

# Utilizza GTM (Global Table Multicast) non segmentato per mVPN

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Architettura](#)

[Quali sono le modifiche apportate alla RFC 6513/6514?](#)

[Modifiche alla configurazione](#)

[Annuncio route](#)

[Esempi](#)

[Esempio 1: profilo 12: MDT - mLDP - P2MP - BGP-AD - BGP C-mcast Signaling](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

[Router per bordo in entrata](#)

[Router del bordo in uscita](#)

[Esempio 2: Profilo 20 MDT predefinito - P2MP-TE - BGP-AD - PIM - Segnalazione C-mcast](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

[Router per bordo in entrata](#)

[Router del bordo in uscita](#)

[Esempio 3: come nell'esempio 1, ma tra PE e Border Router è presente iBGP](#)

[Esempio 4: MPLS perfetto](#)

## Introduzione

Questo documento descrive la tabella globale multicast (GTM) non segmentata per mVPN.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

## Premesse

NG mVPN (RFC 6513/6514) ha molti profili. La maggior parte dei profili dispone di VPN (Virtual Private Network) o VRF (Virtual Routing/Forwarding) sui router PE. Alcuni profili (profili 7 e sono nel contesto globale. Per questi profili che sono già globali, BGP Auto Discovery (AD) viene introdotto con GTM. Per i profili presenti nel contesto VRF, i profili sono ora disponibili nel contesto globale, con la struttura MDT (Multicast Distribution Tree). Si tratta di modelli GTM non segmentati. Le procedure utilizzate dal GTM non segmentato sono descritte in IETF draft-ietf-bess-mvpn-global-table-mcast.

Sia la [RFC 7524](#) che la [RFC 7716](#) (draft-ietf-band-mvpn-global-table-mcast) richiedono che gli indirizzi di origine GTM siano raggiungibili tramite route unicast BGP (unicast IPv4 della famiglia di indirizzi o multicast IPv4 della famiglia di indirizzi).

Il vantaggio della bozza draft-ietf-bess-mvpn-global-table-mcast rispetto alla RFC 7524 è che vengono mantenute le stesse procedure utilizzate per la normale RFC 6514 (NG mVPN).

Con GTM, la mVPN può essere non segmentata o segmentata.

## Architettura

In questo articolo, il termine router di confine viene usato per un router ABR, ASBR o Aggregation, che connette due segmenti della rete. In genere, ABR si trova in reti MPLS senza interruzioni. L'ASBR viene utilizzato quando si utilizza una VPN MPLS Inter-AS. Inoltre, il router di aggregazione viene utilizzato quando un router di overlay GTM non segmentato connette le due parti della rete principale, quando una delle due parti esegue un protocollo albero principale multicast diverso. Ad esempio, il router di aggregazione può connettere la parte PIM della rete principale con la parte mLDP della rete principale.

Per qualsiasi modello, è possibile utilizzare il SAFI 2. Il vantaggio è che SAFI 2 può avere una topologia diversa rispetto a SAFI 1. È quindi possibile modificare la RPF per il multicast senza modificare l'inoltro unicast.

Un router di confine non supporta l'incapsulamento doppio. Ciò significa che il router non può inoltrare il multicast su due protocolli core-tree o in modalità diversa contemporaneamente. Questa opzione può essere utilizzata in genere quando si esegue la migrazione da un albero principale a un altro. Durante la migrazione, il file PE in entrata viene inoltrato su entrambi gli alberi centrali. Ciò non è possibile sui router di confine.

L'architettura GTM supporta GTM non segmentati e segmentati. Il presente documento si riferisce esclusivamente al GTM non segmentato.

Le procedure per la sovrapposizione GTM non segmentata sono quelle descritte in draft-ietf-bess-mvpn-global-table-mcast. Vengono seguite le stesse procedure descritte nella RFC 6513/6514 con alcune modifiche.

## Quali sono le modifiche apportate alla RFC 6513/6514?

Con GTM, si applicano i punti seguenti. Alcuni di essi sono uguali a quelli della RFC 6513/6514, altri sono diversi.

- Selezione inoltro singolo (SFS) non supportata.
- AF IPv6 è supportato.
- È supportata la segnalazione C-PIM e C-BGP.
- Sulle interfacce dei router PE rivolte verso il bordo non è presente alcun VRF. Queste interfacce sono ora globali. Questi router sono noti come Protocol Boundary Router (PBR) nel draft-ietf-bess-mvpn-global-table-mcast. Questi router si interfacciano tra un protocollo LSM Core Tree e un PIM. Questi router li chiamiamo router di confine.
- La rete principale esegue un protocollo LSM (Label Switched Multicast).
- sono supportati mLDP, P2MP TE (statico e dinamico) e IR.
- Sono supportati MDT di dati, partizionati e predefiniti
- Poiché non esistono prefissi VPNv4/6 in GTM, i prefissi VRF Route-Import EC e Source-AS EC sono collegati ai prefissi IPv4 unicast (SAFI 1) o multicast (SAFI 2).

I tipi di route 1, 3 e 5 dispongono di RT. In Cisco IOS® XR questi RT devono essere presenti per GTM, anche se non è richiesto dalla bozza. Affinché GTM possa essere utilizzato, è necessario configurare gli RT in BGP. Questi RT sono simili agli RT utilizzati nei VRF per le mVPN regolari, ma si applicano ora al contesto globale.

I router di tipo 4, 6 e 7 sono dotati di una funzionalità RT che identifica il router PE upstream. Il campo Amministratore globale corrisponde all'indirizzo IP del file PE a monte. Il campo dell'amministratore locale è impostato su 0 per GTM (identifica il VRF in una mVPN non GTM o normale).

I router PE diventano i router di interconnessione tra un protocollo LSM (Label Switched Multicast), mLDP (Core Tree Protocol), P2MP Traffic Engineering, Ingress Replication (IR) e PIM. Quindi, c'è una parte della rete centrale che esegue LSM e noi abbiamo una parte della rete centrale che esegue PIM. Chiamiamo i router principali che agiscono come interfaccia tra la parte LSM della rete e la parte PIM della rete, i router di confine. In alcuni degli esempi seguenti, questi router sono denominati router C-PE (C per Core).

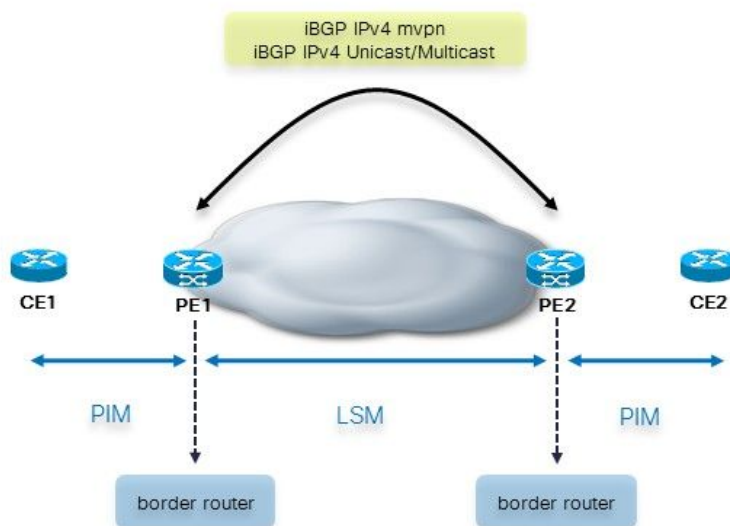
Questi router di confine sono i router con la configurazione necessaria per il GTM. Nessuno degli altri router riconosce il GTM.

La configurazione per GTM è simile a quella richiesta per i normali profili mVPN. Le interfacce verso lo spigolo non sono in un VRF.

Non è disponibile un identificatore di route standard, poiché non sono presenti VRF. Poiché non esistono distintori di route (RD) regolari, ma i RD vengono utilizzati quando si segnala con BGP, i RD di tutti gli zeri e i RD di tutti gli uno vengono utilizzati per la segnalazione in GTM. Per disporre di questa funzionalità, è necessario configurare il comando BGP global-table-multicast.

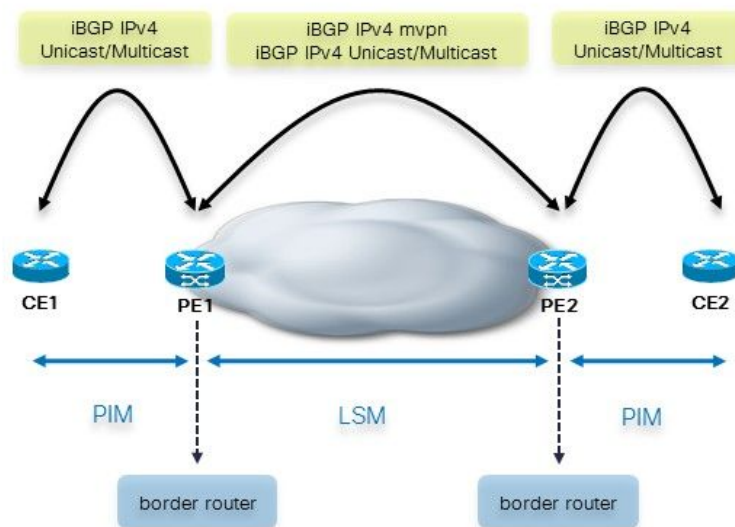
Con GTM, le route unicast non sono in VPNv4/6. Pertanto, la raggiungibilità unicast deve essere fornita in BGP in AF IPv4 o AF IPv6 e SAFI 1 o SAFI 2. Ciò significa che è ancora necessario utilizzare BGP tra i router di confine (router PE senza VRF). Fare riferimento all'immagine 1.

### Immagine 1



Tra il confine e i router CE, non è presente alcun BGP. Il router di confine aggiunge gli attributi multicast quando annuncia le route in iBGP verso gli altri router di confine. È importante notare che potrebbe essere presente BGP tra i router CE e PE. Fare riferimento all'immagine 2.

### Immagine 2



In questo caso, il router PE aggiunge gli attributi multicast quando inoltra le route unicast da eBGP a iBGP, verso gli altri router PE. Se il CE ha annunciato le route unicast con attributi multicast già al router PE, il router PE mantiene gli attributi multicast così come sono e inoltra le route unicast agli altri router PE. Per impostazione predefinita, per le sessioni eBGP, gli attributi multicast vengono rimossi. Pertanto, quando le route PE pubblicizzano le route unicast da iBGP in eBGP alle route CE, non vi sono attributi multicast.

Quando il router PE annuncia il prefisso unicast tramite iBGP, collega la VRF Route Import (VRF-RI) della community estesa (EC) e la Source-AS della CE. L'altro router PE rimuove questi elementi prima di propagare queste route in eBGP.

Quando la sessione eBGP è tra due ASBR, sono presenti una VPN MPLS Inter-AS e una mVPN Inter-AS. In questo caso, è possibile mantenere gli attributi multicast. Poiché il comportamento predefinito prevede la loro rimozione nella sessione eBGP, è necessario configurare il comando `send-multicast-attributes` sulla sessione eBGP tra le due ASBR.

Nei casi in cui si dispone di un RR, può esserci una propagazione da iBGP a iBGP. Questo è il caso della versione inline-ABR (there is next-hop-self) di Seamless MPLS. Poiché il comportamento predefinito prevede di mantenere gli attributi multicast per le sessioni iBGP, per rimuoverli è necessario che il comando inline-ABR disponga del comando `send-multicast-attributes-disable`.

## Modifiche alla configurazione

È necessario configurare `global-table-multicast` nella famiglia di indirizzi (AF) ipv4 mVPN nel router BGP. Ciò consente il funzionamento di tutti gli zero RD e di tutti gli uno RD.

È necessario configurare *import-rt* e *export-rt* in multicast-routing per AF ipv4 nel contesto globale. Questo accade perché non vi sono più RT configurati per i VRF, poiché il GTM non dispone di VRF. Questi RT non devono sovrapporsi ad alcun RT utilizzato per mVPN standard.

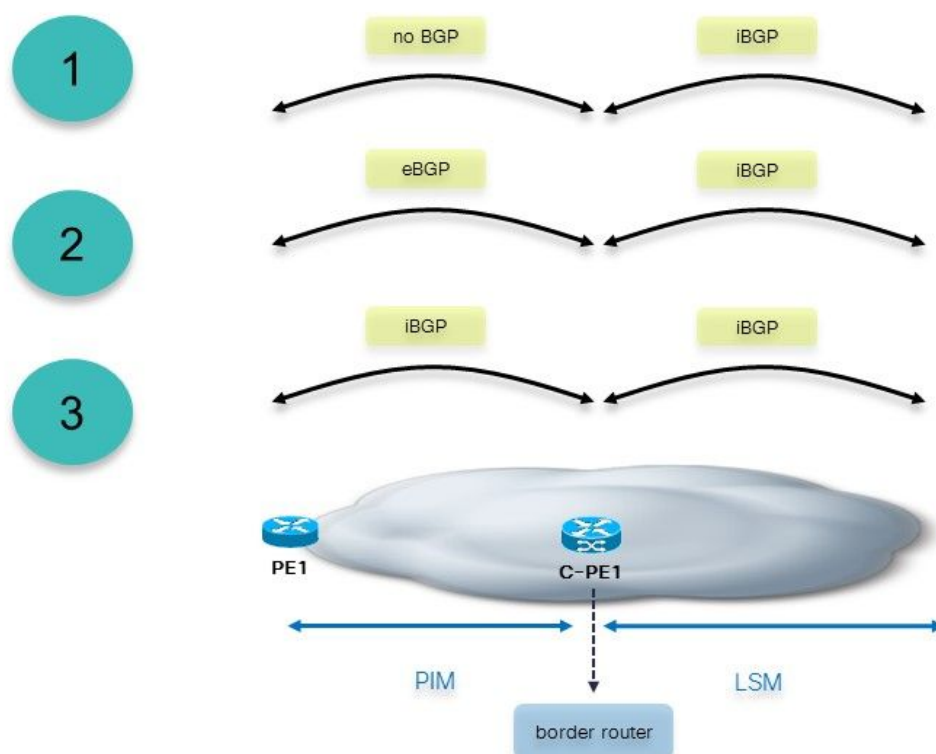
I comandi pim del router (topologia rpf e comandi mdt) sono ora configurati nel contesto globale.

I comandi di routing multicast (rilevamento automatico bgp e comandi mdt) sono ora configurati nel contesto globale.

## Annuncio route

Tra i router di confine c'è un iBGP che annuncia i prefissi di origine. In che modo il router di confine in entrata può imparare il prefisso Source (Origine)? Ci sono tre possibilità.

L'immagine 3 mostra questi tre possibili scenari.



### Immagine 3

1. Il router di confine ha ricevuto i prefissi dal PE come prefissi non BGP. Il router di confine deve ridistribuire questi prefissi in BGP. Questo router di confine aggiunge gli attributi multicast.
2. I router di confine dispongono di una sessione eBGP verso i router PE. Il router di confine aggiunge gli attributi multicast prima di propagare il prefisso su iBGP agli altri router di confine. Se i prefissi ricevuti durante la sessione eBGP hanno già gli attributi multicast, vengono conservati e inoltrati così come sono. Il router di confine non li sovrascrive.
3. Il router di confine in entrata apprende il prefisso Source da iBGP. In questo caso, il router di

confine in entrata è un router di ripristino. Questo scenario viene utilizzato in MPLS Seamless, dove i router di confine sono ABR.

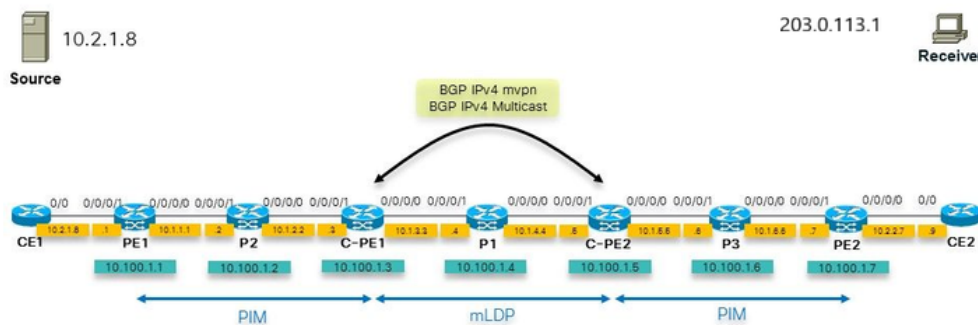
Quando il router di confine annuncia un prefisso iBGP ricevuto da un altro router di confine, rimuove gli attributi multicast prima di inviare il prefisso al router PE. Affinché il comando `send-multicast-attributes` venga disabilitato nel router BGP, i router di confine devono avere il comando `send-multicast-attributes`.

## Esempi

Ecco alcuni esempi. Il primo esempio inizia con la trasformazione del profilo 12 in una distribuzione GTM.

### Esempio 1: profilo 12: MDT - mLDP - P2MP - BGP-AD - BGP C-mcast Signaling

L'immagine 4 mostra questa rete. Non è presente alcun VRF sul router PE verso il router CE.



### Immagine 4

Notare che la rete centrale interna esegue mLDP. La rete core esterna esegue PIM. Quindi, i router di confine, che connettono il PIM al core del mLDP, devono tradurre il PIM in mLDP e viceversa.

Impossibile apprendere l'origine come percorso IGP sul router di confine C-PE2. L'IGP è qui l'ISIS. In questo caso, l'RPF sul router di confine utilizzerebbe il percorso ISIS, che punta a P1. In questo caso, l'RPF fallisce in quanto non esiste un vicinato PIM. Si desidera che il router C-PE2 faccia riferimento a RPF per 10.2.1.8 e che punti a MDT come interfaccia RPF. Potrebbe trattarsi di un MDT basato su mLDP, P2MP o IR.

La soluzione è utilizzare il SAFI 2. Viene utilizzato in modo che l'origine venga appresa come route

SAFI 2 in BGP. Pertanto, il router di confine (C-PE2) dispone dell'origine come route BGP SAFI 2 (show route ipv4 multicast). L'RPF della sorgente punta all'interfaccia MDT.

L'uso di SAFI 2 modifica l'RPF e l'RPF per tutte le fonti ora utilizza SAFI 2. Questo significa che RPF per tutte le origini in globale utilizza SAFI 2, che include RPF per il PE in ingresso, ad esempio, per il servizio VPN. Una volta abilitato il SAFI 2, tutti gli RPF si verificano solo attraverso il SAFI 2. Poiché solo le fonti si trovano in SAFI 2, il RPF per i router PE in entrata non funziona. Per eseguire questa operazione, è possibile configurare il comando **rump always-replicate** in rib router. Poiché solo RPF per i prefissi di origine in globale e RPF per i router PE devono funzionare, è possibile configurare un elenco degli accessi per il comando di replica continua di massa e specificare solo le origini in globale e i router PE in entrata nell'elenco degli accessi. In questo modo, se il router di confine esegue già il BGP per il SAFI 1 e questo SAFI 1 contiene un gran numero di prefissi, questi prefissi non verrebbero ridistribuiti nel SAFI 2 RIB e utilizzerebbero la memoria senza necessità.

In alternativa, è possibile configurare la distanza bgp 20 20 20 per il multicast ipv4 della famiglia di indirizzi con il router BGP. Questo assicura che, se le fonti in globale vengono anche apprese attraverso l'AFI 2 dell'IGP, quelle apprese da BGP sono preferite a causa della distanza inferiore di iBGP rispetto alla distanza dell'IGP.

## Configurazione

Questa è la configurazione del router di confine.

```
hostname C-PE1

router rib
  address-family ipv4
    rump always-replicate
  !
route-policy global-one
  set core-tree mldp-default
end-policy
!
route-policy sources-in-ISIS
  if destination in (10.2.1.0/24) then
    pass
  endif
end-policy

!
router isis 1
  is-type level-1
  net 49.0001.0000.0000.0003.00
  address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-1
  mpls traffic-eng router-id Loopback0
  !
interface Loopback0
  address-family ipv4 unicast
  !
  address-family ipv4 multicast
```



```
!  
!  
interface GigabitEthernet0/0/0/0  
address-family ipv4 unicast  
!  
address-family ipv4 multicast  
!  
!  
interface GigabitEthernet0/0/0/1  
address-family ipv4 unicast  
!  
address-family ipv4 multicast  
!  
!  
!  
router bgp 1  
address-family ipv4 unicast  
!  
address-family ipv4 multicast  
redistribute connected route-policy loopback  
redistribute isis 1 route-policy sources-in-ISIS  
!  
address-family ipv4 mvpn  
global-table-multicast  
!  
neighbor 10.100.1.5  
remote-as 1  
update-source Loopback0  
address-family ipv4 multicast  
next-hop-self  
!  
address-family ipv4 mvpn  
!  
!  
mpls ldp  
mldp  
address-family ipv4  
rib unicast-always  
!  
!  
router-id 10.100.1.3  
address-family ipv4  
!  
interface GigabitEthernet0/0/0/0  
address-family ipv4  
!  
!  
interface GigabitEthernet0/0/0/1  
address-family ipv4  
!  
!  
!  
multicast-routing  
address-family ipv4  
interface Loopback0  
enable  
!  
interface GigabitEthernet0/0/0/1  
enable  
!  
mdt source Loopback0  
export-rt 1:1  
import-rt 1:1  
bgp auto-discovery mldp
```

```

!
mdt default mldp p2mp
mdt data mldp 10 immediate-switch
!
!
router pim
address-family ipv4
rpf topology route-policy global-one
mdt c-multicast-routing bgp
interface Loopback0
    enable
!
interface GigabitEthernet0/0/0/1
!
!
!
!

```

**Nota:** al posto di GTM con mLDP, è possibile eseguire mLDP in banda globale. tra cui l'uso di BGP come protocollo di segnalazione in sovrapposizione o l'uso dell'MDT predefinito per l'aggregazione dei flussi. Con il modello GTM è possibile utilizzare MDT di default e di dati, mentre con mLDP globale in banda è disponibile un flusso multicast per stato mLDP. Inoltre, con GTM, è molto più facile supportare la modalità sparse, mentre con la modalità in banda mLDP, ci sono restrizioni (ad esempio dove viene posizionato l'RP). La modalità sparse è più facile da supportare con PIM come protocollo di segnalazione overlay.

È necessario disporre della configurazione successiva sui router di confine:

- BGP configurato con AF ipv4 mvpn
- BGP AD abilitato
- MDT specificato
- import-rt ed export-rt configurati con il bgp del router
- global-table-multicast configurato sotto il router bgp AF ipv4/6 mvpn

Facoltativamente, il protocollo SAFI 2 deve essere abilitato nel protocollo BGP del router

## Risoluzione dei problemi

- In primo luogo, le route di confine devono avere le route di tipo 1 presenti.
- Verificate l'albero principale nel nucleo interno. Ecco, questo è mLDP. La segnalazione mLDP è corretta? Controllare le voci del database mLDP per individuare gli MDT predefiniti e i possibili MDT dati.
- Controllare la route di origine in BGP.
- Controllare l'RP sul router di confine in uscita.
- Controllare la segnalazione multicast C in BGP (route-type 6 e 7) sui router di confine.

## Router per bordo in entrata

L'interfaccia di uscita sul router di confine in entrata è l'interfaccia Lmdt.

IP Multicast Routing Information Base

Entry flags: L - Domain-Local Source, E - External Source to the Domain,  
C - Directly-Connected Check, S - Signal, IA - Inherit Accept,  
IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,  
MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle  
CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet  
MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary  
MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN

Interface flags: F - Forward, A - Accept, IC - Internal Copy,  
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,  
II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,  
LD - Local Disinterest, DI - Decapsulation Interface  
EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,  
EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,  
MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface  
IRMI - IR MDT Interface

(10.2.1.8,203.0.113.1) RPF nbr: 10.1.2.2 Flags: RPF

Up: 00:08:58

Incoming Interface List

GigabitEthernet0/0/0/1 Flags: A, Up: 00:08:58

Outgoing Interface List

Lmtddefault Flags: F LMI MA, Up: 00:08:58

RP/0/0/CPU0:C-PE1#show mfib route 203.0.113.1 10.2.1.8

IP Multicast Forwarding Information Base

Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,  
IA - Inherit Accept, IF - Inherit From, EID - Encap ID,  
ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,  
MH - MDT interface handle, CD - Conditional Decap,  
DT - MDT Decap True, EX - Extranet, RPFID - RPF ID Set,  
MoFE - MoFRR Enabled, MoFS - MoFRR State, X - VXLAN

Interface flags: F - Forward, A - Accept, IC - Internal Copy,  
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,  
EG - Egress, EI - Encapsulation Interface, MI - MDT Interface,  
EX - Extranet, A2 - Secondary Accept

Forwarding/Replication Counts: Packets in/Packets out/Bytes out

Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other

(10.2.1.8,203.0.113.1), Flags:

Up: 01:47:24

Last Used: 00:00:00

SW Forwarding Counts: 1197/1197/239400

SW Replication Counts: 1197/0/0

SW Failure Counts: 0/0/0/0/0

Lmtddefault Flags: F LMI, Up:01:47:24

GigabitEthernet0/0/0/1 Flags: A, Up:01:47:24

RP/0/0/CPU0:C-PE1#show route ipv4 multicast

Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path  
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 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, su - IS-IS summary null, \* - candidate default  
U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP  
A - access/subscriber, a - Application route  
M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is not set

```

i L1 10.1.1.0/24 [255/20] via 10.1.2.2, 1d21h, GigabitEthernet0/0/0/1
C   10.1.2.0/24 is directly connected, 1d21h, GigabitEthernet0/0/0/1
L   10.1.2.3/32 is directly connected, 3d19h, GigabitEthernet0/0/0/1
i L1 10.1.3.0/24 [115/20] via 10.1.3.4, 3d13h, GigabitEthernet0/0/0/0
L   10.1.3.3/32 is directly connected, 3d19h, GigabitEthernet0/0/0/0
i L1 10.1.4.0/24 [115/20] via 10.1.3.4, 3d13h, GigabitEthernet0/0/0/0
i L1 10.1.5.0/24 [115/30] via 10.1.3.4, 3d12h, GigabitEthernet0/0/0/0
i L1 10.1.6.0/24 [255/40] via 10.1.3.4, 1d21h, GigabitEthernet0/0/0/0
i L1 10.2.1.0/24 [255/30] via 10.1.2.2, 1d21h, GigabitEthernet0/0/0/1
i L1 10.2.2.0/24 [255/50] via 10.1.3.4, 1d21h, GigabitEthernet0/0/0/0
i L1 10.100.1.1/32 [255/30] via 10.1.2.2, 1d21h, GigabitEthernet0/0/0/1
i L1 10.100.1.2/32 [255/20] via 10.1.2.2, 1d21h, GigabitEthernet0/0/0/1
L   10.100.1.3/32 is directly connected, 1d21h, Loopback0
i L1 10.100.1.4/32 [115/20] via 10.1.3.4, 3d13h, GigabitEthernet0/0/0/0
i L1 10.100.1.5/32 [115/30] via 10.1.3.4, 3d12h, GigabitEthernet0/0/0/0
i L1 10.100.1.6/32 [255/40] via 10.1.3.4, 1d21h, GigabitEthernet0/0/0/0
i L1 10.100.1.7/32 [255/50] via 10.1.3.4, 1d21h, GigabitEthernet0/0/0/0

```

```
RP/0/0/CPU0:C-PE1#show pim rpf 10.2.1.8
```

```
Table: IPv4-Multicast-default
```

```
* 10.2.1.8/32 [255/30]
  via GigabitEthernet0/0/0/1 with rpf neighbor 10.1.2.2
```

## Router del bordo in uscita

Per il percorso di origine, le voci VRF Route-Import EC e Source-AS EC sono collegate al prefisso unicast o multicast IPv4. In questo caso, si tratta di una route multicast IPv4:

```

RP/0/0/CPU0:C-PE2#show bgp ipv4 multicast 10.2.1.0/24
BGP routing table entry for 10.2.1.0/24
Versions:
  Process          bRIB/RIB  SendTblVer
  Speaker          32        32
Last Modified: Sep 12 08:34:56.441 for 15:09:58
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
Local
  10.100.1.3 (metric 30) from 10.100.1.3 (10.100.1.3)
  Origin incomplete, metric 30, localpref 100, valid, internal, best, group-best
  Received Path ID 0, Local Path ID 1, version 32
  Extended community: VRF Route Import:10.100.1.3:0 Source AS:1:0

```

**Nota:** se per qualche motivo il VRF RI EC e la Source AS EC non si trovano, il RPF sul router di confine in uscita non funziona.

## Esempio di percorso privo dei seguenti EC:

```

RP/0/0/CPU0:C-PE2#show bgp ipv4 multicast 10.2.1.0/24
BGP routing table entry for 10.2.1.0/24
Versions:
  Process          bRIB/RIB  SendTblVer

```

```
Speaker                277          277
Last Modified: Sep 13 04:08:37.441 for 00:00:02
Paths: (1 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
  10.100.1.3 (metric 30) from 10.100.1.3 (10.100.1.1)
    Origin incomplete, metric 0, localpref 100, valid, internal, best, group-best
    Received Path ID 0, Local Path ID 1, version 277
    Originator: 10.100.1.1, Cluster list: 10.100.1.3
```

**Per questo motivo, l'RPF fallisce:**

```
RP/0/0/CPU0:C-PE2#show pim rpf 10.2.1.8
```

```
Table: IPv4-Multicast-default
* 10.2.1.8/32 [200/30]
  via Null with rpf neighbor 0.0.0.0
```

```
RP/0/0/CPU0:C-PE2#show bgp ipv4 mvpn
```

```
BGP router identifier 10.100.1.5, local AS number 1
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 56
BGP NSR Initial initsync version 4 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
Global table multicast is enabled
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 0:0:0					
*>i[1][10.100.1.3]/40	10.100.1.3		100	0	i
*> [1][10.100.1.5]/40	0.0.0.0			0	i
*>i[3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120	10.100.1.3		100	0	i
*> [7][0:0:0][1][32][10.2.1.8][32][203.0.113.1]/184	0.0.0.0			0	i

```
Processed 4 prefixes, 4 paths
```

**Il comando può essere specificato con le parole chiave rd all-zero-rd. Vengono quindi visualizzate tutte le voci con il RD composto da tutti gli zeri.**

```
RP/0/0/CPU0:C-PE2#show bgp ipv4 mvpn rd all-zero-rd
```

```
BGP router identifier 10.100.1.5, local AS number 1
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 56
BGP NSR Initial initsync version 4 (Reached)
```

```
BGP NSR/ISSU Sync-Group versions 0/0
Global table multicast is enabled
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
               i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 0:0:0					
*>i[1][10.100.1.3]/40	10.100.1.3			100	0 i
*> [1][10.100.1.5]/40	0.0.0.0				0 i
*>i[3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120					
	10.100.1.3			100	0 i
*> [7][0:0:0][1][32][10.2.1.8][32][203.0.113.1]/184					
	0.0.0.0				0 i

```
Processed 4 prefixes, 4 paths
```

## Il percorso di tipo 1:

```
RP/0/0/CPU0:C-PE2#show bgp ipv4 mvpn rd all-zero-rd [1][10.100.1.3]/40
```

```
BGP routing table entry for [1][10.100.1.3]/40, Route Distinguisher: 0:0:0
```

```
Versions:
```

Process	bRIB/RIB	SendTblVer
Speaker	43	43

```
Last Modified: Sep  8 07:42:43.786 for 1d17h
```

```
Paths: (1 available, best #1, not advertised to EBGp peer)
```

```
Not advertised to any peer
```

```
Path #1: Received by speaker 0
```

```
Not advertised to any peer
```

```
Local
```

```
10.100.1.3 (metric 30) from 10.100.1.3 (10.100.1.3)
```

```
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
```

```
Received Path ID 0, Local Path ID 1, version 43
```

```
Community: no-export
```

```
Extended community: RT:1:1
```

```
PMSI: flags 0x00, type 2, label 0, ID 0x060001040a640103000701000400000001
```

```
Source AFI: IPv4 MVPN, Source VRF: default, Source Route Distinguisher: 0:0:0
```

## PMSI decodificato:

```
PMSI: flag 0x00, tipo 2, etichetta 0, ID 0x060001040a640103000701000400000001
```

## Il PMSI decodificato dal comando precedente è:

```
The PMSI Tunnel Type is : 2 : mLDP P2MP LSP The PMSI Tunnel ID is : 0x060001040a640103000701000400000001 FEC
Element FEC Element Type : 6 : P2MP AF Type : 1 Address Length : 4 Root Node Address : 10.100.1.3 MP Opaque Length : 7
MP Opaque Value Element Opaque Type : 1 : LSP ID Global Opaque Length : 4 Global ID (Generic LSP Identifier) : 1
```

L'MDT dei dati è segnalato da una route AD di tipo route 3 da C-PE1.

```
RP/0/0/CPU0:C-PE2#show bgp ipv4 mvpn rd all-zero-rd [3][32][10.2.1.8]
[32][203.0.113.1][10.100.1.3]/120
```

```
BGP routing table entry for [3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120, Route
```

```

Distinguisher: 0:0:0
Versions:
  Process          bRIB/RIB  SendTblVer
  Speaker          56        56
Last Modified: Sep 10 00:51:52.786 for 00:04:57
Paths: (1 available, best #1, not advertised to EBGp peer)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
Local
  10.100.1.3 (metric 30) from 10.100.1.3 (10.100.1.3)
  Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
  Received Path ID 0, Local Path ID 1, version 56
  Community: no-export
  Extended community: RT:1:1
  PMSI: flags 0x00, type 2, label 0, ID 0x060001040a640103000701000400000007
  Source AFI: IPv4 MVPN, Source VRF: default, Source Route Distinguisher: 0:0:0

```

Il PMSI decodificato indica che l'identificatore LSP globale è 7. Viene quindi utilizzato per la voce del database mLDP per questo Data MDT.

PMSI: flag 0x00, tipo 2, etichetta 0, ID 0x060001040a640103000701000400000007

Il PMSI decodificato dal comando precedente è:

```

The PMSI Tunnel Type is : 2 : mLDP P2MP LSP The PMSI Tunnel ID is : 0x060001040a640103000701000400000007 FEC
Element FEC Element Type : 6 : P2MP AF Type : 1 Address Length : 4 Root Node Address : 10.100.1.3 MP Opaque Length : 7
MP Opaque Value Element Opaque Type : 1 : LSP ID Global Opaque Length : 4 Global ID (Generic LSP Identifier) : 7

```

Con i comandi successivi, è possibile controllare gli annunci in ingresso di PE relativi all'MDT dati. Notare che questo è GTM, quindi non c'è VRF nel comando successivo.

```

RP/0/0/CPU0:C-PE2#show pim mdt mldp remote
Core          MDT          Cache Max DIP Local VRF Routes
Identifier    Source          Count Agg      Entry Using Cache
[global-id 7] 10.100.1.3     1      255 N      N      1

RP/0/0/CPU0:C-PE2#show pim mdt mldp cache

Core Source   Cust (Source, Group)          Core Data          Expires
10.100.1.3    (10.2.1.8, 203.0.113.1)      [global-id 7]     never

```

Il tipo di route 7 non dispone di un PMSI collegato:

```

RP/0/0/CPU0:C-PE2#show bgp ipv4 mvpn rd all-zero-rd
[7][0:0:0][1][32][10.2.1.8][32][203.0.113.1]/184

BGP routing table entry for [7][0:0:0][1][32][10.2.1.8][32][203.0.113.1]/184, Route
Distinguisher: 0:0:0
Versions:
  Process          bRIB/RIB  SendTblVer
  Speaker          52        52
Last Modified: Sep 10 00:51:51.786 for 00:07:37

```

```
Paths: (1 available, best #1)
Advertised to peers (in unique update groups):
 10.100.1.3
Path #1: Received by speaker 0
Advertised to peers (in unique update groups):
 10.100.1.3
Local
 0.0.0.0 from 0.0.0.0 (10.100.1.5)
  Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate
  Received Path ID 0, Local Path ID 1, version 52
  Extended community: RT:10.100.1.3:0
```

RT identifica il router PE upstream. Il campo Amministratore globale corrisponde all'indirizzo IP del file PE a monte. Il campo dell'amministratore locale è impostato su 0 per GTM.

```
RP/0/0/CPU0:C-PE2#show mrib route 203.0.113.1 10.2.1.8
```

```
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
  IRMI - IR MDT Interface
```

```
(10.2.1.8,203.0.113.1) RPF nbr: 10.100.1.3 Flags: RPF
Up: 00:52:34
Incoming Interface List
  Lmdtdefault Flags: A LMI, Up: 00:52:34
Outgoing Interface List
  GigabitEthernet0/0/0/0 Flags: F NS, Up: 00:52:34
```

L'interfaccia in ingresso deve essere un'interfaccia Lmdt.

```
RP/0/0/CPU0:C-PE2#show mrib route 203.0.113.1 10.2.1.8
```

```
IP Multicast Forwarding Information Base
Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
  IA - Inherit Accept, IF - Inherit From, EID - Encap ID,
  ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
  MH - MDT interface handle, CD - Conditional Decap,
  DT - MDT Decap True, EX - Extranet, RPFID - RPF ID Set,
  MoFE - MoFRR Enabled, MoFS - MoFRR State, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  EG - Egress, EI - Encapsulation Interface, MI - MDT Interface,
  EX - Extranet, A2 - Secondary Accept
Forwarding/Replication Counts: Packets in/Packets out/Bytes out
Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other
```



```
(10.2.1.8,203.0.113.1),  Flags:
Up: 02:31:00
Last Used: never
SW Forwarding Counts: 0/2037/407400
SW Replication Counts: 0/2037/407400
SW Failure Counts: 0/0/0/0/0
Lmdtdefault Flags:  A LMI, Up:02:31:00
GigabitEthernet0/0/0/0 Flags:  NS EG, Up:02:31:00
```

## Controllare le rotte SAFI 2:

```
RP/0/0/CPU0:C-PE2#show route ipv4 multicast
```

```
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
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 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
A - access/subscriber, a - Application route
M - mobile route, r - RPL, (!) - FRR Backup path
```

```
Gateway of last resort is not set
```

```
i L1 10.1.2.0/24 [115/30] via 10.1.4.4, 3d12h, GigabitEthernet0/0/0/1
i L1 10.1.3.0/24 [115/20] via 10.1.4.4, 3d12h, GigabitEthernet0/0/0/1
C 10.1.4.0/24 is directly connected, 1d21h, GigabitEthernet0/0/0/1
L 10.1.4.5/32 is directly connected, 3d12h, GigabitEthernet0/0/0/1
C 10.1.5.0/24 is directly connected, 1d21h, GigabitEthernet0/0/0/0
L 10.1.5.5/32 is directly connected, 3d12h, GigabitEthernet0/0/0/0
B 10.2.1.0/24 [200/30] via 10.100.1.3, 1d17h
i L1 10.100.1.3/32 [115/30] via 10.1.4.4, 3d12h, GigabitEthernet0/0/0/1
i L1 10.100.1.4/32 [115/20] via 10.1.4.4, 3d12h, GigabitEthernet0/0/0/1
L 10.100.1.5/32 is directly connected, 1d21h, Loopback0
```

Notare che il percorso per l'origine è SAFI 2 (si trova nel multicast IPv4 AF), in quanto si trova nel multicast IPv4 RIB AF.

Notare che l'hop successivo è 10.100.1.3, il loopback di C-PE1, in quanto il router ha il self-hop successivo sotto il multicast AF ipv4 sotto il router BGP.

```
RP/0/0/CPU0:C-PE2#show bgp ipv4 multicast 10.2.1.0/24
```

```
BGP routing table entry for 10.2.1.0/24
```

```
Versions:
```

```
Process          bRIB/RIB  SendTblVer
Speaker          34        34
```

```
Last Modified: Sep  8 07:42:18.786 for 1d17h
```

```
Paths: (1 available, best #1)
```

```
Not advertised to any peer
```

```
Path #1: Received by speaker 0
```

```
Not advertised to any peer
```

```
Local
```

```
10.100.1.3 (metric 30) from 10.100.1.3 (10.100.1.3)
```

```
Origin incomplete, metric 30, localpref 100, valid, internal, best, group-best
```

Received Path ID 0, Local Path ID 1, version 34  
Extended community: VRF Route Import:10.100.1.3:0 Source AS:1:0

L'RPf per l'origine punta all'interfaccia Lmdt e al router adiacente PIM attraverso di essa. L'RPf viene eseguito nella tabella Multicast IPv4.

```
RP/0/0/CPU0:C-PE2#show pim rpf 10.2.1.8
```

```
Table: IPv4-Multicast-default  
* 10.2.1.8/32 [200/30]  
  via Lmdtdefault with rpf neighbor 10.100.1.3
```

Verificare che il router di confine in entrata sia riconosciuto come router PE.

```
RP/0/0/CPU0:C-PE2#show pim pe
```

MVPN Provider Edge Router information

```
PE Address : 10.100.1.3 (0x1071da64)  
RD: 0:0:0 (valid), RIB_HLI 0, RPF-ID 3, Remote RPF-ID 0, State: 1, S-PMSI: 2  
PPMP_LABEL: 0, MS_PMSI_HLI: 0x00000, Bidir_PMSI_HLI: 0x00000, MLDP-added: [RD 0, ID 0, Bidir ID  
0, Remote Bidir ID 0], Counts(SHR/SRC/DM/DEF-MD): 0, 1, 0, 0, Bidir: GRE RP Count 0, MPLS RP  
Count 0RSVP-TE added: [Leg 0, Ctrl Leg 0, Part tail 0 Def Tail 0, IR added: [Def Leg 0, Ctrl Leg  
0, Part Leg 0, Part tail 0, Part IR Tail Label 0  
bgp_i_pmsi: 1,0/0 , bgp_ms_pmsi/Leaf-ad: 0/0, bgp_bidir_pmsi: 0, remote_bgp_bidir_pmsi: 0,  
PMSIs: I 0x106a2d50, 0x0, MS 0x0, Bidir Local: 0x0, Remote: 0x0, BSR/Leaf-ad 0x0/0, Autorp-  
disc/Leaf-ad 0x0/0, Autorp-ann/Leaf-ad 0x0/0  
IIDs: I/6: 0x1/0x0, B/R: 0x0/0x0, MS: 0x0, B/A/A: 0x0/0x0/0x0
```

```
Bidir RPF-ID: 4, Remote Bidir RPF-ID: 0  
I-PMSI: MLDP-P2MP, Opaque: [global-id 1] (0x106a2d50)  
I-PMSI rem: (0x0)  
MS-PMSI: (0x0)  
Bidir-PMSI: (0x0)  
Remote Bidir-PMSI: (0x0)  
BSR-PMSI: (0x0)  
A-Disc-PMSI: (0x0)  
A-Ann-PMSI: (0x0)  
RIB Dependency List: 0x1016446c  
Bidir RIB Dependency List: 0x0  
Sources: 1, RPs: 0, Bidir RPs: 0
```

Il PMSI inclusivo (I-PMSI) è presente.

Vengono visualizzate le due voci P2MP mLDP che formano l'MDT predefinito tra i due router di confine nel database mLDP. Esiste anche una voce P2MP mLDP con C-PE1 come root per Data MDT.

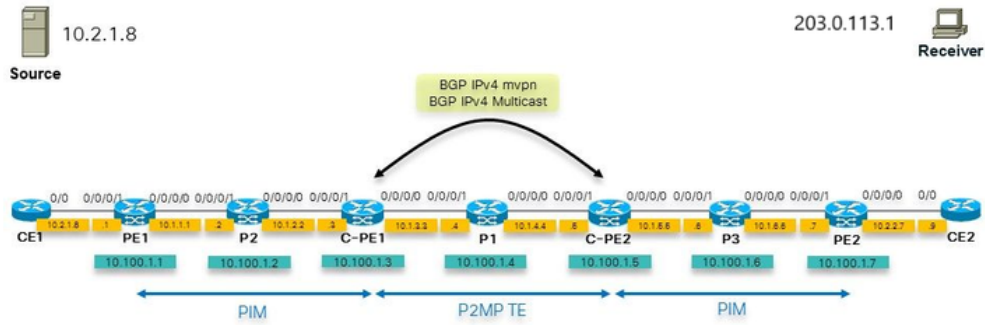
```
RP/0/0/CPU0:C-PE2#show mpls mldp database brief
```

LSM ID	Type	Root	Up	Down	Decoded	Opaque	Value
0x00007	P2MP	10.100.1.3	1	1	[global-id 1]		
0x00008	P2MP	10.100.1.5	0	2	[global-id 1]		
0x0000B	P2MP	10.100.1.3	1	1	[global-id 7]		

**Esempio 2: Profilo 20 MDT predefinito - P2MP-TE - BGP-AD - PIM - Segnalazione**

# C-mcast

Questo è molto simile all'esempio 1. Ora c'è P2MP TE nel nucleo. I tunnel sono impostati come tunnel automatici. I router di coda vengono rilevati tramite BGP AD. Un'altra differenza con l'esempio 1 è che il protocollo di sovrapposizione è ora PIM. Osservare l'immagine 5.



## Immagine 5

## Configurazione

Questa è la configurazione del router di confine:

```
hostname C-PE1
logging console debugging
router rib
  address-family ipv4
  rump always-replicate
  !
  !
line default
  timestamp disable
  exec-timeout 0 0
  !
ipv4 unnumbered mpls traffic-eng Loopback0
interface Loopback0
  ipv4 address 10.100.1.3 255.255.255.255
  !
interface MgmtEth0/0/CPU0/0
  shutdown
  !
interface GigabitEthernet0/0/0/0
  ipv4 address 10.1.3.3 255.255.255.0
  load-interval 30
  !
```

```
interface GigabitEthernet0/0/0/1
  ipv4 address 10.1.2.3 255.255.255.0
!
interface GigabitEthernet0/0/0/2
  shutdown
!
interface GigabitEthernet0/0/0/3
  shutdown
!
interface GigabitEthernet0/0/0/4
  shutdown
!
interface GigabitEthernet0/0/0/5
  shutdown
!
interface GigabitEthernet0/0/0/6
  shutdown
!
interface GigabitEthernet0/0/0/7
  shutdown
!
interface GigabitEthernet0/0/0/8
  shutdown
!
route-policy loopback
  if destination in (10.100.1.3/32) then
    pass
  endif
end-policy
!
route-policy global-one
  set core-tree p2mp-te-default
end-policy
!
route-policy sources-in-ISIS
  if destination in (10.2.1.0/24) then
    pass
  endif
end-policy
!
router isis 1
  is-type level-1
  net 49.0001.0000.0000.0003.00
  address-family ipv4 unicast
metric-style wide
  mpls traffic-eng level-1
  mpls traffic-eng router-id Loopback0
!
interface Loopback0
  address-family ipv4 unicast
!
address-family ipv4 multicast
!
!
interface GigabitEthernet0/0/0/0
  address-family ipv4 unicast
!
address-family ipv4 multicast
!
!
interface GigabitEthernet0/0/0/1
  address-family ipv4 unicast
!
address-family ipv4 multicast
```

```
!  
!  
!  
router bgp 1  
  address-family ipv4 unicast  
  !  
  address-family ipv4 multicast  
  redistribute connected route-policy loopback  
  redistribute ospf 1  
  redistribute isis 1 route-policy sources-in-ISIS  
  !  
  address-family ipv4 mvpn  
global-table-multicast  
  !  
  neighbor 10.100.1.5  
  remote-as 1  
  update-source Loopback0  
  address-family ipv4 multicast  
    next-hop-self  
  !  
  address-family ipv4 mvpn  
  !  
  !  
!  
mpls oam  
!  
rsvp  
  interface GigabitEthernet0/0/0/0  
  bandwidth 1000000  
  !  
  interface GigabitEthernet0/0/0/1  
  bandwidth 1000000  
  !  
!  
mpls traffic-eng  
  interface GigabitEthernet0/0/0/0  
  auto-tunnel backup  
  !  
  !  
  interface GigabitEthernet0/0/0/1  
  auto-tunnel backup  
  !  
  !  
  auto-tunnel p2mp  
  tunnel-id min 1000 max 2000  
  !  
!  
mpls ldp  
  log  
  neighbor  
  !  
  mldp  
  logging notifications  
  address-family ipv4  
    rib unicast-always  
  !  
  !  
  router-id 10.100.1.3  
  address-family ipv4  
  !  
  interface GigabitEthernet0/0/0/0  
  address-family ipv4  
  !  
  !
```

```

interface GigabitEthernet0/0/0/1
address-family ipv4
!
!
!
multicast-routing
address-family ipv4
interface Loopback0
enable
!
interface GigabitEthernet0/0/0/1
enable
!
mdt source Loopback0
export-rt 1:1
import-rt 1:1
bgp auto-discovery p2mp-te
!
mdt default p2mp-te
mdt data p2mp-te 100 immediate-switch
!
!
router pim
address-family ipv4
rpf topology route-policy global-one
interface Loopback0
enable
!
interface GigabitEthernet0/0/0/1
!
!
!

```

## Risoluzione dei problemi

### Router per bordo in entrata

Verificare che il RD all-zero sia presente. Le route di tipo 1 devono essere presenti per poter costruire il TE P2MP basato sui tunnel TE P2MP.

```

RP/0/0/CPU0:C-PE1#show bgp ipv4 mvpn rd all-zero-rd
BGP router identifier 10.100.1.3, local AS number 1
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0 RD version: 0
BGP main routing table version 140
BGP NSR Initial initsync version 4 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
Global table multicast is enabled
BGP scan interval 60 secs

```

```

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 0:0:0					
*> [1][10.100.1.3]/40	0.0.0.0			0	i
*>i[1][10.100.1.5]/40	10.100.1.5	100		0	i

Processed 2 prefixes, 2 paths

## Verificare più dettagliatamente il ciclo di lavorazione di tipo 1:

```
RP/0/0/CPU0:C-PE1#show bgp ipv4 mvpn rd all-zero-rd [1][10.100.1.5]/40
```

BGP routing table entry for [1][10.100.1.5]/40, Route Distinguisher: 0:0:0

Versions:

```
Process          bRIB/RIB  SendTblVer
Speaker          135      135
```

Last Modified: Sep 12 08:21:42.207 for 00:20:14

Paths: (1 available, best #1, not advertised to EBGp peer)

Not advertised to any peer

Path #1: Received by speaker 0

Not advertised to any peer

Local

10.100.1.5 (metric 30) from 10.100.1.5 (10.100.1.5)

Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported

Received Path ID 0, Local Path ID 1, version 135

Community: no-export

Extended community: RT:1:1

PMSI: flags 0x00, type 1, label 0, ID 0x000003e8000003e80a640105

Source AFI: IPv4 MVPN, Source VRF: default, Source Route Distinguisher: 0:0:0

## Controllare i vicini PIM sul valore predefinito MDT:

```
RP/0/0/CPU0:C-PE1#show pim neighbor
```

PIM neighbors in VRF default

Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,

E - ECMP Redirect capable

\* indicates the neighbor created for this router

Neighbor Address	Interface	Uptime	Expires	DR pri	Flags
10.1.2.2	GigabitEthernet0/0/0/1	6d02h	00:01:16	1	B
10.1.2.3*	GigabitEthernet0/0/0/1	6d02h	00:01:15	1 (DR)	B E
10.100.1.3*	Loopback0	6d02h	00:01:32	1 (DR)	B E
10.100.1.3*	Tmtdtdefault	00:36:21	00:01:40	1	
10.100.1.5	Tmtdtdefault	00:17:37	00:01:26	1 (DR)	

## Controllare il percorso MRIB. L'interfaccia in uscita deve essere Tmtd:

```
RP/0/0/CPU0:C-PE1#show mrib route 203.0.113.1
```

IP Multicast Routing Information Base

Entry flags: L - Domain-Local Source, E - External Source to the Domain,

C - Directly-Connected Check, S - Signal, IA - Inherit Accept,

IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,

MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle

CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet

MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary

MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN

Interface flags: F - Forward, A - Accept, IC - Internal Copy,

NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,

II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,

LD - Local Disinterest, DI - Decapsulation Interface  
 EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,  
 EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,  
 MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface  
 IRMI - IR MDT Interface

```
(10.2.1.8,203.0.113.1) RPF nbr: 10.1.2.2 Flags: RPF
Up: 00:09:10
Incoming Interface List
  GigabitEthernet0/0/0/1 Flags: A, Up: 00:09:10
Outgoing Interface List
  Tmtddefault Flags: F NS TMI, Up: 00:09:10
```

Verificare che esista un tunnel P2MP TE per router di confine come router headend:

```
RP/0/0/CPU0:C-PE1#show mpls traffic-eng tunnels tabular
```

Tunnel Name	LSP ID	Destination Address	Source Address	State	FRR State	LSP Role	Path Prot
^tunnel-mte1001	10004	10.100.1.5	10.100.1.3	up	Inact	Head	
auto_C-PE2_mt1000	10005	10.100.1.3	10.100.1.5	up	Inact	Tail	

^ = automatically created P2MP tunnel

Una volta attivato Data MDT, vengono utilizzate le route di tipo 3 e 4:

```
RP/0/0/CPU0:C-PE1#show bgp ipv4 mvpn rd all-zero-rd
```

```
BGP router identifier 10.100.1.3, local AS number 1
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0 RD version: 0
BGP main routing table version 143
BGP NSR Initial initsync version 4 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
Global table multicast is enabled
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> [1][10.100.1.3]/40	0.0.0.0			0	i
*>i[1][10.100.1.5]/40	10.100.1.5	100		0	i
*> [3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120	0.0.0.0			0	i
*>i[4][3][0:0:0][32][10.2.1.8][32][203.0.113.1][10.100.1.3][10.100.1.5]/224	10.100.1.5	100		0	i

```
Processed 4 prefixes, 4 paths
```

Il tipo di percorso 3 annuncia a tutti i router di coda che è segnalato un MDT dati:

```
RP/0/0/CPU0:C-PE1#show bgp ipv4 mvpn rd all-zero-rd
```



```
[3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120
```

BGP routing table entry for [3][32][10.2.1.8][32][203.0.113.1][10.100.1.3]/120, Route Distinguisher: 0:0:0

Versions:

```
Process          bRIB/RIB  SendTblVer
Speaker          141      141
```

Last Modified: Sep 12 08:46:17.207 for 00:00:41

Paths: (1 available, best #1, not advertised to EBGp peer)

Advertised to peers (in unique update groups):

```
10.100.1.5
```

Path #1: Received by speaker 0

Advertised to peers (in unique update groups):

```
10.100.1.5
```

Local

```
0.0.0.0 from 0.0.0.0 (10.100.1.3)
```

Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate

Received Path ID 0, Local Path ID 1, version 141

Community: no-export

Extended community: RT:1:1

PMSI: flags 0x01, type 1, label 0, ID 0x000003ed000003ed0a640103

**PMSI decodificato:**

**PMSI: flag 0x01, tipo 1, etichetta 0, ID 0x000003ed000003ed0a640103**

**Il PMSI decodificato dal comando precedente è:**

The PMSI Tunnel Type is : 1 : RSVP-TE P2MP LSP The PMSI Tunnel ID is : 0x000003ed000003ed0a640103 Extended Tunnel ID : 1005 Reserved part (should be zero): 0X0000 Tunnel ID : 1005 P2MP ID : 10.100.1.3

**Questa condizione può essere rilevata anche qui:**

```
RP/0/0/CPU0:C-PE1#show pim mdt cache
```

Core Source	Cust (Source, Group)	Core Data	Expires
10.100.1.3	(10.2.1.8, 203.0.113.1)	[p2mp 6]	never

```
Leaf AD: 10.100.1.5
```

**Il tipo di routing 4 annuncia al router headend quale router è il terminale di coda:**

```
RP/0/0/CPU0:C-PE1#show bgp ipv4 mvpn rd all-zero-rd
[4][3][0:0:0][32][10.2.1.8][32][203.0.113.1][10.100.1.3][10.100.1.5]/224
```

BGP routing table entry for

[4][3][0:0:0][32][10.2.1.8][32][203.0.113.1][10.100.1.3][10.100.1.5]/224, Route Distinguisher: 0:0:0

Versions:

```
Process          bRIB/RIB  SendTblVer
Speaker          143      143
```

Last Modified: Sep 12 08:46:17.207 for 00:01:25

Paths: (1 available, best #1)

Not advertised to any peer

Path #1: Received by speaker 0

Not advertised to any peer

Local

10.100.1.5 (metric 30) from 10.100.1.5 (10.100.1.5)

Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported

Received Path ID 0, Local Path ID 1, version 143

Extended community: SEG-NH:10.100.1.5:0 RT:10.100.1.3:0

Source AFI: IPv4 MVPN, Source VRF: default, Source Route Distinguisher: 0:0:0

Verificare che Data MDT nel tunnel P2MP TE sia configurato:

```
RP/0/0/CPU0:C-PE1#show mpls traffic-eng tunnels tabular
```

Tunnel Name	LSP ID	Destination Address	Source Address	State	FRR State	LSP Role	Path Prot
^tunnel-mtel1001	10004	10.100.1.5	10.100.1.3	up	Inact	Head	
^tunnel-mtel1005	10002	10.100.1.5	10.100.1.3	up	Inact	Head	
auto_C-PE2_mt1000	10005	10.100.1.3	10.100.1.5	up	Inact	Tail	

^ = automatically created P2MP tunnel

## Router del bordo in uscita

Verificare che l'interfaccia in ingresso sia l'interfaccia Tmdt:

```
RP/0/0/CPU0:C-PE2#show mrib route 203.0.113.1
```

IP Multicast Routing Information Base

Entry flags: L - Domain-Local Source, E - External Source to the Domain,

C - Directly-Connected Check, S - Signal, IA - Inherit Accept,

IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,

MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle

CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet

MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary

MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN

Interface flags: F - Forward, A - Accept, IC - Internal Copy,

NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,

II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,

LD - Local Disinterest, DI - Decapsulation Interface

EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,

EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,

MA - Data MDT Assigned, LMI - mLDP MDT Interface, **TMI - P2MP-TE MDT Interface**

IRMI - IR MDT Interface

```
(10.2.1.8,203.0.113.1) RPF nbr: 10.100.1.3 Flags: RPF
```

```
Up: 00:18:03
```

```
Incoming Interface List
```

```
Tmdtdefault Flags: A TMI, Up: 00:18:00
```

```
Outgoing Interface List
```

```
GigabitEthernet0/0/0/0 Flags: F NS, Up: 00:18:03
```

L'RPF sul router di confine in uscita punta al router di confine in entrata. L'interfaccia in entrata è Tmdtdefault. Notare la T per il tunnel TE:

```
RP/0/0/CPU0:C-PE2#show pim rpf 10.2.1.8
```

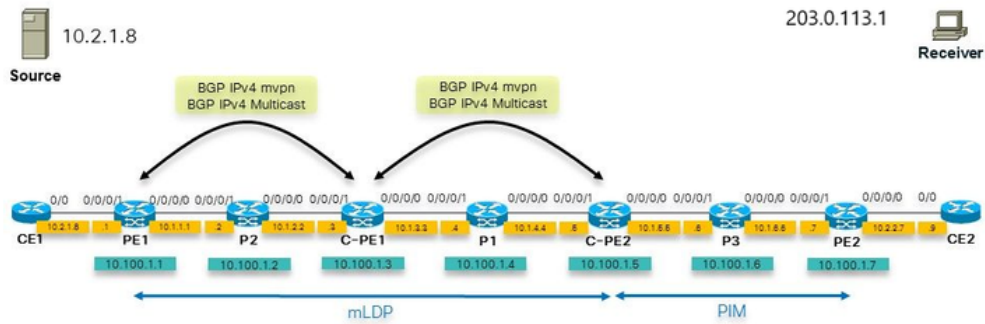
Table: IPv4-Multicast-default

\* 10.2.1.8/32 [200/30]

via Tmtddefault with rpf neighbor 10.100.1.3

### Esempio 3: come nell'esempio 1, ma tra PE e Border Router è presente iBGP

Guardate l'immagine 6.



### Immagine 6

Vediamo una configurazione asimmetrica in cui abbiamo una rete core con mLDP su un lato e PIM ancora sull'altro lato e GTM. Ciò può verificarsi durante la migrazione degli alberi del nucleo. Il router C-PE1 deve essere un router RR per BGP IPv4 multicast e BGP IPv4 mVPN. La configurazione per PIM e multicast-routing disponibile su C-PE1 nell'esempio 1 è ora necessaria su PE1.

### Esempio 4: MPLS perfetto

Il protocollo GTM viene implementato su MPLS (Unified MPLS). Il router PE deve riconoscere il GTM, operazione che può essere eseguita solo da un router Cisco IOS XR, mentre il router PE deve generare il vettore PIM RPF-Proxy nel dominio PIM. Questo vettore PIM RPF-Proxy è necessario affinché i router IP possano eseguire RPF sull'indirizzo IP proxy (ABR). Da Cisco IOS XR 5.3.2, Cisco IOS XR può originare il vettore RPF-Proxy in un contesto globale. GTM può avere il vettore RPF-Proxy.

Per creare il vettore PIM RPF-Proxy, il router PE deve avere la seguente configurazione:

```
router pim
address-family [ipv4|ipv6]
rpf-vector
```

!  
!

**Nota:** il supporto per l'interpretazione del vettore PIM RPF-Proxy (è ciò che deve fare il router IP) è stato introdotto nelle versioni precedenti di Cisco IOS XR.

Ciò consente l'implementazione di GTM su MPLS perfetto.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).