

知 使用packet-capture 抓取设备报文比实际流量少原因

产品特性 周泽昌 2019-10-26 发表

问题描述

Packet Capture是一种报文捕获及分析特性，该特性能够捕获设备接口的入方向报文并对报文进行解析处理，便于用户分析接口接收到的报文；还可以将报文数据存储为pcap格式的文件，方便用户后续查看。

通过packet-capture local interface可以抓取接口上的入方向流量，但是实际使用过程中发现，抓取到的流量会远远小于接口实际接收到的流量。

解决方法

packet-capture local interface 实际上是抓取的接口收到并上送CPU处理的报文，普通的业务转发流量是无法被抓取到。实际应用中，若需要抓取接口流量，可以通过镜像的方式将报文复制到其他端口抓取。