

赛天路由 系统用户使用手册

目录

第一章、 网络基础知识.....	5
1.1 局域网入门.....	5
1.2 IP 地址.....	5
1.3 子网掩码.....	5
第二章、 设备的安装与连接.....	6
2.1 面板布置.....	6
2.2 硬件的安装.....	6
2.3 配置您计算机网络设置.....	7
2.4 连接到路由器.....	10
第三章、 开始.....	12
3.1 网络设置.....	12
3.2 ARP 防御.....	12
3.3 端口映射.....	12
3.4 运行状态.....	12
第四章、 基本配置.....	13
4.1 网络设置.....	13
4.2 路由器名称.....	19
4.3 时间设置.....	19
4.4 DDNS 设置.....	20
4.5 域名特殊解析.....	20
4.6 WAN 扩展.....	21
4.7 WAN 对应列表.....	22
第五章、 高级配置.....	23
5.1 MAC 地址设置.....	23
5.2 镜像端口.....	23
5.3 端口状态.....	24
5.4 路由表设置.....	24
5.5 域名重定向.....	25
5.6 URL 重定向.....	26
5.7 URL 重定向日志.....	26
5.8 云平台设置.....	27
5.9 授权激活.....	27
第六章、 系统管理.....	28
6.1 访问设置.....	28
6.2 系统控制.....	29
6.3 Ping.....	29
6.4 登陆用户记录.....	30
6.5 系统日志.....	30
6.6 流量攻击日志.....	31
6.7 DDOS 日志.....	31
6.8 固件升级.....	32

第七章、 系统状态.....	33
7.1 运行状态.....	33
7.2 状态概述.....	33
7.3 流量分析.....	34
7.4 主机监控.....	35
7.5 PPPoE 客户列表.....	37
7.6 DHCP 客户列表.....	37
7.7 聊天软件列表.....	38
7.8 DNS 缓存列表.....	38
第八章、 用户管理.....	39
8.1 基本设置.....	39
8.2 radius 设置.....	41
8.3 PPPoE Server 管理.....	42
8.4 用户管理.....	42
8.5 PPPoE 日志.....	43
8.6 防御二级路由.....	44
8.7 通告文件编辑.....	44
8.8 通告规则管理.....	45
8.9 通告日志.....	46
第九章、 智能带宽管理.....	47
9.1 带宽设置.....	47
9.2 速度限制.....	47
9.3 带宽保证.....	49
9.4 流控类类型.....	50
9.5 应用程序设置.....	51
9.6 应用程序.....	51
9.7 分组管理.....	51
9.8 程序管理.....	52
第十章、 策略路由.....	55
10.1 负载均衡.....	55
10.2 电信网通地址.....	56
10.3 策略路由.....	57
10.4 线路状态.....	58
10.5 策略路由日志.....	58
10.6 端口映射.....	58
10.7 DMZ 设置.....	59
10.8 端口触发.....	60
10.9 UPnP 设置.....	60
第十一章、 VPN 管理.....	61
11.1 VPN 服务.....	61
11.2 VPN 用户.....	62
11.3 VPN 客户端.....	62
11.4 VPN 状态.....	63
11.5 OVPN 设置.....	64

11.6 OVPN 状态.....	66
11.7 OVPN 证书.....	67
11.8 OVPN 日志.....	67
第十二章、 防火墙.....	69
12.1 IP 地址组.....	69
12.2 应用限制.....	69
12.3 访问控制.....	70
12.4 访问控制日志.....	71
12.5 聊天软件黑白名单.....	71
12.6 域名过滤.....	72
12.7 网址数据库.....	72
12.8 网址防火墙.....	73
12.9 网址日志.....	74
第十三章、 安全配置.....	75
13.1 联线数设置.....	75
13.2 连接限制.....	75
13.3 DDOS 攻击防御.....	76
13.4 ARP 安全防御.....	77
13.5 ARP 绑定.....	78
13.6 ARP 列表.....	79
13.7 ARP 日志.....	80

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您关闭设备。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。

注：

路由器初始 IP：192.168.1.1

初始用户名：admin

初始密码：admin

第二章、设备的安装与连接

2.1 面板布置

接口及指示灯说明

POW 灯：电源指示灯，当路由器加电后该灯常亮

SYS 灯：系统正常运行时，SYS 灯常亮。熄灭时异常

LAN 灯：局域网接口指示灯，线路接通后此灯亮起，有数据传输时此灯会开始闪烁

WAN 灯：广域网接口指示灯，分别对应相应的 WAN 口，有数据传输时此灯会闪烁

LAN1：路由器内网网络接口

WAN1：路由器外网网络接口 1

WAN2：路由器外网网络接口 2

WAN3：路由器外网网络接口 3

WAN4：路由器外网网络接口 4

WAN5：路由器外网网络接口 5

POWER 接口：外置电源配置器接口

USB 接口：外部 USB 设备接口

2.2 硬件的安装

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℃；

工作湿度：10%到 90%不凝结；

存储湿度：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！

2.3 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 灯亮后，表示路由器已经进入工作状态，可以进行配置了。

2、首先需要将您的电脑与路由器的 LAN 口用网线连接起来，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 192.168.1.2-192.168.1.254 范围内（即与路由器内网地址在同一网段内，例如 192.168.1.2），子网掩码为 255.255.255.0，默认网关为 192.168.1.1，DNS 为 192.168.1.1 或者通过 DHCP 自动获取。

我们以 192.168.1.2 为例来介绍其设置方法：

鼠标右键点击桌面“网上邻居”图标，选择属性，打开‘网络连接’菜单，如图 1 所示，（或者点击“开始-设置-网络连接”也可以打开，如图 2 所示）。



（图 1）

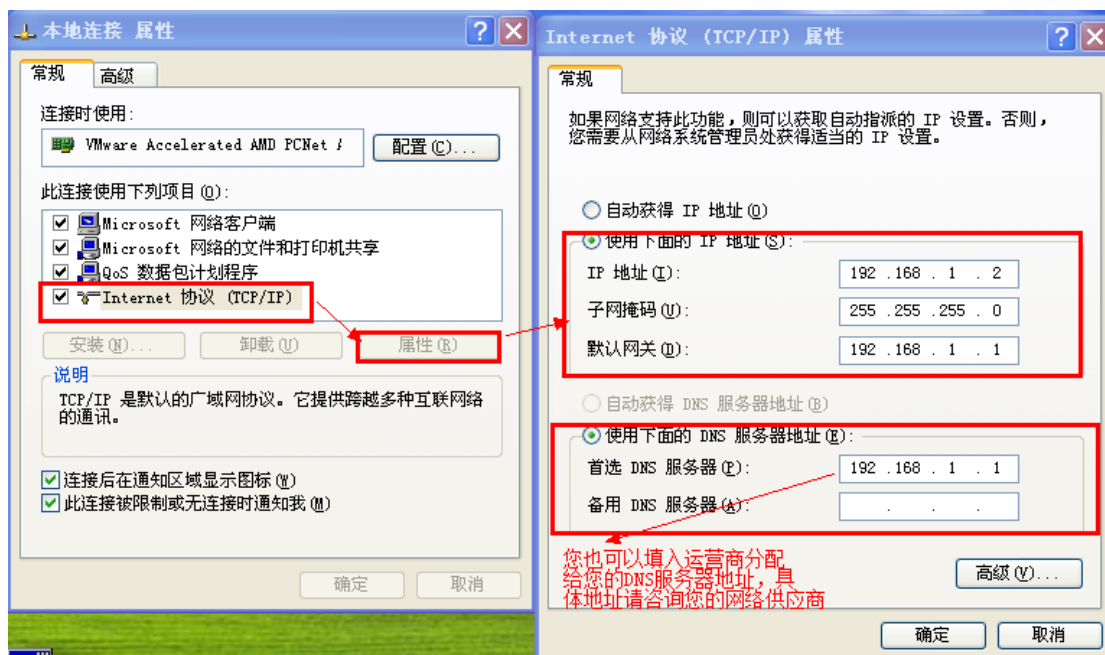
（图 2）

在打开的窗口中找到“本地连接”图标，鼠标右键点击此图标，并选择‘属性’选项，然后在接下来的窗口中选择“Internet 协议(TCP/IP)”并双击（如图 3 所示），进入 IP 地址修改窗口。



(图 3)

将本机 IP 地址修改为 192.168.1.2，子网掩码为 255.255.255.0，网关为 192.168.1.1，DNS 服务器地址填上网络供应商提供给你的 DNS 地址，若不清楚，可以直接填网关 IP，如图 4 所示：



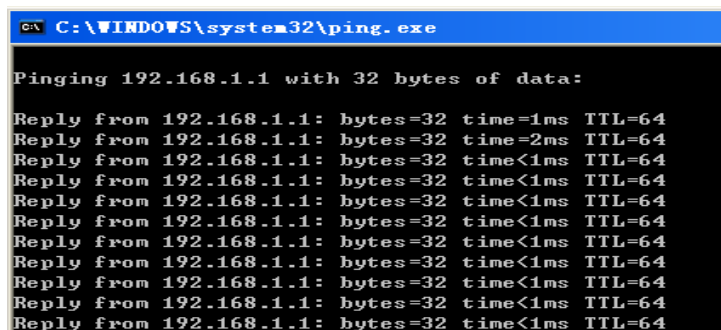
(图 4)

4、设置好本机 IP 之后，我们依次点击计算机的“开始菜单-运行”，在运行窗口中输入‘ping 192.168.1.1 -t’根据返回的结果来检查您的计算机和本产品是否正常连通。如图：

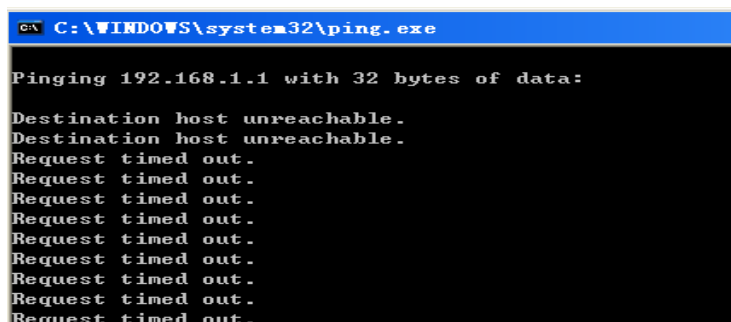


(图 5)

若显示图 6 所示的结果，表示网络连接正确，可以进行下一步操作；



(图 6)



(图 7)

若显示图 7 所示的结果，则表明网络连接有问题，或者设备未正确安装，您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或者已经配置好的交换机(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 192.168.1.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 192.168.1.1。

2.4 连接到路由器

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://192.168.1.1，如下图所示：



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



至此，您的电脑就与路由器连接成功，您可以对路由器进行其他设置了。

温馨提示：

为了安全起见，我们强烈建议您在登陆以后更改管理员密码，并牢记此密码。

第三章、开始

这个功能菜单下显示一下用户常用的功能选择，方便用户设置网络和查看路由器相关信息。

3.1 网络设置

路由的一些基本功能设置，包括 DHCP 配置、局域网设置、广域网设置、及多子网段设置。网络设置功能介绍详见[第四章基本配置中的网络设置](#)。

3.2 ARP 防御

ARP 防御相关参数的设置，ARP 防御设置功能介绍详见[第十三章安全配置中的 ARP 安全防御](#)。

3.3 端口映射

端口映射，使外网可以通过 IP 地址或域名访问到内网机器映射出去的端口。端口映射功能介绍详见[第十章策略路由中的端口映射](#)。

3.4 运行状态

运行状态功能介绍详见[第七章系统状态中的运行状态](#)。

第四章、基本配置

4.1 网络设置

DHCP 服务器

本选项主要提供 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。

DHCP服务器

管理方式

高级设置

开始地址

192.168.1.100

结束地址

192.168.1.200

释放时间

3600

秒

网关地址

192.168.1.1

子网掩码

255.255.255.0

首选 DNS 服务器

192.168.1.1

备份 DNS 服务器

0.0.0.0

管理方式：您可以选择普通、高级或者关闭。普通 DHCP 方式只能分配路由器 LAN 口网段的 IP，高级 DHCP 方式可以任意分配 IP 段、掩码及 DNS 服务器地址。

开始地址：DHCP 服务器自动分配的内部 IP 的起始地址。

结束地址：DHCP 服务器自动分配的内部 IP 的结束地址。

释放时间：设定 DHCP 服务器为客户端租用 IP 地址保留的过期时间，默认是 3600 秒。您可以自行设置。

网关地址：DHCP 服务器给客户机分配的默认网关地址。

子网掩码：DHCP 服务器自动分配给客户机的掩码地址。

首选/备用 DNS 服务器地址：DHCP 服务器自动分配给客户机的 DNS 服务器地址。

局域网设置

本选项主要用于局域网设置的相关参数，如下图所示：

局域网设置

路由IP地址

192.168.1.1

子网掩码

255.255.255.0

DNS 缓存服务器

☒ 启用

DNS的最大老化时间

300

秒(设置范围：60-600 默认是300)

即插即用上网

☐

多子网段

☐

路由 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 192.168.1.1，可以根据需要改变它，如果改变了路由器内网 IP 地址，需要重新连接路由器。

子网掩码：根据内网规模设置合适的掩码值。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。

即插即用上网：开启酒店模式之后，路由器下面的电脑设置任意 IP 地址都可以上网，可以设置跟 LAN 口不在同一个网段。（电脑的 IP、掩码、网关、DNS 允许设置任意地址，但必须都设置）开启酒店模式之后，将放弃本地连接的 IP 地址，而使用虚拟的 IP 地址。

多子网段：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以使用到该功能。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。此地址不要跟 LAN 口地址设置到同一个子网中，否则可能引起冲突。

多子网段的设置如图所示：

子网段列表

子网段列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

IP地址	子网掩码	操作
192.168.3.1	255.255.255.0	 

IP地址: 192.168.3.1

子网掩码: 255.255.255.0

添加

修改

重填

您所添加的 IP 地址相当于是 LAN 口虚拟的另一个网关地址，客户机可以使用您添加的多子网 IP 作为网关地址来上网。此地址不要跟 LAN 口设置到同一个子网，否则可能会引起冲突。

广域网设置

本页面主要用于配置 WAN 口相关参数，我们常用的广域网连接方式主要有 DHCP、static 静态接入跟 PPPoE 拨号接入 3 种。

1. 自动获取 IP



The screenshot shows the '广域网设置' (WAN Settings) page. On the left is a large blue placeholder box. On the right, the configuration for '广域网1' (WAN1) is shown. The '连接类型' (Connection Type) is set to 'DHCP'. The 'MTU设置' (MTU Setting) is set to '默认参数' (Default) with a value of 1500. The '静态DNS' (Static DNS) section has three input fields, all containing '0.0.0.0'. The '工作模式' (Working Mode) is set to '网关模式' (Gateway Mode). The '参与DNS缓存的值' (Value for DNS Cache Participation) is set to 0. The '防御信息检测' (Defense Information Detection) is set to '不启用' (Not Enabled). At the bottom are three buttons: '保存' (Save), '重填' (Reset), and '帮助' (Help).

连接类型：选择 DHCP（动态获取地址）。

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

静态 DNS：填入网络服务商提供给您 DNS 服务器 IP 地址，或者上级设备的网关地址。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

参与 DNS 缓存的值：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，动态获取 IP 时，我们一般不用开启。

2. 静态 IP 接入



广域网设置

选择您要设置的广域网 广域网1

连接类型 Static

IP地址 61.131.3.21

子网掩码 255.255.255.0

默认网关 61.131.3.1

MTU设置 默认参数 1500

静态DNS (放弃广域网获取的DNS) 61.139.2.69
0.0.0.0
0.0.0.0

工作模式 网关模式 (默认:网关模式。)
(网关模式: 接口做NAT地址转换,路由模式:接口路由转发)

参与DNS缓存的值 0 (数值越大,优先作为解析接口)

防御信息检测 不启用
(有效的屏蔽了内部主机的上网信息) 提示: 修改后请保存参数, 重启路由器, 防御功能才会完全生效

保存 重填 帮助

连接类型：选择 static 上网方式。

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

子网掩码：前 IP 所对应的子网掩码，由网络服务商提供。

默认网关：当前 IP 所对应的网关，由网络服务商提供

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

静态 DNS：填入网络服务商提供给您 DNS 服务器 IP 地址，由网络服务商提供，您可以向网络服务商询问获得。

工作模式：通常我们都使用网关模式，接口做 NAT 地址转换；有些特殊环境可能会用到路由模式（如内网机器全部使用公网 IP 的时候）。

参与 DNS 缓存的值：对于多 WAN 口接入时，此值的大小决定了 DNS 解析的出口。

防御信息检测：此功能用于防御运营商对线路的共享限制，静态地址接入时，我们不需要开启此功能。

3. ADSL 拨号上网 (PPPOE 拨号接入)

The screenshot shows a configuration window titled "广域网设置" (WAN Settings). On the left is a large blue sidebar. The main area contains the following settings:

- 选择您要设置的广域网: 广域网2 (dropdown)
- 连接类型: PPPoE (dropdown)
- 用户名称: adibiue (text input)
- 用户密码: 123456 (password input)
- 服务名称: (empty text input)
- 连接检查间隔: 30 (seconds) (text input)
- MTU设置: 默认参数 (dropdown) 1492 (text input)
- 静态DNS (放弃广域网获取的DNS): 0.0.0.0, 0.0.0.0, 0.0.0.0 (three text inputs)
- 工作模式: 网关模式 (dropdown) (默认: 网关模式。)
(网关模式: 接口做NAT地址转换, 路由模式: 接口路由转发)
- 参与DNS缓存的值: 2 (text input) (数值越大, 优先作为解析接口)
- 防御信息检测: 不启用 (dropdown)

At the bottom, there is a red warning message: "提示: 修改后请保存参数, 重启路由器, 防御功能才会完全生效" (Note: After modification, please save the parameters and restart the router for the defense function to take full effect). Below the warning are three buttons: "保存" (Save), "重填" (Reset), and "帮助" (Help).

连接类型: 选择 PPPOE 拨号接入。

用户名称: 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。

用户密码: 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。

服务名称: 一般不填, 某些特殊线路可能需要填入服务器名称才可以。

连接检查间隔: 用户自行设定重新拨接的时间。

MTU 设置: 即最大传输单元, PPPOE 拨号默认使用 1492 字节。通常情况下这个参数不用设置, 保持默认即可。不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

静态 DNS: PPPOE 拨号接入时可以不用填写 DNS 地址, 若您不想使用自动获取的 DNS 地址时, 可以填入网络服务商提供给您的其他 DNS 服务器地址。

工作模式: 通常我们都使用网关模式, 接口做 NAT 地址转换; 有些特殊环境可能会用到路由模式 (如内网机器全部使用公网 IP 的时候)。

参与 DNS 缓存的值: 对于多 WAN 口接入时, 此值的大小决定了 DNS 解析的出口。

防御信息检测: 此功能用于防御运营商对线路的共享限制, 动态获取 IP 时, 我们一般不用开启。

4. 透明桥接

透明桥接的使用较少, 一般在特殊环境如: 不改变现有网络环境, 加入一台路由设备到网络中作为管理, 这个时候就需要用到透明桥接模式。

广域网设置

选择您要设置的广域网

广域网2

连接类型

Transparent Bridge (透明桥接)

IP地址

192.168.12.5

子网掩码

255.255.255.0

默认网关

192.168.12.1

内部主机范围:

192.168.12.100-192.168.12.150 (必须在同一个网段)

MTU设置

默认参数 1500

静态DNS (放弃广域网获取的DNS)

0.0.0.0

0.0.0.0

0.0.0.0

工作模式

网关模式 (默认:网关模式。)

(网关模式:接口做NAT地址转换,路由模式:接口路由转发)

参与DNS缓存的值

2 (数值越大,优先作为解析接口)

不启用

防御信息检测

(有效的屏蔽了内部主机的上网信息) 提示:修改后请保存参数,重启路由器,防御功能才会完全生效

保存

重填

帮助

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

子网掩码: 前 IP 所对应的子网掩码, 由网络服务商提供。

默认网关: 当前 IP 所对应的网关, 由网络服务商提供。

内部主机范围: 需要使用到透明模式的内网机器 IP 范围段, 此 IP 段必须是跟广域网的 IP 在相同 IP 段才可以。

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

静态 DNS: 填入网络服务商提供给您 DNS 服务器 IP 地址, 由网络服务商提供, 您可以向网络服务商询问获得。

工作模式: 通常我们都使用网关模式, 接口做 NAT 地址转换; 有些特殊环境可能会用到路由模式 (如内网机器全部使用公网 IP 的时候)。

参与 DNS 缓存的值: 对于多 WAN 口接入时, 此值的大小决定了 DNS 解析的出口。

防御信息检测: 此功能用于防御运营商对线路的共享限制, 静态地址接入时, 我们不需要开启此功能。

5. 局域网

广域网设置

选择您要设置的广域网

广域网4

连接类型

局域网

IP地址

192.168.22.22

子网掩码

255.255.255.0

MTU设置

默认参数 1500

保存

重填

帮助

IP 地址：必须设置跟 LAN 口不冲突的 IP 段。此 IP 是作为镜像机器的网关来使用的，镜像机器需要单独接到该广域网口，中间不能接入其他交换机设备。

子网掩码：虚拟子网络的掩码地址。

MTU 设置：虚拟子网络的 MTU 值大小，一般保持默认即可。

此处的局域网设置是为了配合基于端口的端口镜像来使用的。如在不带交换芯片的硬件路由上开启了基于端口的镜像，那么就需要将镜像的 WAN 口设置为局域网模式，并填写一个与 LAN 口网段不冲突的虚拟子网。



端口镜像设置

状态 ☐ 启用端口镜像功能

选择镜像的数据方向 全部

镜像出口方式 镜像到端口

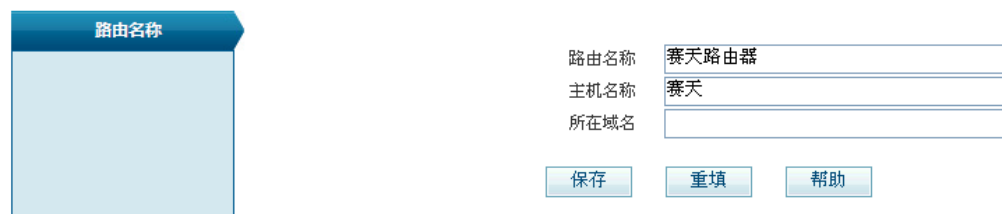
选择镜像端口 WAN1 (注意：必要将广域网接口设为landev (局域网类型)！ WAN1 (广域网1), WAN2 (广域网2))

保存 重填 帮助

如上图所示，开启了 WAN1 口作为镜像口，那么就需要将 WAN1 口设置为局域网模式，并填入一个跟 LAN 口不冲突的虚拟子网。需要镜像的机器单独接到 WAN1 口，并设置 WAN1 口的 IP 作为镜像机器的网关地址，保证镜像机器 IP 与 WAN1 口处于同一个网段，这样镜像机就可以正常镜像到需要的数据信息。

4.2 路由器名称

在这里您可以查看到路由器名称、主机名称以及所在域名信息。



路由名称

路由名称 赛天路由器

主机名称 赛天

所在域名

保存 重填 帮助

路由名称：默认为赛天路由器，您可以自行修改。

主机名称：默认为赛天，您可以自行修改。

所在域名：默认为空，您可以自行修改。

4.3 时间设置

可以手动或者自动设置路由系统时间。时间设置的正确与否直接影响着路由的功能。

时间设置

路由时间

2013-03-05 13:46:07

时区选择

UTC+08:00 中国, 香港, 澳大利亚西部, ▼

自动夏时制时间

☒

自动更新

每4小时 ▼

在需要时触发连接

☐

NTP时间服务器

默认设置 ▼

0.pool.ntp.org, 1.pool.ntp.org 2.pool.ntp.org

保存

重填

帮助

4.4 DDNS 设置

DDNS 动态域名解析服务主要用于将一个动态的 IP 解析成一个静态的域名，以便于网络来访问。

DDNS设置

选择动态域名工作的广域网

广域网1 ▼

IP地址

使用广域网的IP地址 (推荐) ▼

动态域名服务

3322 - 动态地址 ▼ http://www.3322.org/

用户名称

用户密码

需要更新的域名

邮件交换器MX

备份MX

☐

添加

修改

取消

帮助

选择动态域名工作的广域网：选择一个您要绑定域名更新的广域网接口。

动态域名服务：选择一个您要绑定 IP 的域名服务商，后面提供有服务商的官方网址。

用户名称/密码：填写您在域名服务商申请的账号名称及密码。

需要更新的域名：填写您需要绑定此 IP 的一个域名，该域名必须为未被其他 IP 使用过。

设置完毕之后点击“添加”，加入到列表中即可。若域名更新成功，在‘最近响应状态’会显示“Update successful” 的字样，即更新成功的意思。

4.5 域名特殊解析

域名特殊解析主要是用来将一些特定的域名绑定到指定的线路上去解析。如图所示：

特殊DNS解析列表

特殊DNS解析列表

共：条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

域名	出口接口	操作

DNS域名

出口选择 ☐ 广域网1 ☐ 广域网2 ☐ 广域网3 ☐ 广域网4 ☐ 广域网5 ☐ vpn1

添加

修改

取消

4.6 WAN 扩展

用于挂接 VLAN 交换机，对 WAN 口进行扩充，以满足多线路的同时接入。

WAN扩展

WAN扩展状态: ☒ 开启 ☐ 关闭 （设置后保存参数，重启生效！）

提交

规则编辑

描述

外网接口

(外网口名称，如果是广域网1填写1，广域网4填写4。注意:只能填写真实的广域网接口，扩展的接口无效)

扩展WAN数量

(需要扩展的数量，注意不要超过授权允许的最大WAN口数)

VLAN ID

(1-4095)

添加

修改

取消

帮助

WAN 扩展状态： 选择是否启用 WAN 口扩展功能。该功能在启用之后需要重启路由才生效。

描述： 对该规则的简单信息描述。

外网接口： 填入您用于扩展交换机的广域网接口。此接口是用来跟交换机对接，用于扩展 WAN 口使用的，该接口需要是实际的网卡接口（对已经扩展的广域网接口再次扩展将无效）。

扩展 WAN 数量： 允许扩展的最大 WAN 口数量。（此值只能小于或等于授权允许的最大 WAN 口数）

VLAN ID： 用于您在配置扩展交换机时，划分的 VLAN 起始编号（如果是从 VLAN1 开始扩展，那么这里就填 1；如果从 VLAN5 开始扩展，那么就填 5，依次类推）。VLAN ID 的取值范围为 1-4095，超过此范围的 VLAN ID 将不会被系统识别。

4.7 WAN 对应列表

显示 WAN 口对应的 VLAN 列表，用于查看所有已划分的 VLAN 接口对应关系。

WAN口对应列表		
共：60 条记录 当前 1/3 页 首页 上一页 下一页 末页 前往 第 页		
系统广域网	路由器WAN口	扩WAN交换机
广域网1	WAN1	VID1
广域网6	WAN1	VID2
广域网7	WAN1	VID3
广域网8	WAN1	VID4
广域网9	WAN1	VID5
广域网10	WAN1	VID6
广域网11	WAN1	VID7
广域网12	WAN1	VID8
广域网13	WAN1	VID9
广域网14	WAN1	VID10
广域网15	WAN1	VID11
广域网16	WAN1	VID12
广域网17	WAN1	VID13
广域网18	WAN1	VID14
广域网19	WAN1	VID15
广域网20	WAN1	VID16
广域网21	WAN1	VID17
广域网22	WAN1	VID18
广域网23	WAN1	VID19
广域网24	WAN1	VID20

第五章、高级配置

5.1 MAC 地址设置

对局域网以及广域网的 MAC 地址进行修改。

MAC地址设置

您的电脑MAC地址

00:07:4C:68:00:72

局域网的默认MAC地址

00:A0:C9:11:22:85

局域网地址

00:A0:C9:11:22:85

默认

随机

克隆PC

选择您要设置广域网

广域网1

广域网1的默认MAC地址

00:A0:C9:11:22:86

广域网1的MAC地址

00:26:50:A5:17:9E

默认

随机

克隆PC

保存

重填

帮助

- “克隆”表示将该接口的 MAC 地址设置为跟您电脑的 MAC 一样的地址。
- “默认”表示使用系统默认的 MAC 地址。
- “随机”表示随机分配一个 MAC 地址给该接口。

5.2 镜像端口

端口镜像功能主要用于监控端口数据流量，以方便管理人员对网络数据进行分析。

端口镜像设置

状态

☐ 启用端口镜像功能

选择镜像的数据方向

全部

镜像出口方式

镜像到主机IP

将数据包镜像到内部主机的IP

192.168.1.2

保存

重填

帮助

端口镜像设置

状态

☐ 启用端口镜像功能

选择镜像的数据方向

全部

镜像出口方式

镜像到端口

选择镜像端口

WAN1

(注意：必要将广域网接口设为landev
(局域网类型)! WAN1 (广域网1), WAN2 (广域网2))

保存

重填

帮助

- 状态：**选择是否启用端口镜像功能。
- 选择镜像的数据方向：**选择监控的数据包走向，出去的数据或者进来的数据，或是所有的数据。
- 镜像出口方式：**选择是镜像到主机 IP 或者镜像到端口。

将数据包镜像到内部主机的 IP: 设置一个您需要用来作为监控的主机 IP 地址，选择“镜像到主机 IP”时有效。

选择镜像的端口: 选择镜像的端口，选择“镜像到端口”时有效。

5.3 端口状态

主要用于显示路由各个接口的工作状态

当前端口状态

当前端口状态列表

共：6 条记录 当前 1/2 页 首页 上一页 下一页 末页 前往 第 页

接口	线路状态
LAN	联线 negotiated 1000baseT-FD flow-control,
WAN1	断线
WAN2	断线
WAN3	断线
WAN4	联线 negotiated 100baseTx-FD flow-control,

刷新

5.4 路由表设置

所谓路由表，指的是路由器或者其他互联网网络设备上存储的表，该表中存有到达特定网络终端的路径，在某些情况下，还有一些与这些路径相关的度量。路由器的主要工作就是为经过路由器的每个数据报寻找一条最佳传输路径，并将该数据有效地传送到目的站点。

当前路由表
当前路由表是路由器当前自动生成的静态路由表。

当前路由表

当前路由表

共：3 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

目的地址	网关	子网掩码	Metric	网络接口
10.0.0.0	*	255.255.255.0	0	pppsrv
192.168.2.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo

静态路由表
在一些特殊环境中，我们也需要手动去指定静态路由表的走向，此时，我们需要手动去添加静态路由表，如图所示：

静态路由表

静态路由表

共：0 条记录 当前 1 页 首页 上一页 下一页 末页 前往第 页

目的地址	网关	子网掩码	Metric	网络接口	描述信息	操作

描述：

目的地址：

子网掩码：

网关：

Metric：

网络接口：

12

172.15.2.0

255.255.255.0

192.18.1.244

0 (默认：0)

LAN (默认：LAN (代表局域网), WAN1 (广域网1), WAN2 (广域网2), vpn1 (vpn接口1), vpn2 (vpn接口2), , , 或者，您要设置的接口名称)

添加

修改

取消

帮助

举例：如赛天路由下层挂接有一台三层交换机，交换机的 IP 为 192.18.1.244，该三层交换机下发的有一个 172.15.2.1/24 的网段，三层交换机下的主机使用 172.15.2.X 网段的 IP 上网，并使用 172.15.2.1 作为网关地址，那么，我们就需要添加如上图所示的静态路由，才可以使三层交换机下的主机正常上网。

5.5 域名重定向

DNS域名重定向

列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

DNS 域名	重定向到	操作
www.baidu.com	192.168.1.1	

DNS 域名

重定向到

www.baidu.com

192.168.1.1

添加

帮助

DNS 域名：填入被转向的域名。支持通配符 * （例如：*.qq.com 即表示所有带 qq.com 的网站，例如 news.qq.com，qzone.qq.com，mail.qq.com 等等）。

重定向到：填入您需要转向到的一个域名或者 IP。（此域名必须是服务器解析之后只有单一地址的。例如 www.baidu.com 解析出来就有多个 IP，这样的就不行。）

5.6 URL 重定向

URL 重定向是对域名重定向功能的补充跟完善，一些用域名重定向无法转向的域名，通过 URL 重定向就可以实现。

URL重定向规则列表

列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	描述	URL主机名称	目录网页	网页参数	重定向到	主机范围	日志	基于时间控制	操作
启用	百度跳转到淘宝	www.baidu.com	全部	全部	www.taobao.com	192.168.2.100-192.168.2.150	是	OFF	 

URL重定向规则编辑

状态

☒ 激活 ☒ 日志

描述

百度跳转到淘宝

URL的主机名称

www.baidu.com

相同

目录网页 (URL)

not

全部

网页的参数

not

全部

重定向到

www.taobao.com

☐ 将被重定向的URL在末尾

主机IP地址范围

192.168.2.100-192.168.2.150

(为空：表示对该规定所有内部IP有效)

基于时间控制

☐ 启用

添加

修改

重填

帮助

- 状态：选择是否激活应用此规则。
- 日志：是否需要在日志中显示记录。
- 描述：对该条规则的简单描述。
- URL 的主机名称：填入您需要被转向的域名地址。
- 目录网页（URL）：填入被转向域名的目录网页，若没有，则可不填
- 网页的参数：填入被转向域名的网页参数，若没有，则可以不填
- 重定向到：需要被转向到的域名地址。
- 主机 IP 地址范围：内部需要被重定向的主机 IP 地址。
- 基于时间控制：启用则规则只在设定的时间段内生效。

5.7 URL 重定向日志

该功能是用来记录 URL 重定向中勾选日志的规则匹配记录。

URL重定向日志		
共：3 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页		
编号	时间	事件
0	03-04 11:16:37	规则 百度跳转到淘宝 :将192.168.2.100访问 http://www.baidu.com/ 重定向到 www.taobao.com
1	03-04 11:16:40	规则 百度跳转到淘宝 :将192.168.2.100访问 http://www.baidu.com/ 重定向到 www.taobao.com
2	03-04 11:16:41	规则 百度跳转到淘宝 :将192.168.2.100访问 http://www.baidu.com/ 重定向到 www.taobao.com

5.8 云平台设置

云平台功能用户使路由设备与云平台管理系统对接,使用云平台上的功能对路由器功能进行扩充。目前已支持云计费的管理。

云平台设置

设备ID

1915821

*

设备密码

●●●●●●

*

路由器名字

赛天

启用

☒

云计费

保存

刷新

帮助

当前状态信息

登陆成功,发送心跳包间隔时间为60秒

设备 ID: 登录云平台,在“我的设备->设备列表->设备 ID”可以查询到设备的ID。

设备密码: 登录云平台,在“我的设备->设备列表->设备名称”可以修改、设置设备密码。

路由器名字: 当您输入设备 ID 与设备密码,并成功连接到云平台服务器之后,会显示您在云平台添加的路由器名称)。

启用: 根据您的需要,选择是否需要激活相应功能模块。

当前状态信息: 显示该路由器与云平台的连接信息。

5.9 授权激活

使用此路由器需要授权,授权文件导入到路由中就可以使用该路由器。

授权激活

安装的授权文件: ~~zpl301311150001.myy~~

最大允许的广域网数:64

授权文件的服务有效期 >> 2063-12-15 20:37

在服务有效期内享受:固件升级服务、在线技术支持。

点击删除授权文件

第六章、系统管理

6.1 访问设置

Web 访问设置

主要就是让外网用户通过 Web 页面形式来进行远程访问路由器设备。可以通过设置对应的密码来进行安全保证。 这样设置主要就是为了方便一些管理员在其他网络中也可以及时查看设备和解决问题。

web 访问设置

HTTP 访问端口

80

认证通告端口

0

(不填写或者为0,表示和管理端口相同)

远程访问

☐

远程访问端口

8080

管理员

admin

管理员密码

管理员密码确认

启用 guest 用户

☐

guest 用户

guest

guest 用户密码

guest 用户密码确认

保存

重填

其他设置

允许 ping WAN 口

☐

允许接入的 IP 地址

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

保存

重填

帮助

- HTTP 访问端口：**本地局域网访问路由器时的端口。默认为 80。
- 认证通告端口：**认证页面、通告页面等页面的弹出时使用的端口，如果为 0，表示和管理端口相同。
- 远程访问：**勾上表示激活远程访问。激活之后，在广域网也能访问到您的路由器 WEB 控制界面，方便管理员进行远程维护。默认为不启用。
- 远程访问端口：**广域网远程访问路由 WEB 控制界面时的端口。默认为 8080。
- 管理员/密码：**自定义您的管理员账户与密码。管理员具有对路由器的最高管理权限。
- 启用 guest 用户：**是否启用 guest 用户。Guest 用户只能查看路由设置，不能对路由设置做任何更改。默认不启用。
- guest 用户/密码：**自定义您的 guest 用户名及密码。

管理员用户可以修改路由器任何设置，guest 用户只能查看设置，不能修改设置。忘记管理员用户/密码之后只能通过按下 reset 按钮来恢复到出厂默认值，请牢记您的管理员用户名及密码。默认管理员用户名是 **admin** 密码是 **admin**；guest 用户名与密码都是 **guest**。

其它设置

可以设置是否允许 PING WAN 口，默认不允许。另外也可以设置允许访问路由器的 IP 地址。

6.2 系统控制

用于将路由参数导入导出，恢复默认参数以及对路由执行重启操作。

保存参数：保存您的路由器配置参数数据。以备路由器调试后出现问题时能及时恢复到以前的状态。

恢复系统参数：将您预先保存的系统配置文件导入到路由器（配置文件为 .cfg 格式的）。请不要将其他路由器的配置文件导入到本路由器，否则将导致路由器不能工作。

恢复默认设置：选择“恢复默认设置”，并点击确定。恢复之后路由器会自动重启，重启完之后请使用默认 IP 及用户名/密码登录路由。路由器默认 IP：**192.168.1.1**，默认用户名为 **admin** 密码为 **admin**。

重启路由器：点击“重启路由器”按钮，在弹出的对话框中选择“是”，路由将会重新启动一次。

6.3 Ping

此功能主要用于方便管理者了解网络对外联机的实际状况，可以藉由此功能了解网络上的计算机是否存在。

Ping

输入地址

www.baidu.com

网络接口

WAN1

(为空表示默认路由出口, LAN (代表局域网), WAN1 (广域网1), WAN2 (广域网2), vpn1 (vpn接口1), vpn2 (vpn接口2)... 或者, 您要设置的接口名称)

Ping包计数

5 (1 - 10)

Ping包大小

56 (字节)

开始检测

停止检测

检测信息

正在检测中...

PING www.baidu.com (115.239.210.27): 56 data bytes
64 bytes from 115.239.210.27: icmp_seq=0 ttl=57 time=418.1 ms
64 bytes from 115.239.210.27: icmp_seq=1 ttl=57 time=390.5 ms
64 bytes from 115.239.210.27: icmp_seq=2 ttl=57 time=389.7 ms
64 bytes from 115.239.210.27: icmp_seq=3 ttl=57 time=525.7 ms

- 输入地址：

填写您需要检测的 IP 或者域名。

网络接口：

指定您需要检测的网络接口，如果留空，表示从默认的路由出口进行检测。

Ping 包计数：

ping 数据包的检测个数。

Ping 包大小：

每个 ping 数据包的大小限制。

6.4 登陆用户记录

此列表将显示所有登陆路由器的历史用户。

登陆路由器的用户记录

列表

共：9 条记录 当前 1/1 页

首页

上一页

下一页

末页

前往第

页

登陆IP	登陆时间	登陆用户
192.168.2.100	2013-03-04 11:58:36	管理员
192.168.2.100	2013-03-04 10:58:33	管理员
192.168.1.101	2013-03-04 10:55:35	管理员
192.168.1.101	2013-03-04 09:44:29	管理员
192.168.1.16	2013-03-02 15:20:14	管理员
192.168.1.100	2013-03-02 15:02:21	管理员
192.168.1.101	2013-03-02 15:47:11	管理员
192.168.1.101	2013-03-02 16:47:13	管理员
192.168.1.101	2013-03-02 17:47:18	管理员

6.5 系统日志

系统日志主要记录路由器日常工作信息和情况。

系统日志		
共：599 条记录 当前 1/24 页 首页 上一页 下一页 末页 前往第 页		
模块	时间	消息
udhcpd	Mar 4 03:15:04	Sending discover...
udhcpd	Mar 4 03:15:27	Sending discover...
udhcpd	Mar 4 03:15:30	Sending discover...
udhcpd	Mar 4 03:15:33	Sending discover...
kernel	Mar 4 03:15:35	EXT2-fs warning: maximal mount count reached, running e2fsck is recommended
udhcpd	Mar 4 03:15:56	Sending discover...
udhcpd	Mar 4 03:15:59	Sending discover...
udhcpd	Mar 4 03:16:02	Sending discover...
udhcpd	Mar 4 03:16:25	Sending discover...
udhcpd	Mar 4 03:16:28	Sending discover...
udhcpd	Mar 4 03:16:31	Sending discover...
udhcpd	Mar 4 03:16:54	Sending discover...
udhcpd	Mar 4 03:16:57	Sending discover...
udhcpd	Mar 4 03:17:00	Sending discover...
udhcpd	Mar 4 03:17:23	Sending discover...

6.6 流量攻击日志

记录整个网络的非正常流量情况。当网络出现异常攻击等情况时都会记录在日志里面。

流量攻击日志		
共： 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页		
编号	时间	事件

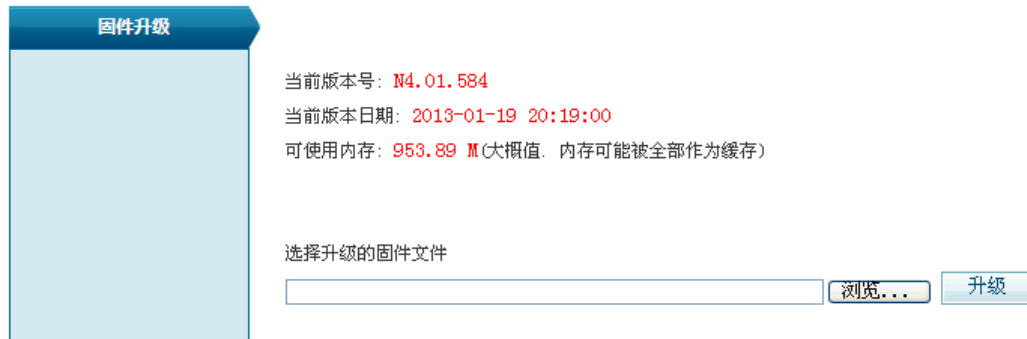
6.7 DDOS 日志

DDOS 日志用于记录 DDOS 攻击的相关日志。

DDOS 日志		
共： 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页		
编号	时间	事件

6.8 固件升级

该界面可以对路由器进行固件升级操作及软恢复操作。如图所示：



固件升级：升级前请先确认好路由器的当前版本，看是否需要进行升级操作。点击‘浏览’按钮，选择新版本的存放路径之后，按下‘升级’按钮开始升级操作。升级时间一般会在二分钟左右完成。

温馨提示：

升级路由器的时候，请不要刷新页面，并且保证机器在不断电的情况完成升级操作，否则将造成路由器升级失败！请尽量选择本地升级路由器，远程升级路由器受到网络影响容易导致升级失败！

第七章、系统状态

7.1 运行状态

查看此界面，可以了解路由器目前工作状况，作为判断网络故障和使用率的依据之一。运行状态下，有图表实时显示目前系统 CPU 占用资源率。



7.2 状态概述

此界面用于显示路由器硬件信息，广域网信息以及局域网信息。

硬件信息：显示当前路由器系统采用的 CPU 信息，以及 CPU 运行能力。

硬件信息

路由名称	赛天路由器
路由型号	ST_8000
CPU 信息	
型号	Intel(R) Atom(TM) CPU D525 @ 1.80GHz
CPU2 信息	
型号	Intel(R) Atom(TM) CPU D525 @ 1.80GHz
CPU3 信息	
型号	Intel(R) Atom(TM) CPU D525 @ 1.80GHz
CPU4 信息	
型号	Intel(R) Atom(TM) CPU D525 @ 1.80GHz

刷新

广域网信息：显示广域网连接状态。 连接状态：Connected 表示连接成功，Connecting...表示正在连接。 连接时间：表示该广域网口与服务器建立连接的时间，以此时间可以判断 WAN 口是否掉线过。

广域网信息

选择您要查看的广域网

广域网5

广域网5信息

MAC 地址	00:AA:6E:AB:E2:97
连接类型	dhcp
IP 地址	192.168.10.124
子网掩码	255.255.255.0
网关	192.168.10.1
DNS	192.168.10.1
MTU	1500
连接状态	Connected
连接时间	0 days, 04:41:57

从新获取IP地址

释放IP地址

刷新

局域网：显示当前局域网的 IP 地址，以及 MAC 地址、子网掩码信息

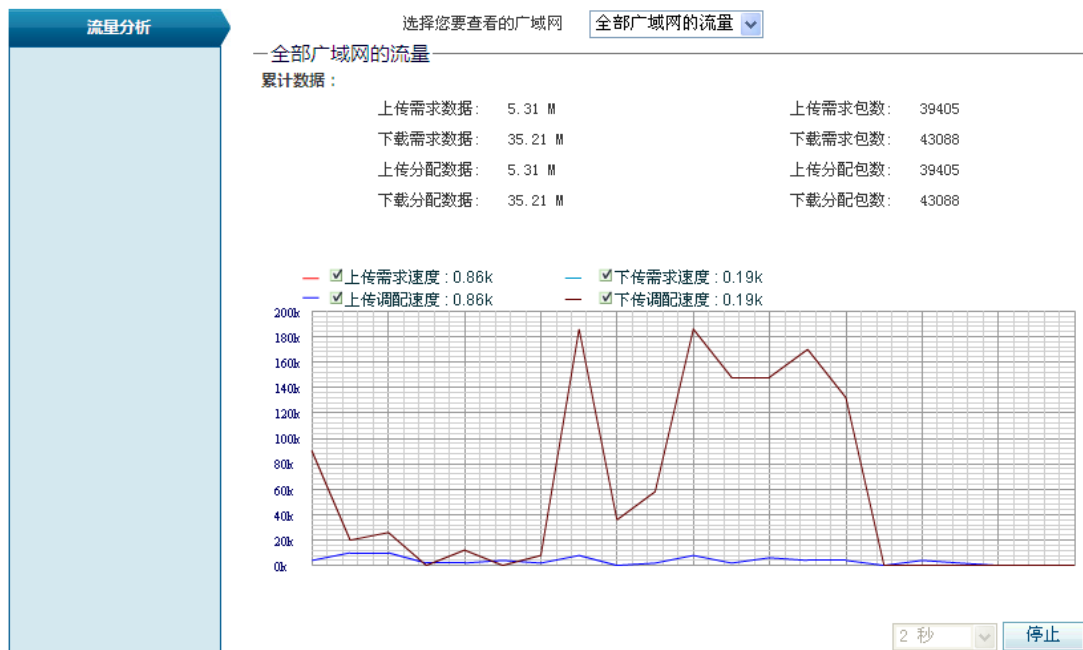
局域网信息

MAC 地址	00:A0:C9:11:22:85
IP 地址	192.168.2.1
子网掩码	255.255.255.0

刷新

7.3 流量分析

显示当前广域网上传和下载流量。



如上图，显示当前广域网的上传和下载流量分析图。

选择查看的广域网：默认显示所有广域网总和的流量，如果需要查看单个广域网流量，请选择相应的广域网口；

上传/下载需求速度：为当前网络中，客户机对外发送请求所需要的流量；

上传/下载调配速度：路由器通过 QoS 规则智能均衡计算之后，分配的速度值。

7.4 主机监控

“主机监控”能显示内网所有用户的网络连接情况。位于“列表”上方的记录数，可以显示当前内网的在线机器数量。

在列表中，可以很直观的看出每台 PC 占用的网络情况，鼠标点击“查看连接”，还能显示该 PC 的网络访问情况，有进程管理的也可以点击查看正在使用的进程。如下图所示：

主机详细信息

上网时间	3时33分32秒
当前连接数	6
连接创建的总数	2980
连接数限制	all:2000 ; TCP:0;UDP:0
DDoS 防御	all:300 ; TCP:0;UDP:0
上传数据总量	4.21 M 数据包:28000个
下载数据总量	21.17 M 数据包:31090个
当前上传需求流量	0 b 数据包:0个
当前上传分配流量	0 b 数据包:0个
当前下传需求流量	0 b 数据包:0个
当前下传分配流量	0 b 数据包:0个

刷新

详细信息页面可以查看当前主机 IP 的规则限制，联机数使用情况及带宽使用情况等。

7.5 PPPoE 客户列表

该记录是显示通过 PPPOE 拨号到路由器的用户信息。

PPPoE客户列表

当前 PPPoE 在线用户

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

session id	用户名	登录时间	IP地址	MAC地址	操作
291	123	10秒	10.0.0.2	00:07:4c:68:00:72	

刷新

7.6 DHCP 客户列表

此列表将显示所有 DHCP 自动获取 IP 的用户信息。

DHCP 客户列表		DHCP 用户列表	
		共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页	
主机名	IP地址	MAC 地址	使用时间
pc	192.168.2.100	00:07:4c:68:00:72	7分22秒

7.7 聊天软件列表

列表显示路由器下的用户聊天软件信息，包括有 QQ、MSN、飞信、淘宝旺旺等。

聊天软件列表		聊天软件列表	
		共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页	
IP地址	类型	帐号	
10.0.0.2	QQ	(点击Q他)	

7.8 DNS 缓存列表

DNS 缓存列表会记录下所有用户 DNS 最大老化时间内缓存的域名解析信息，超过时间的缓存信息将会自动老化掉。对某域名做过规则或该域名正被连续使用，将会加长老化时间。

DNS 缓存列表		DNS 缓存列表	
		共：77 条记录 当前 2/4 页 首页 上一页 下一页 末页 前往第 页	
域名	IP地址	更新时间	老化时间
fun.youku.com	220.181.185.144	10秒	30秒
game.youku.com	220.181.185.144	10秒	30秒
hz.youku.com	211.151.72.29,211.151.72.30	10秒	30秒
i.youku.com	211.151.146.208	10秒	30秒
index.youku.com	220.181.52.112,220.181.52.111	10秒	30秒
jilupian.youku.com	220.181.185.144	10秒	30秒
life.youku.com	220.181.185.144	10秒	30秒
mobile.youku.com	220.181.185.144	10秒	30秒
movie.youku.com	220.181.185.144	10秒	30秒
music.youku.com	220.181.185.144	10秒	30秒
news.youku.com	220.181.185.144	10秒	30秒
paike.youku.com	220.181.185.144	10秒	30秒
sports.youku.com	220.181.185.144	10秒	30秒
tech.youku.com	220.181.185.144	10秒	30秒
travel.youku.com	220.181.185.144	10秒	30秒
tv.youku.com	220.181.185.144	10秒	30秒
www.soku.com	220.181.185.143	10秒	30秒
zy.youku.com	220.181.185.144	10秒	30秒
c.youku.com	220.181.185.144	10秒	30秒
u.youku.com	211.151.50.28	10秒	30秒

刷新

第八章、用户管理

对 WEB 用户、PPPOE 用户进行管理，并设置用户上网的认证方式，以及对上网通告的管理

8.1 基本设置

用户上网控制主要用于对用户上网的方式做控制，允许 3 种上网认证方式，如图所示：

用户上网控制

用户上网方式控制

需要认证

允许上网的方式

☐ ARP绑定用户直接上网

☒ PPPOE用户直接上网

☐ 允许web认证上网

关闭WEB认证页面时

☐ 退出认证

用户帐号到期提前通知

7天

你的帐号快到期了,请缴费!

用户帐号到期提前通知的消息

用户帐号到期查询间隔

0分

（0表示不查询,最短时间间隔为5分钟）

不需要认证的内部主机(基于IP)

(可以为空)

允许访问的外网范围(基于IP)

(可以为空)

允许访问的外网范围(基于域名)

(可以为空)

在“用户上网方式控制”中，默认是关闭的，即路由器下的所有用户不需要经过任何认证，直接填写正确的 IP 就可以直接上网，跟普通路由器共享上网原理一样。若选择“开启”即可激活下面的菜单，出现上图的相关的认证方式选项界面。

- 允许上网的方式：** 选择允许用户上网的认证方式。
 - ARP 绑定用户直接上网：IP 与 MAC 地址进行绑定过的用户可以直接上网；
 - PPPoE 用户直接上网：利用 PPPOE 协议拨号到路由器端的用户验证通过之后才可以上网；
 - 允许 WEB 认证上网：通过网页认证信息登陆过的用户才可以上网。

关闭 WEB 认证页面时：勾选上，表示在关闭 IE 认证的页面就退出 WEB 认证；若不勾选，即表示，只有在网络被重置或者电脑重启的情况下认证才退出。此功能仅对 WEB 认证有效，不使用 WEB 认证时，此选项无效。

用户账号到期提前通知：账号到期之前提醒用户的通知时间。默认为提醒时间内每天第一次开启网页时出现，直到账号到期（或者延长期限）为止。

用户帐号到期查询间隔：此功能用于检测帐号到期但仍持续在线的用户，在帐号到期以后，达到设置的时间之后，在线用户将被强制踢下线，避免了因为到期用户长期不下线导致的带宽资源浪费。此值可以尽量设置大一点，效果更佳。

用户账号到期提前通知的消息: 用户到期的提前通告内容, 由用户自行定义, 不支持加入 html 网页代码。此通知消息是对快到期的 Web 认证用户才有效的; pppoe 用户的提前通知消息是在“认证页面管理”里面进行修改的。如图所示:

你的上网信息		密码修改	联系管理员
登录时间:	0秒		
到期时间:	2013-03-04 15:40		
当前上传流量:	1.08 K		
当前下载流量:	461 b		
上传总流量:	1.53 K		
下载总流量:	551 b		
消息提示:	你的帐号快到期了, 请缴费!		

不需要认证的内部主机(基于 IP): 所添加的 IP 用户将不受任何一种认证方式的管制, 可以直接上网, 即认证排除的内网 IP。

允许访问的外网范围(基于 IP): 没有进行认证的用户也能访问的外网 IP 地址范围。

允许访问的外网范围(基于域名): 没有进行认证的用户也能访问的外网域名。

管理员联系信息: 可以自定义管理员的联系信息, 以方便用户在网络出现问题时方便联系管理员。此信息在 Web 用户登陆后可以查看到, PPPoE 用户在拨号以后需要登陆 IE 才能看到。

管理员联系信息	
电话:	24324353454354
QQ:	3435435233
msn:	
email:	
其他联系方式:	
保存 重填 帮助	

如图所示是 web 认证后, 查看到的管理员联系信息。

你的上网信息		密码修改	联系管理员
电话:	24324353454354		
QQ:	3435435233 (点击Q他)		
MSN:			
email:			
其他:			

认证页面及通告内容用于对认证用户到期发出提醒通告。

Web认证页面	查看当前“Web认证页面” 使用默认“Web认证页面” 重新提交通告文件“Web认证页面”： 浏览... 提交
帐户到期提前通知页面	查看当前“帐户到期提前通知页面” 使用默认“帐户到期提前通知页面” 重新提交通告文件“帐户到期提前通知页面”： 浏览... 提交
阻止上网的通告页面	查看当前“阻止上网的通告页面” 使用默认“阻止上网的通告页面” 重新提交通告文件“阻止上网的通告页面”： 浏览... 提交

WEB 认证页面：使用 WEB 认证上网时，弹出的用户登录认证的界面。您可以根据需要自行修改登录页面文件，但文件大小不要超过 8K。否则无法导入进去、

帐户到期通知：认证用户帐号到期之前的通知提醒页面，用户帐号快到期时，打开网页的时候会自动弹出此通告内容。

阻止上网通告：在开启了 arp 认证或者 pppoe 认证、没有开启 web 认证时，没有认证的用户将会收到此通告文件的提醒；开启了 web 认证则弹出 web 认证页面。

8.2 radius 设置

radius 设置	Radius Server 启用 authserver 192.168.1.230:1812 (192.168.10.230:1812) acctserver 192.168.1.230:1813 (192.168.10.230:1812) 通信密钥 123456 (123456) 本地IP地址 192.168.1.1
管理设置	超级管理员 hadmin 超级管理员密码 ••••• 超级管理员密码确认 ••••• 保存 重填 帮助

Radius Server：启用或关闭 Radius

功能 authserver：Radius 认证服务器的 IP 跟认证端口。

acctserver：Radius 用户数据服务器的 IP 跟对接端口。

通信密钥：与 Radius 相互通信对接所使用的验证密钥。

本地 IP 地址：路由器与 Radius 服务器通信的 IP 地址，若服务器在外网，则使用路由器 WAN 口 IP；若服务器在内网，则使用 LAN 口 IP。

管理设置：设置 radius 服务器超级管理员的用户名和密码。

8.3 PPPoE Server 管理

提供对 PPPOE 拨号服务端的一些参数设置。

PPPoE Server设置

PPPoE Server状态

☒ 启用 PPPoE Server

只允许使用PPPoE接入

☐ 设置后，只有PPPoE拨号后才能访问路由器，用于防止攻击，真正交换层过滤！

PPPoE 服务器名字

saitian

(英文字符)

☒ 允许任意服务器名接入

PPPoE 服务器的地址

10.0.0.1

PPPoE 服务器的子网掩码

255.255.255.0

首选 DNS 服务器

0.0.0.0

(如果未设置，将是默认的服务器地址)

备份 DNS 服务器

0.0.0.0

(如果未设置，将是默认的服务器地址)

空闲检测时间

3

秒 (默认为6, 范围是 3-180)

多少个检测请求未应答则断开连接

3

个 (默认为10, 范围是 3-100)

认证方式

☒ 不用加密的密码 (PAP)

☐ 质询握手身份验证协议 (CHAP)

☐ MS-CHAP

☐ MS-CHAP v2

保存

重填

帮助

PPPoE Server 状态: 是否启用 PPPoE 拨号服务端功能。默认为启用状态，若您关闭了此功能，客户机将无法通过 PPPoE 拨号到路由器。

只允许使用 PPPoE 接入: 激活之后将只有通过 PPPoE 拨号的用户才能访问到路由器跟上网。（且只能使用下方的‘PPPoE 服务器地址’才能访问路由器 WEB 界面，若使用 LAN 口 IP 将无法访问到路由器 WEB 界面）

PPPoE 服务器名字: 拨号服务器的名称，用户可以自定义更改。

PPPoE 服务器的地址: 即 PPPoE 拨号用户的网关地址。（PPPoE 用户可以通过此地址来访问路由器配置页面）

PPPoE 服务器的子网掩码: 即 PPPoE 服务器的掩码地址，您可以根据环境需求来修改此地址。

首选 DNS 服务器: PPPOE 服务器分配给客户机的 DNS 服务器地址。

备份 DNS 服务器: PPPOE 服务器分配给客户机的 DNS 服务器地址。

空闲检测时间: 在达到设定的时间之后，若客户机与服务器之间还没有数据通信，则开始检测客户端是否掉线。默认值为 3 秒。

多少个检测请求未应答则断开连接: 在设定的请求个数之后，客户机若无数据通信应答，则断开其连接。默认值为 3 个。

认证方式: 对于不同应用环境，可以采取不同的认证方式类型。对于一般 PC 电脑，都是采用的 PAP 模式。如果是采用下级路由进行拨号，可以把所有的认证方式都勾选上。

8.4 用户管理

针对 PPPoE 用户及 Web 认证上网的用户进行添加、修改或删除的操作，如用户账号的建立、认证方式、到期时间、MAC 地址的绑定、备注信息等设置。

用户列表

共：2 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	登录名	IP地址	到期时间	备注	上网状态	允许登录数	操作
	123	0.0.0.0-0.0.0.0			离开:58分39秒	1	
	456	0.0.0.0-0.0.0.0	2013-03-04 16:40		登录:11分53秒	1	

用户管理

用户状态

☐ 禁用

登录方式

PPPoE 拨号

用户名

密码

MAC地址

不绑定

到期时间

...

IP地址

-

允许登录的用户数

备注

用户状态：选择禁用即表示禁用此用户，禁用后此用户将不能进行拨号上网（用户当前连接断开以后才生效）。

登陆方式：有 PPPoE 拨号和 Web 认证两种，您可以对不同的用户设定不同的登陆方式。

用户名/密码：为用户创建一个登录的登陆用户名及密码。

MAC 地址：有不绑定、自动绑定、手动绑定 3 种形式可供选择。

到期时间：可以对用户的上网期限进行限定。

IP 地址：用于手动给用户指定 IP 地址。pppoe 用户手动绑定的 ip 为 pppoe 拨号服务器地址池的 Ip, web 认证可以选择自动绑定 ip 和手动绑定 ip。web 认证的 ip 为局域网自动获取或者手动填写的 ip。

允许登陆的用户数：设定该账号可以允许被多少个用户同时登陆使用，即一号多拨功能。（当允许登陆的用户数设置大于 1 时，绑定的 MAC 地址将只会对第一个拨号的用户有效）

备注：对此用户的简单描述，方便管理员进行查看管理。

8.5 PPPoE 日志

记录 PPPoE 拨号连接的相关日志。

PPPoE 日志		
共：10 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页		
编号	时间	事件
0	03-04 14:35:10	session num: 1
1	03-04 14:35:11	123 用户在 00:07:4C:68:00:72 上登录!
2	03-04 14:59:14	对10.0.0.2 发送了 不能上网的通告!
3	03-04 14:59:16	对10.0.0.2 发送了 不能上网的通告!
4	03-04 14:59:32	123 : 收到TERMREQ!
5	03-04 14:59:32	123 : 收到PADT!
6	03-04 14:59:33	pppoe_session_death_by_timeout:372 下线!
7	03-04 14:59:33	123 用户PPPoE认证下线!
8	03-04 15:01:29	jhl_user_mod:1175 下线!
9	03-04 15:01:29	user del session:676 下线!

8.6 防御二级路由

该功能可以对路由器下面接入的用户进行控制，不允许挂接下级路由设备。如果路由下级有挂接二级路由设备，那么在二级路由下的用户（两个以上的上网用户）在开启网页时将会弹出禁止使用二级路由的通告提示。此功能对 PPPoE 拨号认证、WEB 认证、ARP 认证及动态获取 IP 的用户都有效。

防御二级路由器设置

状态

☐ 防御二级路由器

确定

提示页面

查看当前“提示页面”

使用默认“提示页面”

重新提交通告文件“提示页面”：

浏览...

提交

防御二级路由器：防御二级路由的功能开关控制，开启或者关闭此功能。
防御二级路通告页面：查看当前“提示页面”：路由器当前的防御二级路由信息提示页面；使用默认“提示页面”：默认的防御二级路由通告页面
重新提交通告文件“提示页面”：用于让用户导入自定义编辑好的防御二级路由的提示页面。

8.7 通告文件编辑

用于用户对现有的通告文件做修改、添加、删除等操作。

通告板1

还没有通告文件信息。

浏览...

提交新的通告文件

通告板2

还没有通告文件信息。

浏览...

提交新的通告文件

通告板3

还没有通告文件信息。

浏览...

提交新的通告文件

通告板4

还没有通告文件信息。

浏览...

提交新的通告文件

通告模板

下载通告模板

查看通告模板

导入的通告文件必须是‘.htm’格式的，且大小不能超过 8K，新的通告文件导入之后将会自动替换掉旧的通告文件。通告文件最多可以导入四条。

8.8 通告规则管理

通告系统是以 Web 页面的形式弹出的，设置的弹出窗口将只在用户开启浏览器访问英特网的时候将页面自动转向到您设置的通告页面。

通告规则列表

通告规则列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

状态	描述信息	用户范围	间隔时间	通告内容	基于时间控制	日志	操作
启用	12	内网全部IP	60分钟	通告板1	OFF	是	

通告规则管理

描述

12

☒ 激活 ☒ 日志

间隔时间

60

分钟

用户类型

基于IP地址

用户IP范围

(为空表示全部用户)

通告内容

系统通告文件

通告板1

查看通告

基于时间控制

☐ 启用

添加

修改

取消

帮助

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：对此规则的简单描述。

间隔时间：通告文件弹出的间隔时间，单位为分钟。（注：通告文件默认不会象弹窗广告那样自动弹出，只有在开启网页的时候才会将网页强行转向到指定的通告页面。）

用户类型/范围：选择通告文件的适用对象。有“基于 IP 地址”（针对指定 IP 用户弹出通告）、“基于 MAC 地址”（对绑定/未绑定用户弹出通告）、“基于接入类型”（对拨号用户/非拨号用户弹出通告）三种选择方案。

通告内容：选择您导入的通告文件或者直接使用外部 URL 地址。（建议使用本地导入的通告文件，因为外部 URL 地址开启速度会受到网络影响。若外部地址访问超时，用户会误以为网络不正常。）

日志：是否记录到日志。

基于时间控制：启用之后设定的规则将只会在指定的时间段内生效。

设定完毕之后点击‘添加’按钮，将规则加入列表之中。

8.9 通告日志

记录通告管理系统产生的一些日志信息。

通告系统日志		
共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页		
编号	时间	事件
0	03-04 16:16:10	对192.168.2.100 发送了 通告规则12 的通告信息

第九章、智能带宽管理

9.1 带宽设置

该功能用于设置广域网出口带宽以及流量控制例外。

出口线路带宽(智能QoS)

选择您要设置广域网

广域网1

参照值

ADSL 4M

上行带宽

40

Kbyte (千字节) (0 表示不设置)

下行带宽

380

Kbyte (千字节) (0 表示不设置)

流量控制例外

如果有某些外部服务器，访问他的流量不受接入带宽的限制，那么就需要设置这样的例外

流量控制例外 (基于IP)

192.168.2.101

(可以为空)

流量控制例外 (基于域名)

(可以为空)

保存

重填

帮助

设置每个 WAN 口的出口带宽，包括上行和下行，若您不清楚带宽值的换算，可以使用参照值来帮您自动填写。如果您的带宽不在参考值的范围之内，请手动设置出口带宽值大小。

流量控制例外(基于 IP)：填入您要排除的不受 QoS 控制的广域网 IP 地址。设置之后，您访问到该地址时的流量就不受智能 QoS 规则的限制了。

流量控制例外(基于域名)：填入您要排除的不受 QoS 控制的广域网域名地址（域名格式为：www.qq.com、*.baidu.com、xunlei 等）。设置之后，您访问到该域名时的流量就不受智能 QoS 规则的限制了。

注意：当您设置了 QoS 例外之后，您访问该地址时的流量统计就不会在流量监控显示出来了，包括主机监控也不会显示。

9.2 速度限制

在此界面中，您可以对内部机器的带宽使用进行自由控制。

9.3 带宽保证

对单个 IP 或者范围 IP 提供的一个带宽值保障。

[illegible]

状态：控制规则是否生效。选择启用，则表示该规则生效。

描述: 对该规则的描述。

控制方式:独占宽带, 此范围内每个 IP 独立享有设定的带宽保证值。; 共享宽带, 此范围内所有 IP 共享有设定的带宽保证值。

主机 IP 地址范围: 设置您要控制的主机范围 (单个机器 IP 或者是某个 IP 段)。
应用程序范围: 选择“全部”，是针对所有的应用程序。选择“基于程序组”，“基于程序”和“未识别到进程的数据包”，是针对您所选择的相对应的应用程序。

自定义 IP 协议:您可以自行定义远端 IP、域名及端口协议，并以此作为管控对象。

包含关系:对协议的包含关系。全部,表示应用协议与自定义协议都匹配;部分,表示应用协议与自定义协议可以只匹配其中一种。

上传速度:上传最高带宽保证值。如设置为 0 表示不保证。

下载速度: 下载最高带宽保证值。如设置为 0 表示不保证。

广域网选择:选择您要管控的协议对应的广域网。

基于时间控制：如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。（每周：您可以设置一周的哪几天生效，如果没有设置，则表示每天都生效；每天：您可以设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。）

9.4 流控类类型

用于控制路由数据、用户数据的处理优先级。

QoS优先级规则列表

共：1条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	描述信息	优先级	执行顺序	内部主机范围	应用程序	自定义IP协议	包含关系	广域网	基于时间控制	操作
启用	1212	高高	30000	192.168.2.21 ...	全部		全部	全部	OFF	 

流控类型

状态 ☒ 启用 ☐ 禁用

描述

全局优先级 ☐ 高 ☒ 中 ☐ 低 (该选项慎用, 默认为中)

局部优先级 ☐ 高 ☒ 中 ☐ 低

执行顺序 (1-85535)值越大越被执行。

主机IP地址范围 (为空:表示对该规定所有内部IP有效)

应用程序范围

自定义IP协议

包含关系 ☒ 全部 ☐ 部分

广域网的选择 (为空:表示全部广域网)

基于时间控制 ☐ 启用

状态：对规则的控制开关，选择启用表示激活该条规则。

描述：对该条规则的简单信息描述。

全局优先级：在整局域网内具有优先级，规则中的数据在通过路由器的所有数据中的优先级，分高、中、低三个级别。

局部优先级：单个主机中匹配该规则的数据在该主机所有数据中的优先级，分高、中、低三个级别。

执行顺序：规则与规则之间的执行顺序值，值越大的越被优先读取执行。

主机 IP 地址范围：设置您要控制的主机范围（单个机器 IP 或者是某个 IP 段）。

应用程序范围：选择“全部”，是针对所有的应用程序。选择“基于程序组”，“基于程序”和“未识别到进程的数据包”，是针对您所选择的相对应的应用程序。

自定义 IP 协议：您可以自行定义远端 IP、域名及端口协议，并以此作为管控对象。

包含关系:对协议的包含关系。全部，表示应用协议与自定义协议都匹配；部分，表示应用协议与自定义协议可以只匹配其中一种。

广域网选择:选择您要管控的协议对应的广域网。

基于时间控制:如果启用了此功能，那么该速度限制规则将只会在指定的时间段内生效。（每周：您可以设置一周的哪几天生效，如果没有设置，则表示每天都生效；每天：您可以设置一天的哪些时段生效，如果没有设置，则表示所有时间段都生效。）

9.5 应用程序设置

该功能用于设置是否开启进程客户端功能。

基本控制

控制方式 启用但不强制安装客户端

提示页面

查看当前“提示页面” 使用默认“提示页面”

重新提交通告文件“提示页面”

浏览...

提交

保存

重填

帮助

控制方式:控制方式可以用来选择是否开启客户端功能。

不启用:不启用应用程序控制功能。

启用，但不强制安装客户端:开启应用程序策略功能。PC 客户机可以选择安装客户端，也可以不安装客户端。

启用并强制安装客户端:开启应用程序策略功能。PC 客户机在开启网页的时候弹出下载确认，要求客户机必须下载安装客户端。

9.6 应用程序

应用程序列表可以用来查看当前应用程序的带宽使用状况。点击“查看”按钮可以显示当前进程对网络带宽的占用情况。

应用程序列表

应用程序列表

共：2 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

应用	组	文件名	上传数据	下载数据	上传速度	下载速度	操作
搜狗浏览器	网页	c:\program files\sogouexplorer\sogouexplorer.exe	603 b / 7 个	88 b / 2 个	44 b / 44 b	0 b / 0 b	查看
		c:\windows\system32\svchost.exe	0 b / 0 个	0 b / 0 个	0 b / 0 b	0 b / 0 b	查看

9.7 分组管理

分组管理主要是用于为应用程序进行归类，以便进行管理。

应用程序分组列表

应用程序分组列表

共：5 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

id	用户组名	操作
1	网页	
2	游戏	
3	P2P与下载	
4	IM	
255	default	

应用程序分组名

9.8 程序管理

程序管理可以针对程序的进程名、程序的目录/路径进行分类，结合策略路由的控制，以达到让指定的程序或者指定路径的程序按照设定的线路出去。以达到让游戏与下载分开走，互不干扰的效果。

用户列表

用户列表

共：882 条记录 当前 1/89 页 首页 上一页 下一页 末页 前往第 页

ID	标识	进程名	所属组	操作
882	猎豹浏览器	进程名:liebao.exe	网页	
881	糖果浏览器	进程名:tangoweb.exe 进程名:tango3.exe	网页	
880	搜狗浏览器	进程名:sougouexplorer.exe	网页	
879	QQ浏览器进程	进程名:qqbrowserexthost.exe	网页	
878	QQ浏览器	进程名:qqbrowser.exe	网页	
877	OPERA浏览器	进程名:opera.exe	网页	
876	裸奔浏览器	进程名:miniie.exe	网页	
875	遨游浏览器	进程名:maxthon.exe	网页	
874	IE浏览器	进程名:iexplore.exe	网页	
873	火狐浏览器	进程名:firefox.exe	网页	

操作

应用程序标识

QQ

应用程序进程名

0, qq. exe

所属组

IM

应用程序进程名：添加您需要管控的应用程序进程名或是应用程序的路径目录。（可以是进程名，也可以是程序路径目录，还可以是程序的路径目录+进程名）

类型：程序的匹配类型。

 仅匹配进程名：只匹配添加的程序进程名。

 匹配路径目录和进程名：匹配程序路径目录跟进程名。

 仅匹配路径目录：只匹配程序的路径目录。

进程设置

添加进程

类型:

0: 仅匹配进程名 (支持 * 通配符)

进程名:

0: 仅匹配进程名 (支持 * 通配符)

1: 匹配路径目录和进程名

2: 仅匹配路径目录

进程

0, qq.exe

删除

完成

取消

所属组: 选择所属的组别。组的类别是在“进程客户端-进程组”里进行添加的。
查找界面: 点击“查找界面”，可以按照自己的要求来查找进程。

用户列表

用户列表

共: 1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

ID	标识	进程名	所属组	操作
4	腾讯QQ	进程名:qq.exe	IM	

浏览...

导入应用程序分类信息

导出应用程序分类信息

删除所有应用程序分类信息

恢复默认进程分类信息

操作

应用程序标识

QQ

不参与

所属组

IM

and(并)

应用程序进程名

0, qq.exe

and(并)

添加

修改

取消

隐藏查找

查找

显示全部数据

刷新

帮助

比如查找腾讯 QQ 所属规则是 IM 的一条规则。
 添加应用程序之后，我们还需要在策略路由里面设置程序的出口线路，才能达到让指定程序从设定的线路走。

位于列表下方的导入导出功能，可以将您的进程分组信息及进程的配置导出到本地电脑，或者从本地电脑导入到路由器中。如图所示：



下面，我们以设置网页走 WAN1、所有游戏走 WAN2 来举例说明：

首先，我们需要在分组管理里添加新的分组信息，为了便于好记，我们就添加‘网页’跟‘游戏’两个分组。如图 1 所示：

应用程序分组列表		
共：5 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页		
id	用户组名	操作
1	网页	
2	游戏	
3	P2P与下载	
4	IM	
255	default	

(图 1)

之后我们需要在策略路由中设置网页走 WAN1 的规则，如图 2 所示：

状态	描述信息	顺序	广域网	内部主机范围	应用程序	远端IP范围	协议	基于时间控制	日志	操作
启用	网页	1	广域网1,		网页,			OFF	是	

(图 2)

接下来设置游戏走 WAN2 的规则，如图 3 所示：

状态	描述信息	顺序	广域网	内部主机范围	应用程序	远端IP范围	协议	基于时间控制	日志	操作
启用	网页	1	广域网1,		网页,			OFF	是	
启用	游戏	1	广域网2,		游戏,			OFF	否	

(图 3)

第十章、策略路由

10.1 负载均衡

负载均衡：用于设置线路的均衡模式及侦测方式、均衡权值等。

均衡模式

线路配置

智能型负载均衡模式

依会话数均衡

选择广域网

广域网1

该线路是否

参与默认均衡策略

均衡的权值

参照带宽值

线路侦测

激活

侦测间隔

10

秒 (设置范围 10-100, 系统默认值 10)

侦测次数

5

(设置范围 3-10, 系统默认值 5)

当线路连接失败时

移除该线路并记录日志

下载流量超过

0

Kbyte时不进行线路侦测. (为0表示, 不管流量多少都进行线路侦测)

侦测默认网关

www.baidu.com

侦测远程服务器

www.baidu.com

保存

重填

帮助

负载均衡模式分为 IP 地址均衡跟联机数均衡两种。

依 IP 地址均衡：依据内部用户的 IP 地址来决定线路的负载均衡。

依会话数均衡：依据用户的对外联机数来决定线路的负载均衡。

IP 均衡的作用，每条线路上的 IP 用户数目是等同的；会话数均衡的作用，每条线路上的对外联机数目是等同的。当使用会话数均衡的时候，就是将外网的几根线路都叠加起来，相当于是合并了总带宽。

选择广域网：选择您要设置的广域网接口。

是否参与默认均衡策略：勾上即表示参与，若不需要让此线路参与均衡，去掉勾即可。不参与均衡的线路将只接受策略路由里绑定的规则数据走向，若策略路由里也没有绑定数据走该线路，那么该线路将不会有数据流量。

均衡的权值：此值主要用于跟其他线路的均衡做比较，系统会根据值的大小来决定线路的负载大小，默认值是依靠带宽值的大小来自动判定，需填写出口带宽值才有效。若改为自定义，请根据线路的权衡比例来设置此参数，参数越大，通过的数据/用户就会越多。

线路侦测：启用线路侦测功能。激活时下面的选项才起作用，否则无效。线路侦测主要用于检测线路的通畅与否，对于多线路环境，若其中一根线路侦测失败，系统默认会将该线路移除，线路上的所有会话将会自动转移到另外侦测成功且参与均衡的线路上去。

侦测间隔：线路自动侦测的中间间隔时间。

侦测次数：线路侦测的次数。

当线路连接失败时：当线路检测失败时，对该线路的处理方式。

移除该线路并记录日志：将此线路删除，并记录到日志中，该线路上的所有连机将自动转移到其他线路上；仅记录到日志：仅在日志中记录下此次掉线日志，不删除该线路。

下载流量超过*时不进行线路侦测：下行流量超过设置值的时候才进行线路侦测。

侦测默认网关：勾选上即表示侦测此线路的外网网关。内容为空，表示侦测默认的网关。有些 ISP 的默认网关可能不允许 ping，那么可以自己手动指定一个其他的广域网地址来测试。

侦测远程服务器：填入一个稳定的域名或者广域网 IP 地址用于检测线路的通断与否。

注意：线路侦测默认是以 ping 来判断线路的通与断，所以，在填写侦测 IP 或者服务器地址的时候，请尽量选择一个长期稳定在线的地址。

10.2 电信网通地址

策略路由器的IP地址编辑

电信

启用 ☒ 下载电信地址范围 使用默认“电信地址范围”

提交新的电信地址范围: 浏览... 提交

网通

启用 ☒ 下载网通地址范围 使用默认“网通地址范围”

提交新的网通地址范围: 浏览... 提交

移动

启用 ☒ 下载移动地址范围 使用默认“移动地址范围”

提交新的移动地址范围: 浏览... 提交

教育网

启用 ☒ 下载教育网地址范围 使用默认“教育网地址范围”

提交新的教育网地址范围: 浏览... 提交

其它

启用 ☐ 下载其它地址范围 使用默认“其它地址范围”

提交新的其它地址范围: 浏览... 提交

自定义1

启用 ☐ 下载自定义1地址范围 使用默认“自定义1地址范围”

提交新的自定义1地址范围: 浏览... 提交

自定义2

启用 ☐ 下载自定义2地址范围 使用默认“自定义2地址范围”

提交新的自定义2地址范围: 浏览... 提交

查询IP

查询IP所在范围 查询 帮助

用于多条运营商线路的环境中，使用策略路由。只要选择好相应的线路，并设置好策略方式即可实现电信网通分开走，互不干扰。

查询 IP 所在范围:查询该 ip 属于以下已经启用的地址范围列表中的哪一类。
您可以在此界面自行更新电信/网通等的地址范围，或者自定义添加新的地址范围段。

10.3 策略路由

策略主要用于设置您内网用户对不同线路的走向。对于单线路用户，则无需对此功能进行设置。

策略路由规则编辑

状态

☒ 激活 ☐ 日志

描述

游戏

广域网的选择

☐ 广域网1 ☒ 广域网2 ☐ 广域网3 ☐ 广域网4 ☐ 广域网5

执行顺序

1 (1-65535)值越大越先被执行。

主机IP地址范围

(为空：表示对该规定所有内部IP有效)

应用程序范围

2

基于程序组

远端地址范围选择

自定义

远端地址范围 (基于IP)

(可以为空)

远端地址范围 (基于域名)

(可以为空)

协议

(为空：表示对该规定所有协议和端口)

基于时间控制

☐ 启用

添加

修改

重填

帮助

状态：对规则的控制开关，选择开启表示激活该条规则。

描述：对该条规则的简单文字描述，该描述必须是唯一的。

广域网的选择：当数据匹配上时，匹配的数据直接从选择接口出去，不再进行后面规则的匹配。

执行顺序：以 1-65535 之间的数字来表示规则的执行顺序，数值大的规则优先执行。

主机 IP 地址范围：设置您要控制的主机范围。就是“内网地址”。

应用程序范围：选择“全部”，是针对所有的应用程序。选择“基于程序组”，“基于程序”和“未识别到进程的数据包”，是针对您所选择的相对应的应用程序。

自定义 IP 协议：您可以自行定义远端 IP、域名及端口协议，并以此作为管控对象。

日志：对于匹配上的数据包，进行日志记录。

基于时间控制：如果启用了“基于时间控制”，那么该规则，将在指定的时间段内生效。

每周：您可以设置一周的哪几天生效。

每天：您可以设置一天的哪些时段生效。

在列表下方，您可以选择将设置的策略路由规则导入导出，如图所示：

浏览...

导入规则

导出规则

删除所有规则

10.4 线路状态

显示每根线路的在线状态及主机数、会话数信息。

线路状态列表						
共：2 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页						
接口	线路状态	均衡权值	默认均衡	线路侦测	主机数	会话数
广域网1	联机	1000000	参与	测试成功	0	3
广域网5	联机	1000000	参与	测试成功	0	4

10.5 策略路由日志

用于记录策略路由规则的日志记录和广域网口线路的工作状态，策略路由里，该线路开启线路侦测，且该线掉线之后才会在日志中显示。

策略路由日志		
共：34 条记录 当前 1/2 页 首页 上一页 下一页 末页 前往 第 页		
编号	时间	事件
0	03-04 17:46:10	规则 网页 :协议TCP, 本地(192.168.2.101:1216) 远端(118.123.202.251:80) 从广域网1出去
1	03-04 17:46:11	规则 网页 :协议TCP, 本地(192.168.2.101:1217) 远端(118.123.202.240:80) 从广域网1出去
2	03-04 17:46:11	规则 网页 :协议TCP, 本地(192.168.2.101:1218) 远端(182.140.236.240:80) 从广域网1出去
3	03-04 17:46:11	规则 网页 :协议TCP, 本地(192.168.2.101:1221) 远端(110.75.67.10:80) 从广域网1出去
4	03-04 17:46:11	规则 网页 :协议TCP, 本地(192.168.2.101:1224) 远端(182.140.238.241:80) 从广域网1出去
5	03-04 17:46:11	规则 网页 :协议TCP, 本地(192.168.2.101:1225) 远端(119.147.146.82:80) 从广域网1出去

10.6 端口映射

使外网可以通过 IP 地址或域名访问到内网机器映射出去的端口。



The image shows a '端口映射' (Port Mapping) configuration window. It includes a list of rules on the left and a detailed configuration form on the right. The form fields are: '激活' (Activation) with a checkbox, '描述' (Description) with a text box, '协议' (Protocol) with a dropdown menu set to 'TCP', '源地址限制' (Source Address Restriction) with a text box, '外部端口' (External Port) with a text box, '内部端口' (Internal Port) with a text box, '内部地址' (Internal Address) with a text box, and '网口设置' (Network Interface Setting) with a dropdown menu set to 'ALL'. A note for '网口设置' states: '(默认: ALL (表示全部), WAN1 (广域网1), WAN2 (广域网2), 多个用 ',' 分隔如: WAN1, WAN2, WAN4)'. At the bottom are buttons for '添加' (Add), '修改' (Modify), '重填' (Reset), and '帮助' (Help).

状态: 对规则的控制开关, 选择启用表示激活该条规则

描述: 对规则的简单描述。

协议: 分为 TCP、UDP、TCP 和 UDP。

源地址限制: 限制只有处于填入的 IP 或者域名所在的网络才可以访问路由映射出去的端口。不填即表示所有广域网的 IP 都能访问到映射出去的端口。

外部端口: 来自外部广域网的 IP 访问映射机器时的端口, 可以自定义, 但不能跟其他规则的端口相冲突。

内部端口: 内部局域网络访问映射机器时使用的端口, 一般由软件本身决定。若需要映射的内部端口跟外部端口一样, 则可以不用填写内部端口。

内部地址: 内网需要映射的机器 IP 地址。

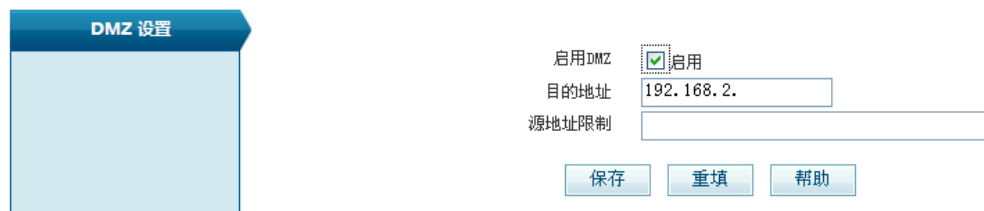
网口设置: 选择您要映射的广域网接口, 默认为所有接口 ALL。

举例: 将内部机器 192.168.1.2 的 TCP-2000 端口映射为外网的 TCP-1000 端口, 那么只需要按照上图这样设置就可以了。

内部机器访问 192.168.1.2 机器时使用 192.168.1.2:2000 这样的方式; 外部广域网网络访问映射机器时就需要使用 WAN 口 IP:1000 这样的方式来访问映射机器了。

10.7 DMZ 设置

当您将内部的某台机器 IP 填入到此 DMZ 选项时, 路由器 WAN 口的合法 IP 地址会直接对应给此台机器使用, 也就是说从 WAN 端进来的封包, 若是不属于内部的任何一台机器, 都会传送到这台机器上 (也就是把此机器完全的映射出去)。



The image shows a 'DMZ 设置' (DMZ Settings) configuration window. It includes a list of rules on the left and a detailed configuration form on the right. The form fields are: '启用 DMZ' (Enable DMZ) with a checked checkbox, '目的地址' (Destination Address) with a text box containing '192.168.2.', and '源地址限制' (Source Address Restriction) with a text box. At the bottom are buttons for '保存' (Save), '重填' (Reset), and '帮助' (Help).

启用 DMZ: 选择开启即表示启用此功能。

目的地址: 需要设为 DMZ 的内部机器 IP 地址。

源地址限制：是可选项，允许外部广域网口访问的地址或地址段。 允许输入“202.103.24.68”，“202.103.24.68-202.103.44.150”，“202.103.24.0/24”这三种格式。

10.8 端口触发

触发端口是初次 LAN 连接至 WAN 的“触发”。如果触发启用,WAN 至 LAN 的映射端口将被打开，这些端口将在不使用时几分钟后被自动关闭。



The screenshot shows the 'Port Triggering' (端口触发) configuration window. It has a blue header with the title. Below the header is a large light blue area for a list of rules. To the right of this area are the configuration fields: '启用' (Enable) with an unchecked checkbox, '描述' (Description) with a text box containing 'ex: open 5000-6000 if 3000-4000', '协议' (Protocol) with a dropdown menu set to 'TCP', '触发端口' (Trigger Port) with a text box containing '3000-4000', and '映射端口' (Mapping Port) with a text box containing '5000-6000'. At the bottom right are four buttons: '添加' (Add), '修改' (Modify), '重填' (Reset), and '帮助' (Help).

启用：选择开启即表示启用此功能。

描述：对规则的简单描述。

协议：分为 TCP、UDP、TCP 和 UDP。

触发端口：内部访问触发条件的端口。允许输入“8080”，“8000-8004”这样的格式。

映射端口：触发之后在广域网口对其开放的端口，WAN 可见。允许输入“8080”，“8000-8004”这样的格式

10.9 UPnP 设置

UPnP(Universal Plug and Play)是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的计算机有支持 UPnP 机制的话，而且您的计算机 UPnP 功能有开启，您可以将路由器的 UPnP 功能启动。开启 UPNP 之后，对 P2P 类的下载软件有一定加速作用，但同时您的网络也会产生更大的负荷，过多的 P2P 下载将会影响到您的网络正常使用，请酌情使用此功能。



The screenshot shows the 'UPnP Settings' (UPnP 设置) configuration window. It has a blue header with the title. Below the header is a large light blue area. To the right are the settings: '启用 UPnP' (Enable UPnP) with a checked checkbox, '广域网接口' (WAN Interface) with a dropdown menu set to '广域网1' (WAN1), and '在网络中显示' (Show in network) with a checked checkbox. At the bottom right are four buttons: '保存' (Save), '重填' (Reset), '刷新' (Refresh), and '帮助' (Help).

启用 UPNP：选择开启即表示启用此功能。。

广域网接口：选择需要设置的网络接口

在网络中显示：选择开启之后需要自动映射端口的应用类型软件就会在列表中显示，便于管理员查看使用的软件类型。

第十一章、VPN 管理

11.1 VPN 服务

PPTP 服务设置

PPTP 服务

打开服务

端口

1723

(默认端口是1723)

地址范围

172.100.1.100

-

200

(起始地址为PPTP的服务
器地址)

分配给客户的DNS

0.0.0.0

0.0.0.0

PPTP 服务：控制 PPTP 服务端功能的开启与关闭。做服务端来使用的时候必须先开启服务，做客户端使用的时候不用开启。

端口：PPTP 连接默认使用的端口，尽量不用去修改，否则可能造成 PPTP 连接失败。

地址范围：服务端分配给客户端的 IP 地址范围。此 IP 是连接 VPN 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障。因 VPN 连接之后会从中分配一个 IP 作为 VPN 网关地址，所以，此地址范围请设置至少 2 个以上的 IP 范围。

分配给客户的 DNS：服务端分配给客户端的 DNS 地址。只有在用到借线或者客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

L2TP 服务设置

L2TP 服务

关闭服务

端口

1701

(默认端口是1701)

地址范围

172.100.2.100

-

200

(起始地址为L2TP的服务
器地址)

分配给客户的DNS

0.0.0.0

0.0.0.0

保存

重填

帮助

L2TP 服务：开启或者关闭 L2TP IPsec 服务。

端口：L2TP IPsec 服务的端口号。默认是 1701。L2TP 连接默认使用的端口，尽量不用去修改，否则可能造成 PPTP 连接失败。

L2TP 客户端地址范围：服务端分配给客户端的 IP 地址范围。此 IP 是连接 L2TP 时的虚拟 IP，请不要将此 IP 与路由上的其他 IP 设置在同样的网段内，否则会造成 IP 冲突，引起网络故障。

分配给客户的 DNS：服务端分配给客户端的 DNS 地址。只有在用到借线或者客户端需要连接到服务端进行上网时才需要用到 DNS，此处应该设置服务端网络的 DNS 地址。

L2TP 客户端连接 VPN 时，需要使用系统自带的虚拟专用网络来创建 L2TP 连接。

11.2 VPN 用户

VPN 用户列表：显示用户管理的基本信息

用户管理列表							
共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页							
状态	登录名	密码	服务	指定IP	类型	备注	操作
正常	1	1	PPTP		VPN隧道192.168.11.0/24		 

用户管理：管理 vpn 的帐号，包括帐号的创建、修改与删除以及帐号类型的设置

用户管理

用户状态 ☐ 禁用

服务类型 PPTP用户

用户名

密码

指定IP

类型 VPN隧道

内网网段

格式：192.168.1.0/24 多个网段用' '分隔

备注

保存 修改 重填 帮助

- 用户状态：**勾选上表示禁用此帐号。
- 服务类型：**选择 pptp 或 l2tp 用户类型
- 用户名/密码：**为客户端分配的账号及密码。可以由英文字母或数字组成。
- 指定 IP：**如果不想用服务端自动分配的 IP，就可以在此处手动指定一个 IP。（指定的 IP 必须与 VPN 服务端分配的 IP 处于同一个网段内。）
- 类型：**有‘VPN 隧道’和‘VPN 借线’两种模式可以选择。
- VPN 隧道：用来连接服务端，与服务端的网络组建一个虚拟的局域网环境，可以共享服务端内部资源。
- VPN 借线：借用服务端的线路出口作为网络接口来上网，共享服务端的网络出口。
- 内网网段：**仅隧道模式有用。填入连接 VPN 的客户端的内网网段地址，格式：192.168.1.0/24 （例如：客户端使用的网段是 192.168.10.X，那么就应该填入：192.168.10.0/24）
- 备注：**对添加的用户账户的简单信息描述，由用户自定义。

当前用户状态：该列表用于显示当前用户连接 vpn 的状态信息

当前用户状态								
共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页								
用户	连接时间	服务	虚拟接口	IP地址	接收数据	接收数据包	发送数据	发送数据包
1	10秒	pptp	ppp150	172.100.1.101	0 b	0	0 b	0

11.3 VPN 客户端

使用路由器作为 VPN 客户端是用两种工作模式：隧道模式和借线模式。隧道

模式下，路由只作为 VPN 连接使用，可以共享虚拟网段的内部资源，但不能访问服务端的外部资源（也就是不能使用借线功能）。借线模式下，路由器客户端可以借用服务端的网络，通过服务端的网络来访问外部资源，但不能访问服务端内部资源。

选择您要设置的VPN

VPN1

VPN1设置

连接类型

L2TP

出口接口

ALL

(默认: ALL (表示全部), WAN1 (广域网1), WAN2 (广域网2), 多个用 ‘,’ 分隔如 , WAN1, WAN2, WAN4)

用户名称

用户密码

服务器地址

MTU设置

默认参数

1400

工作模式

隧道模式

(默认: 隧道模式)

路由网段

格式: 192.168.1.0/24 多个网段用 ‘,’ 分隔

保存

重填

帮助

- 选择你要设置的 VPN:** 选择你要设置的 VPN，默认值 VPN1.
- 连接类型:** 选择 PPTP 连接还是 L2TP 连接
- 出口接口:** 可以选择用哪个广域网作为 VPN 的出口，请尽量选择带宽大且稳定的线路做出口，以保证 VPN 连接的稳定性。默认是 ALL（表示全部）。
- 用户名称/密码:** 填入 VPN 服务端创建的用户名和密码。
- 服务器地址:** VPN 服务端广域网 IP 地址或动态域名地址。
- MTU 设置:** VPN 连接所使用的 MTU 值，默认是 1400。此值一般不做改动，使用默认值即可。
- 工作模式:** 有隧道模式与借线模式两种。默认是隧道模式。
- 路由网段:** 只有在选择隧道模式时此项才生效。这里填写服务端所在的网段（比如，服务器现在是 192.168.2.X 段的 IP，那么这里就填 192.168.2.0/24）。

11.4 VPN 状态

用于查看 VPN 客户端与 VPN 服务端之间的 VPN 连接状态。只有当路由作为客户端并与服务端连接以后，才会显示连接状态。

状态信息

选择您要查看的VPN

VPN1

VPN1设置

连接类型

pptp

连接状态

连接成功

出口广域网

WAN1

设备名

ppp100

本地IP地址

172.100.1.101

对端IP地址

172.100.1.100

DNS

MTU

连接时间

0 days, 00:00:05

连接

断开

帮助

11.5 OVPN 设置

OVPN基本设置

VPN模式

服务端

协议类型

关闭

超时检测时间

服务端

客户端

MTU设置

1400

1400

OVPN 模式： 关闭，不启用 VPN 服务； 服务端，将此路由作为 OVPN 连接的服务器端； 客户端，也就是 OVPN 路由客户端。

路由器的 VPN 连接方式分为路由与路由的连接和路由对 PC 机的连接两种：

路由对路由 即网关对网关的连接方式。也就是将其中一端的路由设置为服务端，另一端路由设置为客户端。在这种连接模式下，两端的路由若外网连接都正常，两者将会自动进行 VPN 连接，VPN 连接成功之后，服务端下面的所有用户与客户端下面的所有用户就组成了一个虚拟的局域网。

路由对 PC 客户机 即路由对客户机的连接方式。就是把路由器作为 OVPN 服务端，然后客户机利用 OVPN 连接软件来与服务端进行连接。在这种连接模式下，客户机必须利用 OVPN 软件手动去连接服务端，VPN 连接成功之后，该客户机就与服务端下面的所有用户组成了一个虚拟的局域网，即加入到服务端的局域网内。

VPN 服务端是提供给客户端做 VPN 连接而用，我们需要在服务端上建立不同的用户，分配给客户端用来连接 VPN。其中分为 PC 客户端的用户建立与路由器客户端的账号建立两种。

在 OVPN 模式中选择‘服务端’，如下图所示：

OVPN基本设置

VPN模式

服务端

协议类型

tcp

超时检测时间

60

秒

MTU设置

1400

(默认1400)

端口

4443

VPN虚拟网段地址

10.98.0.0

VPN虚拟网段掩码

255.255.255.0

用户之间互通

☒ 允许

保存

重填

帮助

然后，填写相关数据参数。

协议类型：自定义 OVPN 服务所走的协议。默认为 TCP 协议。

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时。

MTU 设置：定义 VPN 传送数据的 MTU 值，用于特殊环境中使用，一般保持默认即可。

端口：自定义一个 OVPN 服务使用的端口。默认为 4443，您可以修改为其他未被占用的端口。

OVPN 虚拟网段地址/掩码：自定义一个用来连接 VPN 的虚拟网段地址及子网掩码。（请避开您正在使用的网段。如您正在使用的是 192.168.X.X，请使用 10.X 或者 172.X 的 IP 段）

用户之间互通：即 VPN 客户端与 VPN 客户端之间相互通信的功能。默认允许。

以上已完成了服务端的基本参数设置，接下来我们需要为客户端建立 VPN 连接的账号及密码以供客户端与服务端来进行 VPN 连接。

OVPN用户列表

状态：☒ 激活

用户名：

用户密码：

添加

修改

重填

用户类型：

客户端是路由器

内网网段IP：

内网网段网掩码：

用户列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	用户名	密码	类型	内网网段地址	操作
1	123	123	路由器客户：192.168.2.0/255.255.255.0	192.168.2.0	

状态：激活/禁用此账号。

用户类型：请根据用户类型来建立相应的帐号。

客户端是 PC：建立的帐号只能用于 PC 电脑作为客户端使用 OVPN 客户端软件来连接 VPN 时使用。

客户端是路由器：建立的帐号只能用于路由器作为客户端时连接 VPN 使用。

用户名/密码：新建一个客户端用来连接 VPN 的账号及密码。（此账号是客户端路由用来连接服务端而使用的，用户账号可以由用户自行定义，请使用英文或者数字作为用户名/密码）

内部网段地址/掩码：此项仅对客户端是路由器时适用。填入您客户端连接 VPN 所用的内部 IP 地址及子网掩码。（此处 IP 不能与服务端内网处于同一网段。如，服务端路由 IP 为 192.168.1.X 段，客户端路由 IP 为 192.168.100.X 段，那么此处就需要填 192.168.100.0）

在路由器 OVPN 设置中选择客户端可以使用路由作为客户端来连接 OVPN，其设置方法比较简单，只需要填写几项关键参数就可以了，如图所示：

OVPN基本设置

VPN模式

客户端

协议类型

tcp

超时检测时间

60

秒

MTU设置

1400

(默认1400)

用户名

123

用户密码

●●●

密码确认

●●●

服务器地址

192.168.102.114

:

4443

服务器地址备份1

:

服务器地址备份2

:

服务器地址备份3

:

服务器地址备份4

:

保存

重填

帮助

协议类型：选择 VPN 连接所使用的协议类型，必须与服务端的协议类型一致，否则无法正常连接 VPN。

超时检测时间：在设定的时间内，未收到客户端的数据，则判断为连接超时。

MTU 设置：VPN 连接的 MTU 值大小，可由用户自定义，一般使用默认值即可。

用户名/密码：请填入您在服务端建立的路由客户端用户名及密码，并再次确认密码。

服务器地址：填写您服务端的 WAN 口 IP（外网 IP）地址或者动态域名。冒号后面填入与您服务端相同的协议端口号。

服务器地址备份：当您有多条 WAN 接入时，您可以分别填入其他 WAN 口的 IP 地址或者动态域名，当其中一条线路不通时，另外的线路可以继续保持 VPN 连接，使其不会意外中断；如果您只使用了一个 WAN 口接入，可以不用填写备用地址。

11.6 OVPN 状态

记录 VPN 相关连接的状态，管理员可以由此了解到 VPN 线路的运行状态，以便进行管理。

VPN 状态信息

连接时间：2013-03-05 02:19:48

发送的数据：5.25 K

接收的数据：6.92 K

刷新

重新连接

断开连接

帮助

11.7 OVPN 证书

主要用于用户下载原有的证书文件，或者自行导入新的证书。其中，ca.crt 证书文件是 PC 客户端连接 VPN 必须的文件，您可以将其下载下来保存好，以提供给 PC 客户端连接 VPN 时使用。

鉴于稳定性，建议用户使用默认的证书，以免使用自行导入的证书时出现问题。若您自定导入的证书在使用时出现问题，请点击右上方按钮将证书恢复到默认值。

证书管理

ca.crt

下载 ca.crt

提交新的 ca.crt 证书:

浏览... 提交

dh1024.pem

下载 dh1024.pem

提交新的 dh1024.pem :

浏览... 提交

server.crt

下载 server.crt

提交新的 server.crt :

浏览... 提交

server.key

下载 server.key

提交新的 server.key :

浏览... 提交

使用系统默认的证书

帮助

11.8 OVPN 日志

主要用于记录 OVPN 连接时出现的日志信息。

VPN日志

VPN日志

共：264 条记录 当前 1/27 页 首页 上一页 下一页 末页 前往 第 页

时间	消息
2013-03-05 02:25:17	Current Parameter Settings:
2013-03-05 02:25:17	config = /etc/openvpn/client.conf
2013-03-05 02:25:17	mode = 0
2013-03-05 02:25:17	persist_config = DISABLED
2013-03-05 02:25:17	persist_mode = 1
2013-03-05 02:25:17	show_ciphers = DISABLED
2013-03-05 02:25:17	show_digests = DISABLED
2013-03-05 02:25:17	show_engines = DISABLED
2013-03-05 02:25:17	genkey = DISABLED
2013-03-05 02:25:17	key_pass_file = [UNDEF]

刷新日志

删除日志

第十二章、防火墙

12.1 IP 地址组

添加 IP 地址组，对不同分组的 IP 进行管理。

IP地址组列表

IP地址组列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

组名	IP地址	操作
12	192.168.2.100-192.168.2.150	 

IP地址组

组名

12

IP地址

192.168.2.100-192.168.2.150

添加

修改

取消

帮助

组名称：对分组的名称描述。
IP 地址：添加一个或者多个 IP 地址。您可以对不同的 IP 划分分组来进行管理。

12.2 应用限制

可以有效过滤 P2P 软件、聊天软件、网络游戏、网络电视、其它软件。

应用限制设置

操作状态

☒ 启用 ☐ 禁用

日志

☐ 启用 ☒ 禁用

描述

控制方式

允许通过

执行顺序

65535 (1-65535)值越大越先被执行。

IP地址组

全部用户

被限制的应用类型

☒ P2P软件 ☐ 聊天软件 ☐ 网络游戏 ☐ 网络电视 ☐ 其它软件

被限制的应用

☐ QQ旋风 ☐ BT下载 ☐ 迅雷 ☐ emule电驴

基于时间控制

☐ 全选 ☐ 全不选 ☐ 反选

基于时间控制

☐ 启用

添加

修改

取消

帮助

操作状态：设置该规则是允许通过还是禁止通过。
日志：是否对匹配上的数据包，进行日志记录。
描述：对此规则的简单描述。
执行顺序：设置一个执行顺序值，值越大的规则越被优先执行。

IP 地址组：选择一个 IP 地址组范围。该组别是在‘防火墙-IP 地址组’里面添加的。

被限制的应用：依据您的需求，勾上要过滤的软件类型。

基于时间控制：是否启用按时间段来控制规则生效。

12.3 访问控制

访问控制的方式

禁止规则之外的通过

不启用访问控制

允许规则之外的通过

禁止规则之外的通过

提交

访问控制的方式：设置访问控制的方式，有三种选择：

不启用访问控制：关闭访问控制功能，列表中的所有规则将都不生效；

允许规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则不受控制，直接允许通过；

禁止规则之外通过：列表中的规则按照控制的方式来执行，列表之外的规则受到控制，禁止被通过。要单独设置允许通过的，请在规则中添加相应规则来运行其通过。

访问控制

状态

☐ 激活 ☐ 日志

描述

控制方式

允许通过

执行顺序

1 (1-65535)值越大越先被执行。

主机IP地址范围

(为空：表示对该规定所有内部IP有效)

远端地址范围 (基于IP)

(可以为空)

应用程序范围

全部

远端地址范围 (基于域名)

(可以为空)

协议

(为空：表示对该规定所有协议和端口)

基于时间控制

☐ 启用

添加

修改

重填

帮助

状态：对规则的控制开关，选择启用表示激活该条规则。

日志：对设置的规则记录日志，可以方便观察规则是否生效。

描述：对此规则的简单描述。

控制方式：控制访问规则是允许通过还是禁止通过。

执行顺序：用来比较多条规则的优先级，值越大越优先执行。当出现有相互冲突的两条规则时，会优先执行数值大的那一条规则。

主机 IP 地址范围：需要进行控制的内部主机 IP 地址范围。

应用程序范围：选择“全部”，是针对所有的应用程序。选择“基于程序组”，“基于程序”和“未识别到进程的数据包”，是针对您所选择的相对应的应用程序。

远端地址范围（基于 IP/域名）：您可以自行定义远端 IP、域名及并以此作为管控对象。

协议：需要控制的协议和端口，可以选择 TCP，UDP 和 ICMP，也可以是内部端口和外网端口。

基于时间控制：是否启动按时间段管控功能（若启用，用户可自定义管控时间段）。

12.4 访问控制日志

记录访问控制规则产生的日志记录，需要在添加规则的时候先勾选上日志选项才会记录。

访问控制日志		
共：4 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页		
编号	时间	事件
0	03-05 10:53:18	规则 12 禁止 协议TCP, 本地(192.168.2.100:2065) 远端(115.239.210.27:80)
1	03-05 10:53:20	规则 12 禁止 协议TCP, 本地(192.168.2.100:2066) 远端(115.239.210.27:80)
2	03-05 10:53:37	规则 12 禁止 协议TCP, 本地(192.168.2.100:2076) 远端(115.239.210.27:80)
3	03-05 10:53:38	规则 12 禁止 协议TCP, 本地(192.168.2.100:2077) 远端(115.239.210.27:80)

12.5 聊天软件黑白名单

聊天软件过滤方式

聊天软件过滤方式

允许如下号码, 禁止其他

不启用

允许如下号码, 禁止其他

阻止如下号码, 允许其他

保存

过滤方式：

不启用：不启用该功能。

允许如下号码，禁止其它：允许列表内添加的号码使用，禁止其他的号码使用。

阻止如下号码，允许其它：禁止列表内的号码使用，允许其它号码使用。

聊天软件黑白名单管理：

聊天软件黑白名单管理

描述

类型

号码

飞信

添加

修改

重填

帮助

描述：对规则的简单信息描述。

类型：选择你要管控的聊天软件类型（飞信、淘宝旺旺、MA、QQ）。

号码：您需要进行管制的聊天软件账号。

12.6 域名过滤

DNS 过滤方式

DNS 过滤方式

不启用DNS过滤

不启用DNS过滤

过滤列表中的，允许其他的通过

允许列表中的通过，过滤其他的

提交

NS 过滤方式：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式。

不启用，就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过，列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过，规则之外的所有都不允许通过，规则之内的受规则管控。

DNS 过滤

DNS 过滤

添加

帮助

添加所需过滤的域名或者域名关键字。

12.7 网址数据库

该页面可以往指定的分组里添加域名信息，用于完善已有的分组或者新添加的分组。

网址数据库

标识

百度

所属组

酷站

网址地址

www.baidu.com

添加

修改

重填

查找界面

刷新

帮助

同时您还可以将已有的网址分类信息导入路由或者导出备份，如图所示：

浏览...

导入网址地址分类信息

导出网址地址分类信息

删除所有网址地址分类信息

12.8 网址防火墙

网址过滤功能可以自定义设置规则用来控制用户对网页的访问，如下图所示：

网址过滤方式

允许规则之外的通过

☒ 弹出警告提示

提交

网址过滤规则列表

网址地址列表

共：1 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

状态	动作	标识	顺序	内部主机范围	网址范围	基于时间控制	日志	操作
启用	拒绝	百度	100		酷站,	OFF	是	

网址过滤规则编辑

状态：☐ 激活 ☐ 日志 动作：拒绝

描述：

执行顺序：100 (1-65535)值越小越先被执行。

主机IP地址范围： (为空：表示对该规定所有内部IP有效)

网站地址组： (为空：表示对该规定所有网站有效)

基于时间控制：☐ 启用

添加 修改 取消 帮助

网址过滤方式：有不启用、允许规则之外的通过和禁止规则之外的通过三种方式。

不启用，就是对列表中的规则不做任何控制，规则不会生效；

允许规则之外的通过，列表之外的规则允许通过，列表之中的规则受规则控制；

禁止规则之外的通过，规则之外的所有都不允许通过，规则之内的受规则管控。

弹出警告提示：选择开启，表示在打开被禁止的页面时，会弹出‘您访问的内容被管理员阻止’的警告提示。

状态：是否启用该规则。

日志：是否在日志中记录该规则的发生情况。

动作：该规则为允许通过还是拒绝通过。

描述：对规则的一个描述。

执行顺序：规则的执行优先等级。

主机 IP 地址范围：所限制的 IP

网站地址组：选择您要控制的网址分类组。

基于时间控制：是否启用按时间段来控制规则生效。

12.9 网址日志

记录网址防火墙控制时候产生的日志信息，根据日志可以查看有那些规则是被禁止或者允许的。

网址日志		
共：4 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页		
编号	时间	事件
0	03-05 11:15:04	规则 百度 拒绝 192.168.2.100访问 http://www.baidu.com/s?wd=yhg&ie=UTF-8&oe=UTF-8&bar=13&tn=daemon_cb
1	03-05 11:15:12	规则 百度 拒绝 192.168.2.100访问 http://www.baidu.com/s?wd=yhg&ie=UTF-8&oe=UTF-8&bar=13&tn=daemon_cb
2	03-05 11:15:13	规则 百度 拒绝 192.168.2.100访问 http://www.baidu.com/s?wd=yhg&ie=UTF-8&oe=UTF-8&bar=13&tn=daemon_cb
3	03-05 11:15:14	规则 百度 拒绝 192.168.2.100访问 http://www.baidu.com/s?wd=yhg&ie=UTF-8&oe=UTF-8&bar=13&tn=daemon_cb

第十三章、安全配置

13.1 联机数设置

主要用于设置路由器最大对外联机数目，默认连接数是根据机器内存自动获取的，默认情况下不需要做修改。

联机数设置

连接数容量设置

最大连接数614400

TCP超时设置

无 (None)600

已建立连接超时 (Established)1800

SYN发送超时 (SYN Sent)120

SYN接收超时 (SYN Received)60

FIN 等待超时 (FIN Wait)10

时间等待超时 (Time Wait)12

关闭连接超时 (Close)2

关闭等待超时 (Close Wait)10

最后响应超时 (Last ACK)3

侦听连接超时 (Listen)120

UDP超时设置

未答复超时 (Unreplied)180

已确认超时 (Assured)300

保存

重填

帮助

13.2 连接限制

连接数限制可以控制整个网络对外的联机数量。若对单个 IP 的连接数进行管控可以控制内网的计算机最多能同时建立的连接数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出连接数的软件提供了非常有效的管理。设置恰当的允许连接数可以有效控制 P2P 软件下载时所能产生的连接数，相对也使带宽使用量达到一定的限制。另外，若内网有计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。

默认主机连接数限制

ALL : TCP : UDP : (0 表示不限制)

保存

连接数限制列表

连接数限制列表

共 : 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页

状态	描述信息	主机IP地址范围	限制类型	限制数	基于时间控制	操作

连接数限制编辑

激活

☐ 激活

描述

主机IP地址范围

(为空 : 表示对该规定所有内部IP有效)

连接数限制

ALL (范围 : 1-2000)

基于时间控制

☐ 启用

保存

修改

重填

帮助

默认主机连接数限制：所有用户默认主机的连接数限制。当客户机连接数满了之后，由于新的连接出不去，就形同断网，所以请谨慎设置。

激活：是否启用规则，激活之后规则才会生效。

描述：对规则的简单描述。

主机 IP 地址范围：对指定的 IP 地址范围单独设置连接数规则，那么这些 IP 地址将只受规则限制，不受默认主机连接限制。

连接数限制：可以单独对 TCP/UDP 连接限制或者做全部的限制。

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

13.3 DDOS 攻击防御

对用户的并发连接进行限制。并发连接指一定时间内用户发起的连接的总数。

DDOS攻击防御

默认并发连接数：

ALL:

TCP:

UDP:

默认并发连接间隔时间：

ALL:

TCP:

UDP:

(秒)

保存

DDOS攻击防御列表

DDOS攻击防御列表

共：条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

状态	描述信息	主机IP地址范围	并发类型	并发数	并发时间	基于时间控制	操作

规则配置

激活

☐ 激活

描述

主机IP地址范围

(为空：表示对该规定所有内部IP有效)

并发类型

ALL

并发连接数

(范围：1-65535)

并发连接间隔时间

(秒)

基于时间控制

☐ 启用

保存

修改

重填

帮助

默认并发连接数：单位时间内可以发起的连接总数。规则之中的用户不受默认并发连接影响。

默认并发连接间隔时间：并发连接单位时间。

激活：是否启用规则。

描述：对规则的简单描述。

主机 IP 地址范围：需要单独控制并发连接的主机对象。

并发连接类型：可以单独选择 TCP，UDP 或者所有。

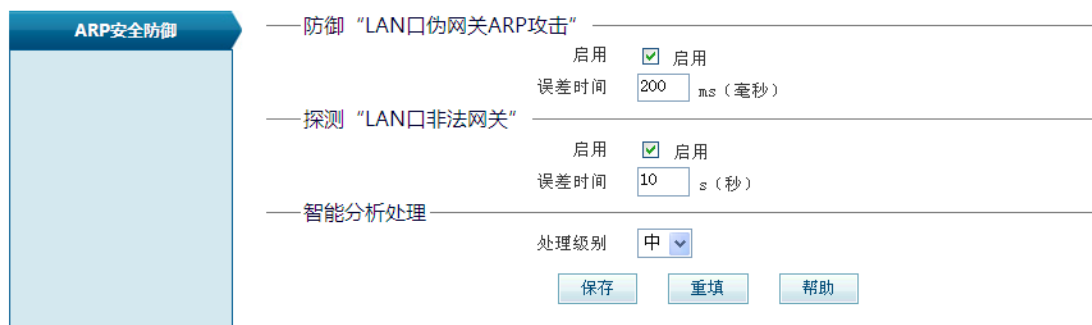
并发连接数：单机所允许的最大并发连接数条目。

并发连接间隔时间：相应的间隔时间，单位为秒。

基于时间控制：如果启用了“基于时间控制”，那么该规则将只在设定的时间范围内生效。

13.4 ARP 安全防御

ARP 用于设定 ARP 主动防御的相关参数。



ARP安全防护

— 防御 “LAN口伪网关ARP攻击” —

启用 ☒ 启用

误差时间 ms (毫秒)

— 探测 “LAN口非法网关” —

启用 ☒ 启用

误差时间 s (秒)

— 智能分析处理 —

处理级别

LAN 口伪网关攻击：防御常用的 ARP 攻击软件！如果“网络执法官”、“P2P 终结者”、等 ARP 攻击软件，对其他电脑的网关攻击！是否存在攻击，将记录在“ARP 日志”。默认时间间隔是 200ms。

探测 LAN 口非法网关：检查内网是否有 IP 和路由器的 LAN 的 IP 相同，如果有，将记录在“ARP 日志”。默认检测时间是 10s。

处理级别：ARP 防御系统智能防御系统的处理级别，级别越高，越安全。您可以根据网络环境做相应调节。

13.5 ARP 绑定

ARP 绑定允许用户对局域网 IP 或者广域网 IP 进行手动绑定。



ARP 绑定

描述

IP地址

MAC地址

类型

接口

描述：对该条绑定信息的简单文字描述，便于管理员区分。

IP 地址：将要绑定的 IP 地址。

查询 MAC：如果该 IP 地址在线则可以点击该按钮查询到其使用的 MAC 地址。

MAC 地址：输入您要进行 ARP 绑定的 MAC 地址，可以通过“查询 MAC”来设置 MAC。如果用户不在线则需要手动输入。

类型：分为两类：“静态”和“唯一”。“静态”：IP 与 MAC 地址绑定为静态以后，用户手动更改 IP 或者 MAC 地址不会影响网络使用，但其他用户不能占用此 IP 跟 MAC 地址。“唯一”：不但限制这个 IP 地址只能在这个 MAC 上使用，同时也限制了这个 MAC 地址只能使用指定的 IP 地址，（等同于，这个 IP 地址只能指定网卡上使用，同时，这个网卡，也能使用指定的 IP 地址）。

接口：如果绑定的 IP 地址属于局域网请选择“局域网”，如果将要绑定的 IP 属于广域网请选择“广域网”。

在列表下方，您可以对所有绑定的 MAC 地址进行导入导出操作，如图所示：

浏览...

导入ARP绑定信息

导出ARP绑定信息

删除所有ARP绑定

13.6 ARP 列表

ARP 列表显示当前局域网连接用户的 IP 及 MAC 信息。

ARP列表

共：5 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往第 页

IP地址	MAC地址	接口	类型	状态	提示	操作		
192.168.2.100	00:07:4c:68:00:72	局域网	动态	正常		取消绑定	设为静态	设为唯一
192.168.102.254	00:0c:29:f1:58:d4	广域网5	动态	正常		取消绑定	设为静态	设为唯一
192.168.102.114	80:81:00:d7:71:92	广域网5	动态	正常		取消绑定	设为静态	设为唯一
192.168.102.1	80:81:00:20:5a:81	广域网5	动态	正常		取消绑定	设为静态	设为唯一
192.168.55.1	80:81:00:56:c2:56	广域网1	动态	正常		取消绑定	设为静态	设为唯一

将LAN所有未绑定的设为静态

将LAN所有未绑定的设为唯一

刷新

将 LAN 所有未绑定的设为唯一： 将局域网未绑定过的用户一键绑定为唯一类型。

将 LAN 口所有为绑定的设为静态： 将局域网为绑定过的用户一键绑定为静态类型。

唯一：指只有 IP 和 MAC 地址对应才能连接网络。

静态：将该 IP 地址指定为只能在该 MAC 地址上使用，但是该 MAC 地址还可使用其他 IP 地址连接网络。

13.7 ARP 日志

ARP 日志：当网络出现广播回路，ARP 绑定错误或者 ARP 攻击时，路由器会在日志里面记录相关信息。

ARP 日志		
共：2 条记录 当前 1/1 页 首页 上一页 下一页 末页 前往 第 页		
编号	时间	事件
0	03-05 11:36:26	在"br0" 口,有一个MAC为"00-07-4C-68-00-72" 的设备的IP与该接口的IP"192.168.2.1" 相 同!请管理员及时处理!
1	03-05 11:36:26	在br0 口出现广播回路，请检查网络