高性能网络数据报文捕获和高性能网络数据报文回放测试解决方案

需求痛点：

不论您是网络和系统运维人员，还是网络设备或者网络安全的研发测试人员，现实中总会碰到一些非常奇怪的偶发故障，一会运行良好，一会出现问题宕机或者服务质量下降。这种时候故障问题的分析和排查总是异常艰难，一边是甲方或者线上用户的投诉，一边是面对巨大在线流量和复杂系统的无从下手。很多这种偶发故障的分析和排查都需要耗费非常长的时间和大量人员精力。花 2 个月分析出故障原因都是常见的状态。迫于甲方或者用户的压力，运维或者测试人员经常被迫熬夜排查问题，但往往收效甚微。

为了排查这种复杂问题，比较好的一个方法是对故障系统或者网络进行镜像抓包，捕获报文进行离线分析。通过 PCAP 报文的分析找到故障线索，还可以回放 PCAP 报文进行重复测试复现故障现象。一旦故障现象可以复现，问题就很容易解决了。但是很不幸的是 Linux 或者 Windows 自带的报文捕获软件或者回放软件，普遍存在不能高性能稳定运行的现象。使用 Linux TCPDUMP 工具或者 Windows 下的 Wireshark 抓包工具，流量稍微超过 100Mbps，就会出现大量丢包或者崩溃的问题。即便抓下来这些数据报文，如何进行高性能的回放重现故障也是很大的挑战。Linux 自带的 TCPReplay 工具对回放性能极为有限无法进行性能测试，也做不到长时间稳定运行。另外最重要的是测试人员无法了解 TCPReplay 工具回放时是否能够保证数据报文的回放顺序和原始报文一致，就是所谓的保序问题。对于前面提到的复杂故障问题，往往都是在性能条件下才会触发的技术问题。如果在现场有大流量数据而无法完整捕获和回放，还是无法有效定位问题。

解决方案：

触点互动的 XproNetworkSimulator 提供了一个非常高性能的在线捕获报文工具和在线报文回放工具，完美的解决了这些问题。在部署上，并不需要专用硬件完成这些高性能测试，只需要在标准的 X86 服务器和 CENTOS 上安装测试工具软件即可实现这样的高性能捕获报文和回放报文的能力。同时提供了非常简洁易用的中文图形化界面，操作人员可以快速进行报文捕获和回放测试。因为使用了高性能的 DPDK 平台开发框架，其报文捕获性能远远超过 TCPDUMP 和 Wireshark，报文回放性能远远超过 TCPReplay。并且支持 GE, 10GE, 100GE 等多种端口的捕获和回放。

测试报告

测试使用的硬件配置：

服务器型号：DELL R730xd

CPU 型号：Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz

内存：256G（16G*16，Speed: 2133 MHz）

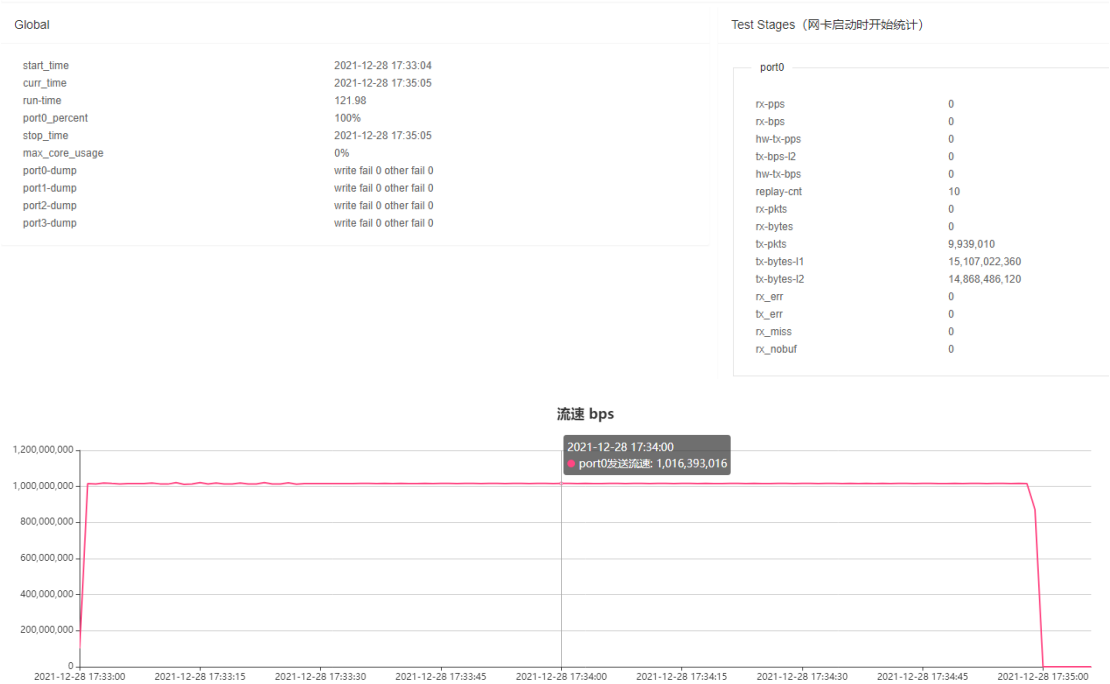
网卡：**X710** 四口 10G 网卡

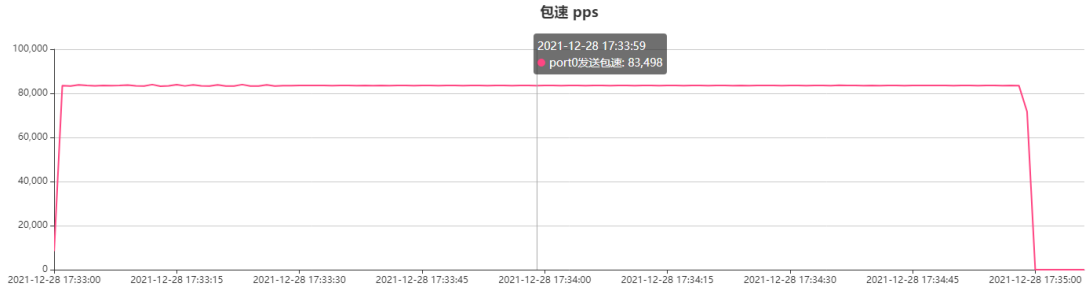
硬盘：300G

高性能报文捕获测试：

捕获报文：**15GByte** 。发送端平均包长：**1500byte** ，发送速率持续在 **1Gbps**，发送侧和捕获侧统计一致。

1、发送侧使用仪表进行 15Gbyte PCAP 数据发放，设定发送速率为 1Gbps，仪表统计结果如下：





2、使用报文捕获工具侧的统计结果



从图中可以看到，捕获工具可以以持续 1Gbps 的速度没有任何丢包的情况下持续向硬盘写入数据。最终数据报文数量和顺序和原始发送端一致。最大存储容量取决于服务器配置的内置硬盘容量，最高可以达到 40 块硬盘和 100TB 以上的持续存储。需要注意的是此次测试只使用了一块 300GB 的 SATA 硬盘，测试人员可以通过部署多块硬盘和 RAID 来提升存储性能从而提升报文捕获速度。

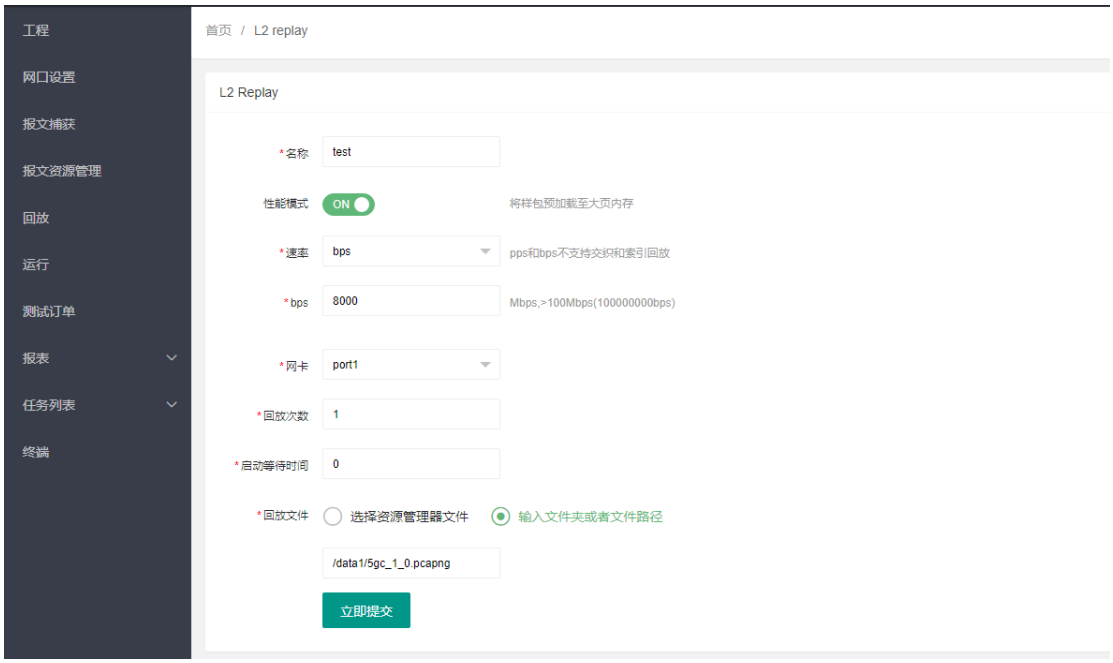
在实际报文捕获流程中，管理员也可以设定过滤策略，在海量流量中只捕获命中策略的数据报文。

高性能报文回放测试：

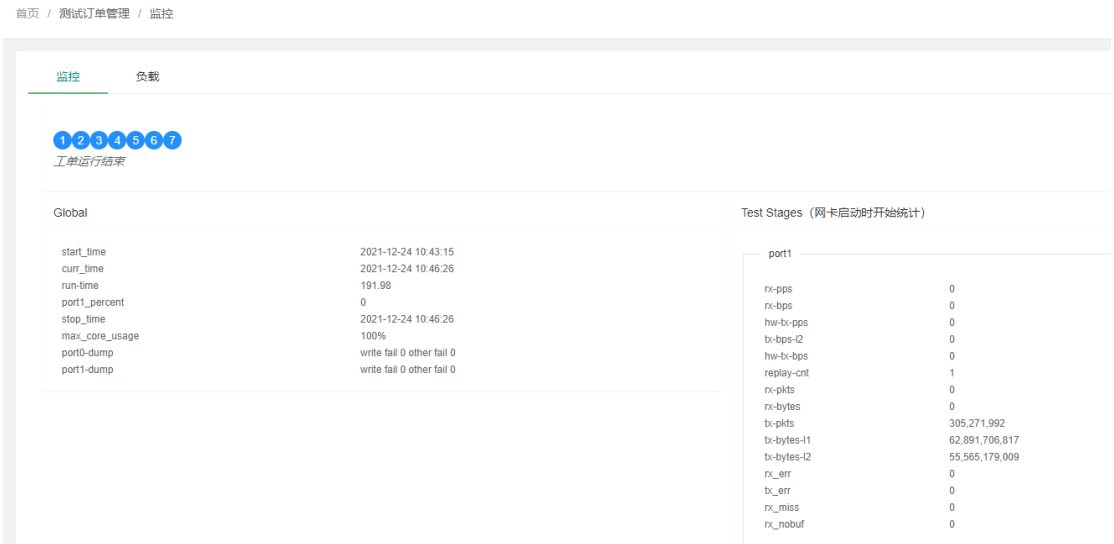
1 报文回放测试

我们选用了现网捕获的一组实际报文，总报文大小：63Gbyte。平均包长：206 byte。设定回放速度为 8Gbps，比现网捕获速度快 8 倍，同时要求回放顺序和现网捕获报文一样。

仪表相关的配置截图如下：



2、仪表运行结果





3. 保序测试

为了验证回放的数据报文顺序是否和现网之前捕获的报文一致，我们开发了一个在线的高性能检查工具，用于接收实时的回放流量，同时对比接收到的实时流量和之前捕获报文的逐包数据是否一致。每一个报文的 CRC 校验和都会被检查是否和之前的同样顺序出现的报文是否一致。如果有不一致就会报错。这一检查工具也是基于 DPDK 框架开发的高性能检查工具。

保序检查工具的测试结果（包数和回放端一致，乱序报文计数 0）

```
[root@localhost ns]# ./rx-pkt-check-pcap-out -l 13,14,15,16,17 -w 0000:44:00.3 -- 184_max_3_0.pcapng 2 1
EAL: Detected 96 lcore(s)
EAL: Detected 4 NUMA nodes
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: Selected IOVA mode 'PA'
EAL: Probing VFIO support...
EAL: PCI device 0000:44:00.3 on NUMA socket 1
EAL:   probe driver: 8086:1581 net_i40e
pcap_file 184_max_3_0.pcapng, working port = 0.
Port 0 MAC: 0c 73 eb 10 ab 58 in sockt 1

WARNING: Too many lcores enabled. Only 1 used.
total count = 47366965.
print_rx_count from core 14
lcore_main from core 15

Core 15 forwarding packets. [Ctrl+C to quit]
start lcore 16 to check
start lcore 17 to check
     rx_pkt_cnt:              0
     miss-match:              0
           drop:              0
        rx-miss:              0
         rx-err:              0
       rx-nobuf:              0
     ___________:  ____________
     rx_pkt_cnt:              0
     miss-match:              0
           drop:              0
        rx-miss:              0
         rx-err:              0
       rx-nobuf:              0
     ___________:  ____________
     rx_pkt_cnt:              0
     miss-match:              0
           drop:              0
        rx-miss:              0
         rx-err:              0
```

结论：

通过触点互动的 XproNetworkSimulator 测试工具，运维人员和测试人员可以在通用服务器上迅速实现超过 1Gbps 的高性能的报文捕获工具，以及极高性能的报文保序回放工具。我们经

过实测的单台服务器报文回放速度最高接近 100Gbps。这些高性能的测试工具可以极大的改善针对现网复杂流量相关的故障的诊断，定位和修复时间及成本。

关于触点互动

触点互动是一家专注研发国产化高性能网络仿真测试产品的创新型企业，其自主研发的 XproNetworkSimulator 高性能网络仿真测试工具，可以仿真常见互联网应用协议和攻击行为。其攻击库目前已经支持近万条攻击行为的仿真，包括常见 CVE 漏洞利用的攻击，高危事件的仿真，病毒传播的仿真，DDOS 攻击的仿真等。目前触点互动 XproNetworkSimulator 高性能网络仿真测试工具被广泛应用于安全设备商的设备研发测试，网络靶场的流量和攻击仿真，护网行动的攻击演练等场景。

在如今的数字化时代，触点互动立志帮助各行业用户更好、更快、更全面、更低成本地去完成产品的开发与测试，以及设备的选型测试，给客户带来实际的价值，向世界领先的网络通信领域测试工具提供商目标迈进，愿为我国在测试工具行业早日实现国产化替代目标贡献力量。