

Configurazione della VPN di base MPLS con RIP sul lato cliente

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Descrizione rete](#)

[Convenzioni](#)

[Procedura di configurazione](#)

[Esempio di rete](#)

[Parte I](#)

[Parte II](#)

[Esempi di configurazione](#)

[Comandi debug e show](#)

[Etichette MPLS](#)

[Indirizzo sovrapposto](#)

[Output di esempio del comando debug](#)

[Risoluzione dei problemi](#)

Introduzione

In questa configurazione di esempio viene mostrato un MPLS (Multiprotocol Label Switching) con rete privata virtuale (VPN) quando il protocollo RIP (Routing Information Protocol) è presente sul lato del cliente.

La funzionalità VPN, se utilizzata con MPLS, consente a più siti di interconnettersi in modo trasparente tramite la rete di un provider di servizi. Una rete di provider di servizi può supportare diverse VPN IP. Ogni VPN IP viene visualizzata come una rete privata, distinta da tutte le altre reti. Ogni sito in una VPN invia pacchetti IP ad altri siti nella stessa VPN.

Ogni VPN è associata a una o più istanze di routing o inoltro VPN (VRF). Un VRF è costituito da una tabella di routing IP, una tabella CEF (Cisco Express Forwarding) derivata e un set di interfacce che utilizzano la tabella di inoltro.

Il router gestisce un routing separato e una tabella CEF per ciascun VRF. In questo modo si impedisce l'invio delle informazioni all'esterno della VPN e si consente l'utilizzo della stessa subnet in più VPN senza causare problemi di indirizzi IP duplicati.

Il router che utilizza il Border Gateway Protocol (BGP) distribuisce le informazioni di routing VPN utilizzando le community estese BGP.

Per ulteriori informazioni sulla propagazione degli aggiornamenti tramite VPN, vedere le sezioni VPN Route Target Communities, BGP Distribution of VPN Routing Information e MPLS Forwarding in [MPLS Virtual Private Network](#).

[Prerequisiti](#)

[Requisiti](#)

Non sono previsti prerequisiti specifici per questo documento.

[Componenti usati](#)

Questa configurazione è stata sviluppata e testata utilizzando le versioni software e hardware riportate di seguito:

- **Router PE:** La funzionalità VPN MPLS risiede nei router PE. Utilizzare [Feature Navigator II](#) (solo utenti [registrati](#)) per determinare le combinazioni hardware e software che è possibile utilizzare.
- **Router CE:** Utilizzare qualsiasi router in grado di scambiare informazioni di routing con il relativo router PE.
- **Router e switch IP:** In questo documento, sono stati usati switch ATM come l'MSR, il BPX e il MGX. Tuttavia, poiché il documento si concentra sulla funzione VPN di MPLS, avremmo potuto usare MPLS basato su frame anche nel core con router, come Cisco 12000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

[Descrizione rete](#)

È stata creata una backbone MPLS ATM standard utilizzando Open Shortest Path First (OSPF) area 0 come IGP (Interior Gateway Protocol). Abbiamo configurato due VPN diverse usando questa backbone. La prima VPN utilizza RIP come protocollo di routing da edge-to-provider (CE-PE); l'altra VPN utilizza BGP come protocollo di routing PE-CE. Sono stati configurati vari router statici e di loopback sui router CE per simulare la presenza di altri router e reti.

Nota: BGP deve essere utilizzato come VPN IGP tra router PE, poiché l'utilizzo delle community estese BGP è l'unico modo per trasportare le informazioni di routing per la VPN tra i router PE.

Nota: per eseguire questa configurazione è stata utilizzata una rete ATM come rete backbone. Questa configurazione si applica ai protocolli ATM (e altri). Affinché la configurazione VPN funzioni, i router PE devono essere in grado di comunicare tra loro utilizzando la rete MPLS.

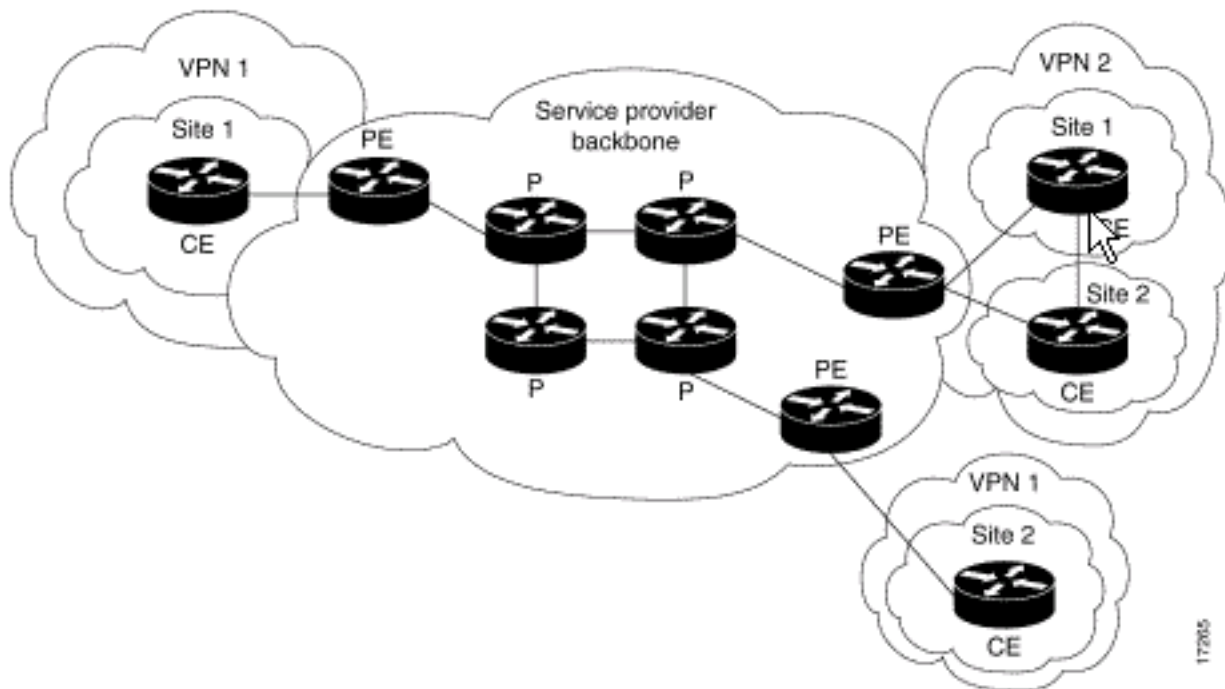
[Convenzioni](#)

Le lettere seguenti rappresentano i diversi tipi di router e switch utilizzati:

- P: Router di base del provider
- PE: Router perimetrale del provider

- CE: Router perimetrale del cliente
- C: Router del cliente

Nel diagramma seguente è illustrata una configurazione tipica che illustra queste convenzioni:



Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

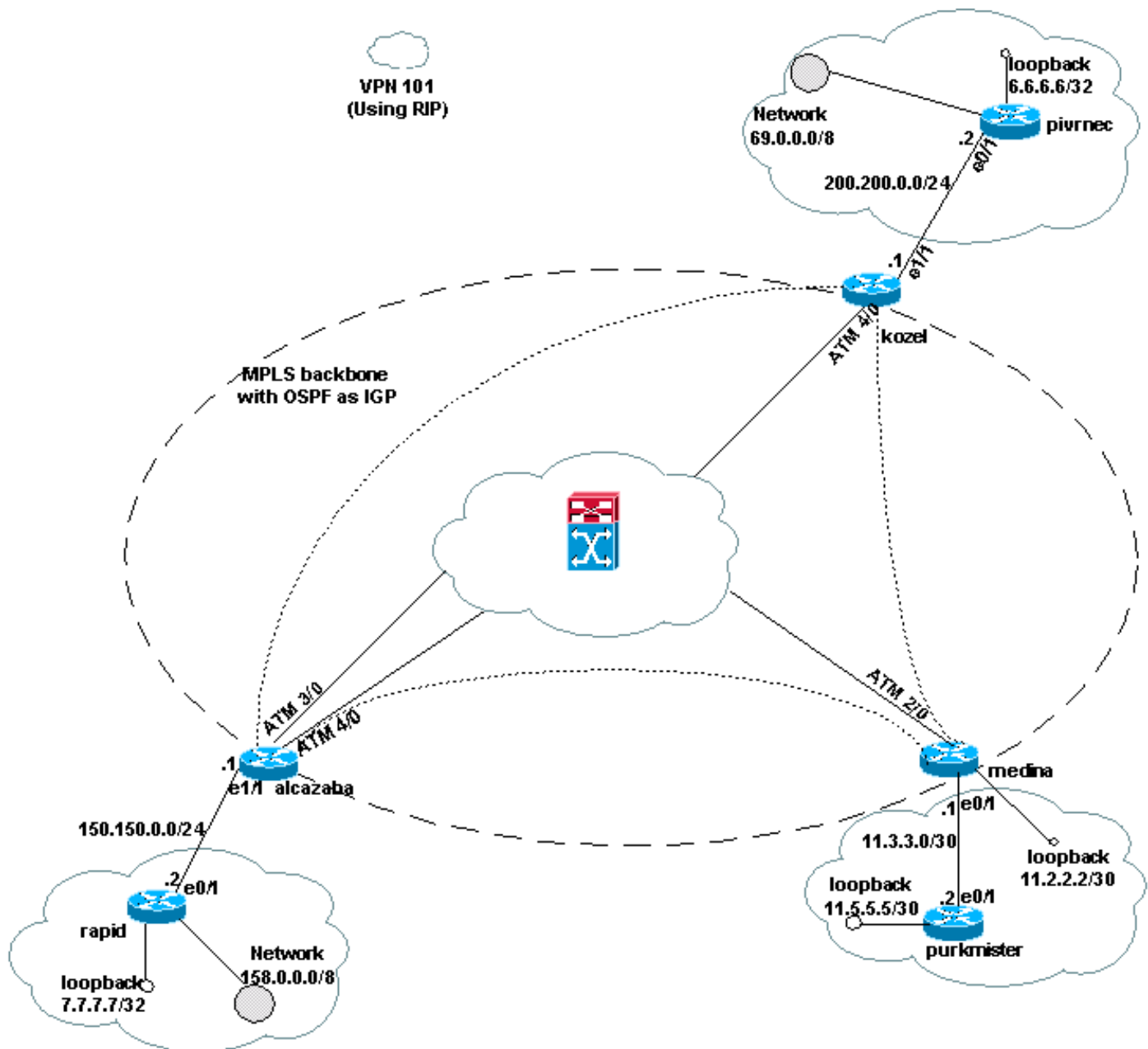
Procedura di configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento. Anche la documentazione di Cisco IOS disponibile in [MPLS Virtual Private Network](#) descrive questa procedura di configurazione.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) IOS (solo utenti [registrati](#))

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Parte I

La procedura seguente consente di eseguire la configurazione corretta.

Abilitare il comando **ip cef**. Se si usa un router Cisco 7500, verificare che il comando **ip cef distributed** sia abilitato, se disponibile, per migliorare le prestazioni sul server PE, una volta configurato MPLS.

1. Creare un VRF per ciascuna VPN utilizzando il protocollo **ip vrf [VPN routing] | forwarding instance name**. Durante la creazione dei VRF, assicurarsi di: Specificare il distinguitore di route corretto utilizzato per la VPN utilizzando il comando seguente. Il distinguitore viene utilizzato per estendere l'indirizzo IP e consente di identificare la VPN a cui appartiene.

```
rd [VPN route distinguisher]
```

Impostare le proprietà di importazione ed esportazione per le community estese BGP utilizzando il comando seguente. Queste proprietà vengono utilizzate per filtrare il processo di importazione ed esportazione.

```
route-target {export | import | both} [target VPN extended community]
```

2. Configurare i dettagli di inoltro per le rispettive interfacce utilizzando il comando **ip vrf forwarding [nome tabella]** e ricordarsi di configurare l'indirizzo IP in seguito.
3. A seconda del protocollo di routing PE-CE utilizzato, eseguire una o più delle operazioni seguenti: Configurare le route statiche nel modo seguente:

```
ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}]
```

Configurare il RIP utilizzando il comando seguente:

```
address-family ipv4 vrf [VPN routing | forwarding instance name]
```

Dopo aver completato uno o entrambi i passaggi precedenti, immettere i normali comandi di configurazione RIP. **Nota:** questi comandi si applicano solo alle interfacce di inoltro del VRF corrente. Ridistribuire il BGP corretto in RIP e ricordare di specificare la metrica utilizzata. Dichiarare le informazioni sui router adiacenti BGP. Configurare OSPF utilizzando il nuovo comando IOS:

```
router ospf process-id vrf [VPN routing | forwarding instance name]
```

Nota: questo comando è valido solo per le interfacce di inoltro del VRF corrente. Ridistribuire le informazioni di routing BGP corrette in OSPF e specificare la metrica utilizzata. Una volta completato il processo OSPF su un VRF, anche se il processo OSPF non è specificato nella riga di comando, questo ID di processo viene sempre utilizzato per il VRF specifico.

Parte II

Configurare il protocollo BGP tra i router PE. Esistono diversi modi per configurare BGP, ad esempio utilizzando il reflector di route o i metodi di confederazione. Il metodo mostrato è la configurazione dei nodi adiacenti diretti. È il più semplice e il meno scalabile.

1. Dichiarate i diversi vicini.
2. Immettere il **percorso della famiglia di indirizzi ipv4 vrf [VPN routing] | forwarding instance name]** per ogni VPN presente in questo router PE. Eseguire una o più delle seguenti operazioni, se necessario: Ridistribuire le informazioni di routing statiche. Ridistribuire le informazioni di routing RIP. Ridistribuire le informazioni di routing OSPF. Attivare BGP adiacente con i router CE.
3. Immettere la modalità **vpn4 della famiglia di indirizzi** e: Attivare i vicini. Specificare che deve essere utilizzata la community estesa. Questa operazione è obbligatoria.

Esempi di configurazione

Nella configurazione Alcalzaba, le linee specifiche della configurazione VPN sono mostrate in **grassetto**.

Alcazaba
!

```
ip vrf vrf101
  rd 1:101
  route-target export 1:101
  route-target import 1:101
!
ip cef
!
interface Loopback0
  ip address 223.0.0.3 255.255.255.255
!
interface Ethernet1/1
  ip vrf forwarding vrf101
  ip address 150.150.0.1 255.255.255.0
!
interface ATM3/0
  no ip address
  no ip mroute-cache
  no ATM ilmi-keepalive
  PVC qsaal 0/5 qsaal
  PVC ilmi 0/16 ilmi
!
!
interface ATM3/0.1 tag-switching
  ip address 10.0.0.17 255.255.255.252
  tag-switching ATM vpi 2-4
  tag-switching ip
!
interface ATM4/0
  no ip address
  no ATM ilmi-keepalive
!
interface ATM4/0.1 tag-switching
  ip address 10.0.0.13 255.255.255.252
  tag-switching ATM vpi 2-4
  tag-switching ip
!
router ospf 1
  network 10.0.0.0 0.0.0.255 area 0
  network 223.0.0.3 0.0.0.0 area 0
!
router rip
  version 2
  !
  address-family ipv4 vrf vrf101
  version 2
  redistribute bgp 1 metric 0
  network 150.150.0.0
  no auto-summary
  exit-address-family
!
router bgp 1
  no synchronization
  neighbor 125.2.2.2 remote-as 1
  neighbor 125.2.2.2 update-source Loopback0
  neighbor 223.0.0.21 remote-as 1
  neighbor 223.0.0.21 update-source Loopback0
  no auto-summary
  !
  address-family ipv4 vrf vrf101
  redistribute rip
  no auto-summary
  no synchronization
  exit-address-family
!
```

```
address-family vpv4
neighbor 125.2.2.2 activate
neighbor 125.2.2.2 send-community extended
neighbor 223.0.0.21 activate
neighbor 223.0.0.21 send-community extended
no auto-summary
exit-address-family
!
```

Kozel

```
!
ip vrf vrf101
  rd 1:101
  route-target export 1:101
  route-target import 1:101
!
ip cef
!
interface Loopback0
  ip address 223.0.0.21 255.255.255.255
!
interface Ethernet1/1
  ip vrf forwarding vrf101
  ip address 200.200.0.1 255.255.255.0
!
interface ATM4/0
  no ip address
  no ATM scrambling cell-payload
  no ATM ilmi-keepalive
  PVC qsaal 0/5 qsaal
  PVC ilmi 0/16 ilmi
!
interface ATM4/0.1 tag-switching
  ip address 10.0.0.6 255.255.255.252
  tag-switching ATM vpi 2-4
  tag-switching ip
!
router ospf 1
  log-adjacency-changes
  network 10.0.0.0 0.0.0.255 area 0
  network 223.0.0.21 0.0.0.0 area 0
!
router rip
  version 2
  !
  address-family ipv4 vrf vrf101
  version 2
  redistribute bgp 1 metric 1
  network 200.200.0.0
  no auto-summary
  exit-address-family
!
router bgp 1
  no synchronization
  neighbor 125.2.2.2 remote-as 1
  neighbor 125.2.2.2 update-source Loopback0
  neighbor 223.0.0.3 remote-as 1
  neighbor 223.0.0.3 update-source Loopback0
  no auto-summary
  !
  address-family ipv4 vrf vrf101
  redistribute rip
```

```
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 125.2.2.2 activate
neighbor 125.2.2.2 send-community extended
neighbor 223.0.0.3 activate
neighbor 223.0.0.3 send-community extended
no auto-summary
exit-address-family
!
```

Medina

Current configuration:

```
!
ip vrf vrf101
  rd 1:101
  route-target export 1:101
  route-target import 1:101
ip cef
!
interface Loopback1
  ip vrf forwarding vrf101
  ip address 11.2.2.2 255.255.255.252
!
interface ATM2/0
  no ip address
  no ATM ilmi-keepalive
!
interface ATM2/0.66 tag-switching
  ip address 125.1.4.2 255.255.255.252
  tag-switching ip
!
interface Ethernet1/1
  ip vrf forwarding vrf101
  ip address 11.3.3.1 255.255.255.252
!
router ospf 1

  network 125.1.4.0 0.0.0.3 area 0
  network 125.2.2.2 0.0.0.0 area 0
!
router rip
  version 2
  network 11.0.0.0
  !
  address-family ipv4 vrf vrf101
  version 2
  redistribute bgp 1 metric 1
  network 11.0.0.0
  no auto-summary
  exit-address-family
!
router bgp 1
  no synchronization
  neighbor 223.0.0.3 remote-as 1
  neighbor 223.0.0.3 update-source Loopback0
  neighbor 223.0.0.21 remote-as 1
  neighbor 223.0.0.21 update-source Loopback0
  !
  address-family ipv4 vrf vrf101
```



```
redistribute connected
redistribute static
redistribute rip
default-information originate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 223.0.0.3 activate
neighbor 223.0.0.3 send-community extended
neighbor 223.0.0.21 activate
neighbor 223.0.0.21 send-community extended
exit-address-family
!
```

Rapido

Current configuration:

```
!
interface Loopback0
 ip address 223.0.0.12 255.255.255.255
!
interface Loopback2
 ip address 7.7.7.7 255.255.255.0
!
interface FastEthernet0/1
 ip address 150.150.0.2 255.255.255.0
 duplex auto
 speed auto
!
router rip
 version 2
 redistribute static
 network 7.0.0.0
 network 10.0.0.0
 network 150.150.0.0
 no auto-summary
!
ip route 158.0.0.0 255.0.0.0 Null0
!
```

Dannazione

```
!
interface Loopback1
 ip address 6.6.6.6 255.0.0.0
!
interface FastEthernet0/0
 ip address 10.200.10.14 255.255.252.0
 duplex auto
 speed autoa
!
router bgp 158
 no synchronization
 network 6.0.0.0
 network 10.200.0.0 mask 255.255.252.0
 neighbor 10.200.10.3 remote-as 1
 no auto-summary
!
```

Pivrnec

```
Current configuration:
!
interface Loopback0
 ip address 223.0.0.22 255.255.255.255
!
interface Loopback1
 ip address 6.6.6.6 255.255.255.255
!
interface FastEthernet0/1
 ip address 200.200.0.2 255.255.255.0
 duplex auto
 speed auto
!
router rip
 version 2
 redistribute static
 network 6.0.0.0
 network 200.200.0.0
 no auto-summary
!
ip route 69.0.0.0 255.0.0.0 Null0
!
```

Fiorino

```
!
interface Loopback2
 ip address 150.150.0.1 255.255.0.0
!
interface Ethernet0/2
 ip address 201.201.201.2 255.255.255.252
!
router bgp 69
 no synchronization
 network 7.7.7.0 mask 255.255.0.0
 network 150.150.0.0
 network 201.201.201.0 mask 255.255.255.252
 redistribute connected
 neighbor 201.201.201.1 remote-as 1
 no auto-summary
!
```

Purkmister

```
Current configuration:
!
interface Loopback0
 ip address 11.5.5.5 255.255.255.252
!
interface FastEthernet0/1
 ip address 11.3.3.2 255.255.255.252
 duplex auto
 speed auto
!
router rip
 version 2
 network 11.0.0.0
!
```

Prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#). I comandi specifici del routing sono elencati di seguito:

- **show ip rip database vrf**: visualizza le informazioni contenute nel database RIP per un particolare VRF.
- **show ip bgp vpnv4 vrf**: visualizza le informazioni sull'indirizzo VPN dalla tabella BGP.
- **show ip route vrf**: visualizza la tabella di routing IP associata a un VRF.
- **show ip route**: visualizza tutte le route IP statiche o quelle installate utilizzando la funzione di download delle route di autenticazione, autorizzazione e accounting (AAA).

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Su un router PE, il metodo di routing PE-CE, ad esempio RIP, BGP o statico, e gli aggiornamenti PE-PE BGP indicano la tabella di routing utilizzata per un determinato VRF. È possibile visualizzare le informazioni RIP per un particolare VRF nel modo seguente:

```
Alcazaba# show ip rip database vrf vrf101
0.0.0.0/0 auto-summary
0.0.0.0/0
[2] via 150.150.0.2, 00:00:12, Ethernet1/1
6.0.0.0/8 auto-summary
6.6.6.6/32 redistributed
[1] via 223.0.0.21,
7.0.0.0/8 auto-summary
7.7.7.0/24
[1] via 150.150.0.2, 00:00:12, Ethernet1/1
10.0.0.0/8 auto-summary
10.0.0.0/8 redistributed
[1] via 125.2.2.2,
10.0.0.0/16
[1] via 150.150.0.2, 00:00:12, Ethernet1/1
10.200.8.0/22
[1] via 150.150.0.2, 00:00:12, Ethernet1/1
11.0.0.0/8 auto-summary
11.0.0.4/30 redistributed
[1] via 125.2.2.2,
11.1.1.0/30 redistributed
[1] via 125.2.2.2,
11.3.3.0/30 redistributed
[1] via 125.2.2.2,
11.5.5.4/30 redistributed
[1] via 125.2.2.2,
69.0.0.0/8 auto-summary
69.0.0.0/8 redistributed
[1] via 223.0.0.21,
150.150.0.0/16 auto-summary
150.150.0.0/24 directly connected, Ethernet1/1
158.0.0.0/8
[1] via 150.150.0.2, 00:00:17, Ethernet1/1
200.200.0.0/24 auto-summary
200.200.0.0/24 redistributed
[1] via 223.0.0.21,
```

Per visualizzare le informazioni BGP di un determinato VRF, usare il comando **show ip bgp vpnv4 vrf**. I risultati PE-PE dal protocollo BGP (iBGP) interno sono indicati da una **i** nell'output sottostante.

```
Alcazaba# show ip bgp vpnv4 vrf vrf101
```

```
BGP table version is 46, local router ID is 223.0.0.3
Status codes: s suppressed, d damped, h history, * valid, best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vrf101)
*i6.6.6.6/32 223.0.0.21 1 100 0 ?
* 7.7.7.0/24 150.150.0.2 1 32768 ?
* 10.0.0.0/16 150.150.0.2 1 32768 ?
* 10.200.8.0/22 150.150.0.2 1 32768 ?
*i11.2.2.0/30 125.2.2.2 0 100 0 ?
*i11.3.3.0/30 125.2.2.2 0 100 0 ?
*i11.5.5.4/30 125.2.2.2 1 100 0 ?
*i69.0.0.0 223.0.0.21 1 100 0 ?
* 150.150.0.0/24 0.0.0.0 0 32768 ?
* 158.0.0.0/8 150.150.0.2 1 32768 ?
*i200.200.0.0 223.0.0.21 0 100 0 ?
```

Controllare se nella tabella di routing globale è presente un VRF su entrambi i router PE e CE. Questi VRF devono corrispondere. Per il router PE, è necessario specificare il VRF utilizzando il comando **show ip route vrf**:

```
Alcazaba# show ip route vrf vrf101
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - ISIS, L1 - ISIS level-1, L2 - ISIS level-2, IA - ISIS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
B 69.0.0.0/8 [200/1] via 223.0.0.21, 00:11:03
B 200.200.0.0/24 [200/0] via 223.0.0.21, 00:11:03
 6.0.0.0/32 is subnetted, 1 subnets
B 6.6.6.6 [200/1] via 223.0.0.21, 00:11:03
 7.0.0.0/24 is subnetted, 1 subnets
R 7.7.7.0 [120/1] via 150.150.0.2, 00:00:05, Ethernet1/1
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R 10.0.0.0/16 [120/1] via 150.150.0.2, 00:00:05, Ethernet1/1
R 10.200.8.0/22 [120/1] via 150.150.0.2, 00:00:05, Ethernet1/1
 11.0.0.0/30 is subnetted, 3 subnets
B 11.3.3.0 [200/0] via 125.2.2.2, 00:07:05
B 11.2.2.0 [200/0] via 125.2.2.2, 00:07:05
B 11.5.5.4 [200/1] via 125.2.2.2, 00:07:05
 150.150.0.0/24 is subnetted, 1 subnets
C 150.150.0.0 is directly connected, Ethernet1/1
R 158.0.0.0/8 [120/1] via 150.150.0.2, 00:00:06, Ethernet1/1
```

Il comando equivalente su PivotConnect è il comando **show ip route**, in quanto per ogni router cliente (e lato cliente) questa è la tabella di routing standard.

```
Pivrnec# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - ISIS, L1 - ISIS level-1, L2 - ISIS level-2, IA - ISIS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route Gateway of last resort is not
set S 69.0.0.0/8 is directly connected, Null0
223.0.0.0/32 is subnetted, 1 subnets
C 223.0.0.22 is directly connected, Loopback0
```

```
C 200.200.0.0/24 is directly connected, FastEthernet0/1
 6.0.0.0/32 is subnetted, 1 subnets
C 6.6.6.6 is directly connected, Loopback1
 7.0.0.0/24 is subnetted, 1 subnets
R 7.7.7.0 [120/1] via 200.200.0.1, 00:00:23, FastEthernet0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R 10.0.0.0/16 [120/1] via 200.200.0.1, 00:00:23, FastEthernet0/1
R 10.200.8.0/22 [120/1] via 200.200.0.1, 00:00:24, FastEthernet0/1
11.0.0.0/30 is subnetted, 3 subnets
R 11.3.3.0 [120/1] via 200.200.0.1, 00:00:24, FastEthernet0/1
R 11.2.2.0 [120/1] via 200.200.0.1, 00:00:25, FastEthernet0/1
R 11.5.5.4 [120/1] via 200.200.0.1, 00:00:25, FastEthernet0/1
150.150.0.0/24 is subnetted, 1 subnets
R 150.150.0.0 [120/1] via 200.200.0.1, 00:00:25, FastEthernet0/1
R 158.0.0.0/8 [120/1] via 200.200.0.1, 00:00:25, FastEthernet0/1
```

Etichette MPLS

Controllare lo stack di etichette utilizzato per qualsiasi route come segue:

```
Alcazaba# show tag-switching forwarding-table vrf vrf101 11.5.5.5 detail
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
None 2/91 11.5.5.4/30 0 AT4/0.1 point2point
MAC/Encaps=4/12, MTU=4466, Tag Stack{2/91(vcd=69) 37}
00458847 0004500000025000
```

È possibile utilizzare i normali comandi per visualizzare le allocazioni dei tag insieme alle relazioni VPI/VCI (Virtual Path Identifier) e VCI (Virtual Channel Identifier), come mostrato in [Come risolvere i problemi della VPN MPLS](#).

Indirizzo sovrapposto

È possibile utilizzare lo stesso indirizzo in VPN diverse senza interferire con altre VPN. Nell'esempio, l'indirizzo 6.6.6.6 viene connesso due volte, a Pivrnec nella VPN 101 e a Damme nella VPN 102. Per verificare questa condizione, usare il comando `ping` su un sito e il comando `debug ip icmp` sull'altro sito.

```
Guilder# ping 6.6.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

```
Damme# debug ip icmp
ICMP packet debugging is on
6d22h: ICMP: echo reply sent, src 6.6.6.6, DST 201.201.201.2
6d22h: ICMP: echo reply sent, src 6.6.6.6, DST 201.201.201.2
6d22h: ICMP: echo reply sent, src 6.6.6.6, DST 201.201.201.2
6d22h: ICMP: echo reply sent, src 6.6.6.6, DST 201.201.201.2
6d22h: ICMP: echo reply sent, src 6.6.6.6, DST 201.201.201.2
```

Output di esempio del comando debug

Per visualizzare l'output di esempio relativo alla stessa configurazione, fare riferimento al [flusso di pacchetto in un ambiente VPN MPLS](#).

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.