

在Cisco SD-WAN中實施QoS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

[配置和實施Cisco SD-WAN QoS](#)

[配置QoS策略](#)

[相關資訊](#)

簡介

本檔案介紹思科全球資訊網方法，以便透過軟體定義廣域網(SD-WAN)實作服務品質(QoS)。SD-WAN是最新的一項創新，旨在與世界各地的企業、企業和組織進行整合。新一波的SD-WAN技術使政府和企業能夠輕鬆提供關鍵應用程式支援。儘管雲已經大大簡化了容量調配過程，但它在QoS管理領域面臨諸多新挑戰。新的SD-WAN需要與應用程式以及託管它的平台或基礎設施所提供的效能、可靠性和可用性級別相匹配。

必要條件

需求

思科建議您瞭解以下主題：

- SD-WAN解決方案
- 傳統QoS和策略結構

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco vEdge硬體裝置
- Cisco vEdge軟體(VM)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

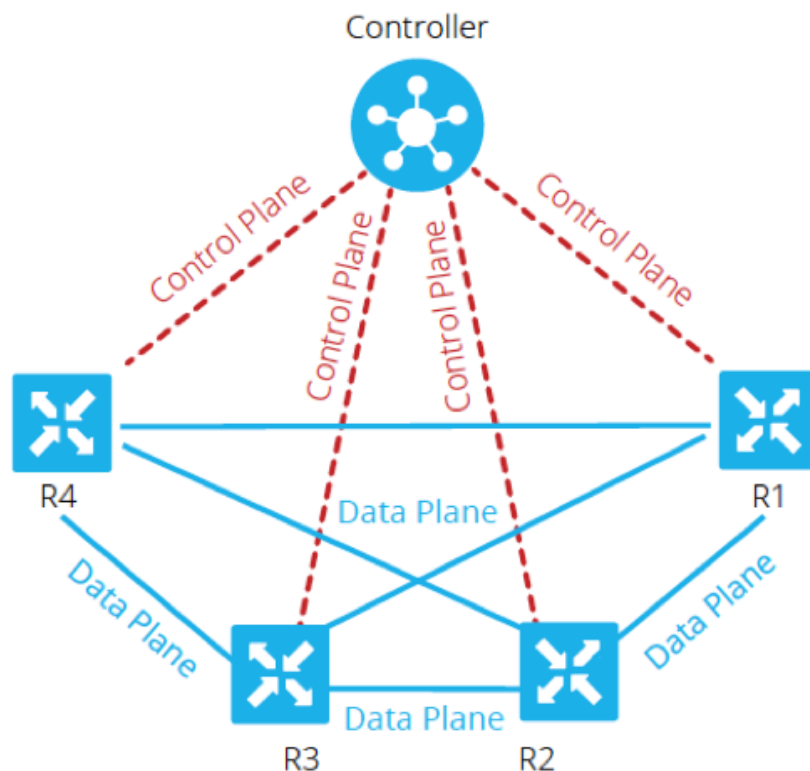
直到最近，網路都是嚴格根據底層傳輸網路構建的。某些解決方案(例如多協定標籤交換(MPLS)流量工程影響了節點之間的路徑選擇，但是從源到目的地的每台裝置都需要進程式設計，以便允許或拒絕在兩個端點之間流動的流量，並做出完全自主的決策。

傳統的運營商服務，如IP VPN或MPLS，被許多人認為是可靠為組織提供QoS服務的唯一途徑，MPLS最大的缺點是頻寬成本。當今的消費者對佔用頻寬的多媒體內容(例如影片和增強現實(AR)/虛擬現實(VR))越來越感興趣，而且MPLS要求的高每兆位元成本可能難以企及。最後，MPLS網路不提供內建的資料保護，如果實施不當，它可能會使網路暴露在漏洞之下。

此外，從安全形度來看，MPLS流量預設情況下不加密。MPLS網路提供了許多安全功能，但是其傳統的VPN解決方案並非沒有挑戰。預共用金鑰用於對VPN IPSec裝置進行身份驗證，但是為了管理多個裝置之間的大量預共用金鑰無法擴展，並且安全性較低。

解決方案

另一方面，SD-WAN方法使用集中式WAN控制器來託管和管理與網路中節點的所有鄰接關係。它提供了制定和執行政策的靈活性。由於每台裝置僅與用於連線和控制平面策略的控制器對等以在服務節點之間傳遞資料流量，因此可以根據網路條件的整體可視性動態調整這些策略。如下圖所示，每台路由器都會將其本地資訊通告給控制器。這樣，中央控制器就可以使用每台本地路由器上強制實施的策略，輕鬆操縱資料流。



在本例中，R1和R4隻有資料平面路徑沒有成對鄰接關係。因此，中央控制器可以容易地控制和修改通訊流。例如，它可以控制R1中通過R3通告給R4的所有字首，或者通過R3將某些字首通告給R4，而直接從R1通告某些字首，其中R3可以是防火牆策略的應用點。此方法使用傳統網路拓撲，顯著減少了每台路由器上需要實施的資料平面策略的數量。SD-WAN是一個重疊網路，可幫助管理員識別關鍵流量，並在整個網路中對其進行特殊處理。

配置和實施Cisco SD-WAN QoS

在SD-WAN重疊網路中，QoS在檢查進入網路邊緣的資料包時發揮作用。必須將網路中的每個vEdge路由器配置為調配QoS。一旦SD-WAN重疊網路和控制平面連線啟動並運行，資料流量就會自動通過vEdge路由器之間的IPsec連線流動。當建立和應用集中資料策略或本地化資料策略時，可以修改預設的資料包轉發流。

集中式資料策略提供管理通過網路路由的流量路徑的控制，並且可以根據資料包IP報頭中的地址、埠和差分服務代碼點(DSCP)欄位控制（允許或阻止）流量。

本地化的資料策略可以控制vEdge路由器介面的進出資料流量，並啟用QoS等功能。如果在出站方向或入站方向應用訪問清單，則可以啟用策略。

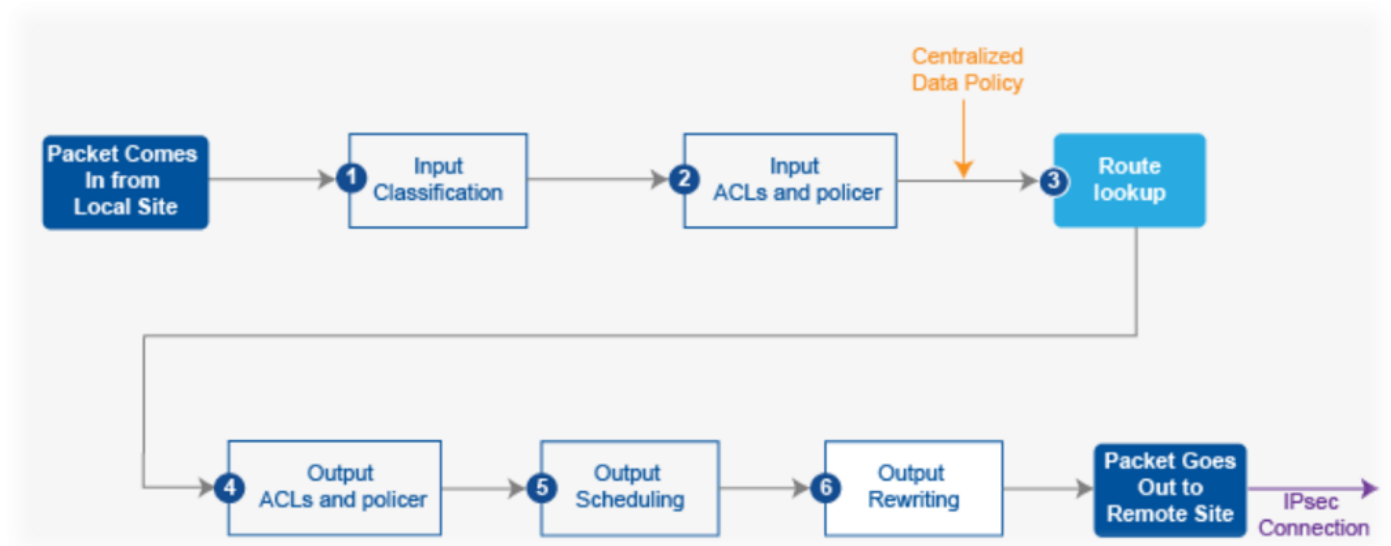
每個介面在硬體vEdge路由器上有八個隊列，編號從0到7。隊列0被保留，用於控制流量和低延遲隊列(LLQ)流量。對於LLQ，對映到隊列0的任何類也必須配置為使用LLQ。傳輸所有控制流量。隊列1到7可用於資料流量。

如圖2所示，當資料包從一個分支傳輸到另一個分支時，QoS策略將應用到該資料包：

1. Classify Input — 通過將每個資料包與轉發類相關聯，可以對傳入流量進行分類。轉發類根據轉發類對資料包進行分組，並將資料包分配給輸出隊列，以便傳輸至其目標。
2. 輸入ACL和定義管制器 — 介面上傳送或接收資料的最大流量速率可通過配置管制器進行控制，並將網路劃分為多個優先順序級別。應用於入站介面流量的策略器允許您通過丟棄不需要通過網路路由的流量來節約資源。
3. 路由查詢 — vEdge路由器檢查本地路由表，以確定資料包應使用哪個介面到達目的地。
4. 輸出ACL和管制器 — 傳輸符合管制器速率的流量，並以降低的優先順序傳送超過管制器速率的流量，或者丟棄該流量。應用於出站介面流量的管制器控制使用的頻寬量。
5. 輸出排程 — 可以通過為每個輸出隊列配置QoS對映來區分資料包的優先順序，以便指定輸出隊列的頻寬、延遲緩衝區大小和丟包優先順序(PLP)。這取決於您可以為資料包分配更高或更低頻寬、緩衝區級別和丟棄配置檔案的流量的優先順序。
6. Rewrite Output — 如果重寫規則，則允許您對映流量，以便在流量退出系統中時進行代碼點。定義重寫規則以覆蓋外部IP報頭的DSCP欄位。在傳出（輸出）介面上套用重新寫入規則。

配置QoS策略

以下步驟描述本地化資料策略(QoS)配置：



步驟1.配置轉發類並對映到輸出隊列。定義類對映，以便按重要性將資料包分類到相應的轉發類中。請參閱訪問清單中的類對映。

policy

class-map

class best-effort queue 3

class bulk-data queue 2

class critical-data queue 1

class voice queue 0

步驟2.配置QoS排程程式轉發類。定義qos scheduler並指定在介面上傳送流量的速率。請參閱存取清單中的管制器。

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

```

步驟3.對QoS排程程式進行分組並定義QoS對映：

```

policy

qos-map MyQoSMap

qos-scheduler be-scheduler
qos-scheduler bulk-scheduler
qos-scheduler critical-scheduler
qos-scheduler voice-scheduler

```

步驟4.將QoS對映應用到輸出介面：

```
interface ge0/1

  qos-map  MyQoSMap
```

步驟5.定義存取清單，以便將資料封包分類到適當的轉送類別中：

```
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
```

步驟6.將存取清單套用至介面：

```
vpn 10

interface ge0/0

access-list MyACL in

!
```

相關資訊

通過SD-WAN實現有保證的QoS的理想要求：

我們很容易理解，為什麼這種解決方案會威脅到現有的傳統MPLS廣域網，因為Cisco SD-WAN QoS解決方案可以使用動態方法，在網際網路上提供匹配的QoS級別。Cisco SD-WAN動態選擇最經濟高效的專用鏈路和公共網際網路連線分類。使用SD-WAN，應用不受標準頻寬的支配，而是選擇最適用於每個應用的連線。

無論MPLS還是SD-WAN是最佳解決方案，必須注意的是，使用SD-WAN的QoS可以不使用對稱網際網路的MPLS實現，而不用使用VPN的丟包。如果流量通過多個ISP經過多個躍點，則企業無法保證任務關鍵型和延遲敏感型服務的運行方式。事實上，SD-WAN產品需要主用 — 主用配置來提高WAN的可靠性和QoS。

總之，SD-WAN是一項極好的技術，能夠降低未來對MPLS網路的依賴性。您可以將部分非互動流量解除安裝到寬頻網際網路連線。例如，SD-WAN可能會通過寬頻網際網路連線路由延遲敏感型流量（例如通過MPLS鏈路傳輸的語音，可保證QoS和其他所有流量），或者可能會結合兩個寬頻鏈路來近似於MPLS。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。