UTT 3640VPN 防火墙

高级配置手册

上海艾泰科技有限公司

http://www.utt.com.cn

版权声明

产品编号（PN）：0900-0080-001

文档编号（DN）：PR-PMMU-1104.22-PPR-CN-1.0A

目 录

导　　读

提示：为了达到最好的使用效果，建议将 Windows Internet Explorer 浏览器升级到 6.0 以上版本。相关下载地址为：

http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=1E1550CB-5E5D-48F5-B02B-20B602228DE6

0.1　手册说明

本手册描述了 UTT3640 VPN 防火墙产品基于 ReOS_VSTART 软件平台的特性和功能，提供基于 WEB 界面的配置方法及其步骤。用户应保证所使用的软件版本与本手册所描述对象一致。由于产品版本升级或其它原因，本手册内容会不定期更新。

0.2　界面风格

WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框　　：选中代表只选用此项功能；

复选框　　：选中代表此选项所述功能被选中；

按钮　　：单击则执行该按钮的动作；

文本框　　：输入相关参数；

列表框　　：通过列表框可以找到供选择的选项；

下拉框　　：通过下拉框可以找到供选择的选项。

0.3　基本约定

0.3.1　列表功能详解

WEB 界面中的列表有可编辑列表和只读列表两种类型，下面分别举例进行说明：

0.3.1.1 可编辑列表

可编辑列表用来显示、编辑各种配置信息，能够编辑、删除列表中的选项，此处以“ DHCP 手工绑定信息列表 ”（如表 0-1）为例说明可编辑列表中各参数的含义。

表 0-1 DHCP 手工绑定信息列表

1/1 ：当前页面序号/总页面数，此处指第 1 页/共 1 页；

第一页 ：超链接，单击即可转到第一页；

上一页 ：超链接，单击即可转到上一页；

下一页 ：超链接，单击即可转到下一页；

最后页 ：超链接，单击即可转到最后页；

前往 第 页 ：在文本框中输入页码，再敲<Enter>键或者单击“ 前往 ”，即可跳到指定页面；

搜索 ：在搜索文本框中输入要查询的字符串，再敲<Enter>键，即可显示所有与该字符串匹配的条目，并且，还可以在搜索结果中继续搜索。搜索完毕后，如果需要查看列表全部信息，则需在空的文本框中直接敲<Enter>键。

注意，如果一个条目有一个参数的值含有指定字符串（即子串匹配）时，就认为该条目与该字符串匹配。

2/200 ：当前已设置数目/最多可设置数目，此处指当前设置了 2 个 DHCP 手工地址绑定条目，最多可设置 200 个条目；

编辑 ：超链接，单击即可进入相应编辑框；

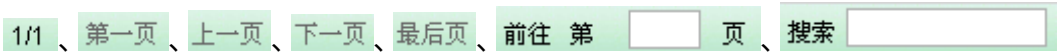
全选 /全不选 ：选中后（方框中出现“ √ ”），当前页面所有条目全部被选中；全选情况下，再单击该方框（方框变为空），当前页面所有条目全部未被选中；

删除 ：先选择某条（或多条）需要删除的条目（单击其首列中的方框，方框中出现“ √ ”，表示选中），再单击“ 删除 ”按钮，即可删除选中的条目。

0.3.1.2 只读列表

只读列表用来显示系统状态信息，不可编辑，此处以“ DHCP 地址池使用信息列表 ”（如表 0-2）为例说明只读列表中各参数的含义。

表 0-2 DHCP 地址池使用信息列表



涵义均同前；

：当前显示状态信息数/状态信息总数，此处指当前显示 DHCP 地址池使用信息 2 条/共 2 条。

0.3.1.3 列表排序功能

设备中，除了***安全配置***—>***防火墙***中的“ 防火墙信息列表 ”之外，WEB 界面的所有列表都支持排序功能。操作步骤如下：

在某个列表中，单击某列的标题，则按照该列数据对表中所有记录进行排序。第一次单击为降序，第二次单击为升序，第三次为降序，依次类推。每次排序后，列表重新从第一页开始显示。

0.3.2 符号约定

- 表示基本参数，描述参数基本涵义；

  如果界面中某参数中有“ * ”号，表示该参数为必填项目。例如，如图 0-1 所示，“ 主 DNS 服务器 ”有“ * ”号，代表在配置 DNS 服务器时，该参数必须配置。

图 0-1 DNS 服务器配置

- 表示按钮，描述操作动作；
- 表示提示，指出重点注意事项。

0.3.3 键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

0.3.4 其他表达约定

1. 进入某配置界面的表达方式

一级菜单名称—>二级菜单名称（斜体加粗字体）用来表示打开某配置界面的路径。例如，***系统管理—>时钟管理***表示在 WEB 界面中，首先单击一级菜单“ 系统管理 ”，之后再单击二级菜单“ 时钟管理 ”，就进入时钟管理界面了。

2. 进行某动作的表达方式

单击“ XXX ”按钮（XXX 表示按钮名），表示进行该按钮所对应的操作。例如，单击“ 删除 ”按钮，就表示进行相应的删除操作，“ 删除 ”对应按钮  。

3. 选中某选项的表达方式

选中“ XXX ”选项（XXX 表示选项名），表示选中该选项所对应的功能。例如，选中“ 启用 ARP 更新限制 ”选项，就表示 ARP 更新限制功能被启用，如图 0-2 所示。

图 0-2 启用 ARP 更新限制

0.4 出厂配置

1. 接口出厂配置如表 0-3 所示：

接口类型	IP 地址	子网掩码
LAN 口	192.168.16.1	255.255.255.0
WAN1 口	192.168.17.1	255.255.255.0
WAN2/DMZ 口	192.168.18.1	255.255.255.0
WAN3 口	0.0.0.0	0.0.0.0
WAN4 口	0.0.0.0	0.0.0.0

表 0-3 接口出厂配置

2. 系统管理员的用户名出厂设置为“ Default ”（区分大小写），出厂密码为空。

0.5 内容简介

本手册主要介绍 UTT 3640VPN 防火墙的各功能的配置及应用，主要包括：产品概述、硬件安装、开始菜单、快速向导、基本配置、系统管理、高级配置、系统状态、上网监控及带宽业务等。

第 1 部分 产品概述

主要介绍 UTT 3640VPN 防火墙的特点及功能特性。

第 2 部分 硬件安装

主要介绍 UTT 3640VPN 防火墙的安装步骤及注意事项。

第 3 部分 开始菜单

主要介绍了如何快速配置上网线路及一些必要的上网防范措施。通过导航条“ 开始菜单 ”可以快速接入下列页面进行相关配置：

- 线路配置上网（推荐）——点击即进入***基本配置—>线路配置***页面，进行上网线路配置；
- 不可不防（推荐）——点击即进入***基本配置—>安全专用配置***页面，进行必要的上网安全防范配置；
- 端口映射——点击既进入***高级配置—>NAT 和 DMZ 配置***页面，进行 NAT 和 DMZ 配置；
- 用户个性化配置——点击即进入***安全配置—>用户管理***页面，可以在该页面针对单个用户进行个性化配置；
- 组策略——点击即进入***高级配置—>组管理***页面，可以在该页面创建工作组和对该组用户设置组策略；
- 防火墙策略——点击即进入***安全配置—>防火墙***页面，可以在该页面设置对局域网用户上网行为的控制；
- 系统信息——点击既进入***系统状态—>系统信息***页面，可以在该页面查看系统的各种信息；
- ARP 欺骗防御——点击既进入***安全配置—>ARP 欺骗防御***页面 ;可以在该页面设置 ARP 欺骗防御。

第 4 部分 快速向导

主要介绍如何快速安装 HiPER，包括：

- 登录密码设置——设置系统新密码；
- 系统时钟配置——手工设置当前系统时间和日期；
- 上网接入线路配置——快速配置上网默认线路，HiPER 提供 PPPoE、动态 IP、固定 IP 这三种接入方式。

第 5 部分 基本配置

主要介绍产品的基本功能，包括：

- 线路配置——配置上网线路，查看线路连接信息；
- 线路组合——配置线路检测方法，选择线路组合方式，设置线路组合相关参数；
- DHCP 和 DNS 服务器——配置 DHCP 服务器、DNS 服务器及 DHCP 手工绑定，查看 DHCP 手工绑定信息以及 DHCP 地址池使用信息；
- 接口配置——配置 HiPER 物理接口的相关参数；

- DDNS 服务——申请、配置 DDNS 服务；
- 时间段配置——配置时间段实例。

第 6 部分 系统管理

主要介绍产品相关管理参数的设置，包括：

- 管理员配置——设置 WEB 管理员，提供三个管理员组：浏览、执行和系统管理；
- 时钟管理——手工或自动设置系统时间和日期；
- 软件升级——备份当前软件版本，下载最新软件进行升级；
- 配置管理——备份系统当前配置，恢复保存过的配置，恢复设备出厂配置；
- WEB 服务器——配置 WEB 服务器；
- SNMP 配置——配置 SNMP 服务；
- SYSLOG 配置——配置 SYSLOG 服务；
- 远程管理——配置远程管理，允许或禁止远程 HTTP、SNMP 或 TELNET 服务。

第 7 部分 高级配置

主要介绍产品的高级功能配置，包括：

- 组管理——定义局域网用户工作组，具有类似性质（如上网要求相同）的用户划分在同一个工作组，并对该组内的用户设置组策略；
- NAT 和 DMZ 配置——配置 NAT 规则、虚拟服务器、NAT 静态映射，查看 NAT 规则列表、NAT 静态映射列表。HiPER 提供 EasyIP、One2One 及 Passthrough 三种类型的 NAT 规则，支持配置多条 NAT 规则、多个虚拟服务器；
- 路由配置——配置静态路由，预先指定对某一网络访问时所要经过的路径；
- IP/MAC 绑定——配置 IP/MAC 绑定用户，防止 IP 地址盗用，配置上网“ 黑名单 ”和“ 白名单 ”；
- 特殊功能——配置快速转发、虚拟局域网及端口镜像；
- DHCP——在指定端口配置 DHCP 服务器功能、DHCP 客户端功能或 DHCP 中继功能，各端口均支持三种 DHCP 功能；
- UPnP——启用 UPnP 服务，查看通过 UPnP 建立起来的 NAT 静态映射信息。

第 8 部分 系统状态

主要介绍如何查看系统相关状态信息，包括：

- 用户统计——查看局域网用户的上传和下载数据包的统计信息；
- NAT 统计——查看针对 NAT 的局域网主机的特别信息，用以发现用户在使用 Internet 过程中发生的 DDoS 攻击，巨量下载，过分占用 Internet 带宽等情况；
- DHCP 统计——查看 DHCP 地址池、DHCP 地址冲突信息，查看各端口作为 DHCP 服务器、DHCP 客户端及 DHCP 中继的统计信息；
- 接口统计——查看 HiPER 各物理接口的统计信息，比如接收、转发数据包的速率，经各端口数据包的统计等；
- 路由和端口基本信息——查看当前使用的路由信息，查看端口配置及工作状态；
- 系统信息——查看系统的版本信息、运行时间、资源使用状态、告警信息及历史记录等；

第 9 部分 上网监控

主要介绍如何监控局域网用户的上网状况，可以根据源地址、目的地址/域名、NAT 地址/域名、目的端口、全部记录以及自定义的“ 线路名称 ”等条件查询局域网用户的上网情况。

第 10 部分 带宽业务

主要提供带宽信用管理功能，有效抑制 BT、比特精灵等 P2P 软件对带宽的滥用，确保正常的商业应用，并大大提高带宽利用率。

第 11 部分 安全配置

主要介绍安全配置相关功能，包括：

- 基本选项——提供基本的网络安全防御配置，用来提升网络的安全性，还可以禁止用户使用 QQ/MSN/P2P 等软件；
- 用户管理——可以查看当前所有用户的状态信息，还可以针对每个用户进行个性化配置、以及 IP/MAC 绑定配置；
- 策略库——可以查看各个策略库实例的相关信息，还允许加载、更新策略库实例；
- ARP 欺骗防御——可以有效防御 ARP 欺骗攻击，还可以一次将内网所有开启 PC 的 IP/MAC 地址对全部绑定；
- DDoS 攻击防御——可以有效防御内网 DDoS 攻击；
- 防火墙——提供“普通”和“视图”两种模式进行防火墙策略配置，可实现对设备所有物理接口的进入和外出数据包进行控制；
- 地址组——配置防火墙策略所要引用的地址组，可包含多个不连续的 IP 地址段或其他地址组；
- 服务组——可配置五种不同类型的服务组被防火墙策略引用，一个服务组可包含多个服务或其他服务组。

第 12 部分 附录

本手册共提供 6 个附录，描述如下：

- 附录 A 配置局域网中计算机——提供配置局域网计算机的 TCP/IP 属性的方法。
- 附录 B FAQ——提供常见问题解答；
- 附录 C 常用 IP 协议号——提供常用 IP 协议号与协议名对照表；
- 附录 D 常用服务端口号——提供常用服务端口号及服务名对照表；
- 附录 E 图索引——提供本手册所有图的索引目录；
- 附录 F 表索引——提供本手册所有表的索引目录。

第1章 产品概述

非常感谢您选用上海艾泰科技有限公司的 UTT 3640VPN 防火墙产品。
本章主要讲述 UTT 3640 的功能和特点。

1.1 关键特性

- 支持 DSL，FTTX+LAN 和 Cable Modem 等多种宽带接入方式
- 支持快速转发，性能优异
- 支持多线路负载均衡和实时备份；还支持网通、电信智能策略路由，实现电信流量走电信、网通流量走网通）
- 内置防火墙，能够有效防止 ARP 欺骗、端口扫描、DoS/DDoS、冲击波、震荡波等病毒攻击
- 支持 NAPT、NAT 以及路由的混合使用
- 支持 NAT 静态映射，支持 DMZ 主机
- 支持 NAT 会话数限制，可限制单机会话数；提供内网主机 NAT 会话数排行榜
- 支持带宽管理，可限制单机带宽；提供内网主机上传/下载速率排行榜
- 支持单键管制 QQ/MSN/P2P
- 基于地址、协议和端口的包过滤
- 基于 MAC 地址的过滤
- 基于站点、关键字、DNS 和 URL 的应用层过滤
- 支持个性化配置，提供按需定制的个性化服务
- 提供全局、工作组、个人三级管理体系，灵活管理内网用户
- 支持 IP/MAC 绑定，可设置上网黑名单和白名单；还支持 IP/MAC 全部绑定和自动绑定功能，配置更加简单智能
- 支持 DHCP 服务器和客户端功能，支持 DHCP 手工绑定；部分产品还支持 DHCP 中继功能
- 支持时间段管理
- 支持网络时间同步
- 支持 DDNS
- 基于端口的 VLAN
- 支持 UPnP
- 支持端口镜像
- 支持 MAC 地址克隆
- 支持静态路由，动态路由 RIP I 和 RIP II
- 支持多个 L2TP/PPTP/IPSec 的 VPN 穿透
- 提供基于 WEB UI 和命令行（CLI）的配置界面，支持远程管理
- 提供标准的 SNMP 接口，可供远程 SNMP 服务器管理
- 提供系统日志功能，可通过远程 SYSLOG 服务器记录
- 支持配置文件备份与导入

- 支持 WEB、TFTP 多种升级方式，方便功能扩展
- 提供多种监控和诊断方式，可动态监控网络运行情况、用户上网行为

1.2　主要特点

1. 局域网接口（LAN）

- 多端口交换机：集成了多端口 10/100Mbps 自适应交换机（MDI/MDI-X 自适应）。
- 支持 DHCP Server：支持 DHCP Server 功能，给局域网中的计算机动态分配 IP 地址以及网关、DNS Server 等信息。
- 支持多网段：支持静态路由和动态路由（RIP I，RIP II），可以连接多个不同的网段。
- 基于端口的 VLAN：一个 VLAN 组成一个逻辑子网，即一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信；不同的 VLAN 之间实现物理隔离。
- 端口镜像：LAN 口的端口 1 为镜像端口，可将其他端口的流量自动复制到镜像端口，以便网络管理人员进行流量监控、性能分析和故障诊断。

2. 广域网接口（WAN）

- 支持多 WAN 口：多个 10/100M 自适应广域网接口（MDI/MDI-X 自适应）。
- 支持 DSL 或者 Cable Modem：HiPER 系列产品通过了市场上众多厂商的 DSL Modem 和 Cable Modem 的兼容性测试。
- 支持 PPPoE：每个广域网接口都支持使用 PPPoE（PPP over Ethernet）协议和 ISP 连接。
- 共享 Internet 访问：局域网的所有用户可以通过 NAT（Network Address Translation）共享多条 Internet 线路上网。
- 支持线路备份和负载均衡：支持多 WAN 口流量负载均衡以及线路冗余备份。

3. IP/MAC 绑定和业务控制

- 支持 IP 地址和 MAC 地址绑定。
- 支持多种 Internet 业务的管理与控制。
- 支持 Internet 不良地址过滤。
- 支持站点、关键字和 URL 过滤。
- 支持按时间段策略控制上网。

4. IP QoS 功能

- CBT 功能可抑制 BT 等 P2P 软件对带宽的大量占用，保证用户对带宽的正常使用，还可以按时间段进行控制。

5. 配置和管理

- 简易配置：基于 Web UI 或者命令行（CLI）的配置界面，方便管理和配置。
- 开始菜单：提供常用页面导航功能，可通过它快速地配置线路上网、基本的病毒防御等。
- 远程管理：在局域网或者广域网上的任何一台计算机上均可实现对设备的远程管理。

6. Internet 高级特性

- 虚拟服务器（DMZ 主机）：支持配置多台 DMZ 主机，DMZ 主机将完全暴露在 Internet 上，方便远程用户访问。
- NAT 静态映射：支持用户自定义多条 NAT 静态映射，方便远程用户访问内部服务器的指定服务端口。
- 高级 DHCP 功能：各端口均支持 DHCP Client、DHCP Server 及 DHCP Relay。DHCP Server 支持配置多个不同地址段的地址池，并提供灵活、充分的地址分配策略，与 DHCP Relay 结合起来，完全能够满足用户的各种需求。
- 特殊应用程序支持：支持一些特殊的 Internet 应用程序（例如腾讯 QQ、网络游戏、视频程序、音频程序）的使用。
- DDNS：支持动态域名服务。
- 快速转发：可以实现各个物理接口数据的快速转发，全面提高性能。
- 带宽信用管理：通过带宽信用管理（CBT）功能实现对内网主机上传/下载速率的控制。

7. 安全特性

- 配置文件：设置管理员口令，可以防止未被授权的用户修改设备的配置。备份配置文件，可以防止配置的意外丢失。
- 访问控制：管理员可以限制局域网中的某些用户对 Internet 或者是 Internet 某些服务的访问。
- 实时监控：管理局域网内的流量和用户，及时发现网络异常以及异常用户。
- 防火墙保护：设备可监控所有来自局域网和 Internet 的包，对局域网用户的上网行为进行控制，过滤所有对局域网内服务器的非法请求，过滤黑客软件对局域网 IP 地址和端口的扫描，以防止外来的恶意攻击。防止 DoS/DDoS 攻击。允许设置上网黑名单和白名单，支持基于包过滤技术和应用层过滤技术的防火墙功能。

1.3　VPN 功能

此外，UTT 3640 提供全面的 VPN 功能，支持 IPSec、L2TP 及 PPTP VPN，它们还可结合使用。

- 支持使用动态地址构建 VPN 隧道
- 可实现网关到网关的 VPN
- 可实现远程拨号的 VPN
- L2TP/PPTP 服务器
- L2TP/PPTP 客户端
- IPSec 具有以下重要特点：
  1. 基于预共享密钥的 IKE
  2. 手动密钥通道
  3. AH、ESP 协议
  4. DES，3DES 和 AES 128 位、AES 192 位及 AES 256 位加密
  5. SHA-1 和 MD5 数据完整性认证
  6. 主模式和野蛮模式
  7. NAT 穿透
  8. 抗重播

1.4　规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由、RIPI/II、SNMP（MIB II）等协议。
- 各个物理端口均支持自动协商功能，自动调整传输方式和传输速度。
- 各个物理端口均支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃
  高度：0-4000m
  相对湿度：10-90%，不结露

第2章 硬件安装

本章主要讲述如何安装 UTT 3640VPN 防火墙及注意事项。

2.1 安装准备

1. 10/100M 以太网和 TCP/IP 协议。
2. 准备 DSL 或者 Cable Modem，并从 ISP 那里获得访问 Internet 的用户名和密码。

2.2 安装流程

在安装设备之前，必须保证设备的电源是关闭的。安装流程如下：
第一步，选择安装地点，一般是将设备安装在工作台上，也可将设备安装在标准机架上。
第二步，建立设备与局域网的连接，即将管理计算机或交换机连接到设备的局域网端口。
第三步，建立设备与广域网的连接，即将 Cable/DSL Modem 连接到设备的广域网端口。
第四步，打开电源，打开电源之前确保电源供电、连接、接地正常。
第五步，检查系统指示灯，查看设备的连接及工作状态是否正常。

2.3 UTT 3640 安装步骤

1. 选择安装地点

在安装前需选择一个适当的地方安装 UTT 3640，确保其电源是关闭的。UTT 3640 是按照 19 英寸标准机架的尺寸进行设计的，一般可以将其安装到机架上，也可将其安装在工作台上。

1) 安装到机架

将 UTT 3640 安装到 19 英寸标准机架上，如图 2-1 所示，可根据机架的情况使用随机附带的固定附件进行安装。

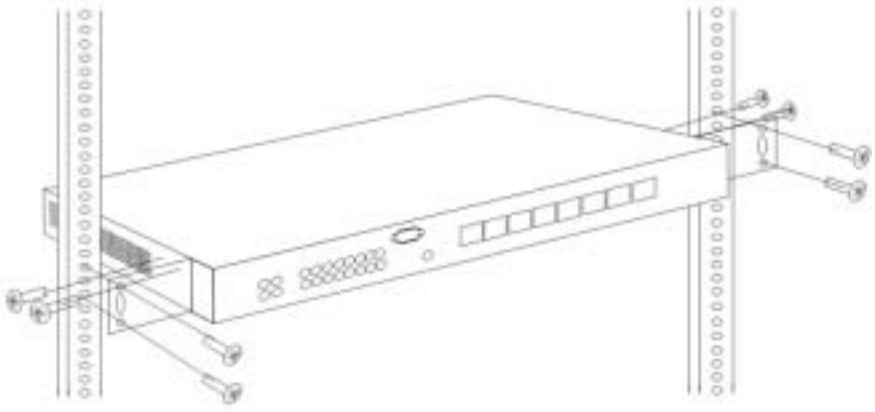


图 2-1 将 UTT 3640 安装到机架

2) 安装到工作台

若没有 19 英寸标准机架，可直接将 UTT 3640 放置在干净的工作台上。

注意：请保证工作台的平稳性和良好接地，同时不要在 UTT 3640 上面放置重物。

2. 连接 UTT 3640 到管理计算机或局域网

使用标准的网线连接管理计算机到 UTT 3640 的局域网（LAN）口，或者连接交换机到 LAN 口，如图 2-2 所示。UTT 3640 将会自动适应 10M 或者是 100M 的局域网设备。

图 2-2 建立局域网和广域网连接

3. 连接 UTT 3640 到 Internet

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 UTT 3640 的广域网口，如图 2-2 所示。如果没有厂商提供的网线，请使用标准网线。

4. 打开电源

将随机配置的电源线连接到 UTT 3640 的电源接口（位于后面板），并将位于后面板的电源开关打开。

注意！连接电源之前确保电源供电、连接、接地正常，否则可能造成系统工作异常或系统损坏。

5. 检查系统指示灯

系统指示灯位于前面板左边，分为 2 组（如图 2-3）：第一组是左边的 2 行 2 列，共 4 个，具体状态如表 2-1 所示；第二组是右边的 2 行 8 列，共 16 个，1-4 对应 LAN 口的四个交换口，5 对应 WAN1 口，6 对应 WAN2，7 对应 WAN3 口，8 对应 WAN4 口，具体状态如表 2-2 所示。

图 2-3 系统指示灯

指示灯	启动时状态	启动后状态
SYS	启动 1 秒后，先快速闪烁 1 秒，熄灭 2 秒后开始以每秒 2 次的频率闪烁	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮或常灭
PWR	常亮	电源工作正常时常亮
TRF	启动时亮	有网络流量时闪烁，无流量时灭
FLT	启动时亮	常灭；有故障时闪烁，闪烁一定次数后重启

表 2-1 前面板第一组指示灯

指示灯	启动时状态	启动后状态
Link/Act	上排灯闪烁后熄灭	当有设备连接到相应端口，协商成功，该端口对应指示灯长亮，该端口有网络流量时闪烁
100Mbps	上排灯熄灭后，下排灯闪烁后熄灭	当有设备连接到相应端口，100M 协商成功，该端口对应指示灯常亮

表 2-2 前面板第二组指示灯

6. Reset 按钮

Reset 按钮指复位按钮。在忘记管理员口令时可以通过此按钮来恢复设备的出厂配置。操作方法为：在带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，UTT 3640 将恢复到出厂配置，并自动重启。

第3章 开始菜单

开始菜单位于 WEB 界面的一级菜单栏的最左边，它提供了快速进入其他页面的接口，通过***开始***菜单，用户可以快速配置上网所需要的基本参数、必要的安全防范措施及查看路由器的相关状态信息等。

3.1 配置正确的网络设置

在通过 WEB 界面登陆到设备之前，首先要对管理计算机进行正确的网络设置。

首先将计算机连接到设备的某个局域网端口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，请参考附录 A。如果已经正确设置完成，请跳过此步。

第二步，设置计算机的 IP 地址为 192.168.16.2-192.168.16.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.16.1（设备的 LAN 口 IP 地址），DNS 服务器为当地运营商提供的地址。

第三步，使用 Ping 命令检查计算机和设备之间是否连通。下面的例子是在 Windows XP 环境中，执行 Ping 命令：**Ping 192.168.16.1**

如果屏幕显示如下，表示计算机已经成功和设备建立连接。

```
Pinging 192.168.16.1 with 32 bytes of data:

Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

如果屏幕显示如下，表示计算机和设备连接失败。

```
Pinging 192.168.16.1 with 32 bytes of data:

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

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

连接失败时，请做以下检查：

1. 硬件连接：设备面板上与该局域网端口对应的 Link/Act 指示灯和计算机上的网卡灯必须亮。

2. 计算机 TCP/IP 属性的配置：如果设备的 IP 地址为 192.168.16.1，那么计算机的 IP 地址必须为 192.168.16.2-192.168.16.254 中的任意一个空闲地址，即计算机的 IP 地址必须和设备的 LAN 口地址在同一个 IP 子网内。

3.2 开始菜单

计算机如果是使用 MS Windows、Macintosh、Unix 或者是 Linux 等任何操作系统，都可以通过浏览器（Internet Explorer 或 Netscape Communicator）来对设备进行配置。

打开浏览器，在浏览器的地址栏里输入设备的 IP 地址，例如 192.168.16.1，如图 3-1 所示。

连接建立起来之后，将会看到如图 3-1 所示的登录界面。首次使用时需要以系统管理员的身份登录，即在该登录界面输入系统管理员的用户名和密码（用户名的出厂设置为“ Default ”，密码的出厂设置为空），然后单击“ 确定 ”按钮。

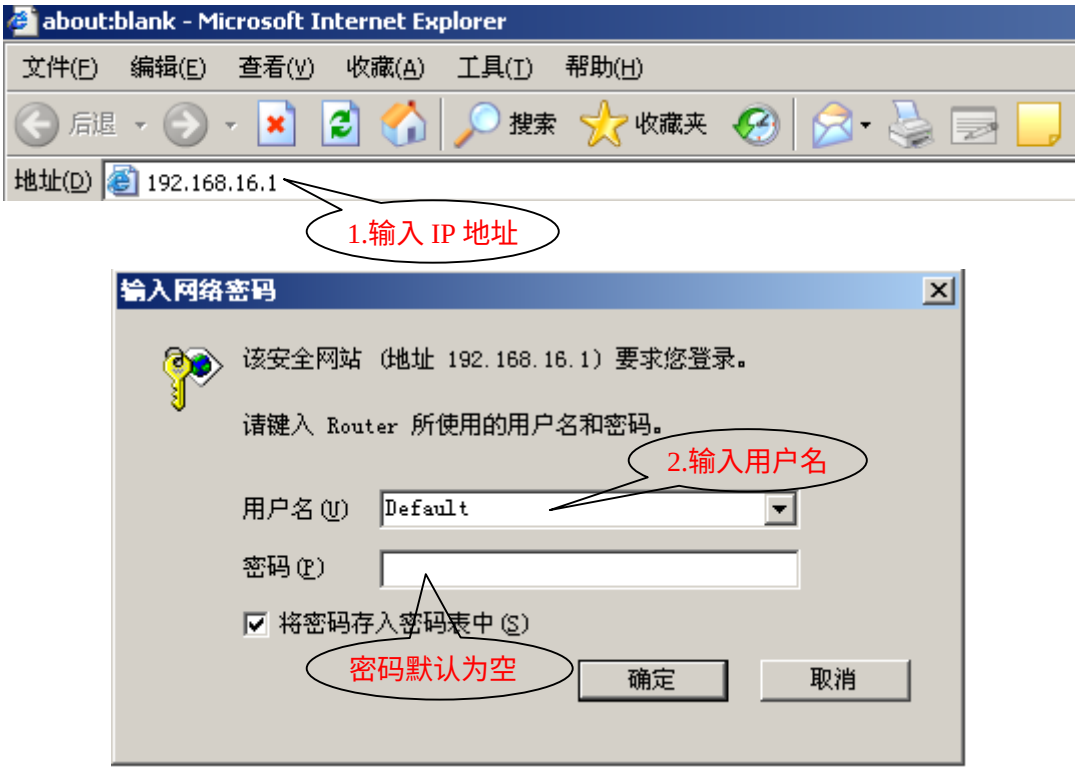


图 3-1 WEB 登录界面

如果用户名和密码正确，浏览器将显示管理员模式的首页，该页面右上角显示系统型号及版本信息。在首页中，针对每个一级菜单，都提供一个图标，单击某个图标即可进入相关页面。

若用户还没配置任何上网线路，系统将显示提示信息 “ 欢迎使用设备！您还没有配置任何线路，请点击“ 开始 ”菜单进行配置 ”，如图 3-2 所示。

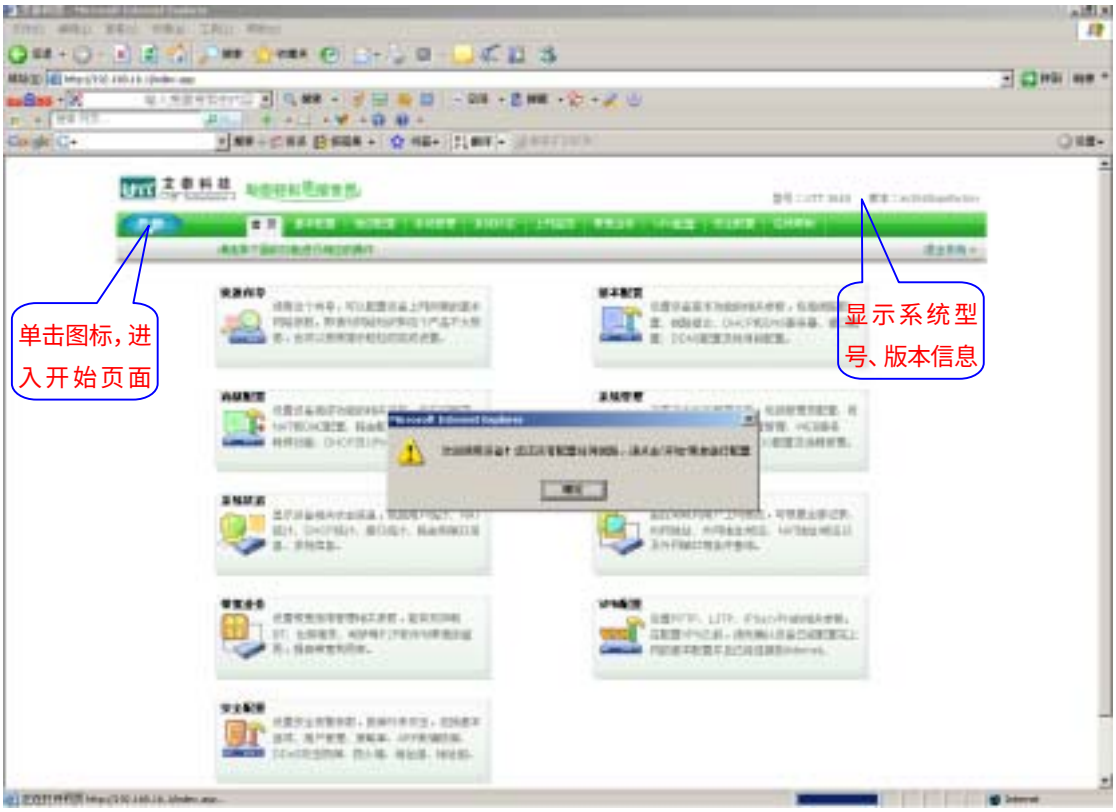


图 3-2 WEB 界面首页

图 3-3 开始菜单的子菜单

单击“确定”，开始菜单下即显示“线路配置上网、不可不防、端口映射、用户个性化配置、分组策略、防火墙策略、系统信息以及 ARP 欺骗防御”8 个子菜单（如图 3-3 所示），通过这些子菜单可以进行快速上网配置。单击各子菜单，即可进入各子菜单对应的页面进行相应的配置。

3.2.1 线路配置上网

单击***线路配置上网，***则转到***基本配置—>线路配置***页面，在该页面不仅可以配置多条线路，也可以根据实际需要修改或删除已配置的线路，还可以查看各条线路的连接状态信息（具体的配置方法及各参数的涵义见***基本配置—>线路配置***<章节 5.1>，这里不重复介绍）。

只有在配置完“ 默认线路 ”之后，才能配置其他上网线路。当配置完默认线路后，系统会提示“ 您需要配置其它线路吗？ ”（如图 3-4 所示）。

图 3-4 提示信息 1

图 3-5 提示信息 2

如果你还需要配置其他上网线路，则单击“ 是 ”进入***基本配置—>线路配置***页面继续配置其他上网线路 ;在配置完上网线路后，建议您进入***不可不防***页面进行必要的安全防御配置。在系统弹出的对话框 “ 将转入“ 不可不防 ”，进行必要的安全防御措施 !”（如图 3-5 所示）中，单击“ 确定 ”则转入***开始—>不可不防***页面。

3.2.2 不可不防

该页面提供上网必要的安全防范措施，包括病毒防御、速率限制，如果是双线路上网，还提供双线路路由配置。

如果用户未配置任何线路而直接进入本页面，系统会提示“ 请先配置默认线路 ”，单击“ 确定 ”，跳转到***基本配置—>线路配置***页面进行上网线路配置。

3.2.2.1 双线路路由配置

在本页面可以进行双线路路由配置，用户可以通过“ WAN1 口/WAN2 口运营商选择 ”选择相应的运营商，系统将根据用户的选择生成相对应的路由，比如电信生成电信路由，网通生成网通路由。

通过 WAN1 口/WAN2 口运营商选择，可以方便地实现电信流量走电信线路，网通流量走网通线路，如图 3-6 所示。

图 3-6 双线路路由配置

- WAN1 口运营商选择：选择 WAN1 口运营商，有三个可选项分别为电信线路、网通线路及其他线路，此处选择电信线路，表示电信流量走 WAN1 口；
- WAN2 口运营商选择：选择 WAN2 口运营商，有三个可选项分别为电信线路、网通线路及其他线路，此处选择网通线路，表示网通流量走 WAN2 口。

3.2.2.2 病毒防御

本页面提供基本的网络安全防御配置，用来提升网络的安全性。通过在本页面进行简单地配置，可以有效防御 ARP 欺骗、DoS/DDoS 攻击、冲击波以及震荡波等常见病毒攻击，为用户提供一个健壮、安全的网络环境。

图 3-7 病毒防御

- 启用 ARP 欺骗防御：打勾表示启用，启用后，并将局域网所有 PC 的 IP/MAC 地址对全部绑定，设备就可以有效防御内网 ARP 欺骗攻击了；
- 启用 IP/MAC 自动绑定功能：打勾表示启用，启用后，系统将每隔一小时自动执行

一次网络扫描，并将局域网所有开启 PC 的 IP/MAC 地址对全部绑定；

- 启用冲击波等病毒防御：打勾表示启用，启用后， 设备 将有效防御冲击波、震荡波等常见病毒攻击。启用此功能后，设备将直接丢弃 LAN 口接收到的协议为 TCP，目的端口为 135、136、137、138、139、445、1025、5554、9996 的数据包，此时，局域网主机将无法访问外网主机提供的相关端口服务，例如 windows 文件共享服务、打印共享服务等；
- 启用 DDoS 攻击防御：打勾表示启用，启用后，设备 将有效防御内网常见的 DoS/DDoS 攻击。目前，只能防御伪造源地址攻击。启用此功能后，设备将只允许源 IP 地址与 LAN 口 IP 地址在同一个网段的数据包通过，此时，三层交换机后的主机将不能通过设备访问外网。

提示：“IP/MAC 自动绑定功能”提供的是自动绑定功能，对于内网主机地址经常发生变化的网络，建议不要使用此功能。若需手动绑定，请到***安全配置—>ARP 欺骗防御***中进行配置，配置方法请参见章节“11.4 ARP 欺骗防御”。

3.2.2.3 速率限制

速率限制主要就是用来控制内网主机的流量，通过限制内网主机的最大下载/上传速率，来控制下载/上传的流量，并确保用户或者应用不会超过所分配的最大下载/上传速率，或者独占网络带宽，简单地说，通过速率限制功能可以限制局域网内每台主机可以使用的最大带宽。

图 3-8 速率限制

- 内网每台 PC 最大下载速率：内网每台主机的最大下载速率（单位：比特/秒）。其中，选项“NoLimit”表示不限制，即在下载方向不启用速率限制功能，“Block”表示禁止传送；
- 内网每台 PC 最大上传速率：内网每台主机的最大上传速率（单位：比特/秒）。其中，选项“NoLimit”表示不限制，即在上传方向不启用速率限制功能，“Block”表示禁止传送。
- 保存：单击保存按钮，双线路路由配置、病毒防御及速率限制的配置生效，同时系统会自动启用网络时间同步（sntp）功能（也可到***系统管理—>时钟管理***中启用此功能）；
- 重填：恢复到修改前的配置参数。

提示：如何设置每台 PC 最大下载速率和最大上传速率请参见章节“10.1 带宽信用管理”，这里不再重复描述。

3.2.3 端口映射

单击***开始—>端口映射***即可转到***高级配置—>NAT 和 DMZ 配置***（章节 7.3）页面，在该页面可以进行 NAT 规则配置、NAT 全局配置、NAT 静态映射配置，还可以在“ NAT 规则列表 ”和“ NAT 静态映射列表 ”中查看已配置的相关信息。

提示：具体的配置方法及参数解释请参见章节“ 7.3 NAT 和 DMZ 配置 ”，这里不再重复描述。

3.2.4 用户个性化配置

单击***开始—>用户个性化配置***即可转到***安全配置—>用户管理***（章节 11.2）页面，在***安全配置—>用户管理***的“ 用户管理信息列表 ”中，单击某条用户记录的“ IP 地址 ”或者“ 编辑 ”超链接之后，方可进入***用户信息配置***页面。在该页面可以进行用户个性化配置，个性化配置包含以下参数：禁止 QQ、禁止 MSN、禁止 P2P、启用 NAT 会话数限制、最大会话数、最大 TCP 会话数、最大 UDP 会话数、最大 ICMP 会话数、昵称、最大下载速率、最大上传速率、最小下载速率、最小上传速率及信用额度。

提示：用户个性化配置的具体方法及相关参数涵义请参见章节“ 11.2.2.1 个性化配置概述 ”，这里不再重复描述。

3.2.5 组策略

单击***开始—>组策略***既可转到***高级配置—>组管理***（章节 7.1）页面，在该页面我们可以将具有共同性质（如业务要求相同）的用户划分在同一个工作组中，并给他们分配连续的 IP 地址，还可以为该组配置组策略，组策略对该组内的所有用户生效。

提示：具体的配置请参见章节“ 7.1 组管理 ”，这里不再重复描述。

3.2.6 防火墙策略

单击***开始—>防火墙策略，***即可转到***安全配置—>防火墙***（章节 7.2）页面，在本页面可以定义若干防火墙策略，从而对流入和流出设备物理接口的数据包进行控制。

提示：相关参数的解释请参见章节“ 11.8 防火墙 ”，这里不再重复描述。

3.2.7 系统信息

单击***开始—>系统信息***，即可转到***系统状态—>系统信息***（章节 8.6）页面，在该页面管理员可以查看系统运行时间、版本及资源状态、端口状态、系统告警信息以及系统历史记录。

提示：相关参数的解释请参见章节“ 8.6 系统信息 ”，这里不再重复描述。

3.2.8 ARP 欺骗防御

单击***开始—>ARP 欺骗防御，***即可转到***安全配置—>ARP 欺骗防御***（章节 11.4）页面，通过在该页面进行简单地配置，就可以有效防止 ARP 欺骗攻击了。

提示：相关参数解释及配置步骤请参见章节“ 11.4 ARP 欺骗防御 ”，这里不再重复描述。

第4章 快速向导

通过阅读本章内容，可以设置设备上网所需的基本网络参数，快速地将设备连接到Internet。如果已经通过开始菜单配置了上网线路，在该页面就无需再配置上网线路。

在进入快速向导配置“ 上网默认线路 ”之前，应正确配置局域网中计算机的网络设置，具体方法见“ 章节 3.1 配置正确的网络设置 ”。

4.1 快速向导

在 WEB 首页单击“ 快速向导 ”图标，进入“ 快速向导 ”设置界面。快速向导提供配置设备的最基本功能，如登录密码、系统时钟、默认线路接入配置等。

4.1.1 登录密码设置

设备出厂的管理员（Default）密码为空，建议修改设备管理员密码并妥善保管，以提高设备的安全性。修改管理员密码后，以 Default 身份登录设备，必须使用新的密码，如图 4-1 所示。

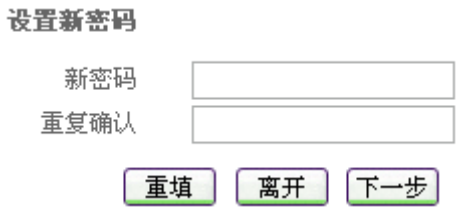


图 4-1 登录密码设置

- 新密码：登录密码；
- 重复确认：登录密码（此处必须和上一栏所填密码一致）；
- 重填：恢复到修改前的密码；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第二页。

提示：

1. 输入密码和确认密码必须一致。请妥善保管新密码，并且不要轻易告诉别人。如果丢失密码，将不能登录设备，必须将设备恢复到出厂配置。
2. 如果不需要更改密码，请直接点击“ 下一步 ”按钮！

4.1.2 系统时钟配置

在修改登录密码页面中，单击“ 下一步 ”按钮，进入修改系统时钟页面（如图 4-2），在这里可以配置系统日期与系统时间。

图 4-2 系统时钟设置

- 系统日期：当前日期，单位为年、月、日；
- 系统时间：当前时间，单位为时、分、秒；
- 上一步：返回到快速向导的第一页；
- 重填：恢复到修改前的系统日期和时间；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 下一步：进入快速向导的第三页。

提示：请正确设置系统时间，设备提供了 DDNS 功能（参见***基本配置—>DDNS 配置***）和上网时间段管理功能（参见***基本配置—>时间段配置***），如果时间设置不正确，将导致 DDNS 功能和时间段管理功能不能正常工作。

4.1.3 上网接入方式设置

在修改系统时钟页面中，单击“ 下一步 ”按钮，进入上网接入方式页面（如图 4-3）。设备支持以下三种常用的上网方式，可以根据实际情况进行选择。

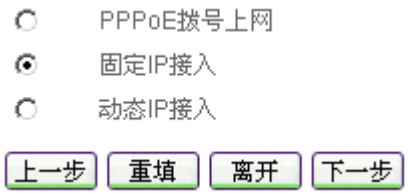


图 4-3 上网接入方式设置

- PPPoE 拨号上网：ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号）；
- 固定 IP 接入：以太网宽带接入方式，ISP（例如中国电信）提供静态的 IP 地址；
- 动态 IP 接入：以太网宽带或者有线通信接入方式，ISP（例如中国电信）通过 DHCP 服务为用户分配 IP 地址。
- 上一步：返回到快速向导的第二页；
- 重填：恢复到修改前的默认线路接入方式；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；

- 选中“ PPPoE 拨号上网 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页 PPPoE 拨号页面；
- 选中“ 固定 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页固定 IP 接入页面；
- 选中“ 动态 IP 接入 ”选项，单击“ 下一步 ”按钮，即可进入快速向导的第四页动态 IP 接入页面。

4.1.4 上网接入线路配置

4.1.4.1 上网接入线路配置的注意事项

1. 通过快速向导配置的上网线路的名称缺省为“ 默认线路 ”，并且，它固定连接到设备的 WAN1 接口；可以在***基本配置***—>***线路配置***的“ 线路连接信息列表 ”中，查看“ 默认线路 ”的配置和状态信息。

2. 如果改变了设备的“ 局域网 IP 地址 ”，系统会出现对话框显示“ 局域网 IP 地址已变为 xxxx ”，“ xxxx ”为更改后的 IP 地址，在完成本向导之后，必须使用新的 IP 地址重新登录设备，才能进行 WEB 界面管理；并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

3. 如果发现完成配置后不能上网，请检查各项配置是否正确；也可以直接到***基本配置***—>***线路配置***中检查线路状态，查看、修改配置参数。

4.1.4.2 PPPoE 拨号上网配置

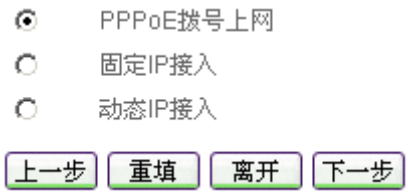


图 4-4 PPPoE 拨号上网方式

在选择上网接入方式页面中，选中“ PPPoE 拨号上网 ”选项，如图 4-4 所示。单击“ 下一步 ”按钮，进入 PPPoE 配置页面（如图 4-5），配置 PPPoE 信息，单击“ 完成 ”按钮，PPPoE 拨号上网线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

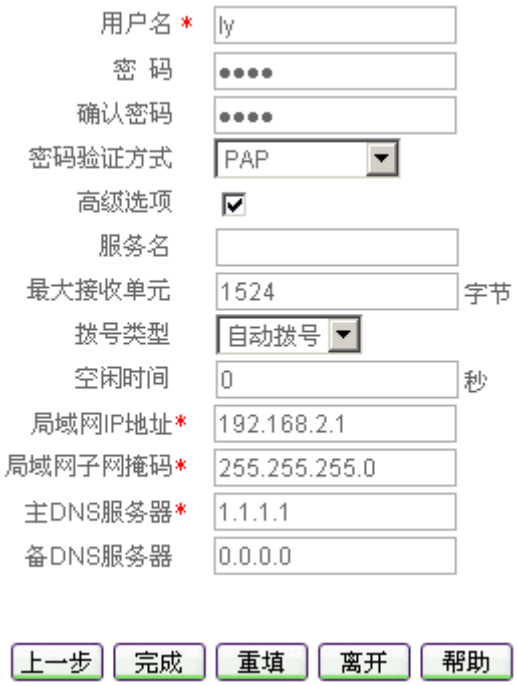


图 4-5 PPPoE 拨号配置

- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码（如有疑问，请询问 ISP）；
- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式（如有疑问，请询问 ISP）；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置（如有疑问，请询问 ISP）；
- 最大接收单元：缺省值为 1524 字节，PPPoE 拨号时设备将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：
  自动拨号：当开启设备或者上一次拨号断线后自动拨号连接；
  手动拨号：在***基本配置—>线路配置***的“ 线路连接信息列表 ”中手动进行连接和挂断；
  按需拨号：在局域网内部有访问 Internet 流量时设备自动进行连接；
- 空闲时间：在没有访问 Internet 流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。

- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的 PPPoE 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

4.1.4.3 固定 IP 接入配置

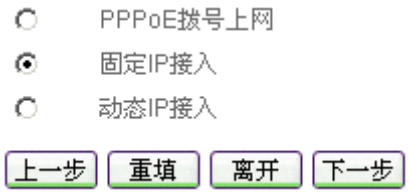


图 4-6 固定 IP 接入方式

在选择上网接入方式页面中，选中“ 固定 IP 接入 ”选项，如图 4-6 所示。单击“ 下一步 ”按钮，进入固定 IP 接入页面（如图 4-7），在这里配置固定 IP 接入信息，单击“ 完成 ”按钮，固定 IP 接入线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

图 4-7 固定 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的广域网 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的固定 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。

提示：

1. 所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）；
2. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）提供的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码，使它们在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部。

4.1.4.4 动态 IP 接入配置

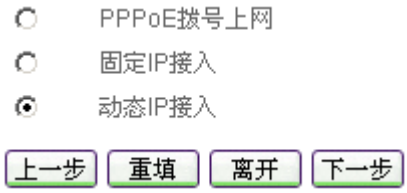


图 4-8 动态 IP 接入方式

在选择上网接入方式页面中，选中“ 动态 IP 接入 ”选项（如图 4-8），单击“ 下一步 ”按钮，进入动态 IP 接入页面（如图 4-9），在这里配置动态 IP 接入信息，单击“ 完成 ”按钮，动态 IP 接入线路配置完成，同时，系统密码、系统日期和系统时间也成功修改。

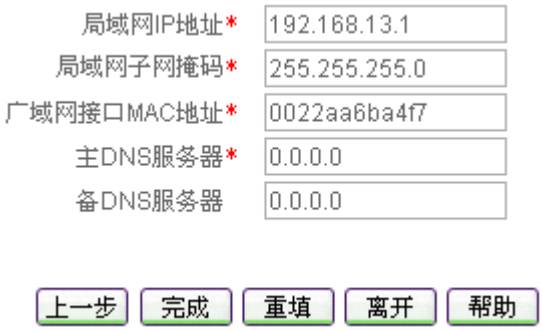


图 4-9 动态 IP 接入配置

- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网接口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备（这里指设备）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器 IP 地址（可能会在线路刷新时更新成 ISP 分配的地址）；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器 IP 地址。
- 上一步：返回到快速向导的第三页；
- 重填：恢复到修改前的动态 IP 配置参数；
- 离开：离开快速向导页面，进入主页面，快速向导所有操作无效；
- 完成：快速向导运行成功，所做的操作在这里生效。
- **提示**：所做的操作，只有单击“ 完成 ”按钮才生效（包括快速向导的前几页）。

4.1.5 小结

配置好快速向导后，设备的一些最基本的功能已经配置完成。如果发现完成配置后不能上网，请检查各项配置是否正确，可以直接到***基本配置—>线路配置***（章节 5.1）中检查“ 默认线路 ”状态，查看、修改配置参数。

第5章 基本配置

设备除提供基本的上网共享功能外，还提供了一些附加的 IP 功能，方便配置、管理网络。本章主要讲述如何设置上网所需的基本网络参数，如线路配置、线路组合、DHCP 和 DNS 服务器、接口配置、DDNS 服务以及时间段配置。

5.1 线路配置

本节主要讲述***基本配置***—>***线路配置***的配置方法。

在本页面不仅可以配置多条线路，也可以根据实际需要修改或删除已配置的线路，还可以查看各条线路的连接状态信息。

在***快速向导***中配置完上网线路之后（注：在***快速向导***中只能配置“ 默认线路 ”），可以到本页面查看该线路的连接状态和配置情况，也可根据需要修改配置。如果是对我们的路由器配置比较熟练的用户，可以不经过***快速向导***而直接在本页面配置“ 默认线路 ”。

提示：若要使用多线路上网，在本页面配置各条线路之后，可到***基本配置***—>***线路组合***中配置线路组合的相关参数。

5.1.1 线路连接信息列表

在“ 线路连接信息列表 ”中可以查看各线路的配置及状态信息，如表 5-1、5-2 所示。

线路连接信息列表 3/10

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

线路名称	物理接口	连接类型	连接状态	NAT状态	下行速率(bps)	上行速率
默认线路	WAN1	PPPoE(1)	关闭	启用	0	0
测试线路一	WAN1	PPPoE(1)	关闭	启用	0	0
网通线路	WAN1	PPPoE(1)	关闭	启用	0	0

刷新

表 5-1 线路连接信息列表

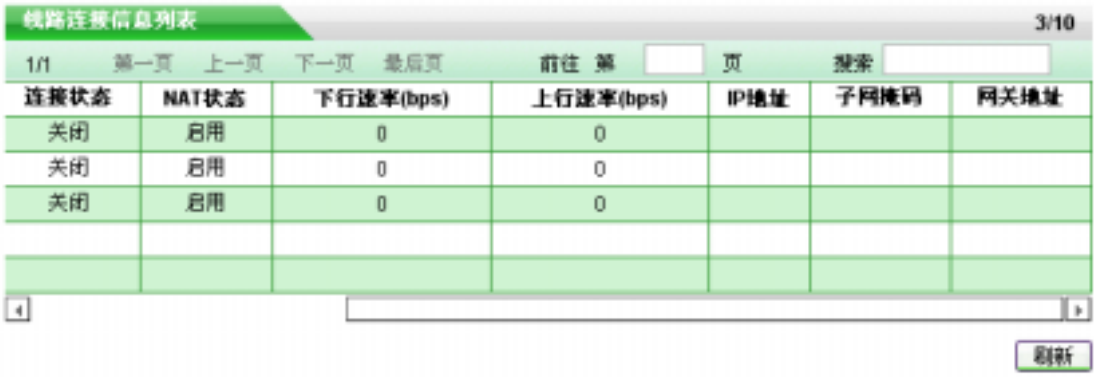


表 5-2 线路连接信息列表（续表 5-1）

5.1.1.1 参数涵义

- 线路名称：当前上网接入线路的名称；
- 物理接口：当前上网接入线路与设备相连的物理接口。注意，“ 默认线路 ”固定连接到 WAN1 口；
- 连接类型：当前上网接入线路的连接类型；特别地，如果是 PPPoE 拨号上网线路，同时还会显示该线路设置的 “ 用户名 ”；；
- 连接状态：线路的当前连接状态。分以下三种情况：

1. PPPoE 拨号线路

如果当前线路是 PPPoE 拨号线路，那么，共有 8 种状态，详见表 5-3。处于“ 已连接 ” 状态时，同时还会显示该线路保持本次连接的时间（单位：天:时:分:秒）。

连接状态	状态描述
关闭	物理接口没有连接，或者没有拨号
拨号中	拨号已经发起，但是服务方还未响应
验证中	服务方已经响应，正在验证用户名、密码
已连接	验证通过，PPPoE 连接已经建立，可以传送数据
断线中	正在拆除 PPPoE 连接
已挂机	一方已经发出挂机请求
已断线	PPPoE 连接已中断，等待拨号
内部错误	其它未定义状态

表 5-3 PPPoE 拨号线路连接状态描述

2. 固定 IP 接入线路

如果当前线路是固定 IP 接入线路，那么，共有 3 种状态，详见表 5-4。

连接状态	状态描述
关闭	物理接口没有连接
已连接	物理接口和对方网络设备建立连接
内部错误	其它未定义状态

表 5-4 固定 IP 接入线路连接状态描述

3. 动态 IP 接入线路

如果当前线路是动态 IP 接入线路，那么共有 3 种状态，详见表 5-5。处于“ 已连接 ”状态时，同时还会看到 ISP 给设备当前分配的 IP 地址的剩余租用时间（单位：天:时:分:秒）。

连接状态	状态描述
关闭	物理接口没有连接，或者已释放地址但尚未请求新地址
连接中	正在请求动态的 IP 地址
已连接	已经获得动态分配的 IP 地址，线路连接正常
内部错误	其它未定义状态

表 5-5 动态 IP 接入线路连接状态描述

- NAT 状态：当前线路是否启用了 NAT 功能，一般自动设置为启用；
- 下行速率(bps)：在两次刷新列表的时间间隔内，当前线路实际的下行平均速率。单位：比特/秒；
- 上行速率(bps)：在两次刷新列表的时间间隔内，当前线路实际的上行平均速率。单位：比特/秒；
- IP 地址、子网掩码、网关地址：分以下三种情况。

1. PPPoE 拨号线路

如果当前线路是 PPPoE 拨号线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址；其中，“ 网关地址 ” 与“ IP 地址 ”的值相同。

2. 固定 IP 接入

如果当前线路是固定 IP 接入线路，则分别为 ISP 提供的广域网接口的静态 IP 地址、子网掩码以及静态路由的网关地址。

3. 动态 IP 接入

如果当前线路是动态 IP 接入线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址。

5.1.1.2 列表功能

- 增加线路：选中“ 添加 ”选项，如图 5-2 所示，输入线路相关配置信息，单击“ 保存 ”按钮，生成新的上网线路；

- 浏览线路：如果已经生成了若干上网线路，则可在“ 线路连接信息列表 ”中查看相关信息，如表 5-1、5-2 所示；
- 编辑线路：如果想编辑某条上网线路，只需单击该线路对应条目的“ 线路名称 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除线路：如果想删除某条上网线路，首先需要单击该线路对应条目的“ 线路名称 ”超链接，然后才能执行删除线路操作，具体操作步骤请参考章节 5.1.2.4；
- 刷新：单击“ 刷新 ”按钮，可获得最新的线路连接信息。

5.1.1.3 PPPoE 拨号接入线路的拨号与挂断

如果某线路为 PPPoE 拨号接入线路，那么，在“ 线路连接信息列表 ”中单击该线路的“ 线路名称 ”超链接后，列表下方才会显示“ 拨号 ”和“ 挂断 ”按钮，如表 5-6、5-7 所示。这两个按钮的功能如下：

- 拨号：手动呼叫 PPPoE 连接，拨号过程中，在“ 连接状态 ”中可见“ 已断开 ”→“ 拨号中 ”→“ 验证中 ”→“ 已连接 ”四个过程。当 PPPoE 连接拨号类型设置为“ 手动拨号 ”时，需在这里完成 PPPoE 拨号；
- 挂断：手动挂断 PPPoE 连接，当 PPPoE 连接拨号类型设置为“ 手动拨号 ”时，需在这里挂断 PPPoE 连接。

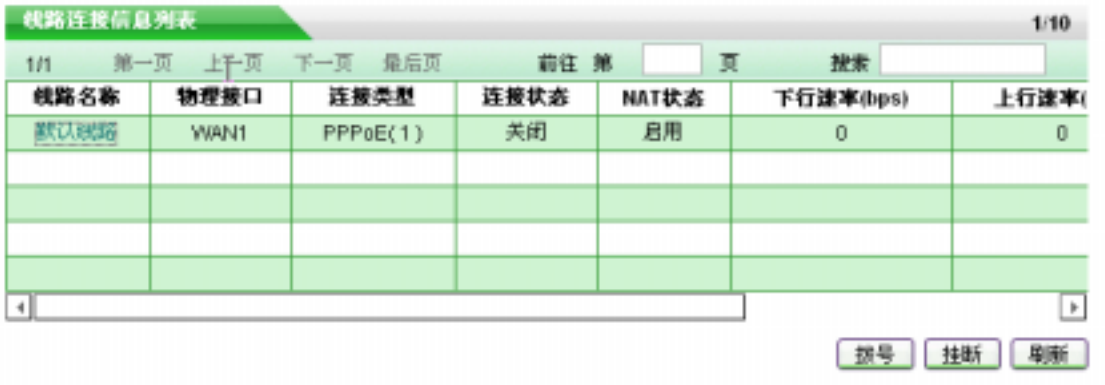


表 5-6 线路连接信息列表——PPPoE 拨号接入

表 5-7 线路连接信息列表——PPPoE 拨号接入（续表 5-6）

5.1.1.4 动态 IP 接入线路的更新与释放

如果某线路为动态 IP 接入线路，那么，在“ 线路连接信息列表 ”中单击该线路的“ 线路名称 ”超链接后，列表下方才会显示“ 更新 ”和“ 释放 ”按钮，如表 5-8、5-9 所示。这两个按钮的功能如下：

- 更新：系统自动完成一次先释放 IP 地址、再重新获得 IP 地址的过程（更新过程，在“ 连接状态 ”中可见“ 已断开 ”→“ 连接中 ”→“ 已连接 ”三个过程）；
- 释放：释放当前得到的动态 IP 地址。

表 5-8 线路连接信息列表——动态 IP 接入

表 5-9 线路连接信息列表——动态 IP 接入（续表 5-8）

5.1.2 线路配置

下面将首先分别介绍 PPPoE 拨号上网、固定 IP 接入、动态 IP 接入三种情况下，如何配置线路，以及如何删除已配置的线路。

提示：只有在配置完“ 默认线路 ”之后，才能配置其他上网线路。如果是直接在本页面配置“ 默认线路 ”，则首先需在“ 线路连接信息列表 ”中，单击“ 默认线路 ”超链接，然后才可以配置它。并且，“ 默认线路 ”固定连接到设备的 WAN1 口，其“ 线路名称 ”和“ 物理接口 ”禁止修改。其他线路的主 DNS 服务器为在默认线路中配置的主 DNS 服务器，不能修改。

5.1.2.1 PPPoE 拨号上网配置

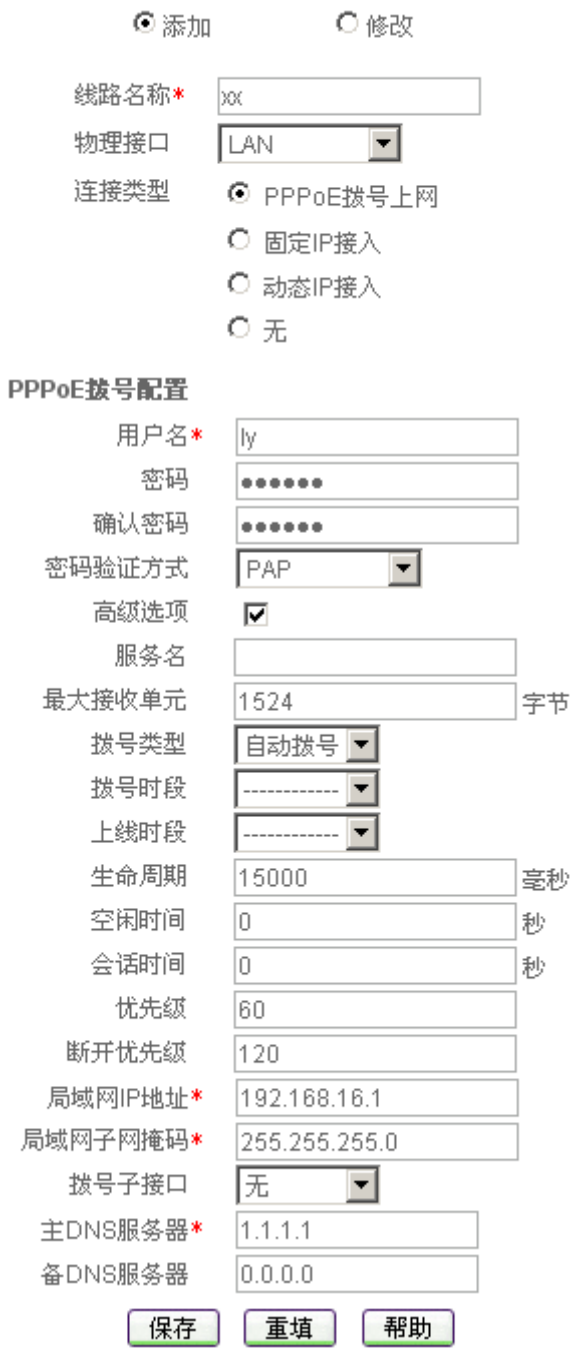


图 5-1 PPPoE 拨号上网线路配置

- 线路名称：当前线路的名称（自定义，不能重复），取值范围：1~11 位字符；
- 物理接口：当前线路与设备相连的物理接口的名称；
- 连接类型：这里选中“ PPPoE 拨号上网 ”；
- 用户名、密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号及密码。如有疑问，请询问 ISP；
- 密码验证方式：ISP 验证用户名及密码的方式，多数地区为 PAP 方式，也有少数地区采用 CHAP 或者是 NONE 等方式；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的

网关地址（出厂值为 192.168.16.1/255.255.255.0）；

- 服务名：ISP 提供的 PPPoE 服务名，一般不需要设置。如有疑问，请询问 ISP；
- 最大接收单元：缺省值为 1524 字节，PPPoE 拨号时设备将自动与对方设备协商，除非特别应用，不要修改；
- 拨号类型：

  自动拨号：当打开设备或者上一次拨号断线后自动拨号连接；

  手动拨号：由用户在***基本配置—>线路配置***的“ 线路连接信息列表 ”（章节 5.1.1）中手动进行连接和挂断；

  按需拨号：在局域网内部有访问 Internet 流量时设备自动进行连接；
- 拨号时段：允许 PPPoE 拨号的时间段（时间段在***基本配置—>时间段配置***〈章节 5.6〉中配置），只有在此时间段内才允许 PPPoE 拨号。不设置代表不对拨号时段进行控制；
- 上线时段：允许设备上线连接到 Internet 的时间段（时间段在***基本配置—>时间段配置***〈章节 5.6〉中配置），超出这个时间段的范围不允许设备上线；如果超出时间段时设备处于连接状态，它将自动断开 PPPoE 连接。不设置代表不对上线时段进行控制；
- 生命周期：在拨号成功后，系统将每隔 1000ms 向对端网络设备发送一个探测包，以探测线路是否可用，如果在“ 生命周期 ”范围内一直没有收到对方回应，则断开此连接，默认值：15000 毫秒；
- 空闲时间：无访问流量后自动断线前等待的时长，0 代表不自动断线（单位：秒）；
- 会话时间：连接生存时间，每次拨号成功到设置的时间后自动断线。一般情况下不要作此设置，0 代表没有时间限制（单位：秒）；
- 优先级：拨号成功后，该线路的路由优先级，目的网段相同的情况下，设备将优先选择优先级高的线路转发数据包，值越低优先级越高；
- 断开优先级：PPPoE 线路断开后，该线路的路由优先级，优先级高的优先拨号，值越低优先级越高；
- 拨号子接口：子接口是指从属于某一个物理接口的逻辑上的虚接口，通常，在单个物理接口上可配置多个子接口。目前，设备仅支持在 WAN1 接口上配置多个子接口，不同子接口按照 802.1Q 值进行区分；
- 主 DNS 服务器：ISP 提供的首选 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP 提供的备用 DNS 服务器的 IP 地址；
- 保存：PPPoE 拨号上网配置生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 如果改变了“ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网；

2. 只有支持 802.1Q tag VLAN 功能的产品才允许配置“ 拨号子接口 ”。通过在 WAN1 口上配置多个 VLAN 的子接口，向外连接一个带 802.1Q tag VLAN 的交换机，每个子接口使用不同的 MAC 地址，可以彻底解决由于运营商宽带接入服务器上限制多条 ADSL 使用一个 MAC 地址连接的问题；

3. 与在***基本配置—>快速向导***中提供的“ PPPoE 拨号上网配置 ”（章节 4.2.4.1）相比较，这里提供了更多的配置参数，包括：“ 拨号时段 ”、“ 上线时段 ”、“ 生命周期 ”、“ 会话时间 ”、“ 优先级 ”、“ 断开优先级 ”等。

5.1.2.2 固定 IP 接入配置

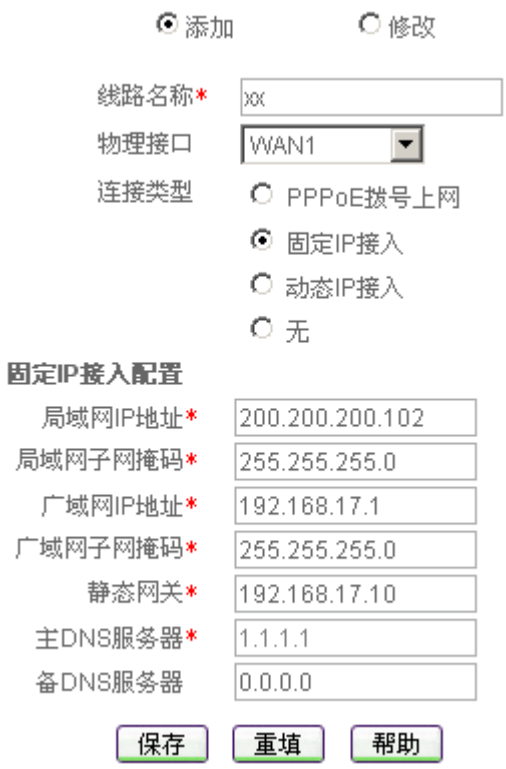


图 5-2 固定 IP 接入线路配置

“ 线路名称 ”、“ 物理接口 ”这几个参数的涵义同“ PPPoE 拨号上网配置 ”中的相关参数，这里不再重述。

- 连接类型：这里选中 “ 固定 IP 接入 ”；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网 IP 地址、子网掩码、静态网关：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备对广域网的 IP 地址、子网掩码和静态网关；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 保存：固定 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 广域网 IP 地址、静态网关要在同一网段，某些 ISP（例如中国电信）给出的广域网 IP 地址和静态网关不在同一网段，请修改子网掩码的值，使它们处在同一网段。如果不清楚网段相关知识，请咨询专业人士或者艾泰科技客户服务部；
2. 如果改变了 “ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

5.1.2.3 动态 IP 接入配置

图 5-3 动态 IP 接入线路配置

“ 线路名称 ”、“ 物理接口 ”这几个参数的涵义同“ PPPoE 拨号上网配置 ”中的相关参数，这里不再重述。

- 连接类型：这里选中 “ 动态 IP 接入 ”；
- 局域网 IP 地址、子网掩码：配置成功后，该地址将作为局域网中计算机用作上网的网关地址（出厂值为 192.168.16.1/255.255.255.0）；
- 广域网接口 MAC 地址：一般情况下不需要设置。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获 IP 地址的现象，此时需要将新的网络设备（这里指 UTT 3640）的 MAC 地址设置成和原有网络设备的 MAC 地址相同；
- 主 DNS 服务器：ISP（例如中国电信）提供的主用 DNS 服务器的 IP 地址，在线路刷新时可能会更新成 ISP 分配的新地址；
- 备 DNS 服务器：ISP（例如中国电信）提供的备用 DNS 服务器的 IP 地址。
- 保存：动态 IP 接入配置生效；
- 重填：恢复到修改前的配置参数。
- **提示**：如果改变了 “ 局域网 IP 地址 ”，在保存之后，必须使用新的 IP 地址重新登录设备才能进行 WEB 界面管理，并且，局域网中所有计算机的默认网关必须设置成该 IP 地址才能正常上网。

5.1.2.4 删除线路

如果要删除某条线路，则需执行以下操作：

1. 在 “ 线路连接信息列表 ” 中，单击该线路对应条目的 “ 线路名称 ” 超链接，该线路相关信息即填充到编辑框中；

2. 在配置界面中，将“连接类型”选择为“无”（如图 5-4），然后单击“保存”按钮；

图 5-4 删除线路

3. 单击“保存”按钮后，系统将弹出如图 5-5 所示对话框，再单击“确定”按钮，该线路立即被删除。

图 5-5 对话框——删除线路

提示：一次只能删除一条线路；并且，只有在没有任何其他线路时，才允许删除“默认线路”。

5.1.3 相关的缺省路由

在***快速向导***中配置完默认线路，或者在本页面中配置完默认线路和其他上网线路后，设备会自动生成各线路对应的缺省路由，可在***系统状态***—>***路由和端口信息***的“路由表信息列表”中查看到对应路由的状态信息，即目的地址为“0.0.0.0/0”的静态路由。

如果上网线路为固定 IP 或动态 IP 接入线路，还可在***高级配置***—>***路由配置***的“路由信息列表”中查看对应路由的配置信息，具体描述详见章节 7.4.1.1。

5.2 线路组合

本节主要讲述***基本配置***—>***线路组合***的配置方法。

在线路组合配置中，可以快速配置多线路上网的线路组合方式及其他相关参数，可以指定多条线路的线路检测方式，还可以为指定范围内的主机限制上网线路，并能通过不同的分配规则来控制线路流量。

5.2.1 线路组合功能介绍

5.2.1.1 线路组合方式

设备提供了 2 个线路组：“ 主线路 ” 组和 “ 备份线路 ” 组。为方便起见，将 “ 主线路 ” 组中的线路统称为主线路，将 “ 备份线路 ” 组中的线路统称为备份线路。所有线路缺省都是主线路，用户可以根据需要将某些线路划分到 “ 备份线路 ” 组中。但是，“ 默认线路 ” 只能作为主线路使用。

设备提供了 “ 所有线路负载均衡 ” 和 “ 部分线路负载均衡，其余备份 ” 这两种线路组合方式。

在 “ 所有线路负载均衡 ” 方式下，所有线路都作为主线路使用。工作原理如下：

1. 当所有线路都正常时，局域网内主机将同时使用所有线路上网。
2. 若某条线路出现故障，则立即屏蔽该线路，原先通过该线路的流量将分配到其他线路上。
3. 一旦故障线路恢复正常，设备会自动启用该线路，流量自动重新分配。

在 “ 部分线路负载均衡，其余备份 ” 方式下，一部分线路作为主线路使用，另一部分线路则作为备份线路使用。工作原理如下：

1. 只要有一条（或更多）主线路正常，局域网内主机就使用主线路上网；此时，如果有多条主线路正常，那么，它们将按照负载均衡方式工作。
2. 若所有主线路都出现故障，则自动切换到使用备份线路上网；此时，如果有多条备份线路都正常，那么，它们也将按照负载均衡方式工作。
3. 一旦有一条（或更多）故障主线路恢复正常，则立即切换回主线路。

提示：当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP 会话的属性决定的。艾泰科技将不承担由此引发的一切用户损失或者法律诉讼。

5.2.1.2 线路检测机制

无论采用哪种线路组合方式，要保证线路故障时网络不中断，都要求设备必须能够实时地监控线路状态。为此，我们为设备设计了灵活的自动检测机制，并提供多种线路检测方法供用户选择，以满足实际应用的需要。

为方便理解，先介绍一下几个相关参数。

检测目标 :检测的对象，设备将向预先指定的检测目标发送检测包以检测线路是否正常。

检测间隔：发送检测包的时间间隔，一次发送一个检测包，缺省值为 1000 毫秒。特别地，该值为 0 时，表示不进行线路检测。

检测次数：每个检测周期内，发送检测包的次数。

检测周期：该值为检测间隔与检测次数的乘积，例如，缺省情况下，该值为 1000×3＝3000 毫秒。

下面将分别介绍在线路正常和线路故障这两种情况下，设备的线路检测机制。

某条线路正常时，检测机制如下所述：设备将每隔指定的检测间隔向该线路的检测目标

发送一个检测包，如果在某个检测周期内，发送的所有检测包都没有回应，就认为该线路出现故障，并立即屏蔽该线路。例如，缺省情况下，若某个检测周期内，发送的 3 个检测包都没有回应，就认为该线路出现故障。

某条线路故障时，检测机制如下所述：同样地，设备也是每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的检测包中有一半及以上数量的检测包有回应时，就认为该线路已经正常，并恢复启用该线路。例如，缺省情况下，若某个检测周期内，有 2 个检测包有回应，就认为该线路恢复正常。

提示：允许不启用线路检测，这时需要将“检测间隔”设为“0”毫秒。

5.2.1.3 线路检测方法

设备支持三种线路检测方法：ICMP、ARP 及 DNS，用户可选择其中的一种来监控各条线路的状态，注意：所有线路只能使用同一种检测方法，但可设置不同的检测参数。各方法的具体描述如下：

1. ICMP 方法：固定时间间隔向检测目标（网关或其他公网地址）发送 ICMP 检测包，以检测线路通断和质量；
2. ARP 方法：固定时间间隔向接入线路网关发出 ARP 请求，以检测线路通断和质量；
3. DNS 方法：固定时间间隔向指定的公网 DNS 服务器发出 DNS 请求，以检测线路通断和质量。

各方法支持的检测目标类型及使用限制如表 5-10 所示，其中，“网关”指对应线路的下一跳网关，“其他”指除网关之外的其他检测目标。“检测目标 IP 地址”用来设置欲检测的其他目标的 IP 地址。

检测方法	检测目标类型	检测目标 IP 地址	说明
ICMP	网关	无需设置	ICMP 可检测网关和其他目标
	其他	需设置	
ARP	网关	无需设置	检测目标只能是网关；PPPoE 上网时，不可使用该方法
DNS	其他	需设置	检测目标只能是 DNS 服务器

表 5-10 各种检测方法支持的检测地址类型

在实际应用中，选择检测方法时，供参考的依据及注意事项如下：

1. ICMP 方法检测线路灵敏度、准确度高，建议优先选用 ICMP 检测。一般情况下，使用 ICMP 检测网关；而当接入线路网关不转发 ICMP 包（禁 ping）时，则需检测其他公网 IP 地址。
2. ARP 检测网关：适用于接入线路全部禁 ping 的环境。注意，ARP 方法只能检测接入线路的网关；PPPoE 上网时，不提供 ARP 方法。
3. DNS 检测：适用于接入线路不断，运营商对接入时间加以限制的环境。注意，DNS 方法只能检测公网 DNS 服务器，建议使用当地运营商提供的 DNS 服务器；此外，不能选择局域网内部主机使用的 DNS 服务器作为检测目标，否则，这些主机将只能使用对应的线路上网，无法使用其他线路上网。
4. 对于 PPPoE 拨号线路来说，缺省不启用线路检测，PPPoE 会使用自身的检测机制

来检测线路；它也可增加 ICMP 或 DNS 检测，但不能用来检测网关。

5.2.2 多线路负载均衡功能介绍

如章节 5.2.1.1 中所述，在设备中，无论使用哪种线路组合方式，当局域网主机正在使用的上网线路多于一条时，这些线路就会按照负载均衡方式工作。在以下各节中，我们将详细介绍设备的多线路负载均衡功能的特点。

5.2.2.1 根据源 IP 地址指定优先线路

设备允许用户预先为局域网中的某些主机指定上网线路，它是通过设置线路的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”来实现的，IP 地址属于两个地址范围内的主机将优先使用指定线路。对于已指定上网线路的主机来说，当指定线路正常时，它们只能通过该线路上网；但是，当指定线路有故障时，它们会使用其他的正常线路上网。

5.2.2.2 根据线路带宽合理分配流量

设备中，用户能够预先指定分配到各条线路的流量的比例，它是通过设置线路的“ 权重 ”来实现的，“ 权重 ”大的线路将比 “ 权重 ”小的线路承担更多流量。在实际应用中，一般可按线路的带宽比来设置各线路的 “ 权重 ”，从而实现按线路带宽比合理分配流量。

例如，假设某用户申请了 4 根线路 A、B、C、D，带宽分别为 10M、6M、4M、4M。分为以下两种情况：

情况一，采用“ 所有线路负载均衡 ”方式，这 4 条线路均作为主线路使用，此时可将 A、B、C、D 的 “ 权重 ”分别设置为 5、3、2、2；

情况二，采用 “ 部分线路负载均衡，其余备份 ” 方式，不妨假设 A 和 B 作为主线路使用、C 和 D 作为备份线路使用，则可将 A、B 的“ 权重 ”分别设置为 5、3，将 C 和 D 的“ 权重 ”都设置为 1。

需要注意的是，当局域网中的某些主机指定了上网线路时，若按照带宽比来设置线路的 “ 权重 ”，线路的实际流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整各线路的 “ 权重 ”。

5.2.2.3 提供两种流量分配规则

“ 分配规则 ”用来控制线路流量，它作用于局域网中没有指定上网线路的计算机，设备提供两种分配规则：“ NAT 会话 ” 和 “ IP 地址 ”，它们的实现机制如下所述：

1. IP 地址

使用 IP 地址作为分配规则时，设备将根据线路的 “ 权重 ”，把未指定上网线路的主机的 IP 地址，按顺序依次分配到当前正在使用的各条线路上。分配到各条线路的 IP 地址的数量比（即主机数量比）为线路的“ 权重 ”比，来自同一个 IP 地址的 NAT 会话使用同一条线路。

例如，若当前同时使用 3 条线路上网，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用第一条线路，第 4、5 台主机将使用第二条线路，第 6 台主机将使用第三条线路，接着第 7、8、9 台主机将使用第一条线路，……，依此类推。注

意，这里假设每台主机均只有一个 IP 地址。

2. NAT 会话

使用 NAT 会话作为分配规则时，设备将根据线路的“ 权重 ”，把未指定上网线路的主机发起的 NAT 会话，按顺序依次分配到当前正在使用的各条线路上。分配到各线路的 NAT 会话的数量比为线路的“ 权重 ”比，同一主机发起的 NAT 会话可使用多条线路。

例如，若当前同时使用 3 条线路上网，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，内网主机发起的第 1、2、3 个 NAT 会话将使用第一条线路，第 4、5 个 NAT 会话将使用第二条线路，第 6 个 NAT 会话将使用第三条线路，接着第 7、8、9 个 NAT 会话将使用第一条线路，……，依此类推。

一般情况下，建议“ 分配规则 ”选择为“ IP 地址 ”。当对带宽要求高，需要多线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择“ NAT 会话 ”，从而能够充分利用多线路带宽，以提高下载速度。需要注意的是，即便选择了“ NAT 会话 ”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

5.2.3 线路组合通用设置

由于“ 所有线路负载均衡 ”和“ 部分线路负载均衡，其余备份 ”这两种线路组合方式下，通用设置的界面不同，因此，以下将分别介绍它们的通用设置参数。

5.2.3.1 所有线路负载均衡

图 5-6 线路组合通用配置——所有线路负载均衡

- 线路检测方法：检测线路是否激活的方法，选项为“ ICMP ”、“ ARP ”及“ DNS ”，更具体的描述请参见章节 5.2.1.3。
  ICMP：使用向网关或预先指定的其他检测目标发送 ICMP 包的方式检测线路是否激活；
  ARP：使用向网关发送 ARP 包的方式检测线路是否激活；
  DNS：使用向预先指定的某 DNS 服务器发送 DNS 包的方式检测线路是否激活；
- 线路组合方式：这里选中“ 所有线路负载均衡 ”。具体描述请参见章节 5.2.1.1；
- 分配规则：控制线路流量时使用的规则。选项为“ NAT 会话 ”或“ IP 地址 ”，缺省

值为“ IP 地址 ”。具体描述请参见章节 5.2.2.3。

- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

5.2.3.2 部分线路负载均衡，其余备份

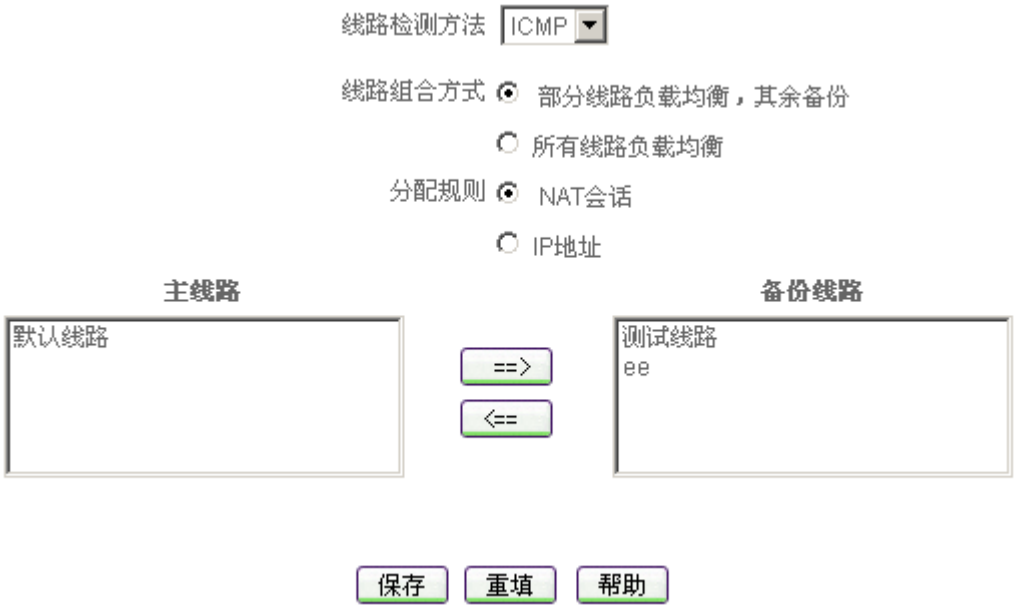


图 5-7 线路组合配置——部分线路负载均衡，其余备份

“ 线路检测方法 ”、“ 分配规则 ” 这两个参数的涵义，与 “ 所有线路负载均衡 ” 方式下相关参数涵义相同，这里不再重述。

- 线路组合方式：这里选中 “ 部分线路负载均衡，其余备份 ”。具体描述请参见章节 5.2.1.1；
- 主线路：该列表框代表 “ 主线路 ” 组，位于该列表框中的线路全部都作为主线路使用；
- 备份线路：该列表框中代表 “ 备份线路 ” 组，位于该列表框中的线路全部都作为备份线路使用。
- ==>（向右箭头）、<==（向左箭头）：首先在 “ 主线路 ” 列表框中选中一条（或更多）线路，然后单击 “ ==> ” 按钮，被选中的线路立即被移到 “ 备份线路 ” 列表框中。类似地，首先在 “ 备份线路 ” 列表框中选中一条（或更多）线路，然后单击 “ <== ” 按钮，被选中的立即被移到 “ 主线路 ” 列表框中。
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 默认线路只能位于 “ 主线路 ” 列表框中，不能移到 “ 备份线路 ” 列表框中；
2. 本方式下，若将 “ 线路组合方式 ” 修改成 “ 所有线路负载均衡 ”，单击 “ 保存 ” 按钮后，系统立即将 “ 备份线路 ” 列表框中的所有线路都移到 “ 主线路 ” 列表框中；
3. 本方式下，若 “ 备份线路 ” 列表框中所有线路都被移到 “ 主线路 ” 列表框中，单击 “ 保存 ” 按钮后，或者若用户删除了所有的备份线路，“ 线路组合方式 ” 将自动切换为 “ 所有线路负载均衡 ”。

5.2.4 线路检测及权重配置

提示：在这里可以分别设置各条线路的线路组合信息（即线路检测、负载均衡）相关参数的配置。在配置前，首先需要在“ 线路组合信息列表 ”（如表 5-11）中，单击欲配置线路的“ 线路名称 ”超链接，其相关信息填充到相应的编辑框以后，然后才可以配置该线路。

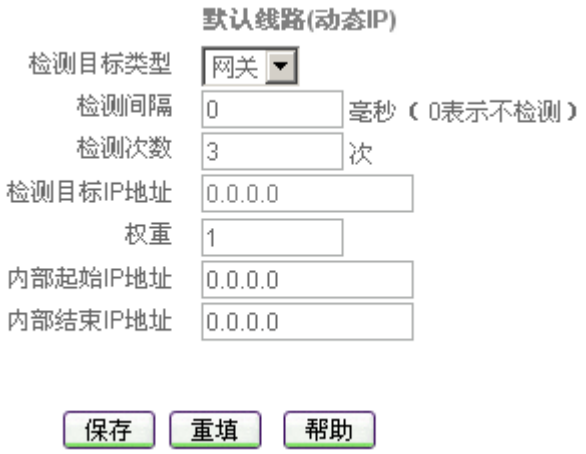


图 5-8 线路检测及权重配置

- 检测目标类型：欲检测的目标的类型，选项为“ 网关 ”、“ 其他 ”。ARP 方式下，仅支持检测“ 网关 ”；DNS 方式下，仅支持检测“ 其他 ”；ICMP 方式下，两个都支持。
  网关：线路的检测目标为该线路下一跳网关；
  其他：线路的检测目标为用户自定义的其他检测目标；
- 检测间隔：发送检测包的时间间隔，单位：毫秒。启用线路检测时，取值范围为 1000～60000，缺省值为 1000。该值为 0 时，表示不启用线路检测；
- 检测次数：检测周期内发送检测包的次数（每次发送一个检测包）。缺省值为 3；
- 检测目标 IP 地址：欲检测的目标的 IP 地址。当“ 检测目标类型 ”为“ 其他 ”时，需配置该参数；“ 检测目标类型 ”为“ 网关 ”时，无需配置，此时，网关地址就是检测目标 IP 地址；
- 权重：当前线路的权重，取值范围为 1~255，缺省值为 1。具体描述请参见章节 5.2.2.2；
- 内部起始 IP 地址、内部结束 IP 地址：局域网内优先使用当前线路上网的主机的起始 IP 地址和结束 IP 地址。具体描述请参见章节 5.2.2.1。
- 保存：上述配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. “ 检测目标类型 ”、“ 检测间隔 ”、“ 检测次数 ”以及“ 检测目标 IP 地址 ”为线路检测相关参数，更详细的说明请参见章节 5.2.1.2、章节 5.2.1.3；
2. “ 权重 ”、“ 内部起始 IP 地址 ”以及“ 内部结束 IP 地址 ”为负载均衡相关参数，更详细的说明请参见章节 5.2.2.1、章节 5.2.2.2。

5.2.5 线路组合信息列表

表 5-11 线路组合信息列表

表 5-12 线路组合信息列表（续表 5-11）

5.2.5.1 部分参数涵义

“ 线路名称 ”、“ 连接类型 ”、“ 连接状态 ”、“ IP 地址 ”这几个参数的涵义同***基本配置—> 线路配置***的“ 线路连接信息列表 ”（章节 5.1.1）的相关参数，其中，若“ 连接状态 ”显示为“ 已连接（*）”，则表示该线路连接正常，但是并未使用；若“ 连接状态 ”显示为“ 已连接（√）”，则表示该线路连接正常，并且正在使用。

“ NAT 会话比 ”、“ 上行流量比 ”、“ 下行流量比 ”的涵义如下：

- NAT 会话比：在两次刷新本列表的时间间隔（即统计时长）内，通过此线路建立的 NAT 会话的数量占所有线路建立的 NAT 会话的总数量的百分比。
  使用单线路上网时，在统计时长内，如果没有建立新的 NAT 会话，则该值为“ 0% ”；否则，该值为“ 100% ”。
  使用多线路上网时，在统计时长内，如果通过此线路没有建立新的 NAT 会话，则该值为“ 0% ”；否则，按实际百分比显示。
- 上行流量比：在统计时长内，通过此线路发送的数据包字节数占所有线路发送的数据包字节数的百分比。
- 下行流量比：在统计时长内，通过此线路接收的数据包字节数占所有线路接收的数

据包字节数的百分比。

5.2.5.2 列表功能

- 编辑线路组合信息：如果想编辑某条线路的线路组合信息的相关参数，只需单击该线路对应条目的“ 线路名称 ”超链接，其信息就会填充到相应的编辑框内（如图 5-8），可修改它，再单击“ 保存 ”按钮，修改完毕；
- 浏览线路组合信息：如果已经配置了若干线路的线路组合信息，则可以在“ 线路组合信息列表 ”中查看相关信息，如表 5-11、5-12 所示；
- 刷新：单击“ 刷新 ”按钮，可获得最新的线路组合信息。

5.2.6 配置线路组合

5.2.6.1 线路组合的配置顺序

只有在使用多线路上网的情况下，才需配置线路组合相关参数。配置顺序如下：

1. 进入***基本配置***—>***线路配置***页面，首先配置“ 默认线路 ”，然后根据需要配置其他自定义线路（也可在***开始***菜单配置线路）。注意，“ 默认线路 ”也可以直接在***基本配置***—>***快速向导***中配置；
2. 进入***基本配置***—>***线路组合***页面，根据需要进行线路组合通用设置，具体步骤请参见章节 5.2.6.2；
3. 在***基本配置***—>***线路组合***页面中，根据需要分别配置各条线路的线路组合信息的相关参数，具体步骤请参见章节 5.2.6.3。

5.2.6.2 线路组合通用设置配置步骤

第一步，进入***基本配置***—>***线路组合***页面；

第二步，根据需要，设置“ 线路检测方法 ”；

第三步，根据需要，设置“ 线路组合方式 ”；如果“ 线路组合方式 ”选择为“ 部分线路负载均衡，其余备份 ”时，还应根据实际需求将“ 主线路 ”列表框中的若干线路移到“ 备份线路 ”列表框中；

第四步，根据需要，设置“ 分配规则 ”；

第五步，单击“ 保存 ”按钮，通用设置相关参数配置完成。

5.2.6.3 线路检测及权重配置步骤

第一步，进入***基本配置***—>***线路组合***页面；

第二步，根据需要，在“ 线路组合信息列表 ”中，单击欲配置线路的“ 线路名称 ”超链接；

第三步，根据需要，设置该线路的线路检测相关参数，包括：“ 检测目标类型 ”、“ 检测间隔 ”、“ 检测次数 ”以及“ 检测目标 IP 地址 ”等；

第四步，根据需要，设置该线路的负载均衡相关参数，包括：“ 权重 ”、“ 内部起始 IP 地址 ”以及“ 内部结束 IP 地址 ”等；

第五步，单击“ 保存 ”按钮，该线路的线路组合信息相关参数配置完成；
第六步，如果还需配置其他线路，则重复第二步至第五步。

5.2.7 相关的检测路由

当默认线路或其他某条上网线路启用线路检测后，系统还会自动生成相应的检测路由，从而保证检测包是通过当前待检测的线路转发的。可在***高级配置***—>***路由配置***（章节 7.4）的“ 路由信息列表 ”中查看对应路由的配置信息，具体描述详见章节 7.4.1.2。

提示：对于固定 IP 或动态 IP 接入线路来说，当“ 检测目标 ”为“ 网关 ”时，系统将直接使用该线路对应的缺省路由来转发检测包，即该缺省路由同时也作为检测路由来使用。

5.3 DHCP 和 DNS 服务器

本节主要讲述***基本配置—>DHCP 和 DNS 服务器***的配置方法。

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、DNS 服务器以及一些扩展信息等。为局域网中的所有计算机正确配置 TCP/IP 协议是一件非常繁琐的事情。设备能够配置成 DHCP 服务器，为局域网计算机动态分配 IP 地址、子网掩码、网关、以及 DNS 服务器、WINS 服务器等信息。

5.3.1 DHCP 服务配置

图 5-9 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或允许设备的 DHCP 服务器功能。选中为允许，如图 5-9 所示；
- 起始 IP 地址：DHCP 服务器给局域网计算机自动分配的起始 IP 地址（一般要和设备的局域网接口的 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给局域网计算机自动分配的子网掩码（一般要和设备局域网接口的子网掩码一致）；
- 总地址数：DHCP 服务器可以分配的地址总数量；
- 网关地址：DHCP 服务器给局域网计算机自动分配的网关 IP 地址（一般要和设备的局域网接口的 IP 地址一致）；
- 租用时间：局域网计算机获得设备分配的 IP 地址的租用时间（单位：秒）；
- 主 DNS 服务器：DHCP 服务器给局域网计算机自动分配的主用 DNS 服务器的 IP 地址，此处会自动识别在***基本配置—>快速向导***或者在***基本配置—>线路配置***默认线路设置的值；
- 备 DNS 服务器：DHCP 服务器给局域网计算机自动分配的备用 DNS 服务器的 IP 地

址，此处会自动识别在***基本配置—>快速向导***或者在***基本配置—>线路配置***中默认线路设置的值；

- 启用 DNS 代理：选中之后，设备会启用 DNS 代理功能，此时给局域网中的计算机分配的主 DNS 服务器的 IP 地址就是设备局域网接口的 IP 地址。
- 主 WINS 服务器：DHCP 服务器给局域网计算机自动分配的主用 WINS 服务器的 IP 地址，没有可以不填；
- 备 WINS 服务器：DHCP 服务器给局域网计算机自动分配的备用 WINS 服务器的 IP 地址，没有可以不填；
- 保存：DHCP 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 启用了 DNS 代理功能之后，必须要设置一个 ISP（例如中国电信）提供的可用的“ 主 DNS 服务器 ”；
2. 如果要使用设备的 DHCP 服务器功能，局域网计算机的 TCP/IP 协议必须设置为“ 自动获得 IP 地址 ”；
3. 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS 服务器设置为代理服务器的 IP 地址，那么，只需将设备的局域网接口的 IP 地址设置为同一个 IP 地址，这样，当设备启用 DNS 代理功能之后，用户不需要修改计算机的配置就可以转换到使用设备的 DNS 代理功能了。

5.3.2 DHCP 地址池使用信息

表 5-13 DHCP 地址池使用信息列表

- 显示 DHCP 地址池使用信息：选中后，系统将显示 “ DHCP 地址池使用信息列表 ”，如表 5-13 所示；
- ID：地址使用者的序号；
- IP 地址：DHCP 服务器分配的 IP 地址；
- MAC 地址：使用该 IP 地址的网络设备的 MAC 地址。“ ?????pending????? ” 表示该 IP 地址在租期时间范围内，但该网络设备已经离线，如果在租期内该网络设备再次申请 IP 地址，仍将获得该 IP 地址；
- 掩码：DHCP 服务器分配的 IP 地址的子网掩码；
- 剩余租期：租用该 IP 地址的剩余时间（时间单位：天:时:分:秒）；
- 刷新：单击 “ 刷新 ” 按钮，可获得最新的 DHCP 池地址使用信息。

5.3.3 配置 DHCP 服务器

第一步，进入***基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 启用 DHCP 服务器 ”选项，根据需要填写“ 起始 IP 地址 ”、“ 子网掩码 ”、“ 总地址数 ”、“ 网关地址 ”、“ 租用时间 ”、“ 主 DNS 服务器 ”、“ 备 DNS 服务器 ” 等信息；

第三步，若希望启用设备的 DNS 代理功能，则需选中 “ 启用 DNS 代理 ”，此时局域网中计算机分配到的 DNS 服务器是设备局域网接口的 IP 地址；

第四步，根据需要选择是否填写 “ 主 WINS 服务器 ”，“ 备 WINS 服务器 ”；

第五步，单击 “ 保存 ” 按钮，DHCP 服务器配置生效。

提示：如果要关闭 DHCP 服务器功能，请取消 “ 启用 DHCP 服务器 ” 的选中，单击 “ 保存 ” 按钮。

5.3.4 DHCP 手工绑定配置

使用 DHCP 服务为局域网中的计算机自动配置 TCP/IP 属性是非常方便的，但是会造成一台计算机不同时间被分配到不同 IP 地址的现象。而某些局域网计算机可能需要固定的 IP 地址，这时就需要使用 DHCP 手工绑定功能，将计算机的 MAC 地址与某个 IP 地址绑定，如图 5-10 所示。当具有此 MAC 地址的计算机向 DHCP 服务器（设备）申请地址时，设备将根据其 MAC 地址寻找到对应的固定 IP 地址分配给该计算机。

图 5-10 DHCP 手工绑定配置

- IP 地址：预留的 IP 地址，必须是 DHCP 服务器指定的地址范围内的合法 IP 地址；
- MAC 地址：固定使用该预留 IP 地址的计算机的 MAC 地址；
- 用户名：欲配置该 DHCP 手工绑定的计算机的用户名（自定义，不能重复）。取值范围：1～31 个字符。
- 保存：DHCP 手工绑定配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：设置成功后，设备将为指定计算机固定分配预设的 IP 地址。

5.3.5 DHCP 手工绑定列表

表 5-14 DHCP 手工绑定信息列表

- 增加 DHCP 手工绑定：选中“ 添加 ”选项，如图 5-10 所示，输入 DHCP 手工绑定信息，单击“ 保存 ”按钮，生成新的 DHCP 手工绑定；
- 浏览 DHCP 手工绑定：如果已经生成了 DHCP 手工绑定条目，只需选中“ 显示 DHCP 手工绑定信息 ”，即可浏览“ DHCP 手工绑定信息列表 ”，如表 4-14 所示；
- 编辑 DHCP 手工绑定：如果想编辑某一个 DHCP 手工绑定条目，只需单击该条目的“ 用户名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除 DHCP 手工绑定：首先选中一些 DHCP 手工绑定信息条目，再单击右下角的“ 删除 ”按钮，即可删除那些被选中的 DHCP 手工绑定。

5.3.6 自定义 DHCP 手工绑定

第一步，进入***基本配置—>DHCP 和 DNS 服务器***页面；

第二步，选中“ 添加 ”选项，填写“ 用户名 ”、“ MAC 地址 ”和预设的“ IP 地址 ”；

第三步，单击“ 保存 ”按钮，然后可以在“ DHCP 手工绑定信息列表 ”中看到添加的记录；

第四步，继续添加新的 DHCP 手工绑定用户。

提示：若要删除 DHCP 手工绑定用户，则只需在“ DHCP 手工绑定信息列表 ”中选中要删除的 DHCP 手工绑定信息条目，单击“ 删除 ”按钮，即可删除。

5.4 接口配置

本节主要讲述***基本配置—>接口配置***的配置方法。

5.4.1 接口配置

在本页面，可以修改设备的物理接口的 IP 地址、MAC 地址及工作模式，并且可以给各个接口配置第二个 IP 地址，实现多网络互相连接，如图 5-11 所示。

图 5-11 接口配置

- 选择接口：欲配置的接口的名称；
- IP 地址 1：该接口的 IP 地址；
- 子网掩码 1：该接口的子网掩码；
- IP 地址 2：该接口的第二个 IP 地址；
- 子网掩码 2：该接口的第二子网掩码；
- MAC 地址：该接口的 MAC 地址（一般情况下不需要修改）；
- ARP 代理：是否在该接口启用 ARP 代理功能。选项如下：
  Disabled：在该接口禁用 ARP 代理功能，为缺省配置；
  Enabled：在该接口启用 ARP 代理功能；
  Nat：在该接口启用 NAT 类型的 ARP 代理功能；
- 模式：该接口的工作模式。Auto—自适应，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
- 保存：接口配置参数生效；
- 重填：恢复到修改前的配置参数。
- **提示**：

1. 设备支持为每个物理接口配置两个不同网段的 IP 地址，支持连接两个不同的网段，而且可以相互通讯；

2. 如果改变了 LAN 口的“ IP 地址 ”，在保存之后，必须使用新的 IP 地址才能登录 WEB 界面管理，并且，局域网中计算机的默认网关必须设置成该 IP 地址才能正常上网；

3. 可以到***系统状态***—>***路由和端口信息***中查看各个端口实际连接状态，其中，LAN 接口集成了多个交换机端口。

5.4.2 接口配置信息列表

表 5-15 接口配置信息列表

- 浏览接口配置信息：如果已经配置了各个接口的相关信息，可在“ 接口配置信息列表 ”中查看各个接口配置状态信息，如表 5-15 所示；
- 编辑接口配置信息：如果需要编辑修改某个接口的配置信息，则首先在配置界面的“ 选择接口 ”中选中该接口的名称，或者在“ 接口配置信息列表 ”中单击对应条目的“ 接口名称 ”超链接，其信息就会填充到相应的编辑框内，然后即可修改该接口的相关信息；
- 刷新：单击“ 刷新 ”按钮，可查看最新的接口配置信息。

5.4.3 配置 IP 地址

第一步，进入***基本配置***—>***接口配置***页面；

第二步，选择需要配置 IP 地址的物理接口；

第三步，设置该接口的 IP 地址和子网掩码：在“ IP 地址 1 ”中填入 IP 地址，在“ 子网掩码 ”中填入子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：在这里可以快速配置、修改各接口的 IP 地址和子网掩码。

5.4.4 配置第二个 IP 地址

第一步，进入***基本配置***—>***接口配置***页面；

第二步，选择需要配置第二个 IP 地址的物理接口；

第三步，设置该接口的第二个 IP 地址和子网掩码：在“ IP 地址 2 ”中填入第二个 IP 地址，在“ 子网掩码 2 ”中填入第二个子网掩码；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置第二个 IP 地址。只有在同一个接口需要配置两个不

同网段的情况下，才配置第二个 IP 地址。

5.4.5 配置 MAC 地址

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置 MAC 地址的物理接口；

第三步，设置该接口的 MAC 地址：在“ MAC 地址 ”中填入该接口的 MAC 地址；

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要配置 MAC 地址。但是某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会造成新的网络设备无法正常获得 IP 地址的现象，此时需要将新的网络设备的 MAC 地址设置成和原有网络设备的 MAC 地址相同。

5.4.6 配置 ARP 代理

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置 ARP 代理的物理接口；

第三步，设置该接口的 ARP 代理：在“ ARP 代理 ”中选择“ Disabled ”（禁用 ARP 代理功能）、“ Enabled ”（启用 ARP 代理功能）或者“ Nat ”（启用 NAT 类型的 ARP 代理功能）。

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要修改，即接口默认关闭 ARP 代理功能。某些情况下，可能需要启用 ARP 代理功能，比如在 PPTP/L2TP VPN 中，当设备作为 PPTP/L2TP 服务器时，如果它分配给客户端（使用移动用户帐号）的 IP 地址和它连接的局域网在一个子网内，就需要在设备上启用 ARP 代理功能。另外，NAT 环境下，当某个广域网接口使用多地址接入时，一般都需启用 NAT 类型的 ARP 代理功能。

5.4.7 配置以太网工作模式

第一步，进入***基本配置—>接口配置***页面；

第二步，选择需要配置以太网工作模式的物理接口；

第三步，设置该接口的工作模式：在“ 模式 ”中选择工作模式。

第四步，单击“ 保存 ”按钮，配置完成。

提示：一般情况下，不需要修改，即接口默认自适应工作模式。如有兼容性问题，或使用的设备不支持自动协商功能，才需要设置该接口的工作模式。

5.5 DDNS 配置

本节主要讲述***基本配置—>DDNS 配置***的配置方法。

提示：只有在***系统管理—>时钟管理***中正确配置了设备的系统时间和时区信息，DDNS 功能才能正常工作。

动态域名解析服务（DDNS）是将一个固定的域名解析成动态变化的 IP 地址（如 ADSL 拨号上网）的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务收取一定的费用。在此情况下，艾泰科技会尽可能及时通知。如拒绝支付该等费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

目前，艾泰科技仅提供对 iplink.com.cn 的 DDNS 服务的支持，将来还将陆续提供对其他 DDNS 服务的支持。

5.5.1 申请 DDNS 帐号

请登录 http://www.utt.com.cn/ddns 申请后缀为 iplink.com.cn 的二级域名。

动态域名注册表

(IPLINK.COM.CN)

公司名称:	上海艾泰科技有限公司
地址:	上海市世纪大道1500号东方大厦1429室
邮编:	200122
电话:	021-50623736
传真:	021-68416675
联系人:	艾泰科技
电子邮件:	support@utt.com.cn
管理员用户名:	support
管理员密码:	********
确认密码:	********
主机名:	utt .iplink.com.cn
动态域名用途:	☐ 网站 ☑ VPN ☐ VoIP ☐ 其它
注册类型:	○ 付费 ○ 购买产品 产品名称: HiPER路由器 序 列 号: 4201183
注：为更好的提供服务，请填写所有栏目，否则注册无效。 我们不会把注册信息在未经您授权的情况下用于其它任何场合。 提示：将鼠标停留在每个项目上可以查看相应的填写说明。	
提交 重填	

表 5-16 动态域名注册表

- 主机名：填入欲申请的二级域名（为避免重复，请填写设备底板上的全球唯一序列号 S/N）；
- 序列号：产品序列号。它和设备的***基本配置—>DDNS 配置***中的“ 注册号 ”必须一致。
- 提交：单击“ 提交 ”按钮，即可获得设备匹配该二级域名的 ENKEY（请妥善保管此密码）；

enKey: T94eOJBlYOK+5gNNP9seYXUMeXvAWpVJtlbVRvNsdID6

- 重填：重新填写动态域名注册表。

提示：同一个域名只能被注册一次，而且在使用不同的设备申请同一个域名时获得的“ enkey ”是不同的，所以在更换设备而没有更换域名时，需要登录 http://www.utt.com.cn/ddns 的管理界面先删除原先申请的域名，之后再重新申请。

5.5.2 配置 DDNS 服务

图 5-12 DDNS 服务配置

- 启用 DDNS 服务：启用或者禁用 DDNS 服务，选中为启用；
- 注册域名：单击 http://www.utt.com.cn/ddns 超链接，即可进入该页面申请域名；
- 注册号：产品注册号；
- 服务商：选择提供域名服务的服务商，目前只支持 iplink.com.cn 的 DDNS 服务；
- 主机名：申请 DDNS 帐号时使用的主机名。为避免重复，建议使用设备的底板上的全球唯一序列号 S/N 申请；
- 域名：选择指定 DDNS 服务商提供的域名；
- 密钥（enKey）：申请 DDNS 帐号时得到的 enKey；
- 确认密钥：申请 DDNS 帐号时得到的 enKey，此处与上一栏中所填密钥一致。
- 保存：DDNS 配置生效；
- 重填：恢复到修改前的配置参数。

5.5.3 DDNS 状态

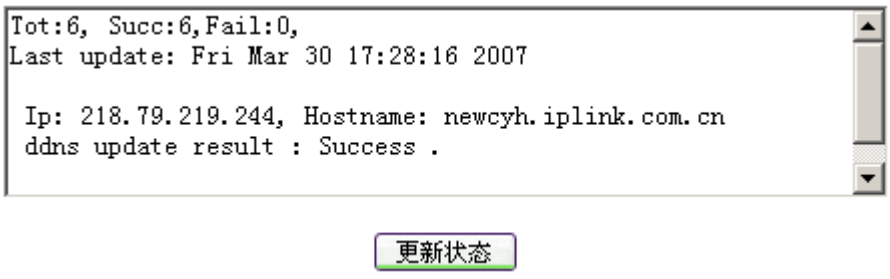


图 5-13 DDNS 状态

- 更新状态：单击“ 更新状态 ”按钮，可将当前 PPPoE 连接的 IP 地址更新到动态域名系统中。

  常用 DDNS 状态信息解释如表 5-17 所示。

状态信息	信息涵义
Tot: 6, Succ: 6, Fail:0	共更新 6 次，成功 6 次，失败 0 次
Last update: Fri Mar 30 17:28:16 2007	最后更新时间为 2007 年 3 月 30 日星期五 17 时 28 分 16 秒
Ip: 218.79.219.244	当前分配的 IP 地址
Hostname: newcyh.iplink.com.cn	主机名（动态域名）
ddns update result : Success	将当前 PPPoE 连接的 IP 地址（218.79.219.244）成功更新到动态域名（newcyh.iplink.com.cn）上

表 5-17 DDNS 状态信息

5.5.4 DDNS 验证

可以在局域网计算机的 DOS 状态下，使用 Ping 命令（例如：ping utt.iplink.com.cn）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：61.171.212.7），证明域名解析正确。注意：一般情况下，设备在使用 NAT 后，从 Internet 上将不能 ping 通设备的 IP 地址，只能解析出该域名对应的 IP 地址。

```
C:\>ping utt.iplink.com.cn

Pinging utt.iplink.com.cn [61.171.212.7] with 32 bytes of data:
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255
Reply from 61.171.212.7: bytes=32 time<1ms TTL=255

Ping statistics for 61.171.212.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

提示：

1. DDNS 功能目前只支持“默认线路”是 PPPoE 拨号接入的情况，而且必须先通过 WEB 管理界面配置了 PPPoE 连接才能正常工作。没有配置或者是通过其他方式配置 PPPoE 连接，系统会弹出如图 5-14 所示对话框：

图 5-14 对话框——请先配置 PPPoE

2. ISP（例如中国电信）分配给“默认线路”的 PPPoE 连接线路的 IP 地址是公网 IP

地址的时候才能保证该域名能被 Internet 的用户访问；

3. 不同设备注册相同的域名得到的 ENKEY 不同；

4. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射；

5. 若出现如下错误信息（如图 5-15），请检查：在***系统管理***—>***时钟管理***中检查当前系统时钟是否正确；在***系统状态***—>***系统信息***的“ 系统历史记录 ”中检查 PPPoE 连接是否成功；在 http://www.utt.com.cn/ddns 检查在线申请的 ENKEY 是否正确。

图 5-15 DDNS 状态

6. 暂停 DDNS 更新服务：在***基本配置***—>***DDNS 配置***中，取消“ 启用 DDNS 服务 ”的选中，单击“ 保存 ”按钮即可暂停 IP 地址的更新。但是，如果你暂停了 DDNS 服务，而且 WAN 口已经离线并且释放了 IP 地址。当这个被释放的 IP 地址被 ISP 分配给其他用户使用时，此时解析域名仍旧会解析到这个 IP 地址，这样就有可能造成域名和实际用户不符的现象。

5.6 时间段配置

本节主要讲述***基本配置—>时间段配置***的配置方法。

提示：只有在***系统管理—>时钟管理***中，为设备设置了正确的时间后，时间段功能才能正常工作。

配置时间段策略，可以被某些高级功能（如拨号时间段、防火墙）引用，以控制这些业务的生效时间，从而达到控制上网费用、控制游戏时间等目的。

一个时间段最多可以由 8 个时间单元组成，同时还可通过参数“ 开始日期和时间 ”和“ 结束日期和时间 ” 设置该时间段的生效时间（如图 5-16）。当时间段有效期已过，该时间段无效。“ 开始日期和时间 ”、“ 结束日期和时间 ” 均设成 1990 年 1 月 1 日 00:00:00，代表该时间段永久有效。

5.6.1 时间段配置

图 5-16 时间段配置

- 时间段名称：时间段策略的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 开始日期和时间：该时间段策略生效的开始日期和时间，系统默认为 1989 年 1 月 1 日 00:00:00（单位：时:分:秒）；
- 结束日期和时间：该时间段策略生效的结束日期和时间，系统默认为 2010 年 1 月 1

日 00:00:00（单位：时:分:秒）；

- 时间单元一～时间单元八：该时间段要控制的时间单元，一个时间段最多可由 8 个时间单元组成；
- 类型：时间单元的类型，类型有每天、星期一、星期二、……、星期日、工作日（周一至周五）、周末（周六、周日）等；
- 开始时间：每个时间单元的开始时间，系统默认为 00:00:00（单位：时:分:秒）；
- 结束时间：每个时间单元的结束时间，系统默认为 23:59:59（单位：时:分:秒）；
- 保存：时间段配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：一个跨越零点的连续时间段，必须配置成两个连续的时间单元，例如，从晚上 8 点到次日凌晨 5 点需要以 24:00:00 分为两个时间段，即第一个时间单元为 20:00:00～23:59:59，第二个时间单元为 00:00:00～05:00:00。

5.6.2 时间段列表

表 5-18 时间段信息列表

- 增加时间段：选中“ 添加 ”选项，输入时间段信息，单击“ 保存 ”按钮，生成新的时间段；
- 浏览时间段：如果已经配置了时间段，可在“ 时间段信息列表 ”中浏览相关信息，如表 5-18 所示；
- 编辑时间段：如果想编辑某一时间段，只需单击此时间段条目中的“ 时间段名称 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除时间段：选中一些时间段，单击右下角的“ 删除 ”按钮，即可删除被选中的时间段；
- 查看时间段详细信息：单击某个时间段条目中的“ 详细 ” 超链接，可显示该时间段的详细信息，以及被其他功能（如防火墙）引用的相关信息，如图 5-17 所示。

图 5-17 时间段详细信息

5.6.3 自定义时间段

第一步，进入***基本配置—>时间段配置***页面；

第二步，单击“ 添加 ”按钮，填写时间段名称；

第三步，根据需要填写该时间段的起止时间；

第四步，填写时间段具体时间单元信息；

第五步，单击“ 保存 ”按钮，时间段配置完成，可在“ 时间段信息列表 ”中看到添加的记录；

第六步，继续添加新的时间段信息。

提示：若要删除时间段，只需在“ 时间段信息列表 ”中选中要删除的时间段，单击“ 删除 ”按钮，即可删除。

5.6.4 时间段配置实例

1. 应用需求

2007 年度某公司为控制销售部门员工的上网行为，针对其实际需求，规定在工作时间中只允许 WEB 业务，在其余时间则开放所有业务。该公司的工作时间为：周一～周五，上午 9 点～12 点，下午 1 点～6 点；中午 12 点～13 点为午间休息时间。

2. 分析

由上，可以将该公司上网时间划分为工作时间（worktime）和休息时间（freetime）两个时间段。

1) 工作时间段划分为 2 个时间单元，具体信息如下：

开始日期和时间：2007 年 1 月 1 日 00:00:00

结束日期和时间：2007 年 12 月 31 日 23:59:59

时间单元一：类型为“ 工作日（周一至周五）”，开始时间 09:00:00，结束时间 11:59:59

时间单元二：类型为“ 工作日（周一至周五）”，开始时间 13:00:00，结束时间 17:59:59

2) 由于休息时间段划分为 4 个时间单元，具体信息如下：
开始日期和时间：2007 年 1 月 1 日 00:00:00
结束日期和时间：2007 年 12 月 31 日 23:59:59
时间单元一：类型为“ 工作日（周一至周五）”，开始时间 00:00:00，结束时间 08:59:59
时间单元二：类型为“ 工作日（周一至周五）”，开始时间 12:00:00，结束时间 12:59:59
时间单元三：类型为“ 工作日（周一至周五）”，开始时间 18:00:00，结束时间 23:59:59
时间单元四：类型为“ 周末（周六、周日）”，开始时间 00:00:00，结束时间 23:59:59

3. 配置步骤

第一步，进入***基本配置—>时间段配置***页面；

第二步，配置工作时间段“ worktime ”。选中“ 添加 ”选项，如图 5-16 所示，在“ 时间段名称 ”中填入 worktime；

第三步，设置 worktime 起止时间：
在“ 开始日期和时间 ”中填入 2007 年 1 月 1 日 00:00:00，
在“ 结束日期和时间 ”中填入 2007 年 12 月 31 日 23:59:59；

第四步，分别设置该时间段的 2 个时间单元，首先选择类型，然后填入开始时间和结束时间：
时间单元一 :在“ 类型 ”中选择“ 工作日（周一至周五）”, 在“ 开始时间 ”中填入 09:00:00，在“ 结束时间 ”中填入 11:59:59；
时间单元二 :在“ 类型 ”中选择“ 工作日（周一至周五）”, 在“ 开始时间 ”中填入 13:00:00，在“ 结束时间 ”中填入 17:59:59；

第五步，单击“ 保存 ”按钮，时间段“ worktime ”设置成功；

第六步，配置休息时间段“ freetime ”。选中“ 添加 ”选项，如图 5-18 所示，在“ 时间段名称 ”中填入 freetime；

图 5-18 时间段配置——实例

第七步，设置 freetime 起止时间：
在“ 开始日期和时间 ”中填入 2007 年 1 月 1 日 00:00:00，

在“结束日期和时间”中填入 2007 年 12 月 31 日 23:59:59；

第八步，分别设置该时间段的 4 个工作单元，首先选择类型，然后填入开始时间和结束时间。

时间单元一：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 00:00:00，在“结束时间”中填入 08:59:59；

时间单元二：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 12:00:00，在“结束时间”中填入 12:59:59；

时间单元三：在“类型”中选择“工作日（周一至周五）”，在“开始时间”中填入 18:00:00，在“结束时间”中填入 23:59:59；

时间单元四：在“类型”中选择“周末（周六、周日）”，在“开始时间”中填入 00:00:00，在“结束时间”中填入 23:59:59；

第九步，单击“保存”按钮，时间段“freetime”设置成功。

至此，时间段“worktime”和“freetime”配置成功，可在“时间段信息列表”（如表 5-18）中查看、编辑它们。

第6章 系统管理

在系统管理中，主要设置设备相关管理参数，包括管理员配置、时钟管理、软件升级、配置管理、WEB 服务器配置、SNMP 配置、SYSLOG 配置等等。

6.1 管理员配置

本节主要讲述***系统管理***—>***管理员配置***的配置方法，如图 6-1 所示。

6.1.1 WEB 界面管理员配置

图 6-1 管理员配置

- 管理员用户名：新 WEB 管理员的用户名。自定义，不能重复。取值范围：1～31 个字符；
- 密码：该管理员的登录密码；
- 确认密码：该管理员的登录密码，此处必须和上一栏所填密码一致；
- 管理员组：该管理员所属的管理员组，不同的管理员组提供不同级别的管理权限。系统提供“ 浏览 ”、“ 执行 ” 及 “ 系统管理 ” 三个管理员组，各组提供的权限如下：
  - 浏览：本组中的管理员只能查看各页面，但***上网监控***页面除外。注意，在本页面只能查看到当前登录用户的配置信息，其登录密码可修改；
  - 执行：本组中的管理员可查看或修改各页面，但***上网监控***页面除外。注意，在本页面只能查看到当前登录用户的配置信息，其登录密码可修改；
  - 系统管理：本组中的管理员可以任意查看和修改所有页面。
- 允许 telnet 远程登录：允许或者禁止该管理员通过 telnet 管理设备，选中为允许。只有 “ 系统管理 ” 组中的管理员才有 telnet 权限，而且最多只允许设置 3 个有 telnet 权限的管理员。
- 保存：管理员配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 设备允许用户使用同一个 “ 管理员用户名 ” 从多个 IP 地址同时登录。注意，为避免配置冲突，建议同时只从一个 IP 地址登录修改配置；

2. 为安全起见，强烈建议修改初始的管理员密码，并谨慎保管管理员用户名及密码。

6.1.2 管理员信息列表

表 6-1 管理员信息列表

- 增加管理员：选中“ 添加 ”选项，输入管理员信息，单击“ 保存 ”按钮，生成新的管理员；
- 浏览管理员：如果已配置了若干管理员，可在“ 管理员信息列表 ”中浏览相关信息，如表 6-1 所示；
- 编辑管理员：如果想编辑某个管理员，只需单击该“ 管理员用户名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除管理员：选中若干管理员，单击右下角的“ 删除 ”按钮，即可删除被选中的管理员。

提示：禁止删除系统默认管理员 Default。

6.1.3 自定义管理员

第一步，进入***系统管理—>管理员配置***页面；

第二步，选中“ 添加 ”选项，根据需要填写“ 管理员用户名 ”、“ 密码 ”和“ 确认密码 ”；

第三步，根据需要设置“ 管理员组 ”。如果“ 管理员组 ”设置为“ 系统管理 ”，还可根据需要设置“ 允许 telnet 远程登录 ”；

第四步，单击“ 保存 ”按钮，该管理员添加成功，可以在“ 管理员信息列表 ”可看到相关记录；

第五步，继续添加新的管理员。

提示：若要删除管理员，只需在“ 管理员信息列表 ”中选中要删除的管理员，单击“ 删除 ”按钮，即可删除。

6.2 时钟管理

本节主要讲述***系统管理—>时钟管理***的配置，如图 6-2 所示。

为了保证设备各种涉及到时间的功能（如 DDNS 服务、时间段配置等）正常工作，需要准确地设定设备的时钟，使其与当地标准时间同步。

设备提供“手工设置时间”或者“网络时间同步”这两种设置系统时间的方式，不过，每次只能选择其中的一种方式来设置时间。

使用“网络时间同步”功能可从互联网上获取标准的时间，当下次开机连接到 Internet 后，设备将会自动获得标准的时间。

图 6-2 时钟管理配置

- 当前系统时间：显示当前设备时钟（单位：年:月:日，时:分:秒）；
- 时区选择：选择设备所在地的国际时区，只有选择了正确的时区，网络时间同步（sntp）功能才能正常工作；
- 手工设置时间：手工输入当前的日期和时间（单位：年:月:日，时:分:秒）；
- 网络时间同步（sntp）：使用网络时间同步功能，设置了正确的 sntp 服务器后，当设备连接到 Internet 之后，就会自动和所设置 sntp 服务器同步时间。系统缺省预设两个 sntp 服务器 192.43.244.18、129.6.15.28，一般情况下不需要修改。若需更多 sntp 知识及服务器，可访问 http://www.ntp.org。
- 保存：时钟管理配置参数生效；
- 重填：恢复到修改前的配置参数。

6.3 软件升级

本节主要讲述***系统管理—>软件升级***的配置方法。

6.3.1 显示和保存当前运行软件

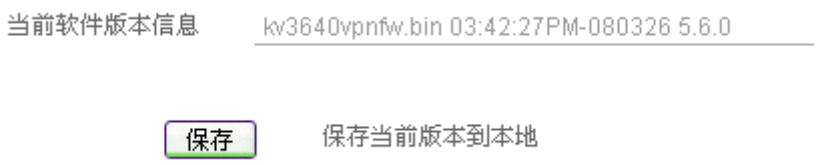
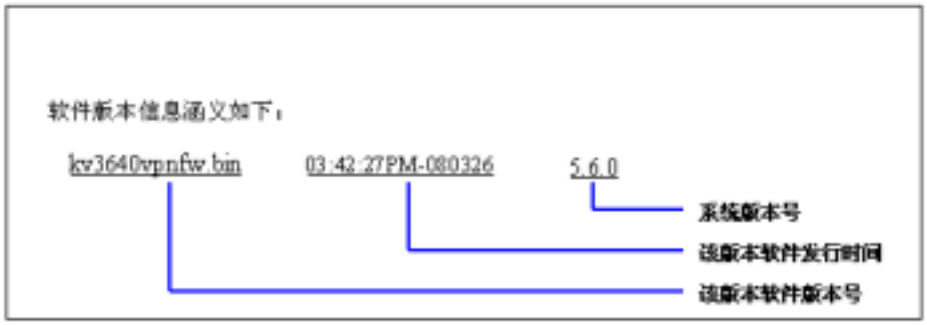


图 6-3 显示和保存当前软件

软件版本信息涵义如下：



保存：将系统当前运行的软件备份到管理计算机的硬盘中。

提示：在这里只保存系统的运行软件，并没有保存系统当前的配置文件。

6.3.2 软件升级

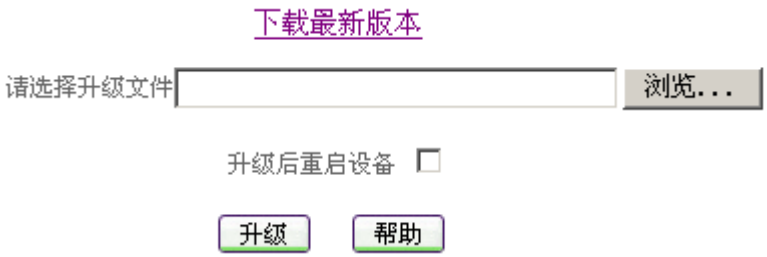


图 6-4 软件升级

第一步 下载最新软件

单击“ 下载最新版本 ”超链接，到上海艾泰科技公司官方网站下载最新的软件版本到本地计算机。

提示：

1. 请选择合适型号的最新软件；下载的软件适用的硬件平台必须和当前产品的硬件平

台一致，软件版本必须比当前使用的软件版本新；

2. 建议升级之前，先到***系统管理***—>***配置管理***备份系统当前配置。

第二步 选择升级软件所在路径

在“请选择升级文件”文本框中输入将要升级的软件在本地计算机的路径，或者是通过“浏览”在本地计算机选择新软件。

- 升级后重启设备：升级软件成功之后，必须重启设备，新软件才能生效。可以选中“升级后重启设备”，设备将在软件升级成功后自动重启。如果没有选中“升级后重启设备”，请在升级成功后选择合适的时间重启设备。

第三步 更新设备的软件

单击“升级”按钮，更新设备的软件。

提示：

1. 强烈建议在设备负载比较轻（用户比较少）的情况下升级；
2. 定期的升级设备的软件，可以使设备获得更多的功能或者更佳的工作性能。正确的软件升级并不会改变当前设备设置；
3. 升级过程不能关闭设备电源，否则将会导致不可预期的错误甚至不可恢复的硬件损坏；

6.4 配置管理

本节主要讲述***系统管理—>配置管理***的配置方法。

6.4.1 保存当前配置

图 6-5 保存配置

- 保存：将设备当前运行的配置下载到管理员计算机中，并保存成一个文本文件。

6.4.2 导入配置

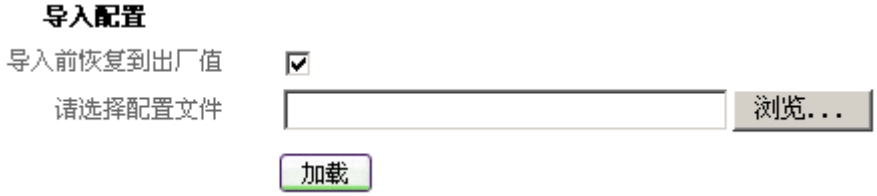


图 6-6 导入配置

- 导入前恢复到出厂值：选中或不选中，缺省为选中。
  如果选中，则表示在单击“ 加载 ”按钮后，系统将首先执行恢复出厂配置的操作，再执行加载配置的操作；
  如果不选中，则表示在单击“ 加载 ”按钮后，系统将直接执行加载配置的操作。
- 请选择配置文件 :可在此输入配置文件在本地计算机存放的路径，也可直接单击“ 浏览 ”按钮选择配置文件。
- 加载：首先在“ 请选择配置文件 ”中选择欲加载的配置文件，再单击“ 加载 ”按钮，就可以将该配置文件加载到设备中。
- **提示**：在加载配置过程中请不要关闭设备电源，以避免不可预期的错误。

6.4.3 恢复出厂配置

图 6-7 恢复出厂配置

- 恢复 ：将设备的配置恢复到出厂时的设置值。
- **提示**：

1. 这是一个非常危险的操作，它将删除所有自定义的配置，并将系统恢复到原始状态。强烈建议在恢复出厂配置之前，在***系统管理—>配置管理***的“ 保存当前配置 ”中，将设备运行的配置保存；

2. 设备的出厂管理员用户名为：Default、默认密码为空；默认 LAN 口 IP 地址/子网掩码为：192.168.16.1/ 255.255.255.0。执行恢复出厂配置之后，建议在***系统管理—>配置管理***的“ 重新启动设备 ”中，重启设备。

6.4.4 重新启动设备

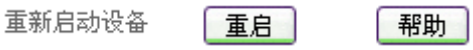


图 6-8 重新启动设备

- 重启：将设备重新启动一次。
- **提示**：重启时，所有的用户将断开到设备的连接，请谨慎使用此功能。

6.5 WEB 服务器

本节主要讲述***系统管理—>WEB 服务器***的配置方法，如图 6-9 所示。在本页面，主要配置设备的 WEB 管理界面后台服务器的相关参数。

图 6-9 WEB 服务器配置

- web 空闲超时时间：通过 WEB 管理界面管理设备时，如果超过该时间没有任何操作，设备的 Web Server 将自动断开与浏览器的连接。缺省值为 300 秒；
- web 最大并发连接数：管理员通过 WEB 配置设备时，将会有多条 TCP 连接连到设备。该参数默认值是 60，范围为 10~60，一般无需设置；
- 内部端口：从局域网通过 WEB 管理设备的 HTTP 端口，默认为 80。若修改该值，就必须用“ IP 地址：端口 ”的方式（如 http://192.168.16.1:88）才能登录设备；
- 登录页面：下次登录设备时，将直接登录到此处设置的页面。
- 更换皮肤：设备提供“ 时尚绿色 ”界面色彩风格；
- 启用自动刷新：启用或者关闭自动刷新功能。启用自动刷新功能后，设备的 Web Server 将每隔单位时间自动刷新***系统状态—>系统信息***、***系统状态—>NAT 统计***等页面；
- 刷新时间间隔：设备的 Web Server 自动刷新 WEB 界面的间隔时间（单位：秒）；
- 保存：WEB 服务器配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：为保障设备有足够的性能提供服务，请尽可能减少 Web 并发连接的数量，同时不要选择自动刷新。

6.6 SNMP 配置

本节主要讲述***系统管理—>SNMP 配置***的配置方法，如图 6-10 所示。

SNMP 是一系列协议组和规范，它提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。在设备上启用了 SNMP 服务，就可以在远程使用 SNMP 软件管理和监视设备。

图 6-10 SNMP 配置

- 启用 SNMP 服务：禁止或者允许 SNMP 服务。为安全起见，目前只允许 SNMP 服务器读设备信息，不允许 SNMP 服务器修改设备信息；
- SNMP 社区名：SNMP 社区名，它必须和 SNMP 网络管理软件包配置匹配。默认的 SNMP 社区名“ uTt22aA ”，为安全起见，建议修改这个系统默认值，从而防止入侵者通过 SNMP 的访问请求获取设备上的网络配置信息；
- 设备名：设备的主机名；
- 联系人：设备的管理员联系方式；
- 位置：设备的物理位置信息；
- 只允许以下主机管理：选中“ 只允许以下主机管理 ”后，可以设置 1～3 台主机，只有这三台主机可以通过 SNMP 管理设备；
- 允许主机 1，2，3：可通过 SNMP 管理设备的主机的 IP 地址。
- 保存：SNMP 配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：只有在***系统管理—>远程管理***中启用 SNMP 远程管理功能之后，才能从 Internet 通过 SNMP 服务器远程管理设备。

6.7 SYSLOG 配置

本节主要讲述***系统管理—>SYSLOG 配置***（如图 6-11）的配置方法。

syslog 里面记载了设备的大量运行信息，是管理员每日需要查看的记录。对管理员分析系统的状况、监视设备的活动来说，是一个相当重要的部分。

图 6-11 SYSLOG 配置

- 启用 syslog 服务：启用或禁用 syslog 服务，选中为启用；
- syslog 服务器的地址：设置 syslog 服务器的地址，可以是域名或 IP 地址；
- syslog 服务器的端口：设置 syslog 服务器所开放的服务端口，一般默认为 514；
- syslog 消息类型：local0～local7，由 syslog 管理员自定义的一些消息类型；
- syslog 消息发送间隔：设备将按照设置的时间间隔定期向 syslog 服务器发送“ 心跳 ”消息，表示自己是存活的。缺省值为 0，表示不主动发送“ 心跳 ”消息。
- 保存：syslog 配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：目前，仅艾泰科技公司的 Xport 设备 Manager 管理软件能识别设备发送的 syslog“ 心跳 ”消息。

6.8 远程管理

本节主要讲述***系统管理—>远程管理***的配置方法。

由于设备内置了防火墙，将会屏蔽所有来自 Internet 的连接。如果要从 Internet 远程管理设备，必须启用相关的远程管理功能。但是如果关闭了 NAT 功能，相关功能将失效。

图 6-12 远程管理

- HTTP：允许或禁止从 Internet 通过 WEB 管理设备，设备默认外部 WEB 管理端口为 8081 。如要从 Internet 通过 WEB 管理设备必须用“ IP 地址：端口 ”的方式（例如 http://218.21.31.3:8081）才能登录设备；
- 外部端口：可以修改设备默认外部端口（默认值为 8081）。注意，这个端口修改成 80 以后，在***高级配置—>NAT 和 DMZ 配置***的“ NAT 静态映射列表 ”中，就会增加一条 TCP80 端口的映射，此时如需要再次增加局域网 WEB 服务器的映射，就会引起冲突。
- SNMP：允许或禁止从 Internet 通过 SNMP 管理设备，选中为允许；
- TELNET：允许或禁止从 Internet 通过 TELNET 管理设备，选中为允许。
- 保存：远程管理配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 设备的 Internet 地址可以从***基本配置—>线路配置***的“ 线路连接信息列表 ”中获得；
2. 为安全起见，如非必要，请不要启用 Internet 远程管理功能；在启用 Internet 远程管理功能之前，请先到***系统管理—>管理员配置***中修改设备默认密码；
3. 如果“ 默认线路 ”采用了 PPPoE 拨号，其 IP 地址是动态的，可以在***基本配置—>DDNS 配置***中配置 DDNS 功能；
4. 打开了 HTTP、SNMP、TELNET 管理功能之后，系统会自动生成 TCP:8081 端口、UDP:161 端口、TCP:23 端口的 NAT 静态映射（可在***高级配置—>NAT 和 DMZ 配置***的“ NAT 静态映射列表 ”查看），它们都绑定在“ 默认线路 ”上；
5. 在寻求艾泰科技客服工程师服务之前，请事先打开相关远程管理功能。

第7章 高级配置

本章主要讲述如何设置设备的组管理、NAT 和 DMZ 配置、路由配置、IP/MAC 绑定、特殊功能、DHCP 高级功能以及 UPnP 高级属性的相关参数。

7.1 组管理

本节主要讲述***高级配置***—>***组管理***的配置方法。

在设备引入了工作组这个概念，可以将具有共同性质（如业务要求相同）的用户划分在同一个工作组中，并给他们分配连续的 IP 地址。并且，允许配置只有一个用户的特殊工作组，其起始 IP 地址和结束 IP 地址相同，我们将之称为个人用户。注意：不同工作组的 IP 地址不能重叠；但是个人用户的 IP 地址可以属于某工作组（非个人用户）的地址范围之内。

设置工作组时，还可以为该组设置组策略，组策略包括以下参数：禁止 QQ、禁止 MSN、禁止 P2P、最大下载速率、最大上传速率、最小下载速率、最小上传速率以及信用额度，其中，最大下载速率、最大上传速率、最小下载速率、最小上传速率以及信用额度用于限制该组用户的上网带宽，具体的涵义及设置方法请参见章节“ 10.1 带宽信用管理 ”。

配置了工作组之后，就可在***安全配置***—>***防火墙***中使用“ 普通视图 ”为工作组中的用户定义上网权限和上网时间。当某个工作组已经被某条防火墙策略引用时，编辑该组的起始/结束 IP 地址，相关策略的引用同时发生改变；此时，禁止删除该工作组，只有在取消相关引用之后，才能删除。

7.1.1 工作组配置

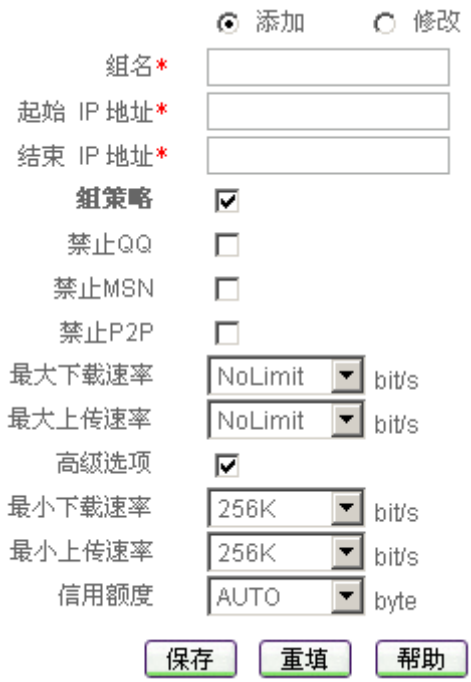


图 7-1 工作组配置

- 组名：工作组的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 起始 IP 地址：该工作组的起始 IP 地址；
- 结束 IP 地址：该工作组的结束 IP 地址；
- 组策略：启用或禁用组策略，打勾表示启用组策略；
- 禁止 QQ：允许或禁止该组内的所有用户使用 QQ 聊天；
- 禁止 MSN：允许或禁止该组内的所有用户使用 MSN 聊天；
- 禁止 P2P：允许或禁止该组内的所有用户进行 P2P 下载；
- 最大下载速率：该组用户的最大下载速率；
- 最大上传速率：该组用户的最大上传速率；
- 最小下载速率：该组用户的最小下载速率；
- 最小上传速率：该组用户的最小上传速率；
- 信用额度：该组用户所能累计的信用的最大值；
- 保存：工作组配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：IPSSG 组为系统默认工作组，其起始 IP 地址和结束 IP 地址均为 0.0.0.0，禁止编辑和删除。IPSSG 组包括局域网中未配置业务策略的所有用户。

7.1.2 工作组列表

组信息列表 4/21

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	组名	起始IP地址	结束IP地址	组策略	禁止QQ	禁止MSN	禁止P2P	最大下载速率	最大上传输率	最小下
☐	Sale	192.168.16.50	192.168.16.70	启用	No	No	No	256K	128K	2
☐	Technique	192.168.16.120	192.168.16.150	启用	Yes	No	Yes	NoLimit	NoLimit	2
☐	Admin	192.168.16.160	192.168.16.180	不启用						
☐	IPSSG	0.0.0.0	0.0.0.0	不启用						

☐ 全选 / 全不选 删除

表 7-1 组信息列表

组信息列表 4/21

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

IP地址	组策略	禁止QQ	禁止MSN	禁止P2P	最大下载速率	最大上传输率	最小下载速率	最小上传输率	信用额度	编辑
8.16.70	启用	No	No	No	256K	128K	256K	128K	AUTO	编辑
8.16.150	启用	Yes	No	Yes	NoLimit	NoLimit	256K	256K	AUTO	编辑
8.16.180	不启用									编辑
0.0.0	不启用									编辑

☐ 全选 / 全不选 删除

表 7-2 组信息列表（续表 7-1）

- 增加工作组：选中“ 添加 ”选项，输入工作组信息，单击“ 保存 ”按钮，生成新的工作组；

- 浏览工作组：如果已经生成了工作组，可在“ 组信息列表 ”中浏览相关信息，如表 7-1、7-2 所示；
- 编辑工作组：如果想编辑某个工作组，只需点击该工作组的“ 组名 ”或 “ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”，修改完毕；
- 删除工作组：选中一些工作组，单击右下角的“ 删除 ”按钮，即可删除被选中的工作组。

提示：如果在***安全配置***—>***防火墙***中使用“ 普通视图 ”定义了新个人用户策略，在“ 组信息列表 ”将自动增加该用户的信息记录，即增加一个个人用户，其“ 组名 ”为该用户的 IP 地址，在本页面可以修改或删除相关信息。

7.1.3 自定义工作组

第一步，规划局域网中的 IP 地址，将局域网 IP 划分成若干个连续的地址段，一般是将具有共同性质的用户划分到同一个工作组，实现统一管理，例如一个部门可以分为一个组。

第二步，进入***高级配置***—>***组管理***页面；

第三步，选择“ 添加 ”选项，输入工作组的“ 组名 ”、“ 起始 IP 地址 ”和“ 结束 IP 地址 ”，并根据该组的性质和权限为该组设置合适的组策略；

第四步，单击“ 保存 ”按钮，该工作组添加成功，可以在“ 组信息列表 ”中看到相应的记录；

第五步，继续配置其他工作组。

提示：若要删除工作组，只需在“ 组信息列表 ”中选中要删除的工作组，单击“ 删除 ”按钮，即可删除。

7.1.4 工作组配置实例

1. 应用要求

某公司为实现上网统一管理，针对各部门上网实际需求，决定对管理部门、技术部门、销售部门进行分组管理，将这三个部门划分成三个工作组，不同的工作组设置不同的组策略，从而能够实现对这三个部门的上网行为控制。各工作组具体配置信息如表 7-3 所示：

部门名	组名	起始 IP 地址	结束 IP 地址	组策略
销售部门	Sale	192.168.16.50/24	192.168.16.70/24	最大下载速率：256K；最大上传速率 128K
技术部门	Technique	192.168.16.120/24	192.168.16.150/24	禁止 QQ；禁止 P2P
管理部门	Admin	192.168.16.160/24	192.168.16.180/24	不启用

表 7-3 工作组配置信息

2. 配置步骤

第一步，规划局域网中的 IP 地址及每组要设置的组策略，如表 7-3 所示；

第二步，进入***高级配置***—>***组管理***页面；

第三步，配置工作组 Sale。选择“ 添加 ”选项，如图 7-2 所示。在“ 组名 ”中填入“ Sale ”，在“ 起始 IP 地址 ”中填入“ 192.168.16.50 ”，在“ 结束 IP 地址 ”中填入“ 192.168.16.70 ”，“ 最

大下载速率 ” 选择 “ 256K ”，“ 最大上传速率 ” 选择 “ 128K ” 然后单击 “ 保存 ” 按钮，工作组 Sale 配置完成。

图 7-2 工作组 Sale 配置

第四步，配置工作组 Technique。选择 “ 添加 ” 选项，如图 7-3 所示。在 “ 组名 ” 中填入 “ Technique ”，在 “ 起始 IP 地址 ” 中填入 “ 192.168.16.120 ”，在 “ 结束 IP 地址 ” 中填入 “ 192.168.16.150 ”，“ 禁止 QQ ” 和 “ 禁止 P2P ” 的勾选中，然后单击 “ 保存 ” 按钮，工作组 Technique 配置完成。

图 7-3 工作组 Technique 配置

第五步，配置工作组 Admin。选择 “ 添加 ” 选项，如图 7-4 所示。在 “ 组名 ” 中填入 “ Admin ”，在 “ 起始 IP 地址 ” 中填入 “ 192.168.16.160 ”，在 “ 结束 IP 地址 ” 中填入 “ 192.168.16.180 ”，然后单击 “ 保存 ” 按钮，工作组 Admin 配置完成。

图 7-4 工作组 Admin 配置

至此，三个工作组均配置完成，可以在“ 组信息列表 ”中查看这三个工作组的相关信息，如表 7-1、7-2 所示。

7.2 NAT 和 DMZ 配置

本节主要讲述***高级配置—>NAT 和 DMZ 配置***的配置方法。

7.2.1 NAT 功能介绍

7.2.1.1 NAT 简介

NAT（网络地址转换）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 日益短缺的问题，NAT 允许专用网络在内部使用任意范围的 IP 地址，而对于公用的 Internet 则表现为有限的公网 IP 地址范围。由于内部网络能有效地与外界隔离开，所以 NAT 也可以对网络的安全性提供一些保证。

设备提供了灵活的 NAT 功能，以下各节将详细介绍它的特点。

7.2.1.2 NAT 地址空间

为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间：一个是局域网主机在内部使用的私有 IP 地址，设备中用“ 内部 IP 地址 ”表示；另一个是用于外部的公网 IP 地址，设备中用“ 外部 IP 地址 ”表示。

7.2.1.3 三种 NAT 类型

设备提供三种 NAT 类型：“ EasyIP ”、“ One2One ”及“ Passthrough ”。

EasyIP：即网络地址端口转换，多个内部 IP 地址映射到同一个外部 IP 地址。它可为每个内部连接动态分配一个与单一外部地址有关的端口，并维护这些内部连接到外部端口的映射，从而实现多个用户同时使用一个公网地址与外部 Internet 进行通信。

One2One：即静态地址转换，内部 IP 地址与外部 IP 地址进行一对一的映射。此方式下，端口号不会改变。它通常用来配置外网访问内网的服务器：内网服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

Passthrough：对指定的 IP 地址不做 NAT，直接按路由方式转发，它经常用于一些会受 NAT 影响制约的特别应用。例如，为保证 IP 语音和视频会议等应用的正常运行，可在内网中专门划分一个语音视频区，该区的主机均采用“ Passthrough ”方式。

我们将每个具体的 NAT 配置称为“ NAT 规则 ”，配置 NAT 规则时必须指定其出口 IP 地址及线路。当有多个合法的公网地址时，每种类型的 NAT 规则均可配置多个。实际应用中，常常需要混合使用不同类型的 NAT 规则。

7.2.1.4 NAT 静态映射和虚拟服务器（DMZ 主机）

启用 NAT 功能后，设备会阻断从外部发起的访问请求。然而，某些应用环境下，广域网

中的计算机希望通过设备访问局域网内部服务器，这时，就需要在设备上设置 NAT 静态映射或虚拟服务器（DMZ 主机）来达到这个目的。

1. NAT 静态映射

通过 NAT 静态映射功能，可建立<**外部 IP 地址+外部端口**>与<**内部 IP 地址+内部端口**>一对一的映射关系，这样，所有对设备某指定端口的服务请求都会被转发到匹配的局域网服务器上，从而，广域网中的计算机就可以访问这台服务器提供的服务了。

2. 虚拟服务器（DMZ 主机）

某些情况下，需要将一台局域网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机）。当有外部用户访问该虚拟服务器所映射的公网地址时，设备会直接把数据包转发到该虚拟服务器上。

设备中，当有多个公网 IP 地址时，可配置 1 个全局虚拟服务器，多个局部虚拟服务器。其中，局部虚拟服务器是在配置 NAT 规则（类型为“ EasyIP ”）时设置的，当前 NAT 规则的外部 IP 地址就是该虚拟服务器所映射的公网地址。

提示：被设置为虚拟服务器的计算机将失去设备的防火墙保护功能。

3. 匹配优先级

NAT 静态映射的优先级高于虚拟服务器。当设备收到一个来自外部网络的请求时，它将首先根据外部访问请求的 IP 地址及端口号，检查是否有匹配的 NAT 静态映射，如果有的话，就把请求消息发送到该 NAT 静态映射匹配的局域网计算机上。如果没有匹配的静态映射，才会检查是否有匹配的虚拟服务器。

另外，局部虚拟服务器的优先级高于全局虚拟服务器，只有在没有匹配的局部虚拟服务器时，才使用全局虚拟服务器。

7.2.1.5 上网线路、NAT 规则与 NAT 静态映射的关系

设备中，上网线路、NAT 规则与 NAT 静态映射的关系如下：

- NAT 规则绑定在上网线路上，允许多个 NAT 规则绑定在同一条线路上；
- NAT 静态映射绑定在 NAT 规则（类型为“ EasyIP ”）上，NAT 规则的“ 外部 IP 地址 ”就是该 NAT 静态映射的“ 外部 IP 地址 ”，允许多个 NAT 静态映射绑定在同一个 NAT 规则上；
- 只有在配置了上网线路后，才能配置 NAT 规则；只有在配置了 NAT 规则后，才能配置 NAT 静态映射。

7.2.2 系统保留 NAT 规则

在***基本配置—>快速向导***中配置完默认线路，或者在***基本配置—>线路配置***中配置完默认线路和其他上网线路后，系统会自动生成各线路对应的 NAT 规则。为方便起见，在本手册中将它们称作“ 系统保留 NAT 规则 ”，可以在本页面的“ NAT 规则信息列表 ”中查看。

“ 系统保留 NAT 规则 ”的“ 类型 ”默认为“ EasyIP ”；“ 外部 IP 地址 ”默认为“ 0.0.0.0 ”，表示直接使用当前线路接口的 IP 地址；“ 绑定 ”默认为当前线路的“ 线路名称 ”；此外，线

路接入情况不同，对应的“ 系统保留 NAT 规则 ”的“ NAT 规则名 ”也不同，具体信息参见表 7-4。

提示：

1. “ 默认线路 ”固定接到 WAN1 口，“ 备份线路 ”固定接到 WAN2(DMZ)口；
2. 对于任何一条“ 系统保留 NAT 规则 ”来说，都禁止修改“ NAT 规则名 ”、“ 类型 ”、“ 外部 IP 地址 ”以及“ 绑定 ”等参数。

上网线路			NAT 规则名
线路名称	接入类型	接口	
默认线路	固定 IP	WAN1	ETHbind
	PPPoE 拨号	WAN1	PEBIND
	动态 IP	WAN1	DYNAeth2
备份线路	固定 IP	WAN2(DMZ)	IBIND
	PPPoE 拨号	WAN2(DMZ)	PBIND
	动态 IP	WAN2(DMZ)	DYNA2eth3
自定义的其他名称	固定 IP	LAN	FIXBIND_01
		WAN1	FIXBIND _02
		WAN2(DMZ)	FIXBIND _03
		WAN3	FIXBIND _04
		WAN4	FIXBIND _05
	动态 IP	LAN	DYNBIND _01
		WAN1	DYNBIND _02
		WAN2(DMZ)	DYNBIND _03
		WAN3	DYNBIND _04
		WAN4	DYNBIND _05
	PPPoE 拨号	此时，NAT 规则名与接口无关。按照配置顺序，各条 PPPoE 拨号线路对应的 NAT 规则的名称依次为 PPPBIND_01、PPPBIND_02 、 PPPBIND_03 、 … … 、 PPPBIND_10 、PPPBIND_11、……。	

表 7-4 系统保留 NAT 规则的名称

在***基本配置—>线路组合***的“ 线路检测及权重 ”中配置各上网线路的“ 权重 ”、“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”等参数，相当于在本页面配置“ 系统保留 NAT 规则 ”。相比之下，本页面提供更多的配置参数。

7.2.3 NAT 与多线路负载均衡功能

7.2.3.1 概述

在章节 5.2.2 中，我们已经介绍了设备的多线路负载均衡功能的特点。实际上，多线路负载均衡功能是依赖 NAT 功能实现的。

7.2.3.2 根据源 IP 地址指定优先通道

在这里，通道是指上网使用的 NAT 规则，它决定了上网使用的 NAT 类型、外部 IP 地址（即出口 IP）及线路。

设备允许用户预先为局域网中的某些主机指定优先通道，它是通过设置 NAT 规则的“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”来实现的，IP 地址属于两个地址范围内的主机将优先使用该 NAT 规则上网。对于已指定优先通道的主机来说，当指定 NAT 规则可用时，它们只能使用该 NAT 规则上网；但是，当指定 NAT 规则失效时，设备就把它们当作没有预先指定 NAT 规则的主机来处理。

7.2.3.3 根据线路带宽合理分配流量

设备中，用户能够预先指定分配到各条线路的流量的比例，它是通过设置线路的“ 权重 ”来实现的，“ 权重 ”大的线路将比“ 权重 ”小的线路承担更多流量。在实际应用中，一般可按线路的带宽比来设置各线路的“ 权重 ”，从而实现按线路带宽比合理分配流量。应用实例请参考章节 5.2.2.2。

注意，对于多地址线路来说，如果有多条“ EasyIP ”类型的 NAT 规则绑定在该线路上，那么，这些 NAT 规则的“ 权重 ”之和就是该线路的“ 权重 ”。

此外，当局域网中某些主机指定了优先通道时，若按照带宽比来设置“ 权重 ”，线路的实际流量比可能会同带宽比相差较大。这时，可以根据实际情况适当调整各线路的“ 权重 ”。

7.2.3.4 两种流量分配规则

“ 分配规则 ”用来控制线路流量，它作用于局域网中没有预先指定 NAT 规则的计算机，设备提供两种分配规则：“ NAT 会话 ”和“ IP 地址 ”，它们的实现机制如下所述。

1. IP 地址

使用 IP 地址作为分配规则时，设备将根据 NAT 规则的“ 权重 ”，把未指定 NAT 规则的主机的 IP 地址，按顺序依次分配到各条“ EasyIP ”NAT 规则上。分配到各“ EasyIP ”NAT 规则的 IP 地址的数量比（即主机数量比）为它们的“ 权重 ”比，来自同一 IP 地址的 NAT 会话使用同一个规则。

例如，若当前同时使用 3 条“ EasyIP ”NAT 规则上网，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，第 1、2、3 台上网的主机将使用第一条规则，第 4、5 台主机将使用第二条规则，第 6 台主机将使用第三条规则，接着第 7、8、9 台主机将使用第一条规则，……，依此类推。注意，这里假设每台主机均只有一个 IP 地址。

2. NAT 会话

使用 NAT 会话作为分配规则时，设备将根据 NAT 规则的“ 权重 ”，把未指定 NAT 规则的主机发起的 NAT 会话，按顺序依次分配到各“ EasyIP ” NAT 规则。分配到各“ EasyIP ” NAT 规则的 NAT 会话的数量比为它们的“ 权重 ”比，同一主机发起的 NAT 会话可使用多条 NAT 规则。

例如，若当前同时使用 3 条“ EasyIP ” NAT 规则上网，“ 权重 ” 分别为 3、2、1，则根据连接的先后顺序，内网主机发起的第 1、2、3 个 NAT 会话将使用第一条规则，第 4、5 个 NAT 会话将使用第二条规则，第 6 个 NAT 会话将使用第三条规则，接着第 7、8、9 个 NAT 会话将使用第一条规则，……，依此类推。

3. 设置依据

一般情况下，建议“ 分配规则 ”选择为“ IP 地址 ”。当对带宽要求高，需要多线路带宽合并时，比如使用网络蚂蚁（NetAnts）、网际快车（FlashGet）、影像传送带（Net Transport）等多线程下载工具时（多线程下载指把一个下载文件分成若干份同时下载，下载后再把它们合并起来），则可选择“ NAT 会话 ”，从而能够充分利用多线路带宽，以提高下载速度。需要注意的是，即便选择了“ NAT 会话 ”，由于网站情况不同仍有可能造成带宽不能完全叠加的情况，同时还可能造成某些应用连接不畅。

7.2.3.5 NAT 规则的匹配次序

当局域网中有主机发起 NAT 访问时，会首先检查这台主机是否符合所有 NAT 规则中“ 内部起始 IP 地址 ”到“ 内部结束 IP 地址 ”所指定的范围。如果有匹配的规则，则使用该条规则上网。如果没有匹配的规则，则使用“ NAT 类型 ”为“ EasyIP ”的 NAT 规则上网；有多个“ EasyIP ”类型的 NAT 规则时，则按照“ 分配规则 ”，根据“ 权重 ”值为各条 NAT 规则分配流量，从而控制线路流量。

7.2.4 NAT 全局配置

图 7-5 NAT 全局配置

- 启用 NAT：打开或者关闭 NAT 功能，选中为打开；
- 分配规则：控制线路流量时使用的规则。选项为“ NAT 会话 ”或“ IP 地址 ”，缺省值为“ IP 地址 ”；
- 最大 Session 数：局域网每台主机所能占用的最大 NAT 会话数；
- 虚拟服务器（DMZ）：欲用作虚拟服务器（DMZ 主机）的局域网计算机的 IP 地址，此处配置的是全局虚拟服务器。
- 保存：NAT 全局配置参数生效；

- 重填：恢复到修改前的配置参数。

提示：

1. 在配置完上网线路后，设备会自动打开 NAT 功能。除非特别需要，请不要关闭此功能，否则设备将失去共享上网功能；

2. 当某些局域网应用（比如网络游戏）发生连接速度变慢的情况时，可以适当提高“ 最大 Session 数 ”。注意，“ 最大 Session 数 ”设置过高可能会导致设备减弱甚至丧失防止 DDoS 攻击的功能。

7.2.5 NAT 规则

7.2.5.1 NAT 规则配置

下面分别介绍“ EasyIP ”、“ One2One ”及“ Passthrough ”这三种类型的 NAT 规则的配置，如图 7-6、7-7、7-8 所示。

1. EasyIP

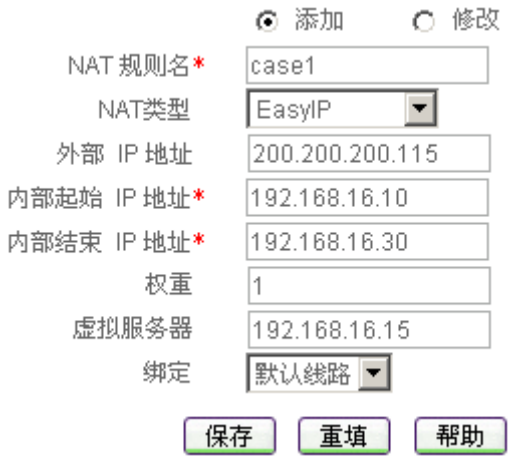


图 7-6 NAT 规则配置——EasyIP

- NAT 规则名：NAT 规则的名称（自定义，不能重复）。取值范围：1～11 个字符；
- NAT 类型：EasyIP、One2One、Passthrough，这里选择“ EasyIP ”；
- 外部 IP 地址：该 NAT 规则中，内部 IP 地址所映射的外部 IP 地址。对于系统保留 NAT 规则来说，它显示为 0.0.0.0，表示默认使用当前接口地址，不能修改；配置其余本类型规则时，只能使用 ISP 分配的除当前接口地址之外的 IP 地址作为映射地址，不能为 0.0.0.0；
- 内部起始 IP 地址、内部结束 IP 地址：局域网中优先使用该 NAT 规则上网的计算机的起始 IP 地址和结束 IP 地址；
- 权重：该 NAT 规则的权重，取值范围为 1-255（整数），缺省值为 1；
- 虚拟服务器：欲用作虚拟服务器的局域网计算机的 IP 地址，此处设置的是局部虚拟服务器，它只能使用该 NAT 规则；
- 绑定：该 NAT 规则绑定的线路；
- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：配置本类型的 NAT 规则时，“ NAT 规则名 ”不能定义为如表 7-4 所示的系统保留 NAT 规则的名称。

2. One2One

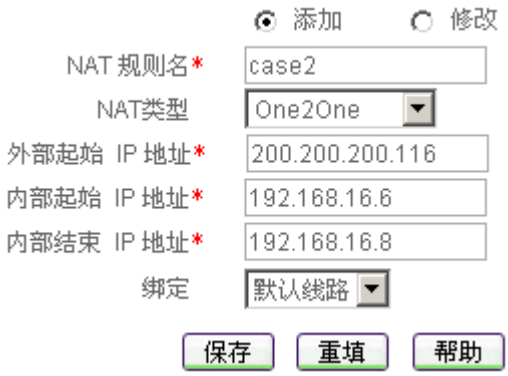


图 7-7 NAT 规则配置——One2One

“ NAT 规则名 ”、“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”、“ 绑定 ”这几个参数的涵义同“ EasyIP ”方式中相关参数，这里不再重述，请参考相关描述。

- 外部起始 IP 地址：该 NAT 规则中，内部起始 IP 地址所映射的外部起始 IP 地址；
- NAT 类型：EasyIP、One2One、Passthrough，这里选择“ One2One ”。
- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：“ 外部起始 IP 地址 ”必须设置，实际映射的外部 IP 地址从设置值开始依次增加。例如，如果“ 内部起始 IP 地址 ”设为 192.168.16.6，“ 内部结束 IP 地址 ”设为 192.168.16.8，“ 外部起始地址 ”设为 200.200.200.116，则 192.168.16.6、192.168.16.7、192.168.16.8 依次映射成 200.200.200.116、200.200.200.117、200.200.200.118。

3. Passthrough

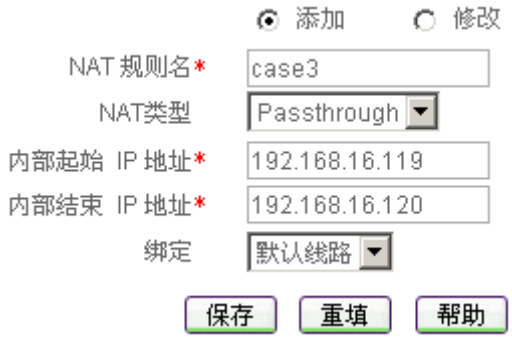


图 7-8 NAT 规则配置——Passthrough

“ NAT 规则名 ”、“ 绑定 ”这两个参数的涵义同“ EasyIP ”方式中相关参数，这里不再重述，请参考相关描述。

- NAT 类型：EasyIP、One2One、Passthrough，这里选择“ Passthrough ”；
- 内部起始 IP 地址、内部结束 IP 地址：局域网中使用该 NAT 规则上网的计算机的起始和结束 IP 地址，这两个地址范围之内的 IP 地址不能与其他规则的外部 IP 地址重叠。

- 保存：NAT 规则的配置参数生效；
- 重填：恢复到修改前的配置参数。

7.2.5.2 NAT 规则列表

表 7-5 NAT 规则信息列表

- 增加 NAT 规则：选中“ 添加 ”选项，输入 NAT 规则配置信息，单击“ 保存 ”按钮，生成新的 NAT 规则；
- 浏览 NAT 规则：如果已经生成了 NAT 规则，则可在“ NAT 规则信息列表 ”中浏览 NAT 规则信息，如表 7-5 所示；
- 编辑 NAT 规则：如果想编辑某条 NAT 规则，只需单击该 NAT 规则的“ NAT 规则名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 NAT 规则：选中一些 NAT 规则，单击右下角的“ 删除 ”按钮，即可删除被选中的 NAT 规则。

7.2.5.3 自定义 NAT 规则

第一步，确定所要配置的 NAT 规则的类型；

第二步，进入***高级配置—>NAT 和 DMZ 配置***页面；

第三步，在“ NAT 规则配置 ”栏，选择“ 添加 ”选项；

第四步，选择“ NAT 类型 ”为“ EasyIP ”、“ One2One ”或“ Passthrough ”。

第五步，分为三种情况：

如果“ NAT 类型 ”选择为“ EasyIP ”，根据需要设置“ 外部 IP 地址 ”、“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”、“ 权重 ”和“ 虚拟服务器 ”；

如果“ NAT 类型 ”选择为“ One2One ”，根据需要设置“ 外部 IP 地址 ”、“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”；

如果“ NAT 类型 ”选择为“ Passthrough ”，根据需要设置“ 内部起始 IP 地址 ”及“ 内部结束 IP 地址 ”；

第六步，选择“ 绑定 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。可以在“ NAT 规则信息列表 ”中看到相应的记录；

第八步，继续配置其他 NAT 规则。

提示：

1. 删除 NAT 规则，在“ NAT 规则信息列表 ”中选中要删除的 NAT 规则，单击“ 删除 ”

按钮，即可删除；注意，不能删除系统保留 NAT 规则；

2. 系统保留 NAT 规则的“ 外部 IP 地址 ”将显示为 0.0.0.0，表示默认使用当前线路接口的地址，不能修改；其余自定义的 NAT 规则的“ 外部 IP 地址 ”不能为当前线路的接口 IP 地址，也不能为 0.0.0.0；所有 NAT 规则的“ 内部 IP 地址 ”不能相互重叠，“ 外部 IP 地址 ”也不能重叠；并且，“ Passthrough ”类型的 NAT 规则的“ 内部 IP 地址 ”不能与另外两种类型的规则的“ 外部 IP 地址 ”重叠；

3. 在实际应用中，如果需要配置多条 NAT 规则，则在统一规划之后，应该首先配置或修改系统保留 NAT 规则，再配置其余自定义的 NAT 规则。如果已在***基本配置—>线路组合***的“ 线路检测及权重配置 ”中配置了系统保留 NAT 规则的相关参数，可直接在本页面修改它们；如果没有配置系统保留 NAT 规则的相关参数，可以在***基本配置—>线路组合***的“ 线路检测及权重配置 ”中进行快速配置，也可以直接在本页面进行配置。

例如，假设某用户已在***基本配置—>快速向导***中配置了上网默认线路，ISP 分配了 2 个可用地址给默认线路。现在希望整个局域网用户分为两部分，一部分使用当前 WAN1 口地址作为外部地址，即使用默认线路对应的系统保留 NAT 规则上网；另一部分使用 ISP 分配的另外一个地址作为外部地址。则必须首先将局域网用户根据 IP 地址划分为两组，同组内用户将使用同一条 NAT 规则上网；然后再在本页面配置系统保留 NAT 规则的相关参数：“ 内部起始 IP 地址 ”、“ 内部结束 IP 地址 ”、“ 权重 ”等，最后才能在本页面配置另一条 NAT 规则的相关参数。

7.2.5.4 NAT 规则配置的注意事项

设备中，要保证 NAT 正常工作，还需注意以下事项，并进行相关配置。

1. 一般需启用快速转发功能

如果在 NAT 规则中配置了“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”这两个参数，要保证 NAT 正常工作，必须启用快速转发功能。

配置方法为：进入***高级配置—>特殊功能***页面，启用快速转发功能。

2. 某个广域网接口为多地址接入时，必须启用 NAT 类型的 ARP 代理功能

配置方法为：进入***基本配置—>接口配置***页面，首先在“ 选择接口 ”中选择使用多地址接入线路的广域网接口的名称，然后在“ ARP 代理 ”选中“ Nat ”。

3. 某个广域网接口为多地址接入时，局域网主机要访问 ISP 分配的当前广域网接口 IP 地址之外的公网 IP 地址时，需配置相关的静态路由。

主要应用：

局域网其他主机需要通过公网地址访问“ One2One ”类型的 NAT 规则所指定的内部主机时，需进入***高级配置—>路由配置***页面设置相关的静态路由。

一般情况下，相关的静态路由为主机路由，其目的地址为需要访问的公网地址，掩码为 255.255.255.255，网关为对应的广域网接口当前使用的 IP 地址。因此，如果需要访问多个 IP 地址，则需要设置多条主机路由。

当然，如果需要访问的公网地址可以划分在同一个子网（该子网地址数更少，不能包括当前广域网接口 IP 地址）中，也可以通过为它们设置一条子网路由来实现：其目

的地址为新的子网的网络号，掩码为新的子网掩码，网关仍为对应的广域网接口当前使用的 IP 地址。

为避免无谓的错误，一般采用设置主机路由的方式即可。

7.2.5.5 NAT 规则配置实例

1. EasyIP 方式应用实例

某网吧使用单线路上网，ISP 为该线路分配了 8 个地址：218.1.21.0/29 ~218.1.21.7/29，其中 218.1.21.1/29 是该线路的网关地址，218.1.21.2/29 是设备的 WAN1 口 IP 地址。注意，218.1.21.0/29、218.1.21.7/29 分别为相关子网的子网号和广播地址，不可使用。

现游戏 B 区（IP 地址范围：192.168.16.10/24~192.168.16.100/24）希望以 218.1.21.3/29 作为 NAT 映射地址通过 WAN1 口上网，其对外虚拟服务器为 192.168.16.15，权重为 2。

配置步骤如下：

第一步，进入***高级配置—>NAT 和 DMZ 配置***页面；

第二步，在“ NAT 规则配置 ”栏，单击“ 添加 ”按钮，如图 7-9 所示；

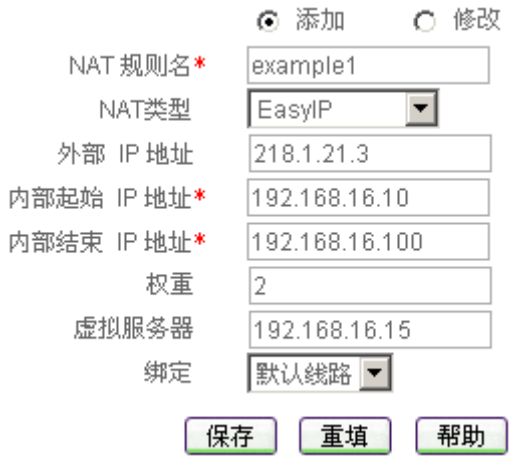


图 7-9 NAT 规则配置——实例一

第三步，在“ NAT 规则名 ”中填入 example1；

第四步，选择“ NAT 类型 ”为“ EasyIP ”；

第五步，在“ 外部 IP 地址 ”中填入 218.1.21.3；在“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.10 和 192.168.16.100；

第六步，在“ 权重 ”中填入 2，在“ 虚拟服务器 ”中填入 192.168.16.15；

第七步，选择“ 绑定 ”为“ 默认线路 ”；

第八步，单击“ 保存 ”按钮，该条 NAT 规则配置成功。

2. One2One 方式应用实例

1) 需求

如图 7-10 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽为 6M。电信给它分配了 8 个地址：202.1.1.128/29～202.1.1.1.135/29，其中，202.1.1.129/29 是该线路的网关地址，202.1.1.130/29 是设备的 WAN1 口 IP 地址。注意，202.1.1.128/29、202.1.1.1.135/29 分别为相关子网的子网号和广播地址，不可使用。

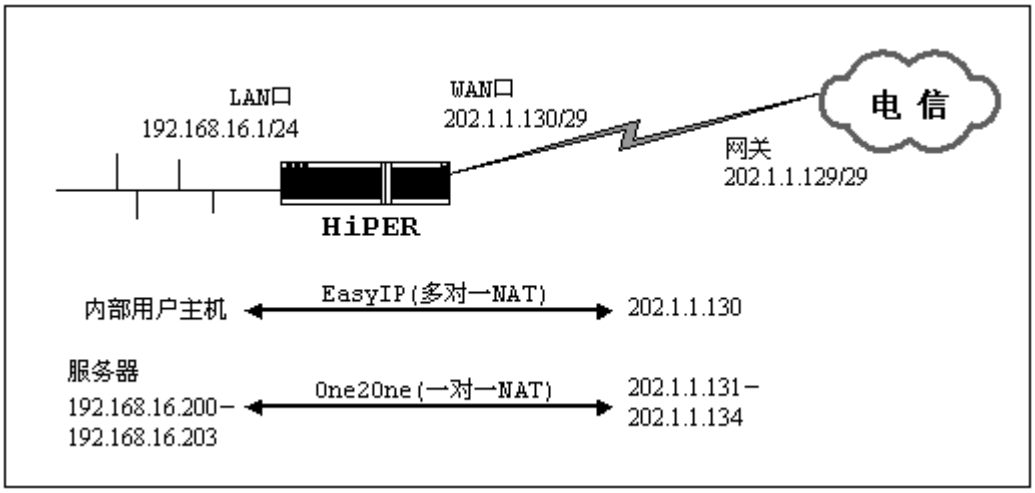


图 7-10 NAT 规则配置实例方案图——One2One 方式

该企业希望内部的人员上网通过 NAT 后使用 202.1.1.130/29 共享上网，另外有四台服务器做一对一 NAT（One2One）使用 202.1.1.131/29～202.1.1.1.134/29 对外提供服务。内部网络的地址是 192.168.16.0/24，4 台服务器的内部地址是 192.168.16.200/24～192.168.16.203/24。

2) 分析

由于该线路是采用固定 IP 接入方式上网，首先需要在***基本配置***—>***快速向导***页面中配置固定 IP 接入上网默认线路，或直接进入***开始***—>***上网线路配置***和***基本配置***—>***线路配置***页面中配置该线路。上网默认线路正确配置后，将自动生成与默认线路对应的系统保留 NAT 规则，NAT 功能也自动启用。

而该企业使用提供四台内部服务器供外部访问，因此还需为它们设置一个类型为“ One2One ”的 NAT 规则。

最后，为保证 NAT 工作正常，还需进入***高级配置***—>***特殊功能***页面，启用快速转发功能；而由于 WAN1 口是多地址接入，因此还需进入***基本配置***—>***接口配置***页面，在 WAN1 口启用 NAT 类型的 ARP 代理功能；另外，如果局域网用户需要通过外部地址（202.1.1.131～202.1.1.134）访问内部服务器，还需设置相关的静态路由。

3) One2One 类型的 NAT 规则配置

配置步骤如下：

第一步，进入***高级配置***—>***NAT 和 DMZ 配置***页面；

第二步，在“ NAT 规则配置 ”栏，单击“ 添加 ”按钮，如图 7-11 所示；

图 7-11 NAT 规则配置——实例二

第三步，在“ NAT 规则名 ”中填入 example2；

第四步，选择“ NAT 类型 ”为“ One2One ”；

第五步，在“ 外部 IP 地址 ”中填入 202.1.1.131；在“ 内部起始 IP 地址 ”和“ 内部结束 IP 地址 ”中分别填入 192.168.16.200 和 192.168.16.203；

第六步，选择“ 绑定 ”为“ 默认线路 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。

3. Passthrough 方式应用实例

1) 需求

如图 7-12 所示，某企业申请了一条电信的线路，固定 IP 接入方式，带宽是 6M。电信提供给企业使用的连接地址为 202.96.97.2/30，电信使用的连接地址（即网关地址）为 202.96.97.1/30。该企业的内部用户主机将使用 202.96.97.2/30 共享上网，内部网络的地址是 192.168.16.0/24。

此外，电信还分配了一段地址给该企业使用，地址范围为 202.96.100.0/27~202.96.100.31/27，该企业将利用这些地址采用 Passthrough 方式配置多台服务器，对外提供服务；注意，202.96.100.0/27 和 202.96.100.31/27 分别为相关子网的子网号和广播地址，不可使用。

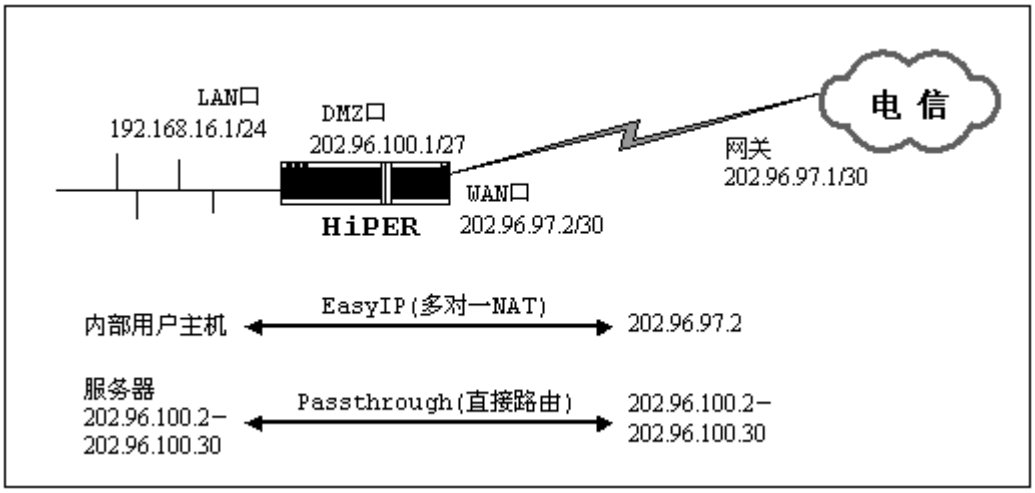


图 7-12 NAT 规则配置实例方案图——Passthrough 方式

2) 分析

由于该线路是采用固定 IP 接入方式上网，首先需要在***基本配置***—>***快速向导***中配置固定 IP 接入上网默认线路，或直接进入***基本配置***—>***线路配置***页面中配置该线路。上网默认线路正确配置后，将自动生成默认线路对应的系统保留 NAT 规则，NAT 功能也自动启用。

另外，由于要求对外服务器采用 Passthrough 方式直接路由出网，因此，需将服务器通过交换机连接到设备的 WAN2/DMZ 口，将 DMZ 口的地址设为 202.96.100.1/27，并将服务器的地址设为 202.96.100.2/27~202.96.100.30/27 中的任一个，并且这些对外服务器的网关都是 202.96.100.1/27。之后，再为它们设置一个类型为“ Passthrough ”的 NAT 规则，地址范围为：202.96.100.2/27~202.96.100.30/27

最后，为保证 NAT 工作正常，还需进入***高级配置***—>***特殊功能***页面，启用快速转发功能

3) Passthrough 类型的 NAT 规则配置

配置步骤如下：

第一步，进入***高级配置—>NAT 和 DMZ 配置***页面；

第二步，在“ NAT 规则配置 ”栏，单击“ 添加 ”按钮，如图 7-13 所示；

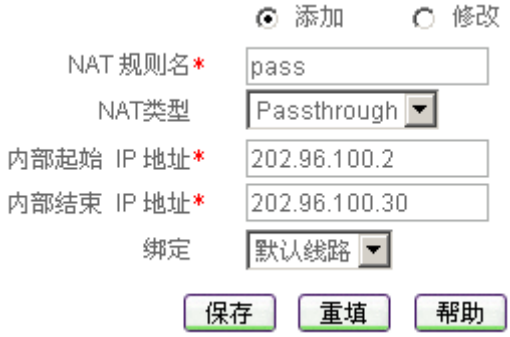


图 7-13NAT 规则配置——实例三

第三步，在“ NAT 规则名 ”中填入 pass；

第四步，选择“ NAT 类型 ”为“ Passthrough ”；

第五步，在“ 内部起始 IP 地址 ”填入 202.96.100.2，和“ 内部结束 IP 地址 ”中填入 202.96.100.30；

第六步，选择“ 绑定 ”为“ 默认线路 ”；

第七步，单击“ 保存 ”按钮，该条 NAT 规则添加成功。

7.2.6 NAT 静态映射

7.2.6.1 NAT 静态映射配置

图 7-14 NAT 静态映射配置

- NAT 静态映射名：NAT 静态映射的名称（自定义，不能重复）。取值范围：1～11 个字符；
- 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 GRE；
- 外部起始端口：设备提供给 Internet 的服务端口；
- 内部 IP 地址：局域网中作为服务器的计算机的 IP 地址；
- 内部起始端口：局域网服务器所开服务的起始端口；

- 端口数量：从内部起始端口开始的一段连续的端口，最大设置为 20。例如：内部端口为 21，外部端口为 21，端口数量为 20，就代表内部端口范围为：21~40，同时外部端口与之一一对应，范围相应为：21~40；
- NAT 绑定：NAT 静态映射所绑定的 NAT 规则，其“ 外部 IP 地址 ”就是该 NAT 静态映射的“ 外部 IP 地址 ”。选项包括：
  - 当前所有类型为“ EasyIP ”的 NAT 规则的“ NAT 规则名 ”，分别代表相应的 NAT 规则；
  - 当前所有上网线路的“ 线路名称 ”，分别代表各条线路对应的系统保留 NAT 规则。
- 保存：NAT 静态映射配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 除“ TCP ”和“ UDP ”之外，对于其他类型的协议来说，“ 外部起始端口 ”、“ 内部起始端口 ”这两个参数必须设置为“ 0 ”，“ 端口数量 ”必须设置为“ 1 ”；
2. 系统某些功能（***系统管理—>远程管理***）会添加一些默认 NAT 映射，在本页面无法编辑或删除它们。

7.2.6.2 NAT 静态映射列表

表 7-6 NAT 静态映射列表

- 增加 NAT 静态映射：选中“ 添加 ”选项，输入 NAT 静态映射信息，单击“ 保存 ”按钮，生成新的 NAT 静态映射；
- 浏览 NAT 静态映射：如果已经生成了 NAT 静态映射，则可在“ NAT 静态映射列表 ”中浏览 NAT 静态映射信息，如表 7-19 所示；
- 编辑 NAT 静态映射：如果想编辑某条 NAT 静态映射，只需单击该 NAT 静态映射的“ NAT 静态映射名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除 NAT 静态映射：选中一些 NAT 静态映射，单击右下角的“ 删除 ”按钮，即可删除被选中的 NAT 静态映射。

7.2.6.3 自定义 NAT 静态映射

第一步，进入***高级配置—>NAT 和 DMZ 配置***页面；

第二步，在“ NAT 静态映射 ”配置栏，选择“ 添加 ”选项，填写“ NAT 静态映射名 ”；

第三步，根据需要填写局域网服务器的“ 内部 IP 地址 ”，所开服务的“ 协议 ”和“ 内部

起始端口 ”；

第四步，根据需要填写对外服务的 “ 外部起始端口 ”，“ 外部起始端口 ” 可以和 “ 内部起始端口 ” 不一致；

第五步，如果局域网服务器开设的服务是一段连续的端口，需要设置 “ 端口数量 ”；

第六步，根据需要选择 “ NAT 绑定 ”，绑定的 NAT 规则决定了映射的外部 IP 地址；

第七步，单击 “ 保存 ” 按钮，该 NAT 静态映射添加成功。可以在 “ NAT 静态映射列表 ” 中看到相应的记录；

第八步，继续配置其他的 NAT 静态映射。

提示：删除 NAT 静态映射，在 “ NAT 静态映射列表 ” 中选中要删除的 NAT 静态映射，单击 “ 删除 ” 按钮，即可删除被选中的 NAT 静态映射。

7.2.6.4 NAT 静态映射配置实例

1. 实例一

局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，但是希望外部通过 210 端口访问这个服务，具体配置如图 7-15 所示：

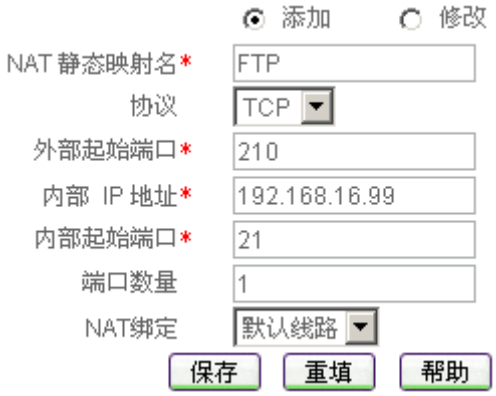


图 7-15 NAT 静态映射配置——实例一

2. 实例二

局域网计算机 192.168.16.100 开设了 UDP30000~UDP30019 端口的服务，希望可以映射到外部的 UDP30000~UDP30019 端口，则可将 “ 端口数量 ” 设为 20，具体配置如图 7-16 所示：

图 7-16 NAT 静态映射配置——实例二

3. 实例三

例如，ISP 分配了 218.1.21.0/29~218.1.21.7/29 八个地址，其中 218.1.21.1/29 是设备的网关地址，218.1.21.2/29 是设备的 WAN1 口 IP 地址，局域网计算机 192.168.16.99 开设了 TCP21 端口的服务，希望外部通过 218.1.21.3 的 TCP21 端口来访问这个服务。

首先需配置一条 NAT 规则，使其外部地址为 218.1.21.3，将其“规则名”设为“example1”（具体配置参见***高级配置—>NAT 和 DMZ 配置***的“NAT 规则配置实例”）。然后再配置该 NAT 静态映射，“NAT 绑定”选择“example1”，具体配置如图 7-17 所示：

图 7-17 NAT 静态映射配置——实例三

7.3 路由配置

本节主要讲述***高级配置—>路由配置***的配置方法。

在本页面不仅可以配置静态路由，还可以配置静态路由策略库。通过后者可以一次配置大量静态路由，轻松实现电信走电信、网通走网通。以下将分别介绍它们的配置及使用方法。

7.3.1 静态路由

7.3.1.1 静态路由概述

在本页面可配置静态路由，静态路由就是由网络管理员手工配置的路由，使得到指定目的网络的数据包的传送，按照预定的路径进行。静态路由不会随未来网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改路由表中相关的静态路由信息。

正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，比如实现流量控制、为重要的应用保证带宽等。

7.3.1.2 系统保留路由

在设备中，有两类保留的静态路由：缺省路由和检测路由，以下两节将分别介绍它们。用户自定义其他静态路由时，不允许使用保留路由名。

1. 缺省路由

缺省路由是一种特殊的静态路由，简单地说，就是在没有找到匹配的路由时使用的路由。在路由表中，缺省路由以目的网络为 0.0.0.0、子网掩码为 0.0.0.0 的形式出现。如果数据包的目的地址不能与任何路由相匹配，那么系统将使用缺省路由转发该数据包。

在***基本配置—>快速向导***中配置完默认线路，或者在***基本配置—>线路配置***中配置完默认线路和其他上网线路后，系统会自动生成各线路对应的缺省路由，可在***系统状态—>路由和端口信息***的“ 路由表信息列表 ”查看到对应路由的状态信息，即目标地址为“ 0.0.0.0/0 ”的静态路由。

如果上网线路为固定 IP 或动态 IP 接入线路，还可在本页面的“ 路由信息列表 ”中查看到对应路由的配置信息。不同情况下，各条上网线路对应的缺省路由的名称不同，具体信息参见表 7-7。

提示：“ 默认线路 ”固定接到设备的 WAN1 口，“ 备份线路 ”固定接到设备的 WAN2(DMZ)口。

上网线路			缺省路由名
线路名称	接入类型	接口	
默认线路	固定 IP	WAN1	Default
	动态 IP	WAN1	Default
备份线路	固定 IP	WAN2(DMZ)	IPETH
	动态 IP	WAN2(DMZ)	DefaultDMZ
自定义的其他名称	固定 IP	LAN	FIXRT_01
		WAN1	FIXRT_02
		WAN2(DMZ)	FIXRT_03
		WAN3	FIXRT_04
		WAN4	FIXRT_05
	动态 IP	LAN	DYNRT_01
		WAN1	DYNRT_02
		WAN2(DMZ)	DYNRT_03
		WAN3	DYNRT_04
		WAN4	DYNRT_05

表 7-7 系统保留的缺省路由名

2. 检测路由

在***基本配置—>线路组合***中，当默认线路或其他某条上网线路启用线路检测后，系统还会自动生成相应的检测路由，从而保证检测包是通过当前待检测的线路转发的。可在本页面的“ 路由信息列表 ”中查看到对应路由的配置信息。不同情况下，各条上网线路对应的检测路由的名称不同，具体信息参见表 7-8。

提示：对于固定 IP 或动态 IP 接入线路来说，当“ 检测目标 ”为“ 网关 ”时，系统将直接使用该线路对应的缺省路由来检测线路，即该缺省路由同时也作为检测路由来使用。

上网线路			检测路由名
线路名称	接入类型	接口	
默认线路	任意	WAN1	Detect
备份线路	任意	WAN2(DMZ)	DetectDMZ
自定义的其他名称	固定 IP	LAN	DETEFIX _01
		WAN1	DETEFIX _02
		WAN2(DMZ)	DETEFIX _03

		WAN3	DETEFIX _04
		WAN4	DETEFIX _05
	动态 IP	LAN	DETEDYN _01
		WAN1	DETEDYN _02
		WAN2(DMZ)	DETEDYN _03
		WAN3	DETEDYN _04
		WAN4	DETEDYN _05
	PPPoE 拨号接入	此时，检测路由名与接口无关。按照配置顺序，各条 PPPoE 拨号线路对应的检测路由的名称依次为 DETEPPP _01、DETEPPP _02、DETEPPP _03、……、DETEPPP _10、DETEPPP _11、……。	

表 7-8 系统保留的检测路由名

7.3.1.3 静态路由配置

图 7-18 静态路由配置

- 路由名：静态路由的名称（自定义，不可重复）。取值范围：1~11 个字符；
- 预定义：配置单条静态路由时，必须使用缺省值“ 无 ”。只有在配置静态路由策略库时才需修改；
- 目的网络：此静态路由的目的网络号；
- 子网掩码：此静态路由的目的网络的掩码；
- 网关地址：下一跳路由器入口的 IP 地址，设备通过接口和网关定义一条跳到下一个路由器的线路。通常情况下，接口和网关须在同一网段；
- 绑定：指定数据包的转发接口，与该静态路由匹配的数据包将从指定接口转发。固

定 IP 或动态 IP 线路对应的接口为物理接口；PPPoE 等拨号线路对应的接口为拨号接口。选项包括：

- 各条线路的“ 线路名称 ”；
- 各个物理接口的名称；
- 其他内部接口。

其中，各个内部接口含义如下：

- Blackhole-内部接口，转发到该接口的所有包都被设备丢弃；
- Local-内部软路由接口，转发到设备本身；
- Reject-内部接口，转发到该接口的所有包都被设备拒绝，并回应一个 ICMP 不可达；
- Loopback-回环地址，代表 127.0.0.0/8 网段，不被转发。

◆ 检测间隔：同***基本配置—>线路组合***中的“ 检测间隔 ”，线路检测时发送检测包的时间间隔；

◆ 优先级：该路由的优先级，目的网段相同的情况下，设备将优先选择优先级高的路由转发数据包，值越低优先级越高；

◆ 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1。跳数也表示该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由，设备会采用跳数值小的那条路由。

▶ 保存：静态路由配置参数生效；

▶ 重填：恢复到修改前的配置参数。

提示：

1. 配置静态路由时，必须明确下一跳地址，可通过“ 网关地址 ”或“ 绑定 ”设置。若转发接口是物理接口，则必须设置“ 网关地址 ”，但可以不设置“ 绑定 ”，此时，设备将会自动选择一条最优路径；若转发接口是拨号接口，则必须将“ 绑定 ”设置为对应的“ 线路名称 ”，但无需设置“ 网关地址 ”，此时，下一跳网关是 PPPoE 拨号所得的 IP 地址。

2. 一般情况下，请不要修改“ Default ”、“ DefaultDMZ ”、“ IPETH ”、“ Detect ”及“ DetectDMZ ”等系统保留路由，以免上网异常。

7.3.1.4 路由信息列表

表 7-9 路由信息列表

- 增加静态路由：选中“ 添加 ”选项，输入静态路由信息，单击“ 保存 ”按钮，生成新的静态路由；
- 浏览静态路由：如果已经生成了静态路由，可以查看“ 路由信息列表 ”，浏览静态路由信息；
- 编辑静态路由：如果想编辑某条静态路由，只需单击此静态路由的“ 路由名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除静态路由：选中一些静态路由，单击右下角的“ 删除 ”按钮，即可删除被选中的静态路由；
- 查看路由表：单击“ 查看路由表 ”超链接，立即转到***系统状态—>路由和端口信息***页面，在该页面的“ 路由表信息列表 ”中可查看系统中当前生效的全部路由的最新状态信息。

7.3.1.5 自定义静态路由

第一步，进入***高级配置—>路由配置***页面；

第二步，选择“ 添加 ”选项，填入静态路由的名称；

第三步，输入该条路由指向的目的网段及子网掩码；

第四步，根据实际情况，设置网关地址或者绑定的接口（注意：若转发接口是物理接口，则必须设置“ 网关地址 ”，但可以不设置“ 绑定 ”，此时设备将会自动选择一条最优路径；若转发接口是拨号接口，则必须将“ 绑定 ”设置为对应的“ 线路名称 ”，但无需设置“ 网关地址 ”）；

例如，某条路由的目的网段为 192.168.1.0/24，转发接口为物理接口，“ 网关地址 ”为 192.168.16.254，则可以不设置“ 绑定 ”，设备会自动选择路径，具体配置如下图所示。

图 7-19 静态路由配置——实例一

例如，某条静态路由的目的网段为 218.19.213.45/32，转发接口为 PPPoE 拨号接口，则必须将“ 绑定 ”设置为对应线路的“ 线路名称 ”（此处假设为“ 测试线路 1 ”），而无需设置“ 网关地址 ”，此时，其下一跳网关是 PPPoE 拨号所得的 IP 地址。具体配置如下图所示。

图 7-20 静态路由配置——实例二

第五步，如果需要监测线路状态，则需要设定检测间隔；

第六步，根据需要设置该条路由的优先级和路由跳数；

第七步，单击“ 保存 ”按钮，该静态路由添加成功。可以在“ 路由信息列表 ”中看到相应的记录；

第八步，继续配置其他静态路由。

提示：若要删除路由，只需在“ 路由信息列表 ”中选中要删除的路由，单击“ 删除 ”按钮即可。

7.3.2 静态路由策略库

7.3.2.1 静态路由策略库概述

使用多线路上网的用户（网吧或企业），往往会申请不同运营商的线路，例如一条电信线路，一条网通线路。某些情况下，运营商之间相互访问对方的服务器速度很慢，运营商可能还会禁止别的运营商访问自己的服务器。这时，就可以通过配置静态路由策略库的方法，方便地实现到电信服务器的流量走电信线路、到网通服务器的流量走网通线路，以保证局域网主机能够正常使用网络服务器。

目前，系统提供了两个预定义路由策略库，名称分别为：TEL 和 CNC。其中，TEL 是电信静态路由策略库，CNC 是网通静态路由策略库。TEL 策略库中，封装了若干电信网段信息（IP 地址以及子网掩码）；类似地，CNC 策略库中，封装了若干网通网段信息（IP 地址以及子网掩码）。通过引入路由策略库，使得用户无需一条条地添加静态路由，只需操作一次，就能批量配置大量电信路由或者网通路由，从而保证电信流量走电信线路、网通流量走网通线路。

根据用户实际需求，艾泰科技将会陆续提供更多的路由策略库。用户可以进入***安全配置—>策略库***页面，在“ 策略库信息列表 ”中查看路由策略库的版本、引用状态等信息。

此外，考虑到各个运营商提供的服务器的 IP 地址经常会有变化，艾泰科技公司技术人员会在第一时间收集相关信息，并根据实际情况定期提供最新版本的策略库。同时，为了方

便用户使用，设备还提供了策略库在线更新功能：用户只需要进入***安全配置***—>***策略库***页面，在“ 策略库信息列表 ”中单击对应策略库的“ 更新 ”超链接，系统就会连接到指定站点下载并自动更新该策略库。

7.3.2.2 静态路由策略库配置

图 7-21 静态路由策略库配置

如图 7-21 所示，由于路由策略库中封装若干目的网络的 IP 地址以及子网掩码，因此，配置路由策略库时，无需设置“ 目的网络 ”和“ 子网掩码 ”这两个参数了。

通过本页面配置路由策略库之后，系统将会自动生成若干静态路由，这些静态路由的各个参数的值如下：

- “ 目的网络 ”和“ 子网掩码 ”由策略库预定义；
- “ 网关地址 ”、“ 绑定 ”、“ 检测间隔 ”、“ 优先级 ”、“ 跳数 ”的值都相同：即分别为配置该策略库时所设置的值。注意，配置策略库时，“ 检测间隔 ”只能设置为 0，因此，这些静态路由的“ 检测间隔 ”都为 0；
- “ 路由名 ”的值分别为 **xxx001**、**xxx002**、**xxx003**、…，依次递增，其中，**xxx** 为配置该策略库时自定义的“ 路由名 ”。例如若配置静态路由策略库时输入的“ 路由名 ”为**网通路由**，则这些静态路由的“ 路由名 ”的值分别为**网通路由 001**、**网通路由 002**、**网通路由 003**、…，依次递增。

◆ 预定义：系统提供了两个预定义路由策略库，其中，“ TEL ”为电信静态路由策略库，“ CNC ”为网通路由策略库。注意，“ TEL ”必须绑定到电信线路上，“ CNC ”必须绑定到网通线路上；

◆ 检测间隔：配置路由策略库时，“ 检测间隔 ”只能设置为 0。

提示：当某个静态路由策略库所绑定的线路激活后，通过该策略库生成的所有静态路由立即生效，此时，可以进入***系统状态***—>***路由和端口信息***页面，在“ 路由信息列表 ”中查看到这些静态路由的配置及状态信息。

7.3.2.3 如何设置静态路由策略库

第一步，进入***高级配置—>路由配置***页面；

第二步，选择“ 添加 ”选项，设置路由名；

第三步，在预定义中选中某个路由策略库；

第四步，根据实际情况，设置网关地址或者绑定的接口（注意：若转发接口是物理接口，则必须设置“ 网关地址 ”，但可以不设置“ 绑定 ”，此时设备将会自动选择一条最优路径；若转发接口是拨号接口，则必须将“ 绑定 ”设置为对应的“ 线路名称 ”，但无需设置“ 网关地址 ”）；

例如，若配置的是电信策略库，而电信线路为固定 IP 接入线路（转发接口为物理接口），该线路的网关地址为 200.200.200.254，则必须设置“ 网关地址 ”，但可以不设置“ 绑定 ”，设备会自动选择路径，具体配置如下图所示。

图 7-22 静态路由策略库配置——实例一

例如，若配置的是网通策略库，而网通线路为 PPPoE 拨号线路（转发接口为拨号接口），则必须将“ 绑定 ”设置为该线路的“ 线路名称 ”（此处为“ 网通线路 ”），而无需设置“ 网关地址 ”，此时，其下一跳网关是 PPPoE 拨号所得的 IP 地址。具体配置如下图所示。

图 7-23 静态路由策略库配置——实例二

第七步，根据需要设置该条路由的优先级和路由跳数（一般使用缺省值即可）；

第八步，单击“ 保存 ”按钮，该静态路由策略库添加成功。可以在“ 路由信息列表 ”中看到相应的记录。

提示：若要删除路由策略库，只需在“ 路由信息列表 ”中选中该策略库，单击“ 删除 ”按钮即可。

7.3.2.4 如何更新静态路由策略库

如前所述，用户只需要进入***安全配置***—>***策略库***页面，在“策略库信息列表”中单击对应策略库的“更新”超链接，系统就会连接到指定站点下载并自动更新该策略库。需要注意的是，如果该路由策略库已经被引用，那么，必须在本页面重新引用并保存之后，相关配置才能生效。操作步骤为：首先单击该路由策略库的“编辑”超链接，再重新设置“预定义”一次，最后单击“保存”按钮，相关配置立即生效。

7.4 IP/MAC 绑定

本节主要讲述***高级配置—>IP/MAC 绑定***的配置方法。

7.4.1 IP/MAC 绑定功能介绍

7.4.1.1 IP/MAC 绑定概述

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权工作。在***安全配置—>防火墙***中，我们详细地介绍了如何实现对局域网用户上网行为的控制。在本节，我们将介绍如何解决用户的身份识别问题。

在设备中，通过 IP/MAC 绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址对作为用户唯一的身份识别标识，可以保护设备和网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到设备或者通过设备。这台电脑的 IP 地址可以轻易地改变为受信任的地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

通过在“ IP/MAC 绑定配置 ”中添加可信的计算机的静态 IP 地址和对应的 MAC 地址，即可在“ IP/MAC 绑定信息列表 ”中形成对应的 IP/MAC 地址对条目。注意，在“ IP/MAC 绑定信息列表 ”中，还可设置 IP/MAC 绑定条目的上网状态，从而控制对应的 IP/MAC 绑定用户是否可以上网。当某个 IP/MAC 绑定条目选中“ 允许 ”时（方框中出现“ √ ”），表示上网状态为“ 允许 ”，即允许与该 IP/MAC 地址对完全匹配的用户上网；未选中“ 允许 ”时（方框中没有“ √ ”），表示上网状态为“ 禁止 ”，即禁止与该 IP/MAC 地址对完全匹配的用户上网。

7.4.1.2 IP/MAC 绑定的工作原理

为方便起见，我们先介绍一下设备中，合法用户、非法用户及身份未知用户的概念。

合法用户：其 IP 及 MAC 地址与“ IP/MAC 绑定信息列表 ”中的某条目的 IP 及 MAC 地址完全匹配，且该条目的“ 允许 ”被选中。

非法用户：其 IP 及 MAC 地址与“ IP/MAC 绑定信息列表 ”中的某条目的 IP 及 MAC 地址完全匹配，且该条目的“ 允许 ” 未被选中；或者，其 IP 和 MAC 地址中有且只有一个某绑定条目的对应信息匹配。

身份未知用户：即**非 IP/MAC 绑定用户**，其 IP 或 MAC 地址均不与“ IP/MAC 绑定信息列表 ”中的任何条目的 IP 或 MAC 地址匹配，也就是除合法用户以及非法用户之外的所有用户。

对于身份未知的用户，是在 IP/MAC 绑定全局设置中统一控制的。如果选中“ 允许非 IP/MAC 绑定用户 ”,就表示允许这些用户连接或者通过设备 ;如果没有选中“ 允许非 IP/MAC 绑定用户 ”，就表示禁止这些用户连接或者通过设备。

IP/MAC 绑定应用于来自于局域网内部，连接到设备的数据包或者通过设备上网的数据包。当局域网用户有数据流量连接和通过设备时，将首先和“ IP/MAC 绑定信息列表 ”中的

条目相比较，即进行身份识别；之后，根据用户身份的不同，来自该用户的数据包将被丢弃或进入 IP 业务管理功能模块处理（即继续去匹配业务策略）。具体描述如下：

1. 如果该用户是合法用户，则允许该数据包通过，并继续去匹配业务策略；
2. 如果该用户是非法用户，则丢弃该数据包；
3. 如果该用户身份未知，则根据 IP/MAC 绑定全局配置执行：
   1) 若允许身份未知用户，即选中“ 允许非 IP/MAC 绑定用户 ”时，则允许该数据包通过，并继续去匹配业务策略；
   2) 若禁止身份未知用户，即没有选中“ 允许非 IP/MAC 绑定用户 ”时，则丢弃该数据包。

例如，如果某用户 IP/MAC 地址对 192.168.16.221 和 00:22:aa:00:22:bb 已经添加到“ IP/MAC 绑定信息列表 ”，且上网状态为“ 允许 ”（方框中出现“ √ ”），如表 7-10 所示：

表 7-10 IP/MAC 绑定信息列表——实例一

那么，当设备接收到来自局域网的数据包时，将会根据以下几种情况处理：

1. 一个 IP 地址为 192.168.16.221，MAC 地址为 00:22:aa:00:22:bb 的数据包将被允许通过，并继续去匹配业务策略；
2. 一个 IP 地址为 192.168.16.221，但是使用了其他 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击；
3. 一个使用了其他 IP 地址，但是 MAC 地址是 00:22:aa:00:22:bb 的数据包也将被丢弃，以防止 IP 欺骗攻击；
4. 如果这个数据包的 IP 地址和 MAC 地址在“ IP/MAC 绑定信息列表 ”都没有定义：
   1） 如果选中“ 允许非 IP 和 MAC 绑定用户 ”，则允许该数据包通过，并继续去匹配业务策略。
   2） 如果没有选中“ 允许非 IP 和 MAC 绑定用户 ”，则禁止该数据包通过。

如果希望禁止该用户上网，则可以直接取消“ 允许 ”的选中，即可将其上网状态改为“ 禁止 ”，如表 7-11。这时，IP 地址为 192.168.16.221，MAC 地址为 00:22:aa:00:22:bb 的数据包将被丢弃，其他情况下设备对数据包的处理同上。

表 7-11 IP/MAC 绑定信息列表——实例二

注意，在启用了 IP/MAC 绑定功能之后，如果修改了一台电脑的 IP 地址或者 MAC 地址，而且此 IP 地址和 MAC 地址已经在“ IP/MAC 绑定信息列表 ”中，则必须同时修改“ IP/MAC 绑定信息列表 ”中的相应的条目。否则这台电脑将无法访问设备或者通过设备。当未选中“ 允许非 IP/MAC 绑定用户 ”时，如果希望局域网中新增的主机可以访问或通过设备，则必须为该主机在 “ IP/MAC 绑定信息列表 ” 中添加 IP/MAC 绑定地址对，并选中 “ 允许 ”，即允许该主机上网。

IP/MAC 绑定功能只能影响用户访问设备或通过设备访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该设备的通信）。如果用户修改了 IP 或 MAC，将有可能无法访问设备或通过设备访问其他网络（如 Internet），但是不会影响局域网内部通信，比如网络邻居浏览。

7.4.2 IP 和 MAC 绑定配置

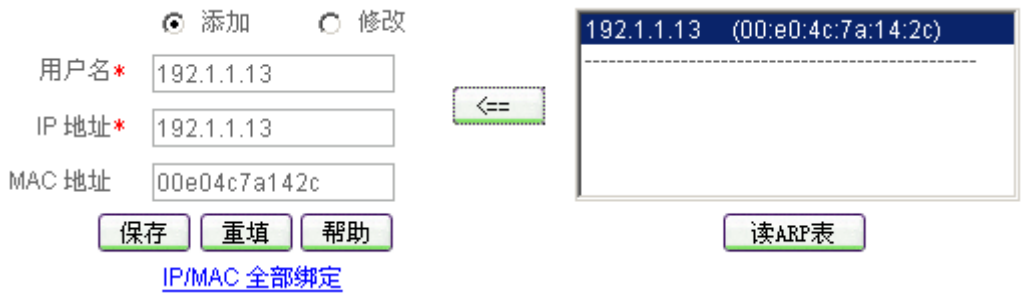


图 7-24 IP/MAC 地址绑定配置

- 用户名：欲进行 IP 和 MAC 地址绑定的用户名称。自定义，不能重复，取值范围：1～31 个字符；
- IP 地址：该用户的 IP 地址（可使用 ipconfig /all 命令获得）；
- MAC 地址：该用户的 MAC 地址（可使用 ipconfig /all 命令获得）。
- 保存：IP/MAC 绑定用户配置参数生效；
- 重填：恢复到修改前的配置参数；

- 读 ARP 表：显示 LAN 口的动态 ARP 列表，即设备通过 LAN 口动态学习到的用户的 ARP 信息。注意，如果已经将某用户的 IP/MAC 地址对添加到“ IP/MAC 绑定信息列表 ”中，该用户的 IP/MAC 地址对将不再显示。
- <==（向左箭头）：用于自动添加 IP/MAC 绑定条目。在动态 ARP 列表中，先选中一个 IP/MAC 地址对，比如 200.200.200.139（00:07:95:a8:1c:3d），再双击它或单击“ <== ”按钮，相关信息即可填充到配置框中（“ 用户名 ”也被 IP 地址填充，可修改），然后单击“ 保存 ”按钮，即可将之添加到“ IP/MAC 绑定信息列表 ”中；
- IP/MAC 全部绑定：若希望一次性将局域网主机的 IP/MAC 地址对全部绑定，则可以直接单击“ IP/MAC 全部绑定 ”超链接，转到***安全配置—>ARP 欺骗防御***页面，然后在“ 动态 ARP 表 ”中执行全部绑定操作。

7.4.3 IP/MAC 绑定全局配置

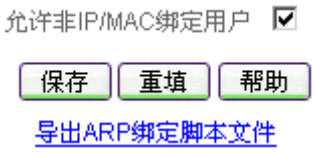


图 7-25 IP/MAC 绑定全局配置

- 允许非 IP/MAC 绑定用户：允许或禁止非 IP/MAC 绑定用户连接到设备。
- 保存：IP/MAC 绑定全局配置参数生效；
- 重填：恢复到修改前的配置参数；
- 导出 ARP 绑定脚本文件：单击“ 导出 ARP 绑定脚本文件 ”超链接，即可下载 ARP 绑定脚本文件到本地主机。运行该文件并重启主机，可将设备的 LAN 口 ARP 信息添加主机中，从而防止 ARP 欺骗。

提示：当决定取消“ 允许非 IP/MAC 绑定用户 ”功能前，必须确认管理计算机已经被添加到“ IP/MAC 绑定信息列表 ”中，否则将会造成管理计算机无法连接到设备的现象。

7.4.4 IP/MAC 绑定信息列表

表 7-12 IP/MAC 绑定信息列表

- 增加 IP/MAC 绑定条目：选中“ 添加 ”选项，输入 IP 和 MAC 绑定信息，单击“ 保存 ”按钮，生成新的 IP/MAC 绑定条目；或者，通过动态 ARP 列表来添加用户；
- 浏览 IP/MAC 绑定条目：如果已经生成了 IP/MAC 绑定条目，可以查看“ IP/MAC 绑定信息列表 ”，浏览 IP/MAC 绑定条目信息；
- 编辑 IP/MAC 绑定条目：如果想编辑某个 IP/MAC 绑定条目的 MAC 地址，只需单击该条目的“ 用户名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改 MAC 地址，再单击“ 保存 ”按钮，修改完毕；如果想编辑某个 IP/MAC 绑定条目的上网状态，则只需直接单击“ 允许 ”列中的方框，即可修改。选中“ 允许 ”时，表示上网状态为“ 允许 ”，即允许与该条目完全匹配的用户上网；未选中“ 允许 ”时，表示上网状态为“ 禁止 ”，即禁止与该条目完全匹配的用户上网。
- 删除 IP/MAC 绑定条目：选中一些 IP/MAC 绑定条目，单击右下角的“ 删除 ”按钮，即可删除被选中的条目。

7.4.5 自定义 IP/MAC 绑定条目

配置 IP/MAC 绑定条目的步骤如下：

第一步，进入***高级配置—>IP/MAC 绑定***页面；

第二步，选择“ 添加 ”选项，输入 “ 用户名 ”（自定义）、“ IP 地址 ”和“ MAC 地址 ”，然后单击“ 保存 ”按钮；或者，通过动态 ARP 列表来添加用户。

第三步，该 IP/MAC 绑定条目添加成功后，可以在“ IP/MAC 绑定信息列表 ”中查看，对于匹配该条目的数据包，将被允许连接或者通过设备。如果在***安全配置—>防火墙***中为该用户配置了防火墙策略，这些数据包还将继续去匹配这些业务策略；

第四步，继续配置其他 IP/MAC 绑定条目；

第五步，如果要禁止身份未知的用户连接或者是通过设备，则需取消“ 允许非 IP/MAC 绑定用户 ”的选中，然后单击“ 保存 ”按钮。否则的话，身份未知的用户也将被允许连接或者是通过设备；

第六步，如果要暂时禁止某个 IP/MAC 绑定用户上网，则可在“ IP/MAC 绑定信息列表 ”中修改对应条目的上网状态，即取消“ 允许 ”的选中，则表示禁止与该条目完全匹配的用户上网。

当配置完 IP/MAC 绑定之后，所有发送到设备的数据包将首先和“ IP/MAC 绑定信息列表 ”中的条目相比较。然后根据相关配置，该数据包将被丢弃或进入 IP 业务管理功能模块处理。

提示：若要删除 IP/MAC 绑定条目，在“ IP/MAC 绑定信息列表 ”中选中要删除的 IP/MAC 绑定条目，单击“ 删除 ”按钮即可。

7.4.6 配置上网“ 白名单 ”和“ 黑名单 ”

灵活地运用 IP/MAC 绑定功能，可以为局域网用户配置上网“ 白名单 ”和“ 黑名单 ”。

通过配置上网“ 白名单 ”，将只允许“ 白名单 ”中的用户通过设备上网，禁止其他所有用户通过设备上网。因此，如果要求只允许局域网中的少数用户上网，可通过配置上网“ 白名单 ”来实现。

通过配置上网“ 黑名单 ”，将只禁止“ 黑名单 ”中的用户通过设备上网，允许其他所有用户通过设备上网。因此，如果要求只禁止局域网中的少数用户上网，可通过配置上网“ 黑名单 ”来实现。

在设备中，“ 白名单 ”中的用户即为合法用户——其 IP 及 MAC 地址与“ IP/MAC 绑定信息列表 ”中的某条目完全匹配，且该条目选中“ 允许 ”。

“ 黑名单 ”中的用户即为非法用户——其 IP 及 MAC 地址与“ IP/MAC 绑定信息列表 ”中的某条目完全匹配，且该条目没有选中“ 允许 ”；或者，其 IP 和 MAC 地址中有且只有一个与某个绑定条目的对应信息匹配。

7.4.6.1 配置上网“ 白名单 ”

为局域网用户配置上网“ 白名单 ”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定合法用户，将具有上网权限的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，并添加到“ IP/MAC 绑定信息列表 ”中，还需选中“ 允许 ”，即允许与该 IP/MAC 地址对完全匹配的用户上网。

第二， 不选中“ 允许非 IP/MAC 绑定用户 ”，从而，其他所有不在“ IP/MAC 绑定信息列表 ”中的主机将不能上网。

例如，如果要允许某个 IP 地址为 192.168.16.88，MAC 地址为 0022aa112233 的主机连接和通过设备，则可添加一个 IP/MAC 绑定条目，输入该主机的 IP 地址和 MAC 地址，并选中“ 允许 ”，如下表所示。

表 7-13 IP/MAC 绑定信息列表——实例三

7.4.6.2 配置上网“ 黑名单 ”

为局域网用户配置上网“ 黑名单 ”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定非法用户，有三种方法：

1. 将禁止上网的主机的 IP 地址和任意一个非本局域网网卡的 MAC 地址作为 IP/MAC 地址绑定对，并添加到“ IP/MAC 绑定信息列表 ”中；
2. 将禁止上网的主机的 MAC 地址和任意一个非本局域网网段的 IP 地址作为 IP/MAC 地址绑定对，并添加到“ IP/MAC 绑定信息列表 ”中；

3. 可将禁止上网的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，添加到“IP/MAC 绑定信息列表”中，并取消“允许”的选中（方框中无“√”），即禁止与该 IP/MAC 地址对完全匹配的用户上网。

第二， 选中“允许非 IP/MAC 绑定用户”，从而，其他所有 IP 地址和 MAC 地址均不在“IP/MAC 绑定信息列表”中的主机将能够上网。

例如，如果要禁止具有某个 MAC 地址（例如 002244002244）的主机连接和通过设备，可以添加一个 IP/MAC 地址绑定对，输入该 MAC 地址，而 IP 地址则设置成一个任意的非本局域网的 IP 地址，如下表所示。

表 7-14 IP/MAC 绑定信息列表——实例四

例如，如果要禁止具有某个 IP 地址（例如 192.168.16.100）的主机访问和连接设备，可以添加一个 IP/MAC 地址绑定对，输入该 IP 地址，而 MAC 地址则设置成任意一个非本局域网网卡的 MAC 地址，如下表所示。

表 7-15 IP/MAC 绑定信息列表——实例五

例如，如果要禁止某个 IP 地址为 192.168.16.88，MAC 地址为 0022aa112233 的主机连接和通过设备，则可添加一个 IP/MAC 地址绑定对，输入该主机的 IP 地址和 MAC 地址，并取消“允许”的选中（方框中无“√”），如下表所示。

表 7-16 IP/MAC 绑定信息列表——实例六

7.5 特殊功能

本节主要讲述***高级配置—>特殊功能***的配置方法。

7.5.1 快速转发

7.5.1.1 快速转发功能概述

快速转发功能，是通过使用转发缓存来简化分组的转发操作，从而提高分组转发速率和转发的吞吐量。在快速转发过程中，只需对一组具有相同目的地址和原地址的分组的前几个分组进行传统的路由转发处理，并把成功转发的分组的目的地址、源地址和下一网关地址（下一路由器地址）放入转发缓存中。当其后的分组要进行转发时，会首先查看转发缓存，如果该分组的目的地址和源地址与转发缓存总的匹配，则直接根据转发缓存中的下一网关地址进行转发，而无须经过传统的复杂操作，大大减轻了路由器（网关）的负担，达到了提高路由器吞吐量的目标。

7.5.1.2 快速转发配置

图 7-26 启用快速转发

- 启用快速转发：启用或者是关闭快速转发，选中是启用。快速转发功能可以实现各个物理接口数据的快速转发，全面提高性能。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

7.5.2 虚拟局域网

7.5.2.1 虚拟局域网功能概述

虚拟局域网（VLAN）是一种通过将局域网内设备的逻辑地址而不是物理地址划分成一个个网段从而实现虚拟工作组的技术，一个 VLAN 组成一个逻辑子网，即一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信；不同的 VLAN 之间实现物理隔离，一个 VLAN 内部的单播、广播和多播包都不会转发到其他 VLAN 中，从而有助于控制流量、简化网络管理、加强网络安全性。设备可实现基于端口的虚拟局域网（VLAN），将 LAN 口（集成多端口以太网交换机）的多个端口设置成不同的组号，相同组号的端口即构成一个 VLAN。

7.5.2.2 虚拟局域网配置

图 7-27 虚拟局域网

- 端口 1 组号~端口 4 组号：LAN 口的 4 个交换口可以配置不同的组号，相同组号的端口在一个交换机广播域内，不同组号的端口之间相互隔离。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。
- **提示**：

1. 相同组号的端口构成一个虚拟局域网（即 VLAN），同一 VLAN 中的端口可互相连通；不同 VLAN 之间的端口，相当于硬件隔离，不能相互通信；

2. 缺省情况下所有端口都属于同一个 VLAN，最复杂情况每个端口分别属于不同的 VLAN。如图 7-27 中，表示端口 1 和端口 2 同属一个 VLAN（组号均为 1），端口 3、端口 4 分别各属一个 VLAN；

7.5.3 端口镜像

7.5.3.1 端口镜像功能概述

端口镜像功能可将设备其他端口的流量自动复制到镜像端口，实时提供各端口的传输状况的详细资料，以便网络管理人员进行流量监控、性能分析和故障诊断。设备中，LAN 口的端口 1 为镜像端口。由于设备的端口镜像功能完全由硬件提供，因此不会影响设备的性能、速度以及各个应用功能。

7.5.3.2 端口镜像配置

图 7-28 启用端口镜像

- 启用端口镜像：启用或者关闭端口镜像，选中是启用。设备中，LAN 口的端口 1 实现端口镜像的功能，端口 2、3、4 的流量将镜像到端口 1，以便进行流量和协议分析，提供诊断便利。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。
- **提示**：如果 LAN 口的 4 个端口不在同一个虚拟局域网内，那么只有与端口 1 同属一个虚拟局域网的端口的流量才能镜像到端口 1。

7.5.3.3 端口镜像应用实例

传统方式下，为实现对网吧或企业内部流量得监控和管理，一般是在设备下再接一台 HUB，而 HUB 是共享型网络设备，放在总出口，无疑会大大降低网络速度，造成网络瓶颈。如果采用设备，则只需将监控主机直接连到 LAN 口的端口 1，如图 7-29 所示，再在***高级配置—>特殊功能***中启用端口镜像功能，即可在监控主机上监控到整个局域网的流量。

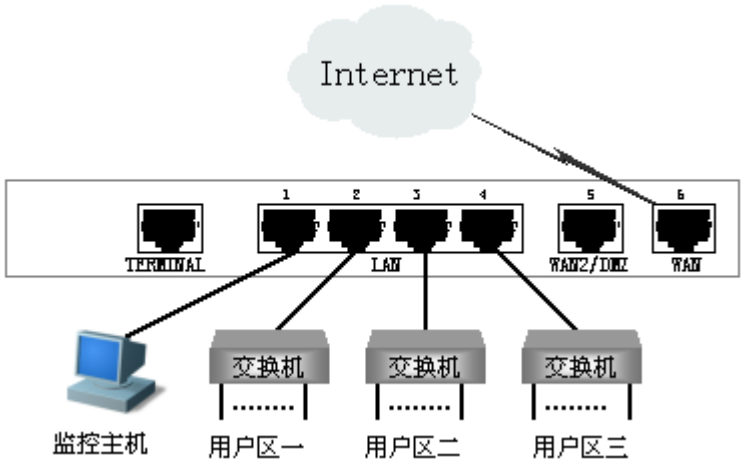


图 7-29 端口镜像应用实例

7.6 DHCP 配置

7.6.1 DHCP 简介

7.6.1.1 DHCP 介绍

动态主机配置协议（DHCP）是一种用于简化主机 IP 配置管理的协议标准。通过采用 DHCP 标准，可以使用 DHCP 服务器为网络上所有启用了 DHCP 的客户端分配、配置、跟踪和更改（必要时）所有 TCP/IP 设置。此外，DHCP 还可以确保不使用重复地址、重新分配未使用的地址，并且可以自动为连接的子网分配适当的 IP 地址。

针对不同的需求，DHCP 服务器有三种机制分配 IP 地址：

- 静态分配，DHCP 服务器给首次连接到网络的某些客户端分配固定 IP 地址，该地址由用户长期使用；
- 动态分配，DHCP 服务器给客户端分配有时间限制的 IP 地址，使用期限到期后，客户端需要重新申请地址，客户端也可以主动释放该地址。绝大多数客户端主机得到的是这种动态分配的地址；
- 手动分配，由网络管理员为客户端指定固定的 IP 地址。

三种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。设备支持后面两种机制。

7.6.1.2 DHCP 的工作原理

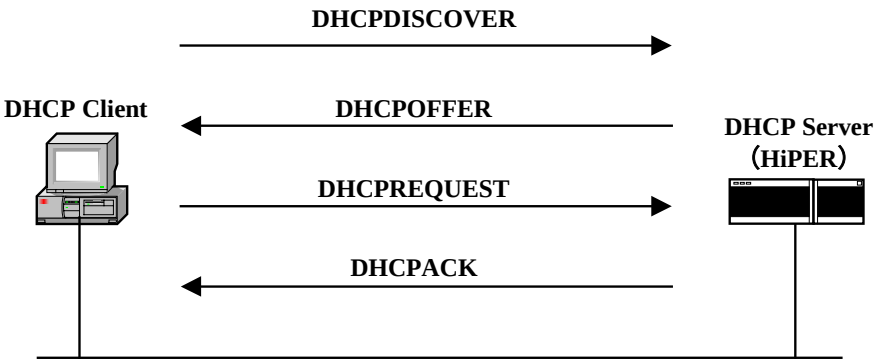


图 7-30 DHCP 基本工作流程

DHCP 工作的基本流程如图 7-30 所示，下面将分别介绍 DHCP 请求 IP 地址、续租地址及释放地址这三个业务的过程。

1. DHCP 请求 IP 地址的过程

- 发现阶段：即 DHCP 客户端寻找 DHCP 服务器的阶段。客户端以广播方式发送 DHCPDISCOVER 包，只有 DHCP 服务器才会响应。
- 提供阶段：即 DHCP 服务器提供 IP 地址的阶段。DHCP 服务器接收到客户端的 DHCPDISCOVER 包后，从 IP 地址池中选择一个尚未分配的 IP 地址分配给客户端，向

该客户端发送包含租借的 IP 地址和其他配置信息的 DHCPOFFER 包。

- 选择阶段：即 DHCP 客户端选择 IP 地址的阶段。如果有多台 DHCP 服务器向该客户端发送 DHCPOFFER 包，客户端从中随机挑选，然后以广播形式向各 DHCP 服务器回应 DHCPREQUEST 包，宣告使用它挑中的 DHCP 服务器提供的地址，并正式请求该 DHCP 服务器分配地址。其它所有发送 DHCPOFFER 包的 DHCP 服务器接收到该数据包后，将释放已经 OFFER（预分配）给客户端的 IP 地址。
  如果发送给 DHCP 客户端的 DHCPOFFER 包中包含无效的配置参数，客户端会向服务器发送 DHCPDECLINE 包拒绝接受已经分配的配置信息。
- 确认阶段：即 DHCP 服务器确认所提供 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户端发送的 DHCPREQUEST 包后，便向客户端发送包含它所提供的 IP 地址及其他配置信息的 DHCPACK 确认包。然后，DHCP 客户端将接收并使用 IP 地址及其他 TCP/IP 配置参数。

2. DHCP 客户端续租 IP 地址的过程

- DHCP 服务器分配给客户端的动态 IP 地址通常有一定的租借期限，期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 租约。实际使用中，在 IP 地址租约期限达到一半时，DHCP 客户端会自动向 DHCP 服务器发送 DHCPREQUEST 包，以完成 IP 租约的更新。如果此 IP 地址有效，则 DHCP 服务器回应 DHCPACK 包，通知 DHCP 客户端已经获得新 IP 租约。
  如果 DHCP 客户端续租地址时发送的 DHCPREQUEST 包中的 IP 地址与 DHCP 服务器当前分配给它的 IP 地址（仍在租期内）不一致，DHCP 服务器将发送 DHCPNAK 消息给 DHCP 客户端。

3. DHCP 客户端释放 IP 地址的过程

- DHCP 客户端已从 DHCP 服务器获得地址，并在租期内正常使用，如果该 DHCP 客户端不想再使用该地址，则需主动向 DHCP 服务器发送 DHCPRELEASE 包，以释放该地址，同时将其 IP 地址设为 0.0.0.0。

7.6.1.3 DHCP 数据包的类型

DHCP 协议采用 CLIENT－SERVER 方式进行交互，其数据包格式共有 8 种，具体含义如表 7-17 所示：

格式	中文解释	含义
DHCPDISCOVER	发现包	此为 Cilent 在 DHCP 过程中发送的第一个包
DHCPOFFER	提供包	此为 Server 对 DHCPDISCOVER 包的响应
DHCPREQUEST	请求包	此为 Client 在 DHCP 过程中对 Server 的 DHCPOFFER 包的回应，或是 Client 续租 IP 地址时发出的数据包
DHCPDECLINE	拒绝包	当 Client 发现 Server 分配给它的 IP 地址无法使用，如 IP 地址冲突时，将发出此数据包，通知 Server 拒绝使用这个 IP 地址
DHCPACK	确认包	Server 对 Client 的 DHCPREQUEST 包的确认响应包，Client 收到此数据包后，才真正获得了 IP 地址和相关的配置信息

DHCPNAK	否认包	Server 对 Client 的 DHCPREQUEST 包的拒绝响应包，Client 收到此数据包后，一般会重新开始新的 DHCP 过程。
DHCPRELEASE	释放包	Client 主动释放 Server 分配给它的 IP 地址的数据包，当 Server 收到它后，就可以回收这个 IP 地址，从而可将该地址分配给其他的 Client。
DHCPINFORM	信息包	Client 已经获得了 IP 地址，发送此报文，只是为了从 Server 处获得其他的一些网络配置信息，如 route ip、DNS IP 等，此数据包的应用非常少见。

表 7-17 DHCP 数据包的类型

7.6.2 设备的 DHCP 功能概述

通过不同的设置，设备可以充当 DHCP 客户端、DHCP 服务器或 DHCP 中继，下面分别简要介绍它们的特点。

提示：在某一个接口上，若启用了 DHCP 客户端功能，则不允许启用 DHCP 服务器（不允许配置绑定在该接口的 DHCP 地址池）或 DHCP 中继功能 如果 DHCP 服务器与 DHCP 中继同时打开，则优先使用 DHCP 服务器处理 DHCP 包，只有当 DHCP 服务器无法处理时，才将 DHCP 数据包转交由给 DHCP 中继处理。

7.6.2.1 DHCP 服务器

将设备配置成为 DHCP 服务器，设备可提供 DHCP 服务——为局域网计算机动态分配 IP 地址、子网掩码、网关以及 DNS 服务器、WINS 服务器等信息。

1. 地址冲突检测方式

DHCP 服务器为客户端分配地址前，需要先对该地址进行探测，以防止 IP 地址重复分配导致地址冲突。设备支持两种地址检测方式：ARP 方式和 ICMP 方式。ARP 方式为系统缺省方式，不能关闭；ICMP 方式可配置，可关闭。

ARP 方式：DHCP 服务器在分配某 IP 地址之前，首先会通过 ARP 方式检测该 IP 地址是否已被使用。如果连续发两个 ARP 包后均无回应，则认为该地址是空闲地址；否则，将认为该地址正被使用，就试图分配另外一个 IP 地址，直到检测通过。

ICMP 方式：经 ARP 方式检测通过的 IP 地址，还要通过 ICMP 方式进行进一步检测。它是通过发送 ICMP ECHO REQUEST 包（一次一个数据包）实现的，检测是否能在指定时间内得到应答。如果没有得到应答，则继续发送 ICMP 检测包，直到发送包数量达到最大值，如果一直没有应答，DHCP 服务器认为该地址为空闲地址，就将该地址分配给 DHCP 客户端；如果有应答，就认为该地址正被使用，将试图分配另外一个 IP 地址，直到分配成功。

缺省情况下，ICMP 方式中，ICMP 检测包的数量为 2，最长等待回应时间为 500 毫秒。特别地，如果将检测包的数量设为 0，则表示关闭 ICMP 检测。

2. DHCP 地址池

在设备中，DHCP 服务器的给客户端分配地址及 DHCP 各项参数时，都需要在 DHCP 地址池中进行定义。设备支持配置多个地址池，从而实现在局域网中存在多个子网时，方便

用户使用。在配置地址池之前，必须指定该地址池绑定的接口。

3. DHCP 手工绑定

设备是通过配置 DHCP 手工绑定来实现手动分配地址的，即为某些需要使用固定 IP 地址的客户端主机预先指定 IP 地址，可通过设置 MAC 地址（MAC address）与 IP 地址绑定来实现，也可通过设置远程标识（Remote ID）或客户端标识（Client ID）与 IP 地址绑定来实现。当具有此 MAC 地址（或 Remote ID，或 Client ID）的客户端向 DHCP 服务器申请地址时，服务器会根据客户端 MAC 地址（或 Remote ID，或 Client ID）寻找到对应的固定 IP 地址分配给客户端。

4. IP 地址的分配策略

DHCP 服务器将根据客户端发送的数据包所携带的信息为它分配 IP 地址，可以作为分配依据的参数如下：远程标识（Remote ID)、DHCP 中继标识（Circuit ID)、DHCP 中继地址（giaddr)、客户端标识（Client ID）或 MAC 地址（MAC address)。DHCP 服务器将按顺序依次照上述参数，如果发现某个参数相匹配，将按照该参数指定的配置来分配 IP 地址。如果上述参数均不匹配，将按照缺省方式，顺序查找可供分配的 IP 地址。

具体地说，DHCP 服务器将按如下次序给 DHCP 客户端分配 IP 地址：

1） 如果客户端发送的数据包带有远程标识（Remote ID）选项，则先搜索 DHCP 手工绑定信息列表，检查是否有与该 Remote ID 绑定的 IP 地址，如果有，就将这个 IP 地址分配给该客户端；如果没有，执行下一步。
2） 如果客户端发送的数据包带有 DHCP 中继标识（Circuit ID）选项，则搜索 DHCP 地址池信息列表，检查是否有地址池设置了该 Circuit ID，如果有，使用这个地址池里面的 IP 地址进行分配；如果没有，执行下一步。
3） 如果客户端发送的数据包的 DHCP 中继地址（giaddr）不为 0，则搜索 DHCP 地址池信息列表，检查是否有地址池设置了该 giaddr，如果有，则使用这个地址池里面的 IP 地址进行分配；如果没有，执行下一步。
4） 如果客户端发送的数据包带有客户端标识（Client ID）选项，则搜索 DHCP 手工绑定信息列表，检查是否有与该 Client ID 绑定的 IP 地址，如果有，就将这个 IP 地址分配给该客户端；如果没有，执行下一步。
5） 搜索 DHCP 手工绑定信息列表，检查是否有与该客户端的 MAC 地址绑定的 IP 地址，如果有，就将这个 IP 地址分配给该客户端；如果没有，执行下一步。
6） 如果客户端发送的数据包中带有请求 IP 地址（Requested IP Address）选项，则查找这个 IP 地址所从属的地址池，并尝试将请求的 IP 地址分配给该客户端；如果该 IP 地址已分配，则尝试从这个地址池中动态分配另一个地址。如果没有该地址选项，执行下一步。
7） 上述参数均不匹配，则按照配置 DHCP 地址池的顺序，依次查找可供分配的 IP 地址，将最先找到的 IP 地址分配给客户端；
8） 如果未找到可用的 IP 地址，则报告错误。

注意事项：

1) 配置 DHCP 手工绑定时，有三个与 IP 地址绑定的参数可选，按优先级从高到低排列为 :远程标识(Remote ID)、客户端标识(Client ID)及 MAC 地址(MAC Address)。如果三个全部都设置或设置了其中的两个，只有优先级最高的一项起作用。举例说明，如果设置了 Remote ID，则 Client ID 对地址分配不起作用，即当 Remote ID 不

符合时，即使客户端发送的数据包携带该 Client ID，也得不到该 IP 地址。

2) 如果客户端发送的数据包携带的 Circuit ID 或 giaddr 与某个地址池的相关参数匹配，会在该地址池中优先检查 DHCP 手工绑定的 Client ID 或 MAC 地址，看是否有匹配项，如果有匹配项，将把与该 Cilent ID 或 MAC 地址绑定的 IP 地址分配给该客户端 如果没有匹配的 Cilent ID 或 MAC 地址，还会检查 Requested IP Address，如果请求的 IP 地址存在，将把该地址分配给该客户端。如果 Client ID、MAC 地址和 Requested IP Address 均无匹配值，将使用这个地址池中的 IP 地址进行动态分配。
3) 如果某个地址池设置了 DHCP 中继标识（Circuit ID）选项，那么当客户端发送的数据包不匹配该 Circuit ID，但是匹配某条 DHCP 手工绑定时，将会把此绑定条目指定的 IP 地址分配给该客户端。某个地址池设置了 DHCP 中继地址（giaddr）时，情况类似。
4) 如果某客户端发送的数据包与某条 DHCP 手工绑定匹配，但是该 IP 地址已被其他人使用（即地址检测有冲突），则 DHCP 服务器不会将该地址分配给该客户端，也不会为该客户端分配其他地址。
5) 当某个定义了 DHCP 中继标识（Circuit ID）或中继地址（giaddr）的地址池中的地址已全部分配，设备会为匹配该 Circuit ID 或 giaddr 的客户端分配其他地址池中的地址。

7.6.2.2 DHCP 客户端

将设备配置成为 DHCP 客户端，设备可自动地从 DHCP 服务器，得到 IP 地址及其他配置参数。设备的所有以太网接口都支持 DHCP 客户端，允许各接口同时启用 DHCP 客户端功能。

设备支持配置客户端标识（Client ID），允许客户端以广播或单播方式发送 DHCPREQUEST 包，可以通知 DHCP 服务器以单播或广播方式回复客户端发送的数据包，从而满足各种不同需要。

设备还支持 AutoIP 功能，允许 DHCP 客户端在无法得到 IP 地址的情况下，给自己分配 IP 地址（地址范围：169.254.1.0/16~169.254.254.0/16）。

7.6.2.3 DHCP 中继

将设备设置成 DHCP 中继，设备就能在 DHCP 服务器和客户端之间转发 DHCP 数据包。当 DHCP 客户端与服务器不在同一个子网时，必须有 DHCP 中继来转发 DHCP 请求和应答信息。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。DHCP 中继的工作原理如下：

1. 当 DHCP 客户端启动并进行 DHCP 初始化时，它在本地网络广播发现的报文；
2. 若本地子网存在 DHCP 服务器，将直接进行 DHCP 配置，不需要 DHCP 中继；
3. 若本地子网没有 DHCP 服务器，则与本地子网相连的、带 DHCP 中继功能的网络设备收到该广播报文后，进行适当处理并转发给指定的、其它子网上的 DHCP 服务器；
4. DHCP 服务器根据客户端提供的信息进行相应的配置，并通过 DHCP 中继将配置信息发送给客户端，完成对客户端的动态配置。从开始配置到最终完成配置，可能存在多次这样的交互过程。

设备通过选项（option）和策略（policy）这两个参数来定义对 DHCP 数据包的转发策

略，当 DHCP 中继接收到 DHCP 客户端发出的数据包后，将根据这两个参数的配置进行不同的处理，如下表所示。

	option	policy	直接由 client 发出，无 82option	由 Relay 发出，含有 82option
合法 DHCP 数据包	insert	drop	加 82 option 转发	丢弃此数据包
		keep	加 82 option 转发	保持原有 82option 转发
		replace	加 82 option 转发	取代原有 82option 转发
	disable	drop	转发	丢弃此数据包
		keep	转发	转发
		replace	转发	转发

表 7-18 选项和策略对中继行为的影响

上表中，部分参数涵义解释如下：

82option——DHCP 数据包中的中继信息选项；

option——选项，包括 insert（插入）和 disable（禁用）；

policy——策略，包括 drop（丢弃）、keep（保留）和 replace（替换）。

当 option 为 disable 时，如果 policy 为 drop，且数据包由 relay 发出（含有 82option），该数据包将被丢弃；其他任何情况下，均是直接转发该数据包。

当 option 为 insert 时，根据策略和数据包来源不同，将对该数据包进行不同的转发处理。

7.6.2.4 自定义选项（Raw Option）

DHCP 提供了一个机制，允许在 TCP/IP 网络中将配置信息传送给主机。DHCP 报文中有专门 Option 字段，该部分内容为可变化内容，可以根据实际情况进行定义，DHCP 客户端必须能够接收携带至少 312 字节 Option 信息的 DHCP 报文。关于当前 DHCP Option 的定义，请参见 RFC 2131、RFC1541。

随着 DHCP 的不断发展，新的可选配置项会不断出现，为了支持这些新的选项，设备提供了自定义选项（Raw Option）功能，设备的 DHCP 服务器和客户端均支持该功能。

7.6.3 DHCP 客户端

进入***高级配置—>DHCP*** 页面，选中“ DHCP 客户端 ”选项，如下图所示，即可进入 DHCP 客户端配置界面。

图 7-31 选择 DHCP 客户端

7.6.3.1 DHCP 客户端配置

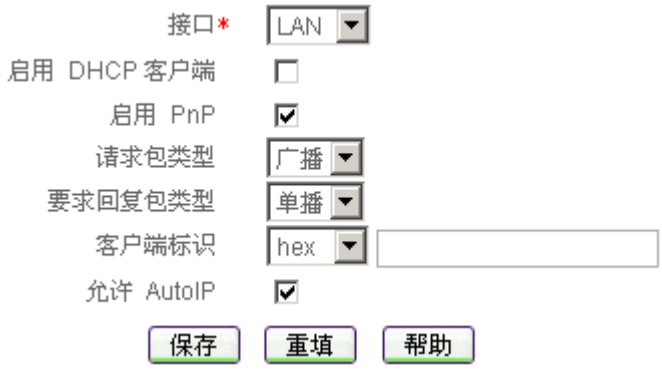


图 7-32 DHCP 客户端配置界面

- 接口：指定欲启用 DHCP 客户端功能的物理接口；
- 启用 DHCP 客户端：启用或禁用 DHCP 客户端功能，选中为启用；
- 启用 PnP：启用或禁用 PnP 功能，选中为启用。若设备启用了 DHCP 客户端功能，并启用 PnP 功能，则设备开机后，可从 DHCP 服务器或 DHCP 代理获得 IP 地址、子网掩码、网关地址及 DNS 服务器；如果禁用 PnP 功能，则只能获得 IP 地址和子网掩码，不能获得网关地址和 DNS 服务器。
- 请求包类型：DHCP 客户端发送请求包（即 DHCPREQUEST 包）的方式，缺省为广播方式，也可以将其设为单播方式。
  广播：DHCP 客户端通过广播方式发送请求包；
  单播：DHCP 客户端通过单播方式发送请求包；
- 要求回复包类型：DHCP 客户端发送 DHCP 数据包时，要求 DHCP 服务器发送回复包的方式，缺省为单播方式，也可将其设置为广播方式；
  单播：DHCP 客户端发送数据包时，要求 DHCP 服务器通过单播方式发送回复包；
  广播：DHCP 客户端发送数据包时，要求 DHCP 服务器通过广播方式发送回复包；
- 客户端标识：指定客户端标识，有 hex，ascii，ip 三种表示方式。
  hex：定义一个十六进制字符串，取值范围：1～27 个字符；
  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；
  ip：定义一个 IP 地址，点分式十进制表示；
- 允许 AutoIP：允许或禁止使用 AutoIP 功能，选中为启用；AutoIP 功能是指 DHCP 客户端在无法得到 IP 地址的情况下，可自动设置地址，并保证此地址在网络中不会产生冲突。自动设置的地址范围：169.254.1.0/16~169.254.254.0/16。
- 保存：DHCP 客户端配置生效；
- 重填：恢复到修改前的配置参数。

7.6.3.2 DHCP 客户端信息列表

表 7-19 DHCP 客户端信息列表

表 7-20 DHCP 客户端信息列表（续表 7-19）

- 配置 DHCP 客户端：选择欲启用客户端功能的“ 接口 ”，选中“ 启用 DHCP 客户端 ”，输入其他相关配置信息，单击 “ 保存 ” 按钮，DHCP 客户端配置完成；
- 浏览 DHCP 客户端：如果已经启用了 DHCP 客户端，可在 “ 客户端信息列表 ” 中查看相关配置及状态信息；
- 编辑 DHCP 客户端：如果需要编辑修改 DHCP 客户端相关信息，直接进入原配置界面修改即可；
- 释放：选中某个启用 DHCP 客户端功能接口对应的条目，单击 “ 释放 ” 按钮，该 DHCP 客户端将释放当前得到的 IP 地址；
- 更新：选中某个启用 DHCP 客户端功能接口对应的条目，单击 “ 更新 ” 按钮，该 DHCP 客户端将自动完成一次 “ **释放 IP 地址—>重新获得 IP 地址** ” 的过程；
- 刷新：单击 “ 刷新 ” 按钮，将显示最新的 DHCP 客户端使用信息。

7.6.3.3 配置 DHCP 客户端

第一步，进入***高级配置—>DHCP*** 页面，然后选中 “ DHCP 客户端 ”，进入 DHCP 客户端配置页面；

第二步，选择欲启用 DHCP 客户端功能的 “ 接口 ”；

第三步，选中 “ 启用 DHCP 客户端 ”；

第四步，一般情况下，选中 “ 启用 PnP ”；

第五步，如有需要，选择 “ 请求包类型 ” 和 “ 要求回复包类型 ”；

第六步，如有需要，选择 “ 客户端标识 ”；

第七步，一般情况下，选中“ 允许 AutoIP ”；

第八步，单击“ 保存 ”按钮，指定接口的 DHCP 客户端功能配置完成，可在“ DHCP 客户端信息列表 ”中查看相关信息。

提示：如果要禁用某端口的 DHCP 客户端功能，请取消指定端口“ 启用 DHCP 客户端 ”的选中，单击“ 保存 ”按钮。

7.6.4 DHCP 服务器

进入***高级配置—>DHCP*** 页面，选中“ DHCP 服务器 ”选项，即可进入 DHCP 服务器配置界面，该页面包括 DHCP 服务器全局配置、DHCP 地址池配置、DHCP 手工绑定配置三个配置部分。

图 7-33 选择 DHCP 服务器

7.6.4.1 DHCP 服务器全局配置

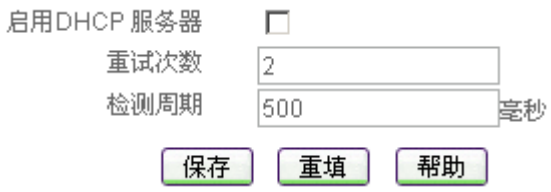


图 7-34 DHCP 服务器全局配置

- 启用 DHCP 服务器：禁用或允许 DHCP 服务器功能。选中为允许；
- 重试次数：ICMP 方式地址检测时，发送 ICMP ECHO REQUEST 检测包的最大次数（一次一个数据包）。取值范围：0～10，缺省值为 2。特别地，0 表示不进行 ICMP 检测。
- 检测周期：ICMP 方式地址检测时，每个 ICMP 检测包的最长等待回应时间。单位：毫秒；取值范围：100～10000，缺省值为 500。
- 保存：DHCP 服务器全局配置生效；
- 重填：恢复到修改前的配置参数。

7.6.4.2 DHCP 地址池配置

如章节 7.6.2.1 中所述，DHCP 服务器通过 DHCP 地址池给用户分配 IP 地址。当 DHCP 客户端向服务器发出 DHCP 请求时，DHCP 服务器根据一定的策略选择合适的地址池，并从中挑选一个空闲的 IP 地址，与其他 TCP/IP 相关配置参数（如网关地址、DNS 服务器地址、WINS 服务器地址、地址租用时间等）一起传送给客户端。设备支持配置多个 DHCP 地址池。

图 7-35 DHCP 服务器地址池配置

- 接口：当前 DHCP 地址池绑定的接口，可以是 LAN、WAN1 或 WAN2/DMZ 口；
- 地址池名：当前 DHCP 地址池的名称。自定义，不可重复，取值范围：1~11 个字符；
- 起始地址：当前 DHCP 地址池给客户端自动分配的起始 IP 地址；
- 子网掩码：当前 DHCP 地址池给客户端自动分配的 IP 地址的子网掩码；
- 总地址数：当前 DHCP 地址池可分配的地址数目；
- 网关地址：当前 DHCP 地址池给客户端自动分配的网关地址；默认为空，表示将使用该地址池所绑定的接口的 IP 地址作为网关地址；
- 租用时间：当前 DHCP 地址池给客户端自动分配的 IP 地址的有效租用期限，缺省为 3600 秒；对于不同的地址池，DHCP 服务器可以指定不同的地址租用时间，但同一 DHCP 地址池分配的 IP 地址都具有相同的期限；
- 主 DNS 服务器：当前 DHCP 地址池给 DHCP 客户端自动分配的首先 DNS 服务器的 IP 地址；
- 备 DNS 服务器：当前 DHCP 地址池给 DHCP 客户端自动分配的备用 DNS 服务器的 IP 地址；
- 主 WINS 服务器：当前 DHCP 地址池给 DHCP 客户端自动分配的首先 WINS 服务器的 IP 地址；
- 备 WINS 服务器：当前 DHCP 地址池给 DHCP 客户端自动分配的备用 WINS 服务器的 IP 地址；
- 域名：当前 DHCP 地址池给客户端自动分配的域名。通过指定客户端的域名，使得

客户端通过主机名访问网络资源时，不完整的主机名会自动加上域名后缀形成完整的主机名。可以为每个地址池分别指定客户端使用的域名；

- DHCP 中继地址：当前 DHCP 地址池使用的 DHCP 中继地址，它可作为分配地址策略的依据；
- 允许 AutoIP：是否允许 DHCP 客户端使用 AutoIP 功能获得的地址与 DHCP 服务器分配的地址共存，选中表示允许；
- 回复包类型：DHCP 服务器接收到客户端发送的数据包后，发送回复包的方式。可指定 DHCP 服务器按照单播或广播发送回复包，也可要求服务器按照客户端指定的方式发送回复；。

  客户端决定：要求 DHCP 服务器按照 DHCP 客户端指定的方式发送回复包；

  单播：要求 DHCP 服务器按照单播方式发送回复包；

  广播：要求 DHCP 服务器按照广播方式发送回复包；
- NetBIOS 节点类型：当前 DHCP 地址池给客户端指定的 NetBIOS 节点类型；可以为空，表示不限制；

  B 节点：即广播型节点（Broadcast Node），通过广播方式进行 NetBIOS 名字解析；

  P 节点：即对等型节点(Peer-to-Peer Node)，通过直接请求 WINS 服务器进行 NetBIOS 名字解析；

  M 节点：即混合型节点（Mixed Node），先通过广播方式请求名字解析，后通过与 WINS 服务器连接进行名字解析；

  H 节点：即复合型节点（Hybrid Node），先通过直接请求 WINS 服务器进行 NetBIOS 名字解析，如果没有得到应答，就通过广播方式进行 NetBIOS 名字解析；
- DHCP 中继标识：当前 DHCP 地址池使用的 DHCP 中继标识，它可作为分配地址策略的依据，有 hex，ascii，ip 三种表示方式；

  hex：定义一个十六进制字符串，取值范围：1～27 个字符；

  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；

  ip：定义一个 IP 地址，点分式十进制表示；
- 保存：DHCP 地址池配置生效；
- 重填：恢复到修改前的配置参数。

提示：系统提供一个缺省地址池，地址池名为“ pool1 ”，绑定在 LAN 口，起始地址为 192.168.16.65，总地址数为 62。该地址池不能删除，只能编辑修改。在***基本配置—>DHCP 和 DNS 服务器***中，启用 DHCP 服务器后，提供的 DHCP 地址池就是“ pool1 ”。

7.6.4.3 DHCP 地址池信息列表

表 7-21 DHCP 地址池信息列表

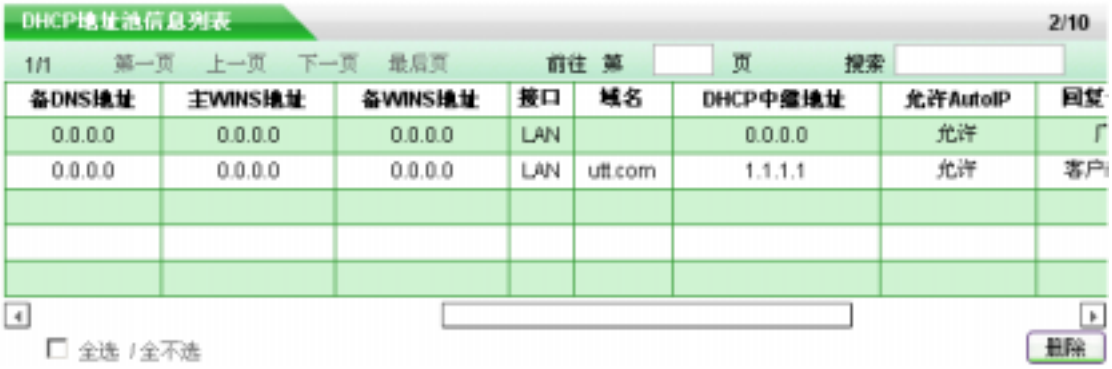


表 7-22 DHCP 地址池信息列表（续表 7-21）

表 7-23 DHCP 地址池信息列表（续表 7-22）

- 增加 DHCP 地址池：选中“ 添加 ”选项，输入相关配置信息，单击“ 保存 ”按钮，生成 DHCP 地址池；
- 浏览 DHCP 地址池：如果已经生成了 DHCP 地址池，可在“ DHCP 地址池信息列表 ”中查看相关配置信息；
- 编辑 DHCP 地址池：如果想编辑某个 DHCP 地址池，只需单击此地址池的“ 地址池名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”，修改完毕；
- 删除 DHCP 地址池：选中一些 DHCP 地址池，单击右下角的“ 删除 ”按钮，即可删除那些被选中的 DHCP 地址池。

7.6.4.4 自定义 DHCP 地址池

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 地址池配置 ”栏，选中“ 添加 ”选项，选择 DHCP 地址池绑定的“ 接口 ”；

第三步，填写“ 地址池名 ”、“ 起始地址 ”、“ 总地址数 ”及“ 主 DNS 服务器 ”等信息；

第四步，根据需要，填写“ 子网掩码 ”、“ 网关地址 ”、“ 租用时间 ”等信息；

第五步，如有需要，填写“ 备 DNS 服务器 ”、“ 主 WINS 服务器 ”、“ 备 WINS 服务器 ”；

第六步，如有需要，填写“ 域名 ”、“ DHCP 中继地址 ”、“ DHCP 中继标识 ”；

第七步，一般情况下，选中“ 允许 AutoIP ”；

第八步，如果需要，配置“ 回复包类型 ”、“ NetBIOS 节点类型 ”；

第八步，单击“ 保存 ”按钮，当前 DHCP 地址池配置完成，可在“ DHCP 地址池信息

列表 ” 中看到添加的记录。

提示：如果要删除 DHCP 地址池，在 “ DHCP 地址池信息列表 ” 中选中要删除的 DHCP 地址池，单击 “ 删除 ” 按钮，即可删除被选中的 DHCP 地址池。

7.6.4.5 DHCP 手工绑定配置

图 7-36 DHCP 手工绑定配置

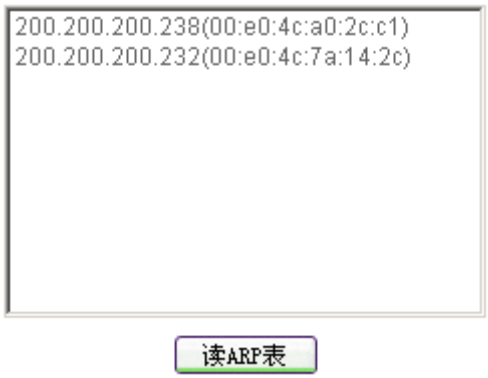


图 7-37 读 ARP 表

- 绑定：DHCP 手工绑定条目所属的 DHCP 地址池；
- 用户名：欲配置该 DHCP 手工绑定的计算机的用户名（自定义，不能重复）。取值范围：1～31 个字符；
- IP 地址：预留的 IP 地址，必须是当前绑定地址池中的合法 IP 地址；
- MAC 地址：固定使用该预留 IP 地址的计算机的 MAC 地址；
- 客户端标识：固定使用该预留 IP 地址的计算机的客户端标识，有 hex，ascii，ip 三种表示方式。
  hex：定义一个十六进制字符串，取值范围：1～27 个字符；
  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；
  ip：定义一个 IP 地址，点分式十进制表示；
- 远程标识：固定使用该预留 IP 地址的计算机的远程标识，有 hex，ascii，ip 三种表示方式。
  hex：定义一个十六进制字符串，取值范围：1～27 个字符；
  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；
  ip：定义一个 IP 地址，点分式十进制表示；

- 主机名：欲配置 DHCP 手工绑定的计算机的主机名。自定义，不能重复，取值范围：1～31 个字符。
- 保存：DHCP 手工绑定配置生效；
- 重填：恢复到修改前的配置参数；
- 读 ARP 表：显示当前的动态 ARP 映射条目，即设备通过 LAN 口动态学习到的用户的 ARP 信息。注意，如果已经将某用户的 IP/MAC 地址对添加到“ DHCP 手工绑定信息列表 ”中，该用户的 IP/MAC 地址对将不再显示。双击 ARP 表中某条信息，对应 IP 地址和 MAC 地址即可填充到如图 7-36 所示的编辑栏中。

7.6.4.6 DHCP 手工绑定列表

表 7-24 DHCP 手工绑定信息列表

表 7-25 DHCP 手工绑定信息列表（续表 7-24）

- 增加 DHCP 手工绑定：选中“ 添加 ”选项，输入相关配置信息，单击“ 保存 ”按钮，生成 DHCP 手工绑定；
- 浏览静态 DHCP 映射：如果已经生成了 DHCP 手工绑定，可在“ DHCP 手工绑定信息列表 ”中查看相关配置信息；
- 编辑 DHCP 手工绑定：如果想编辑某一 DHCP 手工绑定条目，只需单击该条目的“ 用户名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”，修改完毕；
- 删除 DHCP 手工绑定：选中一些 DHCP 手工绑定条目，单击右下角的“ 删除 ”按钮，即可删除那些被选中的 DHCP 手工绑定条目。

7.6.4.7 自定义 DHCP 手工绑定

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 手工绑定配置 ”栏，选中“ 添加 ”选项，选择欲配置的 DHCP 手工绑定所属的 DHCP 地址池名；

第三步，填写“ 用户名 ”、“ IP 地址 ”及“ MAC 地址 ”等信息；

第四步，根据需要，填写“ 客户端标识 ”、“ 远程标识 ”、“ 主机名 ”等信息；

第五步，单击“ 保存 ”按钮，当前 DHCP 手工绑定配置完成，可在“ DHCP 手工绑定信息列表 ”中看到添加的记录。

提示：如果要删除 DHCP 手工绑定，只需在“ DHCP 手工绑定信息列表 ”中选中要删除的 DHCP 手工绑定，单击“ 删除 ”按钮，即可删除被选中的 DHCP 手工绑定。

7.6.5 DHCP 中继

进入***高级配置—>DHCP*** 页面，选中“ DHCP 中继 ”选项，如下图所示，即可进入 DHCP 中继配置界面。

图 7-38 选择 DHCP 中继

7.6.5.1 DHCP 中继配置

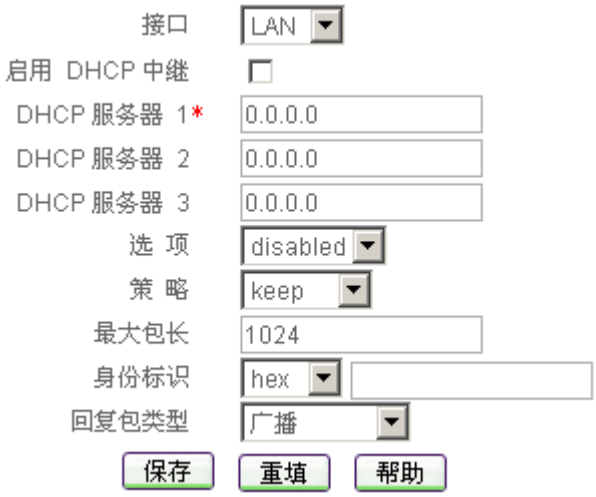


图 7-39 DHCP 中继配置界面

- 接口：指定启用 DHCP 中继功能的接口，可以是 LAN、WAN1 或 WAN2/DMZ 口；
- 启用 DHCP 中继：启用或禁用 DHCP 中继功能，选中代表启用；
- DHCP 服务器 1，2，3：DHCP 服务器的 IP 地址，从当前接口上收到的 DHCP 数据

包将发送到指定服务器。最多可以配置 3 个 DHCP 服务器；

- 选项：允许或禁用插入 DHCP 中继信息，disabled——禁用，insert——插入。该参数需和“策略”结合起来使用；
- 策略：接收到 DHCP 数据包后 DHCP 中继执行的策略，keep——保留，drop——丢弃，replace——替换。该参数需和“选项”结合起来使用；
- 最大包长：DHCP 中继转发的数据包的最大长度，缺省值为 1024。单位：字节；
- 身份标识：DHCP 中继的身份标识，有 hex，ascii，ip 三种表示方式。
  hex：定义一个十六进制字符串，取值范围：1～27 个字符；
  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；
  ip：定义一个 IP 地址，点分式十进制表示；
- 回复包类型：DHCP 中继接收到客户端发送的数据包后，发送回复包的方式。
  客户端决定：要求 DHCP 服务器按照 DHCP 客户端指定的方式发送回复包；
  单播：要求 DHCP 服务器按照单播方式发送回复包；
  广播：要求 DHCP 服务器按照广播方式发送回复包；
- 保存：DHCP 中继配置生效；
- 重填：恢复到修改前的配置参数。

7.6.5.2 DHCP 中继信息列表

DHCP中继信息列表 3/3

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

接口	状态	DHCP服务器1	DHCP服务器2	DHCP服务器3	选 项	策 略	最大包长	身份标识	回复包类型
LAN	禁用	0.0.0.0	0.0.0.0	0.0.0.0	禁用	保留	1024		广播
WAN	禁用	0.0.0.0	0.0.0.0	0.0.0.0	禁用	保留	1024		广播
DMZ	禁用	0.0.0.0	0.0.0.0	0.0.0.0	禁用	保留	1024		广播

表 7-26 DHCP 中继信息列表

- 配置 DHCP 中继：选择欲启用 DHCP 中继功能的“接口”，选中“启用 DHCP 中继”，输入其他相关配置信息，单击“保存”按钮，DHCP 中继配置完成；
- 浏览 DHCP 中继：如果已经启用了 DHCP 中继，可在“DHCP 中继信息列表”中查看相关配置信息；
- 编辑 DHCP 中继：如果需要编辑修改 DHCP 中继相关配置信息，直接单击该条目的“接口”超链接或进入原配置界面修改即可。

7.6.5.3 配置 DHCP 中继

第一步，进入***高级配置—>DHCP*** 页面，然后选中“DHCP 中继”，进入 DHCP 中继配置页面；

第二步，选择欲启用 DHCP 中继功能的“接口”；

第三步，选中“启用 DHCP 中继”；

第四步，填写“DHCP 服务器 1”，如有需要，填写“DHCP 服务器 2”及“DHCP 服务器 3”；

第五步，如有需要，需配置“选项”和“策略”等；

第六步，如有需要，需配置“ 最大包长 ”、“ 身份标识 ”、“ 回复包类型 ” 等信息；

第七步，单击“ 保存 ” 按钮，指定接口的 DHCP 中继功能配置完成，可在“ DHCP 中继信息列表 ” 中查看相关信息。

提示：如果要禁用某接口的 DHCP 中继功能，请取消指定接口“ 启用 DHCP 中继 ” 的选中，单击“ 保存 ” 按钮。

7.6.6 Raw Option

进入***高级配置—>DHCP*** 页面，选中“ 自定义选项（raw option）” 选项，如下图所示，即可进入 DHCP Raw Option 界面。

图 7-40 选择自定义选项

7.6.6.1 Raw Option 配置

图 7-41 自定义选项配置

- 选项名：该 Raw Option 的名称。自定义，不能重复，取值范围：1～31 个字符；
- 类型值：该 Raw Option 的类型，用数字表示，取值范围：1～254；
- 数据：该 Raw Option 的值，有 hex，ascii，ip 三种表示方式。
  hex：定义一个十六进制字符串，取值范围：1～27 个字符；
  ascii：定义一个 ASCII 字符串，取值范围：1～25 个字符；
  ip：定义一个 IP 地址，点分式十进制表示；
- 接口：可使用该 Raw Option 的接口，可以是 LAN、WAN1 或 WAN2/DMZ 口；
- 保存：Raw Option 配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：有关 option 的类型请参考 RFC 1533、RFC2131、RFC2132 等相关文档；

7.6.6.2 Raw Option 信息列表

表 7-27 Raw Option 信息列表

- 增加 Raw Option：选中“ 添加 ”选项，输入相关配置信息，单击“ 保存 ”按钮，生成 Raw Option；
- 浏览 Raw Option：如果已经生成了 Raw Option，可在“ Raw Option 管理列表 ”中查看相关配置信息；
- 编辑 Raw Option：如果想编辑某个 Raw Option 条目，只需单击该条目的“ 选项名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，然后修改它，再单击“ 保存 ”，修改完毕；
- 删除 Raw Option：选中一些 Raw Option 条目，单击右下角的“ 删除 ”按钮，即可删除那些被选中的 Raw Option 条目。

7.6.6.3 自定义 Raw Option

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ 自定义选项（raw option）”，进入 DHCP Raw Option 配置页面；

第二步，在“ Raw Option 配置 ”栏，选中“ 添加 ”；

第三步，填写“ 选项名 ”、“ 类型值 ”及“ 数据 ”等信息；

第四步，根据需要，选择能使用当前 Raw Option 的接口；

第五步，单击“ 保存 ”按钮，当前 Raw Option 配置完成，可在“ Raw Optioon 信息列表 ”中看到添加的记录。

提示：如果要删除 Raw Option，在“ Raw Optioon 信息列表 ”中选中要删除的 Raw Option，单击“ 删除 ”按钮，即可删除被选中的 Raw Option。

7.6.7 DHCP 典型配置实例

7.6.7.1 DHCP 服务器典型配置实例

常见的 DHCP 组网方式可分为两类：一种是 DHCP 服务器和 DHCP 客户端都在一个子网内，直接进行 DHCP 协议的交互；另外一种是 DHCP 服务器和 DHCP 客户端分别处于不同的子网中，必须通过 DHCP 中继代理实现 IP 地址的分配。无论哪种情况下，DHCP 的配置都是相同的。

1. 组网需求

DHCP 服务器为同一网段中的客户端动态分配 IP 地址，DHCP 服务器（设备）LAN 口地址为 192.168.16.1/24，欲配置两个地址池（地址池名分别为 pool1、pool2），它们均绑定在 LAN 口，pool1 的地址范围为：192.168.16.2/24～192.168.16.101/24，pool2 的地址范围为：192.168.16.102/24～192.168.16.254/24。

两个地址池的主 DNS 服务器的 IP 地址均为 202.96.209.5、备 DNS 服务器的 IP 地址均为 202.96.199.133，无 WINS 服务器；域名均为 utt.com.cn；出口网关地址均为设备的 LAN 口地址；pool1 的租用时间为 3600 秒，pool2 的租用时间为 7200 秒。

另外局域网中某主机要求使用固定 IP 地址，因此需为它配置 DHCP 手工绑定。其用户名为 binding1，预分配的 IP 地址为 192.168.16.10/24，MAC 地址为 000795a81c3d，主机名为 wgw，客户端标识使用“类型＋MAC 地址”方式，即采用 hex 表示方式，值为 01000795a81c3d。显然，该 DHCP 手工绑定需绑定到 pool1。

2. 组网图

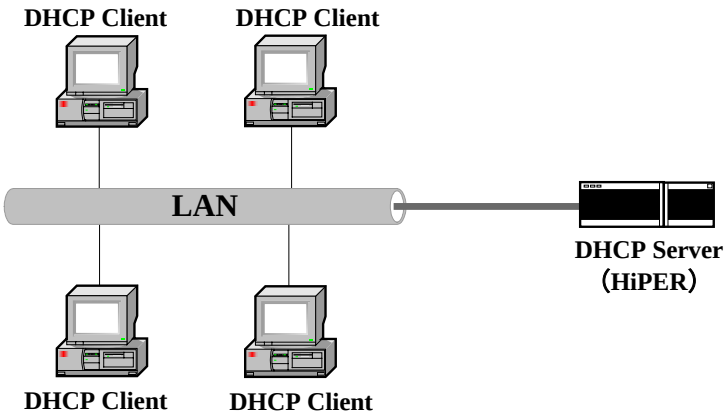


图 7-42 DHCP 服务器与 DHCP 客户端在同一网络

3. 配置步骤

1） DHCP 全局配置

第一步，进入***高级配置—>DHCP*** 页面，然后选中“DHCP 服务器”，进入 DHCP 服务器配置页面；

第二步，在“DHCP 服务器全局配置”栏，选中“启用 DHCP 服务器”选项，如下图所示；

图 7-43 DHCP 服务器全局配置——实例

第三步，单击“保存”按钮，DHCP 全局配置完成。

2） 配置 DHCP 地址池“pool1”

由于系统缺省地址池名为“pool1”，因此，只需修改“pool1”相关信息即可。由于“pool1”

不能删除，地址池不能同名，也只能通过修改“ pool1 ”来配置所需地址池。

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 地址信息列表 ”中单击“ 地址池名 ”为“ pool1 ”条目后的“ 编辑 ”超链接，即进入如图 7-44 所示 DHCP 地址池配置界面；

图 7-44 DHCP 地址池配置——实例 pool1

第三步，在“ 起始地址 ”中填入“ 192.168.16.2 ”，在“ 总地址数 ”中填入“ 100 ”，在“ 主 DNS 服务器 ”中填入“ 202.96.209.6 ”，在“ 备 DNS 服务器 ”中填入“ 202.96.199.133 ”，在“ 域名 ”中填入“ utt.com.cn ”。其余未填参数为系统缺省值。特别需要注意的是，“ 网关地址 ”为“ 0.0.0.0 ”，表示默认使用设备当前 LAN 口地址；

第四步，单击“ 保存 ”按钮，地址池“ pool1 ”配置完成，可在“ DHCP 地址池信息列表 ”中可查看到相应的记录。

3） 配置 DHCP 地址池“ pool2 ”

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 地址池配置 ”栏，选中“ 添加 ”选项，如下图所示；

图 7-45 DHCP 地址池配置——实例 pool2

第三步，在“ 起始地址 ”中填入“ 192.168.16.102 ”，在“ 总地址数 ”中填入“ 153 ”，在“ 主 DNS 服务器 ”中填入“ 202.96.209.6 ”，在“ 备 DNS 服务器 ”中填入“ 202.96.199.133 ”，在“ 网关地址 ”中填入“ 192.168.16.1 ”，在“ 租用时间中 ”填入“ 7200 ”，在“ 域名 ”中填入“ utt.com.cn ”。其余未填参数为系统缺省值。

第四步，单击“ 保存 ”按钮，地址池“ pool2 ”配置完成，可在“ DHCP 地址池信息列表 ”中可查看到相应的记录。

4） 配置 DHCP 手工绑定

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 手工绑定配置 ”栏，选中“ 添加 ”选项，如下图所示；

图 7-46 DHCP 手工绑定配置

第三步，“ 绑定 ”选择为 “ pool1 ”，在 “ 用户名 ”中填入 “ binding1 ”，在 “ IP 地址 ”中填入 “ 192.168.16.10 ”，在 “ MAC 地址 ”中填入 “ 000795a81c3d ”，在 “ 主机名 ”中填入 “ ly ”；

第四步，“ 客户端标识 ”表示方式选择为 “ hex ”，并填入 “ 01000795a81c3d ”；

第五步，单击 “ 保存 ”按钮，该 DHCP 手工绑定配置完成，可在 “ DHCP 手工绑定信息列表 ”中查看到相应的记录。

7.6.7.2 DHCP 客户端典型配置实例

设备的 LAN 口、WAN 口及 DMZ/WAN2 口均可启用 DHCP 客户端功能，这里以 WAN 口启用 DHCP 客户端为例进行说明。

1. 组网需求

设备的 WAN 口接入 LAN 中，在该 LAN 中有一个 DHCP 服务器。LAN 所在网段为 200.200.200.0/24，要求配置设备的 WAN 口通过 DHCP 的方式获取地址。并使用 “ 类型＋MAC ”地址作为客户端标识，为 “ 01000695a81d4c ”。

2. 组网图

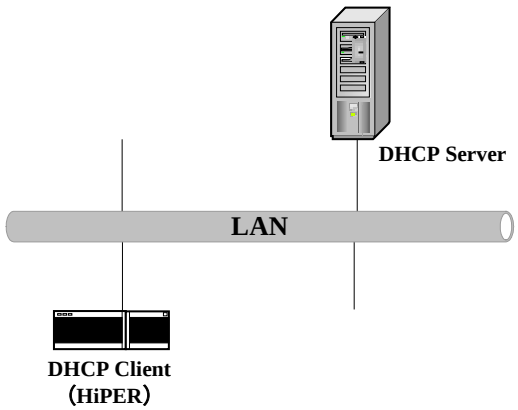


图 7-47 设备的 WAN 口作为 DHCP 客户端

3. 配置步骤

第一步，进入***高级配置—>DHCP*** 页面，然后选中 “ DHCP 客户端 ”，进入 DHCP 客户端配置页面，如下图所示；

图 7-48 DHCP 客户端配置——实例

第二步，“ 接口 ” 选择为 “ WAN ”；

第三步，选中 “ 启用 DHCP 客户端 ”，选中 “ 启用 PnP ”，选中 “ 允许 AutoIP ”；

第四步，“ 客户端标识 ” 表示方式选择为 “ hex ”，并填入 “ 01000695a81d4c ”；

第五步，单击 “ 保存 ” 按钮，当前 DHCP 客户端功能配置完成，可在 “ DHCP 客户端信息列表 ” 中查看相关信息。

7.6.7.3 DHCP 中继典型配置实例

1. 组网需求

DHCP 客户端所在的网段为 192.168.16.0/24，而 DHCP 服务器所在的网段为 200.200.200.0/24。需要通过带 DHCP 中继功能的设备中继 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。设备的 LAN 口启用 DHCP 中继功能，DHCP 客户端都连到设备的 LAN 口上。

DHCP 服务器应当分配一个 192.168.16.0/24 网段的 IP 地址池，以便将适当的 IP 地址分配给该网段上的 DHCP 客户端，并且 DHCP 服务器上应当配置到 192.168.16.0/24 网段的路由。

2. 组网图

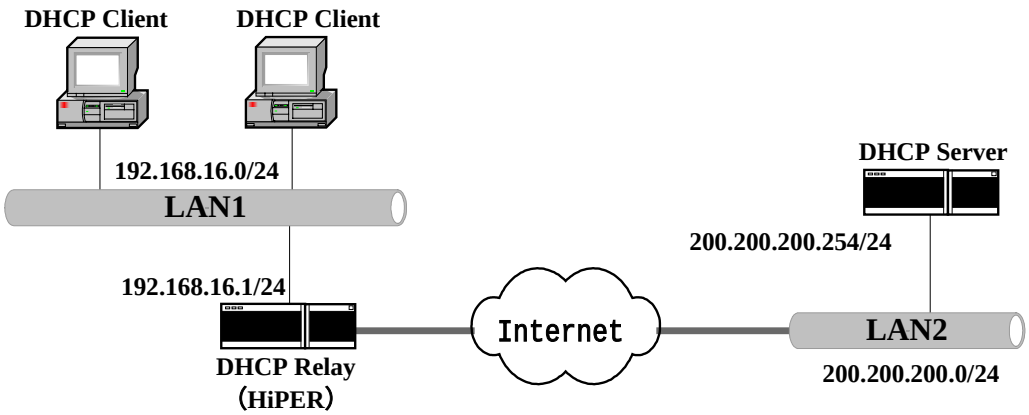


图 7-49 DHCP 中继的典型组网应用

3. 配置步骤

第一步，进入***高级配置—>DHCP*** 页面，然后选中 “ DHCP 中继 ”，进入 DHCP 中继配置页面，如下图所示；

图 7-50 DHCP 中继配置——实例

第二步，“ 接口 ”选择“ LAN ”；

第三步，选中“ 启用 DHCP 中继 ”；

第四步，在“ DHCP 服务器 1 ”中填入“ 200.200.200.254 ”。其余未填参数为系统缺省值。

第五步，单击“ 保存 ”按钮，当前 DHCP 中继功能配置完成，可在“ DHCP 中继信息列表 ”中查看相关信息。

7.6.7.4 Raw Option 典型配置实例

1. 需求

增加一个自定义选项：其名称为 ven_inf；类型为 option 43——vendor-specific information，即厂商专用信息；内容为设备，ASCII 码表示方式；作用于 LAN 口。

2. 配置步骤

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ 自定义选项（raw option）”，进入 DHCP Raw Option 配置页面，如下图所示。

图 7-51 Raw Option 配置——实例

第二步，选中“ 添加 ”选项；

第三步，在“ 选项名 ”中填入“ ven_inf ”，在“ 类型值 ”中填入“ 43 ”，“ 数据 ”选择“ ascii ”，并填入“ 设备 ”；

第四步，接口选择“ LAN ”；

第五步，单击“ 保存 ”按钮，当前 Raw Option 配置完成，可在“ Raw Optioon 信息列表 ”中看到添加的记录。

7.6.7.5 综合应用实例

设备的 DHCP 服务器支持配置多个 DHCP 地址池（最多 10 个），每个地址池可使用不同的中继地址或中继标识来区分。通常情况下，具有匹配的中继标识或中继地址的客户端将获得对应地址池中的 IP 地址，从而，中继标识或中继地址相同的客户端将处于同一个子网中。

1. 组网需求

某学校为实现对校园网上网主机的统一管理，要求按大楼（办公楼或宿舍楼）来划分子网，这样，同一个大楼中的主机位于同一个子网。现在，该学校在网络中心放置一台设备作为 DHCP Server。各大楼通过一台设备接入网络中心，这些设备将启用 Relay 功能。

如图 7-52 所示，在这里将 10 个需要上网业务的大楼分别记为大楼 1、大楼 2、……、大楼 10，各大楼的接入网络中心所使用的设备分别记为 DHCP Relay1、DHCP Relay2、……、DHCP Relay10，它们各自具有自己的身份标识。

网络中心的设备在 LAN 口启用 DHCP Server 功能，IP 地址：200.200.200.254/24；

各大楼的设备通过 WAN 口连接到网络中心的设备的 LAN 口，它们均在 LAN 口启用 DHCP Relay 功能，各大楼的主机均接到其设备的 LAN 口，将作为 DHCP 客户端向 DHCP Server 申请 IP 地址。它们的中继标识（ASCII 格式）、LAN 口和 WAN 口的 IP 地址，以及各大楼的客户端所在子网的 IP 地址如表 7-28 所示。

名称	WAN 口 IP	LAN 口 IP	客户端子网	中继标识(ascii)
DHCP Relay1	200.200.200.1/24	192.168.1.1/24	192.168.1.0/24	设备_Relay1
DHCP Relay2	200.200.200.2/24	192.168.2.1/24	192.168.2.0/24	设备_Relay2
DHCP Relay3	200.200.200.3/24	192.168.3.1/24	192.168.3.0/24	设备_Relay3
DHCP Relay4	200.200.200.4/24	192.168.4.1/24	192.168.4.0/24	设备_Relay4
DHCP Relay5	200.200.200.5/24	192.168.5.1/24	192.168.5.0/24	设备_Relay5
DHCP Relay6	200.200.200.6/24	192.168.6.1/24	192.168.6.0/24	设备_Relay6
DHCP Relay7	200.200.200.7/24	192.168.7.1/24	192.168.7.0/24	设备_Relay7
DHCP Relay8	200.200.200.8/24	192.168.8.1/24	192.168.8.0/24	设备_Relay8
DHCP Relay9	200.200.200.9/24	192.168.9.1/24	192.168.9.0/24	设备_Relay9
DHCP Relay10	200.200.200.10/24	192.168.10.1/24	192.168.10.0/24	设备_Relay10

表 7-28 DHCP 中继的接口地址——综合实例

对于 DHCP Server 来说，为保证每个大楼的主机获得上述指定子网中的 IP 地址，在 DHCP 服务器需配置 10 个地址池，它们的配置如下：

均绑定在 LAN 口；

“地址池名”分别为 pool1、pool2、……、pool10；

“起始地址”分别为 192.168.x.2（x 为 1、2、……、10）；

“总地址数”均为各客户端子网允许的最大合法 IP 地址数，即 253；

“租用时间”均为 3600 秒；

“主 DNS 服务器”均为 202.96.209.6，“备 DNS 服务器” 均为“202.96.199.133”；

“DHCP 中继标识”的表示方式均为“ascii”，值分别为各大楼设备的 DHCP Relay 的中继标识。

另外，在 DHCP Server 中，还需配置到各个客户端子网的静态路由。

对于 DHCP Relay 来说，配置如下：

均在 LAN 口启用；

“DHCP 服务器 1”均为 200.200.200.254；

“选项”均设为“insert”；

“身份标识”的表示方式均为“ascii”，值分别为各自的中继标识。

提示：由于 DHCP 服务器是采用中继标识来区分各个地址池的，因此需将 DHCP 中继中的“选项”设为“insert”，这样，DHCP 中继在接收到 PC 机发出的数据包时，才会先将数据包加上中继标识之后再转发，DHCP 服务器才能根据中继标识选择匹配的地址池为客户端分配地址。

2. 组网图

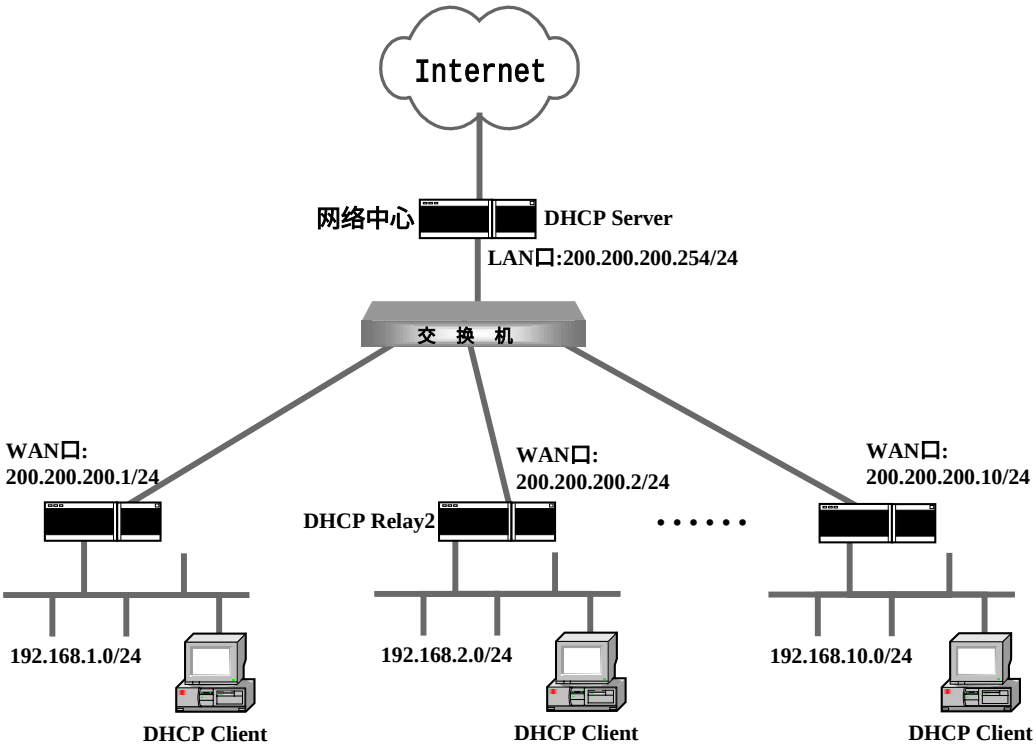


图 7-52 DHCP 综合应用组网图

3. 配置步骤

由于 DHCP Server 中，各个地址池的配置类似；各 DHCP Relay 的配置也类似；因此，在这里，仅以 DHCP 地址池 pool1、DHCP Relay1 的配置为例进行说明。

1) DHCP 服务器配置

a) DHCP 全局配置

第一步，进入***高级配置—>DHCP*** 页面，然后选中“DHCP 服务器”，进入 DHCP 服务器配置页面；

第二步，在“ DHCP 服务器全局配置 ”栏，选中“ 启用 DHCP 服务器 ”选项，如下图所示；

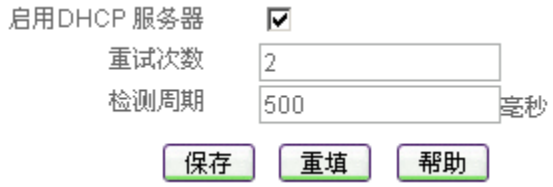


图 7-53 DHCP 服务器全局配置——综合实例

第三步，单击“ 保存 ”按钮，DHCP 全局配置完成。

b) 配置 DHCP 地址池“ pool1 ”

由于系统缺省地址池名为“ pool1 ”，因此，只需修改“ pool1 ”相关信息即可。由于“ pool1 ”不能删除，地址池不能同名，也只能通过修改“ pool1 ”来配置所需地址池。

第一步，进入***高级配置—>DHCP*** 页面，然后选中“ DHCP 服务器 ”，进入 DHCP 服务器配置页面，在“ DHCP 地址池信息列表 ”中，单击“ 地址池名 ”为“ pool1 ”的条目后的“ 编辑 ”超链接，即进入如图 7-54 所示 DHCP 地址池配置界面。

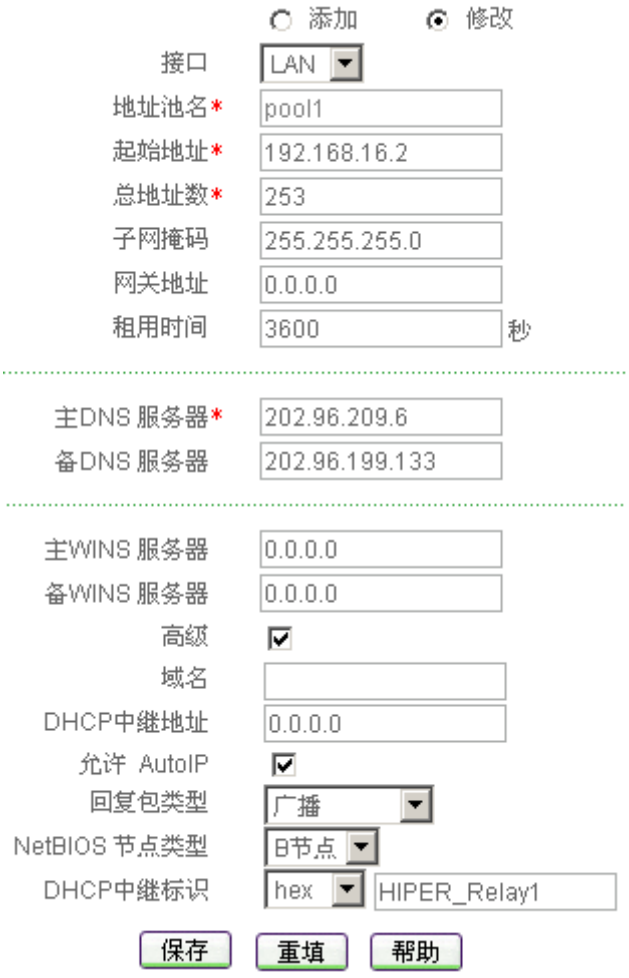


图 7-54 DHCP 地址池配置——综合实例 pool1

第三步，在“ 起始地址 ”中填入“ 192.168.1.2 ”，在“ 总地址数 ”中填入“ 253 ”，在“ 主 DNS 服务器 ”中填入“ 202.96.209.6 ”，在“ 备 DNS 服务器 ”中填入“ 202.96.199.133 ”，“ DHCP

中继标识 ” 选择 “ ascii ”，并输入 “ 设备_Relay1 ”。其余未填参数为系统缺省值。特别需要注意的是，“ 网关地址 ” 为 “ 0.0.0.0 ”，表示默认使用设备当前 LAN 口地址；

第四步，单击 “ 保存 ” 按钮，地址池 “ pool1 ” 配置完成，可在 “ DHCP 地址池信息列表 ” 中可查看到相应的记录。

2) DHCP Relay1 配置

第一步，进入***高级配置—>DHCP*** 页面，然后选中 “ DHCP 中继 ”，进入 DHCP 中继配置页面，如图 7-55 所示；

图 7-55 DHCP 中继配置——综合实例 DHCP Relay

第二步，“ 接口 ” 选择 “ LAN ”；

第三步，选中 “ 启用 DHCP 中继 ”；

第四步，在 “ DHCP 服务器 1 ” 中填入 “ 200.200.200.254 ”；“ 选项 ” 选择 “ insert ”；“ 身份标识 ” 选择 “ ascii ”，并输入 “ 设备_Relay1 ”，其余未填参数为系统缺省值。

第五步，单击 “ 保存 ” 按钮，当前 DHCP 中继功能配置完成，可在 “ DHCP 中继信息列表 ” 中查看相关信息。

提示：其余 DHCP Relay 的配置类似，仅参数 “ 身份标识 ” 各不相同，具体步骤略，请参考 DHCP Relay1 的配置步骤。

7.7 UPnP 配置

UPnP（Universal Plug and Play，通用即插即用）主要用于实现设备的智能互联互通，旨在实现一种“零”配置和“隐性”的联网过程，自动发现和控制来自各家厂商的各种网络设备。

在设备上启用 UPnP 功能后，可以实现穿透 NAT：当局域网的主机通过设备与 Internet 上的终端进行通讯时，可以根据需要自动增加、删除 NAT 映射，从而保证支持 UPnP 的软件可以在 NAT 后正常使用。

通过 UPnP NAT 映射列表，可以查看经 UPnP 建立的 NAT 静态映射的相关信息，包括：内部地址、内部端口、协议、对端地址、外部端口以及信息描述。

7.7.1 启用 UPnP

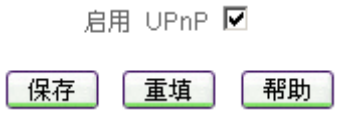


图 7-56 UPnP 配置

- 启用 UPnP：启用或者禁用 UPnP 功能，选中为启用。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：WEB UI 中，仅支持在 LAN 口启用 UPnP 功能。

7.7.2 UPnP NAT 映射列表

表 7-29 UPnP NAT 映射列表

表 7-30 UPnP NAT 映射列表（续表 7-29）

- 序号：该 UPnP NAT 映射的序号；
- 内部地址：局域网主机的 IP 地址；
- 内部端口：局域网主机提供的服务端口；
- 协议：该 UPnP NAT 映射使用的协议；
- 对端地址：对端主机的 IP 地址；
- 外部端口：内部端口经 NAT 转换后的端口，即设备提供给 Internet 的服务端口；
- 描述：用来描述相关 UPnP 设备厂家的信息。
- 刷新：选中“ 刷新 ”按钮，即可查看最新的 UPnP NAT 映射信息；
- 删除：选中一些 UPnP NAT 映射，单击右下角的“ 删除 ”按钮，即可删除那些被选中的 UPnP NAT 映射。

第8章 系统状态

系统状态里面记载了设备中运行的大量状态信息，通过查看、分析这些运行信息，对于管理员分析系统的状况、监视设备的活动来说，是一个相当重要的部分。

设备在 NAT 的环境下，提供强大的监控功能，主要分为两类：一类是分类统计，可以帮助管理员发现过去网络运行中出现过的问题；另一类是在线监控，可以帮助管理员分析目前网络运行中哪个主机出现了问题，出现了何种问题，以及对其他主机造成的影响。

设备的运行状态管理分为三个层次：

物理状态：各接口物理状态信息以及收发数据包信息，路由表信息等；

用户状态：每一个局域网用户的信息，包括收发包信息、带宽占用情况等；

NAT 状态：针对 NAT 的特别信息，帮助管理员发现用户在使用 Internet 过程中发生的 DDoS 攻击，巨量下载，过分占用 Internet 带宽等情况。

8.1 用户统计

本节主要讲述***系统状态***—>***用户统计***的使用。

用户统计信息列表 27/27

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	用户名	IP地址	MAC地址	活动记录	广播包 / 发送包	发送数据包	发送广播包
8		192.168.16.13	00:e0:4c:7a:14:2c	0:00:00:41	0%	0	40
27		192.168.16.87	00:0c:76:de:b8:2c	0:00:03:47	0%	24	745
4		200.200.200.15	00:14:85:d4:f0:01	0:00:02:46	0%	78	81
26		200.200.200.24	00:22:aa:3e:9e:71	0:00:00:29	0%	2479	0
16	200.200.200.33	200.200.200.33	00:03:0d:19:ca:5f	0:00:00:32	1%	13807	117
23		200.200.200.87	00:0c:76:de:b8:2c	0:00:00:01	0%	6895	6
3		200.200.200.89	00:22:aa:4d:d2:83	0:00:33:00	0%	0	1
6		200.200.200.131	00:e0:4c:7a:14:2c	0:00:02:02	0%	0	3
9		200.200.200.136	00:e0:4c:19:03:2e	0:00:00:16	3%	6071	211
12		200.200.200.137	00:e0:4c:19:03:2d	0:00:00:01	0%	7203	72
19		200.200.200.150	00:00:e8:00:05:05	0:00:00:42	0%	2	0
17	200.200.200.172	200.200.200.172	00:14:2a:67:fd:b4	0:00:00:16	3%	5830	188
24		200.200.200.174	00:e0:4c:40:76:ef	0:00:00:51	20%	699	139
21		200.200.200.182	00:22:aa:5b:e6:25	0:00:00:01	0%	41048	0
7		200.200.200.205	00:15:c5:67:41:0f	0:00:00:01	0%	8664	23
13		200.200.200.207	00:05:5d:33:56:1d	0:00:00:32	0%	730	1
18		200.200.200.208	00:14:85:d6:97:45	0:00:00:38	0%	1760	51
20		200.200.200.216	00:17:31:a6:b3:ad	0:00:04:14	0%	0	12
22		200.200.200.219	00:22:aa:3e:9f:32	0:00:00:01	0%	3783	0
11		200.200.200.223	00:16:e6:51:e7:95	0:00:00:05	0%	0	35

清除 刷新

表 8-1 用户统计信息列表

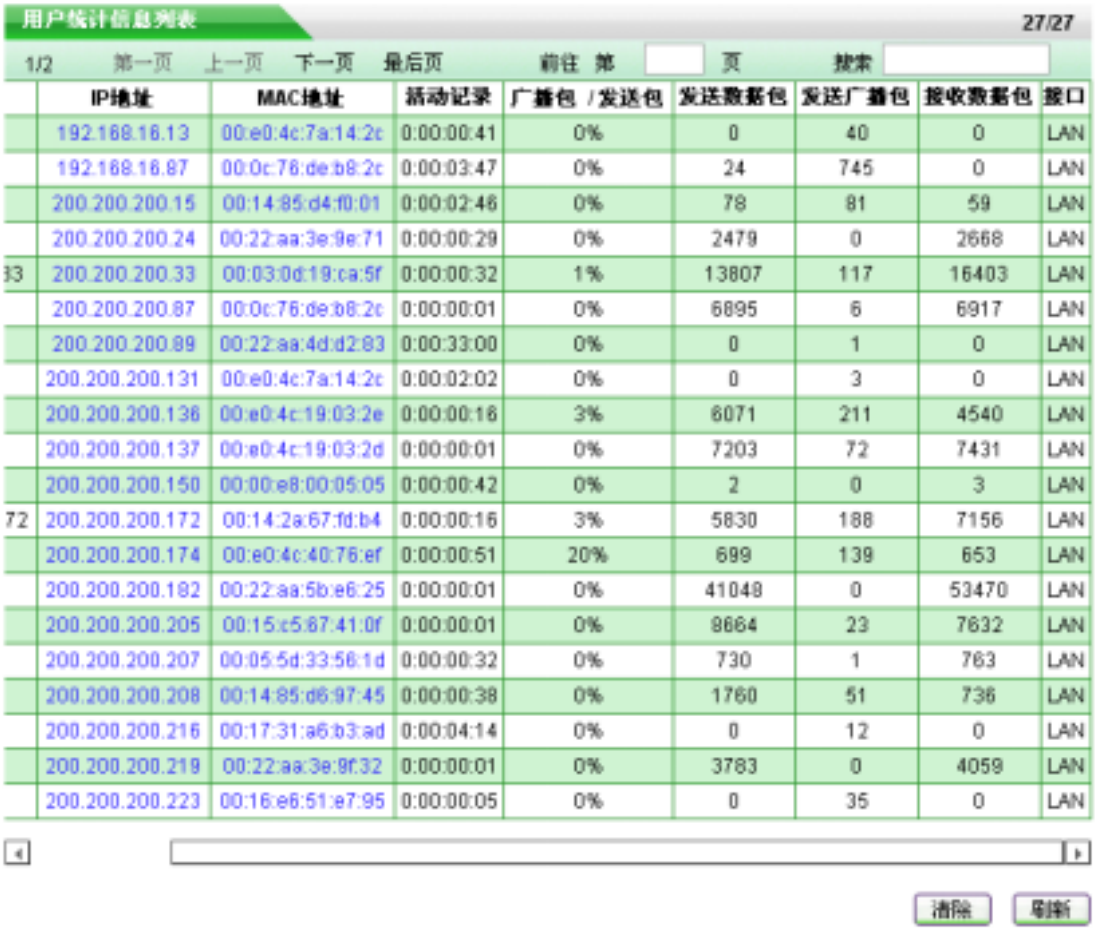


表 8-2 用户统计信息列表（续表 8-1）

- ID：序号；
- 用户名：如果是 IP/MAC 绑定用户，则显示为对应的“ 用户名 ”；否则显示为空。注意，可以在***高级配置—>IP/MAC 绑定***或者***安全配置—>用户管理—>用户信息配置***中配置 IP/MAC 绑定；
- IP 地址：某用户的 IP 地址信息；
- MAC 地址：某用户的 MAC 地址信息；
- 活动记录：某用户上一次与设备通信距离查询时刻的时间；
- 广播包/发送包：某用户向设备发送的广播包（包括多播包）和单播包的数量比；
- 发送数据包：某用户向设备发送的单播包的数量，一般是该用户上网时向 Internet 发送的数据包；
- 发送广播包：某用户向设备发送的广播包（包括多播包）的数量；
- 接收数据包：某用户从设备接收的单播包的数量，一般是该用户上网时从 Internet 下载的数据包；
- 接口：某用户与设备相连的接口。
- 清除：单击“ 清除 ”按钮，可将“ 用户统计信息列表 ”全部信息清除，配合“ 刷新 ”按钮，可查看清除时刻至今这段时间内的用户统计信息。
- 刷新：单击“ 刷新 ”按钮，可以看到“ 用户统计信息列表 ”的最新信息。

提示：

1. 发现内网流量最大的用户：上表中发送数据包或者广播包一列中数量最大的用户；
2. 一般来说，计算机在开机的时候会发送一些广播包，某些软件在运行的时候也会发

送一些广播包，计算机运行一段时间后（一般是开机运行 20 分钟后或上网 10 分钟后，开始考量这个数值），其发送广播包的数量应该小于单播包数量的 10%，如果比例远大于 10%，该计算机可能感染了病毒；

3. 某些软件（如网吧计费管理软件）在使用的时候会发送大量的广播包，这时“广播包/发送包”将远大于 10%，此时应该忽略这种异常情况；

4. “用户统计信息列表”中 IP 地址为 0.0.0.0 的用户是一些只发送广播包而没有和设备通讯过的网络设备，设备只能识别出它们的 MAC 地址，而不能识别 IP 地址。这些网络设备可能来自局域网，也可能来自广域网（ISP 采用 LAN 形式为用户提供接入线路），当它们发送的广播包过高时，会造成设备的接口的拥塞，网速变慢。

8.2 NAT 统计

本节主要讲述***系统状态—>NAT 统计***的使用，本页面包括“ NAT 状态信息列表 ”（如表 8-3）和“ NAT 统计信息列表 ”（如表 8-4、8-5）。

提示：如果在***系统管理—>WEB 服务器***中启用了自动刷新功能，本页面将按照“ 刷新时间间隔 ”设置的时间定期自动刷新。

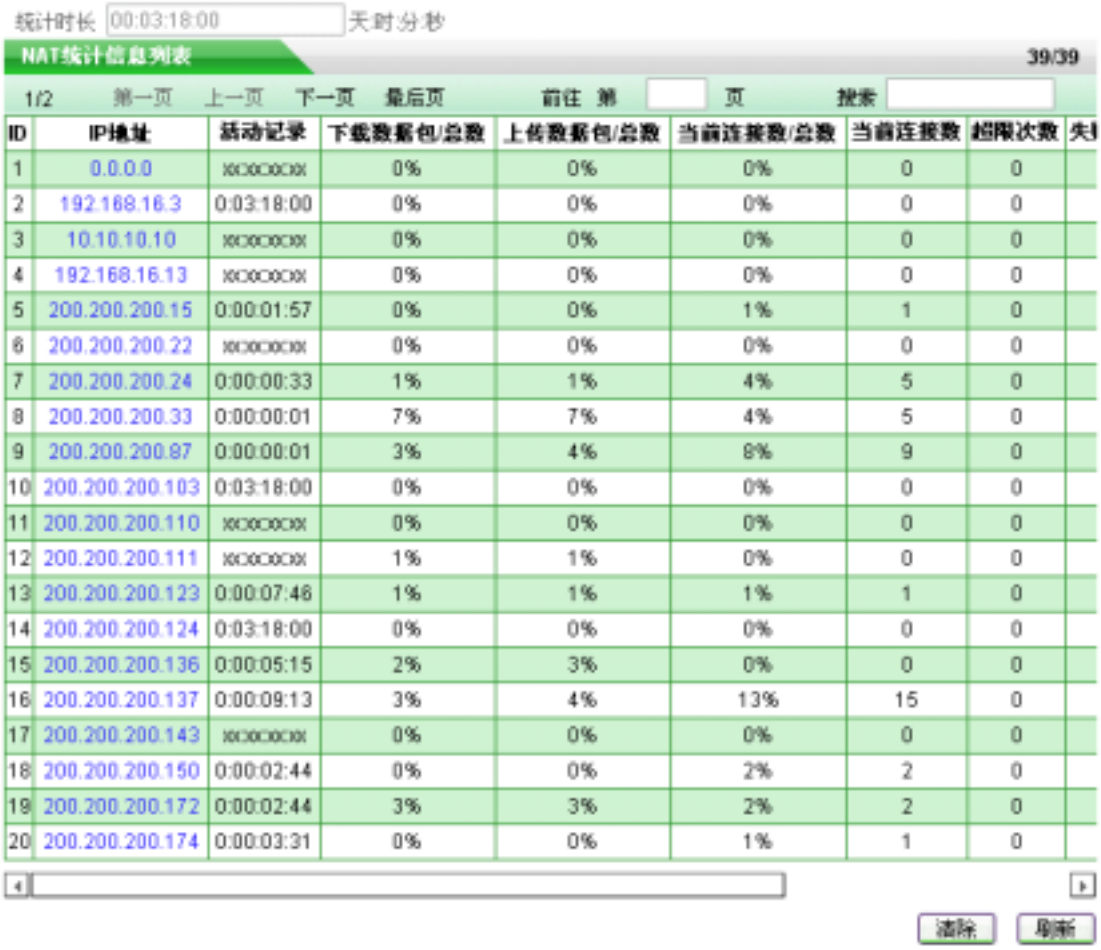
8.2.1 NAT 状态信息列表

表 8-3 NAT 状态信息列表

- ID：序号；
- 起始 IP、结束 IP：该 NAT 规则设置的起始 IP 地址和结束 IP 地址；
- 外部 IP：该 NAT 规则对应的外部 IP 地址；
- 类型：该 NAT 规则的类型，可以是 EasyIP、One2One 或 Passthrough；
- 虚拟服务器：该 NAT 规则设置的虚拟服务器，它通过该 NAT 规则上网；
- 接口 :该 NAT 规则所绑定线路的接口名称，可以是物理接口 ie0-LAN 口、ie1-WAN1 口、ie2-WAN2/DMZ、ie3-WAN3、ie4-WAN4；或者是拨号虚接口 ptpx-虚接口 x、ptpdial0-待拨虚接口；
- 权重：该 NAT 规则的权重值；
- 选择计数：在“ 租期 ”这段时间内，使用该 NAT 规则的 NAT 会话的累计数量。如果该 NAT 规则未生效或未被使用，则该值为 0；
- 租期：该 NAT 规则上一次状态变化距离查询时刻的时间。
- 刷新：单击“ 刷新 ”按钮，可以看到最新的“ NAT 状态信息列表 ”。

提示：同***高级配置—>NAT 和 DMZ 配置***中的“ NAT 规则信息列表 ”相比，在这里将“ One2One ”类型的 NAT 规则进行了细分，一个外部地址对应一条记录。

8.2.2 NAT 统计信息列表


统计时长 00:03:18:00 天:时:分:秒

NAT统计信息列表 39/39

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	IP地址	活动记录	下载数据包/总数	上传数据包/总数	当前连接数/总数	当前连接数	超限次数	失
1	0.0.0.0	xxxxxxxx	0%	0%	0%	0	0	
2	192.168.16.3	0:03:18:00	0%	0%	0%	0	0	
3	10.10.10.10	xxxxxxxx	0%	0%	0%	0	0	
4	192.168.16.13	xxxxxxxx	0%	0%	0%	0	0	
5	200.200.200.15	0:00:01:57	0%	0%	1%	1	0	
6	200.200.200.22	xxxxxxxx	0%	0%	0%	0	0	
7	200.200.200.24	0:00:00:33	1%	1%	4%	5	0	
8	200.200.200.33	0:00:00:01	7%	7%	4%	5	0	
9	200.200.200.87	0:00:00:01	3%	4%	8%	9	0	
10	200.200.200.103	0:03:18:00	0%	0%	0%	0	0	
11	200.200.200.110	xxxxxxxx	0%	0%	0%	0	0	
12	200.200.200.111	xxxxxxxx	1%	1%	0%	0	0	
13	200.200.200.123	0:00:07:46	1%	1%	1%	1	0	
14	200.200.200.124	0:03:18:00	0%	0%	0%	0	0	
15	200.200.200.136	0:00:05:15	2%	3%	0%	0	0	
16	200.200.200.137	0:00:09:13	3%	4%	13%	15	0	
17	200.200.200.143	xxxxxxxx	0%	0%	0%	0	0	
18	200.200.200.150	0:00:02:44	0%	0%	2%	2	0	
19	200.200.200.172	0:00:02:44	3%	3%	2%	2	0	
20	200.200.200.174	0:00:03:31	0%	0%	1%	1	0	

清除 刷新

表 8-4 NAT 统计信息列表

表 8-5 NAT 统计信息列表（续表 8-4）

- 统计时长：上一次清除至查询时刻的时间间隔，单位：天:时:分:秒；
- ID：序号；
- IP 地址：某用户的 IP 地址。单击某用户的“ IP 地址 ”，立即跳转到***上网监控***页面，自动查询该用户的全部 NAT 会话记录（即查询“ 内网地址 ”为当前“ IP 地址 ”的全部会话记录），并在“ 查询结果列表 ”中显示查询结果；
- 活动记录：某用户上一次使用 NAT 至查询时刻的时间；
- 下载数据包/总数：“ 统计时长 ”内，某用户下载的数据包在整个局域网用户下载数据包总数中所占的百分比；
- 上传数据包/总数：“ 统计时长 ”内，某用户上传的数据包在整个局域网用户上传数据包总数中所占的百分比；
- 当前连接数/总数：某用户的实时 NAT 会话数在设备当前 NAT 会话总数中所占的百分比；
- 当前连接数：某用户正在使用的 NAT 会话的数量；
- 超限次数：“ 统计时长 ”内，某用户 NAT 请求超过设备内部限制的数量，用户最大 NAT 会话数在***高级配置—>NAT 和 DMZ 配置***的“ NAT 全局配置 ”中配置；
- 失败次数：“ 统计时长 ”内，某用户 NAT 请求失败的数量；
- 下载数据包：“ 统计时长 ”内，某用户做 NAT 下载数据包的数量；
- 上传数据包：“ 统计时长 ”内，某用户做 NAT 上传数据包的数量；
- 总连接数：“ 统计时长 ”内，某用户使用的 NAT 会话的总数量。

- 清除：单击“ 清除 ”按钮，可清除“ NAT 统计信息列表 ”中的大部分信息，包括“ 下载数据包/总数 ”、“ 上传数据包/总数 ”、“ 超限次数 ”、“ 失败次数 ”、“ 下载数据包 ”、“ 上传数据包 ”、“ 总连接数 ”。配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的 NAT 统计信息。
- 刷新：单击“ 刷新 ”按钮，可以看到最新的“ NAT 统计信息列表 ”。

提示：

1. 设备的防攻击功能会限制用户 NAT 会话的总数量，当某用户 NAT 请求超过最大 NAT Session 数时，超过的连接将会被丢弃，并在“ 超限次数 ”中增加记录；同时通过查看 Syslog 服务的日志记录，可帮助管理员发现可能的 DDoS 攻击；
2. 当系统资源不足（可能由于系统繁忙，或是遭受攻击引起）时，将会导致用户请求 NAT 失败，并在“ 失败次数 ”中增加记录；
3. 查询“ 统计时长 ”内，从 Internet 下载数据包最多的用户：即上表中“ 下载数据包/总数 ”数值最大的用户；
4. 查询“ 统计时长 ”内，向 Internet 上传数据包最多的用户：即上表中“ 上传数据包/总数 ”数值最大的用户；
5. 查询目前上网最活跃的用户：“ 当前连接数/总数 ”数值最大的用户；
6. 查询“ 统计时长 ”内，可能使用端口扫描软件的用户：“ 超限次数 ”大于 100，或是“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量；
7. 查询“ 统计时长 ”内，可能使用 DoS/DDoS 攻击设备的用户：“ 上传数据包 ”数量很大，“ 下载数据包 ”数量很小或者没有。

8.3 DHCP 统计

本节主要讲述***系统状态—>DHCP 统计***的使用。

DHCP 统计—>服务器页面包括“ DHCP 地址池使用信息列表 ”、“ DHCP 服务器统计信息列表 ”及“ DHCP 冲突信息列表 ”三个列表；***DHCP 统计—>客户端及中继***页面包括“ DHCP 客户端统计信息列表 ” 和 “ DHCP 中继统计信息列表 ” 两个列表。

8.3.1 DHCP 地址池使用信息列表

通过“ DHCP 地址池使用信息列表 ”，可以查看各地址池的使用信息，包括：已分配的 IP 地址，与当前 IP 地址对应的 MAC 地址、剩余租期、绑定地址池名称等。同时在该表中还可配置 DHCP 手工绑定：选中欲配置 DHCP 手工绑定的 IP 地址所在条目，单击右下方“ 绑定 ”按钮，即可生成该 IP 地址对应的 DHCP 手工绑定，可在***高级配置—>DHCP 配置***的“ DHCP 手工绑定信息列表 ” 中查看到相应信息记录。

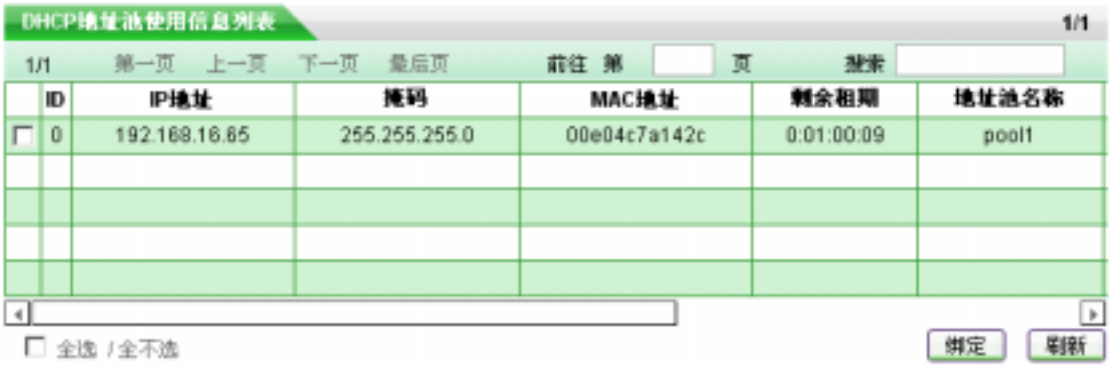


表 8-6 DHCP 地址池使用信息列表

表 8-7 DHCP 地址池使用信息列表（续表 8-6）

- ID：IP/MAC 绑定的序号；
- IP 地址：分配给 DHCP 客户端的 IP 地址；
- 掩码：当前 IP 地址的子网掩码；
- MAC 地址：DHCP 客户端的 MAC 地址；
- 剩余租期：当前 IP 地址离租期到期的时间，单位为：天:时:分:秒；
- 地址池名称：当前 IP 地址所属地址池的名称；

- 状态：当前 IP 地址的状态。
  正在验证：DHCP 服务器正在检测当前 IP 地址是否冲突；
  已分配：DHCP 服务器已将该 IP 地址分配给客户端；
  冲突：DHCP 服务器检测到该 IP 地址冲突；
- 静态/动态：当前 IP 地址的分配方式；
  静态：静态分配，当前 IP 地址是通过 DHCP 手工绑定指定的；
  动态：动态分配，当前 IP 地址是从 DHCP 地址池中动态分配的；
- 客户端标识：当前 IP 地址对应的客户端标识；
- DHCP 中继标识：当前 IP 地址对应的 DHCP 中继标识；
- 绑定：选中某个动态分配的 IP 地址对应的条目，单击“ 绑定 ”按钮，即可生成与该 IP 地址对应的 DHCP 手工绑定，可在***高级配置—>DHCP 配置***的“ DHCP 手工绑定信息列表 ”中查看、编辑。
- 刷新：单击“ 刷新 ”按钮，即可查看最新的 DHCP 地址池使用信息。

提示：已经配置了 DHCP 手工绑定的 IP 地址（用户），不能再在这里对与该 IP 地址对应的条目进行手工绑定。

8.3.2 DHCP 服务器统计信息列表

通过“ DHCP 服务器统计信息列表 ”，可以查看 DHCP 服务器的统计信息，主要包括 DHCP 服务各个阶段的数据包的统计信息，以及各接口 DHCP 地址池中的已分配的 IP 地址的数量。

表 8-8 DHCP 服务器统计信息列表

- 接口：DHCP 服务器的应用接口，LAN、WAN1、WAN2/DMZ、WAN3 或者 WAN4 口；
- 发现包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器接收的发现包的统计数量；
- 提供包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器发送的提供包的统计数量；
- 请求包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器接收的请求包的统计数量；
- 确认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器发送的确认包的统计数量；
- 释放包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器接收的释放包的统计数量；
- 拒绝包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器接收的拒

绝包的统计数量；

- 否认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器发送的否认包的统计数量；
- 冲突次数：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器为 DHCP 客户端分配地址时，检测到地址冲突的次数；
- 信息包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 服务器接收的信息包的统计数量；
- 未知包：上一次清除至查询时刻这段时间内，经过此接口的未知类型的数据包的统计数量；
- 客户端个数：当前接口作为 DHCP 服务器时，绑定在该接口上的所有 DHCP 地址池中已分配的地址个数。
- 清除：单击“ 清除 ”按钮，可将“ DHCP 服务器统计信息列表 ”中除“ 客户端个数 ”外的全部信息清除，配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的 DHCP 服务器统计信息。
- 刷新：单击“ 刷新 ”按钮，即可查看最新的 DHCP 服务器统计信息。

8.3.3 DHCP 冲突信息列表

通过“ DHCP 冲突信息列表 ”，可以查看 DHCP 服务器为客户端分配地址时，检测到的地址冲突的相关信息，包括：发生冲突的 IP 地址、MAC 地址、检测方法以及冲突时刻等信息。

表 8-9 DHCP 冲突信息列表

- IP 地址：发生冲突的 IP 地址；
- MAC 地址：冲突 IP 地址所绑定的 MAC 地址；
- 检测方法：检测到地址冲突时使用的检测方法；
  ARP 方式：通过 ARP 方式检测到地址冲突信息；
  ICMP 方式：通过 ICMP 方式检测到地址冲突信息；
- 冲突时间：检测到地址冲突的时刻，单位为：年-月-日，时:分:秒。
- 刷新：单击“ 刷新 ”按钮，即可查看最新的 DHCP 冲突信息。

8.3.4 DHCP 客户端统计信息列表

通过“ DHCP 客户端统计信息列表 ”，可以查看 DHCP 客户端的统计信息，主要包括 DHCP

服务各个阶段的数据包的统计信息。

表 8-10 DHCP 客户端统计信息列表

- 接口：DHCP 客户端的应用接口，LAN、WAN1、WAN2/DMZ、WAN3 或者 WAN4 口；
- 发现包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端发送的发现包的统计数量；
- 提供包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端接收的提供包的统计数量；
- 请求包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端发送的请求包的统计数量；
- 确认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端接收的确认包的统计数量；
- 释放包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端发送的释放包的统计数量；
- 拒绝包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端发送的拒绝包的统计数量；
- 否认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端接收的否认包的统计数量；
- 冲突次数：上一次清除至查询时刻这段时间内，DHCP 服务器为当前 DHCP 客户端分配地址时，检测到地址冲突的次数；
- 信息包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 客户端发送的信息包的统计数量；
- 未知包：上一次清除至查询时刻这段时间内，经过此接口的未知类型的数据包的统计数量；

- 清除：单击“ 清除 ”按钮，可将“ DHCP 客户端统计信息列表 ”中全部信息清除，配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的 DHCP 客户端统计信息。
- 刷新：单击“ 刷新 ”按钮，即可查看最新的 DHCP 客户端统计信息。

8.3.5 DHCP 中继统计信息列表

通过“ DHCP 中继统计信息列表 ”，可以查看 DHCP 中继的统计信息，主要包括 DHCP 服务各个阶段的数据包的统计信息。

表 8-11 DHCP 中继统计信息列表

- 接口：DHCP 中继的应用接口，LAN、WAN1、WAN2/DMZ、WAN3 或者 WAN4 口；
- 发现包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的发现包的统计数量；
- 提供包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的提供包的统计数量；
- 请求包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的请求包的统计数量；
- 确认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的确认包的统计数量；
- 释放包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的释放包的统计数量；
- 拒绝包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的拒绝包的统计数量；
- 否认包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的否认包的统计数量；
- 信息包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的信息包的统计数量；
- 增加超长包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的因超长而不增加中继信息的数据包的个数；
- 替换超长包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的因超长而不替换原有中继信息的数据包的个数；
- 策略丢弃包：上一次清除至查询时刻这段时间内，当前接口作为 DHCP 中继转发的由转发策略指定丢弃的数据包的个数；

- 清除：单击“ 清除 ”按钮，可将“ DHCP 中继统计信息列表 ”中全部信息清除，配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的 DHCP 中继的统计信息。
- 刷新：单击“ 刷新 ”按钮，即可查看最新的 DHCP 中继统计信息。

8.4 接口统计

本节主要讲述***系统状态—>接口统计***的使用。


接口统计信息列表 6/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	接口/方向	字节数	数据包	广播包	平均速率(bps)	平均速率(pps)	入流量/出流
0	LAN/In	12938653	1979	210776	220k	3	108%
0	LAN/Out	1228635	1829	12105	21k	3	108%
1	WAN1/In	511879	1740	0	9k	3	103%
1	WAN1/Out	225247	1697	20	4k	3	103%
2	WAN2(DMZ)/In	0	0	0	0	0	0
2	WAN2(DMZ)/Out	34980	0	583	596	0	0

查看内网用户带宽使用情况 清除 刷新

表 8-12 接口统计信息列表


接口统计信息列表 6/6

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

K(bps)	平均速率(pps)	入流量/出流量	广播包 / 数据包	抛弃包	错误包	未知包	非路由包
)k	3	108%	10651%	0	0	0	0
k	3	108%	662%	0	0	0	0
	3	103%	0%	0	0	0	0
	3	103%	1%	0	0	0	0
	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0

查看内网用户带宽使用情况 清除 刷新

表 8-13 接口统计信息列表（续表 8-12）

- ID：序号；
- 接口/方向：物理接口名和数据流方向。In（接收）指数据包从该接口进入设备，Out（发送）指数据包从该接口离开设备；
- 字节数：上一次清除至查询时刻这段时间内，经过此接口的数据包字节数的统计；
- 数据包：上一次清除至查询时刻这段时间内，经过此接口的数据包数量的统计；
- 广播包：上一次清除至查询时刻这段时间内，经过此接口的广播包（包括多播包）数量的统计；
- 平均速率：上一次清除至查询时刻这段时间内，此接口接收或发送数据包的平均速率，提供每秒比特数（bps）和每秒数据包数（pps）两种统计方式；
- 入流量/出流量：上一次清除至查询时刻这段时间内，从该接口进入设备的数据包数量和从该接口离开设备的数据包数量的百分比；
- 广播包/数据包：上一次清除至查询时刻这段时间内，经过此接口广播包数量和单播包数量之百分比；
- 丢弃包：上一次清除至查询时刻这段时间内，经过此接口的被丢弃包数量的统计。注意：设备把超过处理能力而来不及处理的数据包丢弃；

- 错误包：上一次清除至查询时刻这段时间内，经过此接口的错误包数量的统计；
- 未知包：上一次清除至查询时刻这段时间内，经过此接口的未知类型数据包数量的统计；
- 非路由包：上一次清除至查询时刻这段时间内，经过此接口的非路由数据包（例如桥接、VLAN 发的包）数量的统计。

- 清除：单击“ 清除 ”按钮，可清除“ 接口统计信息列表 ”中的全部信息。配合“ 刷新 ”按钮，可查看清除时刻至刷新时刻这段时间内的接口统计信息；
- 刷新：单击“ 刷新 ”按钮，可以看到最新的“ 接口统计信息列表 ”；
- 查看内网用户带宽使用情况：单击“ 查看内网用户带宽使用情况 ”超链接，立即转到***带宽业务—>带宽信用管理***页面。

提示：设备正常运行时应该具备的特征，以下描述中，广域网接口可能是一个或者多个（多线路接入）。

1. 广域网接口接收的数据包与局域网接口发出的数据包的数量相近；
2. 广域网接口发出的数据包与局域网接口接收的数据包的数量相近；
3. 广域网接口接收的数据包与局域网接口发出的数据包的字节数相近；
4. 广域网接口发出的数据包与局域网接口接收的数据包的字节数相近；
5. 每个接口的“ 广播包/数据包 ”的百分比小于 5%；
6. 整个网络流量比较平衡，流量缓增缓减，不会出现瞬间流量突增的情况。

8.5 路由和端口信息

本节主要讲述***系统状态—>路由和端口信息***的使用。

8.5.1 路由表信息

路由器（网关）的主要工作就是为经过路由器的每个数据包寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表，供路由选择时使用。路由表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

路由表信息列表 21/21

1/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	58.246.187.125	ie1	lugpaN	60	1	13384198	722602
100.100.100.0/24	200.200.200.118	ie0	lugpa	60	1	0	722602
127.0.0.0/8	-	bhole0	cup	20	0	0	722604
127.0.0.1/32	-	local	cuhp	20	0	0	722604
127.0.0.2/32	-	reject0	cuhp	20	0	0	722604
127.0.0.3/32	-	bhole0	cuhp	20	0	0	722604
192.168.1.0/24	-	ie0	cua	20	0	2387	722602
192.168.1.1/32	-	local	cuhp	20	0	1322	722602
200.200.200.0/24	-	ie0	cua	20	0	494755	722602
200.200.200.251/32	-	local	cuhp	20	0	184940	722602

查看路由配置 刷新

表 8-14 路由表信息列表

路由表信息列表 21/21

2/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
224.0.0.0/4	-	mcast	cup	20	0	0	722604
224.0.0.1/32	-	local	cuhp	20	0	0	722604
224.0.0.18/32	-	bhole0	cuhp	20	0	0	722604
224.0.0.2/32	-	local	cuhp	20	0	0	722604
224.0.0.5/32	-	bhole0	cuhp	20	0	0	722604
224.0.0.6/32	-	bhole0	cuhp	20	0	0	722604
224.0.0.9/32	-	local	cuhp	20	0	0	722604
239.255.255.250/32	-	local	cuhp	20	0	6343	722604
255.255.255.255/32	-	ie0	cuhp	20	0	2557	722602
58.246.187.124/30	-	ie1	cuaN	20	0	5	722602

查看路由配置 刷新

表 8-15 路由表信息列表（续表 8-14）

- 目的地址：目的网段的 IP 地址；
- 网关地址：到目的网段的网关 IP 地址；
- 接口号：与该路由匹配的数据包将从指定接口转发。
  ie0-物理接口 LAN；ie1-物理接口 WAN；ie2-物理接口 WAN2/DMZ；
  ptpdial0-待拨的虚接口；ptpx-虚接口 x；
  bhole0-内部接口，转发到该端口的所有包都被设备丢弃；
  local-内部软路由接口，转发到设备本身；
  reject-内部接口，转发到该端口的所有数据包都被设备拒绝，并回应一个 ICMP 不可达；
  loopback-回环地址，代表 127.0.0.0/8 网段，不被转发；
  mcast-多播；
- 路由状态：*-Hidden，o-OSPF，i-ICMP，l-Local，r-RIP，n-SNMP， c-Connected，s-Static，R-Remote， g-Gateway， h-Host， p-Private， u-Up，t-Temp，M-Multiple，N-NAT，F-Float，a-Append，?-Unknown；
  *-Hidden：此条路由目前不生效，一般是此条路由处于备份状态或是线路失效导致路由中断；
  N-NAT：此条路由上启用了 NAT，局域网用户正通过此条路由共享上网；
  F-Float：此条路由配置了路由优先级等信息，目前处于浮动状态，会因为线路的生效或者失效而决定该条路由是否启用。
- 优先级：该路由的优先级，目的网段相同的情况下，设备将优先选择优先级高的路由转发数据包，值越低优先级越高；
- 跳数：从源到目的的路径中每一跳被赋以一个跳数值，此值通常为 1，优先级相同情况下，优先选择跳数值较低的路由；
- 使用次数：该路由被使用的次数；
- 使用时间：该路由生成的年龄（单位：秒）。
- 刷新：单击“ 刷新 ”按钮，可以在“ 路由表信息列表 ”看到最新相关信息；
- 查看路由配置：单击“ 查看路由配置 ”超链接，立即转到***高级配置***—>***路由配置***页面，在该页面可查看已配置的静态路由相关信息。

下面以表 8-14、表 8-15 为例，对一些路由信息进行解释：

- 0.0.0.0/0——缺省路由：当一个数据包的目的网段不在路由记录中，那么，设备将把该数据包发送到缺省路由的网关。缺省路由的网关是由配置的静态网关或者 PPPoE 拨号所得 IP 地址决定的；
- 127.0.0.0/8——本地环路：127.0.0.0 这个网段内所有地址都指向设备本身，如果收到这样一个数据包，应该发向设备本身；
- 100.100.100.0/24——指定网段的路由记录：当设备收到发往指定网段的数据包时，会将数据包发送到该条路由指定的网关（200.200.200.118）；
- 192.168.1.1——本地主机路由（其“ 接口名 ”为 local）：当设备收到发送给自己的数据包时会将该数据包收下，并且不再转发；
- 224.0.0.0/4——组播路由：设备收到一个组播数据包时，以组播的形式发送；
- 255.255.255.255/32——广播路由：当设备收到一个链路层广播包时将该数据包发送到 ie0。

8.5.2 端口信息

表 8-16 端口信息列表

- 端口所在的接口：该端口所在的物理接口。通常，LAN 接口有 4 个交换端口。
- 端口状态：该端口是否激活。
  UP-激活；DOWN-未激活。
- 速率状态：该端口的连接速率。
  100M-协商结果为 100M 连接；10M-协商结果为 10M 连接。
- 工作状态：该端口的工作状态。
  Half-半双工；Full-全双工。
- 模式状态：该端口的工作模式。
  MDI：正接；MDI-X：反接。

▶ 刷新：单击“ 刷新 ”按钮，可以看到最新的“ 端口信息列表 ”。

提示：MDI 是指通过收发器发送的 100BASE-T 信号，即 100BASE-TX、FX、T4 或 T2 信号。将集线器连接网络接口卡时，其发送和接收对通常是相互连接的。集线器之间连接时，通常需要一条跨接电缆，其中的发送和接收对是反接的。MDI 是正常的 UTP 或 STP 连接，而 MDI-X 连接器的发送和接收对是在内部反接的，这就使得不同的设备（如集线器-集线器或集线器-交换机），可以利用常规的 UTP 或 STP 电缆实现背靠背的级联。

8.6 系统信息

本节讲述***系统状态***—>***系统信息***的使用，主要包括系统版本、系统运行时间、系统历史记录等信息。

8.6.1 页面刷新功能

图 8-1 页面刷新功能配置

- 下拉框：用于设置采用手动或自动刷新本页面及相关页面。
  手动刷新：表示不启用自动刷新功能，只能通过单击“ 刷新 ”按钮手动刷新本页面；
  自动刷新/10 秒、自动刷新/30 秒或者自动刷新/60 秒：表示启用自动刷新功能，本页面和***系统状态***—>***NAT 统计***页面将每隔指定的时间间隔自动刷新。
- 刷新：单击“ 刷新 ”按钮，可查看本页面最新信息。
- **提示**：若修改了下拉框的值，只有在单击“ 刷新 ”按钮之后，修改的配置才能被保存并生效。

8.6.2 系统运行时间

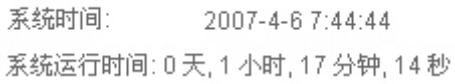


图 8-2 系统运行时间

- 系统时间：显示设备当前的日期和时间；
- 系统运行时间：显示设备本次启动至查看时刻的时间。

8.6.3 系统资源状态

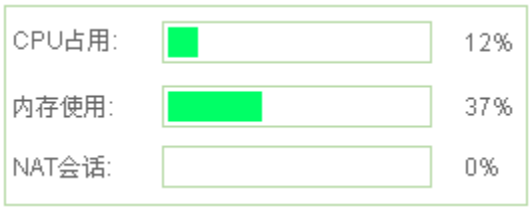


图 8-3 系统资源状态

- CPU 占用：显示当前 CPU 占用的百分比；
- 内存使用：显示当前内存使用的百分比；
- NAT 会话：显示当前建立的 NAT 会话数占设备所能处理的最大 NAT 会话数的百分

比。

提示：

1. 上述三个参数的值都通过进度条和数值（百分比）两种方式显示，数值的取值范围为 0%~100%；根据数值的大小，进度条可能会显示为空、绿色、黄色或者红色：

- 当数值＜1%时，进度条为空；
- 当 1%≤数值＜50%时，进度条为绿色；
- 当 50%≤数值＜70%时，进度条为黄色；
- 当数值≥70%时，进度条为红色。

2. 上述三个参数显示了设备接近于满负荷运行的程度。如果它们的值都比较低，就表明设备还有能力处理比它现在所运行的更多的网络通讯。如果它们的值都很高，就表明设备已经接近于满负荷工作，此时再增加更多的任务可能会导致系统对通讯的处理出现延迟。

8.6.4 系统版本信息

图 8-4 系统版本信息

- 序列号：产品的内部序列号（和表面序列号可能不同）；
- 功能号：产品具有的功能模块；
- 软件版本：产品的软件版本号。

8.6.5 系统端口状态

端口	状态	外出/进入速率(kbit/s)
lan1	100M Full MDI-X	23 / 0
lan2	DOWN	
lan3	DOWN	
lan4	DOWN	

端口	状态	外出/进入速率(kbit/s)
wan1	DOWN	0
wan2	DOWN	0
wan3	DOWN	0
wan4	DOWN	0

图 8-5 系统的端口状态

- 端口：其中，LAN 接口有 4 个交换端口；
- 状态：若某端口未激活，其“ 状态 ”显示为 DOWN；若已经激活，则依次显示该端口的速率状态、工作状态（Full-全双工，Half-半双工）以及模式状态（MDI-正接，MDI-X-反接）；
- 外出/进入速率（kbit/s）：相关速率是针对接口统计的，即 4 个交换端口按照 1 个 LAN 口来统计，各个 WAN 口分别统计。

8.6.6 系统告警信息

图 8-5 系统告警信息

系统告警信息中记录的都是被设备拒绝的数据包的相关信息。一般情况下，当设备的某个接口收到不能处理的多播数据包、非法数据包时，或者当 NAT 功能阻挡外网发起的数据包时，就会在这里增加一条信息。并且，信息按照从新到旧的顺序从上往下排列，最上面的信息为最新的一条信息。

每条告警信息记录的内容为：时间、协议（TCP、UDP 或者 ICMP）、源 IP 地址以及目的 IP 地址。

8.6.7 系统历史记录

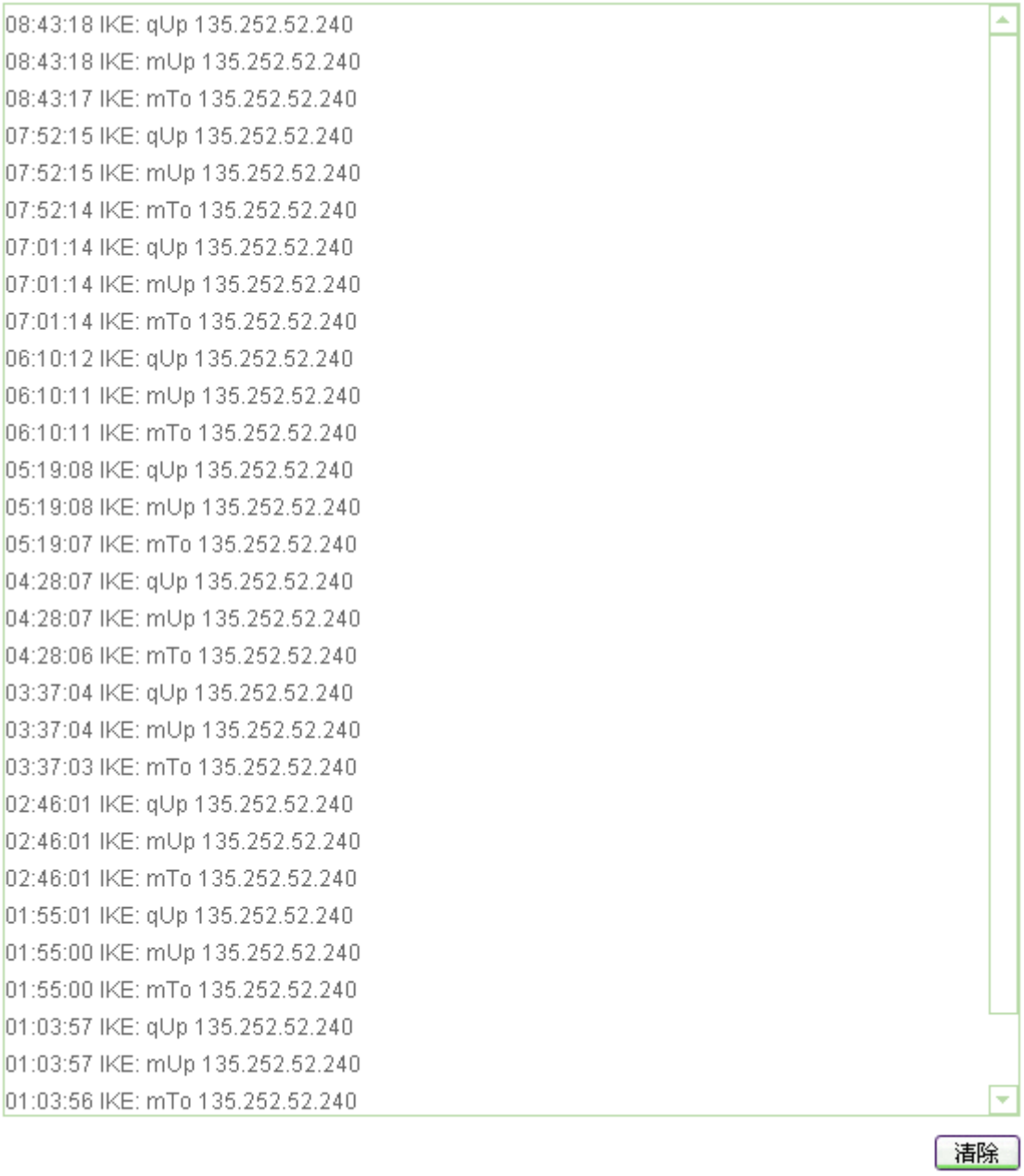


图 8-6 系统历史记录

系统历史记录中，信息按照从新到旧的顺序从上往下排列，最上面的信息为最新的一条信息。

- 清除：通过单击“ 清除 ”按钮可以删除旧的系统历史记录。

常见的记录及含义如表 8-17 所示：

历史记录	记录含义
Ethernet Up	某个物理接口被激活
MAC New 00:22:aa:00:22:bb MAC Old 00:22:aa:00:22:aa MAC Chged 192.168.16.221	该用户变化后的 MAC 地址 该用户变化前的 MAC 地址 连接到设备的 IP 地址为 192.168.16.221 的用户的 MAC 地址发生变化
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @61:1-1	某连接成功建立，[x]为连接名 PPPoE 成功和 MAC 地址为 00:0c:f8:f9:66:c6 的设备建立连接 物理层/链路层连接完成，但 IP 仍不可用 连接开始呼出
Call Terminated @clearSession: 1 Outgoing Call @61:1-1	呼叫失败 连接开始呼出
Session down [x]	某连接挂断，[x]为连接名
Session up [x] Assigned to port Call Connected, on Line1, on Channel0 Incoming Call	某连接成功建立，[x]为连接名 协商成功，为拨入的连接分配端口 物理层/链路层连接完成，但 IP 仍不可用 有远端呼叫拨入
Security error [x]	安全层错误
Route Up ethX： Route Down ethX：	该物理接口上配置的路由生效（一般是该接口物理线路启用所致） 该物理接口上配置的路由中断（一般是该接口物理线路中断所致）
NAT exceeded [IP 地址]	表示具有该 IP 地址的计算机的 NAT 并发 session 数超过了系统限定的最大 session 数（在***高级配置—>NAT 和 DMZ 配置***的“ NAT 全局配置 ”中配置）。一般情况下是这台计算机感染了病毒或者是在进行黑客攻击，如果一切正常，请适当调高最大 session 数。
ARP exceeded [IP 地址]	表示该 IP 地址的 ARP 请求超过系统限制：设备产品在出厂的时候定义了 ARP 表的最大数量，当超过这个限制的时候系统会提示此信息。
DHCP:IP conflicted arp: [IP 地址]	表示 DHCP 地址冲突：设备的 DHCP Server 在准备分配该 IP 地址给某用户时，发现在内网中已存在该 IP 地址，系统会再次分配其他 IP 地址给用户。

表 8-17 系统历史记录

第9章 上网监控

本章主要讲述如何监控局域网用户上网状况。在设备中，可以根据全部记录、内网地址、外网地址/域名、外网端口以及 NAT 地址/域名、各线路的“ 线路名称 ”等条件查询内网用户上网情况。这里查询的是局域网用户当前使用 NAT 的信息，并不是 NAT 统计信息。

当内网中有主机向外发出连接请求时，设备将会在 NAT 表中为该请求建立一条 NAT 会话（NAT Session）的记录，从而将该主机内部的 IP 地址转换为合法的 IP 地址进行通信。这种由内到外、或者由外向内的连接就是一个 NAT 会话。

9.1 查询条件

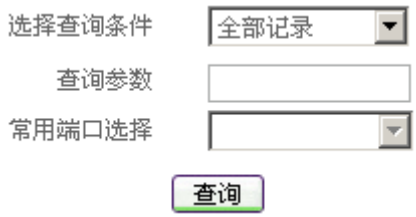


图 9-1 选择查询条件

- 选择查询条件：
  - 全部记录——查询当前全部用户的上网信息；
  - 默认线路——查询当前使用默认线路上网的局域网用户的上网信息；
  - 内网地址——填写局域网内某用户的 IP 地址，查询该用户此时的上网信息；
  - 外网地址/域名——填写 Internet 地址或者网站的域名，查询当前局域网用户到此地址的连接信息；
  - 外网端口——填写目的端口，查询局域网用户此时使用某种 Internet 上网业务的信息（常用协议端口号：TCP21：ftp；TCP22：ssh；TCP23：telnet；TCP25：smtp；UDP53：dns；TCP79：finger；TCP80：http；TCP110：pop3；UDP161：snmp）；
  - NAT 地址/域名——填写局域网用户上网使用的 IP 地址，使用多地址 NAT 时，可以查询正在使用该 IP 地址上网的局域网用户的上网信息；
  - 各条线路的线路名称——选择某条线路的“ 线路名称 ”，即可查询使用该线路上网的局域网用户的上网信息。除“ 默认线路 ”之外，其余线路的“ 线路名称 ”均按用户自定义的名称显示。
- 查询参数：根据选择的查询条件，输入相应的查询参数；
- 常用端口选择：当选择查询条件为“ 外网端口 ”时，在这里可以选择常用的业务端口。
- 查询：单击“ 查询 ”按钮，即可按条件查询。

提示：只有系统管理员才有上网监控权限，在***系统管理—>管理员配置***中可查看和配置管理员权限。

9.2 查询结果列表

查询结果列表 66/66

1/4 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	192.168.18.1	10	I	192.168.18.2	1056	2200	0	192.168.18.1	1056
2	192.168.1.2	4500	U	0.0.0.0	0	0	0	218.79.219.244	4500
3	192.168.1.2	500	U	0.0.0.0	0	0	0	218.79.219.244	500
4	200.200.200.15	5778	T	0.0.0.0	0	0	0	218.79.219.244	5757
5	200.200.200.16	23	T	0.0.0.0	0	0	0	218.79.219.244	1623
6	200.200.200.24	15004	T	207.46.108.52	msn	113	71	218.79.219.244	1042
7	200.200.200.33	69	U	0.0.0.0	0	0	0	218.79.219.244	9000
8	200.200.200.87	3339	T	218.83.175.154	1027	3	3	218.79.219.244	1038
9	200.200.200.87	3338	T	218.83.175.154	1027	3	3	218.79.219.244	1030
10	200.200.200.87	3337	T	218.83.175.154	1027	3	3	218.79.219.244	1029
11	200.200.200.87	3333	T	222.186.190.36	http	18	24	218.79.219.244	1359
12	200.200.200.87	3321	T	222.186.190.36	http	86	122	218.79.219.244	1345
13	200.200.200.87	3285	T	209.85.167.104	http	14	15	218.79.219.244	1303
14	200.200.200.87	3284	T	209.85.167.104	http	19	19	218.79.219.244	1302
15	200.200.200.87	3241	T	61.172.207.71	http	8	9	218.79.219.244	1178
16	200.200.200.87	3239	T	61.172.207.71	http	9	8	218.79.219.244	1176
17	200.200.200.87	3238	T	61.172.207.71	http	11	12	218.79.219.244	1175
18	200.200.200.87	3139	T	61.172.207.70	http	121	185	218.79.219.244	1266
19	200.200.200.87	3005	T	203.86.9.90	1347	23	26	218.79.219.244	1039
20	200.200.200.87	2817	T	207.46.110.51	msn	150	130	218.79.219.244	1162

全选 / 全不选 清除

表 9-1 查询结果列表

- ID：序号；
- 内网地址：该 NAT 会话的源 IP 地址；
- 内网端口：该 NAT 会话使用的源端口；
- 协议类型：该 NAT 会话使用的协议类型（T：TCP；U：UDP；I：ICMP）或协议号；
- 外网地址：该 NAT 会话要访问的目的 IP 地址；
- 外网端口：该 NAT 会话的目的端口。系统预设了一些标准业务，如 dns 解析、ftp 下载、www 浏览、smtp 发信、pop3 收信、qq、msn、qiji2（奇迹 2）、cq（传奇）、cs（cs 游戏）等；
- 上传包：通过该 NAT 会话上传数据包的数量；
- 下载包：通过该 NAT 会话下载数据包的数量；
- NAT 地址：该 NAT 会话经过 NAT 转换后的 IP 地址；
- NAT 端口：该 NAT 会话经过 NAT 转换后使用的端口。

▶ 清除：进入本页面执行查询操作后，若单击“ 清除 ”按钮，则可清除表中所有动态生成的 NAT 会话记录。

提示：执行清除操作可能导致当前正连接的会话断开，请谨慎使用。

9.3 查询实例

9.3.1 查询局域网 IP 地址为 200.200.200.87/24 的用户当前上网行为

第一步，进入***上网监控***页面，如图 9-2 所示；
第二步，在“选择查询条件”中选择“内网地址”；
第三步，在“查询参数”中填入 200.200.200.87；
第四步，单击“查询”按钮，即可查询，查询结果如表 9-2 所示。

图 9-2 选择查询条件——实例一

查询结果列表 131/131

1/7 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.87	3677	T	61.129.67.199	http	1	0	218.79.219.244	1101
2	200.200.200.87	3676	T	61.129.67.121	http	3	1	218.79.219.244	1098
3	200.200.200.87	3675	T	61.129.67.121	http	5	6	218.79.219.244	1097
4	200.200.200.87	3674	T	61.129.67.121	http	5	5	218.79.219.244	1096
5	200.200.200.87	3673	T	61.129.67.121	http	7	6	218.79.219.244	1095
6	200.200.200.87	3672	T	61.129.67.199	http	15	21	218.79.219.244	1094
7	200.200.200.87	3671	T	61.129.67.121	http	5	5	218.79.219.244	1093
8	200.200.200.87	3670	T	61.129.67.121	http	5	5	218.79.219.244	1092
9	200.200.200.87	3669	T	61.129.67.121	http	6	7	218.79.219.244	1091
10	200.200.200.87	3668	T	61.129.67.121	http	6	7	218.79.219.244	1087
11	200.200.200.87	3667	T	218.83.175.154	1027	3	3	218.79.219.244	1085
12	200.200.200.87	3666	T	61.129.67.199	http	16	23	218.79.219.244	1084
13	200.200.200.87	3665	T	61.129.67.121	http	7	7	218.79.219.244	1083
14	200.200.200.87	3453	T	220.134.94.151	4662	1	0	218.79.219.244	1082
15	200.200.200.87	3664	T	61.129.67.121	http	7	7	218.79.219.244	1081
16	200.200.200.87	3663	T	61.129.67.123	http	3	0	218.79.219.244	1080
17	200.200.200.87	3662	T	61.129.67.123	http	6	7	218.79.219.244	1078
18	200.200.200.87	3661	T	61.129.67.123	http	6	6	218.79.219.244	1076
19	200.200.200.87	3660	T	61.129.67.121	http	6	6	218.79.219.244	1075
20	200.200.200.87	3659	T	61.129.67.199	http	7	8	218.79.219.244	1073

全选 / 全不选 清除

表 9-2 查询结果列表——实例一

9.3.2 查询局域网内目前访问 www.utt.com.cn 的用户

第一步，进入***上网监控***页面，如图 9-3 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网地址/域名 ”；
第三步，在“ 查询参数 ”中填入 www.utt.com.cn ；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 9-3 所示。

图 9-3 选择查询条件——实例二

查询结果列表 3/3

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	200.200.200.232	2183	T	218.5.74.92	http	14	12	218.79.219.244	1423
2	200.200.200.232	2182	T	218.5.74.92	http	16	14	218.79.219.244	1422
3	200.200.200.232	2181	T	218.5.74.92	http	14	18	218.79.219.244	1421

全选 / 全不选 删除

表 9-3 查询结果列表——实例二

9.3.3 查询局域网内目前使用 MSN 的用户

第一步，进入***上网监控***页面，如图 9-4 所示；
第二步，在“ 选择查询条件 ”中选择“ 外网端口 ”；
第三步，在“ 查询参数 ”中填入 1863，或者直接在“ 常用端口选择 ”中选取“ 1863（msn）”；
第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 9-4 所示。

图 9-4 选择查询条件——实例三

查询结果列表 22/22

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	10.10.10.5	2641	T	207.46.106.29	msn	76	95	218.79.219.244	1399
2	200.200.200.22	1283	T	207.46.109.50	msn	5870	6409	218.79.219.244	2558
3	200.200.200.87	2773	T	207.46.110.93	msn	872	742	218.79.219.244	1815
4	200.200.200.87	2718	T	64.4.36.22	msn	37	51	218.79.219.244	1202
5	200.200.200.87	1487	T	207.46.107.37	msn	794	730	218.79.219.244	1141
6	200.200.200.139	39239	T	207.46.110.80	msn	916	726	218.79.219.244	1839
7	200.200.200.139	1957	T	207.46.110.16	msn	231	191	218.79.219.244	1215
8	200.200.200.174	2159	T	207.46.111.44	msn	317	259	218.79.219.244	1460
9	200.200.200.174	1906	T	207.46.106.91	msn	334	245	218.79.219.244	1044
10	200.200.200.205	2631	T	207.46.27.186	msn	28	29	218.79.219.244	1182
11	200.200.200.205	2181	T	207.46.109.29	msn	2186	2318	218.79.219.244	1792
12	200.200.200.205	1052	T	207.46.106.67	msn	2467	2566	218.79.219.244	1191
13	200.200.200.208	2971	T	207.46.108.48	msn	3242	3338	218.79.219.244	1940
14	200.200.200.208	1857	T	207.46.106.69	msn	1184	1205	218.79.219.244	1338
15	200.200.200.219	5783	T	207.46.106.16	msn	123	147	218.79.219.244	1044
16	200.200.200.231	2031	T	207.46.110.68	msn	227	134	218.79.219.244	1146
17	200.200.200.238	4106	T	207.46.111.85	msn	212	117	218.79.219.244	1078
18	200.200.200.238	1035	T	207.46.109.49	msn	424	234	218.79.219.244	1362
19	200.200.200.249	3605	T	65.54.171.17	msn	11	11	218.79.219.244	1201
20	200.200.200.249	3310	T	207.46.107.15	msn	385	408	218.79.219.244	1164

全选 / 全不选 清除

表 9-4 查询结果列表——实例三

9.3.4 查询局域网内目前使用 WAN2 口 IP 地址上网的信息

提示：如果使用双线路上网，可在***基本配置***—>***线路配置***的“ 线路连接信息列表 ”中，查询与 WAN2/DMZ 口相连的线路的“ IP 地址 ”，即可得到 WAN2/DMZ 口的 IP 地址。

第一步，进入***上网监控***页面，如图 9-5 所示；

第二步，在“ 选择查询条件 ”中选择“ NAT 地址/域名 ”；

第三步，在“ 查询参数 ”中填入 58.246.187.126（本例中，WAN2 口的当前 IP 地址为 58.246.187.126）；

第四步，单击“ 查询 ”按钮，即可查询，查询结果如表 9-5 所示。

图 9-5 选择查询条件——实例四

查询结果列表 16/16

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	50.50.50.3	1032	I	202.96.209.5	1318	2	0	58.246.187.126	1318
2	200.200.200.33	4020	T	218.80.196.46	8081	3	0	58.246.187.126	1297
3	200.200.200.33	4018	T	218.80.196.46	8081	1	0	58.246.187.126	1294
4	200.200.200.87	1490	T	207.46.110.55	http	3	0	58.246.187.126	1314
5	200.200.200.87	1489	T	207.46.110.55	http	3	0	58.246.187.126	1310
6	200.200.200.87	1486	T	218.83.175.154	1027	3	0	58.246.187.126	1306
7	200.200.200.87	1485	T	207.46.96.154	http	3	0	58.246.187.126	1300
8	200.200.200.118	4721	U	202.96.209.6	dns	4	0	58.246.187.126	1029
9	200.200.200.139	40305	T	218.85.134.158	pop3	3	0	58.246.187.126	1307
10	200.200.200.172	2510	T	59.40.167.164	52669	3	0	58.246.187.126	1028
11	200.200.200.172	2438	T	59.40.167.164	51416	5	0	58.246.187.126	1094
12	200.200.200.182	1036	T	219.149.44.125	telnt	3	0	58.246.187.126	1289
13	200.200.200.182	1032	I	219.129.255.52	1237	4	0	58.246.187.126	1237
14	200.200.200.182	1030	I	218.74.198.248	1074	5	0	58.246.187.126	1074
15	200.200.200.208	4572	T	61.129.49.7	http	2	0	58.246.187.126	1033
16	200.200.200.208	4571	T	61.154.219.108	cgame	3	0	58.246.187.126	1299

全选 / 全不选 清除

表 9-5 查询结果列表——实例四

9.3.5 查询局域网内目前使用默认线路上网的信息

第一步，进入***上网监控***页面，如图 9-6 所示；

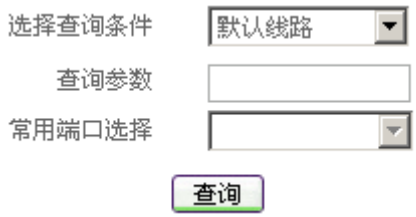


图 9-6 查询条件——实例五

第二步，在“ 选择查询条件 ”中选择“ 默认线路 ”；

第三步，单击“ 查询 ”按钮，即可查询，查询结果如表 9-6 所示。

查询结果列表 218/218

1/11 第一页 上一页 下一页 最后页 前往 第 页 搜索

ID	内网地址	内网端口	协议	外网地址	外网端口	上传包	下载包	NAT地址	NAT端口
1	192.168.1.2	4500	U	0.0.0.0	0	0	0	218.79.219.244	4500
2	192.168.1.2	500	U	0.0.0.0	0	0	0	218.79.219.244	500
3	200.200.200.15	5778	T	0.0.0.0	0	0	0	218.79.219.244	5757
4	200.200.200.16	23	T	0.0.0.0	0	0	0	218.79.219.244	1623
5	200.200.200.24	15004	T	207.46.108.52	msn	165	99	218.79.219.244	1042
6	200.200.200.33	69	U	0.0.0.0	0	0	0	218.79.219.244	9000
7	200.200.200.87	4607	T	61.129.67.199	http	37	57	218.79.219.244	1361
8	200.200.200.87	4606	T	61.129.67.29	http	5	5	218.79.219.244	1360
9	200.200.200.87	4605	T	61.129.67.106	http	7	6	218.79.219.244	1359
10	200.200.200.87	4604	T	61.129.67.199	http	36	55	218.79.219.244	1358
11	200.200.200.87	4603	T	61.129.67.29	http	5	5	218.79.219.244	1357
12	200.200.200.87	4602	T	61.129.67.106	http	7	6	218.79.219.244	1356
13	200.200.200.87	4601	T	61.129.67.199	http	42	64	218.79.219.244	1355
14	200.200.200.87	4600	T	61.129.67.29	http	6	5	218.79.219.244	1354
15	200.200.200.87	4599	T	61.129.67.106	http	7	6	218.79.219.244	1353
16	200.200.200.87	4598	T	61.129.67.199	http	129	175	218.79.219.244	1352
17	200.200.200.87	4597	T	61.129.67.29	http	5	5	218.79.219.244	1351
18	200.200.200.87	4596	T	61.129.67.106	http	7	6	218.79.219.244	1350
19	200.200.200.87	4595	T	218.83.175.154	1027	3	3	218.79.219.244	1347
20	200.200.200.87	4594	T	61.129.67.199	http	78	118	218.79.219.244	1343

全选 / 全不选 清除

表 9-6 查询结果列表——实例五

第10章 带宽业务

本章主要讲述如何对内网用户进行带宽业务管理，目前提供带宽信用管理功能，该功能可以实现带宽的公平合理分配，限制 P2P 软件的使用，并能保证较高的带宽利用率。

10.1 带宽信用管理

10.1.1 带宽信用管理功能概述

10.1.1.1 概述

带宽信用管理功能主要就是用来控制内网主机的流量。利用该功能，系统管理员可以控制下载和上传方向的流量，以确保内网主机公平合理使用网络带宽，有助于提高带宽利用率、控制网络拥塞，避免少数用户上下载大型文件时可能会导致的网络速度急剧下降，保证实时应用（如 IP 电话和视频会议）的质量。

从实现原理和实际效果来看，设备的带宽信用管理功能的实现可划分为两个阶段：

1. 内网主机速率限制功能，简称为 IP RATE 功能；
2. 带宽信用管理功能，简称为 CBT DRR 功能。

10.1.1.2 IP RATE 功能

IP RATE 功能，是通过基于 IP 地址的 RED（Random Early Detection，随机早期检测）流量控制算法来实现的。具体功能如下所述：

通过限制内网主机的最大下载/上传速率，来控制下载/上传的流量，并确保用户或者应用不会超过所分配的最大下载/上传速率，或者独占网络带宽。此外，还可通过时间段策略控制 IP RATE 功能的生效时间。

简单地说，通过 IP RATE 功能可以限制局域网内每台主机可以使用的最大带宽，而且，对于每台主机的带宽限制是完全公平的。虽然这种方法很公平，但是，在实际应用中，它的使用可能会引起以下两个问题：

1. 当最大速率设置过小时，对突发流量损伤太大（由于丢包），同时，也会导致内网的带宽利用率较低。如果内网中有主机出现突发流量，即使其他主机很空闲，也必须按照限制的最大速率来使用带宽，从而造成空闲资源浪费。举个例子来说，如果限制带宽过小（<256Kbps），当突然打开一个很大的网页，此时瞬间流量超过 256 Kbps，用户会反映速度很慢。
2. 当最大速率设置过大时，可能会导致总带宽不足的现象。如果在内网中有多台主机出现较大流量（每台主机的流量都在限速范围内而总流量需求却超出了总的带宽资源），就会发生相互挤占带宽的情况。此时使用 P2P 软件的主机可能过多占用带宽资源，从而影响其他内网主机正常上网。

10.1.1.3 CBT DRR 功能

为了更公平合理的分配内网带宽资源，就需采用基于信用的流量控制方法，即 CBT（Credit Based Traffic Control）方法。CBT 算法结合了原有的 IP RATE 功能，在原来的 RED 方法上增加了采用 CBT 技术的 DRR（Deficit Round Robin）方法，以实现对突发流量的控制。

CBT 方法的出发点就是有效提高带宽利用率和限制 P2P 软件的使用，即对于正常上网的内网主机，设备将允许它偶尔突破最大限速；相反，对于长期使用 P2P 工具的内网主机，设备将会减小它的带宽，使其对其他主机的影响降到最低。

在 CBT 方法中，借用了银行信用体系中的“ 信用 ”的概念，其流量控制机制类似于银行信用体系。为方便理解，下面先介绍几个相关概念：

最小下载速率：内网主机可以保证的最小下载速率，单位为比特/秒（bit/s）；

最小上传速率：内网主机可以保证的最小上传速率，单位为比特/秒（bit/s）；

初始信用：内网主机开机登录网络时的初始信用值，它同时作用于上传和下载两个方向，单位为字节（byte）；

信用额度：内网主机所能累计的信用的最大值，它同时作用于上传和下载两个方向，单位为字节（byte）；

赤字额度：内网主机所能透支的信用的最大值，它同时作用于上传和下载两个方向，单位为字节（byte）。

下载/上传信用值：内网主机在下载/上传方向的实际信用值，单位为字节（byte）。下载/上传信用值的大小是动态变化的，将随着内网主机的实际下载/上传速率的变化而增加或减少，具体描述如下：

1. 当内网主机的下载/上传速率小于预设的“ 最小下载/上传速率 ”时，“ 下载/上传信用值 ”就增加，增加的速度＝“ 最小下载/上传速率 ”－实际下载/上传速率。当“ 下载/上传信用值 ”增加到“ 信用额度 ”后就不再增加，以避免单个主机的突发流量占用过多的带宽。
2. 相反，当内网主机的下载/上传速率大于“ 最小下载/上传速率 ”时，若“ 下载/上传信用值 ”大于 0，系统不会马上限速，而是从中消耗，消耗的速度＝实际下载/上传速率－“ 最小下载/上传速率 ”。一旦“ 下载/上传信用值 ”消耗完毕（即该值减少到 0），就使用 IP RATE 功能进行限速。
3. 当某主机的“ 下载/上传信用值 ”降低到“ 赤字额度 ”后就不再降低，系统将会强行将其下载/上传速率限制为 64Kbit/s；并且，该主机的速度无法自动恢复，除非手工解除。

信用良好与信用不良：通过“ 下载/上传信用值 ”来衡量内网主机的信用是否良好。当某台主机的“ 下载/上传信用值 ”大于 0 时，就认为该主机信用良好；否则，就认为该主机信用不良。

严重失信：某主机信用不良时，如果其实际下载/上传速率达到“ 最大下载/上传速率 ”的 2 倍及以上时（比如使用 P2P 软件下载），就认为该主机严重失信。

自适应惩罚机制：某主机严重失信时，系统将会强制使其速度降至“ 最大下载/上传速率 ”的一半，并持续一段时间（即“ 管制时间 ”）。如果在“ 管制时间 ”内，该主机的速率还是能够达到“ 最大下载/上传速率 ”的 2 倍，系统将在原有降速一半的基础上再次降速一半，即强行将其速度降至“ 最大下载/上传速率 ”的四分之一，直至带宽降低到“ 最小下载/上传速率 ”或条件不满足。“ 管制时间 ”结束后，将立即恢复对该主机的带宽供给，如果该主机仍是严重失信，则再次强行降速，依次循环。

管制时间：内网主机严重失信时，使用“ 自适应惩罚机制 ”进行流量控制的时间，单位为秒（s）。

10.1.1.4 工作流程

提示：目前，只有在使用了 IP RATE 功能后，CBT DRR 功能才能使用；而 IP RATE 功能则可以脱离 CBT DRR 功能独立使用。

启用了 IP RATE 功能和 CBT DRR 功能后，带宽信用管理功能的工作流程如下：

1. 当某台内网主机信用良好时，由 CBT DRR 控制其流量。此时，“ 下载/上传信用值 ”将随着内网主机的实际下载/上传速率而增加或减少。
2. 当某台内网主机信用不良时，由 IP RATE 控制其流量。此时，如果其实际下载/上传速率超过了预设的“ 最大下载/上传速率 ”，系统将会自动将其下载/上传速率限制为“ 最大下载/上传速率 ”。
3. 当某台内网主机严重失信时，使用“ 自适应惩罚机制 ”控制其流量。
4. 如果某台内网主机的“ 下载/上传信用值 ”降低到“ 赤字额度 ”，系统将会强行将其下载/上传速率限制为 64Kbit/s ；并且，该主机的速度无法自动恢复，除非手工解除。

10.1.2 带宽信用管理配置

图 10-1 带宽信用管理配置

最大下载速率：内网主机的最大下载速率（单位：比特/秒）。其中，选项“ NoLimit ”

表示不限制，即在下载方向不启用 IP RATE 功能；“ Block ”表示禁止传送；

- 最大上传速率：内网主机的最大上传速率（单位：比特/秒）。其中，选项“ NoLimit ”表示不限制，即在上传方向不启用 IP RATE 功能；“ Block ”表示禁止传送；
- 时间段：IP RATE 功能生效的时间，不设置为所有时间。如果配置之后需要删除，可以选择“ 时间段 ”下拉列表中的空选项。如果该时间段已经超过执行的起止生效时间，系统将认为 IP RATE 功能没有时间限制；
- 最小下载速率：正常情况下，内网主机可以保证的最小下载速率（单位：比特/秒）。其中，选项“ Disabled ”表示关闭 CBT DRR 功能；
- 最小上传速率：正常情况下，内网主机可以保证的最小上传速率（单位：比特/秒）。其中，选相“ Disabled ”表示关闭 CBT DRR 功能；
- 管制时间：内网主机严重失信时，使用“ 自适应惩罚机制 ”进行流量控制的时间，单位为秒。其中，“ Disabled ”表示禁止自动降速，“ Forever ”表示自动降速后不恢复速度，除非手工解除；
- 信用额度：内网主机所能累计的信用的最大值（单位：字节）。其中，选项“ Auto ”表示由系统自动设置；
- 赤字额度：内网主机所能透支的信用的最大值（单位：字节）。其中，选项“ NoLimit ”表示不限制；
- 初始信用：内网主机开机登录网络时的初始信用值（单位：字节）。其中，选项“ Auto ”表示由系统自动设置；
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 参数“ 最大下载速率 ”、“ 最大上传速率 ”以及“ 时间段 ”用来设置 IP RATE 功能；
2. 参数“ 最小下载速率 ”、“ 最小上传速率 ”、“ 管制时间 ”、“ 信用额度 ”、“ 赤字额度 ”、“ 初始信用 ”用来设置 CBT DRR 功能，其中“ 管制时间 ”、“ 信用额度 ”、“ 赤字额度 ”、“ 初始信用 ”同时作用于上传和下载两个方向。
3. 参数“ 最大下载速率 ”和“ 最小下载速率 ”具有连动性；当改变“ 最大下载速率 ”的值时，系统会自动为“ 最小下载速率 ”提供一个最接近“ 最大下载速率 ”且小于等于“ 最大下载速率 ”的值；同理，“ 最大上传速率 ”和“ 最小上传速率 ”也具有连动性。

10.1.3 带宽信用管理信息列表

表 10-1 带宽信用管理信息列表

- 用户名：如果是 IP/MAC 绑定用户，则显示为对应的“ 用户名 ”；否则显示为空。注意，可以在***高级配置—>IP/MAC 绑定***或者***安全配置—>用户管理—>用户信息配置***中配置 IP/MAC 绑定；
- IP 地址：某用户的 IP 地址；
- MAC 地址：某用户的 MAC 地址；
- 下载速率（Kbit/s）：某用户当前的实际下载速率，单位：千比特/秒；
- 上传速率（Kbit/s）：某用户当前的实际上传速率，单位：千比特/秒；
- 下载信用值（Mbyte）：某用户当前累计的下载信用值，单位：兆字节；
- 上传信用值（Mbyte）：某用户当前累计的上传信用值，单位：兆字节。
- 清除：选中若干带宽信用管理信息条目，单击“ 清除 ”按钮，对应主机的“ 下载信用值 ”和“ 上传信用值 ”立即恢复到初始信用值；
- 刷新：单击“ 刷新 ”按钮，可以查看“ 带宽信用管理信息列表 ”的最新信息；
- 查看各接口速率：单击“ 查看各接口速率 ”超链接，立即转到***系统状态—>接口统计***页面。

10.1.4 配置方法及实例

以下各节将介绍在不同的网络环境及实际要求下，如何设置“ 最大下载速率 ”、“ 最大上传速率 ”、“ 最小下载速率 ”、“ 最小上传速率 ”以及“ 管制时间 ”这几个参数。

10.1.4.1 相关概念

为方便起见，首先引入几个相关概念：

平均速率：在线路质量最好的情况下，即线路总带宽达到 ISP 分配的带宽时，内网主机实际可以获得的平均速率。它是由 ISP 分配的带宽和共享用户数计算出来的，由于一般 ISP 分配的上行带宽和下行带宽不一样，因此，下载和上传两个方向上的“ 平均速率 ”的值是不同的，这里将它们分别称为“ **平均下载速率** ”和“ **平均上传速率** ”。计算方法如下：

“ 平均下载速率 ” =“ ISP 分配的线路下行带宽 ”÷“ 共享用户数 ”；

“ 平均上传速率 ” =“ ISP 分配的线路上行带宽 ”÷“ 共享用户数 ”

例如，某公司使用 2Mbit/s 的 ADSL 线路上网，共有 32 个用户，那么，“ 平均下载速率 ”的值为 2M/32 = 64Kbit/s；由于 2M 的 ADSL 线路的上行带宽通常只有 512Kbit/s，因此，“ 平均上传速率 ”=512K/32=16Kbit/s。

10.1.4.2 如何设置“ 最大下载速率 ”和“ 最大上传速率 ”

设置“ 最大下载速率 ”和“ 最大上传速率 ”的方法类似，这里以如何设置“ 最大下载速率 ”为例进行说明。

在实际的应用中，一般建议 “ 最大下载速率 ”与“ 平均下载速率 ”的比值不大于 4:1。这个值设置得过小，将会降低线路的带宽利用率；但是，如果这个值设置过大，则会造成绝对带宽严重不足。以下举例进行说明。

例如，2M ADSL 接入时，若有 32 个共享用户，则“ 平均下载速率 ”=2M/32=64Kbit/s。如果将“ 最大下载速率 ”设为 512Kbit/s，那么，“ 最大下载速率 ”与“ 平均下载速率 ”的比值将高达 8:1。这时，如果在内网中有主机使用 BT 等 P2P 软件，就会强占过多的带宽，从而影响其他用户的正常上网，甚至无法上网。这时候，如果将“ 最大下载速率 ”修改为 256Kbit/s，即“ 最大下载速率 ”与“ 平均下载速率 ”的比值降至 4:1，就可大大减小因使用 P2P 软件造成的对其他上网应用的影响。

提示：为保证局域网用户都能正常上网，一般建议设置“ 最大下载速率 ”不低于 512kbit/s，“ 最大上传速率 ”不低于 128 kbit/s。

10.1.4.3 如何设置“ 最小下载速率 ”和“ 最小上传速率 ”

“ 最小下载速率 ”与“ 最大下载速率 ”具有连动性，在设置“ 最大下载速率 ”时，系统会自动为“ 最小下载速率 ”提供一个最接近“ 最大下载速率 ”且小于等于“ 最大下载速率 ”的值。同理，“ 最大上传速率 ”和“ 最小上传速率 ”也具有连动性，“ 最小上传速率 ”也会随着“ 最大上传速率 ”的改变而改变，其值为最接近“ 最大上传速率 ”且小于等于“ 最大上传速率 ”的值。下面将举例进行说明。

例如，当设置“ 最大下载速率 ”的值为 1Mbit/s，“ 最小下载速率 ”的值会自动改变为 1Mbit/s；当设置“ 最大下载速率 ”的值为 10Mbit/s 时，“ 最小下载速率 ”的值会自动改变为 8Mbit/s。

如何设置“ 最小下载速率 ”和“ 最小上传速率 ”随您的具体情况而定，为了提高线路带宽的利用率，而又不会造成绝对带宽的严重不足，使局域网中的用户都能正常上网且相互之间在上网时又都互不影响。在实际的应用中，我们一般建议不对“ 最小下载速率 ”和“ 最小上传速率 ”进行设置，使它们保持与“ 最大下载速率 ”和“ 最大上传速率 ”的连动性，它们的值为您在设置“ 最大下载速率 ”和“ 最大上传速率 ”时，系统自动提供的值。

如果有客户有特殊情况需要设置“最小下载/上传速率”时，我们建议“最小下载/上传速率”与“平均下载/上传速率”的比值不大于 2:1。如果这个值设置过大，则会造成绝对带宽严重不足。如果用户使用 P2P 软件或下载文件比较多，还要降低这个比例。如果没有人下载，都是交互（如 MSN、QQ、IE 浏览）应用，可以适当增加这一个比例。以下举例进行说明。

例如，2M ADSL 接入时，有 32 个用户共享，则“平均下载速率”=2M/32= 64Kbit/s，这时可将“最小下载速率”设置为 64Kbit/s。这样可保证大家在带宽有限的情况下“公平优先”，各个用户基本上不能占用他人的带宽。这样的配置对使用 MSN，IE 浏览（不是下载），QQ 等应用的用户是非常好的保证，即使有人用 P2P 软件，对其他用户也不会有什么影响。

如果将“最小下载速率”设置为 256Kbit/s，“最小下载速率”与“平均下载速率”的比值=256:64=4:1，实际上就是允许带宽复用。如果大家一起使用，实际上谁也不能达到 256Kbit/s，就会出现即使有信用，也不能有最低带宽保证，更会出现无法透支信用的问题。不过，如果大家不是一起使用，尽管信用不良的用户仍不能借用别人的空闲带宽，但是，信用良好的用户却有可能借用一些空闲带宽。为什么只是“有可能”呢？这取决于用户的数量及空闲带宽。例如，如果有 15 个用户都希望借用，根据配置，每个用户可以借到 256Kbit/s-64Kbit/s=192Kbit/s，就需要 15*192Kbit/s=3Mbit/s 带宽才能满足需要，但总带宽只有 2Mbit/s，再除掉那些不需要借用的用户使用的带宽，可供借用的带宽实际上将远远小于 2Mbit/s，显然很多用户是借不到所需带宽的。此外，因为 P2P 软件都专门优化过对带宽的“挤压”能力，因此它借到带宽的概率要比普通应用大得多。

10.1.4.4 如何设置“管制时间”

“管制时间”主要就是对付 BT 下载等 P2P 应用的，而对一般的应用基本上没有影响。众所周知，P2P 软件“挤压”的能力要比其他应用强得多，如果管不住 P2P，其他应用是无法保障的。这里的 P2P 应用就是那些能长时间、大量占用带宽并影响其他人使用的应用的总称。CBT 算法对这类应用采取了一种主动的控制带宽的策略，具体请参考章节 10.1.1.3 中的“自适应惩罚机制”的涵义。

实践证明，如果设置了“管制时间”，P2P 应用的平均速度一般不会超过其他应用的平均速度。在实际应用中，如果使用 P2P 软件或者以其他方式持续大量下载的人较多，“管制时间”就可以设置得大一些；相反，上述应用比较少，则“管制时间”就可以设置得小一些。

例如，“最大下载速率”设置为 512Kbit/s，“最小下载速率”设置为 64Kbit/s，“管制时间”设置为 120s，那么，如果局域网中有某个用户使用 BT 下载，下载速度就可能会在 64Kbit/s~512Kbit/s 之间来回变化。具体地说，当该用户信用不良时，如果其下载速度超过了 512Kbit/s，系统将会将其下载速度限制在 512Kbit/s。若该用户的下载速度达到 1Mbit/s，系统就会强行将其速度降至 256Kbit/s，并持续 120s。120s 后，立即恢复对该用户的带宽供给，若此用户的下载速度再次达到 1Mbit/s 时，系统会再次强行将其速度降至一半，依次循环。此外，在管制期间，如果该用户的带宽还是能达到 512Kbit/s，系统将在原有降速一半的基础上再次降速一半，即降至 128Kbit/s，直至带宽降至 64Kbit/s。

10.1.4.5 如何恢复信用

当局域网中某用户因长时间大量下载透支的信用值比较大时，若使用 BT 等 P2P 软件的话，下载速度还是能够维持在设置的“ 最小下载速率 ”和“ 最大下载速率 ”之间，这时该用户还是在透支信用，信用在负增长。当停止使用 BT 下载后，其他普通应用（如 IE 浏览）就会受到很大限制，因为必须先还掉透支的信用值，才能用正常速度访问。

显然，如果某个用户透支信用过多，将会大大影响正常的上网应用，若希望快速恢复信用，则可采取以下方法：

1. 停止上网一段时间——方法 1

针对某主机采取这种方法时，“ 下载/上传信用值 ”恢复到 0 的时间为：“ 下载/上传信用值 ”÷“ 最小下载/上传速率 ”。比如说，“ 最小下载速率 ”为 64Kbit/s，当前的“ 下载信用值 ”是-3MB，那么，“ 下载信用值 ”恢复到 0 的时间=3Mbyte/64Kbit=384 秒。

2. 关机 10 分钟——方法 2

针对某主机采取这种方法时，“ 下载/上传信用值 ”恢复到初始信用的时间为固定值：10 分钟。

3. 手工强制恢复 ——方法 3

在***带宽业务—>带宽信用管理***的“ 带宽信用管理信息列表 ”中，先选中若干条目，再单击“ 清除 ”按钮，对应主机的“ 上传信用值 ”和“ 下载信用值 ”立即恢复到初始信用值。

第11章 安全配置

本章主要介绍如何配置基本选项、用户管理、策略库、ARP 欺骗防御、以及 DDoS 攻击防御功能。

11.1 基本选项

本节主要讲述***安全配置***—>***基本选项***的配置及使用方法。

本页面提供基本的网络安全防御配置，用来提升网络的安全性。通过在本页面进行简单地配置，可以有效防御 ARP 欺骗、DoS/DDoS 攻击、冲击波以及震荡波等常见病毒攻击；有效屏蔽 MSN、QQ 等即时聊天软件的使用；有效屏蔽 BT、迅雷搜索等常用 P2P 软件的使用；通过 NAT 会话数限制，可以有效对 P2P 海量下载软件以及蠕虫病毒的控制，避免部分主机占用过多系统资源和网络带宽。

图 11-1 基本选项配置

- 允许响应外部 PING：启用后，设备的各个广域网接口都能响应来自外网的 PING 请求。一般情况下，为安全性起见，请关闭此功能。只有在某些特别情况下，例如网络调试时，才需开启此功能；
- 启用 ARP 欺骗防御：启用此功能，并将局域网所有 PC 的 IP/MAC 全部绑定（可在***安全配置—>ARP 欺骗防御***中配置），设备就可以有效防御 ARP 欺骗攻击了；
- 启用 DoS/DDoS 攻击防御：启用后，设备将有效防御内网常见的 DoS/DDoS 攻击。目前，只能防御伪造源地址攻击。启用此功能后，设备将只允许源 IP 地址与 LAN 口 IP 地址在同一个网段的数据包通过，此时，三层交换机后的主机将不能通过设备访问外网；
- 启用冲击波等病毒防御：启用后，设备将有效防御冲击波、震荡波等常见病毒攻击。启用此功能后，设备将直接丢弃 LAN 口接收到的协议为 TCP，目的端口为 135、136、137、138、139、445、1025、5554、9996 的数据包，此时，局域网主机将无法访问外网主机提供的相关端口服务，例如 windows 文件共享服务、打印共享服务等；

- 禁止 QQ：选中后，就可以禁止局域网用户使用 QQ 聊天；
- 禁止 MSN：选中后，就可以禁止局域网用户使用 MSN 聊天；
- 禁止 P2P：选中后，就可以禁止局域网用户使用常用 P2P 软件。目前，可以禁止使用 BitComet、比特精灵，此外，还可以禁止迅雷搜索资源；
- 启用 NAT 会话数限制：选中后，可以限制局域网每台主机所能占用的“最大会话数”；如有需要，还可以分别限制每台主机所能占用的“最大 TCP 会话数”、“最大 UDP 会话数”以及“最大 ICMP 会话数”。如果不选中，将被设置为系统最大的会话数；
- 最大会话数：局域网每台主机所能占用的最大并发 NAT 会话数；
- 最大 TCP 会话数：局域网每台主机所能占用的由 TCP 协议构成的最大并发 NAT 会话数。构成 TCP 会话的主要应用有 WEB 浏览、FTP 文件传输、网络游戏、SMTP/POP3 邮件传输等；
- 最大 UDP 会话数：局域网每台主机所能占用的由 UDP 协议构成的最大并发 NAT 会话数。构成 UDP 会话的主要应用有 DNS 服务、网络游戏、TFTP 文件传输等；
- 最大 ICMP 会话数：局域网每台主机所能占用的由 ICMP 协议构成的最大并发 NAT 会话数。构成 ICMP 会话的主要应用有 PING 检测、网络扫描工具等。

- 更新策略：在“禁止 QQ”、“禁止 MSN”或者“禁止 P2P”栏，单击“更新策略”超链接，系统立即连接到指定 WEB 站点，下载并自动更新对应的策略库。更新成功后，相关配置立即生效。此外，还可以在***安全配置***—>***策略库***中的“策略库信息列表”中，查看并更新相关策略库。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 当某些局域网应用（比如网络游戏）发生连接速度变慢的情况时，可以适当提高“最大会话数”以及“最大 UDP 会话数”（或者“最大 TCP 会话数”）。注意，上述会话数设置过高可能会导致设备减弱甚至丧失防止 DDoS 攻击的能力；

2. 一般情况下，最大会话数不能设置得太小：建议“最大 NAT 会话数”和“最大 TCP 会话数”均不小于 100、“最大 UDP 会话数”不小于 50、“最大 ICMP 会话数”不小于 10，如果它们的值太小，将导致局域网用户不能上网或上网异常。

11.2 用户管理

本节主要讲述***安全配置—>用户管理***的配置及使用方法。

通过本页面提供的“ 用户管理信息列表 ”可以查看局域网当前所有主机的地址、速率等信息。该表还提供编辑功能，通过它可以进入“ 用户信息配置 ”页面，在该页面可以分别为各台主机进行个性化配置，即可以为每台主机分配不同的带宽、设置不同的 NAT 会话数限制、是否禁止使用 QQ/MSN/常见 P2P 软件等。

11.2.1 用户管理信息列表

表 11-1 用户管理信息列表

- 用户名 :如果是 IP/MAC 绑定用户或者是 DHCP 手工绑定用户，则显示为对应的“ 用户名 ”；否则显示为空；
- IP 地址：某用户的 IP 地址。单击某条记录的“ IP 地址 ”超链接，即可进入***安全配置—>用户管理—>用户信息配置***页面。若将鼠标移向 IP 地址超链接，将显示该用户的当前的生效配置（如表 11-1 所示）；
- MAC 地址：某用户的 MAC 地址；
- 绑定状态 :如果是 IP/MAC 绑定用户，则显示为“ 已绑定 ”，反之则显示为“ 未绑定 ”；
- 下载速率（Kbit/s）：某用户当前实时下载速率，即两次刷新间隔内，该用户的平均

下载速率，单位：千比特/秒；

- 上传速率（Kbit/s）：某用户当前实时上传速率，即两次刷新间隔内，该用户的平均上传速率，单位：千比特/秒；
- NAT 会话数：某用户当前所占用的 NAT 会话的数量。单击某条记录的“ NAT 会话数 ”超链接，立即跳转到***上网监控***页面，自动查询对应用户的当前全部 NAT 会话记录，并在“ 查询结果列表 ”中显示查询结果；而且，通过该表还可以清除该用户的部分或全部 NAT 会话；
- 昵称：某用户的别名，如果未设置，则显示为空。
- 编辑：单击某条记录的“ 编辑 ”超链接，即可进入***安全配置—>用户管理—>用户信息配置***页面；
- 刷新：单击“ 刷新 ”按钮，可以查看“ 用户管理信息列表 ”的最新信息；

提示：可以在***安全配置—>用户管理—>用户信息配置***或者***高级配置—>IP/MAC 绑定***中配置 IP/MAC 绑定，在***基本配置—>DHCP 和 DNS 服务器***或者***高级配置—>DHCP—>DHCP 服务器***中配置 DHCP 手工绑定用户。

11.2.2 用户信息配置

提示：只有在***安全配置—>用户管理***的“ 用户管理信息列表 ”中，单击某条用户记录的“ IP 地址 ”或者“ 编辑 ”超链接之后，方可进入本页面，进而查看对应用户的状态信息，查看并修改该用户的 IP/MAC 绑定以及个性化配置信息。

11.2.2.1 个性化配置概述

在本页面可以进行个性化配置，个性化配置可以使单个用户独立于整个群体之外。个性化配置功能不仅可以大大加强管理的灵活性，并在一定程度上降低了管理员的工作量。

个性化配置包含以下参数：禁止 QQ、禁止 MSN、禁止 P2P、启用 NAT 会话数限制、最大会话数、最大 TCP 会话数、最大 UDP 会话数、最大 ICMP 会话数、昵称、最大下载速率、最大上传速率、最小下载速率、最小上传速率以及信用额度。

个性化配置中，“ 禁止 QQ ”、“ 禁止 MSN ”、“ 禁止 P2P ”以及“ 启用 NAT 会话数限制 ”相关参数对应的全局配置详见***安全配置—>基本选项***；“ 最大下载速率 ”、“ 最大上传速率 ”、“ 最小下载速率 ”、“ 最小上传速率 ”以及“ 信用额度 ”对应的全局配置详见***带宽业务—>带宽信用管理***；“ 禁止 QQ ”、“ 禁止 MSN ”、“ 禁止 P2P ” 、“ 最大下载速率 ”、“ 最大上传速率 ”、“ 最小下载速率 ”、“ 最小上传速率 ”以及“ 信用额度 ”对应的组策略详见***高级配置—>组管理。***

提示：个性化配置、组策略及全局配置的关系及配置步骤见附录 B“ 全局配置、组策略与个性化配置 ”。

11.2.2.2 用户信息配置

图 11-2 用户信息配置

- IP/MAC 绑定：选中后，就可以将当前用户设置为 IP/MAC 绑定用户，并使用“ IP 地址 ”作为“ 用户名 ”。只有选中“ IP/MAC 绑定 ”时，参数“ 允许该用户上网 ”才生效。注意，还可以在***高级配置—>IP/MAC 绑定***中配置 IP/MAC 绑定；
- 允许该用户上网：用于设置 IP/MAC 绑定用户的上网状态。若选中“ 允许该用户上网 ”，则表示允许该 IP/MAC 绑定用户上网，反之，则禁止上网；
- **个性化配置**：选中后，就可以对当前用户进行个性化配置。只有“ 个性化配置 ”被选中时，个性化配置相关参数才生效。
- 禁止 QQ：选中后，就可以禁止当前用户使用 QQ 聊天；
- 禁止 MSN：选中后，就可以禁止当前用户使用 MSN 聊天；
- 禁止 P2P：选中后，就可以禁止当前用户使用常用 P2P 软件。目前，可以禁止使用 BitComet、比特精灵，此外，还可以禁止迅雷搜索资源；
- 启用 NAT 会话数限制：选中后，可以限制当前用户所能占用的“ 最大会话数 ”；如有需要，还可以分别限制当前用户所能占用的“ 最大 TCP 会话数 ”、“ 最大 UDP 会

话数 ”以及“ 最大 ICMP 会话数 ”。如不选中，将被设置为系统的最大会话数。

- 最大会话数：当前用户所能占用的最大并发 NAT 会话数；
- 最大 TCP 会话数：当前用户所能占用的由 TCP 协议构成的最大并发 NAT 会话数。构成 TCP 会话的主要应用有 WEB 浏览、FTP 文件传输、网络游戏、SMTP/POP3 邮件传输等；
- 最大 UDP 会话数：当前用户所能占用的由 UDP 协议构成的最大并发 NAT 会话数。构成 UDP 会话的主要应用有 DNS 服务、网络游戏、TFTP 文件传输等；
- 最大 ICMP 会话数 :当前用户所能占用的由 ICMP 协议构成的最大并发 NAT 会话数。构成 ICMP 会话的主要应用有 PING 检测、网络扫描工具等；
- 昵称：当前用户的别名，如果未设置，则显示为空；
- 最大下载速率：当前用户的最大下载速率（单位：比特/秒）。其中，选项“ NoLimit ”表示不限制，即在下载方向不限速；“ Block ”表示禁止传送；
- 最大上传速率：当前用户的最大上传速率（单位：比特/秒）。其中，选项“ NoLimit ”表示不限制，即在上传方向不限速；“ Block ”表示禁止传送；
- 最小下载速率：正常情况下，当前用户可以保证的最小下载速率（单位：比特/秒）。其中，选项“ Disabled ”表示关闭 CBT DRR 功能；
- 最小上传速率：正常情况下，当前用户可以保证的最小上传速率（单位：比特/秒）。其中选项“ Disabled ”表示关闭 CBT DRR 功能；
- 信用额度：当前用户所能累计的信用的最大值（单位：字节）。其中，选项“ Auto ”表示由系统自动设置。

- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 如果某用户通过设备上网（比如网络游戏）发生连接速度变慢的情况时，可以适当提高“ 最大会话数 ”以及“ 最大 UDP 会话数 ”（或者“ 最大 TCP 会话数 ”）。注意，上述会话数设置过高可能会导致设备减弱甚至丧失防止 DDoS 攻击的能力；

2. 一般情况下，最大会话数不能设置得太小：建议“ 最大 NAT 会话数 ”和“ 最大 TCP 会话数 ”均不小于 100、“ 最大 UDP 会话数 ”不小于 50、“ 最大 ICMP 会话数 ”不小于 10，如果它们的值太小，将导致当前用户不能上网或上网异常；

3. 可以在***安全配置***—>***基本选项***页面，或者在***安全配置***—>***策略库***的“ 策略库信息列表 ”中，更新“ 禁止 QQ ”、“ 禁止 MSN ”、“ 禁止 P2P ”对应的策略库。

11.2.2.3 用户当前状态

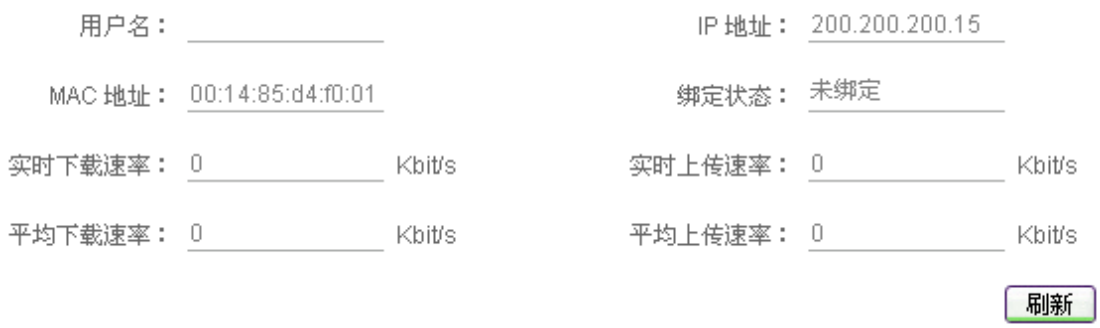


图 11-3 用户当前状态

“ 用户名 ”、“ IP 地址 ”、“ MAC 地址 ”、“ 绑定状态 ” 这几个参数的涵义同 “ 用户管理信息列表 ” 中的对应参数，这里不再重述。

- 实时下载速率：两次刷新间隔内，该用户的平均下载速率，单位：千比特/秒；
- 实时上传速率：两次刷新间隔内，该用户的平均上传速率，单位：千比特/秒；
- 平均下载速率：设备本次开机（或重启）至今所运行的时间内，该用户的平均下载速率，单位：千比特/秒；
- 平均上传速率：设备本次开机（或重启）至今所运行的时间内，该用户的平均上传速率，单位：千比特/秒。
- 刷新：单击 “ 刷新 ” 按钮，可以查看该用户的最新状态信息。

提示：“ 实时下载速率 ”、“ 实时上传速率 ” 分别与 “ 用户管理信息列表 ” 中的 “ 下载速率 ”、“ 上传速率 ” 相同。

11.3 策略库

本节主要讲述***安全配置—>策略库***的配置及使用方法。

11.3.1 策略库概述

在本页面，不仅可以查看各个策略库实例的相关信息，还允许加载、更新策略库。通过引入策略库，将复杂的多条策略当作一个策略库处理，并且可以直接通过 Internet 在线更新某个策略库或全部策略库，大大方便了用户的使用。目前，系统提供两种类型的策略库：路由策略库和防火墙策略库。以后，根据用户实际需求，艾泰科技将会陆续提供更多策略库。

路由策略库在***高级配置—>路由配置***中配置和引用，通过引入路由策略库，使用户无需一条条地添加静态路由，只需操作一次，就能批量配置大量电信路由或者网通路由，从而保证电信流量走电信线路、网通流量走网通线路。

防火墙策略库在***安全配置—>基本选项***或者***安全配置—>用户管理—>用户信息配制***中配置和引用，通过引入防火墙策略库，使用户无需设置大量业务策略，只需一键操作，就可实现禁止或允许局域网用户使用 QQ/MSN/P2P 了。

11.3.2 策略库信息列表

表 11-2 策略库信息列表

- 名称：该策略库的名称；
- 类型：该策略库的类型。目前，系统提供“ 防火墙 ”和“ 路由 ”两种类型的策略库；
- 说明：用于说明该策略库的作用；
- 引用状态：该策略库是否被引用。如果被引用，则显示为“ 已引用 ”，反之，则显示为“ 未引用 ”；
- 版本号：该策略库的版本号，版本号是根据策略库的创建日期生成的，例如 070701 就表示当前版本是 2007 年 7 月 1 号创建的。可以通过版本号来判断该策略库是否需要更新，版本号越大，就表示版本越新。
- 更新：单击某条策略库的“ 更新 ”超链接后，系统立即连接到指定 WEB 站点，下载并自动更新该策略库；
- 更新全部策略：单击“ 更新全部策略 ”超链接后，系统立即连接到指定 WEB 站点，

下载并自动更新“策略库信息列表”中的全部策略库；

- 删除：首先选中一些策略库条目，再单击右下角的“删除”按钮，即可删除被选中的策略库；
- 加载：用户可以加载自定义的策略库文件。

提示：

1. 仅系统提供的缺省策略库支持“更新”和“更新全部策略”操作；
2. 当成功更新了某条被引用的策略库之后，若该策略库为防火墙策略库，则配置立即生效。若该策略库为路由策略库，则必须进入***高级配置—>路由配置***页面，重新引用并保存之后，配置才能生效；
3. 禁止删除系统提供的缺省策略库。

11.3.3 策略库版本检查

图 11-4 策略库版本检查

- 策略库版本检查：
  自动检查：系统会在指定时刻触发一次策略库版本检查，并把检查结果保存在***系统管理—>系统信息***的“系统历史记录”中，此处主要记录经检查需要更新的策略库；
  不检查：系统不再主动检查策略库版本。
- 检查时间：当“策略库版本检查”设置为“自动检查”时，可以在这里设置策略库版本检查的触发时刻。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：当“策略库版本检查”设置为“自动检查”时，为保证相关功能工作正常，必须在***系统管理—>时钟管理***中准确地设置设备的时钟，使其与当地标准时间同步。

11.3.4 导入策略库

图 11-5 导入策略库

- 选择策略库文件：可在此输入策略库文件在本地计算机存放的路径，也可直接单击“ 浏览 ”按钮选择配置文件。
- 加载：首先在“ 选择策略库文件 ”中选择欲加载的策略库文件，再单击“ 加载 ”按钮，就可以将该策略库文件加载到设备中；同时，还会在“ 策略库信息列表 ”中增加该策略库的相关记录。

提示：在加载策略库文件的过程中请不要关闭设备电源，以避免不可预期的错误。

11.4 ARP 欺骗防御

本节主要讲述***安全配置—>ARP 欺骗防御***的配置及使用方法。

通过在本页面进行简单地配置：同时启用 ARP 更新限制和 ARP 广播功能，并将局域网当前所有 PC 的 IP/MAC 地址对全部绑定，就可以有效防止 ARP 欺骗攻击。

11.4.1 ARP 欺骗防御配置

图 11-6 ARP 欺骗防御配置

- 启用 ARP 更新限制：选中表示启用。启用 ARP 更新限制功能后，设备收到免费 ARP 包时，就会直接丢弃它，不更新动态 ARP 表。此功能可以有效保护设备免受 ARP 欺骗攻击；
- 启用 ARP 广播：选中表示启用。启用该功能后，设备将定期广播免费 ARP 包，从而向局域网主机广播自己 LAN 口的正确 ARP 信息。此功能可以有效保护局域网主机免受 ARP 欺骗攻击；
- ARP 广播间隔：选中“启用 ARP 广播”后，可以在这里设置设备广播免费 ARP 包的时间间隔，取值范围：100～5000、并且必须为 10 的整数倍，单位：毫秒。注意：若用户输入了非 10 的整数倍的数值，保存时，系统会采用直接舍弃零数的方式处理。例如，若输入 288，保存后，该值就自动被设置为 280。
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

11.4.2 动态 ARP 表管理

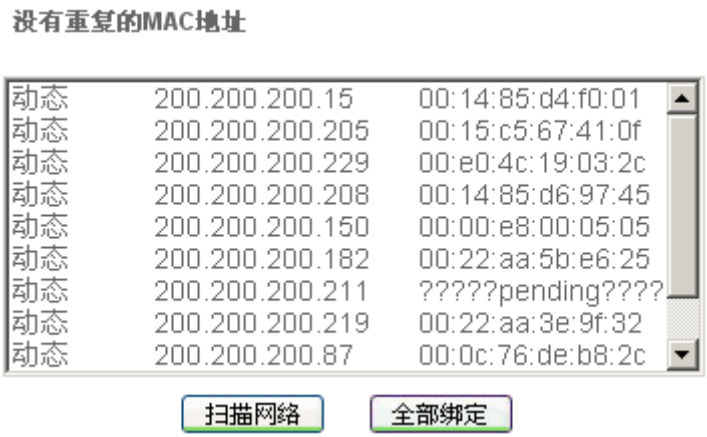


表 11-3 动态 ARP 表

- 扫描网络：单击“ 扫描网络 ”按钮，设备将立即在 LAN 口扫描局域网中所有开启的主机，学习最新的动态 ARP 信息，并在“ 动态 ARP 列表 ”中显示。通过此操作，可以获得局域网中当前的全部动态 ARP 信息；
- 全部绑定：单击“ 全部绑定 ”按钮，立即一次性将当前动态 ARP 表中的 IP/MAC 地址对全部绑定；
- IP/MAC 绑定：若希望删除部分或全部 IP/MAC 绑定条目，则可以直接单击“ IP/MAC 绑定 ”超链接，进入***高级配置—>IP/MAC 绑定***页面，然后在“ IP/MAC 绑定信息列表 ”中执行删除操作。

提示：

1. 如果用户希望一次性将局域网中所有主机的 IP/MAC 地址对全部绑定，那么，首先必须保证这些主机都是开启的，然后执行“ 扫描网络 ”操作，最后执行“ 全部绑定 ”操作。

2. 单击“ 扫描网络 ”或者“ 全部绑定 ”按钮后，系统还会检查动态 ARP 表中是否存在重复的 MAC 地址或 IP 地址，并在列表上方显示相关信息：如果显示“ 没有重复的 MAC 地址 ”，就表示局域网中不存在 ARP 欺骗攻击；如果显示出当前重复的 MAC 地址，就表示局域网中很可能存在 ARP 欺骗攻击；如果显示出当前重复的 IP 地址，就表示局域网中存在 IP 地址冲突或 IP 欺骗。

11.4.3 如何防止 ARP 欺骗攻击

通过在本页面进行简单地配置，就可以有效防止 ARP 欺骗攻击，配置步骤如下：

1. 同时启用 ARP 更新限制和 ARP 广播功能；
2. 开启局域网当前所有主机，再单击“ 扫描网络 ”按钮，设备将学习到最新的动态 ARP 信息；
3. 单击“ 全部绑定 ”按钮，将上一步学习到的动态 IP/MAC 地址对全部绑定。

执行完上述步骤之后，就可以有效防止设备和局域网主机遭受 ARP 欺骗攻击了。

11.5 DDoS 攻击防御

本节主要讲述***安全配置—>DDoS 攻击防御***的配置及使用方法。

提示：只有在***安全配置—>基本选项***中选中“启用 DoS/DDoS 攻击防御”之后，才能进入本页面配置 DDoS 攻击防御相关参数，在本页面选中“启用设备访问限制”，就可以大大提高设备防御内网 DDoS 攻击的能力了。

图 11-7 DDoS 攻击防御

- 启用设备访问限制：此功能可以有效防御一些来自内部网络针对设备本身的 DDoS 攻击。注意，启用此功能之后，就会限制局域网主机从 LAN 口访问设备，访问规则如下：
  1. 允许任意一台局域网主机使用 ICMP 协议访问设备；
  2. 允许任意一台局域网主机访问设备的 UDP 53、67、68 端口，从而保证设备提供的 DNS 代理、DHCP 服务器以及 DHCP 客户端功能能够正常使用；
  3. 只允许由“允许访问设备的主机”所指定的某段局域网主机访问设备的 WEB 和 TELNET 服务端口，禁止局域网其他主机访问 WEB 和 TELNET 服务端口，从而大大的降低了设备遭受 DDoS 攻击的可能性；
  4. 禁止局域网主机对设备的其他所有访问，例如，不能 telnet 到设备。
- 允许访问设备的主机：选中“启用设备访问限制”之后，可以在这里设置允许访问设备的主机。注：局域网中只有在起始地址和结束地址范围之内的主机才允许访问设备的 WEB 和 TELNET 服务端口；
- 允许通过设备的数据包：启用该功能后，设备将根据该值限制每秒通过 LAN 口的数据包个数，取值范围为 0~20000，建议设置为 300~600；
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

11.6 地址组

在进入***安全配置—>防火墙***页面使用“ 高级视图 ”配置防火墙策略之前，必须进入本页面配置防火墙策略所要引用的地址组。防火墙策略使用地址组来匹配设备接收数据包的源地址和目的地址，在服务和时间均匹配的情况下，如果设备接收数据包的源地址和目的地址在某条防火墙策略的源地址组和目的地址组范围内，就对该数据包执行此防火墙策略。

用户在创建一个地址组时，可以自定义此地址组包含的 IP 地址段，也可把已有地址组添加到此地址组中。地址组可以只包含 IP 地址段或只包含其他地址组，也可以既包含 IP 地址段又包含其他地址组，但最多只能包含 10 个 IP 地址段或地址组。

在防火墙中使用地址组，省掉了手工建立多条相同防火墙策略的麻烦。例如，内网中有多个不连续的 IP 地址段，而这些 IP 地址段访问外网的权限又相同，可以配置这些地址段属于同一地址组，然后做一条使用此地址组的防火墙策略即可同时对它们的数据包进行控制。

11.6.1 地址组配置

图 11-8 创建地址组

- 地址组名：自定义地址组的名称，不能重复，取值范围为 1~11 位字符或 1~5 个汉字；
- 所属区域：选择新建地址组所属的区域：
- 新地址：输入欲添加到地址组中的 IP 地址段；
- 已有地址：显示已存在的地址组，可把已有地址组添加到“ 地址范围列表 ”中；
- 地址范围列表：显示地址组包含的 IP 地址段或地址组；
- “ =〉 ”：用于将自定义的 IP 地址段或已有地址组添加到“ 地址范围列表 ”中；
- “ <= ”：用于将“ 地址范围列表 ”中的 IP 地址段或地址组导入到“ 新地址 ”或“ 已有地址 ”框中；
- 删除：用于删除“ 地址范围列表 ”中的 IP 地址段或地址组；
- 保存：单击“ 保存 ”按钮，地址组配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 地址组名称不区分大小写，即地址组“ A ”和“ a ”指的是同一个地址组，在配置时一定要注意。
2. 在配置地址组包含其它地址组时，一定要注意，如果某个地址组已经包含了其它地址组，则这个地址组不能再配置属于其它地址组。

配置地址组：首先输入自定义的地址组名并选择所属区域，然后在“ 新地址 ”配置框中输入 IP 地址段，再单击“ => ”将此 IP 地址段添加到“ 地址范围列表 ”中，可连续添加多个 IP 地址段；也可在“ 已有地址 ”框中选中一个或多个地址组名，单击“ => ”将已有地址组添加到“ 地址范围列表 ”中，最后单击“ 保存 ”按钮即可。

编辑地址组：如果想修改某个地址组的信息，在“ 地址组信息列表 ”中单击此地址组的“ 地址组名 ”或“ 编辑 ”超链接，其配置信息即填充到地址组配置框中，如果想修改地址组包含的 IP 地址段，在“ 地址范围列表 ”中选中此 IP 地址段，单击“ <= ”按钮将此 IP 地址段导入到 “ 新地址 ”配置框中，修改此地址段，保存后修改成功；如果想删除某个 IP 地址段或地址组，在“ 地址范围列表 ”中选中它，单击“ 删除 ”按钮并保存后即可将其从该地址组中删除。

可在“ 地址组信息列表 ”中查看已配置的地址组信息。如表 11-4 所示。

表 11-4 地址组信息列表

- 编辑：如果想修改某个地址组，只需在“ 地址组信息列表 ”中单击“ 地址组名 ”或“ 编辑 ”超链接，其信息即会填充到地址组配置框内，修改并单击“ 保存 ”按钮即可；
- 删除：选中欲删除的一个或多个地址组，单击右下角的“ 删除 ”按钮，即可删除。注意：您无法删除已经在防火墙策略中引用的地址组，必须先修改或删除所有引用它的防火墙策略，才能删除此地址组。

11.7 服务组

在进入***安全配置—>防火墙***页面进行防火墙策略配置之前，必须进入本页面为防火墙策略配置服务组。

防火墙策略使用服务组来匹配设备接收数据包的源 MAC 地址、协议、源端口、目的端口以及包内容等信息。设备提供了普通服务、URL、关键字、DNS 和 MAC 地址 5 种服务类型。在每种服务类型下，用户均可以自定义服务，也可以把已有服务添加到服务组中。

11.7.1 服务组配置

图 11-9 服务组配置

- 服务组名：自定义新服务组的名称，不能重复，取值范围为 1~11 位字符或 1~5 位汉字；
- 服务类型：设备提供了普通服务、URL、关键字、DNS 和 MAC 地址五种服务类型；
  - 普通服务：用来匹配设备接收数据包的协议和端口；
  - URL：用来过滤 URL 网址，可控制用户对站点及网页的访问；
  - 关键字：用来过滤 HTML 页面中的关键字，如果某个网页里包含了你定义的关键字（如色情、法轮功、赌博等），那么设备将直接屏蔽这个网页；
  - DNS：用来设置是否对某域名进行 DNS 解析；
  - MAC 地址：用来过滤某特定源 MAC 地址的数据包。
- 新服务：由用户自定义的新服务，不同的服务类型下需要配置的新服务参数不同；
- 已有服务：显示设备中已存在的服务，系统预定义了 38 种普通服务；
- 服务组列表：显示服务组包含的服务；
- “ =〉 ”：用于将自定义的新服务或已有服务添加到“ 服务组列表 ”中；
- “ <= ”：用于将“ 服务组列表 ”中的服务导入到“ 新服务 ”或“ 已有服务 ”框中；
- 删除：用于删除“ 服务组列表 ”中的服务；
- 保存：单击“ 保存 ”按钮，配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. 服务组最多可配置包含 10 个服务或其它服务组。
2. 服务组名不区分大小写，即服务组“ A ”和“ a ”指的是同一个服务组，在配置时一定要注意。
3. 在配置服务组包含其它服务组时，一定要注意，如果某个服务组已经包含了其它服务组，则这个服务组不能再配置属于其它服务组。

配置服务组：首先输入自定义的服务组名并选择要配置的服务类型，然后根据需要配置新服务，并单击“ => ”将配置的新服务添加到“ 服务组列表 ”中，可连续配置多个新服务；也可在“ 已有服务 ”框中选中一个或多个服务，单击“ => ”将已有服务添加到“ 服务组列表 ”中，最后单击“ 保存 ”按钮即可。

编辑服务组：如果想修改某个服务组的信息，首先在“ 服务组信息列表 ”中单击此服务组的“ 服务组名 ”或“ 编辑 ”超链接，其配置信息即填充到服务组配置框中。如果想修改某个用户自定义的服务，在“ 服务组列表 ”中选中此服务，单击“ <= ”按钮，即可在“ 新服务 ”配置框中修改此服务；如果想删除某个服务，在“ 服务组列表 ”中选中此服务，单击“ 删除 ”按钮即可，上述操作必须在单击“ 保存 ”按钮后才生效。

可在“ 服务组信息列表 ”中查看配置的服务组信息，如表 11-5 所示。

服务组信息列表 5/100

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	服务组名	服务组类型	服务组范围	编辑
☐	cc	普通服务	telnet;(T(20-23,20-23));	编辑
☐	bb	URL	(L(www.sina.com));(L(www.utt.com.cn));	编辑
☐	dd	关键字	(K(法轮功));(K(游戏));	编辑
☐	aa	MAC	(M(0022aabbccdd));(M(001122aabbcc));	编辑
☐	ee	DNS	(D(www.baidu.com.cn));	编辑

☐ 全选 / 全不选 删除

表 11-5 服务组信息列表

- 编辑：如果想修改某个服务组，只需在“ 服务组信息列表 ”中单击“ 服务组名 ”或“ 编辑 ”超链接，其信息即会填充到配置框内，修改并单击“ 保存 ”按钮即可；
- 删除：选中欲删除的一个或多个服务组，单击右下角的“ 删除 ”按钮，即可删除。
  注意：您无法删除已经在防火墙策略中引用的服务组，必须先修改或删除所有引用它的防火墙策略，才能删除此服务组。

11.8 防火墙

本节主要讲述***安全配置—>防火墙***的功能及配置方法。

本页面由“ 防火墙策略配置 ”和“ 防火墙信息列表 ”两大部分组成，可使用“ 普通视图 ”和“ 高级视图 ”两种视图配置防火墙策略，通过这两种视图配置的防火墙策略均可同时在“ 防火墙信息列表 ”中显示。用户自定义的防火墙策略将按配置顺序或预先指定的位置排列在“ 防火墙信息列表 ”中。

11.8.1 防火墙功能介绍

11.8.1.1 使用防火墙功能的意义

Internet 发展的同时也带来了一些副作用，如出现了赌博、色情等和国家法律法规相悖的网站；宽带网络给大众提供快速冲浪的同时，网络蠕虫病毒也得到快速传播，给电脑使用者带来很大的威胁。各个机构需要连接到 Internet，因此也制定了具体的上网规则，如某些

地方规定公务员不能在上班时间炒股和通过即时消息聊天，企业不允许电脑使用者操作和工作无关的事情，家长需要能控制孩子的上网时间，蠕虫病毒和黑客攻击充斥网络，需要将它们挡在攻击电脑之前等，不一而足。

UTT 产品的防火墙功能就是为解决这个问题而开发的。灵活地运用防火墙功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户不同时段的 Internet 访问权限。在实际应用中，可根据各个机构的管理规则，在设备上配置相应的防火墙策略。例如对于学校用户，可通过配置防火墙策略设置学生不能访问游戏网站；而对于家庭用户，可配置只在指定的时间内允许孩子上网；对于企业用户，可配置财务部门的机器不能被互联网访问等。

11.8.1.2 防火墙工作原理

在设备中配置防火墙策略，可以监测流经设备的每个数据包。默认情况下，设备中没有配置任何防火墙策略，设备将转发接收到的所有合法的数据包。如果在某接口配置了防火墙策略，当数据包到达此接口后，它会取出此数据包的源 MAC 地址、源地址、目的地址、上层协议、端口号或包内容进行分析，并从策略表的顶端从上至下搜索策略表，查看是否有匹配的策略，并执行匹配的第一个策略所定义的动作：转发或丢弃。并且不再继续比较其余的策略。如果与所有的策略都不匹配，处于安全的考虑，设备将丢弃这个数据包。

11.8.1.3 普通视图

使用“普通视图”配置防火墙策略的目的是对进入 LAN 口的数据包进行控制。在 LAN IN 方向配置若干防火墙策略，可以控制局域网用户的上网行为，比如限制用户不能访问某些网站，或者只能访问某些网站，限制用户访问一些服务（如只允许访问 WWW 和电子邮件服务，其他服务如 TELNET 则禁止），或只允许一些主机访问 Internet 等等。灵活地运用防火墙功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户在不同时段的 Internet 访问权限。

防火墙策略的过滤条件包括：过滤类型、过滤内容、源地址、源端口、目的 IP 地址、目的端口、协议、时间段等。定义了这些过滤条件以后，就可以利用它们创建防火墙策略，并指定各条防火墙策略的动作（允许或禁止），从而对进入设备的数据包进行控制：转发或丢弃。

11.8.1.3.1 组选择

通过设置“组选择”可以指定防火墙策略要过滤的数据包的源 IP 地址，设备提供三种类型的源 IP 地址对象：工作组，个人用户以及 IPSSG 组。这三种类型的策略分别被称为工作组策略、个人用户策略及 IPSSG 组策略。

1. 工作组

一般情况下防火墙策略是针对工作组定义的，该工作组的地址范围即为该策略要过滤数据包的源 IP 地址。同一个工作组的用户的上网权限完全相同，你只需为工作组定义防火墙策略，而无需为每个用户分别定义防火墙策略。这样的话，不仅方便管理，还可以提高设备的工作效率。当然，你必须首先将上网要求相同的局域网用户定义在同一个工作组中，才能够为他们制定出正确而有效的防火墙策略。

当为某工作组配置了防火墙策略后，系统会自动生成该组的全局策略，默认是禁止该组除定义过的其他业务。工作组全局策略的名称为“ grpx_other ”，x 为阿拉伯数字，按照配置顺序依次为 1、2、3……。

2. 个人用户

同时，设备也允许针对个人用户定义防火墙策略，该个人用户的 IP 地址即为该策略要过滤的数据包的源 IP 地址。如果某个工作组中大部分用户的上网要求都基本相同，只有一个或几个用户有特别需求；或是某个用户突然有了新的上网要求时，就可以对这个用户单独定义防火墙策略。

注意，如果对某个人用户配置了防火墙策略，且该个人用户属于某个已经配置了防火墙策略的工作组，则该工作组的全局策略也对此个人用户起作用。

3. IPSSG 组

系统还提供一个默认工作组：IPSSG 组，包括局域网中没有定义防火墙策略的所有用户。允许针对 IPSSG 组定义防火墙策略，但其起始 IP 地址和结束 IP 地址（均为 0.0.0.0）均不能修改。

注意，如果配置了某个人用户策略，且该个人用户不属于任何已配置了防火墙策略的工作组，则 IPSSG 组策略也对该个人用户起作用。

11.8.1.3.2 过滤类型

可以通过设置“ 过滤类型 ”指定防火墙策略的过滤类型，设备提供三种过滤类型：IP 过滤、URL 过滤以及关键字过滤。这三种类型的防火墙策略，均支持根据时间段进行过滤。

1. IP 过滤

IP 过滤指对数据包的包头信息过滤，例如源 IP 地址和目的 IP 地址。如果 IP 头中的协议字段封装协议为 TCP 或 UDP，则再根据 TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤。

过滤类型为 IP 过滤时，可供设置的过滤条件包括：源 IP 地址、目的 IP 地址、协议、源端口、目的端口、时间段、动作等。

2. URL 过滤

URL 过滤指对 URL 网址过滤，根据 URL 中的关键字进行过滤，不仅可以控制局域网用户对站点的访问，还可以控制用户对网页的访问。

过滤类型为 URL 过滤时，可供设置的过滤条件包括：源 IP 地址、过滤内容（指 URL 地址）、时间段、动作等。

3. 关键字过滤

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果你在某个网页里发表了包含了定义的关键字（如色情、法轮功、赌博等）的言论，将会提交不成功。设备可同时支持对中、英文关键字的过滤。

过滤类型为关键字过滤时，可供设置的过滤条件包括：源地址、过滤内容（指网页中的关键字）、时间段、动作等。

11.8.1.3.3 防火墙策略的动作

防火墙策略的动作包括转发和丢弃，对应的“ 动作 ”分别为“ 允许 ”或“ 禁止 ”。当需要处理的数据包与某条已定义的防火墙策略相匹配时，如果该策略的“ 动作 ”是“ 允许 ”，那么设备将转发该数据包；如果该策略的“ 动作 ”是“ 禁止 ”，那么设备将丢弃该数据包。

11.8.1.3.4 防火墙策略的类型

在启用了防火墙策略之后，系统会形成七种防火墙策略：

1. 为使设备正常工作而自动生成的名称为“ lan ”、“ dns ”以及“ dhcp ”的系统缺省防火墙策略，它们分别用来允许访问 LAN 口、允许 DNS、DHCP 服务；
2. 自定义的个人用户策略，可能是禁止或允许某个人用户的某项上网业务；
3. 自定义的工作组策略，可能是禁止或者允许某工作组的某项上网业务；
4. 系统自动生成的某工作组的全局策略，默认是禁止该组除定义过的其他业务。当为某工作组定义防火墙策略后，系统会自动生成该组的全局策略，名称为“ grpx_other ”，x 为阿拉伯数字，按照配置顺序依次为 1、2、3……；
5. 自定义的系统默认（IPSSG）组策略，可能是禁止或者允许 IPSSG 组的某项上网业务，但是该组的起止 IP 地址不能修改；
6. 系统自动生成的 IPSSG 组的全局策略，默认是允许 IPSSG 组除定义过的其他业务，该防火墙策略的名称为“ pass ”；
7. 系统自动生成的全局策略（作用于局域网所有用户），允许所有数据包（包括其他非 IP 类型的包）通过，该防火墙策略的名称为“ generic ”。

11.8.1.4 高级视图

和“ 普通视图 ”相比，“ 高级视图 ”提供的功能更全面、更强大。使用“ 高级视图 ”配置的防火墙策略可对设备所有物理接口进入和外出的数据包进行控制，而使用“ 普通视图 ”配置的防火墙策略只能对流进入 LAN 口的数据包进行控制。

进入（In） — 当数据包从指定接口进入设备时执行过滤。数据包来自与指定接口相连的网络，希望穿过设备到达另一接口并转发。当指定接口接收到数据包之后，将首先进行防火墙策略的匹配检查，并根据匹配策略定义的动作处理该数据包：转发或丢弃。

外出（Out） — 当数据包从指定接口离开设备时执行过滤。数据包来自与另一接口相连的网络，已经穿过设备到达指定接口，并希望从该接口转发。当指定接口接收到数据包之后，将进行防火墙策略的匹配检查，并根据匹配策略定义的动作处理该数据包：转发或丢弃。

“ 高级视图 ”中通过引用地址组和服务组配置防火墙策略，减少了手工配置多条防火墙策略的麻烦，大大减少了管理员的工作量。例如，内网中有多个不连续的 IP 地址段，而这些 IP 地址段访问外网的权限又相同，可以配置这些地址段属于同一地址组，然后做一条使用此地址组的防火墙策略即可同时对它们的数据包进行控制。

11.8.1.4.1 地址组

通过设置防火墙策略的“ 源地址组 ”和“ 目的地址组 ”来匹配设备接收数据包的源 IP

地址和目的 IP 地址。设备中存在两种地址组，用户在***安全配置—>地址组***中配置的地址组和系统默认地址组。系统默认地址组包括“ Inter_all ”和“ Extern_all ”，分别表示内部所有地址和外部所有地址。

11.8.1.4.2 服务组

通过设置防火墙策略的“ 服务组 ”来匹配设备接收数据包的源 MAC 地址、协议、端口号以及包内容等信息。可在防火墙策略中引用系统预定义的服务，也可引用用户自定义的服务组。您可以针对服务组创建防火墙策略，而无需为服务组包含的每个服务单独创建防火墙策略，大大简化了管理员的工作量。例如，您可以把 telnet、pop3 以及 http 等多个服务配置属于同一服务组，这样您就可以通过配置一条防火墙策略控制对这些服务的访问。关于服务组的更多信息，请参见“ 11.7 服务组 ”。

11.8.1.4.3 防火墙策略的动作

防火墙策略的动作包括转发和丢弃，对应的“ 动作 ”分别为“ 允许 ”或“ 禁止 ”。当需要处理的数据包与某条已定义的防火墙策略相匹配时，如果该策略的“ 动作 ”是“ 允许 ”，那么设备将转发该数据包；如果该策略的“ 动作 ”是“ 禁止 ”，那么设备将丢弃该数据包。

11.8.1.4.4 系统缺省防火墙策略

除了用户自定义的防火墙策略外，设备还会自动生成系统缺省防火墙策略，不同接口和方向上的系统缺省防火墙策略不同。下面将分别介绍这些系统缺省防火墙策略的涵义。

接口和方向	系统缺省防火墙策略	说明
LAN IN	“ lan ”、“ dns ”以及“ dhcp ”	始终位于列表的最上方，并且“ lan ”不在列表中显示。它们分别用来允许访问 LAN 口、允许 DNS、DHCP 服务。
	“ pass ”	IP 包的全局策略，默认是允许所有的 IP 包通过，始终显示在“ 防火墙信息列表 ”的最后。
	“ generic ”	全局策略，允许所有数据包（包括其他非 IP 类型的包）通过，位于“ pass ”的后面，但它不在“ 防火墙信息列表 ”中显示。
LAN OUT	“ lanoutpass ”	IP 包的全局策略，默认是允许所有的 IP 包通过，始终显示在“ 防火墙信息列表 ”的最后。
	“ lanoutgene ”	全局策略，允许所有数据包（包括其他非 IP 类型的包）通过，位于“ lanoutpass ”的后面，但它不在“ 防火墙信息列表 ”中显示。

WAN**X** IN	“ wan**x**inpass ”	IP 包的全局策略，默认是允许所有 IP 包通过，始终显示在“ 防火墙信息列表 ”的最后。
	“ wan**x**ingene ”	全局策略，允许所有数据包（包括其他非 IP 类型的包）通过，位于“ wan**x**inpass ”的后面，但它不在“ 防火墙信息列表 ”中显示。
WAN**X** OUT	“ wan**x**outpass ”	IP 包的全局策略，默认是允许所有 IP 包通过，始终显示在“ 防火墙信息列表 ”的最后。
	“ wan**x**outgene ”	全局策略，允许所有数据包（包括其他非 IP 类型的包）通过，位于“ wan**x**outpass ”的后面，但它不在“ 防火墙信息列表 ”中显示。
备注：“ WAN**X** ”中的“ **X** ”取值范围为 1~4，分别表示设备的 WAN1~WAN4 口。		

表 11-6 系统缺省防火墙策略

注意：所有的系统缺省防火墙策略都不可删除，且只能在列表中编辑其动作。

11.8.2 配置防火墙策略

用户可使用“ 普通视图 ”或“ 高级视图 ”两种视图模式进行防火墙策略配置。为方便配置，减少管理员工作量，强烈建议您使用“ 高级视图 ”配置防火墙策略。

使用“ 普通视图 ”配置的防火墙策略只能控制进入 LAN 口的数据包，而使用“ 高级视图 ”配置的防火墙策略可对设备所有物理接口的进入和外出数据包进行控制。

下面将分别介绍如何使用“ 普通视图 ”和“ 高级视图 ”配置防火墙策略。

11.8.2.1 普通视图

使用“ 普通视图 ”配置的防火墙策略是对进入 LAN 口的数据包进行控制的，在创建一条防火墙策略之前，您必须完成以下任务：

- 进入***高级配置—>工作组***页面为所要创建的防火墙策略定义工作组；
- 进入***基本配置—>时间段***页面为所要创建的防火墙策略定义生效的时间段。

下面将分别介绍 IP 过滤、URL 过滤以及关键字过滤这三种不同的过滤类型下，防火墙策略配置中各参数的涵义，以及注意事项。

11.8.2.1.1 防火墙策略配置—IP 过滤

图 11-10 配置防火墙策略—普通视图

- 策略名：自定义防火墙策略的名称，不能重复，取值范围为 1～11 个字符或 1~5 个汉字；
- 普通视图：设备提供“ 高级视图 ”和“ 普通视图 ”两种视图模式配置防火墙策略，此处选“ 普通视图 ”进行配置；
- 组选择 :该防火墙策略控制的局域网用户，即源 IP 地址范围。提供三种类型的选项：用户自定义的工作组组名、“ 新个人用户 ”及“ IPSSG ”。
  - 组名：为某个工作组配置防火墙策略时，需选择其“ 组名 ”，选定后，右边的两个下划线将分别显示其起始 IP 地址和结束 IP 地址，禁止修改这两个 IP 地址；
  - 新个人用户：如果选择“ 新个人用户 ”，则可以直接在本页面定义一个新个人用户并为它配置防火墙策略。定义时，需要在右边的第一个下划线中输入该个人用户的 IP 地址，单击鼠标后，该 IP 地址将自动填充到第二个下划线；
  - IPSSG：为系统默认组，配置防火墙策略时，需选择“ IPSSG ”。该组作用于局域网中没有配置防火墙策略的所有用户，右边的两个下划线将都显示为 0.0.0.0，禁止修改；
- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“ IP 过滤 ”；
- 协议：该防火墙策略的协议类型。
  供选择的协议如下：6（TCP）、17（UDP）、1（ICMP）、2（IGMP）、4（IPINIP）、47（GRE）、50（ESP）、51（AH）、89（OSPF）、9（IGRP）、46（RSVP）以及 0（所有）。其中，“ 0（所有）”表示所有协议。
  附录 C 提供了常用协议号与协议名称的对照表；

- 常用服务提示：提供使用 TCP 协议或 UDP 协议的常用服务端口。其中，选项“ 所有 ”表示所有端口：即 1～65535 端口。
  选择某个端口号（服务）后，系统自动将该端口号填充到“ 目的起始端口 ”和“ 目的结束端口 ”；特别地，若选择“ 所有 ”，则“ 目的起始端口 ”和“ 目的结束端口 ”分别填充为 1 和 65535。
  附录 D 提供了常用服务端口与服务名对照表；
- 目的起始端口、目的结束端口：该防火墙策略的目的起始端口和结束端口，通过它们可以指定一段范围的目的端口。如果只定义一个目的端口，则将它们设置成同一个值，取值范围均为 1～65535；
- 目的起始地址、目的结束地址：该防火墙策略的目的起始 IP 地址和结束地址，通过它们可以指定一段范围的目的 IP 地址。如果只定义一个目的 IP 地址，则将它们设置成同一个值；
- 源起始端口、源结束端口：该防火墙策略的源起始端口和结束端口，通过它们可以指定一段范围的源端口。如果只定义一个源端口，则将它们设置为同一个值。取值范围均为 1～65535；
- 插入位置（之前）：该防火墙策略的插入位置，选项为已配置防火墙策略的“ 策略名 ”及系统缺省策略“ pass ”。“ pass ”为 IPSSG 组的全局策略。
  - 策略名：选择某“ 策略名 ”后，该防火墙策略将插入到选定的策略之前；
  - pass：选择“ pass ”后，该防火墙策略将插入到策略“ pass ”之前；
- 动作：该防火墙策略的执行动作，选项为“ 允许 ”或“ 禁止 ”。
  - 允许：允许与该防火墙策略匹配的数据包通过，即设备将转发该数据包；
  - 禁止：禁止与该防火墙策略匹配的数据包通过，即设备将丢弃该数据包；
- 时间段：该防火墙策略生效的时间，不设置为所有时间。如果配置之后需要删除，可以选择“ 时间段 ”下拉框中的空选项。如果该时间段已经过期，系统将认为此条策略没有时间限制。
- 保存：防火墙策略配置参数生效；
- 重填：恢复到修改前的配置参数。

11.8.2.1.2 防火墙策略配置——URL 过滤

图 11-11 防火墙策略配置——URL 过滤

“策略名”、“组选择”、“插入位置（之前）”、“动作”、“时间段”这几个参数的涵义同“IP 过滤”类型中的相关参数，这里不再重述，请参考相关描述。

- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“URL 过滤”；
- 过滤内容：该防火墙策略欲过滤的 URL 地址。取值范围：1~31 个字符。
  URL 过滤是根据 URL 的关键字进行过滤的，当访问的网页的 URL 中含有与“过滤内容”完全匹配的字段时，就认为是匹配该策略的。这里可输入一个完整的域名，这时，该域名开头的所有网页都被匹配；也可输入域名的子字符串，这时，URL 中包含该子字符串的所有网页都被匹配，从而实现对某个站点的所有网页的过滤。下面，举几个例子进行说明：
  例 1，如果输入 www.sina.com.cn，那么以 www.sina.com.cn 开头的所有网页都将匹配该策略，如 www.sina.com.cn/index.jsp，但是 tech.sina.com.cn 开头的网页却不被匹配。
  例 2，如果输入 www.utt.com.cn/bbs/，则以 www.utt.com.cn/bbs/ 开头的所有网页都将匹配该策略，从而控制对 utt 这个站点中 bbs 页面的访问。
  例 3，如果输入 sina.com，那么所有出现 sina.com 和 sina.com.cn 的网页都被匹配，相当于整个 sina 站点都被匹配，当然，此时以 tech.sina.com.cn 开头的网页将被匹配。
- 保存：防火墙策略配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：

1. URL 地址中，英文字符不区分大小写。输入 URL 时，请不要包含 http://。另外，也不支持使用通配符“*”或者“?”来代表任意字符。

2. URL 过滤不能控制用户可以使用网页浏览器访问的其它服务。例如，URL 过滤不能控制对 ftp://ftp.utt.com.cn 的访问。在这种情况下，需通过配置 IP 过滤类型的防火墙策略来禁止或允许 FTP 连接。

11.8.2.1.3 防火墙策略配置——关键字过滤

图 11-12 防火墙策略配置——关键字过滤

“ 策略名 ”、“ 组选择 ”、“ 插入位置（之前）”、“ 动作 ”、“ 时间段 ” 这几个参数的涵义同 “ IP 过滤 ” 类型中的相关参数，这里不再重述，请参考相关描述。

- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择 “ 关键字过滤 ”；
- 过滤内容：该防火墙策略欲过滤的关键字，指网页上的关键字。支持中、英文两种输入方式，取值范围：1~31 个字符；其中，一个中文汉字由 2 个字符组成。此外，允许输入含空格的字符串，一个空格为 1 个字符。注意，一条策略只允许设置一个关键字，因此，当输入的字符串中含有空格时，也当作一个关键字处理。
- 保存：防火墙策略配置参数生效；
- 重填：恢复到修改前的配置参数。
- **提示**：

1. 对于过滤类型为 “ 关键字 ” 的防火墙策略，一般情况下，动作都设置为 “ 禁止 ”，这样，当用户在某网站提交含有已设置的关键字的网页内容时，将不能提交成功；
2. 关键字为英文时，不区分大小写；并且，输入关键字时，不支持使用通配符 “ * ” 或者 “ ? ” 等来代表任意字符。

11.8.2.1.4 个人用户防火墙策略的配置方法及注意事项

如果希望对某个人用户定义防火墙策略，有以下两种方法：

- 方法 1——先在***高级配置***—>***组管理***中配置只包含一个用户的工作组，然后在本页面的 “ 组选择 ” 中选择其 “ 组名 ”，即可为该用户配置防火墙策略；
- 方法 2——直接在本页面的 “ 组选择 ” 中选择 “ 新个人用户 ”，然后在右边的第一个下划线中输入该个人用户的 IP 地址，即可为该用户配置防火墙策略。

采用方法 2 时，需注意以下两点：

1. 在本页面配置了新个人用户防火墙策略后，在***高级配置***—>***组管理***的 “ 组信息列表 ”

中将增加该用户的信息记录，“ 组名 ”为该用户的 IP 地址。因此，在为该个人用户继续配置其他防火墙策略时，就需要在“ 组选择 ”中选择其“ 组名 ”（即 IP 地址）；

2. 在本页面可以删除为该个人用户配置的防火墙策略，但无法删除其地址信息，只能在***高级配置—>组管理***的“ 组信息列表 ”中删除。

11.8.2.2 高级视图

在使用“ 高级视图 ”创建一条防火墙策略前，您必须完成以下任务：

- 进入***安全配置—>地址组***页面为所要创建的防火墙策略定义地址组；
- 进入***安全配置—>服务组***页面为所要创建的防火墙策略定义服务组；
- 进入***基本配置—>时间段配置***页面为所要创建的防火墙策略定义生效的时间段。

下面将介绍 “ 高级视图 ”中各配置参数的涵义。

图 11-13 配置防火墙策略—高级视图

- 策略名：自定义防火墙策略的名称，不能重复，取值范围为 1～11 个字符或 1~5 个汉字；
- 高级视图：此处选则“ 高级视图 ”进行配置；
- 接口：选择欲配置防火墙策略的物理接口；
- 方向：选择防火墙策略是对流入（IN）物理接口的数据包进行控制，还是对流出（OUT）物理接口的数据包进行控制；
- 源地址组：用来匹配设备接收数据包的源 IP 地址，当方向为“ IN ”时，显示和接口相关的用户自定义的地址组以及系统默认地址组；当方向为“ OUT ”时，显示所有地址组；
  - 系统默认地址组“ Inter_all ”表示内部网络的所有地址；
  - 系统默认地址组“ Extern_all ”表示外部网络的所有地址；
- 目的地址组：用来匹配设备接收数据包的目的 IP 地址。显示所有用户自定义的地址

组以及系统默认地址组；

- 服务组：用来匹配设备接收数据包的源 MAC 地址、协议、端口号等信息。显示所有用户自定义的服务组以及系统预定义的服务，设备中预定义了 telnet、smtp、web、pop3 等服务，“ All_service ”表示所有服务；
- 插入位置（之前）：选择当前防火墙策略的插入位置，选项为用户自定义的防火墙策略和系统缺省防火墙策略；
- 动作：该防火墙策略的执行动作，选项为“ 允许 ”或“ 禁止 ”；
  - 允许：允许与该防火墙策略匹配的数据包通过，即设备将转发该数据包；
  - 禁止：禁止与该防火墙策略匹配的数据包通过，即设备将丢弃该数据包；
- 时间段：选择防火墙策略生效的时间，不设置为所有时间。如果配置之后需要删除，可以选择“ 时间段 ”下拉列表中的空选项。如果该时间段已经过期，系统将认为此条策略没有时间限制；
- 保存：单击“ 保存 ”按钮，所做的配置生效；
- 重填：恢复到修改前的配置参数。

11.8.2.3 全局配置

使用“ 普通视图 ”或“ 高级视图 ”配置设备某接口和方向的防火墙策略后，必须在“ 全局配置 ”中启用相应的防火墙策略，在此接口和方向上配置的防火墙策略才生效。

图 11-14 全局配置

- 接口：选择所要启用防火墙策略的物理接口；
- 方向：选择在指定物理接口的“ IN ”或“ OUT ”方向启用防火墙策略；
- 启用防火墙：打勾表示启用，启用后，在指定接口和方向上配置的防火墙策略才生效；
- 保存：配置参数生效；
- 重填：恢复到修改前的配置参数。

11.8.3 防火墙信息列表

11.8.3.1 防火墙信息列表的显示

在“ 防火墙信息列表 ”上方的下拉框中选择某接口和方向后，即可在列表中查看该接口和方向上的防火墙策略信息。

如果某条防火墙策略的“ 视图 ”显示为“ 普通 ”，则表示此策略是使用“ 普通视图 ”配置的，列表中显示的参数“ 源地址组、目的地址组、服务组 ”对它没有任何意义。

如果某条防火墙策略的“ 视图 ”显示为“ 高级 ”，则表示此策略是使用“ 高级视图 ”配置的，列表中显示的参数“ 过滤类型、过滤内容、协议、源起始地址、源结束地址、源起始端口、源结束端口、目的起始地址和目的结束地址 ”对它没有任何意义。


接口 LAN 方向 IN

防火墙信息列表 5/195

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	策略名	视图	动作	时间段	源地址组	目的地址组	服务组	过滤类型	过滤内容	协议
☐	dns	普通	允许					IP过滤		17(UDP)
☐	dhcp	普通	允许					IP过滤		17(UDP)
☐	方法	普通	允许					IP过滤		6(TCP)
☐	xx	高级	允许	worktime	sc	sc	cc	IP过滤		0(所有)
☐	pass	普通	允许					IP过滤		0(所有)

☐ 全选 /全不选 删除

表 11-7 防火墙信息列表


接口 LAN 方向 IN

防火墙信息列表 5/195

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

源起始地址	源结束地址	源起始端口	源结束端口	目的起始端口	目的结束端口	目
0.0.0.0	0.0.0.0	0	0	53	53	
0.0.0.0	0.0.0.0	0	0	67	68	
192.168.16.200	192.168.16.200	1	65535	21	21	
0.0.0.0	0.0.0.0	0	0	0	0	
0.0.0.0	0.0.0.0	0	0	0	0	

☐ 全选 /全不选 删除

表 11-8 防火墙信息列表（续表 11-7）


接口 LAN 方向 IN

防火墙信息列表 5/195

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

源起始端口	源结束端口	目的起始端口	目的结束端口	目的起始地址	目的结束地址	编辑
0	0	53	53	0.0.0.0	0.0.0.0	编辑
0	0	67	68	0.0.0.0	0.0.0.0	编辑
1	65535	21	21	0.0.0.0	0.0.0.0	编辑
0	0	0	0	0.0.0.0	0.0.0.0	编辑
0	0	0	0	0.0.0.0	0.0.0.0	编辑

☐ 全选 /全不选 删除

表 11-9 防火墙信息列表（续表 11-8）

- 编辑：如果想编辑某一条防火墙策略，只需单击它的“ 策略名 ”或“ 编辑 ”超链接，其信息就会填充到相应的编辑框内，可修改它，再单击“ 保存 ”按钮，修改完毕；
- 删除：选中一条或多条防火墙策略，单击右下角的“ 删除 ”按钮，即可删除被选中的防火墙策略。

  注意：不能删除“ 防火墙信息列表 ”中的系统缺省防火墙策略，只能修改其动作。

11.8.4 防火墙策略的排列顺序

11.8.4.1 LAN IN 方向

由于使用“ 普通视图 ”和“ 高级视图 ”均可配置 LAN IN 方向的防火墙策略，故 LAN IN 方向的防火墙策略在列表中的排列顺序分三种情况：

一. 只使用“ 普通视图 ”配置防火墙策略

<table>
<tr><th>顺序</th><th colspan="2">类型</th><th>名称</th><th>备注</th></tr>
<tr><td rowspan="8">从上至下</td><td rowspan="3" colspan="2">系统缺省策略</td><td>lan</td><td rowspan="3">始终位于最上方，而且，“lan”未在“防火墙信息列表”中显示，不可编辑删除。“dns”、“dhcp”只可编辑其“动作”，不可删除。</td></tr>
<tr><td>dns</td></tr>
<tr><td>dhcp</td></tr>
<tr><td colspan="2">个人用户策略</td><td>自定义</td><td>由用户自定义的个人策略，始终位于工作组策略之上。</td></tr>
<tr><td rowspan="2">工作组策略</td><td>自定义的工作组策略</td><td>自定义</td><td rowspan="2">“grpx_other”只允许修改其“动作”。工作组策略始终位于IPSSG组策略之上。</td></tr>
<tr><td>工作组全局策略</td><td>grpx_other</td></tr>
<tr><td rowspan="2">IPSSG组策略</td><td>自定义的IPSSG组策略</td><td>自定义</td><td rowspan="2">“pass”始终位于自定义的IPSSG组策略之下，而且，始终在“防火墙信息列表”的最后显示，不可删除，只能编辑其动作。</td></tr>
<tr><td>IPSSG组全局策略</td><td>pass</td></tr>
<tr><td colspan="2">系统全局策略</td><td>generic</td><td>始终位于“pass”的下方，而且，未在“防火墙信息列表”中显示，不可编辑删除。</td></tr>
</table>

表 11-10 防火墙策略类别及排列顺序

一般情况下，所有的防火墙策略将按照如表 11-10 中的顺序排列在“ 防火墙信息列表 ”中，其中，按照从上到下的顺序依次是：最上面为“ lan ”、“ dns ”及“ dhcp ”这 3 条策略，之后是自定义的个人用户策略，然后是工作组策略，最下面为“ pass ”和“ generic ”这 2 条策略。需要指出的是，“ lan ”和“ generic ”这 2 条系统自动生成的策略未在“ 防火墙信息列表 ”中显示。

对于工作组策略来说，缺省情况下，工作组策略将按照配置时的顺序从上到下依次排列，自定义的工作组策略将自动位于该组全局策略上方，但用户可以通过参数“ 插入位置 ”指定或调整某工作组策略的位置，并且，只能是在某工作组内部或工作组之间调整。注意，如果将某条自定义的工作组策略插入到该工作组全局策略下方，这条策略将不再起作用。

对于个人用户策略来说，缺省情况下，个人用户策略将按照配置时的顺序从上到下依次排列，但用户可以通过参数“ 插入位置 ”指定或调整某个人用户策略的位置，并且，只能在个人用户策略之间调整。

二. 只使用“ 高级视图 ”配置防火墙策略

只使用“ 高级视图 ”配置 LAN IN 方向的防火墙策略时，防火墙策略在“ 防火墙信息列

表”中从上到下的排列顺序依次是：最上面是“lan”、“dns”以及“dhcp”这 3 条系统缺省防火墙策略，之后是自定义的防火墙策略，最下面是“pass”和“generic”这 2 条系统缺省防火墙策略，需要注意的是：“lan”和“generic”这 2 条策略未在“防火墙信息列表”中显示。

对于用户自定义的防火墙策略，如果没配置插入位置，它将从列表顶端从上至下比较列表中防火墙策略的源地址组，如果找到第一条相同源地址组的策略，则继续比较下一条策略的源地址组，直到找到一条与自己的源地址组不同的策略后，不再向下比较并排列在此策略的上方。如果在列表中没有找到与自己源地址组相同的策略，此策略将排列在系统缺省策略“pass”的上方。

提示：

1. 用户自定义的服务类型为“DNS”的防火墙策略将自动位于系统缺省防火墙策略“dns”的上方；
2. 用户可以通过参数“插入位置”指定或调整某防火墙策略的位置。
3. 系统缺省防火墙策略“pass”始终排列在列表的最下方，不可调整其位置。

三. 同时使用上述两种策略配置防火墙策略

在列表中即存在使用“普通视图”配置的防火墙策略，又存在使用“高级视图”配置的防火墙策略的情况下，如果用户使用“普通视图”配置了一条防火墙策略，此防火墙策略在查找插入位置时，会认为使用“高级视图”配置的防火墙策略不存在。插入方法同情况一。同样，如果用户使用“高级视图”配置了一条防火墙策略，此防火墙策略在查找插入位置时，如果遇到一条使用“普通视图”配置的防火墙策略，会认为它不存在，跳过去继续比较下一条策略。插入方法同情况二。

11.8.4.2 其他接口和方向

对于用户自定义的防火墙策略，如果没有配置插入位置，它将从列表顶端从上至下比较列表中防火墙策略的源地址组，如果找到第一条相同源地址组的策略，则继续比较下一条策略的源地址组，直到找到一条与自己的源地址组不同的策略，不再继续比较并排列在它的前面。如果在列表中没有找到与自己源地址组相同的策略，将按照配置顺序从上往下排列。

提示：

1. 用户可以通过参数“插入位置”指定或调整某条防火墙策略的位置。
2. 系统自动生成的 IP 包的全局策略始终排列在列表的最后，不可调整其位置。

11.8.5 防火墙策略的执行顺序

当某接口接收到一个数据包后，设备将从“防火墙信息列表”的顶端开始向下搜索该列表，查找与数据包的地址、协议、端口、包内容以及接收到数据包请求的时间相匹配的策略。匹配的第一个策略将被应用于此数据包，并且，后面的策略不再检查。如果没有找到匹配的策略，出于安全考虑，该数据包将被丢弃。

由于设备将会对数据包执行第一个匹配的策略所定义的动作，因此，必须按照从特殊到一般的顺序安排、配置策略。举个例子来说，要求禁止局域网用户使用 FTP 业务，允许其他所有业务。那么就需要先配置禁止 FTP 业务的策略，再配置允许所有业务的策略。

11.8.6 防火墙策略配置实例

11.8.6.1 普通视图

11.8.6.1.1 工作组策略配置实例

当配置了某工作组的防火墙策略后，系统会自动添加一个该工作组的全局策略，该策略的动作默认是禁止该工作组的所有服务，它结合该工作组已设置的其他策略形成该工作组完整的策略体系。在“防火墙信息列表”中，该工作组的全局策略将自动位于为该工作组自定义的防火墙策略的下方（可根据起止地址来判断该全局策略属于哪个工作组）。因此对于该工作组来说，当设备的物理接口收到一个数据包时，将优先匹配该工作组自定义的防火墙策略，当这些防火墙策略均不匹配后，才去匹配该工作组的全局防火墙策略。

例如，当一个工作组设置一个允许 FTP 的策略，并且该工作组的全局策略的动作为禁止，那么，在“防火墙信息列表”中，FTP 策略将位于该组全局策略的上方。所有来自该组的 FTP 连接都将与这个 FTP 策略匹配，于是被允许通过。而其它任何类型服务的连接请求都不会与此 FTP 策略匹配，于是，它们将去匹配该组全局策略，由于该组全局策略的动作为禁止，于是设备将禁止这条连接。

工作组的全局策略只允许编辑“动作”及“插入位置”。如果删除工作组的全局策略，IPSSG 组策略对该工作组用户也起作用。一般情况下，不要删除工作组的全局策略。

注意，可通过设置“插入位置”将某条自定义的工作组策略插入到该工作组全局策略下方，也可通过设置“插入位置”将某工作组全局策略移到该工作组某条自定义的防火墙策略的上方。上述任何一种情况下，对于某工作组来说，位于该工作组全局策略下方的自定义的防火墙策略将不再起作用。

下面将举例说明不同情况下，如何设置工作组的全局策略的动作。

需要说明的是：以下几个例子中的工作组“Sale”的具体配置可参见***高级配置—>组管理***中的“工作组配置实例”部分。时间段“worktime”和“freetime”的具体配置可参见***基本配置—>时间段配置***的“时间段配置实例”部分。

1. 如果要限制某一工作组只允许某些上网业务，那么该工作组的全局策略的动作应该设成禁止。

例如，要求配置只允许“Sale”组的 WEB 业务，禁止该组其他所有上网业务。

要配置的策略是：

自定义策略 1，允许“Sale”组的 WEB 业务；

系统会自动生成一条该组的全局策略 grp1_other，禁止该组用户的所有上网业务，如表 11-19、11-20、11-21 所示。

表 11-19 防火墙信息列表—实例一

表 11-20 防火墙信息列表—实例一

表 11-21 防火墙信息列表-实例一

2. 如果要限制某一工作组只禁止某些上网业务，那么该工作组的全局策略的动作应该设成允许。

例如，要求：只禁止“ Sale ”组的用户访问网站 http://www.playboy.com（IP 地址为 209.247.228.201）和网站 http://www.cnn.com（IP 地址为 64.236.24.12），允许该组其他所有上网业务。

1) 方法 1，过滤类型选择“ IP 过滤 ”

要配置的策略是：

自定义策略 1，禁止“ Sale ”组访问目的地址：209.247.228.201；

自定义策略 2，禁止“ Sale ”组访问目的地址：64.236.24.12；

系统会自动生成一条该组的全局策略 grp1_other，这时需将其动作修改成“ 允许 ”，如表 11-22、11-23、11-24 所示。

表 11-22 防火墙信息列表——实例二

表 11-23 防火墙信息列表——实例二

表 11-24 防火墙信息列表——实例二

2) 方法 2，过滤类型选择“ URL 过滤 ”

要配置的策略是：

自定义策略 1，禁止“ Sale ”组访问目的网站：www.playboy.com；

自定义策略 2，禁止“ Sale ”组访问目的网站：www.cnn.com；

系统会自动生成一条该组的全局策略 grp1_other，这时需将其动作修改成“ 允许 ”，如表 11-25、11-26、11-27 所示。

表 11-25 防火墙信息列表——实例二（2）

表 11-26 防火墙信息列表——实例二（2）

表 11-27 防火墙信息列表——实例二（2）

3. 如果要限制某一工作组的某些上网业务在不同时间段有不同的权限，那么该工作组的全局策略的动作应该设成禁止。

例如，要求：时间段“ worktime ”（工作时间）内只允许“ Sale ”组的 WEB 业务，时间

段“ freetime ”（业余时间）开放 Sale 组的所有业务。

要配置的策略是：

自定义策略 1，允许“ Sale ”组用户在时间段“ worktime ”的 WEB 业务；

自定义策略 2，允许“ Sale ”组用户在时间段“ freetime ”的所有业务；

系统会自动生成一条该组的全局策略 grp1_other，禁止该组其他所有上网业务，如表 11-28、11-29、11-30 所示。

接口 LAN 方向 IN

防火墙信息列表 6/195

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

	策略名	视图	动作	时间段	源地址组	目的地址组	服务组	过滤类型	过滤内容	协议
□	dns	普通	允许					IP过滤		17(UDP)
□	dhcp	普通	允许					IP过滤		17(UDP)
□	1	普通	允许	worktime				IP过滤		6(TCP)
□	2	普通	允许	freetime				IP过滤		0(所有)
□	grp1_other	普通	禁止					IP过滤		0(所有)

全选 /全不选 删除

表 11-28 防火墙信息列表——实例三

接口 LAN 方向 IN

防火墙信息列表 6/195

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

源起始地址	源结束地址	源起始端口	源结束端口	目的起始端口	目的结束端口	目的起
0.0.0.0	0.0.0.0	0	0	53	53	0.0
0.0.0.0	0.0.0.0	0	0	67	68	0.0
192.168.16.50	192.168.16.70	1	65535	80	80	0.0
192.168.16.50	192.168.16.70	0	0	0	0	0.0
192.168.16.50	192.168.16.70	0	0	0	0	0.0

全选 /全不选 删除

表 11-29 防火墙信息列表——实例三

接口 LAN 方向 IN

防火墙信息列表 6/195

1/2 第一页 上一页 下一页 最后页 前往 第 页 搜索

源起始端口	源结束端口	目的起始端口	目的结束端口	目的起始地址	目的结束地址	编辑
0	0	53	53	0.0.0.0	0.0.0.0	编辑
0	0	67	68	0.0.0.0	0.0.0.0	编辑
1	65535	80	80	0.0.0.0	0.0.0.0	编辑
0	0	0	0	0.0.0.0	0.0.0.0	编辑
0	0	0	0	0.0.0.0	0.0.0.0	编辑

全选 /全不选 删除

表 11-30 防火墙信息列表——实例三

11.8.6.1.2 个人用户策略配置实例

如前所述，如果某个工作组中大部分用户的上网需求都基本相同，但同时也有少数用户有特别需求；或是某个用户突然有了新的上网需求时，就需要对这个用户单独定义防火墙策略。

例如，要求：允许“ Sale ”组（配置同上一节）的 WEB 业务，禁止该组的其他所有上网业务。特别地，允许该组 IP 地址为 192.168.16.66 的用户在时间段“ freetime ”的所有上网业务。

要配置的策略是：

自定义策略 1，允许“ Sale ”组的 WEB 业务；系统会自动生成一条该组的全局策略 grp1_other，禁止所有业务；

自定义策略 2，允许 IP 地址为 192.168.16.66 的用户的所有上网业务；该策略将自动位于策略 1 的上方。

当然，也可以先配置策略 2，再配置策略 1。不管配置顺序如何，在“ 防火墙信息列表 ”中，如表 11-31、11-32、3-33 所示，该个人用户的防火墙策略将始终位于“ Sale ”组的防火墙策略的上方。

表 11-31 防火墙策略信息列表——实例四

表 11-32 防火墙策略信息列表——实例四

表 11-33 防火墙策略信息列表——实例四

11.8.6.1.3 源端口的应用实例

一般情况下，防火墙策略是为了控制局域网主机的上网行为，因此无需设置参数“源起始端口”和“源结束端口”，设备将自动开放所有源端口。上述两节中所提供的工作组和个人用户策略配置实例均是用来控制局域网主机的上网行为的。

但是，如果防火墙策略是为了限制 Internet 上的外网主机对局域网内部主机（比如某台服务器）的访问，就需要在该策略中指定“源起始端口”和“源结束端口”。

例如，要求：某网吧有一台游戏服务器（IP 地址为 192.168.16.200/24），现希望该服务器对外只提供某游戏服务（端口号为 7000、7100 和 7200，协议使用 TCP），并且只对它的另外两个连锁网吧开放（公网 IP 分别为：201.222.5.121/29 和 201.222.5.122/29）；同时，禁止该服务器的其他所有上网业务。要配置的相关策略是：

自定义策略 1，允许该服务器的源端口 7000 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

自定义策略 2，允许该服务器的源端口 7100 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

自定义策略 3，允许该服务器的源端口 7200 对指定目的 IP 地址（即 201.222.5.121/29 和 201.222.5.122/29）开放；

自定义策略 4，禁止该服务器的所有上网业务。

策略 1、2、3 的配置步骤类似，下面以策略 1 的配置步骤为例进行说明，如下图所示：

图 11-15 源端口的应用实例

第一步，在“策略名”中填入“1”；

第二步，在“组选择”中选择“新个人用户”，并在第一个下划线上填入“192.168.16.200”；

第三步，在“过滤类型”中选择“IP 过滤”；

第四步，“协议”选择“6（TCP）”，“常用服务提示”选择“所有”；

第五步，在“目的起始地址”和“目的结束地址”中分别填入“201.222.5.121”、“201.222.5.122”；

第六步，在“源起始端口”和“源结束端口”中均填入“7000”；

第七步，“动作”选择“允许”；

第八步，单击“保存”按钮，该策略配置完成。

注意，在配置策略 2 和策略 3 时，在“组选择”中只需直接选择“192.168.16.200”即可。

策略 4 的配置步骤如下：

第一步，在“策略名”中填入“4”；

第二步，在“组选择”中选择“192.168.16.200”；

第三步，“协议”选择“所有”；

第四步，“动作”选择“禁止”；

第五步，单击“保存”按钮，该策略配置完成。

提示：还必须在***高级配置—>NAT 和 DMZ 配置***的“NAT 静态映射”中为该服务器配置相关的 NAT 静态映射，该游戏服务器才能对外提供相关服务。

11.8.6.2 高级视图

使用“高级视图”可在设备所有物理接口的 IN 和 OUT 方向配置防火墙策略。一般情况下，在 LAN IN 方向配置防火墙策略来控制内网用户的上网访问权限（也可通过配置 WAN OUT 方向的防火墙策略来实现）；在 WAN IN 方向配置防火墙策略来控制外网用户对内网用户的访问（也可通过配置 LAN OUT 方向的防火墙策略来实现）。

为了减轻设备对数据包的处理负担，建议在接口的 IN 方向配置防火墙策略，即数据包一进入设备就进行策略检查，不符合策略的数据包将丢弃，而设备无需再对这些数据包进行路由、NAT 处理等操作，减轻了 CPU 的处理负担，提高了设备的效率。

11.8.6.2.1 实例一

某公司内部有研发、客服、财务、销售 4 个部门，这 4 个部门的员工所使用的 IP 地址段分别为 192.168.16.2~192.168.16.30 、 192.168.16.31~192.168.16.60 、 192.168.16.61~192.168.16.70、192.168.16.71~192.168.16.100。

要求：(1) 只允许研发部员工和财务部员工在上班时间的 WEB 和 FTP 业务，禁止其他业务，下班时间允许所有业务。

可通过自定义两条防火墙策略和系统自动生成的策略“pass”共同实现要求，“pass”始终位于列表的最后，默认是允许所有的 IP 包。

自定义策略 1； 允许研发部和财务部员工在上班时间的 WEB 和 FTP 业务；

自定义策略 2：禁止上班时间的其他业务。

a) 配置策略 1

第一步：在***基本配置—>时间段配置***中配置上班时间“worktime”；

第二步：在***安全配置—>地址组***中配置地址组“yfcw”，包括研发部（192.168.16.2~192.168.16.30）和财务部（192.168.16.61~192.168.16.70）的地址，如下图所示：

图 11-16 配置地址组“yfcw”

第三步：在***安全配置—>服务组***中配置服务组“web*ftp”，包括 WEB 和 FTP 服务；

图 11-17 配置服务组“ web*ftp ”

第四步：进入***安全配置—>防火墙***页面，输入策略号“ 1 ”，选择源地址组为 “ yfcw ”，目的地址组为“ Extern_all ”，服务组为 “ web*ftp ”，动作选择为“ 允许 ”，时间段选择为“ worktime ”，最后单击“ 保存 ”按钮。

图 11-18 配置策略 1

b) 配置策略 2

在***安全配置—>防火墙***页面，输入策略号“ 2 ”，选择源地址组为“ yfcw ”，目的地址组为“ Extern_all ”，服务组为“ All_service ”，动作选择为“ 禁止 ”，时间段选择“ worktime ”，最后单击“ 保存 ”按钮。

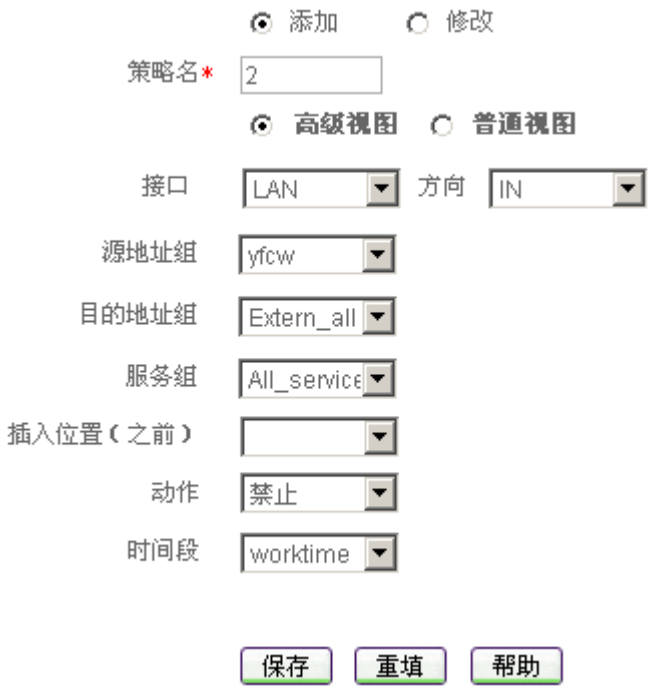


图 11-19 配置策略 2

c) 全局配置

必须启用设备 LAN 口 IN 方向的防火墙策略后，在 LAN IN 方向配置的防火墙策略才生效。

图 11-20 启用防火墙策略

11.8.6.2.2 实例二

某公司使用 UTT 3640 作为网络接入设备，内网用户通过 WAN1 口上网，IP 地址为 200.200.200.251。要求：(1) 禁止外部某一非法 IP 地址（202.106.11.22）对内网用户的恶意攻击；(2) 并且禁止内网用户访问带有 “ 法轮功 ”、“ 色情 ”、“ 台独 ” 等非法内容的网页。

可通过在 WAN1 IN 方向配置防火墙策略 “ 1 ”，禁止来自攻击 IP 地址的所有 IP 包来防止外部攻击。配置防火墙策略 “ 2 ”，禁止内网用户访问带有 “ 法轮功 ”、“ 色情 ”、“ 台独 ” 等内容的网页。

自定义策略 1：防外部攻击；

自定义策略 2：禁止内网用户访问带有 “ 法轮功 ”、“ 色情 ”、“ 台独 ” 等内容的网页。

a) 配置策略 1

第一步：进入***安全配置—>地址组***页面，配置名称为 “ a ” 和 “ b ” 的地址组，所属区域均选择 “ WAN1 ”，地址组 “ a ” 包含设备 WAN1 口的 IP 地址，地址组 “ b ” 包含攻击 IP 地址

202.106.11.22；

图 11-21 配置地址组“ a ”

图 11-22 配置地址组“ b ”

第二步：进入***安全配置—>防火墙***页面，输入策略号“ 1 ”，选择接口为“ WAN1 ”，方向为“ IN ”，选择源地址组为“ b ”，目的地址组为“ a ”，服务组选择“ All_service ”，动作选择为“ 禁止 ”，最后单击“ 保存 ”按钮。

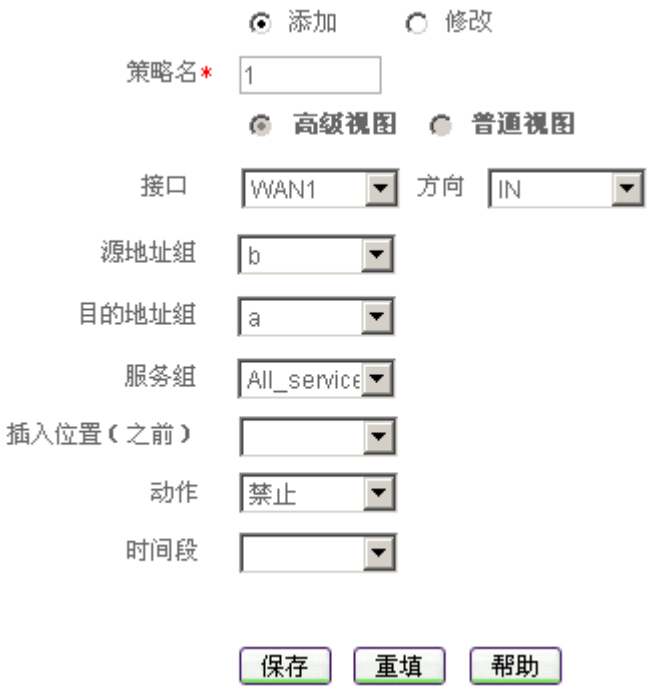


图 11-23 配置防火墙策略—实例二

b) 配置策略 2

第一步：进入***安全配置—>服务组***页面，自定义服务组名称为“ Key ”，服务类型选择为“ 关键字 ”，输入过滤内容为“ 法轮功 ”、“ 色情 ”、“ 台独 ”；

图 11-24 配置服务组“ Key ”

第二步：进入***安全配置—>防火墙***页面，自定义策略号为“ 2 ”，选择接口为“ WAN1 ”，方向为“ IN ”，选择源地址组为“ Extern_all ”，目的地址组为“ a ”，服务组为“ Key ”，动作为“ 禁止 ”，单击“ 保存 ”按钮，如下图所示。

图 11-25 配置策略 2

c) 全局配置

启用设备 WAN1 口 IN 方向的防火墙功能后，在该接口和方向上配置的防火墙策略才生效。

图 11-26 启用防火墙策略

附录 A 配置局域网中的计算机

本章讲述如何在 Windows95/98 环境下配置计算机的 TCP/IP 属性。

第一步 检查网络 IP 状态

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，在“已经安装了下列网络组件”中查看是否已安装网卡的驱动程序与 TCP/IP 协议，如图 A-1 所示，如果出现了“TCP/IP->网卡型号”选项，就表示已经安装：

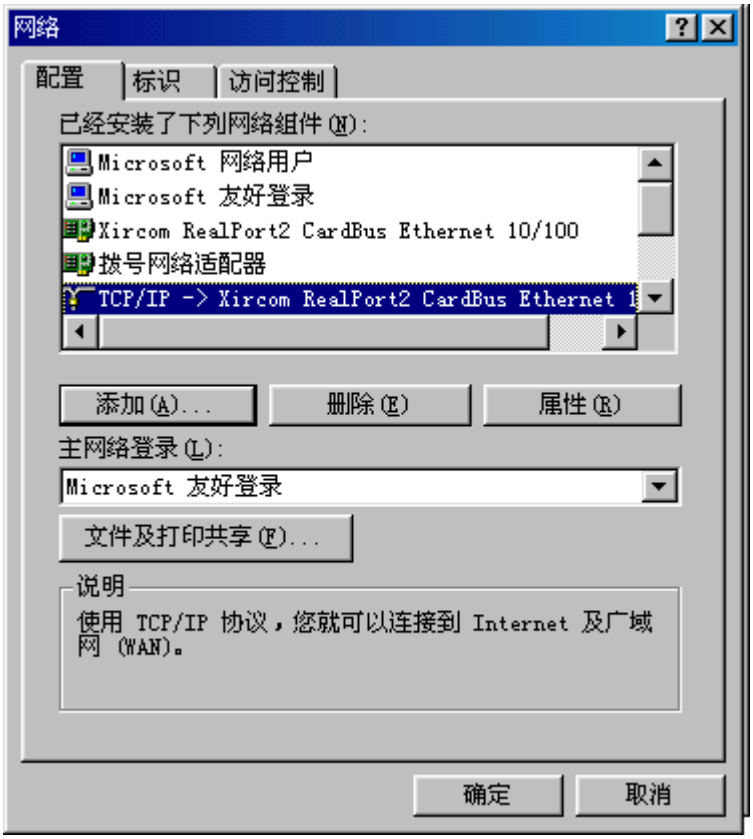


图 A-1 网络配置窗口

3. 如果没有安装网卡驱动程序及 TCP/IP 协议，首先需查阅网卡的原厂文件来安装匹配的网卡驱动程序。
4. 在安装网卡驱动程序之后，需添加 TCP/IP 传输协议。首先打开“网 络”窗口（步骤同前），如图 A-1 所示，再单击“添加”按钮，随后单击“协议”→“添加”→“Microsoft”→“TCP/IP 传输协议”即可。在指定的网卡完成添加 TCP/IP 协议后，需重启计算机来更新系统的网络设定，使其生效。

第二步 配置 TCP/IP 属性

下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

方法一 手工设置 IP 地址

1. 单击“开始”→“设置”→“控制面板”；
2. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，如图 A-1 所示，在“已经安装了下列网络组件” 选择“TCP/IP->网卡型号”选项，再单击“属性”按钮；
3. 单击“IP 地址”菜单进入“IP 地址”配置窗口，如图 A-2 所示，首先选中“指定 IP 地址”选项，然后在“IP 地址”中填入：192.168.16.X（X 在 2 至 254 之间），在“子网掩码”中填入 255.255.255.0；

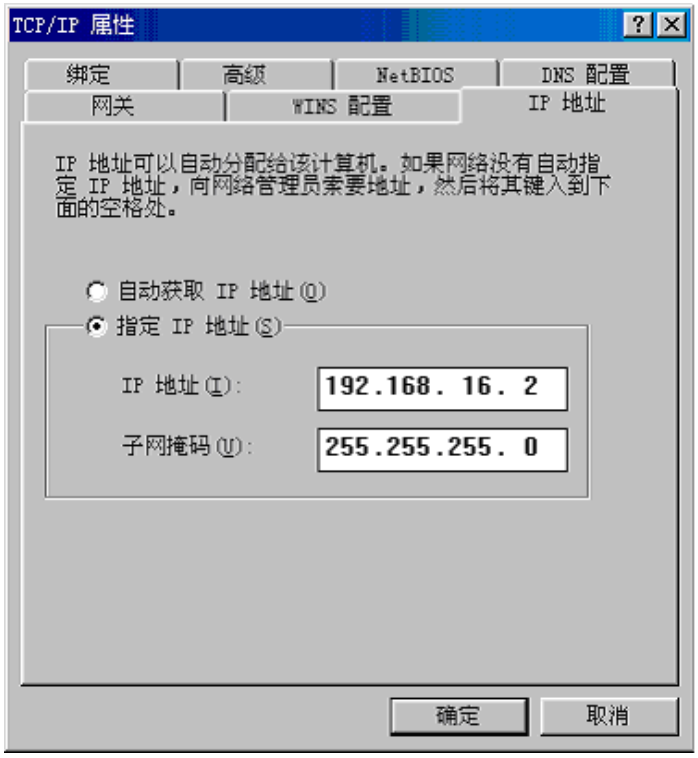


图 A-2 TCP/IP 属性 IP 地址配置窗口

4. 单击“网关”菜单进入“网关”配置窗口，如图 A-3 所示，首先在“新网关”选项中，填入设备的 LAN 口 IP 地址（出厂时为 192.168.16.1），然后单击“添加”按钮，新网关添加成功；

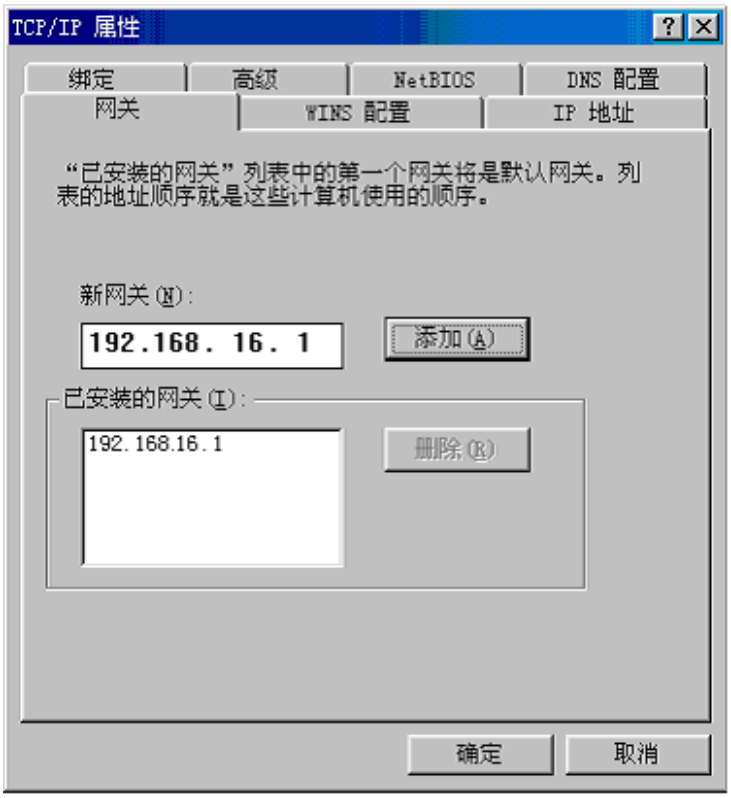


图 A-3 TCP/IP 属性网关配置窗口

5. 单击“ DNS 配置 ”菜单进入“ DNS 配置 ”窗口， 如图 A-4 所示，首先在“ 主机 ”和“ 域 ”中任意填入主机名和域名，然后在 “ DNS 服务搜索顺序 ” 中填入 ISP 所提供的 DNS 服务器的 IP 地址（可向 ISP 询问），单击 “ 添加 ” 按钮，DNS 配置成功；

图 A-4 TCP/IP 属性 DNS 配置窗口

6. 以上配置完成后，单击“确定”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

方法二 通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在设备的***基本配置—>DHCP 和 DNS 服务器***中激活 DHCP Server 功能（章节 4.3.1）；
2. 单击“开始”→“设置”→“控制面板”；
3. 双击“网络（network）”图标，单击“配置”菜单进入“配置”窗口，如图 A-1 所示，在“已经安装了下列网络组件” 选择“TCP/IP->网卡型号”选项，再单击“属性”按钮；
4. 单击“IP 地址”菜单进入“IP 地址”配置窗口，如图 A-5 所示，选中“自动获取 IP 地址”；

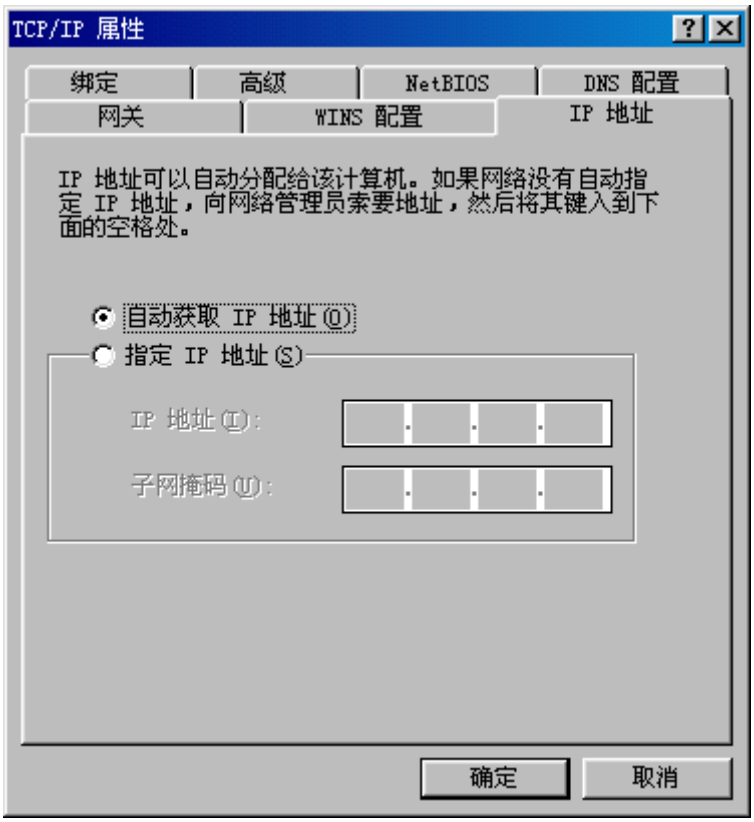


图 A-5 TCP/IP 属性 IP 地址配置窗口

5. 单击“网关”菜单进入“网关”配置窗口，如图 A-6 所示，在“新网关”中不用填入任何值（如果原先有设置，请删除）；

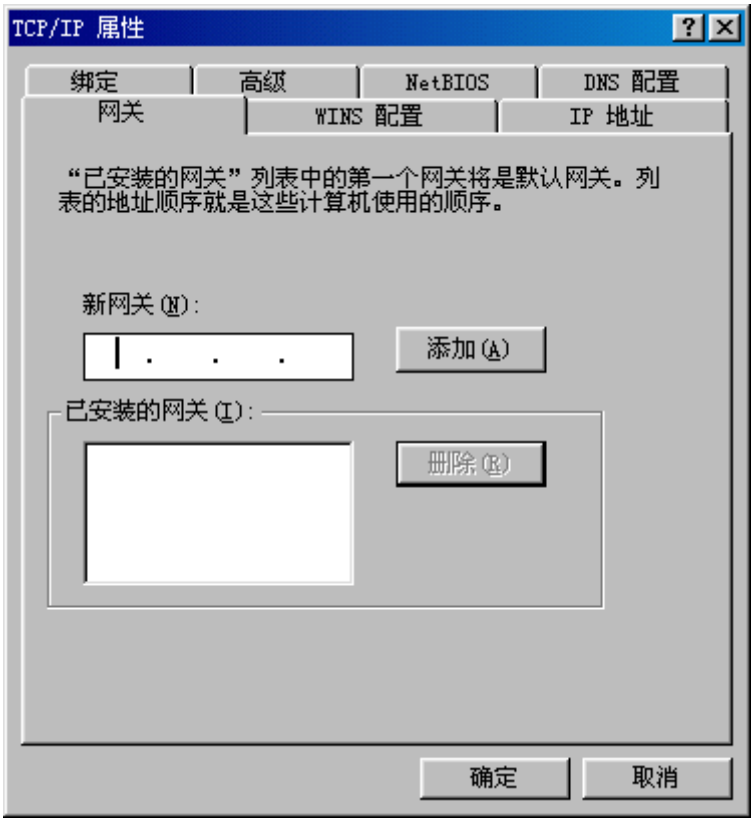


图 A-6 TCP/IP 属性网关配置窗口

6. 单击“ DNS 配置 ”菜单进入“ DNS 配置 ”窗口， 如图 A-7 所示，在 DNS 设置选项中选择“ 禁用 DNS ”；

图 A-7 TCP/IP 属性 DNS 配置窗口

7. 以上配置完成后，单击“确定”按钮，配置 TCP/IP 属性完成，重启计算机后配置才能生效。

第三步 浏览器设定

1. 单击“开始”→“程序”→“附件”→“通讯”→“Internet 连接向导”；
2. 选择“手动设置 Internet 连接或通过局域网（LAN）连接”，单击“下一步”按钮；
3. 选择“通过局域网（LAN）连接”，单击“下一步”按钮；
4. 清除“局域网 Internet 配置”中的所有选项，单击“下一步”按钮；
5. 在“想现在设置一个 Internet 邮件帐户吗？”中，选择“否”，单击“下一步”按钮；
6. 单击“完成”按钮，结束“Internet 连接向导”配置；

至此，TCP/IP 属性全部配置完成，现在已经可以正常使用浏览器、FTP client 或者其他的 Internet 客户端程序。

附录 B FAQ

1. ADSL 用户如何上网？

1) 首先，将 ADSL Modem 设置为桥模式（1483 桥模式）；
2) 确认 PPPoE 线路是标准拨号型的（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）；
3) 用网线将设备的 WAN 口与 ADSL Modem 相连，并将电话线连接到 ADSL Modem 的 Line 口；
4) 在***基本配置—>线路配置***中，配置 PPPoE 上网线路的相关参数（章节 5.1.2.1）；
5) 若是包月上网的用户，则可选择拨号类型为“自动拨号”。若是非包月上网的用户，则可选择拨号类型为“按需拨号”或者“手动拨号”，并且可以输入空闲时间，以防止忘记断线而浪费上网时间；
6) 若选择了“手动拨号”，则需在***基本配置—>线路配置***的“线路连接信息列表”（章节 5.1.1）中进行手动拨号；
7) 拨号成功后，在***基本配置—>线路配置***的“线路连接信息列表”中可以查看该线路的配置和状态信息（如表 B-1、B-2），比如“连接状态”（拨号成功后显示为“已连接”）、ISP 分配的“IP 地址”等信息。

线路连接信息列表 2/20

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

线路名称	物理接口	连接类型	连接状态	NAT状态	下行速率(bps)	上行速率(bps)
默认线路	WAN1	PPPoE(ad51753575)	已连接(持续:00:01:20:53)	启用	294k	47k

刷新

表 B-1 线路连接信息列表——查看 PPPoE 拨号线路信息

线路连接信息列表 2/20

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

连接状态	NAT状态	下行速率(bps)	上行速率(bps)	IP地址	子网掩码	网关地址
连接(持续:00:01:20:53)	启用	294k	47k	218.79.219.244	255.255.255.255	218.79.219.244

刷新

表 B-2 线路连接信息列表——查看 PPPoE 拨号线路信息（续表 B-1）

8) 在***系统状态—>系统信息—>系统历史记录***（章节 8.6.7）中，可以查看连接历史记录，如表 B-3 所示。

呼叫历史记录	呼叫结果
Session Up [x] PPPoE Up 00:0c:f8:f9:66:c6 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	PPPoE 拨号成功。
Call Terminated @clearSession: 1 Outgoing Call @51:1-1	物理连接无法建立，请检查线路是否正常（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）。
Call Terminated @clearSession: 1 Call Connected, on Line1, on Channel 0 Outgoing Call @51:1-1	物理已经建立，但是验证失败，请在***基本配置—>线路配置***中检查 PPPoE 用户名、密码配置是否正确。如果配置正确，请将验证方式修改成 CHAP 或者 NONE（如图 B-1），并且重启设备。

表 B-3 PPPoE 拨号历史记录

图 B-1 PPPoE 拨号配置（部分）

9) 在***系统状态—>路由和端口信息***的“路由表信息列表”中，可以查看 ISP 分配的“网关地址”，以及“路由状态”（必须看到 N，N 代表 NAT 启用）等信息；

路由表信息列表 27/27

1/3 第一页 上一页 下一页 最后页 前往 第 页 搜索

目的地址	网关地址	接口号	路由状态	优先级	跳数	使用次数	使用时间
0.0.0.0/0	218.79.219.244	ptp9	lugaN	60	1	15147	5647

表 B-4 路由表信息列表——实例一

10) 按照本手册附录 A 所述内容配置局域网计算机。

2. 固定 IP 接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；
2) 用网线将设备的 WAN 口与 ISP 网络设备相连；
3) 在***基本配置—>快速向导***或***基本配置—>线路配置***中，配置固定 IP 接入线路的相关参数；
4) 配置完成后，在***系统状态—>路由和端口信息***的“路由表信息列表”中，可以查看“路由状态”（必须看到 N，N 代表 NAT 启用）等信息，如表 B-5 所示；

表 B-5 路由表信息列表——实例二

5) 按照本手册附录 A 所述内容配置局域网计算机。

3. 动态 IP（Cable Modem）接入用户如何上网？

1) 确认线路正常（可以使用计算机测试）；

2) 用网线将设备的 WAN 口与 ISP 网络设备相连；

3) 在***基本配置—>快速向导***或***基本配置—>线路配置***中，配置动态 IP 接入线路的相关参数；

提示：某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会导致设备无法正常获得 IP 地址，此时需要将设备的 WAN 口 MAC 地址设置成和原有网络设备的 MAC 地址相同。在***基本配置—>线路配置***中，选择“连接类型”为“动态 IP 接入”，配置“广域网接口 MAC 地址”，单击“保存”按钮，重启设备后配置生效。

4) 在***基本配置—>线路配置***的“线路连接信息列表”中，可以查看动态 IP 接入时线路的配置和状态信息（如表 B-6、表 B-7），比如“连接状态”（正常连接时显示为“已连接”，并显示剩余租用时间）、ISP 分配的“IP 地址”、“网关地址”等信息。

表 B-6 线路连接信息列表——查看动态 IP 接入线路信息

表 B-7 线路连接信息列表——查看动态 IP 接入线路信息（续表 B-6）

5) 在***系统状态***—>***路由和端口信息***的“路由表信息列表”中，可以查看 ISP 分配的 IP 地址（“网关地址”）、“路由状态”（必须看到 N，N 代表 NAT 启用）等信息，如表 B-8 所示；

表 B-8 路由表信息列表——实例三

6) 按照本手册附录 A 所述内容配置局域网计算机。

4. 如何将设备恢复到出厂配置?

提示：下述方法将删除设备原来所有配置，请谨慎使用。

下面介绍将设备恢复到出厂配置的方法，按知道管理员密码和忘记管理员密码分别说明（注：本节中均以 Windows2000 环境为例进行说明）。

情况一：知道管理员密码

当用户知道管理员密码时，可通过下面的方法恢复设备的出厂配置。

步骤如下：直接进入***系统管理***—>***配置管理***页面，在“恢复出厂配置”配置栏中，单击“恢复”按钮，即可恢复出厂值。

情况二：忘记管理员密码

如果忘记了管理员密码，将无法进入 WEB 界面，可使用下面的方法恢复设备的出厂配置。

通过 RESET 按钮来恢复设备的出厂配置。

步骤如下：在设备带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，设备将恢复到出厂配置，并自动重启。

5. IP/MAC 绑定、工作组/地址组、与防火墙

本节主要讲述设备中，IP/MAC 绑定、工作组/地址组与防火墙的特点及其关系，目的是帮助大家更好地理解它们，并灵活地利用它们实现对用户上网行为的控制、加强网络的安全性。

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权（IP 业务管理）工作。在设备中，通过 IP/MAC 绑定功能解决用户的身份识别问题，通过防火墙功能实现对用户上网行为的控制。

A. IP/MAC 绑定

在 IP/MAC 绑定中，通过 IP/MAC 地址绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址作为用户唯一的身份识别标识，可以防止 IP 地址盗用、MAC 地址盗用以及 IP/MAC 欺骗等常见攻击。

对于没有明确身份鉴别要求（即没有进行 IP/MAC 地址绑定）的用户，系统默认的用户全局策略是允许访问。如果将此策略设为禁止，即在***高级配置***—> ***IP/MAC 绑定***的“ IP/MAC 绑定全局配置 ”中，不选中“ 允许非 IP/MAC 绑定用户 ”，那么将会拒绝所有身份无法识别的用户使用设备。

IP/MAC 绑定功能只能影响用户访问设备或通过设备访问其他网络（如 Internet），但不能影响局域网内部通信（或不经过该设备的通信）。也就是说，如果 IP/MAC 绑定用户修改了 IP 或 MAC，将不能访问设备或通过设备访问其他网络（如 Internet），但是不能影响局域网内部通信，比如网络邻居浏览。

B. 工作组

若干上网要求相同的局域网用户构成一个工作组，一个工作组通常包括多个 IP 地址连续的用户。这里，允许定义只有一个用户（工作组的起始 IP 地址和结束 IP 地址相同）的特殊工作组，我们将之称为个人用户。

C. 地址组

一个地址组可配置包含多个不连续的 IP 地址段或其它地址组，当若干上网要求相同的用户的 IP 地址不连续时，可配置他们属于同一个地址组，然后针对这个地址组统一配置防火墙策略。

D. 防火墙

在防火墙中，可使用“ 普通视图 ”设置各工作组用户的上网权限，也可使用“ 高级视图 ”设置各地址组用户的上网权限。

E. 关系

1) IP/MAC 绑定只能完成用户身份识别、不能控制用户上网行为，用户上网行为的控制是通过防火墙功能完成的；
2) 工作组/地址组由若干上网要求相同的用户组成；
3) 防火墙功能可以针对工作组或地址组用户创建防火墙策略，同一个工作组/地址组的用户的上网权限完全相同，从而，你只需为工作组/地址组定义防火墙策略，而无需为每个用户分别定义防火墙策略。同时，如有需要，也可针对个人用户创建防火墙策略；
4) 在设备中，首先通过 IP/MAC 绑定功能解决用户身份识别问题，然后将上网业务要

求相同的用户划分在同一个工作组或地址组中，再通过对工作组/地址组用户（及个人用户）定义不同的防火墙策略。这样，不仅实现了对用户身份的识别，还实现了对用户上网行为（包括上网权限和时间）的控制，从而保证了网络资源的有效利用及网络的安全性。

F. 功能实现过程

当用户有数据流量通过设备时，顺序发生以下动作：

1) 用户身份识别
   a) 如果是合法用户通过，该数据包进入 IP 业务管理处理；
   b) 如果用户身份非法，丢弃该数据包；
   c) 如果用户身份未知，根据系统的用户全局策略执行：
      i. 若允许未知用户，即在***高级配置—> IP/MAC 绑定***中，选中“ 允许非 IP/MAC 绑定用户 ”时，让该数据包通过，进入 IP 业务管理处理；
      ii. 若禁止未知用户，即在***高级配置—> IP/MAC 绑定***中，不选中 “ 允许非 IP/MAC 绑定用户 ”时，丢弃该数据包。

提示：

a) 合法用户指：其 IP 地址和 MAC 地址与***高级配置—> IP/MAC 绑定***的“ IP/MAC 绑定信息列表 ”中的某条目的 IP 地址和 MAC 地址完全匹配，且该条目的上网状态为 “ 允许 ”。
b) 不合法用户：其 IP 地址和 MAC 地址中只有一个与 “ IP/MAC 绑定信息列表 ” 中的某条目的 IP 地址或 MAC 地址匹配，另一个则不匹配；或者，其 IP 地址和 MAC 地址与 “ IP/MAC 绑定信息列表 ” 中的某条目的 IP 地址和 MAC 地址完全匹配，且上网状态为 “ 禁止 ”。
c) 身份未知用户：其 IP 地址或 MAC 地址均不与 “ IP/MAC 绑定信息列表 ” 中的任何条目的 IP 地址或 MAC 地址匹配，也就是除合法用户以及非法用户之外的所有用户。

2) 业务管理处理流程（包括时间段控制）

设备将从***安全配置—>防火墙***的 “ 防火墙策略信息列表 ” 的顶端开始向下搜索该表，查找第一个与数据包的地址、服务以及接收到数据包请求的时间相匹配的策略。匹配的第一个策略将被应用于数据包，将不再检查后面的策略。如果没有找到匹配的策略，出于安全考虑，该数据包将被丢弃。

注意，对于设置了时间段的防火墙策略来说，首先还需判断该时间段是否是有效时间段。当时间段有效期已过，该时间段无效，将不再起作用；如果需要时间段策略控制，必须重新配置该时间段。

G. 自定义用户身份及其业务权限

由以上分析可知，如果要配置局域网的用户及其上网的业务权限，就应该遵循以下步骤：

1） 规划局域网每个用户，确定用户是否拥有连接和通过设备的权限，以及这些用户上网所能使用的权限；
2） 将上网权限相同的用户合并到一个工作组或地址组中；
3） 根据上一步的规划为每个用户的计算机设置 TCP/IP 属性，并且记录下每个用户的 MAC 地址；
4） 在***高级配置—> IP/MAC 绑定***中，配置 IP 和 MAC 绑定（如果要禁止非允许的 IP/MAC 绑定用户连接和通过设备，请取消 “ 允许非 IP/MAC 绑定用户 ” 的选中）；

5） 根据上网权限相同的用户的 IP 地址是否连续配置工作组和地址组，工作组在***高级配置—>组管理***中配置，地址组在***安全配置—>地址组***中配置；
6） 在***系统管理—>时钟管理***中，校正设备当前系统时间；
7） 如果要限制用户的上网时间，在***基本配置—>时间段配置***中，配置时间段；
8） 在***安全配置—>防火墙***中，配置每个工作组或地址组的上网权限。

6. 全局配置、组策略与个性化配置

针对局域网中不同性质的用户一般对上网的要求不同这个问题，设备提供三种管理策略：全局配置、组策略以及个性化配置，大大加强了管理的灵活性，给用户提供了很大的方便。本节主要讲述这三者的关系及如何利用它们为局域网中的不同用户设置不同的上网权限。

1. 三者的共同点：

均提供以下参数的设置：禁止 QQ、禁止 MSN、禁止 P2P、最大下载速率、最大上传速率、最小下载速率、最小上传速率以及信用额度。

2. 三者的不同点：

全局配置作用于局域网中的所有用户。
组策略只作用于用户定义的某工作组内的所有用户。
个性化配置只作用于局域网中的单个用户。

3. 三者的优先级：

个性化配置>组策略>全局配置，当这三种策略发生冲突时，优先级高的策略生效。

为了帮助用户更好地理解这三者的关系，下面将举例来说明如何利用它们为局域网中不同的用户设置不同的策略。

某公司有三个部门：管理部门、技术部门和销售部门，该公司需求：允许所有人使用 MSN 聊天；禁止所有人使用 P2P 下载；只允许销售部门的员工使用 QQ 聊天；局域网中其他部门中用户的最大下载/上传速率为 256Kbit/s，而管理部门中用户的最大下载/上传速率为 512Kbit/s；特别地，管理部门中某用户 A 的最大下载/上传速率为 1Mbit/s。配置步骤如下：

A. 全局配置

1. 进入***安全配置—>基本选项***页面，选中“ 禁止 QQ ”、“ 禁止 P2P ”，并保存配置；
2. 进入***带宽业务—>带宽信用管理***页面，将“ 最大下载速率 ”和“ 最大上传速率 ”都设为“ 256Kbit/s ”，并保存配置。

B. 组策略

1. 进入***高级配置—>组管理***页面，把这三个部门划分为三个不同的工作组，在销售部门的组策略配置中，取消“ 禁止 QQ ”的选中，并保存配置；
2. 在管理部门的组策略配置中，把“ 最大下载速率 ”和“ 最大上传速率 ”都设为“ 512Kbit/s ”，并保存配置。

C. 个性化配置

进入用户 A 的用户信息配置页面，选中“ 个性化配置 ”，将“ 最大下载速率 ”和“ 最大

上传速率”都设为“1Mbit/s”，并保存配置。

提示：在***安全配置—>基本选项***和***带宽业务—>带宽信用管理***中所做的配置属于全局配置，它对局域网中的所有用户生效；在***高级配置—>组管理***页面所做的配置属于组策略，它只对用户定义的当前工作组内的所有用户生效；而在***用户信息配置***页面所做的配置属于个性化配置，它只对单个用户生效。

7. 如何发现使用带宽最大的用户？

设备提供了查看系统状态功能，可以在***系统状态—>NAT 统计***中，查看“NAT 统计信息列表”，即可发现使用带宽最大的用户。

A. 发现下载量最大的用户

在***系统状态—>NAT 统计***中，查看“NAT 统计信息列表”，查询“下载数据包/总数”，该百分比值越大，就表示下载数据包数量越多，该数值最大的用户就是局域网中通过 Internet 下载量最大的用户。

B. 发现上传量最大的用户

在***系统状态—>NAT 统计***（中，查看“NAT 统计信息列表”，查询“上传数据包/总数”，该百分比值越大，就表示上传数据包数量越多，该数值最大的用户就是局域网中通过 Internet 上传量最大的用户。

C. 发现上网最活跃的用户

在***系统状态—>NAT 统计***中，“查看 NAT 统计信息列表”，查询“当前连接数/总数”，该百分比值越大，就表示用户上网越活跃，该数值最大的用户就是局域网中当前上网最活跃的用户。

8. 如何诊断蠕虫病毒或者黑客攻击造成的设备使用异常的故障？

提示：以下各点仅在排除网络故障时作为参考，不作为发现网络病毒或各种攻击的依据。

A. 发现内部用户使用地址扫描软件扫描 Internet

【地址/端口扫描软件】在使用此类软件时，软件会在单位时间向目标地址或者目标网段发出大量的 ICMP/UDP 包或者 TCP 连接，以扫描目标地址是否存在或者是否有开放的端口。使用这些软件的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点设备负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以通过以下 3 种方式找出使用地址/端口扫描软件的用户。

1) 在***系统状态—>NAT 统计***的“NAT 统计信息列表”中，查看是否有“超限次数”大于 100 的用户。由于设备支持用户在单位时间内最多只能有 800 条 NAT 连接（这完全能保障正常上网的用户），超过的连接将被设备丢弃，并在“超限次数”里面增加记录，因而当“超限次数”大于 100 时，该用户很可能正在使用地址/端口扫描软件。
2) 在***系统状态—>NAT 统计***的“NAT 统计信息列表”中，查看是否有“上传数据包”数量

比“ 下载数据包 ”数量大很多的用户。由于地址/端口扫描软件在往外发送数据包的时候，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回到发送方，因而当某用户“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量时，该用户很可能正在使用地址/端口扫描软件。

3) 在***系统状态***—>***系统信息***的“ 系统历史记录 ”中，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded 192.168.16.221 ”），表示该 IP 地址的计算机 NAT 并发 session 超过了设备限定的最大 session 数，则该用户很可能正在使用地址/端口扫描软件。

提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

B. 发现局域网用户使用 DoS/DDos 方式攻击 Internet 主机

【DoS/DDoS 攻击】俗称洪水攻击、术语称拒绝服务攻击或称分布性拒绝访问。这种攻击方法在很短的时段内向某一网站发出大量信息，使其超出该网站自身的负荷能力而“ 无法对用户提供正常服务 ”，造成网站业务不能正常开展。使用这些攻击方式的客户端会发出很大的数据流量，如果这些流量过大，会造成网络节点设备负载过大，造成网络拥塞，影响其他用户的正常上网。

根据上述特点，可以根据以下方法找出使用地址/端口扫描软件的用户。

1) 在***系统状态***—>***NAT 统计***的“ NAT 统计信息列表 ”中，查看是否有“ 上传数据包 ”数量比其他用户大很多、“ 下载数据包 ”数量却很少的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，会向 Internet 发送大量的数据包，因此如果某用户的“ 上传数据包 ”数量比其他用户大很多、“ 下载数据包 ”数量却很少，那么该用户很可能正在进行 DoS/DDoS 攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

2) 在***系统状态***—>***NAT 统计***的“ NAT 统计信息列表 ”中，查看是否有“ 上传数据包 ”数量比“ 下载数据包 ”数量大很多的用户。由于当用户使用 DoS/DDoS 攻击方式攻击主机时，往往会伪造源地址，这样就会导致对方响应的数据包不能正常返回到发送方，因而当某用户“ 上传数据包 ”数量远远大于“ 下载数据包 ”数量时，该用户很可能正在进行 DoS/DDoS 攻击。

3) 在***系统状态***—>***系统信息***的“ 系统历史记录 ”中，如果发现某用户的 NAT exceeded 信息（例如显示出信息“ NAT exceeded 192.168.16.221 ”），表示该 IP 地址的计算机 NAT 并发 session 数超过了设备限定的最大 session 数，则该用户很可能正在进行 DoS/DDoS 攻击。

提示：解决措施，建议停止该用户正在使用的软件包、杀毒、重新安装操作系统。

C. 发现 RED_WORM（红色代码 Code red）类型的网络攻击型病毒

1) 在***系统状态***—>***用户统计***的“ 用户统计信息列表 ”中，查看是否有“ 发送数据包 ”数量很大的用户；同时在***系统状态***—>***NAT 统计***的“ NAT 统计信息列表 ”中，查看是否有“ 下载数据包 ”数量很小或没有的用户。如果某用户同时满足上述条件，同时该用户也未使用过局域网中的各种服务器，则该用户很可能正在已经感染上 RED_WORM 类型的网络攻击型病毒。

2) 在***系统状态***—>***用户统计***的“ 用户统计信息列表 ”中，查看是否有“ 发送广播包 ”数量很大，大于其“ 发送数据包 ”数量的 10%的用户。如果某用户“ 发送广播包 ”数量与“ 发送数据包 ”数量的百分比大于 10%，则该用户很可能已经感染上 RED_WORM 类型的网络攻击型病毒。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

D. 发现 TCP SYN FLOOD，UDP FLOOD，ICMP FLOOD 类型的网络攻击

在***系统状态***—>***用户统计***的“用户统计信息列表”中，查看是否有“发送数据包”数量很大、“接收数据包”数量很小的用户。如果某用户“发送数据包”数量很大，同时“接收数据包”数量很小，则该用户很可能正在进行 TCP SYN FLOOD、UDP FLOOD 或 ICMP FLOOD 类型的攻击。

提示：做正常 HTTP/FTP 上传的用户应该排除在外。

E. 发现 ARP FLOOD 类型的网络攻击

1) 在***系统状态***—>***用户统计***的“用户统计信息列表”中，查看是否有“发送广播包”数量很大，大于其“发送数据包”数量的 10%的用户。如果某用户“发送广播包”数量与“发送数据包”数量的百分比大于 10%，则该用户很可能正在进行 ARP FLOOD 型攻击。

提示：某些软件在正常使用的时候也会发送大量的广播包，比如网吧计费管理软件，这样就会造成广播包/发送包远大于 10%，此时应该忽略这种异常情况。

2) 在***系统状态***—>***系统信息***的“系统历史记录”中，如果发现某 IP 地址的 MAC 地址经常变化（例如显示出信息“MAC CHGED 192.168.16.221”、“MAC OLD 00:22:AA:00:22:AA”以及“MAC NEW 00:22:AA:00:22:BB”），则该用户很可能正在进行 ARP FLOOD 型攻击。

F. 发现冲击波/震荡波等蠕虫病毒攻击

感染了“冲击波”、“震荡波”病毒的个人电脑会随机向外发送大量的 ICMP 包以及向目的端口为 135/137/139/445 的端口发送大量的广播包，造成设备端口拥塞，直至整个内部网络、外部网络瘫痪。

在***上网监控***中，“选择查看条件”为“全部记录”，查看“查询结果列表”，如果在全部“协议类型”一列中，发现很多类型为 ICMP 的条目；在“外网端口”一列中，发现很多端口为 135/137/139/445 的条目，这些条目占用了大量的 NAT Seesion 条目，则很可能有主机感染了“冲击波”、“震荡波”病毒。

“冲击波”病毒感染计算机之后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；IE 浏览器不能正常地打开链接；不能复制粘贴；有时出现应用程序，比如 Word 异常；网络变慢；在任务管理器里有一个叫“msblast.exe”的进程在运行。

“震荡波”病毒感染计算机后，电脑出现如下症状：莫名其妙地死机或重新启动计算机；任务管理器里有一个叫“avserve.exe”、“avserve2.exe”或者“skynetave.exe”的进程在运行；在系统目录下，产生一个名为 avserve.exe、avserve2.exe、skynetave.exe 的病毒文件；系统速度极慢，CPU 占用 100%。

9. 如何实现允许响应外部 PING？

为了方便诊断和测试的需要，设备提供“允许响应外部 PING”功能，即允许从外网 PING 各个广域网接口的 IP 地址，以检测线路连接是否正常。实现方法如下：在***安全配置***—>***基本选项***中，首先选中“允许响应外部 PING”，再单击“保存”按钮。

配置完成之后，从外网执行 ping 命令，如果能 ping 通与某条线路相连的广域网接口的

IP 地址，则表示该线路连接正常；反之，如果不能 ping 通，则表示该线路连接异常，可能是线路本身有问题，或者是线路中某处设备不转发 ICMP 包（禁 ping），也有可能是设备配置有问题，等等。

附录 C 常用 IP 协议

协议	协议号	全称
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Porotocl
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocl
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhandced Interior Gateway Routing Portocol
OSPF	89	Open Shortest Path First

附录 D 常用服务端口

服务	端口号	协议	描述
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client

tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol

ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	
conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	

remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

附录 E 图索引

附录 F 表索引