Panabit 智能应用网关

产品手册 v5.0

公司名称：北京派网软件有限公司
公司地址：北京市海淀区西北旺东路 10 号院 10 号楼中关村新兴产业联盟大厦一层
邮政编码：100094
公司网址：www.panabit.com
联系电话：86-10-8200 1781
传真：86-10-8209 0830

文档约定

版权声明

版本修订

派网保留不预先通知客户而修改本文档所含内容的权利。本文挡的开发过程是基于 Panabit 专业版 V16.11.29，核心代号（魏晋 R3）以上版本。本文档描述的部分内容可能跟您购买的设备有差异，其原因可能是您购买的设备版本低于或者高于 Panabit 专业版 V16.11.29。

责任限定

派网对于您的使用或不能使用本产品而发生的任何损害不负任何赔偿责任，包括但不限于直接的、间接的、附加的个人损害或商业损失或任何其它损失。

意见反馈

派网非常欢迎和珍惜您的意见和建议，请通过下列方式反馈您对产品文档的意见和建议。

- 通过电子邮件反馈，请发送至 support@panabit.com。
- 通过 HTTP://forum.panabit.com/forum.php 网站在线反馈。
- 通过客户服务电话 4008981066 热线电话反馈。

目录

第一章 产品简介

1.1 产品综述

Panabit 是专门为运营商、金融、政府、教育、医疗、企业、酒店提供高性能、高可用性、功能丰富的出口一体化智能应用网关。目前设备最强处理能力为双向 80Gbps，适用于同时在线 60 万人的网络场景。能够满足用户对网络接入、管控、优化和审计的全方位需求，赋予用户最细粒度的可视、可控的网络管理能力，同时又能够提供高性能防火墙、路由、认证计费、上网行为管理、流量控制、智能链路负载均衡和网络分流器等其它增值服务。

1.2 产品规格

目前 Panabit 分为三大系列：

PA 系列：专门为企业网络提供的一款高性能、高可用性、功能丰富的出口一体化智能应用网关。适用于同时在线 1800 人以下的企业、政府、学校、酒店、商场、车站等有线和无线网络环境。能够满足用户对网络接入、管控、优化和审计的全方位需求，赋予用户最细粒度的可视、可控的网络管理能力，同时能够提供企业所关心的防火墙、路由、认证计费、上网行为管理、流量控制、智能链路负载均衡和网络大数据等其它增值服务。

PB 系列：专门为千兆网络环境提供的一款高性能、高可用性、功能丰富的出口一体化智能应用网关。适用于同时在线 **2 万到 60 万人**的运营商、高校、能源、大型企业集团客户等环境。能够满足用户对网络接入、管控、优化和审计的全方位需求，赋予用户最细粒度的可视、可控的网络管理能力，同时能够提供企业所关心的防火墙、路由、认证计费、上网行为管理、流量控制、智能链路负载均衡和网络大数据等其它增值服务。

PN 系列：专门为小区宽带运营商量身定制的、以租赁模式为主的高性能、高可用性、功能丰富的网络出口一体优化解决方案。特别适用于同时在线 800 人以下的小区宽带网络。不但可以满足用户对网络流量最细致粒度的可视、可控、可审计的核心需求，同时能够提供业内领先的应用分流、应用负载均衡、PPPoE、Radius 对接、共享检测、防封杀等丰富功能。

第二章 产品亮点

2.1 精准的应用识别

Panabit 在现网保持着超过 95%的流量识别率，可以识别和控制常见的 14 大类过千种应用，业界无出其右者。其中由派网自主定义的 PSDL 语言和流量智能分析机器人，让 Panabit 拥有了新应用识别快速反应的卓越能力。籍由互联网助力，派网拥有业内最庞大的测试队伍和最全面的测试环境，这是派网始终保持最快的未知应用样本获取速度、最精确的协议识别率的生态基础。

2.2 开放的操作系统

派网与大多数厂商不同，并未使用改装过的 Linux/Freebsd 等通用操作系统，而是使用派网自主研发的数据面操作系统 PanaOS。Panabit 产品采用虚拟化技术完成了数据层面和控制层面分离，从驱动、内存管理到任务调度等数据面核心任务，都由 PanaOS 一肩承担。利用虚拟化 OS 技术，PanaOS 赋予了产品软件永不宕机的超高稳定性。路由、NAT、负载均衡、应用识别与控制等关键基础设置内置于 PanaOS 之中，成为了为用户提供一体化解决方案的坚实基础。创新的 App 虚拟化引擎可以为加载第三方网关应用时提供环境和接口，PanaOS 具备无限的想象空间。

2.3 超高的处理性能

Panabit 智能应用网关的高性能及高稳定性早已获得业内公认，特别是在铁通、移动、广电等多个城域网 10G 节点案例中用实际表现赢得用户一致好评。当前最高上限性能：单板双向 80Gbit/s 吞吐、并发连接数 1800 万条、并发 IP 数 60 万个、新建会话连接数 65 万个/秒、65535 条策略。

2.4 独特的负载均衡

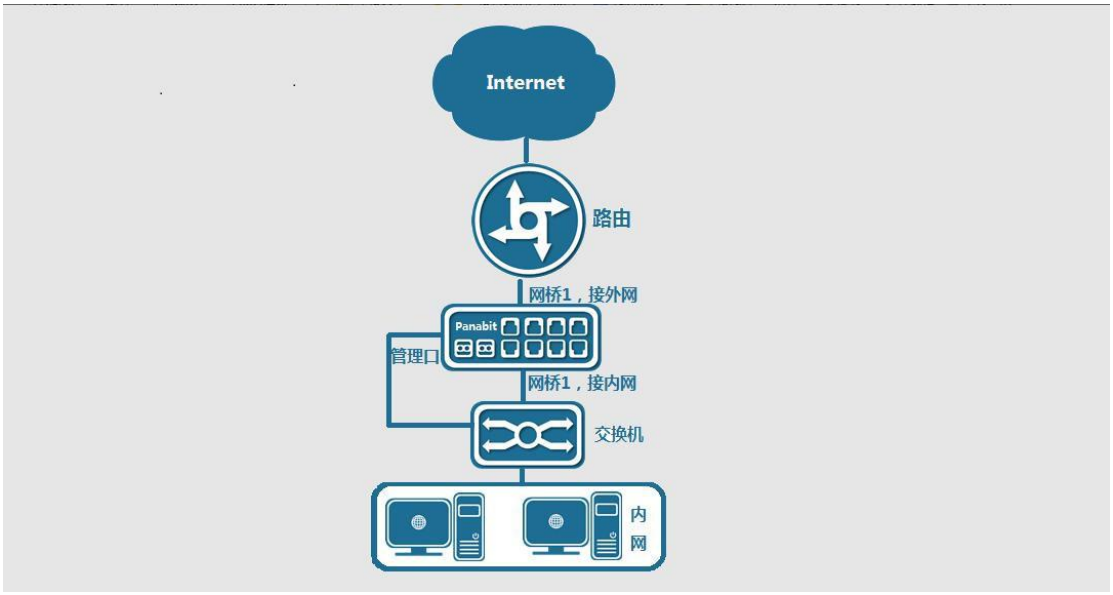
派网在业内率先提出应用路由和应用负载均衡的概念，并在 Panabit 产品中实现基于应用的路由策略、基于应用的负载均衡。以应用协议为调度实体，将数据流量路由到指定的链路和目标地址，并基于应用特性进行有针对性的负载均衡，最高支持多达 1024 条的线路负载汇聚。

第三章 网络部署

3.1 网桥部署

3.1.1概述

以网桥的形式，串接在核心与出口之间，网桥相对上下联设备来说是完全透明的。主要用来做应用分流、流量控制、上网行为管理以及网络分流器等等。



3.1.2基本配置

3.1.2.1 管理接口设置

除 console 口外，MGT（管理口）是管理和设置 Panabit 设备的唯一接口。默认初始 IP 为 192.168.0.200，登录方式 HTTPs://192.168.0.200，默认用户名/密码：admin/panabit

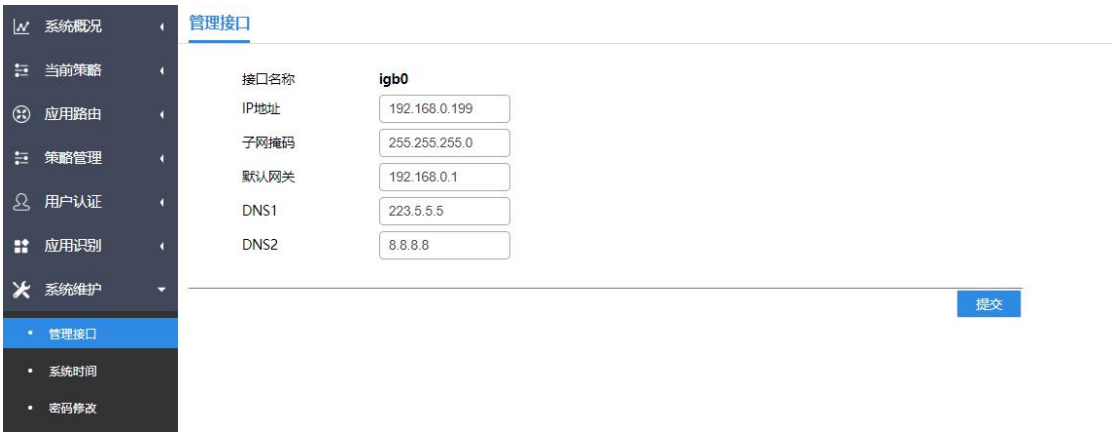
管理口的作用：

1） 管理和配置设备；

2） 发送日志信息给 panalog；

3） 作为 web 认证的 portal 接口；

从【系统维护】--【管理接口】，在这里可以设置管理口的 IP、网关以及 DNS。



通过超级终端连接 console，登录控制台默认用户名/密码：root/panaos

1) 控制台使用 ifconfig 命令，可以查看管理口状态；
2) 使用 ifconfig MGT（网卡名） IP，可以临时设置管理口 IP；
3) 控制台编辑/conf/ifadmin.conf 可以修改管理口 IP，重启生效。

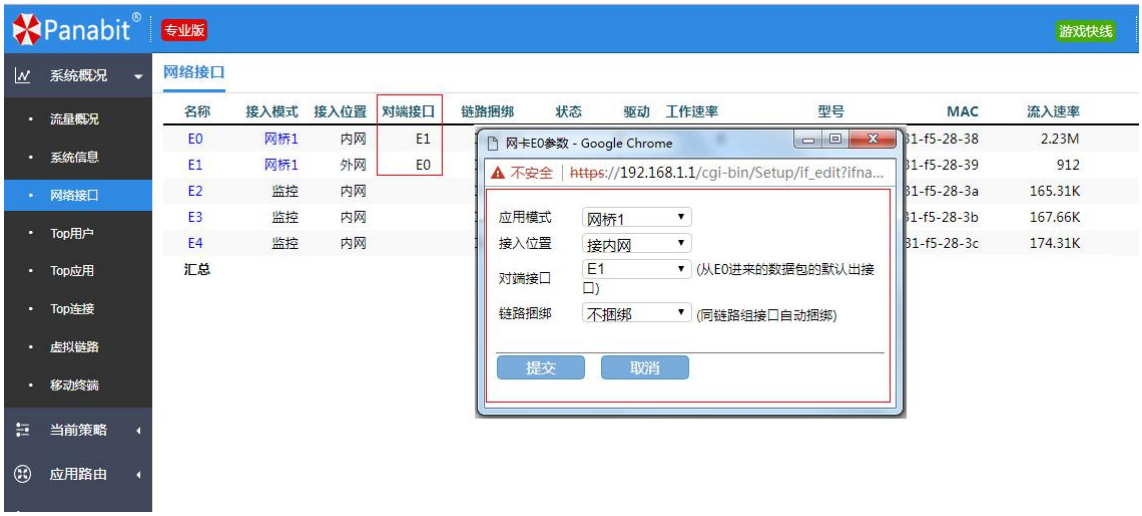
3.1.2.2 数据接口设置

从【系统概况】-【网络接口】进入设置界面，可看到所有的数据接口，并且对它们进行设置。

设置网桥时，每两个数据接口为一组网桥，将一个设置为“接内网”，另一个设置为“接

外网”，并且互为对端接口。

例如，Panabit 以网桥的形式，透明串接在核心路由与防火墙之间。接内网的接口与核心路由（靠近内网的设备）相连，接外网的接口与防火墙（靠近外网的设备）相连。

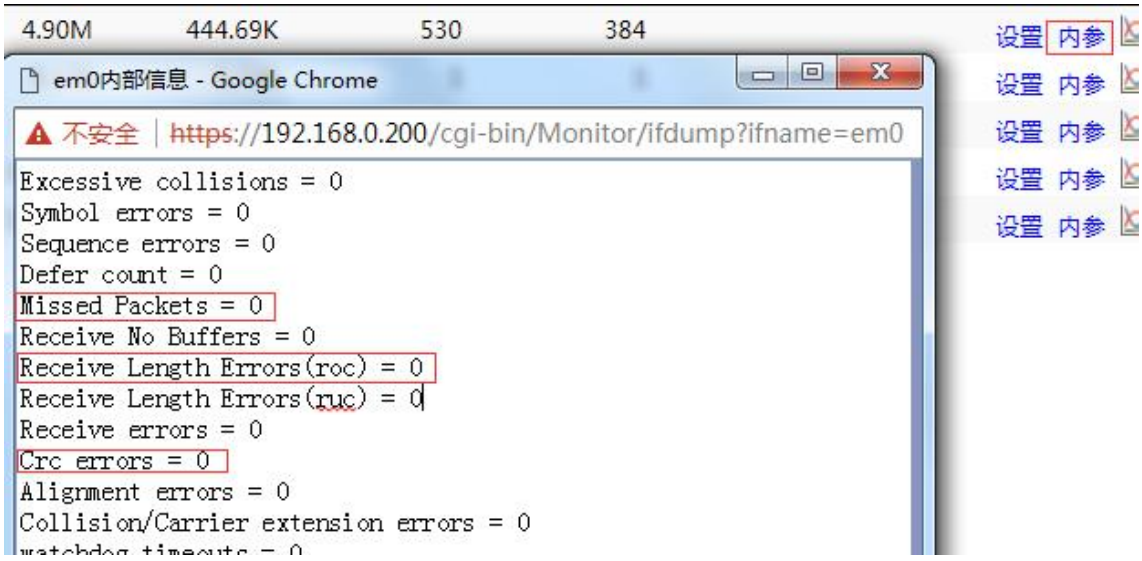


内参：接口内部参数，我们主要关心三个数据：

1） Missed Packets：这个数据如果不为 0 表示网卡有丢包，如果一直在增长表示当前正在丢包。

2） ReceiveLengthError(roc)：如果这个数据不为 0 表示有超过数据接口 MTU 的包被丢弃，默认为数据接口 MTU1516

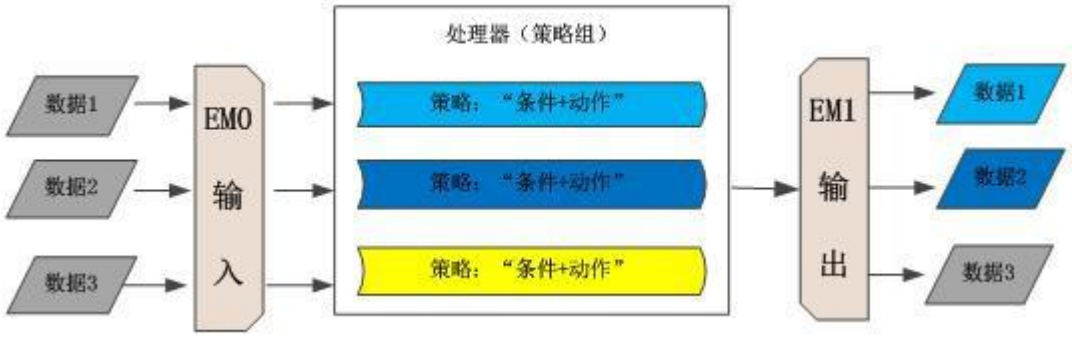
3） Crc error：物理外部原因会导致这个数据增加。



3.1.3流量控制配置

3.2.3.1 概述

在 Panabit 流控控制模块下，数据从内网接口进外网接口出，从外网接口进内网接口出，在这个过程中，Panabit 默认是不会对数据做任何干预的。要对数据进行干预，就需要配置策略。当数据匹配策略条件时，就会执行策略中相应的动作，比如“限速”、“阻断”“优先级”“数据镜像”等等。



3.2.3.2 流量控制配置的逻辑

从【策略管理】->【流量控制】进入配置界面首先建立一个策略组，一个策略组是若干条策略的集合在 Panabit 中所有功能的执行都是通过策略实现的，一条策略主要由三个要素组成：“策略序号”、“匹配条件”、“策略动作”

策略编号：在策略组中唯一标识该策略的编号，该编号区间范围（1~65535），策略编号决定了该策略在该策略组中执行的先后顺序，1 的优先级最高，65535 最低。
匹配条件：数据与策略是否匹配的根据，只有所有的条件都满足时候，Panabit 引擎才会执行策略中指定的动作。

线路及流向：匹配特定线路的数据报文，线路可选择 WAN 线路或网桥，流向可选择任意、上行、下行、上行发起、下行发起；
VLAN：匹配数据所携带的 VLAN-Tag，0 表示对任意 VLAN 均有效；
TTL：匹配数据包的 TTL 值，0 表示对任意 VLAN 均有效；
内网地址：匹配用户侧的 IP 地址，该地址可以是 XXX.XXX.XXX.XXX/NN 或 n.n.n.n-m.m.m.m 或是一个 IP 群组；

内网端口：匹配用户侧的端口号，可以是一个固定值或者一个范围值；

目标地址：如果源地址，目标地址是对匹配访问目标服务的 IP 地址，它的书写格式同源地址相同；

外网端口：匹配访问目标服务的端口号，可以是一个固定值或者一个范围值；协议&应用：对应用进行匹配，该“应用协议”为 Panabit 自身携带的应用特征库，可以选择协议库的某一个应用货某一个分类；

共享用户：匹配共享检测功能模块检测到的内网用户下的二级用户使用 window 客户端个数；

移动设备：匹配识别引擎，检测到内网用户下的移动终端个数；

QQ 用户数：匹配识别引擎，检测到内网用户下的 QQ 用户个数；

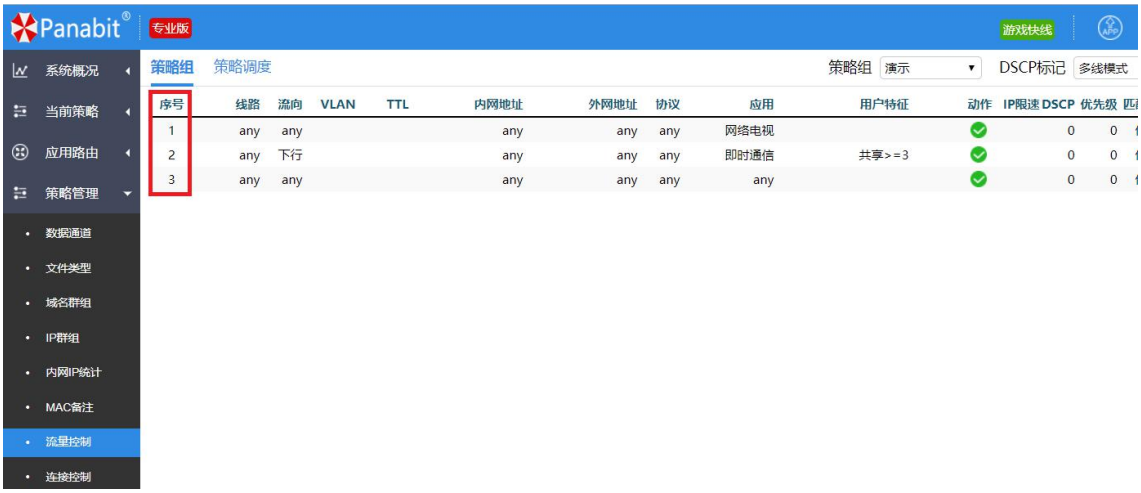
策略动作：当数据包符合策略中指定的所有条件时，Panabit 引擎就根据策略中指定的动作对数据包进行处理。流量控制的动作有“允许”、“阻断”、“调用数据通道”、“数据镜像”、“包转发”、“端口转发”、“优先级”、“内网 IP 限速”、“DSCP 标记”等等，这些动作是同时执行的。
动作过后：停止匹配/继续匹配停止匹配：数据匹配了这条策略后，立即执行动作，不再继续匹配策略组后面的策略继续匹配：数据匹配了这条策略后，立即执行动作后，再继续匹配策略组后面的策略。

策略调度：调度策略组，策略组被调度后策略开始生效。
Panabit 在调度策略组的时候，首先查看策略调度表，当策略调度表里的策略组都没有被调度，则使用缺省策略组。在任一时刻，只能调度一个策略组。

3.2.3.3 策略编号的设置原则

在一个策略组中会有若干条策略，我们在添加这些策略的时候，策略编号不要连续或者间隔太小，否则后期要加策略就会很不方便。

错误的配置方式：



正确的配置方式：

3.2.3.4 数据通道的设置原则

数据通道是对满足匹配条件的数据做整体的限速，如果使用通道优先级功能，通道带宽不要大于 2000000

当日限额：这个参数的单位是 Mbytes，当天流入该通道的数据超过这个限额后，后续进入通道的数据包都被丢弃

保证带宽：在数据通道内可以对每个优先级设置保证带宽，当数据流量没有超过保证带宽的数值时，它们的优先级是最高的。各个优先级保证带宽的数值之和不能超过数据通道大小。

3.2.3.5 优先级使用原则

1） 优先级是执行动作之一，对满足条件的数据报文，按照优先级进行排队；

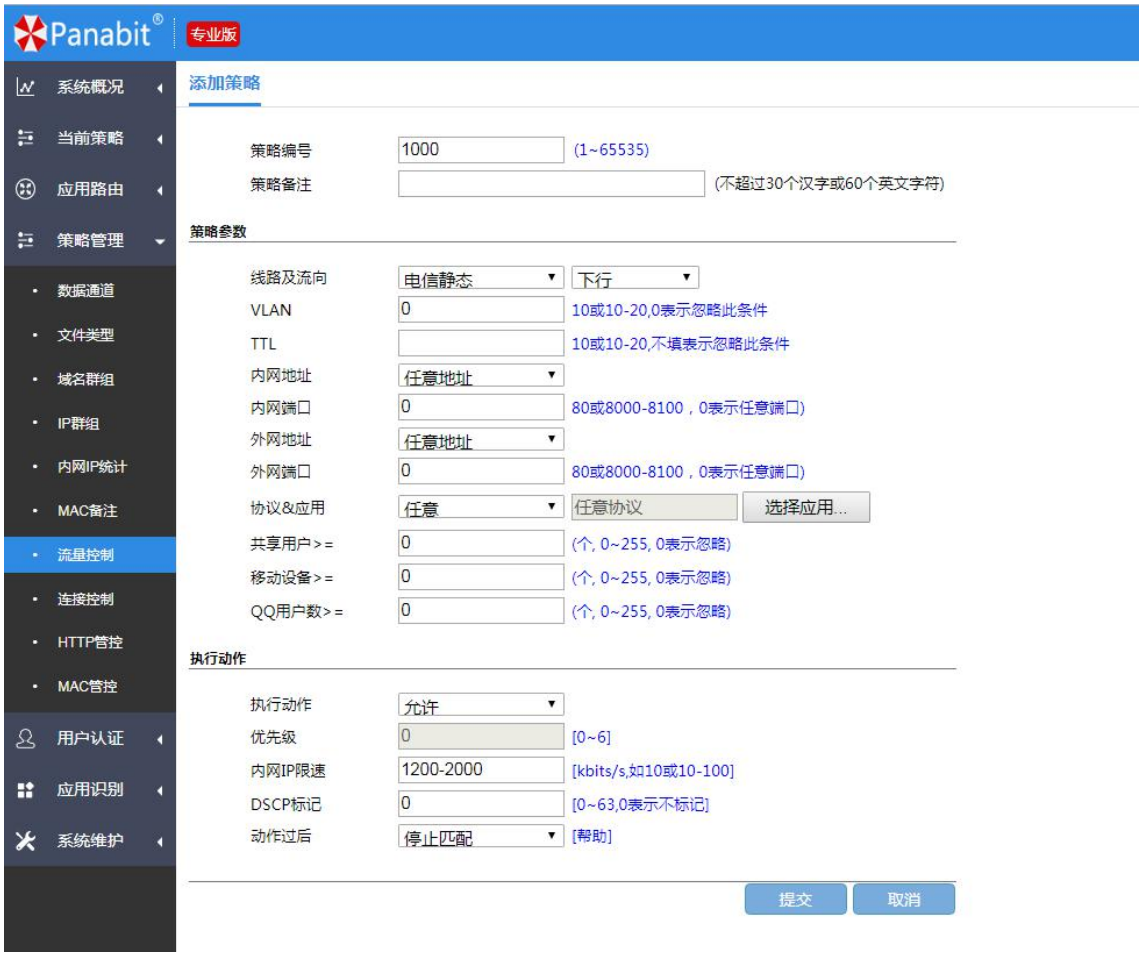
2） 优先级是在数据通道内实现，使用优先级必须先调用通道；

3） 在同一个数据通道内的数据才能彼此做优先排列；

4） 大于 1G 的数据通道不要做优先级，在大带宽的环境下优先级没有意义；

3.2.3.6 内网 IP 限速使用原则

1）内网 IP 限速可以是一个固定值，也可以是一个范围。



2）当内网 IP 限速要设置为一个范围是，需从【策略管理】->【流量控制】->【策略组】->【动态限速设置】，设置动态限速。

每条线路可设置一个带宽值，当动态限速启用后，Panabit 就会实时监控这条线路的流量，根据实时流量与默认带宽的比例，来动态调节内网 IP 限速。

3）当策略的内网 IP 限速是一个范围时，“匹配条件”中的线路必须为一条具体线路，不能是任意线路，并且动态 IP 限速也要处于“启用”状态，否则内网 IP 限速为设置范围的最小值。

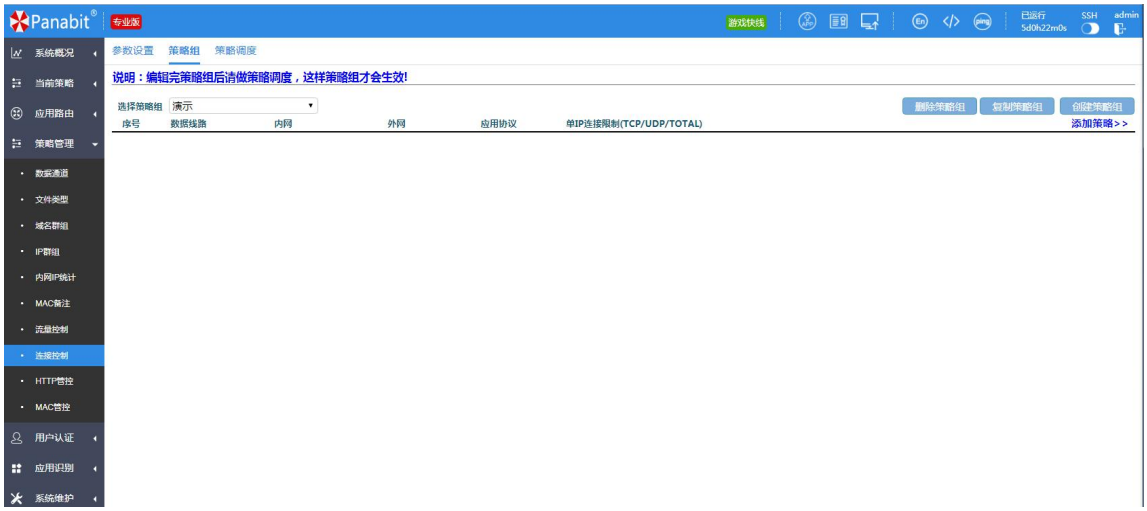
3.1.4 连接数控制配置

3.1.4.1 概述

针对内网每一个 IP 的并发连接数控制，可单独针对内网某个 IP 下的 TCP 连接、UDP 连接或整体的连接数进行管控。该功能适用于内网有主机中毒或木马，爆发疑似攻击现象时的临时处理或预先处理。

3.1.4.2 连接控制配置

从【策略管理】->【连接控制】进入配置界面首先建立一个策略组，一个策略组是若干条策略的集合。



选择创建策略组后，点击按钮“添加策略” 在 Panabit 中所有功能的执行都是通过策略实现的，一条策略主要由三个要素组成:“策略序号”、“匹配条件”、“策略动作”

策略标识：在策略组中唯一标识该策略的编号，该编号区间范围（1~65535），策略编号决定了该策略在该策略组中执行的先后顺序，1 的优先级最高，65535 最低。

匹配条件：数据与策略是否匹配的根据，只有所有的条件都满足时候，Panabit 引擎才会执行策略中指定的动作。在连接控制策略里，“数据线路”、“内网地址”、“内网端口”、“外网地址”、“外网端口”、“应用协议”这些为匹配条件。

策略动作：当数据包符合策略中指定的所有条件时，Panabit 引擎就根据策略中指定的动作对数据包进行处理。连接控制里对满足条件的数据执行的动作有，“每 IP 最大 TCP 连接数”，“每 IP 最大 UDP 连接数”，“每 IP 最大连接数”。

策略调度调度策略组后策略才会开始生效。

Panabit 在调度策略组的时候，首先查看策略调度表，当策略调度表里的策略组都没有被调度，则使用缺省策略组。在任一时刻，只能调度一个策略组。

参数设置从【策略管理】->【连接控制】->【参数设置】进入参数设置页面

对 DNS 连接：控制/不控制，如果选择不控制，即使在策略里做了对 DNS 的连接控制策略，系统也不会对 DNS 的连接做控制动作。

被拒绝的连接保持时间：连接被策略拒绝后，Panabit 在设的时间过后就会删除，如果为 0，那么 Panabit 按照默认的老化时间对连接进行删除。

内网 ip 最大连接数：这个是一个全局配置，内网 IP 的连接数达到设的值后，Panabit 不会再对该内网 IP 新建连接，如果为 0 不进行限制。

3.1.5HTTP 管控配置

3.1.5.1 概述

是针对用户使用 HTTP 协议行为访问外网时的一种控制手段，可根据用户访问的方式、访问的文件类型、访问的网页 URL 进行阻断、信息提示、镜像输出等的功能。

3.1.5.2 HTTP 配置

从【策略管理】->【HTTP 管控】进入配置界面首先建立一个策略组，一个策略组是若干条策略的集合。

选择创建策略组后，点击按钮“添加策略” 在 Panabit 中所有功能的执行都是通过策略实现的，一条策略主要由三个要素组成:“策略序号”、“匹配条件”、“策略动作”

策略标识：在策略组中唯一标识该策略的编号，该编号区间范围（1~65535），策略编号决定了该策略在该策略组中执行的先后顺序，1 的优先级最高，65535 最低。

匹配条件：数据与策略是否匹配的根据，只有所有的条件都满足时候，Panabit 引擎才会执

行策略中指定的动作。

源地址：支持格式为 192.168.0./24，192.168.0.1-192.168.0.254，或者一个 IP 群组，从【策略管理】->【IP 群组】定义 IP 群组；

访问方法：get，以 HTTP 的 get 请求为条件，post，以 HTTP 的 POST 请求为条件；

网站域名：选择一个域名群组，从【策略管理】->【域名群组】定义域名群组，群组内的域名为后缀匹配算法，比如 qq.com 相当于*qq.com，如果要精确匹配 qq.com 在域名前加^

文件类型：选择一个文件类型群组，从【策略管理】->【文件类型】添加文件类型群组；

共享用户：每个内网 IP 下检测到的共享用户个数，从【应用商店】->【共享检测】开启共享检测模块；

移动设备：每个内网 IP 下检测的移动终端个数，移动终端检测模块系统是默认开启的；

QQ 用户数：每个内网 IP 下检测到 QQ 号码

每 IP 只匹配一次：默认值为“否”，如果选择“是”每个内网 IP 匹配了策略条件一次后，这个内网 IP 不再匹配这条策略。

策略动作：当数据包符合策略中指定的所有条件时，Panabit 引擎就根据策略中指定的动作对数据包进行处理。HTTP 管控里对满足条件的数据执行的动作有，“允许”、“阻断”、“信息提示”、“URL 跳转”、“请求镜像报文”、“TCP 重置”

允许：对匹配条件的数据不执行任何动作。

阻断：对匹配条件的数据执行“阻断”动作。

信息提示：用户使用浏览器访问 HTTP 网页时，触发条件后会在浏览器显示弹出所输入的提示信息；

URL 跳转：触发条件后会在将用户访问的目标 URL 跳转至所输入的 URL，URL 重定向目标也可以是 IP；

输出线路/出口：网桥和网关的部署模式下使用 “原路返回”，旁路部署模式下，可以选择一条 WAN 线路，因为旁路模式下，重定向的数据从原路无法到达客户端，需要从其它（三层）接口返回到客户端。

请求报文镜像：将匹配条件的 URL 请求报文数据镜像至“目标接口”；

TCP 重置：对匹配策略的 TCP 连接发送 rst 报文，效果相当于阻断，这个功能适用于 HTTPS 的连接；

策略调度：

调度策略组后策略才会开始生效。

Panabit 在调度策略组的时候，首先查看策略调度表，当策略调度表里的策略组都没有被调度，则使用缺省策略组。在任一时刻，只能调度一个策略组。

3.1.6 MAC 绑定设置

3.1.6.1 概述

该功能模块可以配置内网 IP 与 MAC 的对应关系，将内网 IP 与 MAC 绑定，对不符合绑定规则的数据包做丢弃。

3.1.6.2 功能配置

基本配置

MAC 绑定：功能模块开关，默认关闭
未绑定 MAC 的 IP:对未绑定 MAC 的 IP 做的动作，包括允许通讯，拒绝通讯
白名单：可选择一个 IP 群组，群组内的 IP 不受 MAC 绑定模块的控制

已绑定 MAC
显示已绑定的 IP 和 MAC 列表，在这里可以添加 IP 与 MAC 的绑定关系

MAC 导出

导出已有的 IP 与 MAC

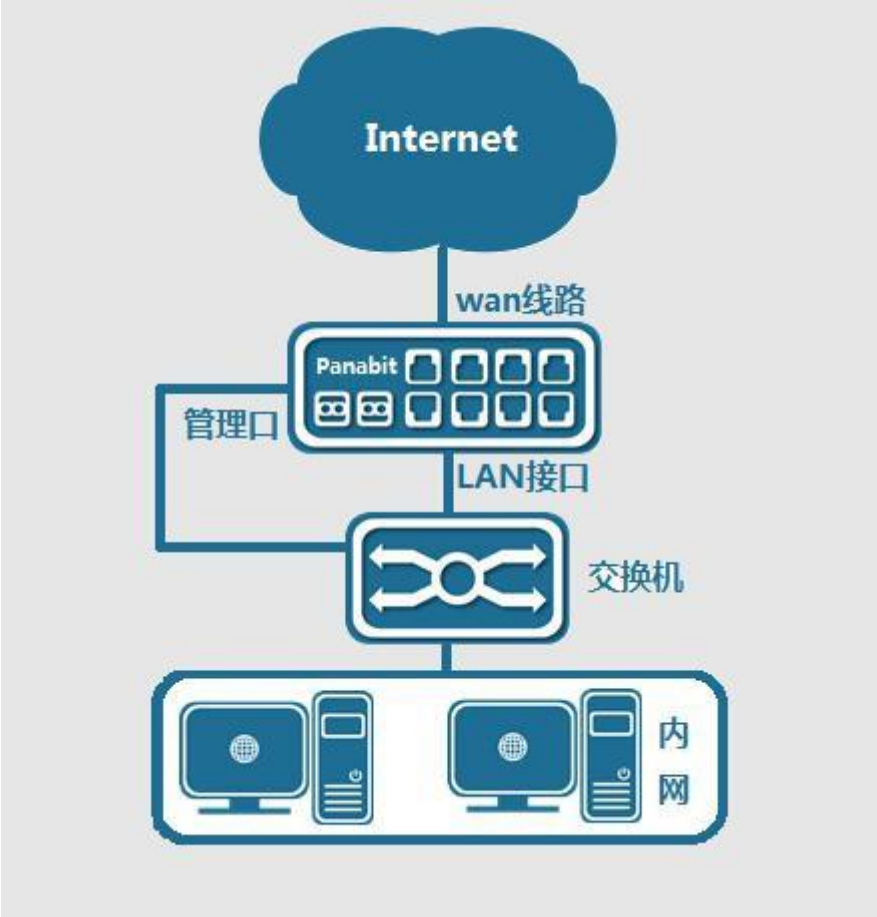
未绑定 MAC

显示当前未绑定的 IP 与 MAC 列表

3.2 网关接入

3.2.1 概述

以网关的形式，部署在网络的出口。提供内网 DHCP，PPPOE 认证，WEB 认证，高性能 NAT，静态路由，多链路负载均衡等服务。



3.2.2 基本配置

3.2.2.1 管理接口配置

除 console 口外，管理接口是管理和设置 Panabit 设备的唯一接口。

MGT（管理口）：管理和设置 Panabit 的唯一接口，默认初始 IP 为 192.168.0.200，登录方式 HTTPs://192.168.0.200，默认用户名/密码：admin/panabit

管理口的作用：

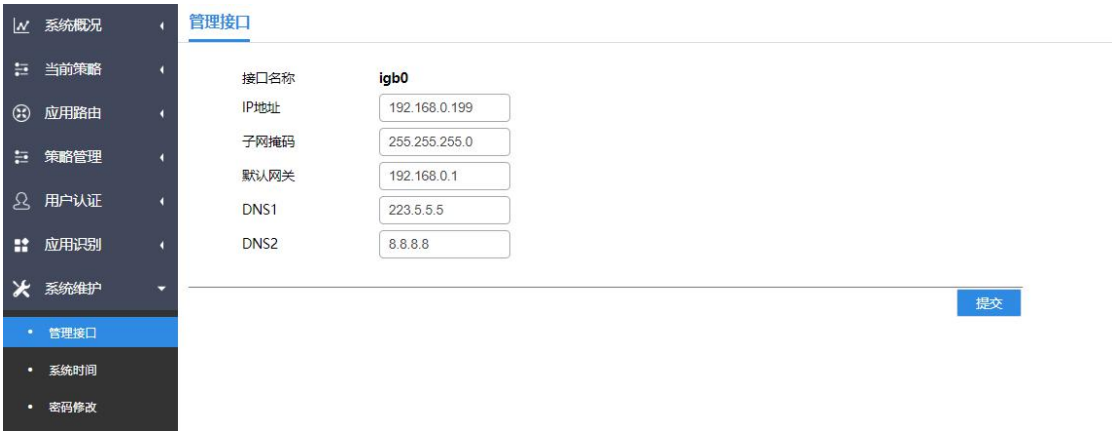
4） 管理和配置设备；

5） 发送日志信息给 panalog；

6） 作为 web 认证的 portal 接口；

管理接口的配置：

从【系统维护】--【系统管理】--【管理接口】，在这里可以设置管理口的 IP、网关及 DNS。



Console 接口

通过超级终端连接 console，登录控制台默认用户名/密码：root/panaos

3） 控制台查看管理口状态使用 ifconfig 命令，可以查看管理口状态；使用 ifconfig MGT（网卡名） IP，可以临时设置管理口 IP。

4） 控制台修改管理口 IP

/conf/ifadmin.conf ，这个是管理口 IP 的配置文件。编辑/conf/ifadmin.conf 可以修改管理口 IP，重启生效！

3.2.2.2 数据接口配置

从【监控统计】-【网络接口】进入设置界面，可看到所有的数据接口，并且对它们进行设置。

Panabit 作为网关时，【接入模式】设置为【监控模式】，对内网接入提供服务（LAN 接口，DHCP，PPPOE 认证等）的接口设置为“接内网”，对外网提供服务（NAT，DNS 管控等）的“接外网”。

3.2.3 接口线路配置

在 Panabit 上添加的不管是 LAN 接口或是 WAN 线路，都是建立在物理接口上的逻辑接口，一个物理接口可以建立多个逻辑接口，每个逻辑接口有自己的 MAC，LAN+WAN 的数量最大为 600。

LAN 接口设置

从【应用路由】--【线路接口】--【LAN 接口】添加 LAN 接口

接口名称：定义该“LAN 接口”的名称，注意建议不要使用特殊字符；
所在网卡：定义该“LAN 接口”是在哪一块物理网卡上所创建，注意数据网卡中必须有“接内网”属性的情况下，所在网卡才能有所选择，如果没有，选择框则为空；
IP 地址：定义 LAN 接口的 IP 地址，即内网用户的网关地址；
网络掩码：定义 LAN 接口 IP 地址的子网掩码位，注意 LAN 接口的掩码只是在端口映射的时候起作用；
VLAN-Tag：定义从该接口的数据报文所携带的 VLAN 标记，0 表示外出的数据不带 vlan 标记；
MTU：定义该接口传输数据的最大报文传输单元；
克隆 MAC：不使用自身携带的 mac 地址，而是使用自定义手工输入的 mac 地址；待机设置--
工作状态：正常状态，按照规则正常转发数据。
待机设置--待机状态：当初始状态为待机状态时，LAN 接口根据唤醒线路的状态来变换自己的状态。当唤醒线路处于激活状态。这个 LAN 接口就处于待机状态，接口相应的规则不会生效，相当于不存在；当唤醒线路处于断开状态，这个 LAN 接口就处于工作状态。

WAN 线路设置
从【应用路由】—>【接口线路】—>【WAN 线路】添加 WAN 线路

线路名称：定义该“WAN 线路”的名称，注意建议不要使用特殊字符；
所在网卡：定义该“WAN 线路”在哪一块物理网卡上所创建，注意数据网卡中必须有“接外网”属性的情况下，所在网卡才能有所选择，如果没有，选择框则为空；
MTU：定义该接口传输数据的最大报文传输单元；
VLAN：定义从该接口出去的数据报文所携带的 VLAN 标记，0 表示外出的数据不带修改 VLAN 标记，与进入接口时的 VLAN 保持一致。
克隆 MAC：不使用自身携带的 mac 地址，而是使用自定义手工输入的 mac 地址；
线路类型：可选择五种接入方式。

【静态 IP】，手动设置 IP、网关、DNS；静态 IP 可以设置 NAT 地址池，策略在做 NAT 的时候会将源地址转换为 NAT 地址池内的地址；

【PPPOE】，通过 PPPOE 的方式获取 IP、网关、DNS、；

【DHCP】，通过 DHCP 的方式获取 IP、网关、DNS；

【L2TP】，通过 L2TP 的方式获取 IP、网关、DNS；

【iWAN】，通过 iWAN 协议获取 IP、网关、DNS；iWAN 是 Panabit 私有隧道协议；

心跳服务器 IP：填写以后该线路地址会 ping 此 IP 进行线路健康的检查，如果 ping 不通心跳服务器的地址，则该线路由“正常”变更为“不通”；

DNS 服务器：当设置 DNS 管控策略的时候，这个选项才会起作用。

NAT 地址池：可以填入一段连续的 IP 地址，当该 WAN 线路作为 NAT 出口时，将轮询使用 NAT 地址池内的 IP

备注：对该线路进行备注，类似路由器的接口描述；

3.2.4 策略路由设置

概述

Panabit 路由控制模块，该模块的策略决定了数据报文转发的方式和方向，支持工作方式有，静态路由，高性能 NAT，或者两者同时工作。与传统路由相比较，基于应用的路由是该功能模块最大的亮点。

从【应用路由】->【策略路由】进入配置界面，点击按钮“添加策略”

每一条策略主要由三个要素组成:“策略序号”、“匹配条件”、“策略动作”

策略编号策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可编辑，也不可上下移动；

匹配条件

源接口：匹配哪一个接口的数据，可选择数据接口也可以选择逻辑接口；

VLAN：匹配数据所携带的 VLAN-Tag，0 表示对任意 VLAN 均有效；

TTL：匹配数据包的 TTL 值；

源地址：匹配用户侧的 IP 地址，该地址可以是 XXX.XXX.XXX.XXX/NN 或 n.n.n.n-m.m.m.m 或是一个 IP 群组；源端口：匹配用户侧的端口号；目标地址：如果源地址，目标地址是对匹配访问目标服务的 IP 地址，它的书写格式同源地址相同；外网端口：匹配访问目标服务的端口号；

传输协议：对使用服务的传输层协议进行匹配，有 TCP、UDP；

应用协议：对应用进行匹配，该“应用协议”为 Panabit 自身携带的应用特征库，可以选择协议库的某一个应用货某一个分类；

DSCP：对 DSCP 值进行匹配；

执行动作：Panabit 的策略路由基于会话的进行数据转发。当数据报文与策略所有的条件匹配后所执行的动作，路由策略里动作主要包含“路由”，“NAT”，“代拨用户”。

【路由】：指对匹配会话的数据包不改变其源地址，并从指定的线路进行数据转发；

【NAT】：指对匹配会话的数据包进行源地址转换，并从指定的线路进行数据转发；

【代拨用户】：将匹配了代拨策略的用户进行源地址转换，并从相应的代拨线路做数据转发；

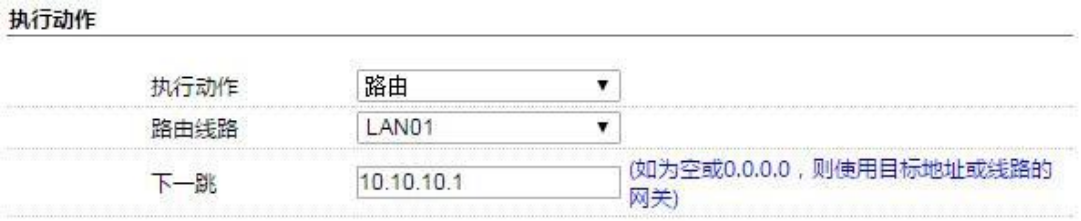
DNAT：当执行动作为“NAT”时，可以将匹配策略条件的会话的目标 IP 进行转换，转换为设定的 IP 地址。

路由线路：当执行动作为“NAT”时，可以选择 WAN 线路，或者 WAN 线路群组，或者“空线路”，选择“空线路”表示数据从网桥转发；当执行动作为“路由”时，可以选择 WAN 线路，或者一个 LAN 接口；

下一跳：指定数据转发的下一跳。

如果执行动作为“NAT”，下一跳为空，动作后的数据报文则向路由线路的网关地址转发，如果不为空，数据报文则向所选择线路的网关转发；

如果执行动作选择的是“路由”，LAN 线路是没有网关的，所以要填写 LAN 对端的互联地址；



3.2.5 负载均衡设置

概述

对多条 WAN 线路进行捆绑，数据包报文会根据策略分摊到多条 WAN 线路上转发，实现基于连接的多线路负载均衡。

线路群组设置从【应用路由】->【线路群组】进入配置界面，系统默认自带 12 个 WAN 群组。

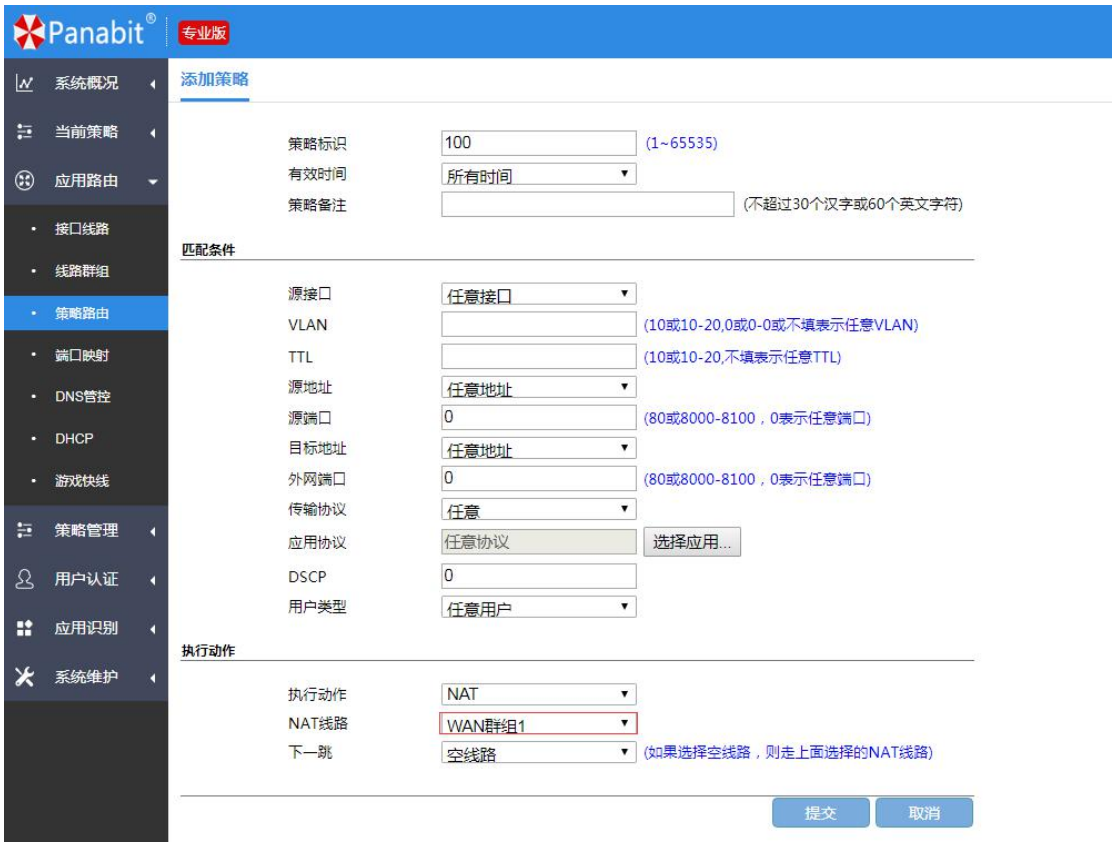
点击按钮“[+]”，进入线路群组成员配置界面。

勾选需要添加到群组内的 WAN 线路成员带宽比重：每条线路的负载比重，比如有 3 条 WAN 线路，带宽分别为 10M、50M、100M，那么带宽比重建议分别使用 1、5、10

点击“群组名称”，进入群组属性配置界面

群组名称：自定义该线路群组的名称
负载类型：根据所选负载类型，决定负载均衡的算法
【源地址+目的地址】：以会话的源地址和目的地址为条件进行计算；
【源目地址+源目端口】：以会话的源端口、目的地址、源端口、目的端为条件进行计算；
【源地址】：以会话的源地址为条件进行计算；
【源地址+源端口】：以会话的源地址和源端口为条件进行计算；
【目的地址】：以会话的目的地址为条件进行计算；
【目的地址+目的端口】：以会话的目的地址和目的端口为条件进行计算；
举例：比如有 2 条 WAN 线路，带宽分别为 10M、50M，那么带宽比分别为 1、5，负载类型为目的地址。用户总共发出 4 个请求，请求报文的目的地址分别是，A、B、C、A。经过以目的地址为条件的负载算法后，结果是，第一个请求负载到 10M 线路，第二个请求负载到 50M 线路，第三个请求负载到 50M 线路，第四个请求负载到 10M 线路。

线路群组调用从【应用路由】->【策略路由】进入配置界面，点击按钮“添加策略”



在执行动作的 NAT 线路选择调用线路群组，满足匹配条件的数据报文会按照线路群组的设置进行负载均衡。

3.2.6 端口映射设置

3.2.6.1 概述

当内网服务器为私网 IP，并且需要对外网用户提供服务时，则需要将内网服务器的 IP 映射到某条公网线线路上，外网用户就能通过映射的公网地址与端口访问内网服务器。

3.2.6.2 策略设置

从【应用路由】->【端口映射】进入配置界面添加映射

WAN 线路：指定映射的公网线路

目标 IP：当 WAN 线路有 NAT 地址池时，可以指定 NAT 地址池中的一个 IP 作为映射的公网 IP

目标端口：指定映射的端口，可以为多个，比如 80,443,8080；可以为一个范围，比如 2000-2100；

协议：TCP 或 UDP

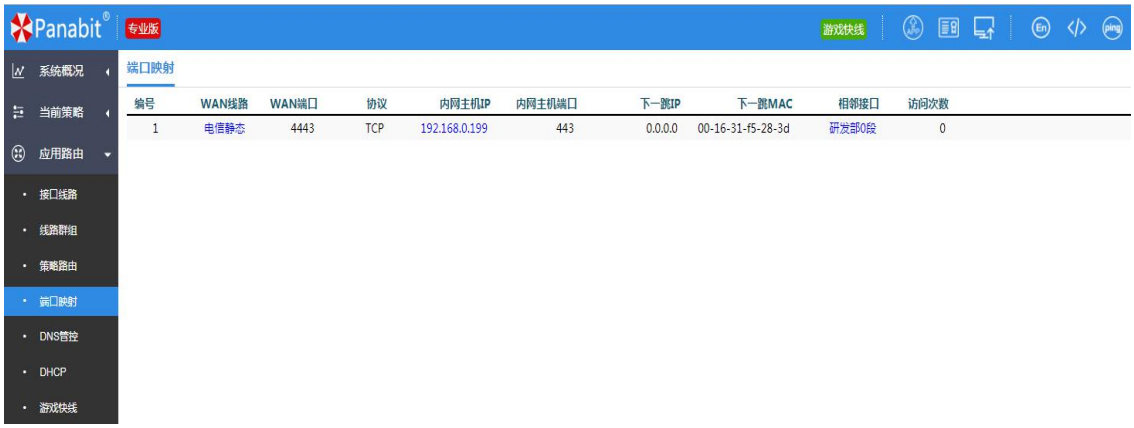
内网主机 IP：指定映射的内网服务器 IP

内网端口：指定映射的内网服务端口，如果为 0，表示与目标端口一致

下一跳：默认为 0.0.0.0，如果内网服务器的网关不是 Panabit 的 LAN 接口，则需要指定 LAN 接口对端路由器的 IP 地址；

当端口映射建立成功后，Panabit 会根据规则所填的内网主机 IP 或者下一跳 IP，自动内网主机定位在哪个 LAN 接口的子网之下，此时 LAN 接口的子网掩码才真正发挥作用。
当下一跳 MAC 显示正常的 MAC 地址，映射规则才算真正生效。

每条端口映射策略相当于一条策略路由策略。



3.2.7 DNS 管控配置

3.2.7.1 概述

针对 DNS 数据报文进行特殊控制的功能模块，可对 DNS 数据报文进行丢弃，劫持，重定向，QPS 限速等操作。

3.2.7.2 DNS 管控

从【应用路由】—>【DNS 管控】—>添加 DNS 管控策略

每一条策略主要由三个要素组成:“策略序号”、“匹配条件”、“策略动作” 策略编号：策略的编号，系统将按照编号从小到大的方式依次执行策略表，该编号不可编辑，也不可上下移动；

策略条件：
路径：可选择某个网桥或全部路径内的数据进行匹配；
VLAN：匹配数据报文的 VLAN-Tag；
源接口：可选择某个内网物理接口或逻辑 LAN 接口进行匹配；
源地址：匹配用户侧的 IP 地址，该地址可以是 XXX.XXX.XXX.XXX/NN 或 n.n.n.n-m.m.m.m 或是一个 IP 群组；
DNS 服务器：匹配用户侧所请求的 DNS 服务器地址；

访问域名：匹配用户侧的 DNS 报文所含的域名，可指定一个域名列表；

应用协议：对应用进行匹配，该“应用协议”可以是特征库或者自定义协议，并且关联了域名特征，否则该策略无意义；

执行动作：执行动作就是当数据报文与上述的策略条件相匹配后所执行的动作，DNS 控制策略里针对
DNS 数据报文的动作主要包含“允许”、“丢弃请求”、“重定向至”、“请求解析”、“QPS 限制”、“代拨重定向”。

【允许】：对匹配策略的 DNS 数据报文不经过任何改变，直接放行；

【丢弃请求】：对匹配策略的 DNS 数据报文直接丢弃；

【重定向至】： 对匹配策略的 DNS 数据报文，将目标 DNS 地址转换为所设 WAN 线路上的 DNS 地址或者牵引 DNS 选项内的 DNS，并且对 DNS 数据报文的源地址转换为 WAN 线路地址；

【牵引 DNS】：对匹配策略的 DNS 数据报文，将目标 DNS 地址转换成所设置的 IP，最多可以设置 4 个，该设置优先于 WAN 线路 DNS 设置。

以下情况不会执行 DNS 重定向动作：

1） WAN 线路的 DNS 服务选项，牵引 DNS 选项为空；

2） DNS 数据报文的目的 DNS 服务器与牵引的目标 DNS 服务器 IP 相同；

【请求解析】：对匹配策略的 DNS 数据报文，直接返回的域名解析结果，返回的解析结果为所填 IP 地址；

QPS 限制：对匹配策略的 DNS 的 QPS 做限制。

【总 QPS】：对整体每秒最大请求数的限制

【单用户 QPS】：对单个 IP 每秒最大请求数的限制

3.2.8 DHCP 配置

3.2.8.1 概述

提供内网 DHCP 接入的功能模块。DHCP 服务依赖于 LAN 接口，每个 LAN 接口相当于一个 DHCP 服务器。目前单台设备 DHCP 客户端最大支持 4096 个。

3.2.8.2 服务配置

从【应用路由】->【DHCP】->【服务设置】进入 DHCP 服务配置页面

DHCP 服务：DHCP 模块控制开关

绑定 IP 与 MAC：当启用后，在个客户端分配 IP 地址后，会自动将客户的 IP 和 MAC 绑定

静态分配：可将指定 IP 分配给指定的 MAC。

租户信息：显示已分配的 IP 与客户机 MAC，可以在该页面对已在线的 DHCP 客户转换为静态。

从【应用路由】->【接口线路】点击一个【LAN 接口】进入单个 DHCP 服务配置页面

DHCP 服务：默认关闭，选择启用后，开启此 LAN 接口的 DHCP 服务；

VLAN 范围：可以为一个固定值或者一个范围值，如 100 或 100-200，不填或填 0 表示只响应不带 VLAN 的 DHCP 报文请求；

可分配地址：DHCP 服务器分配给客户端的地址范围；

默认网关：DHCP 服务器分配给客户端的网关；

网络掩码：DHCP 服务器分配给客户端的网络掩码；

主 DNS 服务器：DHCP 服务器分配给客户端的主 DNS；

次 DNS 服务器：DHCP 服务器分配给客户端的次 DNS；

无线控制器：DHCP 服务器分配给客户端的 AC 地址；

租约时间：DHCP 的租约时间；

3.2.9 iWAN 服务

3.2.9.1 概述

提供 iWAN 接入功能模块。iWAN 是 Panabit 自研的 VPN 隧道技术。其特点为：客户端与服务端建联速度快，报文头小传输效率高，特有加密算法保障安全。再配合 Panabit 的应用识别，可为用户提供优质的 SD-WAN 服务。

3.2.9.2 iWAN 配置

从【应用路由】->【iWAN 服务】->【服务列表】进入 iWAN 服务配置页面

添加服务：

服务器名：定义该服务器（逻辑接口）的名称；

物理网卡：定义逻辑接口所在的数据网卡，前提条件是数据接口的网卡必须设置“接内网”的情况下，该选择框才会有供选择的项；

服务网关：定义该接口的 IP 地址；

MTU：义数据的最大传输单元；

认证方式：提供本地认证（本地提供拨号计费服务）、RADIUS 认证（第三方 RADIUS 提供认证计费）、和免认证（任意用户和密码均可拨号上网）三种认证方式；

默认地址池：默认地址池为免认证时或第三方 RADIUS 认证时使用；

服务映射

iWAN 主要用于外网用户接入到内网，服务映射就是将指定外网线路端口打开。客户端可通过指定的线路 IP 和接口接入到指定的 iWAN 服务。

服务日志

记录 iWAN 客户端接入的日志

在线用户

列出当前在线的 iWAN 用户

3.2.10 应用分流配置

3.2.10.1 概述

介绍 Panabit 基于应用的分流策略。Panabit 在网关部署和网桥部署下，都可以实现基于应用的策略路由。做应用分流的策略时，执行动作使用“NAT”效果最佳。

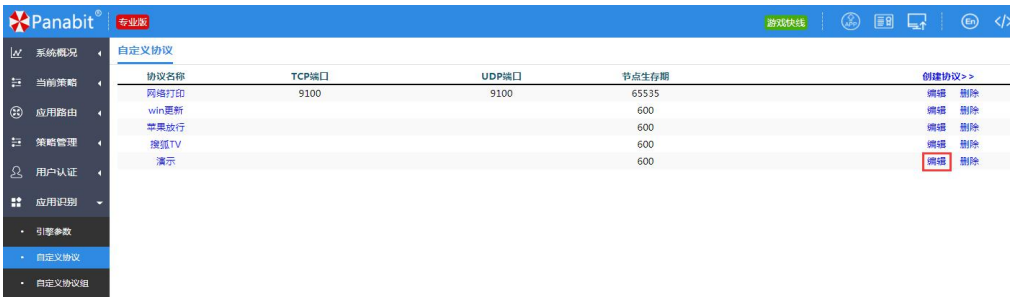
3.2.10.2 基于应用的分流策略

以分流“P2P 下载”为例，网桥模式下没有 LAN 接口的概念，在添加分流策略时，源接口条件选择网桥“接内网”的数据接口、应用协议选择“P2P 下载”、执行动作选择“NAT”，NAT 线路选择一条 WAN 线路。

3.2.10.3 基于域名的分流策略

1） 创建自定义协议从【应用识别】->【自定义协议】创建一个自定义协议，只填定义英文名称和中文名称，其余默认。

2） 关联域名编辑创建好的自定义协议。

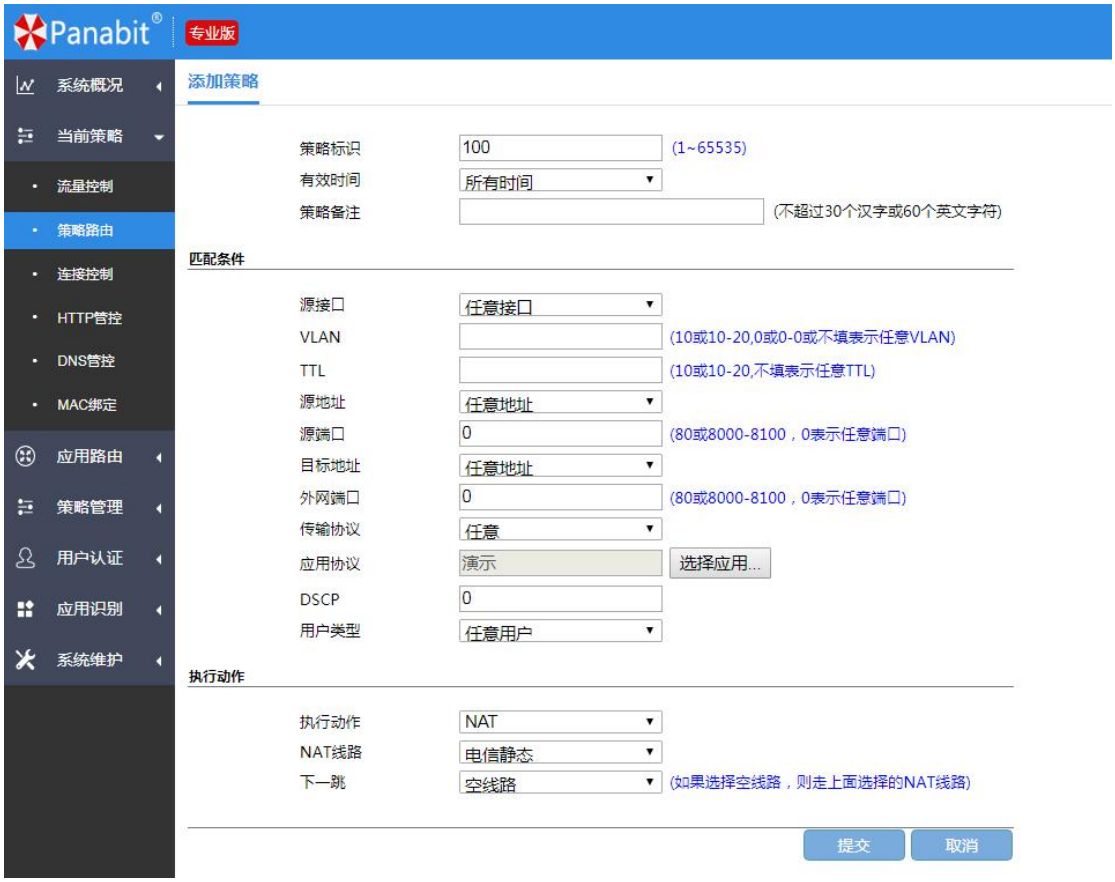


在域名关联选项里，将域名与协议关联。以下图为例：

域名：域名匹配采用后缀匹配算法，比如 qq.com 实际等于*qq.com；端口：可以跟踪两个端口，如果其中一个端口填 65535，那么表示跟踪所有端口；跟踪 DNS：跟踪记录 DNS 解析结果，将 DNS 报文有关*qq.com 的解析的 IP 地址记录到这个自定义协议的节点中；
跟踪 host：跟踪记录数据报文的 host 字段，将 host 字段所含的 IP 地址记录到这个自定义协议的节点中；

3） 添加策略路由

添加策略路由的时候在“应用协议”条件选择创建的自定义协议，这个自定义协议也就代表了*qq.com。



3.2.11 用户认证

概述

Panabit 认证功能模块，涉及的内容包括 PPPOE 认证，PPPOE 代理认证，PPPOE 代拨认证，PPPOE 旁认证，iWAN 接入认证，web 认证；

3.2.12 账号管理

地址池

一个地址池相当于一个用户组，用于对本地用户的归类，每一个本地用户必须关联一个地址池（用户组）。如果是本地认证的 PPPOE 用户，地址池还负责分配 PPPOE 用户的 IP 地址。

用户组名称：自定义，不超过 8 个汉字或者 15 个英文字符；
地址范围：给 PPPOE 用户拨号后分配的 IP 地址范围；
用户上线限制：属于该用户组的用户上行限速；
用户下行限制：属于该用户组的用户下行限速；
用户 DNS：给 PPPOE 用户拨号后分配的 DNS 地址；
在线时间：给 PPPOE 用户拨号后允许连续在线时间；
对过期账号：对到期的 PPPOE 用户是否允许拨号成功；
代拨控制：设置该地址池（用户组）是否输入代拨用户组；
代拨 VLAN：给用户代拨时使用的 VLAN；
代拨服务名：给用户代拨是使用的服务名；

账号并发：设置一个代拨账号关联的内网 IP 数，0 表示不限；
拨号次数：代拨失败后重拨的次数，0 表示不限；

用户账号

添加和管理本地账号，本地账号可以用于，PPPOE 认证，WEB 认证，iWAN 客户端认证

服务组：选择一个地址池（用户组）；
账号名称：自定义不超过 30 个英文字符或者 15 个中文字符；
账号密码：自定义不超过 30 个英文字符；
开通日期：用户生成时间；
最后有效期：用户到期时间；
绑定 MAC：默认不绑定，绑定后不仅认证用户名和密码，还会认证用户的 MAC 地址；
绑定 VLAN：默认不绑定，绑定后不仅认证用户名和密码，还会认证用户的 VLAN；
最大在线用户数：账号允许同时在线的终端数；
代拨 VLAN：给用户代拨时使用的 VLAN；

临时账号

该模块账号用于 web 认证，账号密码由系统生成，也可以自己添加，在一定时间后账号会被删除。

临时账号登录：允许登录/不允许登录；
最大空闲时间：账号生成后，在最大空闲时间内如果无人登录，则账号会被删除；
最大使用时间：账号登录后，在最大使用时间能可以处于已认证状态，超时后系统会将其下线；

代理账号

适用于 PPPOE 拨号场景，当用户使用的 PPPOE 账号命中代理账号拨号时，Panabit 会使用代理账号和用不拨号所使用的密码，去运营商的 bras 上拨号，这个过程对用户无感知。

服务组：选择一个地址池（用户组）；
账号名称：自定义不超过 30 个英文字符或者 15 个中文字符；
网络出口：选择一个“接外网”的数据接口
外层 VLAN：代理拨号时使用的外层 VLAN；
内层 VLAN：代理拨号时使用的内层 VLAN；
开通日期：用户生成时间；
最后有效期：用户到期时间；

3.2.13 PPPOE 认证配置

概述

提供内网 PPPOE 拨号认证接入的功能模块，主要用于小区宽带运营，校园网运营等应用场景。

目前单台最大支持 30000PPPOE 用户同时在线。

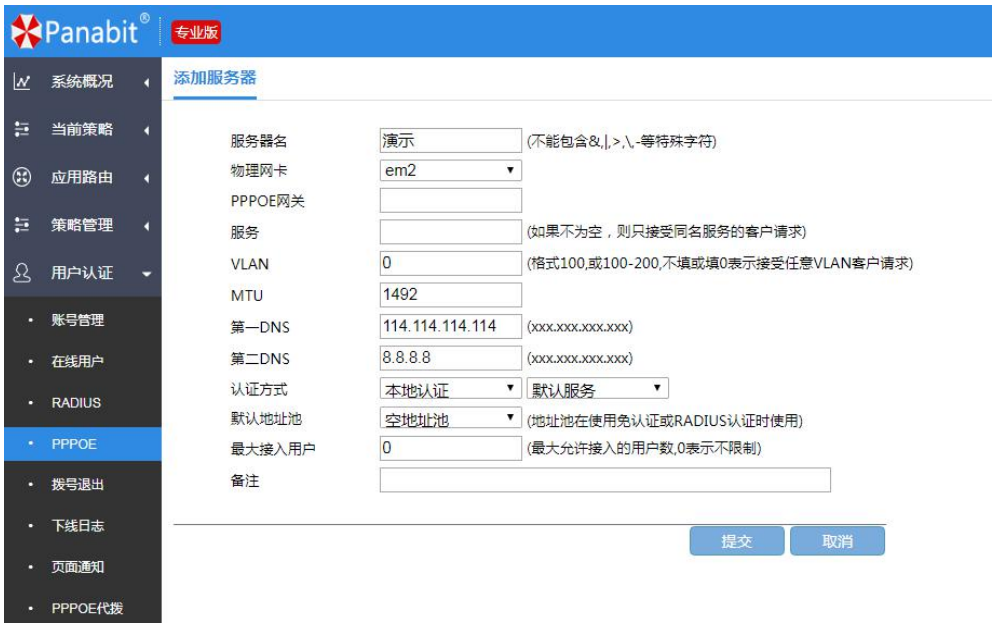
3.2.13.1 基本配置

从【用户认证】->【PPPOE】->【基本配置】进入配置界面

PPPOE 接入服务：功能模块的开关，默认不启用，选择启用会开启 PPPOE 接入服务；
缓存流量限速：当 Panabit 与 iXCache 对接时，可以通过这个选项控制用户访问 iXCache 经过 Panabit 时是否限速；
MAC 自动绑定：默认不启用，选择启用后，对本地账号在第一次登录时自动将账号和对应的 MAC 绑定；
客户端心跳保持：当内网用户无流量时，PPPOE 服务器会发包探测这个用户是否在线，如果指定时间内没有对探测做回应，那么 PPPOE 服务器会删除这个用户的在线状态；
过期用户在线时间：用户过期后允许在线的时间，目的是让用户可以看到过期提醒；

3.2.13.2 服务列表

从【用户认证】->【PPPOE】->【服务列表】添加 PPPOE 服务器



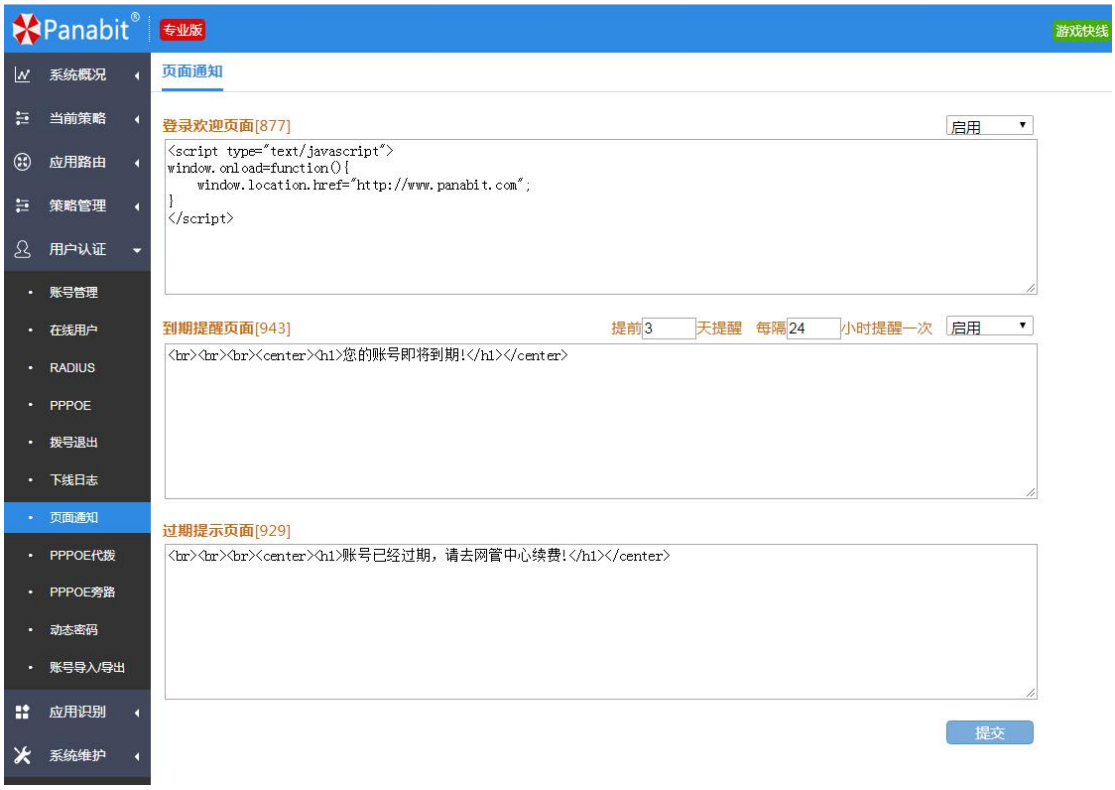
PPPOE 服务器和 LAN 接口一样，属于一个在接入位置为“接内网”的数据接口上的一个逻辑

接口

服务器名：定义该服务器（逻辑接口）的名称；
物理网卡：定义逻辑接口所在的数据网卡，前提条件是数据接口的网卡必须设置“接内网”的情况下，该选择框才会有供选择的项；
PPPOE 网关：定义该接口的 IP 地址；
服务：定义对指定字段的服务进行服务，如果为空则对所有的服务都进行服务；
VLAN：定义相应 PPPOE 请求服务报文的 VLAN，如果为 0 则忽略，相应任意 VLAN 用户的请求服务；
MTU：定义数据的最大传输单元，默认为 1492；
第一、第二 DNS：为拨号用户的拨号请求提供 DNS 服务器的地址和备选地址；
认证方式：提供本地认证（本地提供拨号计费服务）、RADIUS 认证（第三方 RADIUS 提供认证计费）、先本地后 RADIUS 认证、和免认证（任意用户和密码均可拨号上网）四种认证方式；
默认地址池：默认地址池为免认证时或第三方 RADIUS 认证时使用；
最大接入用户：定义该服务接口最大的接入用户的数量；
备注：对该线路进行备注，类似路由器的接口描述；如下为建立的 PPPOE 拨号服务器接口图：

3.2.13.3 其它选项

页面通知：对不同状态下的用户进行 html 页面通知推送登录欢迎页面：用户拨入后打开第一个 html 页面能看到的页面，只推送一次。
到期提醒页面：用户即将到期的通知推送，可根自己定义时间间隔进行反复推送。
过期提示页面：对过期的用进行通知推送，如果用户处于过期状态，浏览器会一直看到这个页面



在线用户：显示所有在线用户的信息

下线日志：显示用户下线原因

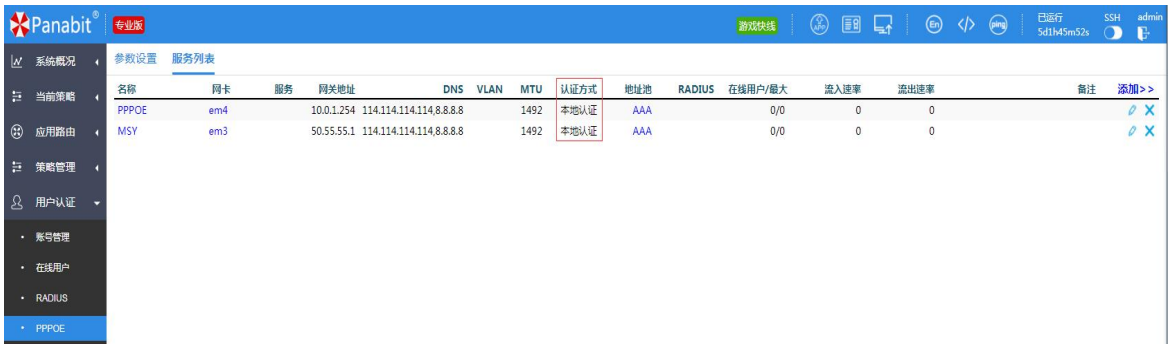
3.2.13.4 本地认证

概述

由 Panabit 完成认证与计费，用户的账号信息都存在 Panabit 里，本地认证最大可添加的用户数为 12K 。

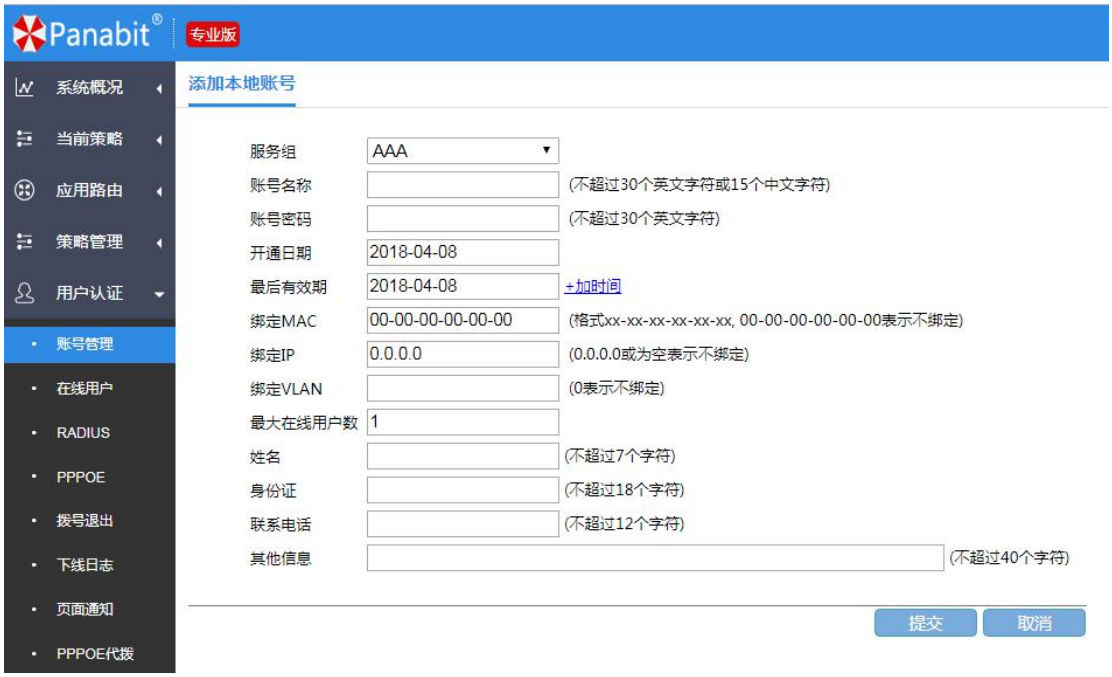
设置方法

1） **建立 PPPOE 服务器**，认证方式选择本地认证



2） **设置地址池**：从【用户认证】->【账号管理】->【地址池】进入配置界面，地址池负责分配用户 PPPOE 拨号后获取到的 IP 地址，DNS，限速值等。

3） 设置账号：从【用户认证】->【账号管理】->【本地账号】，点击添加账号，进入设置界面



服务组：选择一个地址池，表明该账号属于哪个地址池，受哪个地址池的参数控制；
账号名称：用户进行 PPPOE 拨号认证的用户名；
账号密码：用户进行 PPPOE 拨号认证的密码；
开通日期：用户的创建时间；
最后有效期：用户的到期时间，可以点加时间进行快速操作，比如加半年，加一年等等；
绑定 MAC：将用户名与 MAC 绑定，不符合绑定关系拒绝认证；
绑定 IP：将用户名与 IP 绑定，用户认证成功后分配绑定的 IP 给用户，绑定 IP 要在所选服务组的地址池内；
最大在线用户：允许这个用户可以同时认证的次数；姓名、身份证、联系电话、其它信息：用户资料信息

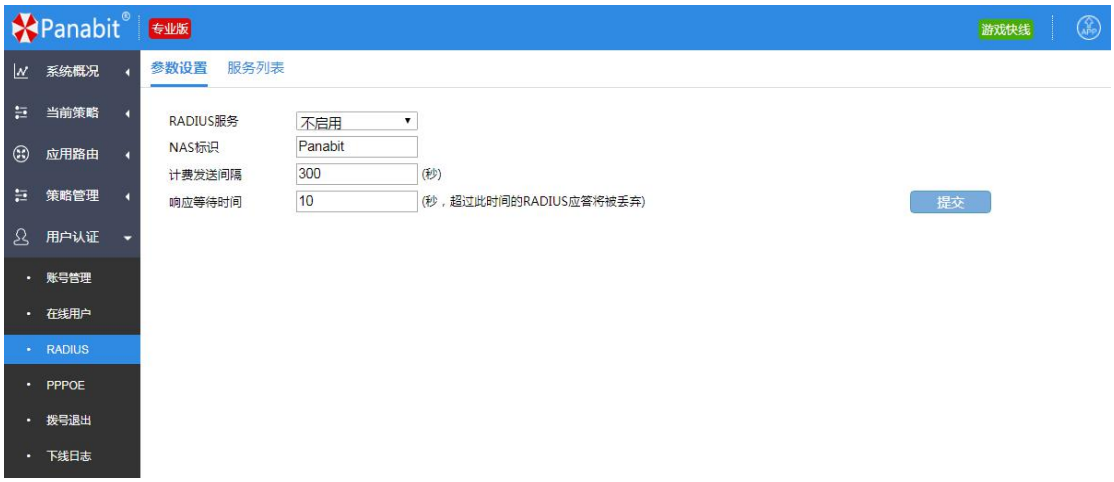
4） 完成以上三步，就可以实现本地认证。

3.2.13.5 Radius 认证

概述

由 Panabit 提供 PPPOE 接入服务，由第三方 radius 软件完成认证与计费，radius 认证最大可支持 30000 用户在线。

基本参数
从【用户认证】->【radius】，进入设置页面。



Radius 服务：控制 radius 认证的开关，默认不启用，选择启用后可以与第三方 radius 对接；
NAS 标识：与 radius 通讯时所带的标识，radius 可以通过这个标识识别数据是否合法；
计费发送时间：向 radius 服务器发送计费包的时间间隔；
响应等等时间：向 radius 服务器发送认证或者计费包后，在设定时间内没有回应，即认为超时；

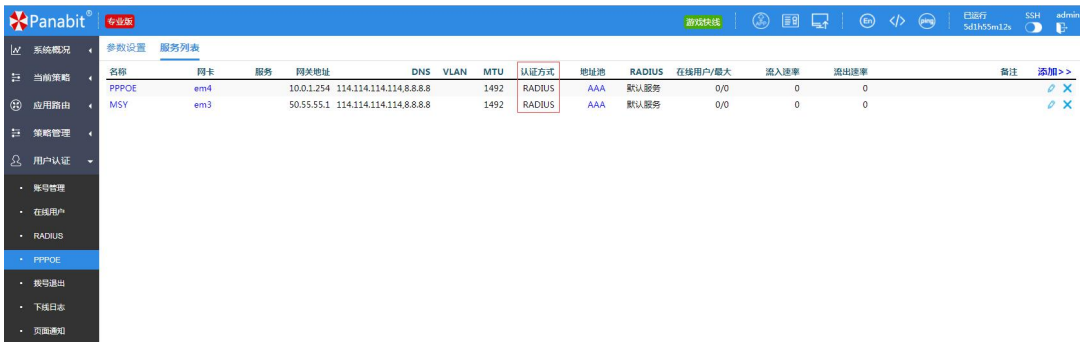
服务列表

从【用户认证】->【radius】，进入设置页面。默认有一个服务，无法删除，可以添加更多的 radius 服务，单台 Panabit 可以 对多台 radius 服务器对接；

服务器名：定义 radius 服务的名称；
服务器 IP：第三方 radius 服务器的 IP；
认证端口：发送认证数据报文的端口，默认 1812；
计费端口：发送计费数据报文的端口，默认 1813；
共享秘钥：用于验证 radius 报文合法性，与 radius 服务器相应的设置一致；
RAAS 域名：与派网 RAAS 产品对接时使用；
主路由线路：发送认证与计费报文的逻辑接口，逻辑接口必须与 radius 服务器 IP 能够互相通讯；
主线下一跳：当 radius 服务器在内网，使用 LAN 口与内网 radius 服务器对接，并且跨路由访问时
备份线路：当主路由线路断开时，使用备份线路与 radius 服务器进行通讯；

调用 radius

建立 PPPOE 服务器，认证方式选择 radius 认证



其它认证方式

先本地后 radius：当 PPPOE 服务器收到认证请求时，先在本地查找，本地没有再发送到 radius 上进行认证；

免认证：任何用户名密码都能认证成功，一般是在调测，或 radius 故障时应急使用；

3.2.13.6 PPPOE 代理认证

概述

在一些小区做带宽运营时，小区宽带运营商在出售自己的 PPPOE 账号（用户获取私网地址），同时也出售一级运营商的账号（可以获得到公网地址）。小区用户都在一个内网里，如何让一级运营商的账号的认证信息，从内网透传到上级运营商的 PPPOE 服务器，这个就是 PPPOE 代理认证要实现的功能。

目前 PPPOE 代理账号可支持 1536 个设置方法

1） PPPOE 服务器的认证方式为本地认证，或者先本地后 radius

2） 从【用户认证】->【账号管理】->【代理账号】添加代理账号

服务组：选择一个地址池；
账号名称：填入需要做代理的运营商账号；
网络出口：选择一个“接外网”的数据接口，这个接口应该与运营商提供的线路二层互通；
外出 VLAN：外出的 VLAN-tag；
开通日期：账号创建日期；
最后有效期：账号到期时间，到期后账号无法拨号成功；

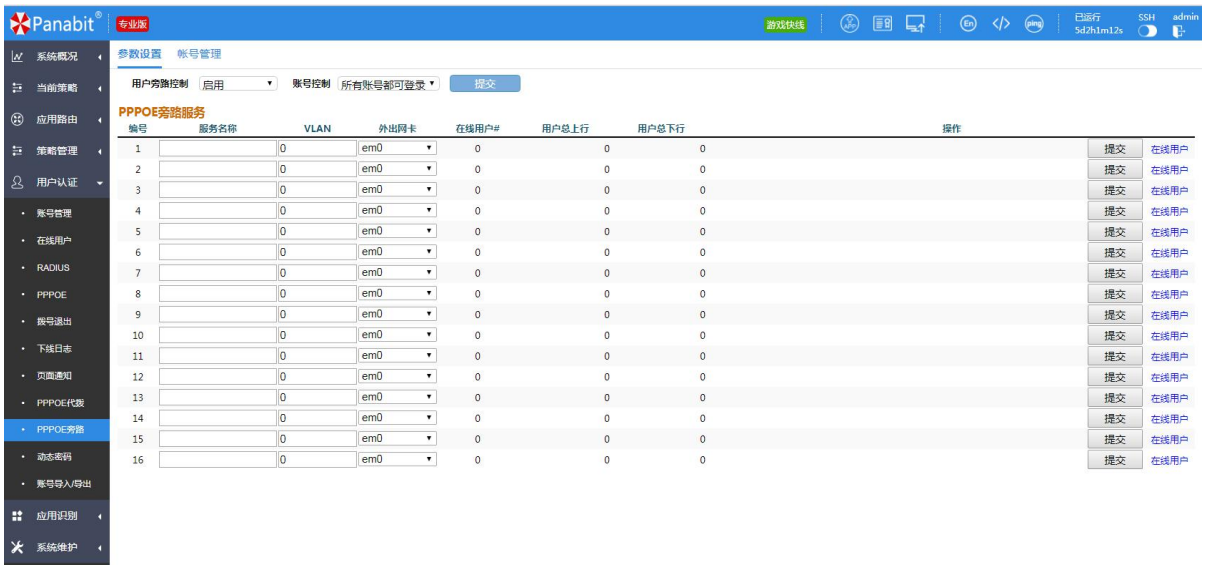
3.2.13.7 PPPOE 旁路认证

在一些小区做带宽运营时，小区宽带运营商在出售自己的 PPPOE 账号（用户获取私网地址），同时也出售一级运营商的账号（可以获得到公网地址）。小区用户都在一个内网里，如何让一级运营商的账号的认证信息，从内网透传到上级运营商的 PPPOE 服务器，这个就是 PPPOE 代理认证要实现的功能。

设置方法

1） PPPOE 服务器的认证方式为本地认证，或者先本地后 radius

2） 从【用户认证】->【PPPOE 旁路】->【参数设置】启用【用户旁路控制】



PPPOE 旁路服务：默认支持 16 个服务，每个服务可以匹配一个服务名称和 VLAN 号；
外出网卡：选择一个“接外网”的数据接口，这个接口应该与运营商提供的线路二层互通；

3） 当【用户认证】->【PPPOE 旁路】->【参数设置】->【账号控制】选择“只允许列表内账号登录”时，从【用户认证】->【PPPOE 旁路】->【账号管理】里新增账号。

账号名称：填入需要旁路的运营商账号；服务组：选择一个服务组；
截止日期：账号到期时间，到期后账号无法拨号成功；

4） 客户端续填入服务名称，比如服务组的服务名称是“panabit”，那么客户端也要填入“panabit”。

3.2.13.8 PPPOE 代理与 PPPOE 旁路的区别

1） 实现方式旁路认证是通过服务名称来实现，代理认证是通过账号区分。
2） 单台支持用户数旁路认证用户限制为 512，代理认证用户限制为 1536 个
3） 实现原理
旁路认证在 PPPOE 的 Discover 阶段就完成了透传，代理账号要在 Authentication 阶段才能实现代理

3.2.14 Web 认证配置

3.2.14.1 概述

提供 web 页面认证服务模块，多用于企业上网管理，校园无线覆盖运营，商业无线覆盖运营等应用场景。

3.2.14.2 技术原理

当开启 Web 认证后，所有会话都会被阻断（免认证和一些关键会话除外），panabit 在阻断会话的同时，给客户端发送 HTTP 重定向请求，重定向客户端访问认证页面，客户端在认证页面输入账号密码，通过认证后放行所有会话。

3.2.14.3 Web 认证模块的安装与升级

从【应用商店】->【应用安装升级】对 web 认证模块进行安装与升级

Web 认证模块更新下载地址：
HTTP://forum.panabit.com/thread-12161-1-1.html

3.2.14.4 基本配置

从【应用商店】->【Web 认证】->【基本配置】进入配置界面

Web 认证：功能模块的开关，默认为关闭。开启后未认证的用户会话不允许通过 Panabit；
免认证 IP：可以选择一个 IP 群组，会话的源地址或目的地址匹配属于这个群组内，那么这个会话运行通过 Panabit；
免认证协议：默认为空，可选择特征库协议或自定义协议，选择协议后，会话如果属于这个协议，那么允许此会话通过 Panabit；
成功后显示页面：认证成功后显示指定页面，如为空则显示原始页面
登录后弹出注销页面：选择“是”浏览器右下角会有一个弹框，用户认证后可以通过关闭弹框主动下线；选择“否”用户 IP 无流量后自动下线；
认证页面配置与认证页面管理：可以对本地的认证页面做自定义处理，比如背景，认证框显示位置等等；

3.2.14.5 认证种类

本地账号：用户信息放在本地，在【用户认证】—【用户账号】里添加账号；
Radius 认证：与第三方 radius 服务器对接认证；
AD/LDAP：与 AD 域服务器对接认证：
第三方认证：通过修改 PortalURL 的选项激活，认证的 portal 页面地址，默认为本地认证界面，即本地认证；使用第三方 portal 页面地址后自动切换到第三方认证；
portalIP：授权安全管理 IP，比如第三方认证服务器对用户发送下线指令，如果不是所填 IP 发送的数据报文，Panabit 不响应指令；
手机短信认证：通过与手机短信平台对接，通过手机号码与短信验证码认证上网；
微信认证：与微信公众号对接进行认证，主要目的是让用户关注公众号；
MAC 记忆：当某用户认证成功后，记录该用户的 MAC，只要用户在 Panabit 没有下线，即使该用户更换了 IP 地址，也无需重新认证。

3.2.14.6 Web 认证使用注意事项

1） 首先满足在不开认证的情况下，客户端都能上网；
2）Web 认证服务模块都和管理口有关，因此客户端和管理口 IP 必须能通讯；
3）与第三方对接的时候 Panabi 提供 API 接口，第三方必须和 API 接口对接；

3.2.15 PPPOE 代拨网关

3.2.15.1 研发背景及应用场景

高校是 IT 应用比较重的客户，基本上各种先进的 IT 技术，高校用的都是比较早的。学校的学生也碰到小区客户一样的情况，就是希望可以直接使用运营商的帐号接入，但是如果使用上面代理的方式，那么学校对学生就无法审计，而且这涉及网络改造问题。

基本上学生都会用到手机，运营商给学生会有套餐流量和帐号，手机要认证，不可能是 PPPoE 一般都是通过 WEB 方式认证，所以手机那侧看到的是 IP，而不是 PPPOE，这是一种全新的 PPPOE 代理，我们将这种方式称之为“PPPOE 代拨”。和 PPPOE 代理相比，PPPOE 代拨最大的不同是，用户侧拿到的 IP 地址不是运营商分配的，而是 Panabit 或校园网内部分配的，所以这里面在技术实现上就要复杂一些。

3.2.15.2 正确理解 PPPOE 代拨

Panabit 是如何看待 PPPOE 代拨的呢？理解了这个，对 Panabit 的各种设置的来由就心里有数了。Panabit 是这么看待 PPPOE 代拨的：

- 创建线路：每次全新的 PPPOE 代拨，实际上是产生一条特定的“WAN 线路”；
- IP 和线路捆绑：PPPOE 代拨就是让内网指定的 IP 走这条特定的 WAN 线路出去，可以看着是将内网 IP 和 WAN 线路绑定的过程，简单说就是让 IP 走代拨的专线出去；

所有一切都是围绕上面两个原则设计的。仅仅让内网 IP 走代拨线路 NAT 出去还不够，还要处理 DNS 请求。因为用户的 IP 是网内分配的，用户肯定有自己的 DNS 服务器，假如这个 DNS 是联通的，但是代拨线路是电信的，使用联通 DNS 解析出来的肯定是联通的 IP 了，从电信线路访问联通 IP，那肯定是要出问题的。所以 Panabit 要有类似于 DNS 重定向的功能。

3.2.15.3 基本配置

默认网卡：是指代拨的外联接口，VLAN 和 MTU 就不多说了。这里重点说一下 TTL 参数，这个参数的单位是秒，这个参数是用来控制空闲的代拨线路滞留时间的。一条代拨线路可以绑定多个内网 IP 地址，如果这条代拨线路下面没有绑定任何 IP 地址，那么就认为这条代拨线路是空闲的，当空闲时间超过 TTL（图上是 60 秒）后，系统会自动将这条代拨线路删除掉。

路由策略

前面说过代拨的结果是 Panabit 创建了一条“特殊”的 PPPOE 拨号 WAN 线路，然后让内网某个（或某些）IP 的流量专门走这条线路出去，简单理解就是代拨为内网某个或某些 IP 开辟“专线”。线路有了，要想流量走线路走，当然就要策略路由了。

在第一个支持 Panabit 的版本里，这个路由过程是默认进行的，而且这个路由发生在所有的策略路由之前，只要启用了 PPPOE 代拨服务，这个路由就会自动完成，但是这个处理方式在实际中会有问题。用户的环境一般都比较复杂，有很多 IP 的访问是不能走代拨”专线“的，比如访问一些 DMZ 区的服务器，就应该走内网，而不是代拨线路。

因此，在第二个版本里（其实也不算了，因为第一个版本在实际中还没有案例）就取消了这种默认机制,取而代之的是通过做路由策略来实现代拨路由。为了较好的支持代拨路由，Panabit 对策略路由做了一些扩展，主要就是 1+1：

- 增加了一个”用户类型“条件，用户类型有”代拨用户“,”非代拨用户“和”任意用户”三种取值；
- 增加了一个“走代拨线”的执行动作，这个动作将流量 NAT 到内网 IP 绑定的对应的代拨线路；

看看 65501 这条策略，这条策略让所有的代拨 IP 走对应代拨线路出去，注意“走代拨线”的动作后面没有线路选择，因为这个线路已经隐藏在内网 IP 中了，是和内网 IP 对应的。

DNS 重定向策略

为了确保用户的正常通信，在做了策略路由后，还要确保用户的 DNS 解析是走正确的 DNS 服务器解析。代拨线路拨号到上级运营商成功后，代拨线路里会有上级运营商提供的 DNS 服务器 IP，使用 DNS 管控策略可以将内网代拨 IP 的 DNS 请求走这个 DNS 解析，下面是一个 DEMO 截图（不要关注序号，就看最后一条，这只是举例子而已）：

3.2.16 游戏快线

3.2.16.1 概述

将游戏流量引入 SD-WAN 的定向优化。

3.2.16.2 基本配置

在主页面点击【游戏快线】进入配置界面

快线功能：启用/关闭，控制游戏快线功能模块的开启和关闭

出口线路：连接 SD-WAN 的出口

内网可服务 IP：可以指定内网 IP 使用游戏快线服务

内网可服务账号：可以指定内网用户组使用游戏快线服务

可加速游戏：可以加速的游戏列表，勾选后，该游戏流量进入加速通道。

3.3 旁路接入

3.3.1 概述

数据通过镜像或者分光的方式将流量牵引到 Panabit 的数据接口，panabit 在旁路分析数据报文，并将分析结果发送到 panalog 日志服务器上，panalog 可以对数据做进一步汇总分析。

3.3.2 基本配置

数据分析设置

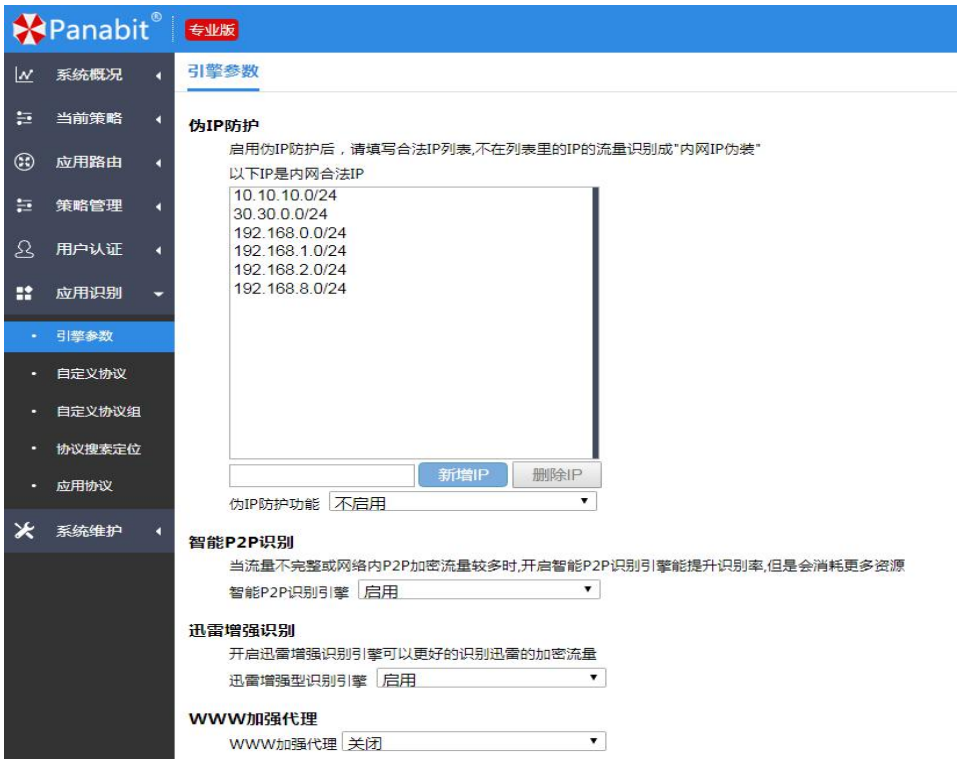
设置数据接口从【监控统计】-【网络接口】进入设置界面，可看到所有的数据接口，并且对它们进行设置。

将接收上行流量的数据接口，工作模式设置为“监控模式”，接入位置设置为“接内网”；将接收下行流量的数据接口，工作模式设置为“监控模式”，接入位置设置为“接外网”；

设置伪 IP 防护

在实际应用中，很多情况都是是将上下行流量都通过同一个网口镜像过来。这个时候，对于 Panabit 来说只有一个方向的流量，因此无法区分上下行。在这样的情况下要区分上下行，可以通过 打开“伪 IP 防护”功能实现。

从【应用识别】->【引擎参数】进入配置界面



将内网 IP 地址段填进去，并且启用【伪 IP 防护功能】。这个功能打开后，实际上就告诉了 Panabit，哪些 IP 是内网的，源地址为内网 IP 的流量就是上行流量；源地址为外网 IP 的就是下行流量。

3.3.3 Panalog 对接配置

接收如何设置与 panalog 日志服务器对接。Panabit 采集并分析数据后，通过管理接口，可以将数据发送给 panalog，panalog 可以对数据进行进一步的统计和分析。

安装日志一键设置 APP
日志一键设置 APP 下载地址：
HTTP://bbs.panabit.com/thread-12279-1-1.html 从【应用商店】->【应用安装升级】安装【日志一键设置】APP

安装【日志一键设置】APP 后
从【应用商店】->【日志一键设置】进入设置界面，

设备编号：设置范围 0-255，这个编号用于让 panalog 区分数据是从哪个 panabit 设备接收的；
日志服务器 IP：panalog 服务器 IP，此 IP 必须与管理接口能互通，否则 panalog 接收不到数据；日志服务器端口：设置范围 0-65535，0 表示不发送日志，自定义发送日志信息的端口，在 panalog 服务器上也要给接收器设置相对应的端口；是否记录：默认不记录，表示不发送日志；
日志类型：选择需要发送到 panalog 的日志数据类型；

3.3.4 缓存牵引配置

Panabit 部署在旁路还有一个作用就是与 iXCache 配合进行缓存牵引，Panabit 作为缓存调度的管理机，实现缓存集群部署。

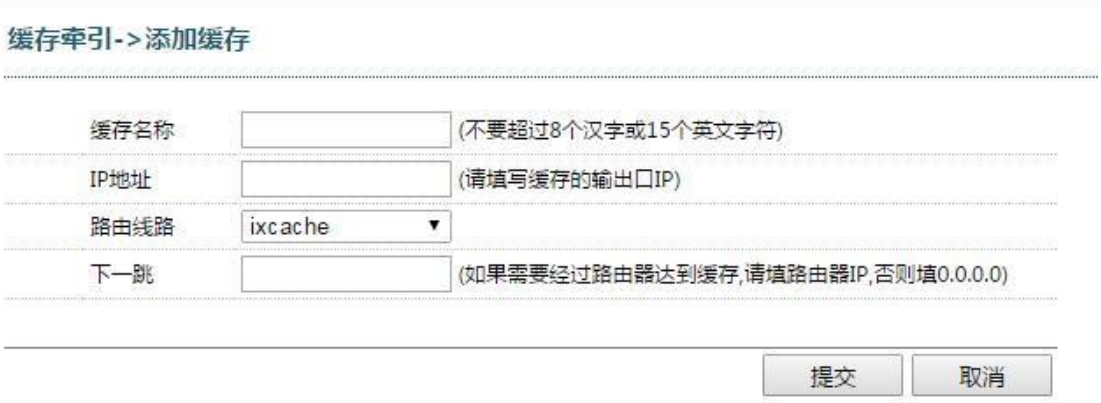
接口设置从【监控统计】-【网络接口】进入设置界面，可看到所有的数据接口，并且对它们进行设置。

将接收镜像上行流量的数据接口，工作模式设置为“监控模式”，接入位置设置为“接内网”；在做 iXCache 缓存牵引时，panabit 只需要接收上行数据；

将用与 iXCache 缓存牵引的数据接口，工作模式设置为“监控模式”，接入位置设置为“接内网”；在这个数据接口上建立一个 LAN 接口，通过 LAN 接口将数据牵引到 iXCache 缓存服务器；

iXCache 牵引设置

从【应用商店】->【iXCache 牵引】->【缓存设备】->【添加设备】添加要进行牵引的 iXCache 服务器。



缓存名称：自定义名称；

IP 地址：目标缓存服务器的 IP 地址；路由线路：选择 Panabit 中添加好的 LAN 或者 WAN 线路；

下一跳：当路由线路是 Panabit 中的一个 LAN 接口，并且与目标缓存服务器的 IP 跨三层时用到，需填入 LAN 对端的路由的 IP 地址；

有多台 iXCache 集群时，添加多个 iXCache 服务器

从【应用商店】->【iXCache 牵引】->【缓存组】->设置缓存组

总共有 16 个缓存组，每个缓存组有 16 个槽位点击缓存组名称，为缓存组添加成员。
名称：自定义缓存组名称；
槽位：每个槽位选择一个缓存服务器，Panabit 将需要缓存的数据均衡的分发到各个槽位上的 iXCache 服务器。注意：所有槽位必须填满！

从【应用商店】->【iXCache 牵引】->【牵引策略】->添加牵引策略

策略主要由三个要素组成:“策略标识”、“匹配条件”、“策略动作” 策略编号：在策略组中唯一标识该策略的编号，该编号区间范围（1~65535），策略编号决定了该策略在该策略组中执行的先后顺序，1 的优先级最高，65535 最低。

匹配条件：包含源接口、源地址、目标地址、VLAN、文件类型、等等，当所有的条件都满足时，才会执行策略中指定的动作；
源接口：设置为“接内网”的数据接口；
源地址：数据报文的源 IP；
目标地址：数据报文的目标 IP；
VLAN：数据报文中所含的 VLAN-tag；
文件类型：数据报文中所含的文件类型，比如 flv，mp4 等等缓存模式：数据牵引，当缓存命中时，由 Panabit 发送 302 重定向报文；数据镜像，当缓存命中时，由 iXCache 发送 302

重定向报文；

缓存服务：将满足条件的数据报文牵引到 iXCache 上，可以选择一台已添加的缓存服务器，或者一个缓存集群；

总结

1） 使用旁路部署模式，不会对现网产生任何影响，Panabit 只是单纯的分析镜像或分光的流量；

2） 不单单旁路部署，其它任何部署方式都可以将日志发送到 Panalog 服务器；

3） 不单单旁路部署，其它任何部署方式都可以使用 iXCache 牵引功能，实现缓存集群部署调度；

第四章 应用商店

4.1 应用商店概述

Panabit 核心引擎十分强大，在 Panabit 核心引擎的基础上可以扩展很多功能，但是某些功能只在特定的应用场景才有存在的意义，为了管理界面简洁清晰，一些特定场景才有用到的功能以 APP 的形式存在于 Panabit 上。

应用商店模块位于管理界面的右上角

Panabit 应用商店模块提供 APP 功能扩展平台，当用户需要这些特定功能时，通过下载安装应用商店的 APP，来获取相关功能设置界面。APP 不使用时也可卸载。

Panabit 应用商店 APP 下载地址：HTTP://forum.panabit.com/forum-31-1.html

4.2 DDNS 服务

Panabit 所有的配置都是通过管理接口配置的，当 Panabit 作为网关部署时，通常管理接口 IP 是私网地址时，如果想要远程管理 Panabit，需要将管理接口 IP 的 443 端口映射到公网 IP。在 Panabit 的 WAN 线路都是动态 IP 的情况下，就要将动态 IP 地址映射到一个固定的域名解析服务上，用户直接通过域名远程管理 Panabit。DDNS 服务的 APP 就提供了这样的功能。

Panabit 应用商店 APP---DDNS 服务下载地址：
HTTP://forum.panabit.com/thread-12174-1-1.html

DDNS 配置从【应用商店】->【DDNS 服务】添加 DDNS 服务

域名：远程访问的域名，与域名提供商要对应绑定线路（主）：默认自动，可以自己选择一条 WAN 线路绑定线路（备）：默认自动，可以自己选择一条 WAN 线，当主线路不通时，会切换到备线路域名提供商：选择一个域名提供商，与所填域名要对应用户名：在域名提供商平台注册的用户名密码：在域名提供商平台注册的用户名密码使用状态：启用/禁用备注：自定义备注信息

添加好 DDNS 服务后，可以点击日志查看，有日志记录表明 DDNS 服务更新成功。

4.3 共享检测

4.3.1概述

在网络普及的过程中，出现这样一个现象：在实际的带宽接入中存在着大量的非法级联，如一个用户通过路由器级联或建立无线热点使得多个用户可以利用同一包月帐号上网。在企业办公，校园网、小区宽带中上述情况非常普遍，并且在迅速蔓延。最终将导致接入商投入的巨额基础建设费用难以正常回收。

在防止用户私接路由器的应用场景上，使用 Panabit“共享检测”功能可以解决这一难题。

配置从【应用商店】->【共享检测】进入配置页面

共享检测：功能开关，默认为不启用，启用后开始检测内网用户的共享；对象生存期：检测到一个浏览器后，如果这个浏览器在所设时间内不被再次检测到，那么就会报老化掉；
IE 对象权重：对检测到的 IE 内核的浏览器做加权算法的系数；
chrome 对象权重：对检测到的 chrome 内核的浏览器做加权算法的系数；注册检测间隔：主动检测客户端浏览器的时间间隔；

在流量控制策略里，共享用户可以作为一个策略条件

图中策略的效果是，当检测到内网用户 IP 下共享用户大于等于 3 的时候，阻断这个内网 IP 的所有流量。

4.3.2 加权算法

共享是通过检测用户端的浏览器个数，来判断共享。实际应用中，1 个浏览器不能代表 1 个共享用户，因为不排除一个用户使用多个浏览器的情况。因此在计算共享用户个数时，我们通过加权算法来计算共享用户的个数，避免误报。
比如在一个内网 IP 下检测到两个浏览器，一个是 IE 一个是 chrome，IE 对象的权值是 75，chrome 对象的权值也是 75，那么通过加权算法，（75+75）/100=1.5 ，1.5 取整数位，最后得出加权值为 1,那么 Panabit 认为这个内网 IP 下的共享用户数为 1。

4.4 云服务

4.4.1概述

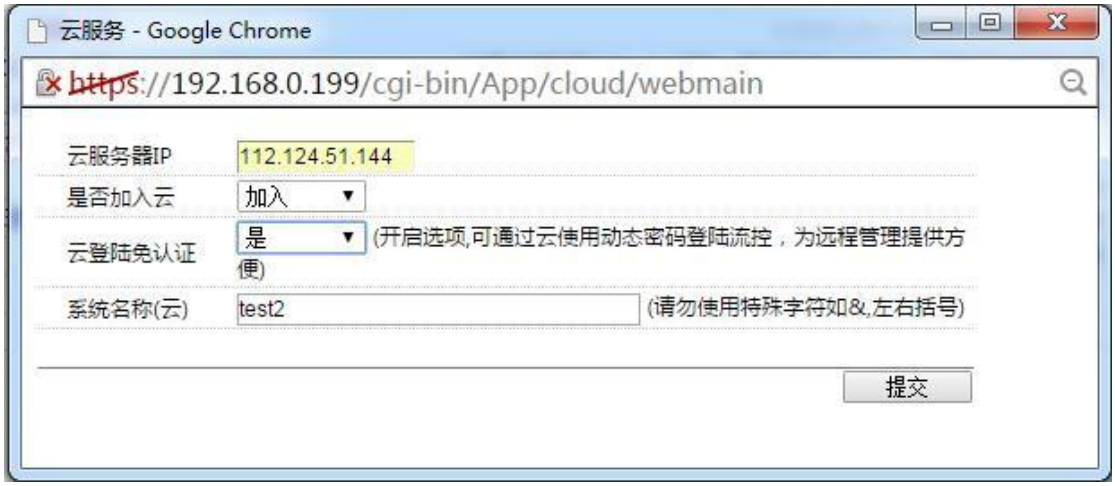
为方便管理员管理自己的 Panabit 设备，管理员可以通过云平台，对加入了云服务的设备进行远程监控、升级版本、安装应用商店 APP、备份设备配置等操作。

4.4.2配置

1） 搭建云平台，即安装 panalog 服务器，panalog 服务器内置云平台。云平台最好在公网上，如果自己没有公网地址，建议使用阿里云。

具体可参照：HTTP://forum.panabit.com/thread-11865-1-1.html

2） 从【应用商店】->【云服务】进入设置页面；



云服务器 IP：填入云平台的 IP；是否加入云：选择加入后，云平台才能看到设备信息；云登录免认证：选择“是”从云平台登录设备时无需输入密码；选择“否”从云平台登录设备时要输入密码；系统名称（云）：加入云平台后，在云平台上显示的设备名称；

云平台是利用反向代理技术实现的远程管理，即使 Panabit 的管理接口 IP 是私网地址，只要能与云平台通讯，无需做端口映射也可以远程登录 Panabit 管理界面。

加入云成功后，云平台会显示设备信息，点击设备名称，即可登录这台设备的管理页面。

第五章 设备维护

5.1 维护概述

介绍维护基本原则，包括：维护过程、故障处理原则。

介绍如何获得派网软件技术有限公司的技术支持。

5.2 维护基本原则

在维护过程中，应该遵循以下基本原则：

- 严禁在维护终端上安装与维护设备无关的软件。
- 根据远程维护指导，对设备进行例行维护，并填写相应的远程维护记录表。
- 对于在例行维护过程中遇到突发性维护任务（如设备故障），应根据故障处理流程及时处理，并做好相关记录。对于处理不了的问题，应及时与北京派网软件有限公司驻当地代表处联系解决。
- 在修改数据前必须做好数据的备份，并做好相关记录。
- 保持机房整洁，防止鼠、虫等小动物进入设备。
- 按照设备接地的要求，将设备正确接地。
- 不要随意插拔、复位网卡模块。
- 按照要求使用防静电腕带或者防静电手套，避免设备受到静电放电的损害。
- 对单板的端口进行防静电控制。在进行相关操作时佩戴防静电腕带或者防静电手套，外接线缆、端口保护套接入设备端口事先进行放电处理。
- 现场维护完成后，确保机柜门关闭正常，以免引起意外事故。
- 对于在例行维护过程中遇到突发性维护任务（如设备故障），应根据故障处理流程及时处理，并做好相关记录。对于处理不了的问题，应及时与北京派网软件有限公司驻当地代表处联系解决。

在进行故障处理时，应该遵循以下基本原则：

- 维护人员要有收集相关信息的意识，在遇有故障时，一定要先弄清楚相关情况后再决定下一步的工作，切忌盲目处理。
- 在故障处理过程中，要对每一步操作内容及操作所产生的现象做详细记录。对处理过程尽可能详细的记录是申请北京派网软件有限公司进一步技术支援的基础，可缩短进一步处理问题的时间。
- 如果故障一时难以排除，请及时联系北京派网软件有限公司客户服务中心。同时，您在向派网工程师反馈问题的时候，请提供或收集以下信息：
  - 故障局点的详细名称（全称）
  - 联系人姓名、电话号码
  - 故障发生的具体时间
  - 故障现象的详细描述
  - Panabit 的软件版本
  - 故障后已采取的措施和结果
  - 问题的级别及希望解决的时间

5.3 如何获取技术支持

如果您在设备维护或故障处理过程中，遇到难以确定或难以解决的问题，通过本文档的指导仍然不能解决，请您直接联系北京派网软件有限公司客户服务中心，我们将为您提供技术支持服务。

您也可以通过电话或电子邮件联系北京派网软件有限公司驻当地办事处的技术支持人员。

客户服务电话：4008981066
客户服务邮箱：support@panabit.com
另外，您也可以从北京派网软件有限公司的技术支持网页上直接获取最新的技术资料，网址是：HTTP://forum.panabit.com/

5.4 接口维护

介绍如何在控制台更改接口，比如增加数据接口，更换管理口接口，查看管理接口 IP 等等

5.4.1 管理接口维护

ifconfig

```
panaos#ifconfig
em5: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=4219b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4,WOL
_MAGIC,VLAN_HWTSO>
        ether 00:16:31:f5:32:63
        inet 192.168.0.199 netmask 0xffffff00 broadcast 192.168.0.255
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
panaos#
```

Inte：接口 IP 地址
Status：接口状态，active 说明网络物理状态已接通，no carrier 表明网络物理状态未接通

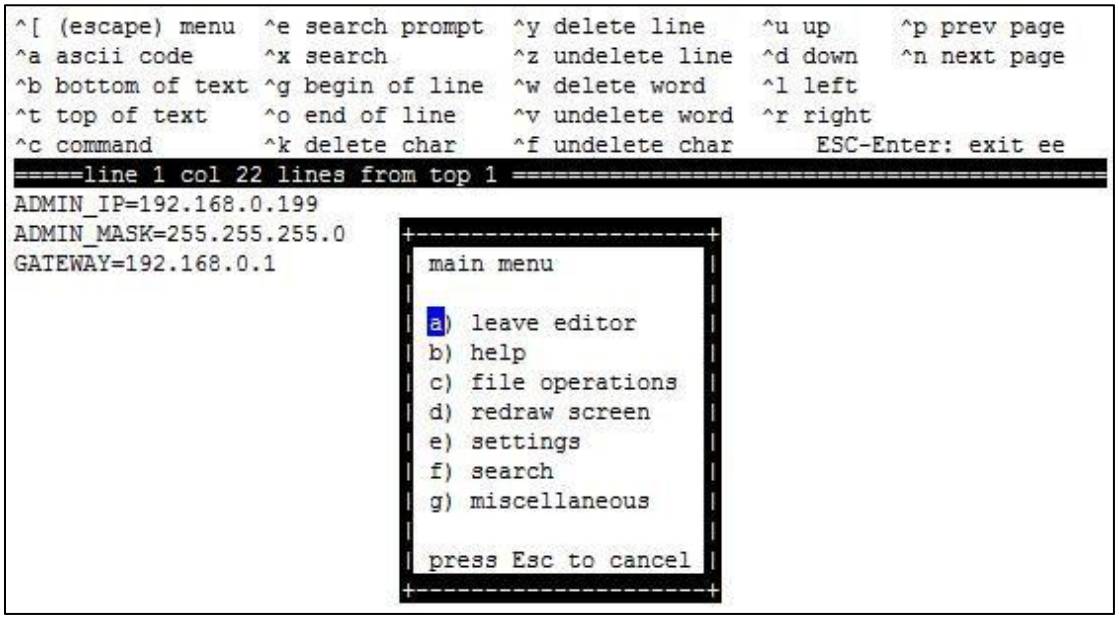
临时修改管理口 IP
ifconfig 管理口网卡名 192.168.0.199/24

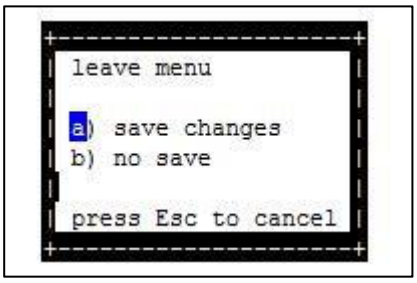
```
panaos#ifconfig em5 192.168.0.199/24
```

修改管理口 IP
ee /conf/ifadmin.conf

```
panaos#ee /conf/ifadmin.conf
^[ (escape) menu  ^e search prompt  ^y delete line    ^u up     ^p prev page
^a ascii code     ^x search         ^z undelete line  ^d down   ^n next page
^b bottom of text ^g begin of line  ^w delete word    ^l left
^t top of text    ^o end of line    ^v undelete word  ^r right
^c command        ^k delete char    ^f undelete char      ESC-Enter: exit ee
=====line 1 col 22 lines from top 1 ============================================
ADMIN_IP=192.168.0.199          移动光标，修改IP
ADMIN_MASK=255.255.255.0        子网掩码
GATEWAY=192.168.0.1             网关
```

修改好之后按 esc 键，选择 a）leaveeditor 按回车，离开编辑，再选择 a）savechanges 保存修改，然后重启设备。

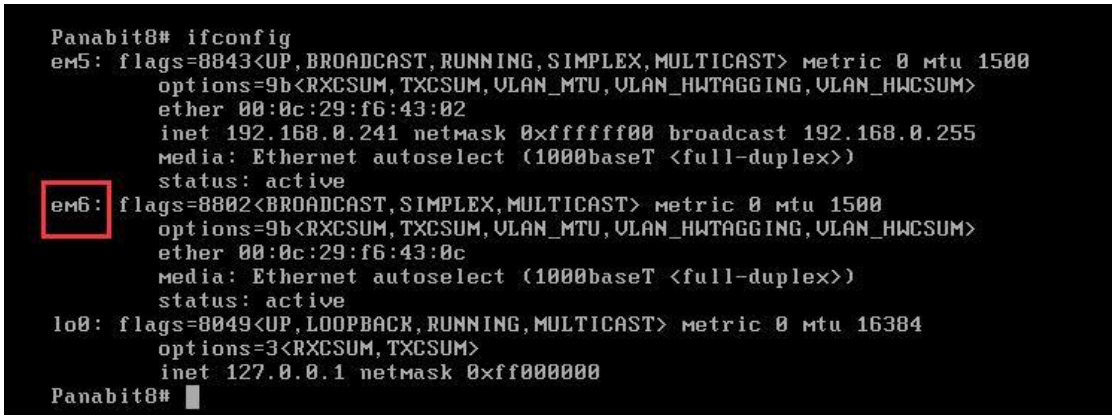




5.4.2数据接口维护

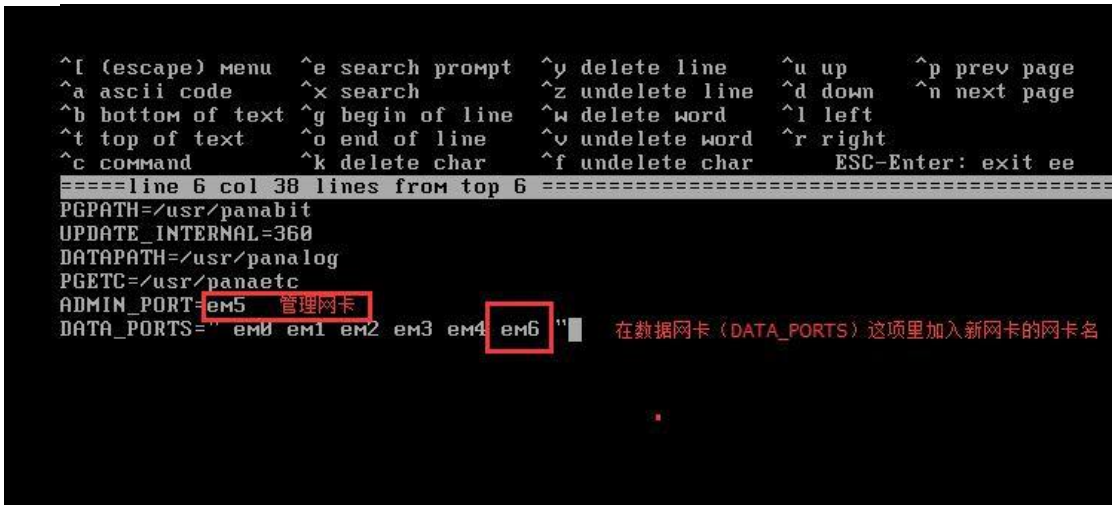
接口配置文件：PG.conf 以添加数据接口为例：

ifconfig 找到新加网卡的网卡名



然后编辑 PG.conf 文件 ee /etc/PG.conf，

将新网卡加入数据网卡



然后 esc 键退出，保存，重启设备生效。
注意，更改了数据网卡后，原有的 license 会失效，必须重新授权。

PG.conf 配置文件可添加的参数有：
1） HTTPS_PORT=4443
将管理页面端口更改为 4443
2） ETHERMTU=15XX
更改数据接口 MTU，默认 MTU 为 1520
3） PPPOE_PORT=emx
将 wan 口 PPPOE 拨号数据报文镜像到其它数据接口

5.5 安全维护

概述

介绍如何修改控制台密码，恢复控制台密码，查看更改管理页面的密码，用户权限等等

修改控制台密码命令：
passwd
控制台默认用户名：root，密码：panaos

控制台密码恢复当忘记控制台密码时，可以通过下列方法进行恢复。
1） 重起设备，并不停的接 Tab 键进入启动选择模式
2） 在 boot:里打上/boot/loader -s，进入单用户模式
3） 单用户模式启动完成后会看到/bin/sh:的提示，回车一下，进到#命令行
4） 输入：/sbin/fsck -y 扫描并修复磁盘
5） 扫描完成后，输入：/sbin/mount -a 挂载磁盘

6） 挂载成后（无提示），输入修改密码命令：passwd

7） 新的密码 设置成功后输入/sbin/reboot 重启后就能用新的密码登入 root 用户了。

查看 WEB 界面密码

cat /usr/ramdisk/admin/.htpasswd

修改管理界面密码

ee /usr/system/admin/.htpasswd

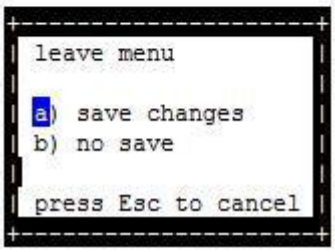
```
panaos:ee /usr/system/admin/.htpasswd
^[ (escape) menu  ^e search prompt  ^y delete line    ^u up     ^p prev page
^a ascii code     ^x search         ^z undelete line  ^d down   ^n next page
^b bottom of text ^g begin of line  ^w delete word    ^l left
^t top of text    ^o end of line    ^v undelete word  ^r right
^c command        ^k delete char    ^f undelete char      ESC-Enter: exit ee
=====line 1 col 0 lines from top 1 ============================================
admin:panabit
guest:guest
pppoeman:panabit
```

管理用户admin，管理用户只有1个

guest只能查看

pppoeman只能修改pppoe服务界面里的内容

修改好之后按 esc 键，选择 a）leaveeditor 按回车，离开编辑，再选择 a）savechanges 保存修改。



admin，guest，pppoeman 这三个用户系统自带，可添用户，所有添加的用户都是 guest 权限，添加格式为，用户名:密码用户名和密码可以使用英文，数字，或者英文+数字，不可使用特殊符号！

访问 WEB 管理界面白单

ee /etc/pawebhosts

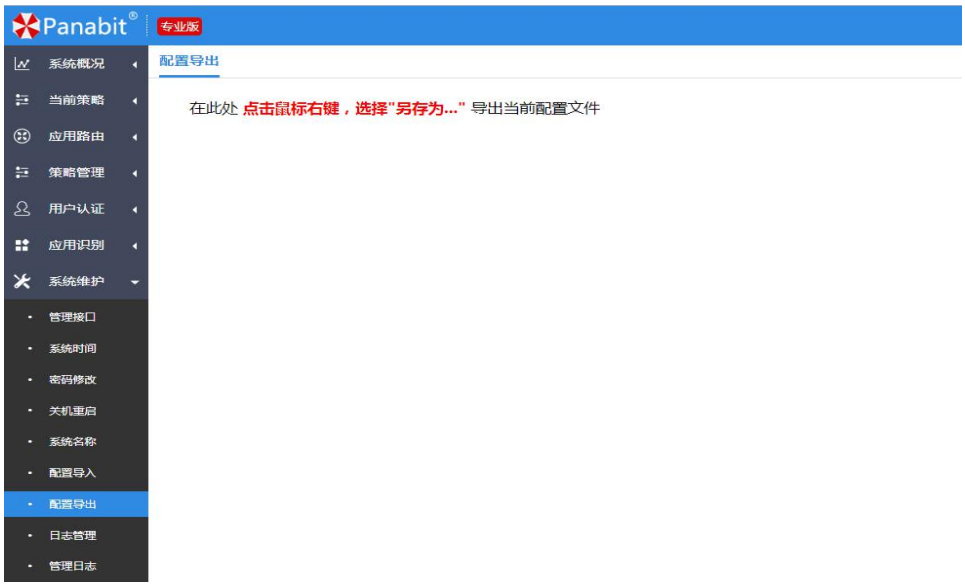
将允许访问 WEB 管理界面的 IP 加入列表，格式为每一行一个 IP

```
rm /etc/pawebhosts
```

删掉白名单文件，允许所有 IP 登录

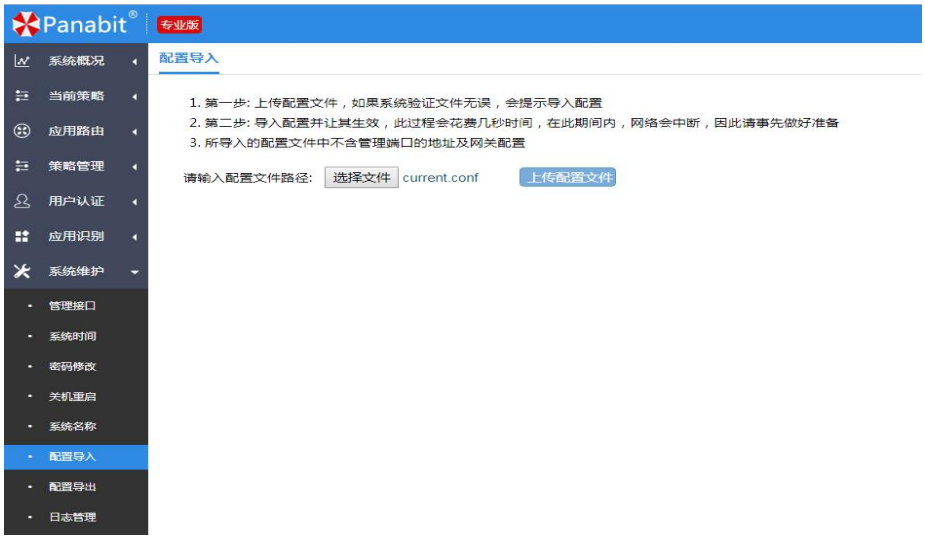
5.6 配置备份

策略配置文件的导出与导入从【系统维护】->【配置管理】->【配置导出】这个页面导出当前策略配置



除管理接口 IP 设置和认证用户信息以外，该配置文件包含管理界面所有设置的配置。导出的文件默认名称是 current.conf。

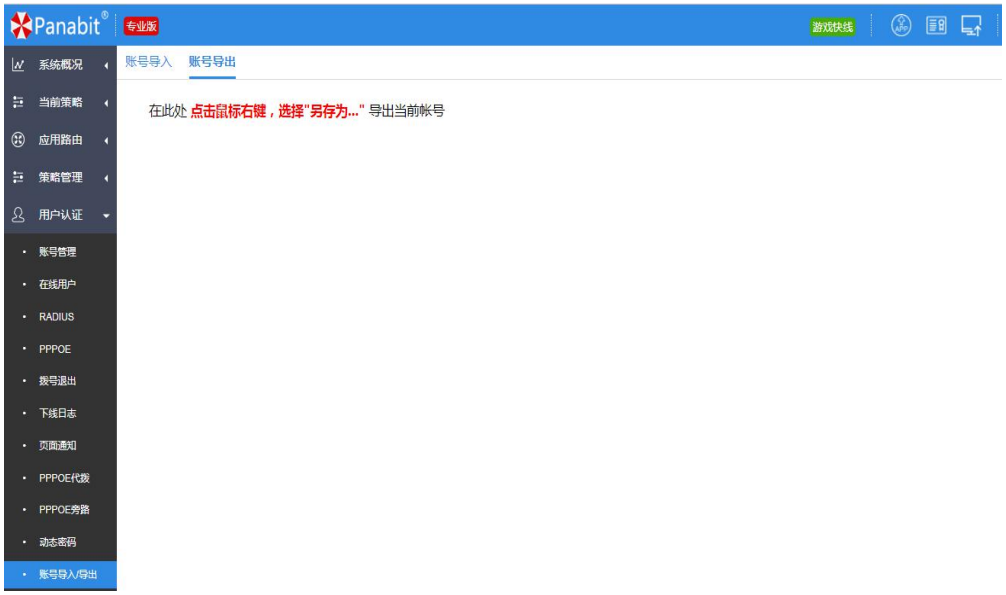
从【系统维护】->【配置管理】->【配置导入】这个页面导入备份配置选择备份的配置文件，点击上传



上传成功后，点击导入上传的配置文件。

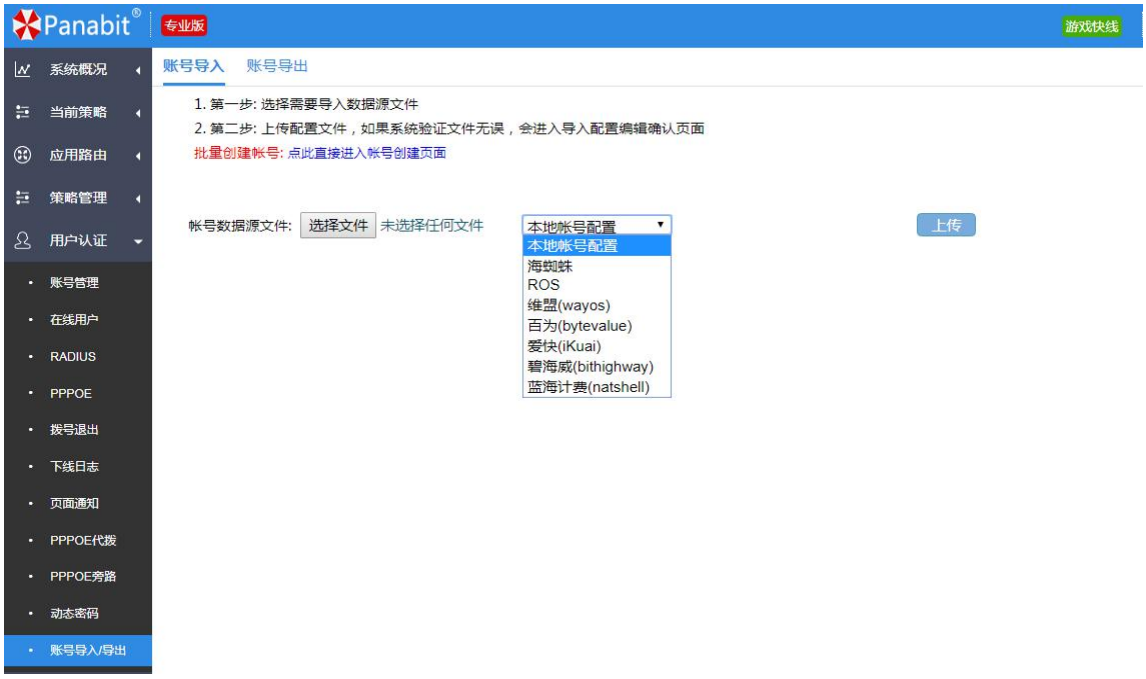
控制台配置文件存放目录：/conf/panabit.conf

PPPOE 用户账号导出与导入
从【用户认证】;>【基本对象】->【账号导出】导出本地账号



导出文件默认文件名是：pppoedb.txt

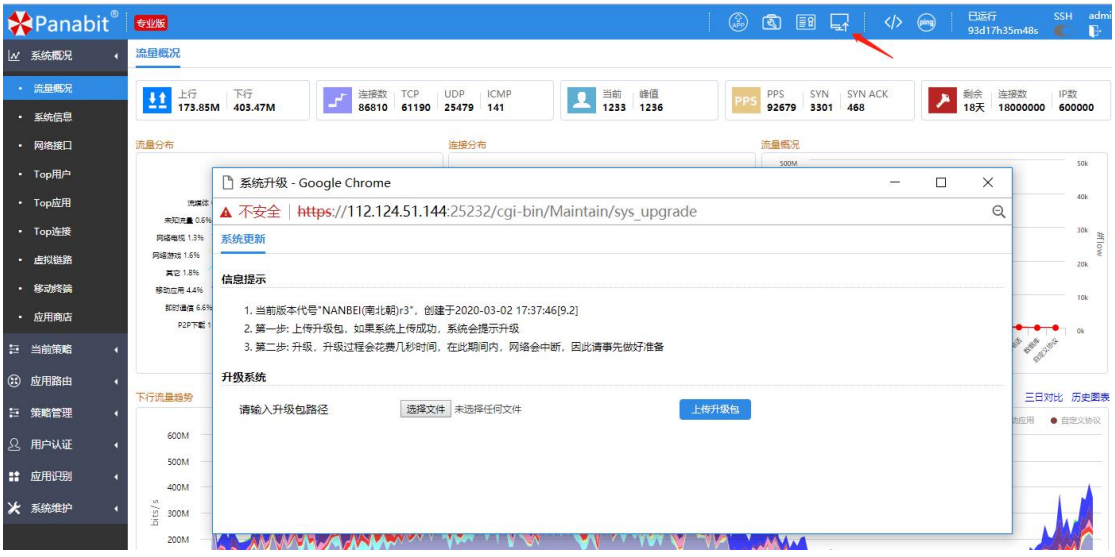
从【用户认证】;>【基本对象】->【账号导入】导入账号
可导入其它路由系统的账号，目前支持的有：海蜘蛛、ROS、维盟（wayos）、白为（bytevalue）、爱快（ikuai）、碧海威（bithinghway）、蓝海计费（natshell）、凌风计费、等等



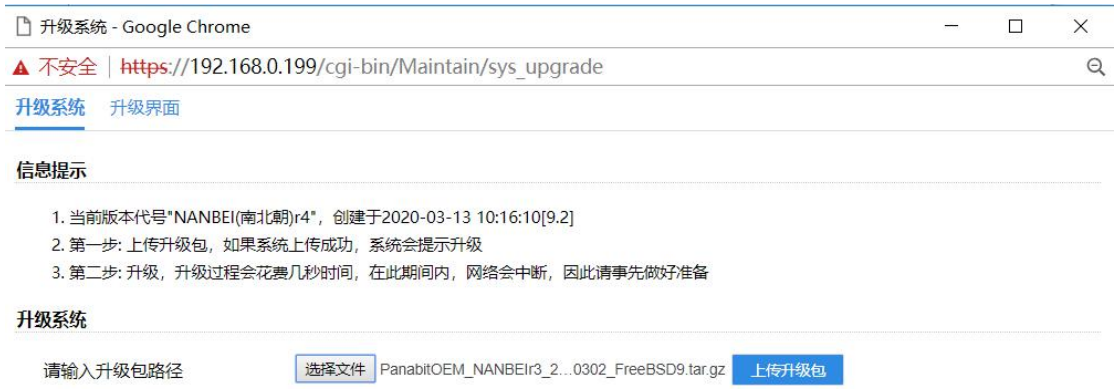
本地账号文件及存放目录：/conf/pppoedb.conf

5.7 固件升级

点击导航栏右上角图标，弹出升级页面



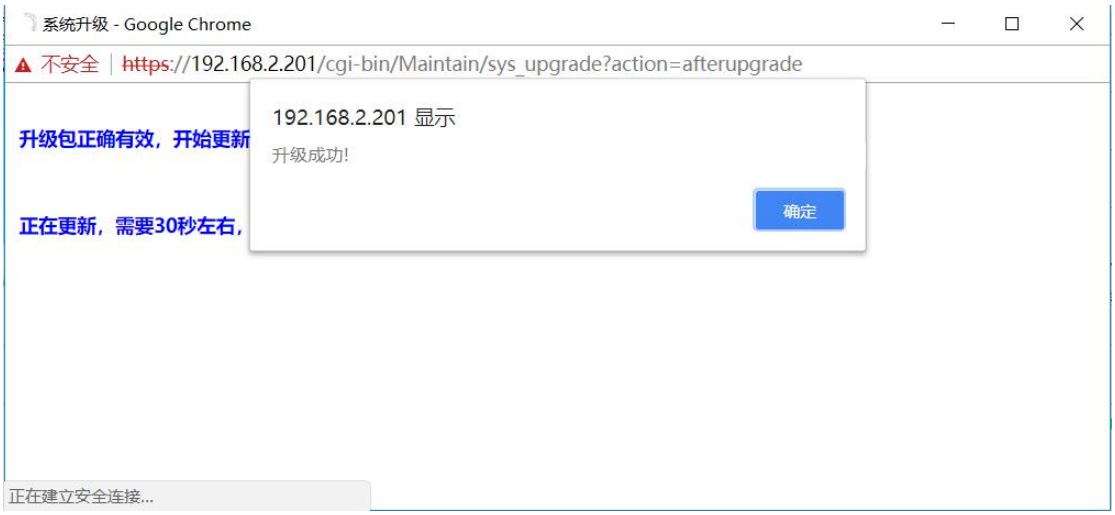
上传系统升级包，系统升级包文件类型是.gz。



上传成功后，提示是否进行升级。点击“进行升级”，开始升级系统。

升级过程中 OS 会重启，如果是网桥或者网关接入，网络会中断几秒。

升级完成后会提示“升级成功”


系统升级 - Google Chrome
不安全 | https://192.168.2.201/cgi-bin/Maintain/sys_upgrade?action=afterupgrade
升级包正确有效，开始更新
正在更新，需要30秒左右，
192.168.2.201 显示
升级成功!
确定
正在建立安全连接...

FAQ