HongKe 虹科

OMNIA

NetFlow / IPFIX / DPI 探针

10. 2020

HongKe 虹科

丰富的IPFIX DPI 输出设备

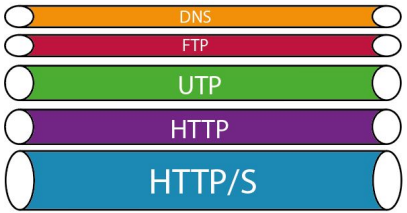
基于流的监控是出于性能和安全目的而监控网络的一种常见方式。一般的网络设备能产生这样的流，然而由于性能限制，通常效率很低。不仅性能会受到影响的，而且还有一个另外的问题，即网络设备缺乏提供DPI信息的能力。这一点越来越重要，因为流量可能在非标准端口上运行，而且这些流量可能是加密的。正因如此，像HK-Cubro Omnia平台这样的外部工具就变得非常有用。

DPI丰富的IPFIX元数据导出为SEC和DEVOPS团队提供卓越的信息，为决策和网络维护/规划提供更多的情报。

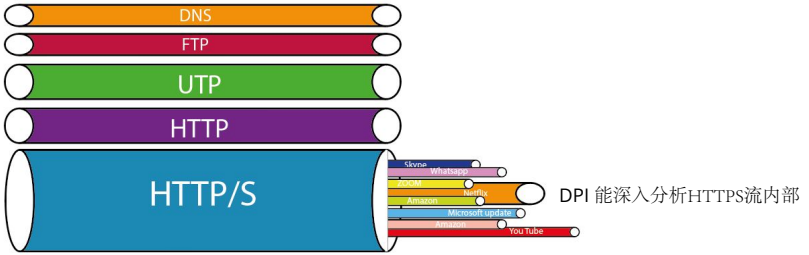
HK-Cubro只提供Netflow导出器，收集器可以是客户选择的或已经拥有的任何平台。市场上有很多商业和开源的采集器产品。 器产品

HK-Cubro DPI 解决方案

深度数据包检测(DPI)和IP流量监控是经常使用的网络监控方法。虽然DPI提供了应用的可视性，但对每个数据包的详细检测需要大量的计算。IP流量监控通过只处理包头来实现高性能，然而，它从根本上来说提供的流量本身的细节较少。应用感知流量监控的提出，是为了尝试做到结合DPI精度和IP流量监控性能。然而，这种方式的影响、优点和缺点是什么？应用流程监控的研究还没有深入。本文旨在试图弥补这种研究的缺乏。我们还提出了一种用于应用监控的下一代流量测量方法。流量将代表应用协议内的事件；比如，下载一个网页而不是下载数据包。最后，我们将研究不同的应用分类方法的性能并考虑到应用解析计算的复杂性。



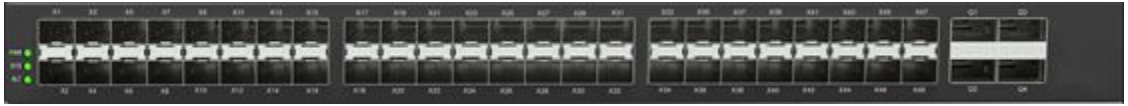
IPFIX



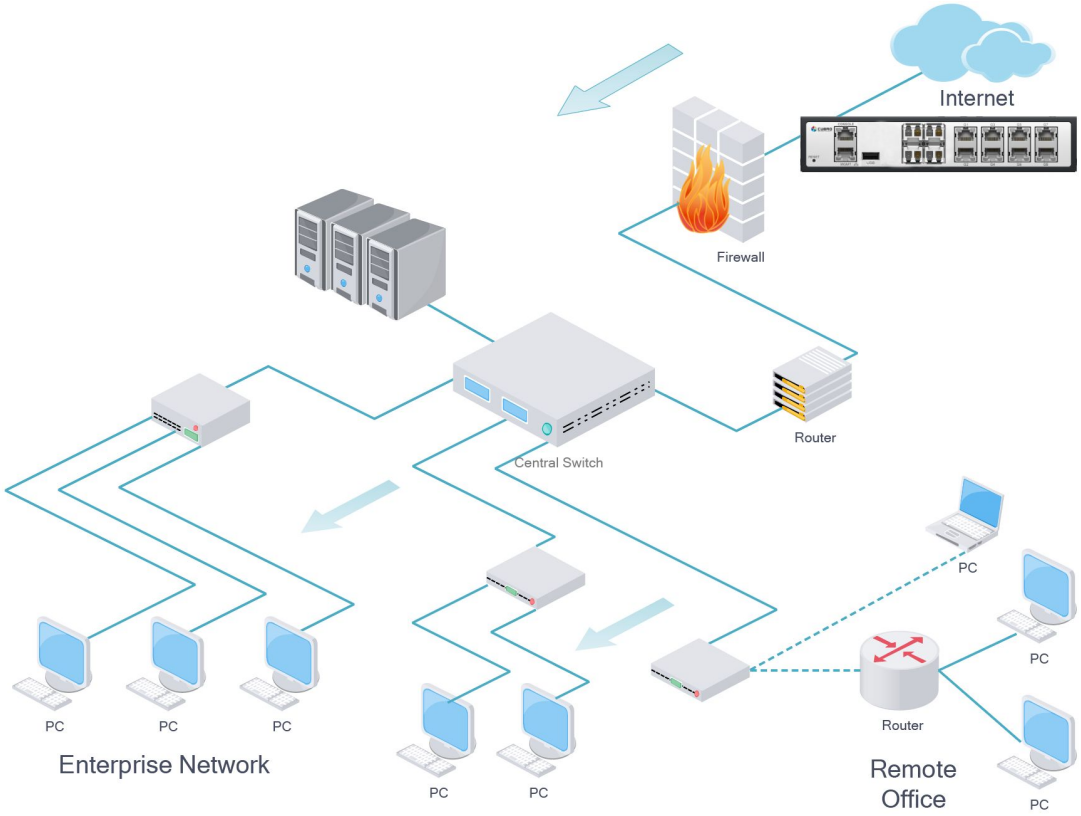
带DPI的IPFIX

HK-Cubro Omnia 企业网络可见化节点

先进的 NPB & Flow & DPI 一体化设备

Omnia 10		含4路铜链路TAP
Omnia 20		含4路铜链路TAP
Omnia 120		48 x 10 Gbit 4 x 100 Gbit

Omnia 10 & 20 应用示例

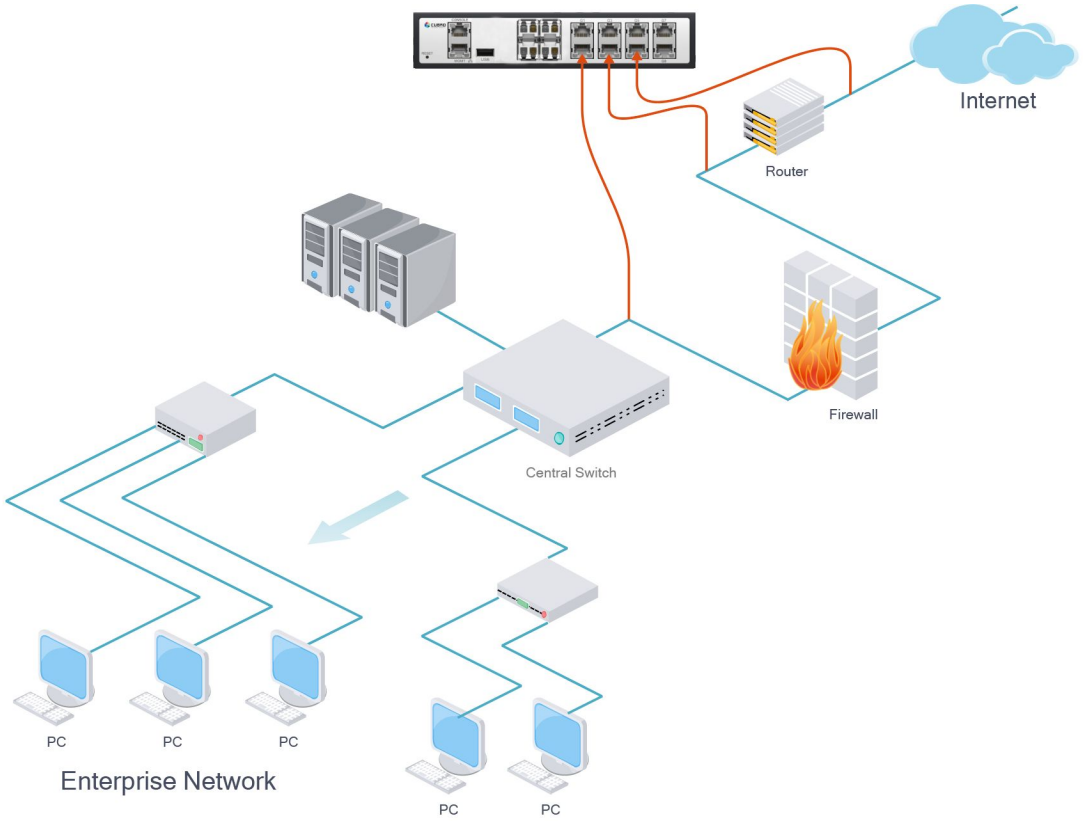


Omnia设备将安装在广域网的上行链路上，以监测和保护广域网网络。

根据所选择的软件，多种功能可供选择。

- DDoS 检测
- DPI
- 数据包捕获捕获
- APM
- 安全监控监控

多段应用



Omnia设备最多支持四条链路作为输入，并通过旁路保护它们，以确保故障安全运行。因此，我们最多可以监控一个网络的四个网段。

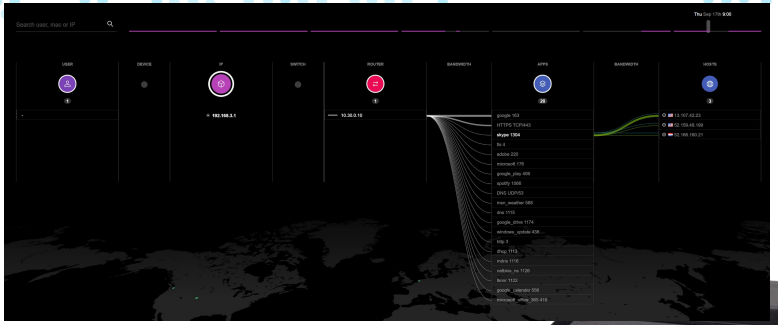
图中显示了Omnia 20在防火墙和路由器前后监控流量的情况。

利用这三条线路的数据，我们可以监控防火墙和路由器的性能。

Omnia的优势是TAP、集合器、Netflow生成器和DPI集成在一个小设备单元中。

Omnia 体积小，功耗小，成本小!

Omnia 10 & 20 典型应用



收集器是一个基于x86的服务器设备，其软件可以将接收到的元数据呈现出来。

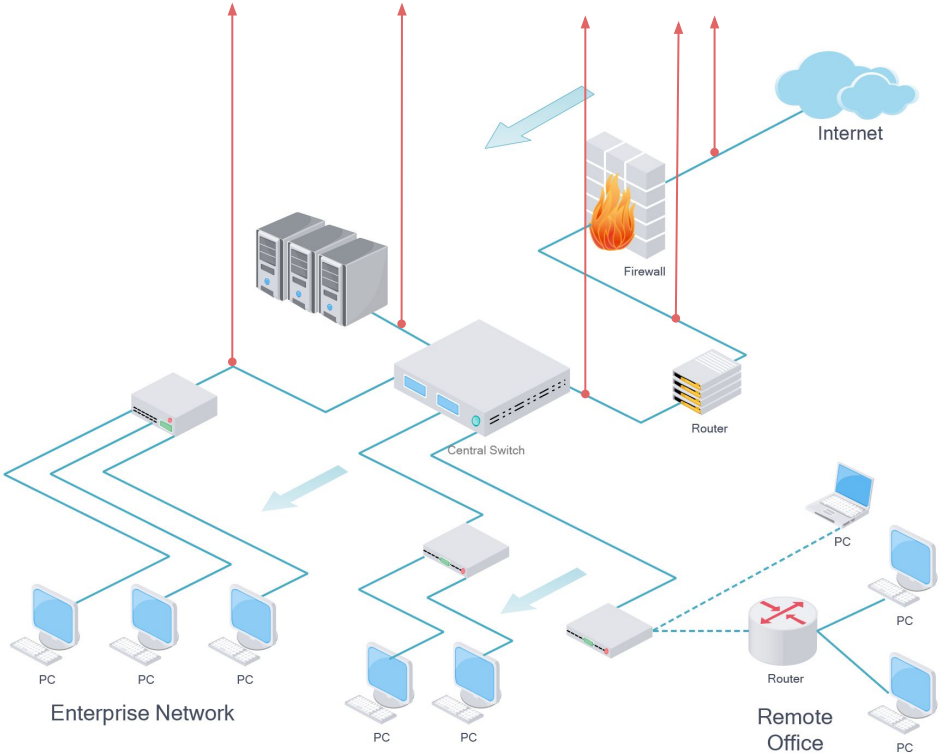
HK-Cubro并没有自己的采集器软件，我们和很多不同的厂商合作，给客户提供他们最喜欢的界面。

市场上有很多收集器，有商业的，也有开源的。

一个组合式19' 1U托盘

4路流量

Omnia 120 平台典型应用



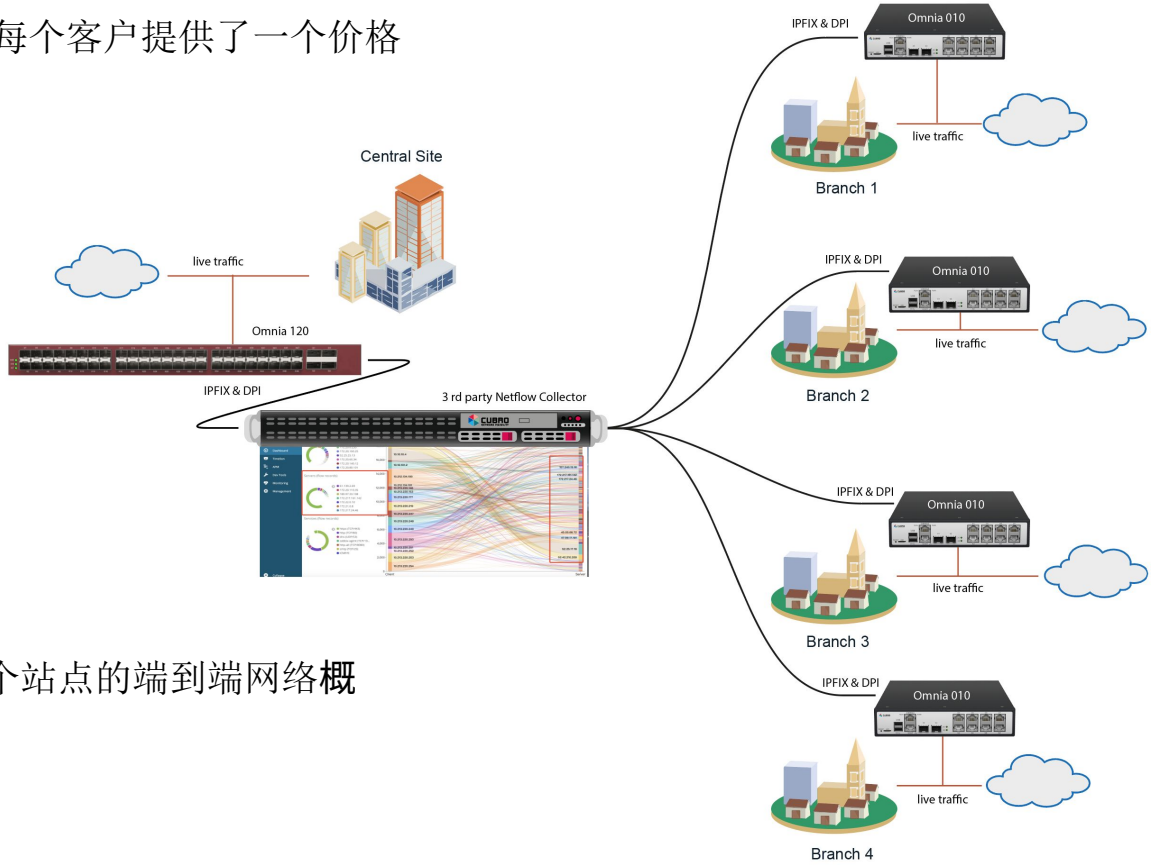
Omnia 120将连接到网络中的所有相关链路以监视和保护网络。

根据所选择的软件，多种功能可供选择。

- DDoS 检测
- DPI
- 数据包捕获
- APM
- 安全监控

典型的多站点应用

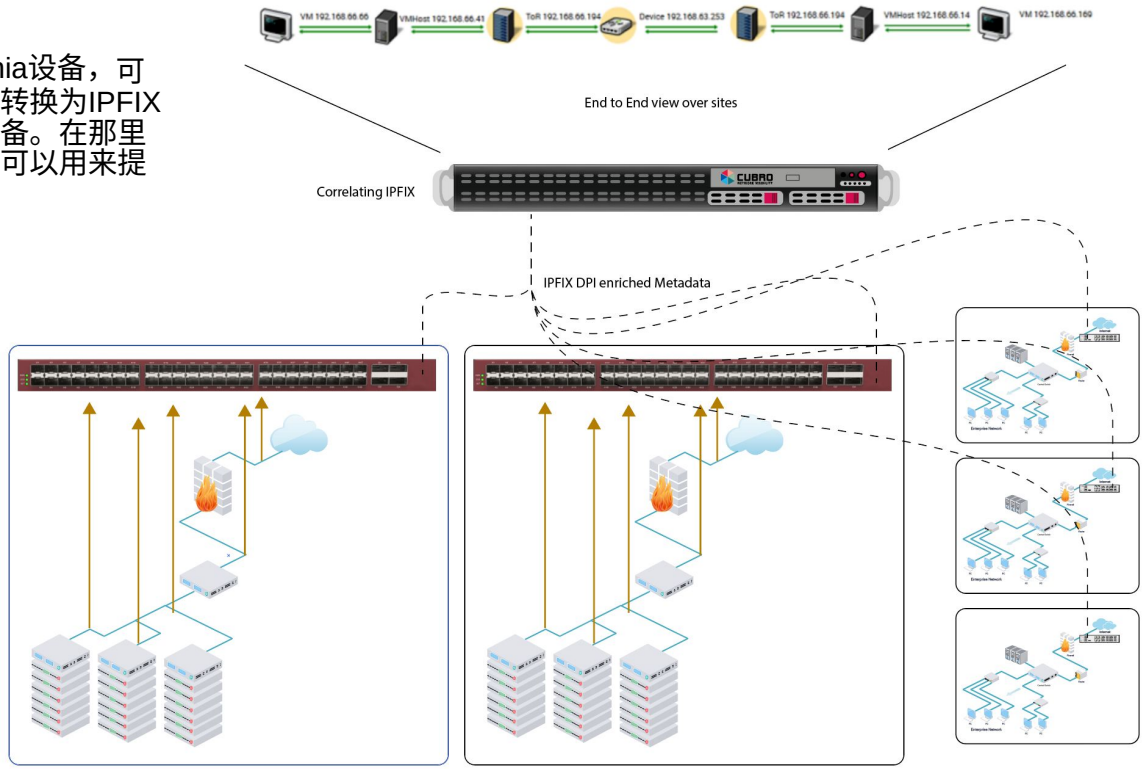
小型和大型设备的组合为每个客户提供了一个价格有竞争力的解决方案。



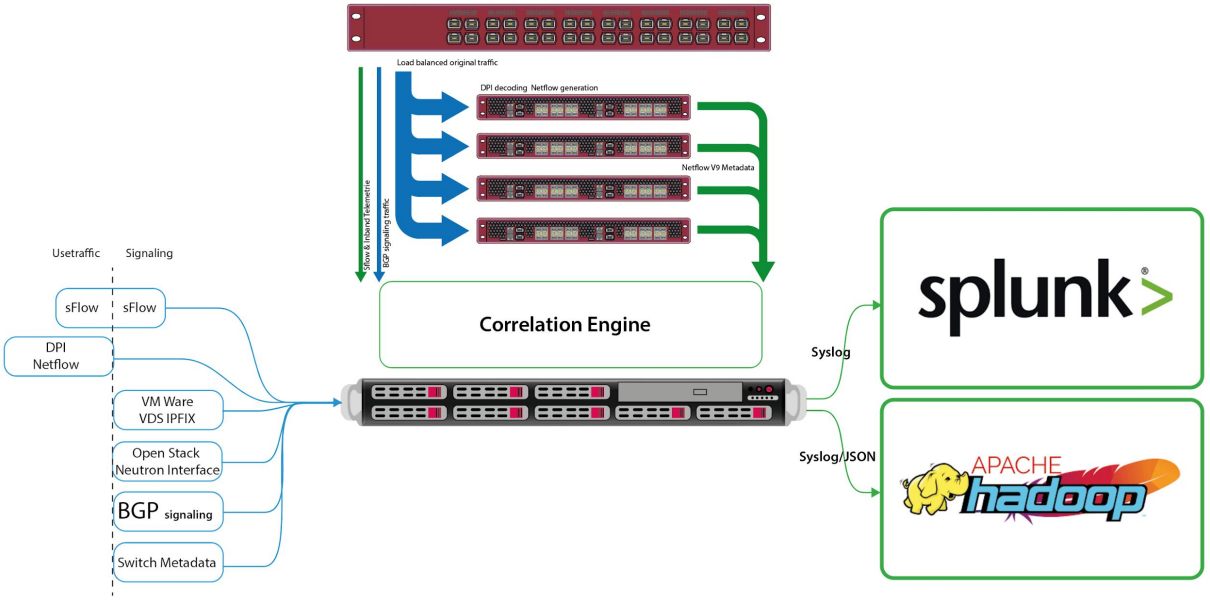
此解决方案提供了跨多个站点的端到端网络概览。

多站点端到端关联解决方案

每个站点都有一个Omnia设备，可以收集原始数据并将其转换为IPFIX流。流被发送到关联设备。在那里，信息是相互关联的，可以用来提供网络的端到端视图。



基于IPFIX和DPI的数据中心监控方法



- 去除并关联流过链路的流量
- 根据底层传输信息关联流量
- 基于BGP的结合流/路径
- 用交换机带内遥测数据丰富数据
- 用交换机表信息丰富数据

网络路径检测

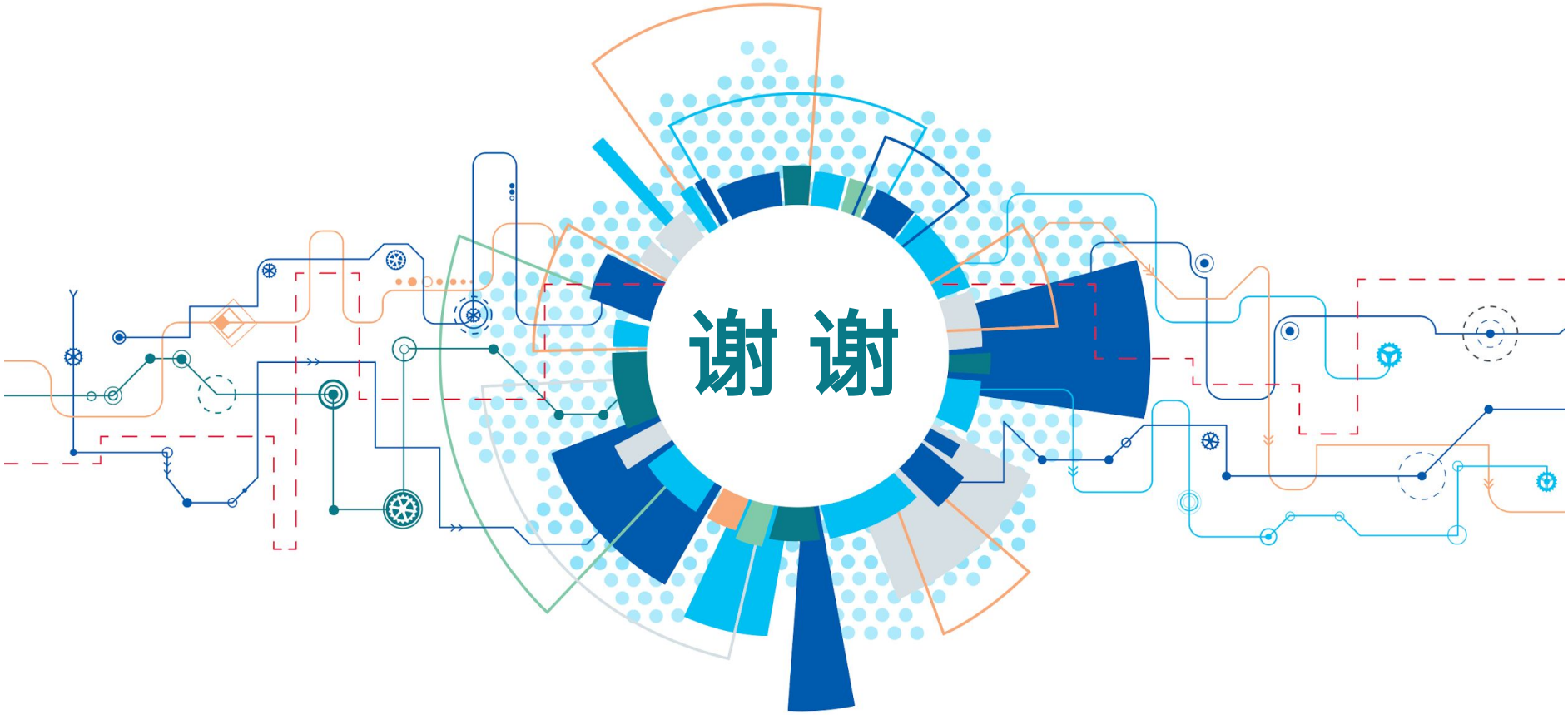
网络路径：现在已经确定了受物理网络中断影响的应用程序和主机，SDDC管理员可以选择末端节点以查看VM到VM通信的封装位置，并可以具体查看哪个物理网络交通通过的备。

现在SDDC管理员可以查明路径中网络设备的应用程序的性能问题。下图显示了VM到VM通信中涉及的网络设备接口。

对于中继跟踪通信的接口，以下信息展示了：

- 此接口上的相对流量负载占其标称容量的百分比
- 此接口上的相对数据包速率，作为在当前平均数据包大小下可持续的最大包速率的百分比
- 选定时间间隔内在每个方向上通过此接口的总数据包数
- 选定时间间隔内在每个方向上通过此接口的总字节数

路径信息不仅可用于数据中心内的VM-to-VM（东西向通信），还可用于VM到网关（南北通信）。此功能在识别网络拥塞和异常活动时非常有用比如数据过滤。



HongKe 虹科

关注我们

hongwangle

广州虹科电子科技有限公司

需要详细信息？请通过sales@hkaco.com

联系我们 | 电话: 400-999-3848办事处：广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国