百为路由用户配置指南

V20221009

目录

1， 登录路由相关问题

1.1， 如何登录百为路由界面

1.2， 如何修改登录端口

1.3， 如何修改登录密码

1.4， 如何远程登录路由

1.4.1，直接用外网 IP+端口登录

1.4.2，ADSL/PPPoE 宽带如何远程访问路由

1.4.3，没有公网 IP 如何远程路由

1.4.4，有公网 IP 无法远程登录如何处理

2，无法登录路由如何通过命令行维护

2.1，使用命令行维护的准备工作

2.2，忘记登录密码怎么恢复

2.3，如何恢复路由出厂设置

2.4，忘记路由网口 IP 如何命令查看

2.5，忘记路由登录端口如何命令查看

2.6，路由能正常上网，仅忘记路由登录端口如何查看

3，路由许可认证相关问题

3.1，百为路由许可证认证是什么

3.2，许可证未认证的原因有哪些

3.3，北京电信通路由许可认证问题

3.4，监控摄像头占用许可证台数问题

4，网口配置相关问题

4.1，WAN 口配置相关

4.1.1，WAN 口配置基础讲解

4.1.2，DNS 配置的意义

4.1.3，线路中断检测

4.1.4，WAN 口带宽配置与智能流控

4.1.5，WAN 口线路已接，配置好后仍显示离线等问题排查

4.2，LAN 口配置相关

4.2.1，LAN 口基础讲解

4.2.2，修改不了网口 IP 信息

4.2.3，排查两个 LAN 口下的电脑无法互通

4.3，子接口的使用

4.3.1，一个内网口（Lan 口）如何设置成多个网关上网

4.3.2，一个外网口（WAN 口）实现多个外网接入

4.4，虚拟 IP 的使用

4.5，VLAN 接口的使用

4.5.1，扩展 WAN 口

4.5.2，作为 VLAN 网关提供上网

4.6，北京地区 WAN 口不使用 NAT 配置注意相关事项

5，多线路汇聚和分流规则讲解

5.1，百为路由是否有带宽叠加

5.2，怎么配置多线路负载（带宽叠加）

5.3，怎么理解分流规则的工作方式

5.4，分流模式讲解

5.5，举例同一运营商下的专线+宽带网吧的典型分流配置

5.6，举例同一运营商下的小带宽专线+宽带的网吧典型分流配置

5.7，举例电信专线+联通专线的网吧典型分流配置

5.8，举例同一个运营商的多条专线或者多条宽带的网吧典型分流配置

5.9，分流内网某个 IP 走一条外网线路出去

5.10，分流内网某个用户走一条外网线路出去

5.11，分流小区内网多个用户/部门走一条外网线路出去

5.12，分流目的端口走一条外网线路出去

5.13，分流外网某个 IP(目的 IP)走一条外网线路出去

5.14，分流外网某个 IP(目的 IP)+目的端口走一条外网线路出去

5.15，分流域名走指定线路出去（查 IP 走指定线路）

5.16，分流某个（协议）走指定线路出去

5.17，典型的分流规则错误讲解

6，限速功能讲解

6.1，什么是智能流控

6.2，策略带宽控制讲解

6.3，策略带宽控制---对指定 IP/IP 段限速

6.4，智能流控和策略带宽控制的关系说明

6.5，举例专线+宽带的网吧的策略带宽规则配置

6.6，举例多条专线或者多条宽带的网吧策略带宽规则配置

6.7，智能流控例外规则讲解

7，连接数相关功能讲解

7.1，需不需要更改默认的连接数控制规则

7.2，如何查看每个机器的连接数和链接跟踪表

7.3，为什么网络连接状态的连接数统计和链接跟踪表的统计不一样

7.4，接口状态显示的连接数的参考意义

7.5，运营商限制了家庭宽带的连接数能否通过路由解决

8，防火墙相关功能讲解

8.1，百为路由防火墙功能的用途

8.2，禁止内网某个 IP 或者用户上网

8.3，禁止外网某个 IP

8.4，禁止外网某个端口

8.5，禁止某个域名解析后的 IP

8.6，禁止某个协议

8.7，禁止外网某个 IP+端口

8.8，禁止两个内网口的网段互访

9，认证上网相关功能讲解

9.1，列举 4 种认证上网讲解说明

9.2，举例网吧用的动态密码认证怎么使用

9.3，举例小区 PPPoE 认证上网怎么使用

9.3.1，配置 PPPoE 服务并开启 PPPoE 认证

9.3.2，PPPoE 服务配合计费管理

9.3.3，PPPoE 透传使用场景以及使用方法

10，VPN 相关功能讲解

10.1，点对网 VPN 的用途

10.2，点对网 VPN 的配置

10.3，网对网 VPN 的用途

10.4，网对网 VPN 的配置

11，百为无线产品讲解

11.1，使用百为路由 AC 控制器管理百为无线 AP

11.1.1，百为路由独立网口连接无线 AP（推荐方案）

11.1.2，从现有交换机连接无线 AP（折衷方案）

11.1.3，配置无线 AP

11.2，如何切换百为无线 AP 工作模式

12，其他功能讲解

12.1，如何让一个域名解析为指定的 IP

12.2，如何禁止某个域名

12.3，如何定时重拨宽带

12.4，端口映射

12.5，如何判断有外网流量攻击

13，异常问题自检

13.1，游戏更新服务器更新速度慢自检步骤

13.2，端口映射无效问题自检步骤

13.3，ping 路由 LAN 口不丢包，ping 外网丢包问题自检

14，常见问题解答

14.1，首页显示工作速率 100M/全双工详解

14.2，网口显示的丢包是什么问题

14.3，系统日志提示有攻击包有没有问题

1，登录路由相关问题

1.1，如何登录百为路由界面

设备出厂的接口的 IP 地址，参考如下表：

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

（备注：BV200H、BV900V 型号至只有 5 个网口，则没有 eth5）

默认登录端口：2011

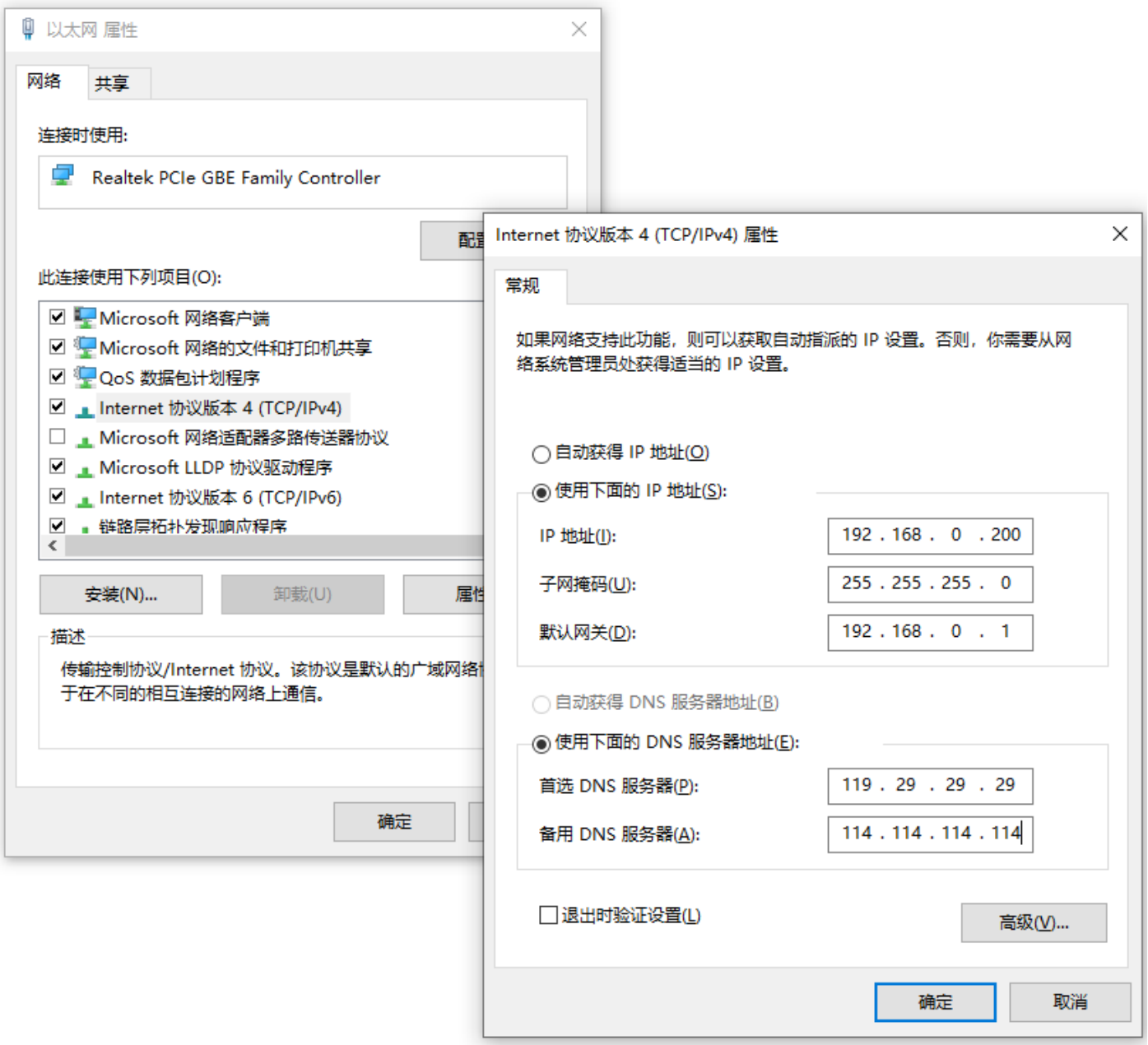
默认登录用户名密码均为：admin

举例说明通过 eth0 口登录路由，操作步骤如下：

（1）客户机通过网线连接到百为路由器的 eth0 口

（2）由于 eth0 口没有启用 DHCP 服务，需要客户机网卡配置与 eth0 同网段的 IP 地址，比如客户机网卡配置 IP 为：192.168.0.200　子网掩码配置为：255.255.255.0

（修改网卡属性---“Internet 协议版本 4（TCP/IPv4）”，填入 IP 地址、子网掩码、默认网关、DNS）



（3）在浏览器输入 http://192. 168.0.1:2011，登录到路由的 web 界面。输入用户名密码“admin”登录。

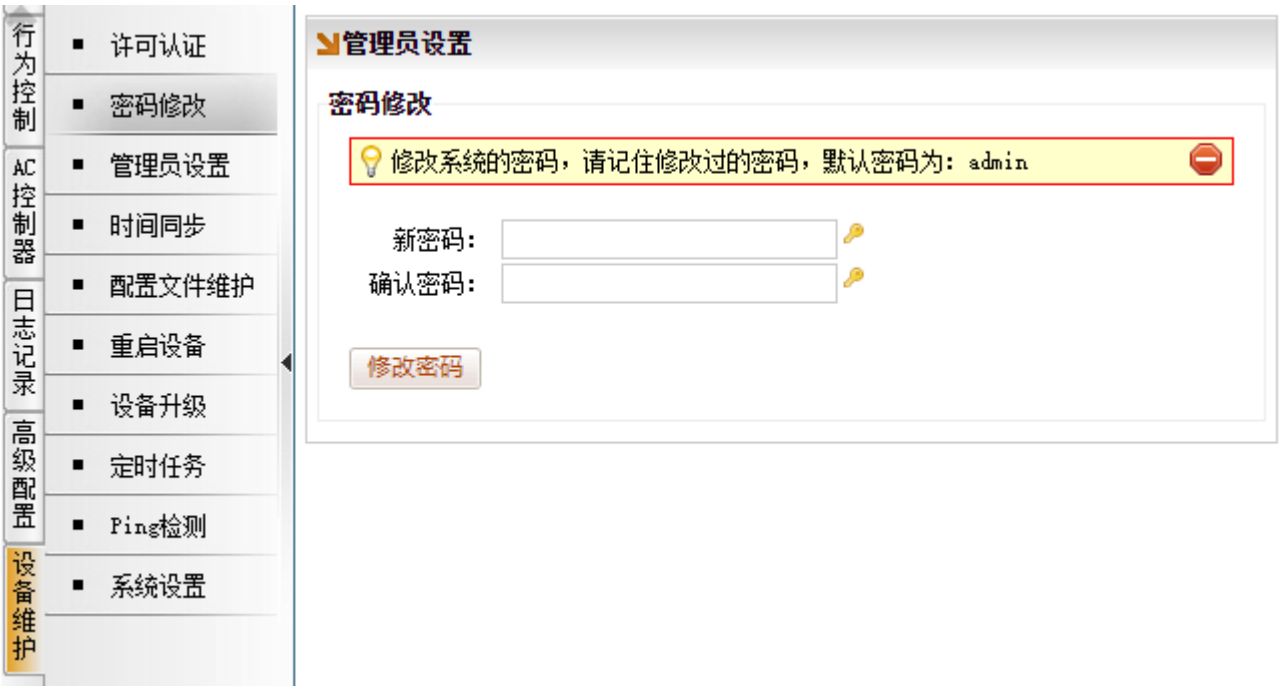
同理，客户机连接 eth1，eth2，eth3，eth4，eth5，只要配置与网口相同网段 IP，登录对应的网口 IP+端口号，同样可以登录路由界面

1.2，如何修改登录端口

[设备维护]→[系统设置]，WEB 服务端口，默认值 “2011” 。根据实际需求，修改后点击 “保存”，刷新浏览器即可用新端口登录路由。

1.3，如何修改登录密码

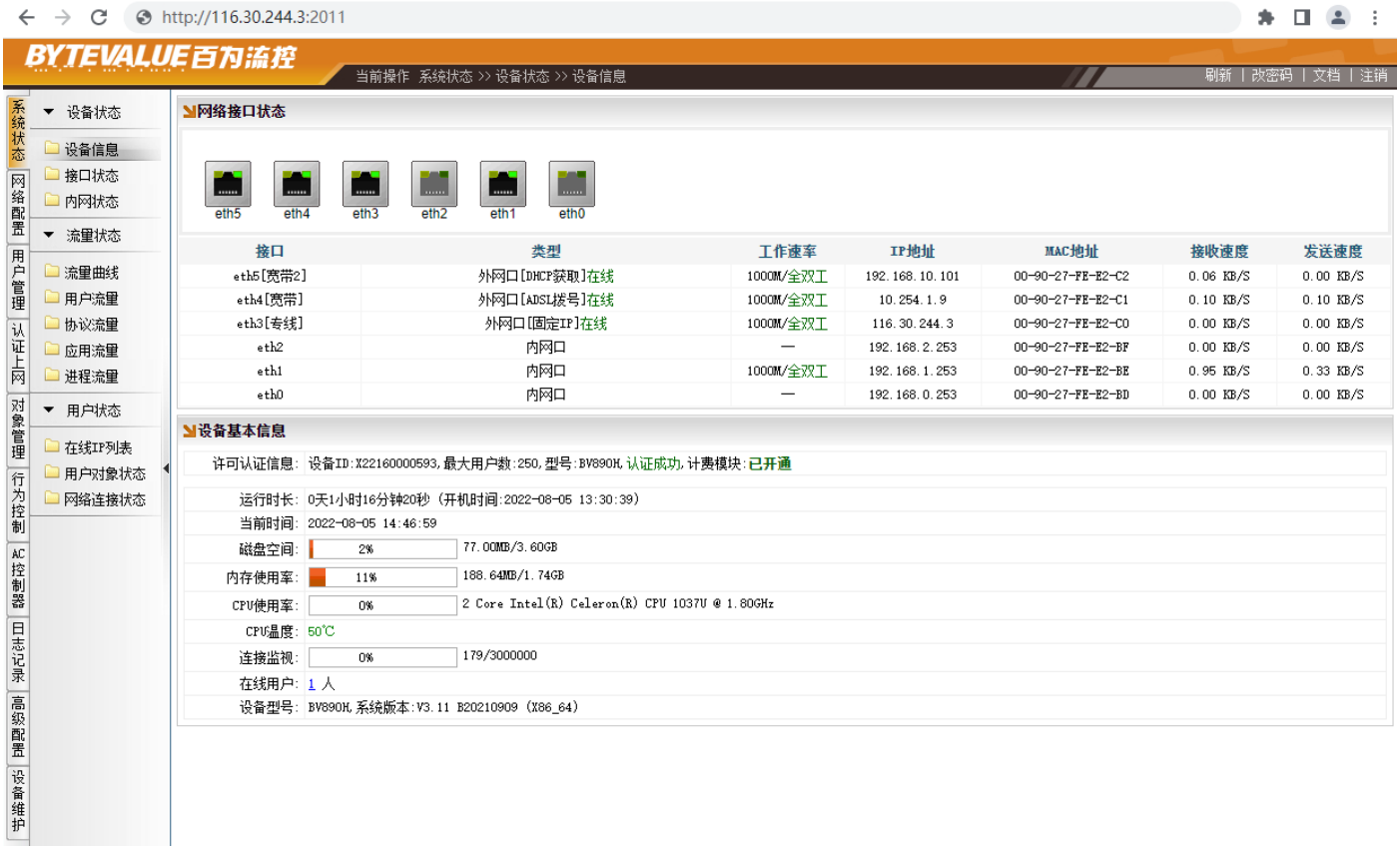
[设备维护]→[密码修改]，输入新密码后点击“修改密码”，刷新浏览器即可用新密码登录路由。



1.4，如何远程登录路由

1.4.1，直接用外网 IP+端口登录

比如专线固定 IP 是：116.30.244.3，路由登录端口是：2011。打开浏览器，地址栏输入 http://116.30.241.25:2011 即可访问到路由界面。



1.4.2，ADSL/PPPoE 宽带如何远程访问路由

首先需要确定 ADSL/PPPoE 宽带拨号后，运营商分配的 IP 地址是否为私网 IP。私网 IP 是属于保留地址，无法远程直接访问。保留地址主要有以下四类：

A 类	10.0.0.0 - 10.255.255.255
A 类	100.64.0.0 - 100.127.255.255
B 类	172.16.0.0 - 172.31.255.255
C 类	192.168.0.0 - 192.168.255.255

若运营商分配的 IP 地址不是以上四类 IP 地址，比如分配的 IP 是 116.30.246.6，就是属于公网 IP，公网 IP 是可以直接访问的，地址栏输入 http://116.30.246.6:2011 即可访问到路由界面。

由于 ADSL/PPPoE 宽带每次拨号，运营商分配的 IP 地址会变化，给访问造成困扰。需要引入域名的方式去访问，让每次拨号得到的 IP 地址，绑定到域名。这就是第三方的服务商提供的服务---动态域名解析服务。

百为路由合作的动态域名服务商有 “PubYun“、” 每步“、” DYN DNS”。用户可登录到动态域名服务商的官网，注册相关的账号、域名。再填入到百为路由的动态域名配置页面去。完成配置后，当宽带拨号，获得到新的 IP 地址，百为路由自动将 IP 地址上报给动态域名服务商，等待动态域名服务商把 IP 绑定到相关的域名，就可以用域名访问。

以下举例用 PubYun，注册了用户名：bytevalue2014 ；密码：123456 ；动态域名：bytevalue2014.3322.org。

[网络配置]→[接口配置]，选择外网口，比如 eth4---[高级配置]，启用动态域名，选择服务商为“公云 PubYUN”，填入动态域名：bytevalue2014.f3322.org；帐号：bytevalue2014；密码：123456。点击“保存”。

保存配置后，路由自动上报了宽带的 IP 给动态域名服务商。等待动态域名服务商绑定了域名，即可用域名+端口的方式访问。比如浏览器地址栏输入 http:// bytevalue2014.f3322.org:2011 访问路由界面。

注意：百为路由只负责上报当前宽带的 IP 地址给动态域名服务商。动态域名服务商绑定 IP 到域名的速度，以及解析的 IP 正确与否，取决于动态域名服务商。比如付费 VIP 的动态域名要比免费的动态域名刷新绑定的速度快。

1.4.3，没有公网 IP 如何远程路由

当 ADSL/PPPoE 宽带拨号，运营商分配的 IP 地址是私网 IP，无法远程直接访问。需要引入内网穿透的方式去访问，也是一种云服务器中转访问。

百为路由公司搭建有中转云服务器，仅提供访问路由界面用。配置前提需要路由已经有许可证认证成功，填入指定域名 www.szcloudnet.com 到百为路由，生成远程中转访问地址。操作如下：

[设备维护]→[系统设置]→[远程管理服务器]，填入域名 www.szcloudnet.com，点保存按钮后，会生成出路由链接地址，比如下图举例的 http://X20120000011.szcloudnet.com:20110 就是可以远程访问的路由登录地址。

注意：百为路由公司搭建的中转云服务器，配置生成的远程访问链接，仅提供访问路由界面使用。由于中转的关系，速度可能较慢，不适合用来导入或者导出大批量的用户数据。如果宽带拨号有分配公网 IP，强烈建议申请动态域名配合使用。对于宽带没分配公网 IP，对访问速度有要求，或者需要映射内网服务。建议购买第三方的内网穿透服务，比如 PubYUN、花生壳提供的解决方案。

1.4.4，有公网 IP 无法远程登录如何处理

考虑以下几种可能性：

（1）[设备维护]→[系统设置]，没有勾选“允许管理员通过外网 IP 远程登录”，请勾选，点击保存，再尝试用外网登录

（2）[设备维护]→[系统设置]， 已勾选“允许管理员通过外网 IP 远程登录”，但配置了允许 IP 范围，比如错误的配置了 IP 地址：172.16.16.0，子网掩码：255.255.255.0。这就表示从外面访问进来的源地址必须是 172.16.16.xxx 网段的才允许登录。检查是否错误配置，如果允许外网任何地方都可以访问路由，点击右边的蓝色字体“允许所有 IP”，生成出 0.0.0.0，再点击下方的“保存”，再尝试外网登录

（3）配置端口映射里包含了路由的 WEB 端口，比如路由 WEB 服务端口是 2011，而端口映射里，把 2011 映射到内网某个主机；或者是映射的端口范围，包含了 2011，导致无法外网远程登录。检查是否错误配置了端口映射，或者修改路由的 WEB 服务端口不与端口映射范围冲突。

下图举例了端口映射规则与 WEB 服务端口（2011）冲突的示例。

规则 1：“外网端口”：2011 映射转发给 192.168.1.253 主机的 2111 端口；规则 2：外网端口范围”：2000-3000 映射转发给 192.168.1.100 主机的 2000-3000 端口。

（4）启用了 DMZ 功能，并添加了 DMZ 主机，比如添加了 DMZ 主机 192.168.1.253 关联到外网线路 eth3。因此访问 eth3 的外网 IP 的任何端口，就相当于访问 DMZ 主机了，删除规则，外网即可正常访问。

2，无法登录路由如何通过命令行维护

2.1，使用命令行维护的准备工作

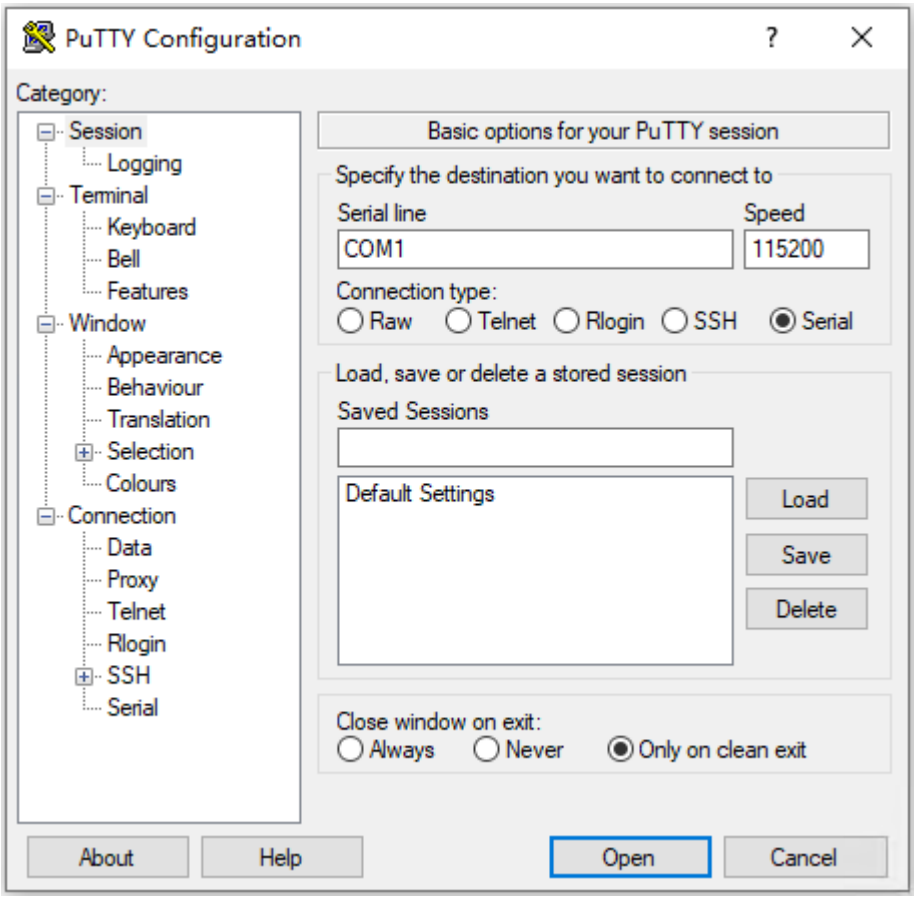
说明：软路由、BV600、BV800、BV890、BV1000、BV1200、BV1800，属于 X86 架构，通常 X86 架构的硬件，使用 VGA 接口外接显示器，通过 USB 外接键盘维护操作。保证接好键盘后，按键盘回车后，屏幕能显示井号 **“#”** 的提示符，表示连接成功，即可使用命令行维护。

BV300、BV390、BV300H、BV390H、BV900W、BV990W、V3000、V3900、V5000、V5900 型号的硬件，属于嵌入式架构。由于此类硬件没有集成显示输出，没有 VGA 接口，需要通过串口维护。(产品出厂时配有串口线一根，规格为 RJ45 转 RS23 console 调试线，也称之为思科串口线)

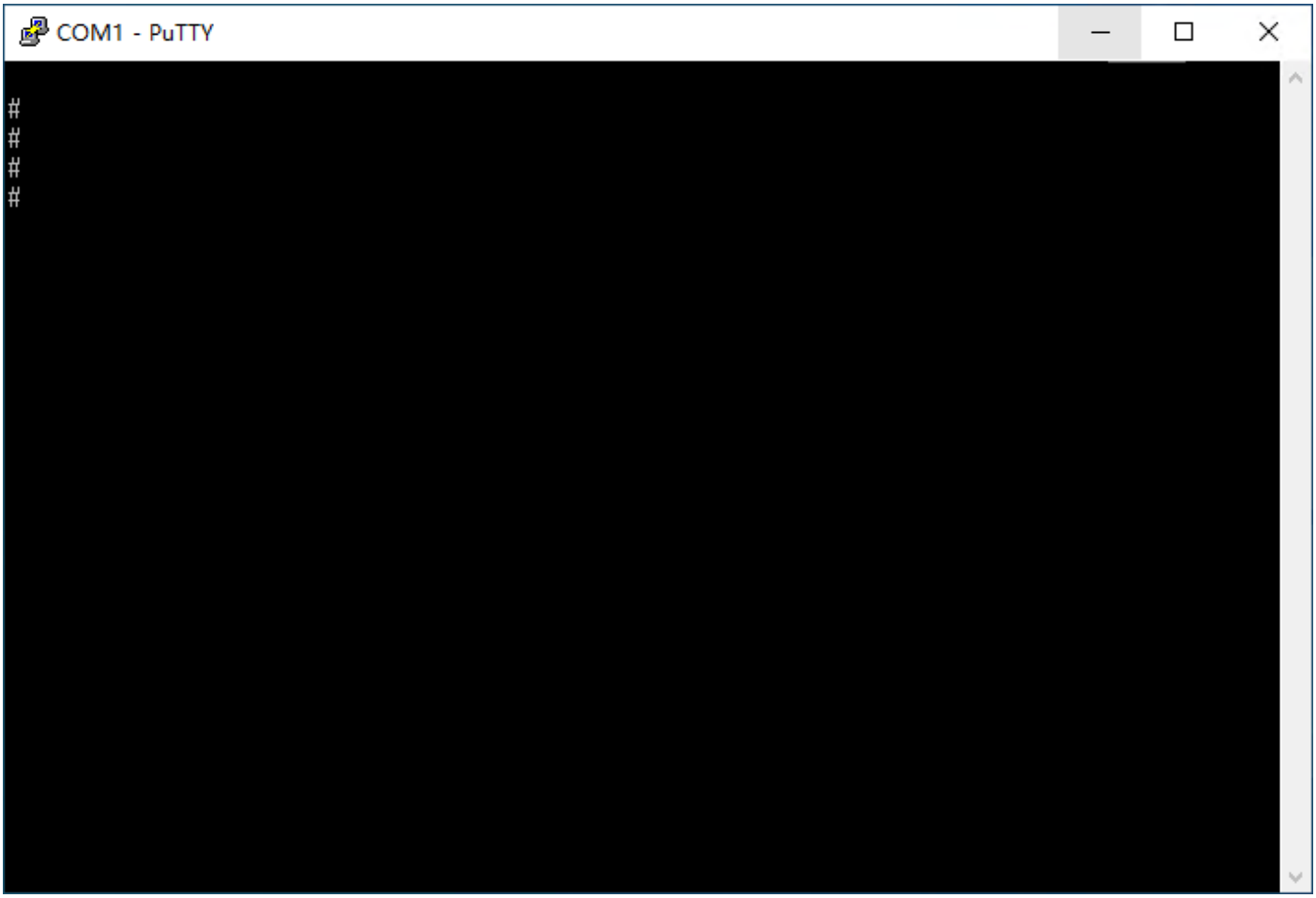
准备好 console 调试线，RJ45 水晶头一端连接路由的“CONSOLE 口”，另一头连接台式机的 D 型九针 COM 口。如下图所示

（备注：多数家用电脑，主板挡板位置已经不提供 COM 口，需要从主板的针脚接出来，而服务器主板多数挡板位置有提供 COM 口。如果客户机，服务器均没有 COM 口，可购置 USB 转 console 线来维护。）

连接后，在插有串口的电脑上操作，使用超级终端，SecureCRT、或者 Putty，连接串口维护。以下演示用 Putty 登录，选择 Serial，填写串口 COM1，波特率 115200。



点击 Open 连接串口，按回车键会出来井号“#”提示符，表示连接成功，即可使用命令行维护。



（在填写的波特率“115200”正确的前提下，如果按回车没有反应，没有出现井号“#”提示符，可能连接的 COM 口不是 COM1，尝试填写 COM2 连接。COM 口的名称，序号，可通过电脑属性---“设备管理器---端口”查看。）

2.2，忘记登录密码怎么恢复

命令：**rpasswd**

输入“rpasswd”，回车，会生成出随机校验码，跟着输入一遍校验码，回车，确认修改。成功修改后，密码恢复为 admin。

比如下图，输入命令后生成出来的随机校验码是 9256 ，跟着输入一遍 9256 ，回车。当提示出“Reset Password Success”，说明恢复成功。（注意，示例中演示随机验证码是 9256，实际操作中需要根据生成出来的随机码跟着填写）

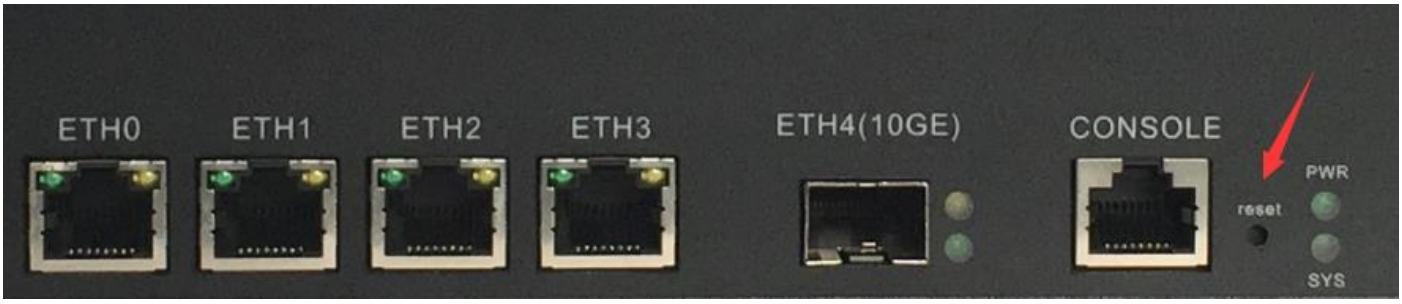
```
#
# rpasswd
Verify Code: 9256
Please enter validation code: 9256
Verification Success.
Password for 'admin' changed
Reset Password Success.
#
```

2.3，如何恢复路由出厂设置

命令：**resetfactory**

请谨慎操作，确定没有数据需要保留的，才操作恢复出厂。命令成功会自动重启路由，并处于出厂状态。

备注：百为原厂硬件，型号分别是 BV300、BV390、BV300H、BV390H、BV900W、V3000、V3900、V5000、V5900。可在通电的前提下，触压内凹的 reset 按钮，持续 8 秒后再松开，将自动执行恢复出厂设置动作



2.4，忘记路由网口 IP 如何命令查看

命令：**ifconfig**

ifconfig 是查看所有网口信息的命令，只查看某个网口可加网口名查看。

比如 **ifconfig eth0** ，表示查看 eth0 网口的信息，同理 **ifconfig eth1**，是查看 eth1 网口.....

```
# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:90:27:FE:E2:BD
          inet addr:192.168.0.253  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:20000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:17 Memory:f7d00000-f7d20000

#
# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:90:27:FE:E2:BE
          inet addr:192.168.1.253  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:4056060 errors:0 dropped:59149 overruns:0 frame:0
          TX packets:249028 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:20000
          RX bytes:402171109 (383.5 MiB)  TX bytes:23068768 (22.0 MiB)
          Interrupt:18 Memory:f7c00000-f7c20000
```

从上图命令的结果可以看出，eth0 网口的 IP 是 192.168.0.253；eth1 网口的 IP 是 192.168.1.253。

2.5，忘记路由登录端口如何命令查看

输入命令“netstat -na | grep LISTEN”

（注意 netstat、grep 后面有空格符，na 后面是竖号符 | ，以及 LISTEN 要大写）。

输入该命令后回车，可看到类似如下信息，

```
# netstat -na | grep LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8088            0.0.0.0:*               LISTEN
netstat: /proc/net/tcp6: No such file or directory
netstat: /proc/net/udp6: No such file or directory
netstat: /proc/net/raw6: No such file or directory
unix  2      [ ACC ]     STREAM     LISTENING         56 /tmp/runproc.sock
unix  2      [ ACC ]     STREAM     LISTENING         85 /tmp/bvdb.sock
unix  2      [ ACC ]     STREAM     LISTENING       1879 /tmp/shttpd.ssl.sock
unix  2      [ ACC ]     STREAM     LISTENING       1882 /tmp/swmonitor.sock
unix  2      [ ACC ]     STREAM     LISTENING       1885 /tmp/bvatup.sock
unix  2      [ ACC ]     STREAM     LISTENING       1890 /tmp/shttpd.sock
unix  2      [ ACC ]     STREAM     LISTENING        109 /tmp/fsm.sock
unix  2      [ ACC ]     STREAM     LISTENING       1722 /tmp/timerun.sock
unix  2      [ ACC ]     STREAM     LISTENING       1992 /tmp/bvacauto.sock
unix  2      [ ACC ]     STREAM     LISTENING       1757 /tmp/goahead.sock
unix  2      [ ACC ]     STREAM     LISTENING       2027 /tmp/acserver.sock
#
```

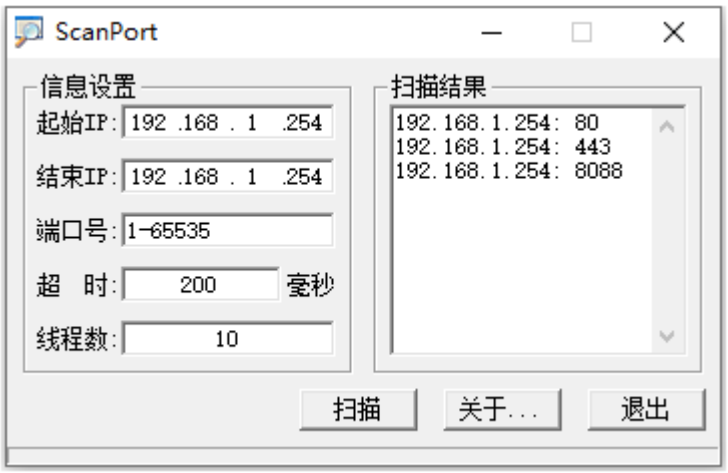
从上图得知，该路由器的正在监听的 TCP 服务端口分别有 80 端口，443 端口，8088 端口，已知 80 端口，443 端口，是路由内网 web 服务所用端口，由此所查到的端口是“8088”可能是路由

的登录端口，可尝试使用该端口登录。

2.6，路由能正常上网，仅忘记路由登录端口如何查看

可借助端口扫描工具扫描路由监听的 TCP 服务端口

比如已知路由 LAN 口 IP 是 192.168.1.254，使用端口扫描工具，扫描起始 IP，结束 IP 为：192.168.1.254，端口号为：1-65535。点击“扫描”，等待扫描结束后，可从扫描结果得知监听的端口号分别有 80 端口，443 端口，8088 端口。已知 80 端口，443 端口，是路由内网用于 Portal 认证的 web 端口（并非用于路由界面登录端口），由此所查到的端口是“8088”可能是路由的登录端口，可尝试使用该端口登录。



3，路由许可认证相关问题

3.1，百为路由许可证认证是什么

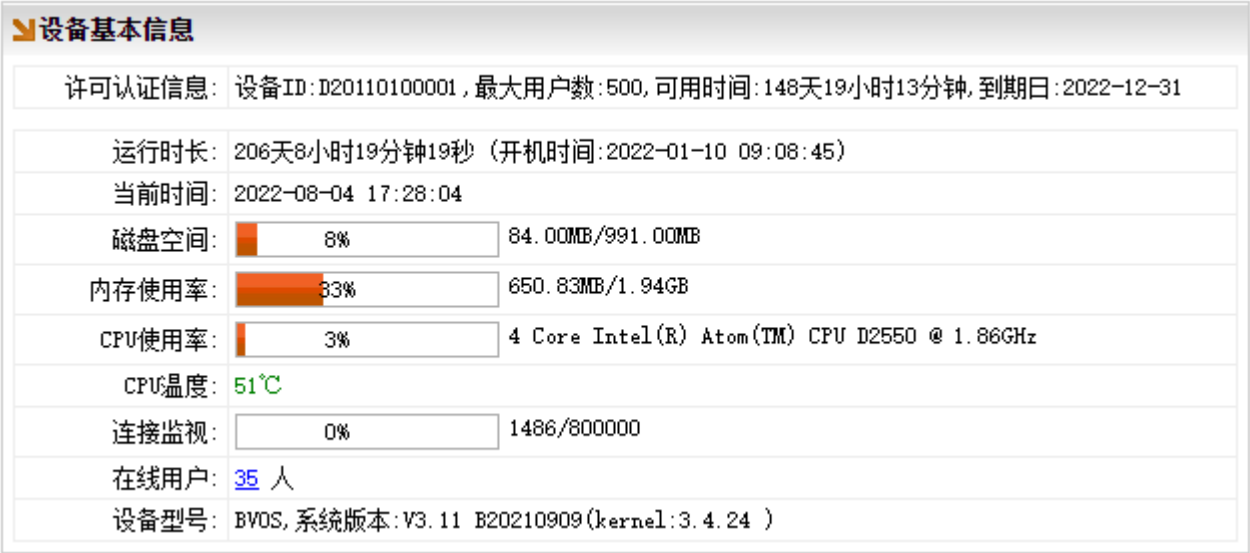
答：百为路由是付费路由产品。需要有许可证联网校验合法性，认证成功才享有智能流控，多线路等功能，没认证仅提供一个 WAN 口联网。

许可证分有：原厂硬件内置许可证和软路由许可证，原厂硬件内置许可证不需要用户申请；软路由许可证是由 ID 和 KEY 组成，需要自行申请，也可以由代理商创建。用户凭借许可证的 ID 进行续费，获得使用时长。

软路由许可证自行申请，可在百为官网首页右上角点 “免费试用“ 进入，或者浏览器输入 http://member.bytevalue.com/index.php?ctl=member/apply-enduser 登录申请页面自行申请。

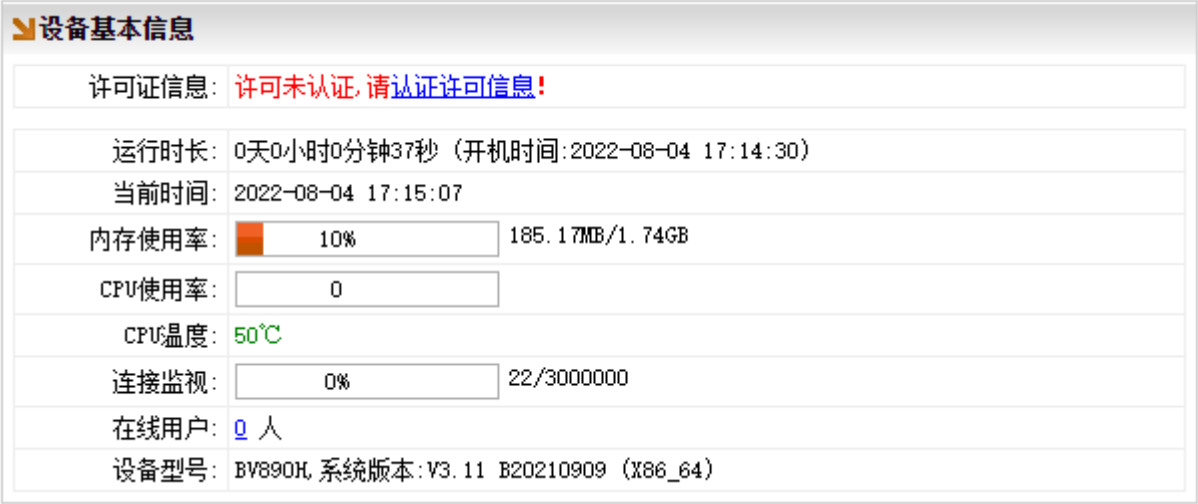
注意：新创建软路由的许可证默认提供 30 天试用时间，试用到期后，凭借许可证 ID 联系代理商或者百为的商务进行续费。(如果许可证 ID 不属于代理商管理平台下，联系百为工程师指派 ID 所属后，代理商即可续费)

通过路由首页，可看到当前的许可状态，许可证通过认证如下图所示



3.2，许可证未认证的原因有哪些

许可证未认证如下图所示



说明：许可认证需要联网校验。如果路由本身没有联网，也会提示许可未认证。许可未认证并不会导致 WAN 口不通的问题。

当首页提示许可证未认证，点击进入授权许可中心设置页面，[设备维护]→[许可认证]，查看具体原因。（原厂硬件内置许可证只显示设备 ID；软路由许可证需要填入设备 ID 和设备 KEY。）

硬件类型	认证状态	处理方法
原厂硬件	设备未激活	点击 “激活设备“ 超链接，或者浏览器输入 http://member.bytevalue.com/?ctl=member/active 登录激活页面自助激活。成功激活后可获取 30 天使用时长。
软路由	设备 Key 与设备 ID 不匹配	填入的设备 ID 或者设备 KEY 不正确，检查是否有空格，或者是没区分英文大小造成。重新填入正确的设备 ID 和设备 KEY 后，先点 “保存“ ，再点 ” 重新认证 “。
软路由	认证被拒绝	存在反复试用新申请的 ID 的可能或者 ID 在别的地方用过需要解绑。需要联系百为工程师处理。
原厂硬件 / 软路由	设备许可已经过	授权许可证过期，凭 ID 联系代理商或者百为商务续费

	期	延期。
原厂硬件 / 软路由	等待认证	等待认证是连接到百为认证服务器的过程。如果一直显示等待认证，可能是当前线路无法与百为认证服务器联通，或者是第一个 WAN 口没有网络造成。如果有多条线路，可尝试指定别的认证接口是否解决，[设备维护]→[许可认证]→[指定认证外网接口]→[认证接口]，选择其他 WAN 口，点“保存“，再点” 重新认证“。（北京电信通没配置地址转换也会显示等待认证）

3.3，北京电信通路由许可认证问题

说明：由于百为路由的授权许可证是通过 WAN 口联网校验。北京电信通是将公网 IP 配置于 LAN 口，WAN 口是使用保留地址对接电信通机房，取消 NAT，通过路由转发的形式上网。需要在百为路由配置地址转换，才能许可证认证成功。

举例当前电信通的网吧，WAN 口为 124.192.222.111；LAN 口为 172.30.55.34

接口	类型	工作速率	IP地址	MAC地址	接收速度	发送速度
eth5[电信通]	外网口[固定IP]在线	1000M/全双工	172.30.55.34	00-90-28-00-3B-AA	99.38 KB/S	1.98 MB/S
eth4	内网口	—	192.168.4.1	00-90-28-00-3B-A9	0.00 KB/S	0.00 KB/S
eth3	内网口	—	192.168.3.1	00-90-28-00-3B-A8	0.00 KB/S	0.00 KB/S
eth2	内网口	—	192.168.2.1	00-90-28-00-3B-A7	0.00 KB/S	0.00 KB/S
eth1	内网口	—	192.168.1.1	00-90-28-00-3B-A6	0.00 KB/S	0.00 KB/S
eth0[LAN]	内网口	1000M/全双工	124.192.222.111	00-A5-00-91-85-00	1.98 MB/S	82.54 KB/S

需要配置地址转换：

[高级配置]→[地址转换]→[源地址转换]，添加转换规则

源地址 IP	172.30.55.34
源地址掩码	255.255.255.255
目的地址	0.0.0.0

目的地址掩码	0.0.0.0
替换源地址为	124.192.222.111

3.4，监控摄像头占用许可证台数问题

说明：网吧里如果有不需要连外网的设备，比如监控摄像头，可以通过配置“特殊 IP”给排除掉。排除后不影响局域网摄像头的通讯。通常监控摄像头是与录像机通讯，录像机需要上网对外提供服务。注意配置特殊 IP 不要包含录像机的 IP。

[设备维护]→[许可认证]→[特殊 IP]，填入监控摄像头的 IP，IP 段，点保存。

对象管理
行为控制
AC控制器
日志记录
高级配置
设备维护
许可认证
密码修改
管理员设置
时间同步
配置文件维护
重启设备
设备升级
定时任务
Ping检测
系统设置
授权许可中心设置
认证配置
特殊IP
特殊IP
特殊IP不计入认证许可终端数，同时也不能连接外网.
开始IP
结束IP
IP(段)1
192.168.1.200
192.168.1.220
IP(段)2
IP(段)3
IP(段)4
IP(段)5
IP(段)6
IP(段)7
IP(段)8
保存

4，网口配置相关问题

4.1，WAN 口配置相关

4.1.1，WAN 口配置基础讲解

[网络配置]→[接口配置]，选择要配置的网口，修改接口类型为“WAN(外网口)”

选择宽带运营商、上网方式并配置

ADSL/PPPOE	填入宽带账号和密码	通常接的是光猫，并且光猫为桥接模式。百为路由拨号到运营商完成用户名密码校验，运营商分配 IP 地址上网。
固定 IP	填入运营商提供的 IP、掩码、网关及 DNS	通常接的是专线，百为路由配置运营商提供的 IP 信息直接上网。 也可以接的是路由模式的光猫，百为路由配置与光猫内同网段的 IP 直接上网。
DHCP	DHCP 形式自动获取 IP	通常接的是光猫，并且光猫为路由模式，开启了 DHCP 服务分配内网 IP 地址，百为路由直接用 DHCP 获取的 IP 地址的方式上网

配置如下图所示

系统状态
网络配置
用户管理
认证上网
对象管理
行为控制
AC控制器
日志记录
高级配置

- 接口配置
- 分流规则
- 智能带宽控制
- 策略带宽控制
- 连接数控制
- 内网防护
- DHCP服务
- 静态路由

网络接口配置 导出账号

eth0
eth1
eth2
eth3[专线]
eth4[宽带]
eth5[宽带2]

基本配置 | 高级配置 | VLAN配置 | 子接口 | VPN接口 | 虚拟IP | BPN接口

基本信息

当前接口：eth3，别名：专线
是否启用：◉启用 ○禁用

接口类型：○LAN(内网口) ◉WAN(外网口) ○BR(桥接口)

外网口配置 点击配置动态域名

宽带运营商：◉中国电信 ○中国联通 ○中国移动 ○长城宽带 ○其他
上网方式：○ ADSL/PPPOE ◉ 固定IP ○ DHCP
IP地址：116.30.244.3　子网掩码：255.255.255.252
默认网关：116.30.244.1
DNS 1：119.29.29.29　DNS 2：114.114.114.114
线路中断检测：◉ 启用 ○ 禁用

网络接口配置 导出账号

eth0
eth1
eth2
eth3[专线]
eth4[宽带]
eth5[宽带2]

基本配置 | 高级配置 | VLAN配置 | 子接口 | VPN接口 | 虚拟IP | BPN接口

基本信息

当前接口：eth4，别名：宽带
是否启用：◉启用 ○禁用

接口类型：○LAN(内网口) ◉WAN(外网口) ○BR(桥接口)

外网口配置 点击配置动态域名

宽带运营商：◉中国电信 ○中国联通 ○中国移动 ○长城宽带 ○其他
上网方式：◉ ADSL/PPPOE ○ 固定IP ○ DHCP
用户名：075500000101@163.gd　批量导入ADSL拨号账号
密码：••••••••
密码确认：••••••••
指定DNS：如果不指定请填写为 0.0.0.0，将会自动使用ISP的默认DNS
DNS 1：0.0.0.0　DNS 2：0.0.0.0
线路中断检测：◉ 启用 ○ 禁用

网络接口配置 导出账号

eth0
eth1
eth2
eth3[专线]
eth4[宽带]
eth5[宽带2]

基本配置 | 高级配置 | VLAN配置 | 子接口 | VPN接口 | 虚拟IP | BPN接口

基本信息

当前接口：eth5，别名：宽带2
是否启用：◉启用 ○禁用

接口类型：○LAN(内网口) ◉WAN(外网口) ○BR(桥接口)

外网口配置 点击配置动态域名

宽带运营商：◉中国电信 ○中国联通 ○中国移动 ○长城宽带 ○其他
上网方式：○ ADSL/PPPOE ○ 固定IP ◉ DHCP
指定DNS：如果不指定请填写为 0.0.0.0，将会自动使用ISP的默认DNS
DNS 1：0.0.0.0　DNS 2：0.0.0.0
线路中断检测：◉ 启用 ○ 禁用
！请填入两个ping值稳定的公网服务器IP作为检测IP，如果未填写两个有效IP，则使用ISP对象的ping检测IP
PING检测IP 1：0.0.0.0　PING检测IP 2：0.0.0.0

带宽配置

上行带宽：5000 KB
下行带宽：50000 KB
☑ 启用智能流控

参考值
ADSL：20M 50M 100M 200M 300M 500M 1G
光纤：10M 20M 50M 100M 200M 500M 1G

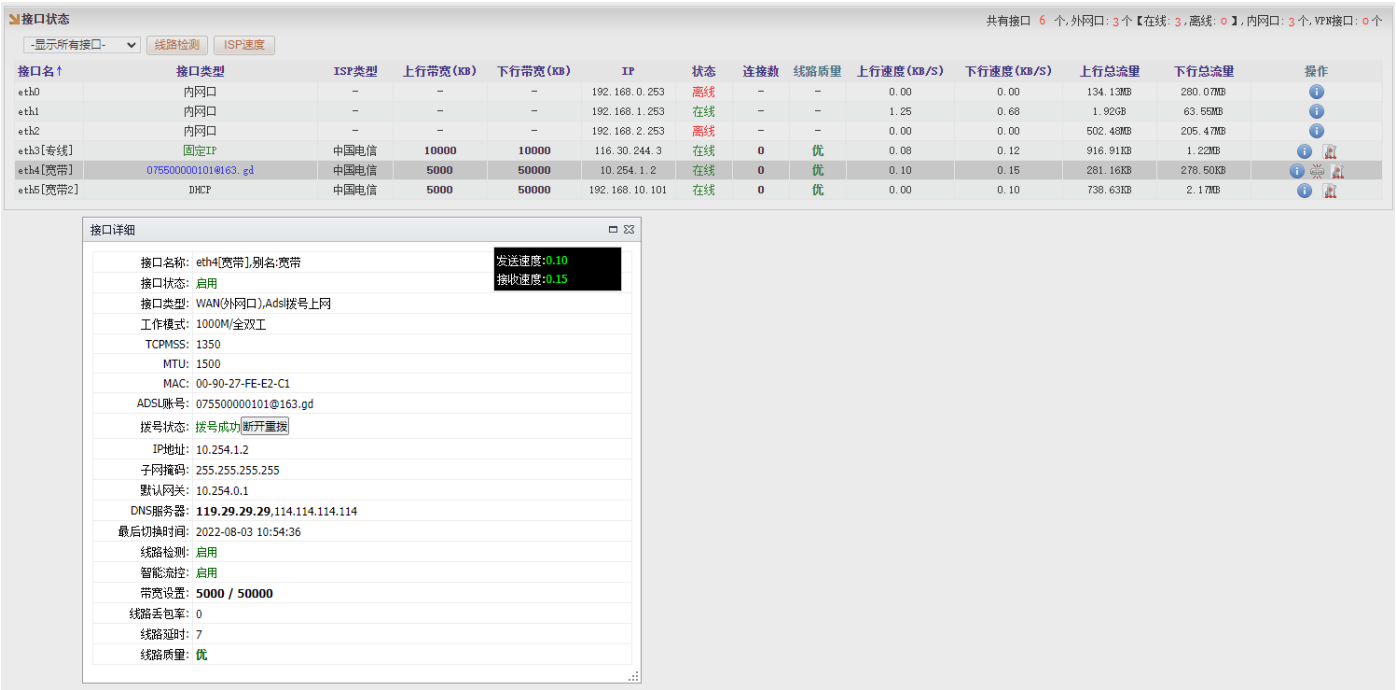
保存　批量保存

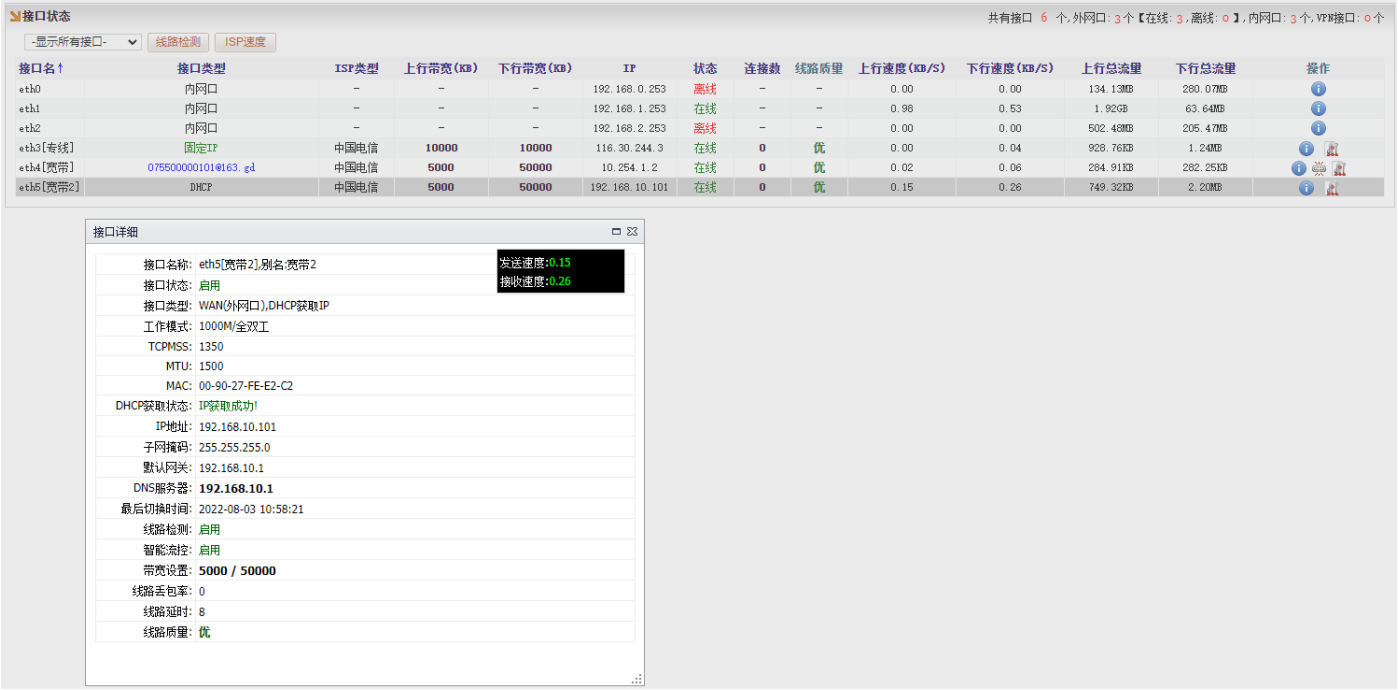
配置正确，线路正常，可在[系统状态]→[接口状态]，看到 WAN 口状态显示“在线”

4.1.2，DNS 配置的意义

说明：ADSL/PPPoE 和 DHCP 通常是可以得到运营商或者上级设备分配到 IP 地址，以及 DNS 的。所以，对于上网方式为 ADSL/PPPoE 和 DHCP 的 DNS 1, DNS 2 的配置项，可以默认用 0.0.0.0 配置，意味着使用运营商分配的 DNS。固定 IP 则需要手工填入能解析的 DNS 服务器地址。

通过[系统状态]→[接口状态]，查看线路的详细---“DNS 服务器”





建议：如果明确某个 DNS 服务器解析效果好的。可根据实际需求自定义填写 DNS 1，DNS 2 。特别是光猫作为路由模式接到百为路由，DHCP 仅分配光猫的网关 IP 作为 DNS 的时候，更推荐自定义填写 DNS 1，DNS 2。

4.1.3，线路中断检测

说明：线路中断检测，是使用 Ping 检测。ping 两个 IP 地址作为检测依据。以优，良，差三个等级提示线路质量。

优	线路质量正常，没有丢包，延迟低
良	线路质量一般，偶有丢包，或者延迟稍高。但需要用户检测线路
差	线路质量差，丢包率高，或者延迟大。需要用户检测线路。路由采取措施，拨号尝试重拨；DHCP 尝试重新获取 IP；固定 IP 离线处理。离线的线路，不参与负载。

PING 检测 IP，可以默认用 0.0.0.0 配置，意味着使用百为路由内置的检测 IP 作为检测依据百为路由内置的检测 IP 为：

114.114.114.114	114 中国公共 DNS IP
119.29.29.29	腾讯公共 DNS IP
223.5.5.5	阿里公共 DNS IP
180.76.76.76	百度公共 DNS IP

如需自定义 PING 检测 IP，请填入两个 ping 值稳定的公网服务器 IP 作为检测 IP。比如填入当地运营商能 ping 通的 DNS 作为 ping 检测 IP。

建议：多线路环境，建议启用线路中断检测。特别是有专线-固定 IP 的线路，需要判断线路是否离线了，才能实现多线路切换。

注意：有些地区是使用专用网，比如社保专用网，医务网，属于内部网络的，没法 ping 通外界，无法进行检测，需要禁用线路中断检测；个别专线，如果运营商禁 ping ，也不能启用线路检测。

4.1.4，WAN 口带宽配置与智能流控

说明：填入线路上行、下行带宽，是用于智能限速。当流量开销超过线路上行、下行带宽的阈值，自动限速，保证线路延迟。

备注：百为路由的流量单位是 KB，运营商的流量单位是 bit。以电信签约 100Mbps 为例，换算为 KB，理论值是 12500KB，去掉一些损耗，以及数据包一些头部信息后，保守配置为 10000KB。

建议：单机连接线路测试实测多次取平均值为准，可使用腾讯电脑管家测速

4.1.5，WAN 口线路已接，配置好后仍显示离线等问题排查

说明：线路离线的原因非常多，必须先基础性的检查---单机测试。找电脑不经过百为路由，直连外网，测试是否能 ping 通外网，比如 ping 114.114.114.114，开网页是否正常。

如果专线，宽带，单机实测 ping 外网不能 ping 通，但上网正常，说明线路是不支持 ping 外网，需要路由关闭线路中断检测。

如果专线，宽带，单机实测 ping 外网能 ping 通，并且上网正常，以下列举常见的几种问题，以及尝试性设置：

- 专线固定 IP 规律性离线又上线

  答：运营商机房的设备可能存在 ARP 老化时间和百为路由 WAN 口的 ARP 老化时间不兼容。尝试在[网络配置]→[接口配置]，选择该的网口，点击[高级配置]，勾选“自动绑定网关 MAC “，观察问题是否能解决。

- DHCP 获取光猫分配的地址后一直反复离线在线；插上光猫获取地址就没网络了；插上光猫获取地址导致路由界面登录不了也断网了。

  答：可能光猫分配的 IP 地址和 LAN 口网段冲突了。比如光猫分配的 IP 地址是“192.168.1.2 “，刚好百为路由其中一个 LAN 口 IP 是 192.168.1.1，这就网段冲突了。必须保证 LAN 口和 WAN 口不能同网段。这通常建议修改光猫网段为别的网段避免冲突，有条件最好联系运营商工作人员，将光猫修改为桥接模式，拨号的动作由百为路由承担，不使用 dhcp 获取。

- 专线固定 IP 或者 ADSL/PPPoE 宽带拨号一直离线

  答：可能路由网口的 MAC 被运营商视为非法，或者黑名单，或者有冲突。尝试在[网络配置]→[接口配置]，选择该线路的网口，点击[高级配置]，勾选 “启用自定义 MAC 地址“ ，并点击[随机 MAC] 按钮，生成出别的 MAC 后保存。观察问题是否能解决。

4.2，LAN 口配置相关

4.2.1，LAN 口基础讲解

说明：百为路由无论是原厂硬件还是软路由，所有 LAN 口都属于独立的网段，不提供合并 LAN 口为一个网段的的功能。不同 LAN 口之间的网段支持互访（路由转发形式实现）。

4.2.2，修改不了网口 IP 信息

修改 IP 地址、掩码的时候，提示“IP 地址与其他网络接口不能在一个网段!”

说明：由于 LAN 口都设计为独立的，要求每个网口之间的网段不能重叠。

百为路由所有网口的 IP 地址默认如下：

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

范例一：提示 IP 信息无法修改

尝试修改 eth0 的 IP 为“192.168.1.254”，掩码为“255.255.255.0”，提示无法修改。原因是 eth1 默认值为 192.168.1.1，掩码为“255.255.255.0”，两个网口都是 1 网段重复，导致冲突。

确认需要 eth0 网口配置为 192.168.1.254。修改之前，需要把 eth1 的网口，修改为别的网段，比如先修改 eth1 的 IP 为“172.16.1.1”掩码为“255.255.255.0”。修改后才可以将 eth0 修改为 192.168.1.254。 同理，修改的网口 IP 也不能和 eth2、eth3、eth4、eth5 网口的网段冲突。

注意：配置 LAN 口 IP 信息，也需要避免与 WAN 口的网段冲突。

范例二：提示掩码无法修改

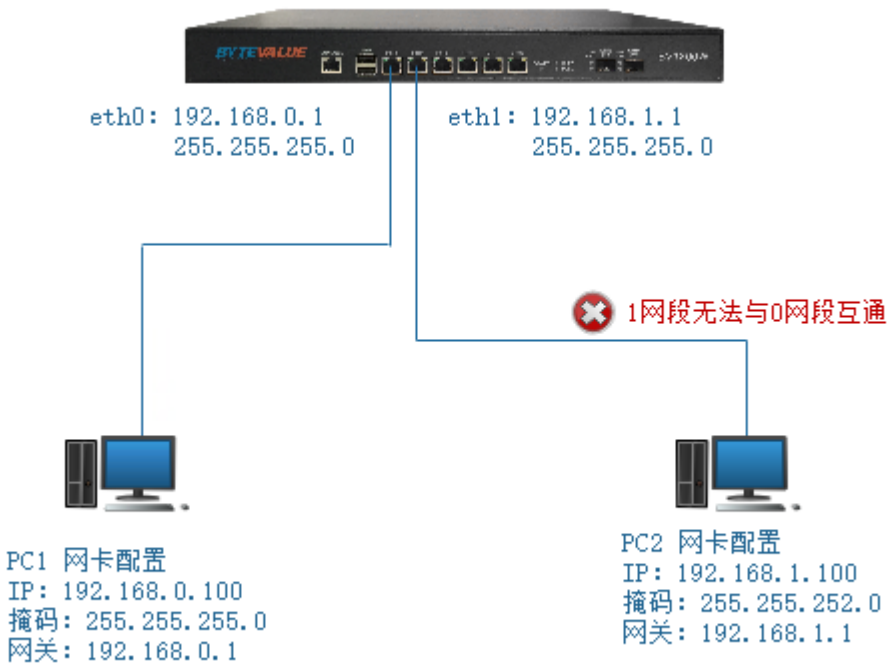
尝试修改 eth0 的 IP 为“192.168.0.1”，掩码为“255.255.252.0”，提示无法修改。原因是 eth0 修改掩码为 255.255.252.0 的话，放大了网段的范围，表示 192.168.0.1---192.168.3.255 的 IP 范围都隶属于 eth0 网口，与 eth1、eth2、eth3 的网口默认值重复，导致冲突

确认需要 eth0 网口配置为 IP 为“192.168.0.1”，掩码为“255.255.252.0”。修改之前，需要把 eth1、eth2、eth3，修改为别的网段的 IP，比如 172.16.1.1、172.16.2.1、172.16.3.1 ……，修改后才可以将 eth0 口的掩码放大。

4.2.3，排查两个 LAN 口下的电脑无法互通

如下图所示：PC1 通过 eth0 网上，配置 0 网段 IP 信息；PC2 通过 eth1 网上，配置 1 网段 IP 信息，具体配置信息见图中标识。在客户机关闭防火墙的前提下，PC1 无法和 PC2 互通。

由于百为路由 LAN 口之间的网段支持互访（路由转发形式实现），该实例中互访不了的主要原因是 PC2 的掩码用了 255.255.252.0，导致访问 0 网段的数据，没有通过 192.168.1.1 转发过去。修改正确的掩码即可解决问题。



4.3，子接口的使用

4.3.1，一个内网口（Lan 口）如何设置成多个网关上网

举例使用场景：网吧使用百为路由，eth0 作为 LAN 口接入到主交换机。由于布线的关系，其他交换机都是通过主交换机级联。网吧的客户机，服务器，监控，属于一个广播域下。为了区分管理，希望网吧客户机使用 192.168.0.1---192.168.0.254；监控设备使用 192.168.10.1---192.168.10.254，掩码均为 255.255.255.0。

[网络配置]→[接口配置]，比如选择 eth0 口，“子接口”一栏，添加子接口 ID（填入数字范围是 1~4096 任意数字），为了便于标识，比如填入数值 10，点击“确定”。

完成子接口 ID 的添加后，左边栏会生成出“eth0-10”的子接口。选择 eth0-10 的子接口，配置接口类型：LAN（内网口），填入 IP 信息，保存后，重启路由。

（注意：添加接口，删除接口的动作，必须要重启，否则会导致整个接口配置功能无效）

重启后，监控设备只要配置 10 网段的 IP，掩码，网关等信息，即可正常上网。

4.3.2，一个外网口（WAN 口）实现多个外网接入

举例使用场景一：接入的宽带能同时拨号多个账号、或者能同时拨号一个账号 N 次。

[网络配置]→[接口配置]，比如选择 eth4 口，“子接口”一栏，添加子接口 ID（填入数字范围是 1~4096 任意数字），为了便于标识，比如填入数值 1 点击“确定”。

完成子接口 ID 的添加后，左边栏会生成出“eth4-1”的子接口。选择 eth4-1 的子接口，配置接口类型：WAN（外网口），填入宽带账号信息，保存。

以此类推，再分别创建 eth4-2、eth4-3，并且填入宽带账号信息，保存，再重启路由。

（注意：添加接口，删除接口的动作，必须要重启，否则会导致整个接口配置功能无效）

以下是 eth4 口一线多拨，成功拨号后的图示。从图中可见得，eth4、eth4-1、eth4-2、eth4-3 分别拨号成功，获得 IP 地址。

注意：

1，宽带账号是否能拨多次，以及成功拨号后，带宽有没有翻倍要以实测为准。

2，注意网口的协商速率，比如光猫是 100M 光猫，多拨后不可能超过网口协商速率 100M。

举例使用场景二：接入的专线有多个公网 IP，两个网吧合并用一个百为路由，要求收银机各走其中一个公网 IP 出去，需要在一个专线上，配置两个专线 IP。

[网络配置]→[接口配置]，比如选择 eth3 口，“子接口”一栏，添加子接口 ID（填入数字范围是 1~4096 任意数字），为了便于标识，比如填入数值 1 点击“确定”。

完成子接口 ID 的添加后，左边栏会生成出“eth3-1”的子接口。选择 eth3-1 的子接口，配置接口类型：WAN（外网口），填入专线的另一个 IP 信息，保存。

以下是子接口配置多个专线 IP 的图示。

4.4，虚拟 IP 的使用

虚拟 IP 的配置方法，和 4.3 章节《子接口的使用》一样，具体操作见 4.3 章节。

虚拟 IP 和子接口的区别：子接口使用独立 MAC，虚拟 IP 使用跟物理口一样的 MAC。比如 eth4 物理口的 MAC 是 00-90-27-FE-E2-C1，所创建的子接口都是随机生成 MAC，且不能配置与 eth4 的 MAC 一样，相反，虚拟 IP 的 MAC 和 eth4 的 MAC 一样为 00-90-27-FE-E2-C1。

建议：由于子接口是独立的 MAC，性质上更类似于一个独立的网卡用于接入光纤，接入宽带。没有特殊的要求，都建议用子接口。如遇到特殊要求，比如极个别运营商的多拨需要用同一个 MAC 来多拨，才选择虚拟 IP。

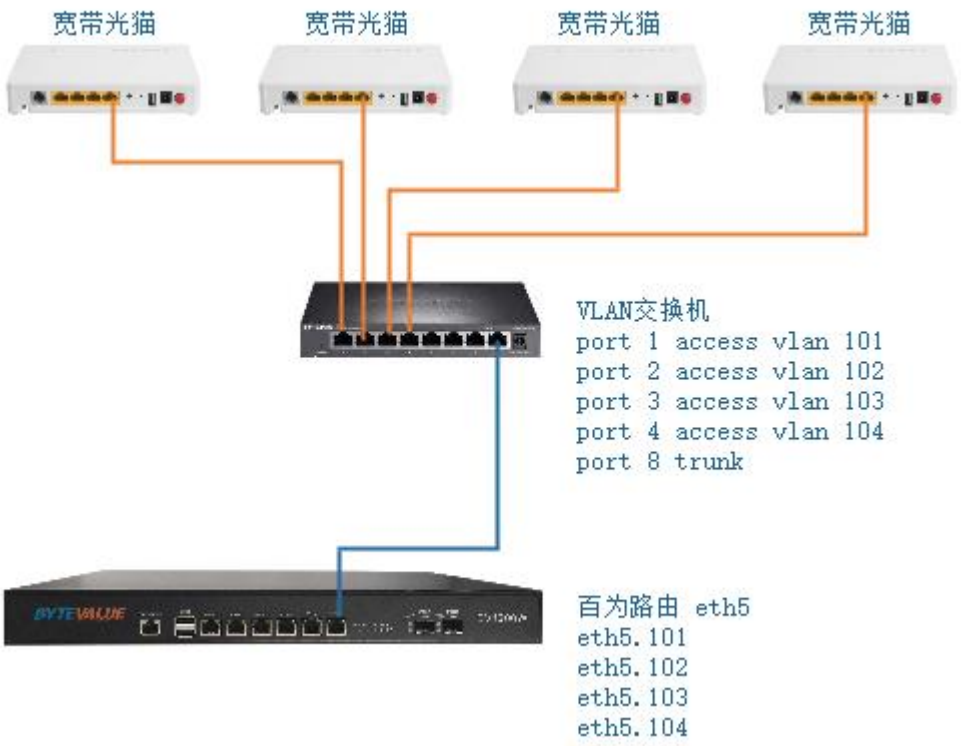
4.5，VLAN 接口的使用

说明：百为路由的 VLAN 是属于 802.1Q 协议 VLAN，通过创建 VLAN 接口，从该 VLAN 接口出来的数据带有 VLAN 标签，通常与交换机的 Trunk 口通讯。

4.5.1，扩展 WAN 口

举例使用场景：当路由网口不够用时，利用 VLAN 交换机划分 802.1Q 协议 VLAN，比如交换机创建 VLAN101---VLAN104，port 1 配置为 access 模式，加入到 vlan 101；port 2 配置为

access 模式，加入到 vlan 102；port 3 配置为 access 模式，加入到 vlan 103；port 4 配置为 access 模式，加入到 vlan 104；port 8 配置为 trunk 模式。百为路由一网口创建 VLAN 接口，VLAN ID 分别为 101-104。路由通过交换机的 trunk 口，扩出多个网口，用于连接运营商的设备。



选择 eth5 口用于扩展 VLAN，将 eth5 设置为禁用（由于 eth5 逻辑层面在启用后有数据包发出来，并且不带 VLAN Tag，为避免发包到交换机影响其它业务，建议禁用）

创建 VLAN101---VLAN104，[网络配置]→[接口配置]→[eth5]→[VLAN 配置]，点击批量添加，输入 101-104，点击确定.

系统状态
网络配置
用户管理
认证上网
对象管理
行为控制
AC控制器
日志记录
高级配置
设备维护
接口配置
分流规则
智能带宽控制
策略带宽控制
连接数控制
内网防护
IP-MAC绑定
异常检测
内网攻击防护
内网限速
DHCP服务
DHCP配置
DHCP分配表
静态路由
静态路由
路由信息
网络接口配置
导出账号
eth0
eth1
eth2
eth3[专线]
eth4[宽带]
eth5[VLAN]
基本配置
高级配置
VLAN配置
子接口
VPN接口
虚拟IP
BPN接口
提示：某些ISP会绑定拨号网卡的MAC地址，会出现拨号失败的情况，使用VLAN拨号的时候最好指定自己的MAC地址
VLAN列表
添加
批量添加
删除
接口名称
VLAN ID
VLAN名称
操作
当前还没有创建VLAN，请添加
批量添加VLAN
格式:VlanId(1~4096)或VlanId区间
比如: 2 或者 3-50 ,支持多行输入
101-104
确定
取消
保存

添加后如下图所示

配置 VLAN 接口的宽带账号。比如宽带账号 075501000101@163.gd 属于光猫 A ，光猫 A 插在 VLAN 交换机的 port1 口上，将宽带账号 075501000101@163.gd 的运营商信息配置于路由的 eth5.101。

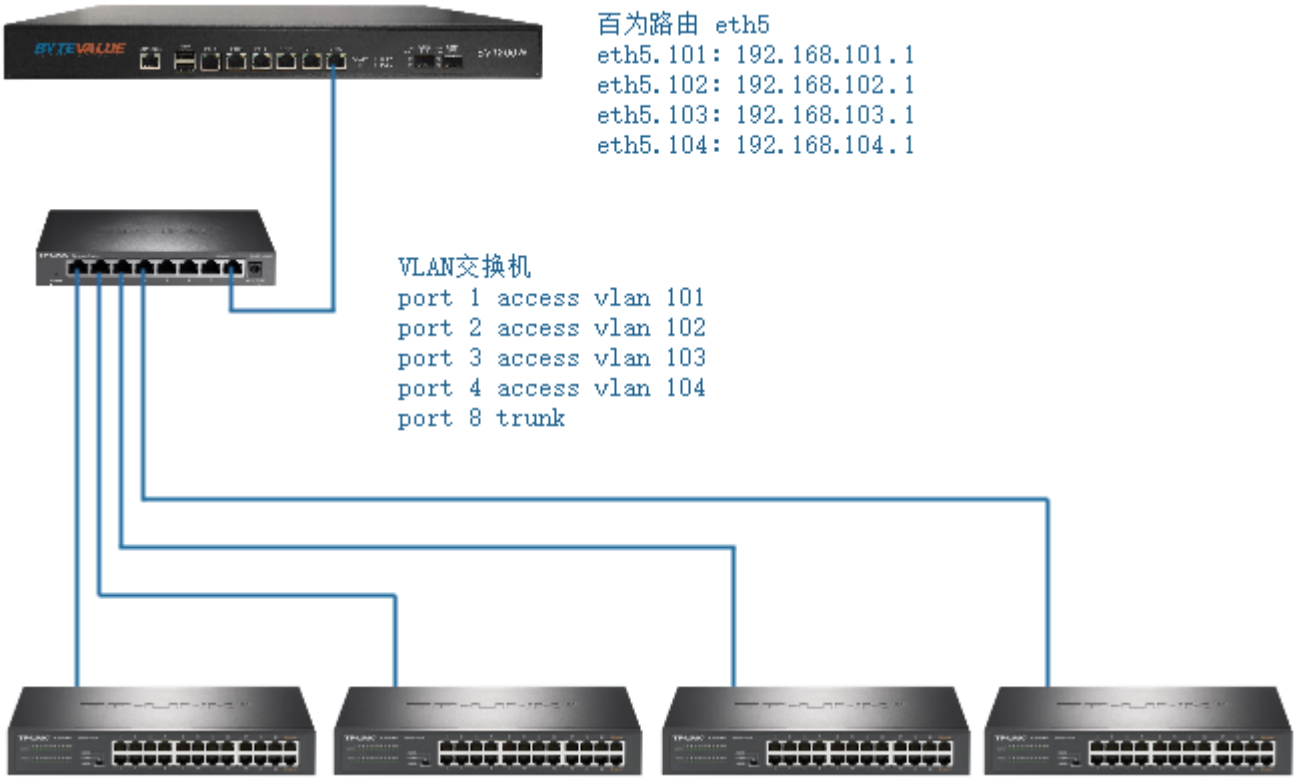
以此类推，分别对 eth5.102、eth5.103、eth5.104，配置对应的宽带账号信息。

保存重启路由（创建 VLAN 接口，配置完所有网口后要重启路由，否则接口配置功能无效），检查接口状态下的 VLAN 扩展口是否能正常拨号

完成

4.5.2，作为 VLAN 网关提供上网

举例使用场景：交换机划分 802.1Q 协议 VLAN，做了隔离。路由创建 VLAN 接口作为 LAN 口提供上网。比如交换机创建 VLAN101---VLAN104，port 1 配置为 access 模式，加入到 vlan 101；port 2 配置为 access 模式，加入到 vlan 102；port 3 配置为 access 模式，加入到 vlan 103；port 4 配置为 access 模式，加入到 vlan 104；port 8 配置为 trunk 模式。百为路由一网口创建 VLAN 接口，VLAN ID 分别为 101-104。路由通过交换机的 trunk 口，提供给 VLAN 101-104 上网。



选择 eth5 口用于扩展 VLAN，将 eth5 设置为禁用（由于 eth5 逻辑层面在启用后有数据包发出来，并且不带 VLAN Tag，为避免发包到交换机影响其他业务，建议禁用）

创建 VLAN101---VLAN104，[网络配置]→[接口配置]→[eth5]→[VLAN 配置]，点击批量添加，输入 101-104，点击确定.

添加后如下图所示

配置 VLAN 接口的 IP。比如 eth5.101，选择接口类型为“LAN（内网口）”，配置 IP 为 192.168.101.1，掩码 255.255.255.0。

以此类推，分别对 eth5.102、eth5.103、eth5.104，配置 LAN 口信息。保存重启路由（创建 VLAN 接口，配置完所有网口后要重启路由，否则接口配置功能无效）

验证 VLAN 网关能否上网

找一台电脑，连接到属于 VLAN 101 的交换机，比如配置电脑的网卡属性，IP 为：192.168.101.100；掩码：255.255.255.0；网关：192.168.101.1；DNS：配置当地运营商 DNS。如电脑能正常上网，说明 VLAN 配置正确。

4.6，北京地区 WAN 口不使用 NAT 配置注意相关事项

说明：北京电信通是将公网 IP 配置于 LAN 口，WAN 口是使用保留地址对接电信通机房，取消 NAT，通过路由转发的形式上网。

举例当前电信通的网吧，WAN 口为 124.192.222.111；LAN 口为 172.30.55.34。需要在百为路由做如下配置

配置地址转换：[高级配置]→[地址转换]→[源地址转换]，添加转换规则

源地址 IP	172.30.55.34
源地址掩码	255.255.255.255
目的地址	0.0.0.0
目的地址掩码	0.0.0.0
替换源地址为	124.192.222.111

配置地址转换：[网络配置]→[接口配置]，选择接电信通的网口，[高级配置]→[NAT]，选择“禁用”，保存。

系统状态
网络配置
用户管理
认证上网
对象管理
行为控制
接口配置
分流规则
智能带宽控制
策略带宽控制
连接数控制
内网防护
DHCP服务
静态路由
网络接口配置
导出账号
eth0[LAN]
eth1
eth2
eth3
eth4
eth5[电信通]
基本配置
高级配置
VLAN配置
子接口
VPN接口
虚拟IP
BPN接口
接口参数
工作模式:
自协商
TCPMSS:
启用自定义TCPMSS
MTU:
启用自定义MTU
MAC地址:
启用自定义MAC地址
NAT:
禁用
高级
自动绑定网关MAC
动态域名配置
启用动态域名:
不启用
保存
批量保存

5，多线路汇聚和分流规则讲解

5.1，百为路由是否有带宽叠加

答：带宽叠加是一个市场宣传的叫法，正确的理解，应该是多线路-会话负载。比如三条 100M 的宽带，迅雷下载的时候，并发了 300 个连接，路由让三条宽带各负载 100 个连接，每个宽带的 100 个连接都有速度回来。汇聚到迅雷后，统计有接近 300M，可理解为带宽叠加。

但现实使用中，如果连接是单线程的。比如使用 QQ 从外地传送一个文件到本地，这是个单线程的传输，一个线程（一个连接）只建立在一个宽带上，则受限于这个宽带的基础带宽，那速度只有接近 100M。

5.2，怎么配置多线路负载（带宽叠加）

答：多线路负载，比如“带宽叠加” 就是配置分流规则实现---勾选多条线路，使用“会话分流”或者 “源+目的地址分流” ，达到连接负载，带宽叠加。

现实中，网吧的宽带组合多种多样，应用都不同。不能单一的考虑 “带宽叠加”。而是有选择性的让一些应用走线路 A，一些应用走线路 B,一些应用走线路 C,D,F . . . . . 这就需要分流规则来实现。细致到只针对某种应用来多线负载-带宽叠加。

5.3，怎么理解分流规则的工作方式

所有通过路由上网的数据，都会经过分流规则。如果分流规则为空，则自动走第一个 WAN 口。比如 eth2，eth3，eth4 都配置为 WAN，并且在线，当分流规则为空，默认只走 eth2。

分流规则里的 “源地址对象” ，“时间” ，“端口” ，“ISP 对象（目的地址）”，“应用类型” ，理解为**条件。**策略里面的勾选的线路，理解为**动作。**

举例下图规则配置，并进行解读

源地址对象-地址-ANY，表示内网所有机器；时间对象-ANY、表示任意时间；端口对象-ANY，表示任意端口；ISP 对象（目的地址对象）-中国联通，表示去联通的网段（中国联通路由表）；应用类型-游戏；分流策略是只勾选了 eth4 ，表示走只 eth4 出去。

整个规则解读为，不管是内网哪个机器，什么端口，什么时间，只要匹配的条件是去联通网段的，并且是游戏类型的（玩联通服的游戏），就走 eth4 的网口出去。

配置分流规则，是有匹配顺序的。所有上网的数据，都会经过分流规则。从第一条规则开始匹配。只要满足条件匹配到了，就会跟着规则所选的线路来走。如果条件没有满足，就接着往下一条规则进行匹配。

所以通常来说，规范的配置，是需要有一个或者多个线路，作为“默认线路”，即最后一条规则，配置条件为全部 ANY。通过“默认线路”用来兜底，匹配没有满足条件的上网数据，走“默认线路”出去。 （没有配置默认线路，路由自动将第一个 WAN 口，作为默认线路）

5.4，分流模式讲解

IP 分流：按照源地址始终分流在一个线路上。以 3 条外网 9 个人上网的环境为例，IP 分流所有

人到 3 条外网上，结果为：张三固定走线路一；李四固定走线路二；王五固定走线路三；赵六固定走线路一，依次将这 9 个人分摊在 3 条线上固定走。由于每个人固定在一个线路上，上网的速度，受限于该线路的带宽。

权重：权重可理解为“比例”，只用于 IP 分流有效。以 3 条外网 12 个人上网的环境为例，IP 分流所有人分流到 3 条外网上，线路一权重 3、线路二权重 2、线路三权重 1。结果为，线路一分得 6 人，线路二分得 4 人，线路三分得 2 人。

（权重就是比例，比如三条线路配置权重为 400，200，100 ，等同于 4 ，2，1，效果一样，也就是 4：2：1）

会话分流：把所有上网的连接，分到每条线上。比如张三开迅雷下载，迅雷并发的很多链接，会话分流到三条线路，每个线路均有连接产生流量回来，汇总到迅雷，达到了带宽叠加的效果。

源+目的地址分流：在会话分流的基础上，识别判断源地址和目的地址再负载到每个线路上。比如张三同时打开了工商银行，京东商城，淘宝三个网站（这里为了讲解说明，就只当这三个网站的 IP 只有 A，B，C)。使用源+目的地址分流，分流所有人走三条外网。最终的效果为：张三的工商银行固定走线路 1；京东商城固定走线路 2，淘宝固定走线路 3。

如今多数网站，都有防止机器人操作，恶意刷登录等限制。网站校验了 IP 地址，多数不允许一个人同时使用多个线路访问网站，建议都默认用源+目的地址分流。

总结：IP 分流适用于线路非常多的条件下，尽量减少 WAN 口的 IP 同时被多人开销，提高 IP 的利用率。多用于小区宽带里的一些做淘宝，亚马逊的电商用户，也多见于一些游戏工作室用到（因为太多人从一个 WAN 口出去访问，可能会被电商会视为刷单，挂机)。

会话分流适用于需要**非常极致**的分流多线程下载业务，比如分流 P2P 下载，游戏更新服务器。

源+目的地址分流，是在会话分流的基础上，做到更好的兼容性，默认推荐使用

备注：当分流规则，勾选的外网线路，只勾选一条时，已无所谓分流模式了。

5.5，举例同一运营商下的专线+宽带网吧的典型分流配置

以下用一个电信 100M 专线+3 条电信 300M 拨号的网吧经典配置作为讲解。

分流规则

添加 删除 注意:分流规则是有优先级的,越靠上优先级越高,可通过操作的上下移动 箭头调整顺序, 置顶, 置底 自动创建分流规则

序号	源地址对象	时间	端口	ISP对象（目的地址）	应用类型	策略	操作
1	地址:ANY	ANY	DNS	ANY	ANY	模式:源IP分流 eth2[专线_100M]|1	
2	地址:ANY	ANY	ANY	ANY	游戏	模式:源IP分流 eth2[专线_100M]|1	
3	地址:游戏更新服务器	ANY	ANY	ANY	ANY	模式:会话分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
4	地址:ANY	ANY	HTTP	ANY	ANY	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
5	地址:ANY	ANY	SSL	ANY	ANY	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
6	地址:ANY	ANY	ANY	ANY	网页	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
7	地址:ANY	ANY	ANY	ANY	网页视频	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
8	地址:ANY	ANY	ANY	ANY	网页下载	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
9	地址:ANY	ANY	ANY	ANY	程序更新下载	模式:源+目的地址分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
10	地址:ANY	ANY	ANY	ANY	P2P与下载	模式:会话分流 eth3[ADSL_1]|1 eth4[ADSL_2]|1 eth5[ADSL_3]|1	
11	地址:ANY	ANY	ANY	ANY	ANY	模式:源+目的地址分流 eth2[专线_100M]|1	

序号 1	匹配到只要包含有 DNS （UDP 53 端口）的数据包，走 eth2 专线出去。
序号 2	匹配到只要识别应用类型属于“游戏”分类的数据包，走 eth2 专线出去。
序号 3	匹配到只要是游戏更新服务器的 IP 的任何数据包，走 eth3，eth4，eth5 宽带出去。（注意：由于序号 1，序号 2 的规则提前匹配了 DNS 包和游戏类型的数据走专线，所以游戏更新服务器的机器的 DNS 包和游戏类型的数据包就没机会走 eth2，eth3，eth4 了）
序号 4	匹配到只要包含有 HTTP （TCP 80 端口）的数据包，走 eth3，eth4，eth5 宽带出

	去。
序号 5	匹配到只要包含有 SSL （TCP 443 端口）的数据包，走 eth3，eth4，eth5 宽带出去。
序号 6	匹配到只要识别应用类型属于“网页”分类的数据包，走 eth3，eth4，eth5 宽带出去。
序号 7	匹配到只要识别应用类型属于“网页视频”分类的数据包，走 eth3，eth4，eth5 宽带出去。
序号 8	匹配到只要识别应用类型属于“网页下载”分类的数据包，走 eth3，eth4，eth5 宽带出去。
序号 9	匹配到只要识别应用类型属于“程序更新下载”分类的数据包，走 eth3，eth4，eth5 宽带出去。
序号 10	匹配到只要识别应用类型属于“P2P 与下载”分类的数据包，走 eth3，eth4，eth5 宽带出去。
序号 11	匹配任何数据包，走 eth2 专线出去。（注意：全部都为 ANY 的规则，是匹配任意的意思，规则置于最底下，作为默认规则，也叫做默认线路。通常，网络中的数据包，经过序号 1-10 的分流规则匹配后，匹配成功的，已经跟着规则所选的线路出去了，但还剩下一些没满足匹配条件的数据包则需要默认规则来承接，这里的默认规则所选的线路，则选择了 100M 专线作为默认规则）

配置的思路，通常是分大流量业务走宽带。比如有 HTTP（80 端口的数据），SSL（443 端口的加密数据），网页，网页视频，网页下载，程序更新下载和 P2P 下载协议，一般也建议把游戏更新服务器的整机分到带宽大的线路去（走拨号）。

流量开销小但连接数开销多的业务，建议走专线。比如 DNS 和游戏，特别是 DNS，非常耗费并发连接。而且多数家庭宽带，运营商出于商业目的，宽带有限制最大并发连接，一旦用超过运营商限制的上限，就会出现各种打不开网页，上网卡的体验，更有可能影响游戏登录。其次，由于 100M 专

线本身的带宽也不小，作为默认线路（分流规则最底下的全 ANY 规则），用于负载一些没匹配到的应用（比如一些聊天语音应用，远程，未知应用），也是充分的利用好专线，减少宽带的连接数负担。

解释说明规则中为什么要分流 HTTP（80 端口）和 SSL（443 端口）。通常来说，标准的网页，网页视频，网页下载的协议数据，几乎采用 80 端口和加密的 443 端口。但从网吧多年的维护经验总结到，有不少应用并不标准，有些大流量业务，不一定就用标准的协议来实现，比如用了 80 和 443 端口来传输，但不属于网页，网页视频，网页下载的协议。同理，用了网页，网页视频，网页下载的协议来传输，未必属于 80 和 443 端口。

5.6，举例同一运营商下的小带宽专线+宽带的网吧典型分流配置

以下用一个电信 20M 专线+3 条电信 300M 拨号的网吧经典配置作为讲解。

序号 1	匹配到只要包含有 DNS （UDP 53 端口）的数据包，走 eth2 专线出去。
序号 2	匹配到只要识别应用类型属于“游戏”分类的数据包，走 eth2 专线出去。
序号 3	匹配任何数据包，走 eth3，eth4，eth5 宽带出去。（注意：全部都为 ANY 的规则，是匹配任意的意思，规则置于最底下，作为默认规则，也叫做默认线路。由于序号 1，序号 2 的规则提前匹配了 DNS 包和游戏类型的数据走专线，所以网吧所有机器的 DNS 包和游戏类型的数据包就没机会走 eth2，eth3，eth4 了。

配置的思路，由于专线的带宽比较小，建议专线就只用来承担 DNS 和游戏数据。值得注意的是 DNS 是非常耗费并发连接的，而且多数家庭宽带，运营商出于商业目的，宽带有限制最大并发连接，

一旦用超过运营商限制的上限，就会出现各种打不开网页，上网卡的体验，更有可能影响游戏登录。由此，DNS 分到专线上，能从一定程度减轻宽带的并发连接开销。

5.7，举例电信专线+联通专线的网吧典型分流配置

以下用一个电信 100M 专线+100M 联通的网吧经典配置作为讲解。

序号 1	匹配到只要包含有 DNS （UDP 53 端口）的数据包。用 IP 分流的方式走 eth2，eth3 专线出去。 （IP 分流 DNS 从电信和联通出去）
序号 2	匹配到只要是去电信网段的，走 eth2 电信专线出去。
序号 3	匹配任何数据包，走 eth3 专线出去。（注意：全部都为 ANY 的规则，是匹配任意的意思，规则置于最底下，作为默认规则，也叫做默认线路。由于序号 2 的规则提前匹配了去电信网段的，走电信专线出去，所以网吧所有机器的非电信业务，就走 eth3 联通出去。

配置的思路，由于是两个不同的运营商，就会有各自的资源。就比如一个网站，一个视频，举例一个电影《盗梦空间》，该影片同时放置于电信机房和放联通机房，这就隶属于电信的资源和联通资源。如何决定这个电影是从电信机房回来，还是从联通机房回来，靠的是 DNS 的解析，比如用联通

DNS 解析，从联通专线发出去，解析回来的资源是联通的 IP，反之就是电信。

通常来说，Windows 客户机默认只用第一个 DNS 来解析，除非第一个 DNS 解析失败，Windows 才会用备用 DNS 解析。如果用联通的 DNS 解析，开网页，开视频，开下载，解析回来的资源，大量隶属于联通机房的资源，走联通专线回来，占用联通压力，（通常也不建议把联通资源的，硬让他从电信回来，容易出问题，无法访问）。就算不用联通 DNS，用公共 DNS，比如 114.114.114.114 ，但从实测来看，国内众多公共 DNS 服务器也似乎判断了源地址的所属，即用联通的线路去请求公共 DNS，还是会解析返回为联通资源。

为了更好的平衡两个不同运营商的线路的资源负载，路由层面建议做 DNS 分流，并且开启 DNS 代理。从规则中可以看出，分流 DNS 同时走两个线路出去，权重都是 1，使用 IP 分流。这个规则的意义在于，分流网吧一半的人的 DNS 请求从联通出去，用联通 WAN 口配置的 DNS 发出去解析；另一半人的 DNS 请求从电信发出去，用电信 WAN 口配置的 DNS 发出去解析。启用 DNS 代理的目的，就是无视客户机电脑配置的 DNS，只要是从 WAN 口出去的，WAN 口配置什么 DNS，就用该 WAN 口的 DNS 发出去解析。

因此，通过配置 DNS 分流到电信和联通出去后，解析回来的资源即有电信资源，也有联通资源。如果是电信资源，按照规则匹配，规则 2 正好满足匹配条件，电信资源就走电信线路出去。非电信资源，就都被最后的默认规则给匹配掉，走联通出去。

总结，多个运营商下，DNS 是一种决定资源倾斜的杠杆。如果说网吧是一条 20M 电信，150M 联通，那你希望电信尽可能少负载，联通多负载，那可以网吧全体机器，都配置联通 DNS，路由也不需要配置 DNS 分流了。如果是一条 80M 电信，200M 联通，希望电信只负载一些，联通负载多挑大梁，那可以 DNS IP 分流的时候，权重设定为电信 1，联通 2 ，差不多也就是 1：2 的比例了，根据实际情况合理配置。

5.8，举例同一个运营商的多条专线或者多条宽带的网吧典型分流配置

以下用 4 条电信 200M 宽带的网吧经典配置作为讲解。

序号 1	匹配任何数据包，使用源+目的地址分流，走 eth2，eth3，eth4，eth5 宽带出去。

配置的思路，由于四条宽带都是同一个运营商，并且都是带宽差不多大的宽带。所以不需要区分应用走特定的线路，使用源+目的地址分流，四条线路不区分应用直接负载。

这样的配置，同样适用于多条专线的时候，比如两条 100M 的电信专线，也是如此配置。

5.9，分流内网某个 IP 走一条外网线路出去

多线路环境，内网某个 IP 地址需要只走一条外网线路出去。比如，网吧要求收银机只走光纤固定 IP。操作如下

[对象管理]→[地址对象]。添加地址对象，比如命名为“收费机”，并填入收费机的 IP。

[网络配置]→[分流规则]，添加“分流规则”，“源地址对象-地址”选择“收费机”，“时间对象、端口对象、ISP 对象、应用对象”均为“ANY”，勾选指定要走的外网线路（专线），使用“IP 分流”，将该规则置顶。

5.10，分流内网某个用户走一条外网线路出去

用户，是指百为路由下，实名成一个用户角色。比如这个用户角色，关联了某个 IP，或者某个 MAC，或者是 PPPoE 拨号用户、Portal 认证用户、VPN 用户。

以分流小区运营的 PPPoE 拨号用户为例。小区网络，多线路环境下，个别用户当访问交易类网站，比如亚马逊，这类网站对 IP 检验比较严格，通常要求用户只能用一个公网 IP 来访问的时候，需要分流这个用户始终走一条线出去。

举例分流用户为“D501A0001”，指定走 eth3 的线路出去。

[网络配置]→[分流规则]，添加“分流规则”，“受控对象-用户”选择“D501A0001”，“时间对象、端口对象、ISP 对象、应用对象”均为“ANY”，勾选指定要走的外网线路，使用”源 IP 分流”，将该规则置顶。

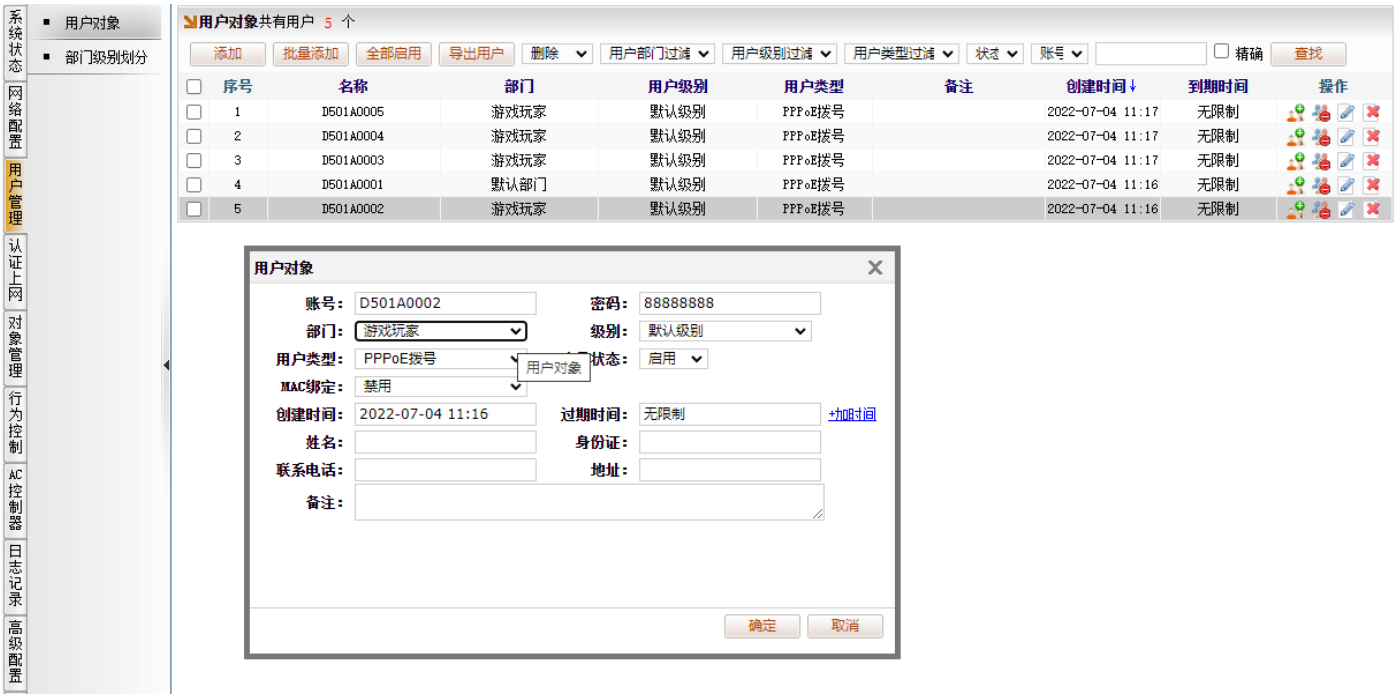
5.11，分流小区内网多个用户/部门走一条外网线路出去

分流多个用户走一条线路出去，可以把用户归类到一个部门，对这个部门分流。

比如小区里一个名为“D501A0001”、“D501A0002”、“D501A0003”、“D501A0004”、“D501A0005”的用户，需要指定走 eth3 的线路出去。(比如用户都是重度游戏玩家，需要 eth3 线路独享专用)

创建一个部门[用户管理]→[部门级别划分]→[部门划分]，添加“部门”，比如命名为“游戏玩家”

[用户管理]→[用户对象]，编辑用户的部门，选择为“游戏玩家”

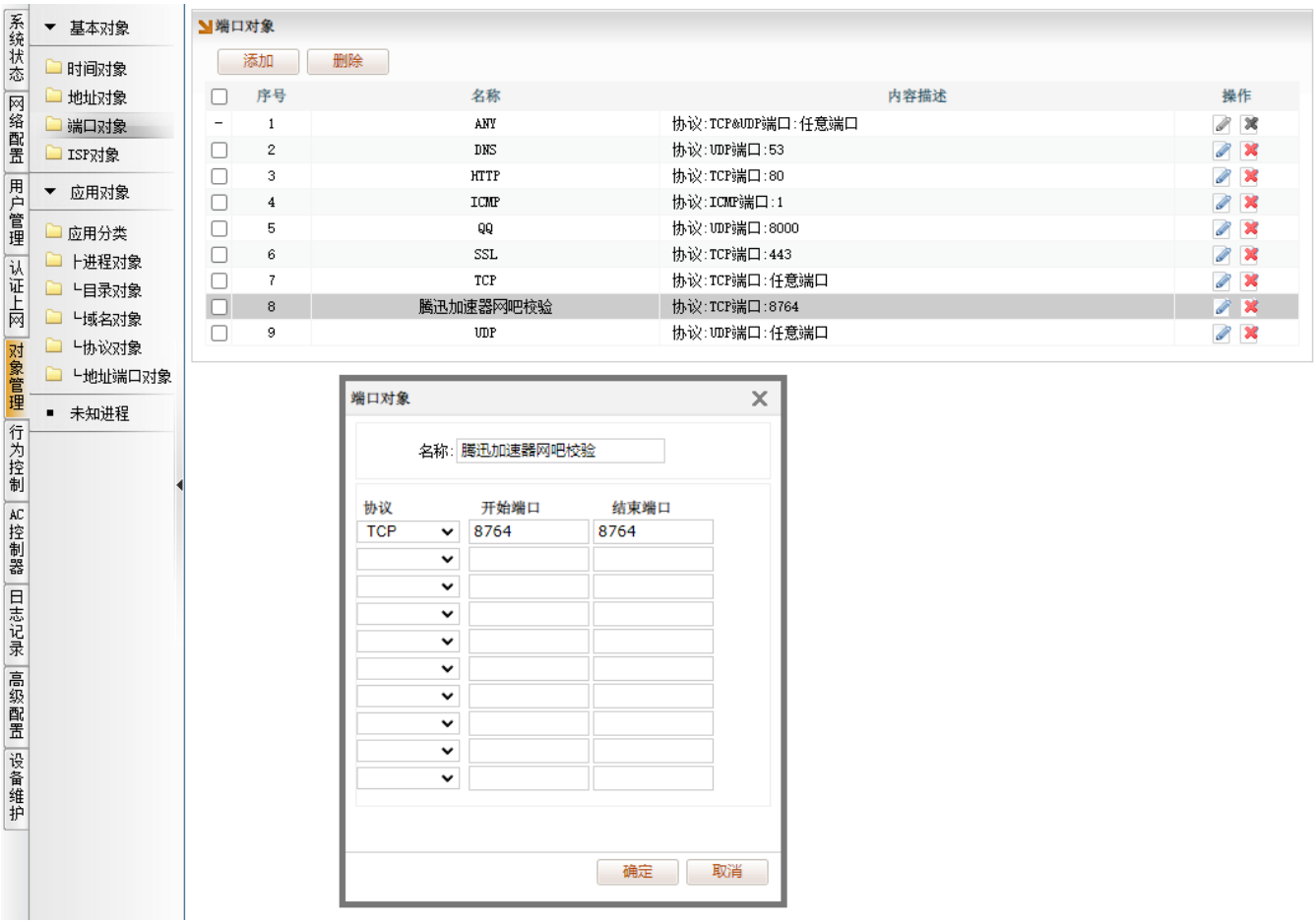


[网络配置]→[分流规则]，添加“分流规则”，“源地址对象-部门”选择“游戏玩家”，“时间对象、端口对象、ISP 对象、应用对象”均为“ANY”，勾选指定要走的外网线路，使用“源 IP 分流”，将该规则置顶。

5.12，分流目的端口走一条外网线路出去

多线路环境，某个目的端口，需要只走一条外网线路出去。这里举例 “腾迅网游加速器网吧版”的校验端口 TCP 8764 分到专线。操作如下

[对象管理]→[基本对象]→[端口对象]，添加，名称比如为“腾迅加速器网吧校验”，选择 TCP 协议，开始端口和结束端口都为 8764，确定



[网络配置]→[分流规则]，添加“分流规则”，“端口”选择“腾迅加速器网吧校验”，“源地址对象、时间、端口、ISP 对象（目的地址）、应用类型”均为“ANY”，勾选指定要走的外网线路。最后将该规则置顶。

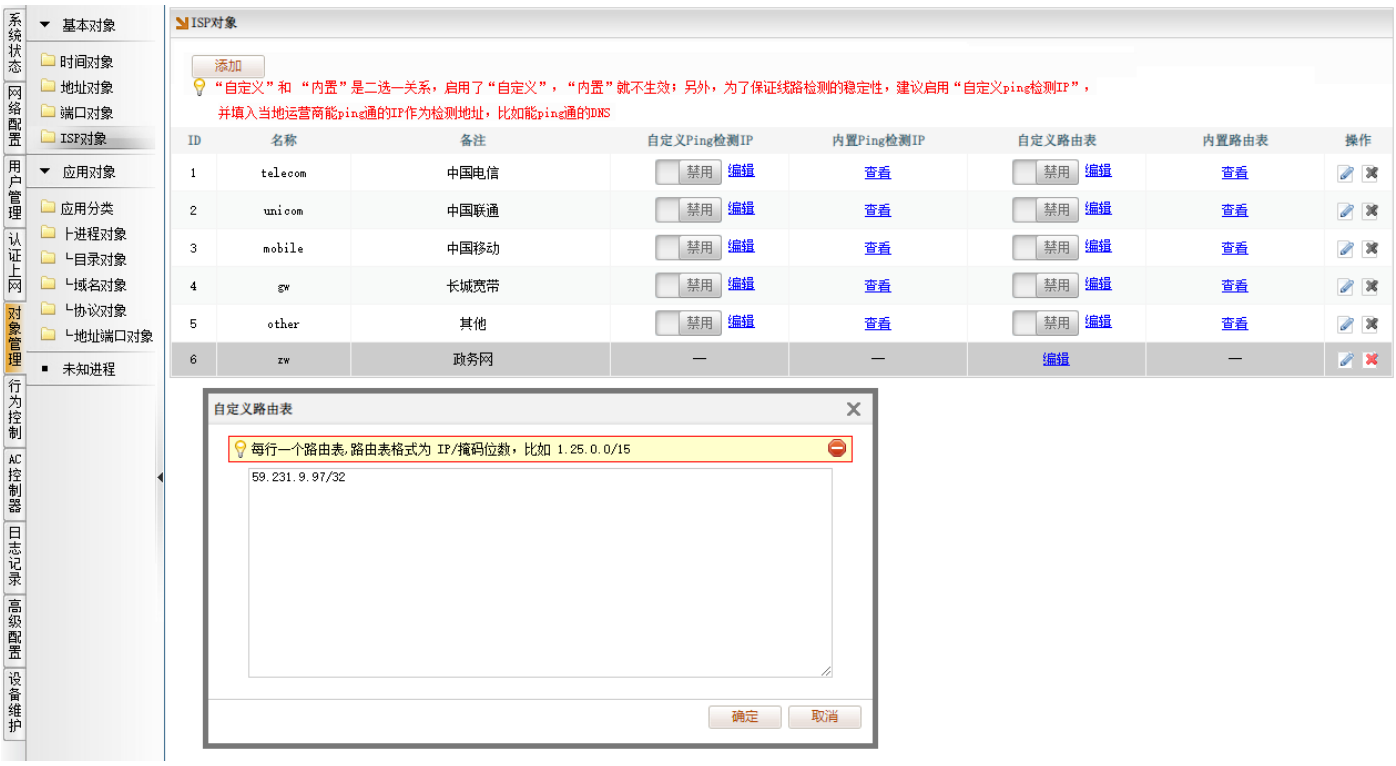
5.13，分流外网某个 IP(目的 IP)走一条外网线路出去

多线路环境，某个外网 IP 地址，甚至是一个 IP 段，需要只走一条外网线路出去。比如，某个政务网，已知站点的 IP 为 59.231.9.97，分流这个 IP 走 专用网的光纤出去。操作如下

[对象管理]→[基本对象]→[ISP 对象]。点击“添加”地址对象，比如名称为“zw”，备注为“政务网”

在生成出来的“政务网”这个 ISP 对象一栏，点击“编辑”,并且在编辑框填入 59.231.9.97/32

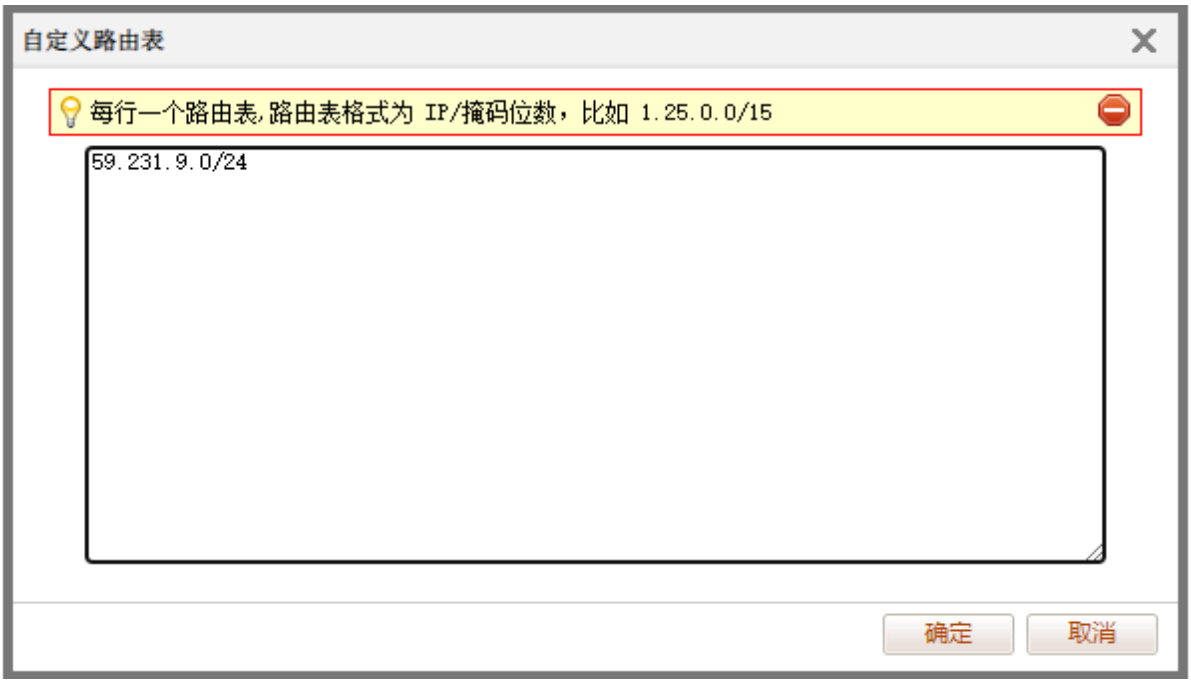
（路由表的编辑方式，采用了 IP+网络位个数的表示方法，即 IP 地址后用有斜杠和数字组合，只是要分一个 IP 地址的时候，用/32）



[网络配置]→[分流规则]，添加“分流规则”，“ISP 对象（目的地址）”选择“政务网”，“源地址对象、时间、端口、应用类型”均为“ANY”，勾选指定要走的外网线路。最后将该规则置顶。

附录:

使用路由表分流整个网段，比如要匹配 59.231.9.1----59.231.9.255 整个网段，只需在路由表编辑为 59.231.9.0/24



现实应用中，比如某个机构，给到的信息是如下:

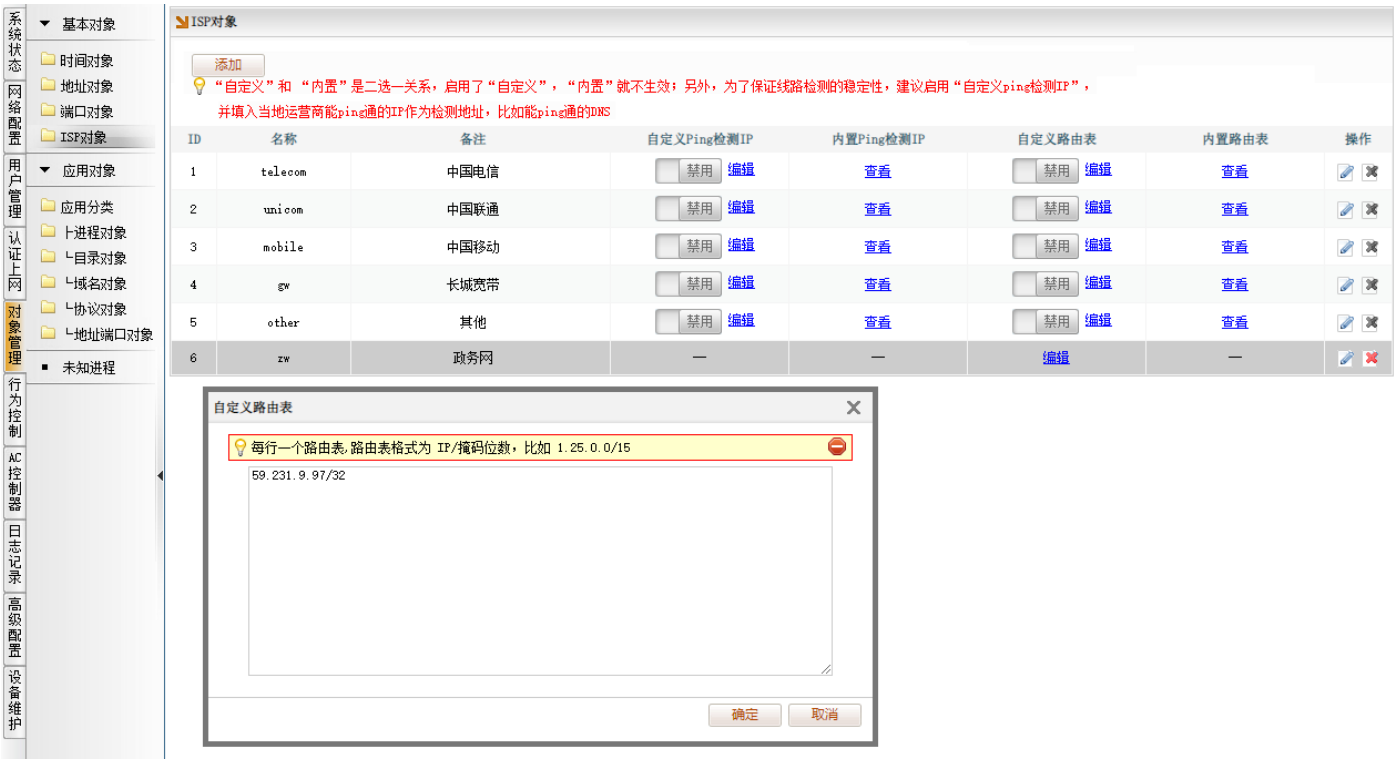
要求分 59.240.1.0 掩码为： 255.255.252.0 的网段，走指定线路出去。转换 255.255.252.0 为 22 （百度可搜索 IP 掩码在线计算工具去计算），编辑到路由表则为 59.240.1.0/22

5.14，分流外网某个 IP(目的 IP)+目的端口走一条外网线路出去

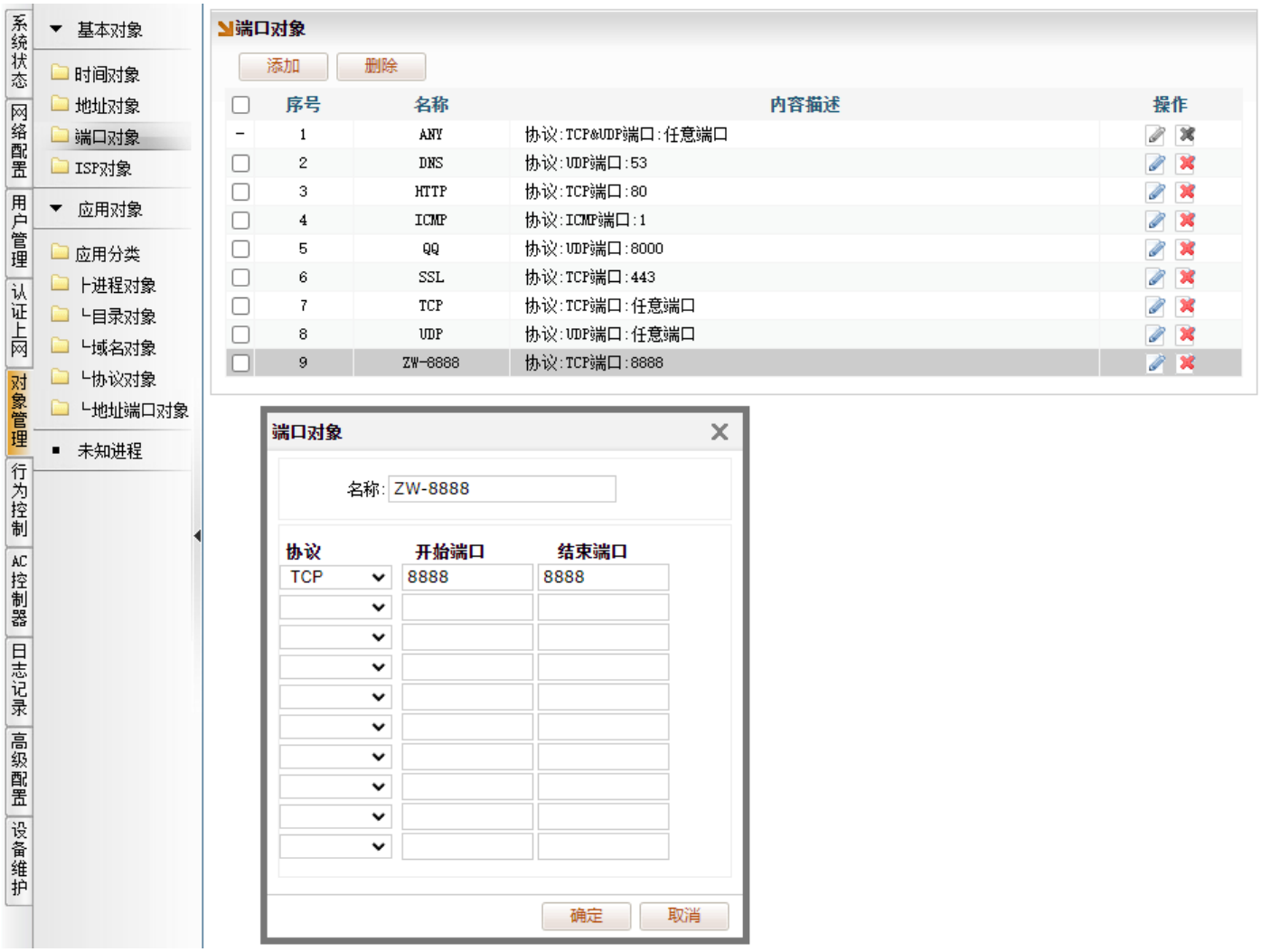
结合 3.12，3.13 章节的教材，多线路环境，某个外网 IP 地址，甚至是一个 IP 段，需要只走一条外网线路出去。比如，某个政务网，已知站点的 IP 为 59.231.9.97，要求只是 TCP 8888 端口的业务，走专用网的光纤出去。可配置分流规则的时候，同时匹配 “端口” +“ISP 对象（目的地址)” 来实现，操作如下：

[对象管理]→[基本对象]→[ISP 对象]。点击“添加”地址对象，比如名称为“zw”，备注为“政务网”

在生成出来的“政务网”的这个 ISP 对象一栏，点击“编辑”,并且在编辑框填入 59.231.9.97/32（路由表的编辑方式，采用了 IP+网络位个数的表示方法，即 IP 地址后用有斜杠和数字组合，只是要分一个 IP 地址的时候，用/32）



[对象管理]→[基本对象]→[端口对象]，添加，名称比如为“ZW-8888”，选择 TCP 协议，开始端口和结束端口都为 8888，确定



[网络配置]→[分流规则]，添加“分流规则”，“端口”选择“ZW-8888”，“ISP 对象（目的地址）”选择“政务网”，“源地址对象、时间、应用类型”均为“ANY”，勾选指定要走的外网线路。最后将该规则置顶。

5.15，分流域名走指定线路出去（查 IP 走指定线路）

多线路环境里，个别网页，需要走某条线路才能打开；或者有些网吧查询 IP 的网站，比如 百度，ip138、ip.com 等查 IP 的网站，显示为专线 IP。可使用“域名分流”来实现。

比如网吧需要把主流查 IP 的站点，让显示为专线 IP

常用的查 IP 的域名如下

i.bdcloudapi.com	百度查询 IP 地址 API
ip138.com	IP138
ip.cn	IP.CN
tool.lu	在线工具站点
ip.tool.chinaz.com	ChinaZ IP 查询

123cha.com	123 查
ip.chacha.cn	查查网

[对象管理] →[应用对象]→[域名对象]。添加要分流的域名、备注，所属分类，比如选择为“自定义 1”。

注意：分流域名，分流“www.ip138.com”和分流“ip138.com”是不同的，前者表示只分流带有“www”开头的完整域名，后者表示只要是“ip138.com”结尾的域名，都参与会被分流。

请根据实际情况填写，一般不匹配 www，更不要填写 http://以及域名后面的地址，比如 / 域名后面斜杠的内容，都不填写

（上图只举例添加了主流的查 IP 站点，有其他查 IP 站点，请自行添加）

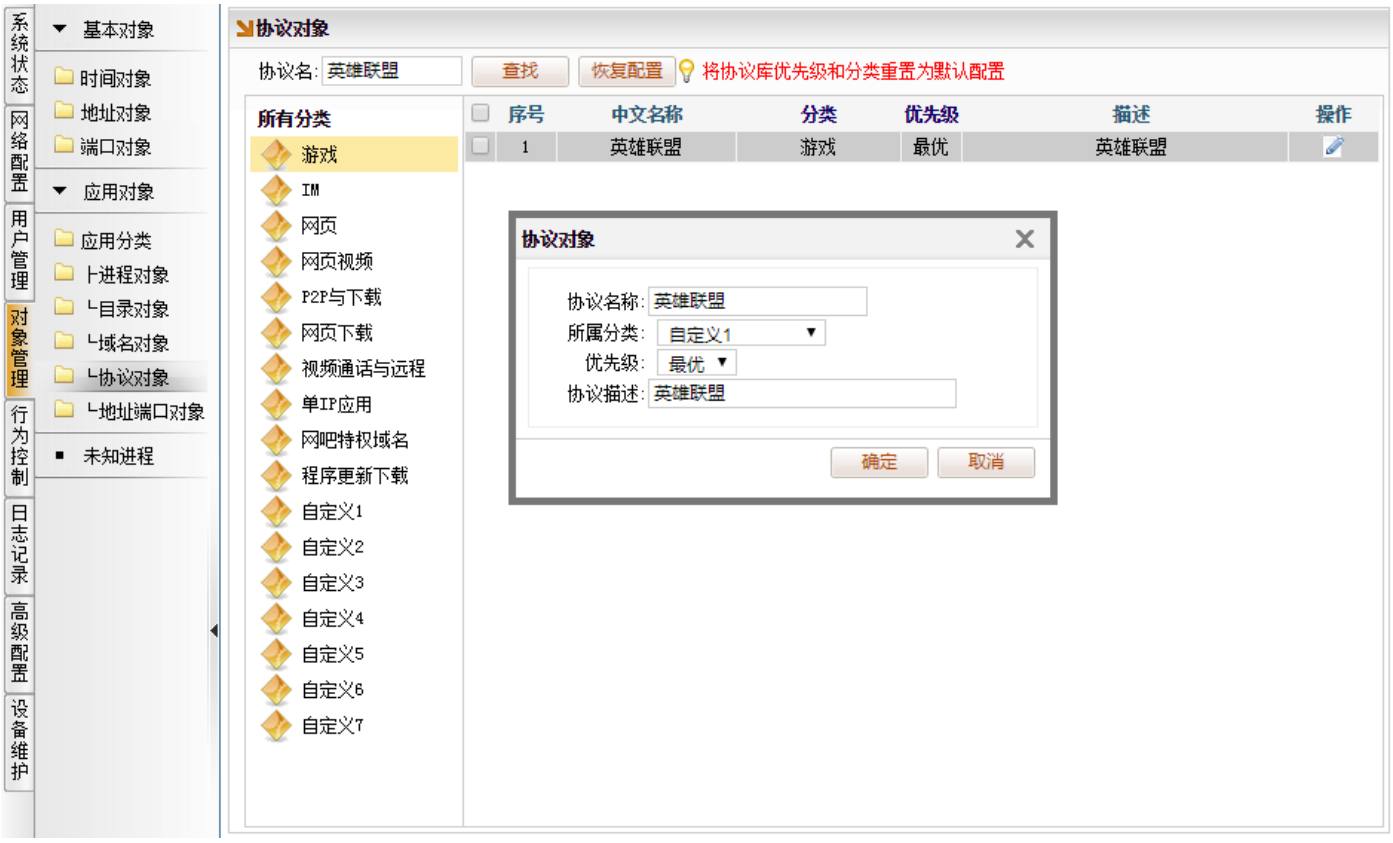
[网络配置]→[分流规则]，添加“分流规则”，“应用类型”选择“自定义 1”，“受控对象、时间对象、端口对象、ISP 对象”均为“ANY”，勾选指定要走的外网线路。最后将该规则置顶。

5.16，分流某个（协议）走指定线路出去

多线路环境里，希望某个协议，只走指定线路。比如把“英雄联盟”，走指定的线路 eth4 的 WAN 口出去。可如下操作

修改英雄联盟的协议分类 （原来“英雄联盟”属于游戏分类）

[对象管理] →[应用对象]→[协议对象]，搜索协议名“英雄联盟”。编辑该 “英雄联盟” 的协议，修改所属分类，为“自定义 1”



[网络配置]→[分流规则]，添加“分流规则”，“应用类型”选择“自定义 1”，“源地址对象、时间、端口、ISP 对象（目的地址）”均为“ANY”，勾选指定要走的外网线路，点击确定。最后将该规则置顶。

如下图所示，表示把自定义 1，分走 eth4 的线路出去。

(备注：规则配置后，需要退出游戏，重新进游戏，游戏才会跟着规则所选的线路来走)

5.17，典型的分流规则错误讲解

错误 1：默认规则（条件全部都为 ANY 的规则）没有置于最底下。

全部为 ANY 的规则，是匹配任意的意思，如果没有置于最底下，那意味着任何业务都会被默认规则给匹配掉，没机会走下一条规则。

比如下图所示：由于第一条规则，源地址对象已经是 ANY，就是匹配任意源地址的意思，自然也包含了“游戏更新服务器”的 IP，当游戏更新服务器的业务请求时，匹配到第一条规则已经满足条件了，走了 eth2 出去。则没机会走第二条规则了

错误 2：没配置默认规则（条件全部都为 ANY 的规则）。

全部为 ANY 的规则，是匹配任意的意思，如果缺少默认规则，没有被匹配到的业务，路由自动走第一个线路。

比如下图所示：由于缺少默认规则，除了网页，网页视频，P2P 与下载的应用走 eth2，eth3，eth4。其他业务，都自动走 eth2 了

分流规则

添加 删除 注意:分流规则是有优先级的,越靠上优先级越高,可通过操作的上下移动 箭头调整顺序, 置顶, 置底 自动创建分流规则

序号	源地址对象	时间	端口	ISP对象（目的地址）	应用类型	策略	操作
1	地址:ANY	ANY	ANY	ANY	网页	模式:源+目的地址分流 eth2[ADSL_1]|1 eth3[ADSL_2]|1 eth4[ADSL_3]|1	
2	地址:ANY	ANY	ANY	ANY	网页视频	模式:源+目的地址分流 eth2[ADSL_1]|1 eth3[ADSL_2]|1 eth4[ADSL_3]|1	
3	地址:ANY	ANY	ANY	ANY	P2P与下载	模式:源+目的地址分流 eth2[ADSL_1]|1 eth3[ADSL_2]|1 eth4[ADSL_3]|1	

错误 3：条件组合错误导致的规则无效、

有一些端口和协议可能存在互斥的，比如下图所示，DNS 的端口是 UDP 53，而网页协议的，通常是不会用 UDP 53 来传输。如果规则这么搭配，第一条规则解读为：即是 DNS 端口的，又是网页而协议的，才走 eth3。但现实中，数据包很少有这种组合，原意只是想分网页走宽带，因为错误的搭配了“端口”这个条件，反而导致规则无效

分流规则

添加 删除 注意:分流规则是有优先级的,越靠上优先级越高,可通过操作的上下移动 箭头调整顺序, 置顶, 置底 自动创建分流规则

序号	源地址对象	时间	端口	ISP对象（目的地址）	应用类型	策略	操作
1	地址:ANY	ANY	DNS	ANY	网页	模式:源+目的地址分流 eth3[宽带]|1	
2	地址:ANY	ANY	ANY	ANY	ANY	模式:源+目的地址分流 eth2[专线]|1	

错误 4：不同运营商的 DNS 分流没有用 IP 分流

以电信+联通的线路组合为例，DNS 分流，是为了平衡解析回来的资源，既有电信的资源，也有联通的资源。必须用 IP 分流。

下图是错误的示例，可能会导致打开一些网站会异常。如今多数网站打开的时候，会请求多个域名，如果一个网站的多个域名，一些域名走联通，一些域名走电信了，就算解析成功，回来的资源即来源于电信，也来源于联通，到了浏览器端可能会异常。

正确的做法是 DNS 分流到电信和联通，用 IP 分流，保证整个客户机的 DNS 请求，始终走电信解析，或者走联通解析。

错误 5：不同运营商的直接负载随机走

以电信+联通的线路组合为例，默认规则直接勾选电信和联通用“源+目的地址分流”，这样就不区分目的地址两条随机负载。可能导致一些业务打不开。比如玩家选择玩电信服，结果有可能随机负载到 eth3 联通出去了。下图为错误配置。

正确的配置如下图所示

分流规则

添加 删除 注意:分流规则是有优先级的,越靠上优先级越高,可通过操作的上下移动 箭头调整顺序, 置顶, 置底 自动创建分流规则

序号	源地址对象	时间	端口	ISP对象（目的地址）	应用类型	策略	操作
1	地址:ANY	ANY	DNS	ANY	ANY	模式:源IP分流 eth2[电信]|1 eth3[联通]|1	
2	地址:ANY	ANY	ANY	中国电信	ANY	模式:源+目的地址分流 eth2[电信]|1	
3	地址:ANY	ANY	ANY	ANY	ANY	模式:源+目的地址分流 eth3[联通]|1	

（规则解读为：DNS 走 eth2 和 eth3 让解析回来的资源均衡，去电信的走电信，非电信的都走联通，把联通作为默认线路）

也可以如下这么配置

分流规则

添加 删除 注意:分流规则是有优先级的,越靠上优先级越高,可通过操作的上下移动 箭头调整顺序, 置顶, 置底 自动创建分流规则

序号	源地址对象	时间	端口	ISP对象（目的地址）	应用类型	策略	操作
1	地址:ANY	ANY	DNS	ANY	ANY	模式:源IP分流 eth2[电信]|1 eth3[联通]|1	
2	地址:ANY	ANY	ANY	中国电信	ANY	模式:源+目的地址分流 eth2[电信]|1	
3	地址:ANY	ANY	ANY	中国联通	ANY	模式:源+目的地址分流 eth3[联通]|1	
4	地址:ANY	ANY	ANY	ANY	ANY	模式:源+目的地址分流 eth2[电信]|1 eth3[联通]|1	

（规则解读为：DNS 走 eth2 和 eth3 让解析回来的资源均衡，去电信的走电信，去联通的走联通，非电信，非联通的，比如阿里云，腾讯云之类的，允许电信线路和联通线路一起负载）

6，限速功能讲解

6.1，什么是智能流控

答：智能流控是百为路由通过动态计算用户的带宽需求，在保证游戏延迟的前提下，给用户自动限速，也称为“动态限速”。

举例 100M 专线的网吧，专线上行带宽、下行带宽分别配置了 10000KB，勾选“启用智能流控”。智能流控将管控所有用户的带宽请求总和不超过 10000KB，对有持续耗费大流量的用户，给予动态限速。

比如有 1 人在专线上持续的下载，智能流控控制这 1 人的带宽为 8000KB~10000KB；4 人在专线上持续的下载，智能流控控制这 4 人的人均带宽为 2000KB~2500KB；20 人在专线上持续的下载，智能流控控制这 20 人的人均带宽为 400KB~500KB。做到人少带宽自动放开，人多带宽收紧。

以下是 WAN 口的配置页面示例，务必正确的配置线路带宽。

备注：[网络配置]→[智能带宽控制]→[智能流控配置] →“智能流控开关”与 [网络配置]→[接口配置]

→WAN 口配置项 ---“启用智能流控” 勾选项，是同一个配置。

6.2，策略带宽控制讲解

策略带宽控制，可以理解为固定限速，并且限速是针对单个 IP。

以下图为例，源地址对象-地址，选择“ANY”、上行限制 1000KB；下行限制 5000KB；P2P 上行允许带宽百分比 70%；P2P 下行允许带宽百分比 80%。

规则解读:源地址对象-地址-ANY 表示内网任意的电脑 IP,限制每人的上行开销不超过 1000KB，下行开销不超过 5000KB。P2P 类别的带宽开销，上行不超过 700KB（1000KB×70%），下行不超过 4000KB（5000KB×80%）。

备注：P2P 类别通常指 BT 协议，P2P 协议，迅雷，电驴，游戏更新服务器协议等耗费上下行带宽的业务

高级功能使用讲解

策略带宽控制高级选项，允许单独控制每个内网 IP 在每个 WAN 口上的速度。勾选生效的 WAN 口，单独带宽控制，不含在总的策略带宽里。

举例一、策略带宽高级选项---勾选生效所有 WAN 口进行配置，具体见下图

规则解读：虽然带宽控制规则配置内网任意的电脑 IP，限制每人的上行开销不超过 1000KB，下行开销不超过 15000KB。P2P 类别的带宽开销，上行不超过 700KB（1000KB×70%），下行不超过 12000KB（15000KB×80%）。(此处我们称第一层的限速规则为“标准限速”)

但由于策略带宽高级选项，勾选生效所有 WAN 口，表示被勾选的 WAN 口不计入“标准限速”的范畴，以高级选项所填入在每个 WAN 口的上下行限速值为准。

该例子的最终效果为：内网任意的电脑 IP，限制在 eth3 上行开销不超过 800KB，下行开销不超过 2000KB；在 eth4 上行开销不超过 500KB，下行开销不超过 10000KB；在 eth5 上行开销不超过 500KB，下行开销不超过 10000KB。因此，上行限速累计不超过 1800KB（800KB+500KB+500KB）；下行累计不超过 22000KB（2000KB+10000KB+10000KB）。

结论，策略带宽高级选项，若勾选生效所有 WAN 口，“标准限速”这一层的限速值是无效值，甚至可以不配置。

高级功能举例二、策略带宽高级选项---只勾选生效个别 WAN 口进行配置，具体见下图

规则解读：带宽控制规则配置内网任意的电脑 IP，限制每人的上行开销不超过 1000KB，下行开销不超过 15000KB。P2P 类别的带宽开销，上行不超过 700KB（1000KB×70%），下行不超过 12000KB（15000KB×80%）。(此处我们称第一层的限速规则为“标准限速”)

由于策略带宽高级选项，只勾选生效 eth3 口，表示被勾选的 WAN 口不计入“标准限速”的范畴，以高级选项所填入在每个 WAN 口的上下行限速值为准。

该例子的最终效果为：内网任意的电脑 IP，限制在 eth3 上行开销不超过 800KB，下行开销不超过 2000KB；在 eth4、 eth5 上行开销累计不超过 1000KB，下行开销累计不超过 15000KB。因此，上行累计不超过 1800KB（800KB+1000KB）；下行累计不超过 17000KB（2000KB+15000KB）。

结论，策略带宽高级选项，若只勾选生效个别 WAN 口，“标准限速”这一层的限速值是对没有勾选生效的 WAN 口的限速值有效。

6.3，策略带宽控制---对指定 IP/IP 段限速

从 6.2 章节了解到。策略带宽控制，源地址对象，选择“地址-ANY”，配置的限速规则，是针对整个内网所有 IP 地址单个限速。

对指定 IP/IP 段限速，配置方法如下：

[对象管理]→[基本对象]→[地址对象]，添加地址对象，比如命名为“VIP”，填入指定限速的 IP/IP

段。比如下图定义了 VIP 的地址对象为 192.168.1.180---192.168.1.190 和 192.168.1.199。

[网络配置]→[策略带宽控制]，添加带宽控制规则，源地址对象，选择“地址-VIP”，填入要限速的上行，下行带宽。比如下图限速该 VIP 网段的上行带宽不超过 2000KB；下行不超过 20000KB。（如需精确到在每个 WAN 口上的限速，请参考 6.2 章节中，高级功能的讲解）

添加的规则会自动排序，“源地址对象--地址-VIP”的限速规则 1，优先匹配。该 IP/IP 段的速度不受规则 2 影响

6.4，智能流控和策略带宽控制的关系说明

答：从 6.1、6.2 章节了解到。智能流控是百为路由的通过动态计算用户的带宽需求，在保证游戏延迟的前提下，给用户自动限速，以下我们称“动态限速”。策略带宽控制属于固定限速。动态限速和固定限速并不冲突，可以开启智能流控的基础上，配置策略带宽控制。二者取交集∩作为准。

比如有 4 人在专线上持续的下载，智能流控控制这 4 人的人均带宽为 2000KB。如果配置了策略带宽控制，限制每人的带宽为 1000KB ，取最小值，最终限速为 1000KB。如果配置了策略带宽控制，限制每人的带宽为 5000KB，取最小值，最终限速为 2000KB。

网吧配置策略带宽控制的意义：

网吧里存在病毒，广告插件，肆意上传，使用策略带宽控制单机的上传带宽小点，可在保证网吧合法业务的基础上，防止有人利用网吧上行带宽实施攻击行为，通常控制上行带宽有 500-1500KB 即可满足网吧的单机上传需求。使用策略带宽控制单机的下行带宽，可防止客户机的下行流量太大，给无盘回写造成太大压力。

6.5，举例专线+宽带的网吧策略带宽规则配置

以下用一个 100M 专线+3 条 300M 拨号的网吧经典配置作为讲解。

（可结合 5.5 章节的分流规则讲解加以学习理解）

图 6.5-1

图 6.5-2

配置的思路：此类型的网吧，通常分流大流量业务走宽带，比如网页，视频，下载业务走宽带，游戏更新服务器走宽带，游戏，聊天，其他业务走专线。由于专线的带宽没有拨号宽带的下行带宽大，建议策略带宽配置，结合高级选项，控制每个机器在专线的带宽开销。

配置解读：图 6.5-1 中，内网任意的电脑 IP，限制在专线 eth2 上行开销不超过 800KB，下行开销不超过 3000KB；在三条宽带 eth3、eth4、 eth5 上行开销累计不超过 800KB，下行开销累计不超过 10000KB。图 6.5-2 中，游戏更新服务器，限制在专线 eth2 上行开销不超过 1500KB，下行开销不超过 5000KB；在宽带 eth3 上行开销不超过 800KB，下行开销不超过 25000KB；在宽带 eth4 上行开销不超过 800KB，下行开销不超过 25000KB；在宽带 eth5 上行开销不超过 800KB，下行开销不超过 25000KB。（由于游戏更新服务器的限速规则为规则 1，优先匹配。游戏更新服务器的速度不受规则 2 影响）

解释说明规则中为什么要限速客户机和服务器：

关于客户机的限速。限制每个客户机的在专线的流量不超过专线的 20%-50%带宽，主要防止个别游戏因异常了，肆意开销专线带宽，起到保险的作用；限制在三条宽带的上行带宽总和，主要因为宽带的上行速度小，网吧里存在病毒，广告插件，肆意上传，防止有人利用网吧上行带宽实施攻击行为；限制在三条宽带的下行带宽总和，主要是防止客户机的下行流量太大，给无盘回写造成太大压力。

关于服务器的限速。限制服务器在专线的流量不超过专线的 20%-50%带宽，主要防止服务器映射的业务，从光纤传入，肆意开销专线带宽，起到保险的作用；限制在每条宽带的上行带宽，主要因为宽带的上行速度小，服务器的游戏更新业务会无节制的上传共享（下载完毕的游戏上传共享给其他网吧）；限制在每条宽带的下行带宽，适当的放大，提高下载速度。

6.6，举例多条专线或者多条宽带的网吧策略带宽规则配置

以下用 4 条 200M 的宽带的网吧经典配置作为讲解。

（可结合 5.8 章节的分流规则讲解加以学习理解）

图 6.6-1

图 6.6-2

配置的思路：此类型的网吧由于每条线路带宽差异不大，比如两条 100M 专线，或者四条 200M 宽带组合。分流规则无需区分应用走某个线路，因此，客户机可以不用高级选项进行配置，服务器用高级选项进行配置。

配置解读：图 6.6-1 中，内网任意的电脑 IP，限制在四条宽带 eth2、eth3、eth4、 eth5 上行开销累计不超过 800KB，下行开销累计不超过 10000KB。图 6.6-2 中，游戏更新服务器，限制在宽带 eth3 上行开销不超过 800KB，下行开销不超过 15000KB；在宽带 eth3 上行开销不超过 800KB，下行开销不超过 15000KB；在宽带 eth4 上行开销不超过 800KB，下行开销不超过 15000KB；在宽带 eth5 上行开销不超过 800KB，下行开销不超过 15000KB。（由于游戏更新服务器的限速规则为规则 1，优先匹配。游戏更新服务器的速度不受规则 2 影响）

解释说明规则中为什么要限速客户机和服务器：

关于客户机的限速。限制每个客户机在四条宽带的上行带宽总和的不超过线路的 20%-50%带宽，主要因为宽带的上行速度小，网吧里存在病毒，广告插件，肆意上传，防止有人利用网吧上行带宽实施攻击行为。其次，限制在四条宽带的下行带宽总和，主要是防止客户机的下行流量太大，给无盘回写造成太大压力，其次，也防止个别游戏因异常了，肆意开销带宽，起到保险的作用。

关于服务器的限速。需要在高级选项，限制在每条宽带的上行带宽，主要因为宽带的上行速度小，服务器的游戏更新业务会无节制的上传共享（下载完毕的游戏上传共享给其他网吧）；限制在每条宽带的下行带宽，适当的放大，提高下载速度。

6.7，智能流控例外规则讲解

答：从 6.1、章节了解到。智能流控是百为路由的通过动态计算用户的带宽需求，在保证游戏延迟的前提下，给用户自动限速，以下我们称“动态限速”。若个别机器需要脱离智能流控的约束，可配置智能流控例外规则来实现。

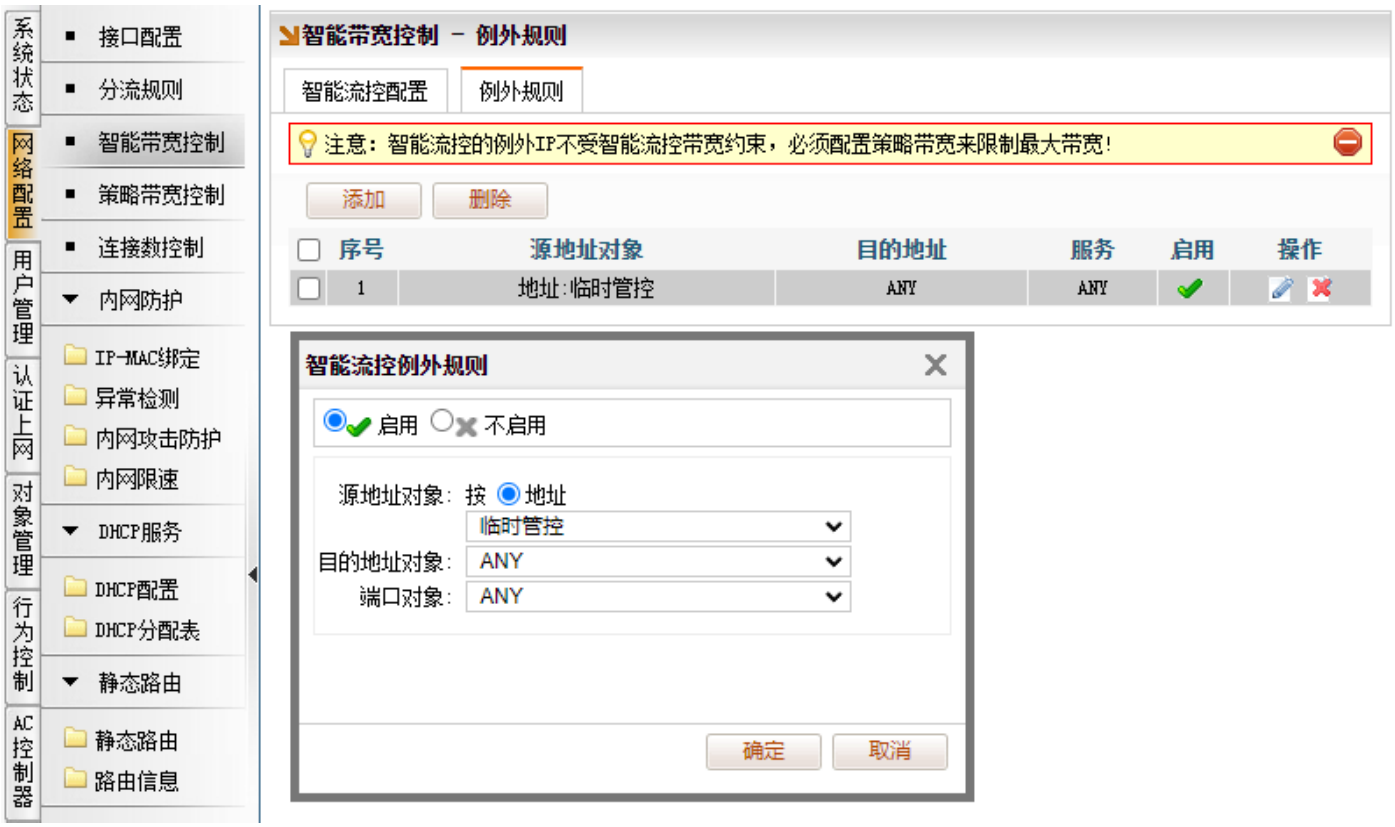
警告：配置智能流控例外的 IP 地址，优先级会大于智能流控下的 IP。比如 100M 专线的网吧，有 50 个客户机同时下载，人均带宽 200KB，当配置了智能流控例外规则，比如例外了 192.168.1.240，在没配置策略带宽控制，约束 192.168.1.240 的前提下，只要 192.168.1.240 有流量开销，其他客户机都会给 192.168.1.240 让出速度，如果耗光 100M 专线的带宽，网吧其他客户机将卡顿，甚至断网。

使用智能流控例外规则的场景，通常是带宽比较紧张的网吧。比如网吧只有一条 100M 专线，当用网高峰时间段，智能流控动态限速，人均带宽差不多为 300KB~400KB。此时游戏更新的速度上不去，恰好有某个重要的游戏需要紧急更新，网吧才能正常运行。急需给游戏更新服务器腾出速度，保证更新速度。配置方法如下：

[对象管理]→[基本对象]→[地址对象]，添加地址对象，比如命名为“临时管控”，填入需要被管

控的 IP/IP 段。比如下图定义了临时管控的地址对象为 192.168.1.240。

[网络配置]→[智能带宽控制]→[例外规则]，添加智能流控例外规则，源地址对象，选择“地址-临时管控”，点击确定。



[网络配置]→[策略带宽控制]，添加带宽控制规则，源地址对象，选择“地址-临时管控”，填入要限速的上行，下行带宽。比如下图限速该临时管控的 IP 上行带宽不超过 2000KB；下行不超过 8000KB。（如需精确到在每个 WAN 口上的限速，请参考 6.2 章节中，高级功能的讲解）

添加的规则会自动排序，“源地址对象--地址-临时管控”的限速规则 1，优先匹配。该 IP/IP 段的速度不受规则 2 影响。

解释说明为什么要对智能流控例外的 IP 地址（以下简称“例外 IP”）配置策略带宽控制。由于例外 IP，优先级大于其他客户机，当例外 IP 地址有流量开销，其他客户机会为其腾出速度，如果耗光线路带宽，网吧其他客户机将卡顿，甚至断网。以 100M 专线网吧为例，配置例外 IP 后，通过配置策略带宽控制规则，限速例外 IP 速度不超过 80M，预留 20M 的带宽给网吧客户机用，尽可能避免网吧其他客户机卡顿，甚至断网。

7，连接数相关功能讲解

7.1，需不需要更改默认的连接数控制规则

[网络配置]→[连接数控制]，默认配置了对内网任意 IP 的连接数限制，TCP、UDP 连接数各限制不超过 5000 个并发连接。

说明：通常，客户机的用网连接数开销，普遍是 100-1500 之间波动，个别客户机开了 P2P 下载，可能连接数开销多至 1000-3000，因此，TCP、UDP 连接数各限制不超过 5000 个的默认值已经很大了，能满足日常的需求。

默认配置的连接数限制，主要是为了防止中毒的客户机，无节制的建立连接，开销系统资源。由于连接数的开销会消耗内存，内存一旦耗光容易引起程序异常，所以该默认规则通常不建议删除。

如果存在个别机器需要更多的连接数，比如收费机安装了某些增值软件服务端，开销超过 5000 个连接。可以再添加连接数控制规则，单独给此类机器，单独放大连接数限制。如下图所示：

备注：配置连接数控制规则，连接数控制的最小值为 1000，填入低于 1000 的数值仍以 1000 为准值。

7.2，如何查看每个机器的连接数和链接跟踪表

[系统状态]→[用户状态]→[网络连接状态]，可以看到每个 IP 地址当前的 TCP 连接数、UDP 连接数、以及总连接数的统计。

通过点击标题栏，可以进行排序处理，如下图是点击“总连接数”排序的结果。

序号	IP地址	用户	TCP连接数	UDP连接数	总连接数↓
1	192.168.5.100	—	925	518	1443
2	192.168.0.125	—	231	149	380
3	192.168.0.73	—	122	232	354
4	192.168.0.131	—	68	94	162
5	192.168.0.109	—	74	71	145
6	192.168.0.111	—	86	49	135
7	192.168.0.114	—	65	60	125
8	192.168.0.76	—	90	23	113
9	192.168.0.19	—	40	69	109
10	192.168.0.99	—	43	65	108
11	192.168.0.107	—	33	58	91
12	192.168.0.71	—	44	44	88
13	192.168.0.10	—	23	55	78
14	192.168.0.14	—	15	58	73
15	192.168.0.81	—	21	49	70
16	192.168.0.112	—	21	49	70
17	192.168.0.29	—	25	41	66
18	192.168.0.38	—	11	47	58
19	192.168.0.39	—	13	43	56
20	192.168.0.201	—	37	13	50
21	192.168.0.200	—	43	5	48
22	192.168.0.93	—	39	7	46
23	192.168.0.28	—	39	6	45
24	192.168.0.204	—	38	7	45
25	192.168.0.69	—	6	38	44
26	192.168.0.241	—	23	17	40
27	192.168.0.27	—	35	4	39
28	192.168.0.12	—	26	5	31
29	192.168.0.92	—	18	12	30
30	192.168.0.244	—	7	1	8

点击 IP 地址的超链接，可查看链接跟踪表（百为路由界面的“流量曲线”、“用户流量”、“在线 IP 表”、“网络连接状态”，如有提供 IP 地址的超链接，均可以展开查看链接跟踪表）

下图举例展开“192.168.0.125”的链接跟踪表，并查看协议“英雄联盟”详情。可观察到“英雄联盟”其中的对战连接，走了 eth1[电信 40M] 的专线出去，连了“59.36.127.155”的服。

7.3，为什么网络连接状态的连接数统计和链接跟踪表的统计不一样

答：链接跟踪表展示的是已经建立成功的连接，即有效链接，比如 TCP 出于 sync 连接状态，没建立成功的连接将不被统计。UDP 的 DNS (UDP 53 端口) 的连接非常多，并且建立的快，消亡的也快，链接跟踪表过滤不显示，也不统计。

7.4，接口状态显示的连接数的参考意义

[系统状态]→[接口状态]，可查看到每个线路的活跃连接数，表示百为路由与运营商建立的连接。

对于多数家庭宽带，可能运营商会禁止用于商用场景，以限制并发连接的方式，来控制台数。一旦上网的连接数开销，超过运营商的上限，可能会出现各种问题，比如网页打不开，视频卡顿，游戏无法登录等等……

特别是家庭宽带，分配的 IP 地址属于私网 IP，即保留地址，多数会限制并发连接。保留地址主要有以下四类：

A 类	10.0.0.0 - 10.255.255.255
A 类	100.64.0.0 - 100.127.255.255
B 类	172.16.0.0 - 172.31.255.255
C 类	192.168.0.0 - 192.168.255.255

所以，以网吧为例，通过观察接口状态的连接数，结合网吧的使用情况。比如宽带的连接数使用接近 3000 个的时候，线路质量提示为“良”，或者提示为“差”，并且此时网吧的网络使用出现异常，打不开网页，进不了游戏等等。从而大概可以猜测运营商限制并发连接可能是 3000 个左右。

结论：接口状态显示的连接数更多用于推测家庭宽带是否有限制并发连接，大概限制多少并发连接。从而指引用户，需要不需要增加宽带来平摊并发连接数。

7.5，运营商限制了家庭宽带的连接数能否通过路由解决

答：运营商限制了家庭宽带的连接数导致的上网问题。通常需要增加宽带的数量，来缓解。如果有专线固定 IP (商用) 接入，路由可以尝试分流“耗费连接数且不耗费大流量的业务”走专线，比如 DNS、游戏的业务走专线，来缓解家庭宽带的并发连接的开销。

有用户疑问，运营商限制了家庭宽带的连接数导致的上网问题，能否通过路由也限制客户机的连接数，来缓解?

关于这个问题，得这么理解，既然运营商因为限制连接数才导致的上网问题，比如网页打不开，游戏进不了。如果百为路由也去限制客户机的并发连接，相当于这个限制的动作，下放到客户机层面，比如限制客户机的连接数为 500。那客户机用光 500 个连接后，该客户机一样也会有上网问题。所以不建议限制小客户机的连接数。

8，防火墙相关功能讲解

8.1，百为路由防火墙功能的用途

[行为控制]→[防火墙]，提供的防火墙规则配置。主要用于禁止内网主机访问外网的行为，以及禁止路由网口之间的互访行为。不支持对外网主机访问路由行为的拦截。

防火墙规则的配置项目说明：

源地址对象	地址	表示内网 IP 地址，可以自定义单个 IP、IP 段，也可以用 ANY 表示所有内网 IP。
	用户	[用户管理]→[用户对象] 的成员
	部门	[用户管理]→[用户对象] 的成员所关联的部门
	级别	[用户管理]→[用户对象] 的成员所关联的级别
时间对象	表示时间范围，可以自定义某个时间段，也可以用 ANY 表示任意时间。	
目的地址对象	表示目的 IP 地址，可以自定义单个 IP、IP 段，也可以用 ANY 表示所有 IP。目的 IP 地址通常指外网 IP，也可以是路由器其他 LAN 口下的 IP。	
端口对象	表示目的端口，可以自定义单个端口号、端口范围，也可以用 ANY 表示所有端口。	
应用类型	表示[对象管理]→[应用对象]→[应用分类]里的 17 个分类，每一个分类可以用于“装载”进程对象、目录对象、协议对象、地址端口对象	

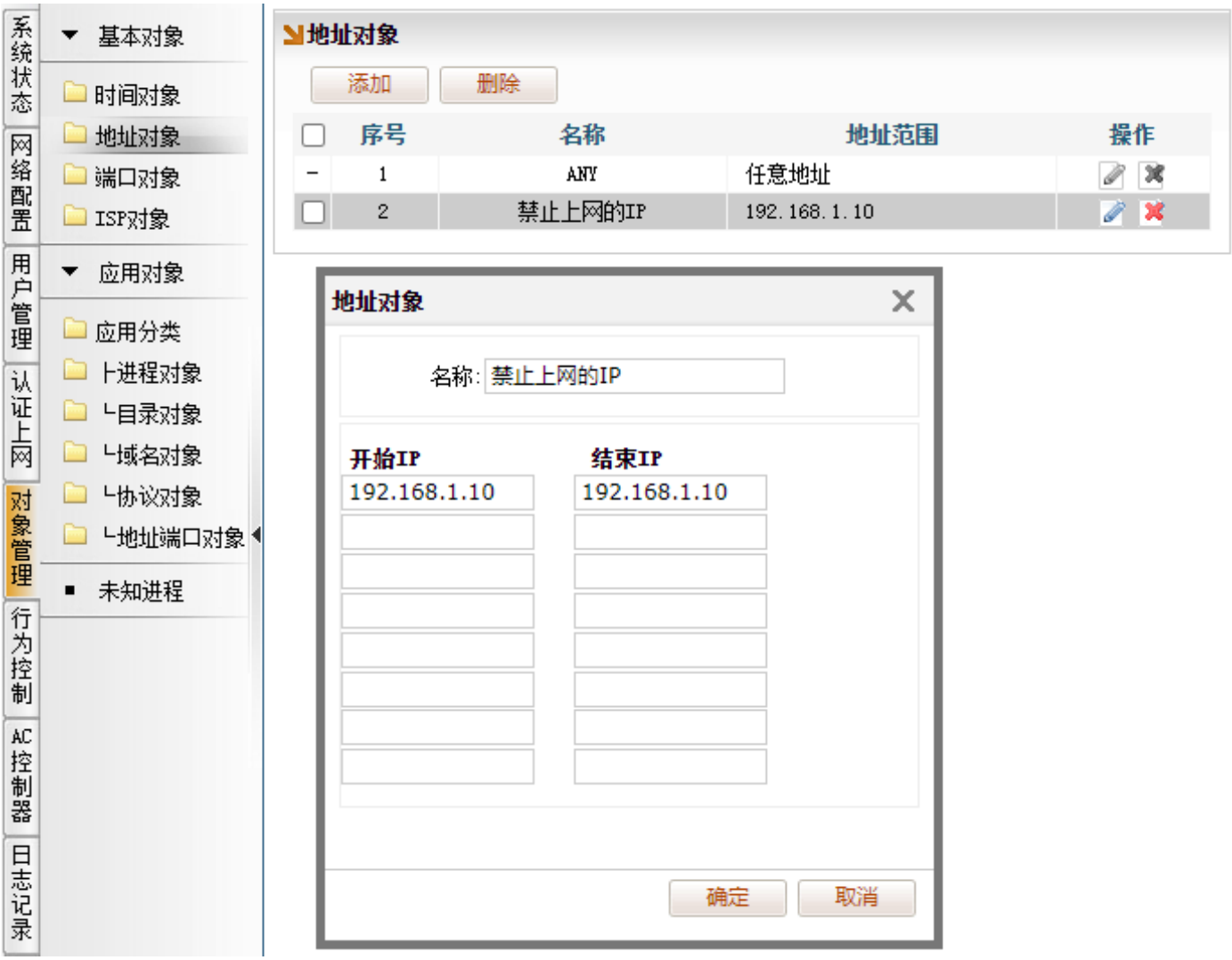
可以把源地址对象、时间对象，目的地址对象、端口对象、应用类型，理解为“条件”，通过条件的组合，勾选相应的 WAN 口，可以实施“放行”或者“直接阻止”，

注意：防火墙规则遵循匹配顺序原则，比如，规则 A-禁止内网某个客户机上网，规则 B-放行所有人上网，如果规则 B 置于规则 A 之上，则规则 A 无效。因此需要注意规则匹配的顺序，以及规则条件包含的范围。

8.2，禁止内网某个 IP 或者用户上网

禁止内网某个 IP 上网

[对象管理]→[地址对象]，添加，比如名称为“禁止上网的 IP”，填入内网需要禁止上网的 IP 地址



[行为控制] →[防火墙]→[防火墙规则]，添加，源地址对象-地址，选择“禁止上网的 IP”、“时间对象”、“目的地址对象”、“端口对象”、“应用类型”均为“ANY”，勾选外网线路，策略为“直接阻止”，点击确定。

设置完毕，192.168.1.10 机器无法上网。

禁止某个用户上网

[用户管理]→[用户对象]，用户通常是用于小区宽带，Portal 认证，VPN 用户，比如需要禁止小区宽带里 A1001 用户上网。

[行为控制]→[防火墙规则]，添加，源地址对象-用户，选择“A1001”这个用户，“时间对象”、“目的地址对象”、“端口对象”、“应用类型”均为“ANY”，勾选外网线路，策略为“直接阻止”，点击确定。

设置完毕，“A1001”这个用户无法上网。

8.3，禁止外网某个 IP

[对象管理]→[地址对象]，添加，比如名称为“广告 IP”， 填入需要禁止的 IP 地址

[行为控制] →[防火墙]→[防火墙规则] ，添加，目的地址对象，选择“广告 IP” ，“源地址对象”、“时间对象”、“端口对象”、“应用类型”均为“ANY” ，勾选外网线路，策略为“直接阻止” ，点击确定。

设置完毕，被禁止的目的 IP 19.18.17.16 将无法访问。

8.4，禁止外网某个端口

[对象管理]→[端口对象]，添加，比如名称为“广告端口”， 填入需要禁止的端口或者端口范围。

[行为控制] →[防火墙]→[防火墙规则] ，添加，端口对象，选择“广告端口”，“源地址对象”、“时间对象”、“目的地址对象”、“应用类型”均为“ANY”，勾选外网线路，策略为“直接阻止”，点击确定。

设置完毕，被禁止的目的端口 65500 将无法访问。

8.5，禁止某个域名解析后的 IP

说明：使用防火墙的方式禁止域名，DNS 解析的动作并不阻止，而是禁止访问域名解析后的 IP 地址。本篇幅的教材仅作为禁止域名的备选方案，更高效快捷的禁止域名手段用“域名跳转”来实现。

原因：在各种云加速，云机房等广泛应用下，不同的域名，有可能域名解析后指向同一个云加速平台的 IP。即存在多个不同域名，解析后的 IP 可能一样。如果用防火墙的方式进行阻止 IP，可能存在误杀其它域名的可能。

使用防火墙禁止域名配置方法如下：

比如色情网站 www.sexxxx.com，解析的 IP 地址为 67.22.42.5。

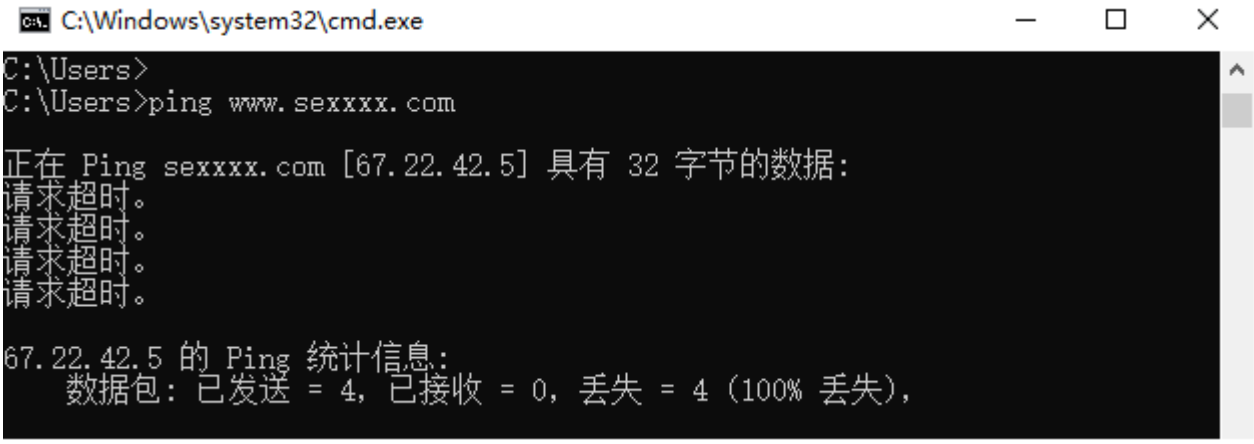
[对象管理]→[应用对象]→[域名对象]，点击“添加”，填入要禁止的域名、备注，选择所属分类，比如选择为“自定义 1”。

注意：填入域名，sexxxx.com，表示匹配 sexxxx.com 结尾的，即 www.sexxxx.com，aaa.sexxxx.com，bbb.sexxxx.com ..... 都被包含了。如果需要精确匹配的话，则需要填入完整的域名，比如 aaa.hhh.sexxxx.com

[行为控制] →[防火墙]→[防火墙规则]，添加，应用类型，选择“自定义 1”，“源地址对象”、“时间对象”、“目的地址对象”、“端口对象”均为“ANY”，勾选外网线路，策略为“直接阻止”，点击确定。

设置完毕，被禁止的域名 www.sexxxx.com 将无法访问。

备注：通过防火墙禁止域名后，ping 被禁止的域名，依然能解析到 IP。但防火墙已经实施 IP 的拦截，如下图测试所示，已经为 ping 不通。



8.6，禁止某个协议

比如企业不允许员工 QQ 聊天，需要单独禁止腾讯 QQ 协议

[对象管理]→[应用分类]→[协议对象]→[IM]，选中“腾讯 QQ”，修改“所属分类”为“自定义 1”，点击确定。

[行为控制] →[防火墙]→[防火墙规则] ，添加，应用类型，选择“自定义 1” ，“源地址对象”、“时间对象”、“目的地址对象”、“端口对象” 均为“ANY” ，勾选外网线路，策略为“直接阻止” ，点击确定。

设置完毕，腾讯 QQ 将无法正常使用。

8.7，禁止外网某个 IP+端口

[对象管理]→[地址对象]，添加，比如名称为“广告 IP”， 填入需要禁止的 IP 地址

[对象管理]→[端口对象], 添加, 比如名称为“广告端口”， 填入需要禁止的端口或者端口范围。

[行为控制] →[防火墙]→[防火墙规则] ，添加，目的地址对象，选择“广告 IP” ，端口对象，选择“广告端口” ，“源地址对象”、“时间对象”、“应用类型”均为“ANY” ，勾选外网线路，策略为“直接阻止” ，点击确定。

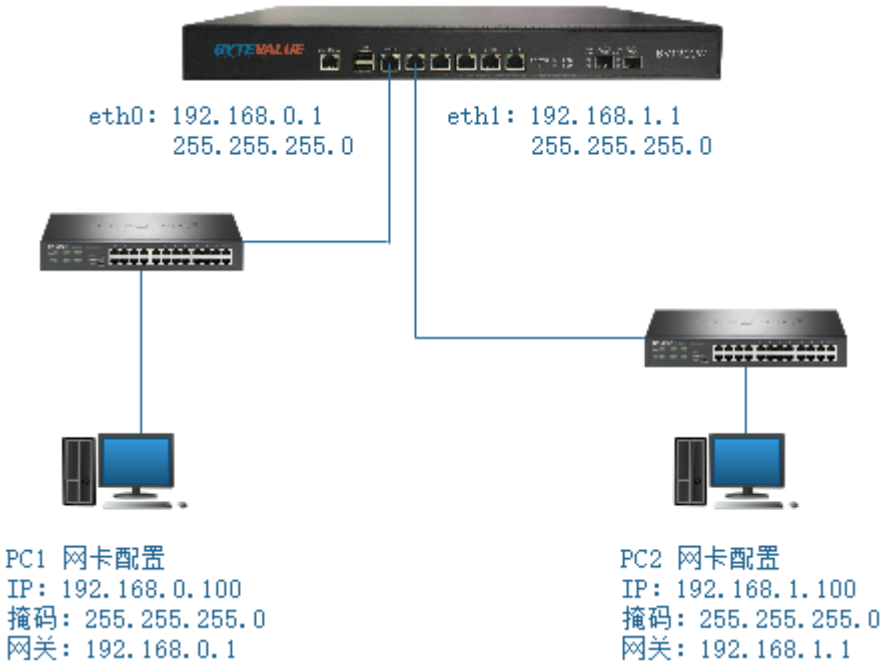
设置完毕，被禁止的目的 IP 19.18.17.16 的 65500 端口将无法访问。

说明：防火墙配置，匹配了“目的地址对象”和“端口对象”实施禁止策略，属于精确了禁止的范围。表示只禁止目的 IP 的相关端口的业务。

8.8，禁止两个内网口的网段互访

说明：百为路由无论是原厂硬件还是软路由，所有 LAN 口都属于独立的网段，默认情况下，不同 LAN 口之间的网段支持互访（路由转发形式实现）。

举例同一路由下，eth0（LAN 口）接到 A 网吧交换机，eth1（LAN 口）接到 B 网吧交换机。A 网吧的 PC1 能与 B 网吧的 PC2 互通。具体配置如下图所示。



如需禁止两个网段互访，需要配置防火墙规则来实现。

[对象管理]→[地址对象]，添加，0 段和 1 段的地址范围，点击“确定”

[行为控制]→[防火墙规则]→[功能启用],添加，添加两条规则

规则 1：“源地址对象”选择“地址---0 网段”、“目的地址对象”选择“地址---1 网段”、“时间、端口、应用类型”均为“ANY”，勾选外网线路。策略为“直接阻止”。

规则 2：“源地址对象”选择“地址---1 网段”、“目的地址对象”选择“地址---0 网段”、“时间、端口、应用类型”均为“ANY”，勾选外网线路。策略为“直接阻止”。

设置完毕，0 网段和 1 网段将无法互通。

备注：由于防火墙界面配置的约束，必须勾选 WAN 口才能完成配置，示例中由于配置有目的地址对象的指向性。规则生效后依然不影响源地址对象的正常上网。

9，认证上网相关功能讲解

9.1，列举 4 种认证上网讲解说明

百为路由提供 4 种类型的用户认证

PPPoE 认证	用于小区宽带，内网用户通过 PPPoE 拨号上网。拨号的帐号密码在路由上创建（对接 radius 计费的，需 radius 计费系统上创建	
Portal 认证	一键认证	用于酒店，宾馆防止有针孔摄像头连接 WIFI 联网。需要多一个人工点击步骤。相当于自助点击放行使用
	WEB 密码认证	连上路由的用户（比如手机），通过弹出的认证窗口，输入用户名密码上网。 WEB 密码的帐号密码在路由上创建（对接 radius 计费的，需 radius 计费系统上创建）
	短信认证	通过输入手机号码，短信平台发送随机密码认证上网（要求用户购买短信网关与之配合，目前对接网易 163 的短信平台）
	动态密码认证	用于网吧，客户机通过一个特定的网页，或者小软件，打开后获得一个随机密码， 连上路由的用户（比如手机），通过弹出的认证窗口，输入随机密码上网
IP 认证	用户的电脑，直接配置好的 IP 地址直接上网。路由创建该 IP 地址，作为为 IP 认证的用户，认证上网 （建议配合 IP-MAC 绑定，防止 IP 盗用）	
MAC 认证	用户的电脑，直接配置好的 IP 地址直接上网。路由创建该 MAC 地址，作为为 MAC 认证的用户，认证上网 （MAC 认证不支持跨三层）	

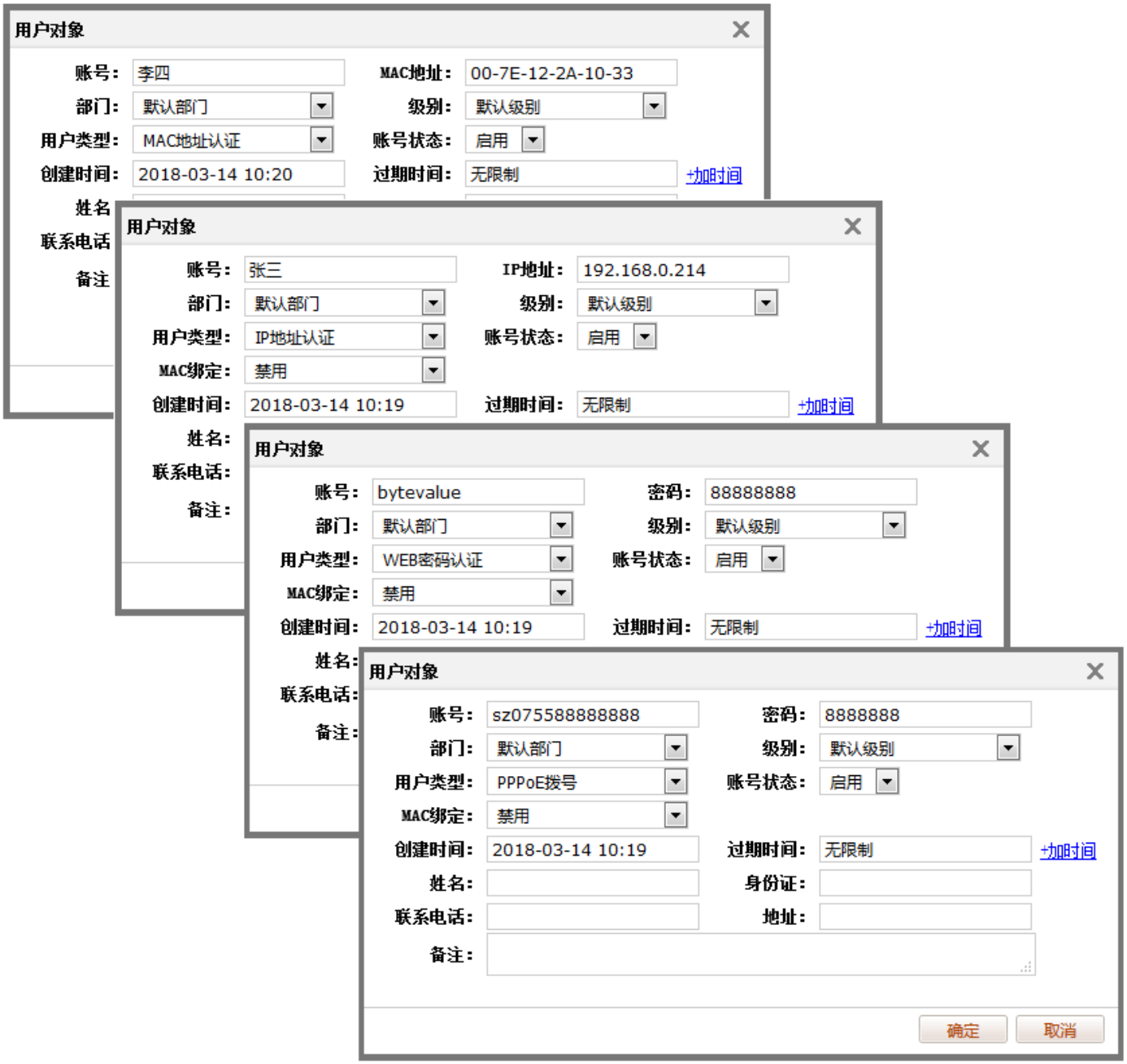
认证白名单---在开启认证的前提下，对指定地址段直接放行，只要配置指定地址段内的 IP 的电脑。无需认证。

如下图所示：eth1 比如是内网口，开启认证开关，允许四种类型的用户认证上网。

注意：只要开启其中任意一个开关，即表示对 eth1 的口，进行拦截。必须通过认证的用户，才允许上网

网吧用户使用该功能需特别注意，切勿对提供网吧上网的内网口，直接开启认证（除非是做了认证白名单放行了网吧客户机和服务器的 IP）

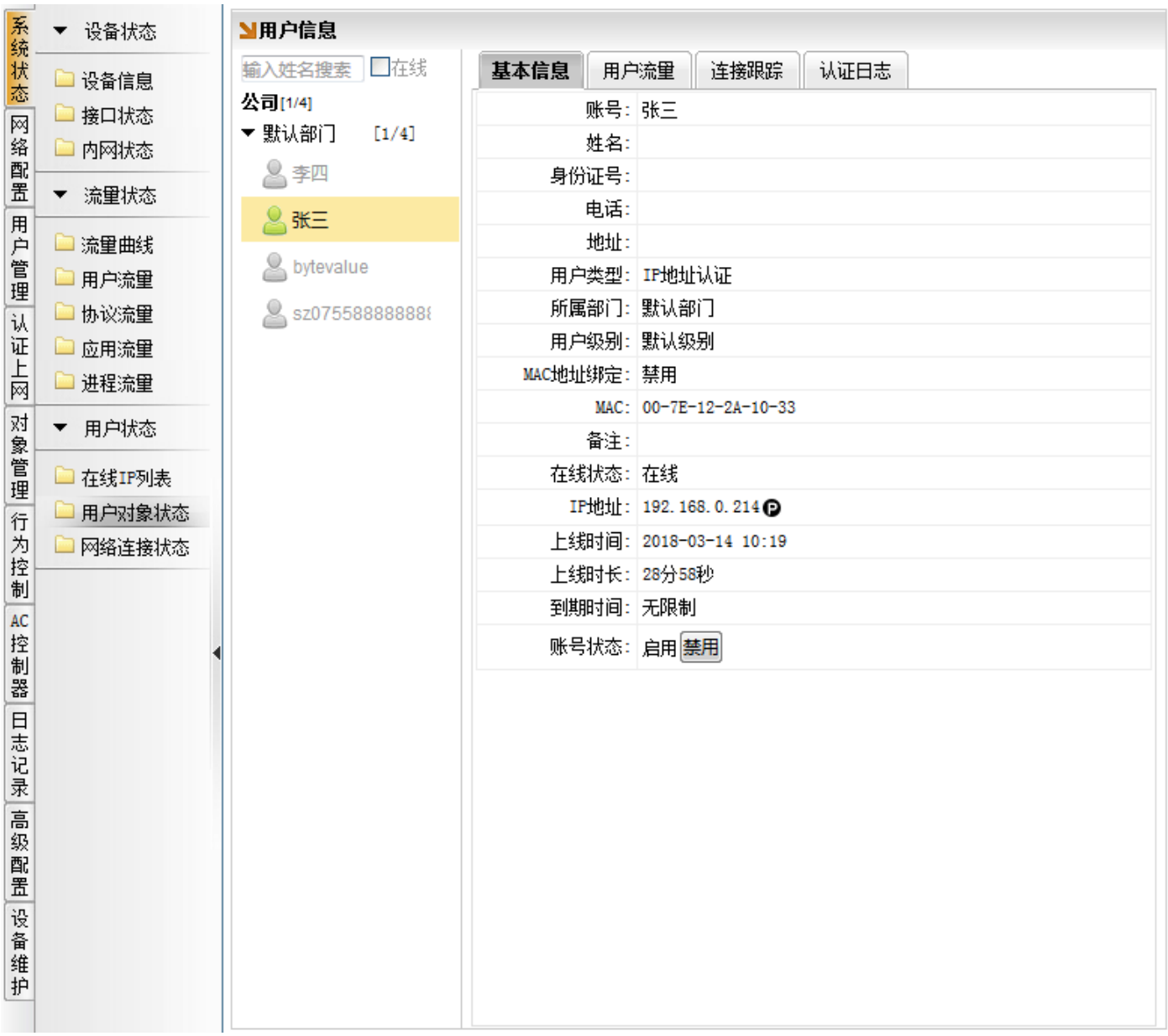
[用户管理]→[用户对象]，添加用户。下图添加的为四种类型的用户。



IP 认证

配置客户机网卡 IP 地址为 192.168.0.214，网关为 eth1 口的 IP，即可直接上网。

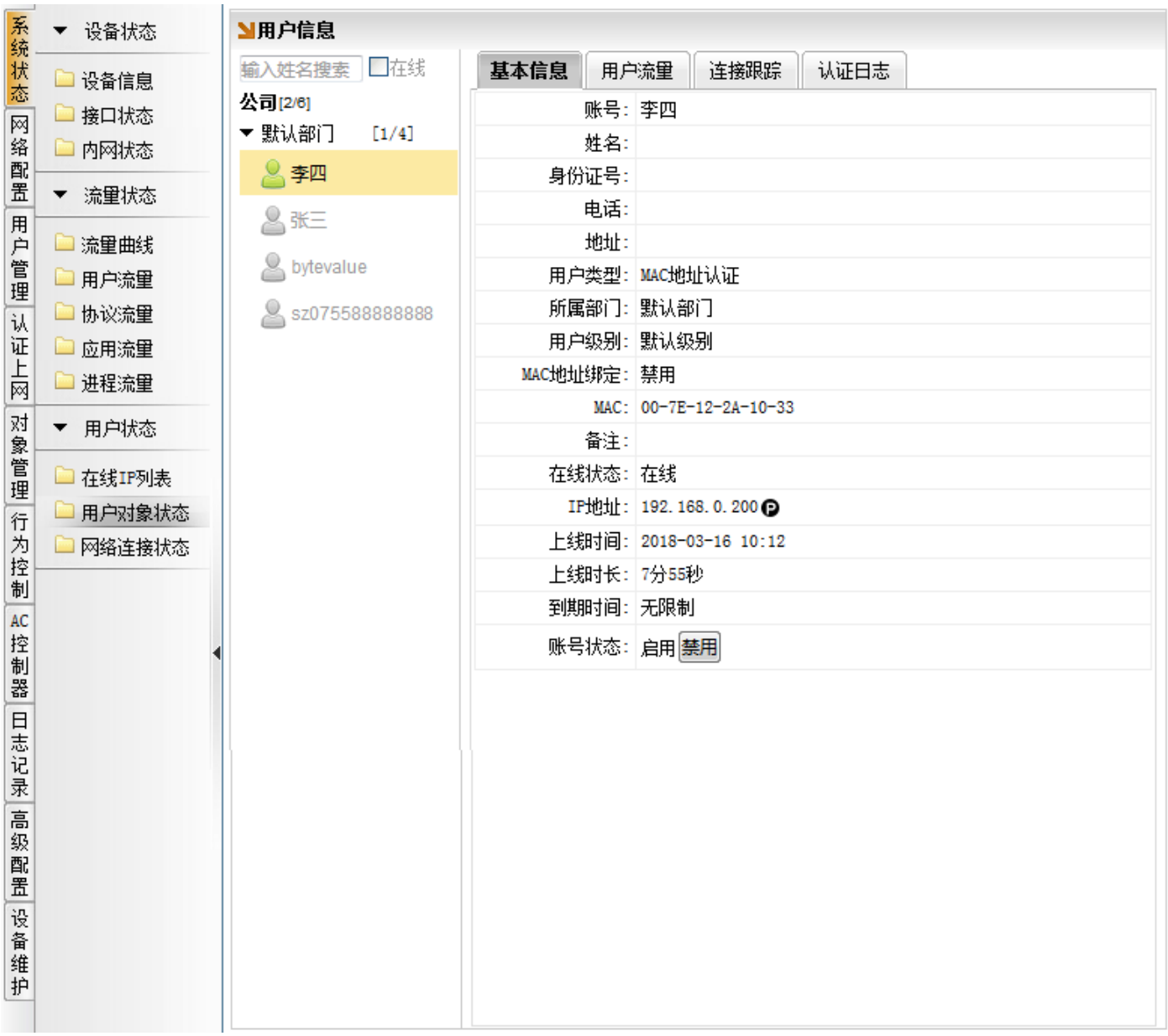
在[系统状态]→[用户对象状态]→[用户信息]，可看到用户上线，表示 IP 认证用户，允许上网。



MAC 认证

客户机配置和 eth1 同个网段的 IP 地址，网关为 eth1 口的 IP，即可直接上网。

在[系统状态]→[用户对象状态]→[用户信息]，可看到用户上线，表示 MAC 认证用户，允许上网



PPPoE 认证

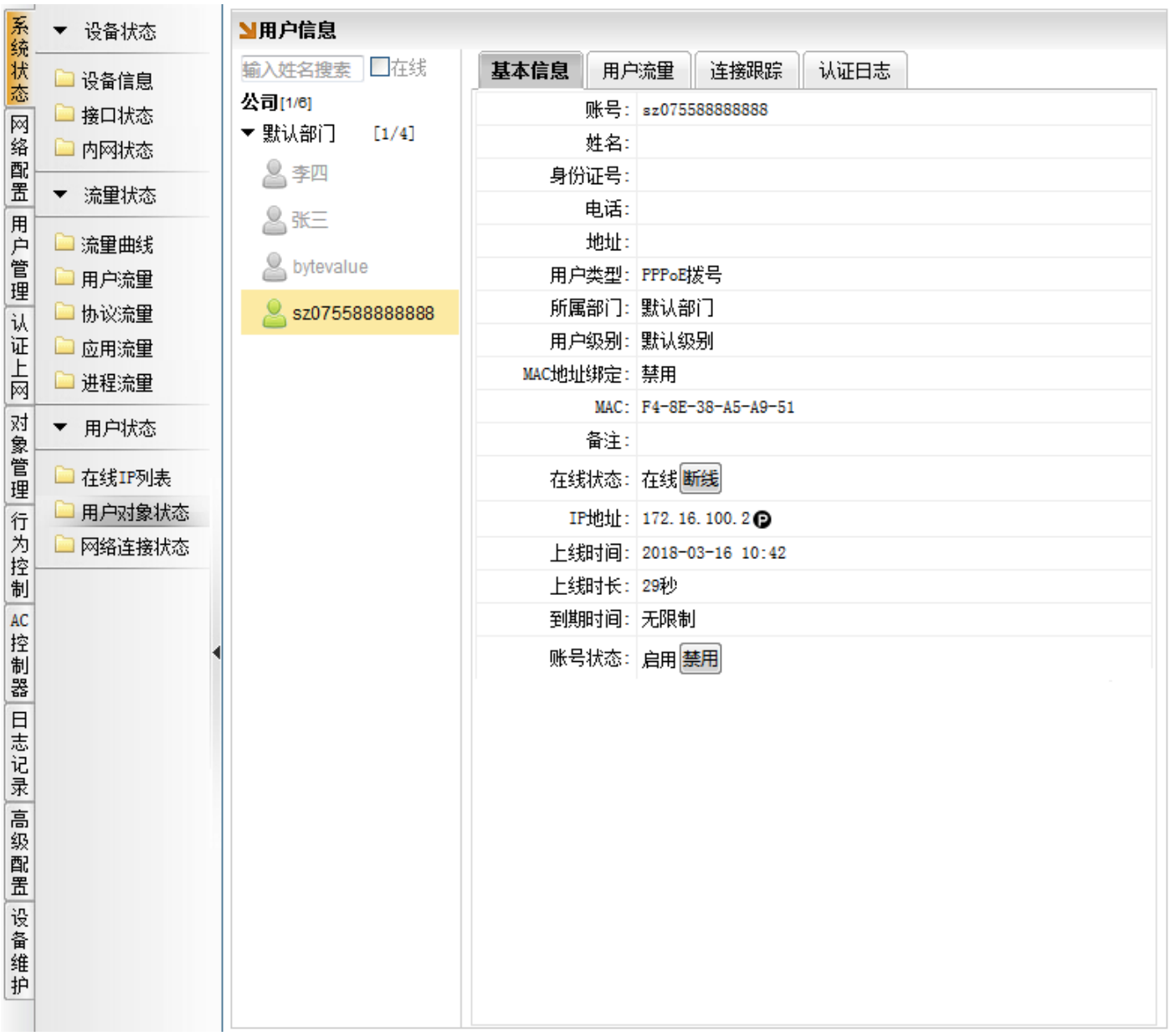
[认证上网]→[PPPoE 认证]→[PPPoE 服务]，开启 eth1 口的 PPPoE 服务，填入分配的地址池以及 DNS

说明：地址池的分配，建议用局域网地址，不能和 eth1 口的 IP 同网段。比如 eth1 口的 IP 是 192.168.1.1。此处地址池不能为 192.168.1.xxx。DNS 建议分配当地运营商的 DNS。

客户机宽带拨号

成功拨号后即可上网。

在[系统状态]→[用户对象状态]→[用户信息]，可看到用户上线，表示 PPPoE 认证用户，允许上网。

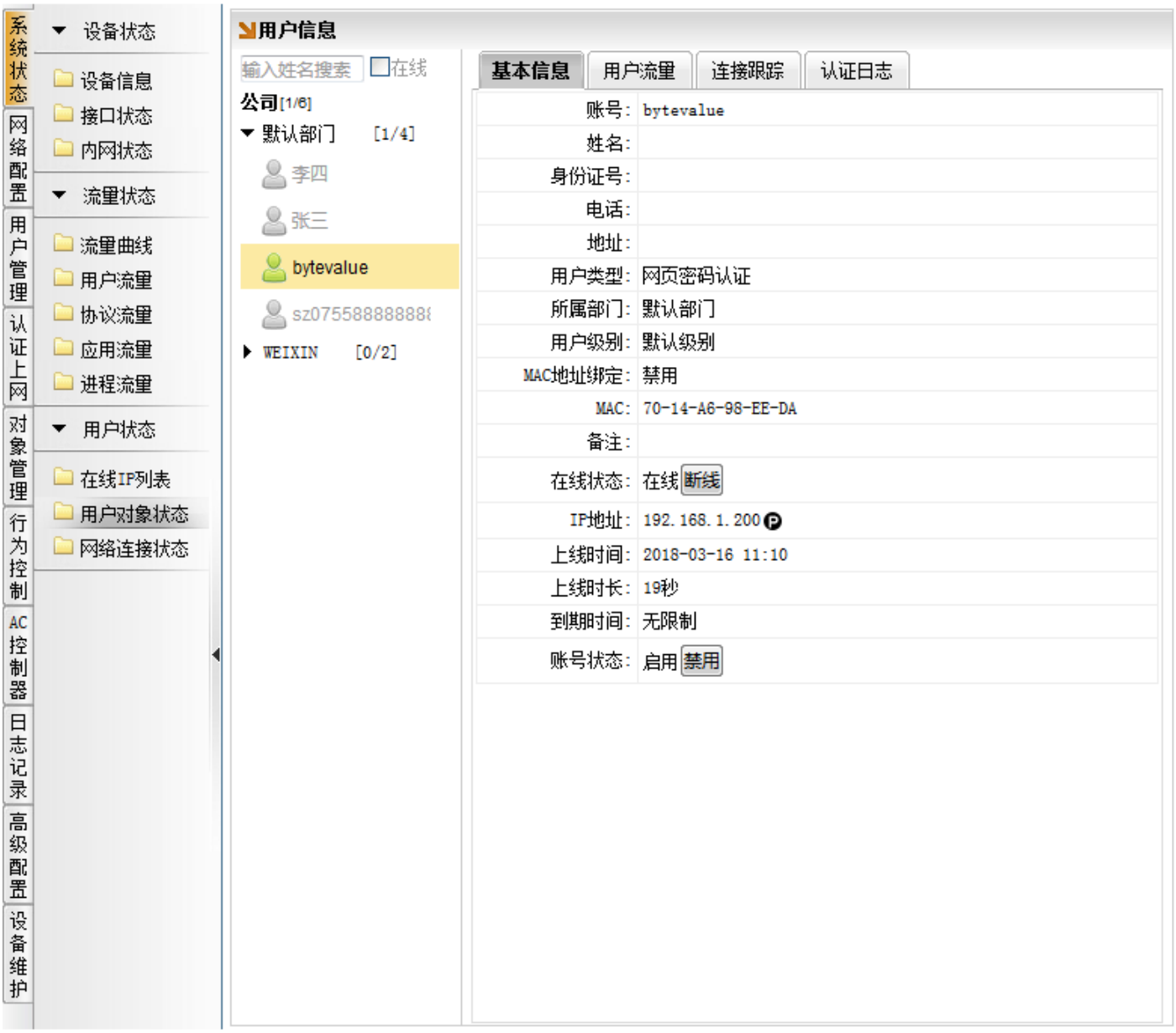


Portal 认证

[认证上网]→[Portal 认证]→[Portal 服务]→[认证选项]，开启 WEB 密码认证，保存

手机连接无线，弹出认证框，选择 WEB 密码认证，输入帐号、密码，认证上网

在[系统状态]→[用户对象状态]→[用户信息]，可看到用户上线，表示 Portal 认证用户，允许上网。



认证白名单

比如 eth1 已开启了认证，有多台服务器需要放行。服务器群的 IP 段为 192.168.1.240---192.168.1.250。[认证上网]→[认证白名单]，点击添加，选择地址对象。（点添加图标，定义所需的地址段）

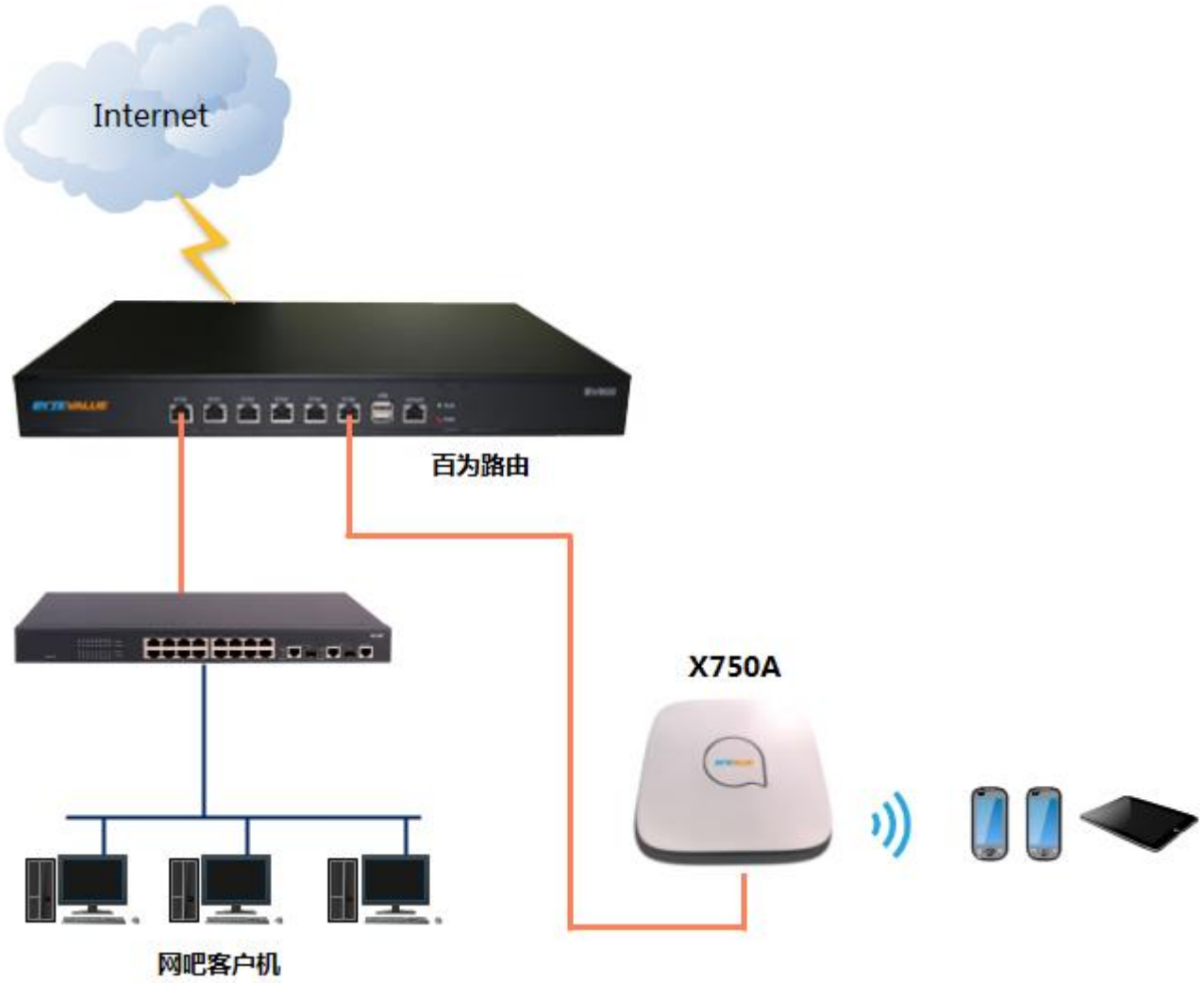
加入到白名单的地址段，直接放行，无需认证

9.2，举例网吧用的动态密码认证怎么使用

动态密码认证：是指网吧的上网用户，手机连接无线后，输入由客户机生成的随机密码，认证上网，用户离开网吧下机，也结束掉该用户的无线认证。

单独提供一个网口，作为 LAN 口，用于接无线 AP

以下拓扑表示，百为路由的 LAN 口 eth5，连接无线 AP（推荐使用 X750A ），eth0 接网吧客户机



动态密码认证相关配置 （以 eth5 口为例），开启 DHCP 给手机等无线终端分配 IP 地址

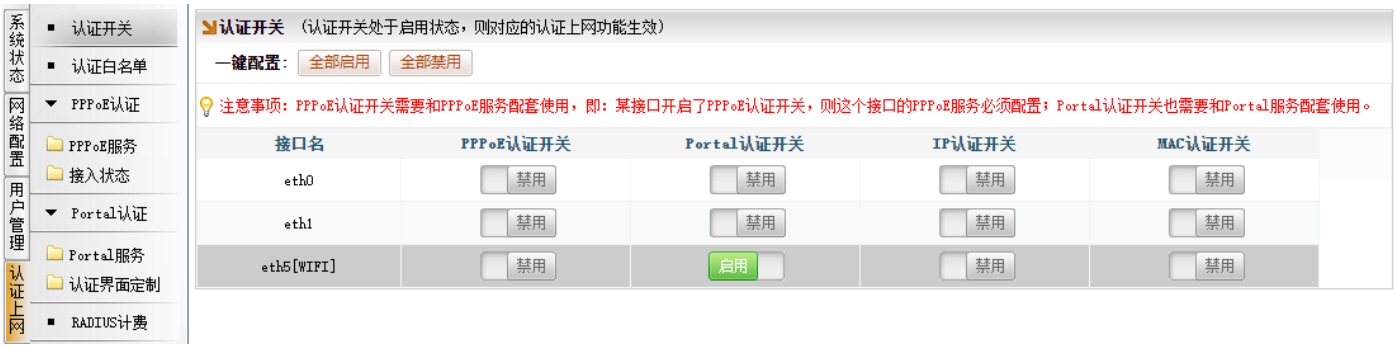
比如百为路由 eth5 口 单独接有交换机，从交换机分到多个无线 AP 。（注意，必须使用 AP，不能使用无线二级路由；建议使用百为无线 AP X750A 更便捷管理）

[网络配置]→[DHCP 服务]→[DHCP 配置]，分配对应 eth5 网口 IP 的地址池，以及分配的 DNS（建议配置当地运营商 DNS）。

开启 eth5 口 Portal 认证

[认证上网]→[认证开关]，开启 eth5 口的 Portal 认证。注意：只要开启其中任意一个开关，即表示对 eth5 的口，进行拦截。必须通过认证的用户，才允许上网。比如用动态密码认证

网吧用户使用该功能需特别注意，切勿对提供网吧上网的内网口，直接开启认证（除非是做了认证白名单放行了网吧客户机和服务器的 IP）



配置动态密码认证

[认证上网]→[Portal 认证]→[Portal 服务]→[认证选项]，启用动态密码认证。保存

[认证上网]→[Portal 认证]→[Portal 服务]→[动态密码认证配置]，WIFI 热点名称，填入无线 AP 的 SSID

打开百为专用的动态密码获取软件

下载连接：http://www.bytevalue.com/uploadfile/firmware/client/DynWebAuth.exe

运行后即可获得密码，并且以任务栏小图标的形式运行

说明：软件默认访问的地址 3.3.3.3。在百为路由下上网的客户机，访问 3.3.3.3，等于百为路由的 LAN 口的 IP。此处可以不作修改。

手机操作无线认证

手机连接无线后，连接后会自动弹出认证页面

选择“动态认证”

输入从客户机，获得的动态密码，点击确认。认证上网.

路由上查看动态密码认证的用户信息

[系统状态]→[用户状态]→[用户对象状态]，查看“默认部门”一栏，即可看到认证成功的在线用户。说明认证成功

常见问题：

1、认证后，刷新下生成动态密码的网页或软件，岂不是多人可以共用？

答：刷新生成出新的动态密码，不影响已认证上的无线用户。如果新生成的动态密码别的手机用，将踢掉之前认证上的用户。一分钟内生效。

2、关掉生成动态密码的网页或软件，已经认证上的手机，多久结束手机上网？

答：关掉生成动态密码的网页或软件，要一分钟后才踢下线，结束手机上网

3、网吧固定人员如何直接使用无线上网？

答复：使用 IP 认证、MAC 认证，认证白名单可达到目的。网吧的网络多数是二层，建议用 MAC 认证。

[认证上网]→[Portal 认证]→[Portal 服务]→[认证选项]，启用 MAC 认证。保存

[用户管理]→[用户对象]，添加 MAC 认证的用户。比如下图

9.3，举例小区 PPPoE 认证上网怎么使用

9.3.1，配置 PPPoE 服务并开启 PPPoE 认证

运营小区宽带为了能让用户能拨号到主路由来，需要开启 PPPoE 服务。

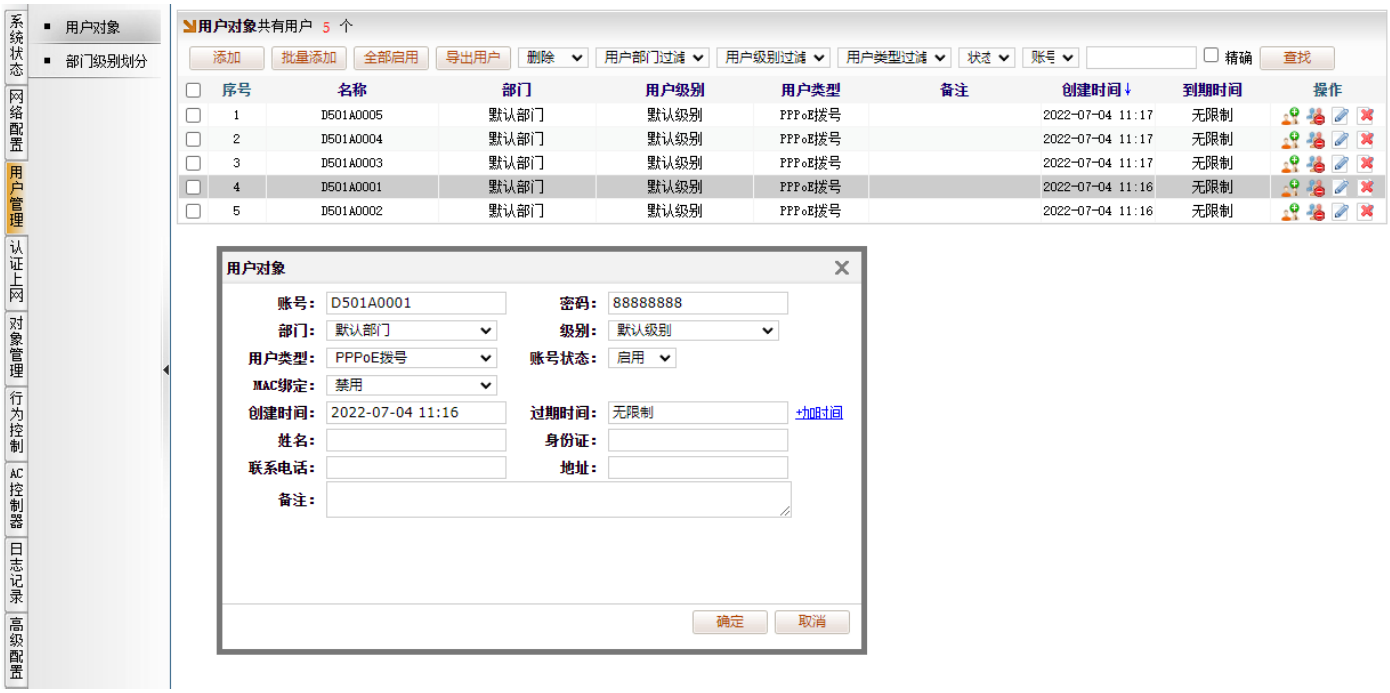
[认证上网]→[PPPoE 认证] →[PPPoE 服务]，选择要开启服务的内网口，比如 eth0 接了内网交换机，选择 eth0，功能启用。

填入分配 IP 范围通常为局域网 IP，但需注意，分配的 IP 范围不能和 LAN 口相同网段，比如 LAN 口 eth0 配置 IP 为 192.168.0.1，PPPo 服务分配的 IP 范围不能是 192.168.0.xxx。

建议用路由默认值，通常用户仅需改动分配的 DNS，比如配置当地运营商的 DNS，也可

配置公共 DNS。

[用户管理]→[用户对象] ，添加用户上网的账号密码，选择用户类型“PPPoE 拨号”，比如下图创建的账号名：D501A0001 ，密码：88888888



为了管控用户只能通过 PPPoE 拨号上网，以及拨号用户的到期限制。需要开启认证上网。

[认证上网]→[认证开关] ，选择 eth0，如下图所示，开启 PPPoE 认证开关

总结说明：开启 PPPoE 服务，是为了应答客户机的 PPPoE 拨号请求，这是一个基础服务。开启 PPPoE 认证开关，是为了筛选客户机通过 PPPoE 拨号到路由的，才允许上网；同时，启用认证上网，会校验拨号用户的到期时间，过期的用户将认证失败。

不开启认证，则客户机随便配置跟 LAN 口同网段的 IP，网关和 DNS 配置对了，则直接上网了。

9.3.2，PPPoE 服务配合计费管理

对接百为计费

百为计费是一款运行于 Windows 上的服务端软件，没有使用标准的 Radius 协议。对接百为计费，用户的增删改操作，均需要在计费端完成。由于是私有协议，在百为计费端的操作，用户列表会同步到路由端的“用户对象”里，小区用户的拨号的认证校验，实则实在路由端完成。由此，即便计费服务端故障了，不通了，一时间也不影响小区用户的拨号认证。

配置方法：

[认证上网]→[RADIUS 计费]，功能启用，选择为“百为计费”

计费线路出口：选择默认 （此处由于 Radius 计费部署在内网，选择默认）

对接类型选择：用于 PPPoE 认证

认证 IP：填写计费服务器的 IP 地址

共享密钥：填入百为计费服务器里的对接密钥

对接第三方 Radius 计费

第三方 Radius 计费，就是用标准的 Radius 协议，用户的增删改，限速、以及踢下线等操作，均计费服务器完成操作，务必保证计费长期开着，保证能与百为路由正常通讯。

Radius 认证配置方法

[认证上网]→[RADIUS 计费]，功能启用，选择为“第三方计费”

计费线路出口：选择默认 （此处由于 Radius 计费部署在内网，选择默认）

对接类型选择：用于 PPPoE 认证

认证 IP：填写计费服务器的 IP 地址

共享密钥：填入 radius 计费服务器里的对接密钥

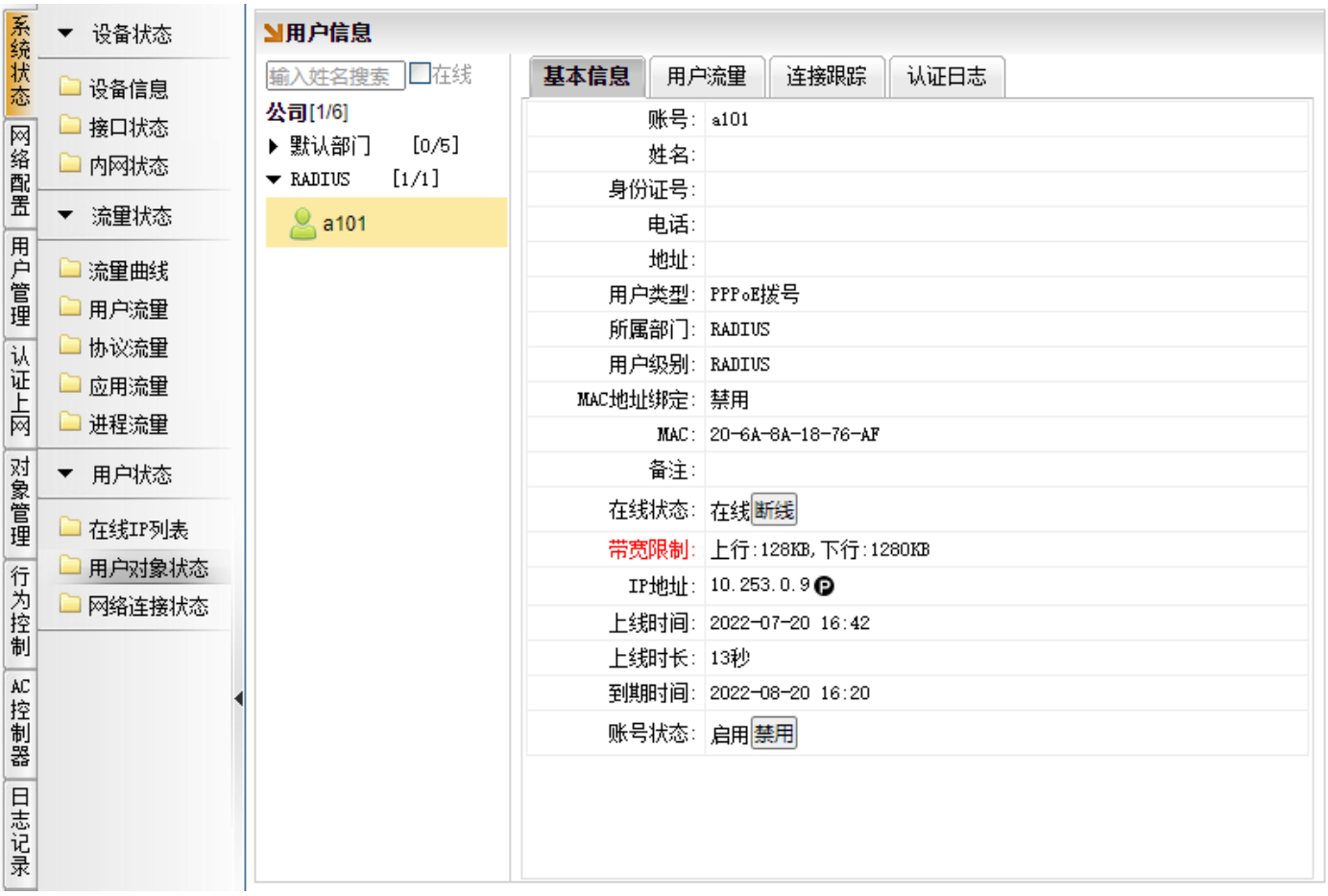
计费标识：计费标识为"凌风计费"独有的标识。用于校验身份。

认证端口：1812

收费端口：1813

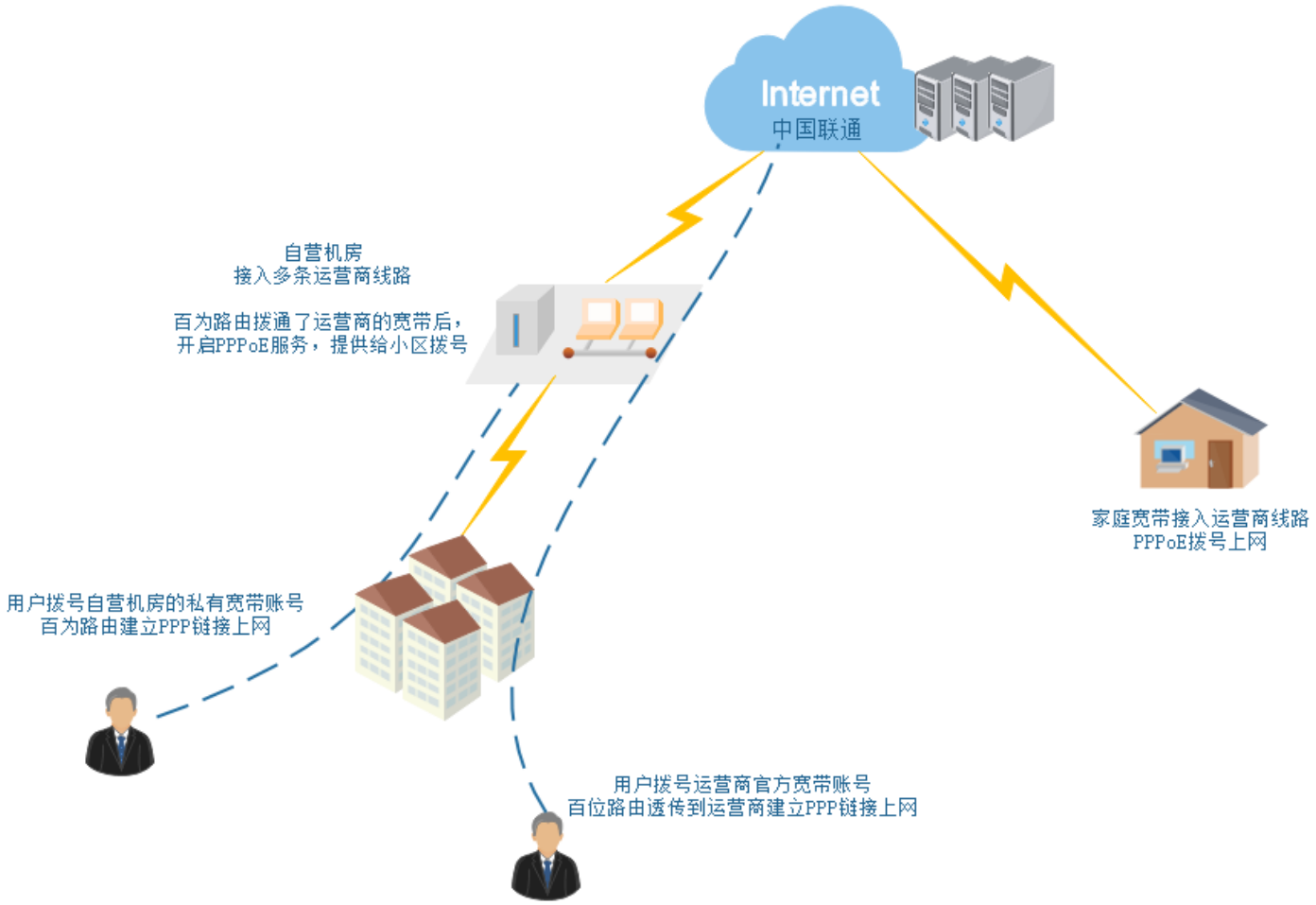
由于 Radius 计费对接成功后，有限速参数的传值。不再需要路由手工配置的限速策略，可以删除。[网络配置]→[策略带宽控制]，清空所有策略

当拨号成功后，可在[系统状态]→[用户状态]→[用户对象状态]，查看到 RADIUS，一栏已经拨号的用户状态信息，以及带宽限制的传值。



9.3.3，PPPoE 透传使用场景以及使用方法

PPPoE 透传，也有称为 PPPoE 代理，或者 PPPoE 代拨。其目的是让客户机原本拨号到主路由的 PPPoE 的数据包，二次呈递到上游的 PPPoE 服务商（通常是运营商），此时主路由只是个负责呈递的角色。



举例使用的场景：

某村网络基础建设由个人承包，村里有 500 户，每户都有光纤接入到机房。机房使用了百为路由，开启 PPPoE 拨号服务，并创建了 500 个账号供 500 户拨号使用。同时，机房接入了 3 路联通光纤，每路光纤带有 100 个联通官方宽带账号，共享光纤 1G 带宽。由此，3 路光纤便是 300 个拨号，3G 带宽。

使用百为路由，接入三路光纤，通过 WAN 口拨号汇聚带宽，再分发到村里每户拨号使用。此时，用户拨号的是百为路由创建的私有账户。有个别用户，需要直接拨号联通官方账号，获得联通的 IP 来使用，可通过配置 PPPoE 透传来实现。

[认证上网]→[PPPoE 透传配置]，功能启用

[认证上网]→[PPPoE 透传配置] →[PPPoE 透传用户管理]

名称：填入的是联通官方宽带账号

认证接口：该宽带账号所属于 eth2 所接的光纤，认证接口选择“eth2”

认证状态：启用

绑定状态：提供 MAC 绑定，只允许该宽带给某个机器用

多播次数：同一个账号可给多个机器拨号，但取决于运营商

过期时间：提供二次定义到期时间，比如运营商的官方宽带账号是三年后到期，该功能可以定义半年后到期，精确到具体时间。

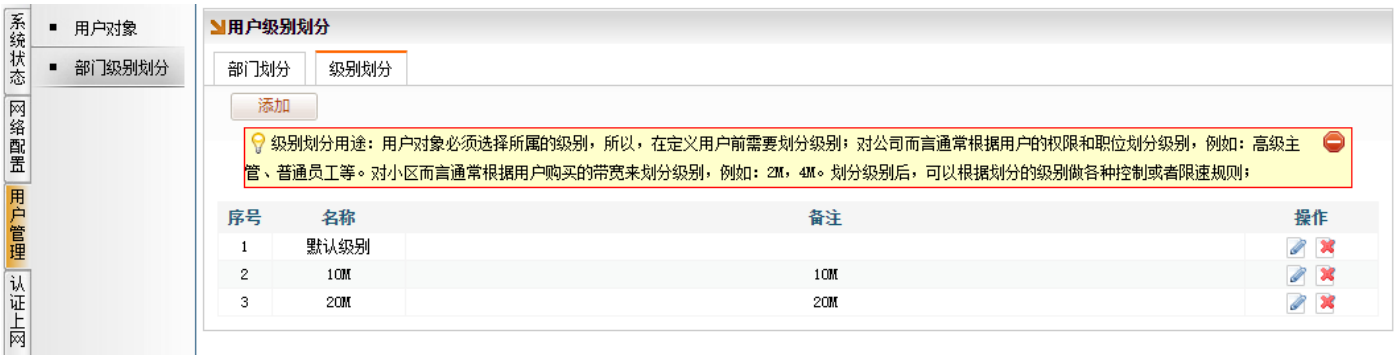
部门，级别：可用于关联限速，图示举例选择了级别为 20M

姓名，身份证，联系电话，地址，备注，仅仅是提供记录和标识作用

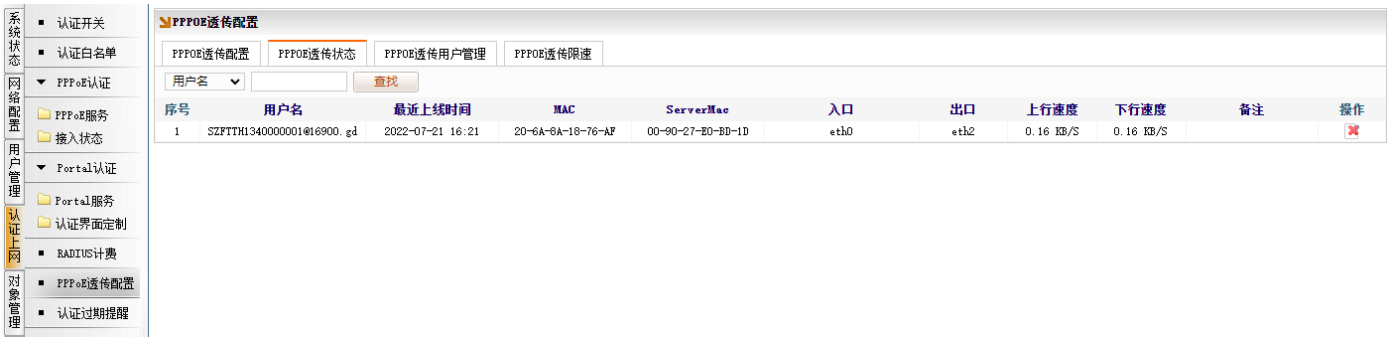
[认证上网]→[PPPoE 透传配置] →[PPPoE 透传限速]

选择级别 20M，配置限速，

备注：级别定义，[用户管理]→[部门级别划分]→[级别划分]，举例创建了 10M,20M 级别。



用户成功拨号后，可在[认证上网]→[PPPoE 透传配置] →[PPPoE 透传状态]，看到拨号后的状态信息



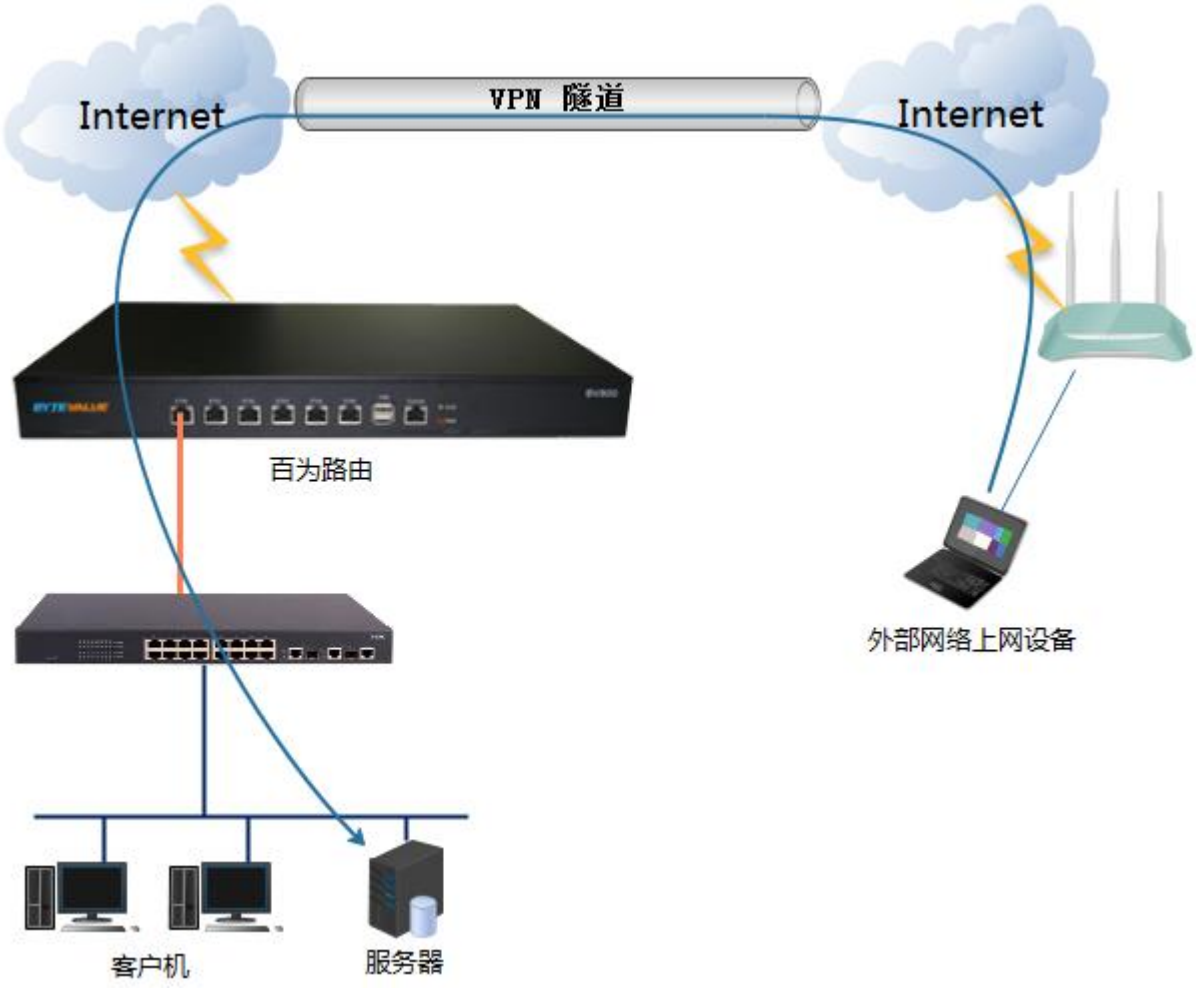
10，VPN 相关功能讲解

10.1，点对网 VPN 的用途

说明：百为路由点对网 VPN 服务，是提供给外部网络的单个用户终端，或者路由设备，VPN 拨号到百为路由。拨号后，就相当于是百为路由内部的成员，既可以访问内网资源，也可以通过配置分流规则，指定该 VPN 用户，走某个 WAN 口出去。

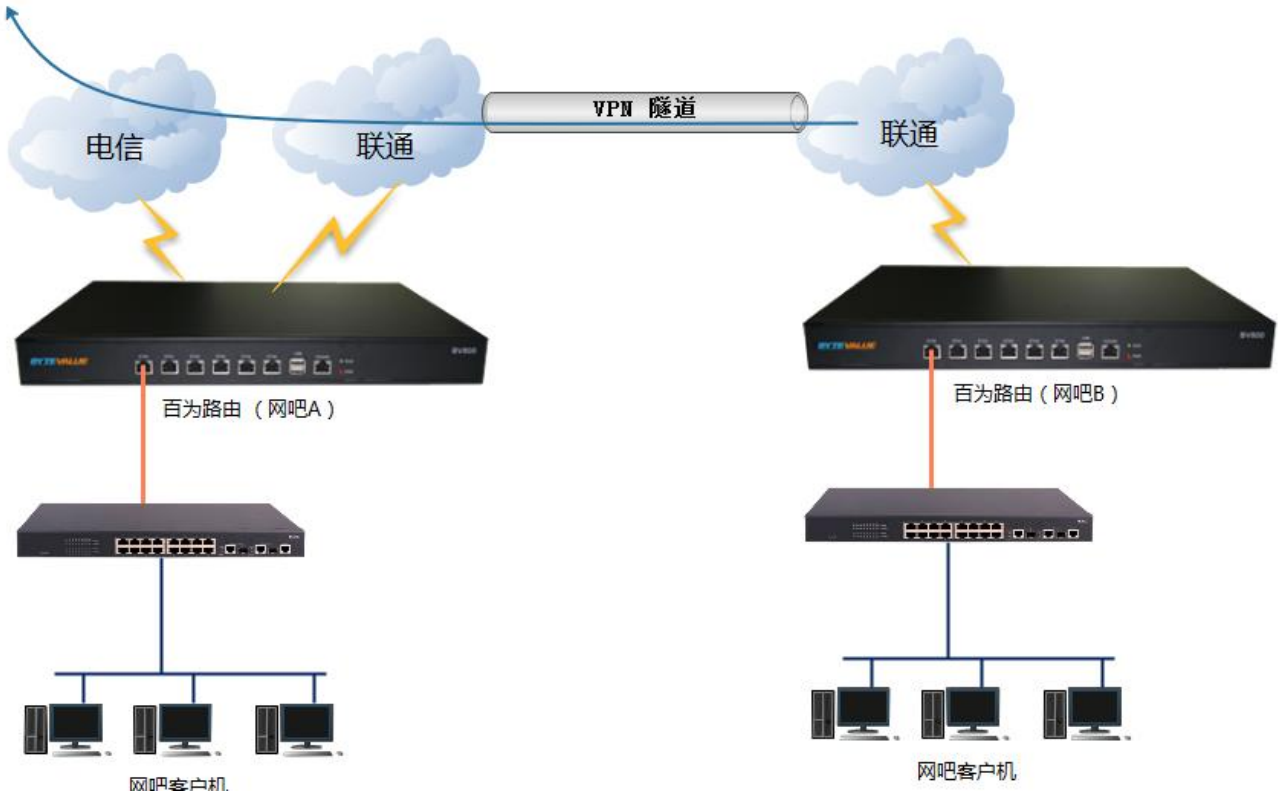
举例应用场景 1：

公司内部有 ERP 服务器，ERP 服务器不对外直接开放，公司的内网为 192.168.100.xxx，ERP 服务器为 192.168.100.200。员工在外面出差，远程访问公司的 ERP 服务器。通过 VPN 拨号到百为路由，可直接访问 ERP 服务器。拓扑图如下：



举例应用场景 2：

网吧 A 有电信光纤 100M ，联通光纤 200M，网吧 B 只有联通光纤 200M，网吧 A 和网吧 B 为同城，联通和联通之间互访速度极快，延迟极低。网吧 B 的客户如果直接玩电信服的游戏，延迟较高，可以通过利用已有的联通和联通之间，建立 VPN 隧道，让网吧 B 的客户，玩电信服的游戏，绕走 VPN 隧道，再从网吧 A 的电信口出去，降低延迟。拓扑图如下：



10.2，点对网 VPN 的配置

百为路由支持的点对网 VPN 类型：PPTP、L2TP、BPN。其中 PPTP/L2TP 为标准 VPN 协议，仅支持 MPPE 加密，不支持 IPsec 加密；BPN 为百为私有协议的 VPN，需要两端均为百为路由才能建立隧道。

从长期的部署经验来看，PPTP、L2TP 的 VPN 拨号后容易掉（多数为运营商原因，中间的握手包容易被运营商丢弃），由此不建议用 PPTP 和 L2TP 拨号后，承载“游戏”业务。而 BPN 的可靠性非常高，适合用来承载“游戏”业务。其次，BPN 隧道的建立，要求两端必须要有公网 IP，必须相互能够直接访问。而 PPTP、L2TP 只需要服务端有公网 IP 即可。

- **点对网 VPN 服务端的配置**

[高级配置]→[点对网 VPN]→[接入配置],提供三种类型的 VPN 服务供选择,根据实际需求开启,并配置分配给 VPN 客户端的 IP 地址范围。

配置建议:

分配的给 VPN 客户端的 IP 地址范围，不能和百为路由的所有内网网段，以及对方路由的内网网段相冲突。比如百为路由内网是 192.168.1.1 、对方路由内网是 192.168.0.xxx，要求填入到分配给 VPN 客户端的 IP 地址范围，不能是 192.168.1.xxx，192.168.0.xxx。建议分配不容易引起冲突的局域网 IP 地址，可以是 172.29.1.1---172.29.1.254；172.30.1.1---172.30.1.254；172.31.1.1---172.31.1.254，DNS 可填入公共 DNS，比如 114.114.114.114；119.29.29.29。

以下列举开启三种类型的 VPN 服务的配置项

PPTP VPN 服务器---开启服务后所有 WAN 口都监听，即 WAN 口有公网 IP 的，都可以拨号进来。

L2TP VPN 服务器---只能选择一个 WAN 口开启服务，即只监听 WAN 口，需要选择有公网 IP 的 WAN 口开启服务。不支持在百为路由上开启 L2TP VPN 服务端的同时，也开启 L2TP VPN 客户端。

BPN 服务器---开启服务后所有 WAN 口都监听，即 WAN 口有公网 IP 的，都可以拨号进来。

- 添加 VPN 账户

[用户管理]→[用户对象]→[接入配置]，添加，自定义账户名称和密码，用户类型，选择为“VPN 拨号”

- **百为路由作为 VPN“客户端”拨号（标准 VPN 拨号）**

[网络配置]→[接口配置]，选择创建 VPN 拨号的外网口，举例 eth3，选择“VPN 接口”，添加，自定义 VPN 接口 ID，以及名称

根据服务端提供的 VPN 类型，选择 PPTP/L2TP，并填入服务端的 IP 地址，VPN 帐号、密码，点保存。

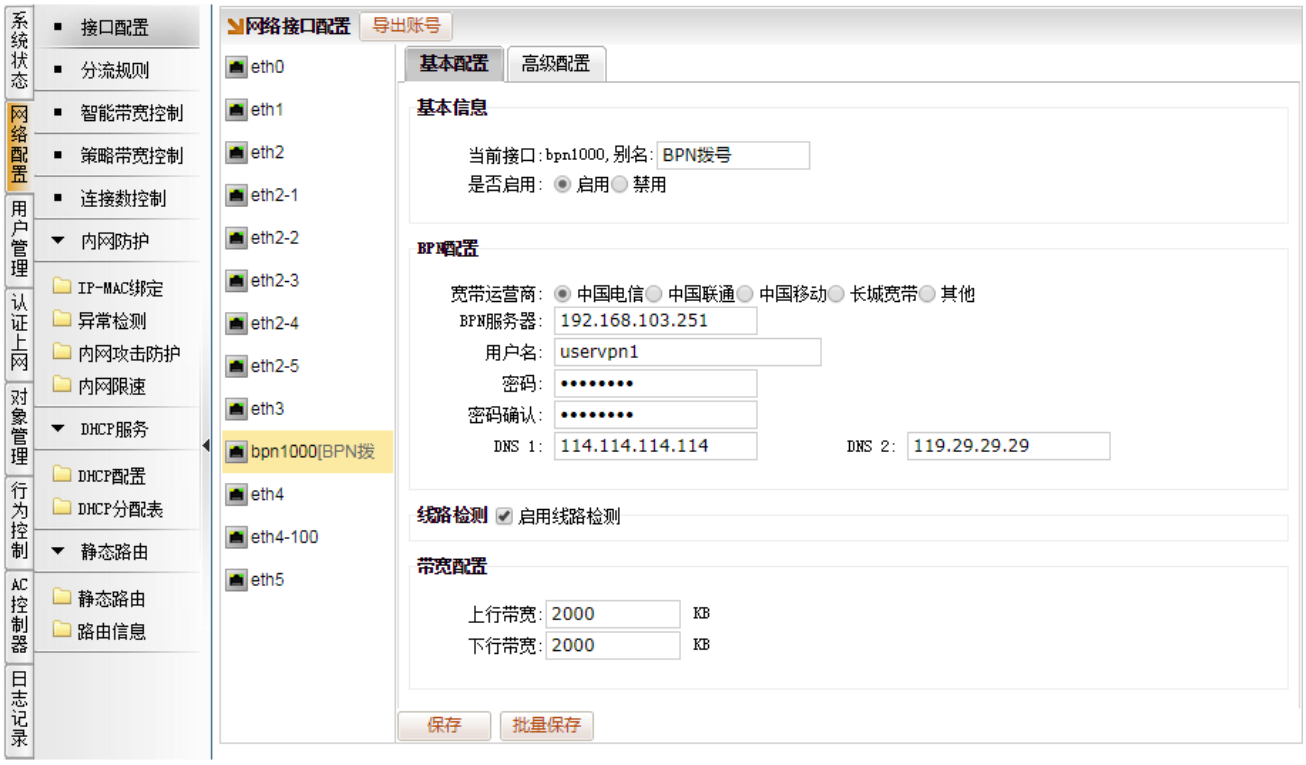
保存，重启路由。

成功拨号后，可以在[系统状态]→[接口状态]，拨号后所得到的 IP 地址。

- **百为路由作为 BPN 客户端拨号**

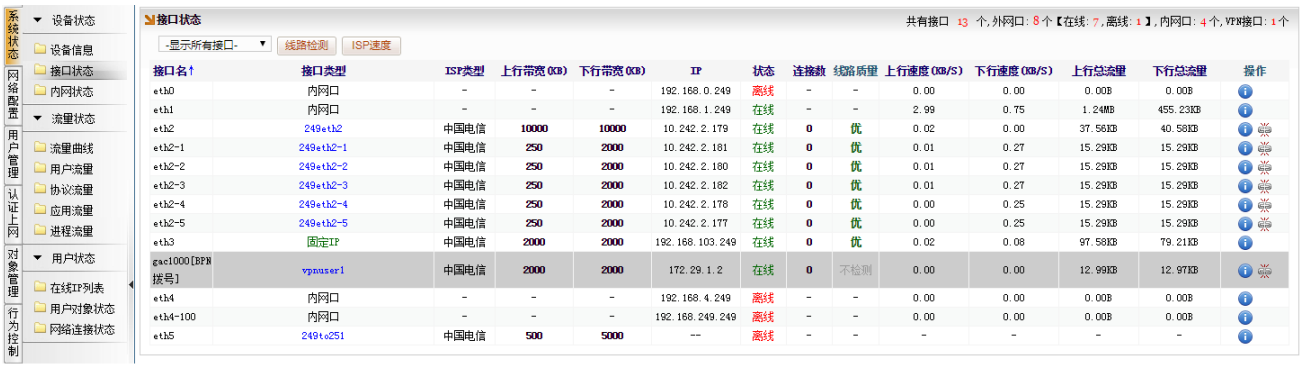
[网络配置]→[接口配置]，选择创建 BPN 拨号的外网口，举例 eth3，选择“BPN 接口”，添加，自定义 VPN 接口 ID，以及名称

填入服务端的 IP 地址，VPN 帐号、密码，点保存。



保存，重启路由。

成功拨号后，可以在[系统状态]→[接口状态]，拨号后所得到的 IP 地址。

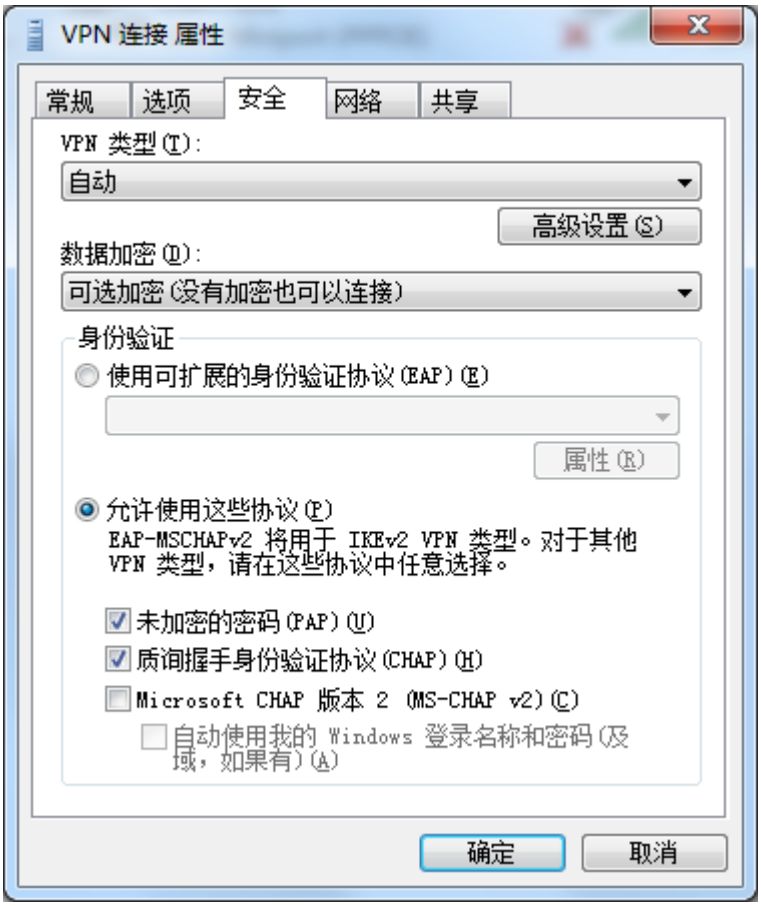


- **电脑作为 VPN“客户端”的配置**

Windows VPN 拨号注意事项：Windows 创建的 VPN 拨号，默认需要加密才能拨号，而百为路由 VPN 服务默认是没有开启加密，需要针对情况做修改。分如下两种情况：

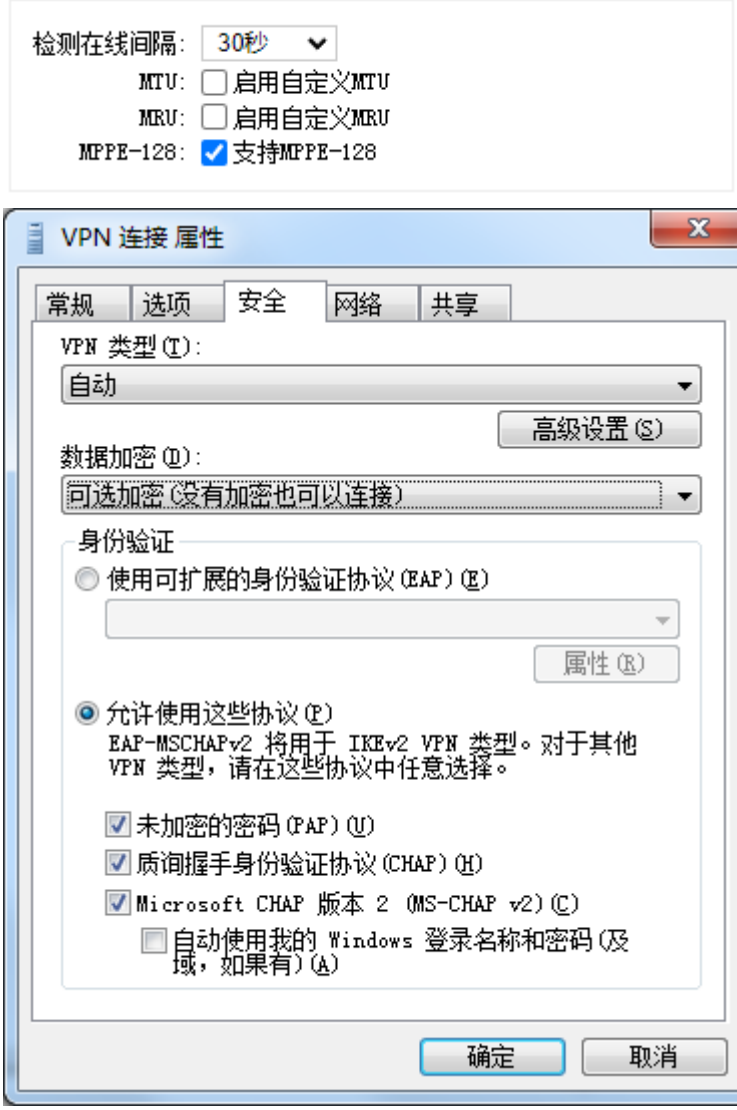
1、路由不开启加密

Windows 的 VPN 拨号属性需要修改 [安全]→[数据加密]的选项，如下图



2、路由开启加密，目前提供 MPPE 加密（暂不支持 L2TP/IPsec 加密）

百为路由点对网 VPN 服务，勾选 MPPE；Windows 的 VPN 拨号属性需要勾选“Microsoft CHAP 版本 2”的加密协议



- 举例 VPN 服务端分流 VPN 用户走指定线路

[网络配置]→[分流规则],添加,源地址对象选择所之前所添加的 VPN 用户,比如“vpnuser1”,勾选要出去的线路，点击确定，并且规则置顶

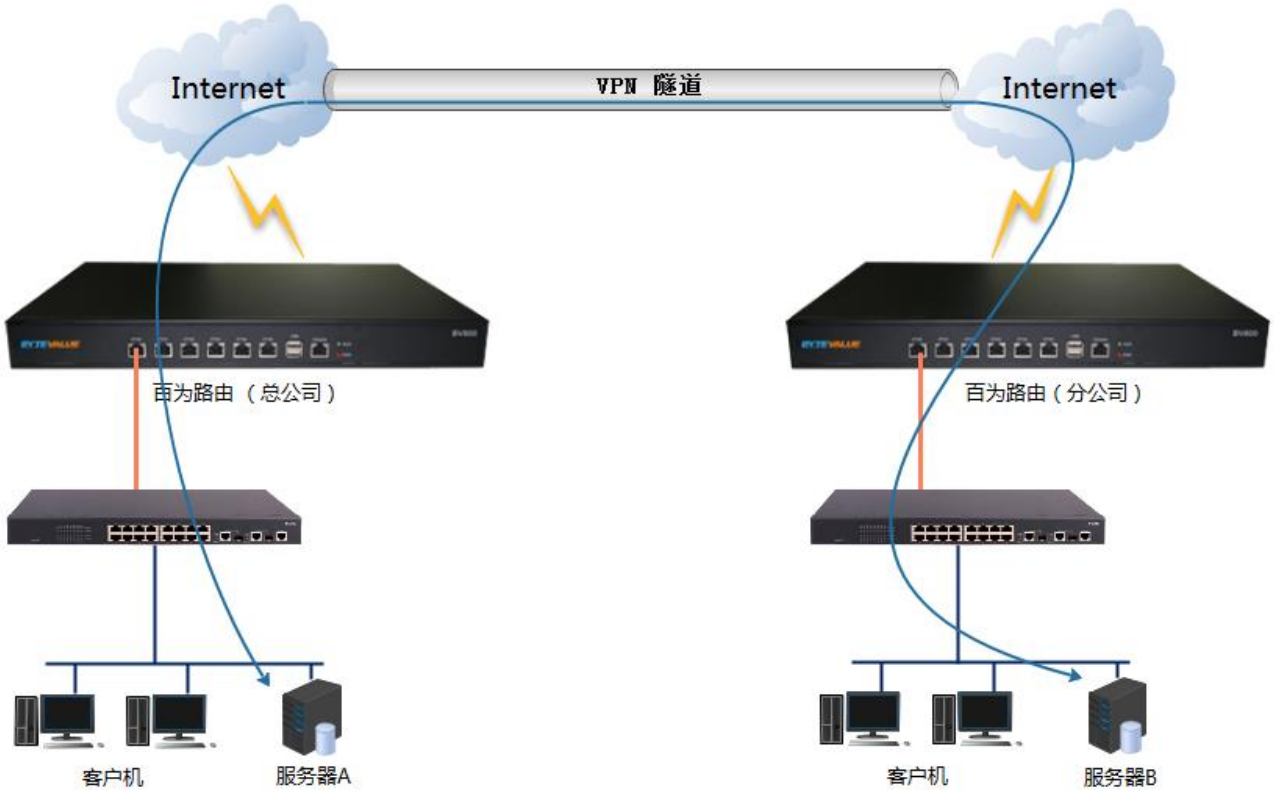
10.3，网对网 VPN 的用途

说明：百为路由网对网 VPN 服务，是为两个独立的网络，建立 VPN 隧道，实现两个内部之间资源互访。

要求：两个内网的网段，不能一样。比如一边的内网是 192.168.0.1---192.168.0.255（192.168.0.0/24），另一边则不能为 0 网段，比如用 1 网段，192.168.1.1---192.168.1.255（192.168.1.0/24），作为服务端的路由需要有公网 IP

举例应用场景：

总公司内部有服务器 A，分公司内部有服务器 B，服务器 A,B 均不对外提供服务，总公司的内网为 192.168.0.xxx，服务器 A 为 192.168.0.200；分公司的内网为 192.168.1.xxx，服务器 A 为 192.168.1.200。要求总公司内部人员能直接访问 192.168.1.200，分公司内部的人员能直接访问 192.168.0.100。拓扑图如下：



10.4，网对网 VPN 的配置

- **网对网 VPN 服务端的配置**

[高级配置]→[网对网 VPN]→[隧道配置]

[参数设置]，选择“将本设备作为 VPN 中心服务器”，自定义密码，加密与压缩均选择“否”

备注：“加密”和“压缩” 仅软路由以及 BV890 以上型号支持

[隧道管理]，添加，自定义隧道名称和隧道 ID，填入 VPN 客户端的内网网段，比如填写 192.168.1.0 ，掩码 255.255.255.0

注意，隧道名称和隧道 ID 必须服务端和客户端，配置一致。

- **网对网 VPN“客户端”的配置**

[高级配置]→[网对网 VPN]→[隧道配置]

[参数设置]，选择 “将本设备作为 VPN 拨号客户端” ，填入 VPN 服务端的 IP，填入与服务端一样的密码。

[隧道管理]，添加，填入与服务端一样的隧道名称和隧道 ID，填入服务端的内网网段，比如填写 192.168.0.0 ，掩码 255.255.255.0。

隧道成功建立后，可在 VPN 服务端、客户端，在[高级配置]→[网对网 VPN]→[隧道状态]，看到建立的连接，如下图所示：

网对网VPN - 隧道状态

序号	隧道名称/ID	状态	上线时间	上传(K/S)	下载(K/S)	连接
1	SZtoGZ/100	在线	2018-12-26 15:10	0.00 KB/S	0.00 KB/S	

注意：百为路由的网对网 VPN，默认是用第一个 WAN 口与之相互建立 VPN 隧道，比如 eth1 eth2 eth3 均为 WAN 口，则 eth1 为第一个 WAN 口，网对网 VPN 使用该口建立连接

建议注意部署的初期，如果有要求指定某个 WAN 口来建立 VPN 隧道，先行调整 WAN 口的顺序。或者是在 [设备维护]→[系统设置]→[其他选项]，将更新线路选择，选择为指定的 WAN 口。

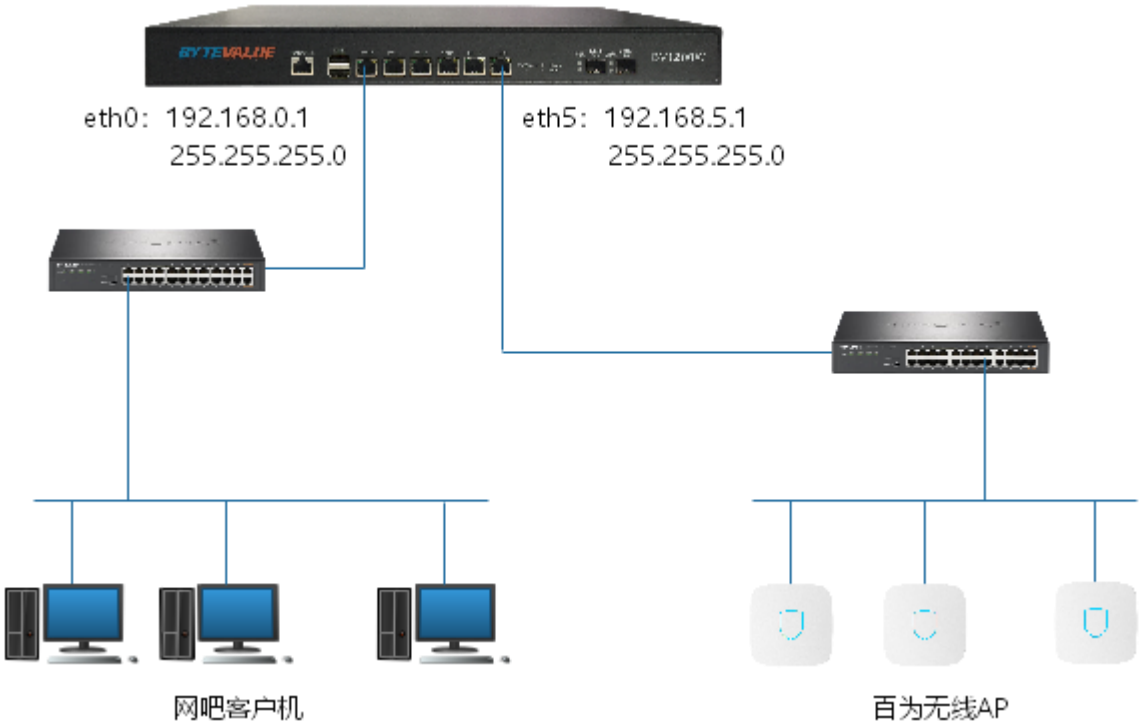
11，百为无线产品讲解

百为无线产品指百为无线 AP，型号包括 W750A、X750A、W1200A、W1200B、X1200A。默认出厂为瘦 AP 模式，需要在百为路由开启 DHCP 服务，给 AP 分配地址，并通过百为 AC 控制器管理使用。（百为 AC 控制器仅支持管理百为无线 AP）

11.1，使用百为路由 AC 控制器管理百为无线 AP

11.1.1，百为路由独立网口连接无线 AP（推荐方案）

由于百为无线 AP 和无线终端都需要百为路由分配 IP 地址才能正常使用(需要开启 DHCP 服务)。通常，网吧场景，无盘服务器已经有 DHCP 服务给客户机分配 IP 地址，原则上，在同一个交换机下（同一个广播域内），不建议路由也开启 DHCP 服务，防止 IP 地址分配异常。推荐使用百为路由闲置的网口，配置为 LAN 口，接独立的交换机再分到无线 AP 去。如下图所示：



举例使用百为路由的 eth5 口用来管理百为无线 AP，并提供无线终端上网。配置如下：

① 启用 DHCP 服务

[网络配置]→[DHCP 服务]→[DHCP 配置]，选择 eth5，开启开关，填入 IP 地址池和 DNS，比如 192.168.5.2---192.168.5.254；填入 DNS，比如 114.114.114.114，119.29.29.29，保存

备注：务必配置能解析的 DNS，比如配置当地运营商的 DNS，或者配置公共 DNS。如果使用 LAN 口 IP 作为 DNS，必须开启 [高级配置]→[模块开关]→[DNS 代理]的开关。

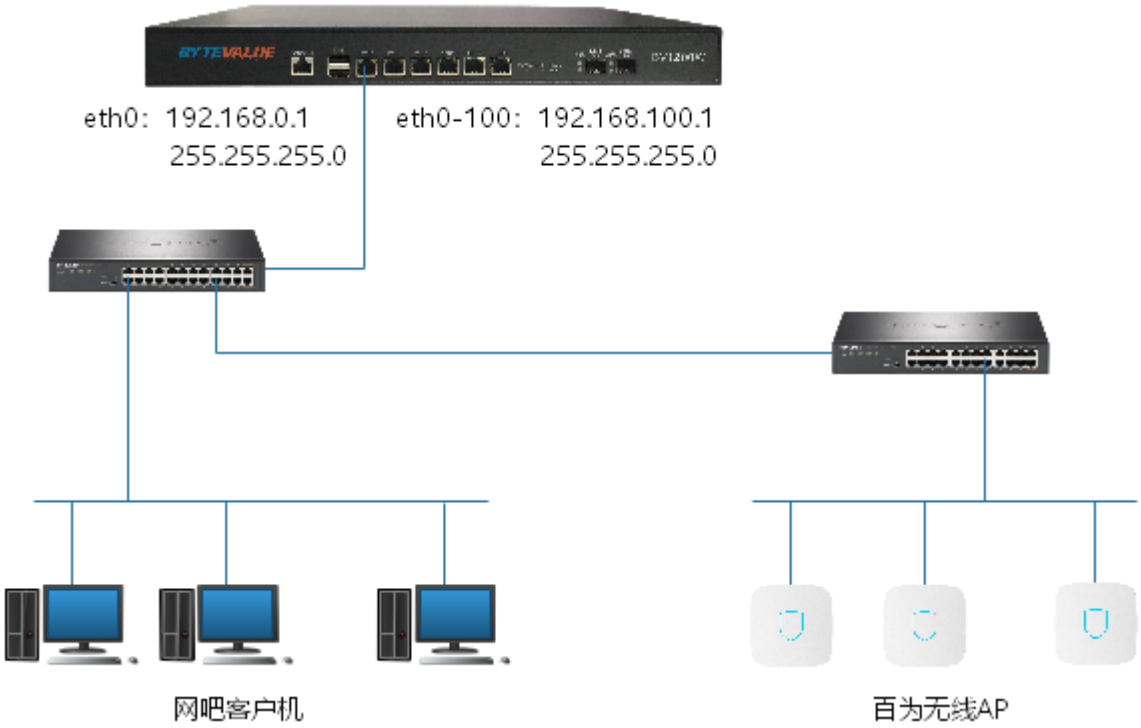
② 查看 AP 是否上线

[AC 控制器]→[AP 设备列表]，如下图所示，看到上线的百为无线 AP，表示可以通过百为 AC 控制器统一对所有 AP 进行管理配置。

11.1.2，从现有交换机连接无线 AP（折衷方案）

由于百为无线 AP 和无线终端都需要百为路由分配 IP 地址才能正常使用(需要开启 DHCP 服务)。通常，网吧场景，无盘服务器已经有 DHCP 服务给客户机分配 IP 地址，原则上，在同一个交换机下（同一个广播域内），不建议路由也开启 DHCP 服务，防止 IP 地址分配异常。

但存在不少网吧，因原来布线的限制，无法从百为路由器的独立网口引网线连接无线 AP。只能从现有的交换机连接无线 AP。如下图所示：



注意：该方法并不规范，仅因为从不少网吧实践得出，多数无盘服务器的 DHCP 服务有绑定客户机 MAC，即使路由器也开启 DHCP 服务，未见影响无盘客户机的开机。因此，可尝试在百为路由的 LAN 口上（连接网吧交换机的 LAN 口），创建其他网段的网关，并开启 DHCP，供无线使用。配置如下：

① 创建子接口

[网络配置]→[接口配置]，比如选择 eth0 口，“子接口”一栏，添加子接口 ID（填入数字范围是 1~4096 任意数字），为了便于标识，比如填入数值 100，点击“确定”。

完成子接口 ID 的添加后，左边栏会生成出“eth0-100”的子接口。选择 eth0-100 的子接口，配置接口类型：LAN（内网口），填入 IP 信息（192.168.100.1），保存后，重启路由。

（注意：添加接口，删除接口的动作，必须要重启，否则将导致整个接口配置功能无效）

② 启用 DHCP 服务

[网络配置]→[DHCP 服务]→[DHCP 配置]，选择 eth0-100，开启开关，填入 IP 地址池和 DNS，比如 192.168.100.2---192.168.100.254；填入 DNS，比如 114.114.114.114，119.29.29.29，保存

备注：务必配置能解析的 DNS，比如配置当地运营商的 DNS，或者配置公共 DNS。如果使用 LAN 口 IP 作为 DNS，必须开启 [高级配置]→[模块开关]→[DNS 代理]的开关。

③ 查看 AP 是否上线

[AC 控制器]→[AP 设备列表]，如下图所示，看到上线的百为无线 AP，表示可以通过百为 AC 控制器统一对所有 AP 进行管理配置。

11.1.3，配置无线 AP

- 配置单个无线 AP

[AC 控制器]→[AP 设备列表]，点击右边的编辑图标对单个 AP 进行设置。

如下图所示，选择要配置的频段，分别对 2.4G、5.8G 设置 SSID 名称，选择安全模式，设置无线密码。

以下是对单个 AP 修改后的示例

- 批量配置多个无线 AP

[AC 控制器]→[AP 配置模版]，点击“添加模版”选择设备型号，点击确定。

点击右边的编辑图标，分别对 2.4G、5.8G 设置 SSID 名称，选择安全模式，设置无线密码。

以下示例，修改 2.4G 和 5.8G 频段用相同的 SSID，密码也一样，模板名称定义为“W1200A 模板”

[AC 控制器]→[AP 设备列表]，勾选要应用模版的 AP，点击“应用配置模版”，勾选模板后，点击“应用模板”。完成对多个 AP 的批量改动。

系统状态
网络配置
用户管理
认证上网
对象管理
行为控制
AC控制器
日志记录
高级配置
设备维护
AP设备列表
AP配置模板
AP升级
无线漫游
自动信道
AP设备列表
AP在线数/AP总数:3 / 3, AC服务状态:【在线】
重启AP
重置AP
删除AP
国家代码选择
应用配置模板
刷新
全部设备
设备型号过滤
查询条件:
设备IP
查找
序号
AP名称
设备IP
MAC地址
SSID(2.4G/5.8G)
用户
状态
信道(2.4G/5.8G)
信道分析
功率
设备型号
设备版本
运行时间
设备备注
配置
1 My WTP 1 192.168.5.3 44-D1-FA-6E-C1-C8 百为网吧_2.4G 百为网吧_2.4G 0 在线 自动[9] 自动[56] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 20 分 51 秒
2 My WTP 1 192.168.5.2 44-D1-FA-6E-C1-E3 Wireless_AP Wireless_AP 0 在线 自动[3] 自动[52] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 22 分 32 秒
3 My WTP 1 192.168.5.4 44-D1-FA-6E-C3-1B Wireless_AP Wireless_AP 0 在线 自动[7] 自动[165] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 19 分 32 秒
应用配置模板
关闭
应用模板
模板名称
设备型号
W1200A模板
W1200A

完成后效果如下

系统状态
网络配置
用户管理
认证上网
对象管理
行为控制
AC控制器
日志记录
高级配置
设备维护
AP设备列表
AP配置模板
AP升级
无线漫游
自动信道
AP设备列表
AP在线数/AP总数:3 / 3, AC服务状态:【在线】
重启AP
重置AP
删除AP
国家代码选择
应用配置模板
刷新
全部设备
设备型号过滤
查询条件:
设备IP
查找
序号
AP名称
设备IP
MAC地址
SSID(2.4G/5.8G)
用户
状态
信道(2.4G/5.8G)
信道分析
功率
设备型号
设备版本
运行时间
设备备注
配置
1 My WTP 1 192.168.5.3 44-D1-FA-6E-C1-C8 百为网吧 百为网吧 0 在线 自动[9] 自动[56] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 22 分 51 秒
2 My WTP 1 192.168.5.2 44-D1-FA-6E-C1-E3 百为网吧 百为网吧 0 在线 自动[3] 自动[52] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 25 分 32 秒
3 My WTP 1 192.168.5.4 44-D1-FA-6E-C3-1B 百为网吧 百为网吧 0 在线 自动[7] 自动[165] 2.4G 5.8G 100% 100% W1200A V5.7-Build20201130091513 22 分 32 秒

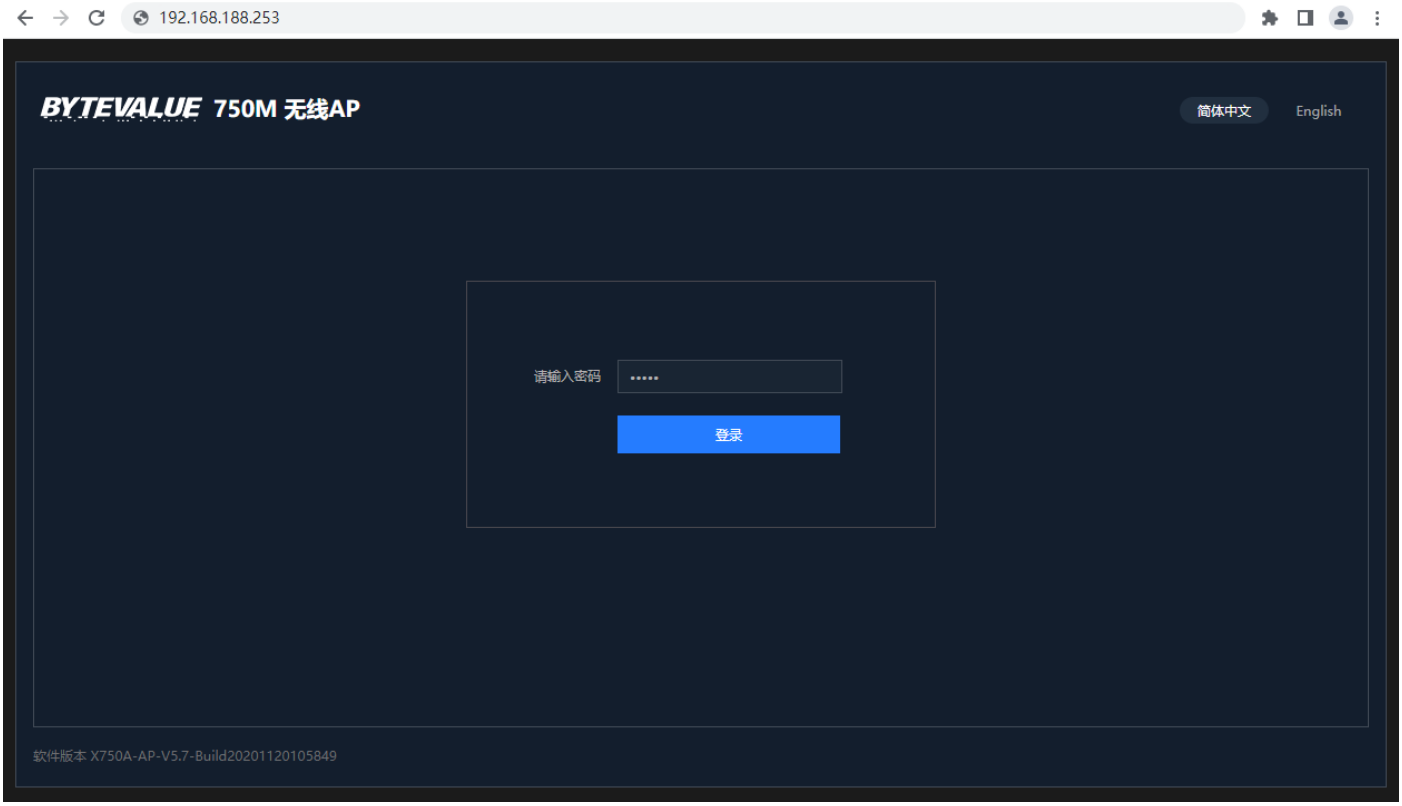
11.2，如何切换百为无线 AP 工作模式

百为无线 AP 默认为瘦 AP 模式，依赖百为主路由进行管理。不使用瘦 AP 模式，可切换为胖 AP 模式或者路由模式，独立管理。

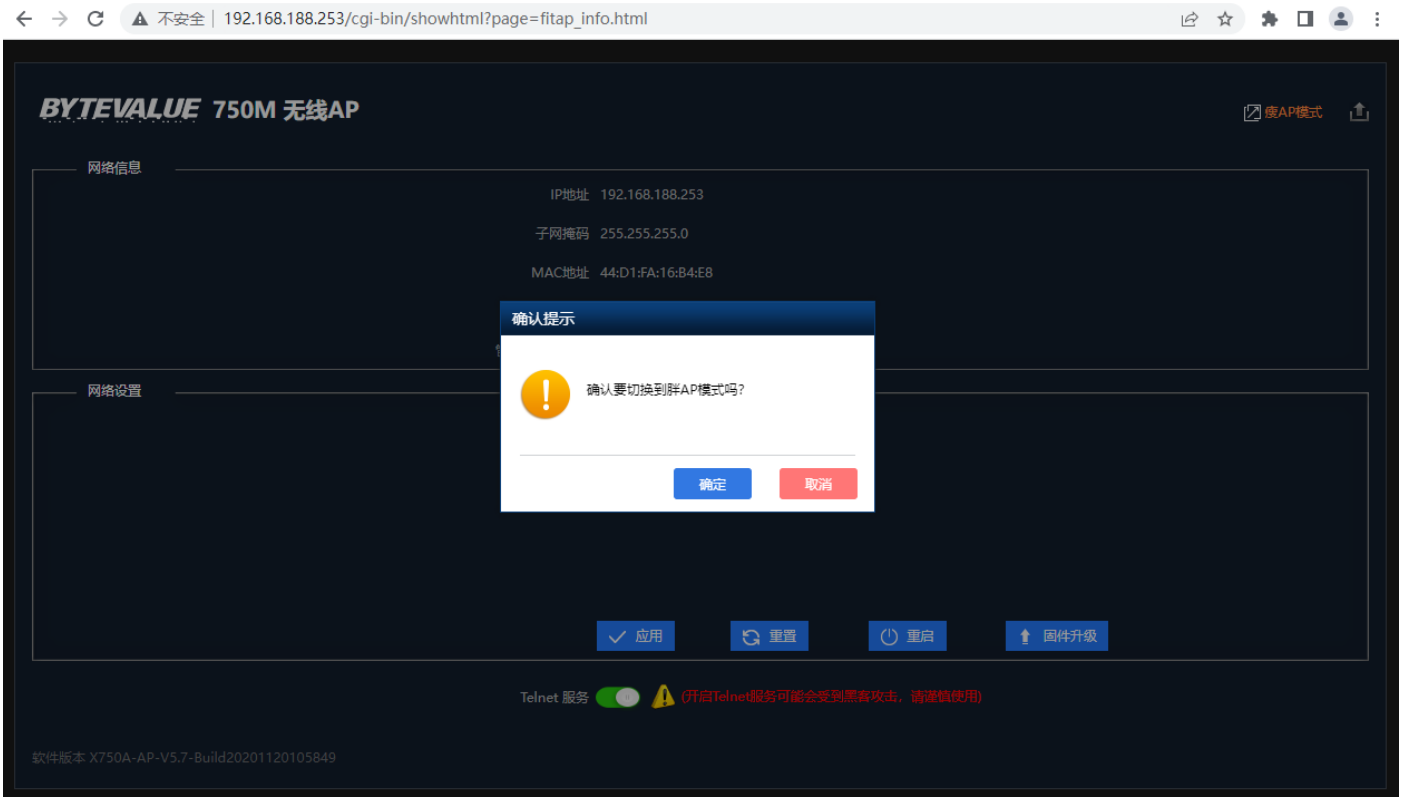
以百为无线 AP，LAN 口默认 IP 为：192.168.188.253。

找一个客户机，网线连接 X750 的 LAN 口，客户机的 IP 比如配置为 192.168.188.200，子网掩码配置为：255.255.255.0。机尝试 ping 192.168.188.253，如果能 ping 通，说明连接正常，则通过浏览器，输入 http://192.168.188.253，登录了路由的 web 界面（web 界面默认密码 admin）

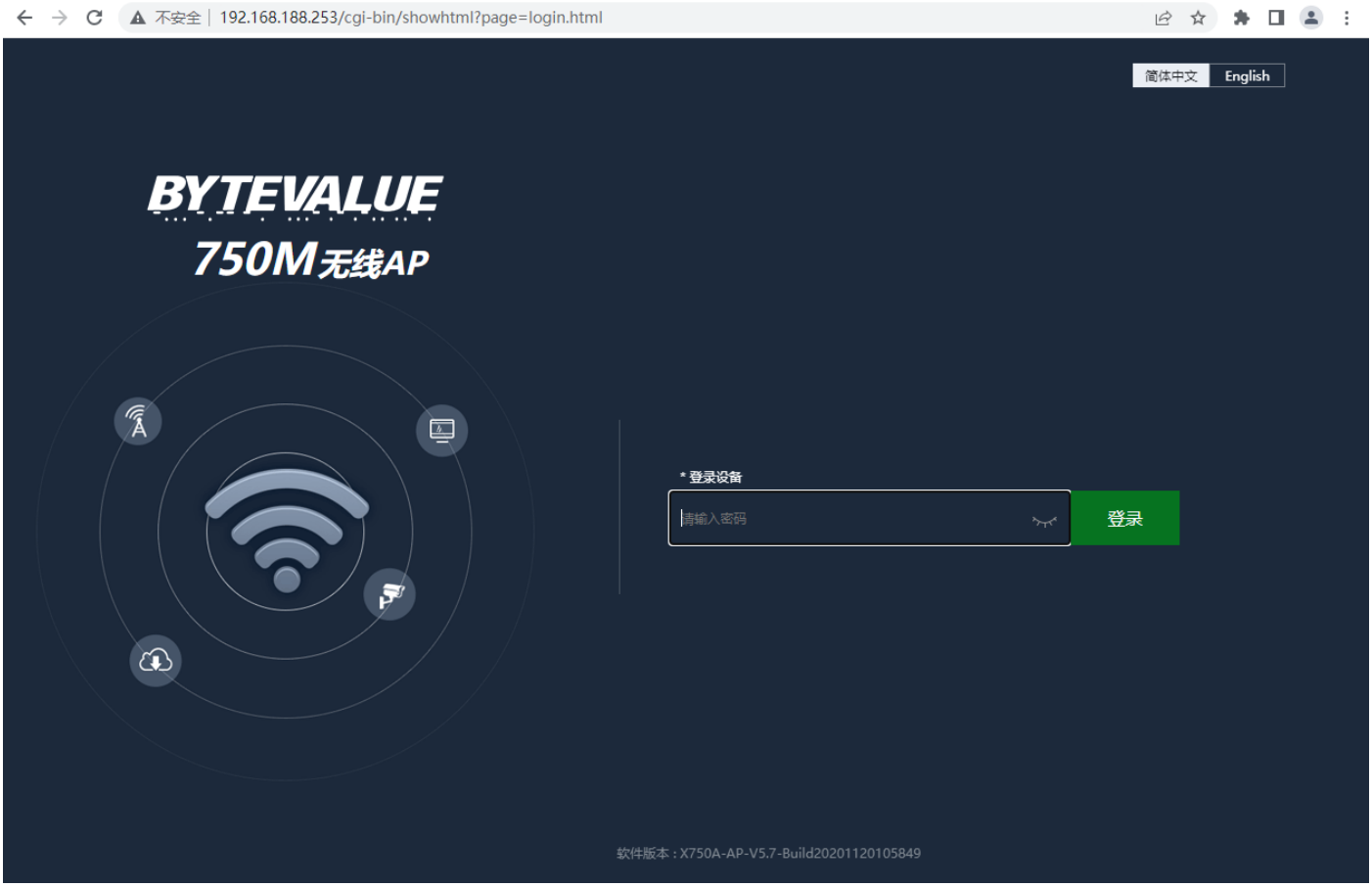
下图所示为瘦 AP 的界面的登录界面



登录后，可见右上角的“瘦 AP 模式”的超链接，点击后有确认提示框。点击确定，则自动切换模式，并自动重启 AP。如下图所示



刷新浏览器重新登录，可见的登录界面有改变。输入密码 admin 登录。



登录后，可独立登录到该无线 AP 进行管理，下图所示为当前的胖 AP 模式的状态页面

如需其他调整，建议通过“设置向导”完成，此处不再赘述

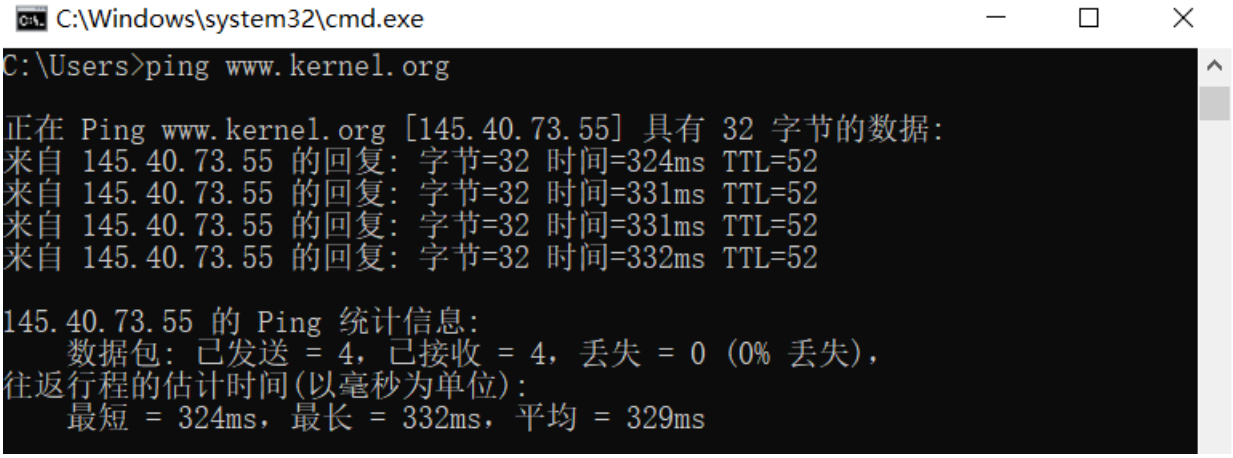
12，其他功能讲解

12.1，如何让一个域名解析为指定的 IP

举例有一站点 www.kernel.org 无法打开，原因是 DNS 解析的 IP 不对，已知该站点正确的 IP 是 145.40.73.55。可以通过百为路由的域名跳转功能，让 www.kernel.org 域名解析为“145.40.73.55”。操作如下：

[行为控制]→[域名跳转]，添加，填入域名和已知 IP，点确定

验证：ping www.kernel.org，如果域名解析的结果为 145.40.73.55 说明功能生效。如果没有解析为正确，可能是客户机有 DNS 缓存，尝试在客户机用命令清空 DNS 缓存，或者重启客户机后，重新测试。



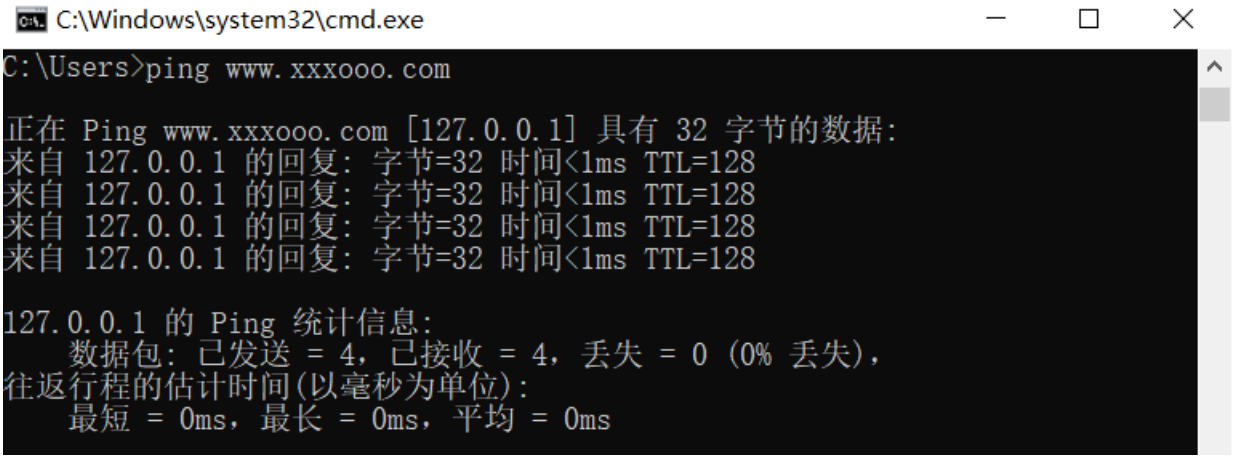
12.2，如何禁止某个域名

[行为管理]→[域名跳转]，添加，填入要禁止的域名，比如“www.xxxooo.com”，IP 地址填写为

“127.0.0.1”。

原理：127.0.0.1 是回送地址，指客户机本机。把需要禁止的域名，解析成 127.0.0.1。 相当于客户机访问这个域名就是访问本机，达到打不开的效果。

验证：ping www.xxxooo.com，如果域名解析的结果为 127.0.0.1 说明功能生效。如果没有解析为正确，可能是客户机有 DNS 缓存，尝试在客户机用命令清空 DNS 缓存，或者重启客户机后，重新测试。



12.3，如何定时重拨宽带

说明：重拨宽带通过配置定时任务，添加断开拨号的命令实现（被断开的拨号会自动重拨）。断开重拨的动作只针对 ADSL/PPPOE 的宽带有效（光猫为桥接类型的宽带），不影响专线固定 IP、DHCP 自动获取的两种上网方式。

- 定时重拨所有宽带

[设备维护]→[定时任务]，添加，选择“周期执行”，并根据实际需求，勾选，并填写时间。执行命令：killall -9 pppd

如下图所示，表示周一至周日，每天 8:00 重拨所有宽带的意思。

说明：该命令会断开所有 ppp 连接，包括宽带拨号，VPN 拨号，小区运营的内网 PPPoE 拨号。所以该命令建议只用于网吧场景，不推荐用于用 PPPoE 拨号的小区运营场景。

- 定时重拨指定宽带

[设备维护]→[定时任务]，添加，选择“周期执行”，并根据实际需求，勾选，并填写时间。执行命令：rm /etc/adsl-ethXXX.stat （XXX 代表网口名词，比如需要重拨 eth2 的宽带，命令为 rm /etc/adsl-eth2.stat）

如下图所示，表示周一至周日，每天 7:00 重拨 eth2、eth3 的宽带，每天 8:00 重拨 eth4 的宽带

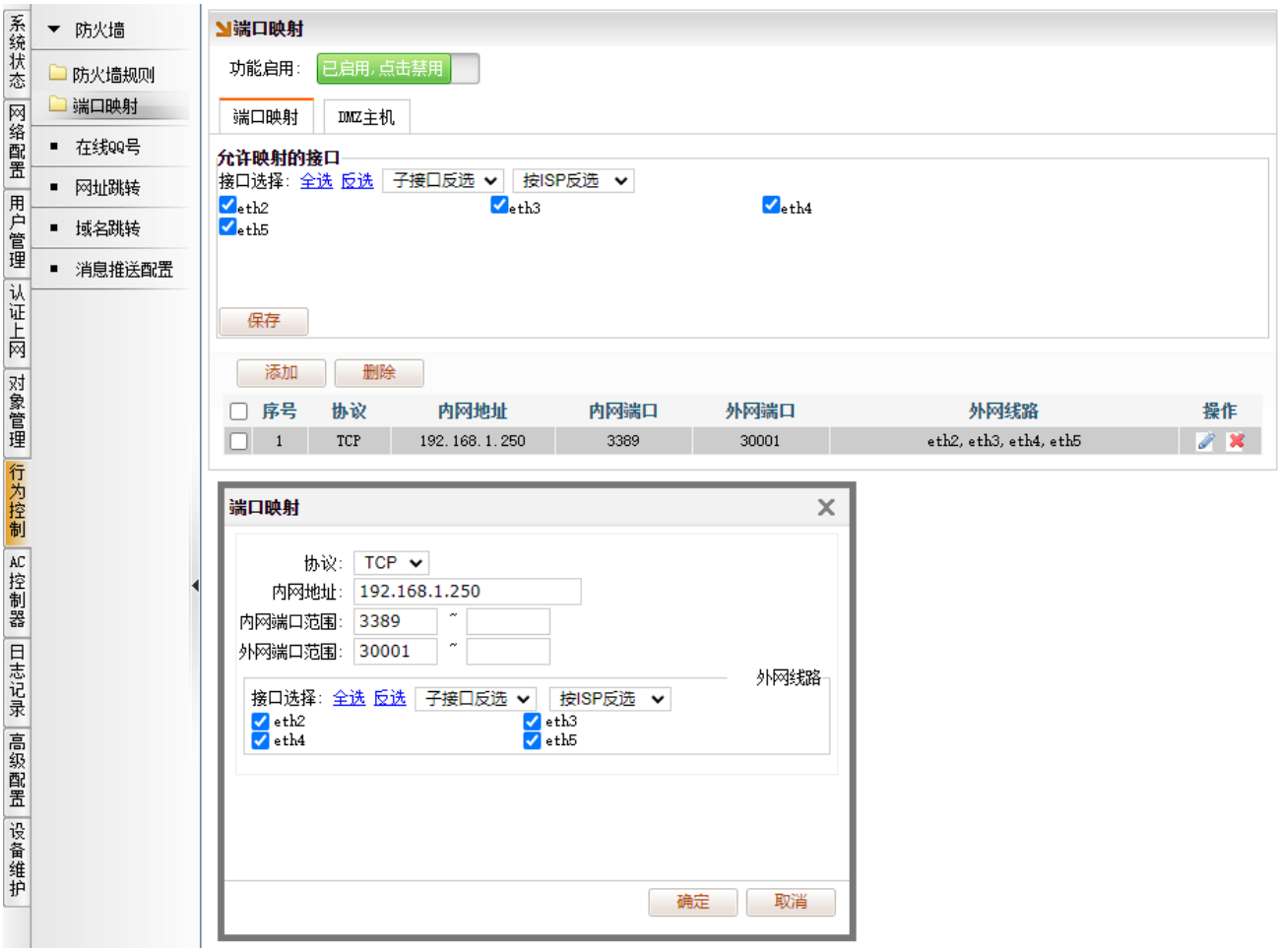
备注：百为硬路由 V3000、V3900、V5000、V5900 由于硬件的特殊性，以命令的形式操作网口，网口名需要+1。比如希望重拨 eth2，命令则需要配置为 rm /etc/adsl-eth3.stat

12.4，端口映射

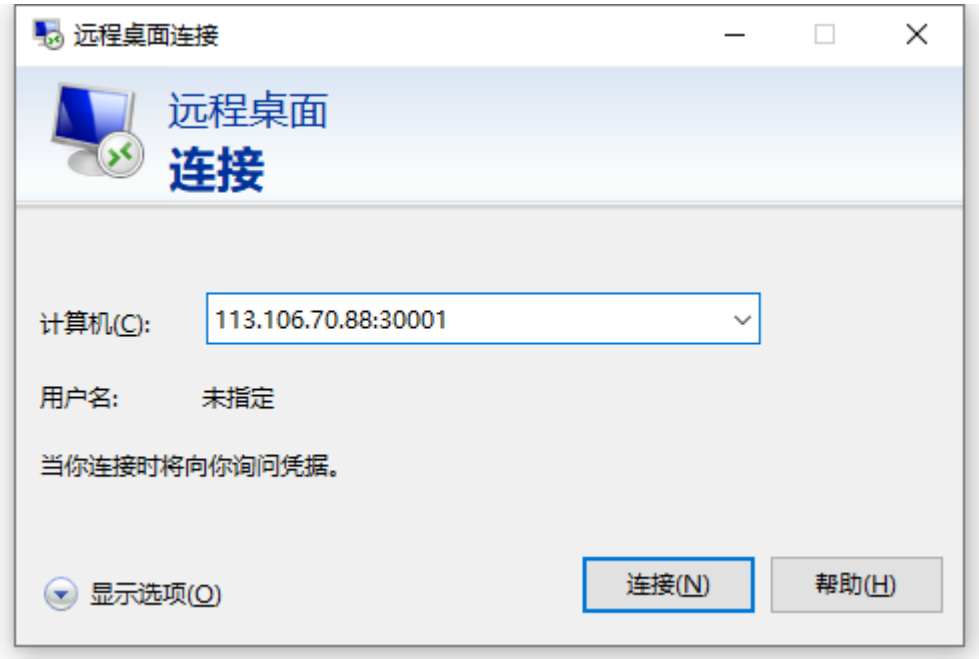
以映射服务器的 windows 远程桌面服务为例。服务器 IP 为 192.168.1.250，远程桌面服务端口为 3389，安全起见，避免直接映射 3389 端口，选择映射 TCP 30001 到服务器的 TCP 3389 端口。操作如下：

[行为控制]→[端口映射]，勾选允许映射的接口，并保存。再点击添加端口映射规则。

协议：TCP	内网地址：192.168.1.250
内网端口范围：3389	外网端口范围：30001



尝试使用网吧的外网 IP 加映射的端口进行访问。



12.5，如何判断有外网流量攻击

网吧是否遭受外网流量攻击，主要看首页的网口流量。

通常情况下，WAN 口接收的流量，要与 LAN 口发送的流量，流量值接近。即使是多线路环境下，多个 WAN 口接收流量的累加值，也应要与多个 LAN 口的发送流量累加值相当。

如下图所示，eth1（WAN 口）的 红色方框的流量值 与 eth0（LAN 口）的红色方框的流量值相当；eth1（WAN 口）的蓝色方框的流量值与跟 eth0（LAN 口）的蓝色方框的流量值也仅一点误差。这种属于正常的网络。

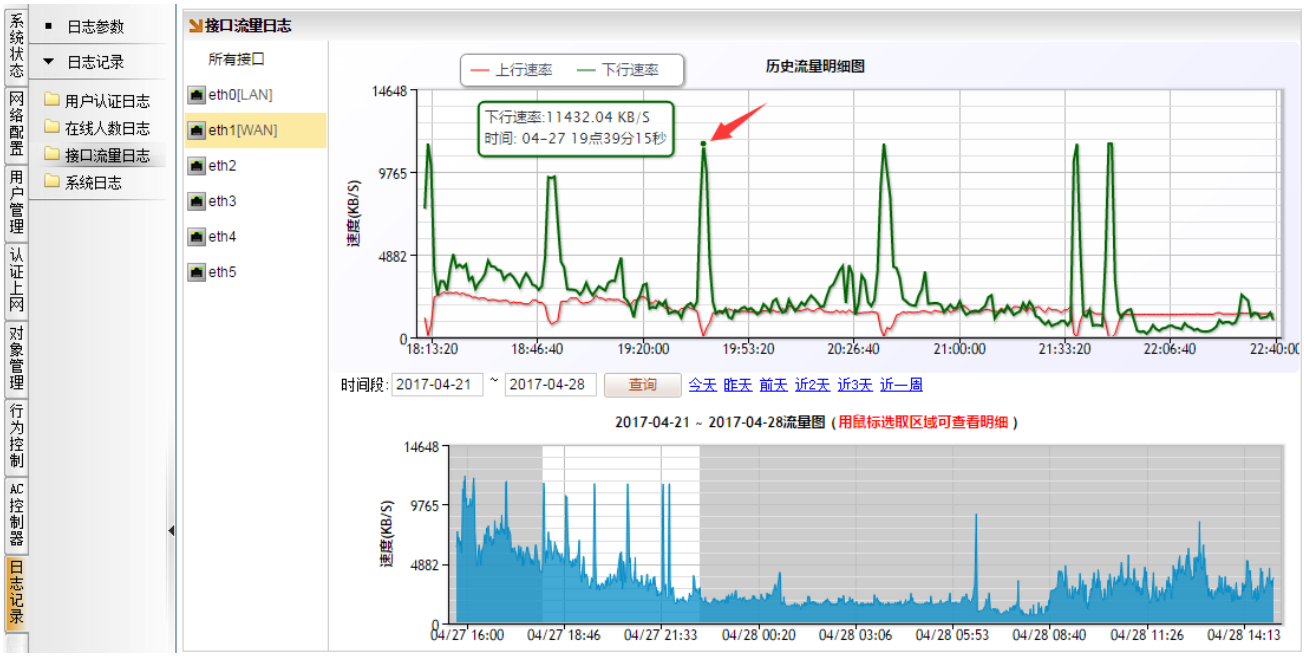
接口	类型	工作速率	IP地址	MAC地址	接收速度	发送速度
eth5	内网口	--	192.168.5.1	00-A6-00-18-45-05	0.00 KB/S	0.04 KB/S
eth4	内网口	--	192.168.4.1	00-A6-00-18-45-04	0.00 KB/S	0.04 KB/S
eth3	内网口	--	192.168.3.1	00-A6-00-18-45-03	0.00 KB/S	0.04 KB/S
eth2	内网口	--	192.168.2.1	00-A6-00-18-45-02	0.00 KB/S	0.04 KB/S
eth1[WAN]	外网口[固定IP]在线	100M	60.31.	00-A6-00-18-45-01	3.29 MB/S	1.32 MB/S
eth0[LAN]	内网口	1000M	192.168.0.1	00-A6-00-18-45-00	1.33 MB/S	3.29 MB/S

如果 WAN 口的接受流量值，远远大于 LAN 口的发送流量值，就有很大的嫌疑是外网流量攻击。如下图所示

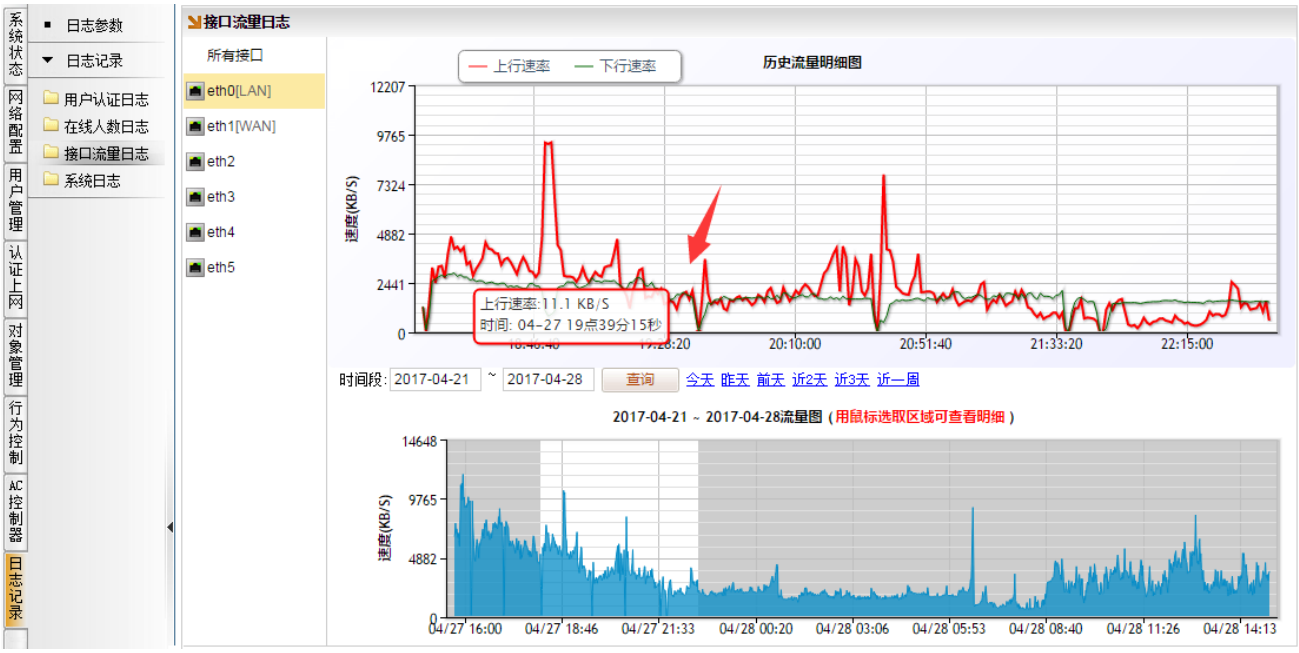
接口	类型	工作速率	IP地址	MAC地址	接收速度	发送速度
eth5	内网口	--	192.168.5.1	00-A6-00-18-45-05	0.00 KB/S	0.04 KB/S
eth4	内网口	--	192.168.4.1	00-A6-00-18-45-04	0.00 KB/S	0.04 KB/S
eth3	内网口	--	192.168.3.1	00-A6-00-18-45-03	0.00 KB/S	0.04 KB/S
eth2	内网口	--	192.168.2.1	00-A6-00-18-45-02	0.00 KB/S	0.04 KB/S
eth1[WAN]	外网口[固定IP]在线	1000M/全双工	60.31.	00-A6-00-18-45-01	8.12 MB/S	1.32 MB/S
eth0[LAN]	内网口	1000M/全双工	192.168.0.1	00-A6-00-18-45-00	1.33 MB/S	2.19 MB/S

如果没法及时观测实时流量，可以通过查看流量日志，观察 LAN 口和 WAN 口的历史流量来判断，[日志流量]→[日志记录]→[接口流量日志]

选中 WAN 口，比如示例中的 eth1，在蓝色流量图，用鼠标拉动时间范围，会显示出流量明细图。比如 19:39 分的时候网络很卡，鼠标移动到曲线图，可看到当时的流量。手工记录下来。



选中 LAN 口，比如示例中的 eth0，在蓝色流量图，用鼠标拉动时间范围，会显示出流量明细图。查看 19:39 分的时候的 LAN 口流量。手工记录下来。



通过对比 19:39 的 WAN 口 LAN 口历史流量发现，WAN 口收到了很大流量，但流量并没有转发到内网口去，就有很大的嫌疑是外网流量攻击。

同理，以上排查方法，反过来的话，就是属于内网流量攻击了

外网流量攻击路由能防么？

答：目前，外网流量攻击，均为 UDP 洪水攻击。攻击者不管路由收不收这些攻击数据。目的也不是为了攻击路由。而是堵塞运营商的带宽。

打比方，签约的光纤带宽为 50M，攻击者发包过来，堵塞 50M 的带宽。路由就算防火墙拒绝这些数据，这条光纤永远是堵塞的，除非停止攻击。或者换 IP。

现实中，流量攻击，多属于雇佣黑客，操纵众多中毒的电脑（俗称肉鸡）同时给目标 IP 发包攻击，源头根本就无从抓起。缓解的手段仅有更换 IP，或者使用宽带，尽可能避免 IP 暴露给攻击者攻击。

13，异常问题自检

13.1，游戏更新服务器更新速度慢自检步骤

步骤一

首先需要判断，是不是游戏更新的资源问题。特别是游戏更新服务器以前更新速度正常，在路由没有改动的前提下，游戏更新速度突然上不去，通常是游戏更新厂家资源问题。

遇到这种更新速度慢的时候，不要急于改动百为路由的配置。建议先在游戏更新服务器上，安装迅雷，使用迅雷下载 Windows10、Windows11，来测试游戏服务器的下载速度（通常 Windows10、Windows11 资源多，下载速度快）。

如果游戏更新服务器使用迅雷下载 Windows10、Windows11 等，速度够快，远比游戏更新软件的下载速度快。说明百为路由层面不存在对游戏更新服务器做什么限制，导致没速度。因此不需要调整路由的配置。尝试重启游戏更新服务看是否下载速度正常，或联系游戏更新厂家客服解决。

说明：百为路由处理转发迅雷的下载业务和处理转发游戏更新服务器的下载业务，没有差异。二者均隶属于 P2P 与下载的类别。以迅雷下载作为参照对比，可以知晓是否游戏更新厂家资源问题。

步骤二

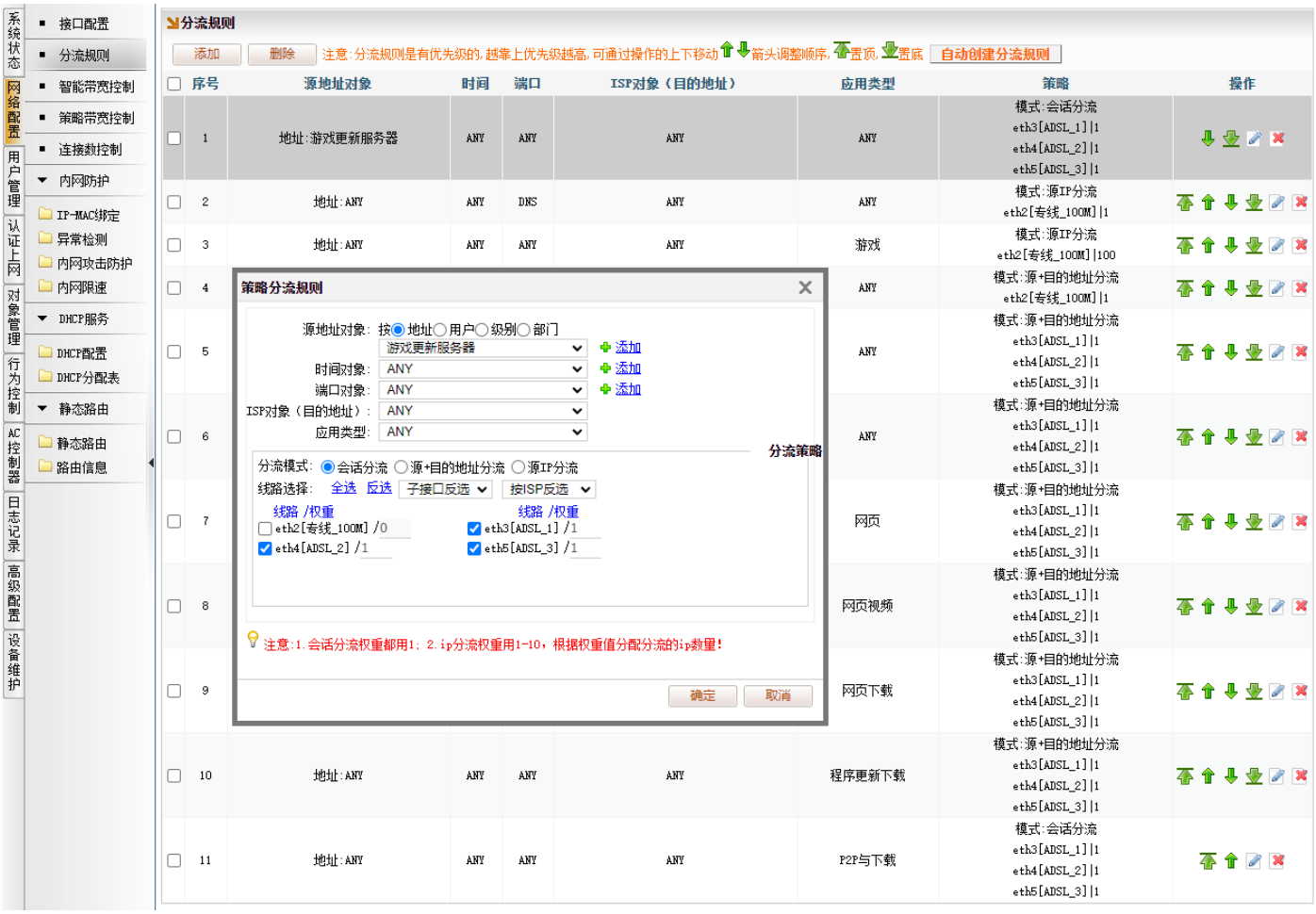
如经过步骤一测试后，游戏更新服务器上用迅雷下载，也一样没有速度。考虑网吧是不是多线路场景，检查服务器是否有分流到带宽大的线路上。比如专线+宽带的网吧，通常宽带带宽较大，建议游戏更新服务器的下载业务分流到宽带来负载。

以下举例 100M 专线+3 条 300M 宽带的场景

①分流游戏更新服务器到宽带：

[对象管理]→[基本对象]→[地址对象]，添加地址对象，比如命名为“游戏更新服务器”，并填入游戏更新服务器的 IP。

[网络配置]→[分流规则]，添加“分流规则”，“源地址对象-地址”选择“游戏更新服务器”，“时间对象、端口对象、ISP 对象、应用对象”均为“ANY”，勾选带宽大的线路（比如这里勾选了三条宽带），使用“会话分流”，将该规则置顶。



配置思路：网吧哪些线路带宽大，适合用来负载大流量业务，就把游戏更新服务器分流到这些带宽大的线路上。

②添加游戏更新服务器限速，并放大限速

[网络配置]→[策略带宽控制]，添加带宽控制规则，源地址对象，选择“地址-游戏更新服务器”，点击“高级”，勾选生效所有 WAN 口进行配置，并配置限速。限制在专线 eth2 上行开销不超过 1500KB，下行开销不超过 5000KB；在三条宽带 eth3、eth4、eth5 的上行开销均不超过 800KB，下行开销均不超过 25000KB。

添加的规则会自动排序，“源地址对象--地址-VIP”的限速规则 1，优先匹配。该 IP/IP 段的速度不受规则 2 影响。

配置思路：游戏更新服务器的单独一条规则来限速，适当的放大在宽带的限速。

③重启游戏更新服务

由于可能没配置百为路由之前，游戏更新的下载业务，都走专线，或者都走带宽小的线路。一些老的连接下载连接没能切换过来。需要停止游戏更新再开启，通常建议停止游戏更新 5 分钟后，再重新开启下载。验证游戏更新是否有速度。

步骤三

配置智能流控例外规则

注意：如果经过步骤一、步骤二的操作后，游戏更新服务器的下载速度快了，不建议还配置智能流控例外规则。此操作，主要是用于带宽比较紧张的网吧。比如网吧只有一条 100M 专线，当用网高峰时间段，智能流控动态限速，人均带宽差不多为 300KB~400KB。此时游戏更新的速度上不去，恰好有某个重要的游戏需要紧急更新，网吧才能正常运行。急需给游戏更新服务器腾出速度，保证更新

速度，才配置配置智能流控例外规则。

配置方法如下：

[网络配置]→[智能带宽控制]→[例外规则]，添加智能流控例外规则，源地址对象，选择“游戏更新服务器”，点击确定。

说明：配置智能流控例外规则，通常是需要结合步骤二的限速来用。由于例外 IP，优先级大于其他客户机，当例外 IP 地址有流量开销，其他客户机会为其腾出速度，如果耗光线路带宽，网吧其他客户机将卡顿，甚至断网。建议控制游戏更新的速度，比如限制上行开销不超过 1500KB，下行开销不超过 5000KB-8000KB。

13.2，端口映射无效问题自检步骤

步骤一

首先需要判断，是不是被映射的机器，没有配置网关，或者网关配置错误的原因。比如网吧用的监控用的录像机，需要登录到录像机检查网关是否配置正确；又比如无盘服务器双网卡，映射错 IP 了（需要映射有配置网关的网卡 IP）

步骤二

判断被映射的机器，有没有网络，能不能上网。（映射是属于访问外网的行为，需要能上网）

步骤三

判断是不是被映射的机器，百为路由是否有规则限制。

- 防火墙规则限制

  [行为管理]→[防火墙]→[防火墙规则]，查看有没有规则禁用了被映射的机器。

- IP-MAC 错误绑定

  [网络配置]→[内网防护]→[IP-MAC 绑定]，查看被映射的机器，是否 IP-MAC 绑定错了 MAC。

- 配置了特殊 IP

  [设备维护]→[许可认证]→[特殊 IP]，查看有没有填入特殊 IP 包含了被映射的机器。

步骤四

判断是不是被映射的机器，建立太多连接，开销光路由限制的连接数。

[系统状态]→[用户状态]→[网络连接状态]，查看被映射的机器，当前开销多少连接数。通常百为路由默认限制单机连接数，TCP、UDP 并发连接各 5000 个。确认因为被映射的机器开销光 5000 个连接导致的问题，则需要在 [网络配置]→[连接数控制]，放大被映射的机器的连接数限制。

13.3，ping 路由 LAN 口不丢包，ping 外网丢包问题自检

步骤一

单机测试，电脑直连光纤，用负载的方式测试。比如 100M 的专线，使用迅雷下载，并且在迅雷软件里设置限速，比如限速上传，下载速度不超过 95M。对于 100M 专线来说，相当于预留 5M。使用迅雷下载的同时，ping 外网，比如同时 ping 114.114.114.114；ping 119.29.29.29；ping 180.76.76.76；ping 223.5.5.5。如果 ping 测试都同时有丢包。有很大可能是运营商问题，寻求运营商排查。

步骤二

如经过步骤一测试后，确认光纤没问题，尝试如下配置：

[网络配置]→[接口配置]，选择光纤网口，勾选“自动绑定网关 MAC”，并保存。

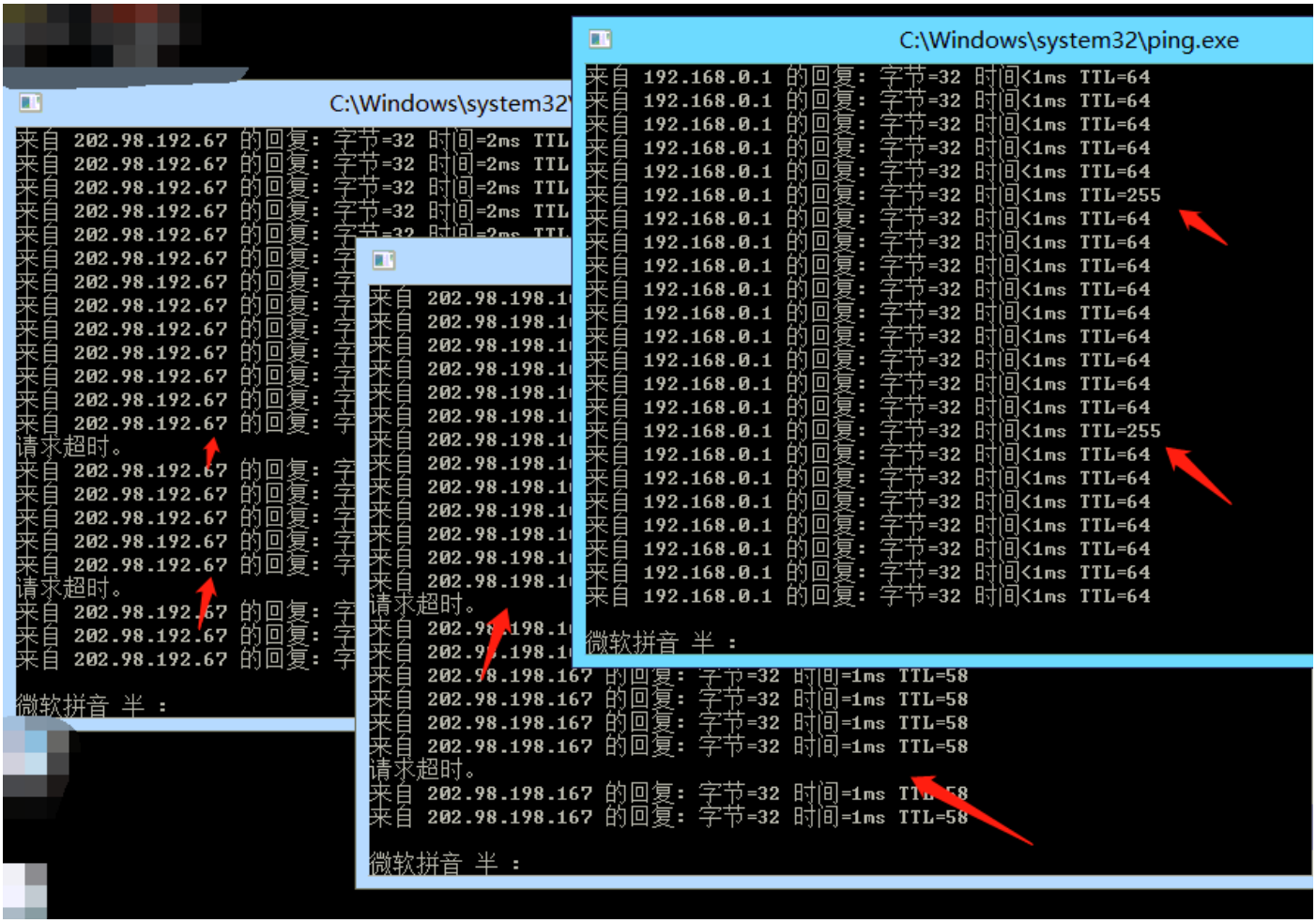
有可能存在运营商的 ARP 的老化时间与百为路由的 ARP 老化时间不兼容的问题。尝试自动绑定网关 MAC，观察问题能否解决。

步骤三

如经过步骤二配置后，依然有丢包，在 ping 测试的过程中，加入 ping LAN 口 IP，观察是否有

可疑。

常见于网吧，比如交换机默认 IP 地址也是 192.168.0.1，跟路由 LAN 口冲突。ping LAN 口 IP，表现为不丢包，一旦 TTL=255 时候，ping 外网丢包。



解决的办法：

修改交换机的 IP 或者修改路由 LAN 口 IP，避免冲突。

步骤四

尝试更换网口或者硬件，观察是否硬件问题。

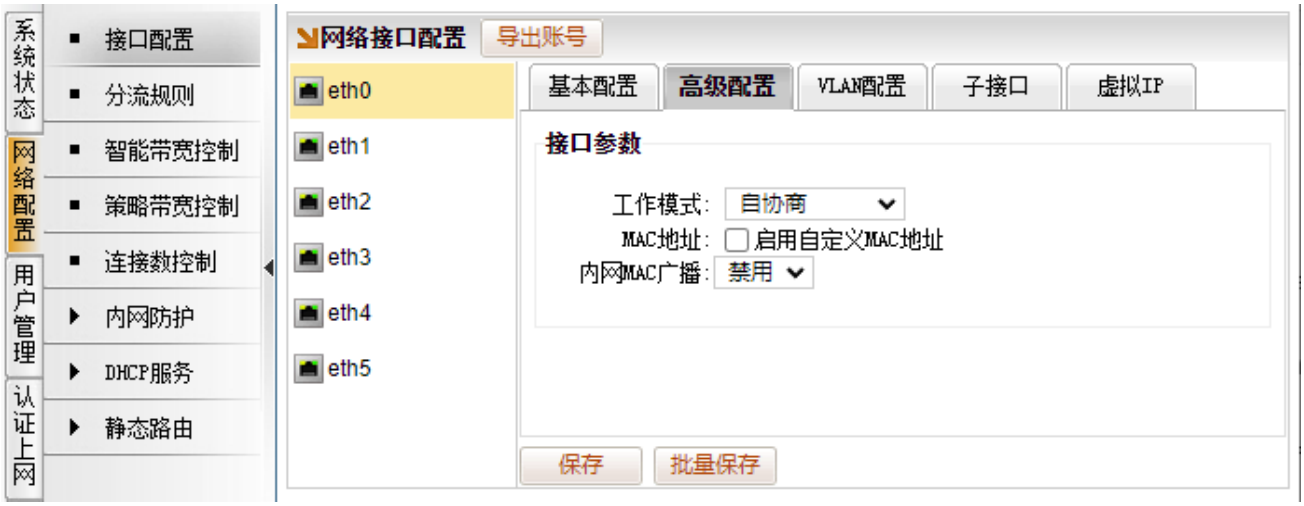
14，常见问题解答

14.1，首页显示工作速率 100M/全双工详解

路由显示的网卡的工作速率，是网卡和所连的设备协商速率。以下图为例，可见 eth0 当前协商速率为 100M/全双工。

接口	类型	工作速率	IP地址	MAC地址	接收速度	发送速度
eth5	外网口[ADSL拨号]在线	1000M/全双工	10.254.0.17	00-90-27-FE-E2-C2	0.13 KB/S	0.13 KB/S
eth4	外网口[ADSL拨号]在线	1000M/全双工	10.254.0.68	00-90-27-FE-E2-C1	0.02 KB/S	0.02 KB/S
eth3	外网口[ADSL拨号]在线	1000M/全双工	10.254.0.67	00-90-27-FE-E2-C0	0.04 KB/S	0.04 KB/S
eth2	外网口[固定IP]在线	1000M/全双工	116.30.244.3	00-90-27-FE-E2-BF	0.31 KB/S	0.08 KB/S
eth1	内网口	100M/全双工	192.168.1.253	00-90-27-FE-E2-BE	3.34 KB/S	0.45 KB/S
eth0	内网口	—	192.168.0.1	00-90-27-FE-E2-BD	0.00 KB/S	0.00 KB/S

先检查网口工作模式，[网络配置]→[接口配置]，选择要查看的网口→高级配置，确保工作模式为："自协商"。



如果网口工作模式已为"自协商"，首页网口工作速率依然为 100M/全双工。则需要检查路由器的网卡是否为千兆网卡；检查所连接的设备网口是否为百兆标准的（百兆光猫、百兆交换机……）；检查网线，水晶头是否接触不良。

14.2，网口显示的丢包是什么问题

点击网口图标可见发送和接受数据详情。通常，此处的网卡显示的“丢包”，属于正常的丢弃动作，丢弃一些无效包，不需要转发的数据包。特别是路由的内网口，由于内网口连接内网交换机，收到无盘服务器和无盘客户机之间通讯的广播包，无效包可能会更多。

通常情况下，只要确认客户机 ping 路由 LAN 口不丢包，即表示正常。无需担心。

需要注意的是，如果每次点开网口，看到不停的新增错包，帧。则可能是网口有问题，或者网线水晶头有问题，需要检修。

14.3，系统日志提示有攻击包有没有问题

[网络配置]→[内网防护]→[内网攻击防护]，开启了内网攻击防护，会记录内网攻击日志。

如下图所示，开启攻击防护开关，设置包阈值为 5000。当内网有机器每秒发包量超过 5000 个包的时候，会丢弃超过阈值的数据包，并进行记录。

[日志记录]→[系统日志]，提示的攻击日志如下：

序号	时间	描述
1	2022-09-26 15:09:09	每秒收到192.168.0.59/00-E0-70-CB-F5-8D机器5000攻击包
2	2022-09-26 14:36:54	每秒收到192.168.0.78/04-D9-F5-35-A1-1E机器5000攻击包
3	2022-09-26 14:35:09	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
4	2022-09-26 13:48:09	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
5	2022-09-26 13:26:54	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
6	2022-09-26 13:18:24	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
7	2022-09-26 13:17:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
8	2022-09-26 13:12:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
9	2022-09-26 13:12:09	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
10	2022-09-26 13:09:24	每秒收到192.168.0.10/1C-1B-0D-77-14-D1机器5000攻击包
11	2022-09-26 13:07:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
12	2022-09-26 13:03:54	每秒收到192.168.0.61/00-E0-70-CB-FD-A0机器5000攻击包
13	2022-09-26 13:02:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
14	2022-09-26 12:57:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
15	2022-09-26 12:52:54	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包
16	2022-09-26 12:47:39	每秒收到192.168.0.233/EC-D6-8A-2C-7B-65机器5000攻击包

说明：

“每秒收到 xxxxxxx 攻击包”的日志，表示在那一刻，有客户机发包量大，可能的原因有：

- 客户机中毒发包量巨大
- 客户机有增值广告程序异常在发包请求
- 客户机可能用了 P2P 工具下载的同时共享发包
- 游戏更新服务器的 P2P 服务在共享发包

通常，提示出现攻击包的时候，客户机 ping 路由 LAN 口不丢包，可以无视该记录。路由仅仅记录某一个的状态，便于定位问题。

内网攻击防御，本质是为了照顾性能低的硬件，减少内网攻击时路由的性能开销。如网吧路由器硬件规格较高，日常使用中没有什么问题，可关闭内网攻击防御的开关，不处理疑似攻击包，不记录此类日志（毕竟网吧客户机下不少正在玩游戏，看网页的同时，可能有病毒，木马，广告在后台偷偷的发包。关闭内网攻击防御，不去处理该疑似客户机的发包，可能该客户机的上网体验会好点）。