通过 AEON 包代理实施 TAP 聚合

简介

为打造稳健的任务关键基础架构，流量监控逐渐成为关键基础环节。流量监控通常用于故障排除、安全防护和容量规划，有时为了满足监管标准而必需实施流量监控。很多不同的环境都会用到监控功能，从企业存储到媒体和娱乐、CDN、移动和电信 NFV 皆不例外。

流量持续激增，现有的封闭式监控解决方案无法在合理的成本和规模下满足需求。AcceleratEd Open Network (AEON) 包代理结构由多种高性能、开放式、标准化组件构成 – Mellanox Spectrum 以太网交换机、开源可视化工具、开放式 SDN 控制器以及可供控制器与交换机开展通信的各种开放式编程接口。

AEON 包代理结构

AEON 包代理结构通过在包代理模式下配置的 Mellanox Spectrum 交换机构建。在这种模式下，标准交换/路由功能被禁用，Spectrum 用于选择性过滤、复制、处理包，并将包从生产网络传输至各种工具执行进一步分析。值得注意的是，包代理功能拥有内置基础系统，无需额外获取许可证即可启用这项功能。此外，结构策略和运行均通过集中控制器进行控制。

AEON 包代理功能本身可分为三层（见图 1）：

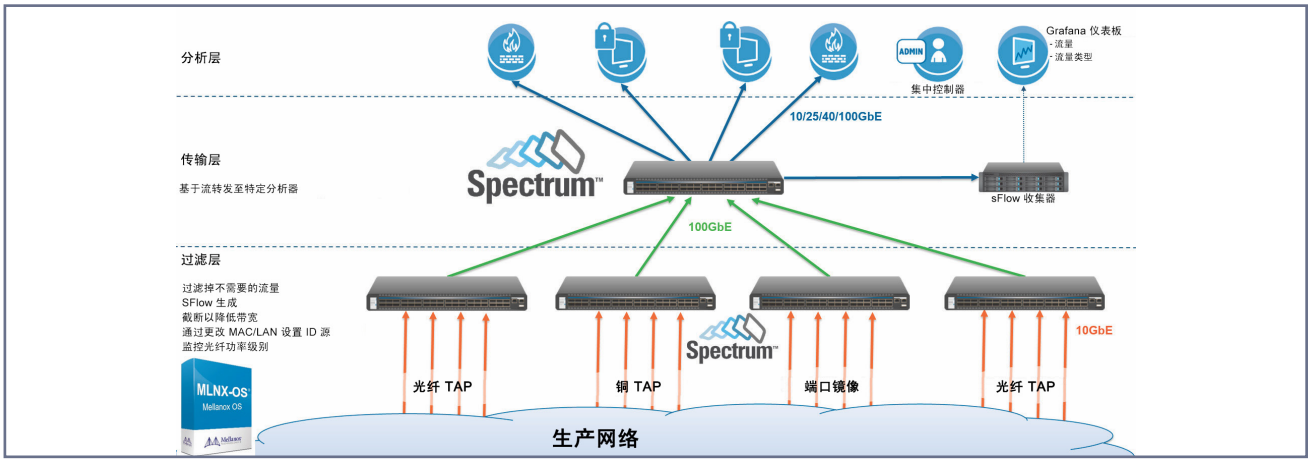

图 1：Mellanox 监控结构

*仅作说明用途。实际产品可能有所不同。

过滤层

过滤层的主要目的在于选择需要分析的流量部分，并将这部分流量发送至传输层。未被过滤层选中的流量将被丢弃。过滤层是包代理结构的第一层。这一层可直接识别流量源。随后可将源标识编码到包的 MAC 或 VLAN 字段，进而选择性地将源标识嵌入包中。在这项功能的帮助下，传输层和分析层可将生产网络流量源上下文嵌入每一个包中。

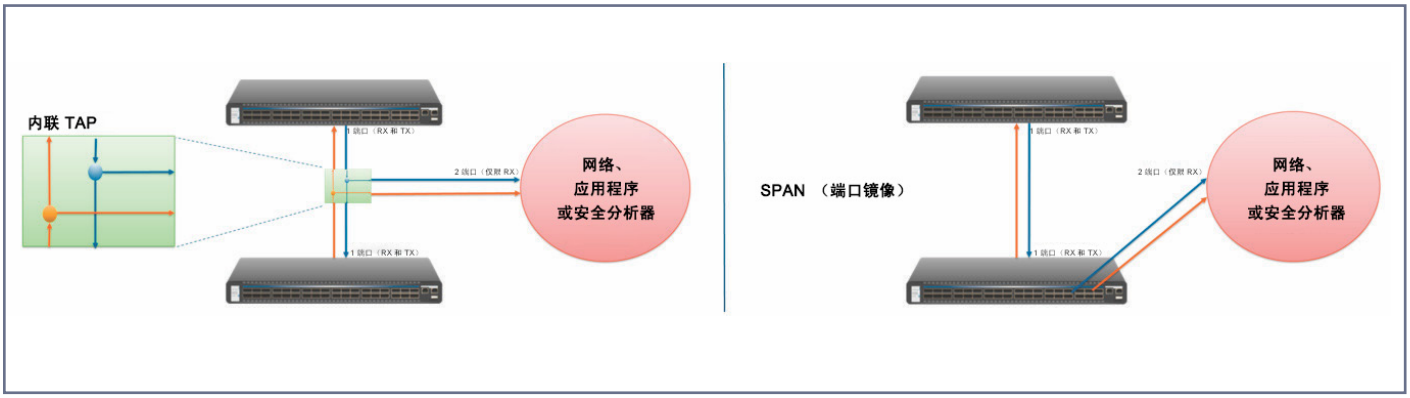

图 2：内联 TAP 或镜像端口可用于从生产网络获取流量

过滤层获取通过光纤/铜 TAP 或镜像端口从生产网络窥探的流量。如果使用 TAP 窥探链接，则必须将窥探链接的接收部分和传输部分单独连接到两个不同的 Mellanox Spectrum 交换机端口，并在仅接收模式下运行（见图 2）。除提供过滤功能外，Mellanox Spectrum 还可以监控光纤 TAP 的功率级别。

过滤层可以在硬件中运用 sFlow 采样技术深度监控生产网络状态。而且还能将 sFlow 数据发送至开源收集器进行分析，并展示流传输排行、用量排行、协议排行、每应用程序流排行以及各种流量异常。不仅可以检测网络问题，还能综合展示哪些应用程序占用的网络资源最多。同时，还会在出现重大更改时发出警报，并确定应当发送哪些流执行进一步分析。

传输层

传输层的主要目的在于执行基于流的一对一或一对多包转发，发送到分析层中的一个或多个分析器。传输层可聚合过滤层流量，根据需要实现流量负载均衡，并将流量传输至分析层。

分析层

分析层由各种分析工具构建而成，每一种分析工具接收生产网络中生成的不同数据流，并且支持不同的监控功能，如安全、应用程序性能测量、网络性能验证及 SLA 符合性。

AEON 包代理的主要功能

通过 Spectrum 执行增强型包过滤

随着网络虚拟化和隧道协议的广泛采用，传统网络监控平台的性能受到挑战。Mellanox Spectrum™ 交换机配有灵活的内置解析器，可对其进行配置，提取数据包内深度达 500B 的包字段。这在处理隧道封装包方面特别有用。Mellanox Spectrum 不仅可以保留外部标头上下文，同时还能对标头的内部字段进行匹配。有了这项功能，Spectrum 可以提供丰富的过滤功能，甚至对叠加 (Overlay) 和隧道流量也不例外。

包代理结构必需可扩展，而且应能够支持大量规则，从而利用这些规则提供丰富的过滤功能。Mellanox Spectrum 交换机具有灵活的 ACL 块，最多可以支持 18,000 项过滤规则。这款灵活的 ACL 引擎可以对各种标头字段进行匹配，包括 TTL、SRC/DST MAC、VLAN ID、VLAN PCP、IP DSCP、IP ECN 等。而且，还能将单个或多个包副本转发至一个或多个目标。

通过 Spectrum 执行高级包头编辑

包代理结构应当能够根据特定用例执行包转换。借助强大的包编辑功能，Mellanox Spectrum 交换机可以：

- 通过修改包的 MAC 地址和 VLAN 字段嵌入生产流量源信息
- 通过编程方式去除 VLAN 标记和隧道封装，以便分析工具仅处理内部负载
- 截断包，从而节省带宽以加速上游数据包分析器设备运行
- 选择性使用故障 CRC 传输包以执行进一步分析。

Spectrum 智能负载均衡

包代理结构可能需要对多个分析工具实例实现流量负载均衡。根据运用一组灵活的可编程包头字段计算得出的哈希，Mellanox Spectrum 交换机可以实现流量负载均衡。

某些分析工具（如 Intrusion Detection Systems (IDS)）需要接收双向流量，从而识别握手和更高级的事务。Mellanox Spectrum 交换机支持对称哈希，确保将流特定双向流量发送至同一物理分析设备。

灵活的控件选择

AEON 包代理结构属于开放式结构，可随意选择通过 CLI、Python 脚本、OpenFlow 1.3、Web GUI 和 REST API 进行编程。Mellanox Spectrum 交换机可以托管运行第三方代理的容器。容器对数据路径具有完全 SDK 访问权限，为用户提供新型交换机功能，构建自定义网络应用程序。Mellanox 监控结构可以轻松集成至现有的业务流程和自动化框架。还可使用下列控制器控制 OpenFlow 1.3 实施：ODL、ONOS、RYU 等。

灵活的尺寸规格

Mellanox 提供了各种灵活而又可扩展的交换机产品，分为不同的尺寸规格，适用于各种 IT 基础架构和拓扑：

图 3：SN2700 - 32x100GbE (64x50GbE)

图 4：SN2410 - 8x100GbE + 48x25GbE

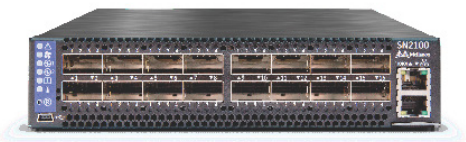

图 5：SN2100 - 16x100GbE

Spectrum 交换机提供半宽和全宽两种尺寸规格。半宽 SN2100 交换机支持 16x100GbE 端口，适合成本/功率限制较为严格的客户机架。SN2700 是一款高密度 32x100GbE 脊交换机。SN2410 支持 48x25GbE 和 8x100GbE 端口。所有 Spectrum 平台均支持对各种规格的包执行线速包处理。

表 1：Mellanox 与竞争对手产品的主要结构功能比较

功能特性	Mellanox	Arista	Big Switch	Gigamon
开放的可编程性	✓	✗	✗	✗
线速 100GbE 包捕获	✓	✗	✗	✗
1GbE/10GbE/25GbE/40GbE/100GbE 支持	✓	✓	✓	✓
过滤/聚合/ 复制/负载均衡	✓	✓	✓	✓
服务层（带时间戳功能）	✓	✓	✓	✓
对称哈希	✓	✓	✓	✓
交换机支持容器且具有完全 SDK 访问权限	✓	✗	✗	✗
保留包错误的选项	✓	✗	✗	✗
深层包匹配 （包匹配高达 500B）	✓	✗	✗	✗
半机架宽尺寸规格平台	✓	✗	✗	✗
自带监控结构，无需许可证	✓	✗	—	—

结论

网络数据流量持续激增，当前网络监控解决方案在规模、性能和成本效率方面将无法满足需求。亟需采用基于以太网的高性能开放式监控解决方案。Mellanox Spectrum™ 开放式以太网交换机兼具灵活的过滤功能、高级包编辑功能和高性能数据路径，堪称 TAP 聚合及网络监控用例的理想之选。AEON 包代理结构采用 Spectrum 开放式以太网交换机构建，不仅可以运用 CLI、REST API 或 OpenFlow 1.3 等方法进行编程，还能轻松集成至现有的业务流程基础架构。Mellanox Spectrum 支持所有这些功能，无需额外获取软件许可证。

关于 Mellanox

Mellanox Technologies（NASDAQ：MLNX）是针对服务器、存储和超融合基础架构的端到端以太网和 InfiniBand 智能互连解决方案和服务的领先提供商。Mellanox 智能互连解决方案可提供最高吞吐量和最低延迟，更快地向应用程序传递数据并充分发挥系统性能，从而提高数据中心效率。Mellanox 提供一系列高性能解决方案：网络和多核处理器、网络适配器、交换机、线缆、软件和芯片，它们可针对广泛的市场（包括高性能计算、企业数据中心、Web 2.0、云、存储、网络安全、人工智能、电信和金融服务）加快应用程序运行时间并最大程度实现业务成果。www.mellanox.com 上提供了详细信息。

北京市朝阳区望京东园七区保利国际广场 T1 15 层
电话：010-5789 2000
www.mellanox.com

53815SB 修订版 1.0