基于 UDPI 构建应用感知的网络

2020 年 4 月 30 日 SDNLAB 一期一会 第 7 期

一、会议主要内容

1. 会议主讲者：倪红军，英特尔的资深工程师

2.会议主要内容

1）应用驱动网络；

2）UDPI 的整体框架；

3）关键技术实现和典型应用解析；

4）UDPI 在 SDWAN 和 5G 中的应用；

5）与人工智能和 Tofino 芯片的融合。

3.UDPI 是什么？

首先，简单介绍 UDPI 是什么？

UDPI (Universal Deep Packet Inspection) 项目旨在基于 VPP 网络栈（什么是 VPP 呢？参见 https://zhuanlan.zhihu.com/p/40049446），为**深度报文检测**功能提供一个高性能的参考框架，是 FD.io 社区的一个子项目。UDPI 利用业界领先的正则匹配库 Hyperscan，提供一系列丰富的功能，被广泛应用于入侵预防系统、入侵检测系统、网络防火墙等产品。同时它也能被集成到如 5G、边缘计算、云网络中，提供基于应用识别的服务。UDPI 20.01 是 UDPI 项目发布的第一个正式版本，提供了流分类、TCP 分段重组、应用数据库、应用识别等功能，支持 TLS/HTTPS 协议。（项目开源链接参加文末）

4.为什么需要应用感知网络？

在传统的网络中，应用程序和网络是分离的，应用程序和网络的依赖性比较少。但是随着云计算、云网络的广泛应用，应用程序虽然有了更好的灵活性，但是也更依赖于底层网络来提供更好的底层服务，如更高的性能、更低的时延等更好额 QoS 特性来满足用户不同的需求。所以我们现在就会希望可以构建网络，能够感知上层的应用程序，在传统的网络中，虽然有一些 QoS 服务，但是通常对于上层的应用程序都是平等对待的，没有区分，也就是说没有去感知我们上面究竟是什么应用程序。所以，现在我们需要去感知不同的应用程序，并赋予不同的优先级，更好的来满足应用对带宽，充分利用网络的特性来给应用程序提供更

大的价值。

5.UDPI 的软件架构

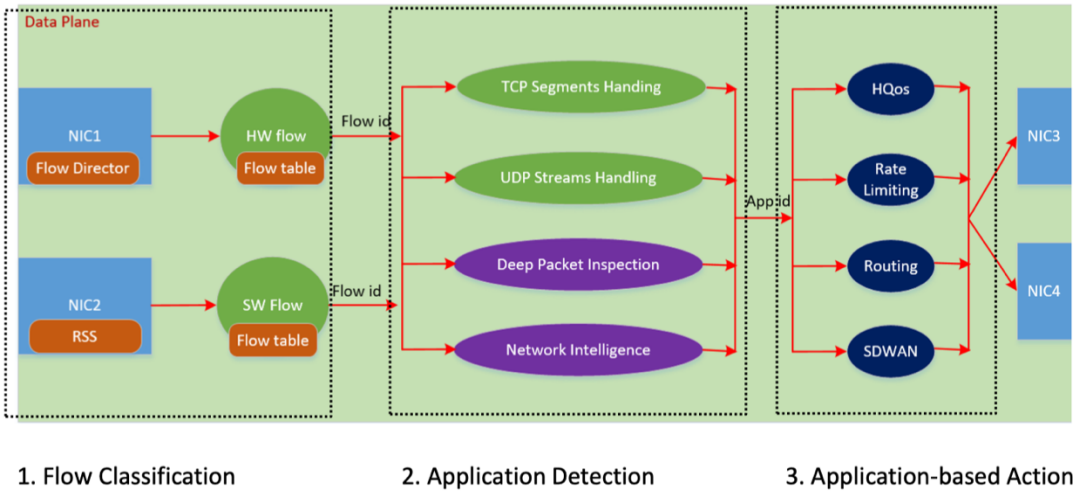

图 1

如图 1，第一部分是流分类和老化机制，第二部分是应用程序检测，第三部分则是根据检测出的不同程序，采用相应的措施。

1）流分类。对于一个新到的流，会创建一个软件的流表，如果底层硬件具有流分类的功能，此时就会同时将流表下放到硬件的 flow director，从流表中匹配到，就会带上一个 flow id 然后传入第二部分应用检测。

2）应用检测。首先包含两部分的预处理功能，对于 TLS 等协议，会对其下层的 TCP 协议进行一个分段重组等处理，对于 QUIC 等协议则是基于 UDP 协议进行一个流排序等处理。预处理之后就会进行一个深度报文检测或网络智能，对于明文流，基于 Hyperscan 进行七层内容的深度扫描；对于 TLS1.2 之后、QUIC 等加密协议，会采用机器学习来训练模型，进行加密流的识别。最后会识别得到一个 app id，然后进行第三阶段。

3）基于不同应用采取措施。如层次化的 QoS、限速、策略路由、SDWAN 等功能。

根据用户需求，用户希望 UDPI 有一个独立可用的 library，所以就有了如图 2 所示的 library。也是类似上面说的三个功能阶段，封装成了 library，包括流处理的 flow_proc.lib，协议处理 proto_proc.lib，以及基于 hyperscan 的规则匹配 rule_manager.lib，这些 library 用户可以选择一起使用，也可以选择只集成其中的某几个 lib。该方案可以支持对明文和加密流量的应用程序识别，并支持对

XSS 和 SQL 注入等异常流量检测。我们对外提供 TADK 开发包，对核心功能以库的形式提供，客户可以有选择的集成这些功能库到他们的产品中。

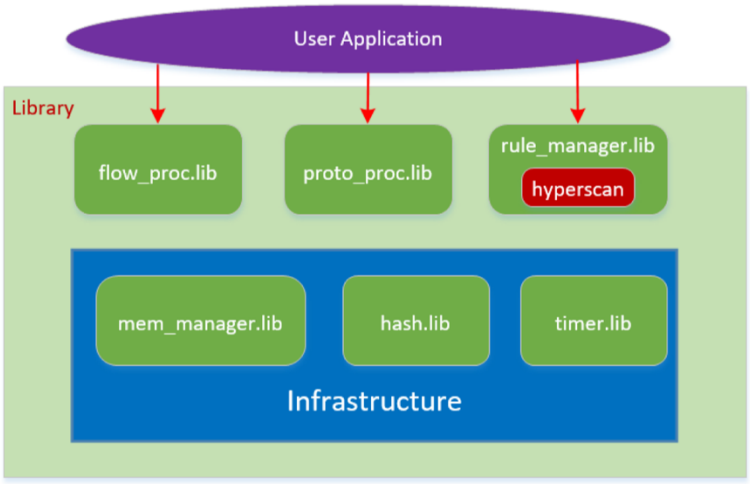

图 2

6.UDPI 的主要功能

1）流分类和老化机制

硬件流卸载，利用 DPDK 中的 rte_flow 机制；超过硬件卸载能力的流，采用软件的流分类功能，那么不管是硬件还是软件，都有老化机制，来老化流表中不太使用的流。

2）基于应用程序的检测

利用 Hypersacn 来提高整体的扫描性能，还包括对 TCP 流分段进行重组去重等操作。

3）对于不同应用程序的上层操作

HQoS、限速、策略路由、SDWAN 等。

4）目前支持的协议和应用

TLS1.0、1.1、1.2，HTTP，HTTPS，DTLS1.0、1.1、1.2，DNS，QUIC 等协议。

7.UDPI 应用于 SD-WAN

如图 3，用 UCPI 即成 uCPE 和 vCPE，在 uCPE 中是 leaf DPI，在叶子 DPI 会对所有进入的包进行扫描，如果成功，就会输出相应的 App id，然后可以给予 App id 进行 WAN 链路的选择，比如对带宽需求大、时延不敏感的应用，就直接通过以太网链路放到上行的 vCPE，如果是对带宽需求小，时延敏感的，可能就

会采用 wifi 或者 5G 等方式送到 vCPE 上去。在 vCPE 一侧，会集成为枝干 DPI，Spine DPI，对下行流进行检测，对检测出来的 app id 选择不同的下行链路，到 uCPE 上去。

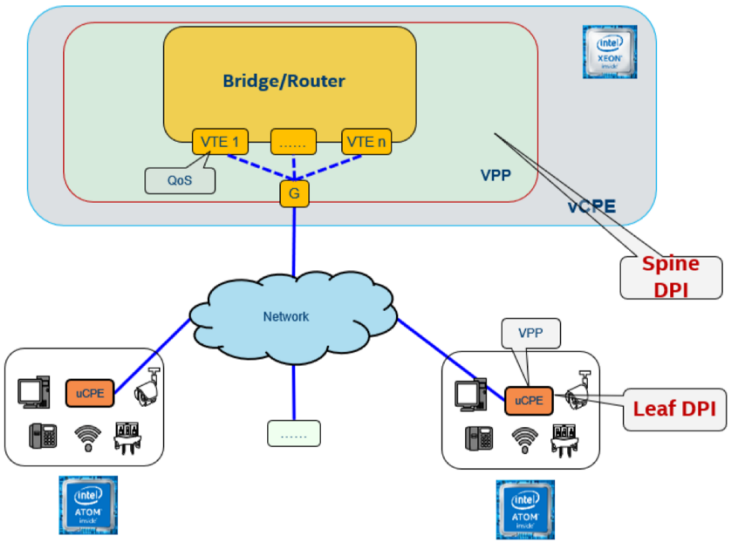

图 3

8.和 tofino switch 芯片进行集成

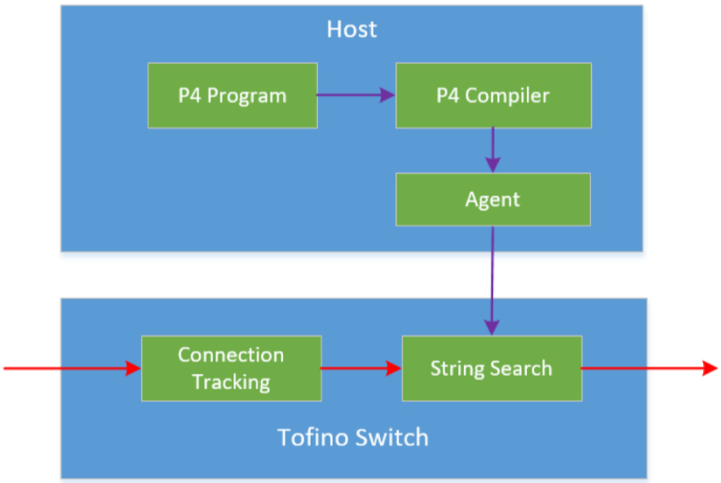

图 4

Tofino 的交换芯片带宽在 Tbps 以上，所以想用其强大的并行处理能力进行一个扫描。在数据面，包含了对流的分类，流跟踪，流搜索等功能，在控制平面，包含了 P4 程序、编译器，编译器会将定义的搜索模式转化成确定有限状态机（DFA），然后将 DFA 转化成一个 match-action 的流水线，那么当流量来的时候

就会通过 tofino 强大的并行能力进行扫描。

9.其他 use case

1）5G

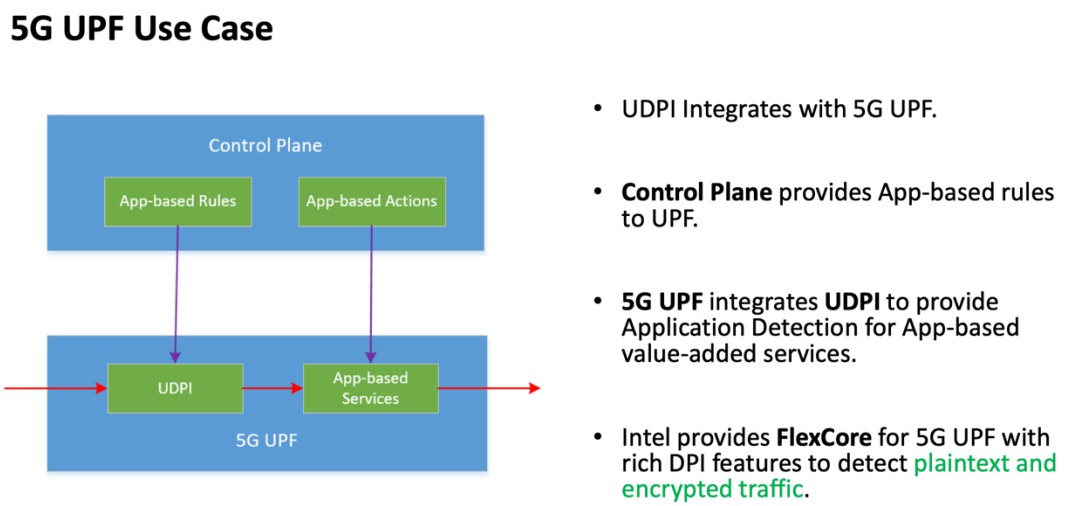

图 5

2）机器学习

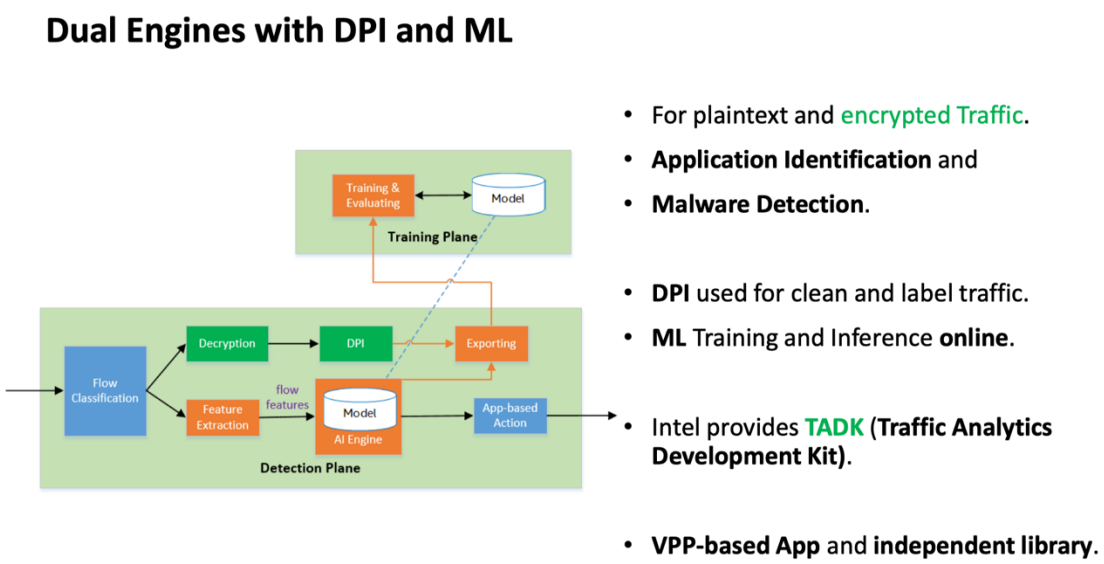

图 6

二、会议信息

参考链接：

会议 PPT：链接：https://pan.baidu.com/s/1l8_8RJNNxqhqM67dZzEDzA 密码：jmfd

会议直播：https://www.bilibili.com/video/BV1d54y1C75s

UDPI 项目主页：https://wiki.fd.io/view/UDPI

UDPI 邮件列表：udpi-dev@lists.fd.io

加入 UDPI 邮件列表：https://lists.fd.io/g/udpi-dev