Configuration de la virtualisation du transport de superposition avec ASR 1000

Table des matières

Introduction

Ce document décrit les topologies réseau OTV (Overlay Transport Virtualization) prises en charge sur les routeurs des gammes ASR1000 et Catalyst 8300/8500.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASR1000, IOS® XE version 16.10.1a et ultérieure
- Catalyst 8300, IOS® XE version 17.5.1a et ultérieure
- Catalyst 8500, IOS® XE version 17.6.1a et ultérieure

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

ASR1000 prend en charge OTV depuis Cisco IOS® XE version 3.5. Le routeur de la gamme Catalyst 8300 commence la prise en charge avec IOS® XE17.5.1a et les routes de la gamme Catalyst 8500 commencent la prise en charge avec IOS® XE version 17.6.1a.

OTV fournit une connectivité de couche 2 entre les sites réseau distants par routage basé sur les adresses MAC et par transfert encapsulé IP (MAC-in-IP) sur un réseau de transport afin de prendre en charge les applications qui nécessitent une contiguïté de couche 2, telles que les clusters et la virtualisation. OTV utilise un protocole de plan de contrôle de superposition pour apprendre et propager les informations de routage MAC sur le réseau de superposition. Le protocole de plan de contrôle OTV utilise des messages IS-IS (Intermediate-System-to-Intermediate-System) pour établir des contiguïtés avec des sites distants et pour envoyer des mises à jour de route MAC à ces sites. OTV crée des contiguïtés de couche 2 vers des sites distants sur le réseau de superposition en détectant automatiquement les périphériques OTV distants.

Les avantages d'OTV pour l'extension de couche 2 sont les suivants :

- Aucune exigence MPLS
- Aucune configuration Ethernet sur commutation multiprotocole par étiquette (EoMPLS) complexe pour le maillage
- Aucun déploiement VPLS (Virtual Private LAN Services) complexe pour les extensions de couche 2
- Isolation Spanning Tree native
    - pas besoin de configurer explicitement les filtres BPDU (Bridge Data Protocol Unit)
    - isolation par défaut des problèmes de spanning tree vers un data center donné
- Isolation de diffusion monodiffusion inconnue native
    - Les paquets MAC de monodiffusion inconnus ne sont pas transférés
    - la prise en charge du transfert de monodiffusion inconnue par MAC est autorisée
- Optimisation du protocole ARP (Address Resolution Protocol) avec la mise en cache ARP OTV
    - Réduit le trafic WAN inutile
- Mise en service simplifiée de l'isolation FHRP (First Hop Redundancy Protocol)
- Ajout simplifié de sites
- Configuration de redondance simplifiée

- Possibilité d'avoir un « drop in appliance » pour les migrations lorsque des services temporaires sont requis

Exigences

Les éléments suivants sont les règles principales à garder à l'esprit lors de la conception d'un déploiement OTV. Si ces règles sont respectées, la conception et le déploiement sont rationalisés.

- Une et une seule interface peuvent être utilisées pour transmettre le trafic encapsulé OTV, appelé interface de jonction, pour toutes les interfaces OTV Overlay configurées
- Une et une seule interface peuvent être utilisées pour configurer les instances de service de couche 2 du centre de données pour le VLAN du site OTV et les VLAN étendus entre les centres de données pour toutes les interfaces OTV Overlay configurées
- Les canaux de port peuvent être utilisés pour la redondance d'interface et la connexion aux commutateurs VSS ou VPC et sont pris en charge en tant qu'interface unique pour la connectivité.
- Tous les routeurs OTV doivent être joignables via l'interface de jonction
- Le protocole Spanning Tree doit être configuré sur le routeur OTV qui pointe vers le data center
- La surveillance et l'interrogation IGMP doivent être configurées pour transférer correctement le trafic de multidiffusion du data center
- Un data center donné peut être configuré avec 1 ou 2 routeurs OTV. Avec deux routeurs, ils distribuent le transfert VLAN de manière impaire/paire en fonction du numéro de VLAN. Chaque routeur OTV d'un data center sert de sauvegarde pour l'autre.
- Les paires multihébergées doivent être configurées avec le même identificateur de site OTV
- ASR1000/Catalyst 8300/Catalyst 8500 et Nexus 7000 peuvent participer au même réseau OTV
    - Nexus 7000 ne prenant pas en charge la fragmentation ou le cryptage OTV, ces fonctionnalités ne peuvent pas être utilisées dans un déploiement « hybride ».

Certaines conceptions de connectivité dos à dos prises en charge ne respectent pas les règles indiquées. Bien que ces configurations soient prises en charge, elles ne sont pas recommandées. Vous trouverez plus de détails à ce sujet dans la section suivante, « Topologie de monodiffusion à cas spécial ».

On ne soulignera jamais assez que le logiciel OTV actuel a la restriction d'interface « un et un seul » lors de la configuration des interfaces de jointure et d'accès L2 pour OTV. Une interface Port-channel peut être utilisée pour la redondance. La connexion du Port-channel aux Nexus 7000 dans un VPC est prise en charge. Une connexion port-channel de base à un seul commutateur est également prise en charge.

Types d'implémentation OTV

OTV nécessite une interface de jointure unique et une interface L2 unique. Un seul de ces routeurs peut être pris en charge par routeur OTV. OTV exige également qu'un VLAN de site soit

configuré de sorte que les routeurs OTV multirésidences puissent communiquer entre eux via le réseau local. Même les routeurs OTV à hébergement unique doivent avoir le VLAN du site OTV configuré. En outre, un identifiant de site unique doit être configuré pour chaque site ou centre de données. Les routeurs OTV à double hébergement doivent utiliser le même identificateur de site et être capables de communiquer sur le même VLAN.

La configuration suivante fournit la configuration fondamentale de base nécessaire pour OTV. Cependant, elle n'est pas complète car la configuration principale de monodiffusion ou de multidiffusion doit être ajoutée. Elles sont détaillées dans les sections suivantes de ce document.

```
otv site bridge-domain 100
otv site-identifier 0000.0000.1111
!
interface Overlay1
  no ip address
  otv join-interface GigabitEthernet0/0/0
  service instance 99 ethernet
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 90 ethernet
    encapsulation dot1q 90
    bridge-domain 90
!
interface GigabitEthernet1/0/1
  no ip address
  negotiation auto
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  !
  service instance 99 ethernet
    encapsulation dot1q 99
    bridge-domain 99
  !
  service instance 98 ethernet
    encapsulation dot1q 98 second-dot1q 1098
    rewrite ingress tag trans 2-to-1 dot1q 90 symmetric
    bridge-domain 90
```

La configuration de l'instance de service est utilisée pour toute la configuration de l'interface L2 avec OTV.

Chaque instance de service sur l'interface L2 doit être associée à une encapsulation à étiquette unique ou double spécifique.

Chacune de ces instances de service doit à son tour être associée à un domaine de pont.

Ce domaine-pont est utilisé sur une instance de service configurée sur l'interface de superposition.

Le domaine-pont est la colle qui relie l'instance de service de superposition à l'instance de service

d'interface de couche 2.

L'encapsulation du trafic sur l'interface de superposition doit correspondre à l'encapsulation du trafic après réécriture en entrée sur l'interface L2.

Dans l'exemple, le trafic qui entre sur l'instance de service 99 Gig1/0/1 a un VLAN 802.1Q unique de 99 et le domaine de pont 99. L'instance de service correspondante avec le domaine de pont 99 sur l'interface de superposition est également configurée pour un VLAN 802.1Q unique de 99. Ce cas est le plus simple.

Dans l'exemple, le trafic qui entre sur l'instance de service 98 Gig1/0/1 a un double VLAN 802.1Q de 99 et 1098 et le domaine de pont 90. L'instance de service correspondante avec le domaine de pont 90 sur l'interface de superposition est configurée pour un seul VLAN 802.1Q de 90. Il est clair que ce ne sont pas les mêmes. La commande rewrite ingress garantit que les balises sont correctement traduites lorsque le trafic passe par l'interface d'entrée. Le trafic entrant dans l'interface de couche 2 est remplacé par les VLAN 802.1Q 98/1098 avec un VLAN unique de 90. Le mot clé symétrique garantit que le trafic sortant de l'interface de couche 2 est remplacé par le VLAN unique 802.1Q de 90 avec 98/1098.

Toutes les instances de service avec plusieurs VLAN 802.1Q étendus par OTV doivent utiliser la commande rewrite ingress. L'encapsulation OTV ne prend en charge qu'un seul identificateur VLAN. Pour cette raison, toute configuration de double VLAN sur les interfaces L2 doit être réécrite dans une balise unique sur l'instance de service d'interface de superposition. Cela empêche la prise en charge de configurations VLAN ambiguës.

Pour plus d'informations sur la réécriture des balises, consultez le document suivant : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

Dans cet exemple, le domaine de pont du site OTV est 100.

- Le domaine-pont du site OTV est configuré uniquement sur l'interface L2.
- Le domaine-pont du site OTV ne doit jamais être configuré sur l'interface de superposition, ce qui rend le déploiement OTV instable.
- Le VLAN du site OTV doit être connecté uniquement aux routeurs OTV et ne doit pas transporter d'autre trafic de data center/utilisateur.
- Le VLAN du site OTV doit se trouver sur la même interface physique que les VLAN étendus OTV.

Multidomicile

Un data center peut être connecté à un seul hôte OTV ou jusqu'à 2 hôtes pour la redondance, également appelée Multihome. La multihabitation est utilisée pour la résilience et l'équilibrage de charge. Lorsque plusieurs périphériques de périphérie sont présents sur un site et participent tous deux au même réseau de superposition, le site est considéré comme multirésident. OTV Multihome répartit les VLAN entre les deux routeurs OTV qui appartiennent au même site de manière impaire/paire en fonction du numéro de VLAN. Un périphérique de périphérie est sélectionné comme AED pour tous les VLAN impairs, tandis que l'autre routeur OTV est sélectionné comme AED pour tous les VLAN pairs. Chaque AED est également en veille pour les

VLAN actifs sur l’autre routeur. En cas de défaillance d’une liaison ou d’un noeud dans l’un des AED, l’AED de secours devient actif pour tous les VLAN.

Si deux ASR1000 sont connectés dans le même data center pour effectuer une connexion multidomicile, il n'est pas nécessaire d'établir une liaison dédiée entre les deux ASR1000. OTV utilise le VLAN du site OTV qui est propagé via l'interface interne et la communication via l'interface de jointure pour déterminer quels routeurs sont responsables des VLAN pairs et impairs.

Les ASR1000 et les Nexus 7000 ne peuvent pas être mélangés dans le même data center avec OTV configuré sur les deux routeurs comme sauvegarde de l'autre. Le multihome dans un data center donné est pris en charge pour les plates-formes correspondantes (ASR1000 ou Nexus 7000). Vous pouvez avoir des ASR1000 dans un data center et des Nexus 7000 dans un autre data center. L'interopérabilité entre ces deux plates-formes a été testée et prise en charge. Certains data centers peuvent être multihébergés tandis que d'autres sont monohébergés.

Les paires de routeurs ASR1000 multirésident doivent exécuter la même version du logiciel Cisco IOS® XE.

Si vous utilisez le mode Multihome, il est fortement recommandé d'activer le protocole Spanning Tree sur les routeurs OTV, car cela permet au routeur OTV d'envoyer une notification de modification de topologie (TCN), ce qui permet au périphérique de commutation L2 adjacent (ainsi qu'aux autres commutateurs du protocole Spanning Tree) de réduire son compteur d'ancienneté de la valeur par défaut à 15 secondes. Ceci augmente considérablement la convergence de vitesse en cas de défaillance ou de récupération entre les paires multirésidentes. Le Spanning Tree peut être activé pour toutes les instances de service configurées (connectées à OTV ou autre) par l'ajout de la ligne suivante à la configuration globale.

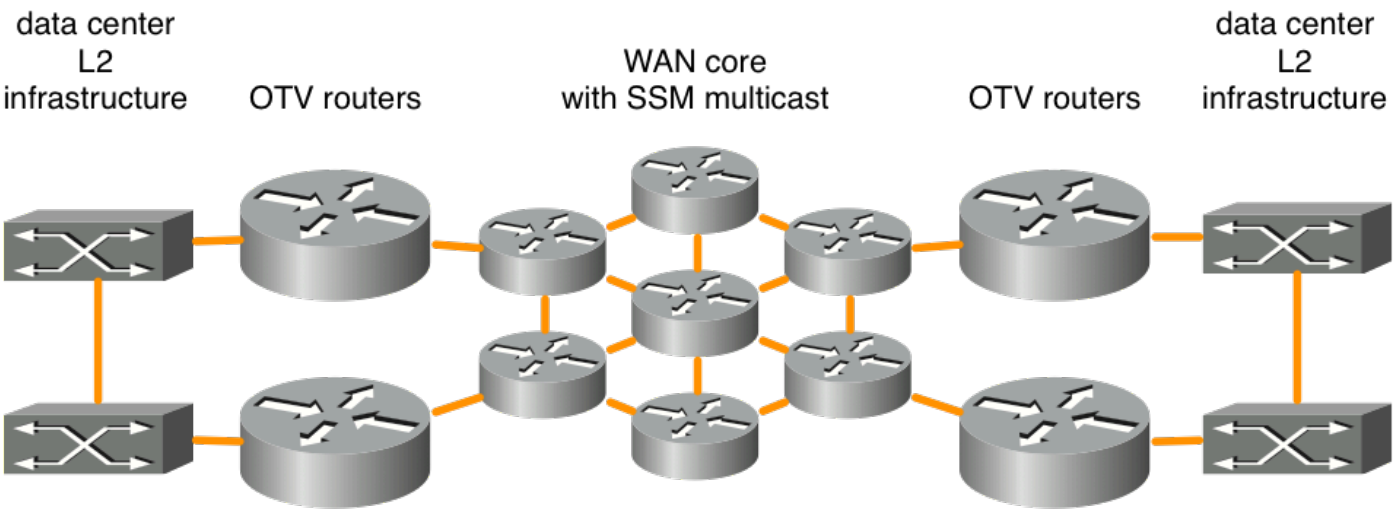
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

Aucune configuration spécifique par VLAN ou par instance de service n'est requise.

Coeur de multidiffusion

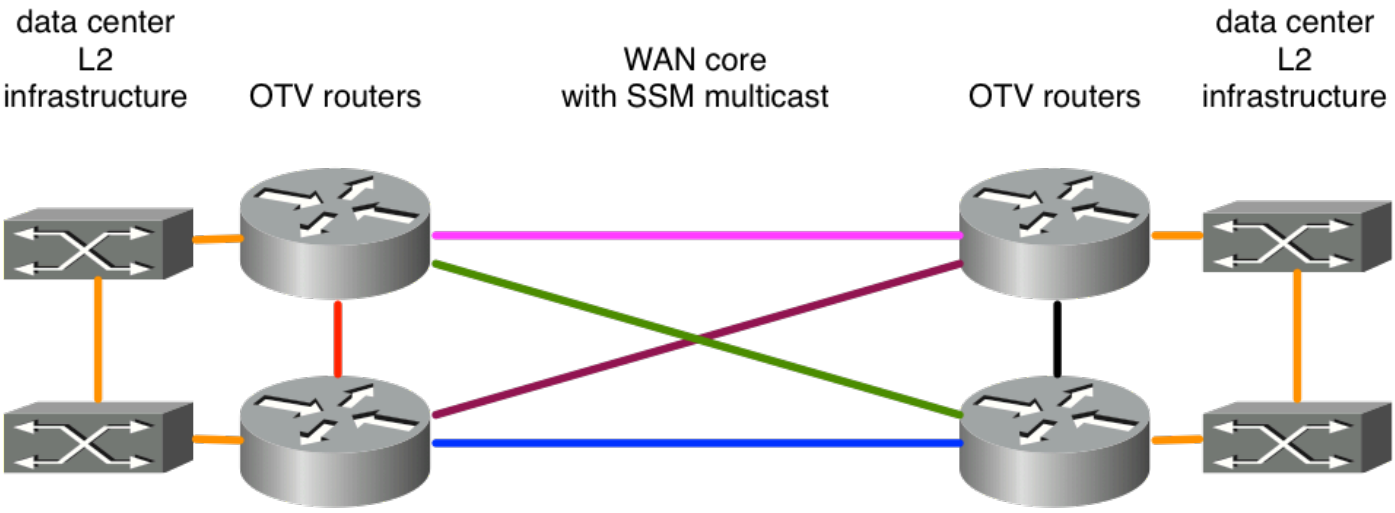
Un réseau multidiffusion nécessite une connectivité maillée complète sur le WAN. Tous les routeurs OTV doivent être connectés ensemble via l'interface de jonction.

Figure 1. Topologie de réseau multidiffusion prise en charge



Cette figure présente un exemple de deux data centers connectés par un coeur en maillage global. La multidiffusion indépendante du protocole (PIM) SSM (Source Specific Multicast) est exécutée entre les routeurs OTV et les routeurs principaux WAN. Un nombre illimité de routeurs principaux est pris en charge tant qu'il existe une connectivité à maillage global. Il n'existe aucune exigence explicite de latence maximale pour la connectivité OTV sur le coeur du WAN.

Figure 2. Topologie de réseau multidiffusion non prise en charge



Comme ASR1000/OTV s'attend à recevoir des messages de multidiffusion sur une seule interface de jointure de tous ses homologues, dans l'exemple, cela entraînerait un déploiement OTV instable. Supposons que les liaisons est-ouest en rose et bleu ont été configurées comme interfaces de jointure. En cas d'échec de la liaison rose, le routeur ne peut plus recevoir de mises à jour OTV sur cette interface. Un autre chemin via les liaisons vertes ou violettes serait inacceptable car l'interface de jointure est explicitement configurée. Les mises à jour doivent être reçues sur cette interface. L'utilisation d'interfaces de bouclage comme interface de jointure n'est pas prise en charge pour le moment.

Si les utilisateurs ne sont pas propriétaires de leur réseau fédérateur, ils doivent s'assurer que leur fournisseur de services prend en charge la multidiffusion dans leur coeur de réseau et qu'il peut répondre aux messages de requête IGMP (Internet Group Management Protocol). OTV sur ASR1000 agit en tant qu'hôte de multidiffusion (transfère les messages de jointure IGMP) et non

en tant que routeur de multidiffusion vers la topologie de multidiffusion WAN principale.

Le réseau de transport entre les routeurs OTV doit prendre en charge le mode intermédiaire PIM (Any Source Multicast [ASM]) pour le groupe de multidiffusion du fournisseur et SSM pour le groupe de distribution.

Les coeurs de multidiffusion nécessitent une configuration spécifique sur l'interface de superposition pour un groupe de contrôle, ainsi qu'une plage de groupes de multidiffusion de données utilisés pour transférer des données.

```
ip multicast-routing distributed
ip pim ssm default
!
interface Port-channel60
 encapsulation dot1Q 30
 ip address 10.0.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
!
interface Overlay99
 no ip address
 otv control-group 239.1.1.1
 otv data-group 232.192.1.0/24
 otv join-interface Port-ch60
```

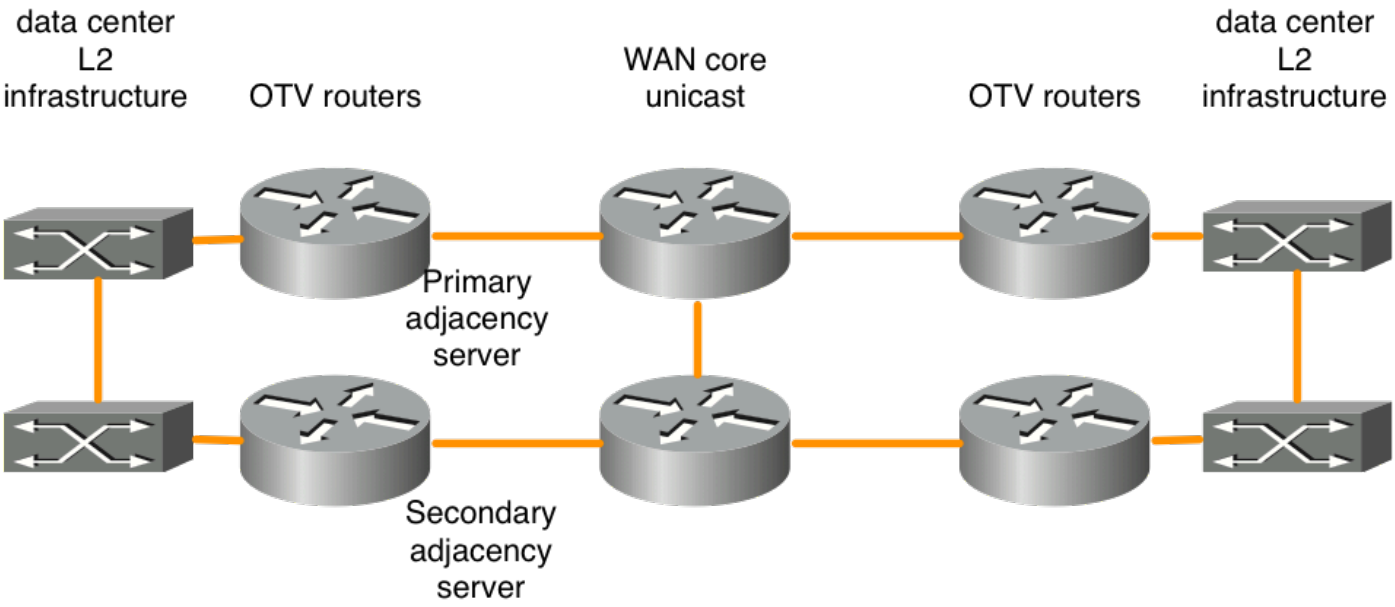
Les déploiements OTV multidiffusion nécessitent que l'interface de jonction soit configurée en tant qu'interface passive PIM. IGMP peut être configuré pour différentes versions selon les besoins. Un groupe de contrôle et un groupe de données doivent être configurés sur l'interface de superposition. Le groupe de contrôle est un groupe de multidiffusion unique utilisé pour la gestion OTV. Le groupe de données est une plage d'adresses de multidiffusion utilisée pour transporter les données utilisateur entre les data centers. Si le groupe de données ne se trouve pas dans l'espace IP 232.0.0.0/8, la commande supplémentaire « ip pim ssm range » doit être configurée pour inclure la plage requise par OTV.

Le réseau de transport entre les routeurs OTV doit prendre en charge le mode intermédiaire PIM (Any Source Multicast [ASM]) pour le groupe de multidiffusion du fournisseur et le mode SSM (Source Specific Multicast) pour le groupe de distribution.

Coeur de monodiffusion avec serveurs de contiguïté

Cisco IOS® XE 3.9 a ajouté la prise en charge d'OTV avec un coeur de monodiffusion. Les coeurs de monodiffusion et de multidiffusion pour OTV continuent d'être pris en charge pour toutes les plates-formes ASR1000 et les versions futures de Cisco IOS® XE 3.9.

Figure 3. Topologie de réseau monodiffusion



La fonctionnalité Serveur de contiguïté OTV permet le transport en monodiffusion uniquement entre la périphérie OTV. Les routeurs OTV configurés avec le rôle de serveur de contiguïté conservent une liste de tous les routeurs OTV connus. Ils fournissent cette liste à tous les routeurs OTV enregistrés afin qu'ils disposent d'une liste de périphériques qui doivent recevoir le trafic de diffusion et de multidiffusion répliqué.

Le plan de contrôle OTV sur un transport de monodiffusion uniquement fonctionne exactement de la même manière que OTV avec le coeur de multidiffusion, à ceci près que dans un réseau de coeur de monodiffusion, chaque périphérique de périphérie OTV doit créer plusieurs copies de chaque paquet de plan de contrôle et les monodiffuser vers chaque périphérique de périphérie distant dans la même superposition logique.

Dans le même ordre d'idées, tout trafic de multidiffusion provenant du data center est répliqué sur le routeur OTV local et plusieurs copies sont envoyées à chacun des data centers distants. Bien que cela soit moins efficace que de dépendre du coeur du WAN pour effectuer la réplication, la configuration et la gestion du coeur du réseau de multidiffusion ne sont pas nécessaires. S'il n'y a qu'une petite quantité de trafic de multidiffusion de centre de données ou qu'il n'y a qu'un petit nombre d'emplacements de centre de données (quatre ou moins), un coeur de monodiffusion pour le transfert OTV est généralement le meilleur choix. Dans l'ensemble, la simplification opérationnelle du modèle de monodiffusion uniquement rend l'option de déploiement de coeur de monodiffusion préférée dans les scénarios où la connectivité d'extension de réseau local n'est requise qu'entre quatre data centers ou moins. Il est recommandé de configurer au moins deux serveurs de contiguïté, un serveur principal et un serveur de sauvegarde. Il n'y a pas d'option pour la configuration du serveur de contiguïté actif/actif.

Les routeurs OTV doivent être configurés en conséquence pour être correctement identifiés et enregistrés auprès du serveur de contiguïté approprié.

	Serveur de contiguïté principal	Serveur de contiguïté secondaire	Autres routeurs OTV
Adresse IP de l'interface OTV join	10.0.0.1	10.2.2.24	autres adresses IP

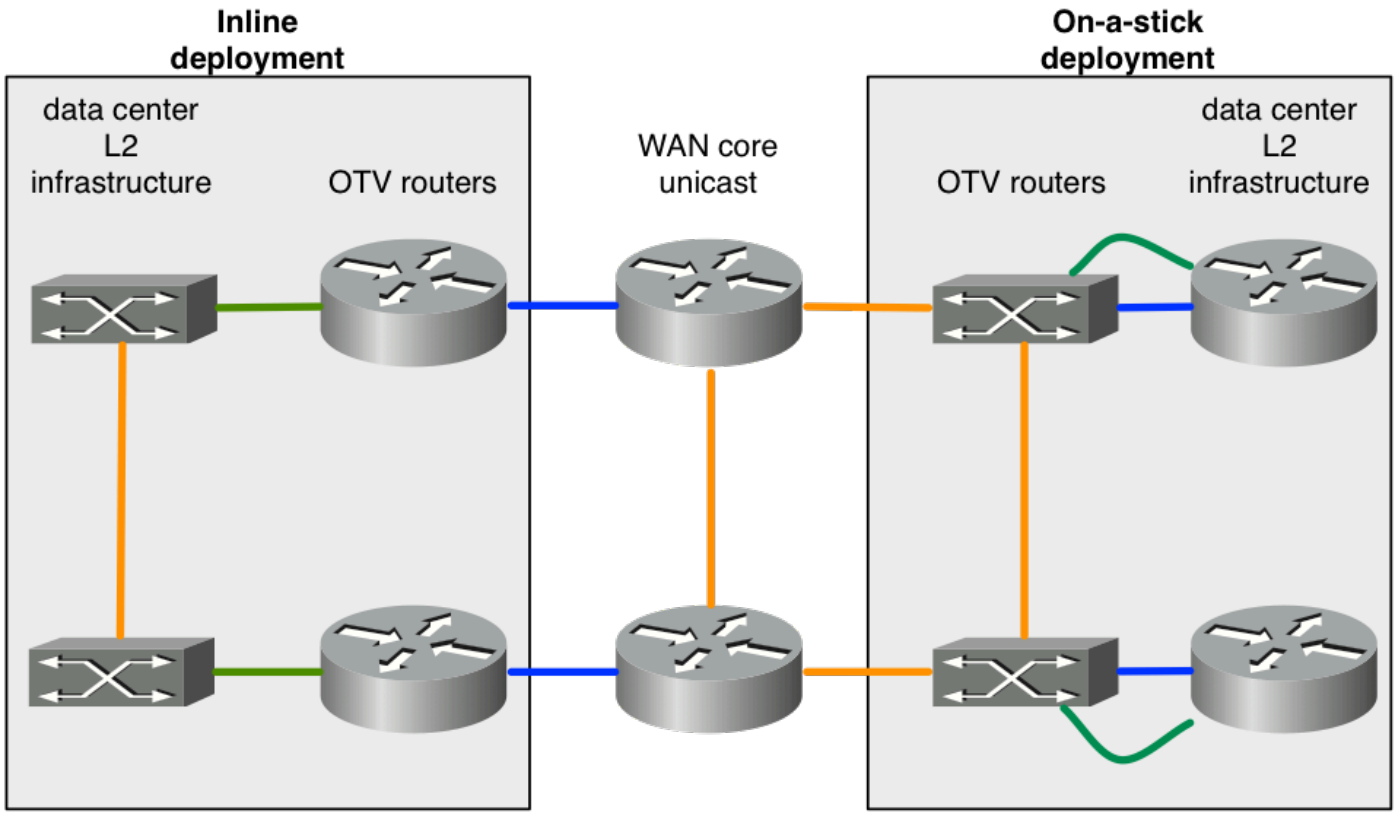
Configuration	interface Overlay 1
	  otv adjacency-server unicast-only
		interface Overlay 1
		  otv adjacency-server unicast-only
		  otv use-adjacency-server 10.0.0.1 monodiffusion uniquement
			interface Overlay 1
			  otv use-adjacency-server 10.0.0.1 10.2.2.24 monodiffusion uniquement

Certaines conceptions de connectivité dos à dos, prises en charge par le transfert OTV monodiffusion, ne respectent pas les règles de « maillage global ». Bien que ces configurations soient prises en charge, elles ne sont pas recommandées. Ce type de déploiement est le plus courant lorsque les data centers sont connectés via la fibre noire. Vous trouverez des détails sur cette option de configuration dans la section suivante, « Topologie de monodiffusion de cas particulier ».

OTV sur un bâton contre en ligne

Il existe deux modèles pour déployer OTV dans votre data center : on a stick et inline. Dans les scénarios de conception présentés précédemment, les routeurs OTV étaient connectés entre le data center et le réseau principal du fournisseur de services. Cependant, l'ajout du routeur OTV en tant qu'appliance qui n'est pas dans le chemin de transport de tout le trafic pourrait être plus souhaitable. Parfois, il est nécessaire de ne pas modifier la topologie actuelle pour se connecter au fournisseur de services par le biais de l'équipement actuel (par exemple, un déploiement de zone de friche avec un commutateur Catalyst 6000 ou un matériel de commutateur Nexus qui ne prend pas en charge OTV). Par conséquent, il est préférable de déployer OTV sur ASR1000 comme sur un stick comme appareil OTV.

Figure 4. Topologie en ligne et topologie « on a stick »



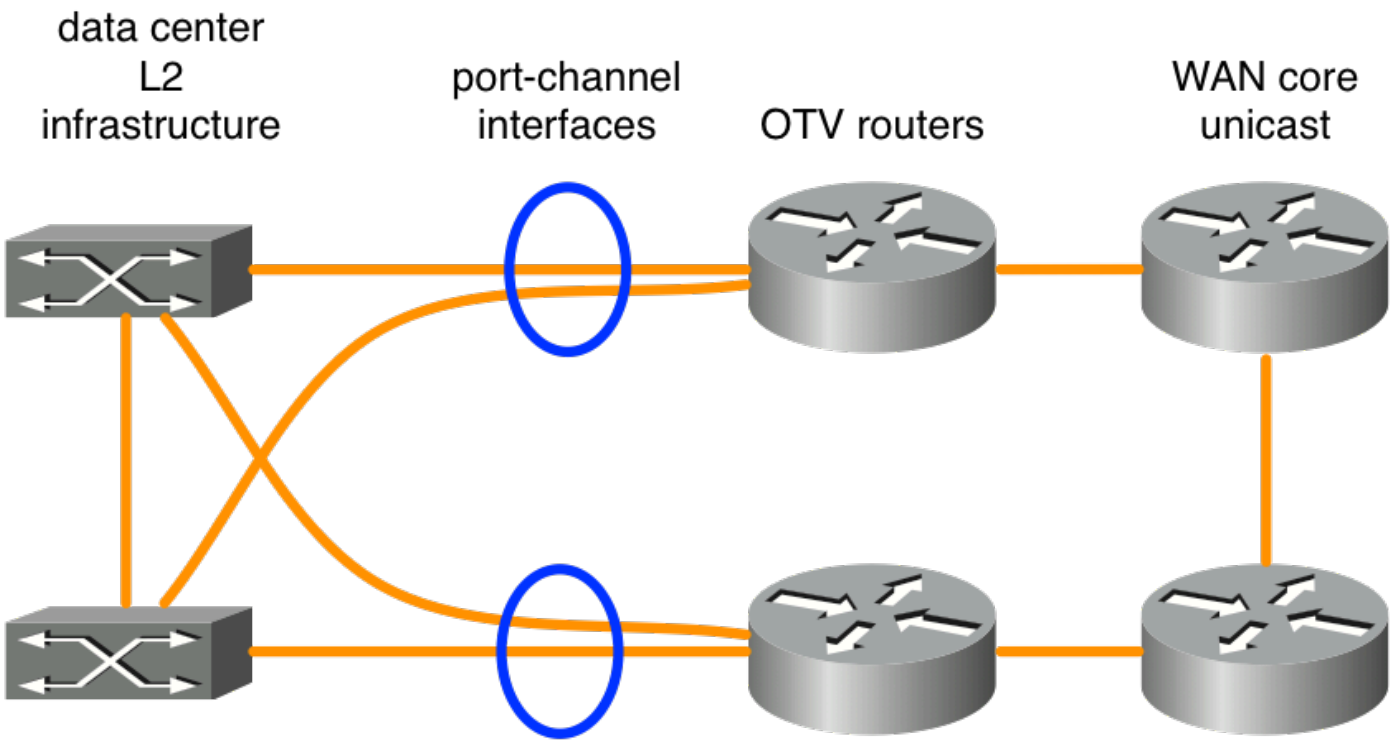
Le schéma illustre les deux modèles de déploiement qui peuvent faire partie de la même superposition. Les liaisons vertes connectées aux routeurs OTV sont configurées en tant qu'interfaces d'accès L2 pour accepter le trafic VLAN. Les liaisons bleues connectées aux routeurs OTV sont les interfaces de jonction qui transportent le trafic VLAN encapsulé OTV.

Il peut être nécessaire de configurer une fonctionnalité qui n'est pas prise en charge par OTV. Par exemple, OTV et MPLS ne peuvent pas être configurés sur le même boîtier. Par conséquent, il peut s'avérer judicieux d'utiliser ASR1000/OTV sur une clé et de configurer MPLS sur le routeur situé en face du routeur OTV.

Canaux de port pour les couches 2 et 3

Le code Cisco IOS® XE 3.10 pour ASR1000 a été ajouté pour prendre en charge la configuration Port-channel de couche 2 et de couche 3 avec OTV. Le port-channel de couche 2 peut être utilisé comme interface interne. Le Port-channel doit comporter jusqu'à 4 interfaces physiques. Le canal de port de couche 3 peut être utilisé comme interface de jointure.

Figure 5. Canaux de port utilisés pour la connectivité L2



Le schéma présente un scénario type Port Channel avec deux commutateurs dans VSS (gamme Catalyst 6000) ou VPC (gamme Nexus 7000). Ce type de conception offre une redondance avec deux routeurs OTV et une double connectivité à l'infrastructure du data center. Aucune configuration spéciale pour OTV autre que la configuration Port-channel de base n'est requise si VSS ou un VPC est utilisé sur un équipement de commutation L2 adjacent aux routeurs OTV.

Passerelle par défaut

Par définition, OTV crée le même sous-réseau L3 à plusieurs emplacements. Cela nécessite quelques considérations spéciales lors du routage du trafic de couche 3 vers et depuis les VLAN étendus. Le routage de couche 3 peut être configuré sur les routeurs OTV eux-mêmes ou sur d'autres périphériques connectés aux VLAN étendus. En outre, dans chaque scénario, les protocoles de redondance au premier saut (FHRP), tels que le protocole HSRP (Hot Standby Redundancy Protocol) ou le protocole VRRP (Virtual Router Redundancy Protocol), peuvent être déployés pour la redondance. Le protocole HSRP peut être exécuté en local sur un data center donné ou s'étendre entre des data centers (ce qui n'est pas habituel).

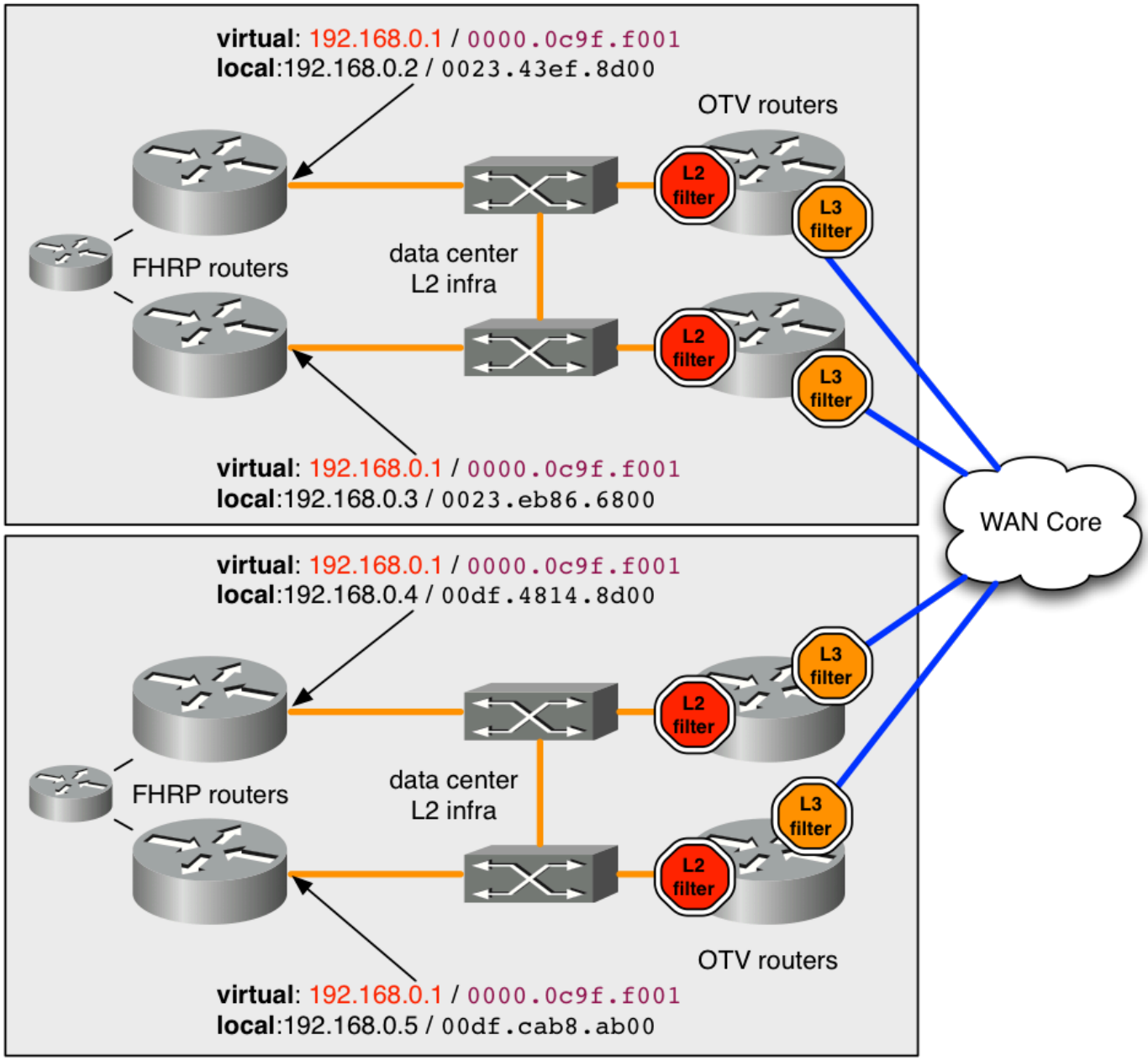
La meilleure pratique pour les déploiements OTV qui utilisent le protocole FHRP consiste à exécuter des instances locales du protocole FHRP dans chaque data center. Ces instances de FHRP utilisent les mêmes adresse MAC et adresse IP virtuelles, de sorte que lorsque des machines virtuelles (VM) se déplacent entre des centres de données, elles disposent d'une connexion ininterrompue. Si l'adresse MAC du routeur par défaut devait changer d'un centre de données à l'autre, les machines virtuelles ne pourraient pas communiquer hors sous-réseau tant que l'entrée ARP de la passerelle par défaut de la machine virtuelle n'aurait pas expiré.

Pour déployer correctement un FHRP avec OTV, il est nécessaire de considérer quel trafic L2 et L3 doit être filtré et isolé d'OTV. Au niveau de L2, ceci est nécessaire pour empêcher OTV de voir le même MAC virtuel L2 utilisé par le FHRP dans plusieurs emplacements. Des filtres sont

nécessaires au niveau de couche 3 pour isoler les annonces HSRP et VRRP sur chaque data center afin que la sélection active/écoute/veille soit localisée sur chaque data center.

Par défaut, les filtres FHRP sont activés lorsque OTV est activé. Elle peut être désactivée si la conception nécessite que le protocole FHRP soit étendu entre les data centers. Le filtrage L2 des adresses MAC virtuelles n'est PAS activé par défaut et doit être configuré manuellement.

figure 6. Exemple de déploiement recommandé pour FHRP



Dans l'exemple, l'adresse MAC virtuelle 0000.0c9f.f001 est utilisée pour l'adresse IP 192.168.0.1 qui héberge le VLAN étendu pour la connectivité du sous-réseau. L'utilisation des mêmes adresses MAC et IP virtuelles dans les deux data centers permet à un hôte de bénéficier d'une connectivité transparente à partir du sous-réseau lorsqu'il effectue des transferts entre les data centers.

Afin de garder l'adresse MAC 0000.0c9f.f001 cachée d'OTV dans plusieurs emplacements, un filtre L2 d'entrée (arrêt rouge dans le schéma) doit être déployé pour le VLAN sur chacun des

routeurs OTV , qui desservent le VLAN. Par le filtre ACL, la liste de contrôle d'accès du filtre configurée sur les instances de service L2 pour l'entrée, tous les paquets provenant de cet MAC sont abandonnés avant que le processus OTV sur l'ASR1000 puisse les voir. Ainsi, OTV n'apprend jamais l'adresse MAC et ne l'annonce pas aux data centers distants.

La configuration recommandée pour intercepter tout le trafic MAC virtuel FHRP par défaut/bien connu est indiquée ici.

```
mac access-list extended otv_filter_fhrp
 deny 0000.0c07.ac00 0000.0000.00ff any
 deny 0000.0c9f.f000 0000.0000.0fff any
 deny 0007.b400.0000 0000.0000.00ff any
 deny 0000.5e00.0100 0000.0000.00ff any
 permit any any
```

Cette liste de contrôle d'accès correspond aux espaces d'adresses MAC bien connus associés aux versions 1 et 2 de HSRP, au protocole GLBP (Gateway Load Balancing Protocol) et au protocole VRRP (dans cet ordre). Si l'adresse MAC virtuelle est configurée pour utiliser une valeur non standard non basée sur le numéro de groupe FHRP, elle doit être explicitement ajoutée à l'exemple de liste de contrôle d'accès. La liste de contrôle d'accès doit être ajoutée à l'instance de service L2 (illustrée ici).

```
interface Port-channel10
  description *** OTV internal interface ***
  no ip address
  no negotiation auto
!
  service instance 800 ethernet
    encapsulation dot1q 800
    mac access-group otv_filter_fhrp in
    bridge-domain 800
```

Il est également nécessaire de gérer la communication entre les hôtes FHRP au niveau de la couche 3 également. Quatre routeurs FHRP sont configurés sur un seul sous-réseau étendu dans le schéma. Sans un certain degré de filtres de couche 3, les quatre routeurs se verraient et sélectionneraient un seul périphérique actif et en auraient 3 dans différents états de veille. Ainsi, un centre de données aurait deux routeurs FHRP de secours locaux, mais n'aurait pas de connectivité L2 au routeur actif distant en raison des filtres L2 décrits précédemment.

Le résultat souhaité est d'avoir un routeur FHRP actif et un routeur FHRP en veille dans chaque centre de données. Le filtre d'entrée de couche 2 évoqué précédemment n'intercepte pas ce trafic de sélection, car le processus de sélection utilise les adresses IP et MAC réelles du routeur. Par défaut, la liste de contrôle d'accès suivante est appliquée en sortie sur l'interface de superposition. La sortie de l’interface de superposition serait le trafic vers le coeur du réseau étendu. La liste de contrôle d’accès n’apparaît pas dans la configuration en cours, mais elle peut

être observée avec « show ip access-list ». Il filtre le trafic de sélection FHRP en fonction du numéro de port UDP.

```
Extended IP access list otv_fhrp_filter_acl
    10 deny udp any any eq 1985 3222
    20 deny 112 any any
    30 permit ip any
```

La seule raison de désactiver ce filtre serait que si vous voulez que tous les routeurs FHRP sur un VLAN participent à la même sélection pour l'état actif. Afin de désactiver ce filtre, configurez « no otv filter-fhrp » sur l'interface Overlay.

Le trafic de monodiffusion inconnu

Par défaut, le trafic de monodiffusion reçu du réseau local par le routeur OTV et destiné à une adresse MAC inconnue sur un site OTV distant est abandonné. Ce trafic est appelé monodiffusion inconnue. Cette action de suppression va vers le coeur du WAN qui limite la quantité de bande passante consommée sur le WAN par le trafic de diffusion. On s'attend généralement à ce que tous les hôtes du réseau local émettent suffisamment de trafic de diffusion (ARP, diffusions de protocole, etc.) qui doit toujours être vu par un routeur OTV, annoncé et donc « connu ».

Certaines applications tirent parti des hôtes silencieux. Sur une infrastructure de commutation normale, ce n'est pas un problème, car la diffusion L2 d'adresses MAC de monodiffusion inconnues sur le LAN permet à l'hôte silencieux de voir le trafic. Cependant, dans un environnement OTV, le routeur OTV bloque le trafic entre les data centers.

Pour compenser cela, une fonctionnalité appelée Selective Unicast Forwarding a été intégrée dans Cisco IOS® XE. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 et toutes les versions ultérieures prennent en charge le transfert sélectif unicast.

Il est configuré par l'ajout d'une seule commande par adresse MAC sur l'interface de superposition. Exemple :

```
interface Overlay1
  service instance 100 ethernet
    encapsulation dot1q 100
    otv mac flood 0000.0000.0001
    bridge-domain 100
```

Tout trafic destiné à 0000.0001.0001 doit être diffusé à tous les routeurs OTV distants avec VLAN 100 dans cet exemple. Ceci peut être observé par la commande suivante :

```
OTV_router_1#
```

show otv route

```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
```

Si cette adresse MAC est apprise sur un site distant, une entrée doit être ajoutée à la table de transfert qui a la priorité sur l'entrée d'inondation.

<#root>

```
OTV_router_1#
```

show otv route

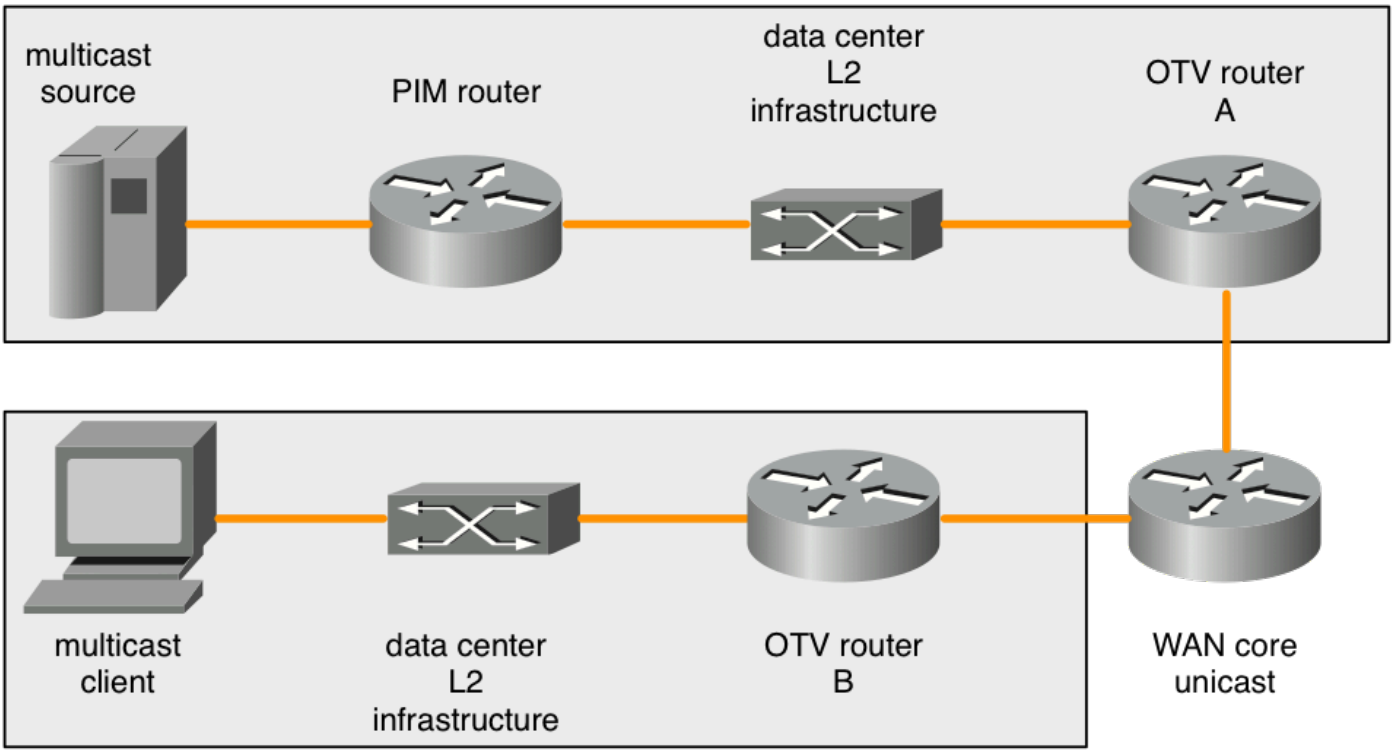
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood
 0    100  100    0000.0000.0001 50    ISIS   OTV_router_3
```

En règle générale, une entrée d'inondation pour une adresse MAC donnée doit être configurée sur tous les routeurs OTV avec ce VLAN.

Sources de multidiffusion distantes

ASR1000 indique qu'un routeur OTV ne transmet pas les demandes de jointure IGMP multidiffusion reçues du réseau local. Le schéma suivant détaille la topologie où cela peut poser problème.

Figure 7. Sources de multidiffusion distantes



Lorsqu'une jonction IGMP de multidiffusion est envoyée par le client de multidiffusion, l'ASR1000 (routeur OTV B) l'observe et annonce son intérêt pour le groupe de multidiffusion. Les routeurs OTV distants (routeur OTV A) doivent transférer tout trafic vers ce groupe de multidiffusion qu'ils voient sur leur domaine de diffusion L2 local. Cependant, l'ASR1000 distant (routeur OTV A) ne régénère pas les demandes de jointure IGMP de multidiffusion lorsque l'intérêt pour un groupe de multidiffusion est annoncé depuis le routeur OTV du client (routeur OTV B).

Lorsque les sources de multidiffusion se trouvent sur le même domaine de diffusion de couche 2 que le routeur OTV, cela ne pose pas de problème. Le routeur OTV doit être configuré comme demandeur IGMP. Cela apparaît dans tout trafic de multidiffusion présent sur le domaine de diffusion L2. Cependant, seule une demande de jointure PIM peut entraîner le transfert d'une source de multidiffusion d'un domaine de diffusion L2 différent vers le domaine de diffusion L2 sur lequel se trouve le routeur OTV.

La demande de jointure IGMP distante n'est pas transférée ou régénérée. Les routeurs OTV ne sont pas non plus des routeurs PIM. Ainsi, les topologies avec des sources de multidiffusion qui ne sont pas directement sur le domaine de diffusion de couche 2 avec le routeur OTV n'ont aucun moyen d'informer les routeurs PIM pour transférer le trafic source lorsqu'un client distant s'y intéresse.

Il y a deux solutions à ce problème.

Tout d'abord, un ou plusieurs clients IGMP locaux peuvent être déployés sur le domaine de diffusion de couche 2 connecté au routeur OTV (routeur OTV A). Ce client IGMP doit s'abonner à tous les groupes de multidiffusion auxquels les clients distants peuvent s'abonner. Le routeur PIM transfère alors le trafic de multidiffusion vers le domaine de diffusion adjacent au routeur OTV A. Les requêtes IGMP dessinaient alors n'importe quel trafic multicast et il était envoyé à travers la superposition.

L'autre solution serait de configurer une « ip igmp static-join » pour tous les groupes auxquels les clients distants pourraient s'abonner. Le routeur PIM transfère également le trafic de multidiffusion vers le domaine de diffusion adjacent au routeur OTV A.

Cette limitation est connue et fait partie du cahier des charges de conception. Il ne s'agit pas d'un bogue, mais d'une limite dans la topologie prise en charge pour le moment.

Considérations QoS

Par défaut sur ASR1000, la valeur TOS dans l'en-tête OTV ajouté est copiée à partir des bits 802.1p du paquet de couche 2. Si le paquet de couche 2 n’est pas étiqueté, une valeur de zéro est utilisée.

Le comportement par défaut de Nexus 7000 est différent dans les versions 5.2.1 et ultérieures. Si le comportement souhaité est de copier la valeur TOS des paquets internes dans le routeur, une configuration QoS supplémentaire peut y parvenir. Cela donne le même comportement que le nouveau logiciel Nexus 7000.

La configuration pour copier la valeur TOS de couche 3 des paquets de couche 2 dans l'en-tête le plus externe du paquet OTV est la suivante :

```
class-map dscp-af11
 match dscp af11
!
class-map dscp-af21
 match dscp af21
!
class-map qos11
 match qos-group 11
!
class-map qos21
 match qos-group 21
!
policy-map in-mark
 class dscp-af11
  set qos-group 11
 class dscp-af21
  set qos-group 21
!
policy-map out-mark
 class qos11
  set dscp af11
 class qos21
  set dscp af21
!
interface Gig0/0/0
 ! L2 interface
 service instance 100 ethernet
  encapsulation dot1q 100
  service-policy in-mark
  bridge-domain 100
!
interface Gig0/0/1
 ! OTV join interface
```

```
 service-policy out-mark
```

La configuration fournie doit correspondre au trafic pour différentes valeurs DSCP en entrée. La balise qos-group significative localement est utilisée pour marquer en interne ce trafic pendant le transit via le routeur. Sur l'interface de sortie, le groupe qos est mis en correspondance, puis l'octet TOS le plus externe est mis à jour en conséquence.

Considérations sur la MTU WAN / Fragmentation

OTV utilise essentiellement un en-tête GRE pour transporter le trafic de couche 2 sur le réseau étendu. Cet en-tête GRE a une taille de 42 octets. Dans un déploiement de réseau idéal, la liaison WAN doit avoir une unité de transmission maximale (MTU) d'au moins 42 octets de plus que le plus grand paquet que l'OTV est censé traiter.

Si l'interface L2 a une MTU de 1 500 octets, l'interface de jointure doit avoir une MTU de 1 542 octets ou plus. Si l'interface L2 a une MTU de 2000 octets, mais qu'elle est censée gérer des paquets de 1500 octets seulement, alors une MTU WAN de 1542 octets est suffisante, cependant l'ajout standard de 42 à la 2000 serait idéal.

```
interface GigabitEthernet0/0/0
  mtu 1600
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
!
interface GigabitEthernet0/0/1
  mtu 1500
  service instance 100 ethernet
    encapsulation dot1q 100
    bridge-domain 100
  service instance 101 ethernet
    encapsulation dot1q 101
    bridge-domain 101
```

Certains fournisseurs de services ne sont pas en mesure de fournir des valeurs MTU plus élevées pour leurs circuits WAN. Si tel est le cas, ASR1000 peut effectuer la fragmentation des données OTV transportées. Nexus 7000 ne dispose pas de cette fonctionnalité. Les réseaux OTV ASR1000 et Nexus 7000 mixtes avec fragmentation activée sur ASR1000 ne sont pas pris en charge.

La configuration de la fragmentation OTV est la suivante :

```
otv fragmentation join-interface GigabitEthernet0/0/0
!
interface Overlay 1
  otv join-interface GigabitEthernet0/0/0
```

Il est important que la commande de niveau global soit configurée avant la commande Overlay interface join-interface. Si la commande otv join-interface de l'interface de superposition a été configurée en premier, supprimez la commande otv join-interface de l'interface de superposition, configurez la commande otv fragmentation join-interface, puis reconfigurez la commande otv join-interface de l'interface de superposition.

Lorsque la fragmentation OTV n'est pas activée, tous les paquets OTV qui transportent des données L2 encapsulées sont envoyés avec le bit DF défini de sorte qu'ils ne soient pas fragmentés en transit. Une fois la commande de fragmentation ajoutée, le bit DF est défini sur 0. Les routeurs OTV eux-mêmes peuvent fragmenter le paquet et le fragmenter en transit par d’autres routeurs.

Il existe un nombre limité de mémoires tampon de réassemblage de paquets disponibles sur les plates-formes ASR1000. Par conséquent, moins un paquet doit contenir de fragments pour être transmis, mieux c'est. Cela augmente l'efficacité et réduit la consommation globale de bande passante sur le WAN si cela pose problème. L'activation de la fragmentation OTV a des conséquences sur les performances. Si la fragmentation est présente et que l'on s'attend à ce que plus de 1 Gbit/s de trafic OTV soit traité, les performances OTV doivent être étudiées plus en détail.

Topologie de monodiffusion de cas particulier

Les déploiements sur site pour OTV ont souvent des connexions directes fibre optique dos à dos entre les routeurs OTV dans deux centres de données.

Pour les topologies à hébergement unique, il s'agit d'un déploiement standard où le trafic OTV et non OTV partagent l'interface de jonction. Aucune considération particulière n'est nécessaire pour cette configuration. Cette section ne s'applique donc pas.

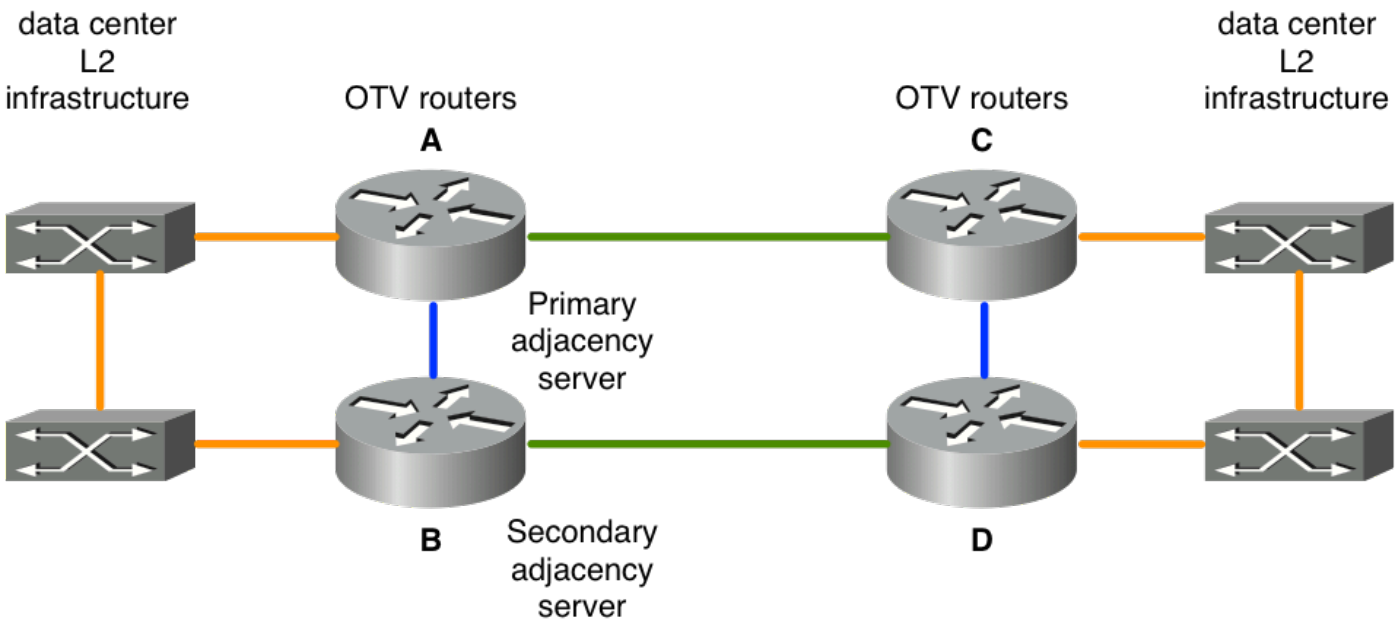
Toutefois, si le déploiement comporte des routeurs OTV multirésidentiels dans les deux data centers, il convient de tenir compte de certains points particuliers. Une configuration supplémentaire est requise.

Si plus de deux data centers sont impliqués, cette configuration spéciale ne s'applique pas.

Pour le scénario avec plus de deux data centers avec des routeurs OTV à hébergement unique ou multiple, un déploiement OTV de monodiffusion ou de multidiffusion standard doit être utilisé.

Il n'existe aucune autre alternative prise en charge.

Figure 8. Monodiffusion cas spécial



Dans la topologie présentée, les liaisons en vert sont les liaisons en fibre noire entre les deux data centers. Ces fibres sombres sont directement connectées aux routeurs OTV. Les liaisons bleues entre les routeurs OTV sont utilisées pour réacheminer le trafic non OTV en cas de défaillance des liaisons vertes. En cas de défaillance de la liaison verte supérieure (A à C), le trafic non OTV qui utilise les routeurs OTV supérieurs comme route par défaut est acheminé via les liaisons bleues nord-sud (A à B et C à D) vers la liaison verte encore opérationnelle entre la paire de routeurs OTV inférieure (B à D).

Ce réacheminement de base du trafic ne fonctionne pas pour le trafic OTV car la configuration OTV spécifie une interface physique comme interface de jointure. Si l'« interface verte » du routeur OTV A tombe en panne, le trafic OTV ne peut pas provenir d'une autre interface du routeur OTV B. En outre, comme il n'y a pas de connectivité complète via le coeur WAN, tous les routeurs OTV ne peuvent pas être informés en cas de panne. Afin de contourner ce problème, la détection de transfert bidirectionnel (BFD) ainsi que les scripts du gestionnaire d'événements intégré (EEM) sont utilisés.

BFD doit surveiller la liaison WAN entre les paires de routeurs OTV est-ouest (A/C et B/D). Si la connexion au routeur distant est perdue, l'interface de superposition OTV est arrêtée via le script EEM sur cette paire de routeurs OTV est-ouest. Le routeur à plusieurs hôtes associé assume ainsi le transfert pour tous les VLAN. Lorsque BFD détecte que la liaison a été restaurée, le script EEM se déclenche pour réactiver l'interface de superposition.

Il est très important d'utiliser BFD pour détecter une défaillance de liaison. En effet, l'interface de superposition doit être arrêtée du côté « défaillant » et de la paire est-ouest. Selon le type de connectivité fourni par le fournisseur de services, une liaison physique peut être interrompue (interface verte sur le routeur OTV A) tandis que l'interface de la paire de routeurs est-ouest correspondante peut rester inactive (interface verte sur le routeur OTV C). BFD détecte la défaillance de l'une des interfaces ou tout autre problème en transit et avertit immédiatement les deux paires simultanément. Il en va de même lorsque les routeurs doivent être informés de la liaison de récupération.

La configuration de ce déploiement est la même que celle de tout autre déploiement, avec l'ajout

des éléments suivants :

- Configuration BFD sur l'interface WAN
- le script EEM suivant
- Identité ISIS OTV correspondant à la distribution VLAN paire/impaire

La configuration de BFD sur l'interface de jonction OTV sort du cadre de ce document. Pour plus d'informations sur la configuration de BFD sur ASR1000, consultez la page :

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/xe-3s/irb-xe-3s-book.html

Une fois que la détection de panne BFD est opérationnelle correctement entre les paires d'interfaces de jonction (liaisons vertes dans le schéma), le script EEM doit être déployé. Le script EEM doit être adapté aux routeurs spécifiques pour modifier les interfaces de superposition correctes et peut-être surveiller les chaînes plus précises dans le journal pour détecter les défaillances et les restaurations BFD.

```
event manager environment _OverlayInt Overlay1
!
event manager applet WatchBFDdown
description "Monitors BFD status, if it goes down, bring OVERLAY int down"
event syslog pattern "BFD peer down notified" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDdown will shut int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "shutdown"
action 5.0 syslog msg "EEM WatchBFDdown COMPLETE ..."
!
event manager applet WatchBFDup
description "Monitors BFD status, if it goes up, bring OVERLAY int up"
event syslog pattern "new adjacency" period 1
action 1.0 cli command "enable"
action 2.0 cli command "config t"
action 2.1 syslog msg "EEM: WatchBFDup bringing up int $_OverlayInt"
action 3.0 cli command "interface $_OverlayInt"
action 4.0 cli command "no shutdown"
action 5.0 syslog msg "EEM WatchBFDup COMPLETE ..."
!
```

Ce type de déploiement nécessite également que les paires de routeurs est-ouest (A/C et B/D) correspondent dans leur transfert de VLAN pairs et impairs.

Par exemple, A et C doivent transférer des VLAN pairs tandis que B et D transfèrent des VLAN impairs en fonctionnement nominal en régime permanent.

La distribution impaire/paire est déterminée par le nombre ordinal OTV qui peut être observé par la commande « show otv site ».

Le nombre ordinal entre les deux routeurs de site est déterminé en fonction de l'ID réseau OTV

ISIS.

```
OTV_router_A#show otv site
Site Adjacency Information (Site Bridge-Domain: 99)
Overlay99 Site-Local Adjacencies (Count: 2)
  Hostname       System ID      Last Change Ordinal    AED Enabled Status
* OTV_router_A   0021.D8D4.F200 19:32:02    0          site       overlay
  OTV_router_B   0026.CB0C.E200 19:32:46    1          site       overlay
```

L'identificateur réseau ISIS OTV doit être configuré sur tous les routeurs OTV. Lors de la configuration de l’identificateur, veillez à ce que tous les routeurs OTV se reconnaissent toujours.

<#root>

```
OTV router A:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000a

.

00

```
OTV router B:
otv isis Site
 net
```

49

.

0001

.

0001

.

0001

.

000b

.

00

OTV router C:
otv isis Site
 net

49

.

0001

.

0001

.

0001

.

000c

.

00

OTV router

D:
otv isis Site
 net

49

.

0001

.

0001

.

0001

.

000d

.

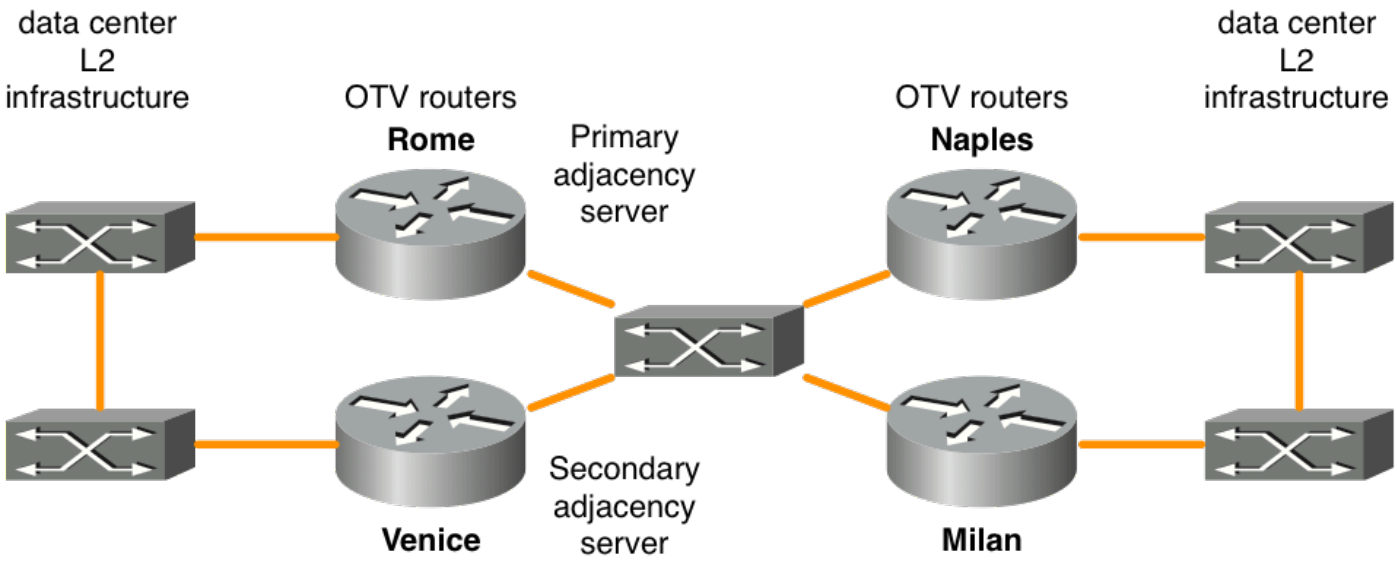
00

Les parties de l'identificateur en noir doivent correspondre sur tous les routeurs OTV qui participent à la superposition. La partie de l'identificateur en rouge peut être modifiée. L'identificateur réseau le plus bas sur un site obtient le numéro ordinal 0 et à son tour transmet les VLAN pairs. L'identificateur réseau le plus élevé d'un site obtient le numéro ordinal 1 et transfère le nombre impair de VLAN.

Exemples de configuration

Monodiffusion

Figure 9. Exemple de configuration de monodiffusion



Configuration de Rome :

```
!
hostname Rome
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv adjacency-server unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
```

```
 !
interface GigabitEthernet1/0/0
 ip address 172.16.0.1 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Configuration de Venise :

```
!
hostname Venice
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv adjacency-server unicast-only
 otv use-adjacency-server 172.16.0.1 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.2 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
```

```
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Configuration de Naples :

```
!
hostname Naples
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.3 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
```

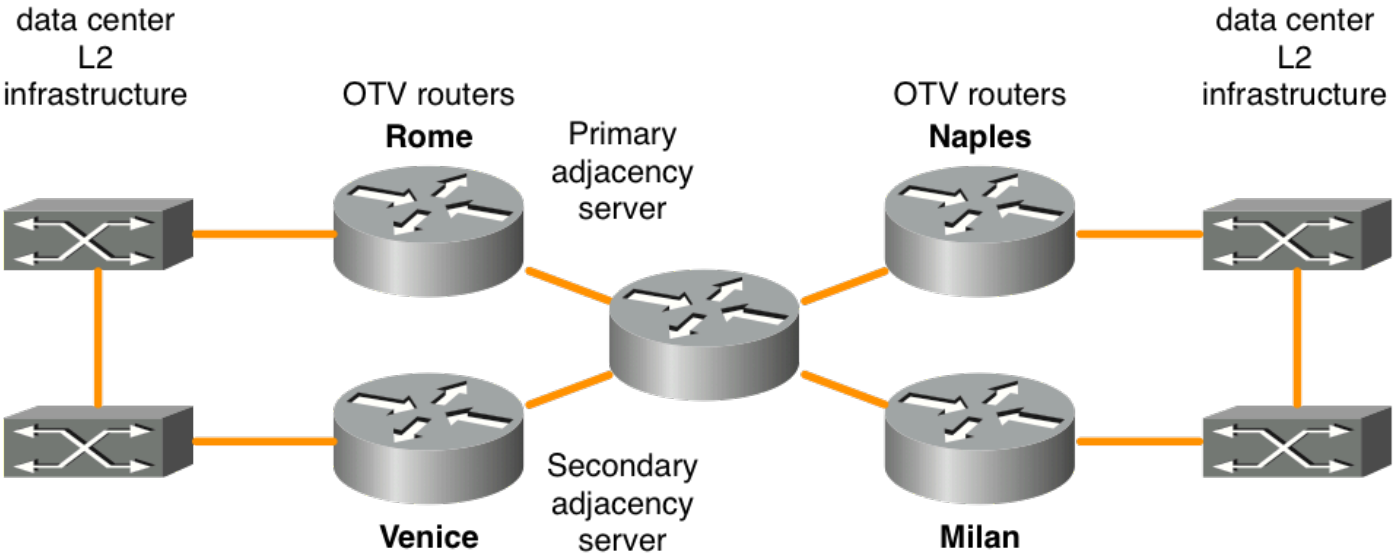
```
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Configuration de Milan :

```
!
hostname Milan
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv use-adjacency-server 172.16.0.1 172.16.0.2 unicast-only
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.16.0.4 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Multidiffusion

Figure 10. Exemple de configuration de multidiffusion



Configuration de Rome :

```
!
hostname Rome
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet1/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
```

```
 cdp enable
!
interface GigabitEthernet1/0/1
 no ip address
 negotiation auto
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Configuration de Venise :

```
!
hostname Venice
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0001
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.17.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
```

```
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
!
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
```

Configuration de Naples :

```
!
hostname Naples
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
 otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.18.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
```

```
 negotiation auto
 cdp enable
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Configuration de Milan :

```
!
hostname Milan
!
ip multicast-routing distributed
!
ip igmp snooping querier version 3
ip igmp snooping querier
!
otv site bridge-domain 99
!
otv site-identifier 0000.0000.0002
!
spanning-tree mode pvst
!
interface Overlay99
 no ip address
 otv join-interface GigabitEthernet0/0/0
otv control-group 239.0.0.1
 otv data-group 238.1.2.0/24
!
  service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
interface GigabitEthernet0/0/0
 ip address 172.19.0.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 cdp enable
```

```
 service instance 99 ethernet
  encapsulation dot1q 99
  bridge-domain 99
 !
 service instance 100 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Forum aux questions

Q) Les VLAN privés sont-ils pris en charge conjointement avec OTV ?

A) Oui, aucune configuration spéciale n'est requise dans OTV. Dans la configuration de VLAN privé, assurez-vous que les ports de commutateur connectés à l'interface L2 OTV sont configurés en mode promiscuité.

Q) OTV est-il pris en charge avec le cryptage IPSEC ?

R) Oui, la configuration Crypto-map sur l'interface de jointure est prise en charge. Aucune configuration spéciale n'est requise pour qu'OTV prenne en charge le chiffrement. Cependant, la configuration du cryptage ajoute une surcharge supplémentaire, qui doit être compensée par l'augmentation de la MTU du WAN par rapport à la MTU du LAN. Si cela n'est pas possible, la fragmentation OTV doit être requise. Les performances OTV sont limitées à celles du matériel IPSEC.

Q) OTV est-il pris en charge avec MACSEC ?

R) Oui, ASR1001-X inclut la prise en charge MACSEC pour les interfaces intégrées. OTV fonctionne avec MACSEC configuré sur les interfaces LAN et/ou WAN. Les performances OTV sont limitées à celles du matériel MACSEC.

Q) Une interface de bouclage peut-elle être utilisée comme interface de jointure ?

R) Non, seules les interfaces Ethernet, Portchannels ou POS peuvent être utilisées comme interfaces de jonction OTV. L'interface de jonction de bouclage OTV figure sur la feuille de route, mais aucune version n'est actuellement prévue pour le moment.

Q) Une interface de tunnel peut-elle être utilisée comme interface de jonction ?

R)Non, les tunnels GRE, les tunnels DMVPN ou tout autre type de tunnel ne sont pas pris en charge en tant qu'interfaces de jointure. Seules les interfaces Ethernet, Portchannels ou POS peuvent être utilisées comme interfaces de jonction OTV.

Q) Différentes interfaces de superposition peuvent-elles utiliser différentes interfaces de couche 2

et/ou de jointure ?

A) Toutes les interfaces de superposition doivent pointer vers la même interface de jointure. Toutes les superpositions doivent être liées à la même interface physique pour la connectivité de couche 2 vers le data center.

Q) Le VLAN du site OTV peut-il se trouver sur une interface physique différente des VLAN étendus OTV ?

A) Le VLAN du site OTV et les VLAN étendus doivent se trouver sur la même interface physique.

Q) Quel ensemble de fonctionnalités est requis pour OTV ?

A) Les services IP avancés (AIS) ou les services d'entreprise avancés (AES) sont requis pour OTV.

Q) Une licence distincte est-elle requise pour OTV sur les plates-formes à configuration fixe ?

R) Non, tant que l'ASR1000 est exécuté avec advipservices ou un niveau de démarrage d'entreprise configuré, OTV est disponible.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.