

目录

第一步：准备路由硬件.....	2
第二步：GHOST 百为流控软件.....	4
第四步：许可认证.....	10
第五步：部署路由到网络.....	11
第六步：管理小区用户.....	16
第七步：多线分流.....	23
第八步：内网防护.....	26
第九步：DHCP 服务器配置.....	28
第十步：用防火墙限制 UDP 上行流量.....	29

第一步：准备路由硬件

小区用户通过两种途径获得硬件：（一）、选用百为官方硬件；（二）、自己 DIY 机器。

自己 DIY 机器，百为流控路由需要一台独立的机器运行系统，不能和其他服务器软件共用一个硬件平台，这台机器最少配置两个网卡（或者一片双口网卡）。

百为流控官方硬件规格

硬件型号	WAN 口数	应用带宽范围	在线用户量
BV100	4WAN（不可扩展）	15M	30 人
BV300	5WAN(可扩展)	60M	100 人
BV600	3WAN(可扩展)	120M	200 人
BV800	5WAN(可扩展)	200M	300 人
BV1000	5WAN(可扩展)	400M	500 人
BV1800	5WAN(可扩展)	2G	1500 人

DIY 硬件配置要求

硬件	要求	说明
内存	512MB，或以上	最好用 DDR2 或者以上的
磁盘	128MB，或者以上	硬盘 - CF 盘 - 电子盘
主板	推荐用 intel 芯片的主板	AMD 芯片的主板可能会遇到一些奇怪的兼容性问题，不推荐使用
CPU	最好用奔腾4以上 Intel CPU	用户上300户推荐用 E5700系列 CPU、用户1000户的推荐用1230V2 或者 I5、I7CPU
网卡	推荐 Intel/BCM 系列网卡，支持部分 Realtek 系列网卡	内网口最好用 PCI-E 的千兆网卡

已知的兼容问题

硬件型号	问题描述
VIA CPU	无法启动
SCSI 旧款硬盘	不支持 SCSI 硬盘

Nforce 网卡	可以使用，但不推荐。桌面级网卡，对于高要求的高负载网吧不建议使用，转发性能差。
Realtek 8139	可以使用，但不推荐。桌面级网卡，对于高要求的高负载网吧不建议使用，转发性能差。

第二步：GHOST 百为流控软件

选用百为官方硬件的用户，由于官方硬件的软件已经自带，直接跳过这一步内容。

自己 DIY 硬件，需要把百为流控软件 GHOST 到准备好的启动磁盘（CF 卡，电子盘）中，百为流控官网（<http://www.bytevalue.com>）提供了 GHOST 文件以及配套的 GHOST 工具。官网提供的 GHOST 安装文件最大支持 8 核心和 4G 内存；对于超过 8 核心和超过 4G 内存配置的硬件，请联系代理或者百为官方获取对应的升级文件，考虑到对老硬件兼容问题，官网暂时不提供下载。



注意

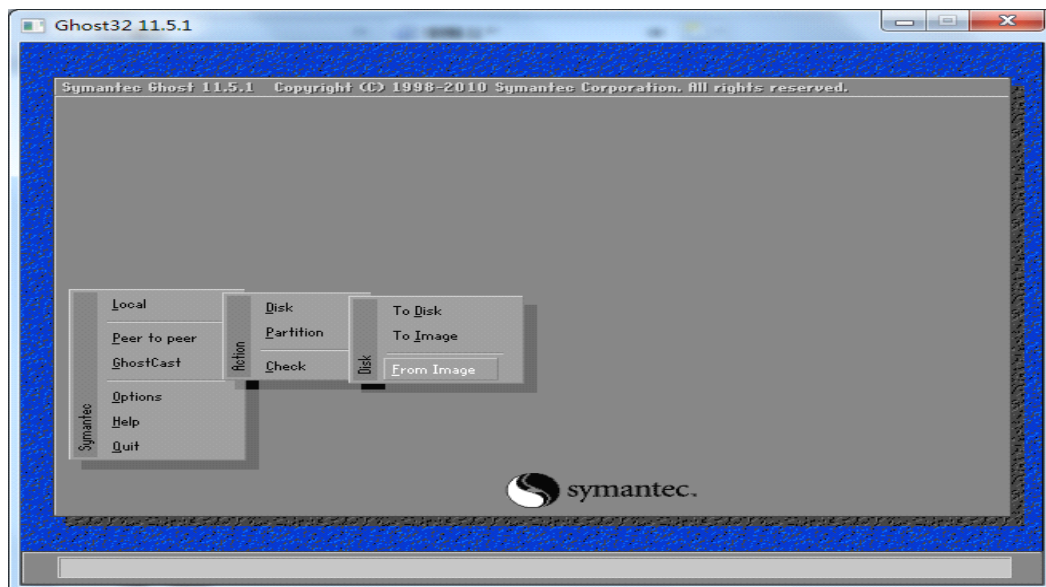
在进行 GHOST 前，必须用官网安装包里面自带的 GHOST（11.5.1 版本）软件进行 GHOST 操作。

需要 GHOST 的磁盘不能分区，如果有分区的，先删除磁盘分区，清空 MBR，然后全盘 GHOST。

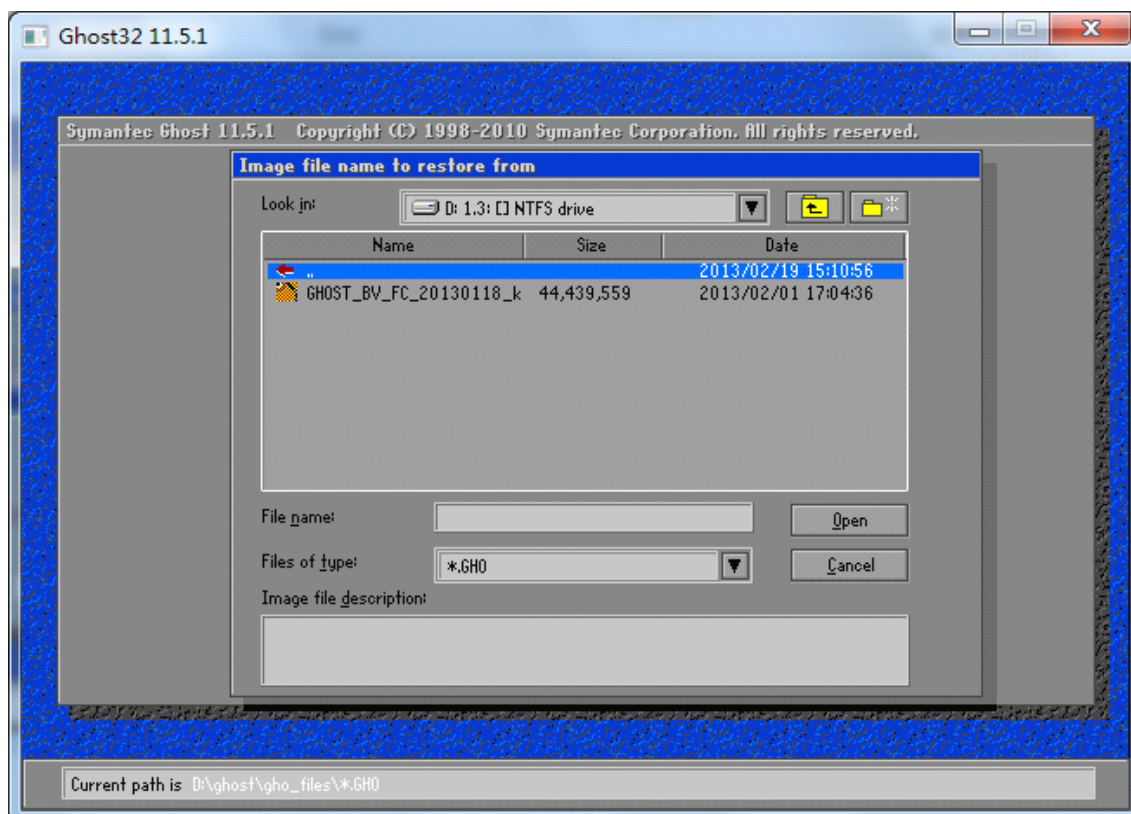
如果是硬盘 GHOST，在 GHOST 过程中可以指定 GHOST 的大小，推荐为 500M，避免漫长的等待。如果需要保存日志到硬盘，选择 10G 空间进行 GHOST。

GHOST 步骤如下：

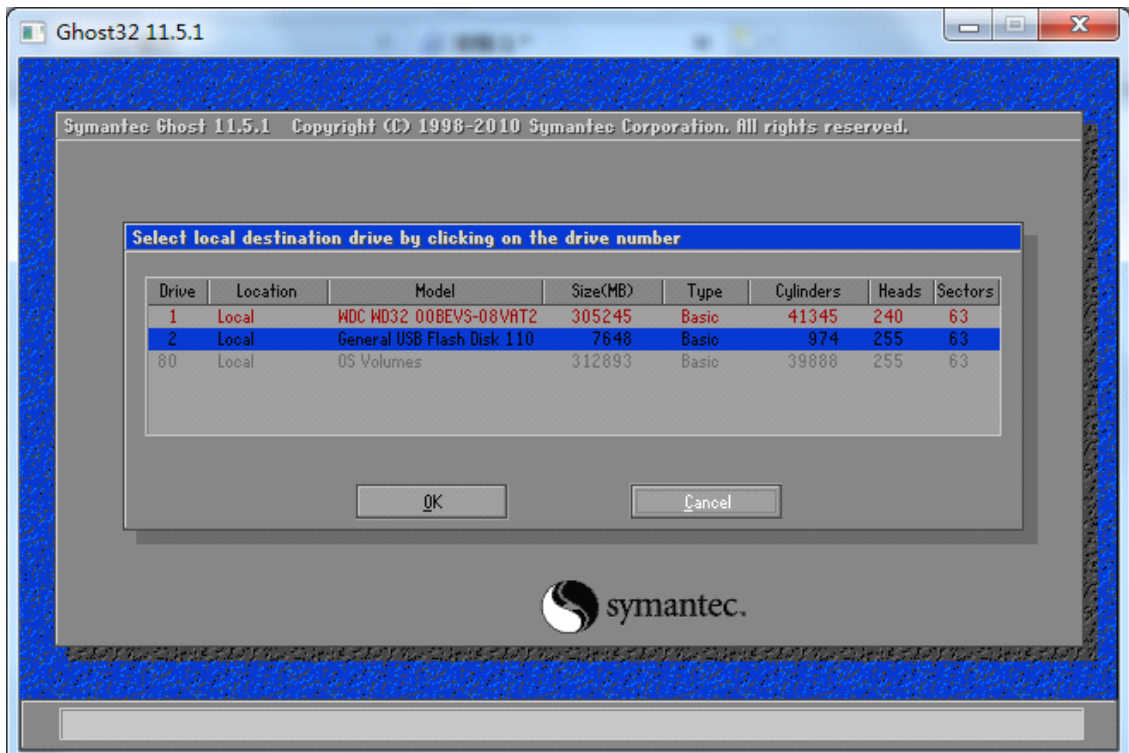
- 1、把准备做软路由的磁盘插入 Windows 主机中，并且确定在 Windows 的【计算机管理】
->【磁盘管理】中能识别出所插磁盘。
- 2、下载百为流控官网提供的 GHOST 安装包，展开，运行 ghost32.exe
(1) 选择【Local】->【Disk】->【From Image】，如下图所示：



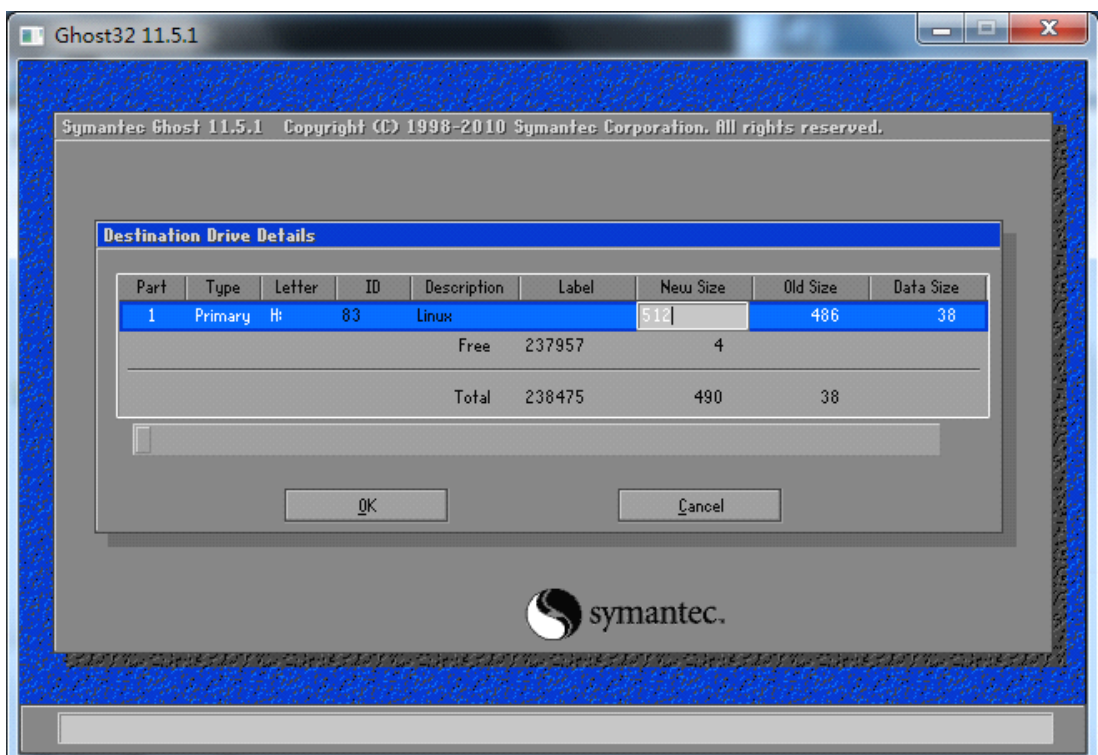
(2) 选择 BYTEVALUE 软路由的 GHO 文件，作为 GHOST 源文件，如下图所示：



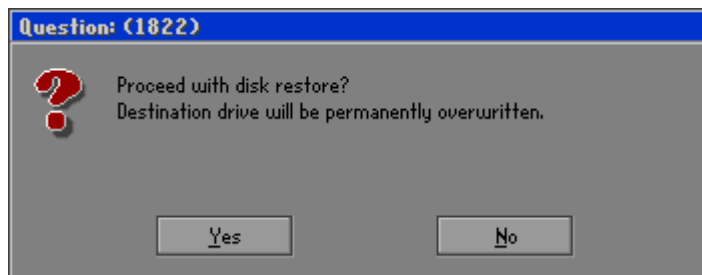
(3) 选择要做软路由的磁盘作为目标磁盘，如下图所示：



- (4) 自定义 GHOST 磁盘大小，GHOST 文件需要的磁盘空间最小为 128M。不修改界面默认值，对整个磁盘进行 GHOST，硬盘越大，GHOST 的时间会越长。推荐做法是在【New Size】位置自定义 GHOST 大小，如下图所示使用 512MB 来还原。



- (5) 选择 Yes，确认写入完成。



3、GHOST 完成后，测试是否可以启动百为流控路由，启动出现“BYTEVALUE”字符画面，则表示启动成功；如果无法启动到“BYTEVLUE”字符画面，则说明 GHOST 失败，可以做如下尝试：

- 更换启动盘的 IDE 或者 sata 接口尝试
- 更换主板

第三步：登录路由

GHOST 成功、路由启动后，所有配置都是出厂默认配置，软路由和硬路由默认配置一致，参考下表：

接口	IP 地址	掩码
eth0	192.168.0.1	255.255.255.0
eth1	192.168.1.1	255.255.255.0
eth2	192.168.2.1	255.255.255.0
eth3	192.168.3.1	255.255.255.0
eth4	192.168.4.1	255.255.255.0
eth5	192.168.5.1	255.255.255.0

举例两种方法，说明通过 eth0 口登录路由。

方法一：通过 eth0 的内网 IP 地址登录路由，具体步骤如下：

- 1、找到 eth0 口，如果是百为硬件，看硬件上的丝印找到 eth0 口，如果是 DIY 硬件，可以通过插拔网线，看路由的显示器上的显示，来判断网线连接的是哪个网口，如果出现，eth0 link up，和 eth0 link down 这样的字符，表示插入的是 eth0 口。
- 2、网线连接到 eth0 口。
- 3、eth0 的默认地址是 192.168.0.1，客户机必须配置和 eth0 一个网段，比如：客户机 IP 配置为 192.168.0.100，掩码配置为 255.255.255.0。
- 4、客户机尝试 ping 192.168.0.1，如果能 ping 通，则通过 <http://192.168.0.1:2011> 登录路由 web 界面，web 界面的默认用户名和密码都是 admin。

方法二：通过 eth0 口的默认拨号帐号登录路由，具体步骤如下：

- 1、找到 eth0 口，如果是百为硬件，看硬件上的丝印找到 eth0 口，如果是 DIY 硬件，可以通过插拔网线，看路由的显示器上的显示，来判断网线连接的是哪个网口，如果出现，eth0 link up，和 eth0 link down 这样的字符，表示插入的是 eth0 口。
- 2、网线连接到 eth0 口。
- 3、eth0 提供了默认的拨号帐号，用户名和密码都是：**bv**，创建拨号连接拨号登录。拨号成功后，通过地址 <http://10.1.0.1:2011> 登录路由 web 界面，web 界面的默认用户名和密码都是 admin。

软路由控制台的常用命令：

- 查看路由识别了几个网卡

`ifconfig`

- 手工配置网卡 ip，提供临时配置使用，重启后不会保存

`ifconfig eth0 192.168.0.100 netmask 255.255.255.0`

- 查看路由密码

`cat/etc/ftpdpass`

- 恢复出厂配置

`resetfactory`

第四步：许可认证

目前，百为提供免费一个月的试用，通过邮箱就可以在网站上直接获得测试许可 ID 和 KEY，测试 ID 在测试到期后，付费延期继续使用，测试期间的路由功能和付费后完全一样。百为的认证服务器会检查测试硬件和网络等信息，确保一个网吧有一次测试一月的机会。

- 获得测试 ID 的网址为：<http://bytevalue.com/index.php?ctl=member/apply-enduser>、代理商可以在自己代理后台直接创建测试 ID。
- 获得 ID 后在路由的【设备维护】->【许可认证】界面输入 ID 和 KEY，然后单击保存和单击重新认证，百为采用在线认证方式，必须确保路由外网口可以上网才能认证成功。
- 百为官方硬件 BV100，BV300，和 BV690，BV890 等设备认证 ID 和 KEY 已经提前写入，不需要申请认证 ID。
- 授权过期，或者无授权的路由不建议用户使用。

第五步：部署路由到网络

把百为流控路由部署到网络中，用户需要根据自己的网络情况，判断路由需要用到几个网卡，是否需要其他配套设备，然后，清楚正确的把路由连接到网络中，最后对网络接口进行配置，确保下面客户机正常上网。

首先需要了解下面几个基本概念：

- 1、**网卡工作速率**——确定好组网方案后，要做的就是通过网线把百为流控路由连接到网络中，网线连接后，用户需要检查物理网卡的工作速率是否正确。经常遇到千 M 网卡工作在百 M 上这种造成网络卡的问题。如果电信提供的是百 M 猫，路由上显示的工作速度是 100M，这属于正常情况；但是，如果内网口和交换机都是千 M，界面却显示工作速度为 100M，就说明物理连接上出了问题，容易造成网络卡；出现此问题的原因通常是没有使用千 M 网线，或者水晶头接触不良造成。

类型	工作速率
外网口 [ADSL拨号] [拓展口]	1000M
外网口 [ADSL拨号] [拓展口]	1000M
内网口	1000M

- 2、**子网掩码**——IP 和子网掩码共同决定一段 IP 地址范围（具体的计算方法这里不做说明，可以参考其他资料），这一段 IP 地址是彼此直接可访问的，是不需要通过路由转发才可以访问的地址，了解子网掩码的概念，帮助解决两个问题。

- 判断 ISP 给我们分配的 IP、掩码和网关是否正确。网关是路由直接可以访问到的 IP，所以路由 IP 和掩码决定的地址范围必须包括网关 IP。经常遇到 ISP 给错了网关或者掩码，造成配置 IP 后无法通的问题。
- 本地内网网段冲突问题；百为流控路由上的所有内网网段禁止 IP 范围冲突。如果界面提示 IP 地址范围错误，意思就是说配置的内网网段和其他的内网网段冲突；例如：eth0 配置 IP 192.168.0.1 子网 255.255.255.0，eth1 配置 IP 192.168.1.1 掩码 255.255.254.0；这就是两个冲突的网段；eth0 的范围是 192.168.0.1~192.168.0.254，eth1 的范围是 192.168.0.1~192.168.1.254，显然 eth0

的地址范围被 eth1 包含了，这种就是百为不允许配置的。

3、线路中断检测——外网接口配置的一个选项。这个选项的作用是检测线路是否正常连通外网，如果没有正常连通，线路会显示为离线状态；对 PPPOE 拨号的线路、除非特例这个选项是必须选择的，多光纤线路网吧，也建议勾选（当某线路断了后，不影响其他线路），单光纤网吧不建议勾选（单线路断了，选择和不选择都一个意义），成都和重庆专网线路不能勾选（无法进行检测）。

4、防御信息检测——外网接口配置的一个选项，只对拨号线路有效。ISP 的信息检测功能，是防止多用户共享一条线路上网，俗称网络尖兵，这个功能的作用，就是防御 ISP 的信息检查，由于各地 ISP 的检测设备不同，所以提供了模式一到模式四的 4 种防御方式，目前的经验是默认都用模式四防御；如果模式四无法防御，然后依次尝试模式三，模式二和模式一。模式四对网速无任何影响，其他模式对网页的访问速度以及部分网站访问造成一定影响。

下面通过典型的小区应用情景来举例说明，逐个说明各情景的具体部署方法：

情景 1——单线路

- 单线路小区，路由需要安装两个物理网卡，分别与外网线路以及内网交换机连接。
- 外网口配置——对固定 IP 线路，在这个网卡上配置外网 IP、掩码和网关以及 DNS；对 PPPOE 拨号线路，配置拨号帐号和密码，DNS 通常不需要手工指定。
- 内网口配置——配置内网 IP 和掩码，通常推荐用户配置 255.255.0.0 作为内网掩码。

这样做 DHCP 服务时，可以为下面用户分配比较大的地址池。

情景 2——用多网卡实现多 WAN

总外网线路不超过 6 条的小区，推荐用户为每条线路配置一个物理网卡实现多 WAN 组网。在每个外网网卡上配置对应的外网信息，然后用一个内网网卡连接内网交换机。具体的接口配置方法和单线路的配置方法是一样。

情景 3——通过 VLAN 交换机扩展多 WAN

小区超过 6 条外网线路（光纤、网线或者电话线）的，推荐用 VLAN 交换机来实现 WAN 口扩展，因为用太多网卡到路由上，网卡出故障的风险增加。

通过 VLAN 扩展 WAN 组网的方法，就是通过 VLANID 来区分不同接口上的线路，路由上只需要两个网卡，一个网卡连接 VLAN 交换机 TRUNK 口，一个网卡连接到内网交换机、具体操作步骤如下：

- (1) 给线路编号，给每条线路确定一个 VLANID，例如：确定的 ID 范围是 101~124，对应第 1 条到第 24 条线路。
- (2) 配置 VLAN 交换机，给 VLAN 交换机对应外网线路的接口上配置 VLANID，依次为 101~124，每个接口对应一个 VLANID。
- (3) 把交换机的 TRUNK 口连接到路由的外网口，然后在路由的外网口上配置 VLAN 子接口，子接口的 VLANID 和交换机的 VLANID 一一对应。然后在每个 VLAN 子接口上配置对应的外网接口信息。
- (4) 对所有的 VLAN 子接口进行随机 MAC 地址生成。因为很多地区，ISP 都做了 MAC 地址检查，避免同样的 MAC 多次拨号，你的所在地区可能有多个百为流控，所以这一步也是有必要。



注意

禁止用于扩展 WAN 的 VLAN 交换机和路由的内网口（或者网吧的内网机器）连接。即使这个扩 WAN 的 VLAN 交换机做了端口隔离，也不允许连接，这种连接会造成网络和路由出现各种奇怪问题。

外网总带宽超过 100M 后，扩 WAN 的 VLAN 交换机 TRUNK 口以及路由的外网口都必须是 1000M 接口，要确保连接的工作速率为 1000M，否则，这里成为瓶颈造成网络卡。

情景 4——通过子接口扩展 WAN

单光纤（或者 LAN 的形式），然后 ISP 提供很多拨号帐号。这种情景用子接口扩展 WAN，不需要用 VLAN 交换机扩展 WAN。路由配置最少需要两张网卡，光纤（或者 LAN）连接路由的外网口，内网口连接内网交换机。具体操作步骤如下：

- (1) 在外网接口上创建子接口、有多少个帐号，就创建多少个子接口。
- (2) 在每个子接口上输入一个帐号的拨号信息；如果一个帐号可以拨号几次的，每次拨号当成一个独立的帐号，在几个子接口上填写同样的帐号。
- (3) 对所有的子接口随机生成 MAC 地址。因为很多地区，ISP 都做了 MAC 地址检查，避免同样的 MAC 多次拨号，你所在地区可能有多个百为流控，所以这一步也是有必要。



注意

目前百为是支持总接口数不超过 180 个；

帐号总带宽超过 100M 的线路，必须用 1000M 网卡并且 ISP 也必须提供 1000M 的接口。如果 ISP 只能提供 100M 的接口对接，路由就需要用多个网卡做子账户，确保每个网卡上帐号总流量不超过 100M，否则，这里成为网络瓶颈造成网络卡。

多线路各种模式混用——有时候需要多线路的各种混用，这些混用就是上面多线路情景的简单组合。

情景 5——内网用户多，通过多个内网口来负载

内网用户较多，网络流量也比较大的时候，推荐用 2 个或者 3 个网卡来负载内网用户。多网卡负载，一方面可以让多核 CPU 发挥更好，另一方面也可以让网卡压力减小。配置方法：为每个内网网卡配置内网网段和掩码，在每个内网口上开启 PPPOE 认证服务。

情景 6——内网用户多，内网用 VLAN 隔离，同时 PPPOE 拨号认证上网

内网用户比较多、需要做 VLAN 隔离、并且采用 PPPOE 拨号上网方式。这种应用情景，需要在交换机上划分 VLAN，把交换机的上行口配置为 TRUNK 口，TRUNK 口连接到路由内网口做认证上网。具体配置步骤如下：

- (1) 在交换机上划分多个 VLAN 子网。
- (2) 在路由内网口上创建对应 VLAN 子网 ID 的 VLAN 子接口。
- (3) 交换机 TRUNK 口连接到路由的内网口。
- (4) 在每个 VLAN 子接口上开启 PPPOE 认证服务。

这种组网方式兼顾了 VLAN 隔离和 PPPOE 拨号认证方式。

情景 8——外部认证

部分地区的小区经营者，逐步的转变成 ISP 的代理商。从 ISP 那里批发帐号，然后把这些帐号销售给自己小区内网的用户，这部分用户直接拨号到 ISP，网速是 ISP 决定的，他们和小区其他用户是共用一个内网，百为专门为这部分小区开发了外部认证功能，兼容本地认证上网和外部认证上网。

在组网上，外部认证的用户和小区其他用户，内网口是公用的，外网口可以公用、也可以单独搞个网卡专门走外部认证用户，并且，外部认证功能可以支持多 ISP 认证，为多个 ISP 同时提供外部认证功能。举例配置如下图：

系统状态

网络配置

用户管理

对象管理

运行

用户对象

部门级别划分

认证上网

认证消息编辑

认证通知设置

本地认证配置

外部认证配置

计费配置

免密码认证

PPPoE服务

外部认证

外部认证配置 | 外部认证状态 | 外部用户管理

功能启用: 已启用, 点击禁用

添加

删除

序号	认证接口	服务名
☐ 1	eth2	10010
☐ 2	eth3	10000

这个小区 eth2 是联通线路光纤（含有 100 个 6M 帐号），eth3 是电信线路光纤（含有 200 个 2M 帐号），小区经验者同时代理电信和联通的帐号；小区内部联通用户、电信用户和共享上网用户并存，通过 eth0 和 eth1 内网口上网，区别在于联通用户走 eth2 认证，电信用户走 eth3 认证，共享上网用户本地认证。外部认证的用户，同时也受到路由管理。



注意

目前的外部认证功能不支持内网是 VLAN 接口的拨号认证。

第六步：管理小区用户

目前支持 4 种用户认证类型：IP 地址认证、MAC 地址认证、PPPOE 拨号认证、WEB 网页认证。IP 地址认证和 MAC 地址认证，通过地址信息直接认证；WEB 认证需要机器获得（或者配置）IP，通过网页输入用户名和密码认证；PPPOE 拨号认证，是通过建立拨号连接认证。前 3 种认证方式都面临内网 A R P 攻击和内网 I P 地址冲突问题，只有解决好这两个问题（通常解决方法是 V L A N 隔离），这些认证上网方式才比较合适。P P P O E 拨号上网，不害怕这两个问题（这两个问题的存在不会用影响用户上网），是目前小区最主流的认证上网方式。

认证用户都在用户对象列表里，下图说明用户的各属性含义。

部门——选择用户所属部门，部门是提前划分好的。

级别——选择用户的限速级别，级别是提前划分好的

帐号状态——“启用”表示帐号可以拨号，如果已经到期则看到过期通知；“禁用”则无法拨号。

MAC 绑定——“禁用”表示不绑定 MAC，“启用”表示绑定 MAC，“自动”则在用户第一次认证的时候，自动修改为“启用”，并且绑定用户当前 MAC 地址。

路由限制——目前通过把 TTL 修改为 0 限制用户使用路由上网，不过，这个功能目前对

部分路由已经失效。

客户端限制——“不限制”表示不需要允许客户端，“必须安装客户端”则表示，路由如果发现这个用户没有允许客户端，就弹出安装客户端提示网页，让用户安装运行。

创建时间——用户创建的时间；

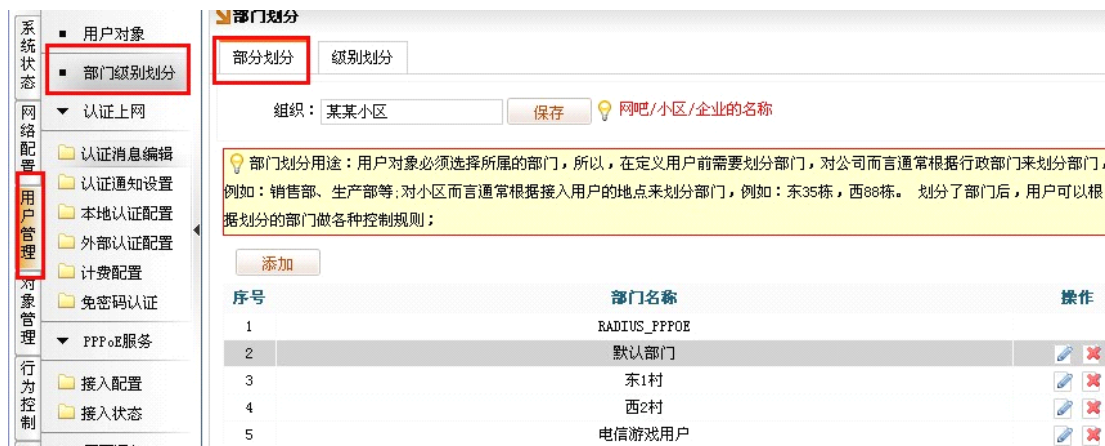
过期时间——用户允许上网的截止时间；

下面逐步说明如何配置和管理小区用户：

1、划分部门和级别

划分部门——用户对象必须选择所属的部门，划分部门为了细化管理用户。对小区而言，列举两种常见的划分方法：

- 按接入用户所在地点来划分部门，例如：东 35 栋，西 88 栋。这种划分方法是为了方便了解用户所在片区。
- 按用户接入性质来划分部门，例如：电信用户，联通用户，游戏用户等，这种划分方法是为了方便对用户做分流。



部门划分

部分划分 级别划分

组织：某某小区 保存 网吧/小区/企业的名称

部门划分用途：用户对象必须选择所属的部门，所以，在定义用户前需要划分部门，对公司而言通常根据行政部门来划分部门，例如：销售部、生产部等；对小区而言通常根据接入用户的地点来划分部门，例如：东35栋，西88栋。划分了部门后，用户可以根据划分的部门做各种控制规则：

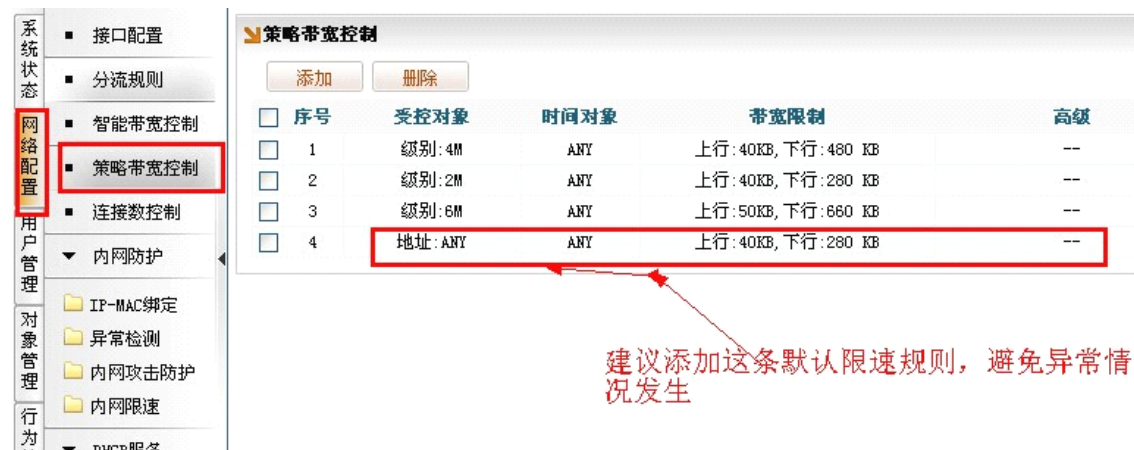
添加

序号	部门名称	操作
1	RADIUS_PPPOE	
2	默认部门	 
3	东1村	 
4	西2村	 
5	电信游戏用户	 

划分级别——用户对象必须选择所属的级别，对小区来说级别的主要用途是做限速级别，为用户分配不同的代理类型。例如：2M、4M、6M 等。



配置级别限速——用户划分级别后，只有配置了对应级别的限速规则，限速才生效。需要强调下，如果是 ADSL 线路（或者上行比较小的光纤），建议给用户的上行在 18KB~30KB 内的范围，如果是对称光纤，给用户的上行在 40KB~100KB，不建议给用户超过 100KB 的上行，给造成网络不必要负担。

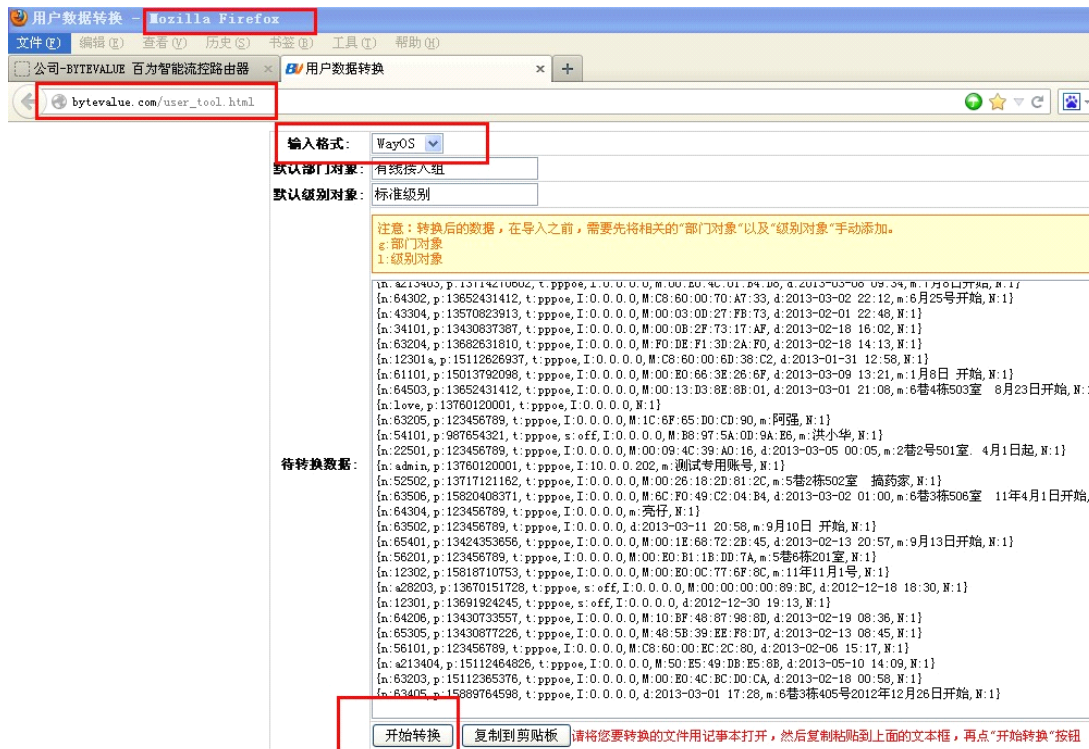


2、导入（或者添加）用户

百为官网提供了用户转换工具，可以把其他路由（包括 ROS、海蜘蛛、WAYOS）的用户数据转换到百为路由上。具体操作为：

- 1、用火狐浏览器打开，http://bytevalue.com/user_tool.html 链接；
- 2、把用户数据粘帖到网页文本框，点开始转换按钮
- 3、把转换后的用户信息拷贝出来，复制到【用户配置】-》【用户对象】-》【批量添加】，完成用户导入。
- 4、修改导入用户的级别和部门；

实例说明将其他路由的用户数据添加到百为路由，具体操作步骤如下图：



把 WAYOS 的用户粘帖进去，点开始转换



把转换过的用户，粘帖到百为的批量添加，点确定导入用户。

3、配置认证上网

使用了 PPPOE 拨号上网的用户，首先检查内网口的 PPPOE 服务器必须开启，如果有多个内网口拨号，每个内网接口都需要开启 PPPOE 服务。

本地认证配置，内网有那些认证类型的用户打开相应的认证开关。每个用到认证的内网

口都需要开启本地认证上网，否则，用户不认证也可以上网。

参考下面对 eth1 口的配置实例图，其他接口配置方法一样：

通过MAC地址，为电影服务器分流固定IP...

当地运营商DNS

用户比较多的这个时间给长点

提示：1、修改PPPoE拨号配置之后，已经拨号上的用户会断开网络，需要重新拨号！
2、PPPoE的拨号用户，统一在用户对象里面管理，点击进入 用户管理 > 用户对象

在 eth1 口开启 PPPOE 服务器，为电信服务器固定了拨号 IP；

在 eth1 口开启本地认证，只允许拨号用户上网。

4、配置小区网页通知

路由默认带了几个小区常用网页，位于【用户管理】-》【认证消息编辑】菜单：

欢迎页——小区用户通过 DHCP 得到 IP 上网后，由于没有拨号认证，在上网时，路由返回欢迎网页，网页内容通常是开户联系信息。

到期提醒页——根据配置，对快到期用户，提示缴费通知。

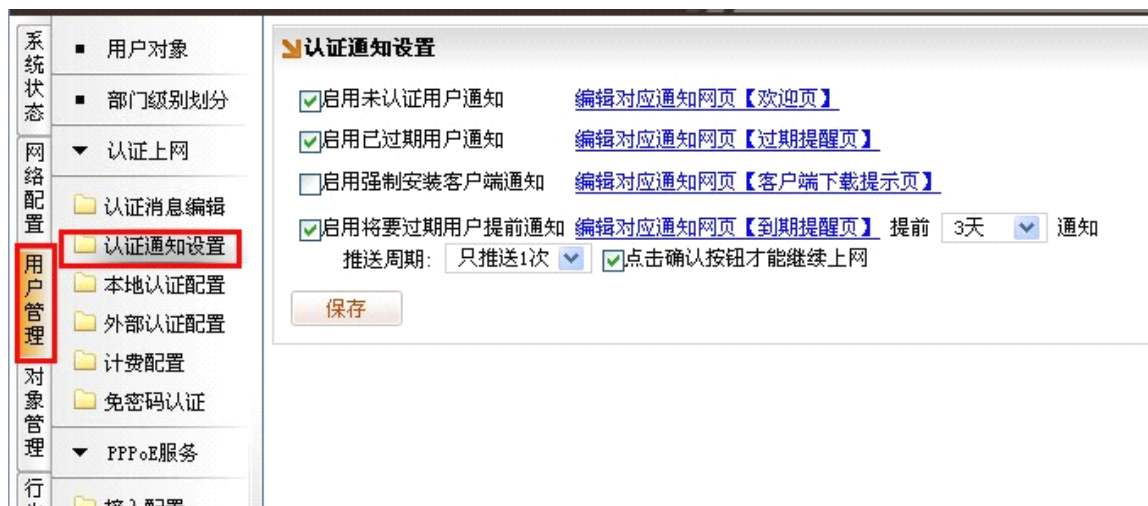
过期提醒页——用户过期后，路由返回的提示用户过期需要缴费的网页。

客户端下载提示页——对必须安装客户端的用户，如果用户未允许客户端，会提示出下载并运行客户端的通知。

实名 WEB 认证页——网页认证的用户，上网时候看到的输入用户名和密码认证的网页。

在这些网页中，如果出现“%用户%”和“%过期时间%”这表示，这些内容会转换成接收到网页的用户的具体用户名和过期时间，属于网页个性化信息。用户自定义网页时，也可以参考应用，实现网页个性化。

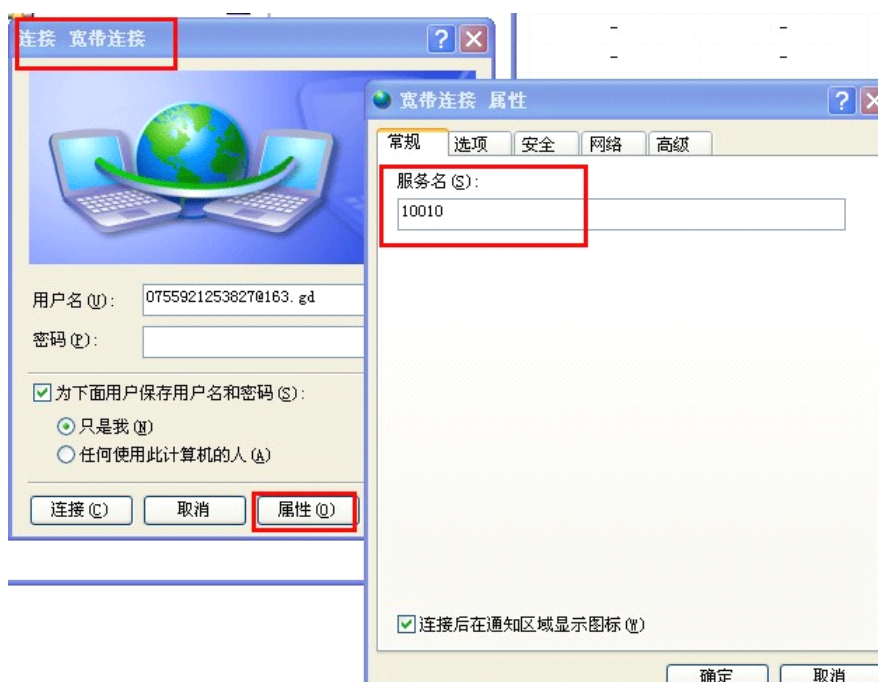
了解了小区通知网页的具体意义，根据需求来配置通知，下图给出一个实例图：



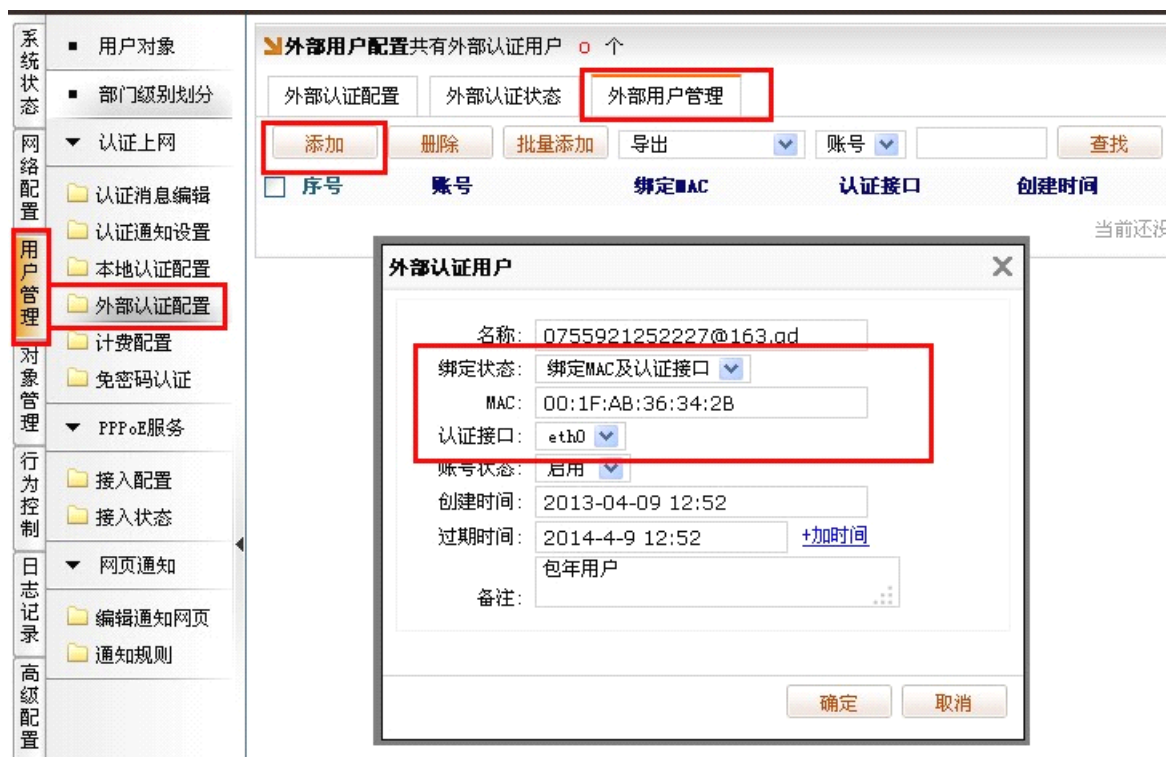
5、外部认证用户管理

没有外部认证需求的忽略这一小节。前面介绍了外部认证的网络部署要求，这里介绍外部认证用户管理，以及相关的限制。路由通过下列两个方法的其中一种来区分外部认证用户，只有识别为外部认证用户后，才可以拨号到对应的 ISP：

方法一：外部认证用户在拨号的时候填写了指定的 ISP 服务名，参考下图：



方法二：在路由上提前把拨号用户的 MAC 地址绑定到指定的 ISP，即开启“绑定 MAC 及认证接口”功能，参考下图：



上面两种方法不建议同时使用，用户选择一种自己比较方便操作的方式就可以。



注意

选用方法 1 的用户，外部帐号也是必须添加到外部用户管理，不能开启“绑定 MAC 及认证接口”功能。如果需要把外部帐号绑定到一个电脑使用，可以开启自动 MAC 绑定。

已经选用方法 1 的用户，如果需要用本地帐号拨号，必须把拨号连接里面先前配置的服务器名清空。

选择方法 2 的用户，用户拨号连接里面的服务器名需配置为空。

另外，外部认证用户管理功能会验证用户名和用户的到期时间。验证到期时间是根据路由里面配置的时间，不一定是 ISP 帐号的到期时间。代理拿来的用户帐号，可能是包年的，但是销售给小区内部用户可能是按月收费。

第七步：多线分流

这章根据小区典型的应用情景来描述分流的配置方法。

要掌握分流需要清楚的了解下面几个概念：

1、规则、规则执行次序以及全 ANY 规则

分流和限速都是通过配置规则控制的，路由的很多配置也都是通过规则来控制，有必要搞清楚下面的概念。

- **规则**——简单说就是在匹配条件后执行相应动作。条件由各种对象构成，包括地址、部门、级别和用户对象、时间，端口、应用和 ISP 对象等，匹配条件就是比较这些对象是否一致，执行的动作就是分流和限速。
- **规则执行次序**——规则从上到下执行，执行过程首先是匹配规则条件，条件不匹配，则规则无效，继续对下一条规则进行匹配，条件匹配了，则执行这条规则的分流（或者限速）动作，后面的规则不再进行匹配和执行。
- **全 ANY 规则**——所有条件对象都选择 ANY 的规则。ANY 的意义就是和任意对象匹配，所有对象都是 ANY 也就是说这条规则无条件匹配，通常，放在规则列表的最后一条，作为默认规则。把这条 ANY 规则放到了第一条，通常都是错误配置，结果就是：第一条规则匹配所有条件，后面的其他规则就没有机会匹配和执行、变的无意义。

2、IP 分流、会话分流以及分流权重

- **IP 分流**——匹配规则条件的内网用户根据分流权重比例选定线路。选定线路后，内网用户所有匹配此规则的网络数据包会固定走这条线路。
- IP 分流的主要用途是对不能同时走多线的应用进行分流，典型应用如下：
 - ✓ 分流特定应用——比如网银，六合彩等博彩网站都只能走单条线路，走多条线路时，这些应用无法认证和登录。
 - ✓ 网通+电信的情况，通过对 DNS 的 IP 分流，让网通和电信各负载部分用户
- **会话分流**——把匹配条件的应用数据均匀的分布在选择的线路上，在这些线路上做负载均衡。大多数的分流规则都是用会话分流。
- **分流的权重**——只对 IP 分流的规则有意义，权重大小通常都根据线路的带宽大小配置。会话分流的权重都必须填写为 1。既然必须是 1 为什么还需要输入值？这是

遗留问题，以后会话分流可能不再需要输入分流权重值，目前务必填写为 1。

3、网页视频和网页下载分流

- **网页视频分流**——【高级配置】-》【模块开关】里面的“网页视频分流”开关决定网页视频分流是否生效。开关开启后，路由会把网页视频从网页中细化出来，开关关闭，则网页视频属于网页应用对象。
- **网页下载分流**——【高级配置】-》【模块开关】里面的“网页下载分流”开关决定网页下载分流是否生效。开关开启后，路由会把网页下载从网页中细化出来，开关关闭，则网页下载属于网页应用对象。
- **一种常见的错误**——网页视频分流模块开关开启，未对网页视频做分流，对网页做了分流，经常习惯性的认为网页视频会走网页分流线路,实际上，此时的网页视频应用类型已经不属于网页应用，会走默认分流线路。为了减少类似错误，建议在没网页视频分流和网页下载分流规则时，关闭掉对应模块开关。

分流的目标是合理高效利用带宽，考虑分流规则主要就是从这个基本点出发。

情景 1——单光纤

分流规则

单线路不需要做分流规则；

情景 2——同 ISP 的多光纤小区

分流规则

- (1) SSL 端口 IP 分流到所有线路（保证网银可用）
- (2) QQ 端口 IP 分流到所有线路（保证 QQ 单 IP 认证）
- (3) 所有线路会话分流

情景 3——联通+电信双光纤

分流规则

- (1) DNS 端口 IP 分流，权重值为带宽比例
- (2) 电信 ISP 对象走电信线路（通常带宽小或者次要的线路进行 ISP 分流）
- (3) 其他所有（ANY 规则）走联通（通常是带宽大或者主要线路做默认规则）

情景 4——大移动+小电信、大长宽+小电信、大联通+小电信

这种情景的主要特点是，小电信走游戏，其他走大线路。

分流规则

- (1) DNS 分流到移动（长宽或者联通）线路
- (2) 电信的游戏分流到电信线路
- (3) 其他所有（ANY 规则）走移动（长宽或者联通）

情景 5——多拨号线路（拨号光纤或者电话线拨号）

对小区来说，游戏用户不多，挑选 1、2 条线路质量好的线路来做游戏线路，其他线路负载其他应用。

分流模式

- (1) 游戏分流走游戏线路
- (2) SSL 端口 IP 分流到非游戏线路
- (3) QQ 端口 IP 分流到非游戏线路
- (4) 其他所有（ANY 规则）会话分流到非游戏线路

游戏分流问题

目前，对用到游戏分流规则的用户。提供两种方法达到游戏分流效果。

1、运行用百为小区客户端

这种方法，就是给小区游戏用户百为客户端，游戏用户可以开机允许即可，会在桌面右下角出现客户端图标，这是目前推荐的方案。特别是对应游戏线路资源紧张，需要精确分流的用戶，目前只有这种方法最可行。

2、通过 IP+端口的方式分流游戏

地址端口对象，可以以 IP+端口形式定义游戏端口。路由可以通过这个对象列表做游戏分流。这个收集工作在不断完善中，需要的用户可以找百为索取配置文件，也可以自己定义。这种方法的缺点是精确度一般，也存在不准确的地方。对于不安装客户端，又很需要游戏分流的用戶可以采纳。



注意

小区客户端不能跨路由使用，如果小区用戶用路由上网，小区客户端无效。

游戏分流的两种方法，暂时不建议同时使用，即，采用客户端的用戶不要配置游戏端口。

地址端口对象的收集还在继续、用到的用戶密切关注

第八步：内网防护

小区环境复杂，没有 VLAN 隔离的网络就更容易出问题。需要配置必要的防护功能。

内网防护配置

- **内网环路检测**——检测内网是否有环路，如果检测到，会显示出来。
- **内网 DHCP 检测和抑制**——部分路由开 DHCP 后会造成网络无法上网的情况，打开这个开关可以对这些路由进行一定的防御，避免无法上网的问题。



内网攻击防护——可以过滤掉在内网口的 DDOS 攻击，并且可以指定在那些接口上防御。



用户连接数限制——防止连接数攻击，造成路由无法上网，或者负担过重。



内网限速——限制内网用户之间的传输速度。内网用户对传数据，有时候经过路由，这种情况下如果不限速内网速度，会由于速度过大而造成交换机阻塞，拖慢整个内网。



内网状态分析

在配置了上面的防护功能后，如果发生异常情况，可以在内网状态菜单判断问题。



内网状态——显示 IP-MAC 冲突、内网 DHCP 服务器和内网环路情况。

内网上行流量——通过显示上行流量，来发现是否存在内网攻击源，这个流量是到达路由接口的流量，并不是路由转发到外网的流量。所以，这个流量比限速的流量大一些，都属于正常情况，只有这个流量异常的大，才是攻击源。

内网 QQ 号在线状态——当一个用户的 QQ 号码超过 4 个，会显示这个帐号，这个功能是防止用户通过 WINDOWS 的连接共享上网。如果一个帐号下 QQ 号多，又发现内网有不拨号就上网的情况，限制掉这个开共享的帐号可以了。

第九步：DHCP 服务器配置

架设 DHCP 服务器有两个目的：

- 用户如果没有配置 IP，开机后获得 IP 能启动快点；否则，启动会慢些。
- 开启 DHCP 后，给用户分配 IP 后，没有拨号的用户，在上网时可以看到通知的欢迎页。

不管小区大小，推荐用户用一个不常用的内网 IP 做内网 IP（例如：192.170.0.1），用 255.255.0.0 的做内网掩码，这样可以有一个比较大的地址池，减少 IP 冲突情况。

如果有多个内网口则再在个内网口开启 DHCP 服务器，参考下图：

DHCP服务配置

所有内网口

eth1
eth2
eth3
eth4
eth5

功能启用： 已启用, 点击禁用

基本参数

接口IP: 192.170.0.1/255.255.0.0
 网关: 192.170.0.1
 主DNS: 114.114.114.114
 备用DNS: 8.8.8.8
 掩码: 255.255.0.0
 域: (可选)
 地址租期: 36000 秒 默认值: 3600
 最长租期: 86400 秒 默认值: 86400

IP地址池

	开始IP	结束IP
地址池1	192.170.100.1	192.170.200.200
地址池2		
地址池3		
地址池4		

如果用其他 DHCP 服务器为内网做 DHCP 服务，则需要关闭路由的 DHCP 功能。

第十步：用防火墙限制 UDP 上行流量

对于上行资源充分的小区，这一步可以忽略。

对于纯 ADSL 或者上行非常紧张的小区，通过配置防火墙规则、限制掉大部分的 UDP 应用（主要 P2P 应用），节约上行流量，有很强的实用价值。

首先，需要做两个准备工作：

- 1、定义一个“不限制 UDP”部门，把实在无法搞定的用户修改为这个部门。不限制他们的 UDP。
- 2、添加地址端口对象，把游戏的 UDP 端口和 QQ 的 UDP 端口添加进来，如果有其他需要允许的 UDP 端口也添加进来。

有了这两个准备，配置防火墙规则如下：

- 1、“不限制 UDP”部门的所有应用放行
- 2、所有 TCP 端口协议放行
- 3、所有游戏应用对象放行
- 4、所有 IM 应用对象放行
- 5、默认规则（ANY 规则）阻止所有 UDP 端口

参考下图：

序号	受控对象	时间	目的地址	端口	应用	线路	动作	操作
1	部门:不限制 UDP	ANY	ANY	ANY	ANY	eth0, ptp11[11]	放行	↓ ↓ ↓ ↓
2	地址: ANY	ANY	ANY	tcp	ANY	eth0, ptp11[11]	放行	↑ ↑ ↑ ↑
3	地址: ANY	ANY	ANY	ANY	游戏	eth0, ptp11[11]	放行	↓ ↓ ↓ ↓
4	地址: ANY	ANY	ANY	ANY	IM	eth0, ptp11[11]	放行	↓ ↓ ↓ ↓
5	地址: ANY	ANY	ANY	udp	ANY	eth0, ptp11[11]	直接阻止	↑ ↑ ↑ ↑



注意

限制 UDP 后，有部分 P2P 软件会用不了，或者速度下降。

如果有遇到游戏无法玩的，应该是端口对象不全，可以补充缺少的游戏端口，也可以做一条游戏分流规则，然后要求客户运行小区客户端解决问题。