

Exemple de configuration de Multidiffusion ASR 1000 OTV

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Schéma de réseau avec la Connectivité L2/L3 de base](#)

[Connectivité L2/L3 de base](#)

[Configuration minimale de Multidiffusion OTV](#)

[Vérification OTV](#)

[Schéma de réseau avec OTV](#)

[Commandes de vérification et sortie prévue](#)

[Problème courant](#)

[Dépannez](#)

[Créez une capture de paquet sur l'interface de jointure afin de voir OTV Hellos](#)

[Vérifiez l'état de Mroute sur OTV ASR](#)

[Créez une capture de paquet sur la Jointure-interface pour voir des paquets de données OTV](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le mode de Multidiffusion de la virtualisation de transport de recouvrement (OTV) sur la plate-forme 1000 du routeur de services d'agrégation de Cisco (ASR). OTV étend la topologie de la couche 2 (L2) à travers les sites physiquement différents, qui permet à des périphériques pour communiquer à L2 à travers un fournisseur de la couche 3 (L3). Les périphériques dans le site 1 croient qu'ils se trouvent sur le même domaine d'émission que ceux dans le chantier 2.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de la connexion virtuelle d'Ethernets (EVC)

- Configuration L2 et L3 de base sur la plate-forme ASR
- La connaissance de Protocole IGMP (Internet Group Management Protocol) de configuration de base de version 3 et de Protocol Independent Multicast (PIM)

Composants utilisés

Les informations dans ce document sont basées sur l'ASR1002 avec la version asr1000rp1-adventerprise.03.09.00.S.153-2.S.bin de Cisco IOS®.

Votre système doit avoir ces conditions requises afin d'implémenter la caractéristique OTV sur l'ASR 1000 :

- Version 3.5S ou ultérieures de Cisco IOS XE
- Maximum Transmission Unit (MTU) de 1542 ou plus élevé

Remarque: OTV ajoute une en-tête 42-byte avec ne fragmente pas le bit (DF-bit) dans tous les paquets encapsulés. Afin de transporter les paquets 1500-byte par le recouvrement, le transit network doit prendre en charge un Maximum Transmission Unit (MTU) de 1542 ou plus élevé. Afin de tenir compte de la fragmentation à travers OTV, vous devez activer le <interface> de joindre-**interface de fragmentation d'otv**.

- Unicast et accessibilité de Multidiffusion entre les sites

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Cette section décrit comment configurer le mode de Multidiffusion OTV.

Schéma de réseau avec la Connectivité L2/L3 de base

Connectivité L2/L3 de base

Début avec une configuration de base. L'interface interne sur l'ASR est configurée pour des services instance pour le trafic dot1q. Les OTV joignent l'interface sont l'interface externe du WAN L3.

```
ASR-1
interface GigabitEthernet0/0/0
  description OTV-WAN-Connection
  mtu 9216
  ip address 172.17.100.134 255.255.255.0
  negotiation auto
  cdp enable
```

```
ASR-2
interface GigabitEthernet0/0/0
```

```
description OTV-WAN-Connection
mtu 9216
ip address 172.16.64.84 255.255.255.0
negotiation auto
cdp enable
```

Puisqu'OTV ajoute une en-tête 42-byte, vous devez vérifier que le fournisseur de services Internet (ISP) passe la taille minimum de MTU du site à site. Afin d'accomplir cette vérification, envoyez une longueur de paquet de 1542 avec le positionnement de DF-bit. Ceci donne l'ISP que la charge utile exigée plus **ne fragmentent pas la** balise sur le paquet afin de simuler un paquet OTV. Si vous ne pouvez pas cingler sans DF-bit, alors vous avez un problème de routage. Si vous pouvez cingler sans lui, mais ne pouvez pas cingler avec le positionnement de DF-bit, vous avez un problème de MTU. Une fois que réussi, vous êtes prêt à ajouter le mode d'unicast OTV à votre site ASR.

```
ASR-1#ping 172.17.100.134 size 1542 df-bit
Type escape sequence to abort.
Sending 5, 1514-byte ICMP Echos to 172.17.100.134, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

L'interface interne est un port L2 configuré avec des services instance pour les paquets balisés L2 dot1q. Il établit également un domaine interne de passerelle de site. Dans cet exemple, c'est le VLAN1 non-marqué. Le domaine interne de passerelle de site est utilisé pour la transmission de plusieurs périphériques OTV au même site. Ceci leur permet pour communiquer et déterminer quel périphérique est le périphérique bien fondé de périphérie (AED) pour lequel domaine de pont.

Le service instance doit être configuré dans un domaine de passerelle qui utilise le recouvrement.

```
ASR-1
interface GigabitEthernet0/0/1
no ip address
negotiation auto
cdp enable
  service instance 1 ethernet
  encapsulation untagged
  bridge-domain 1
!
service instance 50 ethernet
 encapsulation dot1q 100
 bridge-domain 200
!
service instance 51 ethernet
 encapsulation dot1q 101
 bridge-domain 201
```

```
ASR-2
interface GigabitEthernet0/0/2
no ip address
negotiation auto
cdp enable
  service instance 1 ethernet
  encapsulation untagged
  bridge-domain 1
!
service instance 50 ethernet
 encapsulation dot1q 100
 bridge-domain 200
!
service instance 51 ethernet
```

```
encapsulation dot1q 101
bridge-domain 201
```

Configuration minimale de Multidiffusion OTV

C'est une configuration de base qui exige seulement de quelques commandes afin d'installer OTV et se joindre/interfaces internes.

Configurez le domaine de passerelle de site local. Dans cet exemple, c'est VLAN1 sur le RÉSEAU LOCAL. L'identifiant de site est spécifique à chaque emplacement physique. Dans cet exemple, il y a deux sites distants qui sont physiquement indépendants de l'un l'autre. Le site 1 et le site 2 sont configurés en conséquence. La Multidiffusion doit également être configurée selon les conditions requises pour OTV.

ASR-1

```
Config t
otv site bridge-domain 1
otv site-identifiant 0000.0000.0001
ip multicast-routing distributed
ip pim ssm default
interface GigabitEthernet0/0/0
    ip pim passive
    ip igmp version 3
```

ASR-2

```
Config t
otv site bridge-domain 1
otv site-identifiant 0000.0000.0002
ip multicast-routing distributed
ip pim ssm default
interface GigabitEthernet0/0/0
    ip pim passive
    ip igmp version 3
```

Construisez le recouvrement pour chaque côté. Configurez le recouvrement, appliquez l'interface de joindre, et ajoutez le contrôle et les groupements de données à chaque côté.

Ajoutez les deux domaines de passerelle que vous voulez pour étendre. Notez que vous n'étendez pas le domaine de passerelle de site, seulement les deux VLAN requis. Vous établissez un service instance distinct pour les interfaces de recouvrement pour appeler le domaine 200 et 201 de passerelle. Appliquez les balises dot1q 100 et 101 respectivement.

ASR-1

```
Config t
interface Overlay1
    no ip address
    otv join-interface GigabitEthernet0/0/0
otv control-group 225.0.0.1 otv data-group 232.10.10.0/24
service instance 10 ethernet
    encapsulation dot1q 100
    bridge-domain 200
service instance 11 ethernet
    encapsulation dot1q 101
    bridge-domain 201
```

ASR-2

Config t

```
interface Overlay1
  no ip address
  otv join-interface GigabitEthernet0/0/0
otv control-group 225.0.0.1 otv data-group 232.10.10.0/24
service instance 10 ethernet
  encapsulation dot1q 100
  bridge-domain 200
service instance 11 ethernet
  encapsulation dot1q 101
  bridge-domain 201
```

Remarque: N'étendez pas le site VLAN sur l'interface de recouvrement. Ceci fait avoir les deux ASR un conflit parce qu'ils croient que chaque côté distant est dans le même site.

À ce stade, l'ASR à la contiguïté de Multidiffusion ASR OTV est complet et fonctionnel. Les voisins sont trouvés, et l'ASR devrait être AED-capable pour les VLAN qui doivent être étendus.

ASR-1#show otv

```
Overlay Interface Overlay1
VPN name           : None
VPN ID             : 2
State              : UP
AED Capable        : Yes
IPv4 control group : 225.0.0.1
Mcast data group range(s): 232.10.10.0/24
Join interface(s)  : GigabitEthernet0/0/0
Join IPv4 address  : 172.17.100.134
Tunnel interface(s) : Tunnel0
Encapsulation format : GRE/IPv4
Site Bridge-Domain : 1
Capability          : Multicast-reachable
Is Adjacency Server : No
Adj Server Configured : No
Prim/Sec Adj Svr(s) : None
```

ASR-2#show otv

```
Overlay Interface Overlay1
VPN name           : None
VPN ID             : 2
State              : UP
AED Capable        : Yes
IPv4 control group : 225.0.0.1
Mcast data group range(s): 232.10.10.0/24
Join interface(s)  : GigabitEthernet0/0/0
Join IPv4 address  : 172.16.64.84
Tunnel interface(s) : Tunnel0
Encapsulation format : GRE/IPv4
Site Bridge-Domain : 1
Capability          : Multicast-reachable
Is Adjacency Server : No
Adj Server Configured : No
Prim/Sec Adj Svr(s) : None
```

Vérification OTV

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Schéma de réseau avec OTV

Commandes de vérification et sortie prévue

Cette sortie prouve que des VLAN 100 et 101 sont étendus. L'ASR est l'AED, et l'interface interne et le service instance qui trace les VLAN sont affichés dans la sortie.

```
ASR-1#show otv vlan
```

```
Key:  SI - Service Instance
```

```
Overlay 1 VLAN Configuration Information
```

Inst	VLAN	Bridge-Domain	Auth	Site Interface(s)
0	100	200	yes	Gi0/0/1:SI50
0	101	201	yes	Gi0/0/1:SI51

Total VLAN(s): 2
Total Authoritative VLAN(s): 2

```
ASR-2#show otv vlan
```

```
Key:  SI - Service Instance
```

```
Overlay 1 VLAN Configuration Information
```

Inst	VLAN	Bridge-Domain	Auth	Site Interface(s)
0	100	200	yes	Gi0/0/2:SI50
0	101	201	yes	Gi0/0/2:SI51

Total VLAN(s): 2
Total Authoritative VLAN(s): 2

Afin de valider, étendre les VLAN, et exécuter un ping de site à site. L'hôte 192.168.100.2 se trouve au site 1, et l'hôte 192.168.100.3 se trouve au site 2. On s'attend à ce que les pings premiers échouent pendant que vous construisez le Protocole ARP (Address Resolution Protocol) localement et à travers OTV à l'autre côté.

```
LAN-SW1#ping 192.168.100.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
```

```
...!!
```

```
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/5/10 ms
```

```
LAN-SW1#ping 192.168.100.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

```
LAN-SW1#ping 192.168.100.3 size 1500 df-bit
```

```
Type escape sequence to abort.
```

```
Sending 5, 1500-byte ICMP Echos to 192.168.100.3, timeout is 2 seconds:
```

```
Packet sent with the DF bit set
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

Afin de s'assurer que la table de MAC et des tables de routage OTV sont établis correctement avec le périphérique local, apprenez l'adresse MAC du périphérique distant avec l'utilisation de la commande d'artère d'otv d'exposition.

```
LAN-SW1#show int vlan 100
```

```
Vlan100 is up, line protocol is up
  Hardware is Ethernet SVI, address is 0c27.24cf.abd1 (bia 0c27.24cf.abd1)
  Internet address is 192.168.100.2/24
```

```
LAN-SW2#show int vlan 100
```

```
Vlan100 is up, line protocol is up
  Hardware is Ethernet SVI, address is b4e9.b0d3.6a51 (bia b4e9.b0d3.6a51)
  Internet address is 192.168.100.3/24
```

```
ASR-1#show otv route vlan 100
```

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,
       SI - Service Instance, * - Backup Route
```

```
OTV Unicast MAC Routing Table for Overlay1
```

Inst	VLAN	BD	MAC Address	AD	Owner	Next Hops(s)
0	100	200	0c27.24cf.abaf	40	BD Eng	Gi0/0/1:SI50
0	100	200	0c27.24cf.abd1	40	BD Eng	Gi0/0/1:SI50 <--- Local mac is pointing to the physical interface
0	100	200	b4e9.b0d3.6a04	50	ISIS	ASR-2
0	100	200	b4e9.b0d3.6a51	50	ISIS	ASR-2 <--- Remote mac is pointing across OTV to ASR-2

```
4 unicast routes displayed in Overlay1
```

```
-----
4 Total Unicast Routes Displayed
```

```
ASR-2#show otv route vlan 100
```

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,
       SI - Service Instance, * - Backup Route
```

```
OTV Unicast MAC Routing Table for Overlay1
```

Inst	VLAN	BD	MAC Address	AD	Owner	Next Hops(s)
0	100	200	0c27.24cf.abaf	50	ISIS	ASR-1
0	100	200	0c27.24cf.abd1	50	ISIS	ASR-1 <--- Remote mac is pointing across OTV to ASR-1
0	100	200	b4e9.b0d3.6a04	40	BD Eng	Gi0/0/2:SI50
0	100	200	b4e9.b0d3.6a51	40	BD Eng	Gi0/0/2:SI50 <--- Local mac is pointing to the physical interface

```
4 unicast routes displayed in Overlay1
```

```
-----
4 Total Unicast Routes Displayed
```

Problème courant

L'OTV ne forme pas le message d'erreur dans la sortie prouve que l'ASR n'est pas AED-capable. Ceci signifie que l'ASR n'expédie pas les VLAN à travers l'OTV. Il y a plusieurs causes possibles pour ceci, mais le plus commun est que les ASR n'ont pas la Connectivité entre les sites. Vérifiez la Connectivité L3 et le trafic de multidiffusion bloqué possible. Une autre cause possible de cette condition est quand le domaine interne de passerelle de site n'est pas configuré. Ceci crée une

condition où l'ASR ne peut pas devenir l'AED, parce qu'il n'est pas certain si c'est le seul ASR sur le site ou pas.

```
ASR-1#show otv
```

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : No, overlay DIS not elected <--- Not Forwarding
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.0.0.0/8
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address  : 172.17.100.134
  Tunnel interface(s): Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None
```

```
ASR-2#show otv
```

```
Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : No, overlay DIS not elected <--- Not Forwarding
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.0.0.0/8
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address  : 172.16.64.84
  Tunnel interface(s): Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Créez une capture de paquet sur l'interface de joindre afin de voir OTV Hellos

Vous pouvez utiliser le périphérique à bord de capture de paquet sur l'ASR afin d'aider à dépanner des problèmes éventuels.

Créez une liste de contrôle d'accès (ACL) afin de réduire l'incidence et les captures sursaturées. La configuration est installée afin de capturer seulement les hellos de Multidiffusion entre deux sites. Ajustez votre adresse IP pour apparier les interfaces de joindre des voisins.

```
ip access-list extended CAPTURE
 permit ip host 172.16.64.84 host 225.0.0.1
 permit ip host 172.17.100.134 host 225.0.0.1
```

Installez la capture afin de renifler l'interface de joindre dans les deux directions sur les deux ASR

:

```
monitor capture 1 buffer circular access-list CAPTURE interface g0/0/0 both
```

Afin de commencer la capture, entrez :

```
monitor capture 1 start
```

```
*Nov 14 15:21:37.746: %BUFCAP-6-ENABLE: Capture Point 1 enabled.
```

<wait a few min>

```
monitor capture 1 stop
```

```
*Nov 14 15:22:03.213: %BUFCAP-6-DISABLE: Capture Point 1 disabled.
```

```
show mon cap 1 buffer brief
```

La sortie de mémoire tampon prouve que les hellos dans le de sortie de capture l'interface capturée. Il affiche les hellos destinés à l'adresse de multidiffusion 225.0.0.1. C'est le groupe témoin configuré. Voir les 13 premiers paquets dans la capture, et l'avis comment il y a seulement un résultat unidirectionnel. Hellos de 172.17.100.134 sont seulement vus. Une fois que le problème multicast au centre est résolu, le bonjour voisin apparaît au paquet le numéro 14.

```
ASR-1#show mon cap 1 buff bri
```

#	size	timestamp	source	destination	protocol
0	1456	0.000000	172.17.100.134	-> 225.0.0.1	GRE
1	1456	8.707016	172.17.100.134	-> 225.0.0.1	GRE
2	1456	16.880011	172.17.100.134	-> 225.0.0.1	GRE
3	1456	25.873008	172.17.100.134	-> 225.0.0.1	GRE
4	1456	34.645023	172.17.100.134	-> 225.0.0.1	GRE
5	1456	44.528024	172.17.100.134	-> 225.0.0.1	GRE
6	1456	52.137002	172.17.100.134	-> 225.0.0.1	GRE
7	1456	59.819010	172.17.100.134	-> 225.0.0.1	GRE
8	1456	68.641025	172.17.100.134	-> 225.0.0.1	GRE
9	1456	78.168998	172.17.100.134	-> 225.0.0.1	GRE
10	1456	85.966005	172.17.100.134	-> 225.0.0.1	GRE
11	1456	94.629032	172.17.100.134	-> 225.0.0.1	GRE
12	1456	102.370043	172.17.100.134	-> 225.0.0.1	GRE
13	1456	110.042005	172.17.100.134	-> 225.0.0.1	GRE
14	1456	111.492031	172.16.64.84	-> 225.0.0.1	GRE <---Mcast core
fixed and now see neighbor hellos					
15	1456	111.493038	172.17.100.134	-> 225.0.0.1	GRE
16	1456	112.491039	172.16.64.84	-> 225.0.0.1	GRE
17	1456	112.501033	172.17.100.134	-> 225.0.0.1	GRE
18	116	112.519037	172.17.100.134	-> 225.0.0.1	GRE
19	114	112.615026	172.16.64.84	-> 225.0.0.1	GRE
20	114	112.618031	172.17.100.134	-> 225.0.0.1	GRE
21	1456	113.491039	172.16.64.84	-> 225.0.0.1	GRE
22	1456	115.236047	172.17.100.134	-> 225.0.0.1	GRE
23	142	116.886008	172.17.100.134	-> 225.0.0.1	GRE
24	102	117.290045	172.17.100.134	-> 225.0.0.1	GRE
25	1456	118.124002	172.17.100.134	-> 225.0.0.1	GRE
26	1456	121.192043	172.17.100.134	-> 225.0.0.1	GRE
27	1456	122.443037	172.16.64.84	-> 225.0.0.1	GRE
28	1456	124.497035	172.17.100.134	-> 225.0.0.1	GRE
29	102	126.178052	172.17.100.134	-> 225.0.0.1	GRE
30	142	126.629032	172.17.100.134	-> 225.0.0.1	GRE
31	1456	127.312047	172.17.100.134	-> 225.0.0.1	GRE
32	1456	130.029997	172.17.100.134	-> 225.0.0.1	GRE
33	1456	131.165000	172.16.64.84	-> 225.0.0.1	GRE

```

34 1456 132.591025 172.17.100.134 -> 225.0.0.1 GRE
35 102 134.832010 172.17.100.134 -> 225.0.0.1 GRE
36 1456 135.856010 172.17.100.134 -> 225.0.0.1 GRE
37 142 136.174054 172.17.100.134 -> 225.0.0.1 GRE
38 1456 138.442030 172.17.100.134 -> 225.0.0.1 GRE
39 1456 140.769025 172.16.64.84 -> 225.0.0.1 GRE
40 1456 141.767010 172.17.100.134 -> 225.0.0.1 GRE
41 102 144.277046 172.17.100.134 -> 225.0.0.1 GRE
42 1456 144.996003 172.17.100.134 -> 225.0.0.1 GRE

```

ASR-1#

2#show mon cap 1 buff bri

Vérifiez l'état de Mroute sur OTV ASR

Quand vous établissez l'état de routage de Multidiffusion entre les voisins OTV, vous devez avoir l'état approprié PIM. Employez cette commande afin de vérifier l'état prévu PIM sur les ASR :

ASR-1#show otv

```

Overlay Interface Overlay1
  VPN name           : None
  VPN ID             : 2
  State              : UP
  AED Capable        : No, overlay DIS not elected
  IPv4 control group : 225.0.0.1
  Mcast data group range(s): 232.0.0.0/8
  Join interface(s)  : GigabitEthernet0/0/0
  Join IPv4 address  : 172.17.100.134
  Tunnel interface(s) : Tunnel0
  Encapsulation format : GRE/IPv4
  Site Bridge-Domain : 1
  Capability          : Multicast-reachable
  Is Adjacency Server : No
  Adj Server Configured : No
  Prim/Sec Adj Svr(s) : None

```

Notez la même erreur qu'avant : AED capable = aucun, DIS recouvert non élu. Ce que ce le moyen est que l'ASR ne peut pas devenir l'expéditeur AED, parce qu'il n'a pas assez d'informations sur son pair. Il est possible que l'interface interne ne soit pas en hausse, le domaine de passerelle de site est réduit/non créé, ou les deux sites ne peuvent pas se voir à travers l'ISP.

Regardez ASR-1 afin d'identifier le problème. Il prouve qu'aucun voisin PIM n'est vu. Ceci est prévu même lorsque cela fonctionne. C'est parce que PIM exécute le passif sur l'interface de joindre. Le passif PIM est le seul mode PIM pris en charge sur l'interface de joindre pour OTV.

ASR-1#show ip pim neigh

```

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      Interface      Uptime/Expires   Ver   DR
Address                               Prio/Mode

```

Afin de vérifier que des interfaces PIM sont configurées sur l'ASR-1, entrez :

ASR-1#show ip pim int

```

Address      Interface      Ver/  Nbr   Query  DR      DR
              Mode    Count Intvl Prior
172.17.100.134 GigabitEthernet0/0/0 v2/P  0     30     1     172.17.100.134
172.17.100.134 Tunnel0          v2/P  0     30     1     172.17.100.134
0.0.0.0      Overlay1        v2/P  0     30     1     0.0.0.0

```

L'état de mroute de l'ASR fournit une quantité d'informations en vue de le statut de Multidiffusion du lien. Dans cette sortie, vous ne voyez pas le voisin comme S, entrée G sur la table mroute des gens du pays ASR. Quand vous visualisez le compte de mroute pour le groupe témoin, vous voyez seulement les gens du pays joindre l'interface comme source aussi bien. Notez que le compte correspond aux paquets reçus au total expédié. Ceci signifie que vous êtes haut et expédition du côté local au domaine de Multidiffusion.

```
ASR-1#show 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,  
Y - Joined MDT-data group, y - Sending to MDT-data group,  
G - Received BGP C-Mroute, g - Sent BGP C-Mroute,  
Q - Received BGP S-A Route, q - Sent BGP S-A Route,  
V - RD & Vector, v - Vector
```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(* , 225.0.0.1), 00:20:29/stopped, RP 0.0.0.0, flags: DC
```

```
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
Tunnel0, Forward/Sparse-Dense, 00:20:29/00:02:55
```

```
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:20:29/Proxy
```

```
(172.17.100.134, 225.0.0.1), 00:16:25/00:02:19, flags: T
```

```
Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:16:25/Proxy
```

```
Tunnel0, Forward/Sparse-Dense, 00:16:25/00:02:55
```

```
(* , 224.0.1.40), 00:20:09/00:02:53, RP 0.0.0.0, flags: DPC
```

```
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list: Null
```

```
ASR-1#show ip mroute count
```

```
Use "show ip mfib count" to get better response time for a large number of mroutes.
```

```
IP Multicast Statistics
```

```
3 routes using 1828 bytes of memory
```

```
2 groups, 0.50 average sources per group
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

```
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
```

```
Group: 225.0.0.1, Source count: 1, Packets forwarded: 116, Packets received: 117
```

```
Source: 172.17.100.134/32, Forwarding: 116/0/1418/1, Other: 117/1/0
```

```
Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

Quand le principal problème multicast est résolu, vous voyez la sortie prévue de l'ASR.

```
ASR-1#show otv
```

```
Overlay Interface Overlay1
```

```
VPN name : None
```

```
VPN ID : 2
```

```
State : UP
```

```
AED Capable : Yes
```

```
IPv4 control group : 225.0.0.1
```

```
Mcast data group range(s): 232.0.0.0/8
```

```

Join interface(s)      : GigabitEthernet0/0/0
Join IPv4 address     : 172.17.100.134
Tunnel interface(s)  : Tunnel0
Encapsulation format  : GRE/IPv4
Site Bridge-Domain   : 1
Capability            : Multicast-reachable
Is Adjacency Server   : No
Adj Server Configured : No
Prim/Sec Adj Svr(s)  : None

```

Il ne restent aucun voisin PIM et l'examen médical, le recouvrement, et les interfaces de tunnel sont les interfaces locales PIM.

```
ASR-1#show ip pim neigh
```

```
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      Interface      Uptime/Expires  Ver  DR
Address                                     Prio/Mode
```

```
ASR-1#show ip pim int
```

```

Address      Interface      Ver/  Nbr  Query  DR  DR
              Mode  Count  Intvl Prior
172.17.100.134 GigabitEthernet0/0/0  v2/P  0    30     1   172.17.100.134
172.17.100.134 Tunnel0              v2/P  0    30     1   172.17.100.134
0.0.0.0       Overlay1          v2/P  0    30     1   0.0.0.

```

La table mroute et les compteurs fournissent des informations au sujet de l'état de Multidiffusion. La sortie affiche l'interface de joindre aussi bien que le voisin OTV au groupe témoin comme sources. Veillez-vous pour voir le point de rendez-vous (RP) dans le domaine voisin du Reverse Path Forwarding de site distant (RPF) (NBR) aussi bien. Vous également expédiez et recevez les compteurs assortis. Les deux sources devraient se monter au total reçu par groupe.

```
ASR-1#show 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,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector

```

```
Outgoing interface flags: H - Hardware switched, A - Assert winner
```

```
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode
```

```
(* , 225.0.0.1), 00:25:16/stopped, RP 0.0.0.0, flags: DC
```

```
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
Tunnel0, Forward/Sparse-Dense, 00:25:16/00:02:06
```

```
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:25:16/Proxy
```

```
(172.16.64.84, 225.0.0.1), 00:04:09/00:02:50, flags: T
```

```
Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.17.100.1
```

```
Outgoing interface list:
```

```
Tunnel0, Forward/Sparse-Dense, 00:04:09/00:02:06
```

```
(172.17.100.134, 225.0.0.1), 00:21:12/00:01:32, flags: T
```

```
Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
```

```
Outgoing interface list:
```

```
GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:21:12/Proxy
```

```
Tunnel0, Forward/Sparse-Dense, 00:21:12/00:02:06
```

```
(* , 224.0.1.40), 00:24:56/00:02:03, RP 0.0.0.0, flags: DPC  
Incoming interface: Null, RPF nbr 0.0.0.0  
Outgoing interface list: Null
```

```
ASR-1#show ip mroute count
```

Use "show ip mfib count" to get better response time for a large number of mroutes.

```
IP Multicast Statistics
```

```
4 routes using 2276 bytes of memory
```

```
2 groups, 1.00 average sources per group
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
```

```
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
```

```
Group: 225.0.0.1, Source count: 2, Packets forwarded: 295, Packets received:
```

```
297 <----- 32 + 263 = 295
```

```
Source: 172.16.64.84/32, Forwarding: 32/0/1372/1, Other: 32/0/0
```

```
Source: 172.17.100.134/32, Forwarding: 263/0/1137/3, Other: 264/1/0
```

```
Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

Créez une capture de paquet sur la Joindre-interface pour voir des paquets de données OTV

Puisqu'OTV est le trafic encapsulé, on le voit comme trafic d'Encapsulation de routage générique (GRE) avec une source d'interface de joindre à la destination du distant joignent l'interface. Il n'y a pas beaucoup que vous pouvez faire afin de voir le trafic spécifiquement. Une méthode que vous pouvez employer afin de vérifier si votre trafic la fait à travers OTV est d'installer une capture de paquet, spécifiquement avec une longueur de paquet qui est indépendant de vos structures de trafic en cours. Dans cet exemple, vous pouvez spécifier un paquet de Protocole ICMP (Internet Control Message Protocol) avec une taille de 700 et déterminer ce que vous pouvez filtrer hors de la capture. Ceci peut être utilisé afin de valider si un paquet le fait à travers le nuage OTV.

Afin d'installer votre filtre de liste d'accès entre vos deux joignez les interfaces, entrent :

```
ip access-list extended CAPTURE  
permit ip host 172.17.100.134 host 172.16.64.84
```

Afin d'installer votre session de surveillance pour filtrer votre taille spécifiée de 756, entrez :

```
monitor capture 1 buffer size 1 access-list CAPTURE limit packet-len 756  
interface g0/0/0 out
```

Afin de commencer la capture, entrez :

```
ASR-1#mon cap 1 start
```

```
*Nov 18 12:45:50.162: %BUFCAP-6-ENABLE: Capture Point 1 enabled.
```

Envoyez le ping spécifique avec une taille spécifiée. Puisqu'OTV ajoute une en-tête 42-byte avec un ICMP 8-byte avec une en-tête IP 20-byte, vous pouvez envoyer un ping classé à 700 et compter voir les données atteignent le nuage OTV avec une longueur de paquet de 756.

```
LAN-Sw2#ping 192.168.100.2 size 700 repeat 100
```

```
Type escape sequence to abort.
```

```
Sending 100, 700-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Success rate is 100 percent (100/100), round-trip min/avg/max = 10/19/30 ms
```

Afin d'arrêter la capture, entrez :

```
ASR-1#mon cap 1 stop
```

```
*Nov 18 12:46:02.084: %BUFCAP-6-DISABLE: Capture Point 1 disabled.
```

Dans la mémoire tampon de capture, vous voyez chacun des 100 paquets atteindre la capture du côté local. Vous devriez voir chacun des 100 paquets atteindre le côté distant aussi bien. Sinon, des recherches plus approfondies sont exigées dans le nuage OTV pour la perte de paquets.

```
ASR-1#show mon cap 1 buff bri
```

```
-----  
#   size  timestamp      source           destination      protocol  
-----  
0  756    0.000000    172.17.100.134  -> 172.16.64.84    GRE  
1  756    0.020995    172.17.100.134  -> 172.16.64.84    GRE  
2  756    0.042005    172.17.100.134  -> 172.16.64.84    GRE  
3  756    0.052991    172.17.100.134  -> 172.16.64.84    GRE  
<Output Omitted>  
97 756    1.886999    172.17.100.134  -> 172.16.64.84    GRE  
98 756    1.908009    172.17.100.134  -> 172.16.64.84    GRE  
99 756    1.931003    172.17.100.134  -> 172.16.64.84    GRE
```

Remarque: Ce test n'est pas 100% fiable parce que n'importe quel trafic qui apparie la longueur de 756 est capturé, ainsi l'utilisent avec prudence. Ce test est utilisé afin d'aider à recueillir des points d'informations seulement pour de principales questions possibles OTV.

[Informations connexes](#)

- [Configurer la virtualisation de transport de recouvrement](#)
- [Compréhension des circuits virtuels d'Ethernets \(EVC\)](#)
- [Support et documentation techniques - Cisco Systems](#)