恒景科技
Endace产品介绍

关于Endace

Endace始于2001年，当时作为新西兰大学的一个研究项目Endace开发了DAG™数据采集卡。它迅速重新定义了数据包捕获市场，并获得了准确、可靠数据包捕获黄金标准的声誉。

18年过去了，Endace继续为100%准确的包捕获、网络录制和高速回放设置基准。

Endace的网络记录和可见性解决方案被一些世界上最大的公司用来监控一些世界上最快、最强大的网络。

为什么选择 Endace

- 性能，可扩展性和可靠性 100%：精确的数据包捕获记录和回放，行业领先的存储密度，集中管理和延长使用寿命
- 开放式体系结构：Endace的产品被设计为去承载和集成大量的商业、开源和自定义分析应用程序，因此用户可以选择适合他们需要的应用程序。
- Fusion生态系统： Fusion合作伙伴计划使他们能够部署和集成来自世界领先的安全和性能分析公司的分析应用程序

现存挑战

- 网络带宽日益增长，主流的网络环境已升级为1G,2.5G,10G。传统网卡采集大流量环境下已经显然不能满足需求，特别是在大流量小包时容易丢包，丢包问题是网络数据采集不能容忍的问题。
- 传统网卡的工作模式 是将流量上传至主机CPU进行流量的识别与处理，大大的占用了主机的性能，影响应用层的处理能力。

面临的问题

大量丢包会造成安全管理产品失效，所得数据分析结果不准确，所得数据无法满足用户的分析需求。

系统耗费大量CPU性能实现数据包捕获，而留给自身的数据处理能力有限。

综上可知，网卡线速包捕获和零CPU占用对数据分析意义重大。能保证全线速捕获数据可确保拿到完整的原始数据，为后期的分析准确提供保障；不占用主机CPU资源，可确保机器正常运行相关应用，为客户提供全面准确的数据报告。

产品特性-回放

- DAG卡可以线速捕获和传输数据包。使用DAG卡的播放功能，可以在捕获数据包时精确地重发它们-使用捕获的数据包时间戳来确定硬件中的重发时间。流量回放速率也可以精确地按比例放大或缩小，或者可以选择特定的数据包速率或带宽。
- 通过使用精确的捕获时间来重复播放流量，分析人员可以基准测试启用新流量处理规则或更改分析工具中的处理设置对性能的影响。他们可以启用新规则，重新播放流量，并在激活新规则的情况下测量吞吐量差异。在修改生产系统之前离线进行此测试可以优化调整，同时消除或减少维护时段的需求。实际上，我们的许多客户都使用DAG卡进行这种类型的性能测试-高频交易行业中的算法调整就是一个很好的例子。

产品特性-筛选和分类

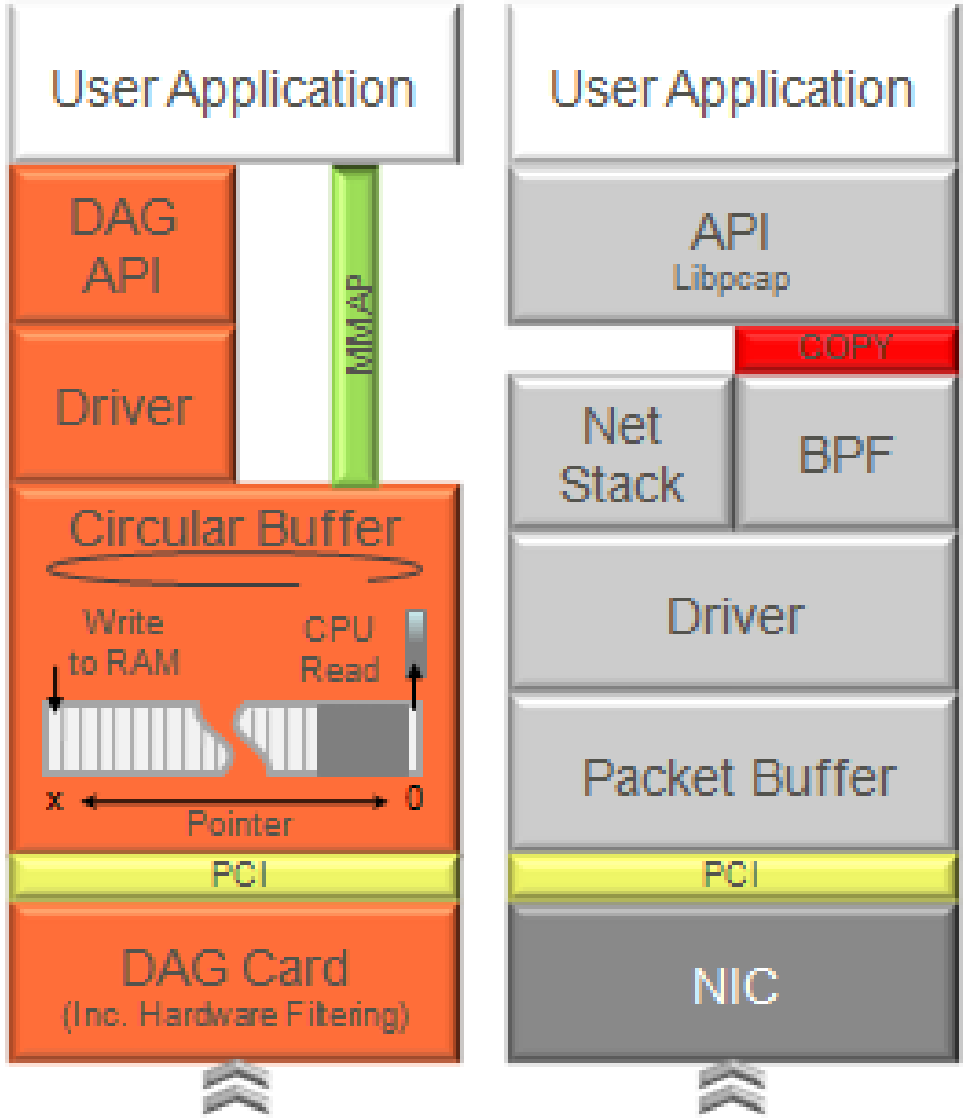
- DAG卡具有复杂的，基于硬件的过滤和分类功能，可对捕获的数据包以100％的线速运行。多个过滤规则可以应用于每个数据包。可以过滤的字段包括IPv4和IPv6地址或子网，VLAN VID，MPLS标签，TCP / UDP端口等。
- 得出的按数据包分类的值可用于过滤掉不必要的流量，或将数据包引导至按应用程序的流。在硬件中过滤掉不需要的流量可以减轻接收应用程序的处理负担，同时还可以减少存储已记录数据包所需的内存和磁盘空间。
- DAG卡还使用一组可配置的字段生成双向流，从而在零CPU开销的情况下实现了流安全的负载平衡。过滤和负载平衡可以同时运行。例如，负载平衡跨越31级个别应用程序的线程的同时将所有DNS流量复制到第32个流。

消除瓶颈

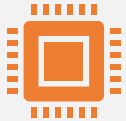
如图，为DAG卡与传统网卡抓包的工作流程：

DAG卡实现对数据的捕获，优化后上传到应用，不占用系统CPU。

而传统网卡所有的数据包捕获，分析，上传都需要与主机CPU进行数据交换复制，占用大量CPU性能，难以对付大流量。



DAG加速卡应用领域
安全产品开发



防火墙：千兆线速in-line接入方式 防火墙，提供包过滤和状态流检测功能。

入侵检测（IPS）：1G，2.5G,10G入侵检测产品开发，千兆in-line方式支持旁路BYPASS功能。

异常流量分析：采集分路器或交换机镜像流量作分析。比基于netflow的解决方案更加准确。

数据存储分析：对链路线速的数据捕获，100%全流量存储到硬盘，后期出现任何问题，对业务数据能完速再现，为事后诊断留下宝贵资料。

DAG加速卡应用领域
流量分析

DAG卡强大的网络数据采集分析能力，支持1G/2.5G/10G全线速流量捕获，

基于网络类型，源/目的以太网地址，IP5元组（源/目的IP地址，源/目的端口号,协议类型，协议标志）的流量捕获及过滤功能。

高精度的时间戳（4-7.5ns），硬件级时间（可与GPS和CDMA时间同步）为远距离延时抖动提供精准的数据。

线速流量捕获可为后期流量审计，故障定位，安全分析留下宝贵数据。

DAG加速卡应用领域
金融交易

合规性：根据大多数金融证券法（例如RegNMS，MiFID和MiFID II），高频交易者必须对涉及的每笔交易都存档高度准确的记录。

性能监控：在毫秒级的延迟可能意味着数百万美元的收益或损失的环境中，监控市场反馈和网络性能问题的故障排除是至关重要的。通过访问所有交易和提要的精确到纳米级的包级历史记录，分析人员可以快速了解微突发和延迟等问题的根源，并优化网络性能。

算法调整：优化交易算法可以使交易者获得竞争优势。有了手头完整的，纳秒级的准确贸易数据副本，分析师可以准确地重放昨天的交易，从而可以准确地调整算法。

Endace产品目录

7.4S

- 双SFP千兆接口
- 支持：SONET和 ATM.
- 100%数据包捕获到主机内存中，所有帧的从64到9600字节（包括巨型帧）。
- 8通道PCI Express总线的设计容易兼容主机平台
- 全包，包头，或设定长度的数据包捕获
- 两路CPU的负载平衡，提高处理性能与外部时间参考时钟精确纳秒包时间戳，包括同步GPS和CDMA。
- 支持在多核主机架构创建多达32个内存缓冲区，提供流的负载均衡功能
- 支持行业标准的数据包捕获格式[libpcap/ WinPcap]
- 可选的基于主机的软件支持先进的AAL2/AAL5的ATM重组在线路速率。
- 时间戳7.5ns

7.5G4

- 四个SFP千兆接口
- 100%全线速数据包捕获(至主机内存)能力，包长从64至9600字节
- 基于以下类型的全线速流量捕获和过滤能力：

  1.以太网类型；

  2.源/目的以太网地址；

  3.5元组IP包信息(源/目的 IP地址、源/目的端口号、协议类型和协议标志)；
- 非阻塞的同步捕获和发送；
- 支持在多核主机架构创建多达32个内存缓冲区，提供流的负载均衡功能。
- 零占用主机CPU利用率；
- 高精度报文时戳，时钟可与GPS同步，为远距离高精度测量应用提供支持；
- 支持标准的PCAP格式（libPCAP、WinPCAP）；
- 时间戳15ns

9.5G4

- 四个SFP千兆接口
- 100％全线速数据包捕获(至主机内存)能力，包长从64至9600字节
- 基于以下类型的全线速流量捕获和过滤能力：

  1.以太网类型；

  2.源/目的以太网地址；

  3.5元组IP包信息(源/目的 IP地址、源/目的端口号、协议类型和协议标志)；
- 非阻塞的同步捕获和发送；
- 进行数据分析,并用于报表和分析的链接、统计计数器；
- 零占用主机CPU利用率；
- 高精度报文时戳，时钟可与GPS同步，为远距离高精度测量应用提供支持；
- 支持标准的PCAP格式（libPCAP、WinPCAP）；
- 时间戳6.7ns
- 支持基于板载的硬件处理（GTP）和（GRE）协议，用于负载平衡，分类和过滤。

9.5G4F

- 四个千兆电口
- 支持串接链路，允许串接监听两条链路
- 100%全线速数据包捕获(至主机内存)能力，包长从64至9600字节
- 基于以下类型的全线速流量捕获和过滤能力：

  1.以太网类型；

  2.源/目的以太网地址；

  3.5元组IP包信息(源/目的 IP地址、源/目的端口号、协议类型和协议标志)；
- 非阻塞的同步捕获和发送；
- 支持在多核主机架构创建多达32个内存缓冲区，提供流的负载均衡功能
- 零占用主机CPU利用率；
- 高精度报文时戳，时钟可与GPS同步，为远距离高精度测量应用提供支持；
- 支持标准的PCAP格式（libPCAP、WinPCAP）；
- 无MAC、IP地址，对网络设透明；
- 时间戳6.7ns
- 支持基于板载的硬件处理（GTP）和（GRE）协议，用于负载平衡，分类和过滤。

10X2-P/ 10X2-S

- 双SFP+接口
- 支持配置为万兆或千兆
- 100%全线速包捕获到主机内存，包长从64到 9600字节
- 零占用主机CPU利用率；
- 能全包捕获、只捕获包头或捕获指定长度能力 。
- 支持在多核主机架构创建多达32个内存缓冲区，提供流的负载均衡功能。
- 基于硬件分类的数据包转发、复制、过滤。

-EndaceDAG 10X2-S - 16 条分类规则

-EndaceDAG 10X2-P – 64条分类规则

- 每一个数据包和时钟同步，从主机，外部时钟参考或专用IEEE 1588端口硬件时间戳
- 易于集成到现有的服务器的PCIe x8的3.0总线技术
- 时间戳4ns
- DAG 10X2-P支持基于板载的硬件处理（GTP）和（GRE）协议，用于负载平衡，分类和过滤。

10X4-P/ 10X4-S

- 四个SFP+接口
- 支持配置为万兆或千兆
- 100%全线速包捕获到主机内存，包长从64到9600字节
- 零占用主机CPU利用率；
- 能全包捕获、只捕获包头或捕获指定长度能力
- 支持在多核主机架构创建多达32个内存缓冲区，提供流的负载均衡功能。
- 基于硬件分类的数据包转发、复制、过滤。

-EndaceDAG 10X4-S - 16 条分类规则

-EndaceDAG 10X4-P – 64条分类规则

- 每一个数据包和时钟同步，从主机，外部时钟参考或专用IEEE 1588端口硬件时间戳
- 易于集成到现有的服务器的PCIe x8的3.0总线技术
- 时间戳4ns
- DAG 10X4-P支持基于板载的硬件处理（GTP）和（GRE）协议，用于负载平衡，分类和过滤。

谢谢

恒景科技