

MULTIDIFFUSION nouvelle génération - GRE MDT par défaut (BGP AD - PIM C : Profil 3)

Contenu

[Introduction](#)

[Qu'est-ce que le MDT par défaut ?](#)

[Qu'est-ce que Data MDT ?](#)

[BGP](#)

[Adressage multidiffusion pour le groupe SSM](#)

[Recommandations](#)

[Signalisation de superposition](#)

[Topologie](#)

[Routage et transfert VPN multidiffusion et domaines multidiffusion](#)

[Tâches de configuration](#)

[Vérification](#)

[Tâche 1 : vérification de la connectivité physique](#)

[Tâche 2 : Vérifiez la monodiffusion VPNv4 de la famille d'adresses BGP.](#)

[Tâche 3 : Vérifiez la monodiffusion MVPN de la famille d'adresses BGP.](#)

[Tâche 4 : Vérifier le trafic multidiffusion de bout en bout](#)

[Comment les interfaces de tunnel sont créées ?](#)

[Création du tunnel MDT](#)

[Voisinage PIM](#)

[Informations connexes](#)

Introduction

Ce document décrit le protocole GRE (MDT) GRE (BGP AD - PIM C) pour Multicast over VPN (mVPN). Il utilise un exemple et la mise en oeuvre dans Cisco IOS afin d'illustrer le comportement.

Qu'est-ce que le MDT par défaut ?

Il est utilisé pour connecter la multidiffusion à tous les PE dans un VRF. Par défaut, il connecte tous les routeurs PE. Par défaut, il transporte tout le trafic. Tout le trafic de contrôle PIM et le trafic du plan de données. Exemple : (*, G) Trafic et (S, G) Trafic. La valeur par défaut est le must. Ce MDT par défaut connecte tous les routeurs PE à connecter. Cela représente multipoint à multipoint. N'importe qui peut envoyer et tout le monde peut recevoir de l'arbre.

Qu'est-ce que Data MDT ?

Elle est facultative et est créée à la demande. Il transporte un trafic spécifique (S, G). Dans la dernière version d'IOS, le seuil est configuré comme 0 et infini. À chaque fois qu'un premier paquet atteint le VRF, le MDT de données est initialisé et, si infini, le MDT de données n'est jamais créé, et le trafic se déplace vers l'avant dans le MDT par défaut. Le MDT de données est

toujours l'arbre de réception, il n'envoie jamais de trafic. Le MDT de données est uniquement destiné au trafic (S, G).

Le seuil auquel le MDT de données est créé peut être configuré par routeur ou par VRF. Lorsque la transmission multidiffusion dépasse le seuil défini, le routeur PE émetteur crée le MDT de données et envoie un message UDP (User Datagram Protocol), qui contient des informations sur le MDT de données à tous les routeurs du MDT par défaut. Les statistiques permettant de déterminer si un flux de multidiffusion a dépassé le seuil MDT de données sont examinées une fois par seconde.

Note: Après qu'un routeur PE envoie le message UDP, il attend 3 secondes de plus avant de basculer ; 13 secondes est le délai de basculement le plus défavorable et 3 secondes le meilleur.

Les MDT de données sont créés uniquement pour les entrées de route de multidiffusion (S, G) dans la table de routage de multidiffusion VRF. Ils ne sont pas créés pour les entrées (*, G) quelle que soit la valeur du débit de données source individuel

- Autorise PE à rejoindre directement une arborescence source pour un MDT.
- Aucun point de rendez-vous n'est nécessaire sur le réseau.
- Les RP sont un point de défaillance potentiel et des frais généraux supplémentaires.
- Mais ils autorisent les arbres partagés et BiDir (moins d'état).
- Réduire le délai de transmission.
- Évitez les frais généraux de gestion pour administrer le mappage de groupe/RP et les RP redondants pour garantir la fiabilité.
- Le compromis est plus nécessaire.
- (S, G) pour chaque mVPN dans un PE.

S'il y a 5 PE chacun tenant mVRF RED, il y a 5 entrées x (S, G).

1. Configurez la commande `ip pim ssm range` sur les routeurs P et PE (évitez la création d'entrées inutiles (*, G)).
2. SSM recommandé pour les Data-MDT.
3. Utilisez BiDir si possible pour Default-MDT (le support BiDir est spécifique à la plate-forme).

Si SSM n'est pas utilisé pour configurer des MDT de données :

- Chaque VRF doit être configuré avec un ensemble unique d'adresses P de multidiffusion ;

deux VRF dans le même MD ne peuvent pas être configurés avec le même ensemble d'adresses.

- De nombreuses autres adresses P multicast sont nécessaires.
- Opérations et gestion compliquées.
- SSM nécessite que le PE rejoigne un (S, G) et non (*, G).

G est connu comme étant configuré, mais PE ne connaît pas directement la valeur de S (S, G) du MDT par défaut propagé par MP-BGP.

L'avantage de SSM est qu'il ne dépend pas de l'utilisation d'un RP pour dériver le routeur PE source pour un groupe MDT particulier.

L'adresse IP du PE source et du groupe MDT par défaut est envoyée via le protocole BGP (Border Gateway Protocol)

BGP peut envoyer ces informations de deux manières :

- Communauté étendue Solution propriétaire CiscoAttribut non transitif (non adapté aux systèmes inter-AS)
- Famille d'adresses BGP MDT SAFI (66) **draft-nalawade-idr-mdt-safi**

Note: Les MVPN GRE ont été pris en charge avant d'utiliser MDT SAFI ; en fait, même avant le SAFI MDT en utilisant RD type 2. Techniquement, pour Profile 3, MDT SAFI ne doit pas être configuré, mais les deux SAFI sont simultanément pris en charge pour la migration.

BGP

- Groupe par défaut PE et MDT source codé dans NLRI de **MP_REACH_NLRI**.
- RD est identique à celui du MVRF pour lequel le groupe par défaut MDT est configuré.
- Le type de RD est 0 ou 1

```

▼ Path Attribute – MP_REACH_NLRI
  ► Flags: 0x80, Optional: Optional, Non-transitive, Complete
  Type Code: MP_REACH_NLRI (14)
  Length: 23
  Address family identifier (AFI): IPv4 (1)
  Subsequent address family identifier (SAFI): MCAST-VPN (5)
  Next hop network address (4 bytes)
  Number of Subnetwork points of attachment (SNPA): 0
  ▼ Network layer reachability information (14 bytes)
    Route Type: Intra-AS I-PMSI A-D route (1)
    Length: 12
  ► Path Attribute – ORIGIN: INCOMPLETE
  ► Path Attribute – AS_PATH: empty
  ► Path Attribute – MULTI_EXIT_DISC: 0
  ► Path Attribute – LOCAL_PREF: 100
  ► Path Attribute – COMMUNITIES: NO_EXPORT
  ► Path Attribute – EXTENDED_COMMUNITIES
  ▼ Path Attribute – PMSI_TUNNEL_ATTRIBUTE
    ► Flags: 0xc0, Optional, Transitive: Optional, Transitive, Complete
    Type Code: PMSI_TUNNEL_ATTRIBUTE (22)
    Length: 13
    Flags: 0
    Tunnel Type: PIM SSM Tree (3)
  ► MPLS Label Stack: (withdrawn)
  ▼ Tunnel ID: < 1.1.1.1, 239.232.0.0 >
    PIM-SSM Tree tunnel Root Node: 1.1.1.1
    PIM-SSM Tree tunnel P-multicast group: 239.232.0.0

```

L'attribut PMSI porte l'adresse source et l'adresse de groupe. Pour former le tunnel MT.

Adressage multidiffusion pour le groupe SSM

232.0.0.0 - 232.255.255.255 a été réservé aux applications multidiffusion spécifiques à la source globales.

239.0.0.0 - 239.255.255.255 est la plage d'espace d'adressage de multidiffusion IPv4 étendue administrativement

Portée locale de l'organisation IPv4 - **239.192.0.0/14**

L'étendue locale est l'étendue d'enceinte minimale et n'est donc pas plus divisible.

Les plages **239.0.0.0/10**, **239.64.0.0/10** et **239.128.0.0/10** ne sont pas affectées et peuvent être étendues à cet espace.

Ces plages doivent rester non attribuées jusqu'à ce que l'espace **239.192.0.0/14** ne soit plus suffisant.

Recommandations

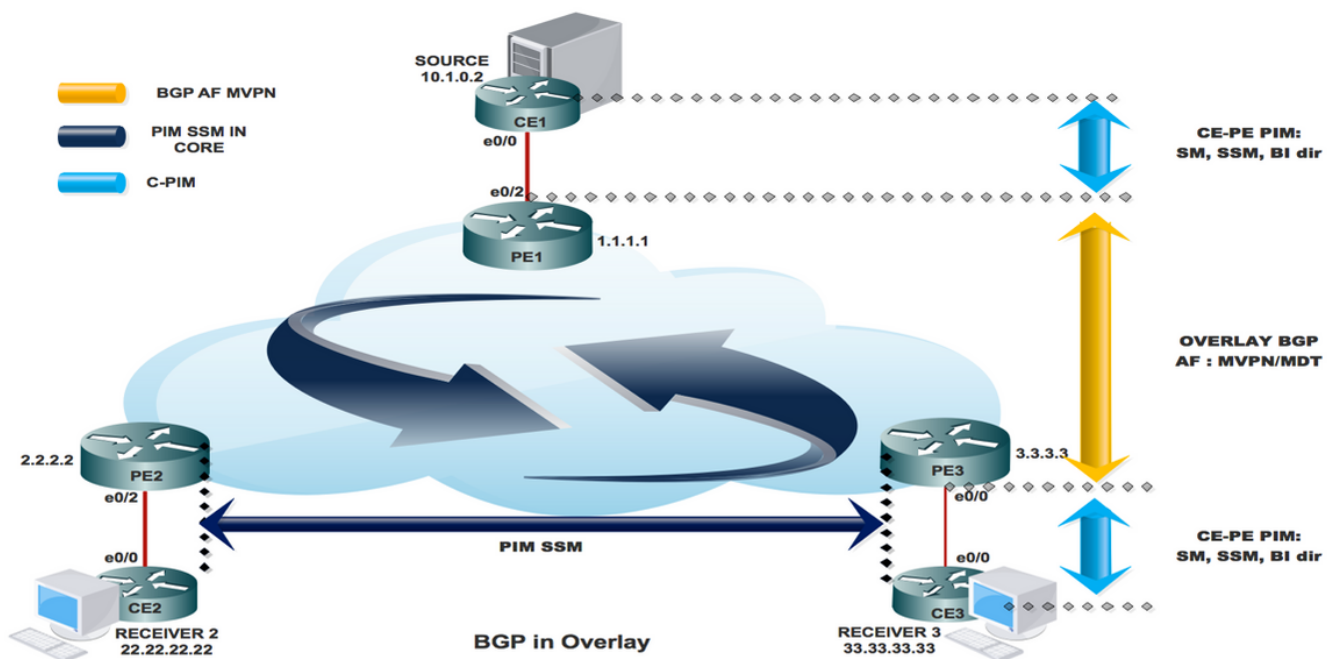
- Default-MDT doit dessiner des adresses de l'espace 239/8 en commençant par la plage définie avec l'étendue locale d'organisation 239.192.0.0/14
- Data-MDT doit dessiner des adresses à partir de l'étendue locale de l'organisation.
- Il est également possible d'utiliser la plage globale SSM 232.0.0.0 - 232.255.255.255

- Comme SSM utilise toujours un état unique (S, G), il n'y a aucune possibilité de chevauchement car le flux de multidiffusion SSM sera initié par différentes sources (avec des adresses différentes), qu'elles se trouvent dans le réseau du fournisseur ou sur Internet.
- Utilisez le même pool Data-MDT pour chaque mVRF dans un domaine de multidiffusion particulier (où Default-MDT est commun).

Par exemple, tous les VRF utilisant Default-MDT 239.192.10.1 doivent utiliser la même plage de données MDT 239.232.1.0/24

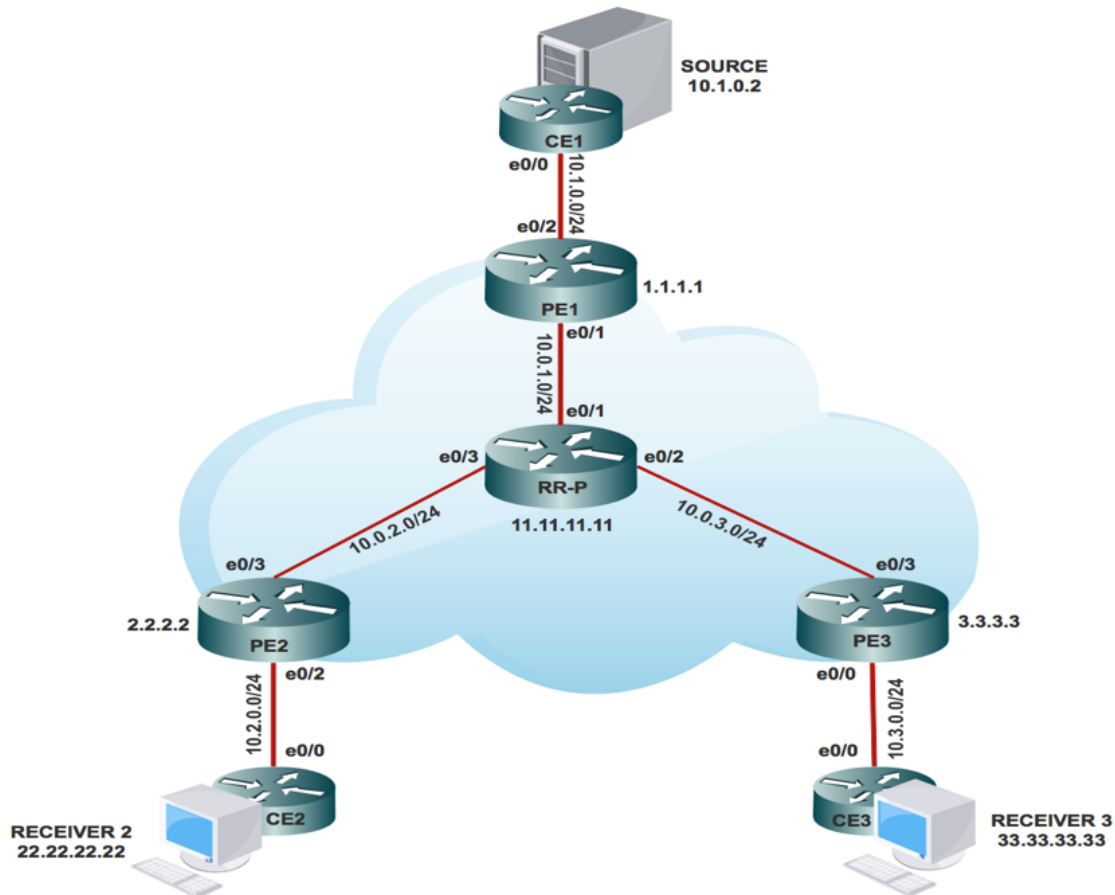
Signalisation de superposition

La signalisation de superposition de Rosen GRE est affichée dans l'image.



Topologie

La topologie de Rosen GRE est affichée dans l'image.



Routage et transfert VPN multidiffusion et domaines multidiffusion

MVPN introduit les informations de routage multidiffusion dans la table de routage et de transfert VPN. Lorsqu'un routeur de périphérie du fournisseur reçoit des données de multidiffusion ou des paquets de contrôle d'un routeur de périphérie du client (CE), le transfert est effectué conformément aux informations de l'instance MVRF (Multicast VPN Routing and Forwarding instance). MVPN n'utilise pas la commutation d'étiquette.

Un ensemble de MVRF pouvant envoyer du trafic de multidiffusion entre eux constitue un domaine de multidiffusion. Par exemple, le domaine de multidiffusion d'un client qui souhaite envoyer certains types de trafic de multidiffusion à tous les employés du monde entier se composerait de tous les routeurs CE associés à cette entreprise.

Tâches de configuration

1. Activez le routage multidiffusion sur tous les noeuds.
2. Activez le mode PIM (Protocol Independent Multicast) dans toutes les interfaces.
3. Avec le VRF existant, configurez le MDT par défaut.
4. Configurez le VRF sur l'interface Ethernet0/x.
5. Activez le routage multidiffusion sur VRF.

6. Configurez PIM SSM Default dans tous les noeuds du coeur de réseau.
7. Configurez la famille d'adresses BGP MVPN.
8. Configurez le RP BSR dans le noeud CE.
9. Préconfiguré :

```
VRF SSM-BGP
mBGP: Address family VPNv4
VRF Routing Protocol
```

Configuration Steps:

Enable Multicast Routing

On All Nodes

```
(conf) # ip multicast-routing
```

Enable "ip multicast-routing" in global mode on all nodes.

Enable PIM Sparse Mode

Enable on all connected Interface

```
(config)#interface Ethernet0/x
(config-if)#ip pim sparse-mode

(config)# interface lo0
(config-if)# ip pim sparse-mode
```

"x" represents the connected interface number on all nodes

Configure Default MDT Group in VRF

On PE1, PE2 and PE3

```
(config)#ip vrf SSM-BGP
(config-vrf)# mdt auto-discovery pim
(config-vrf)# mdt default 239.232.0.0
```

SERVICE PROVIDER : Group : 239.232.0.0 Source : 1.1.1.1

Configure the VRF on the interface Ethernet0/x

On PE1, PE2 and PE3

```
(config)#interface Ethernet0/x
(config-if)# ip vrf forwarding SSM-BGP
(config-if)# ip address 10.x.0.1 255.255.255.0
(config-if)# ip pim sparse-mode
```

"x" represent the interface number that PE connected to CE.

Enable Multicast Routing on VRF

On PE1, PE2 and PE3

```
(conf) # ip multicast-routing vrf SSM-BGP
```

Enable "ip multicast-routing m-GRE" in global mode.

Configure PIM SSM Default in all nodes inside the core.

On PE1, PE2, PE3 and RR-P Node

```
(config) # ip pim ssm default
```

Static RP configuration in the core in global mode.

Configure BSR RP in CE Node (Receiver)

On Receiver 2

```
(config)# ip pim bsr-candidate loopback0  
(config)# ip pim rp-candidate loopback0
```

BSR RP configuration in the Receiver 2 in global mode.

Vérification

Tâche 1 : vérification de la connectivité physique

Vérifiez que toutes les interfaces connectées sont **ACTIVÉES**.

Tâche 2 : Vérifiez la monodiffusion VPNv4 de la famille d'adresses BGP.

- Vérifiez que BGP est activé sur tous les routeurs pour la monodiffusion AF VPNv4 et que les voisins BGP sont **UP**.
- Vérifiez que la table de monodiffusion VPNv4 BGP contient tous les préfixes du client.

Tâche 3 : Vérifiez la monodiffusion MVPN de la famille d'adresses BGP.

- Vérifiez que BGP est activé sur tous les routeurs pour AF IPV4 MVPN et que les voisins BGP sont **ACTIFS**.
- Vérifiez que tous les PE se découvrent mutuellement, avec la route de type 1.

Tâche 4 : Vérifier le trafic multidiffusion de bout en bout

- Vérifiez le voisinage PIM.
- Vérifiez que l'état de multidiffusion est créé dans le VRF.
- Vérifiez l'entrée mRIB sur PE1, PE2 et PE3.
- Vérifiez que (S, G) entrée mFIB, paquet incrémenté dans le transfert de logiciel.
- Vérifier que les paquets ICMP atteignent l'interface CE à CE.

Task 1: Verify Physical Connectivity

Verify all the connected interface are "UP"

```
#sh ip interface brief
```

Task 2: Verify Address Family VPNv4 unicast

Address Family VPNv4 unicast and BGP neighbors

```
# show running-config | s r bgp
# show bgp vpnv4 unicast summary all
```

VPNv4 unicast table has all the Customer prefixes

```
PE1#sh bgp vpnv4 unicast all
BGP table version is 31, local router ID is 1.1.1.1

  Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:100 (default for vrf m-GRE)
*>i 22.22.22.22/32  2.2.2.2           0     100     0 20 i
*>i 33.33.33.33/32  3.3.3.3           0     100     0 30 i
*>  111.111.111.111/32
                               10.1.0.2          0                 0 10 i
```

Check on all the PE nodes (PE1, PE2 and PE3)

Task 3: Verify Address Family IPv4 MVPN

Address Family IPv4 MVPN and BGP neighbors

```
# show running-config | s r bgp
# #sh bgp ipv4 mvpn all
```

IPv4 MVPN table has all the PE routes with Type 1 routes

```
PE1#sh bgp ipv4 mvpn all
BGP table version is 15, local router ID is 1.1.1.1

Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

  Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf SSM-BGP)
*>  [1][1:1][1.1.1.1]/12
                               0.0.0.0           32768 ?
*>i  [1][1:1][2.2.2.2]/12
                               2.2.2.2           0     100     0 ?
*>i  [1][1:1][3.3.3.3]/12
                               3.3.3.3           0     100     0 ?
Route Distinguisher: 2:2
*>i  [1][2:2][2.2.2.2]/12
                               2.2.2.2           0     100     0 ?
Route Distinguisher: 3:3
  Network          Next Hop          Metric LocPrf Weight Path
*>i  [1][3:3][3.3.3.3]/12
                               3.3.3.3           0     100     0 ?
```

Check on all the PE nodes (PE1, PE2 and PE3)

Verify that (S,G) mFIB entry, packet getting incremented

```
PE1#sh ip mfib vrf SSM-BGP 225.1.1.1 verbose

I/O Item Flags:
      NS - Negate Signalling, SP - Signal Present,
      A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
      MA - MFIB Accept,

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:  FS Pkt Count/PS Pkt Count
VRF SSM-BGP
(10.1.0.2,225.1.1.1) Flags: K DDE
  SW Forwarding: 10/0/100/0, Other: 2/1/1
  Ethernet0/2 Flags: RA A MA
  Tunnel0, MDT/239.232.0.0 Flags: RF F NS
  CEF: Adjacency with MAC: 4500000000000000FF2FC9E401010101EFE8000000000800
  Pkts: 10/0
```

Verify that multicast state is created in the VRF

```
PE1#sh ip mroute vrf SSM-BGP verbose
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
      L - Local, P - Pruned, R - RP-bit set, F - Register flag,
      T - SPT-bit set, p - PIM Joins on route,

(10.1.0.2, 225.1.1.1), 00:00:03/00:02:56, flags: Tp
Incoming interface: Ethernet0/2, RPF nbr 10.1.0.2
Outgoing interface list:
Tunnel0, GRE MDT: 239.232.0.0 (default), Forward/Sparse, 00:00:03/00:03:26, p
```

Check on all the PE nodes (PE1, PE2 and PE3)

Verify that (S,G) mFIB entry, packet getting incremented

```
PE1#sh ip mfib vrf SSM-BGP 225.1.1.1 verbose

I/O Item Flags:
      NS - Negate Signalling, SP - Signal Present,
      A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
      MA - MFIB Accept,

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:  FS Pkt Count/PS Pkt Count
VRF SSM-BGP
(10.1.0.2,225.1.1.1) Flags: K DDE
  SW Forwarding: 10/0/100/0, Other: 2/1/1
  Ethernet0/2 Flags: RA A MA
  Tunnel0, MDT/239.232.0.0 Flags: RF F NS
  CEF: Adjacency with MAC: 4500000000000000FF2FC9E401010101EFE8000000000800
  Pkts: 10/0
```

mRIB in the Service Provider Core.

```
PE1#sh ip mroute verbose
IP Multicast Routing Table
Flags: s - SSM Group, C - Connected,
      T - SPT-bit set,
      I - Received Source Specific Host Report,
      Z - Multicast Tunnel, z - MDT-data group sender,
      p - PIM Joins on route,

(1.1.1.1, 239.232.0.0), 01:00:33/00:03:03, flags: sTp
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse, 01:00:33/00:03:03, p

(3.3.3.3, 239.232.0.0), 01:00:33/stopped, flags: sTIZ
  Incoming interface: Ethernet0/1, RPF nbr 10.0.1.2
  Outgoing interface list:
    MVRF SSM-BGP, Forward/Sparse, 01:00:33/00:02:26

(2.2.2.2, 239.232.0.0), 01:00:33/stopped, flags: sTIZ
  Incoming interface: Ethernet0/1, RPF nbr 10.0.1.2
  Outgoing interface list:
    MVRF SSM-BGP, Forward/Sparse, 01:00:33/00:02:26
```

Check on all the PE nodes (PE1, PE2 and PE3)

Verify ICMP packets getting reach from CE to CE

```
SOURCE1#ping 225.1.1.1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 225.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.3.0.2, 29 ms
Reply to request 0 from 10.3.0.2, 29 ms
```

Comment les interfaces de tunnel sont créées ?

Création du tunnel MDT

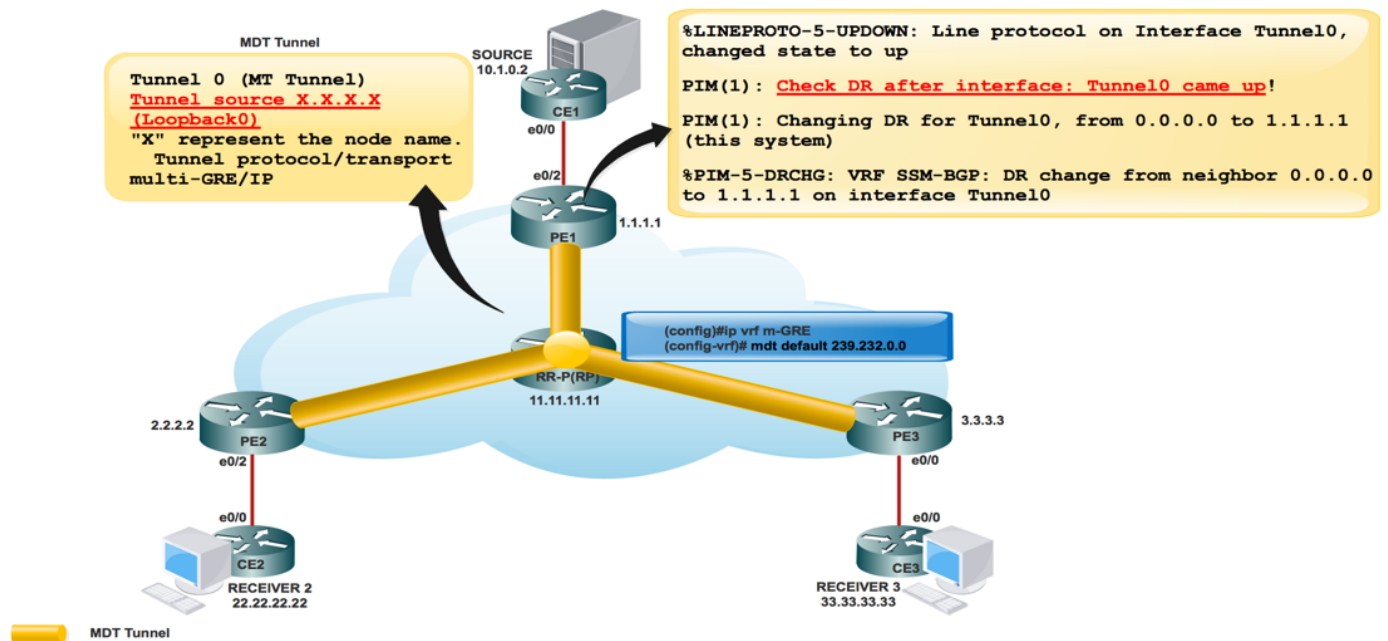
Une fois que nous avons configuré mdt default 239.232.0.0

Le tunnel 0 est apparu et a attribué son adresse de bouclage 0 comme source.

%LINEPROTO-5-UPDOWN : Protocole de ligne sur l'interface Tunnel0, état modifié en up

```
PIM(1): Check DR after interface: Tunnel0 came up!
PIM(1): Changing DR for Tunnel0, from 0.0.0.0 to 1.1.1.1 (this system)
%MIM-5-DRCHG: VRF SSM-BGP: DR change from neighbor 0.0.0.0 to 1.1.1.1 on interface Tunnel0
```

Cette image montre la création de tunnel MDT.



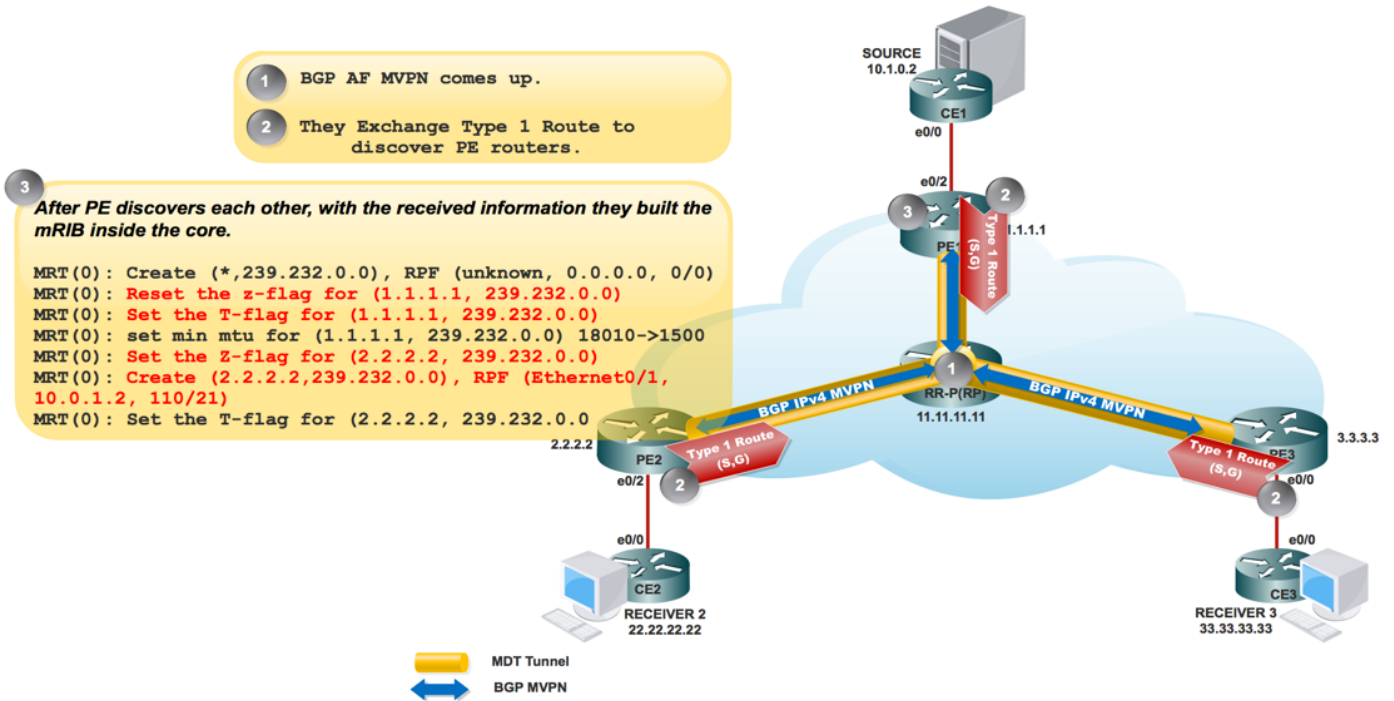
```

PE1#sh int tunnel 0
Tunnel0 is up, line protocol is up
Hardware is Tunnel
Interface is unnumbered. Using address of Loopback0 (1.1.1.1)
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 1.1.1.1 (Loopback0)
Tunnel Subblocks:
  src-track:
    Tunnel0 source tracking subblock associated with Loopback0
    Set of tunnels with source Loopback0, 1 member (includes iterators), on interface <OK>
Tunnel protocol/transport multi-GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled

```

Dès que BGP MVPN est activé, tous les PE se découvrent via la route de type 1. Tunnel de multidiffusion formé. BGP transporte toutes les adresses PE de groupe et source dans l'attribut PMSI.

Cette image montre l'échange d'une route de type 1.



Cette image montre PCAP-1.

- ▼ Path attributes
 - ▼ Path Attribute – MP_REACH_NLRI
 - ▶ Flags: 0x80, Optional: Optional, Non-transitive, Complete
 - Type Code: MP_REACH_NLRI (14)
 - Length: 23
 - Address family identifier (AFI): IPv4 (1)
 - Subsequent address family identifier (SAFI): MCAST-VPN (5)
 - Next hop network address (4 bytes)
 - Number of Subnetwork points of attachment (SNPA): 0
 - ▼ Network layer reachability information (14 bytes)
 - Route Type: Intra-AS I-PMSI A-D route (1) → Type 1 Route
 - Length: 12
 - ▶ Path Attribute – ORIGIN: INCOMPLETE
 - ▶ Path Attribute – AS_PATH: empty
 - ▶ Path Attribute – MULTI_EXIT_DISC: 0
 - ▶ Path Attribute – LOCAL_PREF: 100
 - ▶ Path Attribute – COMMUNITIES: NO_EXPORT
 - ▶ Path Attribute – EXTENDED_COMMUNITIES
 - ▼ Path Attribute – PMSI_TUNNEL_ATTRIBUTE
 - ▶ Flags: 0xc0, Optional, Transitive: Optional, Transitive, Complete
 - Type Code: PMSI_TUNNEL_ATTRIBUTE (22)
 - Length: 13
 - Flags: 0
 - Tunnel Type: PIM SSM Tree (3) → PIM SSM TREE (Tunnel Type)
 - MPLS Label Stack: (withdrawn)
 - ▼ Tunnel ID: < 1.1.1.1, 239.232.0.0 >
 - PIM-SSM Tree tunnel Root Node: 1.1.1.1
 - PIM-SSM Tree tunnel P-multicast group: 239.232.0.0 ↔ PIM SSM Tree Tunnel Root and Group

```
PE1#sh ip mroute
```

```
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
U - URD, I - Received Source Specific Host Report,
Z - Multicast Tunnel, z - MDT-data group sender,
```

```
(3.3.3.3, 239.232.0.0), 00:01:41/00:01:18, flags: sTIZ
Incoming interface: Ethernet0/1, RPF nbr 10.0.1.2
Outgoing interface list:
```

```
MVRF SSM-BGP, Forward/Sparse, 00:01:41/00:01:18
```

```
(2.2.2.2, 239.232.0.0), 00:01:41/00:01:18, flags: sTIZ
Incoming interface: Ethernet0/1, RPF nbr 10.0.1.2
```

Outgoing interface list:
MVRF SSM-BGP, Forward/Sparse, 00:01:41/00:01:18

"Z" Multicast Tunnel formed after BGP mVPN comes up, as it advertises the Source PE and Group Address in PMSI attribute.

Voisinage PIM

```
PE1#sh ip pim vrf SSM-BGP neighbor
```

PIM Neighbor Table

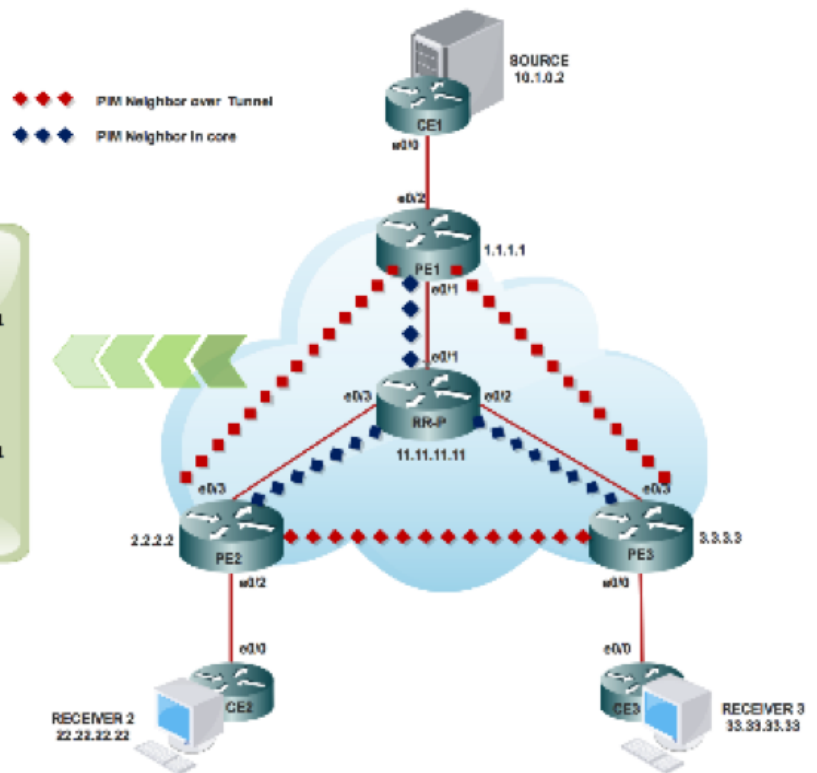
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable

Neighbor Address	Interface	Uptime/Expires	Ver	DR	Prio/Mode
10.1.0.2	Ethernet0/2	00:58:18/00:01:31	v2 1	DR	S P G
3.3.3.3	Tunnel0	00:27:44/00:01:32	v2 1		S P G
2.2.2.2	Tunnel0	00:27:44/00:01:34	v2 1		S P G

Control Plane Scalability:

For Example:

- ⇒ PE anticipating 100 MVPN services which distributed across 100 PEs.
- ⇒ Each PE maintains 9900 (99x100) PIM adjacencies in addition to the adjacency.
- ⇒ In order to preserve 9900 PIM adjacencies, the PE would be sending approx 330 PIM adjacencies per second (Using default 30s PIM hello timer)
- ⇒ The number will get worse as the number of MVPN services or PEs increases.



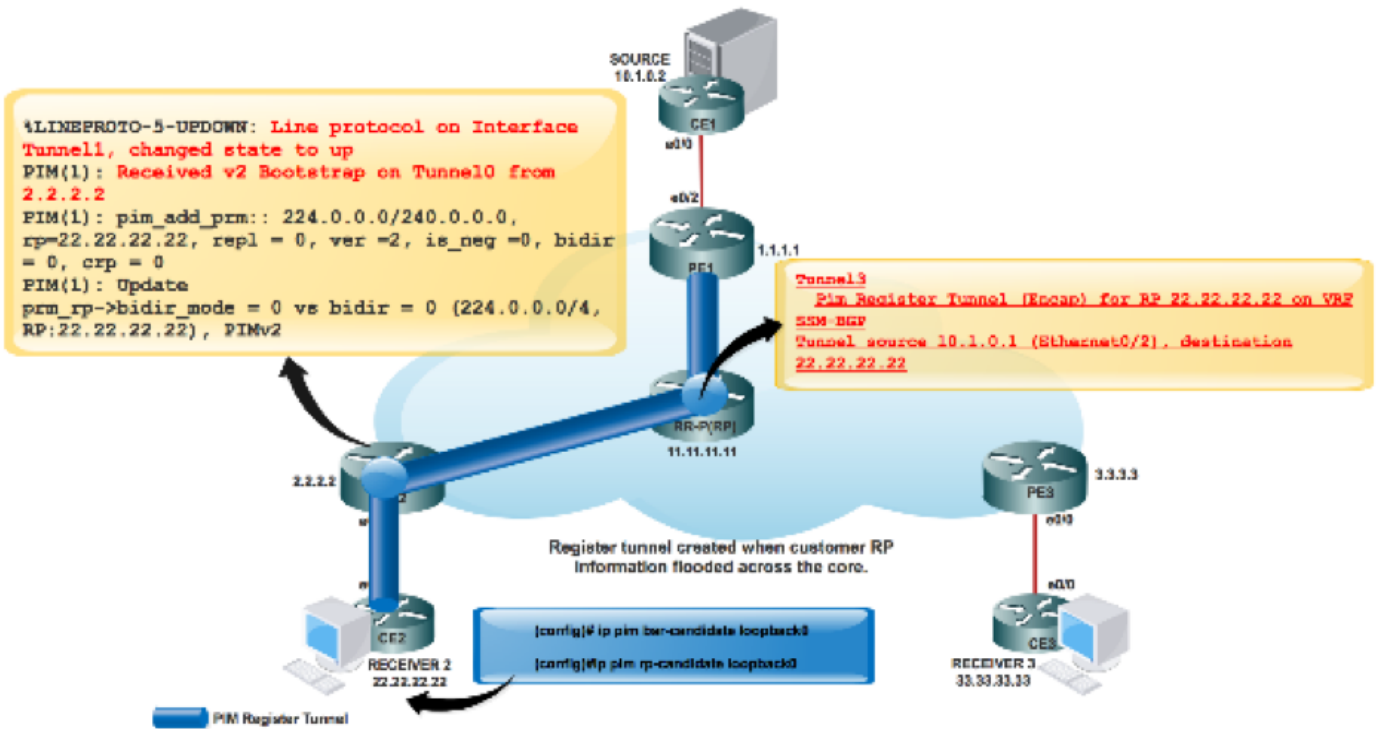
Dès que vous configurez les informations RP :

%LINEPROTO-5-UPDOWN : Protocole de ligne sur l'interface Tunnel1, état modifié en up

L'échange de messages d'amorçage via le tunnel MDT

```
PIM(1): Received v2 Bootstrap on Tunnel0 from 2.2.2.2
PIM(1): pim_add_prm:: 224.0.0.0/240.0.0.0, rp=22.22.22.22, repl = 0, ver =2, is_neg =0, bidir =
0, crp = 0
PIM(1): Update
prm_rp->bidir_mode = 0 vs bidir = 0 (224.0.0.0/4, RP:22.22.22.22), PIMv2
*May 18 10:28:42.764: PIM(1): Received RP-Reachable on Tunnel0 from 22.22.22.22
```

Cette image montre l'échange de messages bootstrap via le tunnel MDT.



```
PE2#sh int tunnel 1
Tunnel1 is up, line protocol is up
Hardware is Tunnel
Description: Pim Register Tunnel (Encap) for RP 22.22.22.22 on VRF SSM-BGP
Interface is unnumbered. Using address of Ethernet0/2 (10.2.0.1)
MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.2.0.1 (Ethernet0/2), destination 22.22.22.22
Tunnel Subblocks:
  src-track:
    Tunnel1 source tracking subblock associated with Ethernet0/2
    Set of tunnels with source Ethernet0/2, 1 member (includes iterators), on interface
<OK>
Tunnel protocol/transport PIM/IPv4
Tunnel TOS/Traffic Class 0xC0, Tunnel TTL 255
Tunnel transport MTU 1472 bytes
Tunnel is transmit only
```

Deux tunnels ont formé le tunnel PIM register et le tunnel MDT.

- Le tunnel 0 est utilisé pour envoyer le trafic de multidiffusion PIM Join et à faible bande passante.
- Le tunnel 1 est utilisé pour envoyer le message PIM encapsulated Register.

Commande à vérifier :

**MDT BGP :

PE1#sh ip pim vrf m-SSM mdt bgp

** envoyer des données FHR :

PE1#sh ip pim vrf m-SSM mdt

Flag	Name	Description
Z	Multicast Tunnel	Indicates that this entry is an IP multicast group that belongs to the Default or Data MDT tunnel. All packets received for this IP multicast state are sent to the MDT tunnel for decapsulation . Set on <u>receiving</u> PE. Global multicast routing table
Y	Joined MDT-data group	Indicates that the traffic was received through a Data MDT tunnel that was set up specifically for this source and group. MVRF multicast routing table
Z	MDT-data group sender	Set on sending PE. Global multicast routing table
y	Sending to MDT-data group	Indicates that the traffic was sent through a Data MDT tunnel that was set up specifically for this source and group. MVRF multicast routing table
V	RD & Vector	
v	Vecor	
E	Extranet source mroute entry	Indicates that a (*, G) or (S, G) entry in the VRF routing table is a source Multicast VRF (MVRF) entry and has extranet receiver MVRF entries linked to it

Informations connexes

- <https://tools.ietf.org/html/rfc4760>
- <https://tools.ietf.org/html/rfc5110>
- <https://tools.ietf.org/html/rfc6513>
- [Support et documentation techniques - Cisco Systems](#)