SMC Networks

SMCBR14VPN
Barricade™
4端口VPN有线宽带路由器

USER GUIDE

SMC(中国)

Barricade™

4 端口 VPN 有线宽带路由器

用户手册

SMCBR14VPN 4 端口 VPN 有线宽带路由器

Barricade™系列 SMCBR14VPN 用户手册

SMC 公司为客户提供全方位的技术支持，用户可与就近的 SMC 办事处或客户服务中心联系，也可直接与公司总部联系。

SMC 网络（中国）公司

地址：上海市虹漕路 421 号 63 号楼 1 楼

邮编：200233

网址：http://www.smc-prc.com

客户服务电话：8008206000

客户服务传真：021-64957924

客户服务邮箱：support@smc-prc.com

声明

目 录

第1章 系统需求

- 需要您的电话公司或网络服务提供商（ISP）为您提供 Internet 接入服务提供，可以通过 DSL modem,cable modem, Dial-up modem 或 ISDN modem。
- 一台使用固定 IP 地址或通过 DHCP 动态获得 IP 地址的计算机，以及由您的网络服务提供商分配给您的网关服务器地址和 DNS 服务器地址。
- 安装有 10/100Mbps 网卡或 USB 到 RJ45 端口的转接卡的计算机
- 在每台需要访问 Internet 的计算机上安装有 TCP/IP 网络协议
- 支持 Java 的网络浏览器，诸如 Microsoft IE 5.0 或以上版本，或者 Netscape communicator 4.0 或以上版本。

第2章 设备清单

当您第一次打开Barricade™ VPN宽带路由器的外包装时，请仔细检查是否包含有如下物品：

- 1 台Barricade™ VPN Cable/DSL 宽带路由器 SMCBR14VPN
- 1 张包含有 EZ 安装向导和用户手册的 CD
- 1 根 5 类线
- 1 个电源变压器
- 1 份快速安装手册

如果您发现原包装中缺少上述任何一样，请立即与当地 SMC 经销商联系，请保存原包装，用来退回有缺损的产品。

请您到SMC网上注册中心注册您的产品，以获得最好的售后服务。http://www.smc-prc.com

第3章 特性和功能

宽带调制解调器和 NAT 路由器	连接多台计算机到您的宽带路由器上，或以太网路由器以访问 Internet。
10/100Mbps 以太网接口	提供一个 10/100 Base-TX 接口连接 DSL 或 Cable modem，以提供 Internet 访问接入
自适应交换端口	内置有 4 个 10/100Mbps 自适应交换端口
支持 VPN	支持多条 IPSec 通道，内建 PPTP 和 L2TP VPN 服务器
防火墙功能	所有未知包都将被屏蔽，以保护您的内部局域网。
支持 DHCP 服务器	所有连接到此设备的计算机都可以获得 IP 地址
基于 WEB 的配置界面	使用任何一台连到宽带路由器的计算机上的 IE 浏览器，都可以对它进行管理
支持网络过滤功能	包过滤功能使您通过分析进来或出去的包，控制网络的访问；这是基于 IP 地址来实现的
支持通用即插即用	使计算机，路由器，打印机等设备可以随时

	插拔，并保证其被自动识别
支持虚拟服务器	使您网内的网页，FTP 网页和其他服务可以被网外的 Internet 用户访问。
支持 DMZ 主机	使一台计算机可以完全访问到 Internet。
支持 SNMP	SNMP（简单网络管理协议）使远程用户通过设置终端数值来管理、监控网络。
支持系统时间	使您与网络时间服务器同步时间
支持虚拟计算机	使您设置一一对应的 Global 和本地 IP 地址
支持 URL 过滤	通过简单地输入网站关键字，屏蔽掉上百个网页连接
日程表规则	为不同的服务设置不同的时间日程规则

第4章 面板图

下图显示了面板的外观图，接下来的表格则描述了不同状态下 LED 的显示。

前面板图：

LED	功能	颜色	状态	描述
Power	电源指示灯	绿	长亮	表示这个设备已被加电

M1	系统状态指示灯	橙色	闪烁	M1 每秒闪一次，表示系统有电
WAN	WAN 端口的活动	绿	长亮	WAN 端口已连接
			闪烁	WAN 端口正在发送或接收数据
Link/Act 1-4	连接状态	绿	长亮	有以太网设备连接到相应的端口上。
			闪烁	相应的 LAN 端口正在发送或接收数据
Speed 10/100	数据速率	绿	长亮	数据正以 100Mbps 传输

后面板图：4LAN，1WAN，1COM 口

端口类型	描述

5 VDC	变压器（5VDC，2A）
WAN	这个端口与 Cable 或 DSL modem 的 WAN 口相连
Port 1-4	这些端口可与交换机或计算机直接连接
COM	串口（可连接 console 控制台）

第5章 硬件安装

路由器可以放置在您办公室或家里的任何地方，没有特别要注意的地方。然而，您还是要注意以下几点：

- 将路由器放置在平整的台面上
- 将路由器远离热源
- 避免灰尘多的，潮湿的地方

(1) 安装 LAN 连接：将网线的一头和您计算机上的所安装的网卡连接，一头和路由器上的 LAN 端口连接；

(2) 安装 WAN 连接： 将网线的一头与路由器后面板上 WAN 口连接，另一头与 Cable/DSL modem 相连。您也可以连接到一个 56k modem 上作为备用连接。

(3) 加电：当为路由器加电后，路由器会自动进行一次自检。当它在自检的时候，M1 指示灯会亮 5 秒钟来检测连接；接着 M1 指示灯将闪烁 2 次，表示自检工作完成。当自检结束后，M1 指示灯每秒闪一次，表示路由器正常工作。

第6章 网络设置和软件安装

默认设置	
IP 地址	192.168.2.1
子网掩码	255.255.255.0
管理者密码	smcadmin
用户密码	smcadmin

您必须首先确认 TCP/IP 协议已正确安装，并且已将计算机设置成 DHCP 自动获得 IP 地址。

6.1 安装 TCP/IP

6.1.1 Windows 95/98/Me

1. 点击开始/设置/控制面板；

2. 双击网络图标，在弹出的网络窗口中，选择配置页；

3. 点击 添加 按钮；

4. 双击 协议

5. 在制造商列表中，选择 Microsoft。在网络协议列表中选择 TCP/IP，点击 OK 按钮，返回到上一级网络窗口中。

6. TCP/IP 协议将会在网络窗口列表中显示

7. 点击 OK。操作系统可能会提示您重新启动。点击是，机器将会自动重启。

6.1.2 Windows 2000/XP

1. 点击开始/设置/网络和拨号连接

2. 双击 局域网连接，在常规页上点击属性按钮

3. 点击安装按钮

4. 双击协议

5. 选择网络协议（TCP/IP）， 点击 OK 返回到上一级网络窗口

6. TCP/IP 协议将会在网络窗口中被列出，点击 OK 完成整个安装过程。

第7章 配置您的 VPN 宽带路由器

在您准备登录到基于 web 的管理者界面时，请确认以下几点：

1. 您的浏览器配置正确

2. 禁用防火墙或任何正在运行的安全软件

3. 确认您所连接到的路由器的相应端口的指示灯显示正确。如果相应的指示灯没有亮，您需要换另外的线缆知道连接完好。

WEB 管理

要访问到路由器的管理界面，在您的web浏览器中输入IP地址：http://192.168.2.1

注意： 此款路由器有两个不同的 web 用户界面，一个是一般用户所看到的，另一个是系统管理者看到的。要以管理者身份登录，输入系

统密码(默认是 smcadmin)， 点击 Login 按钮。如果您正确得输入了密码，WEB 用户界面上的左面会改变为管理者配置。

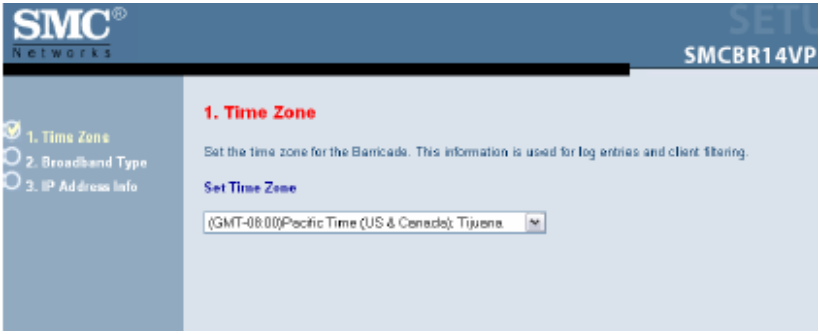
7.1 安装向导

7.1.1 Time Zone 时区设置

登录到 web 管理界面后， 点击 SETUP WIZARD 安装向导。

其中，第一项就是关于时区的设置。这项设置关系到路由器中一些过滤日程表的时间和日志事件的时间。 在下拉菜单中选择您所在的正确的时区。

如果您在中国大陆使用此路由器，请选择（GMT +08:00）时区，即北京时间。

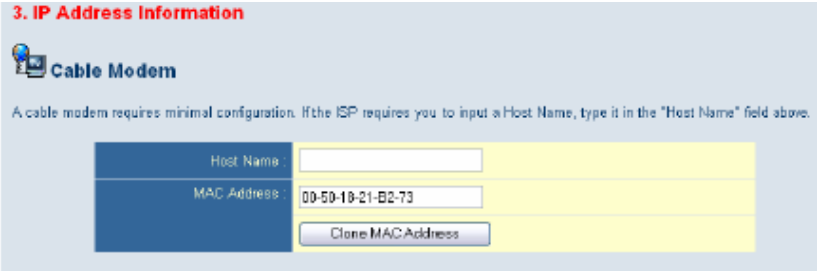


7.1.2 Broadband Type 宽带类型

下面的页面让您选择一个 WAN 类型。选择其一，并点击【Next】。

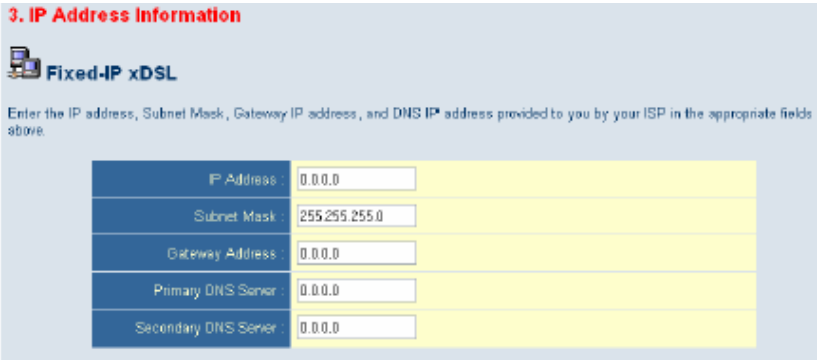
1. Cable Modem

选择 Cable Modem 选项要求您配置一个主机名和 MAC 地址。主机名是可选的，但有些 ISP 也必需这项设置。默认的 MAC 地址是这台宽带路由器的 WAN 口的 MAC 地址。当要注册到 Internet 服务器的时候需要这个 MAC 地址，不要随意改变它，除非您的 ISP 要求。如果您的 ISP Internet 服务提供商需要用连接到计算机的网卡的 MAC 地址作为您第一次登录到 Internet 的认证条件，您就应该在宽带路由器上只连接您的这台电脑，然后点击“Clone MAC Address”绑定 MAC 地址按钮，将网卡上的 MAC 地址复制到这个地方。如果您已经记不清楚到底哪台电脑的 MAC 地址被绑定在宽带公司，您可以和宽带技术人员联系，要求注册一个新的 MAC 地址。



2. Fixed-IP xDSL 固定 IP 地址

有些 xDSL 服务提供商可能会分配一个固定的 IP 地址给用户。如果您的宽带类型是这样的，请选择这个选项，输入分配到的 IP 得之，网关 IP 地址,DNS IP 地址和子网掩码。



3. PPPoE xDSL PPPoE 拨号

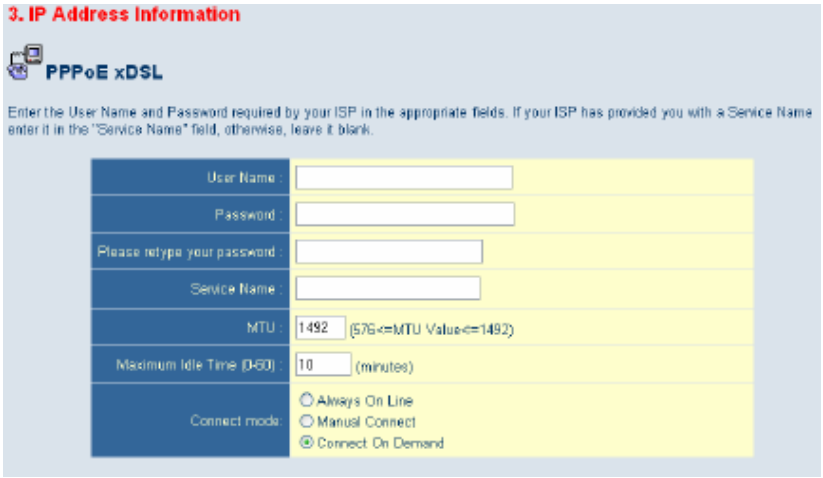
在这里输入您的服务提供商提供给您的用户名和密码。服务名一般是可选的，但有些服务提供商也会提供。将最大传输单位（MTU）设置为默认值，除非您有一个特定的原因要将之改变。最大空余超时时间（Maximum Idle Time）定义了 Internet 连接的最大空闲时间，一旦超过这个时间没有 Internet 连接需求，路由器将自动断线，以分钟计算。（默认：10）。

连接模式：

1) Always on line：永远在线。适用于包月制用户；

2) Manual Connect：手动连接。当您的网络断线后，一定要重新点击“Status”页面中的“Connect”连接按钮后，才能再次上网。适用于包时用户。

3) Connect on demand：按需连接。当您的网络断线后，任何上网的操作都将激活网络连接。



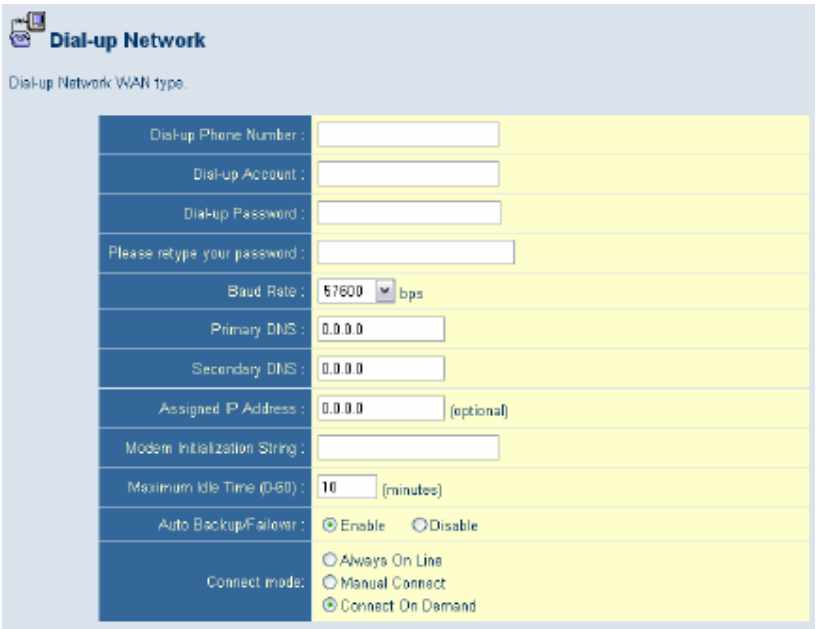
4. Bigpond

5. L2TP

这两种宽带连接方式，在中国大陆地区还没有运营商支持，所以在此掠过。

6. Dian-Up 拨号

大部分拨号用户都将选择这个选项利用一个拨号 modem 连接到 Internet 服务提供商。它是一个备用措施，用于在宽带接入不成功的时候。输入电话号码，由 ISP 提供的用户名，密码。Baud rate 波特率是宽带路由器和您的 modem 之间的数据传输速率。如果您的 ISP 给您提供了 DNS IP 地址，要在这里输入，否则就保持它的默认设置。它的连接方式选择，与 PPPoE xDSL 里的设置一样。



7.2 Advanced Setup 高级设置－SYSTEM 系统

7.2.1 Time Zone 时区设置

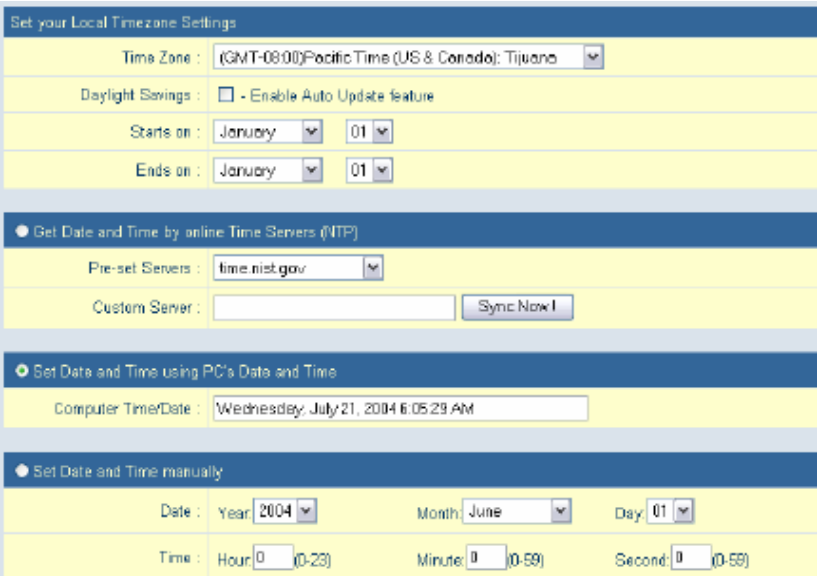
为这台宽带路由器设置时区和时间校对服务器。

- 设置当地时区

在下拉菜单中选择您所在的时区，如果当地有夏令时，就输入开始和结束的夏令时设置。

为了能自动更新路由器的时间，您也可以选择一个时间服务器来同步时间。

- 在线获得时间和日期
- 用 PC 上的时间来设置时间和日期
- 手动设置时间。



7.2.2 Password settings 密码设置

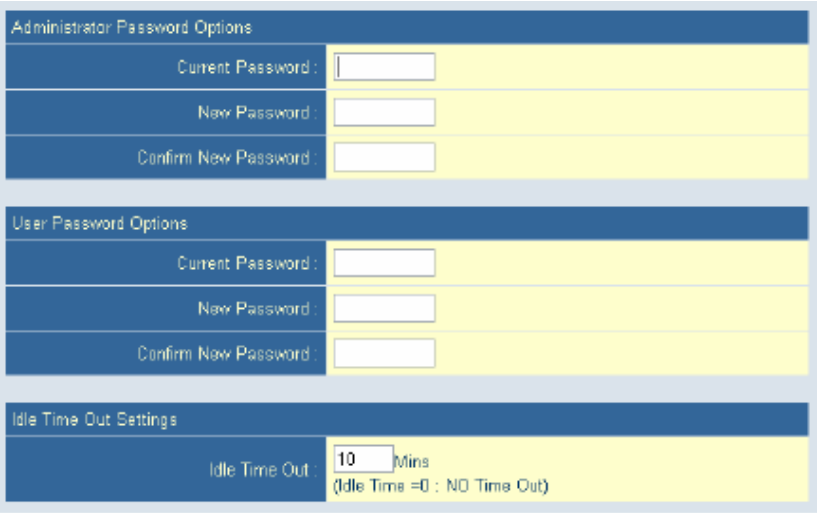
在这里，您可以配置这台宽带路由器的 2 组密码以及超时时间。这台宽带路由器有 2 个级别的管理权限。

管理者帐户有读写权限来查看或改变任何设置。它的默认密码为：smcadmin。

普通用户帐户只有读的权限来查看，但不能改变任何设置。它的默认密码是： password。

如果您之前设置的密码因某种原因遗忘了，可以通过路由器后面板上的 Reset 按钮恢复到出厂设置值。（按住 Reset 按钮至少 5 秒钟）。

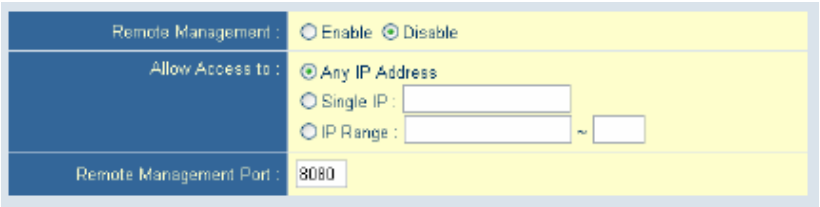
输入最大 Idle 时间（以分钟计），定义管理者访问宽带路由器的管理界面时最大的 Idle 时间。如果超过了您所定义的 Idle 时间，将会自动退出管理者界面，您必须重新登录。（默认时间：10 分钟）



7.2.3 Remote Management 远程管理

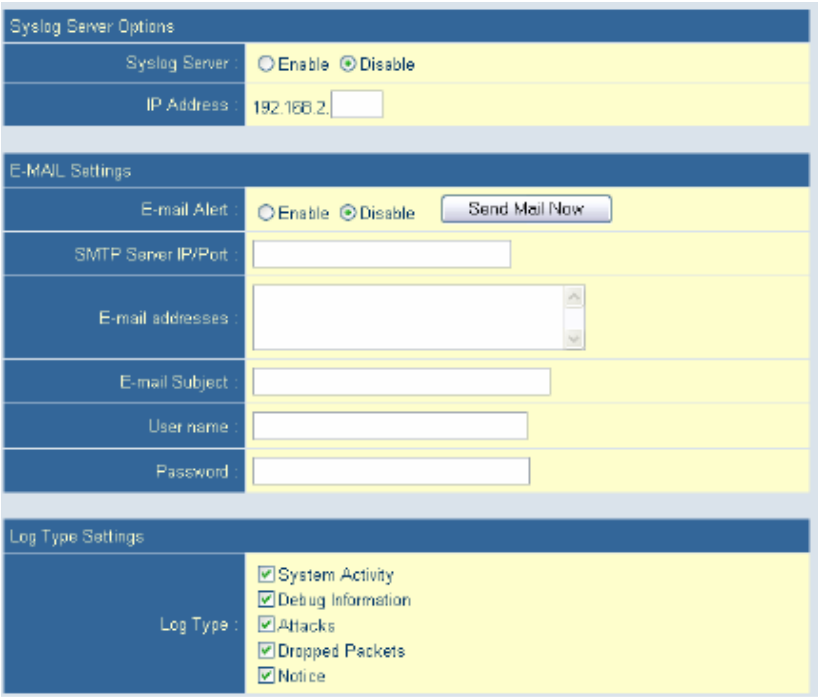
远程管理功能允许一台远程的 PC 通过 Internet 管理配置这台宽带路由器。勾选“Enable”项并且设置那台可管理的远程主机，点击

“Apply”。如果 IP 地址设置为 0.0.0.0，则表示任何在 Internet 上的计算机都可连接到这台路由器进行访问或管理。（默认设置为：Disable，即此功能禁用）



7.2.4 Syslog Server 日志服务器

宽带路由器将日志文件自动存放到这个页面里指定的 IP 地址的 PC 上。输入 LAN IP 地址并选择启用这个功能。 这款宽带路由器还允许您的 log 文件发送到您指定的 Email 地址。（默认设置为：disable，即默认情况下，将不保存这些日志文件。）

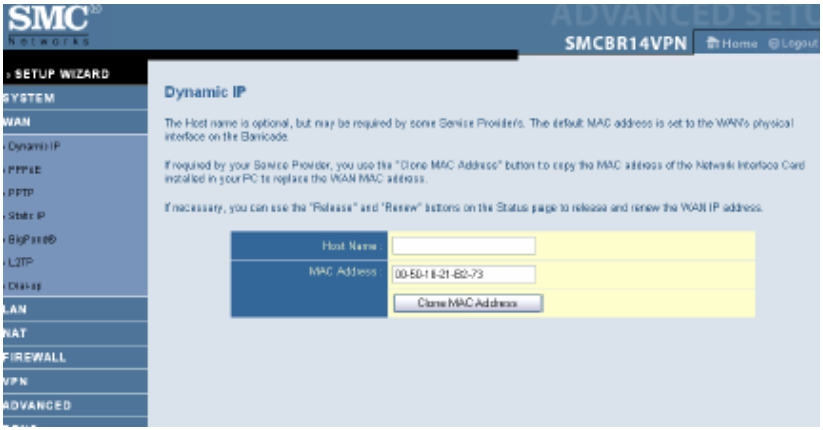


7.3 Advanced Setup 高级设置－WAN 广域网

7.3.1 Dynamic IP 动态 IP

此选项要求您配置一个主机名和 MAC 地址。主机名是可选的，但有些 ISP 也必需这项设置。默认的 MAC 地址是这台宽带路由器的 WAN 口的 MAC 地址。当要注册到 Internet 服务器的时候需要这个 MAC 地址，不要随意改变它，除非您的 ISP 要求。如果您的 ISP Internet 服务提供商需要用连接到计算机的网卡的 MAC 地址作为您第一次登录到 Internet 的认证条件，您就应该在宽带路由器上只连接您的这台电脑，然后点击“Clone MAC Address”绑定 MAC 地址按钮，将网卡上的 MAC 地址复制到这个地方。如果您已经记不清楚到底哪台电脑的 MAC

地址被绑定在宽带公司，您可以和宽带技术人员联系，要求注册一个新的 MAC 地址。



7.3.2 PPPoE

输入您的网络服务提供商的 PPPoE 的用户名和密码。

不要去改变 MTU（最大传输单位）的默认数值，除非你有特定的需求。

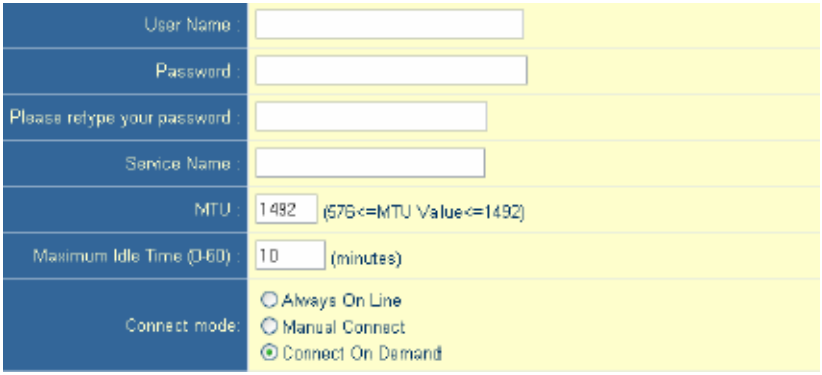
输入一个最大空余超时时间（以分钟计），当超过这个时间，路由器将自动断开与 Internet 的连接。（默认：10 分钟）

连接模式：

Always on line：永远在线。适用于包月制用户；

Manual Connect：手动连接。当您的网络断线后，一定要重新点击“Status”页面中的“Connect”连接按钮后，才能再次上网。适用于包时用户。

Connect on demand：按需连接。当您的网络断线后，任何上网的操作都将激活网络连接。

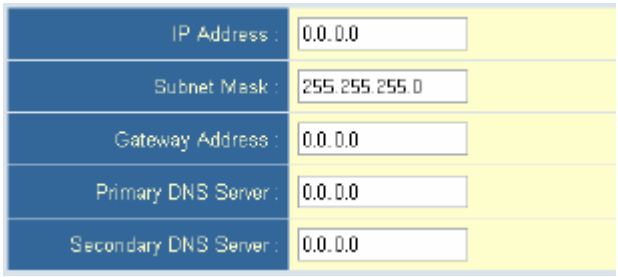


7.3.3 PPTP

中国大陆没有运营商支持此种接入方式，故在此掠过。

7.3.4 Static IP 固定 IP

如果您的 ISP 为您提供了固定 IP，那么您就应该将这些信息输入在此页面，以得到 Internet 服务。



7.3.5 Bigpond

7.3.6 L2TP

这两种宽带接入方式中国大陆运营商没有支持，故在此掠过。

7.3.7 Dial Up 拨号

大部分拨号用户都将选择这个选项利用一个拨号 modem 连接到 Internet 服务提供商。它是一个备用措施，用于在宽带接入不成功的时候。输入电话号码，由 ISP 提供的用户名，密码。Baud rate 波特率是宽带路由器和您的 modem 之间的数据传输速率。如果您的 ISP 给您提供了 DNS IP 地址，要在这里输入，否则就保持它的默认设置。它的连接方式选择，与 PPPoE 里的设置一样。

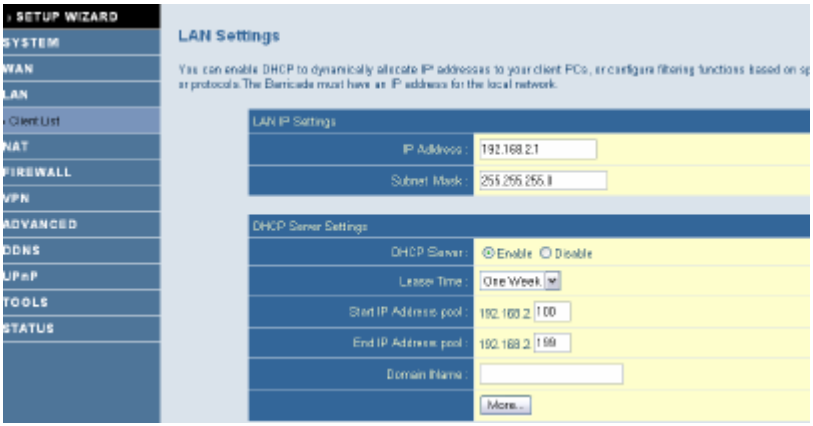
7.4 Advanced Setup 高级设置－LAN 局域网

这是此款路由器的本地 IP 地址。所有连接到它的计算机都必须要以这个地址作为它们的网关地址。然而，如果有需要，您也可以改变这个地址。在这里，您可以为路由器配置 IP 地址，启用/禁用 DHCP 功能

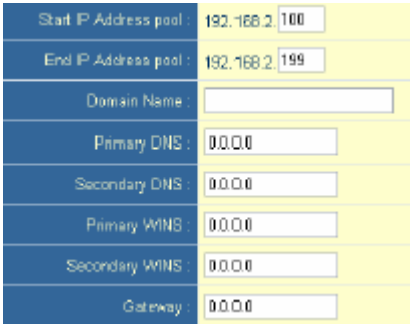
来决定是否自动分配地址给客户端。同时，您也可以设置 IP 地址的租用时间，默认情况下，为 1 周。

对于 IP 地址池，动态 IP 地址的分配必须要有一个范围，默认为 192.168.2.100-199。

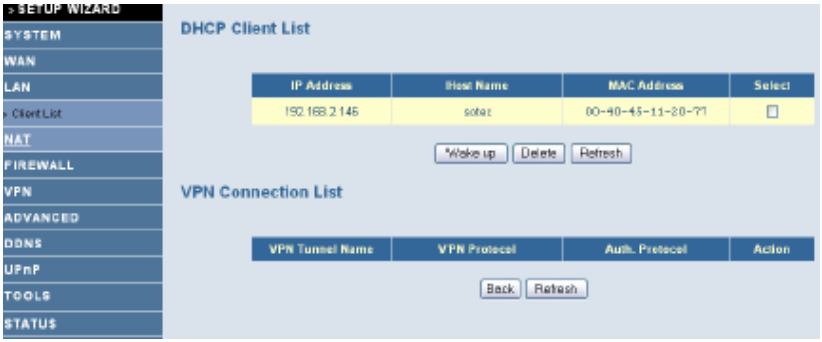
注意：不要将宽带路由器的地址包含在地址池的地址中。



您也可以点击 More 按钮，来作更多的高级设置。您可以设置宽带路由器的 DHCP 服务器，指定主和从 DNS，主和从 WINS,以及可选的网关。



点击“Client List”客户端列表，可以看到 DHCP 客户端列表，它显示了所有通过 DHCP 获得地址的计算机的名字。



7.5 Advanced Setup 高级设置—NAT 网络地址解析

在这部分内容中，您可以配置地址映射，虚拟服务器和特殊应用等功能，也可以支持基于诸如 Web，email，FTP 和 Telnet 等多个 Internet 应用。

7.5.1 Virtual Server 虚拟服务器

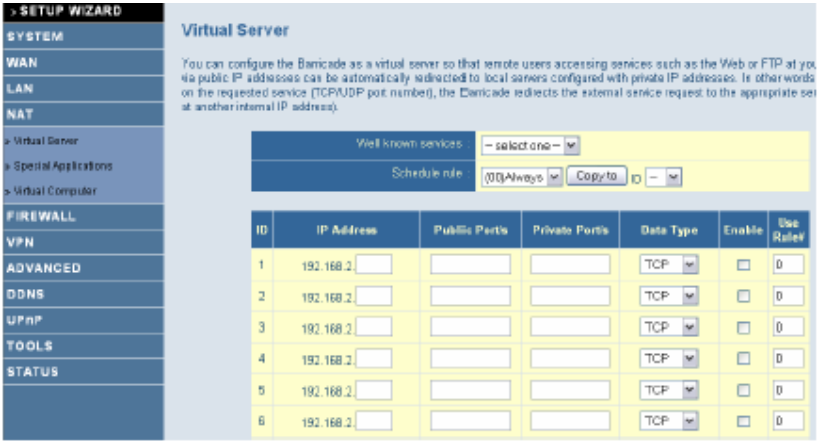
当这款宽带路由器被配置为虚拟服务器后，广域网中的远程用户需要访问局域网中的某些服务器时，诸如 WEB 或 FTP 等服务，远程用户所输入的公网 IP 地址将自动转换为这个页面中所设置的内网 IP 地址。换句话说，根据不同的服务（TCP/UDP 端口号），宽带路由器将重定向到相应的服务器。

例如，您将 Type 设置为 TCP，公共端口号设置为 80，将私有 IP/端口设置为 192.168.2.2/80，那么，所有从外网发送过来的 HTTP 请求

都将重定向到 192.168.2.2 的 80 端口。因此，只要输入 ISP 提供的 WAN 口地址，Internet 用户就可以访问到他们所希望的服务。

常用的 TCP 服务端口号包括：

HTTP:80,FTP:21,Telnet:23,POP3:110



7.5.2 Special Application 特殊应用

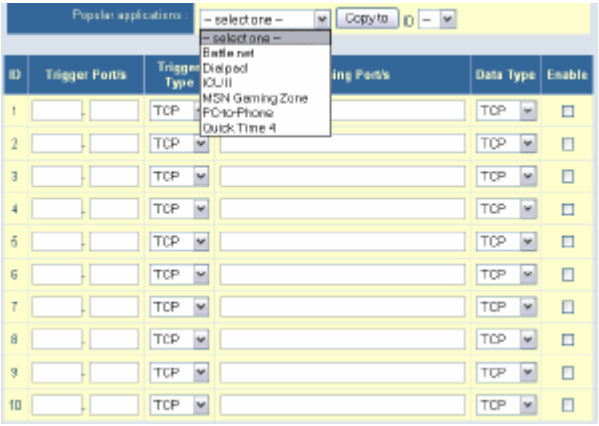
某些应用，诸如网络游戏，视频会议，网络电话等，需要建立多条连接。由于防火墙功能的原因，这些应用无法在 NAT 启用的情况下工作。特殊应用功能使这些应用得以实现。如果用了特殊应用功能后，还是无法实现您想要的功能，您可以试试将这台客户端配置为 DMZ 主机。

在“Trigger Port ”触发端口项中，指定特定的公共端口号，选择 Protocol Type 协议类型为 TCP 还是 UDP，最后输入应用需求的端口号。

常用的应用需求的多个端口号已经在下拉式的应用菜单中，从中，您可以选择特定的端口号。

ID	Trigger Port 触发端口	Trigger Type 触发类型	Public Port 公共端口	Public Type 公共类型	Comment 注释
1	6112	UDP	6112	UDP	Battle.net
2	28800	TCP	2300~2400,47624	TCP	7-1 MSN Game Zone

访问www.iana.org/assignments/port-numbers，可以参考更多端口号和对应服务。



7.5.3 Virtual Computer 虚拟计算机

利用虚拟计算机功能，可以保证本地局域网的安全。虚拟计算机使您可以使用原有的 NAT 功能，并可以使您一一对应地设置外网 IP 地址和本地 IP 地址。

ID	Global IP	Local IP	Enable
1		192.168.2.	☐
2		192.168.2.	☐
3		192.168.2.	☐
4		192.168.2.	☐
5		192.168.2.	☐

7.6 Advance Setup 高级设置－Firewall 防火墙

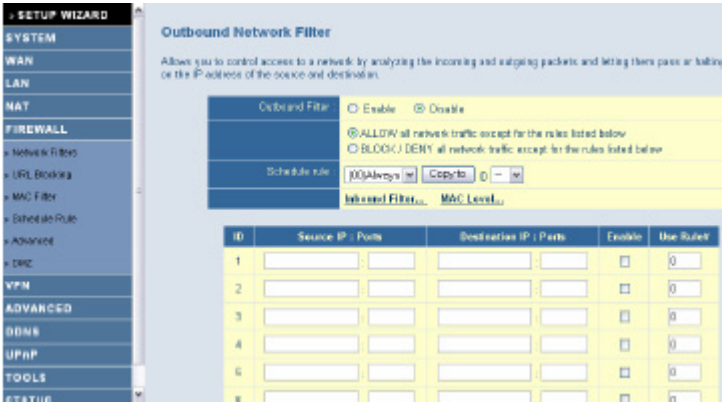
这款宽带路由器可以支持对所连计算机的访问控制，阻止常见的黑客攻击。启用防火墙功能对您的系统性能不会有影响，所以建议您启用此功能，以保证网内用户的安全性。

7.6.1 Network Filters 网络过滤

VPN 宽带路由器防火墙包含了强大的带内和带外包的过滤。包过滤使您可以对能够通过路由器的包进行过滤。 带内的过滤只针对虚拟服务器或 DMZ 主机的地址。

您可以选择两种过滤规则中的一种：

- 允许所有包都通过，除非他们符合特定的规则；
- 阻止所有包通过，除非他们符合特定的规则。



您可以申请最多 8 个规则，每条规则您需要定义以下方面：

- Source IP address 源 IP 地址
- Source port address 源端口地址
- Destination IP address 目标 IP 地址
- Destination port address 目标端口地址
- Protocol 协议：TCP， UDP 或两者都是
- Use Rule# 使用规则号

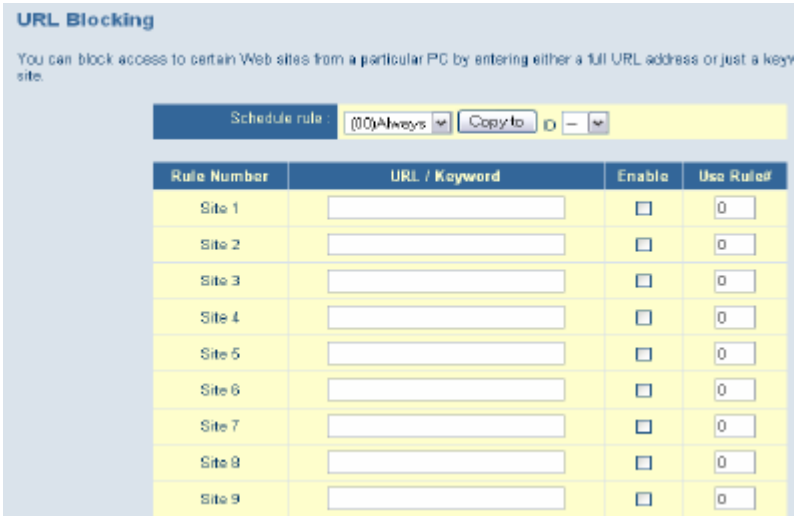
您可以定义一个单独的 IP 地址，或者一个范围内的 IP 地址为源或目标 IP 地址。空的 IP 地址表示所有的 IP 地址被包含了。 您可以定义一个单独的端口号，或者一个范围内的端口号为源或目标端口号。 通过添加 T 或 U 来指定是 TCP 还是 UDP 协议。每个规则都可以启用或禁用。

7.6.2 URL Blocking　URL 过滤

URL 过滤使连接到宽带路由器的计算机无法登录到那些被屏蔽掉的网站。Domain 过滤与 URL 过滤的不同之处在于，Domain 过滤需要您输入一个前缀（.com 或.org）， 然而 URL 过滤只需要您输入一个网

站关键字。换句话说，Domain 过滤只能过滤网页，而 URL 过滤只需要使用一个简单的关键字就可以过滤掉上百个网页。

- URL Blocking：如果您要启用 URL 过滤功能，请勾选。
- URL/Keyword：如果网站 URL 的任何部分与您定义的过滤关键字相符，连接将会被屏蔽。
- Enable：勾选这个框，来启用这条规则。
- Use Rule ＃：应用到一个配置的日程表规则。



7.6.3 MAC Filtering　MAC 地址过滤

MAC 地址过滤功能使您可以为不同的用户分配不同的访问权限。您也可以为一个特定的 MAC 地址指定一个特定的 IP 地址。

勾选 Enable 选项，启用 MAC 地址过滤功能。这个页面上的所有设置将启用。

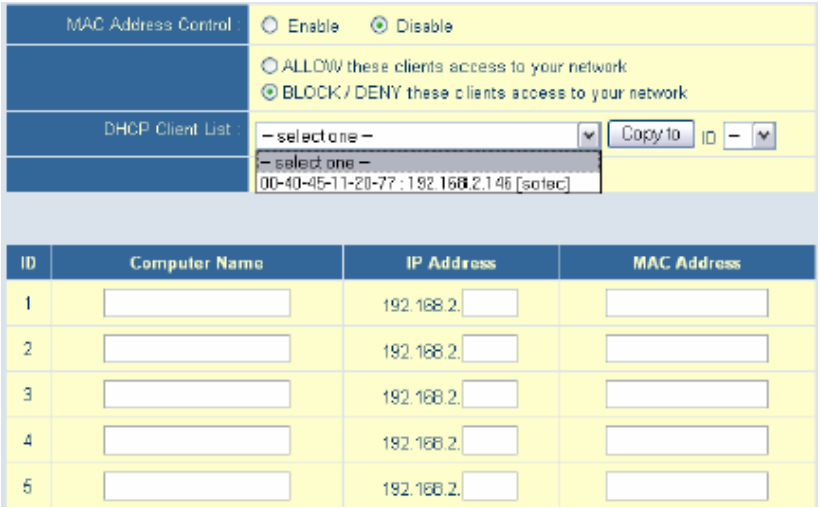
- MAC 地址： 这是每个客户端的唯一地址。

- IP 地址：相应客户端所希望的 IP 地址。您也可以不填，如果您不知道地址。

  DHCP 下拉菜单可使您选择特定的客户端。

从 DHCP 客户端列表中选择特定的客户端，点击“Copy to”，将所选的客户端的 MAC 地址拷贝出来。

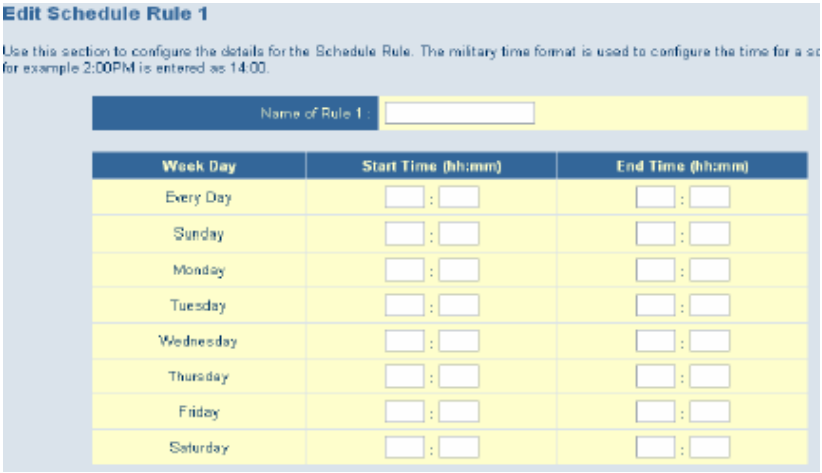
- Previous page/Next page：使用这个链接来访问不同的页面。这个宽带路由器共支持最多 32 个 MAC 过滤。



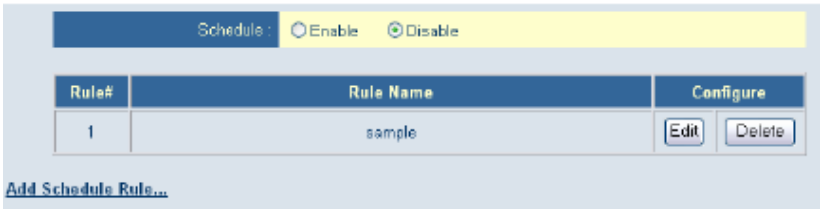
7.6.4 Schedule Rule 时间表规则

在这里可以设置基于时间和日期的时间规则。可以最多设置 10 条时间规则。要新建一个时间表规则，点击【Add Schedule Rule…】。

在“Name of rule 1”中输入规则名字，点击 Save settings 保存您的设置。



时间表规则页面出现，表示您现在可以设置 Rule1 的规则了。如果您要对您之前的设置作修改，点击 Edit 按钮；如果您要删除这个规则，点击 Delete 按钮。

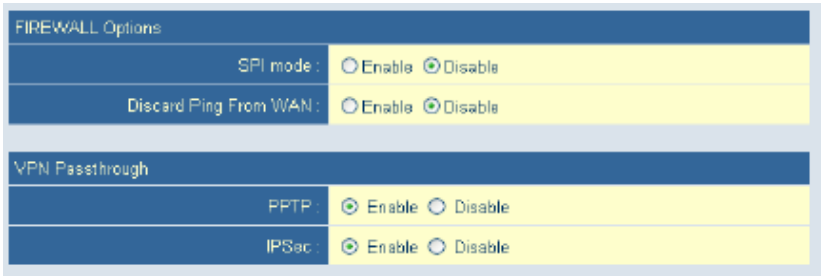


7.6.5 Advanced 高级

在这部分，您可以启用或禁用状态包全检测（SPI），阻止从 WAN 来的 ping， 以及 PPTP 和 IPSec VPN 透传。

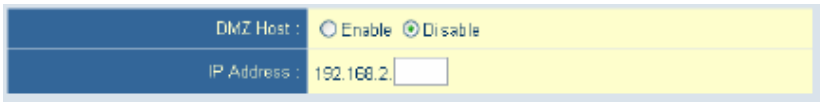
当启用了阻止从 WAN 来的 ping 时，Internet 上的计算机将无法回复给 VPN 宽带路由器关于 ping 的信息。这样会提高安全性。

当启用了 SPI 后，路由器将检测每个将要通过路由器的包，诸如 IP 地址信息，端口信息，ACK 等等。路由器也会检测每个要进来的包来保证网络的安全。



7.6.6 DMZ 非军事区

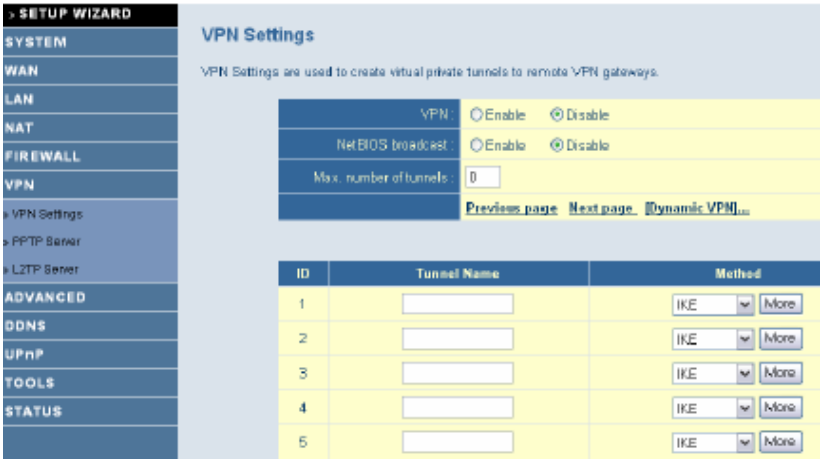
当您的计算机无法在防火墙后访问特定的 Internet 服务时，您可以为那台计算机开启自由的 Internet 访问服务。在这个界面中输入 DMZ 的 IP 地址。添加 PC 到 DMZ，可能会使您的计算机遭到一些安全上的攻击，所以请谨慎使用此功能。



7.7 Advanced Setup 高级设置－VPN

7.7.1 IPSec Tunnel IPSec 通道

VPN 设置用来在远程 VPN 网关间建立虚拟私有通道。通道技术通过利用封装协议，加密算法和散列法算法，支持数据的机密性，数据来源的认证和网络信息的数据完整性。



- VPN： VPN 保护网络信息免受侵入者的盗用。然而，它也大大降低了网络的吞吐量。只有当真正需要这个安全通道时才启用它。默认情况下，这个功能是禁用的。
- Max. Number fof Tunnels 最多通道数：设置能同时使用的通道数量。
- Tunnel Name 通道名：显示了每个通道名称。
- Method 方法：IPSec VPN 支持两种密钥交换方法：手动的密钥交换和自动的密钥交换。手动的密钥交换方法表示两端 VPN 网关的认证和加密是通过系统管理者手动配置的。然而，IKE 方法是自动

的密钥交换，两端 VPN 网关的系统管理者只需要设置相同的 Pre-shared 密钥即可。

- “More”按钮：点击“More”按钮，可以设置更详细的信息。

当启用 IKE 后，有 3 项必须要做的设置：

- 基本设置
- IKE 建议设置
- IPSec 建议设置

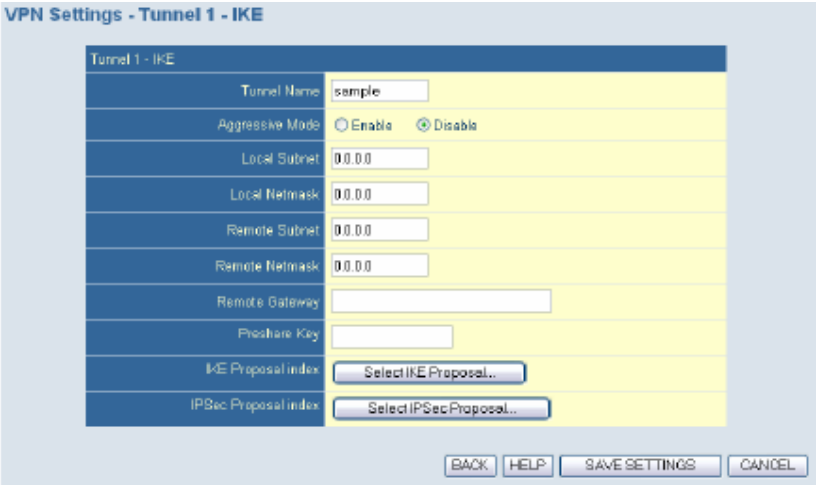
基本设置

- Local Subnet 本地子网：VPN 路由器的本地子网。这个子网可以是一个主机，一个局部的子网，或者是路由器的整个子网。
- Local netmask 本地子网掩码：
- Romote subnet 远程子网：远程 VPN 路由器的子网。这个子网可以是一个主机，一个局部的子网，或者是远程路由器的整个子网。
- Remote netmask 远程子网掩码
- Remote gateway 远程路由器：远程路由器的 IP 地址
- Pre-shared key：两端的 VPN 路由器必须要使用相同的 Pre-shared Key。

选项

- Select IKE proposal 选择 IKE 提议：选择这个按钮进行一系列的 IKE 设置
- Select IPSec proposal 选择 IPSec 提议：选择这个按钮进行一系列的关于 IPSec 的设置

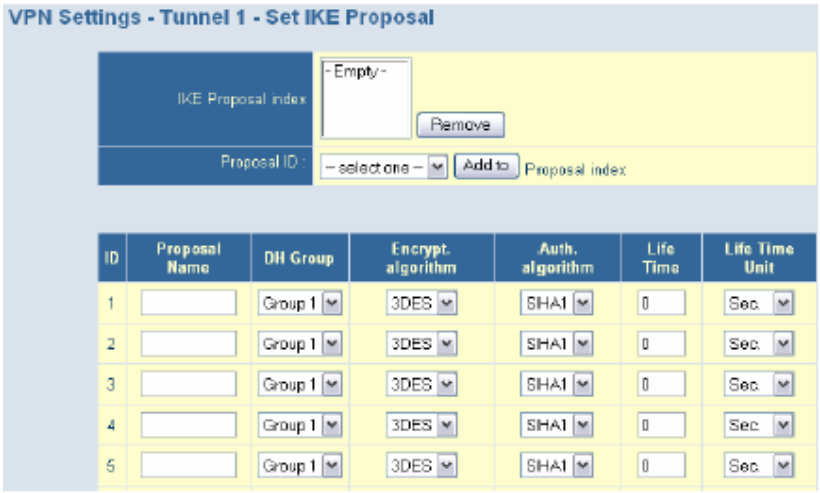
通道名应该与您在前面的 VPN 页中所设置的名称相同。IKE 建议索引包括一系列的常用的 IKE 建议的设置，IPSec 建议索引包括了一系列常用的 IPSec 建议的设置。



7.7.2 IKE Proposal IKE 建议

- IKE Proposal index IKE 建议向导：从 IKE 建议池中所选的一系列建议索引。当您选择一个建议号（proposal ID）并且点击了 Add 键添加到下拉式列表中。 从建议池中，为一个通道，可以最多选择 4 个索引。
- Proposal Name 建议名：建议名用于表示哪个 IKE 建议将被监控如果建议名的第一个字母是 0x00，表示这个 IKE 建议是无效的。
- DH Group DH 组： 有 3 组可以选择：
  - Group1（MODP768）
  - Group2 (MODP1024)
  - Group5 (MODP1536)

- Encryption algorithm 加密机制： 有两种加密机制可以选择：
  - 3DES
  - DES
- Authentication algorithm 认证机制： 有两种认证机制可以选择：
  - SHA1
  - MD5
- Life Time 生命周期：生命周期的数值是基于生命周期的单位的。生命周期单位可以是秒或者 KB。如果以秒为单位，那么生命周期的数值表示两端路由器的 VPN 通道的生命周期，数值可以是从 300 秒到 172800 秒。如果以 KB 为单位，那么生命周期的数值表示两端路由器的 VPN 通道所能传输的总包数，数值可以是从 20480 到 2483647KB。
- Life Time Unit 生命周期单位：可以是以秒或 KB 为单位。
- Proposal ID 建议号： 共有 10 个建议 ID 号可在建议池中被选择。一个通道最多可以从建议池中选择 4 个建议 ID。
- “Add to”button “Add to”按钮：点击这个按钮以添加所选的建议，它们被显示在 IKE 建议索引列表中的 Proposal ID 列中。



7.7.3 IPSec Proposal IPSec 建议

- IPSec Proposal index IPSec 建议索引：在 IPSec 建议池中所选的建议索引列表。当您选择了一个建议 ID 并点击添加按钮后，表示这个建议号即被选中。一个通道最多可以选择 4 个索引。
- Proposal Name 建议名：建议名表示哪个 IPSec 建议将被监控。如果建议名的第一个字母是 0x00，表示这个 IPSec 建议是无效的。
- DH Group DH 组： 有 3 组可以选择：
  - Group1（MODP768）
  - Group2 (MODP1024)
  - Group5 (MODP1536)

  当然，您也可以什么都不选。

• Encapsulation protocol 封包协议： 有两种协议可以选择：

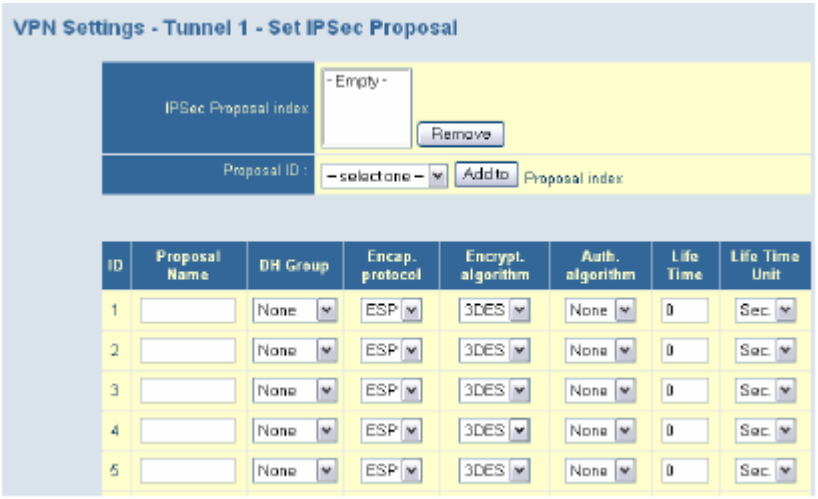
  - ESP

- AH

- Encryption algorithm 加密机制： 有两种加密机制可以选择：
  - 3DES
  - DES

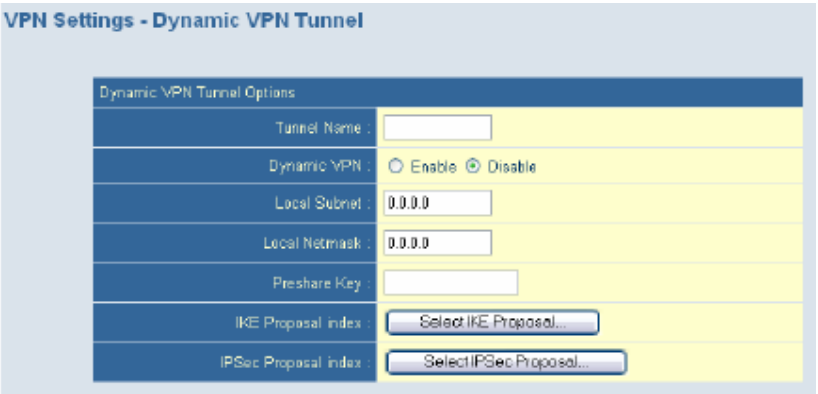
  然而，如果封包协议选择的是 AH，那么加密机制并不是必须的。
- Authentication algorithm 认证机制： 有两种认证机制可以选择：
  - SHA1
  - MD5

  然而，您也可以什么都不选。
- Life Time 生命周期：生命周期的数值是基于生命周期的单位的。生命周期单位可以是秒或者 KB。如果以秒为单位，那么生命周期的数值表示两端路由器的 VPN 通道的生命周期，数值可以是从 300 秒到 172,800 秒。如果以 KB 为单位，那么生命周期的数值表示两端路由器的 VPN 通道所能传输的总包数，数值可以是从 20,480 到 2,483,647KB。
- Life Time Unit 生命周期单位：可以是以秒或 KB 为单位。
- Proposal ID 建议号： 共有 10 个建议 ID 号可在建议池中被选择。一个通道最多可以从建议池中选择 4 个建议 ID。
- “Add to”button “Add to”按钮：点击这个按钮以添加所选的建议，它们被显示在 IPSec 建议索引列表中的 Proposal ID 列中。



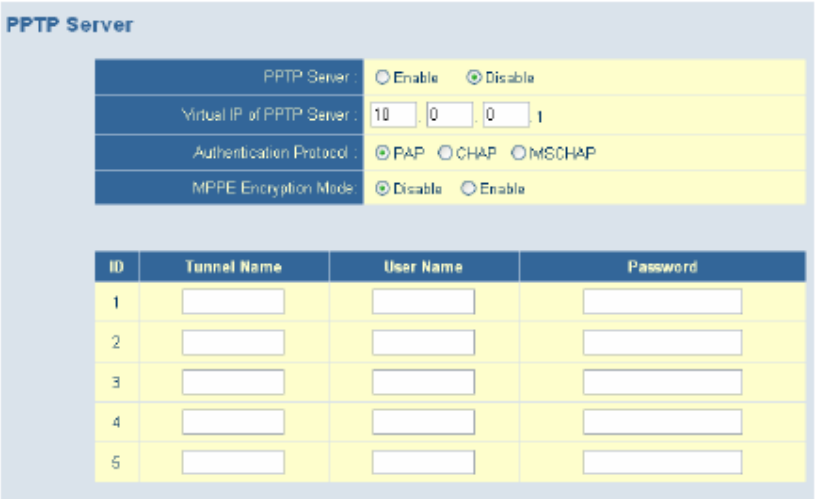
7.7.4 Dynamic VPN 动态 VPN

当使用 VPN 动态 IP 设置时，路由器则作为一个动态 VPN 服务器。动态 VPN 服务器并不检查 VPN 客户端的 IP 信息，这意味着您可以利用一台 VPN 路由器与任何远程主机建立 VPN 通道，而无需考虑 IP 信息。



7.7.5 PPTP/L2TP Server PPTP/L2TP 服务器

PPTP/L2TP 通过 ISP 可在 Internet 上提供安全的远程访问。以下界面显示了在哪里输入远程被认证用户的用户名和密码的管理界面，包括认证协议，以及将为这些用户分配的 IP 地址的起始范围。

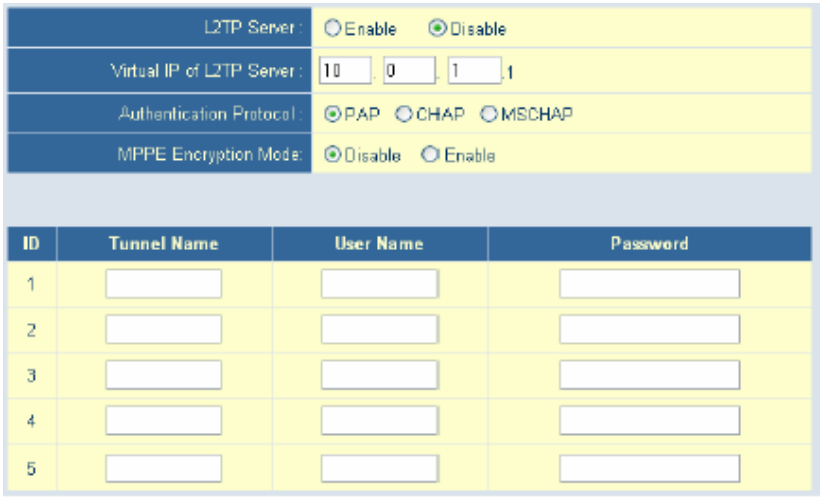


此款 VPN 路由器支持 PAP，CHAP 和 MS-CHAP 认证协议，您也可以启用或禁用微软提供的点到点加密协议 MPPE。我们建议您在任何时候都启用 MPPE。然而，请您注意的是，当您启用 MPPE 后，所支持的认证协议只有 MS-CHAP。这是因为在 MS-CHAP 认证过程中，MPPE 的共享密钥会自动生成。而在 PAP 或 CHAP 认证过程中，则不会。

PAP 是一个简单的认证协议，它的用户名和密码数据是以明文或不加密的方式传输。我们并不建议您使用 PAP 认证机制，因为您的密码在认证过程中会很容易地被截取并被改变。

当使用 CHAP（竞争握手确认协议）进行认证，密码的确认，甚至密码本身是由客户端来传递。 启用 CHAP 后，VPN 宽带路由器给远程的客户端发送一个竞争字符串。远程客户端就利用这个竞争字符串连同密码，建立一个 MD5 转发给 VPN 服务器端。VPN 服务器将两个字符串比较是否相同，如果它们是相同的，则认为远程客户端是一个被认证的合法用户。

注意： PPTP 和 L2TP 服务器将分配给客户端的 IP 地址将不能是冲突的。



7.8 Advanced Setup 高级设置 －SNMP

简单网络管理协议（SNMP） 可以使您远程设置网络并且监控网络事件。

- Enable SNMP 启用 SNMP： 您可以选中 Local,Remote 或两者都选来启用 SNMP 功能。
- 如果选择了 local，路由器只能在局域网 LAN 范围内接受管理；

- 如果选择了 Remote， 路由器可以在 WAN 范围内接受管理。
- Get community：设置此项使您的路由器能响应一个请求。
- Set community：设置此项使您的路由器能接受一个请求。

7.9 Advanced Setup 高级设置－Routing 路由

您可以通过路由表确定通往外部 IP 地址所经过的路径。如果您由一个以上的路由和子网，您应该启用这个路由表，使每个包都可以找到它的路由路径。它实现了不同子网间的互相通信。在此款路由器的路由表中支持静态和动态的路由功能。RIPv1 是 IP 地址通过 Internet 的一个协议。RIPv2 是 RIPv1 的增强版，它添加了诸如认证，路由域，下个节点转发以及子网掩码互交换等功能。

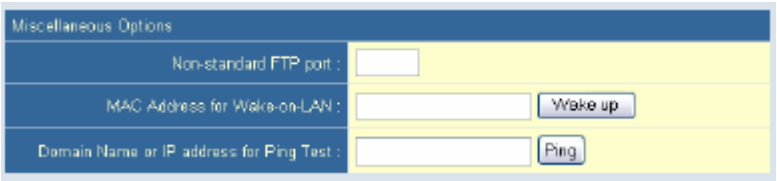
通过点中 Static Routing 的 Enable 选项来启用这个静态路由功能。

- Static Routing 静态路由：您最多可以设置 8 条路由规则。您可以依次输入目的 IP 地址，子网掩码，网关，每条路由规则的跳数，随后通过勾选或去掉勾选来启用或禁用这条路由规则。一旦路由表设置作了改变后，请点击“Save”按钮保存。

7.10 Advanced Setup 高级设置－Miscellaneous 其他

如果您的 FTP 服务器并没有使用默认的 21 端口号，您可以在此界面的“Non-standard FTP”处设置您特定的端口号，并保存这个设置。

“Wake-on-LAN”局域网唤醒功能是使您可以远程地启用这台路由器的技术。要使用这个功能，您的网卡必须也要支持局域网唤醒功能，并且你也必须知道相应网卡的 MAC 地址。按下“Wake up”按钮意味着这台路由器将向目标网卡发送唤醒帧。

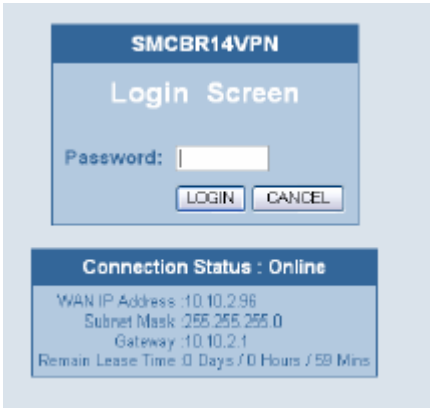


ping 侦测功能使您可以设置一个 IP 地址从路由器发送 ping 包。您可以 ping 一个特定的 IP 地址或域名来检测路由器是否正常在线。

7.11 Advanced Setup 高级设置－Display status 显示状态

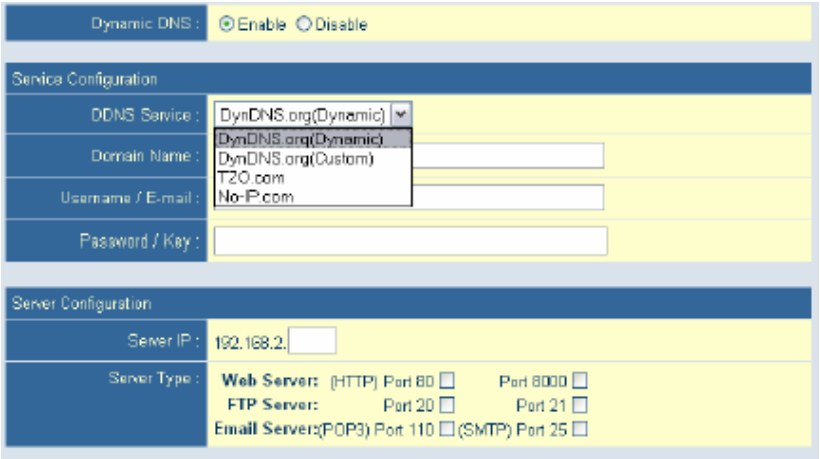
启用显示状态选项，可以在登录页面上看到 WAN 口的连接状态。

当这个选项被启用后，登录页面上将显示如下：



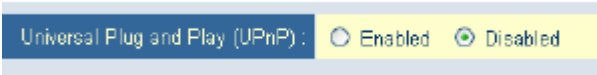
7.12 DDNS（动态 DNS）

动态 DNS 为 Internet 上的用户提供了将他们的域名绑定到计算机或服务器上的方法。DDNS 使您的外网 IP 地址不需要一定要静态 IP 地址，当您的 IP 地址改变时，它所记录的 IP 地址也可以随之改变。在您使用 DDNS 服务前，请在下拉式菜单中选择其中一个动态 DNS 服务商并注册一个帐号。



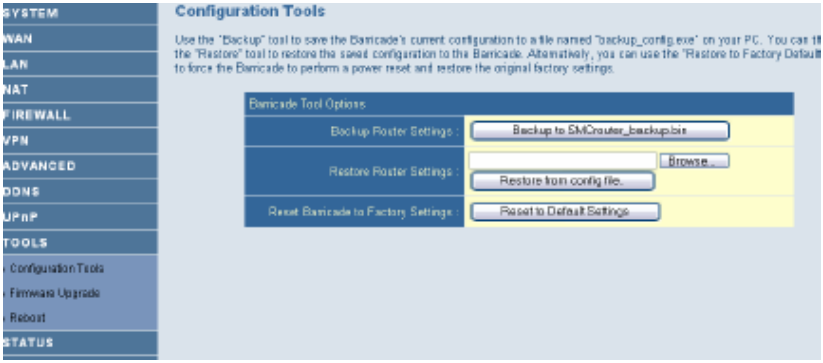
7.13 UPnP（通用即插即用）

UPnP 为 PC，智能应用和无线设备提供了完全意义上的即插即用网络连接。UPnP 使您在家庭，办公室，或任何地方之间都可以进行无缝地网络传输，包括控制信息和数据。



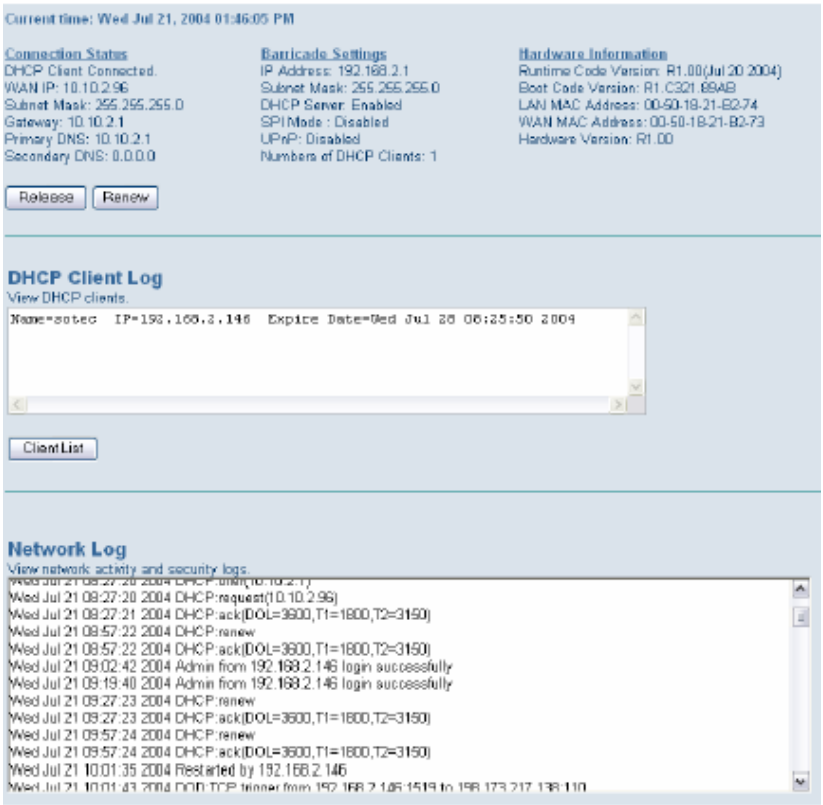
7.14 Tools 工具

工具菜单可以使您查看系统日志，升级固件，设置备份，恢复到出厂设置，重启路由器以及其他一些设置。



7.15 Status 状态

您可以通过状态页面来查看宽带路由器的 WAN/LAN 的连接状态，固件以及硬件的版本信息，任何路由器信息，诸如所有通过 DHCP 服务器获得地址的 PC 信息等等。


Current time: Wed Jul 21, 2004 01:46:05 PM
Connection Status
DHCP Client Connected.
WAN IP: 10.10.2.96
Subnet Mask: 255.255.255.0
Gateway: 10.10.2.1
Primary DNS: 10.10.2.1
Secondary DNS: 0.0.0.0
Barricade Settings
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
SPI Mode : Disabled
UPnP: Disabled
Numbers of DHCP Clients: 1
Hardware Information
Runtime Code Version: R1.00(Jul 20 2004)
Boot Code Version: R1.C321.89AB
LAN MAC Address: 00-50-18-21-B2-74
WAN MAC Address: 00-50-18-21-B2-73
Hardware Version: R1.00
Release
Renew
DHCP Client Log
View DHCP clients.
Name=sotec IP=192.168.2.146 Expire Date=Wed Jul 28 06:25:50 2004
Client List
Network Log
View network activity and security logs.
Wed Jul 21 09:27:20 2004 DHCP:request(10.10.2.96)
Wed Jul 21 09:27:21 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 09:57:22 2004 DHCP:renew
Wed Jul 21 09:57:22 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 09:02:42 2004 Admin from 192.168.2.146 login successfully
Wed Jul 21 09:19:40 2004 Admin from 192.168.2.146 login successfully
Wed Jul 21 09:27:23 2004 DHCP:renew
Wed Jul 21 09:27:23 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 09:57:24 2004 DHCP:renew
Wed Jul 21 09:57:24 2004 DHCP:ack(DOL=3600,T1=1800,T2=3150)
Wed Jul 21 10:01:35 2004 Restarted by 192.168.2.146

第8章 IPSec 设置向导（仅供参考）

8.1 两台 SMCBR14VPN 之间的通道

要建立一条 VPN 通道最简单的方法是利用两台 SMCBR14VPN，当然，它们都应该连接到 Internet。

在两台路由器之间建立一个 IP 通道的步骤为：

1. 转到 VPN 页面，启用 VPN 功能
2. 选择您所希望启用的通道号码
3. 输入一个通道名称，选择 IKE 或 Manual，点选 More，做更多设置
4. 本地子网值为 LAN SUBNET
5. 本地子网掩码值为 LAN SUBNET MASK
6. 远程子网值为 REMOTE NETWORK 的 LAN SUBNET
7. 远程子网掩码值为 REMOTE NETWORK 的 LAN SUBNET MASK
8. 远程网关值为 REMOTE NETWORK 的 WAN IP
9. SAVE SETTINGS 并且配置 IKE 建议或 IPSec 建议。

8.1.1 为路由器 1 设置

VPN 路由器：　　WAN IP 地址： ip1.smc.com

1　　LAN IP 地址：192.168.1.1

PC　　192.168.1.xxx

进行 VPN 设置：

VPN：　　Enable 启用

最多通道数：　2

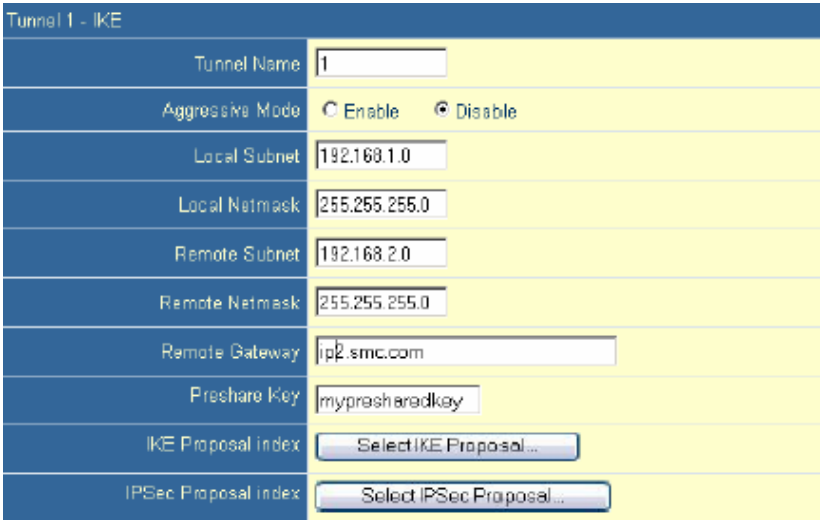
ID：　　1

通道名：　　1

方法：　　IKE

完成后，点击“More”，进行更多设置。

VPN 设置－通道 1－IKE



进行通道 1IKE 设置：

通道 1：　　1

本地子网：　　192.168.1.0

本地子网掩码：　　255.255.255.0

远程子网：　　192.168.2.0

远程子网掩码：　　255.255.255.0

远程网关：　　ip2.smc.com

Preshare Key：　　mypresharedkey

完成设置后，保存。

8.1.2 设置路由器 2

VPN 路由器 2 WAN IP 地址： ip2.smc.com

LAN IP 地址： 192.168.2.1

PC 192.168.2.xxx

进行 VPN 设置：

VPN：　　Enable 启用

最多通道数：2

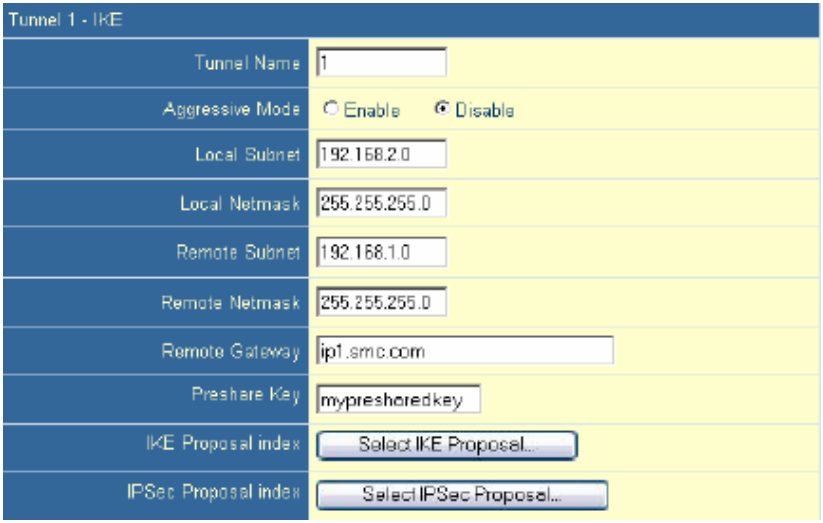
ID：　　1

通道名：　　1

方法：　　IKE

完成后，点击“More”，进行更多设置。

VPN 设置－通道 1－IKE



进行通道 1IKE 设置：

通道 1：　　1

本地子网：　　192.168.2.0

本地子网掩码：　　255.255.255.0

远程子网：　　192.168.1.0

远程子网掩码：　　255.255.255.0

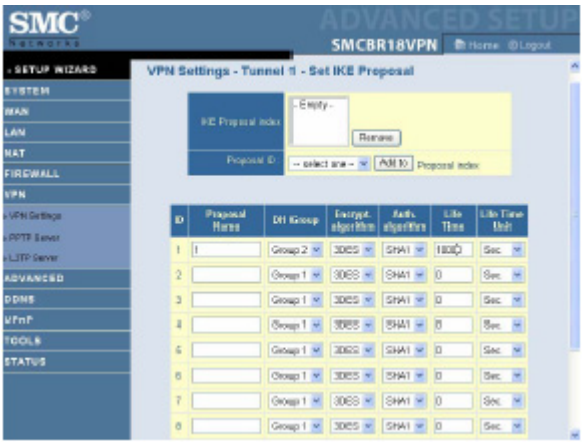
远程网关：　　ip1.smc.com

Preshare Key：　　mypresharedkey

完成设置后，保存。

8.1.3 两台路由器的常见设置

VPN设置－通道 1－进行IKE设置



进行通道 1IKE 建议设置：

ID：　　1

建议名：　　1

DH Group：　　Group2

加密机制：　　3DES

认证机制：　　SHA1

生命周期：　　10000

生命周期单位：　　秒

完成设置后，请保存。

VPN设置－通道 1－进行IPSec设置

进行通道 1IPSec 建议设置：

ID：　　1

建议名：　　1

DH Group：　　Group2

封包机制：　　ESP

加密机制：　　DES

认证机制：　　MD5

生命周期：　　10000

生命周期单位：　　秒

完成设置后，请保存。

现在，要查看 VPN 连接的进程，请转向 Status 状态页面查看系统日志。您可以看到 PC1（WAN IP192.168.1.100）已经可以访问到 PC2（WAN IP 192.168.2.100）。

8.2 在一个 SMCBR14VPN 和另一个独立客户端之间建立一个通道

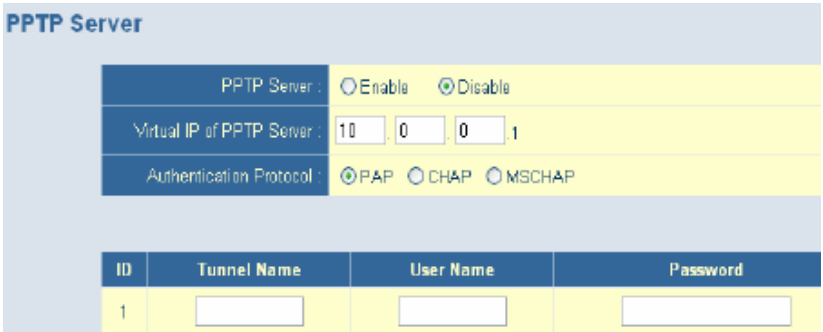
一个通道也可以在 PC 和 SMCBR14VPN 之间建立。最简单的方法是在 PC 上运行一个 IPSEC VPN 客户端软件。在客户端要进行相应的配置，您只需要改变的是远程子网掩码的设置，应该是 255.255.255.255，这是因为我们只为一个客户端配置一个通道。如果客户端将要从不同的 IP 进行连接，动态 VPN 是一个理想的解决方案。

PPTP/L2TP 配置举例

请注意：L2TP 和 PPTP 的虚拟地址必须是不同的。

PPTP

1. 转向 PPTP Server 页面，并启用此功能
2. 如有必要，可以改变 PPTP 的虚拟 IP 地址（这是您的 PPTP 客户端将自动连接上的地址）
3. 设置认证协议
4. 输入一个通道名，并且要设置相应的用户名和密码
5. 配置您远程的 VPN 客户端，使它可以连接到此路由器



L2TP

Microsoft 用户可使用内置的 L2TP/PPTP VPN 功能。为了使用微软提供的标准的 VPN 客户端，您必须在 PC 上禁用 IPSEC。请参考微软关于此的帮助信息。

1. 转向 L2TP Server 页面，并启用此功能
2. 如有必要，可以改变 L2TP 的虚拟 IP 地址（这是您的 PPTP 客户端将自动连接上的地址）
3. 设置认证协议
4. 输入一个通道名，并且要设置相应的用户名和密码
5. 配置您远程的 VPN 客户端，使它可以连接到此路由器

第9章 技术规格

标准：

IEEE802.3 10Base-T 以太网

IEEE 802.3u 100Base-TX 快速以太网

硬件/端口：

LAN 端口： 4*RJ45,10/100 MDI/MDIX

WAN 端口：1*RJ45,10/100 MDI/MDIX

COM 口：1*DB9(公头)，高达 115200bps

输入电源：DC 5V2A

指示灯：

Power 电源： 1*绿色

WAN：1*橙色 10Mbps/绿色 100Mbps，闪烁 数据在传输

VPN透传：

IPSec

PPTP

L2TP

VPN 支持特性：

IPSec Endpoint

PPTP 服务器

L2TP 服务器

密钥管理：IKE，Manual 手动

VPN 的主动/主要模式

支持远程网关 FQDN

支持动态 VPN（Dynamic VPN）

加密机制： DES,3DES, AES

认证机制： MD5, SHA-1

支持 PFS

密钥模式： Pre-shared key

启用 NetBIOS 广播

路由特性：

静态路由

动态路由（RIP1/2）

WAN连接类型：

拨号

ISDN

PPPoE

动态 IP

L2TP

PPTP

BigPond

静态 IP

依从：

FCC

CE

VCCI

UL

SMC NETWORKS Inc. (China)
中国区总部
上海市虹漕路421号63号楼1楼
Tel: +86-21-6485-9922
Fax: +86-21-6495-7924
http://www.smc-prc.com

北京办事处
北京市海淀区中关村南大街2号
数码大厦A座1605室
Tel: +86-10-8251-1550
Fax: +86-10-8251-1551

SMC NETWORKS USA(Headquarter)
38 Tesla
Irvine, CA92618
Tel: +800-SMC-4YOU
+949-679-8000
Fax: +949-679-1481
http://www.smc.com

SMC NETWORKS Asia Pacific
1 Claymore Drive #08-05/06
Orchard Towers (Rear Block)
Singapore 229594
Tel: +65-6238-6556
Fax: +65-6238-6466
http://www.smc-asia.com

SMC NETWORKS Europe
Edificio Conata II
Calle Fructuós Gelabert 4-6, 2º, 4ª
08970 - Sant Joan Despí
Barcelona, Spain
Tel: +34-93-477-4920
Fax: +34-93-477-3774
http://www.smc-europe.com