深圳市启博网络有限公司

MR

系

列

产

品

说

明

书

注：因产品型号不同，不同产品之间可能存在差异

目 录

一、MR 系列产品介绍

MR 系列产品最大的亮点是解决了 VPN 应用中的动态域名寻域不稳定的难题，采用 WEB 智能目录服务很好的解决了 VPN 服务器端 IP 地址变化的问题；该系列有 MR1300、MR-2600、MR5100 等型号产品，产品功能主要包括如下几个方面：

VPN 异地局域网互连

双 VPN 服务器

QOS/IP 限速，合理分配网络带宽

设备流量实时查看，了解电脑流量状况

ARP 绑定，阻止非法用户使用网络

IP/MAC 速度限制

这些都是企业所迫切需要的非常实用的功能，一台设备可以解决客户所有的网络管理需求，在解决用户 VPN 连接的问题外，设备本身还附带有企业常用的上网行为管理功能，是性价比非常高的产品。

二、产品快速使用指南

1. MR 系列产品的默认 IP 地址是 192.168.10.1 ，在配置之前，将电脑网卡和设备 LAN 口相连接，手工设置电脑网卡地址或自动获取 IP 即可。
2. 在浏览器中输入：http://192.168.10.1 输入用户名 admin 密码 admin ，即可进入 WEB 配置界面。
3. 进入基本设置->网络设置中，在 WAN1 设置中选择外网接入方式（DHCP、PPPOE、静态地址、PPTP、L2TP），输入相关上网信息，保存后即可接入互联网。

三、详细配置说明

1．运行状态

运行状态--->系统信息这里是设备的一些基本的信息，如 VPN 客户端授权数、CPU 负载、占用率、开机时长等，以及外网、内网的一些 IP 连接信息。

运行状态--->在线主机列表栏中则可以查看现在正连接在设备上的电脑信息，包括 MAC 地址、IP 地址、计算机名称、剩余租约等。

运行状态--->系统日志可以查看设备最近的访问信息记录。

2. 设备流量状态

设备流量状态--->实时流量用于查看当时网络带宽的运行情况，相应网口(WAN、br0、eth0、tap21、vlan0)流量的多少等。

3.测试工具

测试工具--->Ping 用于判断路由器到 IP 或域名的连接。

地址

输入目标 IP 或目标域名

Ping 次数

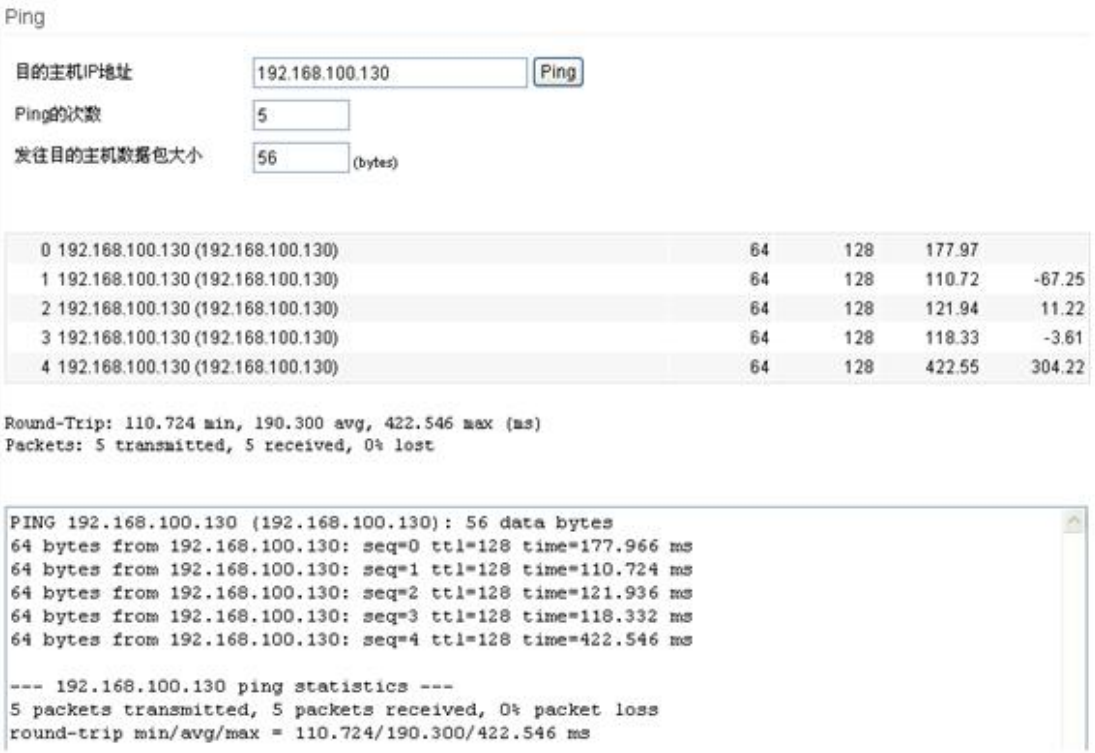
默认就可以

数据包大小

默认就可以

响应时间

响应时间越小表示网络越好



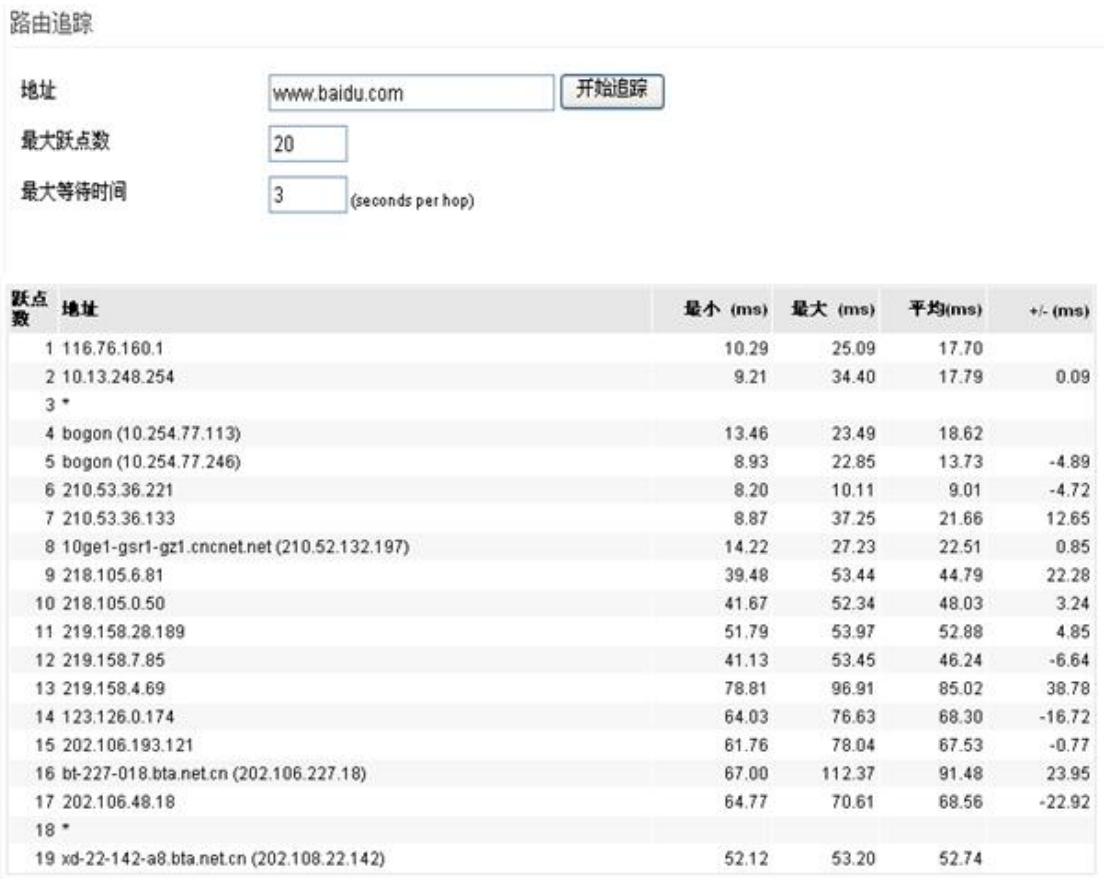
测试工具--->Trace

用于查看目的 IP 或域名所经过的网关。

地址

输入目标 IP 或目标域名

其他默认



跃点数	地址	最小 (ms)	最大 (ms)	平均(ms)	+/- (ms)
1	116.76.160.1	10.29	25.09	17.70	
2	10.13.248.254	9.21	34.40	17.79	0.09
3	*				
4	bogon (10.254.77.113)	13.46	23.49	18.62	
5	bogon (10.254.77.246)	8.93	22.85	13.73	-4.89
6	210.53.36.221	8.20	10.11	9.01	-4.72
7	210.53.36.133	8.87	37.25	21.66	12.65
8	10ge1-gsr1-gz1.cncnet.net (210.52.132.197)	14.22	27.23	22.51	0.85
9	218.105.6.81	39.48	53.44	44.79	22.28
10	218.105.0.50	41.67	52.34	48.03	3.24
11	219.158.28.189	51.79	53.97	52.88	4.85
12	219.158.7.85	41.13	53.45	46.24	-6.64
13	219.158.4.69	78.81	96.91	85.02	38.78
14	123.126.0.174	64.03	76.63	68.30	-16.72
15	202.106.193.121	61.76	78.04	67.53	-0.77
16	bt-227-018.bta.net.cn (202.106.227.18)	67.00	112.37	91.48	23.95
17	202.106.48.18	64.77	70.61	68.56	-22.92
18	*				
19	xd-22-142-a8.bta.net.cn (202.108.22.142)	52.12	53.20	52.74	

测试工具--->网络唤醒

通过网络唤醒路由器局域网内处于关机状态的电脑，目标电脑的网卡及主板需要支持 WOL 功能

在 MAC 地址列表中点击一下即可实现网络开机

也可以把 MAC 填进"MAC 地址列表"然后点击"立刻唤醒"

当前状态

显示 使用中(In ARP)===>表示该电脑与路由器已经在连接上

显示 - ===>表示该电脑与路由器断开连接

4.网络设置

网络设置-->网络设置

这里是最基本的设置,这里没有设置好就不能上网了，跟一般的路由器配置方法相同。

WAN/连接：

对应你的上网方式设置好就可以，一般宽带为 PPPOE；

透明模式连接：

另外不同于普通网络设备的是，MR 系列 VPN 带有透明模式上网连接，选择透明模式时，VPN 设备接在网关路由下面，即接在内网中，可从网关路由中接出一条线到 VPN 的任一网口。

设成透明模式时，LAN 设置方法：路由 IP 地址可以设内网中任意一个空 IP 为设备地址，子网掩码 255.255.255.0，静态 DNS 第一栏填网关路由地址，第二、三栏填当地 ISP 服务器的 DNS 服务器地址。

LAN 设置

路由器 IP 地址===>这里是更改路由器的网关地址,如改了 192.168.100.1 后,你访问路由器就要用 192.168.100.1

子网掩码===>一般用默认就可以了

DHCP 服务器===>选上则打开 不选则关闭,打开 DHCP 可以让客户端自动获取 IP 地址上网，关闭则需要客户端指定 IP 才能上网

IP 地址范围===>DHCP 就分配的起止地址和结束地址，必须跟"路由器 IP 地址"同一网段

租约时间===>DHCP 分配给 IP 使用的时间，过期后会自动续期

WINS===>一般默认可以

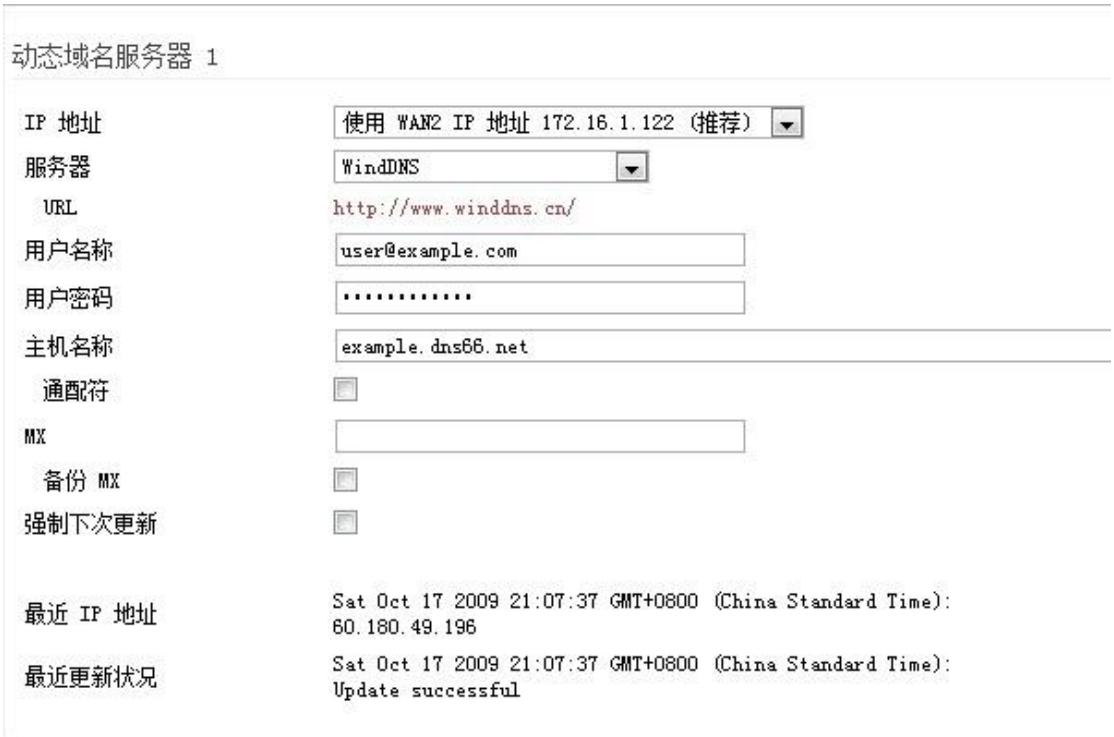
基本设置-->路由时间

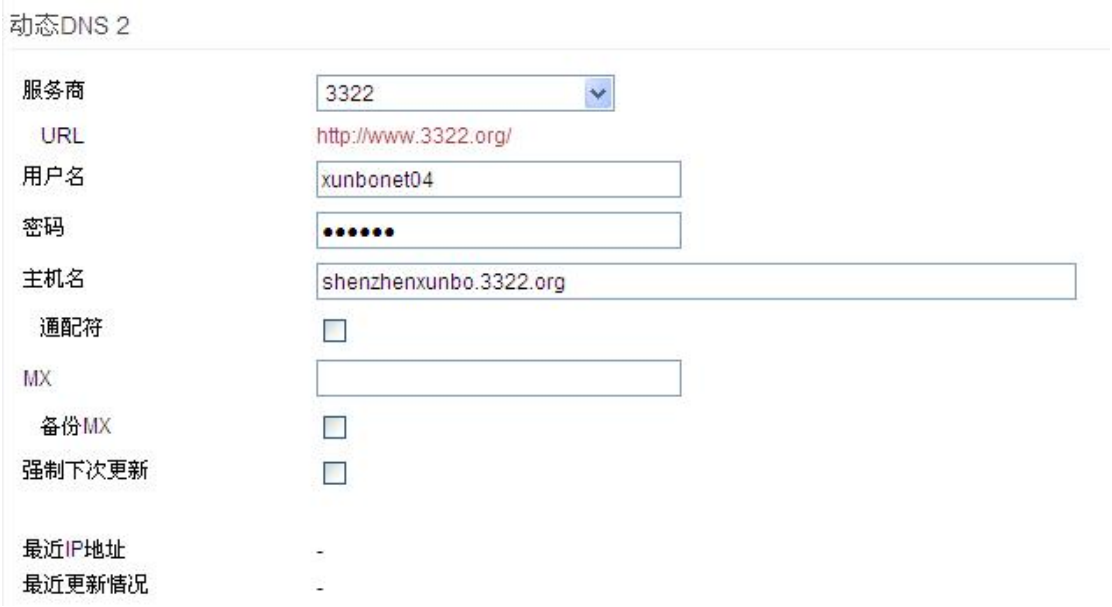
用于路由器与 Internet 时间同步，路由器时间会在系统状态下显示，该时间关乎于以后讲到的"定时重启路由器"，"访问限制"等基于时间执行的功能，中国的时区是+8 区。

如果出现能上网但是时间更新失败，请尝试选择其他的 NTP 时间服务器。

基本设置-->动态域名

当通过互联网进行远程管理路由器或者路由器局域网内建立的服务器时，就需要使用动态域名功能了，MR 系列设备可以设置两个互相独立的动态域名，推荐使用 3322、WindDNS。





动态 DNS1/动态 DNS2

IP 地址===>通常选用使用 WAN IP 地址即可，如多级路由则选用使用外部 IP 地址(但各级路由必须做好端口映射)

服务器===>选你动态域名的服务提供商

用户名===>你注册时的用户名

密码===>你注册时的密码

主机名称===>你所注册的动态域名

通配符===>选上 但好像不起作用 作用是当访问该域名上不存在的目录时自动跳转到域名首页

强制下次更新===>选上后，点击保存按钮时会强制更新一次动态域名

最近 IP 地址====>更新成功后动态域名所指向的 IP，正常情况下应该是你前面选定的 WAN 口的 IP，如果出现不一致可能是你的路由器存在上级路由

最近更新状况====>更新成功后，此处应该显示 Update successful 字样

注意：动态域名更新成功只是表示你的动态域名服务商已经将你的动态域名指向新的 IP，由于 ISP 的 DNS 都是有缓存功能的，可能会出现 ping 你动态域名解析出的 IP 跟你的路由器 IP 不一致的情况，可能过个 10 来分钟(不同的动态域名服务商的缓存时间是不同的，一般是 3-10 分钟)缓存才会失效。

基本设置-->静态 DHCP

该功能是用于给电脑分配指定的 IP，但不同于强行指定，电脑上改其他 IP 地址也不受影响

MAC 地址
填你要指定的电脑的 MAC 地址
IP 地址
填你要指定电脑 MAC 分配的 IP 地址
主机名称
用于备注，目前不支持中文

5. 高级设置

高级设置-->高级网络设置

连接数
最大连接数　支持最大 10240 个连接数，大家根据你带宽和路由器型号所能承受的连接数进行设置

TCP 超时设置和 UDP 超时设置

如果你对这些数据不熟悉的话保持默认就好，修改过的话可能会导致 BT 变慢，QQ 频繁断线等现象

Tracking / NAT Helpers
FTP===>对 FTP 提供 NAT 支持
GRE / PPTP===>对 PPTP VPN 提供 NAT 支持。
H.323===>对基于 H.323 协议的网络电话提供 NAT 支持
RTSP===>对 RTSP 协议提供 NAT 支持
其它设置
TTL 调整===>调整数据包的 TTL 值
下载启用
Layer7 应用过滤===>对下载进行 L7 过滤，可以封诸如网游、QQ、迅雷等应用

高级设置--->DHCP / DNS

开启 DNS 快取快发
启用该功能可以加快 DNS 解析速度，建议打开
使用静态 DNS 服务器 ===>启用该选项后，路由器在请求上级 DNS 解析时将使用 WAN 口连接设置中手工指定的 DNS 服务器（如果有指定的话）和 ISP 那里自动获取的 DNS 服务器进行解析，解析的顺序为先手工指定的 DNS 服务器后 ISP 那里自动获取的 DNS 服务器
截获 DNS 端口 ===>启用该选项后，不管 PC 机的 DNS 服务器设置成什么，路由器都会接管并回复 PC 的 DNS 解析请求
DHCP 分配最大数量
字面意思，没什么好说的
静态租约时间
正常===>即静态 DHCP 列表里的主机使用 网络设置 里的 租约时间
不限制===>即静态 DHCP 列表里的主机的不受租约限制，永久有效
自定义===>手动指定静态 DHCP 列表里的主机的租约时间
Dnsmasq 自定义设置 ===>MR 系列产品使用 Dnsmasq 作为 DNS 缓存和解析服务，专家级用户可以根据需要在此处填写自定义的设置

高级设置--->防火墙

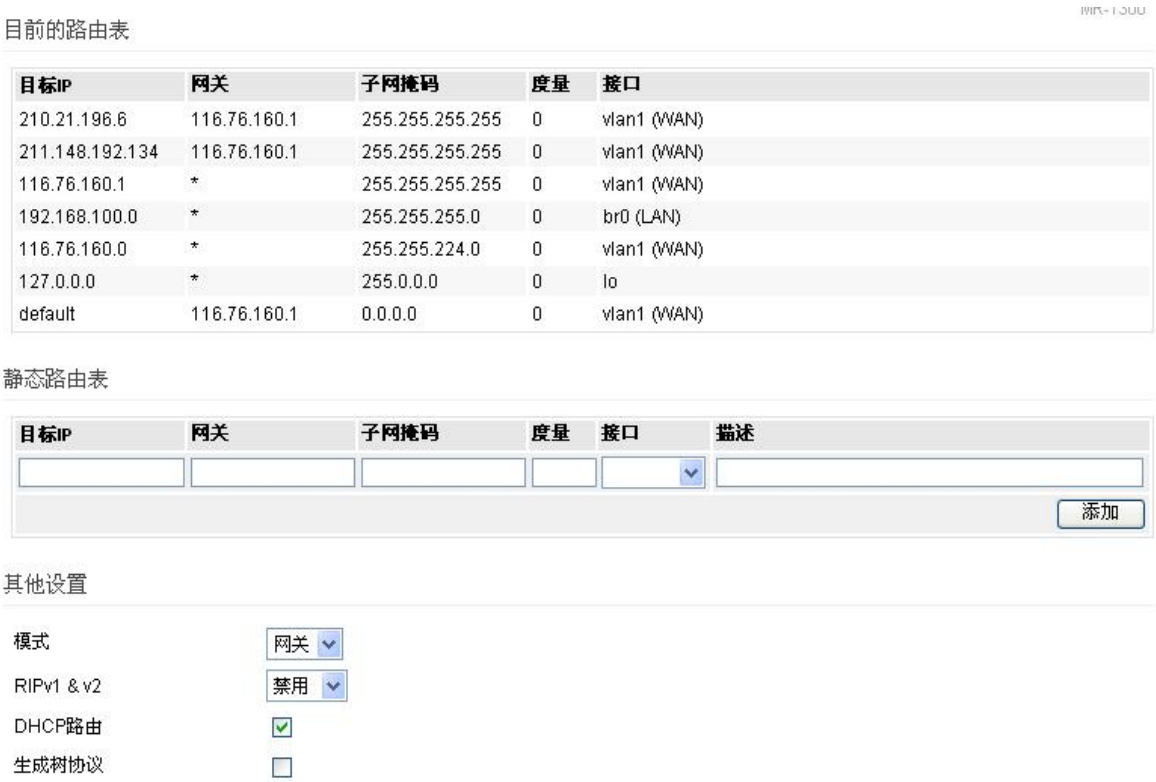
允许回应 ICMP Ping ===>默认不启用，启用该选项后外部可以 ping 通 WAN 口的 IP，如无必要请不要启用该选项，可以提高路由器的安全性
允许多播(multicast) ===> 具体多播的用途请自行搜索资料
NAT Loopback ===> 如果想局域网内的 PC 能访问路由器 WAN 口的 IP，那么请将该选项选择为“全部”，否则选择为“只有被转送的封包”
SYN Cookies ===>启用该选项可以抵御 SYN Flood 攻击

高级设置--->路由 MAC 设置

用于修改路由器的 MAC 地址，当有些 ISP 绑定了你的 PC MAC 后，此时你就需要将 WAN 口的 MAC 地址设置成 PC 的 MAC 来上网
可以修改 WAN 的 MAC，不能修改 LAN 的 MAC

高级设置--->路由表设置

显示路由器当前的路由表和静态路由的管理，可以根据网络实际情况有需要另加路由的在此添加，一般用户不需更改。



在开启了 VPN 服务，并且已经成功建立了 VPN 连接后，如果服务端设备要 PING 通客户端设备需在服务端设备处添加到客户端的静态路由，比如说客户端的内网 IP 网段为 192.168.2.0，客户端设备连通 VPN 后所获取的虚拟 IP 为 10.2.0.11，使用的是服务端接口 1，则可如下图所示添加路由表，添加后保存即可，设备在关闭 VPN 服务后此添加的路由会消失，在再次开启 VPN 服务后会自动添加上来，不需要重复输入。

静态路由表

目标IP	网关	子网掩码	度量	接口	描述
192.168.2.0	10.2.0.11	255.255.255.0	0	服务端接口1	

删除 确定 取消

6. 转发规则

转发规则---> 虚拟服务

这里可以做端口映射，把网内电脑的服务器端口映射到外网，让外网可以通过这个端口访问到服务器，需要根据实际进行设置。

外部 IP *(可选)* - 转发至设定的 IP 范围。例：“1.2.3.4”，“1.2.3.4 - 2.3.4.5”，“1.2.3.,留空为所有 IP。

外部端口 - 从 WAN 对应进来的端口。例：“2345”，“200,300”，“200-300，400”

内部端口 *(可选)* - 若为空，便自动对应 *外部端口* 当 *内部端口* 与 *外部端口* 不同时，才须填入内部端口

内部 IP - 对应局域网内的 IP 地址

注意 当内部 IP 地址为路由的 IP 时，请确保路由的 INPUT 链是允许的。

端口转发

启用	协议	外部IP地址	外部端口	内部端口	内部IP地址	描述
	UDP		1000,2000		192.168.1.2	ex: 1000 and 2000
	Both		1000-2000,3000		192.168.1.2	ex: 1000 to 2000, and 3000
	Both	1.1.1.0/24	1000-2000		192.168.1.2	ex: 1000 to 2000, restricted
	TCP		1000	2000	192.168.1.2	ex: different internal port
On	TCP		80		192.168.10.253	oa
On	TCP		1433-1434		192.168.10.253	sql
On	TCP		1723		192.168.100.109	v
☑	TCP					

添加

转发规则---> DMZ 主机

这里可以做 DMZ 设置，高端用户可以根据自己需要进行设置。

DMZ

开启DMZ ☐

目的IP地址 192.168.100.0

源IP地址定向到

(可选; ex: "1.1.1.1", "1.1.1.0/24" or "1.1.1.1 - 2.2.2.2")

转发规则---> 端口转发

开启触发式端口转发功能，使用“-”指定端口范围 (200-300)，一旦检测到触发程序通讯端口送往指定内部端口的上传数据包便会转向您的计算机，开启的通讯端口若未使用，几分钟之后会自动关闭。

转发规则---> UpnP/NAT-PMP

7.智能 QOS

智能 QOS--->基本设置

从下图可以看到 QOS 的一些基本设置 开启 QOS 选择需要功能。通过使用 QOS 设置，可以保障关键业务的应用，如保证商务邮件不会因为网络拥堵而发不出去；保证 VPN 应用的带宽资源，不至于被 P2P 挤占带宽；通过设置，限制或禁止 P2P 应用。

上传限制设置中，最大上行带宽栏里，一般填为实际带宽的 85%，对于机器较多的情况下尤其重要。通常情况下，只需要设置上行带宽就可以对流量进行优先级分类，对于高优先级

和最高优先级，最高上行带宽都设置为 100%，对于中优先级最大上行带宽建议设置成 80%，对于低优先级，建议最大上行带宽设置成 50%，对于最低优先级，则建议最大上行带宽设置成 10%，如果设置成 5%，则基本可以禁止任何 P2P 应用，如 PPLIVE、EMULE、BT 等。

下行限制则一般不需要设置。
TCP 乱序根据用户自身情况开启或关闭。

智能 QOS--->宽带分类

在 QOS 的设置里，这里也是必不可少的。这里可以让你指定的程序、端口列分等级，以配合上面的等级分配优先权和速度。
这里可以根据自己想要的做规则。
例如：我玩游戏的，想让那个端口处与最悠闲，防止游戏卡机掉线。游戏端口为：12701 把此目标端口 设定为 最高级，就是此端口可以用全速。
同样，相反的也能把指定端口设置为 最低级 。（注：这些规则可以上下移动的哦。鼠标放去规则那里有显示的。想优先也得先把他提高）

端口优先级指定

Match Rule	Class	Description
TCP Dst Port: 80,443 Transferred: 0 - 512KB	High	WWW
TCP/UDP Dst Port: 12701	Highest	game
TCP Dst Port: 80,443 Transferred: 512KB+	Low	WWW (512K+)
TCP/UDP Dst Port: 53 Transferred: 0 - 2KB	Highest	DNS
TCP/UDP Dst Port: 53 Transferred: 2KB+	Lowest	DNS (2K+)
TCP/UDP Dst Port: 1024-65535	Lowest	Bulk Traffic
Any Address	Lowest	
TCP/UDP / Any Port		
IPP2P (disabled) / Layer 7 (disabled)		
- KB Transferred		

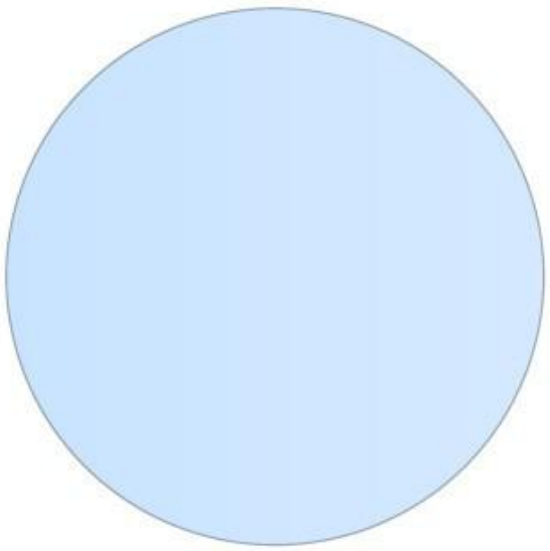
添加

智能 QOS--->视图模式

用于分析流量,QOS 设置关闭则无效

连接分布图表

未分级	7	100.00%
最高级	0	0.00%
高级	0	0.00%
中级	0	0.00%
低级	0	0.00%
最低级	0	0.00%
A 级	0	0.00%
B 级	0	0.00%
C 级	0	0.00%
D 级	0	0.00%
E 级	0	0.00%
合计	7	100%



智能 QOS--->详细信息

可以过滤某个 IP 地址 或某一条线路
可以显示协议类型 内网主机的 IP 内网主机的端口 目的 IP 和端口该条流量所走的线路

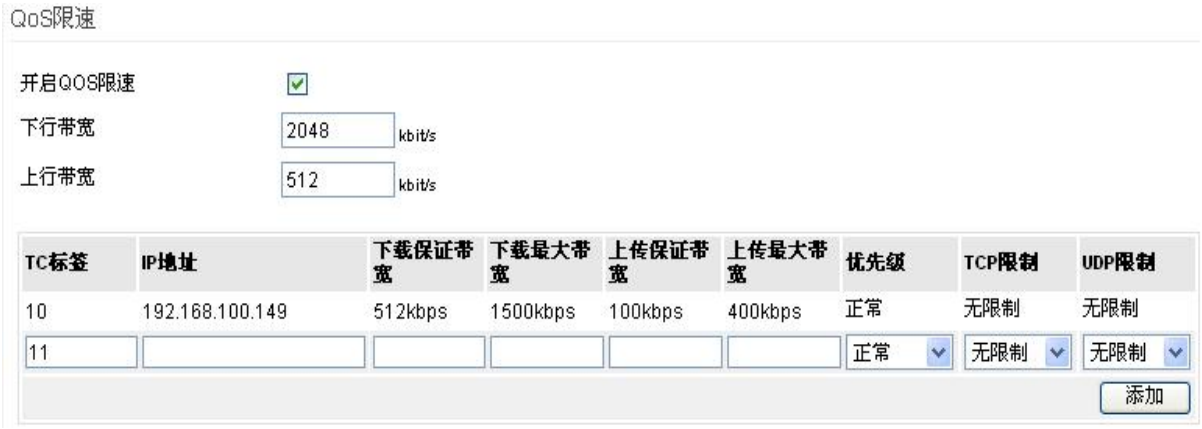
View Details

协议	源地址	源地址端口	目的地址	目的地址端口	等级
UDP	192.168.100.120	3683	115.193.169.4	43253	未指定
TCP	192.168.100.145	1434	192.168.100.1	80	未指定
TCP	192.168.100.145	1425	192.168.100.1	80	未指定
TCP	192.168.100.139	2906	124.89.102.139	80	未指定
TCP	192.168.100.120	139	192.168.1.9	2869	未指定
TCP	192.168.100.145	1439	192.168.100.1	80	未指定
UDP	192.168.100.120	3701	119.141.65.108	22164	未指定
TCP	192.168.100.145	1435	192.168.100.1	80	未指定
UDP	192.168.100.139	4004	219.133.51.241	8000	未指定
UDP	192.168.100.120	3008	192.168.100.1	53	未指定
UDP	192.168.100.120	3712	59.39.125.46	47979	未指定
UDP	192.168.100.120	10013	220.181.126.84	80	未指定
UDP	192.168.100.139	4001	219.133.48.97	8000	未指定
UDP	192.168.100.120	3675	116.76.8.228	46831	未指定
TCP	192.168.100.145	1424	192.168.100.1	80	未指定
UDP	192.168.100.120	3681	123.149.51.199	31764	未指定
UDP	192.168.100.120	3812	255.255.255.255	9200	未指定

8．IP/MAC 速度限制

IP/MAC 速度限制--->IP 限速

此功能可以对个别用户的下载速度和上传速度进行限制，同时限制 TCP 和 UDP 连接数，从而控制个别用户对网络带宽的滥用。**注意：**不适合对整个局域网的机器进行 IP 限速，这样容易浪费带宽，同时难以发挥带宽效率。



IP/MAC 速度限制--->ARP 绑定

此功能可以对 IP/MAC 地址进行绑定，以标志用户合法身份。如开启了“限制未在列表里的主机”选项，则不存在这个列表中的电脑都无法上网，而绑定在这个列表中的电脑，如果绑定的 IP 地址和 MAC 地址不相对应，也无法连接到外网。

9．VPN 设置

VPN 设置--->服务器

在 VPN 服务器设置中的基本设置栏里，设置参数有虚拟 IP 地址、子网掩码、协议、端口号、认证类型、客户端 IP 地址段。

随 WAN 一起启动：设备连上网络后自动启动 VPN 连接服务，一般勾上此选项。
虚拟 IP 地址：一般默认设置 10.2.0.1，也可以设置成其他私有内网地址。作为 VPN 连接的主要参数，若客户端是软件连接，此处设置成跟内网地址一样网段，则服务器和客户端成桥接模式，即可网上邻居访问对端。用户无此需求则保持默认 10.2.0.1 即可。
子网掩码：默认 255.255.255.0，一般不需要更改。

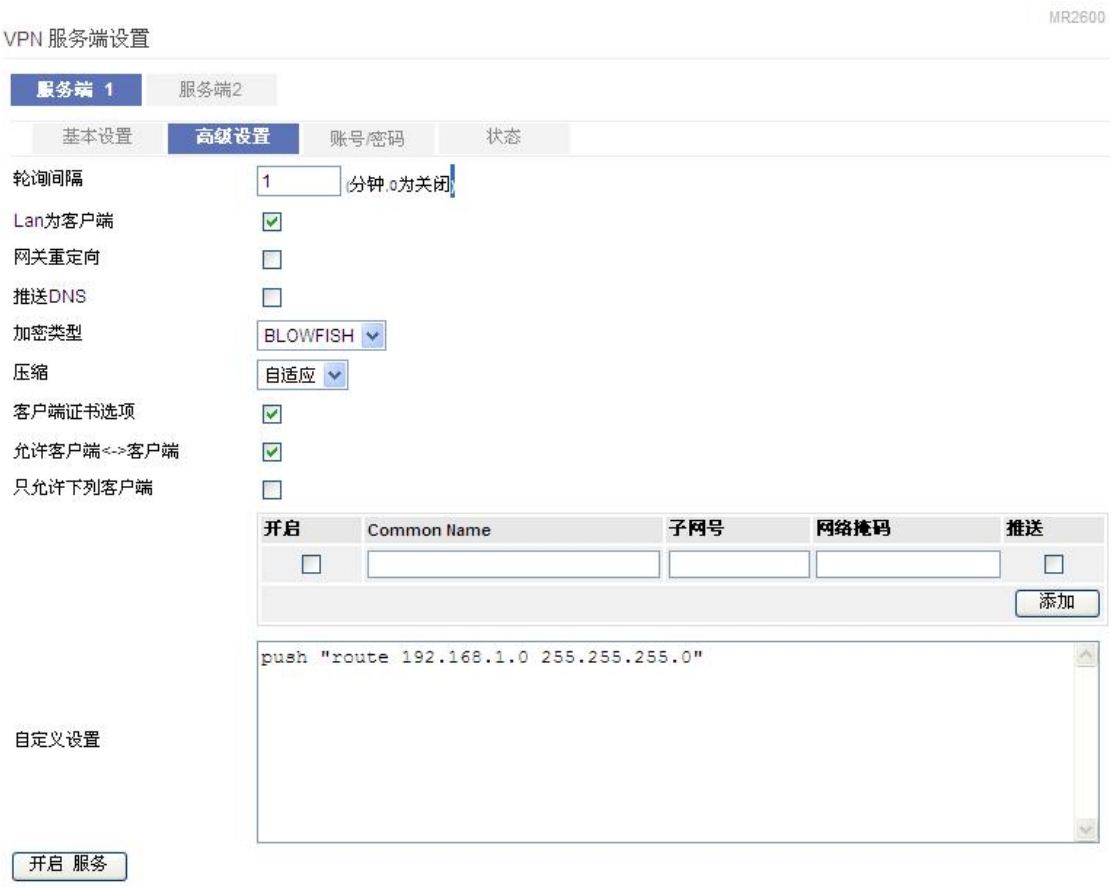
协议：默认 UDP 协议，可选 TCP 协议。此设置也要服务端与客户端保持一致，用户可根据自身网络选择相应的协议使用，因为有部分地区的网络使用 UDP 协议连接更顺畅，也有的使用 TCP 协议连接更顺畅。

端口：VPN 通信所使用的端口号，默认为 1194，可更改，一般默认即可。

认证类型：有帐号认证和 TLS 认证两种类型，帐号认征为管理员创建相应帐号，客户端要连上 VPN 则必须要有其创建的帐号密码才能登陆。TLS 认证为证书认证，客户端要连上 VPN 必须要有跟服务端对应的证书才能登陆，选择此认证类型的，我司会根据不同公司分配相应的认证证书。

允许远端访问 server 端：此选取项允许客户端访问服务端设备，推荐选上。

客户端 IP 地址段：分配给客户端的虚拟 IP 地址段，一般用户自己设定为佳，如上图所示。



在 VPN 服务器设置的高级设置栏中，用户只需设置轮询间隔、加密类型、允许客户端<->客户端、自定义设置这四栏，其余的保持默认，不做更改。

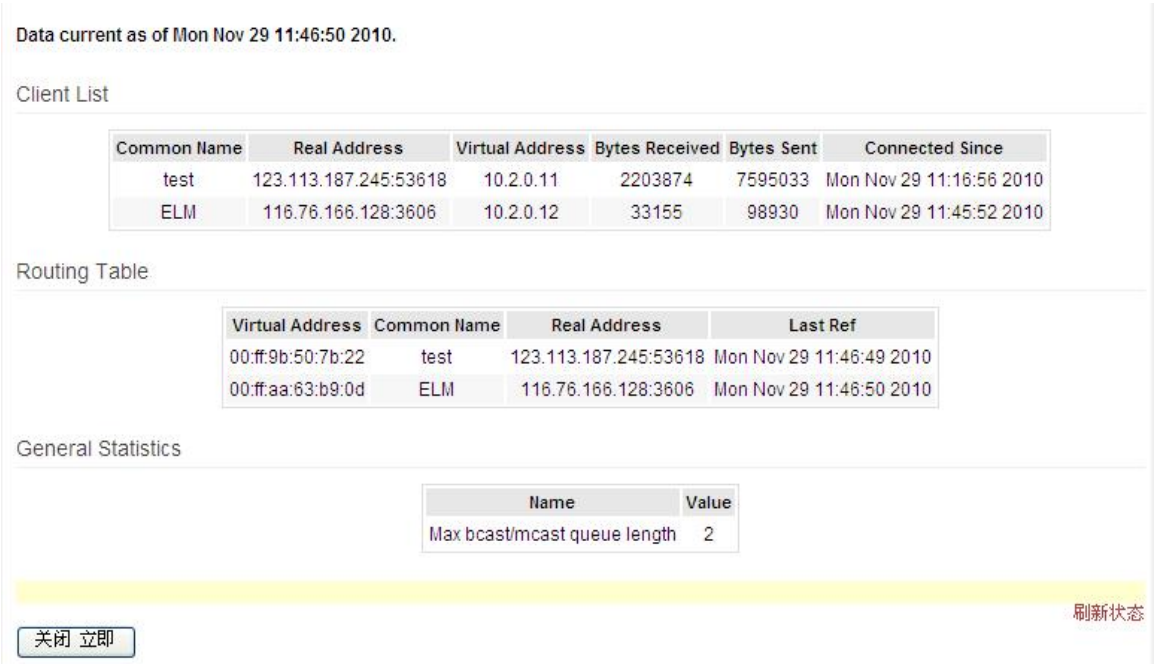
轮询间隔：向客户端发送本端信息的时间间隔，建议设置 1 分钟，每隔一分钟向客户端发送询问信息，此选项使 VPN 连接更稳定。

加密类型：对 VPN 的数据加密类型，一般选择 BLOWFISH 加密类型为佳，也可选择不加密，做出设置后，对应的的客户端也要修改加密类型，两方保持一致，否则数据无法联通。

允许客户端<->客户端：选取此选项，则连上 VPN 的客户端与客户端之间可相互互联。

自定义设置：此处可自己添加相应参数设置，对服务端进行更改，需要添加如图所示代码：push “route 192.168.1.0 255.255.255.0” ，此代码表示把服务端内网网段 192.168.1.0 路由推送给 VPN 客户端，若服务端内网网段为 192.168.10.0，则把相对应代码的 192.168.1.0 改成 192.168.10.0 即可。此推送路由代码若不设置则客户端无法访问服务端内网电脑。

在 VPN 服务端设置的帐号/密码栏中，可设置客户端连接使用的帐号密码等信息，基本设置中的认证类型选择了帐号认证的才需要设置此页面，客户端连接输入的帐号密码跟这里的设置不符合的话将无法登陆 VPN。此处设置的 IP 地址为虚拟 IP 地址，跟之前基本设置栏中的虚拟 IP 地址一个网段，子网掩码也跟之前的设置一样。备注栏中可以对此帐号进行注释，备注栏只支持数字及英文字母，并且不支持空格。前端的开启栏不勾上的话，则这帐号无法使用。



VPN 服务端设置的状态栏中，如图所示可以看到现在正在连接的用户名及其相关信息，如外网地址、虚拟 IP 地址、MAC 地址、收到以及发送的数据包多少等等。

VPN 设置--->客户端

VPN 客户端设置中的基本设置栏里，设置参数有接入类型、协议、服务器域名、防火墙、认证类型、帐号/密码、额外 HMAC 认证等。

接入类型：保持跟服务器端相同，一般为 TAP。

协议：保持跟服务器端相同，有两种协议 TCP 和 UDP。

服务器域名：此处有三种模式，XML、域名、IP 地址，可填入服务器端的 DDNS 动态域名，每个用户我司有相应域名分配，把分配的域名填入即可；也可如图所示般填入 XML 路径，效果一样。

防火墙：此处不需改动，默认自动。

认证类型：保持跟服务器设置相同，有 TLS 认证和帐号认证两种。

帐号/密码：此处输入 VPN 服务端授权的帐号、密码。

额外 HMAC 认证：此项不需更改，保持默认关闭。

服务端在相同子网：此项没特别说明，不需要选择，如上图所示。

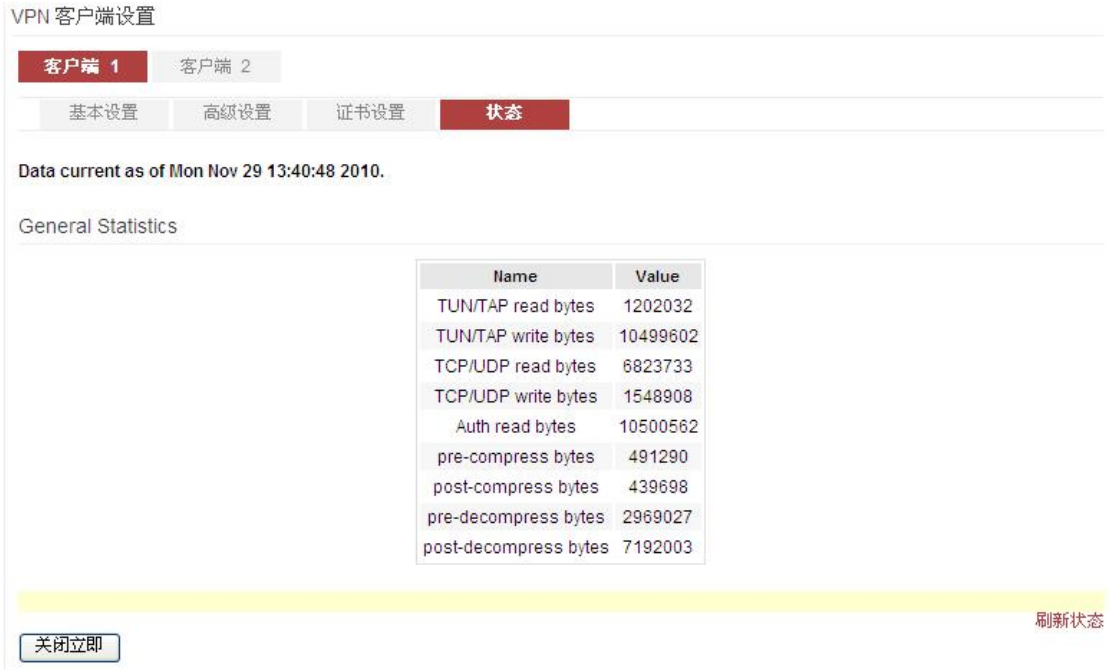
在 VPN 隧道上 NAT：此项一般选择勾上，让 VPN 客户端自动寻找路由。

VPN 客户端设置的高级设置栏中，一般不需多做更改，只需更改自动重连间隔、加密方式两栏。

自动重连间隔：推荐设置 1 分钟，即在 VPN 断开时，每隔一分钟自动重连一次；不设置则在 VPN 断开连接后，设备不自动重连。

加密方式：若服务器端的加密方式为 BLOWFISH，则此处亦选此项，对应着修改即可。

VPN 客户端设置的证书设置栏中，用于输入 VPN 连接需要的相应证书认证，此处设置由我司发布相应证书，用户把相应证书填入即可。



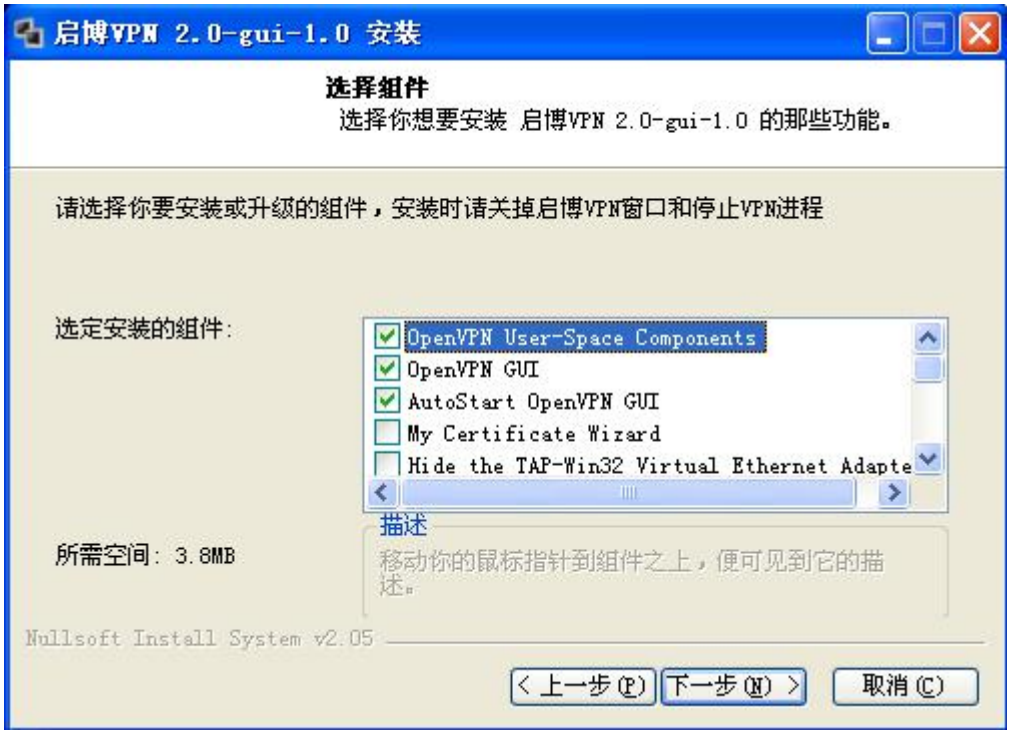
VPN 客户端设置的状态栏中，可以看到 VPN 连接所传输的协议和链接类型数据的大小等信息。

10.VPN 软件客户端

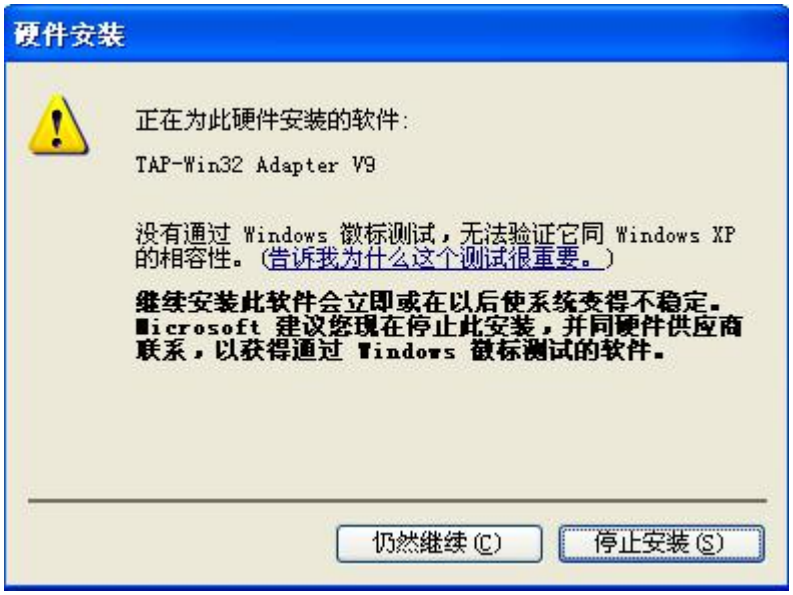
VPN 软件客户端--->VPN 软件安装

我司的 VPN 软件客户端可以与硬件 VPN 联通，使用 VPN 软件客户端连接的用户，需要先在用户电脑上安装指定的 VPN 客户端软件，第一次安装客户端时会要求安装虚拟网卡，选择“仍然继续”即可，安装过程如下图。
下面为安装示意图：


启博VPN 2.0-gui-1.0 安装
欢迎使用 启博VPN 安装向导
本向导将引导您完成启博VPN软件的安装
该软件可以运行在Win 2000, XP, vista,WIN7 系统，包括64位
下一步(N) >
取消(C)


启博VPN 2.0-gui-1.0 安装
选择组件
选择你想要安装 启博VPN 2.0-gui-1.0 的那些功能。
请选择你要安装或升级的组件，安装时请关掉启博VPN窗口和停止VPN进程
选定安装的组件:
OpenVPN User-Space Components
OpenVPN GUI
AutoStart OpenVPN GUI
My Certificate Wizard
Hide the TAP-Win32 Virtual Ethernet Adapte
描述
移动你的鼠标指针到组件之上，便可见到它的描述。
所需空间: 3.8MB
Nullsoft Install System v2.05
< 上一步(P)
下一步(N) >
取消(C)

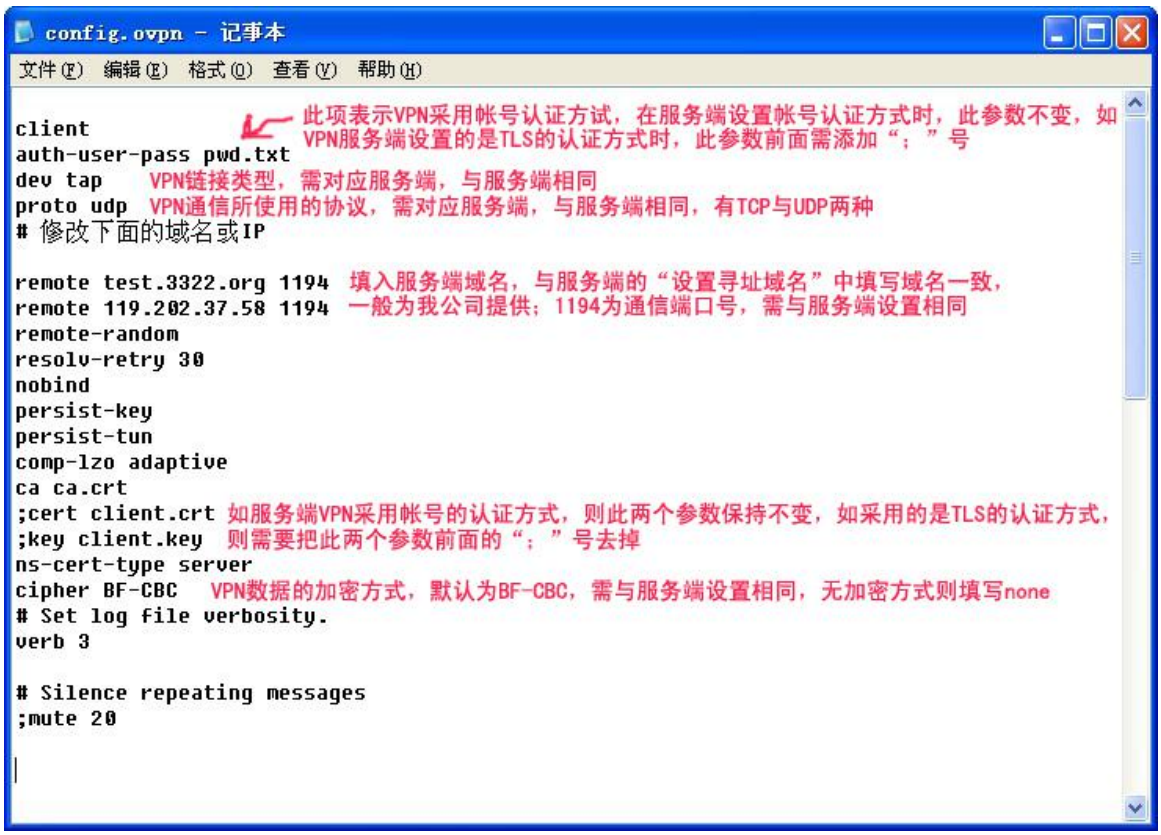

启博VPN 2.0-gui-1.0 安装
选定安装位置
选定 启博VPN 2.0-gui-1.0 要安装的文件夹。
Setup 将安装 启博VPN 2.0-gui-1.0 在下列文件夹。要安装到不同文件夹，单击 [浏览(B)] 并选择其他的文件夹。 单击 [安装(I)] 开始安装进程。
目标文件夹
C:\Program Files\启博VPN
浏览(B)...
所需空间: 3.8MB
可用空间: 14.3GB
Nullsoft Install System v2.05
< 上一步(P)
安装(I)
取消(C)


硬件安装
正在为此硬件安装的软件:
TAP-Win32 Adapter V9
没有通过 Windows 徽标测试，无法验证它同 Windows XP 的相容性。(告诉我为什么这个测试很重要。)
继续安装此软件会立即或在以后使系统变得不稳定。Microsoft 建议您现在停止此安装，并同硬件供应商联系，以获得通过 Windows 徽标测试的软件。
仍然继续(C)
停止安装(S)

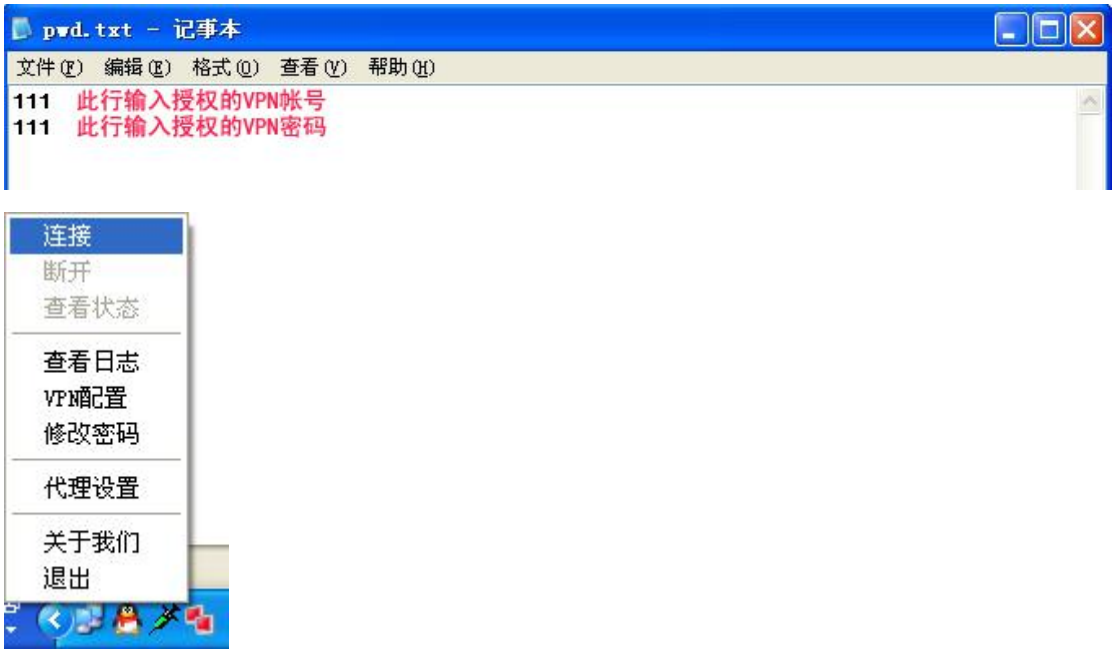
VPN 软件客户端--->VPN 软件参数配置

1．安装好 VPN 客户端软件后，先打开配置文件，路径为“开始”->“程序”->“启博 VPN”->“VPN 配置”。

2．对客户端配置文件进行相应修改，要求与服务端的配置相对应，如下图中说明进行设置，一般不需多作修改，下图中无说明的参数保持默认即可。

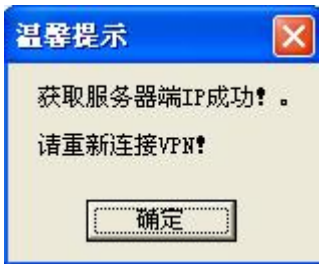


3．参数设置保存完后，如采用的是帐号的认证方式，则需要打开路径为“开始”->“程序”->“启博 VPN”->“用户设置”，或者路径 C:\Program Files\启博 VPN\config，进入配置文件所在文件夹，打开 pwd.txt 文本，如下图所示，输入经服务端授权的接入帐号密码后保存。之后对任务栏中 VPN 程序右键单击选择连接，客户端参数无误，即可以正常连上 VPN。如果采用的是 TLS 认证方式，则直接对任务栏中 VPN 程序右键单击选择连接即可。虚拟网卡中所获得的地址跟服务端分配的虚拟 IP 网段对应。



VPN 软件客户端--->VPN 无法连接时的备用寻址

有些时候软件无法连接上 VPN 服务端，有很大情况下是没有正确找到 VPN 服务端的所在而导致的，在这个时候我们可以打开路径为“开始”->“程序”->“启博 VPN”->“手动寻址”的文件，或者路径 C:\Program Files\启博 VPN\config，进入配置文件所在文件夹，打开“qibo.exe”程序，如下图所示，点击开始获取，在弹出获取服务端 IP 成功对话框后，重新连接 VPN 即可。

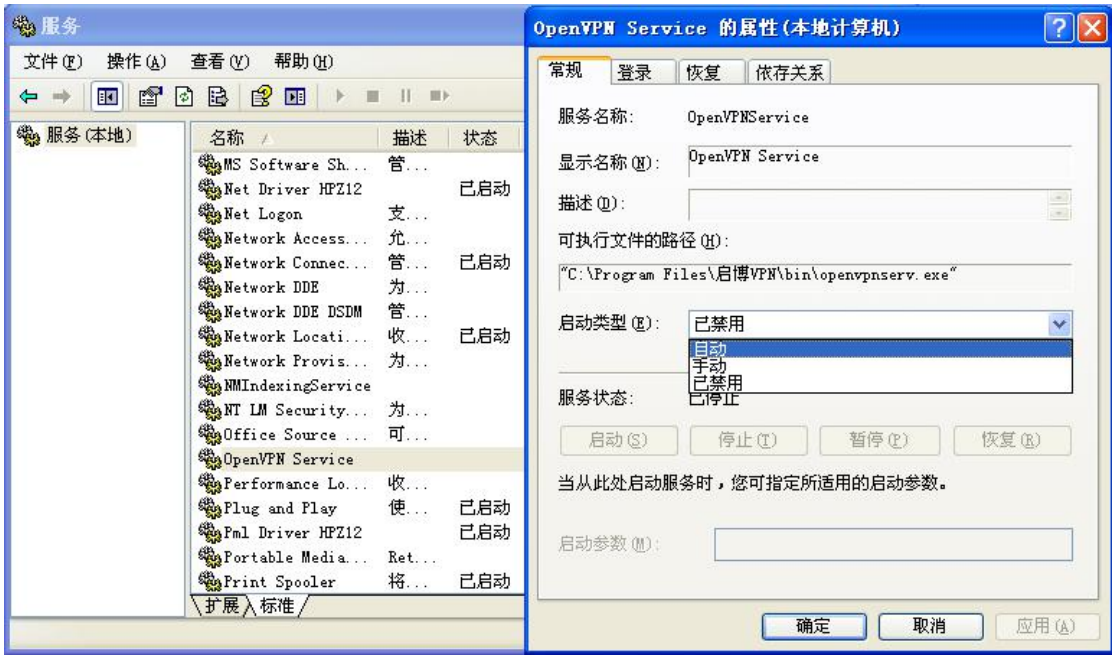


VPN 软件客户端--->VPN 软件开机自启动设置

我司 VPN 客户端支持开机自启动功能，用户只要打开电脑，VPN 即可自动建立连接，同时还有断线自动重连功能，用户感觉不出 VPN 的存在，直接使用上层应用软件访问总部服务器即可。

设置方法：

“控制面板”→“管理工具”→“服务” →“OpenVPN Service”，双击属性，启动类型选择自动，应用之后启动此服务即可实现 VPN 软件开机自启动设置。



11.系统管理

系统管理--->登录管理

本地访问模式===>如选用 HTTP,访问路由器是即 http://192.168.10.1 ,如选用 HTTPS,访问路由器是即 https://192.168.10.1

HTTP 访问端口===>就是访问路由器的端口 假设端口是 20,选用 HTTP,访问路由器是即 http://192.168.10.1:20 ,选用 HTTPS,访问路由器是即 https://192.168.10.1:20

远程访问模式和**远程访问端口**道理跟**本地访问模式端口**一样

允许无线访问===>选上表示内网可以用无线访问路由器,不选则反之

Web 配色方案===>选择字体背景颜色

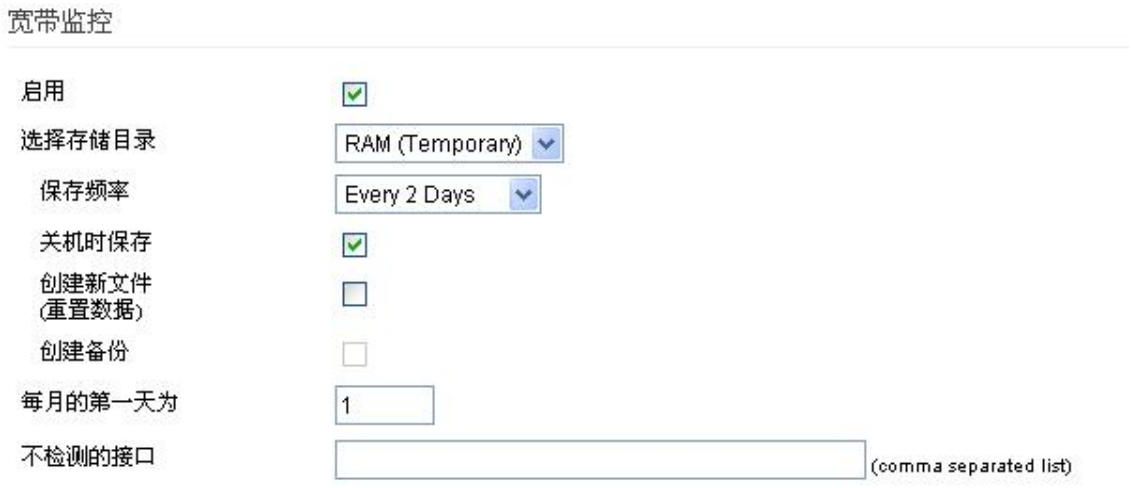
默认展开的菜单===>字面意思，在打开 WEB 界面时，系统默认展开的菜单栏面。

Telnet 访问设置===>开启和关闭 Telnet 服务,访问端口默认 23,如把端口改成 24 则需要 telnet 192.168.1.1:24 ,由于 23 是系统默认端口,所以只需 telnet 192.168.1.1 则可

远程 Web/TELNET 登录限制===>远程 TELNET 的可以设置允许登上来的 IP 地址段，除此外的地址段都无法 TELNET 设备，不填则不做限制，连接次数根据自己实际需要填。

密码设置===>登录设备所需要输入的密码，默认为 admin。

系统管理--->带宽监控



带宽监控跟上面选项的带宽查看相对应，可以设置监控结果的存储目录、每次保存的时间频率、关机时保存等等选项。

系统管理--->设置管理

备份、恢复数据用于备份和恢复配置文件,只能恢复到原来的设备,不能恢复到其他设备,并且需要同一版本设备,MAC 地址需跟原来一样
恢复默认设置可以清除 NVRAM 或恢复出厂设置。

系统管理--->定时任务

此选项栏可根据用户需要，制定定时释放内存、定时重启、定时重新连接等任务。

系统管理--->升级固件

此栏为升级设备所用，在我司发布新版本固件后，可选择相应升级包在此升级，只要在浏览里选择升级包，然后按升级，等设备自动升级完毕即可，升级时间一般不超过 3 分钟。