在思科SD-WAN中实施QoS

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[问题](#)

[解决方案](#)

[配置并实施Cisco SD-WAN QoS](#)

[配置QoS策略](#)

[相关信息](#)

简介

本文档介绍通过软件定义广域网(SD-WAN)实施服务质量(QoS)的Cisco-Viptela方法。SD-WAN是最新的一项创新，旨在与全球的企业、企业和组织进行集成。新一波的SD-WAN技术使政府和企业能够轻松提供关键的应用支持。尽管云已大大简化了容量调配过程，但它在QoS管理方面仍面临一些新的挑战。新的SD-WAN需要与应用以及承载它的平台或基础设施所提供的性能、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：

- Cisco vEdge硬件设备
- Cisco 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

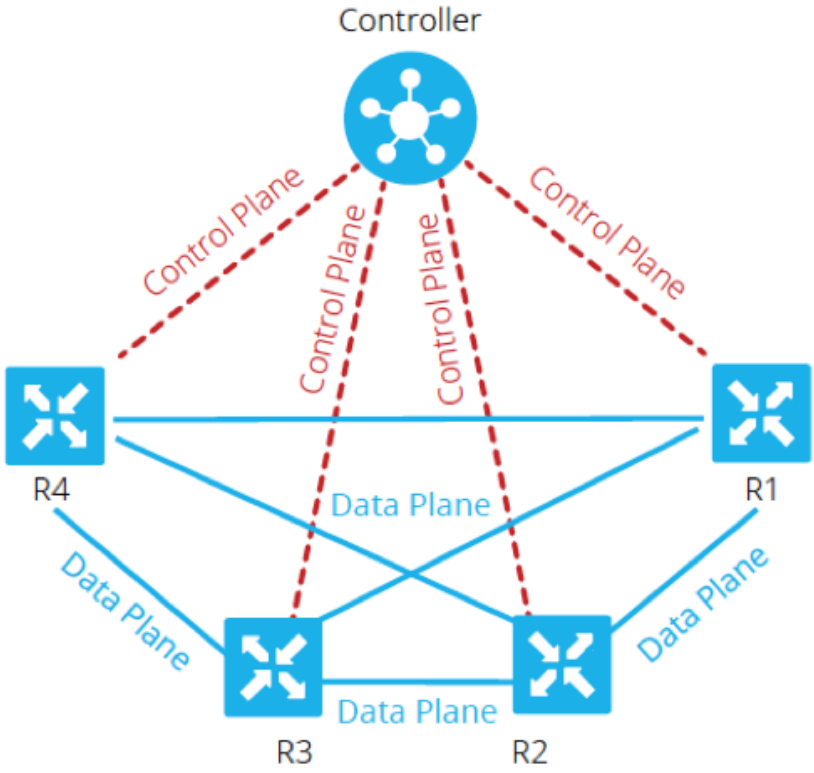
直到最近，网络都是严格按照底层传输网络的构造来构建的。一些解决方案（如多协议标签交换[MPLS]流量工程）影响了节点之间的路径选择，但是从源到目的地的每台设备都需要进行编程，以便允许或拒绝在两个终端之间流动的流量，并做出完全自主的决策。

IP VPN或MPLS等传统运营商服务被许多人认为是组织可靠提供QoS服务的唯一途径，MPLS最大的缺点是带宽成本。当今的消费者越来越关注带宽密集型多媒体内容，例如视频和增强现实(AR)/虚拟现实(VR)，以及MPLS要求的高每兆比特成本。最后，MPLS网络不提供内置的数据保护，如果实施不当，则会使网络暴露于漏洞。

此外，从安全角度来看，MPLS流量在默认情况下不加密。MPLS网络提供许多安全功能，但是其传统的VPN解决方案并非没有挑战。预共享密钥用于对VPN IPSec设备进行身份验证，但为了管理跨多个设备的大量预共享密钥，该密钥无法扩展，且安全性较低。

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。它提供了策略创建和实施的灵活性。由于每个设备仅与连接和控制平面策略的控制器对等，以便在服务节点之间传递数据流量，因此可以根据网络条件的整体可视性动态调整这些策略。如图所示，每台路由器都会向控制器通告其本地信息。这样，中央控制器就可以使用在每个本地路由器上实施的策略轻松控制数据流。



在本示例中，R1和R4只有数据平面路径没有成对邻接关系。因此，中央控制器可以轻松地控制和修改流量。例如，它可以控制从R1通过R3通告给R4的所有前缀，也可以控制某些前缀通过R3通告给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对其进行特殊处理。

配置并实施Cisco 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。必须将网络中的每个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，数据流量就会自动流经vEdge路由器之间的IPsec连接。当创建和应用集中数据策略或本地化数据策略时，可以修改默认的数据包转发流。

集中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IP报头中的地址、端口和差分服务代码点(DSCP)字段控制（允许或阻止）流量。

本地化的数据策略可以控制vEdge路由器接口进出的数据流量，并启用QoS等功能。如果在出站方向或入站方向应用访问列表，则可以激活策略。

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被保留，用于控制流量和低延迟队列(LLQ)流量。对于LLQ，映射到队列0的所有类也必须配置为使用LLQ。传输所有控制流量。队列1至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策略会应用于该数据包：

1. Classify Input — 通过将每个数据包与转发类相关联，可以对传入流量进行分类。转发类根据转发类对数据包进行分组，并将数据包分配到输出队列，以传输到它们的目的地。

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

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来到达其目的地。

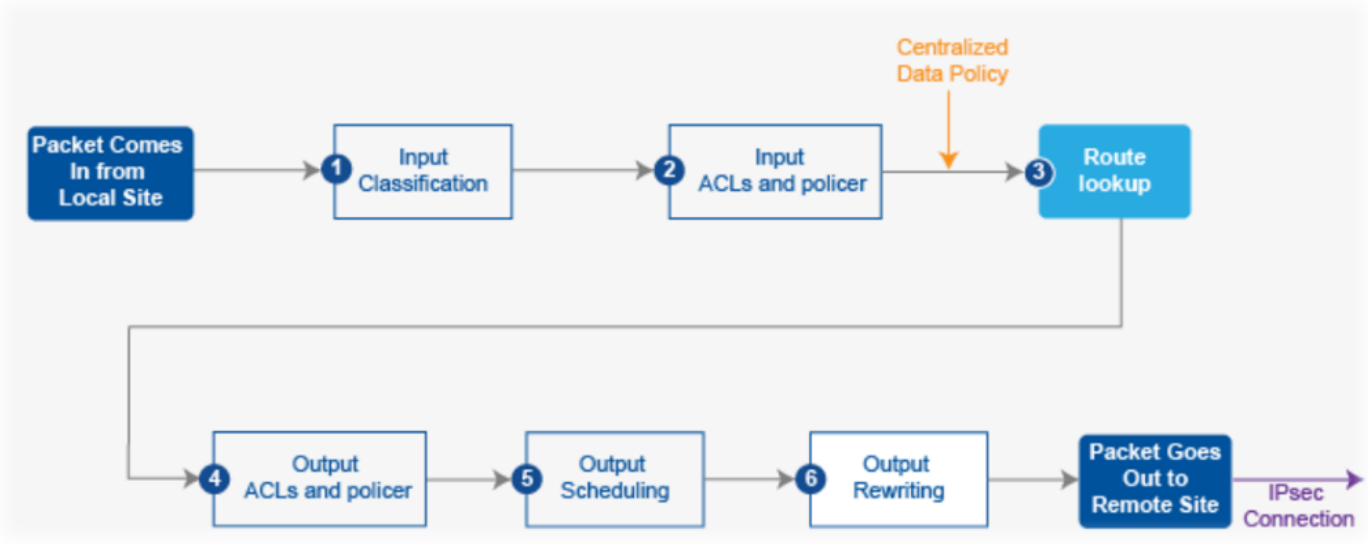
4.输出ACL和监察器 — 传输符合监察器速率的流量，并且以较低的优先级发送超过监察器速率的流量，或者将其丢弃。应用于出站接口流量的监察器控制使用的带宽量。

5.输出调度 — 可以通过为每个输出队列配置QoS映射来区分数据包的优先级，以便指定输出队列的带宽、延迟缓冲区大小和丢包优先级(PLP)。这取决于流量的优先级，您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。

6. Rewrite Output — 如果重写规则，则允许您映射流量，以便在流量退出系统中时为点编码。定义重写规则以覆盖外部IP报头的DSCP字段。在出站（出口）接口上应用重写规则。

配置QoS策略

以下步骤介绍本地化数据策略(QoS)配置：



步骤1.配置转发类并映射到输出队列。定义类映射，以便按重要性将数据包分类到适当的转发类中。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 scheduler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.定义访问列表以将数据包分类到相应的转发类：

```
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.将访问列表应用到接口：

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

相关信息

通过SD-WAN实现有保证的QoS的理想要求：

思科SD-WAN QoS解决方案可以使用动态方法，在互联网上提供匹配的QoS级别。思科SD-WAN动态选择最经济高效的私有链路和公共互联网连接分类，因此我们很容易理解为什么这种解决方案会威胁到传统的多协议标签交换广域网。使用SD-WAN，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或SD-WAN是最佳解决方案，必须注意的是，使用SD-WAN的QoS可以在没有MPLS的情况下实现，使用对称互联网，使用VPN不会丢失数据包。如果流量通过多个ISP经过多个跃点，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产品需要主动 — 主动配置才能提高WAN的可靠性和QoS。

简而言之，SD-WAN是一项极好的技术，可降低将来对MPLS网络的依赖性。您可以将一些非交互式流量分流到宽带Internet连接。例如，SD-WAN可能会路由延迟敏感型流量，例如MPLS链路上的语音（可保证QoS和其他所有内容）通过宽带互联网连接，或者可能会组合两个宽带链路来近似于MPLS。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。