7108501265

MERCURY®

制 造 商：深圳市美科星通信技术有限公司
公司地址：深圳市南山区翠溪路 4 号科苑西 28 栋 4 楼中
网　　址：http://www.mercurycom.com.cn

MERCURY®

水星MR900/MR900B

上网行为管理路由器

用 户 手 册

Rev: 2.1.0

声明

联系信息

网址：http://www.mercurycom.com.cn
技术支持热线：400-8810-500
技术支持 E-mail：fae@mercurycom.com.cn

物 品 清 单

请小心打开包装盒，里面应有以下配件:

- 一台路由器
- 一条电源线
- 一本用户手册
- 一张保修卡
- 其它配件

注意:

如果发现有配件短缺或损坏的情况，请及时和当地经销商联系。

目 录

第 1 章 用 户 手 册 简 介

在准备安装使用本产品之前，请先仔细阅读本手册，以便全面利用本产品的所有功能。

1.1. 用途

本手册的用途是帮助用户熟悉和正确使用MR900/MR900B上网行为管理路由器。

1.2. 约定

在本手册中，

- 所提到的“路由器”、“本产品”等名词，如无特别说明，系指上网行为管理路由器。
- 全文如无特殊说明，Web 界面以MR900B机型为例。
- 用 >> 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**，其中，部分功能无二级菜单。
- 正文中出现的<>尖括号标记文字，表示 Web 界面的按钮名称，如<确定>。
- 正文中出现的“”双引号标记文字，表示 Web 界面出现的除按钮外名词，如“ARP 绑定”界面。

用户在本用户手册中将会看到几种特殊的图形符号（图标），指出标识中的内容很重要，需要引起关注，本用户手册中使用的图标说明如下:

注意: 该图标表示这部分内容很重要，提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。

提示: 该图标为提醒您某些问题出现的可能原因。

举例: 该图标举例说明本设备，具体功能设置的步骤。

1.3. 用户手册概述

第 1 章: 用户手册简介。

第 2 章: 产品概述。简述路由器的功能及主要特性。

第 3 章: 硬件安装。帮助用户进行路由器的硬件安装。

第 4 章: 快速安装指南。帮助用户配置路由器的基本网络参数。

第 5 章: 配置指南。帮助用户配置路由器的高级特性。

附录 A: FAQ。

附录 B: TCP/IP 的详细设置。

附录 C: 技术参数表格。

第 2 章 产品概述

2.1. 产品简介

MR900/MR900B上网行为管理路由器是专为小型企业和办公室开发的高速宽带路由器产品，除 NAT 等基本功能外，还支持 IPSec/PPTP/L2TP VPN、上网行为管理（应用限制/网址过滤/网页安全）、防火墙（ARP 防护/攻击防护/访问控制）、智能 IP 带宽控制、多 WAN 口负载均衡、PPPoE 服务器等丰富的软件功能，适合小型企业和办公室组建经济、安全、高效和易管理的网络。

2.2. 主要特性

上网行为管理

- **应用限制**：支持针对聊天类、P2P 类、金融类、游戏类、代理类及基础类等数十种常见应用的一键管控，有效限制可能降低企业员工工作效率的上网行为；同时支持基于用户组和时间段配置管控策略，方便灵活分配上网权限，保障关键用户的正常上网。

- **网址过滤**：通过配置网站过滤和 URL 过滤规则，可对员工访问各种网站的权限进行管控，除了可以禁止/允许员工访问各种网站外，还可以记录其访问历史信息，甚至可以弹出警告页面。此外还支持网站分组功能，可方便地将庞杂的网站进行归类，供过滤规则调用，灵活而实用，同时路由器出厂默认提供十多种网站分组，对于网管资源有限的中小型企业用户，可节省不少配置工作。

- **网页安全**：支持禁止网页提交，可限制员工登录各种基于网页的论坛、网站、邮箱等发表信息，避免企业敏感数据外泄；支持过滤文件扩展类型，用户可方便地过滤内嵌在网页中的各种小文件，如 exe、rar、swf 文件等，避免病毒、木马等通过这些小文件侵入企业网络，危害网络安全。

VPN

- 提供标准的 IPsec VPN 功能，支持数据完整性校验、防数据包重放和数据加密功能（DES、3DES、AES128、AES192、AES256 等加密算法），支持 IKE 和手动模式建立 VPN 隧道，并支持通过域名方式配置 VPN 连接；

- 提供 L2TP/PPTP VPN 功能，支持 L2TP/PPTP VPN 服务器和客户端模式：服务器模式通常部署在企业总部，允许出差员工或分支结构远程安全接入公司网络；客户端模式通常部署在企业分支，可将分支机构网络远程安全接入到公司网络。

PPPoE 服务器

- PPPoE 服务器可为内网用户分配上网账号，只允许使用合法账号并通过认证的用户通过设备，从而有效控制内网用户的上网权限，同时支持空闲断线、到期断线、地址绑定、例外 IP 等丰富的功能特性，管理更灵活。

防火墙

- **访问策略**：通过配置访问控制策略，可允许或禁止特定应用数据流通过路由器，比如 FTP 下载、收发邮件、Web 浏览等，同时支持基于用户组和时间段配置策略，实现精细化管理。

- **ARP 防护**：支持 IP 与 MAC 地址自动扫描及一键绑定功能，有效防止 ARP 欺骗和非法接入；在遭受 ARP 欺骗时，路由器可按照指定频率发送 ARP 更正信息，及时恢复网络正常状态。

- **攻击防护**：支持内外网攻击防护功能，可有效防范各种常见的 DoS 攻击、扫描类攻击、可疑包攻击行为，如：TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke 攻击、分片报文攻击、WAN 口 ping、TCP Scan（Stealth FIN/Xmas/Null）、IP 欺骗等。

带宽控制

- 支持智能带宽控制功能，可根据实际的带宽利用率灵活启用带宽控制策略，可针对网络中每一台主机（IP）进行双向带宽控制，有效抑制 BT、迅雷等 P2P 应用过度占用带宽，避免造成网络游戏卡、上网速度慢的问题，保障网络时刻畅通。

连接数限制

- 提供基于 IP 的连接数限制功能，可限制每一台电脑的连接数占有量，合理利用有限的 NAT 连接数资源，防止少数用户过度占用大量连接数，确保游戏、上网、聊天、视频语音等顺畅进行。

多 WAN 口（仅MR900B支持）

- 提供 1~4 个 WAN 口，允许用户根据实际需求灵活配置 WAN 口数量，满足多线路接入的组网需求;
- 支持双线路负载均衡，通过采用智能均衡、特殊应用程序选路、ISP 选路、策略选路等多种均衡策略，充分利用 WAN 口带宽，保护用户投资;
- 支持 WAN 口备份功能，提供故障备份和时间备份两种备份模式，可在主线路中断后迅速将流量切换至备份线路，保障网络正常运行。

端口镜像

- 内置简单管理交换机，支持端口带宽控制和端口镜像等功能，满足公安部门的数据监控需求。

设备管理

- 支持全中文 WEB 网管，所有功能均可通过图形化界面进行配置，简单方便;
- 每一项配置均提供必要的帮助说明信息，有效降低配置难度。

设备维护

- 提供系统日志与日志服务器功能，详尽的日志信息便于快速发现网络异常并及时定位问题原因;
- 支持本地及远程管理路由器，方便远程协助;
- 支持 Ping 检测及 Tracert 检测，方便快速确认网络连通状态。

第 3 章　硬 件 安 装

3.1. 面板布置

3.1.1. 前面板

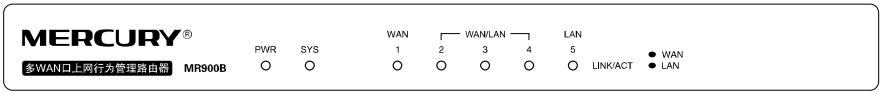


图 3-1 MR900B 前面板示意图

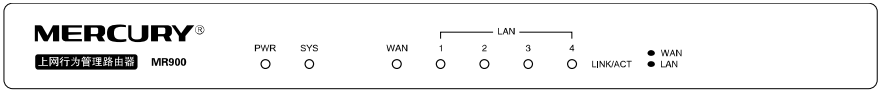


图 3-2 MR900 前面板示意图

指示灯:

指示灯	描述	功能
PWR	电源指示灯	常亮表示系统正在运行
SYS	系统指示灯	闪烁表示系统正常
		常亮或不亮表示系统不正常
LINK/ACT	状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在进行数据传输
		常灭表示相应端口未建立连接

提示:

Link/Act 指示灯亮黄色表示相应端口为 WAN 口，绿色表示端口为 LAN 口。

3.1.2. 后面板

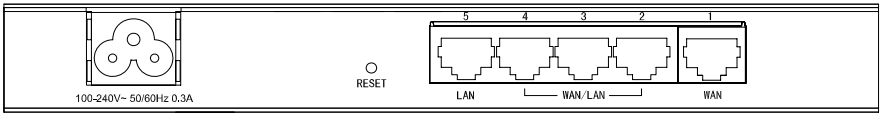


图 3-3 MR900B 后面板示意图

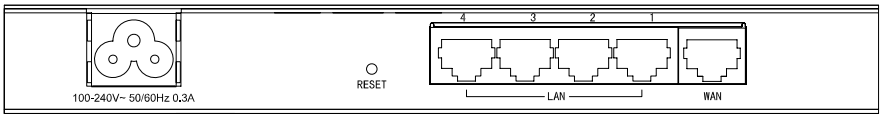


图 3-4 MR900 后面板示意图

WAN 连接 xDSL/Cable Modem 或以太网。

LAN 计算机和集线器/交换机通过这个端口连入局域网。

RESET 复位按钮，可以将设备恢复为出厂设置。复位方式：通电状态下长按 RESET 键，待系统指示灯闪烁 5 次后松开 RESET 键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为 http://192.168.1.1，默认用户名和密码均为 admin。

注意:

在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

电源插孔 这个插孔用于插接电源。电源规格为：100-240V~ 50/60Hz 0.3A。如果使用不匹配的电源，可能会导致路由器损坏。

3.2. 系统需求

- 宽带 Internet 服务（接入方式为 xDSL/Cable Modem 或以太网）
- 具有以太网 RJ45 连接器的调制解调器（直接接入以太网时不需要此物件）
- 每台 PC 的以太网连接（网卡和网线）
- TCP/IP 网络软件（Windows 95/98/ME/NT/2000/XP/Vista/7 自带）
- Internet Explorer 5.0 或更高版本

3.3. 安装环境

安装环境要求:

- 将路由器水平放置。
- 尽量将路由器放置在远离发热器件处。
- 不要将路由器置于太脏或潮湿的地方。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

路由器推荐使用环境:

- 温度：0 ºC～40 ºC
- 湿度：10%～90%RH，不凝结

3.4. 硬件安装步骤

在安装路由器前，请确认是否能通过宽带服务访问网络。如果无法访问，请先和网络服务商（ISP）联系解决问题。成功访问网络后，请遵循以下步骤安装路由器。安装时拔除电源插头，保持双手干燥。

1) 建立局域网连接

用一根网线连接路由器的 LAN 口和局域网中的集线器或交换机，如下图所示。也可以用一根网线将路由器与计算机网卡直接相连。

2) 建立广域网连接

用网线将路由器 WAN 口与 Internet 相连，以MR900B为例，如下图所示。

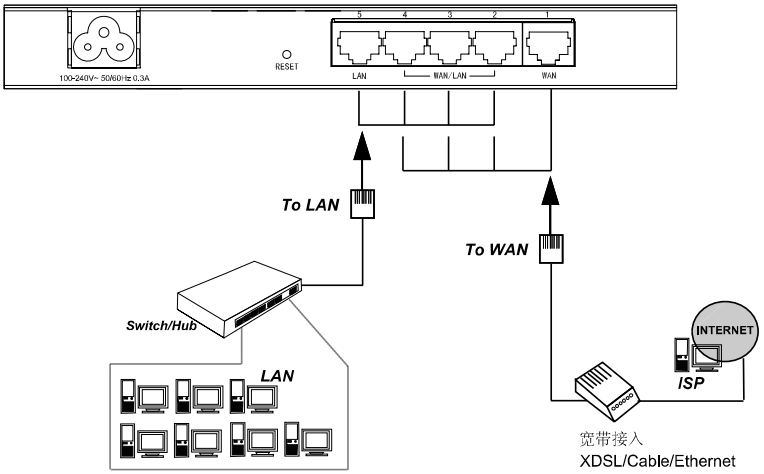


图 3-5 建立局域网和广域网连接

提示:

以上网络拓扑图为您进行网络设置的参照用例，您可以根据实际情况，实际需求配置适合您的网络构架。

3) 连接电源

将电源连接好，路由器将自行启动。

第 4 章　快 速 安 装 指 南

如果对路由器进行基本配置，请阅读本章内容；如果进行高级配置，请继续阅读第 5 章内容。

4.1. 建立正确的网络设置

路由器默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本用户手册上将按默认值说明。

首先请将计算机接到路由器的局域网端口，接下来可以使用两种方法为计算机设置 IP 地址。

方法一：手动设置 IP 地址。

设置计算机的 TCP/IP 协议。如果已经正确设置完成，请跳过第一步。

设置计算机的 IP 地址为 192.168.1.xxx（xxx 范围是 2 至 254），子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

方法二：利用路由器内置 DHCP 服务器自动设置 IP 地址。

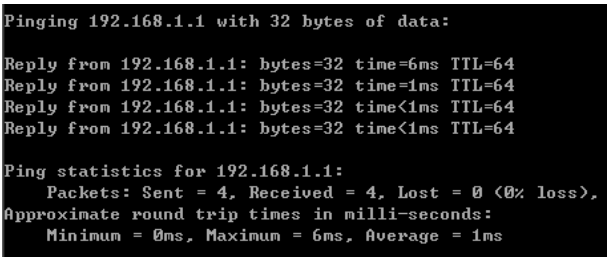
设置计算机的 TCP/IP 协议为“自动获取 IP 地址 ”。

在设置好 TCP/IP 协议后，使用 Ping 命令检查计算机和路由器之间是否连通。下面的例子为一个在 Windows XP 环境中，执行 Ping 命令，操作步骤如下:

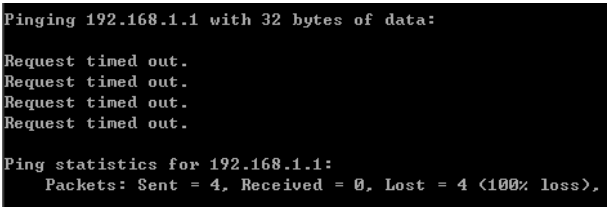
首先请点击桌面的“开始”菜单，再选择“运行”选项，并在随后出现的运行输入框内输入 cmd 命令，然后回车或点击“确认”键即可进入下图所示界面。

最后在该界面中输入命令 Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为:



那么计算机已与路由器成功建立连接。如果屏幕显示为:



这说明设备还未安装好，请按照下列顺序检查:

1) 硬件连接是否正确?

提示:

路由器面板上对应局域网端口的 Link/Act 指示灯和计算机上的网卡灯必须亮。

2) 计算机的 TCP/IP 设置是否正确?

提示:

如果路由器的 IP 地址为 192.168.1.1, 那么计算机 IP 地址必须为 192.168.1.xxx（xxx 范围是 2 至 254）。

4.2. 快速安装指南

本产品提供基于浏览器（Internet Explorer 或 Netscape Communicator）的配置界面，这种配置方案适宜于任何 MS Windows, Macintosh 或 UNIX 平台。

激活浏览器，取消“使用代理服务器”选项或者将路由器的 IP 地址添加到“代理服务器设置”中的“例外”栏中（在 IE 中选择“工具－Internet 选项－连接－局域网设置”，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的 IP 地址，例如 http://192.168.1.1。

连接建立后将会看到下图所示登录界面。输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。

图 4-1 路由器登录界面

成功登录后会弹出设置向导界面。如果没有自动弹出，可以单击主页左侧**设置向导**菜单进入。单击<下一步>，开始设置。

图 4-2 设置向导

请根据实际需求选择 WAN 口模式，如图 4-3所示（MR900无此界面），单击<下一步>，进入 WAN 口选择界面。

图 4-3 WAN 口模式

请选择要设置的 WAN 口，如图 4-4所示（MR900无此界面），单击<下一步>，进入上网方式选择界面。

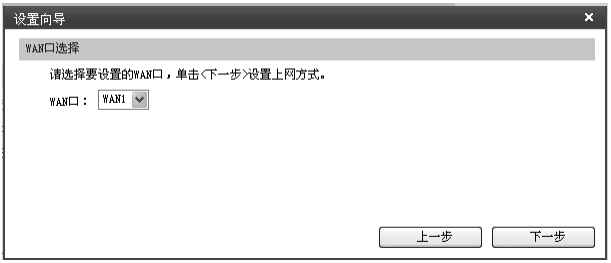


图 4-4 WAN 口选择

下图显示了最常用的三种上网方式，可以根据自身情况进行选择，然后单击<下一步>继续。

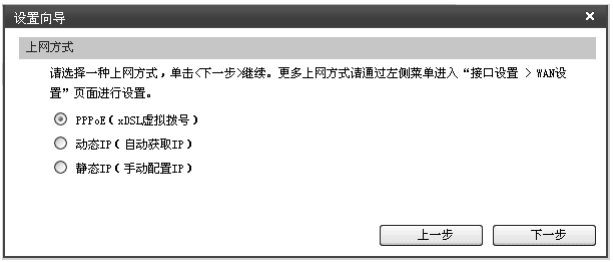


图 4-5 上网方式

1） 如果上网方式为 PPPoE，即 ADSL 虚拟拨号方式，则需要填写以下内容:

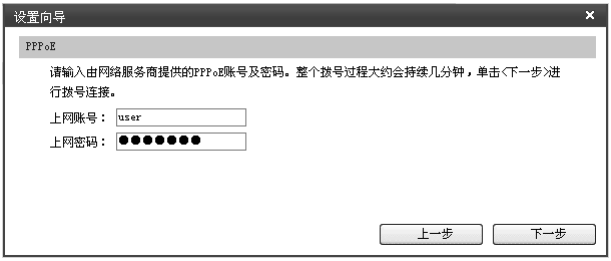


图 4-6 上网方式-PPPoE

上网帐号 填入 ISP 指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。

上网口令 填入 ISP 指定的 ADSL 上网口令，不清楚可以向 ISP 询问。

整个拨号过程大约会持续几分钟，单击<下一步>进行拨号连接，图 4-7为 PPPoE 拨号连接界面。如果在此连接过程中，您关闭了设置向导，该接口的配置工作仍会在后台进行。

图 4-7上网方式-PPPoE 连接

2） 如果上网方式为动态 IP，即可以自动从网络服务商获取 IP 地址，则不需要填写任何内容。图 4-8为动态 IP 连接界面。如果在此连接过程中，您关闭了设置向导，该接口的配置工作仍会在后台进行。

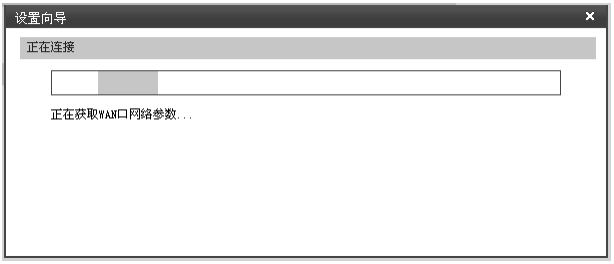


图 4-8 上网方式-动态 IP 连接

3） 如果上网方式为静态 IP，即拥有网络服务商提供的固定 IP 地址，则需要填写以下内容:

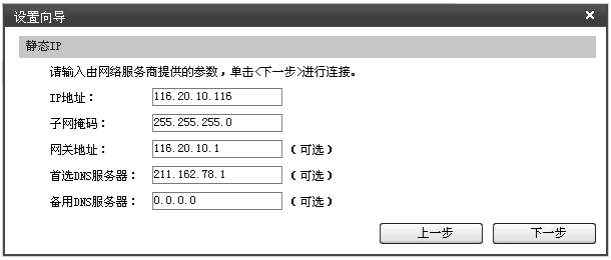


图 4-9 上网方式-静态 IP

IP 地址 本路由器对广域网的 IP 地址，即 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。

子网掩码 本路由器对广域网的子网掩码，即 ISP 提供的子网掩码，一般为 255.255.255.0。

网关 填入 ISP 提供的网关，不清楚可以向 ISP 询问。

DNS 服务器 填入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问。

备用 DNS 服务器 可选项，如果 ISP 提供给了两个 DNS 服务器地址，则可以把另一个 DNS 服务器地址的 IP 地址填于此处。

单击<下一步>进行连接，图 4-10为静态 IP 连接界面。如果在此连接过程中，您关闭了设置向导，该接口的配置工作仍会在后台进行。

图 4-10 上网方式-静态 IP 连接

连接成功后会出现配置完成界面，如图 4-11所示:

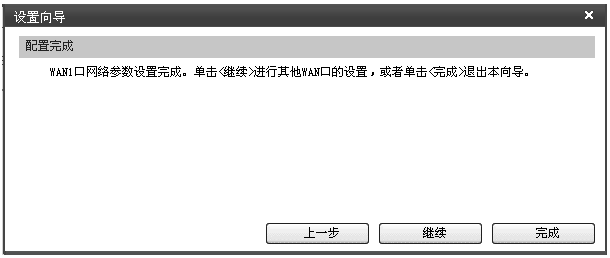


图 4-11 配置完成

单击<完成>退出设置向导，或者单击<继续>进行其他 WAN 口的设置（MR900则直接单击<完成>退出设置向导）。

第 5 章 配 置 指 南

5.1. 系统状态

系统状态界面显示路由器当前硬件和软件版本信息、各接口配置信息以及系统资源使用情况。

界面进入方法：系统状态

图 5-1 系统状态界面

5.2. 设置向导

详见 4.2 快速安装指南。

5.3. 接口设置

5.3.1.WAN 设置

5.3.1.1. WAN 模式

MR900B支持多种 WAN 口模式：单 WAN 口、双 WAN 口、三 WAN 口、四 WAN 口。

界面进入方法：接口设置 >> WAN 设置 >> WAN 模式

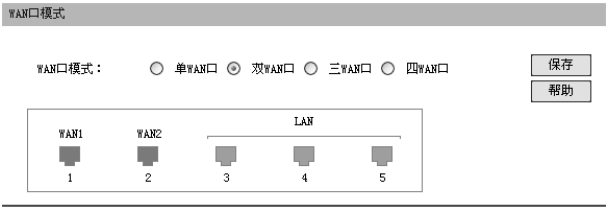


图 5-2 WAN 模式设置界面

请根据实际需求选择路由器的 WAN 模式。路由器会根据不同的 WAN 口模式对各物理端口做出相应配置，具体请参考图 5-2中的产品接口示意图。

提示：

- MR900没有此功能。
- MR900B出厂默认为双 WAN 口模式，切换 WAN 口模式可能导致配置信息丢失。若有重要配置信息，请在切换模式前备份。

5.3.1.2. WAN1 **设置**

上网行为管理路由器提供五种方式接入广域网：静态 IP、动态 IP、PPPoE、L2TP、PPTP，请根据 ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

- 有线宽频一般使用动态 IP 连接方式;
- 光纤接入以及企业、网吧局域网内组网一般使用静态 IP 连接方式;
- xDSL 拨号上网则使用 PPPoE 连接方式;
- 虚拟专用拨号网络一般使用 L2TP 或 PPTP 连接方式。

提示:

- MR900此标签页名称为 **WAN 设置**。
- MR900B允许设置多个 WAN 口的 IP 地址为同一个网段，但需保证这些 WAN 口能连通到同一个网域，比如都连通到因特网或同一个局域网，否则可能会导致通信异常。
- 根据 WAN 口数量的不同，对 WAN 口进行设置的标签页个数也会不同。其他 WAN 口的设置方法请参考本节。

界面进入方法: 接口设置 >> WAN 设置 >> WAN1 设置

1) 静态 IP 连接

若 ISP 提供了固定的 IP 地址，请选择静态 IP 手动配置 WAN 口参数。

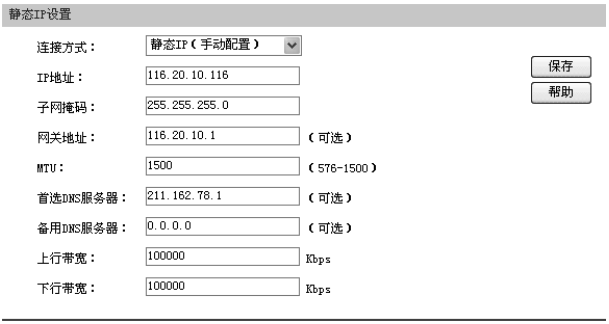


图 5-3 WAN 口设置界面-静态 IP

静态 IP 设置

连接方式　　选择静态 IP 连接方式，进行手动配置。

IP 地址　　设置路由器 WAN 口的 IP 地址。

子网掩码　　设置路由器 WAN 口的子网掩码。

网关地址　　设置网关地址。

MTU　　MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。

首选 DNS 服务器　　设置 DNS（Domain Name Server，域名解析服务器）地址，一般由 ISP 提供，如果留空，则无法通过域名访问互联网。

备用 DNS 服务器　　设置备用 DNS 地址，一般由 ISP 提供，允许留空。

上行带宽　　设置当前 WAN 接口数据流出的带宽大小。

下行带宽　　设置当前 WAN 接口数据流入的带宽大小。

2)　动态 IP 连接

若 ISP 提供 DHCP 自动分配地址服务，请选择动态 IP 自动获取 WAN 口参数。

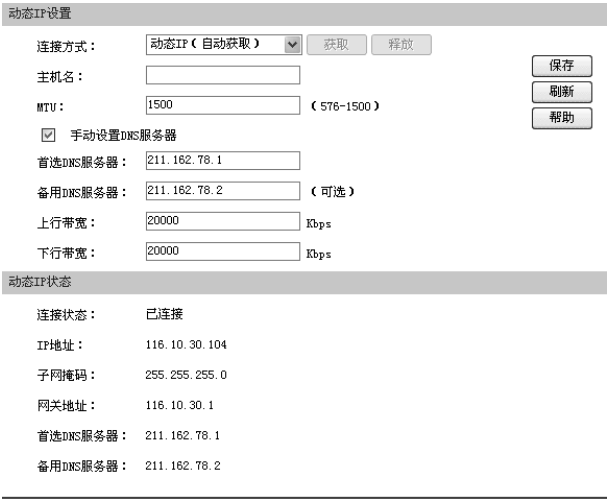


图 5-4 WAN 口设置界面-动态 IP

动态 IP 设置

连接方式	选择动态 IP 连接方式。点击<获取>得到 IP 参数，点击<释放>则不再使用现有 IP 参数。
主机名	输入用于标识路由器的名称。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。
手动设置 DNS 服务器	如果需要手动设置 DNS（Domain Name Server，域名解析服务）地址，请勾选此项。
首选 DNS 服务器	设置 DNS 地址，一般由 ISP 提供。

备用 DNS 服务器	设置备用 DNS 地址，一般由 ISP 提供，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

动态 IP 状态

连接状态	显示当前 WAN 口 DHCP 分配状态。 “未启用”表示当前已选择动态 IP 连接方式但未保存生效; “正在连接”表示当前路由器正在向 ISP 获取 IP 参数; “已连接”表示路由器已成功获取 IP 参数; “未连接”表示已手动释放连接，或路由器已发起请求，但未得到响应，请检查连接线路是否正常，若问题无法解决，请与 ISP 联系。
IP 地址	显示自动获取到的 IP 地址。
子网掩码	显示自动获取到的子网掩码。
网关地址	显示自动获取到的网关地址。
首选 DNS 服务器	显示 DNS 地址。
备用 DNS 服务器	显示备用 DNS 地址。

3) **PPPoE** 连接

若使用 xDSL/Cable Modem 拨号接入互联网，ISP 会提供上网账号及密码，请选择 PPPoE 连接方式。

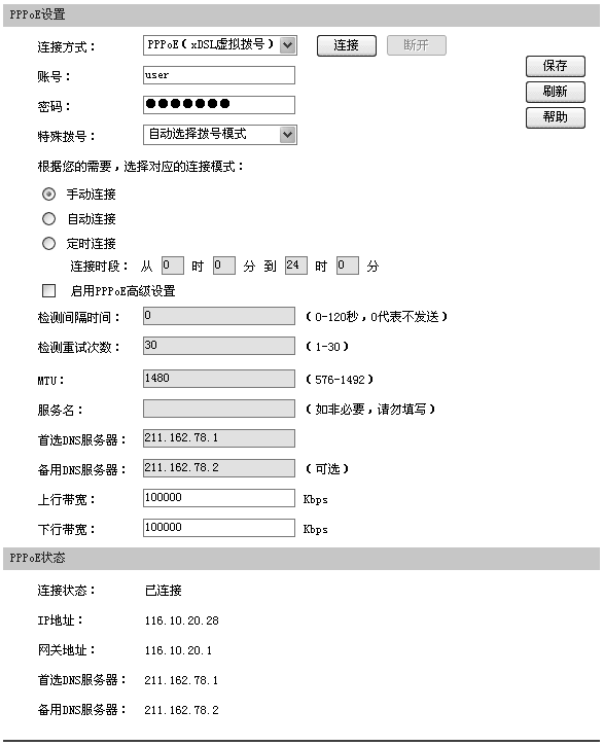


图 **5-5** WAN 口设置界面-PPPoE

PPPoE 设置

连接方式　　选择 PPPoE。点击<连接>开始拨号并获取 IP 参数，点击<断开>则取消与互联网的连接同时释放已获取的 IP 参数。

账号　　PPPoE 拨号的用户名，由 ISP 提供。

密码　　PPPoE 拨号的密码，由 ISP 提供。

特殊拨号　　请根据需求选择拨号模式。如果正常拨号模式下无法连接成功，请依次尝试不同的特殊拨号模式。默认为自动选择特殊拨号模式，路由器会自动尝试不同的特殊拨号模式。

手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
定时连接	设置连接时段，在此时段内路由器如果开启则自动拨号连接，适合用于需要限时上网的场合。
启用 PPPoE 高级设置	可以在此手动指定 MTU 值、服务名及 DNS（Domain Name Server，域名解析服务）地址。如果不清楚这些参数，请勿勾选此项。
检测间隔时间	设置检测间隔时间，路由器将会按照指定的间隔时间向 ISP 发送 Keep Alive 数据包，用于检测链路是否正常。默认值为 0，表示不检测链路。
检测重试次数	设置检测重试次数，路由器按照指定的检测间隔时间向 ISP 发送 Keep Alive 数据包，如果没有收到 ISP 回应包的连续重试次数达到设置的值，路由器会断开连接。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1492 之间的整数，默认值为 1480。若 ISP 未提供 MTU 值，请保持默认值不变。
服务名	输入服务名称，由 ISP 提供。
首选 DNS 服务器	设置 DNS 地址，一般由 ISP 提供。
备用 DNS 服务器	设置备用 DNS 地址，一般由 ISP 提供，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

PPPoE 状态

连接状态	显示当前 WAN 口 PPPoE 拨号连接状态。 “未启用”表示当前已选择 PPPoE 拨号连接方式但未保存生效; “正在连接”表示当前路由器正在向 ISP 获取 IP 参数; “已连接”表示路由器已成功获取 IP 参数; “未连接”表示已手动断开连接，或路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与 ISP 联系。
IP 地址	显示通过 PPPoE 拨号后获取到的 IP 地址。
网关地址	显示通过 PPPoE 拨号后获取到的网关地址。
首选 DNS 服务器	显示 DNS 地址。
备用 DNS 服务器	显示备用 DNS 地址。

4) L2TP 连接

若使用 L2TP 虚拟专用拨号接入网络，ISP 会提供上网账号及密码，请选择 L2TP 连接方式进行设置。

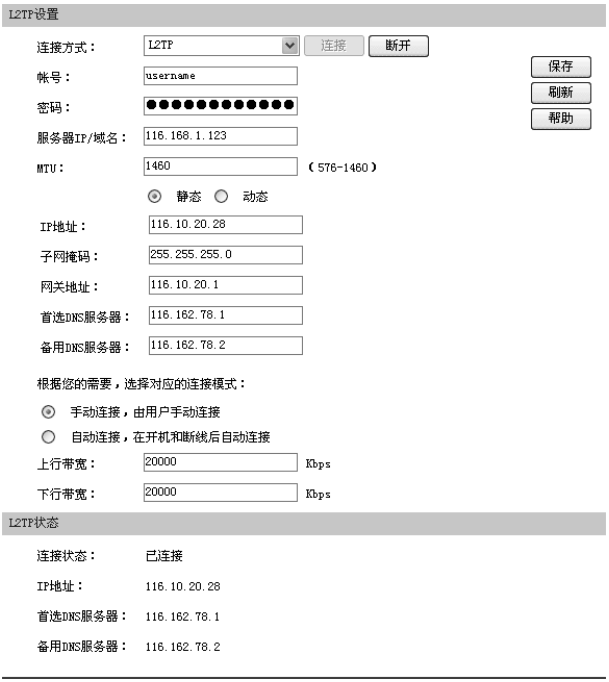


图 5-6 WAN 口设置界面-L2TP

L2TP 设置

连接方式	选择 L2TP。点击<连接>开始拨号并获取 IP 参数，点击<断开>则取消与互联网的连接同时释放已获取的 IP 参数。
帐号	L2TP 拨号的用户名，由 ISP 提供。
密码	L2TP 拨号的密码，由 ISP 提供。
服务器 IP	L2TP 拨号的服务器的 IP 地址，由 ISP 提供。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1460 之间的整数，默认值为 1460。若 ISP 未提供 MTU 值，请保持默认值不变。

静态/动态	选择静态或动态获取 IP 地址。若选择静态方式，则需要手动设置 IP 地址；若选择动态，则外部的 DHCP 服务器将动态分配一个 IP 地址。
IP 地址	若选择静态，设置路由器 WAN 口的 IP 地址；若选择动态，显示路由器 WAN 口获取到的 IP 地址。
子网掩码	若选择静态，设置路由器 WAN 口的子网掩码；若选择动态，显示路由器 WAN 口获取到的子网掩码。
网关地址	若选择静态，设置网关地址；若选择动态，显示获取到的网关地址。
首选 DNS 服务器	若选择静态，设置 DNS（Domain Name Server，域名解析服务器）地址，一般由 ISP 提供，如果留空，则无法通过域名访问互联网；若选择动态，显示分配到的 DNS 地址。
备用 DNS 服务器	若选择静态，设置备用 DNS 地址，一般由 ISP 提供，允许留空；若选择动态，显示分配到的备用 DNS 地址。
手动连接	用户可在需要上网时手动点击<连接>按钮进行连接。
自动连接	每次接通路由器电源，路由器便会进行自动拨号。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

L2TP 状态

连接状态	显示当前 WAN 口 L2TP 拨号连接状态。 “未启用”表示当前已选择 L2TP 拨号连接方式但未保存生效； “正在连接”表示当前路由器正在向 ISP 获取 IP 参数；

“已连接”表示路由器已成功获取 IP 参数;

“未连接”表示已手动断开连接，或路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与 ISP 联系。

IP 地址　　显示通过 L2TP 拨号后获取到的 IP 地址。

首选 DNS 服务器　　显示 DNS 地址。

备用 DNS 服务器　　显示备用 DNS 地址。

5)　PPTP 连接

若使用 PPTP 虚拟专用拨号接入网络，ISP 会提供上网账号及密码，请选择 PPTP 连接方式进行设置。

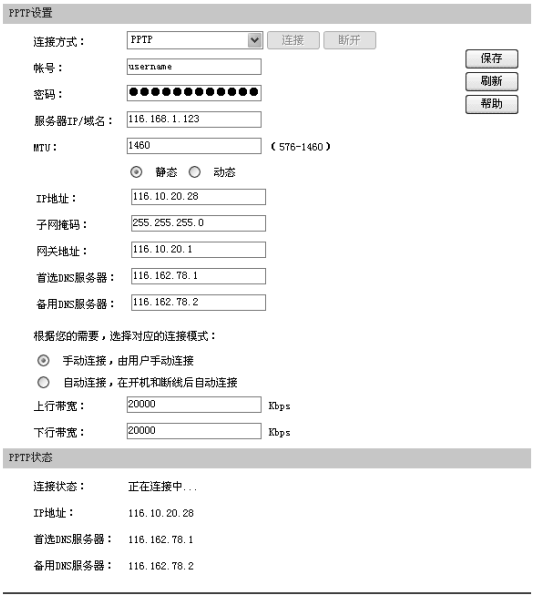


图 5-7 WAN 口设置界面-PPTP

PPTP 设置

连接方式	选择 PPTP。点击<连接>开始拨号并获取 IP 参数，点击<断开>则取消与互联网的连接同时释放已获取的 IP 参数。
账号	PPTP 拨号的用户名，由 ISP 提供。
密码	PPTP 拨号的密码，由 ISP 提供。
服务器 IP	PPTP 拨号的服务器的 IP 地址，由 ISP 提供。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是 576-1460 之间的整数，默认值为 1460。若 ISP 未提供 MTU 值，请保持默认值不变。
静态/动态	选择静态或动态获取 IP 地址。若选择静态方式，则需要手动设置 IP 地址；若选择动态，则外部的 DHCP 服务器将动态分配一个 IP 地址。
IP 地址	若选择静态，设置路由器 WAN 口的 IP 地址；若选择动态，显示路由器 WAN 口获取到的 IP 地址。
子网掩码	若选择静态，设置路由器 WAN 口的子网掩码；若选择动态，显示路由器 WAN 口获取到的子网掩码。
网关地址	若选择静态，设置网关地址；若选择动态，显示获取到的网关地址。
首选 DNS 服务器	若选择静态，设置 DNS（Domain Name Server，域名解析服务器）地址，一般由 ISP 提供，如果留空，则无法通过域名访问互联网；若选择动态，显示分配到的 DNS 地址。
备用 DNS 服务器	若选择静态，设置备用 DNS 地址，一般由 ISP 提供，允许留空；若选择动态，显示分配到的备用 DNS 地址。

手动连接	用户可在需要上网时手动点击<连接>按钮进行连接。
自动连接	每次接通路由器电源，路由器便会进行自动拨号。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

PPTP 状态

连接状态	显示当前 WAN 口 PPTP 拨号连接状态。 “未启用”表示当前已选择 PPTP 拨号连接方式但未保存生效; “正在连接”表示当前路由器正在向 ISP 获取 IP 参数; “已连接”表示路由器已成功获取 IP 参数; “未连接”表示已手动断开连接，或路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与 ISP 联系。
IP 地址	显示通过 PPTP 拨号后获取到的 IP 地址。
首选 DNS 服务器	显示 DNS 地址。
备用 DNS 服务器	显示备用 DNS 地址。

5.3.2.LAN **设置**

5.3.2.1. LAN **口设置**

在此设置路由器 LAN 口的 IP 参数。

界面进入方法：基本设置 >> LAN 设置 >> LAN 口设置

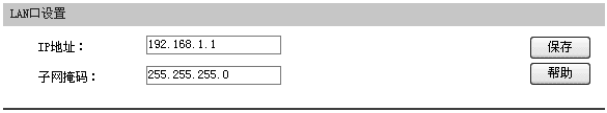


图 5-8 LAN 口设置界面

LAN 口设置

IP 地址　　设置路由器 LAN 口的 IP 地址，默认值为 192.168.1.1，可根据实际网络情况修改此值。局域网内部可通过该地址访问路由器。

子网掩码　　设置路由器 LAN 口的子网掩码，默认为 255.255.255.0，可根据实际网络情况修改此值。

提示:

若 LAN 口 IP 地址有修改，必须在保存配置后使用新的 LAN 口地址登录路由器 Web 管理界面。并且，局域网内所有计算机网关地址、子网掩码必须与修改后的 LAN 口设置保持一致，才能正常通信。

5.3.2.2. DHCP **服务**

DHCP(Dynamic Host Configuration Protocol, 动态主机配置协议)。路由器具有 DHCP 服务功能，能够为所有接入路由器并且应用 DHCP 服务的网络设备自动分配 IP 参数。

界面进入方法: 基本设置 >> LAN 设置 >> DHCP 服务

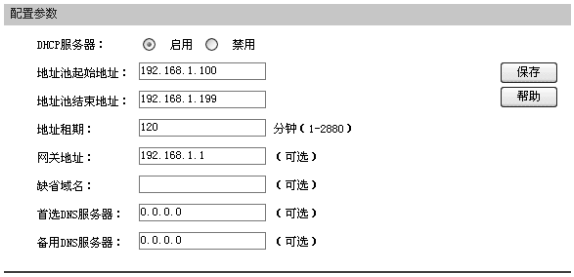


图 5-9 DHCP 服务设置界面

配置参数

DHCP 服务器	选择开启或关闭 DHCP 服务。若希望路由器自动为计算机配置 TCP/IP 参数，请选择“启用”。
地址池起始地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必须与 LAN 口 IP 地址设置在同一网段，默认值为 192.168.1.100。
地址池结束地址	设置 DHCP 服务器自动分配 IP 地址的结束地址，该地址必须与 LAN 口 IP 地址设置在同一网段，默认值为 192.168.1.199。
地址租期	设置 DHCP 分配地址有效时间，超时将重新分配。
网关地址	设置 DHCP 分配给客户端的网关地址，推荐设置为 LAN 口 IP 地址。
缺省域名	设置本地网域名，允许留空。
首选 DNS 服务器	设置 DNS 地址，推荐设为路由器 LAN 口 IP 地址，允许留空。
备用 DNS 服务器	设置备用 DNS 地址，允许留空。

5.3.2.3. 客户端列表

客户端列表显示已由 DHCP 分配 IP 参数的主机信息。

界面进入方法：基本设置 >> LAN 设置 >> 客户端列表

图 5-10 客户端列表界面

可通过客户端列表查询 DHCP 客户端信息。如要获得最新 DHCP 服务分配的客户端信息，请点击<刷新>按钮。

5.3.2.4. 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动为其分配指定的 IP 地址。

界面进入方法：基本设置 >> LAN 设置 >> 静态地址分配

图 5-11 静态地址分配设置界面

静态地址

MAC 地址	设置待分配 IP 地址的客户端的 MAC 地址。
IP 地址	指定当前 MAC 地址所对应的客户端的 IP 地址。
备注	添加对本条目的说明信息。
启用/禁用规则	选择启用或禁用本条静态地址分配规则。

地址列表

在静态地址列表中，可以对已保存的静态 IP 地址分配规则进行相应操作。

图 5-11序号 1 规则的含义：MAC 地址为 00-19-66-83-53-CF 的客户端，指定其 IP 地址为 192.168.1.101，该规则已禁用。

提示:

为了避免冲突，建议先进行 IP MAC 绑定，具体操作请参考**ARP 防护**，然后点击静态地址分配设置界面中的<导入>按钮，直接获取 IP MAC 绑定列表中的静态地址条目。

5.3.3.MAC 设置

路由器 MAC 地址是它在网络中的身份标志，一般来说无需更改。

LAN 口 MAC 设置:

在一个所有设备都进行了 ARP 绑定的复杂拓扑中，如果其中一个网络节点的路由器更换为上网行为管理路由器，为避免该节点下面接入的所有网络设备都更新 ARP 绑定表，直接将上网行为管理路由器系列产品的 LAN 口 MAC 地址设置为原路由器的 MAC 地址即可。

WAN 口 MAC 设置:

有些 ISP 要求上网帐号与拨号设备的 MAC 绑定，若此时拨号设备更换为上网行为管理路由器，只需将路由器 WAN 口的 MAC 地址设置为原拨号设备的 MAC 地址即可。

界面进入方法：接口设置 >> MAC 设置 >> MAC 设置

图 5-12 MAC 设置界面

MAC 设置

接口	显示当前路由器各接口。
当前 MAC 地址	显示当前各接口的 MAC 地址。
设置	如需恢复初始状态，请点击<出厂 MAC>按钮。如需将当前 MAC 地址设置为管理主机 MAC 地址，即当前登录路由器进行配置管理的主机 MAC 地址，请点击<管理主机 MAC>按钮。

提示:

为了防止局域网内 MAC 地址冲突，路由器 LAN 口的 MAC 地址不能设置成当前管理主机的 MAC 地址。

5.3.4. 交换机设置

上网行为管理路由器具备一些简单的交换机端口管理功能。在此可以实时查看路由器各端口的数据流通状况，并进行相应的控制和管理。

以下界面以MR900B为例，MR900产品界面会略有不同。

5.3.4.1. 端口统计

用于交换信息的数据包在数据链路层通常称为“帧”。可以通过此功能查看各个端口收发数据帧的统计信息。

界面进入方法: 接口设置 >> 交换机设置 >> 端口统计

图 5-13 端口统计界面

统计列表

单播帧　　目的 MAC 地址为单播 MAC 地址的正常数据帧数目。

广播帧　　目的 MAC 地址为广播 MAC 地址的正常数据帧数目。

流控帧　　接收/发送的流量控制数据帧数目。

多播帧　　目的 MAC 地址为多播 MAC 地址的正常数据帧数目。

所有帧　　接收/发送所有的数据帧的总字节数（包含校验和错误的帧）。

过小帧　　收到的长度小于 64 字节的数据帧数目（包含校验和错误的帧）。

正常帧　　收到的长度在 64 字节到 1518 字节之间的数据帧数目（包含错误帧）。

过大帧　　收到的长度大于 1518 字节的数据帧数目（包含错误帧）。

勾选最后一行的复选框后，点击<清空统计>按钮，即可清空该列对应端口的统计数据。点击<清空所有>按钮可以一次清空所有统计数据。

5.3.4.2. 端口监控

可以在此开启和设置端口监控功能。被监控端口的报文会被自动复制到监控端口，以便网络管理人员实时查看被监控端口传输状况的详细资料，对其进行流量监控、性能分析和故障诊断。

界面进入方法：接口设置 >> 交换机设置 >> 端口监控

图 5-14 端口监控设置界面

功能设置

启用端口监控　勾选即启用端口监控。推荐勾选，方便及时了解路由器端口报文信息。

监控模式　选择对数据包进行“输入监控”、“输出监控”或者“输入输出监控 。

监控列表

监控端口　只能选择一个端口做监控端口。

被监控端口　被监控端口可以为多个，但不包含当前的监控端口。

上图监控列表的含义是：端口 4 被选作监控端口，它将对端口 1、2、3、5 进行输出监控。

提示:

如果监控端口为 LAN 口，被监控端口中有其他 LAN 口，则这些 LAN 口必须属于同一个 Port VLAN。比如端口 3 和端口 4 都设置成 LAN 口，端口 3 为监控端口，端口 4 为被监控端口，那么端口 3 和端口 4 必须处于相同的 Port VLAN 中，端口监控功能才能生效。

举例:

某企业网络出现异常状况，需要利用端口监控功能捕获网络中的所有数据进行分析。

可通过端口监控实现此需求。勾选“启用端口监控”，并选择“输入输出监控”的监控模式，设置端口 3 为监控端口，监控其它端口的输入输出数据，如下图。设置完成后，点击<保存>按钮。

5.3.4.3. 端口流量限制

可以在此开启各端口的流量限制功能并进行相应设置。

界面进入方法: 接口设置 >> 交换机设置 >> 端口流量限制

图 5-15 端口流量限制设置界面

功能设置

端口　　显示所有物理端口，需要对某个端口进行流量限制时，在其对应行设置即可。

入口限制状态　　勾选“启用”后，后续设置的入口限制速率才会生效。

入口限制速率　　有从小到大 128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps 七种速率，选择其一。

出口限制状态　　勾选“启用”，后续设置的出口限制速率才会生效。

出口限制速率　　有从小到大 128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps 七种速率，选择其一。

图 5-15第一行的含义是：开启端口 1 的入口和出口限制状态，设置端口 1 的入口限制速率为 128Kbps，出口限制速率为 8Mbps。设置完成后，端口 1 的入口数据帧的接收速率将不会超过 128Kbps，所有出口数据帧的发送速率将不会超过 8Mbps。

5.3.4.4. 端口参数

可以在此启用各物理端口及其流量限制，并根据需要设定其协商模式。

界面进入方法：接口设置 >> 交换机设置 >> 端口参数

图 5-16 端口参数设置界面

功能设置

端口状态　只有勾选了“启用”该端口才会有数据包的传输，即物理意义上的开启。

流量控制　推荐勾选“启用”以控制调节各端口数据包转发的速率，避免出现拥塞。

协商模式　有 10M 全/半双工、100M 全/半双工、自协商 5 种模式可选，择需使用。

所有端口　这一栏可对以上所有端口进行统一设置，比如同时启用或禁用。

5.3.4.5. 端口状态

可以在此查看各个端口的基本状态。

界面进入方法：接口设置 >> 交换机设置 >> 端口状态

图 5-17 端口状态界面

5.3.4.6. Port VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是从逻辑上而非物理上，将整个局域网分割成几个不同的广播域，数据只能在 VLAN 内进行交换。

一个稍具规模的网络如果只有一个广播域，那么在网络内不断发送的广播包很容易造成广播风暴，消耗网络整体带宽，并给网络中的主机带来额外的负担。划分 VLAN 以后，数据只会在自己所属的 VLAN 内广播，所以可以控制广播风暴，同时还能增强网络安全，简化网络管理。

上网行为管理路由器提供基于端口划分 VLAN 的 Port VLAN 功能，可以把路由器的若干 LAN 口从逻辑上划分为多个 VLAN。

界面进入方法：接口设置 >> 交换机设置 >> Port VLAN

图 5-18 Port VLAN 设置界面

功能设置

网络　　标识各个物理端口此时属于的逻辑网络。

VLAN　　配置各端口所属 VLAN。

提示:

Port VLAN 的划分只能在 LAN 口中进行。

5.4. 对象管理

5.4.1. 用户管理

5.4.1.1. 组设置

可以在此创建、修改或者删除组。

界面进入方法: 对象管理 >> 用户管理 >> 组设置

图 5-19 组设置界面

组设置

组名称　　输入一个名称来标识一个组，可以输入 1~28 个字符。

备注　　添加对当前组的说明信息。

组列表

在组列表中，可以对已创建的组进行相应设置。

提示:

当删除组时，所有引用该组的规则都会被删除。

5.4.1.2. 用户设置

可以在此添加、修改或者删除用户。

界面进入方法：对象管理 >> 用户管理 >> 用户设置

图 5-20 用户设置界面

用户设置

用户名　　输入一个名称来标识一个用户，可以输入 1~28 个字符。

IP　　输入当前用户的 IP 地址。此处只能输入单个 IP 地址，如果需要设置 IP 地址段，请点击页面下方<批量处理>按钮进行操作。批量增加用户时，如果新增用户的 IP 地址与某个已有用户的 IP 地址重复，那么已有用户的信息将会被删除。

备注　　添加对当前用户的说明信息。

用户列表

在用户列表中，可以对已创建的用户进行相应设置。

5.4.1.3. 视图

可以在此设置用户视图或者组视图。

界面进入方法：对象管理 >> 用户管理 >> 视图

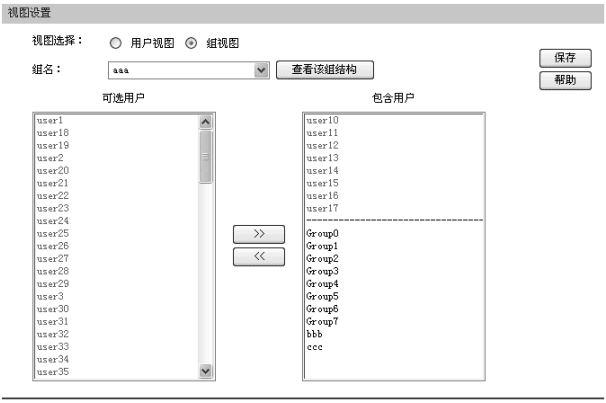


图 5-21 视图界面

视图设置

视图选择　选择需要设置的视图。可以选择“用户视图”为用户指定所属组，也可以选择“组视图”为组添加用户或子组。

用户名　选择“用户视图”，可在下拉菜单中选择所需设置的用户。

可选组　显示可以包含该用户的组。

所属组　显示已经包含该用户的组。

组名　选择“组视图”，可在下拉菜单中选择所需设置的组。

查看该组结构　可以查看以该组为根节点组成的树，树中包含该组的所有子组和用户，其中组名以粗体显示。

可选用户　显示该组可以包含的用户和子组。

包含用户　显示该组已经包含的用户和子组。

5.4.2.时间管理

5.4.2.1. 时间组

可以在此创建、修改或者删除时间组。

界面进入方法: 对象管理 >> 时间管理 >> 时间组

图 5-22 时间组界面

时间组设置

名称　　输入一个名称来标识一个时间组，可以输入 1-28 个字符。

备注　　添加对当前时间组的说明信息。

星期　　选择周循环的具体日期。

时间段　　设置一天 24 小时内的工作时间段。通过输入起止时间进行同一天内的时间段添加。时间段由两个部分组成:

开始时间：时间段的起始时间，由时分组成，格式为（00:00）。

结束时间：时间段的截止时间，由时分组成，格式为（00:00）。

可以输入时间段的范围为 00:00-24:00，时间段的每个设置框最多允许输入两位数字，一个设置框中输入完两位数字后，将自动跳转到下一个设置框。输入完成后，点击< + >按钮可以添加时间

段，点击< - >可以删除已经添加的时间段。最多可以设置 12 个不同时间段，各个时间段之间不能有交叠。

时间组列表

在时间组列表中，可以对已创建的时间组进行相应设置。

图 5-22序号 1 中名称为“ANY”的时间组，是路由器预定义的一个时间组，表示任何时间，此时间组不可修改、删除。序号 2 规则的含义：每一天上午 8 点到 11 点。

提示:

若时间组被其他规则引用，则该时间组无法删除。

5.5. 传输控制

5.5.1. 转发规则

路由器通过 NAT（Network Address Translation，网络地址转换）技术，可以在局域网主机主动发起对广域网的访问时实现双方的互相通信。其原理是：当通信数据包经过路由器时，NAT 技术会将数据包中的 IP 地址在局域网地址与广域网地址间转换，同时也进行端口号的转换。

如今随着计算机的普及，广域网 IP 地址已经供不应求，通过 NAT 技术，局域网内所有主机在通信时可以使用一个广域网 IP 地址，而局域网内不同的主机使用不同的端口号，解决了 IP 地址紧缺的问题。

在应用了 NAT 及其扩展技术的网络环境中，局域网主机是不会直接被广域网主机发现的，因此 NAT 也为局域网提供了一定的网络安全保障。当有广域网主机需要主动访问局域网主机时，就必须通过转发规则来实现。

5.5.1.1. NAT 映射

NAT 映射，可以将特定的局域网 IP 地址与指定的广域网 IP 地址唯一对应，多用于局域网内的服务器搭建。可在此设置 NAT 的端口范围和 NAT 映射关系。

界面进入方法：传输控制 >> 转发规则 >> NAT 映射

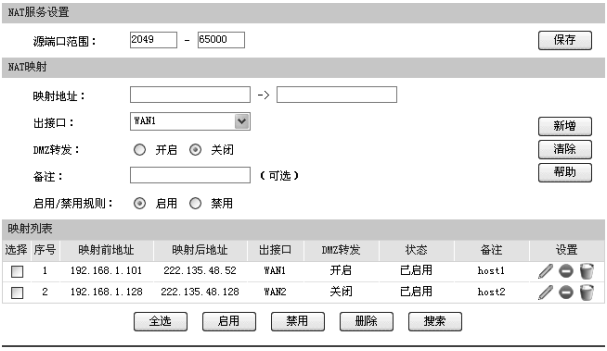


图 5-23 NAT 映射设置界面

NAT 服务设置

源端口范围　　设置作为 NAT 源端口的端口范围，范围跨度必须大于或等于 100。可设置范围为 2049-65000。

NAT **映射**

映射地址　　设置局域网 IP 地址和广域网 IP 地址的一对一映射。第一个输入框中应填写局域网 IP 地址，第二个输入框中应填写广域网 IP 地址。本路由器只允许 LAN 口到 WAN 口的映射。

出接口　　设定数据包发送出去的接口。

DMZ 转发　　设置是否开启该条 NAT 映射条目的 DMZ 转发。开启后所有广域网中发往映射后地址的数据报将被转发至映射前地址。

备注　　添加对本条目的说明信息。

启用/禁用规则　　设置该条 NAT 映射条目是否生效。

映射列表

在映射列表中，可以对已保存的 NAT 映射条目进行相应设置。

图 5-23序号 1 条目的含义：局域网主机 host1 的 IP 地址为 192.168.1.101，指定经 NAT 映射后的广域网 IP 地址为 222.135.48.52，数据包从 WAN1 口发送出去，DMZ 转发已开启，映射设置已启用。当 host1 与广域网通信时，从 WAN1 口发出的数据包源 IP 地址将被 NAT 转换为广域网 IP 地址 222.135.48.52，而从广域网返回的数据包目的 IP 地址会被 NAT 转换为局域网 IP 地址 192.168.1.101。

提示:

NAT 映射只适用于 WAN 口使用静态 IP 连接方式的场合。若 WAN 口连接方式从静态 IP 切换为动态 IP、PPPoE、L2TP 或 PPTP，以前设置的 NAT 映射都将失效，直接在动态 IP、PPPoE、L2TP 或 PPTP 连接状态下设置的 NAT 映射也都不起作用。

5.5.1.2. **多网段** NAT

多网段 NAT，可以支持 LAN 接口下多个网段的 IP 通过 NAT 转换访问广域网。

界面进入方法：传输控制 >> 转发规则 >> 多网段 NAT

图 5-24 多网段 NAT 设置界面

多网段 NAT 规则

网段地址　　设置需要进行 NAT 转换的网段地址，以子网掩码值划分地址范围。

启用/禁用规则　　设置该条多网段 NAT 规则是否生效。

备注　　添加对本条规则的说明信息。

规则列表

在规则列表中，可以对已保存的多网段 NAT 规则进行相应设置。

图 5-24序号 1 规则的含义：这是一条名为 1 的多网段 NAT 规则，路由器 LAN 口下的网段为 220.181.6.0/24，本条规则已启用。在进行相应的静态路由规则设置后，该网段将可以通过本路由器进行 NAT 转换之后访问广域网。

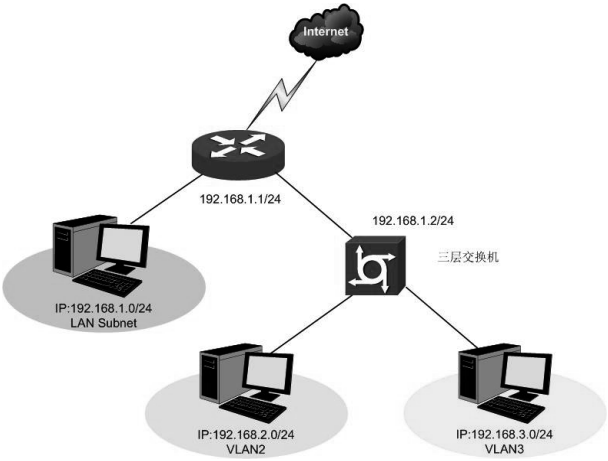
提示:

多网段 NAT 功能需要同时配置静态路由才能生效。

子网掩码值的相关设置请参考附录 A 常见问题中的**问题 5**。

举例:

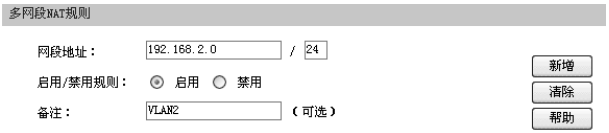
某网吧的网络结构如下:



路由器的 LAN 网段为 192.168.1.0 /24，三层交换机下 VLAN2 网段为 192.168.2.0 /24，VLAN3 网段为 192.168.3.0 /24，三层交换机与路由器的 LAN 口级联 VLAN IP 为 192.168.1.2。现要实现 VLAN2 和 VLAN3 网段可以访问互联网。

可以通过如下设置来实现:

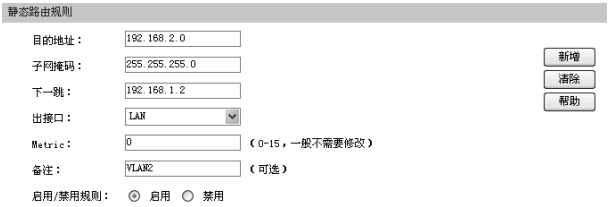
1. 首先设置多网段 NAT 规则，分别添加 VLAN2 与 VLAN3 的网段地址。



设置完成后的规则如下：

2. 然后设置相应的静态路由规则，指定下一跳为网段地址所属三层交换机与本路由器 LAN 口直接相连的接口 IP。

界面进入方法：传输控制 >> 路由设置 >> 静态路由



设置完成后的静态路由如下：

5.5.1.3. 虚拟服务器

在路由器默认设置下，广域网中的主机不能直接与局域网主机进行通信。为了方便广域网的合法用户访问本地主机，又要保护局域网内部不受侵袭，路由器提供了虚拟服务器功能。

可以通过虚拟服务器定义一个服务端口，并以 IP 地址指定其对应的局域网服务器，则广域网所有对此端口的服务请求都将被重定位到该服务器上。这样广域网的用户便能成功访问局域网中的服务器，同时不影响局域网内部的网络安全。

界面进入方法：传输控制 >> 转发规则 >> 虚拟服务器

图 5-25 虚拟服务器设置界面

NAT DMZ 服务

NAT DMZ 服务　　设置是否启用 NAT DMZ 服务。NAT DMZ 是 NAT 应用的一种特殊服务，相当于一条默认的转发规则。若主机开启了 NAT DMZ 服务，路由器会将所有由广域网发起的、不符合所有现有连接和转发规则的数据全部转发至指定的主机。

主机地址　　指定作为 NAT DMZ 服务器的主机 IP 地址。

虚拟服务

服务名称　　用户自定义，标识一条虚拟服务器规则。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。

外部端口　　为本条虚拟服务器规则指定路由器提供给广域网的服务端口或端口范围，广域网对该端口或端口范围的访问都将被重定位到局域网中指定的服务器。

内部端口　　指定局域网内虚拟服务器主机的实际服务端口。

服务协议　　指定应用本条虚拟服务器规则的数据包协议类型。

内部服务器 IP	为本条虚拟服务器规则指定局域网服务器的 IP 地址。外网对局域网指定端口的访问都将发送到该主机。
启用/禁用规则	设置是否应用本条虚拟服务器规则。

提示:

外部端口与内部端口的取值范围均为 1-65535 之间的任意整数。

不同虚拟服务器规则的外部端口取值不能相同，内部端口取值可相同。

服务列表

在服务列表中，可以对已保存的虚拟服务器规则进行相应设置。

图 5-25序号 1 规则的含义：这是一条名为 apply1 的虚拟服务器规则，由广域网向路由器端口 12892-12893 端口发起的 TCP/UDP 数据都将转发到局域网 IP 地址为 192.168.1.103 主机的 12892-12893 端口上，本条规则已启用。

5.5.1.4. 端口触发

由于防火墙的存在，一些如网络游戏、视频会议、网络电话、P2P 下载等应用程序需要通过设置转发规则才能正常工作，而这些应用程序又要求多个端口连接，针对单一端口的虚拟服务器功能已不能满足需求，此时就需要使用端口触发功能。

当一个应用程序向触发端口发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。

界面进入方法：传输控制 >> 转发规则 >> 端口触发

图 5-26 端口触发设置界面

端口触发

服务名称　　用户自定义，标识一条端口触发规则。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。

触发端口　　应用程序首先发起连接的一个或多个端口。只有该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。

触发协议　　设定在触发端口上使用的数据包协议类型。

开放端口　　为应用程序提供服务的一个或多个端口。当触发端口上发起连接后，开放端口打开，之后应用程序便可以通过这些开放端口发起后续连接。

开放协议　　设定在开放端口上使用的数据包协议类型。

启用/禁用规则　　设置是否应用本条端口触发规则。

提示:

触发端口与开放端口的取值范围均为 1-65535 之间的任意整数。开放端口取值可以指定一个连续的范围，如 8690-8696。

每条规则最多支持 5 组触发端口，且这些触发端口不能重叠。

每条规则最多支持 5 组开放端口，每条规则的开放端口数总和需小于或等于 100。

触发列表

在触发列表中，可以对已保存的端口规则进行相应设置。

图 5-26序号 1 规则的含义：这是一条名为 apply1 的端口触发服务规则，当局域网内发起端口为 5350 和 5354 的 TCP 访问时，对 TCP 和 UDP 协议开放 5355-5358 端口。

5.5.1.5. ALG 服务

ALG（Application Layer Gateway，应用层网关）。为了保证一些应用程序的正常使用，请开启 ALG 服务。

界面进入方法：传输控制 >> 转发规则 >> ALG 服务

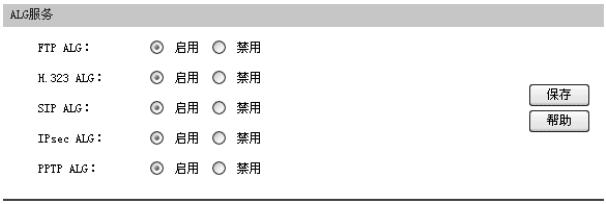


图 5-27 ALG 服务设置界面

ALG 服务

FTP ALG　　选择启用或禁用 FTP ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

H.323 ALG　选择启用或禁用 H.323 ALG 服务，默认为启用， H.323 多媒体协议多用于视频会议、IP 电话等场合。

SIP ALG　选择启用或禁用 SIP ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

IPsec ALG　选择启用或禁用 IPsec ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

PPTP ALG　选择启用或禁用 PPTP ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

5.5.2. 带宽控制

带宽控制功能通过对各种数据流设置相应的限制规则，实现对数据传输的带宽控制，从而使有限的带宽资源得到合理分配，达到有效利用现有带宽的目的。

5.5.2.1. 基本设置

界面进入方法：传输控制 >> 带宽控制 >> 基本设置

图 5-28 带宽控制基本设置界面

功能设置

不启用带宽控制　　勾选此项时，所有带宽控制设置均不生效。

启用普通带宽控制　　勾选此项以启用普通带宽控制功能。

启用智能带宽控制　　勾选此项以启用智能带宽控制功能。当带宽利用率达到指定的值时，带宽控制功能生效。

各接口带宽

接口　　显示路由器当前已启用的 WAN 口，以及总 WAN 口。总 WAN 口的带宽为已启用接口带宽之和。MR900只显示一个 WAN 口。

上行带宽　　显示对应 WAN 口数据流出的带宽上限，如需调整，请至**WAN设置**页面修改相应 WAN 口参数。

下行带宽　　显示对应 WAN 口数据流入的带宽上限，如需调整，请至**WAN设置**页面修改相应 WAN 口参数。

默认规则带宽

数据流向　　“上行”表示由局域网发送数据到广域网，如局域网内计算机向广域网上的 FTP 服务器上传文件；“下行”表示由广域网发送数据到局域网，如局域网内计算机从广域网上的 FTP 服务器下载文件。

最小保证带宽　　设置在物理带宽不足的前提下，对应数据流向至少能够享有的最小带宽。

最大限制带宽　　设置对应数据流向的带宽上限。

提示:

WAN 口的出入带宽必须小于或者等于 ISP 提供的参数。如果超过实际物理带宽，则带宽控制功能失效。

若有数据由 A 接口流入路由器后由 B 接口流出，而 A 接口入口带宽与 B 接口出口带宽不同时，以两者带宽的最小值为有效带宽。

通过页面上的<查看 IP 流量统计>按钮，可跳转至 IP 流量统计页面。

5.5.2.2. 带宽控制规则

可以在此设置带宽控制规则的参数。

界面进入方法: 传输控制 >> 带宽控制 >> 带宽控制规则

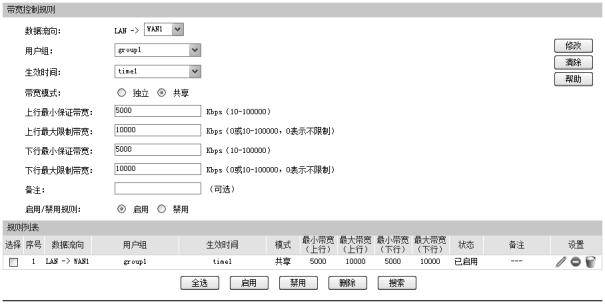


图 5-29 带宽控制规则设置界面

带宽控制规则

数据流向　　选择控制规则的数据流向。箭头方向代表数据流向和受控主机所在的域。MR900无此条目。

用户组　　设置受控数据包发出的源地址范围。由用户管理的组来表示。如需新建组，请参考**5.4.1用户管理**。

生效时间　　设置带宽规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。

带宽模式	独立模式即受控地址范围内每一个 IP 地址都将应用当前规则所设置的带宽限制；共享模式即受控地址范围内所有 IP 地址带宽总和为当前规则所设置的带宽限制。
上行最小保证带宽	设置上行最小保证带宽，即在物理带宽不足的前提下，上行数据流至少能够享有的最小带宽。
上行最大限制带宽	设置上行最大限制带宽，即上行数据流所能享有的最大带宽。
下行最小保证带宽	设置下行最小保证带宽，即在物理带宽不足的前提下，下行数据流至少能够享有的最小带宽。
下行最大限制带宽	设置下行最大限制带宽，即下行数据流所能享有的最大带宽。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条带宽控制规则。

规则列表

在规则列表中，可以对已保存的带宽控制规则进行相应设置。

图 5-29序号 1 规则的含义：处于 LAN 中的用户组“sales”内的主机共享带宽，当这些主机向广域网发送数据包时，保证上行和下行的最小带宽各为 5000Kbps，最大带宽各为 10000Kbps。该规则在时间组“time1”设置的时间段内生效。

提示:

单条规则生效的前提是：这条带宽控制规则所属接口的物理带宽足够大，且尚未被用尽。

异常情况：各带宽控制规则的最小保证带宽之和大于总物理带宽。当某接口所有带宽控制规则的最小保证带宽之和大于此接口的物理带宽时，意味着无论如何都无法同时满足所有带宽控制规则的最小保证带宽。

5.5.3. 连接数限制

作为局域网的统一出口，路由器支持的 TCP 和 UDP 连接数是有限的，如果局域网内有部分主机向广域网发起的 TCP 和 UDP 数目过多，影响局域网其他计算机的通信质量，就有必要对这部分计算机进行连接数限制。

5.5.3.1. 连接数限制规则

可以在此对指定 IP 的计算机连接数限制进行设置。

界面进入方法：传输控制 >> 连接数限制 >> 连接数限制规则

图 5-30 连接数限制规则设置界面

功能设置

启用连接数限制　勾选此项以启用连接数控制。不勾选时，所有连接数限制均不生效。

连接数限制规则

组　设置需要进行连接数限制的主机的 IP 地址段，由用户管理的组来表示，限制规则将对组内每一个用户生效。如需新建组，请参考**5.4.1用户管理**。

最大连接数　为本条规则设置相应的最大连接数。

备注　　添加对本条规则的说明信息。

启用/禁用规则　　选择启用或禁用本条规则。

规则列表

在规则列表中，可以对已保存的连接数限制规则进行相应设置。

图 5-30序号 1 规则的含义：名为“局域网”组内的主机向广域网发起的最大连接数被限制为 100 条，该条规则已启用。

5.5.3.2. 连接数监控

监控列表显示局域网主机的连接数限制情况。

界面进入方法：传输控制 >> 连接数限制 >> 连接数监控

图 5-31 连接数监控界面

可通过监控列表搜索、查询已设置连接数限制规则的用户组主机连接数信息。如需获取最新信息，请点击<刷新>按钮。

5.5.4.流量均衡

合理设置流量均衡，可以使路由器在多 WAN 口模式下更安全、有效地收发数据。本功能仅适用于MR900B。

5.5.4.1. 基本设置

界面进入方法：传输控制 >> 流量均衡 >> 基本设置

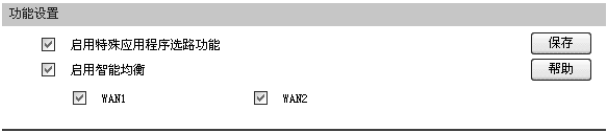


图 5-32 流量均衡基本设置界面

勾选“启用特殊应用程序选路功能”，路由器会将数据包的源 IP 地址与目的 IP 地址，或者源 IP 地址与目的端口地址作为一个整体，记录其通过的 WAN 口信息。后续如果有同一源 IP 地址和目的 IP/端口地址的数据包通过，则优先转发至上次记录的 WAN 口。该功能主要用于保证多连接应用程序的正常工作。

勾选“启用智能均衡”，并在下方选定 WAN 口，在没有任何选路规则的情况下，指定 WAN 口将自动进行流量均衡。

设置完成后点击<保存>按钮生效。

提示:

在实际应用中，如果某些 WAN 口没有连接到因特网，那么这些 WAN 口将不会参与智能均衡，请勿勾选。

5.5.4.2. 策略选路

在此可以通过指定协议、地址范围、端口、WAN 口、生效时间，更精确地控制路由选路。

界面进入方法: 传输控制 >> 流量均衡 >> 策略选路

图 5-33 策略选路设置界面

选路规则设置

协议类型　　在下拉列表中选择本条规则所针对的协议类型，不属于指定范围内的协议将不会应用选路规则。如果列表中没有您想指定的协议类型，可以参见**5.5.4.5 协议类型**进行添加，可通过下拉列表旁边的<协议类型>按钮快速进入设置界面。

源地址范围　　输入需要应用选路规则的源地址范围。输入 0.0.0.0 - 0.0.0.0 时表示匹配所有 IP。

目的地址范围　　输入需要应用选路规则的目的地址范围。输入 0.0.0.0 - 0.0.0.0 时表示匹配所有 IP。

源端口范围　　输入需要应用选路规则的源端口范围。只有当协议类型为 TCP、UDP、TCP/UDP 时可以指定范围，默认为 1 - 65535，表示匹配所有端口。

目的端口范围　　输入需要应用选路规则的目的端口范围。只有当协议类型为 TCP、UDP、TCP/UDP 时可以指定范围，默认为 1 - 65535，表示匹配所有端口。

WAN 接口　　勾选指定数据流通过的 WAN 口。

生效时间　　设置选路规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。

备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条策略选路规则。

规则列表

在规则列表中，可以对已保存的选路规则进行相应设置。

图 5-33序号 1 规则的含义：路由器收到源地址在 192.168.1.100 - 192.168.1.199 范围内，且发往目的地址 116.10.20.28 的数据包，不论端口与协议，全部从 WAN1 接口进行转发，该规则已启用，在时间组“time1”设置的时间段内生效。

5.5.4.3. ISP 选路

通过 ISP 选路功能，可以将数据包转发至对应的 ISP 线路上，从而减少数据包在网络中被转发的次数，提高网络性能。

界面进入方法：传输控制 >> 流量均衡 >> ISP 选路

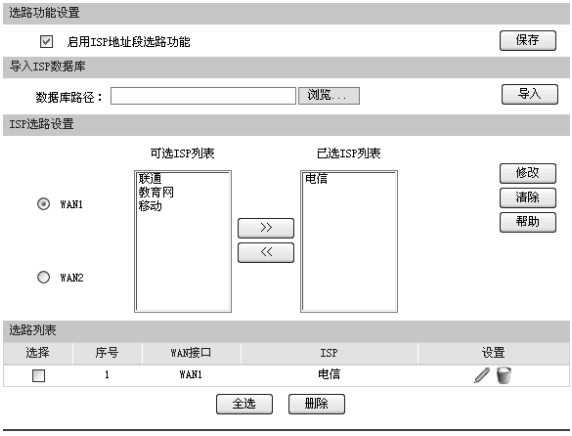


图 5-34 ISP 选路设置界面

选路功能设置

勾选“启用 ISP 地址段选路功能”，点击<保存>按钮，下方的选路设置才能生效。

导入 ISP 数据库

ISP 数据库即各 ISP 所拥有的 IP 地址段的数据库，通过匹配数据包目的 IP 地址与 ISP 数据库，路由器会将数据包从相应 ISP 所对应的 WAN 口转发。请在我司官方网站下载最新 ISP 数据库，单击<浏览>按钮，选择保存路径下的文件，点击<导入>即可。

ISP 选路设置

可选 ISP 列表　　系统定义的 ISP 列表。选中合适的 ISP，点击< >> >按钮将其移至“已选 ISP 列表”中，一个 WAN 口可以选择多个 ISP。如果某 WAN 口对应的 ISP 不在可选列表中，则不需要设置该 WAN 口的 ISP 选路。

已选 ISP 列表　　显示已经选择的 ISP。如果需要删除某个已选 ISP，请选中后点击< << >按钮将其移回“可选 ISP 列表”。

选路列表

在选路列表中，可以对已保存的 ISP 选路进行相应设置。

图 **5-34**序号 1 规则的含义：WAN1 接口对应电信 ISP，所有通过电信线路进入广域网的数据包将从 WAN1 口转发。

提示:

智能均衡、策略选路、ISP 选路三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：策略选路 > ISP 选路 > 智能均衡。

5.5.4.4. 线路备份

路由器默认所有 WAN 口都处于自动备份模式，当有 WAN 口发生故障时，其流量会均衡到其他 WAN 口上，当故障 WAN 口恢复后系统会再次均衡所有 WAN 口的流量。

根据实际需要合理设置线路备份，可以减轻 WAN 口流量负担，提高网络效率。

界面进入方法：传输控制 >> 流量均衡 >> 线路备份

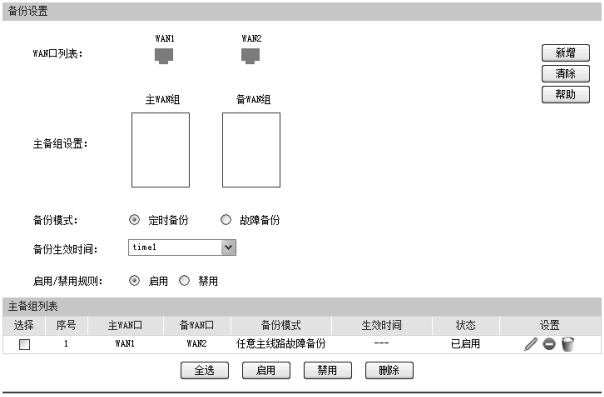


图 5-35 备份配置界面

备份配置

WAN 口列表　显示当前路由器所有正在工作的 WAN 口，可以拖动浅红色的 WAN 口图标，将其添加至下方的主 WAN 组或备 WAN 组中，若 WAN 口图标变为灰色，则表示该 WAN 口已经存在主备关系。

主备组设置　备 WAN 组中的 WAN 口将在指定条件下分担主 WAN 组中 WAN 口的流量。主 WAN 组可以包含一个或多个 WAN 口，备 WAN 组只能指定一个 WAN 口。

备份模式　可以选择定时备份或故障备份。选择定时备份时，下方可进行备份生效时间设置；选择故障备份时，下方可进行故障备份设置。

备份生效时间　设置备份生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。在生效时间内启动备份 WAN 口，关闭主 WAN 口。

故障备份　指定故障备份条件。在主 WAN 口正常工作时备份 WAN 口不工作，只有当符合故障备份条件时才会启动备份 WAN 口。

启用/禁用规则　选择启用或禁用本条主备配置规则。

主备组列表

在主备组列表中，可以对已保存的主备规则进行相应设置。

图 5-35序号 1 规则的含义：WAN1 口与 WAN2 口为主备关系，当 WAN1 口发生故障时启用 WAN2 口，该规则已启用。

提示:

主 WAN 组和备 WAN 组中不能放置相同的 WAN 口，且一个 WAN 口只能置入一个主备组中。

5.5.4.5. 协议类型

为了能够在定制选路策略时比较方便地指定应用选路规则的协议，设备提供了协议类型管理功能。每一个协议类型由协议名称和协议号两部分构成。系统已经预定义了 TCP、UDP、TCP/UDP 三种常用协议类型，也可以根据需要添加自定义协议类型。

界面进入方法：传输控制 >> 流量均衡 >> 协议类型

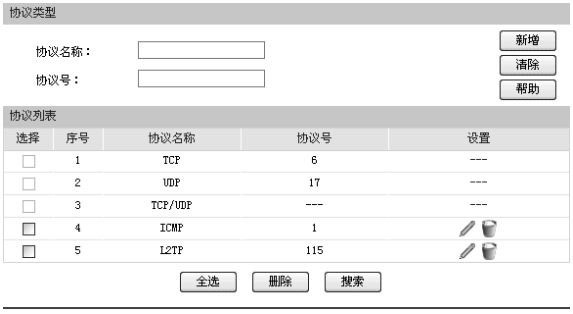


图 5-36 协议类型设置界面

协议类型

协议名称　　用户自定义，标识一条协议类型。该名称将显示在“访问规则”设置的服务类型下拉列表中。

协议号　　IP 数据包中协议字段的内容，取值范围为 0 - 255。

协议列表

在协议列表中，可以对自定义的协议类型条目进行相应设置。

提示:

系统预定义的协议类型不可进行配置操作。

5.5.5.路由设置

5.5.5.1. 静态路由

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

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

界面进入方法: 传输控制 >> 路由设置 >> 静态路由

图 5-37 静态路由设置界面

静态路由规则

目的地址	设定数据包需要到达的目的 IP 地址。
子网掩码	设定目的 IP 地址的子网掩码。
下一跳	指定一个 IP 地址，路由器下一步会将符合条件的数据包转发到该地址上。
出接口	设定数据包发送出去的接口。
Metric	设定路由规则的优先级，数值越低则优先级越高。如无特殊需要请保持默认值 0。
备注	添加对本条规则的说明信息。

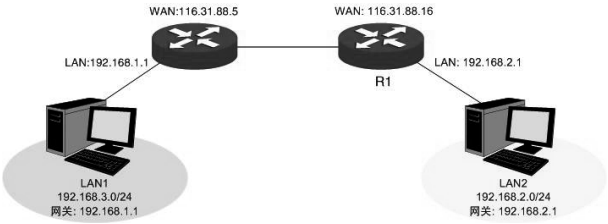
规则列表

在规则列表中，可以对已保存的静态路由规则进行相应设置。

图 5-37序号 1 规则的含义：如果有数据包发往一个 IP 地址为 192.168.3.56，子网掩码为 255.255.255.255 的设备，则路由器会将数据包从 LAN 口转发至下一跳地址 192.168.3.1，该路由规则已启用，优先级为 0。

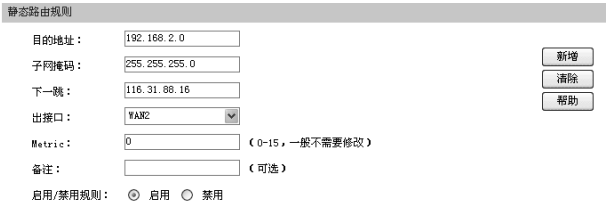
举例：

某拓扑结构如下图所示：



路由器的 LAN 口连接 LAN1（192.168.1.0/24）网段，另一路由器 R1 的 LAN 口连接 LAN2（192.168.2.0/24）网段，两个路由器的 WAN 口互连，WAN 口 IP 地址处于同一网段。现在路由器下 LAN1 网段中的一台主机需要访问 LAN2 网段的主机。

可以通过在路由器上设置一条静态路由来实现。在路由器静态路由界面设置到 LAN2 网段的下一跳地址为路由器 R1 的 WAN 口地址 116.31.88.16，如下图。最后点击<新增>按钮保存规则。



5.6. **防火墙**

5.6.1.ARP **防护**

一台主机向局域网内另一台主机发送 IP 数据包，此时设备需要通过 MAC 地址确定目的接口才能进行通信，而 IP 数据包中不包含有 MAC 地址信息，因此需要将 IP 地址解析为 MAC 地址。ARP（Address Resolution Protocol，地址解析协议）正是用来实现这一目的的网络协议。网络中的所有设备，包括路由器和计算机在内，都各自维护一份 ARP 列表，该列表建立了主机 IP 地址和 MAC 地址一一对应关系。

按照 ARP 协议的设计，设备通过数据包的交互学习到其他设备的 IP 地址和 MAC 地址信息，并将这些信息添加至自身的 ARP 表中。每次通信时会先通过该表查找对应地址，减少网络上过多的 ARP 通信量。但设备同时也会接收不是自己主动请求的 ARP 应答，这就为“ARP 欺骗”创造了条件。

ARP 欺骗是局域网的攻击主机发送 ARP 欺骗包，将伪造的 IP 与 MAC 对应关系替换设备 ARP 列表中的记录，从而导致局域网内计算机不能正常上网。这类 ARP 攻击严重影响了局域网内部通信，由此便产生了 ARP 防护技术。

5.6.1.1. IP MAC **绑定**

IP MAC 绑定是一种防护技术，能够防止 ARP 列表被伪造的 IP MAC 对应信息替换。

界面进入方法：防火墙 >> ARP 防护 >> IP MAC 绑定

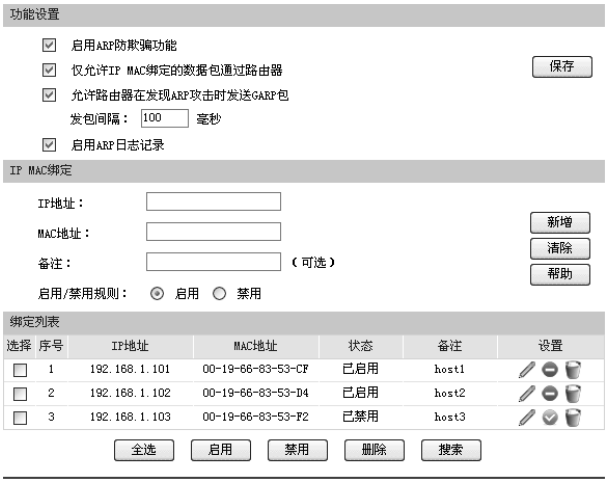


图 5-38 IP MAC 绑定设置界面

功能设置

推荐勾选所有项目，但请注意在勾选“仅允许 IP MAC 绑定的数据包通过路由器”选项前，先将管理主机的 IP MAC 信息导入绑定列表中，并设置生效。

当路由器受到 ARP 攻击时，路由器会将自身正确的 ARP 列表信息以 GARP（Gratuitous ARP，免费 ARP）包的方式主动发送给被攻击的设备，从而替换该设备错误的 ARP 列表信息。可在发包间隔处指定发包速率。

勾选“启用 ARP 日志记录”后路由器会将 ARP 日志发送到指定的日志服务器中。日志服务器地址即**5.10.5系统日志**中设置的服务器地址。

IP MAC 绑定

IP 地址　　手动输入需要进行绑定的 IP 地址。

MAC 地址　　手动输入与 IP 地址正确对应的 MAC 地址。

备注　　添加对本条目的说明信息。

启用/禁用规则　　选择启用或禁用本条绑定规则。

绑定列表

在绑定列表中，可以对已保存的 ARP 绑定条目进行相应设置。

图 5-38序号 1 条目的含义：目前路由器已将 IP 地址 192.168.1.101 与 MAC 地址 00-19-66-83-53-CF 进行绑定，该绑定规则已启用。

提示:

若当前绑定列表中所有条目都未启用，在勾选“仅允许 IP MAC 绑定数据包通过路由器”的功能设置选项并保存后，将无法登录路由器 Web 管理界面，此时必须将路由器恢复出厂配置才能再次登录。

5.6.1.2. ARP **扫描**

ARP 扫描界面可以将指定范围内的 IP 与其对应 MAC 地址全部扫描出来，在扫描列表中显示。

界面进入方法：防火墙 >> ARP 防护 >> ARP 扫描

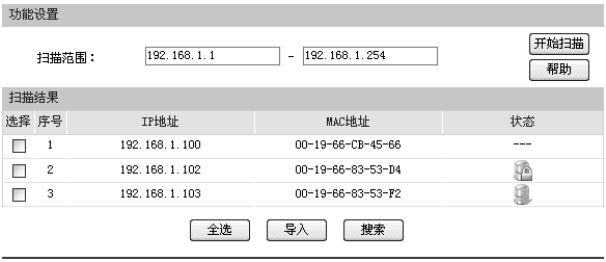


图 5-39 ARP 扫描界面

在扫描范围填入起始 IP 与结束 IP 后，点击<开始扫描>按钮，路由器将扫描该范围内所有正在工作的主机，并将它们对应的 IP MAC 地址信息显示在扫描列表中。

扫描结果中显示的 IP MAC 地址对应信息条目并不代表已经被绑定，在“状态”一列中会标识当前状态:

符号“---”表示当前条目未被绑定，可能会被错误的 ARP 信息更替掉;

图片表示当前条目已导入“IP MAC 绑定”界面的绑定列表中，但还未绑定生效;

图片表示当前条目已进行绑定，可以防御 ARP 攻击。

若现在需要绑定扫描列表中未绑定的条目，可以在“选择”一列勾选这些条目，然后点击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效。

提示:

若局域网内已经存在 ARP 攻击导致部分主机通信异常，则不可通过扫描方式添加绑定，请在“IP MAC 绑定”界面进行手动绑定。

5.6.1.3. ARP **列表**

路由器会将近期与其通信过的主机 IP MAC 对应信息保存在 ARP 列表中。

界面进入方法: 防火墙 >> ARP 防护 >> ARP 列表

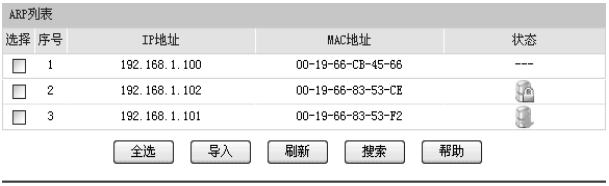


图 5-40 ARP 列表界面

ARP 列表条目的操作可参考**5.6.1.2 ARP 扫描**的扫描列表。

列表中未绑定的条目并不是一直存在，除了会被新的 IP MAC 对应信息更替之外，还会由于长时间未通信而自动从列表中删除，这个时间段就是 ARP 信息的老化时间。

5.6.2.攻击防护

攻击防护可防止广域网对路由器或局域网内计算机进行端口扫描和恶意攻击，以此来保证它们的安全运行。

界面进入方法：防火墙 >> 攻击防护 >> 攻击防护

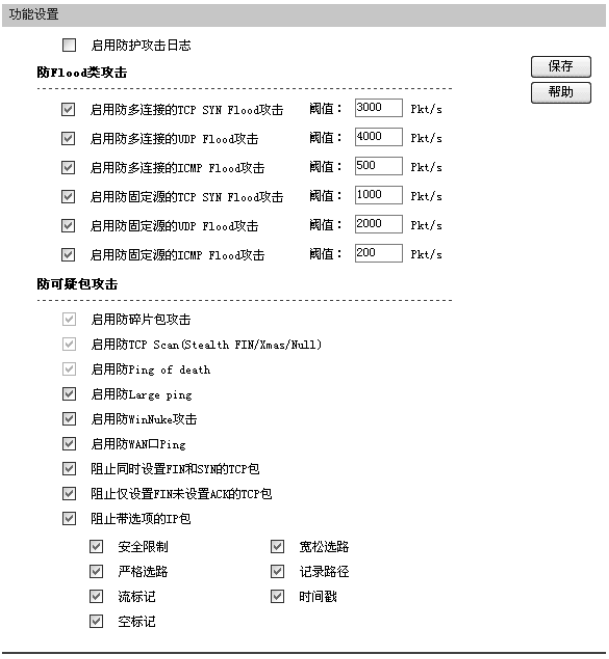


图 5-41 攻击防护设置界面

功能设置

启用防护攻击日志　　勾选此项后路由器会记录相关的防护日志。

防 Flood 类攻击　　Flood 类攻击是 DoS 攻击的一种常见形式。DoS（Denial of Service，拒绝服务）是一种利用发送大量的请求服务占用过多的资源，让目的路由器和服务器忙于应答请求或等待不存在的连接回复，而使正常的用户请求无法得到响应的攻击方式。常使用的 Flood 洪水攻击包括 TCP SYN，UDP，

ICMP 等。推荐勾选界面上所有防 Flood 类攻击选项并设定相应阈值，如不确定，请保持默认设置不变。

防可疑包类　　可疑包即非正常数据包，有可能是病毒或攻击者的扫描试探。推荐勾选界面上所有防可疑包选项。

5.6.3.MAC 过滤

在此可以通过指定 MAC 地址对部分局域网主机进行过滤。

界面进入方法：防火墙 >> MAC 过滤 >> MAC 过滤

图 5-42 MAC 过滤设置界面

功能设置

若需要严格控制局域网内某些计算机访问广域网，推荐勾选“启用 MAC 地址过滤功能”，并根据实际情况选择一种过滤规则。

MAC 地址过滤规则

MAC 地址　　输入需要控制的局域网主机 MAC 地址。

备注　　添加对本条规则的说明信息。

规则列表

在规则列表中，可以对已保存的 MAC 地址条目进行相应设置。

5.6.4. 访问策略

5.6.4.1. 访问规则

界面进入方法：防火墙 >> 访问策略 >> 访问规则

图 5-43 访问规则设置界面

访问规则

策略类型　　在下拉列表中选择适用于本条规则的策略类型，可选择阻塞或者允许。若选择阻塞，则符合该条规则的所有数据包将无法通过路由器；若选择允许，则符合该条规则的数据包能通过路由器。

服务类型　　在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的服务将不会应用过滤规则。例如在策略为阻塞的前提下，只选定了 FTP 一种服务类型时，其他服务类型的数据包仍旧可以通过路由器。如果列表中没有合适的服务类型，可以参见**5.6.4.2服务类型**进行添加，可通过下拉列表旁边的<服务类型>按钮快速进入设置界面。

生效接口域　　在下拉列表中选择本条规则所针对的接口域，可选择 WAN 或者 LAN。选择 WAN（LAN）时表示所有 WAN（LAN）接口。当接收报文的接口为指定接口域时，该规则生效。

源地址范围	选择指定地址范围的方式，若选择“IP/MASK”方式，则应输入需要管理的地址，以子网掩码值划分地址范围；若选择“IP 地址段”方式，则应输入需要管理的 IP 地址范围；若选择“ANY”方式，则表示该范围包括所有 IP 地址；若选择“组”方式，则应在下拉菜单中选择相应的组来指定地址范围，如需新建组，请参考**5.4.1用户管理**。
目的地址范围	选择指定地址范围的方式，若选择“IP/MASK”方式，则应输入需要限制访问的地址，以子网掩码值划分地址范围；若选择“IP 地址段”方式，则应输入需要限制访问的 IP 地址范围；若选择“ANY”方式，则表示该范围包括所有 IP 地址。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
指定位置	勾选该项后，可以将当前设置的条目添加到访问规则列表中指定序号的位置。默认情况下，规则新增生效后会显示在访问规则列表的最后。

规则列表

在规则列表中，可以对已保存的访问规则进行相应设置。在规则列表中，序号数字越小的规则，执行的优先级越高。

图 5-43序号 1 规则的含义：192.168.1.0/24 网段的主机在时间组“time1”设置的时间段内向广域网 116.10.20.0/24 网段发送的 TELNET 服务数据包将无法通过路由器。

提示:

局域网内没有设置规则的 IP 段，默认的策略类型是允许。

子网掩码值的相关设置请参考附录 A 常见问题中的**问题 5**。

5.6.4.2. 服务类型

为了能够在定制防火墙策略时比较方便地指定需要过滤的协议和端口号，设备提供了服务类型管理功能。每一个服务类型由协议类型和端口范围两部分构成。系统已经预定义了如 HTTP、FTP、TELNET 等常用服务类型，也可以根据需要添加自定义服务类型。

界面进入方法：防火墙 >> 访问策略 >> 服务类型

图 5-44 服务类型设置界面

服务类型

服务名称　　用户自定义，标识一条服务类型。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。该名称将显示在“访问规则”设置的服务类型下拉列表中。

协议类型　　设置协议类型，可供用户定义的协议类型有 TCP、UDP、TCP/UDP。

目的端口范围　　设定该服务所使用的端口号范围。起始端口号不能大于结束端口号。

服务列表

在服务列表中，可以对自定义的服务类型条目进行相应设置。

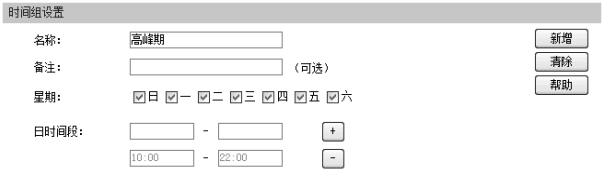
提示:

系统预定义的服务类型不可进行配置操作。

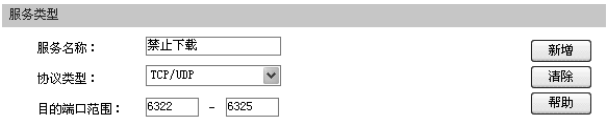
举例:

需求：某企业为使网络顺畅运行，希望实现在上网高峰期（每天上午 10 点到晚上 22 点）禁止 192.168.1.0/24 网段内某下载工具（端口 6322-6325）的使用，而在其它时间不限制该下载工具的使用。

此需求可以通过设置访问规则来实现。首先，需要新增一个时间组，名称为高峰期，设置时间 10：00—22：00，设置完成后点击<新增>按钮保存生效。



然后，需要新增一个服务类型，设置 6322-6325 为服务端口，设置完成后点击<新增>按钮保存生效。



选择刚设置的“高峰期”时间组和“禁止下载”服务类型，新增一条禁止 192.168.1.0/24 网段通过 6322-6325 端口访问广域网的访问规则。最后点击<新增>按钮保存生效，完成设置。

5.7. 行为管控

5.7.1. 应用限制

5.7.1.1. 应用限制

可以在此启用并设置应用限制功能。本路由器可限制的应用包括即时通信、P2P 软件、金融软件、游戏软件、视频软件、音乐软件、网页游戏、基础应用和代理。同时，可以对这些功能的使用情况做日志记录。

界面进入方法：行为管控 >> 应用限制 >> 应用限制

图 5-45 应用限制设置界面

功能设置

勾选“启用应用限制功能”后，应用限制的相关设置才会生效，应用限制生效后局域网指定用户对指定软件的网络应用将受到限制。

应用限制设置

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。
禁用	可以点击<应用列表>在弹出的选择框中对应用进行设置。可以设置的应用包括即时通信、P2P 软件、金融软件、游戏软件、视频软件、音乐软件、网页游戏、基础应用和代理。默认为对除了基础应用和代理的所有应用进行限制。
记录	可以点击<应用列表>在弹出的选择框中勾选进行日志记录的应用。可以设置的应用包括即时通信、P2P 软件、金融软件、游戏软件、视频软件、音乐软件、网页游戏、基础应用和代理。默认为对除了基础应用和代理的所有应用进行记录。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

规则列表

在规则列表中，可以对已保存的应用限制进行相应设置。

图 5-45序号 1 规则的含义：对用户组“group1”内的主机进行了应用限制，点击禁用列表下的“查看”可在弹出的选择框中看到受限制的应用，点击记录列表下的“查看”可在弹出的选择框中看到进行日志记录的应用。在时间组“time1”设置的时间段内应用限制生效。该规则已启用。

5.7.1.2. QQ **黑白名单**

可以在此对特殊 QQ 号码进行相关设置，实现不同用户、不同时间登录 QQ 的需求。同时，可以将用户使用 QQ 的情况，记录到系统日志。

界面进入方法：行为管控 >> 应用限制 >> QQ 黑白名单

图 5-46 QQ 黑白名单界面

全局设置

勾选“启用 QQ 黑白名单功能”后，QQ 黑白名单的相关设置才会生效。

规则设置

用户组　　可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。

规则类型　　可以选择白名单，使规则中的号码不被限制；也可以选择黑名单，使规则中的号码被限制。

QQ 号码　　在此输入 QQ 号码，可以同时输入多个 QQ 号码进行批量添加，通过使用空格、逗号或者回车换行来表示不同的 QQ 号码。

当使用上述 QQ 时　　可以勾选“记录到系统日志”，系统将记录上述号码的使用情况；如果不勾选，系统将不对上述号码作记录。

生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

规则列表

在规则列表中，可以对已保存的规则进行相应设置。序号数字越小的规则，执行的优先级越高。

图 5-46序号 1 规则的含义：该规则已经启用，在用户组 “group1” 内的主机在时间组 “time1” 设置的时间段内，被设置的 QQ 号码不可以登录。

提示:

在没有配置应用限制规则和 QQ 黑名单的情况下，路由器默认所有用户所有 QQ 在任意时间都是可登录的。

举例:

应用需求:

某企业有多名员工，该企业需要设置 IP 地址为 10.1.1.30 - 10.1.1.35 的员工可以在星期一到星期五的 08: 00 到 18: 00 登录 QQ，禁止其余所有员工任何时间登录 QQ。

实现方法:

有两种配置方法可以实现此需求。

方法一：配置一条 QQ 黑名单规则禁止所有员工任何时间登录 QQ，再配置一条 QQ 白名单规则允许 IP 地址为 10.1.1.30 - 10.1.1.35 的员工可以在星期一到星期五的 08：00 到 18：00 登录 QQ。QQ 白名单规则序号要在 QQ 黑名单规则之前。

方法二：配置一条应用限制规则禁止所有员工任何时间登录 QQ，再配置一条 QQ 白名单规则允许 IP 地址为 10.1.1.30 - 10.1.1.35 的员工可以在星期一到星期五的 08：00 到 18：00 登录 QQ。

配置步骤:

在配置应用限制规则或者 QQ 黑白名单规则之前，需要先设置所需用户组与时间组，设置如下:

1. 设置用户组，组内成员 IP 地址为 10.1.1.30 - 10.1.1.35。

界面进入方法：对象管理 >> 用户管理

进入标签页**组设置**，设置用户组名称:

组名称 可使用 QQ 组

进入标签页**用户设置**，设置用户 IP 地址，此处可进行批量添加，批量添加内容如下:

操作 增加

起始 IP 地址 10.1.1.30

结束 IP 地址 10.1.1.35

用户名前缀 可使用 QQ 用户

起始序号 1

步长 1

进入标签页**视图**，将可使用 QQ 用户 1-6 移到可使用 QQ 组中。

视图选择 组视图

组名 可使用 QQ 组

包含用户 可使用 QQ 用户 1、可使用 QQ 用户 2、可使用 QQ 用户 3、可使用 QQ 用户 4、可使用 QQ 用户 5、可使用 QQ 用户 6

2. 设置时间组，时间选择为星期一到星期五的 08：00 到 18：00。

界面进入方法：对象管理 >> 时间管理 >> 时间组

时间组设置内容如下:

名称 上班时间

星期 一、二、三、四、五

日时间段 08：00 - 18：00

设置完成后的时间组如下:

时间组列表

选择	序号	组名称	生效时间	备注	设置
☐	1	ANY	永久生效	---	---
☐	2	上班时间	一 二 三 四 五 08:00-18:00	---	

方法一:

界面进入方法：行为管控 >> 应用限制 >> QQ 黑白名单

全局设置如下:

勾选“启用 QQ 黑白名单功能”，点击<保存>按钮使设置生效。

QQ 黑名单规则设置内容如下:

用户组 ANY

规则类型 黑名单：禁止下列 QQ 号码登录

QQ 号码 禁止登录的员工的 QQ 号码

当使用上述 QQ 时 勾选“记录到系统日志”

生效时间 ANY

启用/禁用规则 启用

QQ 白名单规则设置内容如下:

用户组 可使用 QQ 组

规则类型 白名单：允许下列 QQ 号码登录

QQ 号码 允许登录的员工的 QQ 号码

当使用上述 QQ 时 勾选“记录到系统日志”

生效时间 上班时间

启用/禁用规则 启用

指定位置 勾选，输入 1

设置完成后的规则如下:

规则列表

选择	序号	用户组	规则类型	生效时间	状态	备注	设置
☐	1	可使用QQ组	白名单	上班时间	已启用	---	
☐	2	ANY	黑名单	ANY	已启用	---	

方法二:

1. 设置应用限制，限制任何用户在任意时间登录 QQ。

界面进入方法：行为管控 >> 应用限制 >> 应用限制

功能设置如下:

勾选“启用应用限制功能”，点击<保存>按钮使设置生效。

应用限制设置内容如下:

用户组 ANY

禁用应用列表 腾讯 QQ

记录应用列表 腾讯 QQ

生效时间 ANY

启用/禁用规则 启用

设置完成后的规则如下:

2. 设置 QQ 白名单，允许可使用 QQ 组在上班时间登录 QQ。

界面进入方法：行为管控 >> 应用限制 >> QQ 黑白名单

全局设置如下:

勾选“启用 QQ 黑白名单功能”，点击<保存>按钮使设置生效。

QQ 白名单规则设置内容如下:

用户组 可使用 QQ 组

规则类型 白名单：允许下列 QQ 号码登录

QQ 号码 允许登录的员工的 QQ 号码

当使用上述 QQ 时 勾选“记录到系统日志”

生效时间 上班时间

启用/禁用规则 启用

设置完成后的规则如下:

5.7.1.3. MSN **黑白名单**

可以在此对特殊 MSN 账号进行相关设置，实现不同用户、不同时间登录 MSN 账号的需求。同时，可以将用户使用 MSN 账号的情况，记录到系统日志。

界面进入方法：行为管控 >> 应用限制 >> MSN 黑白名单

图 5-47 MSN 黑白名单界面

全局设置

勾选“启用 MSN 黑白名单功能”后，MSN 黑白名单的相关设置才会生效。

规则设置

用户组　　可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。

规则类型	可以选择白名单，使规则中的账号不被限制；也可以选择黑名单，使规则中的账号被限制。
MSN 账号	在此输入 MSN 账号，可以同时输入多个 MSN 账号进行批量添加，通过使用空格、逗号或者回车换行来表示不同的 MSN 账号。
当使用上述 MSN 时	可以勾选“记录到系统日志”，系统将记录上述账号的使用情况；如果不勾选，系统将不对上述账号作记录。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

规则列表

在规则列表中，可以对已保存的规则进行相应设置。序号数字越小的规则，执行的优先级越高。

图 5-47序号 1 规则的含义：该规则已经启用，在用户组“group1”内的主机在时间组“time1”设置的时间段内，被设置的 MSN 账号不可以登录。

提示:

在没有配置应用限制规则和 MSN 黑名单的情况下，路由器默认所有用户所有 MSN 账号在任意时间都是可登录的。

该功能应用与 QQ 黑白名单应用类似，可参考 QQ 黑白名单介绍后的应用举例。

5.7.2. 网址过滤

5.7.2.1. 网站分组

可以在此对网站进行分组，以便设置网站过滤规则。

界面进入方法：行为管控 >> 网址过滤 >> 网站分组

图 5-48 网站分组设置界面

网站分组设置

组名称　　输入一个名称来标识一个网站组，可以输入 1-28 个字符。

组成员　　在此输入网站分组成员。组成员可以为域名，如 www.mercurycom.com.cn，也可以在域名前面加通配符‘*’，如 *.mercurycom.com.cn，但‘*’只允许输入在域名最前面，而不能夹杂在域名中间或后面。可以同时输入多个网站进行批量添加，通过使用空格、逗号或者回车换行来表示不同的网站。每组最多可以

输入 200 个网站。

文件路径　可以通过上传 txt 文件添加组成员，txt 文件内容需按照组成员添加的格式进行编辑，上传完成后，文件内容将显示在组成员文本框中。

网站分组列表

在网站分组列表中，可以对已保存的网站分组进行相应设置。路由器预定义了部分网站分组，可以在此查看、编辑。

提示:

若网站分组被网站过滤规则引用，则该网站分组只能修改不能删除。

5.7.2.2. 网站过滤

可以在此对不同的用户组设置网站过滤规则，限制不同用户、不同时间登录的网站，同时，可以将用户登录网站的情况，记录到系统日志。还可以设置当用户登录禁止的网站时，弹出警告或者重定向至所设网站。

界面进入方法：行为管控 >> 网址过滤 >> 网站过滤

图 5-49 网站过滤设置界面

功能设置

勾选“启用网站过滤功能”后，网站过滤的相关设置才会生效。

网站过滤设置

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。
规则类型	选择允许或禁止访问下列网站分组。
选择网站	可以选择“所有网站”，使规则对任意网站生效；也可以选择并且点击<网站分组列表>，在弹出的选择框中对已有的网站分组进行勾选。如需新建网站分组，请参考**5.7.2.1网站分组**。
访问上述网站时	勾选“记录到系统日志”，规则条目生效时，符合规则的网站访问会被记录到系统日志； 勾选“弹出警告”，规则条目生效时，符合规则的网站访问发生时会弹出警告窗； 勾选“重定向至”并输入网站，规则条目生效时，符合规则的网站访问发生时会重定向到相应的网站。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

规则列表

在规则列表中，可以对已保存的规则进行相应设置。序号数字越小的规则，执行的优先级越高。

图 5-49序号 1 规则的含义：对用户组“group1”内的主机进行了网站过滤，过滤规则是禁止访问网站分组，点击“查看”可在弹出的选择框中看到被禁止访问的网站分组。在时间组“time1”设置的时间段内网站过滤生效。该规则已启用。

提示:

网站过滤、URL 过滤及网页安全三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：URL 过滤 > 网页安全 > 网站过滤。当访问请求可以匹配优先级高的规则，并被“允许”通过时，将跳过后续的网址匹配功能检查。

5.7.2.3. URL 过滤

URL（Uniform Resource Locator，统一资源定位符），即广域网中标识资源位置的网络地址。URL 过滤能够实现对广域网网址的过滤，方便对局域网访问广域网的通信进行管理。

界面进入方法：行为管控 >> 网址过滤 >> URL 过滤

图 5-50 URL 过滤设置界面

功能设置

勾选“启用 URL 地址过滤功能”，URL 过滤的相关设置才会生效。

URL 地址过滤规则

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。
规则类型	选择允许或禁止访问下列的 URL 地址。 允许访问下列的 URL 地址：表示路由器将允许在 URL 过滤表中的 URL 地址数据包通过，而不受其他应用管理的限制。 禁止访问下列的 URL 地址：表示路由器将禁止在 URL 过滤表中的 URL 地址数据包通过。
过滤方式	选择一种过滤方式。“关键字”过滤即所有包含指定字符的 URL 地址全都进行过滤；“完整 URL”过滤则仅当 URL 地址完全匹配输入的完整 URL 地址时才能进行过滤。 可以同时输入多个关键字或完整 URL 进行批量添加，通过使用空格、逗号或者回车换行来表示不同的关键字或完整 URL。最多可以添加 10 个关键字或完整 URL，每一个关键字或完整 URL 的可输入长度为 1-28 个字符。
关键字	当过滤方式为“关键字”的时候，可在此输入指定的关键字字符。
URL 地址	当过滤方式为“完整 URL”的时候，可在此输入完整的广域网 URL 地址。
访问上述 URL 时	勾选“记录到系统日志”，规则条目生效时，符合规则的 URL 访问会被记录到系统日志； 勾选“弹出警告”，规则条目生效时，符合规则的 URL 访问发生时会弹出警告窗； 勾选“重定向至”并输入网站，规则条目生效时，符合规则的 URL 访问发生时会重定向到相应的网站。

生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

规则列表

在规则列表中，可以对已保存的规则进行相应设置。序号数字越小的规则，执行的优先级越高。

举例：

某企业希望任何时间都禁止局域网内的主机访问网站：www.baidu.com 以及 sina。

可以通过设置 URL 过滤实现此需求。需要设置完整 URL 过滤 “www.baidu.com”，以及关键字过滤 “sina”，如下图所示，设置完成后点击<新增>按钮保存生效。

5.7.3. 网页安全

可以在此对不同的用户组设置网页安全规则，限制不同用户、不同时间可进行的网页操作。可以直接禁止所有的 HTTP POST 提交，使得所有页面上的请求按钮失效，点击页面链接，不会有页面返回。也可以针对网页请求中的文件类型，例如：exe、java、htm 等，限制用户网页操作。

界面进入方法：行为管控 >> 网页安全 >> 网页安全

图 5-51 网页安全设置界面

全局设置

勾选“启用网页安全功能”后，网页安全的相关设置才会生效。

规则设置

用户组　　可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**5.4.1用户管理**。

禁止网页提交　　勾选“启用”，可以禁止所有的 HTTP POST 提交。

过滤文件扩展类型　　可以在过滤文件扩展类型编辑框内输入多个扩展名，并以空格、逗号或者回车换行来分隔。

生效时间　　设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**5.4.2.1时间组**。

备注　　添加对本条规则的说明信息。

启用/禁用规则　　选择启用或禁用本条规则。

规则列表

在规则列表中，可以对已保存的规则进行相应设置。

图 5-51序号 1 规则的含义：对用户组“group1”内的主机设置了网页安全，组内所有主机在“time1”设置的时间段内，都不能访问扩展类型为 exe 的网页。

5.7.4. 策略库升级

可以在此进行应用特征数据库的升级。

界面进入方法：行为管控 >> 策略库升级 >> 策略库升级

图 5-52 策略库升级界面

应用特征数据库即“应用限制”界面限制列表中的所有应用，请在我司官方网站下载最新数据库，单击<浏览>按钮，选择保存路径下的文件，点击<升级>进行数据库升级。

5.8. VPN

VPN（Virtual Private Network，虚拟专用网）是一个建立在公用网（通常是因特网）上的专用网络，但因为这个专用网络只是逻辑存在并没有实际物理线路，故称为虚拟专用网。

随着因特网的发展壮大，越来越多的数据需要在因特网上进行传输共享，不过当企业将自身网络接入因特网时，虽然各地的办事处等外部站点可以很方便地访问企业网络，但同时也把企业内部的私有数据暴露给因特网上的所有用户。于是在这种开放的网络环境上搭建专用线路的需求日益强烈，VPN 应运而生。

VPN 通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。典型拓扑图如所示。

图 5-53 VPN 典型拓扑

隧道是通过对数据报的封装实现的，因为数据报封装和解封的过程都是在路由器上完成，所以对于用户来说是透明的。路由器支持的隧道协议包括三层隧道协议 IPsec 和二层隧道协议 L2TP/PPTP。

5.8.1.IKE

在 IPsec VPN 中，为了保证信息的私密性，通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE（Internet Key Exchange，互联网密钥交换）协议完成。

IKE 其实并非一个单独的协议，而是三个协议的混合体。这三个协议分别是 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议），该协议为交换密钥和 SA（Security Association，安全联盟）协商提供了一个框架；Oakley 密钥确定协议，该协议描述了密钥交换的具体机制；SKEME 安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

整个 IKE 协商过程被分为两个阶段。第一阶段，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在第二阶段中安全交换更多信息。第二阶段，使用第一阶段中建立的 ISAKMP SA 为 IPsec 的安全性协议协商参数，创建 IPsec SA，用于对双方的通信数据进行保护。至此，IKE 协商完毕。

5.8.1.1. IKE 安全策略

可以在此对 IKE 协商过程的相关参数进行设置。

界面进入方法：VPN >> IKE >> IKE 安全策略

图 5-54 IKE 安全策略设置界面

IKE 安全策略设置

安全策略名称　　为 IKE 安全策略命名。设置好的 IKE 安全策略可以被应用在 IPsec 安全策略中。

协商模式　　选择 IKE 的协商模式，通信双方必须使用相同的协商模式。在 IKE 协商的第一阶段定义了两种操作模式：主模式和野蛮模式。主模式中进行交换和认证的报文较多，并提供身份保护，适用于高安全性需求场合；野蛮模式中进行交换和认证的报文较少，不提供身份保护，但是协商速度快。

本地/对端 ID 类型　　设置本地和对端的 ID（Identity，身份标识）类型，用于进行 ID 的交换与验证，可以选择“IP 地址”或“NAME”，通信双方的设置需保持一致。

本地/对端 ID　　ID 类型选择“IP 地址”时，无需进行设置；ID 类型选择“NAME”时，可自定义本地/对端的 ID。路由器的“本地 ID”需与通信对端的“对端 ID”保持一致，而“对端 ID”则

	需与通信对端的“本地 ID”保持一致。
安全提议	选择用于 IKE 协商第一阶段的安全提议，如果下拉菜单中没有想选择的条目，请进入**5.8.1.2 IKE 安全提议**页面创建新条目。最多可以选择四条不同的安全提议。
预共享密钥	设置通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
生存时间	设定 ISAKMP SA 的生存时间。
DPD 检测开启	DPD（Dead Peer Detect，对端存活检测）开启后，IKE 一端能够定时主动检测对端的在线状态。
DPD 检测周期	当开启 DPD 检测时可设置检测周期。

IKE 安全策略列表

在 IKE 安全策略列表中，可以对已保存的 IKE 安全策略进行相应设置。

5.8.1.2. IKE **安全提议**

界面进入方法：VPN >> IKE >> IKE 安全提议

图 5-55 IKE 安全提议设置界面

IKE 安全提议设置

安全提议名称　为 IKE 安全提议命名。设置好的 IKE 安全提议可以被应用在 IKE 安全策略中。

验证算法　选择应用于 IKE 会话的验证算法。路由器支持两种验证算法，以下为其详细介绍。

MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生 128bit 的消息摘要，防止消息被篡改。

SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。

加密算法　选择应用于 IKE 会话的加密算法。路由器支持两种加密算法，以下为其详细介绍。

DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。

AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。

DH 组　Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。DH1/2/5 分别对应着 768/1024/1536 bit 的 DH 组。

IKE 安全提议列表

在 IKE 安全提议列表中，可以对已保存的 IKE 安全提议进行相应设置。

5.8.2.IPsec

IPsec（IP Security，IP 安全性）是一系列服务和协议的集合，在 IP 网络中保护端对端通信的安全性、防止网络攻击。

为了实现安全通信，通信双方的 IPsec 协议必须协商确定用于编码数据的具体算法、用于理解对方数据格式的安全协议，并通过 IKE 交换解密编码数据所需的密钥。

在 IPsec 中有两个重要的安全性协议 AH（Authentication Header， 鉴别首部）和 ESP（Encapsulating Security Payload， 封装安全性载荷）。AH 协议用于保证数据的完整性，若数据报文在传输过程中被篡改，报文接收方将在完整性验证时丢弃报文；ESP 协议用于数据完整性检查以及数据加密，加密后的报文即使被截取，第三方也难以获取真实信息。

5.8.2.1. IPsec **安全策略**

界面进入方法：VPN >> IPsec >> IPsec 安全策略

图 5-56 IPsec 安全策略设置界面

启用 IPsec 功能

只有勾选“启用”后，路由器才能应用 IPsec。

IPsec 安全策略设置

安全策略名称　　为 IPsec 安全策略命名。

启用安全策略	选择启用或禁用当前策略条目。
组网模式	选择 IPsec 安全策略的组网模式，站点到站点或者 PC 到站点。以下为选项的详细介绍。 站点到站点：当对端是一个子网时，可以选择该模式。 PC 到站点：当对端是一台主机时，可以选择该模式。
本地子网范围	设定本地子网地址，以子网掩码值划分地址范围。
对端子网范围	设定对方子网地址，以子网掩码值划分地址范围。当组网模式选择为 PC 到站点时，该项不可填。
选择 WAN 口	指定本地使用的 WAN 口。在通信对端的路由器上设置“对端网关”时必须填入该 WAN 口 IP 地址或域名。
对端网关	当组网模式选择为站点到站点，请在此输入通信对端的路由器相应 WAN 口的 IP 地址或域名。
对端主机	当组网模式选择为 PC 到站点，请在此输入通信对端主机的 IP 地址。
协商方式	建立 IPsec 安全隧道可以有两种协商方式。IKE 为自动协商，手动模式则需手动设定相关的安全参数。
IKE 安全策略	选择“IKE 协商”时，可以指定相应的 IKE 安全策略。如果下拉菜单中没有想选择的条目，请进入**5.8.1.1 IKE 安全策略**页面创建新条目。
安全提议	指定相应的 IPsec 安全提议。如果下拉菜单中没有想选择的条目，请进入**5.8.2.2 IPsec 安全提议**页面创建新条目。
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 第二阶段协商生成一个新的密钥材料，该密钥材料与第一阶段协商生成的密钥材料没有任何关联，这样即使 IKE 第一阶段的密钥被破解，第二阶段的密钥仍然安全。如

	果没有使用 PFS，第二阶段的密钥将根据第一阶段生成的密钥材料来产生，一旦第一阶段的密钥被破解，用于保护通信数据的第二阶段密钥也岌岌可危，这将严重威胁到双方的通信安全。PFS 是通过 DH 算法实现的，通信双方的 PFS 设置需保持一致。
生存时间	设定 IPsec SA 的生存时间。
入 SPI	选择“手动模式”时，可以设定 SPI 参数。SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPsec 安全联盟，通信对端的“出 SPI”值必须与此值相同。
入 AH MD5 密钥	当安全提议指定 IPsec 使用“AH”协议时，可以设定 AH MD5 验证算法的密钥。通信对端的“出 AH MD5 密钥”必须与此值相同。
入 ESP MD5 密钥	当安全提议指定 IPsec 使用“ESP”协议时，可以设定 ESP MD5 验证算法的密钥。通信对端的“出 ESP MD5 密钥”必须与此值相同。
入 ESP 3DES 密钥	当安全提议指定 IPsec 使用“ESP”协议时，可以设定 ESP 3DES 加密算法的密钥。通信对端的“出 ESP 3DES 密钥”必须与此值相同。
出 SPI	选择“手动模式”时，可以设定 SPI 参数。SPI 参数唯一标识一个 IPsec 安全联盟，通信对端的“入 SPI”值必须与此值相同。
出 AH MD5 密钥	当安全提议指定 IPsec 使用“AH”协议时，可以设定 AH MD5 验证算法的密钥。通信对端的“入 AH MD5 密钥”必须与此值相同。
出 ESP MD5 密钥	当安全提议指定 IPsec 使用“ESP”协议时，可以设定 ESP MD5 验证算法的密钥。通信对端的“入 ESP MD5 密钥”必须与此值相同。

出 ESP 3DES 密钥　当安全提议指定 IPsec 使用“ESP”协议时，可以设定 ESP 3DES 加密算法的密钥。通信对端的“入 ESP 3DES 密钥”必须与此值相同。

IPsec 安全策略列表

在 IPsec 安全策略列表中，可以对已保存的 IPsec 安全策略进行相应设置。

图 5-56序号 1 条目的含义：这是一条 IPsec 的隧道，组网模式为站点到站点，本地子网范围是 192.168.1.0/24，对端子网范围是 192.168.3.0/24，隧道使用 IKE 自动协商，该隧道已启用。

提示:

子网掩码值的相关设置请参考附录 A 常见问题中的**问题 5**。

5.8.2.2. IPsec **安全提议**

界面进入方法：VPN >> IPsec >> IPsec 安全提议

图 5-57 IPsec 安全提议设置界面

IPsec 安全提议设置

安全提议名称　为 IPsec 安全提议命名。设置好的 IPsec 安全提议可以被应用在 IPsec 安全策略中。

安全协议　　选择要使用的协议。

AH 验证算法　　当选择 AH 安全协议时可设定 AH 验证算法。路由器支持两种验证算法，以下为其详细介绍。

MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生 128bit 的消息摘要，防止消息被篡改。

SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。

ESP 验证算法　　当选择 ESP 安全协议时可设定 ESP 验证算法。路由器支持两种验证算法，以下为其详细介绍。

MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生 128bit 的消息摘要，防止消息被篡改。

SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。

ESP 加密算法　　当选择 ESP 安全协议时可设定 ESP 加密算法。路由器支持两种加密算法，以下为其详细介绍。

DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。

AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。

IPsec 安全提议列表

在 IPsec 安全提议列表中，可以对已保存的 IPsec 安全提议进行相应设置。

5.8.2.3. IPsec 安全联盟

在此将列出路由器上所有已成功建立的 IPsec 安全联盟相关信息。

界面进入方法：VPN >> IPsec >> IPsec 安全联盟


IPsec安全联盟列表

序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_1	303042544	in	172.30.70.151<- 172.30.70.161	192.168.1.0/24<- 192.168.3.0/24	ESP	---	MD5	3DES
2	IPsec_1	352312306	out	172.30.70.151->>172.30.70.161	192.168.1.0/24->>192.168.3.0/24	ESP	---	MD5	3DES

刷新 搜索 帮助

图 5-58 IPsec 安全联盟界面

图 5-58中显示的是图 5-56中 IPsec 安全策略列表序列 1 条目的连接情况。在本例中路由器使用 WAN2 接口进行隧道连接，WAN2 接口的 IP 地址为 172.30.70.151，对端网关地址为 172.30.70.161。IPsec 隧道的安全提议等相关设置需与对端路由设置相同。

由于安全联盟是单向的，所以当 IPsec 隧道成功建立后，每条隧道会产生一对出和入的安全联盟。出和入的 SPI 值是不同的，但与对端的入和出 SPI 值相同，即本端方向 in 的 SPI 值与对端方向 out 的 SPI 值相同。这条隧道在对端的连接信息如下图所示，SPI 值为 IKE 自动协商得出。


IPsec安全联盟列表

序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_1	352312306	in	172.30.70.161<- 172.30.70.151	192.168.3.0/24<- 192.168.1.0/24	ESP	---	MD5	3DES
2	IPsec_1	303042544	out	172.30.70.161->>172.30.70.151	192.168.3.0/24->>192.168.1.0/24	ESP	---	MD5	3DES

提示:

NAT 穿透

在实际网络应用中，IPsec VPN 通信双方的物理连接线路中可能存在着 NAT 网关，当数据包经过 NAT 网关时，其 IP 地址或端口号会改变，这就导致 VPN 隧道对端收到数据包后验证失败，数据包被直接丢弃。NAT 穿透功能可以解决这一问题，实现方法为在原 ESP 协议的报文外添加新的 IP 首部和 UDP 首部。这样数据包的格式为：新 IP/UDP 首部 | ESP 首部 | IP 首部 |数据。由于 NAT 网关只会改变最外层的 IP 首部，而且 ESP 校验不包含 IP 首部，所以此时 IPsec VPN 的通信不会受到影响。但是 NAT 穿透只适用于 ESP 协议，AH 协议的校验包含了 IP 首部，因此无法与 NAT 共存。

路由器目前仅在 IKE 协商模式为野蛮模式，且本地和对端的 ID 类型都为 NAME 的情况下支持 NAT 穿透。

5.8.3.L2TP/PPTP

二层 VPN 隧道协议包含 L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）和 PPTP（Point to Point Tunneling Protocol，点到点隧道协议）。

L2TP 和 PPTP 都是使用 PPP（Point to Point Protocol，点到点协议）进行数据封装，并都为数据增添额外首部。两者的区别如下表所示:

协议	介质	隧道	首部长度	隧道认证
PPTP	IP 网络	单隧道	至少 6 字节	不支持
L2TP	使用 UDP 的 IP 网络、帧中继虚电路、X.25 虚电路等	多隧道	至少 4 字节	支持

5.8.3.1. L2TP/PPTP **隧道设置**

界面进入方法: VPN >> L2TP/PPTP >> L2TP/PPTP 隧道设置

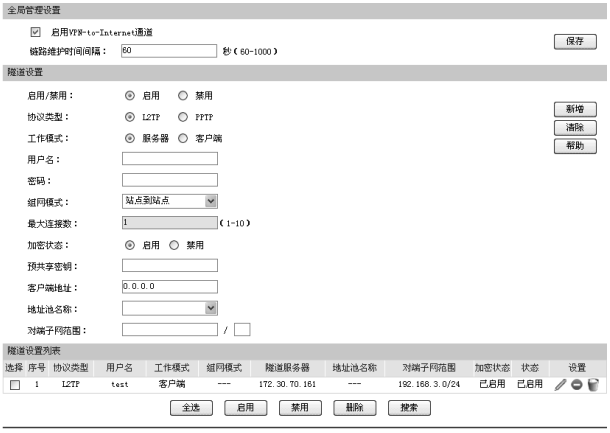


图 5-59 L2TP/PPTP 隧道设置界面

全局管理设置

勾选“启用 VPN-to-Internet 通道”，可以允许 VPN 拨号用户在访问 VPN 网络的同时访问互联网。

链路维护时间间隔	设置发送链路维护检测报文的时间间隔。

隧道设置

启用/禁用	选择启用或禁用当前 L2TP/PPTP 隧道条目。
协议类型	选择使用的隧道协议类型。
工作模式	选择当前路由器的工作模式。根据选择的工作模式不同，后续需要设置的参数也会不同。
用户名	设置 L2TP/PPTP 认证的用户名。客户端与服务器端的设置需一致。
密码	设置 L2TP/PPTP 认证的密码。客户端与服务器端的设置需一致。
组网模式	当连入隧道的用户为接入路由器的一个网段时，请选择“站点到站点”模式；当连入隧道的用户是单个计算机时，请选择“PC 到站点”模式。
最大连接数	当工作模式为“服务器”、组网模式选择“PC 到站点”时，可进行隧道容纳最大连接数的设置。
WAN 接口	当工作模式为“客户端”时，可以选择通过隧道传输报文的 WAN 接口。单 WAN 口路由器无此条目。
隧道服务器地址	当工作模式为“客户端”时，需设置隧道服务器地址。若服务器端为路由器则填入其 WAN 口 IP 地址。
加密状态	单纯的 L2TP/PPTP 隧道安全性仍然不高，可以选择是否对隧道进行加密。本路由将使用 IPsec 对 L2TP 隧道进行加密，使用 MPPE（Microsoft Point-to-Point Encryption，微软点对点加密术）对 PPTP 隧道进行加密。
预共享密钥	设置用于 L2TP 隧道加密的 IPsec 预共享密钥，隧道双方必须使用同一个预共享密钥。

客户端地址　　当协议类型为“L2TP”、工作模式为“服务器”且启用加密时，可以设置允许连接到本路由器的客户端 IP 地址。默认为 0.0.0.0，表示所有 IP 地址。

地址池名称　　当工作模式为“服务器”时，可以选择分配给客户端的静态 IP 地址范围。如果下拉菜单中没有想选择的条目，请进入**5.8.3.3隧道地址池管理**页面创建新条目。

对端子网范围　　输入隧道对端的地址，以子网掩码值划分地址范围。当工作模式为“服务器”、组网模式为“PC 到站点”时，该项无需填写。

隧道设置列表

在隧道设置列表中，可以对已保存的 L2TP/PPTP 隧道信息进行相应设置。

图 5-59序号 1 条目的含义：这条隧道使用 L2TP 协议进行封装，隧道用户名为 test，密码自设，路由器工作模式为“客户端”，隧道对端服务器地址为 172.30.70.161，对端子网为 192.168.3.0/24，目前该条目已生效。

5.8.3.2. L2TP/PPTP **隧道信息**

在此将列出路由器上所有 L2TP/PPTP 隧道的相关信息。

界面进入方法：VPN >> L2TP/PPTP >> L2TP/PPTP 隧道信息

图 5-60 L2TP/PPTP 隧道信息界面

图 5-60中显示的是图 5-59中隧道设置列表序列 1 条目的连接情况。目前这条隧道已成功建立，每条隧道会产生隧道 ID 数值对和会话 ID 数值对，每个数值对都由两个数字 ID 组成，客户端和服务器端显示的数值对是对应的。这条隧道在服务器端的连接信息如下图所示。

每次建立隧道连接时都会生成一组隧道 ID 和一组会话 ID，一般情况下，同一路由器上不同隧道的 ID 数值对不会相同，即使是同一条隧道，在断开已有连接后重新建立连接，也可能会产生不同的 ID 数值对。

5.8.3.3. 隧道地址池管理

界面进入方法：VPN >> L2TP/PPTP >> 隧道地址池管理

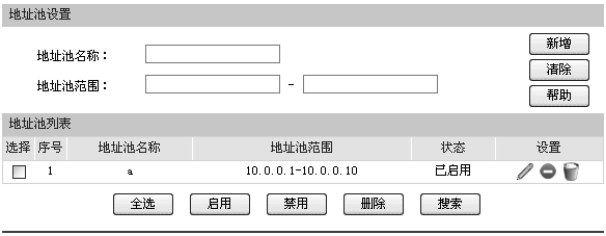


图 5-61 隧道地址池管理界面

地址池设置

地址池名称　为地址池命名。设置好的地址池名称可以被应用在隧道设置中。

地址池范围　设置分配给客户端的 IP 地址范围。此地址池不能与当前路由器 LAN 网段、对端路由器 LAN 网段及 DMZ 网段重复。

地址池列表

在地址池列表中，可以对已保存的地址池进行相应设置。

5.9. 系统服务

5.9.1.PPPoE 服务器

通过 PPPoE 服务器可以为局域网用户分配账号、IP 地址，简化用户的配置操作的同时也加强了路由器对局域网用户的管理功能。

5.9.1.1. 全局设置

可以在此开启 PPPoE 服务器功能，并对其全局参数进行设置。

界面进入方法：系统服务 >> PPPoE 服务器 >> 全局设置

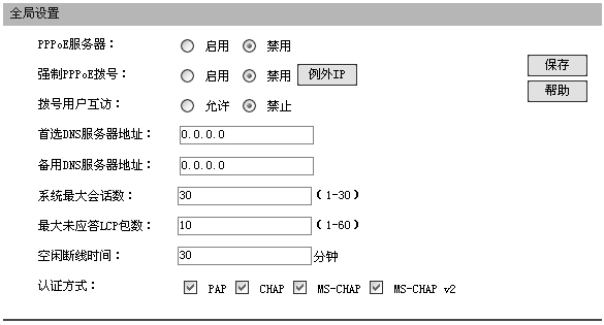


图 5-62 全局设置界面

全局设置

PPPoE 服务器　选择启用或禁用 PPPoE 服务器功能。

强制 PPPoE 拨号　选择是否强制局域网内所有用户通过 PPPoE 拨号连网。在启用模式下，如有特殊用户，可点击右侧<例外 IP>按钮进行设置。

拨号用户互访　选择是否允许通过 PPPoE 拨号连入的用户之间互相通信。

首选 DNS 服务器地址　设置分配给 PPPoE 用户的 DNS 地址，建议与 WAN 口的 DNS 地址一致。

备用 DNS 服务器地址　设置分配给 PPPoE 用户的备用 DNS 地址，建议与 WAN 口的备用 DNS 地址一致。

系统最大会话数　设置同一时间系统允许的 PPPoE 连接会话的最大值。

最大未应答 LCP 包数	LCP（Link Control Protocol，链路控制协议）用于检查 PPPoE 通信双方在数据传输过程中的一些必要信息。当客户端未应答 PPPoE 服务器发出的 LCP 包达到最大值后，将自动断开链接。该值可以留空，默认参数为 10。
空闲断线时间	设置在没有数据传输时的自动断线时间。时间范围为 0~10080 分钟，0 分钟表示永不断线，10080 分钟即 7 天。默认为 30 分钟。
认证方式	本路由器提供 4 种认证方法，请至少选择一项。PAP 协议在网络上明文传送用户名及密码，适用于网络安全需求较低的环境；CHAP 协议使用三次握手过程，而且不会明文传送密码，因此安全性能较高；MS-CHAP 协议是微软提出的认证方式，在密码加密的算法上与 CHAP 不同；MS-CHAP v2 协议是在 MS-CHAP 基础上的改进版本，安全性比 MS-CHAP 要高。

5.9.1.2. 地址池管理

界面进入方法：系统服务 >> PPPoE 服务器 >> 地址池管理

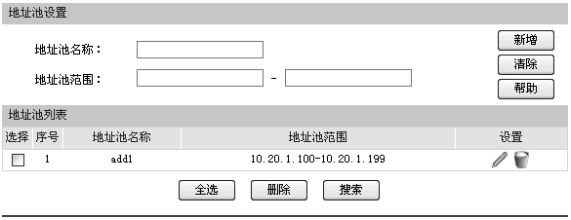


图 5-63 地址池管理设置界面

地址池设置

地址池名称	为地址池命名。设置好的地址池名称可以被应用在账号管理中。
地址池范围	设置分配给 PPPoE 拨号用户的 IP 地址范围。

地址池列表

在地址池列表中，可以对已保存的地址池进行相应设置。

5.9.1.3. 账号管理

可以在此对 PPPoE 拨号用户的账号进行设置。

界面进入方法：系统服务 >> PPPoE 服务器 >> 账号管理

图 5-64 账号管理设置界面

账号设置

账号	设置账号名称。该名称不能与 WAN 口设置中的 L2TP 或 PPTP 连接方式的账号名称重复。
密码	设置账号密码。
地址分配方式	选择该账号用户的 IP 地址分配方式。
地址池	选择“动态分配”方式时，请通过下拉菜单选择地址池。
静态 IP 地址	选择“静态分配”方式时，请在此输入将要分配给该账号的 IP 地址。

最大会话数	设置同一时间系统允许的单个账号连接会话的最大值，默认参数为 1。不同机型支持的会话数目会有所不同。
账号到期时间	设置该账号的到期时间，默认为 2099 年 1 月 1 日。
备注	添加对本账号条目的说明信息。
启用/禁用规则	设置该账号条目是否生效。
启用高级账号设置	勾选此项可对账号进行更多设置。
MAC 绑定方式	请在下拉菜单中选择 MAC 绑定方式。“不绑定”表示账号可以在任何一台主机上登录，“静态绑定”可以手动设置绑定该账号对应的 MAC 地址；“动态绑定”则由路由器记录账号首次登录时的 MAC 地址，并与账号绑定。开启 MAC 绑定后，最大会话数将强制变为 1。
MAC 地址	仅当选择“静态绑定”方式时，该项可编辑。当绑定了 MAC 地址后，该账号将只能在此 MAC 地址主机上登录。
定时断线设置	设置定时断线时间，如果为 0 表示永不断线。默认参数为 48 小时，若没有勾选“启用高级账号设置”，则默认为 0 小时。

账号列表

在账号列表中，可以对已保存的账号进行相应设置。

5.9.1.4. **例外** IP **管理**

在强制使用 PPPoE 拨号才能访问网络的时候，如果有个别主机不受限制，则可在此进行例外设置。

界面进入方法：系统服务 >> PPPoE 服务器 >> 例外 IP 管理

图 5-65 例外 IP 管理设置界面

例外 IP 设置

IP 地址范围　　设置不受 PPPoE 强制拨号限制的 IP 地址范围，可以是 IP 地址段也可以是单个 IP 地址。该地址范围必须在路由器 LAN 口网段中。

备注　　添加对本条目的说明信息。

启用/禁用规则　　设置本条目是否生效。

例外 IP 列表

在例外 IP 列表中，可以对已保存的条目进行相应设置。

5.9.1.5. 账号信息列表

界面进入方法：系统服务 >> PPPoE 服务器 >> 账号信息列表

图 5-66 账号信息列表界面

图 5-66中显示的是 PPPoE 用户账户相关连接信息。点击单个条目后方的“⛔”按钮可以断开当前账号的连接，如果需要断开所有已连接的账号，可以点击列表下方的<断开全部>按钮。

5.9.2.动态 DNS

5.9.2.1. 花生壳动态域名

广域网中，许多 ISP 使用 DHCP 分配公共 IP 地址，因此用户端获得的公网 IP 是不固定的。当其它用户需要访问此类 IP 动态变化的用户端时，很难实时获取它的最新 IP 地址。

DDNS（Dynamic DNS，动态域名解析服务）服务器则为此类用户端提供了一个固定的域名，并将其与用户端最新的 IP 地址进行关联。当服务运行时，DDNS 用户端把最新的 IP 地址通知 DDNS 服务器，服务器会更新 DNS 数据库中域名与 IP 的映射关系。而对于访问它的用户端，将会得到正确的 IP 地址并成功访问服务端。DDNS 常用于 Web 服务器搭建个人网站、FTP 服务器提供文件共享等，访问的用户可以便捷地获取服务。

路由器作为动态 DNS 客户端，本身并不提供动态 DNS 服务。因此，在使用此功能之前，必须进入动态 DNS 服务提供商的官方主页注册，以获得用户名、密码和域名等信息。本路由器提供花生壳动态 DNS 客户端。

界面进入方法：系统服务 >> 动态 DNS >> 花生壳动态域名

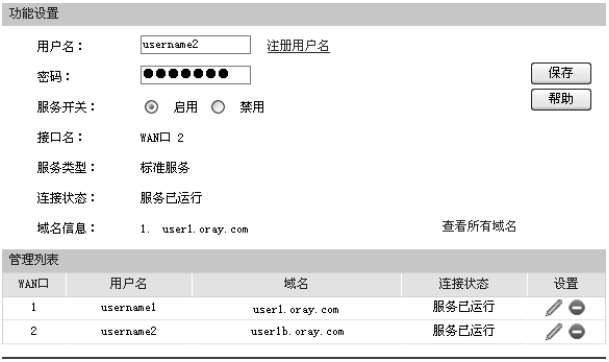


图 5-67 花生壳动态域名设置界面

功能设置

用户名	填入在花生壳网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录花生壳网站进行注册。
密码	填入在花生壳网站注册该用户名时所设置的密码。
服务开关	选择启用或禁用花生壳动态域名服务。
接口名	显示启用花生壳动态域名服务的 WAN 口。
服务类型	服务启用之后，显示当前登录的 DDNS 账号是属于专业服务还是标准服务。这取决于注册时选择的服务类型。
连接状态	显示 DDNS 的工作状态。 “服务没有运行”表示 DDNS 功能未启用; “服务连接中，请等候”表示系统正在连接 DDNS 服务器; “服务已运行”表示 DDNS 工作正常; “用户名或密码错误”表示输入的用户名或密码有误，请重新输入正确的值后再启用 DDNS。
域名信息	显示当前登录的 DDNS 用户所拥有的域名。用户可以申请多个域名，点击“查看所有域名”显示当前用户申请的所有域名，但最多显示 16 条。

管理列表

在管理列表中，可以对当前的 DDNS 条目进行相应设置。

图 5-67条目 1 的含义：应用于 WAN1 口的花生壳用户名是 uername1，对应的域名是 user1.oray.com，该服务已运行。

5.9.3.UPnP 服务

UPnP（Universal Plug and Play， 通用即插即用）协议，遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。

如果应用程序支持 UPnP 协议，而局域网中的主机安装了 UPnP 组件，路由器开启了 UPnP 服务后，局域网中的主机就可以根据软件的需要自动地在路由器上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于 NAT 的功能便可以正常使用。例如，Windows XP 和 Windows ME 系统上安装的 MSN Messenger，在使用音频和视频通话时就可以利用 UPnP 协议。

相对于转发规则而言，UPnP 的应用不需要用户手动设置任何规则，对于一些端口不固定的应用会更加方便。

界面进入方法：系统服务 >> UPnP 服务 >> UPnP 服务

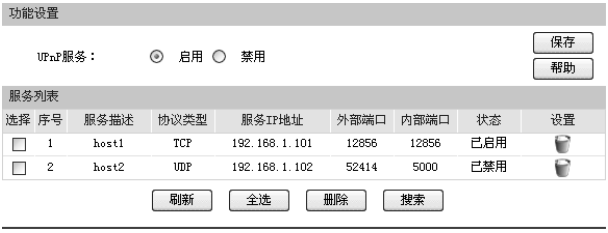


图 5-68 UPnP 服务设置界面

功能设置

UPnP 服务　　选择启用或禁用 UPnP 服务。

服务列表

启用 UPnP 后，所有应用到 UPnP 的连接规则会显示在服务列表中。

图 5-68序号 1 条目的含义：在路由器 WAN 口的 12856 端口接收到的 TCP 数据，将转发到局域网服务器 192.168.1.101 的 12856 端口上。

提示:

应用时不仅要在路由器上启用 UPnP 服务，还需要确认主机操作系统和应用程序也支持此服务，即 Windows XP 系统需安装 UPnP 组件；应用程序本身需支持 UPnP，如 MSN 最新版、电驴、迅雷等。

一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

5.10. 系统工具

5.10.1. 设备管理

5.10.1.1. 修改管理帐号

在此可以修改登录时使用的用户名和密码。

界面进入方法: 系统工具 >> 设备管理 >> 修改管理帐号

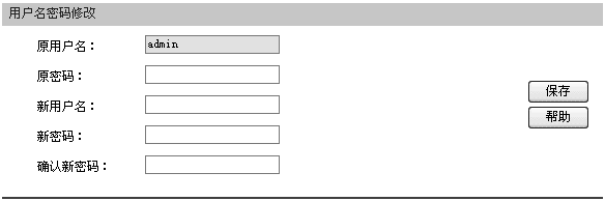


图 5-69 修改管理帐号界面

用户名密码修改

原用户名　　本次登录路由器的用户名。

原密码　　本次登录路由器使用的密码。

新用户名　　重新设置登录路由器的用户名。

新密码　　重新设置登录路由器的密码。

确认新密码　　再次输入新密码。

提示:

出厂的用户名/密码是 admin/admin。更改用户名及密码并保存生效后，后续登录时请使用新用户名及新密码。用户名和密码最多支持 31 个字符，且只能是数字和字母，区分大小写。

5.10.1.2. 远程管理

可以在远程管理界面对允许远程登录的 IP 地址范围进行设置和修改。

界面进入方法: 系统工具 >> 设备管理 >> 远程管理

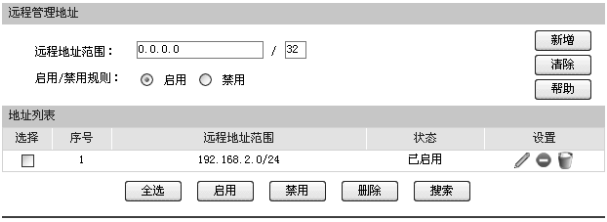


图 5-70 远程管理设置界面

远程管理地址

远程地址范围　　设置需要从外部网络登录路由器的主机地址，可指定单个 IP 或一个网段。

启用/禁用规则　　选择启用或禁用该规则。

地址列表

在地址列表中，可以对已保存的远程管理地址条目进行相应设置。

图 5-70序号 1 条目的含义：允许 IP 地址属于 192.168.2.0/24 网段的主机登录路由器 Web 界面，该规则已启用。

5.10.1.3. 系统管理设置

可以在服务端口界面对 Web、Telnet 服务的端口进行设置和修改。

界面进入方法：系统工具 >> 设备管理 >> 系统管理设置

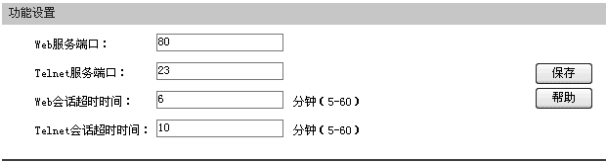


图 5-71 系统管理设置界面

功能设置

Web 服务端口　　设置路由器的 Web 服务端口。

Telnet 服务端口　　设置路由器的 Telnet 服务端口。

Web 会话超时时间　　设置通过 Web 页面访问路由器的超时时间。登录 Web 界面后，用户在该设定时间内如无任何操作，路由器将自动断开连接。

Telnet 会话超时时间　　设置通过 Telnet 远程访问路由器的超时时间，远程登录路由器后，用户在该设定时间内如无任何指令，路由器将自动断开连接。

提示:

路由器默认的 Web 服务端口为 80。如果改为其它值，在局域网或广域网都必须用“http://IP 地址:端口”的方式才能登录路由器。例如，将 Web 管理端口更改为 88，在局域网内登录时的 URL 地址应为 http://192.168.1.1:88。

设置超时时间后，新的超时时间将在下一次登录时生效。

举例:

某企业路由器地址为 210.10.10.50，为方便管理，希望广域网 210.10.10.0/24 网段的 IP 地址能对路由器进行远程管理。

可以通过设置 Web 服务器实现此需求。首先需要设置远端访问路由器的地址段，并选择启用该访问规则，如下图所示:

1. 在服务端口界面为 Web 服务器开放相应的服务端口，设置如下图所示:

2. 在浏览器地址栏输入路由器地址 210.10.10.50 登录路由器 Web 界面。

5.10.1.4. 恢复出厂配置

界面进入方法: 系统工具 >> 设备管理 >> 恢复出厂配置

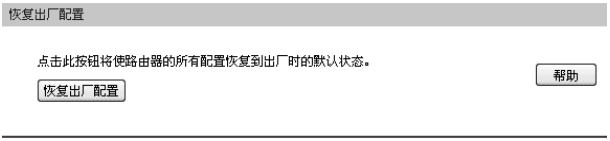


图 5-72 恢复出厂配置界面

点击<恢复出厂配置>按钮，路由器将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

路由器出厂默认 LAN 口 IP 地址为 192.168.1.1，用户名/密码为 admin/admin。

5.10.1.5. 备份与导入配置

界面进入方法：系统工具 >> 设备管理 >> 备份与导入配置

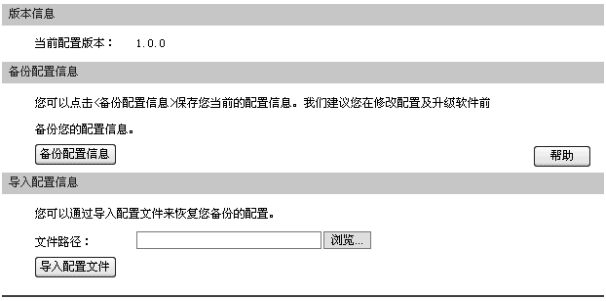


图 5-73 备份与导入配置界面

版本信息

显示当前路由器软件版本。

备份配置信息

单击<备份配置信息>按钮，路由器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

导入配置信息

单击<浏览>按钮，选择已备份的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后点击<导入配置文件>按钮，将路由器恢复到以前备份的配置状态。

注意:

备份及导入文件过程中请保持电源稳定，避免强行断电。

导入的配置文件版本与路由器当前配置版本差距过大，将有可能导致路由器现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

5.10.1.6. 重启路由器

界面进入方法：系统工具 >> 设备管理 >> 重启路由器

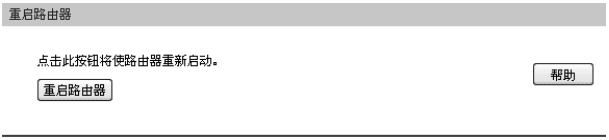


图 5-74 重启路由器界面

单击<重启路由器>按钮，路由器将会重新启动。

重新启动不会丢失已保存的配置，在重启的过程中，网络连接将会暂时中断。

注意:

路由器重启过程中请保证电源稳定，避免强行断电。

5.10.1.7. 软件升级

界面进入方法：系统工具 >> 设备管理 >> 软件升级

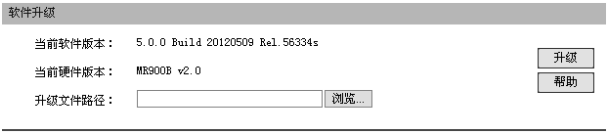


图 5-75 软件升级界面

MERCURY官方网站（http://www.mercurycom.com.cn）会不定期更新路由器的软件升级文件，可将升级文件下载保存在本地。登录路由器后进入软件升级界面，单击<浏览>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。

注意:

软件升级成功后路由器将会自动重启，在路由器重启完成前请保证电源稳定，避免强行断电。

软件升级后由于新旧版本软件的差异可能会恢复出厂默认配置，如有重要配置信息，请在升级前备份。

5.10.2. 流量统计

5.10.2.1. 接口流量统计

接口流量界面显示路由器所有正在工作的接口的数据接收/发送速率，以及 WAN 口的附加信息统计。

界面进入方法: 系统工具 >> 流量统计 >> 接口流量统计

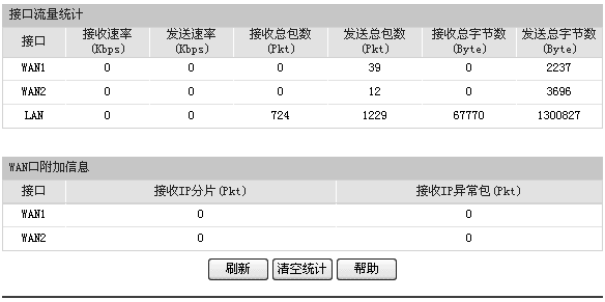


图 5-76 接口流量统计界面

接收/发送速率是以千比特每秒为单位进行统计的，通常所说的 1M 带宽即 1024Kbps。接收/发送总包数统计的是数据包的总个数。接收/发送总字节数统计的则是所有数据包的总字节数。

WAN 口附加信息则是以数据包为单位进行统计。其中，IP 分片是指接收到的大小超过 WAN 口允许接收的最大值，需要分片传输的数据包；IP 异常包是指 IP 封装字段非正常的数据包。

5.10.2.2. IP 流量统计

流量统计界面将显示接入路由器 LAN 口的局域网设备向广域网发出数据的流量统计。

界面进入方法：系统工具 >> 流量统计 >> IP 流量统计

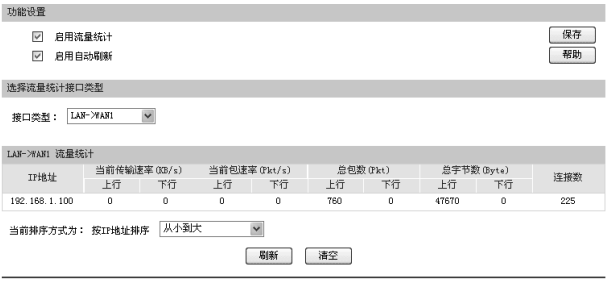


图 5-77 IP 流量统计界面

路由器默认勾选“启用流量统计”、“启用自动刷新”选项，启用自动刷新时，路由器每隔 10 秒刷新一次。在下拉菜单中选择流量统计接口类型后（MR900机型无此条目），相应的流量统计信息将显示在流量统计列表中。可以按照不同的表头对表格进行排序，默认排序方式为从小到大。

5.10.3. 诊断工具

5.10.3.1. 诊断工具

可在诊断工具界面通过 ping 命令或 tracert 命令来诊断当前路由器的网络连接状态。

界面进入方法：系统工具 >> 诊断工具 >> 诊断工具

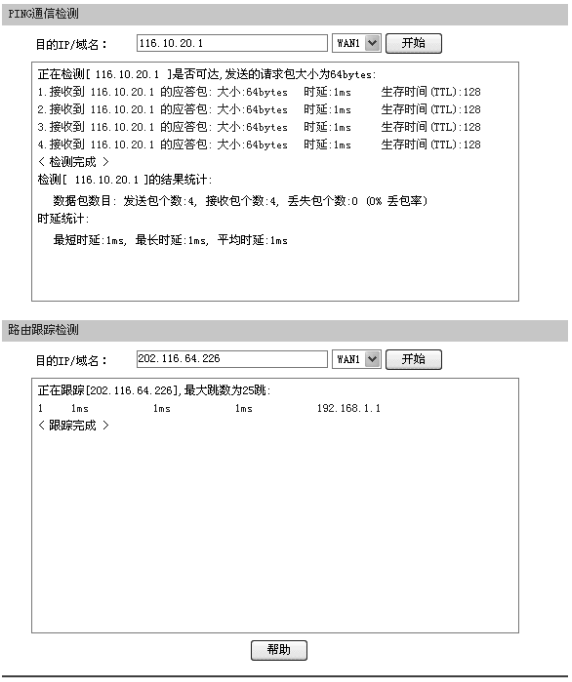


图 5-78 诊断工具界面

Ping 通信检测

目的 IP/域名　　输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 ping 包检测目的地址是否可以到达，并将检测结果显示在下面的方框中。

路由跟踪检测

目的 IP/域名　　输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 tracert 包检测经过哪些路由到达目的地址，并将检测结果显示在下面的方框中。

5.10.3.2. 在线检测

该页面用于检测 WAN 口是否在线。

界面进入方法: 系统工具 >> 诊断工具 >> 在线检测

图 5-79 在线检测界面

检测设置

接口名　　选择需要在线检测的 WAN 口。MR900无此条目。

检测开关　　选择开启或关闭在线检测。开启在线检测时，路由器将综合 PING 检测和 DNS 检测的结果判断是否在线；关闭在线检测时，路由器只根据 WAN 接口的物理连接状态和拨号状态判断是否在线。

检测模式　　选择自动在线检测或者手动在线检测。自动模式下，PING 检测选择网关作为目的地址，DNS 检测选择 WAN 口 DNS 服务器作为目的地址；手动模式下，可以自己设置 PING 检测和 DNS 检测的目的地址。

PING 检测　　在手动在线检测模式下，可以输入 PING 检测的目的 IP 地址。输入 0.0.0.0 表示不进行 PING 检测。

DNS 检测　　在手动在线检测模式下，可以输入 DNS 服务器的 IP 地址。输入 0.0.0.0 表示不进行 DNS 检测。

WAN 口状态列表

接口	显示所检测的 WAN 口。
检测	显示选择的检测开关，即启用或禁用。
WAN 口状态	显示 PING 检测或 DNS 检测的结果。

5.10.4. 时间设置

时间设置界面允许对路由器的系统时间进行设置。若时间设置发生改变，将会影响一些与其相关的功能，如防火墙规则的生效时间、PPPoE 定时拨号、日志等。

界面进入方法：系统工具 >> 时间设置 >> 时间设置

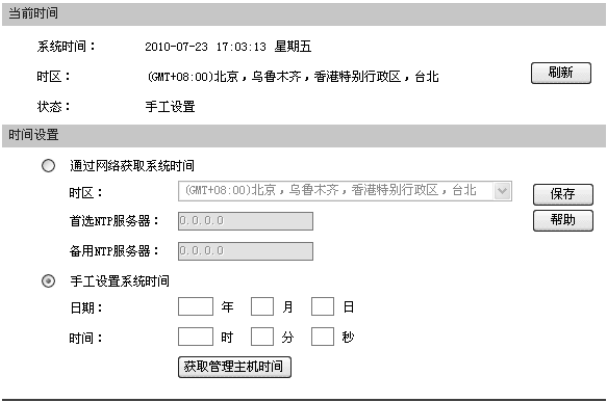


图 5-80 时间设置界面

当前时间

此处将显示目前系统时间及时间获取方式信息。如果想对时间进行更改，可以在下方时间设置区进行改动。

时间设置

通过网络获取系统时间　若路由器可以访问互联网，可选择此项进行网络校时。选择时区后点击<保存>按钮，路由器将在内置 NTP

（Network Time Protocol， 网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置 NTP 服务器地址，由于 NTP 服务器并非固定不变，推荐搜索两个不同的地址，分别填入首选、备用 NTP 服务器输入框，NTP 服务器地址可以为 IP 地址也可以为域名。设置完毕后点击<保存>按钮，路由器会通过指定的 NTP 服务器获取网络时间。

手工设置系统时间　　若路由器暂时不能访问互联网，可以选择对系统时间进行手动设置，或者点击<获取管理主机时间>按钮，系统将自动填入当前管理主机时间信息。设置完毕后点击<保存>生效。

提示:

如果不能正常使用<获取管理主机时间>功能，请在主机的防火墙软件中增加一条 UDP 端口为 123 的例外条目。

断电重启后，断电之前设置的时间将失效，重新变为“通过网络获取时间”，如果未能连网获取时间，默认将从 2010 年 2 月 10 日 0 时 0 分 0 秒开始计时。

5.10.5. 系统日志

可以在日志界面查看路由器系统事件的记录信息。

界面进入方法: 系统工具 >> 系统日志 >> 系统日志

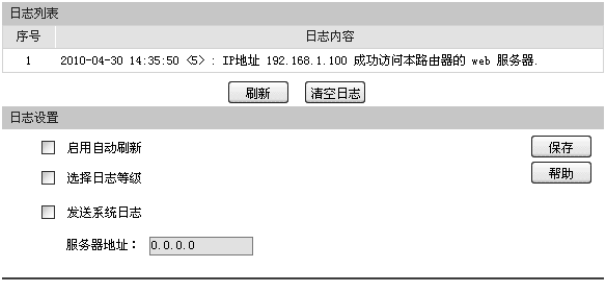
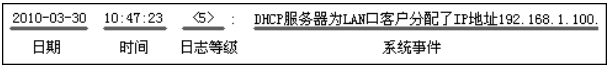
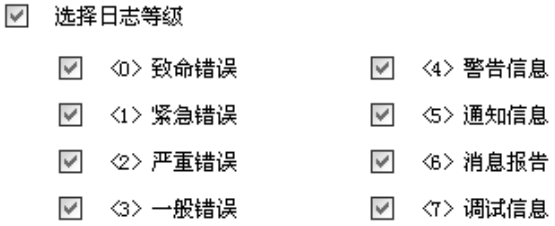


图 5-81 日志界面

日志列表中一条日志内容可分为四个部分:



日志配置部分可以对日志系统进行简单的配置。启用自动刷新后，日志列表将每隔 5 秒刷新一次；选择日志等级可使日志列表中仅列出指定等级的日志记录。



各等级描述:

<0> 致命错误　　导致系统不可用的错误，红色显示。

<1> 紧急错误　　必须对其采取紧急措施的错误，红色显示。

<2> 严重错误　　导致系统处于危险状态的错误，红色显示。

<3> 一般错误　　一般性的错误提示，橙色显示。

<4> 警告信息　　系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。

<5> 通知信息　　正常状态下的重要提示信息。

<6> 消息报告　　一般性的提示信息。

<7> 调试信息　　调试过程产生的信息。

若需要在某台主机上查看路由器日志信息，请首先在这台主机上安装日志服务器，然后勾选路由器日志页面上的“发送系统日志”选项，并输入这台主机的 IP 地址。保存设置后路由器将向指定地址发送系统日志。

附录 A FAQ

问题 1: 无法登录路由器 Web 管理界面该如何处理?

1. 如果第一次使用此路由器，请参考以下步骤:

   1) 确认网线已正常连接到了路由器的 LAN 口，对应的指示灯闪烁或者常亮。

   2) 访问设置界面前，建议将计算机设置成“自动获取 IP 地址”，由开启 DHCP 服务的路由器自动给计算机分配 IP 地址。如果需要给计算机指定静态 IP 地址，请将计算机的 IP 与路由器 LAN 口 IP 设置在一网段，路由器默认 LAN 口 IP 地址为：192.168.1.1，子网掩码：255.255.255.0，计算机的 IP 地址应设置为：192.168.1.X （X 为 2 至 254 之间任意整数），子网掩码为：255.255.255.0。

   3) 使用 ping 命令检测计算机与路由器之间的连通性。

   4) 若上述提示仍不能帮助您登录到路由器管理界面，请将路由器恢复为出厂配置。

2. 如果修改过路由器的管理端口，则注意下次登录时需要以“http://管理 IP:XX”的方式登录，XX 为修改后的端口号，如 **http://192.168.1.1:8080**。

3. 如果之前可以正常登录，现在不能登录，则有可能是他人修改了路由器的配置导致的（尤其在开启了远程 Web 管理的情况下），建议恢复出厂配置，修改路由器的管理端口、修改用户名和密码，做好保密措施。

4. 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了 ARP 欺骗，建议查找欺骗源、查杀病毒或将其隔离。

5. 请检查是否设置了 IE 代理，如果设置了 IE 代理，请先将代理取消。

问题 2: 忘记路由器用户名和密码怎么办？如何恢复出厂配置?

忘记用户名密码时可以将路由器通过 RESET 键恢复至出厂配置。需要注意的是:恢复出厂配置时路由器原有配置信息将丢失。

恢复出厂配置操作方法：通电状态下，长按 RESET 键，待系统指示灯闪烁 5 次后松开 RESET 键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址是 http://192.168.1.1，默认用户名和密码分别为 admin/admin。

问题 3：忘记路由器管理端口怎么办？

出于对路由器管理安全的考虑，在用户不知道路由器管理 IP 或者端口的情况下，需要对路由器进行管理，建议将路由器恢复出厂设置。

问题 4：为什么开启了远端管理后，非局域网段不能登录管理路由器？

1. 非局域网段要登录路由器的 IP 地址是否是被允许远端访问路由器的。

2. 路由器的管理端口是否已经修改过，如果修改过，则应以“http://WAN 口 IP:XX”的方式登录，XX 为修改后的管理端口，如 **http://202.160.58.67:8080**。

3. 路由器的管理端口是否已经在虚拟服务器中被映射为局域网主机的某个服务端口，如果已经被映射为主机的服务端口，则应更改主机服务的端口或更改路由器的管理端口为其它端口。

4. 路由器虚拟服务器的 NAT DMZ 服务是否启用，如需远程管理路由器，请禁用 NAT DMZ 服务。

问题 5：路由器某些功能设置需要填写子网掩码值划分地址范围，一般子网掩码都有哪些值？

子网掩码是一个 32 位的二进制地址，以此来区别网络地址和主机地址。子网划分时，子网掩码不同，所得到的子网不同，每个子网能容纳的主机数目不同。

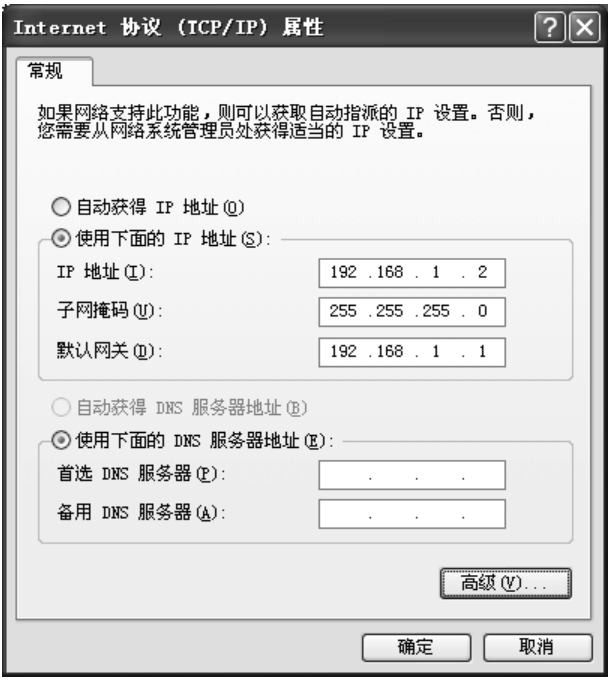
常用的子网掩码值有 8（即 A 类网络的缺省子网掩码 255.0.0.0）、16（即 B 类网络的缺省子网掩码 255.255.0.0）、24（即 C 类网络的缺省子网掩码 255.255.255.0）、32（即单个 IP 地址的缺省子网掩码 255.255.255.255）。

附录 B　TCP/IP 的详细设置

在这一节中将详细介绍 TCP/IP 的配置(本部分内容以 Windows XP 为例):

1. 打开“开始→控制面板”中的“网络连接”，右键点击“本地连接”图标，单击“属性”选项，出现如下图所示页面:

2. 双击“Internet 协议”（TCP/IP），出现如下图所示页面。如果您希望拥有固定的 IP 地址，请选择**使用下面的 IP 地址**和**使用下面的 DNS 服务器地址**，然后手动设置网络参数，其中 IP 地址为 192.168.1.2－192.168.1.254 范围内的任意值，参数设置可以参照下图设置:



3. 如果您希望自动从路由器获得 IP 地址，请选择自动获得 IP 地址和自动获得 DNS 服务器地址，点击确定后设置将生效。

附录 C　技术参数表格

MR900B 规格参数

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPsec
端口	LAN 口	1 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
	WAN 口	1 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
	WAN/LAN 口	3 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
网络介质		10Base-T：3 类或以上 UTP UTP/STP (≤100m)
		100Base-TX：5 类或以上 UTP/STP (≤100m)
LED 指示灯	LAN/WAN 口	LINK/ACT（连接/工作）
	其它	PWR（电源）、SYS（系统状态）
外形尺寸(L x W x H)		209mm×126mm×26mm
使用环境		工作温度：0°C~40°C
		存储温度：-40°C~70°C
		工作湿度：10%~90%RH 不凝结
		存储湿度：5%~90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.3A

MR900 规格参数

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPsec
端口	LAN 口	4 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
	WAN 口	1 个 10/100M 自适应 RJ45 端口（Auto MDI/MDIX）
网络介质		10Base-T：3 类或 3 类以上 UTP
		100Base-TX：5 类 UTP
LED 指示灯	LAN/WAN 口	LINK/ACT（连接/工作）
	其它	PWR（电源）、SYS（系统状态）
外形尺寸(L x W x H)		209mm×126mm×26mm
使用环境		工作温度：0º C~40º C
		存储温度：-40º C~70º C
		工作湿度：10%~90%RH 不凝结
		存储湿度：5%~90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.3A