

技术摘要

具有 SLA 保障的 ARUBA SD-WAN 动态路径控制

基于策略的应用程序监视与控制

简介

Aruba SD-WAN 的动态路径控制 (DPS) 功能可监视并提供一种简单的方式来控制分布式企业内多个 WAN 上行链路的网络流量。分支机构在传统上使用具有 SLA 保障的 MPLS 链路；然而，随着分支机构对互联网带宽的使用越来越多，组织必须在网关上部署 DPS 策略，以便确保卓越的用户体验，同时适应不断变化的广域网状况。

DPS 基于丢包率、延迟、抖动、带宽利用率等广域网链路的性能测量值实现上述能力，这些测量值会根据广域网链路每数秒更新一次。随后，DPS 策略便可为特定用户、应用程序、角色和目的地决定最能满足 SLA 需求的广域网上行链路，从而智能操控这些链路上的流量。这可确保所有的应用程序流量都可以通过最能满足其需求的路径进行传输。

此外，DPS 允许网络管理员根据上面提到的广域网链路特性为应用程序制定服务水平协议 (SLA)；网关将会根据是否满足 SLA 条件来选择一个可用路径。选定的转发路径可以是一个广域网上行链路，也可以是一组负载平衡的广域网上行链路。负载平衡算法是以加权轮询、会话数量或利用率为基础的。

主要优势

- 整个企业广域网流量的可见性和控制
- 全面实施广域网服务水平协议 (SLA)
- 根据基于角色的策略为用户、设备和应用程序选择路径
- 根据广域网链路的实时健康状况智能选择路由
- 根据加权轮询、带宽利用率和会话数量实现链路负载均衡
- 支持私有 MPLS 电路、高速互联网和 LTE
- 能够将应用程序和特定角色的流量映射到最合适的广域网链路

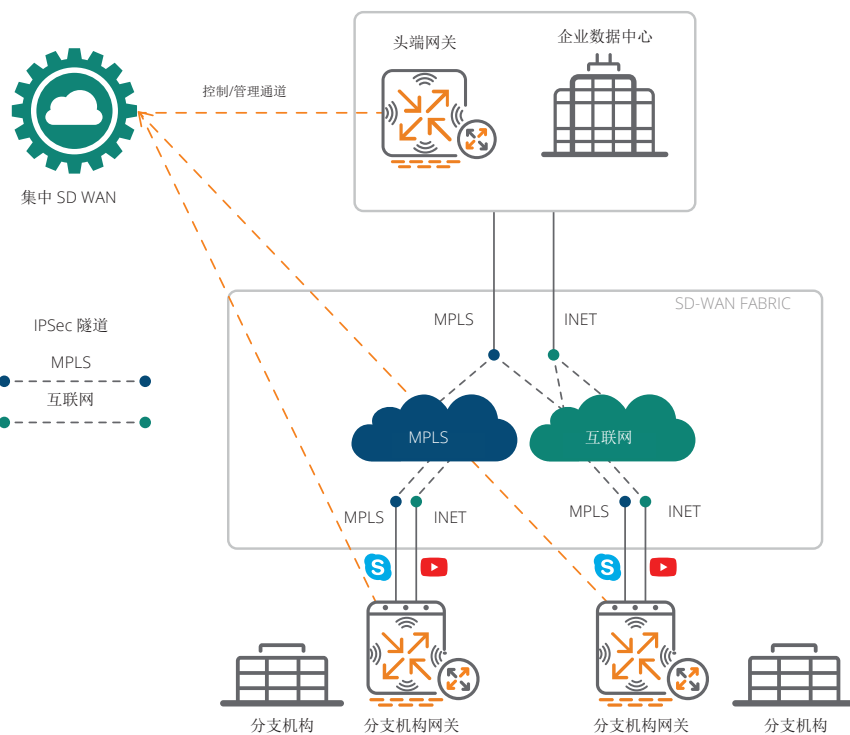


图 1: 不同链路类型上 VoIP 和流媒体流量的默认情形

DPS 情形示例

在以下情形中（图 1），有两个分支机构正在使用多个上行链路：VoIP (Skype) 流量默认发送至 MPLS 上行链路，YouTube 流量默认发送至互联网上行链路。

在下面的屏幕截图中（图 2），我们可以看到一个示例，其中 MPLS 链路无法完全满足在 SLA 中要求的链路质量。由于不满足 SLA，语音流量被切换至互联网链路进行发送。

如果 MPLS 链路不符合 Skype 流量的 SLA 要求，该链路将被重新定向至互联网链接。



图 2: 分支机构上行链路的合规性摘要

探测和测量路径质量

为衡量广域网链路质量，Aruba 分支机构网关将探测已安装的 Aruba 头端网关（测量通过 SD-WAN 叠加隧道传输的应用程序的延迟、丢包率和抖动）或者利用 Aruba 路径质量监视服务 (PQMS)探测通过底层网络进行传输的应用程序质量。PQMS 是一个分布式全球探测响应系统，可用于测量 Aruba Central 所管理的 Aruba 分支机构网关的上行链路的质量。

这项全球服务的服务站点 (PoP) 如下：

- 美洲：北美洲和南美洲
- 欧洲、中东和非洲：欧盟
- 亚太地区：澳大利亚、中国和亚太地区

为防止拒绝服务 (DoS) 攻击，我们会配置此探测响应系统，以限制来自 Aruba Central 管理的分支机构网关之外的任何查询。在通过PQMS定义上行链路的健康状况后，Aruba 的 SD-WAN 解决方案实现了对头端网关 (VPNC) 和分支机构网关所有上行链路的探测和监视（除非被标记为备份）。这允许网关确定哪些链路符合既定的 SLA，哪些不符合。然后，网关会根据这些信息作出路径控制决策。

基于应用程序的策略的配置步骤

本节介绍如何在 Aruba 网关上配置基于应用程序的路由策略。图 3 简要概述了此流程。

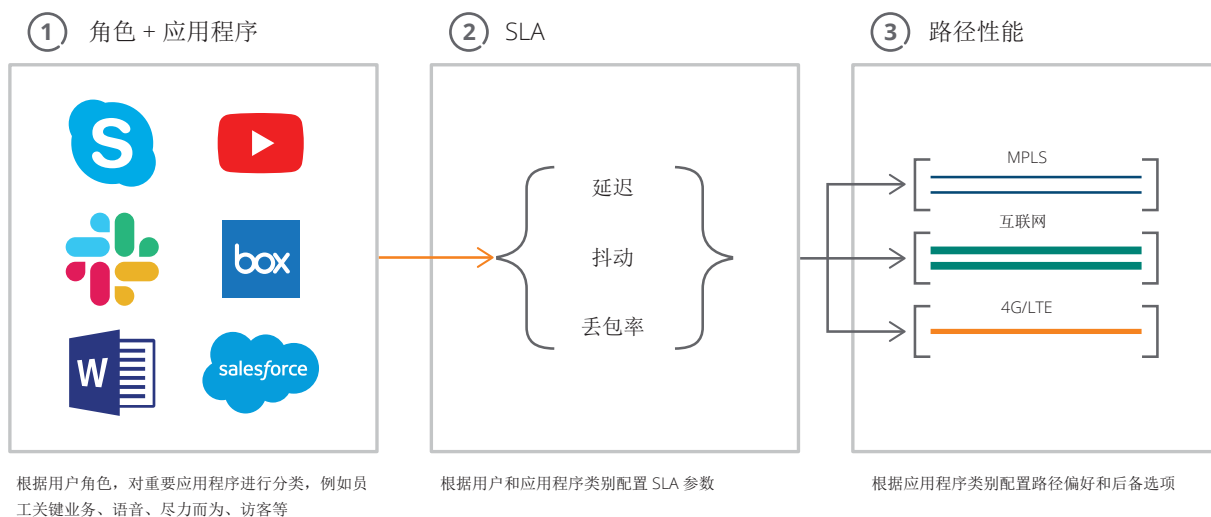


图 3：动态路径控制概览

SD-WAN 解决方案采用基于角色的应用程序策略，通过中心化方式定制并应用于所有用户、实体和网络域。IT管理员不仅可以为大约 3200 个应用程序制定针对性的策略，也可以基于用户和设备角色，例如员工、承包商和访客或者相机、打印机或 HVAC 设备，对流量进行分类控制。应用程序的类别包括但不限于：员工业务关键型应用、语音或视频应用、销售网点 (PoS) 特定应用或与访客互联网访问相关的应用。因此，第一步就是根据特定用户或设备角色对所需的重要应用程序分类。

每个这些类别的 SLA 参数均可根据用户和应用程序类别设置。参数包括延迟、抖动、丢包率和带宽利用率的最大值。例如，您可以指出，语音延迟不应超过 150ms或丢包率不应超过 1%。

这些设置可根据您配置的应用程序类别决定路径偏好（在这种情况下，MPLS、互联网或 LTE）和后备选项。例如，为 MPLS 扩充宽带线路的客户可能会配置用户语音应用程序，以动态方式切换到互联网链路，无需挂断电话。这种情况下，将语音流量从 MPLS 切换至互联网链路，或者反向操作，会最小化线路质量变化对语音质量产生的影响。

建立 DPS 策略

建立策略的流程非常简单，包括指定“感兴趣的”流量和选择用于衡量广域网链路性能的 SLA 参数。然后，您可以为主用、备份以及最终路径配置路径参数（图 4）。

以下是 3 个必要步骤：

1. 为特定的关键任务型应用策略指定分类规则。在这种情况下，这些员工的应用程序包括 Workday、Microsoft Exchange 以及 FTP、SSH 或 SMTP 等。
2. 指定所需的 SLA 阈值。在这种情况下，我们会从以下值当中选择：高度可用、适合互联网或语音流量。
3. 最后一步是通过识别主用（这种情况下是 MPLS）和备份路径（互联网或 LTE）或最终路径（这种情况下没有）来定义路径偏好。在此示例中，出于性能原因选择了 MPLS 路径，并且两个 MPLS 上行链路之间的负载是平衡的。如果无法达到阈值要求，流量将故障切换到备份路径，这会使所有互联网上行链路之间的负载实现平衡。

1 指定“感兴趣的”流量

2 选择 SLA 参数，以衡量广域网性能

3 配置路径偏好参数

图 4: 关键任务型应用程序的 DPS 策略示例

策略和 SLA 示例

如上述示例所示，DPS 允许您面向特定的个别应用程序匹配流量特性，其中包括流量特征规则、SLA 设置和相应的路径选择。表 1 显示分配给不同应用程序的其他策略示例，以及因触发这些策略而引起的路径选择示例。

用于 Zoom 的策略样例专门用于优化协作和即时通信流量。分支机构实施了这一策略，原因是出于成本原因，这些分支机构仅具有互联网和城域以太网。在这种情况下，这些上行链路的流量将会实现负载均衡。

为处理 SaaS 流量（例如 Office 365、Salesforce 和 Dropbox），SD-WAN 网关采用深度数据包检查 (DPI) 匹配流量。SaaS 流量的主要路径是本地互联网；如果出现故障，计划是通过本地城域网的 MPLS 上行链路把流量切换到本地数据中心，然后再从那里连接到 SaaS 云。

还有相应的 SLA 用于娱乐性互联网使用案例。流量类型可能包括流媒体或社交网络应用程序，如 YouTube 或 Netflix。大多数企业不会为此类流量制定 SLA，此类流量通常会采用互联网线路，当互联网线路故障时则切换到 4G/LTE 蜂窝网链路（最后路径）。

服务水平协议 (SLA) 的测量

SLA 的测量会影响 DPS 的决策，可以通过用户进行配置，也可以是被动执行。如果是被动执行，会以每两秒一次的频率更新测量结果。如先前讨论，延迟可通过在广域网上行链路上发送的探测包来测量。此外，还有一个发送至 PQMS (pqm.arubanetworks.com) 的探测包，其目的在于确保测量结果的一致性。当 SLA 参数违反 SLA 策略时，应用程序/角色将被移动至指定的第二个上行链路。

如果没有任何一个广域网上行链路符合指定的 SLA，则有效载荷通常会被发送至最优链路（即：具有“最适宜”SLA 的链路）。当流量被切换至第二个链路且该链路正作为主要链路用于转发其他流量时，可以设置 QoS 参数来确保切换至第二个链路的流量的优先级超过该链路的当前流量。

表 1：简单策略、流量特征、服务水平协议和路径选择示例

策略	流量特征	SLA	路径选择
Zoom	协作和即时通信流量	延迟 < 150 ms。 抖动 < 30 ms。	主要：快速互联网、MPLS 城域以太网（负载均衡）
SaaS	Office 365、Salesforce 和 Dropbox	延迟 < 150 ms。 抖动 < 150 ms。 丢包率 < 1%	主要：快速互联网 备份：MPLS 城域以太网（在不符合 SLA 时进行故障切换）
娱乐性互联网	流媒体或社交网络	延迟 < 150 ms。 抖动 < 150 ms。 丢包率 < 1%	主要：快速互联网 备份：MPLS 城域以太网

可视化的路径控制

路径控制的详细信息可提供有关流量策略契合程度的概述。在以下使用案例（图 5）中，您可以查看单一应用程序的表现。

监视仪表盘可通知管理员当前的活跃 DPS 策略，以及这些策略与配置的 SLA 阈值是否保持一致。然后，管理员可以深入的

了解每个策略，以了解个别策略在选定时间段（3 小时、过去一天、过去一周等）内的表现如何。管理员还可以查看策略选择了哪些链路发送应用程序流量，以及什么时候广域网链路曾发生不合规的情况。详细信息可以让管理员快速了解配置的策略的工作状态，以及它们与 SLA 的匹配情况。

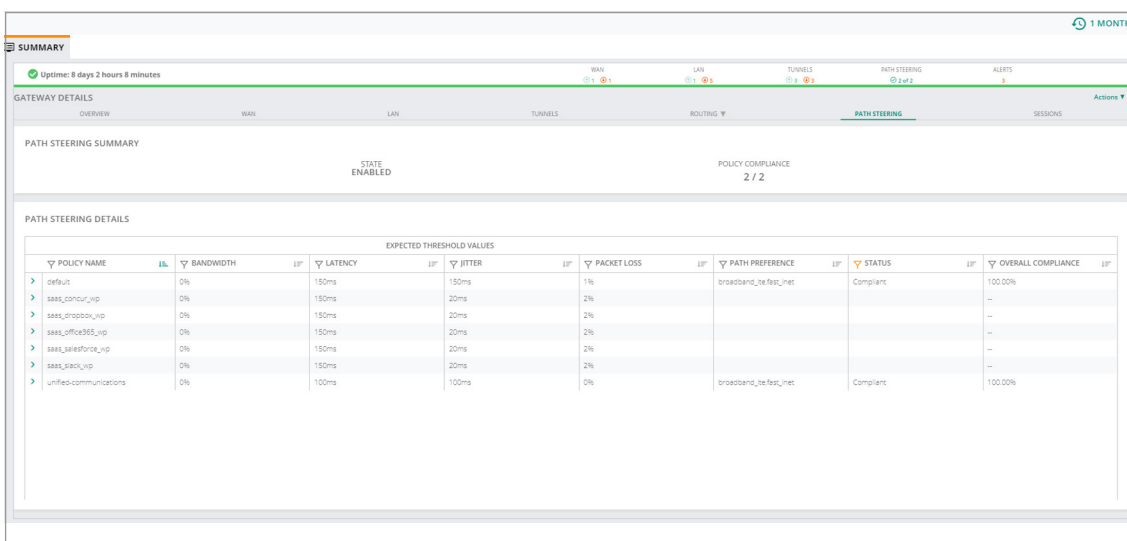


图 5：网关上的路径控制详细信息



图 6：扩展策略合规图

应用程序性能监视

您可以选中已为其单独制定策略的所有流量类型。您也可以进入列出所有关键应用程序的应用程序仪表板（图 7），查看每个应用程序所使用的带宽（发送和接收）等信息。

选择单个应用程序让您查看关键性能指标 (KPI) 和图形化的利用率信息（图 8）。管理员可以查看基于某一应用程序计算出的丢包率、延迟和抖动得分。如果 DPS 策略确实有效，那么管理员应该会在应用程序性能 KPI 中看到该策略的效果。

所有信息均实时显示，同时还会显示历史视图。

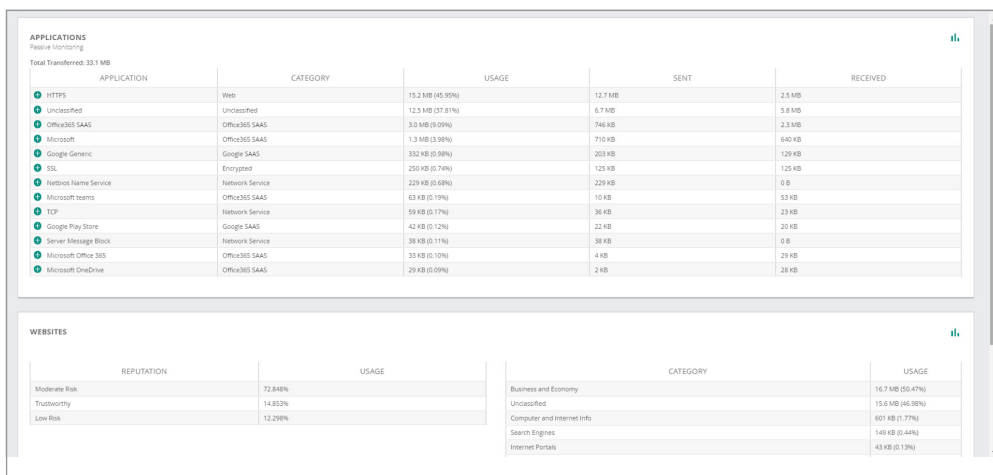


图 7: 网关应用程序详细信息

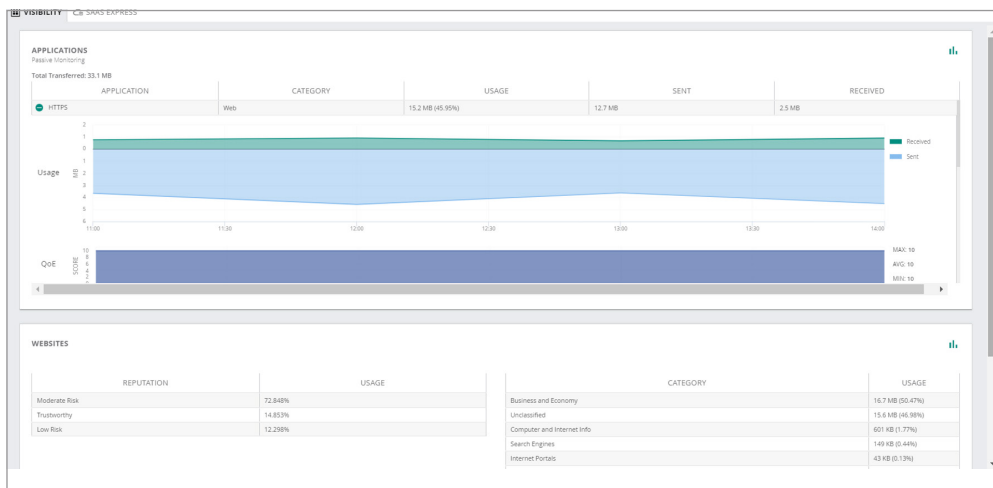


图 8: 关键性能指标应用程序视图

结论

DPS 策略可以显著改善分支机构广域网环境的整体健康状况和用户体验。通过持续探测所有可用链路的广域网性能指标，同时在可用广域网上联链路之间对流量进行实时动态控制，DPS 策略可确保应用程序流量始终通过最佳可用广域网链路进行传输。

这允许管理员以最佳方式使用符合延迟、抖动、丢包率等特定条件的可用上行链路资源，这有助于选择正确的上行链路。假如缺少了动态路径控制，管理员将无法对此进行合理编排。