内网故障定位及业务质量感知

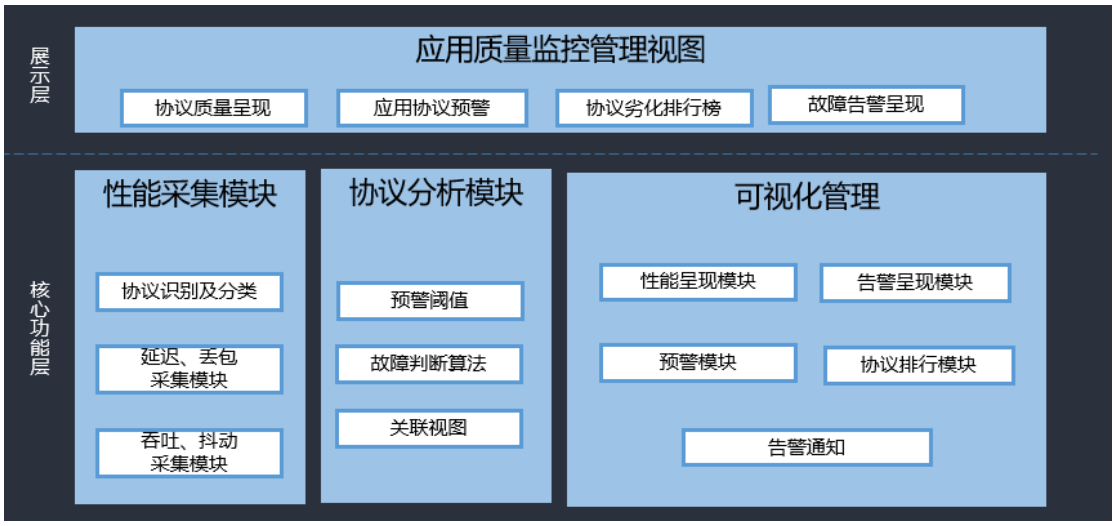
1 应用场景

政府和企业网络的工作状态正常与否，直接影响到政府和企业业务的正常开展。所以对于政企用户来说，网络的运维工作事关重大。

目前政府和企业的网络中经常出现以下问题：

- 关键业务质量无法实时监测，无法感知业务性能指标的异常；
- 当网络出现问题时，故障无法快速定位，排障往往需要消耗大量时间；
- 出了问题运维成为“背锅侠”；

2 功能模块简述



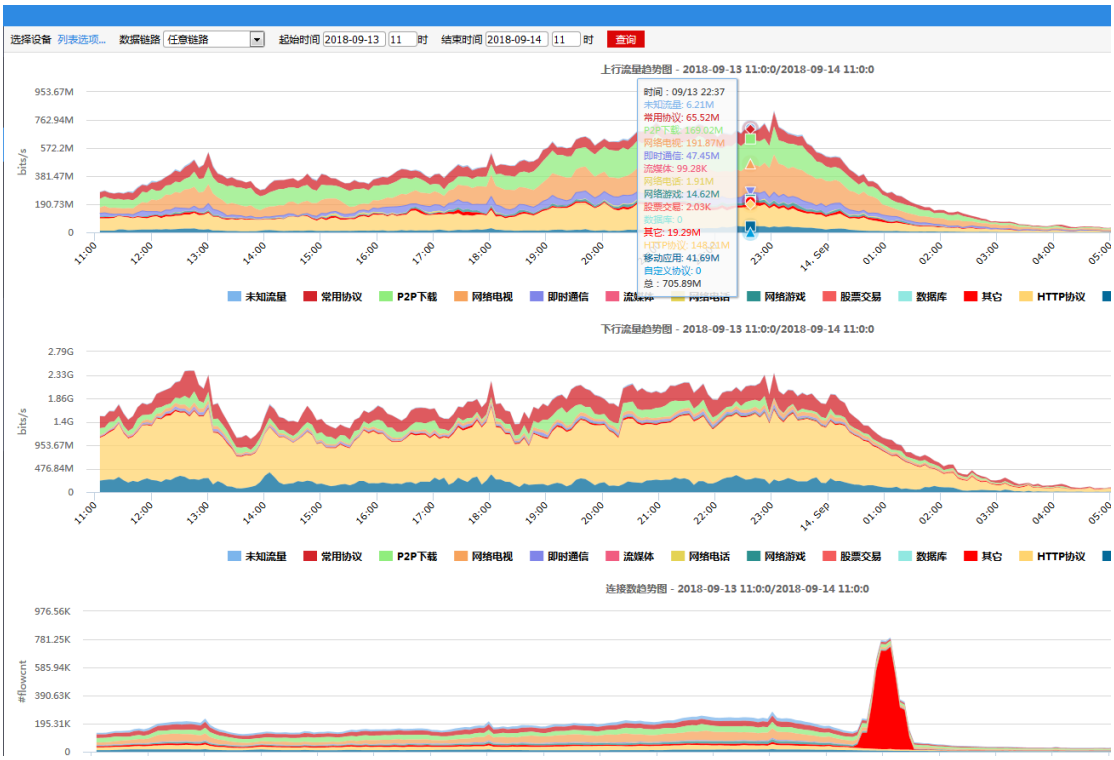
Panabit 提供的网络业务质量感知系统分为性能采集模块、协议分析模块及可视化管理模块几个部分。和传统网络性能感知系统不同的是，原有性能感知系统，大多只能做到基于三层及以下协议的网络性能感知，对于业务缺乏感测能力。

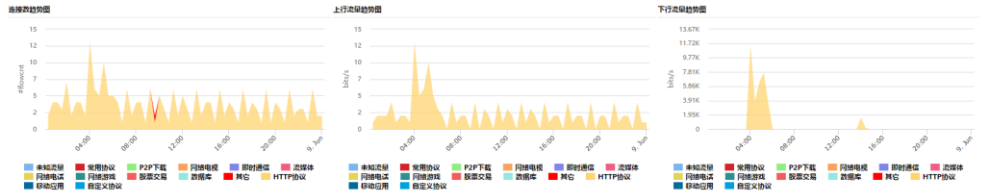
Panabit 基于七层应用识别的深入挖掘能力，将性能评估从网络层延伸到应用层，从上到下剖析网络故障，让网络问题应用问题无所遁形。

3 方案价值

1、网络故障回溯，还原一切真相

Panabit 具备强大的性能处理单元，能够 1:1 记录和还原网络中发生每一件事。它可以完整记录每一条会话信息的协议类型、接口、访问时间、连接时间、源地址、目的地址、NAT 地址、用户账号、域名信息、上下行流量、所属运营商、地理位置等信息。这就为故障回溯提供了最真实有效的依据，让一切只要发生过的问题都有迹可寻。





序号	源IP	连接数	上行流量	下行流量
1	202.118.239.104	296	39.42K	2.99M
2	172.17.104.169	295	39.04K	3.07M
3	219.217.229.37	295	38.41K	3.1M
4	202.118.247.219	295	38.41K	2.82M
5	172.27.62.240	295	38.56K	3.68M
6	202.118.234.198	289	38.54K	3.15M
7	172.17.253.81	223	28.72K	1.28M
8	202.118.240.163	186	25.21K	3.62M
9	219.217.251.34	182	24.43K	3.11M
10	219.217.239.86	177	21.4K	3.89M
11	202.118.234.146	170	23.04K	3M
12	172.27.72.22	169	23.7K	3.75M
13	172.17.132.41	164	21.92K	2.56M
14	202.118.244.113	152	20.45K	3.05M
15	172.27.72.165	151	20.16K	2.47M
16	172.17.13.43	151	21.04K	3.22M
17	210.46.70.18	147	19.39K	2.4M
18	172.17.51.219	142	19.04K	2.5M
19	202.118.246.157	140	18.53K	1.17M
20	219.217.238.130	135	18.27K	2.06M
21	202.118.230.155	133	17.64K	1.5M
22	172.17.253.141	126	16.51K	1.53M
23	172.17.25.20	120	16.03K	2.22M
24	172.17.12.81	117	15.88K	2.74M
25	202.118.244.245	111	13.87K	584.64K
26	172.17.132.63	107	14.26K	1.67M
27	172.17.51.108	106	13.48K	329.69K
28	172.17.253.117	106	14.52K	2.98M
29	219.217.236.222	104	13.36K	661.12K
30	219.217.239.222	103	12.98K	615.83K
31	219.217.237.50	103	13.24K	615.01K
32	202.118.240.141	102	13.49K	868.87K
33	219.217.248.205	101	12.73K	580.25K
34	202.118.229.188	100	11.7K	661.09K
35	219.217.239.69	100	12.86K	686.51K
36	172.27.251.45	99	13K	1.29M
37	172.27.76.248	98	14K	3.23M
38	202.118.231.68	96	13.6K	2.96M
39	202.118.238.165	95	12.11K	921.5K
40	219.217.239.35	90	12.24K	1.5M
41	219.217.236.98	86	22.8K	1.35M
42	202.118.227.25	86	11.98K	1.25M
43	219.217.250.192	85	11.23K	856.72K
44	219.217.234.4	76	10.34K	1.4M
45	202.118.246.165	73	9.45K	599.92K
46	202.118.232.10	72	9.33K	553.69K
47	172.17.164.68	72	10.25K	2.62M
48	172.17.253.112	72	9.96K	2.15M
49	202.118.236.118	67	8.83K	631.87K
50	202.118.239.84	59	7.82K	673.96K

序号	目标IP	连接数	上行流量	下行流量
1	23.234.51.75	1518	203.76K	18.13M
2	23.234.51.145	1080	144.7K	18.91M
3	23.234.51.35	893	124.98K	16.75M
4	23.234.51.123	759	100.48K	9.12M
5	23.234.51.25	737	99.82K	14.21M
6	23.234.51.42	702	90.67K	8.06M
7	23.234.13.64	691	94.62K	10.4M
8	23.234.51.155	555	75.81K	9.98M
9	23.234.13.91	445	57.7K	4.44M

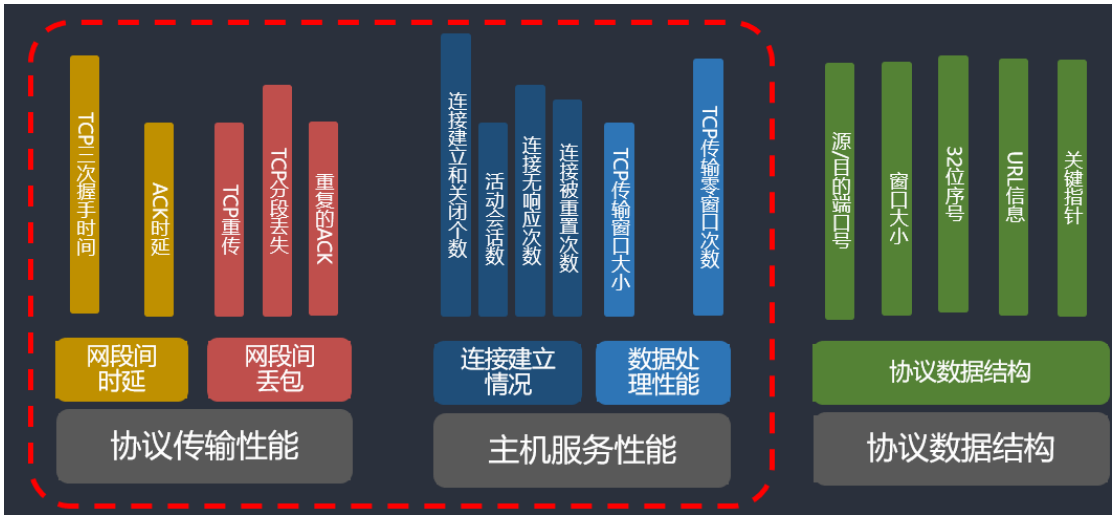
序号	协议名称	连接数	上行流量	下行流量
1	WWW	7359	992.55K	110.01M
2	SYN_ACK	21	0	0

如上图所示，Panabit 有效的记录和还原了一次典型的网络故障。可以看到虽然网络的流量不大，但是连接数已经将政企网络防火墙的连接数消耗完，导致政企网络瘫痪。通过对 1:1 会话的记录和还原，可以快速找到问题所在。

2、网络业务性能感知，故障快速定位

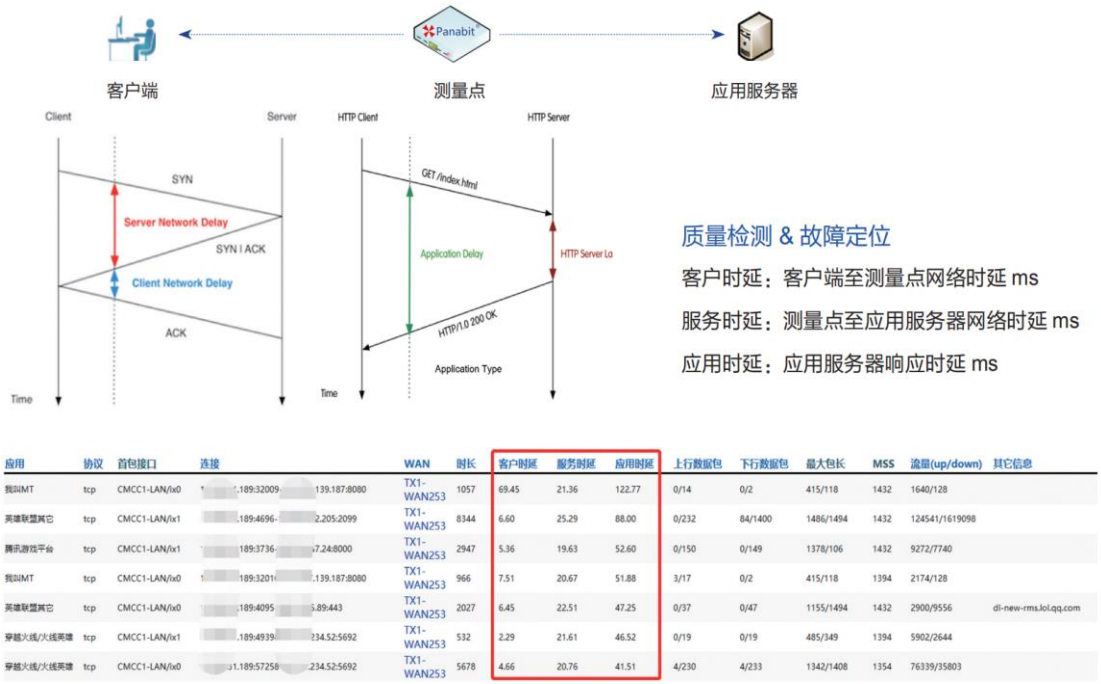
Panabit 的网络业务性能感知系统对比传统网络性能感知系统，在感知的深度、广度上都有很大提升。

首先，在深度上对比网络层性能检测系统，Panabit 检测的目标是会话级的，面向的是七层的应用。看到的更接近网络中实际发生的真相。除了可以识别出应用协议数据结构，还能看到应用协议的交互流程。



其次，在广度上可以实现单个协议时延、抖动等业务性能指标在时间维度、地区维度上的查询。可以实现多个协议和用户的交叉查询，监测异常情况，上报预警或告警。

Panabit 可以区分政企诊疗系统中每条业务的“客户侧时延”、“服务响应时延”和“应用时延”。



应用	协议	首包接口	连接	WAN	时长	客户时延	服务时延	应用时延	上行数据包	下行数据包	最大包长	MSS	流量(up/down)	其它信息
我叫MT	tcp	CMCC1-LAN/ix0	1[redacted].189:32009[redacted].139.187:8080	TX1-WAN253	1057	69.45	21.36	122.77	0/14	0/2	415/118	1432	1640/128	
英雄联盟其它	tcp	CMCC1-LAN/ix1	[redacted].189:4696-[redacted].2.205:2099	TX1-WAN253	8344	6.60	25.29	88.00	0/232	84/1400	1486/1494	1432	124541/1619098	
腾讯游戏平台	tcp	CMCC1-LAN/ix1	[redacted].189:3736-[redacted].7.24:8000	TX1-WAN253	2947	5.36	19.63	52.60	0/150	0/149	1378/106	1432	9272/7740	
我叫MT	tcp	CMCC1-LAN/ix0	1[redacted].189:3201[redacted].139.187:8080	TX1-WAN253	966	7.51	20.67	51.88	3/17	0/2	415/118	1394	2174/128	
英雄联盟其它	tcp	CMCC1-LAN/ix0	[redacted].189:4095-[redacted].89:443	TX1-WAN253	2027	6.45	22.51	47.25	0/37	0/47	1155/1494	1432	2900/9556	dl-new-rms.lol.qq.com
穿越火线/火线英雄	tcp	CMCC1-LAN/ix1	[redacted].189:4939-[redacted]34.52:5692	TX1-WAN253	532	2.29	21.61	46.52	0/19	0/19	485/349	1394	5902/2644	
穿越火线/火线英雄	tcp	CMCC1-LAN/ix0	[redacted]1.189:57258-[redacted]234.52:5692	TX1-WAN253	5678	4.66	20.76	41.51	4/230	4/233	1342/1408	1354	76339/35803	

客户侧时延：指客户内网到 Panabit 的时延；如果此时延大，基本可以将问题定位在内网中毒或者内网网络设备故障等问题。

服务器响应时延：指业务在服务器上停留和响应的时延；如果此时延过大，则说明提供业务的服务器负载或者故障等问题。

应用时延：指业务经过 Panabit，从服务器上返回的时延；如果此时延过大，而服务时延很小，则说明是运营商网络侧出现问题。

区分这些的好处是，当出现网络和业务问题时，可以依据此功能快速定位问题的出处，让问题定位更有针对性，更有效率。