

深圳市迅博信息技术有限公司

MS

系

列

产

品

说

明

书

目 录

MS 系列产品介绍.....	4
产品快速使用指南.....	4
详细配置说明.....	5
一、运行状态.....	5
运行状态——>主机状态.....	5
运行状态——>在线主机列表.....	5
运行状态——>系统日志.....	6
二、流量查看.....	6
设备流量状态 ——>实时流量.....	6
三、测试工具.....	7
测试工具——>Ping.....	7
测试工具——>Trace.....	8
测试工具——>网络唤醒.....	8
四、网络设置.....	9
网络设置——>网络设置.....	9
基本设置——>时间设置.....	11
基本设置——>静态 DHCP.....	11
五、高级设置.....	12
高级设置——>防火墙.....	12
高级设置——>路由 MAC 设置.....	12
高级设置——>路由表设置.....	12
六、转发规则.....	13
转发规则——> 虚拟服务.....	13
转发规则——> DMZ 主机.....	14
转发规则——> 端口转发.....	14
转发规则——> UpnP/NAT-PMP.....	15
七、智能 QOS.....	15
智能 QOS——>基本设置.....	15
智能 QOS——>宽带分类.....	17
智能 QOS——>视图模式.....	18
智能 QOS——>详细信息.....	19
八、网页监控.....	19
九、访问控制.....	20
十、VPN 设置.....	20
VPN 设置——>服务器端配置.....	20
VPN 配置——客户端配置.....	22
VPN 配置——实时管理.....	23
VPN 配置——日志管理.....	23
VPN 配置——寻址服务.....	24
十一、PPTP 配置.....	25
十二、系统管理.....	27
系统管理——>访问管理.....	27

系统管理——>设置管理.....	28
系统管理——>升级固件.....	28
十三. VPN 软件客户端.....	29
VPN 软件客户端——>VPN 软件安装.....	29
VPN 软件客户端——>VPN 软件参数配置.....	32
VPN 软件客户端——>VPN 软件开机自启动设置.....	34
常见组网应用方案.....	35
硬件网关与硬件网关互联.....	35
硬件网关做服务器，客户端用软件方式接入.....	38
总部与分支要在相同网段（硬件之间网上邻居）	40
总部用透明模式接入.....	42
常见问题.....	44

注：因产品型号不同，不同产品之间可能存在差异

MS 系列产品介绍

MS 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；同时质优价廉是 VPN 该系列产品的最大的卖点，价格只有差不多 MR 系列产品的一半，但是性能相差无几，该系列有 MS-400、MS-800 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。

产品快速使用指南

1. MR 系列产品的默认 IP 地址是 192.168.1.1，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://192.168.1.1> 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。

详细配置说明

一、运行状态

运行状态--->主机状态

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 主机状态 在线主机列表 系统日志 流量查看 实时流量 测试工具 网络设置 高级设置 转发规则 网页监控 访问控制 网络流控 VPN 配置 PPTP配置 系统管理 关于我们 重启设备... 退出登录	主机状态 MS-400	
	设备型号	MS-400
	产品名称	企业级VPN安全网关
	VPN接入授权数	5
	系统时间	Thu, 08 Sep 2011 09:06:27 +0800
	开机时间	0 days, 20:10:13
	CPU负载(1 / 5 / 15 分钟)	0.17 / 0.04 / 0.01
	外网信息	
	MAC 地址	00:25:9C:29:80:9A
	连接类型	DHCP
	IP 地址	192.168.10.155
	子网掩码	255.255.255.0
	默认网关	192.168.10.1
	DNS	192.168.10.1:53
	MTU	1500
	连接状态	Connected
	连接时长	0 days, 00:09:37
	剩余租期	0 days, 11:50:23
	重新获取地址	释放地址
	内网信息	
	内网MAC地址	00:25:9C:29:80:99
	内网IP地址	192.168.100.1
	子网掩码	255.255.255.0
	DHCP	192.168.100.100 - 192.168.100.149

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。

在线主机列表

所处接口	MAC地址	IP地址	计算机名	信噪比	信号质量	TX/RX 速率	剩余租期
vlan1	00:30:B8:C3:45:D0 [oui] [绑定地址]	116.76.160.1					
br0	00:0E:1F:02:13:EC [oui] [绑定地址]	192.168.100.110					0 days, 23:11:15
br0	00:FF:1C:DF:76:E7 [oui] [绑定地址]	192.168.100.115					0 days, 01:16:51
eth1	00:13:13:00:05:61 [oui] [绑定地址] [无线过滤]	192.168.100.120	xbserver	-51 dBm	48	48 / 18	0 days, 23:20:16
br0	00:FF:2C:20:E2:67 [oui] [绑定地址]	192.168.100.130	xiarong				0 days, 23:52:52
eth1	00:13:D3:75:21:8F [oui] [绑定地址] [无线过滤]	192.168.100.139	lqw	-59 dBm	40	- / 48	0 days, 23:20:20
br0	00:FF:CE:20:B4:F2 [oui] [绑定地址]	192.168.100.145	20100412-1056				0 days, 23:46:05
br0	F4:CE:46:6E:66:F0 [oui] [绑定地址]	192.168.100.146	HP6E66F0				0 days, 14:22:08
br0	00:E0:4C:A8:97:18 [oui] [绑定地址]	192.168.100.149					0 days, 22:29:39

背景噪声: -99 dBm

测量



3 seconds

Stop

运行状态--->系统日志

可以查看设备最近的访问信息记录。

Logs

查看最后 25 行
查看最后 50 行
查看最后 100 行
查看全部日志

下载日志记录文件

 查找

» 日志记录管理

二、流量查看

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。

三、测试工具

用于判断路由器到 IP 或域名的连接。

目的主机 IP 或域名: 输入目标 IP 或目标域名

Ping 次数: 默认就可以

包大小：默认就可以

响应时间: 响应时间越小表示网络越好

7

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。

路由追踪

地址

最大跃点数

最大等待时间 (seconds per hop)

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

网络唤醒

MAC 地址	IP 地址	当前状态	主机名称	
00:21:00:00:00:00	192.168.0.1	使用中 (In ARP)	DaJin	
00:10:00:00:00:00	192.168.0.2	-	HongLou	
00:E0:00:00:00:00	192.168.0.3	-	JieMeiFaLang	
00:1E:00:00:00:00	192.168.0.4	-	JingPinDian	
00:1F:00:00:00:00	192.168.0.5	使用中 (In ARP)	Me	
00:E0:00:00:00:00	192.168.0.6	使用中 (In ARP)	Ming	
00:30:00:00:00:00	192.168.0.7	使用中 (In ARP)	NeiYiDian	
00:EA:00:00:00:00	192.168.0.8	使用中 (In ARP)	SanLou	
00:11:00:00:00:00	192.168.0.9	使用中 (In ARP)	ShouYiZhan	
00:E0:00:00:00:00	192.168.0.10	-	SiLouFang	
00:E0:00:00:00:00	192.168.0.11	-	SiLouXiaoFang	
00:E0:00:00:00:00	192.168.0.12	使用中 (In ARP)	Xiu	
00:1F:00:00:00:00	192.168.0.13	使用中 (In ARP)	XuZeng	
00:0B:00:00:00:00	192.168.0.14	使用中 (In ARP)	YuJia	

刷新

MAC 地址列表

立即唤醒

四、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 / Internet

连接类型	PPPoE
用户名	sziwnsl63@163.gd
密码	●●●●●●●●
服务名称	
连接模式	永久在线
断线重连时间	30 (秒)
MTU	默认 1492

LAN

路由IP地址	192.168.100.1
子网掩码	255.255.255.0
静态DNS	0.0.0.0 (IP,port)
	0.0.0.0
	0.0.0.0
DHCP服务器	☒
IP地址段	192.168.100.100 - 192.168.100.149 (50)
地址租用时间	1440 (分钟)
WINS	0.0.0.0

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-->时间设置

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。

时间设置

路由时间	Mon, 23 Aug 2010 11:39:45 +0800
时区设置	UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan ▼
日光节省时间	☒
自动更新时间	每隔4小时 ▼
激活需要时开启服务	☐
NTP时间服务器	默认 ▼
	0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org

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-->静态 DHCP

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

静态DHCP

MAC 地址	IP 地址	主机名称
00:E0:A7:09:C9:18	192.168.100.2	
00:00:00:00:00:00	192.168.100.3	
00:00:00:00:00:00		

添加

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

五、高级设置

高级设置--->防火墙

允许 WAN 口接受 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

防火墙设置

允许WAN口接受PING	☒
允许多播	☒
NAT loopback	所有
启用SYN cookies	☐

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

MAC Address

WAN Port	00:1F:A3:9C:E5:24	Default	Random	Clone PC
LAN MAC	00:1F:A3:9C:E5:23	随机生成	克隆PC	
Wireless Interface	00:1F:A3:9C:E5:25	Default	Random	Clone PC

Router's LAN MAC Address: 00:1F:A3:9C:E5:23
Computer's MAC Address:

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。

目前的路由表

目标IP	网关	子网掩码	度量	接口
210.21.196.6	116.76.160.1	255.255.255.255	0	vlan1 (WAN)
211.148.192.134	116.76.160.1	255.255.255.255	0	vlan1 (WAN)
116.76.160.1	*	255.255.255.255	0	vlan1 (WAN)
192.168.100.0	*	255.255.255.0	0	br0 (LAN)
116.76.160.0	*	255.255.224.0	0	vlan1 (WAN)
127.0.0.0	*	255.0.0.0	0	lo
default	116.76.160.1	0.0.0.0	0	vlan1 (WAN)

静态路由表

目标IP	网关	子网掩码	度量	接口	描述
					添加

其他设置

模式	网关
RIPv1 & v2	禁用
DHCP路由	☒
生成树协议	☐

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

六、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
☒	TCP		80		192.168.10.253	oa
☒	TCP		1433-1434		192.168.10.253	sql
☒	TCP		1723		192.168.100.109	v
☒	TCP					

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

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。

端口触发

启用	协议	触发端口	转发到端口	描述
☐	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000
☒	TCP			

转发规则---> UPnP/NAT-PMP

UPnP 转发端口

外部端口	内部端口	内部IP地址	协议	描述
全部删除 刷新				

设置

开启UPnP ☐

开启NAT-PMP ☐

Inactive Rules Cleaning ☒

安全模式 ☒ (当启用该功能时,UPnP客户端只允许添加映射到自己的IP)

在 网上邻居 中显示 ☐

七、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。

基本设置

开启QoS	☒
下列小包优先	☒ ACK ☐ SYN ☐ FIN ☐ RST
ICMP优先	☐
当设置改变时重置等级	☐
默认等级	低
Qdisc队列类型	sfq

上传限制

最大上行宽带	430	kbit/s	
最高	80%	100%	344 - 430 kbit/s
高	10%	100%	43 - 430 kbit/s
中	5%	80%	21 - 344 kbit/s
低	3%	50%	12 - 215 kbit/s
最低	2%	10%	8 - 43 kbit/s
自定义等级A	1%	50%	4 - 215 kbit/s
自定义等级B	1%	40%	4 - 172 kbit/s
自定义等级C	1%	30%	4 - 129 kbit/s
自定义等级D	1%	20%	4 - 86 kbit/s
自定义等级E	1%	10%	4 - 43 kbit/s

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。

下载限制

最大下载宽带	2048 kbit/s
最高	None
高	None
中	None
低	None
最低	None
自定义等级A	None
自定义等级B	None
自定义等级C	None
自定义等级D	None
自定义等级E	None

TCP 乱序 (网络堵塞控制)

开启TCP Vegas	☐
Alpha	2
Beta	6
Gamma	2

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

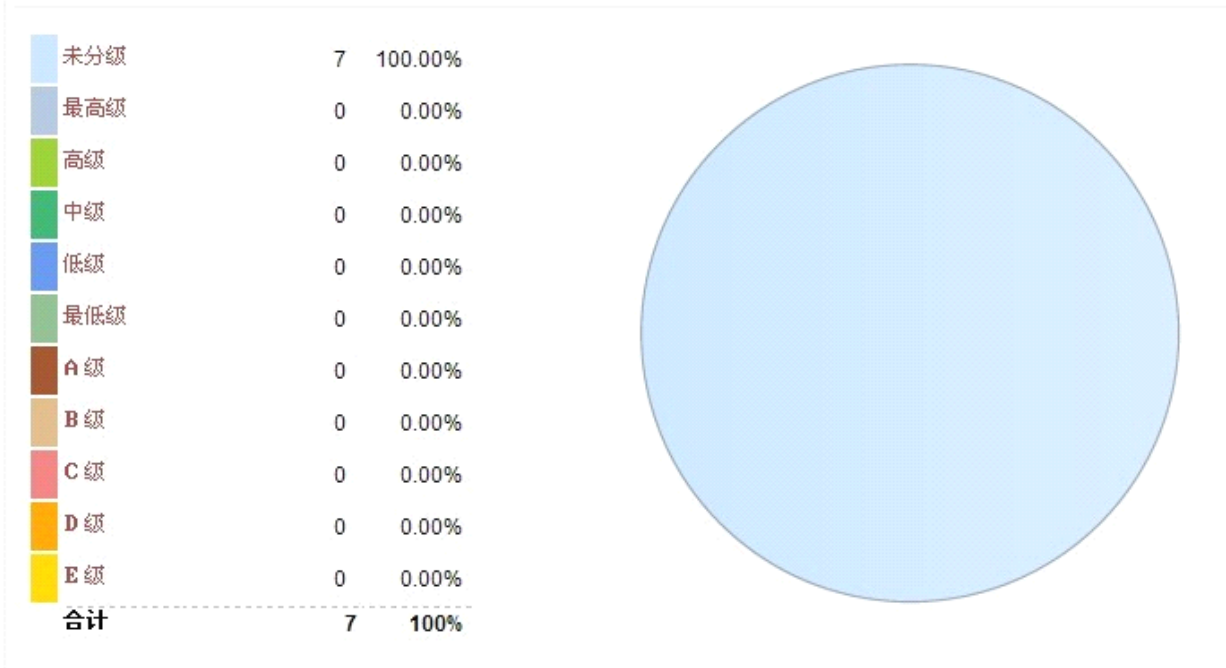
Match Rule	Class	Description
TCP Dst Port: 80,443 Transferred: 0 - 512kB	High	WWW
TCP/UDP Dst Port: 12701	Highest	game
TCP Dst Port: 80,443 Transferred: 512kB+	Low	WWW (512K+)
TCP/UDP Dst Port: 53 Transferred: 0 - 2kB	Highest	DNS
TCP/UDP Dst Port: 53 Transferred: 2kB+	Lowest	DNS (2K+)
TCP/UDP Dst Port: 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



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

八、网页监控

用于查看网页访问记录

网页访问记录

访问时间	主机IP地址	网址
Mon Mar 14 2011, 15:49:38	192.168.6.115	fodder.qq.com
Mon Mar 14 2011, 15:49:23	192.168.6.117	www.skycn.com
Mon Mar 14 2011, 15:49:21	192.168.6.117	track.chinahr.com
Mon Mar 14 2011, 15:49:21	192.168.6.117	searchjob.chinahr.cc
Mon Mar 14 2011, 15:49:21	192.168.6.117	js.mychinahr.com
Mon Mar 14 2011, 15:49:21	192.168.6.117	cookie.monster.com
Mon Mar 14 2011, 15:49:21	192.168.6.117	st.mychinahr.com
Mon Mar 14 2011, 15:48:33	192.168.6.117	image.chinahr.com
Mon Mar 14 2011, 15:48:28	192.168.6.117	ad-apac.doubleclick.
Mon Mar 14 2011, 15:48:28	192.168.6.117	image.mychinahr.coi
Mon Mar 14 2011, 15:48:27	192.168.6.117	www.chinahr.com
Mon Mar 14 2011, 15:48:27	192.168.6.117	promolog.chinahr.co
Mon Mar 14 2011, 15:48:24	192.168.6.117	nsclick.baidu.com
Mon Mar 14 2011, 15:48:22	192.168.6.117	www.hao123.com
Mon Mar 14 2011, 15:48:16	192.168.6.117	drmcm.baidu.com
Mon Mar 14 2011, 15:48:16	192.168.6.117	app.hao123.com
Mon Mar 14 2011, 15:48:16	192.168.6.117	a.baidu.com

九、访问控制

这里可以设置设备下面的计算机限制访问互联网中的程序和网页，如下图：

访问控制列表

MR-1:

设置说明	时间段
MSN	Everyday Disabled
qqq	Everyday 0:00 to 0:00 (the following day) Disabled

添加规则

十、VPN 设置

VPN 设置--->服务器端配置

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、协议等。

MS-400

运行状态

主机状态

在线主机列表

系统日志

流量查看

实时流量

测试工具

网络设置

高级设置

转发规则

网页监控

访问控制

网络流控

VPN 配置

服务器端配置

 客户端配置

 实时管理

 日志管理

 寻址服务

PPTP 配置

系统管理

关于我们

重启设备...

退出登录

VPN 服务端配置

服务端

基本设置 高级设置

封装协议 UDP

通讯端口 1194

虚拟 IP 地址 10.2.0.1

子网掩码 255.255.255.0

无特殊需要用默认即可，只需要在用户管理里添加用户就可以

用户管理

启用	认证类型	帐号	密码	IP 地址	子网掩码	有效期	备注
启用	纯软件客户端	boss	manager	10.2.0.3	255.255.255.0	2060-12-01-12	李总
启用	纯软件客户端	usr1	1234	10.2.0.2	255.255.255.0	2060-12-01-12	广州办事处
☒	纯软件客户端			10.2.0.4	255.255.255.0	2060-12-01-12	

用来备注这个帐号是给哪个人用的，很人性化吧

Add

• **IP 地址** (说明) - 需要服务端自动分配 IP 时可以在 IP 地址栏里填写数字 0，服务端会自动分配 IP 地址。

• **子网掩码** (说明) - 需要服务端自动分配子网掩码时可以在子网掩码栏里填写数字 0，服务端会自动分配。

• **有效期** (说明) - 有效期的格式为: 2011-1-12-13 (2011 年 1 月 12 日下午 1 点到期)，时间采用 24 小时制，时区默认请设置为 +8 区。

保存

取消

封装协议：有 UDP 和 TCP 两种，可以自行选择，但是要保持客户端和服务端一致才能建立连接。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。

通讯端口：VPN 通信所使用的端口号，默认为 1194，可更改，一般默认即可

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。

VPN 服务器—高级设置



IP 伪装：有些特殊情况要求特定的 IP 才能访问业务系统，如航空售票、社保刷卡、保险系统等，或者无法设置路由表，只需打上勾，就不需要设置任何路由表即可实现业务的访问。

代理客户端上网：允许客户端加接 VPN 后，经由总部的宽带上互联网，常用于反电信封锁或一些特殊 IP 地址的转换。

服务器端自动加分支路由：选取此项，客户端如果是硬件分支，VPN 连通后，VPN 服务器端会自动添加分支网段的路由，实现 LAN TO LAN 互访。

自定义设置：一般用于高级用户或特殊网络情况时，留给迅博工程师的高级参数，正常情况无需输入。

将如下路由推给客户端：用于服务器端多子网（多网段）的情况，在 VPN 接入时会推送所输网段路由给客户端。

VPN 配置—用户管理

这里的用户管理是 VPN 服务器端管理要接入到公司的 VPN 系统的帐号信息，添加、删除和编辑帐号信息保存号实时生效，不需要重启 VPN 服务。

用户管理

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	纯软件客户端	boss	manager	10.2.0.3	255.255.255.0	2060-12-01-12	李总
启用	纯软件客户端	usr1	1234	10.2.0.2	255.255.255.0	2060-12-01-12	广州办事处 *
☒	纯软件客户端			10.2.0.4	255.255.255.0	2060-12-01-12	
							Add

- **IP地址** (说明) - 需要服务端自动分配IP时可以在IP地址栏里填写数字0,服务端会自动分配IP地址.
- **子网掩码** (说明) - 需要服务端自动分配子网掩码时可以在子网掩码栏里填写数字0,服务端会自动分配.
- **有效期** (说明) - 有效期的格式为:2011-1-12-13(2011年1月12日下午1点到13点),时间采用24小时制,时区默认请设置为+8区.

启用: 一定要启用, 否则禁止该用户接入

认证类型: 分为纯软件客户端, 硬件分支用户, 硬件认证用户。如果认证类型用错, 无法完成认证, VPN 无法正常连接。

IP 地址和子网掩码: 和服务器端虚拟 IP 地址须设置为同一网段。

有效期: 用于设置帐号的有效期限, 超过有效期会自动停止客户端的连接, 目前精确到小时。

备注: 对每个帐号进行说明描述, 方便管理, 中文的显示方式突显人性化操作。

VPN 配置—客户端配置

这里需设备作为客户端时, 才需要设置, 如果是软件客户端, 则留空。具体设置如图:

封装协议: 保持跟服务器端相同, 有两种协议 TCP 和 UDP。

通讯端口: 保持与服务器端相同, 默认为: 1194

服务器地址: 输入服务器端的寻址脚本, 一定是以.xml 结束

备用服务器地址: 只能是服务器端的域名或 IP 地址, 可选项, 可为空。

帐号/密码: 此处输入 VPN 服务端授权的帐号、密码。

与服务端在相同子网: 如查服务器端和客户端在相同网段上, 选择启用, 可以实现网上邻居的功能, 默认选择禁用。

VPN 配置——实时管理

主要是用于停止启动 VPN 服务，以及查看 VPN 的连接信息，信息包括客户端的用户名、虚拟 IP 地址、外网 IP，接入端口号，接入时间以及所在服务器端的情况；在线用户数帮您统计出 VPN 的在线总人数。



The screenshot shows the XUNBO VPN Management Interface. The top banner includes the XUNBO logo, the text "关注网络安全，关注安全接入" (Pay attention to network security, pay attention to secure access), and the URL "Http://www.vpnsoft.net". The interface is divided into a left sidebar with navigation options and a main content area.

Left Sidebar Navigation:

- 运行状态 (Running Status)
- 主机状态 (Host Status)
- 在线主机列表 (Online Host List)
- 系统日志 (System Log)
- 流量查看 (Traffic View)
- 实时流量 (Real-time Traffic)
- 测试工具 (Test Tools)
- 网络设置 (Network Settings)
- 高级设置 (Advanced Settings)
- 转发规则 (Forwarding Rules)
- 网页监控 (Web Monitoring)
- 访问控制 (Access Control)
- 网络流控 (Network Flow Control)
- VPN 配置 (VPN Configuration)**

Main Content Area:

- 服务端管理 (Server Management):** Includes a "关闭程序" (Close Program) button.
- 客户端管理 (Client Management):** Includes a "启动程序" (Start Program) button.
- 在线用户列表 (Online User List):** Shows the number of online users as 1.

用户名	接入IP地址:端口	虚拟IP地址	接收字节	发送字节	接入时间
usr1	192.168.100.108:4425	10.2.0.2	2142	4961	2011年9月7日星期三 17:20:11

VPN 配置——日志管理

主要用于查看 VPN 的连接活动信息



The screenshot shows the XUNBO VPN Management Interface, specifically the Log Management section. The top banner is identical to the previous screenshot. The left sidebar navigation is also identical.

Main Content Area:

- 日志管理 (Log Management):** Includes tabs for "客户端" (Client) and "服务端" (Server).

Log Entries:

```

Wed Sep 7 17:20:07 2011 OpenVPN 2.1.1 mipsel-unknown-linux-gnu [SSL] [LZO2] [EPOLL] built on Aug 10 2011
Wed Sep 7 17:20:07 2011 NOTE: when bridging your LAN adapter with the TAP adapter, note that the new bridge adapter will often take on its own IP address that is different from what the LAN adapter was previously set to
Wed Sep 7 17:20:07 2011 NOTE: the current --script-security setting may allow this configuration to call user-defined scripts
Wed Sep 7 17:20:09 2011 WARNING: file '/etc/ca/server.key' is group or others accessible
Wed Sep 7 17:20:09 2011 WARNING: POTENTIALLY DANGEROUS OPTION --client-cert-not-required may accept clients which do not present a certificate
Wed Sep 7 17:20:09 2011 ***** WARNING *****: null cipher specified, no encryption will be used
Wed Sep 7 17:20:09 2011 TUN/TAP device tap21 opened
Wed Sep 7 17:20:09 2011 /sbin/ifconfig tap21 10.2.0.1 netmask 255.255.255.0 mtu 1500 broadcast 10.2.0.255
Wed Sep 7 17:20:09 2011 UDPv4 link local (bound): [undef]:1194
Wed Sep 7 17:20:09 2011 UDPv4 link remote: [undef]
Wed Sep 7 17:20:09 2011 Initialization Sequence Completed
Wed Sep 7 17:20:11 2011 192.168.100.108:4425 Re-using SSL/TLS context
Wed Sep 7 17:20:11 2011 192.168.100.108:4425 LZO compression initialized
Wed Sep 7 17:20:15 2011 192.168.100.108:4425 [usr1] Peer Connection Initiated with 192.168.100.108:4425
  
```

VPN 配置——寻址服务

主要用于解决 ADSL 动态 IP 地址变化问题，通过迅博公司的目录服务和动态 DNS 服务，客户不需要申请静态 IP 地址和动态域名，实现 VPN 的稳定高效的联接。

说明：IP 地址一般是采用 WAN 地址，即设备的 WAN 口 IP 地址，常用于 VPN 进行 ADSL 拨号或通过 DHCP 的方式获取公网 IP 地址的情况，但是如果 VPN 工作在路由器后或透明

模式时，一定要选用：

IP address

使用外部地址检测

方

式，否则会造成寻址错误。

寻址地址设置

IP address

使用WAN地址 116.24.186.87 (推荐)

自动刷新次数

28

days (0 = disable)

寻址服务 1

类型

目录服务

URL

http://www.vpnsoft.net/demo/xinyu.asp

(Use @IP for the current IP address)

Force next update



Last IP Address

2011-03-07 15:03:02:
116.24.186.87

Last Result

2011-03-07 15:03:02:
good

寻址服务 2

类型

启博DDNS

URL

http://www.szsec.net/

Username

happy

Password

••••••••

Hostname

xinyu.szsec.net

Force next update



Last IP Address

2011-03-07 15:03:04:
116.24.186.87

2011-03-07 15:03:04:

两种寻址方式互为备份，保证了 VPN 连接的可靠性，再也不会出现什么对端未在线和心跳超时的提示。

十一. PPTP 配置

PPTP 也是一种常见 VPN 连接方式，特别是不需要安装软件，只要管理员分配一个帐号和密码，直接通过 windows 新建连接就可以连接到公司网络，另外通过这种连接方式可以实现 MS-400 与其他厂商的 VPN 设备之间互联。

服务器端配置：



启用：这里点了启用后，以后设备重启后会自动启动 VPN 服务

PPTP 本地地址：是指 PPTP 服务器本身的虚拟 IP 地址要以任意设，但是不可以和设备的路由 IP 在同一个网段上。

PPTP 客户端地址池：这个是客户端通过 PPTP 拨号连接到本设备上后，获取的 VPN 虚拟 IP 地址，注意格式。

PPTP 用户名列表：这里是用来管理 PPTP 拨号进来的帐号信息的，注意点是，如果是单机拨入不需要输入客户端办公网络和子网掩码，如果客户端也是一台硬件设备，实现两个设备之间对接，需要实现 LAN TO LAN 互联，则需要输入对端的办公子网和子网掩码，一定是个网段，不是个 IP 地址。

注意点：只有配置了 **PPTP** 服务器的参数，并添加了用户帐号，并保存后，才能启动 **PPTP** 服务，否则启动不起来

在线用户列表：



主要用来查看 VPN 拨号信息在线用户的信息，看哪个用户在否在线，以判断 VPN 连接是否正常。

PPTP 客户端：



十二. 系统管理

系统管理--->访问管理

Web 远程管理

本地访问	HTTP
HTTP 端口	80
远程访问	HTTP
远程访问端口	8080
允许无线用户访问	☒
Web颜色方案	Blue
默认展开的菜单	
运行状态	☒
带宽查看	☐
测试工具	☐
基本设置	☐
高级设置	☐
转发规则	☐
QoS设置	☐
系统管理	☐

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

开机时启动	☒
端口	23
关闭 立即	

远程 Web /TELNET登录限制

允许登录的IP地址段:	
(optional; ex: "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2" or "me.example.com")	
限制连接次数	☐ SSH / ☐ Telnet
	3 次每 60 秒

密码设置

密码	
(再次输入密码确认)	

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--->设置管理

备份设置

MR_v1270476_mec1310 .cfg

[下载](#)

恢复设置

请选择文件:

恢复默认设置

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--->升级固件

升级固件

选择固件:

☐ 刷机后,清除NVRAM

目前固件的版本: 1.27.0397 K26 VPN

路由剩余容量: 24.43 MB (剩余内存一定要大于固件的大小,才能升级)

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。

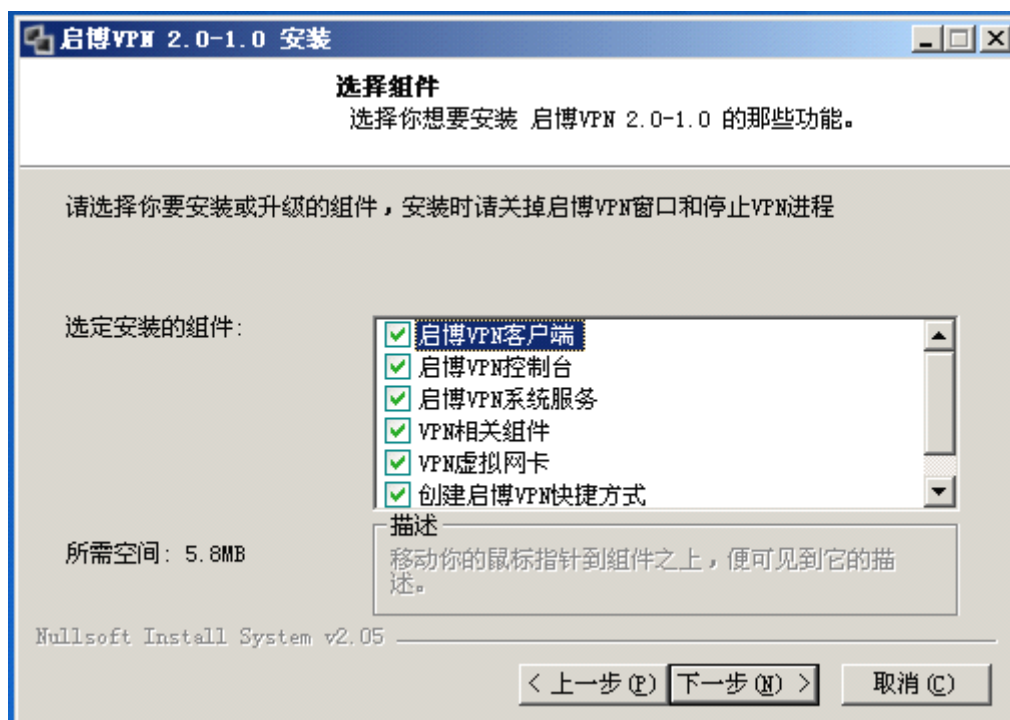
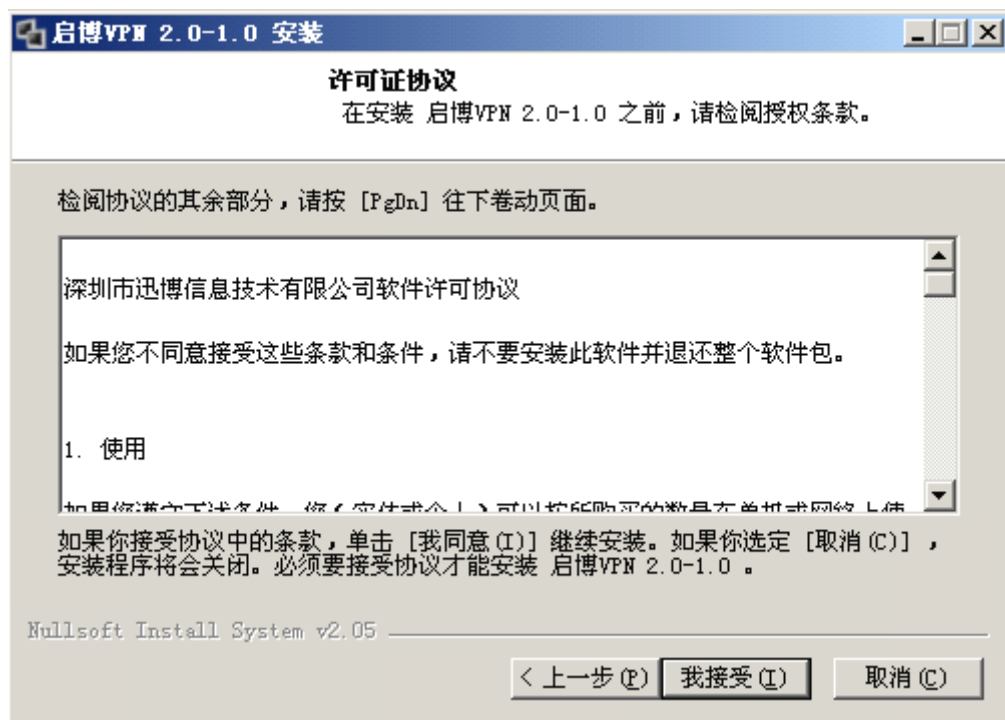
十三. VPN 软件客户端

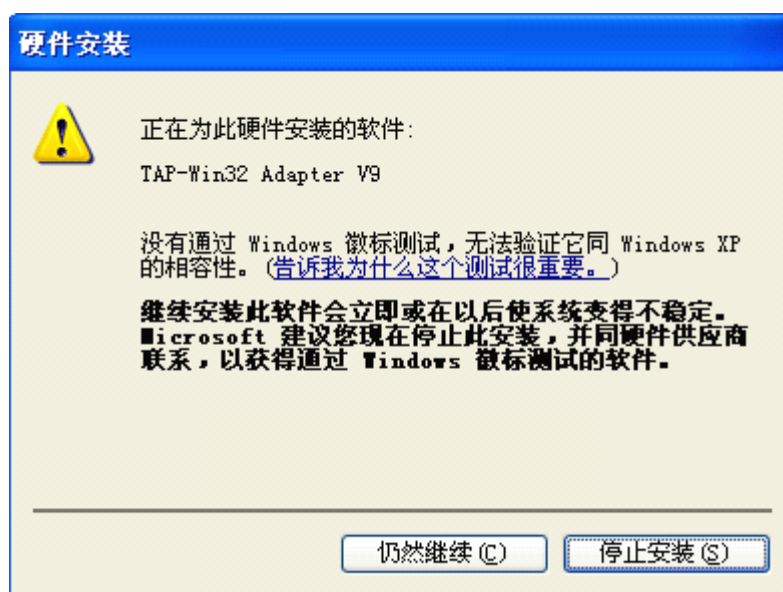
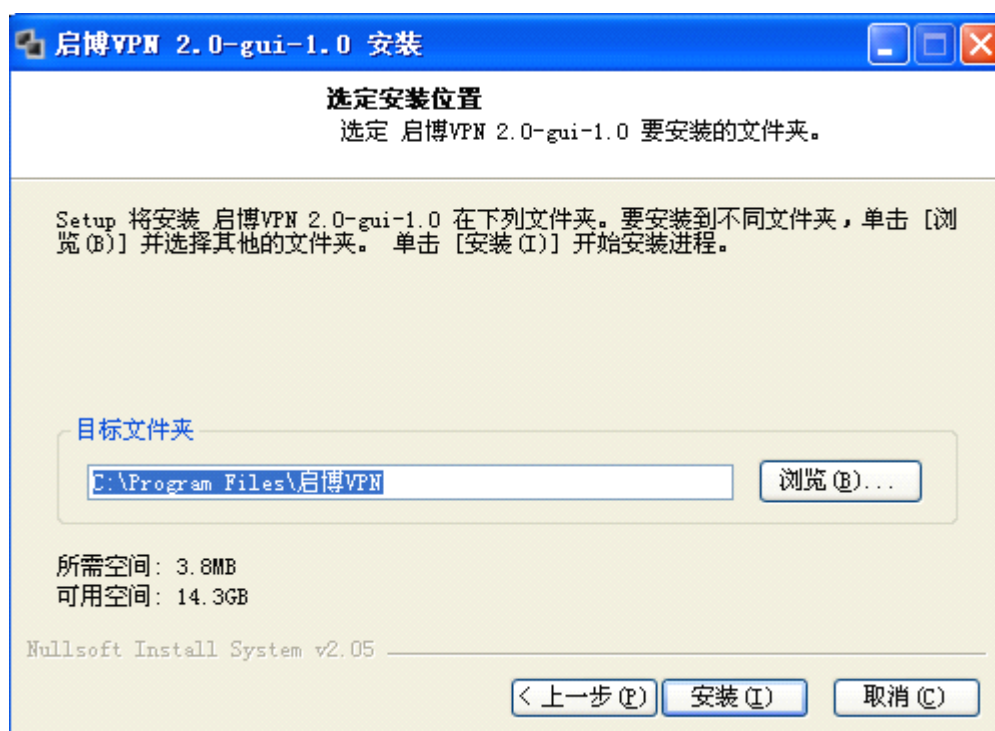
VPN 软件客户端--->VPN 软件安装

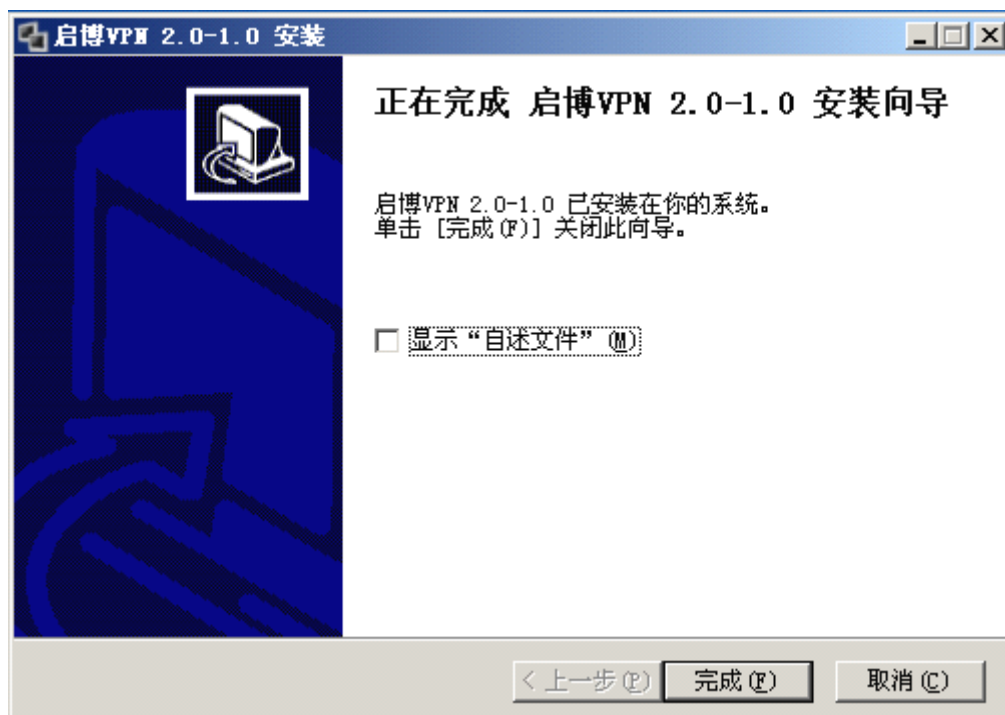
我司的 VPN 软件客户端可以与硬件 VPN 联通，使用 VPN 软件客户端连接的用户，需要先在用户电脑上安装指定的 VPN 客户端软件，第一次安装客户端时会要求安装虚拟网卡，选择“仍然继续”即可，安装过程如下图。

下面为安装示意图：



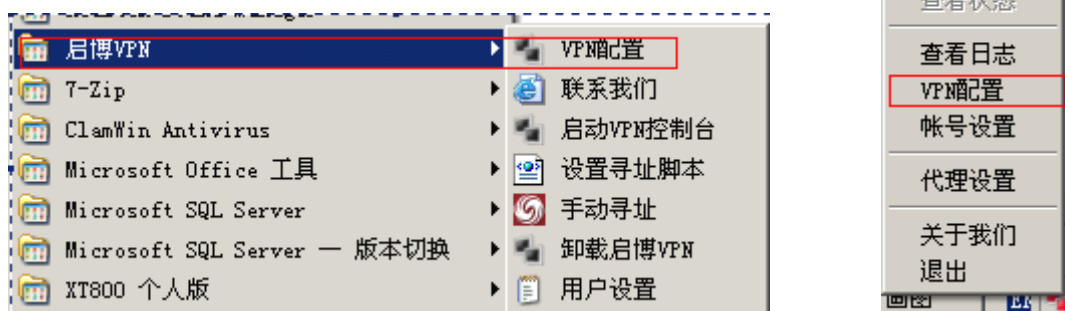




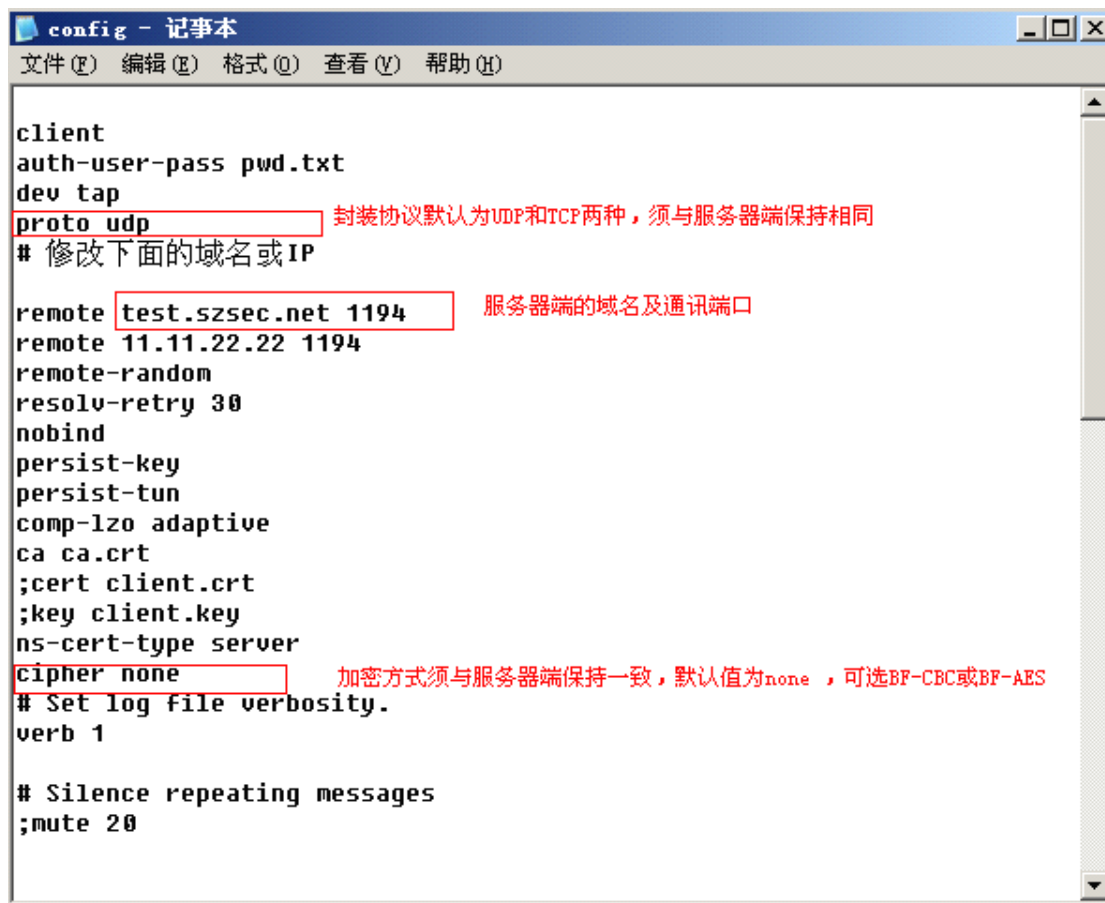


VPN 软件客户端——>VPN 软件参数配置

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”->“启动 VPN 控制台”，然后对任务栏 VPN 控制台图标右键选择“修改配置”来打开。



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。



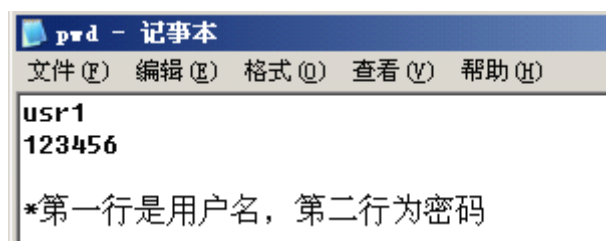
3. 设置寻址脚本：寻址脚本主要用于采用域名方式连接不成功时的备用寻址方式，设置方法为，开始—程序---启博 VPN---设置寻址脚本，以文本的方式打开



输入正常的寻址脚本即可，该脚本的信息在服务器端设备里的寻址服务里有。



4. 帐号设置，对任务栏中 VPN 程序右键单击帐号设置，输入相应 VPN 帐号密码，



输入完毕，点保存，双击右下角的 VPN 图标 ，即开始连接 VPN。VPN 图标变成绿色表示连接成功。

5. 手动寻址：如果 VPN 一直加接不上对端，有时可能是获取对端的 IP 地址不对，这时可以手工执行一下手动寻址，然后再重新连接 VPN 即可。



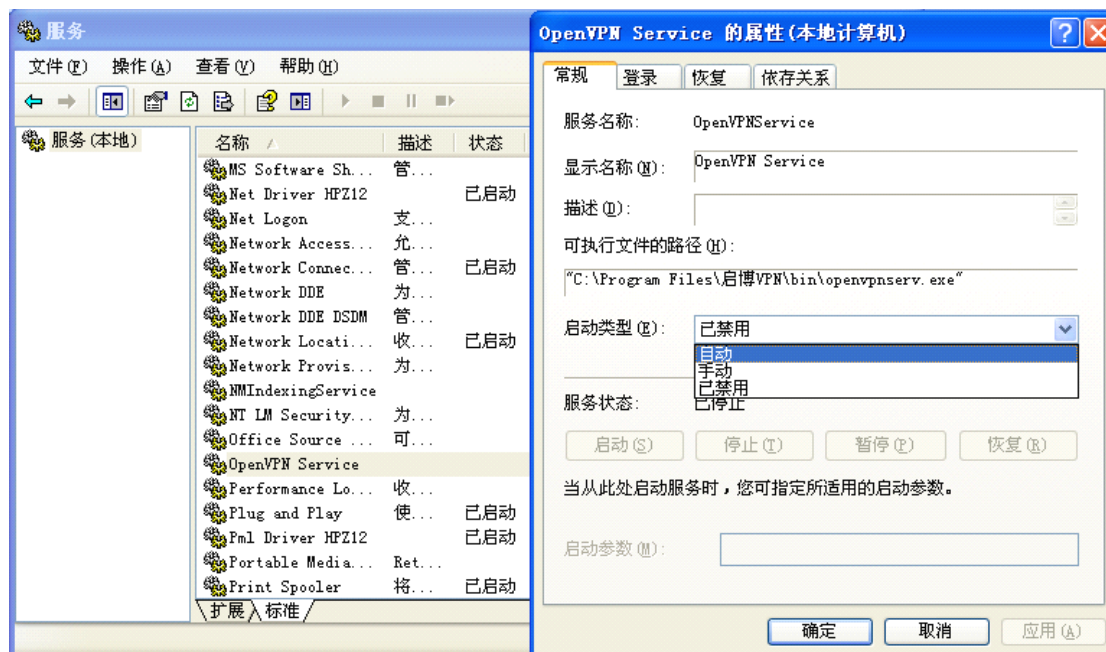
VPN 软件客户端——>VPN 软件开机自启动设置

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。



常见组网应用方案

硬件网关与硬件网关互联

为了保证 VPN 路由正常，习惯上 VPN 服务器端和分支端要在不同的网段上，比如公司总部用 192.168.1.X 的网段，分公司用 192.168.2.X 的网段。这里举例，就以总部用 192.168.1.0 网段，分支用 192.168.2.0 的网段，下面是具体配置方法，其中 VPN 配置里的寻址服务，在出厂时已经设置好，不能随意改动，否则会造成联不通的情况。

先配置 VPN 服务器端：

VPN服务端配置

服务端1

服务端2

基本设置

高级设置

封装协议

UDP

通讯端口

1194

虚拟IP地址

10.2.0.1

虚拟IP可以任意设置

子网掩码

255.255.255.0

加密类型

使用默认

自动路由

启用(推荐)

允许客户端互访

启用(推荐)

IP伪装

☐

代理客户端上网

☐

服务器自动加分支路由

☒

VPN自动路由功能，无须手工添加任何路由，VPN全自动化完成

自定义设置

如果服务器端有多个网段让客户访问，可以在这里添加，VPN服务会自动推送给客户端

将如下路由推给客户端

启用	子网段	子网掩码	注释
☐			

Add

用户管理中新建用户用于 VPN 认证接入：

用户管理

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	硬件分支用户	shanghai	sh123	10.2.0.12	255.255.255.0	2037-07-23-20	
启用	硬件分支用户	chengdu	cd123	10.2.0.11	255.255.255.0	2039-07-23-20	*
☒	纯软件客户端						

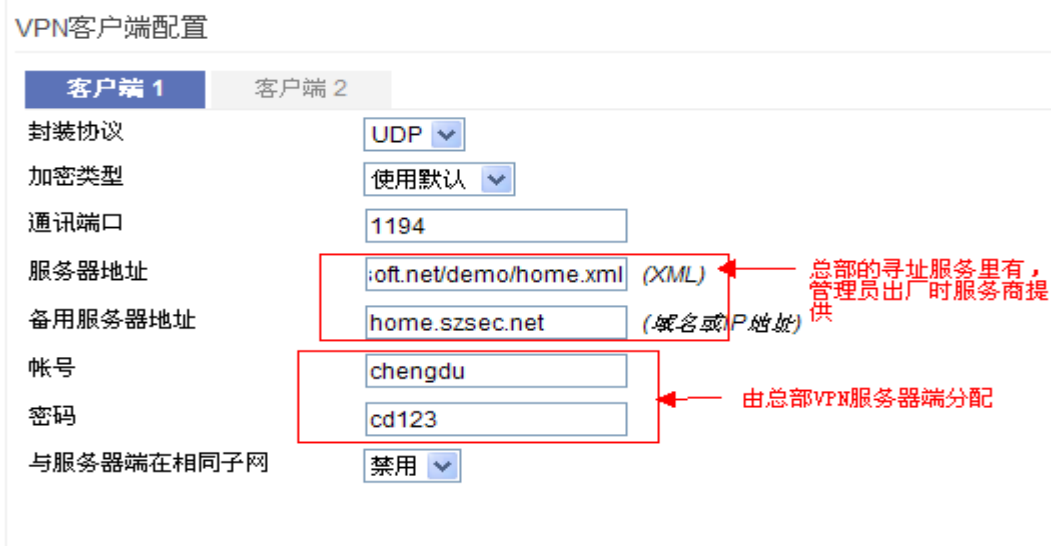
Add

注意点：新建用户的 IP 地址要与 VPN 服务器端配置里的虚拟 IP 地址要在同一个网段上，即前三段要相同。

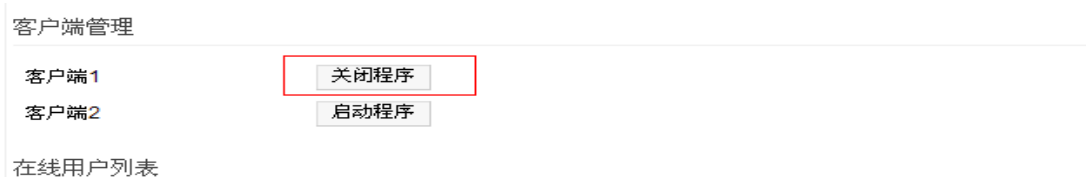
实时管理---启动 VPN 服务：



客户端配置:



启动 VPN 客户端



VPN 连接成功后，在服务器端的 VPN 配置---实时管理中能看到客户接进入的信息，如下图

vpnsort

服务端管理

服务端1 关闭程序

服务端2 启动程序

客户端管理

客户端1 启动程序

客户端2 启动程序

在线用户列表

在线用户数:1

用户名	接入IP地址:端口	虚拟IP地址	接收字节	发送字节	接入时间	所在服务端
chengdu	115.50.6.136:1033	10.2.0.11	1434	3650	2011年7月23日星期六 21:51:15	服务端1

硬件网关做服务器，客户端用软件方式接入

首先配置 MR 硬件 VPN 网关，如下图：

服务端1

服务端2

基本设置

高级设置

封装协议 UDP

通讯端口 1194

虚拟IP地址 10.2.0.1

子网掩码 255.255.255.0

加密类型 使用默认

自动路由 启用(推荐)

允许客户端互访 启用(推荐)

用户管里中，新建 VPN 接入帐号：**认证类型一定选“纯软件客户端”**

用户管理

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	纯软件客户端	usr1	123456	10.2.0.11	255.255.255.0	2099-10-10-10	
启用	纯软件客户端	usr2	123456	10.2.0.12	255.255.255.0	2099-10-10-10	✖
☒	纯软件客户端						

Add

客户端安装 VPN 软件客户端，输入正确的服务器地址和用户名密码即可接入。

这里要特别提到的是，有些客户的 **ERP** 软件或共享文档特别要求，必须通过 **windows** 网上邻居功能才能正常工作，这里我们只需做一些小小的改变就可以，如果 VPN 设备的地址是 192.168.1.1

网络设置

网络设置
时间设置
静态DHCP
高级设置
转发规则
智能Qos
网页监控
访问控制
网络流控
VPN 配置
PPTP配置
系统管理
关于我们
重启设备...
退出登录

连接模式 保持激活

断线重连 30 (seconds)

MTU Default 1492

LAN

路由IP地址 192.168.1.1

子网掩码 255.255.255.0

静态DNS 0.0.0.0 (IP:port)

0.0.0.0

0.0.0.0

DHCP服务器 ☒

IP地址范围 192.168.1.100 - 192.168.1.149 (50)

租约时间 1440 (分钟)

WINS服务器 0.0.0.0

VPN 服务器端配置

VPN服务端配置

服务端1 服务端2

基本设置 高级设置

封装协议 UDP

通讯端口 1194

虚拟IP地址 192.168.1.1

子网掩码 255.255.255.0

加密类型 使用默认

自动路由 禁用

允许客户端互访 启用(推荐)

服务器端虚拟 IP 和路由 IP 设成相同。

用户管理---新建用户时注意 Ip 地址的设置

用户管理

vpnsft

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	纯软件客户端	lxy	345	192.168.1.201	255.255.255.0	2037-07-23-20	✖
启用	纯软件客户端	dylh	123	192.168.1.200	255.255.255.0	2039-07-23-20	
☒	纯软件客户端						

Add

这样客户端接入后就会和总部这里内网 IP 在同一个网段上，直接可以在网上邻居看到总部的内网计算机了。

总部与分支要在相同网段（硬件之间网上邻居）

有时客户的要求实现网上邻居功能或者有一些 ERP 类管理软件，总部和分支必须在同一个网段才能访问，针对这种需求，MR 系列 VPN 都是支持的，配置方法如下
首先规划公司网络，因为总部和分支机构要在同一个网段上，根据每个地方的计算机终端数量，比如总部的 IP 地址:192.168.1.1--192.168.1.100

分支 1 的 IP 地址: 192.168.1.101--192.168.1.150

分支 2 的 IP 地址: 192.168.1.151-192.168.1.200

在网络设置里：总部的设置如下：

网络设置	MTU	Default	1500
流量查看	LAN		
实时流量			
测试工具			
网络设置	路由IP地址	192.168.1.1	
网络设置	子网掩码	255.255.255.0	
时间设置	静态DNS	0.0.0.0	(IP:port)
静态DHCP		0.0.0.0	
高级设置		0.0.0.0	
转发规则	DHCP服务器	☒	
智能Qos	IP地址范围	192.168.1.2 - 192.168.1.100	(50)
网页监控	租约时间	1440	(分钟)
访问控制	WINS服务器	0.0.0.0	
网络流控			
VPN 配置			
PPTP配置			
系统管理			

分支 1 的网络设置如下：

网络设置	路由IP地址	192.168.1.101	
网络设置	子网掩码	255.255.255.0	
时间设置	静态DNS	0.0.0.0	(IP:port)
静态DHCP		0.0.0.0	
高级设置		0.0.0.0	
转发规则	DHCP服务器	☒	
智能Qos	IP地址范围	192.168.1.100 - 192.168.1.150	(51)
网页监控	租约时间	1440	(分钟)
访问控制	WINS服务器	0.0.0.0	
网络流控			
VPN 配置			
PPTP配置			

分支 2 的网络设置如下：

测试工具		LAN	
网络设置	路由IP地址	192.168.1.151	
网络设置	子网掩码	255.255.255.0	
时间设置	静态DNS	0.0.0.0	(IP:port)
静态DHCP		0.0.0.0	
高级设置		0.0.0.0	
转发规则	DHCP服务器	☒	
智能Qos	IP地址范围	192.168.1.150 - 192.168.1.200 (51)	
网页监控	租约时间	1440	(分钟)
访问控制	WINS服务器	0.0.0.0	
网络流控			
VPN 配置			
PPTP配置			

下面要进行 VPN 设置,这里要用到 VPN 的桥接功能, 设置时, VPN 服务器端的虚拟 IP 地址要设置成和 VPN 设备本身的路由 IP 一致; 用户管理中给客户端分配的 VPN 虚拟 IP 地址也要和路由 IP 在同一个网段上的地址, 可不必和客户端的设备 IP 相同,

VPN服务端配置

服务端1		服务端2	
基本设置		高级设置	
封装协议	UDP		
通讯端口	1194		
虚拟IP地址	192.168.1.1		
子网掩码	255.255.255.0		
加密类型	使用默认		
自动路由	禁用		
允许客户端互访	启用 (推荐)		

和网段设置里路由IP保持相同

因为总部和分支相同网段不需要路由, 故禁用

用户管理：

用户管理

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	硬件分支用户	chengdu	cd988789	192.168.1.145	255.255.255.0	2039-07-23-20	成都分公司
启用	硬件分支用户	shanghai	sh8899234	192.168.1.99	255.255.255.0	2037-07-23-20	上海分公司
☒	纯软件客户端						

注意点, 分配给客户端的虚拟 IP 地址和路由 IP 在同一个网段上;

下面看一下分支端的配置：

分支一配置：

VPN客户端配置

客户端 1	客户端 2
封装协议	UDP
加密类型	使用默认
通讯端口	1194
服务器地址	http://www.vpnsoft.net/b (XML)
备用服务器地址	demo.vpnsoft.net (域名或IP地址)
帐号	shanghai
密码	sh8899234
与服务器端在相同子网	启用

与服务器端配置必需一致

这个很关键，如果不启用则前功尽弃

分支二配置：

VPN客户端配置

客户端 1	客户端 2
封装协议	UDP
加密类型	使用默认
通讯端口	1194
服务器地址	http://www.vpnsoft.net/b (XML)
备用服务器地址	demo.vpnsoft.net (域名或IP地址)
帐号	chengdu
密码	cd988789
与服务器端在相同子网	启用

与服务器端必须保持一致

切记：必须一定要启用

服务器地址和备用服务器地址，是在服务器端的 VPN 配置里—寻址服务的内容，但记住服务器地址，结果是.xml，寻址服务里是.asp 或 .php ,注意这个细节变化

至此 VPN 配置完成，在 VPN 配置---实时管理中，启动 VPN 服务即可。

总部用透明模式接入

有时客户那里网络已经规划的很好，上网有专业的路由器防火墙，在安装 VPN 设备时只能放在路由器防火墙后，并具不能对网络拓扑结构进行改变，这里可以用 MR 网关的透明模

式接入方式（也叫单臂直连的方式），具体设置方法如下图：

运行状态 主机状态 在线主机列表 系统日志 流量查看 实时流量 测试工具 网络设置 网络设置 时间设置 静态DHCP 高级设置 转发规则 智能Qos 网页监控	WAN / Internet	
	连接类型	透明模式
	LAN	
	路由IP地址	192.168.6.254
	子网掩码	255.255.255.0
	默认网关	192.168.6.1
	静态DNS	202.96.134.133 (IP, port) 202.96.128.166 0.0.0.0
	DHCP服务器	☐

内网中任一空闲IP地址均可，

路由器防火墙的IP地址，也就是常说的内网电脑的默认网关

这个一定要正常填写当地的ISP的DNS，这里是以深圳电信DNS为例。

为了避免内网中电脑获取错误的网关，透明模式下请关闭DHCP服务

VPN 配置方法和普通的相同，不同的是寻址服务方式，

透明模式接入用下面方式：

寻址地址设置	
IP address	使用外部地址检测
自动刷新次数	1 days (0 = disable)
寻址服务 1	

做为路由网关接入用下面方式：

寻址地址设置	
IP address	使用WAN地址 116.24.75.104 (推荐)
自动刷新次数	1 days (0 = disable)
寻址服务 1	

如果 VPN 服务器端做为透明模式接入，需要在上层的路由器防火墙为 VPN 接入做端口映射，即虚拟服务，如 VPN 用的端口为 1194，VPN 设备的 IP 为 192.168.6.254，我们要在路由防火墙做如下虚拟服务：否则 VPN 客户端无法与 VPN 服务器建立隧道连接。如果客户端是透明模式接入，不需要做端口映射



这样 VPN 客户端就可以接入 VPN 服务器，但是此时只能访问到 VPN 设备本身，却无法访问总部内网的服务器或其他计算机，这是因为其他计算机的默认网关是指向路由器防火墙，所有数据包都不经过 VPN 设备，故此必须在路由器防火墙上做静态路由才可以和 VPN 客户端互访，具体做法如下图，不同品牌路由器会有差异。



第二条路由是到 VPN 虚拟 IP 地址的路由，第一条路由是到 VPN 分支的路由，网关是指向 VPN 设备的 IP 地址，这样分支客户接入后就可以访问总部内网了。

客户端用透明模式接入的情况，只是不需要做端口映射，同样需要在上级路由做静态路由。

透明模式接入是一种复杂应用，如果设置上有问题可以联系供应商提供技术支持。

常见问题

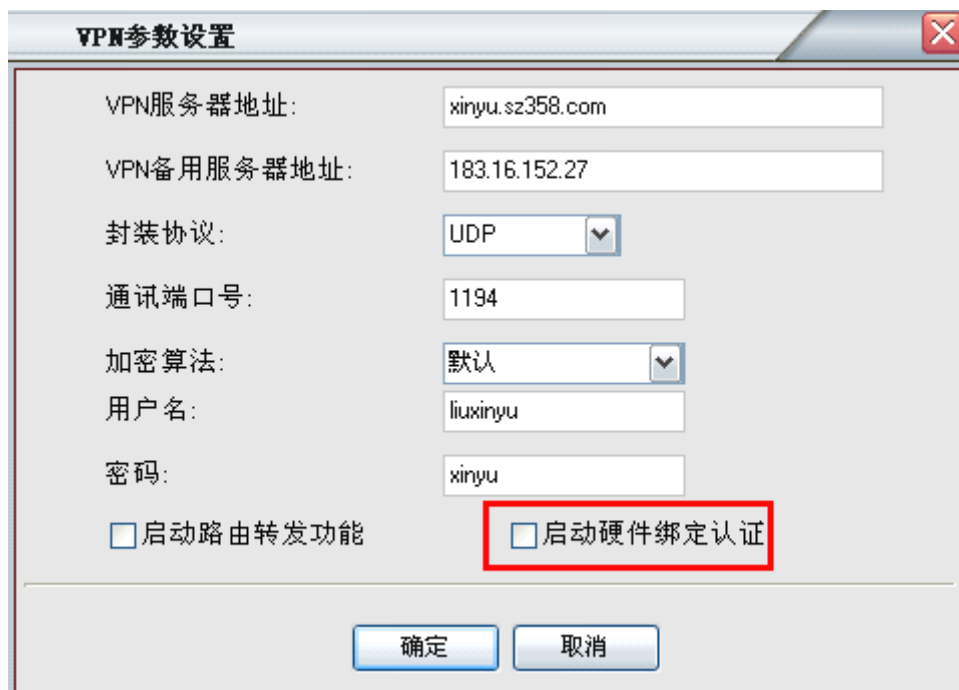
1、VPN 客户端支持哪些版本的 windows 系统。

答：启博 VPN 客户端软件可以工作于 windows 2000 以上的操作系统含 windows 2000,

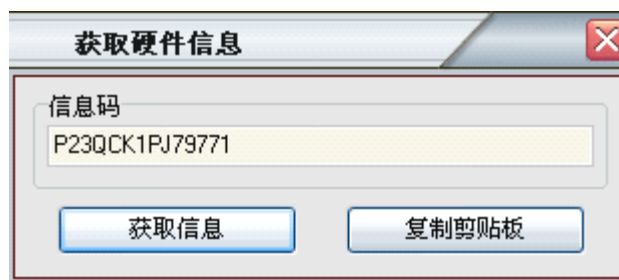
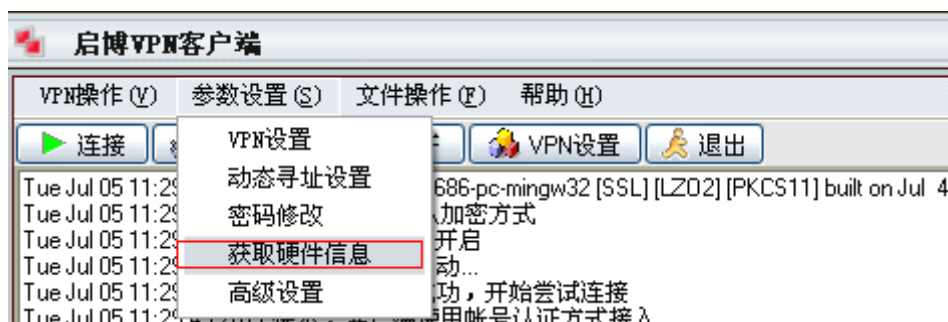
但需要注意的时 32 位的操作系统和 64 位的操作系统差别，安装文件是不同，请正确安装相应版本即可。

2、硬件绑定认证，只有指定计算机才能使用 VPN 客户端接入公司网络可以吗？

答：是可以的，启博 VPN 客户端可以绑定用户电脑上的硬件信息（CPU/硬盘/网卡等），来增强 VPN 接入的安全性。具体使用方法如下：



在 VPN 参数设置中，启动硬件绑定打上勾，并且在获取硬件信息并发送给总部



服务器端在该用户的密码后加上：- 和 客户端发过来的硬件信息即可，如下图，- 是普通中横杠。

用户管理

启用	认证类型	帐号	密码	IP地址	子网掩码	有效期	备注
启用	硬件认证用户	liuxinyu	123456- P23QCK1PJ79771	10.2.0.11	255.255.255.0	2030-07-05-10	✖

这样客户端以后接入时就会认证客户端的硬件信息。

注意点：一旦选用硬件认证，客户端一定要启硬件认证，如下图，否则无法接入

3、如何判断 VPN 是否连通？

答：如果是纯软件用户或 UKEY 用户，VPN 连接后会在桌面右下角会有提示信息，红色的图标也会变成绿色，表示已经成功连接，这时可以用过 PING 服务器端的 IP 地址来判断 VPN 是否联通。

硬件设备之间互联，可以直接利用设备里的测试工具中 PING 命令测试 ping 对方的 IP 地址是否通，同时也可以直接查看 VPN 配置---实在管理中的在线用户列表，来判断 VPN 是否联通，当然也可以查看 VPN 日志。

4、在处理南北通讯，即电信和网通互联方便，你们有没有什么好的方法？

答：MR 系列 VPN 特有的双服务器工作模式是 VPN 应用的一大创举，如果是客户端比较多，或者是客户端分布在不同的 ISP 运营商之间时，比如客户总部是电信的宽带，客户端有的是电信，有的是联通，有的是铁通等，普通 VPN 只能采用某一特定的端口和协议进行 VPN 连接，总会有些客户端无法正常连接进来，深圳迅博公司结合自身多年的 VPN 行业经验，大胆创新，使一台 VPN 设备同时工作两种 VPN 服务器模式，比如服务器 1 采用 4000 端口 UDP 协议，服务器 2 采用 4001 端口的 TCP 协议工作，对于所有客户端 VPN 服务器的公网 IP 是相同的，只需要修改一下本端的端口号或协议，就可以很顺利的接入到总部的 VPN 网络。

5、你们的 VPN 需要每次都拨号连接还是会自动连接呀？

答：MR 系列 VPN 内置心跳程序，每 60 秒会检测一下对端是否在线和对端的外网 IP 地址是否发生变化，如果对端在线 VPN 会自动和对方协商认证建立隧道；如果正常连接中，对端的外网 IP 发生变化，VPN 会根据心跳程序获取的新的 IP 地址与对端进行重新连接，所有的这一切全部实现免人工干预，自动化完成。

6、

7、