

Exemple de configuration de multidiffusion OTV ASR 1000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Schéma du réseau avec connectivité de base de couche 2/couche 3](#)

[Connectivité L2/L3 de base](#)

[Configuration minimale de multidiffusion OTV](#)

[Vérification OTV](#)

[Schéma du réseau avec OTV](#)

[Commandes de vérification et sortie attendue](#)

[Problème courant](#)

[Dépannage](#)

[Créer une capture de paquets sur l'interface de jointure afin de voir les HELLO OTV](#)

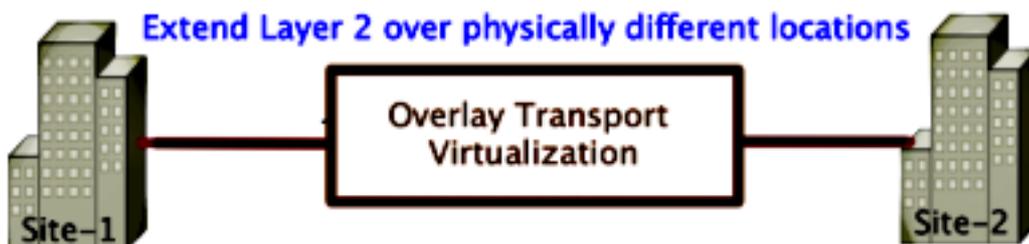
[Vérifier l'état Mroute sur OTV ASR](#)

[Créer une capture de paquets sur l'interface de jointure pour afficher les paquets de données OTV](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le mode de multidiffusion OTV (Overlay Transport Virtualization) sur la plate-forme Cisco Aggregation Services Router (ASR) 1000. OTV étend la topologie de couche 2 (L2) sur les différents sites physiques, ce qui permet aux périphériques de communiquer au niveau de couche 2 via un fournisseur de couche 3 (L3). Les périphériques du site 1 pensent qu'ils se trouvent sur le même domaine de diffusion que ceux du site 2.



Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de la connexion virtuelle Ethernet (EVC)
- Configuration de base de couche 2 et de couche 3 sur la plate-forme ASR
- Connaissances de base en configuration IGMP (Internet Group Management Protocol) version 3 et PIM (Protocol Independent Multicast)

Components Used

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

Votre système doit disposer des conditions suivantes pour mettre en oeuvre la fonctionnalité OTV sur l'ASR 1000 :

- Cisco IOS-XE version 3.5S ou ultérieure
- Unité de transmission maximale (MTU) de 1542 ou plus

Note: OTV ajoute un en-tête de 42 octets avec le bit DF (Do Not Fragment bit) à tous les paquets encapsulés. Afin de transporter des paquets de 1 500 octets via la superposition, le réseau de transit doit prendre en charge une unité de transmission maximale (MTU) de 1 542 ou plus. Afin de permettre la fragmentation à travers OTV, vous devez activer **otv fragmentation join-interface <interface>**.

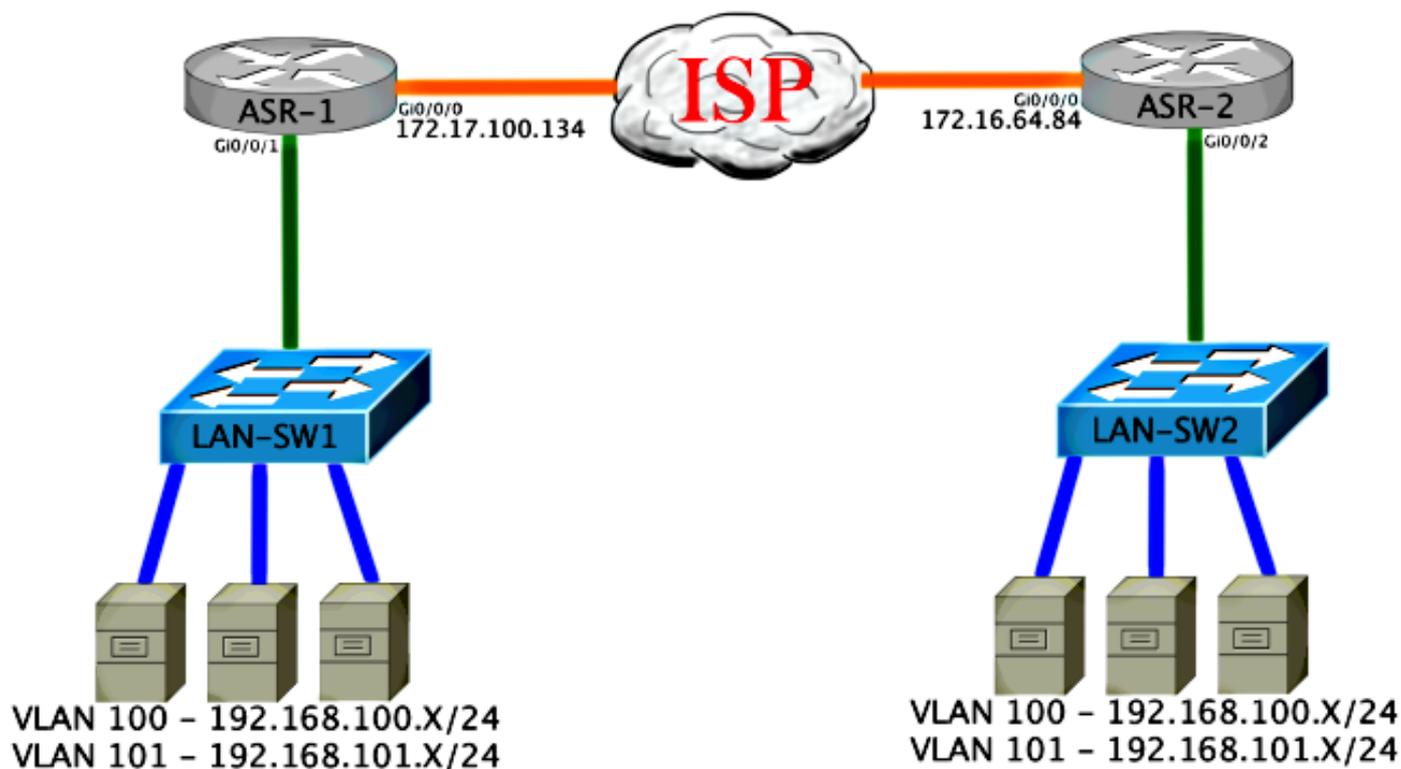
- Accessibilité de monodiffusion et de multidiffusion entre les sites

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cette section décrit comment configurer le mode de multidiffusion OTV.

Schéma du réseau avec connectivité de base de couche 2/couche 3



Connectivité L2/L3 de base

Commencez par une configuration de base. L'interface interne de l'ASR est configurée pour les instances de service pour le trafic dot1q. L'interface de jointure OTV est l'interface externe de couche 3 du WAN.

```
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
```

Étant donné qu'OTV ajoute un en-tête de 42 octets, vous devez vérifier que le fournisseur d'accès à Internet (FAI) dépasse la taille MTU minimale d'un site à l'autre. Pour effectuer cette vérification, envoyez un paquet de taille 1542 avec le bit DF défini. Cela donne au FAI la charge utile requise plus la balise **ne pas fragmenter** sur le paquet afin de simuler un paquet OTV. Si vous ne pouvez pas envoyer de requête ping sans le bit DF, vous avez un problème de routage. Si vous pouvez envoyer une requête ping sans lui, mais que vous ne pouvez pas envoyer de requête ping avec le bit DF défini, vous avez un problème de MTU. Une fois que vous avez réussi, vous êtes prêt à ajouter le mode monodiffusion OTV à vos ASR de site.

```
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 instances de service pour les paquets balisés L2 dot1q. Il crée également un domaine de pont de site interne. Dans cet exemple, il s'agit du VLAN1 non balisé. Le domaine de pont de site interne est utilisé pour la communication de plusieurs périphériques OTV sur le même site. Cela leur permet de communiquer et de déterminer quel périphérique est l'AED (Authoritative Edge Device) pour quel domaine de pont.

L'instance de service doit être configurée dans un domaine de pont qui utilise la superposition.

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

Il s'agit d'une configuration de base qui ne nécessite que quelques commandes pour configurer OTV et joindre / interfaces internes.

Configurez le domaine de pont du site local. Dans cet exemple, il s'agit de VLAN1 sur le LAN. L'identificateur de site est spécifique à chaque emplacement physique. Dans cet exemple, deux emplacements distants sont physiquement indépendants les uns des autres. Les sites 1 et 2 sont configurés en conséquence. La multidiffusion doit également être configurée conformément aux exigences d'OTV.

ASR-1

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

Construisez la superposition pour chaque côté. Configurez la superposition, appliquez l'interface de jointure et ajoutez les groupes de contrôle et de données de chaque côté.

Ajoutez les deux domaines de pont que vous souhaitez étendre. Notez que vous n'étendez pas le domaine du pont de site, seulement les deux VLAN nécessaires. Vous créez une instance de service distincte pour les interfaces de superposition pour appeler le domaine de pont 200 et 201. 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
```

Note: N'étendez PAS le VLAN de site sur l'interface de superposition. Cela provoque un

conflit entre les deux ASR, car ils pensent que chaque côté distant se trouve sur le même site.

À ce stade, la contiguïté de multidiffusion ASR à ASR OTV est complète et fonctionnelle. Les voisins sont détectés et l'ASR doit être compatible AED 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
```

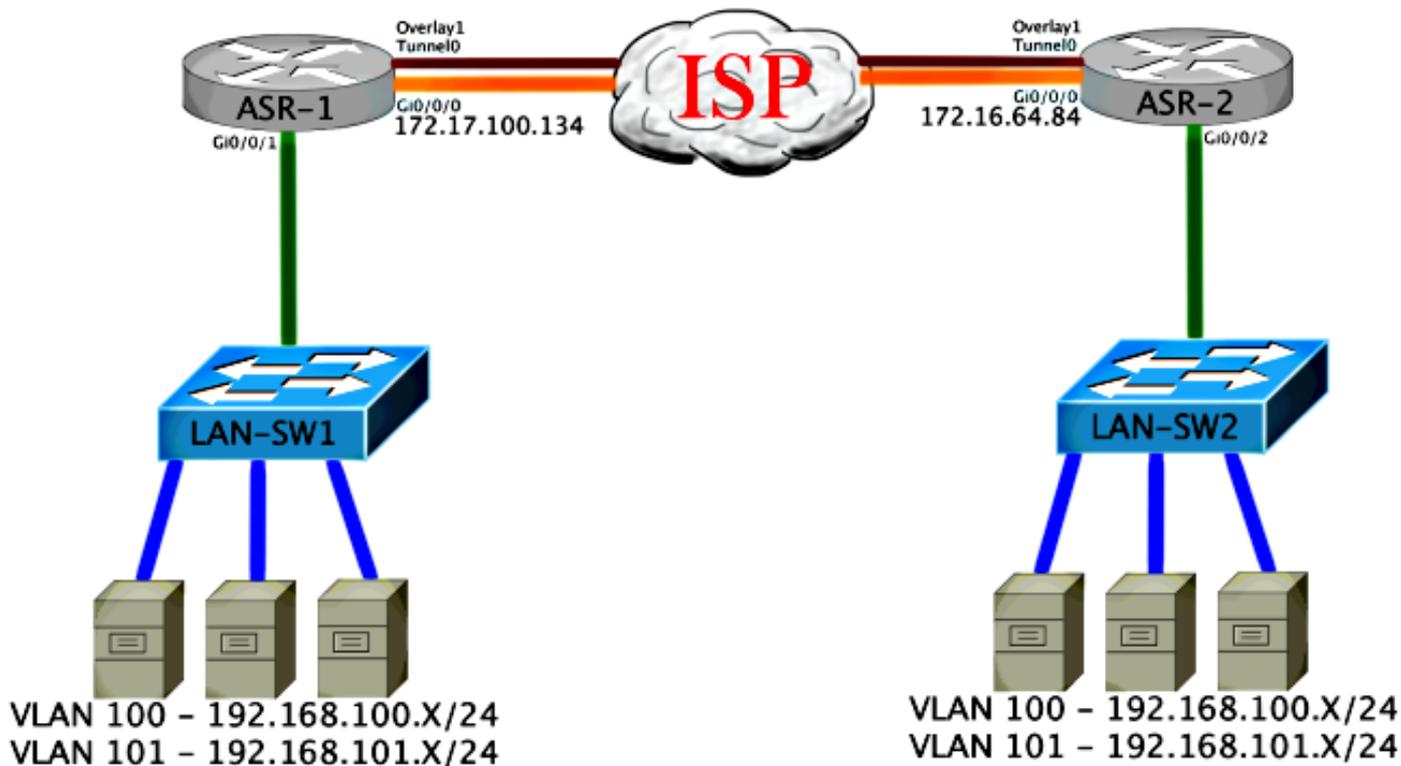
```
ASR-2#show otv
```

```
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 du réseau avec OTV



Commandes de vérification et sortie attendue

Ce résultat montre que les VLAN 100 et 101 sont étendus. L'ASR est l'AED, et l'interface interne et l'instance de service qui mappe les VLAN sont affichées dans le résultat.

```
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, étendez les VLAN et exécutez une requête ping de site à site. L'hôte 192.168.100.2 se trouve sur le site 1 et l'hôte 192.168.100.3 se trouve sur le site 2. Les premières requêtes ping sont censées échouer lorsque vous construisez le protocole ARP (Address Resolution Protocol) localement et à travers OTV de 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 MAC et les tables de routage OTV sont correctement construites avec le périphérique local, apprenez l'adresse MAC du périphérique distant à l'aide de la commande **show otv route**.

```
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

Le message d'erreur OTV ne forme pas dans le résultat indique que l'ASR n'est pas compatible AED. Cela signifie que l'ASR ne transmet pas les VLAN à travers l'OTV. Il existe plusieurs causes possibles, mais la plus courante est que les ASR n'ont pas de connectivité entre les sites. Vérifiez la connectivité de couche 3 et le trafic de multidiffusion bloqué possible. Une autre cause possible de cette condition est lorsque le domaine de pont de site interne n'est pas configuré. Cela crée une condition dans laquelle l'ASR ne peut pas devenir l'AED, car il n'est pas certain qu'il soit le seul ASR sur le site ou non.

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

Dépannage

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

Créer une capture de paquets sur l'interface de jointure afin de voir les HELLO OTV

Vous pouvez utiliser le périphérique de capture de paquets intégré sur l'ASR afin d'aider à résoudre les problèmes éventuels.

Créez une liste de contrôle d'accès (ACL) afin de minimiser l'impact et les captures sursaturées. La configuration est configurée afin de capturer uniquement les HELLO de multidiffusion entre deux sites. Ajustez votre adresse IP pour qu'elle corresponde aux interfaces de jonction 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
```

Configurez la capture afin de détecter l'interface de jointure dans les deux directions sur les deux ASR :

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

Pour démarrer la capture, saisissez :

```
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 la mémoire tampon montre que les paquets Hello de la capture sortent de l'interface capturée. Il affiche les paquets Hello destinés à l'adresse de multidiffusion 225.0.0.1. Il s'agit du groupe de contrôle configuré. Reportez-vous aux 13 premiers paquets de la capture et remarquez qu'il n'y a qu'une sortie unidirectionnelle. Les HELLO de 172.17.100.134 ne sont visibles que. Une fois le problème de multidiffusion dans le coeur résolu, le paquet Hello du voisin apparaît au numéro de paquet 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**

Vérifier l'état Mroute sur OTV ASR

Lorsque vous créez l'état de routage de multidiffusion entre les voisins OTV, vous devez disposer de l'état PIM approprié. Utilisez cette commande afin de vérifier l'état PIM attendu 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 que précédemment : AED compatible = Non, DIS superposé non sélectionné. Cela signifie que l'ASR ne peut pas devenir le redirecteur AED, car il ne dispose pas d'informations suffisantes sur son homologue. Il est possible que l'interface interne ne soit pas activée, que le domaine du pont de site soit désactivé/ne soit pas créé, ou que les deux sites ne puissent pas se voir à travers le FAI.

Examinez ASR-1 afin d'identifier le problème. Il montre qu'aucun voisin PIM n'est vu. On s'y attend même quand cela fonctionne. Ceci est dû au fait que PIM fonctionne de manière passive sur l'interface de jointure. PIM passive est le seul mode PIM pris en charge sur l'interface de jointure 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 les interfaces PIM sont configurées sur l'ASR-1, saisissez :

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

Address	Interface	Ver/ Mode	Nbr Count	Query Intvl	DR Prior	DR
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 mroute de l'ASR fournit une abondance d'informations en ce qui concerne l'état de multidiffusion de la liaison. Dans cette sortie, vous ne voyez pas le voisin comme une entrée S,G dans la table de routage ASR locale. Lorsque vous affichez le nombre de mroute pour le groupe de contrôle, vous ne voyez que l'interface de jointure locale comme source également. Notez que le nombre correspond aux paquets reçus avec le total transféré. Cela signifie que vous êtes actif et que vous êtes en train de transférer 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

Lorsque le problème de multidiffusion principale est résolu, le résultat attendu de l'ASR apparaît.

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 n'y a toujours pas de voisins PIM et les interfaces physiques, de superposition et de tunnel sont des interfaces PIM locales.

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 Address	Interface	Uptime/Expires	Ver	DR	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 sur l'état de multidiffusion. Le résultat montre l'interface de jointure ainsi que le voisin OTV dans le groupe de contrôle en tant que sources. Assurez-vous que vous voyez également le champ Rendezvous Point (RP) dans le champ NBR (Reverse Path Forwarding) du site distant. Vous transférez et recevez également des compteurs correspondants. Les deux sources devraient totaliser le total reçu par le 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

Créer une capture de paquets sur l'interface de jointure pour afficher les paquets de données OTV

Comme OTV est un trafic encapsulé, il est considéré comme un trafic GRE (Generic Routing Encapsulation) avec une source de l'interface de jointure vers la destination de l'interface de jointure distante. Il n'y a pas grand-chose à faire pour voir le trafic spécifiquement. Une méthode que vous pouvez utiliser pour vérifier si votre trafic est acheminé via OTV est de configurer une capture de paquets, en particulier avec une taille de paquet indépendante de vos modèles de trafic actuels. Dans cet exemple, vous pouvez spécifier un paquet ICMP (Internet Control Message Protocol) d'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 parvient à travers le cloud OTV.

Afin de configurer votre filtre de liste d'accès entre vos deux interfaces de jointure, saisissez :

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

Afin de configurer 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
```

Pour démarrer la capture, saisissez :

```
ASR-1#mon cap 1 start
*Nov 18 12:45:50.162: %BUFCAP-6-ENABLE: Capture Point 1 enabled.
```

Envoyez la requête ping spécifique avec une taille spécifiée. Étant donné qu'OTV ajoute un en-tête de 42 octets avec un ICMP de 8 octets avec un en-tête IP de 20 octets, vous pouvez envoyer une requête ping de taille 700 et vous pouvez vous attendre à voir les données atteindre le cloud OTV avec une taille 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
```

Pour arrêter la capture, saisissez :

```
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, les 100 paquets atteignent la capture du côté local. Vous devriez voir que les 100 paquets atteignent également le côté distant. Si ce n'est pas le cas, il est nécessaire d'approfondir les recherches dans le cloud OTV en cas de 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
```

Note: Ce test n'est pas fiable à 100 %, car tout trafic correspondant à la longueur de 756 est capturé, utilisez-le avec prudence. Ce test est utilisé afin d'aider à collecter des points de données uniquement pour les problèmes de base OTV possibles.

Informations connexes

- [Configuration de la virtualisation du transport de superposition](#)
- [Présentation des circuits virtuels Ethernet \(EVC\)](#)
- [Support et documentation techniques - Cisco Systems](#)