



2022

可视化网络领导者

# 派网智能网关典型场景配置 出口负载均衡

01 派网负载均衡介绍

02 典型案例

03 实操负载均衡典型案例配置

04 常见问题



01

## 派网负载均衡特点介绍

# 派网负载均衡特点

**派网出口负载均衡优势** 派网负载均衡不仅仅支持传统五元组链路负载均衡功能，当用户有多条ISP 链路接入时候，还支持基于7层应用协议、域名、服务、时间，通过轮询、带宽权重等要素的灵活负载均衡方式，按照用户需求进行链路的负载均衡。通过特色功能，可以实现把用户的应用、域名进行分流。例如：关键业务到专线，其他业务到一个普通的线路上例如家庭宽带。



派网负载均衡



## 高可用性的负载均衡

- 多出口线路灵活调度（最大支持2048条WAN线路，支持ADSL多线路捆绑），并提供线路间的保护。
- 基于应用级的负载均衡，保障重要业务质量，以及关键域名加速。
- 灵活的自定义虚拟线路，满足多种应用场景。

## 业务级故障定位

- 基于IP、会话级的用户侧、网络承载侧、服务器侧的分段实时质量监测。
- 基于应用业务级质量分析和故障定界。

## 精确的协议识别，提供优质业务负载能力

- 精确的协议识别1400+，现网识别率95%
- 灵活的自定义应用协议（IP节点和域名等），从容应对各类线路负载场景。
- 国内应用协议的实时更新。



## 丰富的流量可视化

- 线路流量实时趋势监控，流量模型展示。
- 对业务流量，访问排名，流量模型等提供全面的展示和分析。
- 基于IP用户、应用协议的画像，助力网络可视化运维和管理。

## 高性能稳定运行

- 系统双OS备份，毫秒级切换。
- 多功能启动下性能依旧稳定。
- **功能全开**后吞吐性能可以达到**100G**的负载均衡产品

## 行为管理日志审计一体化

- 全面的应用识别和精细化上网行为管控。
- 1:1全量日志会话审计，满足等保2.0的审计要求。
- 用户行为跟踪溯源。

降低成本

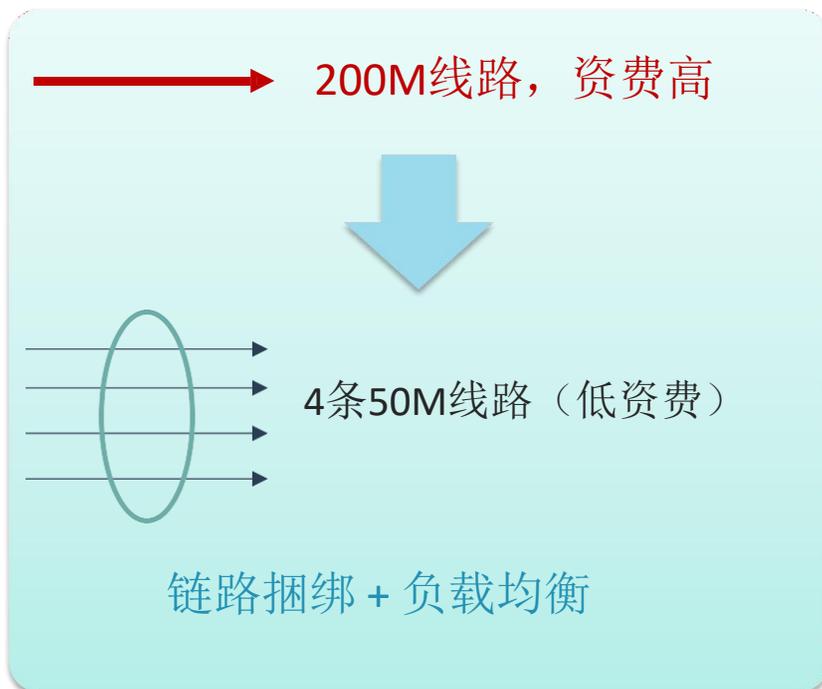
负载优化

质量监测

可视化

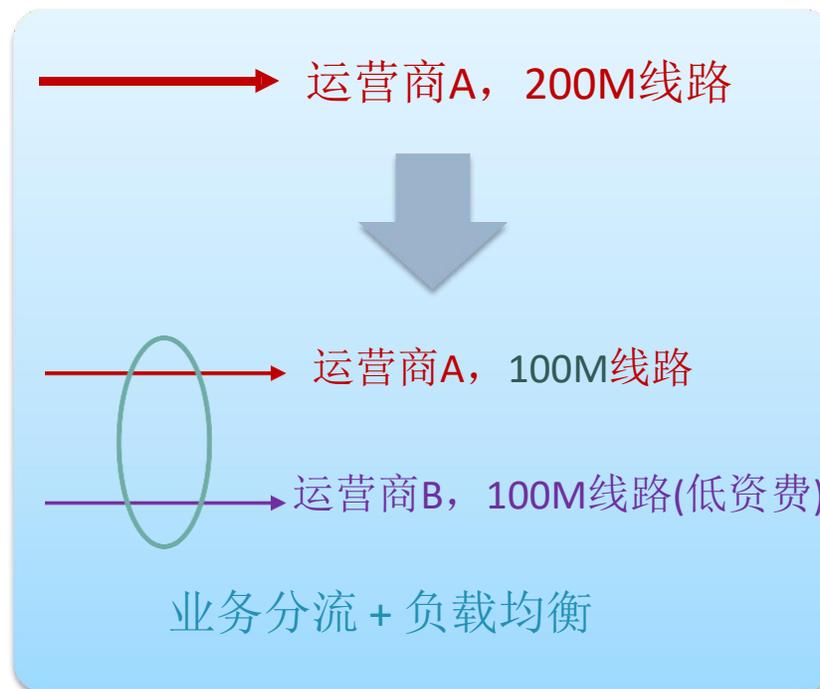
行为审计

高性能



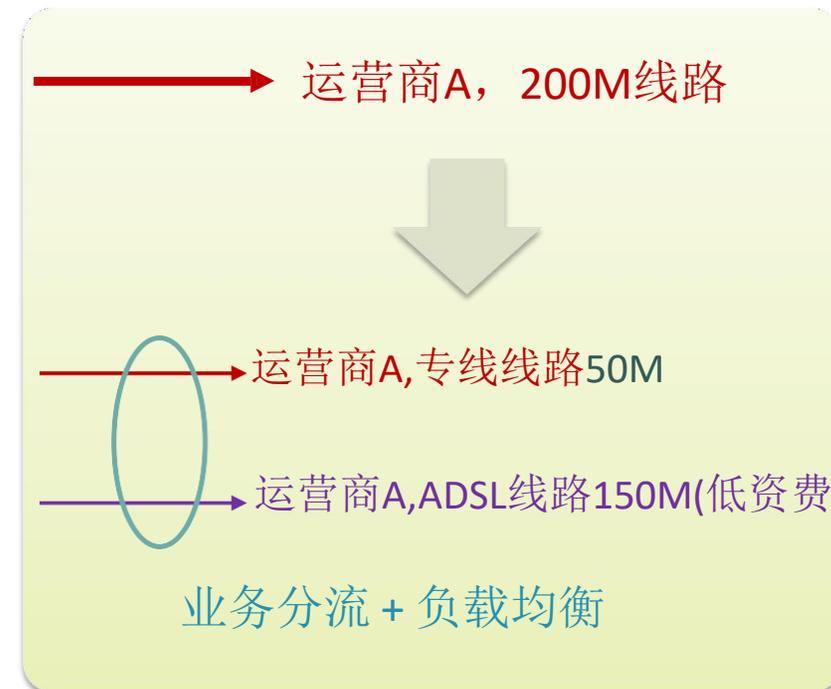
**用户场景：**带宽压力大，有扩容需求，但预算有限

**解决方案：**多条家宽线路（资费低）捆绑，满足带宽需求。



**用户场景：**带宽压力大，有扩容需求，但预算有限

**解决方案：**各运营商线路资费不同，且内容资源有差异，基于传统五元组+DNS管控+应用分流来完成负载均衡，完成多条线路上的负载分担达到线路利用率最大化，节省成本的需求



**用户场景：**带宽压力大，有扩容需求，但预算有限

**解决方案：**单个运营商线路质量有差异，通过基于业务分流和负载均衡，完成多条线路上的负载分担。

降低成本

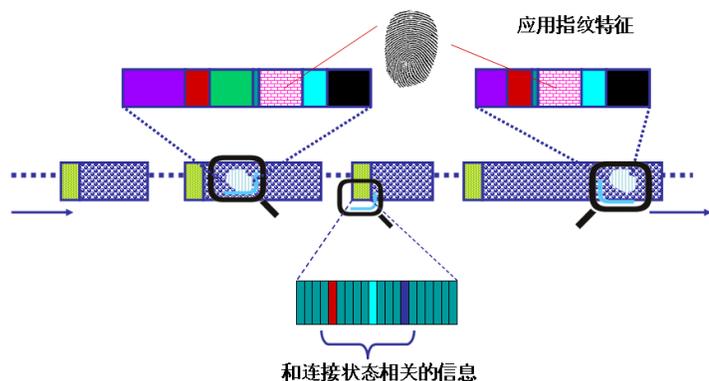
**负载优化**

质量监测

可视化

行为审计

高性能



基于域名和应用负载均衡



传统链路和IP五元组负载均衡



## 精确的应用协议识别

## 灵活的负载均衡调度

## 业务级质量测量

### 用户痛点:

某关键业务卡顿, 且原有负载均衡产品无法解决。

### 解决方案:

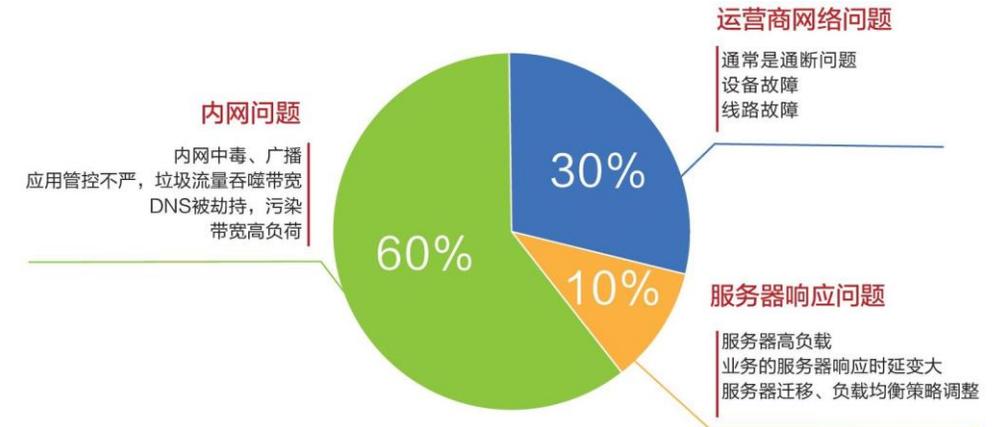
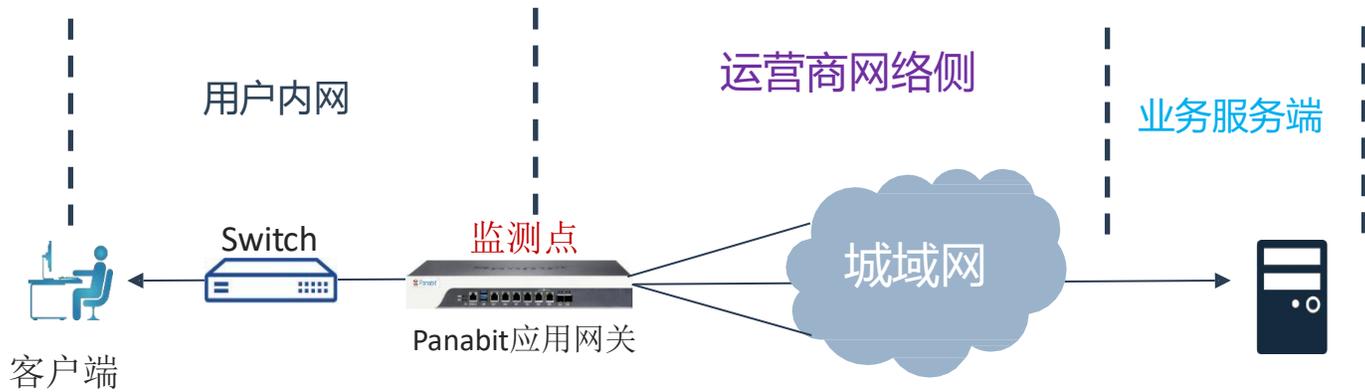
- 基于会话的业务质量检测, 分析该业务卡顿原因;
- 通过应用路由, 域名路由的方式, 将该业务流量分流至最优专线;
- 对该业务流量做带宽保障。

对比项	原有负载均衡	Panabit负载均衡
分流方式	基于五元组分流 部分支持应用分流	基于五元组分流 基于应用分流 基于域名分流 基于自定义对象的分流
识别精准度	中等偏上	国内领先, 识别1400+, 现网识别率大于95%
支持吞吐	5G以内场景居多	100G以内无压力
QOS级别	基于IP+端口号	基于应用
ISP资源	无	有优质的ISP合作资源

# 产品特点&客户价值



降低成本    负载优化    **质量监测**    可视化    行为审计    高性能



流量概况    **连接信息**    对端概况    虚拟身份    共享用户    移动终端    账号信息

应用: 192.168.1.189    端口: 2000    查询

应用	协议	状态	首包接口	策略路由	连接	查询	WAN	时长	客户时延	服务时延	应用	上行数据包	下行数据包	最大包长	MSS	流量(up/down)	其它信息
Bittorrent	udp		em5		192.168.1.189:6881-27.56.234.100:14992	印度		115s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	0	292/0	
DNS	udp		em5		192.168.1.189:51766-101.226.4.6:53	上海电信		8s	0.00ms	0.00ms	39.98ms	0/1	0/1	74/115	0	74/115	star.tianya.cn
未知800端口	tcp	OK	em5		192.168.1.189:51400-180.163.249.3:80	上海电信		1455s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	1460	75374/544654	
腾讯微云	tcp	OK	em5		192.168.1.189:51040-101.89.39.11:443	上海电信		34s	150.52ms	42.07ms	42.34ms	0/5	0/5	571/1199	1460	1374/1706	jump.weiyun.com
Android	tcp	OK	em5		192.168.1.189:52432-118.123.97.190:80	四川德阳电信		72s	4.77ms	5.49ms	6.42ms	0/4	0/203	847/1294	1460	3247/254539	wechatapppro-1252524126.file.myqcloud.com 200
移动QQ	tcp	OK	em5		192.168.1.189:53422-113.96.13.95:8080	广东广州电信		31s	2.82ms	38.47ms	44.83ms	0/3	0/4	426/1436	1460	609/1770	
魔力时代	tcp	OK	em5		192.168.1.189:49479-180.163.238.166:443	上海电信		2405s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	1460	646/496	
微信聊天	tcp	OK	em5		192.168.1.189:56458-113.96.202.106:8080	广东深圳电信		3047s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	1460	20751/30732	
移动QQ	tcp	OK	em5		192.168.1.189:56565-42.81.172.215:443	天津电信		2929s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	1460	6573/13035	
其它HTTPS	tcp	OK	em5		192.168.1.189:60223-125.64.6.150:443	四川成都电信		75s	0.19ms	4.27ms	4.71ms	0/12	0/130	827/1464	1460	8905/176583	p0.ssl.img.360kuai.com
未知800端口	tcp	OK	em5		192.168.1.189:50243-180.163.249.3:80	上海电信		7113s	0.00ms	0.00ms	0.00ms	0/0	0/0	0/0	1460	15836/9416	
其它HTTPS	tcp	OK	em5		192.168.1.189:60222-125.64.6.150:443	四川成都电信		75s	0.24ms	4.84ms	5.13ms	0/10	0/124	827/1464	1460	7251/170494	p0.ssl.img.360kuai.com

## 业务级质量监测:

- 在用网过程中, 经常遇到诸如“视频会议卡顿”、“网页打开慢”等问题。
- 相比于网络通断而言, 运维人员更怕遇到这类问题, 一来无法通过传统网络层手段定位, 二来运维人员, 业务部门人员和运营商, 经常因为此事背锅、扯皮。
- 数据表明, 造成网络慢的原因, 更多是用户内网问题, 但通常苦于没有好的工具和手段去发现和定位这些问题。

## 应用价值:

- 业务级的质量分析和故障定界。
- 基于每会话级的用户侧、网络侧、服务器侧分段检测。
- 反应实际用户访问业务质量的被动测量, 非主动发包探测

# 产品特点&客户价值



降低成本

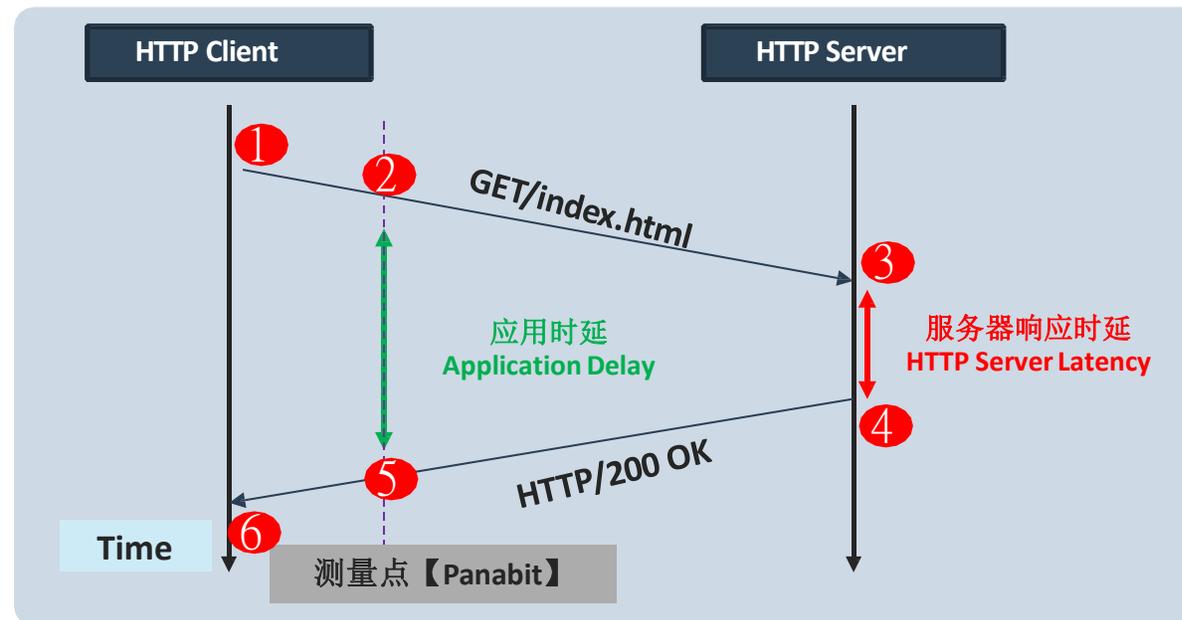
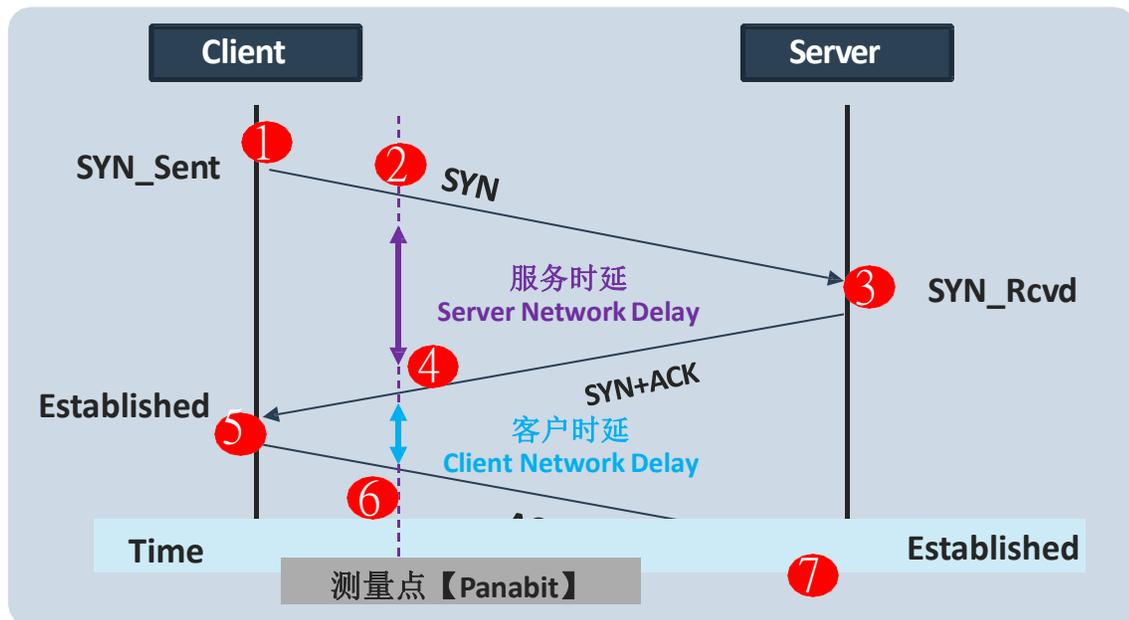
负载优化

质量监测

可视化

行为审计

高性能



时间点2:智能网关记录接收Client的syn包的时间戳  
 时间点4:智能网关记录接收Server的syn+ack包的时间戳  
 时间点6:智能网关记录接收Client的ack包的时间戳

服务时延 = 时间点4 - 时间点2  
 客户时延 = 时间点6 - 时间点4

时间点2:智能网关记录接收Client的HTTP/GET包的时间戳  
 时间点5:智能网关记录接收Server的HTTP/200OK包的时间戳

应用时延 = 时间点5 - 时间点2

客户时延

客户端至测量点的网络时延 (Client Network Delay)

若客户时延过大, 表示内网环境的延迟过大。

服务时延

测量点至服务器的网络时延 (Server Network Delay)

若服务时延过大, 表示中间网络 (运营商) 提供的承载网络延迟过大。

应用时延

应用服务器的响应时延 (Application Delay)

若应用时延过大, 表示服务提供商提供服务的延迟过大。

# 产品特点&客户价值



- 降低成本
- 负载优化
- 质量监测
- 可视化**
- 行为审计
- 高性能

负载均衡线路监测

用户和应用画像

流量可视化

- 网络总览（流量、用户）
- 流量大小和趋势
- 连接数大小和趋势
- 应用协议流量统计





# 产品特点&客户价值



降低成本

负载优化

质量监测

可视化

行为审计

高性能

## 负载均衡线路监测

## 用户和应用画像

- IP用户画像（流量信息、趋势对比、连接信息、对端信息、虚拟身份、移动终端等）
- 应用画像（流量信息、趋势对比、在线用户，连接排名、相关策略等）

## 流量可视化

The screenshot displays the Panabit monitoring dashboard with several key components:

- Top Navigation:** Includes tabs for '流量概况' (Traffic Overview), '连接信息' (Connection Info), '对端概况' (Peer Overview), '虚拟身份' (Virtual Identity), '共享用户' (Shared Users), '移动终端' (Mobile Devices), and '账号信息' (Account Info).
- Application Profiles:** A table listing applications like '淘宝网' (Taobao), '支付宝' (Alipay), and '未知' (Unknown) with their respective IP addresses and connection counts.
- User Profiles:** A table listing users with columns for '序号' (Serial Number), '终端' (Terminal), '协议名称' (Protocol Name), '连接数' (Connections), '节点数' (Nodes), '流量(上行/下行)' (Traffic), '速率(上行/下行)' (Rate), and '代理速率(上行/下行)' (Proxy Rate).
- Traffic Visualization:** A line graph showing traffic trends in bps over time.
- Online Users:** A table showing active users with columns for '序号' (Serial Number), 'IP地址' (IP Address), '账号' (Account), '流入速率' (Inlet Rate), '流出速率' (Outlet Rate), and '总速率' (Total Rate).



# 产品特点&客户价值



降低成本

负载优化

质量监测

可视化

行为审计

高性能

## 负载均衡线路监测

- 灵活的负载均衡调度
- 精细化业务分流
- 线路流量可视化
- 2000条WAN线路调度

## 用户和应用画像

1

## 流量可视化

LAN接口 WAN线路 线路日志 总流入: 50.61M 总流出: 3.91M 连接数: 3862

自动刷新 10秒 输入群组名称或WAN线路名称搜索

ID	序号	名称	类型	流入速率	流出速率	线路数量	操作
<input type="checkbox"/>	1	商务带宽	源目地址+源目端口	10.84M	2.17M	4	<a href="#">+</a> <a href="#">Q</a> <a href="#">🔊</a>
<input type="checkbox"/>	2	WAN群组2	源地址+目的地址	0	0	0	<a href="#">+</a> <a href="#">Q</a> <a href="#">🔊</a>
<input type="checkbox"/>	3	WAN群组3	策略路由				<a href="#">+</a> <a href="#">Q</a> <a href="#">🔊</a>
<input type="checkbox"/>	4	策略路由					<a href="#">+</a> <a href="#">Q</a> <a href="#">🔊</a>

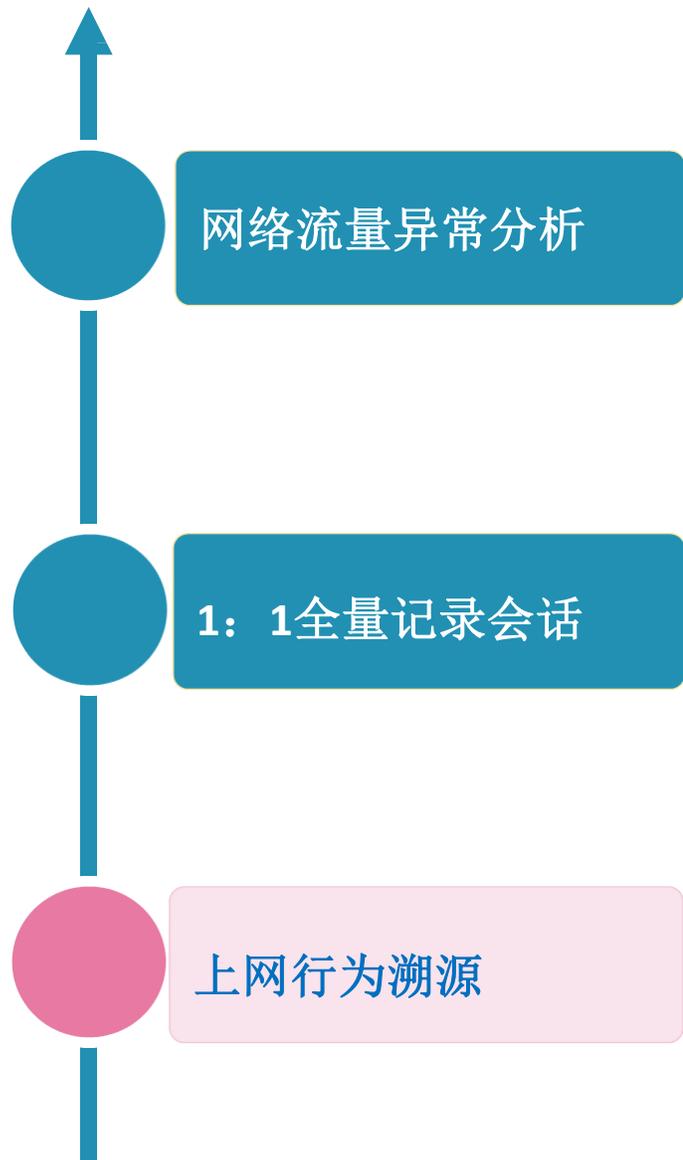
策略路由

自动刷新 10秒 当前时段 所有状态 关键词搜索

序号	时段	用户组	源接口	VLAN	TTL	源地址:端口	目标地址:...	协议	应用	DSCP	用户类型	动作	目标线路	下一跳	DNAT地址	匹配次数	备注	操作
<input type="checkbox"/>	200	any	any	any	any	云专线测试	any	any	any	0	any	路由	云专线	-	-	1205369	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	1000	any	any	any	any	any	any	any	优先保障网址	0	any	NAT	专线	-	-	374172	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	1100	any	any	any	any	172.16.28...	any	any	any	0	any	NAT	专线	-	-	0	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	1500	any	any	any	any	any	any	any	云桌面登录	0	any	NAT	专线	-	-	51357	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	2000	any	any	any	any	any	any	any	云桌面	0	any	NAT	专线	-	-	41953	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	2500	any	any	any	any	any	any	any	DNS	0	any	NAT	专线	-	-	549622	-	<a href="#">🔍</a> <a href="#">🔊</a>
<input type="checkbox"/>	10000	any	any	any	any	any	any	any	any	0	any	NAT	商务带宽	-	-	41686387	-	<a href="#">🔍</a> <a href="#">🔊</a>

- 1、基于业务对象，负载到不同的线路中；
- 2、各线路之间相互形成线路保护。
- 3、对线路中的流量匹配次数实时统计。

降低成本 负载优化 质量监测 可视化 行为审计 高性能



网络流量异常分析

1: 1全量记录会话

上网行为溯源

URL 查询 IPv6

选择设备 列表选项... 访问方式 任意 源地址 源IP群组 源端口 目标IP 目标IP群组 目标端口 运营商 所有 用户账号

域名关键字 全词匹配 URL关键字 用户MAC 协议 任意 选择协议 起始时间 2022-02-15 14 时 41 分 结束时间 2022-02-15 15 时 41 分

返回记录数 500条 查询 后台导出 导出EXCEL 导出TXT 导出CSV 下载列表 显示标题

正常日志数1103986423 非正常日志数65331

序号	设备	用户地址	MAC	用户账号	访问方式	访问时间	应用协议	标题	目标IP	目标位置	运营商	源运营商	源位置	网址
1	2	10.113.1.20:56863	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.231:80	中国 重庆 重庆	电信	其它	保留	http://p2.qhimg.com:80/t012b1dec09a9ba922e.png
2	2	10.113.1.20:56866	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p5.qhimg.com:80/t01e34d3fb7e4dccc31.png
3	2	10.113.1.20:56867	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p5.qhimg.com:80/t01fab1bcb297c196ab.png
4	2	10.113.1.20:56865	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.216:80	中国 重庆 重庆	电信	其它	保留	http://p1.qhimg.com:80/t0167f036f804952c13.png
5	2	10.113.1.20:56864	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.216:80	中国 重庆 重庆	电信	其它	保留	http://p1.qhimg.com:80/t01872368eb468079c2.png
6	2	10.113.1.20:56870	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		119.84.12.27:80	中国 重庆 重庆	电信	其它	保留	http://p4.qhimg.com:80/t0187f2280f55092a26.png
7	2	10.113.1.20:56862	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t01b2cc4b9f98de1251.ico
8	2	10.113.1.20:56868	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		171.13.14.124:80	中国 河南 洛阳	电信	其它	保留	http://p9.qhimg.com:80/t016af0142e7c8c95e4.png
9	2	10.113.1.20:56869	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		171.13.14.124:80	中国 河南 洛阳	电信	其它	保留	http://p9.qhimg.com:80/t013c9427859c1422f5.png
10	2	10.113.1.20:56872	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t012bbafe08c54f0d76.jpg
11	2	10.113.1.20:56873	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t013ec025a409b8941b.ico
12	2	10.113.1.20:56875	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t01ac78fa7e2e7a7d0f.ico
13	2	10.113.1.20:56874	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t013e77cbd9684c6bfb.ico
14	2	10.113.1.20:56871	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t0194c2350d3de0883d.ico
15	2	10.113.1.20:56862	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t0114866adcab499f99.png
16	2	10.113.1.20:56874	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t010fb5a321c9704e03.ico
17	2	10.113.1.20:56871	34-00-a3-3e-20-14		GET	02/15 14:30:12	WWW		219.151.159.230:80	中国 重庆 重庆	电信	其它	保留	http://p0.qhimg.com:80/t0163f0f6e2ddafced3.jpg

# 产品特点&客户价值



降低成本

负载优化

质量监测

可视化

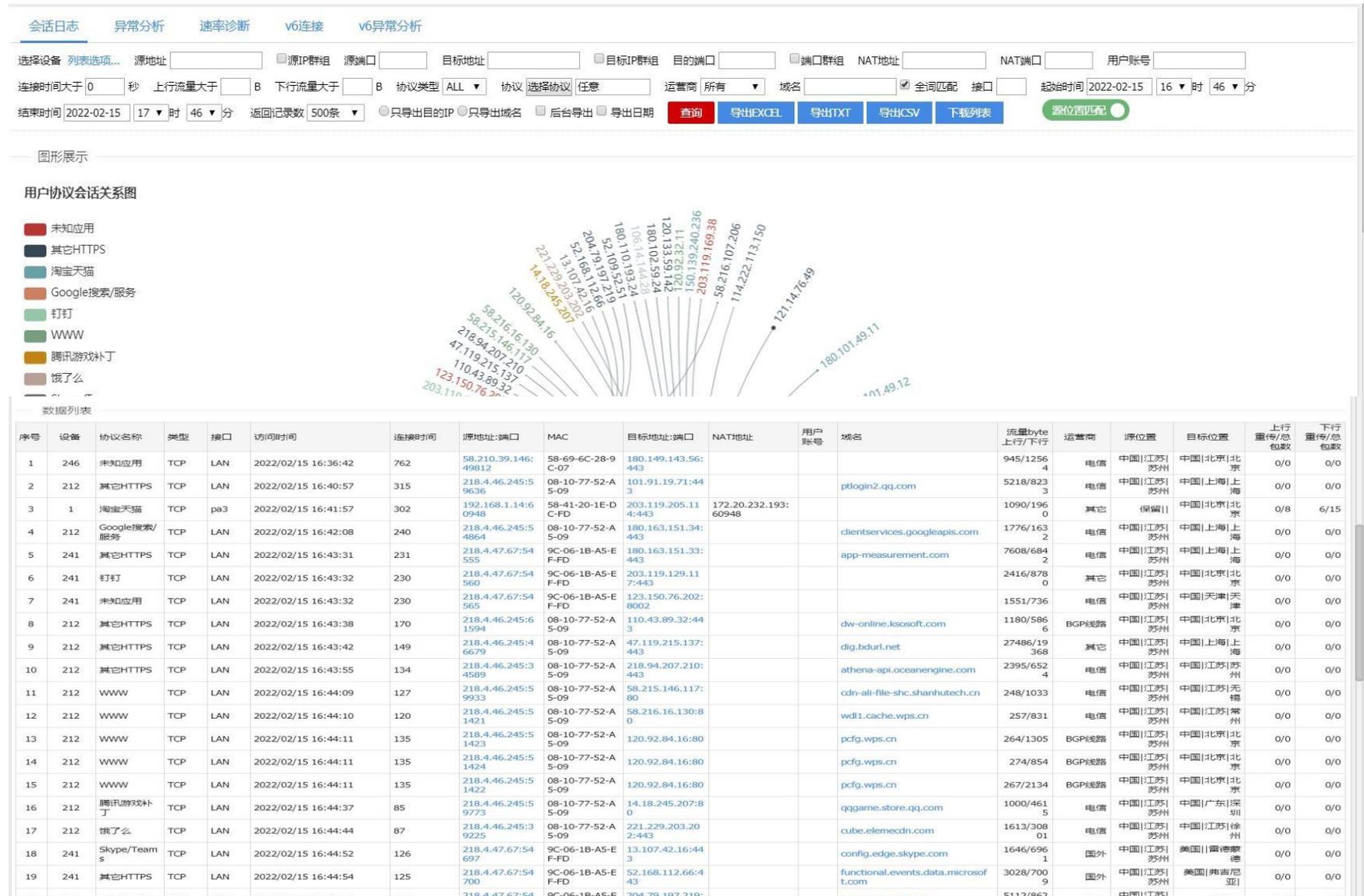
行为审计

高性能

## 网络流量异常分析

## 1: 1 全量记录会话

## 上网行为溯源



# 产品特点&客户价值



降低成本

负载优化

质量监测

可视化

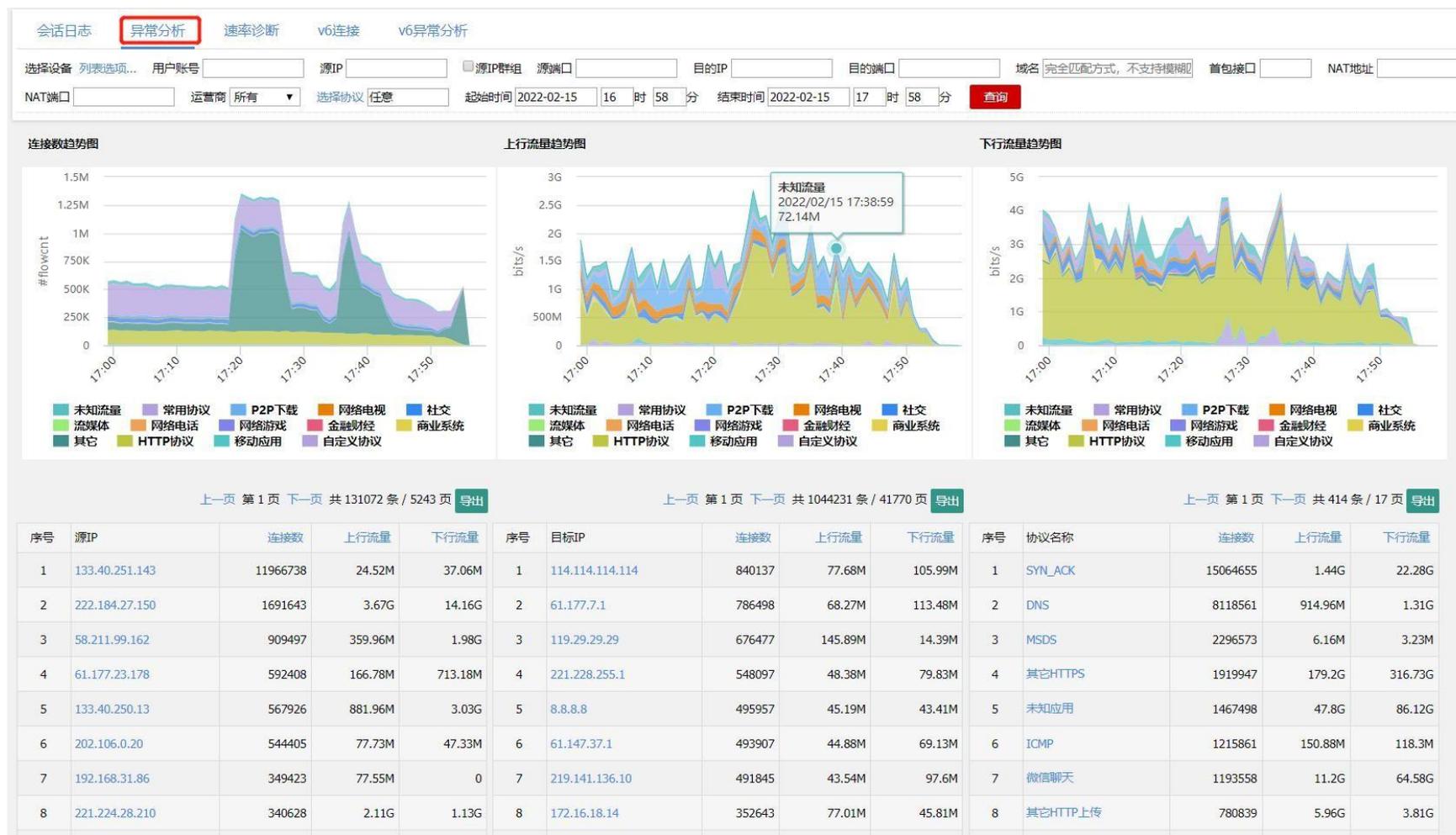
行为审计

高性能

## 网络流量异常分析

## 1: 1全量记录会话

## 上网行为溯源



# 产品特点&客户价值



降低成本

负载优化

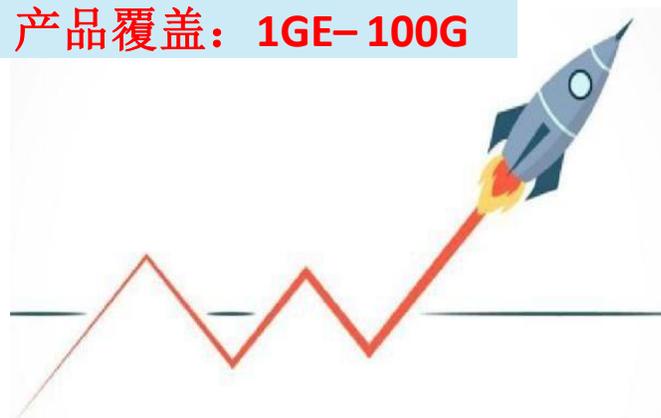
质量监测

可视化

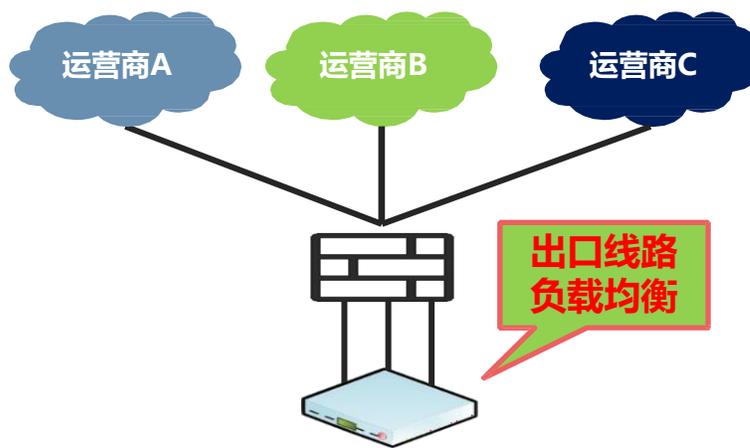
行为审计

高性能

产品覆盖: 1GE-100G



高处理性能



2000+条WAN线路负载稳定运行



Panabit双OS系统保护



规格	吞吐量	新建连接	接口	最大可扩展	尺寸/ 电源
企业型 I	800Mbps	6万/ 秒	5 千兆电口2 千兆光口	无扩展槽位	1 U / 单电源
企业型 II	5Gbps	32万/ 秒	5 千兆电口4 千兆光口2 万兆光口	无扩展槽位	2 U / 单电源
园区型	20Gbps	60万/ 秒	1 千兆电口4 千兆光口4 万兆光口	最大可扩展2 槽位 单板卡最大支持4*10G	2 U / 双电源
汇聚型 I	40Gbps	100万/ 秒	1 千兆电口8 万兆光口	最大可扩展2 槽位 单板卡最大支持2*40G	2 U / 双电源
汇聚型 II	80Gbps	150万/ 秒	1 千兆电口2 个100G 光口	最大可扩展7 槽位 单板卡最大支持2*100G	2 U / 双电源

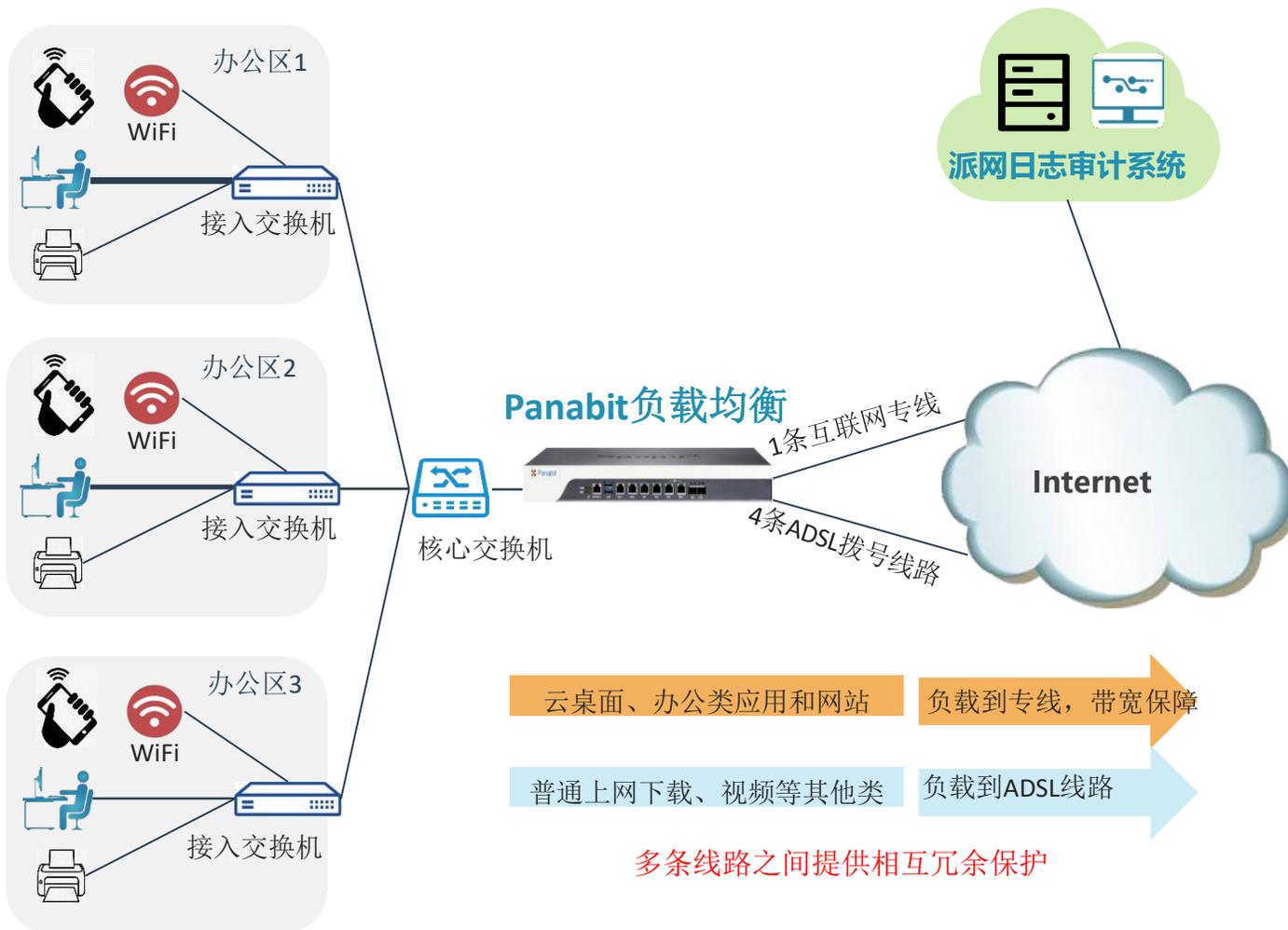


02

## 典型案例



# BJT服务中心云桌面与重要业务负载均衡方案



## 需求背景

1. 缺乏对内网的可视化管理，当前客户计划开通100个云桌面业务，但不清楚需要开通多大的带宽合适。
2. 重要业务保障，云桌面业务，办公应用和网站。
3. 出现问题，无法定位故障，影响正常业务运行。

## 解决方案

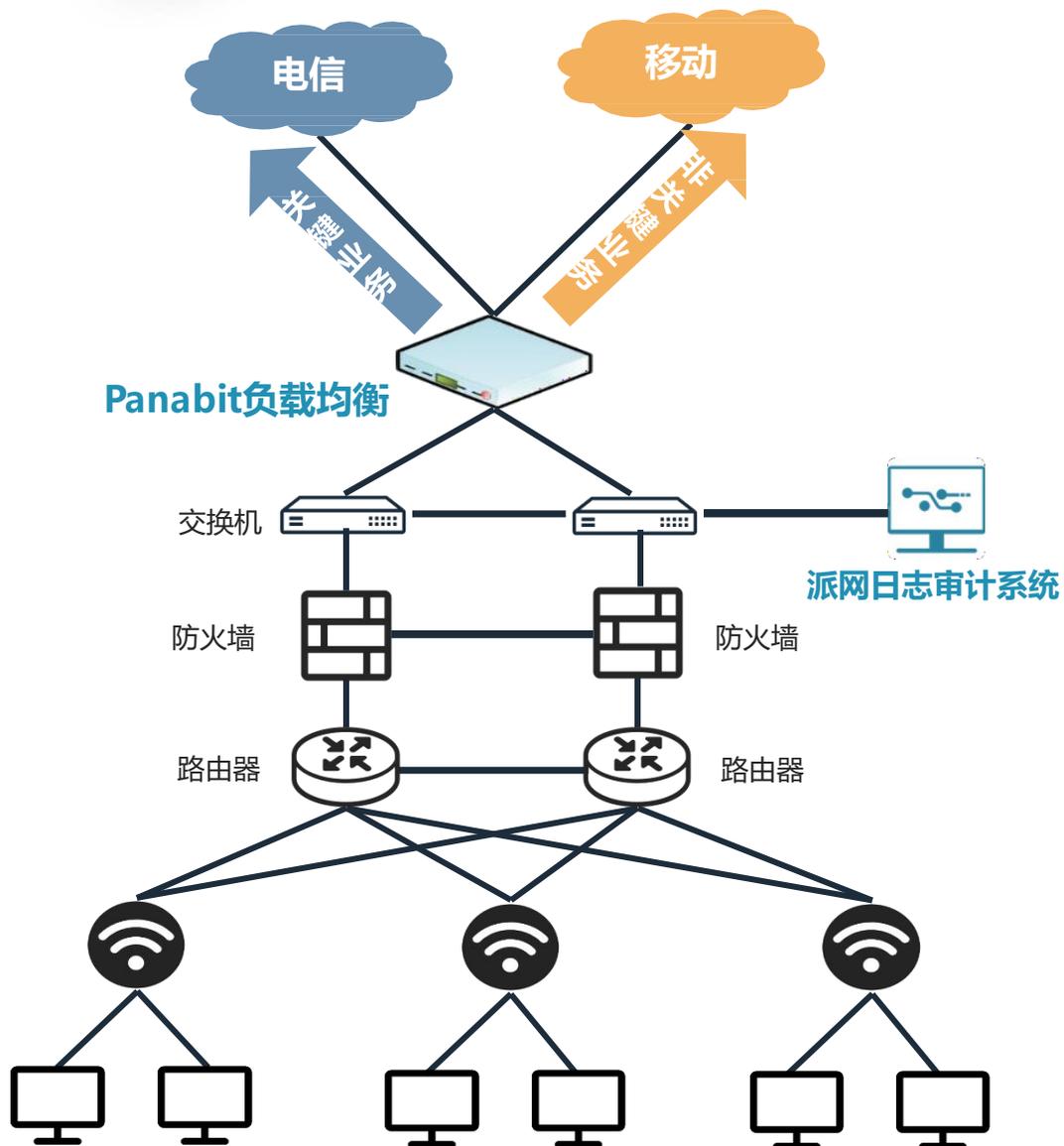
1. 部署派网网关桥接在核心交换机与防火墙之间。
2. 客户购买电信互联网专线1条，和4条ADSL拨号线路
3. 对用户内网的三个网段合理分配带宽资源。
4. 对云专线业务和常用网站进行优先级带宽保障，负载到专线，普通上网业务负载到ADSL线路，线路间提供保护。
5. 开启NPM业务质量监测，实时为业务质量进行监测管理。

## 应用价值

1. 基于关键业务的负载均衡
2. 流量可视化，NPM协助精确故障定位。
3. 重要应用业务，部分IP的带宽保障，对云桌面业务、OA办公应用、常用的网站、进行优质链路选择。
4. 精细化流量控制，对视频流量，网站进行带宽限制。



# XX政府负载均衡方案



## 需求背景

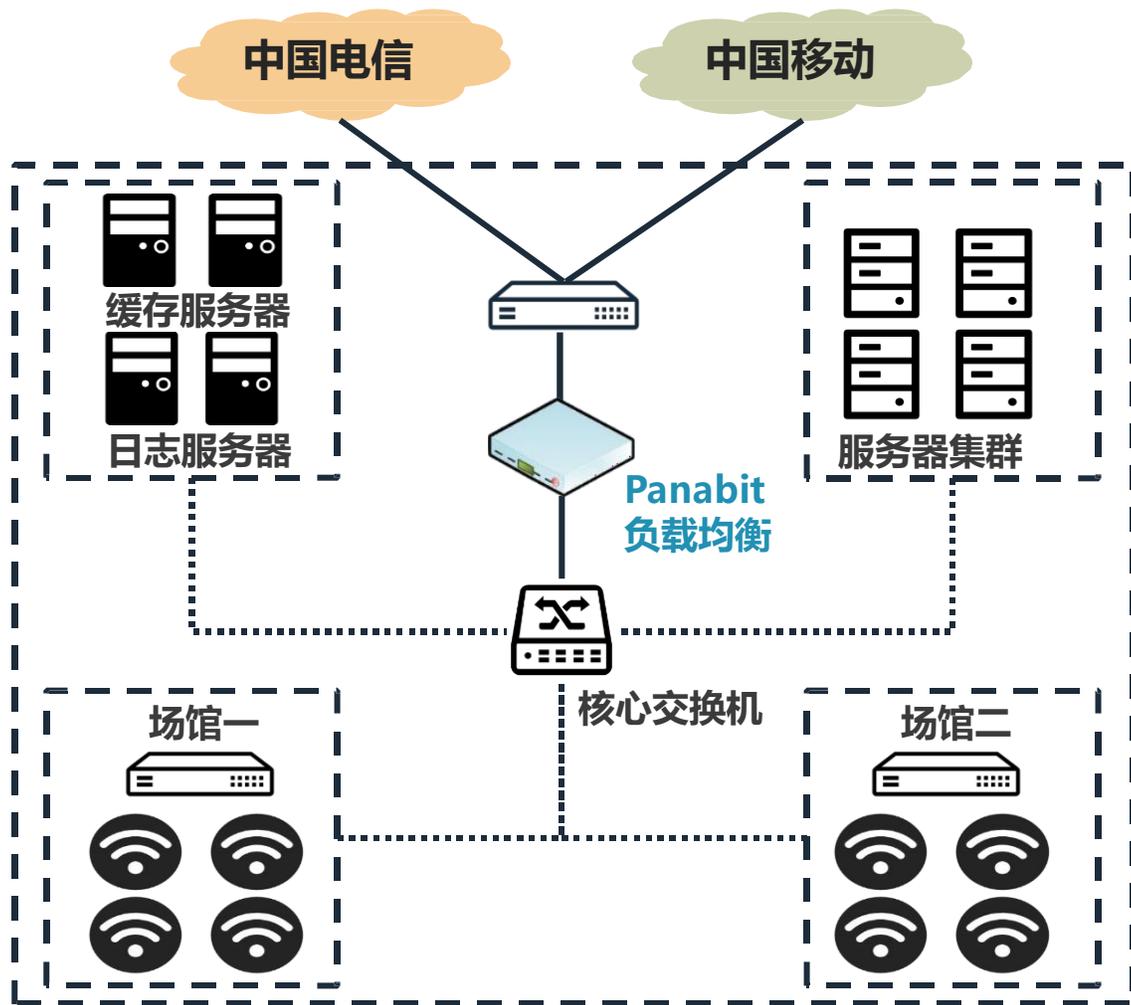
原有电信200M出口，带宽利用率达到80%左右，用户经常投诉办公服务访问慢

## 解决方案

1. 将出口改为电信100M，新购移动300M，整体带宽费用无增加
2. 在网络出口部署Panabit，实现出口负载，将关键业务分流至电信线路，非关键业务分流至移动线路

## 应用价值

1. 应用级出口负载，精准分流
2. 优化用户网络体验，降低带宽成本
3. 在有限的预算中实现带宽扩容



## 需求背景

XXX是世界上第一个以进口为主题的国家级展会

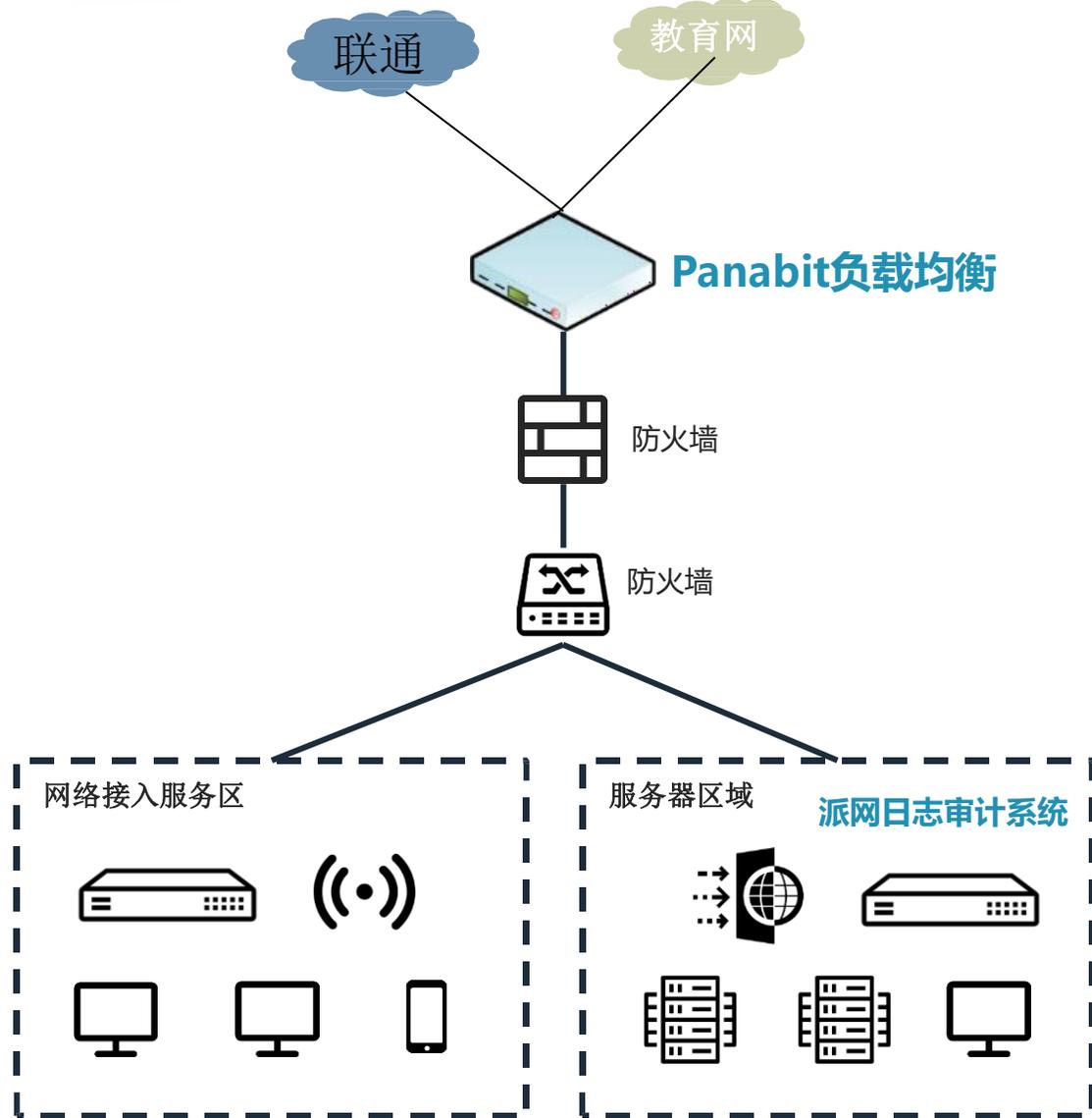
1. 经常收到来自用户的投诉，业务卡顿慢
2. 发生网络故障时，无法快速定位，运维压力大
3. 每年投资大量的带宽费用，关键业务无法保障

## 解决方案

1. 通过网关的模式部署Panabit负载均衡设备，做精准的应用分流和应用负载
2. 支持流量质量监测，来判断网络质量的好坏，从而快速定位故障问题，减轻运维压力
3. 基于域名、应用、IP、端口、协议等负载方式，将关键业务送到质量优良的线路，大流量视频送到带宽费用便宜的线路，在保障关键业务的同时降低带宽成本

## 应用价值

1. 支持基于应用进行分流，国内应用识别率领先
2. 支持基于域名进行分流，技术首创
3. 支持流量质量检测，唯一支持业务性能分析的负载均衡产品



## 需求背景

XX外国语学院大流量的出口负载均衡、主要用于联通教育网的出口优化调度。

1. 保障校园网关键应用的正常访问与被访问
2. 校园内部学生及教职工的上网行为日志分析及数据呈现
3. 全网会话一比一留存，满足网络安全法要求
4. 图书馆资源，通过对校内用户访问图书馆资源进行统计及分析网贷学生，提供及时准确的沟通辅导对象，防止不良后果发生
5. 双非网站排查，Panabit 可协助高校排查双非网站

## 解决方案

1. 在网络出口部署Panabit，实现出口线路捆绑、负载、流量控制及优化
2. 部署Panalog日志服务器，对用户的上网行为进行审计

## 应用价值

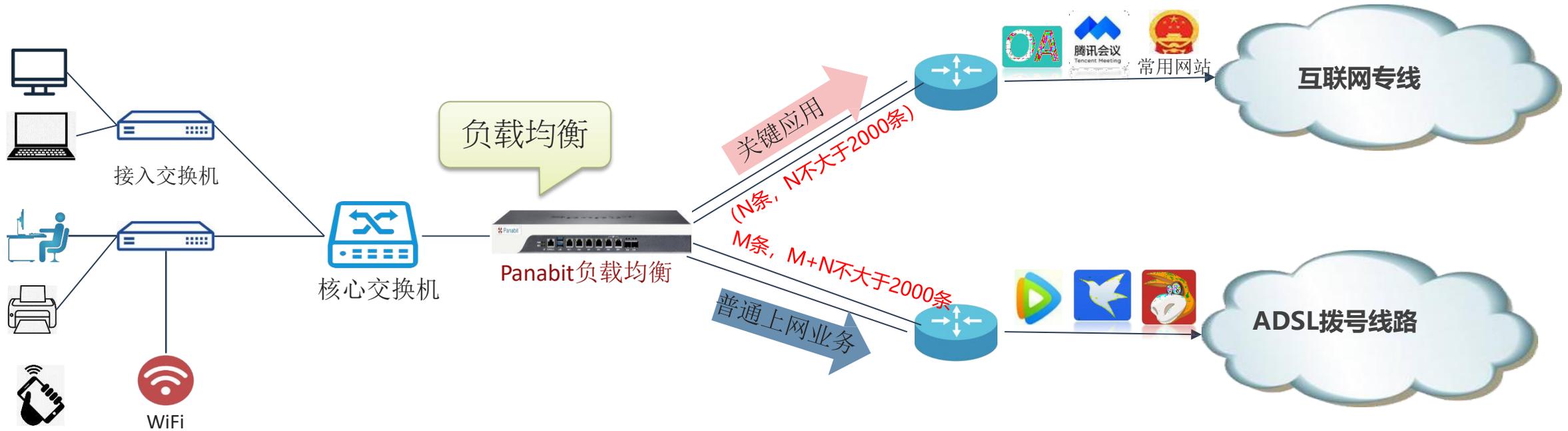
1. 网络出口优化，网络质量分析，故障快速定位
2. 全网会话一比一保存，V4和V6，满足网络安全法要求
3. 校内双非网站排查



03

## 实操负载均衡典型案例配置

# Panabit同运营商线路出口的负载均衡方案



## 场景说明:

- 同一运营商提供的线路的服务质量存在差别, 当前客户投资费用有限情况下, 选择了不同资费的线路进行负载;
- 无法提供基于业务级等精细化的负载分担, 导致重要业务无法使用优质的线路达到好的体验。

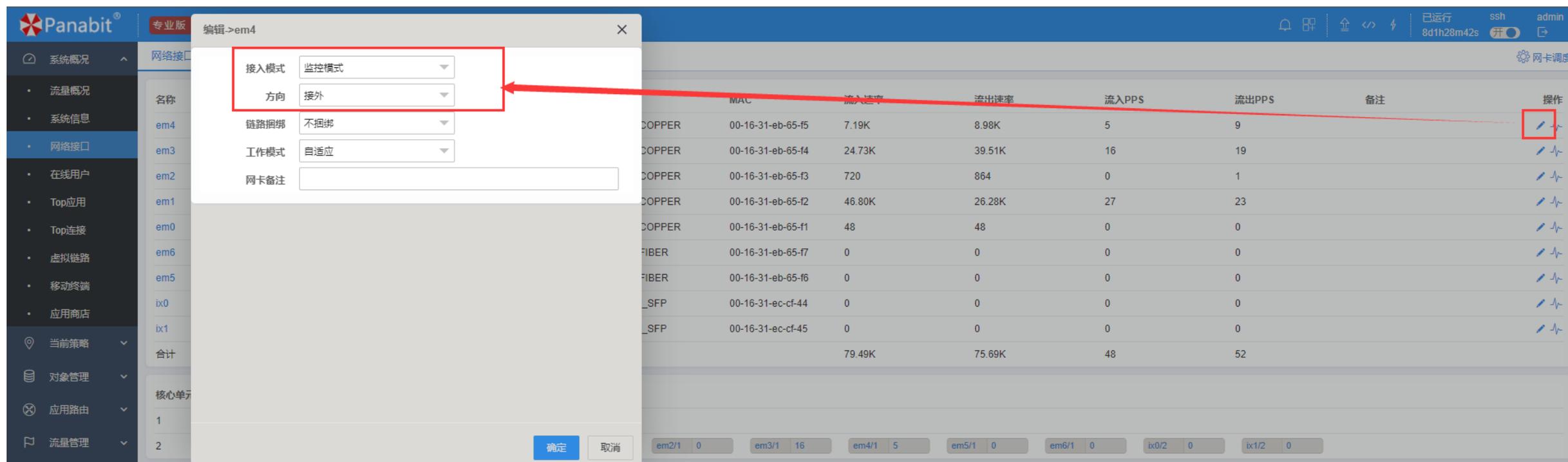
## 应用价值:

- 基于业务精细化分流能力, 以及线路捆绑的负载均衡能力, 满足客户需求同时, **保护客户投资**。
- 通过合理规划业务类型, 沟通不同服务质量的线路, 通过基于业务分流实现链路负载分担; **降低企业扩容成本**。
- 对应用自带业务测量, 记录每会话客户时延, 响应时延, 服务时延, 业务质量一目了然。
- 根据应用时延信息, 结合运营商内容资源分布, 快速进行网络优化, **提高客户体验**。

序号	配置步骤	配置详情
1	网卡配置	配置网卡方向，确认网卡用于做LAN/WAN，网桥，出口负载均衡WAN设置所以选择接外
2	WAN设置	支持多种接入方式的WAN，静态，动态，PPPoE,L2TP,ipsec自研SD-WAN（IWAN）
3	线路群组配置	设置多条线路为群组，进行负载均衡，负载均衡方式可选多种，进行组合
4	自定义业务对象	基于IP，域名，应用特征的归类已方便，路由，流控策略时作为条件调用
5	策略路由	指定路由转发至哪条线路，支持多种条件，优先级，执行动作 路由 NAT DNAT等方式

在【系统概况】-【网络接口】中，点击对应的网卡名称后的铅笔如图

在弹出的窗口中，“接入模式”选择“监控模式”，“方向”选择“接外”。



名称	MAC	流入速率	流出速率	流入PPS	流出PPS	备注	操作
em4	COPPER 00-16-31-eb-65-f5	7.19K	8.98K	5	9		
em3	COPPER 00-16-31-eb-65-f4	24.73K	39.51K	16	19		
em2	COPPER 00-16-31-eb-65-f3	720	864	0	1		
em1	COPPER 00-16-31-eb-65-f2	46.80K	26.28K	27	23		
em0	COPPER 00-16-31-eb-65-f1	48	48	0	0		
em6	FIBER 00-16-31-eb-65-f7	0	0	0	0		
em5	FIBER 00-16-31-eb-65-f6	0	0	0	0		
ix0	_SFP 00-16-31-ec-cf-44	0	0	0	0		
ix1	_SFP 00-16-31-ec-cf-45	0	0	0	0		
合计		79.49K	75.69K	48	52		

进入【应用路由】-【接口线路】-【WAN线路】，点击右上角的【添加】，

①在弹出的窗口中配置线路名称为“电信专线”，网卡选择em3，IP地址为1.1.1.1，网关为1.1.1.2，其余不变。点击【确定】完成配置；

②再次点击【添加】，在弹出的窗口中配置线路名称为“电信拨号线路1”，网卡选择em3，输入账号test1，密码pass123456。点击提交。

重复步骤①或②，即可完成多个线路的添加。

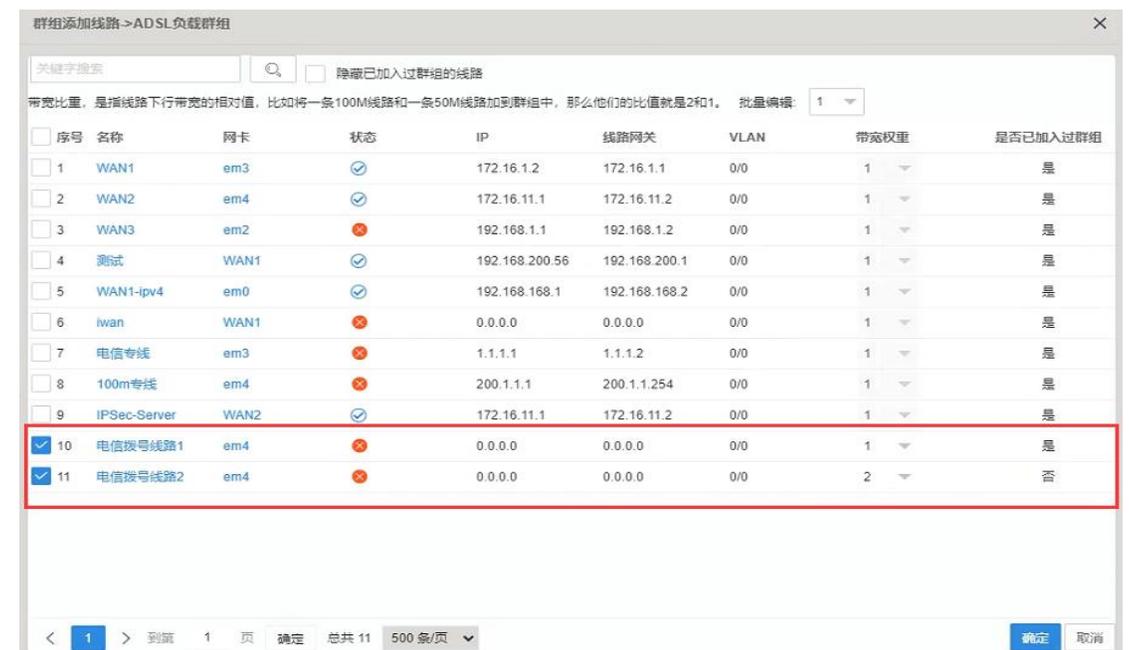
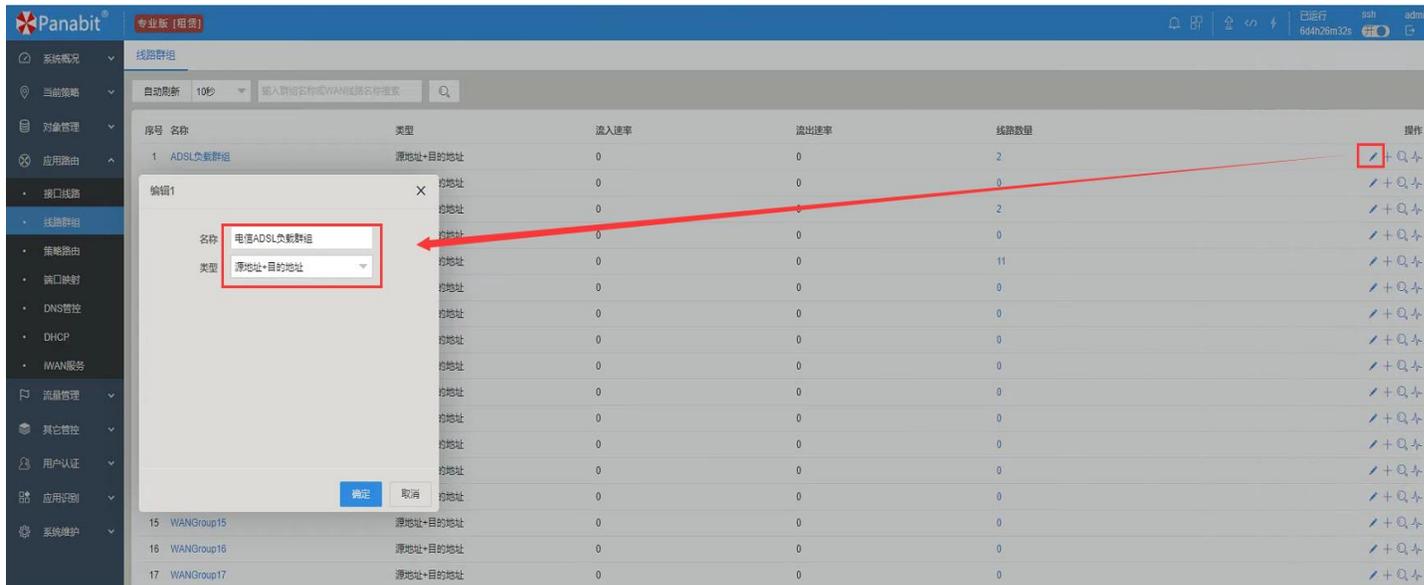


名称	电信专线
线路类型	静态IPv4
网卡	em4
备注	
静态IP参数	
IP	1.1.1.1
网关类型	正常网关
网关地址	1.1.1.2
DNS服务器	
NAT地址池	0.0.0.0
高级	
心跳服务器1	
心跳服务器2	
MTU	1500
外层VLAN	0
内层VLAN	0
克隆MAC	00-00-00-00-00-00
外网Ping不应答	<input checked="" type="radio"/> 关闭

进入【应用路由】-【线路群组】，点击WANGroup1右边的

在弹出的窗口中，“名称”输入“电信ADSL负载均衡”，负载类型选择“源地址+目的地”。点击【确定】。再点击右边

在弹出的窗口中，勾选创建的两条ADSL线路，权重线路1选择1，线路2选择2。



**Tips:** 在线路群组中请根据带宽的不同来调整带宽权重，在该场景下，线路1：线路2的带宽为100M：200M，权重分别设置为1和2。

# 派网负载均衡案例配置

网卡配置

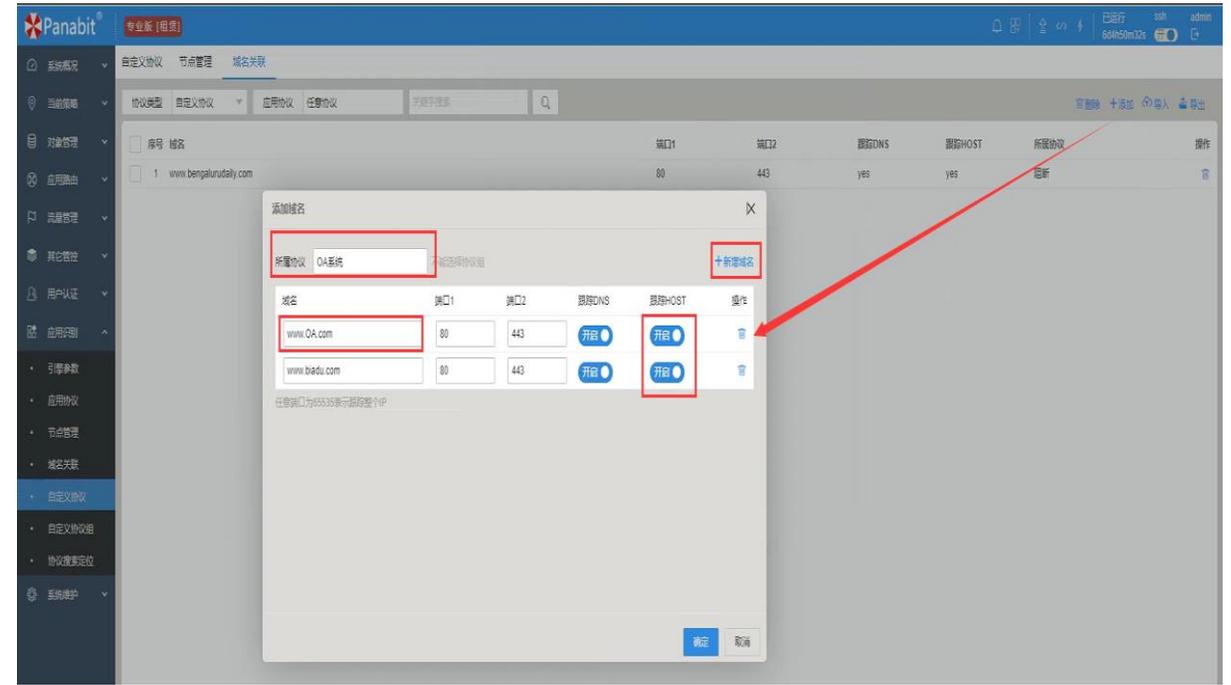
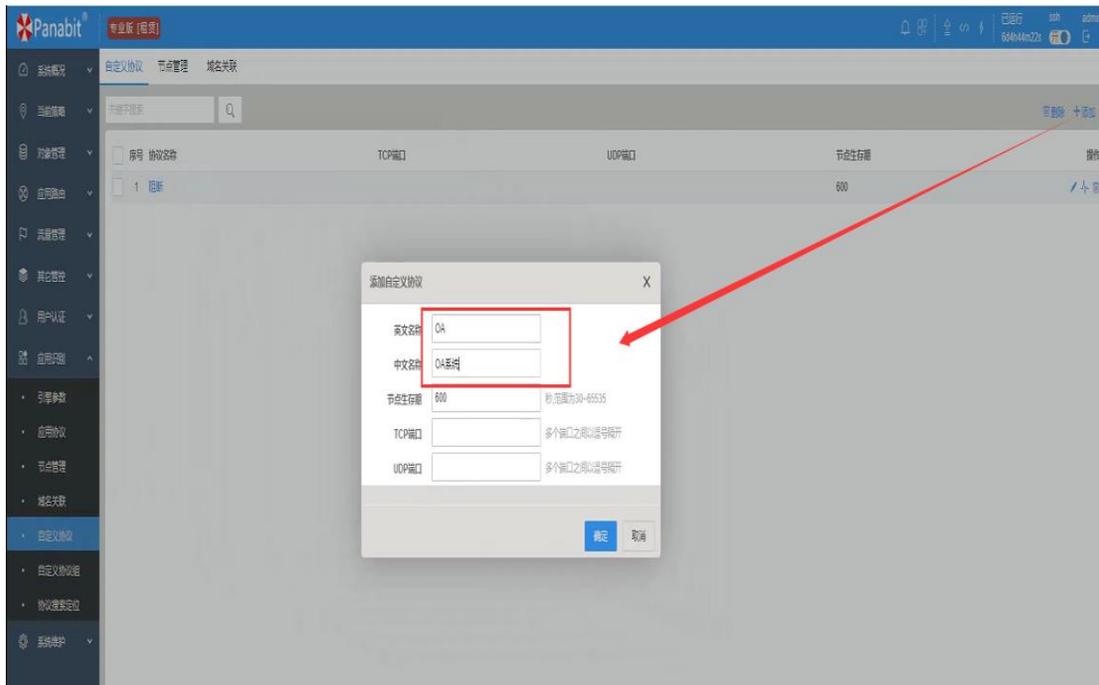
WAN设置

线路群组配置

自定义业务对象

策略路由

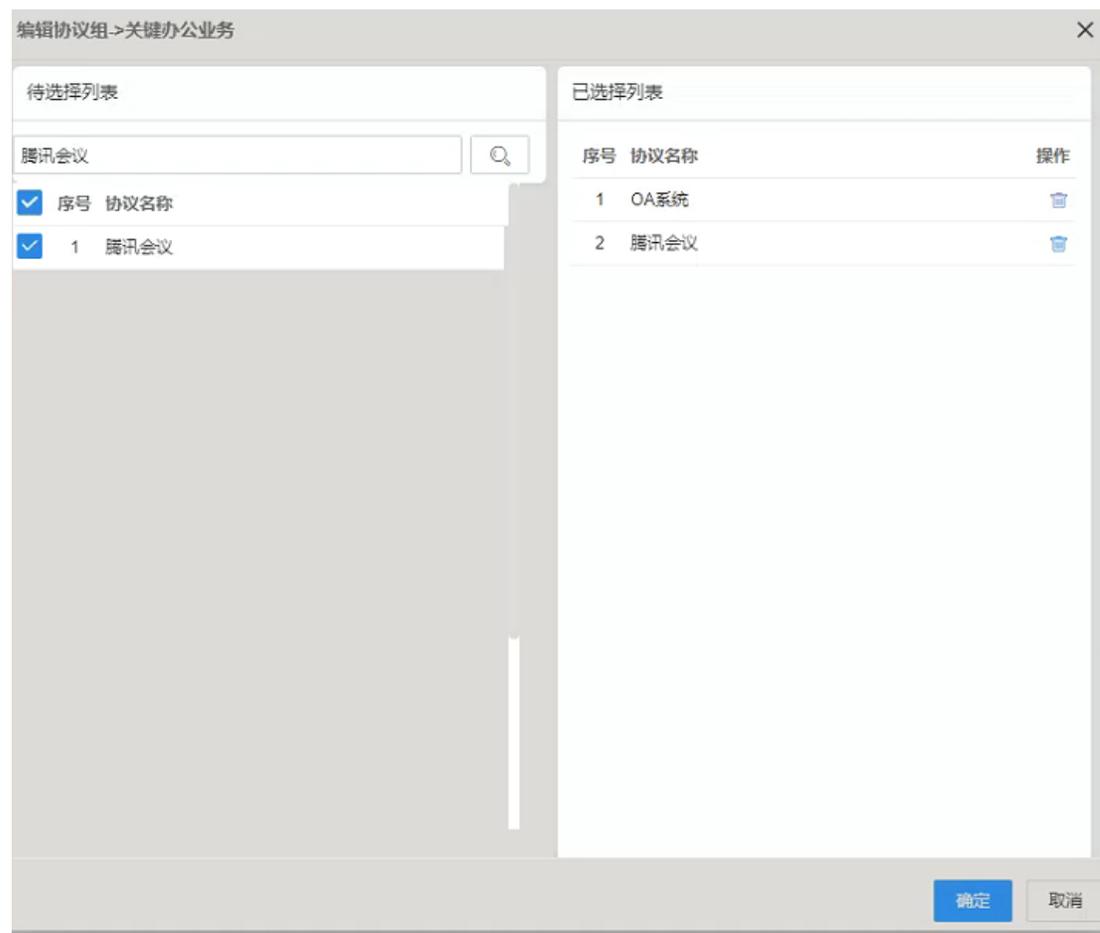
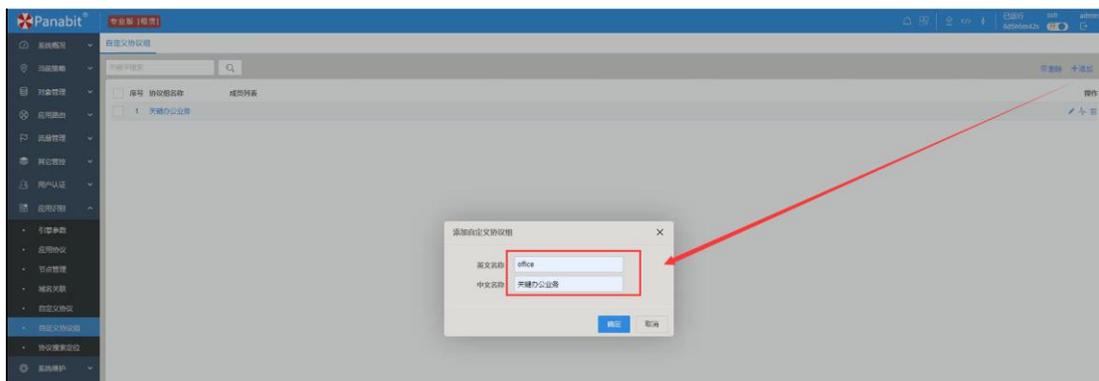
进入【应用识别】-【自定义协议】，在右上角点击【添加】按钮，“英文名称”输入“OA”，“中文名称”输入“OA系统”。再进入【域名关联】，点击【添加】按钮。选择所属协议“OA系统”，开启“跟踪host”。关联相应业务的域名域名：www.oa.com www.baidu.com



## 配置自定义协议组

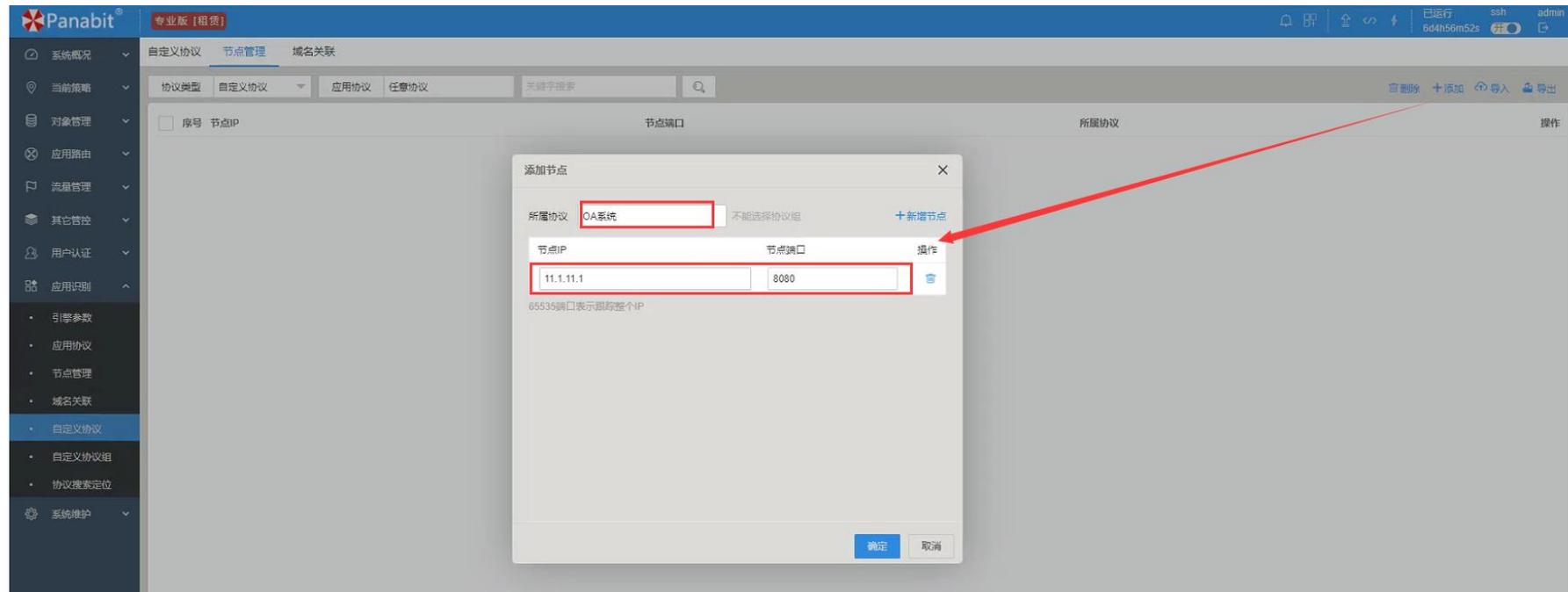
进入【应用识别】-【自定义协议组】，点击右上角【添加】，添加名称为“关键办公业务”，点击【确定】。点击“关键办公业务”右边的

在弹出的窗口选择相应的业务协议，“OA系统”、“腾讯会议”。点击【确定】



**Tips:** 该功能所创建的自定义协议组可应用于【策略路由】、【DNS管控】、【流量管理】和其他有【应用协议】选项的多个功能中。

【应用识别】 - 【自定义协议】 - 【自定义协议】 - 【节点管理】  
也可以根据IP端口来定义节点协议节点管理



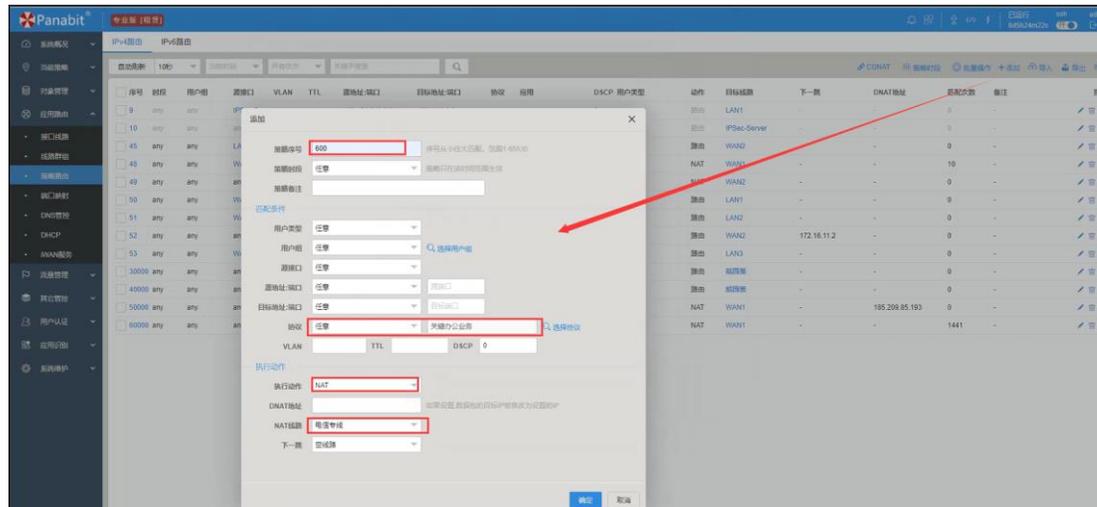
**Tips:** 自定义协议功能可以帮助用户创建当前特征库中没有的协议，主要用于一些内部应用的识别和分流操作。

## 配置策略路由

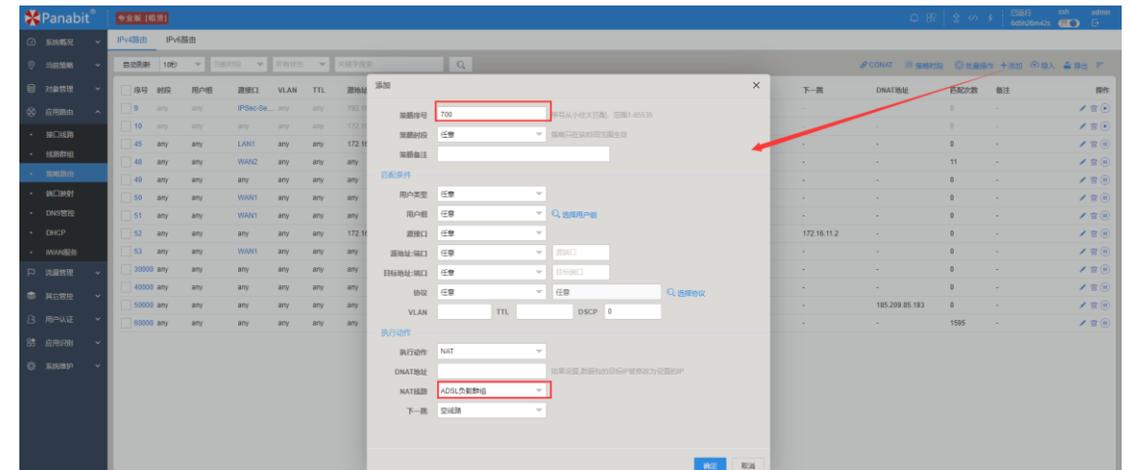
进入【应用路由】-【策略路由】-【IPv4路由】，点击右上角【添加】按钮，在弹出的窗口设置：  
关键业务保障策略：“策略序号”为“600”、“选择”为“关键办公业务”、“执行动作”为“NAT”、“NAT线路”为“电信专线”，其余默认，点击【确定】。

默认路由策略：点击【添加】按钮，在弹出的窗口设置：“策略序号”为“700”、“执行动作”为“NAT”、“NAT线路”为“ADSL负载群组”其余默认，点击【确定】，

冗余路由策略：点击【添加】按钮设置备份线路，当出现两条拨号线路都出问题时，默认走专线出去。在弹出的窗口设置：“策略序号”为“800”、“执行动作”为“NAT”、“NAT线路”为“ADSL负载群组”其余默认，点击【确定】。



配置专线策略路由



配置拨号线路策略路由

Tips:这三条策略基于优先级的不同，构成了分流策略冗余功能。



# 派网负载均衡案例配置



网卡配置

WAN设置

线路群组配置

自定义业务对象

策略路由

## 查看配置是否生效

这里以ADSL负载群组中的WAN1作为示例，匹配次数表示已有流量按照该策略传输。

检查策略是否生效，在【应用路由】-【策略路由】下的策略上能够看到匹配次数，有则代表策略生效。

也能在【系统概况】-【在线用户】中点击想要查看的IP，点击连接信息，查看分流到那条策略和线路，此处以线路WAN1做示例。

如图所示，可以看到示例【连接信息】-【接口线路】栏显示了该应用产生的流量当前走的线路，到这里，我们可以认为是分流设置成功了。

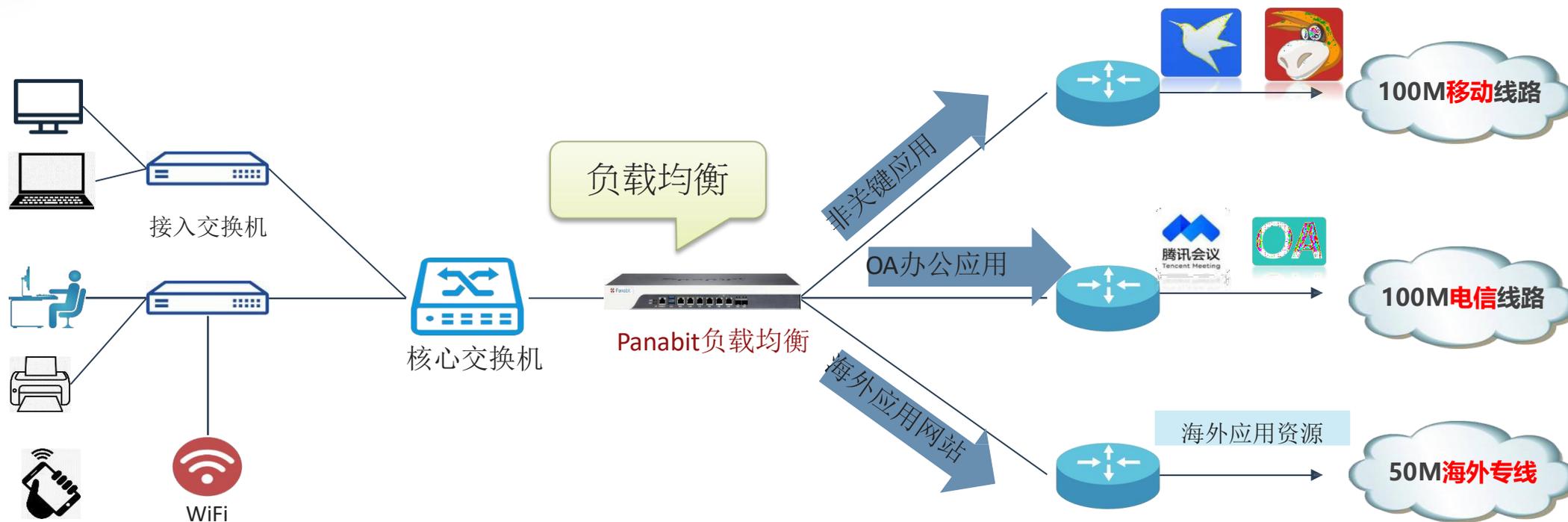
序号	名称	用户组	源接口	VLAN	TTL	源地址-端口	目标地址-端口	协议	应用	DSCP	用户类型	动作	目标线路	下一跳	DNAT地址	匹配次数	备注	操作
9	any	any	IPSec-09...	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
10	any	any	any	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
20	any	any	any	any	any		any	any	any	0	any	路由	LAN1	-	-	1	-	
45	any	any	LAN1	any	any			any	any	0	any	路由	WAN2	-	-	0	-	
46	any	any	WAN2	any	any		any	any	any	0	any	NAT	WAN1	-	-	3	-	
48	any	any	any	any	any			any	any	0	any	NAT	WAN2	-	-	0	-	
50	any	any	WAN1	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
51	any	any	WAN1	any	any			any	any	0	any	路由	LAN2	-	-	0	-	
52	any	any	any	any	any			any	any	0	any	路由	WAN2	172.16.11.2	-	0	-	
53	any	any	WAN1	any	any			any	any	0	any	路由	LAN3	-	-	0	-	
30000	any	any	any	any	any			any	any	0	any	路由	-	-	-	0	-	
40000	any	any	any	any	any			any	any	0	any	路由	-	-	-	0	-	
50000	any	any	any	any	any			any	any	0	any	NAT	WAN1	-	-	0	-	
50050	any	any	any	any	any			any	any	0	any	NAT	ADSL负载均衡	-	-	320	-	

已有匹配次数的策略

应用	协议	状态	源接口	选择	地理位置	策略路由	接口线路	时长	客户端IP	服务端IP	占用时长	上行原文	下行原文	最大包长	MSS	流量	HOST
DNS	udp	OK	IWAN1mem4	源: 192.168.50.5:37441 目: 114.114.114.114:53	114DNS.C...	50050	WAN1	1	0.00	0.00	10.96	0/1	0/1	120/231	0	120/231	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5921	114DNS.C...	50050	WAN1	1	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
DNS	udp	OK	IWAN1mem4	源: 192.168.50.5:42491 目: 114.114.114.114:53	114DNS.C...	50050	WAN1	1	0.00	0.00	14.71	0/1	0/1	120/243	0	120/243	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5920	114DNS.C...	50050	WAN1	2	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5919	114DNS.C...	50050	WAN1	3	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
WWW	tcp	OK	IWAN1mem4	源: [redacted] 目: [redacted]	美国	60000	WAN1	1483	0.05	109.59	607.72	26/630	594/594	446/404	1396	277540/23...	detectportal...
WWW	tcp	OK	IWAN1mem4	源: [redacted] 目: [redacted]	美国	60000	WAN1	1486	0.71	168.10	168.54	0/600	594/595	448/322	1396	267070/19...	detectportal...
其它HTTPS	tcp	OK	IWAN1mem4	源: [redacted] 目: [redacted]	美国	60000	WAN1	226379	1.11	194.41	195.73	84/664	881/881	780/1486	1396	133083/12..._push.servic...	

连接信息

# Panabit跨运营商线路出口的负载均衡方案



## 场景说明:

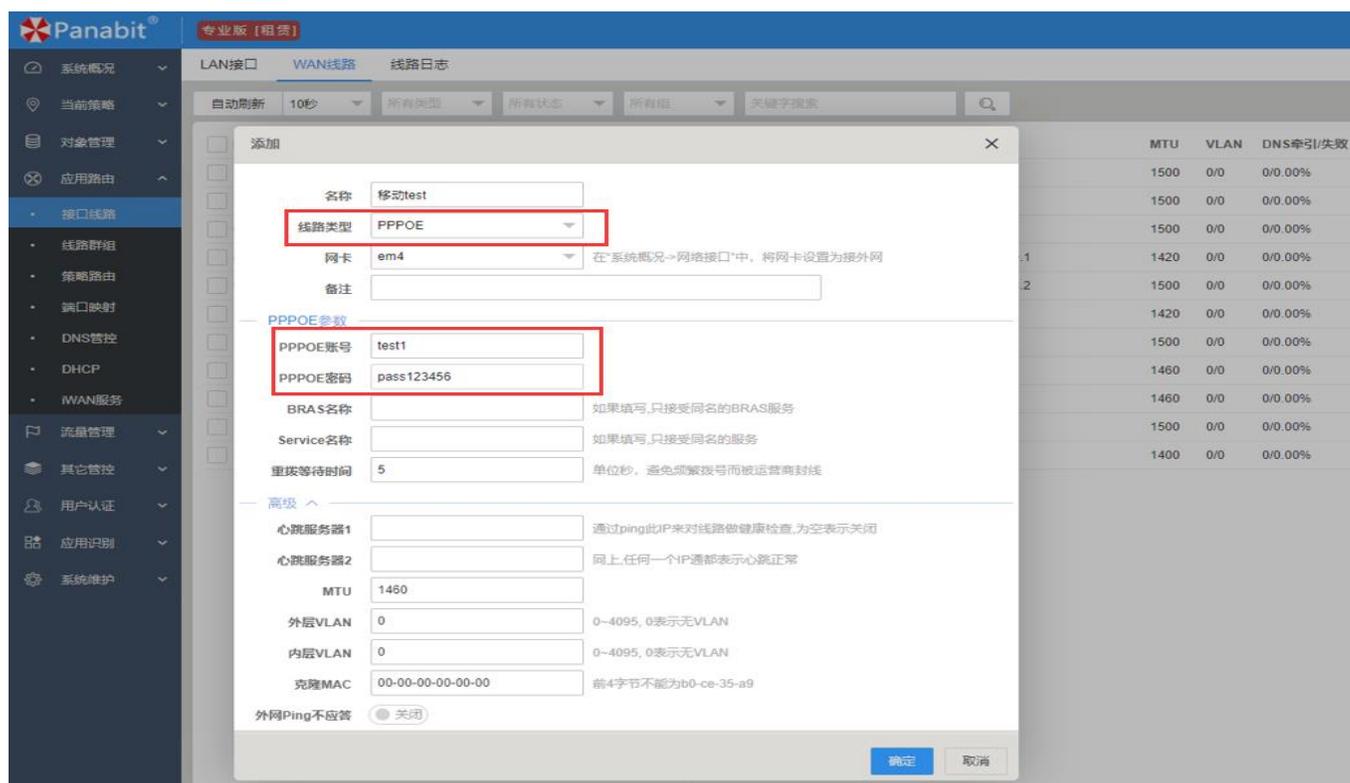
- 各运营商的网络资源和服务有区别，混合传输可能导致业务绕行，增大业务时延，影响体验。
- 购买了多个运营商线路，但当做备用线路来使用，没有发挥实用价值。
- 备用线路空闲状态时，主线跑满，经常被投诉

## 应用价值:

- 对应用自带业务测量，记录每会话客户时延，响应时延，服务时延，业务质量一目了然。
- 根据应用时延信息，结合运营商内容资源分布，快速进行网络优化，**提高客户体验。**
- 将备用线路调整为负载分担，**降低企业扩容成本。**

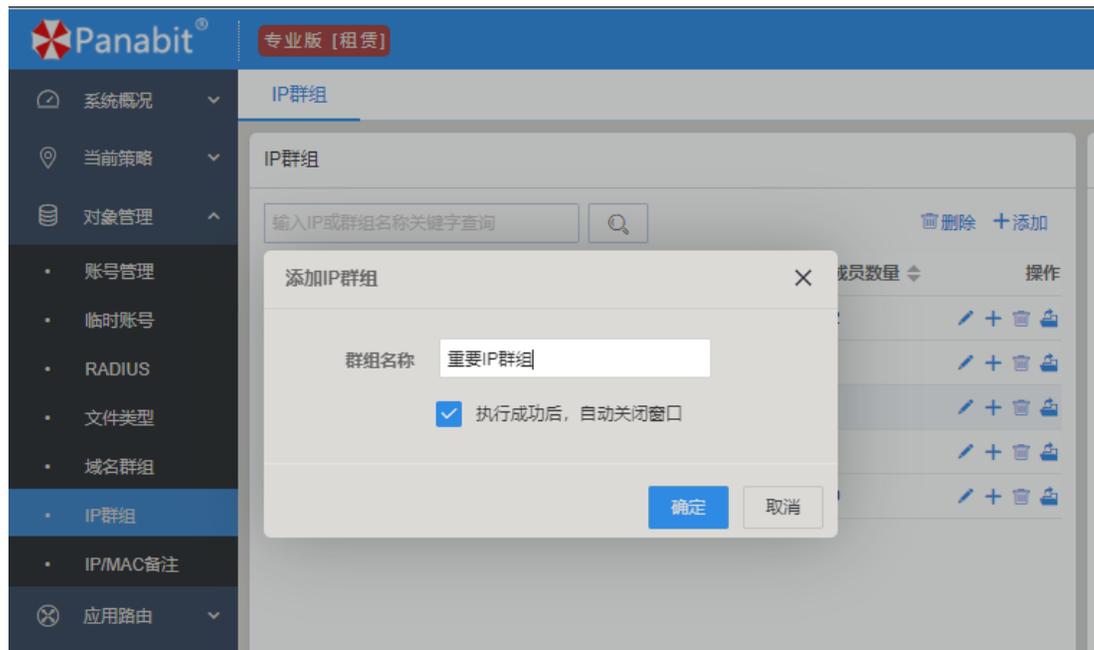
序号	配置步骤	配置详情
1	网卡配置	配置网卡方向，确认网卡用于做LAN/WAN，网桥，出口负载均衡WAN设置接外
2	WAN设置	支持多种线路方式的WAN，静态，动态，PPPoE,L2TP,自研SD-WAN（IWAN）
3	线路群组配置	设置多条线路为群组，进行负载均衡，负载均衡方式可选多种
4	自定义业务对象	基于IP，域名，应用特征的归类已方便，路由，流控策略时作为条件调用
5	策略路由	指定路由转发，支持多种条件，优先级，路由 NAT DNAT

进入【应用路由】-【线路接口】-【WAN线路】。点击右上角的【添加】，在弹出的窗口中配置，点击【线路类型】按钮可按需选择多种类型的线路，

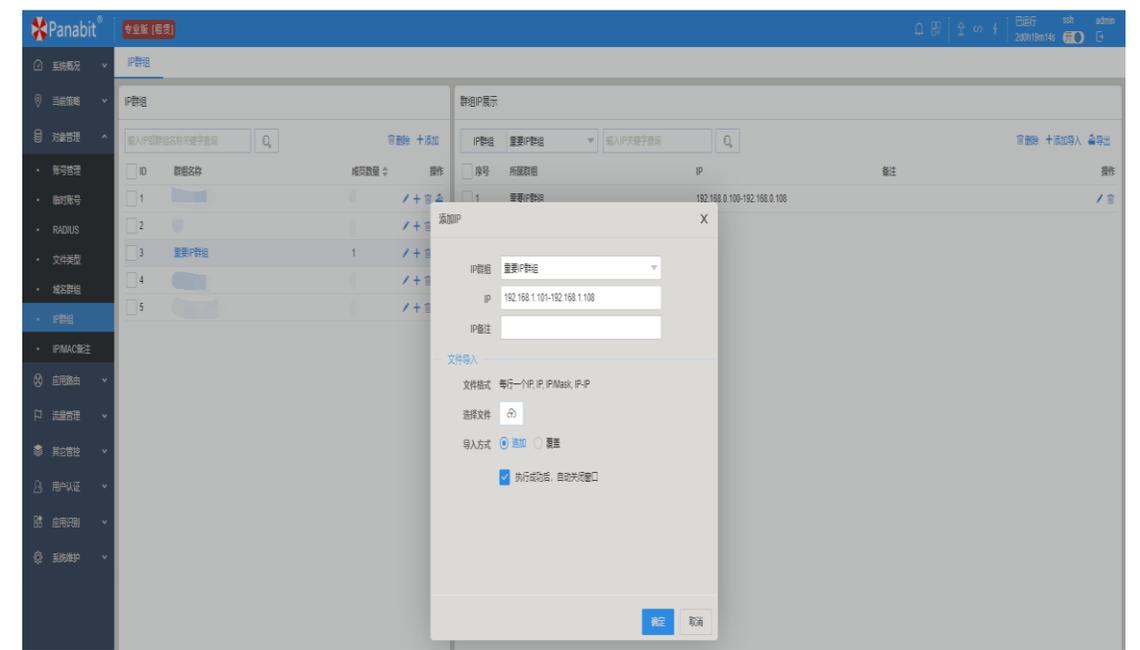


**Tips:** 同一张网卡可添加多个线路。

进入【对象管理】-【IP群组】-【添加】，输入群组名称并创建，点击【重要IP群组】，点击【添加导入】输入IP范围，点击【确定】，向组中添加IP。



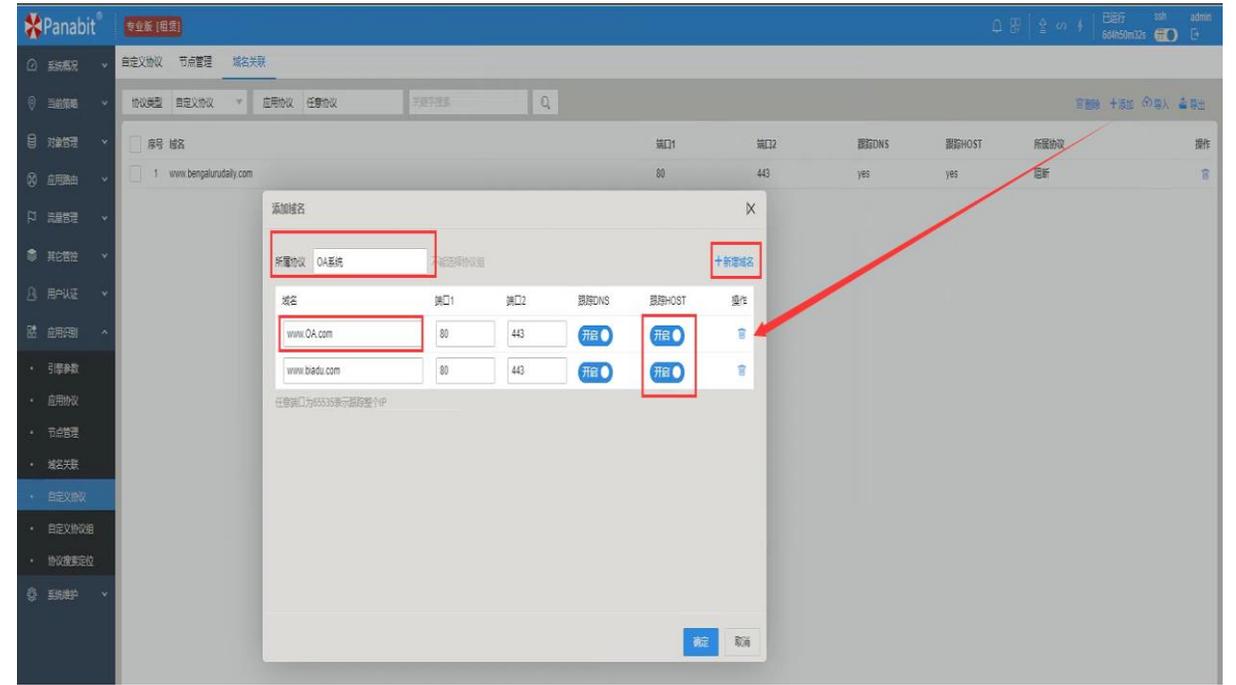
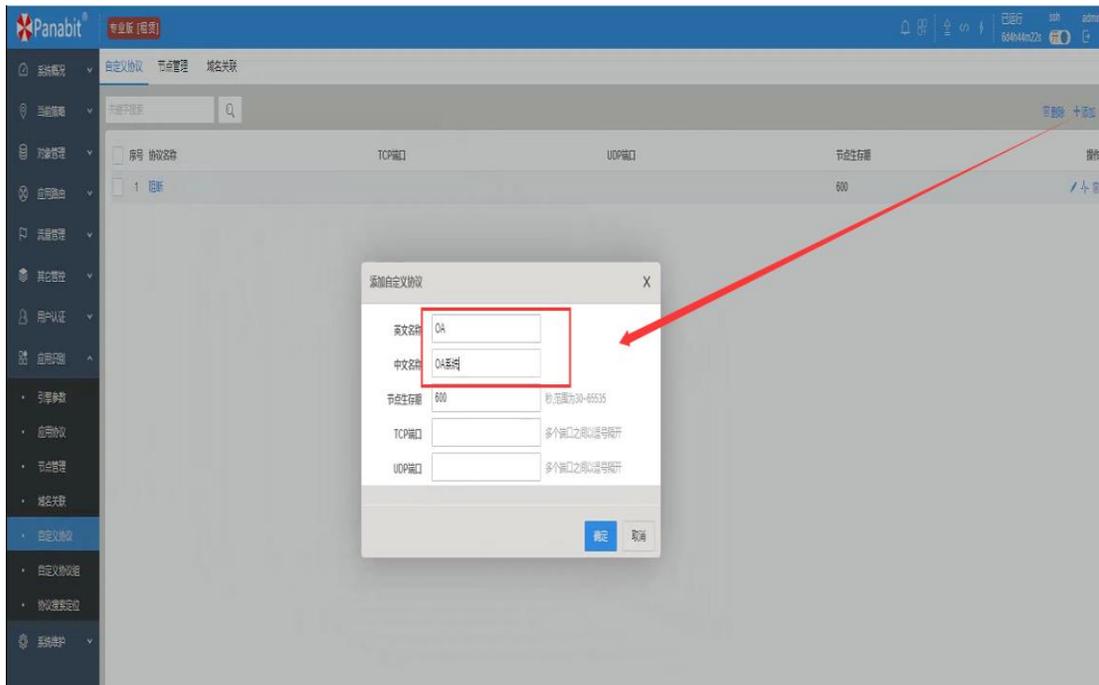
创建IP群组



配置群组IP

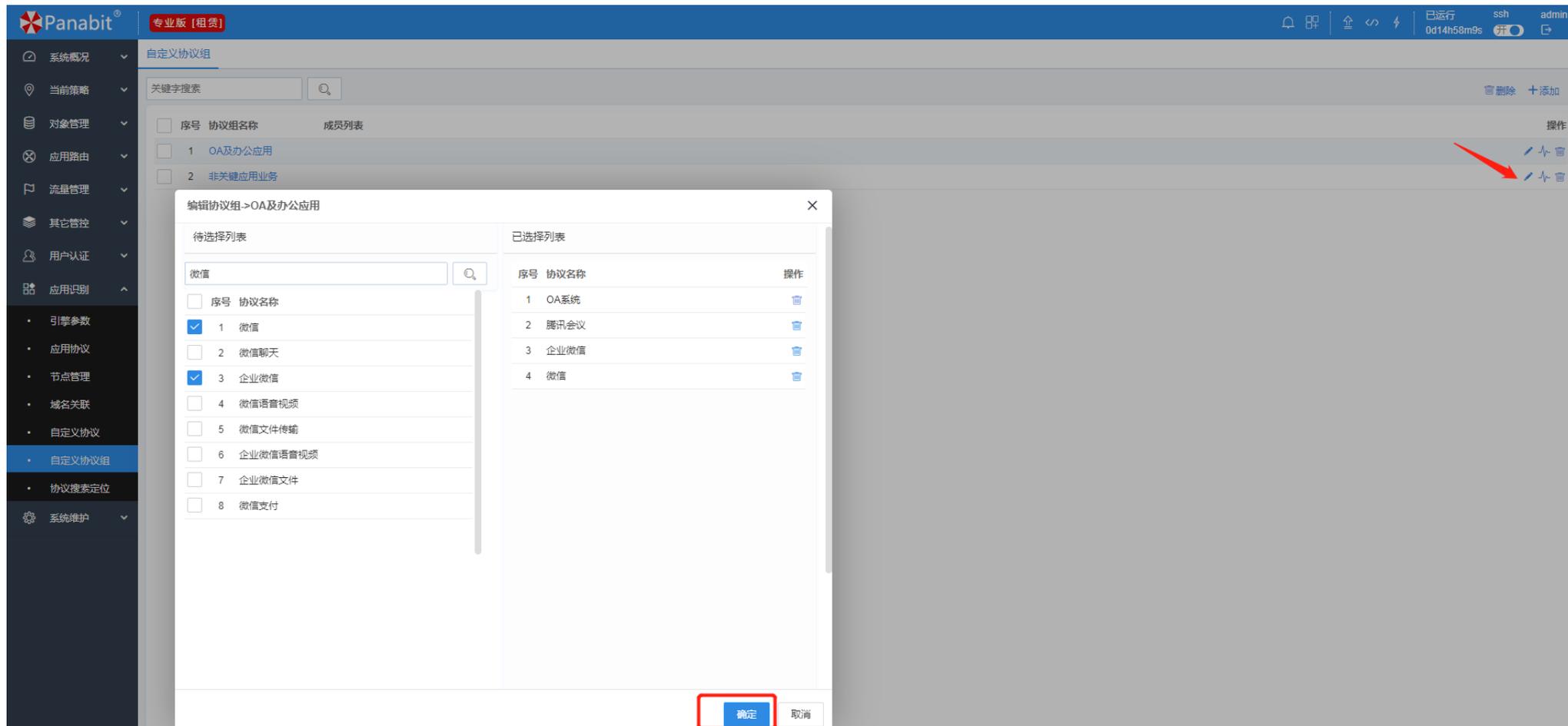
**Tips:** 【IP群组】功能所创建的对象和【自定义协议组】创建的对象一样，都可以在【流量管理】、【策略路由】、【DNS管控】、【连接控制】等流控功能下调用，比如在【流量管理】中调用该对象，可以完成对目标群组的限速、阻断流量等操作。

进入【应用识别】-【自定义协议】-【自定义协议】，在右上角点击【添加】按钮，“中文名称”输入“OA”，“中文名称”输入“OA系统”。再次进入【域名关联】和【节点管理】，点击【添加】按钮。选择所属协议“OA系统”，开启“跟踪host”。关联相应业务的域名域名：www.oa.com www.baidu.com



**Tips:** 自定义协议功能可以帮助用户创建当前特征库中没有的协议，主要用于一些内部应用的识别和分流操作。

关联海外域名，自定义应用层协议，



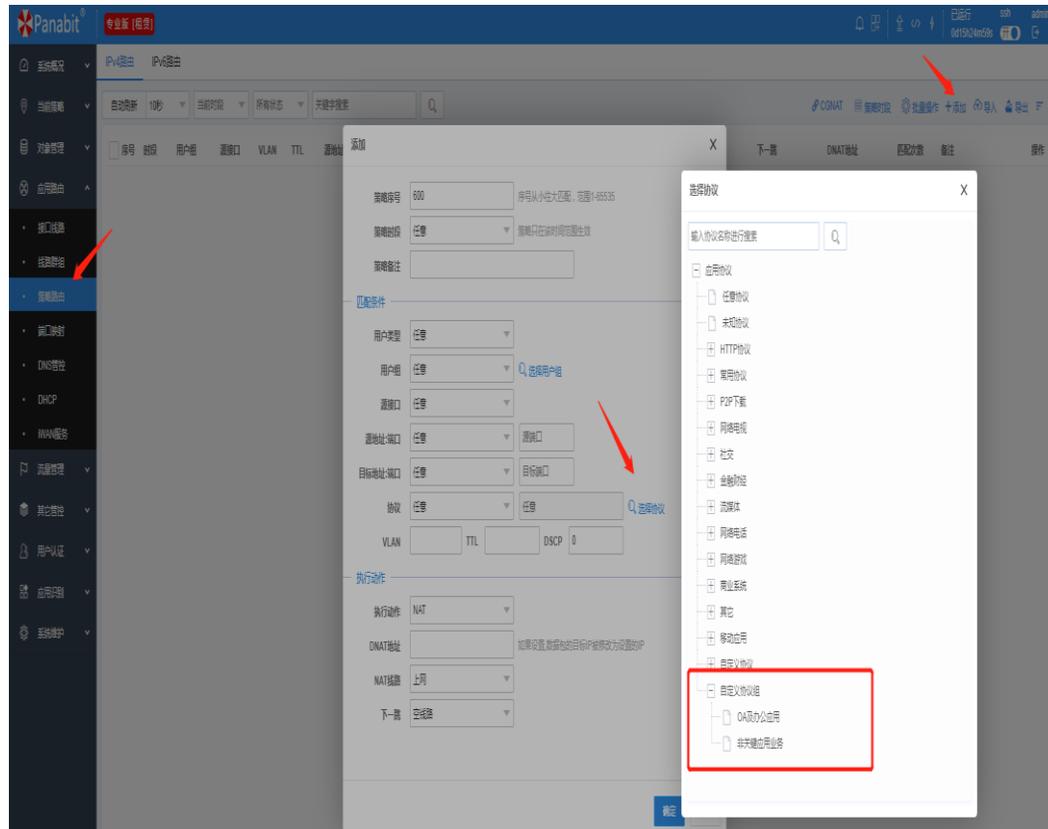
The screenshot shows the Panabit management console interface. The main content area displays the '自定义协议组' (Custom Protocol Group) configuration page. A modal window titled '编辑协议组->OA及办公应用' (Edit Protocol Group -> OA and Office Applications) is open, showing a list of protocols to be added to the group. The '待选择列表' (List to be selected) contains 8 items, with '1 微信' (WeChat) and '3 企业微信' (WeChat Work) selected. The '已选择列表' (List already selected) contains 4 items: '1 OA系统', '2 腾讯会议', '3 企业微信', and '4 微信'. A red arrow points to the '编辑' (Edit) button for the '非关键应用业务' (Non-critical application business) group in the background. The '确定' (Confirm) button in the modal is highlighted with a red box.

待选择列表	已选择列表
<input type="checkbox"/> 序号 协议名称	1 OA系统
<input checked="" type="checkbox"/> 1 微信	2 腾讯会议
<input type="checkbox"/> 2 微信聊天	3 企业微信
<input checked="" type="checkbox"/> 3 企业微信	4 微信
<input type="checkbox"/> 4 微信语音视频	
<input type="checkbox"/> 5 微信文件传输	
<input type="checkbox"/> 6 企业微信语音视频	
<input type="checkbox"/> 7 企业微信文件	
<input type="checkbox"/> 8 微信支付	

## 配置策略路由

进入【应用路由】-【策略路由】-【IPv4路由】，点击右上角【添加】按钮，在弹出的窗口设置：

- “策略序号”为“600”、“选择”为“关键办公业务”、“执行动作”为“NAT”、“NAT线路”为“电信专线”，其余默认，点击【确定】。
- “策略序号”为“700”、“选择”为“内网IP-重要IP群组”、“执行动作”为“NAT”、“NAT线路”为“电信专线”其余默认，点击【确定】。
- “策略序号”为“800”、“选择”为“海外加速域名”、“执行动作”为“NAT”、“NAT线路”为“海外专线”其余默认。点击【确定】。
- “策略序号”为“900”、“执行动作”为“NAT”、“NAT线路”为“移动专线”其余默认。点击【确定】。
- “策略序号”为“1000”、“执行动作”为“NAT”、“NAT线路”为“电信专线”其余默认。点击【确定】。





# 派网负载均衡案例配置



WAN设置

自定义业务对象

策略路由

## 查看配置是否生效

这里以ADSL负载群组中的WAN1作为示例，匹配次数表示已有流量按照该策略传输。

检查策略是否生效，在【应用路由】-【策略路由】下的策略上能够看到匹配次数，有则代表策略生效。

也能在【系统概况】-【在线用户】中点击想要查看的IP，点击连接信息，查看分流到那条策略和线路，此处以线路WAN1做示例。

如图所示，可以看到示例【连接信息】-【接口线路】栏显示了该应用产生的流量当前走的线路，到这里，我们可以认为是分流设置成功了。

序号	名称	用户组	源接口	VLAN	TTL	源地址-端口	目标地址-端口	协议	应用	DSCP	用户类型	动作	目标线路	下一跳	DNAT地址	匹配次数	备注	操作
9	any	any	IF54c-0a...	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
10	any	any	any	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
20	any	any	any	any	any		any	any	any	0	any	路由	LAN1	-	-	1	-	
45	any	any	LAN1	any	any			any	any	0	any	路由	WAN2	-	-	0	-	
46	any	any	WAN2	any	any		any	any	any	0	any	NAT	WAN1	-	-	3	-	
48	any	any	any	any	any			any	any	0	any	NAT	WAN2	-	-	0	-	
50	any	any	WAN1	any	any			any	any	0	any	路由	LAN1	-	-	0	-	
51	any	any	WAN1	any	any			any	any	0	any	路由	LAN2	-	-	0	-	
52	any	any	any	any	any			any	any	0	any	路由	WAN2	172.16.11.2	-	0	-	
53	any	any	WAN1	any	any			any	any	0	any	路由	LAN3	-	-	0	-	
30000	any	any	any	any	any			any	any	0	any	路由	-	-	-	0	-	
40000	any	any	any	any	any			any	any	0	any	路由	-	-	-	0	-	
50000	any	any	any	any	any			any	any	0	any	NAT	WAN1	-	-	0	-	
50050	any	any	any	any	any			any	any	0	any	NAT	ADSL负载均衡	-	-	320	-	

已有匹配次数的策略

应用	协议	状态	源接口	选择	地理位置	策略路由	接口线路	时长	客户时延	服务器时延	应用时延	上行报文	下行报文	最大包长	MSS	流量	HOST
DNS	udp	OK	IWAN1mem4	源: 192.168.50.5:37441 目: 114.114.114.114:53	114DNS C...	50050	WAN1	1	0.00	0.00	10.96	0/1	0/1	120/231	0	120/231	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5921	114DNS C...	50050	WAN1	1	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
DNS	udp	OK	IWAN1mem4	源: 192.168.50.5:42491 目: 114.114.114.114:53	114DNS C...	50050	WAN1	1	0.00	0.00	14.71	0/1	0/1	120/243	0	120/243	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5920	114DNS C...	50050	WAN1	2	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
ICMP	icmp	NIL	IWAN1mem4	源: 192.168.50.5:7979 目: 114.114.114.114:5919	114DNS C...	50050	WAN1	3	0.00	0.00	9.93	0/1	0/1	134/134	0	134/134	detectportal...
WWW	tcp	OK	IWAN1mem4	源: 192.168.50.5:60000 目: 192.168.50.5:80	美国	60000	WAN1	1483	0.05	109.59	807.72	25/630	594/594	446/404	1396	277540/23	detectportal...
WWW	tcp	OK	IWAN1mem4	源: 192.168.50.5:60000 目: 192.168.50.5:80	美国	60000	WAN1	1486	0.71	168.10	168.54	0/600	594/595	448/322	1396	267070/19	detectportal...
其它HTTPS	tcp	OK	IWAN1mem4	源: 192.168.50.5:60000 目: 192.168.50.5:443	美国	60000	WAN1	226379	1.11	194.41	195.73	84/664	881/881	780/1486	1396	133083/12	push.servic...

连接信息



04

## 负载均衡常见问题



## 派负载均衡类型的匹配方式

源地址+目的地址：以数据报文的源地址和目的地址为条件进行计算；

地址+端口：以数据报文的源端口和目的端口为条件进行计算；

源地址：以数据报文的源地址为条件进行计算；

源地址+源端口：以数据报文的源地址和源端口为条件进行计算；

目的地址：以数据报文的为目的地址为条件进行计算；

目的地址+目的端口：以数据报文的为目的地址和目的端口为条件进行计算；

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 负载类型选择的属性越多，各条线路负载越均衡，以上各类负载类型方式互补，没有优劣之划分，建议如下：涉及到网银，需要校验地址的应用可使用“源地址”或“目的地址”的负载类型；涉及网络下载或非实时性的应用可使用“地址+端口”的类型；涉及敏感度比较高比如游戏的应用建议使用“源地址+目的地址”的负载方式。

名称	WANGroup1
类型	源地址+目的地址
	源地址+目的地址
	源目地址+源目端口
	源地址
	源地址+源端口
	目的地址
	目的地址+目的端口

确定

取消



## 派负载均衡类型的匹配方式

新增最大空闲带宽负载方式：当检测到当前线路群组内有比较空闲的线路时，新建的连接会新建在这条低负载的线路上

编辑1 ×

名称

类型

- 源地址+目的地址
- 源目地址+源目端口
- 源地址
- 源地址+源端口
- 目的地址
- 目的地址+目的端口
- 最大空闲带宽



# 基于域名的路由如何实现的



基于域名的路由，本质上是要将域名转换成IP地址  
 从原理上我们跟踪的是DNS解析结果以及包含HOST字段的IP进行记录。  
 再将这些网站定义成协议，域名映射到IP作为协议识别的手段在进行策略路由的指向

## DNS对应IP关系

Source	Destination	Protocol	Length	Info
2-05-13 14:47:14.135197	192.168.8.38	DNS	71	Standard query 0x1e41 A wx.qqlogo.cn
2-05-13 14:47:14.146271	114.114.114.114	DNS	439	Standard query response 0x1e41 A wx.qqlogo.cn CNAME cw.x.qqlogo.cn A 101.91.37.22
2-05-13 14:47:15.723451	192.168.8.38	DNS	70	Standard query 0x9af3 A www.qq.com
2-05-13 14:47:15.727862	114.114.114.114	DNS	467	Standard query response 0x9af3 A www.qq.com CNAME ins-r23tsuuf.ias.tencent-clc
2-05-13 14:47:17.078337	192.168.8.38	DNS	79	Standard query 0xf8f3 A pacaio.match.qq.com
2-05-13 14:47:17.075584	114.114.114.114	DNS	476	Standard query response 0xf8f3 A pacaio.match.qq.com CNAME ins-gwqy79ih.ias.te
2-05-13 14:47:17.103315	192.168.8.38	DNS	74	Standard query 0xcce6 A mat1.gting.com
2-05-13 14:47:17.111073	114.114.114.114	DNS	444	Standard query response 0xcce6 A mat1.gting.com CNAME mat1.gting.com.cloud.tc.
2-05-13 14:47:17.122135	192.168.8.38	DNS	71	Standard query 0xc8f9 A joke.qq.com
2-05-13 14:47:17.127878	114.114.114.114	DNS	468	Standard query response 0xc8f9 A joke.qq.com CNAME ins-7byizn7i.ias.tencent-cl
2-05-13 14:47:17.133628	114.114.114.114	DNS	394	Standard query response 0xeef5 A vm.gting.cn CNAME vm.gting.cn.cloud.tc.qq.com
2-05-13 14:47:17.133624	114.114.114.114	DNS	75	Standard query 0x7e22 A inews.etimg.com
2-05-13 14:47:17.171120	192.168.8.38	DNS	75	Standard query 0x7e22 A inews.etimg.com

Answers	RRs: 2
Authority RRs	2
Additional RRs	6
Queries	6
> sqt.gting.cn: type A, class IN	
Answers	
> sqt.gting.cn: type A, class IN, addr: 113.96.208.119	
> sqt.gting.cn: type A, class IN, addr: 183.3.235.49	
Authoritative nameservers	
> sqt.gting.cn: type NS, class IN, ns ns-tel2.qq.com	
> sqt.gting.cn: type NS, class IN, ns ns-tel1.qq.com	
Additional records	
> ns-tel2.qq.com: type A, class IN, addr 123.151.66.83	
> ns-tel2.qq.com: type A, class IN, addr 58.60.10.100	

## HOST对应IP关系

```

Frame 4229: 1081 bytes on wire (8648 bits), 1081 bytes captured (8648 bits) on interface \Device\NPF_{6FA8FDA5-B9F1-4425-8E84-C0787B4678AF}, id 0
Ethernet II, Src: IntelCor_46:bf:c7 (5c:51:4f:46:bf:c7), Dst: b0:a2:06:2f:00:30 (b0:a2:06:2f:00:30)
Internet Protocol Version 4, Src: 192.168.8.26, Dst: 101.91.5.71
Transmission Control Protocol, Src Port: 8149, Dst Port: 80, Seq: 1, Ack: 1, Len: 1027
Hypertext Transfer Protocol
  POST /q.cgi HTTP/1.1\r\n
  Host: www.qq.com\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)\r\n
  Accept: */*\r\n
  Content-Type: application/octet-stream\r\n
  Content-Length: 834\r\n
  \r\n
[Full request URI: http://www.qq.com/q.cgi]
[HTTP request 1/1]
0040 69 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 i HTTP/1.1..Host
0050 3a 20 77 77 77 2e 71 71 2a 63 6f 6d 0d 0a 55 73 : www.qq.com..Us
0060 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0070 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c a/4.0 (compatibl
0080 65 3b 20 4d 53 49 45 20 38 2e 30 3b 20 57 69 6e e; MSIE 8.0; Win
0090 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 54 72 69 dows NT 6.1; Tri
00a0 64 65 6e 74 2f 34 2e 30 29 0d 0a 41 63 63 65 70 dent/4.0)..Accep
00b0 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74 65 6e 74 2d t: */*.. Content-

```

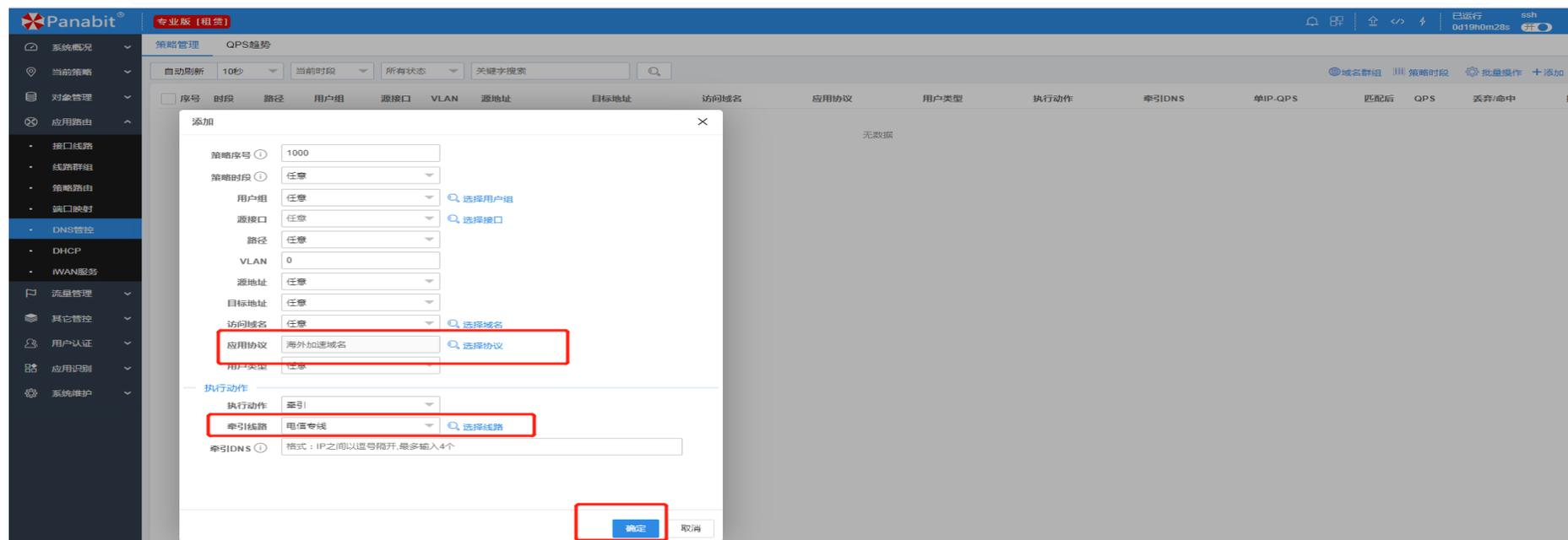


# 域名路由卡顿解决方法



域名分流后卡顿的解决方法：从原理上我们跟踪的是DNS解析结果，以www.qq.com为例，如果我们使用电信DNS来解析，那么解析出来的IP地址肯定是电信的。策略路由将这个域名分流到了联通线路，就会出现绕路访问的情况，我们在打开www.qq.com的时候，就会从联通线路去访问一个在电信上的服务器，这样跨运营商的访问速度肯定比本运营商访问慢甚至严重一些会出现卡顿现象。不过不用担心，在这样的情况下Panabit同样会有解决方案。

我们将这些要分流的域名，让它们通过联通的DNS来解析就行了，Panabit上只需要再加一条DNS管控策略。



## 拨测，主动探测业务质量

参数设置 网站列表

自动刷新	10秒	排序方式	默认排序	端口		关键字搜索	<input type="text"/>	<input type="button" value="Q"/>	<input type="button" value="导入"/>	<input type="button" value="导出"/>	<input type="button" value="+ 添加"/>	<input type="button" value="删除"/>	<input type="button" value="列表"/>	<input type="button" value="卡片"/>
<input type="checkbox"/>	序号	网址	端口	备注	线路1 <sup>i</sup>	线路2 <sup>i</sup>	线路3 <sup>i</sup>	线路4 <sup>i</sup>	推荐路由线路	操作				
<input type="checkbox"/>	1	www.yuketang.cn	443	雨课堂1	电信 13.06 / 3.85 / ...	联通 8.39 / 3.77 / ...	移动 9.13 / 4.41 / ...	教育 11.70 / 3.82 / ...		状态   编辑   删除				
<input type="checkbox"/>	2	xuetangx.com	443	雨课堂2	电信 12.85 / 3.90 / ...	联通 11.32 / 4.08 / ...	移动 9.13 / 4.20 / ...	教育 8.01 / 3.92 / ...		状态   编辑   删除				
<input type="checkbox"/>	3	tx-xuetangx.push.y...	443	雨课堂3	电信 13.36 / 9.88 / ...	联通 9.86 / 9.61 / ...	移动 13.98 / 9.66 / ...	教育 15.78 / 10.47 / ...		状态   编辑   删除				
<input type="checkbox"/>	4	www.wanfangdata....	443	万方	电信 1581.09 / 5.0... / ...	联通 1581.07 / 4.9... / ...	移动 1581.09 / 5.0... / ...	教育 1581.07 / 5.1... / ...		状态   编辑   删除				
<input type="checkbox"/>	5	www.cnki.net	443	知网	电信 86.83 / 15.63... / ...	联通 86.16 / 14.93... / ...	移动 86.16 / 15.32... / ...	教育 85.99 / 14.93... / ...		状态   编辑   删除				
<input type="checkbox"/>	6	www.baidu.com	443	百度	电信 10.56 / 3.07 / ... / ...	联通 10.74 / 3.11 / ... / ...	移动 5.72 / 3.09 / ... / ...	教育 9.11 / 3.81 / ... / ...		状态   编辑   删除				
<input type="checkbox"/>	7	panabit.com	443	派网官网	电信 21.85 / 14.93... / ...	联通 21.42 / 14.35... / ...	移动 1086.03 / 14... / ...	教育 1487.03 / 16... / ...		状态   编辑   删除				
<input type="checkbox"/>	8	qq.com	443	腾讯	电信 43.16 / 25.66... / ...	联通 23.82 / 7.46 / ... / ...	移动 1837.56 / 37... / ...	教育 1681.36 / 24... / ...		状态   编辑   删除				



2022

可视化网络领导者

THANK YOU