在思科SD-WAN中实施QoS

目录

简介

本文档介绍Cisco-Viptela方法，以便通过软件定义广域网(SD-WAN)实施服务质量(QoS)。SD-WAN是最新的创新，可与全球的企业、企业和组织集成。新一波的SD-WAN技术使政府和企业能够提供关键应用支持，而无需额外麻烦。虽然云极大地简化了容量调配过程，但在QoS管理方面，它仍面临着一些新的挑战。新的SD-WAN需要与应用及其托管平台或基础设施提供的性能、可靠性和可用性级别相匹配。

先决条件

要求

Cisco 建议您了解以下主题：

- SD-WAN解决方案
- 传统QoS和策略结构

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科vEdge硬件设备
- 思科vEdge软件(VM)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

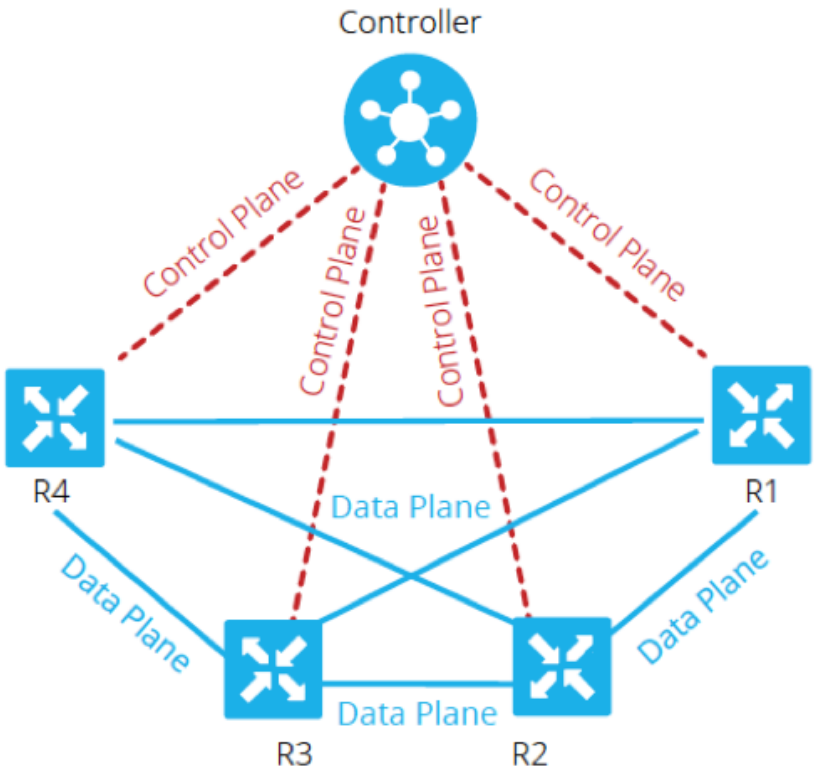
直到最近，网络都严格地基于底层传输网络的构建方式。某些解决方案(如多协议标签交换(MPLS)流量工程)影响了节点之间的路径选择，但是，需要对从源到目的地的每台设备进行编程，以允许或拒绝两个终端之间流动的流量并做出完全自主的决策。

IP VPN或MPLS等传统运营商服务已被许多人认为是可靠地为组织提供QoS服务的唯一方法，MPLS的最大缺点是带宽成本。当今的消费者对占用带宽的多媒体内容(如视频和增强现实(AR)/虚拟现实(VR))以及MPLS要求的高每兆成本越来越感兴趣。最后，MPLS网络不提供内置数据保护，如果实施不当，可能会使网络暴露漏洞。

此外，从安全角度来看，MPLS流量默认不加密。MPLS网络提供许多安全功能，但是，其传统VPN解决方案并非没有挑战。预共享密钥用于验证VPN IPSec设备，但为了在多个设备间管理大量预共享密钥，预共享密钥不能扩展，安全性较低。

解决方案

另一方面，SD-WAN方法使用集中式WAN控制器来托管和管理与网络中节点的所有邻接关系。它在策略的创建和实施方面提供了灵活性。由于每台设备仅与控制器对等，用于连接和控制平面策略以在服务节点之间传递数据流量，因此可以根据对网络状况的整体可视性来动态调整这些策略。如图所示，每台路由器都向控制器通告其本地信息。这允许中央控制器使用在每个本地路由器上实施的策略轻松控制数据流。



在本例中，R1和R4仅与数据平面路径没有成对邻接关系。因此，中央控制器容易控制和修改流量。例如，它可以控制从R1通过R3通告到R4的所有前缀，或者某些前缀通过R3通告到R4，而某些前缀直接从R1通告，其中R3可能是防火墙策略的应用点。此方法使用传统网络拓扑，显着减少了在每台路由器上需要实施的数据平面策略的数量。SD-WAN是一个重叠网络，可帮助管理员识别关键流量

并在整个网络中给予特殊处理。

配置并实施思科SD-WAN QoS

在SD-WAN重叠网络中，QoS在检查进入网络边缘的数据包时起作用。必须将网络中的每台vEdge路由器配置为调配QoS。一旦SD-WAN重叠网络和控制平面连接启动并运行，数据流量将自动通过vEdge路由器之间的IPsec连接流动。创建并应用集中式数据策略或本地化数据策略时，可以修改默认数据包转发流。

集中式数据策略提供管理通过网络路由的流量路径的控制，并且可以根据数据包的IP报头中的地址、端口和差分服务代码点(DSCP)字段来控制(允许或阻止)流量。

本地化数据策略可以控制进出vEdge路由器接口的数据流量并启用QoS等功能。如果您应用访问列表，则可以在出站方向或入站方向激活策略。

每个接口在硬件vEdge路由器上有八个队列，编号从0到7。队列0保留，用于控制流量和低延迟队列(LLQ)流量。对于LLQ，必须将映射到队列0的任何类配置为使用LLQ。传输所有控制流量。队列1到7可用于数据流量。

如图2所示，当数据包从一个分支传输到另一个分支时，QoS策略会应用到该数据包：

1.分类输入 — 传入流量可通过将每个数据包与转发类关联来分类。转发类根据转发类对数据包分组，并将数据包分配到输出队列以便传输到其目的地。

2.输入ACL和定义监察器 — 通过配置监察器并将网络划分为多个优先级，可以控制接口上发送或接收数据的最大流量速率。应用于入站接口流量的监察器允许您通过丢弃不需要通过网络路由的流量来节省资源。

3.路由查找 — vEdge路由器检查本地路由表以确定数据包应使用哪个接口到达其目的地。

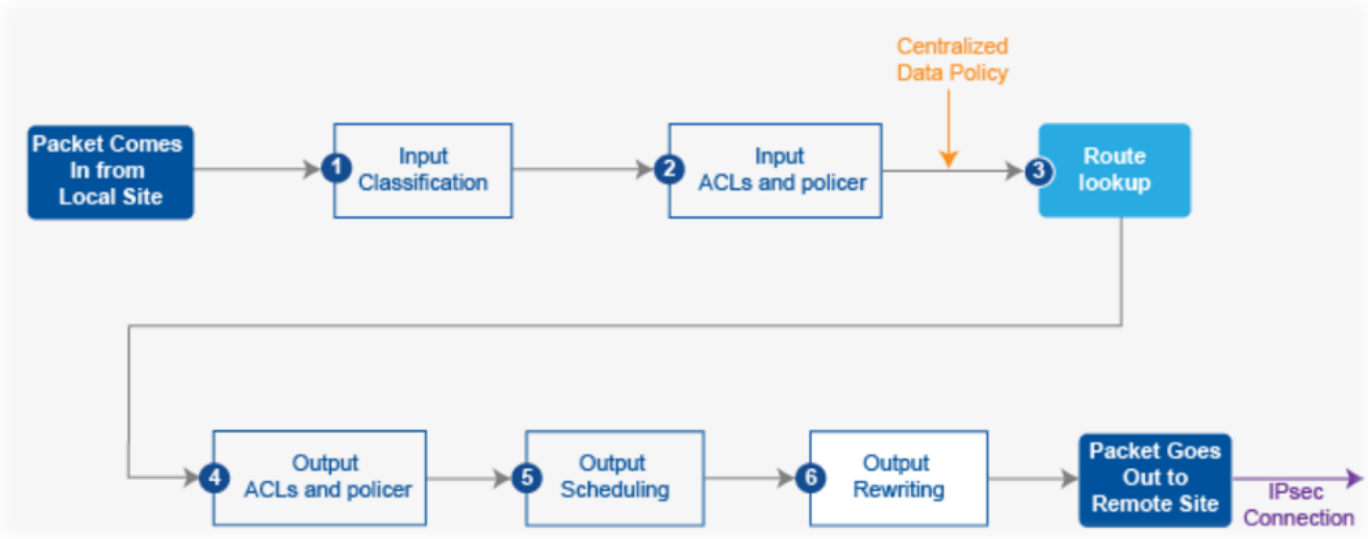
4.输出ACL和监察器 — 传输符合监察器速率的流量，并以降低的优先级发送超过监察器速率的流量或丢弃该流量。应用于出站接口流量的监察器控制使用的带宽量。

5.输出调度 — 可以通过为每个输出队列配置QoS映射来优先处理数据包，以指定输出队列的带宽、延迟缓冲区大小和丢包优先级(PLP)。它取决于可以为数据包分配更高或更低带宽、缓冲区级别和丢弃配置文件的流量优先级。

6.重写输出 — 如果重写规则，则允许映射流量，以便在流量在系统中退出时为代码点编码。定义rewrite-rule以覆盖外部IP报头的DSCP字段。在出站（出口）接口上应用rewrite-rule。

配置QoS策略

以下步骤描述本地化数据策略(QoS)配置：



步骤1.配置转发类和到输出队列的映射。定义**类映射**，以便按重要性将数据包分类为适当的转发类。请参阅访**问列**表中的类映射。

```
policy
 class-map
 class best-effort queue 3
 class bulk-data queue 2
 class critical-data queue 1
 class voice queue 0
```

步骤2.配置QoS调度程序转发类。定义**qos调度程序**并指定接口上发送流量的速率。请参阅访问列表中的监察器。

```
policy
 qos-scheduler be-scheduler
 class                          best-effort
 bandwidth-percent     20
 buffer-percent            20
 scheduling                 wrr
 drops                         red-drop
 !
 qos-scheduler bulk-scheduler
 class                          bulk-data
 bandwidth-percent     20
 buffer-percent            20
```

```
 scheduling                 wrr
 drops                          red-drop
 !
 qos-scheduler critical-scheduler
 class                           critical-data
 bandwidth-percent     40
 buffer-percent            40
 scheduling                 wrr
 drops                          red-drop
 !
 qos-scheduler voice-scheduler
 class                           voice
 bandwidth-percent     20
 buffer-percent            20
 scheduling                 llq
 drops                          tail-drop
```

步骤3.对QoS调度程序进行分组并定义QoS映射：

```
policy
 qos-map MyQoSMap
 qos-scheduler be-scheduler
 qos-scheduler bulk-scheduler
 qos-scheduler critical-scheduler
 qos-scheduler voice-scheduler
```

步骤4.将QoS映射应用到出口接口：

```
interface ge0/1
 qos-map  MyQoSMap
```

步骤5.定义访问列表，以便将数据包分类为适当的转发类：

```
policy
 access-list MyACL
 sequence 10
  match
```

```
  dscp 46
 !
 action accept
  class voice
 !
!
sequence 20
 match
  source-ip          10.1.1.0/24
  destination-ip   192.168.10.0/24
 !
 action accept
  class bulk-data
  set
   dscp 32
  !
 !
!
sequence 30
 match
  destination-ip  192.168.20.0/24
 !
 action accept
  class critical-data
  set
   dscp 22
  !
 !
!
sequence 40
 action accept
  class best-effort
```

```
   set
    dscp 0
   !
  !
 !
 default-action drop
```
步骤6.将访问列表应用于接口：

```
vpn 10
 interface ge0/0
 access-list MyACL in
 !
```

相关信息

通过SD-WAN实现保证QoS的理想要求：

Cisco SD-WAN QoS解决方案可使用动态方法通过Internet提供与QoS相匹配的QoS级别，因此，作为解决方案，它为什么会威胁传统MPLS广域网，而Cisco SD-WAN则动态选择最具成本效益的私有链路和公共互联网连接。使用SD-WAN时，应用不受标准带宽的支配，而是选择最适用于每个应用的连接。

无论MPLS还是SD-WAN是最佳解决方案，都必须注意的是，使用SD-WAN的QoS可以在没有使用对称互联网的MPLS的情况下实现，而VPN不会丢包。如果流量通过多个ISP经过多跳，企业无法保证任务关键型和延迟敏感型服务的性能。事实上，SD-WAN产品需要主用 — 主用配置，以提高广域网的可靠性和QoS。

简而言之，SD-WAN是一项非常出色的技术，可降低未来对MPLS网络的依赖。您可以将一些非交互式流量卸载到宽带互联网连接。例如，SD-WAN可能会路由延迟敏感型流量，例如通过MPLS链路的语音，以保证QoS，以及通过宽带互联网连接进行的所有其他流量，或者可能将两个宽带链路合并为近似的MPLS。