資料中心中資料平面隧道限制的地址數量

目錄

簡介

本文檔介紹一種解決方案，用於解決資料中心SD-WAN cEdge在接近其資料平面隧道限制時的擴展問題。

必要條件

需求

Cisco建議您應具備SD-WAN的相關知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- SD-WAN控制器版本20.6.3.0.54 (ES)
- Cisco IOS® XE（在控制器模式下運行）17.06.03a.0.2 (ES)

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。

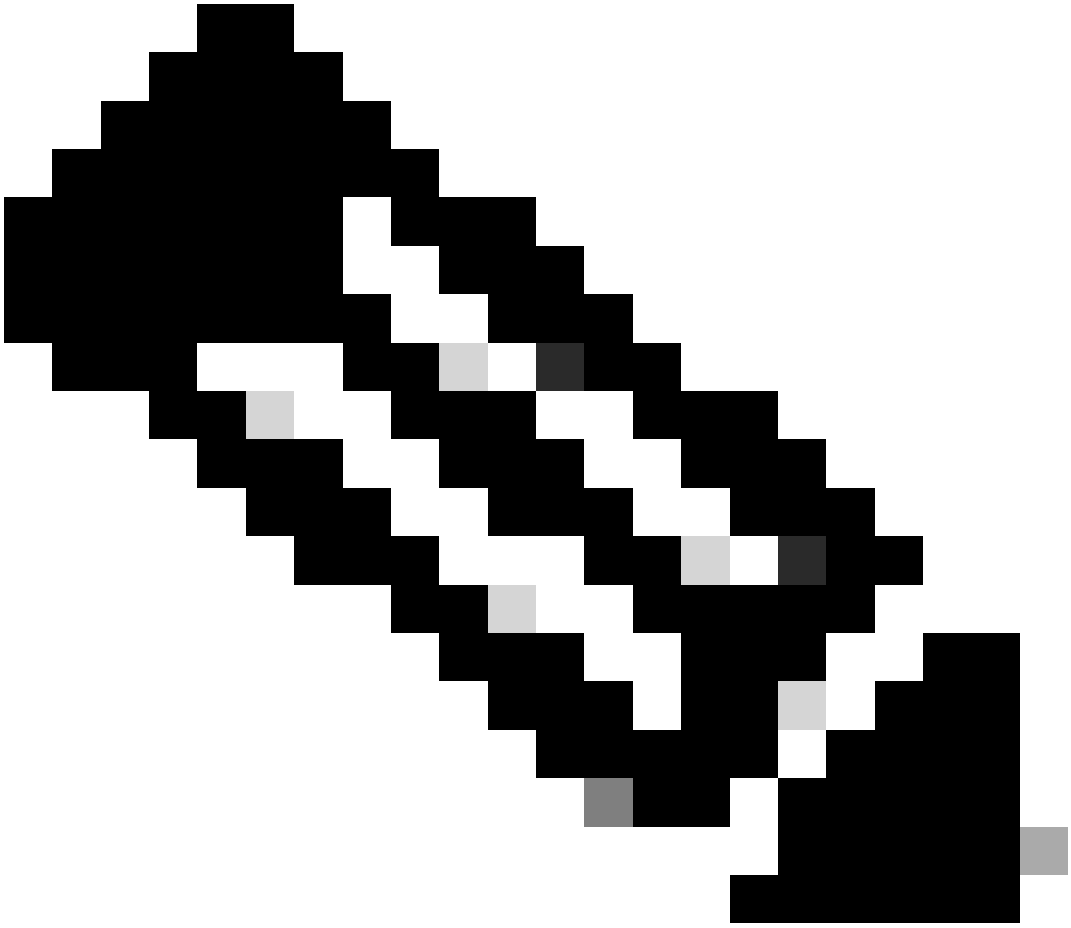
背景資訊

網路設計概述：

- VPN：VPN 10、VPN 20
- 傳輸鏈路：多協定標籤交換(MPLS)、LTE、網際網路
- 路由器詳細資訊：
    - 主要路由器：每個資料中心2個
      - 型號：ASR1002-HX
      - Cisco IOS XE軟體版本：17.06.03a.0.2
    - 輔助路由器：每個資料中心1個
      - 型號：ISR4451-X
      - Cisco IOS XE軟體版本：17.06.03a.0.22
- 路由協定：在資料中心LAN端使用邊界網關協定(BGP)

問題

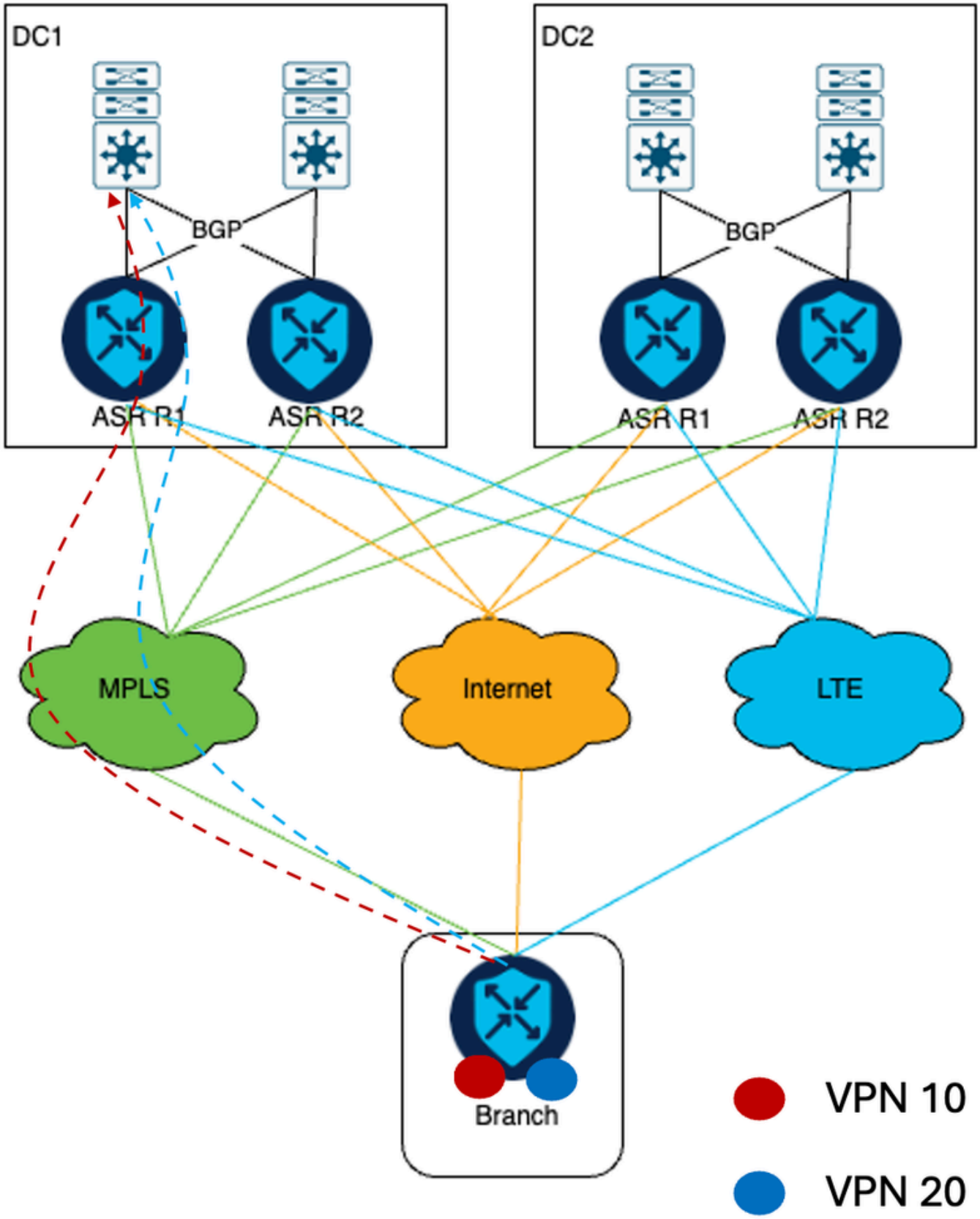
本文檔討論了拓撲圖所示的客戶案例研究，客戶的網路基礎設施包括兩個資料中心，每個資料中心部署兩個ASR1002-HX SD-WAN cEdge。此網路架構旨在將大約3000個儲存位置整合到SD-WAN重疊網路上，利用三條不同的傳輸鏈路的可用性。



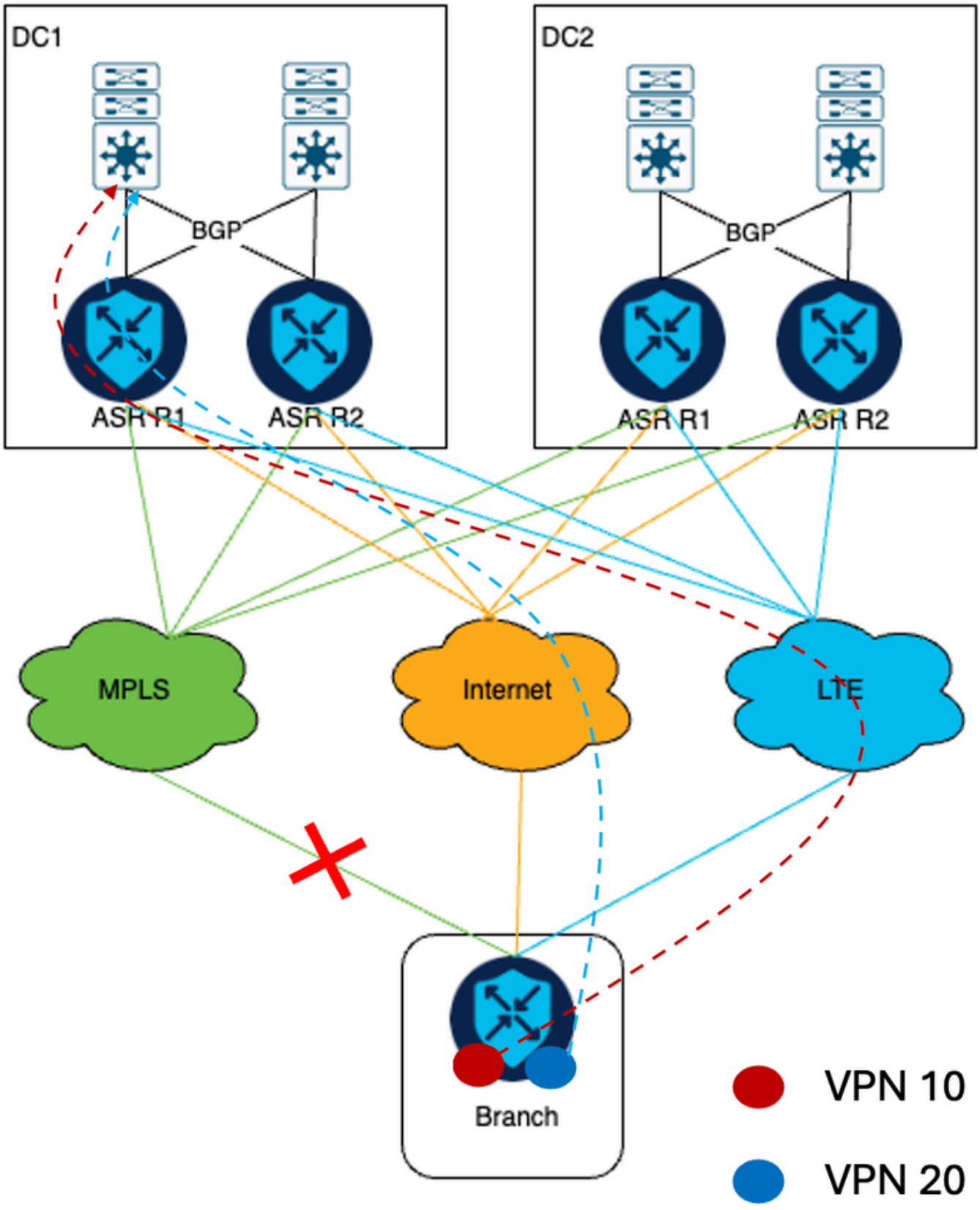
注意：已部署星型拓撲。DC1和DC2 cEdge是集線器。所有遠端分支機構透過3個使用DC cEdge的可用傳輸形成IPsec隧道。

正在退出網路圖

來自VPN 10和VPN 20的所有流量都透過MPLS傳輸。



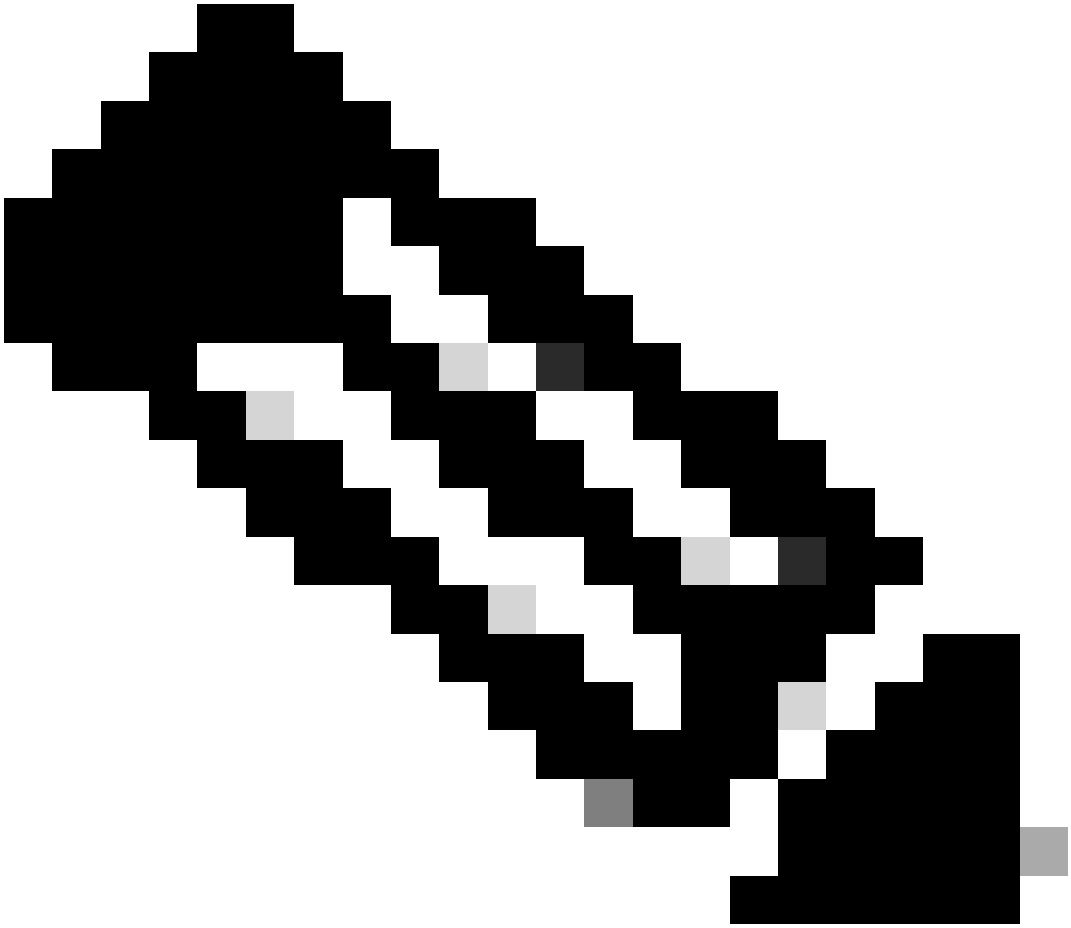
如果MPLS鏈路斷開，VPN 10流量將轉移到LTE傳輸，而VPN 20流量將轉移到Internet傳輸。



此場景中的技術難題源於客戶網路部署的規模和具體要求。 考慮部署3000台SD-WAN路由器，透過三種傳輸型別建立IPSec隧道到資料中心路由器，在ASR1002-HX主前端路由器上形成的IPSec隧道總數達到9000。但是，ASR1002-HX限制為8000個IPSec隧道(來源：ASR1K資料表)。

解決方案

為了解決此問題，客戶決定在每個DC中增加一個ISR4451-X cEdge裝置，以滿足客戶未來的可擴充性需求。

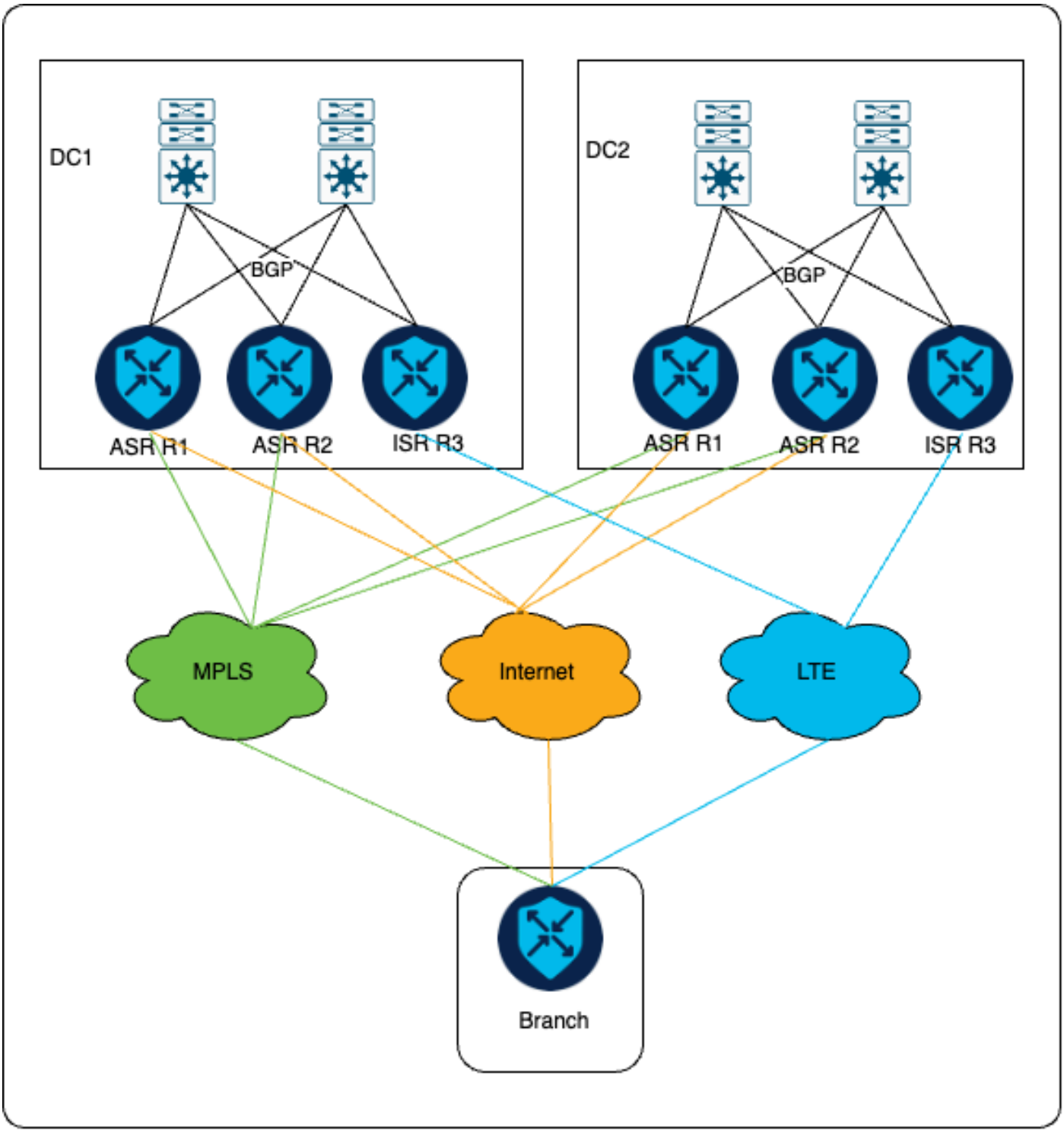


注意：根據客戶的可擴充性要求確定其他裝置型號。

網路拓撲

作為解決方案的一部分，主聚合服務路由器(ASR) cEdge繼續透過MPLS和網際網路傳輸形成IPSec隧道，而新安裝的整合服務路由器(ISR) cEdge僅透過LTE傳輸形成IPsec隧道。

如圖所示，IPSec隧道透過MPLS和網際網路在ASR頭端和分支機構之間建立，而ISR和分支機構之間僅透過LTE建立IPSec隧道。



客戶要求是，在正常情況下，所有VPN 10和VPN 20流量都使用MPLS傳輸進行通訊。但是，在MPLS鏈路發生故障時，VPN 20流量透過網際網路傳輸重新路由，而VPN 10流量透過LTE傳輸重新定向，就像在增加其他cEdge之前一樣。

設定

使用集中和在地化的策略，以確保流量根據客戶的偏好透過正確的傳輸傳送。透過網際網路鏈路和LTE鏈路從分支機構位置傳入的流量被標籤。這些標籤用於確保頭端上的LAN交換機將VPN 10的回覆消息正確傳送到ISR路由器，並確保VPN 20流量傳送到ASR頭端裝置。

集中策略配置

以下是為滿足客戶要求而準備的政策。對於透過網際網路鏈路到達的流量，會分配200的OMP標籤。另一方面，透過LTE鏈路到達的流量分配的OMP標籤為100。

<#root>

Centralized Policy

```
control-policy DataCenter_Outbound_v001
<<omited>>
  sequence 10
   match route
    color-list MPLS
    site-list remote_branches
  vpn-list vpn-10
    prefix-list _AnyIpv4PrefixList
  !
   action accept
    set
     preference 1500
 !
 !
 sequence 20
    match route
      color-list LTE
      site-list remote_branches
      vpn-list vpn-10
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 1000
      omp-tag 100
    !
   !
  !
  sequence 30
    match route
      color-list Internet
      site-list remote_branches
      vpn-list vpn-10
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 500
      omp-tag 200
     !
    !
  !
  sequence 40
   match route
    color-list MPLS
    site-list remote_branches
    vpn-list vpn-20
    prefix-list _AnyIpv4PrefixList
```

```
   !
   action accept
    set
     preference 1500
   !
  sequence 50
    match route
      color-list LTE
      site-list remote_branches
      vpn-list vpn-20
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 500
      omp-tag 100
     !
    !
  !
  sequence 60
    match route
      color-list Internet
      site-list remote_branches
      vpn-list vpn-20
      prefix-list _AnyIpv4PrefixList
    !
    action accept
     set
      preference 1000
      omp-tag 200
    !
   !
  !
<<omited>>
site-list remote_branches
site-id <specifiy site-id range for all remote branch sites>
```

在DC，從SD-WAN路由器向核心交換機轉發流量時，在LAN端將路由通告到BGP時，會對AS-PATH欄位進行操作。在BGP中重分配OMP路由時，在BGP配置中應用路由對映。

當MPLS鏈路正常運行時，由於未通過LTE接收任何流量，因此在BGP中只有主cEdge重分配路由。但是，如果MPLS鏈路出現故障：

- 對於VPN 10，ASR cEdge透過附加AS-PATH欄位四次來重分配路由，而ISR cEdge透過附加AS-PATH欄位三次來重分配。此配置可確保優先使用ISR cEdge來傳送回覆。
- 同樣，對於VPN 20，ASR cEdge重新分發字首而不附加任何AS-PATH，而ISR cEdge透過附加AS-PATH欄位三次來重新分發字首。這可以確保優先使用ASR cEdge。

在地化的策略配置

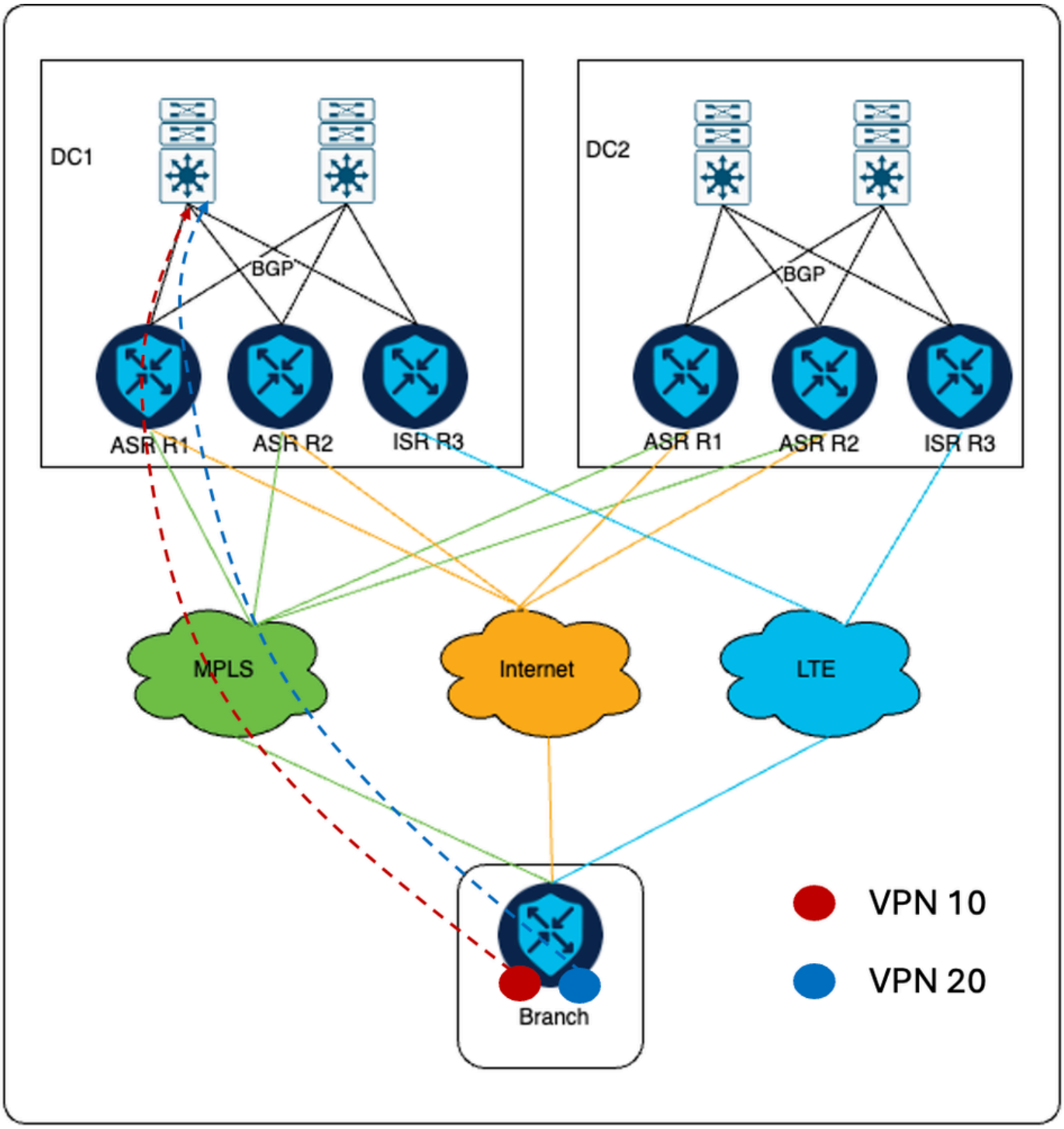
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
```

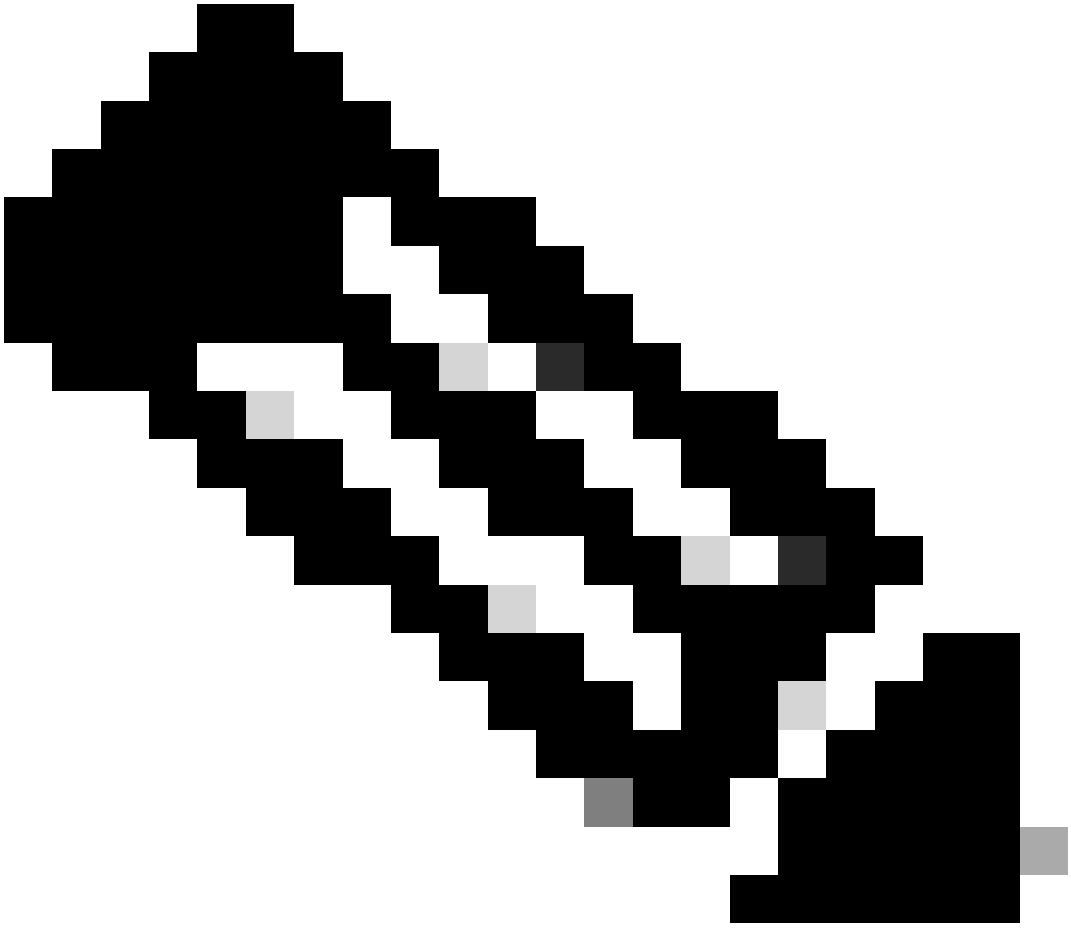
```
route-map DC1_VPN-10_out_v001 permit 65535

route-map DC2_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc2-asnum> <dc2-asnum> <dc2-asnum> <dc2-asnum>
route-map DC2_VPN-10_out_v001 permit 65535

route-map DC1_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum>
route-map DC1_Backup_All_out_v001 deny 65535

route-map DC2_Backup_All_out_v001 permit 1
match omp-tag 100
set as-prepend <dc2-asnum> <dc2-asnum> <dc2-asnum>
route-map DC2_Backup_All_out_v001 deny 65535
```

流量傳輸

正常情境

當MPLS鏈路啟動時，來自VPN 10和VPN 20的所有流量都會透過MPLS傳輸。

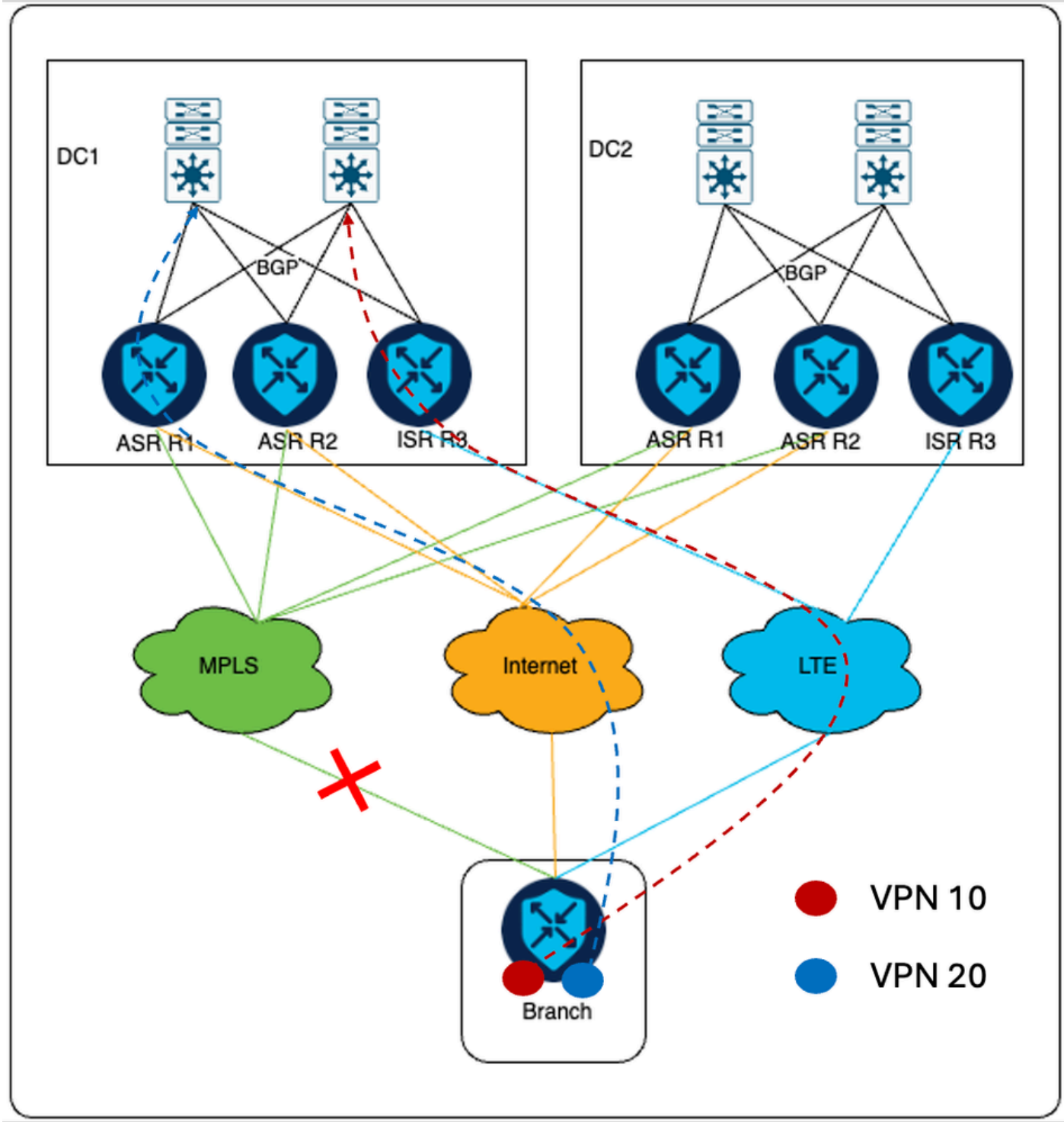

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



註：DC1是主DC。

容錯移轉案例

如果MPLS鏈路發生故障，VPN 10流量將透過LTE傳輸流向ISR cEdge。其中as VPN 20流量透過網際網路傳輸傳送到ASR cEdge裝置。



對於來自核心交換機的返回流量，對於VPN 10流量，將傳送到ISR cEdge，因為與在地化策略部分中指定的ASR相比，透過ISR的AS-PATH長度更短。同樣，由於AS-PATH透過ASR的流量比ISR小，因此VPN 20流量會傳送到ASR cEdge。

其他資訊

在早期設定中，每個DC的所有cEdge僅透過網際網路傳輸連線到SD-WAN控制器。因此，ISR路由器配置了Internet隧道。要求是確保ISR cEdge僅透過LTE傳輸形成到遠端分支機構的IPsec隧道，並且為了達到給定要求，ISR的網際網路傳輸上的隧道顏色必須配置為客戶設定中沒有使用的公共顏色。

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）。