Overlay-transportvirtualisatie configureren met ASR 1000

Inhoud

Inleiding

Dit document beschrijft de netwerktopologieën voor Overlay Transport Virtualization (OTV) die worden ondersteund op ASR 1000- en Catalyst 8300/8500-Series-routers.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASR 1000, IOS® XE versie 16.10.1a en hoger
- Catalyst 3800, IOS® XE versie 17.5.1a en hoger
- Catalyst 8500, IOS® XE versie 17.6.1a en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

ASR 1000 ondersteunt OTV sinds Cisco IOS® XE release 3.5. De Catalyst 8300 Series router begint met ondersteuning met IOS® XE17.5.1a en de Catalyst 8500 Series routers begint met ondersteuning met IOS® XE versie 17.6.1a.

OTV biedt Layer 2-connectiviteit tussen externe netwerksites door op MAC-adressen gebaseerde routing en IP-ingesloten doorsturen (MAC-in-IP) via een transportnetwerk om ondersteuning te bieden voor toepassingen die Layer 2-nabijheid vereisen, zoals clusters en virtualisatie. OTV gebruikt een overlay control-plane protocol om te leren en te verspreiden MAC-routing informatie over het overlay netwerk. Het OTV control-plane protocol maakt gebruik van ISIS-berichten (Intermediate-System-to-Intermediate-System) om nabijheid tot externe locaties te bouwen en MAC-routeupdates naar externe locaties te verzenden. OTV bouwt Layer 2-nabijheid tot externe locaties op het overlay-netwerk door automatisch ontdekken van externe OTV-apparaten.

De voordelen van OTV voor Layer 2-uitbreiding omvatten:

- Geen MPLS-vereiste
- Geen complexe Ethernet-over-Multiprotocol Label Switching (EoMPLS) configuratie voor mesh
- Geen complexe implementatie van Virtual Private LAN Services (VPLS) voor Layer 2-uitbreidingen
- Native Spanning-Tree-isolatie
    - u hoeft de BPDU-filters (Bridge Data Protocol Unit) niet expliciet te configureren
    - standaardisolatie van Spanning-Tree-problemen voor een bepaald datacenter
- Native onbekende unicast overstroming isolatie
    - onbekende unicast MAC-pakketten worden niet doorgestuurd
    - ondersteuning voor per-MAC onbekende unicast voorwaarts is toegestaan
- ARP-optimalisatie (Address Resolution Protocol) met OTV ARP-caching
    - vermindert onnodig WAN-verkeer
- Vereenvoudigde provisioning van FHRP-isolatie (First Hop Redundantie Protocol)
- Vereenvoudigde toevoeging van sites
- Vereenvoudigde redundantieconfiguratie
- Mogelijkheid om een "afname in applicatie" te hebben voor migraties wanneer tijdelijke diensten vereist zijn

Vereisten

De volgende items zijn de primaire regels om in gedachten te houden wanneer een OTV-implementatie wordt ontworpen. Als deze regels worden nageleefd, worden het ontwerp en de implementatie gestroomlijnd.

- Er kan slechts één interface worden gebruikt voor het verzenden van het OTV-ingekapselde verkeer, bekend als de Josef-interface, voor alle geconfigureerde OTV Overlay-interfaces
- Er kan slechts één interface worden gebruikt om de datacenter L2 service-instanties voor de OTV-site VLAN te configureren en de VLAN's te configureren die tussen datacenters voor alle geconfigureerde OTV Overlay-interfaces worden uitgebreid
- Poortkanalen kunnen worden gebruikt voor interfaceredundantie en aansluiting op VSS- of VPC-switches en worden ondersteund als de "één-en-slechts"-interface voor connectiviteit.
- Alle OTV-routers moeten kunnen worden gecontacteerd via de Josef-interface
- De Spanning Tree moet worden geconfigureerd op de OTV-router die naar het datacenter wijst
- IGMP-spionage en -bevraging moeten worden geconfigureerd om datacenter-multicast verkeer correct te doorsturen
- Een gegeven datacenter kan worden geconfigureerd met 1 of 2 OTV-routers. Met twee routers distribueren ze VLAN-doorsturen op een oneven/even manier op basis van VLAN-nummer. Elke OTV-router in een datacenter fungeert als back-up voor de andere.
- Meervoudige paren moeten worden geconfigureerd met dezelfde OTV-siteherkenning
- ASR 1000/Catalyst 8300/Catalyst 8500 en Nexus 7000 kunnen deel uitmaken van hetzelfde OTV-netwerk
    - Nexus 7000 ondersteunt geen OTV-fragmentatie of -encryptie, dus deze functies kunnen niet worden gebruikt in een "hybride" implementatie.

Er zijn bepaalde ontwerpen voor back-to-back connectiviteit die worden ondersteund en die niet voldoen aan de vermelde regels. Hoewel deze configuraties worden ondersteund, worden ze niet aanbevolen. Details hierover vindt u in de latere sectie "Special case unicast topology".

Er kan niet genoeg worden benadrukt dat de huidige OTV-software de "één en slechts één"-interfacebeperking heeft bij de configuratie van de toetredings- en L2-toegangsinterfaces voor OTV. Voor redundantie kan een poortkanaal-interface worden gebruikt. De verbinding van het poortkanaal met Nexus 7000s in een VPC wordt ondersteund. Een basis poort-kanaal verbinding met één switch wordt ook ondersteund.

OTV-implementatietypen

Voor OTV is een enkele Josef-interface en een enkele L2-interface nodig. Een en slechts een van deze kan per OTV router worden ondersteund. OTV vereist ook dat een site VLAN zo wordt geconfigureerd dat multihomed OTV-routers met elkaar kunnen communiceren via het lokale netwerk. Zelfs single-homed OTV routers moeten de OTV site VLAN geconfigureerd hebben. Bovendien moet voor elke locatie of elk datacenter een unieke locatie-identifier geconfigureerd zijn. Tweevoudig gecensureerde OTV-routers moeten dezelfde site-identifier gebruiken en over hetzelfde VLAN kunnen communiceren.

De volgende configuratie levert de basisconfiguratie die nodig is voor OTV. Deze is echter niet compleet, aangezien de unicast- of multicast-kernconfiguratie moet worden toegevoegd. Deze worden in de volgende delen van dit document nader toegelicht.

```
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
```

De configuratie van de service-instantie wordt gebruikt voor alle L2-interfaceconfiguratie met OTV.

Elke service-instantie op de L2-interface moet worden gekoppeld aan een specifieke enkele of dubbele gelabelde inkapseling.

Elk van die diensten moet dan weer gekoppeld worden aan een bridge-domein.

Dat bridge-domein wordt gebruikt op een service-instantie die is geconfigureerd op de Overlay-interface.

Het bridge-domein is de lijm die de Overlay service-instantie koppelt aan de L2 interface service-instantie.

De insluiting van verkeer op de overlay-interface moet overeenkomen met de insluiting van het verkeer na het herschrijven van ingangen op de L2-interface.

In het voorbeeld, verkeer dat ingress op Gig1/0/1 service instantie 99 heeft een enkele 802.1Q

VLAN van 99 en bridge domain 99. De corresponderende service instantie met bridge-domain 99 op de Overlay interface is ook geconfigureerd voor één 802.1Q VLAN van 99. Deze case is het meest rechttoe rechtaan.

In het voorbeeld, verkeer dat ingaast op Gig1/0/1 service instantie 98 heeft een dubbele 802.1Q VLAN van 99 en 1098 en bridge domain 90. De overeenkomstige service instantie met bridge-domain 90 op de Overlay interface is geconfigureerd voor één 802.1Q VLAN van 90. Deze zijn duidelijk niet hetzelfde. De opdracht Indringing herschrijven zorgt ervoor dat de tags correct worden vertaald als verkeer beweegt door de indringingsinterface. Verkeer dat de L2-interface binnendringt, heeft 98/1098/802.1Q VLAN's vervangen door één VLAN van 90. Het symmetrische trefwoord zorgt ervoor dat verkeer dat de L2-interface uitkomt, de enkele 802.1Q VLAN van 90 heeft vervangen door 98/1098.

Alle serviceconstanten met meerdere 802.1Q VLAN's die door OTV worden uitgebreid, moeten de opdracht Toegang herschrijven gebruiken. OTV-insluiting ondersteunt slechts één VLAN-id. Om die reden moet elke dubbele VLAN-configuratie op de L2-interfaces worden herschreven in één tag op de Overlay-interfaceservicesinstantie. Dit sluit ondersteuning voor dubbelzinnige VLAN-configuraties uit.

Zie dit document voor meer informatie over het herschrijven van tags:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

In dit voorbeeld is het OTV-site bridge-domein 100.

- Het OTV site bridge-domein is alleen geconfigureerd op de L2 interface.
- Het OTV site bridge-domein mag nooit worden geconfigureerd op de Overlay-interface, omdat dit de OTV-implementatie onstabiel maakt.
- De OTV-site VLAN moet alleen worden aangesloten op de OTV-routers en mag geen ander datacenter-/gebruikersverkeer dragen.
- De OTV-site VLAN moet op dezelfde fysieke interface staan als de uitgebreide VLAN's van OTV.

Multihome

Een datacenter kan worden aangesloten op één OTV-host of maximaal 2 voor redundantie, ook bekend als Multihome. Multihome wordt gebruikt voor veerkracht en taakverdeling. Wanneer meer dan één randapparaat aanwezig is op een site en beide deelnemen aan hetzelfde overlay-netwerk, wordt de site beschouwd als multihomed. OTV Multihome verdeelt de VLAN's op een oneven/even manier onder de twee OTV-routers die tot dezelfde site behoren, op basis van het VLAN-nummer. Eén randapparaat wordt geselecteerd als AED voor alle oneven VLAN's, terwijl de andere OTV-router wordt geselecteerd als AED voor alle even VLAN's. Elke AED is ook een stand-by voor de VLAN's die actief zijn op de andere router. In het geval van een link- of knoopdefect in een van de AED's wordt de stand-by AED actief voor alle VLAN's.

Als twee ASR 1000's in hetzelfde datacenter zijn aangesloten om Multihome te doen, is er geen behoefte aan een speciale link tussen de twee ASR 1000's. OTV gebruikt de OTV-site VLAN die door de interne interface en de communicatie wordt verspreid via de Josef-interface om te bepalen welke routers verantwoordelijk zijn voor even en oneven VLAN's.

ASR 1000s en Nexus 7000s kunnen niet worden gemengd in hetzelfde datacenter met OTV geconfigureerd op beide routers als back-up voor de andere. Multihome in een gegeven datacenter wordt ondersteund voor overeenkomende platforms (ASR 1000 of Nexus 7000). U kunt ASR 1000s in het ene datacenter hebben en Nexus 7000s in een ander datacenter. De interoperabiliteit tussen deze twee platforms is getest en ondersteund. Sommige datacenters kunnen worden gemultihomed, terwijl anderen single-homed zijn.

Multihomed ASR 1000 routers paren moeten dezelfde versie van Cisco IOS® XE-software uitvoeren.

Als Multihome wordt gebruikt, is het sterk aanbevolen over-boom moet worden ingeschakeld op de OTV-routers omdat dit de OTV-switch in staat stelt om een bericht van topologieverandering (TCN) te sturen, waardoor het aangrenzende L2-routerapparaat (samen met andere switches in de over-boom) hun leeftijdstimer van het standaard tot 15 seconden vermindert. Dit verhoogt de snelheid convergentie wanneer er een storing of herstel is tussen het multihomed paar. Spanning-tree kan worden ingeschakeld voor alle geconfigureerde service-instanties (verbonden met OTV of anderszins) door de toevoeging van de volgende lijn aan de globale configuratie.

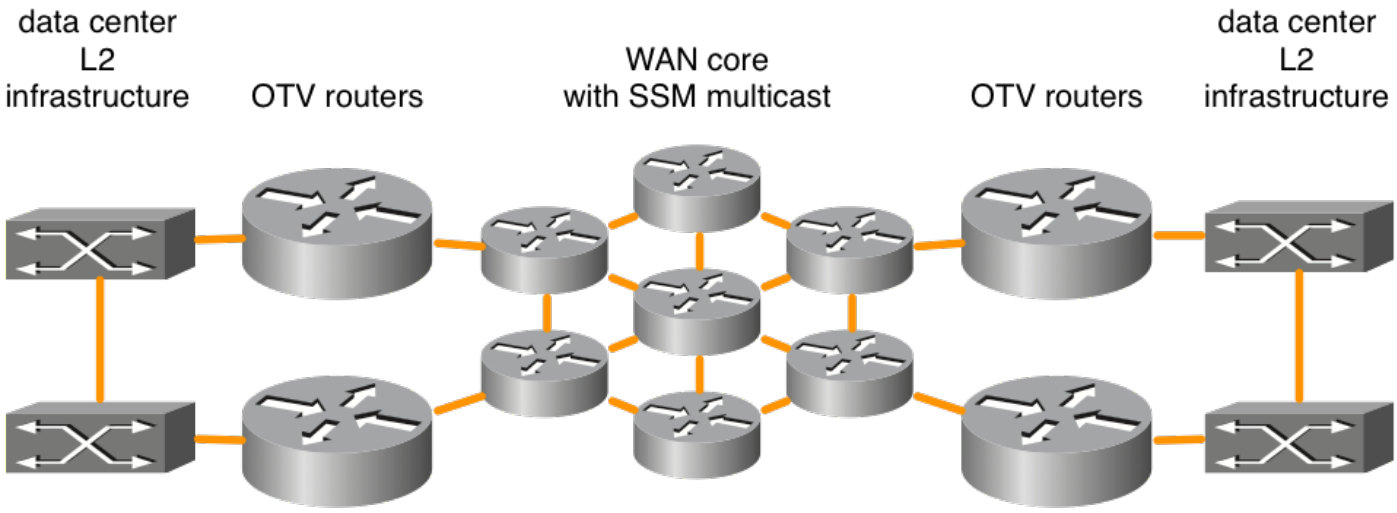
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

Er is geen specifieke configuratie per VLAN of per servicecontract vereist.

Multicastkern

Multicast-netwerk vereist volledige mesh-connectiviteit via het WAN. Alle OTV-routers moeten met elkaar verbonden zijn via de Josef-interface.

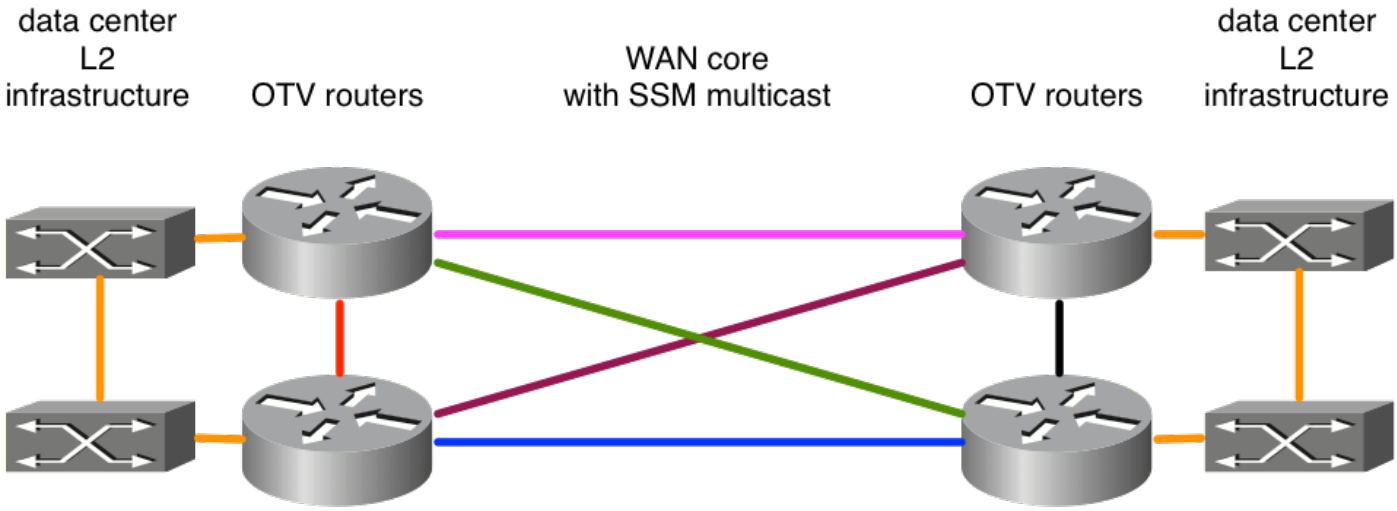
Afbeelding 1. Ondersteunde multicast-netwerktopologie



Dit cijfer toont een voorbeeld van twee datacentra die door een kern in volledig netwerk worden verbonden. Source Specific Multicast (SSM) Protocol Independent Multicast (PIM) wordt uitgevoerd tussen de OTV-routers en WAN-kernrouters. Om het even welk aantal kernrouters

wordt gesteund zolang er volledige netwerkconnectiviteit is. Er is geen expliciete maximale latentie-eis voor OTV-connectiviteit over de WAN-kern.

Afbeelding 2. Niet-ondersteunde multicast netwerktopologie



Omdat ASR1000/OTV verwacht multicast-berichten te ontvangen op een enkele, samengevoegde interface van al zijn peers, zou dit per voorbeeld leiden tot onstabiele OTV-implementatie. Veronderstel de Oost-West verbindingen in roze en blauw als gezamenlijke interfaces werden gevormd. Wanneer de roze link uitviel, zou de router niet langer OTV-updates op die interface kunnen ontvangen. Een alternatief pad via de groene of paarse links zou onaanvaardbaar zijn omdat de samenvoegingsinterface expliciet is geconfigureerd. Updates moeten worden ontvangen op die interface. Op dit moment wordt het niet ondersteund om een Loopback-interfaces te gebruiken als de samenvoeginterface.

Als gebruikers hun backbone niet bezitten, moeten ze ervoor zorgen dat hun serviceprovider multicast ondersteunt in hun kern, en de serviceprovider kan reageren op IGMP-query-berichten (Internet Group Management Protocol). OTV op ASR1000 fungeert als multicast host (forwards IGMP-Josef-berichten), niet als een multicast router voor de kern-WAN-multicast topologie.

Het transportnetwerk tussen de OTV-routers moet de PIM sparse mode (Any Source Multicast [ASM]) ondersteunen voor de provider-multicast groep en SSM voor de bezorgingsgroep.

Multicastkernen vereisen enige specifieke configuratie op de Overlay-interface voor een controlegroep evenals een reeks gegevens multicast groepen die voor het doorsturen van gegevens worden gebruikt.

```
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
```

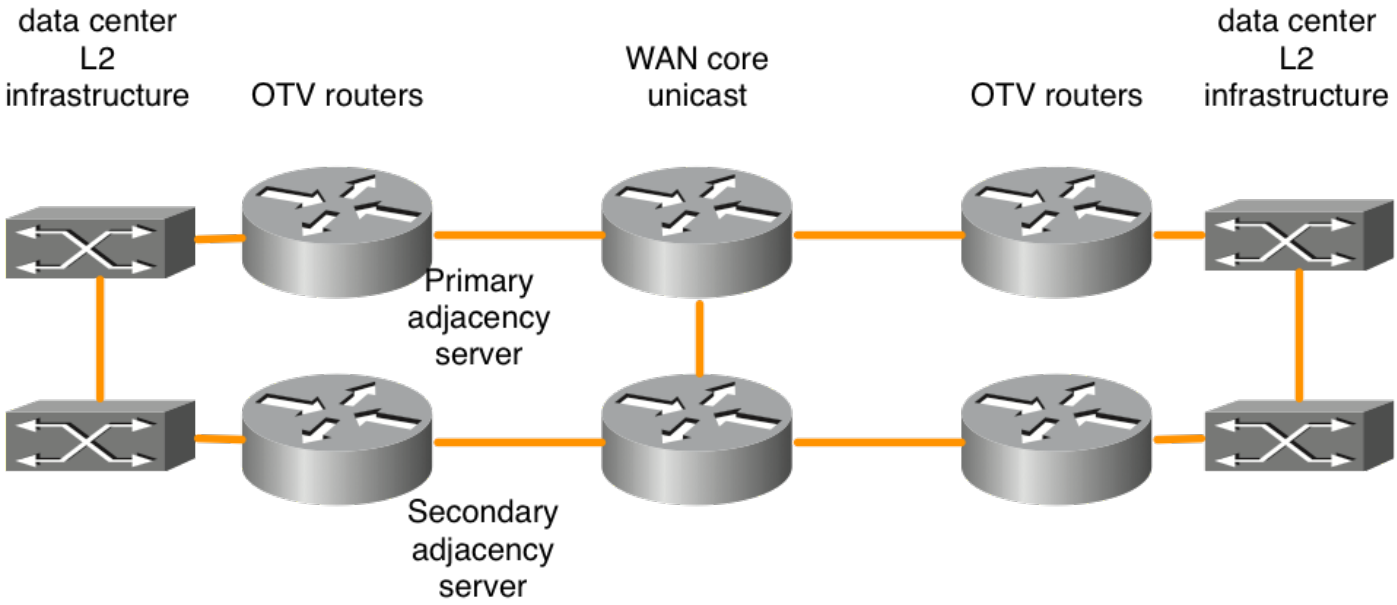
Multicast OTV implementaties vereisen dat de Josef interface als passieve PIM interface wordt gevormd. IGMP kan indien nodig voor verschillende versies worden geconfigureerd. De overlay-interface moet een controle-groep en een gegevensgroep hebben geconfigureerd. De controlegroep is één enkele multicast groep die voor beheer OTV wordt gebruikt. De datagroep is een reeks multicastadressen die worden gebruikt om gebruikersgegevens tussen datacenters te transporteren. Als de gegevensgroep niet in de 232.0.0.0/8 IP-ruimte zit, moet de aanvullende opdracht "ip pim ssm-bereik" zo worden geconfigureerd dat deze het door OTV vereiste bereik bevat.

Het transportnetwerk tussen de OTV-routers moet de dunne PIM-modus (Any Source Multicast [ASM]) ondersteunen voor de provider-multicast groep en Source Specific Multicast (SSM) voor de leveringsgroep.

Unicast Core met aanpassingsservers

Cisco IOS® XE 3.9 voegde ondersteuning toe voor OTV met een unicastkern. Zowel unicast- als multicast-cores voor OTV blijven worden ondersteund voor alle ASR 1000-platforms en toekomstige releases van Cisco IOS® XE 3.9.

Afbeelding 3. Unicast-netwerktopologie



De functie OTV Adjacency Server maakt eenmalig transport tussen OTV Edge mogelijk. OTV-routers die zijn geconfigureerd met de nabijheidsserverrol houden een lijst bij van alle bekende OTV-routers. Zij verstrekken die lijst aan alle geregistreerde routers OTV zodat zij een lijst van apparaten hebben die herhaalde uitzending en multicast verkeer moeten ontvangen.

Het OTV-besturingsplane over een eenfasig transport werkt precies op dezelfde manier als OTV

met multicast core, behalve dat in een unicast-core netwerk elk OTV-randapparaat meerdere kopieën moet maken van elk regelingsplane pakket en ze in dezelfde logische overlay unicast aan elk afstandsbediening apparaat moet toevoegen.

In dezelfde gedachtegang wordt elk multicastverkeer vanuit het datacenter gerepliceerd op de lokale OTV-router en worden meerdere kopieën naar elk van de externe datacenters verzonden. Hoewel dit minder efficiënt is dan afhankelijk te zijn van de WAN-kern om de replicatie uit te voeren, zijn de configuratie en het beheer van het kern-multicast netwerk niet vereist. Als er slechts een kleine hoeveelheid datacenter multicast-verkeer is of als er slechts een klein aantal datacenterlocaties (vier of minder) zijn, is een unicastkern voor OTV-doorsturen doorgaans de beste keuze. In het algemeen geeft de operationele vereenvoudiging van het unicast-only model de voorkeur aan de optie voor de implementatie van de unicast-kern in scenario's waarin slechts tussen vier of minder datacenters LAN-uitbreidingsconnectiviteit vereist is. Aanbevolen wordt ten minste twee nabijheidsservers te configureren, één primaire en één back-up. Er is geen optie voor actieve/actieve configuratie van een nabijheidsserver.

OTV-routers moeten dienovereenkomstig worden geconfigureerd om zich correct te identificeren en te registreren met de juiste nabijheidsserver.

	Primaire nabijheidsserver	Secundaire nabijheidsserver	Andere OTV-routers
OTV-koppeling van IP-interface	10.0.0.1	10.2.2.24	andere IP-adressen
Configuratie	interface-overlay 1 Toetsenbord-nabijheidsserver unicast-only	interface-overlay 1 Toetsenbord-nabijheidsserver unicast-only Toetsenbord use-nabijheidsserver 10.0.0.1 unicast-only	interface-overlay 1 Open use-nabijheidsserver 10.0.0.1 10.2.2.24 unicast-only

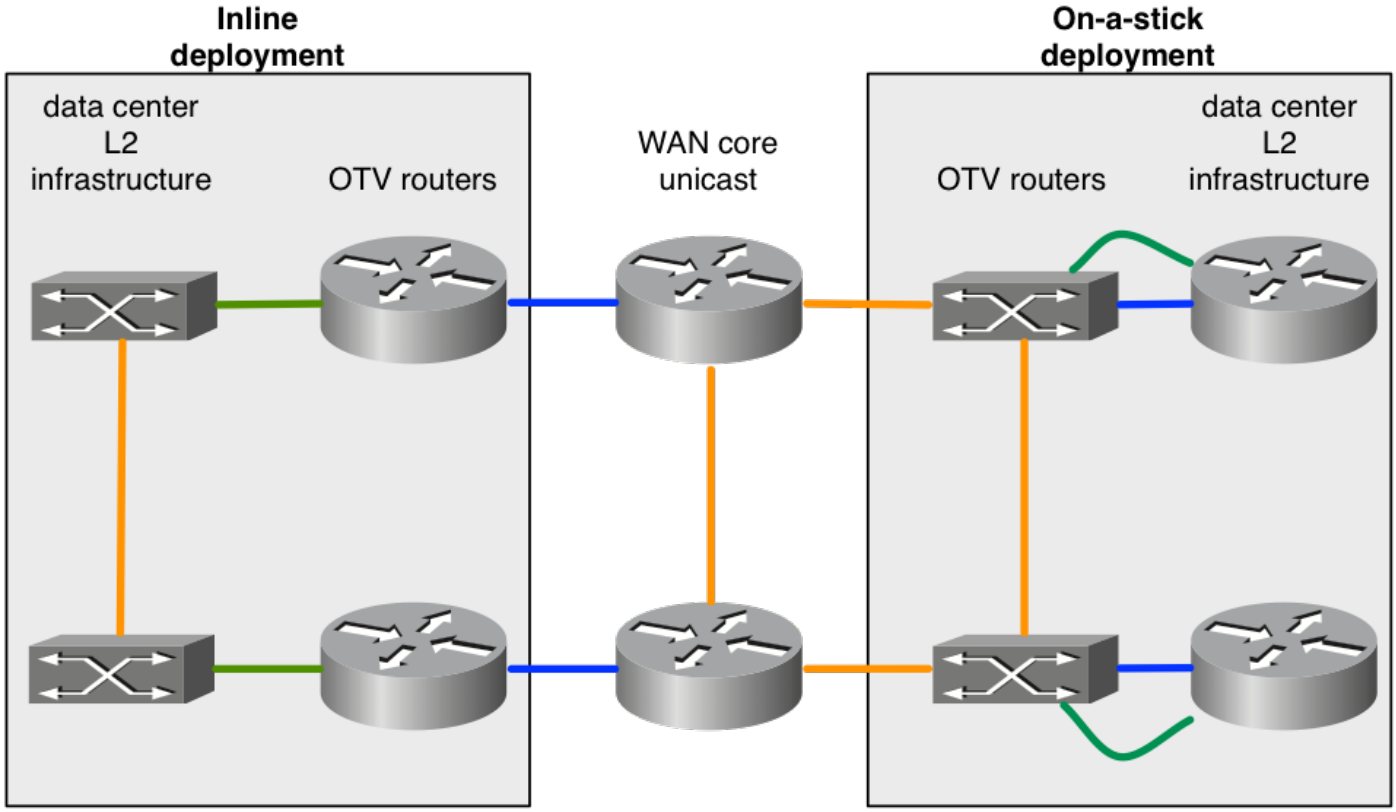
Er zijn bepaalde ontwerpen voor back-to-back connectiviteit die worden ondersteund met unicast OTV-doorsturen die niet voldoen aan de regels voor "volledige mesh". Hoewel deze configuraties worden ondersteund, worden ze niet aanbevolen. Dit type implementatie komt het meest voor wanneer datacenters worden aangesloten via dark fibre. Details over deze configuratieoptie kunnen worden gevonden in de latere sectie "Special case unicast topology".

OTV op een Stick versus Inline

Er zijn twee modellen om OTV in uw datacenter te implementeren: op een stick en inline. In de eerder gepresenteerde ontwerpscenario's waren OTV-routers inline tussen het datacenter en het kernnetwerk van de serviceprovider. De toevoeging van de OTV-router als apparaat dat het niet in

het vervoerspad van al het verkeer is, zou echter meer wenselijk kunnen zijn. Soms is het vereiste om de huidige topologie niet te veranderen om met de dienstverlener door huidig materiaal (bijvoorbeeld, een brownfield plaatsing met Catalyst 6000 switch of de hardware van de Nexus switch die geen OTV steunt) te verbinden. Daarom is het de voorkeur om OTV op ASR1000 als op een stok als OTV apparaat te gebruiken.

Afbeelding 4. Inline versus on-a-stick topologie



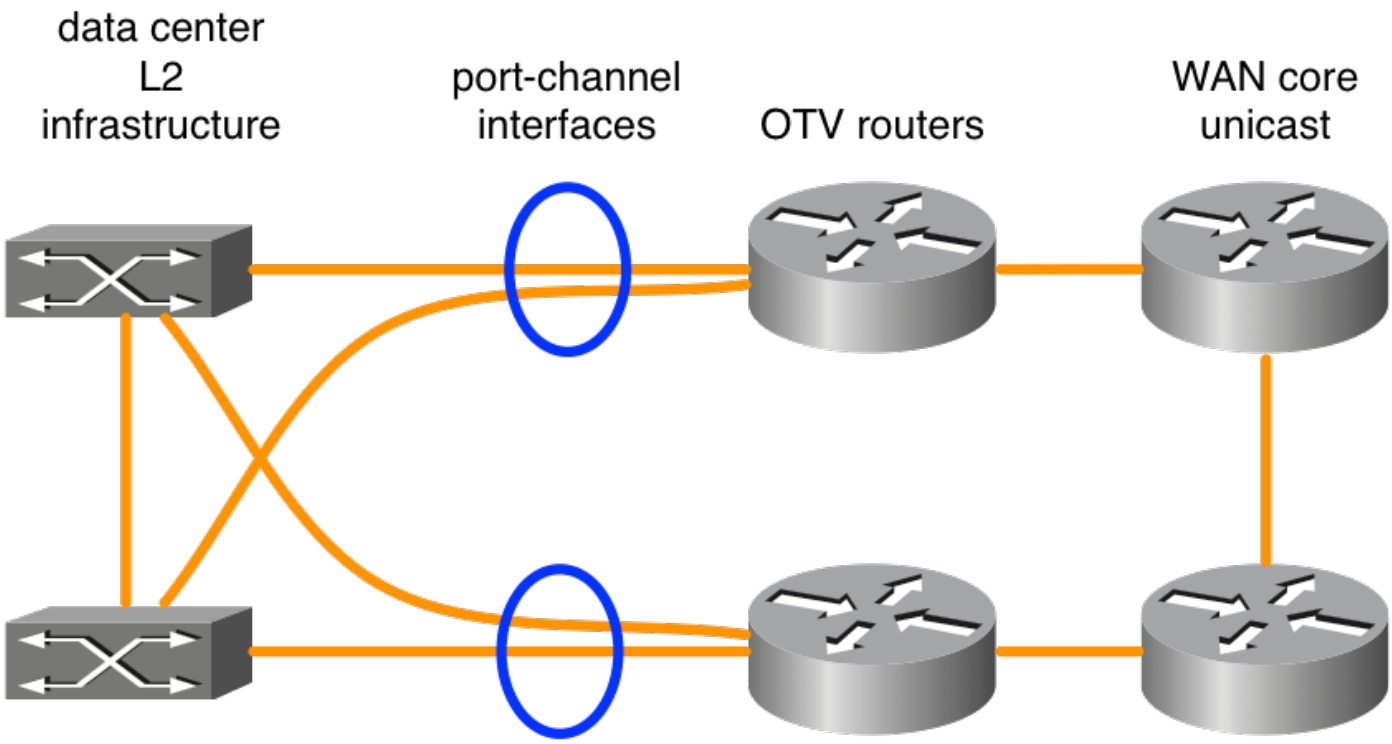
Het diagram toont de twee implementatiemodellen aan die deel kunnen uitmaken van dezelfde overlay. De groene links die zijn aangesloten op de OTV-routers zijn geconfigureerd als L2-toegangsinterfaces om VLAN-verkeer te accepteren. De blauwe koppelingen die met de OTV-routers zijn aangesloten, zijn de samengevoegde interfaces die OTV-ingekapseld VLAN-verkeer dragen.

Het kan nodig zijn om een optie te configureren die niet wordt ondersteund door OTV. OTV en MPLS kunnen bijvoorbeeld niet in hetzelfde vak worden geconfigureerd. Hierdoor kan het een goede optie zijn om ASR 1000/OTV op een stick te gebruiken en MPLS te configureren op de router die voor de OTV router zit.

Poortkanalen voor Layer 2 en Layer 3

Cisco IOS® XE 3.10-code voor ASR 1000 extra ondersteuningslaag 2 en Layer 3-poorts poortkanaals configuratie met OTV. Layer 2-poortkanaal kan als interne interface worden gebruikt. Het poortkanaal moet bestaan uit maximaal 4 fysieke interfaces. Layer 3 Port-channel kan worden gebruikt als de samengevoegde interface.

Afbeelding 5. Poortkanalen gebruikt voor L2-connectiviteit



In het diagram wordt een typisch poortkanaalscenario met twee switches in VSS (Catalyst 6000 Series) of VPC (Nexus 7000 Series) weergegeven. Dit type ontwerp biedt redundantie met dubbele OTV-routers en dubbele connectiviteit met datacenterinfrastructuur. Als VSS of VPC wordt gebruikt op L2-schakelapparatuur die grenst aan de OTV-routers, is er geen speciale configuratie voor OTV anders dan de basis-poortkanaalconfiguratie vereist.

Standaardgateway

OTV maakt per definitie hetzelfde L3-subnet op meerdere locaties. Dit vereist enkele speciale overwegingen bij het routing van L3-verkeer naar en van de uitgebreide VLAN's. L3-routing kan worden geconfigureerd op de OTV-routers zelf of op andere apparaten die zijn aangesloten op de uitgebreide VLAN's. Bovendien kunnen in elk scenario eerste hop redundantie protocollen (FHRP) zoals Hot Standby Redundantie Protocol (HSRP) of Virtual Router Redundantie Protocol (VRRP) worden geïmplementeerd voor redundantie. HSRP kan lokaal naar een bepaald datacenter worden uitgevoerd of tussen datacenters worden uitgebreid (niet standaard).

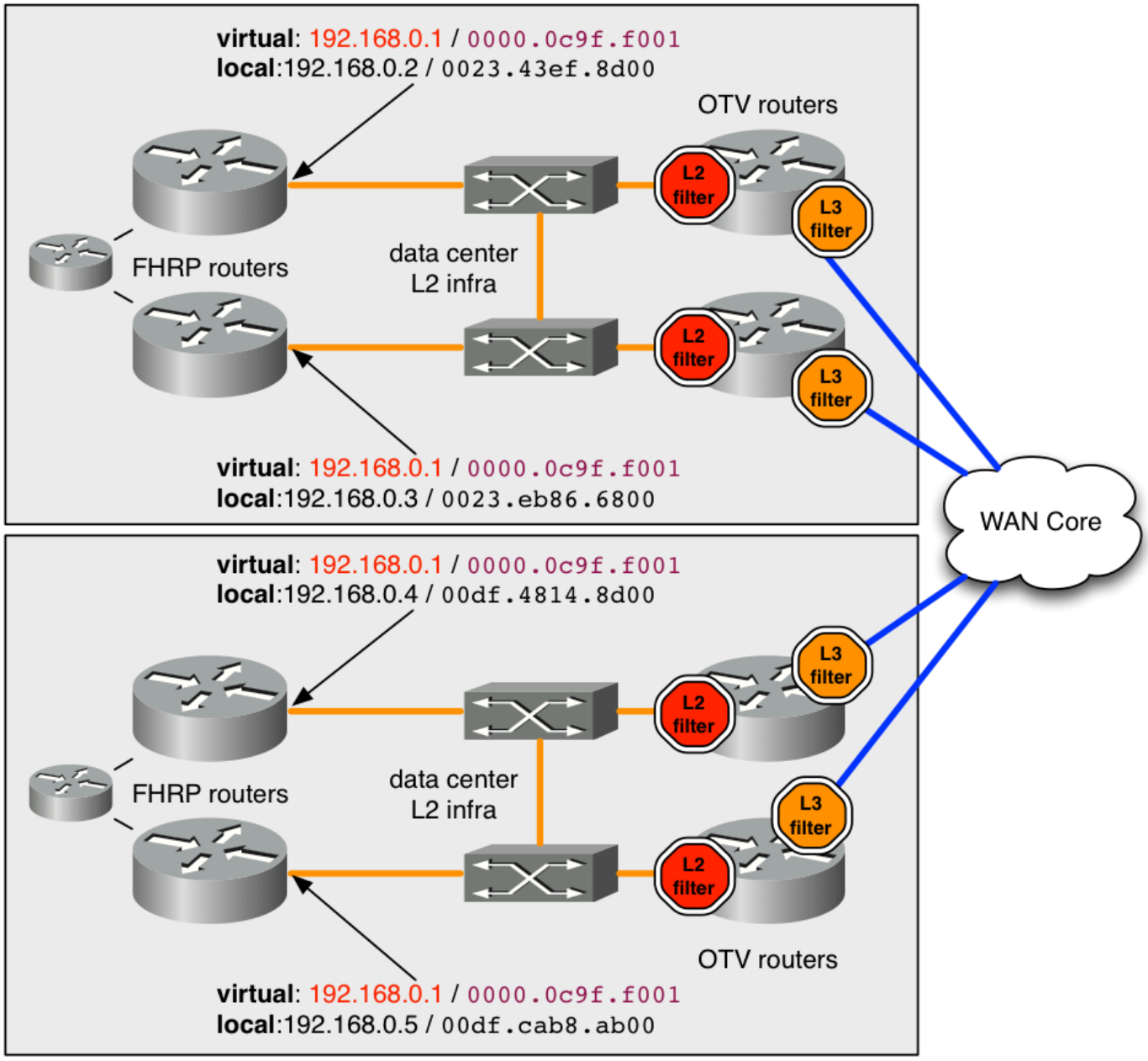
De beste praktijk voor OTV implementaties die gebruik maken van FHRP, is om lokale instanties van de FHRP uitgevoerd te hebben in elk datacenter. Die instanties van FHRP gebruiken hetzelfde virtuele MAC-adres en IP-adres, zodat wanneer virtuele machines (VM's) tussen datacenters bewegen, ze een ononderbroken verbinding hebben. Als het MAC-adres van de standaardrouter tussen datacenters zou veranderen, zouden de VM's niet in staat zijn om van het subnetnetwerk te communiceren totdat de ARP-ingang van de standaardgateway van de VM is uitgezet.

Om een FHRP correct met OTV te implementeren, is het noodzakelijk om te overwegen welk L2- en L3-verkeer moet worden gefilterd en geïsoleerd van OTV. Op L2-niveau is dit nodig om OTV te beschermen tegen het zicht van dezelfde L2 virtuele MAC die door de FHRP op meerdere locaties wordt gebruikt. Er zijn filters op L3-niveau nodig om HSRP- en VRRP-advertenties geïsoleerd te

houden voor elk datacenter, zodat de selectie van actief/luisterend/stand-by is gelokaliseerd naar elk datacenter.

Standaard zijn de FHRP-filters ingeschakeld wanneer OTV ingeschakeld is. Het kan worden uitgeschakeld als het ontwerp vereist dat FHRP wordt uitgebreid tussen datacenters. L2-filtering van virtuele MAC-adressen is standaard NIET ingeschakeld en moet handmatig worden ingesteld.

afbeelding 6. Voorbeeld van aanbevolen inzet voor FHRP



In het voorbeeld wordt het virtuele MAC-adres 0000.0c9f.f001 gebruikt voor het IP-adres 192.168.0.1, dat hosts op het uitgebreide VLAN biedt voor de connectiviteit van het subnet. Gebruik van dezelfde virtuele MAC en IP in beide datacenters, een host heeft naadloze connectiviteit van het subnetnet wanneer het overbrengt tussen datacenters.

Om het MAC-adres 0000.0c9f.f001 op meerdere locaties verborgen te houden voor OTV, moet er een L2-filter (rode stop in het diagram) worden geïmplementeerd voor het VLAN op elk van de OTV-routers , dat het VLAN onderhoudt. Door het ACL-filter wordt de filter ACL die op de L2-

service-instanties is geconfigureerd voor toegang, alle pakketten die afkomstig zijn van die MAC, gedropt voordat het OTV-proces op de ASR1000 ze kan zien. Zo leert OTV nooit over de MAC, en adverteert het niet naar externe datacenters.

De aanbevolen configuratie om al het bekende / standaard FHRP virtuele MAC-verkeer te vangen wordt hier gegeven.

```
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
```

Deze ACL komt overeen met de bekende MAC-adresruimtes die zijn gekoppeld aan HSRP-versies 1 en 2, Gateway Load Balancing Protocol (GLBP) en VRRP (in die volgorde). Als de virtuele MAC is geconfigureerd om een niet-standaardwaarde te gebruiken die niet is gebaseerd op het FHRP-groepsnummer, moet deze expliciet worden toegevoegd aan het ACL-voorbeeld. ACL moet worden toegevoegd aan L2-service (hier getoond).

```
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
```

Het is ook nodig om de communicatie tussen de FHRP-hosts op L3-niveau te beheren. Er zijn vier FHRP-routers geconfigureerd op één uitgebreide subnetvoeding in het diagram. Zonder enige graad van L3 Filters, zouden alle vier routers elkaar zien en één enkel actief apparaat selecteren en 3 in diverse standby staten hebben. Zodoende zou één datacenter twee lokale stand-by FHRP routers hebben maar geen L2-verbinding met de externe actieve router als gevolg van de eerder besproken L2 Filters.

Het gewenste resultaat is een actieve en een stand-by FHRP router in elk datacenter. De eerder besproken toegang L2 filter vangt dit verkiezingsverkeer niet aangezien het verkiezingsproces de daadwerkelijke IP van de router en de adressen van MAC gebruikt. Standaard wordt de volgende ACL toegepast als uitgang op de Overlay-interface. Uitgang voor de interface van de Overlay zou verkeer naar de kern van WAN zijn. ACL verschijnt niet in lopende configuratie, maar het kan met "tonen ip toegang-lijst" worden waargenomen. Het filtert het FHRP-verkiezingsverkeer op basis van UDP-poortnummer.

```
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
```

De enige reden om dit filter uit te schakelen zou zijn als u alle FHRP-routers op een VLAN wilt, om deel te nemen aan dezelfde selectie voor actieve status. Om dit filter uit te schakelen, configureer "geen otv-filter-fhrp" op de Overlay-interface.

Onbekend Unicast-verkeer

Standaard wordt unicastverkeer dat van het LAN wordt ontvangen door de OTV-router en bestemd is voor een MAC-adres dat niet bekend is bij een externe OTV-locatie, verwijderd. Dit verkeer staat bekend als unicast unicast. Deze druppelactie gaat naar de kern van WAN die de hoeveelheid bandbreedte beperkt die op WAN door uitzendingsverkeer wordt verbruikt. De algemene verwachting is dat alle hosts op het LAN probleem genoeg uitzendverkeer (ARP's, protocol uitzendingen, enzovoort) dat altijd moet worden gezien door een OTV-router, geadverteerd, en dus 'bekend'.

Sommige toepassingen maken gebruik van stille hosts. Op een normale schakelinfrastructuur is dit geen probleem, aangezien L2-uitzending van onbekende unicast MAC-adressen op het LAN de stille host in staat stelt het verkeer te zien. In een OTV-omgeving blokkeert de OTV-router echter het verkeer tussen de datacenters.

Om dit te compenseren, is een functie die Selective Unicast Forwarding wordt genoemd, geïntegreerd in Cisco IOS® XE. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 en alle releases hebben daarna ondersteuning voor selectieve unicast Forwarding.

Het wordt geconfigureerd door de toevoeging van één opdracht per MAC-adres in de Overlay-interface. Voorbeeld:

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

Om het even welk verkeer dat voor 0000.001.0001 wordt bestemd moet aan alle verre routers OTV met VLAN 100 in dit voorbeeld worden overstroomd. Dit kan door het verdere bevel worden waargenomen:

<#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
```

Als dat MAC-adres op een externe locatie wordt geleerd, moet een ingang worden toegevoegd aan de voorwaartse tabel die voorrang heeft op de vloedingang.

<#root>

OTV_router_1#

show otv route

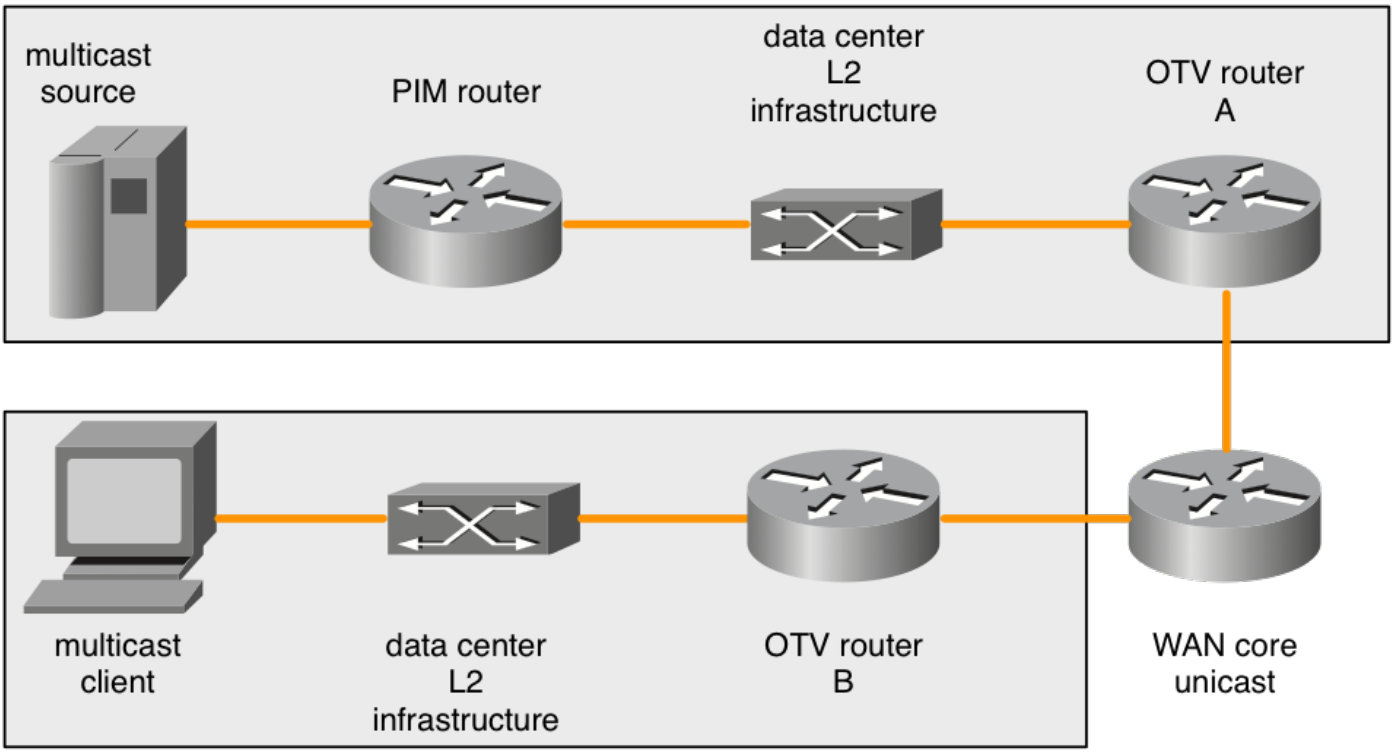
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood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

Over het algemeen, moet een overstroming ingang voor een bepaald adres van MAC op alle routers OTV met dat VLAN worden gevormd.

Remote multicast-bronnen

ASR1000 dat een OTV-router multicast IGMP niet doorstuurt, sluit zich aan bij verzoeken die van het LAN zijn ontvangen. In het volgende diagram wordt de topologie beschreven waar dit een probleem kan zijn.

Afbeelding 7. Remote multicast-bronnen



Wanneer een multicast IGMP-verbinding wordt verzonden door de multicast-client, wordt deze geobserveerd door de ASR 1000 (OTV-router B) en wordt interesse in de multicast groep geadverteerd. De externe OTV-routers (OTV-router A) moeten elk verkeer doorsturen naar die multicast-groep die ze op hun lokale L2-uitzenddomein zien. De externe ASR1000 (OTV router A) regenereert de multicast IGMP-verzoeken echter niet wanneer de interesse in een multicast groep wordt geadverteerd van de OTV-router van de client (OTV router B).

Wanneer multicast bronnen op hetzelfde L2 uitzenddomein zijn als de OTV router dan is dit geen probleem. De router OTV moet worden geconfigureerd als een IGMP-querier. Dit verschijnt in elk multicast verkeer op het L2 broadcast-domein. Echter, alleen een PIM-samenvoegverzoek zou een PIM-router ertoe aanzetten een multicast-bron van een ander L2 broadcast-domein door te sturen naar het L2 broadcast-domein waar de OTV-router is ingeschakeld.

De externe IGMP-deelname wordt niet doorgestuurd of opnieuw gegenereerd. OTV-routers zijn ook geen PIM-routers. Zo hebben topologieën met multicast bronnen niet direct op het L2 uitzendingsdomein met de router OTV geen manier om routers in te lichten PIM om bronverkeer door te sturen wanneer er rente door een verre cliënt is.

Dit probleem kan op twee manieren worden opgelost.

Eerst kunnen een lokale IGMP-client(s) worden geïmplementeerd op het L2-uitzenddomein dat aan de OTV-router is gekoppeld (OTV-router A). Die IGMP-client zou zich moeten abonneren op alle multicast-groepen waarop externe clients zich kunnen abonneren. Dat zou de PIM router veroorzaken om het multicast verkeer aan het uitzendingsdomein naast router A. door:sturen. De IGMP-vragen zouden dan in elk multicast-verkeer worden getekend en over de overlay worden verzonden.

De andere oplossing zou zijn om een "ip igmp statisch-toetreden"voor om het even welke groepen te vormen dat de verre cliënten mogelijk aan konden intekenen. Dit zou ook de PIM router ertoe

aanzetten het multicast verkeer naar het uitzendingsdomein naast OTV router A. door te sturen.

Deze beperking is bekend en maakt deel uit van de ontwerpspecificatie. Het wordt niet beschouwd als een bug, maar een limiet in ondersteunde topologie op dit moment.

QoS-overwegingen

Standaard wordt op ASR 1000 de TOS-waarde in de toegevoegde OTV-header gekopieerd van de 802.1p-bits van het L2-pakket. Als het L2 pakket niet is gelabeld, wordt een waarde nul gebruikt.

Nexus 7000 heeft een ander standaardgedrag in 5.2.1 software en nieuwer. Als het gewenste gedrag de innerlijke pakketten TOS waarde in de router moet kopiëren, kan de extra configuratie QoS dit bereiken. Dit geeft hetzelfde gedrag als de nieuwere Nexus 7000 software.

De configuratie om de L2-pakketwaarde van L3 TOS naar de buitenste header van het OTV-pakket te kopiëren is de volgende:

```
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
```

De verstrekte configuratie moet verkeer voor diverse waarden DSCP op toegang aanpassen. De lokaal significante qos-groep tag wordt gebruikt om dat verkeer tijdens de doorvoer door de router intern te markeren. Bij de uitgangsinterface wordt de qos-groep gekoppeld en wordt de buitenste TOS-byte dienovereenkomstig bijgewerkt.

WAN MTU-overwegingen/fragmentatie

OTV gebruikt in wezen een GRE-header om L2-verkeer over het WAN te transporteren. Deze GRE-header is 42 bytes groot. In een ideale netwerkimplementatie moet de WAN-link een maximale transmissieeenheid (MTU) hebben die ten minste 42 bytes groter is dan het grootste pakket dat OTV naar verwachting zal verwerken.

Als de L2 interface een MTU van 1500 bytes heeft, dan moet de Joop interface een MTU van 1542 bytes of meer hebben. Als de L2 interface een MTU van 2000 bytes heeft, maar alleen wordt verwacht om pakketten te verwerken zo groot als 1500 bytes, dan is een WAN MTU van 1542 bytes voldoende, maar de standaard toevoeging van 42 aan de 2000 zou ideaal zijn.

```
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
```

Sommige serviceproviders zijn niet in staat om grotere MTU-waarden te leveren voor hun WAN-circuits. Als dat het geval is, kan ASR1000 fragmentatie van de OTV getransporteerde gegevens uitvoeren. Nexus 7000 heeft deze mogelijkheid niet. Gemengde ASR 1000- en Nexus 7000 OTV-netwerken met fragmentatie ingeschakeld op de ASR 1000 worden niet ondersteund.

De configuratie voor OTV-fragmentatie is:

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

Het is belangrijk dat de opdracht op mondiaal niveau wordt geconfigureerd voordat de opdracht

Overlay-interface-samenvoeging-interface wordt uitgevoerd. Als de opdracht samenvoegen-interface van de overlay-interface eerst is geconfigureerd, verwijder de opdracht samenvoegen-interface van de otv-interface uit de overlay-interface, configureer de opdracht samenvoegen-interface van de otv-fragmentatie en interface opnieuw.

Wanneer OTV-fragmentatie niet is ingeschakeld, worden alle OTV-pakketten met ingekapselde L2-gegevens met de DF-bitset verzonden, zodat ze tijdens het transport niet worden gefragmenteerd. Zodra de fragmentatieopdracht is toegevoegd, wordt de DF-bit ingesteld op 0. De OTV-routers zelf kunnen het pakket fragmenteren en het kan tijdens het transport worden gefragmenteerd door andere routers.

Er zijn beperkte buffers voor pakkethermontage beschikbaar op de ASR1000-platforms, dus hoe minder fragmenten er in een pakket moeten worden gehakt voor transmissie, hoe beter. Dit verhoogt de efficiëntie en verlaagt het algemene bandbreedteverbruik over het WAN als dat een probleem is. Er zijn gevolgen voor de prestaties om fragmentatie van OTV mogelijk te maken. Als fragmentatie aanwezig is en de verwachting is dat meer dan 1 Gb/sec OTV-verkeer zal worden verwerkt, moeten de prestaties van OTV verder worden onderzocht.

Speciale case voor Unicast-topologie

Veldimplementaties voor OTV hebben vaak directe back-to-back glasvezelverbindingen tussen de OTV-routers in twee datacenters.

Voor single-homed topologieën maakt dit een standaardplaatsing waar OTV en niet-OTV verkeer de samen te voegen interface delen. Voor deze instelling zijn geen speciale overwegingen nodig, dus deze sectie is niet van toepassing.

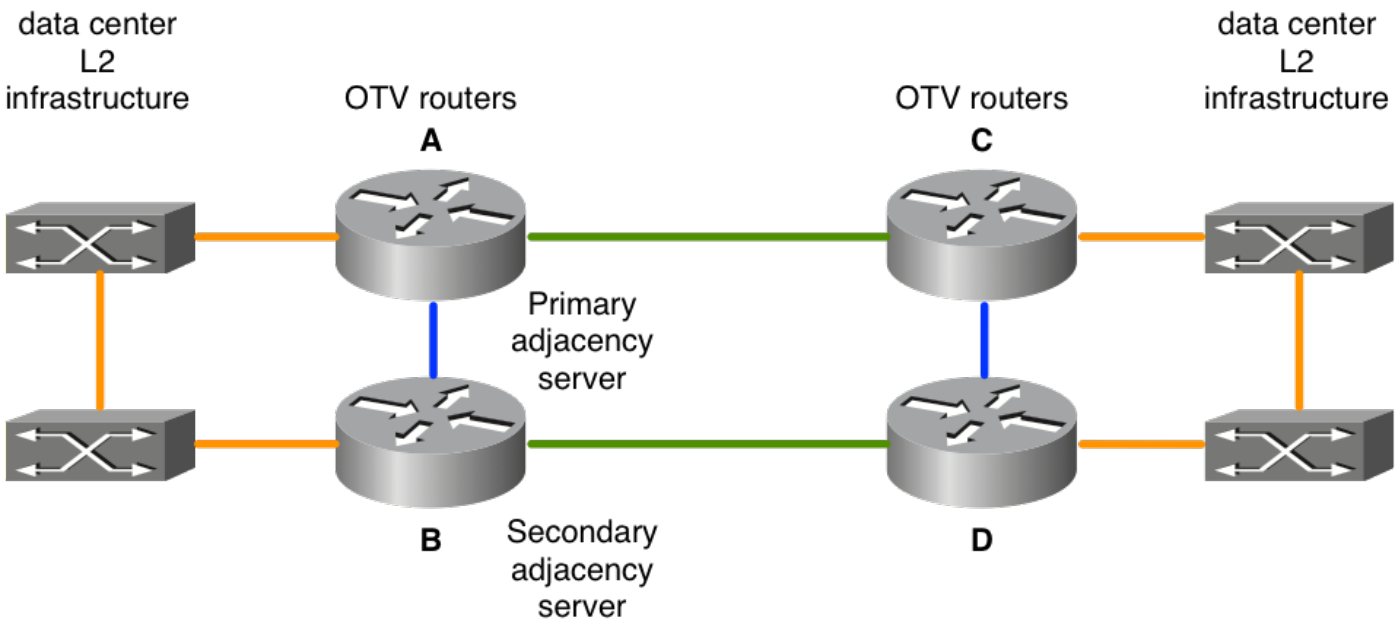
Als de implementatie echter meerdere OTV-routers heeft in de twee datacenters, zijn er enkele speciale overwegingen. Er is een aanvullende configuratie vereist.

Als er meer dan twee datacenters zijn betrokken, is deze speciale configuratie niet van toepassing.

Voor het scenario met meer dan twee datacenters met single- of multi-homed OTV-routers moet een standaard unicast of multicast OTV-implementatie worden gebruikt.

Er is geen ander alternatief dat wordt ondersteund.

Afbeelding 8. Speciale case-unicast



In de voorgestelde topologie, zijn de verbindingen in groen de donkere vezelverbindingen tussen de twee gegevenscentra. Deze donkere vezels zijn direct gekoppeld aan de OTV-routers. De blauwe verbindingen tussen de routers OTV worden gebruikt om niet-OTV verkeer in het geval van een mislukking van de groene verbindingen om te leiden. Als de bovenste groene link mislukt (A naar C), zou niet-OTV verkeer dat de hoogste OTV-routers gebruikt als hun standaardroute via de noord-zuid blauwe links (A naar B en C naar D) worden gerouteerd naar de nog steeds operationele groene link tussen het onderste OTV-routerpaar (B naar D).

Deze basisomleiding van verkeer werkt niet voor OTV-verkeer omdat de OTV-configuratie een fysieke interface specificeert als de samengevoegde interface. Als de "groene interface" op OTV router A daalt, kan het OTV-verkeer niet afkomstig zijn van een alternatieve interface OTV router B. Bovendien, aangezien er geen volledige connectiviteit via de WAN-kern is, kunnen alle OTV-routers niet worden geïnformeerd wanneer er een storing is. Om dit probleem te omzeilen wordt bidirectionele doorsturen detectie (BFD) samen met embedded event manager (EEM) scripting gebruikt.

BFD moet de WAN-verbinding tussen de oost-west OTV routerparen (A / C en B / D) bewaken. Als de verbinding met de afstandsrouter verloren gaat, wordt de OTV Overlay-interface uitgeschakeld via het EEM-script op dat oost-west paar OTV-routers. Dit zorgt ervoor dat de gepaarde multi-home router ervan uitgaat dat alle VLAN’s worden doorgestuurd. Wanneer BFD detecteert dat de link is hersteld, wordt de Overlay-interface opnieuw ingeschakeld door het EEM-script.

Het is van groot belang dat de BFD wordt gebruikt om koppelingsfouten te detecteren. Dit komt doordat de Overlay-interface moet worden afgesloten aan zowel de "mislukte" kant als aan de oost-west-paar. Wat afhankelijk is van het type connectiviteit dat door de dienstverlener wordt verstrekt, kan één fysieke verbinding dalen (groene interface op router OTV A) terwijl de overeenkomstige interface van het oost-westpaarrouter kan omhoog blijven (groene interface op router OTV C). BFD ontdekt mislukking van één van beide interface of een ander probleem in doorgang en brengt onmiddellijk beide paren gelijktijdig op de hoogte. Het zelfde is van toepassing op wanneer de routers van de terugwinningsverbinding moeten worden geïnformeerd.

De configuratie voor deze implementatie is dezelfde als alle andere implementaties met toevoeging van de volgende items:

- BFD-configuratie op de WAN-interface
- het daaropvolgende EEM-script
- OTV IS-identiteit voor even/oneven VLAN-distributie

De configuratie van de BFD op de OTV-koppeling valt buiten het bereik van dit document. Informatie over het configureren van de BFD op de ASR 1000 is te vinden op:

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

Zodra de detectie van BFD-storingen correct werkt tussen de samengevoegde interfaceparen (groene koppelingen in het diagram), moet het EEM-script worden geïmplementeerd. Het EEM-script moet worden aangepast aan de specifieke routers om de juiste Overlay-interfaces aan te passen en wellicht te controleren op meer exacte strings in het log voor BFD-uitval en herstel.

```
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 ..."
!
```

Dit type van plaatsing vereist ook dat de oost-west routerparen (A/C en B/D) in hun het door:sturen van oneven en zelfs VLAN's aanpassen.

Bijvoorbeeld, A en C moeten zelfs VLAN’s doorsturen terwijl B en D oneven VLAN’s doorsturen in stabiele nominale bediening.

De oneven / gelijkmatige verdeling wordt bepaald door het OTV ordinaal nummer dat kan worden waargenomen door de "show tv site" opdracht.

Het rangtelwoord tussen de twee siterouters wordt bepaald op basis van de OTV ISIS net ID.

```
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
```

De OTV ISIS net identifier moet worden geconfigureerd op alle OTV routers. Bij de configuratie van de identifier moet er wel voor worden gezorgd dat alle OTV-routers elkaar nog steeds herkennen.

<#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

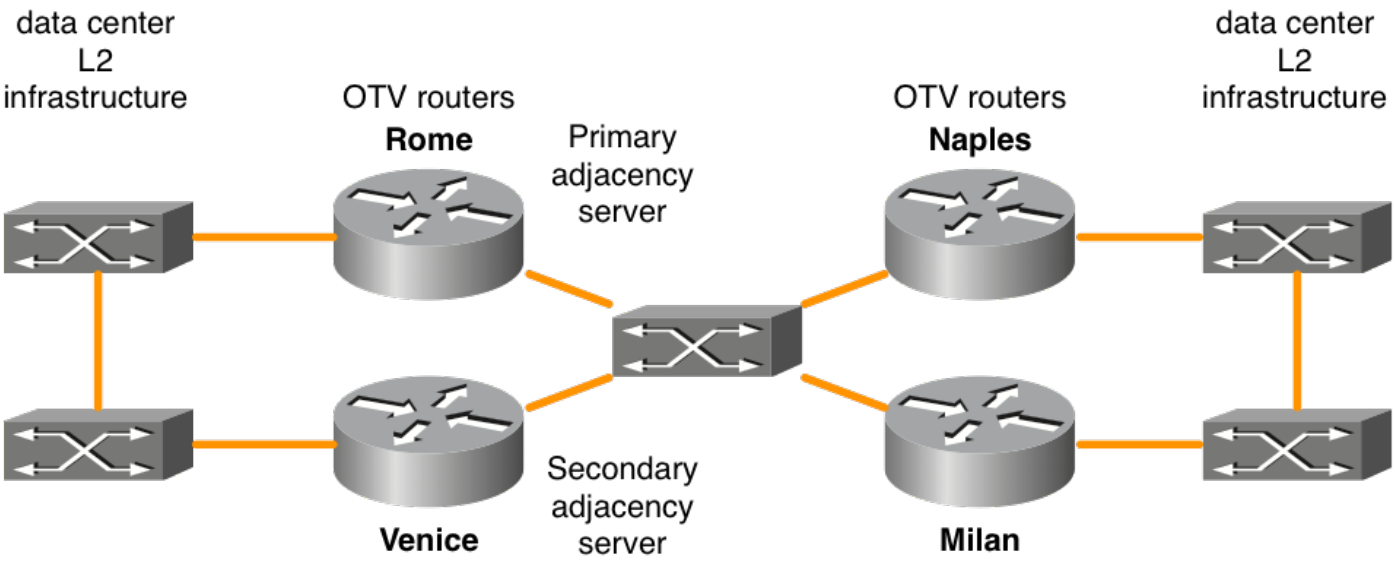
De delen van de herkenningsteken in zwart moeten over alle routers OTV die aan de bekleding

deelnemen aanpassen. Het gedeelte van de identificator in rood kan worden gewijzigd. De laagste netwerkidentificatie op een site krijgt ordinaal nummer 0 en vervolgens de even genummerde VLAN's. Het hoogste netwerkherkenningsteken bij een plaats krijgt rangtelwoord 1 en door:sturen het oneven aantal VLANs.

Configuratievoorbeelden

Unicast

Afbeelding 9. Unicast-configuratievoorbeeld



Rome-configuratie:

```
!
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
 !
```

Configuratie Venetië:

```
!
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
 !
```

Configuratie Napels:

```
!
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
 !
```

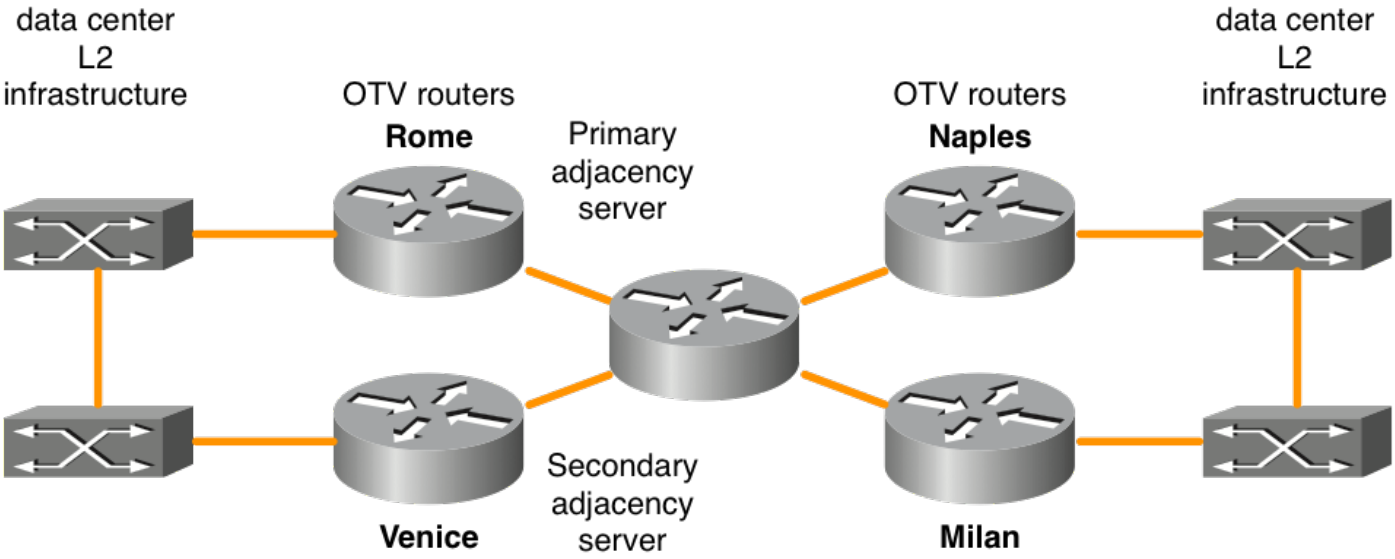
```
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Milaan-configuratie:

```
!
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
 !
!
```

Multicast

Afbeelding 10. Multicastconfiguratievoorbeeld



Rome-configuratie:

```
!
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
 !
```

Configuratie Venetië:

```
!
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
 !
```

Configuratie Napels:

```
!
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
 !
!
```

Milaan-configuratie:

```
!
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
 !
!
```

Veelgestelde vragen

Q) Worden Private VLAN's ondersteund in combinatie met OTV?

A) Ja, in OTV is geen speciale configuratie vereist. Zorg er in de private VLAN-configuratie voor dat de aangesloten switch-poorten op de OTV L2-aansluiting in promiscuous mode zijn geconfigureerd.

Q) Wordt OTV ondersteund met IPSEC-encryptie?

A) Ja, Crypto-kaart configuratie op de toe te voegen-interface wordt ondersteund. Er is geen speciale configuratie vereist voor OTV om crypto te ondersteunen. De cryptoconfiguratie voegt echter extra overheadkosten toe en dit moet worden gecompenseerd door de verhoging van WAN MTU vs LAN MTU. Als dit niet mogelijk is, moet OTV fragmentatie worden vereist. OTV-prestaties zijn beperkt tot die van de IPSEC-hardware.

Q) Wordt OTV ondersteund met MACSEC?

A) Ja, ASR 1001-X bevat MACSEC-ondersteuning voor de ingebouwde interfaces. OTV werkt met MACSEC geconfigureerd op de LAN- en/of WAN-interfaces. OTV-prestaties zijn beperkt tot die van de MACSEC-hardware.

Q) Kan een loopbackinterface als toetreden interface worden gebruikt?

A) Nee, alleen Ethernet-, Portchannel- of POS-interfaces kunnen worden gebruikt als OTV-joint interfaces. OTV Loopback Josef interface is op de roadmap maar is momenteel niet gepland voor een release op dit moment.

Q) Kan een tunnelinterface als toetreden interface worden gebruikt?

A)Nee, GRE-tunnels, DMVPN-tunnels of andere tunneltypen worden niet ondersteund als samenvoeginterfaces. Alleen Ethernet-, Portchannel- of POS-interfaces kunnen worden gebruikt als OTV-koppeling voor interfaces.

Q) Kunnen verschillende Overlay interfaces verschillende L2 gebruiken en/of zich bij interfaces aansluiten?

A) Alle Overlay-interfaces moeten naar dezelfde samenvoeging-interface wijzen. Alle bedekkingen moeten worden gekoppeld aan dezelfde fysieke interface voor L2-connectiviteit met het datacenter.

Q) Kan de OTV-site VLAN op een andere fysieke interface worden geplaatst dan de OTV uitgebreide VLAN's?

A) De OTV-site VLAN en uitgebreide VLAN's moeten op dezelfde fysieke interface staan.

Q) Welke functieset is vereist voor OTV?

A) Voor OTV zijn geavanceerde IP-services (AIS) of Advanced Enterprise Services (AES) vereist.

Q) Is een aparte licentie vereist voor OTV op vaste configuratieplatforms?

A) Nee, zolang de ASR1000 wordt uitgevoerd met advipservices of adventerenterprise bootniveau geconfigureerd, is OTV beschikbaar.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.