# Panabit 智能应用网关产品用户手册

## 声明

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。

责任：

- 派网仅对产品信息中预先说明的部分承担责任。除此之外，不作其它任何担保。
- 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。



北京派网软件有限公司

# 目 录

# 前言

Panabit 智能应用网关可通过 Web 管理页面进行全部管理动作：

（1） 登陆方式： https://192.168.0.200 （注：出厂默认 IP）

（2） 管理接口： EM5（企业级）或 MGT（运营商级）

（3） 用户名： admin

（4） 初始密码： panabit


对 Panabit 智能应用网关进行日常管理监控，Web 方式是最简洁最方便的。Web 管理界面已经支持主流的几种浏览器，如 IE、FireFox、Chrome 等，注意一些较老版本的浏览器可能无法正常工作，推荐最小屏幕分辨率为 1280x1024。虽然 Panabit 智能应用网关产品同样支持 SSH 或 Console 口的命令行管理方式，但我们并不推荐对系统操作命令还不是太熟悉的用户使用。

Panabit 智能应用网关产品主要支持两种模式接入网络：透明网桥模式和旁路监听模式。在网桥模式下，您无需改变原有网络拓扑及配置；旁路模式时，您需要将出口的 Out 和 In 两个方向的流量分别镜像给 Panabit，以便于对应识别出流量的上行、下行。配置 Panabit 智能应用网关产品之前，建议您首先仔细阅读本手册的第一、第四章。

# 第一章、系统维护

本章描述 Panabit 智能应用网关产品进行系统维护的一些常用功能。包含如下功能项：

网络配置

系统管理

配置管理

日志管理

管理日志

系统告警

系统升级

## *1. 网络配置*

网络配置包含管理接口、数据接口：

本章节主要描述执行两个动作： 1、设置管理接口的 IP、掩码、网关；2、通过数据接口，设置系统的工作模式（透明网桥或旁路监控），同时设定各数据接口的定义，如网桥 1 -- 内网卡。

**管理接口**

此处主要完成如下动作：

- 配置/修改管理接口 IP 地址
- 配置/修改管理接口掩码
- 配置/修改默认网关

## 数据接口

此处主要完成如下动作：

- 配置/修改数据接口的应用模式 ： 网桥/监控
- 配置/修改数据接口的接入位置： 接内网/接外网
- 配置/修改数据接口的“速率设置”：默认为“自适应”


**注意：**

- 网桥模式：数据接口必须一一对应构成网桥，一内一外。
- 监控模式：同样需要两个数据接口分别设置为“接内网”、“接外网”，前者接收 out 方向镜像流量，后者接收 in 方向镜像流量，以便在统计报表中正确区分上、下行。
- 连接线缆并且与上下端接口协商成功后，数据接口“状态”即自动显示为“正常”，否则为“未连接线缆”。
- 接口名称，FreeBSD 系统对不同厂商不同速率网卡进行严格的命名区分，Panabit 智能应用网关产品全部使用稳定性与兼容性更平衡的 Intel 网卡。

其中，em 表示 Intel 千兆网卡，ix 表示 Intel 万兆网卡，fxp 表示 Intel 百兆网卡。

## 2. 系统管理

系统管理提供 Panabit 智能应用网关产品主要的几个系统维护动作，包含如下动作：

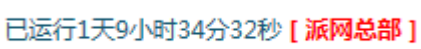
系统时间　配置 NTP 自动校时服务器 IP，手动修改当前系统时间。

密码修改　修改 Web 管理页面当前登陆用户的密码。

系统重启　重启 Panabit 智能应用网关系统，仅 admin 用户具备此权限。

系统关机　执行关机动作，仅 admin 用户具备此权限。

系统名称　修改系统名称，对应显示位置为 Web 管理界面右上角，如未修改，则此处默认显示当前登陆 Web 管理界面的用户名，如 admin。修改后的效果见下图：




## 2.3. 配置管理

配置管理提供了针对 Panabit 智能应用网关产品“配置文件”的管理动作，包含配置导入、配置导出、配置同步，仅 admin 用户具备这些操作权限。

配置导入　将提前导出的配置文件导入到系统。

配置导出　将当前的配置文件从系统中导出。

配置同步　将远端的其他 Panabit 智能应用网关设备的“配置文件”同步到本机；可选择自动或手动同步，可设置执行同步的间隔时间，单位为秒。

**注意：**

- 配置导出/导入：仅限于同一台设备；或同一款设备平台、并且网络接口设置完全相同，否则会由于接口配置不匹配而导致问题。
- 本部分所提到的“配置文件”中，不包含管理接口的相关配置。
- 非同一台或同一款设备平台，熟练用户可通过导出设备 A 的配置文件，本地修改后再执行配置导入设备 B 来实现。

## *3. 日志管理*

Panabit 智能应用网关系统本地仅保存实时数据及一些统计图表，长期历史数据需存储于独立的“Panabit 日志中心”。本章节即描述了如何在 Panabit 智能应用网关系统本地进行配置，以达到输出各种日志数据到“Panabit 日志中心”的说明。

本章节包含：设备编号、流量日志、会话日志、URL 日志、其他事件、清除流量日志。

设备编号　设置本台 Panabit 智能应用网关的设备编号，Panabit 日志中心通过此编号来区分日志来源。

流量日志　设置对应接收本地流量日志的“Panabit 日志中心”服务器 IP、端口、采样间隔；如果将端口设置为 0，则表示不开启流量日志的输出功能。

会话日志　设置对应接收本地会话日志的“Panabit 日志中心”服务器 IP、端口、是否开启会话日志记录、是否开启 HTTPHOST 日志记录；统计当前会话日志的输出信息，如下图所示：


URL 日志　设置对应接收本地 URL 日志的“Panabit 日志中心”服务器 IP、端口、是否开启 URL 日志记录、设置发送速率、选择“忽略文件类型”（需事先设置文件类型，见本手册第 37 页）

其他事件　设置除 URL 之外的其他事件，如 QQ 登陆、MSN 登陆、DNS 请求、用户认证、新浪微博、腾讯微博、淘宝登陆等应用事件的日志中心服务器 IP 及端口。

清除流量日志　清除 Panabit 智能应用网关本地的相关数据。

**注意：**

- Panabit 智能应用网关系统与 Panabit 日志中心，可进行日志数据的交叉输出与保存。比如：三台智能应用网关 A/B/C，统一输出“流量日志”到日志中心 D，统一输出“URL 日志”到日志中心 E；或日志中心 M 分别接收智能应用网关 A 的 QQ 登陆日志和智能应用网关 B 的新浪微博日志。

## *4. 管理日志*

管理日志主要记录 Panabit 智能应用网关系统的用户登陆记录与用户操作记录、设备当前已登陆的用户等信息，包含：今日日志、历史日志、在线用户：

今日日志　最近 24 小时内，登陆过 Web 管理页面的用户名、登陆 IP、登陆时间、操作记录、参数信息。

历史日志　以文件方式，记录系统自启动运行后用户登陆 Web 管理页面的相关记录，包含登陆用户名、登陆 IP、登陆时间、操作记录、参数信息。

在线用户　最近查看当前已经登陆 Web 管理页面的在线用户，非 admin 用户可被强制下线。

## 5. 系统告警

通过系统告警设置，既可以将告警信息发送到远端服务器，也可以将这些信息以文件形式保存在本地。包含：参数设置、今日信息、历史信息。

参数设置　设置远程接收告警信息的服务器 IP、端口。

今日信息　以列表直观显示最近 24 小时内，系统输出的告警信息。

历史信息　以文件形式按天单独保存系统输出的告警信息。如果当天无告警，则无对应文件。

## 6. 系统升级

系统升级是 Panabit 智能应用网关系统进行版本升级和 License 授权文件导入的地方，建议用户在接收到经销商/厂商发布的升级包之后，尽快升级，以确保 Panabit 智能应用网关系统持续发挥最佳的全网流量识别与精确的带宽管控效果。

升级系统　第一步本地上传版本升级包，第二步执行系统升级动作。

升级 License　导入 License 授权文件。

**注意：**

- Panabit 智能应用网关产品除支持正常的“正向升级”，也支持“反向升级”，即可以通过“升级系统”功能进行版本回退动作。
- 正常的进行无间隔版本升级时，无需重启设备。（若需要重启，派网的新版本说明文件或消息中会明确提示）
- 支持“跨版本”升级； 当跨越版本较多时，建议重启设备，以确保其中的某个版本涉及到内核、驱动的变动，否则无法正确生效。
- 升级版本会中断网络约 3-15 秒，因此请避开网络高峰期进行升级动作；升级 License 无影响。后期特征库与系统分离后，升级时可实现真正的“无断网”。
- License 授权信息包含“使用许可时间”和“升级许可时间”两部分，系统使用许可时间默认为 8000 天，License 过期或失效后 Panabit 系统将对数据包自动透传，不分析也不控制；“升级许可时间”过期后，仅无法执行版本升级动作，系统使用最后导入到系统内的版本继续正常运行，由于版本及特征库无法继续更新，流量识别与控制效果将不断下降。
- 进行版本升级时，有时浏览器如 IE 会由于等待超时而返回“升级失败”信息（浏览器原因，非 Panabit 系统返回）。 此时重新点一下“升级系统”，查看当前版本代号及版本日期等是否变更为最新的。如是，则版本已正常升级成功。

- 新版本升级包，通常包含：新功能模块、新特征库、系统优化、BUG 修复等几个部分。

# 第二章、对象管理

## *1. 应用协议*

本章节主要提供了对具体应用协议/软件客户端的参数配置及节点管理功能。

### 1.1 参数配置

对具体应用协议/软件客户端设置是否启用“节点跟踪”选项；如启用，需同步设置“节点生存期”，单位为“秒”。 如下图所示：


**注意：**

- 节点： 一个节点就是一个二元组：“IP+端口”，比如识别了一个游戏服务器 222.222.222.222，其端口为 3724，那么“222.222.222.222 3724”就是一个节点，在一段时间内，此节点后续的流量将不需要再次识别，Panabit 通过这种创新的方式来增强识别效率和节约处理性能。

- 节点生存期： 根据上一条描述，系统在识别并记录一个节点后，在一个时间段以内，该节点后续流量不需要被再次识别，这个被指定的时间段就是“节点生存期”。 （根据各应用协议/客户端软件的特性，Panabit 已默认设置好其“节点生存期”，一般情况下无需改动）

## 1.2 节点管理

手动添加一个节点，主要用于产生误识别后的手动处理。


**注意：**

节点管理通常适用于以下两种情况：

- 发生节点误识别，且来不及反馈或等待厂商更新特征库时：

比如做策略限制了 P2P 下载，但是发现某个游戏经常异常掉线，取消此策略后该游戏即正常，判断为节点误识别所导致。经查找，此游戏节点为： IP 222.222.222.222　端口 9999，那么就可以在“对象管理”--此游戏的“节点管理”中，手动增加这个节点(将被永久保存在该游戏的节点池中，重启系统后仍然有效)。 以后该节点的数据流，都将被正确识别为该游戏。

- 也适用于企业用户，使用到自定义协议功能时：

比如企业内部有 ERP 服务器，用户先自定义一个协议（如 MY ERP），然后再将该 ERP 服务器的 IP 地址和端口作为一个节点手动加进去，这样在后续的流量统计中，将可以统计到这个 ERP 服务器的应用流量。

## *2. 其他对象*

本章节描述了如下两个对象的功能与创建方法：

自定义协议

虚拟链路

### 2.1 自定义协议

此功能主要适用于中小企业和一些专用协议比较多的用户环境，通过对企业内部非热门的、专用的应用协议进行定义与设置，达到被 Panabit 智能应用网关系统识别与统计目的。示例截图如下：


**注意：**

- 英文名称和中文名称必须同时设置。
- 名称中不能含有特殊字符。
- 名称不能与系统已有协议名称重复，如 www、迅雷；否则系统将无法辨别而导致策略无效和统计问题。
- 系统当前最大支持自定义协议数量为 54 种。

## 2.2 虚拟链路

本功能主要适用于受物理链路所限，需要通过“IP 到 IP 方式”从逻辑上对特定“虚拟链路”中的流量进行统计与分析。 比如：针对特定的源 IP/IP 段到特定的目的 IP/IP 段进行单独统计。比如：统计内网所有人或某 IP 群组

到某互联网服务器 A 的流量情况；统计本分支机构到总部/其他分支机构的流量情况；统计内网到某网络运营商 B 的流量情况。如下图所示：


**注意：**

- 系统当前最大支持虚拟链路数量为 4 条。

# 第三章、应用路由

本章描述了 Panabit 启用应用路由功能时的相关配置信息。

Panabit 当前的应用路由功能模块主要包括：NAT、链路负载均衡、端口映射、DNS 管控。

本章通过三个主题进行相关配置动作：

对象

策略

其他

**注意：**

- Panabit 智能应用网关系统目前已支持 NAT、端口映射、PPPOE、链路负载均衡。
- Panabit 智能应用网关系统充当路由角色时，仍然以网桥模式部署，数据接口的内网口可定义为 LAN 接口，外网接口可定义为 WAN 线路。
- Panabit 智能应用网关系统当前最大支持创建 LAN+WAN 的数量为 60 条。

## *1．对象*

在本单元，Panabit 逻辑上将“对象”定义为“承载数据的网关链路”，主要包含接口线路和线路群组两部分。

## 1.1 接口线路

接口线路定义了 Panabit 系统应用路由中单线路的网关，与其它网关设备相似，在配置前同样需要区分 LAN 和 WAN 并对其分别定义，以便在后面章节 “策略路由”中调用。

### 1.1.1 LAN 接口

LAN 接口定义了内网接入网关的相关配置，如下图所示：


### 1.1.2 WAN 线路

WAN 线路的接口配置定义了广域网的接入类型。目前提供两种接入方式：静态 IP 接入和 PPPOE 拨号接入。

- 静态 IP 接入，如下图所示：


- PPPOE 拨号接入，如下图：


## 1.2 线路群组

线路群组将多条 WAN 线路集成为可供调配的负载均衡群组。目前，Panabit 可定义 8 个群组，每个群组可以添加多条广域网链路，如下图：

负载均衡配置群组，“编号”用来添加或删减链路，“群组名称”中主要是定义负载的类型。


群组中添加广域网链路，每条链路可选择不同的权重来决定流量的负载。


定义负载类型，可支持：源地址、目的地址、源+目地址、以及地址+端口号四种负载类型。


## *2. 策略*

Panabit 中“策略”可理解为对“对象”配置不同的参数来执行定义的动作。在本单元中，策略主要有：策略路由、端口映射、DNS 管控。

### 2.1 策略路由

“策略路由”顾名思义，就是对进入 Panabit 的数据包进行路由动作的操作。可根据“接口”、“地址”、“端口”、“协议”、“应用”进行单线路的路由或多线路的集群。如下图所示：


**注意：**

- “执行动作”参数如选择“FWD（Forward）”，则效果为直接转发，不做 NAT。

## 2.2 端口映射

将互联网上的访问映射到内网某个私有 IP，如下图：


## 2.3 DNS 管控

DNS 管控是对用户终端下的 DNS 进行管理。可执行 “重定向至”、“劫持至 IP”、“丢弃请求”等动作。如下图：

**注意：**

- “重定向至”参数中选择的调用对象，需提前在本章节“线路群组”中或者在“策略管理”章节中的“策略对象”--“流量代理”中创建，即 DNS 重定向与匹配。两处分别参见本手册第 23 页和第 39 页。

## *3. 其它*

在其它中 Panabit 提供了应用路由中的线路配置导入和导出功能。

线路导入 将已编写的配置脚本导入到系统

线路导出 将当前的配置脚本导出到系统

# 第四章、 策略管理

本章是 Panabit 智能应用网关系统配置使用的核心部分，包含各类对象的创建、各类策略的具体配置。包括下述主题:

参数配置

策略对象

流量控制

连接控制

HTTP 管控

MAC 管控

Web 认证

## 1. *参数配置*

Panabit 智能应用网关系统若干全局功能的开关与配置。

### 1.1 线路设置

本功能为启用和配置“IP 动态限速”，具体效果是让各 IP 的可用带宽在一定范围内根据带宽占用情况自动调整。 当带宽较空闲时，全体统一加速；当带宽占用紧张时，全体统一减速。


**线路名称** 选择已定义好的接口线路，如 WAN1。

**动态 IP 限速** 选择是否启用动态 IP 限速功能。

**线路默认带宽** 设置该线路总体可用带宽，建议比实际值略小一点，单位为 kbps，最大值为 1Gbps。

**速度维持时间** 线路内全体 IP 统一增速或减速后的停留时间。

**带宽使用下限** 线路内全体 IP 进行统一增速动作的触发阀值，线路带宽较空闲且达到这个比例时触发加速。

**加速比** 线路内全体 IP 统一增速时执行的加速比，新速度 = 当前值 +（最大值-最小值）*加速比。

**带宽使用上限** 线路内全体 IP 进行统一减速动作的触发阀值，带宽占用较紧张且达到这个比例时触发减速。

**减速比** 线路内全体 IP 统一增速时执行的减速比，新速度 = 当前值 * 减速比。

**注意：**

- 启用“动态 IP 限速”功能的两个前提条件：1、将参数“动态 IP 限速”选择为“启用”；2、流量管理策略中，参数“内网 IP 限速”的数值设置为一个范围，如 200-500（kbps），见本手册第 42 页。
- 本功能仅适用于网吧、酒店等出口带宽较小的中小型企业。运营商/高校/大型集团企业等环境强烈不推荐使用，由于用户规模大，极易有突发流量达到阀值，从而导致网络带宽频繁抖动，造成终端用户困扰和投诉。

## 1.2 内网 IP 统计

设置是否对内网 IP 启用统计功能。


**内网 IP 最大空闲时间**　　统计表内的 IP 老化时间。在这个时间内，如果该内网 IP 没有产生新的流量，则该 IP 将从统计表中予以清除。

## 1.3 伪 IP 防护

本功能主要适用于：主动防范由于内网主机中病毒或中木马，伪装成一些非法 IP 进行大量非法数据包的发送，导致内网网络或防火墙等关键设备瘫痪。 工作机制：预先定义内网合法 IP，不在合法 IP 表中的 IP 流量即被系统自动识别“内网 IP 伪装”，一旦发现这种应用流量，即可立即通过策略管理动作对其阻断。

**注意：**

- 一旦启用“伪 IP 防护”功能，则必须添加合法 IP 地址表，否则所有流量将被识别为“内网 IP 伪装”，表现为缺省页面的“统计分析饼图”中几乎全部为“其他协议”。
- 合法 IP 地址表中不能有遗漏，否则同样被识别为“内网 IP 伪装”。

## 1.4 ToS 设置

ToS（type of service，服务类型），初期主要用于对不同的应用协议打标记，配合路由器做策略路由，当前更普遍使用的主要 DSCP 标记，此参数在“流量管理”策略中可调用。

**单线 TOS** 单线（一个网络出口）环境中，每个数据包都被单独标记。例如：连接中的第一个包如 syn_ack 标记为 1，后续第四个包如 youku 被标记为 2。

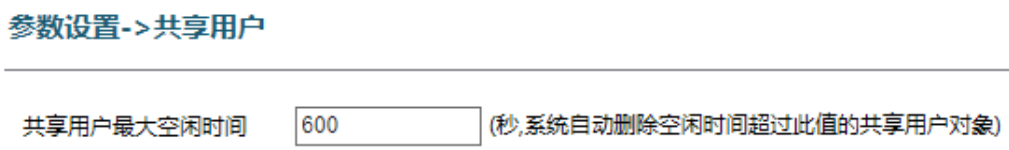
**多线 TOS** 多线(多个网络出口)环境中，需要解决“连接一致性”的问题，因此只对第一个包做标记。原因：如果第一个、第二个包分别被标记为 1 和 2，那么假设 1 走电信出口，2 则会被防火墙丢弃，因为防火墙会发现 2 没有经过“三次握手”。解决办法：引进 Proxy 机制。只有当 Proxy 代替用户完成三次握手并被识别之后，才进行统一标记。

**注意：**

- TOS 标记，仅对启用了“节点跟踪”的应用协议有效。
- 流量控制策略中的相关参数为 DSCP。

## 1.5 共享用户

设置 “共享用户”（一拖 N）的老化时间。在这个老化时间内，被检测到的终端 IP 如果没有产生新的流量，则该共享用户将从统计表中清除。




**共享用户**　　A、B、C 三人通过路由器连接在 D 之后，通过 D 的运营商所提供的帐号共同上网，则 A、B、C 即被定义并识别为“共享用户”。

## 1.6　智能 P2P 识别

设置是否启用“智能 P2P 识别”引擎。主要用于加强对加密类 P2P 协议的识别能力。此功能会适度增大系统性能开销，识别率正常时不建议启用。


## 1.7　迅雷增强识别

设置是否启用“迅雷增强识别”引擎。特别针对迅雷系列协议进行强化识别。此功能建议保持启用。


**源地址** 策略应用的源地址或地址分组。

**目标地址** 策略应用的目标地址或地址分组。

**接口** 策略所应用的接口。

**状态** 选择这个选项时，拒绝服务（DoS）可用。清除复选框使此策略不可以使用。

**编辑** 编辑策略。

**插入** 在相应的策略（出现新策略屏幕）上添加一个新的策略。

**移动** 在列表的另一个策略前后移动相应的策略。

**源接口/域** 可以监控的接口或域。

**源地址** 选择一个地址、地址范围或地址分组，限制监控流量，使其在发送自指定地址或范围内的流量范围。选择“*多选*”包括多个地址或范围。你也可以选择“新建”添加一个新的

地址或地址组。

**目标地址** 选择一个地址、地址范围或地址分组，限制监控流量，使其在发送至指定地址或范围内的流量范围。选择“*多选*”包括多个地址或范围。你也可以选择“新建”添加一个新的地址或地址组。

## 2. *策略对象*

Panabit 智能应用网关系统各类管理策略中需要调用的具体对象，需预先在此处创建与编辑。

### 2.1 数据通道

“流量管理”策略中普遍使用的对象，“集体”概念，以下场景用到：

- 流量管理策略，对指定目标对象（例如全网、IP 群组、应用协议/协议组等）做带宽限速动作。
- 启用“优先级”，对带宽的占用进行优先导向的策略规划时，需要首先创建数据通道，然后在数据通道内进行 6 个优先级子通道的划分，最后在策略中调用。
- 启用“动态 IP 限速”时，通过数据通道“告诉”系统：全局可用的最大带宽值。

下图为创建成功后的数据通道：

策略对象->数据通道

| 编号 | 名称 | 带宽(kbps) | 代发送(Bytes) | 队列长度 | 添加通道>> |
|---|---|---|---|---|---|
| 1 | P2P上行 | 100 | 0 | 24576 | 编辑 删除 |
| 2 | P2P下行 | 1000 | 0 | 24576 | 编辑 删除 |
| 3 | 主通道带宽 | 10000 | 0 | 150000 | 编辑 删除 |

下图为创建数据通道，并在其中划分优先级子通道：

**注意：**

- 通道名称，不得使用特殊字符。
- 通道仅是定义，没有被策略调用时，不具备任何效果。
- 系统当前最大支持通道数量为 128 条。
- 通道最大值为 3G，注意单位为 kpbs。
- 通道内支持 6 个优先级子通道，所有子通道带宽之和不能超过主通道（数据通道）数值。
- 优先级子通道为“保证”性质，即最低可用带宽。当带宽有空闲时，优先级高的对象可以“绝对优先”占用。

## 2.2 流量代理

Panabit 智能应用网关系统通过“流量代理”（Proxy）方式实现“应用分流”效果。此处创建及定义成功后，后续“流量管理”策略中即可调用。

**应用分流**　　以现网不低于 95%的 DPI 识别率为基础，让不同的应用协议走不同的网络出口。如 P2P 下载走 A 出口，Web 视频走 B 出口。

下图为示例，创建一个“流量代理”：


**代理名称**　　所创建的“流量代理”的名称，不得使用特殊字符。

**所在网卡**　　流量代理所在的网卡，仅设置为外网卡的可选择，网桥模式与监听模式均可。

**IP 地址**　　代理的 IP 地址，需与所在链路出口设备同一网段，并确保可路由到外网。

**网关地址**　　代理的网关地址，通常为所在链路出口设备的内网口地址。

**DNS 服务器地址**　　代理所在出口链路所使用的 DNS 服务器地址。

**VLAN-Tag**　　代理所在链路经过 VLAN 时，需配置 VLAN-Tag。

**心跳服务器 IP**　　代理的健康性检测机制，以 ping 方式进行。ping 失败时系统将自动取消代理动作，流量按照原始路径出网。

## 2.3 文件类型

在“HTTP 管控”模块中，需要针对 HTTP 不同文件类型做管控，此处进行这些文件类型的对象创建，如创建一个名为“HTTP 管控类型”的对象，包含 exe、rmvb、flv，mp3 等文件类型，示例截图如下：


**注意：**

- 群组名称不得使用特殊字符，不得与现有协议组名称重复。
- 多个文件类型以 ，隔开。

## 2.4 域名群组

在“HTTP 管控”模块中，需要针对特定域名或域集做管控，此处进行这些域名集的对象创建，如创建一个名为“购物网站”的对象，包含淘宝、京东等购物网站，示例截图如下：


**注意：**

- 群组名称不得使用特殊字符。
- 可以通过本地以文本 txt 格式导入第三方 URL 规则库。

## 2.5 IP 群组

在各种策略管理模块中，需要对特定 IP 集合（群组）进行精确管控，此处进行这些 IP 集合的对象创建，如创建一个名为“2M 包月客户”的对象，示例截图如下：


**注意：**

- 群组名称不得使用特殊字符。
- 可以通过本地以文本 txt 格式导入既有 IP 群组文件。

## 2.6 自定义协议组

在各种策略管理模块中，有时需要对多种不同协议或多个协议组进行管控，为降低手动逐条添加多条策略的工作量，此处进行这些协议组的自定义创建，如创建一个名为“公司严禁使用”的对象，示例截图如下：

**注意：**

- 英文与中文名称必须同时配置，不得使用特殊字符。
- 可选择具体协议、也可选择某个协议组，选中后点“添加至”即可。

## 3. *流量控制*

本节是 Panabit 智能应用网关系统针对带宽/流量进行具体管控动作的核心部分。

您完全可以在一条策略中实现若干组合动作。比如同时对内网所有 IP、某些协议/协议组、某个网桥、某个方向匹配数据通道进行总体限速，同时对其中的每个 IP 进行个体限速。

本节包括以下内容：创建策略组、添加策略、添加策略调度（调度计划表），这也是完成流量控制策略并令其生效的一个标准流程。

### 3.1 创建策略组

创建一个策略组，以便在其中后续创建若干条策略，如 worktime。

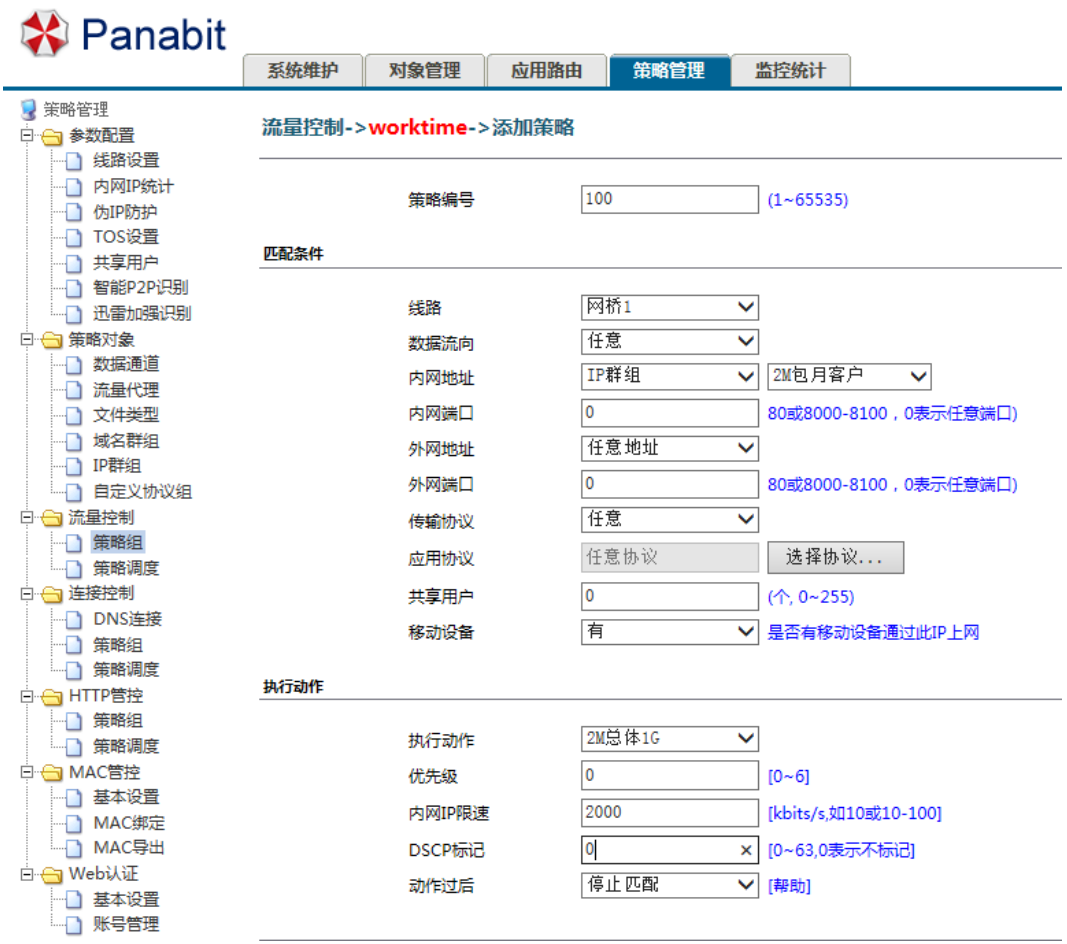
**删除策略组**　　删除选中的策略组。

**复制策略组**　　创建多个相似的策略组时，可直接复制一个策略组，然后对新策略组进行具体修改。

**创建策略组**　　创建一个新的策略组。

## 3.2 添加策略

在策略组中添加具体策略，下面的示例图表示：对经过“网桥 1”的所有“2M 包月客户”在使用所有即“任意协议”时，集体所共有的最大可用带宽为 1G（预先设置好 1 个数值为 1000000kbps 的“数据通道”），同时限定其中每个用户的个人可用带宽上限为 2M。




**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。

**注意：**

Panabit 智能应用网关系统的策略 ID 既不支持修改、也不

支持策略上下移位，这主要是避免在大流量环境中由于 1 条策略的调整导致其他相关策略同步变动而导致系统出现问题。因此在创建策略时，策略 ID 必须避免 1、2、3 这样依次使用，建议用 100、110、120 这样的 ID，以便未来需要及时插入一条策略如 109 时，可直接创建，系统即自动将其放入 110 之前。

**线路** 该策略所匹配的数据流量所经过的路径，可以是“任意”，也可以是具体的一条链路比如“网桥 1”。

**数据流向** 该策略所匹配的数据流量的方向。以内网为参照，上行表示 out，下行表示 in。

**内网地址** 内网的 IP 地址，可以是任意，可以是一个网段，也可以是一个预先定义好的 IP 群组。

**内网端口** 匹配该策略时，内网 IP 所使用的端口号。

**外网地址** 互联网的 IP 地址，可以是任意，可以是一个网段，也可以是一个预先定义好的 IP 群组。

**外网端口** 匹配该策略时，互联网 IP 所使用的端口号。

**传输协议** 任意或 TCP 或 UDP。

**应用协议** 选择并指定匹配该策略的具体应用协议，可以是一个协议，可以是一个协议组（系统默认定义或自定义均可）。

**共享用户** 每个内网 IP 下，可同时上网的终端设备数。达到此处设置的数字比如 6 时，该策略将自动触发。

**移动设备** 是否有移动设备通过此 IP 上网。“不限”表示忽略，“有”则会与策略中其他条件匹配，满足条件时该策略即自动触发。

**执行动作** 满足策略中前面的匹配条件时，所要执行的具体动作。可以是允许，可以是阻断，可以匹配某个“数据通道”，也可以选中某个“流量代理”（此处即实现“应用分流”效果的第二步，第三步是匹配“策略调度”。）

**优先级** 满足该策略前面匹配条件的对象，所对应的子通道优先级（包含在预先定义好的某个“数据通道”中）。

**内网 IP 限速** 针对个体的 IP 限速，即 IP 最大可用带宽。可以是一个特定值如 200kbps，也可以是一个范围如 200-500kbps（此处设定范围，是启用“动态 IP 限速”的前提条件之一）。

**DSCP 标记** 对满足策略中前面的匹配条件的对象进行 DSCP 标记。

**动作过后** 后续其他策略与该策略有包含或关联关系时，选择“继续”，否则“停止”。

**注意：**

- 数据通道是针对全局或集体限速；内网 IP 限速是针对个体限速。

- Panabit 智能应用网关系统与防火墙所具备的传统概念不同，并不区分源地址
  和目的地址，仅区分内网地址和外网地址。
- 实现“应用分流”功能，数据流向必须选择“上行”类，“执行动作”需选择某个“流量代理”对象。
- 创建策略时，策略 ID 避免 1、2、3 这样依次使用，建议用 100、200、210 这样的 ID，以便未来需要及时插入一条策略如 209 时，可直接创建，系统即自动将其放入 210 之前。

## 3.3 策略调度

设置相关策略组在什么时段执行的计划表，也是完成一个策略创建标准流程的最后一步。假设要在周一到周五的早 8：00 到晚 18：00 执行 worktime 策略组，则如下图所示：


**时段编号**　该策略调度的编号。同样的，有多个策略调度时，按照编号从小到大的顺序依次执行。同一时段的不同调度，执行编号小的。

**是否有效**　等同于启用或禁用。

**时段日期**　可以按周选择，也可以选择“月+日”方式。

**开始时刻**　策略调度开始执行动作的时间。

**结束时刻**　策略调度结束执行动作的时刻。

**在线用户**　与指定时段并列，同时在线的 IP 数范围。二者同时匹配时策略调度放可执行。

**策略组**　该时段执行哪个策略组。

**注意：**

- 同一时段，只能执行一个策略组。
- “缺省策略组”的正确含义： 所有有明确设定的策略调度时段之外，所执行的策略组。
- 系统当前最大支持的策略调度数量为 32 个。

## 4. *连接控制*

针对内网每 IP 并发连接做限制，适用于内网有主机中病毒或木马，爆发疑似攻击现象时的临时处理或预先防范。由于 Panabit 智能应用网关系统的性能远高于内网防火墙，此功能也经常用于防火墙实际连接性能不足的用户环境。通过 Panabit 智能应用网关系统的控制，降低上网高峰期间防火墙的连接压力，或保护其免受来自内网的攻击。

本节包括以下内容：DNS 连接、策略组、策略调度

### 4.1 DNS 连接

选择是否让连接管控策略对“DNS 连接”进行控制。这主要是考虑：

选择不控制，那么在创建策略时，考虑单 IP 的可用连接数，要适当考虑到 DNS 的连接数，避免正常的域名解析服务受到影响。

选择控制，主要是考虑当内网有 DNS 欺骗攻击时，通过统一的连接数控制，帮助内网主动过滤掉过量的 DNS 欺骗连接。

选择“控制”与“不控制”，需要根据网络具体现状确定。

## 4.2 策略组

与上一节“流量控制”创建策略组相似，创建过程及注意点不再重复。

下面以添加一条策略，目的是限制内网每 IP 的 TCP 可用连接数 200，UDP 可用数 150 为例，如下图所示：

**每 IP 最大 TCP 连接数**　匹配策略条件的每个内网 IP，所能被 Panabit 智能应用网关系统允许并放行的 TCP 连接数。

**每 IP 最大 UDP 连接数**　匹配策略条件的每个内网 IP，所能被 Panabit 智能应用网关系统允许并放行的 UDP 连接数。

**每 IP 最大连接数**　匹配策略条件的每个内网 IP，所能被 Panabit 智能应用网关系统允许并放行的最大连接数，可以小于上述两项之和。

**注意：**

- 可针对具体应用协议限制连接数。
- 可针对外网特定 IP 地址限制连接数。比如用于防范内网去攻击外网特定服务器。
- “TOP 用户”或“IP 档案”中看到的每 IP 连接数，是该 IP 所发起的原始连接数，并非匹配策略后所放行的连接数。看策略是否生效，在 IP 档案中是否有标记为红色的连接，有即代表策略生效，对应的红色连接即被策略所阻断的连接。

### 4.3 策略调度

与上一节“流量控制”的策略调度一致，本节不再重复。

## 5. *HTTP 管控*

本节主要介绍如何对 HTTP 访问行为进行管控。包含针对 URL 的访问管控、HTTP 文件类型的访问管控、Web 信息提示、URL 重定向等功能。

### 5.1 策略组

创建策略组，然后添加具体策略。比如欲实现上班时间不允许员工上购物网站（预先定义好域名群组“购物”，此处调用该对象），如访问则自动于浏览器弹出提示信息“上班时间，请勿访问购物网站！”

参见如下截图：


**内网地址**　　选择要匹配的内网 IP、IP 段、IP 群组。

**访问方法**　　可近似理解为：ANY =浏览和发帖，GET =浏览，POST =发帖。

**访问域名**　　访问的目标 URL，选择任意域名或相应的“域名群组”对象。

**文件类型**　　选择相应的“文件类型”对象。

**共享上网用户超过（含）**　　设置通过共享他人帐号上网的终端 IP 数，达到此数值时即自动触发该策略。

**每 IP 只匹配一次**　　如下面的执行动作设置了“Web 信息”，此处选择对于每个终端是否只显示一次提示信息。

**动作类型**　　满足上面的匹配条件时，所执行的策略动作。如允许、阻断、信息提示、URL 重定向、请求报文镜像。

**目标接口**　　选择“请求报文镜像”时，指定进行镜像数据接收的接口。

**提示信息**　　动作类型选择“web 信息提示”时，此处输入具体的提示信息。

**注意：**

- URL 重定向，目标也可以是 IP。

### 5.2 策略调度

与流量控制、HTTP 管控等章节的策略调度一致，本节不再重复。

## 6. MAC *管控*

本功能主要适用于中小型网络场境，通常用来实现静态 IP 管理（防止 IP 盗用）、防 ARP 攻击、上网权限管控等需求。

## 6.1 基本设置

MAC 管控的基本设置，如下图所示：


**内网地址**　　选择要匹配的内网 IP、IP 段、IP 群组。

**MAC 绑定**　　打开或关闭 MAC 管控功能。

**未绑定 MAC 的 IP**　　对未绑定 MAC 的 IP 执行什么动作。

**白名单**　　不受未绑定 MAC 的 IP 选项限制的 IP 对象。

**网关 IP 地址**　　指定网关的 IP 地址。

**动态项老化时间**　　一个 MAC 记录从加入地址表开始计时，如果在这个老化时间内 Panabit 智能应用网关系统未收到源地址为该 MAC 地址的帧，那么该 MAC 地址将被删除。

## 6.2 MAC 绑定

MAC 绑定各种执行动作的操作页面，见下图：


**IP 范围**　　比如 192.168.0.1-192.168.0.254

**查询**　　在输入的 IP 范围内执行查询动作，列出当前系统检测到的 IP 与 MAC 信息。

**绑定选中**　　对选中的 IP 与 MAC 执行绑定动作。

**解除选中**　　外对选中的 IP 与 MAC 执行解除绑定动作。

**手工添加**　　手动加入一个 IP 与 MAC 的绑定配对。

**从文件导入** 以文本格式导入 IP 与 MAC 的配对关系表。

### 6.3 MAC 导出

将当前系统中的 IP 与 MAC 配对信息表导出到本地保存，以“另存为”方式。

导出的格式如下图：

```
192.168.0.2 00-30-48-5d-53-96
192.168.0.199 b0-51-8e-00-d9-fa
192.168.0.230 00-21-cc-68-70-1c
192.168.1.230 00-21-cc-68-70-1c
```

## 7. Web *认证*

Web 认证做为一种普遍的安全措施，主要适用于防止未经认证的用户随意使用上网资源。

本节描述的 web 认证功能，已支持本地认证、LDAP 认证、Radius 认证、第三方认证四种方式，可根据实际需要选择具体方式，达到满足用户从通过认证到获取相应权限完成上网目的的使用需求。

### 7.1 基本设置

Web 认证的基本配置页面如下图所示：


**Web 认证** 功能开关，打开或关闭。

**不需要认证的 IP** 无需经过认证的 IP 对象。

**成功后显示页面** 用户认证成功后返回的显示页面。

**认证方式** 选择认证方式：本地认证、LDAP 认证、Radius 认证、第三方认证。

**服务器地址** 选择 LDAP 或 Radius 认证方式时，需要配置服务器的 IP 地址。

**端口号** 与上一条关联，LDAP 或 Radius 服务器使用的端口号。

**帐号目录（DN）** 选择 LDAP 方式时，需输入帐号目录。

**共享密钥** 选择 Radius 方式时，需配置共享密钥。

## 7.2 帐号管理

帐号的具体管理动作。


**创建组** 创建一个帐号组。

**修改名称** 修改被选中帐号组的名称。

**删除组** 删除被选中的帐号组。

**导出至文件** 将选中帐号组的帐号信息导出到文件中。

**从文件导入** 从本地以文件方式导入帐号信息。

**添加帐号** 在当前帐号组下手动添加帐号，并为其配置该帐号下的“最大在线人数”、IP、密码。

**编辑** 编辑相应帐号的相关信息。

**修改密码** 修改相应帐号的密码。

**删除帐号** 删除相应帐号。

# 第五章、监控统计

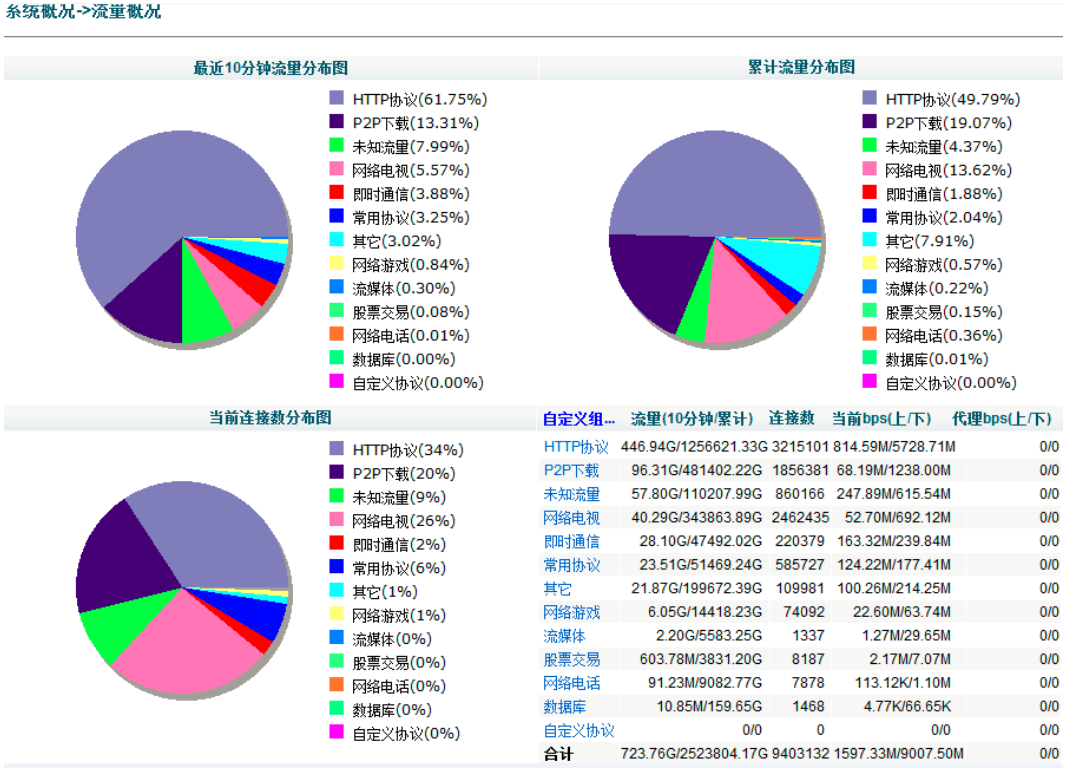
本章描述了有关 Panabit 智能应用网关系统监控统计的功能及使用方法。

## *1. 系统概况*

系统概况中提供一些网络运维管理工作中，常用的监控统计动作。可以让网络运维人员快速的获取网络当前的各种真实信息，并对下一步的管理动作提供数据指导。

### 1.1 流量概况

登陆 Panabit 智能应用网关系统后即进入缺省页面，提供网络（全局/整个系统）的概况统计图表（实时与趋势）。如下图所示：




| 自定义组... | 流里(10分钟/累计) | 连接数 | 当前bps(上/下) | 代理bps(上/下) |
|---|---|---|---|---|
| HTTP协议 | 446.94G/1256621.33G | 3215101 | 814.59M/5728.71M | 0/0 |
| P2P下载 | 96.31G/481402.22G | 1856381 | 68.19M/1238.00M | 0/0 |
| 未知流里 | 57.80G/110207.99G | 860166 | 247.89M/615.54M | 0/0 |
| 网络电视 | 40.29G/343863.89G | 2462435 | 52.70M/692.12M | 0/0 |
| 即时通信 | 28.10G/47492.02G | 220379 | 163.32M/239.84M | 0/0 |
| 常用协议 | 23.51G/51469.24G | 585727 | 124.22M/177.41M | 0/0 |
| 其它 | 21.87G/199672.39G | 109981 | 100.26M/214.25M | 0/0 |
| 网络游戏 | 6.05G/14418.23G | 74092 | 22.60M/63.74M | 0/0 |
| 流媒体 | 2.20G/5583.25G | 1337 | 1.27M/29.65M | 0/0 |
| 股票交易 | 603.78M/3831.20G | 8187 | 2.17M/7.07M | 0/0 |
| 网络电话 | 91.23M/9082.77G | 7878 | 113.12K/1.10M | 0/0 |
| 数据库 | 10.85M/159.65G | 1468 | 4.77K/66.65K | 0/0 |
| 自定义协议 | 0/0 | 0 | 0/0 | 0/0 |
| 合计 | 723.76G/2523804.17G | 9403132 | 1597.33M/9007.50M | 0/0 |

**最近10分钟流量分布图**　最近10分钟，上下行双向流量的协议组分布。

**累计流量分布图**　从上一次启动设备到当前，上下行双向流量的分布。

**当前连接分布图**　当前经过系统的并发连接数的协议组分布。

**流量（10分钟/累计）**　对应协议组在最近10分钟内的双向流量（字节）、从最后一次启动设备到当前的流量（字节）。

**连接数**　被识别并归类到对应协议组的并发连接数，有流量和未超时的。

**当前bps（上/下）** 对应协议组当前所占用的上下行带宽（速率）。

**代理bps（上/下）** 被流量代理成功进行应用分流的匹配带宽（速率）。

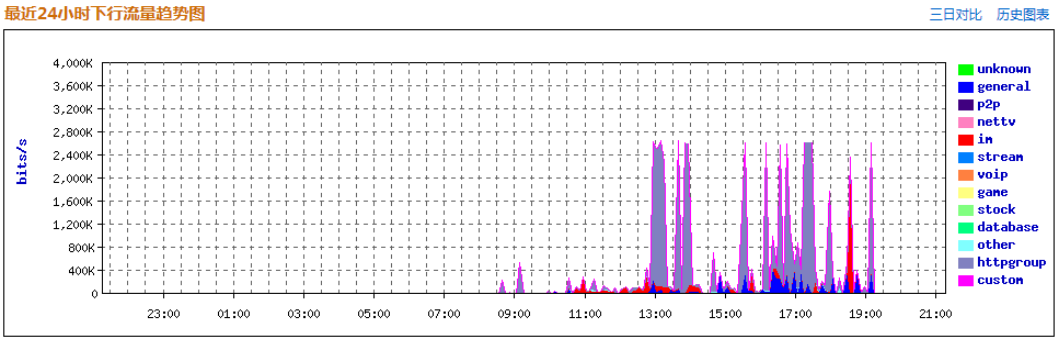
**合计** 网络当前的瞬时数据：连接数、上/下行带宽等。

**注意：**

- 饼图及协议组概况统计，采样时间为 30 秒，取当时瞬时值。
- 协议组概况统计中，各协议组的“蓝色名称”可直接点击进一步查看该协议组的详细统计信息。
- 此处是针对整个系统/全局进行统计。

## 1.2 趋势图表

为网络运维人员提供一段时间内的带宽、流量、连接变化趋势，如：最近 24 小时、三日对比、历史图表（日、周、月）等。通过这些图表，掌握网络的动态变化信息。以“最近 24 小时下行流量趋势图”为例，如下图所示：




**注意：**

- 横坐标表示时间，从左至右表示最近 24 小时，每 5 分钟绘一个点。
- 纵坐标表示带宽（速率）。
- 右侧英文协议组名称从上到下分别对应：未知协议、常用协议、P2P 下载、网络电视、即时通信、流媒体、网络电话、网络游戏、股票证券、数据库、其他协议、HTTP 协议、自定义协议组。

## 1.3 网络接口

各数据接口的信息和统计报表，在这里可直观掌握各数据接口的实时工作状态。如下图所示：


**名称** 数据接口名称。

**线路** 工作模式以及隶属关系。

**接入位置** 数据接口的具体定义，内网口还是外网口。

**状态** 该数据接口当前的状态。

**驱动** 该数据接口当前所加载的驱动类型。增强型表示Panabit定制驱动；BSD表示FreeBSD自带驱动。

**型号** 该数据接口的网络芯片。

**MAC** 该数据接口的MAC地址。

**bps** 该数据接口当前的带宽转发速率。

**pps** 该数据接口当前的PPS（Packets per Second）转发速率。

## 1.4 网桥

如果配置了多路网桥，这里可选择查看单独某个网桥的统计数据，如网桥 1。

## 1.5 虚拟链路

如果在前面的“策略对象”中配置了“虚拟链路”，此处即可选择并查看其具体统计信息。

## 1.6 WAN 线路

启用路由功能后，对 WAN 线路的实时状态统计。比如 PPPOE 所获取的 IP、当前 PPPOE 状态、网关信息、VLAN、连接数、速率等。

示例见下图：


## 1.7 TOP 应用

针对应用协议的 TOP 排名，适用于需要查询网络当前的“最 XX 应用”，比如网络变拥堵时查询最占用带宽的应用排名。查询参数可选择：所有流量（全局）、具体线路如网桥 1、 上行 bps、下行 bps、连接数、最近 10 分钟流量、累计流量、代理上行 bps、代理下行 bps、显示项的数量、刷新时间等。如下图所示：


**注意：**

- 点具体应用名称，可得到该应用的趋势图表、在线用户、相关策略。

## 1.8 TOP 用户

针对用户（IP）的 TOP 排名，适用于需要查询网络当前的“最 XX 用户”，比如网络变拥堵时查询最消耗带宽的用户、怀疑网络遭受内部攻击时的嫌疑。查询参数与“TOP 应用”相似。如下图所示：

**注意：**

- 当怀疑内网受到攻击时，可按照“连接数”排序，查找连接数异常的IP，然后进行相关处理。
- 可指定一个 IP 范围进行查询，如只查找一个 IP 时，起始和终止两处都填写同一个 IP，如 192.168.0.6。
- 可提供精细的 IP 档案，如查询某个 IP 当前的应用概况、连接信息、身份信息、共享用户、移动终端等。 能在数以 10 万计同时在线用户的网络中，在同时进行 DPI 识别、策略匹配并提供内网任意一个 IP 实时的详细统计信息，这是 Panabit 性能优势和 DPI 优势显现的地方之一。

## 1.9 移动终端

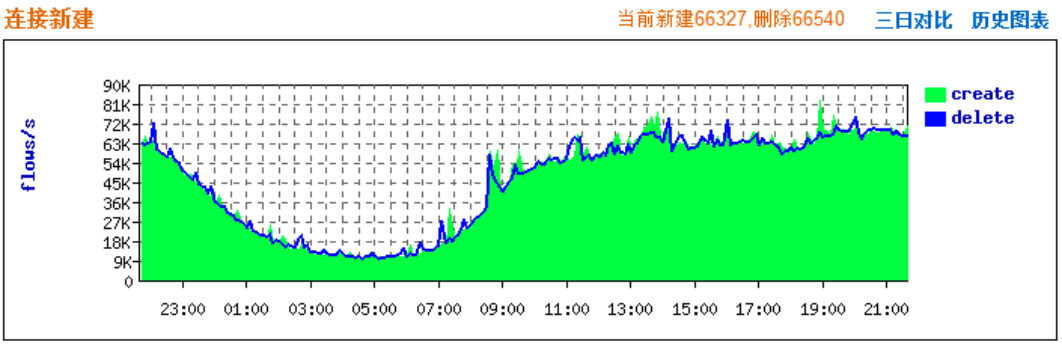
对内网的移动终端进行统计。如下图所示：

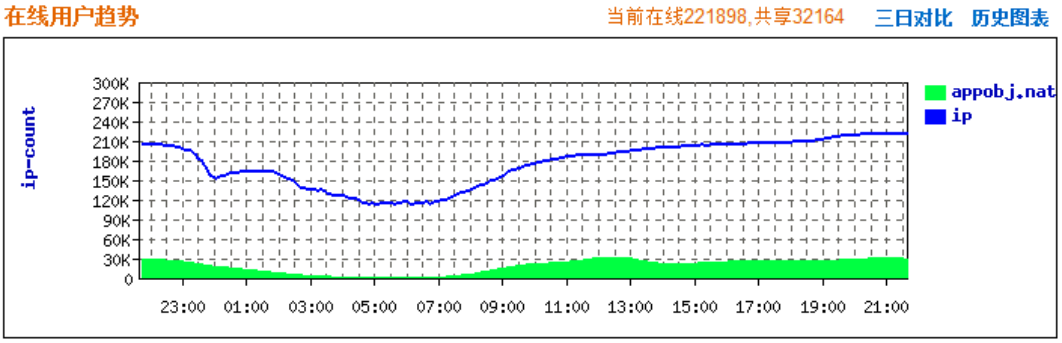
移动终端在线概况

| 编号 | 终端型号 | 当前在线(数目|百分比) | 操作 |
|---|---|---|---|
| 1 | iPhone | 6411 39/% | 三日对比 历史趋势 在线用户 |
| 2 | iPad | 6023 36/% | 三日对比 历史趋势 在线用户 |
| 3 | iPod | 343 2/% | 三日对比 历史趋势 在线用户 |
| 4 | 华为未知型号 | 39 0/% | 三日对比 历史趋势 在线用户 |
| 5 | 摩托未知型号 | 0 0/% | 三日对比 历史趋势 在线用户 |
| 6 | 三星未知型号 | 67 0/% | 三日对比 历史趋势 在线用户 |
| 7 | 中兴未知型号 | 12 0/% | 三日对比 历史趋势 在线用户 |
| 8 | 小米手机 | 159 0/% | 三日对比 历史趋势 在线用户 |
| 9 | 华为C8500S | 1 0/% | 三日对比 历史趋势 在线用户 |
| 10 | 中兴U880 | 50 0/% | 三日对比 历史趋势 在线用户 |
| 11 | 摩托XT910 | 25 0/% | 三日对比 历史趋势 在线用户 |
| 12 | 摩托Milestone | 8 0/% | 三日对比 历史趋势 在线用户 |
| 13 | 三星GT-S5820 | 13 0/% | 三日对比 历史趋势 在线用户 |
| 14 | HTC手机 | 3195 19/% | 三日对比 历史趋势 在线用户 |
| 15 | 宇龙酷派 | 10 0/% | 三日对比 历史趋势 在线用户 |
| 16 | 三星GT-S5830 | 20 0/% | 三日对比 历史趋势 在线用户 |
| 17 | 诺基亚未知型号 | 0 0/% | 三日对比 历史趋势 在线用户 |
| 18 | 诺基亚N9 | 8 0/% | 三日对比 历史趋势 在线用户 |
| 19 | THL_V9 | 0 0/% | 三日对比 历史趋势 在线用户 |
| 20 | 合计 | 16384, 100/% | 三日对比 历史趋势 在线用户 |

## 1.10 其他信息

系统当前使用的版本信息、特征库信息、License 信息、系统新建/删除会话数、在线用户数、共享用户数、CPU 使用率等。




**注意：** Panabit 智能应用网关系统的 CPU 使用率，系统设计为恒定值，目的是充分发挥系统的性能，保证高效率、低延时。

## 2. 当前策略

这里可方便的查看系统当前在运行的各种策略，可方便的对数据通道（仅流量控制策略）进行编辑、删除动作，以及对具体策略进行编辑、删除、禁用、启用等动作。下图为当前执行的“流量控制”策略：


**注意：** 当没有定义策略调度，或当前系统时间处于所有策略调度时间表之外时，当前策略处即为空白。

### 3. 应用协议

对具体应用协议、协议组的统计信息。

Panabit 智能应用网关系统通过多级协议目录对应用协议进行精确定位，如 HTTP 协议---Web 视频---优酷系列---i 酷。

此处可实时查看各应用协议的具体信息，如：连接数、节点数、流量、bps、趋势图表、在线用户、相关策略。