2022

可视化网络领导者

实战--NTM全数据留存在校园网的应用

北京派网软件有限公司

目 录

01

NTM在多校区智能遥测应用

场景一：分校区数据采集+分析

在网络维护的过程中，有时候需要Wireshark抓包分析。例如：分校区某个公寓楼里面的数据包，进行某个IP的故障定位。

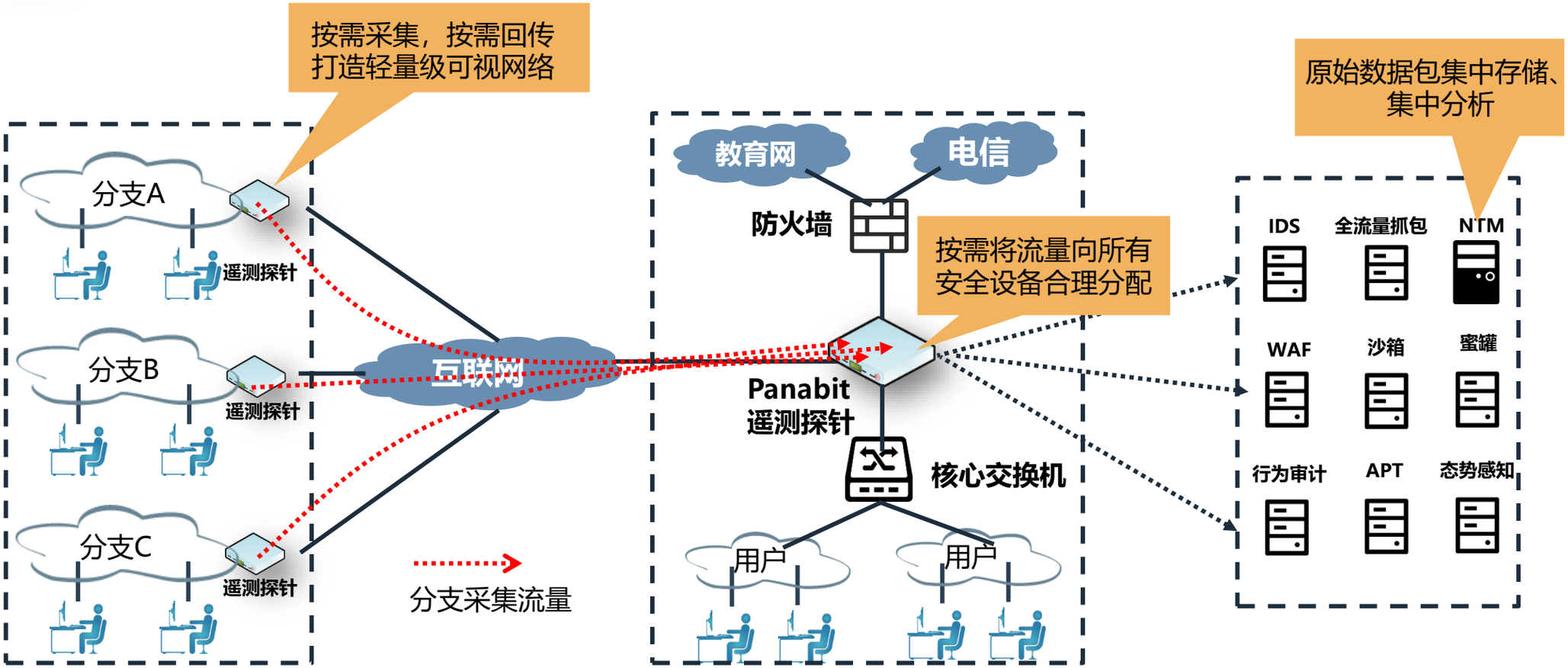
以往操作

需要先到分校区，然后再到公寓楼，通过Wireshark进行抓包分析。抓包过程中，会产生大量“垃圾”数据包。

遥测操作

通过遥测功能，无论人在哪里，都可以将分校区的某些数据“抓包”到总校区进行NTM分析。而且是剔除干扰，基于“数据流”的抓包

场景一：分校区数据采集+分析



遥测探针可以组成一张遥测网络，远端的探针采集的流量可以顺利回传至总部；
总部遥测探针可以将流量按需分给所有安全设备；

Panabit应用级遥测主要特性

1. 基于应用的遥测功能；

通过Panabit DPI功能，实现把某个应用进行遥测，解决了全量数据遥测时候数据量大的问题。

2. 支持SD-WAN组网

支持SD-WAN功能，只要网关可以通，便可以实现应用遥测，解决了专线费用贵的问题。

3. 免费提供智能遥测功能

智能遥测功能为Panabit设备的标准功能，不需要购买额外的License授权。

实战：分校区某台PC，流量抓包分析

Panabit®

报文解析　报文交互　元数据　报文播放

报文显示过滤器

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	10.3.9.162	10.3.53.100	TCP	78	25292 鈥 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval
2	0.000001	10.3.9.162	10.3.53.100	TCP	78	[TCP Out-Of-Order] 25292 鈥 80 [SYN] Seq=0 Win=14600 Len=0 MSS=146
3	0.000242	10.3.53.100	10.3.9.162	TCP	78	80 鈥 25292 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_P
4	0.000243	10.3.53.100	10.3.9.162	TCP	78	[TCP Out-Of-Order] 80 鈥 25292 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
5	0.000332	10.3.9.162	10.3.53.100	TCP	70	25292 鈥 80 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TSval=2843248861 TSe
6	0.000335	10.3.9.162	10.3.53.100	TCP	70	[TCP Dup ACK 5#1] 25292 鈥 80 [ACK] Seq=1 Ack=1 Win=14848 Len=0 TS
7	0.064442	10.3.9.162	10.3.53.100	HTTP	732	GET /images/ztrrg.png HTTP/1.0
8	0.064446	10.3.9.162	10.3.53.100	TCP	732	[TCP Retransmission] 25292 鈥 80 [PSH, ACK] Seq=1 Ack=1 Win=14848
9	0.065893	10.3.53.100	10.3.9.162	TCP	70	80 鈥 25292 [ACK] Seq=1 Ack=663 Win=30336 Len=0 TSval=1600556517 T
10	0.065896	10.3.53.100	10.3.9.162	TCP	70	[TCP Dup ACK 9#1] 80 鈥 25292 [ACK] Seq=1 Ack=663 Win=30336 Len=0
11	0.074198	10.3.53.100	10.3.9.162	TCP	1518	HTTP/1.1 200 OK [TCP segment of a reassembled PDU]

> Frame 11: 1518 bytes on wire (12144 bits), 1518 bytes captured (12144 bits)

> Ethernet II, Src: 0c:da:41:49:5b:ed (0c:da:41:49:5b:ed), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1999

> Internet Protocol Version 4, Src: 10.3.53.100, Dst: 10.3.9.162

> Transmission Control Protocol, Src Port: 80, Dst Port: 25292, Seq: 1, Ack: 663, Len: 1448

```
0000    88 df 9e 39  2a 01 0c da   41 49 5b ed  81 00 07 cf      ...9*...A  I[.....
0010    08 00 45 00  05 dc de 07   40 00 3f 06  05 09 0a 03      ..E.....@  .?.....
0020    35 64 0a 03  09 a2 00 50   62 cc 04 a1  53 e3 c8 ee      5d.....Pb  ...S...
0030    81 e9 80 10  00 ed d9 bc   00 00 01 01  08 0a 5f 66      ..........  ......_f
0040    8d ed a9 78  89 1d 48 54   54 50 2f 31  2e 31 20 32      ...x..HTT  P/1.1 2
0050    30 30 20 4f  4b 0d 0a 44   61 74 65 3a  20 54 75 65      00 OK..Da  te: Tue
0060    2c 20 31 32  20 41 70 72   20 32 30 32  32 20 30 32      , 12 Apr   2022 02
0070    3a 33 37 3a  31 34 20 47   4d 54 0d 0a  53 65 72 76      :37:14 GM  T..Serv
0080    65 72 3a 20  2a 2a 2a 2a   2a 2a 2a 2a  2a 0d 0a 58      er: *****  ****..X
0090    2d 46 72 61  6d 65 2d 4f   70 74 69 6f  6e 73 3a 20      -Frame-Op  tions:
00a0    53 41 4d 45  4f 52 49 47   49 4e 0d 0a  58 2d 58 53      SAMEORIGI  N..X-XS
00b0    53 2d 50 72  6f 74 65 63   74 69 6f 6e  3a 20 31 3b      S-Protect  ion: 1;
```

通过遥测抓包，分析10.3.9.162访问内网服务器的每一个动作，便于我们进行故障定位。

实战：分校区某台PC，流量抓包分析

报文解析 | 报文交互 | 元数据 | 报文播放 | 应用

连接时间	2022-04-12 10:40:04 - 2022-04-12 10:40:04	协议	TCP
源MAC	00:50 0:99:e9	目标MAC	88:df: :2a:01
源IP:端口	10.3.9.162:25292	目标IP:端口	10. .100:80
源	Packets: 26 Bytes: 3160 Databytes: 1324	目	Packets: 30 Bytes: 32306 Databytes: 30190
TCP Flags	SYN: 4, SYN_ACK: 0, ACK: 52, FIN: 0, PSH: 0, RST: 0, URG: 0		
Status code	200	Method	GET
Host	www. edu.cn	Cookie	
Referer		X-forward	2001:da8:2 :2b61:d9f7
User-Agent		URL	/images/ztrrg.png HTTP/1.0

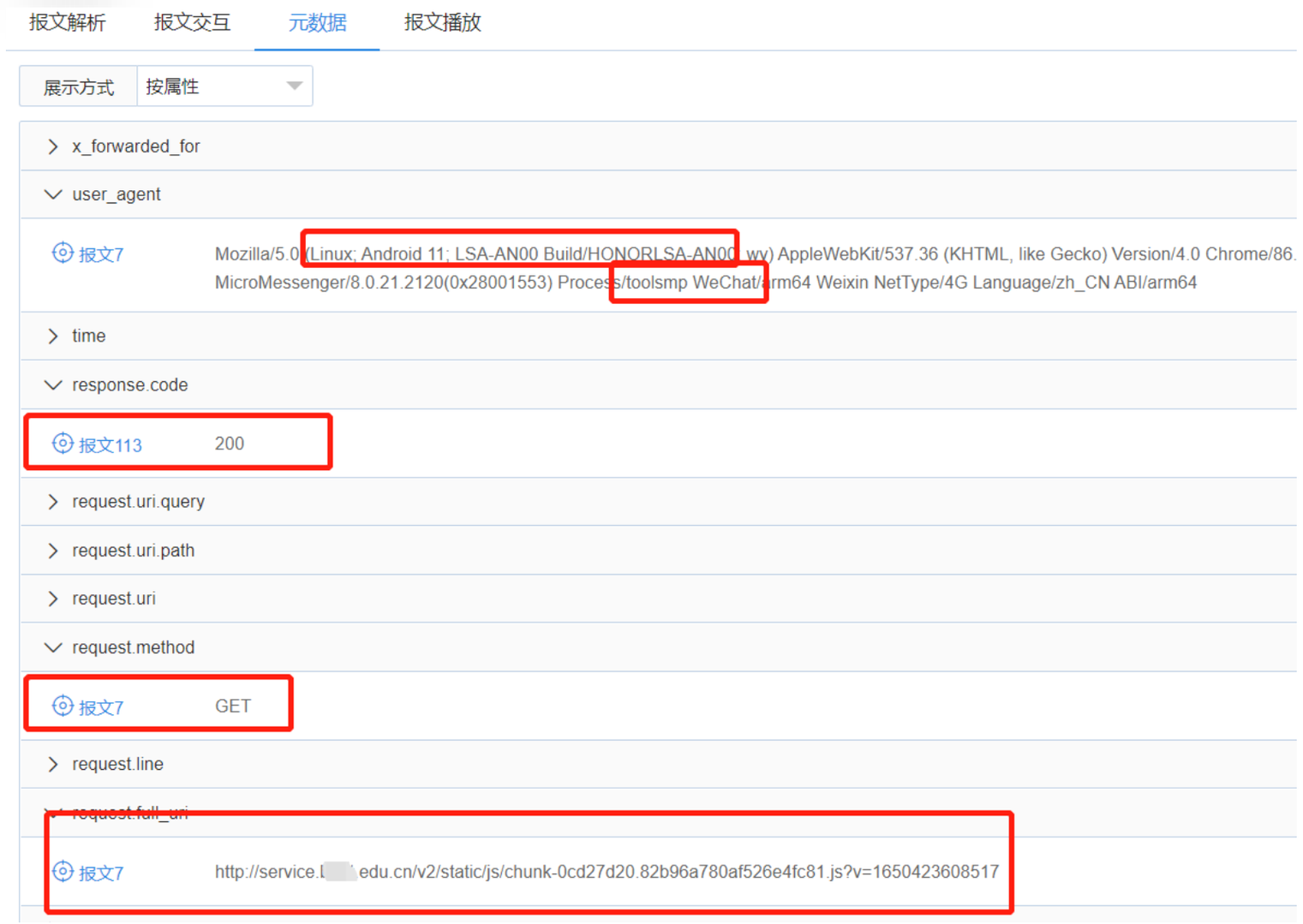
交互过程

Source **Destination**

```
                                                  Num: 1. 2022/04/12 10:40:04 78 bytes
88 df 9e 39 2a 01 00 50 56 80 99 e9 81 00 0f a9   ...9*..PV.......
08 00 45 00 00 3c f7 8f 40 00 40 06 f0 20 0a 03   ..E.....@.@.. ..
09 a2 0a 03 35 64 62 cc 00 50 c8 ee 7f 52 00 00   ....5db..P...R..
00 00 a0 02 39 08 de 36 00 00 02 04 05 b4 04 02   ....9..6........
08 0a a9 78 88 dd 00 00 00 00 01 03 03 09         ...x...........
```

同时，也可以看到客户端和服务器通讯，详细的报文交互详细数据。

实战：分校区某台PC，流量抓包分析



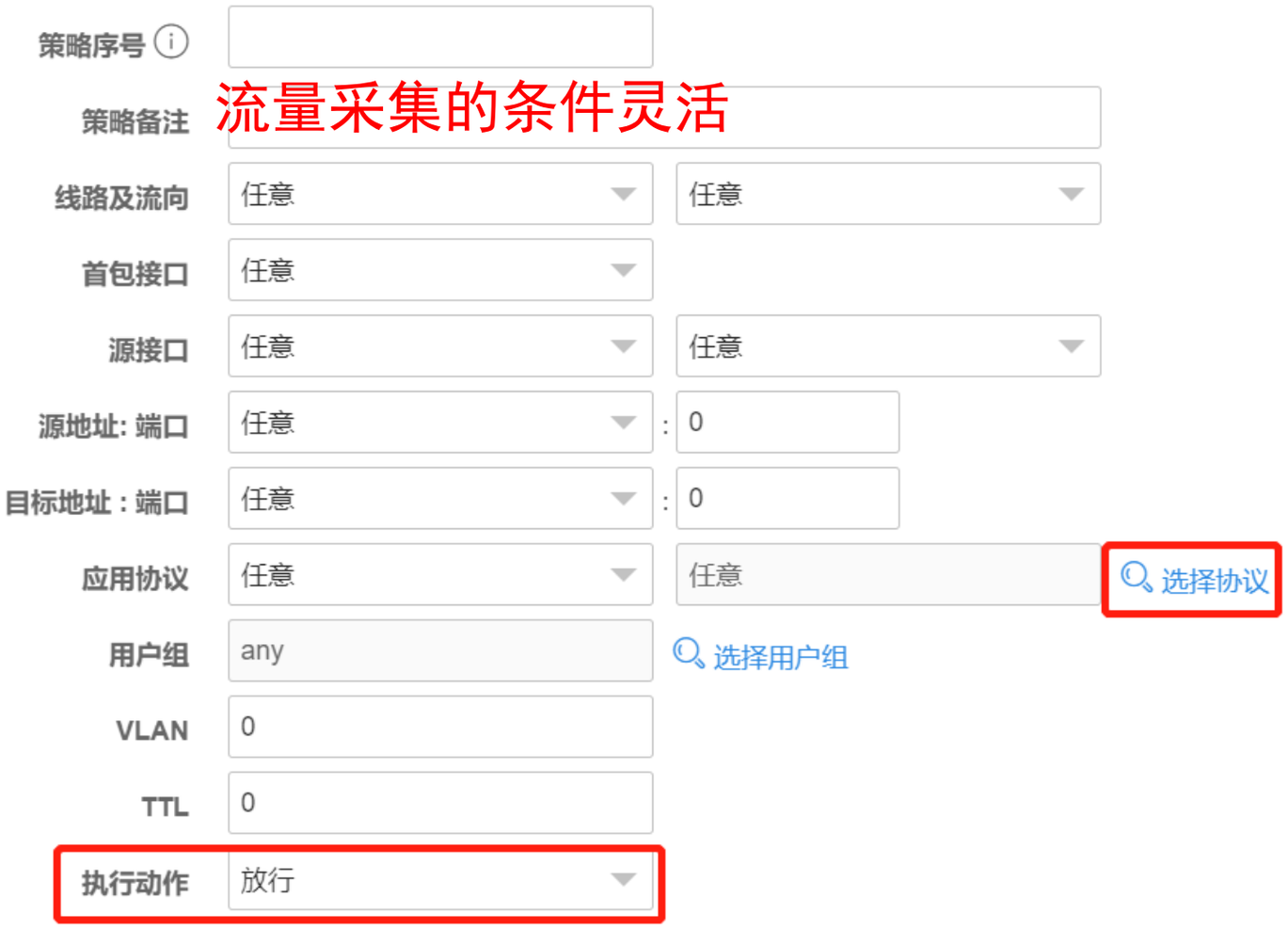
元数据分析：

对相关报文元数据进行统计，发现数据包相关属性。从而对数据包有更多信息了解。

例如：这是一个用户通过华为荣耀60（LSA-AN00），使用微信工具访问内网service.*.edu.cn的一个HTTP数据包，通过get模式从服务器上获得数据，并且访问成功。

Tips1：如何节约回传带宽

Tips2：如何节约NTM硬盘



场景二：5G CPE在遥测的应用

基本概念

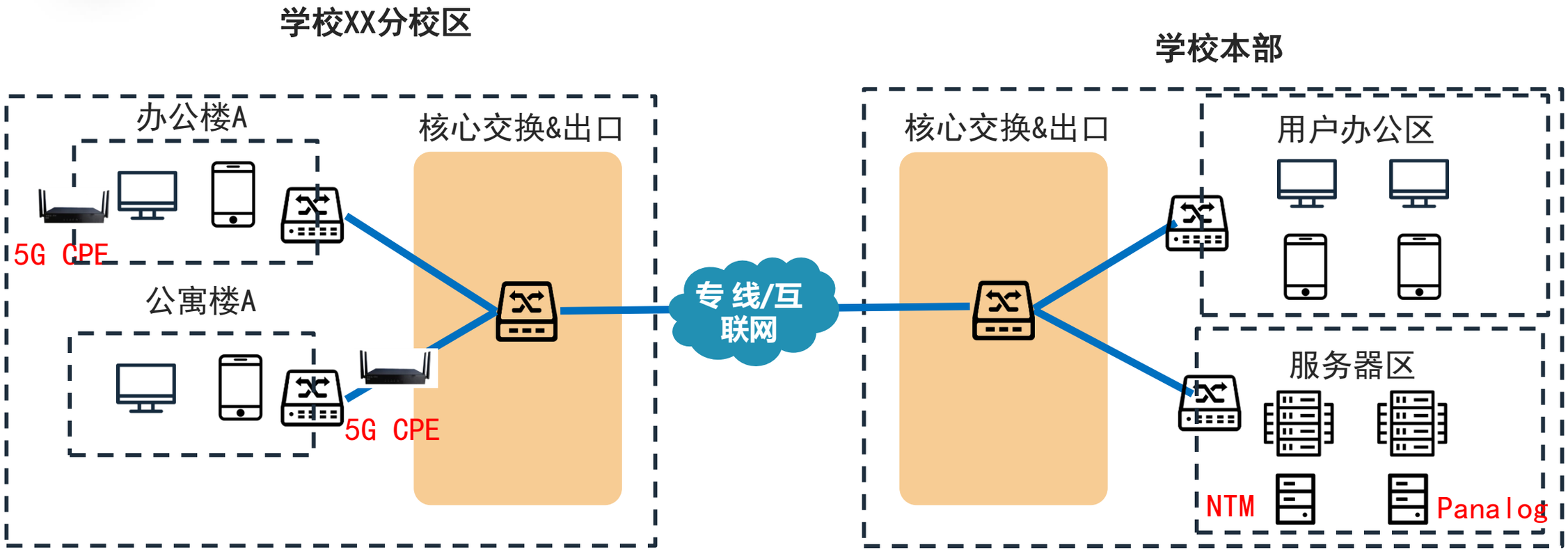
CPE（Customer Premise Equipment）客户终端设备。

Panabit 5G CPE设备是一款支持4G/5G SIM卡的Panabit网关设备，同时具备了目前Panabit智能应用网关的所有功能。

XX大学使用网络现状分析

1. XX大学分校区缺乏IT人员，本地无法做到网络维护和故障定位；
2. 网络病毒爆发时候，分校区和总校区的专线跑满，无法进行远程维护；
3. 缺少主动预警手段，工作比较被动；

场景二：5G CPE在遥测的应用



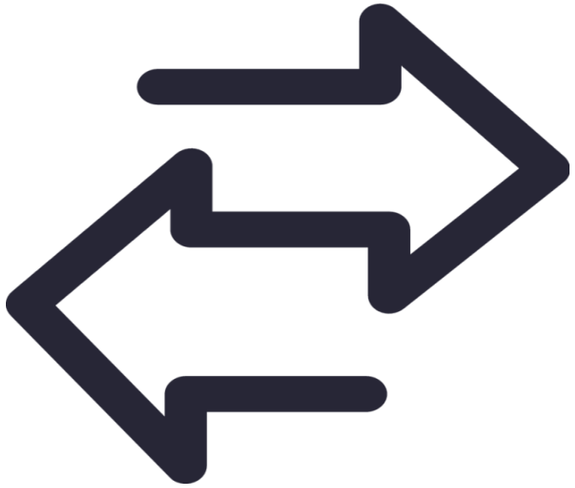
部署说明

1. 在分校区的重点汇集交换机或者楼宇处部署Panabit 5G CPE设备；
2. 在学校本部部署云平台和Panalog 和Panabit NTM 系统；
3. 通过遥测功能，将分校区的某些数据“抓包”到总校区进行NTM分析。

02

NTM分析校园网卡顿问题

实战：校园网卡顿NTM分析



场景1：校园网访问互联网卡顿分析

场景2：互联网访问校园网服务器卡顿分析

协议质量Dashboard—协议时延

序号	应用名称	最大时延	最小时延	平均时延
1	其它HTTP上传	6587.853 ms	0.053 ms	1217.805 ms
2	Office365	3467.394 ms	137.021 ms	443.218 ms
3	QQMail	123.725 ms	37.677 ms	98.496 ms
4	Oracle	1025.406 ms	0.977 ms	96.969 ms
5	腾讯文档	94.656 ms	32.417 ms	94.656 ms
6	QQ游戏	84.119 ms	0 ms	84.119 ms
7	歪歪语音/Bigolive	82.907 ms	63.269 ms	78.154 ms
8	Google搜索/服务	78.551 ms	63.547 ms	77.995 ms
9	QQ聊天	50.431 ms	0 ms	50.431 ms
10	百度云盘	524.912 ms	1.266 ms	38.517 ms
11	Windows补丁	197.38 ms	0.711 ms	38.228 ms
12	伪IE下载	3139.013 ms	0.217 ms	37.416 ms
13	Apex英雄	4260.801 ms	0.004 ms	36.69 ms
14	SNMP	7818.372 ms	0.002 ms	32.424 ms
15	腾讯	84.721 ms	12.215 ms	29.861 ms

协议时延算法：

客户时延+服务时延+应用时延

常规使用：

这里主要看“平均时延”，如果该时延比较大，说明这个业务整体体验感不大好，需要进行优化。

协议质量Dashboard—协议重传

协议重传：

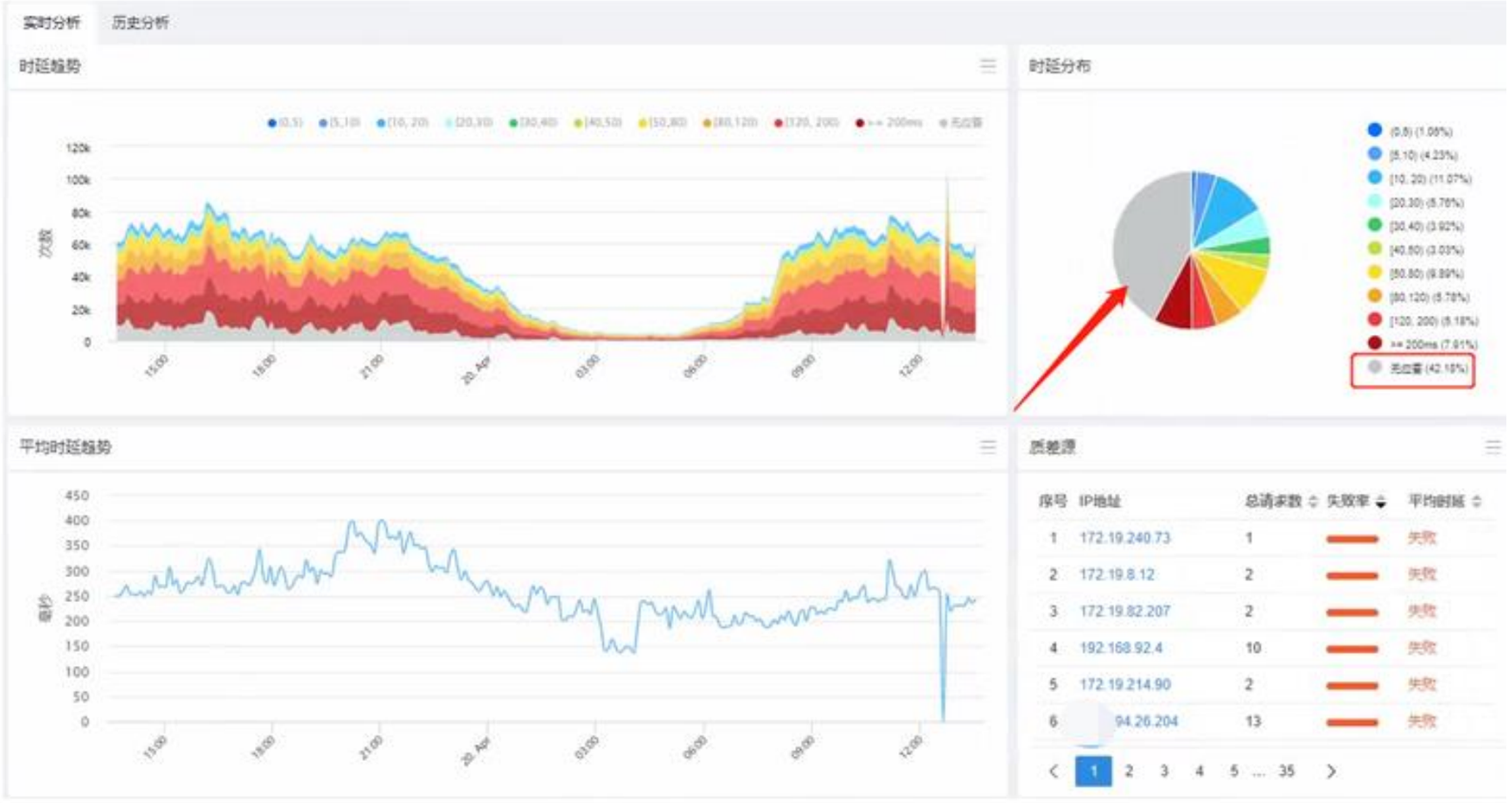
指TCP连接建立后，由于通讯超时或者TCP序列不对产生的重传包。

常规使用：

如果某类应用的重传率非常高，用户体验感肯定不好。

校内网访问互联网应用协议重传 Dashboard

案例1：校园网访问微信卡顿NTM分析



第一步：微信时延分析

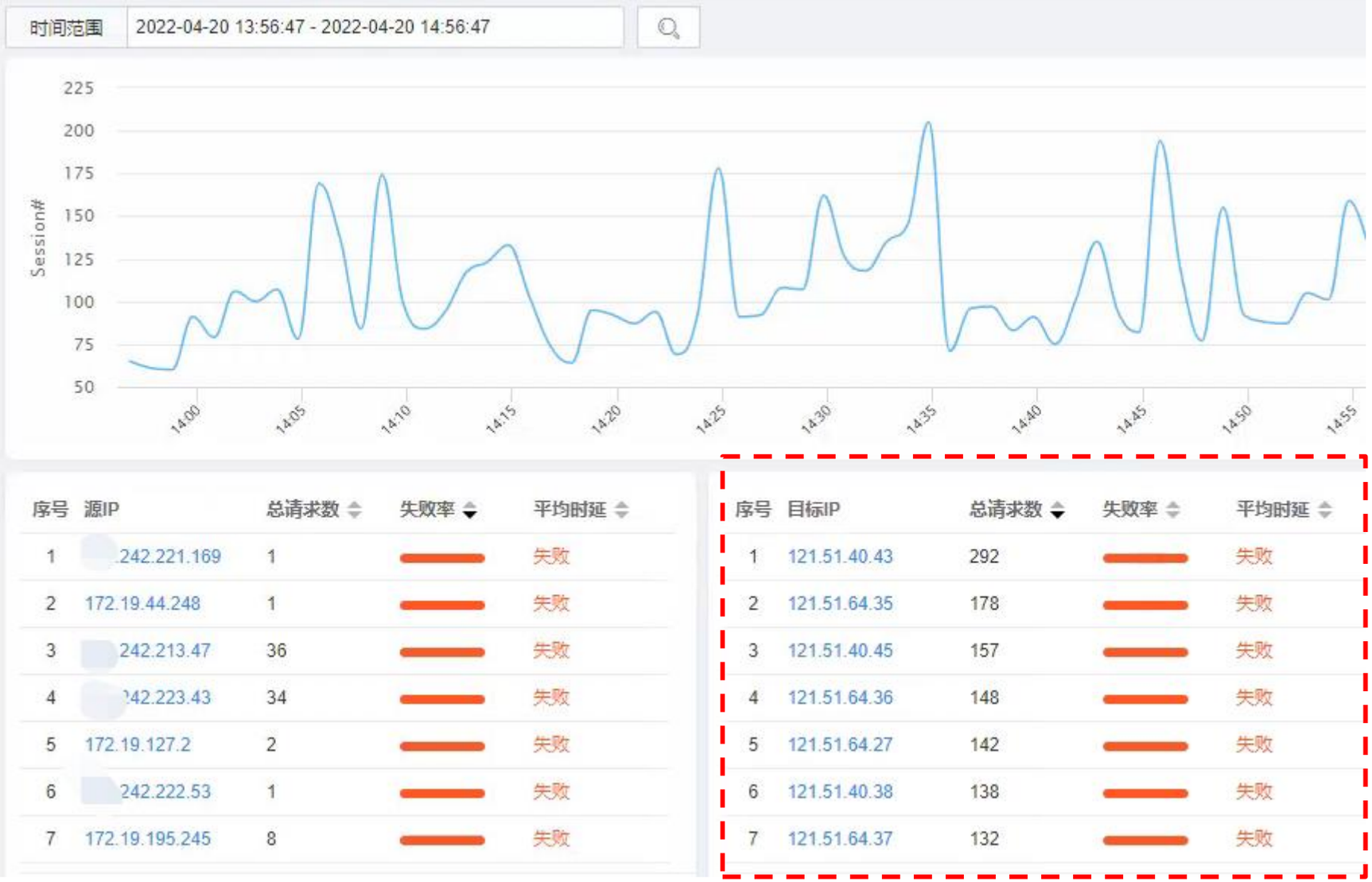
NTM分析

通过时延分析，发现微信的未应答数量非常多，高达42.18%

解决思路：

需要对“未应答”数据包进行分析，找出相关原因

案例1：校园网访问微信卡顿NTM分析



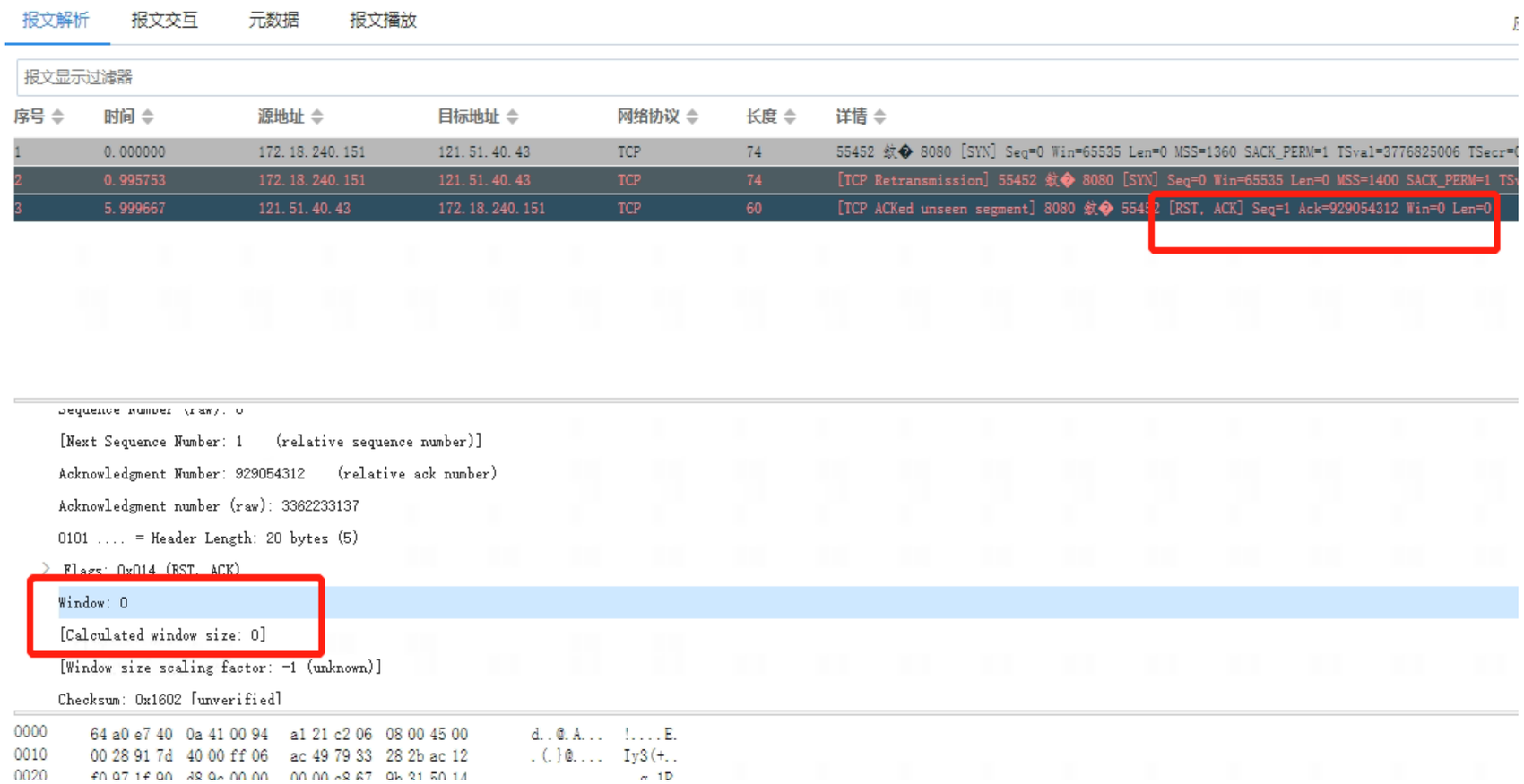
序号	源IP	总请求数	失败率	平均时延
1	.242.221.169	1	[redacted]	失败
2	172.19.44.248	1	[redacted]	失败
3	242.213.47	36	[redacted]	失败
4	242.223.43	34	[redacted]	失败
5	172.19.127.2	2	[redacted]	失败
6	242.222.53	1	[redacted]	失败
7	172.19.195.245	8	[redacted]	失败

序号	目标IP	总请求数	失败率	平均时延
1	121.51.40.43	292	[redacted]	失败
2	121.51.64.35	178	[redacted]	失败
3	121.51.40.45	157	[redacted]	失败
4	121.51.64.36	148	[redacted]	失败
5	121.51.64.27	142	[redacted]	失败
6	121.51.40.38	138	[redacted]	失败
7	121.51.64.37	132	[redacted]	失败

第二步：“未应答” 数据包分析

通过NTM对微信“未应答”数据包进行分析，发现相关目标地址主要集中在121.51.0.0/16这个网段。

案例1：校园网访问微信卡顿NTM分析



第三步：“未应答” 数据包进行报文解析

通过报文解析，发现3个报文。

1. 是客户端对微信服务器进行请求，但服务器没有回应（没看到回包）。
2. 客户端重新请求，但服务器直接进行重置，同时告诉客户端window窗口为0

结论：

腾讯服务器对该请求进行拒绝

案例1：校园网访问微信卡顿NTM分析

问题解决：

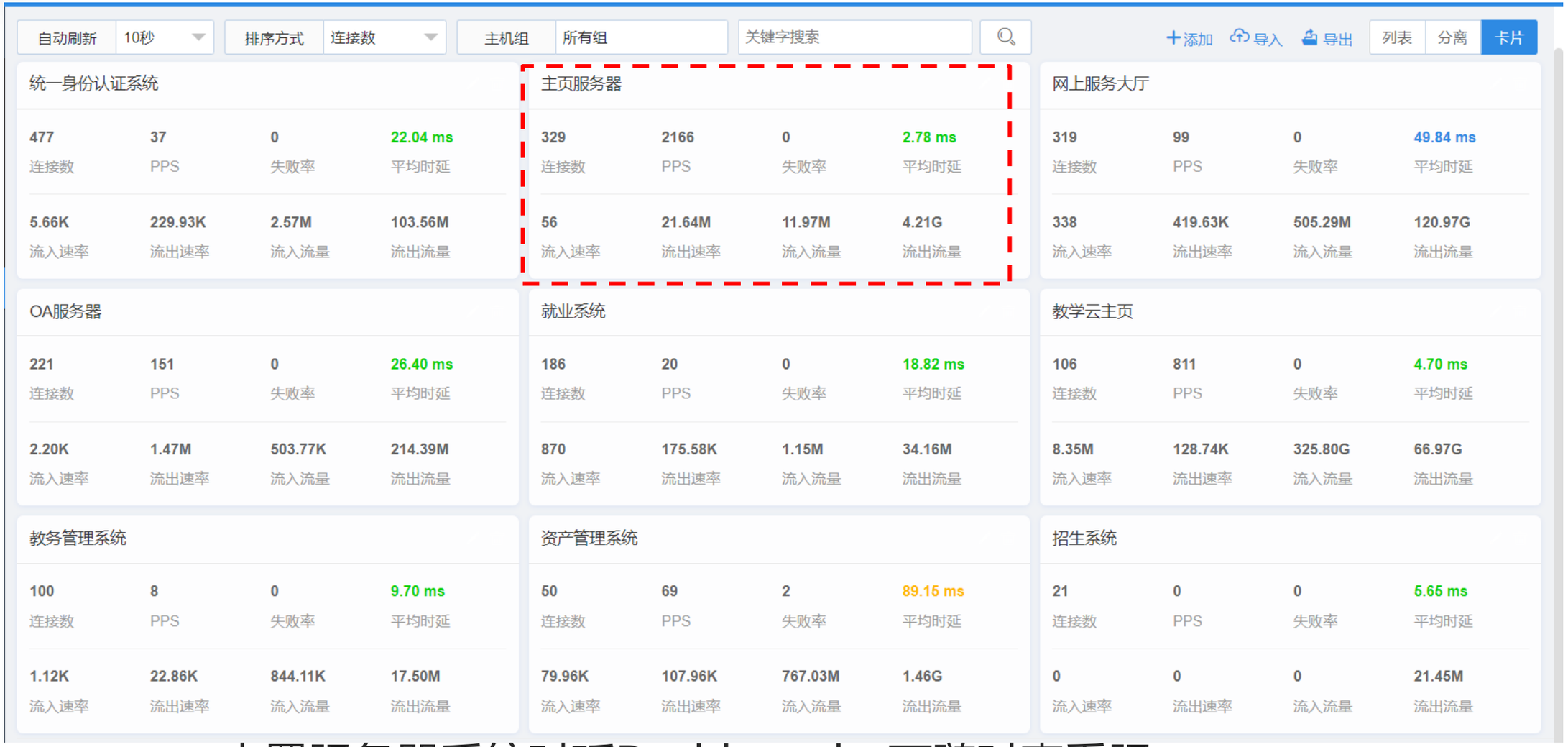
由于这个用户微信“未响应”数据包的目标地址基本上集中在121.51.0.0/16这个网段，怀疑出口ISP到这个网段的问题，更换121.51.0.0/16的路由选择，让到121.51.0.0/16数据包走另外一个ISP，这个问题得以解决。

实战：校园网卡顿NTM分析

场景1：校园网访问互联网卡顿分析

场景2：互联网访问校园网服务器卡顿分析

场景2：校内服务器访问质量分析



内置服务器系统时延Dashboard，可随时查看服务器的连接数、失败率、时延、流量等信息。

场景2：校内服务器访问质量分析

学校主页负载均衡的到3台服务器，每台服务器承载的访问次数

每台服务器的时延指标

某台服务器访问时延DashBoard

场景2：校内服务器访问质量分析

Panabit®

序号	域名	总请求次数	DNS请求次数	HTTP请求次数	HTTPS请求次数	HTTP20x	HTTP30x	HTTP40x	HTTP50x
1	www.b edu.cn	172352	63338	108926	88	105583	514	2722	0
2	service.b .edu.cn	161110	1130	159833	147	158293	959	549	0
3	auth t.edu.cn	141369	1057	140224	88	17768	122315	103	0
4	jwgl.b .edu.cn	36334	512	5201	30621	0	5199	1	0
5	apiucloud. .edu.cn	35796	406	34932	458	32923	0	1956	3
6	ucloud.b edu.cn	24028	904	22235	889	18476	3360	384	0
7	huorong.b edu.cn	13593	4044	119	9430	119	0	0	0
8	yjxt. t.edu.cn	12960	7258	5702	0	4704	495	43	150
9	360.b edu.cn	12117	1228	10889	0	270	10554	51	0
10	oa.bu du.cn	9293	138	9022	133	6321	10	2690	0
11	teac t.edu.cn	8514	242	[illegible]	3	4914	325	214	2383
12	news.b .edu.cn	8216	3212	5002	2	3729	261	1011	0
13	imgservice.b edu.cn	7433	434	6990	9	6924	36	27	0
14	reservation.b edu.cn	6369	559	5790	20	3986	1796	0	0
15	zsb t.edu.cn	6072	86	5984	2	5402	25	556	0
16	scs t.edu.cn	5877	114	5762	1	4392	575	795	0
17	my t.edu.cn	5510	951	4559	0	2825	1377	352	2
18	jwglweixin. .edu.cn	5387	1030	4357	0	3806	446	104	0

资产热度排名

资产访问排名

资产状态码排名

< 1 2 3 4 5 > 到第 1 页 确定 总共 464 1

资产数量

场景2：校内服务器访问质量分析

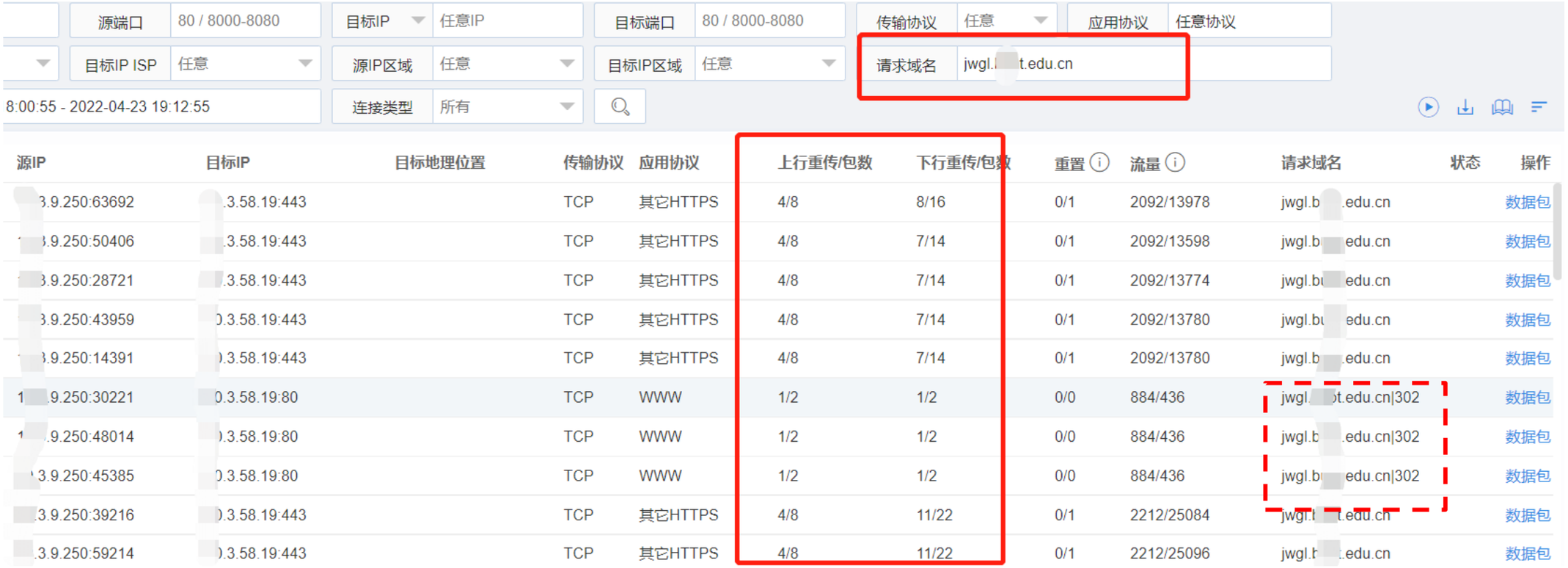
HTTP状态码描述

分类	分类描述	
1**	信息，服务器收到请求，需要请求者继续执行操作	
2**	成功，操作被成功接收并处理	例如：200请求成功。一般用于GET与POST请求
3**	重定向，需要进一步的操作以完成请求	例如：301/302，请求的资源移动到新URI，返回信息会包括新的URI
4**	客户端错误，请求包含语法错误或无法完成请求	例如：404，服务器无法根据客户端的请求找到资源（网页）
5**	服务器错误，服务器在处理请求的过程中发生了错误	例如：503，由于超载或系统维护，服务器暂时的无法处理客户端的请求

根据状态码，可以对服务器访问情况有所评估和判断。

例如：某服务器的HTTP数据包里面包含大量500或者503，说明服务器内部错误，或者由于超载或系统维护，无法完成客户端请求。
例如：某服务器HTTP数据包里面包含301/302状态码，说明资源被重定向，如果重定向的资源有问题，用户访问也会存在问题。

案例2：访问服务器慢，如何进行定位？



案例背景：网络中心接到投诉，说用户访问校内某台服务器特别慢，需要进行排查。

NTM分析：通过NTM分析，发现用户访问存在HTTP 302报文，同时该服务器的重传率非常高，大约50%左右。但这个重传是如何导致的呢？

案例2：访问服务器慢，如何进行定位？

报文解析　报文交互　元数据　报文播放

报文显示过滤器

9	0.000654	3.58.19	3.9.250	HTTP	218	HTTP/1.1 302 Found
10	0.000656	3.58.19	3.9.250	TCP	218	[TCP Out-Of-Order] 80 [illegible]
11	0.001136	3.9.250	3.58.19	TCP	70	48014 [illegible] 80 [FIN, ACK]
12	0.001138	3.9.250	3.58.19	TCP	70	[TCP Out-Of-Order] 48014 [illegible]
13	0.001187	3.58.19	3.9.250	TCP	70	80 [illegible] 48014 [ACK] Seq=15
14	0.001189	3.58.19	3.9.250	TCP	70	[TCP Dup ACK 13#1] 80 [illegible]

```
> Frame 9: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
> Ethernet II, Src: 00:50:56:b5:82:7d (00:50:56:b5:82:7d), Dst: 88:df:9e:39:2a:01 (88:df:9e:39:2a:01)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4018
> Internet Protocol Version 4, Src: 3.58.19, Dst: 3.9.250
> Transmission Control Protocol, Src Port: 80, Dst Port: 48014, Seq: 1, Ack: 373, Len: 148
v Hypertext Transfer Protocol
  > HTTP/1.1 302 Found\r\n
    Cache-Control: no-cache\r\n
  > Content-length: 0\r\n
    Location: https://jwg1.  edu.cn/jsxsd/framework/xsMain.jsp\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000083000 seconds]
    [Request in frame: 7]
    [Request URI: http://jwg1.  edu.cn/jsxsd/framework/xsMain.jsp]
```

HTTP302分析

通过NTM报文解析，发现该报文里面HTTP 302是把通过HTTP访问该服务器的数据包重定向到HTTPS访问。

访问慢不应该是这个原因，对其他报文进行深入分析

案例2：访问服务器慢，如何进行定位?

Panabit®

报文解析 报文交互 元数据 报文播放

报文显示过滤器

1	0.015500	3.9.250	10.3.58.19	TCP	70	53957 [ACK] Seq=736 Ack=6369 Win=43008 Len=0
2	0.015500	3.9.250	10.3.58.19	TCP	70	[TCP Dup ACK 31#1] 53957 [ACK] Seq=736 Ack=6
3	0.015719	3.9.250	10.3.58.19	TLSv1.2	101	Encrypted Alert
4	0.015726	3.9.250	10.3.58.19	TCP	101	[TCP Retransmission] 53957 [PSH, ACK] Seq=73
5	0.015761	10.3.58.19	3.9.250	TCP	64	443 [RST] Seq=6369 Win=0 Len=0
6	0.015762	10.3.58.19	3.9.250	TCP	64	443 [RST] Seq=6369 Win=0 Len=0
7	0.015763	3.9.250	10.3.58.19	TCP	70	53957 [FIN, ACK] Seq=767 Ack=6369 Win=43008
8	0.015764	3.9.250	10.3.58.19	TCP	70	[TCP Out-Of-Order] 53957 [FIN, ACK] Seq=767
9	0.015822	10.3.58.19	3.9.250	TCP	64	443 [RST] Seq=6369 Win=0 Len=0
10	0.015822	10.3.58.19	3.9.250	TCP	64	443 [RST] Seq=6369 Win=0 Len=0

```
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x004 (RST)
Window: 0
[Calculated window size: 0]
[Window size scaling factor: 128]
Checksum: 0x575e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
```

NTM报文解析—看的更深入，看的更明白

通过对重传率高的会话进行抓包分析，发现具体原因。例如：本案例中有大量win=0，Len=0的数据包，说明是因为服务器的缓存区基本满了，无法再接受数据。也推断出该重传是因为服务器负载太重，导致的无法响应。

案例3：国外用户访问服务器卡顿，如何办？

案例背景：网络中心接到投诉，说国外用户访问校内某台服务器特别慢，需要进行排查。

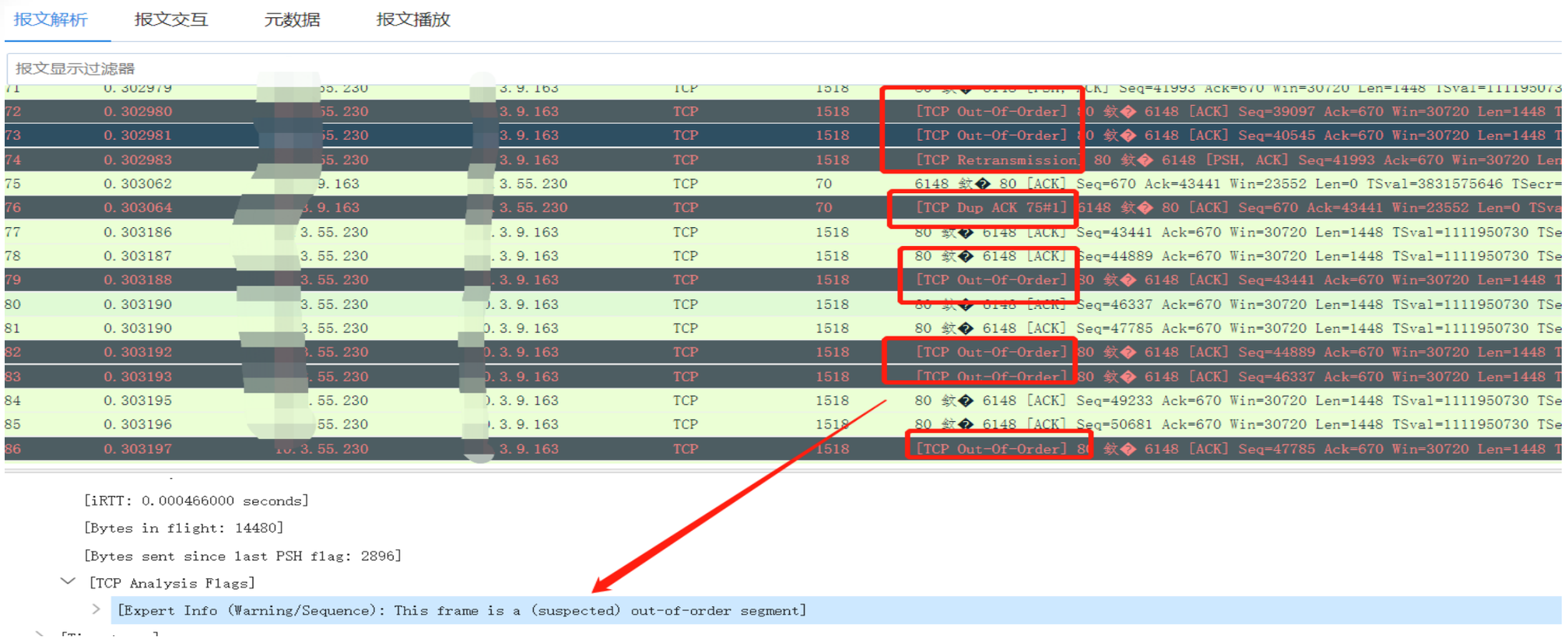
NTM时延分析：在“会话时延”选型里，源ISP选择“其他”，请求域名选择 对应服务器的域名，进行时延分析，发现客户时延比较大，基本判断为从国外到校园网的问题。

案例3：国外用户访问服务器卡顿，如何办？

案例背景：网络中心接到投诉，说国外用户访问校内某台服务器特别慢，需要进行排查。

NTM重传分析：在“会话流量”里面，源ISP选择“其他”，请求域名选择 对应服务器的域名，进行重传分析，发现重传率也比较高，大约50%左右。

案例3：国外用户访问服务器卡顿，如何办？



分析：通过报文解析，发现重传的原因是有大量的TCP Out_of_Order数据包和TCP Retransmission
TCP Out_of_Order的原因分析：一般来说是网络拥塞或者数据包传输路径不同，导致顺序包抵达时间不同，延时太长，或者包丢失，需要重新组合数据单元。
TCP Retransmission原因分析：由于数据包传输超时引发的数据重传。

结论：数据包在传输过程中存在大量丢包，导致重传，因此属于传输过程中的问题。

案例3：国外用户访问服务器卡顿，如何办？

Panabit®

问题判断：

依据1：会话时延里面，客户时延比较大，说明在建立TCP时候，从客户端到服务器需要比较长时间，说明数据包在网络层传输质量不好。

依据2：TCP建立成功后，进行HTTP传输，但HTTP的重传比较多，大约有50%的重传，通过NTM报文解析，发现大量的TCP Out_of_Order数据包和TCP Retransmission，也说明是网络拥塞或者数据包传输路径不同，导致顺序包抵达时间不同，延时太长，或者包丢失，需要重新组合数据单元。

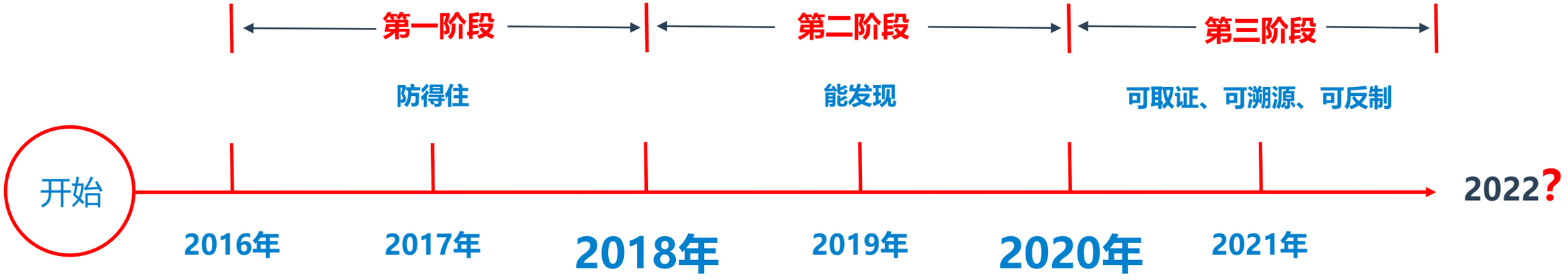
结论：

该问题不是服务器的问题，属于从客户端到服务器的网络问题。

03

全流量数据分析在护网时的应用

护网的三个阶段



防守对策	防守对策	防守对策
1.使用大量的硬性防守手段； 2.下线风险的业务系统； 3.封堵大量的IP地址； 4.畸形的防守手段；	1.使用大量的硬性防守手段； 2.下线风险的业务系统； 3.封堵大量的IP地址； 4.畸形的防守手段； 5.使用大量的安全设备；	1.使用大量的硬性防守手段；× 2.下线风险的业务系统；× 3.封堵大量的IP地址；× 4.畸形的防守手段；× 5.使用大量的安全设备；√

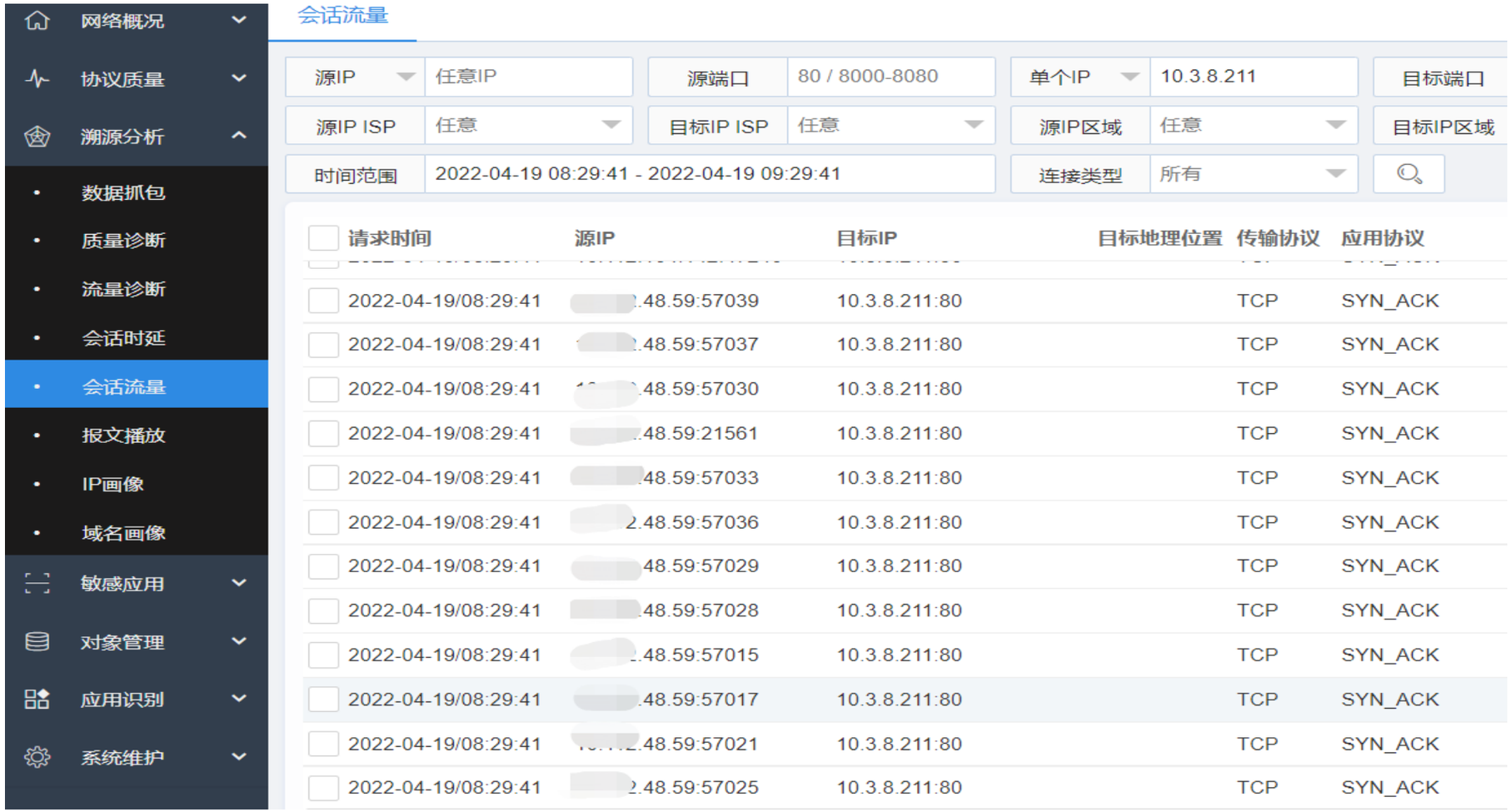
护网期间，防守方加分项目

Panabit®

类别	得分标准	赋值规则	赋值上线	备注
发现类	发现攻击者进入逻辑隔离业务内网区事件	100分/次	1000分	提供的证据必须与攻击方提供的证据相吻合的**详细分析报告**（时间、IP、日志、处置结果等）
消除类	处置异常账号	普通用户：应用层5分，系统层10分，数据库10分，网络设备25分。管理员用户：得分*2	500分	提供包**含确凿证据的详细分析报告**（创建时间、访问日志、登录日志、处置结果等），由裁判组研判后给分
应急处理类	积极配合应急组工作，根据线索能快速准确定位危害系统，**能提供充分的日志记录，配合执法机关有效固定证据完成勘验**	能高效配合完成应急工作的，得分300；配合一般的，得分200；差的-100	/	最高300分，最低-100分
追踪溯源类	对网络攻击事件的进行成功溯源，**提交有效证据材料构成证据链**，还原完整攻击路径，证实攻击者的攻击行为	境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客	/	提供包含确凿证据的详细分析报告（时间、平台截图、访问日志、告警详情等）

PS: 加分项目不止这几个，这里只是摘抄几个举例说明。

实战：护网期间，全流量数据留存可以作什么？



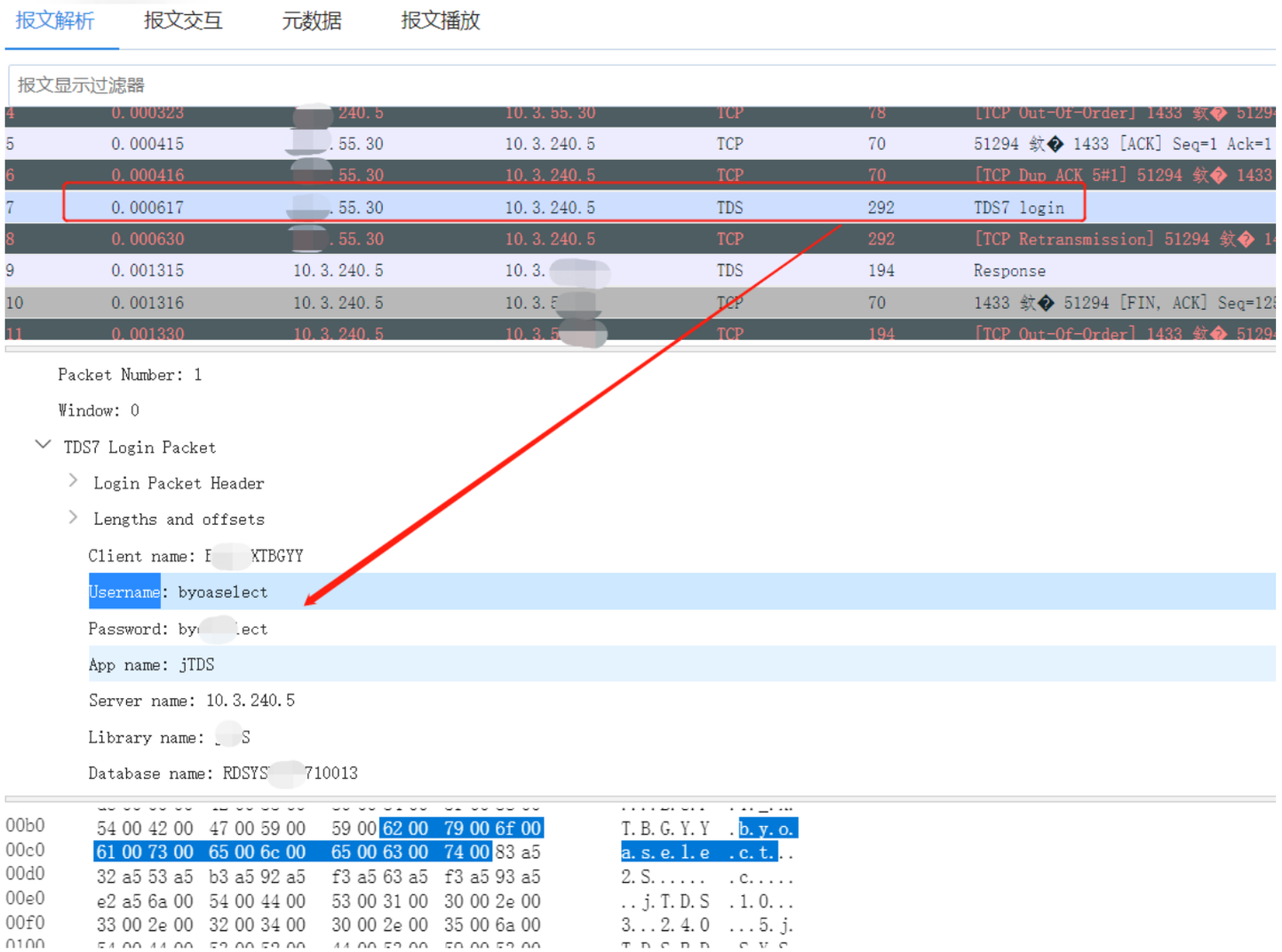
通过全流量的数据留存，发现从外网对内网一台服务器的端口扫描
（很不幸，端口扫描不是加分项）

实战：护网期间，全流量数据留存可以作什么？

	源IP	目标IP	目标地理位置	传输协议	应用协议	上行重传/包数	下行重传/包数	重置	流量
9/08:29:41	55.30:39522	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	5.30:39524	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:41	5.30:39523	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39525	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39526	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:42	5.30:39527	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39529	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39530	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:44	55.30:39528	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39538	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	55.30:39537	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388
9/08:29:45	3.55.30:39536	10.3.240.5:1433		TCP	MSSQL	1/2	1/2	0/0	584/388

通过全流量的数据留存，发现从外网对内网一台数据库服务器的流量非常有规律。
这个是啥原因呢？有可能是加分项目吗？

实战：护网期间，全流量数据留存可以作什么？

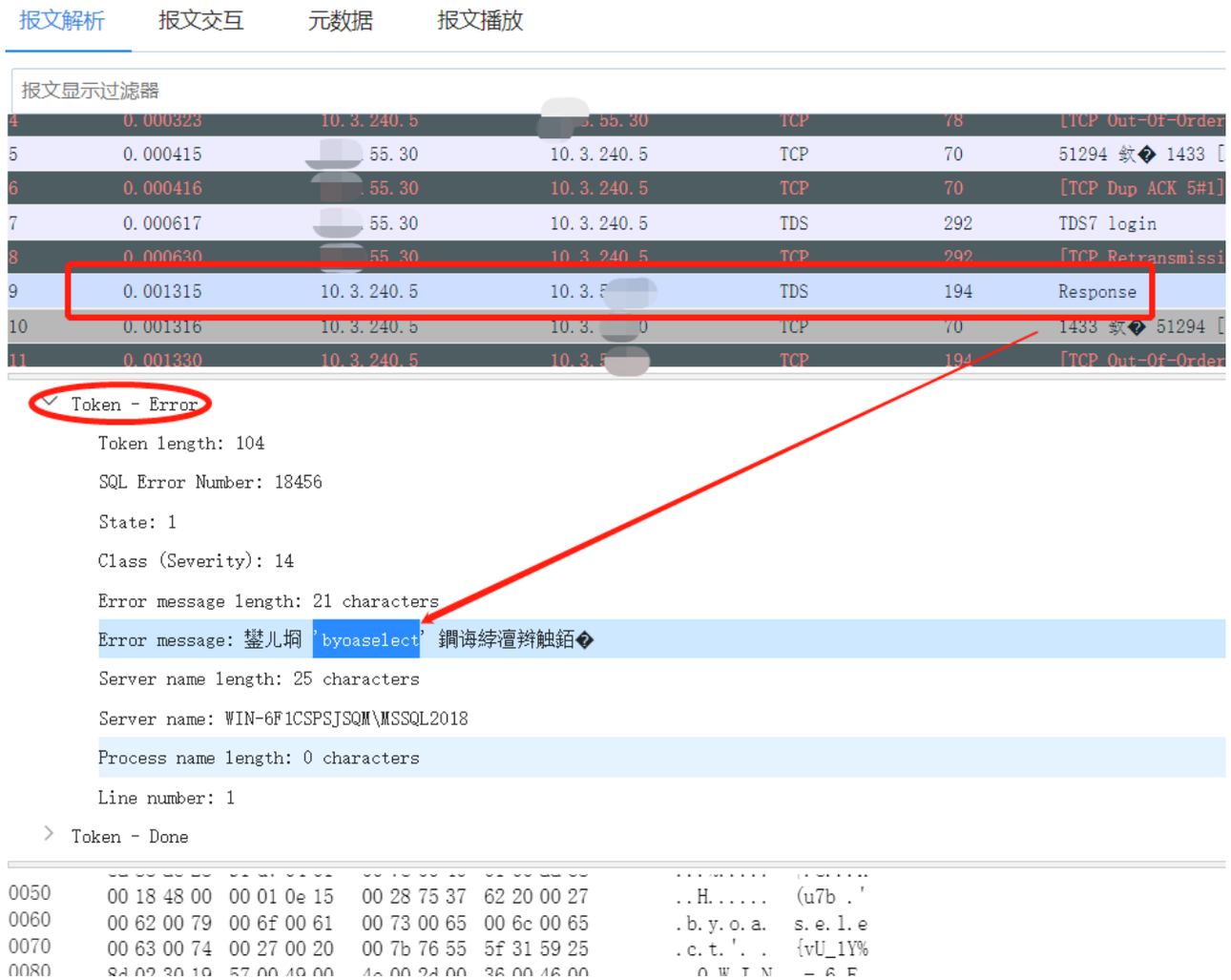


NTM分析

外网某IP对数据库进行进行**连续**的登录操作。

登录的用户名为“byoaselect”

实战：护网期间，全流量数据留存可以作什么？



NTM分析

外网某IP对数据库进行进行**连续**的登录操作。数据库服务器进行响应，提示token 错误，同时，返回错误提示。

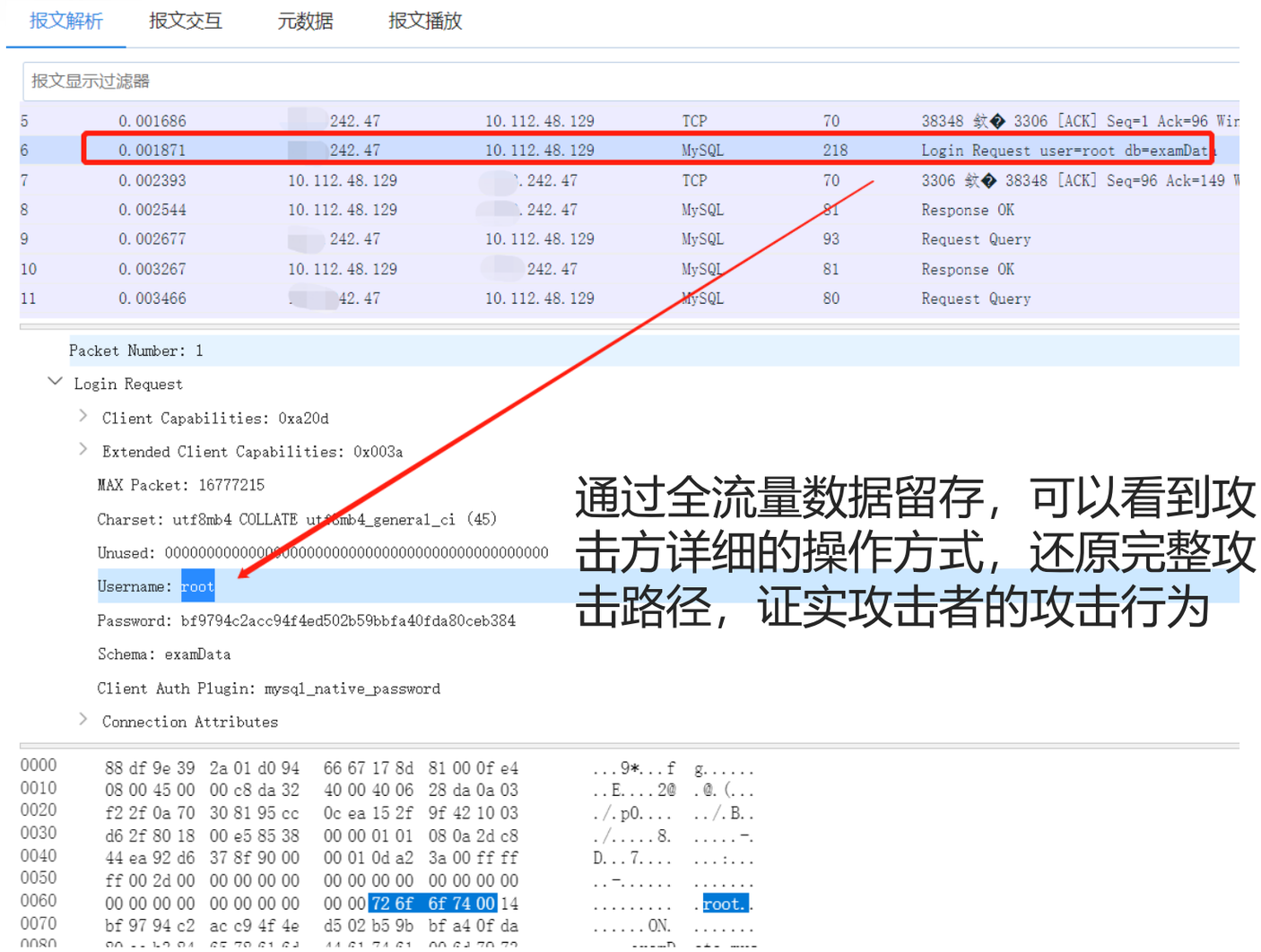
加分项目：

加分类别：发现类

加分标准：发现账号异常

加分：数据库账号10分，上限为500分

实战：护网期间，全流量数据留存可以作什么？



通过全流量数据留存，可以看到攻击方详细的操作方式，还原完整攻击路径，证实攻击者的攻击行为

NTM分析

外网某IP对数据库进行进行**root**登录操作。并且登录成功。

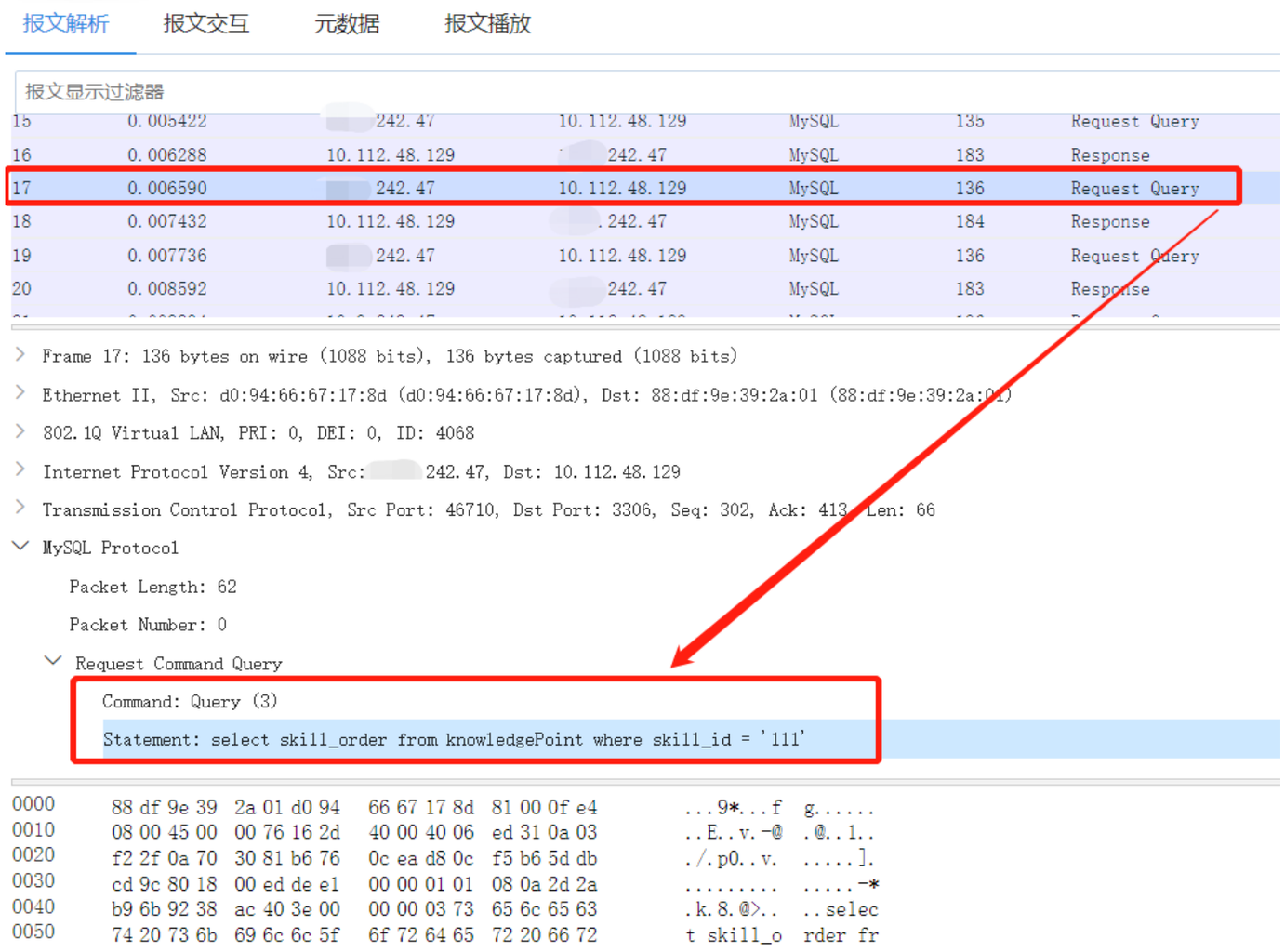
加分项目：

加分类别：发现类

加分标准：发现账号异常

加分：账号异常，加分上限为500分

实战：护网期间，全流量数据留存可以作什么？



NTM分析

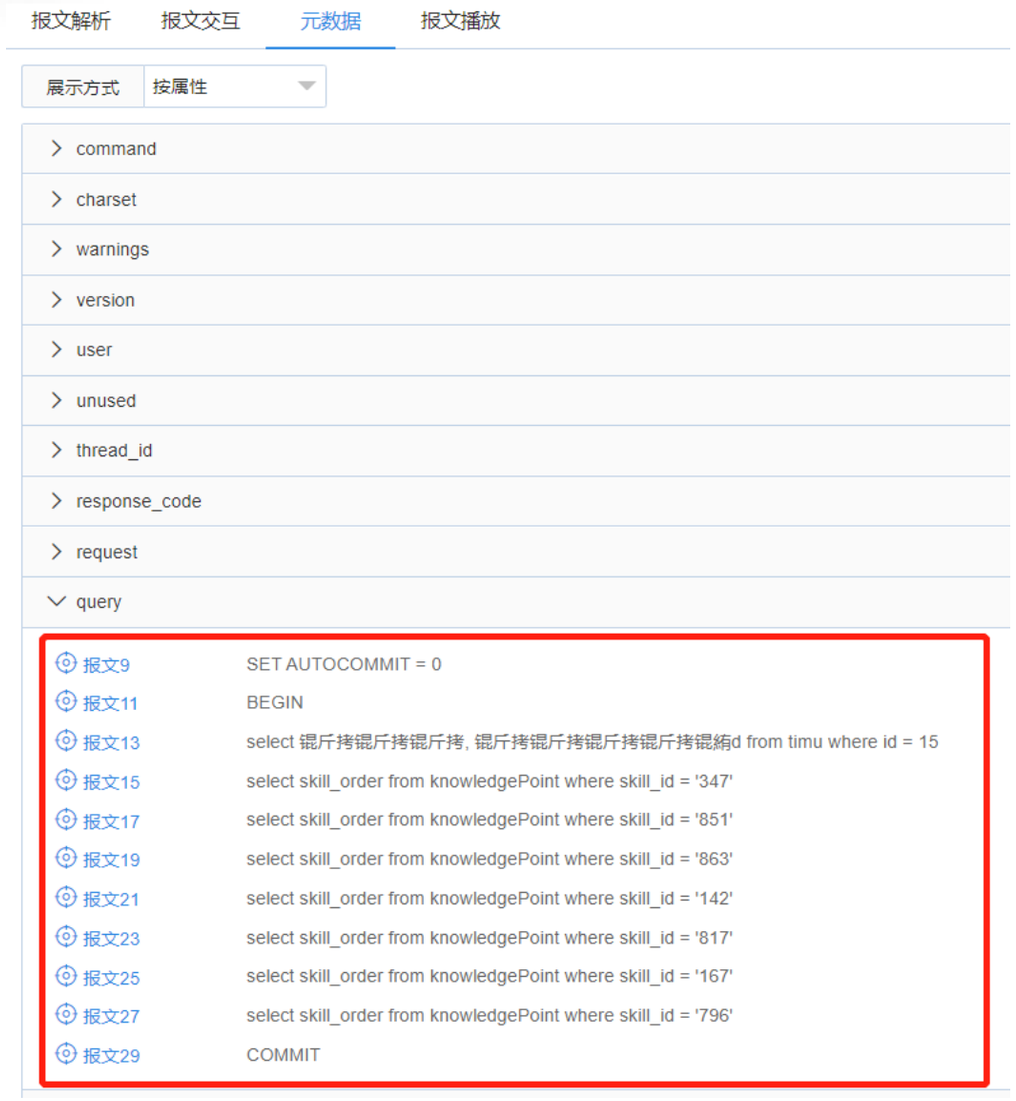
外网某IP对数据库进行进行**root**登录操作。登录成功后，进行数据库相关操作。

加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客



NTM分析

通过元数据分析，将同一会话里面的报文进行数据还原，还原相关操作的细节。

加分项目：

加分类别：追踪溯源类

加分标准：对网络攻击事件的进行成功溯源，提交有效证据材料构成证据链，还原完整攻击路径，证实攻击者的攻击行为

加分：境内黑客200-1000分/个黑客，境外黑客500-3000分/个黑客

实战：护网期间，全流量数据留存可以作什么？

Panabit®

NTM

应用过滤

威胁情报

威胁情报审计系统

- 挖矿分析
- 恶意木马分析
- 勒索软件分析
- APT分析
- 暗网访问分析
- C&C攻击分析
- ……

NTM

应用过滤

杀毒&IDS

已知病毒&木马审计系统

NTM

应用过滤

沙箱

未知病毒&木马分析系统

2022

可视化网络领导者

THANK YOU