



**艾泰科技**

UTT Technologies

# **HiPER 510W**

## **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

版权所有©2000-2010，上海艾泰科技有限公司，保留所有权利。

本档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

遵守所生效的版权法是用户的责任。在未经上海艾泰科技有限公司明确书面许可的情况下，不得对本档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

上海艾泰科技有限公司拥有本档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经上海艾泰科技有限公司明确书面许可的情况下，使用本档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰<sup>®</sup>、UTT<sup>®</sup>文字及相关图形是上海艾泰科技有限公司的注册商标。

HiPER<sup>®</sup>文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0904-0004-002

文档编号（DN）：PR-PMMU-1150.04-PPR-CN-1.1A

# 目 录

导 读 .....	1
0.1 手册说明 .....	1
0.2 界面风格 .....	1
0.3 基本约定 .....	1
0.3.1 符号约定 .....	2
0.3.2 其他表达约定 .....	2
0.3.3 常见按钮的功能 .....	2
0.3.4 列表功能详解 .....	3
0.4 出厂配置 .....	4
0.5 内容简介 .....	5
0.6 联系我们 .....	9
<b>第 1 章 产品概述 .....</b>	<b>10</b>
1.1 产品简介 .....	10
1.2 关键特性 .....	10
1.3 产品规格 .....	11
<b>第 2 章 硬件安装 .....</b>	<b>12</b>
2.1 产品外观 .....	12
2.1.1 前面板 .....	12
2.1.2 后面板 .....	13
2.2 安装步骤 .....	14
<b>第 3 章 快速配置 .....</b>	<b>16</b>
3.1 配置正确的网络设置 .....	16
3.2 登录设备 .....	17
3.3 配置向导 .....	19
3.3.1 配置向导首页 .....	19
3.3.2 配置模式——运行模式 .....	20
3.3.3 配置向导——网络参数 .....	20
3.3.4 配置向导——无线参数 .....	26
<b>第 4 章 开始菜单 .....</b>	<b>28</b>
4.1 配置向导 .....	28
4.2 运行状态 .....	28
4.3 接口流量 .....	30
4.4 重启设备 .....	31
<b>第 5 章 运行模式 .....</b>	<b>32</b>
<b>第 6 章 网络参数 .....</b>	<b>33</b>

6.1	WAN 口配置 .....	33
6.1.1	线路连接信息列表 .....	33
6.1.2	线路配置 .....	37
6.1.3	MAC 地址克隆 .....	40
6.2	LAN 口配置 .....	40
6.3	DHCP 服务器 .....	41
6.3.1	DHCP 服务器设置 .....	41
6.3.2	静态 DHCP .....	42
6.3.3	DHCP 客户列表 .....	44
6.3.4	DHCP 配置实例 .....	46
6.4	DDNS 配置 .....	47
6.4.1	申请 DDNS 帐号 .....	48
6.4.2	配置 DDNS 服务 .....	48
6.4.3	DDNS 验证 .....	50
6.5	UPnP .....	50
6.5.1	UPnP 配置 .....	50
6.5.2	UPnP NAT 映射列表 .....	51
<b>第 7 章</b>	<b>无线配置 .....</b>	<b>52</b>
7.1	基本设置 .....	52
7.1.1	AP Mode .....	52
7.1.2	APClient Mode .....	54
7.1.3	WDS .....	55
7.1.4	配置实例 .....	59
7.2	无线安全设置 .....	62
7.2.1	无线安全设置——无安全机制 .....	62
7.2.2	无线安全设置——WEP .....	63
7.2.3	无线安全设置——WPA/WPA2 .....	64
7.2.4	无线安全设置——WPA-PSK/WPA2-PSK .....	65
7.3	无线 MAC 地址过滤 .....	66
7.3.1	MAC 地址过滤全局配置 .....	66
7.3.2	MAC 地址过滤信息列表 .....	67
7.3.3	MAC 地址过滤配置 .....	67
7.3.4	自定义 MAC 地址过滤条目 .....	68
7.3.5	MAC 地址过滤配置实例 .....	68
7.4	无线高级配置 .....	69
7.4.1	无线高级参数 .....	69
7.5	无线主机状态 .....	71
<b>第 8 章</b>	<b>高级配置 .....</b>	<b>73</b>
8.1	NAT 和 DMZ 配置 .....	73
8.1.1	NAT 功能介绍 .....	73
8.1.2	NAT 静态映射 .....	74
8.1.3	NAT 规则 .....	78

8.1.4	DMZ .....	82
8.2	IP/MAC 绑定 .....	83
8.2.1	IP/MAC 绑定功能介绍 .....	83
8.2.2	IP/MAC 绑定全局配置 .....	84
8.2.3	IP/MAC 绑定信息列表 .....	84
8.2.4	IP 和 MAC 绑定配置 .....	85
8.2.5	自定义 IP/MAC 绑定条目 .....	86
8.2.6	配置上网“白名单”和“黑名单” .....	86
8.3	路由配置 .....	89
8.3.1	静态路由概述 .....	89
8.3.2	路由配置信息列表 .....	89
8.3.3	静态路由配置 .....	90
8.3.4	自定义静态路由 .....	91
<b>第 9 章</b>	<b>用户管理 .....</b>	<b>92</b>
9.1	全局管理 .....	92
9.1.1	全局管理配置 .....	92
9.1.2	全局管理配置实例 .....	93
9.2	组管理 .....	94
9.2.1	组管理信息列表 .....	95
9.2.2	组管理配置 .....	96
9.2.3	组管理配置匹配顺序 .....	98
9.2.4	全局管理、组管理和访问控制策略的匹配顺序 .....	98
9.2.5	组管理配置实例 .....	98
<b>第 10 章</b>	<b>防火墙 .....</b>	<b>103</b>
10.1	访问控制策略 .....	103
10.1.1	访问控制策略简介 .....	103
10.1.2	访问控制策略列表 .....	104
10.1.3	访问控制策略配置 .....	106
10.1.4	访问控制策略配置实例 .....	110
10.2	域名过滤 .....	115
10.2.1	域名过滤全局配置 .....	115
10.2.2	域名过滤配置 .....	115
<b>第 11 章</b>	<b>系统管理 .....</b>	<b>117</b>
11.1	管理员配置 .....	117
11.1.1	管理员配置信息列表 .....	117
11.1.2	创建管理员 .....	118
11.1.3	删除管理员 .....	118
11.2	语言选择 .....	119
11.3	时钟管理 .....	119
11.4	配置管理 .....	121
11.4.1	保存当前配置 .....	121

11.4.2	导入配置 .....	121
11.4.3	恢复出厂配置 .....	122
11.5	软件升级 .....	123
11.6	远程管理 .....	125
<b>第 12 章</b>	<b>系统状态 .....</b>	<b>126</b>
12.1	运行状态 .....	126
12.2	流量统计 .....	127
12.3	系统信息 .....	128
<b>第 13 章</b>	<b>客户服务 .....</b>	<b>130</b>
<b>附录 A</b>	<b>配置局域网中的计算机 .....</b>	<b>131</b>
<b>附录 B</b>	<b>FAQ .....</b>	<b>134</b>
1.	ADSL 用户如何上网? .....	134
2.	固定 IP 接入用户如何上网? .....	135
3.	动态 IP (CABLE MODEM) 接入用户如何上网? .....	135
4.	如何将设备恢复到出厂配置? .....	136
<b>附录 C</b>	<b>常用 IP 协议 .....</b>	<b>137</b>
<b>附录 D</b>	<b>常用服务端口 .....</b>	<b>138</b>
<b>附录 E</b>	<b>图索引 .....</b>	<b>142</b>
<b>附录 F</b>	<b>表索引 .....</b>	<b>145</b>

# 导 读

## 0.1 手册说明

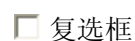
本手册指导您如何快速安装以及配置上海艾泰科技有限公司提供的 HiPER 510W 产品。如要了解更多产品和信息，请您访问艾泰科技官方网站 <http://www.utt.com.cn>。

## 0.2 界面风格

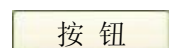
WEB 管理界面遵循浏览器的习惯用法，如下所示：



：选中代表只选用此项功能；



：选中代表此选项所述功能被选中；



：单击则执行该按钮的动作；



：输入相关参数；



：通过列表框可以找到供选择的选项；



：通过下拉框可以找到供选择的选项。

## 0.3 基本约定

0.3.1 符号约定


- ◆ 表示基本参数，描述参数基本涵义；
- ▶ 表示按钮，描述操作动作；
- ⊕ 表示提示，指出重点注意事项。

0.3.2 其他表达约定

0.3.2.1 进入某界面的表达方式

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，无线配置→无线MAC地址过滤表示在 WEB 界面中，首先单击一级菜单“无线配置”，之后再单击二级菜单“无线 MAC 地址过滤”，就进入无线 MAC 地址过滤界面了。

0.3.2.2 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。

0.3.3 常见按钮的功能







按钮	功能
	用于保存当前所做的配置
	用于恢复到修改前的配置参数
	用于删除选中的实例条目
	用于刷新当前页面相关状态信息
	用于清除当前页面相关统计信息
	用于返回上一个页面

表 0-1 常见按钮功能


### 0.3.4 列表功能详解

#### 0.3.4.1 列表基本功能

本产品 WEB 界面中的列表有可编辑列表和只读列表两种类型：

- 可编辑列表用来显示、编辑各种配置信息，能够添加、修改、删除列表条目；
- 只读列表用来显示系统状态信息，不可编辑。

下面将以可编辑列表“MAC 地址过滤信息列表”（如表 0-2）为例说明列表中各参数及按钮的含义。

 **提示：**需要注意的是，与添加、修改及删除操作相关的页面元素及功能，仅可编辑列表支持，只读列表是不支持的。

MAC地址过滤信息列表

2/50

1/1

第一页

上一页

下一页

最后页

前往

第

页

搜索

	ID	MAC地址	编辑
<input type="checkbox"/>	1	00:22:11:00:22:11	 
<input type="checkbox"/>	2	00:22:aa:00:11:bb	 

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 0-2 MAC 地址过滤信息列表

列表中各元素的功能如下表：

列表元素	功能
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 <input type="text"/> 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。

	<p>在搜索文本框中输入要查询的字符串，再敲&lt;Enter&gt;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&lt;Enter&gt;键。</p> <p>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。</p>
	当前已设置数目/最多可设置数目，此处指当前设置了 2 个 MAC 地址过滤条目，最多可设置 50 个条目。
	单击即可进入编辑页面，用于修改当前条目。
	单击即可删除当前条目。
 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。
	单击即可进入 MAC 地址过滤编辑页面，用于添加新条目。
	单击此按钮，即可删除表中所有条目。
	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。

表 0-3 列表基本功能

0.3.4.2 列表排序功能

本产品 WEB 界面的列表支持排序功能。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。

0.4 出厂配置

下表列出了本设备的一些重要参数的出厂设置值。

参数	出厂值	解释说明
管理员用户名	admin	用户使用该帐号登录到 WEB 管理界面，为安全起见，建议修改此值。 <b>注意：</b> 用户名和密码大小写敏感。
管理员密码	admin	
LAN 口的 IP 地址	192.168.1.1	设备的局域网接口地址，局域网用户可以通过该地址对设备进行维护。
LAN 口的子网掩码	255.255.255.0	
WAN 口的 IP 地址	192.168.2.1	设备的广域网接口地址。
WAN 口的子网掩码	255.255.255.0	
SSID	UTT-HiPER-ABCDEF	设备的 SSID 值，无线客户端必须使用相同的 SSID，才能连接到无线设备。其中 ABCDEF 为设备的序列号转换成 16 进制的数字。

表 0-4 设备出厂配置

## 0.5 内容简介

本手册主要介绍艾泰科技 HiPER 510W 无线路由器产品各功能的配置及应用，主要包括：产品概述、硬件安装、快速配置、开始菜单、网络参数、运行模式、无线配置、高级配置、用户管理、防火墙、系统管理、系统状态和客户服务等。

### 第 1 章 产品概述

主要介绍艾泰科技 HiPER 510W 的特点及功能特性。

### 第 2 章 硬件安装

主要介绍艾泰科技 HiPER 510W 产品的安装步骤及注意事项。

### 第 3 章 快速配置

主要介绍了以下几个部分的内容：

- 如何正确配置局域网计算机的网络属性参数；
- 如何登录设备，以及 WEB 页面布局介绍；
- 如何通过配置向导，快速配置设备正常工作所需的基本参数。

### 第 4 章 开始菜单

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：

- 配置向导——可以快速配置设备正常工作所需的基本参数；
- 运行状态——可以分别查看设备的有线和无线运行状态信息；
- 接口流量——可以分别查看设备各接口流量的图形化显示，并查看流量的相应统计值；
- 重启设备——可以进行重启设备的操作。

## 第 5 章 运行模式

主要介绍设备支持的工作模式及如何配置需要的工作模式。

## 第 6 章 网络参数

主要介绍了如何配置本设备的网络属性，包括：

- WAN 口配置——配置无线路由器的线路接入信息及 WAN 口相关参数；
- LAN 口配置——配置 LAN 口相关参数，包括 IP 地址、子网掩码和 MAC 地址等；
- DHCP 服务器——配置 DHCP 服务器、DNS 服务器及静态 DHCP，查看静态 DHCP 信息以及 DHCP 客户列表；
- DDNS 配置——申请、配置 DDNS 服务，查看 DDNS 状态信息；
- UPnP 配置——UPnP 的启用和禁用，查看 UPnP NAT 映射列表。

## 第 7 章 无线配置

主要介绍产品相关无线功能及参数的设置，包括：

- 基本设置——无线基本功能及设置方法；
- 无线安全设置——无线安全机制功能及其设置方法；
- 无线 MAC 地址过滤——无线 MAC 地址过滤功能及设置方法；
- 无线高级配置——无线高级功能及设置方法，设置无线高级参数；
- 无线主机状态——无线主机状态信息的查看及使用方法。

## 第 8 章 高级配置

主要介绍产品的高级功能配置，包括：

- 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；
- 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”；
- 路由配置——配置静态路由，预先指定对某一网络访问时所经过的路径。

## 第 9 章 用户管理

主要介绍产品的用户管理功能，包括：

- 全局管理——分时段允许/禁止内网用户使用 QQ、BT 等软件，对内网用户的行为进行限制和管理；
- 组管理——定义局域网用户工作组，可将具有类似性质的用户划分在同一个工作组，并对该组用户进行分时段的限速、P2P 软件管理控制。

## 第 10 章 防火墙

主要介绍产品的防火墙功能，包括：

- 访问控制策略——设备支持设置访问控制策略，通过配置来控制内网用户的上网访问权限和防御外网攻击；
- 域名过滤——禁止内网用户访问某些指定的域名。

## 第 11 章 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——修改 WEB 管理员的用户名和密码；
- 语言选择——选择设备页面的语言，该型号设备仅支持“简体中文”；
- 时钟管理——手工或自动设置系统时间和日期；
- 配置管理——备份系统当前配置，导入事先保存的配置，恢复设备出厂配置；
- 软件升级——备份当前软件版本，下载最新软件，升级软件；
- 远程管理——配置设备的远程管理功能，允许/禁止远程 HTTP 服务。

## 第 12 章 系统状态

主要介绍如何查看系统相关状态信息，包括：

- 运行状态——可以分别查看设备的有线和无线运行状态信息；
- 流量统计——可以分别查看设备的有线流量和无线流量的统计信息；
- 系统信息——可以查看系统的版本和时间信息，以及系统历史记录。

## 第 13 章 客户服务

主要介绍了本页面提供的快速链接功能：可以分别艾泰科技公司官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目，从而为用户提供了更快捷的获得专业服务的通道。

## 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。

## 0.6 联系我们

如果您在安装或使用过程中有任何疑问，请通过以下方式联系我们。

- 客服热线：4006-120-780、4006-880-780
- 艾泰讨论区：<http://www.utt.com.cn/bbs>
- E-mail 支持：[support@utt.com.cn](mailto:support@utt.com.cn)

# 第1章 产品概述

感谢您选用上海艾泰科技有限公司的 HiPER 510W 产品！

本章主要讲述艾泰科技 HiPER 510W 的功能和特点。

## 1.1 产品简介

HiPER 510W 是上海艾泰科技专为满足小型企业、远程分支机构等的无线上网需求而设计的无线路由产品，集 3G/有线/无线网络连接于一体，秉承了艾泰科技产品一贯的开放、易用、安全、流畅等特点。

HiPER 510W 符合 IEEE 802.11n 标准，同时兼容 IEEE 802.11b 和 IEEE 802.11g 标准，最高无线传输速率可达 150Mbps，提供大范围的无线覆盖和稳定的无线数据传输，多协议兼容更提高了 HiPER 510W 与其他产品的交互能力。

HiPER 510W 支持 WEP、WPA-Enterprise、WPA2-Enterprise、WPA-PSK、WPA2-PSK 多种无线安全机制，并提供简便快捷的无线 MAC 地址过滤功能，为无线主机数据传输的安全提供全面保护。

HiPER 510W 支持 DHCP 服务器、NAT、路由配置、DDNS、IP/MAC 绑定等多种高级配置功能。更为用户提供了丰富的用户管理功能，QQ/MSN/BT 等常用软件的管理配置功能，简单便捷的内网用户限速配置，更可全局或分组对内网用户进行配置。

HiPER 510W 提供灵活的访问控制策略配置、域名过滤等防火墙功能，为局域网用户提供了安全的保障，有效防止网络攻击。

HiPER 510W 提供简洁明了的中文 WEB 配置界面，直观易用、功能丰富。快速向导可帮助用户在短时间内完成基本的无线配置；系统运行状态、无线主机状态、流量统计等实用功能以及内置的“客户服务”界面，为用户提供了更快捷的获得专业服务的通道，帮助网络管理员快速定位和排除网络故障。

## 1.2 关键特性

- 提供静态 IP、动态 IP、PPPoE、3G 四种接入模式
- 提供 10M/100M LAN 口（4 个内置的交换式以太网口）和 1 个 WAN 口
- 整机满足 6KV 防雷特性
- 符合 IEEE 802.11n 标准，兼容 IEEE 802.11b 和 IEEE 802.11g 标准，提供最高 150Mbps

的无线传输速率

- 支持无线安全机制控制, 提供 WEP、WPA-Enterprise、WPA2-Enterprise、WPA-PSK、WPA2-PSK 等多种无线安全机制
- 支持 SSID 隐藏
- 支持多协议 VPN 穿透
- 支持 WMM (Wi-Fi Multimedia, 无线多媒体) 功能
- 支持无线 MAC 地址过滤功能, 可配置白名单、黑名单, 并提供简便的一键过滤无线 MAC 地址功能
- 支持 DHCP 服务器和 DNS 代理
- 支持 DDNS
- 支持 IP/MAC 绑定
- 支持对内网用户进行上行/下行速率限制
- 支持对内网用户进行上网行为管理, 包括禁止 QQ/MSN/BT 下载/迅雷搜索
- 支持防火墙功能
- 支持地址、协议和端口的包过滤
- 支持 URL、关键字过滤
- 支持 DNS 请求过滤
- 支持 HTTP 远程管理
- 中文 WEB 配置界面, 简易快速向导
- 支持 WEB 升级方式, 方便功能扩展
- 支持配置文件备份和导入
- 提供无线主机状态和系统状态的查看

## 1.3 产品规格

- 符合 IEEE 802.11n、IEEE 802.11b 以及 IEEE 802.11g 标准
- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由等协议。
- 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

### 2.1 产品外观

#### 2.1.1 前面板

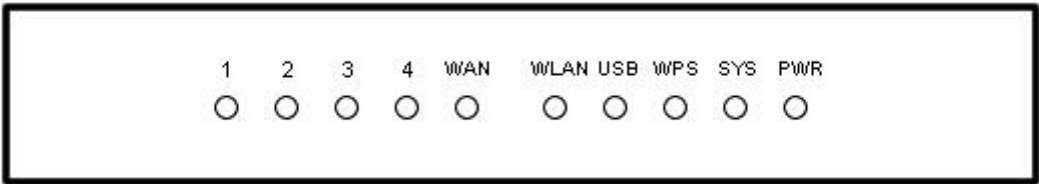


图 2-1 前面板

前面板上的指示灯用于指示设备及接口的工作状态，各指示灯的状态及作用如下表。

指示灯	描述	状态	含义
POWER	电源指示灯	亮	设备正常上电
		灭	设备未上电
SYS	系统指示灯	闪烁	系统工作正常
		亮	系统工作不正常
		灭	系统工作不正常
USB	3G 上网卡状态指示灯	亮	插入 3G 卡后亮
		灭	未插入 3G 卡或 USB 口工作不正常
WLAN	无线状态指示灯	亮	已启用无线功能
		闪烁	正在发送/接收无线数据
		灭	未启用无线功能
WAN	广域网口指示灯	亮	广域网口工作正常
		闪烁	接口有数据通过
		灭	广域网口工作不正常或未使用

LAN	局域网口指示灯	亮	接口工作正常
		闪烁	接口有数据通过
		灭	接口工作不正常或相应接口未使用
备注:	WPS 功能此软件版本暂不支持，故对应状态指示灯也未使用。		

表 2-1 前面板指示灯说明

2.1.2 后面板

1. 后面板示意图

HiPER 510W 后面板由电源、Reset 按钮、USB 卡接口、物理端口、WPS 和天线组成，如图 2-2 所示，其中 WPS 功能此软件版本暂无支持，在此不再赘述，下同。

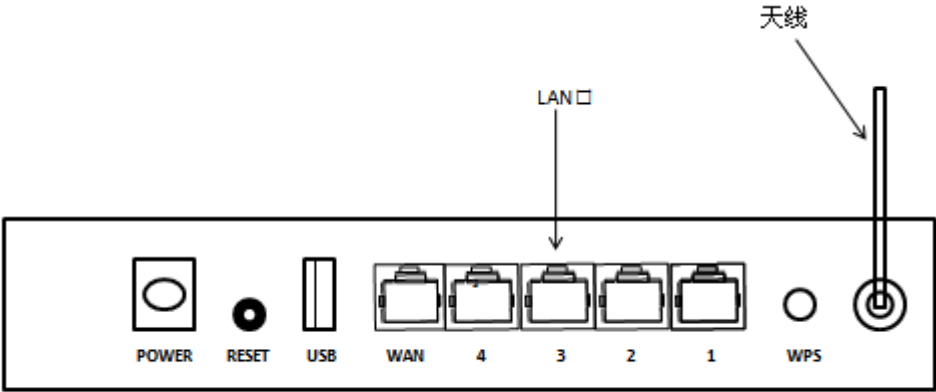


图 2-2 后面板示意图

2. Reset 按钮

Reset 按钮指复位按钮，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，设备将恢复到出厂配置，并自动重启。忘记管理员口令时，可以通过 Reset 按钮来恢复设备的出厂配置。

**提示：**上述操作会删除用户所有自定义的配置，并将系统恢复到出厂状态。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。

### 3. 接口说明

本设备提供四个 LAN 端口、一个 WAN 口和一个 USB 卡接口，相关涵义及作用如下表：

端口	描述	说明
LAN	局域网端口	LAN 口可用于连接局域网中的计算机、交换机和集线器等。
WAN	广域网端口	HiPER 510W 提供 1 个广域网端口，可用于连接到 Internet。
USB	3G 上网卡接口	提供一个 3G 上网卡接口，可用于连接到 Internet。

表 2-2 后面板端口说明

### 4. 部件说明


部件	数量	用途
天线	1	3G 天线上网卡接口，天线用于连接无线客户端、接收/发送无线数据。
电源	1	用来连接电源，为本设备供电。

表 2-3 后面板主要部件用途

## 2.2 安装步骤

### 1. 选择安装地点


选择一个适当的地方安装 HiPER 510W，确保其电源是关闭的，一般是将 HiPER 510W 放置在干净的工作台上。

 **提示：**请保证工作台的平稳性和良好接地，同时不要在设备上面放置重物。

### 2. 安装天线

取出包装盒中的天线，分别将其接入后面板的天线接口，接入方式如下所示：

- 天线的接口对准设备的 ANT 接口；
- 顺时针旋转天线，直至无法旋转；

 **提示：** 请保证设备天线的安装完成，未连接天线的设备其无线信号传输能力将大大降低。

### 3. 建立 HiPER 510W 与局域网的连接


使用标准的网线连接管理计算机到 HiPER 510W 的局域网（LAN）口，或者是连接交换机到 HiPER 510W 的 LAN 口，或通过无线与设备连接。HiPER 510W 将会自动适应 10M 或者 100M 的设备。

### 4. 建立与广域网的连接

使用 Cable/DSL Modem 厂商提供的网线将 Cable/DSL Modem 连接到 HiPER 510W 的广域网口或将 3G 上网卡插进设备 USB 接口。

### 5. 接通电源

将随机配置的电源线连接到 HiPER 510W 后面板的电源接口。

 **提示：** 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。

### 6. 检查系统指示灯

对照《章节 2.1.1 前面板》中的“前面板指示灯说明”（表 2-1）检查系统指示灯，查看 HiPER 510W 的连接及工作状态是否正常。

## 第3章 快速配置

本章主要介绍如何为管理计算机配置正确的网络设置，如何登录设备，以及如何通过**开始→配置向导**快速地配置路由器正常工作所需要的基本参数，并简要介绍了 WEB 页面的布局 and 风格。

### 3.1 配置正确的网络设置

在通过 WEB 界面登录到设备之前，首先要对管理计算机进行正确的网络设置。

1. 首先将计算机连接到设备的某个局域网端口。
2. 接下来设置计算机的 IP 地址。
  - 1) 第一步，设置计算机的 TCP/IP 协议，如果已经正确设置完成，请跳过此步。
  - 2) 第二步，设置计算机的 IP 地址为 192.168.1.2-192.168.1.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.1.1（本路由器设备 LAN 口的缺省 IP 地址），DNS 服务器为当地运营商提供的地址。
  - 3) 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 192.168.1.1。**

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 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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

如果屏幕显示如下，表示计算机和设备连接失败。

```
Pinging 192.168.1.1 with 32 bytes of data:  
  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.168.1.1:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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 192.168.1.1，那么计算机的 IP 地址必须为 192.168.1.2-192.168.1.254 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 登录设备

本节讲述如何登录设备。

计算机使用 MS Windows、Macintosh、Unix 或者是 Linux 等任何操作系统，都可以通过浏览器（例如，Internet Explorer）登录设备，并对设备进行配置。

打开浏览器，在浏览器的地址栏里输入设备的 IP 地址（出厂设置值为 192.168.1.1），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。您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（用户名和密码的出厂设置均“admin”），然后单击“确定”按钮。



图 3-1 WEB 登录页面

如果用户名和密码正确，浏览器将显示管理员模式的首页（如图 3-2 所示）：



图 3-2 WEB 首页

1. 该页面右侧为主操作页面，在主操作页面，您可以配置各个功能、查看配置信息、状态信息和统计信息等等。
2. 该页面右上角显示系统型号，版本信息，以及 3 个快速链接图标。这 3 个快捷图标的作用如下：

- 1) **产品讨论**——链接到艾泰科技官方网站的讨论区，参与产品的讨论；
  - 2) **知识库**——链接到艾泰科技官方网站的知识库，查找相关技术资料；
  - 3) **预约服务**——链接到艾泰科技官方网站预约服务页面，提前预约某一个工作时段의客户服务
3. 该页面左侧显示主菜单条（导航条），它包括一级菜单和二级菜单。单击某个一级菜单，该一级菜单所包含的二级菜单相应展开，再单击，展开的二级菜单会收缩起来。
  4. 如果您是第一次登录设备，那么主操作页面将直接链接到配置向导首页。在下一节我们将讲述如何通过**开始**→**配置向导**页面来快速配置一些设备正常工作所需的基本参数。

## 3.3 配置向导

本节讲述**开始**→**配置向导**页面的配置。

### 3.3.1 配置向导首页

如前所述，如果您是第一次登录设备，那么登录成功后，主操作页面将直接弹出配置向导首页。如下图所示：

用这个向导，您可以设置上网所需的基本网络参数。即使您对网络知识和这个产品不太熟悉，您也可以按照提示轻松地完成设置。如果您是一位专家，您也可以退出这个向导程序，直接到菜单项中选择您需要修改的设置项进行设置。

要继续，请单击“下一步”。

要退出配置向导，请单击“退出向导”。

☐ 下次登录不再自动弹出向导

退出向导    下一步

图 3-3 配置向导——首页

- ◆ 下次登录不再自动弹出向导：若选中此项，则表示下次登录设备后将不再弹出本配置向导页面，系统将直接进入欢迎页面，如图 3-4 所示；若未选中此项，则表示下次登录设备仍将弹出本页面。
- ▶ 退出向导：单击“退出向导”按钮后，系统将离开配置向导页面，并进入欢迎页面（如图 3-4 所示），配置向导所有操作无效；
- ▶ 下一步：单击“下一步”按钮，将进入配置向导第二页，即**配置向导**→运行模式页面，如图 3-5 所示。



图 3-4 欢迎页面

### 3.3.2 配置模式——运行模式

在本页面中，可选择设备工作在不同的运行模式，如下图所示：

设备运行模式选择：

- ☒ 有线网关模式
- ☐ 3G客户端模式
- ☐ 无线客户端模式

图 3-5 运行模式

- ◆ 有线网关模式：是指设备采用有线的方式为用户提供远程接入并作为网络的网关使用；
- ◆ 3G 客户端模式：是指设备作为客户端并采用 3G 的方式为用户提供远程接入；
- ◆ 无线客户端模式：是指设备作为客户端并采用无线的方式为用户提供接入；
- ▶ 上一步：返回上一个配置页面；
- ▶ 重填：重新选择填写设备运行模式；
- ▶ 离开：离开本配置页面；
- ▶ 下一步：进入下一个配置页面。

### 3.3.3 配置向导——网络参数

在本页面，您可以为设备配置基本的网络参数，但在**配置向导—>运行模式**中选择不同的运行模式，会使得本处网络参数的设置不一样。

### 3.3.3.1 网络参数——有线网关

选择有线网关模式后，配置网络参数有三种可供选择上网方式，包括固定 IP 接入，动态 IP 接入，PPPOE 接入。

#### 3.3.3.1.1 固定 IP 接入

本页面配置设备的上网方式，请您根据自身情况进行选择。

接入方式	固定IP接入 ▼
IP地址*	200.200.202.140
子网掩码*	255.255.255.0
网关地址*	200.200.202.254
主DNS服务器*	210.22.70.3
备DNS服务器	

上一步 重填 离开 下一步

图 3-6 网络配置——固定 IP 接入

- ◆ 接入方式：此处选择固定 IP 接入，此时，需要通过手工输入静态 IP 地址、子网掩码以及网关地址；
- ◆ IP 地址：设备使用的 WAN 口 IP 地址；
- ◆ 子网掩码：设备 WAN 口所使用的 IP 地址，必须和网关处于同一子网；
- ◆ 网关地址：设备的网关地址，网关地址必须与设备 IP 地址处于同一个子网中；
- ◆ 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：单击“上一步”按钮，将返回配置向导首页，如图 3-3 所示；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 离开：单击“离开”按钮后，系统将离开配置向导页面，并进入欢迎页面（如图 3-4 所示），配置向导所有操作无效；
- ▶ 下一步：单击“下一步”按钮，将进入配置向导第三页，即**无线参数**页面，如图 3-13 所示。

#### ⊕ 提示：

1. 如果改变了设备的“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；
2. 所有带有符号“\*”的选框为必填项，后面不再一一复述。

#### 3.3.3.1.2 动态 IP 接入

本页面配置设备的上网方式，请您根据自身情况进行选择。

图 3-7 网络配置——动态 IP 接入

- ◆ 接入方式：此处选择动态 IP 接入，设备将通过 DHCP 动态获取 IP 地址、子网掩码以及网关地址信息，此时，无需设置这几个参数；
- ▶ 上一步：返回到上一个配置；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 离开：单击“离开”按钮后，系统将离开配置向导页面，并进入欢迎页面，配置向导所有操作无效；
- ▶ 下一步：单击“下一步”按钮，进入下一个配置页面。

⊕ 提示：

如果设备通过 DHCP 获取了新的“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。

### 3.3.3.1.3 PPPoE 接入

本页面配置设备的上网方式，请您根据自身情况进行选择。

图 3-8 网络配置——PPPOE 接入

- ◆ 接入方式：此处选择 PPPoE 接入，ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号），设备将通过拨号获取 IP 地址、子网掩码以及网关地址信息；
- ◆ 用户名：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号（如有疑问，请询问 ISP）；
- ◆ 密码：申请 PPPoE 业务的时候，ISP（例如中国电信）将提供上网账号所对应的密码（如有疑问，请询问 ISP）；
- ▶ 上一步：单击“上一步”按钮，将返回配置向导首页，如图 3-3 所示；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 离开：单击“离开”按钮后，系统将离开配置向导页面，并进入欢迎页面（如图 3-4 所示），配置向导所有操作无效；

▶ 下一步：单击“下一步”按钮，将进入配置向导第三页，即**无线参数**页面，如图 3-13 所示。

### 3.3.3.2 网络参数——3G 客户端

本页面配置设备的上网方式，请您根据自身情况进行选择。

3G卡类型	HUAWEI E169
运营商	中国移动
认证方法	SIM认证
PIN码	
接入点名	CMNET
拨号	*99***1#
高级PPP配置：	
用户名	CMNET
密码	●●●●●●

上一步 重填 离开 下一步

图 3-9 网络参数——3G 客户端

- ◆ 3G 卡类型：设备目前支持的 3G 卡类型有 HUAWEI E169、HUEWEI E1750、HUAWEI EC1260、HUAWEI ET128；
- ◆ 运行商：提供网络远程接入的服务商，包括中国移动、中国联通、中国电信；
- ◆ 认证方法：采用 3G 方式接入网络时和运营商端采用的认证，共提供 SIM 认证和密码认证两个选项；
- ◆ PIN 码：3G 上网卡的个人身份识别码；
- ◆ 接入点名：运营商用来提供接入的接入点的名称；
- ◆ 拨号：用来连接运营商基站时发出的拨号指令的内容之一；
- ◆ 用户名：PPP 认证的用户名；
- ◆ 密码：PPP 认证的密码；
- ▶ 上一步：返回上一个配置页面；
- ▶ 重填：重新填写 3G 网络接入参数；
- ▶ 离开：离开本配置页面；
- ▶ 下一步：进入下一个配置页面。

⊕ 提示：

配置设备采用“3G 客户端模式”上网时，建议用户只配置 3G 卡类型、运营商两个选项，其余参数保持默认；若需改变，请在专业人士指导下完成。

3.3.3.3 网络参数——无线客户端

配置无线客户端的网络参数时，“安全模式”选择不同选项配置内容时不同的。

3.3.3.3.1 安全模式—无安全机制

本页面配置设备的上网方式，请您根据自身情况进行选择。

AP的SSID

AP的MAC地址\*

安全模式

无安全机制

上一步

重填

离开

下一步

图 3-10 安全模式—无安全机制

- ◆ AP 的 SSID：对端设备的 SSID，大小写敏感；
- ◆ AP 的 MAC 地址：为本设备提供无线接入的 AP 的 MAC 地址；
- ◆ 安全模式： 此处选择无安全机制；
- ▶ 上一步：返回上一个配置页面；
- ▶ 重填：重新填写当前配置参数；
- ▶ 离开：离开本配置页面；
- ▶ 下一步：进入下一个配置页面。

3.3.3.3.2 安全模式—WEP

本页面配置设备的上网方式，请您根据自身情况进行选择。

AP的SSID

UTT-HIPER

AP的MAC地址\*

00:22:aa:11:22:33

安全模式

WEP

认证类型

共享密钥

密钥格式

16进制

密钥选择

WEP密钥

密钥类型

密钥1: ☒

64位

密钥2: ☐

禁用

密钥3: ☐

128位

密钥4: ☐

禁用

上一步

重填

离开

下一步

图 3-11 安全模式—WEP

- ◆ AP 的 SSID：对端设备的 SSID，大小写敏感；
- ◆ AP 的 MAC 地址：无线接入服务器的 MAC 地址；
- ◆ 安全机制：此处选择“WEP”，表示本设备将使用 802.11 协议提供的最基本的 WEP 安全机制；
- ◆ 认证类型：使用 WEP 加密机制时，开放系统、共享密钥 2 个选项。
  - 开放系统：此时，无线客户端主机在不提供认证密钥的前提下，通过认证并关联到无线路由器；但若要进行数据传输，必须提供正确的密钥；
  - 共享密钥：此时，无线客户端主机必须提供正确的密钥才能通过认证，否则无法关联到路由器，从而无法进行数据传输。
- ◆ 密钥格式：提供 16 进制、ASCII 码两种格式。
  - 采用 16 进制时，密钥字符可以为 0~9，A、B、C、D、E、F；
  - 采用 ASCII 码时，密钥字符可以是所有的 ASCII 码。
- ◆ 密钥选择：用户可根据需要输入 1~4 个密钥，这 4 个密钥可以采用不同的密钥类型。
- ◆ WEP 密钥：用于设置密钥值，密钥的长度受密钥类型的影响。
  - 选择 64 位密钥时，输入 16 进制字符 10 个或者 ASCII 码字符 5 个；
  - 选择 128 位密钥时，输入 16 进制字符 26 个或者 ASCII 码字符 13 个。
- ◆ 密钥类型：用于选择密钥类型，提供禁用、64 位、128 位，共 3 个选项。其中，禁用表示不使用当前密钥；而 64 位、128 位、则用于指定 WEP 密钥的长度；
- ▶ 上一步：返回上一个配置页面；
- ▶ 重填：重新填写当前配置参数；
- ▶ 离开：离开本配置页面；
- ▶ 下一步：进入下一个配置页面。

### 3.3.3.3.3 安全模式—WPA-PSK/WAP2-PSK

AP的SSID	UTT-HIPER
AP的MAC地址*	00:22:aa:11:22:33
安全模式	WPA-PSK/WPA2-PSK ▼
WPA版本	WPA2-PSK ▼
加密算法	AES ▼
预共享密钥*	<input type="text"/> (取值范围：8-63个字符)

图 3-12 安全模式——WPA-PSK/WAP2-PSK

- ◆ AP 的 SSID：对端设备的 SSID，最大长度为 32 个字符，大小写敏感；
- ◆ AP 的 MAC 地址：对端设备的 MAC 地址；

- ◆ 安全机制：此处选择“WPA-PSK /WPA2-PSK”，表示本设备将采用 WPA-PSK 或 WPA2-PSK 安全机制。此安全机制下，本设备将采用基于预共享密钥的 WPA 模式。
- ◆ WPA 版本：用来设置本设备将使用的安全模式。
  - WPA：表示本设备将采用 WPA-PSK 的安全模式；
  - WPA2：表示本设备将采用 WPA2-PSK 的安全模式。
- ◆ 加密算法：用来选择对无线数据进行加密的安全算法，选项有 TKIP、AES。
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法。
- ◆ 预共享密钥：预先设置的初始化密钥，取值为 8~63 个字符。
- ▶ 保存：无线安全设置参数生效；
- ▶ 重填：恢复到修改前的无线安全设置参数。

### 3.3.4 配置向导——无线参数

在本页面，您可以为设备配置基本的无线参数。

本页面用于设置设备的无线基本参数。

SSID *	<input type="text" value="UTT-HiPER-89CA35"/>
无线模式	<input type="text" value="11b/g/n混合"/>
信道	<input type="text" value="6"/>
频道带宽	<input type="text" value="20M/40M"/>
<div><input type="button" value="上一步"/> <input type="button" value="重填"/> <input type="button" value="离开"/> <input type="button" value="完成"/></div>	

图 3-13 配置向导——无线参数

- ◆ SSID：SSID（Service Set Identification，服务集标识）用于唯一地标识一个无线网络，其最大长度为 32 个字符，大小写敏感。
- ◆ 无线模式：此参数用于设置无线路由器的模式，提供仅 11g，仅 11n 和 11b/g/n 混合三个选项。
  - 仅 11g：即纯 802.11g 模式，本模式下，最大速率 54M bps。兼容 IEEE 802.11g 标准的无线站点可以接入路由器。
  - 仅 11n：即纯 802.11n 模式，本模式下，最大速率为 150M bps。只有符合 IEEE 802.11n 标准的无线站点可以接入路由器。
  - 11b/g/n 混合：符合 IEEE 802.11b、802.11g 或者 802.11n 标准的无线站点将各自

按照自己的模式接入，最大速率分别为 11M bps、54M bps 和 150M bps。

◆ 信道：此参数用于选择无线网络工作的频率段，可以选择的范围从 1 到 11，另外提供自动选项，表示路由器可以自动选择最优频率段。如果存在多个无线设备时，要注意各个设备的频段设置不能相互影响。

◆ 频道带宽：设置无线数据传输时所占用的频道带宽，可选项为：20M/40M 和 20M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用；对于以 802.11b 或者 802.11g 标准的无线站点来说，只能使用 20M 的频道带宽。

- 20M/40M：选择 20M/40M 时，表示使用 802.11n 接入的无线站点将根据很接入对端协商的结果选择使用 20M 或 40M 的频道带宽。

- 20M：选择 20M 时，表示使用 802.11n 接入的无线站点将使用 20M 的频道带宽。

▶ 上一步：返回到上一个配置页面；

▶ 重填：恢复到修改前的配置参数；

▶ 离开：放弃配置操作并离开当前配置页面；

▶ 完成：单击“完成”按钮后，保存在配置向导几个页面中所做的设置。

#### ⊕ 提示：

- 1、配置向导所做的操作，只有单击“完成”按钮才能保存（包括配置向导的前几步配置操作）。
- 2、如果**配置向导**→**运行模式**选择 3G 客户端模式，那么图 3-13 的页面上出现提示：选择 3G 客户端模式点击保存后请耐心等待。这段时间系统正在拨号，拨号时间为一分钟左右，因 USB 上网卡的型号而定。如果还不能拨号成功，请尝试重新插拔 USB 上网卡或重启路由器。
- 3、如果**配置向导**→**运行模式**选择无线客户端模式，那么图 3-13 的页面上出现提示：选择无线客户端模式点击保存后请耐心等待，这段时间系统正在连接对端设备。

## 第4章 开始菜单

**开始**菜单位于 WEB 界面的一级菜单栏的最上方，它提供了快速进入几个常见页面的接口，通过**开始**菜单，您可以快速地配置设备正常工作所需的基本参数，查看设备的运行状态，查看设备的流量统计信息，还可以重启设备。

### 4.1 配置向导

**开始**→**配置向导**页面可以帮助您快速配置一些设备正常工作所需的基本参数，具体内容及配置方法请参见章节 3.3。

### 4.2 运行状态

本节主要讲述**开始**→**运行状态**的使用，在本页面您可以查看设备的当前运行模式、有线状态和无线状态。

运行模式：

有线网关模式

有线状态：

WAN口状态			
连接类型	固定IP接入	连接状态	已连接
IP地址	200.200.202.140	子网掩码	255.255.255.0
网关地址	200.200.202.254	MAC地址	00:0C:43:30:52:66
主DNS服务器	210.22.7.3	备DNS服务器	
LAN口状态			
IP地址	192.168.1.1	子网掩码	255.255.255.0
MAC地址	00:0C:43:30:52:77		

无线状态：

连接状态	启用	AP工作模式	AP Mode
SSID	UTT	无线模式	11b/g/n混合
信道	6	MAC地址	C8:3A:35:00:57:E0

刷新

图 4-1 运行状态

- ◆ 设备运行模式：当前设备运行的模式。
- ◆ 有线状态：显示设备当前是否正常进行有线连接，包括 WAN 口状态和 LAN 口状态。
  - WAN 口状态：显示当前广域网接口的配置参数及运行状态。包括线路连接类型、连接状态、IP 地址、子网掩码、网关地址、MAC 地址和 DNS 服务器等配置信息；
  - LAN 口状态：显示当前局域网接口的信息，包括 IP 地址、子网掩码和 MAC 地址。
- ◆ 无线状态：显示设备当前是否启用无线功能，以及 SSID、工作频段、AP 工作模式、无线模式、IP 地址、子网掩码和 MAC 地址等信息。
- ▶ 刷新：单击“刷新”按钮，可查看最新的运行状态信息。

### 4.3  接口流量

本节主要讲述**开始—>接口流量**的使用，包括设备 WAN、LAN 和 WLAN 口的流量。如下图所示，从图中可看到相应接口的接收、发送数据的平均值，最大值、总和以及当前时刻的及时速率，并为其提供不了不同的单位（kbit/s 和 KB/s）。

若本页面无法正常显示，请单击“如果不能正常显示请安装 `svgviewer`”超链接，安装 `svgviewer` 插件。

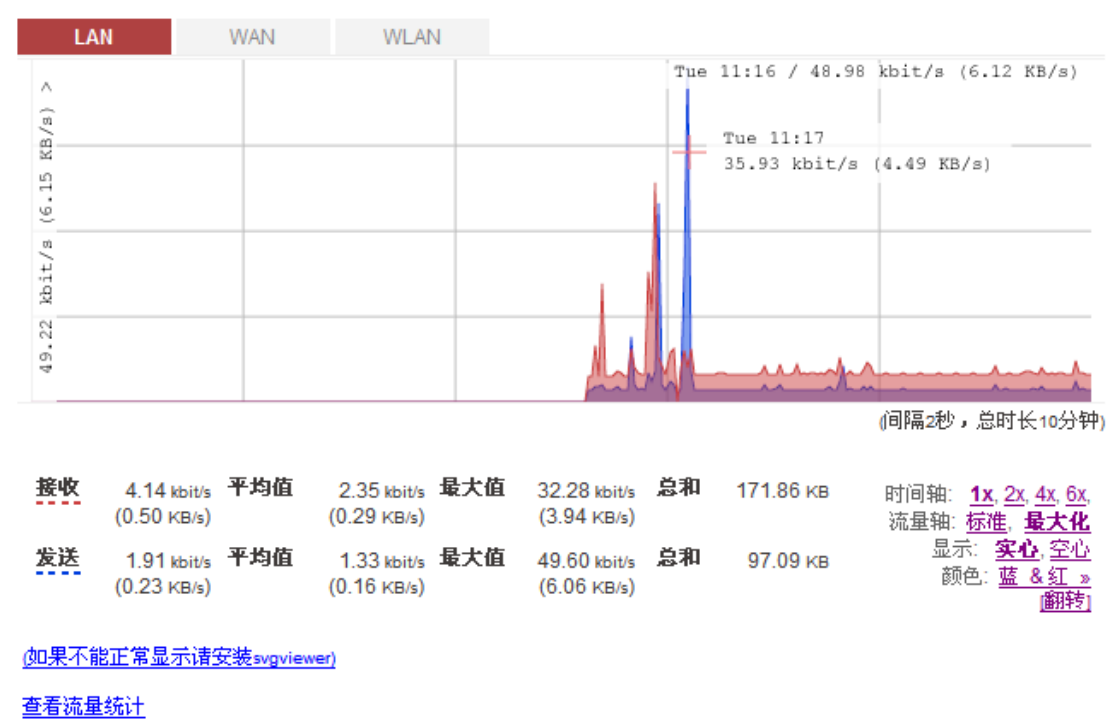


图 4-2  接口流量

- ◆ LAN：设备的局域网口，单击可查看该端口的流量图形化显示；
- ◆ WAN：设备的广域网口，单击可查看该端口的流量的图形化显示；
- ◆ WLAN：单击可查看无线上网时产生的流量的图形化显示；
- ◆ 时间轴：流量图中的横坐标，可通过单击图中时间轴选项（图中的 1x,2x,4x,6x）来确定显示效果；
- ◆ 流量轴：流量图中的纵坐标，可根据需要显示效果（如图中的标准、最大化）；
- ◆ 显示：提供实心和空心两个效果显示选项，可根据需要选择；
- ◆ 颜色：根据需求和显示的喜好，可以选择显示时的颜色，如红、蓝、黑等；
- ◆ 翻转：单击翻转按钮，接受和发送数据的颜色会对调；
- ◆ 如果不能显示请安装 `svgviewer`：若接口流量图形化不能正常显示时，单击该超链接，可下载相应控件，然后根据提示安装使用即可；
- ◆ 查看流量统计：单击该超链接可以查看设备通过有线，无线方式发送接收的数据

流量，如 4-3 所示。



图 4-3 流量统计

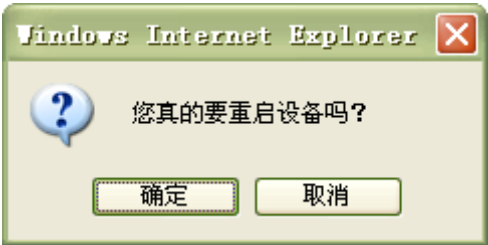
- ◆ 有线流量：设备通过有线接入方式发送、接收的数据包数、字节数；
- ◆ 无线流量：设备通过无线接入方式发送、接收的数据包数、字节数；
- ▶ 清除：单击“清除”按钮，可以清除全部流量统计信息，配合“刷新”按钮，可查看清除时刻至今这段时间内的流量统计信息；
- ▶ 刷新：单击“刷新”按钮，可以查看最新的流量统计信息。

4.4 重启设备



图 4-4 重启设备

- ▶ 重启：用于重新启动设备一次。单击“重启”按钮后，弹出以下提示框，如果您的确需要重启设备，请单击“确定”按钮，设备将开始重启过程。



- ⊕ **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。;

## 第5章 运行模式

在本页面，您可以配置设备的运行模式，选择不同模式的同时，您还可以自行决定是否启用设备的网络地址转换功能，如下图所示：

设备运行模式选择：

- ☒ 有线网关模式
- ☐ 3G客户端模式
- ☐ 无线客户端模式
- ☒ 启用NAT

保存

重填

图 5-1 运行模式

- ◆ 有线网关模式：设备采用有线网关的方式为用户员提供远程接入；
- ◆ 3G 客户模式：设备采用 3G 客户端的方式为用户提供远程接入；
- ◆ 无线客户端模式：设备采用无线客户端的方式为用户提供远程接入；
- ◆ 启用 NAT：包括启用和禁用 NAT 功能两个选项；
- ▶ 保存：保存当前配置参数；
- ▶ 重填：重新填写当前配置参数。

**提示：**图 5-1 中的“启用 NAT”仅对系统默认 NAT 功能生效，即启用该功能时，启用了系统默认的 NAT，禁用时则关闭了系统默认生效的 NAT 功能；而该功能无论是启用还是禁用对用户新建的 NAT 规则均不产生影响。

# 第6章 网络参数

在网络参数配置中，主要包括配置无线路由器的基本网络参数，包括 WAN 口配置、LAN 口配置、DHCP 服务器、DDNS 配置和 UPnP 配置。

## 6.1 WAN 口配置

本节主要讲述 **网络参数—>WAN 口配置** 的配置方法。

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

在 **快速向导** 中配置完上网线路之后，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。

### 6.1.1 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 6-1、表 6-2 所示。

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
固定IP接入	已连接	200.200.202.140	255.255.255.0	200.200.202.254	17080	37912	3
<div><div></div><div></div></div>							刷新

表 6-1 线路连接信息列表

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)		
已连接	200.200.202.140	255.255.255.0	200.200.202.254	17080	37912		
<div><div></div><div></div></div>							刷新

表 6-2 线路连接信息列表（续表 6-1）

► 刷新：单击“刷新”按钮，可获得最新的线路连接信息。

### 6.1.1.1 参数涵义

- ◆ 连接类型：当前上网接入线路的连接类型；
- ◆ 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 2 种状态，详见表 6-3。处于“已连接”状态时，还会显示该线路保持本次连接的时间（单位：小时:分:秒）。

连接状态	状态描述
断开	物理接口没有连接，或者没有拨号，或用户名、密码等参数配置错
已连接	验证通过，PPPoE 连接已经建立，可以传送数据

表 6-3 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 2 种状态，详见表 6-4。

连接状态	状态描述
断开	物理接口没有连接，关闭等。
已连接	物理接口和对方网络设备建立连接。

表 6-4 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 2 种状态，详见表 6-5。处于“已连接”状态时，还会显示该线路保持本次连接的时间（单位：小时:分:秒）（单位：小时:分:秒）。

连接状态	状态描述
断开	物理接口没有连接或接口关闭，DHCP 服务器没有可分配的地址。
已连接	已经获得动态分配的 IP 地址，线路连接正常。

表 6-5 动态 IP 接入线路连接状态描述

#### 4. 3G 接入线路

如果当前线路是 3G 接入线路，那么，共有 2 种状态，详见表 6-6。处于“已连接”状态时，还会显示该线路保持本次连接的时间（单位：小时:分:秒）。

连接状态	状态描述
断开	物理接口连接 3G 卡或运营商、3G 卡类型配置错误
已连接	已经获得动态分配的 IP 地址，线路连接正常

表 6-6 3G 接入线路连接状态描述

◆ IP 地址、子网掩码、网关地址：分以下四种情况。

#### 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。

#### 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 动态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。

#### 4. 3G 接入

如果当前线路是 3G 接入线路，则它们分别是 ISP 分配的是网络地址、子网掩码。

◆ 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；

### 6.1.1.2 PPPOE 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”下方才会显示“拨号”和“挂断”按钮，如表 6-7 所示。这两个按钮的功能如下：

- ▶ 拨号：用以建立和 PPPOE 服务器的连接，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：挂断当前与 PPPOE 服务器的拨号连接；
- ▶ 刷新：单击该按钮可显示线路连接信息列表的最新信息。

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
PPPoE接入	已连接 0小时2分49秒	10.0.0.30	255.255.255.255		16		

表 6-7 线路连接信息列表——PPPoE 拨号接入

6.1.1.3 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”下方才会显示“更新”和“释放”按钮，如表 6-8 所示。

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
动态IP接入	已连接 0小时0分0秒	192.168.1.33	255.255.255.0		9504	6	
<div><div></div><div></div></div>							<div>更新</div> <div>释放</div> <div>刷新</div>

表 6-8 线路连接信息列表——动态 IP 接入

- ▶ 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；
- ▶ 释放：释放当前得到的动态 IP 地址；
- ▶ 刷新：显示当前线路连接的信息列表。

⊕ 提示：

更新动态 IP 连接的线路时，要先单击“释放”按钮释放线路连接，再单击“更新”按钮；更新后单击“刷新”按钮可以看到线路连接信息列表的最新信息。

6.1.1.4 3G 接入线路的连接与挂断

如果某线路选择的是 3G 接入线路，那么在“线路连接信息列表”下方会显示“连接”和“断开”按钮，如表 6-9 所示。这 2 个按钮功能如下：

- ▶ 连接：系统用来连接断开的或未连接的 3G 线路接入；
- ▶ 断开：系统用来将处于连接状态的 3G 线路接入断开。

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
3G接入	已连接 0小时0分18秒	172.17.46.178	255.255.255.255		80		
<div><div></div><div></div></div>							<div>连接</div> <div>断开</div> <div>刷新</div>

表 6-9 线路连接信息列表——3G 接入

## 6.1.2 线路配置

下面将首先分别介绍固定 IP 接入、动态 IP 接入、PPPoE 接入和 3G 四种情况下，如何配置线路，以及如何删除已配置的线路。

### 6.1.2.1 固定 IP 接入

接入方式	固定IP接入 ▼
IP地址*	200.200.202.140
子网掩码*	255.255.255.0
网关地址*	200.200.202.254
主DNS服务器*	210.22.70.3
备DNS服务器	

保存 重填

图 6-1 网络配置——固定 IP 接入

- ◆ 接入方式：此处选择固定 IP 接入，为此通过手工输入静态 IP 地址、子网掩码、网关地址、DNS 服务器地址；
  - ◆ IP 地址：设备使用的 IP 地址；
  - ◆ 子网掩码：设备使用的所在网络的子网掩码，局域网计算机必须与设备处于同一个子网中；
  - ◆ 网关地址：设备的网关地址，网关地址必须与设备 IP 地址处于同一个子网中；
  - ◆ 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。
- ▶ 保存：固定 IP 接入配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。

⚡ 提示：如果改变了设备的“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。

### 6.1.2.2 动态 IP 接入

接入方式	动态IP接入 ▼
------	----------

保存 重填

图 6-2 网络配置——动态 IP 接入

◆ 接入方式：此处选择动态 IP 接入，设备将通过 DHCP 动态获取 IP 地址、子网掩码以及网关地址等网络参数信息；

▶ 保存：动态 IP 接入配置参数生效；

▶ 重填：恢复到修改前的配置参数。

⊕ 提示：如果设备通过 DHCP 获取了新的“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。

### 6.1.2.3 PPPoE 接入

接入方式	PPPoE接入
用户名*	<input type="text"/>
密码*	<input type="password"/>
密码验证方式	Either
拨号类型	自动拨号
空闲时间*	0 分钟
MTU*	1492 字节 (取值范围：1-1492)
<div>保存 重填</div>	

图 6-3 网络配置——PPPoE 接入

◆ 接入方式：此处选择 PPPoE 接入，ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号），设备将通过拨号获取 IP 地址、子网掩码以及网关地址信息；

◆ 密码验证方式：ISP 验证用户名及密码的方式，默认为 Either。多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，Either 表示自动和对方设备协商采用哪种验证方式；

◆ 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 **网络参数—>WAN 口配置** 的“线路连接信息列表”（章节 6.1.1）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；

◆ 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：分钟）；

◆ MTU：最大传输单元，缺省值为 1492 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；

▶ 保存：PPPoE 接入配置参数生效；

▶ 重填：恢复到修改前的配置参数。

### 6.1.2.4 3G 接入

接入方式	3G
3G卡类型	HUAWEI E169
运营商	中国移动
认证方法	SIM认证
PIN码	
接入点名	CMNET
拨号	*99***1#
高级PPP配置：	
用户名	CMNET
密码	●●●●●

**注意：**请按ISP的要求输入正确的参数，设置保存后，请点击本页面中的刷新按钮。拨号时间为一分钟左右，因USB上网卡的型号而定。如果还不能拨号成功，请尝试重新插拔USB上网卡或重启路由器。

保存 重填

图 6-4 网络配置——3G 接入

- ◆ 接入方式：这里选择 3G 接入，选择后设备将采用 3G 无线接入的方式连入网络；
- ◆ 3G 卡类型：设备目前支持的 3G 上网卡型号有 HUAWEI E1750、HUAWEI E169、HUAWEI EC1260、HUAWEI ET128；
- ◆ 运营商：提供 3G 接入的网络服务提供商，包括中国移动、中国联通、中国电信三个选项；
- ◆ 认证方法：采用 3G 方式接入网络时和运营商标采用的认证，共提供 SIM 认证和密码认证两个选项；
- ◆ PIN 码：3G 上网卡的个人身份识别码；
- ◆ 接入点名：用来连接运营商的不同接入点的标识名；
- ◆ 拨号：拨号连接到运营商基站时发送的连接指令内容之一；
- ◆ 用户名：PPP 认证的用户名；
- ◆ 密码：PPP 认证的密码；
- ▶ 保存：保存当前配置参数；
- ▶ 重填：重新填写网络配置参数。

⊕ 提示：

当选择 3G 接入时，强烈建议用户名只配置“3G 卡类型”和“运营商”两个选项，其余参数保持默认，如需修改请按 ISP 的要求输入正确的参数，设置保存后，请点击本页面中的刷新按钮。拨号时长视 USB 上网卡类型而定，如果不能拨上号，请重新插拔 USB 卡或重启路由器。

### 6.1.3 MAC 地址克隆



The image shows a configuration interface for MAC address cloning. It features a label 'MAC地址克隆' followed by a text input field containing the MAC address '00:0C:43:30:52:66'. Below the input field are two buttons: '保存' (Save) and '重填' (Reset).

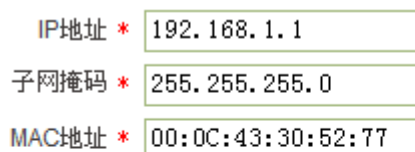
图 6-5 MAC 地址克隆

MAC 地址克隆即修改设备 WAN 口的 MAC 地址，WAN 口的 MAC 地址可在此处进行修改。

- ▶ 保存：MAC 地址克隆配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。

## 6.2 LAN 口配置

本节主要讲述**网络参数—>LAN 口配置**的配置方法。包括 IP 地址、子网掩码和 MAC 地址。



The image shows a configuration interface for LAN port settings. It contains three rows, each with a label and a text input field: 'IP地址 \*' with '192.168.1.1', '子网掩码 \*' with '255.255.255.0', and 'MAC地址 \*' with '00:0C:43:30:52:77'.

**注意：**修改IP地址后，您必须使用新的IP地址才能登录设备。



The image shows two buttons: '保存' (Save) and '重填' (Reset).

图 6-6 LAN 口配置

- ◆ IP 地址：局域网的 IP 地址；
- ◆ 子网掩码：局域网 IP 地址的子网掩码；
- ◆ MAC 地址：LAN 口的 MAC 地址。建议不要随意修改 LAN 口的 MAC 地址。

- ▶ 保存：保存当前配置参数以使其生效；
- ▶ 重填：恢复到修改前的配置参数。

⊕ 提示：

修改过 LAN 口 IP 地址后，必须使用新的 IP 地址，并且登陆主机的 IP 要和其在同一网段才能登陆设备！

## 6.3 DHCP 服务器

本节主要讲述**网络参数—>DHCP 服务器**的配置方法。包括 DHCP 服务设置、静态 DHCP 和 DHCP 客户列表。

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 服务器等信息。

### 6.3.1 DHCP 服务器设置

启用DHCP服务器

☒

打勾表示启用DHCP服务器功能，只有启用该功能，DHCP服务器相关配置才能生效。

起始IP地址 \*

192.168.1.100

结束IP地址 \*

192.168.1.200

子网掩码 \*

255.255.255.0

网关地址 \*

192.168.1.1

租用时间 \*

86400

秒

启用DNS代理

☒

打勾表示启用DNS代理，只有启用该功能，DNS代理相关配置才能生效。

主DNS服务器 \*

192.168.1.1

备DNS服务器

保存

重填

图 6-7 DHCP 服务设置

- ◆ 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 6-7 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）；
- ◆ 结束 IP 地址：DHCP 服务器给局域网计算机自动分配的最终 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）；

- ◆ 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）；
- ◆ 启用 DNS 代理：选中表示启用，启用后设备的 DNS 代理功能才会生效；
- ◆ 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；
- ◆ 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；
- ▶ 保存：DHCP 服务配置参数生效；
- ▶ 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。

## 6.3.2 静态 DHCP

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，这时就需要使用静态 DHCP 功能，将计算机的 MAC 地址与某个 IP 地址绑定，如图 6-8 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。

6.3.2.1 静态 DHCP 信息列表

静态DHCP列表

2/50

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

	用户名	IP地址	MAC地址	编辑
<input type="checkbox"/>	A	192.168.1.15	00:21:85:9B:45:44	
<input type="checkbox"/>	B	192.168.1.10	00:1f:3c:0f:07:f4	

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 6-10 静态 DHCP 信息列表

- ▶ 添加静态 DHCP 条目：单击“添加新条目”按钮，在跳出的静态 DHCP 配置页面中，输入静态 DHCP 配置信息，单击“保存”按钮，生成新的静态 DHCP 条目；
- ▶ 浏览静态 DHCP 条目：如果已经生成了静态 DHCP 条目，则可在“静态 DHCP 信息列表”中浏览静态 DHCP 信息；
- ▶ 编辑静态 DHCP 条目：如果想修改某一个静态 DHCP 条目的配置信息，只需单击该条目的“用户名”或该条目所对应的“”图标，设备就会跳转到静态 DHCP 配置页面，对其配置信息进行修改；
- ▶ 删除静态 DHCP 条目：共有以下 3 种删除方法。
  - 方法 1：单击某条目对应的 图标，即可删除对应静态 DHCP 条目；
  - 方法 2：选中若干静态 DHCP 条目，单击右下角的“删除”按钮，即可删除被选中的条目；
  - 方法 3：若需要删除全部静态 DHCP 条目，则直接单击“删除所有条目”按钮即可。

6.3.2.2 静态 DHCP 配置

用户名 \*

abc

IP地址 \*

192.168.1.100

MAC地址 \*

0022aa001122

保存

重填

返回

图 6-8 静态 DHCP 配置

- ◆ 用户名：配置该 DHCP 绑定的计算机的用户名（自定义，不能重复）；
- ◆ 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；

- ▶ 保存：DHCP 绑定配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。
- ▶ 返回：返回上一页，即 **网络参数**—>**DHCP 服务器**—>**静态 DHCP** 页面。

⊕ 提示：

- 1、 设置成功后，设备将为指定计算机固定分配预设的 IP 地址；
- 2、 配置的 IP 地址要在 DHCP 服务器提供的范围之内，否则会提示错误。

6.3.2.3 自定义静态 DHCP 条目

配置静态 DHCP 条目的步骤如下：

第一步，进入 **网络参数**—>**DHCP 服务器**—>**静态 DHCP** 页面；

第二步，单击“添加新条目”按钮，在弹出的 **静态 DHCP 配置** 页面中，输入“用户名”，“IP 地址”和“MAC 地址”，然后单击“保存”按钮；

第三步，该静态 DHCP 条目添加成功后，可以在“静态 DHCP 条目信息列表”中查看；

第四步，继续配置其他静态 DHCP 条目；

⊕ 提示：如果要删除静态 DHCP 条目，则可以按照《6.3.2.1 静态 DHCP 信息列表》提供的 3 种方法进行删除操作。

6.3.3 DHCP 客户列表

DHCP客户端列表

1/1

1/1 第一页 上一页 下一页 最后页 前往 第  页 搜索

IP地址	子网掩码	MAC地址	剩余租期
192.168.1.100	255.255.255.0	00:E0:4C:19:03:2D	85420秒

刷新

表 6-11 DHCP 客户端信息列表

- ◆ IP 地址：DHCP 服务器分配的 IP 地址；
- ◆ 子网掩码：DHCP 服务器分配的 IP 地址的子网掩码；
- ◆ MAC 地址：使用该 IP 地址的网络设备的 MAC 地址；

◆ 剩余租期：租用该 IP 地址的剩余时间（时间单位：秒）；

▶ 刷新：单击“刷新”按钮，可获得最新的 DHCP 地址池使用信息。

⊕ **提示：**DHCP 客户端信息列表只显示通过 DHCP 服务器自动获取 IP 地址的用户信息，通过客户端配置固定 IP 地址的用户，不会显示在此列表中。

## 6.3.4 DHCP 配置实例

### 1. 应用需求

本实例中，要求无线路由器开启 DHCP 功能，起始地址为 192.168.1.10，共可分配 100 个地址，其中 MAC 地址为 00:21:85:9B:45:44 的主机其 IP 地址固定为 192.168.1.15，MAC 地址为 00:1f:3c:0f:07:f4 其 IP 地址固定为 192.168.1.10。

### 2. 配置步骤

第一步，进入**网络参数**—>**DHCP 服务器**—>**DHCP 服务设置**页面；

第二步，启用 DHCP 功能，并配置相关 DHCP 服务参数，（如下图）

启用DHCP服务器 ☒

打勾表示启用DHCP服务器功能，只有启用该功能，DHCP服务器相关配置才能生效。

起始IP地址 *	192.168.1.10
结束IP地址 *	192.168.1.110
子网掩码 *	255.255.255.0
网关地址 *	192.168.1.1
租用时间 *	3600 秒

---

启用DNS代理 ☒

打勾表示启用DNS代理，只有启用该功能，DNS代理相关配置才能生效。

主DNS服务器 *	210.22.70.3
备DNS服务器	

图 6-9 DHCP 服务设置——实例

第三步，进入**网络参数**—>**DHCP 服务器**—>**静态DHCP** 页面；

第四步，单击“添加新条目”按钮，在弹出的**静态 DHCP 配置**页面中（如下图），在“用户”中输入 A，在“MAC 地址”中输入 00:21:85:9B:45:44，在“IP 地址”中输入 192.168.1.15，然后单击“保存”按钮；

用户名 \*

IP地址 \*

MAC地址 \*

保存

重填

返回

图 6-10 静态 DHCP 配置 1——实例

第五步，继续配置另外 1 条静态 DHCP 条目（MAC 地址为 00:1f:3c:0f:07:f4，IP 地址为 192.168.1.10）；

用户名 \*

IP地址 \*


MAC地址 \*

保存

重填

返回

图 6-11 静态 DHCP 配置 2——实例

至此，配置完成，可以在“静态 DHCP 信息列表”中查看这 2 个静态 DHCP 条目的相关信息，如表 6-12 所示。如果发现配置错误，可以直接单击对应条目的  图标，在弹出的静态 DHCP 配置页面中进行修改并保存。

静态DHCP列表

2/50

1/1

第一页

上一页

下一页





最后一页

前往

第

页

搜索

	用户名	IP地址	MAC地址	编辑
<input type="checkbox"/>	A	192.168.1.15	00:21:85:9B:45:44	 
<input type="checkbox"/>	B	192.168.1.10	00:1f:3c:0f:07:f4	 

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 6-12 静态 DHCP 信息列表——实例

6.4 DDNS 配置

本节主要讲述网络参数—>DDNS 配置的配置方法。在本页面不仅可以配置 DDNS 参数，还可以查看所配置的 DDNS 状态。

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, 艾泰科技设备支持 3322.org 和 iplink.com.cn 的 DDNS 服务, 将来还将陆续提供对其他 DDNS 服务的支持。

## 6.4.1 申请 DDNS 帐号

请登录 <http://www.3322.org> 或 <http://www.utt.com.cn/ddns> 申请相应的域名, 本节则以申请 3322.org 的二级域名为例。

主机名:	<input type="text" value="avery12345"/>	3322.org ▼	HELP
IP地址:	<input type="text" value="58.246.187.126"/>	HELP	
邮件服务器 (mx):	<input type="text"/>	HELP	
备份邮件服务器:	<input type="checkbox"/>	HELP	
通配符:	是 ▼	HELP	
			确定

图 6-12 申请 DDNS 帐号

- ◆ 主机名: 填入欲申请的二级域名, 不能与已注册的域名重复;
- ◆ IP 地址: 当前域名对应的 IP 地址, 即无线路由器的 WAN 口 IP 地址;
- ◆ 确定: 单击“确定”按钮, 成功注册域名。

## 6.4.2 配置 DDNS 服务

配置 DDNS 时, 选择不同的服务商, 配置页面是不同的, 如图 6-13、图 6-14、图 6-15 所示:

服务商	无 ▼
<input type="button" value="保存"/> <input type="button" value="重填"/>	

图 6-13 服务商——无

- ◆ 服务商: 提供 DDNS 服务的运营商, 这里“无”表示没有启用 DDNS 功能;
- ▶ 保存: 保存当前配置参数;

▶ 重填：重新填写当前页面配置参数。

服务商 

3322.org

注册域名 <http://www.3322.org>

主机名 \*

用户名 \*

密码 \*

保存

重填

图 6-14 服务商——3322.org

- ◆ 服务商：提供 DDNS 服务的运营商，这里选择 3322.org;
- ◆ 注册域名：单击超链接 <http://www.3322.org> 即可进入 3322 域名申请页面;
- ◆ 主机名：使用 DDNS 服务的主机的名称;
- ◆ 用户名：申请 DDNS 帐号时使用的主机名;
- ◆ 密码：用户注册时系统生成的密码;
- ▶ 保存：保存当前配置参数;
- ▶ 重填：重新填写当前配置参数;
- ▶ 更新状态，单击该按钮，可以更新 DDNS 的状态，如表 6-13 所示。

DDNS状态：

更新状态	主机名	IP地址	更新时间
已连接	avery12345.3322.org	58.246.187.126	2009/9/28 14:05:55

更新状态

表 6-13 DDNS 状态

⊕ 提示：WAN 地址必须为公网地址才能将路由器的地址映射到域名。

服务商 

iplink.com.cn

注册域名 <http://www.utt.com.cn/ddns>

主机名 \*

密钥 \*

当服务商为iplink.com.cn时，系统时间需要设置为网络时间同步。

保存

重填

图 6-15 服务商——iplink.com.cn

- ◆ 服务商：DDNS 服务的提供商，这里选择 iplink.com.cn;
- ◆ 注册域名：点击 <http://www.utt.com.cn/ddns> 超链接，即可进入该页面申请域名;
- ◆ 主机名：申请 DDNS 帐号时使用的主机名;

- ◆ 用户名：用户注册时输入的用户名；
- ◆ 密钥：用户注册时系统生成的密码；
- ▶ 保存：DDNS 配置生效；
- ▶ 重填：恢复到修改前的配置参数。

### 6.4.3 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 avery12345.3322.org）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：58.246.187.126），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。

**Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:**

```
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
```

**Ping statistics for 58.246.187.126:**

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

1. ISP（例如中国电信）分配给 WAN 口连接线路的 IP 地址是公网地址的时候才能保证该域名能被 Internet 的用户访问；
2. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射。

## 6.5 UPnP

通用即插即用 (UPnP) 是一种用于 PC 机和智能设备（或仪器）的常见对等网络连接的体系结构。使用 UPnP 意味着简单、更多选择和更新颖的体验。支持通用即插即用技术的网络产品只需实际连到网络上，即可开始正常工作。

### 6.5.1 UPnP 配置

在本页面中配置 UPnP 时，只需启用或禁用该功能即可，如下图所示：

启用UPnP ☐

图 6-16 配置 UPnP

- ◆ 启用 UPnP：当图中方框被选中时表示启用了 UPnP，没有选中时表示没有启用 UPnP，启用 UPnP 时点击“保存”按钮配置才能生效；
- ▶ 保存：保存当前配置；
- ▶ 重填：重新填写当前配置参数。

6.5.2 UPnP NAT 映射列表

如果设备上开启了 NAT 功能，那么启用 UPnP 功能后，UPnP NAT 映射列表中可见下图所示内容：

UPnP NAT映射列表

2/2

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

	序号	内部地址	内部端口	协议	对端地址	对端端口	描述
<input type="checkbox"/>	1	192.168.1.100	80	TCP		19972	Thunder5
<input type="checkbox"/>	2	192.168.1.100	21157	UDP		19972	Thunder5

刷新

图 6-17 UPnP NAT 映射列表

- ◆ 序号：是指 NAT 映射的序号；
- ◆ 内部地址：使用 NAT 功能的内部主机的 IP 地址；
- ◆ 内部端口：内部主机的使用 NAT 功能时采用的端口；
- ◆ 协议：NAT 转换的采用的传输层协议，如图中的 TCP；
- ◆ 对端地址：发生 NAT 转换时的公网地址；
- ◆ 对端端口：发生 NAT 转换时公网的 IP 地址所对应的端口；
- ◆ 描述：使用的 NAT 功能的用户或程序的简单描述；
- ▶ 刷新：单击该按钮可显示当前最新的 UPnP NAT 映射信息。

## 第7章 无线配置

在无线配置中，主要设置设备相关无线功能及参数，包括：无线基本参数，无线安全机制设置，无线 MAC 地址过滤以及无线高级参数。此外，还可以查看无线主机的状态信息。

### 7.1 基本设置

本节主要讲述**无线配置**→**基本设置**的配置方法。在本页面，您可以配置路由器的、AP 的工作模式、SSID、无线模式、信道、频道带宽、启用或禁用 SSID 广播等功能。本章配置时按 AP Mode、APClient Mode 和 WDS 的顺序进行。

#### 7.1.1 AP Mode

如图 7-1 所示，在图中可配置设备的基本无线功能，包括启用/禁用无线功能，AP 的工作模式，SSID、无线模式、信道、频道带宽等。

启用无线功能	<input checked="" type="checkbox"/>
只有启用无线功能后，无线站点才能通过该设备相互通信。	
AP工作模式	AP Mode
SSID *	UTT-HiPER-89CA35
用于唯一地标识一个无线网络，大小写敏感。	
无线模式	11b/g/n混合
信道	6
无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。	
频道带宽	20M/40M
启用SSID广播	<input checked="" type="checkbox"/> 00:0C:43:30:52:88
启用后，设备将向无线网络广播自身的SSID。	
<input type="button" value="保存"/> <input type="button" value="重填"/>	

图 7-1 基本设置——AP Mode

- ◆ 启用无线功能：只有启用无线功能后，无线客户端才能连接到路由器，从而通过无线路由器进行无线通信，接入并访问路由器连接的有线网络；
- ◆ AP 工作模式：此处选择 AP Mode，即纯 AP 模式，在此模式下，对端设备可以是 AP Client 模式以及单客户端，进而实现数据交换；
- ◆ SSID：SSID（Service Set Identification，服务集标识）用于唯一地标识一个无线网络的字符串，大小写敏感；
- ◆ 无线模式：此参数用于设置无线设备的模式，提供仅 11g，仅 11n 和 11b/g/n 混合三个选项：
  - 仅 11g：即纯 802.11g 模式，本模式下，最大速率 54M bps。兼容 IEEE 802.11g 标准的无线站点可以接入设备；
  - 仅 11n：即纯 802.11n 模式，本模式下，最大速率为 150M bps。只有符合 IEEE 802.11n 标准的无线站点可以接入设备；
  - 11b/g/n 混合：符合 IEEE 802.11b、802.11g 或者 802.11n 标准的无线站点将各自按照自己的模式接入，最大速率分别为 11M bps、54M bps 和 150M bps；
- ◆ 信道：此参数用于选择无线网络工作的频率段，可以选择的范围从 1 到 11，另外提供自动选项，表示设备可以自动选择最优频率段。如果存在多个无线路由器时，要注意各个路由器的频段设置不能相互影响；
- ◆ 频道带宽：设置无线数据传输时所占用的频道带宽，可选项为：20M/40M 和 20M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用；对于以 802.11b 或者 802.11g 标准的无线站点来说，只能使用 20M 的频道带宽：
  - 20M/40M：选择 20M/40M 时，表示使用 802.11n 接入的无线站点将根据很接入对端协商的结果选择使用 20M 或 40M 的频道带宽；
  - 20M：选择 20M 时，表示使用 802.11n 接入的无线站点将使用 20M 的频道带宽。
- ◆ SSID 广播：启用或禁用 SSID 广播功能。如果开启此功能，那么，路由器将会把自己的 SSID 广播给所有的无线站点，这样，没有 SSID（为空值）的无线站点将获得正确的 SSID，从而连接到无线路由器，并加入到该 SSID 标识的无线网络。由于开启此功能存在安全风险（非法站点很容易获得 SSID 信息），一般建议禁用此功能；
- ▶ 保存：无线基本配置参数生效；
- ▶ 重填：恢复到修改前的无线基本配置参数。

⊕ 提示：

- 1、无线参数修改后，路由器的无线模块将会重启，无线模块重启会断开所有的无线连接，但不会影响有线连接；
- 2、AP 的各种工作模式功能各不相同，配置时请根据场合、使用需要自行选择。

## 7.1.2 APClient Mode

在第 5 章运行模式配置中，如果将设备配置为“无线客户端”，那么在无线基本中“AP 的工作模式”处便会有 APClient Mode 的选项，如图 7-2 所示：

AP工作模式

SSID \*   
用于唯一地标识一个无线网络，大小写敏感。

无线模式

信道   
无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。

频道带宽

启用SSID广播 ☒ C8:3A:35:0E:F0:58  
启用后，设备将向无线网络广播自身的SSID。

AP的SSID \*

AP的MAC地址 \*

安全模式

图 7-2 APClient Mode

- ◆ AP 的工作模式：这里选择“APClient Mode”；
- ◆ AP 的 MAC 地址：为设备提供接入的接入服务器 AP 的物理地址；
- ◆ 安全模式：这里选择“无安全机制”，注意要与对端设备安全机制保持一致；
- ▶ 保存：保存当前页面配置参数；
- ▶ 重填：重新填写当前配置参数。

⊕ 提示：

- 1、 工作在 APClient Mode 模式下的 3G 设备，只能与处于 AP Mode 的设备和无线客户端才能与其连通，实现数据交换。
- 2、 在 APClient Mode 模式下：安全模式和信道都要和对端保持一致，否则不能实现连通。
- 3、 安全模式中：共有：无安全机制、WEP、WPA-PSK/WPA2-PSK 三个选项。其中，WEP 的配置详见章节 7.2.2，WPA-PSK/WPA2-PSK 的配置详见章节 7.2.4。

### 7.1.3 WDS

WDS (Wireless Distribution System)无线分布式系统，是无线连接两个接入点（AP）的协议。在整个 WDS 无线网络中，把多个 AP 通过桥接或中继器的方式连接起来，使整个局域网网络以无线的方式为主。

本设备提供的 WDS 配置包括：Bridge Mode、Repeater Mode、Lazy Mode 三部分，在实际应用中仅起桥接功能，配置时要注意，各设备的 LAN 口 IP 要在同一网段中，同时连接双方的安全模式和信道带宽等参数都要保持一致。

#### 7.1.3.1 Repeater Mode

当设备的工作模式配置为 Repeater Mode 时，可与处于 Bridge Mode、Repeater Mode 以及 Lazy Mode 工作模式的网络设备交换数据，实现网络连通。

当设备的工作模式设为 Repeater Mode 时，如下图所示：

启用无线功能	<input checked="" type="checkbox"/>	只有启用无线功能后，无线站点才能通过该设备相互通信。
AP工作模式	Repeater Mode	
SSID *	UTT	用于唯一地标识一个无线网络，大小写敏感。
无线模式	11b/g/n混合	
信道	6	无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。
频道带宽	20M/40M	
启用SSID广播	<input checked="" type="checkbox"/> C8:3A:35:0E:F0:58	启用后，设备将向无线网络广播自身的SSID。
AP的MAC地址 *		
AP的MAC地址		
AP的MAC地址		
AP的MAC地址		
安全模式	无安全机制	
<div>保存 重填</div>		

图 7-3 Repeater Mode

启用无线功能、AP 工作模式、SSID、无线模式、信道、频道带宽、启用 SSID 广播的含义见章节 7.1.1 相关解释，在后续配置中若遇到上述术语也不再赘述；

- ◆ AP 的 MAC 地址：为设备提供接入的对端设备的物理地址；
- ◆ 安全模式：设备通过 WDS 功能建立连接的时候采用的加密方式，包括“无安全机制”、“WEP”、“TKIP”、“AES”四个选项。
  - 无安全机制：表示在数据交换过程中不采用任何加密算法保护通信数据；
  - WEP：表示在数据交换过程中采用 WEP 加密算法保护通信数据，如图 7-4 所示；
  - TKIP：表示在数据交换过程中采用 TKIP 加密算法保护通信数据，如图 7-6 所示；
  - AES：表示在数据交换过程中采用 AES 加密算法保护通信数据 图 7-7 所示；
- ▶ 保存：保存当前页面配置参数；
- ▶ 重填：重新填写当前配置参数。

安全模式: WEP

密钥格式: 16进制

密钥选择: WEP密钥

密钥类型: 禁用

密钥1:

密钥2:

密钥3:

密钥4:

保存 重填

图 7-4 WEP

- ◆ 安全模式：设备通过 WDS 功能建立连接时采用的加密方式，这里选择“WEP”；
- ◆ 密钥格式：提供 16 进制、ASCII 码两种格式：
  - 采用 16 进制时，密钥字符可以为 0~9，A、B、C、D、E、F；
  - 采用 ASCII 码时，密钥字符可以是所有的 ASCII 码；
- ◆ 密钥类型：用于设置密钥值，密钥的长度受密钥类型的影响：
  - 禁用：不启用对应的密钥；
  - 选择 64 位密钥时，输入 16 进制字符 10 个或者 ASCII 码字符 5 个；
  - 选择 128 位密钥时，输入 16 进制字符 26 个或者 ASCII 码字符 13 个；

#### ⊕ 提示：

- 1、配置 WEP 的密码时，两端配置的密钥对必须匹配且密钥要相同，否则会造成无法通信。

2、配置 WEP 的密钥时，至少要配置一个密钥，否则系统会用弹出框加以提示，如图 7-5 所示：



图 7-5 密钥配置提示

安全模式

预共享密钥\*  (取值范围：8-63个字符)

图 7-6 TKIP

- ◆ 安全模式：设备通过 WDS 功能建立连接时采用的加密方式，这里选择“TKIP”；
- ◆ 预共享密钥：通信双方商定的用于加密数据的密钥，其取值范围是 8 到 63 个字符；

安全模式

预共享密钥\*  (取值范围：8-63个字符)

图 7-7 AES

- ◆ 安全模式：设备通过 WDS 功能建立连接时采用的加密方式，这里选择“AES”；
- ◆ 预共享密钥：通信双方商定的用于加密数据的密钥，其取值范围是 8 到 63 个字符；

### 7.1.3.2 Bridge Mode

当设备的工作模式为 Bridge Mode 时，设备可与处于 Repeater Mode、Lazy Mode 模式的网络产品交换数据、实现网络连通。

启用无线功能 ☒

只有启用无线功能后，无线站点才能通过该设备相互通信。

AP工作模式 Bridge Mode

SSID \*

用于唯一地标识一个无线网络，大小写敏感。

无线模式 11b/g/n混合

信道 6

无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。

频道带宽 20M/40M

AP的MAC地址 \*

AP的MAC地址

AP的MAC地址

AP的MAC地址

安全模式 无安全机制

保存 重填

图 7-8 Bridge Mode

- ◆ AP 的工作模式：这里选择“Bridge Mode”，其参数配置与 Repeater Mode 相同，详见章节 7.1.3.1 中的相关描述。

### 7.1.3.3 Lazy Mode

当设备的工作模式为 Lazy Mode 时，设备可与处于 Repeater Mode、Bridge Mode 模式及单客户端的网络设备交换数据、实现网络连通。

启用无线功能 ☒

只有启用无线功能后，无线站点才能通过该设备相互通信。

AP 工作模式 Lazy Mode

SSID \* UTT

用于唯一地标识一个无线网络，大小写敏感。

无线模式 11b/g/n混合

信道 6

无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。

频道带宽 20M/40M

启用SSID广播 ☒ C8:3A:35:2F:AD:20

启用后，设备将向无线网络广播自身的SSID。

安全模式 无安全机制

保存 重填

图 7-9 Lazy Mode

- ◆ AP 的工作模式：这里选择“Lazy Mode”，其余参数配置与 Reteater Mode 相同，详见章节 7.1.3.1 中的相关描述。

## 7.1.4 配置实例

### 一、需求

现有无线路由器 A 和 B，组网拓扑如图 7-10，现要求 A 工作模式为 Bridge Mode，SSID 为 UTT 123，安全模式为 TKIP，预共享密码为 123456789，LAN 口 IP 为 192.168.1.1/25，B 的 LAN 口 IP 为 192.168.1.2/25。配置设备 A 和 B 使得两者间实现连通。

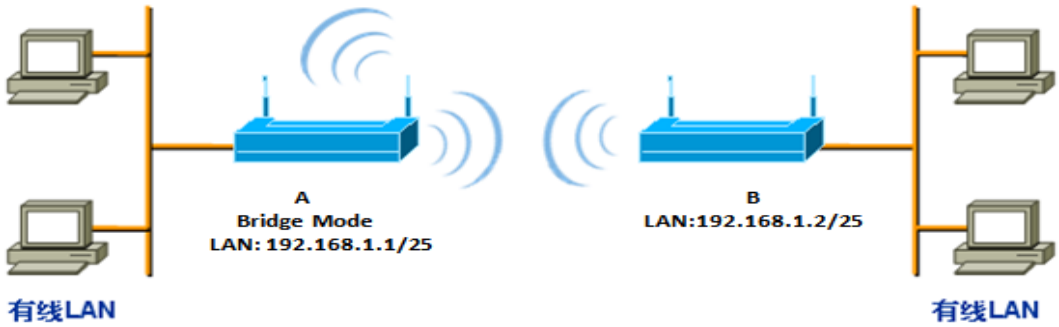


图 7-10 拓扑图

二、配置与验证

由 A 的配置要求可知:B 的工作模式可为 Lazy Mode 或 Bridge Mode(这里以 Lazy Mode 为例), SSID 为 UTT 123, 安全模式为 TKIP, 预共享密码为 123456789, 其余参数和 A 一样取默认值。

1、配置设备 A

启用无线功能 ☒

只有启用无线功能后，无线站点才能通过该设备相互通信。

AP工作模式 Bridge Mode

SSID \* UTT123

用于唯一地标识一个无线网络，大小写敏感。

无线模式 11b/g/n混合

信道 6

无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。

频道带宽 20M/40M

AP的MAC地址 \* c8:3a:35:00:57:e0

AP的MAC地址

AP的MAC地址

AP的MAC地址

安全模式 TKIP

预共享密钥\* 123456789 (取值范围：8-63个字符)

保存 重填

图 7-11 A 的配置

## 2、配置设备 B

启用无线功能



只有启用无线功能后，无线站点才能通过该设备相互通信。

AP工作模式

Lazy Mode



SSID \*

UTT123

用于唯一地标识一个无线网络，大小写敏感。

无线模式

11b/g/n混合



信道

6



无线网络工作的频率段，自动表示自动选择最优信道，也可根据实际情况手动选择。

频道带宽

20M/40M



启用SSID广播



C8:3A:35:00:57:E0

启用后，设备将向无线网络广播自身的SSID。

安全模式

TKIP



预共享密钥\*

123456789

(取值范围：8-63个字符)

图 7-12 B 的配置

## 3、验证 AB 间连通性

如图 7-13，说明 B 上的配置正确。

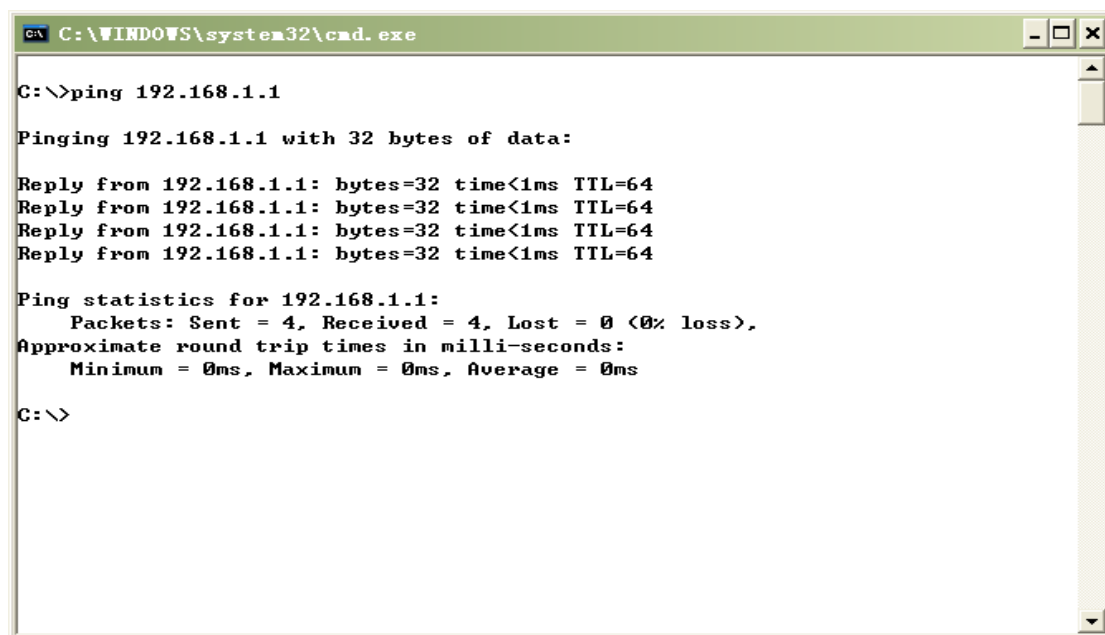


图 7-13 验证 AB 间连通性

⊕ 提示:

1、在实例中，A 的“AP 的 MAC 地址”实则是 B 的 MAC 地址，若两者不相同时，可修改 B 的地址以适应 A 的配置。

## 7.2 无线安全设置

本节主要讲述**无线配置—>无线安全设置**的配置方法，本设备提供 WEP、WPA/WPA2、WPA-PSK/WPA2-PSK 三种无线安全机制，同时，也允许用户不使用安全机制，以下各节将分别介绍它们的配置及使用。

### 7.2.1 无线安全设置——无安全机制

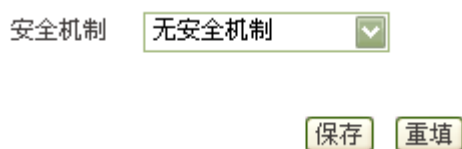


图 7-14 无线安全设置——无安全机制

- ◆ 安全机制：此处选择“无安全机制”，表示本设备当前不使用任何安全机制。
- ▶ 保存：无线安全设置参数生效；
- ▶ 重填：恢复到修改前的无线安全设置参数。

## 7.2.2 无线安全设置——WEP

安全机制 WEP

认证类型 开放系统

自动表示设备会根据无线客户端的请求自动选择开放系统或共享密钥方式。

密钥格式 16进制

密钥选择 WEP密钥 密钥类型

密钥1: ☐  禁用

密钥2: ☒  64位

密钥3: ☐  128位

密钥4: ☐  禁用

保存 重填

图 7-15 无线安全设置——WEP

- ◆ 安全机制：此处选择“WEP”，表示本设备将使用 802.11 协议提供的最基本的 WEP 安全机制；
- ◆ 认证类型：使用 WEP 加密机制时，提供自动、开放系统、共享密钥 3 个选项：
  - 自动：表示路由器会根据无线客户端的请求自动选择开放系统或共享密钥方式；
  - 开放系统：此时，无线客户端主机在不提供认证密钥的前提下，通过认证并关联到无线路由器；但若要进行数据传输，必须提供正确的密钥；
  - 共享密钥：此时，无线客户端主机必须提供正确的密钥才能通过认证，否则无法关联到路由器，从而无法进行数据传输；
- ◆ 密钥格式：提供 16 进制、ASCII 码两种格式：
  - 采用 16 进制时，密钥字符可以为 0~9，A、B、C、D、E、F；
  - 采用 ASCII 码时，密钥字符可以是所有的 ASCII 码；
- ◆ 密钥选择：用户可根据需要输入 1~4 个密钥，这 4 个密钥可以采用不同的密钥类型；
- ◆ WEP 密钥：用于设置密钥值，密钥的长度受密钥类型的影响：
  - 选择 64 位密钥时，输入 16 进制字符 10 个或者 ASCII 码字符 5 个；
  - 选择 128 位密钥时，输入 16 进制字符 26 个或者 ASCII 码字符 13 个；
- ◆ 密钥类型：用于选择密钥类型，提供禁用、64 位、128 位、3 个选项。其中，禁用表示不使用当前密钥，而 64 位、128 位、则用于指定 WEP 密钥的长度；

- ▶ 保存：无线安全设置参数生效；
- ▶ 重填：恢复到修改前的无线安全设置参数。

### 7.2.3 无线安全设置——WPA/WPA2

安全机制 WPA/WPA2

WPA版本 WPA

加密算法 AES

Radius服务器IP\*

Radius端口\* 1812 (取值范围：1-65535)

Radius密码\* (取值范围：1-31个字符)

密钥更新周期\* 3600 秒 (取值范围：60-86400；0表示不更新)

保存 重填

图 7-16 无线安全设置——WPA/WPA2

- ◆ 安全机制：此处选择“WPA/WPA2”，表示本设备将采用 WPA 或 WPA2 安全机制。此安全机制下，本设备将采用 Radius 服务器进行身份认证并得到密钥；
- ◆ WPA 版本：用来设置本设备将使用的安全模式：
  - 自动：表示本设备会根据无线客户端的请求自动选择 WPA 或者 WPA2 安全模式；
  - WPA：表示本设备将采用 WPA 的安全模式；
  - WPA2：表示本设备将采用 WPA2 的安全模式；
- ◆ 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES：
  - 自动：表示本设备将根据需要自动选择加密算法；
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法；
- ◆ Radius 服务器 IP：用来对无线主机进行身份认证的 Radius 服务器的 IP 地址；
- ◆ Radius 端口：Radius 服务器对无线主机进行身份认证时使用的服务端口号；
- ◆ Radius 密码：该项用来设置访问 Radius 服务的密码；
- ◆ 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。缺省值为 3600，值为 0 时表示不更新；
- ▶ 保存：无线安全设置参数生效；

- ▶ 重填：恢复到修改前的无线安全设置参数。

## 7.2.4 无线安全设置——WPA-PSK/WPA2-PSK

安全机制 WPA-PSK/WPA2-PSK

WPA版本 自动

加密算法 自动

预共享密钥\* (取值范围：8-63个字符)

密钥更新周期\* 3600 秒 (取值范围：60-86400；0表示不更新)

保存 重填

图 7-17 无线安全设置——WPA-PSK/WPA2-PSK

- ◆ 安全机制：此处选择“WPA-PSK /WPA2-PSK”，表示本设备将采用 WPA-PSK 或 WPA2-PSK 安全机制。此安全机制下，本设备将采用基于预共享密钥的 WPA 模式；
- ◆ WPA 版本：用来设置本设备将使用的安全模式：
  - 自动：表示本设备会根据无线客户端的请求自动选择 WPA-PSK 或者 WPA2-PSK 安全模式；
  - WPA：表示本设备将采用 WPA-PSK 的安全模式；
  - WPA2：表示本设备将采用 WPA2-PSK 的安全模式；
- ◆ 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES：
  - 自动：表示本设备将根据需要自动选择加密算法；
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法；
- ◆ 预共享密钥：预先设置的初始化密钥，取值为 8~63 个字符；
- ◆ 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。默认值为 3600，值为 0 时表示不更新；
- ▶ 保存：保存无线安全设置参数以使其生效；
- ▶ 重填：恢复到修改前的无线安全设置参数。

## 7.3 无线 MAC 地址过滤

本节主要讲述**无线配置**→**无线 MAC 地址过滤**的配置方法。通过设置 MAC 地址过滤功能，可以允许或禁止无线主机接入本设备以及无线网络。

### 7.3.1 MAC 地址过滤全局配置

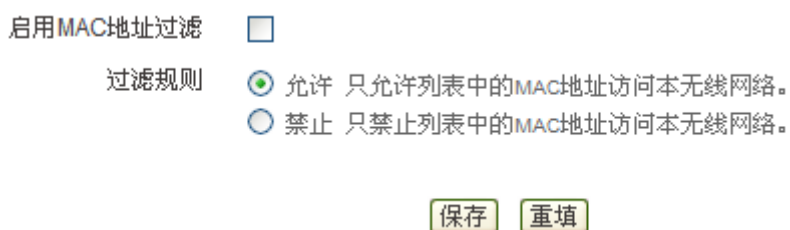


图 7-18 MAC 地址过滤全局配置

- ◆ 启用 MAC 地址过滤：启用或禁用 MAC 地址过滤功能，选中表示启用；
- ◆ 过滤规则：设置 MAC 地址过滤的规则，该规则对“MAC 地址过滤信息列表”生效：
  - 允许：表示只允许“MAC 地址过滤信息列表”中的 MAC 地址对应的无线客户端接入本设备，禁止除过滤表以外的无线客户端接入；
  - 禁止：表示只禁止“MAC 地址过滤信息列表”中的 MAC 地址对应的无线客户端接入本设备，允许除过滤表以外的无线客户端接入。
- ▶ 保存：MAC 地址过滤全局配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。

### 7.3.2 MAC 地址过滤信息列表

MAC地址过滤信息列表				2/50	
1/1	第一页	上一页	下一页	最后页	前往 第 <input type="text"/> 页
		搜索	<input type="text"/>		
	ID	MAC地址	编辑		
<input type="checkbox"/>	1	00:22:aa:04:bc:ca			
<input type="checkbox"/>	2	00:22:aa:11:22:33			

☐ 全选 / 全不选

表 7-1 MAC 地址过滤信息列表

- ▶ 增加 MAC 地址过滤条目：单击“添加新条目”按钮，即可进入 **MAC 地址过滤配置** 页面，输入 MAC 地址，单击“保存”按钮后，将生成新的 MAC 地址过滤条目；
- ▶ 浏览 MAC 地址过滤条目：如果已配置了若干 MAC 地址过滤条目，可在“MAC 地址过滤信息列表”中浏览相关信息，如表 7-1 所示；
- ▶ 编辑 MAC 地址过滤条目：如果想编辑某个 MAC 地址过滤条目，只需单击该条目对应的 图标或对应的 ID 值，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 MAC 地址过滤条目：共有以下 3 种删除方法。
  - 方法 1：单击某条目对应的 图标，即可删除对应 MAC 地址过滤条目；
  - 方法 2：选中若干 MAC 地址过滤条目，单击右下角的“删除”按钮，即可删除被选中的条目；
  - 方法 3：若需要删除全部 MAC 地址过滤条目，则直接单击“删除所有条目”按钮即可。

### 7.3.3 MAC 地址过滤配置

如前所述，单击“添加新条目”按钮或 图标，即可进入 **MAC 地址过滤配置** 页面。

MAC 地址  (例如：0022aa03a4b5)

图 7-19 MAC 地址过滤配置

- ◆ MAC 地址：需要进行过滤的无线主机的 MAC 地址。

- ▶ 保存：MAC 地址过滤配置参数生效；
- ▶ 返回：返回上一页，即 *无线配置—>无线 MAC 地址过滤* 页面。

### 7.3.4 自定义 MAC 地址过滤条目

配置 MAC 地址过滤条目的步骤如下：

第一步，进入 *无线配置—>无线 MAC 地址过滤* 页面；

第二步，单击“添加新条目”按钮，在弹出的 *MAC 地址过滤配置* 页面中，输入“MAC 地址”，然后单击“保存”按钮；


第三步，该 MAC 地址过滤条目添加成功后，可以在“MAC 地址过滤信息列表”中查看；

第四步，继续配置其他 MAC 地址过滤条目；

第五步，如果希望允许列表中 MAC 地址对应的无线主机接入本设备，禁止其他无线主机接入，则选中“启用 MAC 地址过滤”，并将“过滤规则”设置为“允许”；反之，若希望禁止列表中 MAC 地址对应的无线主机接入本设备，允许其他无线主机接入，则选中“启用 MAC 地址过滤”，并将“过滤规则”设置为“禁止”；

当配置完 MAC 地址过滤功能后，系统将根据相关配置决定是否允许各个无线主机接入本设备、访问无线网络。

如果希望临时关闭 MAC 地址过滤功能，但保留 MAC 地址过滤条目相关配置，则直接取消“启用 MAC 地址过滤”的选中即可。

 **提示：**如果要删除 MAC 地址过滤条目，则可以按照《章节 7.3.2 MAC 地址过滤信息列表》提供的 3 种方法进行删除操作。

### 7.3.5 MAC 地址过滤配置实例

#### 1. 应用需求

本实例中，要求禁止 MAC 地址为 00b08c0517ed、001f3c47f481 和 001f3c0f07f4 的无线主机访问本设备，允许其他无线主机访问本设备。

#### 2. 配置步骤

第一步，进入 *无线配置—>无线 MAC 地址过滤* 页面。；

第二步，单击“添加新条目”按钮，在弹出的 *MAC 地址过滤配置* 页面中（如下图），在“MAC 地址”中输入 00b08c0517ed，然后单击“保存”按钮。；

MAC地址

00b08c0517ed

(例：0022AA0011DD)

保存返回

图 7-20 MAC 地址过滤配置——实例

第三步，继续配置另外两条 MAC 地址过滤条目（MAC 地址分别为 001f3c47f481 和 001f3c0f07f4）。

第四步，选中“启用 MAC 地址过滤”，“过滤规则”选择为“禁止”。

启用MAC地址过滤☒


过滤规则

☐ 允许 只允许列表中的MAC地址访问本无线网络。

☒ 禁止 只禁止列表中的MAC地址访问本无线网络。

保存重填

图 7-21 MAC 地址过滤全局配置——实例

至此，配置完成，可以在“MAC 地址过滤信息列表”中查看这三个 MAC 过滤条目的相关信息，如下表所示。如果发现配置错误，可以直接单击对应条目的图标，在弹出的 **MAC 地址过滤配置** 页面中进行修改并保存。

MAC地址过滤信息列表

3/50

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

	ID	MAC地址	编辑
<input type="checkbox"/>	1	00:b0:8c:05:17:ed	 
<input type="checkbox"/>	2	00:1f:3c:47:f4:81	 
<input type="checkbox"/>	3	00:1f:3c:0f:07:f4	 

☐ 全选 / 全不选

添加新条目删除所有条目删除

表 7-2 MAC 地址过滤信息列表——实例

## 7.4 无线高级配置

### 7.4.1 无线高级参数

本节主要讲述**无线配置—>无线高级配置—>无线高级参数**的使用。

在本页面可以设置无线高级参数，一般情况下，这些参数保持默认值即可。如果您有特别需求，可以进入本页面进行配置。

RTS 阈值 *	<input type="text" value="2347"/>	字节 (取值范围: 1-2347)
分段阈值 *	<input type="text" value="2346"/>	字节 (取值范围: 256-2346)
Beacon 间隔 *	<input type="text" value="100"/>	毫秒 (取值范围: 20-999)
DTIM 间隔 *	<input type="text" value="1"/>	(取值范围: 1-255)
启用短前导	<input checked="" type="checkbox"/>	
启用 WMM	<input checked="" type="checkbox"/>	

启用 WMM (无线客户端也需启用), 多媒体数据 (如音频、视频) 将被优先发送。

图 7-22 无线高级参数

- ◆ **RTS 阈值:** 当数据包超过这个阈值时, 就会启动 RTS 机制。设备在发送数据帧前, 会先发 RTS (Request to Send, 请求发送) 包到目的站点进行协商; 接收到 RTS 帧后, 无线站点会回应一个 CTS (Clear to Send, 清除发送) 帧来回应路由器, 表示两者之间可以进行无线通信了。一般, 取值范围为 1~2347 字节, 默认值为 2347; RTS 机制用于在无线局域网中避免数据发送冲突。RTS 包的发送频率需要合理设置, 设置 RTS 门限时需要进行权衡。如果将这个参数值设得较小, 则使 RTS 包的发送频率增加, 消耗更多的带宽, 明显影响其它网络数据包的吞吐量。但 RTS 包发送得越频繁, 系统从中断或冲突中恢复得就越快;
- ◆ **分段阈值:** 用于定义无线 MAC 层允许传输的无线数据包的最大传输长度, 当数据帧长度超过此值时, 将自动被分段成多个数据帧, 然后再进行传送。如果分段传输被中断, 只有未成功发送的部分需要重新发送, 分段包的吞吐量一般较低。一般, 取值范围为 256~2346 字节, 默认值为 2346 字节;  
大的分段传输效率较高, 但如果无线网络中有明显的冲突或者使用频率很高, 分段减小可以提高数据传输的可靠性。在大多数场合, 请保持缺省值 2346;
- ◆ **Beacon 间隔:** 设备通过定期广播 Beacon (信标) 帧进行无线网络连接的同步, 本参数用于定义信标帧的发送间隔, 信标帧按照指定的时间间隔周期性发送。一般, 取值范围为 20~999 毫秒, 默认值为 100 毫秒;
- ◆ **DTIM 间隔:** 本参数用于指定交付指示信息 (DTIM, Delivery Traffic Indication Message) 的发送间隔。DTIM 间隔用于决定含 TIM (Traffic Indication Map) 的信标帧多久传送一次。TIM 会对进入休眠状态的站点发出警告, 表示有数据处于待接收状态。DTIM 通常为信标间隔的倍数, 可使用的范围为 1~255, 默认值为 1;
- ◆ **启用短前导:** 启用或禁用短前导 (Short Preamble)。
  - 启用后, 将使用短前导类型; 短前导类型能提供更好的性能。因为短前导的使用可以使开销减少到最小, 因而使网络数据吞吐量最大化;
  - 禁用时, 则使用长前导类型 (Long Preamble), 长前导类型将能够提供更多可行连接和更大范围的连接;
- ◆ **启用 WMM:** 允许启用或禁用 WMM 支持功能。WMM (Wi-Fi Multimedia, 无线

多媒体) 是 802.11e 标准的一个子集。WMM 允许无线流量根据数据类型拥有一个优先级范围。时间敏感的信息, 如视频或音频, 将比普通流量的优先级更高。要正确使用 WMM 功能, 无线客户端也必须支持 WMM:

- ▶ 保存：无线高级配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。

## 7.5 无线主机状态

本节主要讲述**无线配置—>无线主机状态**的使用。

通过“无线主机状态信息列表”，您可以查看当前连接到无线路由器的无线主机的状态信息，包括：无线主机的 **MAC** 地址，接收/发送数据包的个数，接收/发送数据包字节数等等。

此外，通过“无线主机状态信息列表”，您还可以方便地设置 MAC 地址过滤功能。

**过滤：**当复选框未被选中时，您可以选中它，将当前MAC地址添加到MAC地址过滤表中；反之，当复选框已被选中时，您可以将当前MAC地址从过滤表中删除。

**全部过滤：**将当前状态表中所有无线主机的MAC地址添加到MAC地址过滤表中。

无线主机状态信息列表

1/1

1/1

第一页

上一页

下一页

最后一页

前往第

页

搜索

ID	MAC地址	过滤	频道带宽
1	00:1C:BF:6C:AD:36	<input type="checkbox"/>	20M

全部过滤

刷新

表 7-3 无线主机状态信息列表

- ◆ ID: 序号;
- ◆ 频道带宽: 数据信道的理论数据传输率;
- ◆ 过滤: 选中表示当前 MAC 地址已经被添加到“MAC 地址过滤信息列表”中, 未选中表示当前 MAC 地址未设置过滤。该复选框具有可操作性:
  - 当复选框未被选中时, 您可以选中它, 将当前 MAC 地址添加到 MAC 地址过滤表中;
  - 反之, 当复选框已被选中时, 您可以将当前 MAC 地址从过滤表中删除;
- ▶ 全部过滤: 单击“全部过滤”按钮, 可以将当前列表中未启用过滤的所有无线主机 MAC 地址过滤, 并将所有的 MAC 地址添加到“MAC 地址过滤信息列表”中, 该表

在**无线配置—>无线 MAC 地址过滤**页面中查看；

▶ 刷新：单击“刷新”按钮，可以查看最新的无线主机状态和统计信息。

⊕ 提示：

“MAC 地址过滤信息列表”在**无线配置—>无线 MAC 地址过滤**页面中查看。

## 第8章 高级配置

本章主要讲述如何设置设备的 NAT 和 DMZ 配置、IP/MAC 绑定和路由配置等高级属性的相关参数。

### 8.1 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。

#### 8.1.1 NAT 功能介绍

##### 8.1.1.1 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。

##### 8.1.1.2 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。

##### 8.1.1.3 两种 NAT 类型

设备提供两种 NAT 类型：“EasyIP”和“One2One”。

**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。

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。

### 8.1.1.4 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。

 **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。



## 8.1.2 NAT 静态映射


### 8.1.2.1 NAT 静态映射列表

NAT静态映射列表								2/50
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/>	页	搜索 <input type="text"/>
	静态映射名	状态	协议	外部起始端口	IP地址	内部起始端口	端口数量	编辑
<input type="checkbox"/>	admin	禁用	TCP	8081	192.168.1.1	80	1	 
<input type="checkbox"/>	www	启用	TCP	10000	192.168.1.99	80	1	 

☐ 全选 / 全不选 添加新条目 删除所有条目 删除

表 8-1 NAT 静态映射列表

- ▶ 添加 NAT 静态映射：单击“添加新条目”按钮，在跳出的 **NAT 静态映射配置** 页面中，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；
- ▶ 编辑 NAT 静态映射：如果想修改某一个静态 NAT 映射的配置信息，只需单击该条目的“静态映射名”或该条目所对应的“”图标，设备就会跳转到 **NAT 静态映射配置** 页面，对其配置信息进行修改；
- ▶ 删除 NAT 静态映射：共有以下 3 种删除方法。
  - 方法 1：单击某条目对应的  图标，即可删除对应 NAT 静态映射；
  - 方法 2：选中若干 NAT 静态映射，单击右下角的“删除”按钮，即可删除被选中的映射条目；
  - 方法 3：若需要删除全部 NAT 静态映射，则直接单击“删除所有条目”按钮即可。

 **提示：**系统某些功能（**系统管理**—>**远程管理**）会添加名为 admin 的 NAT 静态映射，在本页面无法编辑或删除它们。

### 8.1.2.2 NAT 静态映射配置

静态映射名 *	<input type="text" value="www"/>
启用该配置	<input checked="" type="checkbox"/>
打勾表示启用该NAT静态映射，只有启用该配置，该NAT静态映射才能生效。	
协议	<input type="text" value="TCP"/>
外部起始端口 *	<input type="text" value="10000"/>
IP地址 *	<input type="text" value="192.168.1.99"/>
局域网中作为服务器的计算机的IP地址。	
内部起始端口 *	<input type="text" value="80"/>
端口数量 *	<input type="text" value="1"/>
<div>保存 重填 返回</div>	

图 8-1 NAT 静态映射配置

- ◆ 静态映射名：NAT 静态映射的名称（自定义，不能重复）；
- ◆ 启用该配置：启用或禁用词 NAT 静态映射，打勾表示启用；
- ◆ 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 TCP/UDP；当用户无法确认该协议所使用的类型为 TCP 或 UDP 时，可选择 TCP/UDP；
- ◆ 外部起始端口：外部访问使用的起始端口；

- ◆ 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；
- ▶ 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；
- ▶ 返回：返回到 **高级配置—>NAT 和 DMZ 配置—>NAT 静态映射** 页面。

### 8.1.2.3 自定义 NAT 静态映射

第一步，进入 **高级配置—>NAT 和 DMZ 配置—>静态 NAT 映射** 页面，单击“添加新条目”按钮；

第二步，在 **NAT 静态映射配置** 页面，填写“NAT 静态映射名”，并启用该配置；

第三步，根据需要填写局域网服务器的“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，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；

第七步，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。

### 8.1.2.4 NAT 静态映射配置实例

#### 1. 实例一

局域网计算机 192.168.1.99 开设了 TCP80 端口的服务，但是希望外部通过 10000 端口访问这个服务，具体配置如下图所示：

静态映射名 *	<input type="text" value="www"/>
启用该配置	<input checked="" type="checkbox"/>
打勾表示启用该NAT静态映射，只有启用该配置，该NAT静态映射才能生效。	
协议	<input type="text" value="TCP"/>
外部起始端口 *	<input type="text" value="10000"/>
IP地址 *	<input type="text" value="192.168.1.99"/>
局域网中作为服务器的计算机的IP地址。	
内部起始端口 *	<input type="text" value="80"/>
端口数量 *	<input type="text" value="1"/>
<input type="button" value="保存"/> <input type="button" value="重填"/> <input type="button" value="返回"/>	

图 8-2 NAT 静态映射配置——实例一

## 2. 实例二

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 192.168.1.99 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“example”（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“example”，具体配置如下图所示：

静态映射名 *	<input type="text" value="example"/>
启用该配置	<input checked="" type="checkbox"/>
打勾表示启用该NAT静态映射，只有启用该配置，该NAT静态映射才能生效。	
协议	<input type="text" value="TCP"/>
外部起始端口 *	<input type="text" value="21"/>
IP地址 *	<input type="text" value="192.168.1.99"/>
局域网中作为服务器的计算机的IP地址。	
内部起始端口 *	<input type="text" value="21"/>
端口数量	<input type="text" value="1"/>
<input type="button" value="保存"/> <input type="button" value="重填"/> <input type="button" value="返回"/>	

图 8-3 NAT 静态映射配置——实例二



## 8.1.3 NAT 规则


### 8.1.3.1 NAT 规则列表

NAT规则信息列表						2/8
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页
	搜索	<input type="text"/>				
	规则名	NAT类型	外部IP地址	内部起始IP地址	内部结束IP地址	编辑
<input type="checkbox"/>	example	One2One	218.1.21.3	192.168.1.99	192.168.1.99	 
<input type="checkbox"/>	default	EasyIP	192.168.1.33	0.0.0.0	0.0.0.0	 

☐ 全选 / 全不选

表 8-2 NAT 规则信息列表

- ▶ 添加 NAT 规则: 单击“添加新条目”按钮, 在跳出的 **NAT 规则配置** 页面中, 输入 NAT 规则的配置信息, 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 规则的信息;
- ▶ 编辑 NAT 规则: 如果想修改某一个 NAT 规则的配置信息, 只需单击该条目的“规则名”或该规则所对应的“ ”图标, 设备就会跳转到 **NAT 规则配置** 页面, 对其配置信息进行修改;
- ▶ 删除 NAT 规则: 共有以下 3 种删除方法:
  - 方法 1: 单击某条目对应的  图标, 即可删除对应 NAT 规则;
  - 方法 2: 选中若干 NAT 规则, 单击右下角的“删除”按钮, 即可删除被选中的映射条目;
  - 方法 3: 若需要删除全部 NAT 规则, 则直接单击“删除所有条目”按钮即可。

 **提示:** 配置本类型的 NAT 规则时, 当用户在 **开始菜单**→**配置向导**→**网络参数** 页面或 **网络参数**→**WAN 口配置** 中配置了线路信息, 系统会自动生成一个名为“default”的默认 NAT 规则, 此规则作为统保留 NAT 规则的名称, 不能修改和删除。

### 8.1.3.2 NAT 规则配置

下面分别介绍“EasyIP”和“One2One”这两种类型的 NAT 规则的配置, 如图 8-4、图 8-5 所示。

#### 1. EasyIP

规则名 \* A

NAT类型 EasyIP

内部IP地址映射到同一个外部IP地址。

外部IP地址 200.200.200.140

内部起始IP地址 \* 192.168.1.50

内部结束IP地址 \* 192.168.1.150

保存 重填 返回

图 8-4 NAT 规则配置——EasyIP

- ◆ NAT 规则名：NAT 规则的名称（自定义，不能重复）；
- ◆ NAT 类型：EasyIP、One2One，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；
- ▶ 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；。
- ▶ 返回：返回到 **高级配置—>NAT 和 DMZ 配置—>NAT 规则** 页面。

## 2. One2One

规则名 \* B

NAT类型 One2One

内部IP地址与外部IP地址进行一对一的映射。

外部起始IP地址 200.200.202.140

内部起始IP地址 \* 192.168.1.10

内部结束IP地址 \* 192.168.1.13

保存 重填 返回

图 8-5 NAT 规则配置——One2One

- ◆ “规则名”、“内部起始 IP 地址”、“内部结束 IP 地址”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，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；
- ▶ 返回：返回到 **高级配置—>NAT 和 DMZ 配置—>NAT 规则** 页面。

 **提示：**

1. 最多只能绑定 20 个外部地址；
2. “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 192.168.1.6，“内部结束 IP 地址”设为 192.168.1.8，“外部起始地址”设为 200.200.200.116，则 192.168.1.6、192.168.1.7、192.168.1.8 依次映射成 200.200.200.116、200.200.200.117、200.200.200.118。

### 8.1.3.3 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—>NAT 规则** 页面，单击“添加新条目”按钮；

第三步，进入 **NAT 规则配置页面**，选择“NAT 类型”为“EasyIP”或“One2One”；

第四步，分为两种情况：

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

第五步，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；

第六步，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 0.0.0.0；
3. NAT 规则的匹配顺序按照 NAT 规则列中的默认排列顺序，列表越上方的越先匹配。

### 8.1.3.4 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。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：192.168.1.10/24~192.168.1.100/24）希望以 218.1.21.3/29 作

为 NAT 映射地址通过 WAN 口上网。

配置步骤如下：

第一步，进入 **高级配置—>NAT 和 DMZ 配置—>NAT 规则** 页面，单击“添加新条目”按钮；

第二步，进入 **NAT 规则配置** 页面，在“规则名”中填入 example1；

The screenshot shows the 'NAT Rule Configuration' page. It contains the following fields and values:

- 规则名 \*: example1
- NAT类型: EasyIP (with a dropdown arrow)
- 外部IP地址: 218.1.21.3
- 内部起始IP地址 \*: 192.168.1.10
- 内部结束IP地址 \*: 192.168.1.100

Below the fields are three buttons: 保存 (Save), 重填 (Reset), and 返回 (Back). A note below the NAT type field states: 内部IP地址映射到同一个外部IP地址的不同端口。

图 8-6 NAT 规则配置——实例一

第三步，选择“NAT 类型”为“EasyIP”；

第四步，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 192.168.1.10 和 192.168.1.100；

第五步，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

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：202.1.1.128/29～202.1.1.135/29，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 WAN 口 IP 地址。注意，202.1.1.128/29、202.1.1.135/29 分别为相关子网的子网号和广播地址，不可使用。

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 202.1.1.131/29～202.1.1.134/29 对外提供服务。内部网络的地址是 192.168.1.0/24，4 台服务器的内部地址是 192.168.1.200/24～192.168.1.203/24。

### 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 **网络参数—>WAN 口配置** 页面中配置固定 IP 接入上网默认线路，或直接进入 **开始—>配置向导—>网络参数** 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。

### 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—>NAT 规则** 页面，单击“添加新条目”按

钮；

第二步，进入 *NAT 规则配置* 页面，在“规则名”中填入 example2；

规则名 \* example2

NAT类型 One2One ▼

内部IP地址与外部IP地址进行一对一的映射。

外部起始IP地址 202.1.1.131

内部起始IP地址 \* 192.168.1.200

内部结束IP地址 \* 192.168.1.203

保存 重填 返回

图 8-7 NAT 规则配置——实例二

第三步，选择“NAT 类型”为“One2One”；

第四步，在“外部起始 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 192.168.1.200 和 192.168.1.203；

第五步，单击“保存”按钮，该条 NAT 规则添加成功。

## 8.1.4 DMZ

启动DMZ功能 ☒

启用DMZ功能后，DMZ主机将完全暴露给 Internet，实现双向通讯。

DMZ主机IP地址 \*

保存 重填

图 8-8 NAT 全局配置

- ◆ 启用 DMZ 功能：打开或者关闭 NAT 功能，选中为打开；
- ◆ DMZ 主机 IP 地址：欲用作虚拟服务器（DMZ 主机）的局域网计算机的 IP 地址。
- ▶ 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：被设置为 DMZ 主机的计算机将失去设备的防火墙保护功能。

## 8.2 IP/MAC 绑定

本节主要讲述 **高级配置**—>**IP/MAC 绑定** 的配置方法。

### 8.2.1 IP/MAC 绑定功能介绍

#### 8.2.1.1 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 **防火墙**—>**访问控制策略** 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。

#### 8.2.1.2 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“允许未被 IP/MAC 绑定的主机通过”，就表示允许这些用户连接或者通过设备；如果没有选中“允许未被 IP/MAC 绑定的主机通过”，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其他功能模块处理。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，并继续去匹配其他策略；
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“允许未被 IP/MAC 绑定的主机通过”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“允许未被 IP/MAC 绑定的主机通过”时，则丢弃该数据包。

8.2.2 IP/MAC 绑定全局配置

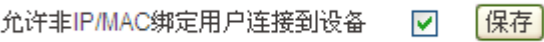


图 8-9 IP/MAC 绑定全局配置

- ◆ 允许非 IP/MAC 绑定用户连接到设备：允许或禁止非 IP/MAC 绑定的用户与设备连接。选中选框表示允许，取消选框表示禁止。
- ▶ 保存：IP/MAC 绑定全局配置参数生效；
- ⚠ 提示：当决定取消“允许非 IP/MAC 绑定用户连接到设备”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。

8.2.3 IP/MAC 绑定信息列表

IP/MAC绑定信息列表					1/50
1/1	第一页	上一页	下一页	最后页	前往 第 <input type="text"/> 页 搜索 <input type="text"/>
	用户名	IP地址	MAC地址	允许	编辑
<input type="checkbox"/>	11	192.168.1.150	00:21:85:9b:43:65	<input type="checkbox"/>	 


☐ 全选 / 全不选

添加新条目

删除所有条目


删除

表 8-3 IP/MAC 绑定信息列表

- ▶ 添加 IP/MAC 绑定条目：单击“添加新条目”按钮，在 *IP/MAC 绑定配置* 页面中，输入 IP/MAC 绑定信息，单击“保存”按钮，生成新的 IP/MAC 绑定条目；
- ▶ 浏览 IP/MAC 绑定条目：在“IP/MAC 绑定信息列表”中可以查看已配置绑定的用户信息，包括用户名、IP 地址、MAC 地址、是否允许等信息；
- ▶ 编辑 IP/MAC 绑定条目：如果想编辑某个 IP/MAC 绑定条目，只需单击该条目的“用户名”或“”按钮，设备就会跳转到 *IP/MAC 绑定配置* 页面，可修改用户名、IP 地址

和 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：共有以下 3 种删除方法。

- 方法 1：单击某条目对应的  图标，即可删除对应 IP/MAC 绑定条目；
- 方法 2：选中若干 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；
- 方法 3：若需要删除全部 IP/MAC 绑定条目，则直接单击“删除所有条目”按钮即可。

#### ⊕ 提示：

当决定取消选中某一 IP/MAC 绑定条目的“允许”选框前，必须确认该 IP 地址或 MAC 与管理计算机不相符，否则将会造成管理计算机无法连接到设备的现象。页面会做相应的提示，如下图所示：

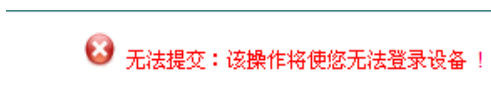


图 8-10 IP/MAC 绑定错误提示

## 8.2.4 IP 和 MAC 绑定配置

用户名 *	<input type="text" value="a"/>
IP地址 *	<input type="text" value="192.168.1.21"/>
MAC地址 *	<input type="text" value="0022cc0022aa"/>

图 8-11 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；
  - ◆ IP 地址：该用户的 IP 地址（windows 平台下“命令行”中使用 `ipconfig /all` 命令获得）；
  - ◆ MAC 地址：该用户的 MAC 地址（windows 平台下“命令行”中使用 `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；

► 返回：返回到**高级配置—>IP/MAC 绑定**页面。

## 8.2.5 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，单击“添加新条目”按钮，进入 **IP/MAC 绑定配置**页面，输入“用户名”（自定义）、“IP 地址”和“MAC 地址”，然后单击“保存”按钮；

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**防火墙—>访问控制策略**中为该用户配置了访问控制策略，这些数据包还将继续去匹配这些策略；

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“允许未被 IP/MAC 绑定的主机通过”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。

## 8.2.6 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。

### 8.2.6.1 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 绑定用户连接到设备”，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 192.168.1.104，MAC 地址为 0021859b4544 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。

IP/MAC绑定信息列表					1/50
1/1	第一页	上一页	下一页	最后页	前往 第 <input type="text"/> 页 搜索 <input type="text"/>
	用户名	IP地址	MAC地址	允许	编辑
<input type="checkbox"/>	A	192.168.1.104	00:21:85:9b:45:44	<input checked="" type="checkbox"/>	 
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					
<input type="checkbox"/>					

☐ 全选 / 全不选 添加新条目 删除所有条目 删除

表 8-4 IP/MAC 绑定信息列表——实例一

### 8.2.6.2 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，有两种方法：

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. 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 绑定用户连接到设备”，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 IP 地址（例如 192.168.1.3）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。

IP/MAC绑定信息列表					1/50
1/1	第一页	上一页	下一页	最后一页	前往 第 <input type="text"/> 页 搜索 <input type="text"/>
	用户名	IP地址	MAC地址	允许	编辑
<input type="checkbox"/>	B	192.168.1.3	99:88:77:66:55:44	<input checked="" type="checkbox"/>	 

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 8-5 IP/MAC 绑定信息列表——实例二

例如，如果要禁止某个 IP 地址为 192.168.1.103，MAC 地址为 0021859b4542 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。

IP/MAC绑定信息列表					1/50
1/1	第一页	上一页	下一页	最后一页	前往 第 <input type="text"/> 页 搜索 <input type="text"/>
	用户名	IP地址	MAC地址	允许	编辑
<input type="checkbox"/>	C	192.168.1.103	00:21:85:9b:45:42	<input type="checkbox"/>	 

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 8-6 IP/MAC 绑定信息列表——实例三

### 8.3 路由配置

本节主要讲述高级配置->路由配置的配置方法。在本页面可以配置静态路由，查看所配置的静态路由信息。

#### 8.3.1 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。

#### 8.3.2 路由配置信息列表

路由配置信息列表

1/253

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

	路由名	状态	目的网络	子网掩码	网关地址	跳数	接口	编辑
<input type="checkbox"/>	route-1	启用	200.200.202.0	255.255.255.0	200.200.202.254	0	WAN	 

☐ 全选 / 全不选


添加新条目

删除所有条目

删除

表 8-7 路由信息列表

- ▶ 添加静态路由条目：单击“添加新条目”按钮，在路由配置页面中，输入静态路由信息，单击“保存”按钮，生成新的静态路由；
- ▶ 浏览静态路由条目：在“静态路由配置信息列表”中可以查看已配置绑定的用户信息，包括路由名、状态、目的网络、子网掩码、网关地址、跳数及接口等信息；
- ▶ 编辑静态路由条目：如果想编辑某个静态路由，只需单击该条目的“路由名”或“编辑”按钮，设备就会跳转到路由配置页面，可修改静态路由的相关信息，再单击“保存”按钮，修改完毕；
- ▶ 删除静态路由条目：共有以下 3 种删除方法。

- 方法 1：单击某条目对应的  图标，即可删除对应静态路由；
- 方法 2：选中若干静态路由，单击右下角的“删除”按钮，即可删除被选中的路由；
- 方法 3：若需要删除全部的静态路由，则直接单击“删除所有条目”按钮即可。

8.3.3 静态路由配置

路由名 \*

route-1

启用该配置

☒

打勾表示启用该路由，只有启用该配置，该路由才能生效。

目的网络 \*

200.200.202.0

子网掩码 \*

255.255.255.0

网关地址 \*

200.200.202.254

跳数 \*

0

接口

WAN

保存

重填

返回

图 8-12 静态路由配置

- ◆ 路由名：静态路由的名称（自定义，不可重复）；
- ◆ 启用该配置：启用该静态路由，选中表示启用，取消选中则表示禁用该路由；
- ◆ 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；
- ◆ 跳数：从源到目的的路径中每一跳被赋以一个跳数值，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；
- ◆ 接口：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；选项包括：
  - WAN：路由器的 WAN 口；
  - LAN：路由器的 LAN 口；
- ▶ 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。
- ▶ 返回：返回到 **高级配置**—>**路由配置** 页面。

⊕ 提示：

配置静态路由时，必须明确下一跳地址，可通过“网关地址”或“接口”设置。若转发接

口是物理接口，则必须设置“网关地址”，但可以 not 设置“接口”，此时，设备将会自动选择一条最优路径；当多条路由的目的网络和跳数相同时，设备会根据越晚建立的越先匹配的原则进行匹配。

### 8.3.4 自定义静态路由

第一步，进入 **高级配置**—>**路由配置** 页面，单击“添加新条目”按钮；

第二步，进入 **路由配置** 页面，输入静态路由的名称；

第三步，输入该条路由指向的目的网段及子网掩码；

第四步，根据需要设置该条路由的跳数；

第五步，根据实际情况，设置网关地址或者绑定的接口

例如，某条路由的目的网段为 192.168.16.0/24，转发接口为物理接口，“网关地址”为 192.168.1.254，则设置“接口”为 LAN，具体配置如下图所示。

路由名 \* router-1

启用该配置 ☒

打勾表示启用该路由，只有启用该配置，该路由才能生效。

目的网络 \* 192.168.16.0

子网掩码 \* 255.255.255.0

网关地址 \* 192.168.1.254

跳数 \* 0

接口 LAN

保存 重填 返回

图 8-13 静态路由配置——实例一

第六步，单击“保存”按钮，该静态路由添加成功。可以在“路由配置信息列表”中看到相应的记录；

第七步，继续配置其他静态路由。

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

## 第9章 用户管理

本章主要讲述如何对设备的用户进行管理配置，包括全局用户的管理和分组管理。

### 9.1 全局管理

本节主要讲述*用户管理*→*全局管理*的配置方法。

使用全局管理策略能在既定的时间段内禁止用户使用 QQ、MSN、BT 以及使用迅雷搜索资源。可以控制用户 QQ、MSN 的使用，可以防止某些用户因为大量下载数据而导致网络阻塞的问题产生，保持网络的畅通。

#### 9.1.1 全局管理配置

**全局策略设置**

禁止QQ ☐ [\[更新策略\]](#)

禁止MSN ☐ [\[更新策略\]](#)

禁止BT ☐ [\[更新策略\]](#)

禁止迅雷搜索 ☐ [\[更新策略\]](#)

**生效时间设置**

日期 ☒ 每天

☐ 星期一 ☐ 星期二 ☐ 星期三 ☐ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期天

时间 ☒ 全天

☐ 从  :  到  :

图 9-1 全局管理

- ◆ 禁止 QQ：允许或禁止该组内的所有用户使用 QQ 聊天，选中表示禁止；
- ◆ 禁止 MSN：允许或禁止该组内的所有用户使用 MSN 聊天，选中表示禁止；
- ◆ 禁止 BT：允许或禁止该组内的所有用户使用 Bitcomet、BitSpirit 等 P2P 软件进行下载，选中表示禁止；
- ◆ 禁止迅雷搜索：允许或禁止该组内的所有用户进行迅雷搜索资源，选中表示禁止；

- ◆ 生效时间设置：带宽限速生效的时间，不设置为所有时间。可以对日期和时间分别进行设置。设备会根据生效时间的日期和时间进行时间的匹配，先对日期进行匹配，若不符合生效日期，则全局配置的内容不会生效，若符合生效日期，则继续匹配时间，时间符合则按照全局配置中的规则进行软件限制；若不符合，则该配置不生效。
  - 日期：设置生效时间的日期。选中“每天”，则表示星期一至星期天每一天都是生效日期；取消选中“每天”，可以对日期分别根据“星期一”、“星期二”、“星期三”、“星期四”、“星期五”、“星期六”、“星期天”的选项进行设置。当选中“星期一”，则表示每个星期的星期一为生效日期。
  - 时间：设置生效时间的时间。若选中“全天”，则表示全天都是生效时间；取消选中“全天”，则可以自定义时间段。当所设置的开始时间大于结束时间时，设备会自动将其分为两段。例如，生效日期为星期一，开始时间设为 23:00，结束时间设为 06:00，则生效时间为星期一的 23:00~23:59 和星期一 00:00~06:00 两段。
- ▶ 更新策略：更新对应程序的策略。单击“更新策略”超链接，此时设备会跳转到更新策略页面，如下图所示，完成策略更新，设备会返回到之前的页面，即用户管理→全局配置页面。

正在更新策略，请稍候...

剩余时间为 8 秒!

图 9-2 更新策略

- ▶ 保存：全局管理配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。

## 9.1.2 全局管理配置实例

某公司使用 HiPER 510W 上网，公司员工禁止在上班时间（周一至周五，早上 9 点到晚上 17 点）使用 QQ，禁止员工使用 BT。

配置步骤如下：

第一步，进入用户管理→全局管理页面；

第二步，选中禁止 QQ 和禁止 BT 两个单选框；

第三步，设置生效时间，将日期设为星期一到星期五，时间设到 9 点到 17 点，以上设置如下图所示：

### 全局策略设置

- 禁止QQ ☒ [\[更新策略\]](#)  
禁止MSN ☐ [\[更新策略\]](#)  
禁止BT ☒ [\[更新策略\]](#)  
禁止迅雷搜索 ☐ [\[更新策略\]](#)

### 生效时间设置

- 日期 ☐ 每天  
☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四 ☒ 星期五 ☐ 星期六 ☐ 星期天  
时间 ☐ 全天  
☒ 从 09 : 00 到 17 : 00

[保存](#) [重填](#)

图 9-3 全局管理——实例

第四步，单击“保存”按钮，配置生效。

## 9.2 组管理

本节主要讲述**用户管理—>组管理**的配置方法。

设备引入了组这个概念，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。

设置组用户时，还可以为该组用户设置组策略，对该组用户进行分时段策略控制，使组用户在不同的时段具有不同的策略控制。组策略包括以下参数：禁止 QQ、禁止 MSN、禁止 BT、禁止迅雷搜索、上下行速率限制等。

9.2.1 组管理信息列表

组管理信息列表										2/5
1/1	第一页	上一页	下一页	最后页	前往	第		页	搜索	
<input type="checkbox"/>	组名	起始IP地址	结束IP地址	限速策略	下载速率限制	上传速率限制	禁止QQ	禁止MSN	禁止BT	禁止迅雷
<input type="checkbox"/>	A	192.168.1.1	192.168.1.20	独享	128k bit/s	128k bit/s	Yes	No	Yes	No
<input type="checkbox"/>	B	192.168.1.19	192.168.1.31	共享	192k bit/s	256k bit/s	Yes	Yes	Yes	Yes
<div><div></div><div></div></div> <div><input type="checkbox"/> 全选 / 全不选</div> <div>添加新条目</div> <div>删除所有条目</div> <div>删除</div>										

表 9-1 组管理信息列表

组管理信息列表

2/5

1/1

第一页

上一页

下一页

最后页

前往

第

页

搜索

上传速率限制	禁止QQ	禁止MSN	禁止BT	禁止迅雷搜索	生效时间
128k bit/s	Yes	No	Yes	No	星期一，星期二，星期三，星期四，星期五；09:00-17:00
256k bit/s	Yes	Yes	Yes	Yes	每天

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 9-2 组管理信息列表（续表 9-1）

组管理信息列表

2/5

1/1

第一页

上一页

下一页

最后页

前往

第

页

搜索

禁止QQ	禁止MSN	禁止BT	禁止迅雷搜索	生效时间	编辑
Yes	No	Yes	No	星期一，星期二，星期三，星期四，星期五；09:00-17:00	
Yes	Yes	Yes	Yes	每天	

☐ 全选 / 全不选


添加新条目

删除所有条目


删除

表 9-3 组管理信息列表（续表 9-12）

- ▶ 添加组管理条目：单击“添加新条目”按钮，在跳出的组管理配置页面中，输入组管理配置信息，单击“保存”按钮，生成新的组管理条目；
- ▶ 浏览组管理条目：在“组管理信息列表”中可以查看已配置的组管理用户信息，包括组名、起始 IP 地址、结束 IP 地址、限速信息、禁止 QQ、禁止 BT、禁止迅雷搜索、生效时间等信息；

▶ 编辑组管理条目：如果想编辑某个组管理条目，只需单击该条目的“组名”或“”按钮，设备就会跳转到**组管理配置**页面，可修改组管理条目的配置信息，再单击“保存”按钮，修改完毕；

▶ 删除组条目：共有以下3种删除方法。

- 方法1：单击某条目对应的  图标，即可删除对应的组管理条目；
- 方法2：选中若干组条目，单击右下角的“删除”按钮，即可删除被选中的条目；
- 方法3：若需要删除全部组管理条目，则直接单击“删除所有条目”按钮即可。

## 9.2.2 组管理配置



The image shows a web-based configuration form for group management. It includes fields for group name, start and end IP addresses, bandwidth limits, and various service restrictions. There are also checkboxes for enabling/disabling services like QQ, MSN, BT, and迅雷搜索. At the bottom, there are buttons for saving, resetting, and returning.

组名 \* A

起始IP地址 \* 192.168.1.1

结束IP地址 \* 192.168.1.20

限速策略 独享

下载速率限制 128 kbit/s <== 128K (0表示不限速)

上传速率限制 128 kbit/s <== 128K (0表示不限速)

禁止QQ ☒ [更新策略]

禁止MSN ☐ [更新策略]

禁止BT ☒ [更新策略]

禁止迅雷搜索 ☐ [更新策略]

**生效时间设置**

日期 ☐ 每天

☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四 ☒ 星期五 ☐ 星期六 ☐ 星期天

时间 ☐ 全天

☒ 从 09 : 00 到 17 : 00

保存 重填 返回

图 9-4 组管理配置

- ◆ 组名：组的名称（自定义，不可重复）；
- ◆ 起始IP地址：该组的起始IP地址；
- ◆ 结束IP地址：该组的结束IP地址；
- ◆ 限速策略：进行速率限制时的策略，分为共享和独享两种；
  - 共享是指组内所有的用户合起来最大能使用的最大带宽；
  - 独享则是指组内所有用户分别都能使用的带宽；

- ◆ 下载速率限制：内网主机的最大下载速率（单位：kbit/s）。其中，选项“不限制”表示在上传方向不启用限速功能，0 表示不限制带宽，下同；
- ◆ 上传速率限制：内网主机的最大上传速率（单位：kbit/s）。下载最大速率和上传最大速率的配置都可以采用两种方式进行配置；
  - 在文本框中直接输入数字；
  - 通过选择下拉框的选项进行配置。
- ◆ 禁止 QQ：允许或禁止该组内的所有用户使用 QQ 聊天，选中表示禁止；
- ◆ 禁止 MSN：允许或禁止该组内的所有用户使用 MSN 聊天，选中表示禁止；
- ◆ 禁止 BT：允许或禁止该组内的所有用户使用 Bitcomet、BitSpirit 等 P2P 软件进行下载，选中表示禁止；
- ◆ 禁止迅雷搜索：允许或禁止该组内的所有用户进行迅雷搜索资源，选中表示禁止；
- ◆ 生效时间设置：组管理配置的生效的时间，不设置为所有时间。可以对日期和时间分别进行设置。设备会根据生效时间的日期和时间进行时间的匹配，先对日期进行匹配，若不符合生效日期，则组管理配置的内容不匹配，若符合生效日期，则继续匹配时间，时间符合则按照组管理配置的规则进行速率及软件限制；若不符合，则不匹配。
  - 日期：设置生效时间的日期。选中“每天”，则表示星期一至星期天每一天都是生效日期；取消选中“每天”，可以对日期分别根据“星期一”、“星期二”、“星期三”、“星期四”、“星期五”、“星期六”、“星期天”的选项进行设置。当选中“星期一”，则表示每个星期的星期一为生效日期。
  - 时间：设置生效时间的时间。若选中“全天”，则表示全天都是生效时间；取消选中“全天”，则可以自定义时间段。当所设置的开始时间大于结束时间时，设备会自动将其分为两段。例如，生效日期为星期一，开始时间设为 23:00，结束时间设为 06:00，则生效时间为星期一的 23:00~23:59 和星期一 00:00~06:00 两段。
- ▶ 更新策略：更新对应程序的策略。单击“更新策略”超链接，对该软件所对应的策略进行更新，具体操作步骤可参见章节 9.1.1。
- ▶ 保存：全局管理配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。
- ▶ 返回：返回到 **用户管理**—>**组管理** 页面。

⊕ 提示：

1. 组管理中的组配置优先级高于全局管理的配置；
2. 设备最多能建立 5 个组，每个组支持 25 个组成成员；
3. 若一个成员同时属于多个组，那么对这个成员生效的是最先建立的组。

## 9.2.3 组管理配置匹配顺序

若某用户的 IP 地址符合多个组管理条目，则根据这些组管理条目的建立时间的来顺序匹配。设备会将这些组管理条目按照其建立时间顺序排列，并根据此顺序进行规则的匹配。即最先建立的组管理条目，会最先匹配，若 IP 地址及生效时间符合该条规则，则按照该组管理配置内容限制。

例如，某公司有以下要求，限制 192.168.1.2~192.168.1.20 地址段的用户，在全天时间内不能使用 QQ 和 MSN；地址为 192.168.1.3 用户不受此限制。

此时就可以先配置组 A，地址为 192.168.1.3，允许 QQ 和 MSN。随后配置组 B，地址段为 192.168.1.2~192.168.1.20，禁止 QQ 和 MSN。

此时由于组 A 先建于组 B 建立，当用户的 IP 地址为 192.168.1.3 时，用户仍然能够使用 QQ 和 MSN 软件，不受组 B 的配置影响。

## 9.2.4 全局管理、组管理和访问控制策略的匹配顺序

若某设备同时配置了全局管理、组管理和访问控制策略。匹配顺序为：访问控制策略>组管理>全局管理；

例如，当某设备配置了全局禁止 QQ 功能，并针对某个 IP 地址段建立了组管理，允许该段地址用户使用 QQ，访问控制策略中又禁止了所有的端口。此时，由于优先匹配访问控制策略，内网用户将都不能上网；而当访问控制策略没有做限制时，则符合组管理配置中 IP 地址的用户可以使用 QQ，非该地址段用户则无法登录 QQ。

## 9.2.5 组管理配置实例

某公司使用无线路由器上网，内网地址为 192.168.1.0/27，公司划分为 3 个区域，分别为管理部，和业务部。管理部 IP 地址段为 192.168.1.2~192.168.1.10；业务部 IP 地址段为 192.168.1.11~192.168.1.30。禁止管理部使用 QQ 和 MSN，其余部门允许；管理部 IP 地址为 192.168.1.2~192.168.1.5 为管理层专用，不作任何使用限制。

**分析：**

建立 3 个组管理条目。

组 A：地址包含管理层地址，不做任何限制；

组 B：地址包含 192.168.1.2~192.168.1.10，禁止 QQ 和 MSN；

组 C：地址包含 192.168.1.11~192.168.1.30，允许所有功能。

**配置步骤如下：**

第一步，进入**用户管理—>组管理**页面；

第二步，单击“添加新条目”，进入**组管理配置**页面，建立组 A，配置信息如下所示：

组名 *	<input type="text" value="A"/>		
起始IP地址 *	<input type="text" value="192.168.1.2"/>		
结束IP地址 *	<input type="text" value="192.168.1.5"/>		
限速策略	<input type="button" value="独享"/>		
下载速率限制	<input type="text" value="0"/> kbit/s	<==	<input type="button" value="不限速"/> (0表示不限速)
上传速率限制	<input type="text" value="0"/> kbit/s	<==	<input type="button" value="不限速"/> (0表示不限速)
禁止QQ	<input type="checkbox"/> <a href="#">[更新策略]</a>		
禁止MSN	<input type="checkbox"/> <a href="#">[更新策略]</a>		
禁止BT	<input type="checkbox"/> <a href="#">[更新策略]</a>		
禁止迅雷搜索	<input type="checkbox"/> <a href="#">[更新策略]</a>		
<b>生效时间设置</b>			
日期	<input checked="" type="checkbox"/> 每天 <input type="checkbox"/> 星期一 <input type="checkbox"/> 星期二 <input type="checkbox"/> 星期三 <input type="checkbox"/> 星期四 <input type="checkbox"/> 星期五 <input type="checkbox"/> 星期六 <input type="checkbox"/> 星期天		
时间	<input checked="" type="radio"/> 全天 <input type="radio"/> 从 <input type="text" value="00"/> : <input type="text" value="00"/> 到 <input type="text" value="00"/> : <input type="text" value="00"/>		
<input type="button" value="保存"/> <input type="button" value="重填"/> <input type="button" value="返回"/>			

图 9-5 组管理配置——实例一之组 A

第三步，建立组 B，配置信息如下所示：

组名 *	<input type="text" value="B"/>		
起始IP地址 *	<input type="text" value="192.168.1.2"/>		
结束IP地址 *	<input type="text" value="192.168.1.10"/>		
限速策略	<input type="button" value="共享"/> ▼		
下载速率限制	<input type="text" value="0"/> kbit/s	<==	<input type="button" value="不限速"/> ▼ (0表示不限速)
上传速率限制	<input type="text" value="0"/> kbit/s	<==	<input type="button" value="不限速"/> ▼ (0表示不限速)
禁止QQ	<input checked="" type="checkbox"/>	<a href="#">更新策略</a>	
禁止MSN	<input checked="" type="checkbox"/>	<a href="#">更新策略</a>	
禁止BT	<input type="checkbox"/>	<a href="#">更新策略</a>	
禁止迅雷搜索	<input type="checkbox"/>	<a href="#">更新策略</a>	
<b>生效时间设置</b>			
日期	<input checked="" type="checkbox"/> 每天		
	<input type="checkbox"/> 星期一 <input type="checkbox"/> 星期二 <input type="checkbox"/> 星期三 <input type="checkbox"/> 星期四 <input type="checkbox"/> 星期五 <input type="checkbox"/> 星期六 <input type="checkbox"/> 星期天		
时间	<input checked="" type="radio"/> 全天		
	<input type="radio"/> 从 <input type="text" value="00"/> : <input type="text" value="00"/> 到 <input type="text" value="00"/> : <input type="text" value="00"/>		
<input type="button" value="保存"/> <input type="button" value="重填"/> <input type="button" value="返回"/>			

图 9-6 组管理配置——实例一之组 B

第四步，建立组 C，配置信息如下所示：

组名 \*

起始IP地址 \*

结束IP地址 \*

限速策略 

独享

下载速率限制  kbit/s <== 

不限速

 (0表示不限速)

上传速率限制  kbit/s <== 

不限速

 (0表示不限速)

禁止QQ ☐ [更新策略](#)

禁止MSN ☐ [更新策略](#)

禁止BT ☐ [更新策略](#)

禁止迅雷搜索 ☐ [更新策略](#)

生效时间设置

日期 ☒ 每天

☐ 星期一 ☐ 星期二 ☐ 星期三 ☐ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期天

时间 ☒ 全天

☐ 从  :  到  :

保存重填返回

图 9-7 组管理配置——实例一之组 C

第五步，完成所有组的建立，查看组管理信息列表，如下表所示：

组管理信息列表3/5

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	限速策略	下载速率限制	上传速率限制	禁止Q
<input type="checkbox"/>	A	192.168.1.2	192.168.1.5	独享	0 bit/s	0 bit/s	No
<input type="checkbox"/>	B	192.168.1.2	192.168.1.10	共享	0 bit/s	0 bit/s	Yes
<input type="checkbox"/>	C	192.168.1.11	192.168.1.30	独享	0 bit/s	0 bit/s	No

☐ 全选 / 全不选

添加新条目删除所有条目删除

表 9-4 组管理信息列表

组管理信息列表

3/5

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

率限制	上传速率限制	禁止QQ	禁止MSN	禁止BT	禁止迅雷搜索	生效时间	编辑
t/s	0 bit/s	No	No	No	No	每天	 
t/s	0 bit/s	Yes	Yes	No	No	每天	 
t/s	0 bit/s	No	No	No	No	每天	 

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 9-5 组管理信息列表（续表 9-4）

## 第10章 防火墙

本章主要讲述如何为设备配置防火墙，包括访问控制策略及域名过滤。

### 10.1 访问控制策略

本节主要讲述**防火墙—>访问控制策略**的功能及配置方法。

本功能由“访问控制策略配置”和“访问控制信息列表”两大页面组成。灵活地运用访问控制功能，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间段的 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访问控制策略。例如对于学校用户，可通过配置访问控制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。

#### 10.1.1 访问控制策略简介

##### 10.1.1.1 访问控制工作原理

在设备中配置访问控制策略，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访问控制策略，设备将转发接收到的所有合法的数据包。如果配置了访问控制策略，当数据包到达设备后，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，并按照策略的优先级从高至低搜索策略表，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。

##### 10.1.1.2 过滤类型

可以通过设置“过滤类型”指定访问控制策略的过滤类型，设备提供三种过滤类型：IP 过滤、URL 过滤以及关键字过滤。这三种类型的访问控制策略，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、动作和生效时间等。

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）、动作和生效时间等。

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）和生效时间等。

10.1.1.3 访问控制策略的动作

访问控制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访问控制策略相匹配时，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。

值得注意的是，关键字过滤由于其特殊的应用性，并不提供“动作”的选择，而是默认“禁止”。

10.1.2 访问控制策略列表

访问控制策略列表

2/100

1/1 第一页 上一页 下一页 最后页 前往 第 页 搜索

	策略名	状态	地址组	优先级	动作	生效时间段	过滤类型
<input type="checkbox"/>	FTP	启用	0.0.0.0--0.0.0.0	0	禁止	每天	IP地址过
<input type="checkbox"/>	HTTP	启用	192.168.1.200--192.168.1.202	5	禁止	每天	IP地址过

☐ 全选 / 全不选

添加新条目 删除所有条目 删除

表 10-1 访问控制策略列表

访问控制策略列表							2/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
过滤类型	过滤内容	协议	目的起始端口	目的结束端口	目的起始地址	目的结束地址	
IP地址过滤		TCP	21	21	0.0.0.0	0.0.0.0	
IP地址过滤		TCP	80	80	0.0.0.0	0.0.0.0	

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-2 访问控制策略列表（续表 10-1）

访问控制策略列表							2/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
端口	目的结束端口	目的起始地址	目的结束地址	源起始端口	源结束端口	编辑	
	21	0.0.0.0	0.0.0.0	1	65535		
	80	0.0.0.0	0.0.0.0	1	65535		

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-3 访问控制策略列表（续表 10-2）

- ▶ 添加访问控制策略：单击“添加新条目”按钮，在跳出的*访问控制策略配置*页面中，输入策略配置信息，单击“保存”按钮，生成新的访问控制策略；
- ▶ 浏览访问控制策略：在“访问控制策略列表”中可以查看已配置的访问控制策略，包括策略名、状态、地址组、优先级、动作、过滤类型、过滤内容、协议、目的起始端口、目的结束端口、目的起始地址、目的结束地址、源起始端口、源结束端口等信息；
- ▶ 编辑访问控制策略：如果想编辑某个访问控制策略，只需单击该策略的“策略名”或“”按钮，设备就会跳转到*访问控制策略配置*页面，可修改访问控制策略的配置信息，再单击“保存”按钮，修改完毕；
- ▶ 删除访问控制策略：共有以下 3 种删除方法。
  - 方法 1：单击某条目对应的 图标，即可删除对应的访问控制策略；
  - 方法 2：选中若干访问控制策略，单击右下角的“删除”按钮，即可删除被选中的策略
  - 方法 3：若需要删除全部访问控制策略，则直接单击“删除所有条目”按钮即可。

### 10.1.3 访问控制策略配置

访问控制策略是对通过设备的数据包进行控制，进入 **访问控制策略配置** 页面，配置所需要的防火墙策略，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，访问控制策略配置中各参数的涵义，以及注意事项。

#### 10.1.3.1 访问控制策略配置—IP 过滤

策略名\* test

启用该策略 ☒

打勾启用该策略，只有启用该策略，该策略才能生效。

IP地址段\* 192.168.1.50 到\* 192.168.1.100

策略控制的内网用户 IP 地址段。

优先级\* 10

优先级序号越小，配置的生效优先级越高。

动作 允许

过滤类型 IP过滤

协议 17 (UDP)

常用服务 53 (dns)

目的起始端口\* 53 目的结束端口\* 53

目的起始地址 0.0.0.0 目的结束地址 0.0.0.0

源起始端口 1 源结束端口 65535

**生效时间设置**

日期 ☐ 每天

☒ 星期一 ☒ 星期二 ☒ 星期三 ☒ 星期四 ☒ 星期五 ☐ 星期六 ☐ 星期天

时间 ☐ 全天

☒ 从 09:00 到 17:00

保存 重填 返回

图 10-1 配置访问控制策略——IP 过滤

- ◆ 策略名：自定义访问控制策略的名称；
- ◆ 启用该策略：启用该访问控制策略，选中表示启用，取消选中则表示禁用该策略；
- ◆ IP 地址段：该访问控制策略控制的局域网用户，即源 IP 地址范围。默认的 IP 地址段 0.0.0.0 到 0.0.0.0 表示局域网内的所有用户。

- ◆ 优先级：该访问控制策略的优先级，取值范围为 0~100，优先级的数字越小，则越先被匹配，优先级不能重复；
- ◆ 动作：该访问控制策略的执行动作，选项为“允许”或“禁止”；
  - 允许：允许与该访问控制策略匹配的数据包通过，即设备将转发该数据包；
  - 禁止：禁止与该访问控制策略匹配的数据包通过，即设备将丢弃该数据包；
- ◆ 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“IP 过滤”；
- ◆ 协议：该访问控制策略的协议类型。供选择的协议如下：1（ICMP）、6（TCP）、17（UDP）、51（AH）、all（所有）。其中，“all（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：该访问控制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：该访问控制策略的目的起始 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：该访问控制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；
- ◆ 生效时间设置：访问控制策略的生效的时间，不设置为所有时间。可以对日期和时间分别进行设置。设备会根据生效时间的日期和时间进行时间的匹配，先对日期进行匹配，若不符合生效日期，则不匹配该条访问控制策略，若符合生效日期，则继续匹配时间，时间符合则按照访问控制策略配置的内容进行操作；若不符合，则不匹配。
  - 日期：设置生效时间的日期。选中“每天”，则表示星期一至星期天每一天都是生效日期；取消选中“每天”，可以对日期分别根据“星期一”、“星期二”、“星期三”、“星期四”、“星期五”、“星期六”、“星期天”的选项进行设置。当选中“星期一”，则表示每个星期的星期一为生效日期。
  - 时间：设置生效时间的时间。若选中“全天”，则表示全天都是生效时间；取消选中“全天”，则可以自定义时间段。当所设置的开始时间大于结束时间时，设备会自动将其分为两段。例如，生效日期为星期一，开始时间设为 23:00，结束时间设为 06:00，则生效时间为星期一的 23:00~23:59 和星期一 00:00~06:00 两段；
- ▶ 保存：访问控制策略配置参数生效；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 返回：返回到 **防火墙—>访问控制策略** 页面。

### 10.1.3.2 访问控制策略配置——URL 过滤

策略名\*

启用该策略 ☒

打勾启用该策略，只有启用该策略，该策略才能生效。

IP地址段\*  到\*

策略控制的内网用户 IP 地址段。

优先级\*

优先级序号越小，配置的生效优先级越高。

动作

过滤类型

过滤内容\*

**生效时间设置**

日期 ☒ 每天

☐ 星期一 ☐ 星期二 ☐ 星期三 ☐ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期天

时间 ☒ 全天

☐ 从  :  到  :

图 10-2 访问控制策略配置——URL 过滤

“策略名”、“IP 地址段”、“优先级”、“动作”、“生效时间”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：该访问控制策略欲过滤的 URL 地址。

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](http://www.sina.com.cn)，那么以 [www.sina.com.cn](http://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](http://www.sina.com.cn/index.jsp)，但是 [tech.sina.com.cn](http://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/](http://www.utt.com.cn/bbs/)，则以 [www.utt.com.cn/bbs/](http://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](http://sina.com)，那么所有出现 [sina.com](http://sina.com) 和 [sina.com.cn](http://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](http://tech.sina.com.cn) 开头的网页将被匹配。

- ▶ 保存：访问控制策略配置参数生效；
- ▶ 重填：恢复到修改前的配置参数。
- ▶ 返回：返回到**防火墙**→**访问控制策略**页面。

 **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://；
2. URL 过滤不能控制用户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 过滤类型的访问控制策略来禁止或允许 FTP 连接。

### 10.1.3.3 访问控制策略配置——关键字过滤

策略名\*

启用该策略 ☒

打勾表示启用该策略，只有启用该策略，该策略才能生效。

IP地址段\*  到\*

策略控制的内网用户IP地址段。

优先级\*

优先级序号越小，配置的生效优先级越高。

动作

过滤类型

过滤内容\*

**生效时间设置**

日期 ☒ 每天

☐ 星期一 ☐ 星期二 ☐ 星期三 ☐ 星期四 ☐ 星期五 ☐ 星期六 ☐ 星期天

时间 ☒ 全天

☐ 从  :  到  :

图 10-3 访问控制策略配置——关键字过滤

“策略名”、“IP 地址段”、“优先级”、“动作”、“生效时间”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：该访问控制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；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：访问控制策略配置参数生效；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 返回：返回到 **防火墙**→**访问控制策略** 页面。

 **提示：**

1. 对于过滤类型为“关键字”的访问控制策略，“动作”只有“禁止”这个选项；
2. 关键字为英文时，区分大小写；
3. 优先级默认为 50，其数值越小优先级越高。

### 10.1.4 访问控制策略配置实例

#### 10.1.4.1 访问控制策略配置实例一

**1. 限制内网某段 IP 只允许某些上网业务**

例如，要求配置只允许 IP 地址为 192.168.1.10~192.168.1.20 的用户使用 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，允许该地址段的 DNS；
- 自定义策略 2，允许该段地址的 WEB；
- 自定义策略 3，禁止该段地址的所有业务；

其中策略 1 和策略 2 的优先级都应该高于策略 3；

需要注意的是，（策略 3）在禁止所有服务时，也会禁止 DNS 服务，为使网络访问正常，应该配置一个优先级高于策略 3 的策略，以保证网络的正常运行。

访问控制策略列表							3/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
	策略名	状态	地址组	优先级	动作	生效时间段	过滤类型
<input type="checkbox"/>	策略1	启用	192.168.1.10~192.168.1.20	5	允许	每天	IP地址过滤
<input type="checkbox"/>	策略2	启用	192.168.1.10~192.168.1.20	10	允许	每天	IP地址过滤
<input type="checkbox"/>	策略3	启用	192.168.1.10~192.168.1.20	15	禁止	每天	IP地址过滤

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-4 访问控制信息列表——实例一

访问控制策略列表							3/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
过滤类型	过滤内容	协议	目的起始端口	目的结束端口	目的起始地址	目的结束地址	
IP地址过滤		UDP	53	53	0.0.0.0	0.0.0.0	
IP地址过滤		TCP	80	80	0.0.0.0	0.0.0.0	
IP地址过滤		all	0	0	0.0.0.0	0.0.0.0	
<input type="checkbox"/> 全选 / 全不选							<input type="button" value="添加新条目"/> <input type="button" value="删除所有条目"/> <input type="button" value="删除"/>

表 10-5 访问控制信息列表——实例一（续表 10-4）

访问控制策略列表							3/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
	目的结束端口	目的起始地址	目的结束地址	源起始端口	源结束端口	编辑	
	53	0.0.0.0	0.0.0.0	1	65535		
	80	0.0.0.0	0.0.0.0	1	65535		
	0	0.0.0.0	0.0.0.0	0	0		
<input type="checkbox"/> 全选 / 全不选							<input type="button" value="添加新条目"/> <input type="button" value="删除所有条目"/> <input type="button" value="删除"/>

表 10-6 访问控制信息列表-实例一（续表 10-5）

2. 限制某段 IP 只禁止某些上网业务。

例如，要求：只禁止 IP 地址为 192.168.1.80~192.168.1.100 的用户访问网站 <http://www.bbc.com>（IP 地址为 220.250.64.23）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。

配置策略 1，禁止 192.168.1.80~192.168.1.100 段用户访问 <http://www.bbc.com>；

配置策略 2，禁止 192.168.1.80~192.168.1.100 段用户访问 <http://www.cnn.com>。

访问控制策略列表								2/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>	
	策略名	状态	地址组	优先级	动作	生效时间段	过滤类型	
<input type="checkbox"/>	1	启用	192.168.1.80--192.168.1.100	10	禁止	每天	URL过滤	
<input type="checkbox"/>	2	启用	192.168.1.80--192.168.1.100	11	禁止	每天	URL过滤	
<input type="checkbox"/> 全选 / 全不选								<input type="button" value="添加新条目"/> <input type="button" value="删除所有条目"/> <input type="button" value="删除"/>

表 10-7 访问控制信息列表——实例一（2）

访问控制策略列表							2/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/>	页 搜索 <input type="text"/>
过滤内容	协议	目的起始端口	目的结束端口	目的起始地址	目的结束地址	源地址	
www.bbc.com							
www.cnn.com							

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-8 访问控制信息列表——实例一（2）（续表 10-7）

3. 限制某段 IP 的某些上网业务在不同时间段有不同的权限

例如，要求：时间段工作时间（周一至周五，9:00~17:00）内只允许 IP 地址为 192.168.1.150~192.168.1.200 的用户访问 WEB 业务，其余时间禁止所有业务。

要配置的策略是：

自定义策略 1，允许该地址段用户在工作时间使用 DNS 业务；

自定义策略 2：允许该地址段用户在工作时间内使用 WEB 业务；

自定义策略 3：其余时间段禁止使用所有业务；

其中策略 1 和策略 2 的优先级都应该高于策略 3。

访问控制策略列表							3/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/>	页 搜索 <input type="text"/>
	策略名	状态	地址组	优先级	动作	生效时间段	
<input type="checkbox"/>	1	启用	192.168.1.150--192.168.1.200	19	允许	星期一，星期二，星期三，星期四，星期五	
<input type="checkbox"/>	2	启用	192.168.1.150--192.168.1.200	20	允许	星期一，星期二，星期三，星期四，星期五	
<input type="checkbox"/>	3	启用	192.168.1.150--192.168.1.200	21	禁止	每天	

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-9 访问控制信息列表——实例一（3）

访问控制策略列表

3/100

1/1

第一页

上一页

下一页

最后页

前往

第

页

搜索

生效时间段	过滤类型	过滤内容	协议	目的起始端口
星期一，星期二，星期三，星期四，星期五；09:00-17:00	IP地址过滤		UDP	53
星期一，星期二，星期三，星期四，星期五；09:00-17:00	IP地址过滤		TCP	80
每天	IP地址过滤		all	0

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-10 访问控制信息列表——实例一（3）（续表 10-9）

访问控制策略列表

3/100

1/1

第一页

上一页

下一页

最后页

前往

第

页

搜索

滤内容	协议	目的起始端口	目的结束端口	目的起始地址	目的结束地址	源起始端口	源结束端口	编辑
	UDP	53	53	0.0.0.0	0.0.0.0	1	65535	
	TCP	80	80	0.0.0.0	0.0.0.0	1	65535	
	all	0	0	0.0.0.0	0.0.0.0	0	0	

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-11 访问控制信息列表——实例一（3）（续表 10-10）

10.1.4.2 访问控制策略配置实例二

如果某段 IP 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访问控制策略。

例如，要求：允许某 IP 地址段（配置同上一节实例一）的 WEB 业务，禁止该地址段的其他所有上网业务。特别地，允许该组 IP 地址为 192.168.1.16 的用户在时间段工作时间的所有上网业务。

- 要配置的策略是：
- 自定义策略 1，允许该段地址的 DNS 业务；
  - 自定义策略 2，允许 IP 地址为 192.168.1.16 的用户在工作时间内的所有业务；
  - 自定义策略 3，允许该段地址的 WEB；
  - 自定义策略 4，禁止该段地址的所有其他服务。

访问控制策略列表

4/100

1/1 第一页 上一页 下一页 最后一页 前往 第 页 搜索

	策略名	状态	地址组	优先级	动作	生效时间段
<input type="checkbox"/>	1	启用	192.168.1.10--192.168.1.120	5	允许	每天
<input type="checkbox"/>	2	启用	192.168.1.16--192.168.1.16	10	允许	星期一，星期二，星期三，星期四，星期五
<input type="checkbox"/>	3	启用	192.168.1.10--192.168.1.120	15	允许	每天
<input type="checkbox"/>	4	启用	192.168.1.10--192.168.1.120	20	禁止	每天

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 10-12 访问控制策略信息列表——实例二

访问控制策略列表					4/100
1/1	第一页	上一页	下一页	最后页	前往 第 <input type="text"/> 页 搜索 <input type="text"/>
生效时间段		过滤类型	过滤内容	协议	目的起始端口
每天		IP地址过滤		UDP	53
星期一，星期二，星期三，星期四，星期五；09:00-17:00		IP地址过滤		all	0
每天		IP地址过滤		TCP	80
每天		IP地址过滤		all	0
<div><div></div><div></div></div> <div><input type="checkbox"/> 全选 / 全不选</div> <div>添加新条目</div> <div>删除所有条目</div> <div>删除</div>					

表 10-13 访问控制策略信息列表——实例二（续表 10-12）

访问控制策略列表									4/100
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/>	页	搜索 <input type="text"/>	
内容	协议	目的起始端口	目的结束端口	目的起始地址	目的结束地址	源起始端口	源结束端口	编辑	
	UDP	53	53	0.0.0.0	0.0.0.0	1	65535		
	all	0	0	0.0.0.0	0.0.0.0	0	0		
	TCP	80	80	0.0.0.0	0.0.0.0	1	65535		
	all	0	0	0.0.0.0	0.0.0.0	0	0		
<div><div></div><div></div></div> <div><input type="checkbox"/> 全选 / 全不选</div> <div>添加新条目</div> <div>删除所有条目</div> <div>删除</div>									

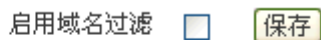
表 10-14 访问控制策略信息列表——实例二（续表 10-13）

## 10.2 域名过滤

本节主要讲述**防火墙→域名过滤**的配置及使用方法。

### 10.2.1 域名过滤全局配置

必须启用域名过滤功能后，配置的域名过滤才生效。



打勾表示启用域名过滤功能，只有启用域名过滤，配置的域名过滤才生效。

图 10-4 域名过滤全局配置

- ◆ 启用域名过滤：打勾表示启用，启用域名过滤功能后，所配置的域名过滤才生效；
- ▶ 保存：域名过滤全局配置参数生效；

### 10.2.2 域名过滤配置

通过在本页面进行简单的配置，可以实现禁止内网用户对某些指定域名的访问。下面将介绍如何配置域名过滤。

域名名称

添加新条目

域名列表

sina

删除

全部删除

图 10-5 域名过滤配置

- ◆ 域名名称：自定义禁止内网用户访问的域名，不可重复；
- ◆ 域名列表：显示用户添加的域名名称，禁止内网所有用户访问这些域名；
- ▶ 添加新条目：输入域名名称后，单击“添加”按钮，即可将输入的域名添加到“域名列表”。

表”中，可添加 100 个域名；

- ▶ 删除：在“域名列表”中选中一条或多条域名，单击“删除”按钮，即可删除选中的域名；
- ▶ 全部删除：单击“全部删除”按钮，即可将“域名列表”中的域名全部删除。

 **提示：**

1. 设备中支持设置 100 个域名过滤；
2. 域名过滤功能是全字匹配的，当内网用户在浏览器里输入的域名与“域名列表”中显示的域名全字匹配时，将无法访问此域名对应的网页。
3. 可以在域名名称中输入通配符“\*”来实现对多个域名的过滤，例如在域名列表中输入域名名称“www.163.\*”，内网用户将不能访问以“www.163.”开头的网页。

# 第11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、配置管理、软件升级等等。

## 11.1 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以及查看已经配置好的管理员信息。

### 11.1.1 管理员配置信息列表

管理员配置信息列表

2/6

1/1	第一页	上一页	下一页	最后一页	前往	第		页	搜索	
<input type="checkbox"/>		用户名		编辑						
<input type="checkbox"/>		admin								
<input type="checkbox"/>		zsd								

☐ 全选 / 全不选

添加新条目

删除所有条目

删除

表 11-1 管理员配置信息列表

- ◆ 用户名：已经配置好的管理员名称；
  - ◆ 编辑：对选定的管理员做名称和密码修改，可通过或点击对应的用户名来进入编辑页面；
  - ▶ 添加新条目：新建系统管理员账户和密码；
  - ▶ 删除所有条目：删除所有的管理员账户信息，但该操作无法删除默认的系统管理员；
  - ▶ 删除：删除已经选定的系统管理员信息。
- ⊕ 提示：
- 对于系统默认管理账户只能编辑不能删除！

### 11.1.2 创建管理员

如下图所示。在本页面，您可以修改系统管理员的登录用户名和密码。

为安全起见，强烈建议修改初始的管理员用户名及密码，并谨慎保管管理员的用户名及密码。修改后，您必需使用新的用户名和密码登录设备。

用户名 \*

密码 \*


确认密码 \*

**注意：**强烈建议修改初始的管理员密码，并谨慎保管用户名及密码。

图 11-1 管理员配置

- ◆ 用户名：系统管理员的用户名，大小写敏感。
- ◆ 密码：该管理员的登录密码，大小写敏感；
- ◆ 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。
- ▶ 保存：管理员配置参数生效；
- ▶ 重填：恢复到修改前的配置参数；
- ▶ 返回：返回到管理员配置信息列表。

### 11.1.3 删除管理员

- ◆ 删除管理员账户时共有下面三种方法：
  - 选中要删除的管理员账户，单击表 11-1 中的“删除”按钮；
  - 单击表 11-1 中的“删除所有条目”，使用该功能选项时会删除除了设备默认的管理员之外的任何账户；
  - 单击表 11-1 编辑栏中的  也可删除相应的管理员账户。

⊕ 提示：

所有的删除操作均不对系统默认管理员用户账户生效，对于系统默认管理员账户只能编辑不能删除。

## 11.2 语言选择

本节主要讲述系统管理—>语言选择的配置，如下图所示：

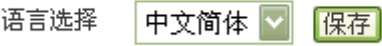


图 11-2 语言选择

- ◆ 语言选择：Web 配置管理设备时的界面语言；
- ▶ 保存：保存当前配置。

## 11.3 时钟管理

本节主要讲述系统管理—>时钟管理的配置，如下图所示。

为了保证设备各种涉及到时间的功能正常工作，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，一般建议使用“网络时间同步”功能来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 11-3 时钟管理

- ◆ 当前系统时间：显示设备当前的日期和时间信息（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：使用网络时间同步功能，设置了正确的 ntp 服务器后，当设备连接到 Internet 之后，就会自动和所设置 ntp 服务器同步时间。系统缺省预设两个 ntp 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 ntp 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。

⊕ 提示：

设备的时钟建议设置为网络时间同步，只有系统的时间配置正确，如防火墙等和时间有关系的配置才会正常生效！

## 11.4 配置管理

本节主要讲述**系统管理**→**配置管理**的配置方法。在本页面，您可以保存当前配置文件到本地，导入新配置文件到设备，恢复设备出厂配置等。

### 11.4.1 保存当前配置

保存当前配置到本地

图 11-4 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。

### 11.4.2 导入配置

导入配置  
导入前恢复出厂配置 ☐  
请选择配置文件

图 11-5 导入配置

- ◆ 导入前恢复到出厂值：选中或不选中，缺省为不选中；  
如果选中，则表示在单击“导入”按钮后，系统将首先执行恢复出厂配置的操作，再执行导入配置的操作；  
如果不选中，则表示在单击“导入”按钮后，系统将直接执行导入配置的操作；
- ◆ 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；
- 导入：首先在“请选择配置文件”中选择欲导入的配置文件，再单击“导入”按钮，就可以将该配置文件导入到设备中。

⊕ 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。

### 11.4.3 恢复出厂配置

恢复设备出厂配置

恢复

**注意：**恢复出厂配置后，所有的配置都删除。建议先备份当前配置。执行本操作之后，需重启设备才能生效

图 11-6 恢复出厂配置

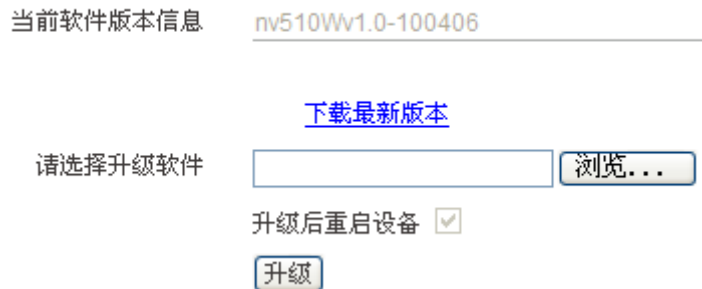
► 恢复：将设备的配置恢复到出厂时的设置值。

⊕ 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，并将系统恢复到出厂状态。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和密码均为：admin，默认 LAN 口 IP 地址/子网掩码为：192.168.1.1/ 255.255.255.0。

## 11.5 软件升级

本节主要讲述**系统管理**→**软件升级**的配置方法。在本页面，您可以查看当前运行软件信息，并能从艾泰科技官方网站下载最新软件，升级设备的软件。



The screenshot shows a software upgrade interface. At the top, it displays '当前软件版本信息' (Current software version information) as 'nv510Wv1.0-100406'. Below this is a blue link '下载最新版本' (Download the latest version). The main section is titled '请选择升级软件' (Please select software to upgrade) and contains a text input field, a '浏览...' (Browse...) button, a checkbox for '升级后重启设备' (Restart device after upgrade) which is checked, and a '升级' (Upgrade) button.

图 11-7 软件升级

- ◆ 当前版本信息：显示设备当前使用的软件版本信息；
- ◆ 下载最新版本：链接到艾泰科技官方网站下载最新版本的软件；
- ◆ 升级：升级设备的软件。

### 第一步 下载最新软件

单击“下载最新版本”超链接，到上海艾泰科技有线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：设备将在软件升级成功后自动重启，重启后新软件才能生效。

### 第三步 更新设备的软件

单击“升级”按钮，更新设备的软件。单击“升级”后，系统会弹出提示信息提示设备将重启，如下图所示，单击“确定”升级并重启，单击“取消”，则取消此次升级。

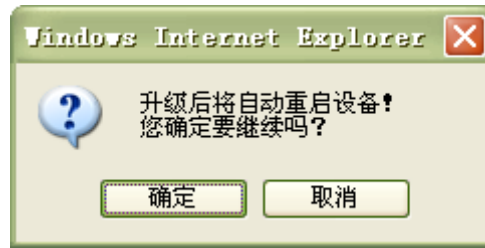


图 11-8 软件升级重启提示

⊕ 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。
4. 升级完成后软件会自动重启生效，无须人工干预。

## 11.6 远程管理

本节主要讲述**系统管理**→**远程管理**的配置方法，在本节中为方便网络维护，您可在**系统管理**→**远程管理**菜单下配置设备的远程管理功能，如图 11-9 所示。

启动HTTP ☐

路由器将允许外部通过WEB进行管理。通过管理时以“IP 地址：端口”的方式访问。

外部端口 \*

图 11-9 远程管理

- ◆ 启用 HTTP：路由器将允许外部通过 WEB 进行远程管理，访问时以“IP 地址：端口”的方式进行；
- ◆ 外部端口：以“IP 地址：端口”方式对设备进行远程管理时客户端输入的端口，如图 11-9 中的外部端口 8081，这里用户可根据实际需要适当添加；
- ▶ 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：

配置远程管理方便了网络的维护，但也存在一定的安全风险。因此为了您的网络安全，一般情况下不建议启动设备的远程管理功能。

# 第12章 系统状态

在系统状态中，您可以方便地查看设备的有线和无线状态，有线和无线流量统计信息，系统软件版本、系统时间、以及历史记录等系统信息。

## 12.1 运行状态

本节主要讲述系统状态—>运行状态的使用，主要包括有线状态和无线状态两大部分。

运行模式：

有线网关模式

有线状态：

WAN口状态			
连接类型	固定IP接入	连接状态	已连接
IP地址	200.200.202.140	子网掩码	255.255.255.0
网关地址	200.200.202.254	MAC地址	00:0C:43:30:52:66
主DNS服务器	210.22.7.3	备DNS服务器	
LAN口状态			
IP地址	192.168.1.1	子网掩码	255.255.255.0
MAC地址	00:0C:43:30:52:77		

无线状态：

连接状态	启用	AP工作模式	AP Mode
SSID	UTT	无线模式	11b/g/n混合
信道	6	MAC地址	C8:3A:35:00:57:E0

刷新

图 12-1 运行状态

- ◆ 运行模式：当前设备运行的模式，如图中设备运行在有线网关模式；
- ◆ 有线状态：显示设备当前是否正常进行有线连接，以及有线接口的 IP 地址、子网掩码和 MAC 地址等信息；

- ◆ 无线状态：显示设备当前是否启用无线功能，以及 SSID、工作频段、AP 工作模式、无线模式、IP 地址、子网掩码和 MAC 地址等信息；
- ▶ 刷新：单击“刷新”按钮，可查看最新的运行状态信息；

## 12.2 流量统计

本节主要讲述**系统状态—>流量统计**的使用，主要包括有线流量统计和无线流量统计两大部分。



图 12-2 流量统计

- ◆ 有线流量：统计并显示设备发送/接收的有线数据包的字节数和数据包个数；
- ◆ 无线流量：统计并显示设备发送/接收的无线数据包的字节数和数据包个数；
- ▶ 清除：单击“清除”按钮，可以清除全部流量统计信息，配合“刷新”按钮，可查看清除时刻至今这段时间内的流量统计信息；
- ▶ 刷新：单击“刷新”按钮，可以查看最新的流量统计信息。

### 12.3 系统信息

本节主要讲述**系统状态**→**系统信息**的使用，主要包括系统软件版本，系统当前时间，系统运行时间，以及历史记录等信息，通过系统信息网络管理员能及时了解网络发生的或潜在的问题，进而有利于网络性能的提高与增强网络安全。



图 12-3 系统信息

- ◆ 系统当前时间：显示设备当前的日期和时间信息（单位：年:月:日，时:分:秒）；
- ◆ 系统运行时间：显示设备本次启动至查看时刻的时间；
- ◆ 软件版本：显示设备的软件版本号；

◆ 历史记录：系统历史记录中，记录了系统启动、无线功能开启等信息；

▶ 刷新：单击“刷新”按钮，可查看最新的系统信息。

⊕ 提示：

图 12-3 中的内存的使用率不同，显示的颜色不同：

- 使用率隶属[0 ， 50%)时，是绿色；
- 使用率隶属在[50% ， 70% )时，是橙色；
- 使用率隶属在[70% ， 100]时，是红色。

# 第13章 客户服务

在客户服务页面，您可以快捷地链接到艾泰科技公司官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目，方便您更快的了解艾泰科技服务体系，享受艾泰科技提供的贴心服务。

艾泰科技是中国领先的中小型网络解决方案提供商和服务商。成立于2000年，总部及研发中心位于上海市漕河泾开发区松江高科技园，在全国设有12个分支机构，是国家重点扶持的高新技术企业和软件企业。艾泰科技产品已广泛应用于企业、网吧、酒店、学校、连锁机构、宽带社区等众多行业，业绩稳健成长。针对中小型网络用户的特点，艾泰科技坚持以服务为中心的战略，坚持“简单+专业=成长”的市场理念，产品和服务一体化，帮助用户建设井然有序的网路。

艾泰科技全国客户服务热线：4006-120-780



图 13-1 客户服务

如图 13-1，单击图中各个“了解更多”超链接，即可分别链接到艾泰科技公司官方网站对应栏目：

- **UTTCare**——链接到艾泰科技官方网站的客户服务页面，提供全面的客户服务和技术支持；
- **产品讨论**——链接到艾泰科技官方网站讨论区，参与产品的讨论；
- **知识库**——链接到艾泰科技官方网站的知识库，查找相关技术资料；
- **预约服务**——链接到艾泰科技官方网站预约服务页面，提前预约某一个工作时段的服务。

## 附录A 配置局域网中的计算机

本章讲述如何在 Windows XP 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”→“控制面板”；
2. 双击“网络连接”图标，右键单击“本机连接”，选择属性。在“本地连接 属性”中“此连接使用下列项目”中查看是否已安装 TCP/IP 协议，如图 A-1 所示，如果出现了“Internet 协议（TCP/IP）”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 TCP/IP 协议，首先安装 TCP/IP 协议，在“本地连接 属性”中选择“Internet 协议（TCP/IP）”，单击“安装（R）”按钮，进行 TCP/IP 协议的安装。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”→“控制面板”；

2. 双击“网络连接”图标，右键单击“本机连接”，选择属性，进入“本地连接 属性”窗口，如图 A-1 所示，在“此连接使用下列项目”选择“Internet 协议 (TCP/IP)”选项，再单击“属性”按钮；
3. 进入“Internet 协议 TCP/IP 属性”窗口，如图 A-2 所示，在常规选项卡中选择“使用下面的 IP 地址”，然后在“IP 地址”中填入：192.168.1.X (X 在 2 至 254 之间)，在“子网掩码”中填入 255.255.255.0，在“网关地址”中填入 192.168.1.1；
4. 选择“使用下面的 DNS 服务器地址”选项，如图 A-2 所示，在“首选 DNS 服务器”中输入 ISP 所提供的 DNS 服务器的 IP 地址（可向 ISP 询问），“备用 DNS 服务器”可选填，当首选 DNS 无法连接时，设备会自动使用备用 DNS 服务器。单击“确定”按钮，TCP/IP 属性配置成功。

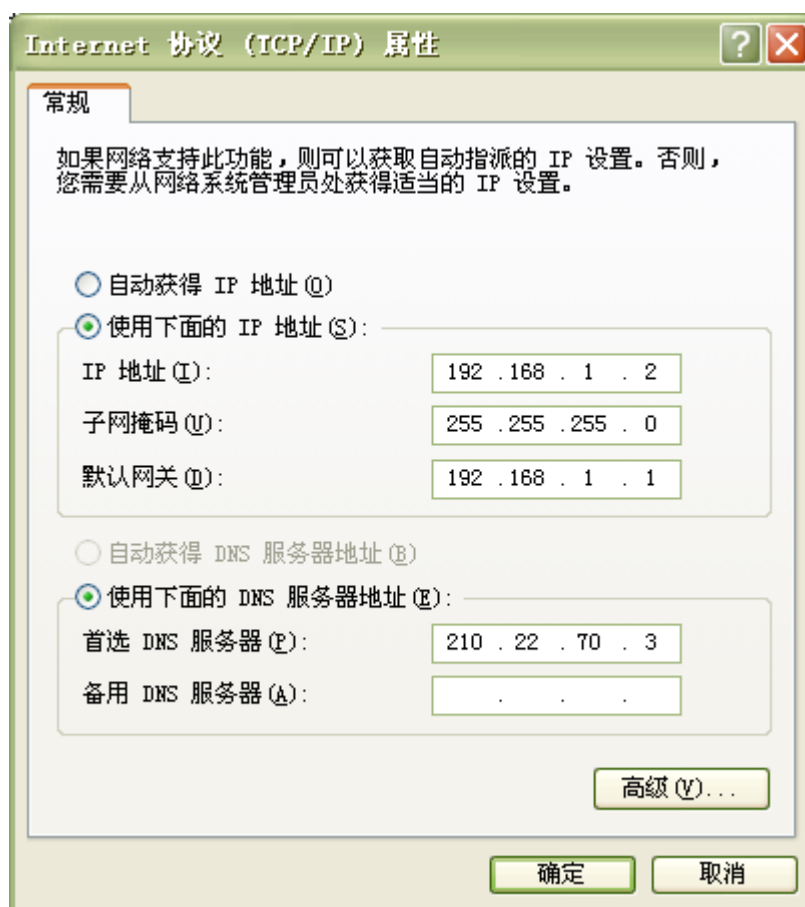


图 A-2 TCP/IP 属性 IP 地址配置窗口

## 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 **网络参数—>DHCP 服务器** 中激活 DHCP Server 功能（章节 5.3.1）；
2. 单击“开始”→“控制面板”；
3. 双击“网络连接”图标，右键单击“本机连接”，选择属性，进入“本地连接 属性”窗口，如图 A-1 所示，在“此连接使用下列项目”选择“Internet 协议 (TCP/IP)”选项，再单击“属性”按钮；
4. 进入“Internet 协议 TCP/IP 属性”窗口，如图 A-3 所示，在常规选项卡中选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”；

5. 以上配置完成后，单击“确定”按钮，配置 TCP/IP 属性完成。

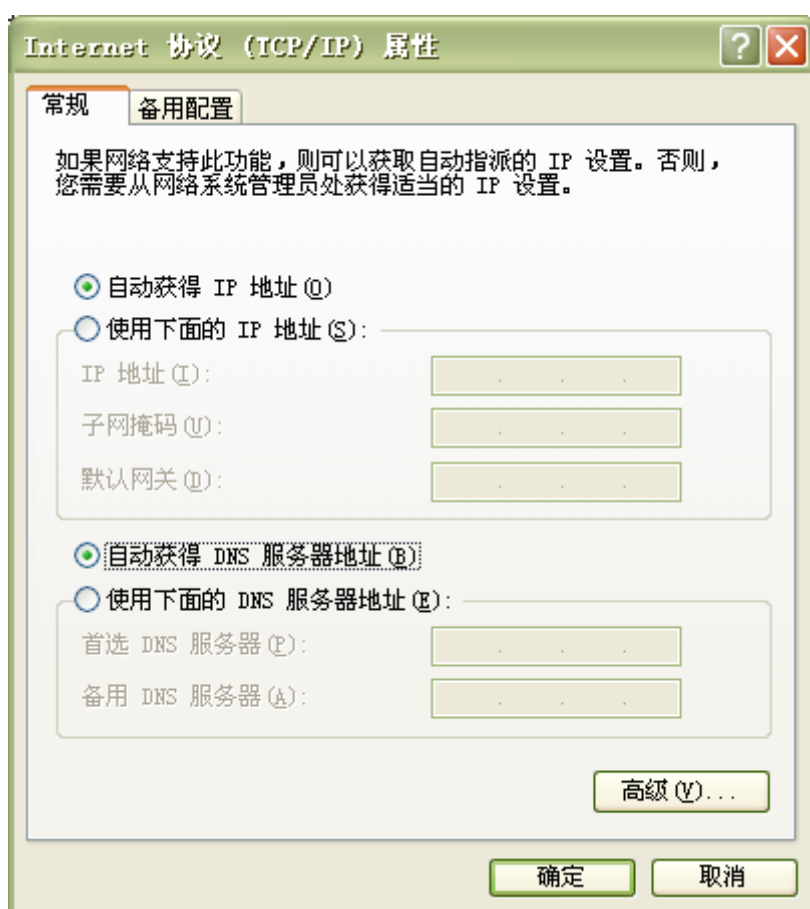


图 A-3 TCP/IP 属性 IP 地址配置窗口

## 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**开始**→**配置向导**→**网络参数**或**网络参数**→**WAN 口配置**中，配置 PPPoE 上网线路的相关参数；
- 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**网络参数**→**WAN 口配置**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**网络参数**→**WAN 口配置**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							1/1
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
PPPoE接入	已连接 0小时1分22秒	10.0.0.195	255.255.255.255	0.0.0.0	392		
<div> <input type="button" value="拨号"/> <input type="button" value="挂断"/> <input type="button" value="刷新"/> </div>							

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							1/1
1/1	第一页	上一页	下一页	最后一页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
PPPoE接入	已连接 0小时1分22秒	10.0.0.195	255.255.255.255	0.0.0.0	392	224	
<div> <input type="button" value="拨号"/> <input type="button" value="挂断"/> <input type="button" value="刷新"/> </div>							

表 B-2 线路连接信息列表——查看 PPPoE 拨号线路信息（续表 B-1）

接入方式	PPPoE接入
用户名*	ad51753515
密码*	●●●●●●
密码验证方式	Either
拨号类型	自动拨号
空闲时间*	0 秒
MTU*	1492 字节 (取值范围：1-1492)

图 B-1 PPPoE 拨号配置


- 8) 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**开始—>配置向导—>网络参数或网络参数—>WAN 口配置**中，配置固定 IP 接入线路的相关参数；
- 4) 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**开始—>配置向导—>网络参数或网络参数—>WAN 口配置**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**网络参数—>WAN 口配置**中，在“MAC 地址克隆”中输入原始的 MAC 地址，单击“保存”按钮。

- 4) 在**网络参数—>WAN 口配置**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-3，表 B-4），比如“连接状态”（正常连接时显示为“已连接”，并显示连接时间）、ISP 分配的“IP 地址”、上行速率和下行速率等信息。

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
连接类型	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
动态IP接入	已连接 0小时0分25秒	192.168.1.98	255.255.255.0		5480	182568	
<div><div></div><div></div></div>							<div>更新 释放 刷新</div>


表 B-3 线路连接信息列表——查看动态 IP 接入线路信息

线路连接信息列表							1/1
1/1	第一页	上一页	下一页	最后页	前往	第 <input type="text"/> 页	搜索 <input type="text"/>
	连接状态	IP地址	子网掩码	网关地址	上行速率(bits)	下行速率(bits)	
\	已连接 0小时0分25秒	192.168.1.98	255.255.255.0		5480	182568	
<div><div></div><div></div></div>							<div>更新 释放 刷新</div>

表 B-4 线路连接信息列表——查看动态 IP 接入线路信息（续表 B-3）

5) 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。

情况一：知道管理员密码

当用户知道管理员密码时，可以通过 WEB 界面来恢复出厂配置。

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，可以通过 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。

## 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	Enhanced 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
rtnet	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	
nnrp	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

图 2-1	前面板 .....	12
图 2-2	后面板示意图 .....	13
图 3-1	WEB 登录页面 .....	18
图 3-2	WEB 首页 .....	18
图 3-3	配置向导——首页 .....	19
图 3-4	欢迎页面 .....	20
图 3-5	运行模式 .....	20
图 3-6	网络配置——固定 IP 接入 .....	21
图 3-7	网络配置——动态 IP 接入 .....	22
图 3-8	网络配置——PPPOE 接入 .....	22
图 3-9	网络参数——3G 客户端 .....	23
图 3-10	安全模式——无安全机制 .....	24
图 3-11	安全模式——WEP .....	24
图 3-12	安全模式——WPA-PSK/WAP2-PSK .....	25
图 3-13	配置向导——无线参数 .....	26
图 4-1	运行状态 .....	29
图 4-2	接口流量 .....	30
图 4-3	流量统计 .....	31
图 4-4	重启设备 .....	31
图 5-1	运行模式 .....	32
图 6-1	网络配置——固定 IP 接入 .....	37
图 6-2	网络配置——动态 IP 接入 .....	37
图 6-3	网络配置——PPPoE 接入 .....	38
图 6-4	网络配置——3G 接入 .....	39
图 6-5	MAC 地址克隆 .....	40
图 6-6	LAN 口配置 .....	40
图 6-7	DHCP 服务设置 .....	41
图 6-8	静态 DHCP 配置 .....	43
图 6-9	DHCP 服务设置——实例 .....	46
图 6-10	静态 DHCP 配置 1——实例 .....	47
图 6-11	静态 DHCP 配置 2——实例 .....	47
图 6-12	申请 DDNS 帐号 .....	48
图 6-13	服务商——无 .....	48
图 6-14	服务商——3322.org .....	49
图 6-15	服务商——iplink.com.cn .....	49
图 6-16	配置 UPnP .....	51
图 6-17	UPnP NAT 映射列表 .....	51
图 7-1	基本设置——AP Mode .....	53

图 7-2	APClient Mode .....	54
图 7-3	Repeater Mode .....	56
图 7-4	WEP .....	56
图 7-5	密钥配置提示 .....	57
图 7-6	TKIP .....	57
图 7-7	AES .....	57
图 7-8	Bridge Mode .....	58
图 7-9	Lazy Mode .....	59
图 7-10	拓扑图 .....	60
图 7-11	A 的配置 .....	60
图 7-12	B 的配置 .....	61
图 7-13	验证 AB 间连通性 .....	61
图 7-14	无线安全设置——无安全机制 .....	62
图 7-15	无线安全设置——WEP .....	63
图 7-16	无线安全设置——WPA/WPA2 .....	64
图 7-17	无线安全设置——WPA-PSK/WPA2-PSK .....	65
图 7-18	MAC 地址过滤全局配置 .....	66
图 7-19	MAC 地址过滤配置 .....	67
图 7-20	MAC 地址过滤配置——实例 .....	69
图 7-21	MAC 地址过滤全局配置——实例 .....	69
图 7-22	无线高级参数 .....	70
图 8-1	NAT 静态映射配置 .....	75
图 8-2	NAT 静态映射配置——实例一 .....	77
图 8-3	NAT 静态映射配置——实例二 .....	77
图 8-4	NAT 规则配置——EasyIP .....	79
图 8-5	NAT 规则配置——One2One .....	79
图 8-6	NAT 规则配置——实例一 .....	81
图 8-7	NAT 规则配置——实例二 .....	82
图 8-8	NAT 全局配置 .....	82
图 8-9	IP/MAC 绑定全局配置 .....	84
图 8-10	IP/MAC 绑定错误提示 .....	85
图 8-11	IP/MAC 地址绑定配置 .....	85
图 8-12	静态路由配置 .....	90
图 8-13	静态路由配置——实例一 .....	91
图 9-1	全局管理 .....	92
图 9-2	更新策略 .....	93
图 9-3	全局管理——实例 .....	94
图 9-4	组管理配置 .....	96
图 9-5	组管理配置——实例一之组 A .....	99
图 9-6	组管理配置——实例一之组 B .....	100
图 9-7	组管理配置——实例一之组 C .....	101
图 10-1	配置访问控制策略——IP 过滤 .....	106
图 10-2	访问控制策略配置——URL 过滤 .....	108
图 10-3	访问控制策略配置——关键字过滤 .....	109

图 10-4	域名过滤全局配置 .....	115
图 10-5	域名过滤配置 .....	115
图 11-1	管理员配置.....	118
图 11-2	语言选择 .....	119
图 11-3	时钟管理 .....	119
图 11-4	保存配置 .....	121
图 11-5	导入配置 .....	121
图 11-6	恢复出厂配置.....	122
图 11-7	软件升级 .....	123
图 11-8	软件升级重启提示.....	124
图 11-9	远程管理 .....	125
图 12-1	运行状态 .....	126
图 12-2	流量统计 .....	127
图 12-3	系统信息 .....	128
图 13-1	客户服务 .....	130

## 附录 F 表索引

表 0-1	常见按钮功能 .....	2
表 0-2	MAC 地址过滤信息列表 .....	3
表 0-3	列表基本功能 .....	4
表 0-4	设备出厂配置 .....	5
表 2-1	前面板指示灯说明 .....	13
表 2-2	后面板端口说明 .....	14
表 2-3	后面板主要部件用途 .....	14
表 6-1	线路连接信息列表 .....	33
表 6-2	线路连接信息列表（续表 6-1） .....	33
表 6-3	PPPoE 拨号线路连接状态描述 .....	34
表 6-4	固定 IP 接入线路连接状态描述 .....	34
表 6-5	动态 IP 接入线路连接状态描述 .....	34
表 6-6	3G 接入线路连接状态描述 .....	35
表 6-7	线路连接信息列表——PPPoE 拨号接入 .....	36
表 6-8	线路连接信息列表——动态 IP 接入 .....	36
表 6-9	线路连接信息列表——3G 接入 .....	36
表 6-10	静态 DHCP 信息列表 .....	43
表 6-11	DHCP 客户端信息列表 .....	44
表 6-12	静态 DHCP 信息列表——实例 .....	47
表 6-13	DDNS 状态 .....	49
表 7-1	MAC 地址过滤信息列表 .....	67
表 7-2	MAC 地址过滤信息列表——实例 .....	69
表 7-3	无线主机状态信息列表 .....	71
表 8-1	NAT 静态映射列表 .....	75
表 8-2	NAT 规则信息列表 .....	78
表 8-3	IP/MAC 绑定信息列表 .....	84
表 8-4	IP/MAC 绑定信息列表——实例一 .....	87
表 8-5	IP/MAC 绑定信息列表——实例二 .....	88
表 8-6	IP/MAC 绑定信息列表——实例三 .....	88
表 8-7	路由信息列表 .....	89
表 9-1	组管理信息列表 .....	95
表 9-2	组管理信息列表（续表 9-1） .....	95
表 9-3	组管理信息列表（续表 9-12） .....	95
表 9-4	组管理信息列表 .....	101
表 9-5	组管理信息列表（续表 9-4） .....	102
表 10-1	访问控制策略列表 .....	104
表 10-2	访问控制策略列表（续表 10-1） .....	105
表 10-3	访问控制策略列表（续表 10-2） .....	105

表 10-4	访问控制信息列表——实例一.....	110
表 10-5	访问控制信息列表——实例一（续表 10-4） .....	111
表 10-6	访问控制信息列表-实例一（续表 10-5） .....	111
表 10-7	访问控制信息列表——实例一（2） .....	111
表 10-8	访问控制信息列表——实例一（2）（续表 10-7） .....	112
表 10-9	访问控制信息列表——实例一（3） .....	112
表 10-10	访问控制信息列表——实例一（3）（续表 10-9） .....	112
表 10-11	访问控制信息列表——实例一（3）（续表 10-10） .....	113
表 10-12	访问控制策略信息列表——实例二.....	113
表 10-13	访问控制策略信息列表——实例二（续表 10-12） .....	114
表 10-14	访问控制策略信息列表——实例二（续表 10-13） .....	114
表 11-1	管理员配置信息列表.....	117