Cisco IOS NAT — 與MPLS VPN整合

目錄

簡介

Cisco IOS®網路位址轉譯(NAT)軟體允許從多個MPLS VPN存取共用服務，即使VPN中的裝置使用重疊的IP位址也是如此。Cisco IOS NAT可感知VRF，可在MPLS網路中的提供商邊緣路由器上配置。

注意：只有傳統NAT支援IOS中的MPLS。目前，Cisco IOS不支援帶MPLS的NAT NVI。

MPLS VPN的部署預計將在未來幾年內迅速增加。允許快速擴展和靈活連線選項的通用網路基礎設施無疑將推動向Internetwork社群提供的服務的進一步增長。

然而，阻礙增長的障礙依然存在。IPv6及其在可預見的未來超出連線需求的IP地址空間的承諾仍處於早期部署階段。現有網路通常使用RFC 1918 中定義的私有IP編址方案。當存在地址空間重疊或重複時，網路地址轉換通常用於互連網路。

服務提供商和有網路應用程式服務想要提供或與客戶和合作夥伴共用的企業，將希望儘可能減輕服務使用者承受的任何連線負擔。最好是儘可能多的潛在使用者使用該產品，以實現預期目標或回報，甚至是強制性的。正在使用的IP編址方案不得成為排除潛在使用者的障礙。

通過在公共MPLS VPN基礎設施中部署Cisco IOS NAT，通訊服務提供商可以減輕客戶的部分連線負擔，並加快將更多共用應用服務連結到這些服務的更多消費者的能力。

NAT的優勢 — MPLS整合

NAT與MPLS的整合對服務提供商及其企業客戶都有好處。它為服務提供商提供了更多部署共用服務和訪問這些服務的選項。其他服務產品可能是競爭對手的獨特優勢。

對於服務提供商	對於VPN
更多服務產品	降低成本
增加訪問選項	更簡單的訪問
增加收入	解決靈活性

尋求外包某些當前工作量的企業客戶也可以從服務提供商提供的更廣泛的服務中受益。將執行任何必要地址轉換的負擔轉移到服務提供商網路可以減輕他們的複雜管理任務。客戶可以繼續使用私有編址，但仍可以訪問共用服務和網際網路。在服務提供商網路中整合NAT功能還可降低企業客戶的總成本，因為客戶邊緣路由器不必執行NAT功能。

設計注意事項

在考慮在MPLS網路中呼叫NAT的設計時，第一步是從應用的角度確定服務需求。您需要考慮使用的協定以及應用實施的任何特殊客戶端/伺服器通訊。確保Cisco IOS NAT支援和處理對所用協定的必要支援。文檔Cisco IOS NAT應用層網關中提供了支援的協定清單。

接下來，需要確定共用服務的預期使用率和預期流量速率（以每秒資料包數為單位）。NAT是路由器CPU密集型功能。因此，效能要求將成為選擇特定部署選項和確定所涉及的NAT裝置數量的一個因素。

另外，考慮應採取的任何安全問題和預防措施。雖然MPLS VPN根據定義是私有的，並且有效地分離流量，但共用服務網路通常在許多VPN中很常見。

部署方案

在MPLS提供商邊緣內部署NAT有兩種選項：

- 集中使用出口NAT PE
- 通過入口NAT PE分佈

在離共用服務網路最近的MPLS網路的出口點配置NAT功能的一些優勢包括：

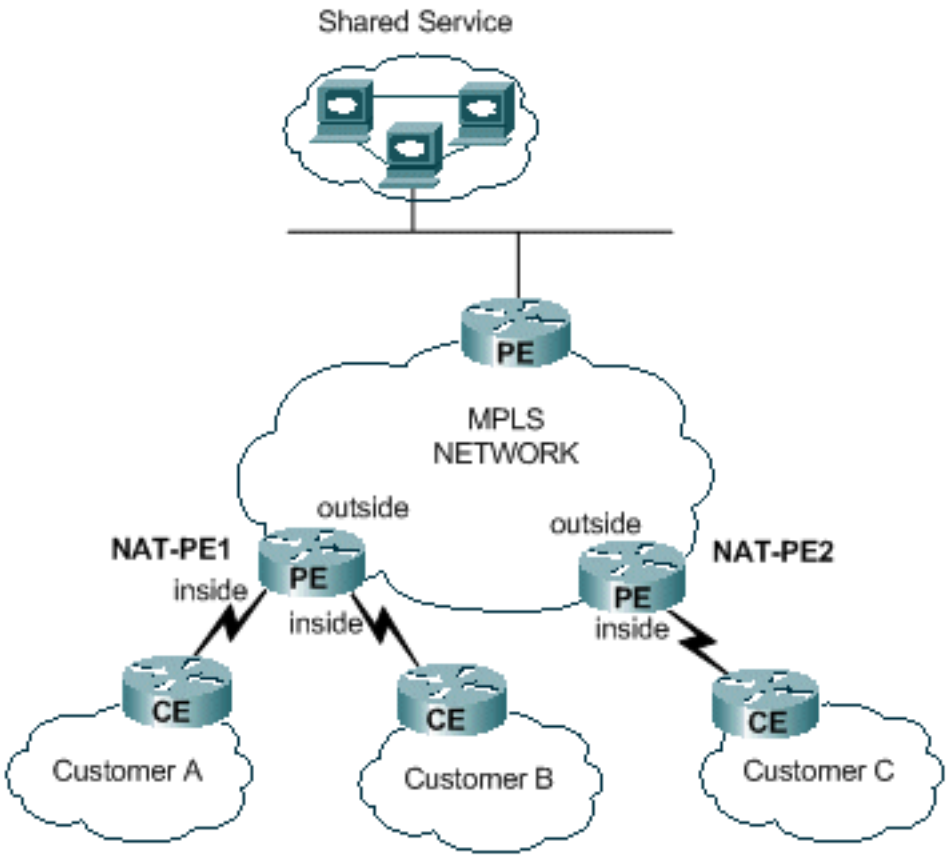
- 促進更簡單服務調配的集中配置
- 簡化的故障排除
- 增強的運營可擴充性
- 降低IP地址分配要求

但是，可擴充性和效能下降抵消了優勢。這是必須考慮的主要權衡。當然，如果確定不需要將此功能與MPLS網路整合，也可以在客戶網路中執行NAT功能。

輸入PE NAT

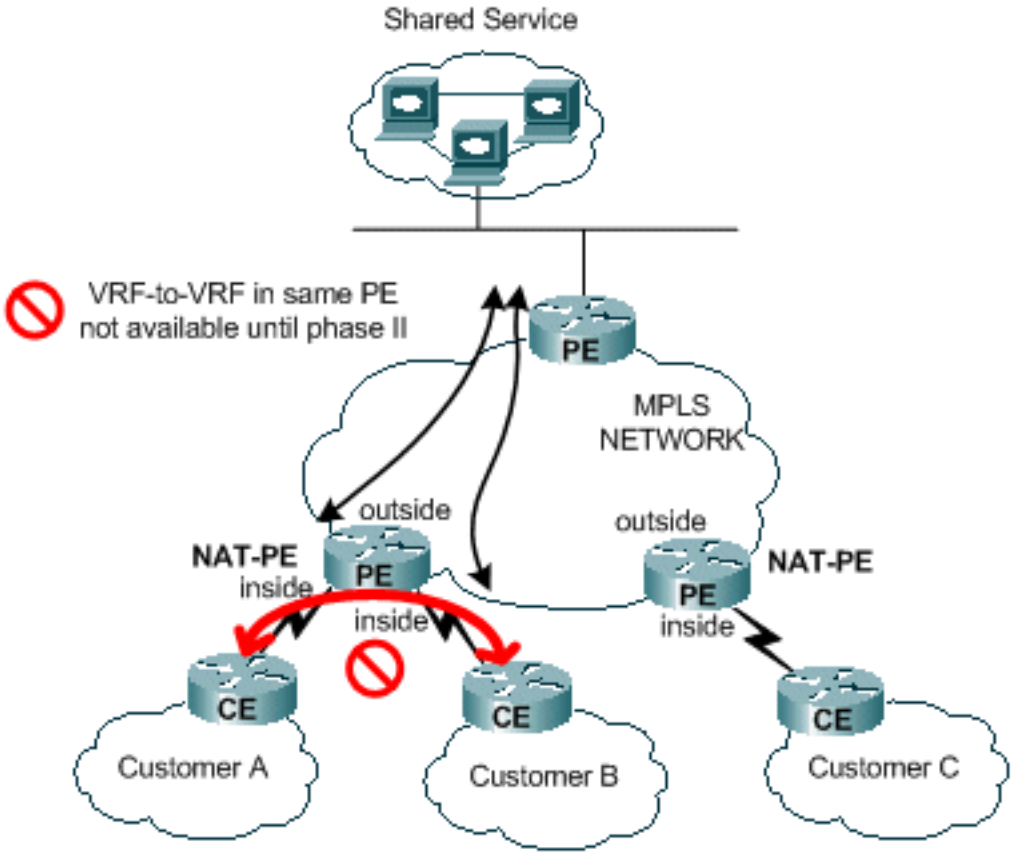
如圖1所示，可以在MPLS網路入口PE路由器上配置NAT。使用此設計，可以在很大程度上保持可擴充性，同時通過在多個邊緣裝置上分配NAT功能來最佳化效能。每個NAT PE處理本地連線到該PE的站點的流量。NAT規則和訪問控制清單或路由對映控制哪些資料包需要轉換。

圖1:輸入PE NAT



有一個限制阻止兩個VRF之間的NAT，同時也為共用服務提供NAT，如圖2所示。這是因為需要將介面指定為NAT「內部」和「外部」介面。未來的Cisco IOS版本計畫支援單個PE中的VRF之間的連線。

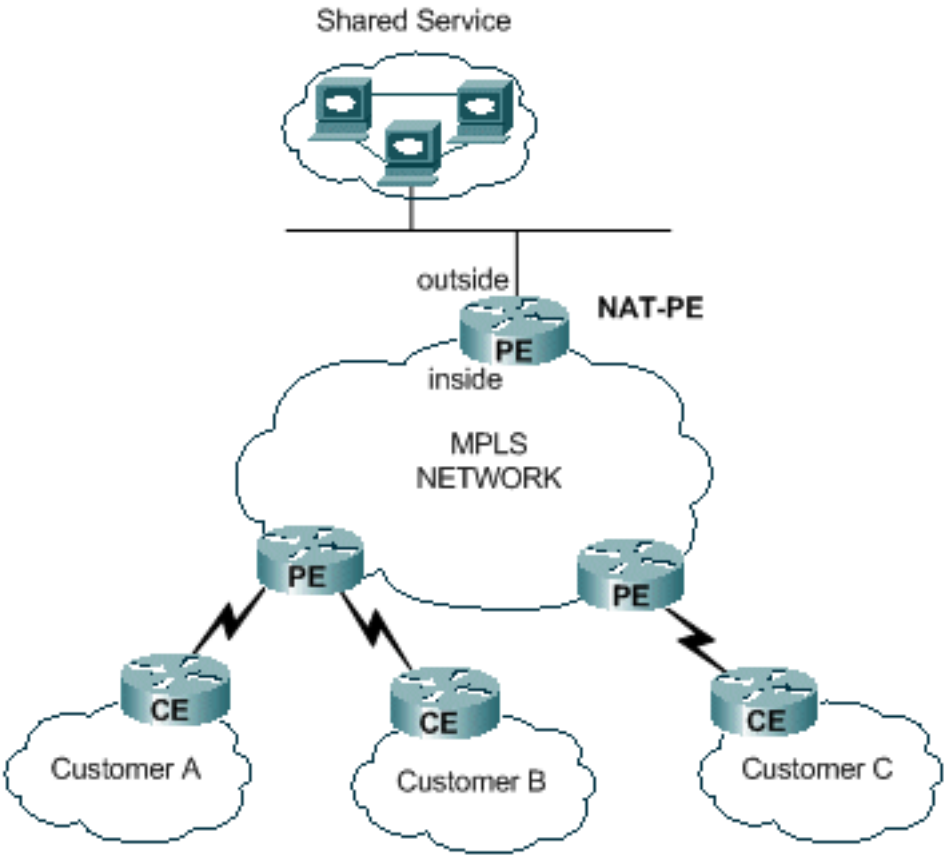
圖2:企業對企業



[輸出PE NAT]

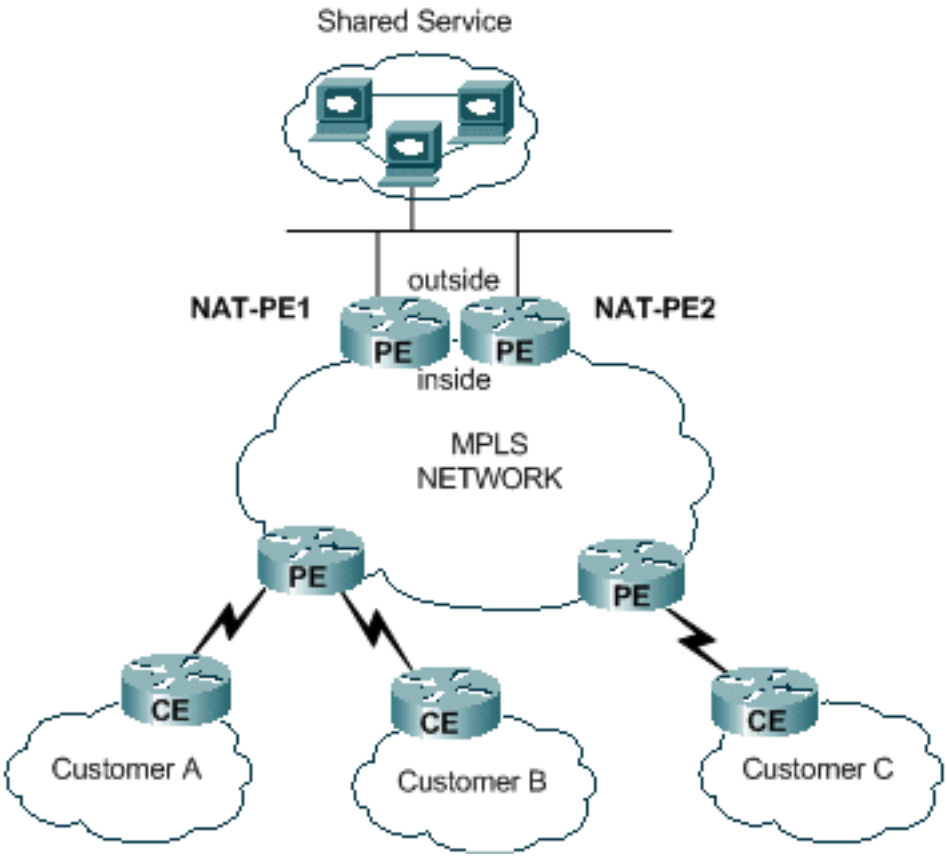
如圖3所示，可以在MPLS網路出口PE路由器上配置NAT。通過此設計，可擴充性在一定程度上降低，因為中央PE必須為訪問共用服務的所有客戶網路維護路由。還必須考慮應用效能要求，以便流量不會使必須轉換資料包IP地址的路由器負擔過重。因為對於使用此路徑的所有客戶都集中進行NAT，所以可以共用IP地址池；因此，所需的子網總數減少了。

圖3:輸出PE NAT



可以部署多台路由器來提高出口PE NAT設計的可擴充性，如圖4所示。在此方案中，可以在特定NAT路由器上「調配」客戶VPN。對於這組VPN的往返共用服務的聚合流量，將進行網路地址轉換。例如，來自客戶A和B的VPN的流量可以使用NAT-PE1，而來自客戶C的VPN的流量使用NAT-PE2。每個NAT PE將僅承載已定義的特定VPN的流量，並且僅維護返回這些VPN中站點的路由。可以在每台NAT PE路由器中定義單獨的NAT地址池，以便將資料包從共用服務網路路由到正確的NAT PE以進行轉換並路由回客戶VPN。

圖4:多個輸出PE NAT



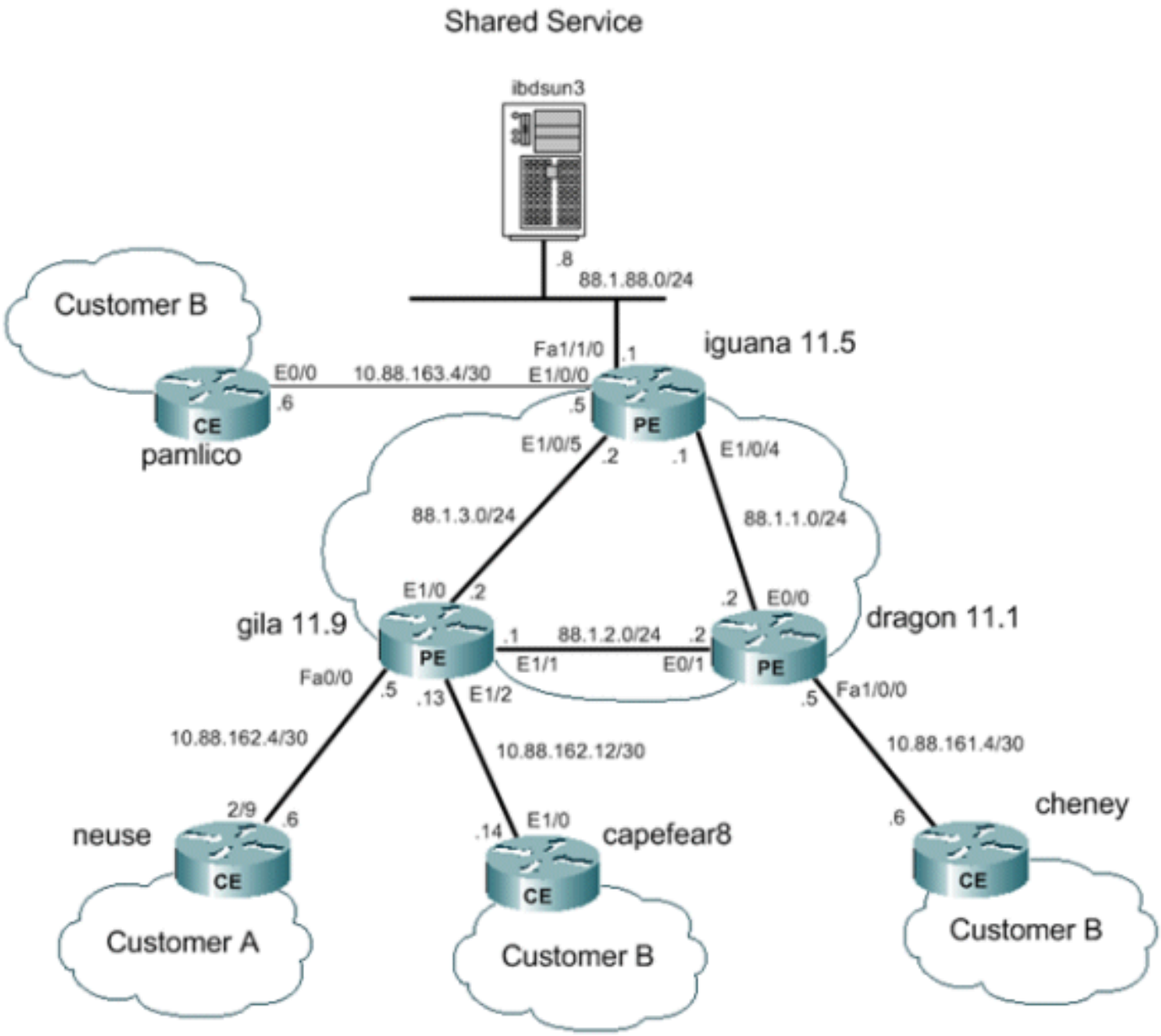
集中式設計確實對共用服務網路的配置方式施加了限制。具體而言，無法在共用服務VPN和客戶VPN之間使用MPLS VPN路由的匯入/匯出。這是由RFC 2547 所指定的MPLS操作的性質所引起的。當使用擴展社群和路由描述符匯入和匯出路由時，NAT無法從進入中央NAT PE的資料包確定源VPN。通常的情況是使共用服務網路成為通用介面而不是VRF介面。然後，將到共用服務網路的路由新增到與需要訪問共用服務的客戶VPN關聯的每個VRF表的中心NAT PE中，作為調配過程的一部分。稍後將對此進行更詳細的描述。

部署選項和配置詳細資訊

本節包含與每個部署選項相關的一些詳細資訊。這些示例全部取自圖5所示的網路。請參閱本圖瞭解本節的其餘部分。

注意：在用於說明本文VRF NAT運行的網路中，僅包括PE路由器。沒有核心「P」路由器。但是，基本機制仍然可以看到。

圖5:VRF NAT配置示例



輸出PE NAT

在本示例中，標有gila和dragon的提供商邊緣路由器配置為簡單PE路由器。共用服務LAN(iguana)附近的中心PE配置為NAT。需要訪問共用服務的每個客戶VPN共用一個NAT池。NAT僅對發往地址為88.1.88.8的共用服務主機的資料包執行。

輸出PE NAT資料轉送

利用MPLS，每個資料包在入口PE進入網路，並在出口PE退出MPLS網路。標籤交換路由器從入口到出口經過的路徑稱為標籤交換路徑(LSP)。 LSP是單向的。返回流量使用不同的LSP。

當使用出口PE NAT時，為來自共用服務使用者的所有流量有效定義轉發等價類(FEC)。換句話說，所有發往共用服務LAN的資料包都是通用FEC的成員。僅在網路的入口邊緣將資料包分配給特定FEC一次，並遵循LSP到出口PE。通過新增特定標籤在資料包中指定FEC。

從VPN到共用服務的資料包流

為了讓多個VPN中具有重疊地址方案的裝置訪問共用服務主機，需要NAT。當在出口PE配置NAT時，網路地址轉換表條目將包含VRF識別符號以區分重複地址並確保正確的路由。

圖6:傳輸到出口PE NAT的資料包

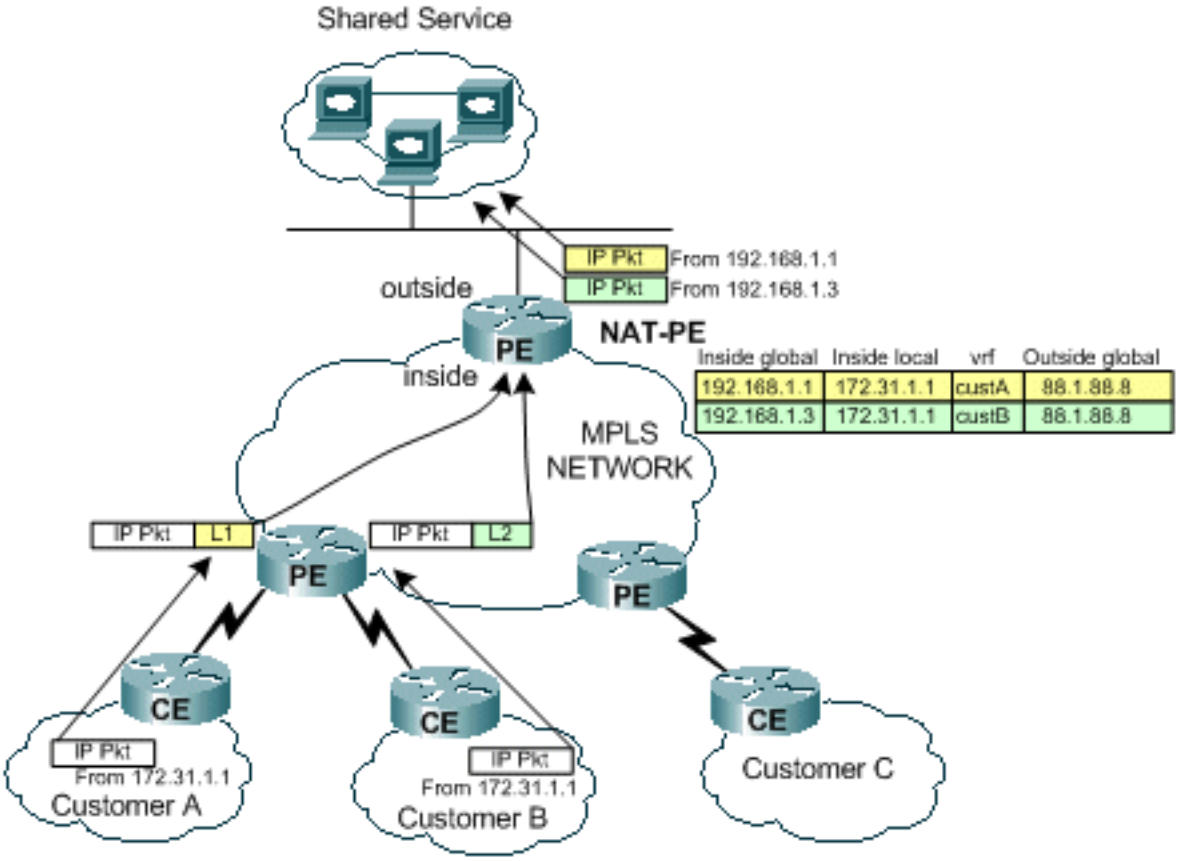


圖6顯示了來自具有重複IP編址方案的兩個客戶VPN的發往共用服務主機的資料包。圖中顯示了一個源自客戶A且源地址為172.31.1.1的資料包，該資料包將發往一台位於88.1.88.8的共用伺服器。另一個來自客戶B且源IP地址相同的資料包也將傳送到同一共用伺服器。當資料包到達PE路由器時，在轉發資訊庫(FIB)中對目標IP網路進行第3層查詢。

FIB條目指示PE路由器使用標籤堆疊將流量轉發到出口PE。堆疊中的底部標籤由目的地PE路由器(本例中為路由器iguana)分配。

```
iguana#
show ip cef vrf custA 88.1.88.8
88.1.88.8/32, version 47, epoch 0, cached adjacency 88.1.3.2
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
  via 88.1.11.5, 0 dependencies, recursive
    next hop 88.1.3.2, Ethernet1/0 via 88.1.11.5/32
    valid cached adjacency
    tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
```

```
iguana# show ip cef vrf custB 88.1.88.8
88.1.88.8/32, version 77, epoch 0, cached adjacency 88.1.3.2
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0, 88.1.3.2, tags imposed: {28}
  via 88.1.11.5, 0 dependencies, recursive
    next hop 88.1.3.2, Ethernet1/0 via 88.1.11.5/32
    valid cached adjacency
    tag rewrite with Et1/0, 88.1.3.2, tags imposed: {28}
```

```
iguana#
```

從顯示中可以看到，來自VRF custA的資料包將具有24(0x18)的標籤值，來自VRF custB的資料包將具有28(0x1C)的標籤值。

在本例中，由於網路中沒有「P」路由器，因此不會強加其他標籤。如果存在核心路由器，則會強制實施外部標籤，並且標籤交換的正常過程將在核心網路中進行，直到資料包到達出口PE。

由於gila路由器直接連線到出口PE，因此我們看到標籤在新增之前被彈出：

```
gila#
show tag-switching forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     88.1.1.0/24       0          Et1/1      88.1.2.2
       Pop tag     88.1.1.0/24       0          Et1/0      88.1.3.2
17     Pop tag     88.1.4.0/24       0          Et1/1      88.1.2.2
18     Pop tag     88.1.10.0/24      0          Et1/1      88.1.2.2
19     Pop tag     88.1.11.1/32      0          Et1/1      88.1.2.2
20     Pop tag     88.1.5.0/24       0          Et1/0      88.1.3.2
21     19          88.1.11.10/32     0          Et1/1      88.1.2.2
       22          88.1.11.10/32     0          Et1/0      88.1.3.2
22     20          172.18.60.176/32  0          Et1/1      88.1.2.2
       23          172.18.60.176/32  0          Et1/0      88.1.3.2
23     Untagged    172.31.1.0/24[V]  4980       Fa0/0      10.88.162.6
24     Aggregate   10.88.162.4/30[V] 1920
25     Aggregate   10.88.162.8/30[V] 137104
26     Untagged    172.31.1.0/24[V]  570        Et1/2      10.88.162.14
27     Aggregate   10.88.162.12/30[V]   \
                                     273480
30     Pop tag     88.1.11.5/32      0          Et1/0      88.1.3.2
31     Pop tag     88.1.88.0/24      0          Et1/0      88.1.3.2
32     16          88.1.97.0/24      0          Et1/0      88.1.3.2
33     Pop tag     88.1.99.0/24      0          Et1/0      88.1.3.2
gila#
```

```
gila# show tag-switching forwarding-table  88.1.88.0 detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
31     Pop tag     88.1.88.0/24      0          Et1/0      88.1.3.2
        MAC/Encaps=14/14, MRU=1504, Tag Stack{}
        005054D92A250090BF9C6C1C8847
        No output feature configured
    Per-packet load-sharing
gila#
```

下一頁顯示輸出PE NAT路由器（在iguana的E1/0/5介面）接收的回應數據。

```
From CustA:
DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 1 arrived at  16:21:34.8415; frame size is 118 (0076 hex)
            bytes.
        DLC:  Destination = Station 005054D92A25
        DLC:  Source      = Station 0090BF9C6C1C
        DLC:  Ethertype   = 8847 (MPLS)
```

```
       DLC:
  MPLS: ----- MPLS Label Stack  -----
       MPLS:
       MPLS: Label Value                   = 00018
       MPLS: Reserved For Experimental Use = 0
       MPLS: Stack Value                   = 1 (Bottom of Stack)
       MPLS: Time to Live                  = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
       IP:       .... .0.. = normal reliability
       IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
           bit
       IP:       .... ...0 = CE bit - no congestion
       IP: Total length    = 100 bytes
       IP: Identification  = 175
       IP: Flags           = 0X
       IP:       .0.. .... = may fragment
       IP:       ..0. .... = last fragment
       IP: Fragment offset = 0 bytes
       IP: Time to live    = 254 seconds/hops
       IP: Protocol        = 1 (ICMP)
       IP: Header checksum = 5EC0 (correct)
       IP: Source address      = [172.31.1.1]
       IP: Destination address = [88.1.88.8]
       IP: No options
       IP:
  ICMP: ----- ICMP header -----
       ICMP:
       ICMP: Type = 8 (Echo)
       ICMP: Code = 0
       ICMP: Checksum = 4AF1 (correct)
       ICMP: Identifier = 4713
       ICMP: Sequence number = 6957
       ICMP: [72 bytes of data]
       ICMP:
       ICMP: [Normal end of "ICMP header".]
```

From CustB:

```
DLC:  ----- DLC Header -----
       DLC:
       DLC:  Frame 11 arrived at  16:21:37.1558; frame size is 118 (0076 hex)
           bytes.
       DLC:  Destination = Station 005054D92A25
       DLC:  Source      = Station 0090BF9C6C1C
       DLC:  Ethertype   = 8847 (MPLS)
       DLC:
  MPLS: ----- MPLS Label Stack  -----
       MPLS:
       MPLS: Label Value                   = 0001C
       MPLS: Reserved For Experimental Use = 0
       MPLS: Stack Value                   = 1 (Bottom of Stack)
       MPLS: Time to Live                  = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
```

```
        IP: Version = 4, header length = 20 bytes
        IP: Type of service = 00
        IP:       000. ....   = routine
        IP:       ...0 .... = normal delay
        IP:       .... 0... = normal throughput
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
            bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 165
        IP: Flags           = 0X
        IP:       .0.. .... = may fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
        IP: Header checksum = 5ECA (correct)
        IP: Source address      = [172.31.1.1]
        IP: Destination address = [88.1.88.8]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 8 (Echo)
        ICMP: Code = 0
        ICMP: Checksum = AD5E (correct)
        ICMP: Identifier = 3365
        ICMP: Sequence number = 7935
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

這些ping會導致在出口PE路由器的iguana的NAT表中建立以下條目。為上面顯示的封包建立的特定專案可以透過其ICMP識別碼進行配對。

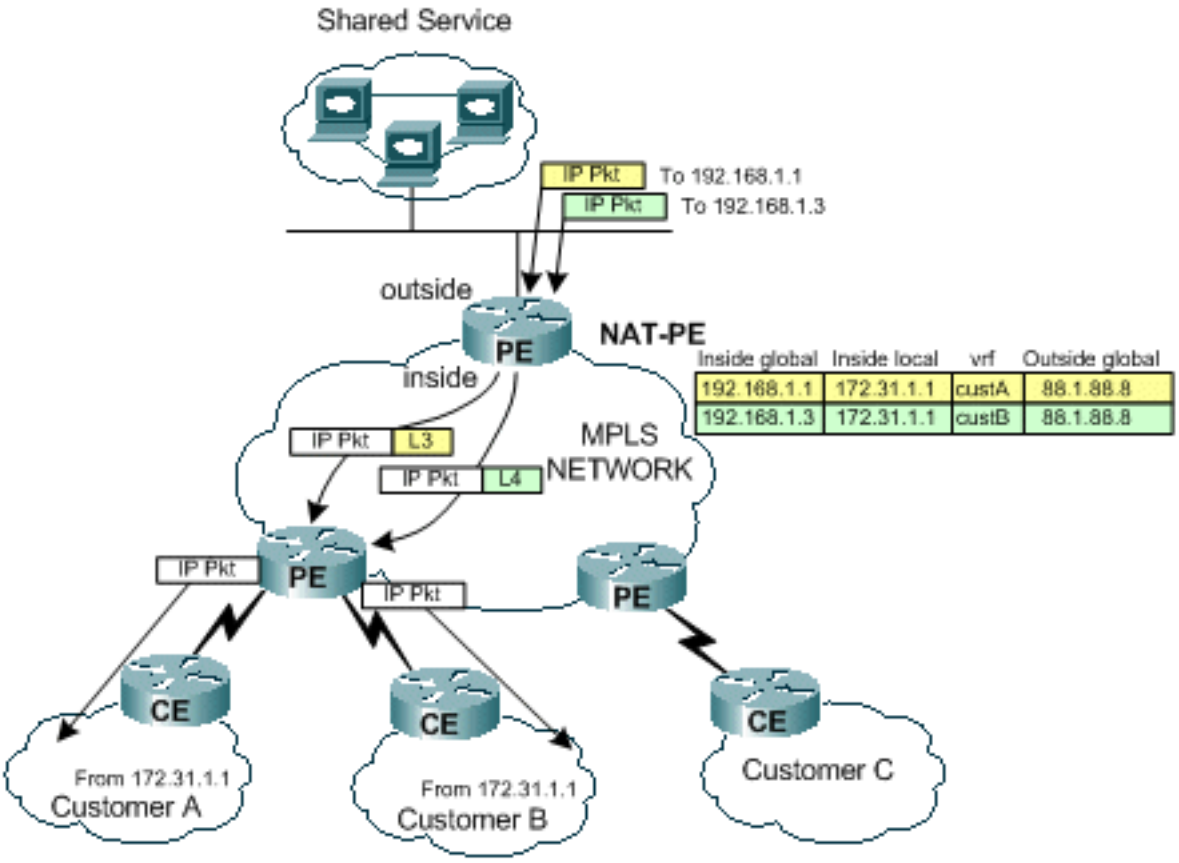
```
iguana#
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.3:3365  172.31.1.1:3365    88.1.88.8:3365     88.1.88.8:3365
icmp 192.168.1.3:3366  172.31.1.1:3366    88.1.88.8:3366     88.1.88.8:3366
icmp 192.168.1.3:3367  172.31.1.1:3367    88.1.88.8:3367     88.1.88.8:3367
icmp 192.168.1.3:3368  172.31.1.1:3368    88.1.88.8:3368     88.1.88.8:3368
icmp 192.168.1.3:3369  172.31.1.1:3369    88.1.88.8:3369     88.1.88.8:3369
icmp 192.168.1.1:4713  172.31.1.1:4713    88.1.88.8:4713     88.1.88.8:4713
icmp 192.168.1.1:4714  172.31.1.1:4714    88.1.88.8:4714     88.1.88.8:4714
icmp 192.168.1.1:4715  172.31.1.1:4715    88.1.88.8:4715     88.1.88.8:4715
icmp 192.168.1.1:4716  172.31.1.1:4716    88.1.88.8:4716     88.1.88.8:4716
icmp 192.168.1.1:4717  172.31.1.1:4717    88.1.88.8:4717     88.1.88.8:4717


iguana#
show ip nat translations verbose

Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.3:3365  172.31.1.1:3365    88.1.88.8:3365     88.1.88.8:3365
    create 00:00:34, use 00:00:34, left 00:00:25, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:3366  172.31.1.1:3366    88.1.88.8:3366     88.1.88.8:3366
    create 00:00:34, use 00:00:34, left 00:00:25, Map-Id(In): 2,
```

```
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:3367  172.31.1.1:3367    88.1.88.8:3367     88.1.88.8:3367
    create 00:00:34, use 00:00:34, left 00:00:25, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:3368  172.31.1.1:3368    88.1.88.8:3368     88.1.88.8:3368
    create 00:00:34, use 00:00:34, left 00:00:25, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:3369  172.31.1.1:3369    88.1.88.8:3369     88.1.88.8:3369
    create 00:00:34, use 00:00:34, left 00:00:25, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.1:4713  172.31.1.1:4713    88.1.88.8:4713     88.1.88.8:4713
    create 00:00:37, use 00:00:37, left 00:00:22, Map-Id(In): 1,
Pro Inside global      Inside local       Outside local      Outside global
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:4714  172.31.1.1:4714    88.1.88.8:4714     88.1.88.8:4714
    create 00:00:37, use 00:00:37, left 00:00:22, Map-Id(In): 1,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:4715  172.31.1.1:4715    88.1.88.8:4715     88.1.88.8:4715
    create 00:00:37, use 00:00:37, left 00:00:22, Map-Id(In): 1,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:4716  172.31.1.1:4716    88.1.88.8:4716     88.1.88.8:4716
    create 00:00:37, use 00:00:37, left 00:00:22, Map-Id(In): 1,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:4717  172.31.1.1:4717    88.1.88.8:4717     88.1.88.8:4717
    create 00:00:37, use 00:00:37, left 00:00:22, Map-Id(In): 1,
    flags:
extended, use_count: 0, VRF : custA
iguana#
```

從共用服務返回源VPN的資料包流

當資料包流回訪問共用服務主機的裝置時，在路由之前會檢查NAT表（資料包從NAT「outside」介面傳到「inside」介面）。 由於每個唯一條目包括相應的VRF識別符號，因此可以相應地轉換和路由資料包。

圖7:發回共用服務使用者的資料包



如圖7所示，NAT首先檢查返回流量以查詢匹配的轉換條目。例如，將資料包傳送到目標192.168.1.1。搜尋NAT表。找到匹配項時，將對「內部本地」地址(172.31.1.1)執行適當的轉換，然後使用來自NAT條目的相關VRF ID執行鄰接查詢。

```
iguana# show ip cef vrf custA 172.31.1.0
172.31.1.0/24, version 12, epoch 0, cached adjacency 88.1.3.1
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0/5, 88.1.3.1, tags imposed: {23}
  via 88.1.11.9, 0 dependencies, recursive
    next hop 88.1.3.1, Ethernet1/0/5 via 88.1.11.9/32
    valid cached adjacency
    tag rewrite with Et1/0/5, 88.1.3.1, tags imposed: {23}
```

```
iguana# show ip cef vrf custB 172.31.1.0
172.31.1.0/24, version 18, epoch 0, cached adjacency 88.1.3.1
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0/5, 88.1.3.1, tags imposed: {26}
  via 88.1.11.9, 0 dependencies, recursive
    next hop 88.1.3.1, Ethernet1/0/5 via 88.1.11.9/32
    valid cached adjacency
    tag rewrite with Et1/0/5, 88.1.3.1, tags imposed: {26}
iguana#
```

標籤23(0x17)用於在VRF custA中發往172.31.1.0/24的流量，標籤26(0x1A)用於在VRF custB中發往172.31.1.0/24的資料包。

從路由器Iguana傳送的回應回覆封包中會看到這種情況：

To custA:

```
  DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 2 arrived at  16:21:34.8436; frame size is 118 (0076 hex)
            bytes.
        DLC:  Destination = Station 0090BF9C6C1C
        DLC:  Source      = Station 005054D92A25
        DLC:  Ethertype   = 8847 (MPLS)
        DLC:
  MPLS: ----- MPLS Label Stack  -----
        MPLS:
        MPLS: Label Value                    = 00017
        MPLS: Reserved For Experimental Use = 0
        MPLS: Stack Value                    = 1 (Bottom of Stack)
        MPLS: Time to Live                   = 254 (hops)
        MPLS:
  IP: ----- IP Header -----
        IP:
        IP: Version = 4, header length = 20 bytes
        IP: Type of service = 00
        IP:       000. ....   = routine
        IP:       ...0 .... = normal delay
        IP:       .... 0... = normal throughput
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
            bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 56893
        IP: Flags           = 4X
        IP:       .1.. .... = don't fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
        IP: Header checksum = 4131 (correct)
        IP: Source address      = [88.1.88.8]
        IP: Destination address = [172.31.1.1]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 0 (Echo reply)
        ICMP: Code = 0
        ICMP: Checksum = 52F1 (correct)
        ICMP: Identifier = 4713
        ICMP: Sequence number = 6957
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

當資料包到達目的PE路由器時，標籤用於確定傳送資料包的適當VRF和介面。

```
gila#
show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Pop tag     88.1.1.0/24       0          Et1/1      88.1.2.2
       Pop tag     88.1.1.0/24       0          Et1/0      88.1.3.2
```

```
17     Pop tag     88.1.4.0/24       0          Et1/1      88.1.2.2
18     Pop tag     88.1.10.0/24      0          Et1/1      88.1.2.2
19     Pop tag     88.1.11.1/32      0          Et1/1      88.1.2.2
20     Pop tag     88.1.5.0/24       0          Et1/0      88.1.3.2
21     19          88.1.11.10/32     0          Et1/1      88.1.2.2
       22          88.1.11.10/32     0          Et1/0      88.1.3.2
22     20          172.18.60.176/32  0          Et1/1      88.1.2.2
       23          172.18.60.176/32  0          Et1/0      88.1.3.2
23     Untagged    172.31.1.0/24[V]  6306       Fa0/0      10.88.162.6
24     Aggregate   10.88.162.4/30[V] 1920
25     Aggregate   10.88.162.8/30[V] 487120
26     Untagged    172.31.1.0/24[V]  1896       Et1/2      10.88.162.14
27     Aggregate   10.88.162.12/30[V]   \
                                     972200
30     Pop tag     88.1.11.5/32      0          Et1/0      88.1.3.2
31     Pop tag     88.1.88.0/24      0          Et1/0      88.1.3.2
32     16          88.1.97.0/24      0          Et1/0      88.1.3.2
33     Pop tag     88.1.99.0/24      0          Et1/0      88.1.3.2
gila#
```

組態

為了簡潔，已從配置中刪除了一些無關的資訊。

```
IGUANA:
!
ip vrf custA
 rd 65002:100
 route-target export 65002:100
 route-target import 65002:100
!
ip vrf custB
 rd 65002:200
 route-target export 65002:200
 route-target import 65002:200
!
ip cef
mpls label protocol ldp
tag-switching tdp router-id Loopback0
!
interface Loopback0
 ip address 88.1.11.5 255.255.255.255
 no ip route-cache
 no ip mroute-cache
!
interface Loopback11
 ip vrf forwarding custA
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet1/0/0
 ip vrf forwarding custB
 ip address 10.88.163.5 255.255.255.252
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0/4
 ip address 88.1.1.1 255.255.255.0
 ip nat inside
 no ip mroute-cache
 tag-switching ip
!
```

```
interface Ethernet1/0/5
 ip address 88.1.3.2 255.255.255.0
 ip nat inside
 no ip mroute-cache
 tag-switching ip
!
!
interface FastEthernet1/1/0
 ip address 88.1.88.1 255.255.255.0
 ip nat outside
 full-duplex
!
interface FastEthernet5/0/0
 ip address 88.1.99.1 255.255.255.0
 speed 100
 full-duplex
!
router ospf 881
 log-adjacency-changes
 redistribute static subnets
 network 88.1.0.0 0.0.255.255 area 0
!
router bgp 65002
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 88.1.11.1 remote-as 65002
 neighbor 88.1.11.1 update-source Loopback0
 neighbor 88.1.11.9 remote-as 65002
 neighbor 88.1.11.9 update-source Loopback0
 neighbor 88.1.11.10 remote-as 65002
 neighbor 88.1.11.10 update-source Loopback0
 no auto-summary
 !
 address-family ipv4 multicast
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.1 send-community extended
 neighbor 88.1.11.9 activate
 neighbor 88.1.11.9 send-community extended
 no auto-summary
 exit-address-family
 !
 address-family ipv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.9 activate
 neighbor 88.1.11.10 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf custB
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf custA
 redistribute static
```

```
 no auto-summary
 no synchronization
 exit-address-family
!
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
ip nat inside source list 181 pool SSPOOL1 vrf custB overload
ip classless
ip route 88.1.88.0 255.255.255.0 FastEthernet1/1/0
ip route 88.1.97.0 255.255.255.0 FastEthernet5/0/0 88.1.99.2
ip route 88.1.99.0 255.255.255.0 FastEthernet5/0/0 88.1.99.2
ip route 192.168.1.0 255.255.255.0 Null0
ip route vrf custA 88.1.88.8 255.255.255.255 FastEthernet1/1/0 88.1.88.8 global
ip route vrf custB 10.88.208.0 255.255.240.0 10.88.163.6
ip route vrf custB 64.102.0.0 255.255.0.0 10.88.163.6
ip route vrf custB 88.1.88.8 255.255.255.255 FastEthernet1/1/0 88.1.88.8 global
ip route vrf custB 128.0.0.0 255.0.0.0 10.88.163.6
no ip http server
!
access-list 181 permit ip any host 88.1.88.8
!
```

GILA:

```
!
ip vrf custA
 rd 65002:100
 route-target export 65002:100
 route-target import 65002:100
!
ip vrf custB
 rd 65002:200
 route-target export 65002:200
 route-target import 65002:200
!
ip cef
mpls label protocol ldp
tag-switching tdp router-id Loopback0
!
interface Loopback0
 ip address 88.1.11.9 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding custA
 ip address 10.88.162.5 255.255.255.252
 duplex full
!
interface Ethernet1/0
 ip address 88.1.3.1 255.255.255.0
 no ip mroute-cache
 duplex half
 tag-switching ip
!
interface Ethernet1/1
 ip address 88.1.2.1 255.255.255.0
 no ip mroute-cache
 duplex half
 tag-switching ip
!
interface Ethernet1/2
 ip vrf forwarding custB
 ip address 10.88.162.13 255.255.255.252
```

```
 ip ospf cost 100
 duplex half
!
interface FastEthernet2/0
 ip vrf forwarding custA
 ip address 10.88.162.9 255.255.255.252
 duplex full
!
router ospf 881
 log-adjacency-changes
 redistribute static subnets
 network 88.1.0.0 0.0.255.255 area 0
 default-metric 30
!
router bgp 65002
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 88.1.11.1 remote-as 65002
 neighbor 88.1.11.1 update-source Loopback0
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.5 remote-as 65002
 neighbor 88.1.11.5 update-source Loopback0
 neighbor 88.1.11.5 activate
 no auto-summary
 !
 address-family ipv4 vrf custB
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf custA
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.1 send-community extended
 neighbor 88.1.11.5 activate
 neighbor 88.1.11.5 send-community extended
 no auto-summary
 exit-address-family
!
ip classless
ip route vrf custA 172.31.1.0 255.255.255.0 FastEthernet0/0 10.88.162.6
ip route vrf custB 172.31.1.0 255.255.255.0 Ethernet1/2 10.88.162.14
!
```

路由器dragon的配置與gila非常相似。

不允許匯入/匯出路由目標

當共用服務網路自身配置為VRF例項時，輸出PE上的中央NAT是不可能的。這是因為傳入資料包無法區分，並且只有一條返回始發子網的路由存在於輸出PE NAT中。

註：以下顯示用於說明無效配置的結果。

配置示例網路後，共用服務網路被定義為VRF例項（VRF名稱= sserver）。 現在，輸入PE上的CEF表顯示如下：

```
gila# show ip cef vrf custA 88.1.88.0
88.1.88.0/24, version 45, epoch 0, cached adjacency 88.1.3.2
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
  via 88.1.11.5, 0 dependencies, recursive
    next hop 88.1.3.2, Ethernet1/0 via 88.1.11.5/32
    valid cached adjacency
    tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
gila#
```

```
gila# show ip cef vrf custB 88.1.88.0
88.1.88.0/24, version 71, epoch 0, cached adjacency 88.1.3.2
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
  via 88.1.11.5, 0 dependencies, recursive
    next hop 88.1.3.2, Ethernet1/0 via 88.1.11.5/32
    valid cached adjacency
    tag rewrite with Et1/0, 88.1.3.2, tags imposed: {24}
gila#
```

```
iguana#
show tag-switching forwarding vrftags 24
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
24     Aggregate   88.1.88.0/24[V]   10988
iguana#
```

註：請注意標籤值*24是如*何為VRF custA和VRF custB強加的。

此顯示顯示了共用服務VRF例項「伺服器」的路由表：

```
iguana#
show ip route vrf sserver 172.31.1.1
Routing entry for 172.31.1.0/24
  Known via "bgp 65002", distance 200, metric 0, type internal
  Last update from 88.1.11.9 1d01h ago
  Routing Descriptor Blocks:
  * 88.1.11.9 (Default-IP-Routing-Table), from 88.1.11.9, 1d01h ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
```

註：從輸出PE路由器(Iguana)的角度來看，目的網路只存在一條路由。

因此，無法區分來自多個客戶VPN的流量，並且返回流量無法到達適當的VPN。**在必須將共用服務定義為VRF例項的情況下，必須將NAT函式移至輸入PE。**

輸入PE NAT

在本示例中，標有**gila**和**dragon**的提供商邊緣路由器配置了NAT。為需要訪問共用服務的每個連線的客戶VPN定義NAT池。每個經過NAT的客戶網路地址都使用相應的池。NAT僅對發往地址為88.1.88.8的共用服務主機的資料包執行。

```
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat pool SSPOOL2 192.168.2.1 192.168.2.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
ip nat inside source list 181 pool SSPOOL2 vrf custB overload
```

注意：在此方案中，不支援共用池。如果共用服務LAN（在出口PE）通過通用介面連線，則可以共用NAT池。

來自連線到**neuse**和**capefear8**的每個網路內的重複地址(172.31.1.1)的ping會導致以下NAT條目：

在**Gila**上：

```
gila#
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.1:2139  172.31.1.1:2139    88.1.88.8:2139     88.1.88.8:2139
icmp 192.168.1.1:2140  172.31.1.1:2140    88.1.88.8:2140     88.1.88.8:2140
icmp 192.168.1.1:2141  172.31.1.1:2141    88.1.88.8:2141     88.1.88.8:2141
icmp 192.168.1.1:2142  172.31.1.1:2142    88.1.88.8:2142     88.1.88.8:2142
icmp 192.168.1.1:2143  172.31.1.1:2143    88.1.88.8:2143     88.1.88.8:2143
icmp 192.168.2.2:676   172.31.1.1:676     88.1.88.8:676      88.1.88.8:676
icmp 192.168.2.2:677   172.31.1.1:677     88.1.88.8:677      88.1.88.8:677
icmp 192.168.2.2:678   172.31.1.1:678     88.1.88.8:678      88.1.88.8:678
icmp 192.168.2.2:679   172.31.1.1:679     88.1.88.8:679      88.1.88.8:679
icmp 192.168.2.2:680   172.31.1.1:680     88.1.88.8:680      88.1.88.8:680
```

注意：相同的內部本地地址(172.31.1.1)會根據源VRF轉換為每個定義的池。在**show ip nat translation verbose**命令中可以看到VRF:

```
gila# show ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.1:2139  172.31.1.1:2139    88.1.88.8:2139     88.1.88.8:2139
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:2140  172.31.1.1:2140    88.1.88.8:2140     88.1.88.8:2140
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:2141  172.31.1.1:2141    88.1.88.8:2141     88.1.88.8:2141
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:2142  172.31.1.1:2142    88.1.88.8:2142     88.1.88.8:2142
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:2143  172.31.1.1:2143    88.1.88.8:2143     88.1.88.8:2143
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.2.2:676   172.31.1.1:676     88.1.88.8:676      88.1.88.8:676
```

```
    create 00:00:10, use 00:00:10, left 00:00:49, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.2.2:677   172.31.1.1:677     88.1.88.8:677      88.1.88.8:677
    create 00:00:10, use 00:00:10, left 00:00:49, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.2.2:678   172.31.1.1:678     88.1.88.8:678      88.1.88.8:678
    create 00:00:10, use 00:00:10, left 00:00:49, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.2.2:679   172.31.1.1:679     88.1.88.8:679      88.1.88.8:679
    create 00:00:10, use 00:00:10, left 00:00:49, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.2.2:680   172.31.1.1:680     88.1.88.8:680      88.1.88.8:680
    create 00:00:10, use 00:00:10, left 00:00:49, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
```

這些顯示顯示了客戶A和客戶B的每個本地連線VPN的路由資訊：

```
gila# show ip route vrf custA
Codes: C - connected, S - static, 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
       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 88.1.11.1 to network 0.0.0.0

     172.18.0.0/32 is subnetted, 2 subnets
B       172.18.60.179 [200/0] via 88.1.11.1, 00:03:59
B       172.18.60.176 [200/0] via 88.1.11.1, 00:03:59
     172.31.0.0/24 is subnetted, 1 subnets
S       172.31.1.0 [1/0] via 10.88.162.6, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
B       10.88.0.0/20 [200/0] via 88.1.11.1, 00:03:59
B       10.88.32.0/20 [200/0] via 88.1.11.1, 00:03:59
C       10.88.162.4/30 is directly connected, FastEthernet0/0
C       10.88.162.8/30 is directly connected, FastEthernet2/0
B       10.88.161.8/30 [200/0] via 88.1.11.1, 00:04:00
     88.0.0.0/24 is subnetted, 2 subnets
B       88.1.88.0 [200/0] via 88.1.11.5, 00:04:00
B       88.1.99.0 [200/0] via 88.1.11.5, 00:04:00
S    192.168.1.0/24 is directly connected, Null0
B*   0.0.0.0/0 [200/0] via 88.1.11.1, 00:04:00


gila# show ip route vrf custB
Codes: C - connected, S - static, 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
       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 not set

     64.0.0.0/16 is subnetted, 1 subnets
B       64.102.0.0 [200/0] via 88.1.11.5, 1d21h
     172.18.0.0/32 is subnetted, 2 subnets
B       172.18.60.179 [200/0] via 88.1.11.1, 1d21h
B       172.18.60.176 [200/0] via 88.1.11.1, 1d21h
     172.31.0.0/24 is subnetted, 1 subnets
S       172.31.1.0 [1/0] via 10.88.162.14, Ethernet1/2
     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
B       10.88.194.16/28 [200/100] via 88.1.11.1, 1d20h
B       10.88.208.0/20 [200/0] via 88.1.11.5, 1d21h
B       10.88.194.4/30 [200/100] via 88.1.11.1, 1d20h
B       10.88.163.4/30 [200/0] via 88.1.11.5, 1d21h
B       10.88.161.4/30 [200/0] via 88.1.11.1, 1d21h
C       10.88.162.12/30 is directly connected, Ethernet1/2
     11.0.0.0/24 is subnetted, 1 subnets
B       11.1.1.0 [200/100] via 88.1.11.1, 1d20h
     88.0.0.0/24 is subnetted, 2 subnets
B       88.1.88.0 [200/0] via 88.1.11.5, 1d21h
B       88.1.99.0 [200/0] via 88.1.11.5, 1d21h
S    192.168.2.0/24 is directly connected, Null0
B    128.0.0.0/8 [200/0] via 88.1.11.5, 1d21h
```

注意：已從靜態配置中新增了每個NAT池的路由。這些子網隨後會匯入到出口PE路由器iguana的共用伺服器VRF中：

```
iguana# show ip route vrf sserver


Routing Table: sserver
Codes: C - connected, S - static, 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
       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 not set

     64.0.0.0/16 is subnetted, 1 subnets
B       64.102.0.0 [20/0] via 10.88.163.6 (custB), 1d20h
     172.18.0.0/32 is subnetted, 2 subnets
B       172.18.60.179 [200/0] via 88.1.11.1, 1d20h
B       172.18.60.176 [200/0] via 88.1.11.1, 1d20h
     172.31.0.0/24 is subnetted, 1 subnets
B       172.31.1.0 [200/0] via 88.1.11.9, 1d05h
     10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
B       10.88.194.16/28 [200/100] via 88.1.11.1, 1d20h
B       10.88.208.0/20 [20/0] via 10.88.163.6 (custB), 1d20h
B       10.88.194.4/30 [200/100] via 88.1.11.1, 1d20h
B       10.88.162.4/30 [200/0] via 88.1.11.9, 1d20h
B       10.88.163.4/30 is directly connected, 1d20h, Ethernet1/0/0
B       10.88.161.4/30 [200/0] via 88.1.11.1, 1d20h
B       10.88.162.8/30 [200/0] via 88.1.11.9, 1d20h
B       10.88.162.12/30 [200/0] via 88.1.11.9, 1d20h
```

```
     11.0.0.0/24 is subnetted, 1 subnets
B       11.1.1.0 [200/100] via 88.1.11.1, 1d20h
     12.0.0.0/24 is subnetted, 1 subnets
S       12.12.12.0 [1/0] via 88.1.99.10
     88.0.0.0/24 is subnetted, 3 subnets
C       88.1.88.0 is directly connected, FastEthernet1/1/0
S       88.1.97.0 [1/0] via 88.1.99.10
C       88.1.99.0 is directly connected, FastEthernet5/0/0
B    192.168.1.0/24 [200/0] via 88.1.11.9, 1d20h
B    192.168.2.0/24 [200/0] via 88.1.11.9, 01:59:23
B    128.0.0.0/8 [20/0] via 10.88.163.6 (custB), 1d20h
```

組態

為了簡潔，已從配置中刪除了一些無關的資訊。

```
GILA:
ip vrf custA
 rd 65002:100
 route-target export 65002:100
 route-target export 65002:1001
 route-target import 65002:100
!
ip vrf custB
 rd 65002:200
 route-target export 65002:200
 route-target export 65002:2001
 route-target import 65002:200
 route-target import 65002:10
!
ip cef
mpls label protocol ldp
!

interface Loopback0
 ip address 88.1.11.9 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding custA
 ip address 10.88.162.5 255.255.255.252
 ip nat inside
 duplex full
!
interface Ethernet1/0
 ip address 88.1.3.1 255.255.255.0
 ip nat outside
 no ip mroute-cache
 duplex half
 tag-switching ip
!
interface Ethernet1/1
 ip address 88.1.2.1 255.255.255.0
 ip nat outside
 no ip mroute-cache
 duplex half
 tag-switching ip
!
interface Ethernet1/2
 ip vrf forwarding custB
 ip address 10.88.162.13 255.255.255.252
 ip nat inside
 duplex half
```

```
!
router ospf 881
 log-adjacency-changes
 redistribute static subnets
 network 88.1.0.0 0.0.255.255 area 0
 default-metric 30
!
router bgp 65002
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 88.1.11.1 remote-as 65002
 neighbor 88.1.11.1 update-source Loopback0
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.5 remote-as 65002
 neighbor 88.1.11.5 update-source Loopback0
 neighbor 88.1.11.5 activate
 no auto-summary
 !
 address-family ipv4 vrf custB
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf custA
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.1 send-community extended
 neighbor 88.1.11.5 activate
 neighbor 88.1.11.5 send-community extended
 no auto-summary
 exit-address-family
!
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat pool SSPOOL2 192.168.2.1 192.168.2.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
ip nat inside source list 181 pool SSPOOL2 vrf custB overload
ip classless
ip route vrf custA 172.31.1.0 255.255.255.0 FastEthernet0/0 10.88.162.6
ip route vrf custA 192.168.1.0 255.255.255.0 Null0
ip route vrf custB 172.31.1.0 255.255.255.0 Ethernet1/2 10.88.162.14
ip route vrf custB 192.168.2.0 255.255.255.0 Null0
!
access-list 181 permit ip any host 88.1.88.8
!
```

注意：面向客戶網路的介面被指定為NAT「內部」介面，而MPLS介面被指定為NAT「外部」介面。

```
iguana:
ip vrf custB
 rd 65002:200
 route-target export 65002:200
 route-target export 65002:2001
 route-target import 65002:200
```

```
 route-target import 65002:10
!
ip vrf sserver
 rd 65002:10
 route-target export 65002:10
 route-target import 65002:2001
 route-target import 65002:1001
!
ip cef distributed
mpls label protocol ldp
!

interface Loopback0
 ip address 88.1.11.5 255.255.255.255
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0/0
 ip vrf forwarding custB
 ip address 10.88.163.5 255.255.255.252
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0/4
 ip address 88.1.1.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 tag-switching ip
!
interface Ethernet1/0/5
 ip address 88.1.3.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 tag-switching ip
!
interface FastEthernet1/1/0
 ip vrf forwarding sserver
 ip address 88.1.88.1 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 full-duplex
!
router ospf 881
 log-adjacency-changes
 redistribute static subnets
 network 88.1.0.0 0.0.255.255 area 0
!
router bgp 65002
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 88.1.11.1 remote-as 65002
 neighbor 88.1.11.1 update-source Loopback0
 neighbor 88.1.11.9 remote-as 65002
 neighbor 88.1.11.9 update-source Loopback0
 neighbor 88.1.11.10 remote-as 65002
 neighbor 88.1.11.10 update-source Loopback0
 no auto-summary
 !
 address-family ipv4 multicast
 no auto-summary
 no synchronization
 exit-address-family
```

```
 !
 address-family vpnv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.1 send-community extended
 neighbor 88.1.11.9 activate
 neighbor 88.1.11.9 send-community extended
 no auto-summary
 exit-address-family
 !
 address-family ipv4
 neighbor 88.1.11.1 activate
 neighbor 88.1.11.9 activate
 neighbor 88.1.11.10 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf sserver
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf custB
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
```

路由器dragon的配置與gila非常相似。

輸入PE NAT後到達中央PE的資料包

以下跟蹤說明將目標共用服務網路配置為VRF例項時，對唯一NAT池的要求。再次參閱圖5中的圖表。以下顯示的資料包是在進入路由器Iguana的MPLS IP介面e1/0/5時被**捕獲的**。

來自客戶A VPN的回應

在這裡，我們看到來自VRF custA中的源IP地址172.31.1.1的回應請求。源地址已轉換為NAT配置所指定的192.168.1.1:

```
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
```

```
DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 1 arrived at  09:15:29.8157; frame size is 118 (0076 hex)
            bytes.
        DLC:  Destination = Station 005054D92A25
        DLC:  Source      = Station 0090BF9C6C1C
        DLC:  Ethertype   = 8847 (MPLS)
        DLC:
  MPLS: ----- MPLS Label Stack  -----
        MPLS:
        MPLS: Label Value                   = 00019
        MPLS: Reserved For Experimental Use = 0
```

```
       MPLS: Stack Value                  = 1 (Bottom of Stack)
       MPLS: Time to Live                 = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
       IP:       .... .0.. = normal reliability
       IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
           bit
       IP:       .... ...0 = CE bit - no congestion
       IP: Total length    = 100 bytes
       IP: Identification  = 0
       IP: Flags           = 0X
       IP:       .0.. .... = may fragment
       IP:       ..0. .... = last fragment
       IP: Fragment offset = 0 bytes
       IP: Time to live    = 254 seconds/hops
       IP: Protocol        = 1 (ICMP)
       IP: Header checksum = 4AE6 (correct)
       IP: Source address      = [192.168.1.1]
       IP: Destination address = [88.1.88.8]
       IP: No options
       IP:
  ICMP: ----- ICMP header -----
       ICMP:
       ICMP: Type = 8 (Echo)
       ICMP: Code = 0
       ICMP: Checksum = 932D (correct)
       ICMP: Identifier = 3046
       ICMP: Sequence number = 3245
       ICMP: [72 bytes of data]
       ICMP:
       ICMP: [Normal end of "ICMP header".]
       ICMP:
```

來自客戶B VPN的回應

此處我們看到來自VRF custB中的源IP地址172.31.1.1的回應請求。源地址已轉換為NAT配置所指定的192.168.2.1:

```
ip nat pool SSPOOL2 192.168.2.1 192.168.2.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL2 vrf custB overload
```

```
DLC:  ----- DLC Header -----
       DLC:
       DLC:  Frame 11 arrived at  09:15:49.6623; frame size is 118 (0076 hex)
           bytes.
       DLC:  Destination = Station 005054D92A25
       DLC:  Source      = Station 0090BF9C6C1C
       DLC:  Ethertype   = 8847 (MPLS)
       DLC:
  MPLS: ----- MPLS Label Stack  -----
       MPLS:
       MPLS: Label Value                  = 00019
       MPLS: Reserved For Experimental Use = 0
```

```
       MPLS: Stack Value                  = 1 (Bottom of Stack)
       MPLS: Time to Live                 = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
       IP:       .... .0.. = normal reliability
       IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
           bit
       IP:       .... ...0 = CE bit - no congestion
       IP: Total length    = 100 bytes
       IP: Identification  = 15
       IP: Flags           = 0X
       IP:       .0.. .... = may fragment
       IP:       ..0. .... = last fragment
       IP: Fragment offset = 0 bytes
       IP: Time to live    = 254 seconds/hops
       IP: Protocol        = 1 (ICMP)
       IP: Header checksum = 49D6 (correct)
       IP: Source address      = [192.168.2.2]
       IP: Destination address = [88.1.88.8]
       IP: No options
       IP:
  ICMP: ----- ICMP header -----
       ICMP:
       ICMP: Type = 8 (Echo)
       ICMP: Code = 0
       ICMP: Checksum = AB9A (correct)
       ICMP: Identifier = 4173
       ICMP: Sequence number = 4212
       ICMP: [72 bytes of data]
       ICMP:
       ICMP: [Normal end of "ICMP header".]
```

注意：上述兩個資料包中*的*MPLS標籤值為0019。

回應回覆客戶A VPN

接下來，我們看到一條回應要求返回VRF custA中的目標IP地址192.168.1.1。目標地址通過輸入PE NAT功能轉換為172.31.1.1。

```
To VRF custA:
  DLC:  ----- DLC Header -----
       DLC:
       DLC:  Frame 2 arrived at  09:15:29.8198; frame size is 118 (0076 hex)
           bytes.
       DLC:  Destination = Station 0090BF9C6C1C
       DLC:  Source      = Station 005054D92A25
       DLC:  Ethertype   = 8847 (MPLS)
       DLC:
  MPLS: ----- MPLS Label Stack  -----
       MPLS:
       MPLS: Label Value                  = 0001A
       MPLS: Reserved For Experimental Use = 0
       MPLS: Stack Value                  = 1 (Bottom of Stack)
```

```
       MPLS: Time to Live                 = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
       IP:       .... .0.. = normal reliability
       IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
           bit
       IP:       .... ...0 = CE bit - no congestion
       IP: Total length    = 100 bytes
       IP: Identification  = 18075
       IP: Flags           = 4X
       IP:       .1.. .... = don't fragment
       IP:       ..0. .... = last fragment
       IP: Fragment offset = 0 bytes
       IP: Time to live    = 254 seconds/hops
       IP: Protocol        = 1 (ICMP)
       IP: Header checksum = C44A (correct)
       IP: Source address      = [88.1.88.8]
       IP: Destination address = [192.168.1.1]
       IP: No options
       IP:
  ICMP: ----- ICMP header -----
       ICMP:
       ICMP: Type = 0 (Echo reply)
       ICMP: Code = 0
       ICMP: Checksum = 9B2D (correct)
       ICMP: Identifier = 3046
       ICMP: Sequence number = 3245
       ICMP: [72 bytes of data]
       ICMP:
       ICMP: [Normal end of "ICMP header".]
       ICMP:
```

回應回覆客戶B VPN

此處我們看到回應要求回VRF custB中的目的地IP位址192.168.1.1。目標地址通過輸入PE NAT功能轉換為172.31.1.1。

```
To VRF custB:
DLC:  ----- DLC Header -----
       DLC:
       DLC:  Frame 12 arrived at  09:15:49.6635; frame size is 118 (0076 hex) bytes.
       DLC:  Destination = Station 0090BF9C6C1C
       DLC:  Source      = Station 005054D92A25
       DLC:  Ethertype   = 8847 (MPLS)
       DLC:
  MPLS: ----- MPLS Label Stack  -----
       MPLS:
       MPLS: Label Value                  = 0001D
       MPLS: Reserved For Experimental Use = 0
       MPLS: Stack Value                  = 1 (Bottom of Stack)
       MPLS: Time to Live                 = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
```

```
        IP:
        IP: Version = 4, header length = 20 bytes
        IP: Type of service = 00
        IP:       000. ....   = routine
        IP:       ...0 .... = normal delay
        IP:       .... 0... = normal throughput
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 37925
        IP: Flags           = 4X
        IP:       .1.. .... = don't fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
        IP: Header checksum = 75BF (correct)
        IP: Source address      = [88.1.88.8]
        IP: Destination address = [192.168.2.2]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 0 (Echo reply)
        ICMP: Code = 0
        ICMP: Checksum = B39A (correct)
        ICMP: Identifier = 4173
        ICMP: Sequence number = 4212
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

注意：在返回的資料包中，MPLS標籤值包含並不同：*001A*用於VRF custA，*001D*用於VRF custB。

客戶回應A VPN — 目的地是通用介面

當通往共用服務LAN的介面是通用介面而非VRF例項的一部分時，此下一組資料包顯示差異。在這裡，配置已更改為對具有重疊IP地址的兩個本地VPN使用公共池。

```
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
ip nat inside source list 181 pool SSPOOL1 vrf custB overload
```

```
DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 1 arrived at  09:39:19.6580; frame size is 118 (0076 hex)
            bytes.
        DLC:  Destination = Station 005054D92A25
        DLC:  Source      = Station 0090BF9C6C1C
        DLC:  Ethertype   = 8847 (MPLS)
        DLC:
  MPLS: ----- MPLS Label Stack  -----
        MPLS:
        MPLS: Label Value                   = 00019
        MPLS: Reserved For Experimental Use = 0
        MPLS: Stack Value                   = 1 (Bottom of Stack)
```

```
        MPLS: Time to Live                 = 254 (hops)
        MPLS:
  IP: ----- IP Header -----
        IP:
        IP: Version = 4, header length = 20 bytes
        IP: Type of service = 00
        IP:       000. ....   = routine
        IP:       ...0 .... = normal delay
        IP:       .... 0... = normal throughput
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
            bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 55
        IP: Flags           = 0X
        IP:       .0.. .... = may fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
        IP: Header checksum = 4AAF (correct)
        IP: Source address      = [192.168.1.1]
        IP: Destination address = [88.1.88.8]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 8 (Echo)
        ICMP: Code = 0
        ICMP: Checksum = 0905 (correct)
        ICMP: Identifier = 874
        ICMP: Sequence number = 3727
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

來自客戶B VPN的回應 — 目的地是通用介面

此處我們看到來自VRF custB中的源IP地址172.31.1.1的回應請求。源地址已轉換為192.168.1.3（來自公共池SSPOOL1），如NAT配置所指定：

```
ip nat pool SSPOOL1 192.168.1.1 192.168.1.254 prefix-length 24
ip nat inside source list 181 pool SSPOOL1 vrf custA overload
ip nat inside source list 181 pool SSPOOL1 vrf custB overload
```

```
DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 11 arrived at  09:39:26.4971; frame size is 118 (0076 hex)
            bytes.
        DLC:  Destination = Station 005054D92A25
        DLC:  Source      = Station 0090BF9C6C1C
        DLC:  Ethertype   = 8847 (MPLS)
        DLC:
  MPLS: ----- MPLS Label Stack  -----
        MPLS:
        MPLS: Label Value                  = 0001F
        MPLS: Reserved For Experimental Use = 0
        MPLS: Stack Value                  = 1 (Bottom of Stack)
```

```
       MPLS: Time to Live                 = 254 (hops)
       MPLS:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
       IP:       .... .0.. = normal reliability
       IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
           bit
       IP:       .... ...0 = CE bit - no congestion
       IP: Total length    = 100 bytes
       IP: Identification  = 75
       IP: Flags           = 0X
       IP:       .0.. .... = may fragment
       IP:       ..0. .... = last fragment
       IP: Fragment offset = 0 bytes
       IP: Time to live    = 254 seconds/hops
       IP: Protocol        = 1 (ICMP)
       IP: Header checksum = 4A99 (correct)
       IP: Source address      = [192.168.1.3]
       IP: Destination address = [88.1.88.8]
       IP: No options
       IP:
  ICMP: ----- ICMP header -----
       ICMP:
       ICMP: Type = 8 (Echo)
       ICMP: Code = 0
       ICMP: Checksum = 5783 (correct)
       ICMP: Identifier = 4237
       ICMP: Sequence number = 977
       ICMP: [72 bytes of data]
       ICMP:
       ICMP: [Normal end of "ICMP header".]
```

注意：當出口PE的介面是通用介面（不是VRF例項）時，所施加的標籤不同。在本例中，*0x19*和*0x1F*。

回應回覆客戶A VPN — 目的地是通用介面

接下來，我們看到一條回應要求返回VRF custA中的目標IP地址192.168.1.1。目標地址通過輸入PE NAT功能轉換為172.31.1.1。

```
DLC:  ----- DLC Header -----
       DLC:
       DLC:  Frame 2 arrived at  09:39:19.6621; frame size is 114 (0072 hex)
           bytes.
       DLC:  Destination = Station 0090BF9C6C1C
       DLC:  Source      = Station 005054D92A25
       DLC:  Ethertype   = 0800 (IP)
       DLC:
  IP: ----- IP Header -----
       IP:
       IP: Version = 4, header length = 20 bytes
       IP: Type of service = 00
       IP:       000. ....   = routine
       IP:       ...0 .... = normal delay
       IP:       .... 0... = normal throughput
```

```
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
            bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 54387
        IP: Flags           = 4X
        IP:       .1.. .... = don't fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
        IP: Header checksum = 3672 (correct)
        IP: Source address      = [88.1.88.8]
        IP: Destination address = [192.168.1.1]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 0 (Echo reply)
        ICMP: Code = 0
        ICMP: Checksum = 1105 (correct)
        ICMP: Identifier = 874
        ICMP: Sequence number = 3727
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

回應回覆客戶B VPN — 目的地是通用介面

此處我們看到回應要求回VRF custB中的目的地IP位址192.168.1.3。目標地址通過輸入PE NAT功能轉換為172.31.1.1。

```
DLC:  ----- DLC Header -----
        DLC:
        DLC:  Frame 12 arrived at  09:39:26.4978; frame size is 114 (0072 hex)
            bytes.
        DLC:  Destination = Station 0090BF9C6C1C
        DLC:  Source      = Station 005054D92A25
        DLC:  Ethertype   = 0800 (IP)
        DLC:
  IP: ----- IP Header -----
        IP:
        IP: Version = 4, header length = 20 bytes
        IP: Type of service = 00
        IP:       000. ....   = routine
        IP:       ...0 .... = normal delay
        IP:       .... 0... = normal throughput
        IP:       .... .0.. = normal reliability
        IP:       .... ..0. = ECT bit - transport protocol will ignore the CE
            bit
        IP:       .... ...0 = CE bit - no congestion
        IP: Total length    = 100 bytes
        IP: Identification  = 61227
        IP: Flags           = 4X
        IP:       .1.. .... = don't fragment
        IP:       ..0. .... = last fragment
        IP: Fragment offset = 0 bytes
        IP: Time to live    = 254 seconds/hops
        IP: Protocol        = 1 (ICMP)
```

```
        IP: Header checksum = 1BB8 (correct)
        IP: Source address      = [88.1.88.8]
        IP: Destination address = [192.168.1.3]
        IP: No options
        IP:
  ICMP: ----- ICMP header -----
        ICMP:
        ICMP: Type = 0 (Echo reply)
        ICMP: Code = 0
        ICMP: Checksum = 5F83 (correct)
        ICMP: Identifier = 4237
        ICMP: Sequence number = 977
        ICMP: [72 bytes of data]
        ICMP:
        ICMP: [Normal end of "ICMP header".]
```

注意：由於回覆的目的地是全域性地址，因此不會強加任何VRF標籤。

將共用服務LAN網段的送出介面定義為通用介面，允許使用通用池。Ping會導致路由器gla中出現以下NAT條目：

```
gila# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.3:4237  172.31.1.1:4237    88.1.88.8:4237     88.1.88.8:4237
icmp 192.168.1.3:4238  172.31.1.1:4238    88.1.88.8:4238     88.1.88.8:4238
icmp 192.168.1.3:4239  172.31.1.1:4239    88.1.88.8:4239     88.1.88.8:4239
icmp 192.168.1.3:4240  172.31.1.1:4240    88.1.88.8:4240     88.1.88.8:4240
icmp 192.168.1.3:4241  172.31.1.1:4241    88.1.88.8:4241     88.1.88.8:4241
icmp 192.168.1.1:874   172.31.1.1:874     88.1.88.8:874      88.1.88.8:874
icmp 192.168.1.1:875   172.31.1.1:875     88.1.88.8:875      88.1.88.8:875
icmp 192.168.1.1:876   172.31.1.1:876     88.1.88.8:876      88.1.88.8:876
icmp 192.168.1.1:877   172.31.1.1:877     88.1.88.8:877      88.1.88.8:877
icmp 192.168.1.1:878   172.31.1.1:878     88.1.88.8:878      88.1.88.8:878
gila#

gila# show ip nat tr ver
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.3:4237  172.31.1.1:4237    88.1.88.8:4237     88.1.88.8:4237
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:4238  172.31.1.1:4238    88.1.88.8:4238     88.1.88.8:4238
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:4239  172.31.1.1:4239    88.1.88.8:4239     88.1.88.8:4239
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:4240  172.31.1.1:4240    88.1.88.8:4240     88.1.88.8:4240
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.3:4241  172.31.1.1:4241    88.1.88.8:4241     88.1.88.8:4241
    create 00:00:08, use 00:00:08, left 00:00:51, Map-Id(In): 2,
    flags:
extended, use_count: 0, VRF : custB
icmp 192.168.1.1:874   172.31.1.1:874     88.1.88.8:874      88.1.88.8:874
    create 00:00:16, use 00:00:16, left 00:00:43, Map-Id(In): 3,
Pro Inside global      Inside local       Outside local      Outside global
    flags:
```

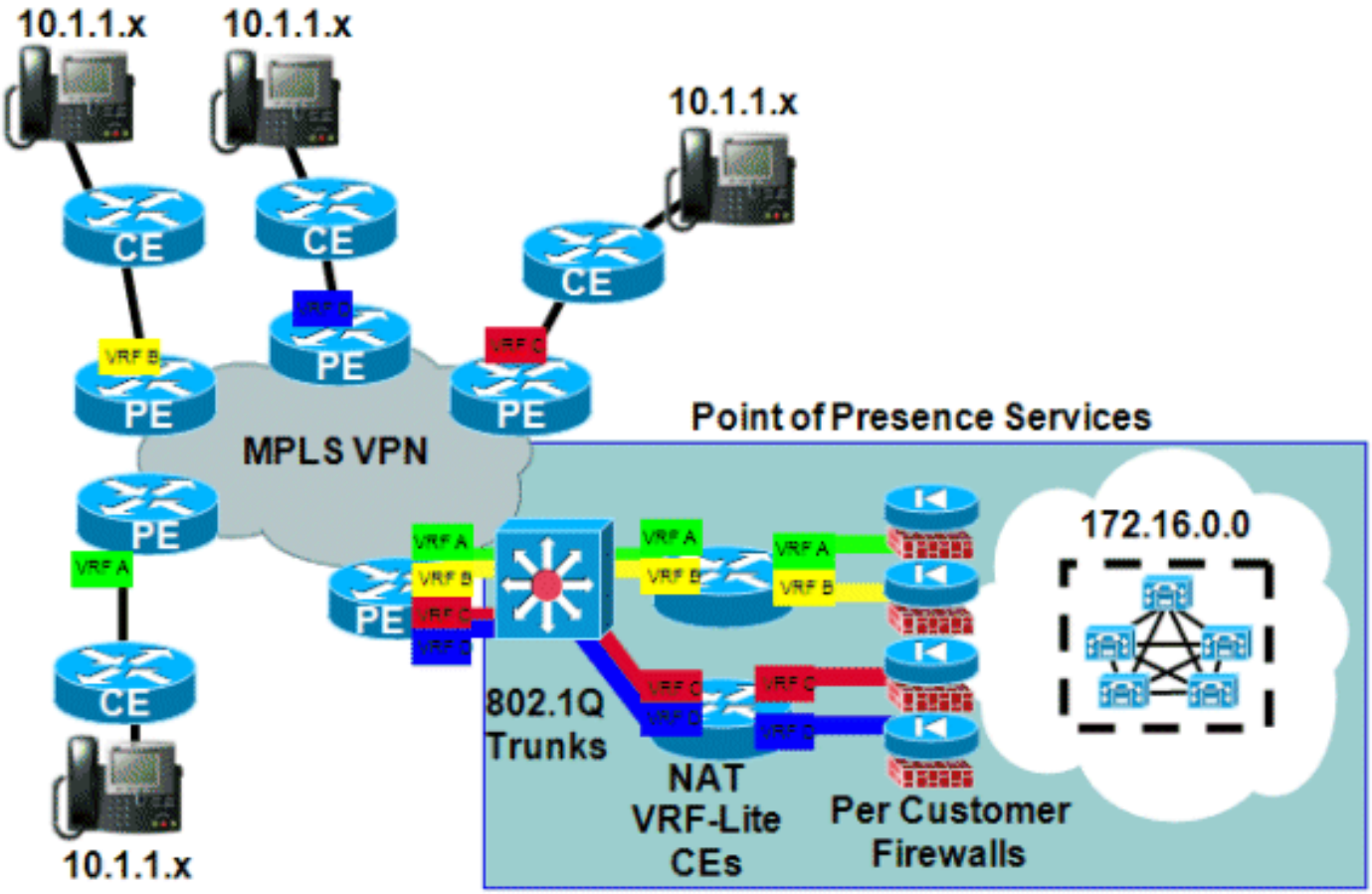
```
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:875   172.31.1.1:875     88.1.88.8:875      88.1.88.8:875
    create 00:00:18, use 00:00:18, left 00:00:41, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:876   172.31.1.1:876     88.1.88.8:876      88.1.88.8:876
    create 00:00:18, use 00:00:18, left 00:00:41, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:877   172.31.1.1:877     88.1.88.8:877      88.1.88.8:877
    create 00:00:18, use 00:00:18, left 00:00:41, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA
icmp 192.168.1.1:878   172.31.1.1:878     88.1.88.8:878      88.1.88.8:878
    create 00:00:18, use 00:00:18, left 00:00:41, Map-Id(In): 3,
    flags:
extended, use_count: 0, VRF : custA


gila#
debug ip nat vrf
IP NAT VRF debugging is on
gila#
.Jan  2 09:34:54 EST: NAT-TAGSW(p) : Tag Pkt s=172.18.60.179, d=10.88.162.9, vrf=custA
.Jan  2 09:35:02 EST: NAT-TAGSW(p) : Tag Pkt s=172.18.60.179, d=10.88.162.13, vrf=custB
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:19 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custB
.Jan  2 09:35:19 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:19 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custB
.Jan  2 09:35:19 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:19 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custB
.Jan  2 09:35:19 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:19 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custB
.Jan  2 09:35:19 EST: NAT-ip2tag: Punting to process
.Jan  2 09:35:19 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custB
.Jan  2 09:35:19 EST: NAT-ip2tag: Punting to process
gila#
```

服務範例

圖8中顯示了共用虛擬IP PBX服務的示例。該示例說明了前面介紹的入口和出口示例的變體。

在此設計中，共用VoIP服務由一組執行NAT功能的路由器前端。這些路由器具有使用稱為VRF-Lite的功能的多個VRF介面。然後，流量流向共用Cisco CallManager集群。防火牆服務也按公司提供。公司間呼叫必須通過防火牆，而公司內呼叫則使用公司的內部編址方案通過客戶VPN進行處理。

圖8:託管虛擬PBX服務示例



可用性

適用於MPLS VPN的Cisco IOS NAT支援在Cisco IOS版本12.2(13)T中提供，且適用於支援MPLS且可以執行此早期部署版本系列的所有平台。

結論

Cisco IOS NAT具有允許當前對共用服務進行可擴展部署的功能。Cisco繼續為客戶重要的協定開發NAT應用級網關(ALG)支援。轉換功能的效能改進和硬體加速將確保NAT和ALG在未來一段時間提供可接受的解決方案。思科正在監控所有相關標準活動和社群活動。在開發其他標準時，將根據客戶的需求、要求和應用來評估其使用。

相關資訊

- Cisco IOS NAT應用層閘道器
- MPLS和VPN架構
- 高級MPLS設計和實施
- 技術支援與文件 - Cisco Systems