根据实际情况选择运营商
工作模式:	自动设置	
速度:	自动设置	
负载权重:	1	
其他参数:	<input type="checkbox"/> 启用调试 <input type="checkbox"/> 不自动加入多线负载 <input type="checkbox"/> 禁止NAT	
线路检测:	运行中 (PID:1867)	[检测日志 清除]

图 5.13. 配置图

网络运营商根据您的实际情况选择，负载权重指此WAN口占总网络应用的比例大小，例如两条线WAN1设置负载权重1，WAN2设置负载权重2，那么在其它设置一样的情况下WAN2会占网络总流量的2/3，WAN1仅占网络总流量的1/3。多线路接入时才需要开启线路检测。

 注意

设置单线路工作时，不论选择何种 Internet 接入方式，以下两项，一般都选上。

此网关作为默认路由:	<input checked="" type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)

图 5.14. 单线设置



第 6 章 3G无线接入设置

目录

[6.1. 3G无线上网简介](#)

[6.2. 参数设置](#)

[6.3. 设置多线负载及策略](#)

[6.4. 支持的3G无线上网卡](#)

6.1. 3G无线上网简介

随着国内3G市场日渐成熟，越来越多用户趋向于用无线上网卡来上网。无线上网可以不受地域的控制，做到网随人走，而且3G的数据下载比普通家庭用的宽带还要快。目前中国市场有移动的TD-CDMA，联通的WCDMA，电信的2000-EVDO三种网络制式的无线上网卡。国内销售的3G上网卡主流品牌有华为和中兴。

下面举一个应用案例来介绍3G无线配置。

现有中国联通的ADSL和中国联通的WCDMA两条外网线路，我们将ADSL宽带设为主线路，将WCDMA设置为备用线路。



提示

无线上网的费用较高，所以设置为备用线路。

网络结构如下：

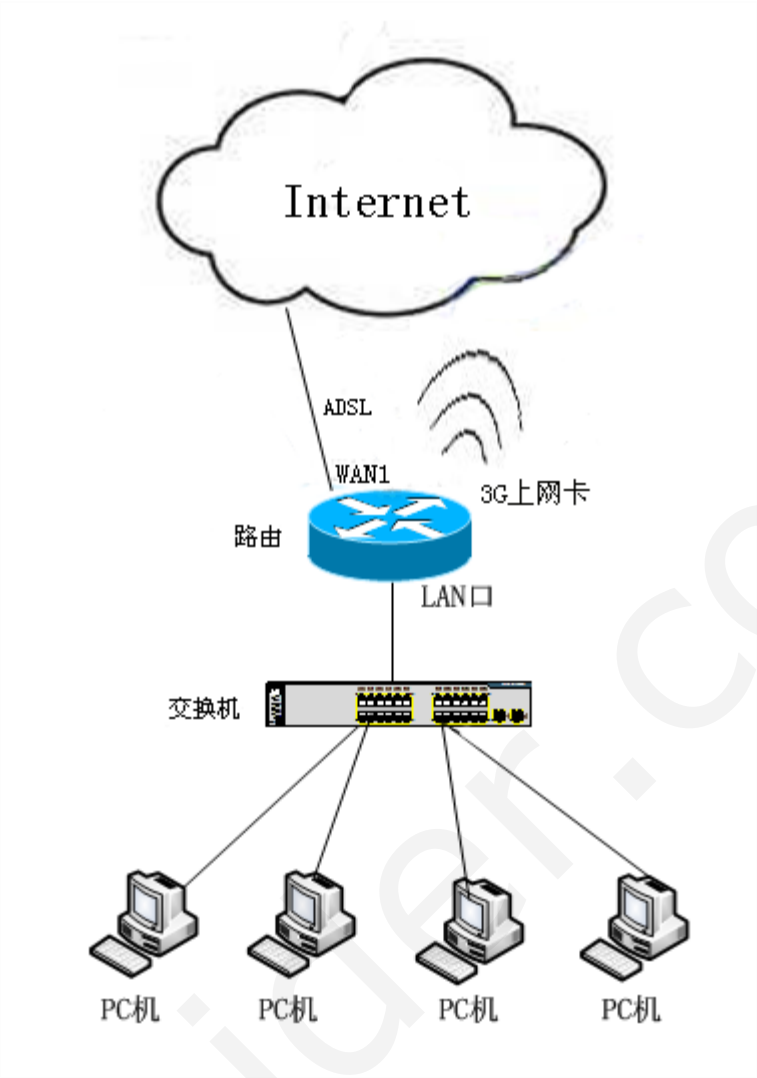


图 6.1. 网络拓扑图



5.3. 设置广域网 (WAN)



6.2. 参数设置

6.2. 参数设置

登录 Web 远程管理，进入“网络接口配置”->“3G无线接入”，如图：

带宽：	下行：3 Mbit， 上行：3 Mbit	<input type="checkbox"/> 限制总下行 <input type="checkbox"/> 限制总上行	确定
网卡位置：	* Bus 001 Device 004: ID 19d2:0031 ONDA Communication S.p.A. ZTE MF636		
线路别名：	wcdma-3g <small>别名只能由汉字、数字、大小写字母、下划线、圆点及减号组成</small>		
协议类型：	WCDMA		
用户名：	XXXXXX		
密码：	●●●●●●		
电话号码：	<input type="text"/> (WCDMA 默认为 *99#, 其他默认为 #777)		
波特率：	115200 (默认为 115200)		
网关：	<input type="text"/> (255.255.255.255 表示使用本地IP作为网关, 不确定请留空)		
额外初始化指令：	<input type="text"/>		
最大传输单元(MTU)：	1492 (默认为 1492)		
最大接收单元(MRU)：	1492 (默认为 1492)		
发送 LCP(连接控制协议)数据包间隔：	20 s (20~60)		
多少个LCP请求未应答则断开连接：	3 (3~6)		
开机自动启动：	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)		
负载权重：	1 ?		
其他参数：	<input type="checkbox"/> 默认路由 ? <input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?		
运营商：	中国联通 (用于多线策略及负载)		

图 6.2. 3G上网参数

选择您所使用的无线上网卡，这里使用的是ZTE MF636 3G上网卡。选择上网卡所支持的带宽上下线，选择相应的运营商和协议类型，这里使用的是中国联通的WCDMA，用户名和密码选择相应运营商所提供的（有时可以为空），线路别名可以自定义，其它都为默认设置。

设置好后保存设置，点击连接，过会儿显示3G网络连接成功，如图：

连接状态: 正常, 3G 网络连接成功 !

连接名:	ppp0
上线时间:	2010-07-22 11:09:20
已连接时间:	0 天 2 小时 38 分 29 秒
IP地址:	172.24.23.39
网关:	10.64.64.64
流量统计:	发送字节 234.90 KB, 发送包 2.42K, 出错 0, 丢弃 0 接收字节 1.08 MB, 接收包 4.14K, 出错 0, 丢弃 0

保存设置

重设

断开

删除配置

图 6.3. 3G上网连接

连接成功后，会在主页面的网络接口状态多出一个3G上网的图标：

网络接口状态

LAN1

LAN2

WAN1

WAN2

PPTP-1

wcdma-3g

系统监测

内网监测

线路检测

图 6.4. 3G上网图标





6.3. 设置多线负载及策略

按照[设置广域网 \(WAN\)](#) 来设置好联通ADSL线路。

再进入“网络接口配置”->“3G无线接入”，勾选“不自动加入多线负载”，如下图：

网卡位置:	Bus 001 Device 003: ID 12d1:1001 Huawei Technologies Co., Ltd. E620 USB Modem
协议类型:	WCDMA
用户名:	<input type="text"/> (如果不确定, 请留空, 默认为 CARD)
密码:	<input type="password"/> (如果不确定, 请留空, 默认为 CARD)
电话号码:	<input type="text"/> (WCDMA 默认为 *99#, 其他默认为 #777)
波特率:	115200 (默认为 115200)
网关:	<input type="text"/> (255.255.255.255 表示使用本地IP作为网关, 不确定请留空)
额外初始化指令:	<input type="text"/>
最大传输单元(MTU):	1492 (默认为 1492)
最大接收单元(MRU):	1492 (默认为 1492)
发送 LCP(连接控制协议) 数据包间隔:	20 s (20~60)
多少个LCP请求未应答则断开连接:	3 (3~6)
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)
负载权重:	1 ?
其他参数:	<input type="checkbox"/> 默认路由 ? <input type="checkbox"/> 启用调试 ? <input checked="" type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?
运营商:	中国联通 (用于多线策略及负载)
线路检测:	已禁用 [检测日志 清除]

图 6.5. 不自动加入多线负载

然后进入“网络设置”->“多线负载及策略”，选择启用多线负载及策略，并将策略路由工作模式设置为“正常模式、掉线自动切换”，如图：

☒ 启用多线负载及策略

线路设置...

策略路由工作模式: 正常模式、掉线自动切换

图 6.6. 启用多线负载及策略

这里下面会显示已设置好的的两条线路WAN1和3GNET1，线路类型都设置为默认线路，如图：

线路	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国联通	eth0/eth0/220.249.124.205/255.255.255.224	默认线路	中国联通 (232 条 v3.4)	<input checked="" type="checkbox"/> 是
3GNET1	中国联通	3g/ppp0/172.28.2.94/255.255.255.255	默认线路	中国联通 (232 条 v3.4)	<input checked="" type="checkbox"/> 是

保存设置后，正常情况下，内网数据都只会走WAN1，当WAN1的线路出故障时，路由就会自动转由3GNET1的线路来无线上网。



6.2. 参数设置



6.4. 支持的3G无线上网卡

6.4. 支持的3G无线上网卡

第 6 章 3G无线接入设置

6.4. 支持的3G无线上网卡

目前3G无线接入支持以华为中兴为主的USB或Mini PCI-E接口无线上网卡，网络类型支持WCDMA、TD-CDMA、CDMA1x和CDMA2000-EVDO。

- 联通的WCDMA，支持如：华为 E1750、EM770、E261，中兴 MF637U，Sierra MC8775



图 6.7. 华为 E1750



图 6.8. 华为 EM770

- 在移动的TD-CDMA方面，支持如：华为 ET128，中兴 MU350



图 6.9. 华为 ET128

- 在电信的CDMA1x和CDMA2000-EVDO方面，支持如：华为 EC122、EC1260、EC1261、EM660、MC703，中兴 ZTE AC2746



图 6.10. 华为 EC122



6.3. 设置多线负载及策略



部分 IV. 防火墙



部分 IV. 防火墙

目录

[7. 基本安全设置](#)

[7.1. 普通模式](#)

[7.2. 高级应用](#)

[7.3. 特殊应用](#)

[8. 黑白名单](#)

[9. IP-MAC绑定](#)

[9.1. IP与MAC地址绑定的作用](#)

[9.2. 启用IP与MAC绑定](#)

[10. DNS/IP过滤](#)

[10.1. 什么是DNS/IP过滤](#)

[10.2. 启用DNS/IP过滤](#)

[11. 网址/关键字过滤](#)

[11.1. 网址/关键字过滤的好处](#)

[11.2. 规则说明](#)

[11.3. 启用网址/关键字过滤](#)

[12. ACL 规则](#)

[13. 端口镜像](#)

[13.1. 端口镜像简介](#)

[13.2. 设置步骤](#)

[14. 端口映射](#)

[14.1. 端口映射简介](#)

[14.2. 启用端口映射](#)

[14.3. 端口映射不成功，如何找出问题原因](#)

[14.4. 端口443映射不成功的原因](#)

[15. DMZ主机](#)

[15.1. DMZ简介](#)

[15.2. DMZ主机设置](#)

[16. UPnP支持](#)

- [16.1. UPnP简介](#)
- [16.2. 启动UPnP服务](#)

[17. 一对一NAT](#)

- [17.1. 一对一NAT简介](#)
- [17.2. 启动一对一NAT服务](#)
- [17.3. 一对一NAT与端口映射及DMZ的区别](#)

[18. No NAT](#)

- [18.1. No NAT简介](#)
- [18.2. 启动No NAT功能](#)



6.4. 支持的3G无线上网卡



第 7 章 基本安全设置



第 7 章 基本安全设置

目录

- [7.1. 普通模式](#)
- [7.2. 高级应用](#)
- [7.3. 特殊应用](#)

7.1. 普通模式

- ICMP-Flood 攻击防御

防止路由对 ICMP ping 产生的大量回应请求超出了系统的最大限度，以至于系统耗费所有资源来进行响应直至再也无法处理有效的网络信息流。启用此功能可以控制每个IP每秒最大允许的 ICMP 包个数，超过部分自动丢弃。

- TCP SYN 连接数限制

启用此功能可以控制每个IP每秒最大允许发起的 TCP 新连接数，超过部分自动丢弃。

- UDP-Flood 攻击防御

UDP-Flood 攻击是利用大量UDP小包冲击服务器。攻击者可发送大量伪造源IP地址的小UDP包，只要服务器开了一个UDP的端口提供相关服务的话，那么就可针对相关的服务进行攻击。启用此功能可以控制每个IP每秒最大允许的 UDP 包个数，超过部分自动丢弃。



注意

以上三项功能网吧用户可以不用勾选，否则可能会有部分游戏掉线等问题。

- DNS 攻击防御

启用此功能可以控制每个IP每秒最大允许发起的 DNS 请求数，超过部分自动丢弃。用以防止 DNS 请求超出了服务器承载范围。

- IP 碎片(Fragment) 攻击防御

对于IP数据包长度超过65535字节就会产生IP碎片，如果分片之间偏移量经过精心构造，一些系统就无法处理，最后导致系统出错。 启用此功能可以控制每个IP每秒最大允许的 UDP 包个数，超过部分自动丢弃。

- 修改 TCP 数据包的最大报文长度，随线路自动调整

ADSL用户用户需要勾选，否则可能出现开网页慢或者打不开的情况；如果光纤用户打开网页缓慢也可以勾选此选项。





7.2. 高级应用

- 防止外部源路由欺骗：防止攻击者通过自封包和修改网络节点的IP地址，冒充某个可信节点的IP地址，进行攻击。
- 防止 Smurf DoS 攻击：防止由ICMP应答请求(ping)数据包，来淹没受害主机，或拒绝服务而导致网络阻塞。
- 启用 SYN Cookie 功能：SYN Flood 攻击发送了大量伪造的TCP连接请求，使得被攻击方资源耗尽，无法及时回应或处理正常的服务请求。
- 防止 TCP Land 攻击：TCP Land 攻击会产生源端口和目的端口相同的ICMP echo 报文或TCP syn 请求报文，导致主机不断地向自己发送报文，最终导致系统崩溃。通过报文的源地址和目的地址是否相等来判断 TCP Land 攻击。
- Proxy ARP 功能：代理ARP能够将一个主机作为对另一个主机ARP进行应答。使得在不影响路由表的情况下添加一个新的Router
- 修改IPID为随机数：指的修改网络身份标识号码。





7.3. 特殊应用

以下两项当内网PPTP_VPN 客户端访问外网 PPTP_VPN 服务端时需选上。

- PPTP_VPN NAT 穿透支持
- GRE 协议穿透支持

其它特殊应用协议简介：

- DCCP 协议 和 SCTP 协议：数据报拥塞控制协议和流控制传输协议，用于数据传输和递交实现多流传送。
- UDPLite 协议：类似于UDP协议，应用于网络的差错率比较大，但是对轻微差错不敏感的网络环境。
- H.323/SIP 协议：用于应用层的信令控制，实现多方会话，主要应用于网络语音、视讯。
- TFTP 协议：简单文件传输协议，用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。
- IRC 协议：因特网在线聊天协议，用于客户端软件以IRC协议通过因特网连接到一台IRC服务器。
- NetBIOS 协议：网络基本输入/输出系统协议，使用户能够通过应用程序编程接口来访问局域网的资源。





第 8 章 黑白名单

黑白名单中的IP或者MAC地址将不经过防火墙规则优先处理，即防火墙里定义的一些过滤规则（DNS/IP过滤、URL/keywords过滤）对位于白名单列表中的IP/MAC地址无效。

• 白名单

IP/MAC绑定、DNS/IP过滤、网址关键字过滤、ACL、上网行为管理规则对位于白名单中的IP地址无效。

格式举例：

192. 168. 0. 123	IP地址为192. 168. 0. 123的客户机
192. 168. 0. 10-192. 168. 0. 20	IP地址从192. 168. 0. 10到192. 168. 0. 20的所有客户机
192. 168. 0. 0/24	IP地址从192. 168. 0. 1到192. 168. 0. 254的所有客户机
192. 168. 0. 0/255. 255. 255. 0	同上

同时也支持加载预定义对象中的 IP 对象规则名称，在“上网行为管理”->“预定义对象”里新增IP对象，如下图所示：

编辑...

名称：	<input type="text" value="11"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
备注：	<input type="text" value="BOSS"/>	
共 1 条记录 清空列表		
172. 16. 11. 100-172. 16. 11. 120		

然后在防火墙白名单列表中输入如下所示规则：

☒ 启用防火墙白名单功能

白名单列表 (每条记录占一行): [清空列表](#)

@11
@18 127. 1. 1. 1
172. 16. 2. 42

这就直接利用了预定义IP对象里名称为11的规则，相当于172.16.11.100-172.16.11.120这一段IP地址已经加入白名单了。

格式举例：

@11	表示名称为11的这条规则中的IP地址不经过防火墙规则优先处理
@11 119. 75. 216. 20	表示名称为11的这条规则中的IP地址可以访问119. 75. 216. 20

• 黑名单

黑名单可以用来禁止局域网某些IP访问局域网或者互联网，书写规则如下所示：

00-12-34-56-78-ab	表示MAC地址为00-12-34-56-78-ab的客户机不能访问路由网关及上网
@11	表示名称为11的这条规则中的IP地址不能访问路由网关以及局域网IP
@11 119. 75. 216. 20	表示名称为11的这条规则中的IP地址不能访问119. 75. 216. 20，可以
正常访问其它网站	
@11 @12	表示名称为11的这条规则中的IP不能访问名称为12的这条规则中的IP

使用@加载预定义对象的规则的方法同样也适合在ACL规则中使用，如下图所示：

优先级：	<input type="text" value="10"/> (只能为数字，数字越小优先级越高)
协议类型：	<input type="text" value="TCP+UDP"/>
数据流向：	<input type="text" value="转发"/>
源IP：	<input type="text" value="@11"/>
源端口：	<input type="text"/>
目的IP：	<input type="text" value="@12"/>
目的端口：	<input type="text"/>
匹配数据包大小：	<input type="text"/> - <input type="text"/> bytes
时间限制：	<div><input type="checkbox"/> 启用</div> <div><div>起始日期 <input type="text"/></div><div>结束日期 <input type="text"/></div><div>起始时间 <input type="text"/></div><div>结束时间 <input type="text"/></div></div> <div>星期：<input type="checkbox"/>一 <input type="checkbox"/>二 <input type="checkbox"/>三 <input type="checkbox"/>四 <input type="checkbox"/>五 <input type="checkbox"/>六 <input type="checkbox"/>日 <input type="checkbox"/>工作日 <input checked="" type="checkbox"/>全部</div>
动作：	<input type="text" value="拒绝"/> <input type="checkbox"/> 并记录到日志, 日志标识: <input type="text"/>
备注：	<input type="text" value="-"/>
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用





第 9 章 IP-MAC绑定

目录

[9.1. IP与MAC地址绑定的作用](#)

[9.2. 启用IP与MAC绑定](#)

9.1. IP与MAC地址绑定的作用

IP与MAC地址绑定的作用

- IP与MAC地址绑定可以严格控制局域网主机，防止局域网用户随意改变自己的 IP 地址来获得非法权限或导致 IP 冲突
- 服务器与客户机通讯时将使用静态 ARP 表，可以减少局域网内的 ARP 广播流量



9.2. 启用IP与MAC绑定

Web登录海蜘蛛路由->防火墙->IP-MAC绑定，勾选 启用IP与MAC地址绑定，然后点击扫描导入。即可将局域网所有计算机的IP与MAC地址载入绑定列表框即可完成IP与MAC地址的绑定。

☒ 启用IP与MAC地址绑定

绑定列表

强制绑定

ID	IP地址	MAC地址	备注	状态	编辑	删除
1	192.168.100.53	96-3c-6e-53-04-15	ARP_扫描	✓		
2	192.168.100.66	f6-03-77-94-b8-d4	ARP_扫描	✓		
3	192.168.100.67	96-18-03-da-34-92	ARP_扫描	✓		
4	192.168.100.68	04-c8-d2-2e-11-23	ARP_扫描	✓		
5	192.168.100.69	04-c8-d2-2e-11-24	ARP_扫描	✓		
6	192.168.100.80	06-c1-49-76-cb-9b	ARP_扫描	✓		
7	192.168.100.97	c8-60-00-83-94-96	ARP_扫描	✓		
8	192.168.100.100	52-54-00-12-99-16	ARP_扫描	✓		
9	192.168.100.115	14-da-e9-75-de-cd	ARP_扫描	✓		
10	192.168.100.119	14-da-e9-75-de-e2	ARP_扫描	✓		

进入强制绑定页面，启用 强制进行 IP/MAC 地址绑定 后，则只允许绑定列表中 MAC 地址匹配的 IP 访问 Internet，否则会弹出访问受限提示。

访问受限

尊敬的用户：

您好！

由于您的 IP 不在防火墙的IP / MAC地址绑定列表内，您将无法访问 Internet, 请与管理员联系。

--- 网络管理中心 QQ: 123456, Tel: 1234567





第 10 章 DNS/IP过滤

目录

[10.1. 什么是DNS/IP过滤](#)

[10.2. 启用DNS/IP过滤](#)

10.1. 什么是DNS/IP过滤

1. DNS过滤简介

DNS过滤即在域名解析时就进行限制，可以过滤内部电脑向互联网发出的域名查询请求(DNS协议)，域名解析不成功，客户机自然就访问不了该网页

启用DNS过滤的作用

- 可以更加有效的限制客户机对域名的访问
- 过滤更彻底, 强于URL过滤

2. IP过滤简介

这里的IP过滤是指外网IP

启用IP过滤的作用

- 可以禁止客户机访问某些外网IP
- 为DNS过滤增加了一道防护，避免了某些客户机不能通过域名正常访问网址时，采用IP访问网址。



9.2. 启用IP与MAC绑定



10.2. 启用DNS/IP过滤



10.2. 启用DNS/IP过滤

- 启用DNS过滤

Web登录海蜘蛛路由->“防火墙”->“DNS/IP过滤”，将要过滤的域名输入过滤域名列表即可，如下图：



书写规则

对单个IP进行DNS过滤：.baidu.com 1.1.1.1


对多个IP进行DNS过滤：.baidu.com 1.1.1.1,2.2.2.2

对IP段进行DNS过滤：.baidu.com 192.168.1.1-192.168.1.24

对子网进行DNS过滤：.baidu.com 192.168.1.0/24

对单个IP进行多个域名DNS过滤：.baidu.com, .sohu.com 192.168.1.1

复合型DNS过滤：.baidu.com, .sohu.com 192.168.1.0/24,172.16.1.1-172.16.1.24,172.16.1.254



提示

添加域名.xx.com，即可过滤所有.xx.com相关的DNS请求信息，比如 www.xx.com，new.xx.com等；如果只想过滤特定的域名，比如 mail.xx.com，请填写该域名的完整地址。

计算机在解析域名时，首先在本地的DNS缓存中查找，如果找不到才向外发送域名查询数据包，否则直接将缓存中的DNS解析项返回。因此对DNS域名进行过滤时有一定的滞后性，新加入的策略可能不会立即影响到被限制的计算机，须等这些计算机上的DNS缓存过期后才能生效。

- 启用IP过滤

将外网IP地址直接写入IP过滤列表中皆可，如土豆IP：202.102.83.90/202.102.83.91



此时，客户机不管是访问土豆域名还是IP都不能成功访问了。



第 10 章 DNS/IP过滤



第 11 章 网址/关键字过滤



第 11 章 网址/关键字过滤

目录

[11.1. 网址/关键字过滤的好处](#)

[11.2. 规则说明](#)

[11.3. 启用网址/关键字过滤](#)

11.1. 网址/关键字过滤的好处

开启网址/关键字过滤的好处:

- 过滤一些您不希望客户机看到或访问的站点，如广告、含有病毒、暴力或色情等内容的网址。
- 关键字过滤可以针对网址 (URL) 中输入的关键字或路径进行过滤，一般对搜索引擎或网站的特定目录比较有效；此外，还可以阻止用户下载指定扩展名的文件，只需将文件名后缀加入URL关键字过滤即可。



10.2. 启用DNS/IP过滤



11.2. 规则说明

11.2. 规则说明

网址过滤可以对匹配域名或参数过滤；URL关键字过滤可以对匹配一个网址中的任意部分参数过滤。

例：这个网址 `http://lady.163.com/10/0315/17/61R5T9V0002626K1.html` 中的域名部分为：lady.163.com 参数部分为 10/0315/17/61R5T9V0002626K1

网址过滤、关键字过滤书写规则要符合[正则表达式](#)。简单说明如下(免费版不支持)：

1. ^符号：匹配输入字符串的开始位置

例：^mp3表示所有以mp3开头的网址，如mp3.baidu.com

2. \$符号：匹配输入字符串的结束位置

例：.mp3\$表示所有以.mp3为文件名结尾的网址

3. *符号：表示匹配所有字符

例：.*?js 既可以匹配 .djo?js 也可以表示匹配 .yg?js 等等

4. [a-z]符号：匹配指定范围内的任意字符，这里的字符范围可以是字母也可以是数字

例：mp[1-4]表示所有含有 mp1/mp2/mp3/mp4 的网址

5. #号为注释符：#www.baidu.com表示注释www.baidu.com规则，即不对百度网址进行过滤

www.baidu.com #过滤百度 表示对www.baidu.com规则的作用进行注释



提示

网址过滤和URL过滤支持过滤含有以下字符的网址：

汉字、字母、数字、点(.)、下划线(_)、斜线(/)、问号(?)、等号(=)、逻辑与符号(&)、逗号(,)、分号(;)、

例：输入 &tn 即可过滤百度在线音乐链接



11.3. 启用网址/关键字过滤

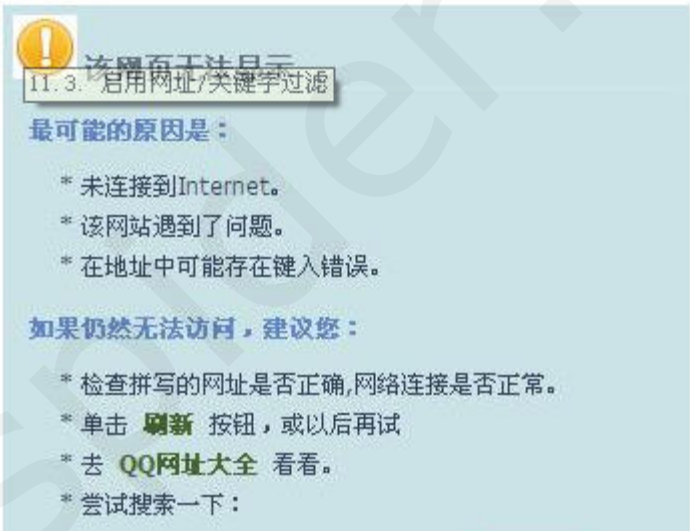
Web登录海蜘蛛路由器->“防火墙”->“网址/关键字过滤”

- 启用网址过滤

您可以在网址过滤列表中输入需要过滤的网址即可，这样当客户机访问该网址时会显示该页面无法访问，如下图所示：



客户机访问该网址时：



提示

若在过滤网址列表中输入*.xxx.com 可以过滤所有以 .xxx.com 结尾的网址。

- 只允许访问以下网址

开启“只允许访问以下网址”后，客户端就只可以访问目录列表中的网址，过滤其它所有网址的访问，设置如下图所示：

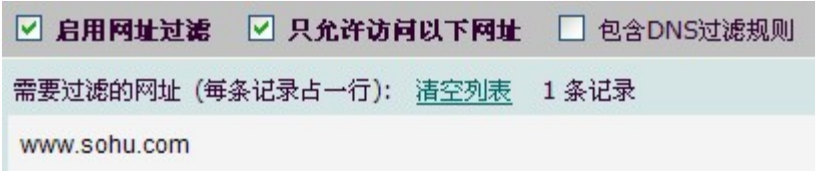


图 11.1.

此时客户端便只可以访问www.sohu.com了，并且客户端打开搜狐页面时会看到很多叉叉，这是此页面加载的一些广告被过滤掉的原因。

- 包含DNS过滤规则

开启包含DNS过滤规则功能可以有效防止客户机通过已经缓存的DNS解析结果来访问已经被DNS过滤掉的网址，这相当于为DNS过滤外又增加了一道防线。

例：如果在DNS过滤中过滤了www.baidu.com，可是客户机的DNS缓存或者hosts文件中自定义了百度的域名对应的IP地址，则客户端仍然可以访问百度域名，如果开启了“包含DNS过滤规则”就可以有效的阻止这种情况发生。

- 启用关键字过滤

关键字就是用户在使用搜索引擎时输入的、能够最大程度概括用户所要查找的信息内容的字或者词。

这里以关键字“在线”为例，可以禁止客户机在线观看视频影响网速。



图 11.2.

此时客户机如果查找“在线电影”等，浏览器将会提示该页面无法显示或者拦截警告。

恶意网址拦截警告

尊敬的用户：

您好！

您访问的网址由于可能损害您的计算机，被列入恶意网址黑名单。

如果您有什么疑问，请与网络管理员联系，感谢您的支持！

30 秒钟后自动跳转到 <http://www.google.com>

--- 网络管理中心 QQ: 9257321, Tel: 8835

图 11.3.

提示

在启用关键字过滤时，如果用户也同时启用了[恶意网址拦截功能](#)，则

浏览器会弹出恶意网址拦截警告，否则提示该页面无法显示。

• 过滤时间段

按照 时:分-时:分 的格式来自定义，如果有多段用，隔开，如下图：

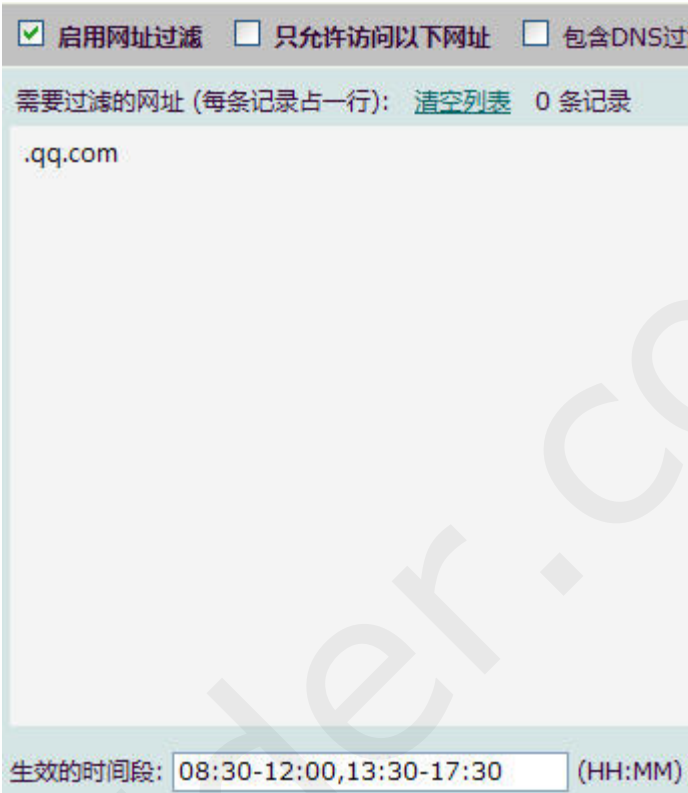


图 11.4.

这样配置就能在上午八点半到十二点，下午一点半到五点半这两个时段内的内网主机访问不了QQ相关网页。





第 12 章 ACL 规则

ACL 是指根据协议类型、IP 地址、端口等特征自定义防火墙规则，根据数据包传输的方向和对象不同，可以分为以下两种：

- 进入(Incoming)

数据包的最终目的地是路由，来源是外网IP或内网主机。

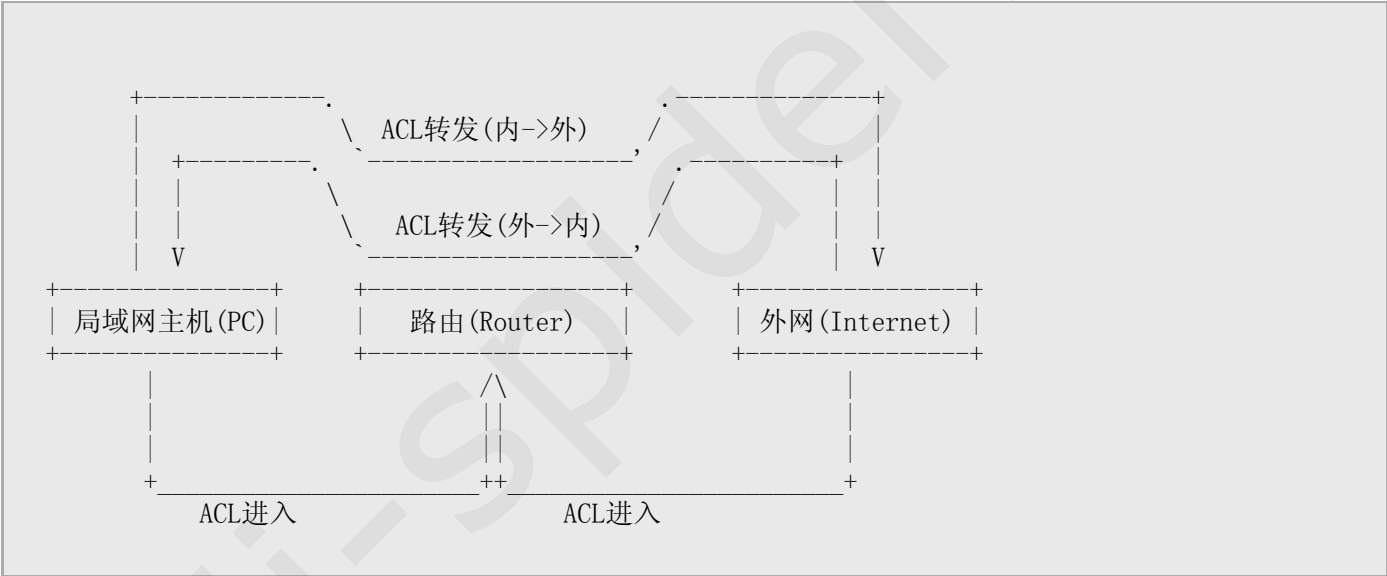
应用场合举例：禁止外网某些IP访问路由，比如要禁止 210.249.xx.xx 这个IP访问路由的Web管理。

- 转发(Forward)

数据包的最终目的地是内网主机或外网IP，来源是外网IP或内网主机。路由处于中间，对数据包进行转发。

应用场合举例：禁止内网访问外网的某些IP或端口，比如要禁止迅雷的 15000/UDP 下载端口。

下面这个图描述了两者之间的区别：



主要参数格式说明：

- 源/目的IP

为空表示所有IP，有如下3种表示方法：

1. 单个IP，比如：192.168.0.1
2. IP网络，比如：192.168.0.0/24 或 192.168.0.0/255.255.255.0
3. IP地址段，比如：192.168.0.1-192.168.0.200

- 源/目的端口

为空表示所有端口，有如下3种表示方法：

1. 单个端口，比如：8080
2. 多个离散端口，比如：137,139,445
3. 连续端口，比如：80-8000 (80到8000之间的所有端口)

- 匹配动作
 1. 通过：允许匹配的数据包通过
 2. 丢弃：丢弃匹配到的数据包，不反馈任何错误信息
 3. 拒绝：丢弃匹配到的数据包，并向发送者(源IP)反馈相关错误信息
 4. 忽略：对来访的数据包不做任何处理，直接记录到日志，此动作必须配合 记录到日志 功能一起使用。

案例-1：内网用迅雷下载的人太多，影响网速，需要禁止掉迅雷的 15000/UDP 端口

优先级：	<input type="text" value="1"/> (只能为数字, 数字越小优先级越高)
协议类型：	<input type="text" value="UDP"/>
数据流向：	<input type="text" value="转发"/>
源IP：	<input type="text"/>
源端口：	<input type="text" value="15000"/>
目的IP：	<input type="text"/>
目的端口：	<input type="text"/>
匹配数据包大小：	<input type="text"/> - <input type="text"/> bytes
时间限制：	<div><input checked="" type="checkbox"/> 启用</div> <div><div>起始日期 <input type="text"/></div><div>结束日期 <input type="text"/></div><div>起始时间 <input type="text"/></div><div>结束时间 <input type="text"/></div></div> <div>星期：<input type="checkbox"/>一 <input type="checkbox"/>二 <input type="checkbox"/>三 <input type="checkbox"/>四 <input type="checkbox"/>五 <input type="checkbox"/>六 <input type="checkbox"/>日 <input type="checkbox"/>工作日 <input checked="" type="checkbox"/>全部</div>
动作：	<input type="text" value="丢弃"/> <input type="checkbox"/> 并记录到日志, 日志标识: <input type="text"/>
备注：	<input type="text" value="禁止迅雷下载"/>
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用

图 12.1. 禁止下载端口

案例-2：内网某主机中了“机器狗”病毒，经观察，发现其会定时访问一些外网IP，并下载病毒和木马程序，为了安全期间，需要禁止内网访问这些IP。这些IP是 218.30.64.194, 60.190.118.211, 58.221.254.103。

添加3条规则，每条规则的设置和下面类似，只是目的IP不同：

优先级:	<input type="text" value="1"/> (只能为数字, 数字越小优先级越高)
协议类型:	TCP+UDP ▾
数据流向:	转发 ▾
源IP:	<input type="text"/>
源端口:	<input type="text"/>
目的IP:	<input type="text" value="218.30.64.194"/>
目的端口:	<input type="text"/>
匹配数据包大小:	<input type="text"/> - <input type="text"/> bytes
时间限制:	<div><input checked="" type="checkbox"/> 启用</div> <div><div>起始日期 </div><div>结束日期 </div></div> <div><div>起始时间 </div><div>结束时间 </div></div> <div>星期: <input type="checkbox"/>一 <input type="checkbox"/>二 <input type="checkbox"/>三 <input type="checkbox"/>四 <input type="checkbox"/>五 <input type="checkbox"/>六 <input type="checkbox"/>日 <input type="checkbox"/>工作日 <input checked="" type="checkbox"/>全部</div>
动作:	丢弃 ▾ <input type="checkbox"/> 并记录到日志, 日志标识: <input type="text"/>
备注:	<input type="text"/>
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用

图 12.2. 禁止访问目的IP





第 13 章 端口镜像

目录

- [13.1. 端口镜像简介](#)
- [13.2. 设置步骤](#)

13.1. 端口镜像简介

端口镜像 (Port Mirroring) 功能可以让指定IP或协议的流量复制并转发到某一特定的IP(一般是监控机器)，对于网吧而言，由于公安监控的需要，端口镜像功能通常是必须的。

端口镜像一般通过带端口镜像的交换机来实现，但这种交换机价格比较贵，故有些小型网吧，在路由和局域网之间串联了一个集线器 (HUB) 来解决这个问题，然而，这对网络性能造成了很大影响，尤其是当内网数据流量较大时，因为HUB的速率只有10Mbit，这无疑成了网络设备中的瓶颈。

针对此问题，海蜘蛛实现了利用路由来做端口镜像，这样做有以下几个优点：

- 1. 节省购买镜像端口交换机的成本
- 2. 不改变现有网络结构，对网络性能没有影响
- 3. 比硬件方式实现流量复制更为灵活，效率更高



注释

硬件方式是指对经过端口的所有类型的流量都进行复制监控，而一般在网吧需要监控的主要是浏览网页，浏览网页所产生的流量只占很小一部分，网吧内大部分流量是由在线电影、玩游戏、视频聊天、P2P下载等产生的，而这一部分通常不需要监控，也无法监控到有用数据。

在路由上，可以设定特定协议、特定端口的流量复制到监控机上，这样端口镜像的效率大大提高，对路由网卡的负荷也大大减少。





13.2. 设置步骤

浏览网页使用的是 TCP/HTTP 协议，端口为80，假设监控机的IP地址为 192.168.0.2，进入路由主界面->“防火墙”->“端口镜像”，设置如下：

新增规则1：对内网发出去的数据进行监控，源IP不填表示监控内网所有IP

优先级：	1	(只能为数字, 数字越小优先级越高)
协议类型：	TCP	
数据流向：	LAN-to-WAN	
源IP：	填写需要监控的IP地址	
源端口：		
目的IP：		
目的端口：	80	监控端口
匹配数据包大小：		
管理IP：	192.168.0.2	监控机IP
备注：	内网到外网数据	
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

新增规则2：对外网进来的数据进行监控

优先级：	1	(只能为数字, 数字越小优先级越高)
协议类型：	TCP	
数据流向：	WAN-to-LAN	
源IP：		
源端口：	80	监控端口
目的IP：	填写要监控的IP地址	
目的端口：		
匹配数据包大小：		
管理IP：	192.168.0.2	监控机IP
备注：	外网到内网数据	
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

最后，启用端口镜像即可

☒ 启用端口镜像功能

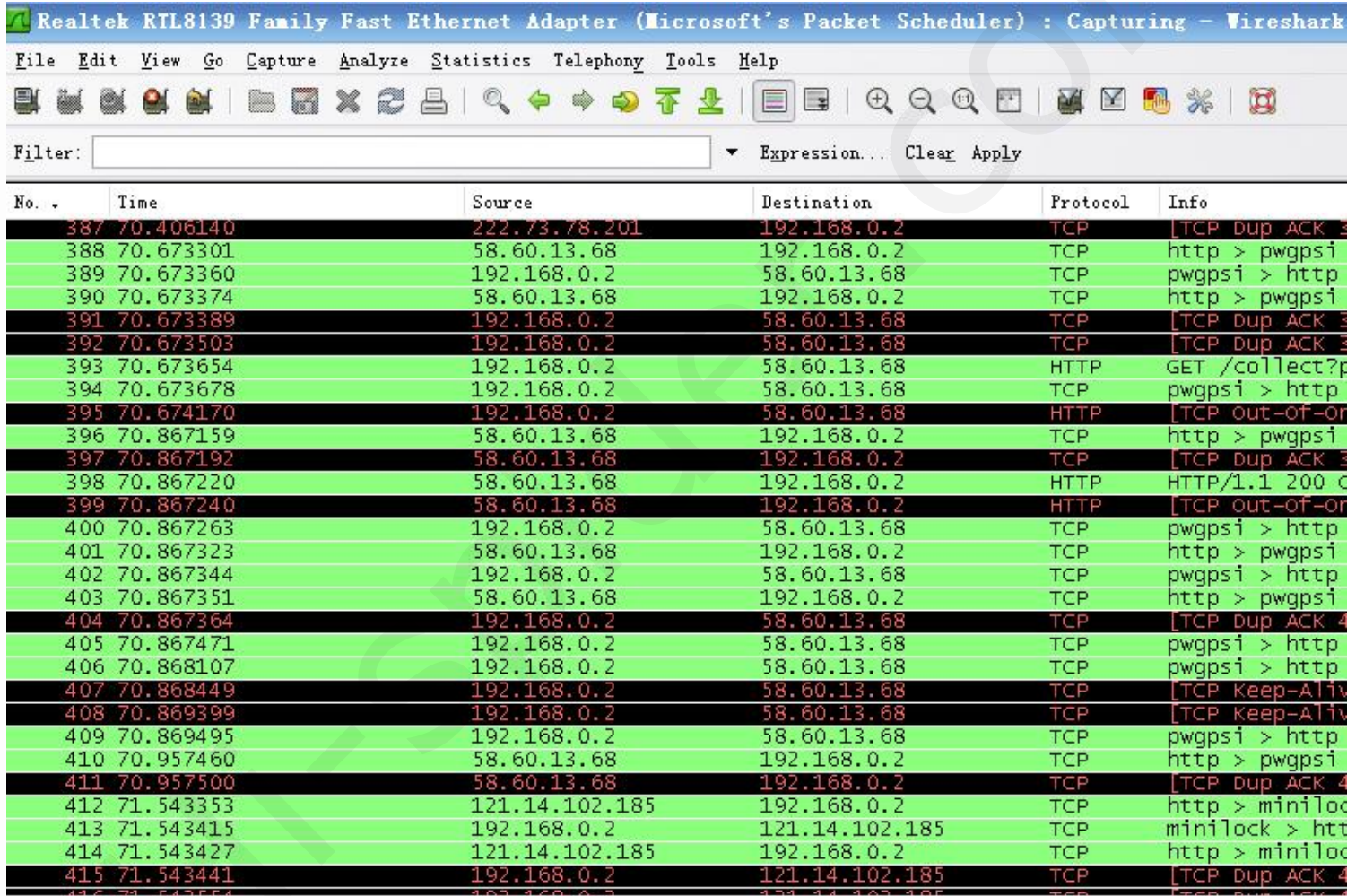
全选/全不选

ID	优先级	协议类型	数据流向	源IP/段:端口 目的IP/段:端口	管理IP	备注	激活/编辑/删除/选择			
1	1	TCP	LAN-to-WAN	ALL:ALL ALL:80	192.168.0.2	-内网出去数据	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><input type="checkbox"/></div>
2	1	TCP	WAN-to-LAN	ALL:80 ALL:ALL	192.168.0.2	-外网进来数据	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>	<div><input type="checkbox"/></div>

如果要监控所有内外网端口则源和目的端口号都不填；如果要监控所有协议，协议类型选“TCP+UDP”即可。

下一步就可以在监控机上面打开抓包软件或分析工具对监听到的流量进行分析了。

下面是用 [wireshark](#) 抓取到数据包截图：



为了减少局域网网卡的压力，可以在路由上增加一块网卡，专门用于转发监控的数据。增加网卡后，将这块网卡配置为私有IP地址（不能和局域网网卡IP在同一网段）。比如新增网卡的IP设为192.168.10.1，监控机的IP为 192.168.10.254，然后修改上面的设置，将管理IP从192.168.0.2改为192.168.10.254即可。



第 14 章 端口映射

目录

- [14.1. 端口映射简介](#)
- [14.2. 启用端口映射](#)
- [14.3. 端口映射不成功，如何找出问题原因](#)
- [14.4. 端口443映射不成功的原因](#)

14.1. 端口映射简介

什么是端口映射

端口映射功能是将内网中一台主机的私有IP地址映射成一个可以被路由器转发的公有IP地址，当用户访问提供映射端口主机的某个端口时，服务器将请求转到内部一主机的提供这种特定服务的主机；端口映射可以实现从 Internet 到局域网内部机器的特定端口服务的访问。

使用端口映射的好处

- 实现从Internet到局域网内部机器的特定端口服务的访问。
- 由于访问者并不知道服务器的真实IP，这样可以保护服务器的安全。



13.2. 设置步骤



14.2. 启用端口映射



14.2. 启用端口映射

Web登录海蜘蛛软路由->“防火墙”->“NAT 策略”->“端口映射”->新增规则，如下图所示：



图 14.1. 启用端口映射

进入新增端口映射页面，这里以 Web端口 和 FTP服务器映射 为例：

- Web服务

端口映射配置如下图所示：

名称：	<input type="text" value="rule"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)	
优先级：	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)	
协议类型：	TCP+UDP		
对外端口：	<input type="text" value="8000"/> - <input type="text"/>		
对外 IP：	== 所有外网IP (默认) ==		
对内端口：	<input type="text" value="80"/> - <input type="text"/>		
对内 IP：	<input type="text" value="192.168.0.2"/>		
忽略端口：	<input type="text"/>		(您很可能需要将Web管理端口 880,443 加入忽略端口之列)
备注：	<input type="text"/>		
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用		
<div>保存设置 重置 取消</div>			

图 14.2. 端口映射配置示例



提示

上图中对外IP为路由器的WAN口，对外端口为访问者访问Web服务所使用的端口。（对外支持 PPTP/L2TP）

对内IP为服务器的实际IP地址，对内端口为服务器上设置Web服务所使用的端口。

外网用户访问 <http://218.36.24.34:8000> 时实际访问的是内网服务器 192.168.0.2:80 上面的资源。内网用户访问该服务器时只需在浏览器中输入 <http://192.18.0.2> 即可。


如果需要映射一段连续的端口地址如800-1000，其中可能将880等端口排除在端口映射之外，需要将此端口号填入 忽略端口 中。

支持3G无线接入，映射到无线局域网内主机。

• FTP服务器的端口映射

名称:	FTP_rule	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	1	(只能为数字, 数字越小优先级越高)
协议类型:	TCP	
对外端口:	21,20	-
对外 IP:	== 所有外网IP (默认) ==	
对内端口:	21,20	-
对内 IP:	192.168.0.2	
忽略端口:		
(您很可能需要将Web管理端口 880,443 加入忽略端口之列)		
备注:	FTP服务器	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
<div>保存设置 重置 取消</div>		

图 14.3. FTP服务器端口映射配置示例



提示

与Web服务不同的是FTP服务有两个端口：21（连接端口）、20（数据传输端口），所以这里需要映射两个端口

20端口在端口映射时不变，否则客户可以访问服务器，却不能查看文件。

内网有VLAN，也可以按照此方法将各VLAN的用户映射到外面去。具体的VLAN配置参照 [路由上划分VLAN](#) 和 [路由上不划分VLAN](#)



14.3. 端口映射不成功，如何找出问题原因

第 14 章 端口映射

14.3. 端口映射不成功，如何找出问题原因

映射例子：

路由器局域网接口 IP 地址： 192.168.0.1
广域网接口 IP 地址： 211.X.X.X
对外映射端口： 800

内网映射主机 IP 地址： 192.168.0.100
对内映射端口： 80（提供Web网站服务）

内网测试主机 IP 地址： 192.168.0.2
外网测试主机 IP 地址： 220.X.X.X

对映射主机的要求：

- 1. 映射主机的IP地址需和路由局域网IP在同一网段，子网掩码需和路由局域网接口一致，网关应指向路由局域网IP，简而言之，该映射主机能通过路由上网。
- 2. 如果路由启用了IP与MAC地址绑定，请确认映射主机的IP地址在绑定列表中。主页中“防火墙”->“IP与MAC绑定”，如图：

☒ 启用IP与MAC地址绑定

绑定列表

强制绑定

确认映射主机ip地址在此列表中

ID	IP地址	MAC地址	备注	状态	编辑	删除
1	192.168.1.22	e0-cb-4e-d9-d7-2b	测试	✓		
2	192.168.1.33	00-90-27-a1-5b-40		✓		

图 14.4. IP与MAC绑定列表

- 3. 如果路由启用了强制用户通过PPPoE拨号上网，请确认映射主机的IP地址在IP白名单中。“服务应用”->“PPPoE 拨号服务”，点击高级选项，如图：

强制用户通过PPPoE拨号上网：☒ 是(客户机通过PPPoE拨号才能上网)

IP白名单 (两种方式均可上网):

192.168.12.53
192.168.26.58
192.168.1.24

确认映射主机IP在此白名单列表中

图 14.5. PPPoE拨号上网IP白名单



注意

这里的IP白名单填局域网的IP地址而不是PPPoE服务分配给客户机的IP地址

4. 如果路由启用了Web认证，请确认映射主机的IP地址在此IP白名单中。“服务应用”->“Web认证服务”，如图：

启用上网 Web 认证:	<input checked="" type="checkbox"/> 是
在 PPPoE 上启用 Web 认证:	<input type="checkbox"/> 是
认证模式:	<input checked="" type="radio"/> 所有用户上网都必须通过 Web 认证
上网时需要经过验证的IP:	
会话存活超时时间:	<input type="text" value="120"/> s (多长时间没有检测到用户
IP白名单 (无需验证可直接上网):	<div>192.168.53.26 192.168.0.24 192.168.1.23</div>

确认映射主机IP地址在此白名单中

图 14.6. Web认证IP白名单

5. 映射主机所提供的服务（端口）应开启，并确保映射主机自身的防火墙对此端口没有限制。可以利用路由的PING功能来检验，进入“系统工具”->“PING 测试”，IP地址填入内网作为端口映射的主机IP，在PING类型下拉列表里选择TCP/SYN，TCP端口选择要映射的端口，如下图是检验192.168.0.10这个主机的80端口是否通：



图 14.7. 主机端口检验

映射前，在内网测试机上应可直接访问映射主机提供的服务，即可通过 **http://192.168.0.100** 正常打开网页；

映射成功后，在内网和外网测试机上均可通过 **http://211.x.x.x:800** 访问内网的Web服务。

如果映射不成功，请按照以下步骤逐步排除故障：

- 1. 检查路由器上的“端口映射”是否启用？此外，需注意：如果同时启用了“DMZ”主机，端口映射将自动失效；
- 2. 检查路由器上的端口映射规则是否设置正确，映射的对外端口有无重复？协议类型是否正确（如HTTP映射时，协议类型选成了UDP）；
- 3. 检查映射的主机是否满足上述提到的“对映射主机的要求”；
- 4. 检查该服务所需要的所有端口是否已全部映射；
- 5. 在局域网内通过映射后的外网IP和端口访问映射主机，看是否正常；
- 6. 修改对外端口为其他端口，并重新测试映射，部分ISP可能会对某些端口有限制；
- 7. 由于路由系统的管理默认端口为880，所以需使用此端口映射时要先修改Web页面管理端口；



14.4. 端口443映射不成功的原因

第 14 章 端口映射



14.4. 端口443映射不成功的原因

当您启用端口映射时使用了端口443却无法成功时，可能是SSL连接在使用443端口。您可以在主页中进入“系统设置”-“web远程管理”，点击“端口设置”，把是否启用SSL连接加密的勾去掉，如图：

登录帐号

端口设置

安全策略

WEB 管理端口:

880

(范围: 1-65535) 运行中 (PID: 1366)

是否启用 SSL 连接加密:

☐ 启用

去掉此勾
(SSL 连接使用 443 端口)

强制使用 SSL 连接加密:

☐ 启用 (适用于对安全性要求较高的场合)

保存设置

重设

端口测试

提示

您也可以在此页面上直接更改web服务器默认端口880

保存后再重新设置其端口映射。



14.3. 端口映射不成功，如何找出问题原因



第 15 章 DMZ主机



第 15 章 DMZ主机

目录

[15.1. DMZ简介](#)

[15.2. DMZ主机设置](#)

15.1. DMZ简介

什么是DMZ?

DMZ (Demilitarized Zone) 即俗称的非军事区，与军事区和信任区相对应，作用是把Web、E-mail等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ可以理解为一个不同于外网或内网的特殊网络区域，DMZ内通常放置一些不含机密信息的公用服务器，比如Web、Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。

划分DMZ区的好处

- DMZ可以为主机环境提供网络级的保护，能减少为不信任客户提供服务而引发的危险，是放置公共信息的最佳位置。
- DMZ使包含重要数据的内部系统免于直接暴露给外部网络而受到攻击，攻击者即使初步入侵成功，还要面临DMZ设置的新的障碍。





15.2. DMZ主机设置

web登录海蜘蛛路由->“防火墙”->“DMZ 主机”，进入DMZ主机设置页面，如下图所示：

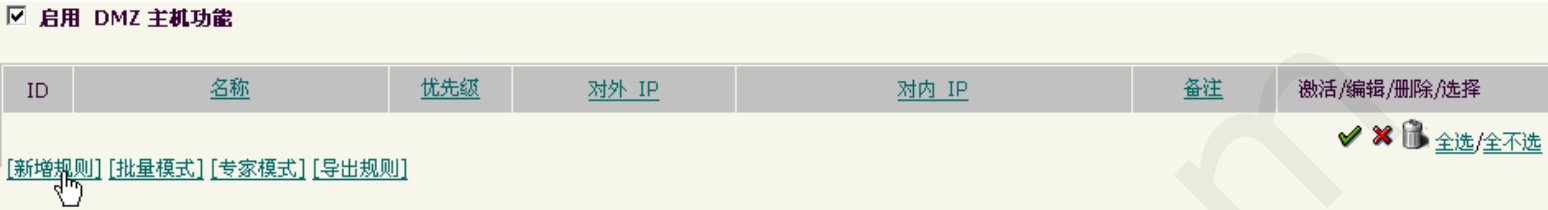


图 15.1. 启用DMZ主机

进入新增DMZ主机设置页面：

名称: (只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级: (只能为数字, 数字越小优先级越高)

对内 IP: (局域网IP)

对外 IP:

忽略端口: (您很可能需要将Web管理端口 880,443 加入忽略端口之列)

备注:

状态: ☒ 激活 ☐ 禁用

图 15.2. DMZ主机配置示例



提示

外网用户访问该服务器时使用的IP地址为：218.36.24.34；内网用户访问该服务器时使用的IP地址为：192.168.0.2。

DMZ主机可以把不使用的端口号如880，443等添加到 忽略端口。

被 DMZ 主机使用的广域网 IP，其相应的端口映射规则将自动失效。计算机设置为 DMZ 主机后，如同直接具有广域网 IP，并且将不再受到防火墙的保护。



重要

如果您设置的DMZ主机需要用到443和880端口的话，请在主页中进入“系统设置”->“Web远程管理”，点击“端口设置”，把web管理端口更改掉，并把是否启用SSL连接加密的勾去掉，保存后再重新设置。

登录帐号

端口设置

安全策略

WEB 管理端口: 880 (范围: 1-65535) 运行中 (PID: 1366)

是否启用 SSL 连接加密: ☐ 启用 **去掉此勾** (SSL 连接使用 443 端口)

强制使用 SSL 连接加密: ☐ 启用 (适用于对安全性要求较高的场合)

保存设置

重设

端口测试

第 15 章 DMZ主机

第 16 章 UPnP支持



第 16 章 UPnP支持

目录

- [16.1. UPnP简介](#)
- [16.2. 启动UPnP服务](#)

16.1. UPnP简介

什么是UPnP

UPnP (Universal Plug and Play)：是实现对等网络连接（P2P）的结构。是一种分布式的，开放的网络架构。它不依赖于特定的设备驱动程序，而是使用标准的协议。

UPnP协议的作用

- 对于一台内网电脑，UPnP功能可以使网关或路由器的NAT模块做自动端口映射，将监听的端口从网关或路由器映射到内网电脑上。
- 网关或路由器的网络防火墙模块开始对Internet上其他电脑开放这个端口。



15.2. DMZ主机设置



16.2. 启动UPnP服务



16.2. 启动UPnP服务

- 在服务器端开启UPnP服务

Web登录海蜘蛛路由->“防火墙”->“UPnP支持”->启动防火墙UPnP支持，SSDP/UPnP 广播时间间隔是路由自动查找下面主机需要映射的周期时间，一般选择允许所有内网IP映射大于1024的所有端口：

☒ 启用防火墙 UPnP 支持

UPnP 服务状态： 运行中 (PID:2391)

SSDP/UPnP 广播时间间隔：

s (默认为 30)

安全策略：

☒ 允许所有内网IP映射大于1024的所有端口(默认)

☐ 允许所有内网IP映射指定的端口, 范围: (如 50000-60000)

☐ 通过自定义规则来指定允许映射的端口

- 开启支持UPnP的软件（迅雷、bitcomet、BTspirit、pps、tuotu等）的UPnP服务，在路由器端会自动映射端口，如图：

ID	协议类型	局域网 IP	对内端口	对外端口	客户端描述
1	TCP	192.168.0.2	14614	6724	迅雷5
2	UDP	192.168.0.2	14614	17872	迅雷5
3	TCP	192.168.0.2	17263	17263	BitComet (192.168.0.2
4	UDP	192.168.0.2	17263	17263	BitComet (192.168.0.2
5	TCP	192.168.0.2	19388	19388	BitSpirit - The powerful and easy-to-use BitTorrent client
6	UDP	192.168.0.2	19388	19388	BitSpirit - The powerful and easy-to-use BitTorrent client
7	TCP	192.168.0.2	4795	4795	2
8	UDP	192.168.0.2	4805	4805	2
9	TCP	192.168.0.2	10950	10950	PPStream
10	UDP	192.168.0.2	10950	10950	PPStream





第 17 章 一对一NAT

目录

- [17.1. 一对一NAT简介](#)
- [17.2. 启动一对一NAT服务](#)
- [17.3. 一对一NAT与端口映射及DMZ的区别](#)

17.1. 一对一NAT简介

什么是一对一NAT

所谓一对一NAT就是在ISP给您提供的多个合法IP地址有剩余的时候，把外部多个合法IP地址直接对应到内部多个虚拟服务器IP地址，让这些对应到的服务器访问外部网络时都有自己的合法IP地址。

使用一对一NAT的好处

- 提高了外网用户访问服务器的速度



16.2. 启动UPnP服务



17.2. 启动一对一NAT服务



17.2. 启动一对一NAT服务

这里我们假设您已经从当地ISP那里获得的多个合法IP地址为：218.36.24.33-218.36.24.38，两个Web服务器的内网IP分别为：192.168.0.2、192.168.0.3，WAN1口已经使用了218.36.24.34，Gateway使用218.36.24.33，那么还剩下4个IP地址没有使用，此时您就可以使用一对一NAT让内网服务器映射为剩下的IP地址，具体设置如下所示：

Web登录海蜘蛛路由->“防火墙”->“一对一NAT”，如下图：



图 17.1. 开启一对一NAT

进入新增一对一NAT页面，填入局域网的IP和外网的IP，如下图所示：

名称：	<input type="text" value="NAT"/>	(只能由字母、数字、汉字、下划线)
优先级：	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
对内 IP：	<input type="text" value="192.168.0.2"/>	(局域网IP地址)
对外 IP：	<input type="text" value="218.36.24.35"/>	(Internet 上使用的公网IP地址)
忽略端口：	<input type="text"/>	(您很可能需要将Web管理端口 880,443 加入)
备注：	<input type="text"/>	
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 17.2. 一对一NAT配置1

名称：	<input type="text" value="NAT"/>	(只能由字母、数字、汉字、下划线)
优先级：	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
对内 IP：	<input type="text" value="192.168.0.3"/>	(局域网IP地址)
对外 IP：	<input type="text" value="218.36.24.36"/>	(Internet 上使用的公网IP地址)
忽略端口：	<input type="text"/>	(您很可能需要将Web管理端口 880,443 加入)
备注：	<input type="text"/>	
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 17.3. 一对一NAT配置2

此时，一对一NAT映射就已经设置完成了。

此时外网用户如果要访问IP地址为192.168.0.2的Web服务器，那么就只需要访问IP:218.36.24.35；外网用户如果要访问IP地址为192.168.0.3的服务器，那么就只需要访问IP:218.36.24.36



注意

对于您不想对公网开放的端口地址如880等可以填入到 忽略端口。



17.3. 一对一NAT与端口映射及DMZ的区别

第 17 章 一对一NAT



17.3. 一对一NAT与端口映射及DMZ的区别

在启用一对一NAT时，该服务器向外网发送的数据包的源地址为其所映射的外网IP地址，设置 该服务器映射的对外IP为218.36.24.36， 下图是IP为192.168.0.2的web服务器访问外网时外网服务器上显示的流量信息。

```
10:45:38 218.36.24.36:1856 Requested GET /
10:45:40 218.36.24.36:1856 Requested GET /
10:45:41 218.36.24.36:1856 Requested GET /
```

此时关闭一对一NAT服务，启用端口映射服务，该服务器映射的对外IP为218.36.24.35

此时虽然外网用户访问该服务器时其使用的IP为218.36.24.35，可是此服务器访问外网服务器时数据包的源地址为218.36.24.34（路由器WAN口IP），如下图所示：

```
10:45:40 218.36.24.36:1856 Requested GET /
10:45:41 218.36.24.36:1856 Requested GET /
10:54:21 218.36.24.34:1911 Requested GET /
10:54:23 218.36.24.34:1912 Requested GET /
11:01:36 218.36.24.34:1915 Requested GET /
11:01:36 218.36.24.34:1916 Requested GET /
11:01:36 218.36.24.34:1917 Requested GET /
11:01:36 218.36.24.34:1918 Requested GET /
11:01:37 218.36.24.34:1920 Requested GET /
11:01:37 218.36.24.34:1922 Requested GET /
```



总结

一对一NAT的对外IP具有双向性：对于外网客户端来说其是目的地址，对于外网服务器来说其是源地址。

端口映射和DMZ映射的对外IP只是作为客户端的目的地址，对于外网服务器其源地址仍为该服务器所在的局域网的路由器WAN口IP地址。

DMZ映射可以理解为开启了映射所有端口的主机。





第 18 章 No NAT

目录

- [18.1. No NAT简介](#)
- [18.2. 启动No NAT功能](#)

18.1. No NAT简介

什么是No NAT

No NAT指数据传输离开本地网络时路由不进行网络地址转换，常用于 LAN-to-LAN 局域网互联的场合。



17.3. 一对一NAT与端口映射及DMZ的区别



18.2. 启动No NAT功能

18.2. 启动No NAT功能

第 18 章 No NAT



18.2. 启动No NAT功能

Web登录海蜘蛛路由->“防火墙”->“No NAT规则”，勾选启用No NAT功能，点击新增规则，如图：



图 18.1. 启用No NAT功能

填写源局域网和目的局域网的IP网段和子网掩码，保存后即可。

名称:	<input type="text" value="LAN-to-LAN"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
源IP:	<input type="text" value="192.168.1.0/24"/>	
目的IP:	<input type="text" value="192.168.101.0/24"/>	
备注:	<input type="text"/>	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
<div>保存设置 重置 取消</div>		

图 18.2. 新建No NAT规则

这样192.168.1.0网段的计算机访问192.168.101.0网段的计算机就会留下其局域网的IP地址信息。





部分 V. 上网行为管理

目录

[19. 恶意网址拦截](#)

- [19.1. 恶意网站简介](#)
- [19.2. 自定义恶意网址](#)
- [19.3. 拦截动作设定](#)

[20. URL 重定向](#)

[21. 推送网页通知](#)

- [21.1. 通知内容的几种形式](#)
- [21.2. 编写网页通知](#)
 - [21.2.1. 指定推送用户](#)
 - [21.2.2. 上传文件](#)
 - [21.2.3. 编写网页通知](#)

[22. 预定义对象](#)

[23. 对象分组管理](#)

[24. 应用协议过滤](#)

[25. 上网期限管理](#)

[26. 上网行为管理综合应用](#)

- [26.1. 网络拓扑结构](#)
- [26.2. 新建用户与分组](#)
- [26.3. 新建时间与网址对象](#)
- [26.4. 设置各组的应用协议控制](#)
- [26.5. 仅允许收发Web邮件](#)
- [26.6. 特征库的更新](#)





第 19 章 恶意网址拦截

目录

- [19.1. 恶意网站简介](#)
- [19.2. 自定义恶意网址](#)
- [19.3. 拦截动作设定](#)

19.1. 恶意网站简介

什么是恶意网站

恶意网站是指利用IE漏洞，嵌入恶意代码，在用户不知情的情况下，对用户的机器进行篡改或破坏的网站。对于弹出插件或提示用户是否将其设为首页的网站，因为需要用户选择确认，则不被定义为恶意网站。对于内容不合法、不健康的网站，如果它并未对用户的计算机进行篡改或破坏，也不被定义为恶意网站。

恶意网站的危害

恶意网站往往都含有病毒，比如木马。病毒一旦侵入个人电脑，会在您的系统中植入木马并窃取您的隐私信息甚至直接控制您的电脑。

恶意网址拦截功能的好处

恶意网址拦截功能可以用来禁止内网访问已经被确认为恶意网址的网站，当用户访问此网址时会自动跳转到自定义的页面上。

海蜘蛛软路由的数据库中不仅收录了大量的恶意网址，同时还提供了[自定义恶意网址](#)功能使用户可以随心所欲的设置自己不想访问的网址。





19.2. 自定义恶意网址

海蜘蛛路由器的数据库中收录了91646条恶意网址，当用户访问这些网址时，路由器会自动拦截这些网址。

进入“上网管理”->“恶意网址拦截”，勾选启用恶意网址拦截功能。这里我们以www.3721.com为例，输入域名www.3721.com会发现已经收录在海蜘蛛路由器的恶意网址数据库中：

☒ 启用恶意网址拦截功能

当前恶意网址数据库版本: v3.5.0 [71346 条记录], 发布时间: 2010-09-13 20:40:08

域名:

提示: www.3721.com 存在于恶意网址数据库中！

当用户登录这个恶意网址时会看到如下图所示的页面：

恶意网址拦截警告

尊敬的用户：

您好！

您访问的网址由于可能损害您的计算机，被列入恶意网址黑名单。

如果您有什么疑问，请与网络管理员联系，感谢您的支持！

在IE中输入www. 3721.com时路由器会自动拦截并出现此提示

30 秒钟后自动跳转到 <http://www.google.cn>

--- 网络管理中心 QQ: 123456, Tel: 1234567

若用户启用恶意网址拦截功能，单击下面的拦截日志后还可以看到相关的拦截记录：

2009-07-08 15:18:15 192.168.0.2 访问 http://www.3721.com/ 时被拦截

图 19.1. 拦截日志



提示

如果发现需要访问的网址位于恶意网址数据库中，用户可以启用恶意网址白名单并将其加入到白名单列表中。

很多时候，用户都需要自定义恶意网址。海蜘蛛路由系统同样也提供了自定义恶意网址功能。

用户只需将恶意网址添加到恶意网址列表中即可，每条记录占一行。这里我们以百度为例，勾选自定义恶意网址：



当用户登录百度时会看到如下图所示的页面：





19.3. 拦截动作设定

海蜘蛛路由系统提供了两种拦截方式：替换成指定页面和中断/重置连接（客户机会显示无法打开网页的错误）。

当拦截方式为 替换成指定页面时 用户可以自己设置提示标题、提示内容、自动跳转时间以及跳转网址等。

拦截方式:	<input checked="" type="radio"/> 替换成指定页面 <input type="radio"/> 中断/重置连接(客户机会显示无法打开网页的错误) <input checked="" type="checkbox"/> 同时记录到日志
提示标题:	<input type="text" value="恶意网址拦截警告"/> (显示在浏览器标题栏)
提示内容:	<div>尊敬的用户: 您好! 您访问的网址由于可能损害您的计算机,被列入恶意网址黑名单. 如果您有什么疑问,请与网络管理员联系,感谢您的支持!</div>
多长时间后自动跳转:	<input type="text" value="30"/> s (0表示不显示提示直接跳转)
跳转网址:	<input type="text" value="www.google.com"/>
管理签名信息:	<input type="text" value="网络管理中心 QQ: 123456, Tel: 1234567"/> (显示在提示框右下角)
<div>保存设置 默认设置 页面预览 重设</div>	

图 19.2. 拦截动作设置

当用户访问路由器设定的恶意网址时就会出现以下提示：

恶意网址拦截警告

尊敬的用户：

您好！

您访问的网址由于可能损害您的计算机，被列入恶意网址黑名单。

如果您有什么疑问，请与网络管理员联系，感谢您的支持！

在IE中输入www.3721.com时路由器会自动拦截并出现此提示

30 秒钟后自动跳转到 <http://www.google.cn>

--- 网络管理中心 QQ: 123456, Tel: 1234567

当拦截方式为中断/重置连接时，用户访问路由器设定的恶意网址时会显示该页面无法显示：

 该网页无法显示

最可能的原因是：

- * 未连接到Internet。
- * 该网站遇到了问题。
- * 在地址中可能存在键入错误。

如果仍然无法访问，建议您：

- * 检查拼写的网址是否正确，网络连接是否正常。
- * 单击 **刷新** 按钮，或以后再试。
- * 去 **QQ网址大全** 看看。
- * 尝试搜索一下：

 搜搜

第 20 章 URL 重定向

有时运营商对您访问的URL进行DNS劫持，或者您需要自定义访问URL跳转到指定网址，这时就需要使用URL重定向功能。

在路由主页面下，进入“上网管理”->“URL 重定向”，勾选启用 URL 重定向功能，这里分为两种设置方式：

- 将单一网址设置跳转指定页面，如这里把 `www.baidu.com` 跳转到 `www.sina.com.cn`

☒ 启用 URL 重定向功能

重定向列表 (每条记录占一行): [清空列表](#)

`www.baidu.com www.sina.com.cn`

 注意

跳转定义前后的网址间需要空格！

当局域网内的电脑打开百度页面时，就会自动跳转到新浪主页。



- 用正则表达式将含特征的一系列网址设置跳转到指定页面，例如这里加入.*把含百度特征的网址跳转到 `www.sina.com.cn`

☒ 启用 URL 重定向功能

重定向列表 (每条记录占一行): [清空列表](#)

`www.baidu.com/. * www.sina.com.cn`

 注意

跳转定义前后的网址间需要空格！正则表达式设置功能仅ISP运营商版才拥有。

当局域网内的电脑打开以 `www.baidu.com` 开头的任何页面时，都会跳转到新浪主页。



重要

URL重定向前后的网址需要都是可访问的才能实现跳转



19.3. 拦截动作设定



第 21 章 推送网页通知



第 21 章 推送网页通知

目录

[21.1. 通知内容的几种形式](#)

[21.2. 编写网页通知](#)

[21.2.1. 指定推送用户](#)

[21.2.2. 上传文件](#)

[21.2.3. 编写网页通知](#)

21.1. 通知内容的几种形式

网页通知可以使网络管理员以网页的形式对[指定的用户](#)推送指定的通知，只要用户一上网就可以看到。海蜘蛛软路由提供的网页通知的内容形式有以下4种：

1. 默认形式

在默认形式下书写通知内容就如同在word下编写文档一样，可以达到所见即所得的效果

2. 自定义html形式

在html形式下书写网页通知需用户了解基本的html标签编写规则

3. 图片形式

选择图片形式来推送网页通知可以达到图文并茂的效果

4. 外部链接形式

在这种形式下编写网页通知，用户只需在链接地址一栏输入通知内容的URL地址。



提示

免费版和网吧版仅支持默认形式，后面三种模式需其它版本才能支持。





21.2. 编写网页通知

21.2.1. 指定推送用户

进入“上网管理”->“推送网页通知”，在通知内容形式中选择推送方式，默认为文字形式，通知对象可分为通知所有在线用户或指定用户推送。

管理员只需要在推送IP列表中输入用户的IP地址即可，当然也可以对不同的通知设置不同的接受用户，如下图中就只有192.168.0.2和192.168.0.214两台计算机接收到通知。

通知内容形式:	默认
通知标题:	网页推送通知 (显示在浏览器标题栏)
通知对象:	<input type="radio"/> 向所有在线用户推送 <input checked="" type="radio"/> 推送给指定IP 清空列表
推送IP列表:	192.168.0.2 192.168.0.214

图 21.1. 推送IP



提示

这里推送的IP可以是内网固定IP地址，也可以是拨号IP地址

最下面可以配置相关的推送签名、时间等。

管理签名信息:	李经理 13333333333 (显示在提示框右下角)
定时推送:	2012-12-21 12:12:12 (YYYY-MM-DD HH:MM:SS)
启用通知接收回执:	<input checked="" type="checkbox"/> 是

图 21.2. 推送相关配置

管理员签名会显示在推送页面的右下角。



图 21.3. 推送通知

定时推送指所有信息会在指定的时间推送到下面主机，对于没有开机的主机会在开机打开网页后自动接收
启用通知接收回执会让用户打开页面有个确定页面：

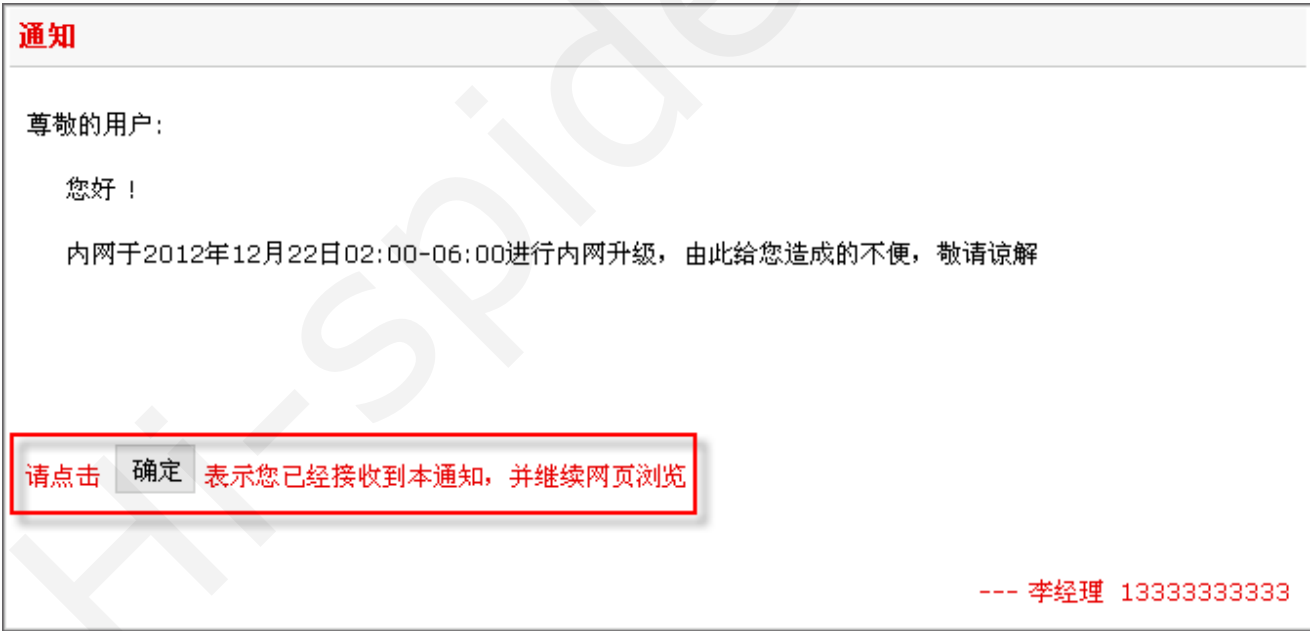


图 21.4. 通知接收回执

用户点击确定后路由端会有推送相关信息：

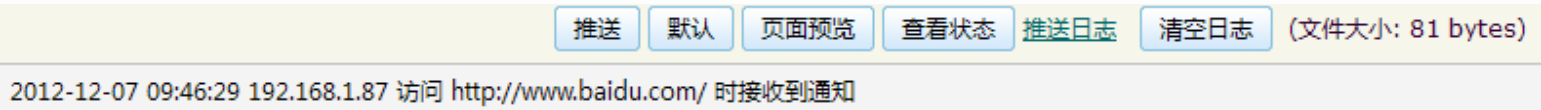


图 21.5. 推送信息

21.2.2. 上传文件

海蜘蛛软路由提供了文件管理功能，用户可以使用上传文件管理功能将需要经常用到的文件上传。这些文件将保留在路由系统的内存中，重启或自动保存时将写入到磁盘。

海蜘蛛软路由支持多种文件上传格式，这里我们以上传doc为例。进入“系统工具”->“文件管理”，选择上传文件页面：

文件列表		
上传文件		
ID	文件名	大小
1	MAC地址修改器.lnk	576.0 bytes
2	x.tar	485.12 KB
3	网页通知.gif	2.71 KB
4	附件上传失败.jpg	47.17 KB

图 21.6. 上传文件

点击浏览按钮，选择需要上传的文件：参考资料.doc ，点击上传按钮。

上传文件		
文件名：	<input type="text" value="C:\Documents and Settings\Administrato"/>	<div>浏览... (最大不超过 30M)</div>
重命名：	<input type="text"/>	(为空表示不重命名)
备注：	<input type="text"/>	
是否自动覆盖已经存在的文件：	<input type="checkbox"/> 是	
上传后是否自动解压缩：	<input type="checkbox"/> 是 (仅支持 ZIP/TAR/TGZ 格式压缩文件)	

图 21.7. 选择本地文件



重要

上传的文件大小不超过5M，支持扩展名：txt,html,htm,pdf,chm,ppt,doc,xls,gif等。

回到刚才的文件列表页面，刚添加的参考资料.doc文件已上传成功。

文件列表		
上传文件		
ID	文件名	大小
1	MAC地址修改器.lnk	576.0 bytes
2	x.tar	485.12 KB
3	参考资料.doc	10.50 KB
4	网页通知.gif	2.71 KB
5	附件上传失败.jpg	47.17 KB

图 21.8. 上传成功

这些文件可以随时通过外网或内网提供下载，您只需要在任意一台联网的计算机上输入“http://路由的IP地址:端口号/upload/文件名”就能下载指定文件。

21.2.3. 编写网页通知

- 1. 当用户选择默认通知内容形式时，在通知内容一栏的编辑内容以及页面预览效果如下图所示：

通知

因天气比较炎热~~~~~

通知

因天气比较炎热~~~~~

- 2. 当通知内容形式为html形式时的html代码以及相应的网页预览效果，如图：

```
<html>
<head>
  <title> 通知</title>
</head>

<body>
  <p>由于天气比较炎热，大家注意多喝水~~~</p>
  
</body>
</html>
```

由于天气比较炎热，大家注意多喝水~~~



提示

使用[% upload %]代表上传的图片路径，这里的路径和下面的图片通知路径都是相对路径，需要先上传文件后，再输入图片地址，格式：[% upload %]/文件名.后缀

用户如果希望推送出个性化的网页通知，可在头文件中编写相关的css样式

3. 若用户选择图片通知内容形式，用户只需将负载相关信息的图片载入图片地址框即可。

图片地址：

[% upload %]/1.jpg
[% upload %]/1.jpg






提示

在图片地址框中编辑图片路径时，每个图片的信息占一行。如果并排显示，图片显示不出。

4. 在通知内容形式为外部链接方式时URL链接形式及页面预览效果如下图所示，这里我们以百度为例：

链接地址：

http:// www.baidu.com

推送

默认消息

页面预览

查看状态



[新闻](#)[网页](#)[贴吧](#)[知道](#)[MP3](#)[图片](#)[视频](#)

百度一下

设置高级



提示

这里只需要输入地址即可，http://无需重新输入，否则找不到地址。



第 21 章 推送网页通知






第 22 章 预定义对象

file:///C:/Documents%20and%20Settings/Administrator/%D7%C0%C3%E6/share/user_guide.V8/notice.html[2013-12-9 15:10:08]



第 22 章 预定义对象

预定义对象分为IP对象、时间对象、网址对象和自定义端口。

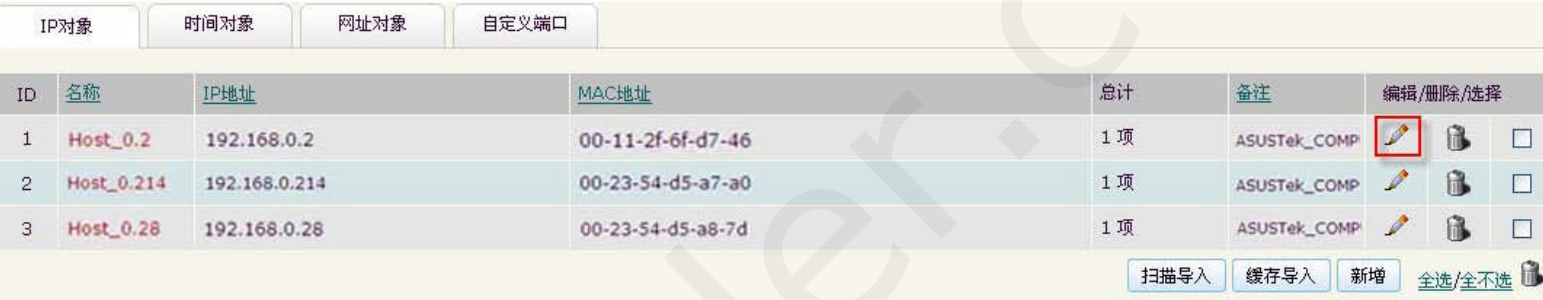
IP对象用于为局域网内的所有计算机命名易于记忆的名称来代替那些枯燥难记的IP地址和MAC地址等信息。

单击预定义对象，选择IP对象选项卡，单击扫描导入能将在一个局域网内的所有计算机导入到IP对象中。



图 22.1. 扫描导入所有计算机

单击每条后面的编辑按钮可以对各台计算机的相关属性进行编辑。



在这里，您可以填写名称标识符和相关个人信息。

名称:

Host_0.2

备注:

A主管

共 0 条记录

192.168.0.2

IP地址:

图 22.2. 编辑相关属性

您也可以点击下方新增按钮手动进行添加。



图 22.3. 手动新增

时间对象用于为上网行为管理添加时间模板。

新增...

名称:	<input type="text" value="工作时间"/> (只能由字母、数字、汉字、下划线、圆点及减号组成)					
备注:	<input type="text" value="技术支持部"/>					
日期/时间:	起始日期	✖	<input type="text" value="2011-07-01"/>	结束日期	✖	<input type="text" value="2011-07-31"/>
	起始时间	✖	<input type="text" value="09:00"/>	结束时间	✖	<input type="text" value="18:00"/>
	星期: <input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input checked="" type="checkbox"/> 工作日 <input type="checkbox"/> 全部					

保存设置 重置 取消

图 22.4. 添加时间模板

此名称和备注任意定义，起始时间和结束时间是此时间模板的生效时间，起始和结束时间是定义内的每天时间段，工作日默认指周一到周五。如上图，此模板是从2011年7月1日到31日，每周的周一到周五早9点到下午6点时间段生效。

网址对象用于自定义网址列表，用于集中设置允许访问或者不允许访问的网址。

名称:	<input type="text" value="不允许访问网址"/>
备注:	<input type="text" value="研发部"/>
	共 1 条记录 清空列表
	<div><div>.sina.com.cn</div><div>.qq.com</div></div>

图 22.5. 自定义网址

网址列表的域名最好填写网站的顶级域名，并保留域名前的“.”。这样才能更好地起到网站过滤的作用。

自定义端口用于定义多个端口列表，对列表中端口号进行统一管理。

名称:	<input type="text" value="服务器端口"/>
备注:	<input type="text" value="允许外网访问"/>
	共 0 条记录
	<div><div>80</div><div>4000</div><div>8000</div></div>

图 22.6. 自定义端口



第 23 章 对象分组管理

分组管理功能能够将多台计算机放在同一个分组内，使用该功能是为了将需要统一管理的计算机放在同一分组内，以组来整体配置提高管理效率。

选择对象分组管理进入IP分组选项卡，单击“新增”按钮进入以下界面，从成员列表（[预定义对象](#)将会自动显示在成员列表中）中选择需要进行统一管理的对象。

新增...

名称: (只能由字母、数字、汉字、下划线、圆点及减号组成)

备注:

成员:

当前成员

成员列表

<- 新增

删除 ->

<< 全部

全部 >>

保存设置

重设

取消

图 23.1. 新增组成员

此时，对象分组就完成了。如果需要对分组修改相关属性，可以单击编辑按钮重新设置相关属性。

ID	名称	成员	备注	状态/编辑/删除/选择
1	aa	Host_0.28, Host_0.214, Host_0.2		<input checked="" type="checkbox"/> <input type="checkbox"/>
2	bb	Host_0.28, Host_0.214, Host_0.2		<input checked="" type="checkbox"/> <input type="checkbox"/>

新增 全选/全不选

图 23.2. 编辑相关属性

协议分组用于自定义管理内容列表，如下图：

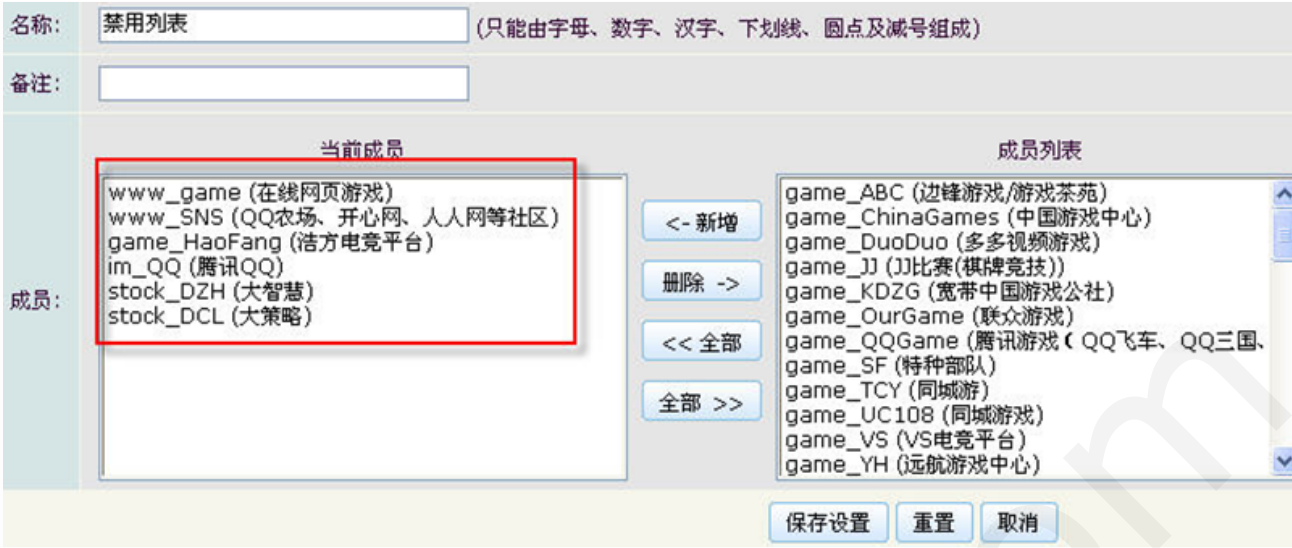


图 23.3. 协议分组

自定义一个名称，然后从右边的列表框中，抽出若干项需要管理的集合，新增到左边成员中。

时间列表用于对预定义的时间进行分组管理。



图 23.4. 时间列表

网址分组指对预定义对象里的网站进行分组管理，便于在应用协议控制里进行整体选择控制，如下：



图 23.5. 网址分组

端口分组也是对预定义对象列表中的端口进行分组管理。

名称:	服务器访问端口	(只能由字母、数字、汉字、下划线、圆点及减号)
备注:		
成员:	当前成员	
	<div>VPN端口 () web端口 (允许外网访问)</div>	<div>远程端口 ()</div> <div><- 新增</div> <div>删除 -></div>

图 23.6. 端口分组





第 24 章 应用协议过滤

- 设置指定的IP或者IP段只能访问特定的网页

1. 指定IP对象

进入“上网管理”->“预定义对象”->IP对象页面，新增IP对象：

IP对象					
应用协议对象					
时间对象					
网址对象					
自定义端口					
ID	名称	IP地址	MAC地址	备注	编辑/删除/选择
1	2.42	172.16.2.42		要控制的IP地址	

2. 定义允许访问的网址

进入 网址对象 页面，设定允许访问的网址，如下图所示：

IP对象					
应用协议对象					
时间对象					
网址对象					
自定义端口					
ID	名称	网址/域名	备注	编辑/删除/选择	
1	允许访问的网站	www.baidu.com .sina.com.cn	allow_url		

提示

网址过滤支持过滤含有以下字符的网址：

汉字、字母、数字、点 (.)、下划线(_)、斜线(/)、问号(?)、等号(=)、逻辑与 (&)、逗号(,)、分号(;))

例：可在网址列表中输入 video.*.*、/video

3. 进入“上网管理”->“应用协议控制”，对172.16.2.42的上网行为进行控制，设置如下：

<input checked="" type="checkbox"/> 启用应用协议过滤, 对象: <input checked="" type="checkbox"/> LAN-1 <input type="checkbox"/> LAN-2 <input type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> WLAN <input type="button" value="确定"/>								
ID	名称	IP对象	控制类别	时间对象	优先级	动作	备注	状态/编辑/删除
1	允许访问的网址	2.42	允许访问的网站 (allow_url)		1	通过	允许访问的网址	
2	拒绝访问所有网址	2.42	所有网站 (all)		2	拒绝		

新增 | 协议特征数据库 | 拦截日志 (文件大小: 21.89Kb)

提示

这里的对象根据实际过滤需要选择LAN-1、LAN-2、PPPoE、PPTP_VPN、WLAN等。并且允许访问的和不允许访问的网站优先级要设置的不一樣，并且允许访问的优先级要高些。

这样172.16.2.42这台PC机就只能访问百度和新浪的网页了，如果这台电脑访问其它网页可以在应用协议过滤页面下的拦截日志里

查看到拦截记录。

- 设置指定的IP拒绝访问某些网站，其它网站都能访问

1. 指定IP对象

进入“上网管理”->“预定义对象”->IP对象页面，新增IP对象：

IP对象					
应用协议对象					
时间对象					
网址对象					
自定义端口					
ID	名称	IP地址	MAC地址	备注	编辑/删除/选择
1	2.42	172.16.2.42		要控制的IP地址	  <input type="checkbox"/>

2. 定义拒绝访问的网站

进入 网址对象 页面，添加拒绝访问的网站，如下图所示：


IP对象				
应用协议对象				
时间对象				
网址对象				
自定义端口				
ID	名称	网址/域名	备注	编辑/删除/选择
1	允许访问的网站	www.baidu.com .sina.com.cn	allow_url	  <input type="checkbox"/>
2	所有网站	0.0.0.0	all	  <input type="checkbox"/>
3	拒绝访问的网站	.tudou.com		  <input type="checkbox"/>

3. 进入“上网管理”->“应用协议控制”，对172.16.2.42的上网行为进行控制，设置如下：

☒ 启用应用协议过滤, 对象: ☒ LAN-1 ☐ LAN-2 ☐ PPPoE ☐ PPTP_VPN ☐ WLAN 确定

ID	名称	IP对象	控制类别	时间对象	优先级	动作	备注	状态/编辑/删除
1	允许访问所有网址	2.42	所有网站 (all)		2	通过		  
2	允许访问的网址	2.42	允许访问的网站 (allow_url)		2	通过	允许访问的网址	  
3	拒绝访问的网站	2.42	拒绝访问的网站 ()		1	拒绝		  

新增 | [协议特征数据库](#) | [拦截日志](#) (文件大小: 21.96Kb)

 注意

这里设置时需修改允许访问的网址的优先级和动作！

这样172.16.2.42这台PC机就不能访问土豆网页了，但是可以访问其它网页，如果这台电脑访问土豆网可以在应用协议过滤页面下的拦截日志里查看到拦截记录。

- 设置其它应用协议控制如禁止登陆QQ

1. 进入“上网管理”->“应用协议控制”

2. 自定义名称和优先级，在控制对象里选择预定义的IP对象，在应用控制里选择“腾讯QQ”，下面的动作选择丢弃。

名称:	禁止QQ	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	1	(只能为数字, 数字越小优先级越高)
备注:		
控制对象:	10	
控制类别:	<input checked="" type="radio"/> 应用 im_QQ 腾讯QQ	
	<input type="radio"/> 网址	
	<input type="radio"/> 端口	
	<input type="radio"/> QQ号码: (如有多个请用逗号分割)	
时间限制:	<input type="checkbox"/> 是	
动作:	丢弃	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

3. 保存后，再运行QQ就会出现超时无法登陆





第 25 章 上网期限管理

上网期限管理功能可以对用户的上网时间进行有效的管理。

海蜘蛛软路由提供的上网期限管理功能可以方便地使管理员对特定的用户设置不同的上网期限，以及对即将到期的用户设置通知提醒。



注意

此种方式仅需对内网固定IP做此配置，对于PPPoE拨号帐号到期会自动提醒

- 登录海蜘蛛路由器进入 上网期限管理 页面，选择“新增”按钮，如图所示：



图 25.1. 新增项目

- 在新增页面中用户可以对指定的 IP对象 (可以为单个用户或者用户组) 进行上网时间段管理。这里以单个IP为例，如图：

新增...

名称:	qq	(只能由字母、数字、汉字、下划线、圆点及减号组成)
备注:		
IP对象:	Host_0.2 (ASUSTek_Computer_Inc.)	
时间段:	起始日期	2009-07-08
	结束日期	2009-07-11
	起始时间	11:25
	结束时间	23:25
优先级:		
(只能为数字, 数字越小优先级越高)		
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
<div>保存设置 重设 取消</div>		

图 25.2. 新增期限管理1

- 单击保存设置后页面将会自动跳转到期限管理页面显示刚刚新增的信息，如图：

参数设置		期限管理				
ID	名称	IP对象	时间段	优先级	备注	状态/编辑/删除
1	qq	Host_0.2	2009-07-08 11:25 ~ 2009-07-11 23:25	0		<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
新增						

图 25.3. 新增期限管理2

这样对不同的用户或者用户组的上网期限的设置就完成了，下面设置对即将到期的用户通知提醒。

选择“参数设置”进入参数设置管理页面，用户可以设置提醒时间、提醒频率、提示标题、提示内容以及跳转地址等的设置。

置

期限管理

启用上网期限管理:	<input checked="" type="checkbox"/> 是
启用到期通知提醒:	<input checked="" type="checkbox"/> 是
通知提醒时间:	用户上网到期之前 <input type="text" value="3"/> 天开始提醒 (默认为0, 即只在到期当天提醒)
通知提醒频率:	每隔 <input type="text" value="120"/> 分钟提醒一次 (范围: 1~720, 推荐 120)
提示标题:	<input type="text" value="宽带上网到期通知"/>
提示内容:	<div>尊敬的用户: 您好! 首先感谢您对我们宽带网业务的支持! 您的宽带网络使用即将到期, 为了不影响您的使用, 请您尽快到网络接入中心缴费. 特此通知!</div>
跳转网址:	<input type="text" value="http://www.baidu.com"/> (http://xx.yy.com, 用户点击 '我知道了' 后跳转到此网址)
管理签名信息:	<input type="text" value="网络接入管理中心"/>
已过期提示:	<input type="text" value="抱歉! 您由于上网到期已不能访问 Internet, 请续费. 谢谢"/>
未开通提示:	<input type="text" value="抱歉! 您的上网开通时间未到, 不能访问 Internet, 请等待"/>

保存设置

默认

页面预览

清空日志

日志记录 (0byte)

图 25.4. 上网到期提醒设置

此时主机名称为qq的用户可以访问Internet的期限以及其快到期时的页面提示都已经设置好了，以下是其在上网到期三天之前会看到的页面提示：

宽带上网到期通知

尊敬的用户:

您好!

首先感谢您对我们宽带网业务的支持!

您的宽带网络使用即将到期, 为了不影响您的使用, 请您尽快到网络接入中心缴费. 特此通知!

您的上网期限: 自 2009-07-08 00:18:00 至 2009-07-11 22:18:00

请您点击

我知道了

 恢复网页正常浏览。

--- 网络接入管理中心

图 25.5. 上网到期提醒页面



提示

上网期限管理功能仅对内网用户有效，对PPTP等VPN用户无效。



Hi-Spider.com



第 26 章 上网行为管理综合应用

目录

- [26.1. 网络拓扑结构](#)
- [26.2. 新建用户与分组](#)
- [26.3. 新建时间与网址对象](#)
- [26.4. 设置各组的应用协议控制](#)
- [26.5. 仅允许收发Web邮件](#)
- [26.6. 特征库的更新](#)

26.1. 网络拓扑结构

这里我们以下的网络结构为例来列举上网各种应用限制。

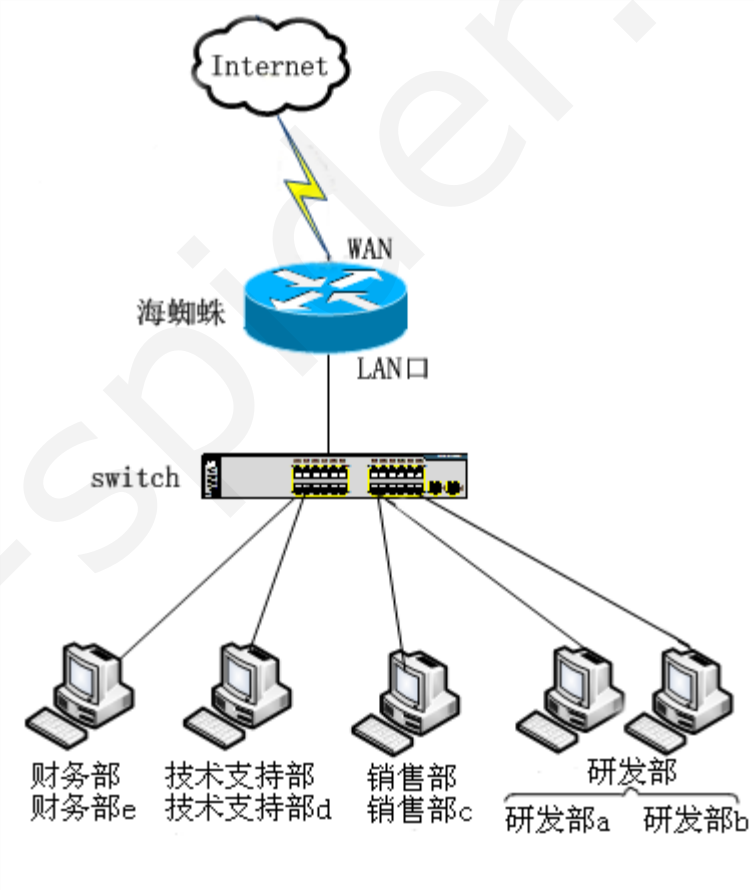


图 26.1. 网络拓扑图

此网络分4个部门，在各部门之间用不同的网络限制，具体如下：

1. 财务部只能访问工商银行。
2. 技术支持部只能收发电子邮件。

- 3. 销售部不能玩网页游戏，不能上QQ聊天。
- 4. 研发部上网不能访问百度和新浪网页，另外对研发部员工a禁止其使用炒股软件。



26.2. 新建用户与分组
第 26 章 上网行为管理综合应用



26.2. 新建用户与分组

登陆海蜘蛛路由主页面，进入“上网管理”->“预定义对象”，进入IP对象页面，选择“新增”，如图：

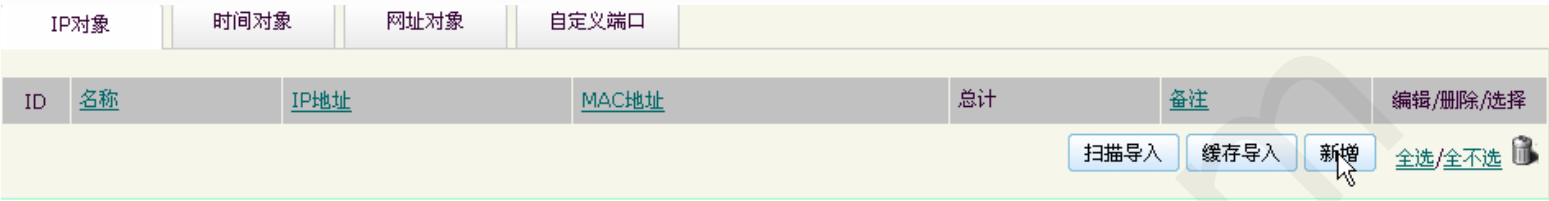


图 26.2. 用户对象

输入要管理对象的名称（自定义）和IP地址，然后点击“获取”，系统可根据IP地址自动获取其MAC地址，然后保存设置。



图 26.3. 新增对象

设置好所有用户后，我们再进行分组设置。进入“上网管理”->“对象分组管理”，进入IP分组页面，选择“新增”，如图：



图 26.4. 分组管理

这里我们按部门划分不同的组，例如我们这里把研发部a、研发部b划分为研发组，并保存。

名称：

备注：

当前成员

成员列表

研发部b ()
研发部a ()

<- 新增

删除 ->

<< 全部

全部 >>

技术支持部d ()
财务部e ()
销售部c ()

保存设置

重设

取消

图 26.5. 新增分组

分好组后，核对确认各组成员准确无误。如图：

IP分组					
协议分组					
时间分组					
网址分组					
端口分组					
ID	名称	成员	备注	状态/编辑/删除/选择	
1	技术支持部	技术支持部d		✓	
2	研发部	研发部b, 研发部a		✓	
3	财务部	财务部e		✓	
4	销售部	销售部c		✓	

图 26.6. 分组图



26.3. 新建时间与网址对象

第 26 章 上网行为管理综合应用

26.3. 新建时间与网址对象

进入“上网管理”->“预定义对象”，选择“时间对象”页面，选择“新增”，如图：


IP对象						
时间对象						
网址对象						
自定义端口						
ID	名称	日期段	时间段	星期	备注	编辑/删除/选择
新增 全选/全不选						

图 26.7. 时间对象

在编辑页面里，填好名称，选择起始与结束的日期，以及每天的起止时间：

名称：	<input type="text" value="上班时间"/> (只能由字母、数字、汉字、下划线、圆点及减号组成)			
备注：	<input type="text"/>			
日期/时间：	起始日期	<input type="text" value="2010-07-01"/>	结束日期	<input type="text" value="2010-07-31"/>
	起始时间	<input type="text" value="09:00"/>	结束时间	<input type="text" value="18:00"/>
星期： <input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input checked="" type="checkbox"/> 工作日 <input type="checkbox"/> 全部				
保存设置 重设 取消				

图 26.8. 时间设置

 注意

这里的星期是指每周上网管理限制的时间，工作日指周一到周五。

设定好后保存，再进入网址对象，选择“新增”，填写名称与网址并保存，如图：

名称：

访问工商银行

(只能由字母、数字、汉字、下划线、圆点及减号组成)

备注：

共 1 条记录 [清空列表](#) [?](#)

.icbc.com.cn

网址列表：

保存设置

重设

取消

图 26.9. 网址设置

注意

网址列表的域名最好填写网站的顶级域名，并保留域名前的“.”。这样才能更好地起到网站过滤的作用。

建立好所有相关网址，如图：

IP对象		时间对象		网址对象		自定义端口	
ID	名称	网址/域名		总计	备注	编辑/删除/选择	
1	访问工商银行	.icbc.com.cn		1 项			
2	访问新浪	.sina.com.cn		1 项			
3	访问百度	.baidu.com		1 项			

图 26.10. 网址对象

注意

这里的网址对象要包括允许用户访问的和禁止用户访问的两类网址。





26.4. 设置各组的应用协议控制

进入“上网管理”->“应用协议控制”。勾选“启用应用协议控制”，选择需要控制的对象，选择“新增”，如下图：



图 26.11. 应用协议管理

先设置可访问网站，设置一个高优先级，把控制对象设置为财务部，控制类别的网址设置为刚设定的“访问工商银行”，时间限制设置选择刚设定的上班时间，动作设为通过。

名称： (只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级： (只能为数字，数字越小优先级越高)

备注：

控制对象：

控制类别：

☐ 应用

☒ 网址

☐ 端口 [您尚未定义对象，请点击添加](#)

☐ QQ号码： (如有多个请用逗号分割)

时间限制：☒ 是

动作：

状态：☒ 激活 ☐ 禁用

保存设置

重设

取消

图 26.12. 财务部设置1

保存设置后还要设定其限制访问网站，点击“新增”，设定一个比刚才低的优先级，控制对象也设置为财务部，应用选择“ALL（所有Internet应用）”，时间限制选择上班时间，动作设为丢弃。

名称:

不可访问外网

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级:

2

(只能为数字, 数字越小优先级越高)

备注:

控制对象:

财务部

控制类别:

应用

ALL (所有Internet应用)

网址

端口

您尚未定义对象, 请点击添加

QQ号码:

(如有多个请用逗号分割)

时间限制:

☒ 是

上班时间

动作:

丢弃

状态:

☒ 激活

☐ 禁用

保存设置

重设

取消

图 26.13. 财务部设置2

这样两项设置好后，财务部在上班时间就只能访问工商银行了。

不可访问外网	财务部	ALL	所有Internet应用	上班时间 ()	2	丢弃			
只能访问工行	财务部	网址	访问工商银行 ()	上班时间 ()	1	通过			

图 26.14. 财务部设置3

接着设置技术支持部，点击“新增”，设置一个高优先级，把控制对象设置为技术支持部，控制类别应用设置为“general_Email 电子邮件收发（客户端方式）”，时间限制设置也选择上班时间，动作设为通过，如下图：

名称:

只能收发邮件

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级:

1

(只能为数字, 数字越小优先级越高)

备注:

控制对象:

技术支持部

控制类别:

应用

general_Email | 电子邮件收发(客户端方式)

网址

端口

您尚未定义对象, 请点击添加

QQ号码:

(如有多个请用逗号分割)

时间限制:

☒ 是

上班时间

动作:

通过

状态:

☒ 激活

☐ 禁用

保存设置

重设

取消

图 26.15. 技术支持部设置1



注意

这里的“电子邮件收发（客户端方式）”指的是允许用OUTLOOK，FOXMAIL等邮件客户端工具的收发，网页形式的邮箱不包含在内。

保存设置，继续设定其限制访问网站，点击“新增”，设定一个比刚才低的优先级，控制对象也设置为技术支持部，应用选择“ALL（所有Internet应用）”，时间限制选择上班时间，动作设为丢弃，如图所示：

名称：

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

(只能为数字，数字越小优先级越高)

备注：

控制对象：

控制类别：

☒ 应用

☐ 网址

☐ 端口 [您尚未定义对象，请点击添加](#)

☐ QQ号码：

(如有多个请用逗号分割)

时间限制：☒ 是

动作：

状态：☒ 激活 ☐ 禁用

保存设置

重设

取消

图 26.16. 技术支持部设置2

这样技术支持部就只能以客户端方式收发电子邮件了，接着设置销售部，点击“新增”，设置一个高优先级，把控制对象设置为销售部，控制类别应用设置为“www_game (在线网页游戏)”，时间限制设置选择上班时间，动作设为丢弃，如图所示：

名称：

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

(只能为数字，数字越小优先级越高)

备注：

控制对象：

控制类别：

☒ 应用

☐ 网址

☐ 端口 [您尚未定义对象，请点击添加](#)

☐ QQ号码：

(如有多个请用逗号分割)

时间限制：☒ 是

动作：

状态：☒ 激活 ☐ 禁用

保存设置

重设

取消

图 26.17. 销售部设置1

继续限制销售部使用QQ，点击“新增”，设定一个高优先级，控制对象设置为销售部，应用选择“im_QQ 腾讯QQ”，时间限制选择上班时间，动作设为丢

弃，如图：

名称：

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

(只能为数字, 数字越小优先级越高)

备注：

控制对象：

控制类别：

☒ 应用

☐ 网址

☐ 端口

☐ QQ号码

您尚未定义对象, 请点击添加

(如有多个请用逗号分割)

时间限制：☒ 是

动作：

状态：☒ 激活

☐ 禁用

保存设置

重设

取消

图 26.18. 销售部设置2

这样销售部就既不能玩网页游戏，也不能上QQ聊天了。

最后设置研发部，点击“新增”，设置一个高优先级，把控制对象设置为研发部，控制类别网址选择为“访问百度”，时间限制设置选择上班时间，动作设为丢弃，如图所示：

名称：

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

(只能为数字, 数字越小优先级越高)

备注：

控制对象：

控制类别：

☐ 应用

☒ 网址

☐ 端口

☐ QQ号码

您尚未定义对象, 请点击添加

(如有多个请用逗号分割)

时间限制：☒ 是

动作：

状态：☒ 激活

☐ 禁用

保存设置

重设

取消

图 26.19. 研发部设置1

这样研发部就不能访问百度了，同理可设置其不能访问新浪。

对于研发部的a，我们还要设置其不能使用炒股软件，点击“新增”，设置一个高优先级，把控制对象设置为研发部a，控制类别应用选择为“STOCK 股票类软件（包含特征库所有的炒股工具）”，时间限制设置选择上班时间，动作设为丢弃，如图：

名称:	<input type="text" value="不能上网炒股"/>		(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	<input type="text" value="0"/>	(只能为数字, 数字越小优先级越高)	
备注:	<input type="text"/>		
控制对象:	<input type="text" value="研发部a"/>		
控制类别:	<input checked="" type="radio"/> 应用 * STOCK 股票类软件 (包含特征库中所有炒股工具) *		
	<input type="radio"/> 网址 <input type="text"/>		
	<input type="radio"/> 端口 您尚未定义对象, 请点击添加		
	<input type="radio"/> QQ号码: <input type="text"/> (如有多个请用逗号分割)		
时间限制:	<input checked="" type="checkbox"/> 是	<input type="text" value="上班时间"/>	
动作:	<input type="text" value="丢弃"/>		
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用		
<div>保存设置 重设 取消</div>			


图 26.20. 研发部设置2

这样我们就按需求设置好了所有的限制管理，保存设置即可，如下图：

☒ 启用应用协议过滤, 对象:
 ☒ LAN-1
 ☒ LAN-2
 ☐ PPPoE
 ☐ PPTP_VPN
 ☐ WLAN
 确定

ID	名称	IP对象	控制类别		时间对象	备注	优先级	动作	状态/编辑/删除		
1	不能玩网页游戏	销售部	www_game	在线网页游戏	上班时间 ()		0	丢弃			
2	禁止聊QQ	销售部	im_QQ	腾讯QQ	上班时间 ()		1	丢弃			
3	不可访问外网	财务部	ALL	所有Internet应用	上班时间 ()		2	丢弃			
4	只能访问工行	财务部	网址	访问工商银行 ()	上班时间 ()		1	通过			
5	不能上网炒股	研发部a	STOCK	股票类软件(包含特征库中所有炒股工具)	上班时间 ()		0	丢弃			
6	不可访问新浪	研发部	网址	访问新浪 ()	上班时间 ()		1	丢弃			
7	不可访问百度	研发部	网址	访问百度 ()	上班时间 ()		1	丢弃			
8	只能收发邮件	技术支持部	general_Email	电子邮件收发(客户端方式)	上班时间 ()		1	通过			
9	不允许访问外网	技术支持部	ALL	所有Internet应用	上班时间 ()		2	丢弃			

图 26.21. 设置总图

 **重要**

这里我们把时间对象都设为了上班时间周一到周五每天的早9点到晚6点，如果想设置为无论何时都一直有这些管理限制，则在应用协议过滤设置页面里把时间限制的选择都去掉。



26.5. 仅允许收发Web邮件



注意

Build20121107以后的版本支持此项功能配置，应用协议特征库需升级到最新

应用协议控制中需要控制内网部分主机仅允许发送接收Web邮件，按如下方式来配置。

先预定义受控制的对象，进入“上网管理”->“预定义对象”，建立相应主机的IP对象：

IP对象						
时间对象						
网址对象						
自定义端口						
ID	名称	IP地址	MAC地址	总计	备注	编辑/删除/选择
1	小李	192.168.0.59		1 项		<input type="checkbox"/>
2	小王	192.168.0.58		1 项		<input type="checkbox"/>

图 26.22. 预定义对象

接着进入对象分组管理中，将要管理受控的主机分为一个组

IP分组				
协议分组				
时间分组				
网址分组				
端口分组				
ID	名称	成员	备注	状态/编辑/删除/选择
1	仅允许发送web邮件	小李, 小王		<input type="checkbox"/>

图 26.23. 分组管理

最后应用协议控制中对此组做如下三条设置：

禁止一切internet，优先级2，控制对象选择刚设立的分组，动作选择丢弃：

名称：

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

(只能为数字, 数字越小优先级越高)

备注：

控制对象：

仅允许发送web邮件

控制类别：

☒ 应用

ALL (所有 Internet 应用)

☐ 网址

禁访问网站

☐ 端口

服务器访问端口

☐ QQ 号码：

(如有多个请用逗号分割)

时间限制：☐ 是 ☐ 否

工作时间

动作：

丢弃

状态：☒ 激活 ☐ 禁用

图 26.24. 禁止一切internet

允许https协议通过，优先级1，控制对象选择刚设立的分组，动作选择通过：

名称：

允许https协议通过

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

1

(只能为数字, 数字越小优先级越高)

备注：

控制对象：

仅允许发送web邮件

控制类别：

应用

general_HTTPS

HTTPS 安全网页浏览

网址

禁访问网站

端口

服务器访问端口

QQ号码：

(如有多个请用逗号分割)

时间限制：

☐是

工作时间

动作：

通过

状态：

☒激活

☐禁用

图 26.25. 允许https协议

允许WebMail网页电子邮箱通过，优先级1，控制对象选择刚设立的分组，动作选择通过：

名称：

允许WebMail网页电子邮箱

(只能由字母、数字、汉字、下划线、圆点及减号组成)

优先级：

1

(只能为数字, 数字越小优先级越高)

备注：

控制对象：

仅允许发送web邮件

控制类别：

应用

www_webmail (WebMail/网页电子邮箱)

网址

禁访问网站

端口

服务器访问端口

QQ号码：

(如有多个请用逗号分割)

时间限制：

☐是

工作时间 (技术支持部)

动作：

通过

状态：

☒激活

☐禁用

图 26.26. 允许WebMail网页电子邮箱

全部配置好以后保存，启用应用协议过滤确定即可

☒ 启用应用协议过滤, 对象：☒ LAN-1 ☒ LAN-2 ☒ LAN-3 ☐ PPPoE ☐ PPTP_VPN

确定

ID	名称	IP对象	控制类别		时间对象	备注	优先级	动作	状态/编辑/删除		
1	允许https协议通过	仅允许发送web邮件	general_HTTPS	HTTPS 安全网页浏览			1	通过			
2	允许WebMail网页电子邮箱	仅允许发送web邮件	www_webmail	WebMail/网页电子邮箱			1	通过			
3	禁止一切internet	仅允许发送web邮件	ALL	所有Internet应用			2	丢弃			

图 26.27. 配置预览




26.6. 特征库的更新

对于新出来的某些上网软件，上网行为管理里设置可能会限制不了，这时请您做特征库的更新。进入“产品中心”->“特征库更新”，将后面的自动更新都勾选上，如图：

ID	名称	备注	版本	更新时间	自动更新	动作
1	f2154	恶意(病毒/木马)网址数据库	3.4.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新
2	rtable	多线策略路由表	2.0.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新
3	dnsserver_list	主要城市 DNS 地址列表	1.5.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新
4	ads_domain	广告域名数据库	1.2.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新
5	dnscap_list	常用网址域名 DNS 加速列表	1.4.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新
6	appmark	应用协议特征库	1.0.0	2010-06-18 10:33:00	<input checked="" type="checkbox"/>	检查更新
7	isp_list	主要 ISP 官方网址列表	1.5.0	2010-05-28 11:55:42	<input checked="" type="checkbox"/>	检查更新

图 26.28. 特征库更新

 注意

特征库更新并不一直都是更新状态，而是每隔12小时在网上检测，有新特征库时路由会自动下载。





部分 VI. 服务应用

目录

[27. 用户账号管理](#)

[28. DHCP服务](#)

[28.1. DHCP简介](#)

[28.2. 启动服务器端DHCP服务](#)

[28.3. 客户端配置](#)

[29. DNS代理解析](#)

[29.1. 启用DNS代理解析](#)

[29.2. DNS重定向](#)

[29.3. DNS劫持](#)

[30. NTP时间服务器](#)

[31. 网络打印服务](#)

[31.1. 网络打印解决方案](#)

[31.2. 服务端设置](#)

[31.3. 客户端设置](#)

[32. 上网Web认证](#)

[32.1. 上网Web认证简介](#)

[32.2. Web认证设置](#)

[32.2.1. 参数设置](#)

[32.2.2. 认证页面设置](#)

[32.2.3. 在线用户管理](#)

[32.3. Web用户帐号管理](#)

[32.4. 自定义Web认证页面](#)

[33. 局域网PPPoE服务](#)

[33.1. 什么是局域网 PPPoE](#)

[33.2. PPPoE 服务端的设定](#)

[33.3. PPPoE 客户端设置\(Windows \)](#)

[33.4. PPPoE 拨号专线客户端](#)

[33.4.1. PPPoE 拨号专线设置](#)

[33.5. 与第三方计费系统对接](#)

[33.5.1. 与蓝海卓越计费系统对接](#)

[33.6. 测试 PPPoE 连接](#)

[33.7. 管理已拨号用户](#)

[33.8. 客户机无法访问Internet](#)

[34. 虚拟专用网\(VPN\) PPTP 服务](#)

[34.1. 什么是 PPTP VPN](#)

[34.2. PPTP VPN 典型解决方案](#)

[34.3. PPTP VPN 服务端的设定](#)

[34.4. 使用内网 PPTP VPN 服务器](#)

[34.5. PPTP VPN 客户端设置\(Windows\)](#)

[34.6. 测试 VPN 连接](#)

[34.7. 常见错误及问题](#)

[34.8. PPTP VPN 虚拟双线（借线）](#)

[34.8.1. 借线服务器端设置](#)

[34.8.2. 借线客户端的设置](#)

[34.9. 和Win Server建立PPTP VPN连接](#)

[35. 虚拟专用网\(VPN\) SSL服务](#)

[35.1. 什么是 SSL VPN](#)

[35.2. SSL VPN 典型解决方案](#)

[35.3. SSL VPN 服务端的设定](#)

[35.4. 使用内网 SSL VPN 服务器](#)

[35.5. SSL VPN 客户端设置\(Windows\)](#)

[35.6. 测试 VPN 连接](#)

[35.7. 常见错误及问题](#)

[35.8. 局域网互连\(路由模式\)](#)

[35.8.1. 服务器端设置](#)

[35.8.2. 客户端设置](#)

[35.8.3. 测试连接](#)

[35.9. 局域网互连（桥接模式）](#)

[35.9.1. 服务器端设置](#)

[35.9.2. 客户端设置](#)

[35.10. 路由 SSL VPN 互联导入证书](#)

[36. IP 隧道服务](#)

[36.1. 什么是 IP 隧道服务](#)

[36.2. IP 隧道服务的网络拓扑图](#)

[36.3. IP 隧道服务服务端的设定](#)

[36.4. IP 隧道服务客户端设置](#)

[36.5. 测试 IP 隧道连接](#)





第 27 章 用户账号管理

用户帐号管理包括采用RADIUS认证模式时的PPPoE用户管理

- 新增用户
- 进入“服务应用”->“用户账号管理”->“新增用户”填写基本的信息。
- 例如用户名和密码都为：test

用户ID:	<input type="text" value="test"/>	(能由数字、字母、下划线、减号、@ 及圆点组成)
真实姓名:	<input type="text" value="张三"/>	
登录密码:	<input type="password" value="...."/>	(为空表示不修改)
密码确认:	<input type="password" value="...."/>	
帐号使用周期:	<div><div> </div>2009-06-01</div> [生效] <div><div> </div>2009-06-30</div> [到期]	
允许拨号的时间段:	<input type="text" value="Wk0800-2300"/>	
分配固定IP:	<input type="text" value="10.8.0.2"/>	(客户连接后始终获取此IP,仅适用于PPPoE/PPTP用户)
可用功能列表:	<input checked="" type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input type="checkbox"/> Web	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 27.1. 新增登录用户

“允许拨号的时间段”规则说明如下：

按照 周 表示法:

Su	表示 星期日
Mo	表示 星期一
Tu	表示 星期二
We	表示 星期三
Th	表示 星期四
Fr	表示 星期五
Sa	表示 星期六
Wk	表示 星期一~星期五
Al	表示 每天

时间采用 24 小时制，格式为： HHMM-HHMM
如果您想设置允许拨号的时间段为 早上8：00 至 晚上11:00 用 0800-2300 表示
例子： Wk0800-2300, Sa, Su2305-1655 （之间用 “,” 隔开）
这里表示您设置的时间段为： 周一至周五的早上8：00到晚上11：00，周六全日，周日晚上11：05之后 和 下午4：55之前。

“分配固定IP”规则说明如下：

客户使用 PPPoE/PPTP 连接后始终获取此IP ， 不做规定则自动分配。
此IP必须在 “ PPPoE 拨号服务 ” ——> “分配给客户机的地址空间” 的IP段内。

- “用户账号管理”——>“新增用户”其他设置说明：

安全设置

允许同时登录的最大用户数——>设置此账户最多可供登录的用户数
绑定客户机 MAC ——>使用于 PPPoE 服务，只允许从此 MAC 地址进行PPPoE拨号

允许同时登录的最大用户数:	<input type="text" value="100"/>
绑定客户机IP:	<input type="text"/> (只允许从此IP地址登录,仅适用于PPTP/Web用户)
PPPoE 属性	
绑定客户机MAC:	<input type="text" value="14-da-e9-75-de-e2"/> (只允许从此MAC地址登录,仅适用于PPPoE/Web用户)
自动绑定客户机MAC	<input checked="" type="checkbox"/> 是 (客户机第一次PPPoE拨号时,自动将其帐号与MAC地址绑定)

图 27.2. 安全设置

• 带宽限制

这些值依据您的实际情况来设置，不超过总带宽即可。

限制上行带宽:	<input type="text" value="100"/> Kb/s , 峰值速度: <input type="text" value="150"/> Kb/s (0表示不限制)
限制下行带宽:	<input type="text" value="100"/> Kb/s , 峰值速度: <input type="text" value="150"/> Kb/s (0表示不限制)

图 27.3. 带宽限制

• 模板管理（只对PPPoE和PPTP_VPN拨号时有效）

用户账号管理->模板管理->进入模板管理界面，选择新增模板：

编辑...

名称:	<input type="text" value="10:15-10:25限速"/> (只能由字母、数字、汉字、下划线、
备注:	<input type="text" value="10:15-10:25"/>
上行速度:	<input type="text" value="20"/> Kbyte/s (0表示不限制)
下行速度:	<input type="text" value="60"/> Kbyte/s (0表示不限制)
时间参数:	<input type="text" value="10:15-10:25"/>

图 27.4. 新建模板

建立如下模板：


ID	名称	时间参数	上行速度	下行速度	备注	编辑/删除/选择
1	10:00-10:15限速	10:00-10:15	20	100		<input type="checkbox"/>
2	10:15-10:25限速	10:15-10:25	20	60	10:15-10:25	<input type="checkbox"/>
3	10:25-10:35限速	10:25-10:35	80	150		<input type="checkbox"/>

图 27.5. 模板管理

设置好模板后，进入账号管理，开启使用模板功能，从模板列表中选择刚设定的模板：



图 27.6. 使用模板



提示

“时间参数”设置规则与“允许拨号的时间段”规则相同。

进入“信息监测”->“PPP连接信息”->日志记录，即可查看各个时间点的速度切换信息：

== 验证用户名: 002
== 在数据库中查找到匹配的帐号: 002
== 限制下行带宽为 300 kbps，通过设备 ppp0 ...
应用模板: 10:00-10:15限速，上行: 20 kbps，下行: 100 kbps
2009-11-24 10:15:08 调整 002|002 限速为上行: 20 kbps，下行: 60 kbps
2009-11-24 10:25:09 调整 002|002 限速为上行: 80 kbps，下行: 150 kbps
2009-11-24 10:35:10 调整 002|002 限速为上行: 100 kbps，下行: 300 kbps

您也可以在用户模板里设置成按星期建立不同规则。

名称:	<input type="text" value="按日限速规则"/>	(只能由字母、数字、汉字、下划线、
备注:	<input type="text"/>	
上行速度:	<input type="text" value="30"/> Kbyte/s (0表示不限制)	
下行速度:	<input type="text" value="100"/> Kbyte/s (0表示不限制)	
时间参数:	<input type="text" value="Wk0830-1800,Sa1600-0700,Su"/>	
<div>提交修改 重置 取消</div>		

图 27.7. 建立限速规则

这样，每周一到周五的08:30到18:00，周六的7点以前和16点以后，周日这些时间段都限制网速为上传为30K，下载为100K。



第 28 章 DHCP服务

目录

- [28.1. DHCP简介](#)
- [28.2. 启动服务器端DHCP服务](#)
- [28.3. 客户端配置](#)

28.1. DHCP简介

1. 什么是DHCP服务

DHCP (动态主机配置协议) 是Dynamic Host Configuration Protocol的缩写，它是TCP/IP协议簇中的一种，主要是用来给网络客户机分配动态的IP地址。这些被分配的IP地址都是DHCP服务器预先保留的一个由多个地址组成的地址集，并且它们一般是一段连续的地址。

2. 使用DHCP服务的好处

- 管理员可以集中为整个互联网指定通用和特定子网的TCP/IP参数，并且可以定义使用保留地址的客户机的参数。
- 提供安全可信的配置。DHCP避免了在每台计算机上手工输入数值引起的配置错误，还能防止网络上计算机配置地址的冲突。
- 使用DHCP服务器能大大减少配置花费的开销和重新配置网络上计算机的时间，服务器可以在指派地址租约时配置所有的附加配置值。
- 客户机不需手工配置TCP/IP协议。
- 客户机在子网间移动时，旧的IP地址自动释放以便再次使用。在再次启动客户机时，DHCP服务器会自动为客户机重新配置TCP/IP。
- 大部分路由器可以转发DHCP配置请求，因此，互联网的每个子网并不都需要DHCP服务器。



28.2. 启动服务器端DHCP服务
第 28 章 DHCP服务

28.2. 启动服务器端DHCP服务

- 登录海蜘蛛路由，进入“服务应用”->“DHCP服务”，在参数设置页面下启用DHCP服务：

参数设置

IP地址池

固定IP分配

当前IP分配信息

启用 DHCP 服务：

☒ 是

图 28.1. 开启DHCP服务

- 为客户机分配动态IP

选择“IP地址池”页面，选择新增地址池，如下图所示：

参数设置

IP地址池

固定IP分配

当前IP分配信息

ID	接口	分配的IP地址段	子网掩码	网关	备注	激活/编辑/删除/选择
<div>新增地址池</div>						

全选/全不选

☒

☐

☐

图 28.2. 新增地址池

进入IP分配地址池界面，选择您要配置DHCP的网络，例如这里是LAN-1，填入分配的IP地址范围、子网掩码、网关和DNS地址：

监听网络接口：

☐ 所有 LAN

☒ LAN-1 (eth2/eth2/192.168.0.11/255.255.255.0)

☐ LAN-2 (eth1/eth1/192.168.100.1/255.255.255.0)

☐ 无线局域网 (WLAN)

分配的IP范围：

192.168.0.2

-

192.168.0.254

(例如：10.0.0.1-10.0.0.100)

子网掩码：

255.255.255.0

(例如：255.255.255.0)

租约时间：

2

小时

(默认为2小时)

网关：

192.168.0.1

一般填系统局域网IP

首选DNS地址：

218.104.111.114

(这里一定要填写正确,否则客户机可能无法上网)

辅助DNS地址：

202.103.24.68

获取

WINS地址：

(NetBIOS名字解析服务器,可选)

NTP地址：

(时间服务器,可选)

PXE 启动文件：

TFTP 服务器IP：

备注：

状态：

☒ 激活

☐ 禁用

保存设置

重置

取消

图 28.3. IP地址池设置

下面的PXE启动和TFTP服务器IP属于可选项，对于无盘等内网环境才需要配置。



重要

IP地址分配范围需与所监听网络的LAN在同一网段下。

• 为客户机分配指定IP

DHCP在不同的时间对同一台客户机分配的IP地址一般都不相同，如果管理员想给某台客户机始终分配同一IP地址，则可使用固定IP分配功能。进入固定分配IP页面，如下图所示：



图 28.4. 新增固定IP

MAC地址:	<input type="text" value="00-F3-DE-9C-75-42"/>
IP地址:	<input type="text" value="192.168.0.93"/>
备注:	<input type="text"/>
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用

图 28.5. 固定IP设置

DHCP参数设置里的其它选项：

启用固定IP分配:	<input checked="" type="checkbox"/> 是				
第一次分配IP时自动将IP与MAC固定:	<input checked="" type="checkbox"/> 是				
第一次分配IP后自动将IP与MAC绑定到防火墙:	<input checked="" type="checkbox"/> 是				
访问控制策略:	<div><input checked="" type="radio"/> 为局域网中所有的用户提供 DHCP 服务 (*) <input type="radio"/> 只允许指定的 MAC 地址使用 DHCP 服务, 其他用户均不能使用 <input type="radio"/> 只允许 [固定IP分配] 列表中的用户使用 DHCP 服务, 其他均不能使用 <input type="radio"/> 禁止指定的 MAC 地址使用 DHCP 服务, 其他用户均可使用</div>				
MAC 地址列表:	<table><tr><td>允许</td><td>拒绝</td></tr><tr><td colspan="2"><div></div></td></tr></table>	允许	拒绝	<div></div>	
允许	拒绝				
<div></div>					

图 28.6. DHCP 其它设置

启用固定IP分配后，对接入路由的主机，路由系统会自动去查找固定IP分配页面里的固定列表项，对MAC地址匹配的主机会优先按固定IP列表进行分配。

启用第一次分配IP时自动将IP与MAC固定后，对新接入路由的主机，路由系统会自动按地址池分配IP并且将其IP-MAC信息自动导入到固定IP分配列表中。

启用第一次分配IP后自动将IP与MAC绑定到防火墙，需要先进入“防火墙”->“IP-MAC 绑定”中，启用IP与MAC地址绑定。路由系统会自动将新分配IP的主机信息导入到IP-MAC地址绑定列表中。

访问控制策略中，只允许指定的 MAC 地址使用 DHCP 服务是指填入下面 MAC 地址列表内允许栏里的地址，禁止指定的 MAC 地址使用 DHCP 服务是指填入下面 MAC 地址列表内拒绝栏里的地址。

下面的探测是检测内网有没有其它主机开启了DHCP服务，便于如小区检测下面用户有无私自架设DHCP服务器的，点击下面的探测按钮：

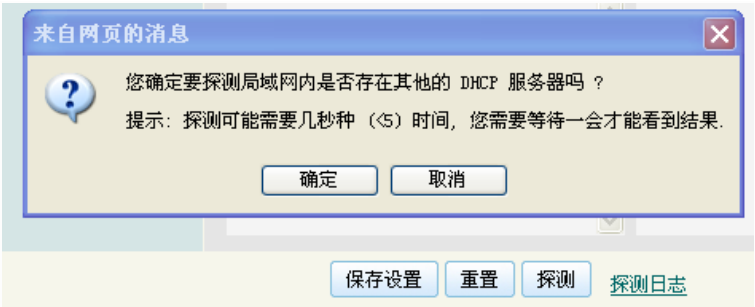


图 28.7. DHCP探测

探测后，点击后面的探测日志即可查看到探测结果，然后根据此IP和网卡地址找到相关的用户信息，如拨号帐号等。

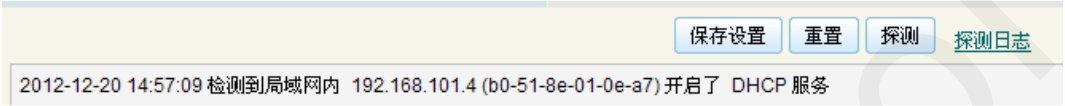


图 28.8.



28.3. 客户端配置

打开网络连接，进入TCP/IP协议栈，将IP地址与DNS服务器地址设置为 自动获取。如图：

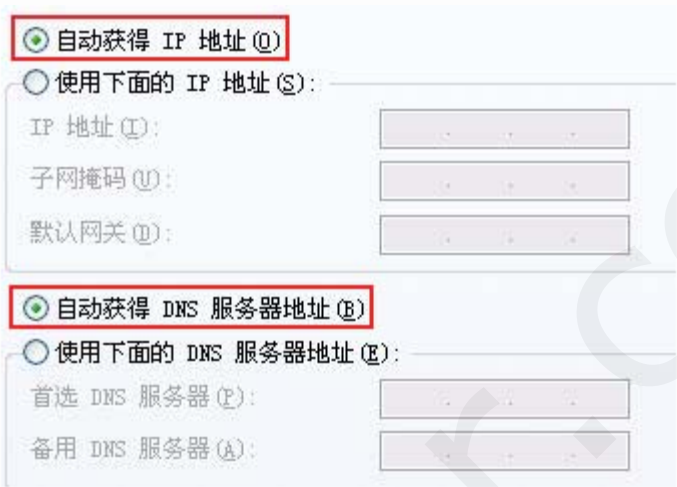


图 28.9. 客户机自动获取IP

客户机同样也可以查看其自动获取的IP信息

双击“本地连接”，进入“支持”->“详细信息”，如下图所示：

网络连接详细信息 (I):	
属性	数值
实际地址	00-11-2F-6F-D7-46
IP 地址	192.168.0.129
子网掩码	255.255.255.0
默认网关	192.168.0.254
DHCP 服务器	192.168.0.254
获得了租约	2009-7-13 15:47:32
租约过期	2009-7-13 17:47:32
DNS 服务器	219.149.194.55
WINS 服务器	219.150.32.132

图 28.10. 客户机获取IP信息





第 29 章 DNS代理解析

目录

- [29.1. 启用DNS代理解析](#)
- [29.2. DNS重定向](#)
- [29.3. DNS劫持](#)

29.1. 启用DNS代理解析

1. DNS代理简介

缓存中存放有DNS服务器已经解析的域名与其所对应的IP地址，并在客户机再次访问相同的域名时，DNS代理直接在缓存中查找并将结果返回客户端。

2. DNS代理解析的优点

缓存DNS解析结果，加快客户机域名解析的速度。

3. 启用DNS代理解析

Web方式登录海蜘蛛路由系统，进入“服务应用”下的“DNS 代理解析”，如下图所示：

DNS 解析服务状态: 运行中 (PID:1736) [查询日志](#) (888bytes) [统计分析](#) (需开启查询日志)

运行参数

DNS 重定向

高级

启用 DNS 域名解析服务:	<input checked="" type="checkbox"/> 是
强制使用 DNS 代理:	<input checked="" type="checkbox"/> 是 (DNS即插即用, 启用后客户机可任意配置DNS地址)
DNS查询记录缓存大小:	8192 (缓存DNS查询记录, 默认8192, 最大32768)
DNS缓存时间:	300 s (60~3600, 默认为 300)
记录查询日志:	<input checked="" type="checkbox"/> 是 (用于调试或分析网络)
查询时严格遵循DNS服务器顺序:	<input checked="" type="checkbox"/> 是 (一般开启)
一次查询所有DNS服务器:	<input type="checkbox"/> 是 (一般不开启)

图 29.1.

- 不启用海蜘蛛DNS代理解析时客户端的首选DNS配置情况如下所示，首选DNS服务器填当地的DNS域名服务器：

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

192 . 168 . 0 . 2

子网掩码 (M):

255 . 255 . 255 . 0

默认网关 (G):

192 . 168 . 0 . 254

☐ 自动获得 DNS 服务器地址 (B)

☒ 使用下面的 DNS 服务器地址 (E):

首选 DNS 服务器 (P):

219 . 149 . 194 . 55

备用 DNS 服务器 (A):

图 29.2.

- 启用海蜘蛛DNS代理解析时客户端的首选DNS配置情况如下所示，首选DNS服务器填路由的IP地址:

☒ 使用下面的 IP 地址(S):

IP 地址(I):

192 . 168 . 0 . 2

子网掩码(U):

255 . 255 . 255 . 0

默认网关(Q):

192 . 168 . 0 . 254

☐ 自动获得 DNS 服务器地址(E)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(Q):

192 . 168 . 0 . 254

备用 DNS 服务器(A):

图 29.3.

4. 查看DNS查询日志

DNS查询日志可以帮助用户了解域名解析的情况，单击“统计分析”，进入 DNS查询日志分析 界面，如下图所示：

DNS查询日志分析

域名服务器:	219.149.194.55, 219.150.32.132, 219.146.0.130		
域名服务器查询统计			
219.149.194.55	查询次数:	252	
	查询百分比:	98.82%	
219.150.32.132	查询次数:	3	
	查询百分比:	1.18%	
详细统计信息			
查询请求次数:	308	总回应次数:	737
缓存回应次数 :	83	缓存命中率:	11.26%
回应NXDOMAIN次数:	0	缓存NXDOMAIN总个数:	57
回应CNAME次数:	77	缓存CNAME总个数:	1
查询域名总个数:	173	回应域名总个数:	156
缓存域名总个数:	6	不存在域名总个数:	0
请求查询的客户数:	3		

请求查询次数前10名的域名		回应次数前10名的域名		请求查询次数前10名的IP	
域名	次数	域名	次数	IP	次数
search.114.vnet.cn	42	safebrowsing.cache.l.google.com	96	192.168.0.2	146
search.114.vnet.cn.diy.org	15	c.cnzz.com	75	192.168.0.214	110
search.114.vnet.cn.example.com	12	httpupdate.cpanel.net	22	127.0.0.1	52
www.newhua.com	12	sz6.tencent.com	21		
www.xdowns.com	11	www-google-analytics.l.google.com	18		
hsdfkj3.dfj-032424kdf.-hi.com	5	pingfore.qq.com	15		
ksdafjasdf.uisadfj.cjh.cjk	5	img1.qq.com	15		
ksdafjasdf.uisadfj.cjh.cjk.diy.o...	5	clients.l.google.com	15		
asdfkji.sdufisdfj.com.diy.org	5	profile.qshop.qq.com	12		
asdfkji.sdufisdfj.com	5	www.l.google.com	12		



29.2. DNS重定向

• DNS重定向的意义

DNS重定向可以用来禁止内网访问某些外网网址或域名，如果管理员需要禁止客户机访问某个网站，则可启用此功能。如下图：

<input checked="" type="checkbox"/> 启用内网DNS转向	
单个域名转向 每条记录占一行，例子：mydomain.com 192.168.0.1	<input checked="" type="checkbox"/> 批量域名重定向 将以下域名重定向到IP: 192.168.101.30
.microsoft.com 192.168.101.4 .xunlei.com 192.168.101.3 ###www.sina.com.cn 192.168.101.30	.www.hao123.com www.baidu.com



提示

这里重定向的IP地址可以随意书写，只要其不可达就行。

重定向设定为 .xunlei.com 192.168.101.3 则所有为.xunlei.com的域名都会被重定向，比如movie.xunlei.com，www.xunlei.com；重定向设定为www.xunlei.com 192.168.101.3 则只有www.xunlei.com这个域名会被重定向。

用户也可以在DOS环境下使用nslookup查看域名经过DNS重定向后的地址，这里以百度为例。如下图：

```
C:\Documents and Settings\Administrator>nslookup www.baidu.com
*** Can't find server name for address 192.168.0.254: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.0.254

Name: www.baidu.com
Address: 192.168.101.30

C:\Documents and Settings\Administrator>nslookup www.baidu.com
*** Can't find server name for address 192.168.0.254: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.0.254

Non-authoritative answer:
Name: www.a.shifen.com
Addresses: 119.75.213.61, 119.75.216.30
Aliases: www.baidu.com
```



Hi-Spider.com



29.3. DNS劫持

1. 什么是DNS劫持？

DNS劫持：通过某些手段取得某一服务提供商的DNS解析控制权，进而修改相应的域名记录值，使用该服务提供商DNS的用户在访问该域名时，并不会通过轮循的机制查询到域名真实的IP，而是会访问服务提供商DNS里面的记录值。

2. DNS劫持造成的影响

- 访问不到正确的网址
- 总是弹出恶意网站

3. 启用DNS劫持防护

单击“高级”选项卡，进入DNS劫持防护界面，用户只需将劫持后DNS解析的IP写入IP列表中即可防护DNS劫持。如下图所示：



图 29.4. DNS劫持防护





第 30 章 NTP时间服务器

NTP 是用来使系统和一个精确的时间源保持时间同步的协议，您可以将本系统配置成为一个时间服务器，为局域网提供时间同步服务。

1. 进入“服务应用”->“NTP时间服务”，在海蜘蛛上开启NTP时间服务器如下图所示：

时间服务器状态： 运行中 (PID:10385)

启用时间服务器：	<input checked="" type="checkbox"/> 是
强制使用时间服务器代理：	<input checked="" type="checkbox"/> 是 (启用后客户机通过任意时间服务器同步时都将指向本系统)
上级 NTP 服务器地址：	<input type="text" value="time.nist.gov"/> (多个地址用逗号分割)

图 30.1. 路由上设置NTP时间服务器

2. 客户机设置

双击客户机右下角的时间图标--选择 Internet时间 选项卡，将服务器IP地址设置路由LAN口IP地址，如下图所示：

日期和时间 属性

时间和日期 时区 Internet 时间

☒ 自动与 Internet 时间服务器同步 (S)

服务器:

与 172.16.2.2 同步时间成功，在 2010-3-22 在 11:58。

下次同步: 2010-3-29 在 11:58

同步只有在您的计算机与 Internet 连接时才能进行。有关更多信息，请参阅帮助和支持中心的[时间同步](#)。

图 30.2. 客户机上设置时间同步

点击“立即更新”即可同步时间：

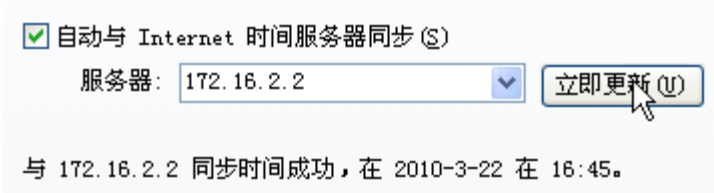


图 30.3. 同步更新





第 31 章 网络打印服务

目录

- [31.1. 网络打印解决方案](#)
- [31.2. 服务端设置](#)
- [31.3. 客户端设置](#)

31.1. 网络打印解决方案

- 网络打印简介

打印机使用外置的打印服务器，通过并口或USB口与安装海蜘蛛路由系统的电脑相连，再经路由实现网络打印功能。

- 详细拓扑图：

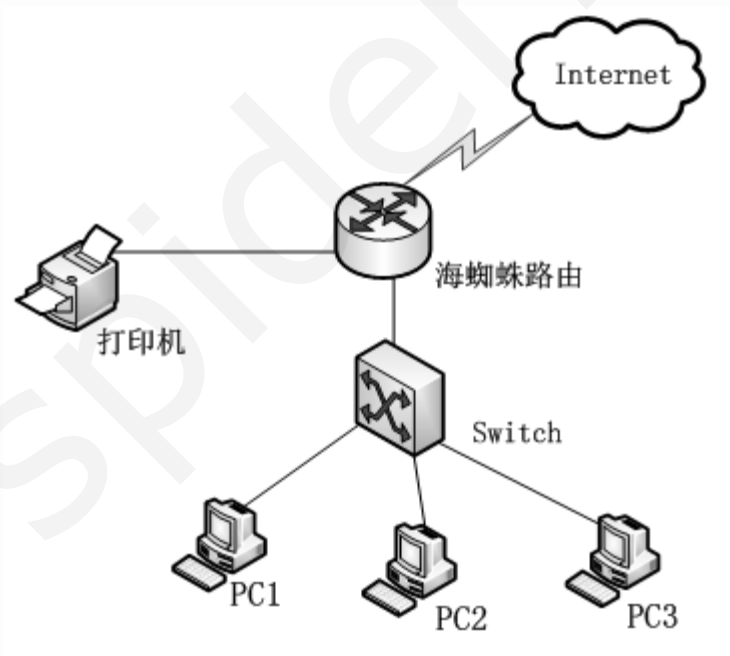


图 31.1. 网络拓扑图



31.2. 服务端设置

第 31 章 网络打印服务



31.2. 服务端设置

Web登录海蜘蛛路由->“服务应用”->“网络打印服务”，点击添加打印机，选择网络打印机及名字，页面设置如下如所示：

打印机:	Samsung ML-800 Series (Samsung ML-800 Series USB #1) ▾	
打印机名字:	<div>SX</div>	(只能由数字、字母或下划线组成)
是否设为默认打印机:	<input checked="" type="checkbox"/> 是	
打印机描述:	<div>sf</div>	



31.3. 客户端设置

第 31 章 网络打印服务

31.3. 客户端设置

- 需要打印服务的客户端首先安装打印驱动。
- 进入控制面板->打印机和传真->添加打印机，选择网络打印机：



图 31.2. 选择网络连接打印机

点击下一步，选择连接到Internet、家庭或办公网络上的打印机。URL里填入连接打印机的路由的IP地址，端口号设置为631，再加入printers，最后填入打印机名字，如下图：



图 31.3. 输入打印机地址端口及名称

继续点下一步，选择自己所要添加的打印机的型号即可成功将打印机添加到客户机上使用。





第 32 章 上网Web认证

目录

[32.1. 上网Web认证简介](#)

[32.2. Web认证设置](#)

[32.2.1. 参数设置](#)

[32.2.2. 认证页面设置](#)

[32.2.3. 在线用户管理](#)

[32.3. Web用户帐号管理](#)

[32.4. 自定义Web认证页面](#)

32.1. 上网Web认证简介

什么是上网Web认证

顾名思义，上网Web认证就是通过Web登录验证身份的一种方式。用户在浏览器中通过Web页面输入用户名和密码认证上网，不需要安装任何客户端软件。这种认证方式省去了在客户端创建连接的麻烦。



31.3. 客户端设置



32.2. Web认证设置




32.2. Web认证设置

32.2.1. 参数设置

Web登录海蜘蛛路由，进入“服务应用”->“Web 认证服务”，勾选启用上网 Web 认证，参数设置如下图所示：

启用上网 Web 认证:	<input checked="" type="checkbox"/> 是 运行中 (PID:2875)
在 PPPoE 上启用 Web 认证:	<input type="checkbox"/> 是
认证模式:	<input type="radio"/> 所有用户上网都必须通过 Web 认证 <input checked="" type="radio"/> 指定IP上网时须通过 Web 认证
上网时需要经过验证的IP:	<div>192.168.0.2</div>
会话存活超时时间:	<input type="text" value="300"/> s (多长时间没有检测到用户在线则强制重新认证, 默认300, 最少120)

图 32.1. 启用Web认证



提示

表示单个IP:192.168.0.2

表示一段连续的IP 192.168.0.2-192.168.0.6

表示网段: 192.168.0.0/24

若认证模式选择 所有用户必须通过Web认证，则连接在该路由器下的所有客户端在上网前都必须通过Web认证来验证身份。

若认证模式为 指定IP，则管理员可以将其IP地址填写在 上网时需要经过验证的IP 列表框中即可。

您也可以进入 认证页面 勾选下面的 登陆时启用验证码，这样Web登陆时在账号和密码下面会多出了个随机数字验证。

管理签名信息:	<input type="text"/>
允许用户自主修改密码	<input checked="" type="checkbox"/> 是
登录时启用验证码	<input checked="" type="checkbox"/> 是

图 32.2. 启用验证码

此时IP地址为192.168.0.2的客户机上网时将会看到如下[认证页面](#)：

上网认证


您好！

您需要使用合法的账户名和密码才能访问互联网！

请在以下输入框中输入帐号和密码登录，如果您有什么疑问，请与网络管理员联系，感谢您的支持！

帐号：

密码：

验证码：  [看不清？](#)

登录

--- 网络管理中心 QQ: 123456, Tel: 1234567

图 32.3. 客户端的Web认证登陆

32.2.2. 认证页面设置

用户可自行设置认证页面样式及各种属性，进入认证页面设置：

提示标题：	上网认证	(显示在浏览器标题栏)
提示内容：	<div>您好！</div> <div>您需要使用合法的账户名和密码才能访问互联网！</div> <div>请在以下输入框中输入帐号和密码登录，如果您有什么疑问，请与网络管理员联系，感谢您的支持！</div>	
多长时间后自动跳转：	0	s (0表示不显示提示直接跳转)
跳转网址：	http:// <input type="text" value="www.google.cn"/>	
管理签名信息：	网络管理中心 QQ: 123456, Tel: 1234567 (显示在提示框右下角)	

图 32.4. Web认证管理

32.2.3. 在线用户管理

管理员往往会基于某种原因需要断开用户连接。单击 在线用户 选项卡，单击其 IP地址 即可强制断开连接：

ID	IP地址	MAC地址	用户名	真实姓名	上线时间	备注
1	192.168.0.2	00-11-2f-6f-d7-46	001	001	2009-07-16 11:24:31	web

图 32.5. 在线用户管理

32.3. Web用户帐号管理

- 新增用户

Web登录海蜘蛛路由->“服务应用”->“用户帐号管理”，点击新增用户：

ID	用户名	真实姓名	可用功能	备注	使用期限（开通 - 到期）	状态	激活/编辑/删除/选择
1	222	222	PPPoE	-	~	正常	   <input type="checkbox"/>
2	333	333	PPPoE, Web	-	~	正常	   <input type="checkbox"/>
3	555	555	PPPoE	-	~	正常	   <input type="checkbox"/>
4	777	777	PPTP_VPN	-	~	正常	   <input type="checkbox"/>

[新增用户](#) [导出用户信息](#) [导入用户信息](#) [批量修改](#)

[全选/全不选](#)   

图 32.6. 新增账户

进入新增登录用户界面。输入用户名及密码，勾选Web认证，如图：

用户ID:

(能由数字、字母、下划线、减号、@ 及圆点组成)



真实姓名:

登录密码:



(为空表示不修改)

密码确认:

帐号使用周期:


 

[生效]

[到期]

允许拨号的时间段:



分配固定IP:

(客户连接后始终获取此IP,仅适用于PPPoE/PPTP用户)

可用功能列表:

☐ PPPoE

☐ PPTP_VPN

☐ SSL_VPN

☒ Web

状态:

☒ 激活

☐ 禁用


图 32.7. 账户设置

- 用户管理

管理员可编辑、修改、删除用户配置进行管理。

32.4. 自定义Web认证页面
第 32 章 上网Web认证

32.4. 自定义Web认证页面



注意

此功能仅20120824以后版本支持

进入Web认证->认证页面标签，勾选下面的使用自定义上传的认证页面：

参数设置

认证页面

在线用户

提示标题：

上网认证

(显示在浏览器标题栏)

提示内容：

您好！

您需要使用合法的账户名和密码才能访问互联网, 无线测试帐号及密码：1/1

请在以下输入框中输入帐号和密码登录, 如果您有什么疑问, 请与网络管理员联系, 感谢您的支持！

管理签名信息：

网络管理中心 QQ: 123456, Tel: 1234567

(显示在提示框右下角)

使用自定义上传的认证页面

☒ 是 (点击 [这里](#) 上传)

图 32.8. 使用自定义上传的认证页面

接着点击“这里”进入上传页面，将自定义的网页和图片都放在同一文件夹中压缩成ZIP/TAR/TGZ 格式，然后浏览找到该文件，勾选上传后是否自动解压缩后点击“上传”按钮

文件列表

上传文件

文件名：

C:\Documents and Settings\Administrat

浏览...

(最大不超过 30M)

重命名：

(为空表示不重命名)

备注：

是否自动覆盖已经存在的文件：

☐ 是

上传后是否自动解压缩：

☒ 是 (仅支持 ZIP/TAR/TGZ 格式压缩文件)

上传

重置

图 32.9. 上传自定义页面



图 32.10. 所有文件都在压缩包根目录

接下来用户Web认证就可以用新的页面打开了，如果需要页面预览，也需要在路由内网网关指向路由才能实现



图 32.11. 认证页面

也有不经过用户名密码自动认证跳转的认证方式，将此模板按上述方式上传后，需要在用户帐号管理中加入一个用户名密码为**hs**的特殊帐号，添加大数量级的允许同时登录数：

用户ID:	<input type="text" value="hs"/>	(能由数字、字母、下划线、
真实姓名:	<input type="text" value="特殊帐号"/>	
登录密码:	<input type="password" value=".."/>	(为空表示不修改)
密码确认:	<input type="password" value=".."/>	
帐号使用周期:	<input type="text" value=""/> <input type="button" value="X"/> [生效] <input type="text" value=""/> <input type="button" value="X"/> [到期]	
允许拨号的时间段:	<input type="text"/>	<input type="button" value="i"/>
分配固定IP:	<input type="text"/>	(客户连接后始终获取此IP,仅适用于PPPoE/PPTP)
可用功能列表:	<input type="checkbox"/> FTP <input type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input checked="" type="checkbox"/> Web	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
联系电话:	<input type="text"/>	
联系地址:	<input type="text"/>	
备注:	<input type="text" value="-"/>	
允许同时登录的最大用户数:	<input type="text" value="999"/>	

图 32.12. 添加特殊帐号

客户端打开会有两次页面跳转，打开任意一个网页会弹出如下页面：




图 32.13. 第一次跳转

点击“开始免费之旅”进行第二次跳转：



图 32.14. 第二次跳转

点击“开始上网”后即可通过认证正常上网。



注意

手机版本的认证页面会和PC版的认证页面的界面效果略微不同，功能上还是一致的。手机建议用UC、QQ、九天等浏览器

如果需要自行设计模板请注意以下几点：

- 所有文件都在一个文件夹下包括js css htm样式
- 所有页面文件都采用相对路径
- webauth_mobile.htm和webauth_pc.htm为手机和PC认证页面，文件名固定不能改变
- 打包时所有文件必须都为一级目录下，打包为zip格式
- html里面的images,css,js 文件路径必须加upload 例如：在webauth_mobile.html中有代码“upload/1.jpg” 而1.jpg与webauth_mobile.html放在同级目录

下面这段代码是配置自动登录时所需的：

```
$.ajax({
    type: 'POST',
    url: '/api/webauth',
    data: "username=hs&passwd=hs&action=login",
    dataType: 'json',
    success: function(data) {
        $("#btn_login").attr("disabled", "");
        $("#msg").html(data.msg);

        if (data.ret == 1 && from != ''){
            var url = '';
        }
    }
});
```

```

        if (data.redir == undefined){
            url = decodeURIComponent(from);
        }else{
            if (data.redir.match(/\?/)){
                url = data.redir + '&from='+from;
            }else{
                url = data.redir + '?from='+from;
            }
            window.location = url;
        }
    }
    });
    return false;
});
});
```





第 33 章 局域网PPPoE服务

目录

- [33.1. 什么是局域网 PPPoE](#)
- [33.2. PPPoE 服务端的设定](#)
- [33.3. PPPoE 客户端设置\(Windows \)](#)
- [33.4. PPPoE 拨号专线客户端](#)
 - [33.4.1. PPPoE 拨号专线设置](#)
- [33.5. 与第三方计费系统对接](#)
 - [33.5.1. 与蓝海卓越计费系统对接](#)
- [33.6. 测试 PPPoE 连接](#)
- [33.7. 管理已拨号用户](#)
- [33.8. 客户机无法访问Internet](#)

33.1. 什么是局域网 PPPoE

局域网PPPoE就是在一个局域网内所有客户机都采用PPPoE拨号到网关，通过网关的共享上网。

内网使用 PPPoE 的优点：

- 安装与操作方式简单，终端用户只需要建立一个宽带拨号
- 允许多个终端用户共享一个高速数据接入链路
- 利用 RADIUS 协议可以进行认证服务，针对不同的用户进行计费和控制管理
- 可避免传统网关模式ARP欺骗的困扰
- 适应小型企业和小区楼宇宽带运营商
- 可与现有网络结构相融合



注意

如果在划分了VLAN后使用PPPoE拨号，则只有与路由器LAN口IP处于同一网段的客户机可以拨号成功。



33.2. PPPoE 服务端的设定

第 33 章 局域网PPPoE服务



33.2. PPPoE 服务端的设定

登录Web主页面，进入“服务应用”->“PPPoE 拨号服务”，勾选 启用 PPPoE 拨号服务，具体配置如下：

运行参数

高级

带宽限制

专用PPPoE

在线用户

启用 PPPoE 拨号服务:	<input checked="" type="checkbox"/> 是
监听设备:	<input checked="" type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> 无线局域网 (WLAN)
PPPoE 服务器名字:	<input type="text" value="PPPoE_Server"/> 英文字符
用户认证模式:	<div><input type="radio"/> 无需验证(任意用户名和密码均可拨入)</div> <div><input type="radio"/> 简单验证模式(一个帐号可同时拨入多次) 帐号管理</div> <div><input checked="" type="radio"/> 本地RADIUS认证(可限制帐号拨入次数,有效期等) 帐号管理</div> <div><input type="radio"/> 外部 RADIUS 服务器认证计费</div>
服务端 PPP 连接IP地址:	<input type="text" value="87.0.0.1"/> (不能和局域网在同一网段)
分配给客户机的地址空间:	<input type="text" value="87.0.0.2"/> - <input type="text" value="87.0.10.254"/>
分配给客户机的 DNS 地址:	<input type="text" value="87.0.0.1"/> , <input type="text" value="8.8.8.8"/> <input type="checkbox"/> 自动设置
PPP 连接的 MTU (最大传输单元)值:	<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)
PPP 连接的 MRU (最大接收单元)值:	<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)
发送LCP(连接控制协议)数据包间隔:	<input type="text" value="30"/> 秒(默认为30,一般不超过60)
多少个LCP请求未应答则断开连接:	<input type="text" value="4"/> 个(默认为4,一般不超过6)
最大空闲时间(超过则主动断开连接):	<input type="text" value="0"/> 分钟 (0表示不自动断开)
拨号用户名区分大小写:	<input type="checkbox"/> 是
自动绑定客户机的 MAC 地址:	<input checked="" type="checkbox"/> 是
允许 PPPoE 客户之间互访	<input type="checkbox"/> 是
调试模式运行:	<input type="checkbox"/> 是
日志保存位置:	-- 内存 -- <input type="button" value="v"/>

保存设置

重置

默认

清空日志

图 33.1. PPPoE 拨号服务

在“用户认证模式”中有以下四个选项（用户可依据需求选择）：

- 1. 无需验证 ——> 任何用户名和密码均可拨入。
- 2. 简单验证模式 ——> 设置的账号可以同时拨入多次。
- 3. RADIUS 认证 ——> 可以限制账户拨入次数、时间、带宽、有效期等。
- 4. 外部 RADIUS 服务器认证计费 ——> 用于和第三方RADIUS服务器对接，采用对端设备来验证和限速等。

下面的 自动绑定客户机的MAC地址 是针对RADIUS认证账号而设置的，勾选后即对所有含PPPoE拨号服务的RADIUS认证账号启用MAC地址绑定，当客户机第一次运行PPPoE拨号时，自动将其帐号与MAC地址绑定。允许 PPPoE 客户之间互访选项根据实际需求选择，例如小区内居民用户就设置为不互访。

RADIUS 认证 的带宽限制和套用模板等设置参照 [用户账号管理](#)

设置完后点击“保存设置”。



注意

PPPoE 拨号服务分配给客户机的地址空间不要太大，否则会影响到客户端拨号的连接速度。

在高级页面中，可以设置PPPoE用户上网主页，是否允许用户自行修改拨号密码，是否显示用户MAC及绑定信息等，如下图：

重定向 PPPoE 用户上网首页	<input checked="" type="checkbox"/> 是
首页 URL 地址:	<input type="text" value="http://www.hao123.com"/> (http://xxx.yyy.com)
PPPoE 客户服务页面入口 IP 地址	<input type="text"/> (此IP的80端口必须能被访问)
允许用户自主修改密码	<input checked="" type="checkbox"/> 是
显示客户MAC地址信息	<input type="checkbox"/> 是
显示MAC地址绑定状态信息	<input type="checkbox"/> 是
启用 MAC 地址黑名单	<input checked="" type="checkbox"/> 列表中的客户机不能进行 PPPoE 拨号
MAC地址黑名单:	<div>90-E6-BA-DC-87-42</div>
强制用户通过PPPoE拨号上网:	<input checked="" type="checkbox"/> 是(客户机通过PPPoE拨号才能上网)
IP白名单 (两种方式均可上网):	<div>192.168.0.93 192.168.0.95</div>
名单 (访问列表中的IP段时不限速):	<div>192.168.0.55</div>

图 33.2. PPPoE拨号服务高级设置

上图中位于MAC黑名单中网卡MAC地址为90-E6-BA-DC-87-42的计算机，即使用户名和密码正确也无法通过RADIUS用户认证进行拨号上网。对于内网所有计算机均强制采用PPPoE拨号上网，仅对于IP白名单中为192.168.0.93和192.168.0.95的两台计算机可以无需拨号。限速白名单是用于内网服务器IP，例如这里IP为192.168.0.55提供影音服务，那么内网其它所有用户访问这个影音服务器时不受其帐号带宽限制。



注意

如果勾选了 允许用户自主修改密码，各用户拨号登录后需通过进入

http://pppoe.emufly.com 这个页面来修改密码，您也可以把此网址设置到 PPPoE 服务 下的重定向 首页 URL 地址。

如果勾选了启用强制 PPPoE 上网提示，下面用户如果不拨号会有提示页面

启用强制 PPPoE 上网提示	<input checked="" type="checkbox"/> 是 (未使用 PPPoE 拨号的用户上网时将会看到此提示)
拨号客户端文件名:	<input type="text"/> 未设置
提示标题:	<input type="text" value="用户认证方式更改通知"/> (显示在浏览器标题栏)
提示内容:	<div>尊敬的用户:</div> <div>为进一步优化宽带网络、减少病毒对网络的影响, 现已改用 PPPoE 虚拟拨号认证上网方式.</div> <div>PPPoE 拨号设置方法请 [link] [点击这里] [/link], 如果您有什么疑问, 请与网络管理员联系, 感谢您的支持 !</div>
管理签名信息:	<input type="text" value="网络管理中心 QQ: 123456, Tel: 1234567"/> (显示在提示框右下角)

保存设置

默认

重置

页面预览

清空日志

[日志记录](#) (0.0 byte)

图 33.3. 强制拨号提醒

路由下面的主机未拨号情况下，打开任意一个网页会出现如下提示：

用户认证方式更改通知

尊敬的用户：

为进一步优化宽带网络、减少病毒对网络的影响, 现已改用 PPPoE 虚拟拨号认证上网方式。

PPPoE 拨号设置方法请 [\[点击这里\]](#) , 如果您有什么疑问, 请与网络管理员联系, 感谢您的支持 !

--- 网络管理中心 QQ: 123456, Tel: 1234567

图 33.4. 提醒页面



重要

如果下面客户机未有此提示页面, 可在路由上设置DHCP, 将客户机的网关指向海蜘蛛的LAN口, 如果内网不设置网关指向路由, 客户端的本地连接是微软169开头的私有地址, 那么要保证内网就海蜘蛛路由一个网关设备才会出现此提示页面。





33.3. PPPoE 客户端设置(Windows)

使用海蜘蛛的 PPPoE 服务器功能，不需改变局域网的拓扑结构，很容易就能实现内网 PPPoE 拨号，具有方便可靠、成本低廉的特点。

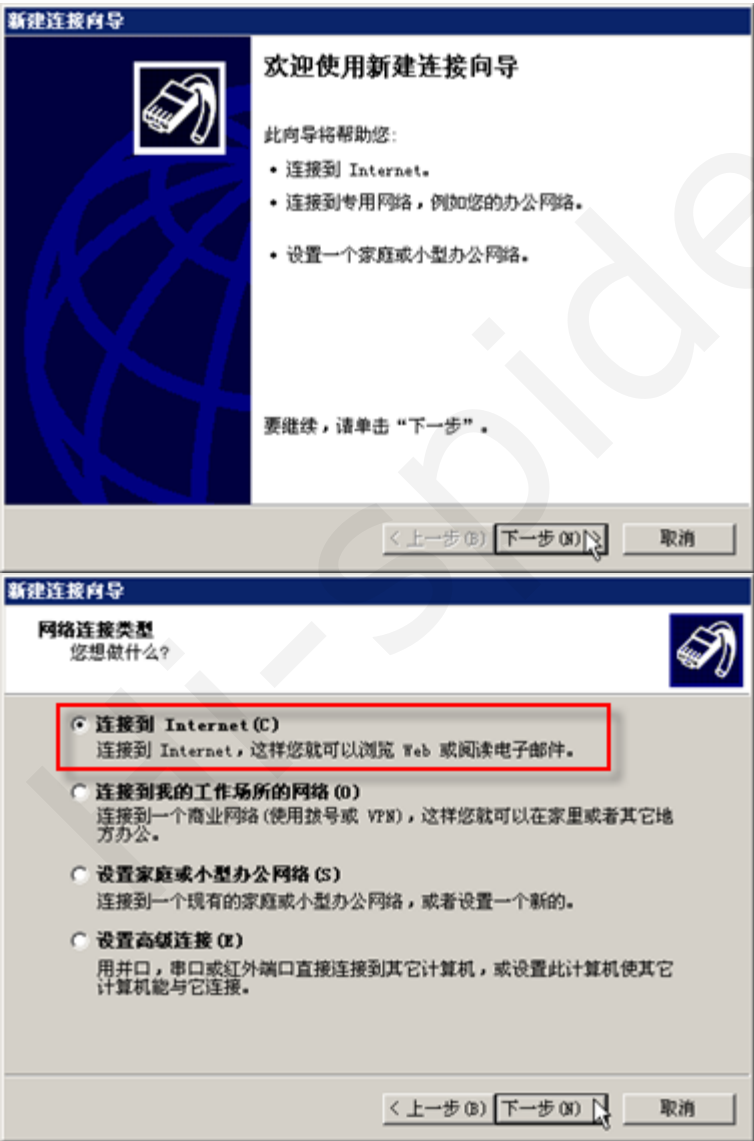
Windows 2000/XP/2003/Vista 自带有 PPPoE 的拨号客户端，无需另外安装软件。以 Windows XP 为例，设置步骤如下：

1. 启动新建连接向导

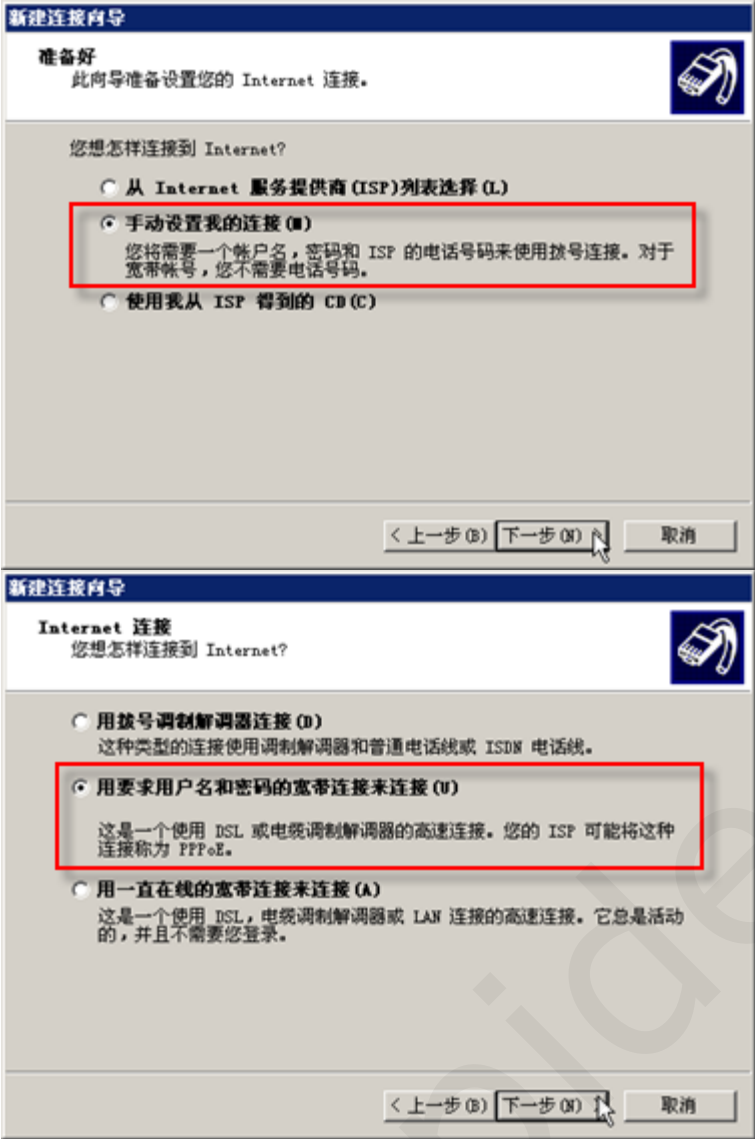
依次点击“开始”->“设置”->“网络连接”->“新建连接向导”即可。

或右键单击桌面上的“网上邻居”图标，选择“属性”，在“向导”栏双击“新建连接向导”。

点击“下一步”继续



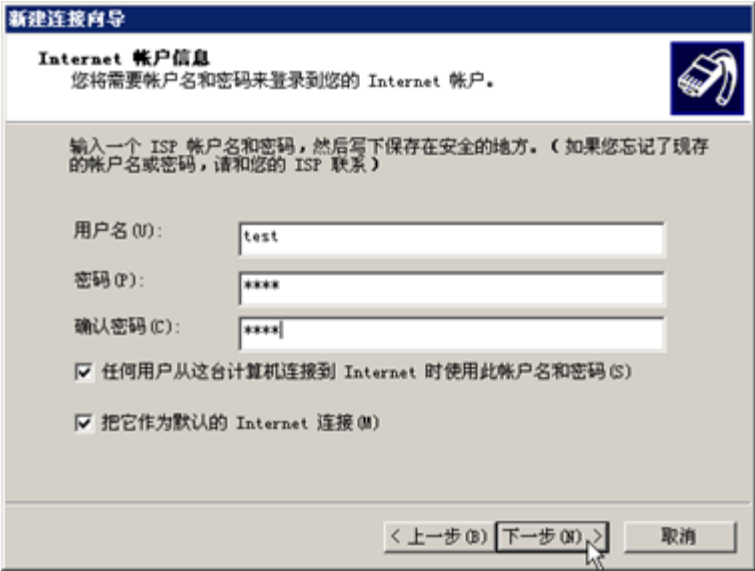
2. 选择连接类型



3. 设置连接名和账户信息

此用户名和密码必须是路由器上“服务应用”->“用户账号管理”里面已配置好的用户名和密码。





4. 完成连接向导

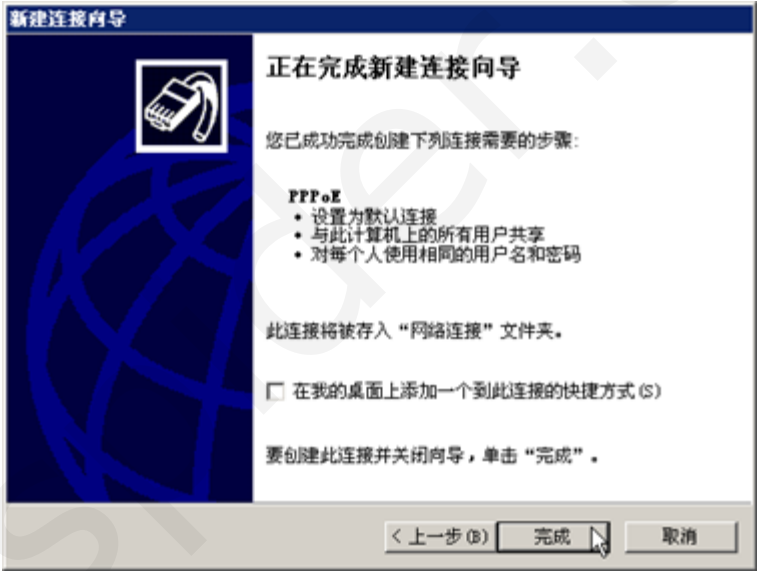


图 33.5. 完成连接向导

5. 打开建立的拨号连接，输入您的用户名和密码（test/test），点击“连接”即可。



图 33.6. PPPoE 连接



33.2. PPPoE 服务端的设定



33.4. PPPoE 拨号专线客户端



33.4. PPPoE 拨号专线客户端

利用PPPoE 拨号专线客户端的优势：

- 1. 在客户端到服务端之间形成加密体制，防止帐号密码被盗。
- 2. 杜绝PPPoE用户自行使用二级路由。
- 3. 禁止Windows系统的wifi共享。
- 4. 支持32位和64位全系列的Windows系统
- 5. 同时支持标准PPPoE拨号和海蜘蛛专用PPPoE拨号并自动识别
- 6. 能够和海蜘蛛认证计费系统的专用拨号客户端配置对接
- 7. 能够开机自动拨号到服务端

33.4.1. PPPoE 拨号专线设置

首选在服务端开启PPPoE 专线支持。

进入Web管理主页面，“服务应用”->“PPPoE 拨号服务”，进入专用 PPPoE 标签页。启用专用 PPPoE 拨号支持：

高级	带宽限制	专用PPPoE	在线用户
启用专用 PPPoE 拨号支持:		<input checked="" type="checkbox"/> 是	
强制所有帐号使用专用 PPPoE 拨号客户端:		<input type="checkbox"/> 是	
拨号客户端加密算法		<input checked="" type="radio"/> MD5 <input type="radio"/> SHA1	
自定义字符串		<input type="text" value="123qwe"/>	

图 33.7. 专用PPPoE服务

这里启用后，服务端对于专线拨号客户端和windows自带的拨号客户端都支持，是否需要加密由用户帐号管理中设置来决定。如果选用强制所有帐号使用专用 PPPoE 拨号客户端，那么所有客户端都必须用PPPoE 专线加密拨号才能拨成功。拨号客户端加密算法和字符串可以自定义。

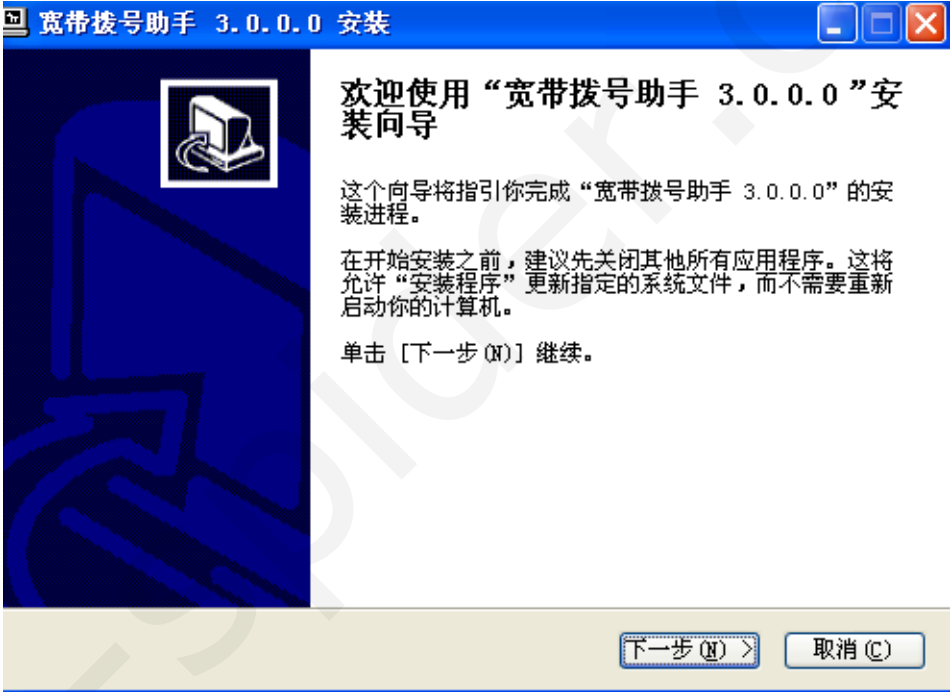
进入“服务应用”->“用户帐号管理”，勾选拨号客户端限制，如下图：

PPPoE 属性	
绑定客户机MAC:	<input type="text"/> (只允许从此MAC地址登录,仅适用于PPPoE/Web用户)
自动绑定客户机MAC	<input type="checkbox"/> 是 (客户机第一次PPPoE拨号时, 自动将其帐号与MAC地址绑定)
绑定拨入的 LAN 口:	<input checked="" type="radio"/> 任意接口(不绑定) <input type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> 无线局域网 (WLAN) (仅适用于 PPPoE)
终端负载数量	<input type="text"/> (0表示不限制)
拨号客户端限制:	<input checked="" type="checkbox"/> 是 (需要使用专用客户端才能PPPoE拨号成功)
是否强制拨号客户端在线:	<input type="checkbox"/> 是

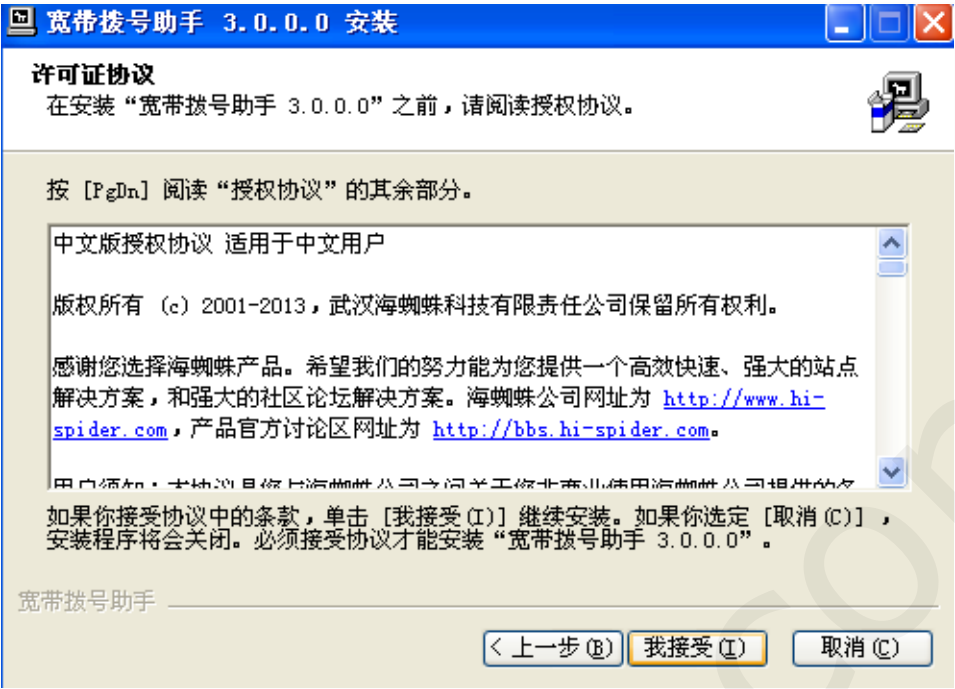
图 33.8. 拨号客户端限制

下载PPPoE 拨号专线客户端 [下载地址](#)

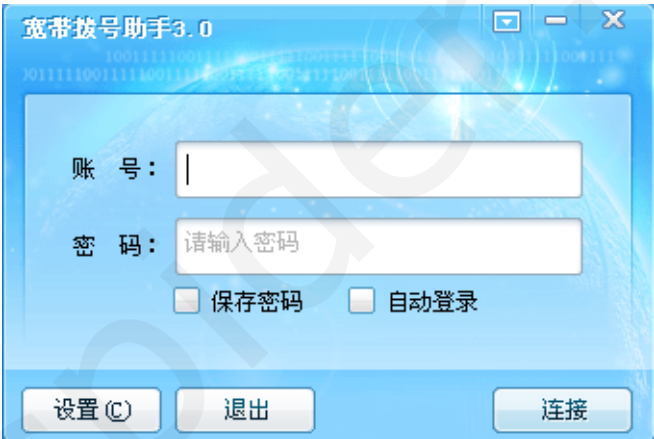
下载完成后，打开程序执行文件，双击HiRAS_Setup.exe安装程序，出现如下欢迎界面，点“下一步”继续安装：



安装程序进入许可协议界面，点“我接受”按钮接受许可协议并开始安装，并安装完成，如下图：



安装完成，启动客户端主窗口，如下图：



账号：这里输入运营商分配的宽带拨号账号。如果不知道账号，请与您的宽带运营商联系。

密码：这里输入运营商分配的宽带拨号密码。如果遗失密码，请与您的宽带运营商联系。

保存密码：强烈建议选中此选项，这样不需要重复输入密码。

自动登录：如果选中此选项，下次打开此软件时，将跳过此界面，自动使用保存的账号和密码进行拨号连接。选中此选项时，也自动选中“保存密码”。建议选中此选项。将运营商分配的账号和密码正确的输入后，点“连接”将进行拨号，拨号成功后，系统任务栏托盘中显示“蓝色”的带宽拨号助手图标，如下图：



拨号成功后，在任务栏托盘的宽带拨号助手图标上点右键，将出现如下菜单，选择“连接状态”查看当前的连接状态，如下图：



服务器IP：PPPoE 服务器端的IP地址。

客户端IP：本系统获得的IP地址。

状态：显示当前网络状态，显示为“已连接”或“未连接”。

持续时间：拨号成功后的上网时间。

发送字节：拨号成功后上传数据总量。

接收字节：拨号成功后下载数据总量。

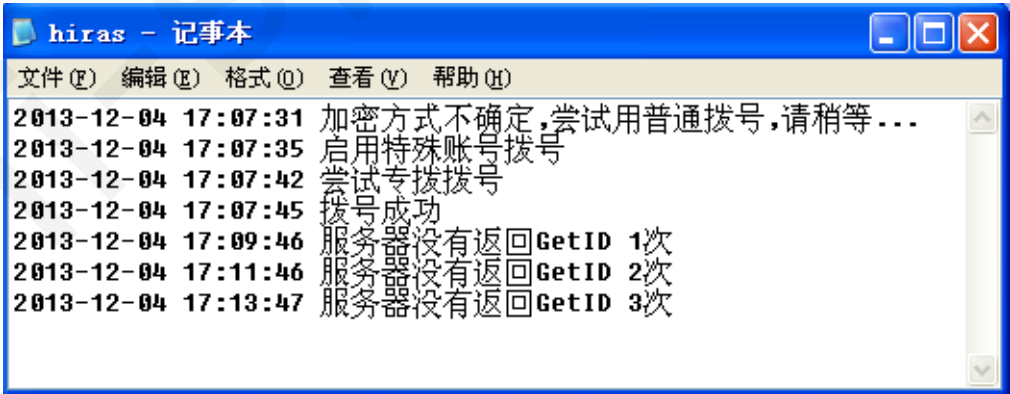
上传速度：当前上传网速。

下载速度：当前下载网速。

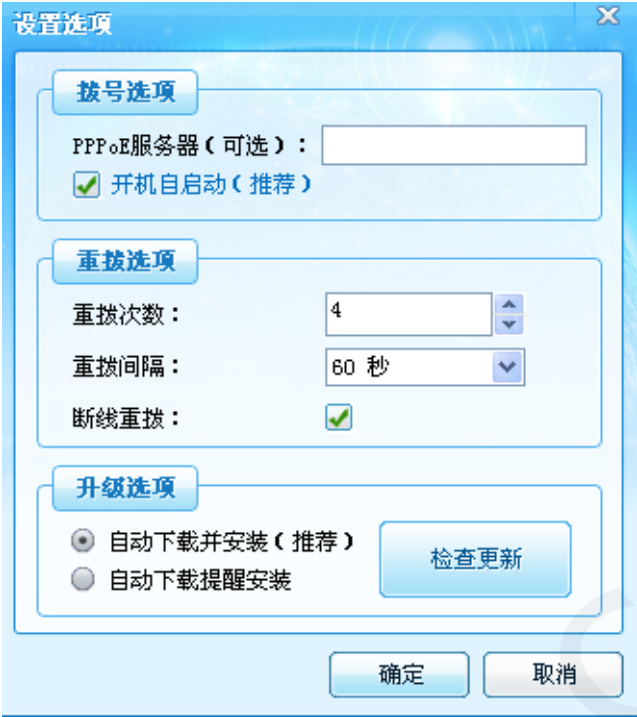
拨号日志：查看客户端拨号日志。

断开连接：断开当前已连接拨号。

在任务栏托盘的宽带拨号助手图标上点右键，菜单中选择“拨号日志”可以查看客户端拨号日志，如下图：



在主界面点“设置”或者在任务栏图标上点右键，选“设置选项”，进入设置选项配置界面，如下图：



PPPoE 服务器：输入PPPoE服务器的名称，系统将使用指定的PPPoE服务器进入拨号验证，当局域网中有多个PPPoE服务器时需要填写。

开机自启动：如果选中此选项，系统启动后将自动运行此程序；如果配置主界面中的“自动登录”选项，将可以做到开机自动拨号上网。建议使用此选项。

重拨次数：拨号失败后，将再尝试的次数。

重拨间隔：两次重拨之间间隔的时间。

断线重拨：意外掉线后，是否自动重拨，建议使用此选项。

自动下载并安装：系统将自动检查新版本，下载并在下次运行此软件时进行安装。建议使用此选项。

自动下载提醒安装：系统将自动检查新版本，并提醒您是否进行安装。

在主界面点击最小化按钮旁边的关于，有如下信息：



这里有上网助手的版本号、Build号和客户端标识信息，在路由的专用PPPoE拨号页面有相对应的设置

高级

带宽限制

专用PPPoE

在线用户

拨号监测

启用专用 PPPoE 拨号支持:	<input checked="" type="checkbox"/> 是
强制所有帐号使用专用 PPPoE 拨号客户端:	<input type="checkbox"/> 是
拨号客户端加密算法	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA1
自定义字符串	<input type="text" value="123qwe"/>
启用专拨V2	<input checked="" type="checkbox"/> 是
是否强制拨号客户端在线	<input checked="" type="checkbox"/> 是
是否检查拨号客户端版本	<input checked="" type="checkbox"/> 是, 版本号必需大于等于: <input type="text" value="20130913"/>
是否检测PC共享上网	<input checked="" type="checkbox"/> 是
是否检查客户端标识	<input checked="" type="checkbox"/> 是, 客户端标识: <input type="text" value="hispider"/>

是否强制拨号客户端在线是开启拨号客户端是否每隔5分钟向路由发送信息。

是否检查拨号客户端版本是检测客户端版本号，例如图中客户端要是20130913以后的版本才能拨上。

是否检测PC共享上网是开启对下面内网Windows的wifi共享上网的限制

是否检查客户端标识是开启标识检测，如上图标识是hispider，不一致则无法拨通。



33.5. 与第三方计费系统对接

33.5.1. 与蓝海卓越计费系统对接

进入“服务应用”下的“PPPoE拨号服务”项。勾选启用PPPoE拨号服务，在下面的用户认证模式里选择第三方外部 RADIUS 服务器认证，如下图：

启用 PPPoE 拨号服务：

☒ 是

监听设备：

☒ LAN1 ☐ LAN2 ☐ 无线局域网 (WLAN)

PPPoE 服务器名字：

test_pppoe_test 英文字符

用户认证模式：

☐ 无需验证(任意用户名和密码均可拨入)

☐ 简单验证模式(一个帐号可同时拨入多次) [帐号管理](#)

☐ RADIUS认证(可限制帐号拨入次数,有效期等) [帐号管理](#)

☒ 第三方外部 RADIUS 服务器认证

RADIUS 服务器地址：

111.111.111.111

共享密钥：

123

NAS 服务器标识：

认证端口：

1812 (默认 1812)

记账端口：

1813 (默认 1813)

图 33.9. 对接认证的海蜘蛛配置

其中RADIUS 服务器地址为蓝海卓越的WAN口IP地址，共享密钥在海蜘蛛上要与蓝海卓越上一致，NAS服务器标识为服务器名称，可以不填。认证端口和记账端口默认为1812和1813

登录计费后台管理员界面（默认IP地址为：192.168.1.250），添加对海蜘蛛客户端的支持：具体位置为“系统服务”下的“RADIUS管理”项，在此项中添加NAS，每一台海蜘蛛拨号服务器，均需单独添加为一个NAS设备，如下图所示：



图 33.10. 添加NAS

RADIUS项目添加完成后，登录前台用户管理的界面（默认IP端口是：192.168.1.250:7788，默认用户名密码admin）。登录后进入项目管理建立新项目：



图 33.11. 添加项目

项目建立完成后，在产品管理里添加各种不同的产品类别，定义诸如带宽速率、包月年等：

计费管理系统

系统信息

项目管理

产品管理

添加产品

产品管理

内网限速

规则管理

用户管理

营帐管理

报修管理

运营管理

产品管理

产品添加

产品名称：

产品类型：

包年

计费周期：

年

周期价格：

元

信用额度：

天

上传速率：

kbit

下载速率：

kbit

所属项目：

☐ 所有项目

产品描述：

提交

图 33.12. 添加产品种类

最后是添加用户，为每个用户选择项目和产品种类及个人信息等：

系统信息

项目管理

产品管理

用户管理

添加用户

用户管理

更换产品

停机恢复

用户销户

即将到期

到期用户

暂停用户

营帐管理

报修管理

运营管理

卡片管理

备份恢复

系统设置

用户添加

用户帐号：

用户密码：

所属项目：

选择项目

真实姓名：

证件号码：

工作电话：

家庭电话：

手机号码：

电子邮件：

联系地址：

选择产品：

请选择产品

预存金额：

0

元

地址分配：

☒ BRAS分配

☐ 系统分配

计时类型：

☒ 立即计时

☐ 上线计时

允许在线人数：

0

这里设置此用户允许同时在线个数，0表示不限制。当在线人数不等于 1 时地址必需为 “BRAS分配”。

开始时间：

计时类型如果为“立即计时”，开始时间为空表示从当前时间开始计算

MAC 地址：

☐ 是否绑定MAC地址

NAS 地址：

☐ 是否绑定NAS地址

提交

图 33.13. 添加用户

全部配置完后，就能够进行远程认证对接了。

重要



应确保蓝海卓越计费与海蜘蛛相互之间能通过IP地址正常通讯，UDP端口的1812和1813端口不能被封锁



33.4. PPPoE 拨号专线客户端



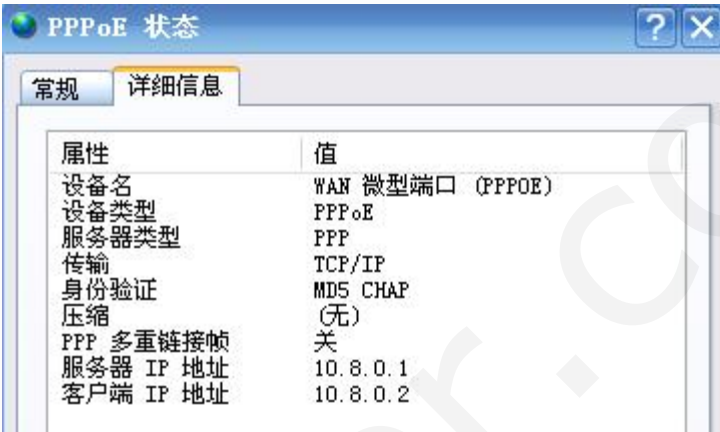
33.6. 测试 PPPoE 连接



33.6. 测试 PPPoE 连接

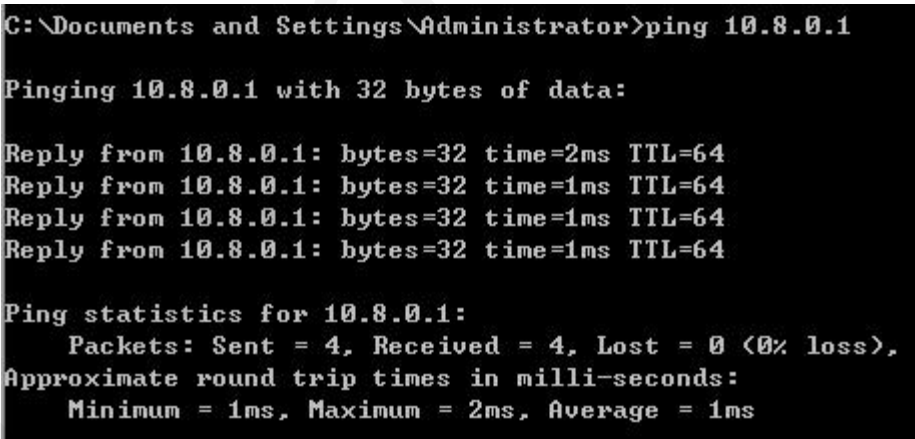
- 查看服务器端IP

在windows客户端打开网络连接，双击拨号连接图标，进入支持页面，单击详细信息选项卡，如下图所示：



- 测试PPPoE连接

进入DOS环境，使用ping命令测试连接是否正常。



注意

如果路由设置了“防火墙”->“基本安全设置”中“完全禁止了PING”，客户端是无法 Ping 通的。

☒ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求)





33.7. 管理已拨号用户

已拨号用户管理是对已经通过PPPoE方式拨号成功的用户进行管理。

登录海蜘蛛路由系统，进入“服务应用”下的“PPPoE 拨号服务”，单击“在线用户”进入PPP连接信息页面，这里显示了所有通过PPPoE拨号的连接信息，如下图所示：

ID	连接名	用户名	连接类型	本地IP 远程IP	总接收 总发送	连接时间 已连接	备注
1	ppp0	cs	本地 PPTP_VPN	172.16.0.101 172.16.0.1	136 Byte 146 Byte	2009-07-10 14:05:00 0 天 3 小时 10 分 34 秒	pptp1 -> 219.157.127.117
2	ppp1	0078008	PPPoE 客户	10.8.0.1 10.8.0.2	1.3 MB 10.6 MB	2009-07-10 16:27:22 0 天 0 小时 48 分 12 秒	00-11-2f-6f-d7-46 xiaoshenyang

图 33.14. 管理在线用户

单击 用户名 即可进入修改用户信息界面。

在某种情况下，管理员需要强制断开某个客户端的连接，此时只需点击“连接名”就可以断开相应连接，在客户端会出现断开提示：

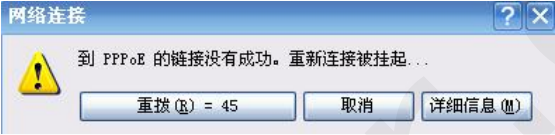


图 33.15. 断开用户链接

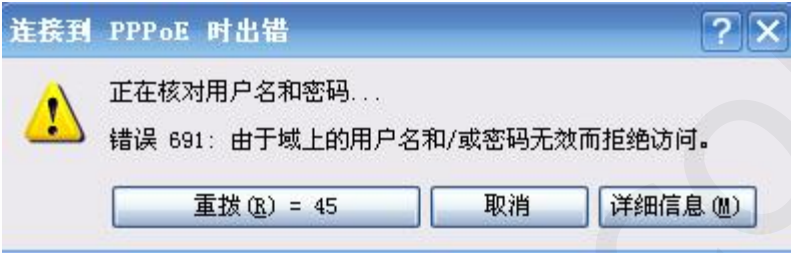




33.8. 客户机无法访问Internet

使用PPPoE服务的用户无法正常访问Internet时可能出现的情况：

1. 用户PPPoE拨号不能成功登录，一般会出现如下提示：



出现这种情况的原因：

- 输入的用户名和密码不正确
- 用户被设定在该时间内不能上网
- 上次的拨号连接非正常断线导致服务商后台系统没有收到用户下线信息，造成PPPOE接入服务器认为你的帐号重复拨号。

2. 用户PPPoE拨号成功，但不能上网

- 在DOS环境下用ping命令测试任何一个网址，比如百度，查看其连接是否正常。如果ping的通，则可能是DNS服务器的地址设置不正确。如果ping不同，则是外网线路出现故障或其它原因。

3. 错误678：无法连接到远程计算机，远程计算机无响应。

原因是不能连接到PPPOE接入服务器，可能是由于从用户端一直到PPPOE接入服务器整个链路中的某一个环节连接不通。

- 检查MODEM是否与局端设备同步上、网卡是否工作正常。
- 网络线路（电话线、网线）是否正常连接。

4. 错误619：无法连接到指定的服务器，用于此连接的端口已关闭。

原因是由于上次的连接出错，且重拨间隔时间过短，造成服务器对您的用户名和密码来不及响应。

- 间隔一到二分钟后重试。

5. 错误769：无法连接到指定目标。

原因可能是电脑的网络连接设备有问题。

- 打开“我的电脑”->“控制面板”->“网络连接”，查看本地连接的是否处在“禁用”状态，如果是，双击“本地连接”，将其启用。若是无法找到“本地连接”，重新安装网卡驱动程序。





第 34 章 虚拟专用网(VPN) PPTP 服务

目录

- [34.1. 什么是 PPTP VPN](#)
- [34.2. PPTP VPN 典型解决方案](#)
- [34.3. PPTP VPN 服务端的设定](#)
- [34.4. 使用内网 PPTP VPN 服务器](#)
- [34.5. PPTP VPN 客户端设置\(Windows\)](#)
- [34.6. 测试 VPN 连接](#)
- [34.7. 常见错误及问题](#)
- [34.8. PPTP VPN 虚拟双线（借线）](#)
 - [34.8.1. 借线服务器端设置](#)
 - [34.8.2. 借线客户端的设置](#)
- [34.9. 和Win Server建立PPTP VPN连接](#)

34.1. 什么是 PPTP VPN

VPN 即虚拟专用网 (Virtual Private Network)。是通过一个公用网络 (通常是Internet) 建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的隧道。

在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是利用某种公众网的资源动态组成的。由于 VPN 是在 Internet 上临时建立的安全专用虚拟网络，用户就节省了租用专线的昂贵费用。

通常，VPN是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立安全可信的连接，并保证数据的安全稳定传输。

建立VPN隧道有多种方式，包括 L2TP、IPSEC、PPTP、GRE、SSL 隧道，其中 PPTP (PPTP: Point to Point Tunneling Protocol) 点对点隧道协议 是VPN隧道中部署最为简单、方便的实现方式之一。利用Windows系统默认自带PPTP VPN客户端，只需几个步骤可以轻松完成VPN的设定。



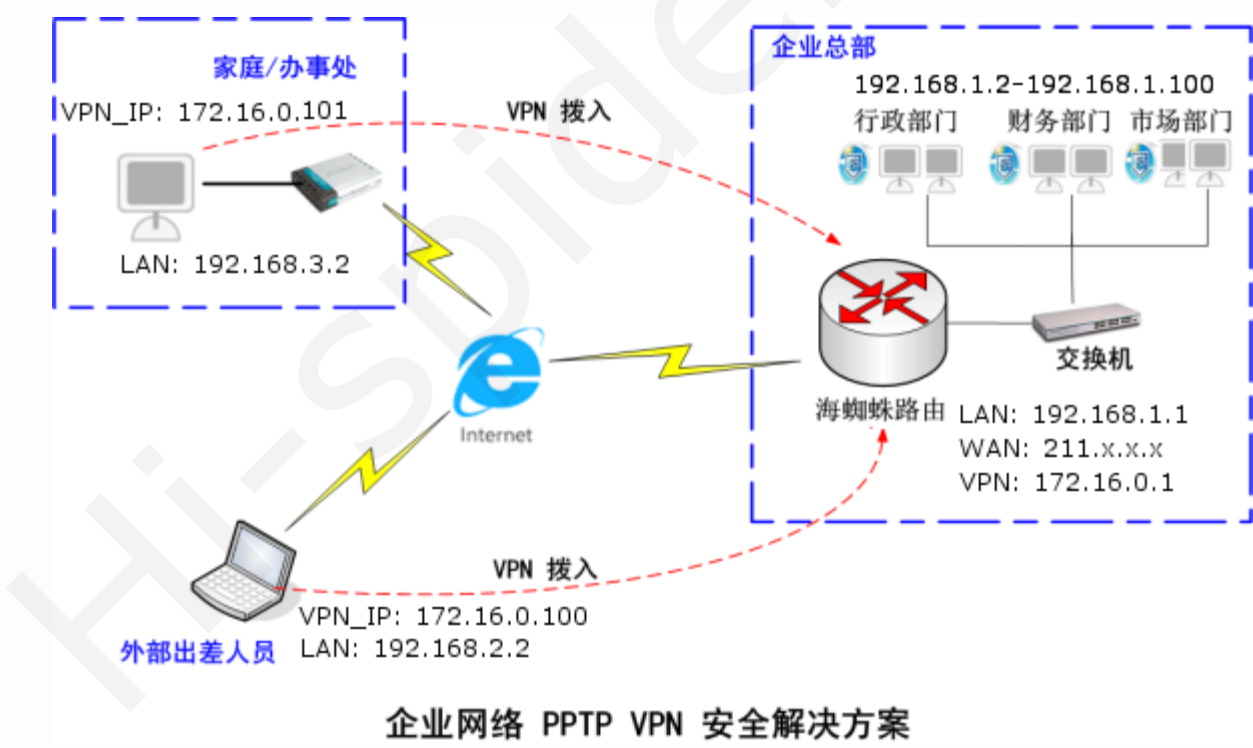


34.2. PPTP_VPN 典型解决方案

应用环境说明：

- 企业总部 (VPN服务端)
架设 VPN 服务器，允许远程用户拨入，外网IP为 211.X.X.X，VPN 服务器端 IP 为 172.16.0.1
- 某办事处 (VPN客户端)
需要经常和总部交换数据，通过 VPN 拨号到总部。拨入成功后虚拟通道被建立，获得虚拟 IP: 172.16.0.101。
由VPN通道进入总部内部局域网，上传和下载数据。
- 出差人员 (VPN客户端)
需要和总部交换数据时，通过 VPN 拨号到总部。拨入成功后虚拟通道被建立，获得虚拟 IP: 172.16.0.100。
由VPN通道进入总部内部局域网，上传和下载数据，或和其他拨入点(如办事处或其他出差人员)相互通讯。

相关图示如下：





34.3. PPTP_VPN 服务端的设定

如果内网已有 PPTP_VPN 服务器，想让其对外提供拨入服务，请参考：[使用内网 PPTP_VPN 服务器](#)


如果使路由自己充当 VPN 服务器，需要进行如下设置：

1. 设定 PPTP_VPN 服务参数

进入“服务应用”->“PPTP VPN服务”，如下图：

VPN服务端IP:	172.16.0.1
VPN客户端IP范围:	172.16.0. 100 - 200
VPN连接的最大传输单元(MTU):	1492 (请谨慎修改, 默认为1492)
VPN连接的最大接收单元(MRU):	1492 (请谨慎修改, 默认为1492)
发送LCP(连接控制协议)数据包间隔:	20 秒(默认为20, 一般不超过60)
多少个LCP请求未应答则断开连接:	3 个(默认为3, 一般不超过6)
允许VPN客户端之间互相访问:	<input checked="" type="checkbox"/> 是
启用 VPN-to-Internet 通道:	<input checked="" type="checkbox"/> 是
启用调试模式:	<input type="checkbox"/> 是
支持的身份验证协议:	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
强制MPPE数据加密(没有就断开):	<input checked="" type="checkbox"/> 是

VPN 网络上使用的是内部保留IP地址，一般用 192.168.x.x 或 172.16.x.x 或 10.10.x.x，这里我们使用 172.16.0.x，可根据实际情况自行调整。

 重要

VPN 网络地址不能和本地局域网地址重复，也不要和远程拨入端的局域网地址重复。

为了防止冲突，建议把 VPN 网络地址设为比较特殊，比如 172.16.100.x 或 192.168.123.x 等。

2. 添加 VPN 用户

进入“服务应用”->“用户账号管理”，点击新增用户，在可用功能列表中勾选PPTP_VPN，如下图：

新增...

用户ID:	<input type="text" value="test"/>	(能由数字、字母、下划线、减号、@ 及圆点组成)
真实姓名:	<input type="text" value="test"/>	
登录密码:	<input type="password" value="...."/>	(为空表示不修改)
密码确认:	<input type="password" value="...."/>	
帐号使用周期:	<div> <input type="text"/></div>	<div> <input type="text"/></div> [生效] [到期]
允许拨号的时间段:	<input type="text"/>	
分配固定IP:	<div><div>172.16.0.100</div><input type="text"/></div>	(客户连接后始终获取此IP,仅适用于PPPoE/PPTP用户)
可用功能列表:	<div><input type="checkbox"/> PPPoE <input checked="" type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input type="checkbox"/> Web</div>	
状态:	<div><input checked="" type="radio"/> 激活 <input type="radio"/> 禁用</div>	

如果需要让某个帐户拨号后始终获得一个固定的VPN IP，在“分配固定 IP”项输入想要分配的IP即可，比如这里是172.16.0.100。

提示

分配给用户的固定IP必须在服务端所设定的VPN网络地址内。





34.4. 使用内网 PPTP_VPN 服务器

如果想让内网已经有 PPTP_VPN 的服务器对外提供拨入服务，假设其IP地址为192.168.1.254，那么在路由上只需要做如下设置：

1. 映射 PPTP_VPN 端口 (TCP/1723)

进入“防火墙”->“端口映射”，点击新增规则，添加一条规则，如图：

优先级：	1	(只能为数字, 数字越小优先级越高)
协议类型：	TCP	
对外端口：	1723 -	
对外 IP：	== 所有外网IP (默认) ==	
对内端口：	1723 -	
对内 IP：	192.168.1.254	
备注：	pptp vpn server	

2. 启用 PPTP_VPN NAT 穿透支持

进入“防火墙”->“基本安全设置”，点击“特殊应用”，勾选如下选项：

☒ 启用 PPTP_VPN NAT 穿透支持 (PPTP VPN 拨号时需要选上)

然后在内网 PPTP_VPN 服务器上添加相关的 VPN 帐户即可。



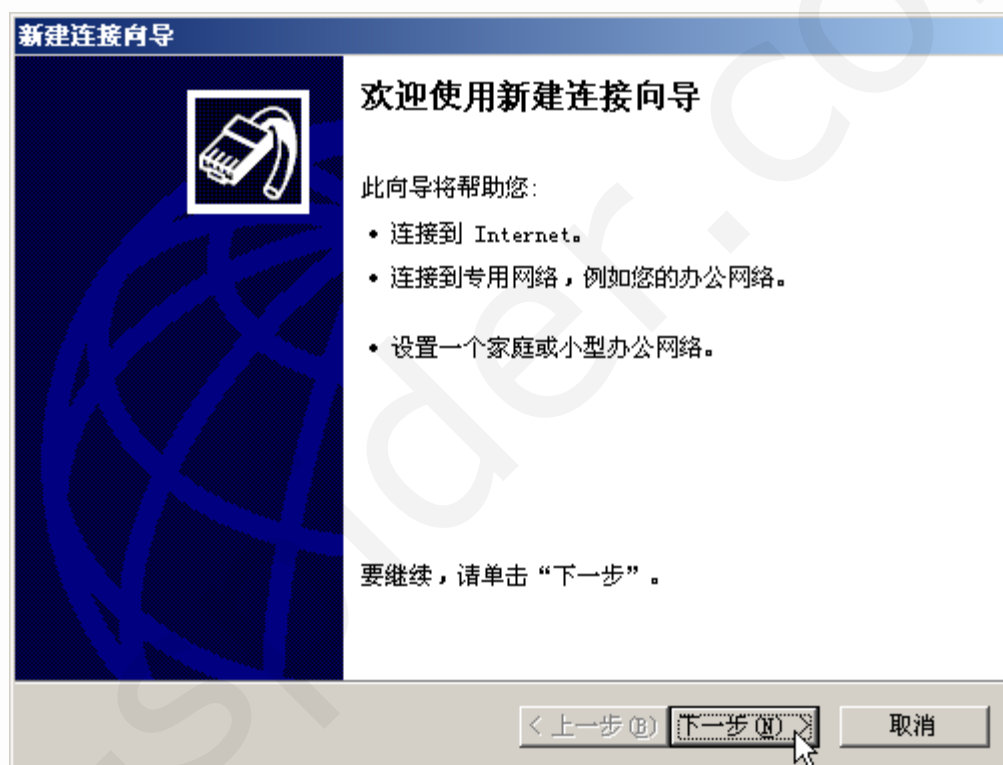
34.5. PPTP_VPN 客户端设置(Windows)

Windows 2000/XP/2003/Vista 自带有 PPTP_VPN 的拨号客户端，无需另外安装软件。以 Windows XP 为例，设置步骤如下：

1. 启动新建连接向导

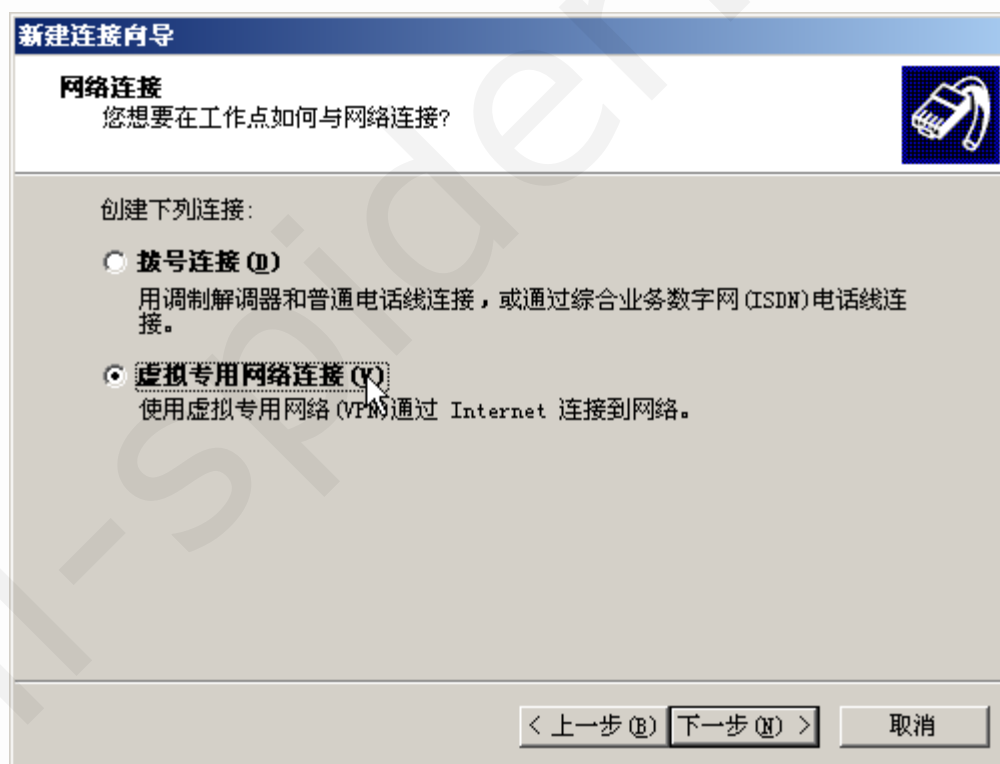
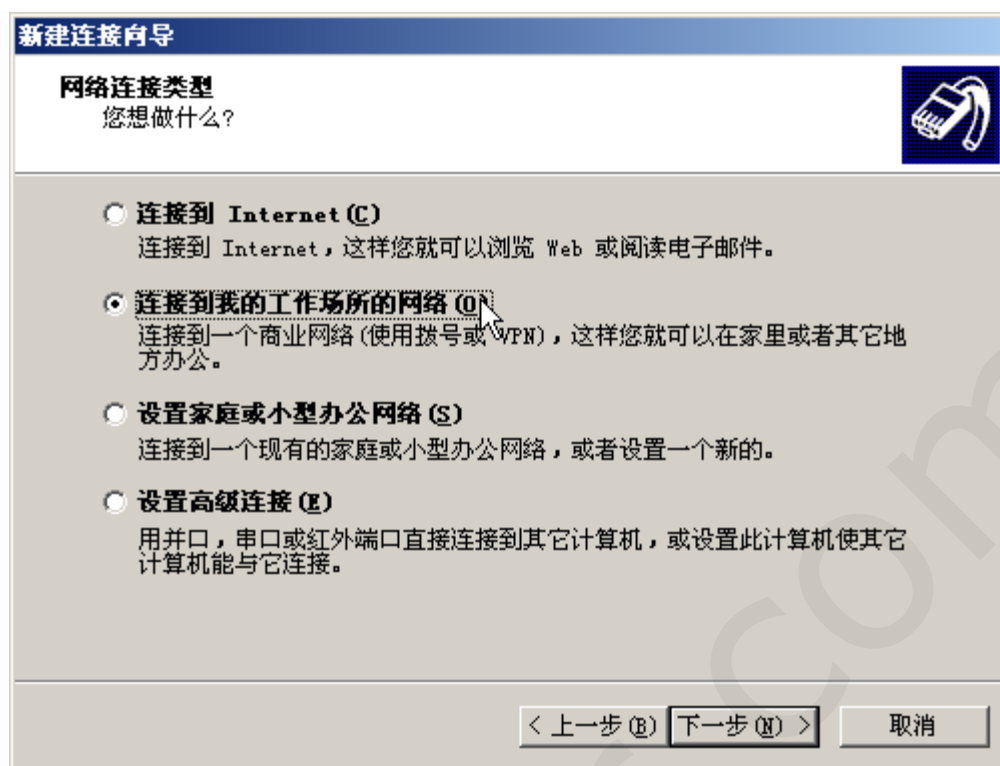
依次点击“开始”->“设置”->“网络连接”->“新建连接向导”即可。

或右键单击桌面上的“网上邻居”图标，选择“属性”，在“向导”栏双击“新建连接向导”。

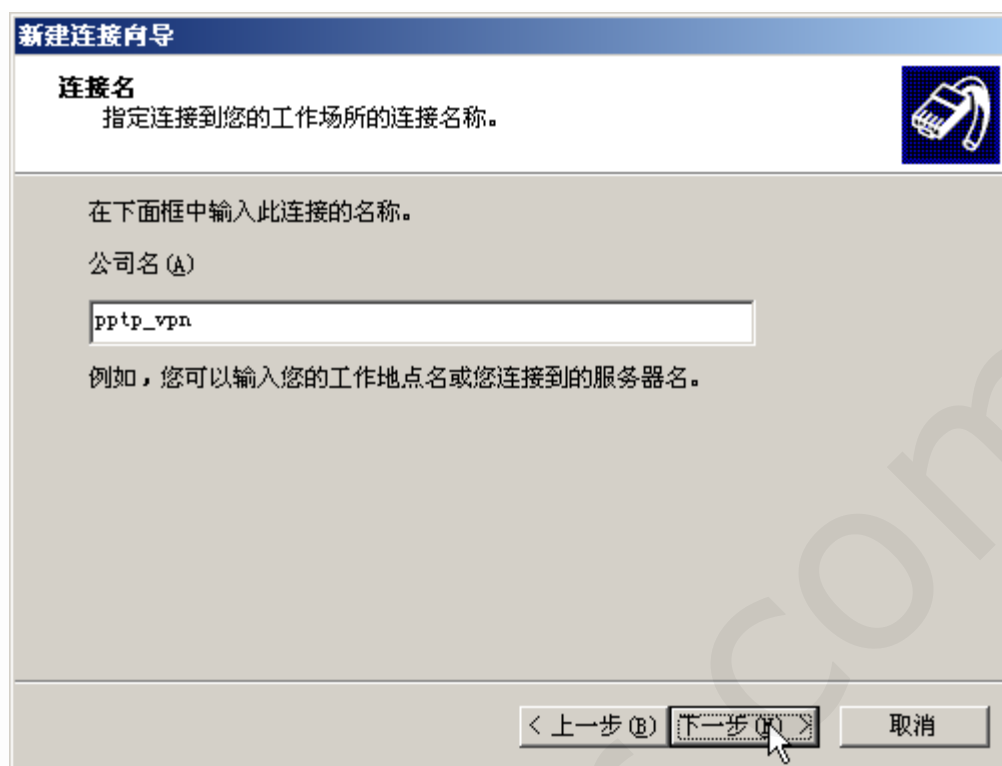


点击“下一步”继续

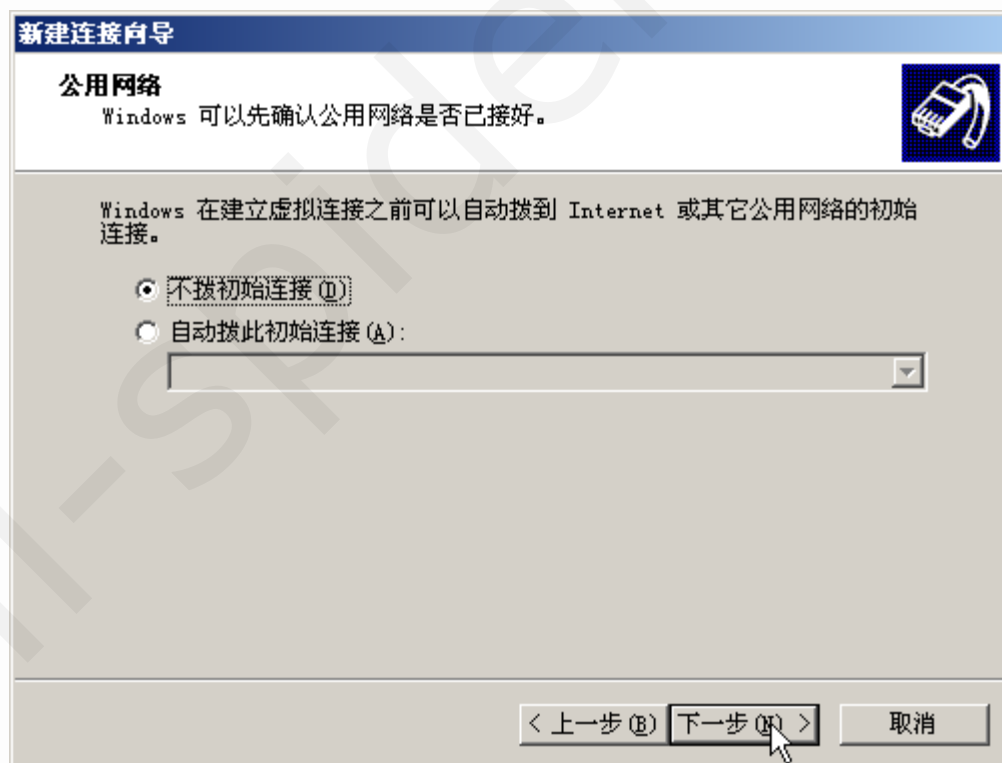
2. 选择连接类型



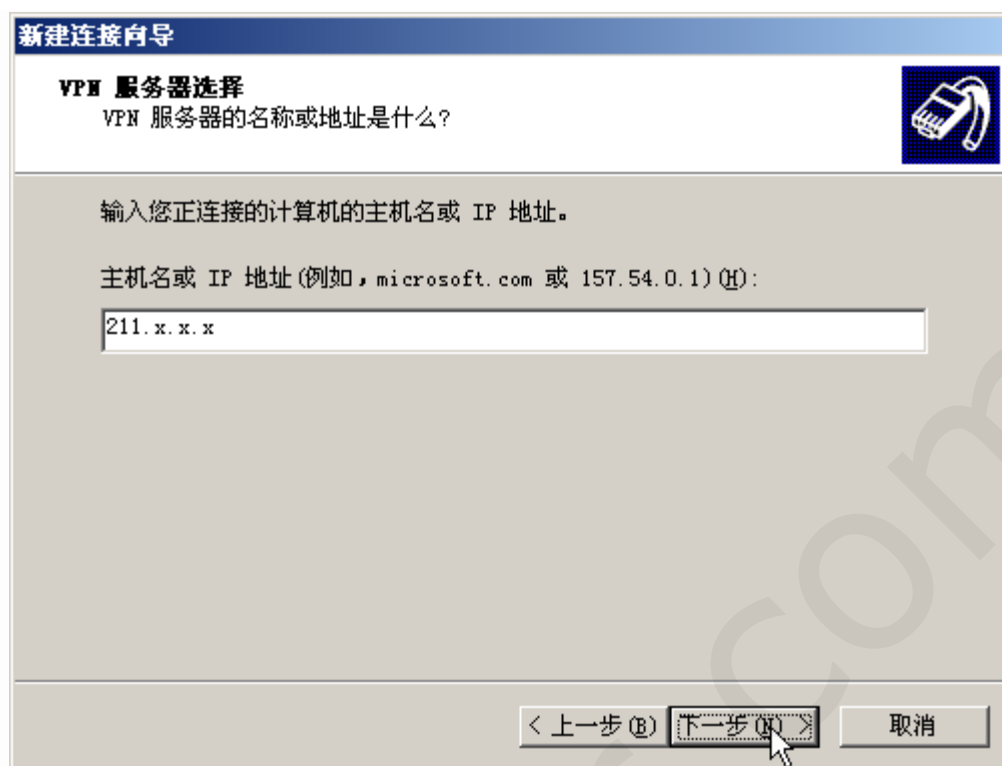
3. 设置连接名和VPN服务器端地址



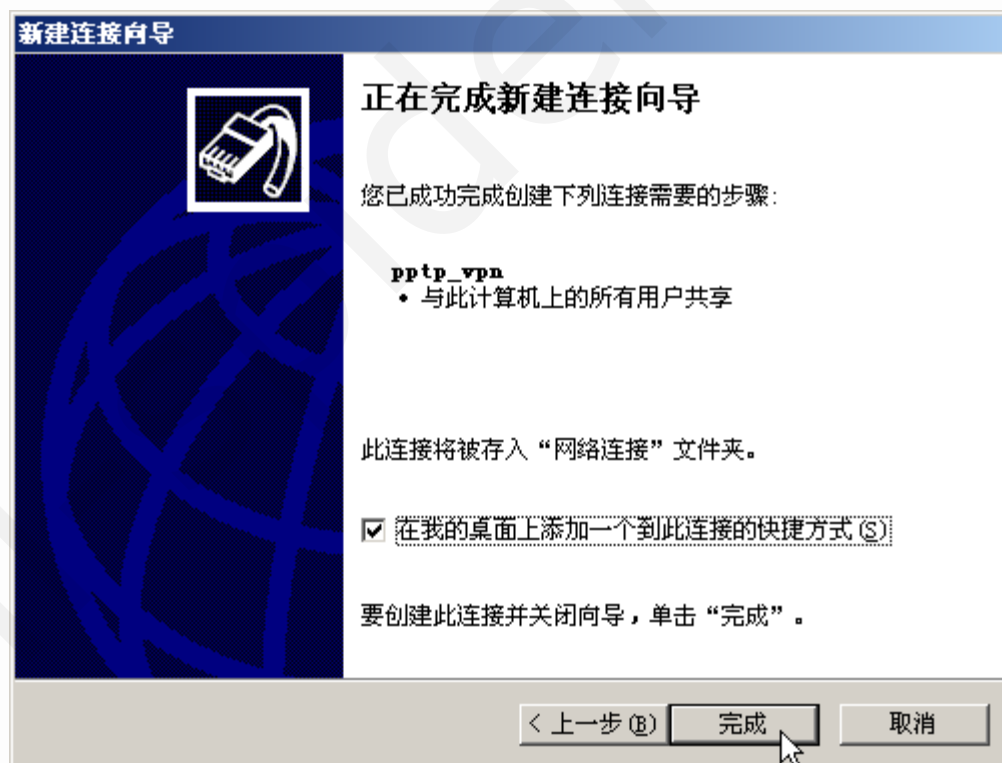
连接名只是一个标识，可以随意设置。



VPN 服务器地址可以是IP或域名。



4. 完成连接向导

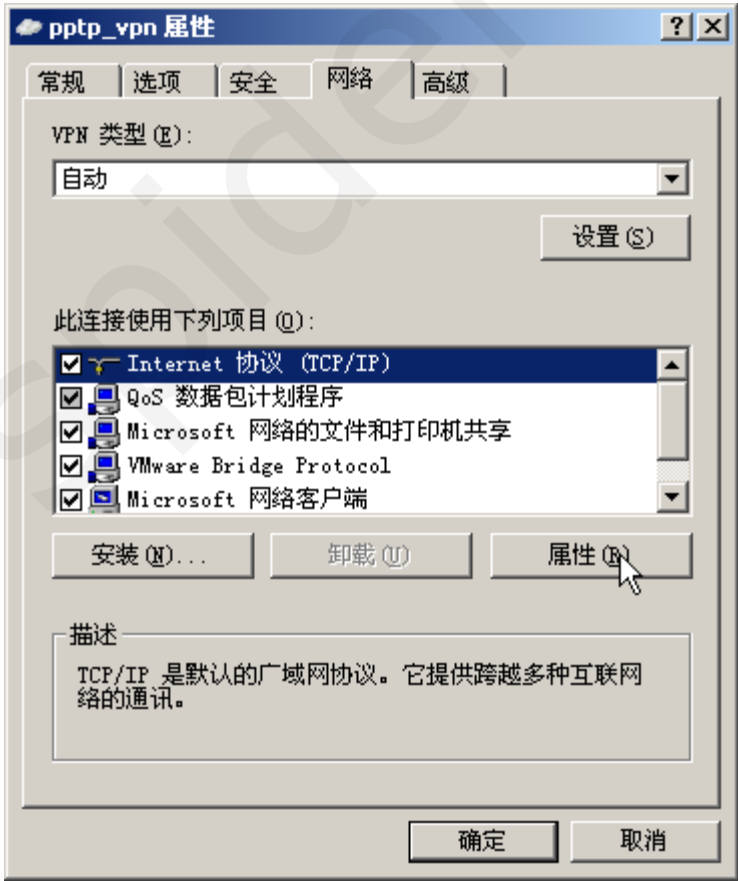


5. 设置拨号连接参数

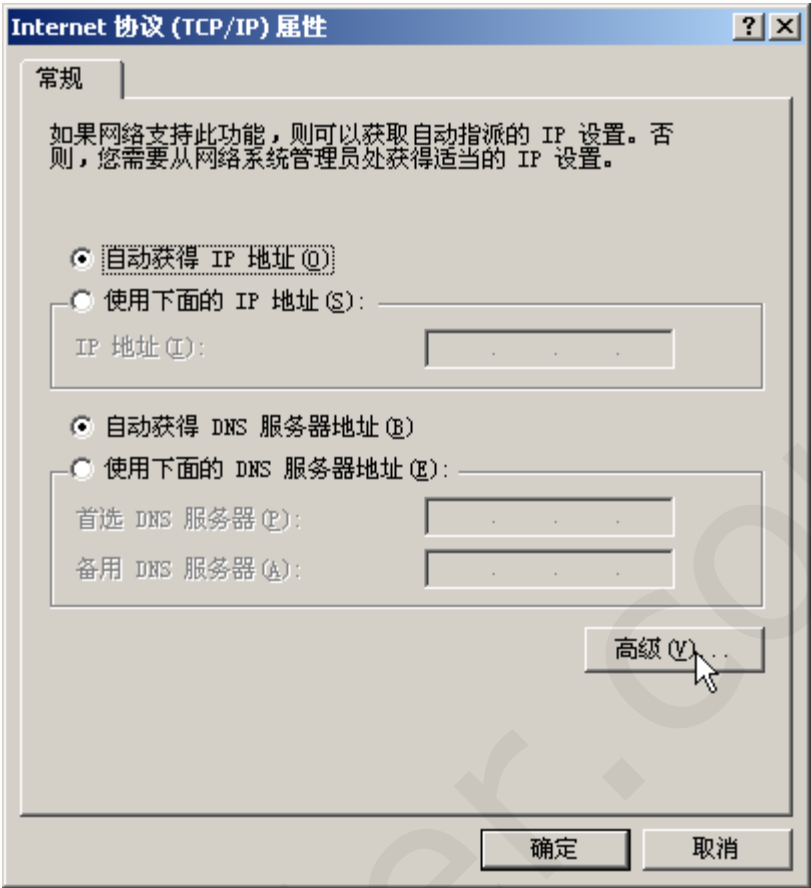
打开建立的拨号连接，点击“属性”进入连接属性设置：



选择“网络”选项卡 -> “Internet 协议 (TCP/IP)”:

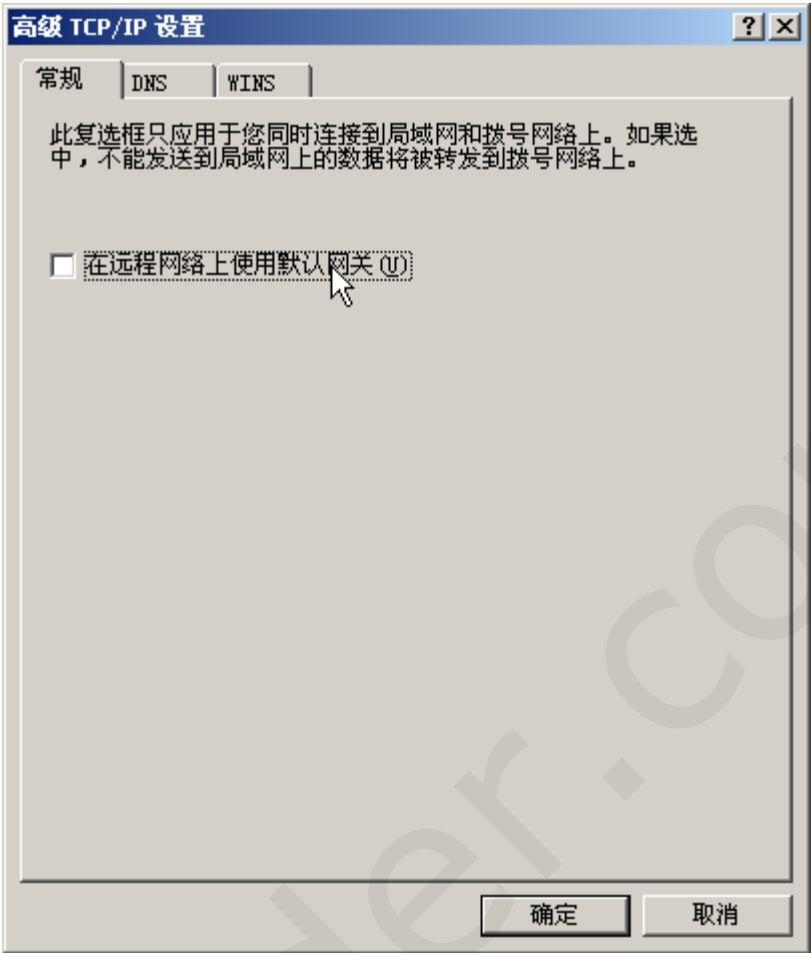


点击“属性”进入TCP/IP协议设置:



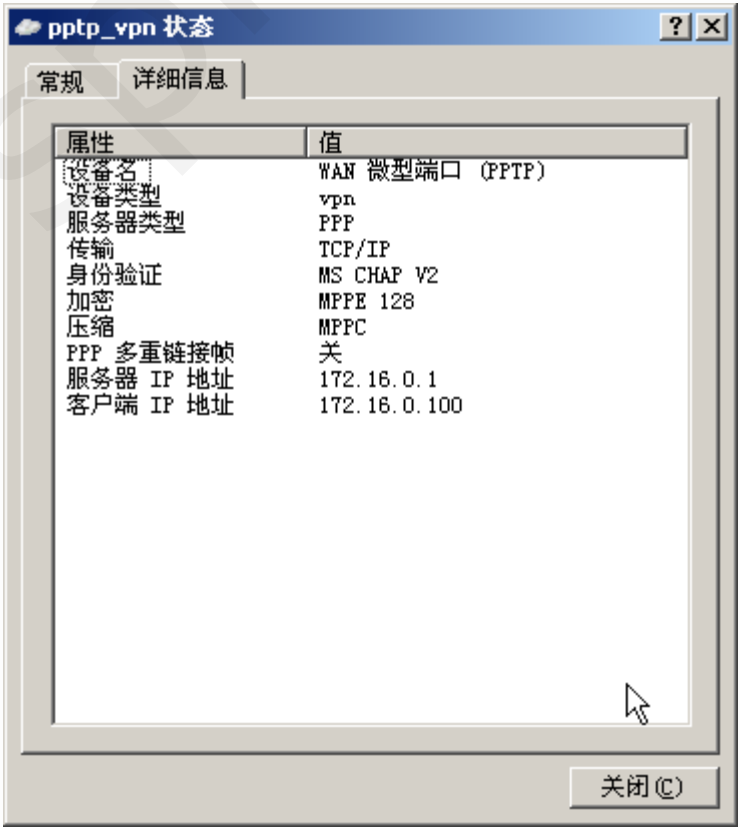
重要

一般情况下，请去掉“在远程网络上使用默认网关”前面的勾，否则VPN拨号后将无法 上网(访问Internet)。



6. 开始 VPN 拨号

点击“连接”进行 VPN 拨号，拨号成功后，点击“连接成功”的提示图标，查看详细的连接信息：



上图中，可以看到拨号后本地 VPN 连接的IP 为 172.16.0.100，VPN 服务器IP 为 172.16.0.1。



34.4. 使用内网 PPTP_VPN 服务器



34.6. 测试 VPN 连接

34.6. 测试 VPN 连接

1. 在“开始”->“运行”，输入 cmd 进入DOS命令提示符，使用 ping <服务器IP> 测试VPN通道是否正常。

```
C:\Documents and Settings\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Reply from 172.16.0.1: bytes=32 time<1ms TTL=64
Reply from 172.16.0.1: bytes=32 time=11ms TTL=64
Reply from 172.16.0.1: bytes=32 time=4ms TTL=64
Reply from 172.16.0.1: bytes=32 time=10ms TTL=64

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 6ms
```



提醒


如果路由“防火墙”->“基本安全设置”中“完全禁止了PING”，是无法 ping 通VPN服务器的。

☒ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求)

2. 加入静态路由，访问VPN服务器所在局域网（远程局域网）

这里远程局域网网络地址为 192.168.1.0/255.255.255.0，那么需要添加一条 静态路由：访问远程局域网时走 VPN 线路

```
C:\>route add -p 192.168.1.0 mask 255.255.255.0 172.16.0.100
```



提示

如果需要删除静态路由，将上述 route add 命令中 add 改为 delete 参数即可。

输入 route print 命令查看路由表：

```
Default Gateway:      192.168.2.1
=====
Persistent Routes:
  Network Address      Netmask  Gateway Address  Metric
    192.168.1.0        255.255.255.0   172.16.0.100      1
```

从上图可以看到，VPN 拨上后，本地的默认网关没有发生变化，如果在 VPN 连接属性中勾选了“在远程网络上使用默认网关”，则默认网关将变成本地 VPN 连接的IP (172.16.0.100)。

此时，就可以访问远程局域网的资源了，比如内部共享（文件服务器）等。



34.5. PPTP_VPN 客户端设置(Windows)



34.7. 常见错误及问题

34.7. 常见错误及问题

1. “远程网络上使用默认网关”到底勾选与否？

这句话的意思是：VPN 连接建立后，是否改变本地的默认网关。

勾选和不勾选各有优劣：

- 选上

好处：无需添加静态路由即可访问 VPN 服务后面的局域网资源。

不足：VPN 拨上号后，本地无法上网，需要在 VPN 服务器上开通“到Internet的VPN路由通道”才行。此外，即使开通了VPN路由通道，通过 VPN 上网速度可能会比较慢（没有本地线路快）。

评点：需要访问远程局域网时，进行 VPN 拨号，不需要时断开，但不适合“本地上网”和“访问远程局域网”同时进行的场合。

- 不选

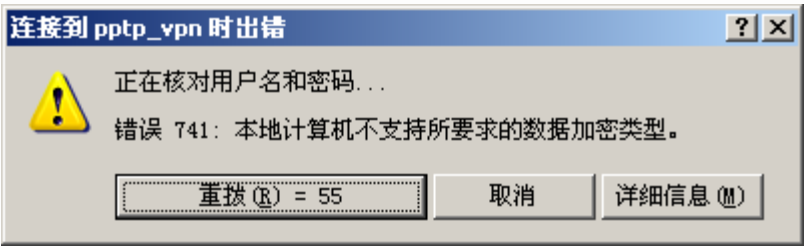
好处：不改变本地默认网关，VPN 拨号后本地上网不受影响，仍然走本地线路。

不足：访问远程局域网资源时，需要手动添加静态路由。

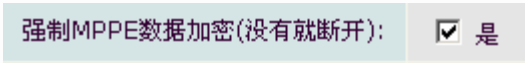
点评：手动添加静态路由比较麻烦，可以通过批处理文件来辅助完成。


综合以上分析，得出以下结论：

- a. 如果 VPN 客户端不需要访问远程局域网，只需要拨入客户端之间可以相互访问，则不用勾选“默认网关”；如果需要，但是又不想手动添加静态路由，则可以采用b种方案。
 - b. 对远程局域网里提供服务的主机，也让其通过 VPN 拨号到 VPN 服务器上，并分配固定的VPN IP，比如 172.16.0.2 分配给文件服务器。这样 VPN 客户端拨入后，无需勾选“默认网关”，也无需手动添加静态路由，通过 172.16.0.2 这个虚拟 IP 就可访问远程的文件服务器了。
2. 错误 741: 本地计算机不支持所要求的数据加密类型



可能原因：VPN 服务器上强制要求 MPPE (微软点对点加密协议)，而客户端不支持或未设置。

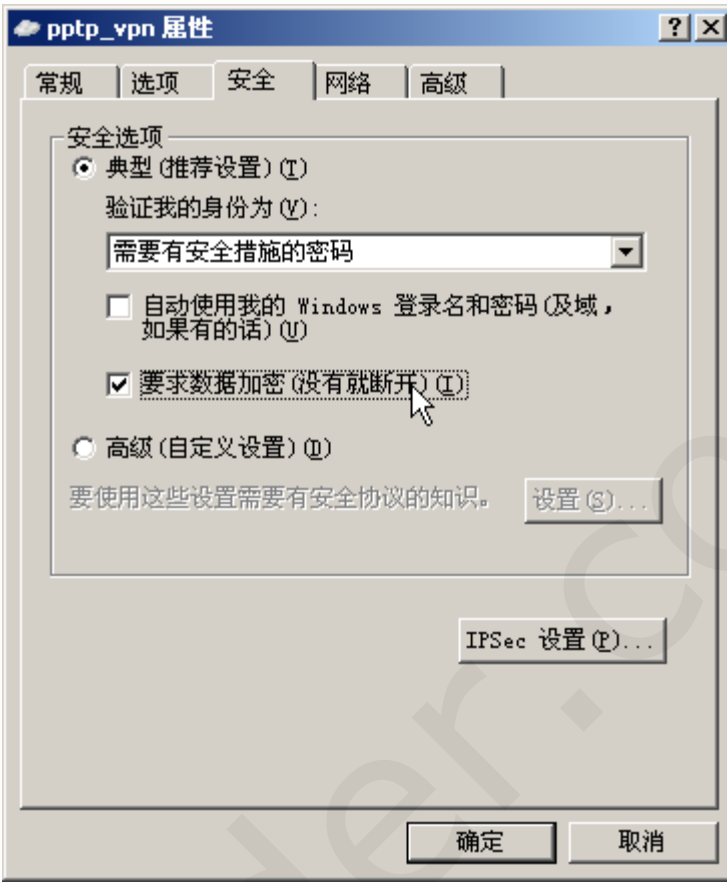




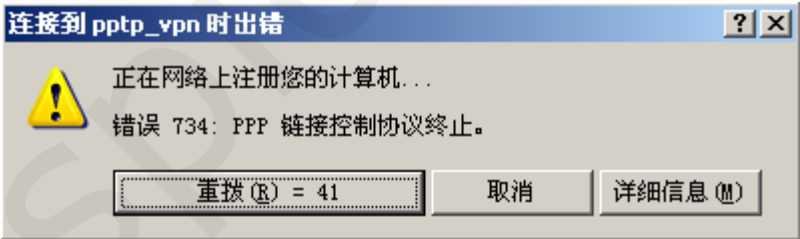
重要

VPN 连接建立后，第一次连接前，需要进入 VPN 连接属性设置，在“安全”选项卡中，先取消“要求数据加密（没有就断开）”前面的

勾，然后再勾选上，否则会出现上面的错误。



3. 错误 734: PPP 链接控制协议终止



原因：VPN 服务器上强制要求 MPPE (微软点对点加密协议) 支持，而客户端没有选上“要求数据加密”。

解决办法：在 PPTP_VPN 服务参数设置中去掉“强制数据加密”，或在客户端选上“要求数据加密”。

4. 错误 721: 远程 PPP 对等机不响应

这种情况大多数原因为客户系统，如果为 WinXP 并且安装了 SP2，则可能会出现这种情况，服务器端 PPP 协议配置不正确也会导致此类错误。

解决办法：修改注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}<000x>，其中其中 <000x> 是 WAN 微型端口 (PPTP) 驱动程序的网络适配器，在此项中新建一个 DWORD 值 ValidateAddress，然后设置为 0 即可。

5. 错误 800: 不能建立 VPN 连接。VPN 服务器可能不能到达，或者此连接的安全参数没有正确配置。

这种情况大多数原因为客户系统连接服务器时使用域名，因临时 DNS 无法解析而出现这种错误，可更换 DNS 试一下，如果还是出错此类错误，则可能是无法连接到 VPN 服务器，可能是 VPN 服务器关闭或出现故障，也可能是客户电脑上的防火墙阻止了 VPN 连接请求，关闭防火墙试一下。

有些使用中转服务器连接到 VPN 服务器的客户端，也可能出现此类错误，原因为中转服务器中转功能出现故障。

6. 错误 619: 端口已断开连接。

这种情况大多数原因为客户机连接 Internet 的网关（如家庭宽带路由或公司上网网关路由或防火墙）NAT-T功能关闭或对VPN支持性不好，主要是对 GRE 及 PPTP 协议的 NAT-T 不支持。可打开网关路由的 NAT-T 功能，如果还是出现错误，则需要更换网关设备，现在市面上大多数设备已经对此支持。

此外，某些地方的ISP可能禁用了 GRE 协议，导致VPN无法连接。

7. 错误 691: 由于域上的用户名和/或密码无效而拒绝访问。

一般是因为 VPN 拨号时的帐户和密码不正确，或没有使用 PPTP_VPN 服务的权限。

此外，如果客户机连接VPN服务器异常中断，因多数服务器限制一个帐户同时只有一个人使用，所以一旦异常断开，则需等待 1 分钟后才能再次拨上。

8. 错误 733: 针对此网络协议的 PPP 控制协议在此服务器上不可用。

这种情况大多数原因为客户机拨入VPN服务器后无法获取IP地址，可修复DHCP服务器或设置静态IP地址或地址池。

9. 错误 718: PPP 超时。

拨入时用户名和密码出错误，有时也因为服务器端认证服务出现故障。



34.6. 测试 VPN 连接



34.8. PPTP_VPN 虚拟双线（借线）



34.8. PPTP_VPN 虚拟双线（借线）

借线实例：有电信+网通双线接入的客户A，只有网通单线接入的客户B。A做VPN服务器端，B做客户端，B通过PPTP_VPN 拨入到A，拨号成功后，B相当于拥有了双线接入(虚拟)，访问网通走本地线路，访问电信走VPN，通过A然后出口到 Internet。

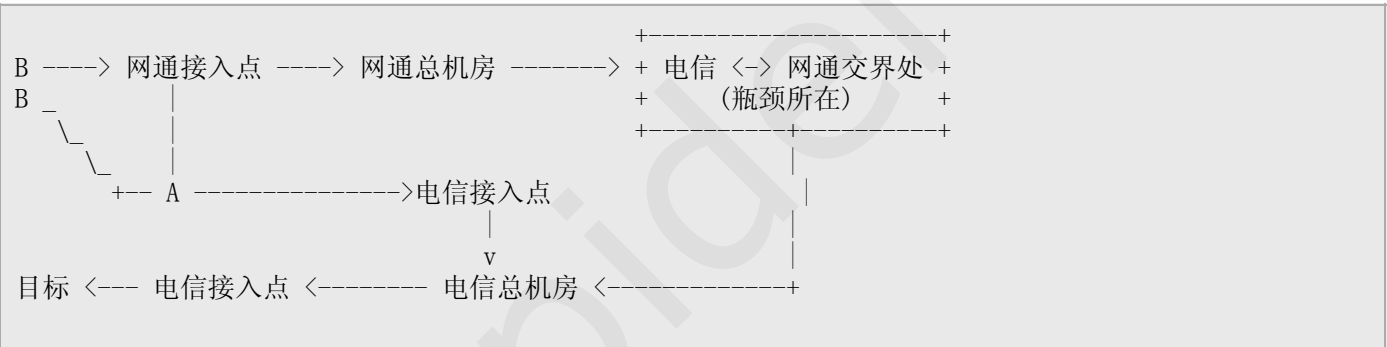
由于电信网通南北割据，电信和网通之间的互访非常缓慢，即：电信用户访问网通的资源 (网页或游戏等)，非常慢；反之，网通用户访问电信资源也是一样。

借线之前，只有网通接入的B原来访问电信的网站或玩电信的游戏是非常慢的；借线之后，由于B和A之间的连接是通过网通，其速度非常快，所以B访问电信资源速度也如同接入了电信线路一样。

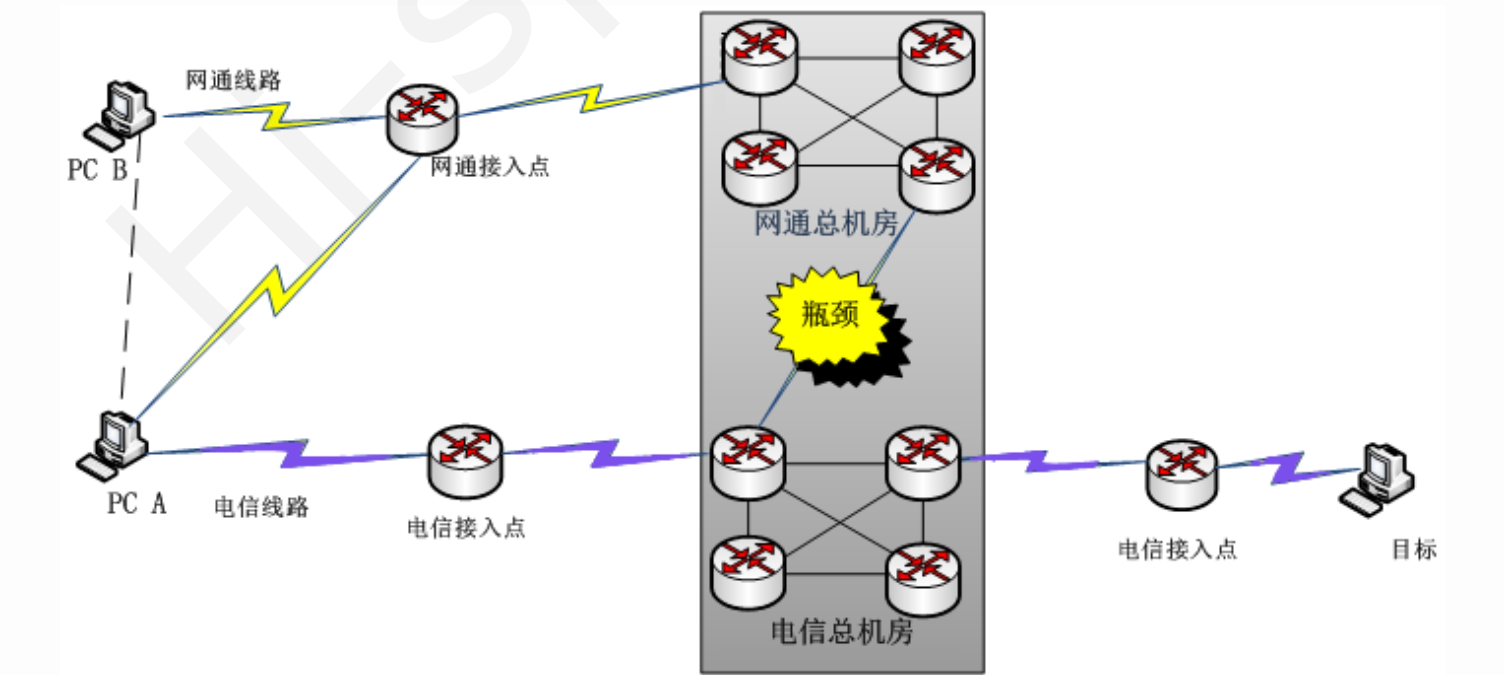


注记

借线是用一部分带宽换取另一运营商的部分带宽，并不能提升带宽的总量，只是对带宽资源进行有效的重组和充分利用。



借线前后 B 访问电信情况对比:



从上图可以看到，借线前，B 访问电信（黄色线条表示）要绕上一大圈，而且要经过电信网通交汇处，此处是互访速度 慢的源头所在；借线后，B 访问电信（紫色线条表示）不经过此瓶颈地，而是借助A的物理网通线路，速度自然比较快。

34.8.1. 借线服务器端设置

进入“服务应用” -> “PPTP VPN 服务”设置页面，设置如下：

☒ 启用PPTP VPN服务(只有勾选了此项, 下面的设置才起作用)

PPTP VPN服务状态: 运行中 (PID:17977)

重新加载

详细日志

VPN服务端IP:	10.10.0.1
VPN客户端IP范围:	10.10.0.2 - 254
VPN连接的最大传输单元(MTU):	1492 (请谨慎修改, 默认为1492)
VPN连接的最大接收单元(MRU):	1492 (请谨慎修改, 默认为1492)
发送LCP(连接控制协议)数据包间隔:	20 秒(默认为20, 一般不超过60)
多少个LCP请求未应答则断开连接:	3 个(默认为3, 一般不超过6)
允许VPN客户端之间互相访问:	<input checked="" type="checkbox"/> 是
启用 VPN-to-Internet 通道:	<input checked="" type="checkbox"/> 是
启用调试模式:	<input type="checkbox"/> 是
支持的身份验证协议:	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
强制MPPE数据加密(没有就断开):	<input type="checkbox"/> 是
禁止内网访问本 PPTP VPN 服务:	<input type="checkbox"/> 是
最大空闲时间(超过则主动断开连接):	0 分钟 (0表示不自动断开)

保存设置

默认

重置

因为只是借线，对安全没有要求，故不需选“强制MPPE数据加密”。

34.8.2. 借线客户端的设置

进入“网络设置”->“网络接口配置”->“PPTP VPN客户端”设置页面，设置如下：

PPTP 连接选项...

PPTP 服务器地址:	<input type="text" value="202.103.XX.XX"/>	PPTP服务器的WAN口IP地址
首选线路:	<input type="text" value="WAN-1 (eth0/eth0/202.103.XX.XX /255.255.255.224)"/>	
备份线路:	<input type="text" value="WAN-1 (eth0/eth0/202.103.XX.XX /255.255.255.224)"/>	
PPTP 拨号连接名:	<input type="text" value="test"/> 连接名只能由数字、大小写字母、下划线、圆点及减号组成	
PPTP 拨号用户名:	<input type="text" value="test"/>	
PPTP 拨号密码:	<input type="password" value="....."/>	
最大传输单元(MTU):	<input type="text" value="1492"/> (默认为 1492)	
最大接收单元(MRU):	<input type="text" value="1492"/> (默认为 1492)	
发送 LCP(连接控制协议) 数据包间隔:	<input type="text" value="20"/> s (20~60)	
多少个LCP请求未应答则断开连接:	<input type="text" value="3"/> (3~6)	
启用代理 ARP:	<input type="checkbox"/> 是	
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)	
负载权重:	<input type="text" value="1"/> ?	
其他参数:	<input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?	
运营商:	<input type="text" value="中国电信"/> (用于多线策略及负载)	
线路检测:	已禁用 [检测日志 清除]	

身份验证 & 加密...

身份验证协议:	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
启用数据加密 (MPPE):	<input type="checkbox"/> 是 (需要 MS-CHAP 或 MS-CHAP v2 协议支持)
启用软件压缩(MPPC):	<input type="checkbox"/> 是 (微软点对点压缩协议支持)

客户端连接成功后会提示：

PPTP 连接状态:	正常, VPN 连接成功 !
PPTP 连接名:	ppp0
连接建立时间:	2009-07-31 12:17:48
已连接时间:	0 天 2 小时 9 分 17 秒
IP地址:	10.10.0.2

上图中将 PPTP 服务器地址改成借线服务器的IP地址，PPTP 拨号连接名可以自己定义。
然后进入“网络设置”->“多线负载及策略”，启用“多线负载及策略”，如下：

☒ 启用多线负载及策略

☐ 自动从服务器更新路由表（最后更新时间：2009-05-26 10:38:49）

线路变化日志 清除

线路设置...

策略路由工作模式：

正常模式、掉线自动切换

☐ 所有数据全部走策略线路（仅用于VPN借线）

默认线路：所有不符合策略的数据将全部走默认线路。策略线路：如果用户访问的IP在策略线路对应的ISP路由表中，则走此线路。默认线路和策略线路可以是一条或者多条，同一ISP应选择同一线路类型。

线路名	ISP	连接状态（网卡/设备名/IP/子网掩码）	线路类型	使用路由表	激活
WAN1	中国联通/网通	eth2/eth2/58.1.0.2/255.255.255.255	默认线路	中国联通/网通（192条 v2.4）	<input checked="" type="checkbox"/> 是
PPTP1	中国电信	virtual/ppp0/10.10.0.2/255.255.255.255	策略线路-1	中国电信（222条 v2.4）	<input checked="" type="checkbox"/> 是

此外，还需修改防火墙中 TCPMSS 值，进入“防火墙”->“基本安全设置”，在“普通模式”中，设置如下：

☒ 修改 TCP 数据包的最大报文长度（PPPoE/VPN 拨号时需要选上）

TCPMSS 值大小：☒ 随线路自动调整（推荐）；手动指定为

1436

（范围 1200 ~ 1500）

★

重要

如果没有启用 TCPMSS 值大小自动调整，可能会造成借线后某些网址无法正常打开、某些游戏登录时超时或无法登录等问题。

进入路由首页，点击系统监测按钮，可以查看借线后各路线的流量信息，如下图所示：

网络接口	状态	工作模式	累计下行流量	累计上行流量	总累计流量	即时下行速度	即时上行速度	总实时速度	流量图
LAN-1 eth1/eth1		100Mb/s 全双工	1.49G	180.13M	1.67G	323.54K Bps	806.38K Bps	1.10M Bps	查看
PPTP-1 vpn/ppp0			2.02G	546.31M	2.55G	223.02K Bps	93.11K Bps	316.13K Bps	查看
WAN-1 eth2/eth2		100Mb/s 全双工	1.33G	1.43G	2.75G	871.11K Bps	346.06K Bps	1.19M Bps	查看

Bps = byte/s（字节/秒） pps = packet/s（包/秒）

★

重要

路由上防火墙如果开启了UDP/TCP并发总连接数限制会影响VPN借线效果，要将借线方的VPN帐号分配固定IP后加入防火墙白名单中

☒ 启用 TCP 单机总连接数限制

最大允许的 TCP 单机总连接数（范围 10-10000）：

200

（推荐 200-250）

☒ 启用 UDP 单机总连接数限制

最大允许的 UDP 单机总连接数（范围 10-10000）：

200

（推荐 200-300）

进入服务应用->用户帐号管理，找到如下选项，填入PPTP VPN拨号段的IP，然后将此IP加入防火墙白名单

分配固定IP: 10.10.20.2 (客户连接后始终获取此IP,仅适用于PPPoE/PPTP用户)



34.7. 常见错误及问题



34.9. 和Win Server建立PPTP VPN连接

34.9. 和Win Server建立PPTP VPN连接
第 34 章 虚拟专用网(VPN) PPTP 服务



34.9. 和Win Server建立PPTP VPN连接

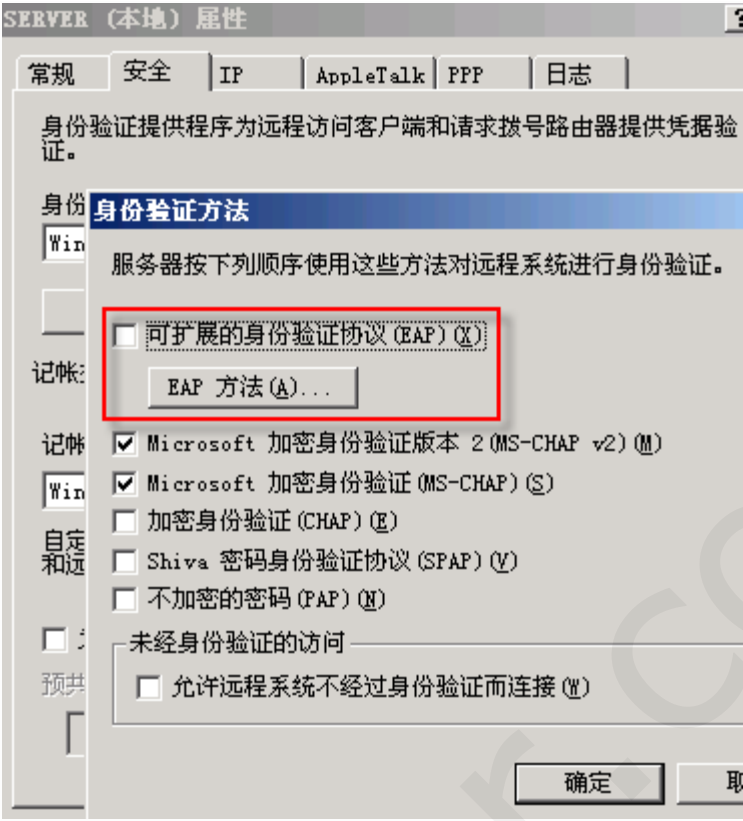
进入“网络设置”->“网络接口配置”->“PPTP VPN客户端”设置页面，设置如下：

PPTP 服务器地址:	123.123.123.123	Win 服务端IP
首选线路:	WAN-1 (eth0/eth0/220.249.123.123/255.255.255.224) ▾	
备份线路:	WAN-1 (eth0/eth0/220.249.123.123/255.255.255.224) ▾	
PPTP 拨号连接名:	vpn 连接名只能由数字、大小写字母、下划线、圆点及减号组成	
PPTP 拨号用户名:	vpn	
PPTP 拨号密码:	●●●●●●	
最大传输单元(MTU):	1492 (默认为 1492)	
最大接收单元(MRU):	1492 (默认为 1492)	
发送 LCP(连接控制协议) 数据包间隔:	20 s (20~60)	
多少个LCP请求未应答则断开连接:	3 (3~6)	
启用代理 ARP:	<input type="checkbox"/> 是	
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)	
负载权重:	1 ?	
其他参数:	<input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?	
运营商:	中国电信 ▾ (用于多线策略及负载)	
线路检测:	已禁用 [检测日志 清除]	
验证 & 加密		
身份验证协议:	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2	
启用数据加密 (MPPE):	<input checked="" type="checkbox"/> 是 (需要 MS-CHAP 或 MS-CHAP v2 协议支持)	
启用软件压缩(MPPC):	<input type="checkbox"/> 是 (微软点对点压缩协议支持)	

和服务端配置一致

如果路由客户端连接不上，而用Win客户端可以连接上，需要检查下Win服务器的设置。

以Win Server 2003为例，进入“开始”->“管理工具”->“路由和远程访问”，在配置的本地SERVER上点击右键-属性，选择安全标签，点击身份验证方法，去掉可扩展的身份验证协议，并核对其它验证方式是否和路由上一致。





第 35 章 虚拟专用网(VPN) SSL服务
目录

- [35.1. 什么是 SSL VPN](#)
- [35.2. SSL VPN 典型解决方案](#)
- [35.3. SSL VPN 服务端的设定](#)
- [35.4. 使用内网 SSL VPN 服务器](#)
- [35.5. SSL VPN 客户端设置\(Windows\)](#)
- [35.6. 测试 VPN 连接](#)
- [35.7. 常见错误及问题](#)
- [35.8. 局域网互连\(路由模式\)](#)
 - [35.8.1. 服务器端设置](#)
 - [35.8.2. 客户端设置](#)
 - [35.8.3. 测试连接](#)
- [35.9. 局域网互连（桥接模式）](#)
 - [35.9.1. 服务器端设置](#)
 - [35.9.2. 客户端设置](#)
- [35.10. 路由 SSL VPN 互联导入证书](#)

35.1. 什么是 SSL VPN

SSL VPN 即指采用 SSL (Security Socket Layer) 协议来实现远程接入的一种新型 VPN 技术。SSL 是一种在 Internet 上保证发送信息安全的通用协议。SSL 用公钥加密通过 SSL 连接传输的数据来工作。

SSL VPN 通信基于标准 TCP/UDP 协议传输，因而能穿透所有 NAT 设备、基于代理的防火墙和状态检测防火墙。这使得用户能够从任何地方接入，无论是处于其他公司网络中基于代理的防火墙之后，或是宽带连接中。



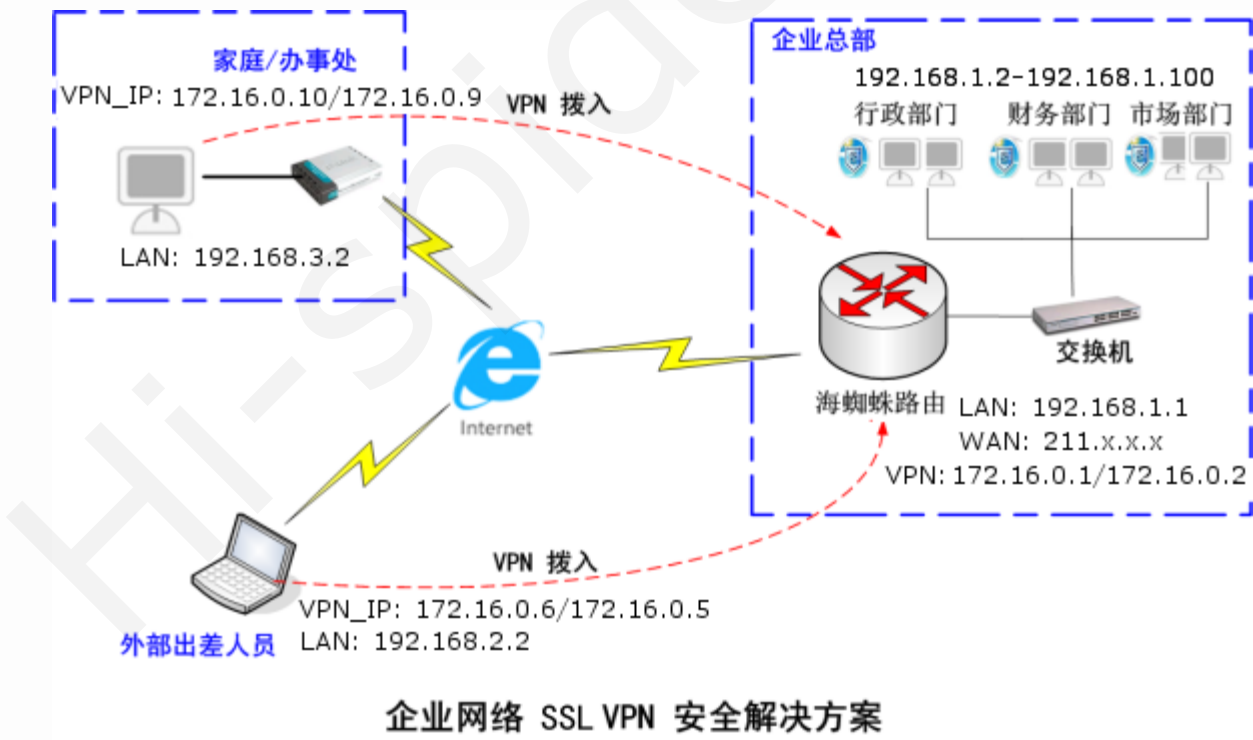


35.2. SSL_VPN 典型解决方案

应用环境说明:

- 企业总部 (VPN服务端)
架设 VPN 服务器，允许远程用户拨入，外网IP为 211.X.X.X，VPN 服务器端 IP 为 172.16.0.1
- 某办事处 (VPN客户端)
需要经常和总部交换数据，通过 VPN 拨号到总部。拨入成功后虚拟通道被建立，获得虚拟 IP: 172.16.0.10/172.16.0.9。
由VPN通道进入总部内部局域网，上传和下载文档。
- 出差人员 (VPN客户端)
需要和总部交换数据时，通过 VPN 拨号到总部。拨入成功后虚拟通道被建立，获得虚拟 IP: 172.16.0.6/172.16.0.5。
由VPN通道进入总部内部局域网，上传和下载文档，或和其他拨入点(如办事处或其他出差人员)相互通讯。

相关图示如下:



和 PPTP 不一样，SSL VPN 拨号后一个VPN连接会有2个IP，一个是本地IP，一个远程网关IP。





35.3. SSL_VPN 服务端的设定

如果内网已有 SSL_VPN 服务器，想让其对外提供拨入服务，请参考: [使用内网 SSL_VPN 服务器](#)

如果使路由自己充当 VPN 服务器，需要进行如下设置：

1. 设定 SSL_VPN 服务参数

进入“服务应用”->“SSL VPN服务”，如下：

初次使用 需要生成证书、密钥等文件，点击在右下角的“证书密钥文件管理”在弹出的窗口中单击“这里”即可“重新生成 CA、服务器端证书及TLS密钥”，如下：

证书密钥文件管理...

☐ 下载/导出服务器现有文件:

导出

☐ 上传/导入已有文件到服务器:

浏览...

上传

注意

1. 请将所有证书/密钥文件压缩后上传, 仅支持 ZIP/TAR 格式
2. 压缩包内必需包含 ca.key ca.crt server.key server.crt ta.key 五个文件

☐ 重新生成 CA、服务端证书/密钥及 TLS 密钥:

请点击 [这里](#) 继续

然后单击导出按钮即可导出刚刚生成的证书文件：ca.crt 、ca.key、server.key、ta.key 、server.crt

证书密钥文件管理...

☐ 下载/导出服务器现有文件:


导出

如果之前导出过上述5个文件，则可以上传其到服务器，沿用原有的证书及密钥，无需重新生成。

下面是设置VPN的连接参数：

协议类型/监听端口:	<input type="radio"/> TCP <input checked="" type="radio"/> UDP (默认) 端口: 1194
对VPN连接启用压缩:	<input checked="" type="checkbox"/> 是
连接模式:	<input checked="" type="radio"/> 路由模式(默认) <input type="radio"/> 桥接模式(用于LAN Game)
VPN子网地址:	10.10.0.0 / 255.255.0.0
最大用户连接数:	100 (1-5000)
VPN连接保持及超时:	存活信息发送间隔: 10 s (5~60) 超时时间间隔: 120 s (60~300)
连接日志记录详细程度:	<input type="radio"/> 简单 <input type="radio"/> 标准 <input checked="" type="radio"/> 详细 <input type="radio"/> 调试

VPN 网络上使用的是内部保留IP地址，一般用 192.168.x.x 或 172.16.x.x 或 10.x.x.x，这里我们使用 10.10.0.0，可根据实际情况自行调整。



重要

VPN 网络地址不能和本地局域网地址重复，也不要和远程拨入端的局域网地址重复。

为了防止冲突，建议把 VPN 网络地址设为比较特殊，比如 172.16.100.x 或 192.168.123.x 等。

安全参数设置：

如果想让客户端拨入后能访问远程局域网，只需勾选“允许客户端访问本地局域网”。

和 PPTP_VPN 不同，无需在客户端手动添加静态路由或修改默认网关，VPN服务器会自动推送必要的动态路由给客户端，简化客户端的工作。

允许VPN客户端之间相互访问：	<input checked="" type="checkbox"/> 是
允许VPN客户端访问本地局域网：	<input checked="" type="checkbox"/> 是
允许VPN客户端和本地 PPTP 客户之间互访	<input type="checkbox"/> 是
允许客户的通过 VPN 通道访问 Internet：	<input checked="" type="checkbox"/> 是
强制重定向客户机的网关：	<input type="checkbox"/> 是
推送给客户机的DNS地址：	<input type="text" value="10.10.0.1"/>
推送的WINS服务器地址：	<input type="text" value="10.10.0.1"/>

2. 添加 VPN 用户

进入“服务应用”->“用户账号管理”，点击新增用户，输入帐号密码后勾选SSL_VPN，保存帐号配置即可，如下：

编辑...

用户ID：	<input type="text" value="test"/>	(能由数字、字母、下划线、减号、@ 及圆点组成)
真实姓名：	<input type="text" value="test"/>	
登录密码：	<input type="password"/>	(为空表示不修改)
密码确认：	<input type="password"/>	
帐号使用周期：	<div>  <input type="text"/></div> [生效] <div>  <input type="text"/></div> [到期]	
允许拨号的时间段：	<input type="text"/>	
分配固定IP：	<input type="text"/>	(客户连接后始终获取此IP,仅适用于PPPoE/PPTP/Web用户)
可用功能列表：	<input type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input checked="" type="checkbox"/> SSL_VPN <input type="checkbox"/> Web	
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
备注：	<input type="text" value="测试1"/>	



35.2. SSL_VPN 典型解决方案



35.4. 使用内网 SSL_VPN 服务器

35.4. 使用内网 SSL_VPN 服务器

如果想让内网已经有 SSL_VPN 服务器对外提供拨入服务，假设其 IP 地址为 192.168.1.254，端口为 UDP/1194，那么在路由上只需要做如下设置：

进入“防火墙”->“端口映射”->“规则设置”，添加一条规则，如下：

优先级：	1	(只能为数字, 数字越小优先级越高)
协议类型：	UDP	
对外端口：	1194 -	
对外 IP：	== 所有外网IP (默认) ==	
对内端口：	1194 -	
对内 IP：	192.168.1.254	
备注：	ssl-vpn-server	

然后在内网 SSL_VPN 服务器上添加相关的 VPN 帐户即可。



35.5. SSL_VPN 客户端设置(Windows)

从 OpenVPN [官方网站](#) 下载 [OpenVPN 2.2.1 for Windows](#) 程序。

下载后双击下载文件进行安装，其安装使用默认参数即可，一直点击 **Next** 直到完成。默认安装在 C:\Program Files\OpenVPN 目录下。

配置步骤:

- 1. 进入 C:\Program Files\OpenVPN 目录，将从服务器导出的2个文件（ca.crt、ta.key）放到 config 子目录下。
- 2. 拷贝 sample-config 目录下的 client.ovpn 到 config 子目录下。
- 3. 用记事本打开 client.ovpn 文件，清空里面的内容，并加入如下几行：

```
### 文件中以 # 号开头的行是注释内容

client
dev tun

#-----#
#           以下内容是需要修改的部分
#-----#
### 如果服务器端采用TCP协议，将udp改成tcp
proto udp

### 服务器地址(可以是域名)及端口，中间用空格分割
remote 211.x.x.x 1194

### 如果服务器端没有启用压缩，跳过下面这一行
comp-lzo
#-----#

resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
auth-user-pass
ns-cert-type server
tls-auth ta.key 1
verb 3
```

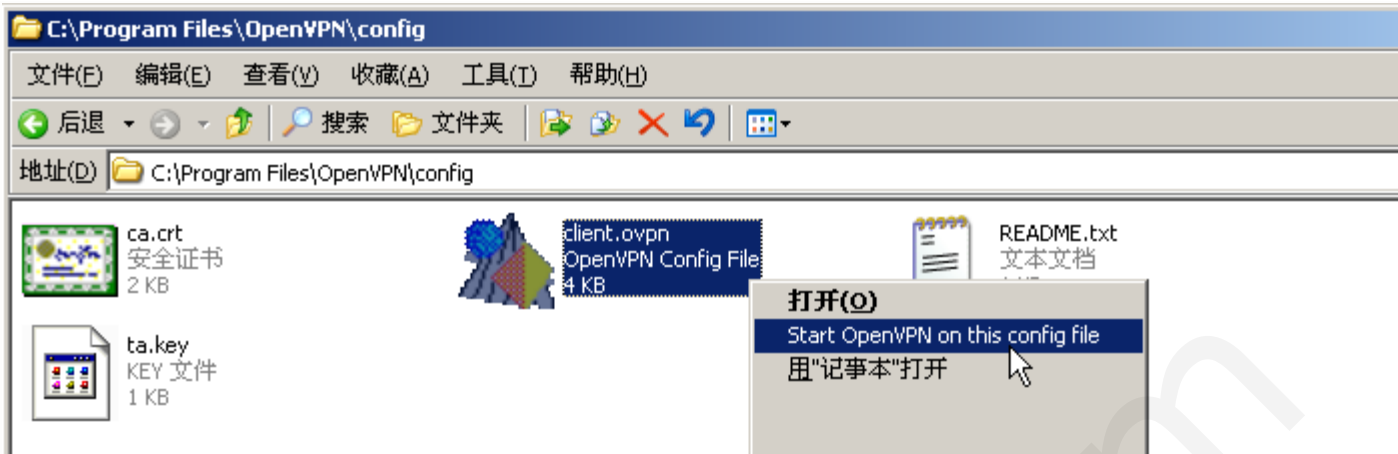
根据服务器端设置的情况，修改上面的参数。



重要

如果从内网连接SSL VPN服务器，服务器地址需填路由的LAN口IP

- 4. 右键单击 client.ovpn 配置文件，选择“Start OpenVPN on this config file” 启动 VPN 连接。



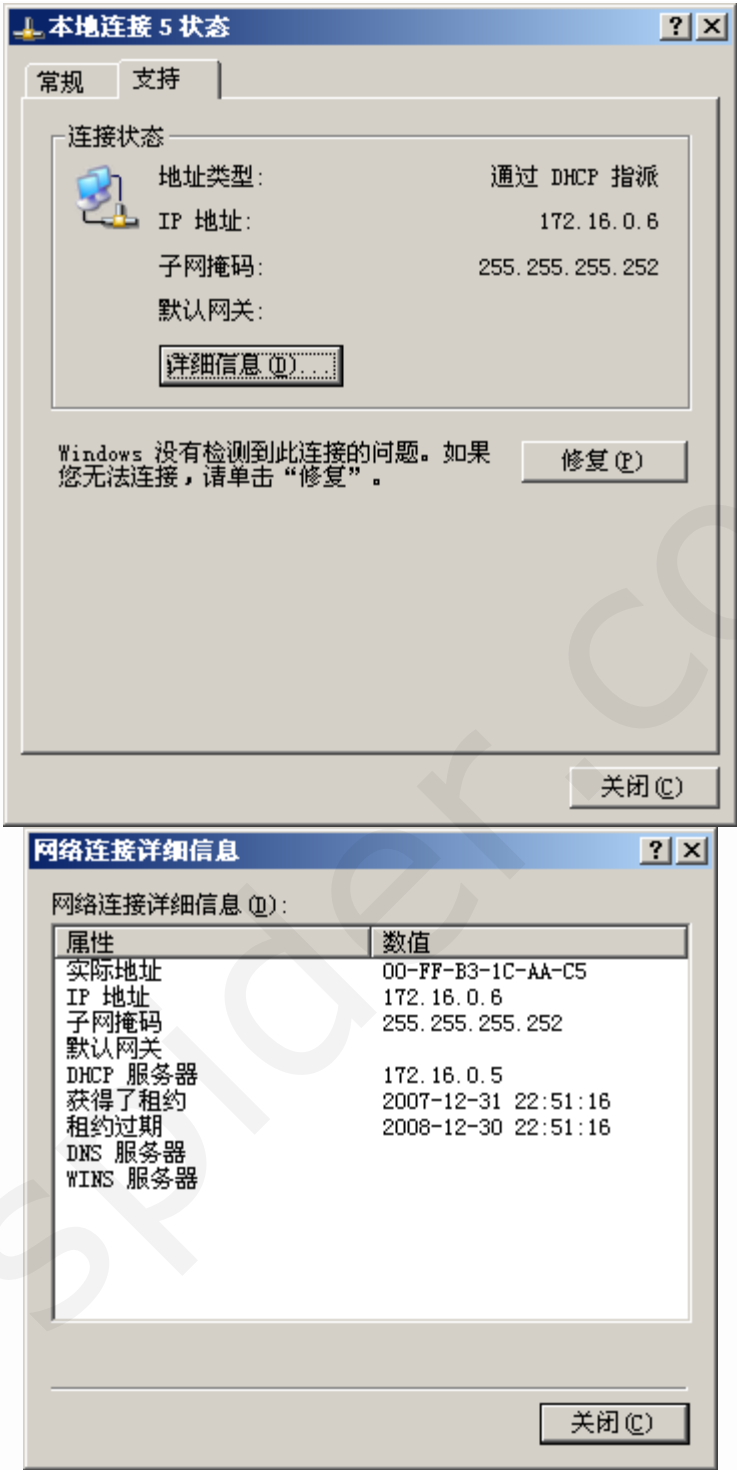
5. 输入VPN帐号及密码，进行连接：

```
Mon Dec 31 22:43:58 2007 OpenVPN 2.0.9 Win32-MinGW [SSL] [LZO] built on Oct 12 2006
Enter Auth Username:test
Enter Auth Password:
```

如果一切正常，最后会看到连接完成的提示，如下：

```
Mon Dec 31 22:51:12 2007 TAP-WIN32 device [本地连接 5] opened: \\.\Global\{B31CAAC5-C3B3-4C3D-ADAB-D2FBBBC4980D}.tap
Mon Dec 31 22:51:12 2007 TAP-Win32 Driver Version 8.4
Mon Dec 31 22:51:12 2007 TAP-Win32 MTU=1500
Mon Dec 31 22:51:12 2007 Notified TAP-Win32 driver to set a DHCP IP/netmask of 172.16.0.6/255.255.255.252 on interface {B31CAAC5-C3B3-4C3D-ADAB-D2FBBBC4980D} [DHCP-serv: 172.16.0.5, lease-time: 31536000]
Mon Dec 31 22:51:12 2007 Successful ARP Flush on interface [262148] {B31CAAC5-C3B3-4C3D-ADAB-D2FBBBC4980D}
Mon Dec 31 22:51:12 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Mon Dec 31 22:51:12 2007 Route: Waiting for TUN/TAP interface to come up...
Mon Dec 31 22:51:13 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Mon Dec 31 22:51:14 2007 Route: Waiting for TUN/TAP interface to come up...
Mon Dec 31 22:51:15 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Mon Dec 31 22:51:15 2007 Route: Waiting for TUN/TAP interface to come up...
Mon Dec 31 22:51:15 2007 TEST ROUTES: 0/0 succeeded len=2 ret=0 a=0 u/d=down
Mon Dec 31 22:51:15 2007 Route: Waiting for TUN/TAP interface to come up...
Mon Dec 31 22:51:16 2007 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Mon Dec 31 22:51:16 2007 route ADD 192.168.0.0 MASK 255.255.255.0 172.16.0.5
Mon Dec 31 22:51:16 2007 Route addition via IPAPI succeeded
Mon Dec 31 22:51:16 2007 route ADD 172.16.0.0 MASK 255.255.255.0 172.16.0.5
Mon Dec 31 22:51:16 2007 Route addition via IPAPI succeeded
Mon Dec 31 22:51:16 2007 Initialization Sequence Completed
```

6. 右键单击“网上邻居”，选择“属性”进入网络连接页面，在“LAN 或高速 Internet”栏中会多出一个已连接的图标，双击它，会看到相关的VPN连接信息：



可以看到拨号后，本地获取的IP地址为 172.16.0.6，远程网关为 172.16.0.5。





35.6. 测试 VPN 连接

在“开始” ->“运行” 输入 cmd 进入 DOS 命令提示符，使用 ping <服务器IP> 测试 VPN 通道是否正常。

```
C:\Documents and Settings\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Reply from 172.16.0.1: bytes=32 time<1ms TTL=64
Reply from 172.16.0.1: bytes=32 time=11ms TTL=64
Reply from 172.16.0.1: bytes=32 time=4ms TTL=64
Reply from 172.16.0.1: bytes=32 time=10ms TTL=64

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 6ms
```



提醒

如果路由“防火墙”->“基本安全设置” 中 “完全禁止了PING”，是无法 Ping 通 VPN 服务器的。

☒ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求)

如果一切正常，就可以通过 172.16.0.1 安全访问 VPN 服务器，或远程局域网的资源了，比如内部共享(文件服务器)、ERP服务器等。





35.7. 常见错误及问题

1. 配置文件参数缺少或不正确

```
Options error: You must define CA file <--ca> or PKCS#12 file <--pkcs12>
Use --help for more information.
Press any key to continue...
```

解决办法：参照 [SSL VPN 客户端设置](#) 检查客户端配置文件的相关参数是否正确。

2. VPN 拨入帐号或密码错误

```
Tue Jan 01 10:47:55 2008 AUTH: Received AUTH_FAILED control message
Tue Jan 01 10:47:55 2008 TCP/UDP: Closing socket
Tue Jan 01 10:47:55 2008 SIGTERM[soft,auth-failure] received, process exiting
Press any key to continue...
```

解决办法：确认用户名和秘密是否输入错误，检查该用户是否有权使用 SSL VPN 服务。



35.8. 局域网互连(路由模式)

现有局域网A，网络地址为192.168.0.0/24，其路由器的WAN口IP为：218.36.24.34，现在此路由器上设置SSL VPN服务作为局域网互连的服务端。

局域网B，网络地址为192.168.10.0/24，在局域网B所接的路由器上启用SSL VPN客户端服务。

使用SSL VPN服务成功连接两路由器后，两局域网内的PC机便可互相访问。

35.8.1. 服务器端设置

进入“服务应用”->“SSL VPN服务”设置页面，设置如下图所示：


协议类型/监听端口：	<input type="radio"/> TCP <input checked="" type="radio"/> UDP (默认)	端口：1194
对VPN连接启用压缩：	<input checked="" type="checkbox"/> 是	
连接模式：	<input checked="" type="radio"/> 路由模式(默认) <input type="radio"/> 桥接模式(用于LAN Game)	
VPN子网地址：	10.10.0.0 / 255.255.0.0	
最大用户连接数：	100 (1-5000)	
VPN连接保持及超时：	存活信息发送间隔：10 s (5~60) 超时时间间隔：60 s (60~300)	
连接日志记录详细程度：	<input type="radio"/> 简单 <input checked="" type="radio"/> 标准 <input type="radio"/> 详细 <input type="radio"/> 调试	
允许VPN客户端之间相互访问：	<input checked="" type="checkbox"/> 是	
允许VPN客户端访问本地局域网：	<input checked="" type="checkbox"/> 是	
允许VPN客户端和本地 PPTP 客户之间互访：	<input checked="" type="checkbox"/> 是	
允许客户的通过 VPN 通道访问 Internet：	<input checked="" type="checkbox"/> 是	
强制重定向客户机的网关：	<input type="checkbox"/> 是	
推送给客户机的DNS地址：	10.10.0.1	
推送的WINS服务器地址：	10.10.0.1	
<div>保存设置 重置 默认 证书密钥文件管理</div>		

图 35.1. 局域网互连路由模式服务端设置1

此外，在添加SSL VPN用户时，还需要在SSL VPN属性（进入“服务应用”->“用户帐号管理”）中做如下设置：

SSL VPN 属性...		
远程VPN网络：	10.10.0.4	/ 255.255.255.252 (客户连接后始终获取此网络地址)
远程局域网网络：	192.168.10.0	/ 255.255.255.0 (用于局域网互联,如172.16.1.0/255.255.255.0)
客户端公网IP地址：		(可选,用户客户端IP为固定IP)

图 35.2. 局域网互连路由模式服务端设置2

提示

这里远程 VPN 网络地址需以4的倍数增加，如 10.10.0.4, 10.10.0.8 等；远程局域网网络填写远程局域网的网段地址。

35.8.2. 客户端设置

进入“网络设置”->“SSL VPN 客户端”设置页面，设置如下图所示：

远程服务器地址：	<input type="text" value="218.36.24.34"/>	协议类型：	<input type="text" value="UDP"/>	端口：	<input type="text" value="1194"/> (默认为 1194)
拨号连接名：	<input type="text" value="sslvpn"/> 连接名只能由数字、大小写字母、下划线、圆点及减号组成				
拨号用户名：	<input type="text" value="sslvpn"/>				
拨号密码：	<input type="password" value="....."/>				
是否启用连接压缩：	<input checked="" type="checkbox"/> 是				
连接模式：	<input checked="" type="radio"/> 路由模式(默认) <input type="radio"/> 桥接模式(用于LAN Game)				
开机自动启动：	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)				
负载权重：	<input type="text" value="1"/> ?				
其他参数：	<input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input checked="" type="checkbox"/> 禁止NAT ?				
运营商：	<input type="text" value="中国电信"/> (用于多线策略及负载)				
线路检测：	已禁用 [检测日志 清除]				
SSL VPN 连接状态：	正常, VPN 连接成功 !				
SSL VPN 连接名：	tun0				
连接建立时间：	2009-08-03 14:36:38				
已连接时间：	0 天 0 小时 46 分 47 秒				
IP地址：	10.10.0.5				
网关：	10.10.0.6				

图 35.3. 局域网互连路由模式客户端设置1

这里远程服务器地址为SSL VPN服务器的WAN口IP地址，拨号连接名自定义。

“网络设置”->“多线负载及策略”，启用多线路负载及策略：

启用多线负载及策略

自动从服务器更新路由表（最后修改时间：2009-08-10 10:38:49）

线路变化日志

清除

线路设置...

策略路由工作模式：

正常模式、掉线自动切换

☐ 所有数据全部走策略线路（仅用于VPN借线）

默认线路：所有不符合策略的数据将全部走默认线路，策略线路：如果用户访问的IP在策略线路对应的ISP路由表中，则走此线路。默认线路和策略线路可以是一条或者多条，同一ISP应选择同一线路类型。

线路名	ISP	连接状态（网卡/设备名/IP/子网掩码）	线路类型	使用路由表	激活
WAN1	中国电信	eth0/ppp0/59.173.128.176/255.255.255.255	<div>默认线路</div>	<div>中国电信（233条 v2.5）</div>	<div><input checked="" type="checkbox"/>是</div>
SSLVPN1	中国电信	virtual/tun0/10.10.0.5/255.255.255.255	<div>默认线路</div>	<div>中国电信（233条 v2.5）</div>	<div><input checked="" type="checkbox"/>是</div>

图 35.4. 局域网互连路由模式客户端设置2

35.8.3. 测试连接

在一个局域网中的任意一台PC机的DOS环境中ping另一个局域网中的任意一台PC机的IP地址来检测是否通路:

```
C:\Users\Administrator>ping 192.168.10.2
```

正在 Ping 192.168.10.2 具有 32 字节的数据:

来自 192.168.10.2 的回复:	字节=32	时间=2ms	TTL=126
来自 192.168.10.2 的回复:	字节=32	时间=2ms	TTL=126
来自 192.168.10.2 的回复:	字节=32	时间=1ms	TTL=126
来自 192.168.10.2 的回复:	字节=32	时间=1ms	TTL=126

此时，两个局域网之间便可以互相访问其内部的共享资源或FTP服务器等。



35.9. 局域网互连（桥接模式）

桥接模式，即通过OpenVPN计算机将服务器所在网络扩展到要连接的客户端。

环境描述：现有局域网A，其路由器的WAN口IP为：59.175.215.26，现在此路由器上设置SSL VPN服务作为局域网互连的服务端。

局域网B，网路地址为192.168.0.0/24，在局域网B所接的路由器上启用SSL VPN客户端服务。

使用SSL VPN服务成功连接两路由器后，两局域网内的PC端便可建立局域网游戏，解决了只能在同一个局域网内建立局域网游戏的局限性。

35.9.1. 服务器端设置

进入“服务应用”->“SSL VPN服务”设置页面，设置如下图所示：

服务参数...	
协议类型/监听端口：	<input type="radio"/> TCP <input checked="" type="radio"/> UDP (默认) 端口： <input type="text" value="1194"/>
对VPN连接启用压缩：	<input checked="" type="checkbox"/> 是
连接模式：	<input type="radio"/> 路由模式(默认) <input checked="" type="radio"/> 桥接模式(用于LAN Game)
VPN子网地址：	<input type="text" value="10.10.0.0"/> / <input type="text" value="255.255.0.0"/>
最大用户连接数：	<input type="text" value="100"/> (1-5000)
VPN连接保持及超时：	存活信息发送间隔： <input type="text" value="10"/> s (5~60) 超时时间间隔： <input type="text" value="120"/> s (60~300)
连接日志记录详细程度：	<input type="radio"/> 简单 <input type="radio"/> 标准 <input checked="" type="radio"/> 详细 <input type="radio"/> 调试
安全相关选项...	
允许VPN客户端之间相互访问：	<input checked="" type="checkbox"/> 是
允许VPN客户端访问本地局域网：	<input checked="" type="checkbox"/> 是
开启INTERNET的VPN路由通道：	<input checked="" type="checkbox"/> 是
强制重定向客户机的网关：	<input type="checkbox"/> 是
推送给客户机的DNS地址：	<input type="text" value="10.10.0.1"/>
推送的WINS服务器地址：	<input type="text" value="10.10.0.1"/>

图 35.5. 局域网互连桥接模式服务端设置1

此外，在添加SSL VPN用户时，还需要在SSL VPN属性（进入“服务应用”->“用户帐号管理”）中做如下设置：

SSL VPN 属性...

远程VPN网络：	<div>10.10.0.2</div>	/ 255.255.255.252 (客户连接后始终获取此网络地址)
远程局域网网络：	<div>192.168.0.0</div>	/ <div>255.255.255.0</div> (用于局域网互联,如172.16.1.0/255.255.255.0)
客户端公网IP地址：	<div></div>	(可选,用户客户端IP为固定IP)

图 35.6. 局域网互连桥接模式服务端设置



提示

这里远程 VPN 网络填写服务参数里 VPN 子网地址中的任意一IP即可，远程局域网网络填写远程局域网的网段地址。

35.9.2. 客户端设置

进入“网络设置”->“SSL VPN客户端”设置页面，设置如下图所示：

SSL VPN 连接参数...

远程服务器地址：	<div>59.175.215.26</div>	协议类型： <div>UDP</div>	端口： <div>1194</div> (默认为 1194)
拨号连接名：	<div>123</div>	连接名只能由数字、大小写字母、下划线、圆点及减号组成	
拨号用户名：	<div>123</div>		
拨号密码：	<div>.....</div>		
是否启用连接压缩：	<input checked="" type="checkbox"/> 是		
连接模式：	<input type="radio"/> 路由模式(默认) <input checked="" type="radio"/> 桥接模式(用于LAN Game)		
开机自动启动：	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)		
负载权重：	<div>1</div>	<div>?</div>	
其他参数：	<input type="checkbox"/> 启用调试 <div>?</div> <input checked="" type="checkbox"/> 不自动加入多线负载 <div>?</div> <input checked="" type="checkbox"/> 禁止NAT <div>?</div>		
运营商：	<div>中国电信</div>	(用于多线策略及负载)	

SSL VPN 连接状态: 正常, VPN 连接成功 !

SSL VPN 连接名：	tap0
连接建立时间：	2009-10-22 15:55:52
已连接时间：	3 天 18 小时 17 分 51 秒
IP地址：	10.10.0.2
网关：	10.10.0.1

图 35.7. 局域网互连桥接模式客户端设置1

这里远程服务器地址为SSL VPN服务器的WAN口IP地址，拨号连接名自定义。

“网络设置”->“SSL VPN 客户端设置”->“线路检测设置”，设置如下图所示：

线路检测设置...

运营商：	中国电信	(用于多线策略及负载时需要)
是否启用线路检测	<input checked="" type="checkbox"/> 启用 (用于探测是否掉线, 及掉线后进行自动切换)	运行中 (PID:18096)
检测时间间隔：	10 s	(每隔多长时间探测一次线路的通断, 最少5秒, 默认为10秒)
线路探测模式：	PING/ICMP 网关探测 (默认)	
重复探测次数：	2	(连续多少次探测不通才认为是掉线, 默认为2次)
PING/ICMP 探测对象：	10.10.0.1	(为空表示网关), 延时不大于 0 ms
SYN/TCP 探测对象：		端口: 80 (默认为 80) 延时不大于 0 ms == 中国电信 ==
线路工作时间：		(线路非24小时连通时才需设置, 如 08:00 表示上午8点)
调试模式运行：	<input checked="" type="checkbox"/> 是 (一般不用开启)	
测试模式运行：	<input type="checkbox"/> 是 (掉线后不切换)	

图 35.8. 局域网互连桥接模式客户端设置2

35.10. 路由 SSL VPN 互联导入证书
第 35 章 虚拟专用网(VPN) SSL服务



35.10. 路由 SSL VPN 互联导入证书

海蜘蛛路由 SSL VPN 对接时，客户端那方需导入服务端方证书。

首先进入服务端的SSL VPN服务，点击“证书密钥文件管理”

允许VPN客户端之间相互访问:	<input checked="" type="checkbox"/> 是
允许VPN客户端访问本地局域网:	<input checked="" type="checkbox"/> 是
允许VPN客户端和本地 PPTP 客户之间互访	<input type="checkbox"/> 是
允许客户的通过 VPN 通道访问 Internet:	<input checked="" type="checkbox"/> 是
强制重定向客户机的网关:	<input type="checkbox"/> 是
推送给客户机的DNS地址:	<input type="text" value="30.30.0.1"/>
推送的WINS服务器地址:	<input type="text" value="30.30.0.1"/>
<div>保存设置 重置 默认 证书密钥文件管理</div>	

然后点击导出按钮

证书密钥文件管理...

○ 下载/导出服务器现有文件:

导出

○ 上传/导入已有文件到服务器:

浏览...

上传

接着进入客户端的SSL VPN服务，点击“证书密钥文件管理”

允许VPN客户端之间相互访问:	<input checked="" type="checkbox"/> 是
允许VPN客户端访问本地局域网:	<input checked="" type="checkbox"/> 是
允许VPN客户端和本地 PPTP 客户之间互访	<input type="checkbox"/> 是
允许客户的通过 VPN 通道访问 Internet:	<input checked="" type="checkbox"/> 是
强制重定向客户机的网关:	<input type="checkbox"/> 是
推送给客户机的DNS地址:	<input type="text" value="10.10.0.1"/>
推送的WINS服务器地址:	<input type="text" value="10.10.0.1"/>
<div>保存设置 重置 默认 证书密钥文件管理</div>	

选择浏览找到刚才导出的证书文件，然后选择上传导入即可

证书密钥文件管理...

☐ 下载/导出服务器现有文件:

导出

☐ 上传/导入已有文件到服务器:

C:\Documents and Settings\Administrato

浏览...

上传





第 36 章 IP 隧道服务

目录

- [36.1. 什么是 IP 隧道服务](#)
- [36.2. IP 隧道服务的网络拓扑图](#)
- [36.3. IP 隧道服务服务端的设定](#)
- [36.4. IP 隧道服务客户端设置](#)
- [36.5. 测试 IP 隧道连接](#)

36.1. 什么是 IP 隧道服务

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式，使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将其它协议的数据帧或包重新封装然后通过隧道发送，新的帧头提供路由信息，以便通过互联网传递被封装的负载数据。

IPIP (IP over IP) 隧道属于第3层隧道协议，是在两个路由器间将IP包封装在附加的IP包头中，通过IP网络传送。

GRE (Generic Routing Encapsulation) 是指一种网络层协议PDU封装于任一种网络层协议PDU中的技术，它可以使两个办公室的用户像访问同一局域网网络一样访问对方的专用网络（LAN to LAN）。

IPIP和GRE隧道模式在因特网上传输数据是没有经过加密和压缩的，适合于对网络传输数据安全要求不高的场合使用。



35.10. 路由 SSL VPN 互联导入证书



36.2. IP 隧道服务的网络拓扑图

36.2. IP 隧道服务的网络拓扑图

第 36 章 IP 隧道服务

36.2. IP 隧道服务的网络拓扑图

我们这里按照以下拓扑图来设置IP隧道，服务端公网IP地址为111.174.XX.XX，内网为192.168.101.0/24，客户端公网IP地址为220.249.XX.XX，内网为192.168.10.0/24。

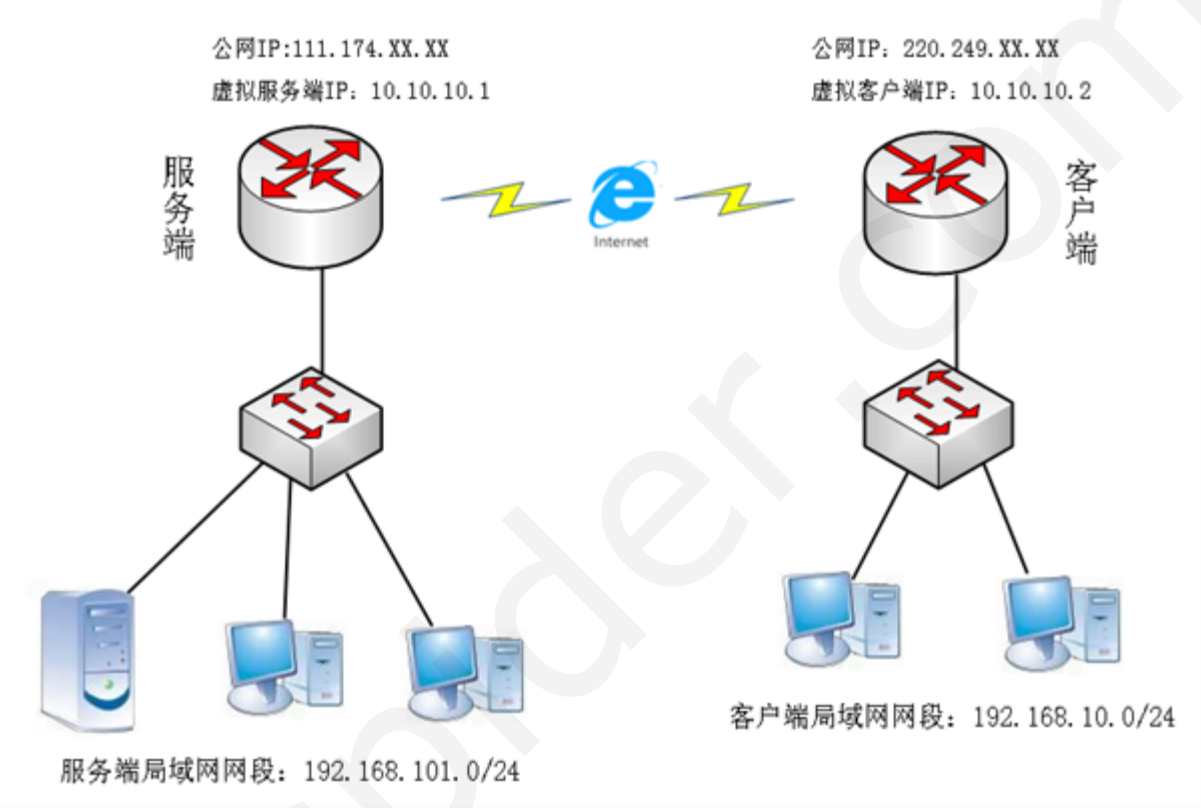


图 36.1. IP 隧道网络拓扑图

36.3. IP 隧道服务服务端的设定

第 36 章 IP 隧道服务



36.3. IP 隧道服务服务端的设定

登录服务端路由的Web主页面，进入“服务应用”->“IP 隧道服务”，勾选 启用 IP 隧道服务，本地隧道IP地址填写一个虚拟IP地址：

启用 IP 隧道服务：	<input checked="" type="checkbox"/> 是
本地隧道IP地址：	<input type="text" value="10.10.10.1"/> / <input type="text" value="255.255.255.0 (默认)"/>

图 36.2. 开启 IP 隧道服务



重要

本地隧道IP地址是路由提供服务端的虚拟隧道地址，不能和两端局域网IP地址在同一网段！

接着进入隧道管理页面，点击增加隧道进入设置页面。填写名称和客户端公网IP，这里的远程隧道IP要和本地隧道IP地址在同一网段，附加路由填写客户端的局域网网段，下面限制上下行带宽如果不填默认为不限速，如下图：

名称：	<input type="text" value="iptun"/> (只能由字母、数字、汉字、下)
本地公网IP：	<input type="text" value="WAN-3 (eth1/ppp1/111.174.XX.XX/255.255.255.255)"/>
客户端公网IP：	<input type="text" value="220.249.XX.XX"/>
远程隧道IP：	<input type="text" value="10.10.10.2"/> 和本地隧道IP地址在同一网段
隧道模式：	<input checked="" type="radio"/> GRE (默认) <input type="radio"/> IPIP
附加路由：	<input type="text" value="192.168.10.0/24"/> 客户端的局域网网段
状态：	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用
备注：	<input type="text"/>
限制上行带宽：	<input type="text"/> ~ <input type="text"/> Kbyte/s (0表示不限制)
限制下行带宽：	<input type="text"/> ~ <input type="text"/> Kbyte/s (0表示不限制)

图 36.3. IP 隧道服务端设置

填写完毕后提交修改即可。








36.2. IP 隧道服务的网络拓扑图

36.4. IP 隧道服务客户端设置

36.4. IP 隧道服务客户端设置

第 36 章 IP 隧道服务



36.4. IP 隧道服务客户端设置

进入客户端路由的Web主页面，进入“网络设置”->“IP 隧道客户端”，选择Tunnel-1页面。

IP 隧道模式选择和服务端相同的GRE模式，远程服务器地址填写服务端的公网IP地址，本地隧道IP地址填写虚拟客户端IP，远程隧道IP地址填写虚拟服务端IP，附加路由填写服务端局域网网段和虚拟服务端IP，如图：

IP隧道模式：	GRE (默认)	
远程服务器地址：	111.174.XX.XX	服务端的公网IP地址
本地公网IP地址：	WAN-1 (eth0/eth0/ 220.249.XX.XX/255.255.255.224)	
本地隧道IP地址：	10.10.10.2	/ 255.255.255.0
远程隧道IP地址：	10.10.10.1	
附加路由：	192.168.101.0/24 10.10.10.1 服务端局域网网段和 虚拟服务端IP	
开机自动启动：	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)	
负载权重：	1 ?	
其他参数：	<input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?	
运营商：	中国电信 (启用多线策略及负载时需要)	
线路检测：	运行中 (PID:3474) [检测日志 清除]	

图 36.4. IP 隧道客户端设置

填写完毕后保存设置即可。





36.5. 测试 IP 隧道连接

在服务端192.168.101.0/24的网段内用一主机ping客户端192.168.10.0/24的网段内一主机，在此主机上运行DOS提示符。

```
C:\Documents and Settings\Administrator>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=39ms TTL=126
Reply from 192.168.10.10: bytes=32 time=39ms TTL=126
Reply from 192.168.10.10: bytes=32 time=39ms TTL=126
Reply from 192.168.10.10: bytes=32 time=43ms TTL=126

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 43ms, Average = 40ms
```

图 36.5. 服务端主机ping客户端主机

接着由客户端192.168.10.0/24的网段内一主机ping服务端192.168.101.0/24的网段内一主机。


```
C:\Documents and Settings\Administrator>ping 192.168.101.93

Pinging 192.168.101.93 with 32 bytes of data:

Reply from 192.168.101.93: bytes=32 time=49ms TTL=126
Reply from 192.168.101.93: bytes=32 time=38ms TTL=126
Reply from 192.168.101.93: bytes=32 time=40ms TTL=126
Reply from 192.168.101.93: bytes=32 time=41ms TTL=126

Ping statistics for 192.168.101.93:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 36.6. 客户端主机ping服务端主机



提醒

如果路由“防火墙”->“基本安全设置”中“完全禁止了PING”，是无法 Ping 通 VPN 服务器的。

☒ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求)

您也可以登陆Web页面查看隧道状态，进入服务端路由主页面->“服务应用”->“IP 隧道服务”，进入IP 隧道状态栏查看：

ID	名称	远程隧道IP	客户端公网IP	本地隧道IP地址	本地公网IP	隧道模式
1	tun1	10.10.10.2	220.249.XX.XX	10.10.10.1	111.174.XX.XX	GRE

图 36.7. IP 隧道状态





部分 VII. 流量控制

目录

[37. 流量控制](#)

[37.1. 流控简介](#)

[37.2. 流量控制的设置步骤](#)

[37.3. 流量控制说明](#)

[37.3.1. 带宽使用模式](#)

[37.3.2. 限速设置说明](#)

[37.4. 针对 PPPoE 用户限速](#)

[38. 如何查看路由流量](#)

[38.1. SSH简介](#)

[38.2. 启动SSH远程登录服务](#)

[38.3. 利用Putty查看路由流量](#)



36.5. 测试 IP 隧道连接



第 37 章 流量控制

目录

[37.1. 流控简介](#)[37.2. 流量控制的设置步骤](#)[37.3. 流量控制说明](#)[37.3.1. 带宽使用模式](#)[37.3.2. 限速设置说明](#)[37.4. 针对 PPPoE 用户限速](#)

37.1. 流控简介

流量控制的目的主要有以下2个：

- 合理分配带宽资源

在外网接入带宽有限的情况下，如果不对流量进行合理的分配和管理，当内网某一台主机占用带宽过高时，就会影响其他主机的正常网络通讯，造成网速变慢，甚至网络阻塞、无法正常访问Internet。P2P下载（BT/迅雷/电驴等）或在线直播就是一个很明显的例子。

为此，对内网每台主机进行流量控制是很有必要的，即：限制其上传、下载的最大速度，不管进行何种操作，其能够使用的带宽都是有限度的，不会消耗过高的带宽资源，当然也不会对其他主机造成影响。

- 优化网络质量(Quality of Service)

针对某些重要的数据包进行优化，比如长度不超过64字节的小包、ICMP包、ACK包、DNS包等等。当网络过载或拥塞时，QoS 能确保这些重要数据包不受延迟或丢弃，同时保证网络的高效运行。



37.2. 流量控制的设置步骤

第 37 章 流量控制

37.2. 流量控制的设置步骤

登录控制页面后，进入“流量控制”->“手动限速规则”，启用上传或者下载流量控制。

勾选启用上传流量控制或启用下载流量控制，选择新增规则：

☒ 启用上传流量控制

☒ 启用下载流量控制

ID	名称	优先级	方向	限速对象	速度范围 (Kbyte/s)	带宽模式	时间	备注	激活/编辑/删除/选择
1	down	10	下载	192.168.10.10	20-40	独享			<input checked="" type="checkbox"/> <input type="checkbox"/>
2	up	100	上传	192.168.10.240	10-20	独享			<input checked="" type="checkbox"/> <input type="checkbox"/>

[\[新增规则\]](#) [\[专家模式\]](#) [\[导出规则\]](#)

☒ ☒ [全选](#)/[全不选](#)

图 37.1. 新增限速规则

例如这里选择限制下载速度，将IP地址为192.168.1.10-192.168.1.100网段的下载速度都限制为30-50K，限速时间为08:00-17:30，对于192.168.1.30的IP地址采取不限速。

名称:	<input type="text" value="下载限速"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
规则优先级:	<input type="text" value="100"/>	(只能为数字, 范围 10-300, 默认100, 越小优先级越高)
剩余带宽抢占优先级:	<input type="text"/>	(只能为数字, 范围 0-7, 默认0, 越小优先级越高)
限制速度:	<input type="text" value="30"/> - <input type="text" value="50"/>	Kbyte/s (1-100000)
限速类型:	<input checked="" type="radio"/> 下载限速 <input type="radio"/> 上传限速	
带宽使用模式:	<input type="radio"/> 共享带宽 <input checked="" type="radio"/> 独立带宽/单机分别限速	
限速对象:	<input type="text" value="192.168.1.10-192.168.1.100"/> (例如: 192.168.0.1-192.168.0.254 或 192.168.0.0/24 或 192.168.0.100,192.168.0.200)	
例外 IP:	<div><div>192.168.1.30</div><div></div></div>	
目的IP:	<input type="text"/>	
源端口:	<input type="text"/>	
目的端口:	<input type="text"/>	
时间:	<input type="text" value="08:00-17:30"/> (24小时制, 如 08:00-17:30)	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
备注:	<input type="text"/>	
<div>保存设置 重置 取消</div>		

图 37.2. 限制下载速度

提交修改后，点击“应用”后才能生效。

[\[新增规则\]](#) [\[专家模式\]](#) [\[导出规则\]](#)

提交修改

应用

重设

日志记录

图 37.3. 应用规则

提示
也可以按目的IP、源端口、目的端口来进行限速

重要
手动限速的子网范围必须是22以内，也就是说子网不能大于255.255.252.0，否则将无效！



37.3. 流量控制说明

37.3.1. 带宽使用模式

带宽使用模式 中有“共享带宽”和“独享带宽”两种模式：

带宽使用模式：

☐ 共享带宽 ☒ 独立带宽/单机分别限速

两者的区别及主要用途如下：

• 共享带宽

所有限速对象使用带宽的累加。通常是针对某一特定的应用，设置的带宽为该特定应用所能使用的总带宽。例如需要设定当访问某一网站时带宽不受限制，则可以使用此种模式。

也可以用于多网段的场合，比如内网有 A(192.168.2.X) 和 B(192.168.3.X) 两个网段，总带宽为 10M，需要设定A网段能使用 6M，B网段为 4M，则可以分别针对A、B两个网段按共享带宽模式限速。

带宽的分配方式是“抢占式”的。

• 独享带宽

每个限速对象能使用的带宽。通常是对内网所有主机进行单机限速，设定的带宽为限速对象中每个IP所能使用的带宽。比如要限制内网每一台主机的下载速度时，要用此种模式进行限速。

带宽的分配方式是“独立平均式”的。

以上两种模式能够混合使用，来适应复杂的网络环境需求。

37.3.2. 限速设置说明

以下载限速为例，比如总带宽为 8Mbit (总最大下载速度为 1000 KBytes/s)。共20人使用，限速为100K-200KBytes/s。这里的100K为保证速度，200K为最大速度,详细阐述如下：

1. 带宽空闲时，速度可达到“最大速度”

如果带宽有空闲（上网的人比较少，带宽使用率在 50% 左右，比如只有10人在线），则下载速度最大可以达到 200K，200K 是下载的峰值速度，即使带宽只有一个人使用，也不会超过这个峰值速度。这 200K 里面的 100K 是暂时借用他人的，当别人需要时，将会自动退让出来。

2. 带宽有一定的使用率，速度在“保证速度”和“最大速度”之间

如果带宽有一定的使用率（有一定的上网人数，带宽使用率在 80% 左右，比如有15人在线），则下载速度会降低到“保证下载速度”和“最大下载速度”之间，即 100K-200K。

通常，这种情况占多数。

3. 带宽使用率较高或全部使用，速度等于或小于“保证速度”

如果带宽使用率比较高（上网的人比较多，带宽使用率在90%以上，比如20人全部上线），则下载速度将不会超过100K，即：如果总带宽不能满足每人都可以达到“保证速度”，那么最终每个人的速度将会小于“保证速度”（平均分配后）。

例如，如果20人全部同时下载，1000KBytes/s 的总下载速度，即每人分得 50K 的下载速度。



提示

可以利用下面的“带宽与速度换算”计算您的带宽。

带宽与速度换算

带宽单位为 bit(位), 下载/上传速度单位为 byte/s (字节/秒)。1Byte = 8bit, 故 1Mbit = 125 Kb, 以 1Mbit 接入为例：

- ADSL 接入：理论最大下载速度为 125 Kb/s, 最大上传速度为 40 Kb/s
- 光纤或以太网接入：理论最大下载和上传速度均为 125 Kb/s

您的接入方式：

光纤或以太网

接入带宽大小：

1

 Mbit

计算

请根据实际情况设置上述参数, 如您不清楚, 请与 ISP 接入商联系。





37.4. 针对 PPPoE用户限速

内网采用 PPPoE 拨号，可以防止 ARP 攻击。



小知识

ARP ——> ARP (Address Resolution Protocol) 是地址解析协议，是一种将 IP 地址转化成物理地址的协议。ARP 就是将网络层 (IP 层，也就是相当于 OSI 的第三层) 地址解析为数据链接层 (MAC 层，也就是相当于 OSI 的第二层) 的MAC地址。

首先进入控制页面“服务应用”->“PPPoE 拨号服务”，进入 PPPoE 服务运行参数页面。

运行参数	高级	带宽限制	专用PPPoE	在线用户
启用 PPPoE 拨号服务:		<input checked="" type="checkbox"/> 是		
监听设备:		<input checked="" type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> 无线局域网 (WLAN)		
PPPoE 服务器名字:		<input type="text" value="aaa"/> 英文字符		
用户认证模式:		<div><input type="radio"/> 无需验证(任意用户名和密码均可拨入) <input checked="" type="radio"/> 简单验证模式(一个帐号可同时拨入多次) 帐号管理 <input type="radio"/> 本地RADIUS认证(可限制帐号拨入次数,有效期等) 帐号管理 <input type="radio"/> 外部 RADIUS 服务器认证计费</div>		
服务端 PPP 连接IP地址:		<input type="text" value="87.0.0.1"/> (不能和局域网在同一网段)		
分配给客户机的地址空间:		<input type="text" value="87.0.0.2"/> - <input type="text" value="87.0.10.254"/>		
分配给客户机的 DNS 地址:		<input type="text" value="87.0.0.1"/> , <input type="text" value="8.8.8.8"/> <input type="checkbox"/> 自动设置		
PPP 连接的 MTU (最大传输单元)值:		<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)		
PPP 连接的 MRU (最大接收单元)值:		<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)		
发送LCP(连接控制协议)数据包间隔:		<input type="text" value="30"/> 秒(默认为30,一般不超过60)		
多少个LCP请求未应答则断开连接:		<input type="text" value="4"/> 个(默认为4,一般不超过6)		
最大空闲时间(超过则主动断开连接):		<input type="text" value="0"/> 分钟 (0表示不自动断开)		

图 37.4. PPPoE 服务参数

一般只需选择默认设置，设置好后，点击保存设置即可。继续设置 PPPoE 服务的带宽限制，如果您的用户认证模式使用的是上图中无需验证模式或简单验证模式。那么只需要进入带宽限制页面，对所有用户进行相同的带宽管理设置。

是否对拨号连接进行带宽限制:	<input checked="" type="checkbox"/> 是
每个拨号连接的下载速度:	<input type="text" value="100"/> ~ <input type="text" value="100"/> Kbyte/s (为 0 表示无限制)
每个拨号连接的上传速度:	<input type="text" value="10"/> ~ <input type="text" value="10"/> Kbyte/s (为 0 表示无限制)
<div>保存设置 重置</div>	

图 37.5. 带宽限制

用户可依据实际情况来进行设置，设置好后点击保存设置。

如果是采用的RADIUS认证，那么需要在“服务应用”->“用户账号管理”内进行限速，编辑任何一个PPPoE账号，下面都有带宽限制选项：

带宽限制...	
限制上行带宽:	<input type="text" value="15"/> Kbyte/s (0表示不限制)
限制下行带宽:	<input type="text" value="10"/> Kbyte/s (0表示不限制)

图 37.6. 针对账号带宽限制

填入上行和下行带宽限制，保存后即可。



第 38 章 如何查看路由流量

目录

- [38.1. SSH简介](#)
- [38.2. 启动SSH远程登录服务](#)
- [38.3. 利用Putty查看路由流量](#)

38.1. SSH简介

SSH（安全外壳协议）是一种在不安全网络上提供安全远程登录及其它安全网络服务的协议。

通过使用SSH，可以把所有传输的数据进行加密，使数据不可能在传输过程中被“中间人”篡改，而且也能够防止DNS和IP欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替telnet，又可以为ftp、pop、甚至ppp提供一个安全的“通道”。



37.4. 针对 PPPoE用户限速



38.2. 启动SSH远程登录服务

38.2. 启动SSH远程登录服务

第 38 章 如何查看路由流量



38.2. 启动SSH远程登录服务

Web登录海蜘蛛路由，进入“流量控制”->“流量实时监测”，勾选启用 SSH 远程登录服务：

☒ 启用 SSH 远程登录服务

SSH 服务状态: 运行中 (PID:2973)

SSH 登录端口:	<input type="text" value="2345"/>	(默认为 2345)
只监听内网IP:	<input checked="" type="checkbox"/> 是 (不允许从外网登录)	
SSH 登录密码:	<input type="password"/>	(密码只能由数字、字母、下划线、减号、@符号组成, 长度 4-20 位)
登录密码确认:	<input type="password"/>	
可选参数:	<input type="text"/>	

保存设置

重置

图 38.1. SSH远程登录服务

勾选只监听内网IP，这样可以防止外网用户SSH远程登录到路由。用户名和密码自定义。



38.3. 利用Putty查看路由流量

第 38 章 如何查看路由流量

38.3. 利用Putty查看路由流量

1. 首先下载SSH登录工具Putty

Putty的下载地址为: <http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>

2. 打开 putty, 输入登录用户名、路由 IP 和端口, 点击 "Open" 进行登录:

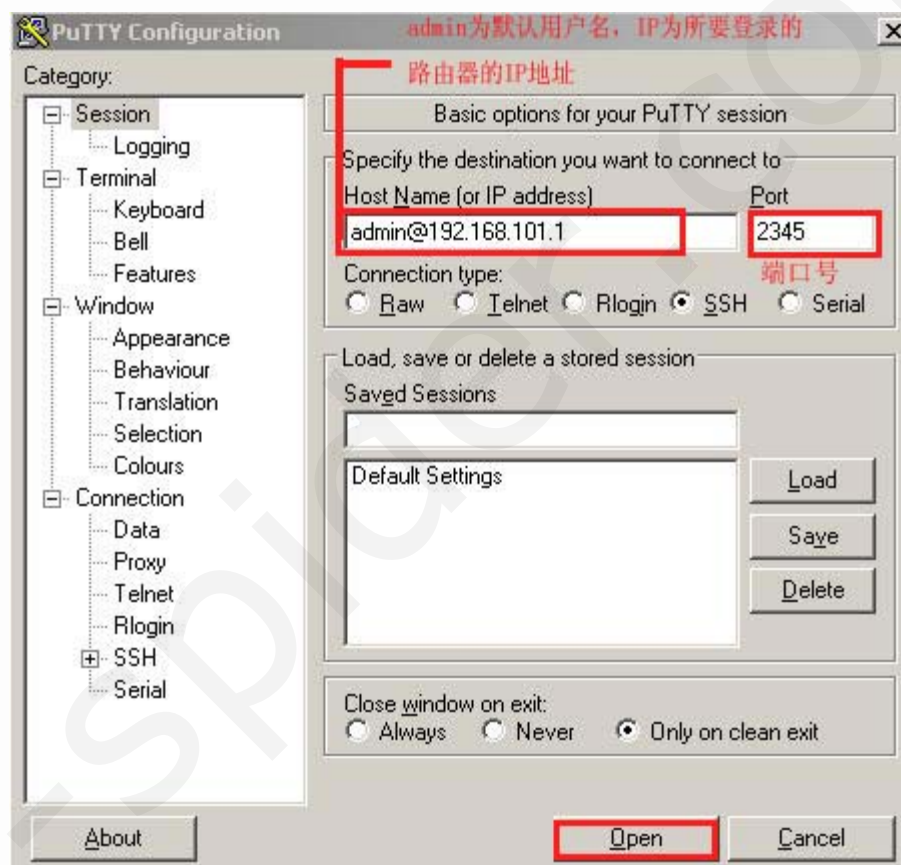


图 38.2. 登录路由器



提示


这里的用户名和密码默认均为admin, 192.168.101.1即为所要登录的路由器的IP地址, 端口号为2345

第一次连接时, 会提示是否将主机密钥加入到缓存中, 选择“是”继续, 下次就不会出现此提示了。



进入以下界面，输入密码admin后回车。





提示

为了安全起见，这里我们是看不到自己所输入的字符的。

进入到主界面：



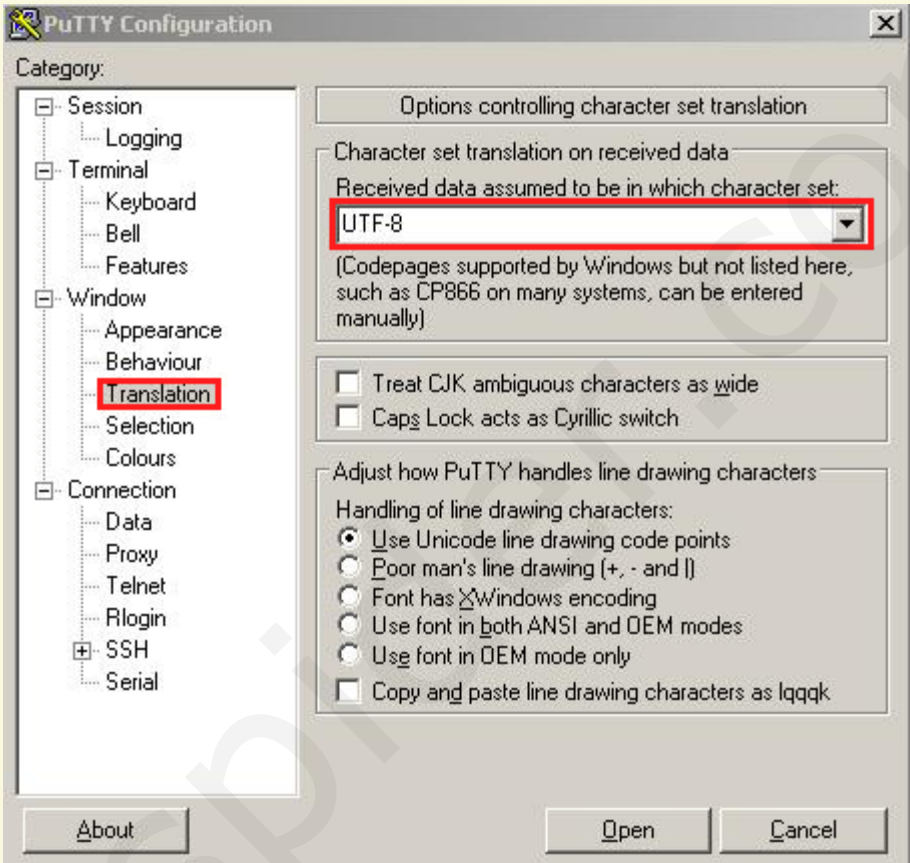
注意

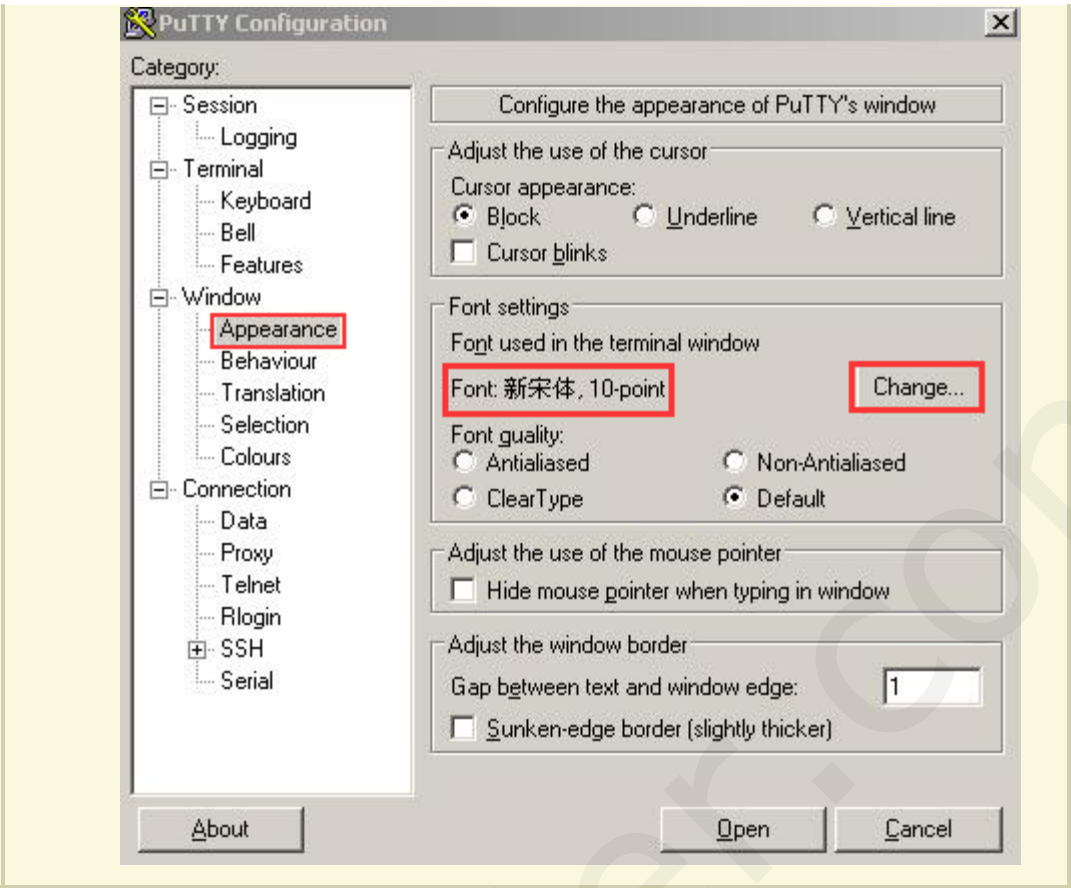


这里可能会出现上图中所示的乱码界面，若出现此种情况，需修改putty属性。

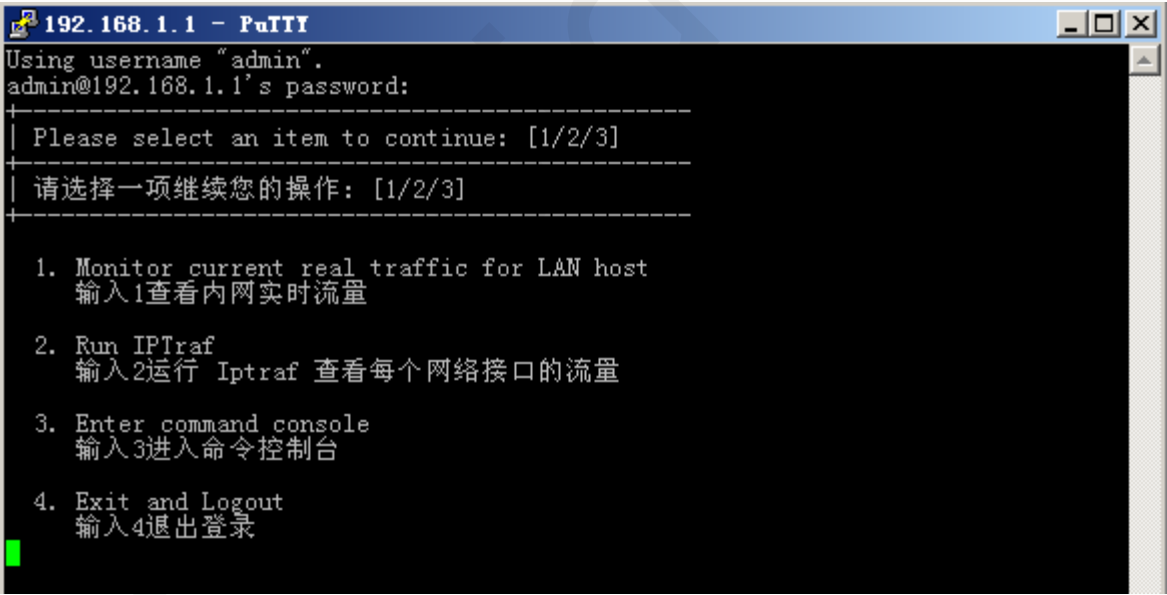
此时可按ctrl+c 关闭putty在重新打开，更改Translation (编码) -> UTF-8 (默认为Use font encoding)

更改Appearance (界面) 字体为中文字体，单击change键选择自己喜欢的中文字体，这里我们选择10号新宋体。如下图所示：





重新点击"Open"打开即可恢复正常：



对上图中出现了四个选项，我们可以根据自己的需要选择不同的查看方式。这里先选择1后回车进入查看实时内网流量界面：

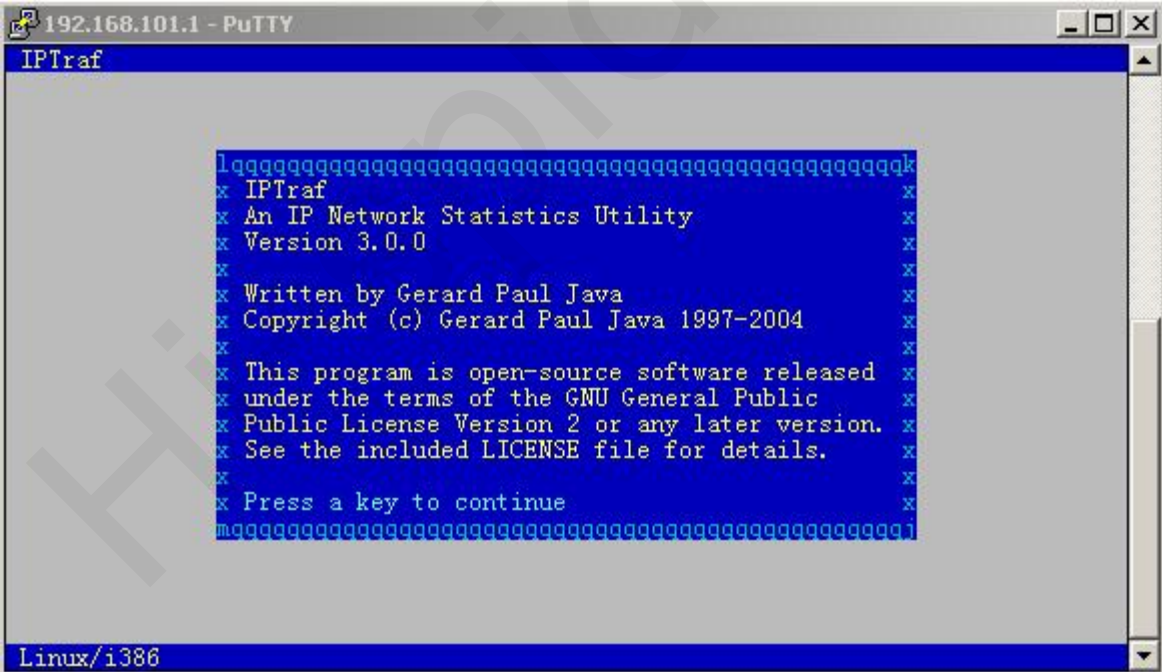
192.168.101.1 - PuTTY

==
== 内网实时流量统计 (Top-30), 刷新时间: 2009-07-03 09:24:09
==

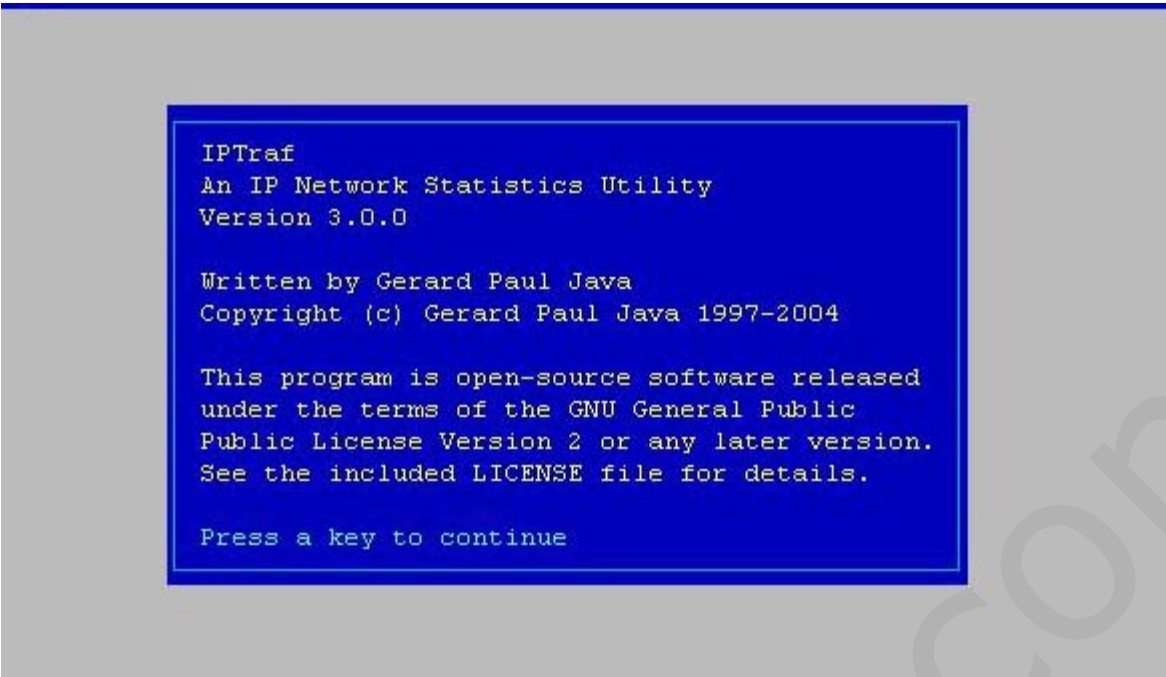
IP地址	总流量	累计上传	累计下载	上传速度	下载速度	总速度	备注
192.168.101.23	122.77M	38.42M	84.36M	4.20K	39.40K	43.60K	
192.168.101.42	10.29M	790.16K	9.52M	2.64K	34.28K	36.92K	
192.168.101.35	1.40G	436.46M	996.57M	12.02K	14.57K	26.59K	
192.168.101.34	8.56M	833.50K	7.75M	624.50	9.98K	10.59K	
192.168.101.33	33.18M	3.12M	30.06M	252.00	2.68K	2.93K	
192.168.101.7	238.30M	166.07M	72.23M	607.00	334.50	941.5	
10.19.0.2	15.09M	1.33M	13.77M	224.50	102.00	326.5	
192.168.101.30	6.30M	1.68M	4.61M	108.00	160.00	268	
192.168.101.9	15.56M	13.67M	1.89M	60.00	44.00	104	
192.168.101.47	3.65M	605.08K	3.06M	0.00	42.00	42	
192.168.101.5	590.40K	577.62K	12.78K	0.00	0.00	0	
192.168.101.214	18.25M	697.31K	17.57M	0.00	0.00	0	
192.168.101.99	4.82M	674.86K	4.16M	0.00	0.00	0	
192.168.101.249	4.07M	672.94K	3.41M	0.00	0.00	0	
192.168.101.28	42.78M	3.27M	39.50M	0.00	0.00	0	
192.168.101.8	51.50K	50.24K	1.26K	0.00	0.00	0	
192.168.101.200	68.35K	42.14K	26.21K	0.00	0.00	0	
10.19.0.1	37.79K	37.79K	0	0.00	0.00	0	
192.168.101.88	13.54M	2.00M	11.55M	0.00	0.00	0	
192.168.101.3	41.29K	28.81K	12.48K	0.00	0.00	0	文件服务器
192.168.101.255	158.64K	0	158.64K	0.00	0.00	0	
192.168.101.6	1.55M	202.81K	1.35M	0.00	0.00	0	邮件服务器

图 38.3. 查看实时内网流量

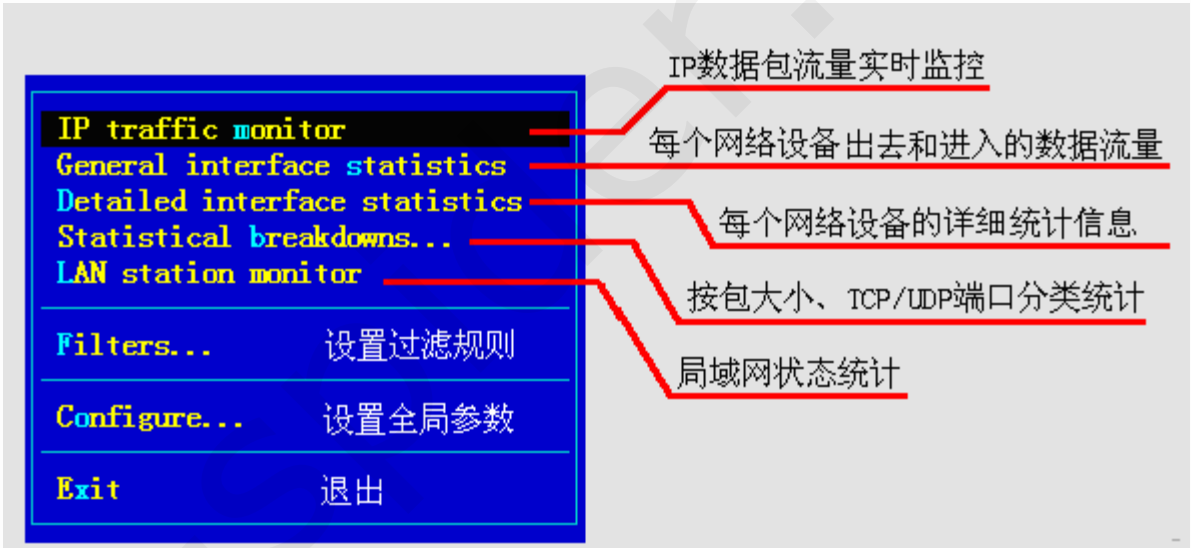
按ctrl+c键返回主界面，选择2进入这里可能出现下图所示的边框乱码界面：



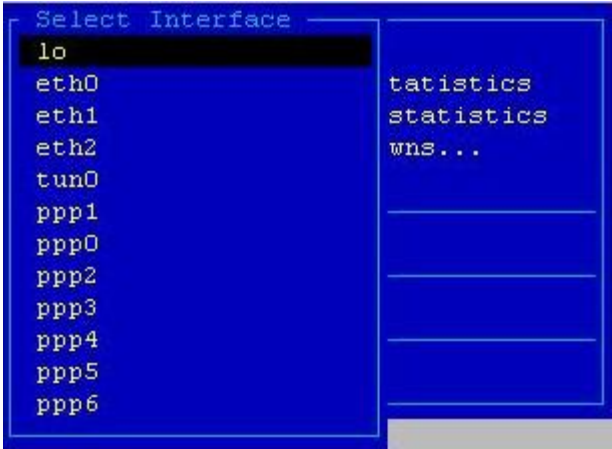
此时需要将之前所修改的putty的Appearance (界面)属性值和Translation(编码)属性值改为其默认值即可恢复正常。



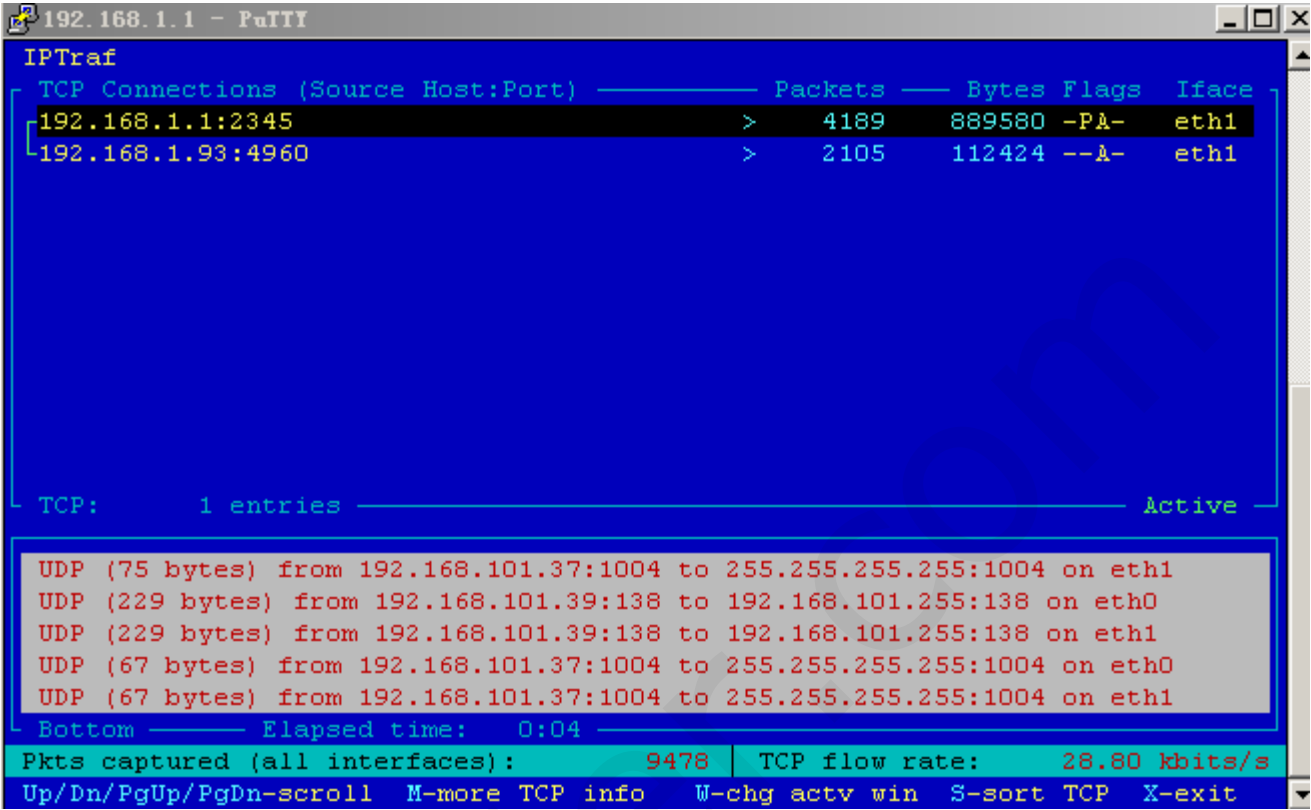
回车后进入



菜单的上面五项是查看实时流量统计信息，可按上下方向键选择不同的菜单，进行相关的信息查看。此五项中，除了第2项，其他4项查看时都会要求选择网络设备：



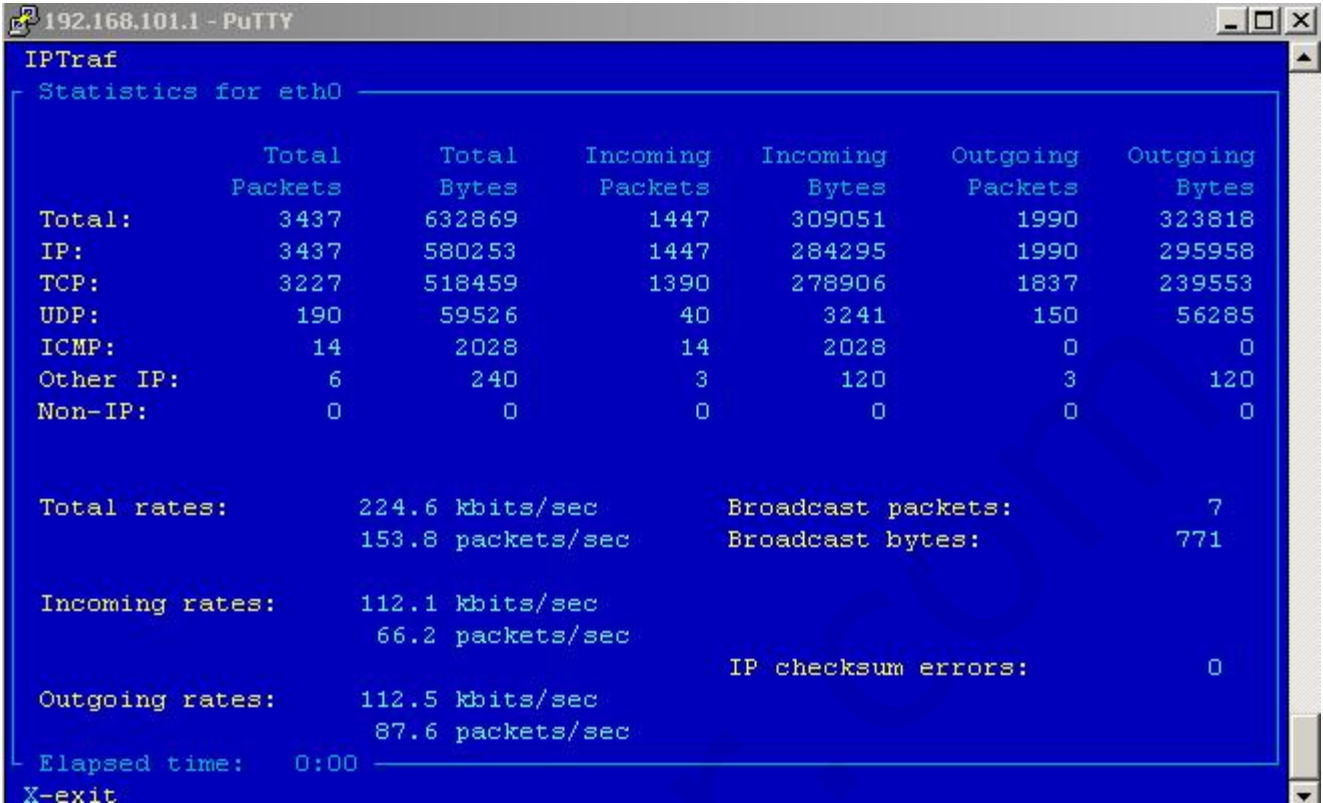
- 选择“第1项”，查看TCP连接信息，IP数据包的实时流量：



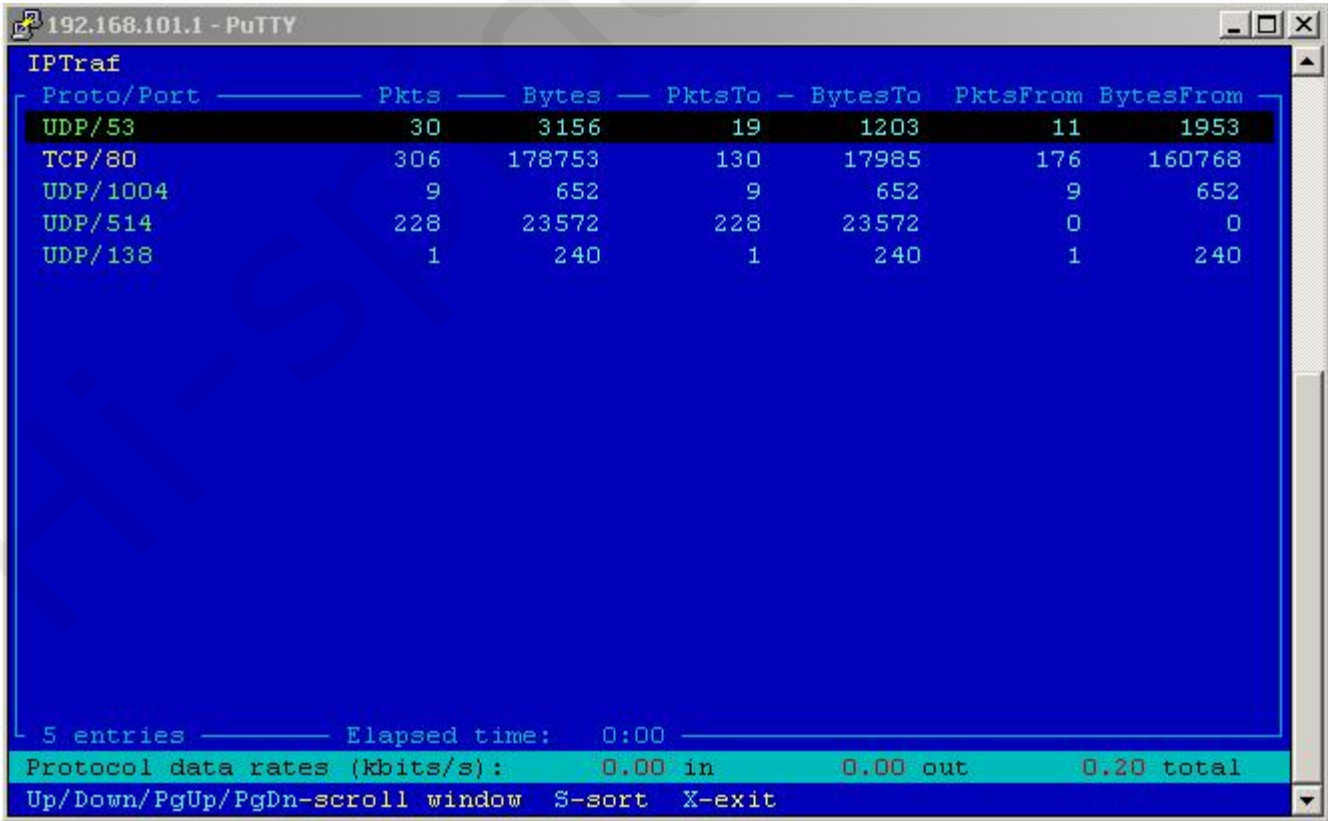
- 选择“第2项”，查看每个网络接口的一般统计信息：

IPTraf						
Iface	Total	IP	NonIP	BadIP	Activity	
lo	48	48	0	0	0.00 kbits/sec	
eth0	2603	2603	0	0	324.00 kbits/sec	
eth1	0	0	0	0	0.00 kbits/sec	
eth2	9897	9897	0	0	1633.20 kbits/sec	
tun0	0	0	0	0	0.00 kbits/sec	
ppp1	4617	4617	0	0	627.20 kbits/sec	
ppp0	1	1	0	0	0.00 kbits/sec	
ppp2	481	481	0	0	28.20 kbits/sec	
ppp3	215	215	0	0	11.20 kbits/sec	
ppp4	34	34	0	0	0.20 kbits/sec	
ppp5	2676	2676	0	0	652.00 kbits/sec	
ppp6	71	71	0	0	0.40 kbits/sec	
ppp7	178	178	0	0	25.40 kbits/sec	
ppp8	26	26	0	0	0.00 kbits/sec	
ppp9	48	48	0	0	0.20 kbits/sec	

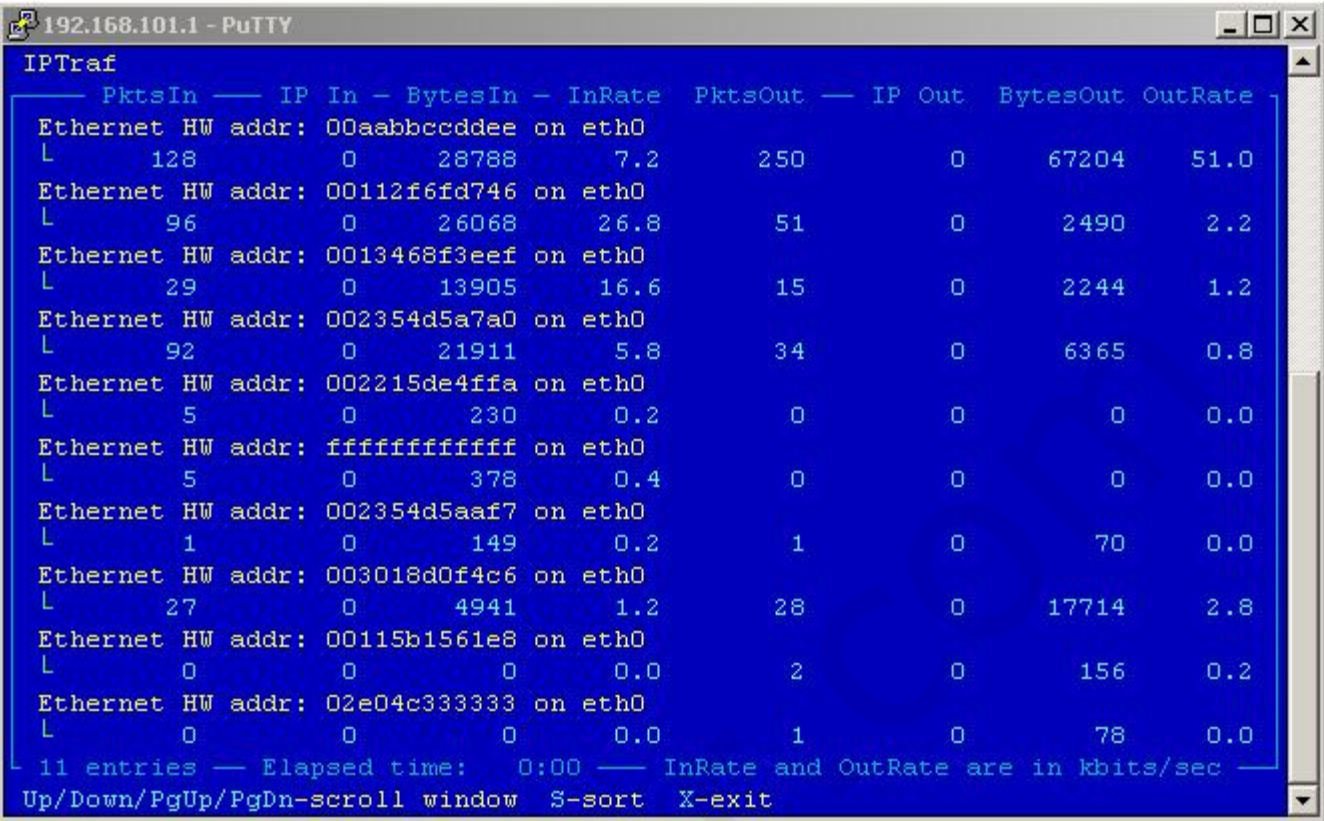
- 选择第3项，查看局域网网卡的详细统计信息，出现网卡选择菜单时，选择“eth0”



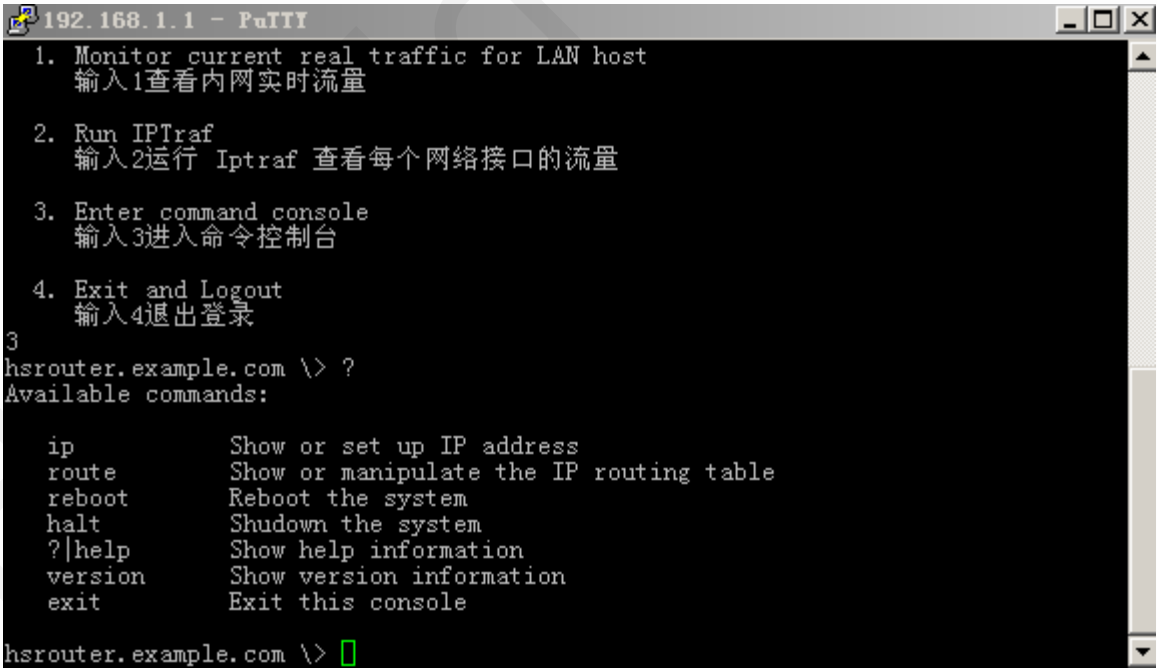
- 选择第4项 -> 统计方式选择"By TCP/UDP port", 查看各端口的流量信息, 出现网卡选择菜单时, 选择 "eth0"



- 选择第5项, 查看局域网状态统计信息, 出现网卡选择菜单时, 选择 "eth0"



在主菜单里选择第3项即可进入命令控制台，这里可以配置IP和路由表，输入"?"可以查看命令：



在主菜单里选择第4项即退出登录。





部分 VIII. 扩展模块

目录

[39. ha \(高可用性套件\) 模块](#)

[40. msgw \(短信网关\) 模块](#)

[41. FTP 服务](#)

[41.1. 什么是 FTP 服务](#)

[41.2. FTP 服务器参数设置](#)

[41.3. FTP 账号管理](#)

[42. PXE 无盘服务](#)

[42.1. 什么是 PXE 无盘服务](#)

[42.2. PXE 无盘分组启动的典型解决方案](#)

[42.3. PXE 无盘分组启动的设置](#)

[42.4. 制作PXE的多重启动](#)

[43. 无线接入服务](#)

[43.1. 服务端设置](#)

[43.2. 客户端设置](#)

[43.3. 无线AP支持网卡列表](#)

[44. IPsec VPN 模块](#)

[44.1. 什么是 IPsec VPN](#)

[44.2. IPsec VPN 的典型解决方案](#)

[44.3. IPsec VPN 的设置](#)

[44.4. 测试 VPN 连接](#)

[44.5. 与其它设备建立IPsec VPN](#)

[44.5.1. 与天融信网络卫士防火墙建立IPsec VPN](#)

[45. 智能 QoS 模块](#)

[46. 安全流控模块](#)

[46.1. 安全流控简介](#)

[46.2. 安全流控配置](#)

[46.3. 安全流控的升级](#)

[46.4. 安全流控的部署](#)

[46.4.1. 万象2004版+易游有盘整合版安装部署](#)

[46.4.2. PUBWIN2007+易游有盘整合版安装部署](#)

- [46.4.3. 顺网无盘安装部署](#)
- [46.4.4. 易游无盘安装部署](#)
- [46.4.5. 信佑无盘安装部署](#)

- [47. 第四代流控](#)
- [48. ipgeodbs \(IP地理位置数据库\) 模块](#)
- [49. npnp 即插即用服务](#)



38.3. 利用Putty查看路由流量



第 39 章 ha (高可用性套件) 模块

第 39 章 ha (高可用性套件) 模块
部分 VIII. 扩展模块

第 39 章 ha (高可用性套件) 模块

名称: ha (High Availability)

功能: 实现 VRRP (Virtual Router Redundancy Protocol) 虚拟路由器冗余协议, 具体功能如下图:

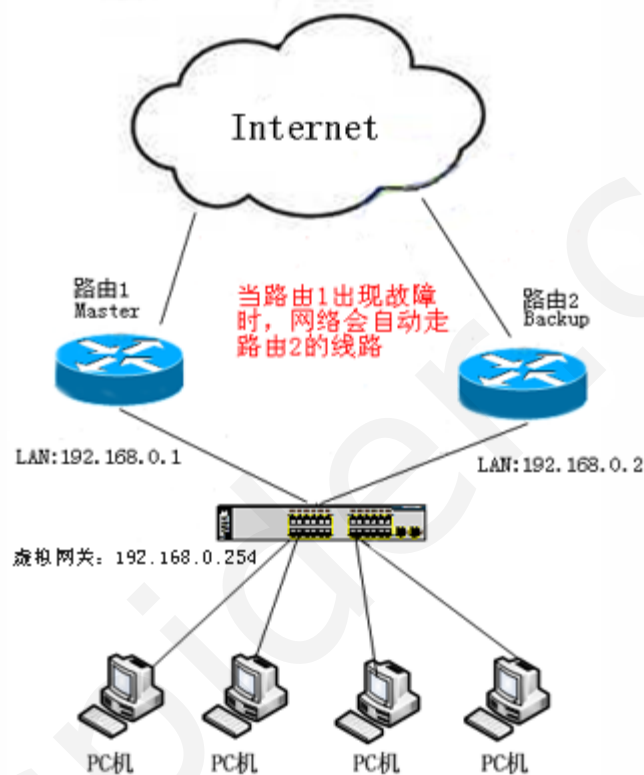


图 39.1. 网络拓扑图

安装此模块后在Web主页中进入“系统设置”->“高可用性 (VRRP)”, 设置工作模式, 通告时间间隔, 虚拟网关IP地址等, 如下图:

☒ 启用 VRRP 服务

服务运行状态: 运行中 (PID:14972)

	工作模式:	<input checked="" type="radio"/> 主路由	<input type="radio"/> 备份路由
主路由和备份路由ID号相同	虚拟路由ID:	254	(主路由和备份路由的ID必须相同, ID范围: 1~254)
	优先级:	254	(主路由的优先级数字必须大于备份路由, 优先级范围: 1~254)
单位为秒	通告时间间隔:	3	(3~30)
	验证密码:	123456	
	虚拟网关IP地址:	192.168.0.254	
选择监控的WAN口	需要额外监控的网络设备:	<input checked="" type="checkbox"/> WAN-1 (eth0/eth0/220.249. XXX. XXX/255.255.255.224)	
		<input checked="" type="checkbox"/> WAN-2 (eth3/ppp0/119.24. xx. xx/255.255.255.255)	

确定

重置

清空日志

日志记录

图 39.2. 主路由的VRRP设置

☒ 启用 VRRP 服务

	工作模式:	<input type="radio"/> 主路由	<input checked="" type="radio"/> 备份路由
主路由和备份路由ID号相同	虚拟路由ID:	254	(主路由和备份路由的ID必须相同, ID范围: 1~254)
	优先级:	100	(优先级为数字: 1~254, 越大优先级越高, 主路由的优先级须大于备份路由)
时间为秒	通告时间间隔:	3	(3~30)
	验证密码:	123456	
	虚拟网关IP地址:	192.168.0.254	
选择监控的WAN口	需要额外监控的网络设备:	<input checked="" type="checkbox"/> WAN-1 (eth1/ppp1/59.173. XX. XX /255.255.255.255)	

确定

重置

清空日志

日志记录

图 39.3. 备份路由的VRRP设置



注意

通告时间间隔是指主路由发生故障时, 需要多长时间自动切换到备份路由。此时间单位为秒。

需要额外监控的网络设备指的是监听WAN口接入, 这里指当WAN-1或WAN-2口任意一个断线后就会走备份路由线路。

主路由和备份路由的虚拟ID必须相同, 优先级主路由应大于备份路由。

设置完后就可以开始测试，在局域网内任意计算机的命令提示符下输入"arp -a"，就会显示当前网关和相应的路由MAC地址，下图是两台路由都正常运作的测试结果，此时网关的MAC地址为主路由的MAC地址。

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.0.33 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.0.1           00-1b-21-54-15-6f    dynamic
  192.168.0.2           00-40-63-e3-7d-23    dynamic
  192.168.0.254         00-1b-21-54-15-6f    dynamic
```

虚拟网关MAC地址为主路由的MAC地址

图 39.4. 网关测试图1

下图是主路由断开，自动启用备份路由的测试结果，此时网关的MAC地址为备份路由的MAC地址。

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.0.33 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.0.1           00-1b-21-54-15-6f    dynamic
  192.168.0.2           00-40-63-e3-7d-23    dynamic
  192.168.0.254         00-40-63-e3-7d-23    dynamic
```

虚拟路由的MAC地址为备份路由的MAC地址

图 39.5. 网关测试图2



第 40 章 msgsw (短信网关) 模块
部分 VIII. 扩展模块

第 40 章 msgsw (短信网关) 模块

名称: msgsw (short message service gateway)

功能: 在路由上实现群发短信

安装此模块后在web主页中进入“系统设置”->“短信网关”，选择短信猫的接口类型，再输入要发送的手机号和内容后，点击发送 即可。

短信猫设备类型:	RS232 串口	确定
短信网关状态:	工作正常	
手机号码:	<div>1395687XXXX 1512485XXXX 1592874XXXX 1395646XXXX 1305942XXXX 1860125XXXX 1375724XXXX 1365724XXXX 1532493XXXX 1894785XXXX</div> <div>(每个号码占一行, 最多10行)</div>	
短信内容:	<div>测试发送!</div> <div>清空</div>	
队列状态:	空	
<div>发送 重置 日志记录 清除</div>		

图 40.1. 短信群发



重要

实现此功能需要在路由上添加一块GSM MODEM，将任意SIM卡置入后才能使用，短信群发目前支持一次最多发10个号码。

点击 日志记录 你也可以看到刚才的发送信息记录，如图：



图 40.2. 日志记录

路由系统目前支持USB和串口两种接口，支持的GSM MODEM型号如：wavecom Q2303



图 40.3. wavecom Q2303





第 41 章 FTP 服务

目录

- [41.1. 什么是 FTP 服务](#)
- [41.2. FTP 服务器参数设置](#)
- [41.3. FTP 账号管理](#)

41.1. 什么是 FTP 服务

FTP (File Transfer Protocol) 是一种用于Internet上的控制文件的双向传输协议。FTP 服务的作用是使路由具有文件服务器功能，为用户提供网络存储空间并实现信息共享。



小提示

FTP服务一般配合PXE无盘服务用于为无盘主机提供文件的存储和读取。



41.2. FTP 服务器参数设置

第 41 章 FTP 服务

41.2. FTP 服务器参数设置

登录路由主页面，进入“服务应用”->“FTP 服务”进入参数设置，勾选启用 FTP 服务，配置匿名登录：

启用 FTP 服务:	<input checked="" type="checkbox"/> 是
FTP 监听端口:	21 (默认为 21)
FTP 被动模式端口范围:	10000 - 20000 (默认为 30000-50000)
FTP 主目录:	/dev/sda3 -- /data/sda3
仅允许匿名登录(用作匿名 FTP 服务器):	<input type="checkbox"/> 是
禁止匿名登录(需要用户名/密码才能登录):	<input type="checkbox"/> 是
最大允许的同时在线人数:	1000 (服务器超过此连接将不再接受新的登录)
同一IP最大允许同时登录的帐号数:	10
同一帐号最大允许的并发连接数:	5
匿名用户最大并发连接数:	1000 (最多允许多少匿名用户同时登录)
最大空闲时间(断开连接超时时间):	10 分钟 (用户超过此时间没有任何操作, 则断开连接)
匿名用户上传/下载比率:	0 (如 1:5, 0 表示没有限制)
匿名用户上传/下载带宽限制:	100 KByte/s (0 表示没有限制)
最大可用磁盘空间(占总磁盘空间百分比):	90 % (磁盘使用率超过此百分比 FTP 上传将被禁止, 以防磁盘爆满, 为 0 表示无限制)
SSL/TLS 连接支持(加密方式登录及数据传输):	禁用 SSL/TLS (仅允许明文登录, 默认)
登录欢迎消息:	== 欢迎登录海蜘蛛 FTP 服务器 == == 海蜘蛛网络, 做最好的中文软路由! ==

图 41.1. FTP 匿名登录配置

FTP被动模式端口范围用于服务器开放一系列TCP数据端口供多个客户端连接，FTP主目录选择挂载的大容量硬盘（系统设置-磁盘分区管理中查看），最大允许的同时在线人数和匿名用户最大并发连接数根据您的实际需要填写，同一IP最大允许同时登录的帐号数是用来限制单个IP同时连接此服务器的账号数，SSL/TLS 连接支持(加密方式登录及数据传输) 是指连接时是否启用SSL/TLS加密认证，此选项适用于安全性较高的场合，其它选项采用默认即可。



提示

登录欢迎消息里的内容仅在使用 FlashFXP 等工具登录时显示在日志中，用户Web登陆时并不显示。



警告

仅允许匿名登录（用作匿名 FTP 服务器）这一项勾选后会使管理账户无法登录，慎选！

FTP 主目录 不支持FAT32、NTFS文件格式，这两种文件格式建立的FTP主目录会导致文件无法上传，您可以在“系统设置”->“磁盘分区管理”中查看：

sda - WDC WD5000ADS-0 [500.1 GB]		
分区	大小	文件系统
/dev/sda1	100.0 GB	reiserfs
Free	400.1 GB	

* hda - Fordisk IDE DOM [523.8 MB]		
分区	大小	文件系统
/dev/hda1	256.5 MB	reiserfs
Free	267.3 MB	



小知识——FTP被动模式

一般的主动FTP在建立数据连接时是由FTP服务器的20端口主动向客户机连接，但这有可能被客户机的防火墙所拦截。启用被动模式在建立数据连接时是由客户端向服务端发起，这样数据就不会被客户端的防火墙所拦截掉。例如这里的被动模式端口范围为10000-20000，用类似FlashFXP工具进行上传时，在站点管理器的选项中启用被动模式传送：

常规选项传输高级SSL书签

☒ 对于被动模式连接使用站点 IP

☒ 该站点禁用“强制主动模式使用该 IP”

☐ 发送反空闲保持连接

☐ 传输期间发送 noop *

☐ 使用 APPE 继续上传

☐ 显示隐藏的文件 (LIST -al)

☒ 使用被动模式

☐ 使用跳过列表

☐ 缓存目录

☐ 使用“STAT -L”来列出目录 *

☐ 站点不支持 FEAT 命令

☐ Activate Synchronize Browsing on Connect

* = 并非与所有 FTP 服务器都兼容

任意传一个文件，可以看到已启用被动模式PASV，端口范围也在设定的10000-20000之内：

```
[R] TYPE A
[R] 200 TYPE目前是 ASCII
[R] PASV
[R] 227 Entering Passive Mode (192,168,0,1,66,56)
[R] 正在打开数据连接 IP: 192.168.0.1 端口: 16952
[R] LIST -al
[R] 150 接受数据连接
[R] 226-Options: -a -l
[R] 226 总共 4 符合
[R] 列表完成: 294 字节 用时 0.03 秒 (9.0 KB/s)
传输队列已完成
已传输 1 个文件, 总计 20 KB 用时 0.09 秒 (1.30 MB/s)
```

在任意一联网电脑上输入ftp://路由IP/，即可匿名登陆到服务器。

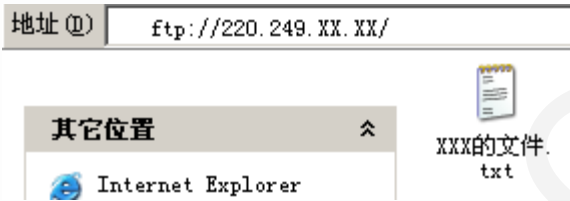


图 41.2. 匿名登陆



提示

匿名登陆时所有用户登陆是在同一目录/ftp下操作，在此目录下匿名用户只能上传和下载文件，不能修改和删除文件。

如果您需要设置全部都用账户登录，则勾选禁止匿名登录（需要用户名/密码才能登录）

启用 FTP 服务:	<input checked="" type="checkbox"/> 是
FTP 监听端口:	21 (默认为 21)
FTP 被动模式端口范围:	10000 - 20000 (默认为 30000-50000)
FTP 主目录:	/dev/sda1 -- /data/data1
仅允许匿名登录(用作匿名 FTP 服务器):	<input type="checkbox"/> 是
禁止匿名登录(需要用户名/密码才能登录):	<input checked="" type="checkbox"/> 是
最大允许的同时在线人数:	1000 (服务器超过此连接将不再接受新的登录)
同一IP最大允许同时登录的帐号数:	10
同一帐号最大允许的并发连接数:	10
匿名用户最大并发连接数:	0 (最多允许多少匿名用户同时登录)
最大空闲时间(断开连接超时时间):	10 分钟 (用户超过此时间没有任何操作, 则断开连接)
匿名用户上传/下载比率:	0 (如 1:5, 0 表示没有限制)
匿名用户上传/下载带宽限制:	0 KByte/s (0 表示没有限制)
最大可用磁盘空间(占总磁盘空间百分比):	90 % (磁盘使用率超过此百分比 FTP 上传将被禁止, 以防磁盘爆满, 为 0 表示无限制)
SSL/TLS 连接支持(加密方式登录及数据传输):	禁用 SSL/TLS (仅允许明文登录, 默认)
登录欢迎消息:	== 欢迎登录海蜘蛛 FTP 服务器 == == 海蜘蛛网络, 做最好的中文软路由! ==

图 41.3. FTP 认证登录配置

最大允许的同时在线人数根据您的实际需要填写，同一帐号最大允许的并发连接数指设置的每个账户可以允许多少个线程同时登陆服务器，其它选项采用默认值。



警告

FTP 主目录 不支持FAT32、NTFS文件格式，这两种文件格式建立的FTP主目录会导致文件无法上传，您可以在“系统设置”->“磁盘分区管理”中查看：

sda - WDC WD5000AADS-0 [500.1 GB]		
分区	大小	文件系统
/dev/sda1	100.0 GB	reiserfs
Free	400.1 GB	

* hda - Fordisk IDE DOM [523.8 MB]		
分区	大小	文件系统
/dev/hda1	256.5 MB	reiserfs
Free	267.3 MB	

在任意一联网电脑上输入ftp://路由IP/，进入认证页面，输入用户ID和密码，点击登陆：

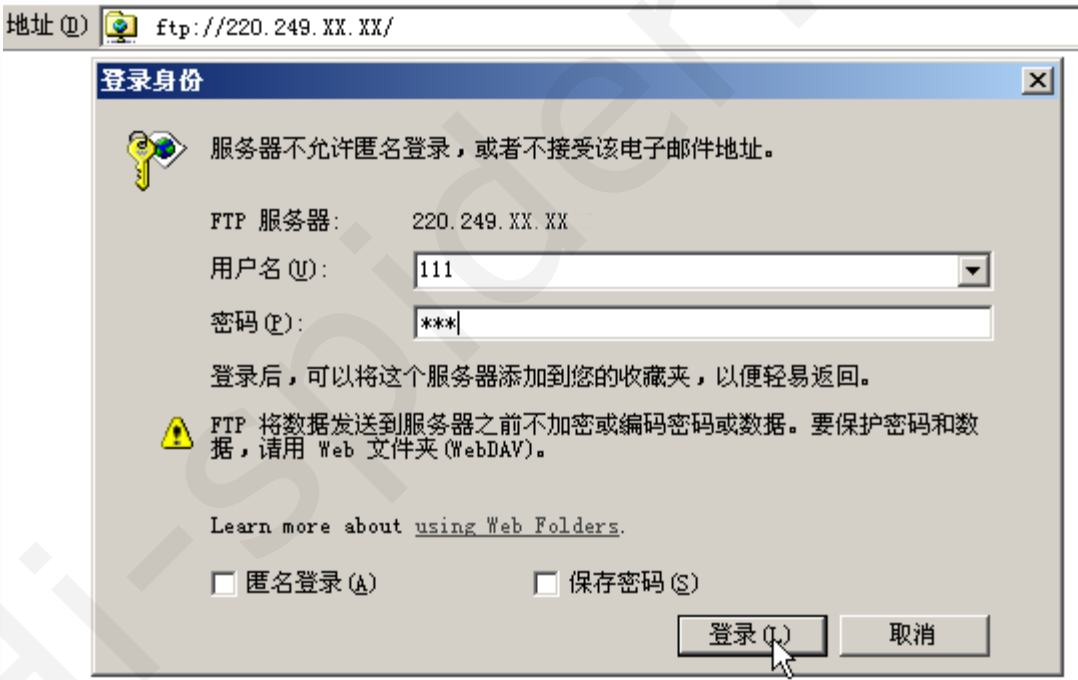


图 41.4. 登陆认证

此种方法登陆后，每个账户都是单独隔离出来的目录，并且每个账户拥有自己目录内的所有操作权限。

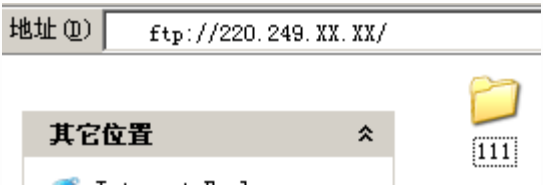


图 41.5. 登陆页面



第 41 章 FTP 服务



41.3. FTP 账号管理



41.3. FTP 账号管理

配置认证账号，点击账号管理页面，点击新增用户进入设置页面。填入用户ID、姓名和密码，在可用功能列表中勾选FTP。

用户ID:	<input type="text" value="111"/>	(能由数字、字母、下)
真实姓名:	<input type="text" value="111"/>	
登录密码:	<input type="password" value="..."/>	(为空表示不修改)
密码确认:	<input type="password" value="..."/>	
帐号使用周期:	<input type="text" value=""/> [生效] <input type="text" value=""/> [到期]	
允许拨号的时间段:	<input type="text"/>	
分配固定IP:	<input type="text"/>	(客户连接后始终获取此IP,仅适用于PPPoE/
可用功能列表:	<input checked="" type="checkbox"/> FTP <input type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input type="checkbox"/> Web	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 41.6. FTP 账户设置1

在此页面下端有 FTP 帐号高级属性可供选填：

FTP 空间大小:	<input type="text" value="100"/>	MB (0 表示不限大小)
可存储文件总数:	<input type="text" value="50"/>	(0 表示不限文件数)
最大上传速度:	<input type="text" value="50"/>	KByte/s (0 表示不限速)
最大下载速度:	<input type="text" value="100"/>	KByte/s (0 表示不限速)
上传/下载比率:	<input type="text" value="0"/> : <input type="text" value="0"/>	(限制用户下载前必须先上传文件, 为0表示不限制)

图 41.7. FTP 账户设置2

此属性请您根据实际需要自定义配置。



重要

初期建立账号时一定要建立以下三个特殊账号来用于总体管理：
ftpadmin 拥有管理所有匿名账户的权限

pxeadmin 拥有管理pxe无盘文件的权限

ftpsuper 拥有管理所有账户的权限

用户ID:	<input type="text" value="ftpsuper"/>
真实姓名:	<input type="text" value="ftpsuper"/>
登录密码:	<input type="password" value="....."/>
密码确认:	<input type="password" value="....."/>
帐号使用周期:	<input type="text" value=""/>
允许拨号的时间段:	<input type="text" value=""/>
分配固定IP:	<input type="text" value=""/>
可用功能列表:	<input checked="" type="checkbox"/> FTP <input type="checkbox"/> PPPoE
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用

图 41.8. 建立特殊账号





第 42 章 PXE 无盘服务

目录

- [42.1. 什么是 PXE 无盘服务](#)
- [42.2. PXE 无盘分组启动的典型解决方案](#)
- [42.3. PXE 无盘分组启动的设置](#)
- [42.4. 制作PXE的多重启动](#)

42.1. 什么是 PXE 无盘服务

PXE (preboot execute environment) 是RPL的升级品，工作于 Client/Server 的网络模式，它可以使工作站通过网络从远端服务器下载映像，并由此映像来网络启动计算机。

PXE 无盘服务包括无盘安装和无盘启动，无盘安装部分参考 [路由下的PXE无盘安装](#)



小知识

PXE无盘工作站的启动过程：客户端个人电脑开机后，Bootprom 在组内广播送出 BOOTP/DHCP 要求取得IP。如果网内有服务器收到个人电脑所送出的要求，就会送回 BOOTP/DHCP 回应，内容包括客户端的IP地址、预设网关及开机映像文件。Bootprom 由TFTP通讯协议从服务器下载开机映像文件。远程客户端通过这个开机影像文件启动电脑。



41.3. FTP 账号管理



42.2. PXE 无盘分组启动的典型解决方案



42.2. PXE 无盘分组启动的典型解决方案

某一网吧内划分了两个VLAN：

- VLAN1：192.168.10.10 - 192.168.10.20 为管理区，网管在此区域计算机上启动DOS工具箱方便对整个系统的管理。
- VLAN2：192.168.20.100 - 192.168.20.200 为用户区，网吧上网用户在此区域计算机上启动windows xp系统以便进行各种娱乐活动。

网络拓扑图如下：

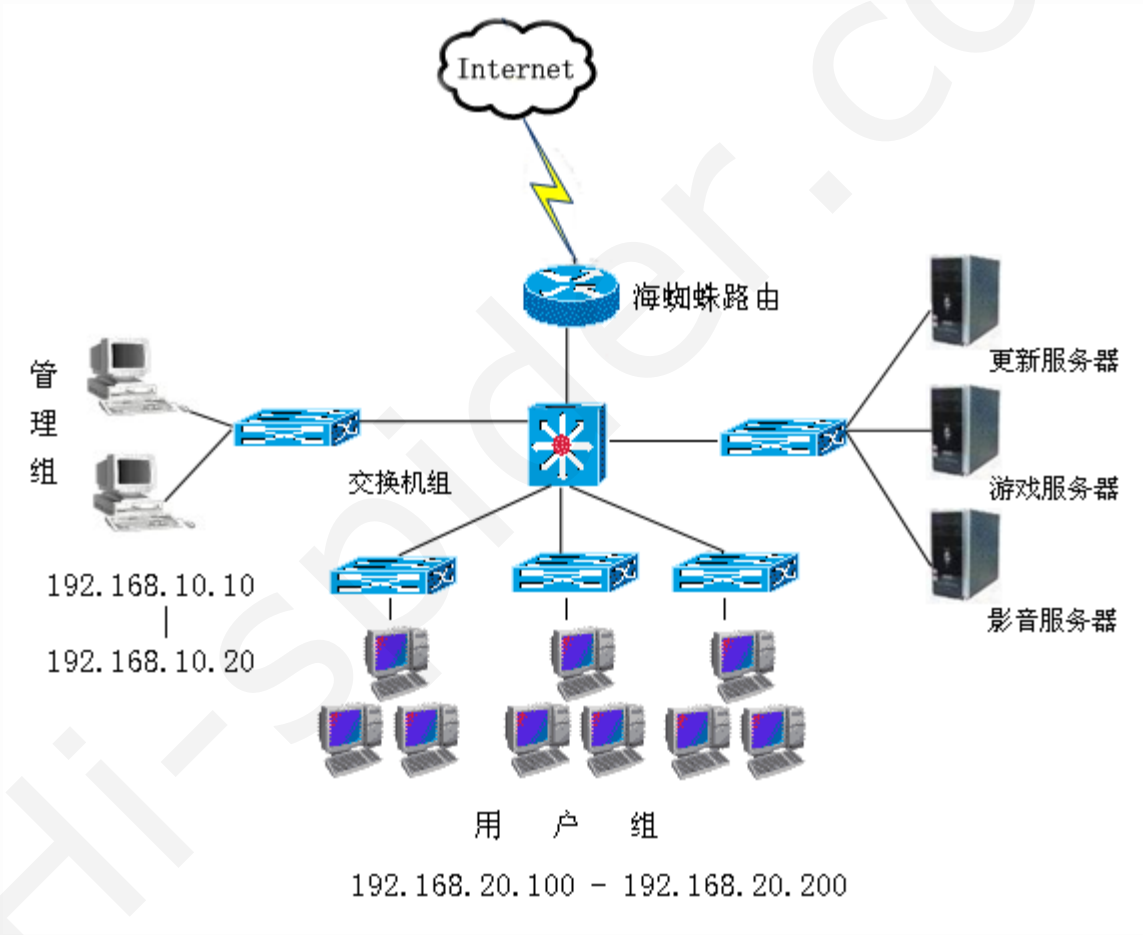


图 42.1. 网吧拓扑图



42.3. PXE 无盘分组启动的设置
第 42 章 PXE 无盘服务



42.3. PXE 无盘分组启动的设置

首先新建两个VLAN，具体设置参照 [虚拟局域网](#)

☒ 启用 VLAN (虚拟局域网)功能

ID	VLAN_ID	IP地址	子网掩码	线路	备注	激活	编辑
1	10	192.168.10.1	255.255.255.0	lan1			
2	20	192.168.20.1	255.255.255.0	lan1			

[\[专家模式\]](#) [\[导出规则\]](#)

[提交修改](#) [重置](#) [新增](#) [查看状态](#) [日志记录](#)

图 42.2. 设置VLAN

然后启用DHCP 服务，具体设置参照 [启动DHCP服务](#)

[参数设置](#) [IP地址池](#) [固定IP分配](#) [当前IP分配信息](#)

ID	接口	分配的IP地址段	子网掩码	网关	备注	激活/编辑/删除/选择
1	LAN1.10	192.168.10.10-192.168.10.20	255.255.255.0	192.168.10.1		<input type="checkbox"/>
2	LAN1.20	192.168.20.100-192.168.20.200	255.255.255.0	192.168.20.1		<input type="checkbox"/>

[新增地址池](#) [全选/全不选](#)

图 42.3. 启用DHCP

接着启用 PXE 无盘服务，进入“服务应用”->“PXE 无盘服务”，勾选 启用 PXE/TFTP 服务，选择上传文件页面，将DOS工具映像文件DOS_tools.ima上传到tftp的根目录：

文件名： [浏览...](#)

配置文件目录：

这里为空表示根目录

重命名： (为空表示不重命名)

是否自动覆盖已经存在的文件：☐ 是

上传后是否自动解压缩：☐ 是 (仅支持 ZIP/TAR/TGZ 格式压缩文件)

[上传](#) [重置](#)

图 42.4. 上传文件

文件上传后会在文件列表的根目录下显示（以开头的目录）。最后配置启动文件，进入分组管理，编辑需要设定的组，启动文件类型选择GRUB4DOS，配置信息如下：

IP地址:	192.168.10.10-192.168.10.20	(192.168.0.100-192.168.0.200)
优先级:	1	
启动文件类型:	GRUB4DOS	
配置信息:	<pre>fontfile (pd)/fonts.gz pxe blksize 1456 default 0 timeout=0 title DOS 工具箱 map --mem (pd)/DOS_tools.ima (fd0) map --hook chainloader (fd0)+1 rootnoverify (fd0)</pre>	

填写您上传的
DOS工具映像

图 42.5. 管理区配置

IP地址:	192.168.20.100-192.168.20.200	(192.168.0.100-192.168.0.200)
优先级:	1	
启动文件类型:	GRUB4DOS	
配置信息:	<pre>fontfile (pd)/fonts.gz pxe blksize 1456 default 0 timeout=0 title 启动硬盘上 WIN NT/03/XP map (hd0) (hd0) map (hd0) (hd1) root (hd0,0) chainloader (hd0,0)+1 boot rootnoverify (hd0,0) chainloader +1 clear</pre>	

图 42.6. 用户区配置

这里的DOS_tools.ima是上传到tftp的根目录DOS工具映像文件。保存设置后，就可以在内网电脑上使用 PXE 无盘分组启动了。

 重要

内网电脑主板要支持从网络启动，并且需要在BIOS里都设置好从网络启动！



42.4. 制作PXE的多重启动

有时我们需要制作网络多重启动方式，就如在电脑上安装多系统启动那样。

进入PXE无盘服务的文件列表页面，编辑menu.lst目录下的default文件：

6	menu.lst/	default	0.0 bytes	2010-09-27 14:35:47	2010-09-27 13:59:59			
7	pxelinux.cfg/	0	133.0 bytes	2010-09-27 14:51:17	2010-09-27 14:51:17			
8	pxelinux.cfg/	default	133.0 bytes	2010-09-27 14:35:47	2010-09-09 09:57:45			

共 59.73 MB

[全选](#)/[全不选](#)

编辑 /menu.lst/default:

图 42.7. 编辑default文件

在编辑框内输入以下内容：/* */内为注释

```
fontfile (pd)/fonts.gz
pxe blksize 1456
default 0      /* default 0 指默认启动项为第一项 */
timeout=5     /* timeout=5 指多重启动菜单停留时间为5秒钟，设置为0则不选择直接进入默认启动项。您可以根据实际需要自行修改。 */

title DOS 工具箱
map --mem (pd)/DOS_tools.ima (fd0)  /* 这里的DOS_tools.ima是上传的映像文件名 */
map --hook
chainloader (fd0)+1
rootnoverify (fd0)

title 启动一键还原Ghost系统
map --mem (pd)/ghost.img (fd0)      /* 这里的ghost.img是上传的镜像文件名 */
map --hook
chainloader (fd0)+1
rootnoverify (fd0)

title 启动 WinPE
map --mem (pd)/BootCD_070911.iso (0xff)  /* 这里的BootCD_070911.iso是上传的镜像文件名 */
map --hook
chainloader (0xff)
boot

title pxe install hsrouter  /* 此选项为安装海蜘蛛路由需要先上传vmlinuz、initrd.gz和ISO镜像文件 */
kernel (pd)/vmlinuz
initrd (pd)/initrd.gz

title 启动硬盘上 Win NT/03/XP
map (hd0) (hd0)
map (hd0) (hd1)
root (hd0,0)
chainloader (hd0,0)+1
boot
rootnoverify (hd0,0)
chainloader +1
clear

title 启动硬盘上 VISTA
find --set-root /bootmgr
chainloader /bootmgr
```

```
clear

title 从光驱启动
cdrom --init
map --hook
chainloader (cd0)
boot

title 重启计算机
reboot
clear

title 关闭计算机
halt
```

以上的每个**title**对应一个启动项，可以自行选择填写。**default 0** 代表默认启动选项为第一项也就是 **title DOS 工具箱**，如果设置成**default 1** 代表默认启动选项为第二项也就是 **title 启动一键还原Ghost系统**，依此类推。



第 43 章 无线接入服务

目录

[43.1. 服务端设置](#)

[43.2. 客户端设置](#)

[43.3. 无线AP支持网卡列表](#)

无线接入是在路由电脑上安装一个无线 AP(Access Point)，使信号内的计算机能够通过无线网卡来接入路由上网。

43.1. 服务端设置

进入Web登陆主页面，“服务应用”->“无线 AP 服务”，勾选 启用无线接入服务，输入无线网络ID名称，如图：

<input checked="" type="checkbox"/> 启用无线接入服务		
无线网卡:	wlan0 (选择要启用AP功能的无线网卡)	
无线网络ID (SSID):	Wireless_AP (只能由字母、数字、下划线、圆点及减号组成)	
IP地址:	192.168.168.1	
子网掩码:	255.255.255.0	
模式:	54M (802.11g)	
信道:	Channel-1	
安全设置...		
启用无线接入访问保护 (WPA):	<input checked="" type="checkbox"/> 是	
WPA 类型:	自动设置	
认证算法:	自动设置	
加密算法:	自动设置	
密码:	12345678 (密码长度 8-32 位, 只能由数字、字母、下划线、减号和圆点组成)	
组密钥更新周期:	600 (0为不更新, 最小值30, 默认600)	
MAC 地址访问控制...		
ACL 策略:	<input type="radio"/> 允许指定MAC地址访问, 拒绝所有其他访问 <input type="radio"/> 拒绝指定MAC地址访问, 允许所有其他访问 <input checked="" type="radio"/> 无	
MAC 地址列表:	允许	拒绝

图 43.1. 无线接入服务设置

这里的IP地址为无线AP的接入地址，相当于设置路由的LAN口地址，子网掩码来设置此网络段能容纳的客户机数量，例如上图的子网掩码就可以让客户机自动获取从192.168.168.2到192.168.168.254的IP地址，安全设置一般情况下选择默认，手动输入密码。下面的MAC地址列表是允许或禁止特定的无线网卡来接入路由的无线AP。



敬生日

这里无线AP的接入IP地址不要和有线局域网内的IP地址同网段，否则会造成冲突无法上网。





Hi-Spider.com



43.2. 客户端设置

这里以TP-link的TL-WN322G+型号为例，插入USB无线网卡，安装无线网卡驱动。安装好后电脑右下角会有个无线网络标识，单击进入无线网络连接页面，选择刚才设置的无线网络ID名称Wireless_AP：

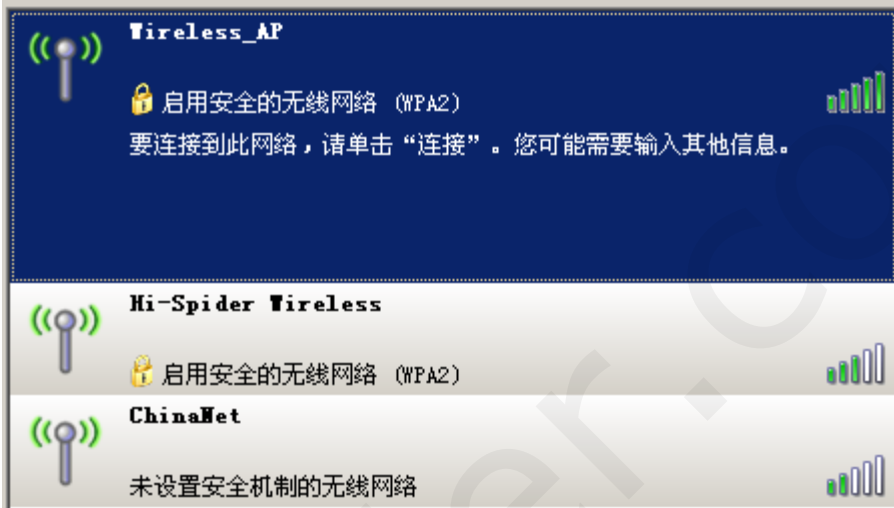


图 43.2. 选择 Wireless_AP

点击连接会要求输入网络密钥，输入刚才设定的密码12345678，点击连接。

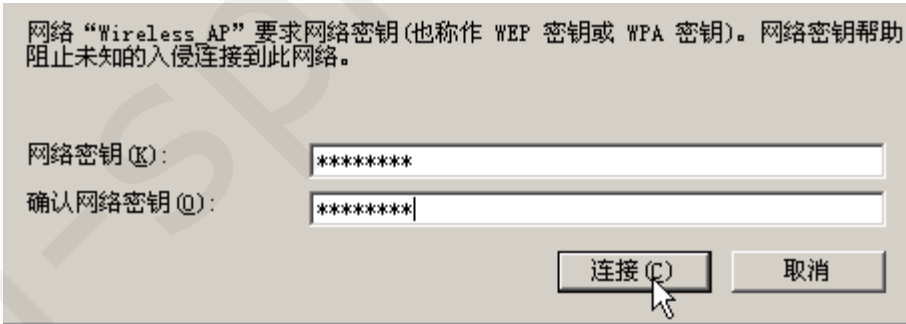


图 43.3. 连接 Wireless_AP

连接成功后右下角的无线网络标识会显示已连接上，现在就可以利用无线网络来上网了。



43.3. 无线AP支持网卡列表

第 43 章 无线接入服务



43.3. 无线AP支持网卡列表

无线AP服务支持USB、PCI或PCI-E接口。

- Ralink RT2870/RT2070 芯片 IP-COM W323G+ Mini 54M无线USB网卡和W827U 11N 无线USB网卡
- Ralink RT2561/RT61芯片 D-Link DWL-G520+A 802.11g 54M 无线PCI网卡
- Ralink RT3070芯片 SK-8TN USB无线网卡
- Atheros Communications Inc. AR928X Wireless Network Adapter (PCI-Express)



43.2. 客户端设置



第 44 章 IPSec VPN 模块



第 44 章 IPsec VPN 模块

目录

[44.1. 什么是 IPsec VPN](#)

[44.2. IPsec VPN 的典型解决方案](#)

[44.3. IPsec VPN 的设置](#)

[44.4. 测试 VPN 连接](#)

[44.5. 与其它设备建立IPsec VPN](#)

[44.5.1. 与天融信网络卫士防火墙建立IPsec VPN](#)

44.1. 什么是 IPsec VPN

IPsec (IP Security) 协议族是IETF制定的一系列协议，它为IP数据包提供了高质量的、可互相操作的、基于密码学的安全保护。特定的通信方之间在IP层通过加密与数据源验证等方式，来保证数据包在网络上传输的私有性、完整性、真实性和防重放。

IPsec是一个基于IP协议的安全标准，用于保证IP数据包传输时的安全性。IPsec协议由安全协议（包括AH协议和ESP协议）、密钥管理协议（如IKE）以及认证和加密算法组成。IPsec VPN适用于局域网互联（LAN to LAN），管理者只需要在路由两端做好配置，两异地局域网内任意两台计算机之间互访就会自动建立 IPsec VPN 通道。

IPsec是目前唯一一种能为任何形式的Internet通信提供安全保护的协议。



[43.3. 无线AP支持网卡列表](#)



[44.2. IPsec VPN 的典型解决方案](#)



44.2. IPSec VPN 的典型解决方案

应用环境说明：

- 企业总部
外网IP为220.249.XX.XX，内局域网为192.168.1.0/24 。
- 某分公司办事处
需要经常和总部交换数据，通过外网和总部相连，外网IP为59.173.XX.XX，内局域网为192.168.101.0/24 。

网络拓扑图如下：

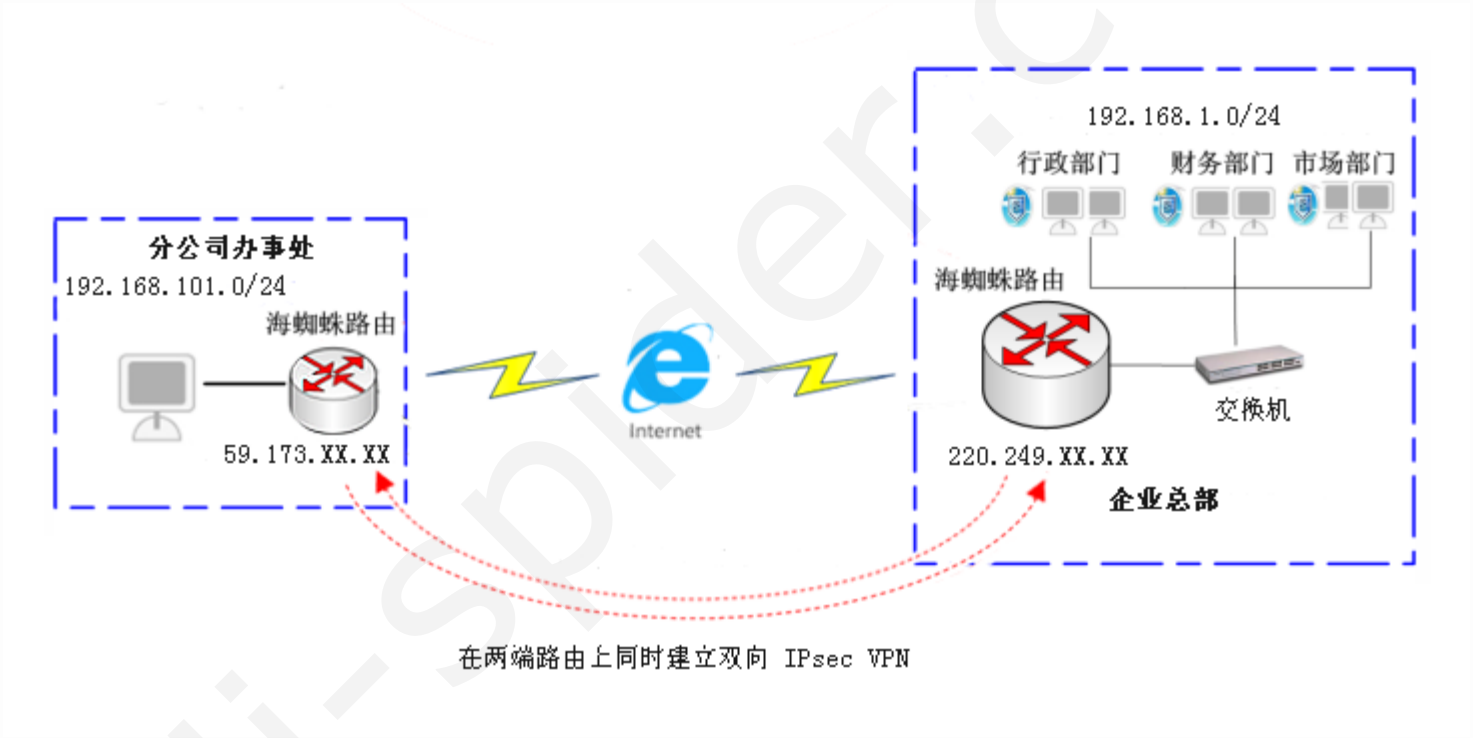



图 44.1. 企业网络 IPSec VPN 安全解决方案



44.3. IPSec_VPN 的设置

IPSec_VPN 的配置分为三步：

- 1. 在两端路由器上设置静态路由。
- 2. 在两端路由器上设置IPSec VPN服务。
- 3. 在两端路由器上设置No NAT规则。



警告

本地和远程两端的局域网段不能相同，不然运行后会导致两端主机都无法正常上网。

下面介绍企业总部和分公司办事处路由器 IPSec_VPN 的详细设置。

- 1. 首先进入路由Web管理页面，“网络设置”->“静态路由”，启用静态路由功能，点击新增。这里的目的网络填写远程局域网的网络号和子网掩码，出口网关勾选自动。

☒ 启用静态路由功能

ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	192.168.101.0/24	<input type="text"/> <input checked="" type="checkbox"/> 自动	WAN-1 (eth0/220.249.XX)	1	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

提交修改

新增

查看状态

日志记录

图 44.2. 总部静态路由设置

☒ 启用静态路由功能

ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	192.168.1.0/24	<input type="text"/> <input checked="" type="checkbox"/> 自动	WAN-1 (eth0/59.173. XX)	1	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

提交修改

新增

查看状态

日志记录

图 44.3. 分公司静态路由设置

- 2. 接下来设置IPSec VPN，进入“服务应用”->“IPSec VPN 服务”，勾选 启用 IPSec VPN 服务，点击新增隧道，如图：

☒ 启用 IPsec VPN 服务

隧道列表

隧道状态

ID	名称	本地局域网 远程局域网	本地IP	远程IP	模式	备注	激活/编辑/删除/选择
<div><div>新增隧道</div><div><div>✔</div><div>✖</div><div>🗑️</div><div>全选/全不选</div></div></div>							

图 44.4. 启用 IPSec VPN 服务

填写名称、远程IP地址、本地局域网段和子网掩码、远程局域网段和子网掩码。模式一般选用Aggressive，根据传递数据的重要性选择不同的加密验证算法，两端的路由都填写相同的共享密钥和DPD 检测间隔。如下图：

名称:	1网段对101网段	(只能由字母、数字、汉字、下划线、圆点及减号组成)
本地IP:	WAN-1 (eth0/eth0/220.249.XX.XX/255.255.255.224)	
远程IP:	57.173.XX.XX	
本地标识:	headquarter	
对方标识:	branch	
本地局域网:	192.168.1.0/24	
远程局域网:	192.168.101.0/24	
模式:	<input checked="" type="radio"/> Aggressive (默认) <input type="radio"/> Main <input type="radio"/> Base	
DH 算法:	DH-2 (modp1024, 默认)	
哈希算法:	SHA1 (默认)	
验证算法:	HMAC_SHA1 (默认)	
Phase 1 加密算法:	3DES (默认)	
Phase 2 加密算法:	3DES (默认)	
共享密钥:	123456	
SA 生存期:	86400 s	
DPD 检测间隔:	20 s (5~120)	
其他参数:	<input type="checkbox"/> 启用调试	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
备注:		

图 44.5. 企业总部 IPSec VPN 设置

名称:	101网段对1网段 (只能由字母、数字、汉字、下划线、圆点及减号组成)
本地IP:	WAN-1 (eth0/ppp0/57.173.XX.XX/255.255.255.224)
远程IP:	220.249.XX.XX
本地标识:	branch
对方标识:	headquarter
本地局域网:	192.168.101.0/24
远程局域网:	192.168.1.0/24
模式:	<input checked="" type="radio"/> Aggressive (默认) <input type="radio"/> Main <input type="radio"/> Base
DH 算法:	DH-2 (modp1024, 默认)
哈希算法:	SHA1 (默认)
验证算法:	HMAC_SHA1 (默认)
Phase 1 加密算法:	3DES (默认)
Phase 2 加密算法:	3DES (默认)
共享密钥:	123456
SA 生存期:	86400 s
DPD 检测间隔:	20 s (5~120)
其他参数:	<input type="checkbox"/> 启用调试
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用
备注:	

图 44.6. 分公司 IPSec VPN 设置



小技巧

如果对方路由为动态IP的话，您只需要在本地路由上设置 [动态域名解析](#)，然后将此域名填入上图的 远程IP 内。

3. 最后设置No NAT，进入“防火墙”->“NAT 策略”->“No NAT 规则”，勾选启用 No NAT 功能，点击新增规则，进入设置页面。

<input checked="" type="checkbox"/> 启用 No NAT 功能								
<table><tr><th>ID</th><th>优先级</th><th>源IP</th><th>目标IP</th></tr><tr><td colspan="4">[新增规则] [批量模式] [专家模式] [导出规则]</td></tr></table>	ID	优先级	源IP	目标IP	[新增规则] [批量模式] [专家模式] [导出规则]			
ID	优先级	源IP	目标IP					
[新增规则] [批量模式] [专家模式] [导出规则]								
保存设置 重置								

图 44.7. 启用 No NAT

填写本地局域网段的网络号和子网掩码，远程局域网的网络号和子网掩码，保存设置即可。

名称:	<input type="text" value="NO NAT"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
源IP:	<input type="text" value="192.168.1.0/24"/>	
目的IP:	<input type="text" value="192.168.101.0/24"/>	
备注:	<input type="text"/>	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
<div>保存设置 重置 取消</div>		

图 44.8. 总部 No NAT 设置

名称:	<input type="text" value="NO NAT"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
源IP:	<input type="text" value="192.168.101.0/24"/>	
目的IP:	<input type="text" value="192.168.1.0/24"/>	
备注:	<input type="text"/>	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
<div>保存设置 重置 取消</div>		

图 44.9. 分公司 No NAT 设置





44.4. 测试 VPN 连接

首先测试两端局域网LAN口是否能互通，进入路由主页面“系统工具”->“PING 测试”，填入对方路由局域网LAN口和本地路由局域网LAN口后，点击开始按钮，如图：

请输入 IP 地址或域名: 192.168.101.4

开始重置清除

分公司路由局域网地址

可选参数:

PING 类型: ICMP/PING (默认)

总部路由局域网地址 指定源IP进行PING: 192.168.1.1

TCP 端口: 80 (默认为 80)

数据包个数: 10 (默认为 10)

数据段大小或长度: 0 bytes (默认为 0)

包发送时间间隔: 100 ms (默认为 100)

等待超时时间: 10 s (默认为 10)

Target IP address: 192.168.101.4
Using interface: eth0 [220.249.124.205]

Echo reply from 192.168.101.4: seq=01 time=58.088 ms
Echo reply from 192.168.101.4: seq=02 time=41.907 ms
Echo reply from 192.168.101.4: seq=03 time=38.391 ms
Echo reply from 192.168.101.4: seq=04 time=38.307 ms
Echo reply from 192.168.101.4: seq=05 time=39.336 ms
Echo reply from 192.168.101.4: seq=06 time=38.754 ms
Echo reply from 192.168.101.4: seq=07 time=66.762 ms
Echo reply from 192.168.101.4: seq=08 time=43.404 ms
Echo reply from 192.168.101.4: seq=09 time=38.494 ms
Echo reply from 192.168.101.4: seq=10 time=38.369 ms

--- 192.168.101.4 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max = 38.307/44.181/66.762 ms

图 44.10. 测试ping分公司路由局域网端口

请输入 IP 地址或域名: 192.168.1.1

开始重置清除

总部路由局域网地址

可选参数:

PING 类型: ICMP/PING (默认)

分公司路由局域网地址 指定源IP进行PING: 192.168.101.4

TCP 端口: 80 (默认为 80)

数据包个数: 10 (默认为 10)

数据段大小或长度: 0 bytes (默认为 0)

包发送时间间隔: 100 ms (默认为 100)

等待超时时间: 10 s (默认为 10)

Target IP address: 192.168.1.1
Using interface: ppp0 [111.173.75.23]

Echo reply from 192.168.1.1: seq=01 time=40.344 ms
Echo reply from 192.168.1.1: seq=02 time=57.472 ms
Echo reply from 192.168.1.1: seq=03 time=79.366 ms
Echo reply from 192.168.1.1: seq=04 time=51.485 ms
Echo reply from 192.168.1.1: seq=05 time=39.073 ms
Echo reply from 192.168.1.1: seq=06 time=53.517 ms
Echo reply from 192.168.1.1: seq=07 time=39.437 ms
Echo reply from 192.168.1.1: seq=08 time=45.262 ms
Echo reply from 192.168.1.1: seq=09 time=48.664 ms
Echo reply from 192.168.1.1: seq=10 time=51.826 ms

--- 192.168.1.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max = 39.073/50.645/79.366 ms

图 44.11. 测试ping总部路由局域网端口

接着测试局域网两端的计算机是否能ping通对方。

```
C:\Documents and Settings\Administrator>ping 192.168.101.178

Pinging 192.168.101.178 with 32 bytes of data:

Reply from 192.168.101.178: bytes=32 time=39ms TTL=126
Reply from 192.168.101.178: bytes=32 time=39ms TTL=126
Reply from 192.168.101.178: bytes=32 time=39ms TTL=126
Reply from 192.168.101.178: bytes=32 time=43ms TTL=126

Ping statistics for 192.168.101.178:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 43ms, Average = 40ms
```

图 44.12. 测试ping分公司局域网内主机

```
C:\Documents and Settings\Administrator>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=49ms TTL=126
Reply from 192.168.1.33: bytes=32 time=38ms TTL=126
Reply from 192.168.1.33: bytes=32 time=40ms TTL=126
Reply from 192.168.1.33: bytes=32 time=41ms TTL=126

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 49ms, Average = 42ms
```

图 44.13. 测试ping总部局域网内主机



提醒

如果路由“防火墙”->“基本安全设置”中“完全禁止了PING”，是无法 Ping 通 VPN 服务器的。

☒ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求)

利用路由系统的抓包功能测试数据加密，进入“系统工具”->“在线抓包分析”，输入对方路由的WAN口地址，任意传送一个文件给远程主机，再点击“开始”，如图：

请输入 IP 地址: 开始 重置 清除

参数:

接口:	WAN-1 (eth0/eth0/220.249.XX.XX/255.255.255.224)
协议类型:	ALL
端口:	0
数据包个数:	10 (10~1000, 默认为 50)
等待超时时间:	15 s (默认为 15)

文件大小: 2.83 KB 点击打开抓包文件

Target IP address: 59.173.XX.XX
Using interface: eth0 [220.249.XX.XX]

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20 packets captured
20 packets received by filter
0 packets dropped by kernel

图 44.14. 总部抓包测试

请输入 IP 地址: 开始 重置 清除

参数:

接口:	WAN-1 (eth0/ppp0/59.173.XX.XX/255.255.255.255)
协议类型:	ALL
端口:	0
数据包个数:	10 (10~1000, 默认为 50)
等待超时时间:	15 s (默认为 15)

文件大小: 1.34 KB 点击打开抓包文件

Target IP address: 220.249.XX.XX
Using interface: eth0 [59.173.XX.XX]

tcpdump: listening on ppp0, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel

图 44.15. 分公司抓包测试

将抓包的文件用sniffer软件来打开，会发现传输的数据都经过了ESP协议加密。

Source	Destination	Protocol	Info
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)
59.173.XX.XX	220.249.XX.XX	ESP	ESP (SPI=0x025b142e)

图 44.16. 总部抓包数据

Source	Destination	Protocol	Info
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)
220.249.XX.XX	59.173.XX.XX	ESP	ESP (SPI=0x0aa6f82d)

图 44.17. 分公司抓包数据

此时在路由两端建立好了VPN隧道，进入“服务应用”->“IPSec VPN 服务”，隧道状态页面里有SA（安全联盟）和SP（安全策略）的详细信息。

☒ 启用 IPsec VPN 服务

隧道列表

隧道状态

SA 列表信息

ID	本地IP	远程IP	建立时间	存活时间	SPI	加密算法	验证算法
1	59.173.XX.XX	220.249.XX.XX	Aug 20 08:53:51 2010	Aug 20 09:21:12 2010	39523374	3des-cbc	hmac-sha1
2	220.249.XX.XX	59.173.XX.XX	Aug 20 08:53:51 2010	Aug 20 09:21:12 2010	178714669	3des-cbc	hmac-sha1

SP 列表信息

ID	隧道	数据流向	建立时间	存活时间
1	59.173.XX.XX-220.249.XX.XX	192.168.101.0/24 => 192.168.1.0/24	Aug 20 08:52:24 2010	
2	220.249.XX.XX-59.173.XX.XX	192.168.1.0/24 => 192.168.101.0/24	Aug 20 08:52:24 2010	Aug 20 09:21:12 2010

图 44.18. 隧道状态

经过 IPsec VPN 加密后的数据都经过了ESP封装，只有到达目的路由后才能够解封装，即使在互联网上此数据被劫也无法破解。在局域网两端交换的任何数据都会自动加上这层封装来保证通信的安全。



44.5. 与其它设备建立IPSec VPN

44.5.1. 与天融信网络卫士防火墙建立IPSec VPN

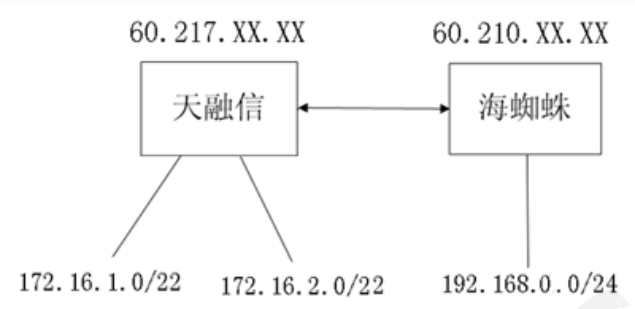


图 44.19. 网络结构

1. 首先设置天融信的虚接口绑定:

虚接口绑定 [添加]					
虚接口名	绑定接口名	绑定接口地址	通告IP地址	修改	删除
ipsec0	eth3	60.217.XX.XX	0.0.0.0		

图 44.20. 天融信的虚接口绑定

配置天融信的静态路由:

静态路由表 [添加] [清空]					
标记: U-Up, G-Gateway specified, L-Local, C-Connected, S-Static O-Ospf, R-Rip, B-Bgp, D-Dhcp, I-Ipsec, i-Interface specified					
目的	网关	标记	度量值	接口	删除
192.168.0.0/24	60.217.XX.XX	UGIi	100	ipsec0	

图 44.21. 天融信的静态路由

在海蜘蛛上也设置对应的静态路由:

<input checked="" type="checkbox"/> 启用静态路由功能								
ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	172.16.0.0/22	<input type="text"/> <input checked="" type="checkbox"/> 自动	WAN-1 (eth1/60.210.XX.XX)	1	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

图 44.22. 海蜘蛛静态路由设置

2. 接下来配置IPSec VPN，在天融信的静态隧道选项中，填入相同的共享密钥，本地标识和对方标识前加上"@"符号，IKE协商模式中野蛮模式对应海蜘蛛里的Aggressive模式，IPSec链路选择刚设定的虚接口绑定ipsec0，如下图：

第一阶段协商

第二阶段协商

隧道名：

sdsd-zbdc

*

认证方式：

预共享密钥

预共享密钥：

●●●●●●

*[最多输入63个字符]

本地标识：

@sdsd

[填写格式：@XXX或者XXX@XXX, XXX为字母或者数字]

对方标识：

@zbdc

[填写格式：@XXX或者XXX@XXX, XXX为字母或者数字]

对方地址或域名：

60.210.XX.XX

*

☒高级配置

隧道描述：

IKE协商模式：

野蛮模式

选择IPSEC链路：

ipsec0

主动发起隧道协商：

是

SA协商重试次数：

3

[范围：1~100, 缺省：3]

ISAKMP-SA存活时间：

86400

[单位：s, 最大：86400, 缺省：86400]

ISAKMP-SA的安全策略属性：

3des-sha1-modp1024

<-

3DES

-

SHA1

-

DH1

第一阶段协商

第二阶段协商

本地子网：

172.16.0.0

本地掩码：

255.255.252.0

对方子网：

192.168.0.0

对方掩码：

255.255.255.0

☒高级配置

IPSEC-SA存活时间：

28800

[单位：s, 最大：86400, 缺省：28800]

ESP的算法提议列表：

加密算法

3DES

校验算法

SHA1

IPSEC-SA的安全策略属性：

☐完美向前加密☒隧道模式☐压缩☒ESP☐AH

DPD间隔：

30

[单位：s, 范围：1~3600, 缺省：30]

DPD超时时间：

300

[单位：s, 范围：1~28800, 缺省：300]

DPD失败隧道操作：

clear

[缺省：clear]

度量值：

100

☐启用GRE隧道关联

启用：

☐扩展认证☐扩展认证/模式配置

海蜘蛛路由根据天融信的配置来做相应设置，标识与局域网设置与天融信的设置对调，其中DH算法为了和对方路由的modp1024保持一致而选择DH-2。

名称:	sdsc-zbssc	(只能由字母、数字、
本地IP:	WAN-1 (eth1/eth1/60.210.XX.XX/255.255.255.252)	
远程IP:	60.217.XX.XX	
本地标识:	zbssc	
对方标识:	sdsc	
本地局域网:	192.168.0.0/24	
远程局域网:	172.16.0.0/22	
模式:	<input checked="" type="radio"/> Aggressive (默认) <input type="radio"/> Main <input type="radio"/> Base	
DH 算法:	DH-2 (modp1024, 默认)	与对方路由一致
哈希算法:	SHA1 (默认)	
验证算法:	HMAC_SHA1 (默认)	
Phase 1 加密算法:	3DES (默认)	
Phase 2 加密算法:	3DES (默认)	
共享密钥:	talent	
SA 生存期:	86400	s
DPD 检测间隔:	30	s (5~120)
其他参数:	<input checked="" type="checkbox"/> 启用调试	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	
备注:	-	

图 44.23. 海蜘蛛端路由配置IPSec VPN

3. 最后做NO NAT设置，进入天融信地址子网页面，设置添加子网。

子网						[添加] [清空]
名称	IP地址	掩码地址	除去地址	修改	删除	
sub_intranet	172.16.1.0	255.255.252.0			-	
sub_ssn	172.16.2.0	255.255.252.0			-	
sub_192.168.0.0	192.168.0.0	255.255.255.0			-	

图 44.24. 天融信路由添加子网

再进入天融信地址转换选项，对刚设置的子网设置不做地址转换。

ID	类型	源	目的	服务	转换	修改	复制	移动	插入	删除	状态
8150	不作转换	地址: sub_intranet sub_ssn sub_192.168.0.0	地址: sub_intranet sub_ssn sub_192.168.0.0								

图 44.25. 天融信设置不做地址转换

在海蜘蛛路由上也设置对应的NO NAT。

名称:	<input type="text" value="192to172"/>	(只能由字母、数字、汉字、下划线、圆点及减号组成)
优先级:	<input type="text" value="1"/>	(只能为数字, 数字越小优先级越高)
源IP:	<input type="text" value="192.168.0.0/24"/>	
目的IP:	<input type="text" value="172.16.0.0/22"/>	
备注:	<input type="text"/>	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 44.26. 海蜘蛛路由设置NO NAT





第 45 章 智能 QoS 模块

这里我们先介绍一下优先级的问题，例如现网络中有6种应用需求：VPN、视频、文字、未识别应用、P2P下载、图片，在网络使用中，路由系统会按照默认的优先级来对应用排序，如下图：

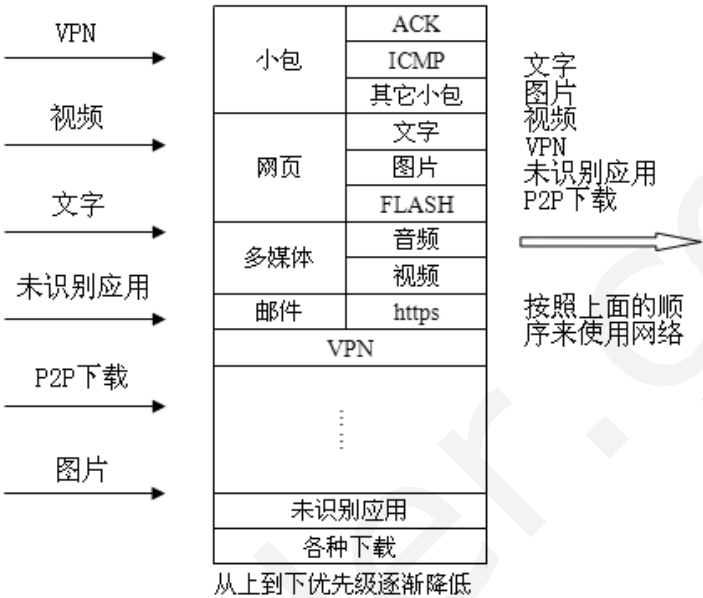


图 45.1. 优先级

根据此设定的优先级顺序，在路由系统中会按照文字、图片、视频、VPN、未识别应用、P2P下载的顺序来控制其占用网络资源。这样一些特别占网络资源的应用就不会影响到网络的常规使用。

在路由系统的主页面进入“流量控制”->“智能 QoS”，进入运行参数页面：

☒ 启用智能 QoS 流量限速

总上行带宽最大使用率：	<input type="text" value="85%"/> (60~90%)	100000KBit => 10625 KB/s
总下行带宽最大使用率：	<input type="text" value="95%"/> (75~95%)	100000KBit => 11875 KB/s
启用下载智能识别限制：	<input checked="" type="checkbox"/> 是 (检测到IP在进行下载时自动将其放入下载队列)	
P2P/大文件HTTP下载总带宽：	<input type="text" value="10%"/> (10~15%)	10000KBit => 1250 KB/s
未识别应用总带宽：	<input type="text" value="30%"/> (20~30%)	30000KBit => 3750 KB/s
单机初始分配的上传带宽：	<input type="text" value="20"/> KB/s	
单机初始分配的下行带宽：	<input type="text" value="60"/> KB/s	

图 45.2. 智能QoS设置

使用QoS时先勾选“启用智能QoS流量限速”。这里我们设置的都为默认值，您可以根据自行需要进行调整。

- 总上行带宽最大使用率这里设为85%，如果设置过大则会影响下行速度。例如普通家用2M的ADSL宽带，上行最大为40-50K，下行最大

为250K，如果在运用中上行达到最大值则下行速度可能会很小，这样会影响网络的利用率。

- 总下行带宽最大使用率这里设为**95%**，同理如果设置过大则会影响上行速度。
- 启用下载智能识别限制与下面的**P2P/大文件HTTP**下载总带宽是合在一起使用的。当启用下载智能识别限制时，路由系统检测到有任何**IP**在进行**P2P**下载或大文件的**HTTP**下载，则会自动将其分配到最低优先级来使用网络资源，并且会给这组用户自动添加一个占下载总带宽的上限如这里设置的**10%**，这样就使得即使网络中有大量下载也不会影响到网络的正常应用。
- 未识别应用总带宽指的是非常规的网络应用，这些应用的优先级都是低于常规的网页、图片等操作，给这些未识别操作加上带宽限制也防止了其大量占用网络资源。
- 单机初始分配的上传带宽和下载带宽分别指为刚入网的客户机分配的上行速率为**20K**和下行速率为**60K**。

这两个值会根据各客户机入网后的使用情况不断地变化，如图所示：

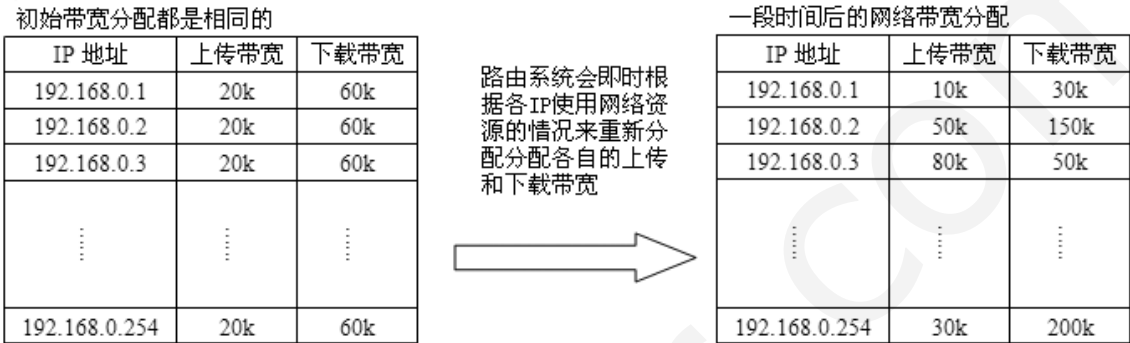


图 45.3. 带宽分配

在**QoS**白名单内可以添加例外的**IP**地址来进行单独限速，如图：

ID	优先级	IP地址	上传速度	下载速度	备注	激活	删除
1	<input type="text" value="1"/>	<input type="text" value="192.168.10.10"/>	<input type="text" value="100"/> KB/s	<input type="text" value="300"/> KB/s	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

图 45.4. QoS白名单

启用智能**QoS**流量限速后，您可以在 状态 页面下随时查看当前网内的各种应用分布及流量情况：

ID	类型	累计包	累计字节
1	网页文字	5029	2045K
2	图片	1516	1013K
3	Flash动画	1535	1350K
4	音频播放	26	24424
5	视频播放	5120	2002K
6	下载	191	159K
7	HTTP加密传输	567	211K
8	VPN	0	0

图 45.5. 智能QoS查看

第 46 章 安全流控模块

目录

- [46.1. 安全流控简介](#)
- [46.2. 安全流控配置](#)
- [46.3. 安全流控的升级](#)
- [46.4. 安全流控的部署](#)

- [46.4.1. 万象2004版+易游有盘整合版安装部署](#)
- [46.4.2. PUBWIN2007+易游有盘整合版安装部署](#)
- [46.4.3. 顺网无盘安装部署](#)
- [46.4.4. 易游无盘安装部署](#)
- [46.4.5. 信佑无盘安装部署](#)

46.1. 安全流控简介

安全流控模块是集上网流量控制与安全防护于一体，能够将各种网络应用分级处理，按网页、游戏、通讯、视频、下载的基本顺序进行排列处理带宽，以保证即时性需求高的应用得到带宽保障。主要用于在网络资源有限的情况下，更合理地调整带宽分配。

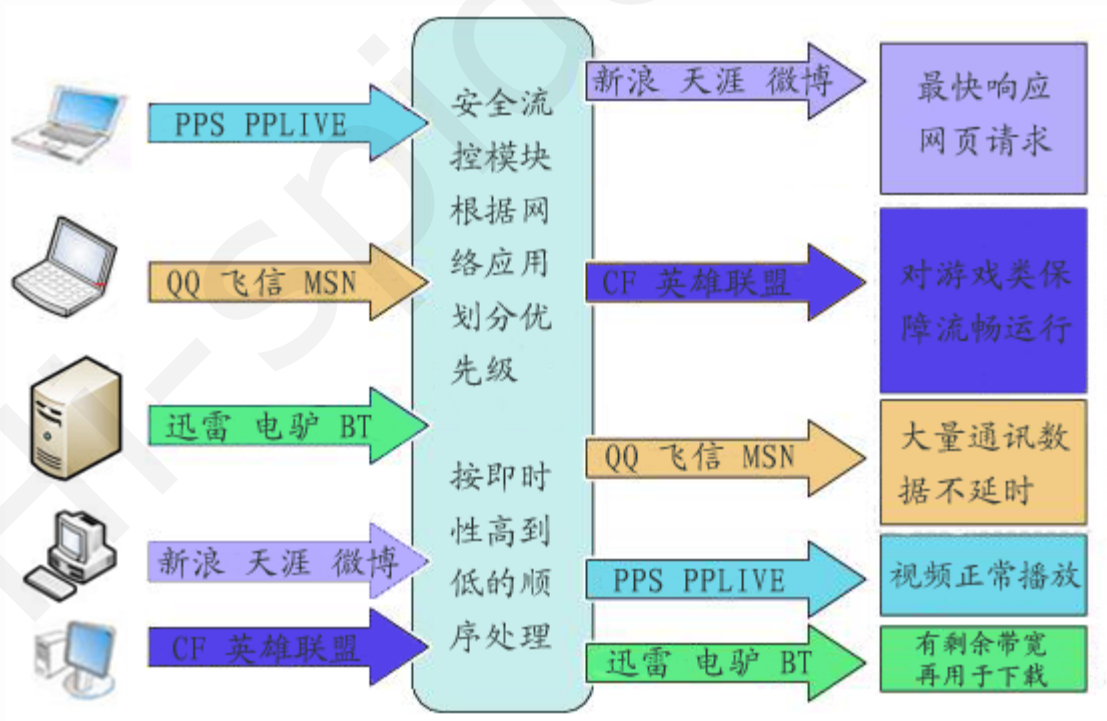


图 46.1. 带宽分配图例



Hi-Spider.com

46.2. 安全流控配置
第 46 章 安全流控模块

46.2. 安全流控配置

首先登陆路由Web管理系统主界面，查看路由上面的版本号，只有Build20120331以后的版本才能安装使用此功能。
接着配置准确WAN口带宽，进入网络设置-广域网（WAN）选项，在每个WAN口的标签页下修改准确各自的带宽：

带宽：下行：2 Mbit 上行：2 Mbit ☐ 限制总下行 ☐ 限制总上行 确定

图 46.2. 配置WAN口带宽



提示

上面图例是2M固定单光纤接入，如果是2M的ADSL，下载设置2M，上传需调整为512K。

登录路由的Web主页面，进入“流量控制”->“安全流控”，选启用安全流控和下面的强制安全流控客户端：

运行参数 推送页面 在线客户端

当前所有WAN口总带宽为：上行 2Mbit, 下行 2Mbit, 如果和实际情况不符，请在 [\[WAN口配置\]](#) 修改，以免影响流控效果。

☒ 启用安全流控 (当前特征库版本：2.3.5, 最后更新于 2012-03-30 13:40:53)

上行带宽使用率：	85% (60~90%) 2000KBit => 212 KB/s
下行带宽使用率：	95% (75~95%) 2000KBit => 237 KB/s
未识别应用带宽使用率：	30% (20~30%) 63/71 KB/s
白名单带宽使用率：	30% (30~50%) 75/75 KB/s
白名单IP上传带宽：	20 ~ 50 KB/s
白名单IP下载带宽：	60 ~ 100 KB/s
强制使用安全流控客户端：	<input checked="" type="checkbox"/> 是
IP白名单 (不安装客户端也可上网)：	192.168.0.10

图 46.3. 安全流控配置页面

总上行带宽最大使用率这里设为**85%**，如果设置过大则会影响下行速度。例如普通家用**2M**的**ADSL**宽带，上行最大为**40-50K**，下行最大为**250K**，如果在运用中上行达到最大值则下行速度可能会很小，这样会影响网络的利用率。

总下行带宽最大使用率这里设为**95%**，同理如果设置过大则会影响上行速度。

未识别应用带宽使用率指现有**sqos**特征库里未识别的网络应用程序所占的总带宽。有些网络应用或新出的网络应用都未包含在这里面。初始时此百分率可以设置大点，如果发现网络应用更卡再调小此值。未识别的网络应用是所有网络应用程序里响应最慢的。

白名单带宽使用率指启用强制安全流控客户端后，下面的**IP**白名单中不安装安全流控客户端的用户所占整个网络带宽的总比值。白名单带宽为弹性带宽，当白名单用户不使用网络时，流控客户端用户都可以使用这部分带宽。白名单带宽不宜设置过大。

白名单**IP**上传带宽和下载带宽是指不安装安全流控客户端的用户每个单机上传或下载的速度限制范围。

强制使用安全流控客户端指强制内网所有用户都安装安全流控客户端，如没有安装安全流控又不在流控白名单的主机将无法上网，并且会自动推送相应的页面提醒。

最下面的**IP**白名单如这里**192.168.0.10**这个主机，即使整个内网都部署了安全流控，这个**IP**的主机不安装流控客户端的也能正常访问外网。白名单格式目前仅支持单**IP**形式(如 **192.168.0.10**)，每个**IP**占一行。



重要

如果启用安全流控而没有强制安全流控客户端，那么内网未装流控的客户机会慢于安装了流控的客户机。并且这些未安装流控客户机的总带宽仅为未识别应用带宽使用率的带宽比值。

例如**2M**带宽，未识别应用带宽使用率为**30%**，那么未安装流控的客户机带宽就是相当于共享一个**600K**的带宽。

安全流控客户端启用后，手动限速规则页面里面的配置将自动失效。

点击推送页面标签页，点击默认按钮，在此基础上修改您需要发布的提示页面：

运行参数

推送页面

在线客户端

提示标题:	<div>请安装安全流控客户端</div> <div>(显示在浏览器标题栏)</div>
提示内容:	<div>您好！</div> <div>为进一步优化宽带网络、提升上网体验,您需要安装“安全流控客户端”,如果您已经安装过,请保持该程序处于运行状态。</div> <div>客户端下载地址: [tools][点击下载] [/tools]</div> <div>如果您有什么疑问,请与网络管理员联系,感谢您的支持！</div>
管理签名信息:	<div>XX网络管理中心 QQ: 123456, Tel: 123456</div> <div>(显示在提示框右下角)</div>

保存设置

默认

页面预览

图 46.4. 流控推送页面配置

下面未安装流控的客户机在打开任意一个网页时会自动出现相关的提示:

请安装安全流控客户端

您好！

为进一步优化宽带网络、提升上网体验,您需要安装“安全流控客户端”,如果您已经安装过,请保持该程序处于运行状态。

客户端下载地址: [\[点击下载\]](#)

如果您有什么疑问,请与网络管理员联系,感谢您的支持！

--- xx网络管理中心 QQ: 123456, Tel: 1234567

图 46.5. 流控推送页面

对于已经安装了流控客户端的主机,可以点击在线客户端页面进行查看:

运行参数		推送页面		在线客户端			
ID	IP地址				更新时间		
1	192.168.100.94				2012-04-01 14:07:42		
2	192.168.100.115				2012-04-01 14:07:55		
3	192.168.100.119				2012-04-01 14:07:44		
4	192.168.100.162				2012-04-01 14:07:55		

图 46.6. 查看在线客户端



46.3. 安全流控的升级

第 46 章 安全流控模块



46.3. 安全流控的升级

登录路由Web页面后，进入产品中心->扩展模块，在 sqos 安全流控后面选择自动更新或点击后面的检查更新：

8	sqos	安全流控	1.4.8	2012-03-31 16:10:35	548.63 KB	1.74 MB	永久	<input checked="" type="checkbox"/>	检查更新		
---	------	------	-------	---------------------	-----------	---------	----	-------------------------------------	------	--	--

图 46.7. 安全流控服务端更新

接着进行特征库更新，进入产品中心->特征库更新，在 sqos 安全流控特征库后面选择自动更新或点击后面的检查更新：

6	sqos	安全流控特征库	2.3.7	2012-03-31 11:39:24				<input checked="" type="checkbox"/>	检查更新
---	------	---------	-------	---------------------	--	--	--	-------------------------------------	------

图 46.8. 安全流控服务端更新



提示

有些网络应用程序可能不在安全流控控制范围内，如果您发现请联系官方的客服人员，研发人员会针对这些网络应用程序进行调整更新。



46.2. 安全流控配置

46.4. 安全流控的部署

46.4. 安全流控的部署



重要

目前测试成功的网吧平台有易游有盘，顺网/易游/信佑无盘，其它网吧平台处于测试阶段。

46.4.1. 万象2004版+易游有盘整合版安装部署

把安全流控安装包放到易游服务端数据文件夹(路径如下：`*:\UserData$\Globalconfig`)



图 46.9. 复制安装包

在此文件夹下新建一个批处理文件system.bat



图 46.10. 新建启动项

右键打开用记事本编写这个批处理文件，写入如下脚本：

```
start /wait D:\Sysset\Menu\qos.exe
ping 127.0.0.1 -n 125
start C:\hiqos\hiqos.exe
```

保存后即可，客户机开机首次需启动两次方可正常加载hiqos

46.4.2. PUBWIN2007+ 易游有盘整合版安装部署

把安全流控客户端海盾II程序放到易游服务端数据文件夹。(如: *:\UserData\$\Globalconfig)



图 46.11. 复制安装包

打开易游网娱平台管理更新服务端，进入参数设置-开机启动项，在程序文件一栏填海盾II的软件路径(如: *:\UserData\$\Globalconfig\qos.exe),启动说明处填相关说明(如海蜘蛛海盾)，点击添加保存

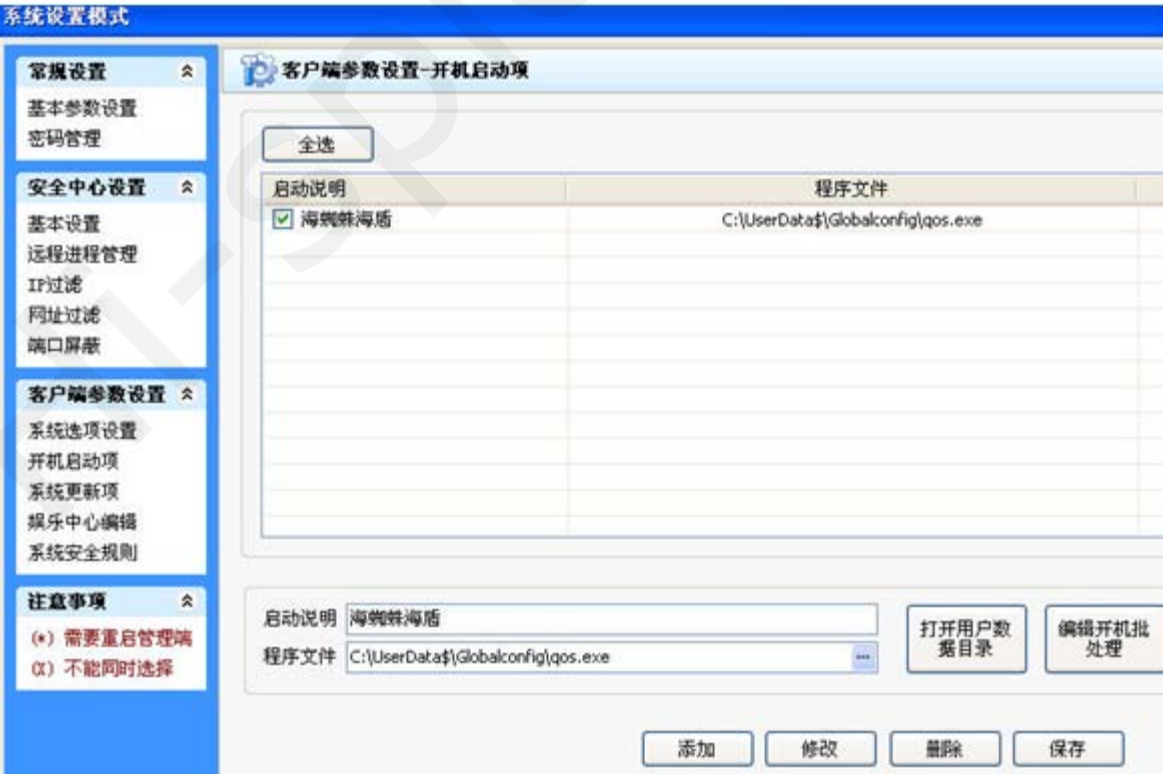


图 46.12. 添加启动项

这样客户机开机后就会自动下载并在后台运行安装，运行后会在右下角出现海盾II的小图标，说明部署正常



图 46.13. 启动图标

46.4.3. 顺网无盘安装部署

先在任意一客户机安装源硬盘母盘，选择硬盘启动，将sqos安装版文件复制到此主机上，双击运行hiqos.exe，会有短暂的安装界面闪过



图 46.14. 复制sqos

安装完毕后，系统右下角会自动生成一个图标



图 46.15. 启动图标

将桌面的hiqos.exe安装文件删除，再次进入网维大师-系统虚拟盘客户端工具，提示输入超管密码

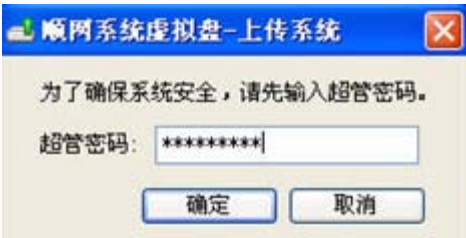


图 46.16. 超管密码

输入超管密码，新建镜像



图 46.17. 超管密码

点击确定，开始上传。

客户端镜像上传完毕后，在网维大师服务端里开启网维大师系统虚拟盘控制台，进入客户机管理，对要运行流控的主机点击右键-修改



图 46.18. 修改客户机

在修改页面内将系统镜像选择刚上传的system2_hiqos 确定保存



图 46.19. 修改客户端镜像

主机重新启动后即自动加载安全流控客户端

46.4.4. 易游无盘安装部署

先在易游服务端新建一个启动盘



图 46.20. 新建启动盘

在任意客户机安装源硬盘母盘，在服务机上将此主机设为超级工作站



图 46.21. 设超级工作站

然后再双击设置客户机信息



图 46.22. 设置客户机信息

接着将系统启动磁盘菜单第一系统的系统启动磁盘选择刚创建的启动盘



图 46.23. 设置启动盘

安装源硬盘母盘的客户机开机选择硬盘启动，在服务端将sqos安装版文件复制到此主机上，双击运行hiqos.exe，会有短暂的安装界面闪过



图 46.24. 复制sqos

安装完毕后，系统右下角会自动生成一个图标



图 46.25. 运行图标

将此镜像上传至服务端，进入程序-易游网娱平台-无盘上传，先安装必要驱动



图 46.26. 安装必要驱动

接着进入连接服务器标签，点击“连接”



图 46.27. 连接服务器

再选择上传系统标签，勾选完全上传，选择目标分区，点击开始上传



图 46.28. 上传镜像

上传完毕后，关闭客户机，拔下硬盘。易游服务端将此主机取消超级工作站，将所有客户机设置成此镜像启动。进入易游网娱平台，点击参数设置



图 46.29. 平台参数设置

点击左边栏的开机启动项，然后点击右下角的编辑开机批处理

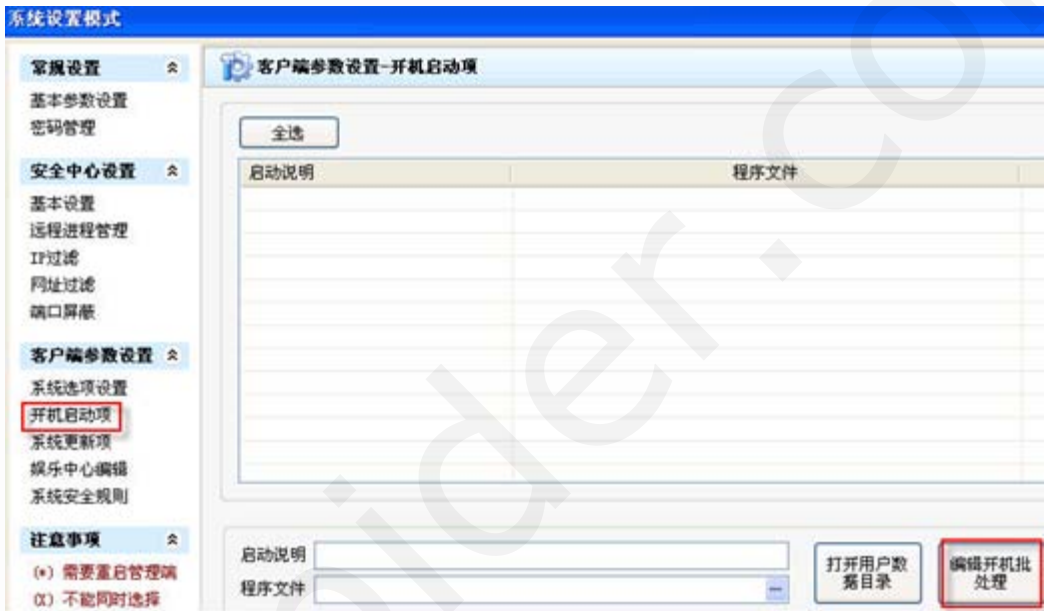


图 46.30. 编辑批处理

在记事本里输入如下两排

```
ping 127.0.0.1 -n 5
C:\hiqos\HiQos.exe
```

保存后，客户机无盘启动即可自动加载新的安全流控系统

46.4.5. 信佑无盘安装部署

信佑无盘可以随意设置一个客户机为超管部署，进入信佑管理服务器界面，点击基本管理标签，选择需要做超管的主机，鼠标右键选择“无盘超级工作站”，此客户机重启后即进入超管，超管主机会自动标红：



图 46.31. 设置超管

在超管主机上运行sqos



图 46.32. 运行sqos

双击运行一个注册文件 [Hispider.reg](#) 即可

最后再服务端添加一个开机自启动命令。进入任务管理-常规任务，点击增加，添加一个任务名称，将过期时间选择不过期，机器分组选择默认组所有，下面的路径填写C:\hiqos\HiQos.exe 保存确定后客户端即可自启动运行安全流控。



第 47 章 第四代流控

首先安装扩展模块，安装方法参照 [此链接](#)

安装完毕后，先进入网络设置->广域网（WAN），将WAN口带宽改成实际值并按此值限制总上下行：

带宽：

下行：

Mbit

上行：

Mbit

☒ 限制总下行

☒ 限制总上行

确定

图 47.1. 设置WAN口上下行带宽

如果是多线配置需要将每个WAN口都按照实际值进行配置，双线、多线、多运营商的具体配置方法参照 [此链接](#)，配置完毕后进入网络设置->多线负载及策略中开启并激活各线路

☒ 启用多线负载及策略

线路设置...

策略路由工作模式：

正常模式、掉线自动切换

☐ 所有数据全部走策略线路（仅用于VPN借线）

默认线路：所有不符合策略的数据将全部走默认线路。策略线路：如果用户访问的IP在策略线路对应的ISP路由表中，则走此线路。默认线路和策略线路可以是一条或者多条。同一ISP应选择同一线路类型。

线路	ISP	连接状态（网卡/设备名/IP/子网掩码）	线路类型	使用路由表	激活
WAN2	中国电信	eth3/ppp0/ <div></div> /255.255.255.255	<div>默认线路</div>	中国电信（1974 条 v3.3.4）	<input checked="" type="checkbox"/> 是
WAN3	中国电信	eth4/ppp1/ <div></div> /255.255.255.255	<div>默认线路</div>	中国电信（1974 条 v3.3.4）	<input checked="" type="checkbox"/> 是
WAN1	中国联通	eth2/eth2/ <div></div> /255.255.255.224	<div>策略线路-1</div>	中国联通（654 条 v3.7.5）	<input checked="" type="checkbox"/> 是

保存设置

重置

图 47.2. 开启多线负载

确定后进入流量控制->安全流控，如下图：

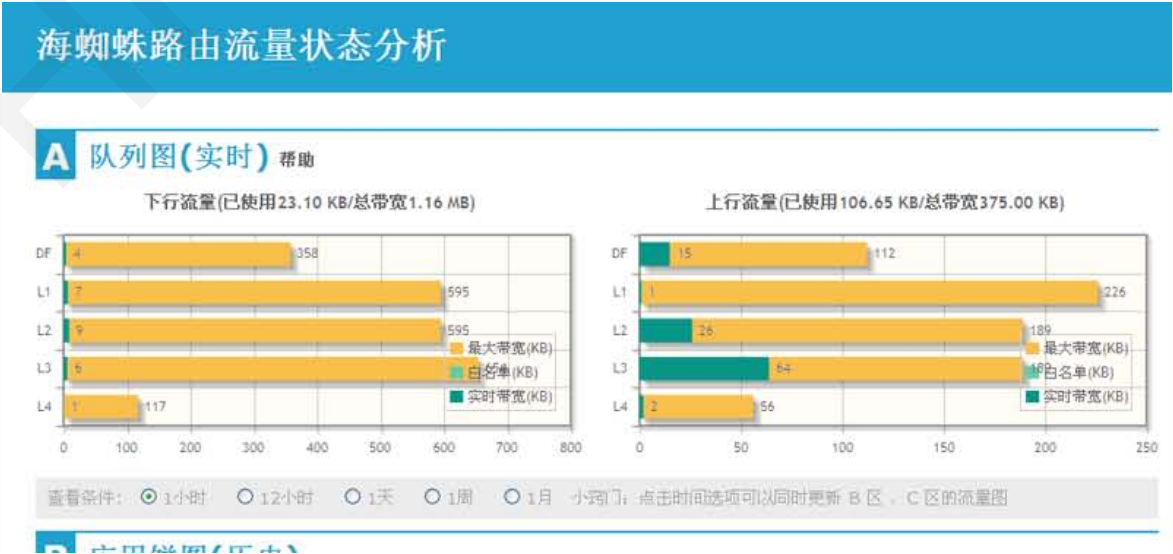


图 47.3. 第四代qos配置主页

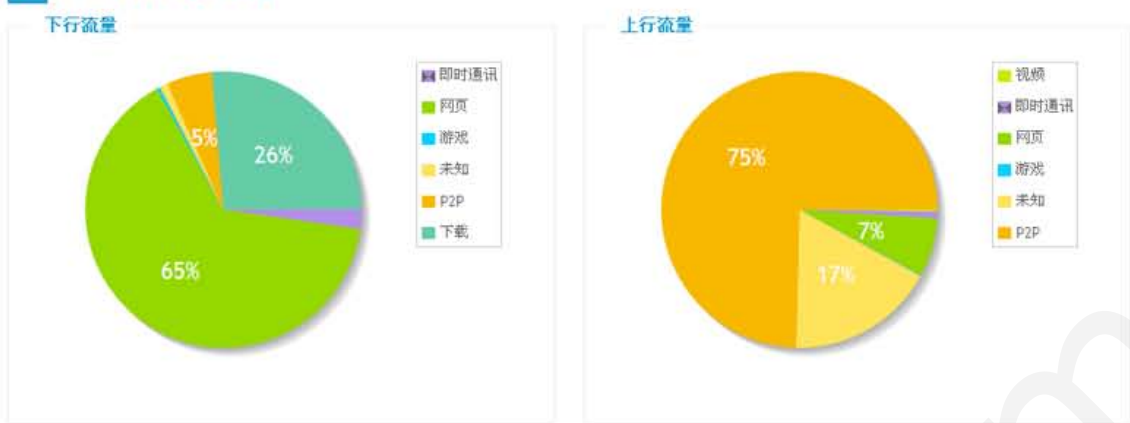
启用成功后, 如果硬件符合要求会显示 驱动加载成功

流控的网卡对象一般都选择所有的内外线路, 勾选出所有外线之后, 系统会根据线路叠加自动算出外线的上行可用总带宽和下行可用总带宽。

工作模式有两种选择: 流控模式和分析模式。流控模式包括各种网络应用类型的识别、分析实时图队列及记录并统计历史各网络应用饼图、各类型网络应用流量控制。而分析模式仅包括各种网络应用识别和分析统计, 不含控制网络应用。这两种模式都可以在下面的 流量状态分析 里查看到实时与历史相关信息。



B 应用饼图(历史)



C 应用线型图(历史)

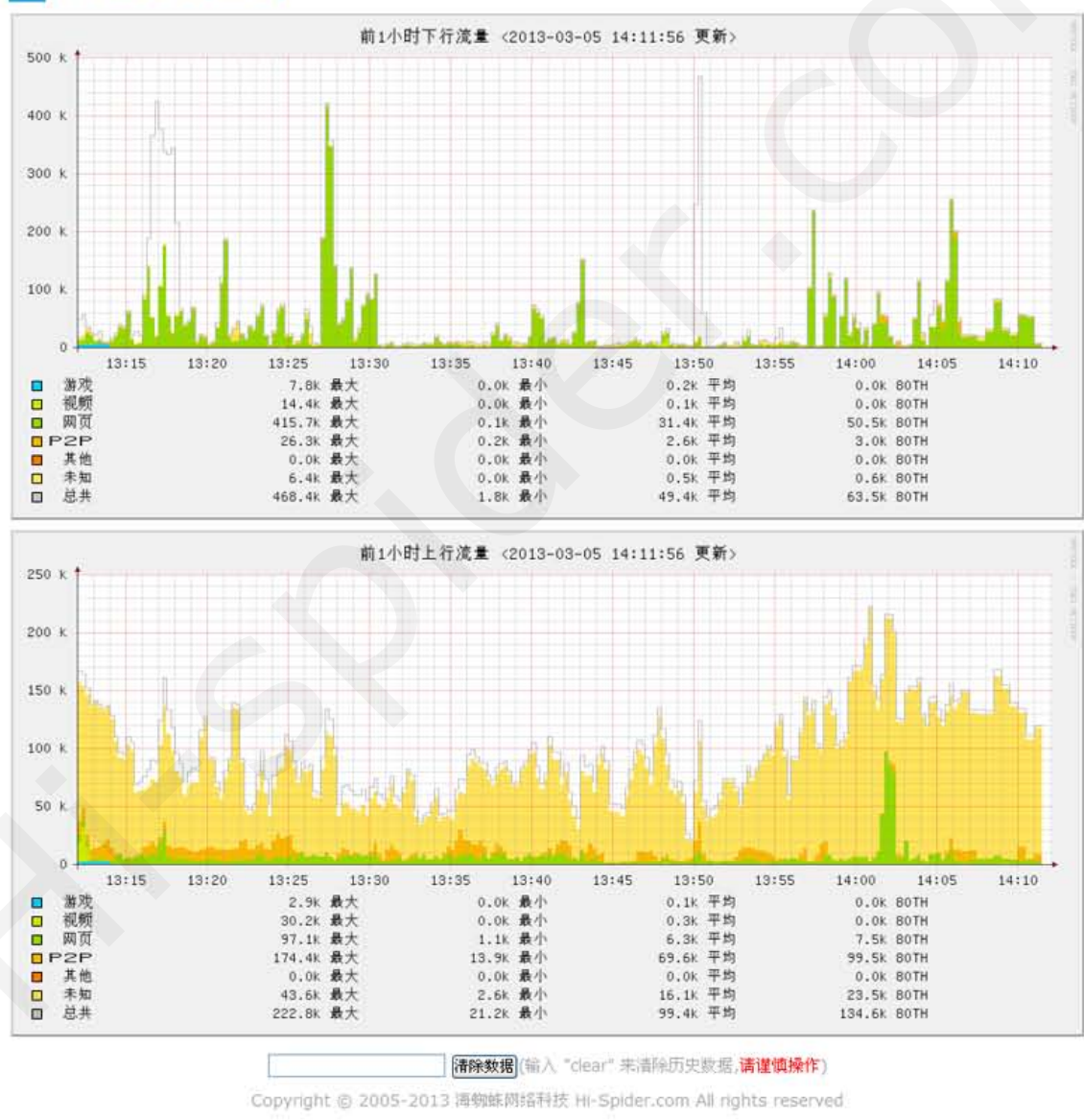


图 47.4. 流量状态分析

未识别应用带宽使用率指路由上未加入特征库的网络应用，例如一些偏门游戏或新的网络软件，在还未加入特征库前都为未识别应用。一定要保留一部分带宽给这些未识别的网络应用。安全流控中默认对未识别应用保留30%的带宽，对这部分未识别的网络应用实行单独走线，不影响已识别网络应用的转发速率。这部分带宽使用率配置过小会影响新的网络应用程序运行速度，配置过大会影响已识别网络应用的转发速度。对于路由下面上网用户类型混杂，更新网络应用较多或者P2P应用较多的情况下，建议适当增加此带宽使用率的值。

qos流控默认是针对路由下固定IP和DHCP用户客户端，如果流控要包含PPPoE拨号客户端，勾选针对PPPoE用户使用安全流控即可，勾选后对于PPPoE客户来说既有帐

号限速效果也有qos流控限速效果。

流控白名单列表及其限速值针对不受qos管控的IP，内网白名单列表填写从内网访问外网不受限的主机IP，如这里内网的192.168.10.54这台主机就不受qos的流控限制，并且能够优先保证至少50k上行，至少100k下行的带宽。外网白名单每IP速度指所有外网访问某一特定网站不受控，例如这里202.24.103.58是个ERP服务器，所有路由下的主机访问这个服务器都不受流控的限制



提示

当启动安全流控后显示 驱动加载成功，这时最好重启一次路由，让整个硬件驱动重新复位一次以达到最好的流控效果。



队列图说明

DEFAULT:未识别流量 L1:游戏 L2:IM/股票软件 L3:网页视频/网页 L4:P2P下载/视频客户端

流控会将些常见的小网络应用如网页游戏等优先，而将P2P视频下载等大流量应用滞后响应。

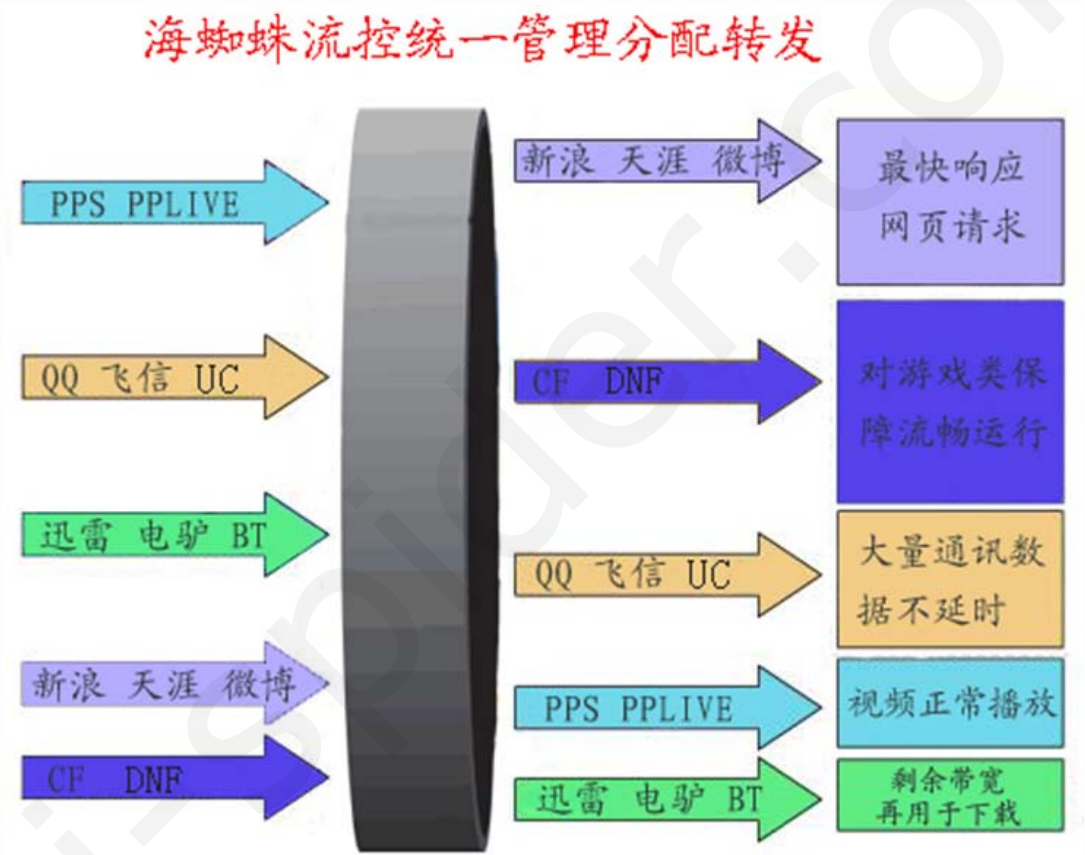


图 47.5. 第四代QoS效果简图



重要

流控模块必须在海蜘蛛路由20130319以后的版本上运行，路由内核版本必须为2012-03-09以后的版本，路由内核必须以单核或者多核模式运行，内存至少需要512M以上。



第 48 章 ipgeodbs (IP地理位置数据库) 模块

部分 VIII. 扩展模块



第 48 章 ipgeodbs (IP地理位置数据库) 模块

名称: ipgeodbs

功能: IP地理位置数据库, 需查询IP地址归属地时安装。安装后在“信息监测”->“NAT 信息监测”中可查看IP地理位置, “系统工具”->“IP 归属地查询”, 如下图所示:

总上传流量 (Byte)	总下载流量 (Byte)	IP地理位置
47.6K	98.9K	局域网
13.1K	14.3K	湖北省武汉市 电信
22.5K	54.5K	湖北省武汉市 电信

图 48.1. IP地理位置1

目的IP	IP地理位置
59.175.24.38	湖北省武汉市 电信
59.175.24.38	湖北省武汉市 电信
59.175.24.38	湖北省武汉市 电信

图 48.2. IP地理位置2

请输入您要查询的 IP 地址或域名:

已安装IP地理位置数据库, 更新日期: 2010-05-05

202.103.24.68

开始

查询结果:

湖北省武汉市 电信

图 48.3. IP归属地查询



第 49 章 npnp 即插即用服务



图 49.1. 海蜘蛛路由行业版

Web登录海蜘蛛路由后，在服务应用->即插即用上网中，勾选此服务保存即可：

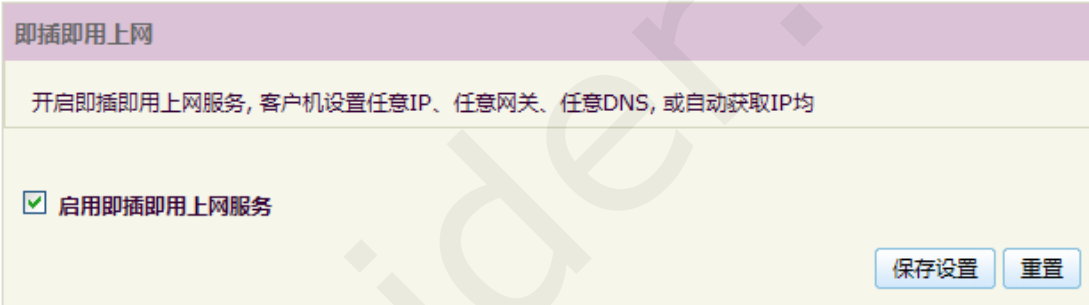


图 49.2. 即插即用上网服务

接着在服务应用->DNS代理解析中，勾选强制使用DNS代理：



图 49.3. 强制DNS代理解析

在实际应用中还需开启路由上的DHCP服务，进入服务应用->DHCP服务，打开DHCP服务，接着添加路由LAN口地址池：



<div>参数设置IP地址池固定IP分配当前IP分配信息</div>				
ID	接口	分配的IP地址段	子网掩码	网关
1	LAN1	192.168.0.2-192.168.0.200	255.255.255.0	192.168.0.1

配置好后，下面的用户各用户可以使用自动获取：

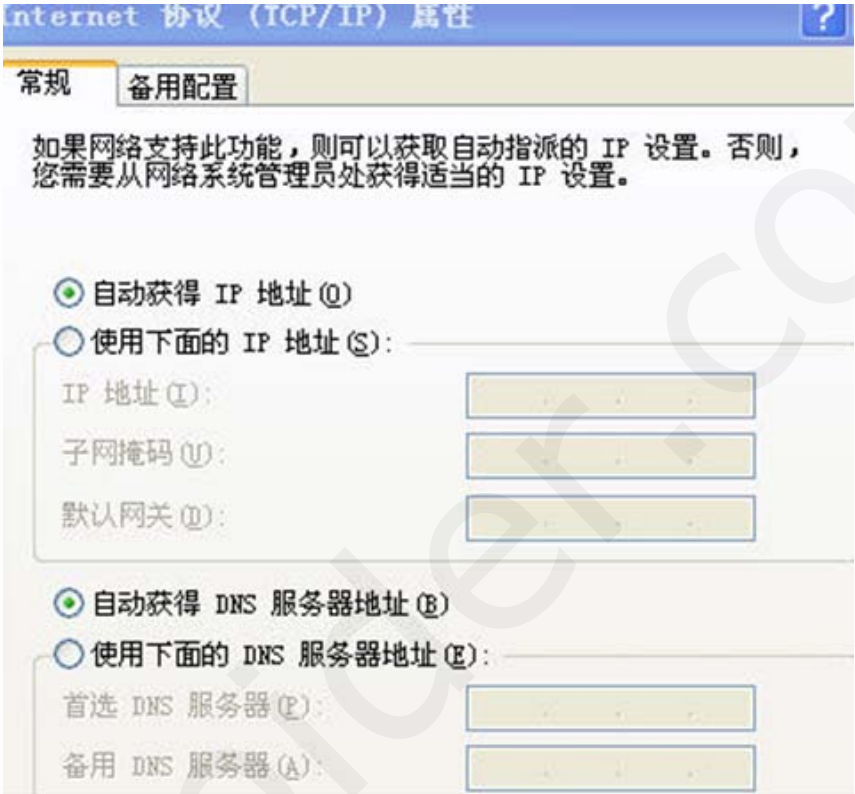


图 49.4. 客户机自动获取

也可以手动指定各固定IP，这里的IP要和网关同网段，下面的DNS可以任意：

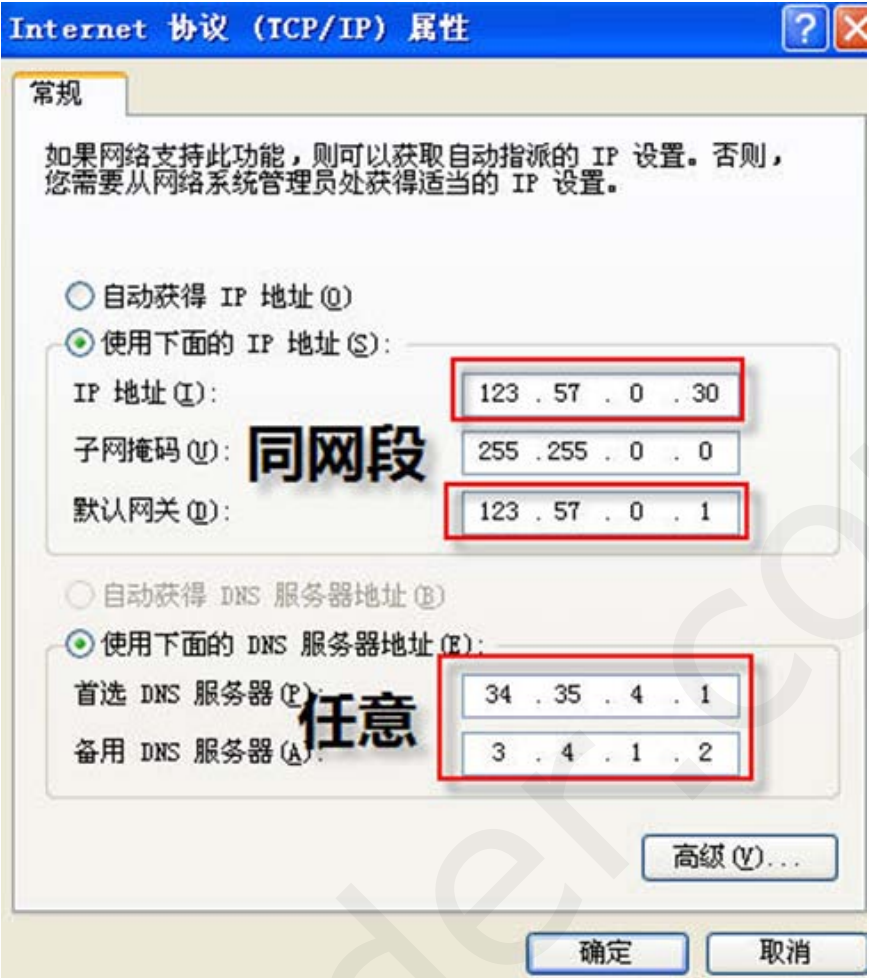


图 49.5. 客户机固定IP



重要

路由下面的网络设备不能有VLAN和二级路由，npnp信息无法穿透VLAN，对于二级路由也无法穿透，二级路由反接的DHCP也会影响到海蜘蛛上的DHCP





部分 IX. 解决方案

目录

[50. 企业三层交换网络解决方案](#)

[50.1. 路由上不划分VLAN](#)

[50.1.1. 路由器设置](#)

[50.1.2. 三层交换机设置](#)

[50.1.3. 常见问题及解答](#)

[51. 单WAN口通过交换机扩展接入多线路解决方案](#)

[51.1. 单WAN口通过交换机扩展接入多ADSL解决方案](#)

[51.1.1. 网络拓扑结构](#)

[51.1.2. 三层交换机上的配置](#)

[51.1.3. 路由上的配置](#)

[51.1.4. 采用支持VLAN的二层交换机](#)

[51.2. 单WAN口通过交换机扩展多个固定IP解决方案](#)

[51.2.1. 单WAN口通过交换机扩展接入同一ISP的多个固定IP](#)

[51.2.2. 单WAN口通过交换机扩展接入不同ISP的多个固定IP](#)

[52. 关于光纤接入的几种解决方案](#)

[52.1. 光纤接入绑定多个固定IP地址解决方案](#)

[52.1.1. 网络拓扑图](#)

[52.1.2. 路由器上的设置](#)

[52.2. 光纤接入绑定多个PPPoE账号解决方案](#)

[52.2.1. 网络拓扑图](#)

[52.2.2. 交换机设置](#)

[52.2.3. 路由器设置](#)

[53. 光纤接入无需交换机扩展多线路解决方案](#)

[53.1. 光纤接入绑定多个固定IP无交换机扩展解决方案](#)

[53.1.1. 网络拓扑图](#)

[53.1.2. 路由器上的设置](#)

[53.2. 光纤接入绑定多个PPPoE账号无交换机扩展解决方案](#)

- [53.2.1. 网络拓扑图](#)
- [53.2.2. 路由器设置](#)

[54. PPPoE 认证+web 认证+验证码的三重安全认证方案](#)

[54.1. PPPoE 服务器模式简介](#)

- [54.1.1. 三重安全认证的优点](#)
- [54.1.2. 网络拓扑图](#)

[54.2. PPPoE 拨号的设置](#)

[54.3. Web 认证设置和验证码](#)

[55. 路由无线局域网解决方案](#)

- [55.1. 路由无线局域网模式简介](#)
- [55.2. 建立内网网段](#)
- [55.3. 内网利用 PPPoE 服务 上网](#)
- [55.4. 内网利用 Web 认证上网](#)

[56. 主机电脑和手机平板设备分别认证解决方案](#)





第 50 章 企业三层交换网络解决方案

目录

[50.1. 路由上不划分VLAN](#)

- [50.1.1. 路由器设置](#)
- [50.1.2. 三层交换机设置](#)
- [50.1.3. 常见问题及解答](#)

网络拓扑图如下所示：

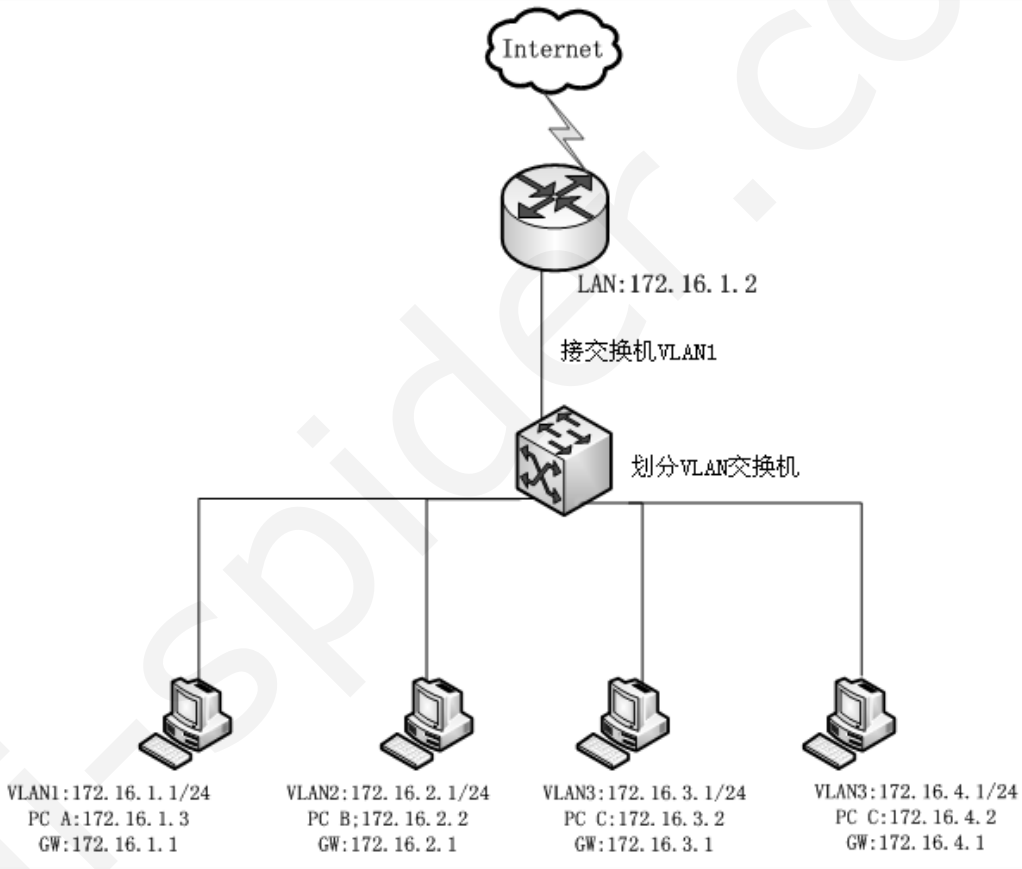


图 50.1. 网络拓扑图

由上图可知，现在交换机上划分四个VLAN，每个VLAN的接口地址如上图所示，现将交换机VLAN1接口与海蜘蛛路由LAN口相连，各VLAN通过VLAN1上网。

50.1. 路由上不划分VLAN

50.1.1. 路由器设置

1. 添加静态路由

“网络设置”->“静态路由”，添加静态路由如下图所示：

☒ 启用静态路由功能

ID	目的网络	出口网关	线路	跳数	VLAN_ID	备注	状态	删除
1	<input type="text" value="172.16.0.0/16"/>	<input type="text" value="172.16.1.1"/> <input type="checkbox"/> 自动	LAN-1 (eth2/172.16.1.2 <input type="button" value="v"/>)	<input type="text" value="1"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[\[专家模式\]](#) [\[导出规则\]](#)

[日志记录](#)

图 50.2. 启用静态路由

2. 为VLAN网络加入NAT上网支持

默认情况下，只有和路由局域网IP在同一网段的机器才能上网。进入“网络设置”->“局域网（LAN）”，在VLAN网络地址栏里添加三层交换上所划分的VLAN网络，如下：

IP地址:

子网掩码:

(默认)

[此网段可容纳 254 台机器]

扩展 IP地址:

IP地址:

子网掩码:

新增

删除

VLAN 网络地址:

172.16.2.0 / 255.255.255.0
172.16.3.0 / 255.255.255.0
172.16.4.0 / 255.255.255.0

网络地址:

子网掩码:

新增

删除

图 50.3. VLAN网络

此时，三层交换下的各VLAN网络里的客户机都可以通过路由联入互联网了。



注意

使用这种方法划分VLAN时，客户机的网关地址设置三层交换机上的VLAN接口IP地址。



重要

用此种方式划分内网VLAN，内网主机无论是否配置本地IP网关地址，都无法使用PPPoE拨号穿透三层交换机到路由。如果要PPPoE拨号穿透三层交换机，请参考在路由器上划分VLAN的解决方案参考 [路由上划分VLAN](#)

50.1.2. 三层交换机设置

这里以华为s3526c为例，配置如下：

```
#
vlan 1
#
vlan 2
#
vlan 3
#
vlan 4
#
interface Vlan-interface1
 ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface2
 ip address 172.16.2.1 255.255.255.0
#
interface Vlan-interface3
 ip address 172.16.3.1 255.255.255.0
#
interface Vlan-interface4
 ip address 172.16.4.1 255.255.255.0
#
interface Aux0/0
#
interface Ethernet0/1
 flow-control
#
interface Ethernet0/2
 flow-control
#
interface Ethernet0/3
#
interface Ethernet0/4
#
```



```
interface Ethernet0/5
#
interface Ethernet0/6
#
interface Ethernet0/7
port access vlan 2
#
interface Ethernet0/8
port access vlan 2
#
interface Ethernet0/9
port access vlan 2
#
interface Ethernet0/10
port access vlan 2
#
interface Ethernet0/11
port access vlan 2
#
interface Ethernet0/12
port access vlan 2
#
interface Ethernet0/13
port access vlan 3
#
interface Ethernet0/14
port access vlan 3
#
interface Ethernet0/15
port access vlan 3
#
interface Ethernet0/16
port access vlan 3
#
interface Ethernet0/17
port access vlan 3
#
interface Ethernet0/18
port access vlan 3
#
interface Ethernet0/19
port access vlan 4
#
interface Ethernet0/20
port access vlan 4
#
interface Ethernet0/21
port access vlan 4
#
interface Ethernet0/22
port access vlan 4
#
interface Ethernet0/23
port access vlan 4
#
```

```
interface Ethernet0/24
  port access vlan 4
#
interface GigabitEthernet1/1
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.1.2 preference 60
```

50.1.3. 常见问题及解答

客户机不能上网

- 检查线路连接是否正确
- 确保客户机设置的网关为其所属VLAN的IP地址，使用ping命令ping路由LAN口IP，若不通，则交换机默认路由设置错误
- 确保和路由相接的是交换机的默认VLAN接口
- 检查路由和三层交换机都配置了到对方的静态路由



第 51 章 单WAN口通过交换机扩展接入多线路解决方案
目录

51.1. 单WAN口通过交换机扩展接入多ADSL解决方案

- 51.1.1. 网络拓扑结构
- 51.1.2. 三层交换机上的配置
- 51.1.3. 路由上的配置
- 51.1.4. 采用支持VLAN的二层交换机

51.2. 单WAN口通过交换机扩展多个固定IP解决方案

- 51.2.1. 单WAN口通过交换机扩展接入同一ISP的多个固定IP
- 51.2.2. 单WAN口通过交换机扩展接入不同ISP的多个固定IP

51.1. 单WAN口通过交换机扩展接入多ADSL解决方案

实例分析：某网吧现有20条ADSL线路，通过海蜘蛛路由实现带宽叠加上网，由于主板上资源有限，同时插上20块网卡无疑不太现实，而且很难保证每块网卡都能正常工作。此时，通过交换机来扩展 ADSL 接入无疑是一个非常好的选择。

51.1.1. 网络拓扑结构

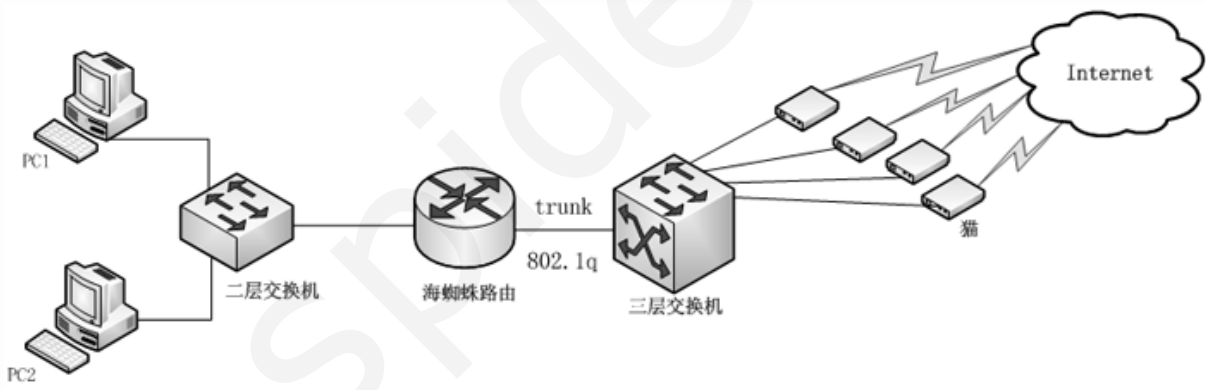


图 51.1. 基于多猫的网络拓扑结构

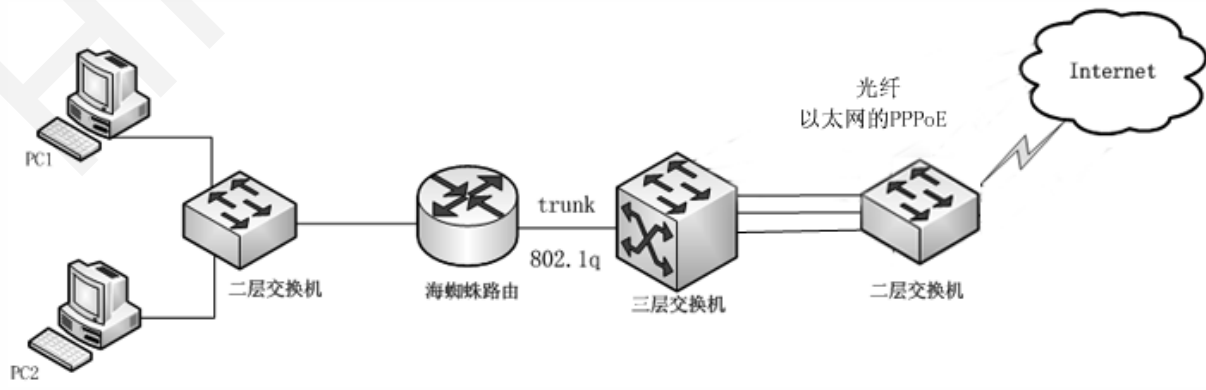


图 51.2. 基于光纤以太网的网络拓扑结构

- 通过建立以上的网络拓扑结构，就可以实现路由上只有一个WAN口时仍然可以接入多条ADSL线路。
- 这种方法有效的解决了多网卡IRQ冲突问题以及当用户有多条ADSL接入时PCI插槽不够的问题。

51.1.2. 三层交换机上的配置

1. 华为 s3526c 配置示例

由于有20条ADSL需要接入，故需要在三层交换机上划分20个VLAN，每个VLAN中只包括一个端口，每个端口与一根ADSL相连。以华为s3526c为例，交换机配置如下所示：

```
#
interface Ethernet0/1

#
interface Ethernet0/2
 port access vlan 2
#
interface Ethernet0/3
 port access vlan 3
#
interface Ethernet0/4
 port access vlan 4
#
interface Ethernet0/5
 port access vlan 5
#
interface Ethernet0/6
 port access vlan 6
#
interface Ethernet0/7
 port access vlan 7
#
interface Ethernet0/8
 port access vlan 8
#
interface Ethernet0/9
 port access vlan 9
#
interface Ethernet0/10
 port access vlan 10
#
interface Ethernet0/11
 port access vlan 11
#
interface Ethernet0/12
 port access vlan 12
#
interface Ethernet0/13
 port access vlan 13
#
interface Ethernet0/14
 port access vlan 14
#
interface Ethernet0/15
 port access vlan 15
#
interface Ethernet0/16
 port access vlan 16
#
interface Ethernet0/17
 port access vlan 17
#
interface Ethernet0/18
 port access vlan 18
#
interface Ethernet0/19
 port access vlan 19
#
```

```
interface Ethernet0/20
 port access vlan 20
#
interface Ethernet0/21

#
interface Ethernet0/22

#
interface Ethernet0/23

#
interface Ethernet0/24
```

这里用24号端口与海蜘蛛路由WAN接口相连，24号端口不需要划入任何VLAN，默认属于VLAN1即可。

交换机上24号端口的配置：

```
#
interface Ethernet0/24
 port link-type trunk
 port trunk permit vlan all
 dot1x
```

2. H3C S3600 配置示例

```
#
interface Ethernet1/0/1

#
interface Ethernet1/0/2
 port access vlan 2
#
interface Ethernet1/0/3
 port access vlan 3
#
interface Ethernet1/0/4
 port access vlan 4
#
interface Ethernet1/0/5
 port access vlan 5
#
interface Ethernet1/0/6
 port access vlan 6
#
interface Ethernet1/0/7
 port access vlan 7
#
interface Ethernet1/0/8
 port access vlan 8
#
interface Ethernet1/0/9
 port access vlan 9
#
interface Ethernet1/0/10
 port access vlan 10
#
interface Ethernet1/0/11
 port access vlan 11
#
interface Ethernet1/0/12
 port access vlan 12
#
interface Ethernet1/0/13
 port access vlan 13
#
interface Ethernet1/0/14
 port access vlan 14
#
```

```
interface Ethernet1/0/15
port access vlan 15
#
interface Ethernet1/0/16
port access vlan 16
#
interface Ethernet1/0/17
port access vlan 17
#
interface Ethernet1/0/18
port access vlan 18
#
interface Ethernet1/0/19
port access vlan 19
#
interface Ethernet1/0/20
port access vlan 20
#
interface Ethernet1/0/21

#
interface Ethernet1/0/22

#
interface Ethernet1/0/23

#
interface Ethernet1/0/24

port link-type trunk
port trunk permit vlan all
```

每种交换机配置都不全一样，具体配置请参考各交换机的VLAN配置说明书。

51.1.3. 路由上的配置

进入 Web管理 ->“网络设置”-> “广域网(WAN)”，选择相应的WAN口，选择ADSL/PPPoE拨号的Internet接入方式，填入用户名和密码，如下图所示：

PPPoE 拨号用户名：	<input type="text" value="wh9807"/>
PPPoE 密码：	<input type="password" value="....."/>
服务提供商名字(一般为空)：	<input type="text"/>

 重要


在主界面拨号的账号所对应的ADSL线路为默认接入交换机VLAN1接口的ADSL线路。

单击后面的“在此WAN口上绑定多个账号”：

[在此WAN口上绑定多个帐号](#) (已绑定 0, 激活 0)

进入多账号配置，如下图所示：

ID	名称 备注	用户名 密码	服务名	ISP	线路检测	带宽大小 上行 / 下行	负载权重	VLAN	MAC	激活	不自动负载	删除
1	<input type="text" value="10"/>	<input type="text" value="wh4567"/> <input type="password" value="....."/>	<input type="text"/>	<div>中国电信</div>	<div>✗</div>	<div>10 Kbit</div> <div>20 Kbit</div>	<div>1</div>	<div>10</div>	<input type="text"/>	<div><input checked="" type="checkbox"/> 是</div>	<div><input type="checkbox"/> 是</div>	<input type="checkbox"/>
2	<input type="text" value="20"/>	<input type="text" value="wh3435"/> <input type="password" value="....."/>	<input type="text"/>	<div>中国电信</div>	<div>✗</div>	<div>20 Kbit</div> <div>30 Kbit</div>	<div>1</div>	<div>20</div>	<input type="text"/>	<div><input checked="" type="checkbox"/> 是</div>	<div><input type="checkbox"/> 是</div>	<input type="checkbox"/>

 重要

每个账号对应的VLAN ID必须与交换机上划分的VLAN ID相对应，这里的VLAN ID唯一，

不能有2个账号有相同的VLAN ID号。这里的服务名可以选填，如果外线有多个拨号验证服务器需填写。每条单线的带宽上下行速度与MAC地址也可以选填。

同样的方法，继续新增另外的账号。



提示

在拨号之前，在上面的VLAN号后面填入对于的VID可以测试，测试成功后会发现拨号服务端的MAC地址

(VLAN 范围: 2~4094):

PPPoE 拨号, 请输入 VLAN 号:

	服务名	ISP	线路检测	带宽大小 上行 / 下行	负载权重	VLAN
<input type="text"/>	<input type="text"/>	<div>中国电信</div>	✓	<div>10 Kbit</div> <div>20 Kbit</div>	<div>1</div>	<div>10</div>
<input type="text"/>	<input type="text"/>	<div>中国电信</div>	✓	<div>20 Kbit</div> <div>30 Kbit</div>	<div>1</div>	<div>20</div>

提示: 在 VLAN-10 上 (eth1.10) 发现 PPPoE 服务器, MAC 地址为 00:25:9e:84:0b:8e

拨号成功后，可以在对应的网卡界面查看线路监测日志，掉线后会自动切换：

[wan2.10/aaa/]	正常, 拨号成功 !	断开
连接名:	ppp2 @ eth2.10	
上线时间:	2011-01-19 09:11:45	
已连接时间:	0 天 0 小时 0 分 52 秒	
IP地址:	59.172.189.102	
网关:	59.172.189.1	
DNS-1:	8.8.8.8	
DNS-2:	8.8.8.4	
PPPoE 服务器 MAC 地址:	00-40-63-e2-0f-bb	
流量统计:	共发送 54.0 bytes, 发送包 3, 出错 0, 丢弃 0 共接收 54.0 bytes, 接收包 3, 出错 0, 丢弃 0	
线路检测:	运行中 (PID:2525) [检测日志 清除]	

[wan2.20/bbb/]	正常, 拨号成功 !	断开
连接名:	ppp3 @ eth2.20	
上线时间:	2011-01-19 09:11:48	
已连接时间:	0 天 0 小时 0 分 49 秒	
IP地址:	59.172.189.103	
网关:	59.172.189.1	
DNS-1:	8.8.8.8	
DNS-2:	8.8.8.4	
PPPoE 服务器 MAC 地址:	00-40-63-e2-0f-bb	
流量统计:	共发送 54.0 bytes, 发送包 3, 出错 0, 丢弃 0 共接收 54.0 bytes, 接收包 3, 出错 0, 丢弃 0	
线路检测:	运行中 (PID:2526) [检测日志 清除]	

在路由主页面上也会有相应的线路显示，如图：

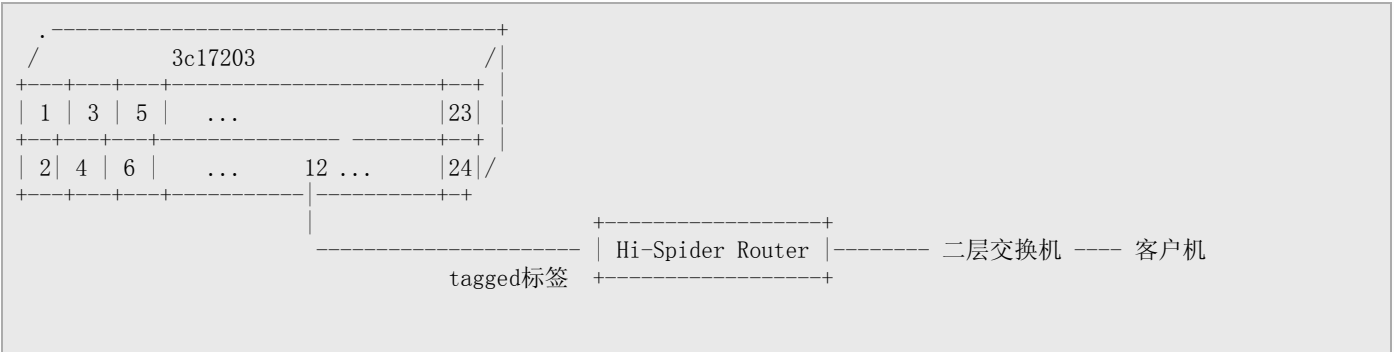
WAN2.20:	ppp3/eth2.20@59.172.189.103/255.255.255.255 <湖北省武汉市 (武昌区)电信ADSL> <14分18秒>
WAN2.10:	ppp2/eth2.10@59.172.189.102/255.255.255.255 <湖北省武汉市 (武昌区)电信ADSL> <14分21秒>

51.1.4. 采用支持VLAN的二层交换机

支持VLAN的二层交换机也可以实现扩展多 ADSL 接入，比使用三层交换机具有成本更低的优势。

网络结构与通过三层交换机扩展多ADSL接入方案一致。

二层交换机图例



有多少条ADSL需要接入，就需要在二层交换机上划分对应数量的VLAN，每个VLAN中只包括一个端口，每个端口与一根ADSL相连，这里以3c17203二层交换机接入2条ADSL为例，交换机配置如下所示：

1. 创建VLAN2，具体命令如下图所示：

```
Menu options: -----3Com SuperStack 3 Switch 4400-----
create          - Create a VLAN
delete          - Delete a VLAN
detail          - Display detailed information
modify          - Modify a VLAN
summary         - Display summary information

Type "quit" to return to the previous menu or ? for help
----- (1) -----
Select menu option (bridge/vlan): create
Select VLAN ID (2-4094) [2]: 2
Enter VLAN Name [VLAN 2]: vlan 2
```

将交换机端口2划入VLAN2，划分成功后将一根ADSL接入端口2，具体命令如下图所示：

```
                Select menu option (bridge/vlan): modify

Menu options: -----3Com SuperStack 3 Switch 4400-----
addPort         - Add a port to a VLAN
name            - Name a VLAN
removePort      - Remove a port from a VLAN

Type "quit" to return to the previous menu or ? for help
----- (1) -----
Select menu option (bridge/vlan/modify): addport
Select VLAN ID (1-5) [1]: 2
Select bridge port (1-24, AL1-AL4, all) [all]: 2
Enter tag type (untagged, tagged): untagged
```

2. 同样的方法创建VLAN3，并将交换机端口3划入VLAN3，划分成功后将另一根ADSL接入端口3
3. 将交换机端口12与海蜘蛛路由wan口连接，并将端口12同时划入VLAN2和VLAN3，并设置tagged标签，设置成功后查看端口12信息如下图所示：

```
Select menu option (bridge/port): detail
Select bridge port (1-24, AL1-AL4): 12

Unit 1, Port 12 Detailed Information

State:           Forwarding           fwdTransitions:      9
StpCost:         18                    BroadcastStormControl: Enabled
DefaultPriority:  0

VLAN ID          VLAN Name          Tagging Mode
-----
1                Default VLAN      Tagged
2                vlan 2            Tagged
3                vlan 3            Tagged
```



提示

通过以上设置可以得知，与路由相连的交换机端口即中继端口必须设置成属于每个VLAN

例：如果有20根ADSL接入，中继端口必须设置成同时属于20个VLAN

路由器上的配置和通过三层交换机扩展多ADSL接入方案一致。





51.2. 单WAN口通过交换机扩展多个固定IP解决方案

有时您会遇到拥有多个固定IP，但路由上网络接口不够的情况。这时您就可以将路由WAN口外接交换机，通过交换机外接多个固定IP来上网。

51.2.1. 单WAN口通过交换机扩展接入同一ISP的多个固定IP

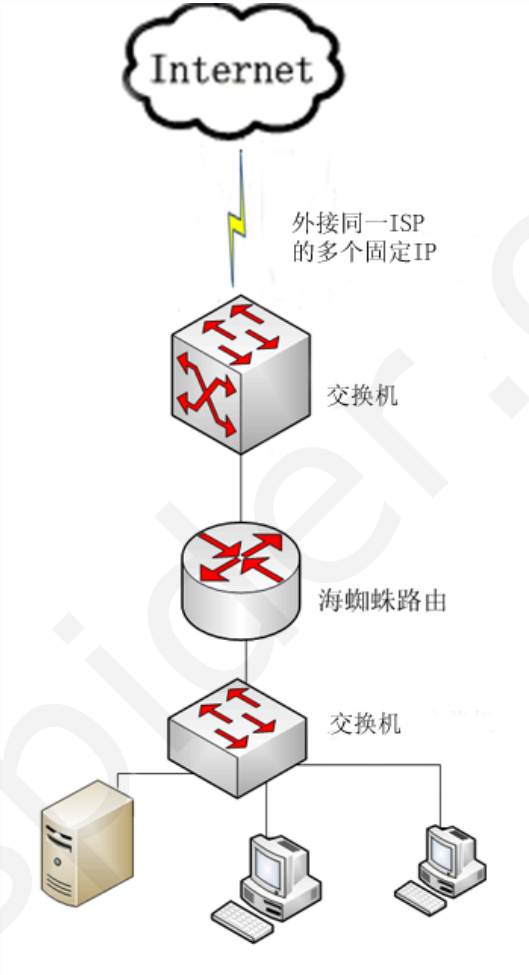


图 51.3. 同一ISP的多个固定IP的网络拓扑图

路由配置如下：

- 进入 Web管理 ->“网络设置”-> “广域网(WAN)”，选择相应的WAN口，选择 以太网/静态IP 接入方式，填入运营商所提供的IP地址、子网掩码和网关：

IP地址:	59.178.12.10
子网掩码:	255.255.255.248
网关:	59.178.12.9

图 51.4. 固定IP配置

- 点击后面的 在此WAN口上捆绑多个IP/网关:

在此WAN口上捆绑多个IP/网关 (已绑定 0, 激活 0)

图 51.5. 捆绑多个IP/网关

- 进入后添加多个IP/网关:

ID	名称	IP子网掩码	网关	备注	ISP	线路检测	负载权重	VLAN	MAC唯一MAC地址	激活	不自动负载	删除
1	10	59.178.12.11 255.255.255.	59.178.12.9		中国电信	✖	1	10	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
2	20	59.178.12.12 255.255.255.	59.178.12.9		中国电信	✖	1	20	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
3	30	59.178.12.13 255.255.255.	59.178.12.9		中国电信	✖	1	30	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
4	40	59.178.12.14 255.255.255.	59.178.12.9		中国电信	✖	1	40	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>

图 51.6. 添加多个同一ISP的IP/网关

注意

每个账号对应的VLAN号对应交换机上的VLAN号，不能有2个固定IP有相同的VLAN号。MAC唯一可勾选也可不勾选，勾选后每条线路都是独立的。MAC地址可以都为空或者自定义，自定义时不能有两个MAC地址相同

- 进入“网络设置”->“DNS参数”，选择手动指定DNS，填入当地的DNS服务器地址。

DNS 获取方式:	手动指定		
首选 DNS:	202.103.44.150	运营商:	中国电信
辅助 DNS:	202.103.0.68	运营商:	中国电信

图 51.7. 手动配置DNS

配置成功后，主页上会有对应的线路显示：

WAN2.2:	eth2/eth2@59.178.12.12/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2.1:	eth2/eth2@59.178.12.11/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2.3:	eth2/eth2@59.178.12.13/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2.4:	eth2/eth2@59.178.12.14/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr

图 51.8. 同一ISP的多个固定IP线路

51.2.2. 单WAN口通过交换机扩展接入不同ISP的多个固定IP

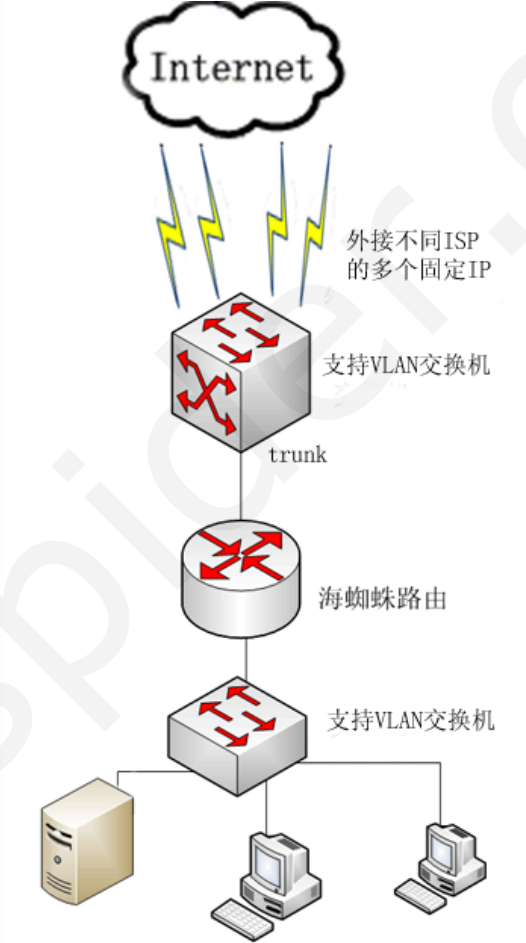


图 51.9. 不同ISP的多个固定IP的网络拓扑图

交换机上的配置类似 [多ADSL拨号方案的交换机配置](#)

路由配置如下：

- 进入 Web管理 ->“网络设置”-> “广域网(WAN)”，选择相应的WAN口，选择 以太网/静态IP 接入方式，填入运营商所提供的IP地址、子网掩码和网关：

IP地址：	59.178.12.10
子网掩码：	255.255.255.248
网关：	59.178.12.9

图 51.10. 固定IP配置

 重要

在主界面的固定IP线路默认为接入交换机VLAN1接口的固定IP线路。

- 点击后面的 在此WAN口上捆绑多个IP/网关：


在此WAN口上捆绑多个IP/网关 (已绑定 0, 激活 0)

图 51.11. 捆绑多个IP/网关

- 进入后添加多个IP/网关：

ID	名称	IP 子网掩码	网关	备注	ISP	线路检测	负载权重	VLAN	MAC唯一 MAC地址	激活	不自动负载	删除
1	10	59.178.12.11 255.255.255.	59.178.12.9		中国电信	✗	1	10	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab.	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
2	20	220.250.34.1 255.255.255.	220.250.34.1		中国铁通	✗	1	20	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab.	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
3	30	220.250.34.1 255.255.255.	220.250.34.1		中国铁通	✗	1	30	<input checked="" type="checkbox"/> 是 00-30-67-1b-ab.	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>

图 51.12. 添加多个不同ISP的IP/网关

 重要

每个账号的VLAN必须与交换机上划分的VLAN ID相对应，不能有2个固定IP有相同的VLAN号。MAC唯一可勾选也可不勾选，勾选后每条线路都是独立的。MAC地址可以都为空或者自定义，自定义时不能有两个MAC地址相同

- 进入“网络设置”->“DNS参数”，选择手动指定DNS，填入当地的DNS服务器地址。

DNS 获取方式:	手动指定	
首选 DNS:	202.103.44.150	运营商: 中国电信
辅助 DNS:	202.103.0.68	运营商: 中国电信
可选 DNS-1:	218.104.111.122	运营商: 中国铁通
可选 DNS-2:	218.104.111.114	运营商: 中国铁通

图 51.13. 手动配置DNS

配置成功后，主页上会有对应的线路显示：

WAN2.20:	eth2/eth2@220.250.34.18/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2.10:	eth2/eth2@59.178.12.11/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2.30:	eth2/eth2@220.250.34.19/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr
WAN2:	eth2/eth2@59.178.12.10/255.255.255.248 Intel Corporation 82541PI Gigabit Ethernet Contr

图 51.14. 不同ISP的多个固定IP线路





第 52 章 关于光纤接入的几种解决方案

目录

[52.1. 光纤接入绑定多个固定IP地址解决方案](#)

[52.1.1. 网络拓扑图](#)

[52.1.2. 路由器上的设置](#)

[52.2. 光纤接入绑定多个PPPoE账号解决方案](#)

[52.2.1. 网络拓扑图](#)

[52.2.2. 交换机设置](#)

[52.2.3. 路由器设置](#)

52.1. 光纤接入绑定多个固定IP地址解决方案

52.1.1. 网络拓扑图

案例分析：某公司申请了一根光纤，ISP为此光纤分配了多个公网IP地址如59.175.215.34/29，则您不仅可以在WAN接口主界面设置IP地址和对应的网关，同时也可以使用“在此WAN口上绑定多个IP/网关”来分配剩下的IP地址。网络拓扑结构图如下所示：

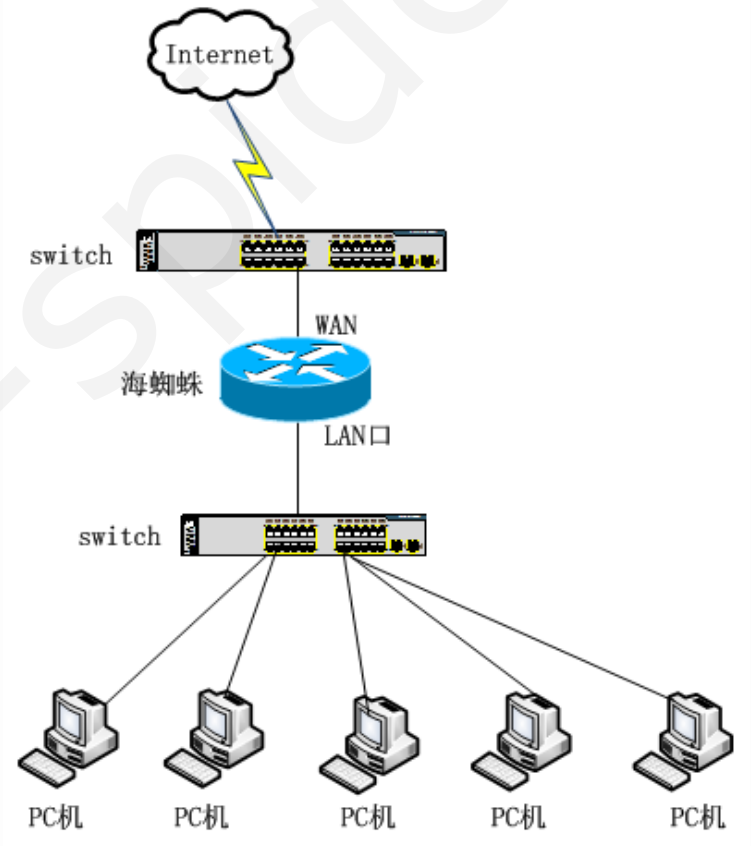


图 52.1. 多个固定IP地址的网络拓扑图



提示

以上拓扑图中的交换机均可使用二层交换机，即此功能的实现对交换机没有特殊的要求。

52.1.2. 路由器上的设置

这里我们假设您从ISP那里获得的合法IP地址段为59.175.215.34/29，若59.175.215.33作为网关使用，则还剩下5个公网IP可以使用：59.175.215.34-59.175.215.38，具体设置如下：

进入“网络设置”->“广域网（WAN）”，如下图所示：

IP地址：	<input type="text" value="59.175.24.34"/>	在此WAN口上捆绑多个IP/网关 (已绑定 0, 激活 0)
子网掩码：	<input type="text" value="255.255.255.248"/>	[此网段可容纳 6 台机器]
网关：	<input type="text" value="59.175.24.33"/>	

进入“在此WAN口上绑定多个IP/网关”，如下图所示：

ID	名称	IP子网掩码	网关	备注	ISP	线路检测	负载均衡	VLAN	MAC唯一MAC地址	激活	不自动负载	删除
1	<input type="text" value="4"/>	<input type="text" value="59.175.215.3"/> <input type="text" value="255.255.255."/>	<input type="text" value="59.175.215.3"/>	<input type="text"/>	<input type="text" value="中国电信"/>		<input type="text" value="1"/>	<input type="text" value="38"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-30-67-1b-ab-"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
2	<input type="text" value="10"/>	<input type="text" value="59.175.215.3"/> <input type="text" value="255.255.255."/>	<input type="text" value="59.175.215.3"/>	<input type="text"/>	<input type="text" value="中国电信"/>		<input type="text" value="1"/>	<input type="text" value="35"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-30-67-1b-ab-"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
3	<input type="text" value="20"/>	<input type="text" value="59.175.215.3"/> <input type="text" value="255.255.255."/>	<input type="text" value="59.175.215.3"/>	<input type="text"/>	<input type="text" value="中国电信"/>		<input type="text" value="1"/>	<input type="text" value="36"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-30-67-1b-ab-"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
4	<input type="text" value="30"/>	<input type="text" value="59.175.215.3"/> <input type="text" value="255.255.255."/>	<input type="text" value="59.175.215.3"/>	<input type="text"/>	<input type="text" value="中国电信"/>		<input type="text" value="1"/>	<input type="text" value="37"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-30-67-1b-ab-"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>

以上设置成功后，5个静态IP地址就可以同时作为外网IP。



重要

这里的VID可以随机填写，但必须唯一，即不同的IP地址必须对应不同的VID号。
若您的网络环境为2根不同的ISP光纤接入，则IP地址必须与所接入的ISP商一一对应

保存成功后，可以单击红色叉叉按钮进入线路检测设置页面，如下图所示：

编辑 wan1.2 ...

启用:	<input checked="" type="checkbox"/> 是
运营商:	中国电信 (启用多线策略及负载时需要)
检测时间间隔:	10 s (每隔多长时间探测一次线路的通断, 最少 5 秒, 默认为 10 秒)
线路探测模式:	PING/ICMP 网关探测 (默认)
重复探测次数:	3 (连续多少次探测不通才认为是掉线, 默认为 2 次)
PING/ICMP 探测对象:	(为空表示网关), 延时不大于 0 ms
SYN/TCP 探测对象:	www.hbtelecom.com.cn 端口: 80 (默认为 80), 延时不大于 0 ms 湖北省电信公司
线路工作时间:	- (线路非 24 小时连通时才需设置, 如 08:00 表示上午 8 点)
调试模式运行:	<input type="checkbox"/> 是 (一般不用开启)
测试模式运行:	<input type="checkbox"/> 是 (掉线后不切换)

首页-线路监测，可以查看当前线路状态，如下图所示：

ID	状态	线路	检测模式	检测间隔	探测次数	PING对象	PING延时	SYN对象/端口	SYN延时	线路工作时间	激活	删除	编辑
1		wan1	PING/ICMP	10 s	3	网关	-	www.hbtelecom.com.cn:80	-				
2		wan1.3	PING/ICMP	10 s	3	网关	-	:80	-				
3		wan1.4	PING/ICMP	10 s	3	网关	-	:80	-				
4		wan1.2	PING/ICMP	10 s	3	网关	-	:80	-				
5		wan1.1	PING/ICMP	10 s	3	网关	-	:80	-				



52.2. 光纤接入绑定多个PPPoE账号解决方案

52.2.1. 网络拓扑图

案例分析：某公司从ISP商那里申请了一根光纤，多个PPPoE账号，若按照传统的接入方式，则只有一个账号可以使用；若采用以下方法搭建网络并结合海蜘蛛的“一张网卡上可以绑定多个账号”的功能，则可以让所有账号同时拨号成功，达到增大带宽的效果，拓扑图如下所示：

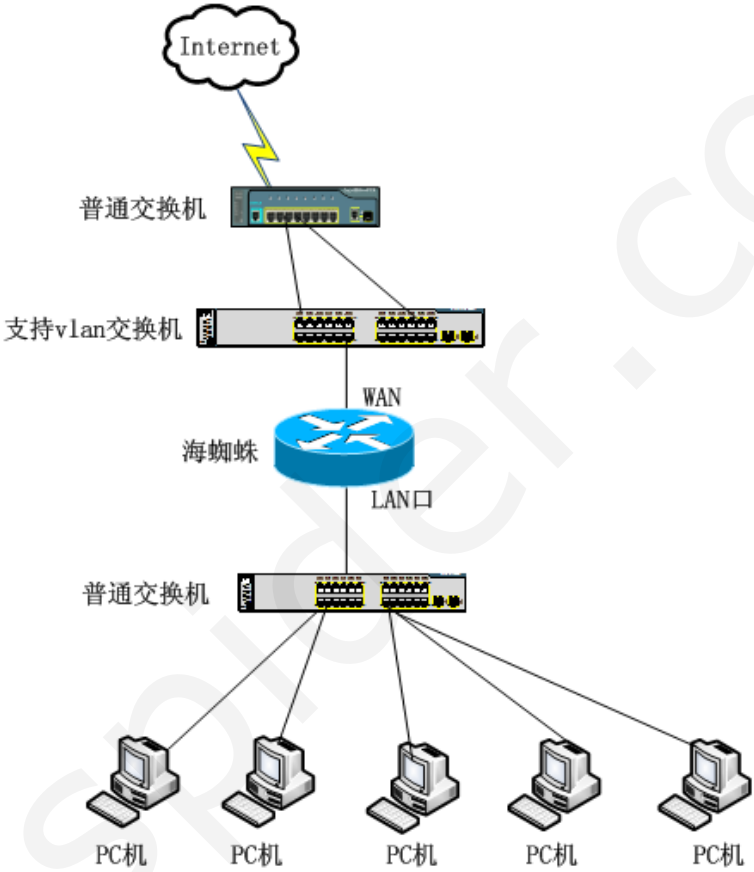


图 52.2. 光纤接入绑定多个账号的网络拓扑图

以上结构图表示光纤经过光纤转换器后接入普通交换机，普通交换机与支持VLAN的交换机之间的连线数与PPPoE 账号数相对应

52.2.2. 交换机设置

这里以2个PPPoE账号为例，交换机上需要的设置：

- 1.建立2个VLAN ，并且为每一个VLAN添加一个端口，这里以默认VLAN1和新建VLAN3为例
- 2.设置中继接口用来与路由WAN口相连接，这里用24口作为中继口。

```
#
vlan 1 默认vlan1
#
vlan 3 新建vlan3
#
interface Ethernet1/0/1 默认属于vlan1
#
interface Ethernet1/0/3 将3端口加入vlan3
```

```
port access vlan 3

#
interface Ethernet1/0/24   设置24口为中继接口
port link-type trunk
port trunk permit vlan all
```



重要

一个端口只能加入一个VLAN

52.2.3. 路由器设置

进入“网络设置”->“广域网（WAN）”，选择Internet接入方式为 PPPoE 拨号后，如下图所示：

PPPoE 拨号用户名:	<input type="text" value="test"/>	在此WAN口上捆绑多个帐号 (已绑定 2, 激活 2)
PPPoE 密码:	<input type="password" value="....."/>	
服务提供商名字(一般为空):	<input type="text" value="R2"/>	
发送 LCP(连接控制协议) 数据包间隔:	<input type="text" value="20"/> s (20~60, 如果频繁掉线, 请适当增大此值)	
多少个LCP请求未应答则断开连接:	<input type="text" value="3"/> (2~6, 如果频繁掉线, 请适当增大此值)	
此网关作为默认路由:	<input checked="" type="checkbox"/> 是 (一般选上, 如果有多条WAN线, 请只选一个)	
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)	
运营商:	<input type="text" value="中国电信"/> (启用多线策略及负载时需要)	
关闭网卡自动协商功能:	<input type="checkbox"/> 是	
工作模式:	<input type="text" value="自动设置"/>	
速度:	<input type="text" value="自动设置"/>	
负载权重:	<input type="text" value="1"/> ?	
其他参数:	<input type="checkbox"/> 启用调试 ? <input type="checkbox"/> 不自动加入多线负载 ? <input type="checkbox"/> 禁止NAT ?	
<div>保存设置 删除配置 重设</div>		



提示

此界面的拨号对应于VLAN1接口的线路

单击“在此WAN口上捆绑多个帐号”，设置如下图所示：

ID	名称备注	用户名密码	服务名	ISP	线路检测	带宽大小 上行 / 下行	负载权重	VLAN	MAC	激活	不自动负载
1	<input type="text" value="10"/>	<input type="text" value="004"/> <input type="password" value="....."/>	<input type="text"/>	<input type="text" value="中国电信"/>	<input checked="" type="checkbox"/>	<input type="text" value="40"/> Kbit <input type="text" value="150"/> Kbit	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="00-30-65-89-45-"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是



提示

这里的VLAN ID与交换机上的相对应，否则会造成拨号连接不成功。



第 53 章 光纤接入无需交换机扩展多线路解决方案
目录

53.1. 光纤接入绑定多个固定IP无交换机扩展解决方案


- 53.1.1. 网络拓扑图
- 53.1.2. 路由器上的设置

53.2. 光纤接入绑定多个PPPoE账号无交换机扩展解决方案

- 53.2.1. 网络拓扑图
- 53.2.2. 路由器设置

53.1. 光纤接入绑定多个固定IP无交换机扩展解决方案

53.1.1. 网络拓扑图

 重要

此功能需20120711以后的版本才能实现。

单根光纤进入到路由，含有同网段网关的多个IP地址。

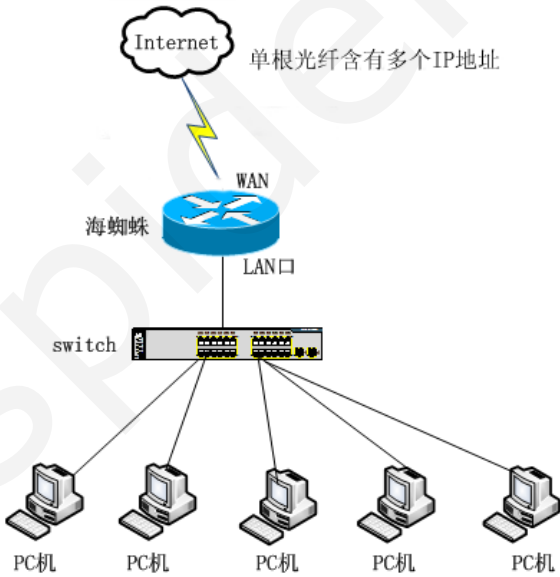


图 53.1. 多个固定IP地址的网络拓扑图

53.1.2. 路由器上的设置

例如这里我们假设您从ISP那里获得的IP地址段为61.183.11.224/27，若61.183.11.226为网关，有5个公网IP为：61.183.11.227-61.183.11.231，具体设置如下：
进入“网络设置”->“广域网（WAN）”，如下图所示：

IP地址:	61.183.11.227
子网掩码:	255.255.255.224
网关:	61.183.11.226

进入“在此WAN口上绑定多个IP/网关”，如下图所示：

ID	名称	IP 子网掩码	网关	备注	ISP	线路检测	负载权重	VLAN	MAC唯一 MAC地址	激活	不自动负载
1	<input type="text" value="1"/>	<input type="text" value="61.183.11.22
255.255.255."/>	<input type="text" value="61.183.11.22"/>	<input type="text"/>	<input type="text" value="中国电信"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-24-15-a2-25"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是
2	<input type="text" value="2"/>	<input type="text" value="61.183.11.22
255.255.255."/>	<input type="text" value="61.183.11.22"/>	<input type="text"/>	<input type="text" value="中国电信"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-24-15-a2-25"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是
3	<input type="text" value="3"/>	<input type="text" value="61.183.11.23
255.255.255."/>	<input type="text" value="61.183.11.22"/>	<input type="text"/>	<input type="text" value="中国电信"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="00-24-15-a2-25"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是
4	<input type="text" value="4"/>	<input type="text" value="61.183.11.23
255.255.255."/>	<input type="text" value="61.183.11.22"/>	<input type="text"/>	<input type="text" value="中国电信"/>	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> 是 <input type="text" value="12-24-15-a2-25"/>	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是

这里的VLAN必须都为0

后面的MAC地址唯一都需要勾选，这样每个IP才会有流量。对于MAC地址只要编写不同的合法地址即可

保存成功后，首页可以看到多条IP信息：

LAN1 WAN1 系统监测 内网监测 线路检测

WAN1:	eth1/eth1@61.183.11.227/255.255.255.224 <湖南> Intel Corporation 82540EM Gigabit Ethernet Controller
WAN1.3:	eth1.3/eth1.3@61.183.11.230/255.255.255.224
WAN1.4:	eth1.4/eth1.4@61.183.11.231/255.255.255.224
WAN1.2:	eth1.2/eth1.2@61.183.11.229/255.255.255.224
WAN1.1:	eth1.1/eth1.1@61.183.11.228/255.255.255.224

然后进入网络设置->多线负载与策略中勾选所有的IP并启用多线负载。

☒ 启用多线负载及策略 日志记录 | 清空日志

线路设置...

策略路由工作模式: ☐ 所有数据全部走策略线路 (仅用于VPN借线)

默认线路: 所有不符合策略的数据将全部走默认线路. 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条. 同一ISP应选择同一线路类型.

线路	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth1/eth1/61.183.11.227/255.255.255.224	<input type="text" value="默认线路"/>	<input type="text" value="中国电信 (269 条 v2.9)"/>	<input checked="" type="checkbox"/> 是
WAN1.1	中国电信	eth1.1/eth1.1/61.183.11.228/255.255.255.224	<input type="text" value="默认线路"/>	<input type="text" value="中国电信 (269 条 v2.9)"/>	<input checked="" type="checkbox"/> 是
WAN1.4	中国电信	eth1.4/eth1.4/61.183.11.231/255.255.255.224	<input type="text" value="默认线路"/>	<input type="text" value="中国电信 (269 条 v2.9)"/>	<input checked="" type="checkbox"/> 是
WAN1.3	中国电信	eth1.3/eth1.3/61.183.11.230/255.255.255.224	<input type="text" value="默认线路"/>	<input type="text" value="中国电信 (269 条 v2.9)"/>	<input checked="" type="checkbox"/> 是
WAN1.2	中国电信	eth1.2/eth1.2/61.183.11.229/255.255.255.224	<input type="text" value="默认线路"/>	<input type="text" value="中国电信 (269 条 v2.9)"/>	<input checked="" type="checkbox"/> 是

这时内网的应用就会分流走各个外网线路了

★ 重要

此方案对路由硬件CPU、网卡等配置要求较高



53.2. 光纤接入绑定多个PPPoE账号无交换机扩展解决方案



重要

此功能需20120711以后的版本才能实现。

53.2.1. 网络拓扑图

从运营商那边申请了单根光纤，光纤可以拨多个不同的帐号或者单个帐号可以重复拨多次。

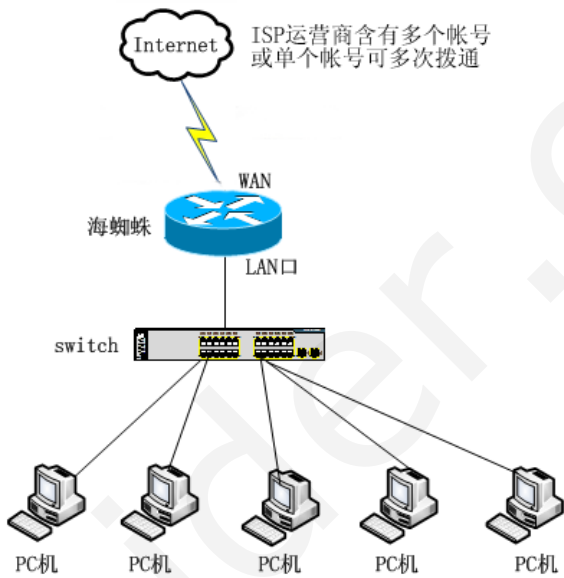


图 53.2. 光纤接入绑定多个账号的网络拓扑图

53.2.2. 路由器设置

进入“网络设置”->“广域网（WAN）”，选择Internet接入方式为 PPPoE 拨号，设置任意初始账号，如下图所示：

WAN-1

网卡位置: 01:06.0 | eth1 | Intel 82540EM Gigabit Ethernet Controller (rev 02) |

Internet 接入方式: ADSL/PPPoE 拨号 (通过电话线+猫或以太网/光纤拨号上网) ▼

流量统计:

共发送 14.30 KB, 发送包 0.26K, 出错 0, 丢弃 0
共接收 26.31 KB, 接收包 0.22K, 出错 0, 丢弃 0

物理连接状态: 已连接, 速度: 1000Mb/s (工作模式: 全双工)

参数设置...

带宽:	下行: 100 Mbit ▼, 上
MAC地址:	00-07-e9-2e-e8-05
MAC地址克隆:	
PPPoE 拨号用户名:	dsfd4353
PPPoE 密码:	●●●●●●

单击“在此WAN口上捆绑多个帐号”，设置如下图所示：

ID	名称 备注	用户名 密码	服务名	ISP	线路检测	带宽大小 上行 / 下行	负载均衡	VLAN	MAC	激活	不自动负载	删除
1	q21	frewtr34 *****		中国电信	✓	10 Kbit 50 Kbit	1	0	00-30-65-90-45-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
2	e	dgd35435 *****		中国电信	✓	20 Kbit 80 Kbit	1	0	00-30-65-89-45-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
3	a7	dfgrdg *****		中国电信	✓	40 Kbit 50 Kbit	1	0	00-30-65-89-a3-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>
4	err	534tgf *****		中国电信	✓	45 Kbit 90 Kbit	1	0	00-30-65-00-a3-	<input checked="" type="checkbox"/> 是	<input type="checkbox"/> 是	<input type="checkbox"/>

这里的VLAN号都需要为0，每条线路的上下行带宽可以选填，后面的MAC地址可以编写任意不同的合法地址。

保存成功后，拨通每个帐号，首页中可以看到每条拨号信息：

网络接口状态	
LAN1	WAN1 系统监测 内网监测 线路检测
WAN1.3:	ppp2/eth1.3@111.173.153.19/255.255.255.255 <...
WAN1.6:	ppp6/eth1.6@111.173.153.23/255.255.255.255 <...
WAN1.8:	ppp7/eth1.8@111.173.153.24/255.255.255.255 <...
WAN1.99:	ppp9/eth1.99@111.173.153.26/255.255.255.255 <...
WAN1:	ppp0/eth1@111.173.153.17/255.255.255.255 <湖北 Intel Corporation 82540EM Gigabit Ethernet Controller (rev 01)
WAN1.q21:	ppp3/eth1.q21@111.173.153.20/255.255.255.255
WAN1.e:	ppp1/eth1.e@111.173.153.18/255.255.255.255 <海
WAN1.x1:	ppp8/eth1.x1@111.173.153.25/255.255.255.255 <
WAN1.vdd:	ppp4/eth1.vdd@111.173.153.21/255.255.255.255
WAN1.a7:	ppp11/eth1.a7@111.173.153.28/255.255.255.255
WAN1.10:	ppp10/eth1.10@111.173.153.27/255.255.255.255
WAN1.err:	ppp5/eth1.err@111.173.153.22/255.255.255.255 <

然后进入网络设置->多线负载与策略中勾选所有线路并启用多线负载。

☒ 启用多线负载及策略

[日志记录](#) | [清空日志](#)

线路设置...

策略路由工作模式: 正常模式、掉线自动切换 ☐ 所有数据全部走策略线路 (仅用于VPN信线)

默认线路: 所有不符合策略的数据将全部走默认线路. 策略线路: 如果用户访问的IP在策略线路对应的ISP路由表中, 则走此线路. 默认线路和策略线路可以是一条或者多条. 同一ISP应选择同一线路类型.

线路	ISP	连接状态 (网卡/设备名/IP/子网掩码)	线路类型	使用路由表	激活
WAN1	中国电信	eth1/ppp0/111.173.153.17/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.E	中国电信	eth1.e/ppp1/111.173.153.18/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.3	中国电信	eth1.3/ppp2/111.173.153.19/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.6	中国电信	eth1.6/ppp6/111.173.153.23/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.8	中国电信	eth1.8/ppp7/111.173.153.24/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.X1	中国电信	eth1.x1/ppp8/111.173.153.25/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.99	中国电信	eth1.99/ppp9/111.173.153.26/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.10	中国电信	eth1.10/ppp10/111.173.153.27/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.A7	中国电信	eth1.a7/ppp11/111.173.153.28/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.Q21	中国电信	eth1.q21/ppp3/111.173.153.20/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.VDD	中国电信	eth1.vdd/ppp4/111.173.153.21/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是
WAN1.ERR	中国电信	eth1.err/ppp5/111.173.153.22/255.255.255.255	默认线路	中国电信 (269 条 v2.9)	<input checked="" type="checkbox"/> 是

这时内网的应用就会分流走各个外网线路了



重要

此方案对路由硬件CPU、网卡等配置要求较高



第 54 章 PPPoE认证+web认证+验证码的三重安全认证方案

部分 IX. 解决方案

第 54 章 PPPoE认证+web认证+验证码的三重安全认证方案

目录

[54.1. PPPoE服务器模式简介](#)

[54.1.1. 三重安全认证的优点](#)

[54.1.2. 网络拓扑图](#)

[54.2. PPPoE拨号的设置](#)

[54.3. Web认证设置和验证码](#)

54.1. PPPoE服务器模式简介

54.1.1. 三重安全认证的优点

- PPPoE给每台客户机与路由之间单独建立了一条虚拟线路，有效地防止了局域网ARP攻击，避免造成网络瘫痪。
- 能够杜绝用户私接二级路由造成的线路复用现象。
- 多重身份验证防止单独一环节的账号和密码被别人盗用上网。

54.1.2. 网络拓扑图

某公司申请了一根光纤，外网通过路由进入交换机，交换机下连接各独立的PC机。各PC机需通过PPPoE拨号到路由认证来实现上网。网络拓扑结构图如下：

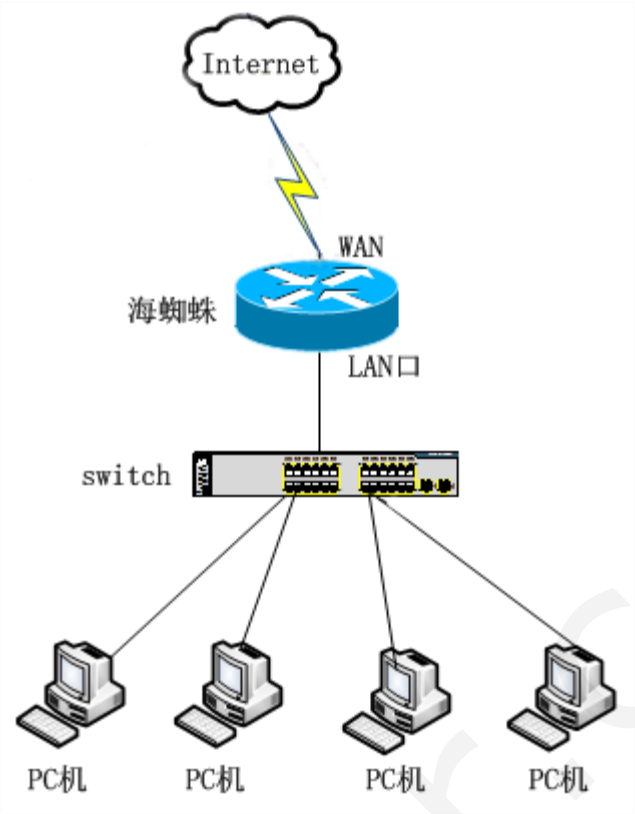


图 54.1. 网络拓扑图



53.2. 光纤接入绑定多个PPPoE账号无交换机扩展解决方案



54.2. PPPoE拨号的设置

54.2. PPPoE拨号的设置



54.2. PPPoE拨号的设置

首先登陆路由主页面，进入“服务应用”->“PPPoE拨号服务”，启用PPPoE拨号服务：

运行参数

高级

带宽限制

专用PPPoE

在线用户

启用 PPPoE 拨号服务:	<input checked="" type="checkbox"/> 是
监听设备:	<input checked="" type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> 无线局域网 (WLAN)
PPPoE 服务器名字:	<input type="text" value="PPPoE_Server"/> 英文字符
用户认证模式:	<div><input checked="" type="radio"/> 无需验证(任意用户名和密码均可拨入)</div> <div><input type="radio"/> 简单验证模式(一个帐号可同时拨入多次) 帐号管理</div> <div><input type="radio"/> 本地RADIUS认证(可限制帐号拨入次数,有效期等) 帐号管理</div> <div><input type="radio"/> 外部 RADIUS 服务器认证计费</div>

图 54.2. PPPoE 拨号服务的设置

这里用户认证模式选择无需验证，在任意一台PC下建立宽带连接即可进行PPPoE拨号，客户端设置的账户和密码可以任意。具体设置详见 [PPPoE 客户端设置](#)。

在高级页面里勾选 强制用户通过PPPoE拨号上网

强制用户通过PPPoE拨号上网:	<input checked="" type="checkbox"/> 是(客户机通过PPPoE拨号才能上网)
------------------	---

图 54.3. 强制用户通过PPPoE拨号上网



54.3. Web认证设置和验证码

在路由上设置好PPPoE拨号登陆后，还可以设置Web登陆方式，这样必须再经过一道Web页面账号密码的输入才能通过路由访问外网。

- 进入“服务应用”->“Web 认证服务”，勾选“启用上网 Web 认证”和“在 PPPoE 上启用 Web 认证”，下面的“会话存活超时时间”指的是如果客户机在服务器所设定的时间内没有任何操作，则需要重新进行PPPoE拨号认证。

参数设置

认证页面

在线用户

启用上网 Web 认证:

☒ 是

运行中 (PID:2937)

在 PPPoE 上启用 Web 认证:

☒ 是

认证模式:

☒ 所有用户上网都必须通过 Web 认证

☐ 指定IP上网时须通过 Web 认证

上网时需要经过验证的IP:

会话存活超时时间:

120

s (多长时间没有检测到用户在线则强制重新认证, 默认300, 最少120)

图 54.4. Web认证参数设置

- 在认证页面可以写下未经过Web认证前的提示和刚登陆时跳转的页面，在下面勾上允许用户自行修改密码和登录时启用验证码以加强安全，如图：

参数设置

认证页面

在线用户

提示标题:

上网认证

(显示在浏览器标题栏)

提示内容:

您好！

您需要使用合法的账户名和密码才能访问互联网！

请在以下输入框中输入帐号和密码登录, 如果您有什么疑问, 请与网络管理员联系, 感谢您的支持 !!

多长时间后自动跳转:

0

s (0表示不显示提示直接跳转)

跳转网址:

http://web.emuflly.com

管理签名信息:

网络管理中心 QQ: 123456, Tel: 1234567

(显示在提示框右下角)


允许用户自主修改密码

☒ 是

登录时启用验证码

☒ 是

图 54.5. Web认证页面设置



注意

此“跳转网址”是刚通过Web认证登陆时所显示的网页。

- 在线用户可以显示当前正在使用拨号的用户名及连接时间，如图所示：

ID	IP地址	MAC地址	用户名	真实姓名	上线时间	已连接时间	备注
1	22.22.22.20		123	123	2010-07-19 15:46:33	0天 0小时 1分 32秒	-

图 54.6. 在线用户信息

- 进入“服务应用”->“用户账号管理”，在这里添加账号及密码，在“可用功能列表”中勾选Web，如图所示：

用户ID:

(能由数字、字母、下划线、减号、@ 及圆点组成)

真实姓名:

登录密码:

(为空表示不修改)

密码确认:

帐号使用周期:

[生效]

[到期]

允许拨号的时间段:

分配固定IP:

(客户连接后始终获取此IP,仅适用于PPPoE/PPTP用户)

可用功能列表:

☐ PPPoE

☐ PPTP_VPN

☐ SSL_VPN


☒ Web

状态:

☒ 激活

☐ 禁用

图 54.7. 账号及密码管理



注意

账户使用周期是为账户添加使用时间，账户到期客户端会停止使用，必须在服务器上重新调整时间来启用。

- 这样在已拨号的客户PC上开启网页都会显示需要上网认证页面，如图：

上网认证

您好！

您需要使用合法的账户名和密码才能访问互联网！


请在以下输入框中输入帐号和密码登录，如果您有什么疑问，请与网络管理员联系，感谢您的支持！！

帐号:

密码:

登录

验证码:



看不清?

图 54.8. Web认证页面

- 输入服务器上所设定的用户名和密码，再输入随机验证码，点击“登陆”，系统会提示您已经登陆，如图：

上网认证

您好！

您需要使用合法的账户名和密码才能访问互联网！

请在以下输入框中输入帐号和密码登录，如果您有什么疑问，请与网络管理员联系，感谢您的支持！！

帐号：

密码：

注销

修改密码

提示：您当前已经登录，登录时间：2010-07-19 14:15:31

图 54.9. Web认证登陆

- 您也可以点击修改密码进行自行修改，如图所示：

上网认证

提示：密码只能由字母、数字、下划线、圆点、@符号、减号组成，最多32个字符。

您的旧密码：

您的新密码：

确认新密码：

确定

重置

返回

提示：您当前已经登录，登录时间：2010-07-19 15:46:33

图 54.10. 登陆密码修改





第 55 章 路由无线局域网解决方案

目录

[55.1. 路由无线局域网模式简介](#)

[55.2. 建立内网网段](#)

[55.3. 内网利用 PPPoE 服务上网](#)

[55.4. 内网利用 Web 认证上网](#)

55.1. 路由无线局域网模式简介

随着办公自动化的普及，越来越多的企业、酒店等采用了无线局域网的方式接入上网。它避免了使办公室里网线多如“盘丝洞”，也使用户不用担心网线接口松动或意外事故导致的网线物理损伤而无法联网。

例如某公司采用如下混合网络结构：

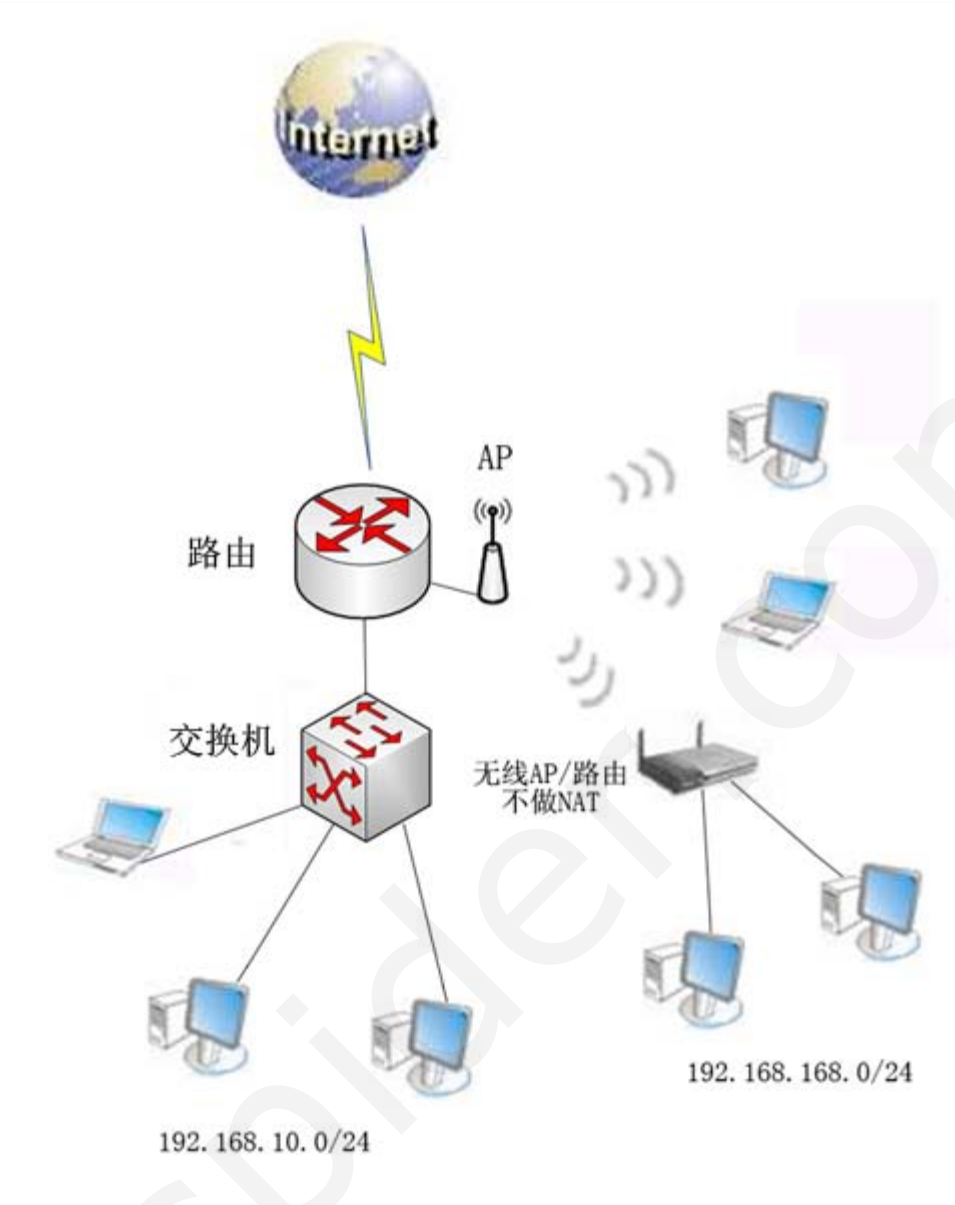


图 55.1. 网络拓扑图

路由LAN口下接交换机，接有线网络部分。路由电脑上安装无线网卡提供AP服务，接无线网络主机，另外一无线路由用作接收装置，不做网络地址转换，这里需要将无线连接的主机都保持在同一网段（这里也可以用无线交换机或AP加上普通交换机），其下再有线连接各主机。



54.3. Web认证设置和验证码



55.2. 建立内网网段



55.2. 建立内网网段

首先建立无线AP服务，进入“服务应用”->“无线 AP 服务”，勾选启用无线接入服务，配置如下图：

☒ 启用无线接入服务

服务状态： 运行中 (PID:1745) [已连接客户列表](#)

无线网卡：	wlan0 (选择要启用的无线网卡)
无线网络ID (SSID)：	Wireless_AP
IP地址：	192.168.168.1
子网掩码：	255.255.255.0
模式：	54M (802.11g)
信道：	Channel-1

安全设置...

启用无线接入访问保护 (WPA)：	<input checked="" type="checkbox"/> 是
WPA 类型：	自动设置
认证算法：	自动设置
加密算法：	自动设置
密码：	123456
组密钥更新周期：	600 (0为不更新, 最大值由无线网卡支持)

图 55.2. 无线AP配置

无线网卡选择插在路由电脑上的无线网卡，IP地址填写一个特殊网段的IP以避免和有线局域网网段相同，模式根据无线网卡支持的标准来选择，密码自定义。

保存设置后再进入“服务应用”->“DHCP 服务”，勾选启用 DHCP 服务，在IP地址池内新增地址池，添加有线和无线局域网IP地址池：

监听网络接口:	<div><input type="radio"/> 所有 LAN</div> <div><input checked="" type="radio"/> LAN-1.10 (eth2.10/eth2/192.168.10.1/255.255.255.0)</div> <div><input type="radio"/> LAN-1.20 (eth2.20/eth2/192.168.20.1/255.255.255.0)</div> <div><input type="radio"/> 无线局域网 (WLAN)</div>
分配的IP范围:	<div>192.168.10.100 - 192.168.10.200 (例如: 10.0.0.1-10.0.0.100)</div>
子网掩码:	<div>255.255.255.0 (例如: 255.255.255.0)</div>
租约时间:	<div>2 小时 (默认为2小时)</div>
网关:	<div>192.168.10.1 一般填系统局域网IP</div>
首选DNS地址:	<div>202.103.0.68 (这里一定要填写正确,否则客户机可能无法上网)</div>
辅助DNS地址:	<div>202.103.24.68 获取</div>
WINS地址:	<div>(NetBIOS名字解析服务器,可选)</div>
NTP地址:	<div>(时间服务器,可选)</div>
PXE 启动文件:	<div></div>
TFTP 服务器IP:	<div></div>
备注:	<div></div>
状态:	<div><input checked="" type="radio"/> 激活 <input type="radio"/> 禁用</div>

图 55.3. 有线局域网IP地址池

这里的监听网络接口选择 LAN-1.10 ，因为此例路由局域网配置已经建立了2个VLAN，所以在网关这里就填此VLAN的网关192.168.10.1。

监听网络接口:	<div><input type="radio"/> 所有 LAN</div> <div><input type="radio"/> LAN-1.10 (eth2.10/eth2/192.168.10.1/255.255.255.0)</div> <div><input type="radio"/> LAN-1.20 (eth2.20/eth2/192.168.20.1/255.255.255.0)</div> <div><input checked="" type="radio"/> 无线局域网 (WLAN)</div>
分配的IP范围:	<div>92.168.168.100 - 92.168.168.200 (例如: 10.0.0.1-10.0.0.100)</div>
子网掩码:	<div>255.255.255.0 (例如: 255.255.255.0)</div>
租约时间:	<div>2 小时 (默认为2小时)</div>
网关:	<div>192.168.168.1 一般填系统局域网IP</div>
首选DNS地址:	<div>218.104.111.112 (这里一定要填写正确,否则客户机可能无法上网)</div>
辅助DNS地址:	<div>218.104.111.114 获取</div>
WINS地址:	<div>(NetBIOS名字解析服务器,可选)</div>
NTP地址:	<div>(时间服务器,可选)</div>
PXE 启动文件:	<div></div>
TFTP 服务器IP:	<div></div>
备注:	<div></div>
状态:	<div><input checked="" type="radio"/> 激活 <input type="radio"/> 禁用</div>

图 55.4. 无线局域网IP地址池

这里的监听网络接口选择 无线局域网 (WLAN)，网关填写无线AP接入点的IP地址，此IP只要在192.168.168.0/24网段并且不在 分配的IP范围 内就行。



55.3. 内网利用 PPPoE 服务 上网

登录Web主页面，进入“服务应用”->“PPPoE 拨号服务”，勾选 启用 PPPoE 拨号服务：

启用 PPPoE 拨号服务：	<input checked="" type="checkbox"/> 是
监听设备：	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> 无线局域网 (WLAN)
PPPoE 服务器名字：	<input type="text" value="server"/> 英文字符
用户认证模式：	<p><input type="radio"/> 无需验证(任意用户名和密码均可拨入)</p> <p><input type="radio"/> 简单验证模式(一个帐号可同时拨入多次) 帐号管理</p> <p><input checked="" type="radio"/> 本地RADIUS认证(可限制帐号拨入次数,有效期等) 帐号管理</p> <p><input type="radio"/> 外部 RADIUS 服务器认证计费</p>
服务端 PPP 连接IP地址：	<input type="text" value="30.30.30.1"/> (不能和局域网在同一网段)
分配给客户机的地址空间：	<input type="text" value="30.30.30.2"/> - <input type="text" value="30.30.30.254"/>
分配给客户机的 DNS 地址：	<input type="text" value="30.30.30.1"/> , <input type="text" value="218.104.111.114"/> <input type="checkbox"/> 自动设置
PPP 连接的 MTU (最大传输单元)值：	<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)
PPP 连接的 MRU (最大接收单元)值：	<input type="text" value="1492"/> (请谨慎修改, 默认为 1492)
发送LCP(连接控制协议)数据包间隔：	<input type="text" value="30"/> 秒(默认为30,一般不超过60)
多少个LCP请求未应答则断开连接：	<input type="text" value="4"/> 个(默认为4,一般不超过6)
最大空闲时间(超过则主动断开连接)：	<input type="text" value="0"/> 分钟 (0表示不自动断开)
拨号用户名区分大小写：	<input type="checkbox"/> 是
自动绑定客户机的 MAC 地址：	<input type="checkbox"/> 是
允许 PPPoE 客户之间互访	<input type="checkbox"/> 是
调试模式运行：	<input type="checkbox"/> 是
日志保存位置：	-- 内存 --

图 55.5. PPPoE 拨号服务设置

这里的配置和有线局域网类似，只是在监听设备栏里一定要勾选无线局域网。用户认证模式这里采用的是RADIUS认证，所以还需建立新账号，点击后面的账号管理，选择新增用户：

用户ID:	<input type="text" value="ABC"/>	(能由数字、字母、下划
真实姓名:	<input type="text" value="用户10"/>	
登录密码:	<input type="password" value="....."/>	(为空表示不修改)
密码确认:	<input type="password" value="....."/>	
帐号使用周期:	<input type="text" value=""/> [生效] <input type="text" value=""/> [到期]	
允许拨号的时间段:	<input type="text" value=""/>	
分配固定IP:	<input type="text" value=""/>	(客户连接后始终获取此IP,仅适用于PPPoE/P
可用功能列表:	<input type="checkbox"/> FTP <input checked="" type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input type="checkbox"/> Web	
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 55.6. PPPoE 拨号账号

建立好所有的账号后，服务端设置就完成了。客户端只需建立拨号拨号连接即可，具体设置参照 [PPPoE 客户端设置\(Windows\)](#)

提示

对于无线拨号账户需先连接到无线AP再进行拨号连接。





55.4. 内网利用 Web 认证上网

登录Web主页面，进入“服务应用”->“Web 认证服务”，勾选 启用上网 Web 认证：

启用上网 Web 认证：	<input checked="" type="checkbox"/> 是 运行中 (PID:3290)
在 PPPoE 上启用 Web 认证：	<input type="checkbox"/> 是
认证模式：	<input checked="" type="radio"/> 所有用户上网都必须通过 Web 认证 <input type="radio"/> 指定IP上网时须通过 Web 认证
上网时需要经过验证的IP：	<div></div>

图 55.7. Web 认证设置

这里的认证模式选用的是所有用户上网都必须通过 Web 认证，您也可以选用指定IP上网时须通过 Web 认证来自定义。接下来进入认证页面进行设置：

认证页面

在线用户

提示标题：	Web 认证
提示内容：	请输入账号和密码！
多长时间后自动跳转：	0 s (0表示不显示提示)
跳转网址：	http:// www.google.com
管理签名信息：	admin

图 55.8. 认证页面设置

最后再设立Web账号，进入“服务应用”->“用户帐号管理”，新增用户：

用户ID:	<input type="text" value="123"/>	(能由数字、字母、下划线)
真实姓名:	<input type="text" value="用户20"/>	
登录密码:	<input type="password" value="....."/>	(为空表示不修改)
密码确认:	<input type="password" value="....."/>	
帐号使用周期:	<div><div>📅 ❌</div><input type="text"/></div> [生效] <div><div>📅 ❌</div><input type="text"/></div> [到期]	
允许拨号的时间段:	<input type="text"/>	?
分配固定IP:	<input type="text"/>	(客户连接后始终获取此IP,仅适用于PPPoE/PTTP_VPN)
可用功能列表:	<div><input type="checkbox"/> FTP <input type="checkbox"/> PPPoE <input type="checkbox"/> PPTP_VPN <input type="checkbox"/> SSL_VPN <input checked="" type="checkbox"/> Web</div>	
状态:	<div><input checked="" type="radio"/> 激活 <input type="radio"/> 禁用</div>	

图 55.9. 建立Web认证账户



提示

对于无线拨号账户需先连接到无线AP才能登陆浏览器进行Web认证。



第 56 章 主机电脑和手机平板设备分别认证解决方案

内网有主机和平板设备，对于内网主机电脑需要经过PPPoE拨号认证就可以上网，而对于手机平板设备无法设置PPPoE拨号，对于这些设备直接用Web认证来上网。如酒店等地可能需要多种上网认证方式混合。

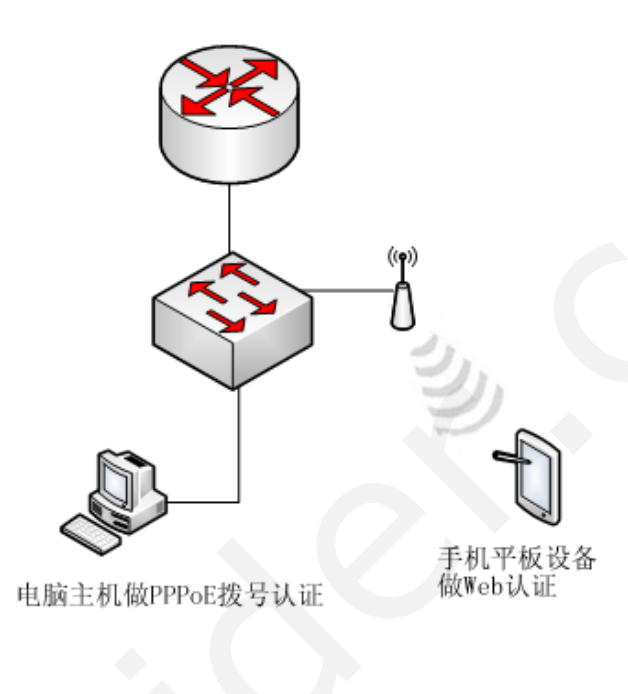


图 56.1. 网络拓扑简图

首先进入服务应用->PPPoE拨号服务，开启PPPoE拨号服务，选用RADIUS认证

PPPoE 服务状态: 运行中 (PID:4223) [日志记录 \(301.74 KB\)](#)

运行参数	高级	带宽限制	专用PPPoE	在线用户
启用 PPPoE 拨号服务:		<input checked="" type="checkbox"/> 是		
监听设备:		<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4 <input type="checkbox"/> 无线局域网 (WLAN)		
PPPoE 服务器名字:		<input type="text" value="PPPoE_123"/> 英文字符		
用户认证模式:		<div><input type="radio"/> 无需验证(任意用户名和密码均可拨入)</div> <div><input type="radio"/> 简单验证模式(一个帐号可同时拨入多次) 帐号管理</div> <div><input checked="" type="radio"/> 本地RADIUS认证(可限制帐号拨入次数,有效期等) 帐号管理</div> <div><input type="radio"/> 外部 RADIUS 服务器认证计费</div>		

图 56.2. 开启RADIUS认证

重要



在PPPoE拨号服务->高级页面中不能开启强制PPPoE拨号，否则影响Web认证用户

强制用户通过PPPoE拨号上网:	<input type="checkbox"/> 是(客户机通过PPPoE拨号才能上网)
IP白名单 (两种方式均可上网):	

图 56.3. 不启用强制PPPoE拨号

接着进入服务应用->Web认证服务，选择所有用户上网都必须通过 Web 认证

参数设置

认证页面

在线用户

启用上网 Web 认证:	<input checked="" type="checkbox"/> 是
在 PPPoE 上启用 Web 认证:	<input type="checkbox"/> 是
认证模式:	<input checked="" type="radio"/> 所有用户上网都必须通过 Web 认证 <input type="radio"/> 指定IP上网时须通过 Web 认证
上网时需要经过验证的IP:	<div></div>
会话存活超时时间:	<input type="text" value="3600"/> s (多长时间没有检测到用户在线则强制重新认证, 默认300, 最少120)

图 56.4. 启用Web认证

这样对于不拔号的如手机平板用户来说，必须通过Web认证，如果想跳过Web认证就需要通过PPPoE拨号，这里的帐号在用户帐号管理中分两种配置就行。



部分 X. 常见问题

目录

[57. 路由不能上网相关初步分析思路图](#)

[58. 网络慢卡的初步分析排查思路图](#)

[59. 关于重新绑定网卡](#)

[59.1. LAN口之间重新绑定](#)

[59.2. LAN接口与WAN接口之间重新绑定](#)

[60. 关于CPU中断](#)

[60.1. 中断简介](#)

[60.2. 影响CPU中断频率的因素](#)

[61. 特征库升级不成功](#)

[62. 路由上突然很多功能都失效](#)

[63. 即时通讯监控里看不到qq号或qq不能被禁止登录](#)

[64. 怎样查看路由上过去的日志](#)

[65. 变路由为透明网桥后可用哪些功能](#)

[66. 路由自动重启或关机的原因](#)

[67. 路由上的优先级顺序](#)

[68. 网卡突然全部启动不了，控制台无IP信息](#)

[69. 客户机PPTPVPN拨号成功后无法访问对端内网](#)

[70. DNS检测失败的原因](#)

[71. 内网主机ping网址不通或掉包的原因](#)

[72. 内网用户限速不了](#)

[73. 某个网页打不开或出错](#)

[74. 网卡不能正常工作相关问题](#)

[75. 网页打开非常慢或者基本都打不开](#)

[76. 磁盘错误引起的问题](#)

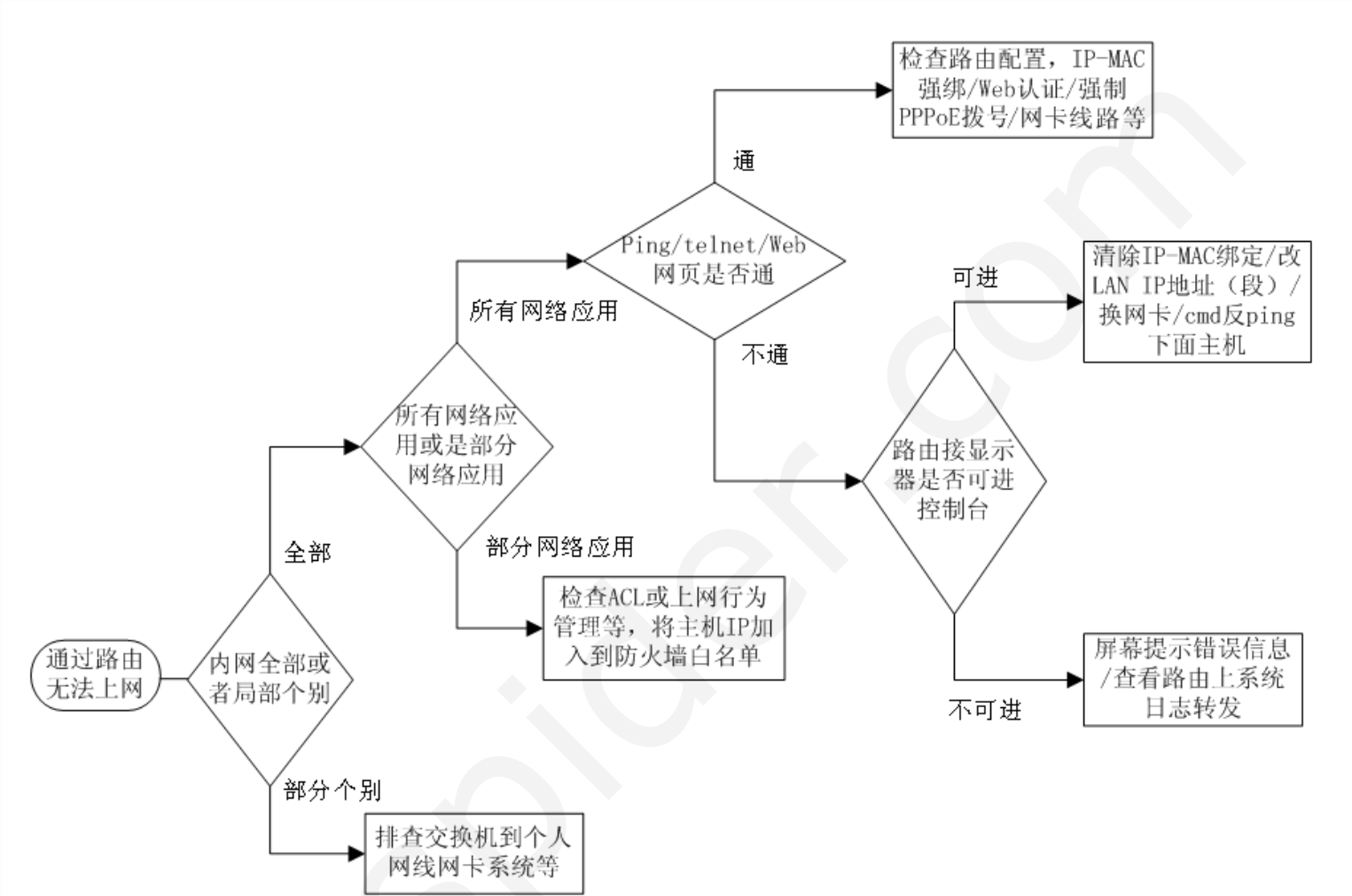
[77. 内网主机无法上网，并且路由上ping不通网关](#)

[78. WAN口LAN口流量不对称](#)

[79. 内网ARP攻击检测与防护](#)

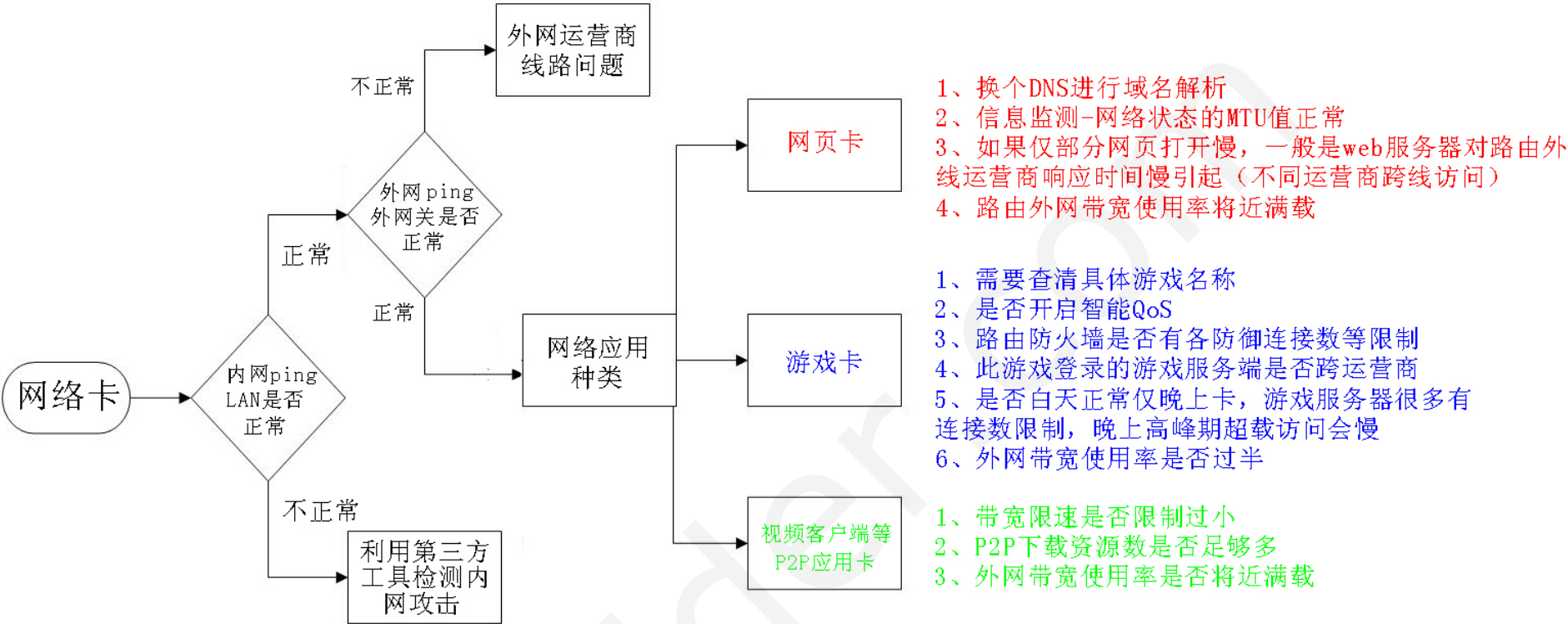


第 57 章 路由不能上网相关初步分析思路图



对于不能上网的情况，还需观察其周期、系统的负载等情况

第 58 章 网络慢卡的初步分析排查思路图



上网慢还有其它原因，例如路由网卡或主板硬件与海蜘蛛安全路由的兼容性。需要根据实际网络环境来分析。



第 59 章 关于重新绑定网卡

目录

- [59.1. LAN口之间重新绑定](#)
- [59.2. LAN接口与WAN接口之间重新绑定](#)

重新绑定网卡的规则：

LAN1	LAN2	WAN1	WAN2.....	WAN24
高-----优先级----->低				

- 重新绑定时需先将优先级高的接口绑定到优先级低的接口所对应的网卡，绑定后优先级高的接口之前绑定的网卡会自动释放
- 再将优先级低的接口绑定到优先级高的接口之前所对应的网卡

59.1. LAN口之间重新绑定

当前网络接口配置如下：

网卡位置: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN1*

流量统计: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN1*

02:00.0	eth1	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN1
03:00.0	eth2	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN2
04:00.0	eth3	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN2

物理连接状态: 已连接, 速度: 100Mb/s (工作模式: 全双工)

MAC地址: 00-e0-4c-68-00-de

1. 现在需要将LAN1和LAN2绑定的网络接口互换
- 将LAN1绑定到LAN2接口对应的网卡
- Web登录海蜘蛛路由->“网络设置”->“局域网 LAN”，在LAN-1页面下的“网卡位置”选择LAN2，点击“绑定”并“保存设置”，如下图所示：

网卡位置: 03:00.0 | eth2 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2

流量统计: 共发送 710.66KB, 发送包 2.84K, 出错 0, 丢弃 0
共接收 238.60KB, 接收包 2.65K, 出错 0, 丢弃 0 [注]: 此统计信息会定期清零

物理连接状态: 已连接, 速度: 100Mb/s (工作模式: 全双工)

MAC地址: 00-e0-4c-68-00-e0

保存成功后的网络接口配置图如下所示：

网卡位置：	03:00.0 eth2 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN1*
流量统计：	01:00.0 eth0 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	空闲
	02:00.0 eth1 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN1
	03:00.0 eth2 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN1*
	04:00.0 eth3 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN2
物理连接状态：		网线被拔出或网卡未启动
MAC地址：		00-e0-4c-68-00-e0

- 更改物理线路
将LAN1的网线插到LAN2所接的网卡上
- 测试局域网连接

2. 将LAN2绑定到LAN1接口对应的网卡

进入LAN-2的配置界面，当前网卡配置如下图所示：

LAN-1	LAN-2
网卡位置：	NULL 提示：此接口尚未配置与之关联的网卡！
	01:00.0 eth0 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... 空闲
	02:00.0 eth1 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... WAN1
	03:00.0 eth2 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... LAN1
	04:00.0 eth3 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... WAN2
	NULL 提示：此接口尚未配置与之关联的网卡！

选择处于空闲状态的接口，即原来为LAN1之前绑定的接口网卡，如下图所示：

网卡位置:	01:00.0 eth0 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... 空闲	
物理连接状态:	已连接, 速度: 未知 (工作模式: 未知)	
MAC地址:	00-e0-4c-68-00-de	

绑定保存设置后的网络接口配置情况如下图所示：

网卡位置:

01:00.0	eth0	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN2*
---------	------	---	-------

流量统计:

01:00.0	eth0	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN2*
02:00.0	eth1	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN1
03:00.0	eth2	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN1
04:00.0	eth3	Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN2

物理连接状态:

已连接, 速度: 100Mb/s (工作模式: 全双工)

MAC地址:

00-e0-4c-68-00-de

将LAN2的网线接到LAN1之前接的网卡并测试内网连接。



59.2. LAN接口与WAN接口之间重新绑定

第 59 章 关于重新绑定网卡

59.2. LAN接口与WAN接口之间重新绑定

当前网络接口配置如下：

网卡位置: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2*

流量统计: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2*

02:00.0 eth1 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN1
03:00.0 eth2 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	LAN1
04:00.0 eth3 Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern...	WAN2

物理连接状态: 已连接, 速度: 100Mb/s (工作模式: 全双工)

MAC地址: 00-e0-4c-68-00-de

1. 现在需要将LAN2和WAN2绑定的网络接口互换

- 将LAN2绑定到WAN2接口对应的网卡

Web登录海蜘蛛路由->“网络设置”->“局域网（LAN）”，进入LAN-2的配置界面，在“网卡位置”选择WAN2，单击“绑定”并“保存设置”，如下图所示：

网卡位置: 04:00.0 | eth3 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | WAN2

流量统计: 共发送 759.23KB, 发送包 3.31K, 出错 0, 丢弃 0
共接收 363.54KB, 接收包 4.29K, 出错 0, 丢弃 0 [注]: 此统计信息会定期清零

物理连接状态: 网线被拔出或网卡未启动

MAC地址: 00-e0-4c-68-00-e1

保存成功后的网络接口配置图如下所示：

网卡位置: 04:00.0 | eth3 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2*

流量统计: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | 空闲
02:00.0 | eth1 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | WAN1
03:00.0 | eth2 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN1
04:00.0 | eth3 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2*

物理连接状态: 网线被拔出或网卡未启动

MAC地址: 00-e0-4c-68-00-e1

- 更改物理线路
将LAN2的网线插到WAN2所接的网卡上
- 测试局域网连接

2. 将WAN2绑定到LAN2接口对应的网卡

选择“广域网（WAN）”，进入WAN-2的配置界面，选择处于空闲状态的接口，即为LAN2之前绑定的接口网卡，如下图所示：

网卡位置: 01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | 空闲 绑定

此接口尚未配置与之关联的网卡！

绑定成功并保存设置后的网络接口配置情况如下图所示：

网卡位置:

Internet 接入方式:

流量统计:

01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | WAN2*

01:00.0 | eth0 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | WAN2*

02:00.0 | eth1 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | WAN1

03:00.0 | eth2 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN1

04:00.0 | eth3 | Realtek Semiconductor RTL8111/8168B PCI Express Gigabit Ethern... | LAN2

共发送 759.23KB, 发送包 4.29K, 出错 0, 丢弃 0

共接收 363.54KB, 接收包 4.29K, 出错 0, 丢弃 0

绑定

[注]: 此统计信息会定期清零

WAN2的网线接到LAN2之前接的网卡并测试外网连接。





第 60 章 关于CPU中断

目录

- [60.1. 中断简介](#)
- [60.2. 影响CPU中断频率的因素](#)

60.1. 中断简介

中断是CPU处理外部突发事件的一个重要技术。它能使CPU在运行过程中对外部事件发出的中断请求及时地进行处理，处理完成后又立即返回断点，继续进行CPU原来的工作

中断分类

1. 硬中断

- 外部中断

外部中断一般是指由计算机外设发出的中断请求，如：键盘中断、打印机中断、定时器中断等。外部中断是可以屏蔽的中断，也就是说，利用中断控制器可以屏蔽这些外部设备的中断请求。

- 内部中断

内部中断是指因硬件出错（如突然掉电、奇偶校验错等）或运算出错（除数为零、运算溢出、单步中断等）所引起的中断。内部中断是不可屏蔽的中断。

2. 软中断

软件中断其实并不是真正的中断，它们只是可被调用执行的一般程序。例如：ROMBIOS中的各种外部设备管理中断服务程序（键盘管理中断、显示器管理中断、打印机管理中断等），以及DOS的系统功能调用（INT 21H）等都是软件中断。

中断优先级（由高到低）

- 除法错、溢出中断、软件中断
- 不可屏蔽中断
- 可屏蔽中断
- 单步中断



60.2. 影响CPU中断频率的因素

第 60 章 关于CPU中断



60.2. 影响CPU中断频率的因素

- 网卡性能
- CPU性能
- 内网恶意流量



第 60 章 关于CPU中断



第 61 章 特征库升级不成功



第 61 章 特征库升级不成功

特征库升级中，升级应用协议特征库，显示升级成功，版本号却一直没变

特征库升级

系统中包含多个特征库，如路由表、恶意网址库等，每个特征库是一个小型的数据库文件，随着网络的变化可能更新比较频繁，它独立于系统程序，可单独升级。

ID	名称	备注	版本	更新时间	自动更新	动作
1	f2154	恶意(病毒/木马)网址数据库	3.6.2	2012-07-09 16:13:27	<input checked="" type="checkbox"/>	检查更新
2	dnsserver_list	主要城市 DNS 地址列表	1.5.3	2011-06-30 08:51:24	<input checked="" type="checkbox"/>	检查更新
3	rtable	多线负载策略路由表	2.3.4	2012-07-05 09:41:36	<input checked="" type="checkbox"/>	检查更新
4	ads_domain	广告域名数据库	1.2.4	2012-07-09 16:16:32	<input checked="" type="checkbox"/>	检查更新
5	dnscap_list	常用网址域名 DNS 加速列表	1.4.6	2011-12-28 11:38:05	<input checked="" type="checkbox"/>	检查更新
6	appmark	应用协议特征库	3.1.3	2012-07-23 14:03:30	<input checked="" type="checkbox"/>	检查更新
7	sqos	安全流控特征库	2.5.3	2012-07-13 14:14:15	<input type="checkbox"/>	检查更新
8	isp_list	主要 ISP 官方网址列表	1.5.5	2012-01-09 09:45:54	<input checked="" type="checkbox"/>	检查更新

[检查所有更新](#)
[日志记录](#) | [清除](#)

2012-07-25 14:03:45 获取升级信息 ...
2012-07-25 14:03:45 下载升级文件, 请稍后 **appmark-v3.1.4** ... 成功

图 61.1. 特征库升级

这个情况有三种可能：

- 1. 磁盘空间不够，这个可以在信息监测-硬件信息里查看磁盘的使用率。如果磁盘已满请更换新磁盘再升级。
- 2. 磁盘有损害，在非正常情况下关机断电过，这时磁盘的配置文件更改会无法保存。需要把配置文件导出，重新安装海蜘蛛路由再将配置文件导入升级。
- 3. 服务使用到期，对于appmark应用协议特征库是针对企业和ISP版的，这里的升级服务有年限限制。您如果还需要升级请联系售后服务期。





第 62 章 路由上突然很多功能都失效

路由上如即时通讯监控、上网到期通知、各种提醒等、流量统计图、强制进行 IP/MAC 地址绑定、恶意网址拦截功能、网址过滤、强制用户通过PPPoE拨号上网、WEB认证、端口镜像等功能都突然失效了。

Web登录路由，进入系统设置->基本设置中，将最下面的极速前面的勾去掉保存即可。

NAT 会话中是否显示外网IP:	<input type="checkbox"/> 是
开机自动检查修复文件系统错误:	<input type="checkbox"/> 是
启用路由转发极速模式:	<input checked="" type="checkbox"/> 是, 生效时间段: <input type="text"/> (格式: HH:MM-HH:MM, 如 19:00-23:00)

保存设置 重置

图 62.1. 极速模式



第 63 章 即时通讯监控里看不到qq号或qq不能被禁止登录

部分 X. 常见问题

第 63 章 即时通讯监控里看不到qq号或qq不能被禁止登录

在路由的上网管理->即时通讯监控里，启用后下面登录的QQ号也都看不到

在路由的上网管理->应用协议控制中，启用了禁止QQ，下面的用户却仍然能登录QQ

这是因为用户登录的QQ版本特征库不在应用协议特征库受控范围之内，将用户的登录QQ版本找到，点击QQ面板左下角图像->帮助->关于QQ，如下图：




图 63.1. QQ版本

将图中红框部分的信息汇报给我们的售后（最后面4位数也包括在内），经过官方添加此QQ版本特征后，再进入产品中心->特征库更新中，点击升级 appmark 应用协议特征库 后即可。



第 64 章 怎样查看路由上过去的日志

 备注

仅企业版和ISP版才能查看过去的日志记录

首先确认您的路由是用的本地磁盘保存日志，Web登录海蜘蛛，进入上网管理->用户上网日志，这里的日志保存方式选择是在本地磁盘，如下图：

启用用户上网日志记录：

☒ 是

日志保存方式：

☒ 保存在本地：磁盘 /dev/vdb1 -- /data/data2

☐ 发送到SYSLOG服务器：192.168.101.172，端口：514 (默认为 514)

当前日志文件：/data/data2/www-20120726.log 3.06Mb

上网日志最长保存时间：

60 天 (默认为 7)

单个日志文件最大容量：

30 M

图 64.1. 日志保存本地

然后在路由内网形式下登录海蜘蛛（需确定本机的是通过海蜘蛛网关上网），进入系统设置->磁盘分区管理，找到刚才日志保存路径对应的映射目录：

sda - WDC WD5000AADS-0 [500.1 GB]												
分区	大小	文件系统		使用率	已使用	剩余	挂载点	自动挂载	启用 HTTP 映射	映射目录	动作	
/dev/sda1	100.0 GB	reiserfs	<div></div>	3%	2.6G	90.5G	/data/vm	<div></div>	<div></div>		卸载	- <div></div>
/dev/sda2	300.0 GB	reiserfs	<div></div>	0%	32.4M	279.3G	/data/sda2.4937	<div></div>	<div></div>	sda2.4937	卸载	- <div></div>
/dev/sda3	100.1 GB	reiserfs	<div></div>	3%	3.1G	90.2G	/data/sda3	<div></div>	<div></div>	sda3	卸载	- <div></div>

图 64.2. 日志映射目录

点击进入，会有各个带日期的文件列表，带log后缀的日期名文件就是当天的日志记录，将此文件下载解压即可查看：

Name	Last Modified	Size	Type
Parent Directory /		-	Directory
tftp/	2012-Jul-26 08:54:38	-	Directory
www-20120713.log.gz	2012-Jul-14 00:04:39	1.2M	application/x-gzip
www-20120714.log.gz	2012-Jul-15 00:03:58	360.7K	application/x-gzip
www-20120715.log.gz	2012-Jul-16 00:03:18	22.6K	application/x-gzip
www-20120716.log.gz	2012-Jul-17 00:02:37	3.0M	application/x-gzip
www-20120717.log.gz	2012-Jul-18 00:02:07	3.3M	application/x-gzip
www-20120718.log.gz	2012-Jul-19 00:05:37	3.2M	application/x-gzip
www-20120719.log.gz	2012-Jul-20 00:05:36	3.2M	application/x-gzip
www-20120720.log.gz	2012-Jul-20 17:05:35	3.3M	application/x-gzip
www-20120720_0001.log.gz	2012-Jul-21 00:05:33	591.9K	application/x-gzip
www-20120721.log.gz	2012-Jul-22 00:05:34	320.9K	application/x-gzip
www-20120722.log.gz	2012-Jul-23 00:12:44	22.3K	application/x-gzip
www-20120723.log.gz	2012-Jul-23 16:12:38	3.1M	application/x-gzip
www-20120723_0001.log.gz	2012-Jul-24 00:12:44	584.5K	application/x-gzip
www-20120724.log.gz	2012-Jul-24 17:12:43	3.7M	application/x-gzip
www-20120724_0001.log.gz	2012-Jul-25 00:12:43	197.4K	application/x-gzip
www-20120725.log.gz	2012-Jul-25 17:12:45	3.5M	application/x-gzip
www-20120725_0001.log.gz	2012-Jul-26 00:12:41	285.4K	application/x-gzip
www-20120726.log	2012-Jul-26 09:36:02	5.6M	text/plain

图 64.3. 日志列表

对于第三方日志查看所支持的软件及配置请咨询我们的售后人员。





第 65 章 变路由为透明网桥后可用哪些功能

进入网络设置->透明网桥，启用透明网桥功能：



图 65.1. 开启透明网桥

开启透明网桥后，原来的NAT功能失效，原来大部分三层应用都将失效，能够实现的功能如下：

- 1. 透明网桥PPPoE拨号认证（20110812以后的版本支持）
- 2. 透明网桥VLAN流控和统计报表（20110926以后的版本支持）
- 3. 透明网桥web认证（20110402以后的版本支持）
- 4. 透明网桥共享限速扩展网段（20111231以后的版本支持）
- 5. 透明网桥下应用协议控制（20110602以后的版本支持）
- 6. 透明网桥下DHCP服务应用（20120106以后的版本支持）
- 7. 透明网桥下IP-MAC绑定（2013.GoldenSnake以后的版本支持）
- 8. 透明网桥下ACL访问控制列表（20130806以后的版本支持）



第 66 章 路由自动重启或关机的原因
部分 X. 常见问题

第 66 章 路由自动重启或关机的原因

没有web登录路由点击重启或在路由控制台选择重启，但路由却自动重启了。这个情况有以下几种可能：

- 路由上设置了计划任务，web登录路由，系统设置->计划任务，看这里的定时重启是否配置：

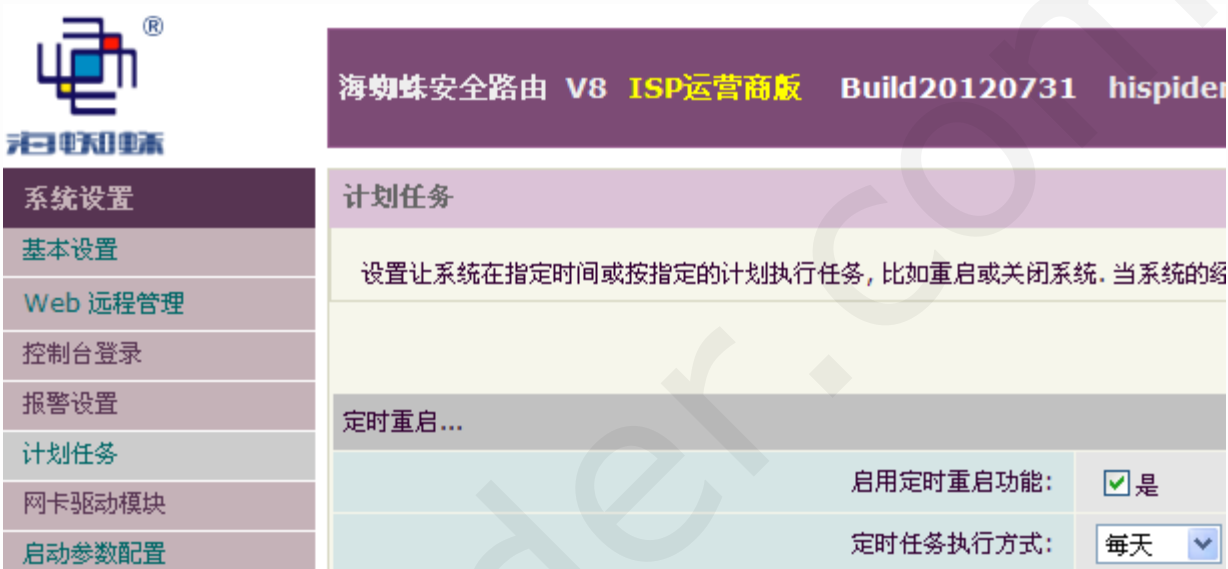


图 66.1. 配置计划任务

- 路由上的隐藏任务里有显示，web登录路由，在上面地址栏admin/后面换成cfgedit.pl，进入文本文本配置界面：

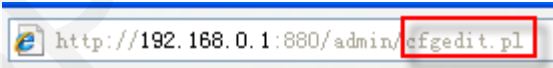


图 66.2. 文本配置界面

在此界面上输入 mytask ，看能否搜索到相关的计划任务，如果在 mytask 列表下有诸如reboot、halt等字样就表示设置了定时重启和关机。

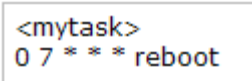


图 66.3. 文本配置重启关机

- 路由上开启了保护性过载重启措施等，进入系统设置->保存重启，在下面的电源管理有相关的重启和关机条件选项

电源管理...

☐ 启用硬盘自动休眠功能, 空闲时间: 5 分钟 确定

☒ 启用负载监测(超过自动重启), 触发条件: 1分钟 > 36 * 5分钟 > 27 * 15分钟 > 18 * 确定

☒ 启用断线自救功能(WAN口连续指定时间不通则自动重启), 触发条件: 5 分钟 确定

☒ 启用无人上网自动关机, 触发条件: 30 分钟 *, 生效时间段: - 确定 ?

☐ 无人上网自动关机后重新开机, 开机方式: 延时等待: 0 小时 0 分钟 指定时间: -

图 66.4. 自动重启关机触发条件

- 有些主板自带看门狗程序，会自动复位系统。在主板的BIOS里寻找 Watchdog 并关闭即可。
- 主板电源管理里有带电自启动功能，在电源线接触不良或当地电压不稳时会产生断电后的带电自启动。这个选项在主板的BIOS里的 Power Management Setup 列表中的 Restore On AC Power loss，选择 off 关闭即可

Phoenix - AwardBIOS CMOS Setup Utility		
Power Management Setup		
ACPI Function	[Enabled]	Item Help Menu Level ▶
ACPI Standby State	[S1(POS)]	
Video Off In Suspend	[Yes]	
Suspend Time Out(Minute)	[Disabled]	
Power Button Function	[Power Off]	
Wakeup Event Setup	[Press Enter]	
Restore On AC Power Loss	[Off]	

图 66.5. Restore On AC Power loss



提示

检查自动关机的方式和上面所述类似。





第 67 章 路由上的优先级顺序

/ 防火墙 \	
+-----+-----+	
白 名 单	
+-----+-----+	
黑 名 单	
+-----+-----+	
DNS 过滤 IP 过滤	
+-----+-----+	
DNS 重定向	
+-----+-----+	
全局网址过滤 全局关键字过滤	
+-----+-----+	
恶意网址拦截/重定向	
+-----+-----+	
协议特征过滤	
+-----+-----+	
ACL进入 / 转发规则	
+-----+-----+	
端口映射	
+-----+-----+	



第 66 章 路由自动重启或关机的原因



第 68 章 网卡突然全部启动不了，控制台无IP信息

第 68 章 网卡突然全部启动不了，控制台无IP信息

部分 X. 常见问题

第 68 章 网卡突然全部启动不了，控制台无IP信息

原来可以使用的网卡突然全部启动不了，控制台无IP信息，更换网卡也加载不了一个驱动，如下图：

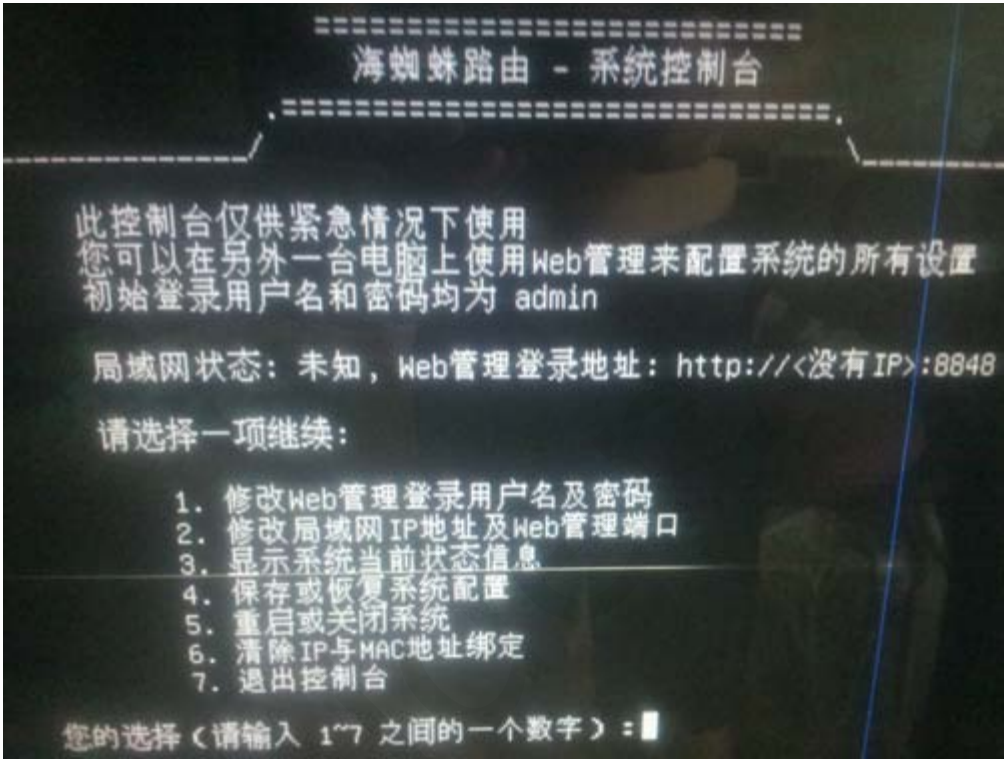


图 68.1. 无网卡IP信息

这个需要重新启动路由禁用原厂网卡驱动模块，操作步骤如下：

1. 系统启动时，在经过启动菜单后，不停按c，出现配置文件列表：

```
Copyright (C) 2005-2012 Hi-Spider Network Technology Co., Ltd.
[Linux-initrd @ 0x1f912000, 0x6cdcac bytes]

Mount essential kernel-base filesystem ...
Available memory size: 504720K
Loading USB-Storage driver ...
Searching and mount root device ...
Mounted root device at /dev/hda1 with reiserfs ok
Booting with i686-smp kernel ...
Loading system core into memory, please wait ...
Loading kernel modules ...
Loading system configuration ...
Press the key [C] to load specified configuration ... [1s]
c
** Welcome to interactive mode **

Please select configuration file to load:

1. current configuration
2. last good configuration
3. default configuration

Your choice please: [1-3]
```

图 68.2. 按c出现配置文件列表

2. 接着按e，进入配置文件编辑模式，输入/system找到[system]字段：

```
[system]
config_savetime = 2012-08-13 11:07:33
language = en
page_max = 12
root_passwd = $1$xxxxxxxx$8yHoNX3W.aK293K.aT4uJ/
time_zone = +08:00
```

图 68.3. 进入system文本编辑

3. 按o进入编辑，输入disable_pkg = native_drv

```
[system]
disable_pkg = native_drv
config_savetime = 2012-08-13 11:07:33
language = en
page_max = 12
root_passwd = $1$xxxxxxxx$8yHoNX3W.aK293K.aT4uJ/
time_zone = +08:00
```

图 68.4. 禁用原厂网卡驱动

编辑完毕后按2下ESC，按2下SHIFT+z保存，继续启动即可



第 69 章 客户机PPTPVPN拨号成功后无法访问对端内网

部分 X. 常见问题

第 69 章 客户机PPTPVPN拨号成功后无法访问对端内网

win系统客户机PPTPVPN拨号成功后无法访问对端内网，有如下几种可能：

1. 首先进入客户机PPTPVPN属性，选择“网络”选项卡 -> “Internet 协议 (TCP/IP)”，点击“属性”进入TCP/IP协议设置，点击高级按钮，确认勾选了“在远程网络上使用默认网关”前面的勾

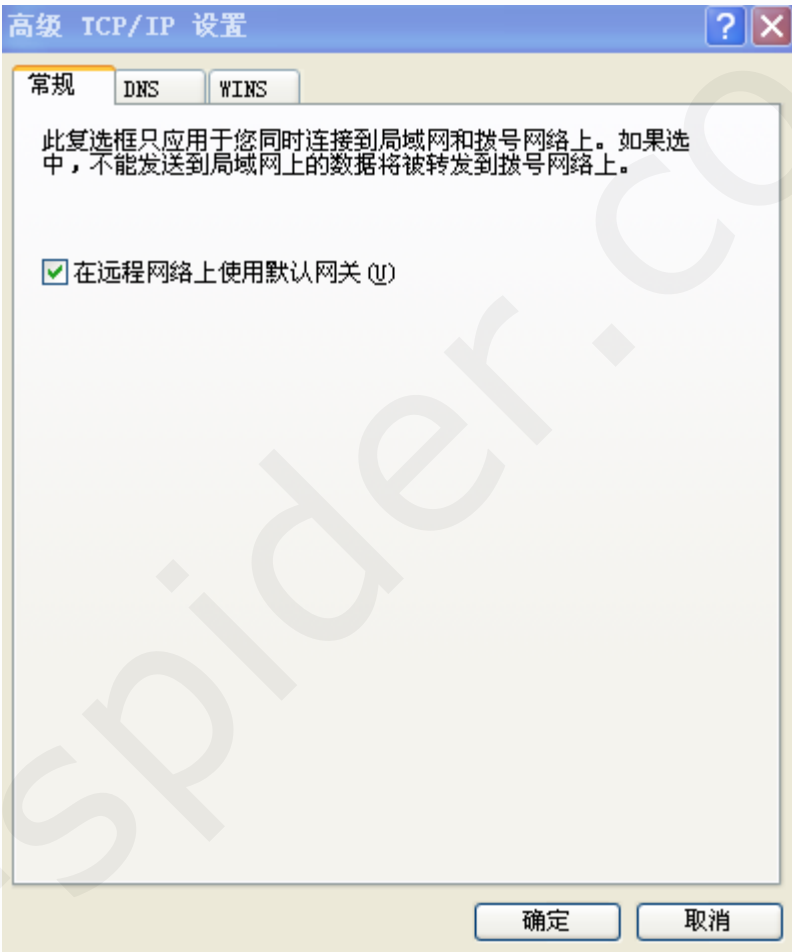


图 69.1. 使用远程网关

2. 对端待访问主机网关必须指向海蜘蛛路由LAN，也就是需通过海蜘蛛路由上网。
3. 客户机这边的本地连接不能和对端海蜘蛛局域网同网段，也不能一个子网包含另一个子网范围，如客户机VPN拨号这边本地连接是192.168.20.0/16网段的，对端海蜘蛛局域网为192.168.1.0/24网段的。
4. 如果对端海蜘蛛路由强制了PPPoE拨号或者Web认证之类的，需保证待访问主机在白名单之列，也就是说通过路由上网要正常。
5. 在海蜘蛛防火墙里的黑名单或者ACL配置有对VPN网段的访问限制
6. VPN进来可以ping通对端内网主机，却访问不了共享文件夹，这个一般是由于待访问主机的防火墙设置仅有允许本地局域网子网访问访问引起的。进入待访问主机控制面板中防火墙，找到例外标签页中的文件和打印机共享

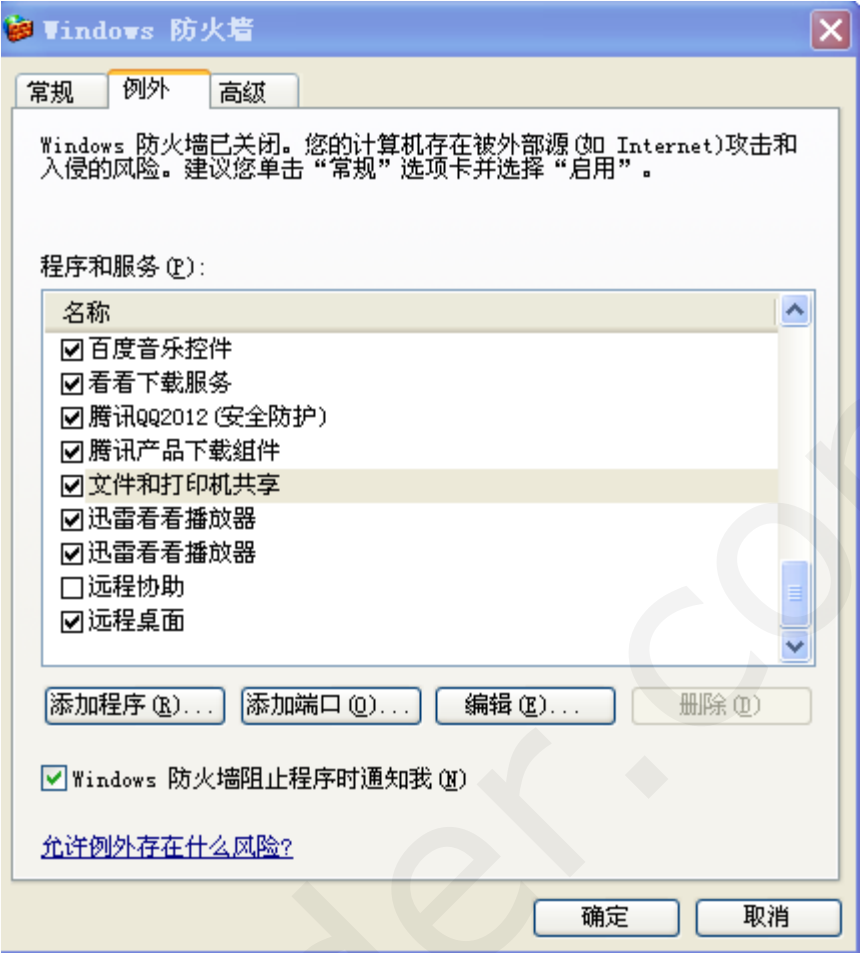


图 69.2. 文件和打印机共享

点击编辑，更改列表中每个端口的子网范围，从仅我的子网更改到任何计算机：

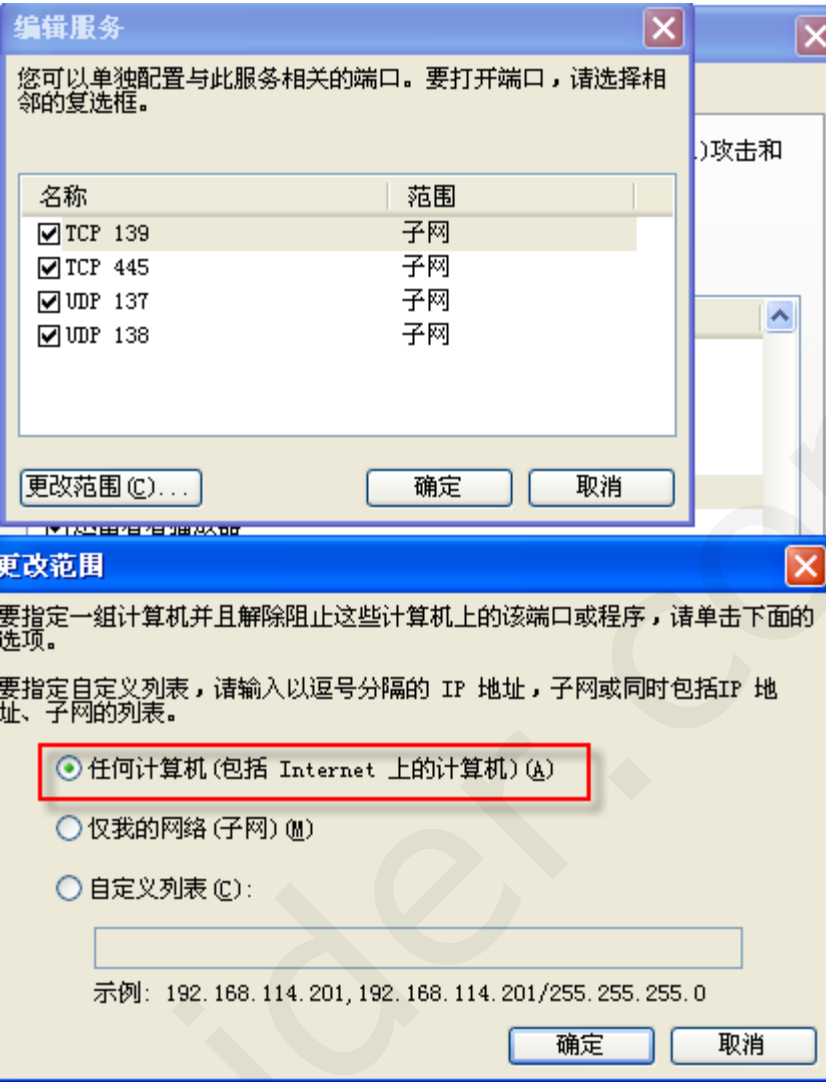


图 69.3. 更改子网范围

也可以直接关闭win防火墙和其它防火墙。



第 70 章 DNS检测失败的原因
部分 X. 常见问题



第 70 章 DNS检测失败的原因

网络设置->DNS参数，点击下面的诊断按钮，在诊断日志里显示失败：

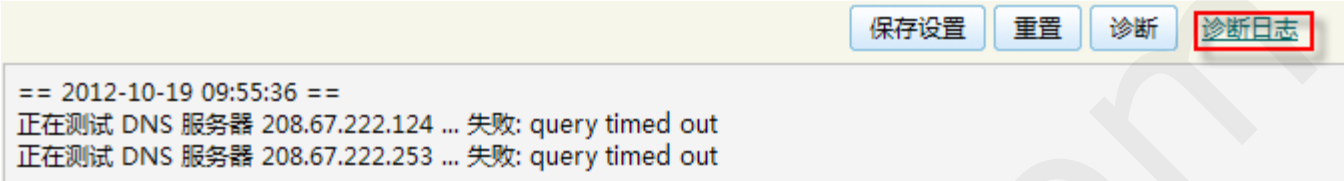


图 70.1. DNS诊断失败

- 首先检查路由网络是否通，进入系统工具->PING测试，输入WAN口的网关IP，看检测是否通：



图 70.2. PING网关

- 查看下DNS的IP本身是否有效，和运营商所提供的进行核对。
- 进入防火墙->访问控制列表，查看ACL有没进入路由的UDP丢弃配置：

优先级:	1	(只能为数字, 数字越小优先级越高)
协议类型:	UDP	
数据流向:	进入	
源IP:		
源端口:		
目的IP:	59.124.38.215	WAN口IP
目的端口:		
匹配数据包大小:		
时间限制:	<input type="checkbox"/> 启用	
	起始日期	结束日期
	起始时间	结束时间
	星期: <input type="checkbox"/> 一 <input type="checkbox"/> 二 <input type="checkbox"/> 三 <input type="checkbox"/> 四 <input type="checkbox"/> 五 <input type="checkbox"/> 六 <input type="checkbox"/> 日 <input type="checkbox"/> 工作日 <input checked="" type="checkbox"/> 全部	
动作:	丢弃 <input type="checkbox"/> 并记录到日志, 日志标识:	
备注:		
状态:	<input checked="" type="radio"/> 激活 <input type="radio"/> 禁用	

图 70.3. ACL丢弃

- 磁盘是否正常，进入系统设置->保存重启，点击这里的写入磁盘看能否正常写入保存：

备注
当前使用的配置 *已修改*
最后一次正确的配置

图 70.4. 检查磁盘



第 71 章 内网主机ping网址不通或掉包的原因

部分 X. 常见问题

第 71 章 内网主机ping网址不通或掉包的原因

路由下内网任意一主机ping外网网址出现非如下界面

```
C:\Documents and Settings\Administrator>ping www.baidu.com

Pinging www.a.shifen.com [220.181.111.188] with 32 bytes of data:

Reply from 220.181.111.188: bytes=32 time=41ms TTL=54
Reply from 220.181.111.188: bytes=32 time=40ms TTL=54
Reply from 220.181.111.188: bytes=32 time=40ms TTL=54
Reply from 220.181.111.188: bytes=32 time=44ms TTL=54

Ping statistics for 220.181.111.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 44ms, Average = 41ms
```

图 71.1. ping百度正常状态

- 如果出现如下图所示，就表示本机的DNS解析有问题，这个需要设置正确本机DNS或者借用路由上的DNS代理解析：

```
C:\Documents and Settings\Administrator>ping www.baidu.com
Ping request could not find host www.baidu.com. Please check the name and try again.
```

图 71.2. DNS解析错误

- 如果出现延时大或者掉包，先ping路由的LAN地址，看是否有掉包，如下图所示，如果有严重的掉包问题，内网可能有环路或者类似ARP攻击等

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

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

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 71.3. ping内网LAN口

- 路由上ping外网掉包或不通，先从路由上ping网关，如果网关正常的话，就是运营商所提供的线路问题

请输入 IP 地址或域名:

220.181.111.83

开始

重置

清除

可选参数:

PING 类型:	ICMP/PING (默认) ▼	
指定源IP进行PING:		
TCP 端口:	80	(默认为 80)
数据包个数:	10	(默认为 10)
数据段大小或长度:	0	bytes (默认为 0)
包发送时间间隔:	100	ms (默认为 100)
等待超时时间:	10	s (默认为 10)

Target IP address: 220.181.111.83

Using interface: eth0 [192.168.0.114]

PING request timed out.

PING request timed out.

PING request timed out.

PING request timed out.

Operation timedout for 10(s), exit

图 71.4. ping外网IP

请输入 IP 地址或域名:

192.168.0.1

开始

重置

清除

可选参数:

PING 类型:	ICMP/PING (默认) ▼	
指定源IP进行PING:		
TCP 端口:	80	(默认为 80)
数据包个数:	10	(默认为 10)
数据段大小或长度:	0	bytes (默认为 0)
包发送时间间隔:	100	ms (默认为 100)
等待超时时间:	10	s (默认为 10)

Target IP address: 192.168.0.1

Using interface: eth0 [192.168.0.114]

Echo reply from 192.168.0.1: seq=01 time=6.852 ms

Echo reply from 192.168.0.1: seq=02 time=5.562 ms

Echo reply from 192.168.0.1: seq=03 time=3.593 ms

Echo reply from 192.168.0.1: seq=04 time=1.491 ms

图 71.5. ping网关

- 路由上ping外网正常，内网ping不通外网网站或者IP。进入信息检测->网络状态中，查看默认路由是否存在

接入方式:	以太网/固定IP
DNS 服务器 IP:	208.67.222.124, 208.67.222.253
默认路由:	

图 71.6. 查看默认路由

如果不存在的话，进入网络设置->广域网WAN设置页面中，对于各WAN口标签中，确定有一个勾选了此网关作为默认路由：

此网关作为默认路由:	<input checked="" type="checkbox"/> 是（一般选上, 如果有多条WAN线, 请只选一个）
开机自动启动:	<input checked="" type="checkbox"/> 是（随系统启动, 一般选上）

图 71.7. 网关作为默认路由





第 72 章 内网用户限速不了

内网用户无论是PPPoE拨号用户或者手动限速都无法限速，相比限速值高太多。

需要进入防火墙->基本安全设置中，普通模式标签中限制TCP和UDP的单机总连接数，如下图：

☒ 启用 TCP 单机总连接数限制
最大允许的 TCP 单机总连接数 (范围 10-10000): (推荐 200-250)

☒ 启用 UDP 单机总连接数限制
最大允许的 UDP 单机总连接数 (范围 10-10000): (推荐 200-300)

图 72.1. 防火墙

有些网络应用是外网到路由的主动连接，需要限制单机连接数来控制速度，或者您将此超速的网络应用记下来提交到客服，我们这边根据网络应用来找出具体超限速的原因。



第 71 章 内网主机ping网址不通或掉包的原因



第 73 章 某个网页打不开或出错

第 73 章 某个网页打不开或出错

当上网某个网页打不开或打不开出错时，下载firefox浏览器，安装后在菜单栏里选择添加组件。

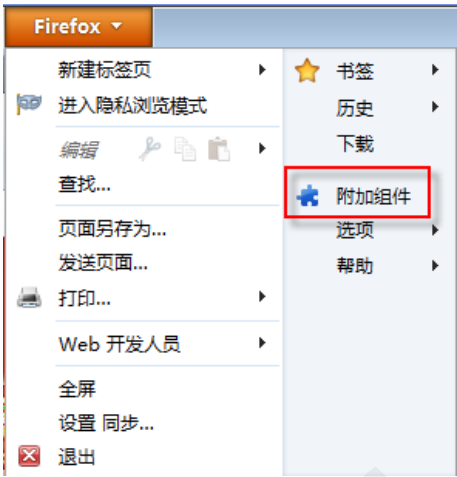


图 73.1. 添加组件

在上面的搜索栏中填入“firebug”，然后搜索



图 73.2. 添加 firebug

安装好后重启firefox，按下F12进入firebug，点击网络标签，选择启用：

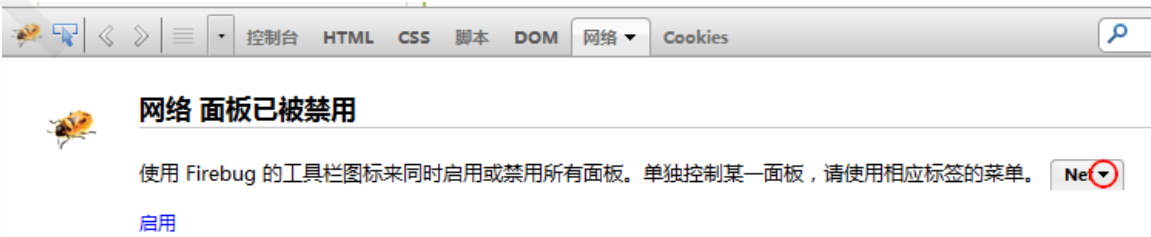


图 73.3. 启用firebug

打开一个网页正常时下面的状态里都显示 OK 字样：

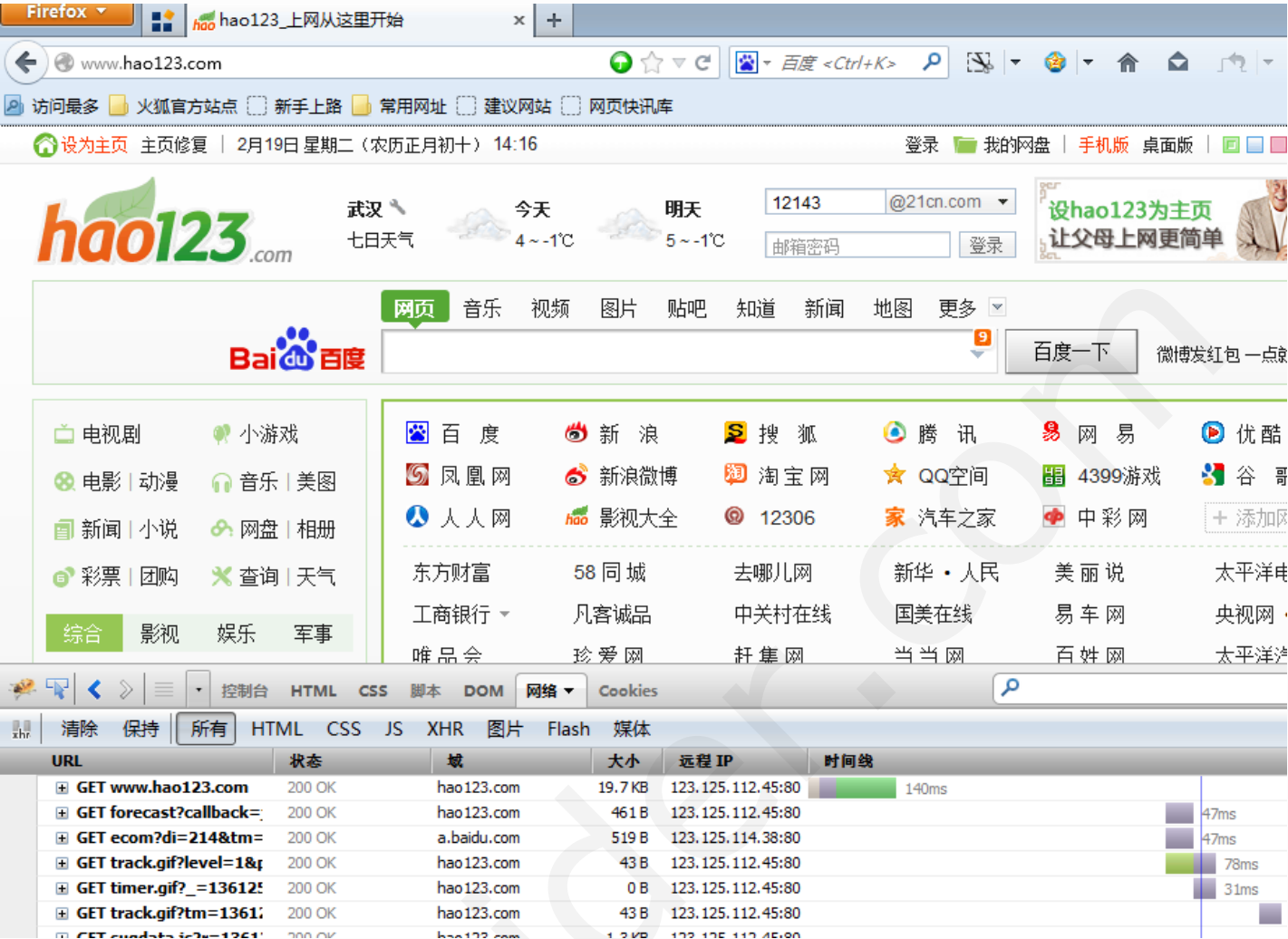


图 73.4. 正常状态

当打开一个页面异常时会显示有红色错误，这里红色错误有多种如404 not found等。将此状态记录反馈给官方的客服人员以便找出原因

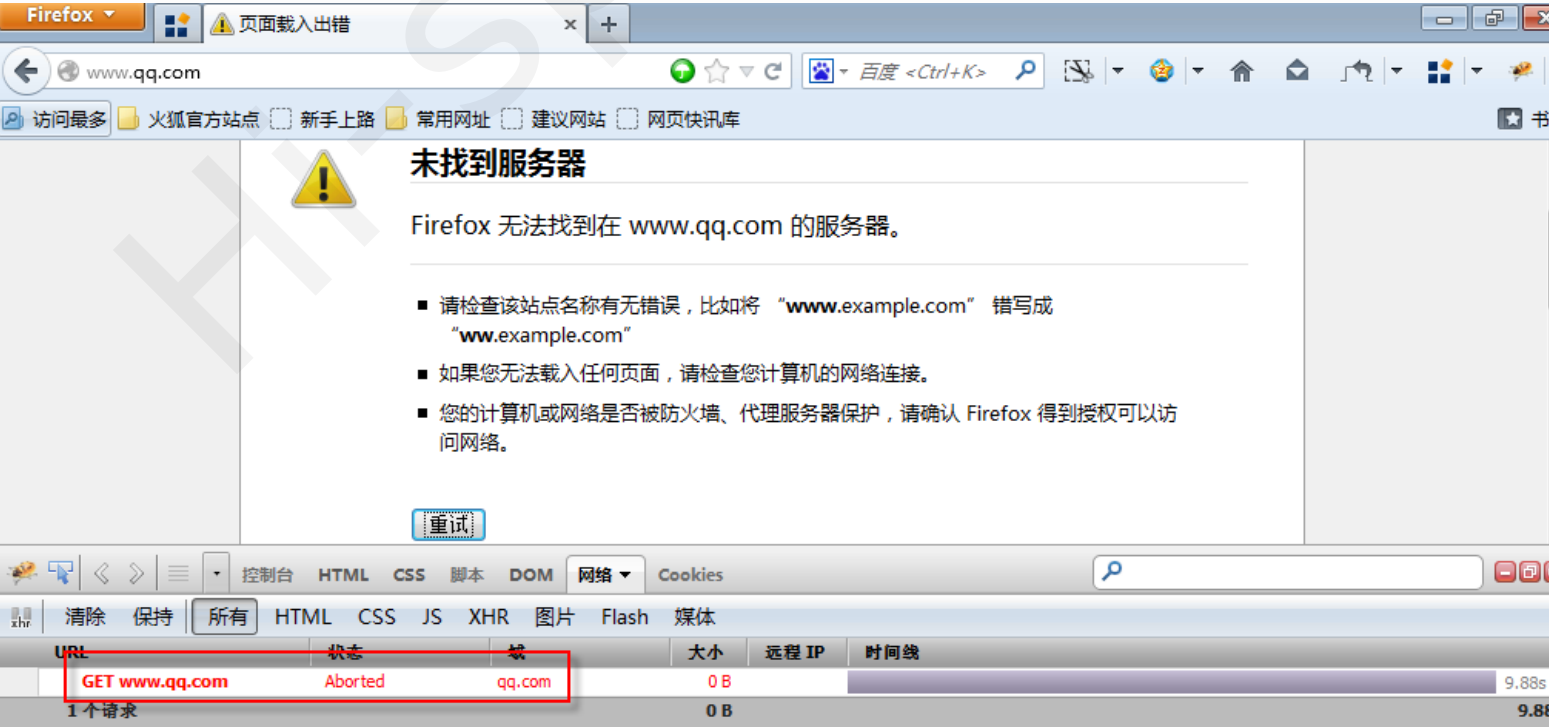


图 73.5. 异常状态



第 72 章 内网用户限速不了



第 74 章 网卡不能正常工作相关问题

第 74 章 网卡不能正常工作相关问题
部分 X. 常见问题

第 74 章 网卡不能正常工作相关问题

1. Intel网卡硬件可以识别，首页里也会出现，但连接网线后仍然是蓝色：



点击网卡进入后会发现状态显示是已连接网线：

物理连接状态:	已连接, 速度: 100Mb/s (工作模式: 全双工)
自动协商通告:	Yes
连接模式通告:	10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
Advertised_pause_frame_use:	No
自动协商:	on
当前消息级别:	0x00000007 (7)
双工模式:	Full
已插入网线:	yes
MDI-X:	off
PHY 地址:	1
当前接口类型:	Twisted Pair
当前连接速度:	100Mb/s
支持的连接模式:	10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full
支持的接口类型:	[TP]
支持的远程唤醒选项:	pumbg
自动协商支持:	Yes
发送器:	internal
当前远程唤醒选项:	pumbg

这时进入信息监测-网络状态中，查看系统初始化日志里，会有如下信息：

```
DRHD: handling fault status reg 3
DMAR:[DMA Write] Request device [04:00.0] fault addr fffff000
DMAR:[fault reason 02] Present bit in context entry is clear
DRHD: handling fault status reg 3
DMAR:[DMA Write] Request device [04:00.0] fault addr fffff000
DMAR:[fault reason 02] Present bit in context entry is clear
DRHD: handling fault status reg 3
DMAR:[DMA Write] Request device [04:00.0] fault addr fffff000
DMAR:[fault reason 02] Present bit in context entry is clear
```

这是由于IOMMU对旧设备的支持引起的，在系统设置-启动参数配置里，在内核参数中勾选“禁止Intel_IOMMU”

系统设置	启动参数配置	
基本设置	设置系统启动的相关参数, 比如默认启动的选项等.	
Web 远程管理		
控制台登录		
报警及邮件设置		
计划任务		
网卡驱动模块		
启动参数配置	默认要启动的内核:	<div><input type="radio"/> i386 (适用于工控机/嵌入式系统/老式主板或CPU)</div> <div><input type="radio"/> 单核 (适用于大多数硬件场合)</div> <div><input checked="" type="radio"/> 多核 (适用于双核等多CPU场合)</div>
磁盘分区管理	启动菜单等待时间:	<div><input type="text" value="1"/> s (多长时间后自动启动默认菜单)</div>
高可用性(VRRP)	内核参数 (请勿随意修改):	<div><input type="checkbox"/> 禁止USB</div> <div><input type="checkbox"/> 禁止APIC</div> <div><input type="checkbox"/> 禁止本地APIC</div> <div><input type="checkbox"/> 禁止HPET</div> <div><input checked="" type="checkbox"/> 禁止Intel_IOMMU</div> <div><input type="checkbox"/> 禁用PCI-E设备的节能模式</div> <div><input type="checkbox"/> 内核崩溃自动重启</div> <div><input type="checkbox"/> 禁止hda上的DMA</div> <div><input type="checkbox"/> 禁止hdb上的DMA</div> <div><input type="checkbox"/> 禁止hdc上的DMA</div> <div><input type="checkbox"/> 禁止hdd上的DMA</div> <div><input type="checkbox"/> 关闭超线程</div>
保存 & 重启		
网络设置		
防火墙		
上网管理		
服务应用		
流量控制		
信息监测		
产品中心		
系统工具		

保存后重启网卡即可恢复正常使用。

2. Intel 千兆网卡无法识别，在BIOS里可以识别，路由的硬件信息里可以检测到网卡存在，路由首页里却没有发现此网卡接口。进入路由信息监测-系统日志查看，选择系统初始化日志，看到有类似如下信息：

```
igb 0000:01:00.0: PCI INT A -> GSI 16 (level, low) -> IRQ 16
igb 0000:01:00.0: setting latency timer to 64
igb 0000:01:00.0: irq 27 for MSI/MSI-X
igb 0000:01:00.0: irq 28 for MSI/MSI-X
igb 0000:01:00.0: The NVM Checksum Is Not Valid
igb 0000:01:00.0: PCI INT A disabled
igb: probe of 0000:01:00.0 failed with error -5
igb 0000:01:00.1: PCI INT B -> GSI 17 (level, low) -> IRQ 17
igb 0000:01:00.1: setting latency timer to 64
igb 0000:01:00.1: irq 27 for MSI/MSI-X
igb 0000:01:00.1: irq 28 for MSI/MSI-X
igb 0000:01:00.1: The NVM Checksum Is Not Valid
igb 0000:01:00.1: PCI INT B disabled
igb: probe of 0000:01:00.1 failed with error -5
```

如果看到 The NVM Checksum Is Not Valid 字样，表示该网卡的EEPROM已经损坏，无法正常加载，windows下会直接忽略这个错误照常使用，而linux却不会。

需要将此网卡放入windows主机中，利用相关工具修复，请联系官方客服人员提供相关工具进行修复。

3. intel 82580/i350 网卡无法加载成功，需要登录路由后，在系统设置-网卡驱动模块中加入igb后重启路由即可。
4. Atheros AR8161 网卡无法加载成功，需要先升级路由到最新内核，登录路由后，在系统设置-网卡驱动模块中加入alx后重启路由。
5. PCI接口的无线AP RT3090无法加载成功，登录路由后，在系统设置-网卡驱动模块中加入rt2800pci后重启路由。
6. USB接口的IP-COM无线网卡W827U 无法加载成功，登录路由后，在系统设置-网卡驱动模块中加入rt2800usb后重启路由。
7. 对于多口网卡，有部分网卡会出现控制台中网卡连接未识别，首页中所有接口全蓝色的情况，这时需要将多线网卡所有接口都接通才能显示已连接的情况。



Hi-Spider.com

第 75 章 网页打开非常慢或者基本都打不开

路由下面的所有主机，在打开网页时非常慢或者基本都打不开，看视频、网络聊天等都基本正常，这有可能是强制DNS代理引起的。Web登录路由后，进入服务应用-DNS代理解析，去掉 强制使用 DNS 代理，保存后即可。

系统设置	DNS 域名解析服务
网络设置	DNS 域名解析服务用于缓存 DNS 解析结果, 以加快客户机域名解析的速度。
防 火 墙	
上网管理	DNS 解析服务状态: 运行中 (PID:4230) 查询日志 (71.44 KB) 统计分析 (需开启查询日志)
服务应用	<div>运行参数DNS 重定向高级</div>
DHCP 服务	
DNS 代理解析	启用 DNS 域名解析服务: <input checked="" type="checkbox"/> 是
NTP 时间服务	强制使用 DNS 代理: <input type="checkbox"/> 是 (DNS即插即用, 启用后客户机可任意配置DNS地址)
FTP 服务	



提示

如果内网是PPPoE拨号上网的话还有一种可能性，登录路由后，进入信息监测-网络状态中，查看下面的网络负载列表中有没有MTU值单元有没有不正常的，一般固定IP都为1500，拨号为1480或者1492都属正常值，如果出现比这要小的MTU值就会出现打不开网页，一般都为客户机系统问题。

网络负载 [会话数: 10441]

设备名	连接状态	工作模式	连接速度	MTU	接收字节	发送字节	接收包	发送包	出错/丢弃
eth0	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth1	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth2	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth3	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth4	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth5	Down	未知	未知	1500	0.0 byte	0.0 byte	0	0	0/0
eth6	Up	全双工	1000 Mb/s	1500	15120.77 GB	33710.98 GB	3.44G	2.84G	0/0
eth7	Up	全双工	1000 Mb/s	1500	37355.74 GB	12588.50 GB	1.68G	2.62G	0/0
ppc0	Up	-	-	1480	34.50 MB	276.02 MB	0.29M	0.24M	0/0
ppc1	Up	-	-	1480	113.35 MB	534.68 MB	0.42M	0.54M	0/0
ppc2	Up	-	-	1480	17.89 MB	295.98 MB	0.24M	0.26M	0/0
ppc3	Up	-	-	1480	161.69 KB	352.92 KB	1.38K	1.16K	0/0
ppc4	Up	-	-	1492	32.12 GB	45.07 GB	76.14M	74.21M	0/0
ppc5	Up	-	-	1432	1.01 MB	3.64 MB	8.31K	6.86K	0/0
ppc6	Up	-	-	1480	182.25 MB	425.40 MB	0.73M	0.59M	0/0
ppc7	Up	-	-	1480	6.63 MB	139.49 MB	88.38K	0.14M	0/0
ppc8	Up	-	-	1416	2.96 MB	5.89 MB	16.15K	15.50K	0/0
ppc9	Up	-	-	1492	413.25 KB	2.77 MB	3.96K	3.38K	0/0





第 76 章 磁盘错误引起的问题

当出现无法升级、法安装扩展模块、添加用户帐号、改配置都无效时都有可能是磁盘问题，按如下方法来检查磁盘：

- 随便更改一个设置如添加一个DNS地址或者添加一个用户帐号，然后进入 系统设置->保存重启 中，点击写入磁盘按钮，看能否写入到磁盘中

系统设置	系统配置管理			
基本设置	由于系统在内存运行, 您修改的配置信息也保存在内存中, 重启后这些配置将会丢失. 这就需要您统一保存写入到磁盘, 使配置永久生效. 如果您由于误配置' 恢复以前的备份设置来挽回损失.			
Web 远程管理				
控制台登录				
报警及邮件设置	ID	文件名	最后修改时间	备注
计划任务	1	current	2013-09-17 09:06:40	当前使用的配置 (已写入磁盘, 无须保存)
网卡驱动模块	2	lastgood	2013-09-17 09:06:40	最后一次正确的配置
启动参数配置	3	default	0000-00-00 00:00:00	出厂设置
磁盘分区管理	4	main.conf.20130607111534	2013-06-07 11:15:34	1
高可用性(VRRP)	5	main.conf.20130304104729	2013-03-04 10:02:32	
保存 & 重启				

图 76.1. 正常写入

系统设置	系统配置管理			
基本设置	由于系统在内存运行, 您修改的配置信息也保存在内存中, 重启后这些配置将会丢失. 这就需要您统一保存写入到磁盘, 使配置永久生效. 如果您由于误配置' 恢复以前的备份设置来挽回损失.			
Web 远程管理				
控制台登录				
报警及邮件设置	ID	文件名	最后修改时间	备注
计划任务	1	current	2013-09-17 09:06:40	当前使用的配置 *已修改* <input type="button" value="写入磁盘"/>
网卡驱动模块	2	lastgood	2013-09-16 15:55:09	最后一次正确的配置
启动参数配置	3	default	0000-00-00 00:00:00	出厂设置
磁盘分区管理	4	main.conf.20130607111534	2013-06-07 11:15:34	1
高可用性(VRRP)	5	main.conf.20130304104729	2013-03-04 10:02:32	
保存 & 重启				

图 76.2. 不能写入

- 如果写入正常，再重启一次路由，看刚才改动的配置还在不在，如果不在则磁盘也有问题。



第 77 章 内网主机无法上网，并且路由上ping不通网关

部分 X. 常见问题

第 77 章 内网主机无法上网，并且路由上ping不通网关

内网主机无法上网，单WAN口的情况下，在路由上ping不通网关，ping显示如图：

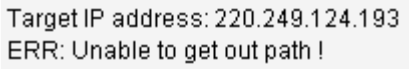


图 77.1. ping不通网关

这时您如果进入“信息监测”->“网络状态”中查看，会发现默认路由后是空的：

接入方式：	以太网/固定IP
DNS 服务器 IP：	218.104.111.122, 218.104.111.114, 8.8.8.8
默认路由：	

图 77.2. 默认路由为空

进入“网络设置”->“广域网（WAN）”，把其中的 此网关作为默认路由 勾选：



图 77.3. 勾选默认路由

保存后网络即可正常使用。



第 78 章 WAN口LAN口流量不对称

一般来说，路由系统的WAN口和LAN口上行下行速度是对应的，进入系统实时状态监测点可以查看到对应信息

网络接口	状态	工作模式	累计下行/接收 bytes	累计上行/发送 bytes	总累计流量 bytes	即时下行速度 byte/s	即时上行速度 byte/s	总实时速度 byte/s	流量图
LAN-1 eth0/eth0		1000Mb/s 全双工	95.50 GB	53.73 GB	149.24 GB	3.63 MB	1016.46 KB	4.62 MB	查看
LAN-2 eth1/eth1		未知	0.0 byte	0.0 byte	0.0 byte	0.0 byte	0.0 byte	0.0 byte	查看
WAN-1 eth2/eth2		100Mb/s 全双工	27.48 GB	44.89 GB	72.37 GB	525.06 KB	1.61 MB	2.12 MB	查看
WAN-2 eth3/eth3		100Mb/s 全双工	28.70 GB	48.49 GB	77.19 GB	642.09 KB	2.28 MB	2.91 MB	查看

这里WAN口的下行带宽总和应该和LAN口的上行带宽总和基本一致，WAN口的上行带宽总和和LAN口下行带宽总和基本一致

如出现不一致的状态，如LAN口总和远多于WAN口，如下图：

网络接口	状态	工作模式	累计下行/接收 bytes	累计上行/发送 bytes	总累计流量 bytes	即时下行速度 byte/s	即时上行速度 byte/s	总实时速度 byte/s	流量图
LAN-1 eth2/eth2		1000Mb/s 全双工	1.70 GB	11.06 GB	12.77 GB	111.37 KB	1.01 MB	1.12 MB	查看
WAN-3 eth0/eth0		100Mb/s 全双工	4.31 GB	802.13 MB	5.09 GB	443.49 KB	66.59 KB	510.09 KB	查看
WAN-4 eth1/eth1		100Mb/s 全双工	785.95 MB	711.54 MB	1.46 GB	21.03 KB	40.47 KB	61.50 KB	查看

则有如下可能：

- 路由开启了端口镜像功能，进入防火墙-端口镜像中查看：

系统设置

网络设置

防火墙

基本安全设置

黑白名单

IP-MAC 绑定

DNS/IP过滤

网址/关键字过滤

访问控制列表(ACL)

防火墙日志

端口镜像

端口镜像

端口镜像 (Port Mirroring) 功能可以让指定IP或协议的流量复制并转发到某一特定的IP(一般是监控机器). 此功能对网卡要求比较高, 且开启后对系统性能会有一定的影响, 尤其在网流量比较大的场合, 请谨慎使用!

☒ 启用端口镜像功能

ID	优先级	协议类型	数据流向	源IP/段:端口 目的IP/段:端口	管理IP	备注	激活/编辑/删除/选择			
1	1	TCP+UDP	LAN-to-WAN	ALL:ALL ALL:ALL	192.168.1.180	lan-wan				<input type="checkbox"/>
2	1	TCP+UDP	WAN-to-LAN	ALL:ALL ALL:ALL	192.168.1.180	wan-lan				<input type="checkbox"/>

全选/全不选

- 有大量不符合网络传输标准的数据包遭丢弃，信息监测-网络状态，看下面网络负载表格中出错/丢弃数量是否很大

网络负载 [会话数:3886]

设备名	连接状态	工作模式	连接速度	MTU	接收字节	发送字节	接收包	发送包	出错/丢弃
eth0	Up	全双工	1000 Mb/s	1500	102.81 GB	59.01 GB	0.13G	0.10G	64821/219532
eth1	Up	全双工	100 Mb/s	1500	31.32 GB	51.69 GB	54.01M	63.83M	0/0
eth2	Up	全双工	100 Mb/s	1500	30.22 GB	48.53 GB	51.63M	61.10M	0/0

如果这时路由接显示器，很可能会出现bad length 56byte的相关提示

- 内网有DoS/DDoS攻击，Web登录路由，将防护墙中攻击防护启用，如下图：

防火 墙

基本安全设置

黑白名单

IP-MAC 绑定

DNS/IP过滤

网址/关键字过滤

访问控制列表(ACL)

防火墙日志

端口镜像

NAT 策略

端口映射

DMZ 主机

UPnP 支持

一对一 NAT

No NAT规则

上网管理

服务应用

普通模式高级模式特殊应用

☐ 忽略来自 WAN 口的 PING 包 (禁止从外网 PING 服务器, 推荐选上)

☐ 禁止内网 PING 网关 (不允许局域网 PING 服务器, 不推荐开启)

☐ 完全关闭 PING 功能 (不响应所有 ICMP echo 请求, 不推荐开启)

☒ 启用 ICMP-Flood 攻击防御 (范围 10-10000):
每个IP每秒最大允许的 ICMP 包个数: 100 pps (推荐 50-150) , 突发数据包: 20 (推荐 10-30)

☒ 启用 DNS 攻击防御 (范围 10-10000):
每个IP每秒最大允许发起的 DNS 请求数: 50 (推荐 30-80) , 突发数据包: 30 (推荐 10-30)

☒ 启用 IP 碎片(Fragment) 攻击防御 (范围 10-10000)
每个IP每秒最大允许的 IP 碎片包个数: 80 pps (推荐 50-150) , 突发数据包: 20 (推荐 10-30)

☒ 启用 TCP SYN 连接数限制
每个IP每秒最大允许发起的 TCP 新连接数 120 (推荐 80-150)

☒ 启用 TCP 总连接数限制
每个IP最大允许的 TCP 总连接数: 200 (推荐 800-1500)

☒ 启用 UDP 总连接数限制
每个IP最大允许的 UDP 总连接数: 300 (推荐 800-1500)

防火 墙

基本安全设置

黑白名单

IP-MAC 绑定

DNS/IP过滤

网址/关键字过滤

访问控制列表(ACL)

防火墙日志

端口镜像

NAT 策略

普通模式高级模式特殊应用

☐ 防止外部 IP 地址欺骗 (伪造内网IP)

☐ 防止外部源路由欺骗 (伪造非法路由路径)


☐ 防止 ICMP 重定向欺骗 (不接受和发送 ICMP 重定向消息)

☐ 启用 ICMP 错误消息保护 (出错时不发送 ICMP 报文)

☒ 防止 Smurf DoS 攻击 (不响应 ICMP echo 广播和多播请求)

☒ 启用 SYN Cookie 功能 (有助于防止 SYN Flood 攻击)

路由上看NAT会话信息，找出过大不正常的主机。如还看不出来则利用第三方查找DOS/DDOS攻击源软件，查找出攻击的主机



注释

DDOS是英文Distributed Denial of Service的缩写，意即“分布式拒绝服务”。其攻击原理是通过很多“僵尸主机”向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝正常网络请求服务，导致合法用户无法正常访问服务器的网络资源。常见的DDOS攻击手段有SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Connections Flood、Script Flood、Proxy Flood等

第 79 章 内网ARP攻击检测与防护

部分 X. 常见问题



第 79 章 内网ARP攻击检测与防护

当内网出现上网变慢甚至断线，重启下路由或者核心交换机后暂时正常，过段时间又出现断网等症状。这时首先ping一下路由的LAN口IP地址如192.168.101.4

```
C:\Documents and Settings\Administrator>ping 192.168.101.4
Pinging 192.168.101.4 with 32 bytes of data:
Reply from 192.168.101.4: bytes=32 time<1ms TTL=64
Reply from 192.168.101.4: bytes=32 time<1ms TTL=64
Reply from 192.168.101.4: bytes=32 time<1ms TTL=64
Reply from 192.168.101.4: bytes=32 time<1ms TTL=64
```

图 79.1. ping LAN口

出现延时小于1ms都是正常状态，如果是出现延时过大甚至是超时：

```
C:\Documents and Settings\Administrator>ping 192.168.101.4
Pinging 192.168.101.4 with 32 bytes of data:
Reply from 192.168.101.4: bytes=32 time=45ms TTL=64
Reply from 192.168.101.4: bytes=32 time=295ms TTL=64
Request timed out.
Request timed out.
```

图 79.2. 内网非正常

这时如果重启一下路由器或者核心交换机设备，能够暂时正常一段时间；或者将一主机直连到路由LAN，直接PPPoE拨号到路由，然后ping下PPPoE拨号服务端那个IP，延时和上网都变稳定的话。就可以初步断定是ARP等内网攻击问题。

常用的解决方式有如下几种：

- Web登录海蜘蛛路由，进入信息检测-ARP攻击检测，勾选启用ARP攻击检测，隔一段时间后，将此详细日志查看一下，将异常的主机IP和MAC找出来，然后对应找到各个终端主机用户。

上网管理

服务应用

流量控制

信息监测

端口信息

硬件信息

网络状态

PPP 连接信息

在线 Web 用户

系统日志查看

统计报表

ARP & NAT

局域网扫描

ARP 高速缓存

ARP 攻击检测

☒ 启用ARP攻击检测 (建议开启, 此外您还可以在 [这里](#) 启用ARP广播)

状态: 运行中 (PID:4796) [详细日志](#) [清除](#)

= 2013-09-28 14:39:41 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1150

= 2013-09-28 14:49:08 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1200

= 2013-09-28 14:58:43 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1250

= 2013-09-28 15:07:39 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1300

= 2013-09-28 15:17:06 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1350

= 2013-09-28 15:26:45 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1400

= 2013-09-28 15:33:38 Query: 192.168.1.164 50-46-5d-67-59-e6 200

= 2013-09-28 15:35:51 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1450

= 2013-09-28 15:44:24 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1500

= 2013-09-28 15:53:37 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1550

= 2013-09-28 16:02:40 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1600

= 2013-09-28 16:11:37 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1650

2013-09-28 16:20:44 Alteration_IP: 50-46-5d-67-59-e6 changed from 192.168.1.164 to 192.168.0.164

= 2013-09-28 16:21:02 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1700

= 2013-09-28 16:30:22 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1750

= 2013-09-28 16:39:01 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1800

= 2013-09-28 16:47:57 Query: 192.168.1.132 00-1b-21-5c-f7-3a 1850

检测时间间隔: s (5~15)

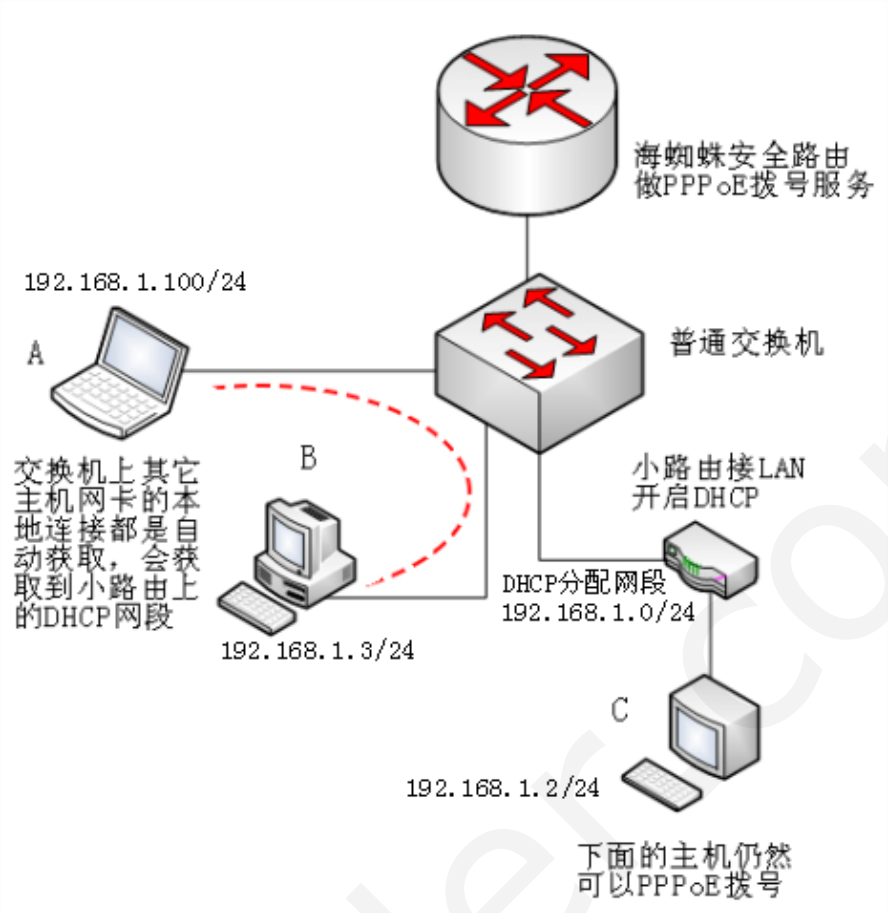
检测到ARP攻击时发送正确ARP数据包的个数: (30~100)

- 利用海蜘蛛海盾技术，将所有内网主机安装海盾客户端，然后进入路由防火墙-基本安全设置，在普通模式标签下启用海盾安全防护

☒ 启用海盾安全防护 (彻底防御ARP攻击、DoS/DDoS 流量攻击, 需在客户机安装海盾)

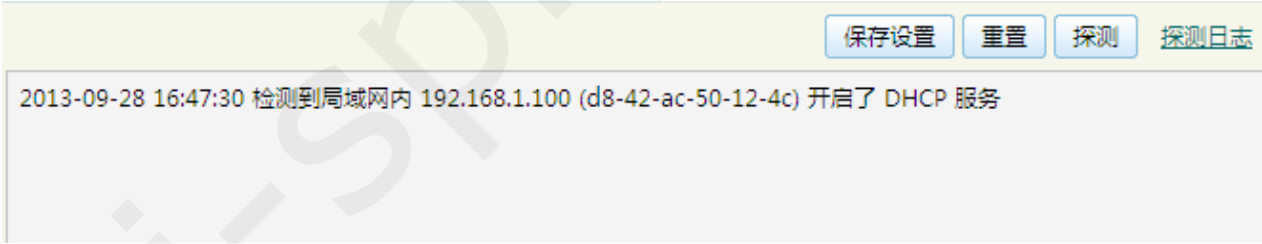
- 利用拨网线的方式一个个寻找，从核心交换机开始，拔掉一根网线后，内网其它用户到路由和上网都正常了，再接上就整个内网又产生大延时丢包，就基本可以确认是这根网线下的设备引起的，这样一级级地查找直到最终客户机。
- 将路由下的交换机等网络设备全部换成端口隔离交换机/VLAN交换机（每户一个VLAN）/DHCP-Snooping交换机

即使内网全部是PPPoE拨号用户，也有可能出现ARP攻击，如下图：



因为内网有其它设备提供DHCP或者各主机本身有自己的网卡本地连接IP地址，这几个主机A、B、C处于同一网段，即使这几个主机都PPPoE拨号到路由上网，但它们之间互访（例如192.168.1.2这个主机查找192.168.1.3）这个主机可以直接经过普通交换机，不经过路由，这样路由就没法控制它们之间的互访，下面主机就能够通过本地网卡IP找到对方进行攻击并影响拨号。

此时Web登录路由，进入服务应用-DHCP服务，点击下面的探测按钮，有可能会发现内网多个DHCP服务：



这时内网会有多个主机仍然有网卡本地连接的IP地址，并且它们都在同网段，仍然可以不经过路由互相广播查找到对方引起的。