数据中心中数据平面隧道限制的地址数量

目录

简介

本文档介绍一种解决方案，用于解决数据中心SD-WAN cEdge在数据平面隧道限制附近出现的扩展问题。

先决条件

要求

Cisco建议您应具备SD-WAN的相关知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

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。

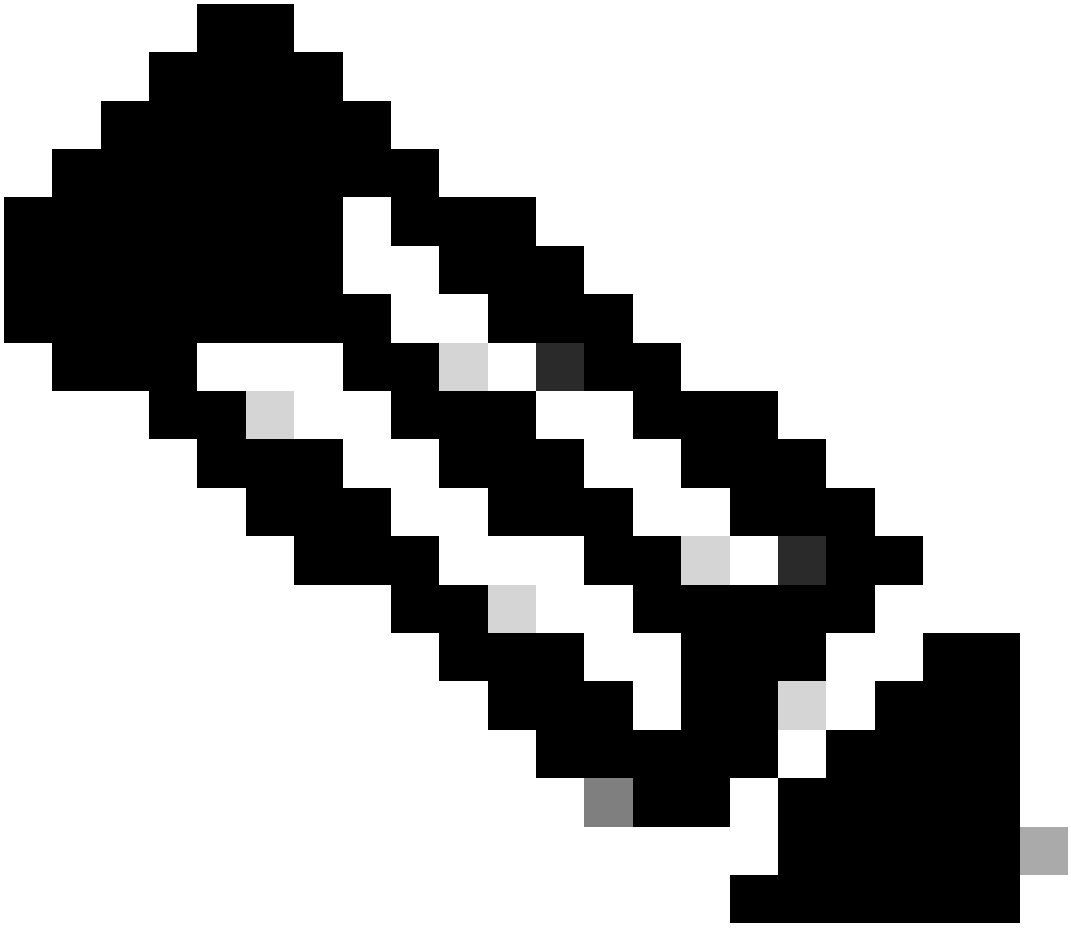
背景信息

网络设计概述:

- VPN：VPN 10、VPN 20
- 传输链路：多协议标签交换(MPLS)、LTE、互联网
- 路由器详细信息：
  - 主路由器：每个数据中心2个
    - 型号：ASR1002-HX
    - Cisco IOS XE软件版本：17.06.03a.0.2
  - 辅助路由器：每个数据中心1个
    - 型号：ISR4451-X
    - Cisco IOS XE软件版本：17.06.03a.0.22
- 路由协议：在数据中心LAN端使用边界网关协议(BGP)

问题

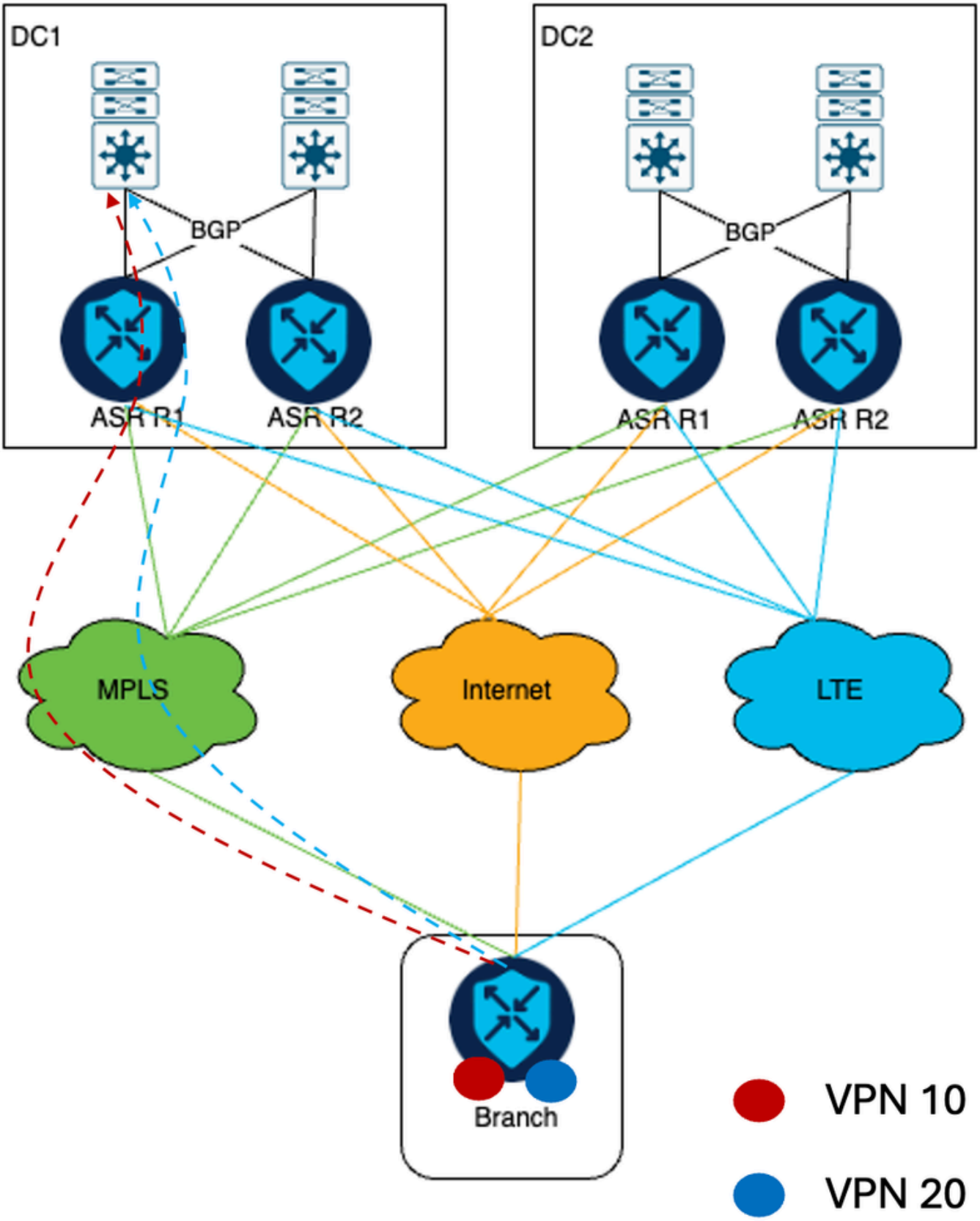
本文档讨论了拓扑图所示的客户案例研究，该客户的网络基础设施包括两个数据中心，每个数据中心部署两个ASR1002-HX SD-WAN cEdge。此网络架构旨在将大约3000个存储位置合并到SD-WAN重叠网络上，同时利用三个不同的传输链路的可用性。



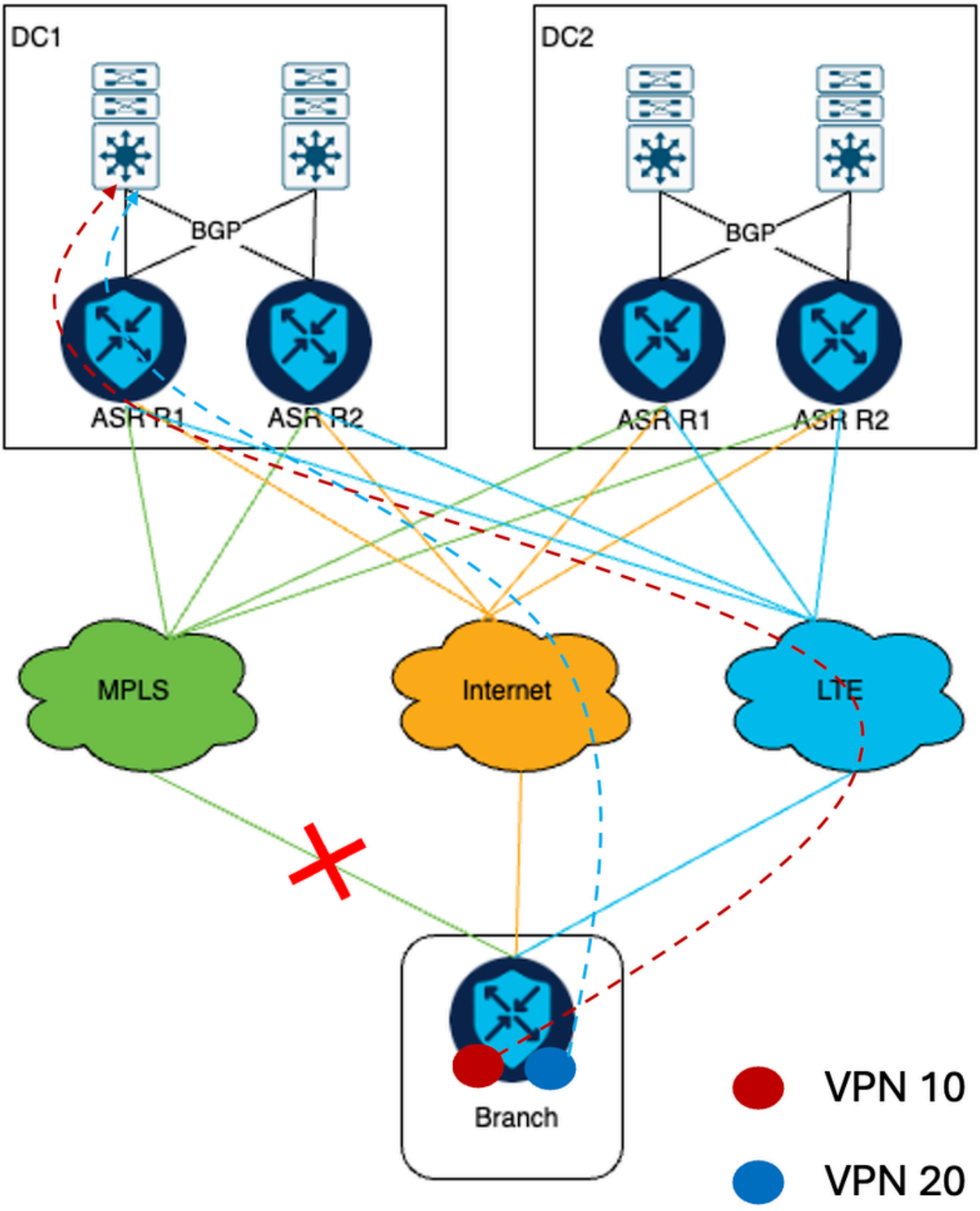
注意：集中星型拓扑已部署。DC1和DC2 cEdge是集线器。所有远程分支机构都使用DC cEdge通过三个可用传输形成IPsec隧道。

现有网络图

来自VPN 10和VPN 20的所有流量都会通过MPLS传输。



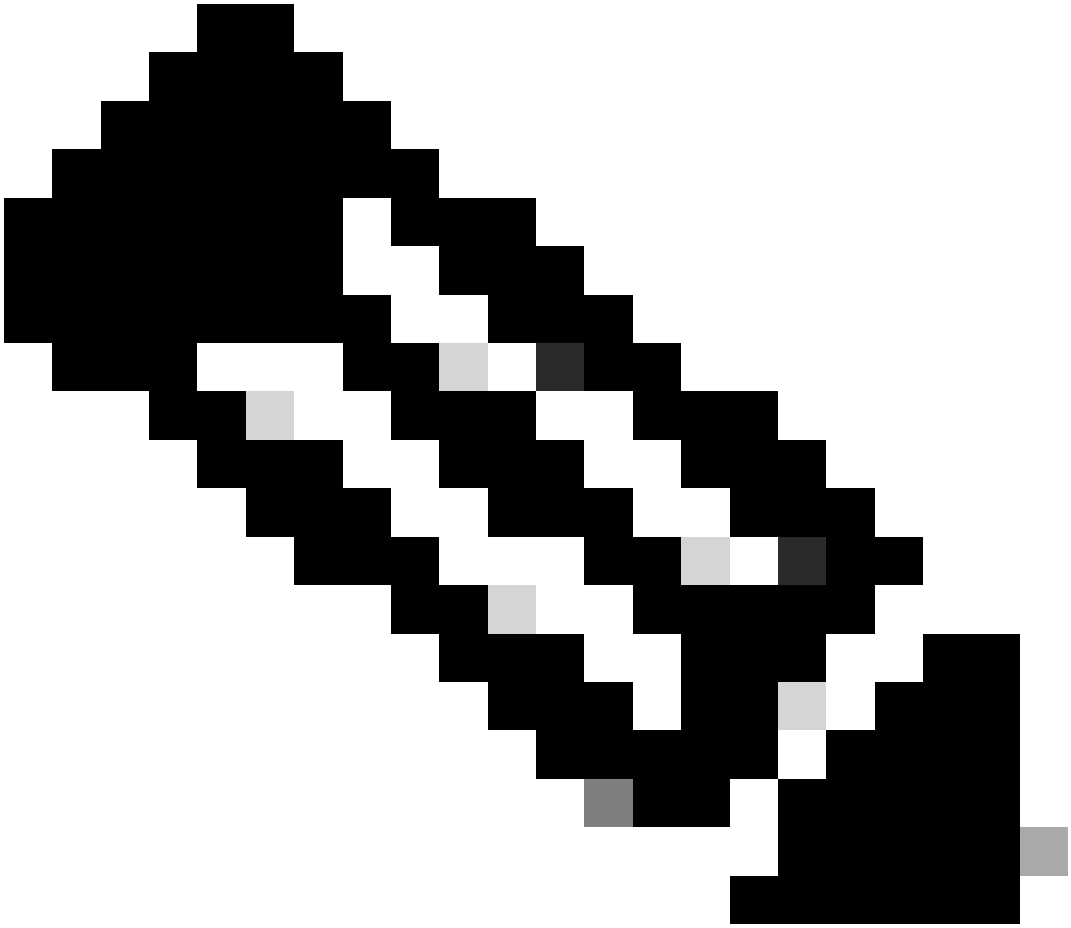
如果MPLS链路断开，VPN 10流量将转移到LTE传输，而VPN 20流量将转移到Internet传输。



此场景中的技术难题源于客户网络部署的规模和特定要求。 考虑部署3000台SD-WAN路由器，这些路由器通过三种类型的传输建立IPSec隧道到数据中心路由器，因此ASR1002-HX主前端路由器上形成的IPSec隧道总数达到9000。但是，ASR1002-HX仅限于8000个IPSec隧道(来源：ASR1K数据表)。

解决方案

为了解决此问题，客户决定在每个DC中根据客户未来的可扩展性需求添加一个ISR4451-X cEdge设备。

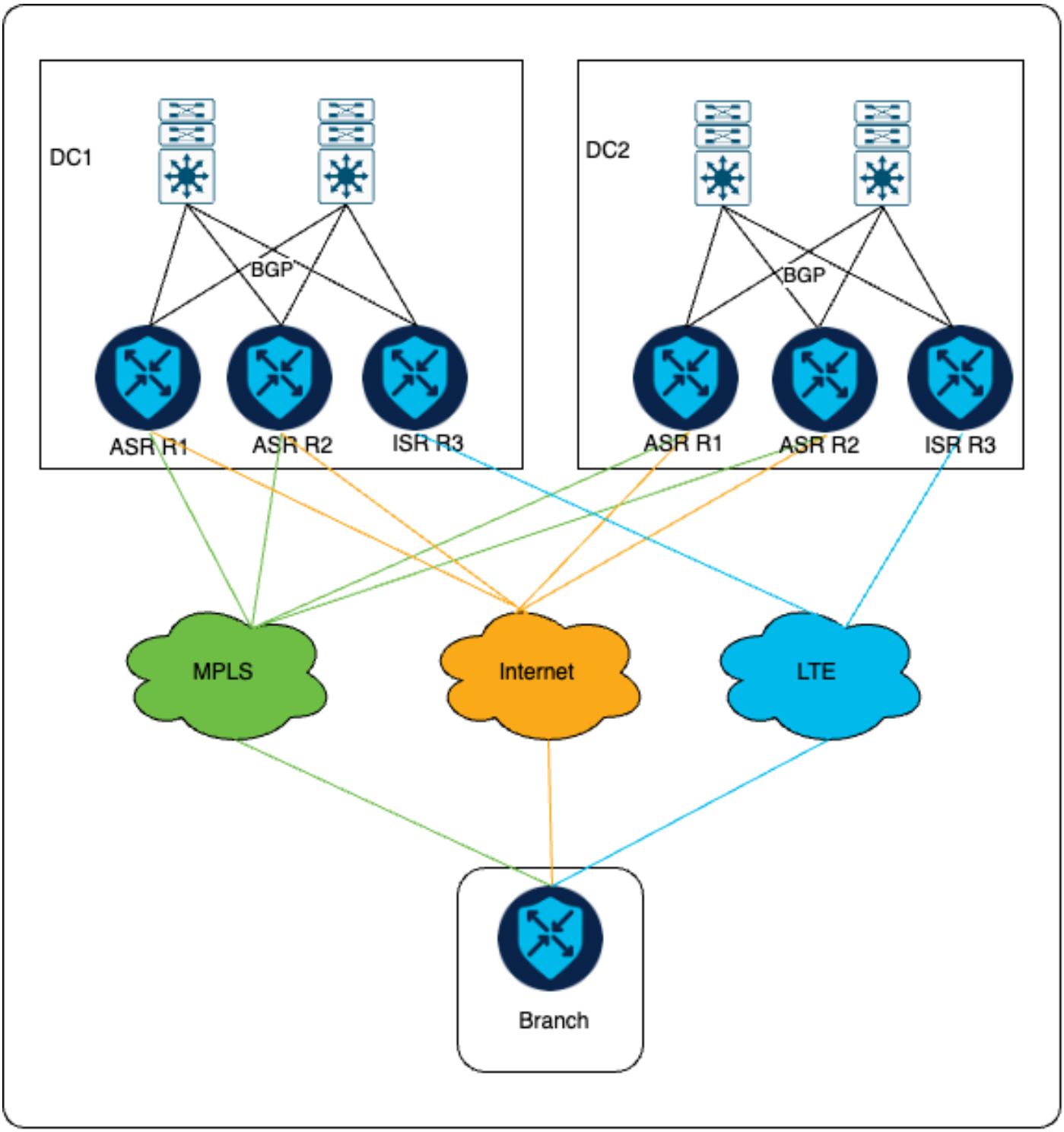


注意：根据客户的可扩展性要求确定其他设备型号。

网络拓扑

作为解决方案的一部分，主聚合服务路由器(ASR) cEdge继续通过MPLS和互联网传输形成IPSec隧道，而新安装的集成服务路由器(ISR) cEdge仅通过LTE传输形成IPsec隧道。

如图所示，IPSec隧道通过MPLS和互联网在ASR前端和分支机构之间建立，而ISR和分支机构之间则通过LTE单独建立IPSec隧道。



客户要求是，在正常情况下，所有VPN 10和VPN 20流量都使用MPLS传输进行通信。但是，在MPLS链路发生故障时，VPN 20流量通过互联网传输重新路由，而VPN 10流量通过LTE传输重新路由，其行为与添加其他cEdge前一样。

配置

使用集中和本地化的策略，以确保流量根据客户的偏好通过正确的传输发出。对通过互联网链路和LTE链路从分支机构位置传入的流量进行标记。这些标记用于确保头端上的LAN交换机向ISR路由器正确发送VPN 10的应答消息，并确保VPN 20流量发送到ASR头端设备。

集中策略配置

下面是为满足客户要求而准备的策略。对于通过互联网链路到达的流量，会分配OMP标记200。另一方面，通过LTE链路到达的流量分配的OMP标签为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，从SD-WAN路由器向核心交换机转发流量时，在LAN端将路由通告到BGP时，会控制AS-PATH字段。在BGP中重分配OMP路由时，在BGP配置中应用路由映射。

当MPLS链路正常运行时，由于未通过LTE接收流量，因此只有主cEdge在BGP中重分布路由。但是，如果MPLS链路出现故障：

- 对于VPN 10，ASR cEdge通过附加AS-PATH字段四次来重新分发路由，而ISR cEdge通过附加AS-PATH字段三次来进行重新分发。此配置可确保首选ISR cEdge来发送应答。
- 同样，对于VPN 20，ASR cEdge重新分发前缀而不附加任何AS-PATH，ISR cEdge通过附加AS-PATH字段三次来重新分发前缀。这可确保首选ASR cEdge。

本地化的策略配置

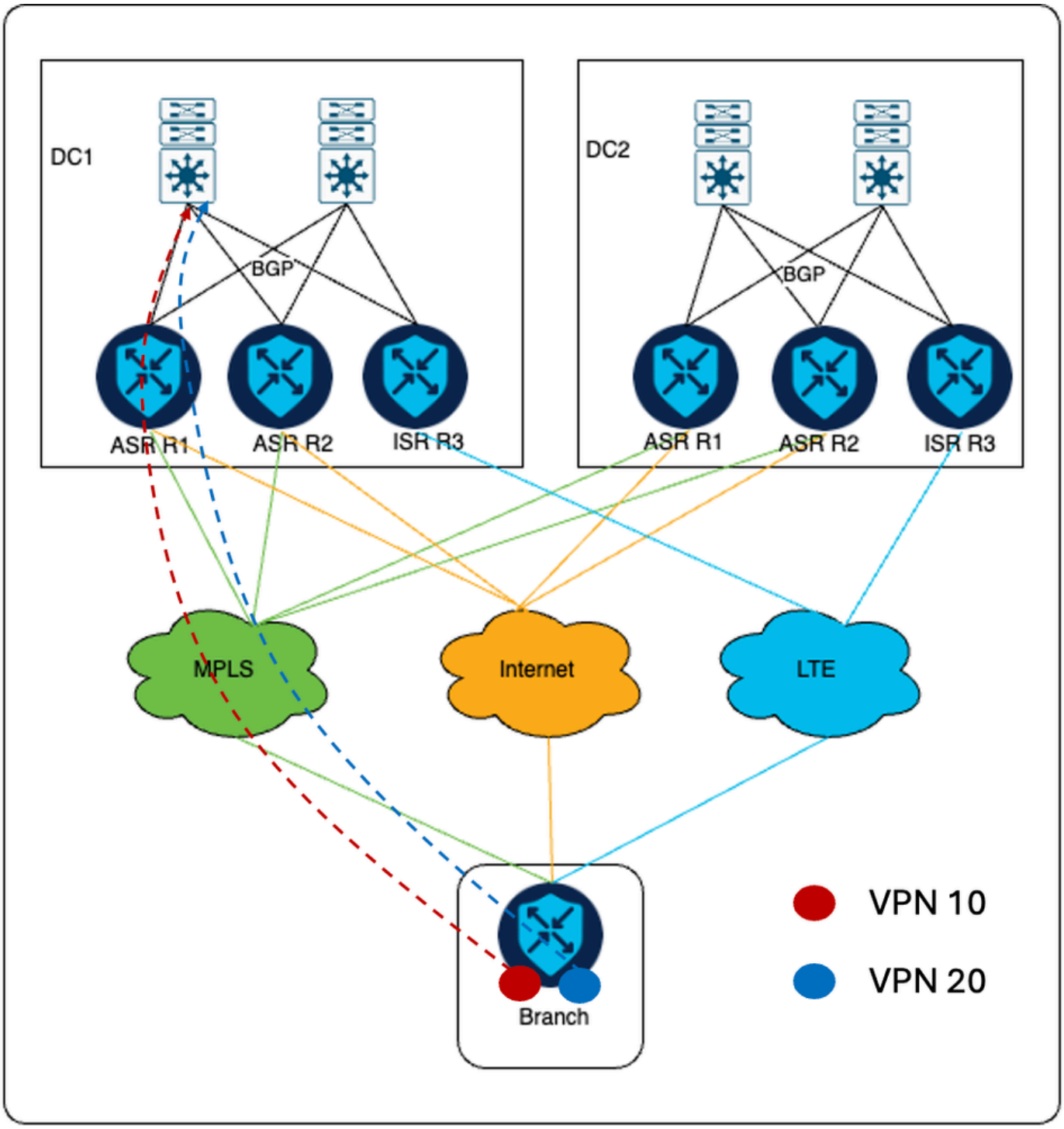
```
route-map DC1_Primary_VPN-10_out_v001 permit 1
match omp-tag 200
set as-prepend <dc1-asnum> <dc1-asnum> <dc1-asnum> <dc1-asnum>
```

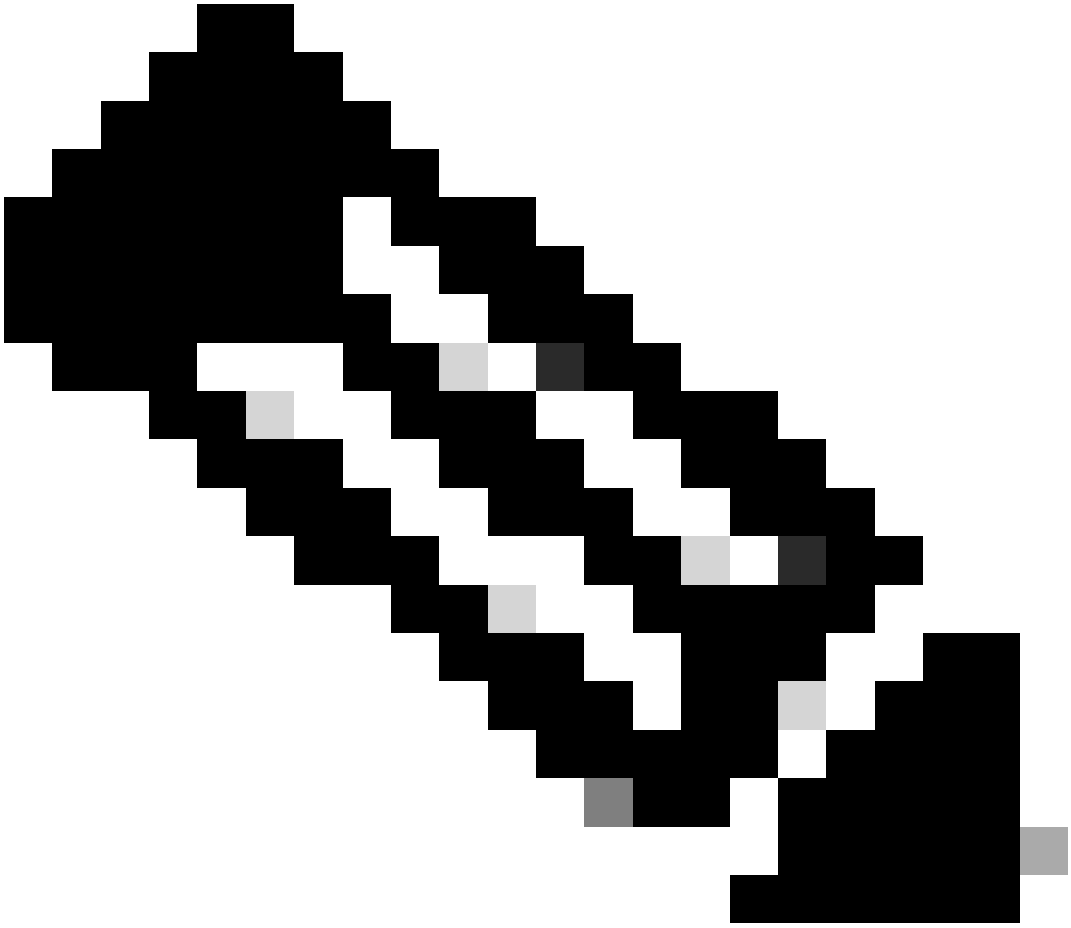
```
route-map DC1_VPN-10_out_v001 permit 65535

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
```

流量传输

正常情况

当MPLS链路启动时，来自VPN 10和VPN 20的所有流量都会通过MPLS传输。

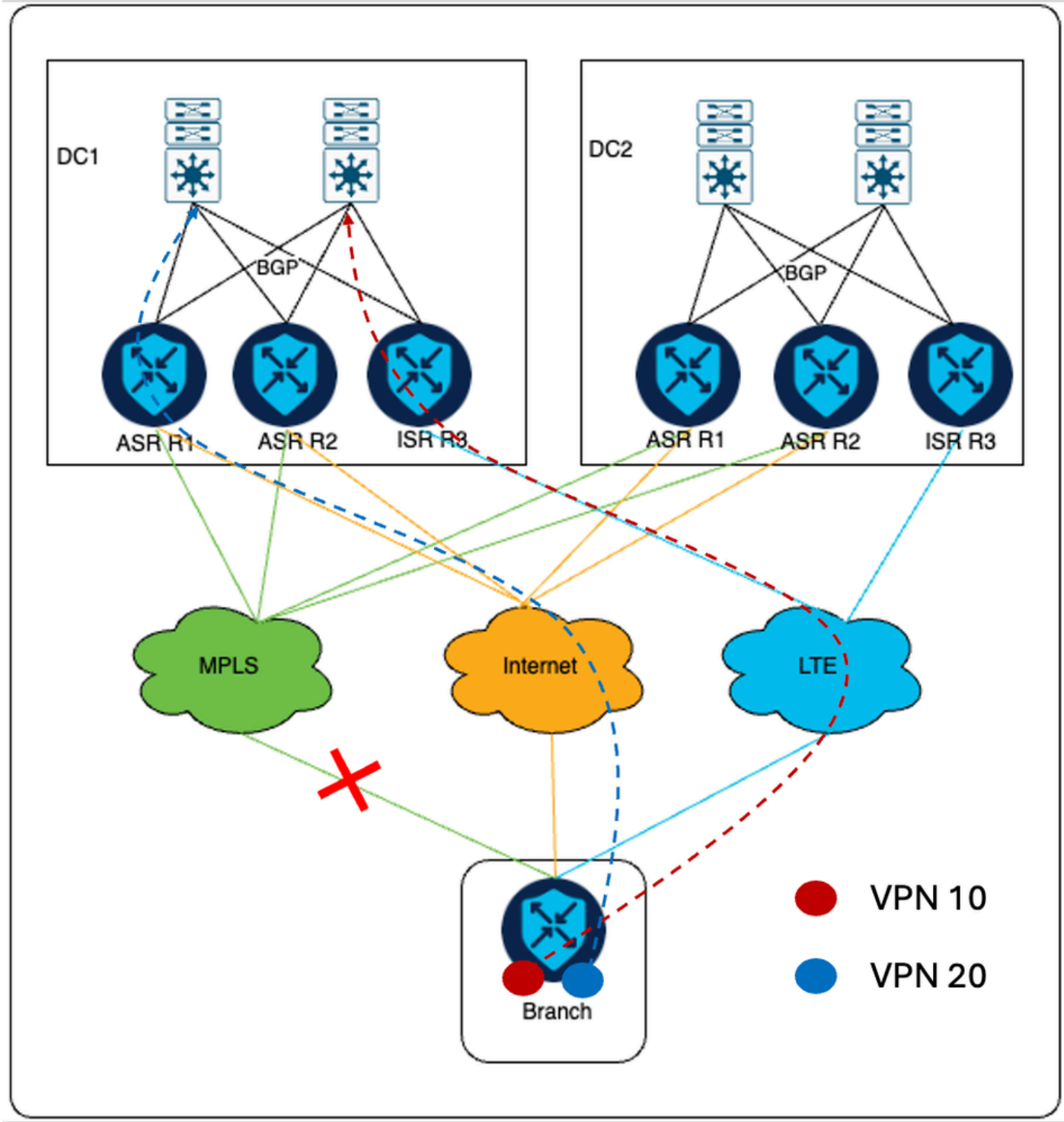

DC1
BGP
ASR R1
ASR R2
ISR R3
DC2
BGP
ASR R1
ASR R2
ISR R3
MPLS
Internet
LTE
Branch
VPN 10
VPN 20



注意：DC1是主DC。

故障切换方案

如果MPLS链路发生故障，VPN 10流量将通过LTE传输流向ISR cEdge。其中，VPN 20流量通过互联网传输发送到ASR cEdge设备。



对于来自核心交换机的返回流量，对于VPN 10流量，将发送到ISR cEdge，因为通过ISR的AS-PATH长度比本地化策略部分中指定的ASR更短。同样，由于AS-PATH通过ASR比ISR更小，因此VPN 20流量会发送到ASR cEdge。

其他信息

在早期设置中，每个DC的所有cEdge仅通过互联网传输连接到SD-WAN控制器。因此，ISR路由器配置了Internet隧道。要求是确保ISR cEdge仅通过LTE传输形成到远程分支机构的IPsec隧道，并且为了实现给定的要求，必须将ISR的互联网传输上的隧道颜色配置为在客户设置中未使用的公共颜色。

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）。