Cisco IOS NAT - Integration mit MPLS VPN

Inhalt

Einführung

Die Cisco IOS® Network Address Translation (NAT)-Software ermöglicht den Zugriff auf gemeinsam genutzte Services über mehrere MPLS-VPNs, selbst wenn die Geräte in den VPNs IP-Adressen verwenden, die sich überschneiden. Cisco IOS NAT ist VRF-kompatibel und kann auf Provider Edge-Routern im MPLS-Netzwerk konfiguriert werden.

Hinweis: MPLS in IOS wird nur mit älterer NAT unterstützt. Cisco IOS bietet derzeit keine Unterstützung für NAT NVI mit MPLS.

Die Bereitstellung von MPLS-VPNs wird in den nächsten Jahren voraussichtlich rapide zunehmen. Die Vorteile einer gemeinsamen Netzwerkinfrastruktur, die eine schnelle Erweiterung und flexible Verbindungsoptionen ermöglicht, werden zweifellos das weitere Wachstum der Dienste fördern, die der Internetwork-Community angeboten werden können.

Allerdings bestehen nach wie vor Wachstumshemmnisse. IPv6 und sein Versprechen, einen IP-Adressbereich einzurichten, der die Verbindungsanforderungen in absehbarer Zukunft übersteigt, befinden sich noch in der Anfangsphase der Bereitstellung. Vorhandene Netzwerke verwenden in der Regel private IP-Adressierungsschemata, wie in RFC 1918 definiert. Die Netzwerkadressenübersetzung wird häufig zum Verbinden von Netzwerken verwendet, wenn sich Adressbereiche überschneiden oder doppelte Adressen vorhanden sind.

Service Provider und Unternehmen, die Netzwerkanwendungsservices anbieten oder mit Kunden und Partnern gemeinsam nutzen möchten, möchten den Aufwand für die Anbindung der Benutzer minimieren. Es ist wünschenswert, sogar obligatorisch, das Angebot auf so viele potenzielle Benutzer wie nötig zu erweitern, um die gewünschten Ziele zu erreichen oder die gewünschte Rendite zu erzielen. Das verwendete IP-Adressierungsschema darf keine Barriere darstellen, die potenzielle Benutzer ausschließt.

Durch die Bereitstellung von Cisco IOS NAT in der gemeinsamen MPLS VPN-Infrastruktur können Anbieter von Kommunikationsservices die Verbindungslast für Kunden teilweise reduzieren und ihre Fähigkeit beschleunigen, mehr gemeinsam genutzte Anwendungsservices mit einer größeren Anzahl von Nutzern dieser Services zu verknüpfen.

Vorteile von NAT - MPLS-Integration

Die NAT-Integration mit MPLS bietet Vorteile für Service Provider und ihre Unternehmenskunden. Service Providern stehen mehr Optionen für die Bereitstellung gemeinsam genutzter Services und die Bereitstellung des Zugriffs auf diese Services zur Verfügung. Zusätzliche Serviceangebote können sich von Mitbewerbern abheben.

Für Service Provider	Für VPN
Mehr Serviceangebote	Kostensenkung
Erweiterte Zugriffsoptionen	Einfacherer Zugriff
Höhere Umsätze	Flexible Adressierung

Unternehmenskunden, die einen Teil ihrer aktuellen Workloads auslagern möchten, können auch von umfassenderen Angeboten von Service Providern profitieren. Die Verlagerung des Verwaltungsaufwands für die Adressenübersetzung auf das Netzwerk des Service Providers entfällt auf diese Weise auf eine komplizierte Verwaltungsaufgabe. Kunden können weiterhin private Adressen verwenden, jedoch weiterhin auf gemeinsam genutzte Services und das Internet zugreifen. Durch die Konsolidierung der NAT-Funktion im Service Provider-Netzwerk können auch die Gesamtkosten für Unternehmenskunden gesenkt werden, da die Edge-Router des Kunden die NAT-Funktion nicht ausführen müssen.

Überlegungen zum Design

Bei Designs, die NAT im MPLS-Netzwerk aufrufen, besteht der erste Schritt darin, die Service-Anforderungen aus Anwendungssicht zu bestimmen. Sie müssen die verwendeten Protokolle und die spezielle Client/Server-Kommunikation berücksichtigen, die von der Anwendung vorgeschrieben wird. Stellen Sie sicher, dass die erforderliche Unterstützung für die verwendeten Protokolle von Cisco IOS NAT unterstützt und behandelt wird. Eine Liste der unterstützten Protokolle finden Sie im Dokument Cisco IOS NAT Application Layer Gateways.

Als Nächstes müssen die erwartete Nutzung des gemeinsam genutzten Services und die erwartete Datenverkehrsrate in Paketen pro Sekunde ermittelt werden. NAT ist eine CPU-intensive Funktion des Routers. Aus diesem Grund sind Leistungsanforderungen ein Faktor bei der Auswahl einer bestimmten Bereitstellungsoption und bei der Bestimmung der Anzahl der beteiligten NAT-Geräte.

Berücksichtigen Sie außerdem alle Sicherheitsprobleme und erforderlichen Vorsichtsmaßnahmen. Obwohl MPLS-VPNs definitionsgemäß privater und effektiv separater Datenverkehr sind, ist das Shared Service-Netzwerk bei vielen VPNs üblich.

Bereitstellungsszenarien

Es gibt zwei Optionen für die NAT-Bereitstellung am MPLS-Provider-Edge:

- Zentralisiert mit Ausgangs-NAT-PEs
- Verteilt mit Eingangs-NAT-PEs

Die Konfiguration der NAT-Funktion am Ausgangspunkt des MPLS-Netzwerks, das dem Shared Service-Netzwerk am nächsten liegt, bietet u. a. folgende Vorteile:

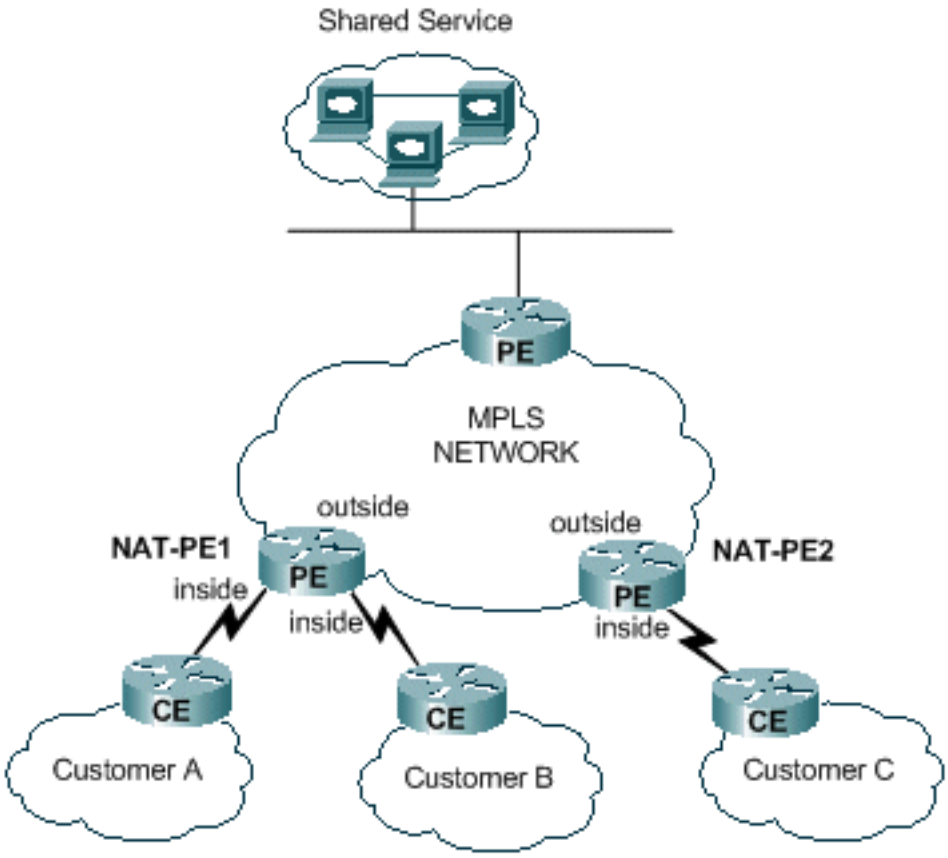
- Zentralisierte Konfiguration für eine einfachere Servicebereitstellung
- Vereinfachte Fehlerbehebung
- Verbesserte betriebliche Skalierbarkeit
- Geringere Anforderungen an die IP-Adresszuweisung

Die Vorteile werden jedoch durch eine geringere Skalierbarkeit und Leistung kompensiert. Dies ist der Hauptkonflikt, der berücksichtigt werden muss. Natürlich kann die NAT-Funktion auch innerhalb der Kundennetzwerke ausgeführt werden, wenn festgestellt wird, dass eine Integration dieser Funktion in ein MPLS-Netzwerk nicht wünschenswert ist.

Eingangs-PE NAT

NAT kann auf dem PE-Router des MPLS-Netzwerkeingangs konfiguriert werden, wie in Abbildung 1 gezeigt. Bei diesem Design wird die Skalierbarkeit weitgehend beibehalten, während die Leistung durch die Verteilung der NAT-Funktion auf viele Edge-Geräte optimiert wird. Jeder NAT-PE verarbeitet Datenverkehr für Standorte, die lokal mit diesem PE verbunden sind. NAT-Regeln und Zugriffskontrolllisten oder Routenzuordnungen steuern, welche Pakete übersetzt werden müssen.

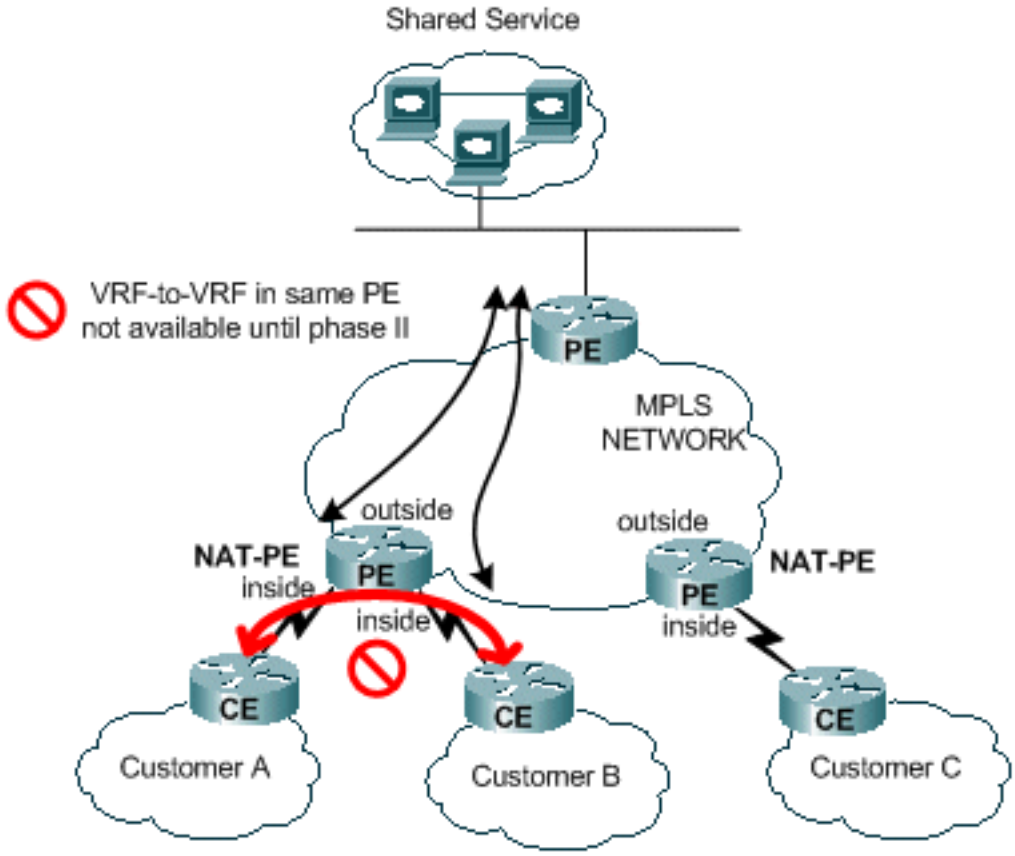
Abbildung 1: Eingangs-PE NAT



Es gibt eine Einschränkung, die NAT zwischen zwei VRFs verhindert und gleichzeitig NAT für einen gemeinsam genutzten Dienst bereitstellt (siehe Abbildung 2). Dies liegt daran, dass Schnittstellen als "interne" und "externe" NAT-Schnittstellen definiert werden müssen. Die Unterstützung von Verbindungen zwischen VRFs in einem einzigen PE ist für eine zukünftige

Cisco IOS-Version geplant.

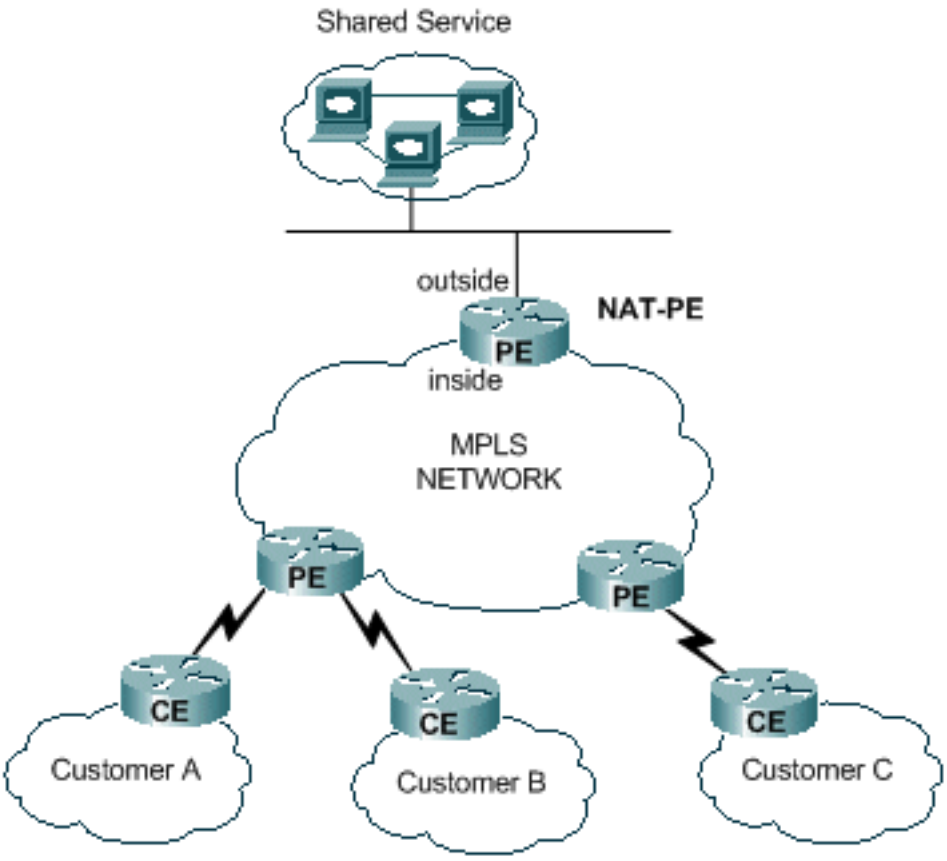
Abbildung 2: Business-to-Business



Ausgangs-PE NAT

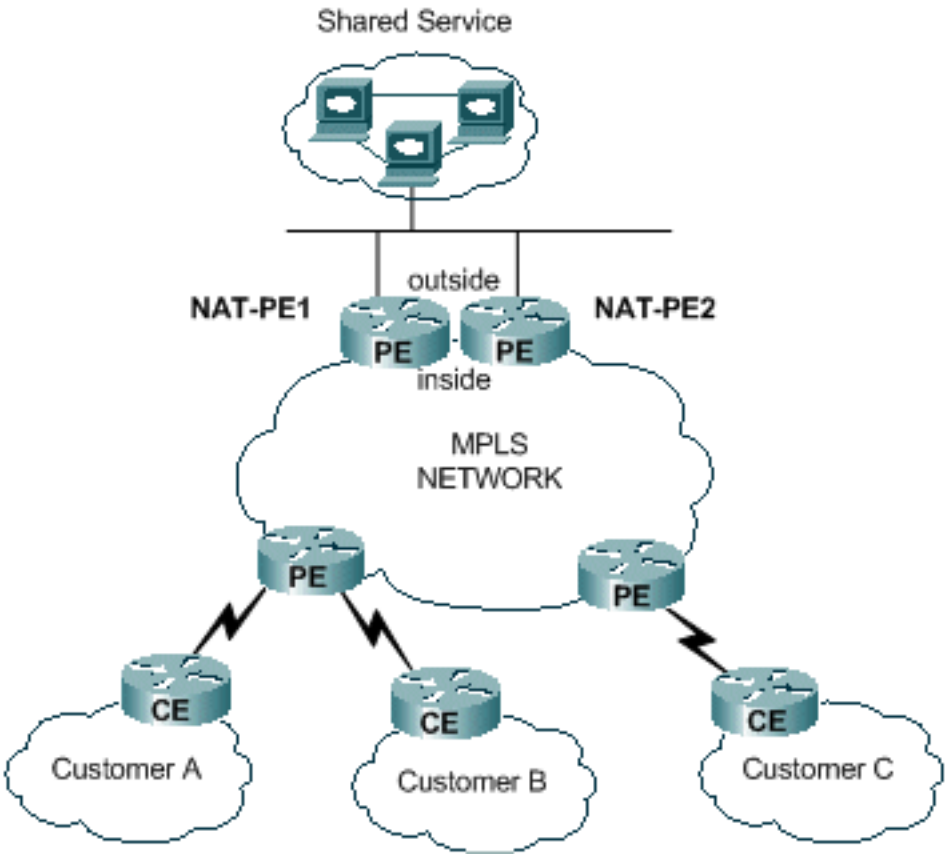
NAT kann am MPLS-Netzwerk-Egress-PE-Router konfiguriert werden, wie in Abbildung 3 gezeigt. Bei diesem Design wird die Skalierbarkeit bis zu einem gewissen Grad verringert, da der zentrale PE Routen für alle Kundennetzwerke aufrechterhalten muss, die auf den gemeinsamen Dienst zugreifen. Die Anforderungen an die Anwendungsleistung müssen ebenfalls berücksichtigt werden, damit der Datenverkehr den Router, der die IP-Adressen der Pakete übersetzen muss, nicht überlastet. Da NAT zentral für alle Kunden erfolgt, die diesen Pfad verwenden, können IP-Adresspools gemeinsam genutzt werden. Dadurch wird die Gesamtzahl der benötigten Subnetze verringert.

Abbildung 3: Ausgangs-PE NAT



Es können mehrere Router bereitgestellt werden, um die Skalierbarkeit des Ausgangs-PE-NAT-Designs zu erhöhen, wie in Abbildung 4 gezeigt. In diesem Szenario können Kunden-VPNs auf einem bestimmten NAT-Router "bereitgestellt" werden. Die Netzwerkadressumwandlung erfolgt für den gesamten Datenverkehr zum und vom gemeinsam genutzten Service für diese VPN-Gruppe. Beispielsweise könnte der Datenverkehr von den VPNs für Kunde A und B NAT-PE1 verwenden, während der Datenverkehr zum und vom VPN für Kunde C NAT-PE2 verwendet. Jeder NAT-PE würde nur den Datenverkehr für die definierten VPNs übertragen und nur Routen zu den Standorten in diesen VPNs verwalten. In jedem NAT-PE-Router können separate NAT-Adresspools definiert werden, sodass Pakete vom Netzwerk des gemeinsam genutzten Dienstes zum entsprechenden NAT-PE weitergeleitet werden, um übersetzt und an das Kunden-VPN zurückgeleitet zu werden.

Abbildung 4: Multiple Egress PE NAT



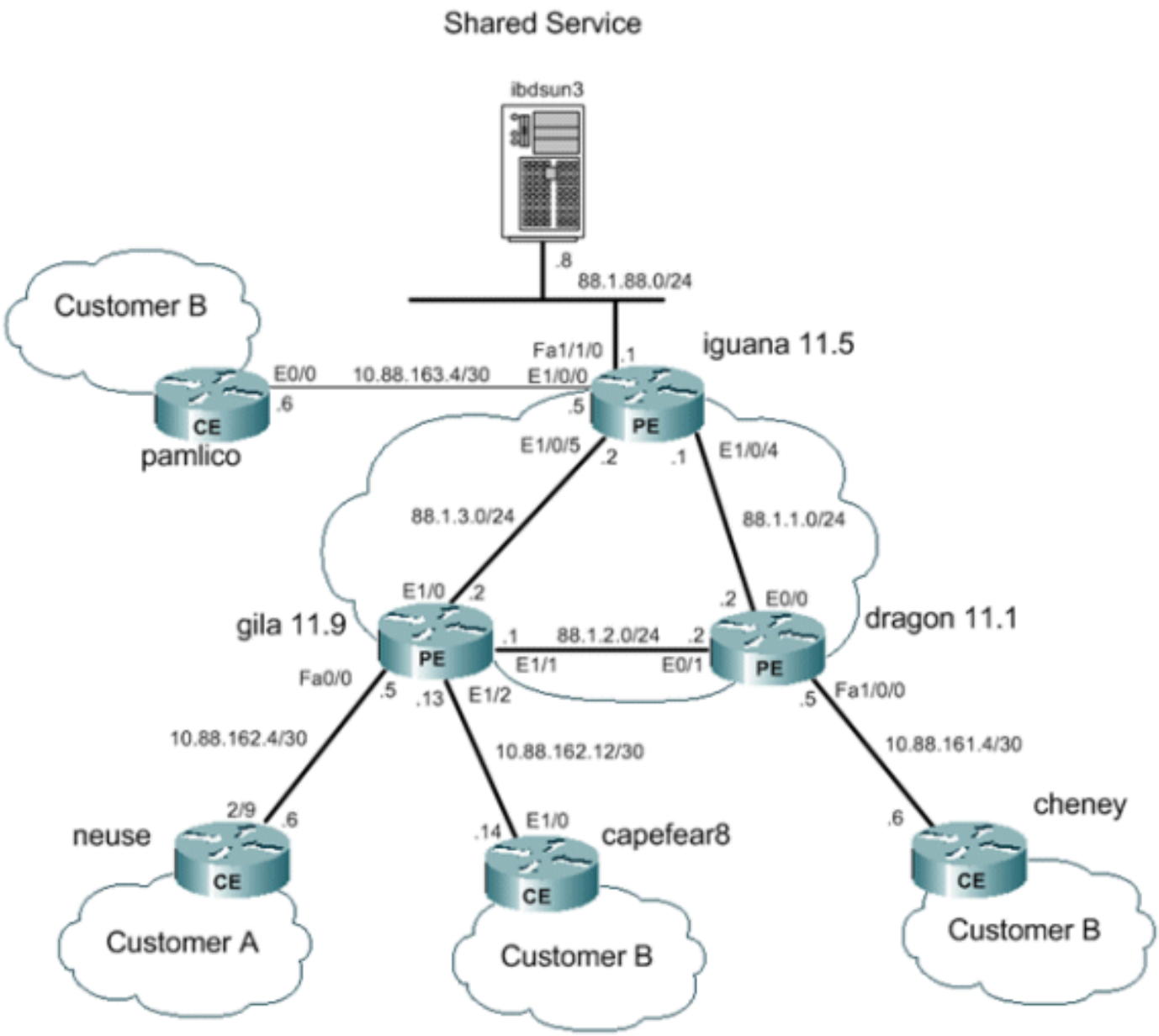
Das zentrale Design schränkt die Konfiguration des Shared-Service-Netzwerks ein. Insbesondere ist der Import/Export von MPLS-VPN-Routen zwischen einem Shared Service-VPN und Kunden-VPNs nicht möglich. Dies liegt an der Beschaffenheit des MPLS-Vorgangs gemäß RFC 2547 . Beim Import und Export von Routen mithilfe der erweiterten Communitys und Routendeskriptoren kann die NAT das Quell-VPN des Pakets, das in den zentralen NAT-PE gelangt, nicht bestimmen. Üblicherweise wird das Shared Service-Netzwerk zu einer generischen Schnittstelle und nicht zu einer VRF-Schnittstelle. Im zentralen NAT-PE wird dann für jede VRF-Tabelle, die einem Kunden-VPN zugeordnet ist, das im Rahmen des Bereitstellungsprozesses Zugriff auf den gemeinsam genutzten Service benötigt, eine Route zum Shared Service-Netzwerk hinzugefügt. Dies wird später genauer beschrieben.

Bereitstellungsoptionen und Konfigurationsdetails

Dieser Abschnitt enthält einige Details zu den einzelnen Bereitstellungsoptionen. Die Beispiele stammen alle aus dem in Abbildung 5 gezeigten Netzwerk. Weitere Informationen finden Sie in diesem Diagramm.

Hinweis: Im Netzwerk, das zur Veranschaulichung des Betriebs von VRF NAT für dieses Whitepaper verwendet wird, sind nur PE-Router enthalten. Es gibt keine Core-"P"-Router. Die wesentlichen Mechanismen sind jedoch noch sichtbar.

Abbildung 5: VRF NAT-Konfigurationsbeispiel



Ausgangs-PE NAT

In diesem Beispiel werden die Provider-Edge-Router mit der Bezeichnung **gila** und **Dragon** als einfache PE-Router konfiguriert. Der zentrale PE in der Nähe des Shared Service LAN (**iguana**) ist für NAT konfiguriert. Jeder Kunde-VPN, der Zugriff auf den gemeinsam genutzten Service benötigt, nutzt einen einzelnen NAT-Pool. Die NAT wird nur für Pakete ausgeführt, die für den Host des gemeinsam genutzten Dienstes unter 88.1.88.8 bestimmt sind.

Ausgangs-PE NAT-Datenweiterleitung

Mit MPLS tritt jedes Paket an einem Eingangs-PE in das Netzwerk ein und verlässt das MPLS-Netzwerk an einem Ausgangs-PE. Der Pfad der Label Switching-Router, die von ein- bis ausgehen, wird als Label Switched Path (LSP) bezeichnet. Der LSP ist unidirektional. Für den Rückverkehr wird ein anderer LSP verwendet.

Bei der Verwendung von Egress-PE-NAT wird effektiv eine Weiterleitungsäquivalenzklasse (FEC) für den gesamten Datenverkehr von Benutzern des gemeinsam genutzten Dienstes definiert. Mit anderen Worten: Alle Pakete, die für das LAN des gemeinsam genutzten Dienstes bestimmt sind, gehören einem gemeinsamen FEC an. Ein Paket wird einem bestimmten FEC nur einmal am

Eingangs-Edge des Netzwerks zugewiesen und folgt dem LSP zum Ausgangs-PE. Der FEC wird im Datenpaket durch Hinzufügen eines bestimmten Labels gekennzeichnet.

Paketfluss zum freigegebenen Service vom VPN

Für Geräte in mehreren VPNs mit sich überschneidenden Adressierungsschemata für den Zugriff auf einen Host für gemeinsam genutzte Dienste ist NAT erforderlich. Wenn NAT am Ausgangs-PE konfiguriert wird, enthalten die Einträge der Netzwerkadressenübersetzungstabelle eine VRF-ID, um doppelte Adressen zu identifizieren und ein ordnungsgemäßes Routing sicherzustellen.

Abbildung 6: An die Egress-PE-NAT übertragene Pakete

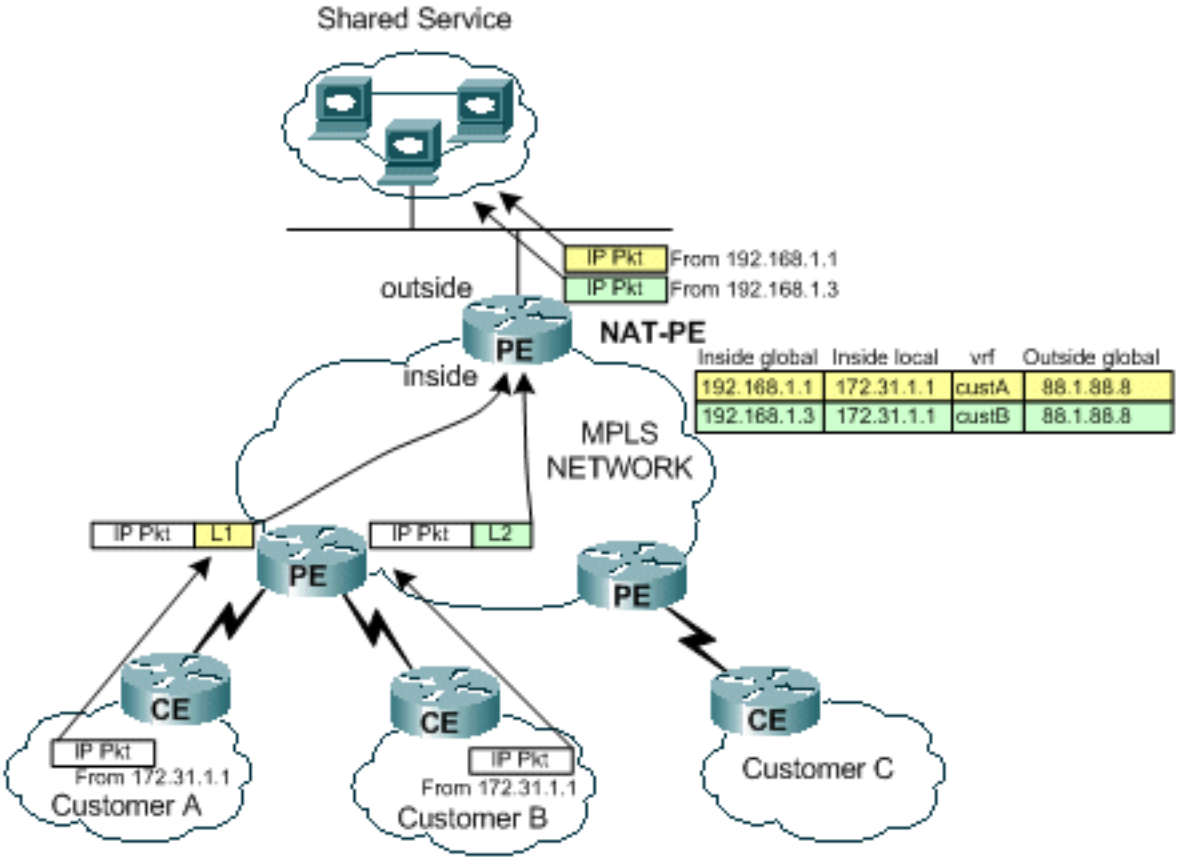


Abbildung 6 zeigt Pakete, die von zwei Kunden-VPNs mit doppelten IP-Adressierungsschemata für einen Host für gemeinsam genutzte Dienste bestimmt sind. Die Abbildung zeigt ein von Kunde A stammendes Paket mit der Quelladresse 172.31.1.1, das für einen gemeinsam genutzten Server unter 88.1.88.8 bestimmt ist. Ein weiteres Paket von Kunde B mit derselben Quell-IP-Adresse wird ebenfalls an denselben freigegebenen Server gesendet. Wenn die Pakete den PE-Router erreichen, wird eine Layer-3-Suche für das Ziel-IP-Netzwerk in der Forwarding Information Base (FIB) durchgeführt.

Der FIB-Eintrag weist den PE-Router an, den Datenverkehr mithilfe eines Label-Stacks an den Egress-PE weiterzuleiten. Das untere Label im Stack wird vom Ziel-PE-Router zugewiesen, in diesem Fall Router-**Leguana**.

```
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#
```

Die Anzeige zeigt an, dass Pakete von VRF custA einen Tagwert von 24 (0x18) haben und Pakete von VRF custB einen Tagwert von 28 (0x1C) aufweisen.

Da in diesem Fall keine "P"-Router in unserem Netzwerk vorhanden sind, wird kein zusätzliches Tag festgelegt. Hätte es Core-Router gegeben, wäre ein externes Label festgelegt worden, und der normale Prozess des Label-Austauschs hätte im Core-Netzwerk stattgefunden, bis das Paket den Egress-PE erreicht hätte.

Da der **Jila-**Router direkt mit dem Egress-PE verbunden ist, wird das Tag vor dem Hinzufügen immer wieder angehoben:

```
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#
```

Die nächste Anzeige zeigt Echo-Pakete, die vom ausgehenden PE NAT-Router empfangen wurden (an der Schnittstelle E1/0/5 auf iguana).

```
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".]
```

Diese Pings führen dazu, dass die folgenden Einträge in der NAT-Tabelle in der iguana des Ausgangs-PE-Routers erstellt werden. Die spezifischen Einträge, die für die oben gezeigten Pakete erstellt wurden, können mit ihrer ICMP-Kennung abgeglichen werden.

```
iguana#
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
```

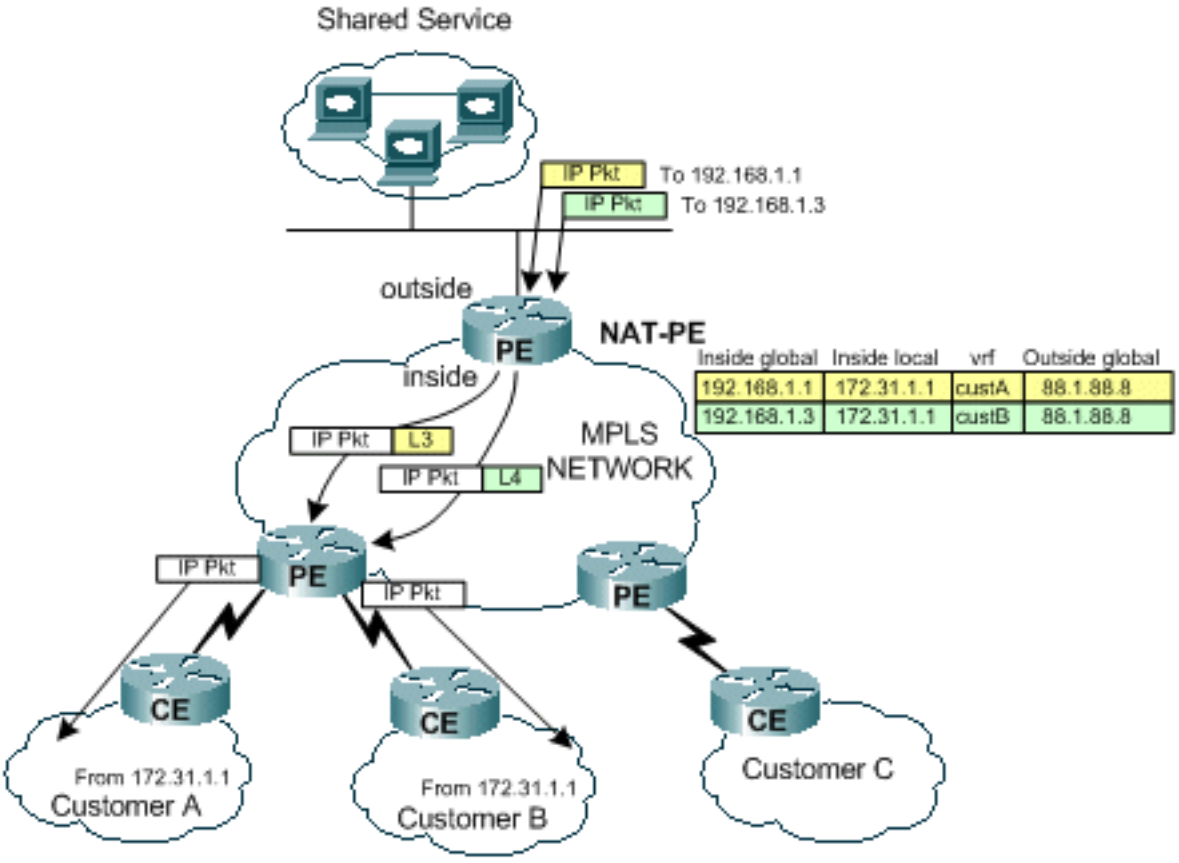
```
icmp 192.168.1.3:3365  172.31.1.1:3365    88.1.88.8:3365     88.1.88.8:3365
icmp 192.168.1.3:3366  172.31.1.1:3366    88.1.88.8:3366     88.1.88.8:3366
icmp 192.168.1.3:3367  172.31.1.1:3367    88.1.88.8:3367     88.1.88.8:3367
icmp 192.168.1.3:3368  172.31.1.1:3368    88.1.88.8:3368     88.1.88.8:3368
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#
```

Paketfluss vom Shared Service Back-to-Origin VPN

Wenn Pakete an Geräte zurückfließen, die auf den Host für den gemeinsam genutzten Service

zugegriffen haben, wird die NAT-Tabelle vor dem Routing überprüft (Pakete werden von der "externen" NAT-Schnittstelle zur "internen" Schnittstelle gesendet). Da jeder einzelne Eintrag die entsprechende VRF-ID enthält, kann das Paket entsprechend übersetzt und weitergeleitet werden.

Abbildung 7: Pakete werden zurück an Benutzer des gemeinsam genutzten Dienstes übertragen



Wie in Abbildung 7 gezeigt, wird der Rückverkehr zunächst von NAT überprüft, um einen passenden Übersetzungseintrag zu finden. Beispielsweise wird ein Paket an das Ziel 192.168.1.1 gesendet. Die NAT-Tabelle wird durchsucht. Wenn eine Übereinstimmung gefunden wurde, wird die entsprechende Übersetzung an die "interne lokale" Adresse (172.31.1.1) durchgeführt, und anschließend wird eine Adjacency-Suche mit der zugehörigen VRF-ID des NAT-Eintrags durchgeführt.

```
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#
```

Label 23 (0x17) wird für Datenverkehr verwendet, der für 172.31.1.0/24 im VRF-KundeA bestimmt ist, und das Label 26 (0x1A) wird für Pakete verwendet, die für 172.31.1.0/24 im VRF-KundeB bestimmt sind.

Dies wird in den Echo-Antwortpaketen angezeigt, die von Router **iguana** gesendet wurden:

```
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".]
```

Wenn das Paket den Ziel-PE-Router erreicht, wird das Label verwendet, um die entsprechende VRF-Instanz und Schnittstelle zum Senden des Pakets zu ermitteln.

```
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#
```

Konfigurationen

Einige externe Informationen wurden aus Gründen der Kürze aus den Konfigurationen entfernt.

```
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
!
```

Der **Drache** des Routers hätte eine sehr ähnliche Konfiguration wie die **Gila**.

Import/Export von Route Targets nicht zulässig

Wenn das Shared-Service-Netzwerk selbst als VRF-Instanz konfiguriert ist, ist eine zentrale NAT am Egress-PE nicht möglich. Der Grund hierfür ist, dass die eingehenden Pakete nicht unterschieden werden können und nur eine Route zurück zum ursprünglichen Subnetz im Egress-PE-NAT vorhanden ist.

Hinweis: Die folgenden Anzeigen sollen das Ergebnis einer ungültigen Konfiguration veranschaulichen.

Das Beispielnetzwerk wurde so konfiguriert, dass das Shared Service-Netzwerk als VRF-Instanz definiert wurde (VRF-Name = Server). Eine Anzeige der CEF-Tabelle auf dem Eingangs-PE zeigt Folgendes:

```
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#
```

Hinweis: Beachten Sie, dass der Tag-Wert *24* sowohl für VRF-KundeA als auch für VRF-KundeB festgelegt wird.

Diese Anzeige zeigt die Routing-Tabelle für die VRF-Instanz "Server" des Shared Service:

```
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
```

Hinweis: Aus der **Leguana**-Perspektive des Egress-PE-Routers ist für das Zielnetzwerk nur eine Route vorhanden.

Aus diesem Grund konnte der Datenverkehr von mehreren Kunden-VPNs nicht ausgezeichnet werden, und der zurückkehrende Datenverkehr konnte das entsprechende VPN nicht erreichen. **Wenn der gemeinsam genutzte Service als VRF-Instanz definiert werden muss, muss die NAT-Funktion in den Eingangs-PE verschoben werden.**

Eingangs-PE NAT

In diesem Beispiel werden die Provider Edge-Router mit den **Namen "gila"** und **"Dragon"** für NAT konfiguriert. Für jedes angeschlossene Kunden-VPN, das Zugriff auf den gemeinsam genutzten Service benötigt, wird ein NAT-Pool definiert. Der entsprechende Pool wird für jede NAT-Adresse des Kundennetzwerks verwendet. Die NAT wird nur für Pakete ausgeführt, die für den Host des gemeinsam genutzten Dienstes unter 88.1.88.8 bestimmt sind.

```
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
```

Hinweis: In diesem Szenario werden gemeinsame Pools nicht unterstützt. Wenn das LAN des gemeinsam genutzten Dienstes (am Ausgangs-PE) über eine generische Schnittstelle verbunden ist, kann der NAT-Pool gemeinsam genutzt werden.

Ein Ping, der von einer doppelten Adresse (172.31.1.1) in jedem der Netzwerke stammt, die an das **Netzwerk** angeschlossen sind, und **capeFurcht8** führen zu folgenden NAT-Einträgen:

Von **gila**:

```
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
```

Hinweis: Dieselbe interne lokale Adresse (172.31.1.1) wird entsprechend der Quell-VRF-Instanz in jeden der definierten Pools übersetzt. Die VRF-Instanz wird im Befehl **show ip nat translation Ausführse** angezeigt:

```
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
```

Diese Anzeigen zeigen die Routing-Informationen für die lokal angeschlossenen VPNs für Kunde A und Kunde B an:

```
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
```

Hinweis: Aus der statischen Konfiguration wurde eine Route für jeden der NAT-Pools hinzugefügt. Diese Subnetze werden anschließend in die gemeinsam genutzte Server-VRF-Instanz am Ausgangs-PE-Router **iguana** importiert:

```
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
```

Konfigurationen

Einige externe Informationen wurden aus Gründen der Kürze aus den Konfigurationen entfernt.

```
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
!
```

Hinweis: Die Schnittstellen zu den Kundennetzwerken werden als "interne" NAT-Schnittstellen festgelegt, und die MPLS-Schnittstellen werden als "externe" NAT-Schnittstellen festgelegt.

```
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
```

Der **Drache** des Routers hätte eine sehr ähnliche Konfiguration wie die **Gila**.

Pakete, die nach dem Eingangs-PE NAT am zentralen PE ankommen

Die nachfolgenden Nachverfolgungen veranschaulichen die Anforderung an eindeutige NAT-Pools, wenn das Ziel-Shared-Service-Netzwerk als VRF-Instanz konfiguriert ist. Weitere Informationen finden Sie im Diagramm in Abbildung 5. Die unten gezeigten Pakete wurden erfasst, als sie bei der **iguana** des Routers die MPLS-IP-Schnittstelle e1/0/5 betraten.

Echo von Kunde A VPN

Hier sehen wir eine Echoanfrage, die von der Quell-IP-Adresse 172.31.1.1 in VRF CustA ausgeht. Die Quelladresse wurde gemäß der NAT-Konfiguration in 192.168.1.1 übersetzt:

```
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:
```

Echo von Customer B VPN

Hier sehen wir eine Echoanfrage, die von der Quell-IP-Adresse 172.31.1.1 in VRF CustB ausgeht. Die Quelladresse wurde gemäß der NAT-Konfiguration in 192.168.2.1 übersetzt:

```
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".]
```

Hinweis: Der Wert des MPLS-Labels ist in beiden oben gezeigten Paketen *0019*.

Echoantwort auf Kunde A VPN

Als Nächstes wird eine Echoantwort in VRF-KundeA an die Ziel-IP-Adresse 192.168.1.1 zurückgesendet. Die Zieladresse wird durch die Eingangs-PE-NAT-Funktion in 172.31.1.1 übersetzt.

```
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:
```

Echoantwort auf Customer B VPN

Hier sehen wir eine Echo-Antwort, die in VRF custB an die Ziel-IP-Adresse 192.168.1.1 zurückgeht. Die Zieladresse wird durch die Eingangs-PE-NAT-Funktion in 172.31.1.1 übersetzt.

```
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".]
```

Hinweis: In den Rückgabepaketen sind die Werte des MPLS-Labels enthalten und unterscheiden sich: *001A* für VRF-KundeA und *001D* für VRF-KundeB.

Echo von Kunde A VPN - Ziel ist eine generische Schnittstelle

Die folgenden Pakete zeigen den Unterschied, wenn die Schnittstelle zum gemeinsam genutzten Service-LAN eine generische Schnittstelle und nicht Teil einer VRF-Instanz ist. Hier wurde die Konfiguration geändert, um einen gemeinsamen Pool für beide lokalen VPNs mit sich überschneidenden IP-Adressen zu verwenden.

```
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".]
```

Echo von Customer B VPN - Ziel ist eine generische Schnittstelle

Hier sehen wir eine Echoanfrage, die von der Quell-IP-Adresse 172.31.1.1 in VRF CustB ausgeht. Die Quelladresse wurde gemäß der NAT-Konfiguration in 192.168.1.3 (aus dem gemeinsamen Pool SSPOOL1) übersetzt:

```
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".]
```

Hinweis: Wenn es sich bei der Schnittstelle am Ausgangs-PE um eine generische Schnittstelle (keine VRF-Instanz) handelt, unterscheiden sich die angegebenen Labels. In diesem Fall *0 x 19* und *0 x 1 F*.

Echoantwort an Kunde A VPN - Ziel ist eine generische Schnittstelle

Als Nächstes wird eine Echoantwort in VRF-KundeA an die Ziel-IP-Adresse 192.168.1.1 zurückgesendet. Die Zieladresse wird durch die Eingangs-PE-NAT-Funktion in 172.31.1.1 übersetzt.

```
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".]
```

Echo Reply to Customer B VPN - Das Ziel ist eine generische Schnittstelle.

Hier sehen wir eine Echo-Antwort, die in VRF custB an die Ziel-IP-Adresse 192.168.1.3 zurückgeht. Die Zieladresse wird durch die Eingangs-PE-NAT-Funktion in 172.31.1.1 übersetzt.

```
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".]
```

Hinweis: Da die Antworten für eine globale Adresse bestimmt sind, werden keine VRF-Labels bereitgestellt.

Wenn die Exit-Schnittstelle zum Shared-Service-LAN-Segment als generische Schnittstelle definiert ist, ist ein gemeinsamer Pool zulässig. Die Pings führen zu folgenden NAT-Einträgen in Router **gila**:

```
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
```

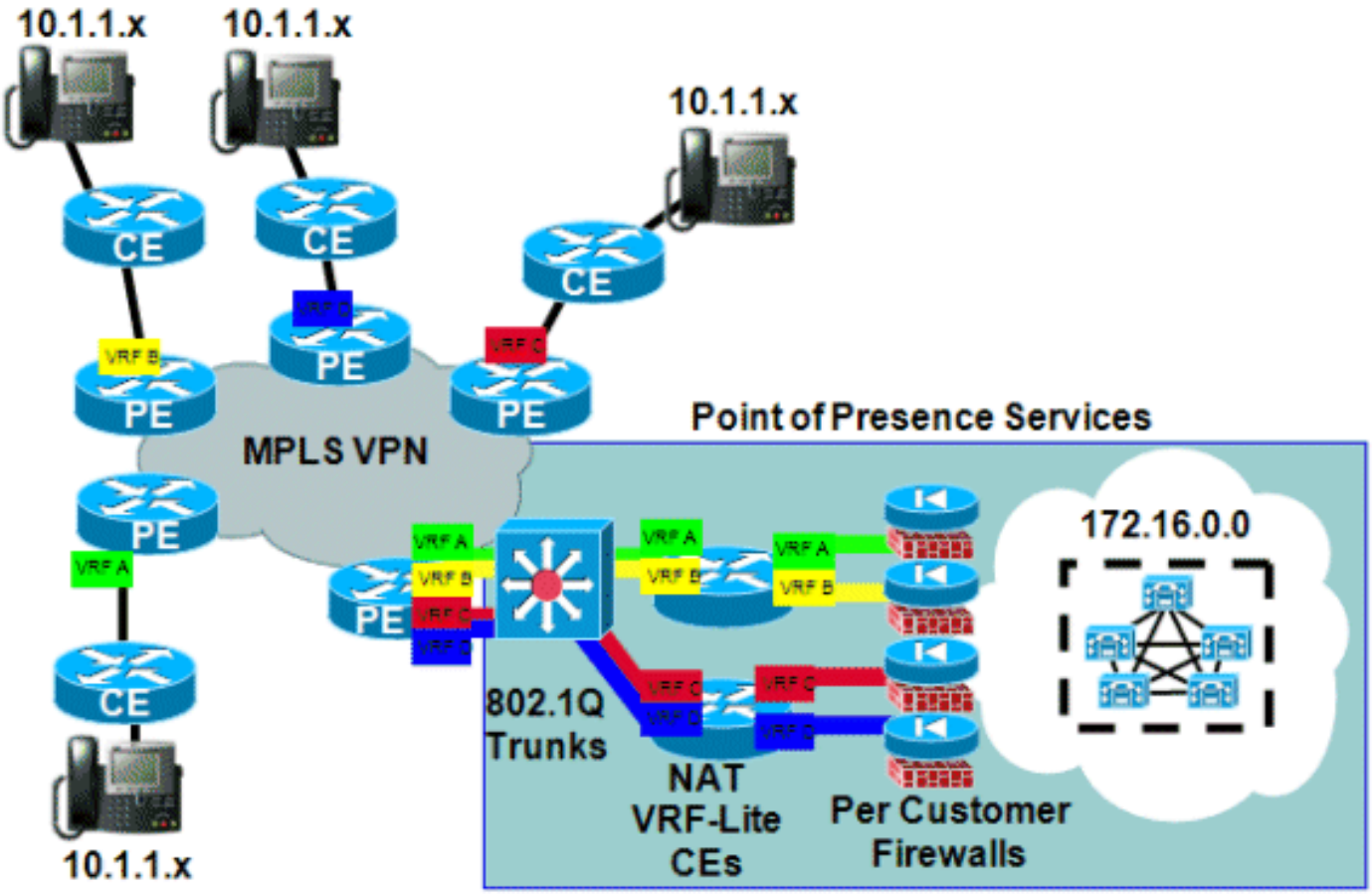
```
gila#
.Jan  2 09:34:54 EST: NAT-TAGSW(p) : Tag Pkt s=172.18.60.179, d=10.88.162.9, vrf=custA
.Jan  2 09:35:02 EST: NAT-TAGSW(p) : Tag Pkt s=172.18.60.179, d=10.88.162.13, vrf=custB
.Jan  2 09:35:12 EST: NAT-ip2tag : Tag Pkt s=172.31.1.1, d=88.1.88.8, vrf=custA
.Jan  2 09:35:12 EST: NAT-ip2tag: Punting 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#
```

Beispiel für einen Service

Ein Beispiel für einen gemeinsam genutzten virtuellen IP-PBX-Dienst ist in Abbildung 8 dargestellt. Dies zeigt eine Variante der zuvor beschriebenen Eingangs- und Ausgangsbeispiele.

Bei diesem Design ist der gemeinsam genutzte VoIP-Service mit einer Reihe von Routern verbunden, die die NAT-Funktion ausführen. Diese Router verfügen über mehrere VRF-Schnittstellen, die die Funktion VRF-Lite verwenden. Der Datenverkehr fließt dann zum gemeinsam genutzten Cisco CallManager-Cluster. Firewall-Services werden auch auf Unternehmensbasis bereitgestellt. Firmenübergreifende Anrufe müssen die Firewall passieren, während firmeninterne Anrufe über das Kunden-VPN mithilfe des internen Adressierungsschemas des Unternehmens verarbeitet werden.

Abbildung 8: Beispiel für einen Managed Virtual PBX Service



Verfügbarkeit

Die Cisco IOS NAT-Unterstützung für MPLS-VPNs ist in Cisco IOS 12.2(13)T verfügbar und steht für alle Plattformen zur Verfügung, die MPLS unterstützen. Sie kann diesen Zug für die vorzeitige Bereitstellung ausführen.

Schlussfolgerung

Cisco IOS NAT verfügt über Funktionen, die eine skalierbare Bereitstellung gemeinsam genutzter Services ermöglichen. Cisco entwickelt auch weiterhin die Unterstützung von NAT-Gateways (ALGs) für Protokolle, die für Kunden wichtig sind. Leistungsverbesserungen und Hardware-Beschleunigung bei Übersetzungsfunktionen sorgen dafür, dass NAT und ALGs noch in der Zukunft akzeptable Lösungen bieten. Alle relevanten Standardisierungsaktivitäten und Community-Aktionen werden von Cisco überwacht. Wenn andere Standards entwickelt werden, wird deren Verwendung anhand der Wünsche, Anforderungen und Anwendungen des Kunden bewertet.

Zugehörige Informationen

- Cisco IOS NAT Application Layer Gateways
- MPLS- und VPN-Architekturen
- Erweitertes MPLS-Design und Implementierung
- Technischer Support und Dokumentation - Cisco Systems