D-Link DI 企业路由器
用户手册

VER: 20110613

声　　明

由于产品版本升级或其它原因，本手册内容会不定期进行更新，为获得最新版本的信息，请定时访问公司网站。具体的产品型号具有的功能以固件版本本身为准，该手册仅为路由器通用用户操作指导文档，友讯电子设备(上海)有限公司试图在本资料中提供准确的信息，但对于可能出现的疏漏概不负责。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

物品清单

在包装箱完整的情况下，开启包装箱。箱内应包含如下各项：

- 一台路由器主机
- 一条电源线
- 一条网线
- 一本快速安装手册
- 一张安装指导光盘
- 一张保修卡
- 一张产品合格证

注意：

- 如果发现有任何配件损坏或遗漏，请及时与经销商联系。
- 本手册为 D-Link DI 系列企业路由器通用用户操作指导文档，具体包括的产品型号有：DI-7001、 DI-7100、DI-7200、DI-7300、DI-7400、DI-7500

目　　录

第一章　网络基础知识

1.1 局域网入门

路由器是指能将两个网络连接起来的设备，路由器能连接局域网或者一组电脑到互联网，处理并校验在网络中传输的数据。

路由器网络地址转换技术（NAT）保护网络中的电脑，使互联网用户侦测不到，这是保护局域网的有效方法。路由器检查互联网端口的数据包，只转发允许通过的数据包到内网，增加了局域网的安全性。

1.2 IP地址

IP 是建立在互联网协议上的。每个基于 IP 的网络设备如计算机，打印服务器和路由器等都需要一个 IP 地址来识别它在网络中的位置。

有两种为网络设备分配 IP 地址的方法：静态地址分配和动态地址分配。

静态地址即手工为网络设备分配的固定 IP 地址，此地址会一直有效到你关闭设备。一般将固定地址分配给需要经常访问的网络设备。

动态地址即 DHCP 服务器自动为网络中设备分配的 IP 地址，此地址一般都有生存期，如果超过生存期，DHCP 服务器再次为其分配新的 IP 地址。

1.3 子网掩码

子网掩码和 IP 地址一样，都是 32 位，它不能单独存在，必须结合 IP 地址一起使用。子网掩码的作用是将某个 IP 地址划分成网络号和主机号两部分。这对于采用 TCP/IP 协议的网络来说非常重要，只有通过子网掩码，才能表明一台主机所在的子网与其他子网的关系，使网络正常工作。

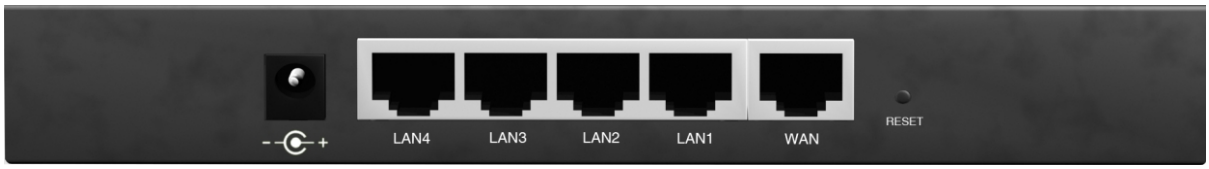
第二章　快速安装指南

2.1 认识和连接路由器

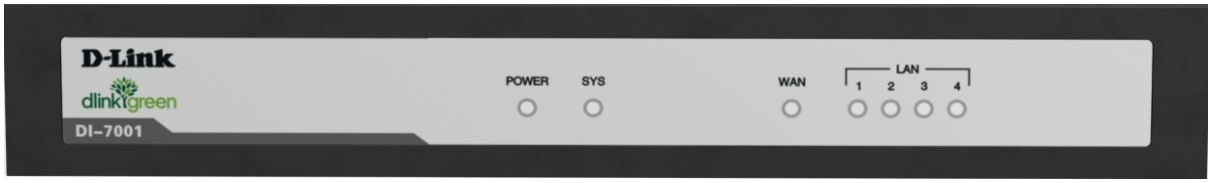
注：图片为 DI-7001 型号示意图，具体型号以实物为准

2.1.1 面板布置

- **后面板**



- **前面板**



POWER	电源指示灯，当路由器加电后该灯常亮
SYS	系统正常运行时，以 1Hz 的速率闪烁。熄灭或常亮时异常
WAN	路由器外网网络接口
LAN1	路由器内网网络接口 1
LAN2	路由器内网网络接口 2
LAN3	路由器内网网络接口 3
LAN4	路由器内网网络接口 4
RESET 按钮	运行中按住按钮后松开，路由器恢复出厂设置

2.1.2 设备安装

- **安装环境要求**

请不要将本产品放置在潮湿、粉尘的环境中；

请不要将本产品置于阳光下暴晒或置于其他热源附近；

- **推荐使用环境**

工作温度：0℃到 40℃；

存储温度：-40℃到 70℃；

工作温度：10%到 90%不凝结；

存储温度：5%到 90%不凝结；

提示：为了您的安全，安装时请关闭电源，拔掉电源插头，保持双手干燥！

2.2 配置您计算机网络设置

1、打开路由器电源，等待片刻，当路由器前面板的 system 灯匀速闪烁以后，表示路由器已经进入工作状态，可以接受配置了。

2、请正确配置计算机的网络设置，并加载 TCP/IP 协议。

3、设置计算机的 IP 地址在 192.168.0.2-192.168.0.254 范围内（即与路由器内网地址在同一网段内，例如 192.168.0.2），子网掩码为 255.255.255.0，默认网关为 192.168.0.1，DNS 为 192.168.0.1。

4、依次点击计算机的开始菜单→程序→附件→命令提示符，您现在可以使用下面的命令来检查您的计算机和本产品是否正常连通，在命令提示符下输入：

```
C:\>ping  192.168.0.1
Pinging  192.168.0.1  with  32  bytes  of  data:
Reply  from  192.168.0.1:  bytes=32  time<10ms  TTL=128
Reply  from  192.168.0.1:  bytes=32  time<10ms  TTL=128
Reply  from  192.168.0.1:  bytes=32  time<10ms  TTL=128
Reply  from  192.168.0.1:  bytes=32  time<10ms  TTL=128
```

如果出现以上显示，表示网络连接正确，可以进行下一步操作。如果屏幕提示为：

```
Pinging  192.168.0.1  with  32  bytes  of  data:
Request  timed  out.
Request  timed  out.
Request  timed  out.
Request  timed  out.
```

说明设备未正确安装，可以按照下面的步骤检查：

1、设备的物理连接是否正确？

与计算机网卡相连的双绞线的另外一端必须接路由器的内网口(例如 LAN1 口)，并且网线两端的网络接口的指示灯必须正确点亮。

2、计算机的 TCP/IP 协议是否设置正确？

您的计算机 IP 地址必须为 192.168.0.x (x 的范围是 2-254)，子网掩码为：255.255.255.0(即在同一网段内)，默认网关为 192.168.0.1。

2.3 配置您的路由器

本产品提供基于浏览器的配置界面，打开浏览器，在浏览器的地址栏中输入路由器默认 IP 地址：http://192.168.0.1，如下图所示：

按回车键，下图所示的用户界面将会出现在您的面前：

请输入用户名：admin，密码：admin，单击“确定”按钮，您将会看到以下界面：

2.3.1 内网设置

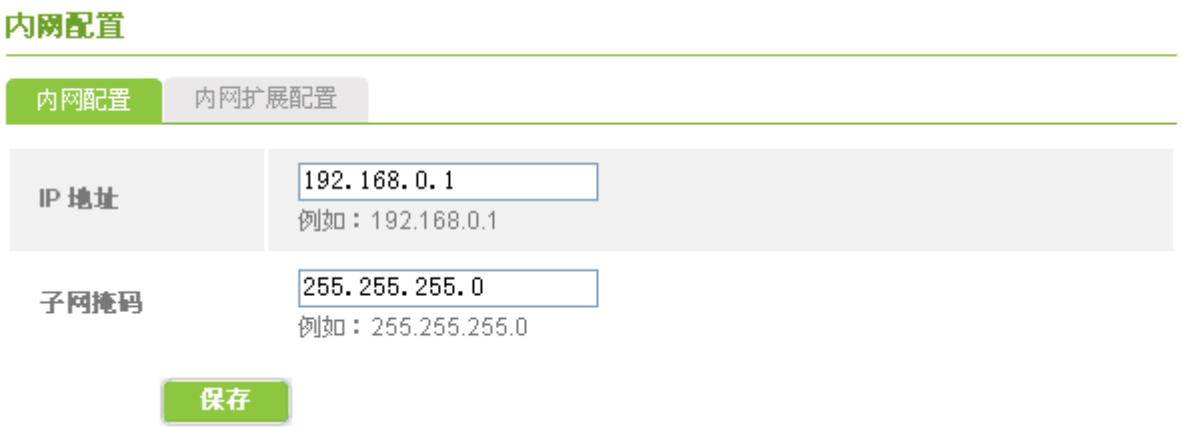
点击“基础设置”→“内网设置”选项：

在内网设置里，可以“设置路由器的内网 IP 地址和子网掩码”：

1、“IP 地址”，通常是内网计算机指的网关地址。

2、“子网掩码”，通常是内网计算机指的子网掩码。

然后点击“保存”按钮，便完成了对路由器内网的设置，如下图所示：



接下来我们继续对外网进行设置。

2.3.2 外网设置

点击“基础设置”→“外网配置”选项，路由器的 WAN 口支持三种连接方式，静态地址线路、PPPoE 拨号线路、动态获取地址线路。

A. 如果您的 WAN 口线路所用的连接方式是静态地址线路，在“类型”下拉菜单中，选中“静态线路”。配置的参数都是由 ISP 提供的。举例如下：

1、“IP 地址”，例如填写：222.219.32.65

2、“子网掩码”，例如填写：255.255.255.0

3、“缺省网关”，例如填写：222.219.32.1

4、“DNS 服务器 1”，例如填写：202.98.96.68

5、“DNS 服务器 2”，例如填写：61.139.2.69

6、“网络服务商”，例如申请的是电信的光纤。

7、“线路带宽”，例如申请的光纤的带宽是 10M，那么上行填写 10,下行填写 10。

8、“MTU 设置”，我们保持默认设置“自动”。

9、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改。

完成后点击“保存”按钮即可。

B．如果您的 WAN 口线路所用的连接方式是 PPPoE 拨号线路，在“类型”下拉菜单中，选中“PPPoE 拨号线路”。配置的参数都是由 ISP 提供的。举例如下：

1、“帐户”，例如填写：CD88888888

2、“密码”，请正确填写 ISP 给您的密码。

3、“按需拨号”，一般在这里保持默认设置，留空。

4、“网络服务商”，例如申请的是电信的线路。

5、“线路带宽”，例如您申请的线路带宽是 2M，那么请根据 ISP 提供的上行与下行速率的准确数值填写。例如上行填写 1，下行填写 2。

6、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改。

完成后点击“保存”按钮即可。

C．如果您的 WAN 口线路所用的连接方式是动态获取地址线路，在“类型”下拉菜单中，选中“动态获取地址线路”。配置的参数都是由 ISP 提供的。举例如下：

1、“主机名”，请根据 ISP 的具体需求填写。提示：某些以太网动态获取地址线路服务提供商可能需要，通常留空。

2、“网络服务商”，例如申请的是电信的线路。

3、“线路带宽”，例如您申请的线路的带宽是 10M，那么请根据 ISP 提供的上行与下行速率的准确数值填写。例如上行填写 10,下行填写 10。

4、“MTU 设置”，保持默认设置“自动”。

5、“工作模式”，默认选择“启用 NAT 模式”，可以根据需要进行修改。

6、“通断检测”，默认选择“不启用”。

完成后点击“保存”按钮即可。

以上操作便完成了对路由器内网和外网的配置。

2.3.3 重新启动路由器

完成以上操作后，请将路由器重新启动，点击“系统工具”→“重新启动”选项，点击“确定”按钮。系统会提示您路由器开始重启，并且有进度显示，大约过 30 秒，system 灯匀速闪烁以后，路由器就进入工作状态了。

恭喜您！您已经完成路由器的配置。您可以在浏览器输入 www.dlink.com.cn 来测试路由器。如果您想对路由器有更多的了解，请您查看第三章“详细安装指南”。

第三章　详细安装指南

3.1 启动和登录

本产品默认 IP 地址为：192.168.0.1，子网掩码为：255.255.255.0，管理帐户是：admin，密码是：admin。在启动和登录以后，浏览器会显示本产品的 WEB 管理界面。如下图：

界面左侧菜单栏里有如下选项：“系统状态”、“基础设置”、“上网行为管理”、“USB 扩展应用”（DI-7100 和 DI-7200 具有）、“网络安全”、“流量控制”、“高级选项”、“VPN”、“系统工具”等，单击某个选项，即可进行相应的功能设置。下面将详细讲解各个选项的功能。

3.2 系统状态

3.2.1 系统信息

通过“系统信息”界面可观察路由器的状态信息、版本信息、连接数排行等。

路由器运行时间：路由器的连续工作时间。本例中显示路由器已经工作了 13 分钟。

路由器负荷：路由器运行过程中当前的系统负荷。本例中显示当前系统负荷很小，是 5%，负荷在 0%－40%之间属于正常，在 40%-100%之间属于繁忙。

当前网络连接数：当路由器工作在 NAT 模式时，内网计算机出访会在路由器上产生 NAT 连接。NAT 连接数和网络流量是影响路由器负荷最关键的两个指标。本例中当前的 NAT 连接数是 2400 条，

当前活动主机数：显示当前内网通过路由器 NAT 以后访问外网的机器的数量。

网络连接限制：打开，表示“启用网络连接数限制”。该功能对内网每台主机能够占用的最大网络

连接数进行限制，以保证内网整体的可靠性和可用性。

网络防御拦截到：当在“网络安全”→“攻击防御”→“内网防御”中启用“内网病毒防御”和“广播风暴抑制”功能以后，路由器会显示当前拦截到的内网病毒包和广播包的数量，拦截这些包的主要目的是保证内网整体的可靠性和可用性。

网络攻击报警：路由器一旦遭遇来自内网或者外网的网络攻击，便会在此做出相应提示。方便网络管理员排查故障。

产品型号：路由器的型号。本例是 DI-7001

版本型号：路由器的当前固件版本。本例是 Beta 1017[2010-07-12 17:38:55]。

产品序列号：路由器的序列号。路由器序列号是每个路由器的唯一标识。

策略库版本：路由器内置的电信策略包和网通策略包，当前版本是 100706。点击“立即更新”按钮可以自动更新策略路由包的版本。

客户机网络连接数排行：在这里可以显示当前占用网络连接数最多的 10 台内网主机的排行情况。在正常使用情况下，单台内网主机的网络连接数在 300 以内，如果某台内网主机网络连接数长时间明显大于这个值，请检查该主机是否感染网络病毒。一旦某台内网主机作为服务器对外开放，则网络连接数会显著上升。可以通过“网络安全”→“攻击防御”→“网络连接数限制”功能对每台内网主机能够占用的最大网络连接数进行限制，以保证网络整体的可靠性和可用性。

在实际应用中，一台计算机正常情况下一般只有 10-50 条 NAT 连接。某些感染了蠕虫病毒或滥用 P2P 下载工具的内网计算机会对外发起众多的连接请求，严重干扰网络的正常运行，通过查看

客户机网络连接数排行榜，可以轻松定位到染毒主机，为网络故障的排查带来方便。如果染毒的内网主机网络连接数过大，需要及时将染毒主机断网并杀毒，从而保护其他主机的正常网络使用。

3.2.2 网络接口

显示路由器当前网络接口详细信息。

可以通过本界面观察路由器的广域网和局域网的连接状态以及接口信息。其中包括：设备接口的物理地址（MAC 地址），IP 地址，子网掩码，网关地址，接受/发送数据量等信息。对于 ADSL PPPoE 拨号线路，提供手动断开与连接按钮，并显示已连接的时间。

3.2.3 系统日志

本界面提供的功能是将网络日志和系统日志通过标准协议传输到日志服务器上进行保存。日志服务器使用“精简版本的 DI 日志服务器”软件接收日志数据。

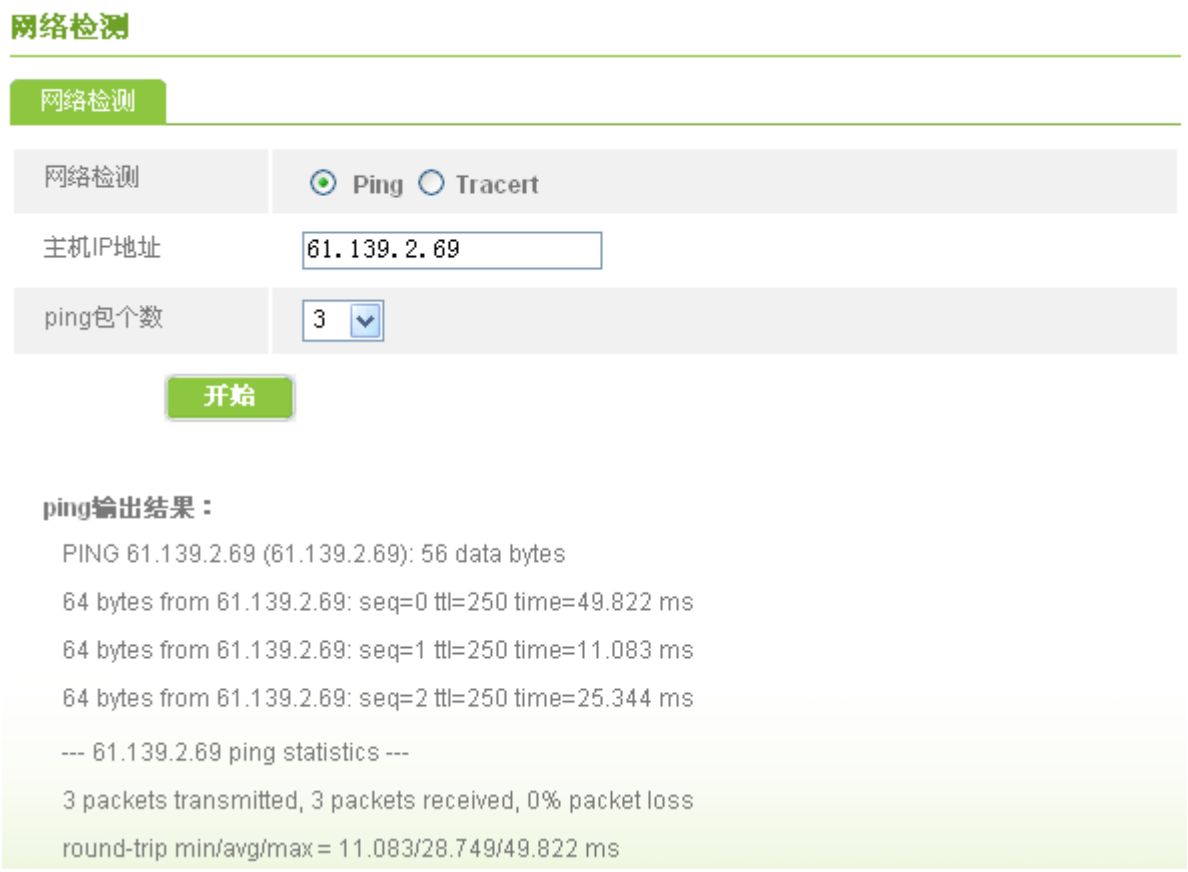
启用系统日志服务：启用并保存后，重启路由器，将会在本界面中的“系统日志”选项看到系统日志。

启用日志服务器：指定日志服务器的 IP 地址，在日志服务器上结合“精简版本的 DI 日志服务器”软件接收网络日志信息。

如果在路由器上查看系统日志信息，点击“系统日志”即可。如下图所示：

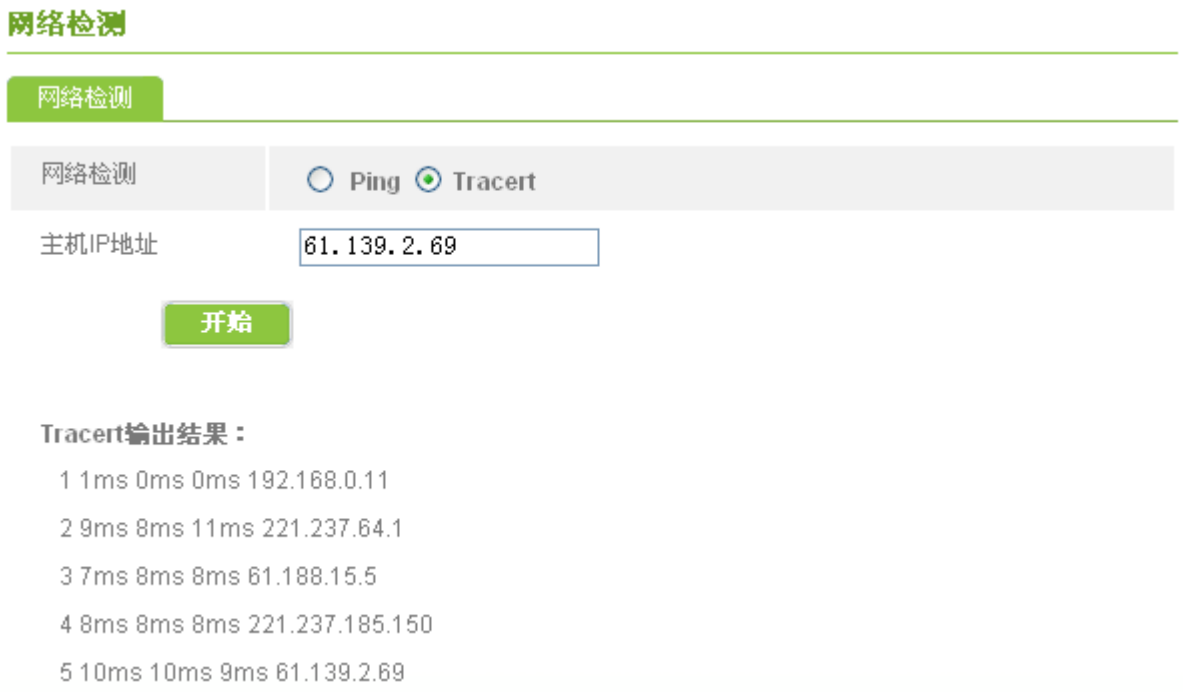
3.2.4 网络检测

本界面提供两个使用频率最高的网络命令，ping 和 tracert，命令的发起端都是路由器。使用 ping 可以检测目标地址是否可以到达。例如，ping 61.139.2.69 的结果如下图所示：(ping 包个数选择 3 个)



由于 61.139.2.69 是一个外网地址，根据使用 ping 命令的结果得出的结论是：从路由器发出的数据包可以到达外网，并且路由器可以收到外网回应的数据包，说明外网是通的；只要路由器没有配置任何限制规则，内网的用户就可以通过路由器上网。

再举个例子来说明 tracert 的使用情况， tracert 61.139.2.69 的结果如下图所示：



3.2.5 内网监控

内网监控功能采用高速网络流量采集和分析技术，精确统计内网每个 IP 的累计流量、实时速度、网络连接数等关键指标，并可以按任意指标排名分析；实时分析各 IP 的网络连接详情，轻松掌握网络资源分配情况，定位问题易如反掌。

内网监控的“管控”功能可以一键禁止内网异常活动 IP 上网。

启用内网分析：将分析服务状态选择为“启用”，并保存。如下图所示：

排序方式：可以将内网的活动主机按照累计下载、累计上传、下载速度、上传速度、网络连接数等指标排名，本例是按照主机 IP 地址排名。点击绿色字体“主机”即可。通过 IP/MAC 的“描述”选项可为内网的主机添加主机名，如下图：

管控：当您发现某个 IP 活动异常时，可以使用管控功能，单击管控列的绿色按钮即可一键阻断其访问外网。

当您阻断某个 IP 地址上网后，您可以在禁止列表中看到该 IP：

当您删除所有规则以后，此 IP 地址又可以正常上网了。

刷新：点击“刷新”按钮后，路由器更新在线 IP 的上下行速率和连接数信息。

通过点击相应的主机 IP 地址或者该主机的网络连接数，可以查看该主机的 NAT 连接数详情。点击“192.168.1.195”出现如下图所示的界面：

主机分析结果

协议	源地址		目标地址	连接时间
TCP(http)	192.168.1.195:2008	<-->	192.168.1.236:80	2009-02-11 16:27:31
TCP(http)	192.168.1.195:2007	<-->	192.168.1.236:80	2009-02-11 16:27:29
TCP(http)	192.168.1.195:2006	<-->	192.168.1.236:80	2009-02-11 16:27:29
TCP(http)	192.168.1.195:2005	<-->	192.168.1.236:80	2009-02-11 16:27:28
TCP(http)	192.168.1.195:2004	<-->	192.168.1.236:80	2009-02-11 16:27:27
TCP(http)	192.168.1.195:2003	<-->	192.168.1.236:80	2009-02-11 16:27:22
TCP(http)	192.168.1.195:2002	<-->	192.168.1.236:80	2009-02-11 16:26:41
TCP(http)	192.168.1.195:2001	<-->	192.168.1.236:80	2009-02-11 16:26:40
TCP(http)	192.168.1.195:2000	<-->	192.168.1.236:80	2009-02-11 16:26:31
TCP(http)	192.168.1.195:1999	<-->	192.168.1.236:80	2009-02-11 16:26:27
UDP(unknow)	192.168.1.195:4000	<-->	219.133.48.100:8000	2009-02-11 16:26:19

3.2.6 报文捕获

报文捕获功能提供在路由器上直接抓取经过路由器 LAN 口或 WAN 口的数据包，便于分析当前网络运行情况。如下图所示：

数据包文件：点击“开始抓包”后，被捕获的数据包会形成名为 packet.cap 的文件，该文件可以使用 wireshark（ethereal）等软件打开。

类型：希望捕获哪种类型的数据包。可选项有，ARP、ICMP、TCP、UDP 或者 ALL（全部类型）。默认捕获全部类型的数据包。

源 IP 地址：被捕获的数据包的源地址。

目标 IP 地址：被捕获的数据包的目的地址。

源端口与目标端口：被捕获的数据包的源端口与目的端口。

接口：希望捕获哪个接口的数据包。可选项有 LAN、WAN、ALL（全部）。

数量：每次捕获数据包的个数，每次最多可以捕获 1000 个数据包。设置并点击“开始抓包”后，系统会提示剩余包个数，当剩余包为 0 个时，系统自动停止本次抓包。

3.3 基础设置

3.3.1 配置向导

通过快速配置向导可以轻松地完成上网所需要的基本设置，直接点击“下一步”进行操作，按照系统提示正确输入参数即可。

3.3.2 基本选项

本界面包含路由器系统的一些基本配置信息，通常情况下，基本选项保持默认配置即可。如下图所示：

注意：如果您将本界面的配置参数（除手动设置时间）做了修改以后需要重新启动路由器才生效。

主机名称：路由器的名称。可以在这里给路由器设定一个名称，默认是 router

域名：路由器作为内网 DHCP 服务器时所使用的名称。

时间服务器地址：路由器通过时间服务器获取准确的系统时间。

手动设置时间：如果时间服务器故障导致不能正常更新路由器系统时间，用户可以自己设置时间。

最大数据分段：对于某些特殊地区的 ISP，用户只有手动设置最大数据分段以后才能更流畅地使用网络。最大数据分段的范围是 536-1460 字节，通常情况下保持默认即可，错误的数据分段会导致您的网络无法正常使用。

支持端口回流：当您访问内网主机对公网提供的服务时，可能出于习惯使用路由器 WAN 口 IP 地址进行访问，此时就需要端口回流功能来支持您的应用，打勾表示启用此功能；如果不启用此功能您

只能使用服务器内网 IP 地址访问内网服务器。

阻止共享检测：可用于避免某些 ISP 网络尖兵共享检测封锁。

H323 穿透：启用该功能后，内网用户可以使用基于 H323 协议的语音业务，如 netmeeting 等。

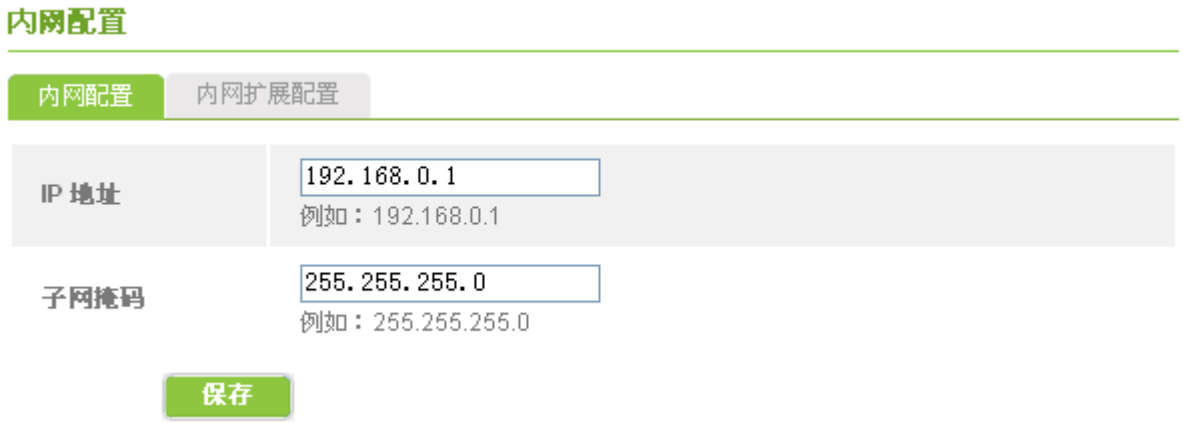
VEF(高速转发功能)：开启高速转发后，会提高路由器的性能，建议开启该功能。

高性能模式：启用该功能后将会失去内网监控、报文捕获、聊天软件过滤、P2P 软件过滤、病毒检测、应用调度等高级功能，从而在高负荷网络环境得到更好的性能表现，该功能重启生效！

3.3.3 内网配置

本界面用于配置内网接口参数，如下图所示：

注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。



IP 地址：设置路由器内网口的 IP 地址，这个地址就是内网计算机的网关地址。该地址出厂时设置为 192.168.0.1，可以根据需要改变它，如果改变了路由器内网 IP 地址，重新启动路由器后才能生效。重启成功后，必须用新设置的 IP 地址才能登录路由器进行 WEB 界面管理。局域网中所有主机的 IP 地址需与路由器内网口 IP 地址在同一网段，并且默认网关设置为路由器内网口 IP 地址才能正常上网。

子网掩码：根据内网规模选择，一般填 255.255.255.0 即可。路由器默认使用的子网掩码是 255.255.255.0，可以根据需要更改。

内网扩展配置：本路由器内网口允许配置多个 IP 地址，当内部有多于一个子网时可能会使用到该功能。可以在“内网扩展 IP 地址”中添加 16 个地址，其功能与路由器内网地址基本一致，通常作为相应子网的网关使用。

3.3.4 外网配置

本界面用于配置 WAN 口的接口参数。WAN 口支持三种连接方式，静态地址线路、PPPoE 拨号线路、动态获取地址线路。

注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。

1．静态地址线路

IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，可以向网络服务商询问获得。

子网掩码：当前 IP 所对应的子网掩码，由网络服务商提供，可以向网络服务商询问获得。

缺省网关：当前 IP 所对应的网关，由网络服务商提供，可以向网络服务商询问获得。

DNS 服务器 1/DNS 服务器 2：填入网络服务商提供的 DNS 服务器 IP 地址，可以向网络服务商询问

获得。

网络服务商：您申请线路的 ISP，例如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN 口静态线路的带宽，可以向网络服务商询问获得。

MTU 设置：MTU（最大传输单元），系统默认使用 1500 字节。通常情况下这个参数不用设置，保留“自动”即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

工作模式：本路由器对于 WAN 口提供三种工作模式。

1．NAT（网络地址转换）模式。如果内网使用了一个私有的网络地址段，例如 10.x.x.x/172.16.x.x/192.168.x.x，并且需要访问互联网，则路由器需要工作在 NAT 模式下。路由器工作在 NAT 模式时，内网中的出访数据包的源地址将被转换为路由器 WAN 口配置的合法 IP 地址。目前绝大多数用户使用的是这种工作模式。

2．路由模式。如果内网的主机全部是合法的公网地址，可以配置路由器工作在路由模式下。路由器工作在路由模式时，内网中出访数据包的源地址将使用本机的合法公网地址，不会被转换为路由器 WAN 口配置的 IP 地址。目前使用这种工作模式的客户比较少。

3．透明桥模式。WAN 和 LAN 之间通过 ARP 代理实现伪网桥。

4．桥接模式。WAN 和 LAN 之间实现纯网桥功能。

2．PPPOE 拨号线路

PPPOE 帐号：填入网络服务商提供的 PPPOE 线路帐号，可以向网络服务商询问获得。

PPPOE 口令：填入网络服务商提供的 PPPOE 线路口令，可以向网络服务商询问获得。

按需拨号：当使用计时收费类型的 PPPOE 线路时，可以配置这个功能。配置该功能后，如果内网有上网请求，路由器会自动拨号连接，无需人工干预；PPPOE 线路空闲的时间达到设定的值后，系统自动切断 PPPOE 线路，节省费用。这个值应大于 30 秒，通常设置为 300 秒（5 分钟）。

网络服务商：您申请线路的 ISP，例如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN 口 PPPOE 线路的带宽，可以向网络服务商询问获得。

工作模式：参考静态线路说明，默认使用“NAT 模式”。

3．动态获取地址线路

主机名：某些提供以太网动态获取地址线路的网络服务商可能需要，可以向服网络务商询问获得。

网络服务商：您申请线路的 ISP，例如中国网通或者中国电信。如果选择“不指定”，则该线路需与静态路由功能配合使用。

线路带宽：申请的 WAN 口以太网动态获取地址线路的带宽，可以向网络服务商询问获得。

MTU 设置：MTU（最大传输单元），系统默认使用 1500 字节。通常情况下这个参数不用设置，保留“自动”即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

工作模式：参考静态线路说明，默认使用“NAT 模式”。

3.3.5 DHCP 服务器

本界面主要提供 DHCP 服务器功能。如果内网计算机的 TCP/IP 协议配置为“自动获得 IP 地址”，并且在内网没有 DHCP 服务器的情况下，可以使用该功能。

DHCP 是 Dynamic Host Configuration Protocol（动态主机配置协议）的缩写，它是 TCP / IP 协议簇中的一种，主要是用来给网络客户机分配 IP 地址。这些被分配的 IP 地址都是 DHCP 服务器预先保留的一个由多个地址组成的地址集，此地址集一般是一段连续的地址。

起始 IP 地址：DHCP 服务器自动分配的内部 IP 的起始地址。

结束 IP 地址：DHCP 服务器自动分配的内部 IP 的结束地址。

默认网关：DHCP 服务器给客户机分配的默认网关地址。

DNS 服务器 1/DNS 服务器 2：分配的 DNS 服务器地址。

租期（分钟）：设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间，系统默认留空。如果留空，租期默认为 60 分钟。

绑定：启用自动绑定 IP/MAC 功能后，路由器会自动绑定已分配的 IP 地址与相应主机的 MAC 地址，避免内网由于 ARP 欺骗所带来的掉线问题。

当前内网 DHCP 服务器： 当此路由器作为一台 DHCP 服务器时，它会主动探测同一局域网是否也存在其他 DHCP 服务器，如果有则显示其 IP 和 MAC 地址，避免 DHCP 服务冲突。

可以使用地址池分配功能为内网 PC 分配一个地址段。

DHCP 服务器支持静态 IP 地址分配。如果希望内网某台主机每次启动以后都会获取 DHCP 服务器分配的同一 IP 地址，可以使用此功能。

例如：内网有台计算机的 MAC 地址是 **00:01:02:03:04:05**，希望它每次启动以后都会获取 IP **192.168.0.2**。首先，点击“添加新规则”添加一条规则；然后填写相应的 IP 地址与 MAC 地址，并保存。配置的结果如下图所示：

您也可以批量的添加静态地址，如下图：

添加并保存后显示：

3.3.6 DHCP 地址池

DHCP 地址池显示路由器的 DHCP 服务当前状态。可以看到的信息有，已经分配的 IP 地址、该 IP 所对应的 MAC 地址、获取该 IP 的计算机名称、IP 地址租约到期时间。如下图所示：

3.3.7 端口管理

端口管理功能可以调整路由器 WAN 口的工作模式，改变路由器内网口与外网口的 MAC 地址。

注意：如果您将本界面的配置参数做了修改以后需要重新启动路由器才生效。

接口模式：可以调整路由器 WAN 口的工作模式。提供四种工作模式供选择：10M 全双工模式、10M 半双工模式、100M 全双工模式、100M 半双工模式。通常情况下网络接口之间自动协商工作模式，用户不需要手动配置，保留“自动模式”即可。也可查看其中某一端口的数据统计：

WAN1数据即时统计

接收数据包	174237
接收丢弃包	0
接收错误包	0
发送数据包	10471
发送丢弃包	0
发送错误包	0

MAC 克隆：可以修改 LAN 口和 WAN 口的 MAC 地址，留空表示使用系统默认的 MAC 地址。某些网络服务商将提供给您的线路同某一个固定的 MAC 地址绑定起来，在这种情况下，MAC 地址克隆就非常有用。

3.4 上网行为管理

3.4.1 IP 地址组

IP 地址组：用于将 IP 地址进行分组管理。这个 IP 组可以是内网的 IP 段，也可以是公网的某些 IP 段。设置好的 IP 组将与上网行为管理的各个子功能配合使用，可用于定义源 IP 或者目的 IP。

例如企业研发部的 IP 段：192.168.0.20-192.168.0.30，将研发部配置为一个 IP 组的方法是，点击“添加新规则”。

1、 组名称：yanfabu

2、 IP 段：192.168.0.20-192.168.0.50，点击“添加”按钮。

3、 描述：添加注释“研发部”。

4、 点击“保存”后出现如下的界面。

类似地，可以添加企业行政部、市场部，或者添加一组外网的不安全 IP 段 221.50.50.0-221.50.50.254。

3.4.2WEB 访问控制

WEB 访问控制功能将大多数热门网站进行分类，用于对外网网站的访问进行管控，杜绝员工访问与工作无关网站。例如：市场部同事由于业务需要，工作时间可以访问所有网站；但是在工作

时间只允许其他部门员工访问合作伙伴网站 www.abc.com，而不允许访问其他网站。配置如下：

1、 将“启用功能”打勾。

2、 在白名单中添加 www.abc.com。

3、 将“休闲娱乐”→ “其他网址”的所有分类全部“阻断”。

4、 点击“保存”按钮。

阻断：启用后，禁止用户访问“被阻断网站”，并将网址自动跳转到指定页面。

记录：启用后，日志会记录某个 IP 什么时候访问过哪些网站。

警告：启用后，当用户访问“被警告网站”时，浏览器会显示警告信息。

跳转地址设置：当内网用户试图访问被禁止的网站时，浏览器自动跳转到用户设置的域名地址。

在例外 IP 地址组，可以添加不受以上规则约束的 IP 地址组。如：市场部

此时，市场部同事可以访问所有的网站，而其他组的同事只能访问 www.abc.com。

3.4.3 WEB 安全

WEB 安全可以实现禁止内网用户在论坛发帖、防止企业信息外泄；禁止用户下载指定扩展名（例如 exe；torrent）的文件、禁止用户访问 URL 包含指定关键字的网站等功能。

例如禁止除了市场部（shichangbu）的所有计算机在论坛发帖、下载扩展文件名为.exe、.torrent 的文件、访问 URL 包含 bbs、org 的网站。配置方法如下：

1、 将“启用 WEB 安全功能”打勾。

2、 将“shichangbu”添加到例外 IP 地址组。

3、 将“禁用 WEB 页面提交”打勾。

4、 过滤文件扩展类型填写：torrent,exe。（用英文的逗号分隔）

5、 过滤的 URL 关键字填写：bbs,org。（用英文的逗号分隔）

6、 点击“保存”按钮。

禁用 WEB 页面提交：启用该功能后，内网用户（除市场部外）不能在论坛发帖。

3.4.4 电子公告

电子公告功能将按照您设置的公告周期定时向内网用户发送您所设置的公告内容，用户可以通过浏览器查看到公告内容。

3.4.5 聊天软件过滤

聊天软件过滤提供对 QQ、MSN、飞信、SKYPE、阿里旺旺软件的过滤。对于 QQ 的封锁，除了可以封锁 QQ 通过代理登陆外，还可以针对 QQ 号码封锁，允许例外的 QQ 号码登陆。

由于某些 P2P 软件或者聊天软件的版本不同或是有更新，可能应用软件过滤功能会对该版本的软件失效，我司会不定期更新软件特征库，确保过滤功能对绝大多数的软件版本有效。

例如禁止所有计算机使用 QQ、MSN、飞信、SKYPE、阿里旺旺等聊天软件，并且只允许市场部登陆工作 QQ12345678、23456789，其余私人 QQ 不能登陆。配置方法很简单，首先启用“聊天软件过滤”，然后对禁止使用的聊天软件选择“开启”，并保存即可。如下所示：

1、 点击“例外的 QQ 号”，添加新规则。

2、 输入允许使用的 QQ 号码 12345678 和 23456789，并添加注释。

3、 点击“保存”按钮。

完成后界面如下图所示：

批量添加功能可通过复制→粘贴，一次添加多条记录。

3.4.6 股票软件过滤

股票软件过滤可禁止内网用户使用大智慧、钱龙、同花顺、证券之星、指南针等股票软件。例如禁止内网用户使用几款热门股票软件。

3.4.7 P2P 软件过滤

例如禁止内网的所有用户组使用迅雷、电驴、BT、PPLIVE/PPSTREAM 等 P2P 软件和在线视频软件。

3.4.8 网页游戏过滤

可禁止内网用户玩开心网、QQ 农场等网页游戏，简单配置如下：

3.4.9 防火墙设置

本界面提供了 D-Link 路由器内置的高性能防火墙的配置。防火墙访问控制规则一旦设置后，路由器将运用所配置的规则来匹配报文中的相关信息，决定允许或者拒绝报文通过。

例如禁止市场部（shichangbu）的计算机在每周二、周三的 9:00-10:00 禁止访问 virus 组的所有服务。点击“添加新规则”，在出现的界面中这样配置：

1、 不使用：保持默认，不勾选。若勾选，则本条规则配置后不生效。

2、 动作：禁止。

3、 接口：LAN。

4、 协议：ALL[ALL/1-65535]

5、 目的端口范围：当协议为 ALL 时，目的端口范围默认为所有端口。

6、 目的地址组：选择下拉菜单“virus”

7、 源地址组：选择下拉菜单“shichangbu”

8、 时间：9:00-10:00

9、 工作日期：周二、周三

完成后点击“保存”即可。如下图所示：

注意：规则的匹配顺序是从上到下，一旦匹配了一条规则就会马上执行，下面的规则不再进行匹配。因此一般将比较细化的规则放在上面，可以使用“上下移动”键来调整规则顺序。

如果想让内网的用户通过路由器仅能收发邮件，不能浏览网页、聊 QQ 等，可通过“一键添加”功能快速配置：

3.4.10 WEB 认证

WEB 认证功能只允许通过认证的内网用户上网，禁止未授权用户访问互联网。认证方式可分为身份认证（用户名+密码）、MAC 地址认证、IP 地址认证等方式。

启用 WEB 认证：即打开该功能的总开关。

启用身份认证时，需在路由器上配置合法用户的用户名以及密码。打开 WEB 认证总开关后，内网用户用浏览器尝试访问 www.163.com 时，会弹出认证界面，此时需输入登记的用户名和密码，通过认证，该用户才可以上网。

可通过批量添加用户输入框，复制→粘贴多个用户。

启用 MAC 认证后，内网用户的 MAC 地址若与列表内的 MAC 地址相同，则该用户可直接通过路由器上网。

启用 IP 认证后，IP 认证组里的用户可直接通过路由器上网。例如，只允许 192.168.1.48 上网。

通过 Web 认证用户信息，可以看见目前认证成功用户的相应信息，如下图：

3.5 USB扩展应用

当正确接入 USB 移动存储设备时，本界面会显示存储设备的状态信息。在断开 USB 移动存储设备之前，建议先点击“移除”按钮，可更安全地卸载 USB 设备。

3.5.1 设备状态

3.5.2 共享服务

启用 USB 共享可以使局域网用户共享 USB 设备上指定目录中的资源。具体配置界面如下图所示：

系统根据用户使用权限，分别设置了“共享目录”和“私有目录”。直接将 USB 移动设备插到路由器上后，路由器会在 USB 设备上自动建立目录。

共享目录：用户可直接登录，可对共享目录中的资源进行访问、添加和删除操作。

私有目录：用户登录时需要输入设置的用户名和密码，默认用户名为 login。登录私有目录后，可对私有目录中的资源进行访问、添加和删除操作。

3.6 网络安全

3.6.1 攻击防御

D-Link 路由器的网络自防御机制能够侦测及阻挡 ARP 欺骗，源路由攻击，IP/端口扫描，DoS 等网络攻击，可以有效防止多种病毒攻击。

ARP 欺骗防御保护：内网 ARP 欺骗保护功能，请使用默认配置。

广播风暴抑制：在一个布局不合理的局域网中或者局域网有某些病毒时，内网会有很大比例的广播包，大量广播包会导致内网速度变慢，运行不稳定。此功能通过拦截内网的大量广播包来保证内网的稳定运行。

内网病毒防御：此功能可以阻断来自内网中毒计算机对路由器的攻击。

过滤未知协议：如果“启用”，路由器可以阻止来自 LAN 口的特殊类型的乱包攻击。

Syn-flood 攻击防御/ udp-flood 攻击防御/ icmp-flood 攻击防御：防御来自内网的针对路由器的 DoS 攻击。建议保持默认配置。

禁用内网诊断：默认启用。可在路由器负荷比较高的环境下对路由器进行调试。

响应外网 ping 请求：出于安全考虑，请保持默认“禁止”。选项如果启用，外网用户将可以 ping 通路由器的 WAN 口地址，这样配置会增加风险。

阻断外网请求：默认选择“禁止”。如果启用，外网用户将不能访问内网的虚拟服务器。

外部开放端口保护：保护内网的虚拟服务器。使内网虚拟服务器在受到来自外网的恶意攻击的情况下，不至于瘫痪，确保网络整体的正常运营。

外网 ARP 公告：主动发送 ARP 更新信息，可解决一些与 ISP 直连设备 MAC 地址更新缓慢的问题。

3.6.2 连接限制

通过网络连接数限制功能，可以设置内网每台计算机能够使用的最大连接数，每台主机 300 条连接数是一个标准值。

连接限制功能既可以统一对内网的所有计算机进行最大 NAT 连接数限制，也可以单独限制某些特殊功能计算机（例如服务器）的最大连接数，还可以启用高级连接数限制，保证某些游戏更加快速地连接到服务器。该功能针对网络实际的应用情况，更加合理地分配连接数资源，有效的保证内网整体的可用性与可靠性。

例如配置内网每台计算机的连接数为 300 条，并且启用高级连接数限制，内网 DMZ 主机 192.168.0.99 连接数为 10000 条，UDP 连接数 300 条，内网段 192.168.0.22-192.168.0.24 的几台 web 服务器的连接数为 1000 条，UDP 连接数 300 条。结果如下图所示：

3.6.3 IP/MAC 绑定

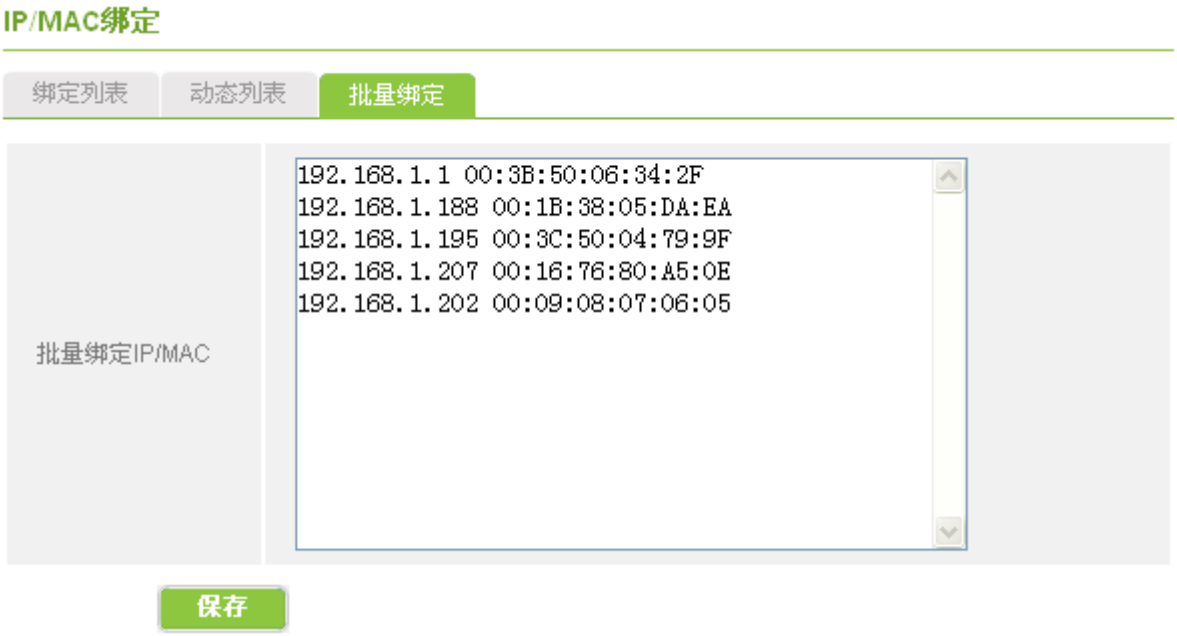
本功能用于实现内网计算机的 IP 地址与 MAC 地址之间的绑定。路由器的 ARP 映射表如果被更改，整个网络将陷于瘫痪。使用 D-Link DI 系列路由器集成的 IP-MAC 扫描工具，一键绑定内网计算机的 IP 和 MAC，可以极大降低因 ARP 欺骗造成的“掉线”故障。

地址绑定一旦配置完成后，指定的 IP 地址就只能被指定的计算机使用，解决了局域网中 IP 地址被随意改动而导致的 IP 地址冲突。另外也可以通过选中“禁止未绑定 ARP 信息的主机通过”选项来禁止所有未被绑定的计算机出访互联网。

点击“动态列表”→“扫描 MAC”，可以扫描出内网活动主机的 IP/MAC 地址，如下图所示：

该扫描列表中的主机可以被单台绑定或者全部绑定（点击“绑定所有 IP/MAC 项”）。

点击“批量绑定”，在此手动添加内网主机的 IP/MAC 项，IP 和 MAC 之间用一个空格分开。点击“保存”按钮，可以将绑定内容添加到绑定列表。



点击“绑定列表”，该列表显示目前已被绑定的内网主机的 IP/MAC 信息。

可以通过点击“编辑”图标为每条 IP/MAC 添加注释内容。

如果将“禁止未绑定 IP/MAC 的主机通过”打勾，则内网未被路由器绑定 IP/MAC 的计算机不能通过该路由器上网。

3.6.4 ARP 信任机制

ARP 信任设置的基本选项如下图：

启用 ARP 信任检测功能：启用 ARP 信任检测功能，路由器将自动对学习的 ARP 信息进行验证，保证路由器学习到正确的 ARP 信息。

启用 ARP 超时机制：在启用 ARP 信任检测功能后，可以开启超时机制，使路由器定期对已经学习到的 ARP 信息进行重新学习和验证，大大提高了路由器自动对 IP/MAC 表维护的正确性。

启用“ARP 信任检测功能”后，可以在信任列表里查看当前已被路由器信任的 IP/MAC 信息。“绑定所有 IP/MAC 项”可以将已信任的 IP/MAC 添加到绑定列表中，“删除所有 IP/MAC 项”可以清空该列表内容。

3.6.5 MAC 地址过滤

MAC 地址过滤功能可以禁止内网计算机上网。有时候可能需要禁止内网某些计算机上网，只要找到该计算机的 MAC 地址，在 MAC 地址过滤里添加一条规则，便可以实现。

例如：想禁止 MAC 地址是 00:01:02:03:04:05 的计算机上网。首先，点击“添加新规则”并填写计算机 MAC 地址，然后点击“保存”按钮，配置结果如下图所示：

3.7 流量控制

3.7.1 QoS 流量控制

流量控制功能可对内网每个 IP 或者网段进行带宽限制。它可以有效地防止 P2P 应用过渡消耗带宽资源。D-Link 独特的流控算法灵活分配剩余带宽，在“保障带宽”的前提下充分利用带宽总资源，进退自如的“弹性流控”即使在高负荷的大型网络中，也能充分体现其灵敏，高效，弹性的特点，且不影响路由器的整体性能。

在“功能配置”界面可以对流量控制的一些特性进行配置：

启用传统流控：传统流控功能总开关，启用该选项流量控制功能才会生效。

启用优先级流控：启用优先级流控之后可以在优先级流控规则中配置优先保障的重要应用，从而保证单机在带宽达到限制峰值的情况下部分数据优先传输，以保障企业关键业务的正常开展。

启用游戏优先保障：启用游戏优先保障后，路由器会对当前热门游戏，例如魔兽世界、跑跑卡丁车、劲舞团等游戏数据优先转发。

例如配置优先级流控，要求内网所有计算机访问网页的数据优先传输，配置的方法如下图所示：

不使用：本条规则配置后不生效，但规则并不被删除。

协议：可选项有 TCP、UDP、TCP/UDP 或者 ALL。本例为 TCP。

端口：目的端口范围。本例为 80 端口。

地址：规则生效的 IP 地址范围。本例为内网所有主机。

描述：可以为本规则添加注释。

完成后，点击“保存”，将出现如下所示的界面：

流量控制功能的典型应用

例如：内网有 253 台计算机，IP 地址范围是 192.168.0.2－192.168.0.254，申请的带宽是 6M，控制内网每台计算机的最大使用带宽为上行 50KB，下行 50KB，当下行带宽有剩余时，可使用更多带宽，且规则生效时间为上午 9:00-下午 18:00。

点击“规则列表”→“添加新规则”，在出现的界面中做如下的配置：

不使用：打勾表示不使用本条规则，规则并不被删除。

地址：需要做流量控制的计算机的 IP 地址。“类型”下拉菜单可以选择为一个网段或者一台主机。

上行限制：设置流量控制的上行流量，默认单位为 KB。

下行限制：设置流量控制的下行流量，默认单位为 KB。

上行模式、下行模式：在地址类型为“网段”的情况下，可以设置本网段的计算机每一 IP 地址使用设定的带宽或者本网段的计算机所有 IP 共享设定的带宽。

上行策略、下行策略：即是否选择“弹性流控”。

举个例子，内网 100 台计算机，申请的带宽是 10M，限制内网所有计算机上下行流量均是 80KB，策略配置为“仅能使用设定的带宽”，在只有 5 台计算机上网并且这 5 台计算机都在下载软件的情

况下，总带宽最多使用 5×80KB=400KB。也就是说还有接近 6M 带宽没有被使用，白白“浪费”了。如果策略配置为“当带宽有剩余时，可使用更多带宽”，这 5 台计算机就会充分利用之前“不属于”他们的 6M 带宽，于是获得更快的下载速度，当有其他计算机上网时，他们会将这 6M 带宽“公平地”交出，每台计算机在保证总带宽没有被占满的情况下，可以使用多余带宽，直到可使用带宽达到给它设定的最大值。

接口：单 WAN 口设备，选择任意。

时间：本规则生效的时间段范围。

描述：添加对于本条规则的注释。

点击“保存”按钮，出现如下的界面：

3.8 高级选项

3.8.1 端口映射

本界面提供端口映射的配置。端口映射又称虚拟服务器，当内网使用私有地址时，例如 10.x.x.x/172.16.x.x/192.168.x.x，外部网络无法直接访问内网中的服务器。通过在路由器上做端口映射，配置内网服务器的 IP 与端口以后，外部网络便可以访问内网服务器，从而使用内网提供的服

务。

例如：内网有 100 台计算机，已经配置好一台 FTP 服务器，它的 IP 地址是 192.168.0.5，如果想让外网用户也可以访问此服务器，可以这样操作：

点击“添加新规则”，做如下的配置：

不使用：打勾表示不使用本条规则，规则并不被删除。

外部端口：指定一个对外开放的端口，映射到内部服务器开放的端口上，外部端口可以指定为一个连续的端口范围，但是需与内部开放端口相对应。如果不指定，则外部端口与内部端口相同。填写范围 1－65535。

内部 IP：内网的服务器的 IP 地址。

内部端口：内网服务器提供的服务所使用的端口。内部端口可以指定为一个连续的端口范围，但是需与外部开放端口相对应。请参考“常见的端口和服务对照表”。

协议：服务器提供的服务所使用的协议，如不清楚是哪种协议，可以选择“TCP/UDP”。请参考“常

见的端口和服务对照表”。

映射线路：单 WAN 口设备，选择任意。

注释：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下的界面：

网络服务		使用协议	端口
ftp	文件传输	TCP	21
Ssh	安全远程管理	TCP	22
telnet	远程登录	TCP	23
Smtp	简单邮件传输	TCP	25
Time	时间同步	TCP	37
DNS	域名解析	UDP	53
www	网页浏览	TCP	80
POP3	邮局协议 3	TCP	110
Snmp	简单网络管理协议	UDP	161
CS server	CS 网络游戏	TCP	27015

常见的端口和服务对照表

3.8.2 静态路由

静态路由就是静态的路由表信息。在某些网络环境下，需要修改静态路由表，指定静态路由信息来实现正常通信。

例如：指定内网的主机访问 221.12.12.0/24 这个网络的资源从 WAN1 出去，WAN1 的网关地址是 61.121.13.1，可以按此操作：

点击添加新规则，做如下的配置：

不使用：打勾表示不使用本条规则，规则并不被删除。

目标网络地址：输入目标网络的网络地址。

掩码：目标网络地址的子网掩码，可以根据实际情况选择。

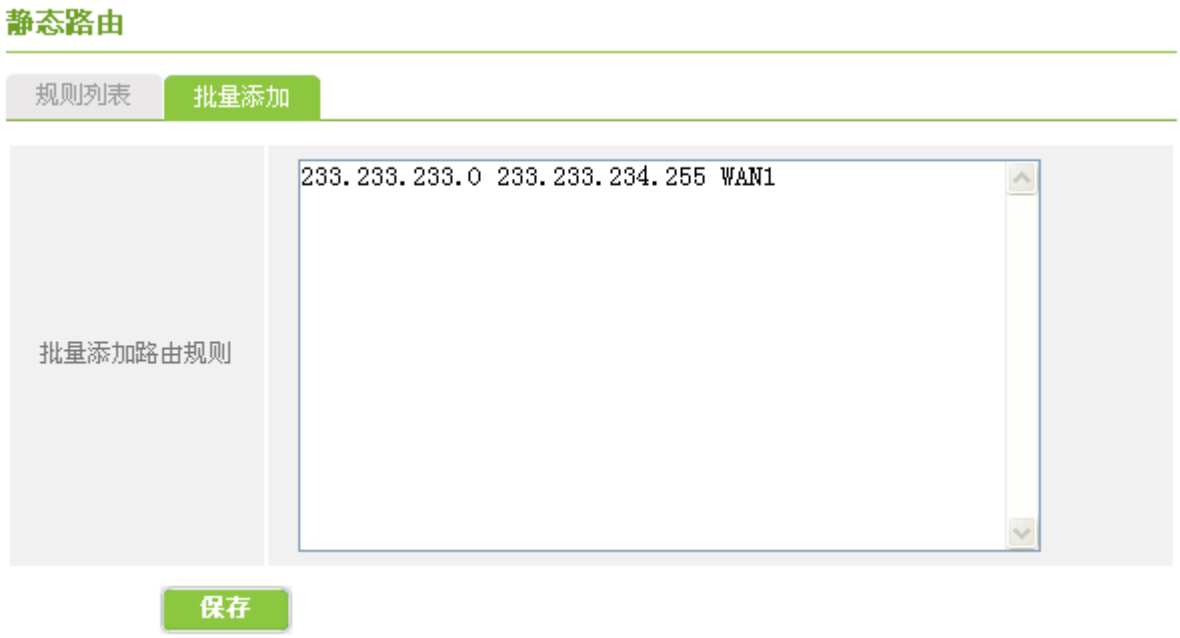
网关：输入与目标网络匹配的数据交付的网关地址，在本例是 WAN1 口的网关。

接口：指定数据交付的接口，在本例是 WAN1 口。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下的界面：

静态路由的批量添加功能可以快速地一次性添加多条静态路由规则。使用批量添加时请注意书写格式，例如 233.233.233.0 233.233.234.255 WAN1 每个条目之间用一个空格隔开，尤其注意 IP 地址一定要填写正确，否则错误的静态路由规则会导致您的网络不流畅，甚至无法使用。



点击“保存”按钮以后，所添加的静态路由信息会自动加载到规则列表中。

3.8.3 地址转换

随着 Internet 网络爆炸性的膨胀，IP 地址短缺及路由规模越来越大已成为一个相当严重的问题。

为了解决这个日益严重的问题，出现了多种方案。目前在应用中最有效的解决方案为网络地址转换(NAT)。

一个组织网络内部可以自定义其 IP 地址（不需要经过申请，即私有的 IP 地址，如 10.x.x.x/172.16.x.x/192.168.x.x），在本组织内部，各计算机之间通过私有 IP 地址进行通讯。而当组织内部的计算机要与外部 Internet 网络进行通讯时，具有 NAT 功能的设备负责将私有的 IP 地址转换为公网 IP 地址（即申请的合法 IP 地址）进行通信。简单地说，NAT 就是通过将私有 IP 地址转换为公网 IP 地址。

本界面的地址转换功能提供多对一转换和一对一转换两种模式。

1. NAT 外出规则

注意：此功能配置以后需要重新启动路由器才生效。

例如：内网有主网段 192.168.0.0/24，有一个扩展网段 192.168.1.0/24（已经在内网设置→内网扩展 IP 里配置）。外网单 WAN 接入，WAN 口光纤有 2 个 IP 地址，218.6.90.34 和 218.6.90.35，WAN 口已经配置了一个 IP 地址 218.6.90.34，默认情况下主网段和扩展网段的计算机 NAT 以后都用 218.6.90.34 出访；但是，如果想让扩展网段的计算机 NAT 以后用 IP 地址 218.6.90.35 出访，可以按此操作：

点击添加新规则，做如下的配置：

不使用：打勾表示不使用本条规则，规则并不被删除。

源地址：内网扩展地址已经在内网设置里面配置，所以不需要将“设为内网扩展地址”打勾。IP 地址和掩码请填写需要 NAT 转换的计算机的网段和掩码，本例是 192.168.1.1/24。

目标地址：需要访问的目的地址。“类型”可以选择“任意”或者“子网”。如果选择“任意”，表示源地址出访到任意目标地址的数据包都需要用转换地址做 NAT 出访。如果选择“子网”，则表示源地址出访到指定目标地址段的数据包才用转换地址做 NAT 出访。通常情况下这里保持默认配置。

转换接口：如果选择“不指定接口”，则必须填写转换地址，该地址是 ISP 提供的合法 IP 地址；如果指定相应的 WAN 口，则转换地址自动为当前 WAN 口 IP（仅用于 WAN 口是 PPPoE 情况）。本例选择“不指定接口”。

转换地址：NAT 以后，源地址使用填写的转换地址访问外网。这里可以填写一个地址或一个地址段，

设置地址段时，最大长度为 16 个地址。

注释：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下的界面：

2．NAT 一对一

本路由器通过 NAT 一对一的方式支持 DMZ 功能。这个功能可以使内网某台特定计算机向互联网完全开放，支持更多的网络应用。本路由器支持 DMZ 主机的数量只取决于您所拥有的合法 IP 地址的数量，如果一台 PC 设置成 DMZ 主机后，就完全暴露在公网上，这时候这台 PC 失去了 NAT 防火墙的保护，所以请谨慎使用。

例如：内网有网段 192.168.0.0/24，外网单 WAN 接入，WAN 口光纤有 2 个 IP 地址，218.6.90.34 和 218.6.90.35，WAN 口已经配置了一个 IP 地址 218.6.90.34，将内网计算机 192.168.0.4 作 NAT 一对一转换，外部地址选择 218.6.90.35，可以按此操作：

将标签切换到“NAT 一对一”，点击添加新规则，做如下的配置：

不使用：打勾表示不使用本条规则，规则并不被删除。

内部地址：填写主机的内部 IP 地址。

外部地址：填写一个外网 IP 地址用来作一对一的映射。请注意：填写的外网地址必须是网络服务商已经提供的合法的静态地址，否则 NAT 一对一功能无法实现。

转换接口：单 WAN 设备，选择默认。

规则描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下的界面：

3.8.4 域名转发

本界面提供域名服务功能，路由器直接向内网的计算机转发其域名缓存列表中的域名地址。域名转发工作的前提是“启用 DNS 缓存转发”功能。通过域名转发规则，可以将指定的域名同指定的 IP 地址绑定起来，在内网中生效，这个设置同外部网络的 DNS 解析没有关系。

例如：内网有台 WEB 服务器，IP 地址为 192.168.0.3，设定域名为 www.myweb.com 。设置内网所有的计算机的 DNS 值和内网网关相同。然后点击添加新规则，做如下的配置：

名称：填写内部主机的名称。

域名：指定内部主机的域名，注意：这个域名仅在局域网内网生效，并且需要开启 DNS 缓存转发功能。

IP 地址：填写内部主机的 IP 地址。

描述：可以在这里简单备注一下本条规则。

点击“保存”按钮，出现如下的界面：

重启路由器使域名转发功能生效后，您就可以在内网计算机的浏览器上输入 www.myweb.com 来访问内网的 WEB 服务器了。

3.8.5 动态域名

Internet 上的域名解析一般是静态的，即一个域名所对应的 IP 地址是静态的，长期不变的。动态域名的功能，就是实现固定域名到动态 IP 地址之间的解析。 因为 ADSL PPPoE 用户上网的时候分配到的 IP 地址都是动态的(每次重新拨号所获取的 IP 地址不同)，用传统的静态域名解析方法，ADSL 用户想把自己上网的计算机做成一个有固定域名的网站，是不可能的。而有了动态域名，这个美梦就可以成真。用户可以申请一个域名，利用动态域名解析服务，把域名与自己上网的计算机联系在一起，这样就可以很方便地搭建自己的网站。。

例如在www.3322.org上申请了一个动态域名xxxx.3322.org，用户名xxxx，密码 1234。具体的配置方法为：

点击“编辑”按钮添加一条规则，按照如下图所示的格式填写：

WAN1：启用动态 DNS 客户端后，本条规则才生效。

服务类型：选择提供动态域名服务的服务商类型，在本例是 3322.org

主机名称：申请的主机名称。

时限：某些服务商可能要求填写，本例中的服务商无时限要求。

用户名：申请动态域名时使用的用户名称。

口令：申请动态域名时使用的口令。

3.8.6 UPnP 设置

UPnP（Universal Plug and Play），通用即插即用，是一组协议的统称，不能简单理解为 UPnP=“自动端口映射”。在 BitComet 下载中，UPnP 包含了 2 层意思：

1、对于一台内网电脑，BitComet 的 UPnP 功能可以使网关或路由器的 NAT 模块做自动端口映射，将 BitComet 监听的端口从网关或路由器映射到内网电脑上。

2、网关或路由器的网络防火墙模块开始对 Internet 上其他电脑开放这个端口。

通过使用 UPnP，BitComet 等 P2P 软件可以获得更快的下载速度。

UPnP 的配置方法如下，点击“UPnP”设置，将“使用 UPnP”打勾，并保存。

点击“允许 IP 列表”，并“添加新规则”，在这里设置使用 UPnP 的计算机 IP 地址范围。例如设置 192.168.0.1-192.168.0.254 范围的计算机使用 UPnP 功能，配置的结果如下所示：

点击“UPnP”使用信息，可以查看当前的 UPnP 服务状态：

3.9 VPN

VPN（Virtual Private Network），即虚拟专用网络。它是通过一个公用网络（通常是因特网）在两个局域网或者工作站之间建立一个临时的、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。

有两种方法建立 VPN 连接，第一种是从计算机到 VPN 路由器，第二种是从 VPN 路由器到 VPN 路由器。

D-Link 路由器均支持这两种方法建立 VPN 连接。

3.9.1 PPTP 客户端

PPTP 客户端支持从 VPN 路由器客户端连接到 VPN 路由器服务端。例如：企业分支机构 A 与企业总部之间需要实现简单安全的信息互访，可以在分支机构路由器中使用 PPTP 客户端完成上述操作。具体配置方法如下：

启用 PPTP 客户端：打勾表示启用 PPTP 客户端功能。

PPTP 服务器地址：需要拨入的 PPTP 服务端地址。

用户名：使用的 PPTP 用户名，由服务端分配。

密码：用户名所对应的密码，由服务端分配。

PPTP 网段：通过 PPTP 隧道访问的网段，一般配置为 PPTP 服务端内网地址段。

PPTP 掩码：PPTP 服务端内网地址段掩码。

是否启用加密：根据服务端配置选择是否启用加密，保证服务器和客户端配置相同才可以正常通信。

做好上述配置之后，还需要在服务端配置“PPTP 用户管理”，客户端内网主机才可以通过 PPTP 隧道来访问服务端内网主机，从而实现内网互访。

3.9.2 PPTP 服务端

如果 PPTP 客户端要拨入服务端内网，则必须配置 PPTP 服务端。例如：企业员工出差在外，需要每天晚上将出差报告发送到主管的企业内部邮箱，同时收取企业内部邮箱里面的邮件，这时候就需要用到 PPTP VPN，出差员工通过 VPN 拨号进入企业内网来完成上述操作。具体的配置方法如下图所示：

启用 PPTP 服务：打勾表示启用 PPTP　VPN 服务端。

最大 PPTP 连接数：服务端最多支持同时拨入的 PPTP 客户端数量。系统允许 64 个不同用户同时拨入。

PPTP 服务端地址：服务端 LAN 口的 IP 地址。

PPTP 客户端地址范围：客户通过 VPN 拨进来以后，服务端给它随机分配的内网 IP 地址范围。此地址段设置应当与服务端内网地址在同一网段并且不要与内网产生地址冲突。

启用 128-bit 数据加密：支持 128-bit 数据加密功能，此配置必须服务端同客户端保持一致才能正常通信。打勾表示两端的通信会以 128-bit 密钥加密的方式进行。

拨入列表：您将在这里看到哪些用户拨入了 VPN，以及分配到的 IP 地址和他的拨入地址。

以上配置完成后，还需要在服务端新建 PPTP 用户。方法是点击“PPTP 用户”，点击添加用户。例如，用户名为 user1，密码 1234，如图所示：

保存后的界面如下图所示：

这时候，出差员工通过在自己的电脑上启动 VPN 客户端程序，使用 PPTP 服务端当前 WAN 口

IP 和相应的用户名、密码配置客户端，就可以通过拨入公司内网。

若企业分支机构 A 需要通过 VPN 拨入公司总部局域网，实现分支机构 A 内的所有计算机可以访问公司总部内网资源。可以通过如下的配置实现，在服务端配置用户名 user2，密码 1234，勾选“用户所在客户端为一个网络”，客户端网段与掩码分别填写分支机构 A 的内网网段和掩码。如下图所示：

保存后的界面如下图所示：

3.9.3 IPSec 网对网

IPSec 协议是网络层协议，是为保障 IP 通信安全而提供的一系列协议族。IPSec 针对数据在通过公共网络时的数据完整性、安全性和合法性等问题设计了一整套隧道、加密和认证方案。IPSec 能为 IPv4 网络提供能共同使用的、高品质的、基于加密的安全机制。提供包括存取控制、无连接数据的完整性、数据源认证、防止重发攻击、基于加密的数据机密性和受限数据流的机密性服务。

IPSec VPN 的配置方法如下：

启用 IPsec VPN ，并保存。

点击“IPSec VPN 隧道列表”，并添加新规则。

名称：IPSec 隧道名，请用英文字母开头。

主动连接：若在两个路由器之间建立 IPSec VPN 隧道，只需在其中一个启用主动连接即可。

本地隧道接口：选择使用哪个 WAN 口进行 IPSec VPN 连接。

本地网络/掩码：与该路由器的内网网段/掩码一致。

远程隧道地址：对端 WAN 口的当前 IP 地址，可以填写域名。

远程网络/掩码：与对端路由器的内网网段/掩码一致。

IKE 验证模式：默认为 IKE-PSK，两端的验证模式必须相同。

PSK 密钥：密钥由数字和英文字母组成，两端的 PSK 密钥必须相同。

保存后如下图所示：

在两端都配置完毕并保存后，IPSec VPN 会自动拨号。可以查看“隧道状态”查看拨号是否成功。

3.9.4 IPSec 点对网

D-Link 路由器支持客户机 IPSec 点对网拨入，此时客户端需要专用的 IPSec 拨号软件。软件填写参数必须与路由器相关配置一致，才可以正常拨入。

3.9.5 L2TP IPSec

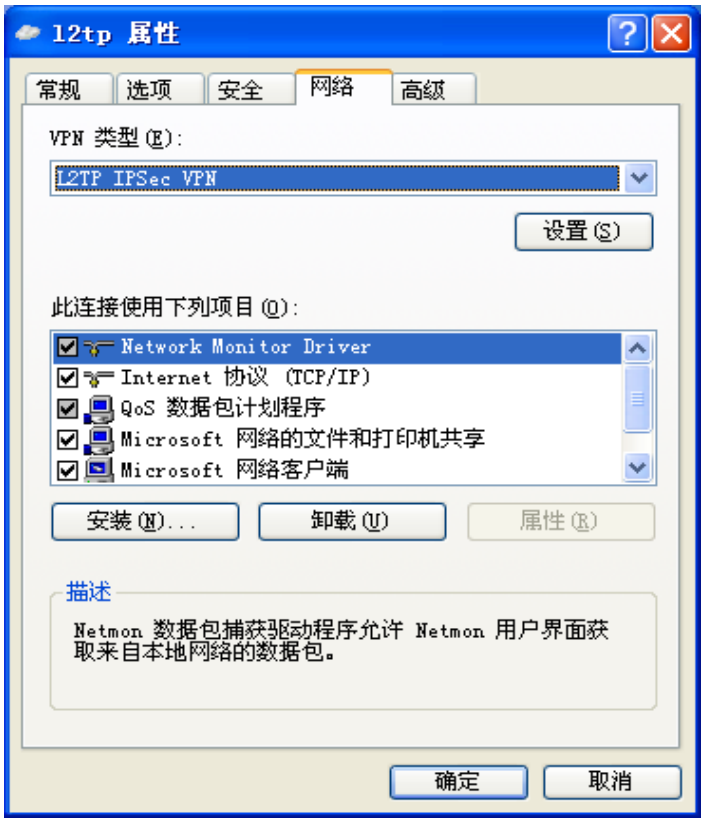
D-Link 路由器支持 L2TP IPSec VPN，这种方式的 VPN 与 PPTP VPN 相比，安全性更高。具体配置方法与拨号方法如下所示：

启用该功能，设置 PSK 密钥为 123456，客户端地址段为 192.168.0.100-192.168.0.105，与路由器的 LAN 口在同一个网段。

添加用户名 test，密码 test。

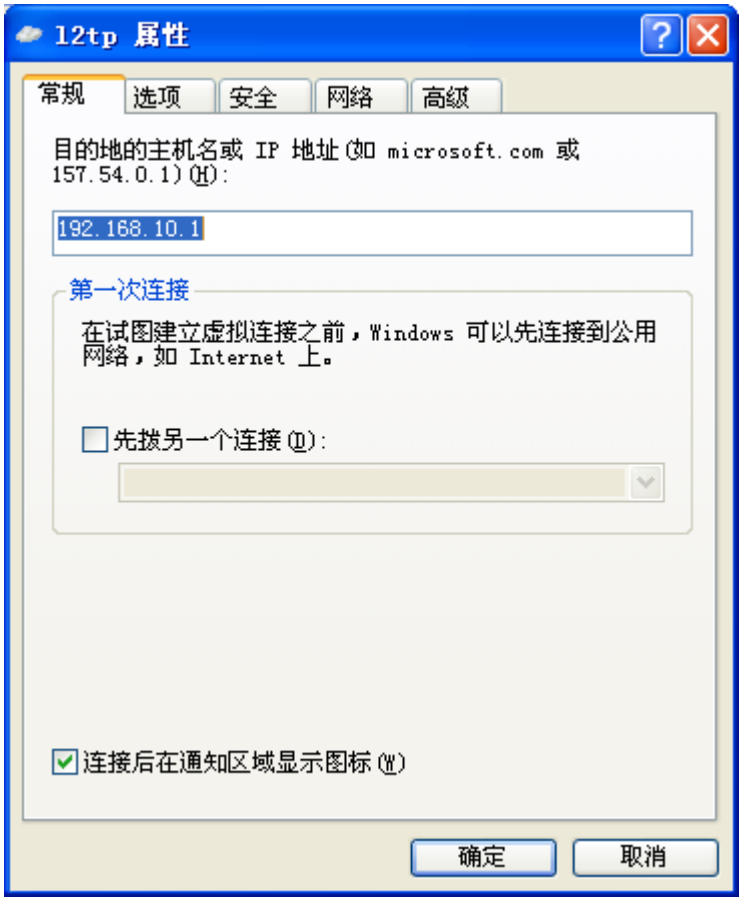
保存用户名和密码。

在 PC 机上的配置方法如下，注意“网络”标签下的“VPN 的类型”必须选择为“L2TP IPSec VPN”。



“安全”标签下的 IPSec 设置，密钥设置为 123456，与路由器上的设置保持一致。

“常规”标签下的目的地址设置为路由器的 WAN1 口 IP 地址。



填写用户名和密码，开始拨号。

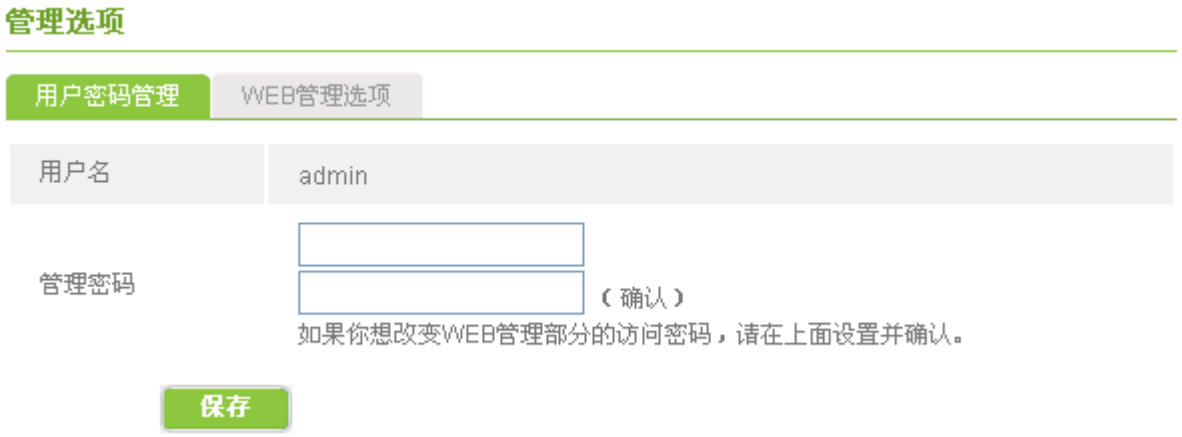
可通过“拨入列表”查看拨号是否成功

3.10 系统工具

3.10.1 管理选项

本界面提供修改路由器的 WEB 管理密码和 WEB 管理端口功能。

修改路由器 WEB 管理密码界面如下图所示：



点击“保存”后，所做的修改立即生效。

WEB 管理选项提供 WEB 管理端口的修改，WEB 管理 IP 的添加等功能。

管理地址：需要增加对路由器 WEB 界面访问的安全性时可以使用此配置。如果设置了管理地址，则除管理地址以外的其他地址不能访问路由器的 WEB 界面，如果此地址留空则所有地址主机都可以访问路由器的 WEB 界面。

WEB 管理端口：修改路由器的 WEB 管理端口（在路由器重新启动后生效）。系统默认使用 80 端口，如果要修改 WEB 管理端口，请注意不要用系统中已经使用的标准端口，例如 53 等，建议使用 8000－60000 之间的端口号。更改 WEB 管理端口后请牢记端口号。

允许外部使用 WEB 管理：如果希望外网可以通过 WEB 管理路由器，将“是否允许外部主机使用 WEB 管理”打勾，保存即可。请注意：开放路由器的外网 WEB 管理存在一定风险，请谨慎使用。系统默认不允许对外部主机开放 WEB 管理功能。

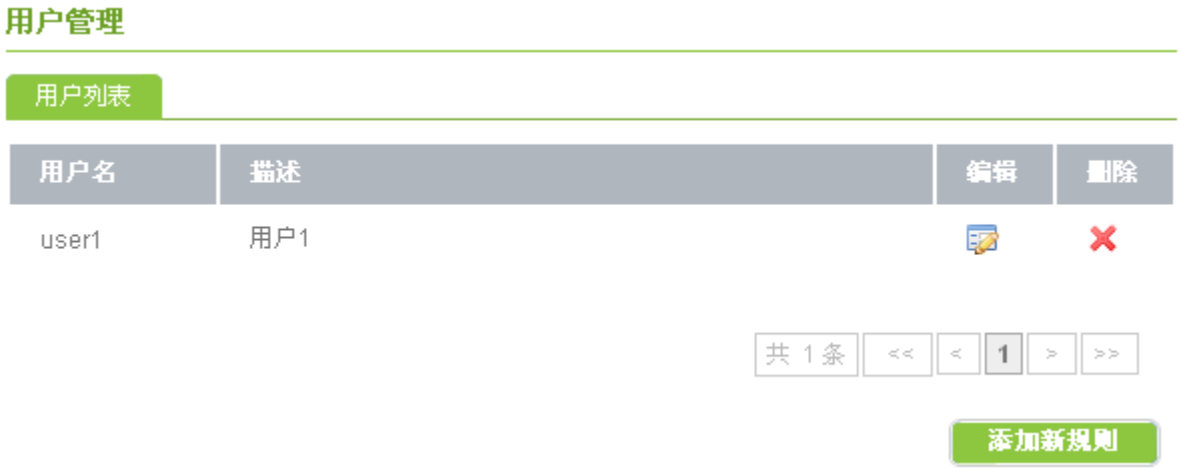
登陆保留时间：若设置时间为 5 分钟，使用 admin 打开路由器的 WEB 界面，5 分钟内不做任何操作，则再次访问路由器 WEB 时，系统要求重新认证。

显示行数设置：配置显示行数来修改系统日志、防火墙等列表每一页的行数。

3.10.2 用户管理

本界面提供的功能是添加 user 组，以便对路由器的访问权限实行分级管理。路由器将管理用户划分为 admin 组与 user 组。admin 组对路由器的配置有修改的权限，user 组只能查看路由器在运行过程中的重要参数，不能修改路由器的配置。这样大大提高了管理的安全性，减少了由于配置不当而引起的网络故障。

配置方法是，首先点击添加新规则，添加用户名，密码等；然后点击“保存”按钮，如下图所示，添加了一个用户名为 user1 的用户。通过使用 user1 用户与相应的密码登陆路由器的 WEB 管理界面，就可以查看路由器在运行过程中的一些参数。

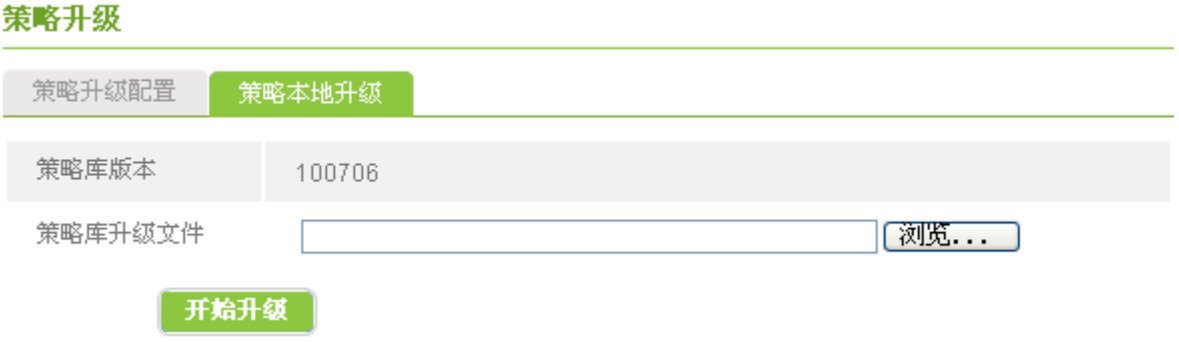


3.10.3 策略升级

本界面提供的功能是升级路由器的策略库，如策略路由引擎库、聊天软件特征库、P2P 软件特征库等，确保路由器对于聊天软件，P2P 软件的较新版本达到最佳封锁效果。建议配置为自动更新，并设置自动更新时间。

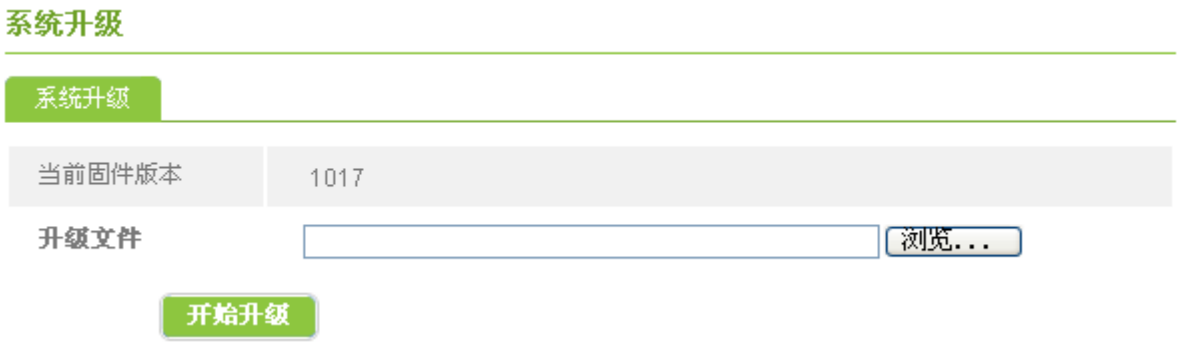
例如设置自动更新时间为每月的 1 号上午 10 时，可以做如下图所示的配置：

支持导入策略库文件离线更新策略库：



3.10.4 固件升级

本界面提供路由器的固件升级功能。路由器需要相应的软件才能提供各种丰富的功能。在厂家发布路由器的升级固件后，会提供一个固件升级包。通常情况下，新的固件升级包都可以得到更多的功能和更好的性能。在厂家的官方网站下载得到最新的固件升级包后，就可以使用“固件升级”功能给路由器升级固件。升级成功并自动重启后，就可以看到“当前固件版本”已经发生了变化。界面如下图所示：



当前固件版本：显示路由器的当前固件版本号。

升级文件：点击“浏览”按钮，指定路由器固件升级包在本地电脑中的位置。确定后，点击“开始升级”按钮。在升级的过程中系统有提示，大概 2 分钟完成升级，升级成功后路由器会自动重启。

注意事项：

1. 固件升级之前请确认固件升级包与设备之间是否匹配，不同型号的设备使用不同的固件升级包。
2. 升级过程请不要断开电源，否则升级无法完成。
3. 升级之前请重新启动路由器，启动正常后，断开外网连线。内网仅连接一台 PC 机，使用 IE 正常打开路由器 WEB 升级界面，选择正确的升级包操作。

3.10.5 备份恢复配置

本界面提供的功能是将路由器的所有配置保存为文件，如果因为操作不当导致配置出现错误时，可以使用原先保存的配置文件恢复配置。界面如下图所示：

保存配置：点击“保存配置”按钮，将路由器的所有配置保存为文件。

恢复配置：点击“浏览”按钮，指定原先保存的配置文件在本地电脑中的位置，确定后，点击“恢复配置”按钮开始恢复配置，恢复成功后路由器自动重启。

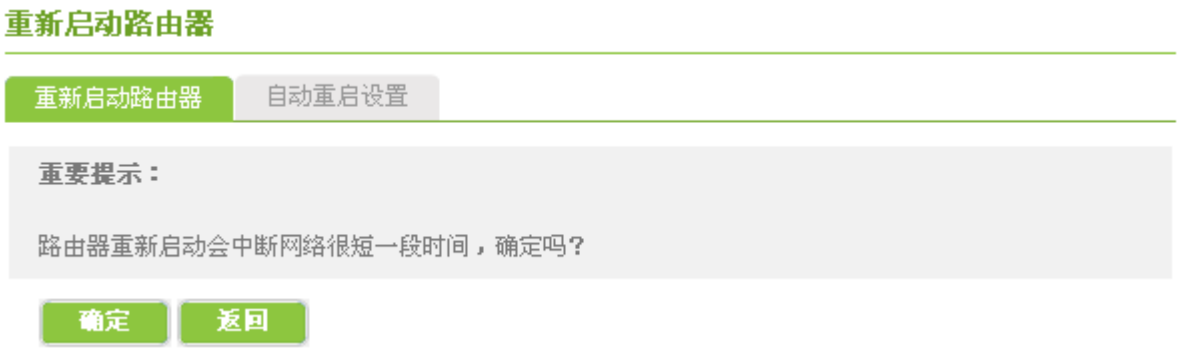
3.10.6 恢复出厂配置

本界面提供将路由器的所有配置清空，恢复到出厂配置的功能。它的效果和按一下路由器前面板上的“RST”键（复位按钮）相同。界面如下图所示：

提示：路由器恢复出厂配置后，所有的配置都将被清空。可以通过 http://192.168.0.1 来重新配置路由器，登录用户名和密码都是 admin

3.10.7 重新启动

本界面提供的功能是从软件上重启路由器。通过 WEB 管理界面重启路由器在某些时侯可能非常方便，例如路由器放置在一个无法触及到的地方时。路由器的重启过程大概需要 30 秒。界面如下图所示：



支持定时重启路由器，设置如下：

附录A　路由器选配电缆说明

1，以太网接口电缆

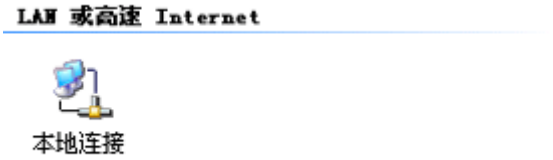
路由器的以太网接口电缆为 8 芯非屏蔽双绞线，1、2 脚为发送端，3、6 脚为接收端；和计算机网卡的 10BASE-T 接口相同，可以与 HUB 直接相连。

RJ-45 管脚号	信号	信号描述
1	**TxData+**	发送数据
2	**TxData-**	发送数据
3	**RxData+**	接收数据
4	---	电话接头
5	---	电话接头
6	**RxData-**	接收数据
7	---	网络测试
8	---	网络测试

附录B　WindowsXP环境下的TCP/IP配置

本章介绍如何为您的个人计算机配置 TCP/IP 协议。首先请您确认在计算机中已经正确安装了网卡。以下步骤将指导您正确设置计算机与路由器连接时的 TCP/IP 配置。

1、依次点击：开始 → 控制面板 → 网络连接。



2、双击“网络连接”，选中“本地连接”击右键选择“属性”。

3、双击 Internet 协议（TCP/IP）。

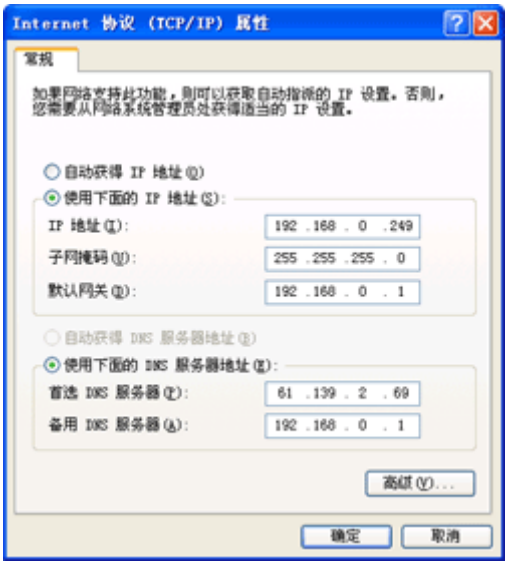
4、现在，您有两种设置方法：

- 第一种，手工设置 IP 地址

1） 选中“使用下面的 IP 地址”，在 IP 地址栏中填写 IP 地址：192.168.0.249，子网掩码：255.255.255.0，缺省网关： 192.168.0.1（因为路由器的默认 IP 地址为 192.168.0.1）。

2） 选中“使用下面的 DNS 服务器地址”，在 DNS 设置栏中，首选 DNS 服务器填写 ISP 为您提供的 DNS 服务器地址，备用 DNS 服务器填写路由器的默认 IP 地址。

3） 单击“确定”即可。配置结果如下图所示：



- 第二种，通过 DHCP 服务器设置 IP 地址

1）选中“自动获得 IP 地址”；

2）选中“自动获得 DNS 服务器地址”，

3）单击“确定”即可。配置结果如下图所示：