



# Vigor 2910 系列

## 双 WAN 口企业防火墙路由器

### 用户手册

版本: 2.1

日期: 2006/8/15

© 2006 版权所有，翻版必究

此出版物所包含信息受版权保护。未经版权所有人书面许可，任何人不得对其进行拷贝、传播、转录、摘抄、存储到检索系统或转译成其它语言。交货以及其他详细资料的范围若有变化，恕不预先通知。

Microsoft 为微软公司注册商标。

Windows 视窗系列，包括 Windows 95, 98, Me, NT, 2000, XP 以及其 Explorer 均属微软公司商标。

Apple 以及 Mac OS 均属苹果计算机公司的注册商标。

其他产品则为各自生产厂商之商标或注册商标。

## 1

序言 .....	1
1.1 设定按键说明 .....	1
1.2 LED 指示灯和接口 .....	1
1.2.1 对于Vigor2910 .....	2
1.2.2 对于Vigor2910G .....	3
1.2.2 对于Vigor2910G .....	3
1.2.3 对于Vigor2910i .....	5
1.2.4 对于Vigor2910V .....	7
1.2.5 对于Vigor2910VG .....	9
1.2.6 对于Vigor2910VGi .....	11
1.3 硬件安装 .....	13

## 2

配置基本设定 .....	15
2.1 修改密码 .....	15
2.2 快速开始向导 .....	16
2.2.1 PPPoE .....	18
2.2.2 PPTP .....	20
2.2.3 静态IP .....	21
2.2.4 DHCP .....	22
2.3 在线状态 .....	23
2.4 状态栏 .....	26

## 3

高级设定 .....	27
3.1 WAN .....	27
3.1.1 IP网络基础 .....	27
3.1.2 基本设定 .....	27
3.1.3 Internet接入 .....	29
3.1.4 负载均衡策略 .....	36
3.2 LAN .....	39
3.2.1 局域网基础 .....	39
3.2.2 基本设定 .....	41
3.2.3 静态路由 .....	43
3.2.4 绑定IP到MAC .....	45
3.3 NAT（网络地址转换） .....	46
3.3.1 设定虚拟服务器 .....	47
3.3.2 DMZ主机设定 .....	49

3.3.3 开放端口设定 .....	52
3.4 对象与组 .....	54
3.4.1 IP对象 .....	54
3.4.2 IP 组 .....	57
3.4.3 服务类型对象 .....	58
3.4.4 服务类型组 .....	59
3.4.5 CSM 设定档 .....	60
3.5 防火墙 .....	62
3.5.1 基本防火墙设定 .....	62
3.5.2 基本设定 .....	65
3.5.3 过滤器设定 .....	67
3.5.4 拒绝服务 (DoS) 攻击防御功能设定 .....	72
3.5.5 URL内容过滤 .....	75
3.5.6 Web内容过滤 .....	77
3.6 带宽管理 .....	78
3.6.1 限制会话 .....	78
3.6.2 限制带宽 .....	79
3.6.3 服务质量 (QoS) .....	80
3.7 应用程序 .....	86
3.7.1 动态DNS .....	86
3.7.2 计划任务 .....	88
3.7.3 远程认证拨入用户服务 .....	89
3.7.4 UPnP .....	91
3.7.5 局域网唤醒 .....	92
3.8 VPN和远程拨入设置 .....	94
3.8.1 远程接入控制功能设定 .....	95
3.8.2 PPP一般设定 .....	96
3.8.3 IPSec一般设定 .....	97
3.8.4 端点认证 .....	98
3.8.5 为远程接入用户设定帐号 .....	101
3.8.6 LAN to LAN .....	104
3.8.7 连接管理 .....	113
3.9 证书管理 .....	114
3.9.1 本地证书 .....	114
3.9.2 可信CA证书 .....	116
3.9.3 证书备份 .....	117
3.10 VoIP .....	118
3.10.1 电话簿 .....	119
3.10.2 SIP 帐号 .....	122
3.10.3 电话设定 .....	125
3.10.4 状态 .....	135
3.11 ISDN .....	136
3.11.1 基本设定 .....	136
3.11.2 拨到单一ISP .....	137
3.11.3 拨到双ISP .....	138
3.11.4 虚拟TA .....	138

3.11.5 拨号控制 .....	142
3.12 无线局域网 .....	144
3.12.1 基本概念 .....	144
3.12.2 基本设定 .....	147
3.12.3 安全性 .....	149
3.12.4 接入控制设定 .....	151
3.12.5 WDS .....	151
3.12.6 AP扫描 .....	154
3.12.7 接入者列表 .....	155
3.12.8 接入者速率控制 .....	156
3.13 VLAN .....	156
3.13.1 有线VLAN .....	156
3.13.2 无线VLAN .....	157
3.13.3 VLAN 交叉设定 .....	161
3.13.4 无线速率控制 .....	162
3.14 系统维护 .....	164
3.14.1 系统状态 .....	164
3.14.2 系统管理员密码 .....	165
3.14.3 备份/还原设定档 .....	165
3.14.4 系统日志 (Syslog) /邮件警示 .....	167
3.14.5 时间和日期 .....	169
3.14.6 管理设定 .....	170
3.14.7 重启系统 .....	171
3.14.8 固件升级 .....	172
3.15 诊断 .....	173
3.15.1 拨号触发 .....	173
3.15.2 查看路由表 .....	173
3.15.3 查看ARP缓存表 .....	174
3.15.4 查看DHCP分配的IP地址 .....	174
3.15.5 NAT 会话表 .....	175
3.15.6 无线VLAN在线客户端 .....	176
3.15.7 PING诊断 .....	177
3.15.8 流量监控 .....	177
3.15.9 流量图 .....	179
3.15.10 路由追踪 .....	179

## 4

范例与应用 .....	181
4.1 在总公司与分公司之间建立一条LAN-to-LAN 连接 .....	181
4.2 在企业网络和远程用户之间建立一个远程拨入连接 .....	189
4.3 QoS设置范例 .....	193
4.4 局域网架设——基于NAT功能 .....	196
4.5 VoIP功能通话方案 .....	198
4.5.1 通过SIP服务器 .....	198
4.5.2 点到点通话 .....	200

4.6 升级路由器固件..... 201

4.7 从Windows CA服务器上申请一个证书 ..... 203

4.8 申请一个证书然后设置为Windows CA服务器上的可信证书..... 207

5

**故障排查..... 209**

5.1 检查路由器硬件状态是否正常 ..... 209

5.2 检查您电脑的网络连接设置是否正常 ..... 209

5.3 在您电脑Ping路由器..... 212

5.4 检查ISP设定是否正确 ..... 214

5.5 如果必要将路由器恢复至默认出厂设置 ..... 215

5.6 联系代理商..... 216



# 1 序言

Vigor2910 系列路由器是一款提供有双WAN口（第二WAN口是可配置）的路由器，可以保障Internet连接更加的稳定。其无线局域网功能传输速度可达 108Mbps（SuperG™）。新型的面向对象防火墙提供给您更加灵活，更加安全网络环境。此外，通过VoIP功能，您可大大减少与外地，甚至国外的通讯费用。

## 1.1 设定按键说明

一些出现在 web 界面上的主要按键按如下定义：

确定	保存并应用当前设定。
取消	取消当前设定并恢复到之前保存的设定。
清除	废除当前设定并允许用户重新输入。
添加	为指定项目添加新的设定。
编辑	编辑被选项目的设定。
删除	删除被选项目的相关设定。

**注释：**对于 web 界面上面的其它按键定义，请参考第四章的详细解释。

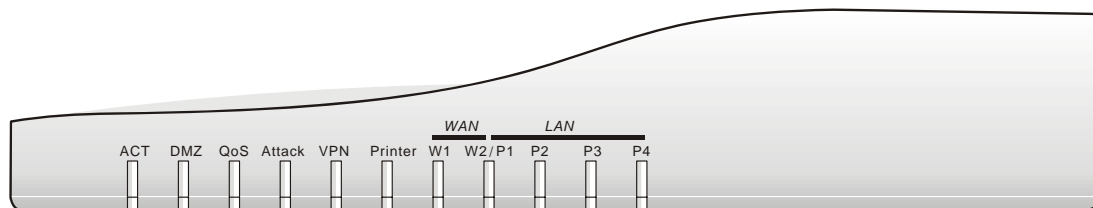
## 1.2 LED 指示灯和接口

在使用 Vigor 路由器之前，请先熟悉 LED 指示灯和接口。

路由器的 LED 指示灯和接口显示会略有些不同，以下章节将会分别对它们进行说明。

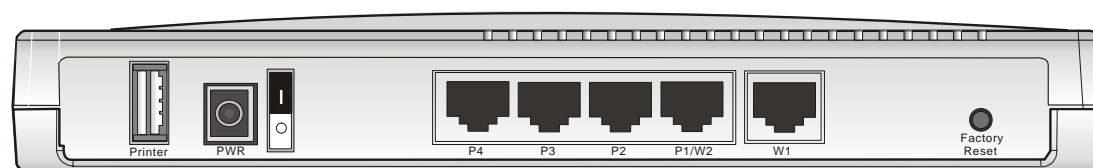
## 1.2.1 对于 Vigor2910

### LED 说明



LED	状态	说明
ACT（活动）	闪烁	路由器已开机并正常运行
	暗	路由器已关机
DMZ	亮	DMZ 主机已指定
QoS	亮	QoS 功能已启用
	暗	QoS 功能已关闭
Attack	亮	DoS 防御功能已启用
	闪烁	检测到攻击
VPN	亮	VPN 隧道已建立
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

### 接口说明

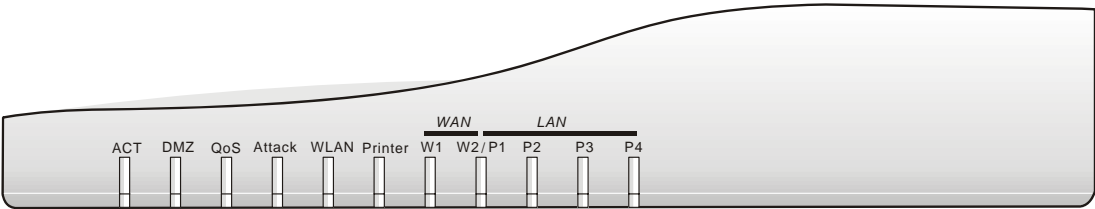


接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口
ON/OFF	电源开关
LAN P4 – P1	连接本地网络的接口
W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口
Factory Reset	还原出厂默认设置 用法：当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 Factory Reset 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，松开此按键，路由器将会还原成出厂默认值



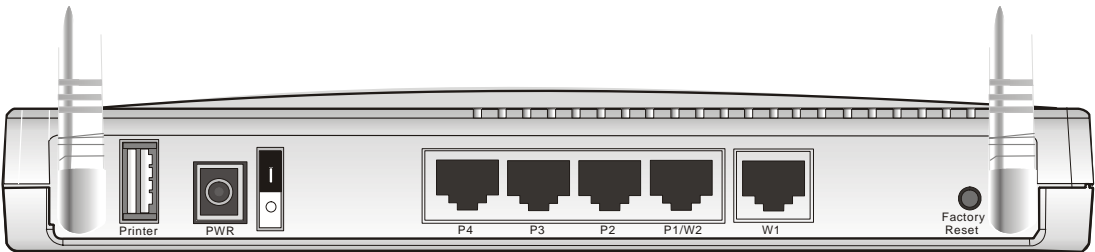
1.2.2 对于 Vigor2910G

LED 说明



LED	状态	说明
ACT (Activity)	闪烁	路由器已开机并正常运行
	暗	路由器已关机
DMZ	亮	DMZ 主机已指定
QoS	亮	QoS 功能已启用
	暗	QoS 功能已关闭
Attack	亮	DoS 防御功能已启用
	闪烁	检测到攻击
WLAN	亮	无线接入点已就绪
	闪烁	无线流量正在通过
	暗	无线接入点已关闭
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

接口说明

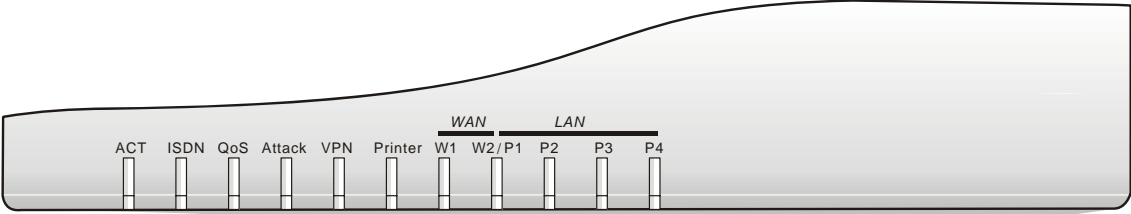


接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口

ON/OFF	电源开关
LAN P4 – P1	连接本地网络的接口
W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口
Factory Reset	<p>还原出厂默认设置</p> <p>用法：当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 Factory Reset 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，松开此按键，路由器将会还原成出厂默认值</p>

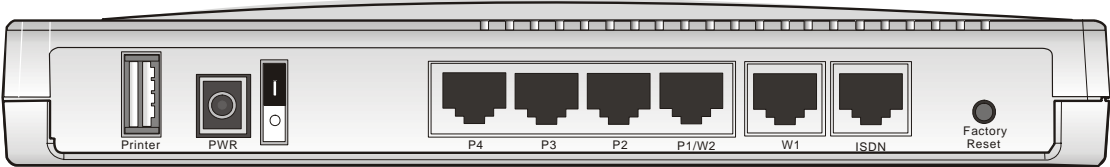
1.2.3 对于 Vigor2910i

LED 说明



LED	状态	说明
ACT (Activity)	闪烁	路由器已开机并正常运行
	暗	路由器已关机
ISDN	亮	ISDN 网络已正确设置
	闪烁	ISDN BRI B1/B2 通道已成功建立连接
QoS	亮	QoS 功能已启用
	暗	QoS 功能已关闭
Attack	亮	DoS 防御功能已启用
	闪烁	检测到攻击
VPN	亮	VPN 隧道已建立
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

接口说明

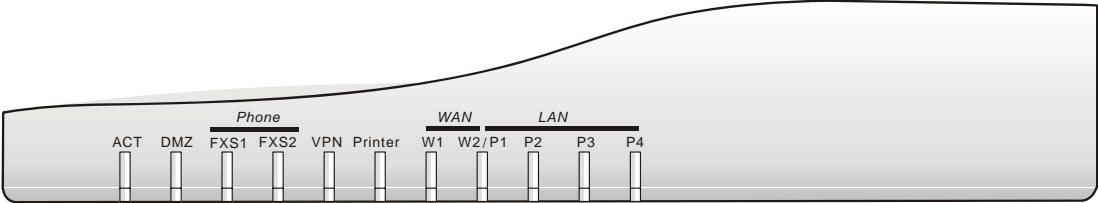


接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口
ON/OFF	电源开关
LAN P4 – P1	连接本地网络的接口
W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口

ISDN	连接 ISDN 服务供应商所提供的 NT1 机盒的接口
Factory Reset	<p>还原出厂默认设置</p> <p>用法：当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 Factory Reset 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，松开此按键，路由器将会还原成出厂默认值</p>

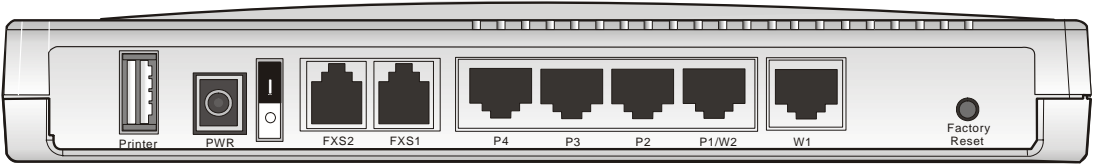
### 1.2.4 对于 Vigor2910V

#### LED 说明



LED	状态	说明
ACT (Activity)	闪烁	路由器已开机并正常运行
	暗	路由器已关机
DMZ	亮	DMZ 主机已指定
FXS1/FXS2	亮	电话接听中（听筒被提起）
	闪烁	有电话呼叫或正在通话
VPN	亮	VPN 隧道已建立
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

#### 接口说明

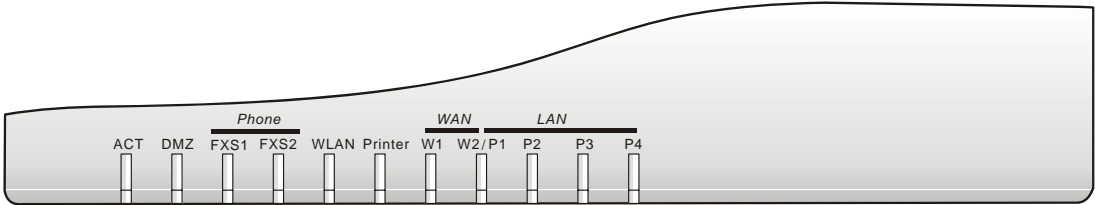


接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口
ON/OFF	电源开关
FXS2 & FXS1	连接座机以及模拟电话机的 VoIP 通讯接口
LAN P4 – P1	连接本地网络的接口
W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口
Factory Reset	还原出厂默认设置 用法: 当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 Factory Reset 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，

	松开此按键，路由器将会还原成出厂默认值
--	---------------------

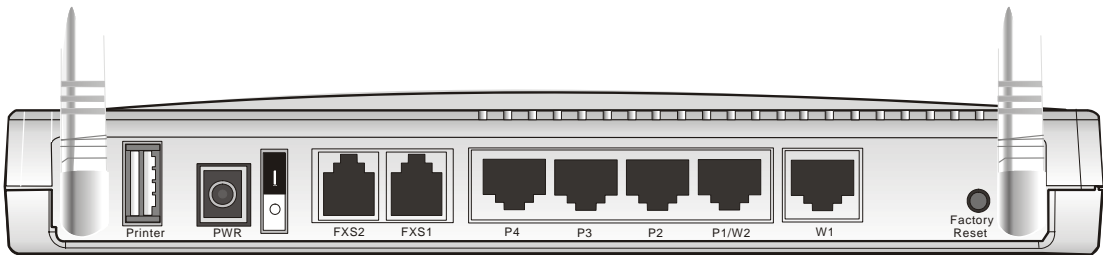
## 1.2.5 对于 Vigor2910VG

### LED 说明



LED	状态	说明
ACT (Activity)	闪烁	路由器已开机并正常运行
	暗	路由器已关机
DMZ	亮	DMZ 主机已指定
FXS1/FXS2	亮	电话接听中（听筒被提起）
	闪烁	有电话呼叫或正在通话
WLAN	亮	无线接入点已就绪
	闪烁	无线流量正在通过
	暗	无线接入点已关闭
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

### 接口说明



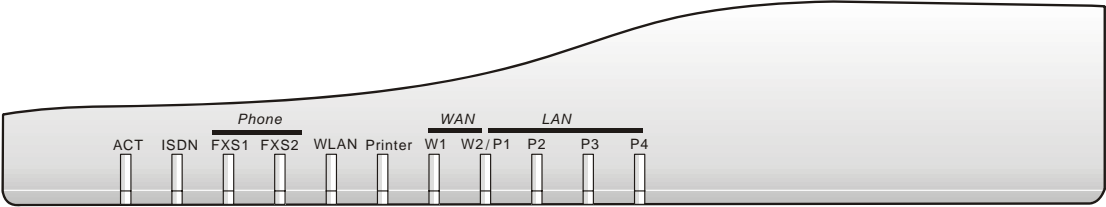
接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口
ON/OFF	电源开关
FXS2 & FXS1	连接座机以及模拟电话机的 VoIP 通讯接口
LAN P4 – P1	连接本地网络的接口

W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口
Factory Reset	<p>还原出厂默认设置</p> <p>用法：当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 <b>Factory Reset</b> 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，松开此按键，路由器将会还原成出厂默认值</p>



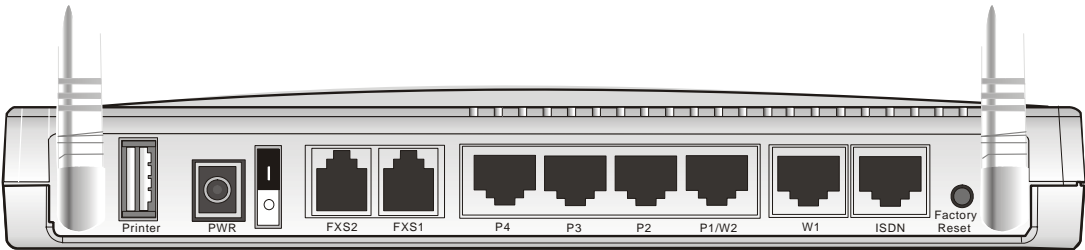
1.2.6 对于 Vigor2910VGi

LED 说明



LED	Status	Explanation
ACT (Activity)	闪烁	路由器已开机并正常运行
	暗	路由器已关机
ISDN	亮	ISDN 网络已正确设置
	闪烁	ISDN BRI B1/B2 通道已成功建立连接
FXS1/FXS2	亮	电话接听中（听筒被提起）
	闪烁	有电话呼叫或正在通话
WLAN	亮	无线接入点已就绪
	闪烁	无线流量正在通过
	暗	无线接入点已关闭
Printer	亮	USB 接口已就绪
WAN(W1-W2)	橘色	10Mbps WAN 口连接已就绪
	绿色	100Mbps WAN 口连接已就绪
	闪烁	以太网封包正在传输
LAN (P1, P2, P3, P4)	橘色	相应接口以 10Mbps 速度连接
	绿色	相应接口以 100Mbps 速度连接
	闪烁	以太网封包正在传输

接口说明



接口	描述
Printer	连接 USB 打印机的接口
PWR	连接 12-15VDC 电源的接口

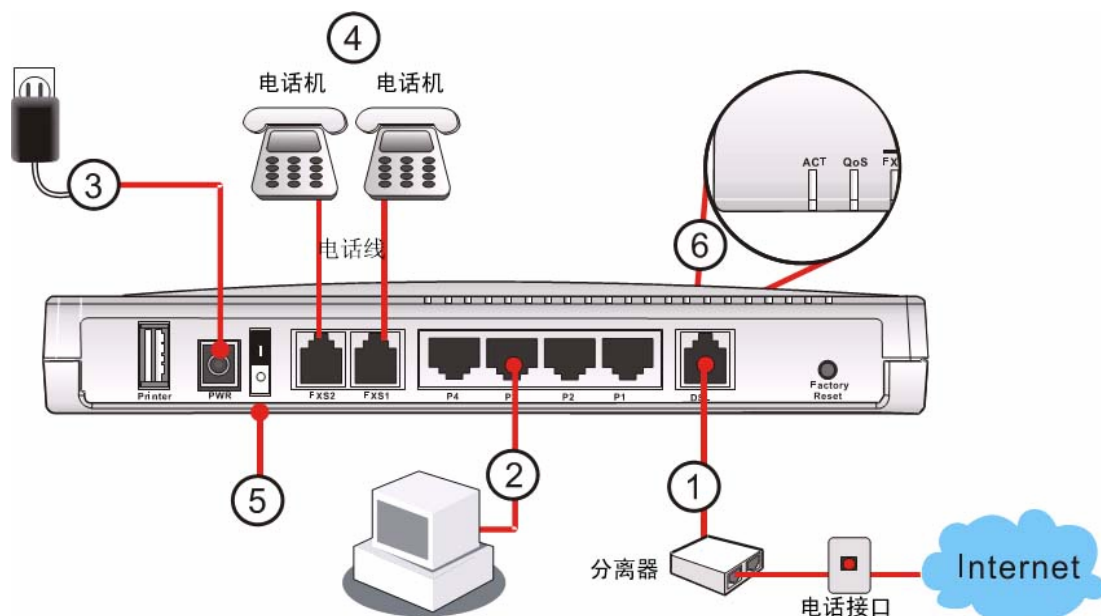
ON/OFF	电源开关
FXS2 & FXS1	连接座机以及模拟电话机的 VoIP 通讯接口
LAN P4 – P1	连接本地网络的接口
W2/W1	连接 ADSL、ADSL2/2+ Internet 线路的接口
ISDN	连接 ISDN 服务供应商所提供的 NT1 机盒的接口
Factory Reset	<p>还原出厂默认设置</p> <p>用法：当路由器在运行时（ACT LED 灯号闪烁），利用尖锐的物品（例如：原子笔）压住 Factory Reset 超过 5 秒；当 ACT LED 灯号开始迅速闪烁时，松开此按键，路由器将会还原成出厂默认值</p>

## 1.3 硬件安装

在开始配置路由器前，您首先要正确的连接到路由器。

1. 用一根以太网网线将此设备连接到一个路由器/Modem。
2. 用一根 RJ-45 网线将您的电脑连接到路由器的 4 个交换口的其中之一。您可以在  
此设备后直接接上 4 台电脑。
3. 将电源线插入此设备的电源接口，将电源另一端接到插座或墙上的电源接口。
4. 将电话座机用电话线连接到此设备的 FXS 口（用于 VoIP 功能）。对于不含 VoIP  
接口的型号，请跳过此步。
5. 将 ISDN NT1/1+机盒用 ISDN 线接到此设备的 ISDN 口。此连接仅用于欧洲。
6. 打开电源
7. 检查 LED 指示灯以确认设备状况。

（有关 LED 指示灯状态的详细信息，请参考 1.1 章节）



**警告：**路由器的 FXS 口只可以接电话座机。请不要将 FXS 口接到墙内的电话线接口，因为这将有可能损坏您的路由器。



# 2

## 配置基本设定

若要安全有效的使用路由器，有必要先修改密码和一些基本设定。

本章将介绍如何修改管理员密码以及如何修改Internet接入设定。请注意，只有管理员才可以修改设定。

### 2.1 修改密码

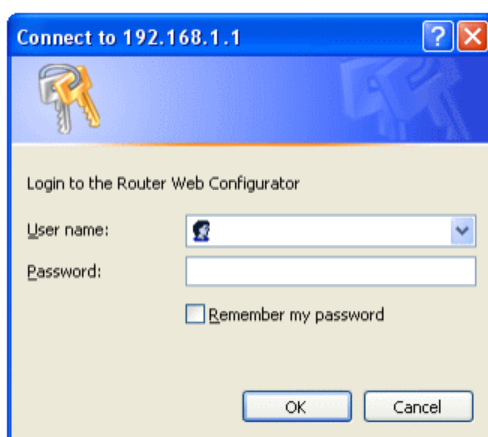
要修改密码，首先请用默认密码登录到路由器 Web 管理界面。

1. 确保电脑已正确连接到路由器。



注意：您可以让您的电脑自动从路由器获取 IP 地址，也可以手动为电脑设置路由器默认 IP 地址 **192.168.1.1** 的同网段地址。详细的信息请参考最后章节——故障排查。

2. 打开网页浏览器，然后输入<http://192.168.1.1>。将有一个窗口弹出，要求您输入用户名和密码。您不用输入任何内容，只需直接点击**确定**即可进入路由器配置界面。



3. 浏览器将显示路由器配置的主页面。

### Vigor2910 系列

双WAN口VPN防火墙路由器

快速开始向导  
连线状态  
WAN  
LAN  
NAT  
防火墙  
对象与组  
带宽管理  
应用程序  
VPN和远程接入  
证书管理  
VoIP  
ISDN  
无线局域网  
VLAN  
系统维护  
诊断

版权所有。

### DrayTek

www.draytek.com.cn

#### 系统状态

型号名称 : DrayTek Vigor2910  
固件版本 : v3.0.2  
建立日期/时间 : Tue Aug 22 16:41:58.53 2006

LAN	
MAC地址	: 00-50-7F-33-31-EC
LAN IP 地址	: 192.168.1.1
子网掩码	: 255.255.255.0
DHCP服务器	: 启用
DNS	: 194.109.6.66

VoIP	
端口	: 1 2
SIP注册	:
帐号ID	: change_me change_me
注册	:
Codec	:
拨入电话	: 0 0
呼出电话	: 0 0

WAN 1 (172)	
连接状态	: 已连接
MAC地址	: 00-50-7F-33-31-ED
连线	: Static IP
IP地址	: 172.17.1.11
默认网关	: 172.17.1.3

无线局域网	
MAC地址	: 00-14-85-d8-50-d6
频率区域	: 欧洲
固件版本	: v2.01.10.10.5.4

4. 点击**系统维护**并选择**系统管理员密码**。

系统管理 >> 管理员密码设定

---

**管理员密码**

原密码	<input type="password"/>
新密码	<input type="password"/>
重新输入新密码	<input type="password"/>

5. 输入新密码并重复输入确认，最后点**确定**。
6. 此时，密码已经完成变更。会再次显示如下窗口，要求输入新密码重新登录到路由器管理界面。

连接到 192.168.1.1



Login to the Router Web Configurator

用户名 (U):

密码 (P):

☐ 记住我的密码 (R)

## 2.2 快速开始向导

若您所在环境可以提供高速 NAT，以下设定可以帮助您快速配置并使用路由器。使用**快速开始向导**可以用最快捷的方式完成路由器部署，快速开始向导的第一个页面就是修改登录密码。请输入密码，然后点击**下一步**。

## 快速开始向导

### 输入登录密码

请输入一个由字母或数字组成的字符串作为您的 **密码**（最多23个字符）。

新密码

确认密码

< 返回

下一步 >

完成

取消

下一个页面如下图所示，请选择您使用的 WAN 口。选择**自适应**作为您路由器的物理类型，然后点击**下一步**。

## 快速开始向导

### 选择WAN口

选择WAN口:

显示名称:

物理模式: Ethernet

物理类型:

- 自适应
- 10M半双工
- 10M全双工
- 100M半双工
- 100M全双工

< 返回

下一步 >

完成

取消

下一个页面如下图所示，请根据您的 ISP 提供的信息选择合适的 Internet 接入方式。比如，如果您 ISP 提供的是 PPPoE 接口，您应该选择 PPPoE 模式。然后点击**下一步**。

## 快速开始向导

### 连接到Internet

**WAN 1**

从下列互联网连线方式类型中选择您的Internet供应商所提供的服务类型。

- ☒ PPPoE
- ☐ PPTP
- ☐ 静态IP
- ☐ DHCP

< 返回

下一步 >

完成

取消

在 **快速开始向导** 中，您可以设置路由器以不同的协议/模式接入 Internet，包括 **PPPoE**、**PPTP**、**静态 IP** 或 **DHCP** 等协议。路由器支持 DSL WAN 口接入 Internet。

## 2.2.1 PPPoE

PPPoE 即 **Point-to-Point Protocol over Ethernet**（基于以太网的点对点协议），主要依赖于两种广泛使用的标准：PPP 和 Ethernet。它使得用户可以通过一个公共的宽带媒介（比如一根 DSL 线路、无线设备或光纤 Modem）由以太网连接到 Internet。所有通过此以太网的用户都可共享一个公共连接。

PPPoE 通常用于 ADSL 用户的联网方式。所有的本地用户可以通过共享一条 PPPoE 线路来上网。ISP 将提供用户名、密码以及认证方式等必要的拨入信息。（而 PPPoA 是指 Point-to-Point Protocol over ATM，即基于 ATM 网的点对点协议）。

如果 ISP 提供 **PPPoE** 连接方式，在此页面请选择 **PPPoE** 并继续：

**快速开始向导**

### PPPoE客户端模式

#### WAN 1

请输入您的Internet服务供应商所提供的用户名和密码。

用户名	84005755@hinet.net
密码	●●●●●●
重新输入密码	●●●●●●

[< 返回](#) [下一步 >](#) [完成](#) [取消](#)

**用户名** 输入 ISP 提供的用户名。

**密码** 输入 ISP 提供的密码。

**重新输入密码** 重新输入密码。

点击**下一步**，查看该连接的总结信息。

**快速开始向导**

### 请确认您的设定：

WAN口：	WAN1
物理模式：	Ethernet
物理类型：	自适应
Internet接入：	PPPoE

点击 **返回** 更改设定，若必要的话。否则，请点击 **完成** 保存当前设定并重启Vigor路由器。

[< 返回](#) [下一步 >](#) [完成](#) [取消](#)

点击**完成**，一个快速开始向导设置完成!!! 的页面将会出现。然后此协议下的系统状态将会显示。



快速开始向导设置完成!!!

## 2.2.2 PPTP

点击 **PPTP** 作为协议，并输入您 ISP 提供的有关此协议的信息。

**快速开始向导**

### PPTP客户端模式

**WAN 1**  
请输入由您的Internet服务供应商所提供的用户名、密码、WAN IP设定及PPTP服务器IP。

用户名	<input type="text"/>
密码	<input type="password"/>
重新输入密码	<input type="password"/>
WAN IP设置	
<input type="radio"/> 自动获取一个IP地址	
<input checked="" type="radio"/> 指定一个IP地址	
IP地址	<input type="text" value="172.16.3.229"/>
子网掩码	<input type="text" value="255.255.255.0"/>
PPTP服务器地址	<input type="text"/>

点击 **下一步**，查看该连接的总结信息。

**快速开始向导**

### 请确认您的设定：

WAN口：	WAN1
物理模式：	Ethernet
物理类型：	自适应
Internet接入：	PPTP

点击 **返回** 更改设定，若必要的话。否则，请点击 **完成** 保存当前设定并重启Vigor路由器。

点击**完成**，一个**快速开始向导设置完成!!!**的页面将会出现。然后此协议下的系统状态将会显示。

**快速开始向导设置完成!!!**

### 2.2.3 静态 IP

点击**静态 IP**作为协议。输入您的ISP提供的有关此协议的所有信息。

#### 快速开始向导

##### 静态IP客户端模式

<b>WAN 1</b>	
请输入您的Internet服务供应商所提供的静态IP设置。	
WAN IP	<input type="text" value="172.16.3.229"/>
子网掩码	<input type="text" value="255.255.255.0"/>
网关	<input type="text" value="172.16.3.1"/>
首选DNS服务器	<input type="text" value="168.95.1.1"/>
备用DNS服务器	<input type="text"/> (可选)

[< 返回](#) [下一步 >](#) [完成](#) [取消](#)

完成此页面的设定后，点击**下一步**，就可以看到以下信息。

#### 快速开始向导

##### 请确认您的设定：

WAN口：	WAN1
物理模式：	Ethernet
物理类型：	自适应
Internet接入：	Static IP

点击 **返回** 更改设定，若必要的话。否则，请点击 **完成** 保存当前设定并重启Vigor路由器。

[< 上一步](#) [下一步 >](#) [完成](#) [取消](#)

点击**完成**，一个**快速开始向导设置完成!!!**的页面将会出现。然后此协议下的系统状态将会显示。

**快速开始向导设置完成!!!**

### 2.2.4 DHCP

点击 **DHCP** 作为协议。输入您 ISP 所提供的所有相关信息。

**快速开始向导**

**DHCP客户端模式**

**WAN 1**

如果您的Internet服务供应商要求您输入特定的主机名称或特定的MAC地址，请在此输入。

主机名

(可选)

MAC

00

-

50

-

7F

-

33

-

31

-

ED

(可选)

[< 返回](#) [下一步 >](#) [完成](#) [取消](#)

完成此页面的设定后，点击 **下一步**，就可以看到以下信息。

**快速开始向导**

**请确认您的设定：**

WAN口：

物理模式：

物理类型：

Internet接入：

WAN1

Ethernet

自适应

DHCP

点击 **返回** 更改设定，若必要的话。否则，请点击 **完成** 保存当前设定并重启Vigor路由器。

[< 上一步](#) [下一步 >](#) [完成](#) [取消](#)

点击 **完成**，一个快速开始向导设置完成!!! 的页面将会出现。然后此协议下的系统状态将会显示。

**快速开始向导设置完成!!!**

## 2.3 在线状态

在线状态页面显示系统状态，WAN 状态，ADSL 信息以及其它路由器相关信息。如果您选择 PPPoE 作为上网方式，请您在在线状态页面里查找 **断开 PPPoE** 或者 **PPPoE 连接**。

### PPPoE 在线状态

#### 连线状态

系统状态			系统已运行时间： 0: 27: 27		
局域网状态		首选DNS服务器: 194.109.6.66		备用DNS: 168.95.1.1	
IP地址	上行封包	下行封包			
192.168.1.1	44	0			
WAN 1状态					
已启用	线路	名称	模式	在线时间	>> <u>断开PPPoE</u>
是	Ethernet		PPPoE	0:00:00	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
219.81.160.205	211.78.218.40	6	29	6	12
WAN 2 状态					
已启用	线路	名称	模式	在线时间	
是	Ethernet	172	Static IP	0:07:50	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
172.17.1.11	172.17.1.3	963	3489	1070	845

### PPTP 在线状态（WAN 2）

#### 连线状态

系统状态				系统已运行时间： 0： 27： 27	
局域网状态		首选DNS服务器： 194.109.6.66		备用DNS： 168.95.1.1	
IP地址	上行封包	下行封包			
192.168.1.1	44	0			
WAN 1状态					
已启用	线路	名称	模式	在线时间	>> <u>断开PPPoE</u>
是	Ethernet		PPPoE	0:00:00	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
219.81.160.205	211.78.218.40	6	29	6	12
WAN 2 状态					
已启用	线路	名称	模式	在线时间	>> <u>断开PPTP</u>
是	Ethernet	WAN2	PPTP	0:00:15	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
192.168.29.202	192.168.29.1	103	119	14	6

### Static IP 在线状态（WAN 1）

## 连线状态

系统状态				系统已运行时间: 0: 36: 41	
局域网状态		首选DNS服务器: 194.109.6.66		备用DNS: 168.95.1.1	
IP地址	上行封包	下行封包			
192.168.1.1	60	0			
WAN 1状态					
已启用	线路	名称	模式	在线时间	
是	Ethernet	WAN 1	Static IP	0:17:04	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
172.17.1.11	172.17.1.3	2753	1953	2974	393
WAN 2 状态					
已启用	线路	名称	模式	在线时间	
否	以太网		---	00:00:00	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
---	---	0	0	0	0

## DHCP 在线状态

### 连线状态

系统状态				系统已运行时间: 0: 36: 41	
局域网状态		首选DNS服务器: 194.109.6.66		备用DNS: 168.95.1.1	
IP地址	上行封包	下行封包			
192.168.1.1	60	0			
WAN 1状态					
已启用	线路	名称	模式	在线时间	
是	Ethernet		DHCP Client	0:01:49	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
192.168.22.10	192.168.22.105	3	3	7	9
WAN 2 状态					
已启用	线路	名称	模式	在线时间	
否	以太网		---	00:00:00	
IP	网关IP	上行封包	上行速率	下行封包	下行速率
---	---	0	0	0	0

详细解释显示如下:

**主 DNS** 显示主 DNS 地址。

**备用 DNS** 显示备用 DNS 地址。

### 局域网状态部分

**IP 地址** 显示 LAN 接口 IP 地址。

**TX Packets** 显示 LAN 接口发出的封包。

**RX Packets** 显示 LAN 接口收到的封包。

### WAN1 和 WAN2 状态部分

**线路** 显示 WAN 口的物理连接方式（以太网）。

**名称** 显示您对 WAN1 或 WAN2 口的描述。

**模式** 显示 WAN 连接类型（如：PPPoE）。

**在线时间** 显示路由器连线时间。

**网关 IP 地址** 显示默认网关的 IP 地址。

<b>IP 地址</b>	显示路由器连线时间。
<b>上行封包</b>	显示 WAN 接口发出的封包。
<b>上行速率</b>	显示 WAN 接口发出封包的速率。
<b>下行封包</b>	显示 WAN 接口收到的封包。
<b>下行速率</b>	显示 WAN 接口收到封包的速率。

**注释：**绿色字体表示 WAN（WAN1/WAN2）已经连接到以太网；红色字体表示 WAN（WAN1/WAN2）没有连接到以太网。

## 2.4 状态栏

每次当点击**确定**保存设定后，web 页面下方状态栏将显示下列信息，表示系统已经接受了设定的更改。



**已就绪**      表示系统已经可以接受输入。



**设定已保存**      说明设定已保存。



# 3

## 高级设定

当完成路由器的基本设定之后，连接好路由器，路由器就可以访问 Internet 了。如果需要做更多的设定，可以参照本章。第四章将介绍一些应用的举例。

### 3.1 WAN

**快速开始向导**为用户提供了一种快速设置路由器的连接方法。此外，如果您想要调整更多的设置参数，请您点击路由器设置网页里 **WAN** 下的 **Internet 接入** 项。

#### 3.1.1 IP 网络基础

IP 代表 Internet 协议。IP 网络里面的所有设备，包括路由器，打印服务器以及主机，都需要 IP 地址来标记它在网络中的位置。为了避免地址冲突，IP 地址公开注册到网络信息中心（NIC）。互联网上每台设备的 IP 地址必须是唯一的，不过对于路由器维护的内部网络而言，可以使用一些保留的永远不被注册到 NIC 的地址，这些地址被称为私网地址，列表如下：

从 10.0.0.0 到 10.255.255.255  
从 172.16.0.0 到 172.31.255.255  
从 192.168.0.0 到 192.168.255.255

#### 什么是公网地址和私网地址

路由器管理着内部局域网络，所有的内部 PC 都有一个**私网 IP 地址**，路由器使用私网 IP 192.168.1.1 与局域网络交换数据。同时，路由器还通过 WAN 接口的**公网 IP** 和 Internet 上的其他设备进行数据交换，当数据通过时，路由器进行网络地址转换（NAT），实现私网地址和公网地址之间的数据交换，所有的数据都会发到正确的 PC 上去。因此，所有的主机都可以共享一个 Internet 连接。

#### 从 ISP 获取公网 IP 地址

在 ADSL 应用中，用户终端设备需要做 PPP 认证和授权以桥接到网络上。Point to Point Protocol over Ethernet (PPPoE)通过一个远程的接入集中器或集中器集合来将网络上的主机连接起来。这种应用根据用户需求可以提供接入控制、付费以及服务类型，因此给用户带来了极大的便利。

当路由器开始连接 ISP 时，经过一连串的发现过程后，路由器请求连接 ISP，之后会话会被建立。您的用户名和密码会使用 **RADIUS** 认证系统，通过密码认证协议(**PAP**) 或挑战握手协议 (**CHAP**) 进行认证。然后 ISP 会将 IP 地址，域名服务器以及其它的相关信息赋予您的路由器。

以下显示的是 **Internet 接入** 的菜单项。



#### 3.1.2 基本设定

这部分内容将介绍一些 Internet 的基本设定并详细解释 WAN1 和 WAN2 口的连接方式。

Vigor2910 路由器支持双 WAN 口，它允许用户结合两个 WAN 口的带宽来提升访问 Internet 的速度。路由器的每一个 WAN 口（路由器上的 WAN 口就是 WAN1 口，路由器的 LAN1 口可以作为 WAN2 口），都可以连接不同的 ISP，不管这些 ISP 是提供 DSL 服务还是宽带服务等等。如果其中一个 WAN 口连接发生问题，路由器会自动选用另一条正常的线路传输数据。当然这是需要您作相关设置的。

您可以在下面的网页上分别设置 WAN1 和 WAN2 的一些基本设定。

**注释：**默认情况下，WAN1 口是开启的，而 WAN2 口是处于可选状态的。

#### WAN >> 基本设定

基本设定	
<b>WAN1</b>	<b>WAN2</b>
启用： <input checked="" type="checkbox"/> 是	启用： <input type="checkbox"/> 否
显示名称： <input type="text" value="172"/>	显示名称： <input type="text"/>
物理模式： <input type="text" value="以太网"/>	物理模式： <input type="text" value="以太网"/>
物理类型： <input type="text" value="自适应"/>	物理类型： <input type="text" value="自适应"/>
负载均衡模式： <input type="text" value="自动平衡"/>	负载均衡模式： <input type="text" value="自动平衡"/>
线路速度 (Kbps)： 下行 <input type="text" value="0"/> 上行 <input type="text" value="0"/>	线路速度 (Kbps)： 下行 <input type="text" value="0"/> 上行 <input type="text" value="0"/>
启用模式： <input type="text" value="一直在线"/>	启用模式： <input type="text" value="一直在线"/>
按需拨接： <input type="radio"/> WAN2失效 <input checked="" type="radio"/> WAN2上行速度超过 <input type="text" value="0"/> Kbps WAN2下行速度超过 <input type="text" value="0"/> Kbps	按需拨接： <input type="radio"/> WAN1失效 <input checked="" type="radio"/> WAN1上行速度超过 <input type="text" value="0"/> Kbps WAN1下行速度超过 <input type="text" value="0"/> Kbps

**注意：**WAN2和LAN P1共用同硬件接口P1。当WAN2启用时，P1口被用作WAN2。

确定

#### 启用

选择“是”以启用 WAN1 口。

选择“否”以禁用 WAN1 口。

#### 显示名称

您可以在这里输入对 WAN1 或 WAN2 口的描述。

#### 物理模式

这里显示的是 WAN 口的物理连接方式。

#### 物理类型

您可以在这里选择 WAN1 或 WAN2 口的物理类型。一般情况下都是选择“自适应”来由系统自己检测。

物理类型：

自适应

10M半双工

10M全双工

100M半双工

100M全双工

#### 负载均衡模式

如果您知道您 WAN 口的实际带宽，您可以选择“根据线路速度”来实现负载均衡。如果您不知道的话，可以选择“自动平衡”选项来交由路由器自动将负载均衡到最佳状态。

负载均衡模式：

自动平衡

根据线路速度

## 线路速度

如果您在“**负载均衡模式**”里选择了“**根据线路速度**”来实现负载均衡的话，请在这里输入 WAN1 和 WAN2 口线路的上、下行速度，单位是 kbps。

## 启用模式

通过选择“**一直在线**”选项来使得 WAN1 和 WAN2 口总是处于在线的状况；或者您也可以选择“**按需拨接**”选项来使得 WAN1 或 WAN2 口只有在需要的情况下才上线。

启用模式：



如果您选择了“**按需拨接**”，WAN 口 Internet 访问页面下的“**超时**”选项就会被启用，您可以在设置 WAN 口的 PPPoE 和 PPTP 访问模式时对“**超时**”选项进行设置。此外，当您启用了“**按需拨接**”，以下三项就会被启用。

按需拨接：

- ☒ WAN2失效  
☐ WAN2上行速度超过  Kbps  
WAN2下行速度超过  Kbps

**WAN2 失效** – 这项是指只有当 WAN2 不在线的情况下 WAN1 才会被启用。

**WAN2 上行速度超过 XX kbps** – 这项是指当 WAN2 口的上行速度超过您所设定的值的时候，在 15 秒之内 WAN1 口会上线。

**WAN2 下行速度超过 XX kbps** – 这项是指当 WAN2 口的下行速度超过您所设定的值的时候，在 15 秒之内 WAN1 口会上线。

**WAN1 失效** – 这项是指只有当 WAN1 不在线的情况下 WAN2 才会被启用。

**WAN1 上行速度超过 XX kbps** – 这项是指当 WAN1 口的上行速度超过您所设定的值的时候，在 15 秒之内 WAN2 口会上线。

**WAN1 下行速度超过 XX kbps** – 这项是指当 WAN12 口的下行速度超过您所设定的值的时候，在 15 秒之内 WAN2 口会上线。

## 3.1.3 Internet 接入

因为 Vigor2910 路由器支持双 WAN 口功能，这使得用户将两个 WAN 口设置不同的网络连接提供了可能。由于 WAN1 和 WAN2 口的物理模式不同，接入模式也有所不同。


WAN >> Internet 接入

Internet 接入

索引	显示名称	物理模式	接入模式
WAN1	172	Ethernet	静态或动态IP <a href="#">详情页面</a>
WAN2		Ethernet	无 <a href="#">详情页面</a>

## 索引

此项显示路由器支持的 WAN 类型。WAN1 口是路由器默认的 WAN 口，WAN2/LAN1 口是另一个可选 WAN 口。

显示名称	此显示 WAN1 和 WAN2 口所描述的名称。
物理模式	此项显示 WAN1 和 WAN2 口的物理接口。
接入模式	您可以在下面的下拉菜单中选择一个您所配置接入模式。
	
	<p>这里有三种接入模式：PPPoE, 静态或动态 IP 和 PPTP 三种模式可供选择。</p>
详情页面	此按钮会根据您所选择不同的接入模式而显示不同的设置页面。

## PPPoE 的详情页面

在 Internet 接入页面选择 **PPPoE** 作为接入模式，请您在 **WAN** 菜单里选择 **Internet 接入**，就会出现以下的设置页面。

WAN >> Internet接入

WAN 1

PPPoE客户端模式

☐ 启用 ☒ 禁用

ISP接入设置

用户名84005755@hinet.net

密码

索引 (1-15) [计划任务](#) 设定:  
=> , , ,

ISDN拨号备份设置

拨号备份设置无

PPP/MP设定

PPP验证PAP或CHAP

闲置超时-1 秒

IP地址分配方法 (IPCP)

WAN IP别名

固定IP: ☐ 是 ☒ 否 (动态IP)

固定IP地址

☒ 默认MAC地址  
☐ 指定一个MAC地址

MAC地址:  
00 . 50 . 7F : 33 . 31 . ED

确定

取消

### PPPoE 接入

选择 **Enable** 启用 PPPoE 接入。如果选择 **Disable** 就会禁用 PPPoE 接入。这时您在此页面所做的所有设置都会失效。

### ISP 接入设定

在此输入由您的 ISP 提供的 ADSL 上网的用户名和密码。如果您想要让您的路由器一直连接 Internet，请选择“**一直在线**”选项。

**用户名** - 在此输入由您的 ISP 提供的 ADSL 上网的用户名。

**密码** - 在此输入由您的 ISP 提供的 ADSL 上网的密码。

**计划任务 索引 (1-15)** - 您可以键入四个计划任务项。所有的计划任务可以在 **应用程序** 下的 **计划任务** 页面进行定义。您只要在这里填入计划任务的相应编号就可以了。

### ISDN 拨号备份设置

只有支持 ISDN 的 Vigor2910 路由器 (Vigor2910i 系列) 拥有此功能。在使用 ISDN 拨号备份功能之前，您必须在路由器主菜单下的“**拨到单一 ISP**”页面填写相关的备份信息。

#### ISDN拨号备份设置

拨号备份设置

无

无

封包触发

由于 Vigor2910 的某些型号不支持 ISDN 功能，所以 ISDN 拨号备份功能在这些路由器上是不可用的，因此使用这些路由器的用户可以忽略下面的设定。

**无** - 禁用 ISDN 拨号备份功能。

**数据包触发** - 如果本地有数据包经过路由器连接到 Internet 上，就会触发 ISDN 拨号。

**一直在线** - 如果宽带线路不能正常使用，ISDN 备份线路会自动启用，直到宽带线路恢复正常。如果您在路由器的 LAN 里的

主机向外界提供 Web 服务的话，我们强烈建议您选取此项，以便外边的客户可以随时访问到您的 Web 服务器。

PPP/MP 设定

PPP 验证 – 您可以在这里选择仅 PAP 或 PAP 或 CHAP。

闲置超时 –您可以在这里设置一个时间段，如果在这段时间里没有数据流经路由器，路由器就会自动断开与 Internet 的连接。此项设定只有当您在 WAN 下的基本设定页面里设置了按需拨接才会有效。

IP 地址分配方法 (IPCP)

通常 ISP 在每次接入时动态分配 IP 地址。也有些 ISP 会提供静态 IP 地址，这种情况下，可以将指定的 IP 填写到固定 IP 栏。您可以在使用此功能之前联系到您的 ISP 以获取相关信息。

WAN IP 别名 - 如果您有多个公网 IP 地址，可以将它们设定到 WAN IP 别名中，在这里您最多可以设置 8 个公网 IP 地址。请注意，只有 WAN 1 口有此功能。

WAN IP别名 (多NAT)

索引值	启用	辅助WAN IP
1.	<input checked="" type="checkbox"/>	172.17.1.11
2.	<input type="checkbox"/>	<input type="text"/>
3.	<input type="checkbox"/>	<input type="text"/>
4.	<input type="checkbox"/>	<input type="text"/>
5.	<input type="checkbox"/>	<input type="text"/>
6.	<input type="checkbox"/>	<input type="text"/>
7.	<input type="checkbox"/>	<input type="text"/>
8.	<input type="checkbox"/>	<input type="text"/>

固定 IP – 点选“是”以启用此功能，然后请您在固定 IP 地址项里填写由您的 ISP 提供的固定 IP 地址。

默认 MAC 地址 – 您可以在这里选用默认 MAC 地址或者自己为您的路由器指定一个 MAC 地址。

指定一个 MAC 地址 – 您可以在这里自己手工指定一个 MAC 地址。

在完成以上设置之后，请您点击“确定”键以激活您所做的设置。

静态或动态 IP 的详情页面

您通常会从您的 ISP 那里获取一个或多个公网 IP 地址。一般情况下，宽带服务提供商会为您提供一个固定的 IP 地址，而 ADSL 服务提供商会为您提供一组动态的 IP 地址，在您每次连接到 Internet 时会随机分配一个 IP 地址给您。

如果您想要使用静态或动态 IP 访问 Internet，请您在 WAN 菜单下的 Internet 接入页面里选择静态或动态 IP 作为接入模式，然后点击详情页面就会出现以下的设置页面。



**WAN 1**

**静态或动态IP (DHCP客户端)**  
☒ 启用 ☐ 禁用

**ISDN拨号备份设置**  
 拨号备份模式: [无]

**保持WAN连接**  
☐ 启用PING保持在线  
 PING IP: [ ]  
 PING间隔: [0] 分钟

**RIP协议**  
☐ 启用RIP

**WAN IP网络设置** WAN IP别名

☐ 自动获取IP地址  
 路由器名: [ ] \*  
 域名: [ ] \*  
 \*: 某些ISP需要

☒ 指定一个IP地址  
 IP地址: [172.17.1.11]  
 子网掩码: [255.255.255.0]  
 网关IP地址: [172.17.1.3]

☒ 默认MAC地址  
☐ 指定一个MAC地址  
 MAC地址: [00] . [50] . [7F] . [33] . [31] . [ED]

**DNS服务器IP地址**  
 首选IP地址: [ ]  
 备用IP地址: [ ]

**静态或动态 IP (DHCP客户端)** 点选**启用**以启用此项功能。如果点选**禁用**，此项功能就会被禁止使用，这时您在此页面所做的所有设置都会失效。

**ISDN 拨号备份设置** 只有支持 ISDN 的 Vigor2910 路由器 (Vigor2910i 系列) 拥有此功能。在使用 ISDN 拨号备份功能之前，您必须在路由器主菜单下的“**拨到单一 ISP**”页面填写相关的备份信息。

#### ISDN拨号备份设置

拨号备份设置

[无] [无] [封包触发]

由于 Vigor2910 的某些型号不支持 ISDN 功能，所以 ISDN 拨号备份功能在这些路由器上是不可用的，因此使用这些路由器的用户可以忽略下面的设定。

**无** – 禁用 ISDN 拨号备份功能。

**数据包触发** – 如果本地有数据包经过路由器连接到 Internet 上，就会触发 ISDN 拨号。

**一直在线** – 如果宽带线路不能正常使用，ISDN 备份线路会自动启用，直到宽带线路恢复正常。如果您在路由器的 LAN 里的主机向外界提供 Web 服务的话，我们强烈建议您选取此项，以便外边的客户可以随时访问到您的 Web 服务器。

#### 保持 WAN 口连接

此项功能只是用在一些特殊环境下，有时候一些 ISP 为了节省 IP 资源会将一些一直在线却没有流量的连接断掉。如果您不想在没有流量的情况下断开与 Internet 的连接，就需要启用此功能了。请您选择**启用 PING 保持在线**选项以启用此功能。

**PING to the IP** – 如果您启用了**启用 PING 保持在线**选项，请您在这里填写一个可以 Ping 到的公网 IP 地址让路由器一直 Ping 它，以保持和 Internet 的连接不被断开。

**PING 时间间隔** – 您可以在这里填写一个让路由器执行 Ping 操作的时间间隔。

#### RIP 协议

路由信息协议是用来指明路由器之间如何交换路由表的。选择**启用 RIP**启用此功能。

## WAN IP 网络设定

在这里您可以选择自动从 DHCP 服务器那里获取 IP 地址，也可以在这里手工填写一个 IP 地址。

**WAN IP 别名** - 如果您有多个公网 IP 地址，可以将它们设定到 WAN IP 别名中，在这里您最多可以设置 8 个公网 IP 地址。请注意，只有 WAN 1 口有此功能。

**WAN IP 别名 (多 NAT)**

索引值	启用	辅助 WAN IP
1.	<input checked="" type="checkbox"/>	172.17.1.11
2.	<input type="checkbox"/>	<input type="text"/>
3.	<input type="checkbox"/>	<input type="text"/>
4.	<input type="checkbox"/>	<input type="text"/>
5.	<input type="checkbox"/>	<input type="text"/>
6.	<input type="checkbox"/>	<input type="text"/>
7.	<input type="checkbox"/>	<input type="text"/>
8.	<input type="checkbox"/>	<input type="text"/>

确定

全部清除

关闭

**自动获取 IP 地址**— 点选此项让路由器从 DHCP 服务器那里自动获取一个 IP 地址。

**路由器名称**: 您可以在这里填写由 ISP 提供的路由器名。

**域名**: 您可以在这里填写您的域名。

**指定 IP 地址** - 点选此项以填写静态 IP 的信息。

**IP 地址**: 请在这里填写路由器 WAN 口的 IP 地址。

**子网掩码**: 请在这里填写子网掩码。

**网关 IP 地址**: 请在这里填写网关 IP 地址。

**默认 MAC 地址**: 点选此项以使用默认的 MAC 地址。

**指定 MAC 地址**: 一些宽带服务提供商会将使用绑定网卡的方法来禁止用户共享宽带服务。不过有了**指定 MAC 地址**功能，您就可以在这里填上那个绑定网卡的 MAC 地址，然后就可以通过路由器来实现宽带共享了。

## DNS 服务器 IP 地址

如果您手动填写您路由器 WAN 口的 IP 地址，那么您也需要在这里手动填写一个主 DNS 服务器的 IP 地址。如果有必要的话，您还可以在这里填写一个备用 DNS 服务器的地址。

## PPTP 的详情页面

如果您想要使用 **PPTP** 访问 Internet，请您在 **WAN** 菜单下的 **Internet 接入** 页面里选择 **PPTP** 作为接入模式，然后点击**详情页面**就会出现以下的设置页面。



**WAN 1**

<p><b>PPTP客户端模式</b></p> <p><input checked="" type="radio"/> 启用 <input type="radio"/> 禁用</p> <p>PPTP服务器 <input type="text" value="10.0.0.138"/></p>	<p><b>PPP设置</b></p> <p>PPP验证 <input type="text" value="PAP 或 CHAP"/></p> <p>闲置超时 <input type="text" value="-1"/> 秒</p>
<p><b>ISP接入设置</b></p> <p>用户名 <input type="text"/></p> <p>密码 <input type="text"/></p> <p>索引 (1-15) <b>计划任务</b> 设置:</p> <p>=&gt; <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p>	<p><b>IP地址分配方法 (IPCP)</b></p> <p>固定IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (动态IP)</p> <p>固定IP地址 <input type="text"/></p>
<p><b>ISDN拨号备份设置</b></p> <p>拨号备份模式 <input type="text" value="无"/></p>	<p><b>WAN IP网络设定</b></p> <p><input type="radio"/> 自动获取一个IP地址</p> <p><input checked="" type="radio"/> 指定一个IP地址</p> <p>IP地址 <input type="text" value="10.0.0.150"/></p> <p>子网掩码 <input type="text" value="255.0.0.0"/></p>

## PPTP 设定

**PPTP 连接** – 点选启用以启用 PPTP 客户端和 ISP 之间建立一条 PPTP 隧道。

**PPTP 服务器** – 您可以在这里填写 PPTP 服务器的 IP 地址。

## ISP 接入设定

**用户名** – 在此输入由您的 ISP 提供的 ADSL 上网的用户名。

**密码** – 在此输入由您的 ISP 提供的 ADSL 上网的密码。

**计划任务 索引 (1-15)** – 您可以键入四个计划任务项。所有的计划任务可以在应用程序下的计划任务页面进行定义。您只要在这里填入计划任务的相应编号就可以了。

## ISDN 拨号备份设置

只有支持 ISDN 的 Vigor2910 路由器 (Vigor2910i 系列) 拥有此功能。在使用 ISDN 拨号备份功能之前，您必须在路由器主菜单下的“拨到单一 ISP”页面填写相关的备份信息。

### ISDN拨号备份设置

拨号备份设置

由于 Vigor2910 的某些型号不支持 ISDN 功能，所以 ISDN 拨号备份功能在这些路由器上是不可用的，因此使用这些路由器的用户可以忽略下面的设定。

**无** – 禁用 ISDN 拨号备份功能。

**数据包触发** – 如果本地有数据包经过路由器连接到 Internet 上，就会触发 ISDN 拨号。

**一直在线** – 如果宽带线路不能正常使用，ISDN 备份线路会自动启用，直到宽带线路恢复正常。如果您在路由器的 LAN 里的主机向外界提供 Web 服务的话，我们强烈建议您选取此项，以便外边的客户可以随时访问到您的 Web 服务器。

## PPP 设定

**PPP 验证** – 您可以在这里选择仅 PAP 或 PAP 或 CHAP。

**闲置超时** – 您可以在这里设置一个时间段，如果在这段时间里没有数据流经路由器，路由器就会自动断开与 Internet 的连接。此项设定只有当您在 WAN 下的基本设定页面里设置了按需拨接才会有效。

## IP 地址分配方法 (IPCP)

通常 ISP 在每次接入时动态分配 IP 地址。也有些 ISP 会提供静态 IP 地址，这种情况下，可以将指定的 IP 填写到固定 IP 栏。您可以在使用此功能之前联系到您的 ISP 以获取相关信息。

**固定 IP** – 点选“是”以启用此功能，然后请您在**固定 IP 地址**项里填写由您的 ISP 提供的固定 IP 地址。

**WAN IP 别名** - 如果您有多个公网 IP 地址，可以将它们设定到 WAN IP 别名中，在这里您最多可以设置 8 个公网 IP 地址。请注意，只有 WAN1 口有此功能。

WAN IP 别名 (多 NAT)

索引值	启用	辅助 WAN IP
1.	<input checked="" type="checkbox"/>	172.17.1.11
2.	<input type="checkbox"/>	<input type="text"/>
3.	<input type="checkbox"/>	<input type="text"/>
4.	<input type="checkbox"/>	<input type="text"/>
5.	<input type="checkbox"/>	<input type="text"/>
6.	<input type="checkbox"/>	<input type="text"/>
7.	<input type="checkbox"/>	<input type="text"/>
8.	<input type="checkbox"/>	<input type="text"/>

确定

全部清除

关闭

**默认 MAC 地址** – 您可以在此选用**默认 MAC 地址**或者自己为您的路由器指定一个 MAC 地址。

**指定一个 MAC 地址** – 您可以在这里自己手动指定一个 MAC 地址。

## WAN IP 网络设定

**自动获取 IP 地址** – 点选此项使路由器自动获取 IP 地址。

**指定 IP 地址** – 点选此项然后填写下列信息。

**IP 地址** – 请在这里填写 IP 地址。

**子网掩码** – 请在这里填写相应的子网掩码。

### 3.1.4 负载均衡策略

Vigor2910 路由器支持负载均衡功能，此功能可以根据协议类型，IP 地址，端口等参数来为 WAN1 和 WAN2 分配流量。用户可以通过设置负载均衡策略来方便的规划路由器的流量分布。在这里，您最多可以设置 20 条负载均衡策略。

**注释：**只有当 WAN1 口和 WAN2 口同时启用时才能使用负载均衡策略功能。

负载均衡策略									
索引	启用	协议	WAN	源起始地址	源终止地址	目标起始地址	目标终止地址	目标起始端口	目标终止端口
1	<input checked="" type="checkbox"/>	TCP	WAN1						
2	<input type="checkbox"/>	所有	WAN1						
3	<input type="checkbox"/>	所有	WAN1						
4	<input type="checkbox"/>	所有	WAN1						
5	<input type="checkbox"/>	所有	WAN1						
6	<input type="checkbox"/>	所有	WAN1						
7	<input type="checkbox"/>	所有	WAN1						
8	<input type="checkbox"/>	所有	WAN1						
9	<input type="checkbox"/>	所有	WAN1						
10	<input type="checkbox"/>	所有	WAN1						

<< 1-10 | 11-20 >>

下一页 >>

- 索引

点击索引号可以进入负载均衡策略的设置页面。
- 启用

选择此项以启用对应的负载均衡策略。
- 协议

您可以在下拉菜单里选择您需要做负载均衡的协议。
- WAN

您可以在下拉菜单里选择需要做负载均衡的 WAN 口。
- 源起始 IP

显示的是用于此负载均衡策略的源起始 IP 地址。
- 源终止 IP

显示的是用于此负载均衡策略的源终止 IP 地址。
- 目标起始 IP

显示的是用于此负载均衡策略的目标起始 IP 地址。
- 目标终止 IP

显示的是用于此负载均衡策略的目标终止 IP 地址。
- 目标起始端口

显示的是用于此负载均衡策略的目标起始端口。
- 目标终止端口

显示的是用于此负载均衡策略的目标终止端口。
- 点击索引 1

进入以下负载均衡策略的配置页面。

索引: 1

<input checked="" type="checkbox"/> 启用	
协议	TCP
绑定 WAN 口	WAN1
源起始地址	192.168.1.3
源终止地址	192.168.1.5
目标起始地址	168.95.0.0
目标终止地址	198.95.0.100
目标起始端口	80
目标终止端口	100

确定

取消

- 启用

选择此项以启用此策略。
- 协议

您可以在这里使用下拉菜单来选择您认为适当的协议。

协议

所有

所有

TCP

UDP

TCP/UDP

ICMP

IGMP
- 绑定 WAN 口

您可以在这里选择此策略应用的 WAN 口。
- 源起始 IP

您可以在这里输入用于此负载均衡策略的源起始 IP 地址。
- 源终止 IP

您可以在这里输入用于此负载均衡策略的源终止 IP 地址。如果这里为空白则意味着只有**源起始 IP** 项的 IP 地址会被应用到此负载均衡策略里。
- 目标起始 IP

您可以在这里输入用于此负载均衡策略的目标起始 IP 地址。
- 目标终止 IP

您可以在这里输入用于此负载均衡策略的目标终止 IP 地址。如果这里为空白则意味着只有**目标起始 IP** 项的 IP 地址会被应用到此负载均衡策略里。
- 目标起始端口

您可以在这里输入用于此负载均衡策略的目标起始端口。
- 目标终止端口

您可以在这里输入用于此负载均衡策略的目标终止端口。如果这里为空白则意味着只有**目标起始端口** 项的端口会被应用到此负载均衡策略里。

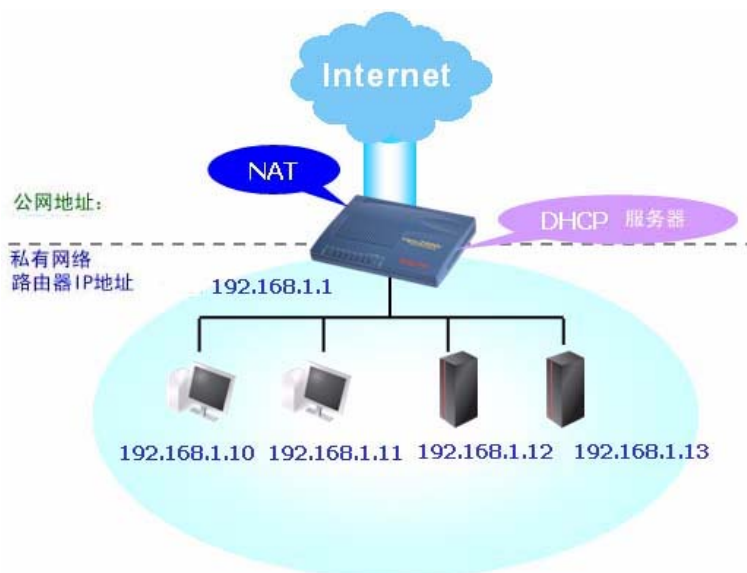
## 3.2 LAN

局域网这里指的是被路由器管理的内部子网。网络结构的设计与 ISP 提供的公网 IP 有关。

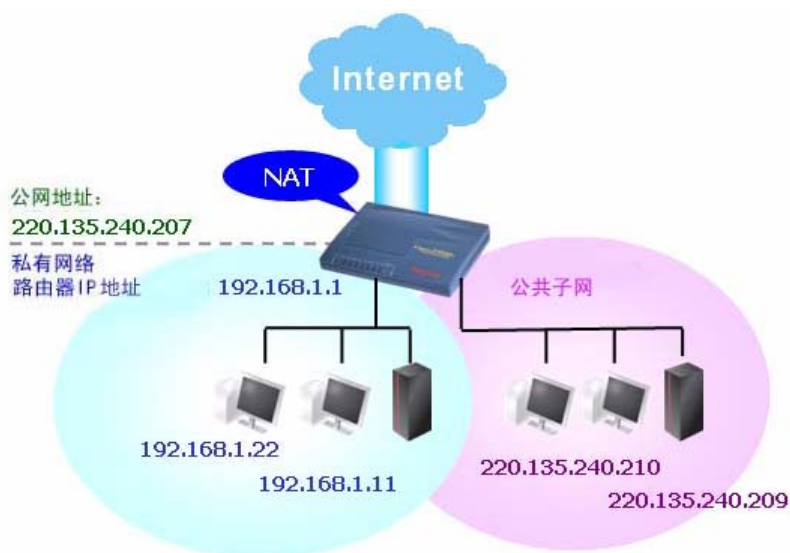


### 3.2.1 局域网基础

NAT 是 Vigor 路由器的基本功能。它创建并维护一个私有内部网络。根据前述，Vigor 路由器可以使用公网 IP 和 Internet 主机交流，同时可以使用私网地址和内网主机交流。NAT 的作用是将上行封包的私网地址转换成公网地址发出，数据下行时又进行反向的转换，将数据发送到正确的主机，从而实现了多个私网地址的主机分享同一个公网 IP 地址。Vigor 路由器还具有内置的 DHCP 服务器给主机分配私网 IP 地址。可参照下图进行一个简单的了解。



在某些特殊情况下，ISP 可能会多分配一个子网的公网地址，例如 220.135.240.0/24。这意味着内网可以有一个公网子网（第二子网）。作为第二子网的一部分，Vigor 路由器将为所有的内部公网主机做 IP 路由，使他们可以和 Internet 上的主机进行数据交换。因此，路由器是作为公网主机的网关而存在的。



## 什么是路由信息协议（RIP）

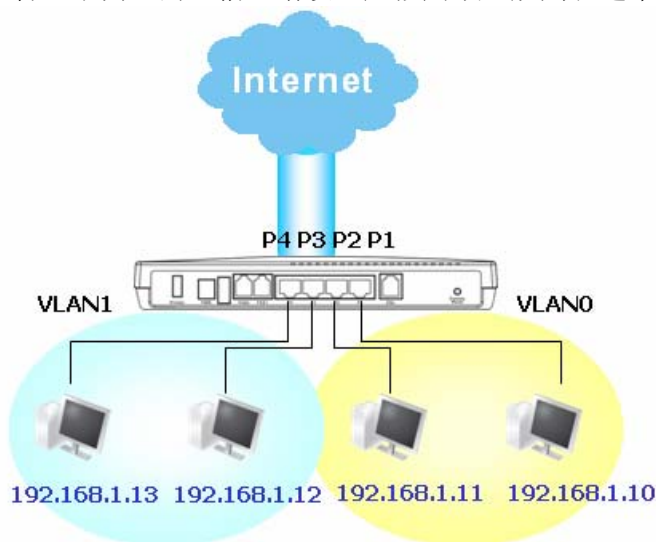
Vigor 路由器可以与临近的路由器进行路由信息的交换以实现 IP 路由。这一特性使得用户对 IP 地址等信息的改变可以自动互相通知。

## 什么是静态路由

当局域网内有多个子网时，更有效率，更快的方法是配置**静态路由**，使用静态路由器，可以在没有 RIP 的情况下，让路由器知道发到特定子网的数据应该通过哪个地址转发。

## 什么是虚拟局域网（VLAN）

您可以根据物理端口把局域网内的主机进行分组，最多可以创建 4 个虚拟局域网。为了管理不同组的通信，请设置虚拟局域网规则和速率控制。



### 3.2.2 基本设定

此页提供了局域网的基本设定。

点击**局域网**打开局域网设定并选择**基本设定**。

LAN >> 基本设定

TCP/IP和DHCP设定

局域网端IP网络设定

NAT子网

路由器第一子网IP地址192.168.1.1

第一子网掩码255.255.255.0

路由子网 ☐ 启用 ☒ 停用

路由器第二子网IP地址192.168.2.1

第二子网掩码255.255.255.0

第二子网DHCP服务器

RIP协议控制

停用

DHCP服务器设定

☒ 启用服务器 ☐ 停用服务器

DHCP 中继代理: ☐ 第一子网 ☐ 第二子网

起始IP地址192.168.1.10

IP池可分配IP数量50

网关IP地址192.168.1.1

中继代理使用的DHCP服务器IP地址

DNS服务器IP地址

☐ 强制使用设定的DNS

主DNS IP地址

副DNS IP地址

确定

- 第一子网 IP

输入路由器的私网 IP 地址（默认：192.168.1.1）。
- 第一子网掩码

输入子网掩码，来决定网络的大小（默认：255.255.255.0/ 24）。
- 路由子网

选择启用以使用此功能，默认设定是停用。
- 第二子网 IP

输入第二子网 IP 地址(默认: 192.168.2.1/ 24)
- 第二子网掩码

输入子网掩码，来决定网络的大小（默认：255.255.255.0/ 24）。
- 第二子网 DHCP 服务器

可以配置路由器为第二子网主机动态分配 IP 地址。

路由器Web界面设置程序

第二子网DHCP服务器

开始IP地址

IP池IP数0 (最多10个)

索引值

匹配的MAC地址

分配的IP地址

MAC地址:

添加

移除

编辑

取消

确定

全部清除

关闭

**开始 IP 地址：**输入第二子网可以 DHCP 分配的 IP 地址的起始地址。例如路由器地址为 220.135.240.1，那么开始 IP 地址就应该是 220.135.240.2 或更大值，但小于 220.135.240.254。

**IP 池 IP 数：**输入地址池中的 IP 数，最大值为 10。例如，如果



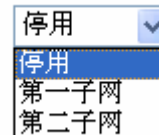
您输入 3，第二 IP 地址是 220.135.240.1，那么 DHCP 服务器签发的 IP 范围从 220.135.240.2 到 220.135.240.4。

**MAC 地址：**输入要添加的 MAC 地址，然后按**添加**创建列表，您也可以从 IP 池删除或者编辑 IP 地址。第 2 子网 DHCP 服务器将签发正确的 IP 地址到正确的主机。因此第 2 子网的主机不会获得属于第 1 子网的 IP 地址。

## RIP 协议控制

**禁用：**停用 RIP 协议。这将停止在路由器间进行路由信息的交换（默认）。

RIP协议控制



**第一子网** - 选择路由器与临近路由器交换第一子网的路由信息。

**第二子网** - 选择路由器与临近路由器交换第二子网的路由信息。

## DHCP 服务器设定

DHCP 即动态主机配置协议。路由器默认情况下开启了 DHCP 服务器功能，为接入的 PC 自动分配 IP 等相关的网络设定。如果您的网络中没有 DHCP 服务器，推荐您启用此功能。

如果想要使用其它的 DHCP 服务器，可以使用中继代理功能来转发 DHCP 信息到 DHCP 服务器。

**启用服务器** - 让路由器为每个主机分配 IP 地址。

**禁用服务器** - 手动分配 IP 地址给网内主机。

**中继代理** - （**第一子网/第二子网**）指定 DHCP 服务器所在的子网以便中继代理转发 DHCP 请求。

**起始 IP 地址** - 输入 IP 池可以分发的 IP 地址的第一个地址。如果路由器第一 IP 地址是 192.168.1.1，那么起始 IP 地址必须为 192.168.1.2 或更大，但小于 192.168.1.254。

**IP 池 IP 数** - 输入 DHCP 服务器最多可以分配的 IP 数。默认值为 50，最大为 253。

**网关 IP 地址** - 输入给 DHCP 服务器的网关 IP 地址，该值等同于路由器第一 IP 地址，即路由器是默认网关。

**中继代理使用的 DHCP 服务器 IP 地址** - 设定需要使用的外接 DHCP 服务器的 IP 地址。

## DNS 服务器设定

DNS 服务器域名解析服务器，每个网络主机都有唯一的 IP 地址，而他们也可以拥有人性化的，容易记忆的名字。例如，[www.yahoo.com](http://www.yahoo.com)。DNS 服务器就是用来将大家熟知的域名解析成 Internet 传输所需的 IP 地址。

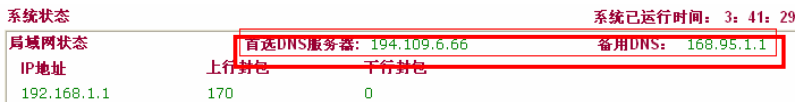
**强制使用设定的 DNS** - 迫使 Vigor2910 使用页面上提供的 DNS 服务器，而不使用由网络接入服务器提供的 (PPPoE, PPTP, L2TP 或 DHCP 服务器)。

**主 DNS IP 地址**- 此处必须指定 DNS 服务器 IP 地址，因为您的 ISP 通常会提供不止一个 DNS 服务器。如果您的 ISP 不提供 DNS 服务器，路由器将自动使用默认的 DNS 服务器 194.109.6.66。



**副 DNS IP 地址-** 您可以指定副 DNS 服务器 IP 地址, 因为您的 ISP 通常会提供不止一个 DNS 服务器。如果您的 ISP 不提供 DNS 服务器, 路由器将自动使用默认的副 DNS 服务器 194.98.1.1 。

默认 DNS 服务器 IP 地址可以在在线状态页面看到:



如果主 DNS 和副 DNS 都没有填, 路由器会在 DHCP 分配 IP 的时候将自己的 IP 地址作为 DNS 地址分配给主机, 同时充当 DNS 代理的角色, 并维护 DNS 缓存。

另外, 如果客户机发起的 DNS 请求在缓存里面已经有记录, 那么路由器会立即解析, 否则路由器将通过 WAN 口连接(例如 DSL/Cable)转发 DNS 请求到外部的 DNS 服务器。

第四章会具体介绍两种常见的局域网环境设定。关于配置, 您可以在第四章获得详细的信息。

3.2.3 静态路由

在局域网菜单下选择静态路由。

LAN >> 静态路由设定

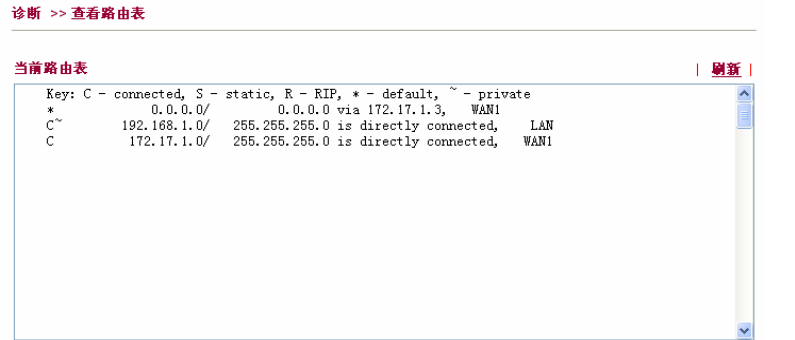
静态路由设定

[恢复出厂设置](#) | [查看路由表](#)

索引值	目标地址	状态	索引值	目标地址	状态
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

状态: v — 使用中, x — 未使用, ? — 空白

- 索引值
- 目标地址
- 状态
- 查看路由表
- 点击任何索引值(1 to 10)可以进入相应的静态路由设置页面。
- 显示静态路由的目标地址。
- 显示静态路由是否启用。
- 显示路由表, 供您参考。

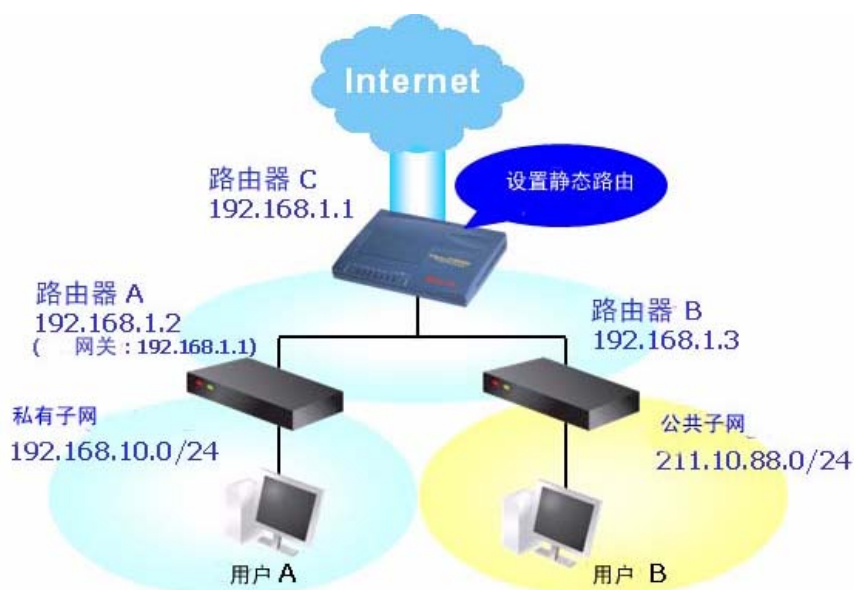


添加静态路由到私网或公网

下面为一个静态路由的范例，A 和 B 是不同子网中的设备，可以通过路由器相互通讯。假设网络已经配置完成，路由器正常工作。

- 使用主路由器访问 Internet
- 在内部路由器 A（192.168.1.2）上创建了一个私网 192.168.10.0
- 在内部路由器 B（192.168.1.3）上创建了一个公网 211.100.88.0
- 路由器 A 的默认网关为主路由器的 IP 192.168.1.1

设置静态路由前，用户 A 不能和用户 B 进行通信，因为 A 只会将数据包发到默认网关路由器 A。



1. 在**局域网的基本设定**中，选择第一子网作为 **RIP 协议控制**，然后点击**确定**。

**注释：**这里有两个原因需要在第一子网应用 RIP 协议。第一个是 LAN 端可以在第一子网内（192.168.1.0/24）与相邻的路由器交换 RIP 包；第二个是内部子网的主机（192.168.10.0/24）可以通过路由器访问到 Internet，并且还可以与不同的子网交换路由信息。

2. 点击**局域网 - 静态路由**然后点击**索引值 1**。添加下图所示的静态路由。该路由表示所有发到 192.168.10.0 的数据包都发向 192.168.1.2，点击**确定**。

LAN >> 静态路由设定

索引值编号 1

☒ 启用

目标IP地址	192.168.10.0
子网掩码	255.255.255.0
网关IP地址	192.168.1.2
网络接口	LAN

确定

取消

3. 返回到**静态路由设定**页面。点击另外一个**索引值**，添加另一条路由。该路由表示所有发到 211.100.88.0 网段的数据包都发送到 192.168.1.3。

LAN >> 静态路由设定

索引值编号 2

<input checked="" type="checkbox"/> 启用	
目标IP地址	211.100.88.0
子网掩码	255.255.255.0
网关IP地址	192.168.1.3
网络接口	LAN

确定

取消

4. 访问**诊断**并选择**路由表**以查看当前路由表。

诊断 >> 查看路由表

当前路由表

| 刷新 |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*      0.0.0.0/      0.0.0.0 via 172.17.1.3,   WAN1
C~     192.168.1.0/  255.255.255.0 is directly connected,   LAN
C      172.17.1.0/  255.255.255.0 is directly connected,   WAN1
```

## 删除静态路由

1. 请您到 **LAN** 设置菜单, 点击**静态路由**到设置页面, 选择进入您想要删除的索引号。
2. 请清空**目标 IP 地址**栏, 直接点击**确定**, 路由器将会自动删除此条静态路由。

## 3.2.4 绑定 IP 到 MAC

该功能用来将局域网内的 IP 地址和 MAC 地址进行绑定, 以便对网络加强管控。当启用该功能后, 如果修改 IP 或 MAC 地址, 将无法上网。

在**局域网**菜单下选择**绑定 IP 到 MAC** 打开配置页面。

LAN >> 绑定IP到MAC

绑定IP到MAC

注意：

IP-MAC绑定将会预设DHCP IP分配。  
如果选择了“强制绑定”，使用非列表中匹配的IP，MAC组合将无法接入Internet。

☒ 启用

☐ 禁用

☐ 强制绑定

ARP表

| 全选 | 排序 | 刷新 |

IP地址	MAC地址
192.168.1.101	00-E0-4C-97-61-9A

IP绑定列表

| 全选 | 排序 |

索引	IP地址	MAC地址
----	------	-------

添加和编辑

IP地址

MAC地址

添加

编辑

移除

确定

- 启用

功能处于启用设置状态,但是没有列在该列表中的IP/MAC 仍然能够上网。
- 禁用

禁用此功能，所有该页面设置将无效。
- 强制绑定

强制执行绑定，所有和列表中不匹配的 IP/MAC 对将无法上网。
- ARP 表

路由器的 ARP 表，会将现在开机的所有的 IP、MAC 信息显示出来。可以使用鼠标点击选择后，点击**添加**将选中的 IP/MAC 加入列表。使用 SHIFT/CTRL 键可以进行批量选择。
- 添加和编辑

IP 地址 – 输入给指定的 MAC 地址使用的 IP 地址

Mac 地址 – 输入绑定到 IP 地址的 MAC 地址
- 刷新

刷新 ARP 列表，当有新 PC 加入网络时，可以点刷新获得最新的 ARP 表信息。
- IP 绑定列表

显示已经加入绑定列表的 IP/MAC 信息。
- 添加

将 ARP 表中选中的项或**添加和编辑**中输入的项添加到 **IP 绑定列表**。
- 编辑

编辑和修改选定的 IP 地址和 MAC 地址。
- 移除

选中 **IP 绑定列表**中的项，然后点**移除**可以删除指定的项。

注释：

在选择**强制绑定**之前，请至少先绑定一台 PC 的 IP MAC 信息，否则，任一 PC 都会无法上网，并无法进入路由器配置页面。

### 3.3 NAT（网络地址转换）

通过 NAT（网络地址转换）技术，我们可以将一个或多个私网 IP 地址映像到一个公网 IP 地址。简单来说，NAT 是将一个网络中使用的 IP 地址转换为其它网络中的 IP 地址

一个是外部地址，一个是内部地址。当一个信息包从外部网络进入内部网络时，NAT 会将包中的目标地址信息转化为内网的 IP，代替其原来的值。

使用 NAT 技术一方面可以节省网络资源，防止公网 IP 地址枯竭，另一方面又可以增加内部网络的安全性，使其免遭外部网络的侵袭。在绝大多数情况下，Vigor 路由器是作为 NAT 路由器来使用的。当 NAT 后的主机访问外部网络时，从外部网络将无法看到这台主机的内网 IP 地址，通过路由器的 NAT 技术，外网只能看到由 ISP 提供的公网 IP 地址。通过这一方法，所有的内部主机都可以共享一个公网 IP 地址来同时访问 Internet。

NAT 的好处包括：

- 合理利用公网 IP 地址,节约公网 IP 的使用量。

通过 NAT, 路由器后局域网内的多个私网 IP 地址可以共享一个公网 IP 上网。

- 通过 NAT 保护路由器后局域网的网络安全。

目前有很多针对 IP 地址的攻击，但是这些攻击对 NAT 后的私网 IP 不会生效。

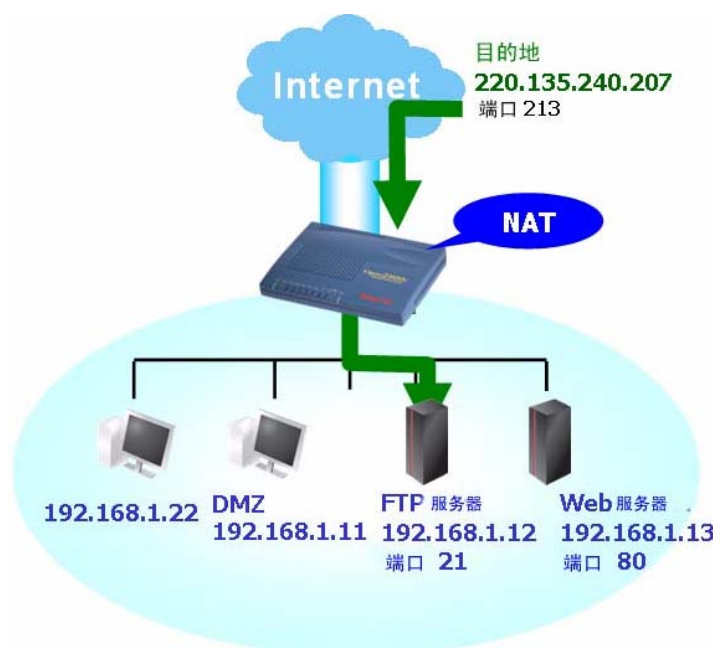
对于私网 IP 的定义，请参见 RFC-1918。我们一般将 192.168.1.0/24 作为路由器后局域网的网段 IP。NAT 功能是通过端口映射来实现的。

下面显示的是 NAT 目录



### 3.3.1 设定虚拟服务器

设定虚拟服务器功能通常用于为局域网内的服务器，如 web 服务器或者 FTP 服务器等设定端口映射。根据设定,发送到路由器外部特定端口的包会被映射到路由器内部服务器的特定端口。由于服务器位于路由器后的局域网，这样很好的保障了其网络安全。



设定虚拟服务器只应用在针对从外进来的数据包。

要使用此项功能，请点击 **NAT** 并选择**虚拟服务器**。设定**虚拟服务器**为内部主机提供了 10 条端口映射。

**NAT >> 设定虚拟服务器**

**虚拟服务器表**

#	模式	服务名称	协议	外部端口	私有 IP	私网端口	启用
1	范围		---	0 -		0	<input type="checkbox"/>
2	单一		---	0		0	<input type="checkbox"/>
3	单一		---	0		0	<input type="checkbox"/>
4	单一		---	0		0	<input type="checkbox"/>
5	单一		---	0		0	<input type="checkbox"/>
6	单一		---	0		0	<input type="checkbox"/>
7	单一		---	0		0	<input type="checkbox"/>
8	单一		---	0		0	<input type="checkbox"/>
9	单一		---	0		0	<input type="checkbox"/>
10	单一		---	0		0	<input type="checkbox"/>

**注意:** In "Range" Mode the End Port will be calculated automatically once the Start IP, End IP and Private Port have been entered.

- 模式** 有两个选项，对于特定“范围”设定，请选择范围。
- 服务名称** 输入该网络服务的名称。
- 协议** 选择一个传输层协议（TCP 或 UDP）。
- 外部端口** 指定某个**私网 IP** 和**端口**映射到的外部端口。
- 私有 IP** 指定提供服务的内部主机的私有 IP。
- 私网端口** 指定被映射的私网端口。
- 启用** 启用您所定义的该项端口映射。

请注意,路由器有自己的内置服务(服务器),比如 Telnet、HTTP and FTP 等等. 由于这些服务使用的端口可能会和局域网内的服务器使用的端口冲突,如果遇到这种情况,必须更改内置服务的使用端口。

举例来说, 如果您要在局域网建立一台 WEB 服务器使用 TCP 80 端口,则您必须把路由器的 **HTTP 通讯端口**由 80 改为其它值。

具体操作请点击**系统维护>>管理**。

**管理设定**

**管理接入控制**

☐ 启用远端固件升级 (FTP)

☒ 允许从Internet进行管理

☐ 禁止来自Internet的PING

**接入列表**

列表	IP	子网掩码
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

**管理通讯端口设定**

☐ 默认端口 (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)

☒ 用户自定义通讯端口

Telnet通讯端口

HTTP通讯端口

HTTPS通讯端口

FTP通讯端口

**SNMP设定**

☐ 启用SNMP代理程序

Get Community

Set Community

管理员主机IP

Trap Community

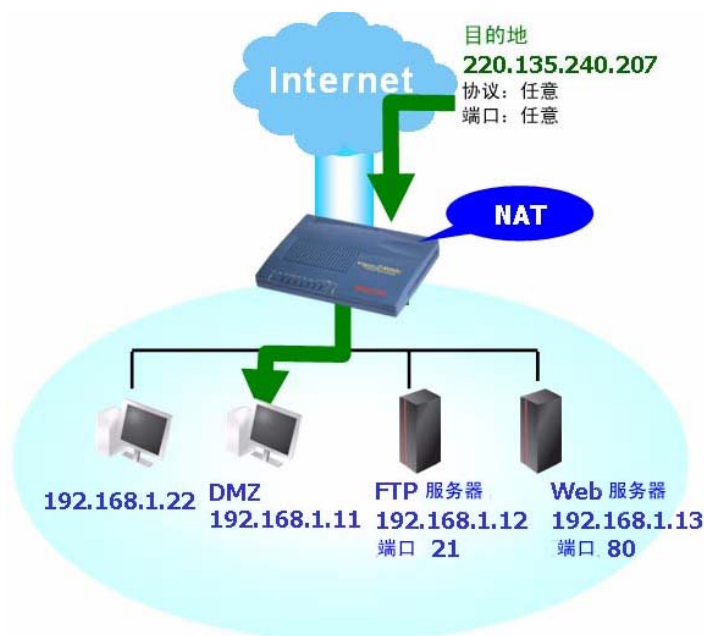
通知主机IP

Trap超时  秒

### 3.3.2 DMZ 主机设定

如前所述，**虚拟服务器设定**可以将进入方向的 TCP/UDP 数据的端口重定向到某个指定的私网 IP 地址。然后，有些 IP 协议，比如协议 50 (ESP) 和协议 51 (AH) 并不是使用固定的端口。Vigor 路由器提供了 DMZ 主机设定可以将任何主动进入的数据使用的端口映射到内部的某一个主机上。

**DMZ 主机**设定功能允许将一台预先设定好的内部主机完全暴露于公网之下，DMZ 主机设定适用于一些特定的功能比如视频会议或网络游戏。



我们建议您设定附加的 IP 过滤规则来保护开启 DMZ 功能的主机。

点击 **DMZ 主机设定**，显示如下页面：

DMZ主机设定

WAN 1

无

私有IP

实IP DMZ主机的MAC地址

00

00

00

00

00

00

选择PC

Note: 当一个实IP DMZ主机开启后，它将强制路由器的WAN口连接一直在线。

WAN 2

启用

私有IP

选择PC

确定

**DMZ 主机设定** 有三种类型的 DMZ 主机设定：**无**、**私有 IP** 和**启用实 IP**。如果选择**私有 IP**，可以使用**选择 PC** 来指定一台 PC 作为 DMZ 主机。如果选择**启用实 IP**，则可以输入实 IP DMZ 主机的 MAC 地址。

**WAN1** 您可以允许设定 **无**、**私有 IP** 和**启用实 IP**。

WAN 1

启用实 IP

无

私有IP

启用实IP

**私有 IP** 输入一个私网 IP 地址作为 DMZ 主机。点击此按钮将会有 一个窗口跳出，其中包含了您的内部私网的所有开启主机的 IP 地址，选择其中之一作为 DMZ 主机。

**实 IP DMZ 主机的 MAC 地址** 如果您选择了**启用实 IP**，请输入实 IP DMZ 主机的 MAC 地址。

如果您已经在先前在WAN1 界面里设定**WAN IP 别名**，同时配置**PPPoE, Static or Dynamic IP or PPTP**（通过WAN >> Internet接入），您可以在**辅助 WAN IP**里进行选择。

NAT >> DMZ主机设定

DMZ主机设定

WAN 1

索引	启用	辅助 WAN IP	私有IP	
1.	<input type="checkbox"/>	172.17.1.11	<input type="text"/>	选择PC
2.	<input type="checkbox"/>	172.17.1.55	<input type="text"/>	选择PC
3.	<input type="checkbox"/>	218.18.26.98	<input type="text"/>	选择PC

WAN 2

启用

私有IP

选择PC

确定

清除

**启用** 点击启用 DMZ 功能。

**私有 IP** 输入一个私网 IP 地址作为 DMZ 主机。

50

Vigor2910 系列中文手册



**选择 PC** 点击此按钮将会有有一个窗口跳出,其中包含了您的内部私网的所有开启主机的 IP 地址, 选择其中之一作为 DMZ 主机:



选择完毕后, 点击**确定**完成设定。如果要开启 DMZ 的主机没有打开, 也可以通过手动输入的形式完成设定。

NAT >> DMZ主机设定

DMZ主机设定

WAN 1				
索引	启用	辅助 WAN IP	私有IP	
1.	<input checked="" type="checkbox"/>	172.17.1.11	<input type="text"/>	<input type="button" value="选择PC"/>
2.	<input type="checkbox"/>	172.17.1.55	<input type="text"/>	<input type="button" value="选择PC"/>
3.	<input type="checkbox"/>	218.18.26.98	<input type="text"/>	<input type="button" value="选择PC"/>

WAN 2

启用

☐

私有IP

确定

清除

### 3.3.3 开放端口设定

开放端口设定允许您为一些特殊的应用服务打开一段范围内的端口。

开放端口普遍应用在 P2P 应用程序（如：BT, KaZaA, Gnutella, WinMX, eMule），网络视频等。为了避免任何不必要的安全隐患，您始终要确保更新相关的应用程序。

点击**开放端口设定**，显示如下页面：

NAT >> 开放端口

开放端口设定

恢复至出厂默认设置

索引	注解	WAN接口	本地IP地址	状态
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >>

下一页 >>

- 索引

显示了个相关条目的号码，需要点击索引号才能进行编辑。
- 注解

显示指定的网络服务的名称。
- WAN 接口

显示输入的 WAN 接口。
- 本地 IP 地址

显示提供服务的内部主机的私网 IP 地址。
- 状态

显示当前条目的状态。用 x 表示未启用，v 表示已启用。

要添加或修改此项功能，请点击设置页面的索引号，会跳出如下窗口。并且在每项设置里，可以为不同的服务提供 10 条区段端口映射。

索引值编号 1

☒ 启用开放端口

注解

WAN接口

WAN IP

本地计算机

p2p

WAN1

172.17.1.11

192.168.1.34

选择PC

	协议	起始端口	终止端口		协议	起始端口	终止端口
1.	TCP	4500	4700	6.		0	0
2.	UDP	4500	4700	7.		0	0
3.		0	0	8.		0	0
4.		0	0	9.		0	0
5.		0	0	10.		0	0

确定

清除

取消

- 启用开放端口

点击启用此项。
- 注解

输入所定义的网络服务的名称。

<b>WAN Interface</b>	显示输入的 WAN 接口。
<b>WAN IP</b>	从下拉菜单中选择一个 WAN IP 地址。这个选择是有效的并且显现的 WAN IP 是先前在 WAN IP 别名中设定的那些 IP。
<b>本地计算机</b>	输入内网主机的私网 IP。
<b>选择 PC</b>	点击此按钮将会有有一个窗口跳出，其中包含了您的内部私网的所有主机的 IP 地址，选择其中之一作为启用开放端口的主机。
<b>协议</b>	选择一个传输层的协议，此处可选 <b>TCP</b> 或者 <b>UDP</b> 。
<b>起始端口</b>	为本地的主机所提供的开放端口功能指定一个开始端口。
<b>终止端口</b>	为本地的主机所提供的开放端口功能指定一个终止端口。

### 3.4 对象与组

Vigor 路由器支持基于**组**配置防火墙策略。我们可以将 IP 地址、服务、端口定义为不同的对象组，这样就可以减少策略规则的数量，简化策略配置的复杂性。譬如，公司有研发，生产，销售，管理等四个部门，您就可以把这四个部门的 IP 地址归为四个 IP 对象；这四个 IP 对象又可以分别设到不同的 IP 组里。在设定 IP 过滤器规则的时候就可以基于 IP 对象或 IP 组来统一设定。

除了 Vigor 路由器能够定义 IP 对象和组，还可以定义服务类型对象和组。这里服务类型指的是协议（TCP，UDP，ICMP，IGMP 以及 IP 协议）及相应的端口。在设定 IP 过滤器规则的时候就可以基于服务类型对象或组来统一设定。同时，Vigor 路由器除了按照协议设定防火墙策略，还能够提供了内容安全管理策略。它以应用程序为对象，譬如即时通讯程序：MSN，QQ，Skype 等，以及 P2P 下载软件：eMule，BitTorrent 等。

综上所述，Vigor 路由器可以以 IP 对象（或组）为对象，设定允许（或禁止）使用的服务类型对象（或组），以及禁止使用的应用程序。显而易见的，基于对象的管理可以为我们日常维护管理中带来极大方便。例如，人员的变动，导致策略的改变，您可以很方便地通过调整所定义的相应对象即可。



#### 3.4.1 IP 对象

这里您可以设定最多 192 个 IP 对象。

[对象设定](#) >> [IP对象](#)

IP对象设定档: 恢复至出厂默认设置

索引	名称	索引	名称
<a href="#">1.</a>	HR	<a href="#">17.</a>	
<a href="#">2.</a>	Development	<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >>

[下一页](#) >>

[恢复至出厂默认设置](#)      清除所有的设定档。

点击[索引号](#)，进入设定页面。

设定档索引：1

名称:	HR
接口:	LAN
地址类型:	地址范围
起始地址:	172.17.1.20
终止地址:	172.17.1.30
子网掩码:	0.0.0.0
反选:	<input type="checkbox"/>

确定

取消

名称

键入设定档的名称，譬如 Sales。最多 15 个字符。

接口

选择正确的接口（WAN，LAN 或 Any）。

接口:

LAN

所有

LAN

WAN

例如，在**过滤器设定**页面里，您需要在**方向**选项里选择一个方向（**LAN -> WAN** 或 **WAN -> LAN**）。如果选择 **LAN -> WAN**，那么在源 IP 栏点击**编辑**按钮，在弹出窗口里，您可以选择的 IP 对象（或组）就只有接口定义为 LAN 的 IP 对象（或组）；而在目标 IP 的**编辑**窗口里可以选择的 IP 对象（或组）就只有接口定义为 WAN 的 IP 对象（或组）。

Address Type

定义 IP 地址的类型。

**任意地址**：对象是任意 IP 地址。

**单一地址**：对象只包含了一个 IP 地址。

**地址范围**：对象包含了一组连续的 IP 地址。

**子网掩码**：对象包含了某个子网的 IP 地址。

起始地址

选择 **Single Address** 的时候，在这里输入对应的 IP 地址；选择 **Range Address** 的时候，在这里输入 IP 地址段的起始 IP 地址；选择 **Subnet Address** 的时候，在这里输入该子网里所包含的任意一个 IP 地址。

终止地址

选择 **Range Address** 的时候，在这里输入 IP 地址段的终止 IP 地址。

子网掩码

选择 **Subnet Address** 的时候，在这里输入该子网的掩码。

反选

选择此项，对所设定的 IP 地址以外的地址起效。

下面是 IP 对象设定的举例：

## 对象设定 >> IP对象

IP对象设定档:

索引	名称	索引
<a href="#"><u>1.</u></a>	HR	<a href="#"><u>17.</u></a>
<a href="#"><u>2.</u></a>	Development	<a href="#"><u>18.</u></a>
<a href="#"><u>3.</u></a>		<a href="#"><u>19.</u></a>
<a href="#"><u>4.</u></a>		<a href="#"><u>20.</u></a>
<a href="#"><u>5.</u></a>		<a href="#"><u>21.</u></a>

3.4.2 IP 组

在这里您可以把 IP 对象绑定到不同的组里。

对象与组 >> IP组

IP组列表: 恢复至出厂默认设置

索引	名称	索引	名称
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

恢复至出厂默认设置 清除所有的设定档。

点击索引号，进入设定页面。

对象设定 >> IP组

设定档索引: 1

名称: 不能上网

接口: 所有

可用IP对象

1-HR  
2-Development

>>

<<

被选定IP对象

确定

取消

- 名称

键入设定档的名称，譬如 Sales。最多 15 个字符。
- 接口

选择 WAN, LAN 或 Any，对应的 IP 对象将被列出在选框里。
- 可用 IP 对象

根据选择的接口类型，对应的所有可选 IP 对象都列在选框里。
- 被选定 IP 对象

点>>按钮将对应的 IP 对象加入该 IP 组。

3.4.3 服务类型对象

这里您可以设定最多 96 个服务类型对象。

对象与组 >> 服务类型对象

服务类型对象设定档: | 恢复至出厂默认设置 |

索引	名称	索引	名称
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 >> 下一页 >>

恢复至出厂默认设置 清除所有设定档。

点击索引号，进入设定页面。

对象设定 >> 服务类型对象设置

设定档索引: 1

名称

不能访问web

协议

TCP 6

源端口

= 1 ~ 65535

目标端口

= 80 ~ 65535

确定 取消

名称 键入设定档的名称。

协议 选择想要配置的协议。

TCP 6

Any  
ICMP  
IGMP  
TCP  
UDP  
TCP/UDP  
Other

源/目标端口 源端口和目标端口仅对 TCP 和 UDP 协议有效。其它协议不使用端口信息。有效的端口定义如下：

(=) – “等于”。当前后两个值相等的时候，表示使用一个端口；如果前后两个值不同，表示这两个端口号（包括这两个端口）之间的所有端口号。

(!=) – “不等于”。当前后两个值不同的时候，这里定义的有效端口是除这个端口外的所有端口。当前后两个值不同的



时候，这里定义的有效端口是除去该端口范围外的所有端口。  
(>) – “大于”。这里定义的有效端口是大于该值的所有端口号。  
(<) – “小于”。这里定义的有效端口是小于该值的所有端口号。

下面是一个设定的举例。

对象设定 >> 服务类型对象

服务类型对象设定档：

索引	名称
<a href="#">1.</a>	不能访问web
<a href="#">2.</a>	不能访问FTP
<a href="#">3.</a>	
<a href="#">4.</a>	

3.4.4 服务类型组

在这里您可以将服务类型对象绑定到不同的组里。

对象与组 >> 服务类型组

服务类型组列表：

[恢复至出厂默认设置](#)

组	名称	组	名称
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

恢复至出厂默认设置          清除所有设定档。

点击索引号，进入设定页面。

设定档索引: 1

名称:

禁止

可用服务类型对象

1-不能访问web  
2-不能访问FTP

被选定服务类型对象

>>

<<

确定

取消

- 名称

键入设定档的名称。
- 可用服务类型对象

所有定义的服务类型对象都在这里列出了。
- 被选定服务类型对象

点>> 按钮将服务类型对象加入组。

3.4.5 CSM 设定档

您可以定义不同的策略包含不同的 IM（即时通讯软件）/P2P（点对点传输软件）组合。您可以在过滤器规则里选择这些设定档。

内容安全管理设定档列表:

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

16.

名称

17.

18.

19.

20.

21.

22.

23.

24.

25.

26.

27.

28.

29.

30.

31.

32.

名称

恢复至出厂默认设置

- 恢复至出厂默认设置

清除所有设定档。
- 点击索引号，进入设定页面。

设定档索引：1

设定档名称:

勾选以屏蔽:

即时聊天软件 (IM)		VoIP
<input type="checkbox"/> MSN	<input type="checkbox"/> Yahoo Messenger	<input type="checkbox"/> ICQ
<input type="checkbox"/> AIM	<input type="checkbox"/> QQ	<input type="checkbox"/> iChat
<input type="checkbox"/> Google Talk		<input type="checkbox"/> jajah
<input type="checkbox"/> Web IM (http://www.e-messenger.net/)		<input type="checkbox"/> Skype
<input type="checkbox"/> Web MSN (http://webmessenger.msn.com/)		

P2P	
协议	应用程序
<input type="checkbox"/> SoulSeek	SoulSeek
<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza
<input type="checkbox"/> FastTrack	Kazaa, iMesh
<input type="checkbox"/> Gnutella	BearShare, Limewire, Shareaza
<input type="checkbox"/> BitTorrent	BitTorrent

设定档名称                      输入设定档名称。

这里您可以选择禁止用户使用的程序。包括即时通讯软件和 P2P 下载应用。您只要点选相关的应用名称，并点击**确定**键。然后，在防火墙的**过滤器配置规则**里，就能在**内容安全管理**的下拉菜单里选择这些设定档。

## 3.5 防火墙

### 3.5.1 基本防火墙设定

当宽带用户在享受网络多媒体服务、交互式应用程序或远程学习时，安全一直是他们最关切的问题。Vigor2910 路由器的防火墙功能可以帮助您的本地网络防范来自外界的非  
法攻击。它也可以用于限制本地用户访问 Internet。此外，它还可以用于过滤掉某些能触发路由器向外界建立联接的数据包，而在有些时候，这种联接是用户并不需要的。

最基本的安全观念就是在安装路由器的时候设置用户名和密码，使得只有网络管理员才能访问路由器的配置页面，杜绝其它未经授权的非法访问。

快速开始向导

输入登录密码

请输入一个字母或数字组成的字符串作为您的 **密码**（最多23个字符）。

新密码

确认密码

< 返回

下一步 >

完成

取消

如果您忘了在安装路由器的时候设置密码，您还可以去**系统管理**选项里设置您的密码。

系统管理 >> 管理员密码设定

管理员密码

原密码

新密码

重新输入新密码

确定

### 防火墙工具

处于 Vigor2910 路由器 LAN 里的用户享有以下防火墙防护工具：

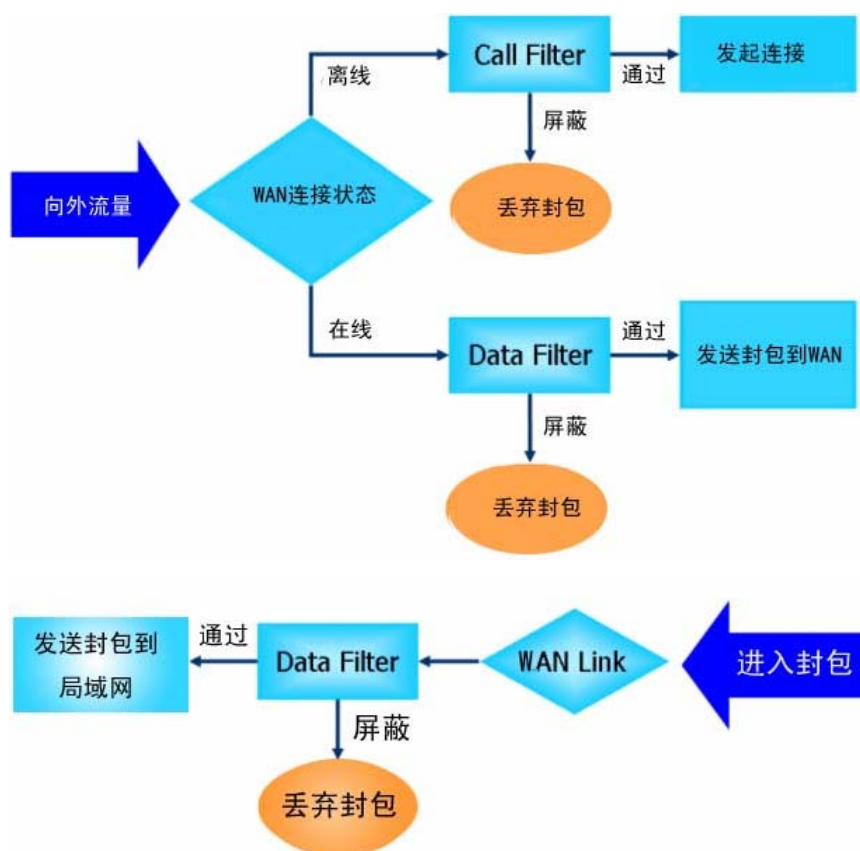
- 可供用户自由配置的 IP filter 规则(Call Filter/ Data Filter)
- 状态包检测(SPI)：它能够追踪数据包并能拒绝一切未经许可的主动连接数据
- 可供用户自由选择的攻击防御功能(DoS)，以及分布式攻击防御功能(DDoS)
- URL 内容过滤器

## IP 过滤概述

根据是否存在 Internet 连接或者 WAN 口状态是连接还是未连接, 可以将 IP 过滤分为两种: 一种是**呼叫过滤器**, 另一种是**数据过滤器**。

- **呼叫过滤器**: 当路由器没有连接 Internet 时, **呼叫过滤器**用于检查所有外出的数据流。它将根据用户设定好的过滤规则检查数据包。如果是规则允许的, 数据就被允许通过。然后路由器就会“**发起一个呼叫**”以建立 Internet 连接, 并将此数据包发送到 Internet。
- **数据过滤器**: 当路由器已经连接了 Internet 时, **数据过滤器**就用于检查进出的数据。它将根据用户设定好的过滤规则检查数据包。如果是规则允许的, 数据就被允许通过。

下面的流程图用于解释路由器如何处理进出的数据包。



## 状态包检测(SPI)

状态检测是一种工作在网络层的防火墙功能。和传统的状态包过滤不同, 它是基于包头信息检测的。状态检测增进了状态机制以追踪穿越防火墙每个连接, 并确认它们是有用的。Vigor2910 路由器的状态检测机制不仅检测头信息, 而且监视连接状态。

## 内容安全管理(CSM)

当各种即时聊天软件的不断涌现并逐渐流行起来的时候, 通讯就变得不那么容易了。然而, 当一些行业以此做为联系客户的一种利器时, 另一些行业则因为要减少他们的雇员在上班时间滥用这些软件而影响正常工作或者为了防止造成一些未知的安全漏

洞，而对此持保留态度。这和有些公司对待 P2P 软件的态度一样的，虽然文件共享为大家带来的便利，但与之相关的安全问题也同样令人堪忧。为了解决用户在这方面的困扰，Vigor2910 路由器适时的提供了内容安全管理功能（CSM）。

## 攻击防御功能 (DoS)

**DoS 防御**功能可以帮助您侦测并缓和 DoS 攻击。这些攻击通常分为两种，即 flooding-type 攻击和 vulnerability 攻击。前者是一种企图耗尽您的系统资源的攻击方式，后者则是攻击通讯协议或作业系统的弱点从而使整个系统瘫痪。

**DoS 防御**功能能使 Vigor2910 路由器对照攻击特征资料库检查每个流入的封包。任何可能使主机瘫痪的封包会被封锁，此时如果您已设置了 Syslog 服务器，一个系统记录会被作为警告马上被发送出去。

Vigor2910 路由器也会监视流量的变化，任何违反设定好的规则的不正常的流量，例如极限数，都会被当作攻击，并且 Vigor2910 路由器会实时的启用它的防御体系来减轻攻击。

下面显示的是 DoS 攻击防御功能所能够侦测出的攻击类型。

- |                  |                      |
|------------------|----------------------|
| 1. SYN flood 攻击  | 9. Smurf 攻击          |
| 2. UDP flood 攻击  | 10. SYN flood 攻击     |
| 3. ICMP flood 攻击 | 11. ICMP 分片攻击        |
| 4. TCP Flags 扫描  | 12. Tear Drop 攻击     |
| 5. 路由追踪          | 13. Fraggle 攻击       |
| 6. IP 选项         | 14. Ping of Death 攻击 |
| 7. 不明封包通讯协定      | 15. TCP/UDP 端口扫描     |
| 8. Land 攻击       |                      |

## URL 内容过滤

为了提供一个合适的网络空间给用户，Vigor2910 路由器配备了 **URL 内容过滤**功能，它不仅可以用于限制非法访问不当网站，也可以用于禁止那些隐藏了恶意代码的网站。

当用户输入或点击一个已经存在于 URL 内容过滤里的链接时，URL 关键字阻塞工具将会拒绝 HTTP 请求，该网页也会被限制访问。您可以把 **URL 内容过滤**想象成一个训练有素的便利店员不会将成人杂志卖给十几岁的孩子一样。同样，在办公室里，**URL 内容过滤**也能够提供一个和工作有关的环境，以提高雇员的工作效率。怎么样才能使 URL 内容过滤在过滤领域比传统的防火墙工作的好呢？因为它检查 URL 字符串或是 HTTP 数据的一些 TCP 数据的附载，而传统防火墙则只是基于 TCP/IP 包头来检查数据包。

另一方面，Vigor2910 路由器可以阻止用户意外的下载来自网页里的恶意代码。恶意代码包含在可执行文件里这是十分常见的，比如 ActiveX，Java 程序，压缩文件以及其它可执行文件。当您从网站上下载这些类型的文件时，这将会对您的系统带来威胁。例如，ActiveX 控件常常被用于提供交互式的网页特性。如果恶意代码隐藏在里面的话，它将占据用户的系统。

## Web 内容过滤

众所周知，有时候 Internet 上某些内容，比如某些类型的媒体有时是不健康的。作为负责任的父母或老板，您应该禁止他们访问。拥有 Vigor2910 路由器的 Web 内容过滤服务，您就可以保护您的生意免于这些公共的首要威胁，比如生产力，法律责任，网络安全威胁。而对于父母来说，您也可以保护您的孩子避免访问成人网站或聊天室。

当您开启了 Vigor2910 路由器上的 Web 内容过滤服务，并且设置了您想要限制的网站的分类，每一个 URL 地址请求将会依照由 SurfControl 提供的服务器数据库的记录来检查。这个数据库里包含了超过 70 种语言以及 200 个国家，超过 10 亿个网页，并将其分成 40 种容易理解的类别。这个数据库每天都会由 Internet 研究员的全球小组更新。这个服务器将查寻 URL 并返回一个类型给您的路由器。您的 Vigor2910 路由器然后将会根据您的类别以决定是否允许访问这个网站。请注意，这个部分将不会引入任何的延迟在您要访问的网站里，因为每一个多种负载平衡数据库服务器可以处理数百万的分类请求。

下面显示的是防火墙菜单。



### 3.5.2 基本设定

基本设定允许您调整 IP 过滤的设置以及其它常用选项。在这里，您可以开启或关闭**呼叫过滤**或**数据过滤**。在一些环境下，您的过滤规则可以连接到一系列方式下工作。所以在这里，您可以只指派**起始过滤器集**。同样，您可以设置**日志标记设定**，对下行 VPN 数据应用 IP 过滤，以及接受大 UDP/ICMP 封包分片进入。

点击**防火墙**，并点击**基本设置**可以打开基本设定页面。

防火墙 >> 基本设定

基本设定

拨号过滤器	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用	起始过滤器	集#1
数据过滤器	<input checked="" type="radio"/> 启用 <input type="radio"/> 停用	起始过滤器	集#2

---

默认规则动作:

功能	动作/设定档	记录日志
过滤器	通过	<input type="checkbox"/>
内容安全管理 (CSM)	无	<input type="checkbox"/>

---

☐ 对流入的VPN数据应用过滤规则

☒ 接受大UDP/ICMP封包分片进入 (常用于某些游戏, 例如CS)

确定 取消

拨号过滤器

点击**启用**来激活拨号过滤器，并指定起始过滤器组别。

数据过滤器

点击**启用**来激活数据过滤器，并指定起始过滤器组别。

记录日志

为了及时发现并维修故障，请点选记录日志。

在**过滤器**后，点选**记录日志**，路由器系统日志将记录此应用；不点选此项，路由器系统日志将不记录此应用。

在**内容安全管理**后，点选**记录日志**，路由器系统日志将记录此

应用；不点选此项，路由器系统日志将不记录此应用。

**注释：**当您输入“**log -f**”指令后，过滤器和内容安全管理的记录会显示在 Telnet 终端机上。

## 过滤器

请在此项选择对于不匹配过滤规则的封包的处理方法，是让其**通过**还是立即**封锁**。

## 内容安全管理

在这里选择您不允许使用即时通讯软件或是 P2P 软件的安全组别，这样以来处于安全组里的所有 PC 都不能使用您在安全组里设置的禁止使用的即时通讯软件或是 P2P 软件。关于安全组别的设置，请您参阅相关的章节。

一些在线游戏（比如 CS）会使用大量的 UDP 碎片包来传输游戏数据。而作为一个安全的防火墙，Vigor2910 路由器会本能的拒绝这些碎片包以防止攻击，除非您启用“**接受大 UDP/ICMP 封包分片进入**”。通过启用这项功能，您就可以随心所欲地玩各种在线游戏了。而如果您考虑更多的是安全因素的话，可以禁用**此项**。



3.5.3 过滤器设定

点击**防火墙**，并点击**过滤器设定**以打开设置页面。

防火墙 >> 过滤器设定

过滤器设定				恢复出厂设定	
设定集	注解	设定集	注解		
<u>1.</u>	Default Call Filter	<u>7.</u>			
<u>2.</u>	Default Data Filter	<u>8.</u>			
<u>3.</u>		<u>9.</u>			
<u>4.</u>		<u>10.</u>			
<u>5.</u>		<u>11.</u>			
<u>6.</u>		<u>12.</u>			

想要编辑或增加一个过滤，请点击设定的数字以编辑单个设定，接着会出现下面的页面。每个过滤设定包含了最多 7 条规则。点击规则号按钮来编辑每一条规则。检查是否已启用来启用这条规则。

防火墙 >> 过滤器设定 >> 编辑过滤器集

过滤器设定集 1

注解:

过滤器规则	启用	注解	上移	下移
<div>1</div>	<input checked="" type="checkbox"/>	Block NetBios		<a href="#">向下</a>
<div>2</div>	<input type="checkbox"/>		<a href="#">向上</a>	<a href="#">向下</a>
<div>3</div>	<input type="checkbox"/>		<a href="#">向上</a>	<a href="#">向下</a>
<div>4</div>	<input type="checkbox"/>		<a href="#">向上</a>	<a href="#">向下</a>
<div>5</div>	<input type="checkbox"/>		<a href="#">向上</a>	<a href="#">向下</a>
<div>6</div>	<input type="checkbox"/>		<a href="#">向上</a>	<a href="#">向下</a>
<div>7</div>	<input type="checkbox"/>		<a href="#">向上</a>	

下一个过滤器集 

无

确定

清除

取消

- 过滤器规则

点选 1~7 的数字按钮编辑过滤器规则。点击这些按钮将打开编辑过滤规则页面。关于详细的信息，请参照下面的页面。
- 启用

启用或停用过滤器规则。
- 注解

输入过滤器注解描述，最多输入 23 个字符。
- 上移/下移

您可以通过点击[向上](#)或[向下](#)项来将当前的过滤规则上移或下移。
- 下一个过滤器集

在执行完当前过滤设置之后，设置连接到下一个过滤器设定继续执行。注意，请不要设置成循环的顺序。

为了编辑**过滤器规则**，点击**过滤规则**索引按钮进入过滤规则设置页面。

**过滤器集 1 规则 1**

☒ 启用此规则

注解: Block NetBios

索引 (1-15) **计划任务** 设置: , , ,

---

方向: LAN -> WAN

源地址: Any 编辑

目标地址: Any 编辑

服务类型: TCP/UDP, Port: from 137~139 to any 编辑

分片: 忽略

---

**应用**

过滤器: 立即封锁

链接到其他过滤器集: 无

**内容安全管理:** 无

**动作/设定档**

**系统日志**

☐

☐

确定 清除 取消

**启用此规则**

点此项启用此功能。

**注解**

输入过滤器组别注解描述，最多输入 14 字符。

**索引(1-15)**

您可以在这里设置此过滤规则在哪个时间段起效。您最多可以在这里设置 4 个计划任务号，不过在此之前，您需要在**应用程序**下**计划任务**页面做好相关设置。默认情况下，这里是空白的，即此过滤规则在任何时间都有效。

**方向**

您可以在方向选项里选择数据包的流经方向是从 LAN->WAN 还是从 WAN->LAN。这一项只对**数据过滤**有效。对于**拨号过滤**，尽管**拨号过滤**只是用于外出的数据包，但是此项设置仍然不可用。

**源/目标地址**

点击**编辑**进入到下面的对话框以选择源和目的 IP 或 IP 地址范围。

http://172.17.1.11 - IP地址编辑 - Microsoft Internet Explorer

**IP地址编辑**

**地址类型** 组与对象

---

起始地址 0.0.0.0

终止地址 0.0.0.0

子网掩码 0.0.0.0

反选 ☐

**IP组** 无

**或 IP对象** 无

或IP对象 无

或IP对象 1-HR

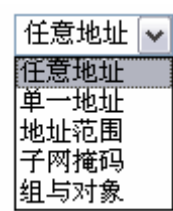
或IP对象 2-Development

确定 关闭

Done Internet

您可以在这里手动选择**所有 IP 地址**、**单个 IP 地址**、**IP 地址范围**或是**子网地址**作为地址类型，然后请到相应的项目里输入您

想要设置的地址。另外，如果您想要使用您在组类别里自己定义的 IP 地址范围，那么您可以在这里选择**组类别**选项。



请您从 **IP 组** 下拉菜单中选择一个您想要应用在此过滤规则的组别。或者您也可以在 **IP 类** 下拉菜单中选择一个您想要应用在此过滤规则的类别。

服务类型

点击**编辑**按钮进入到下面的对话框来设置适当的服务类型。



如果您想要手动设置服务类型，请在服务类型里选择用户自定义，然后在相关的对话框里输入您的设定。另外，如果您想要使用在组或类里设置的服务类型，请在此项选择**组和类**。



**协议** – 请在这里设置应用于此过滤规则的协议类型。

**源/目的端口** -

(=) -如果终止端口不填，过滤规则将只适用于起始端口所填的端口；若有填入数值，则过滤规则适用于从起始端口起到终止端口终止的所有端口。

(!=) -如果终止端口不填，过滤规则将只不适用于起始端口所填的端口；若有填入数值，则过滤规则不适用于从起始端口起到终止端口终止的所有端口。其它的端口都适用。

(>) -过滤规则适用于所有端口大于等于起始端口的端口。

(<) -过滤规则适用于所有端口小于等于起始端口的端口。

**服务组/类** -在这里的下拉菜单里选择您想要应用的组类别。

分片

指定处理数据包时对分片数据的处理。它只用于数据包过滤。

**忽略** -过滤规则适用于所有的封包切割形式。

**完整无分片** - 过滤规则适用于没有被切割的封包。

**片段** - 过滤规则适用于被切割的封包。

**太短** - 过滤规则适用于太短的封包。

## 过滤器

设定当封锁包符合条件时所采取的动作。

**立刻通过** - 当封锁包符合条件时立刻放行。

**立刻封锁** - 当封锁包符合条件时立刻丢弃。

**若无其他规则符合则通过** - 当封锁包只符合此规则，不符合其它规则时被通过。

**若无其他规则符合则封锁** - 当封锁包只符合此规则，不符合其它规则时会封锁。

## 连接到其它过滤器集设定

如果封包符合此规则，则跳过余下的规则而直接用所选规则作为下一条规则。请注意，如果路由器在执行完指定的规则之后将不再返回到之前的过滤规则了。

## 系统日志

在此点选启动记录功能。当您输入“log -f”指令后，过滤器的记录会显示在 Telnet 终端机上。

## 内容安全管理

所有在配置范围内的主机遵循 CSM 里的设置规则来执行。关于详细的设置，请您参阅相关的章节。

## 举例

在设置之前，所有的数据流将会被分别成为两种 IP 过滤器的一种：呼叫过滤器或数据过滤器。您可以预先设置 12 个呼叫过滤器和数据过滤器在过滤器设置里，并且可以将它们连接到一系列其它的过滤规则里。每一条过滤集由 7 个过滤规则组成，也可以进一步定义。之后，在**基本设定**里，您可以指定一个过滤集给呼叫过滤器，一个过滤集给数据过滤器。

# Firewall >> General Setup

## General Setup

Call Filter ☒ Enable  
☐ Disable

Start Filter Set Set#1

Data Filter ☒ Enable  
☐ Disable

Start Filter Set Set#2

Log Flag None

Actions for packet not matching any rule:

Pass or Block Pass

Content Management None

☐ Apply IP filter to VPN incoming packets

☒ Accept large incoming fragmented UDP or ICMP p

OK

Clear

## Firewall >> Filter Setup

### Filter Setup

Set	Comments	Set	Comments
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

## Firewall >> Filter Setup >> Edit Filter Set

### Filter Set 1

Comments: Default Call Filter

Filter Rule	Active	Comments
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

OK

Clear

## Firewall >> Edit Filter Set >> Edit Filter Rule

### Filter Set 1 Rule 1

☒ Check to enable the Filter Rule

Comments: Block NetBios

Index(1-15) in Schedule Setup: , , ,

Direction: LAN -> WAN

Source IP: Any Edit

Destination IP: Any Edit

Service Type: TCP/UDP, Port: from 137~139 to any Edit

Fragments: Dont Care

Pass or Block: Block Immediately

Branch to Other Filter Set: None

Log: ☒ Enable

Content Management: None

OK

Clear

Cancel

3.5.4 拒绝服务（DoS）攻击防御功能设定

作为 IP 过滤器/防火墙的子功能，总共有 15 种防御功能。DoS 攻击防御功能在路由器的默认设定中是禁用的。点击防火墙并选择拒绝服务（DoS）攻击防御功能设定就可以打开设置页面。

防火墙 >> 拒绝服务（DoS）攻击防御功能设定

拒绝服务（DoS）攻击防御功能设定

☐ 启用拒绝服务（DoS）攻击防御功能

☐ 启用SYN flood攻击防御功能

临界值50封包 / 秒

超时10秒

☐ 启用UDP flood攻击防御功能

临界值150封包 / 秒

超时10秒

☐ 启用ICMP flood攻击防御功能

临界值50封包 / 秒

超时10秒

☐ 启用通讯端口扫描侦测功能

临界值150封包 / 秒

☐ 封锁IP选项

☐ 封锁TCP flag扫描

☐ 封锁Land攻击

☐ 封锁Tear Drop攻击

☐ 封锁Smurf攻击

☐ 封锁Ping of Death攻击

☐ 封锁路由追踪（Trace Route）

☐ 封锁ICMP分片攻击

☐ 封锁SYN分片攻击

☐ 封锁不明数据包通讯协议

☐ 封锁Fraggle攻击

确定

全部清除

取消

启用拒绝服务（DoS）攻击防御功能 点选以启用 DoS 攻击防御功能。

启用 SYN flood 攻击防御 如果从互联网来的 TCP SYN 数据包超过用户设置的临界值，Vigor2910 路由器将会在用户设置的超时时间内随机丢弃 TCP SYN 数据包。主要的目标是保护 Vigor2910 路由器不受企图耗尽路由器资源的 TCP SYN 数据包的威胁。默认情况下，临界值和超时值被设置为每秒 50 个包和 10 秒钟。

启用 UDP flood 攻击防御功能 点选以启用 UDP flood 攻击防御功能。一旦从因特网来的 UDP 封包超过使用者设定的临界值，Vigor2910 路由器将会在使用者设定的超时时间内丢弃所有随后的 UDP 封包。预设的临界值和超时值分别被预设为 300 封包/秒和 10 秒。

启用 ICMP flood 攻击防御功能 点选以启用 ICMP flood 攻击防御功能。如同 UDP flood 攻击防御功能，一旦从因特网来的 ICMP 响应请求封包超过使用者设定的临界值(预设为 300 封包/秒)，Vigor2910 路由器将会在使用者定义的超时时间(预设为 10 秒)内丢弃所有随后的 UDP 封包。

启用通讯端口扫描侦测功能 通讯端口扫描攻击是指传送很多不同通讯端口的封包，企图扫描有哪些通讯端口正在被使用，得知有哪些可用的服务。为了侦测通讯端口扫描行为，请点选以启用 Vigor2910 路由器内的防御通讯端口扫描侦测功能。如果通讯端口扫描速率超过使用者设定的临界值，Vigor2910 路由器将会发现并且发出警告讯息。预设中，Vigor2910 路由器将临界值设定为 300 封包/秒。

封锁 IP 选项 点选以启用封锁 IP Options 功能。Vigor2910 路由器将会忽略任何在数据文件头中有 IP Options 字段的封包。IP Options 让主机可以传送一些重要讯息，例如 Security,Compartmentation,TCC (closed user group)参数，一连串的网址，路由信息等。别人可能会加以分析，而搞清楚您的内部网络。

封锁 Land 攻击	点选以启用 Vigor2910 路由器防御 Land 攻击。Land 攻击结合了 SYN 攻击技术和 IP 伪造。Land 攻击方式是攻击者传送伪造的 SYN 封包，封包内含相同的来源和目的地址(和受害者地址相同)以及相同的通讯端口。
封锁 Smurf 攻击	点选以启用封锁 Smurf 攻击功能。Vigor2910 路由器会拒绝任何指向广播地址的 ICMP 响应请求。
封锁路由追踪	点选以启用此功能。Vigor2910 路由器将不会传送任何路由追踪封包。
封锁 SYN 分片攻击	点选以启用封锁 SYN Fragment 封包功能。任何具有 SYN Flag 以及 More Fragment 位设为 1 的封包会被丢弃。
封锁 Fraggle 攻击	点选以启用封锁 Fraggle 攻击功能。任何从因特网收到的广播 UDP 封包都会被封锁。注意启用 Dos/DDos 攻击防御功能可能会封锁一些合法的封包。例如，当您启用封锁 Fraggle 攻击功能，所有从因特网上广播的 UDP 封包都会被封锁。所以从因特网上来的 RIP 封包也会被丢弃。
封锁 TCP Flags 扫描	点选以启用封锁 TCP Flags 扫描功能。任何具有不正常 Flag 设定的 TCP 封包会被丢弃。这些扫描的活动包含 <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FIN scan</i> , <i>Xmas scan</i> , 以及 <i>full Xmas scan</i> 。
封锁 Tear Drop 攻击	点选以启用封锁 Tear Drop 攻击功能。这种攻击是指攻击者传输部份重送的封包到目标主机，当那些主机要重组封包时就会当机。Vigor2910 路由器会封锁这些封包。
封锁 Ping of Death 攻击	点选以启用封锁 Ping of Death 攻击功能。许多机器在收到超过最大长度的 ICMP 封包可能会当机。为了避免这种攻击，路由器必须能丢弃任何长度超过 1024 字节的切割封包。
封锁 ICMP 分片攻击	点选以启用封锁 ICMP Fragment 封包功能。任何以二进制 Bit 为单位的分片 ICMP 封包会被丢弃。
封锁不明封包通讯协定	点选以启用封锁不明通讯协议封包功能。每个 IP 封包在档头都会有一个通讯协议字段，用来指出在上层使用哪种通讯协议。然而，超过 100 的通讯协议代号目前仍然保留没有被定义，所以路由器要能侦测并拒绝这种封包。
警告信息	Vigor2910 路由器为用户提供了 Syslog 功能以接受 DOS 信息。用户作为 Syslog 服务器可以接受到来自 Syslog 客户端的信息报告。所有关于 DOS 防御的警告信息都将被发送给用户。用户可以在信息中通过查找 Dos 关键字来显示受到了何种攻击。

系统日志(Syslog)/邮件警告设定

日志 (SysLog) 设定

☐ 启用

服务器IP地址

目标端口

启用的系统日志消息:

☒ 防火墙日志

☒ VPN日志

☒ 用户接入日志

☒ 拨号日志

☒ WAN日志

☒ 路由器/DSL信息

邮件预警功能设定

☐ 启用

SMTP 服务器

收件人

回信地址

☐ 认证

用户名

密码

确定

清除

取消

控制台

172.17.1.3

172.17.1.3

Vigor Pro100 series

WAN状态

网关IP (固定)

218.242.130.1

发送封包

3143342

发送速度

5754

WAN IP (固定)

218.242.130.18

接收封包

4009187

接收速度

22962

局域网状态

发送封包

4683008

接收封包

4442011

防火墙日志

VPN日志

用户访问日志

拨号日志

WAN日志

其它

网络信息

会话状态

时间	主机	消息
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2007 -> 218.83.153.243:80 (TCP) close connection
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2007 -> 218.83.153.243:80 (TCP)Web
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2003 -> 60.191.30.212:80 (TCP) close connection
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2006 -> 60.191.55.45:80 (TCP) close connection
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2005 -> 60.191.55.45:80 (TCP) close connection
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2006 -> 60.191.55.45:80 (TCP)Web
Oct 10 01:11:57	Vigor	Local User: 202.211.200.58:6102 -> 64.34.180.200:3592 (UDP)
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2005 -> 60.191.55.45:80 (TCP)Web
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2004 -> 202.165.105.240:80 (TCP)Web
Oct 10 01:11:57	Vigor	Local User: 172.17.1.30:2003 -> 60.191.30.212:80 (TCP)Web
Oct 10 01:11:55	Vigor	Local User: 172.17.1.50:1656 -> 211.100.33.58:80 (TCP) close connection
Oct 10 01:11:54	Vigor	Local User: 172.17.1.41 -> 130.158.6.56 (ICMP) Echo
Oct 10 01:11:54	Vigor	Local User: 172.17.1.50:1656 -> 211.100.33.58:80 (TCP)Web
Oct 10 01:11:53	Vigor	Local User: 172.17.1.41:1004 -> 202.62.0.104:80 (TCP) close connection

ADSL状态

模式

状态

上行速度

下行速度

SNR Margin

Loop Att



3.5.5 URL 内容过滤

Vigor2910 路由器的 **URL 内容过滤**工具会基于用户自定义关键字列表，对每一个外出的 HTTP 请求都要对其 URL 字符串进行检查。不管此 URL 字符串和所设关键字是完全匹配还是部分匹配，Vigor2910 路由器都将会阻挡相关 HTTP 连接。

例如，您添加了一个关键字里加了一个“sex”，Vigor2910 路由器将会限制访问“www.sex.com”，”www.backdoor.net/images/sex/p\_386.html” 等诸如此类网站或网页。同样，Vigor2910 路由器也将会丢弃所有已含有恶意代码的请求。

点击**防火墙**并点击 **URL 内容过滤**可以打开设置页面。

防火墙 >> URL 内容过滤

内容过滤器设定

☐ 启用URL访问控制

☐ 启用URL访问日志记录

☒ 黑名单（屏蔽下列匹配关键词）

☐ 白名单（允许下列匹配关键词）

编号	启用	关键字	编号	启用	关键字
1	<input type="checkbox"/>		5	<input type="checkbox"/>	
2	<input type="checkbox"/>		6	<input type="checkbox"/>	
3	<input type="checkbox"/>		7	<input type="checkbox"/>	
4	<input type="checkbox"/>		8	<input type="checkbox"/>	

空白处可同时指定数个关键字。例如： hotmail yahoo msn

☐ 防止使用IP地址对网站进行访问

☐ 启用限制网络功能

☐ Java

☐ ActiveX

☐ 压缩文件

☐ 可执行程序

☐ 多媒体文件

☐ Cookie

☐ 代理

时间表

索引(1-15) **计划任务设定** 设定: , , ,

注意：动作和超时设定被忽略。

确定

全部清除

取消

- 启用 URL 访问控制

点选此选择框以启用此功能。
- 黑名单 (屏蔽下列匹配关键词)

点选此选择框以限制访问已出现在关键字列表里的相应的网页。
- 白名单 (允许下列匹配关键词)

点选此选择框以允许访问已出现在关键字列表里的相应的网页。
- 关键字

Vigor2910 路由器提供 8 个关键字列表给用户自定义关键字，而每个关键字列表又可以同时输入多个关键字。关键字可以是名词，名词的一部分，或者是完整的 URL 字符串。在同一个关键字列表里的多个关键字可以以空格，逗号或分号分隔。另外，每个关键字列表里最多可以 32 个字符。在指定好关键字之后，Vigor2910 路由器会拒绝一切和所设置的关键字相匹配的网页链接请求。

防止使用 IP 地址对网站进行访问	<p>点选此选择框以拒绝任何使用 IP 地址访问网页，比如 <code>http://202.6.3.2</code>。这样做的目的是防止有些人以此来躲避 URL 内容过滤的控制。</p> <p>您必须清除所使用的浏览器的缓存以便 URL 内容过滤工具在过滤网页时可以准确无误的运行。</p>
启用限制网络功能	<p>点选此选择框以启用此功能。</p> <p><b>Java</b> -点选此选择框以启用阻挡从 Internet 上下载 Java 文件。</p> <p><b>ActiveX</b> -点选此选择框以启用阻挡从 Internet 上下载 ActiveX 文件。</p> <p><b>压缩文件</b> - 点选此选择框以启用阻挡从 Internet 上下载压缩文件。VIGOR2910 路由器能够阻挡的压缩文件包括以下几种： <b>zip, rar, .arj, .ace, .cab, .sit</b></p> <p><b>可执行文件</b> -点选此选择框以启用阻挡从 Internet 上下载可执行文件。VIGOR2910 路由器能够阻挡的可执行文件包括以下几种： <b>.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg</b></p> <p><b>Co 确定 ie</b> - 点选此选择框以阻止您的主机向外发送主机的 co 确定 ie 信息，以保护用户的隐私。</p> <p><b>代理</b> - 点选此选择框以拒绝一切代理，以有效的控制带宽的使用。这是一个很好的保护机制以阻挡从网页上下载多媒体文件。Vigor2910 路由器能够阻挡的多媒体文件包括以下几种： <b>.mov .mp3 .rm .ra .au .wmv</b> <b>.wav .asf .mpg .mpeg .avi .ram</b></p>
允许例外子网	<p>用户可以指定 4 个例外的 IP 地址或子网以便他们可以不受 URL 内容过滤的限制，而能自由的访问 Internet。请点击启用以使您的设置生效。</p>
计划任务设定	<p>指定在什么时间执行 URL 内容过滤。</p>

3.5.6 Web 内容过滤

点击**防火墙**并选择 **Web 内容过滤**以打开设置页面。

关于这部分的详细说明，请参照 **Web 内容过滤**的用户指南。

防火墙 >> Web内容过滤设定

CPA（内容认证）Web内容过滤设定

选择一个CPA服务器：

asia site

[激活免费使用和购买申请](#)

[检查有效性](#)

[测试一个站点以验证其是否已经分类](#)

☐ 启用Web内容过滤

组

类别（选中类别表示屏蔽，不选则表示允许）

保护儿童	<input type="checkbox"/> 聊天	<input type="checkbox"/> 犯罪	<input type="checkbox"/> 烟酒
<div>全部选择</div>	<input type="checkbox"/> 赌博	<input type="checkbox"/> 黑客	<input type="checkbox"/> 粗口
<div>全部清除</div>	<input type="checkbox"/> 性	<input type="checkbox"/> 暴力	<input type="checkbox"/> 武器
休闲	<input type="checkbox"/> 广告	<input type="checkbox"/> 娱乐	<input type="checkbox"/> 食品
<div>全部选择</div>	<input type="checkbox"/> 游戏	<input type="checkbox"/> 时尚	<input type="checkbox"/> 健康
<div>全部清除</div>	<input type="checkbox"/> 业余爱好	<input type="checkbox"/> 生活方式	<input type="checkbox"/> 骑车
	<input type="checkbox"/> 婚介/约会	<input type="checkbox"/> 相片搜索	<input type="checkbox"/> 购物
	<input type="checkbox"/> 体育	<input type="checkbox"/> 流媒体	<input type="checkbox"/> 旅游
商业	<input type="checkbox"/> 计算机/网络	<input type="checkbox"/> 金融	<input type="checkbox"/> 求职
<div>全部选择</div>	<input type="checkbox"/> 政治	<input type="checkbox"/> 房地产	<input type="checkbox"/> 参考资料
<div>全部清除</div>	<input type="checkbox"/> 远程代理	<input type="checkbox"/> 搜索引擎	<input type="checkbox"/> Web邮件
其他	<input type="checkbox"/> 教育	<input type="checkbox"/> 主页托管站	<input type="checkbox"/> 儿童站点
<div>全部选择</div>	<input type="checkbox"/> 新闻	<input type="checkbox"/> 宗教	<input type="checkbox"/> 性教育
<div>全部清除</div>	<input type="checkbox"/> 新闻组	<input type="checkbox"/> 屏蔽所有未分类站点	

计划任务

索引（1-15）[计划任务](#) 设置：，，，

[注意](#)：动作和超时设定将被忽略。

确定

取消

## 3.6 带宽管理

下图为带宽管理的菜单。



### 3.6.1 限制会话

一台拥有私网 IP 地址的 PC 可以通过 NAT 设备访问 Internet, 通过这样的连接 NAT 记录里就会有一条 NAT 会话生成。例如象 BitTorrent P2P 应用程序每次连接都要发起大量的会话，占用系统资源和网络带宽，从而影响网络中其他重要的应用。为了解决这个问题，您可以使用限制会话功能来限制每台客户机的会话数。

在带宽管理菜单，选择限制会话，将显示如下页面：

带宽管理 >> 限制会话

限制会话

☐ 启用

☒ 禁用

默认会话限制:

自定义限制列表

索引	起始 IP	结束 IP	限制会话
----	-------	-------	------

自定义限制

开始IP:

结束IP:

最大会话数:

添加

编辑

移除

计划任务

索引(1-15) **计划任务** 设定: , , ,

注: 计划任务中的动作和超时设定将被忽略。

确定

启用限制会话功能，只需要在该页面选中启用并设置一个默认会话限制即可。

启用	启用会话控制功能。
禁用	禁用会话控制功能。
默认会话限制	网内每台 PC 默认可以使用的会话数。
自定义限制列表	该列表中的 IP 地址可以使用指定的会话数，不受默认会话限制的约束。
起始 IP	自定义的起始的 IP 地址。
结束 IP	自定义的结束的 IP 地址。

限制会话数	自定义 IP 可使用会话数。如果您不设定会话数，路由器将会对每个特定限制项使用默认会话限制机制。
添加	将设定的例外会话限制添加到列表。
移除	除列表中已经存在的设定。
索引 (1-15)计划任务	可以键入四个计划任务项。所有的计划任务可以在 <b>应用程序—计划任务</b> 页面进行定义。在这里就填入计划任务的相应编号就可以了。

## 3.6.2 限制带宽

FTP, HTTP 或一些 P2P 的经常会导致一台 PC 占据大量的带宽，而其它多数 PC 却无法保障最基本的上网带宽，从而影响大多数人的网络使用。请使用限制带宽功能使带宽使用更加合理。

在**带宽管理**菜单，选择**限制带宽**，将显示如下页面：

限制带宽

☐ 启用
☒ 禁用

默认上行速度限制:  Kbps
默认下行速度限制:  Kbps

自定义限制列表

索引	起始 IP	结束 IP	上行限制	下行限制

自定义限制

开始IP: 
结束IP:

上行限制:  Kbps
下行限制:  Kbps

计划任务

索引(1-15) **计划任务** 设定: , , ,

**注意:** 计划任务中的动作和超时值设定将被忽略。

启用**限制带宽**功能，只需要在该页面选中**启用**并设置默认上行下行速度限制即可。

启用	启用带宽使用限制功能。
禁用	禁用带宽使用限制功能。
默认上行限制	网内每台 PC 默认上行的限制速度。
默认下行限制	网内每台 PC 默认下行的限制速度。
自定义限制列表	该列表中的 IP 地址可以使用指定的带宽，不受默认带宽的限制。
开始 IP	自定义的起始的 IP 地址。
结束 IP	自定义的结束的 IP 地址。
上行限制	自定义的上行速度限制

下行限制	自定义的下行速度限制。
添加	将设定的例外速度限制添加到列表。
移除	移除列表中已经存在的设定。
索引 (1-15)计划任务	可以键入四个计划任务项。所有的计划任务可以在应用程序—计划任务页面进行定义。在这里就填入计划任务的相应编号就可以了。

### 3.6.3 服务质量 (QoS)

启用 QoS (Quality of Service) 管理来保证所有的应用都能得到相应的服务等级和足够的带宽，符合用户所期盼的效果，这对现代企业网络来说是极其重要的。

使用 QoS 其中一个原因是许多基于 TCP 的应用会不断的增加传输速度从而占用了所有的可用带宽，这被称作 TCP 慢启动。如果在拥挤的网络环境中其他的应用不被 QoS 所保护，这些应用的性能会被大大影响。这对那些对于丢包，延迟，抖动（变化延迟）敏感的应用是十分必要的。

另外一个原因是当网络节点处电路不匹配或者流量突然增加时，数据包会进行排队等待，使得某些数据包会在低速端被丢弃。如果没有事先定义好哪些数据包应该从过载的队列里被丢弃，上面所提到的敏感的应用的数据包可能被丢弃。这些情况将影响应用的性能。

QoS 基本设置有两大主要方式：

- 分类：对应用进行区分，对高优先级的应用进行标记，保障其最及时被发送。
- 安排：根据服务级别分级安排数据包通过的顺序，保障最高优先级的最先被发送。

Vigor 路由器中最基本的 QoS 应用是根据 IP 头中的服务类型来对服务进行分类和安排。例如，为了在其它网络流量较多的时候，保障 HTTPS 连接的速度不被影响，可以在 QoS 中对 HTTPS 服务进行设置。这样，HTTPS 的带宽将被保障。

在大规模的 QoS 网络应用中，应用 DSCP（区分服务代码）和 IP 优先级来对网络流量分类和安排。DSCP 可以建立 64 级的优先级并且向下兼容 IP 优先级。在一个 QoS 被应用的网络/区分服务的架构中，一个区分服务的域需要和其它区分服务域的拥有者签订一个服务许可协议（SLA）以定义和其它域之间发送数据的服务级别。这被称作单次跳跃行为（PHB），PHB 的定义包含了迅速发送（EF），确保发送（AF）和尽可能发送（BE）。AF 定义了四种发送级别，在每一级别中，分别定义了三种丢弃优先级。

Vigor 路由器在作为 DS 域的边界路由器时，要检查通过的流量中 IP 头的 DSCP 值，来安排相应的分类、发送。主干网的核心路由器在执行转发操作之前应该做同样的工作以确保服务级别在整个 QoS 网络中以同一标准被执行。





然而，由于不同的域的拥有者的不同 SLA 商务应用，网络中其他的结点对于数据包的优先级标记可能会有不同作法。因此，仅仅依靠 Vigor 路由器的努力，在整个网络传输中，是很难获得一个稳定而持续的高优先级的 QoS 数据流。

在应用程序菜单，点击**服务质量（QoS）**，打开如下页面。

**带宽管理 >> 服务质量（QoS）**

**基本设定**

索引	状态	带宽	方向	级别 1	级别 2	级别 3	其它	UDP带宽控制	
WAN1	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>
WAN2	禁用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>

**级别规则**

索引	名称	规则	服务类型
级别 1		<a href="#">编辑</a>	<a href="#">编辑</a>
级别 2		<a href="#">编辑</a>	
级别 3		<a href="#">编辑</a>	

此页面显示了 WAN 口的 QoS 设定。点击 **Setup** 连接访问 WAN(1/2)口的 general setup 页面。在 Class rule 中，简单地点击 **Edit** 连接就可以进入下一步的设置页面。

您可以按照您的实际需求设定 WAN 口的基本设定，编辑级别和服务类型。

## WAN 接口基本设定

当点击 **Setup** 后，您可以为 WAN 口的 QoS 设定带宽比例。对 QoS 控制来说有四个队列。前三个 (Class 1 to Class 3) class rules 可以依据您的需求设定。然后，最后一个队列是为哪些没有被定义过的应用保留的。

**带宽管理 >> 服务质量（QoS）**

**WAN1 基本设定**

☒ 开启 QoS 控制
 

上行

WAN口下行带宽

10000 Kbps

WAN口上行带宽

10000 Kbps

索引	级别名称	保留带宽比率
级别 1		25 %
级别 2		25 %
级别 3		25 %
	其它	25 %

☐ 启用 UDP 带宽控制
 

受限带宽比率 25 %

[在线统计](#)

## 开启 QoS 控制

默认状况下是启用。

请定义 QoS 控制的方向。

下行-仅应用在下行流量。

上行-仅应用在上行流量。

双向-对下行和上行流量都起作用。

选中并点击**确定**，再次点击**设置**的时候，您可以看到页面上出现了**在线状态统计**链接。

WAN 口下行带宽

设置连接的宽带线路的下行带宽，例如，连接的 ADSL 线路支持 1M 的下行和 256K 的上行带宽，可以在此处设置 10000。默认值是 10000kbps。

WAN 口上行带宽

设置连接的宽带线路的上行带宽，例如，连接的 ADSL 线路支持 1M 的下行和 256K 的上行带宽，可以在此处设置 256。默认值是 10000kbps。

保留带宽比率

对指定的组保留相应的上行带宽和下行带宽。

启用 UDP 带宽控制

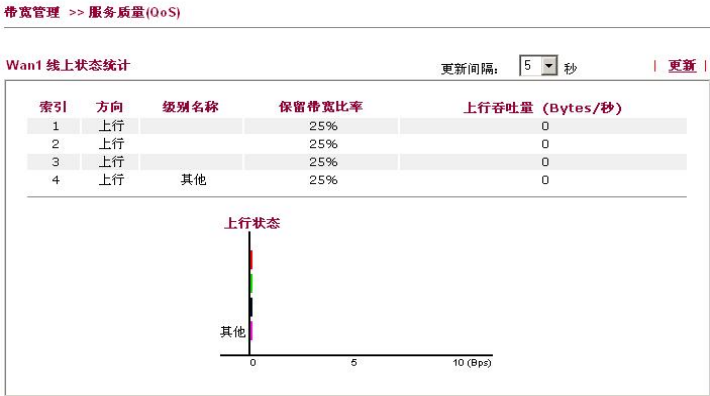
选中此项则根据设置的带宽比率限制 UDP 流量。因为无节制的 UDP 流量（例如在线点播）会耗尽带宽，影响 TCP 应用。

受限带宽比率

指定 UDP 使用的带宽比例。

在线统计

显示当前 QoS 的状态作为您的参考。



编辑 QoS 的级别规则

前三个（级别 1 到级别 3）级别规则可以依据您的需求设定。请点击**编辑**链接来增加，编辑，删除级别规则。

带宽管理 >> 服务质量 (QoS)

基本设定									
索引	状态	带宽	方向	级别 1	级别 2	级别 3	其它	UDP带宽控制	
WAN1	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	设置
WAN2	禁用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	设置

级别规则			
索引	名称	规则	服务类型
级别 1		编辑	编辑
级别 2		编辑	
级别 3		编辑	

在您点击**编辑**链接之后，您可以看到如下页面。现在您可以设定级别的名称。此时，我们选择”Test”作为级别索引 1 的名称。



级别索引 #1

名称

号码	状态	本地地址	远端地址	DiffServ CodePoint	服务类型
1	<input checked="" type="radio"/> 激活	任意	任意	ANY	ANY

添加

编辑

删除

确定

取消

需要增加一条新的规则，点击**添加**，打开如下页面。

规则编辑

☐ 启用

本地地址

编辑

远端地址

编辑

DiffServ CodePoint

服务类型

注意： 请首先选择/设置 **服务类型** 。

启用

选中启用

本地地址

点击**编辑** 设定本地 IP 地址。

远端地址

点击**编辑** 设定远端 IP 地址。

编辑

用来编辑本地地址和远端信息。

http://172.17.1.11/doc/QosIpEdt.htm

地址类型

起始IP地址:

结束IP地址

子网掩码

确定

关闭

**地址类型** – 定义地址的类型

选择**单个地址**，请输入单个 IP 地址。

选择**地址范围**，请输入开始 IP 地址和终止 IP 地址。

选择**子网地址**，请输入开始地址和子网掩码。

**DiffServ CodePoint**

所有的数据包会被系统 QoS 控制功能根据它们的分级类型进行分级处理。此项要求分配一个等级用作 QoS 控制。

**服务类型**

决定了 QoS 控制处理的服务类型，出厂预设了常用的服务类型，通过选择可以快速设置，对于自定义服务类型，可以自行编辑后加入列表。

您最多可以给一个 class 设定 20 条 rules。如果您需要编辑一条已经存在的 rule，请选中它并且点击**编辑**进行修改。

[带宽管理](#) >> [服务质量 \(QoS\)](#)

级别索引 #1

名称

号码	状态	本地地址	远端地址	DiffServ CodePoint	服务类型
1 <input type="radio"/>	激活	任意	任意	IP precedence 5	IPSEC-ESP(IP:50)
2 <input type="radio"/>	激活	192.168.1.5	172.17.2.1	IP precedence 5	IPSEC-AH(IP:51)
<div>添加 编辑 删除</div>					

确定 取消

编辑级别规则的服务类型

请点击**编辑**链接来增加，编辑，删除服务类型。

[带宽管理](#) >> [服务质量 \(QoS\)](#)

基本设定

索引	状态	带宽	方向	级别 1	级别 2	级别 3	其它	UDP带宽控制	
WAN1	<input checked="" type="radio"/> 启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>
WAN2	<input type="radio"/> 禁用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>

级别规则

索引	名称	规则	服务类型
级别 1		<a href="#">编辑</a>	<a href="#">编辑</a>
级别 2		<a href="#">编辑</a>	
级别 3		<a href="#">编辑</a>	

在您点击**编辑**链接之后，您可以看到如下页面。

[带宽管理](#) >> [服务质量 \(QoS\)](#)

用户自定义服务类型

号码	名称	协议	端口
1	空	-	-
<div>添加 编辑 删除</div>			

取消

如果您想要编辑一个存在的服务类型，请点击**单选框**进行编辑，如下图所示。

用户自定义服务类型

号码	名称	协议	端口
<div><div>1</div><div></div></div>	test	TCP	3454

添加

编辑

删除

取消

需要增加一条新的服务类型，点击**添加**，打开如下页面。

Service Type Edit

服务名称

服务类型

TCP

6

端口设置

类型

☒ 单个

☐ 范围

端口号

0

-

0

OK

取消

服务名称

输入您需要的新的服务。

服务类型

选择服务类型 (TCP, UDP or TCP/UDP) 。

**端口设置** 选择单个或范围。点击**单个地址**或**地址范围**。如果您选择了地址范围，您需要定义起始端口号和终止端口号。

**端口号** -如果您选择了范围，您需要在下面的框输入开始端口号和终止端口号。

另外，您可以最多设置 40 条服务类型。如果您需要编辑一条已经存在的服务类型，请选中它并且点击**编辑**进行修改。

### 3.7 应用程序

以下显示的应用程序的菜单项。



#### 3.7.1 动态 DNS

通常 ISP 会分配给您一个动态 IP，这意味着每次连接 Internet，您都会获取不同的 IP 地址。动态 DNS 功能可以将域名绑定到您的动态 IP，每次当路由器连接到 Internet，它都会自动更新自己的动态 IP 与域名的绑定。当您使用 Web Server，FTP Server 或其它 Server 时，该功能使客户端的连接更加方便。

在您使用该功能之前，您需要在 DDNS 服务的提供商那里进行注册，以获取您的动态域名。路由器支持您使用 3 个动态域名，而且路由器支持目前流行的大部分动态域名服务提供商，比如 [www.dyndns.org](http://www.dyndns.org), [www.no-ip.com](http://www.no-ip.com), [www.dtdns.com](http://www.dtdns.com), [www.changeip.com](http://www.changeip.com), [www.dynamic-nameserver.com](http://www.dynamic-nameserver.com) 以及中国用户常用的 [www.ddns.com.cn](http://www.ddns.com.cn) 和花生壳 [www.oray.net](http://www.oray.net)。您可以访问他们的主页进行注册。

启用该功能并添加一个动态 DNS 帐号

1. 首先确认您已经完成了 DDNS 服务的注册。我们以 [hostname.dyndns.org](http://hostname.dyndns.org) 为例，用户名和密码均为 test。
2. 在动态 DNS 设定页面，点选启用动态 DNS 设定。

应用程序 >> 动态DNS设定

动态DNS设定

恢复出厂设置

☐ 启用动态DNS设定

检查日志

强制更新

帐号:

索引值	WAN接口	域名	启用
1.	WAN1优先	.	×
2.	WAN1优先	.	×
3.	WAN1优先	.	×

确定

全部清除

恢复出厂设置

您可以点击此处将动态域名的所有设定都恢复到出厂设置。

启用动态域名设定

点选此项以启用动态域名设定。

索引

点击索引下的数字进入动态域名设置页面填写您的动态域名账号。

WAN 接口

这里显示的是动态域名用在哪个 WAN 接口。

域名

这里显示的您在动态域名设置页面设置的动态域名的名称。

- 启用** 如果动态域名账号被启用就会在这里显示以启用。
- 检查日志** 您可以点击此按钮显示动态域名的注册和更新的日志信息。
- 强制更新** 您可以点击此按钮来强制更新您所设置的动态域名。
3. 选择索引 1 并为路由器添加一个新的 DDNS 帐号。点选启用动态域名账号，并选取正确的域名服务提供商 **dyndns.org**，输入已注册的主机名和域名 **dyndns.org**。在下面两项里填入您在域名服务提供商网站的登录名和密码。

应用程序 >> 动态DNS设定 >> 动态DNS帐户设定

索引值: 1

☐ 启用动态DNS帐号

WAN接口

服务提供商

服务类型

域名

登录名称

密码

☐ 通配符

☐ 备份MX

邮件扩展 (Mail Extender)

WAN1优先

dyndns.org (www.dyndns.org)

动态

(最多23个字符)

(最多23个字符)

确定

清除

取消

- 启用动态域名账号** 点选此项以启用当前账号。如果您点选此项，就可以在之前的页面的状态里看到已被启用的标志。如果您在这里启用了动态域名设置，您就会在这前的页面里看到此动态域名已被启用的标志。
- WAN 接口** 请在此处选择您希望将此动态域名应用在哪一个 WAN 口上。
- 服务提供商** 请在此处选择您动态域名的提供商。
- 服务类型** 请在此处选择您动态域名的服务类型（静态、动态或是自定义）。如果您选择自定义，您需要自己填写您所申请的域。
- 域名** 请在此处填写您所申请的动态域名
- 登录名称** 输入您在此域名服务提供商网站的登录名称。
- 密码** 输入您在此域名服务提供商网站的登录密码。

4. 点击**确定**键保存以上设置。

通配符和备份 MX 功能不是所有的动态域名提供商都支持的，您可以从他们的网站上获取相关信息。

#### 禁用此功能并清除所有动态域名账号

在动态域名设置菜单里去除**启用动态域名设置**，并点击**清除所有**按键去禁用此功能并清除路由器上的所有的账号。

删除动态域名账号

在动态域名设置菜单，点选您要删除的索引号并点击清除所有按键去删除这个账号。

3.7.2 计划任务

Vigor2910 路由器有一个内置的时钟系统，并可以随时通过手动/自动的方式与 NTP 服务器同步。这样，您不仅可以让路由器在指定的时间内连接 Internet，而且可以控制连接 Internet 的时间长度，比如只有在工作时间才允许路由器连接 Internet。

在使用计划任务之前，您必须在系统维护>> 时间和日期菜单对时间进行设置。点击获取时间按钮来使路由器和您 PC 的时间同步。该时钟会在路由器断电或者重置时恢复出厂值。另外，您可以设置路由器使得路由器的时间与 NTP 服务器同步，此功能只有在路由器连接到 Internet 上时才生效。

高级设定 >> 计划任务

计划任务: 恢复出厂设置

索引值	状态	索引值	状态
1.	×	9.	×
2.	×	10.	×
3.	×	11.	×
4.	×	12.	×
5.	×	13.	×
6.	×	14.	×
7.	×	15.	×
8.	×		

状态: ☒ 已启用, ☐ 未启用

- 恢复出厂设置
- 点击此处以清除所有的计划任务设定。
- 索引值
- 点击数字以进入计划任务的设置页面。
- 状态
- 这里显示的是计划任务的状态是否被启用。

您可以设置多达 15 条时间表，然后将他们应用到 Internet 接入或者 VPN 和远端访问下的 LAN-to-LAN 设定等应用。

您可以选择任何一个索引来进行设定，比如说索引 1，进入设置页面，如下图：

高级设定 >> 计划任务

索引值编号 1

☒ 启用计划任务设定

开始日期 (yyyy-mm-dd)

2000-1-1

开始时间 (hh:mm)

9:00

持续时间 (hh:mm)

2:00

动作

强制在线

闲置超时

0 分钟。(最大值255, 预设值0)

频率

☐ 一次

☒ 日期 (工作日)

☐ 周日

☒ 周一

☒ 周二

☒ 周三

☒ 周四

☒ 周五

☐ 周六

确定

清除

取消

- 启用计划任务设定
- 启用该时间表。
- 开始日期 (yy-mm-dd)
- 设置启用该时间表的日期。
- 开始时间 (hh:mm)
- 设置启用该时间表的具体开始时间。

**持续时间 (hh:mm)** 设置该时间表生效的持续时间。

**动作** 设置计划任务在指定时间段内执行的操作。

**强制在线** -强制建立连接。

**强制离线** -强制断开连接。

**启用按需拨接** -设置连接为按需拨接模式，并且在闲置超时项中设定闲置超时时间。

**禁用按需拨接** -如果有网络数据流量则保持连接，没有连接时，超过闲置超时时间则断掉连接，并强制路由器处于断线状态。

**闲置超时** 指定计划任务的时间段。

**频率** -指定计划任务应用的频率。

**一次** -您所设定的计划任务只被应用一次。

**日期** -指定一周哪些天执行该计划。

### 范例：

假设您想控制路由器的 PPPoE 连接，使得它在在一周内，从早上 9 点到下午 6 点处于一直在线（强制在线）的状态，其它时间断开 Internet 连接（强制离线）。

上班时间：

（强制在线）



周一 — 9:00 am to 6:00 pm  
周日

1. 确定 PPPoE 连接和时间设定工作正常。
2. 设置路由器，使得 PPPoE 一周内从早上 9:00 到晚上 6 点一直处于连线状态。
3. 设置路由器，使得每天从晚上 6 点到第二天早上 9 点强制断线。
4. 将这两个时间表应用到 PPPoE 网络连接。然后，PPPoE 连接将会根据在计划任务里预先设置的设定去执行强制在线或强制离线。

### 3.7.3 远程认证拨入用户服务

远端认证拨入用户服务（RADIUS）是一个安全认证客户端和服务器端协议，它支持认证，授权和统计，因此被 Internet 服务提供商所广泛的采用。它也是十分常用的鉴别和认证拨入用户以及隧道网络用户的方法。

内建的 RADIUS 客户端功能使得路由器可以协助远端拨入用户或无线站点和 RADIUS 服务器以执行相互认证。它可以为网络管理集中远端访问授权。

RADIUS设置

☒ 启用

服务器IP地址

目标端口

1812

共享密码

重新输入共享密码

确定

清除

取消

启用	启用 RADIUS 客户端功能。
服务器 IP 地址	输入 RADIUS 服务器的 IP 地址。
目标端口	输入 RADIUS 服务器所使用的 UDP 端口号。默认值是基于 RFC2138 的 1812 端口。
共享密码	RADIUS 服务器和客户端共享一个用于鉴别相互发送消息的密钥，双方必须使用相同的密码。
重新输入共享密码	再次输入共享密码以确认。



### 3.7.4 UPnP

**UPnP**（通用即插即用协议）可以方便的支持网络连接设备的安装和配置，它已经被广泛的应用于拥有 Windows 即插即用系统的 PC 外围设备。为了解决 NAT 穿透问题，出现了许多技术。比如端口映射和应用级网关等。这些是“透明穿透”，即应用程序不用更改，而在路由层面上动手脚。这类方案虽有这些好处，却有缺点，即需要大量的人工配置才能完成这项工作。为了减少用户的工作量，让配置自动进行，新的解决方案 UPnP 出现了。UPnP 是让网络上任意 2 个设备能够发现对方，并进行通讯的一项技术。通过这项技术，一个希望能跨越 NAT 的应用程序或者设备，能够主动去找到一个同样支持 UPnP 协议的 NAT 路由器，并与之协商，在其帮助下将相应端口映射到自己，从而使外网能够访问到自己。这样的协商工作是程序和设备自行完成的，完全无需用户的参与配置。因而无论该用户使用什么牌子的路由器，什么上网方式，也无论内网中 IP 地址是自动分配还是手动填写，一切都将在幕后自动完成。只有一切配置妥当，程序才能开始运行。

目前，支持 UPnP 的应用有微软的 MSN Messenger 和 Emule 下载软件等。通过 UPnP，MSN messenger 可以进行通畅的语音，视频聊天。

高级设定 >> UPnP

**UPnP**

☒ 启用 UPnP服务

☐ 启用连线控制服务

☐ 启用连线状态服务

**注意：**如果您想在您的局域网中运行UPnP服务，您必须勾选上面的相应的服务，同时进行相应的UPnP设定。

确定

清除

取消

#### 启用 UPNP 服务

参照上图，您可以选择启用**连线控制服务**或者**连线状态服务**。

您可以在路由器的 Web 配置主界面里点击应用程序->UPnP 服务设置进入 UPnP 设定。选择**启用 UPNP 服务**，这样以来您就打开了连接控制服务或连接状态服务。在 WindowsXP 的网络连接里点击“**路由器上的 IP Broadband Connection**”，如下图所示。您能够查看连接状态和控制状态。



路由器的 UPnP 工具可以使那些 UPnP 发现程序（譬如 MSN Messenger）侦测到他们在 NAT 路由器后面，获得外部的 IP 地址，并在路由器上配置端口映像。之后，从外网发往路由器相应端口的数据包会被转发到对应的 UPnP 客户端的应用程序。



关于防火墙和 UPNP 的提示：

#### PC 上有防火墙软件时 UNnP 可能会失效

打开 PC 上的防火墙可能导致 UPNP 功能不能正常使用，因为防火墙会关闭某些连接端口。

#### 安全提示

启用 UPNP 功能会增加 PC 受到的网络威胁，在打开该功能之前，您必需考虑到以下风险：

- 请确定您已经打好最新的补丁来完善您的系统。
- 非法用户可以控制路由器的某些功能，比如添加或者删除端口映射。

UPnP 为支持 UPnP 的程序动态添加端口映像，当这些程序非正常关闭时，这些映射可能不会被清除。

### 3.7.5 局域网唤醒

Vigor2910 路由器提供了**局域网唤醒**功能，处于 Vigor2910 路由器 LAN 里的 PC 处于关闭状态时可以被它唤醒。如果您想唤醒 LAN 里的 PC 的时候，您只要在这里输入您想要唤醒的 PC 网卡的 MAC 地址就可以轻松将其唤醒。

需要说明的是，这些需要被唤醒的 PC 的主板和网卡必须支持唤醒功能，而且您必须先主板的 BIOS 设置中启用唤醒功能。

局域网唤醒

注意:局域网唤醒功能协同 **绑定IP到MAC** 功能工作，只有绑定的PC可以通过IP唤醒。

唤醒通过:

MAC地址

IP地址:

MAC地址:

:

:

:

:

唤醒!

结果

唤醒通过

这里提供了两种唤醒类型，您可以在这里选择使用 MAC 地址唤醒或是使用 IP 地址唤醒。如果您选择使用 MAC 地址唤醒，您需要在下面的 **MAC 地址** 栏里填入正确的 MAC 地址。如果您选择使用 IP 地址唤醒，您还需要在下面的 **IP 地址** 栏里选择正确的 IP 地址。

唤醒通过:

MAC地址

MAC地址

IP地址

IP 地址

如果您已经在**防火墙**下的**绑定 IP 到 MAC** 页面下为路由器 LAN 里的 PC 设置了 IP 地址到 MAC 地址绑定，您就可以在此处的下拉框中看到这些 IP 地址。这样您就可以从中选择您想要唤醒 PC 的 IP 地址。

MAC 地址

您可以在这里输入您想要唤醒 PC 的 MAC 地址。

唤醒

点击此按钮以唤醒您想要唤醒的 PC，结果会显示在下面的消息框里。

局域网唤醒

注意:局域网唤醒功能协同 **绑定IP到MAC** 功能工作，只有绑定的PC可以通过IP唤醒。

唤醒通过:

MAC地址

IP地址:

MAC地址:

:

:

:

:

唤醒!

结果

Send command to client done.

### 3.8 VPN 和远程拨入设置

VPN 即虚拟专用网，是通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。通常，VPN 是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

有两种类型的 VPN 连接：**远程拨入用户连接**和 **LAN-to-LAN VPN 连接**。

**远程拨入用户**允许一个远端接入节点，一台 NAT 路由器或一台单一的用户 PC

通过 Internet 建立 VPN 隧道到 Vigor 路由器，从而能够访问 VPN 路由器后面的网络资源。如图 1 所示。

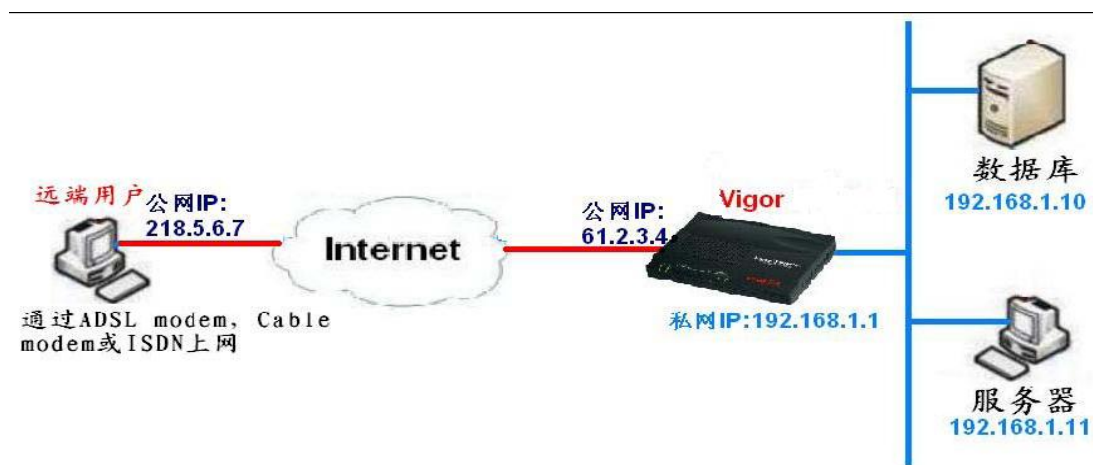


图1. 远程拨入用户连接

**LAN-to-LAN VPN 连接**可将两个独立的局域网连接起来，为共享双方的网络资源提供了一种解决方案。譬如，总公司网络可以访问分支办公室的网络，反之亦然。如图 2 所示。



图2. LAN-to-LAN VPN连接

**注意：** 在 i 型号里，该功能可应用于 ISDN 远端拨入或 ISDN LAN-to-LAN 连接。

下面显示的是 VPN 和远程拨入的目录菜单。



### 3.8.1 远程接入控制功能设定

该功能允许您启用或关闭特定的 VPN 服务（IPSec、PPTP、L2TP）。默认设置是所有 VPN 服务都已启用。

VPN和远程访问 >> 远程接入设定

#### 远程接入设定

<input checked="" type="checkbox"/>	启用PPTP VPN服务
<input checked="" type="checkbox"/>	启用IPSec VPN服务
<input checked="" type="checkbox"/>	启用L2TP VPN服务
<input type="checkbox"/>	启用ISDN拨入

**注意：**如果您想在您的局域网中架设VPN服务器，您必须禁用上面相关的VPN服务并做适当的NAT设定，以便使相应的通信协议能够通过。

确定

清除

取消

如果您想要运行一台 VPN 服务器在路由器的内网里，这时您就需要路由器提供 VPN pass-through 功能，必须在该页面关闭相应的 VPN 服务。譬如，如果您不想使用 Vigor 路由器本身提供的 PPTP 服务器，而是要在 Vigor 路由器后面连一台 PPTP 服务器（如图 3 所示），您就必须将 PPTP 服务关闭，并做相关的 NAT 设定，以便路由器能正确处理相关的数据包。具体设置如下：

**PPTP：**关闭启用 **PPTP 服务**，打开 TCP 1723 到 VPN 服务器。

**L2TP：**关闭启用 **L2TP 服务**，打开 UDP 1701 到 VPN 服务器。

**IPSec：**关闭启用 **IPSec 服务**，打开 UDP 500 到 VPN 服务器。

**ISDN 拨入：**此功能适用于 Vigor 2910i 系列，点选此项启用 ISDN 拨入。

关于如何打开端口，请参考“NAT 设置”。

您也可以访问<http://www.draytek.com.cn> 并查看 技术支持 -> 常见问题-> VPN 问题 -> 如何设定VPN Pass-through





图 3. 在 Vigor2910 上设置 VPN pass-through

如果您没有点选启用 **ISDN 拨入**，Vigor 路由器将不会接受 ISDN 拨入连接。

### 3.8.2 PPP 一般设定

该页面的设置仅与 PPP 相关的 VPN 连接有关，包括 PPTP、L2TP 和 L2TPover IPsec。并且，该设定仅对远端拨入用户 VPN 或拨入的 LAN-to-LAN VPN 有效，若 Vigor 路由器拨出 LAN-to-LAN VPN 到远端 VPN 路由器 那么相关的 PPP 设定是在 **LAN-to-LAN 设定档** 里设置的。下面介绍各选项含义：

**VPN和远程访问 >> PPP基本设定**

PPP基本设定	
<b>PPP/MP协议</b> 拨入PPP验证: <span>PAP或CHAP</span> 拨入PPP加密 (MPPE): <span>可选MPPE</span> 相互验证 (PAP): <input type="radio"/> 是 <input checked="" type="radio"/> 否 用户名: <input type="text"/> 密码: <input type="text"/>	<b>分配IP给拨入用户</b> 起始IP地址: <span>192.168.1.8</span>
<input type="button" value="确定"/>	

#### 拨入 PPP 验证

**仅 PAP** - 若选择该设置，那么在 VPN 建立的 PPP 协商阶段，将只使用固定 PAP 协议认证远端拨入用户或拨入的 LAN-to-LAN 连接。

**PAP 或 CHAP** - 若选择该设置，那么在 VPN 建立的 PPP 协商阶段 Vigor2910 路由器将接受远端拨入用户或拨入的 LAN-to-LAN VPN 使用以下任意一种验证协议：MS-CHAPv2 MS-CHAPv1, CHAP, PAP。并且 Vigor2910 路由器总是先提议对方使用 MS-CHAPv2。

#### 拨入 PPP 加密 (MPPE)

**可选 MPPE** - 若选择该设置，那么 MPPE 加密是可选的。如果远端拨入用户或拨入的 LAN-to-LAN VPN 不支持 MPPE 加密算法，那么 Vigor2910 路由器将不加密 VPN 数据，否则 Vigor 路由器将用相应的 MPPE 加密算法加密 VPN 数据。

可选MPPE 可选MPPE 要求MPPE (40/128 位) MPPE最大值 (128 位)
--

**要求 MPPE (40/128 位)**-若选择该设置, 那么拨入端 (远端拨入用户或拨入的 LAN-to-LAN VPN) 必须使用 MPPE 加密算法, 或者 MPPE 40 位, 或者 MPPE 128 位。若拨入端同时提议这两个算法, Vigor 路由器将首选 MPPE 128 位。

**MPPE 最大值 (128 位)**-若选择该设置, 那么 Vigor2910 路由器将只接受拨入端 (远端拨入用户或拨入的 LAN-to-LAN VPN) 使用最大强度的 MPPE 加密算法 (MPPE 128 位)。

#### 相互验证 (PAP)

有些路由器 (譬如 Cisco) 支持相互验证 (Mutual Authentication) 功能, 建立 VPN 的时候需要两个方向上的验证, 可以提供更强的安全性。默认情况下该功能是关闭的。注意, 如果您启用了该功能, 就必须正确输入用于验证的用户名和密码。

用户名

为相互验证输入用户名。

密码

为相互验证输入密码。

分配 IP 给拨入用户

**起始 IP 地址** - 该起始 IP 地址规定了一个 IP 范围, 用于 VPN 建立的 PPP 协商阶段分配 IP 给拨入端 (远端拨入用户或拨入的 LAN-to-LAN VPN), 它必须在本地私网范围内。譬如, 如果本地私网范围是 192.168.1.0/255.255.255.0, 那么起始 IP 地址就必须是 192.168.1.1~192.168.1.254 中的一个。

### 3.8.3 IPSec 一般设定

该页面的设置仅与 IPSec 相关的 VPN 连接有关, 包括 IPSec 和应用 IPSec 策略的 L2TP。您可以为这些 IPSec 相关的 VPN 连接设置一个公用的预共享密钥 (Pre-shared key) 以及安全方法 (Phase 2 协商阶段)。这些设定用于远程拨入用户或拨入的 LAN-to-LAN VPN。通常他们都使用动态 IP 地址。

在后面的介绍里, 您将发现在远程拨入用户帐号和 LAN-to-LAN VPN 设定档里, 您都可以为相应的设定档单独配置 IPSec 拨入设定 (包括预共享密钥和安全方法)。如果您没有为那些设定档专门配置拨入设定, 它们将使用 VPN IPSec/IKE 基本设定里的设置。

IPSec 协商分两个阶段

- 阶段 1: 协商 IKE 参数, 包括加密方式, hash, Diffie-Hellman 参数值, 阶段 1 的密钥存活期。在阶段 1 会通过 Pre-Shared Key 或者数字证书 (X.509) 来认证 VPN 双方的身份。VPN 拨出端在协商开始后会发送一个或多个 IKE 参数提议到 VPN 拨入端, 拨入端将接受符合它的且具有最高优先权的提议。最终双方完成协商后, 将建立一个安全隧道, 为 IKE 阶段 2 所使用。
- 阶段 2: 协商 IPSec 安全方法, 为之后的 IKE 通信选择一个保护机制。可选的模式有认证头 (AH) 和封装安全载荷 (ESP)。

根据封装的载荷内容不同, 可分为两种模式:

隧道模式 (Tunneling Mode), 将整个 IP 分组封装到 ESP/AH 载荷中。

传输模式 (Transporting Mode), 将上层协议部分封装到 ESP 载荷中。

认证头(AH)机制主要用于为通信提供完整性服务。

封装安全载荷(ESP)机制主要为通信提供机密性保护。依据建立安全关联时的选择,它也能提供鉴别保护。

VPN和远程访问 >> IPSec基本设定

VPN IKE / IPSec基本设定

远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。

IKE认证方法

预共享密钥

...

重新键入预共享密钥

...

IPSec安全方法

☒ 中等 (AH)

会对数据进行认证, 但不会加密。

高等 (ESP)

☒ DES

☒ 3DES

☒ AES

会对数据进行认证及加密。

确定

取消

在 IPSec 基本设定, 有两个部分的配置。

IKE 认证方法

这里设置的**预共享密钥**通常在以下情况下被使用: 远端用户拨入的 Host-to-LAN IPSec VPN, 以及拨出端使用动态 WAN IP 的 LAN-to-LAN IPSec VPN。

**预共享密钥** - 输入预共享密钥

**重新键入预共享密钥** - 确认输入的预共享密钥

IPSec 安全方法

选择允许的 IPSec 安全方法。 **注意:** 该设定仅用于 IPSec 第二阶段的协商。

**中等 (AH)** - 数据将被认证, 但不会被加密。默认该选项被启用。

**高等 (ESP)** - 数据将被认证和加密。这里我们支持 DES、3DES 和 AES 加密方式。默认所有选项都被启用。

3.8.4 端点认证

远程拨入用户以及 **LAN-to-LAN VPN** 连接都可以使用数字证书对 VPN 双方进行身份认证。您可以在此栏编辑可供选择的证书。如下图所示,一共可以添加 32 个数字证书。



X509端点ID帐户：

恢复出厂设置

索引	名称	状态	索引	名称	状态
<a href="#">1.</a>	???	×	<a href="#">17.</a>	???	×
<a href="#">2.</a>	???	×	<a href="#">18.</a>	???	×
<a href="#">3.</a>	???	×	<a href="#">19.</a>	???	×
<a href="#">4.</a>	???	×	<a href="#">20.</a>	???	×
<a href="#">5.</a>	???	×	<a href="#">21.</a>	???	×
<a href="#">6.</a>	???	×	<a href="#">22.</a>	???	×
<a href="#">7.</a>	???	×	<a href="#">23.</a>	???	×
<a href="#">8.</a>	???	×	<a href="#">24.</a>	???	×
<a href="#">9.</a>	???	×	<a href="#">25.</a>	???	×
<a href="#">10.</a>	???	×	<a href="#">26.</a>	???	×
<a href="#">11.</a>	???	×	<a href="#">27.</a>	???	×
<a href="#">12.</a>	???	×	<a href="#">28.</a>	???	×
<a href="#">13.</a>	???	×	<a href="#">29.</a>	???	×
<a href="#">14.</a>	???	×	<a href="#">30.</a>	???	×
<a href="#">15.</a>	???	×	<a href="#">31.</a>	???	×
<a href="#">16.</a>	???	×	<a href="#">32.</a>	???	×

恢复出厂设置

点击此处可以清除以前所设定的所有证书。

索引

点击数字可以进入编辑页面。

名称

显示该项证书的名字。

点击索引号进入编辑页面。有三种安全等级的数字证书认证方式可供选择。请添写必要的信息，与对端认证。请参考以下指导添写必要的信息。

☐ 启用此帐户

☒ 接受任意端点ID

☐ 接受可替换识别名称（Subject Alternative Name）

类型

IP地址

IP

☐ 接受识别名称（Subject Name）

国家（C）

州（ST）

区域（L）

组织（O）

组织单位（OU）

通用名称（CN）

Email（E）

确定

清除

取消

设定档名

输入该项证书的名程。

接受任何端点 ID（Peer ID）

接受来自任何端点的证书。

接受可替换名称

只接受符合特定值的证书的认证。这些特定值包括 **IP 地址**、**域名**或者 **E-mail**。 在选择了其中以上一项后,会出现对应的方框供填入具体内容。

## 接受识别名

只接受符合以下全部特定内容的证书。这些特定内容包括国家(C)、州(ST)、区域(L)、组织(O)、组织单位(OU)、通用名称(CN)和 Email (E)。

3.8.5 为远程接入用户设定帐号

您可以在这里为远端拨入用户设置相应的设定档。Vigor 2910 为远端拨入用户提供了 32 个拨入帐号。此外，您也可以使用 RADIUS 服务器来扩充用户帐号的个数，因为 Vigor2910 本身也支持 RADIUS 客户端功能。下图显示了**远程拨入用户**的主界面。

VPN和远程访问 >> 远程拨入用户

远程接入用户帐号:			恢复至出厂默认设置		
索引	用户	状态	索引	用户	状态
<a href="#">1.</a>	???	×	<a href="#">17.</a>	???	×
<a href="#">2.</a>	???	×	<a href="#">18.</a>	???	×
<a href="#">3.</a>	???	×	<a href="#">19.</a>	???	×
<a href="#">4.</a>	???	×	<a href="#">20.</a>	???	×
<a href="#">5.</a>	???	×	<a href="#">21.</a>	???	×
<a href="#">6.</a>	???	×	<a href="#">22.</a>	???	×
<a href="#">7.</a>	???	×	<a href="#">23.</a>	???	×
<a href="#">8.</a>	???	×	<a href="#">24.</a>	???	×
<a href="#">9.</a>	???	×	<a href="#">25.</a>	???	×
<a href="#">10.</a>	???	×	<a href="#">26.</a>	???	×
<a href="#">11.</a>	???	×	<a href="#">27.</a>	???	×
<a href="#">12.</a>	???	×	<a href="#">28.</a>	???	×
<a href="#">13.</a>	???	×	<a href="#">29.</a>	???	×
<a href="#">14.</a>	???	×	<a href="#">30.</a>	???	×
<a href="#">15.</a>	???	×	<a href="#">31.</a>	???	×
<a href="#">16.</a>	???	×	<a href="#">32.</a>	???	×

- 恢复出厂设置

点击该图标将清除所有的设定档。
- 索引值

要进入某个用户帐号配置页面必须点击相应的索引值号码。
- 用户

这里显示的值是设定档里**用户名**栏里的设定。如果您在**用户名**一栏里什么都没有输入，将显示默认的符号**???**。因为只有当 VPN 类型是 PPTP、L2TP 或应用 IPSec 策略的 L2TP 的时候才需要设定**用户名**一栏，所以当 VPN 类型是 IPSec，**用户**将显示为**???**。当然您也可以在 IPSec 连接的设定档里键入一个用户名来标识此设定档，并区分其它设定档，它不会影响 IPSec 的正常建立。
- 状态

显示该设定档是否被启用了。符号 **v** 表示设定档已经启用，符号 **x** 表示设定档已经禁用。
- 点击索引号可以进入编辑页面。每次您需要在编辑页面的右侧填写相应的不同拨入类型。如果设置栏是灰色的，那就说明此项不可修改。接下来的说明将会引导您去填写所有必要的设置。

## 索引号 1

<b>用户帐户与验证</b> <input type="checkbox"/> 启用此帐号 闲置超时 <input type="text" value="300"/> 秒		用户名 <input type="text" value="???"/> 密码 <input type="password"/>
<b>允许接入类型</b> <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec隧道 <input checked="" type="checkbox"/> 应用IPsec策略的L2TP <input type="text" value="无"/>		<b>IKE认证方法</b> <input checked="" type="checkbox"/> 预共享密钥 IKE预共享密钥 <input type="text"/> <input type="checkbox"/> 数字证书 (X.509) <input type="text" value="无"/>
<input type="checkbox"/> 指定远端结点 远程用户IP或对端ISDN号码 <input type="text"/> 或对端ID <input type="text"/>		<b>IPsec安全方法</b> <input checked="" type="checkbox"/> 中等 (AH) 高等 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 本地ID <input type="text"/> (可选)
<b>回拨功能</b> <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 指定回拨号码 回拨号码 <input type="text"/> <input checked="" type="checkbox"/> 启用回拨定额控制 回拨定额 <input type="text" value="30"/> 分钟		

## 启用此帐号

开启此帐号。

**闲置超时** - 如果没有任何数据传输通过这条建立好的 VPN 隧道超过**闲置超时**规定的时间，路由器将断掉该连接。默认设置是 300 秒，也就是说如果有个远端用户使用该设定档建立了一条 VPN 连接，一旦超过 300 秒的时间没有任何数据通过该 VPN 隧道传输，VPN 连接将被自动断开。如果您不想有此时间限制，请将该值设为 0 秒。

## ISDN

允许远端拨入用户通过 PPTP VPN,用此帐号接入。您还需要设定此帐号的用户名和密码。

## PPTP

允许远端拨入用户通过 PPTP VPN,用此帐号接入。您还需要设定此帐号的用户名和密码。

## IPsec 隧道

允许远端拨入用户通过 IPsec VPN,用此帐号接入。

## L2TP (使用 IPsec 策略)

允许远端拨入用户通过 L2TP/IPsec VPN,用此帐号接入。您可以选择单独使用 L2TP 或者应用 IPsec 策略的 L2TP:  
**无** - 建立单纯的 L2TP VPN

**最好能使用** - 如果拨入端的设定也是应用 IPsec 策略的 L2TP 则启用 IPsec,否则建立单纯的 L2TP VPN 连接。

**一定要有** - 拨入端必须使用应用 IPsec 策略的 L2TP VPN 而不能使用单纯的 L2TP VPN 连接。

## 指定远端节点

该选项是可选的。默认是禁用的，也就是说任何远程用户（特别是使用动态 IP 地址的用户）都可以使用此设定档的设置建立 IPsec VPN 到 Vigor 路由器。此时该设定档使用 **IPsec 基本设定**中的 **IKE 认证方法**和 **IPsec 安全方法**的设定。如果为了安全性需要限制特定的用户才能拨入 VPN，

	<p>您可以启用<b>指定远端节点</b>功能，并在<b>远端用户 IP 或端点 ISDN 号码</b>栏里填入该特定用户的公网 IP 地址。这样，即使其他用户的 IPsec 设置都匹配此设定档，由于他们的公网 IP 地址不被允许拨入，他们也无法建立 VPN 连接。</p>
用户名	为该远程拨入用户设置用户名。
密码	为该远程拨入用户设置密码。
IKE 认证方法	<p>一旦启用了<b>指定远端节点</b>功能，就必须为此设定档单独配置 <b>IKE 认证方法</b>和 <b>IPsec 安全方法</b>。这里的设定与 <b>IPsec 基本设定</b>里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。这里的设置适用于 IPsec VPN 和应用 IPsec 策略的 L2TP VPN。但是即使<b>指定远端节点</b>没有被启用,您仍然可以编辑数字证书的设定。</p> <p><b>预共享密钥</b> - 输入预共享密钥。必须和 VPN 拨出端的设定相同。</p> <p><b>数字签名 (X.509)</b> - 选择一个在 <b>IPsec 端点 ID</b> 中设定好的 ID 帐号。</p> <p><b>IPsec 安全方法</b> 选择允许的 IPsec 安全方法。注意：该设定仅用于 IPsec 第二阶段的协商。</p> <p><b>中等 (AH)</b> - 数据将被认证，但不会被加密。默认该选项被启用。</p> <p><b>高等 (ESP)</b> - 数据将被认证和加密。这里我们支持 DES, 3DES 和 AES 加密方式。默认所有选项都被启用。</p> <p><b>本地 ID</b> -为 LAN-to-LAN 拨入设置指定一个本地 ID。这项为可选的，而且仅用于 <b>IKE 积极模式</b>。</p>
回拨功能	<p>回拨功能为 ISDN 拨入用户提供了回拨服务。</p> <p><b>启用回拨功能</b> - 启用回拨功能。</p> <p><b>指定回拨号码</b> - 此项设定是为了增加安全性，一旦启用此选项,路由器只会对该特定的<b>回拨号码</b>回拨。</p> <p><b>启动回拨定额控制</b> - 根据默认设置，回拨功能有一个时间限制,一旦回拨资费被耗尽，则回拨功能将自动停止。</p> <p><b>回拨定额 (单元:分钟)</b> - 定义远端拨入用户的时间资费，该资费会随着每次回拨连接而递减。</p>

3.8.6 LAN to LAN

下面将介绍如何在两台 VPN 路由器之间建立一条 VPN 隧道，从而将两个局域网连接起来。点击进入 **LAN-to-LAN 设定档** 页面，总共可以创建 32 个设定档。

VPN和远程访问 >> LAN to LAN

LAN-to-LAN设定档: 恢复至出厂默认设置

索引	名称	状态	索引	名称	状态
<a href="#">1.</a>	???	×	<a href="#">17.</a>	???	×
<a href="#">2.</a>	???	×	<a href="#">18.</a>	???	×
<a href="#">3.</a>	???	×	<a href="#">19.</a>	???	×
<a href="#">4.</a>	???	×	<a href="#">20.</a>	???	×
<a href="#">5.</a>	???	×	<a href="#">21.</a>	???	×
<a href="#">6.</a>	???	×	<a href="#">22.</a>	???	×
<a href="#">7.</a>	???	×	<a href="#">23.</a>	???	×
<a href="#">8.</a>	???	×	<a href="#">24.</a>	???	×
<a href="#">9.</a>	???	×	<a href="#">25.</a>	???	×
<a href="#">10.</a>	???	×	<a href="#">26.</a>	???	×
<a href="#">11.</a>	???	×	<a href="#">27.</a>	???	×
<a href="#">12.</a>	???	×	<a href="#">28.</a>	???	×
<a href="#">13.</a>	???	×	<a href="#">29.</a>	???	×
<a href="#">14.</a>	???	×	<a href="#">30.</a>	???	×
<a href="#">15.</a>	???	×	<a href="#">31.</a>	???	×
<a href="#">16.</a>	???	×	<a href="#">32.</a>	???	×

- 恢复出厂设置
- 名称
- 状态
- 点击该处将清除所有的设定档。
- 这里显示 LAN-to-LAN 设定档里用户名 一栏内的字符。如果您在该栏里什么都没有输入，将显示默认的符号???
- 显示该设定档是否被启用了。符号 v 表示设定档已经启用，符号 x 表示设定档已经禁用。

点击索引值号可以进入 LAN-to-LAN 设定档。每个 LAN-to-LAN 设定档包含四个部分：一般设定、拨出设定、拨入设定和 TCP/IP 网络设定。以下将详细介绍这四个部分的设定。

VPN和远程访问 >> LAN to LAN

设定档索引 : 1

1. 一般设定

设定档名称

???

☐ 启用此设定档

VPN隧道通过: WAN1优先

拨叫方向

☒ 双向 ☐ 拨出 ☐ 拨入

☐ 一直在线

闲置超时 300 秒

☐ 启用PING以维持在线

PING IP

2. 拨出设定

我拨叫的服务器类型

☒ ISDN

☐ PPTP

☐ IPSec隧道

☐ 应用IPSec策略的L2TP 无

ISDN拨号号码或  
VPN服务器IP/主机名  
(比如 5551234, draytek.com 或 123.45.67.89)

连接类型64k bps

用户名???

密码

PPP验证PAP/CHAP

VJ压缩开 关

IKE认证方法

☒ 预共享密钥

IKE预共享密钥

☐ 数字签名(X.509)

无

IPSec安全方法

☒ 中等(AH)

☐ 高等(ESP) DES无验证

高级

索引(1-15) 计划任务 设置:

回拨功能(CBCP)

☐ 要求远端回拨

☐ 提供ISDN号码给远端

设定档名称

为该设定档设定一个名字，便于区分其它设定档。

启用此设定档

要启用此设定档必须点此选项。

VPN 隧道通过

使用下拉菜单选择适当的 WAN 界面。这项设置仅适用于 VPN 拨出。

VPN隧道通过:

WAN1优先

WAN1优先

仅WAN1

WAN2优先

仅WAN2

**WAN1 优先** – 连线时，路由器会将 WAN1 视为 VPN 连线的首要选择，如果 WAN1 连线失败，路由器将使用另一个 WAN 介面来代替。

**仅 WAN1** – 连线时，路由器会将 WAN1 视为 VPN 连接的唯一选择。

**WAN2 优先** – 连线时，路由器会将 WAN2 视为 VPN 连线的首要选择，如果 WAN2 连线失败，路由器将使用另一个 WAN 介面来代替。

**仅 WAN2** – 连线时，路由器会将 WAN1 视为 VPN 连接的唯一选择。

拨叫方向

选择该设定档建立 VPN 拨叫方向。

**双向**-该设定档的**拨出设定**部分和**拨入设定**部分均被启用，Vigor 路由器即能主动拨 VPN 连接到远端 VPN 路由器，又能接受远端 VPN 路由器拨入的 VPN 连接。

**拨出**-仅**拨出设定**部分被启用，使用此设定档 Vigor 路由器只能主动拨 VPN 到远端 VPN 路由器，不能做为 VPN 服务器接受拨入的 VPN 连接。

**拨入**-仅**拨入设定**部分被启用，使用此设定档 Vigor 路由器

Vigor2910 系列中文手册

105

只能接受远端 VPN 路由器拨入的 VPN, 不能主动拨出 VPN 连接。

#### 一直在线或闲置超时

**一直在线**-启用该功能后, 只要 VPN 连接还未建立, Vigor 路由器就会以固定的时间间隔不断尝试连接, 直到 VPN 连接建立。连接建立后, 会保持该连接一直在线, 除非连接被手动断开或由于线路问题导致断线。并且一旦 VPN 连接断开, Vigor 路由器就又开始不断尝试连接。该选项仅对**拨出**方向的 VPN 有效, 所以启用该功能后, **拨叫方向**会被自动设定为**拨出**。另外, 该功能被启用后, **闲置超时**会被自动设为**-1**, 并且变成不可设置。

**闲置超时** - 如果没有任何数据传输通过这条建立好的 VPN 隧道超过“闲置超时”规定的时间, 路由器将断掉该连接。默认设置是 300 秒, 如果您不想有此时间限制, 请将该值设为 0 秒。

#### 启用 PING 以维持在线

启用该功能并在**指定 IP 地址** 栏里输入远端 VPN 网络里的一个可以 ping 通的 IP 地址。当该 IP 地址 ping 不通的时候, Vigor 路由器即认为该 VPN 隧道已经无效, 便会将该连接断开。**该功能是专门为 IPSec 设计的, 而对 PPTP, L2TP 和应用 IPSec 策略的 L2TP 是无效的。**因为 PPTP, L2TP 和应用 IPSec 策略的 L2TP 这类基于 PPP 的 VPN 连接会使用相关的 PPP 机制来实时侦测 VPN 连接的状态, 而 IPSec 只能在重新交换密钥的时候发现对端是否还存在, 由于重建密钥的时间间隔一般都是一个小时以上, IPSec 无法实时侦测 VPN 连接的状态。使用该功能就能帮助 IPSec 快速发现并断开有问题的 VPN 连接。**注意, 此功能独立于 DPD(Dead peer detection)功能。**

#### PING IP

输入远端 VPN 网络里的一个可以 ping 通的 IP 地址。

#### ISDN

建立 ISDN LAN-to-LAN VPN 连接。您还需要为 VPN 拨出端设定**连接类型**、**用户名**和**密码**来进行安全认证。您也可以进一步设定**回拨功能**。

#### PPTP

建立 PPTP LAN-to-LAN VPN 连接。 您还需要为 VPN 拨出端设定**用户名**和**密码**来进行安全认证。

#### IPSec 隧道

建立 IPSec LAN-to-LAN VPN 连接。

#### 应用 IPSec 策略的 L2TP

建立 L2TP/IPSec LAN-to-LAN VPN 连接。您可以选择单独使用 L2TP 或者应用 IPSec 策略的 L2TP:

**无** - 建立单纯的 L2TP VPN。

**最好使用** - 如果拨入端的设定也是应用 IPSec 策略的 L2TP, 则启用 IPSec, 否则建立单纯的 L2TP VPN 连接。

**一定要有** - 拨入端必须使用应用 IPSec 策略的 L2TP, 而不能使用单纯的 L2TP VPN 连接。

#### 用户名

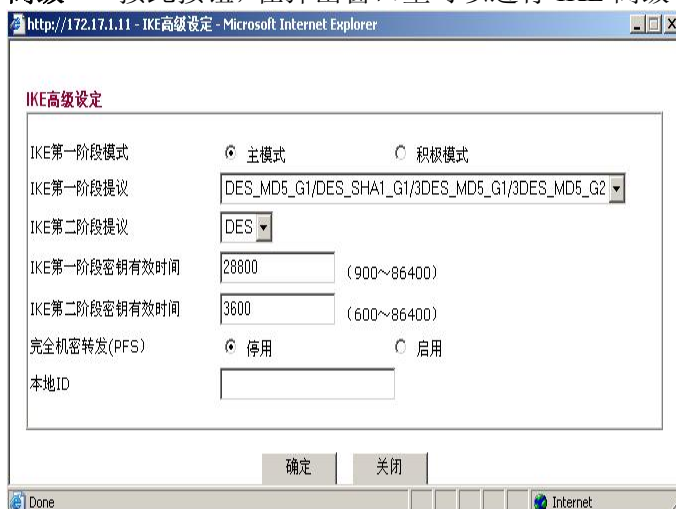
为 VPN 拨出端用户设置用户名。当您选择的 VPN 模式为 ISDN, PPTP 或 L2TP 时必须设置此项。

#### 密码

为 VPN 拨出端用户设置密码。当您选择的 VPN 模式为 ISDN, PPTP 或 L2TP 时必须设置此项。



<b>PPP 验证</b>	<p><b>仅 PAP</b> - 若选择该设置，那么在 VPN 建立的 PPP 协商阶段，将只支持使用 PAP 协议进行认证。</p> <p><b>PAP/CHAP</b> - 若选择该设置，那么 Vigor 路由器支持以下任意一种验证协议：MS-CHAPv2，MS-CHAPv1，CHAP，PAP。具体使用哪一种由 VPN 服务器决定。推荐选择此设定。</p>
<b>VJ 压缩</b>	它用于 TCP/IP 协议头的压缩，可以稍微节省一点带宽。建议使用默认设定开启。
<b>IKE 认证方法</b>	<p>这里的设置只适用于 IPSec VPN 和应用 IPSec 策略的 L2TP VPN。</p> <p><b>预共享密钥</b> - 输入 1-63 个字符作为预共享密钥。</p> <p><b>数字签名 (X.509)</b> - 选择一个在 <b>IPSec 端点 ID</b> 中设定好的 ID 帐号。</p>
<b>IPSec 安全方法</b>	这里的设置只适用于 IPSec VPN 和应用 IPSec 策略的 L2TP VPN。
<b>中级</b>	<p><b>中等 (AH)</b> 数据将被认证，但不会被加密。</p> <p><b>高等 (ESP)</b> 数据将被认证和加密,下拉菜单里有 6 个选项：</p> <p><b>DES 无验证</b>  <b>DES 有验证</b>  <b>3DES 无验证</b>  <b>3DES 有验证</b>  <b>AES 无验证</b>  <b>AES 有验证</b></p> <p>无验证指的是不使用 MD5 或 SHA1 认证算法。当选择有验证的时候，Vigor 将发送两个提议，按先后顺序是 SHA1，MD5。譬如，若您选择了 3DES 有验证，Vigor 将先后发送 3DES+SHA1 和 3DES+MD5 到远端 VPN 服务器。</p> <p><b>高级</b> 按此按钮，在弹出窗口里可以进行 IKE 高级设定。</p>



**IKE 第一阶段模式** - 可以选择主模式（Main mode）或积极模式（Aggressive mode）。该设定必须匹配 VPN 服务器的设定。注意：如果选择了积极模式，必须配置本地 ID；

若没有，则不要配置本地 ID。

**IKE 第一阶段提议** - 在第一阶段（Phase 1），Vigor 支持的加密算法是 **DES** 和 **3DES**；支持的认证算法是 **MD5** 和 **SHA1**；支持的 **DH** 组是 **Group 1（768-bit）** 和 **Group 2（1024-bit）**。这些参数的组合总共有 8 组，在下拉菜单里您可以单独选择一组，它必须与 VPN 服务器的相关设定匹配。此外 Vigor 还提供了一个包含了 4 组提议的选项

（DES\_MD5\_G1 / DES\_SHA1\_G1 / 3DES\_MD5\_G1 / 3DES\_MD5\_G2），在 VPN 建立过程中，Vigor 将发送这四个提议给 VPN 服务器，这四个提议中，第一个匹配 VPN 服务器设定的组将被 VPN 服务器采用。当您不确定 VPN 服务器的配置的时候，可以选择该选项。

**IKE 第二阶段提议** - 支持的认证算法是 **MD5** 和 **SHA1**

**IKE 第一阶段密钥有效时间** - 设定第一阶段的密钥存活时间，时间一到，IKE 将协商一个新的密钥。单位是秒，有效值是 900 秒到 86400 秒，默认值是 28800 秒。

**IKE 第二阶段密钥有效时间** - 设定第二阶段的密钥存活时间，时间一到，IKE 将协商一个新的密钥。单位是秒，有效值是 600 秒到 86400 秒，默认值是 3600 秒。

**完全机密转发（PFS）** - 启用该功能将在第二阶段引入一个新的 DH 密钥交换，从而提供了更强的安全性。通常是不需要 PFS 的，因为危及加密或认证密钥安全性的可能性很小，而且启用 PFS 也会影响 IPSec 的速度。如果 VPN 服务器要求使用 PFS，请点选启用。

**本地 ID** - 只有在 **IKE 第一阶段模式**是积极模式

（Aggressive mode）的时候才需要设定本地 ID。它的格式可以是 Email 地址，域名或字符串。该 ID 必须匹配 VPN 服务器里的相关设定，如果远端 VPN 服务器是 Vigor 路由器，对应的值是服务器**拨入设定**里的**端点（Peer）ID**。该 ID 的长度被限制在 47 个字节以内。

**回拨功能（仅用于 i 型号）** 回拨功能为 ISDN 拨入用户提供了回拨服务。

**要求远端回拨** - 启用此选项后可以让本地路由器发出请求,使之后的连接由 VPN 另一端回拨。

**提供 ISDN 号码给远端** - 如果在 VPN 另一端的路由器需要知道本地路由器 ISDN 号码的情况下要开启此选项。随后路由器会发送本地的 ISDN 号码给 VPN 远端的路由器。

### 3. 拨入设定

<b>允许拨入类型</b> <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec隧道 <input checked="" type="checkbox"/> 应用IPSec策略的L2TP <span>无</span>  <input type="checkbox"/> 指定 ISDN CLID 或 远端VPN网关 对端ISDN号码或 对端VPN服务器IP <input type="text"/> 或端点ID <input type="text"/>	用户名 <input type="text" value="???"/> 密码 <input type="text"/> VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关  <b>IKE认证方法</b> <input checked="" type="checkbox"/> 预共享密钥 IKE预共享密钥 <input type="text"/> <input type="checkbox"/> 数字签名 (X.509) <span>无</span>  <b>IPSec安全方法</b> <input checked="" type="checkbox"/> 中等 (AH) 高等 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES  <b>回拨功能 (CBCP)</b> <input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 <input type="text"/> 回拨定额 <input type="text" value="0"/> 分钟
--	---

### 4. TCP/IP网络设定

我的WAN IP <input type="text" value="0.0.0.0"/> 远端网关IP <input type="text" value="0.0.0.0"/> 远端网络IP <input type="text" value="0.0.0.0"/> 远端子网掩码 <input type="text" value="255.255.255.0"/> <input type="button" value="更多"/>	RIP方向 <span>禁用</span> RIP版本 <span>Ver. 2</span> 在NAT操作中, 将远端子网视为 <span>私网IP</span>  <input type="checkbox"/> 变更默认路由到此VPN隧道
---	--

#### 允许拨入的类型

确定允许拨入的 VPN 类型。

#### ISDN

允许远端拨入的 ISDN LAN-to-LAN VPN 连接。您还需要为 VPN 拨出端设定用户名和密码来进行安全认证。您也可以进一步设定回拨功能。

#### PPTP

允许远端拨入的 PPTP LAN-to-LAN VPN 连接。您还需要为 VPN 拨出端设定用户名和密码来进行安全认证。

#### IPSec 隧道

允许远端拨入的 IPSec LAN-to-LAN VPN 连接。

#### 应用 IPSec 策略的 L2TP

允许远端拨入的 L2TP/IPSec LAN-to-LAN VPN 连接。您可以选择单独使用 L2TP 或者应用 IPSec 策略的 L2TP: 无-建立单纯的 L2TP VPN。

**最好使用**-如果拨入端的设定也是应用 IPSec 策略的 L2TP, 则启用 IPSec, 否则建立单纯的 L2TP VPN 连接。

**一定要有**-拨入端必须使用应用 IPSec 策略的 L2TP VPN, 而不能使用单纯的 L2TP VPN 连接。

#### 指定远端 VPN 网关

#### 端点 VPN 服务器 IP 或端点 IP

如果拨入的 VPN 类型是 PPTP L2TP 或 IPSec 主模式(Main mode), 那么该选项是可选的。如果拨入的 VPN 类型是 IPSec 极模式 (Aggressive mode), 那么该选项是必选的。

该功能默认是禁用的, 也就是说任何远端用户 (特别是使用动态 IP 地址的用户) 都可以使用此设定档的设置建立 VPN 到 Vigor 路由器。

如果为了安全性需要限制特定的用户才能拨入 VPN, 您可

以启用**指定远端节点**功能，并在**端点（Peer）VPN 服务器 IP** 栏里填入该特定 VPN 服务器的公网 IP 地址。这样，即使其他用户的设置都匹配此设定档，由于他们的公网 IP 地址不被允许拨入，他们也无法建立 VPN 连接。如果拨入的 VPN 类型是 IPSec 积极模式，必须启用此功能，并在**端点 ID** 栏里设置一个 ID（不需要设置**端点（Peer）VPN 服务器 IP**）。ID 的格式可以是 Email 地址，域名或字符串。这个 ID 在远端 VPN 路由器里也要输入，如果远端 VPN 路由器也是 Vigor，对应的值是**拨出设定里的本地 ID**。如果之前**拨入类型**选择 ISDN 则在开启此选项后，请在空白栏输入 VPN 远端路由器的 ISDN 号码。

如果您没有选择此选项，那么该条 LAN to LAN VPN 的认证方式和安全方法将使用在 **IPSec 基本设定** 里面所设定的值。

用户名	当您选择的 VPN 模式为 ISDN, PPTP 或 L2TP 时必须设置此项，该用户名必须匹配远端 VPN 路由器上的相关设定。
密码	当您选择的 VPN 模式为 ISDN, PPTP 或 L2TP 时必须设置此项，密码必须匹配远端 VPN 路由器上的相关设定。
VJ 压缩	它用于 TCP/IP 协议头的压缩，可以稍微节省一点带宽。建议使用默认设定：开启。
IKE 认证方法	<p>一旦启用了<b>指定远端 VPN 网关</b>功能，就必须为此设定档单独配置 <b>IKE 认证方法</b>和 <b>IPSec 安全方法</b>。这里的设定与 <b>IPSec 基本设定</b>里的设置在功能上是一样的，只不过它被限定只能用于指定的用户。这里的设置适用于 IPSec VPN 和应用 IPSec 策略的 L2TP VPN。但是即使<b>指定远端 VPN 网关</b>没有被启用，您仍然可以编辑数字证书的设置。</p> <p><b>预共享密钥</b> - 输入预共享密钥。必须和 VPN 拨出端的设定相同。</p> <p><b>数字签名 (X.509)</b> - 选择一个在 IPSec 端点认证中设定好的 Peer ID 项</p>
IPSec 安全方法	<p>选择允许的 IPSec 安全方法。注意：该设定仅用于 IPSec 第二阶段的协商。</p> <p><b>中等 (AH)</b> - 数据将被认证，但不会被加密。默认该选项被启用。</p> <p><b>高等 (ESP)</b> - 数据将被认证和加密。这里我们支持 DES, 3DES 和 AES 加密方式。默认所有选项都被启用。</p>
回拨功能	<p>回拨功能为 ISDN 拨入用户提供了回拨服务。</p> <p><b>启用回拨功能</b> - 启用回拨功能。</p> <p><b>使用以下号码回拨</b> - 此项设定是为了增加安全性，一旦启用此选项，路由器只会对该特定的<b>回拨号码</b>回拨。</p> <p><b>回拨定额</b>（单位：分钟）- 定义远端拨入用户的时间资费，该资费会随着每次回拨连接而递减。回拨功能有一个时间限制，一旦回拨资费被耗尽，则回拨功能将自动停止。</p>

以下两个设定仅用于 PPP 相关的 VPN 连接，包括 PPTP, L2TP, 应用 IPSec 策略的 L2TP，如果是纯 IPSec VPN，请保留此处的默认设定。

**我的 WAN IP/远端网关 IP** PPP 协商阶段完成安全参数的协商后，会立即开始 IPCP 协商阶段，作用是为 PPP 链路两端的 PPP 接口协商 IP 地址。从本地路由器的角度看，**我的 WAN IP** 对应 PPP 链路的本地 PPP 接口，**远端网关 IP** 对应 PPP 链路的远端 PPP 接口。**注意：这两个 IP 是虚拟 IP，用于 VPN 隧道，并不是实际的公网 IP 地址或本地网关。如果您不熟悉 IPCP 协议，请使用默认的设置：0.0.0.0，在协商 IPCP 的时候将使用远端 VPN 路由器分配的 IP 地址。**

以下设定用于所有类型 VPN：

**远端网络 IP** 指定远端 VPN 子网。注意，这里必须输入一个网络 IP，而不是一个具体的 IP 地址。譬如远端 VPN 子网是一个 C 类网，内网机器的 IP 是 192.168.100.x（x：1~254），那么您应该在这里输入 192.168.100.0。

**远端网络掩码** 指定远端 VPN 子网的掩码。

**更多** 按此按钮将弹出一个窗口，如下图所示。在这个窗口里您可以添加静态路由。在**网络 IP** 栏里输入要访问的网络 IP，在下拉菜单里选择相应的子网掩码，然后点击**新增**按钮。**注意，在这里添加的静态路由必须是能通过远端 VPN 子网可路由访问的（请先确认您可以从远端 VPN 子网访问那些添加的网络）。另外，如果您连接的 VPN 是 IPSec，并且远端 VPN 路由器是其它厂商的路由器，最好不要使用这个功能，因为它是专门针对 Vigor 和 Vigor 建 VPN 而设计的，我们不保证其它厂商的路由器能配合此功能**

**RIP 方向** 除了在**更多**里添加静态路由，您也可以通过 VPN 隧道使用 RIP 协议传送路由信息。**TX/RX** 两者是指即发送 RIP 路由信息，又接收 RIP 路由信息；**仅 RX** 是指仅接收 RIP 路由信息；**仅 TX** 是指仅发送 RIP 路由信息；**停用**是指禁止通过 VPN 隧道传送 RIP 路由信息。

**RIP 版本** 选择 RIP 协议的版本。为获得最大的兼容性，请使用版本 2。

**F 在 NAT 操作中，将远端子网络视为** 默认设置是**私网 IP**，绝大多数应用都应该选这个默认设置。如果没有特殊的目的，请不要选择**公网 IP**。这里的**公网 IP** 是一个逻辑概念，并不是真正的公众网。当两个路由器建立了一条 VPN，两边的网络便能通过 VPN 隧道互相访问，如果您希望只有一个方向能访问，另一个方向不能访问，可以选择**公网 IP**。

譬如，您在路由器 A 里选择**公网 IP**，路由器 B 里选择**私网 IP**，那么 VPN 建好后，路由器 A 的网络可以访问路由器 B 的网络，而路由器 B 的网络不能访问路由器 A 的网络。此时路由器 A 的网络被当作 NAT LAN，而路由器 B 的网络被当作公网。**注意：请慎用此功能。**

**变更默认路由到此 VPN 隧道** 当 VPN 连接建立好后，将使用远端 VPN 路由器的网关做为本地的默认网关。也就是说，所有访问 Internet 的数据包都先通过 VPN 隧道路由到远端 VPN 路由器，再通过远端 VPN 路由器被发送到 Internet。该设定仅对**拨出**方向的

VPN 有用，所以一旦您启用了这个功能，**一般设定**栏里面的**拨叫方向**将被自动设定为**拨出**。**注意：**一旦该 VPN 连接建立好后，就无法建立其它任何 VPN 连接了。

3.8.7 连接管理

在 VPN 连接管理页面,您可以看到所有连接中的 VPN 列表及其状态,您可以通过 Drop 键来终止某条 VPN 连接,也可以通过拨号键来初始某条选中的 VPN 连接。

VPN和远程访问 >> 连接管理

拨出工具

更新间隔: 10 刷新

▼ 拨号

VPN 连接状态

当前页: 1 页码 转到 >>

VPN	类型	远端IP	虚拟网络	发送封包数	传送速率	接收封包数	接收速率	运行时间
xxxxxxxx: 数据已加密。 xxxxxxxx: 数据未加密。								

- 拨号

点击可以初始选中的 VPN 连接。
- 更新间隔

可以选择 VPN 列表的刷新时间,可选的值为 5, 10 以及 30 秒。
- 刷新

点击可以刷新连接种的 VPN 列表及其状态。

注释: 对于 LAN to LAN ISDN 连接状态显示在连线状态栏。

系统状态				系统已运行时间: 4: 27: 31			
局域网状态		首选DNS服务器: 194.109.6.66				备用DNS: 168.95.1.1	
IP地址	上行封包	下行封包					
192.168.1.1	137	0					
WAN 1状态							
已启用	线路	名称	模式	在线时间			
是	Ethernet		Static IP	4:27:23			
IP	网关IP	上行封包	上行速率	下行封包	下行速率		
172.17.1.11	172.17.1.3	24283	1649	30003	399		
WAN 2 状态							
已启用	线路	名称	模式	在线时间			
否	以太网		---	00:00:00			
IP	网关IP	上行封包	上行速率	下行封包	下行速率		
---	---	0	0	0	0		
ISDN状态							
频道	已启用连接	上行封包数	上行速率	下行封包数	下行速率	在线时间	AOC
B1	Idle [---]	0	0	0	0	0: 0: 0	0
B2	Idle [---]	0	0	0	0	0: 0: 0	0
D	DOWN						

### 3.9 证书管理

数字证书用于在 IPSec 通讯会话双方之间建立一个加密的 VPN 通道之前，保证会话双方的可信性。数字证书提供了这一保证。一个数字证书包括一个公开密钥和一些识别信息。这些识别信息是由一个受信任的第三方签名的。这个第三方是一个证书授权中心（CA）。因为这个 CA 是可信的，所以它发行的证书也就是可信的。要获得一个证书，VPN 会话的一方需要在一个证书申请表中将它自己的公钥发送到 CA。这个证书请求包括用来唯一识别这个 VPN 会话方的身份的信息，例如一个 IP 地址，域名或者电子邮件地址。根据所申请的数字签名，CA 创建一个数字证书，这个数字证书和 VPN 会话方自己的证书一同生效。一旦 VPN 会话方获得了他们的数字证书和 CA 证书，他们就准备好开始通讯了。当一个会话开始时，IKE 包括一个 VPN 对等的双方交换他们的数字证书的阶段。在这期间他们是由 CA 证书验证的。在这一验证过程之后，公共密钥被从这个数字证书中提取出来，并应用到要建立的 IPSec VPN 通道中去。

Vigor 路由器支持基于 X.509 标准的证书，VPN 的对端也必须支持基于 X.509 标准的证书。

在这里您可以生成，设置本地数字证书以及设定 CA 证书。请您在设定和配置证书前，先调整路由器的系统时间到准确的值，以获得有效的证书。



#### 3.9.1 本地证书

证书管理 >> 本地证书

X509本地证书设定

名称	主题	状态	修改
本地	---	---	<input type="button" value="查看"/> <input type="button" value="删除"/>

X509本地证书



生成

点击此处可以打开生成证书请求的窗口。  
证书管理 >> 本地证书

生成证书请求

可替代识别名称 (Subject Alternative Name)

类型

IP地址

IP

识别名称 (subject name)

国家 (C)

洲 (ST)

区域 (L)

组织 (O)

组织 (OU)

通用名 (CN)

Email (E)

密钥类型

RSA

密钥大小

1024 位

生成

导入

点击此键来上传一个获得签名的本地证书。

刷新

点击此键来刷新关于本地证书的信息列表。

查看

点击此键来查看选中项本地证书的具体参数。

删除

点击此键删除证书。

点击生成按键后，生成的信息如下图所示：

证书管理 >> 本地证书

X509本地证书设定

名称	主题	状态	修改
本地	/C=53/ST=7657/L=53/O=7567/OU...	Requesting	<div>查看</div> <div>删除</div>

生成

导入

刷新

X509本地证书请求

-----BEGIN CERTIFICATE REQUEST-----  
MIIBzDCCATUCAQAwajELMAkGA1UEBhMCNTMxDTALBgNVBAgTBDbc2NTcxZzAJBgNV  
BAAjUzMQ0wCwYDVQQKEwQ3NTY3MQswCQYDVQQLEwIOMzEOMAwGA1UEAxMFNTc2  
NTcxZzARBgkqhkiG9w0BCQEWDG2NzgwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ  
AoGBAPHxUFbGNuLNaZEihAJNMuyN24fvNqsoG0vffwCV5GWqY/zViNqa/OXCMLd  
zKA85Sbgj8hp81lnIXFsirexEzxdul+YupiYDHR2QZA28VofbJXE/51KBNgyzIe  
Dg+ffgyw/A+h9fB4nlLpp9tu+Jt83DH2QzuHlyKkP/WSHi6xAgMBAAGgIjAgBgkq  
hkiG9w0BCQ4xEzARMA8GA1UdEQQIMAaHBMCoARcwDQYJKoZIhvcNAQEFBQADgYEA  
lrWzyYt0IGSq/QCs9Nuhx3ESF2KUciBzMKwR3+jSUy/PqyQ4bcgnakuCin++dGP  
wIRjiUvLrROG6zorn3naxTP53r797LuobklwoDazC15bgffSHZvVbq3X0JU46BgX  
GR82Q7twmCDfKyCr+GeP6tx7F/IZ6gaQZ1ZPsJ0uGrM=  
-----END CERTIFICATE REQUEST-----

注意：您需要将该证书请求提交到 CA 服务器，以获取一份签名的本地证书。随后再将获得 CA 服务器签名的本地证书导入 Vigor 路由器。

Vigor2910 系列中文手册

115

### 3.9.2 可信 CA 证书

VPN端点为了彼此向对方证明它们自己，必须都从同一个证书发布中心获得一个CA证书。这个CA证书为VPN端点提供了验证它们从其它设备收到的数字证书的方法。Vigor路由器获取CA 证书是为了验证它从VPN另一端收到的数字证书。同样地，VPN另一端获取CA证书是为了验证它从Vigor路由器收到的数字证书。

可信 CA 证书列表中可以设定三类 CA 证书。

证书管理 >> 可信CA证书

#### X509可信CA证书设定

名称	主题	状态	修改	
可信CA-1	---	---	查看	删除
可信CA-2	---	---	查看	删除
可信CA-3	---	---	查看	删除

导入 刷新

点击**导入**后，会弹出下图所示的页面。点击 **浏览...**，找到证书后再点击**导入**上传 CA 证书。

证书管理 >> 可信CA证书

#### 导入X509可信CA证书

选择可信CA证书文件

Browse...

点击 **导入** 上传证书

点击**查看**可以显示所选 CA 证书的详细信息。点击**删除**可以删除所选 CA 证书。



### 3.9.3 证书备份

路由器的本地证书和可信 CA 证书可以被保存在一个文件中。请点击下图中的**备份**按钮来备份路由器的本地证书和可信 CA 证书。您需要为证书添加**加密密码**和**重新输入密码**。

证书管理 >> 证书备份

证书备份 / 还原

备份

加密密码:

重新输入密码:

点击  以将证书以文件形式下载到你的电脑。

还原

选择一个备份文件以还原。

解密密码:

点击  以上传文件。

## 3.10 VoIP

网络电话(VoIP)允许您使用宽带线路通过 Internet 进行高质量语音通话。

目前有许多不同的信令协议,使得 VoIP 设备可以互相通话。其中,最流行的协议有 SIP, MGCP, Megaco 和 H.323。这些协议互相之间不兼容(除非通过一个 soft-switch 服务器)。

Vigor 路由器支持 SIP 协议因其已被 ITSP(Internet 电话服务提供商)广泛使用,且广泛应用于软件电话方面。SIP 是一个端到端信令协议可实现用户在线和移动性。每个用户可以使用其 SIP 格式的源地址身份, SIP 地址。标准格式的 SIP 地址如下:

**sip: user:password @ host: port**

在一些领域的不同应用是可选的。通常来说,“host”表示一个域。“userinfo”包括“user”区,密码区和一个跟在它们后面“@”符号。这和 URL 十分相似所以也可以称为“SIP URL”。SIP 协议支持点到点直接通话和通过 SIP 代理服务器(一个和 H.323 网络维护器相类似的设备)进行通话。而 MGCP 协议使用客户端—服务器结构,通话拓扑和传统电话网络类似。

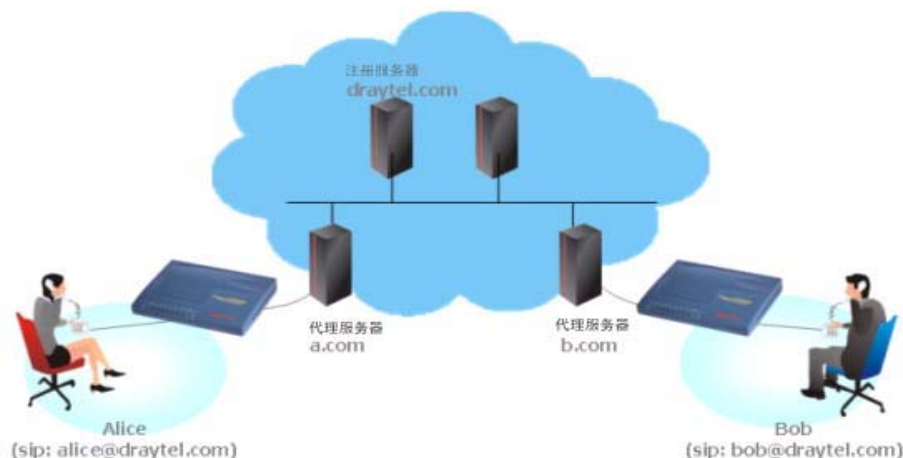
当通话建立之后,语音流量使用 RTP(实时通话协议)进行传输。不同的编码方式(用来压缩和解压语音)可以装入 RTP 包中。ZTE 路由器提供多种编码方式,包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B。每种编码使用不同带宽,因为提供了不同的语音质量。使用越高带宽意味着越好的语音质量,然而编码一定要适应 Internet 带宽。

以下为通常的两种通话方式:

- **通过 SIP 服务器**

首先,您的 Vigor 路由器必须发送注册消息向 SIP 注册服务器注册,然后,双方 SIP 代理会转发一些消息给对方来建立一个会话。

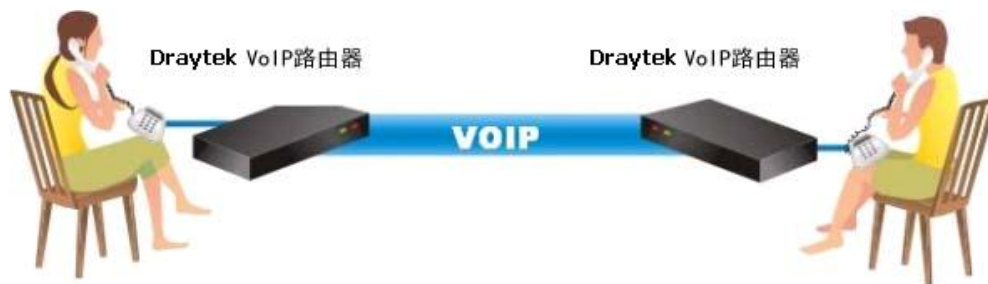
如果双方注册到相同的 SIP 注册服务器,如下图所示:



这个方式主要好处就是您不必记忆对方的 IP 地址,这些 IP 地址可能常常动态地改变。如果您使用相同的 SIP 注册服务器您只需要使用电话簿或者直接拨打对方的帐户名。请参考例 1 和例 2。

- **点到点**

在通话前,您必须知道对方的 IP 地址。Vigor VoIP 路由器将建立一条连接。请参考例 3



Vigor 路由器首先使用最有效率的编码来最大程度的利用带宽，但 Vigor 路由器同时具有自动服务质量保证。服务质量保证协助给语音流量分配高优先级。上行和下行的带宽将一直给语音流量以高的优先级，但是代价只是数据流量会稍稍变慢在可承受的范围内。

以下是认证管理的菜单条目：



### 3.10.1 电话簿

此页面允许您给 VoIP 功能设置**电话簿**和**号码规则**。点击电话簿和号码规则连接来进入下一页设定电话簿。

VoIP >> 电话簿设定

电话簿设定

<a href="#">电话簿</a> <a href="#">号码规则</a>
---

#### 电话簿

在这个部分中，您可以在电话簿中设定 VoIP 的联系人来帮助您快速的拨号和容易使用快速拨号电话簿。在电话簿中共有 60 条允许储存您朋友和家人的 SIP 地址。如果您是用的 Vigor 2910VGi 路由器将显示显示**备用自和 后备电话号码**。

电话簿

索引值	电话号码	显示名	SIP URL	备用自	后备电话号码	状态
<a href="#">1.</a>				None		x
<a href="#">2.</a>				None		x
<a href="#">3.</a>				None		x
<a href="#">4.</a>				None		x
<a href="#">5.</a>				None		x
<a href="#">6.</a>				None		x
<a href="#">7.</a>				None		x
<a href="#">8.</a>				None		x
<a href="#">9.</a>				None		x
<a href="#">10.</a>				None		x
<a href="#">11.</a>				None		x
<a href="#">12.</a>				None		x
<a href="#">13.</a>				None		x
<a href="#">14.</a>				None		x
<a href="#">15.</a>				None		x
<a href="#">16.</a>				None		x
<a href="#">17.</a>				None		x
<a href="#">18.</a>				None		x
<a href="#">19.</a>				None		x
<a href="#">20.</a>				None		x

<< [1-20](#) | [20-40](#) | [40-60](#) >>

状态: v - 使用中, x - 未使用, ? - 空白

下一页 >>

点击任意索引值会显示电话簿设定页面。

电话簿索引 1

☒ 启用

电话号码

显示名

SIP URL

688

david

8201 @ iptel.org

确定

清除

取消

- 启用

选中启用此条目。
- 电话号码

索引值的快速拨号号码。您可以选择任何号码，**0-9** 和\*号。
- 显示名

想在对方屏幕上显示的呼叫者身份。这使对方可以辨识来电者的身份而不用去记忆许多 SIP 地址。
- SIP URL

输入对方的 SIP 地址。

此页面在不同的路由器型号会有不同的显示。以下是 Vigor 2910VGi 的显示页面。**备援线路**和**备用电话号码**仅在 2910VGi 型号支持。

电话簿索引 1

☒ 启用

电话号码

688

显示名

david

SIP URL

8201

@iptel.org

备援线路

ISDN

备用电话号码

12345678

确定

清除

取消

- 启用

选中启用此条目。
- 电话号码

索引值的快速拨号号码。您可以选择任何号码，0-9 和\*号。
- 显示名

想在对方屏幕上显示的呼叫者身份。这使对方可以辨识来电者的身份而不用去记忆许多 SIP 地址。
- SIP URL

输入对方的 SIP 地址。
- 备援线路

在 Vigor 2910VGi 中，此页面显示如下。

备援线路

ISDN

None

ISDN

- 备用电话号码

当 Voip 电话不能拨通或者互联网连接断开时，备用电话号码就会取代 VoIP 电话号码被拨出。此时，VoIP 电话就会依据所设置的备援线路方向被 PSTN 线路电话所取代。请注意，在切换电话的过程中，会有短时的蜂鸣声。而且当切换到 PSTN 电话时，电信服务提供商可能进行收费。请在 VoIP 电话设定中输入备用电话号码（PSTN 号码）。

号码规则

为了使用者方便，此页面允许用户编辑 SIP 帐号前缀号码，包括添加号码，剥离号码或替代号码。这可以用来帮助用户快速且简便的通过 VoIP 接口拨号。

号码规则设定

#	启用	前缀号码	模式	OP号码	最小长度	最大长度	接口
1	<input checked="" type="checkbox"/>	03	替代	8863	7	9	
2	<input checked="" type="checkbox"/>	886	剥离	886	7	9	
3	<input type="checkbox"/>		无		0	0	
4	<input type="checkbox"/>		无		0	0	
5	<input type="checkbox"/>		无		0	0	
6	<input type="checkbox"/>		无		0	0	
7	<input type="checkbox"/>		无		0	0	
8	<input type="checkbox"/>		无		0	0	
9	<input type="checkbox"/>		无		0	0	

- 启用

选中启用此设定。

## 前缀号码

### 模式

用来添加，剥离或替代的号码。

无 - 无操作

添加 - 一旦选择此模式，OP 号码会被添加在到从特定 VoIP 接口拨号号码前缀号码。

剥离 - 一旦选择此模式，OP 号码会被从特定 VoIP 接口拨号号码前缀号码中剥离。以图片中的设置为例，前缀号码为 886 时，OP 号码 886 会被全部剥离。

替代 - 一旦选中此模式，OP 号码会被替代成特定 VoIP 接口拨号号码中的前缀号码，以图片中的设置为例，OP 号码 8863 会被设置的前缀号码 03 完全替代。

#### 模式



## OP 号码

这里输入的号码是您需要进行特殊处理帐号号码的第一部分。

## 最小长度

设置用来应用前缀号码设定的最小拨号号码的长度。如图所示，如果拨号号码在 7-9 位之间，这些号码可以应用这里设置的前缀号码。

## 最大长度

设置用来应用前缀号码设定的最大拨号号码的长度。

## 接口

从六个预保存帐号选择您需要启用前缀号码设定的接口。

## 3.10.2 SIP 帐号

在这一部分里，您可以设定 SIP 参数。当您申请一个帐号，您的 SIP 服务提供商将给您一个帐号名或者用户名，SIP 注册服务器，SIP 代理和域名。（最后三项可能在某些情况下，可能完全相同）。您可以告知对方您的 SIP 地址**帐号名称@网域名称**

当 Vigor VoIP 路由器打开之后，将首先注册帐号名称@网域名称到注册服务器。之后，您的通话将 SIP 代理服务器以帐号名称@网域名称转发到目的地。

### VoIP >> SIP帐号

#### SIP帐户列表

刷新

索引	设定档	域名	代理	帐户名	振铃端口	状态
1	david	iptel.org	iptel.org	8201	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
2				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
3				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
4				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
5				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
6				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-

R: 成功注册到SIP服务器  
-: 注册SIP服务器失败

#### NAT穿透设定

STUN服务器:	<input type="text" value="stun.fwdnet.net"/>
外部IP:	<input type="text"/>
SIP PING间隔:	<input type="text" value="150"/> 秒

确定



索引	点击此链接来进入下一页设定 SIP 帐户。
设定档	显示帐户的设定档名称。
域名	显示 SIP 注册服务器的域名或 IP 地址。
代理	显示 SIP 代理服务器的域名或 IP 地址。
帐户名	显示 SIP 地址中@之前的帐户名。
振铃端口	指定收到来电后哪一个端口振铃。
STUN 服务器	输入 STUN 服务器的 IP 地址。
外部 IP	输入网关 IP 地址。
SIP PING 间隔	默认值是 150 秒。对 Nortel 服务器做 NAT 穿透时使用。
状态	显示相对应的 SIP 帐户的状态。 <b>R</b> 意味着成功注册到服务器。—则表示注册 SIP 服务器失败。

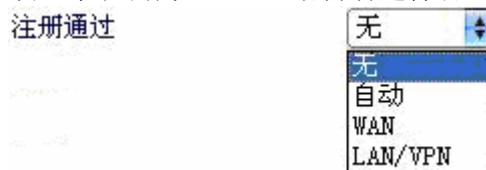
#### SIP帐户索引值 2

设定档名称	test (最多11个字符)
注册通过	无 <input type="checkbox"/> 不注册拨打电话
SIP端口	5060
域名	iptel.org (最多63个字符)
代理	iptel.org (最多63个字符)
<input type="checkbox"/> 作为通话代理	
显示名称	(最多23个字符)
帐户号/名	8201 (最多63个字符)
<input type="checkbox"/> 认证 ID	(最多63个字符)
密码	(最多63个字符)
过期时间	1小时 3600 秒
NAT穿越支持	无
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
振铃模式	1

确定 取消

**设定档名称** 制定一个名称给设定档。您可使用和域名相类似的名字。例如，如果域名是 draytel.org，您可以使用 draytel-l。

**注册通过** 如果您需要拨打语音电话而不注册个人信息，请选择**无**。一些 SIP 服务器允许用户使用 VoIP 功能而不注册。对于这类服务器，请选择**不注册拨打电话**选项。推荐使用**自动**选项，系统会为 VoIP 通话自动选择合适的路径。



**SIP 端口** 设定建立回音时发送/接收 SIP 消息的端口号。默认值是 **5060**。您设定的端口号必须与注册服务器端相同。

**域名** 设置 SIP 注册服务器的域名或 IP 地址。

代理	设置 SIP 代理服务器的域名或 IP 地址。您可以输入:端口来制定数据传输的端口（例如，nat.dryatel.org:5065）。
作为通话代理	选中此项来使代理作为一个通话代理。
显示名称	想在对方屏幕上显示的通话者名称。
帐户号/名	输入您的 SIP 地址的帐号名，例如@之前的所有文本。
认证 ID	选中此项来启用此功能，并且输入用来和 SIP 注册服务器验证名称或号码，但不是必须的。
密码	注册 SIP 服务中所需的密码。
过期时间	注册服务器保留您的注册信息的时间长度。在时间过期之前，路由器会发送另外一个注册请求。
NAT 穿越支持	如果路由器通过另外一台设备连接到 Internet，您必须设置此选项。

NAT穿越支持



**无**—禁用此功能。

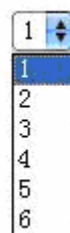
**Stun**—选择此项如果您使用 Stun 服务器。

**手动**—选择此项如果您想手动制定一个外部地址来穿越 NAT。

**Nortel**—如果您使用的 soft-switch 支持 nortel 解决方案，您可以选择此项。

振铃端口	设定 VoIP1 或者 VoIP2 作为默认振铃端口。
振铃模式	给 VoIP 通话选择一种振铃类型。

振铃模式



以下展示了成功的 SIP 帐户设定，仅供参考。

SIP帐号列表

刷新

索引	设定档	域名	代理	帐户名	振铃端口	状态
1	david	iptel.org	iptel.org	8201	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
2	draytek_1	draytel.org	draytel.org	813177	<input type="checkbox"/> VoIP1 <input checked="" type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
3				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
4				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
5				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
6				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-

R: 成功注册到SIP服务器  
-: 注册SIP服务器失败

NAT穿透设定

STUN服务器:

stun.fwdnet.net

外部IP:

SIP PING间隔:

150

秒

确定

3.10.3 电话设定

此页面允许用户分别设定 VoIP1 和 VoIP2 的电话设定。

VoIP >> 电话设定

电话列表

索引	端口	呼叫功能	Codec	声音	增益(麦克风/话筒)	默认SIP帐户	DTMF中转
1	FXS 1		G.729A/B	用户自定义	5/5	david	InBand
2	FXS 2		G.729A/B	用户自定义	5/5	david	InBand
3	ISDN		G.729A/B	用户自定义	5/5	david	InBand

RTP

☐ 对称RTP

动态RTP开始端口

10050

动态RTP结束端口

15000

RTP TOS

IP precedence 5

10100000

确定

电话列表

端口-共有三个电话端口可供配置。

呼叫功能-这里显示这个端口启用的呼叫功能的大致描述。

Codec-显示所选择的默认编码。您可以点击索引号来改变默认编码。

声音-显示用户设置的声音设定。

增益-显示麦克风/话筒的增益，可以通过高级设定进行修改。

默认 SIP 帐户 -“david” 是当前默认的 SIP 帐户。您可以点击索引号更改每个电话口的 SIP 帐户。

DTMF 中转-显示在高级设定中设置的 DTMF 模式。

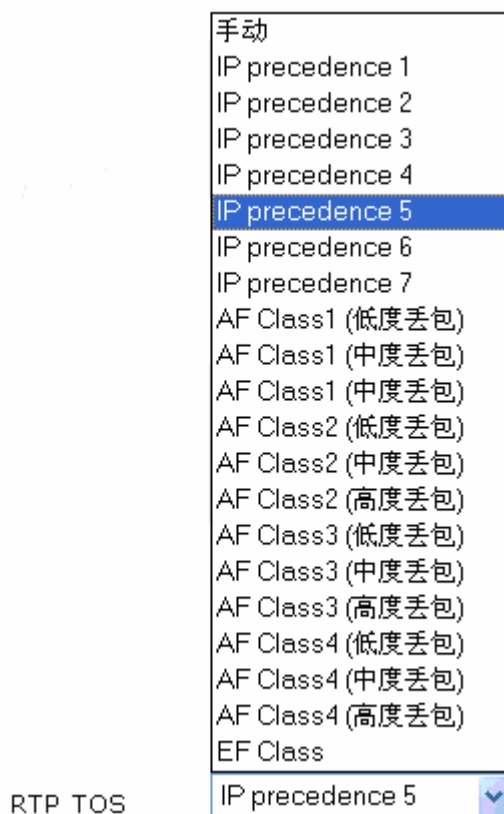
## RTP

**对称 RTP** –选中此项来启用此功能。您可以选中此项解决数据传输过程中两端路由器的不兼容（例如，从远端路由器公网地址发送数据到本地路由器的私网地址）。

**动态 RTP 开始端口**-指定 RTP 流量的开始端口。默认值是 10050。

**动态 RTP 结束端口**- Specifies the end port for RTP stream. The default value is 15000.

**RTP TOS** –指定 VoIP 封包的优先级。使用下拉式菜单来选择。



## VoIP1 和 VoIP2 的详细设定

点击索引栏中的数字 **1** 或者 **2**，您可以访问如下页面来配置电话设定。  
VoIP >> 电话设定

电话索引号1

呼叫功能

☐ 热线

☐ 会话计时器

☐ T.38传真功能

3600

秒

呼叫转移

禁用

SIP URL

超时

30

秒

☐ DND(免打扰)模式

索引(1-15) 计划任务 设定:

注: 计划任务中的动作和超时设定将被忽略。

Index(1-60) in Phone Book as Exception List:

☐ CLIR (隐藏呼叫者ID)

☐ 呼叫等待

☐ 呼叫转接

编码

优先编码

G.729A/B (8Kbps)

☐ 单一编码

数据包大小

20毫秒

声音状态检测(VAD)

关

默认SIP帐户

1-david

☐ 当帐户注册成功时有拨号音

默认呼叫路由

☐ 到ISDN:拨号 \*# 给VoIP

☒ 到VoIP:拨号 #\* 为ISDN

确定

取消

高级

**热线** 选中此选项来启用。输入 SIP URL，此 URL 会在您拿起听筒时自动拨出。

**会话计时器** 选中此选项来启用。您在此所设定的限制时间内如果无响应，则通话会被自动挂断。

**T.38 传真功能** 如果远端也支持 FAX 功能，您可以选中来启用此功能。

**呼叫转移** 此处有四个选项。**禁用**关闭呼叫转移功能。**一直**意味着所有来电将会被无条件转移到 SIP URL。**遇忙**意味着来电只有在本地系统忙时才会被转移到 SIP URL。**无应答**意味着来电在没有相应时才会被转移到 SIP URL。



**SIP URL** –输入 SIP URL（例如 aaa@draytel.org 或者 abc@iptel.org）作为呼叫转移目的地。

**超时** –设置呼叫转移超时时间。默认设定为 30 秒。

**DND（免打扰）模式** 设置一段时间不被 VoIP 电话打扰。在这段时间内，呼叫方将听到忙音，而本地用户将不会听到任何振铃声。

**索引(1-15) 计划任务** -输入计划任务的索引号来控制DND模式。详细设定请参考 **3.5.2 计划任务**。

**索引（1-60）电话簿** -输入电话簿的索引号。详细设定请参考 **3.10.1 电话簿**。

**呼叫等待** 选中启用此功能。当有新电话打入时会给用户一个提示音。请您按闪断键接听等待的来电。

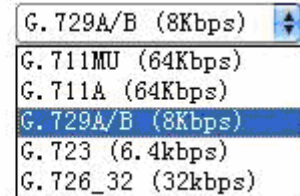
## 呼叫转接

选中启用此功能。请您按闪断键转接另一个通话。当新的通话连接成功时，挂断电话。此时另外两方可以直接通信。

## 优先编码

从五个编码中选择 VoIP 通话的默认编码。由于每次通话之前会协商双方使用的编码，很有可能不使用您的默认值。默认编码为 G.729A/B，它在提供不错的通话质量外占用很小的带宽。如果您的上行带宽只有 64Kbps，不要使用 G.711 编码。使用 G.711 时，您的上行带宽至少在 256Kbps 以上。

优先编码



**单一编码**—如果选中，则只有选择的编码会被应用。

**数据包大小**—单一数据包包含的数据容量，默认值为 20ms，则单一数据包包含 20ms 的语音信息。

数据包大小



**声音状态检测** - 此项功能可以侦测双方的语音是否活动。如果不活动，路由器会保留带宽给其他应用。

声音状态检测(VAD)



## 默认 SIP 帐户

有六组 SIP 帐号可供选择。使用下拉式菜单来选择默认帐户。

**当帐户注册成功时有拨号音**—选中启用此功能。

## 默认呼叫路由

定义路由器的默认呼叫的方向。

**到 ISDN (给 VoIP)**— 路由器默认使用 ISDN 拨号。如要改用 VoIP 拨号，请拨打前缀号码来转换。您可以输入的字符为\*, #, and 0~9。

**到 VoIP (给 ISDN)** -路由器默认使用 VoIP 拨号。如要改用 ISDN 拨号，请拨打前缀号码来转换。您可以输入的字符为\*, #, and 0~9。

另外，您可以使用**高级**选项来进行声音设定，声音增益，MISC 和 DTMF 模式。**高级**设定用来使路由器和本地通讯系统协同工作。错误的声音设定可能导致用户的不便。简单地选择合适的区域（已预先设定好声音设定和来电显示类型），就能改变电话的声音模式。或者您可以手动来调整声音设定，选择用户自定义模式。TOn1, TOff1, TOn2 和 TOff2 表示声音的音调 TOn1 和 TOn2 代表有声音的时段; TOff1 和 TOff2 无声音的时段。

高级设定 >> 电话索引号1

声音设定

区域

UK

来电显示ID类型

FSK\_ETSI (UK)

	低频(Hz)	高频(Hz)	T on 1 (毫秒)	T off 1 (毫秒)	T on 2 (毫秒)	T off 2 (毫秒)
拨号音	350	440	0	0	0	0
振铃音	400	450	400	200	400	2000
忙音	400	0	375	375	0	0
拥塞音	480	620	400	350	225	525

声音增益

麦克风增益(1-10)

5

话筒增益(1-10)

5

DTMF

DTMF模式

InBand

载荷类型(rfc2833)

101

MISC

拨号音功率

27

振铃频率

25

确定

取消

**区域** 选择您所在的区域。**来电显示 ID 类型**，**拨号音**，**振铃音**，**忙音**和**拥塞音**会被自动设定。如果您不能找到合适的，请选择**用户自定义**，来手动设定拨号音，振铃音，忙音和拥塞音的值。

区域

UK

用户自定义

UK

US

丹麦

意大利

德国

荷兰

葡萄牙

瑞典

澳大利亚

Slovenia

Czech

Slovakia

当然，您可以手动设置每个值。推荐使用 VoIP 通讯中的默认设定。

**来电显示 ID 类型** 在电话机上显示来电者的 ID 具有许多不同的标准。选择适合您的电话的标准依据您所在的地域。如果您不知道选择

何种标准，请选择默认设定。

来电显示ID类型

FSK_ETSI
FSK_ETSI
FSK_ETSI (UK)
FSK_BELLCORE (US/AU)
DTMF
DTMF (DK)
DTMF (SE/NL/FIN)

## 声音增益

**麦克风增益(1-10)/听筒增益 (1-10)** – 输入数字 0-10 来调整麦克风和听筒的音量。数字越大，声音越响。

## MISC

**拨号音功率** – 用来调整拨号音的响度。数值越小，声音越大。推荐使用默认设定。

**振铃频率** – 用来调整振铃的频率。推荐使用默认设定。

## DTMF

**InBand** -选择此项，当您按动电话的号码盘时，Vigor 路由器会直接像发送声音信号发送 DTMF 信息。

**OutBand** -选择此项，Vigor 路由器会先在号码盘上捕捉按键号码，然后转换成数字进行发送。接受方会依据接受到的数字信号产生一个 DTMF 信号。此功能在网络拥塞时能保证准确地 DTMF 传输。

**SIP INFO**-选择此项，Vigor 路由器会捕捉 DTMF 信号并转换成 SIP 的格式。然后使用 SIP 信息发往远端。

DTMF模式

InBand
InBand
OutBand ( RFC2833)
SIP INFO (cisco格式)
SIP INFO (nortel格式)

## 载荷类型 (rfc2833)

从 96 到 127 进行选择，默认值为 101。此设定只对 OutBand (RFC2833) 模式有效。

## ISDN 的详细设定 (只适用于 VGi 型号)

点击索引栏中的数字 **3**，您可以访问如下页面来配置电话设定。



ISDN

呼叫功能

☐ 热线

☐ 会话计时器

呼叫转移

SIP URL

超时

☐ DND(免打扰)模式

索引(1-15) **计划任务** 设定:

注: 计划任务中的动作和超时设定将被忽略。

Index(1-60) in **Phone Book** as Exception List:

☐ CLIR (隐藏呼叫者 ID)

编码

优先编码

数据包包大小

声音状态检测(VAD)

默认SIP帐户

☐ 当帐户注册成功时有拨号音

FXO功能

☐ 启用ISDN到VoIP (在网) 呼叫

☐ 启用VoIP到ISDN (离网) 呼叫

确定

取消

高级

热线

选中此选项启用。输入 SIP URL，此 URL 会在您拿起听筒时自动拨出。

会话计时器

选中此选项启用。在此项设定了有限的时间后，如果无响应，则通话会被自动挂断。

呼叫转移

此处有四个选项。**禁用**关闭呼叫转移功能。**一直**意味着所有来电将会被无条件转移到 SIP URL。**遇忙**意味着来电只有在本地系统忙时才会被转移到 SIP URL。**无应答**意味着来电在没有相应时才会被转移到 SIP URL。

呼叫转移

禁用

禁用

一直

遇忙

无应答

**SIP URL** –输入 SIP URL（例如 aaa@draytel.org 或者 abc@iptel.org）作为呼叫转移目的。

**超时** –设置呼叫转移超时时间。默认设定为 30 秒。

DND（免打扰）模式

设置一段时间不被 VoIP 电话打扰。在这段时间内，呼叫您的朋友将听到忙音，而本地用户将不会听到任何振铃声。

**索引(1-15) 计划任务** -输入计划任务的索引号来控制DND模式。详细设定请参考 **3.5.2 计划任务**。

**索引 (1-60) 电话簿** –输入电话簿的索引号。详细设定请参考 **3.10.1 电话簿**。

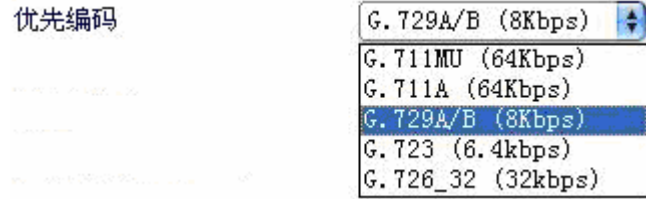
CLIR (隐藏呼叫者 ID)

选中启用此功能。在电话机屏幕上将不会显现隐藏呼叫者 ID。

优先编码

从五个编码中选择 VoIP 通话的默认编码。由于每次通话之前会协商双方使用的编码，很有可能不使用您的默认值。默认编码为 G.729A/B，它在提供不错的通话质量外占用很

小的带宽。如果您的上行带宽只有 64Kbps, 不要使用 G.711 编码。使用 G.711 时, 您的上行带宽至少在 256Kbps 以上。

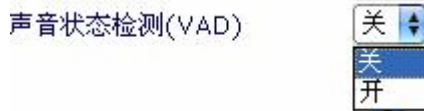


**单一编码**-如果选中, 则只有选择的编码会被应用。

**数据包大小**-单一数据包包含的数据容量, 默认值为 20ms, 则单一数据包包含 20ms 的语音信息。



**声音状态检测**-此项功能可以侦测双方的语音是否活动。如果不活动, 路由器会保留带宽给其他应用。



#### 默认 SIP 帐户

有六组 SIP 帐号可供选择。使用下拉式菜单来选择默认帐户。

#### 当帐户注册成功时有拨号音

选中启用此功能。

#### FXO 功能

**启用 ISDN 到 VoIP (在网) 呼叫** - 选中此项使得所有从 ISDN 线路呼入的电话被转移到因特网上的接受者。

**启用 VoIP 到 ISDN (离网) 呼叫** - 选中此项使得所有从 VoIP 线路呼入的电话被转移到 ISDN 的接受者。

另外, 您可以使用**高级**选项来进行声音设定, 声音增益, MISC 和 DTMF 模式。**高级**设定用来使路由器和本地通讯系统协同工作。错误的声音设定可能导致用户的不便。简单地选择合适的区域 (已预先设定好声音设定和来电显示类型), 就能改变电话的声音模式。或者您可以手动来调整声音设定, 选择用户自定义模式。TOn1, TOff1, TOn2 和 TOff2 表示声音的音调 TOn1 和 TOn2 代表有声音的时段; TOff1 和 TOff2 无声音的时段。

## 高级设定 &gt;&gt; ISDN

**声音设定**

区域 用户自定义

	低频(Hz)	高频(Hz)	T on 1 (毫秒)	T off 1 (毫秒)	T on 2 (毫秒)	T off 2 (毫秒)
拨号音	350	440	0	0	0	0
振铃音	400	450	400	200	400	2000
忙音	400	0	375	375	0	0
拥塞音	0	0	0	0	0	0

**声音增益**

麦克风增益(1-10) 5

话筒增益(1-10) 5

**DTMF**

DTMF模式 InBand

载荷类型(rfc2833) 101

**MISC**

拨号音功率 27

**认证PIN码**

☐ 选中可使用ISDN到VoIP呼叫 0000

☐ 选中可使用VoIP到ISDN呼叫 0000

**有下列前缀时禁止VoIP到ISDN呼叫**

☐  ☐

☐  ☐

确定 取消

## 区域

选择您所在的区域。来电显示 ID 类型，拨号音，振铃音，忙音和拥塞音会被自动设定。如果您不能找到合适的，请选择用户自定义，来手动设定拨号音，振铃音，忙音和拥塞音的值。

区域 UK

- 用户自定义
- UK
- US
- 丹麦
- 意大利
- 德国
- 荷兰
- 葡萄牙
- 瑞典
- 澳大利亚
- Slovenia
- Czech
- Slovakia

当然，您可以手动设置每个值。推荐使用 VoIP 通讯中的默认设定。

## 声音增益

**麦克风增益(1-10)/听筒增益 (1-10)** – 输入数字 0-10 来调整麦克风和听筒的音量。数字越大，声音越响。

## MISC

**拨号音功率** – 用来调整拨号音的响度。数值越小，声音越大。推荐使用默认设定。

## 认证 PIN 码

**选中可使用 ISDN 到 VoIP 呼叫**—设定路由器使用的 PIN 码来认证谁被允许拨打 ISDN 到 VoIP 呼叫。您可以输入 3 至 8 位的“0-9”数字。

**选中可使用 VoIP 到 ISDN 呼叫**—设定路由器使用的 PIN 码来认证谁被允许拨打 Voip 到 ISDN 呼叫。您可以输入 3 至 8 位的“0-9”数字。

## DTMP

**InBand** – 选择此项，当您按动电话的号码盘时，Vigor 路由器会直接像发送声音信号发送 DTMF 信息。

**OutBand** – 选择此项，Vigor 路由器会先在号码盘上捕捉按键号码，然后转换成数字进行发送。接受方会依据接受到的数字信号产生一个 DTMF 信号。此功能在网络拥塞时能保证准确地 DTMF 传输。

**SIP INFO**— 选择此项，Vigor 路由器会捕捉 DTMF 信号并转换成 SIP 的格式。然后使用 SIP 信息发往远端。

DTMF模式



InBand
InBand
OutBand (RFC2833)
SIP INFO (cisco格式)
SIP INFO (nortel格式)

**载荷类型 (rfc2833)**— 从 96 到 127 进行选择，默认值为 101。此设定只对 OutBand (RFC2833) 模式有效。

## 有下列前缀时禁止 VoIP 到 ISDN 呼叫

设置前缀号码用来禁止用户从 VoIP 电话拨出到 PSTN 线路。具有这些前缀号码的电话将不能被接通。如果用户强行拨打，路由器将自动切断。您只能在此项输入最多 11 位的 0-9 的数字。

3.10.4 状态

在 VoIP 通话状态页中，您可以找到 VoIP1 和 VoIP2 接口的编码，连接和其他重要通话状态。

VoIP >> 状态

状态

刷新秒数: 10 刷新

端口	状态	编码	对端 ID	持续时间 (hh:mm:ss)	Tx 包	Rx 包	Rx 丢 失	Rx 抖动(毫 秒)	呼入电 话	呼出电 话	话筒增 益
FXS 1	空闲			00:00:00	0	0	0	0	0	0	5
FXS 2	空闲			00:00:00	0	0	0	0	0	0	5
ISDN1	空闲			00:00:00	0	0	0	0	0	0	5
ISDN2	空闲			00:00:00	0	0	0	0	0	0	5

记录

Date (mm-dd-yyyy)	Time (hh:mm:ss)	Duration (hh:mm:ss)	In/Out	Peer ID
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	
00-00- 0	00:00:00	00:00:00	-	

**刷新秒数** 指定获得最新 VoIP 通话信息的刷新秒数。一旦点击刷新键，通话信息会被立即刷新。



**端口** 显示 VoIP1 和 VoIP2 端口的当前连接状态。只有当路由器装备了 ISDN 接口时，ISDN1/2 才会被显示。ISDN1 代表物理 ISDN 端口的 B1 信道，ISDN2 代表物理 ISDN 端口的 B2 信道。注，ISDN1/2 端口只对欧洲使用的 Vigor 2910VGi 型号有效。对于 V 型号的路由器，此页只显示 VoIP1 和 VoIP2。

**状态** 显示 VoIP 连接状态。  
**空闲**- VoIP 功能空闲。  
**连接尚未建立**-连接尚未建立（忙音）。  
**连接** -用户正在拨出，正在发起 VoIP 连接。  
**等待回应** -连接已建立等待远端用户回应。  
**振铃** -有拨入电话。  
**通话**-正在通话中。

**编码** 当前信道使用的编码。

**对端 ID** 拨入或拨出的对端 ID（IP 或者域名格式）。

**持续时间** 以秒为单位。

**Tx 包** 当前连接发送的语音包总量。

<b>Rx 包</b>	当前连接接收的语音包总量。
<b>Tx 丢失</b>	当前连接丢失的语音包总量。
<b>Rx 抖动</b>	接收到语音包的抖动。
<b>呼入电话</b>	总计呼入电话时间。
<b>呼出电话</b>	总计呼出电话时间。
<b>话筒增益</b>	当前通话音量。
<b>记录</b>	显示 VoIP 通话记录。

## 3.11 ISDN

只有 Vigor 2910i 和 2910VGi 路由器有 ISDN 功能，对于其它类型的用户可以忽略此章节。

下面显示的是 ISDN 的主菜单。



### 3.11.1 基本设定

此页面提供一些 ISDN 的基本设定，比如是否启用 ISDN 通讯端口，MSN 号码和禁止 MSN 号码等设置。

ISDN >> 基本设定

#### ISDN 设定

<b>ISDN通讯埠</b> <input checked="" type="radio"/> 启用 <input type="radio"/> 停用		<b>路由器封锁的MSN号码</b>	
<b>国码</b> <input type="text" value="国际的"/>	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> 5. <input type="text"/>		
<b>自己的号码</b> <input type="text"/>			
<small>"自己的号码"代表路由器正在准备拨出通话时，会将ISDN号码告知远端。</small>			
<b>给路由器的MSN号码</b>			
1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>			
<small>"MSN号码"代表路由器可接受号码符合的来电。另外，MSN服务应该为本机ISDN网络提供商所支持。</small>			

确定

清除

**ISDN 通讯埠**

选择**启用**以启用 ISDN 通讯端口。

**国码**

请在此处选择正确的国码。

**自己的号码**

请在此处输入您的 ISDN 号码。

**给路由器的 MSN 号码**

**MSN 号码**是指路由器只能接收到和此处号码相匹配的打来的电话，而您当地的 ISDN 服务器只有支持

MSN 服务您才能使用此功能。Vigor2910 为您提供三组 MSN 号码。注：前提是您所在地的电信局必须是支持 MSN 功能。默认情况下，MSN 功能是处于关闭状态的。如果您在这里没有填写任何号码，所有的来电都会被接收。

路由器封锁的 MSN 号码      请在此填写您不希望路由器拨打的 MSN 号码。

3.11.2 拨到单一 ISP

如果您只是使用一个 ISP 访问 Internet，请选择此项。

ISDN >> 拨到单一ISP

单ISP

ISP接入设定

ISP名称tt

拨接号码123

用户名123

密码123456

☐ 要求ISP回拨 (CBCP)

索引(1-15) 计划任务 设定:

=>  ,  ,  ,

PPP/MP设定

连接类型拨接BOD

PPP验证PAP或CHAP

闲置超时180 秒

IP地址分配方法 (IPCP)

固定IP ☐ 是 ☒ 否 (动态IP)

固定IP地址

确定

- ISP 名称

请在此填写您的 ISP 名称。
- 拨接号码

请在此填写由您的 ISP 提供的 ISDN 访问号码。
- 用户名

请在此填写由您的 ISP 提供的用户名。
- 密码

请在此填写由您的 ISP 提供的密码。
- 要求 ISP 回拨(CBCP)

如果您的 ISP 支持回拨功能，请点此项以便在 PPP 验证过程中启用回拨控制协议。
- 计划任务(1-15)

您可以在这里填写您预先设置好的计划任务以便控制上网时间。
- 连接类型

这里提供了四种连接类型，分别是连接停用、拨接 64 Kbps 、拨接 128 Kbps 和拨接 BOD。

连接停用 – 是指禁用 ISDN 的拨出功能。

拨接 64 Kbps – 使用一个 ISDN B 通道访问 Internet。

拨接 128Kbps -使用两个 ISDN B 通道访问 Internet。

拨接 BOD – BOD 是指按需分配带宽。路由器在低流量的情况下只启用一个 B 通道，当一个 B 通道的带宽被占满的情况下，其它 B 通道将会被自动启用。关于 BOD 的详细说明，请参阅高级设置下的呼叫控制和 PPP/MP 设定。
- PPP 验证

仅 PAP – 仅使用 PAP 协议和 ISP 验证 PPP 连接的用户名和密码。

PAP 或 CHAP -使用 PAP 协议或 CHAP 来和 ISP 验证 PPP 连接的用户名和密码。



### 闲置超时

闲置超时是指路由器在闲置超过规定时间之后会自动断开连接。默认的闲置时间为 180 秒。如果您将其设置为 0 秒，那么 ISDN 连接将一直在线。

### 固定 IP

如果您的 ISP 为您提供的是动态 IP 地址，您就不需要在这里做任何设置了。而如果您的 ISP 为您提供的是固定的 IP 地址，您就需要这里选择是启用此功能，并且在**固定 IP 地址**栏里填入由您的 ISP 分配给您的固定 IP 地址。

### 固定 IP 地址

请在此处填写 ISP 分配给您的固定 IP 地址。

## 3.11.3 拨到双 ISP

如果您拥有超过一个 ISP 请在此页面下配置相关参数，这样您就可以同时拨到两个 ISP，而这关键取决于这些 ISP 是否支持多连接的 PPP (ML-PPP) 功能。一般情况下，拨到两个 ISP 会将 ISDN 通道的带宽增加到 128 kbps。

### ISDN >> 拨到双ISP

#### 双 ISP

<b>一般设定</b> 1. <input type="checkbox"/> 启用双ISP功能 2. <input type="checkbox"/> 要求ISP回拨 (CBCP)	<b>PPP/MP设定</b> 连接类型: 拨接BOD PPP验证: PAP或CHAP 闲置超时: 180 秒
<b>主ISP设定</b> ISP名称: tt 拨接号码: 123 用户名: 123 密码: 123456 <b>IP地址分配方法 (IPCP)</b> 固定IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (动态IP) 固定IP地址: <input type="text"/>	<b>第二ISP设定</b> ISP名称: <input type="text"/> 拨接号码: <input type="text"/> 用户名: <input type="text"/> 密码: <input type="text"/> <b>IP地址分配方法 (IPCP)</b> 固定IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (动态IP) 固定IP地址: <input type="text"/>

确定

这里的大部分的设置参数和前一部分是差不多的，在这里只是多了一个第二 ISP 设定，您可以在这里参照之前的设置在这里填写相关的设定。

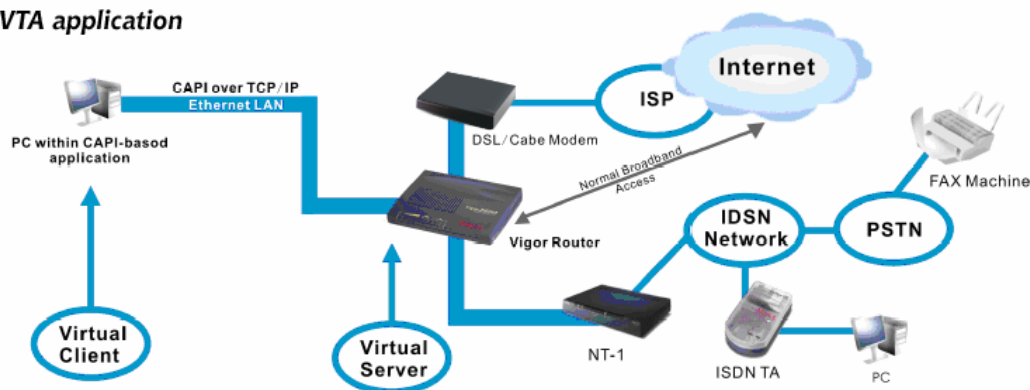
## 3.11.4 虚拟 TA

**虚拟 TA** 是指本地主机或 PC 使用基于 CAPI 的软件比如 RVS-COM 或 BVRP 等软件访问路由器作为本地的 ISDN 的 TA 来通过 ISDN 线路来发送或接收传真信息。基本上这是一个基于客户端/服务器的网络模型。内置的虚拟 TA 服务器可处理连接的确立和释放。虚拟 TA 的客户端安装在本地主机或 PC 上，建立了一个基于 CAPI 驱动器来在应用程序和路由器 CAPI 之间转发所有的 CAPI 消息。在描述 Vigor2910 路由器的**虚拟 TA** 之前请注意以下的限制。

- 虚拟 TA 客户端只支持微软的 Windows 95 OSR2.1/98/98SE/Me/2000 平台。
- 虚拟 TA 客户端只支持 CAPI2.0 协议，并且它没有内置的传真驱动。
- 一个 ISDN BRI 接口吸两个 B 通道，客户端最多也只有两个。
- 在配置虚拟 TA 之前，您必须设置好正确的国码。



## VTA application



正如图所描述的应用，虚拟 TA 客户端可以实现从传真机或 ISDN TA 上打电话或是接电话等功能。

在您配置虚拟 TA（远端的 CAPI）设定之前，请先安装虚拟 TA 客户端。您可以从路由器附带的 CD 中找到相关的安装文件。其中 **Vsetup95.exe** 是用于 Windows 98, 98SE 和 windowsMe 的，**Vsetup2k.exe** 是用于 Windows 2000 的，请参照下面的截图来安装虚拟 TA 客户端。在最后一步时系统会提示您重启计算机，请点击 **OK** 重启。

在重启计算机之后，您将会在 PC 的任务栏中看到 VT 的图标（通常它会出现在任务栏的右侧靠近时间的地方）如下所示：



当字是绿色时，是指虚拟 TA 客户端是连接在服务器上的，这时您可以运行您的基于 CAPI 的软件使用客户端访问路由器，关于软件的详细设置，请参阅相关的手册。如果字是红色的则意味着客户端断开了和服务器的连接，这时请检查物理连接。



接下来，请点击**快速设定**下的**虚拟 TA (远端的 CAPI) 设定**来配置虚拟 TA。

因为虚拟 TA 程序是基于客户端/服务器的，所以您必须要在两端都做配置以运行虚拟 TA 程序。

默认情况下，虚拟 TA 服务器是启用的，并且用户名和密码都是空。任何虚拟 TA 客户端都可以登录服务器。而当您填写了用户名和密码时，则只有符合用户名和密码才能登录。虚拟 TA 的配置页面如下所示：

## ISDN >> 虚拟TA

### 虚拟TA设定

虚拟TA服务器 : ☒ 启用 ☐ 禁用

虚拟TA用户设定档		MSN1	MSN2	MSN3	启用
序号	用户名	密码			
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

确定

虚拟 TA 服务器	<p><b>启用：</b> 点选此项以启用虚拟 TA 服务器。</p> <p><b>禁用：</b> 点选此项以禁用虚拟 TA 服务器，所有的虚拟 TA 服务程序都会被中止。</p>
用户名	在此输入指定客户端的用户名。
密码	在此输入指定客户端的密码。
MSN1/ MSN2/MSN3	MSN 是指 <b>多用户号</b> ，它是指您可以在一条线上运用多个 ISDN 线路号。注：您所在的当地电信局必须支持此服务，这样您才能为特定的客户端指定特定的 MSN 号。如果您没有 MSN 服务，就不需在这里填写任何信息。
启用	点选此项以使客户端可以访问服务器。

## 用户设置

注意这里只是建立一个单用户访问账号来限制只有指定的账号才能访问虚拟 TA 服务器。

假设您的 ISDN 提供商不支持 MSN 服务。

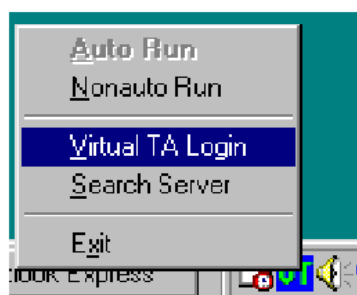
在服务器端 – 点击**虚拟 TA（远端 CAPI）设定**来填写用户名和密码。选择**启用**以启用此账号。

**虚拟TA设定**

虚拟TA服务器 : ☒ 启用 ☐ 禁用

虚拟TA用户设定档						
	用户名	密码	MSN1	MSN2	MSN3	启用
1.	alan	123456	123			<input checked="" type="checkbox"/>
2.						<input type="checkbox"/>

在客户端 – 在 VT 标图上右击鼠标将会弹出一个菜单，如下所示：



点击**虚拟 TA 登录**。

**Virtual TA Login**

User Name :

Password :

输入用户名和密码并点击 **OK**，之后 VT 图标会变成绿色。

## MSN 配置

如果您运行 MSN 服务，虚拟 TA 服务器会分配给客户端一个指定的 MSN 号。当有来电时，服务器会告诉相关的客户端。现在我们来举例说明 MSN 号的设置。

假设您分配一个 MSN 号 **123** 给客户“alan”。

**虚拟TA设定**

虚拟TA服务器 : ☒ 启用 ☐ 禁用

---

**虚拟TA用户设定档**

	用户名	密码	MSN1	MSN2	MSN3	启用
1.	alan	skkksk	123			<input checked="" type="checkbox"/>
2.						<input type="checkbox"/>

在基于 CAPI 的软件上输入指定的 MSN 号，当虚拟 TA 服务发送警告信号给指定的虚拟 TA 客户端时，基于 CAPI 的软件也会接收到这个信号，而软件却不会接收到打来的电话。

3.11.5 拨号控制

一些应用程序要求路由器（只针对 i 型路由器而言）可以远程启用或者能够通过 ISDN 接口拨到 ISP。Vigor2910 路由器提供了这一特性，即允许用户打电话给路由器让它拨到 ISP。

**注释：**拨号控制只适用于 i 型有 ISDN 接口的 Vigor 路由器。

请在配置以下页面之前设置好**拨到单一 ISP** 页面下的相关选项。

ISDN >> 拨号控制

拨号控制设定

重拨	0 次	远端启动	
拨号延迟间隔	0 秒		

PPP/MP拨出设定

<div>基本设定</div> <div>连接类型 PAP或CHAP TCP标头压缩 闲置超时</div>	<div>随选频宽 (BOD) 设定</div> <div>高水线 高水时间 低水线 低水时间</div>
<div>拨接BOD PAP或CHAP 无 180 秒</div>	<div>7000 cps 30 秒 6000 cps 30 秒</div>

确定

**重拨** 这里指定了每个触发包的重拨次数。触发包是指发向外部网络的数据包。默认的设置不为重拨。如果设为 5，则对于每个触发包来说，路由器都会拨 5 次号直到拨到 ISP 或远端路由器为止。

**拨号延迟间隔** 这里指定了两次重拨的时间间隔。默认的时间是 0 秒。

**远端启动** 这里指定了远端启动的电话号码，它用于启用远端激活功能。如果路由器接到号码为 12345678 的电话，它会中断此电话并立刻拨到 ISP。

**连接类型** 因为 ISDN 有两个 B 信道(64Kbps/per)，您可以指定您是否使用一个 B 信道、两个 B 信道或是 BOD(按需分配带宽)。您有四个选项可以选择：连接停用、拨接 64Kbps、拨接 128Kbps 和拨接 BOD。

连接类型

拨接BOD  
连接停用  
拨接64Kbps  
拨接128Kbps  
拨接BOD

**PPP 验证** 在这里为 PPP/MP 连接指定 PPP 验证的方法，通常您最好设置为 **PAP 或 CHAP** 。

**TCP 标头压缩** **VJ 压缩** – 它是用于 TCP/IP 协议头压缩。通常此项被设置为无以改善带宽利用率。

TCP标头压缩

无  
无  
VJ 压缩

#### 闲置超时

因为我们的 ISDN 连接类型是按需拨接，连接只有当需要时才被发起。

#### 高水线和高水时间

BOD 是指对于多连接的 PPP 来说是按需分配带宽的。**高水线和高水时间**，**低水线**和**低水时间**参数只有当您将**连接类型**设置为**拨接 BOD**时才可用。ISDN 通常会在您选用拨接 BOD 后使用一条 B 信道来访问 Internet 或远端网络。路由器根据参数来决定用户什么时候来启用或断开另一条 B 信道。注：**cps** (characters-per-second) 测的是总的连接利用。

这此参数指的是第二条通道启用的情况。对于第一条连接信道，如果它的利用超过了高水线，并且这条信道的使用超过了高水时间，另一条信道就会被启用。因此总连接速度会是 128kbps (两条 B 信道)。

#### 低水线和低水时间

这些参数指出第二条信道会在何种情况下会断开。如果使用两条 B 信道，如果他们的利用率低于低水线，并且两条信道的使用超过了高水时间，另一条信道会被断开。这时，总连接速度会是 64kbps (一个 B 信道)。

**注释：**如果您不能确定您的ISP是否支持BOD或ML-PPP，请向您的ISP、当地代理商或我们的技术支持[support@draytek.com](mailto:support@draytek.com)咨询相关问题。

## 3.12 无线局域网

此功能只用于 G 模式。

### 3.12.1 基本概念

近年来，无线通讯市场正以难以想象的速度增长。现在无线技术可以触及甚至完全有能力触及到地球上的各个角落。数以百万的人们每天通过无线产品彼此交换信息。Vigor G系列路由器，又称为Vigor无线路由器。它被设计成专门为中小SOHO企业和家庭提供更高速度，更灵活的无线传输。任何授权无线用户都不必通过复杂的传统网络布线就可以便捷地携带无线手掌电脑或笔记本进入会议室参加会议。无线局域网具有高度的灵活机动性，使无线用户同时能象有线局域网那样自由的享用网络资源甚至可以畅游因特网。

Vigor无线路由器配有一个符合IEEE 802.11g标准的无线接口，为了进一步提高性能，Vigor无线路由器同时装配了高级无线技术Super G™，数据传输高达 108Mbps。因此，用户可以顺畅地享受的音频或视频。

**注释：**\*实际的数据流量会根据不同的网络环境而改变，包括无线信号强度，网络覆盖率和建筑材料等。

在无线网络的基础模式中，Vigor 无线路由器作为接入点（AP）和许多无线客户端相连。所有无线客户端通过 Vigor 无线路由器共享同一网络资源。在**基本设定**中包括些无线网络信息，如 SSID，频道等。



### 安全机制

**实时硬件加密：**Vigor 路由器装有 AES 加密硬件，方便用户更好的保护数据信息。

**完善的安全标准选择：**为了确保用户无线通信的安全性和私密性，我们提供了常用的安全标准。

WEP (有线等价机密) 采用 64 位或 128 位密钥加密无线传输数据的安全机制。一般接入点预设了四组密钥，每个无线客户端使用其中的一组密钥与接入点通信。

WPA(Wi-Fi 保护接入), 是工业应用中最安全的机制, 主要分为两类: WPA-personal 或称为 WPA Pre-Share Key (WPA/PSK), 和 WPA-Enterprise 或称为 WPA/802.1x.

对于 WPA-Personal, 在数据传输过程中采用预定义密钥加密。WPA 采用动态密钥完整性协议 (TKIP) 进行加密, 而 WPA2 采用 AES 加密。WPA-Enterprise 不仅使用加密机制还运用了认证机制。

由于 WEP 已证明是易受攻击的, 所以为了安全的通信, 请使用 WPA 加密。您可以根据您的需要选择合适的安全机制。不管您选择那种安全手段, 他们都可以提高无线网络传输数据的安全性和私密性。Vigor 无线路由器可以非常灵活的在同一时间用 WEP 和 WPA 提供多种安全连接。

### 例 1



### 例 2



### 例 3



**无线局域网和有线局域网分离机制** 为了安全或限制接入，可以使用分离有线和无线局域网机制。这表示双方将不能彼此通信。例如，您可以构建允许客户上网，但不可访问有线局域网络的无线局域网以确保公司的内部机密。您还可以使用 MAC 地址过滤来隔离有线局域网客户的接入。

**管理无线接入者 – 接入者列表** 显示了无线网络中所有的接入者以及连接状态。

以下是无线局域网菜单条目。





3.12.2 基本设定

点击**基本设置**，将可以设置 SSID 和无线频道等，请参考下图。

无线局域网 >> 基本设定

基本设定 (IEEE 802.11)

☒ 启用无线局域网

模式：

混合模式 (11b+11g)

索引 (1-15) **计划任务** 设置：

SSID：

default

频道：

频道6, 2437MHz

**注意：**如果启用了SuperG模式，频道固定到6。

☐ 隐藏SSID

☐ 长封包头处理 (Long Preamble)

**隐藏SSID：**方式SSID被扫描到。

**长封包头处理 (Long Preamble)：**一些比较老的802.11b设备需要此选项 (会降低性能)。

确定

取消

启用无线局域网

点选此项开启无线局域网。

模式

选择合适的无线模式。

**混合 (11b+11g+SuperG)** – 同时支持 IEEE802.11b, IEEE802.11g 和 SuperG 协议。

**混合 (11b+11g)** – 同时支持 IEEE802.11b 和 IEEE802.11g 协议。

**SuperG** – 支持 SuperG.

仅 **11g** – 只支持 IEEE802.11g.

仅 **11b** – 只支持 IEEE802.11b.

模式：

混合模式 (11b+11g)

混合 (11b+11g+SuperG)

混合模式 (11b+11g)

仅SuperG

仅 11g

仅 11b

索引(1-15)

您可以配置路由器的无线功能仅在某些特定时段工作，总共可以设置四个时段。默认情况下，路由器的无线功能没有时限。您可以到> **应用程序 >计划任务设定**配置相关计划任务。

SSID

SSID 默认值是 "default"。我们建议您更换到其他名字。它是您无线网络的标识。SSID 可以由任何字符或特殊字符组成。

## 频道

无线局域网的信道频率。默认频道是 6。如果您所选择的频道有干扰，可以更改到其他频道。

频道：



频道6, 2437MHz
频道1, 2412MHz
频道2, 2417MHz
频道3, 2422MHz
频道4, 2427MHz
频道5, 2432MHz
频道6, 2437MHz
频道7, 2442MHz
频道 8, 2447MHz
频道9, 2452MHz
频道10, 2457MHz
频道11, 2462MHz

## 隐藏 SSID

启用此功能可以阻止无线探测，防止未经认证的客户端加入到您的无线网络。而用户可以看到除了 SSID 的任何信息。当站点扫描时，不能探测到无线路由器的任何信息。

## 长封包标头处理

此选项定义了 802.11 信息包同步域的长度。现在许多的无线路由器使用 56 位同步域的短封包代替 128 位的长封包。但是，一些原来的 11b 无线网络设备只支持长封包，如果需要和这样的设备通信，请选择此选项。

3.12.3 安全性

点击安全性设置，将出现 WEP 和 WPA 等安全设置的配置页面。

无线局域网 >> 安全性设定

安全性设定

模式：

停用

设定 **RADIUS 服务器** 若启用了 802.1x。

WPA:

类型：

☒ 混合 (WPA+WPA2)

☐ 仅 WPA2

预共享密钥 (PSK)

\*\*\*\*\*

键入8~63个ASCII字符或以"0x"为首后接64个十六进制字符，例如"cfgs01a2..."或"0x655abcd..."。

WEP:

加密模式：

64 位

使用

☒ 密钥 1:

\*\*\*\*\*

☐ 密钥 2:

\*\*\*\*\*

☐ 密钥 3:

\*\*\*\*\*

☐ 密钥 4:

\*\*\*\*\*

关于 64 位 WEP密钥

键入5个ASCII字符或开头为"0x"的10个十六进制数字，如"AB312"或"0x4142333132"。

关于 128 位 WEP密钥

键入13个ASCII字符或开头为"0x"的26个十六进制数字，如"AB312"或"01234567890x4142333132"。

确定

取消

模式

有多种安全模式可供选择。

模式：

停用

仅 WEP

仅 WEP/802.1x

WEP 或 WPA/PSK

WEP/802.1x 或 WPA/802.1x

仅 WPA/PSK

仅 WEP/802.1x

- 停用 – 停用加密机制。
- 仅 WEP – 要求客户端只能使用 WEP 密钥加密，加密密钥在 WEP 密钥中输入。
- 仅 WEP/802.1x – 要求客户端只能使用通过 802.1x 的机制认证。由于密钥是在认证过程中自动协商，所以密码不可手动设置。
- WEP 或 WPA/PSK – 客户端可以使用 WEP 和 WPA 加密。如果选择 WPA/PSK,只可采用混合模式 (WPA+WPA2)加密。
- WEP/802.1x 或 WPA/802.1x – 客户端可以使用 802.1 机制生成的 WEP 和 WPA 加密。如果选择 WPA/PSK,只可采用混合模式 (WPA+WPA2)加密。由于密钥是在认证过程中自动协商，所以密码不可手动设置。
- 仅 WPA/PSK – 客户端采用 WPA 加密，在 PSK 中输入加密密钥。请记住在选择 WPA 加密时，需在下面的类型中定义混合或仅 WPA2 类型。
- 仅 WPA/802.1x – 客户端采用 802.1 机制的 WPA 加密

协议。请记住在选择 WPA 加密时，需在下面的**类型**中定义混合或仅 WPA2 类型。

## WPA

WPA 采用密钥加密每个无线传输的数据包，可以手动输入 PSK,或者有 802.1 机制自动协商。

**类型** – 选择混合(WPA+WPA2)或仅 WPA2。

**预共享密钥**- 输入 **8~63** 个 ASCII 字符，例如 012345678..(或者以 0x 开头的 64 位十六进制数，例如 "0x321253abcde...")。

## WEP

**64 位** – 64 位 WEP 密钥，输入 **5** 个 ASCII 字符，例，12345 (或者以 0x 开头的 10 位十六进制数，例如 0x4142434445.)

**128 位** – 128 位 WEP 密钥，输入 **13** 个 ASCII 字符，例，ABCDEFGHJKLM (或者以 0x 开头的 26 位十六进制数，例如 0x4142434445464748494A4B4C4D).

**加密模式：**



所有的无线设备必须使用相同的密钥位数和相同的密钥。此处可以输入 4 组密钥，但是每次只可以使用一组。密钥可采用 ASCII 码或十六进制数。

3.12.4 接入控制设定

为了进一步加强无线安全，接入控制功能可以通过无线客户端的 MAC 地址来控制网络接入。只有已经配置的 MAC 地址才能接入无限局域网。点击接入控制进入如下页面。

无线局域网 >> 接入控制

接入控制

恢复出厂设置

☐ 启用接入控制

策略：

启用MAC地址过滤

MAC地址过滤

索引

属性

MAC地址

客户机 MAC 地址：:::::

属性：

☐ s: 将无线接入用户和局域网分开

添加

移除

编辑

取消

确定

全部清除

启用接入控制

策略

MAC 地址过滤

属性

添加

移除

编辑

取消

确定

全部清除

點選启用接入控制启用此功能。

选择启用 MAC 地址过滤 可以手动输入允许接入无线局域网客户的 MAC 地址。选择将无线接入用户和局域网分开，则 MAC 地址列表中的所有无线接入者将和局域网分离。

策略：

启用MAC地址过滤

启用MAC地址过滤

将无线接入用户和局域网分开

显示之前编辑过的所有 MAC 地址。（增加,移除客户机 MAC 地址 - 手动输入无线客户端的 MAC 地址。

s - 选择该 MAC 地址将无线接入用户和局域网分开。

添加新的 MAC 地址到列表中。

从列表中删除一个 MAC 地址。

编辑存在于列表中的某个 MAC 地址。

放弃本次设置。

保存接入控制列表。

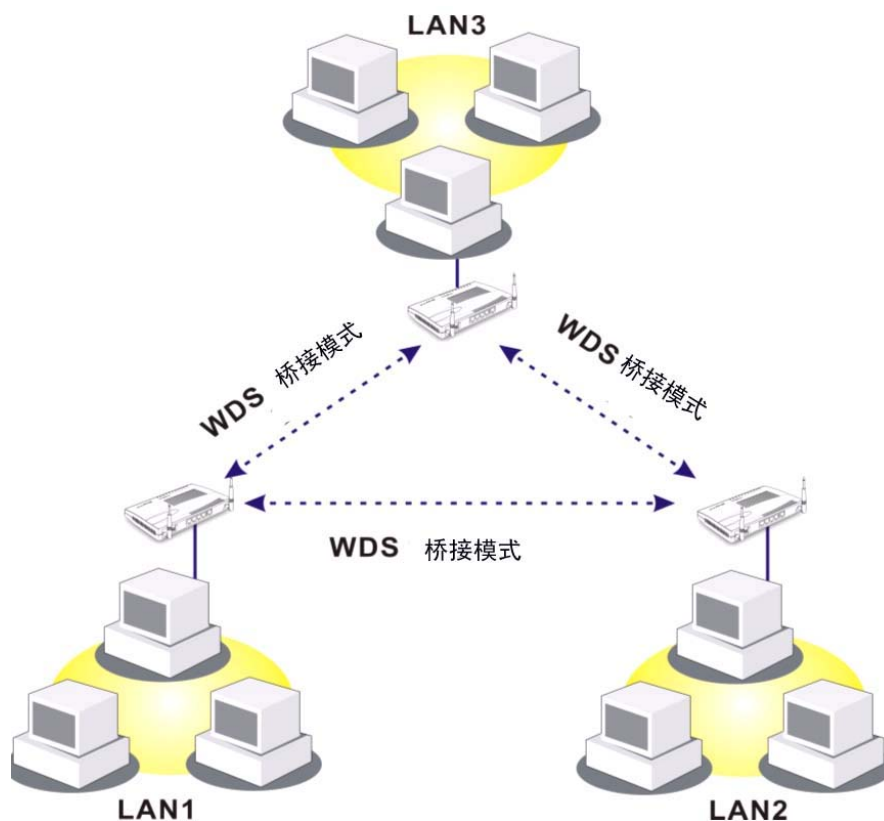
清除 MAC 地址列表中的所有条目。

3.12.5 WDS

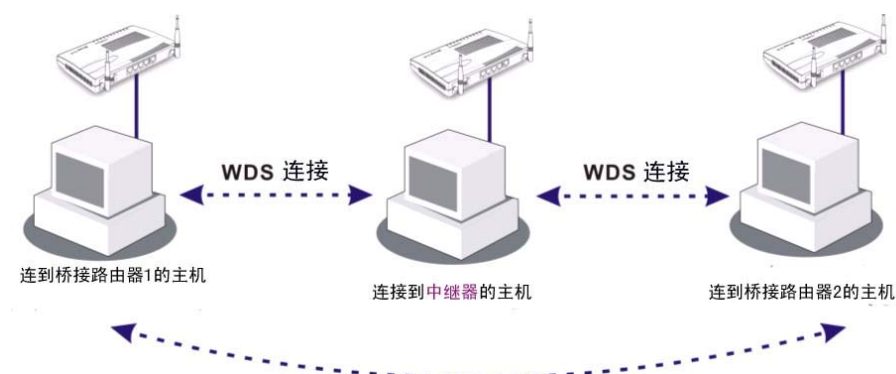
WDS 是指无线分布系统，是无线连接两个接入点（AP）的协议。通常有以下应用：

- 以桥接方式无线连接两个局域网
- 扩展无线局域网的覆盖范围。

Vigor 路由器可以实现以上两种模式，一种是桥接，另一种是中继。下图显示了 WDS 桥接功能。



下图显示 WDS 中继功能:



两种模式的主要不同点在于：对于**中继**模式，从某一接入点接收的信息包可以通过 WDS 连接转发到另一个接入点。然而**桥接**模式，通过 WDS 连接接收的信息包只能被转发到有线网络或无线主机。换句话说，只有中继模式可以进行 WDS 到 WDS 信息包的转发。

如下例，连接到 Bridge 1 或 Bridge 3 的主机可以通过 WDS 链接和连接到桥 2 的主机通信。但是，连接到 Bridge1 的主机无法透过 Bridge2 与 Bridge3 主机相通。





<b>WEP</b>	选择此项将采用和之前 <b>安全性</b> 设置中相同的密钥。如果您在安全设置中没有设置任何密钥，此条目将显示为灰色。
<b>设置</b>	<p><b>加密模式</b> - 选择您想使用的加密模式。如果您点选<b>使用与安全性设定相同的 WEP 密钥</b>，就不必再选择 64 位或 128 位加密模式。如果您没有点选此功能，那么您可以再此页设置 WEP 密钥。</p> <p><b>密钥索引</b> - 在选择加密模式后选择您想使用的密钥索引。</p> <p><b>密钥</b> - 输入您想使用的密钥。</p>
<b>预共享密钥</b>	输入 8 ~ 63 位 ASCII 码字符或者 64 位十六进制数，以“0x”打头。
<b>桥接</b>	如果您选择桥接模式，请输入对端的 MAC 地址。可以同时输入 6 个对端的 MAC 地址。但为了保证更好的性能，请禁用无效的连接。如果您想启动该 MAC 地址，只需在输入的 MAC 地址前打点选启用即可。
<b>中继</b>	如果您选择中继模式，请输入对端的 MAC 地址。可以同时输入 2 个对端的 MAC 地址。同样，如果您想启动某个 MAC 地址，只需在输入的 MAC 地址前打点选启用即可。
<b>接入点功能</b>	点击 <b>启用</b> ，可将路由器作为接入点使用，点击 <b>禁用</b> 取消此功能。
<b>状态</b>	允许用户发送“hello”信息到对端。但此功能仅在对方也支持时才起效。

### 3.12.6 AP 扫描

Vigor 路由器可以扫描信道寻找可用的无线接入点。根据扫描结果，用户可以清楚地知道哪个信道可以使用，此功能也能应用于寻找 WDS 连接的接入点。注意，在扫描过程中（大约 5 秒），任何客户端都不允许接入路由器。

下图显示了在无线局域网中所扫描到的接入点。但是，只有在相同频道的路由器才能被扫描到。请点击**扫描**来寻找所有连接的接入点。

无线局域网 >> AP 扫描

**AP 列表**

BSSID	频道	SSID

**扫描**

参考 **统计**。

**注意：**在扫描过程中（5秒），不允许客户端连接到路由器。

---

**添加到 WDS 设定：**

AP 的 MAC 地址  :  :  :  :  :  **添加**

如果您想寻找应用 WDS 设置的接入点，请手动输入接入点的 MAC 地址，然后按**添加**，这样 AP 的 MAC 地址将被添加到 WDS 设置页面。



3.12.7 接入者列表

接入者列表显示了所有连接的无线客户端，以及他们的状态。 状态码在页面中有详细解释。为了方便接入控制的设置，您可以选择其中的一个无线接入者，然后按添加以添加到接入控制，如下图所示：

无线局域网 >> 接入者列表

接入者列表

状态	MAC地址
----	-------

更新

**状态码：**  
C: 已经连接，无加密。  
E: 已连接，WEP。  
P: 已连接，WPA。  
A: 已连接，WPA2。  
B: 受到接入控制功能的封锁。  
N: 正在连接。  
F: 无法通过802.1x 或 WPA/PSK认证。

**注意：** 当一个客户端连接到路由器之后，它可能会在不通知路由器的情况下断开连接。在这种情况下，它将仍旧显示在列表中，直到连接过期。

添加到 **接入控制**：

客户端的MAC地址     :  :  :  :  :

更新

按此按钮可以更新接入者列表。

添加

添加所选择的 MAC 地址到接入控制。

### 3.12.8 接入者速率控制

该页允许控制每个无线客户端的上传和下载速率。点击**启用**使用该功能。速率范围控制在 100 ~ 30,000 kbps 之间。

**无线局域网 >> 接入者速率控制**

**接入者速率控制**

☐ 启用

上传速率:

00 Kbps

下载速率:

00 Kbps

**注意:**  
1. 速率: 100~30,000 Kbps, 增量: 100 Kbps。  
2. 指定的速率将应用到每台无线客户端。

确定

取消

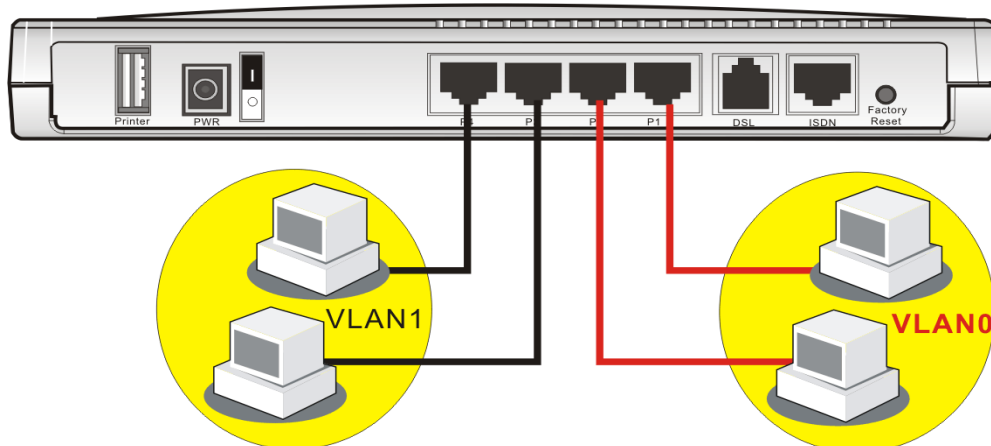
## 3.13 VLAN

虚拟局域网通过对物理端口分组，提供您一个非常方便的方法管理主机。



### 3.13.1 有线 VLAN

连接到路由器以太网接口的 PC 可以被分到不同的 VLAN 组。在相同组内的成员可以相互通讯，但是与其他组的成员就无法往来。



您可以通过设置 **VLAN >> 有线 VLAN** 以达到以上目的。简单地在 VLAN0 里点选 P1 和 P2；在 VLAN1 里点选 P3 和 P4。

## 有线 VLAN 设定

☒ 启用

	P1	P2	P3	P4
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 启用

点击以启用 VLAN 配置功能。

## P1 – P4

在指定 VLAN 中选中所连主机的端口，以划分到同一组 VLAN。每个端口可以同时分配给不同的 VLAN。例如，如果您选中 VLAN0-P1 和 VLAN1-P1，您可以同时把 P1 端口分配给 VLAN0 和 VLAN1。

## VLAN0-3

路由器可以设置 4 组 VLAN。

**注释：**如果 WAN2 口被启用，P1 口将作为 WAN 接口，在此处不能被选中，如下图所示。

## 有线 VLAN 设定

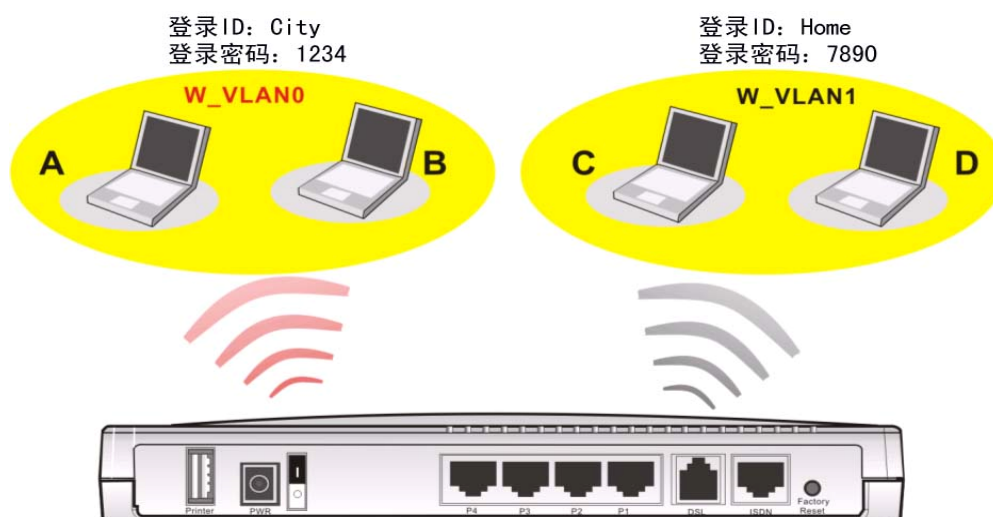
☒ 启用

	P1	P2	P3	P4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 3.13.2 无线 VLAN

通过无线接口连接到路由器的 PC（装配有无线网卡）同样可以分成不同组和形式的 W\_VLAN。同组下的无线 PC 可以相互通讯，但不同组的成员则不行。

在同组下的无线 PC 使用相同的登录 ID 和密码接入 Internet。例如下图的示例。A 和 B 都使用相同的登录 ID（City）和密码（1234）。这样他们就被分在了同一组 W\_VLAN 内。



您可以在 **VLAN >> 无线 VLAN**，通过无线连接配置无线 VLAN 的设置。只需简单地在 W\_VLAN0 一栏中输入登录 ID 以及密码 **City** 和 **1234**，而在 W\_VLAN1 一栏中输入 **Home** 和 **7890** 即可。用户总共可以配置 15 组不同的无线 VLAN。

#### VLAN >> 无线 VLAN 设置

##### 无线 VLAN 设置

☒ 启用
 查看 [无线 VLAN 在线客户端列表](#)

W_VLAN	登录 ID	密码	属性	W_VLAN	登录 ID	密码	属性
0	City	1234	<a href="#">详情</a>	8			<a href="#">详情</a>
1	Home	7890	<a href="#">详情</a>	9			<a href="#">详情</a>
2			<a href="#">详情</a>	10			<a href="#">详情</a>
3			<a href="#">详情</a>	11			<a href="#">详情</a>
4			<a href="#">详情</a>	12			<a href="#">详情</a>
5			<a href="#">详情</a>	13			<a href="#">详情</a>
6			<a href="#">详情</a>	14			<a href="#">详情</a>
7			<a href="#">详情</a>	15			<a href="#">详情</a>

☐ 禁止广播和多播流量。

**注意：**

1. 登录 ID: 1~11 字符，密码: 1~11 字符
2. 禁用广播和多播以最大化无线 VLAN 安全性；不过，无线局域网吞吐量将会降低。
3. 无线客户端登录 URL:  
<http://www.draytek.vlan/login.htm> 或 [http://\(Vigor IP 地址\)/login.htm](http://(Vigor IP 地址)/login.htm)

确定

取消

启用

点选以启用无线 VLAN 功能。

登录 ID

输入 W\_VLAN 组的登录 ID 的 1~11 个字符。

密码

输入 W\_VLAN 组的密码的 1~11 个字符。

## 详情

点击此键将可设定 W\_VLAN 的额外属性设置。

VLAN >> 无线VLAN设置

**W\_VLAN0 属性**

激活日期:	2006	1	1
过期日期:	2010	1	1
<input type="checkbox"/> 连接所有的WDS连接和此VLAN组。			
<input type="checkbox"/> 隔离该VLAN中的每个用户			

确定 取消

**激活日期** – 点击下拉菜单选择无线 VLAN 的激活日期。  
无线 VLAN 功能在那时起被激活。

**过期日期** – 点击下拉菜单选择无线 VLAN 的过期日期。  
无线 VLAN 功能在那时起失效。

**连接所有的 WDS 连接和此 VLAN 组** – 点选此选框将激活此连接。

**隔离该 VLAN 组中的每个用户** – 点选此选框将隔离 VLAN 组中的各个用户，它们之间将无法共享信息。

## 禁止广播和多播流量

点选此选框以禁止所有发向 W\_VLAN 的广播和多播流量。

## 您（无线用户）如何接入 Internet 呢？

在配置好无线 VLAN 后，无线用户必须完成以下步骤以接入 Internet。

1. 打开浏览器，然后在地址栏内输入<http://www.draytek.vlan/login.htm>或者http://(Vigor router's IP address)/login.htm
2. 将出现如下页面。

**DrayTek 无线 VLAN**

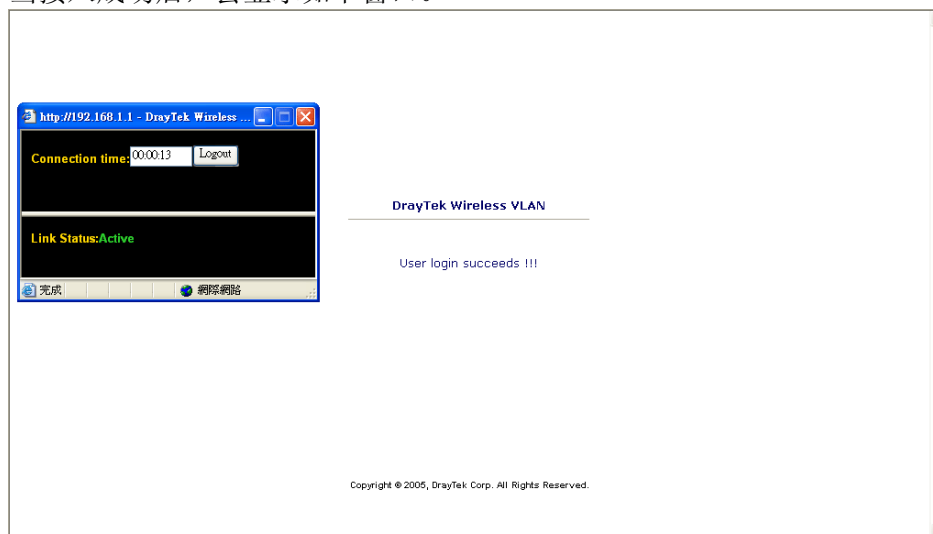
---

登录 ID	City
密码	•••••

确定

3. 输入您在无线 VLAN 组页面所设置的登录 ID 和密码。在这个例子中，我们选用第一组的 W\_VLAN 配置。(City 和 1234).

4. 当接入成功后，会显示如下窗口。



**注释：**弹出的连线时间窗口将一直显示，直到您登出。

5. 您可以到**诊断 >> 无线 VLAN 在线客户端**查看无线 VLAN 的连线状态。  
**诊断 >> 无线VLAN在线客户端**

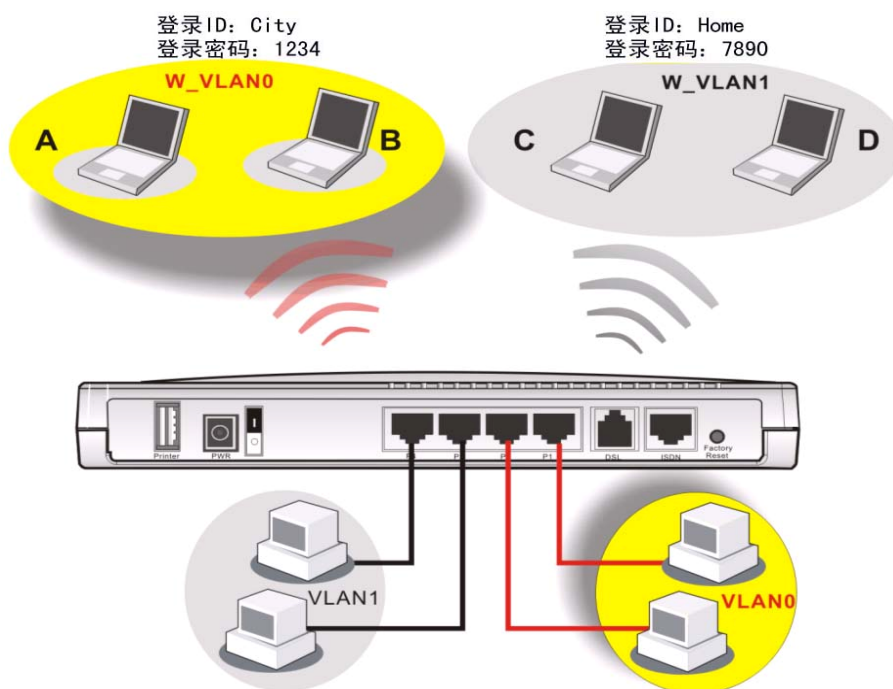
无线VLAN在线客户端列表

| 刷新 |

IP Address	MAC Address	Login ID
192.168.1.15	00-14-85-26-00-8C	City
192.168.1.16	00-0E-35-A8-A4-E7	Home

### 3.13.3 VLAN 交叉设定

这个功能允许通过组合有线 VLAN 和无线 VLAN，来管理不同的电脑（笔记本），使得网络架设更加灵活。通过 **VLAN 交叉设定**，笔记本 A/B 和 VLAN0 内的 PC 可以共享资源。



**VLAN >> VALN 交叉设定** 好似在有线 VLAN 和无线 VLAN 之间架起了一座桥梁。为了达到以上目的，只需简单的点选 W\_VLAN0 一行上的 VLAN0 选框即可。

VLAN 交叉设定

☒ 启用

	VLAN0	VLAN1	VLAN2	VLAN3
W_VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WDS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**注意:**  
1. W\_VLANi: 无线 VLAN i, 参考 **无线 VLAN 设置** 获得详细信息。  
2. 所有的 WDS 连接属于同一 VLAN 组。  
3. VLANi: 有线VLAN i, 参考 **有线 VLAN 设置** 获得详细信息。  
4. 必须同时启用有线和无线VLAN以使VLAN交叉设置生效。

- 启用

点选此选框以启用 VLAN 交叉设定。
- VLAN0-3

指以太网接口的有线 VLAN 组。
- W\_VLAN0-15

指以无线接口的无线 VLAN 组。

3.13.4 无线速率控制

速率控制控制着通过路由器数据的输入和输出速率。而**无线速率控制**则还可以控制每个无线 VLAN 的进/出速度。请到 **VLAN** 菜单，选择**无线速率控制**，将会出现如下页面。按启用激活 VLAN 功能。



无线VLAN速率控制

☒ 启用范围 : 100~30,000 Kbps, 增量 : 100 Kbps

W_VLAN	上行速率(Kbps)	下行速率 (Kbps)	W_VLAN	上行速率(Kbps)	下行速率 (Kbps)
0	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	8	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
1	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	9	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
2	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	10	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
3	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	11	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
4	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	12	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
5	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	13	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
6	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	14	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>
7	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>	15	<input type="text" value="300"/> <input type="text" value="00"/>	<input type="text" value="300"/> <input type="text" value="00"/>

**注意：**指定的速率是整个VLAN组的总速率。

确定

取消

- 启用

点此选框以激活此功能。此速率控制可以控制上行以及下行的传输速率。
- 上行速率

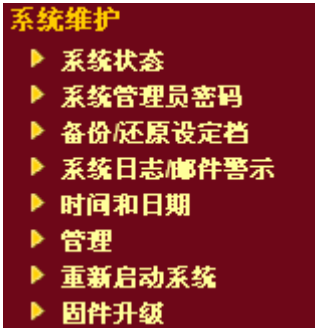
这里指向外的数据传输速度。默认设置为 300。设置范围为 100kbps~20000kbps。请根据您的需求设置合适的数值。
- 下行速率

这里指向内的数据传输速度。默认设置为 300。设置范围为 100kbps~20000kbps。请根据您的需求设置合适的数值。

### 3.14 系统维护

系统管理提供了一些基本和必要的设定，包括：系统状态、管理员密码设定、备份设定、系统日志(Syslog)、时间设定、重启系统、固件升级以及特征库升级。

下面显示的是系统维护的目录



#### 3.14.1 系统状态

系统状态页面提供了 Vigor 路由器的基本网络设定的信息，包括 LAN 和 WAN 接口的信息。同时，您可以在这里查到当前运行的固件的版本或其它相关信息。

系统状态	
型号名称	: DrayTek Vigor2910
固件版本	: v3.0.2
建立日期/时间	: Tue Aug 22 16:41:58.53 2006
LAN	
MAC地址	: 00-50-7F-33-31-EC
LAN IP 地址	: 192.168.1.1
子网掩码	: 255.255.255.0
DHCP服务器	: 启用
DNS	: 194.109.6.66
WAN 1 (172)	
连接状态	: 已连接
MAC地址	: 00-50-7F-33-31-ED
连线	: Static IP
IP地址	: 172.17.1.11
默认网关	: 172.17.1.3
VoIP	
端口	: 1 2
SIP注册	:
帐号ID	: change_me change_me
注册	:
Codec	:
拨入电话	: 0 0
呼出电话	: 0 0
无线局域网	
MAC地址	: 00-14-85-d8-50-d6
频率区域	: 欧洲
固件版本	: v2.01.10.10.5.4

型号名称	显示路由器的型号名称。
固件版本	显示路由器的固件版本。
建立日期/时间	显示当前固件产生的日期和时间。
LAN 部分	
MAC 地址	显示 LAN 接口的 MAC 地址。
LAN IP 地址	显示 LAN 接口的 IP 地址。
子网掩码	显示 LAN 接口 IP 地址的子网掩码。
DHCP 服务器	显示 LAN 接口的 DHCP 服务器的当前状态。
WAN 部分	
MAC 地址	显示 WAN 接口的 MAC 地址。
连线	显示 WAN 连线的模式。

IP 地址	显示 WAN 接口的 IP 地址。
默认网关	显示默认网关的 IP 地址。
DNS	显示主 DNS 的 IP 地址。
<i>无线部分</i>	
MAC 地址	显示 LAN 接口的 MAC 地址。
频段范围	显示在不同的国家无线产品适用的频段是不同的。欧洲国家:13 个可用频段, 美国:11 个可用频段等。
固件版本	显示无线迷你 PCI 卡的型号。同时提供了在迷你 PCI 卡上可使用功能的信息。

### 3.14.2 系统管理员密码

您可以在这里更改管理员密码。

系统管理 >> 管理员密码设定

#### 管理员密码

原密码	<input type="password"/>
新密码	<input type="password"/>
重新输入新密码	<input type="password"/>

**原密码** 输入当前的管理员密码，默认密码为空。

**新密码** 在该栏输入新的密码。

**重新输入新密码** 再输入一遍新的密码。

点击**确定**后，将弹出登录窗口。请使用新的密码重新进入路由器的 web 配置界面。

### 3.14.3 备份/还原设定档

#### 备份设定档

请按照以下步骤来备份路由器的设定档。

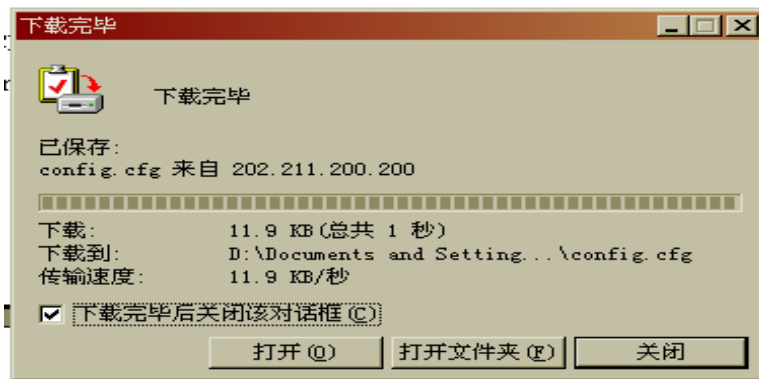
1. 进入**系统管理 >> 备份设定**页面。将显示如下窗口。

系统管理 >> 备份设定

#### 备份 / 还原设定档

<b>还原</b>	
选取一个设定档	
<input type="text"/>	<input type="button" value="浏览..."/>
按一下"还原"将档案上传。	
<input type="button" value="还原"/>	
<b>备份</b>	
按一下"备份"将路由器当前设定保存为文件。	
<input type="button" value="备份"/>	<input type="button" value="取消"/>

2. 点击**备份**按钮，将弹出以下对话框。点击**保存**按钮将打开另一个对话框，可将设定档保存为一个文件。



3. 在另存为对话框里，默认的文件名是 **config.cfg**，您可以给它另取一个名字。



4. 点击**保存**按钮，设定档将被自动下载到您的机器上并保存为一个叫 **config.cfg** 的文件。

以上例子采用 **Windows** 平台示范。**Mac** 或 **Linux** 平台将显示不同的窗口，但是备份功能都是可用的。

**注释：** 备份认证证书必须单独完成。设置备份不包括证书信息。

## 还原设定档

1. 进入**系统管理 >> 备份设定**页面。将显示如下窗口。

系统管理 >> 备份设定

### 备份 / 还原设定档

<b>还原</b>
选取一个设定档 <input type="text"/> <input type="button" value="浏览..."/>
按一下"还原"将档案上传。 <input type="button" value="还原"/>
<b>备份</b>
按一下"备份"将路由器当前设定保存为文件。 <input type="button" value="备份"/> <input type="button" value="取消"/>

2. 点击**浏览**按钮，选择正确的设定档文件。
3. 点击**还原**按钮，等待几秒钟。出现如下图片即表明还原操作成功。

## 3.14.4 系统日志 (Syslog) / 邮件警示

系统日志功能用来监控路由器。通过运行系统日志后台程序来捕捉路由器的所有活动，以便监视路由器的工作状况。

系统管理 >> 系统日志(Syslog)/邮件警示设定

### 系统日志(Syslog)/邮件警示设定

<b>日志 (SysLog) 设定</b>	<b>邮件预警功能设定</b>
<input checked="" type="checkbox"/> 启用	<input type="checkbox"/> 启用
服务器IP地址 <input type="text" value="192.168.1.40"/>	SMTP 服务器 <input type="text"/>
目标端口 <input type="text" value="514"/>	收件人 <input type="text"/>
启用的系统日志消息:	回信地址 <input type="text"/>
<input checked="" type="checkbox"/> 防火墙日志	<input type="checkbox"/> 认证
<input checked="" type="checkbox"/> VPN日志	用户名 <input type="text"/>
<input checked="" type="checkbox"/> 用户接入日志	密码 <input type="text"/>
<input checked="" type="checkbox"/> 拨号日志	
<input checked="" type="checkbox"/> WAN日志	
<input checked="" type="checkbox"/> 路由器/DSL信息	

启用

点选**启用**启动 Syslog 服务。

服务器 IP 地址

指定用于接收 Syslog 信息的主机的 IP 地址。

目标端口

指定 Syslog 服务器监听的 UDP 端口。默认端口为 514。

SMTP 服务器

指定发送邮件的 SMTP 服务器的 IP 地址。

收件人

指定接收者的电子邮件地址，用于接收系统日志信息。

回信地址

指定另一个电子邮件地址，在收件人的邮箱出现问题时，用于接收返回的信息。

认证

如果用该 SMTP 服务器发送邮件需要认证，请点选认证框。

用户名

输入用于认证的用户名。

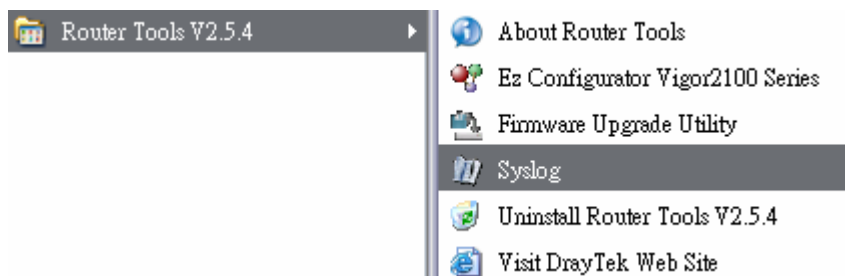
密码

输入用于认证的密码。

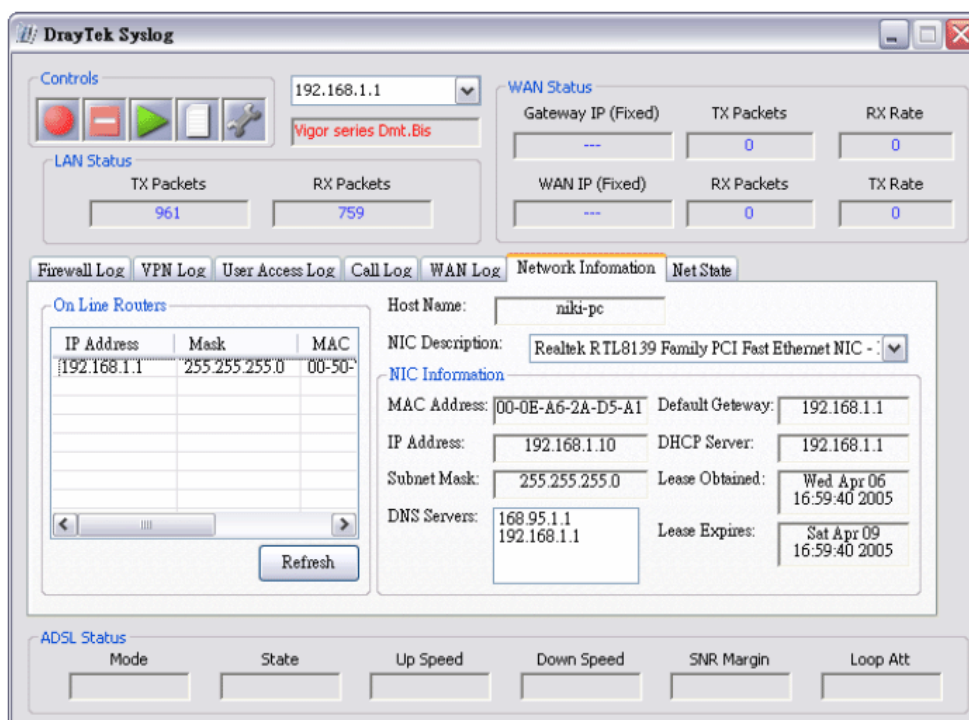
点击**确定**保存设定。

要查看系统日志，请按照以下步骤：

1. 在服务器 IP 地址栏里输入用于监控的 PC 的 IP 地址。
2. 在提供的光盘里找到 **Utility** 文件夹，安装里面的 Router Tools。安装好后，在程序菜单里点击 **Router Tools>>Syslog**



3. 打开 Syslog 工具后，选择您想要监控的路由器的 IP 地址。如果接收不到系统日志，请确保在 **Network Information** 里（图中的 192.168.1.1）选择了正确的网卡（连接路由器的网卡）。



3.14.5 时间和日期

在这个页面您可以设定路由器的系统时间。

系统管理 >> 时间和日期

时间资讯

当前系统时间

2000 Jan 1 Sat 3 : 0 : 6

获取时间

时间设定

☒ 使用PC时间

☐ 连接Internet时间服务器

时间协议

服务器IP地址

时区

启用夏令时

自动更新间隔

NTP (RFC-1305)

pool.ntp.org

(GMT) 格林威治标准时间: 都柏林

☐

30分钟

确定

取消

当前系统时间

使用 PC 时间

使用互联网时间服务器

时间协议

服务器 IP 地址

时区

自动更新间隔

点击确定保存设定。

点击**获取时间**来获得当前的时间和日期。

选择该选项将从当前管理员的 PC 上获取系统时间。

选择该选项将使用指定的协议从 Internet 上的一台时间服务器获取系统时间。

选择一个时间协议。

输入时间服务器的 IP 地址。

选择路由器所在地区的时区。

选择从时间服务器更新时间的间隔。

3.14.6 管理设定

它提供了一些基本的管理条目，包括接入列表，端口设定，SNMP 设定等。例如，作为访问控制管理，端口号被用在发送或接收 SIP 文件的会话中。当打网络电话时，SIP 端口必须与注册端口相同。默认的 SIP 端口是 5060。

管理设定

管理接入控制

☐ 启用远端固件升级 (FTP)

☒ 允许从Internet进行管理

☐ 禁止来自Internet的PING

接入列表

列表	IP	子网掩码
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

管理通讯端口设定

☐ 默认端口 (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)

☒ 用户自定义通讯端口

Telnet通讯端口

23

HTTP通讯端口

80

HTTPS通讯端口

443

FTP通讯端口

21

SNMP设定

☐ 启用SNMP代理程序

Get Community

public

Set Community

private

管理员主机IP

Trap Community

public

通知主机IP

Trap超时

10

秒

- 启用远端固件升级

点选该功能可允许从 Internet 通过 FTP 远程升级固件。
- 允许从 Internet 进行管理

点选该功能可允许系统管理员从 Internet 上远程登录路由器。此功能默认是关闭的。
- 禁止来自 Internet 的 Ping

点选该功能可以防止别人利用 ping 命令来探测您是否在线。此功能默认是打开的。
- 接入列表

您可以指定哪些特定的主机或网段可以从 Internet 远程访问您的路由器。最多可以设置三条记录。

列表 IP - 设定哪些 IP 地址的主机可以访问路由器。

子网掩码 - 设定在哪些子网中的主机可以访问路由器。
- 默认端口

路由器出厂时预先设好的通讯端口。.
- 用户自定义通讯端口

为路由器内建的管理服务器设置用户自定义的端口。
- 启用 SNMP 代理程序

点选此框可以开启路由器内建的 SNMP 代理程序。
- Get Community

为 SNMP GET 命令的管理 community 指定一个字符串。默认是 **public**。
- Set Community

为 SNMP SET 命令的管理 community 指定一个字符串。默认是 **private**。
- 管理员主机 IP

指定 SNMP 管理主机的 IP 地址。



<b>Trap Community</b>	为 SNMP TRAP 的管理 community 指定一个字符串。默认是 <b>public</b> 。
<b>通知主机 IP</b>	指定一个 IP 地址用于接收 TRAP 通告。
<b>Trap 超时</b>	默认设定是 10 秒。

### 3.14.7 重启系统

在这个页面里您可以重新启动路由器。在设置页面里点击**重启系统**就会打开如下页面。

系统管理 >> 重启系统

#### 重启系统

您想重新启动路由器吗？

- ☒ 使用当前设置  
☐ 使用出厂默认设定

确定

有两种重启方式：**使用当前设置重启**和**使用出厂默认设定重启**。

如果您想要路由器重启后保存当前设置，就选择第一项并点击**确定**重启。

如果您想要路由器重启后恢复到出厂时的默认设置，就选择第二项重启。注：路由器重启需要大约 5 秒。

### 3.14.8 固件升级

在升级您的路由器的固件之前，您需要安装一个路由器工具——Router Tools。固件升级工具(Firmware Upgrade Utility)就包含在这个工具包里。下面我们将为您举例说明如何升级您路由器的固件。

注：这个例子是运行在 Windows 操作系统之上的。

从DrayTek网站或FTP站点下载最新的固件文件。DrayTek的网址是[www.draytek.com](http://www.draytek.com)，（或者在您当地的DrayTek代理商的站点也可以下载）。FTP的地址是[ftp.draytek.com](ftp://ftp.draytek.com)。

点击 **开始 > 程序 > Router Tools > Firmware Upgrade Utility**，打开固件升级工具。

系统维护 >> 固件升级

#### 固件升级

当前固件版本： v3.0.2

##### 固件升级步骤：

- 1. 点击“确定”启动TFTP服务器。
- 2. 打开固件升级工具或其他第三方TFTP客户端软件。
- 3. 检查固件文件名是否正确
- 4. 在固件升级工具中按一下"升级（Upgrade）"以开始升级。
- 5. 升级完成后，TFTP服务器将自动停止执行。

您要升级固件吗？

确定

进入**系统管理>>固件升级**页面，点击**确定**按钮，将出现以下界面。

系统维护 >> 固件升级



TFTP服务器已经运行。请执行固件升级工具升级路由器的固件。当固件升级完成后，此服务器将自行关闭。

关于升级的具体步骤，请参考第四章。

3.15 诊断

使用诊断工具可以观察或诊断您的路由器的运行状态。点击**系统管理>诊断**，就会出现如下所示的画面，接下来我们将对每个工具如何设定做详细的介绍。



3.15.1 拨号触发

点击**诊断 >> 拨号触发**打开如下页面。通过从源地址发送的包触发上网连接。(例如, 像 ISDN , PPPoE, PPPoA 等)

诊断 >> 拨号触发

已触发的拨出封包标头

刷新

HEX格式:

00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

已解码格式:

0.0.0.0 -> 0.0.0.0

Pr 0 len 0 (0)

已解码格式

这显示了触发包的源 IP 地址（本地）、目标 IP 地址（远端）、协议以及包的长度。

刷新

点击此按钮刷新页面。

3.15.2 查看路由表

点击**诊断 >> 路由表**，打开如下页面

当前路由表

刷新

Key: C - connected, S - static, R - RIP, \* - default, ~ - private  
\* 0.0.0.0/ 0.0.0.0 via 172.17.1.3, WAN1  
C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN  
C 172.17.1.0/ 255.255.255.0 is directly connected, WAN1

刷新

点击此按钮刷新页面。

3.15.3 查看 ARP 缓存表

点击**查看 ARP 缓存表**就可以看到保存在路由器中的 ARP（地址解析协议）缓存里的信息。这张表显示了以太网硬件地址（即 MAC 地址）和 IP 地址之间的对应。

以太网ARP缓存表

清除刷新

IP Address	MAC Address
172.17.1.204	00-0A-E4-F5-40-96
172.17.1.72	00-16-76-30-18-E3
172.17.1.201	00-50-7F-28-6E-12
172.17.1.24	00-0E-A6-19-D3-25
172.17.1.41	00-E0-4C-97-62-A8
172.17.1.36	00-14-22-63-66-42
172.17.1.23	00-E0-4C-41-3F-37
172.17.1.31	00-13-20-90-3F-8D
172.17.1.188	00-14-78-32-5F-98
172.17.1.50	00-10-5C-B7-B7-E5
172.17.1.21	00-10-DC-D5-5C-8D
172.17.1.39	00-05-5D-71-D8-A8
172.17.1.88	00-16-76-31-8E-98
172.17.1.112	00-0A-E4-F5-26-19
172.17.1.40	00-13-20-64-23-37

清除

按钮清除所有的 ARP 记录。

刷新

点击此按钮刷新页面。

3.15.4 查看 DHCP 分配的 IP 地址

使用查看 DHCP 分配的 IP 地址工具可以查看 IP 地址分配情况。这个信息对诊断网络问题，如 IP 地址冲突问题很有帮助。

点击**诊断 >> DHCP 表**，打开如下页面。

**诊断 >> 查看DHCP分配的IP地址**

### DHCP IP 分配表

刷新

DHCP server: Running				
Index	IP Address	MAC Address	Leased Time	HOST ID

**Index** DHCP 记录的索引值。

**IP Address** 被分配的 IP 地址。

**MAC Address** IP 地址被分配到的 MAC 地址。

**Leased Time** IP 分配的租约时间。

HOST ID	分配到 IP 的主机名。
1	192.168.1.1
2	192.168.1.2
3	192.168.1.3
4	192.168.1.4
5	192.168.1.5
6	192.168.1.6
7	192.168.1.7
8	192.168.1.8
9	192.168.1.9
10	192.168.1.10
11	192.168.1.11
12	192.168.1.12
13	192.168.1.13
14	192.168.1.14
15	192.168.1.15
16	192.168.1.16
17	192.168.1.17
18	192.168.1.18
19	192.168.1.19
20	192.168.1.20
21	192.168.1.21
22	192.168.1.22
23	192.168.1.23
24	192.168.1.24
25	192.168.1.25
26	192.168.1.26
27	192.168.1.27
28	192.168.1.28
29	192.168.1.29
30	192.168.1.30
31	192.168.1.31
32	192.168.1.32
33	192.168.1.33
34	192.168.1.34
35	192.168.1.35
36	192.168.1.36
37	192.168.1.37
38	192.168.1.38
39	192.168.1.39
40	192.168.1.40
41	192.168.1.41
42	192.168.1.42
43	192.168.1.43
44	192.168.1.44
45	192.168.1.45
46	192.168.1.46
47	192.168.1.47
48	192.168.1.48
49	192.168.1.49
50	192.168.1.50
51	192.168.1.51
52	192.168.1.52
53	192.168.1.53
54	192.168.1.54
55	192.168.1.55
56	192.168.1.56
57	192.168.1.57
58	192.168.1.58
59	192.168.1.59
60	192.168.1.60
61	192.168.1.61
62	192.168.1.62
63	192.168.1.63
64	192.168.1.64
65	192.168.1.65
66	192.168.1.66
67	192.168.1.67
68	192.168.1.68
69	192.168.1.69
70	192.168.1.70
71	192.168.1.71
72	192.168.1.72
73	192.168.1.73
74	192.168.1.74
75	192.168.1.75
76	192.168.1.76
77	192.168.1.77
78	192.168.1.78
79	192.168.1.79
80	192.168.1.80
81	192.168.1.81
82	192.168.1.82
83	192.168.1.83
84	192.168.1.84
85	192.168.1.85
86	192.168.1.86
87	192.168.1.87
88	192.168.1.88
89	192.168.1.89
90	192.168.1.90
91	192.168.1.91
92	192.168.1.92
93	192.168.1.93
94	192.168.1.94
95	192.168.1.95
96	192.168.1.96
97	192.168.1.97
98	192.168.1.98
99	192.168.1.99
100	192.168.1.100

**Refresh** 点击刷新页面。

### 3.15.5 NAT 会话表

点击**诊断 >> NAT 会话表**，打开如下页面。

## 诊断 >> NAT会话表

## NAT活动会话表

刷新

Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface
192.168.1.11	2491	52078	24.9.93.189	443	WAN1
192.168.1.11	2493	52080	207.46.25.2	80	WAN1
192.168.1.10	3079	52665	207.46.5.10	80	WAN1

**Private IP:Port** 本地 PC 的私网地址和端口。

**#Pseudo Port** 路由器用于 NAT 的临时端口。

**Peer IP:Port** 访问的远端目标主机的 IP 地址和端口。

**Ifno** 不同的数字代表不同的界面。

0:	LAN
1~2:	ISDN

3: WAN  
4 or above: VPN

**Status** 不同的状态值分别有以下定义

0: other TCP status  
1: TCP fin incoming  
2: TCP fin out  
3: TCP fin closing  
4: TCP syn  
5: TCP syn,ack  
6: TCP ack

**刷新** 点击此按钮刷新页面。

3.15.6 无线 VLAN 在线客户端

点击**诊断 >> 无线 VLAN 在线客户端列表**打开如下页面。无线 VLAN 在线客户端将显示 IP 地址，MAC 地址和登陆 ID 信息。

**诊断 >> 无线VLAN在线客户端**

无线VLAN在线客户端列表 | 刷新 |

IP Address	MAC Address	Login ID
192.168.1.15	00-14-85-26-00-8C	City
192.168.1.16	00-0E-35-A8-A4-E7	Home

**IP 地址** 显示无线客户端的 IP 地址。

**MAC 地址** 显示无线客户端的 MAC 地址。

**登陆 ID** 显示属于无线客户端的登陆 ID。

3.15.7 PING 诊断

点击**诊断>>PING 诊断**，打开如下页面。

诊断 >> Ping诊断

Ping诊断

注意：：如果您要ping一个局域网地址，或者想要设置自行选择使用的WAN口，请选择“未指定”作为WAN接口。

Ping通过：

未指定

Ping地址：

主机/IP

IP地址：

运行

结果

清除

**Ping 通过** 使用下拉菜单选择您要 PING 通过的 WAN 界面或选择路由器自动定义的未指定选项。

Ping通过：

未指定

未指定

WAN1

WAN2

**Ping 地址** 使用菜单选择您想要 PING 的目标地址。

**IP 地址** 输入您想要 PING 的主机/IP 目标地址。

**运行** 点击**运行**按键数据结果将显现。

**清除** 点击**清除**按键数据结果将清除。

3.15.8 流量监控

通过**流量控制**，可以全面监控 LAN 内各主机的带宽、会话等资源的使用状况。甚至，您可以根据需要封锁那些占用了过多网络资源的 IP 地址。在**带宽管理**里配置 IP 地址列表。调用流量监控之前请您启用 IP 限制带宽和 IP 限制会话。如果没有启用，将有个提示对话框提醒您启用它。

限制会话

启用

禁用

默认会话限制：

100

自定义限制列表

索引	起始 IP	结束 IP
----	-------	-------

点击**诊断>>流量监控**打开如下页面

Vigor2910 系列中文手册

177

[illegible]

**注意：**

1. 点击“封锁”可以停止指定PC上网5分钟。
2. 被屏蔽上网的IP显示为红色，会话数会显示该IP被屏蔽的剩余时间。

**启用流量监控** 点选启用流量监控启用此项。

**排序方式** 使用下拉菜单选择排序方式。

排序方式: IP

**刷新闻隔秒数** 使用下拉菜单选择刷新闻隔秒数。

刷新闻隔秒数: 5

刷新 手动刷新流量监控页面

索引 流量控制记录的索引值。

**IP 地址** 显示内部网络主机的 IP 地址。

上行速率 显示某 IP 地址所占用的上行带宽。

下行速率 显示某 IP 地址所占用的下行带宽。

**会话** 显示某 IP 地址所占用的会话数量。若您已封锁了此 IP，那么这一栏将会显示它剩余的禁封时间。

**动作** 根据需要对某 IP 地址采用相应动作。**封锁**—封锁此 IP 上网 5 分钟。之后，路由器将自动解封。



页:	1	刷新
会话	动作	
1 / 100	封锁	

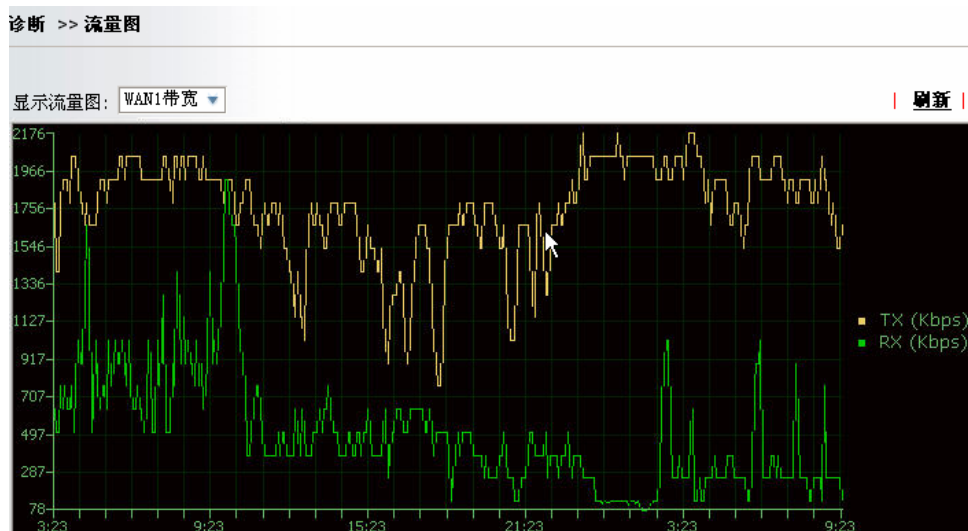
解封-手动解封此 IP 地址。

页:	1	刷新
会话	动作	
blocked / 266	解封	

注意：若监控内部网络流量，您必须先启用**带宽管理的限制会话**以及**限制带宽**功能！

### 3.15.9 流量图

流量图可以用来观察 WAN1，WAN2 以及路由器会话的使用情况，路由器记录 30 小时内的数据，并进行统计绘图。通过下拉框，可选择 WAN1，WAN2 以及会话，来查看 30 小时内路由器带宽和会话的使用情况。



### 3.15.10 路由追踪

点击**诊断>>路由追踪**打开如下页面。这个设置页面允许您从路由器到主机之间的路由追踪。简单地输入主机的 IP 地址点击**运行**。路由追踪的结果将显示页面中。

追踪路由

追踪路由通过:

未指定

主机 / IP地址:

运行

结果

清除

Trace through WAN1.  
traceroute to 172.16.3.229, 30 hops max  
1 Request timed out. \*  
2 Request timed out. \*  
Trace complete.

- Ping 通过

使用下拉菜单选择您要 PING 通过的 WAN 界面或选择路由器自动定义的未指定选项。
- 主机/IP 地址

显示主机/IP 地址。
- 运行

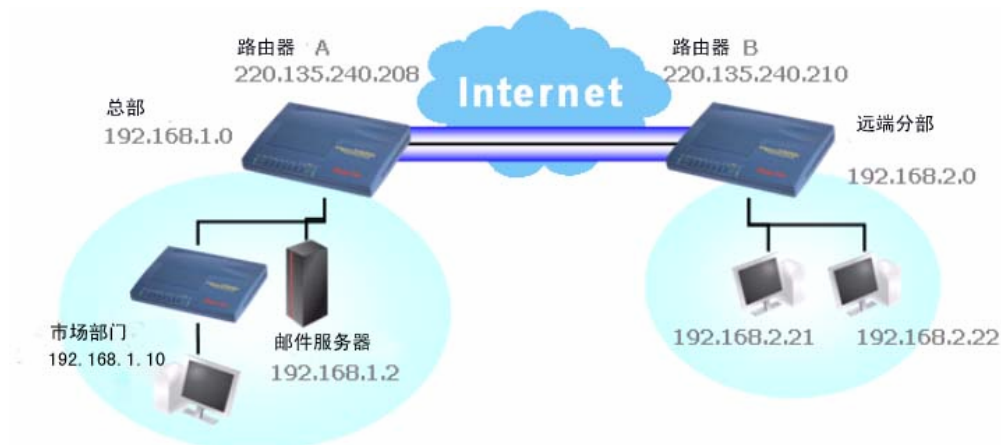
点击**运行**按钮开始路由跟踪。
- 清除

点击**清除**按钮数据结果被清除。

## 4 范例与应用

### 4.1 在总公司与分公司之间建立一条 LAN-to-LAN 连接

一个比较常见的安全网络连接的应用，就是连接总公司与分公司各自的网络。下图显示了这种连接的一个常见的网络结构。您可以按照下列步骤来配置 LAN-to-LAN 设定档。注意，两个网络的网段地址不可以网段。



总公司路由器 A 的设置：

1. 到 **VPN 和远程访问**，点击**远程接入设定**，开启所需 VPN 服务并点击**确定**。
2. 然后，对于基于 **PPP** 的服务（比如 PPTP、L2TP），请到 **PPP 基本设定**作相关设置。

**VPN和远程访问 >> PPP基本设定**

#### PPP基本设定

<b>PPP/MP协议</b>		<b>分配IP给拨入用户</b>
拨入PPP验证	PAP或CHAP	起始IP地址: 192.168.1.8
拨入PPP加密 (MPPE)	可选MPPE	
相互验证 (PAP)	<input type="radio"/> 是 <input checked="" type="radio"/> 否	
用户名		
密码		

确定

对于基于 **IPSec** 的服务（比如 IPSec、应用 IPSec 策略的 L2TP），请到 **IPSec 基本设定**进行设置。

## VPN IKE / IPSec基本设定

远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。

<b>IKE认证方法</b>	
预共享密钥	<input type="password"/>
重新键入预共享密钥	<input type="password"/>
<b>IPSec安全方法</b>	
<input checked="" type="checkbox"/> 中等 (AH) 会对数据进行认证, 但不会加密。	
<input type="checkbox"/> 高等 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 会对数据进行认证及加密。	

确定 取消

- 进入 **LAN-to-LAN**。点击某个索引值号, 进行编辑。
- 按以下图所示配置**一般设定**。您可以选择**双向**, 这样两边都可以发起 VPN 连接。

## VPN和远程访问 &gt;&gt; LAN to LAN

## 设定档索引 : 1

## 1. 一般设定

设定档名称 <input type="text" value="branch1"/>	拨叫方向 <input checked="" type="radio"/> 双向 <input type="radio"/> 拨出 <input type="radio"/> 拨入
<input checked="" type="checkbox"/> 启用此设定档	<input type="checkbox"/> 一直在线
VPN隧道通过: <input type="text" value="WAN1优先"/>	闲置超时 <input type="text" value="300"/> 秒
	<input type="checkbox"/> 启用PING以维持在线
	PING IP <input type="text"/>

- 设置**拨出设定**, 以便主动拨向路由器 B。  
如果选择了**基于IPSec**的服务, 您应该为此拨出连接指定**服务器 IP 或域名**、**IKE 认证方法**以及 **IPSec 安全方法**。

## 2. 拨出设定

<b>我拨叫的服务器类型</b> <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec隧道 <input type="radio"/> 应用IPsec策略的L2TP <span>无</span>	连接类型 <span>64k bps</span> 用户名 <span>???</span> 密码 <span></span> PPP验证 <span>PAP/CHAP</span> VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) <span>172.17.1.100</span>	<b>IKE认证方法</b> <input checked="" type="radio"/> 预共享密钥 <span>IKE预共享密钥</span> <span>.....</span> <input type="radio"/> 数字签名 (X.509) <span>无</span>
	<b>IPsec安全方法</b> <input type="radio"/> 中等 (AH) <input checked="" type="radio"/> 高等 (ESP) <span>DES无验证</span> <span>高级</span>
	索引 (1-15) <b>计划任务</b> 设置: <span></span> , <span></span> , <span></span> , <span></span>
	<b>回拨功能 (CBCP)</b> <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端

如果选择了**基于PPP**的服务,您应该为此拨出连接指定远程端点 IP、用户名、密码 PPP 验证以及 VJ 压缩。

## 2. 拨出设定

<b>我拨叫的服务器类型</b> <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec隧道 <input type="radio"/> 应用IPsec策略的L2TP <span>无</span>	连接类型 <span>64k bps</span> 用户名 <span>123</span> 密码 <span>...</span> PPP验证 <span>PAP/CHAP</span> VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) <span>172.17.1.100</span>	<b>IKE认证方法</b> <input checked="" type="radio"/> 预共享密钥 <span>IKE预共享密钥</span> <span>.....</span> <input type="radio"/> 数字签名 (X.509) <span>无</span>
	<b>IPsec安全方法</b> <input type="radio"/> 中等 (AH) <input checked="" type="radio"/> 高等 (ESP) <span>DES无验证</span> <span>高级</span>
	索引 (1-15) <b>计划任务</b> 设置: <span></span> , <span></span> , <span></span> , <span></span>
	<b>回拨功能 (CBCP)</b> <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端

6. 设置**拨入设定**,以便让路由器 B 建立 VPN 拨入连接。  
如果选择了**基于IPsec**的服务,您应该为此拨入连接指定远端 VPN 网关、IKE 认证方法以及 IPsec 安全方法。否则,它将使用 **IPsec 基本设定**中的设置。

### 3. 拨入设定

允许拨入类型	
<input type="checkbox"/> ISDN	用户名 <input data-bbox="1161 255 1369 291" type="text" value="???"/>
<input type="checkbox"/> PPTP	密码 <input data-bbox="1161 300 1369 336" type="text" value=""/>
<input checked="" type="checkbox"/> IPsec隧道	VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
<input type="checkbox"/> 应用IPsec策略的L2TP <input data-bbox="644 374 756 409" type="text" value="无"/>	
<b>IKE认证方法</b>	
<input checked="" type="checkbox"/> 指定 ISDN CLID 或 远端VPN网关 对端ISDN号码或 对端VPN服务器IP <input data-bbox="413 515 620 551" type="text" value="202.211.100.23"/>	<input checked="" type="checkbox"/> 预共享密钥 IKE预共享密钥 <input data-bbox="1161 472 1377 508" type="text" value="..."/>
或端点ID <input data-bbox="493 560 700 595" type="text" value=""/>	<input type="checkbox"/> 数字签名 (X.509) <input data-bbox="916 553 963 589" type="text" value="无"/>
<b>IPsec安全方法</b>	
	<input checked="" type="checkbox"/> 中等 (AH) 高等 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
<b>回拨功能 (CBCP)</b>	
	<input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 <input data-bbox="1161 882 1369 918" type="text" value=""/> 回拨定额 <input data-bbox="1161 934 1225 969" type="text" value="0"/> 分钟

如果选择了**基于PPP**的服务，您应该为此拨入连接指定远端**VPN**网关、用户名、密码**PPP**验证以及**VJ**压缩。

### 1. 拨入设定

允许拨入类型	
<input type="checkbox"/> ISDN	用户名 <input data-bbox="1161 1120 1361 1155" type="text" value="123"/>
<input checked="" type="checkbox"/> PPTP	密码 <input data-bbox="1161 1164 1361 1200" type="text" value="..."/>
<input type="checkbox"/> IPsec隧道	VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
<input type="checkbox"/> 应用IPsec策略的L2TP <input data-bbox="644 1247 756 1283" type="text" value="无"/>	
<b>IKE认证方法</b>	
<input checked="" type="checkbox"/> 指定 ISDN CLID 或 远端VPN网关 对端ISDN号码或 对端VPN服务器IP <input data-bbox="413 1395 612 1431" type="text" value="202.211.100.23"/>	<input checked="" type="checkbox"/> 预共享密钥 IKE预共享密钥 <input data-bbox="1161 1352 1369 1388" type="text" value=""/>
或端点ID <input data-bbox="493 1440 692 1476" type="text" value=""/>	<input type="checkbox"/> 数字签名 (X.509) <input data-bbox="916 1433 963 1469" type="text" value="无"/>
<b>IPsec安全方法</b>	
	<input checked="" type="checkbox"/> 中等 (AH) 高等 (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
<b>回拨功能 (CBCP)</b>	
	<input type="checkbox"/> 启用回拨功能 <input type="checkbox"/> 使用以下号码回拨 回拨号码 <input data-bbox="1161 1785 1361 1821" type="text" value=""/> 回拨定额 <input data-bbox="1161 1836 1225 1872" type="text" value="0"/> 分钟

- 最后，在 **TCP/IP 网络设定**中，配置远端网络 IP/子网，这样路由器 A 可以通过 PVN 连接发送数据包到远端网络。

#### 4. TCP/IP网络设定

我的WAN IP	<input type="text" value="0.0.0.0"/>	RIP方向	<input type="button" value="禁用"/>
远端网关IP	<input type="text" value="0.0.0.0"/>	RIP版本	<input type="button" value="Ver. 2"/>
远端网络IP	<input type="text" value="192.168.2.0"/>	在NAT操作中，将远端子网视为	<input type="button" value="私网IP"/>
远端子网掩码	<input type="text" value="255.255.255.0"/>		
<input type="button" value="更多"/>		<input type="checkbox"/> 变更默认路由到此VPN隧道	

子公司路由器B的设置：

- 到 **VPN 和远程拨入**中，点击**远程接入控制**，开启需要的 VPN 服务并点击**确定**。
- 然后，对于基于 **PPP** 的服务（比如 PPTP、L2TP），请到 **PPP 基本设定**进行设置。

**VPN和远程访问 >> PPP基本设定**

<b>PPP基本设定</b>		<b>分配IP给拨入用户</b>	
<b>PPP/MP协议</b>		起始IP地址：	<input type="text" value="192.168.1.8"/>
拨入PPP验证	<input type="button" value="PAP或CHAP"/>		
拨入PPP加密（MPPE）	<input type="button" value="可选MPPE"/>		
相互验证（PAP）	<input type="radio"/> 是 <input checked="" type="radio"/> 否		
用户名	<input type="text"/>		
密码	<input type="text"/>		
<input type="button" value="确定"/>			

对于基于 **IPSec** 的服务（比如 IPSec、应用 IPSec 策略的 L2TP），请到 **IPSec 基本设定**进行设置。

**VPN和远程访问 >> IPSec基本设定**

<b>VPN IKE / IPSec基本设定</b>	
远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。	
<b>IKE认证方法</b>	
预共享密钥	<input type="text" value="..."/>
重新键入预共享密钥	<input type="text" value="..."/>
<b>IPSec安全方法</b>	
<input checked="" type="checkbox"/> 中等（AH）	会对数据进行认证，但不会加密。
<input type="checkbox"/> 高等（ESP）	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	会对数据进行认证及加密。
<input type="button" value="确定"/>	<input type="button" value="取消"/>

- 进入 **LAN-to-LAN**。点击某个索引值号，进行编辑。
- 按以下图所示配置**一般设定**。您可以选择**双向**，这样两边都可以发起 VPN 连接。

**VPN和远程访问 >> LAN to LAN**

**设定档索引：1**

#### 1. 一般设定

设定档名称	<input type="text" value="branch1"/>	拨叫方向	<input checked="" type="radio"/> 双向 <input type="radio"/> 拨出 <input type="radio"/> 拨入
<input checked="" type="checkbox"/> 启用此设定档		<input type="checkbox"/> 一直在线	
VPN隧道通过：	<input type="button" value="WAN1优先"/>	闲置超时	<input type="text" value="300"/> 秒
		<input type="checkbox"/> 启用PING以维持在线	
		PING IP	<input type="text"/>

5. 设置**拨出**设定，以便主动拨向路由器 A。  
如果选择了**基于IPSec**的服务，您应该为此拨出连接指定**服务器 IP 或域名**、**IKE 认证方法**以及 **IPSec 安全方法**（两边路由器须一致）。

## 2. 拨出设定

<b>我拨出的服务器类型</b> <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec隧道 <input type="radio"/> 应用IPSec策略的L2TP <span>无</span>	连接类型 <span>64k bps</span> 用户名 <span>???</span> 密码 <span></span> PPP验证 <span>PAP/CHAP</span> VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) <span>172.17.1.100</span>	<b>IKE认证方法</b> <input checked="" type="radio"/> 预共享密钥 IKE预共享密钥 <span>.....</span> <input type="radio"/> 数字签名 (X.509) <span>无</span>
	<b>IPSec安全方法</b> <input type="radio"/> 中等 (AH) <input checked="" type="radio"/> 高等 (ESP) <span>DES无验证</span> <b>高级</b>
	索引 (1-15) <b>计划任务</b> 设置: <span></span> , <span></span> , <span></span> , <span></span>
	<b>回拨功能 (CBCP)</b> <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端

如果选择了**基于PPP**的服务，您应该为此拨出连接指定服务器 IP 或域名、用户名、密码 PPP 验证以及 VJ 压缩（两边路由器须一致）。

## 2. 拨出设定

<b>我拨出的服务器类型</b> <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPSec隧道 <input type="radio"/> 应用IPSec策略的L2TP <span>无</span>	连接类型 <span>64k bps</span> 用户名 <span>123</span> 密码 <span>...</span> PPP验证 <span>PAP/CHAP</span> VJ压缩 <input checked="" type="radio"/> 开 <input type="radio"/> 关
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) <span>172.17.1.100</span>	<b>IKE认证方法</b> <input checked="" type="radio"/> 预共享密钥 IKE预共享密钥 <span>.....</span> <input type="radio"/> 数字签名 (X.509) <span>无</span>
	<b>IPSec安全方法</b> <input type="radio"/> 中等 (AH) <input checked="" type="radio"/> 高等 (ESP) <span>DES无验证</span> <b>高级</b>
	索引 (1-15) <b>计划任务</b> 设置: <span></span> , <span></span> , <span></span> , <span></span>
	<b>回拨功能 (CBCP)</b> <input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端

6. 配置**拨入**设定，以便让路由器 A 建立 VPN 拨入连接。  
如果选择了**基于IPSec**的服务，您应该为此拨入连接指定远端点 VPN 网关、IKE 认证方法以及 IPSec 安全方法。否则，它将使用 **IPSec 基本设定**中的设置。



### 3. 拨入设定

允许拨入类型	
<input type="checkbox"/> ISDN	
<input type="checkbox"/> PPTP	
<input checked="" type="checkbox"/> IPSec隧道	
<input type="checkbox"/> 应用IPSec策略的L2TP	无
<input checked="" type="checkbox"/> 指定 ISDN CLID 或 远端VPN网关 对端ISDN号码或 对端VPN服务器IP 202.211.100.23 或端点ID	

用户名	???
密码	
VJ压缩	<input checked="" type="radio"/> 开 <input type="radio"/> 关
<b>IKE认证方法</b>	
<input checked="" type="checkbox"/> 预共享密钥	
IKE预共享密钥	...
<input type="checkbox"/> 数字签名 (X.509)	
无	
<b>IPSec安全方法</b>	
<input checked="" type="checkbox"/> 中等 (AH)	
高等 (ESP)	
<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	
<b>回拨功能 (CBCP)</b>	
<input type="checkbox"/> 启用回拨功能	
<input type="checkbox"/> 使用以下号码回拨	
回拨号码	
回拨定额	0 分钟

如果选择了**基于PPP**的服务，您应该为此拨入连接指定远端 VPN 网关、用户名、密码 PPP 验证以及 VJ 压缩。

### 4. 拨入设定

允许拨入类型	
<input type="checkbox"/> ISDN	
<input checked="" type="checkbox"/> PPTP	
<input type="checkbox"/> IPSec隧道	
<input type="checkbox"/> 应用IPSec策略的L2TP	无
<input checked="" type="checkbox"/> 指定 ISDN CLID 或 远端VPN网关 对端ISDN号码或 对端VPN服务器IP 202.211.100.23 或端点ID	

用户名	123
密码	...
VJ压缩	<input checked="" type="radio"/> 开 <input type="radio"/> 关
<b>IKE认证方法</b>	
<input checked="" type="checkbox"/> 预共享密钥	
IKE预共享密钥	
<input type="checkbox"/> 数字签名 (X.509)	
无	
<b>IPSec安全方法</b>	
<input checked="" type="checkbox"/> 中等 (AH)	
高等 (ESP)	
<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	
<b>回拨功能 (CBCP)</b>	
<input type="checkbox"/> 启用回拨功能	
<input type="checkbox"/> 使用以下号码回拨	
回拨号码	
回拨定额	0 分钟

7. 最后，在 **TCP/IP 网络设定**中，配置远端网络 IP/子网，这样路由器 A 可以通过 PVN 连接发送数据包到远端网络。

**4. TCP/IP网络设定**

我的WAN IP	<input type="text" value="0.0.0.0"/>	RIP方向	<input type="button" value="禁用"/>
远端网关IP	<input type="text" value="0.0.0.0"/>	RIP版本	<input type="button" value="Ver. 2"/>
远端网络IP	<input type="text" value="192.168.1.0"/>	在NAT操作中，将远端子网视为	<input type="button" value="私网IP"/>
远端子网掩码	<input type="text" value="255.255.255.0"/>		
<input type="button" value="更多"/>		<input type="checkbox"/> 变更默认路由到此VPN隧道	

## 4.2 在企业网络和远程用户之间建立一个远程拨入连接

另一个常见的情形就是，一个远程用户安全地连回企业网络获取信息。根据下图所示网络结构，请按照以下的步骤配置一个路由器上的远程拨入用户帐号，以及在远程主机上用 Smart VPN Client 设置一个拨出帐号。



企业网络中VPN路由器上的设置：

1. 到 **VPN 和远程拨入** 中，点击**远程接入控制**，开启需要的 VPN 服务并点击**确定**。
2. 然后，  
对于**基于PPP 的服务**（比如 PPTP、L2TP），请到 **PPP 基本设定** 作相关设置。

VPN和远程访问 >> PPP基本设定

PPP基本设定	
<b>PPP/MP协议</b>	
拨入PPP验证	PAP或CHAP
拨入PPP加密 (MPPE)	可选MPPE
相互验证 (PAP)	<input type="radio"/> 是 <input checked="" type="radio"/> 否
用户名	
密码	
<b>分配IP给拨入用户</b>	
起始IP地址:	192.168.1.8

确定

对于**基于IPSec 的服务**（比如 IPSec、应用 IPSec 策略的 L2TP），请到 **IPSec 基本设定** 进行设置。

## VPN IKE / IPSec基本设定

远程拨入用户及动态IP客户的拨入设定(LAN to LAN)。

<b>IKE认证方法</b>	
预共享密钥	●●●
重新键入预共享密钥	●●●
<b>IPSec安全方法</b>	
<input checked="" type="checkbox"/> 中等 (AH) 会对数据进行认证, 但不会加密。	
高等 (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 会对数据进行认证及加密。
<div>确定</div> <div>取消</div>	

3. 到远程拨入用户，点击某个索引值，进行编辑。
4. 按下图设置拨入设定，以便让远端用户建立 VPN 拨入连接。

如果选择了**基于IPSec**的服务，您应该指定此拨入连接**远程端点 IP**、**IKE 认证方法**以及**IPSec 安全方法**。若没有特别指定，它将使用**IPSec 基本设定**中的配置。

## 2. 拨出设定

<b>我拨出的服务器类型</b>	
<input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec隧道 <input type="radio"/> 应用IPSec策略的L2TP <span>无</span>	
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) <input type="text" value="172.17.1.100"/>	
连接类型	<span>64k bps</span>
用户名	<input data-bbox="1177 929 1358 958" type="text" value="???"/>
密码	<input type="password"/>
PPP验证	<span>PAP/CHAP</span>
VJ压缩	<input checked="" type="radio"/> 开 <input type="radio"/> 关
<b>IKE认证方法</b>	
<input checked="" type="radio"/> 预共享密钥	
IKE预共享密钥	●●●●●●●●
<input type="radio"/> 数字签名 (X.509)	
<span>无</span>	
<b>IPSec安全方法</b>	
<input type="radio"/> 中等 (AH)	
<input checked="" type="radio"/> 高等 (ESP) <span>DES无验证</span>	
<b>高级</b>	
索引 (1-15) <b>计划任务</b> 设置:	
<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	
<b>回拨功能 (CBCP)</b>	
<input type="checkbox"/> 要求远端回拨	
<input type="checkbox"/> 提供ISDN号码给远端	

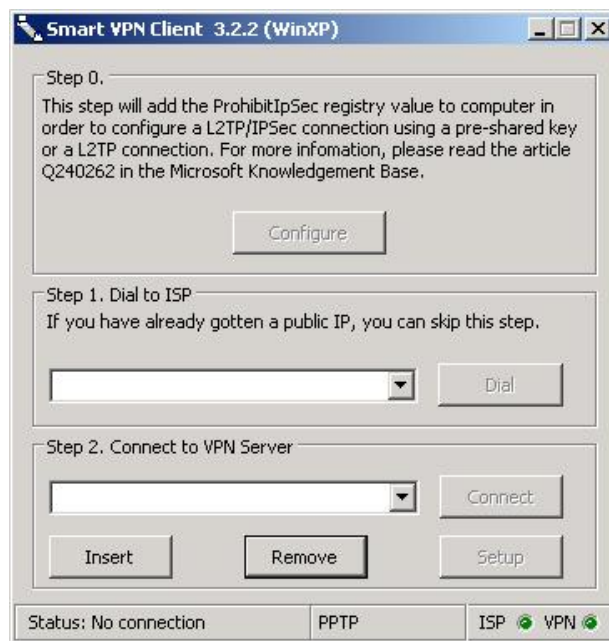
如果选择了**基于PPP**的服务，您应该指定此拨入连接**远程端点 IP**、**用户名**、**密码**以及**VJ 压缩**。

## 2. 拨出设定

<b>我拨叫的服务器类型</b>	
<input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPSec隧道 <input type="radio"/> 应用IPSec策略的L2TP 无	
ISDN拨号号码或 VPN服务器IP/主机名 (比如 5551234, draytek.com 或 123.45.67.89) 172.17.1.100	
连接类型	64k bps
用户名	123
密码	...
PPP验证	PAP/CHAP
VJ压缩	<input checked="" type="radio"/> 开 <input type="radio"/> 关
<b>IKE认证方法</b>	
<input checked="" type="radio"/> 预共享密钥 IKE预共享密钥 .....	
<input type="radio"/> 数字签名 (X.509) 无	
<b>IPSec安全方法</b>	
<input type="radio"/> 中等 (AH) <input checked="" type="radio"/> 高等 (ESP) DES无验证	
高级	
索引 (1-15) 计划任务 设置: , , ,	
<b>回拨功能 (CBCP)</b>	
<input type="checkbox"/> 要求远端回拨 <input type="checkbox"/> 提供ISDN号码给远端	

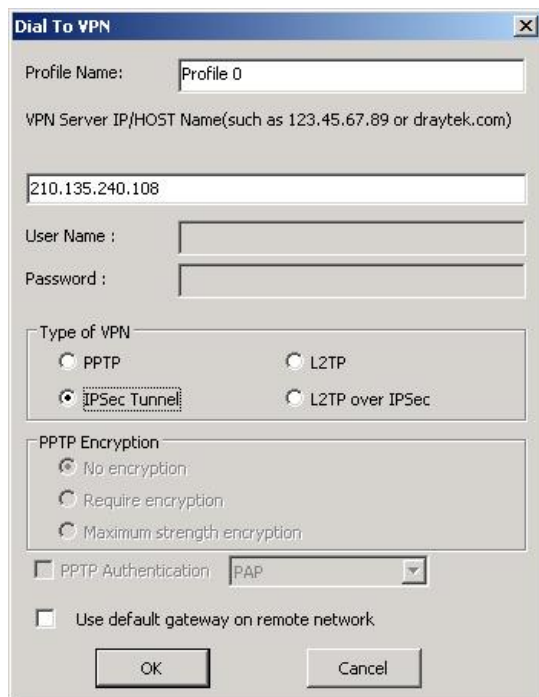
### 远端主机上的设置:

1. Win98/ME的用户, 可以使用**拨号网络**来建立PPTP隧道到Vigor路由器。  
Win2000/XP的用户, 可以使用**网络与拨号连接**或**Smart VPN Client**作为补充工具, 来建立PPTP、L2TP以及应用IPSec策略的L2TP 隧道。您可以在包装盒内的CD包找到这个工具, 或者也可以到[www.draytek.com.cn](http://www.draytek.com.cn) 下载, 并按照指导进行安装。
2. 完成安装后, 第一次使用此工具的用户, 请点击 **Step 0. Configure** 按键。然后重启电脑。



3. 在 **Step 2. Connect to VPN Server** 中, 点击 **Insert** 按键以添加一条新的设定档。

若选择了**基于IPSec**的服务, 比如 IPSec 隧道, 请参考以下图示



**Dial To VPN**

Profile Name:

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

User Name :

Password :

Type of VPN

☐ PPTP ☐ L2TP

☒ IPsec Tunnel ☐ L2TP over IPsec

PPTP Encryption

☒ No encryption

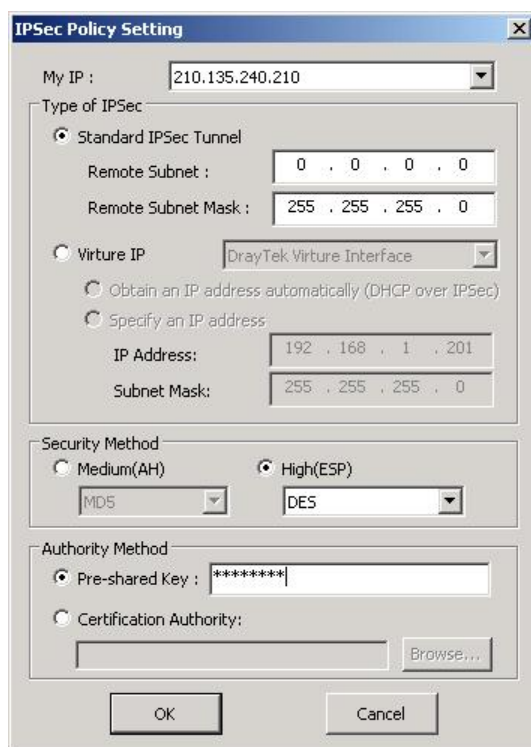
☐ Require encryption

☐ Maximum strength encryption

☐ PPTP Authentication:

☐ Use default gateway on remote network

您可以指定 IPsec 类型（Standard IPsec Tunnel 或 Virture IP，若是 Virture IP 将从路由器的 LAN 获取一个本地私网 IP）、安全方法、认证方法等。若选择了预共享密钥，它必须与 VPN 路由器上的一致。



**IPsec Policy Setting**

My IP :

Type of IPsec

☒ Standard IPsec Tunnel

Remote Subnet :

Remote Subnet Mask :

☐ Virture IP

☐ Obtain an IP address automatically (DHCP over IPsec)

☐ Specify an IP address

IP Address:

Subnet Mask:

Security Method

☐ Medium(AH) ☒ High(ESP)

Authority Method

☒ Pre-shared Key :

☐ Certification Authority:

若是选择了**基于PPP**的服务，您应该指定远端 VPN 服务器的 IP 地址、用户名、密码以及加密认证方式。用户名和密码应与 VPN 服务器上的设置一致。**Use default gateway on remote network** 是指远端主机上的所有数据流都将先发送到 VPN 服务器，然后再发往 Internet，这样就好像远端主机在企业网络中工作一样。

4. 点击 **Connect** 按键发起连接。连接成功后，您可以在右下角的系统任务栏看到绿色的指示灯。

### 4.3 QoS 设置范例

假设有个远程用户有时候需要在家里工作以便照看孩子。工作时，他使用家中 Vigor 路由器连接到总公司的服务器上，通过 HTTPS 或者 VPN 连接来收发邮件和访问内部数据库。同事，孩子们可能在使用 VoIP 或 skype 软件聊天。

1. 确保QoS控制已经被选中。并且选中**双向**。

2. 点击**编辑**链接，输入级别 1 的名称，并且设置为Email （使用POP3 和SMTP）服务保留的带宽。

**带宽管理 >> 服务质量 (QoS)**

#### 基本设定

索引	状态	带宽	方向	级别 1	级别 2	级别 3	其它	UDP带宽控制	
WAN1	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>
WAN2	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>

#### 级别规则

索引	名称	规则	服务类型
级别 1	email	<a href="#">编辑</a>	<a href="#">编辑</a>
级别 2		<a href="#">编辑</a>	
级别 3		<a href="#">编辑</a>	

3. 点击**编辑**链接，输入级别 1 的名称，并且设置为HTTPS（使用POP3 和SMTP）服务保留的带宽。点击右边的基本按钮。

带宽管理 >> 服务质量 (QoS)

#### 基本设定

索引	状态	带宽	方向	级别 1	级别 2	级别 3	其它	UDP带宽控制	
WAN1	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>
WAN2	启用	10000Kbps/10000Kbps	上行	25%	25%	25%	25%	未激活	<a href="#">设置</a>

#### 级别规则

索引	名称	规则	服务类型
级别 1	E-mail	<a href="#">编辑</a>	<a href="#">编辑</a>
级别 2	HTTP	<a href="#">编辑</a>	
级别 3		<a href="#">编辑</a>	

4. 点击WAN1 的**设置**链接。选中下面的**启用UDP带宽控制**来保证UDP的数据包不会影响其他应用。

带宽管理 >> 服务质量 (QoS)

#### WAN1 基本设定

☒ 开启QoS控制 双向

WAN口下行带宽		<input type="text" value="10000"/> Kbps
WAN口上行带宽		<input type="text" value="10000"/> Kbps

索引	级别名称	保留带宽比率
级别 1	E-mail	<input type="text" value="25"/> %
级别 2	HTTP	<input type="text" value="25"/> %
级别 3		<input type="text" value="25"/> %
	其它	<input type="text" value="25"/> %

☒ 启用UDP带宽控制 受限带宽比率  % [在线统计](#)

确定

清除

取消

5. 如果用户使用host to host VPN隧道来连接到总公司。（请参考章节 3 VPN）,他需要设定为这条链接设定一条索引。输入索引 3 的名称。在这个索引中，他可以为VPN隧道保留带宽。



6. 点击**编辑**打开一个新的窗口。首先，选中启用选项。然后，点击**编辑（本地地址）**来设定用户的子网地址。点击**编辑（远端地址）**来设定总公司的子网地址。点击确定。



带宽管理 >> 服务质量 (QoS)

级别索引 #1

名称

号码	状态	本地地址	远端地址	DiffServ CodePoint	服务类型
1	空	-	-	-	-
<div><div>添加</div><div>编辑</div><div>删除</div></div>					

确定

取消

带宽管理 >> 服务质量(QoS)

规则编辑

☒ 启用

本地地址

Any

编辑

远端地址

Any

编辑

DiffServ CodePoint

ANY

服务类型

ANY

注意：

请首先选择/设置 服务类型。

确定

取消

#### 4.4 局域网架设——基于 NAT 功能

下面给一个包含具体设置和部署的范例。Vigor 路由器的默认 IP 地址/子网掩码是 192.168.1.1/255.255.255.0。内置的 DHCP 服务器默认开启，因此它会给每一个通过 NAT 出去的主机都分配一个从 192.168.1.10 开始的同网段 IP（192.168.1.\*）。

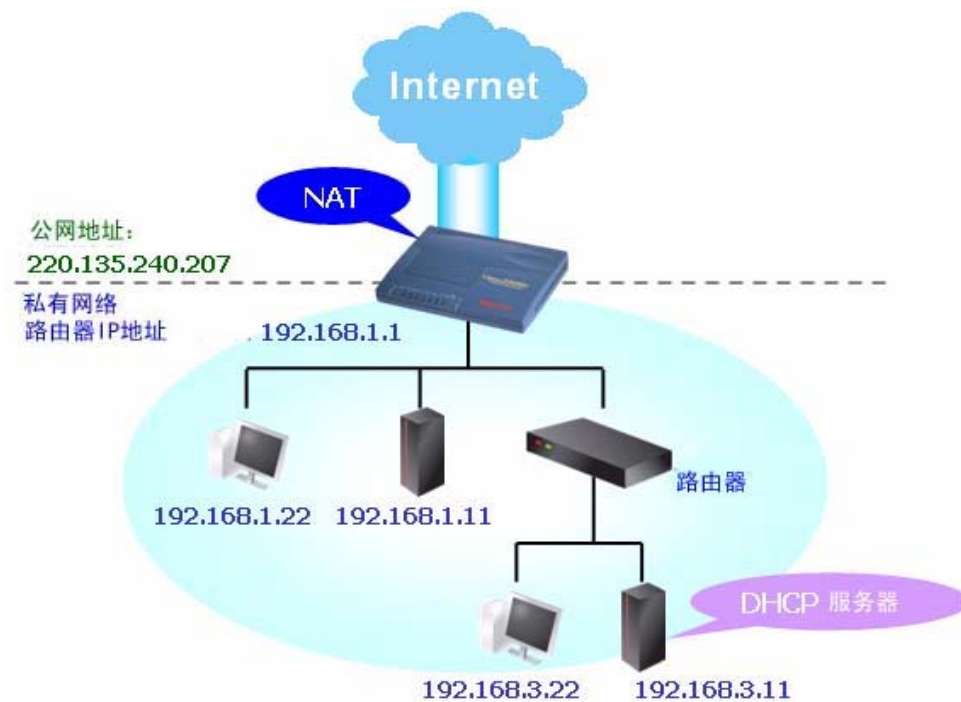


您只需对下面红框中的内容进行配置即可。

LAN >> 基本设定

TCP/IP和DHCP设定	
<b>局域网端IP网络设定</b>	
NAT子网	
路由器第一子网IP地址	192.168.1.1
第一子网掩码	255.255.255.0
路由子网 <input type="radio"/> 启用 <input checked="" type="radio"/> 停用	
路由器第二子网IP地址	192.168.2.1
第二子网掩码	255.255.255.0
<input type="button" value="第二子网DHCP服务器"/>	
RIP协议控制 <input type="button" value="停用"/>	
<b>DHCP服务器设定</b>	
<input checked="" type="radio"/> 启用服务器 <input type="radio"/> 停用服务器	
DHCP 中继代理: <input type="radio"/> 第一子网 <input type="radio"/> 第二子网	
起始IP地址	192.168.1.10
IP池可分配IP数量	50
网关IP地址	192.168.1.1
中继代理使用的DHCP服务器IP地址	
<input type="text"/>	
<b>DNS服务器IP地址</b>	
<input type="checkbox"/> 强制使用设定的DNS	
主DNS IP地址	<input type="text"/>
副DNS IP地址	<input type="text"/>

若网内有其它的 DHCP 服务器，且您不希望使用 Vigor 路由器内置的 DHCP 服务器，那您需要参照下面的网络部署。



然后按照下面红框中的内容进行设置。

LAN >> 基本设定

#### TCP/IP和DHCP设定

##### 局域网端IP网络设定

NAT子网

路由器第一子网IP地址 192.168.1.1

第一子网掩码 255.255.255.0

路由子网 ☐ 启用 ☒ 停用

路由器第二子网IP地址 192.168.2.1

第二子网掩码 255.255.255.0

第二子网DHCP服务器

RIP协议控制 停用

##### DHCP服务器设定

☐ 启用服务器 ☒ 停用服务器

DHCP 中继代理: ☐ 第一子网 ☐ 第二子网

起始IP地址 192.168.1.10

IP池可分配IP数量 50

网关IP地址 192.168.1.1

中继代理使用的DHCP服务器IP地址 192.168.3.11

##### DNS服务器IP地址

☐ 强制使用设定的DNS

主DNS IP地址

副DNS IP地址

确定

## 4.5 VoIP 功能通话方案

### 4.5.1 通过 SIP 服务器

**例 1: John 和 David 使用不同 SIP 服务提供商的 SIP 地址。**

John's SIP URL: 1234@draytel.org, David 的 SIP URL: 4321@iptel.org

#### John 的设定

电话簿索引 1

电话号码: 1111

显示名: David

SIP URL: 4321@iptel.org

#### SIP 帐号设定---

设定档名称: draytel1

注册通过: Auto

端口: 5060 (缺省)

域名: draytel.org

代理: draytel.org

作为通话代理: 未选中

显示名称: John

帐户号/名: 1234

认证 ID: 未选择

密码: \*\*\*\*

过期时间: (使用缺省值)

**编码/RTP/DTMF ---**

(使用缺省值)

#### David 的设定

电话号簿索引 1

电话号码: 2222

显示名: John

SIP URL: 1234@draytel.org

#### SIP 帐户设定---

设定档名称: iptel 1

注册通过: Auto

SIP 端口: 5060(缺省)

域名: iptel.org

代理: iptel.org

作为通话代理: 未选中

显示名: David

帐户名: 4321

认证 ID: 未选择

密码: \*\*\*\*

过期时间: (使用缺省值)

**编码/RTP/DTMF ---**(使用缺省值)

VoIP >> 电话簿设定

电话簿索引 1

<input checked="" type="checkbox"/> 启用	电话号码	1111
	显示名	David
	SIP URL	4321@iptel.org
	备援线路	None
	备用电话号码	

确定 清除 取消

SIP帐户索引值 1

设定档名称	draytel1	(最多11个字符)
注册通过	自动	<input type="checkbox"/> 不注册拨打电话
SIP端口	5060	
域名	draytel.org	(最多63个字符)
代理	draytel.org	(最多63个字符)
<input type="checkbox"/> 作为通话代理		
显示名称	John	(最多23个字符)
帐户号/名	1234	(最多63个字符)
<input type="checkbox"/> 认证 ID		(最多63个字符)
密码	****	(最多63个字符)
过期时间	1小时	3600 秒
NAT穿越支持	无	
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	
振铃模式	1	

确定 取消

#### John 拨打 David ---

拿起电话拨打 1111# (David 在电话号簿里面的号码)

VoIP >> 电话簿设定

电话簿索引 1

<input checked="" type="checkbox"/> 启用	电话号码	2222
	显示名	John
	SIP URL	1234@draytel.org
	备援线路	None
	备用电话号码	

确定 清除 取消

SIP帐户索引值 1

设定档名称	iptel1	(最多11个字符)
注册通过	自动	<input type="checkbox"/> 不注册拨打电话
SIP端口	5060	
域名	iptel.org	(最多63个字符)
代理	iptel.org	(最多63个字符)
<input type="checkbox"/> 作为通话代理		
显示名称	David	(最多23个字符)
帐户号/名	4321	(最多63个字符)
<input type="checkbox"/> 认证 ID		(最多63个字符)
密码	****	(最多63个字符)
过期时间	1小时	3600 秒
NAT穿越支持	无	
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	
振铃模式	1	

确定 取消

#### David 拨打 John

拿起电话拨打 2222# (John 在电话号簿里面的号码)

## 例 2: John 和 David 使用相同 SIP 服务提供商的 SIP 地址。

John's SIP URL: 1234@draytel.org , David 的 SIP URL: 4321@draytel.org

### John 的设定

电话簿索引 1

电话号码: 1111

显示名: David

SIP URL: 4321@draytel.org

### SIP 帐户设定---

设定档名称: draytel 1

注册通过: 自动

SIP 端口: 5060 (缺省值)

域名: draytel.org

代理: draytel.org

作为通话代理: 未选中

显示名: John

帐户号/名: 1234

认证 ID: 未选择

密码: \*\*\*\*

过期时间: (使用缺省值)

### 编码/RTP/DTMF ---

(使用缺省值)

### David 的设定

电话簿索引 1

电话号码: 2222

显示名: John

SIP URL: 1234@draytel.org

### SIP 帐户设定---

设定档名称: draytel 1

注册通过: 自动

SIP 端口: 5060 (缺省值)

域名: draytel.org

代理: draytel.org

作为通话代理: 未选中

显示名: David

帐户号/名: 4321

认证 ID: 未选择

密码: \*\*\*\*

过期时间: (使用缺省值)

### 编码/RTP/DTMF ---

(使用缺省值)

VoIP >> 电话簿设定

电话簿索引 1

<input checked="" type="checkbox"/> 启用	电话号码	1111
	显示名	David
	SIP URL	4321@draytel.org
	备援线路	None
	备用电话号码	

确定 清除 取消

SIP 帐户索引值 1

设定档名称	draytel1 (最多11个字符)
注册通过	自动 <input type="checkbox"/> 不注册拨打电话
SIP 端口	5060
域名	draytel.org (最多63个字符)
代理	draytel.org (最多63个字符)
<input type="checkbox"/> 作为通话代理	
显示名称	John (最多23个字符)
帐户号/名	1234 (最多63个字符)
<input type="checkbox"/> 认证 ID	(最多63个字符)
密码	**** (最多63个字符)
过期时间	1小时 3600 秒
NAT 穿越支持	无
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
振铃模式	1

确定 取消

### John 拨打 David

拿起电话拨打 1111# (David 在电话簿中的号码)  
或者拨打 4321# (David 的帐户名)

VoIP >> 电话簿设定

电话簿索引 1

<input checked="" type="checkbox"/> 启用	电话号码	2222
	显示名	John
	SIP URL	1234@draytel.org
	备援线路	None
	备用电话号码	

确定 清除 取消

VoIP >> SIP 帐户

SIP 帐户索引值 1

设定档名称	draytel1 (最多11个字符)
注册通过	自动 <input type="checkbox"/> 不注册拨打电话
SIP 端口	5060
域名	draytel.org (最多63个字符)
代理	draytel.org (最多63个字符)
<input type="checkbox"/> 作为通话代理	
显示名称	David (最多23个字符)
帐户号/名	4321 (最多63个字符)
<input type="checkbox"/> 认证 ID	(最多63个字符)
密码	**** (最多63个字符)
过期时间	1小时 3600 秒
NAT 穿越支持	无
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
振铃模式	1

确定 取消

### David 拨打 John

拿起电话拨打 2222# (John 在电话簿中的号码) 或者  
拨打 1234# (John 的帐户名)

## 4.5.2 点到点通话

例 3, Arnor 和 Paulin 分别使用 ZTE 路由器, 他们可以不通过 SIP 注册进行通话。首先他们必须获得对方的 IP 地址并且给端口分配一个帐户名。

Arnor 的 SIP URL: 1234@214.61.172.53    Paulin 的 SIP URL: 4321@ 203.69.175.24

### Settings for Arnor 的设置

电话簿索引 1

电话号码: 1111

显示名: paulin

SIP URL: 4321@ 203.69.175.24

VoIP >> 电话簿设定

电话簿索引 1

☒ 启用

电话号码	1111
显示名	paulin
SIP URL	4321 @ 203.69.175.24
备援线路	None
备用电话号码	

### SIP 帐户设定---

设定档名称: Paulin

注册通过: None

SIP 端口: 5060(缺省)

域名: (空白)

代理: (空白)

作为通话代理: 未选中

显示名: Arnor

帐户名: 1234

认证 ID: 未选择

密码: (空白)

过期时间: (使用缺省值)

SIP 帐户索引值 1

设定档名称	Paulin (最多11个字符)
注册通过	无 <input type="checkbox"/> 不注册拨打电话
SIP 端口	5060
域名	(最多63个字符)
代理	(最多63个字符)
<input type="checkbox"/> 作为通话代理	
显示名称	Arnor (最多23个字符)
帐户号/名	1234 (最多63个字符)
<input type="checkbox"/> 认证 ID	(最多63个字符)
密码	(最多63个字符)
过期时间	1小时 3600 秒
NAT 穿越支持	无
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
振铃模式	1

### Arnor 拨打 Paulin

He picks up the phone and dials 1111#. (DialPlan Phone Number for Arnor)拿起电话拨打 1111# (Arnor 在电话簿中的号码)

### 编码/RTP/DTMF ---

(使用缺省值)

### Paulin 的设置

电话簿索引 1

电话号码: 2222

显示名: Arnor

SIP URL: 1234@214.61.172.53

VoIP >> 电话簿设定

电话簿索引 1

☒ 启用

电话号码	2222
显示名	Arnor
SIP URL	1234 @ 214.61.172.53
备援线路	None
备用电话号码	

### SIP 帐户设定---

设定档名称: Arnor

注册通过: None

SIP 端口: 5060(缺省)

域名: (空白)

代理: (空白)

作为通话代理: 未选中

显示名: Paulin

帐户名: 4321

认证 ID: 未选择

密码: (空白)

过期时间: (使用缺省值)

SIP 帐户索引值 1

设定档名称	Arnor (最多11个字符)
注册通过	无 <input type="checkbox"/> 不注册拨打电话
SIP 端口	5060
域名	(最多63个字符)
代理	(最多63个字符)
<input type="checkbox"/> 作为通话代理	
显示名称	Paulin (最多23个字符)
帐户号/名	4321 (最多63个字符)
<input type="checkbox"/> 认证 ID	(最多63个字符)
密码	(最多63个字符)
过期时间	1小时 3600 秒
NAT 穿越支持	无
振铃端口	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
振铃模式	1

### Paulin 拨打 Arnor

拿起电话拨打 2222# (Paulin 在电话簿中的号码)

### 编码/RTP/DTMF ---

(使用缺省值)

## 4.6 升级路由器固件

在升级路由器前，您需要先安装路由器工具。升级工具 **Firmware Upgrade Utility** 就在工具内。

1. 请将附赠的 CD 盘插入您的 CD 光驱。
2. 从页面上找到 **Utility** 菜单并点击它。
3. 在 **Utility** 的页面上，点击现在安装（在 **Syslog** 描述的下方）。

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

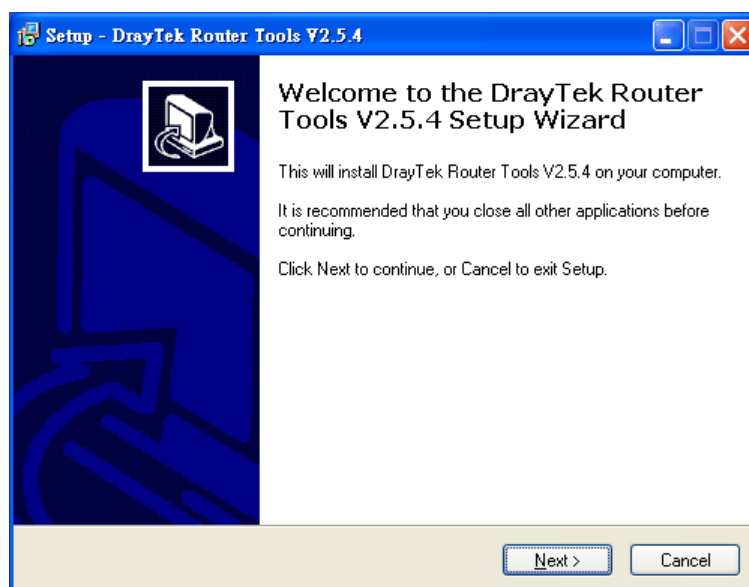
**Install Now!**

4. 您需要将 **RTSxxx.exe** 文件复制到您的电脑上。请记住存放此文件的路径。
5. 请到[www.draytek.com.cn](http://www.draytek.com.cn) 找到路由器的最新固件。
6. 进入**技术支持 >> 相关下载**，找到相关型号的路由器后，点击进入，然后下载固件。另外，您还可以获取 **Vigor** 的路由器工具。

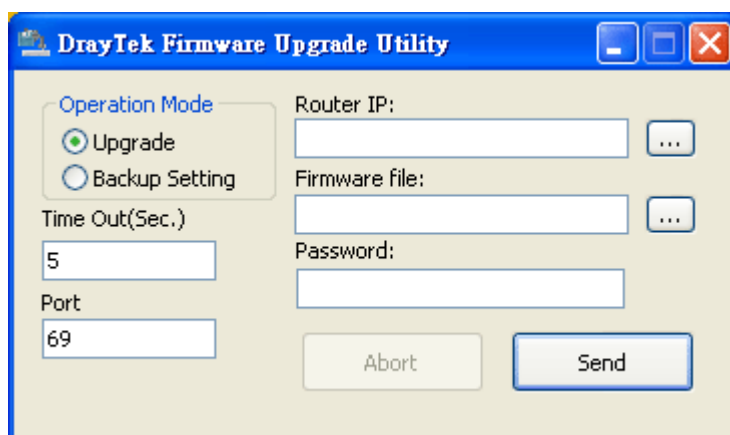
**Note :** [Brief introduction for Tools](#)

Tools of Vigor						
Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	<a href="#">hgx</a>	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	<a href="#">hgx</a>	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	<a href="#">zip</a>	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	<a href="#">zip</a>	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	<a href="#">zip</a>	0.85 MB
LPR	1.0	English	20/06/2005	Windows	<a href="#">zip</a>	0.54 MB
<a href="#">TOP</a>						

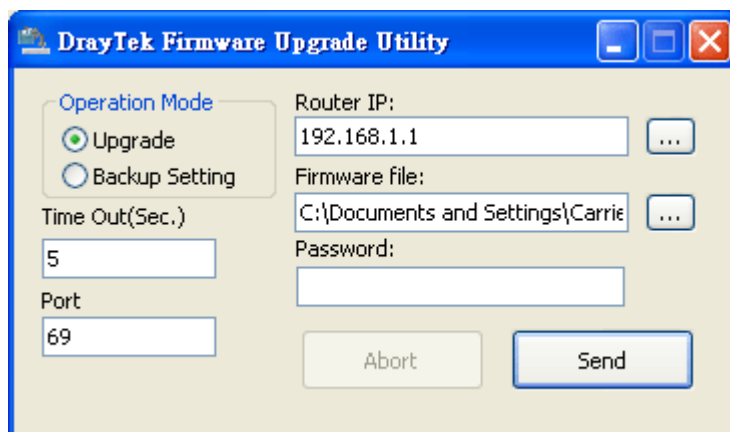
7. 选择与电脑的操作系统相匹配的路由器工具，以及路由器的固件文件，然后下载。
8. 然后解压缩.zip 文件。
9. 双击路由器工具图表，将会出现安装指导。



10. 按照提示页面上的指导进行安装。最后点击**结束**以完成安装。
11. 在 Windows 操作系统里，到**开始**菜单，打开**程序**，然后选择 **Router Tools XXX >> Firmware Upgrade Utility**。

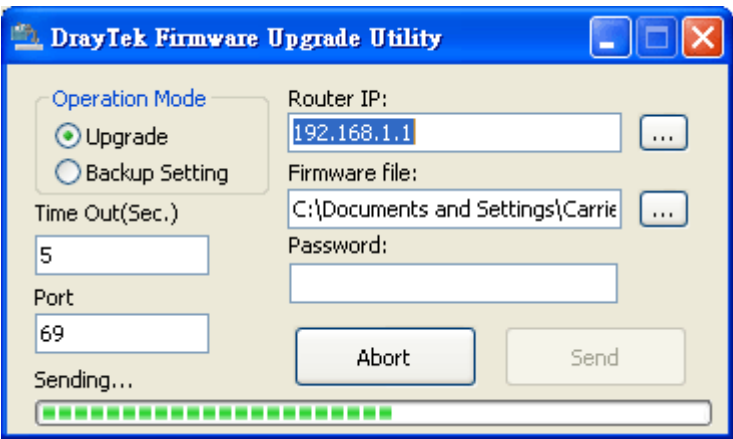


12. 输入您路由器 IP，通常是 192.168.1.1。
13. 点击固件输入框右侧的按钮。找到您在电脑上存放固件的位置。您将发现有两个文件，分别有不同的后缀名**.all**（升级后会保留旧的设置）和**.rst**（升级后会擦除旧的设置）。您可以选择任意一个文件升级。



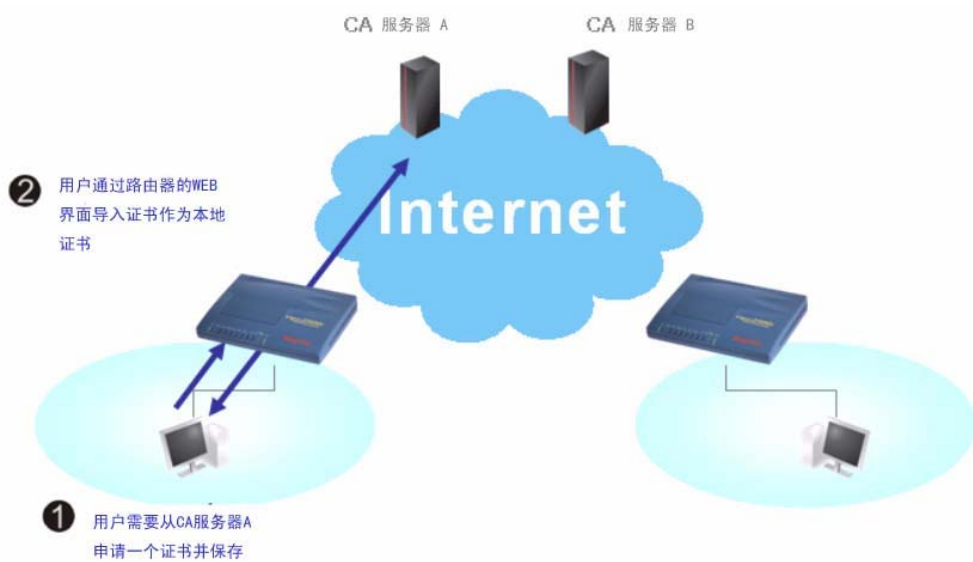


14. 点击 **Send**，升级将如下进行。



15. 耐心等待一段时间，直到升级完成。

### 4.7 从 Windows CA 服务器上申请一个证书



1. 到**证书管理**中，选择**本地证书**。  
**证书管理 >> 本地证书**

**X509本地证书设定**

名称	主题	状态	修改
本地	---	---	<a href="#">查看</a> <a href="#">删除</a>

[生成](#) [导入](#) [刷新](#)

**X509本地证书**

2. 您可以点击**生成**，编辑一个证书请求。请输入证书请求的相关信息。

**可替代识别名称 (Subject Alternative Name)**

类型

IP

---

**识别名称 (subject name)**

国家 (C)

洲 (ST)

区域 (L)

组织 (O)

组织 (OU)

通用名 (CN)

Email (E)

---

**密钥类型**

**密钥大小**

3. 将 X.509 本地证书请求复制并保存为一个文本文件，以备日后之用。

[证书管理](#) >> [本地证书](#)

#### X509本地证书设定

名称	主题	状态	修改
本地	/C=TW/O=Draytek/emailAddress...	Requesting	<input type="button" value="查看"/> <input type="button" value="删除"/>

**X509本地证书请求**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTElMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYX10ZWszIDAe
BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDx8VBWxjbsCzWsxIoQCTTLsjduH7zarKbtL3xcA1eR1qmP81Yj
amv9FwjC3c5APOUm4I/IafNdZyFxbIq3sRM8XbpfmLqYmAx60dkGQNvFaH2yVxP+
dSgTYMsyHg4PrxYMsPwPofXweJ5S6afbbvibfNwx9kM7h5cipD/1koYusQIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANGgtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQBIA3jKgAFiwvbpEqJ6BKacvUxgIrGGINTg1j5Mq+kxtAun
tTwjT+7eCA7f/EAQax6egJeiHs7NIGuDM+8JjZZWU7fK02Da9WKmJ1vgB/dMOT1l
UPM+y/hPVdvwurJrZMdLxt1Z4QkFe1x1FI59RODFr6jk3CgY6TZNkqkFCRb348g==
-----END CERTIFICATE REQUEST-----
```

4. 通过 Web 浏览器连接到 CA 服务器，按照提示提交请求。下面是以 Windows 2000 CA 服务器作为范例。连入 CA 服务器后，请选择**申请证书**，并点**下一步**。

Microsoft 证书服务 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 刷新 搜索 收藏夹 打印 邮件 任务栏 开始

地址(D)  转到 Google

---

Microsoft 证书服务 -- PQA 主页

**欢迎**

您使用此 Web 站点为您的 Web 浏览器，电子邮件客户端，或其它安全程序申请一个证书。一旦您获得一个证书，您将能够安全地向 Web 上的其他人标识您自己，为电子邮件签名，加密电子邮件，以及其它，基于您申请的证书类型。

**选择一个任务：**

- ☐ 检索 CA 证书或证书吊销列表
- ☒ 申请证书
- ☐ 检查挂起的证书

选择 **高级申请**，并点下一步。

Microsoft 证书服务 — PQA 主页

选择申请类型

请选择您要进行的申请类型：

☐ 用户证书申请：

用户证书

☒ 高级申请

下一步 >

选择 **使用 base64 编码的 PKCS #10 文件提交一个证书申请**，或使用 **base64 编码的 PKCS #7 文件更新证书申请**，点下一步。

Microsoft 证书服务 — PQA 主页

高级证书申请

您可以用下列方法之一为您自己，其他用户，或计算机申请一个证书。请注意证书颁发机构 (CA) 的策略将决定您能获得的证书。

☐ 使用表格向这个 CA 提交一个证书申请。

☒ 使用 base64 编码的 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件更新证书申请。

☐ 使用智能卡注册站为代表另一用户的智能卡申请一个证书。  
您必须有一个注册代理证书以为另一用户提交一个申请。

下一步 >

导入 X509 本地证书请求的文本文件，证书模板选择 **Router (离线申请)** 或 **IPSec (离线申请)**。

Microsoft 证书服务 — PQA 主页

提交一个保存的申请

粘贴一个 base64 编码的 PKCS #10 证书申请或由外部应用程序 (如 web 浏览器) 生成的 PKCS #7 更新申请到申请字段以提交一个申请到证书颁发机构 (CA)。

保存的申请：

Base64 编码  
证书申请  
(PKCS #10 或 #7):

-----BEGIN CERTIFICATE REQUEST-----  
MIIB1cCAQACAQAwLjELMAkGA1UEBhMCQ04xHzAd  
ZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD  
vFRgxGsuFBHhVvhSY/1G3OLfclfaUscVzLQP=4y34  
QKacYn8LiYmXNUNWCIQHyrDwMLvCk16EXXwPw5A  
XeLrNfmVxz7Ih1AeUREwXe4pCN5ctb6/AgMBAAGg  
-----

浏览 要插入的文件。

证书模板：

用户

附加属性：

属性：

提交 >

这样就完成了请求，然后服务器会发行一个证书给您。选择 **Base 64 编码** 证书，并**下载 CA 证书**。您就会得到一个证书 (.cer 文件)，请将它保存在电脑上。

5. 回到 Vigor 路由器上，进入**本地证书**。点击**导入**，再浏览找到那个证书 (.cer 文件)，然后导入到 Vigor 路由器。

恭喜！  
可信CA证书导入成功

请点击 

返回

 查看证书。

Vigor2910 系列中文手册

205

- 完成后点击**刷新**，您将看到以下窗口显示“-----BEGIN CERTIFICATE-----.....”  
**证书管理 >> 本地证书**

#### X509本地证书设定

名称	主题	状态	修改
本地	/C=TW/O=Draytek/emailAddress...	Requesting	<a href="#">查看</a> <a href="#">删除</a>

生成 导入 刷新

**X509本地证书请求**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTElMAkGA1UEBhMCVFcxEDAOBgNVBAoTB0RyYX10ZWsxIDAe
BgkqhkiG9w0BCQEWEWEXByZXNzQG9yYX10ZWsxIDAeMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDx8VBWxjbsCzWsxIoQCTTLsjduH7zarKBtL3xcAleRlqmP81Yj
amv9FwjC3c5APOUm4I/IafNdZyFxbIq3sRM8XbpfmLqYmAx60dkGQNVFaH2yVxP+
dSgTYMsyHg4PrxYMsPwPofXweJ5S6afbbvibfNwx9kM7h5cipD/1koYusQIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANGgtkcmF5dGVrLmNvbTANBgkq
hkiG9w0BAQUFAAOBgQBIA3jKgAFiwvbpEqJ6BKacvUxgIrGGINTg1j5Mq+kxtAun
tTwjT+7eCA7f/EAQax6egJeiHs7NIGuDm+8JjZZWU7fK02Da9WKmJ1vgB/dM0T11
UPM+y/hPVdwurJrZMdLxt1Z4QkFe1x1FI59R0DFr6jk3CgY6TZNkqkFCRb348g==
-----END CERTIFICATE REQUEST-----
```

- 点击**查看**按钮可以再次查看证书的详细信息。

http://172.17.1.11 - 证书请求信息 - Microsoft Internet Explorer

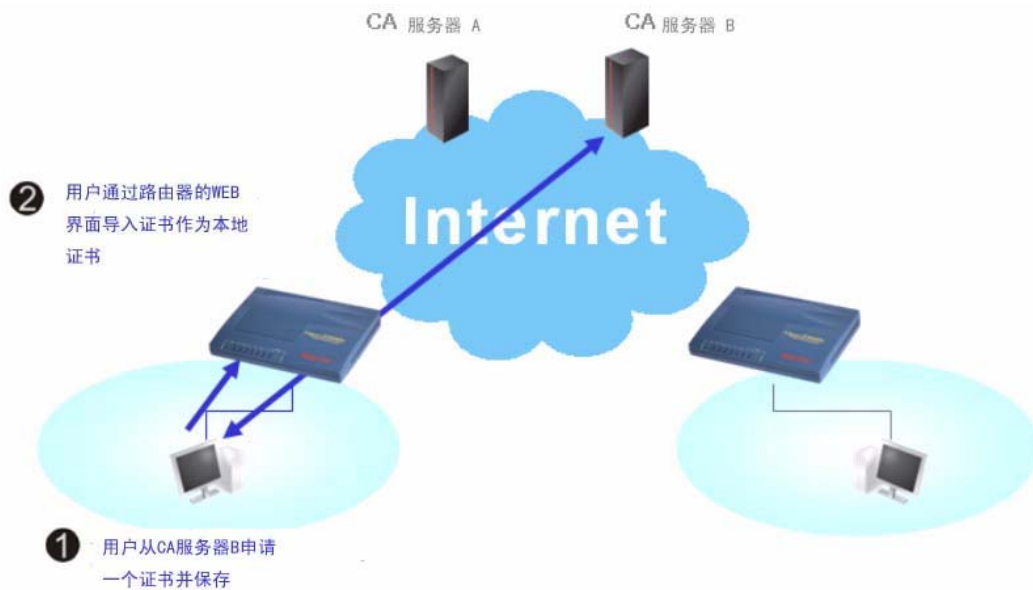
**证书请求信息**

名称:	本地
签发机构:	
主题 (Subject):	/C=TW/O=Draytek/emailAddress=press@draytek.com
主题可替代识别名称 (Subject Alternative Name):	DNS:draytek.com
有效自:	
有效至:	

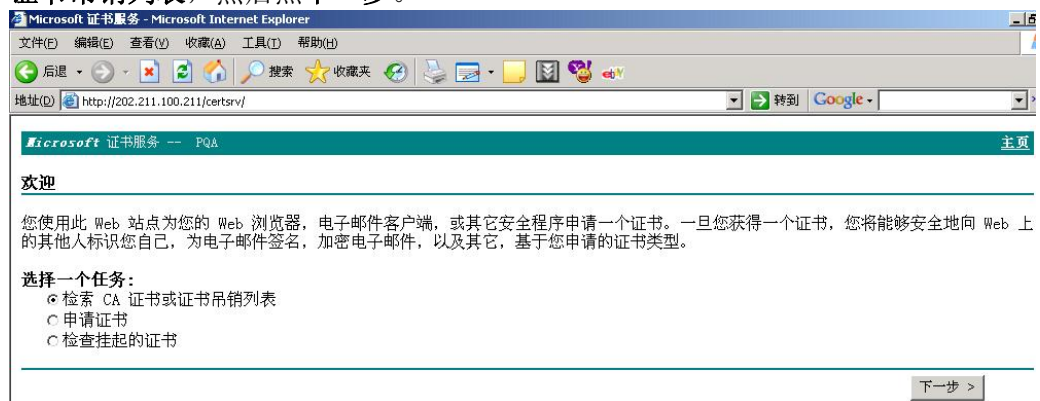
关闭

Done Internet

## 4.8 申请一个证书然后设置为 Windows CA 服务器上的可信证书



1. 通过 Web 浏览器连接到您想获取 CA 证书的 CA 服务器，点击 **检索 CA 证书或证书吊销列表**，然后点下一步。



2. 在 **选择要下载的文件** 中，选择 CA 证书当前以及 **Base 64 编码**，并点击下载 CA 证书，以保存.cer 文件。



3. 回到 Vigor 路由器，进入**可信 CA 证书**，点击**导入**，浏览找到那个证书（.cer 文件）并将其导入 Vigor 路由器。完成后点击**刷新**，您将看到以下图示。

证书管理 >> 可信CA证书

**X509可信CA证书设定**

名称	主题	状态	修改	
可信CA-1	/emailAddress=pqa@draytek.co...	OK	查看	删除
可信CA-2	---	---	查看	删除
可信CA-3	---	---	查看	删除

导入 刷新

4. 点击**查看**按键可以再次查看证书的详细信息。

**证书详细信息**

证书名:	可信CA-1
签发机构:	/C=US/CN=vigor
主题(Subject):	/C=US/CN=vigor
可替代识别名称 (Subject Alternative Name) :	DNS: draytek.com
有效自:	Aug 30 23:08:43 2005 GMT
有效至:	Aug 30 23:17:47 2007 GMT

关闭

**注释:** 在设置证书设定前，请先到**系统维护>>时间和日期**配置路由器当前的时间。

# 5

## 故障排查

这个章节将会指导您如何解决在完成安装和设置路由器后依然无法上网的问题。请按以下方法一步一步地进行检查。

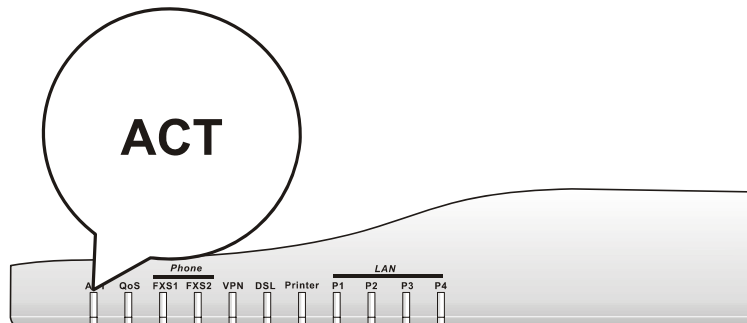
- 检查路由器硬件状态是否正常
- 检查您电脑的网络连接设置是否正确
- 试试看能否从电脑 ping 到路由器
- 检查 ISP 的设置是否正常
- 必要的话将路由器恢复至默认出厂设置

如果以上步骤仍无法解决您的问题，您需要联系代理商获取进一步的帮助了。

### 5.1 检查路由器硬件状态是否正常

按以下步骤检查硬件状态

1. 检查电源线以及 WAN/LAN 的连接。详细信息请参考“**1.2 章节 硬件安装**”。
2. 开启路由器，确认 **ACT** 指示灯差不多每秒闪烁一次，以及相应的 **LAN** 指示灯是否亮着。



3. 如果没有，意味着路由器的硬件有问题。那么请回到“**1.2 章节 硬件安装**”，再重新执行一次硬件安装，然后再试试。

### 5.2 检查您电脑的网络连接设置是否正常

有些时候无法上网是由错误的网络连接设置造成的。若在尝试过上面的方法，连接依然失败，请按以下步骤确认网络连接是否正常。

## 对于 Windows 系统



我们以 Windows XP 系统为例。

对于其它操作系统，请到[www.draytek.com.cn](http://www.draytek.com.cn) 上参考相关技术文件的步骤。

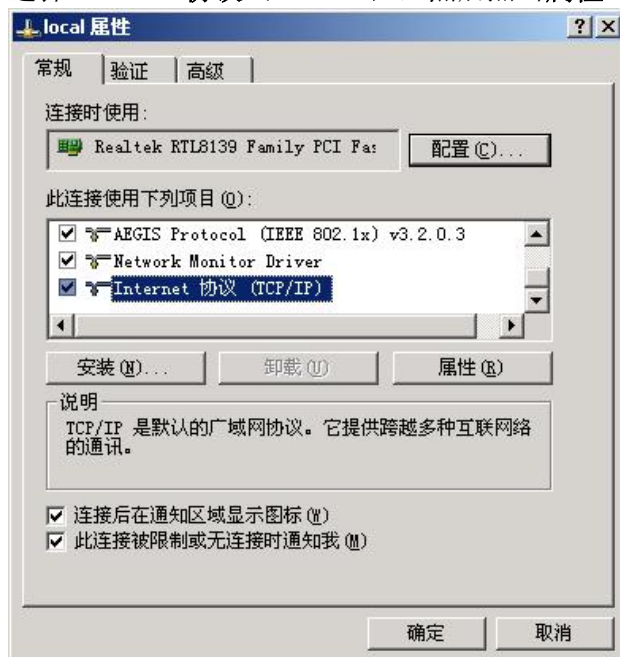
1. 到**控制面板**中，双击**网络连接**。



2. 右键点击**本地连接**图标，然后点击**属性**。

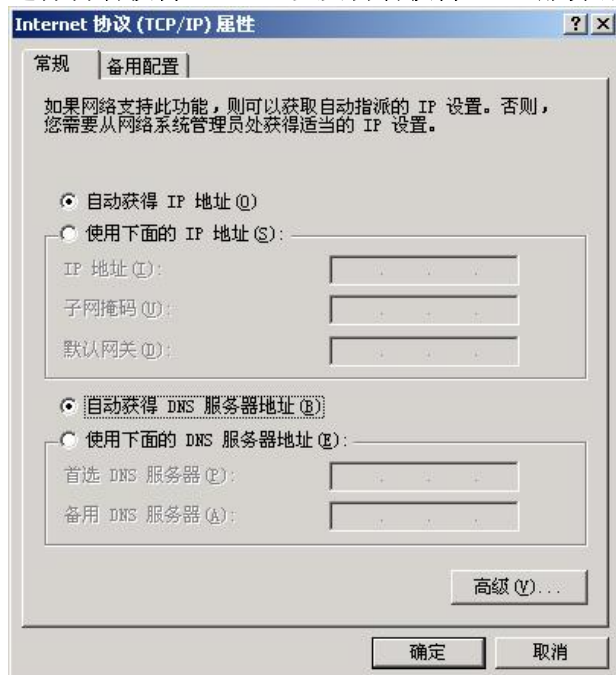


3. 选择 **Internet 协议 (TCP/IP)**，然后点击**属性**。



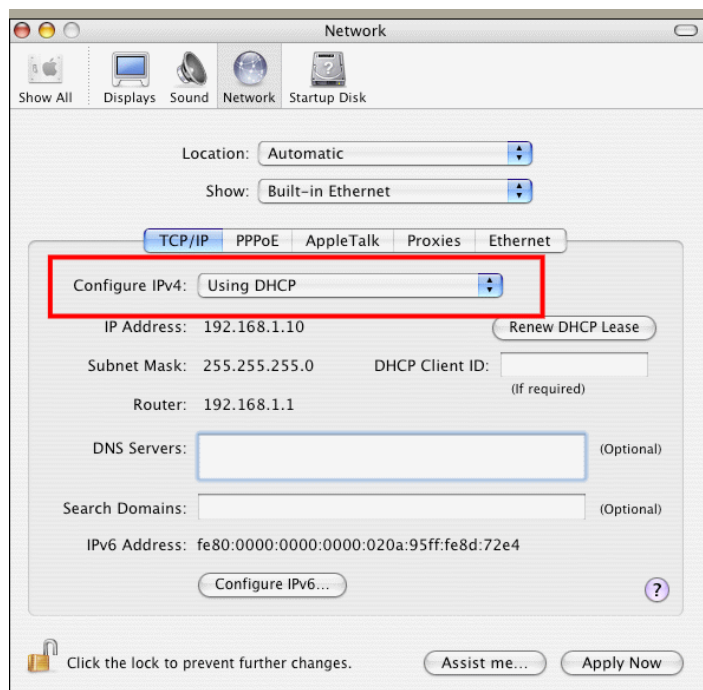


4. 选择自动获得 IP 地址以及自动获得 DNS 服务器地址。



### 对于 Mac 系统

1. 双击当前使用的 Mac 系统。
2. 打开应用，然后进入网络。
3. 在**网络**页面上，在**设置 IPv4**的下拉菜单中选择**使用 DHCP**。



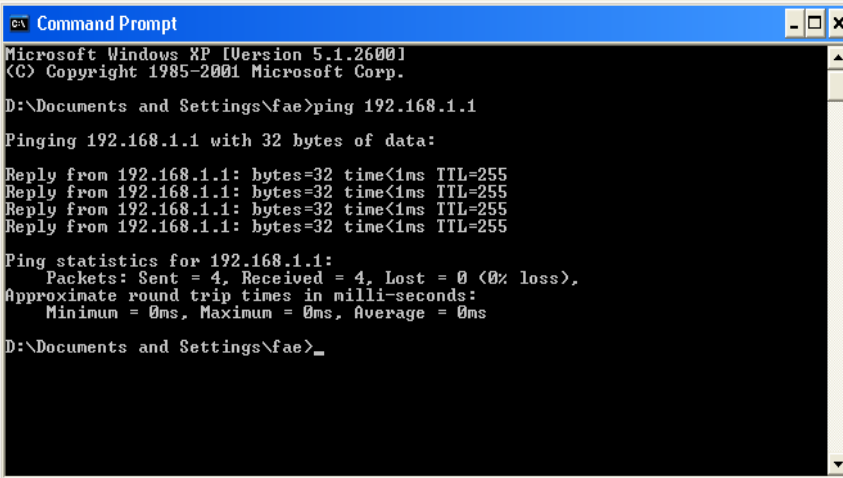
## 5.3 在您电脑 Ping 路由器

路由器的默认 IP 地址是 192.168.1.1。您可以使用“ping”命令检查到路由器的连接状态。最重要的是要看电脑是否可以收到从 **192.168.1.1** 返回的响应。若没有，请检查您电脑的 IP 地址是多少。我们建议您将网络连接设置为**自动获得 IP 地址**。（请参考 5.2 章节）

请按以下步骤 ping 路由器。

### 对于 Windows 系统

1. 打开**命令提示窗口**（开始 > 运行）。
2. 输入 **command** (Windows 95/98/ME 系统)或 **cmd** (Windows NT/ 2000/XP 系统)。将会出现 DOS 界面的对话框。



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

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

D:\Documents and Settings\fae>_
```

3. 输入 **ping 192.168.1.1** 然后回车。若是连接没有问题，将会有“**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**”消息出现。
4. 若回应消息没有出现，请检查您电脑的 IP 地址设置。

### 对于 Mac 系统（终端）

1. 双击当前使用的 Mac 系统。
2. 打开**应用文件夹**，进入**工具**。
3. 双击**终端**，将会弹出终端窗口。
4. 输入 **ping 192.168.1.1** 然后回车。若是连接没有问题，将返回“**64 bytes from 192.168.1.1: icmp\_seq=0 ttl=255 time=xxxx ms**”消息。

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

# 5.4 检查 ISP 设定是否正确

点击 **Internet 接入**，然后检查 ISP 设置是否正确。

WAN >> Internet接入

## Internet接入

索引	显示名称	物理模式	接入模式	
WAN1		Ethernet	静态或动态IP	详情页面
WAN2		Ethernet	无	详情页面

无

无

PPPoE

静态或动态IP

PPTP

## 对于 PPPoE 用户

1. 检查 PPPoE 是否已启用。
2. 检查您是否正确地输入了 **ISP** 提供给您的用户名和密码。

WAN >> Internet接入

### WAN 1

PPPoE客户端模式

☒ 启用 ☐ 禁用

ISP接入设置

用户名

密码

索引 (1-15) 计划任务 设定:

=> , , ,

ISDN拨号备份设置

拨号备份设置

无

PPP/MP设定

PPP验证

PAP或CHAP

闲置超时

-1 秒

IP地址分配方法 (IPCP)

WAN IP别名

固定IP: ☐ 是 ☒ 否 (动态IP)

固定IP地址

☒ 默认MAC地址

☐ 指定一个MAC地址

MAC地址:

00 . 50 . 7F . 33 . 31 . ED

确定

取消

## 对于静态 IP/DHCP 用户

1. 检查宽带接入是否已启用。
2. 若您选择了指定 IP 地址，请检查 IP 地址、子网掩码和网关 IP 地址是否正确（一定要与您的 ISP 确认相关设置）。

## WAN 1

## 静态或动态IP (DHCP客户端)

☒ 启用 ☐ 禁用

## ISDN拨号备份设置

拨号备份模式

无

## 保持WAN连接

☐ 启用PING保持在线

PING IP

PING间隔

0 分钟

## RIP协议

☐ 启用RIP

## WAN IP网络设置

WAN IP别名

☐ 自动获取IP地址

路由器名

域名

\* : 某些ISP需要

☒ 指定一个IP地址

IP地址

172.17.1.11

子网掩码

255.255.255.0

网关IP地址

172.17.1.3

☒ 默认MAC地址

☐ 指定一个MAC地址

MAC地址:

00 . 50 . 7F : 33 . 31 . ED

## DNS服务器IP地址

首选IP地址

备用IP地址

确定

取消

## 5.5 如果必要将路由器恢复至默认出厂设置

有些时候, 恢复路由器至默认出厂设置可以解决错误设置导致的连接失败。请尝试软件或硬件重置路由器。



**警告:** 在按下使用出厂默认设定后, 您将失去您所有的旧设定。请确认您在确定前记下了重要的设定。重启后的密码为空。

## 软件重置

您可以在路由器的 web 界面直接将它回复至出厂默认设置。

到 Web 界面上的**系统管理>>重启系统**, 点击**重启系统**, 然后会到下图界面。选择**使用出厂默认设定**, 并点击**确定**。

## 系统管理 &gt;&gt; 重启系统

## 重启系统

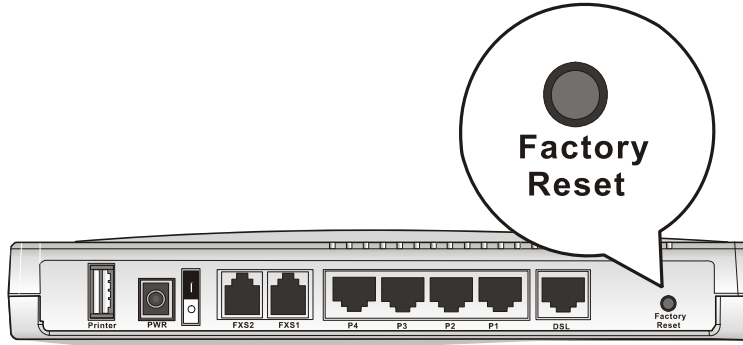
## 您想重新启动路由器吗?

- ☒ 使用当前设置  
☐ 使用出厂默认设定

确定

## 硬件重置

当路由器电源开启的时候（ACT 指示灯正在闪烁），按下 **RST** 键，并保持 5 秒钟。当您看到 **ACT** 指示等开始快速闪烁时，再放开 **RST** 键。然后路由器就会恢复到出厂默认设定了。



恢复至默认出厂设定后，您就可以按个人需要重新配置路由器了。

## 5.6 联系代理商

若经过大量尝试，网络仍然无法正常工作，请联系您的代理商以获得进一步的帮助。或者，您还可以发送电子邮件到[support@draytek.com](mailto:support@draytek.com) 或登录<http://www.draytek.com.cn>在线提出您的问题。