

使用全局路由表从 MPLS VPN 访问互联网

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景理论](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[CE 1 和 CE 2 之间的 VPN 连通性](#)

[CE 1 到因特网的连通性](#)

[故障排除](#)

[相关信息](#)

简介

使用全局路由表，本文目的将展示用于的配置示例访问从多协议标签交换(MPLS)的互联网-基于VPN。

在某些网络环境中，它要求访问从基于MPLS的VPN的互联网除维护之外在公司站点中的VPN连通性的继续。此配置示例着重提供从包含默认路由到互联网网关路由器的VPN路由与转发(VRF)的互联网访问(IGW)。

先决条件

要求

[MPLS转发](#)和[MPLS VPN](#)基本的了解要求充分地了解本文内容。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS软件版本12.1(3)T。版本12.0(5)T包括MPLS VPN功能
- 从3600系列的任何Cisco路由器或以上，例如Cisco 3660或7206

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

背景理论

在此配置示例中，这些策略到位：

- 有连通性的一个路由器对互联网附加对MPLS网络。它可能或可能不注入边界网关协议(BGP)路由全球路由表。**注意：** PE路由器了解BGP。路由器例如(执行作为供应商核心路由器)的千兆交换路由器(GSR)根本不运行BGP。
- 没有VRF的需求能有从互联网(全局BGP表)的一完整路由表，因此静态默认路由在指向IGW的全局下一跳地址的VRF放置。
- VPN客户使用是可路由的在全球互联网路由表里的注册的唯一地址范围。在本文讨论的访问方法不推荐客户有仅专用地址在他们的网络的地方。

规则

这些缩略语用于本文：

- CE -用户边缘路由器
- PE -供应商边缘路由器
- P - 提供商核心路由器

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置

- 有关此配置的图示，请参阅[网络图](#)。在本示例中，CE 1 与 CE 2 在同一 VPN 内。它们配置于 customer1 VRF 下，因为不要求 VRF 拥有来自 Internet 的完整路由表（根据本文档[背景理论](#)部分中的策略）。
- 在 CE 1 上的 customer1 VRF 中配置有静态默认路由，指向 IGW。通过在 customer1 VRF 中设置静态默认路由，与 customer1 VRF 内的任何路由都不匹配的数据包将发送至 IGW。

注意： 因为 Internet 网关下一跳 192.168.67.1 不是 customer1 VRF 的一部分，所以在 customer1 VRF 下配置有默认路由，指向 Internet 网关接口 s8/0 IP 192.168.67.1。到 192.168.67.1 的路由不在 customer1 VRF 内，因此，需要在配置于 customer1 VRF 之下的静态默认路由内设置一个全局关键字。该全局关键字指定静态路由的下一跳地址在全局路由表内进行解析，而不是在 customer1 VRF 内进行解析。

下面是静态路由的示例。

```
ip route vrf customer1 0.0.0.0 0.0.0.0 192.168.67.1 global
```

在 customer1 VRF 中为静态路由设置全局关键字可确保发往 Internet 的所有数据包都路由至 Internet 网关，继而路由至 Internet。

注意： PE 1 中的默认路由配置为指向 Internet 网关的串行接口 IP 地址 (192.168.67.1)，而不是指向环回地址 (10.1.1.6)。如果 Internet 网关与 Internet (R7) 之间出现连接故障，可避免出现路由黑洞。如果默认路由指向 Internet 网关的环回地址，并且 Internet 网关与 R7 中断连接，所有数据包会继续路由至 Internet 网关。这是因为环回地址保持正常工作（不同于 192.168.67.1，当接口 s8/0 出现故障时，会从全局路由表中撤消该地址），默认路由继续存在于路由表中。

下一步是确保从 Internet 返回目标 CE 1 网络 11.11.11.0/24 的数据包从 Internet 网关路由至 PE 1，然后通过 MPLS 核心路由至 CE 1。实现这一任务的方法是为 CE 1 网络配置静态路由，指向

PE 1 上的全局路由表中的 Serial 8/0 接口。将其重新分配到开放最短路径优先 (OSPF) 中，以便 Internet 网关的全局路由表中有该路由。这样，Internet 网关将来自 Internet 的所有数据包路由至 PE 1，并路由至 CE 1 之外的最终目标。

下面的示例是在 PE 1 上的配置中使用的 `ip route` 命令。

```
ip route 11.11.11.0 255.255.255.0 Serial8/0 192.168.10.1
```

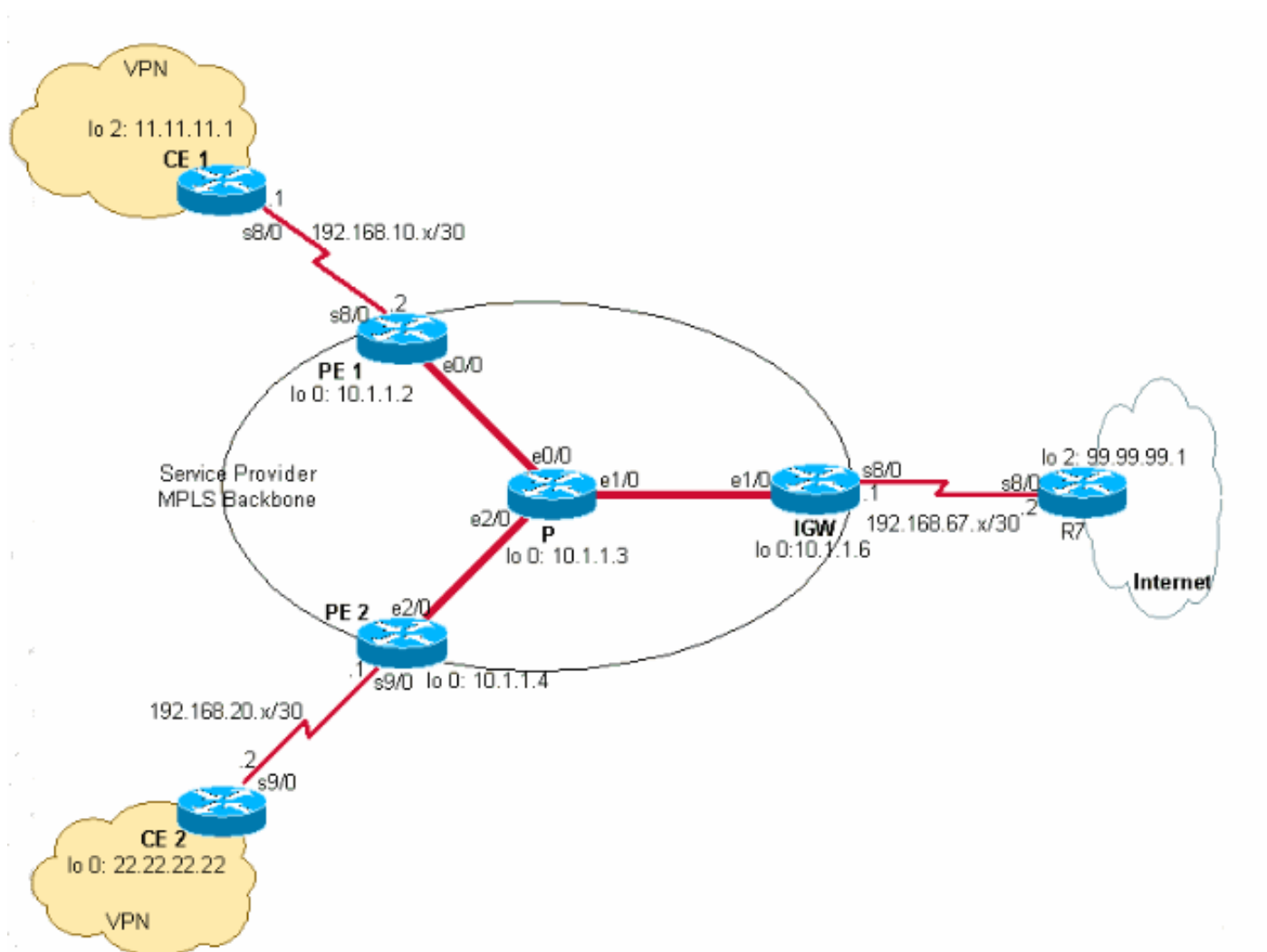
注意：除了上述在全局路由表中配置的静态路由，还有 customer1 VRF 内配置的静态路由，该路由用于 VPN 网络层可达性信息 (NLRI)。在 PE 1 上，它的配置如下所示。

```
ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1
```

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用下图所示的网络设置。



配置

本文档使用如下所示的配置。

- [CE 1](#)

- [PE 1](#)
- [P](#)
- [IGW](#)
- [PE 2](#)
- [CE 2](#)

CE 1
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>
PE 1
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>
P
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>
IGW
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>
PE 2
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>
CE 2
<code>ip route vrf customer1 11.11.11.0 255.255.255.0 192.168.10.1</code>

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

[CE 1 和 CE 2 之间的 VPN 连通性](#)

若要验证 CE 1 与 CE 2 之间的 VPN 连接，CE 1 应能到达 CE 2 的网络 22.22.22.0/24，反之亦然。若要对此进行检查，请在 PE 1 上的 customer1 VRF 中验证到网络 22.22.22.0/24 的路由。

[命令输出解释程序工具](#) ([仅限注册用户](#)) 支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

1. **show ip route vrf customer1** 命令确认从 10.1.1.4 (PE 2 的环回地址) 所获知的到网络 22.22.22.0/24 的路由，如以下输出中的突出显示部分所示。PE-1# `show ip route vrf customer1`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.67.1 to network 0.0.0.0

```
192.168.10.0/30 is subnetted, 1 subnets
C    192.168.10.0 is directly connected, Serial8/0
    22.0.0.0/24 is subnetted, 1 subnets
B    22.22.22.0 [200/0] via 10.1.1.4, 01:00:50
    11.0.0.0/24 is subnetted, 1 subnets
S    11.11.11.0 [1/0] via 192.168.10.1
S*   0.0.0.0/0 [1/0] via 192.168.67.1
```

2. 同样，在 PE 2，customer1 VRF 中到网络 11.11.11.0/24 的路由如下例所示。PE-2# show ip route vrf customer1

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is 192.168.67.1 to network 0.0.0.0

```
192.168.10.0/30 is subnetted, 1 subnets
B    192.168.10.0 [200/0] via 10.1.1.2, 01:00:09
    22.0.0.0/24 is subnetted, 1 subnets
S    22.22.22.0 [1/0] via 192.168.20.2
    192.168.20.0/30 is subnetted, 1 subnets
C    192.168.20.0 is directly connected, Serial9/0
    11.0.0.0/24 is subnetted, 1 subnets
B    11.11.11.0 [200/0] via 10.1.1.2, 01:00:09
S*   0.0.0.0/0 [1/0] via 192.168.67.1
```

3. 现在检查 CE 1 与 CE 2 之间的连接，方法是从 CE 1 使用源 IP 地址 11.11.11.1 ping CE 2 上的主机 22.22.22.22。CE-1# ping

```
Protocol [ip]:
Target IP address: 22.22.22.22
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 11.11.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

[CE 1 到因特网的连通性](#)

执行下列步骤验证从 CE1 到 Internet 的连接。

1. 所有从 CE 1 到 Internet 或 VPN 的数据包都使用在 CE 1 中配置的、指向 PE 1 的默认路由进行路由，如下所示。CE-1# show ip route 0.0.0.0

```
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
    * 192.168.10.2
  Route metric is 0, traffic share count is 1
```

2. 传入 PE 1 接口 s8/0 的数据包使用 customer1 VRF 路由表进行路由。PE 1 在 customer1 VRF 中有一个默认路由，指向 IGW IP 地址 192.168.67.1，如 PE 1 上 show ip route vrf customer1 的输出所示。PE-1# show ip route vrf customer1

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.67.1 to network 0.0.0.0
```

```
192.168.10.0/30 is subnetted, 1 subnets
C    192.168.10.0 is directly connected, Serial8/0
22.0.0.0/24 is subnetted, 1 subnets
B    22.22.22.0 [200/0] via 10.1.1.4, 01:21:11
11.0.0.0/24 is subnetted, 1 subnets
S    11.11.11.0 [1/0] via 192.168.10.1
s*   0.0.0.0/0 [1/0] via 192.168.67.1
```

3. 因为 PE 1 上的默认路由配置有一个全局关键字，所以它会在其全局路由表中寻找下一跳 192.168.67.1，并路由至 IGW，如下所示。PE-1# show ip route 192.168.67.1

```
Routing entry for 192.168.67.0/30
  Known via "ospf 1", distance 110, metric 84, type intra area
  Last update from 10.10.23.3 on Ethernet0/0, 00:21:54 ago
  Routing Descriptor Blocks:
    * 10.10.23.3, from 10.1.1.6, 00:21:54 ago, via Ethernet0/0
  Route metric is 84, traffic share count is 1
```

4. 到达 IGW 的数据包根据自己从 R7 获知的 BGP 路由，路由至 Internet。在本示例中，您可以查看从 R7 获知的 BGP 路由以展示到 Internet 的连接。下面是 IGW 路由表中从 R7 获知的 BGP 路由（网络 99.99.99.0/24）。IGW# show ip route 99.99.99.0

```
Routing entry for 99.99.99.0/24
  Known via "bgp 100", distance 20, metric 0
  Tag 200, type external
  Last update from 192.168.67.2 01:37:25 ago
  Routing Descriptor Blocks:
    * 192.168.67.2, from 192.168.67.2, 01:37:25 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1源自 CE-1 的数据包路由至 Internet。
```

5. 对于要从 Internet 返回 CE 1 网络 11.11.11.0/24 的数据包，IGW 在其全局路由表中应有一个指向 PE 1 的路由。在 PE 1 的全局路由表中配置有一个静态路由，指向与 CE 1 相连的 PE 1 上的 s8/0 接口，并会重新分配到 OSPF 中。这样可确保 IGW 在其全局路由表中拥有一个指向 PE 1 的路由。PE 1 上的静态路由以及 IGW 上的 OSPF 获知路由如下所示。IGW# show ip route 11.11.11.0

```
Routing entry for 11.11.11.0/24
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward metric 20
  Last update from 10.10.36.3 on Ethernet2/0, 00:34:34 ago
  Routing Descriptor Blocks:
    * 10.10.36.3, from 10.1.1.2, 00:34:34 ago, via Ethernet2/0
      Route metric is 20, traffic share count is 1
```

```
PE-1# show ip route 11.11.11.0
Routing entry for 11.11.11.0/24
  Known via "static", distance 1, metric 0
```

```
Redistributing via ospf 1
Advertised by ospf 1 subnets
Routing Descriptor Blocks:
* 192.168.10.1, via Serial8/0
  Route metric is 0, traffic share count is 1
```

6. 现在检查从 CE 1 到 Internet 的连接，方法是对 CE 1 源地址 11.11.11.1 ping R7 IP 地址 99.99.99.1。CE-1# ping

```
Protocol [ip]:
Target IP address: 99.99.99.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 11.11.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 99.99.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/32 ms
CE-1#
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [配置基本 MPLS VPN](#)
- [使用 OSPF 配置基本的 MPLS](#)
- [如何排除 MPLS VPN 故障](#)
- [MPLS 故障排除](#)
- [对初学者的MPLS 常见问题](#)
- [MPLS \(多协议标签交换\) 支持页](#)
- [MPLS for VPN \(VPN 多协议标签交换\) 支持页](#)
- [技术支持 - Cisco Systems](#)