Konfigurieren der Overlay Transport Virtualization mit ASR 1000

Inhalt

Einleitung

In diesem Dokument werden die Overlay Transport Virtualization (OTV)-Netzwerktopologien beschrieben, die von den Routern der Serien ASR 1000 und Catalyst 8300/8500 unterstützt werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASR1000, IOS® XE Version 16.10.1a und höher
- Catalyst 8300, IOS® XE Version 17.5.1a und höher
- Catalyst 8500, IOS® XE Version 17.6.1a und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

ASR1000 unterstützt OTV seit Cisco IOS® XE Release 3.5. Der Catalyst Router der Serie 8300 unterstützt IOS® XE17.5.1a und die Routen der Serie Catalyst 8500 die IOS® XE Version 17.6.1a.

OTV bietet Layer-2-Verbindungen zwischen Remote-Netzwerkstandorten durch MAC-Adressen-basiertes Routing und IP-gekapselte Weiterleitung (MAC-in-IP) über ein Transportnetzwerk, um Anwendungen zu unterstützen, die Layer-2-Nachbarschaft erfordern, wie z. B. Cluster und Virtualisierung. OTV verwendet ein Overlay Control Plane Protocol, um MAC-Routing-Informationen zu erfassen und an das Overlay-Netzwerk weiterzugeben. Das OTV-Steuerungsprotokoll verwendet IS-IS-Nachrichten (Intermediate-System-to-Intermediate-System), um Adjacencies für Remote-Standorte zu erstellen und MAC-Routen-Updates an Remote-Standorte zu senden. OTV erstellt Layer-2-Nachbarschaften zu Remote-Standorten im Overlay-Netzwerk durch automatische Erkennung von Remote-OTV-Geräten.

OTV für Layer-2-Erweiterung bietet u. a. folgende Vorteile:

- Kein MPLS erforderlich
- Keine komplexe Ethernet over Multiprotocol Label Switching (EoMPLS)-Konfiguration für Mesh
- Keine komplexe VPLS-Bereitstellung (Virtual Private LAN Services) für Layer-2-Erweiterungen
- Native Spanning-Tree-Isolierung
    - BPDU-Filter (Bridge Data Protocol Unit) müssen nicht explizit konfiguriert werden.
    - Standard-Isolierung von Spanning-Tree-Problemen in einem bestimmten Rechenzentrum
- Native unbekannte Unicast-Flutungsisolierung
    - Unbekannte Unicast-MAC-Pakete werden nicht weitergeleitet
    - Unterstützung für unbekannte Unicast-Weiterleitung pro MAC zulässig
- Optimierung des Address Resolution Protocol (ARP) durch OTV-ARP-Caching
    - reduziert unnötigen WAN-Datenverkehr
- Vereinfachte Bereitstellung der First Hop Redundancy Protocol (FHRP)-Isolierung
- Vereinfachtes Hinzufügen von Standorten
- Vereinfachte Redundanzkonfiguration

- Möglichkeit der "Dropdown"-Liste für Migrationen, wenn temporäre Services erforderlich sind

Anforderungen

Die nachfolgenden Elemente stellen die wichtigsten Regeln dar, die bei der Entwicklung einer OTV-Bereitstellung zu beachten sind. Wenn diese Regeln eingehalten werden, werden Design und Bereitstellung optimiert.

- Für die Übertragung des gekapselten OTV-Datenverkehrs (die so genannte Join-Schnittstelle) für alle konfigurierten OTV-Overlay-Schnittstellen kann nur eine einzige Schnittstelle verwendet werden.
- Es kann nur eine Schnittstelle verwendet werden, um die L2-Serviceinstanzen des Rechenzentrums für das VLAN des OTV-Standorts und die zwischen den Rechenzentren erweiterten VLANs für alle konfigurierten OTV-Overlay-Schnittstellen zu konfigurieren.
- Port-Channels können für die Schnittstellenredundanz und die Verbindung mit VSS- oder VPC-Switches verwendet werden und werden als "One and Only One"-Schnittstelle für die Verbindung unterstützt.
- Alle OTV-Router müssen über die Join-Schnittstelle kontaktierbar sein.
- Spanning Tree muss auf dem OTV-Router konfiguriert werden, der auf das Rechenzentrum verweist.
- IGMP-Snooping und -Abfrage müssen für die korrekte Weiterleitung von Multicast-Datenverkehr im Rechenzentrum konfiguriert sein.
- Ein Rechenzentrum kann mit einem oder zwei OTV-Routern konfiguriert werden. Mit zwei Routern wird die VLAN-Weiterleitung auf ungerade/gerade Weise basierend auf der VLAN-Nummer verteilt. Jeder OTV-Router in einem Rechenzentrum fungiert als Backup für den jeweils anderen.
- Multihomed-Paare müssen mit derselben OTV-Standortkennung konfiguriert werden.
- ASR1000/Catalyst 8300/Catalyst 8500 und Nexus 7000 können demselben OTV-Netzwerk angehören
    - Der Nexus 7000 unterstützt keine OTV-Fragmentierung oder -Verschlüsselung, daher können diese Funktionen in einer "hybriden" Bereitstellung nicht verwendet werden.

Es gibt bestimmte Designs für Back-to-Back-Verbindungen, die unterstützt werden und nicht den angegebenen Regeln entsprechen. Diese Konfigurationen werden zwar unterstützt, aber nicht empfohlen. Einzelheiten hierzu finden Sie im späteren Abschnitt "Spezialfall-Unicast-Topologie".

Es kann nicht genug betont werden, dass die aktuelle OTV-Software bei der Konfiguration der Join- und L2-Zugangsschnittstellen für OTV die "One and Only One"-Schnittstelleneinschränkung aufweist. Eine Port-Channel-Schnittstelle kann zur Redundanz verwendet werden. Die Verbindung des Port-Channels mit dem Nexus 7000 in einer vPC wird unterstützt. Eine einfache Port-Channel-Verbindung zu einem einzelnen Switch wird ebenfalls unterstützt.

OTV-Implementierungstypen

OTV erfordert eine einzelne Join-Schnittstelle und eine einzelne L2-Schnittstelle. Pro OTV-Router kann jeweils nur einer unterstützt werden. Für OTV muss außerdem ein Standort-VLAN

konfiguriert werden, damit die Multihomed-OTV-Router über das lokale Netzwerk miteinander kommunizieren können. Auch bei Single-Homed-OTV-Routern muss das OTV-Standort-VLAN konfiguriert sein. Darüber hinaus muss für jeden Standort bzw. jedes Rechenzentrum eine eindeutige Standort-ID konfiguriert sein. Dual-Homed OTV-Router müssen die gleiche Standort-ID verwenden und über dasselbe VLAN kommunizieren können.

Die nachfolgende Konfiguration enthält die grundlegende, für OTV erforderliche Konfiguration. Sie ist jedoch nicht vollständig, da die Unicast- oder Multicast-Core-Konfiguration hinzugefügt werden muss. Diese werden in den folgenden Abschnitten dieses Dokuments näher erläutert.

```
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
```

Die Serviceinstanzkonfiguration wird für alle L2-Schnittstellenkonfigurationen mit OTV verwendet.

Jede Serviceinstanz auf der L2-Schnittstelle muss einer bestimmten Kapselung mit einem oder zwei Tags zugeordnet werden.

Jede dieser Serviceinstanzen muss wiederum einer Bridge-Domäne zugeordnet werden.

Diese Bridge-Domäne wird für eine Serviceinstanz verwendet, die auf der Overlay-Schnittstelle konfiguriert ist.

Die Bridge-Domäne ist die Verbindung, die die Overlay-Service-Instanz mit der L2-Schnittstellenservice-Instanz verbindet.

Die Kapselung des Datenverkehrs auf der Overlay-Schnittstelle muss mit der Kapselung des Datenverkehrs nach dem erneuten Schreiben auf die L2-Schnittstelle übereinstimmen.

Im Beispiel hat der Datenverkehr, der in der Gig1/0/1-Serviceinstanz 99 eingeht, ein einzelnes 802.1Q-VLAN von 99 und eine Bridge-Domäne 99. Die entsprechende Serviceinstanz mit der Bridge-Domäne 99 auf der Overlay-Schnittstelle ist ebenfalls für ein einzelnes 802.1Q-VLAN von 99 konfiguriert. Dieser Fall ist der einfachste.

Im Beispiel hat der Datenverkehr, der in der Gig1/0/1-Serviceinstanz 98 eingeht, ein doppeltes 802.1Q-VLAN von 99 und 1098 sowie eine Bridge-Domäne 90. Die entsprechende Serviceinstanz mit Bridge-Domäne 90 auf der Overlay-Schnittstelle ist für ein einzelnes 802.1Q-VLAN von 90 konfiguriert. Diese sind eindeutig nicht identisch. Der Befehl rewrite ingress stellt sicher, dass die Tags korrekt übersetzt werden, wenn der Datenverkehr die Eingangsschnittstelle durchläuft. Der Datenverkehr, der die L2-Schnittstelle erreicht, wird durch die 98/1098 802.1Q-VLANs ersetzt, die durch ein einzelnes VLAN von 90 ersetzt werden. Das symmetrische Schlüsselwort stellt sicher, dass der Datenverkehr, der die L2-Schnittstelle verlässt, durch ein einzelnes 802.1Q-VLAN von 90 ersetzt wird.

Alle Serviceinstanzen mit mehreren durch OTV erweiterten 802.1Q-VLANs müssen den Befehl "rewrite ingress" verwenden. Die OTV-Kapselung unterstützt nur eine einzelne VLAN-Kennung. Aus diesem Grund muss jede doppelte VLAN-Konfiguration auf den L2-Schnittstellen auf ein einzelnes Tag in der Overlay Interface Service Instance neu geschrieben werden. Dadurch wird die Unterstützung mehrdeutiger VLAN-Konfigurationen ausgeschlossen.

Weitere Informationen zum Umschreiben von Tags finden Sie in diesem Dokument: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

In diesem Beispiel lautet die Bridge-Domäne des OTV-Standorts 100.

- Die Bridge-Domäne des OTV-Standorts wird nur auf der L2-Schnittstelle konfiguriert.
- Die Bridge-Domäne des OTV-Standorts darf niemals auf der Overlay-Schnittstelle konfiguriert werden, da die OTV-Bereitstellung dadurch instabil wird.
- Das VLAN des OTV-Standorts darf nur mit den OTV-Routern verbunden sein und keinen anderen Datenverkehr von Rechenzentren/Benutzern übertragen.
- Das VLAN des OTV-Standorts muss sich an derselben physischen Schnittstelle wie die erweiterten OTV-VLANs befinden.

Multihome

Ein Rechenzentrum kann aus Redundanzgründen mit einem einzelnen OTV-Host oder mit bis zu zwei Servern verbunden werden (auch bekannt als Multihome). Multihome wird für Ausfallsicherheit und Lastenausgleich verwendet. Wenn mehr als ein Edge-Gerät an einem Standort vorhanden ist und beide Teil desselben Overlay-Netzwerks sind, gilt der Standort als Multihomed. OTV Multihome teilt die VLANs basierend auf der VLAN-Nummer ungerade/gerade auf die beiden OTV-Router, die zum gleichen Standort gehören. Ein Edge-Gerät wird als AED für alle ungeraden VLANs ausgewählt, während der andere OTV-Router als AED für alle geraden VLANs ausgewählt wird. Jede AED ist auch ein Standby-VLAN für die VLANs, die auf dem anderen Router aktiv sind. Bei einem Verbindungs- oder Knotenausfall in einem der AEDs wird

das Standby-AED für alle VLANs aktiviert.

Wenn zwei ASR1000 im selben Rechenzentrum für Multihome verbunden sind, ist keine dedizierte Verbindung zwischen den beiden ASR1000 erforderlich. OTV verwendet das VLAN des OTV-Standorts, das über die interne Schnittstelle und die Kommunikation über die Join-Schnittstelle übertragen wird, um zu bestimmen, welche Router für gerade und ungerade VLANs zuständig sind.

ASR1000s und Nexus 7000s können nicht im gleichen Rechenzentrum mit OTV gemischt werden, das auf beiden Routern als Backup für den jeweils anderen Router konfiguriert ist. Multihoming wird in einem bestimmten Rechenzentrum für übereinstimmende Plattformen (ASR1000 oder Nexus 7000) unterstützt. Sie können ASR1000 in einem Rechenzentrum und Nexus 7000 in einem anderen Rechenzentrum verwenden. Die Interoperabilität zwischen diesen beiden Plattformen wurde getestet und unterstützt. Manche Rechenzentren können mehrere Standorte gleichzeitig haben, während andere über ein Single-Homed-Netz verfügen.

Auf Multihomed ASR1000-Routerpaaren muss dieselbe Version der Cisco IOS® XE Software ausgeführt werden.

Bei Verwendung von Multihome sollte Spanning-Tree auf den OTV-Routern aktiviert werden, da der OTV-Router auf diese Weise eine Benachrichtigung über eine Topologieänderung (TCN) senden kann, wodurch das benachbarte L2-Switch-Gerät (zusammen mit anderen Switches im Spanning-Tree) seinen Alter-Timer von der Standardeinstellung auf 15 Sekunden verringert. Dadurch wird die Geschwindigkeitskonvergenz bei einem Ausfall oder einer Wiederherstellung zwischen dem Multihomed-Paar erheblich erhöht. Spanning-Tree kann für alle konfigurierten Service-Instanzen (mit OTV oder auf andere Weise verbunden) aktiviert werden, indem die entsprechende Leitung zur globalen Konfiguration hinzugefügt wird.

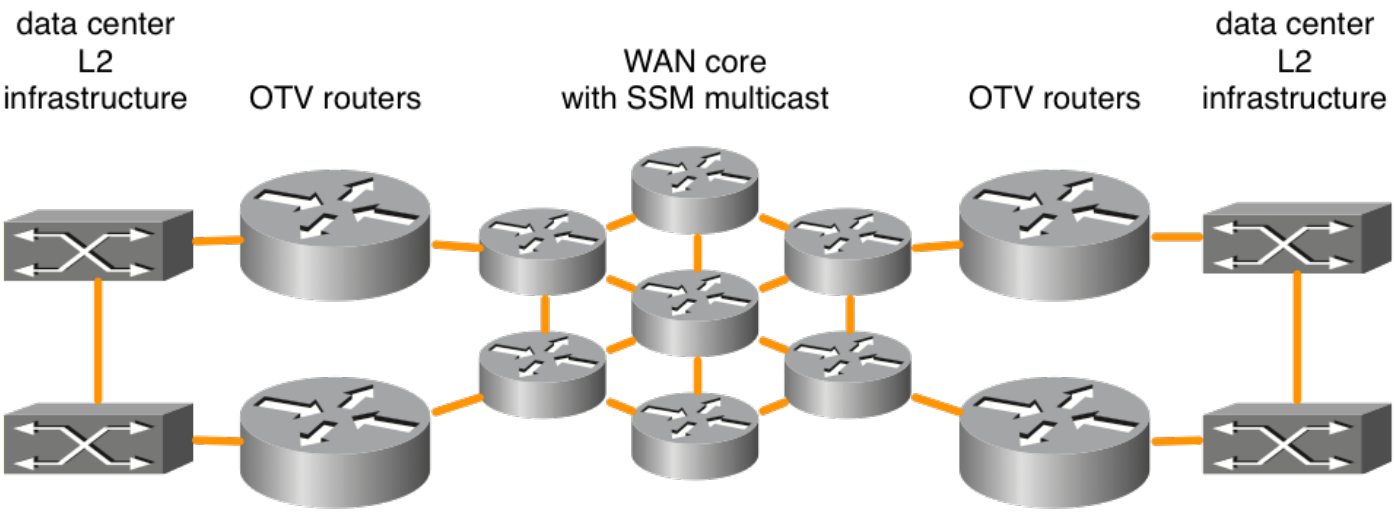
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

Es ist keine Konfiguration pro VLAN oder pro Serviceinstanz erforderlich.

Multicast

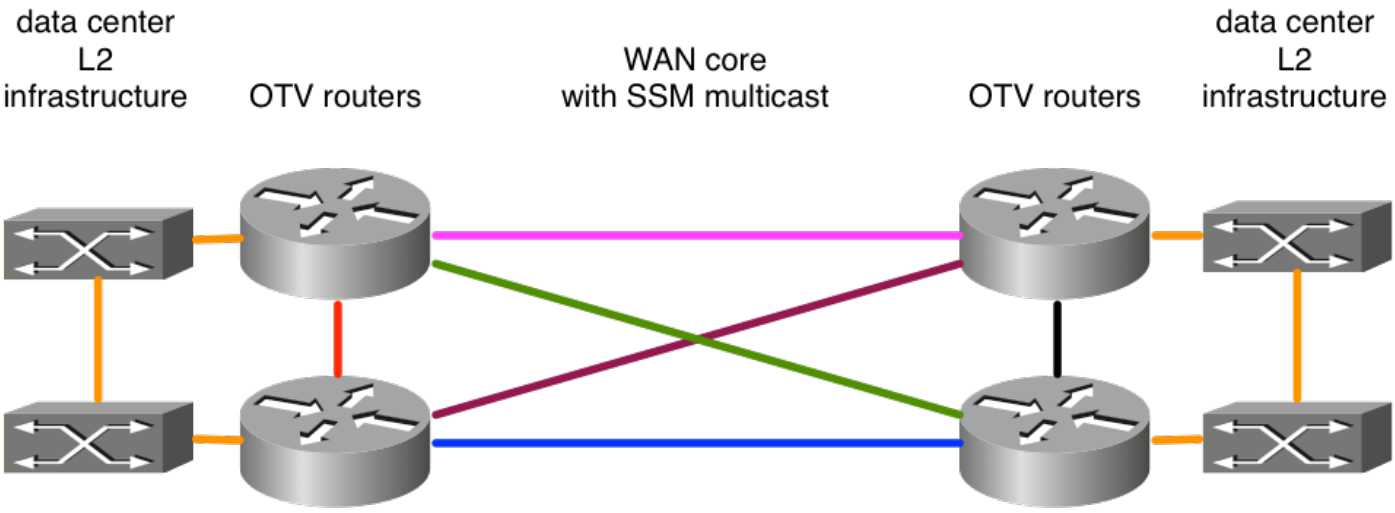
Für ein Multicast-Netzwerk ist eine Full-Mesh-Konnektivität über das WAN erforderlich. Alle OTV-Router müssen über die Join-Schnittstelle miteinander verbunden werden.

Abbildung 1. Unterstützte Multicast-Netzwerktopologie



Diese Abbildung zeigt ein Beispiel für zwei Rechenzentren, die über einen vollständig vernetzten Core verbunden sind. Source Specific Multicast (SSM) Protocol Independent Multicast (PIM) wird zwischen den OTV-Routern und den WAN-Core-Routern ausgeführt. Es wird eine beliebige Anzahl von Core-Routern unterstützt, solange eine Full-Mesh-Verbindung besteht. Es besteht keine explizite Anforderung für die maximale Latenz für OTV-Verbindungen über den WAN-Core.

Abbildung 2. Nicht unterstützte Multicast-Netzwerktopologie



Da ASR1000/OTV erwartet, dass Multicast-Nachrichten von allen Peers auf einer einzelnen Join-Schnittstelle empfangen werden, würde dies beispielsweise zu einer instabilen OTV-Bereitstellung führen. Angenommen, die Ost-West-Verbindungen in Pink und Blau wurden als Join-Schnittstellen konfiguriert. Wenn die pinkfarbene Verbindung ausfällt, kann der Router keine OTV-Updates mehr für diese Schnittstelle empfangen. Ein alternativer Pfad über die grünen oder lila Links wäre inakzeptabel, da die Join-Schnittstelle explizit konfiguriert ist. Auf dieser Schnittstelle müssen Updates empfangen werden. Derzeit wird die Verwendung einer Loopback-Schnittstelle als Join-Schnittstelle nicht unterstützt.

Wenn Benutzer ihren Backbone nicht besitzen, müssen sie sicherstellen, dass ihr Service Provider Multicast in ihrem Core unterstützt, und der Service Provider kann auf IGMP-Abfragenachrichten (Internet Group Management Protocol) antworten. OTV auf dem ASR1000 fungiert als Multicast-Host (leitet IGMP-Join-Nachrichten weiter) und nicht als Multicast-Router in

der Multicast-Topologie des WAN.

Das Transportnetzwerk zwischen den OTV-Routern muss den PIM Sparse Mode (Any Source Multicast [ASM]) für die Provider Multicast Group und SSM für die Delivery Group unterstützen.

Multicast-Kerne erfordern eine bestimmte Konfiguration auf der Overlay-Schnittstelle für eine Kontrollgruppe sowie eine Reihe von Daten-Multicast-Gruppen, die für die Weiterleitung von Daten verwendet werden.

```
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
```

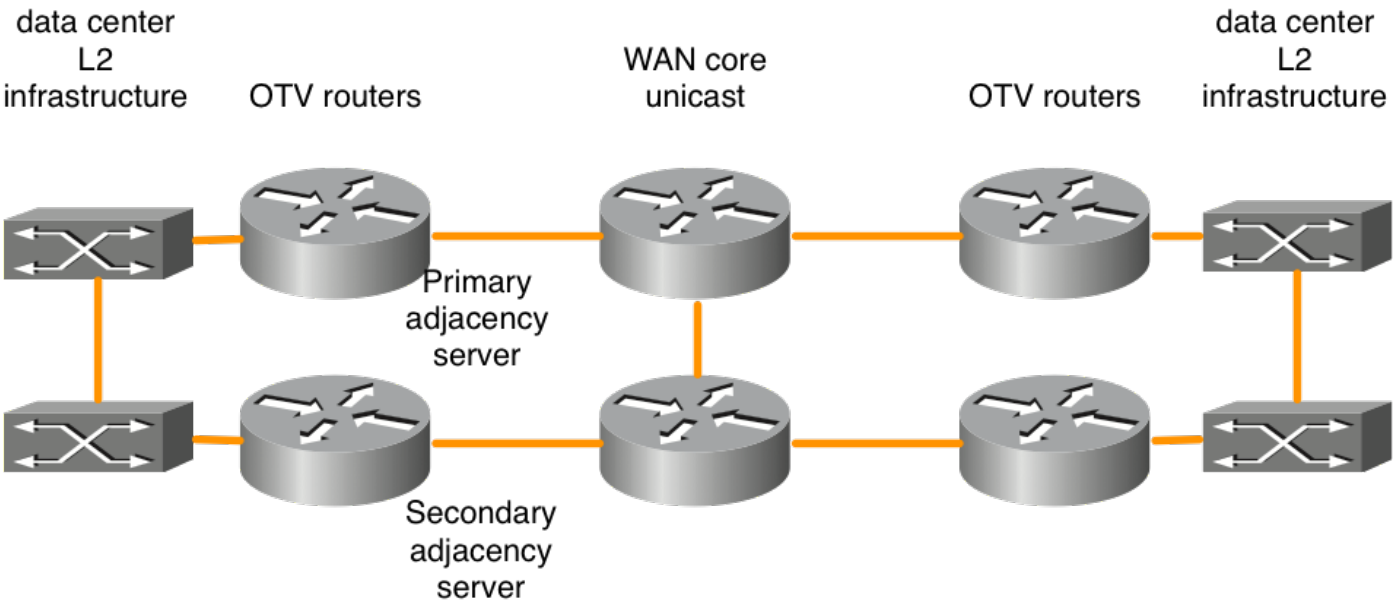
Für Multicast-OTV-Bereitstellungen muss die Join-Schnittstelle als passive PIM-Schnittstelle konfiguriert werden. IGMP kann je nach Bedarf für verschiedene Versionen konfiguriert werden. Für die Overlay-Schnittstelle muss eine Steuergruppe und eine Datengruppe konfiguriert sein. Die Kontrollgruppe ist eine einzelne Multicast-Gruppe, die für die OTV-Verwaltung verwendet wird. Bei der Datengruppe handelt es sich um einen Bereich von Multicast-Adressen, die zum Transport von Benutzerdaten zwischen Rechenzentren verwendet werden. Wenn sich die Datengruppe nicht im IP-Bereich 232.0.0.0/8 befindet, muss der zusätzliche Befehl "ip pim ssm range" konfiguriert werden, um den für OTV erforderlichen Bereich einzuschließen.

Das Transportnetzwerk zwischen den OTV-Routern muss den PIM Sparse Mode (Any Source Multicast [ASM]) für die Provider Multicast Group und Source Specific Multicast (SSM) für die Delivery Group unterstützen.

Unicast-Core mit Adjacency-Servern

Cisco IOS® XE 3.9 bietet zusätzliche Unterstützung für OTV mit einem Unicast-Core. Sowohl Unicast- als auch Multicast-Cores für OTV werden weiterhin für alle ASR 1000-Plattformen und künftige Versionen von Cisco IOS® XE 3.9 unterstützt.

Abbildung 3: Unicast-Netzwerktopologie



Die Funktion "OTV Adjacency Server" ermöglicht den reinen Unicast-Transport zwischen dem OTV-Edge. OTV-Router, die mit der Adjacency-Server-Rolle konfiguriert wurden, führen eine Liste aller bekannten OTV-Router. Sie stellen diese Liste allen registrierten OTV-Routern zur Verfügung, sodass diese über eine Liste von Geräten verfügen, die replizierten Broadcast- und Multicast-Datenverkehr empfangen müssen.

Die OTV-Kontrollebene über einen reinen Unicast-Transport funktioniert genau wie OTV mit Multicast Core, abgesehen davon, dass in einem Unicast-Core-Netzwerk jedes OTV-Edge-Gerät mehrere Kopien jedes Kontrollebenen-Pakets erstellen und diese an jedes Remote-Edge-Gerät im selben logischen Overlay senden muss.

In der gleichen Denkweise wird jeglicher Multicast-Verkehr vom Rechenzentrum auf dem lokalen OTV-Router repliziert, und es werden mehrere Kopien an jedes der Remote-Rechenzentren gesendet. Dies ist zwar weniger effizient als eine Abhängigkeit vom WAN-Core für die Replikation, die Konfiguration und das Management des Multicast-Core-Netzwerks sind jedoch nicht erforderlich. Wenn nur wenig Multicast-Datenverkehr über Rechenzentren übertragen wird oder nur wenige Rechenzentrumsstandorte (maximal vier) vorhanden sind, ist ein Unicast-Core für die OTV-Weiterleitung in der Regel die beste Wahl. Insgesamt wird die Option für die Unicast-Core-Bereitstellung durch die Vereinfachung der Betriebsabläufe des reinen Unicast-Modells in Szenarien bevorzugt, in denen eine LAN-Anschlussverbindung nur zwischen vier oder weniger Rechenzentren erforderlich ist. Es wird empfohlen, mindestens zwei Adjacency-Server zu konfigurieren, einen primären und einen Backup. Es gibt keine Option für die Konfiguration des Aktiv/Aktiv-Adjacency-Servers.

OTV-Router müssen entsprechend konfiguriert werden, um den entsprechenden Adjacency Server korrekt zu identifizieren und zu registrieren.

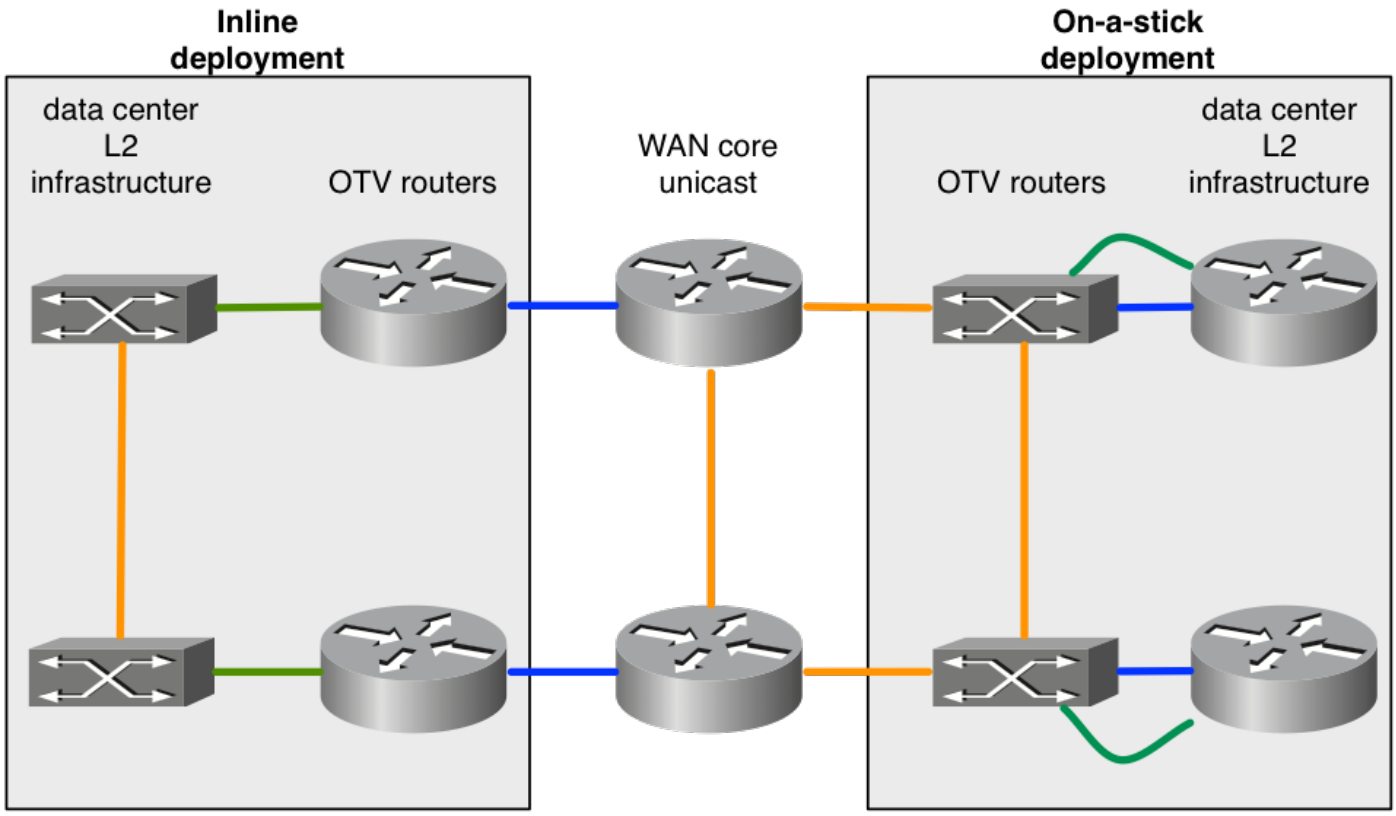
	Primärer Adjacency Server	Sekundärer Adjacency-Server	Andere OTV-Router
IP-Adresse der OTV-Join-Schnittstelle	10.0.0.1	10.2.2.24	andere IP-Adressen
Konfiguration	interface Overlay 1 otv adjacency-server nur unicast	interface Overlay 1 otv adjacency-server nur unicast otv use-adjacency-server 10.0.0.1 Nur Unicast	interface Overlay 1 otv use-adjacency-server 10.0.0.1 10.2.2.24 nur Unicast

Es gibt bestimmte Designs für Back-to-Back-Verbindungen, die von der Unicast-OTV-Weiterleitung unterstützt werden und nicht den Regeln der "Full Mesh" entsprechen. Diese Konfigurationen werden zwar unterstützt, aber nicht empfohlen. Diese Bereitstellungsart ist am häufigsten, wenn Rechenzentren über Dark Fiber verbunden sind. Einzelheiten zu dieser Konfigurationsoption finden Sie im späteren Abschnitt "Unicast-Topologie für Sonderfälle".

OTV auf einem Stick oder Inline

Es gibt zwei Modelle für die Bereitstellung von OTV in Ihrem Rechenzentrum: auf einem Stick und Inline. In den zuvor vorgestellten Designszenarien waren OTV-Router inline zwischen dem Rechenzentrum und dem Core-Netzwerk des Service Providers angeordnet. Wünschenswerter ist jedoch, dass der OTV-Router als Appliance hinzugefügt wird, sodass er sich nicht im Transportpfad des gesamten Datenverkehrs befindet. Manchmal besteht die Anforderung darin, die aktuelle Topologie nicht zu ändern, um über die aktuelle Ausrüstung eine Verbindung zum Service Provider herzustellen (z. B. eine bestehende Bereitstellung mit Catalyst 6000-Switch oder Nexus-Switch-Hardware, die OTV nicht unterstützt). Daher ist es bevorzugt, OTV auf dem ASR1000 als auf einem Stick als OTV-Gerät bereitzustellen.

Abbildung 4: Inline- und On-a-Stick-Topologie



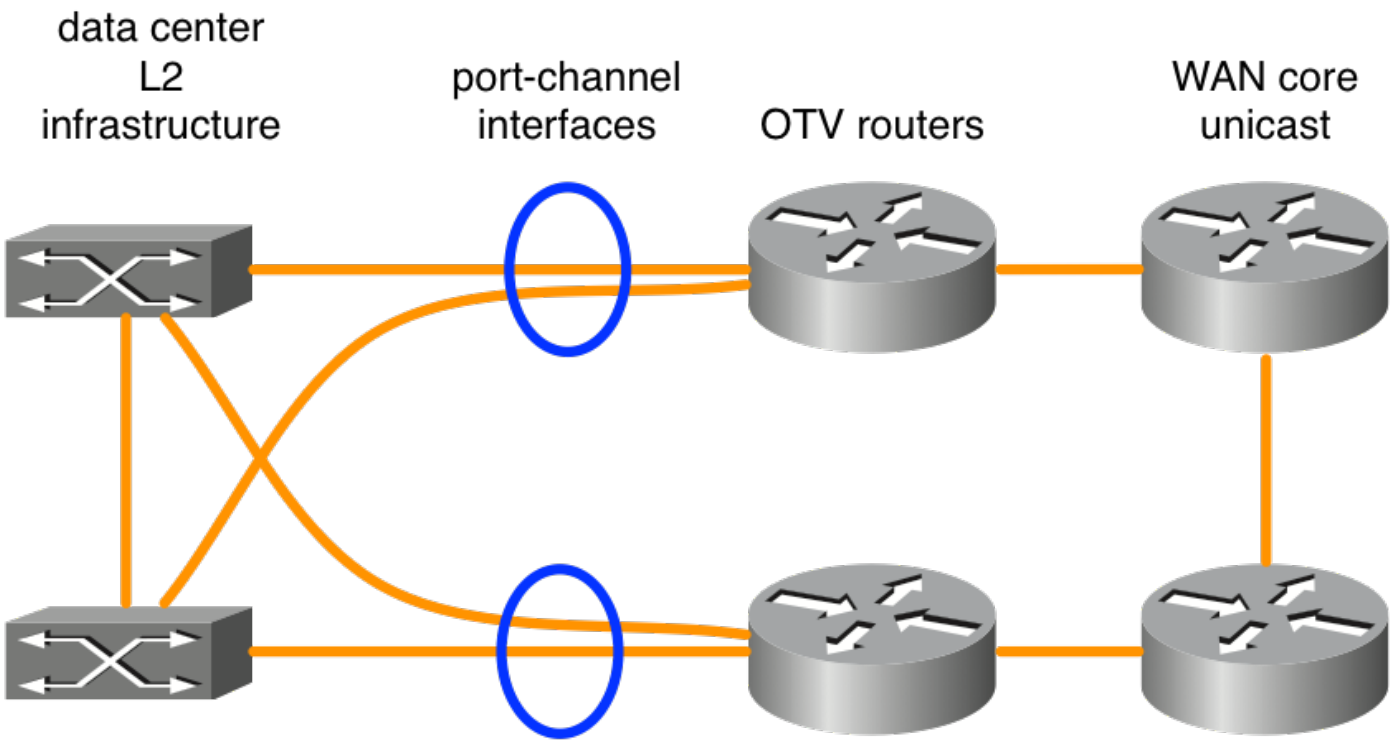
Das Diagramm zeigt die beiden Bereitstellungsmodelle, die Teil desselben Overlays sein können. Die grünen Verbindungen, die mit den OTV-Routern verbunden sind, werden als L2-Zugriffsschnittstellen konfiguriert, um VLAN-Datenverkehr zu akzeptieren. Die blauen Verbindungen, die mit den OTV-Routern verbunden sind, sind die Join-Schnittstellen, die OTV-gekapselten VLAN-Datenverkehr übertragen.

Möglicherweise müssen Sie eine Funktion konfigurieren, die von OTV nicht unterstützt wird. Beispielsweise können OTV und MPLS nicht auf demselben Gerät konfiguriert werden. Daher kann es sinnvoll sein, ASR1000/OTV auf einem Stick zu verwenden und MPLS auf dem Router zu konfigurieren, der sich vor dem OTV-Router befindet.

Port-Channels für Layer 2 und Layer 3

Der Cisco IOS® XE 3.10-Code für ASR1000 unterstützt nun die Port-Channel-Konfiguration von Layer 2 und Layer 3 mit OTV. Layer-2-Port-Channel können als interne Schnittstelle verwendet werden. Der Port-Channel muss aus bis zu 4 physischen Schnittstellen bestehen. Layer-3-Port-Channel kann als Join-Schnittstelle verwendet werden.

Abbildung 5: Für L2-Verbindungen verwendete Port-Kanäle



Das Diagramm zeigt ein typisches Port-Channel-Szenario mit zwei Switches in VSS (Catalyst Serie 6000) oder VPC (Nexus Serie 7000). Dieses Design bietet mit zwei OTV-Routern und dualen Verbindungen zur Rechenzentrumsinfrastruktur Redundanz. Für OTV ist abgesehen von der Port-Channel-Basiskonfiguration keine andere spezielle Konfiguration erforderlich, wenn VSS oder ein VPC auf L2-Switching-Geräten neben den OTV-Routern verwendet wird.

Standardgateway

OTV erstellt dasselbe L3-Subnetz an mehreren Standorten. Dies erfordert einige besondere Überlegungen beim Routing von L3-Datenverkehr zu und von den erweiterten VLANs. L3-Routing kann auf den OTV-Routern selbst oder auf anderen Geräten konfiguriert werden, die mit den erweiterten VLANs verbunden sind. Darüber hinaus können in jedem Szenario First Hop Redundancy Protocols (FHRP) wie Hot Standby Redundancy Protocol (HSRP) oder Virtual Router Redundancy Protocol (VRRP) zur Redundanz bereitgestellt werden. HSRP kann lokal in einem bestimmten Rechenzentrum ausgeführt werden oder sich zwischen Rechenzentren erstrecken (nicht typisch).

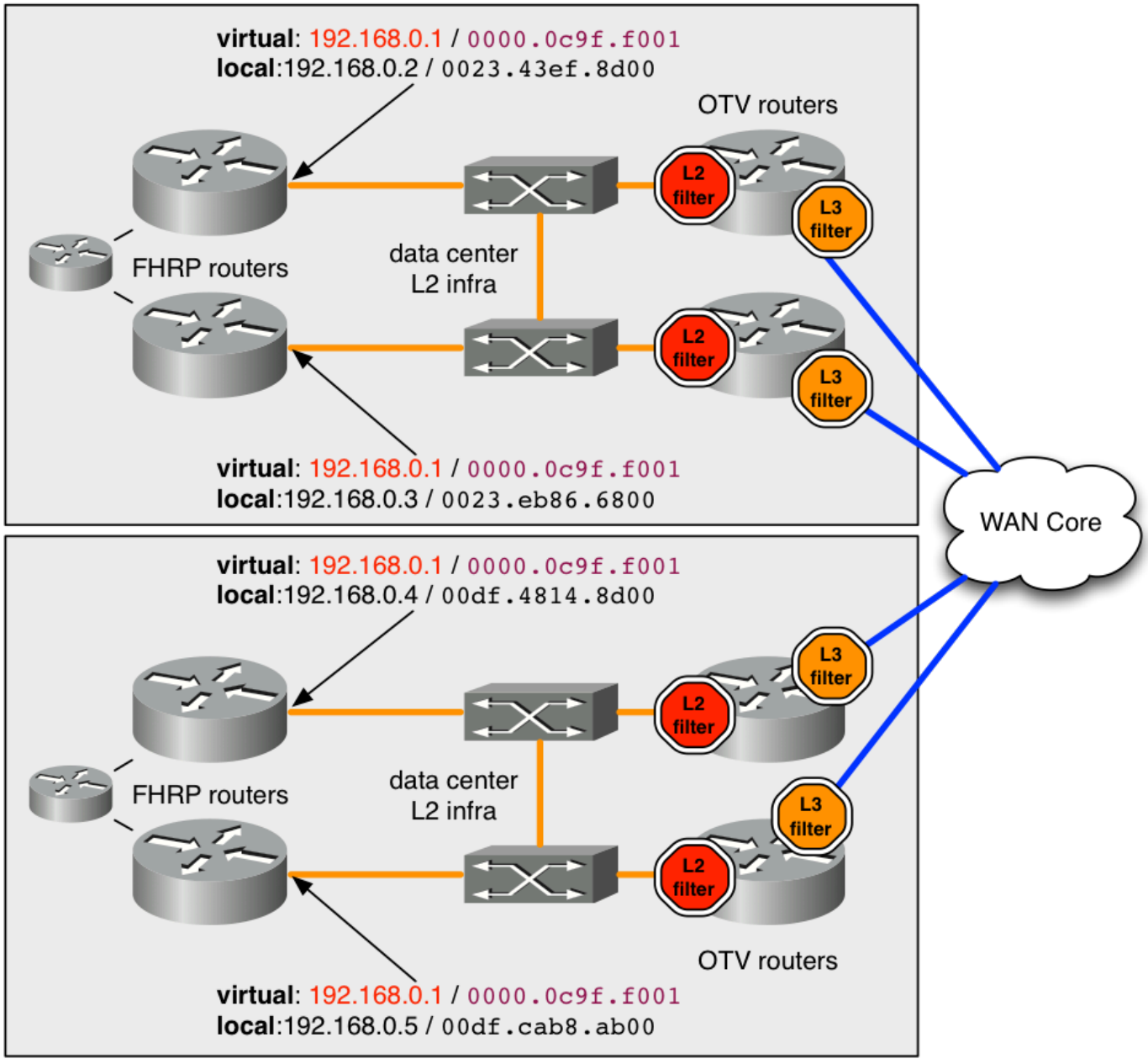
Die Best Practice für OTV-Bereitstellungen, die FHRP verwenden, besteht darin, lokale Instanzen des FHRP in jedem Rechenzentrum ausführen zu lassen. Diese FHRP-Instanzen verwenden dieselbe virtuelle MAC- und IP-Adresse, sodass virtuelle Systeme, die zwischen Rechenzentren verschoben werden, über eine ununterbrochene Verbindung verfügen. Wenn sich die MAC-Adresse des Standardrouters zwischen den Rechenzentren ändern würde, könnten die virtuellen Systeme nicht außerhalb des Subnetzes kommunizieren, bis das Zeitlimit für den ARP-Eintrag des Standardgateways des virtuellen Systems überschritten wurde.

Um ein FHRP mit OTV richtig bereitzustellen, muss berücksichtigt werden, welcher L2- und L3-Datenverkehr gefiltert und von OTV isoliert werden muss. Auf L2-Ebene ist dies erforderlich, um zu verhindern, dass OTV dieselbe virtuelle L2-MAC sieht, die vom FHRP an mehreren Standorten

verwendet wird. Auf L3-Ebene sind Filter erforderlich, um HSRP- und VRRP-Werbung für jedes Rechenzentrum zu isolieren, sodass die Auswahl für Aktiv/Überwachend/Standby für jedes Rechenzentrum lokalisiert wird.

Standardmäßig sind die FHRP-Filter aktiviert, wenn OTV aktiviert ist. Sie kann deaktiviert werden, wenn das Design eine Erweiterung von FHRP zwischen Rechenzentren erfordert. Die L2-Filterung virtueller MAC-Adressen ist NICHT standardmäßig aktiviert und muss manuell konfiguriert werden.

abbildung 6: Beispiel für die empfohlene Bereitstellung für FHRP



Im Beispiel wird die virtuelle MAC-Adresse 0000.0c9f.f001 für die IP-Adresse 192.168.0.1 verwendet, die auf dem erweiterten VLAN für die Verbindung mit dem Subnetz gehostet wird. Wenn in beiden Rechenzentren dieselbe virtuelle MAC- und IP-Adresse verwendet wird, kann ein Host beim Transfer zwischen Rechenzentren nahtlos mit dem Subnetz verbunden werden.

Um die MAC-Adresse 0000.0c9f.f001 für OTV an mehreren Standorten verborgen zu halten, muss

für das VLAN auf jedem der OTV-Router, die das VLAN bedienen, ein L2-Eingangsfilter (roter Stopp im Diagramm) bereitgestellt werden. Durch den ACL-Filter wird die auf den L2-Dienstinstanzen konfigurierte Filter-ACL für den Eingang verwendet. Alle von dieser MAC bezogenen Pakete werden die entfernt wurden, bevor sie für den OTV-Prozess auf dem ASR1000 sichtbar sind. Daher erfährt OTV nie etwas über die MAC und kündigt sie auch nicht an entfernten Rechenzentren an.

Die empfohlene Konfiguration zum Abfangen des gesamten bekannten/standardmäßigen virtuellen FHRP-MAC-Verkehrs ist hier angegeben.

```
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
```

Diese ACL stimmt mit den bekannten MAC-Adressräumen überein, die HSRP-Versionen 1 und 2, Gateway Load Balancing Protocol (GLBP) und VRRP (in dieser Reihenfolge) zugeordnet sind. Wenn die virtuelle MAC-Adresse so konfiguriert ist, dass sie einen nicht standardmäßigen Wert verwendet, der nicht auf der FHRP-Gruppennummer basiert, muss sie dem ACL-Beispiel explizit hinzugefügt werden. Die ACL muss der L2-Service-Instanz hinzugefügt werden (hier abgebildet).

```
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
```

Außerdem muss die Kommunikation zwischen den FHRP-Hosts auf L3-Ebene verwaltet werden. In diesem Diagramm sind vier FHRP-Router in einem erweiterten Subnetz konfiguriert. Ohne einen gewissen Grad an L3-Filtern würden sich alle vier Router sehen und ein aktives Gerät auswählen, und hätten drei in verschiedenen Standby-Zuständen. Ein Rechenzentrum verfügt also über zwei lokale Standby-FHRP-Router, hat jedoch aufgrund der zuvor besprochenen L2-Filter keine L2-Verbindung mit dem aktiven Remote-Router.

Das angestrebte Ergebnis ist ein aktiver und ein Standby-FHRP-Router in jedem Rechenzentrum. Der zuvor erläuterte Eingangs-L2-Filter erfasst diesen Datenverkehr nicht, da bei der Auswahl die tatsächliche IP- und MAC-Adresse des Routers verwendet wird. Standardmäßig wird die nachfolgende ACL als Egress auf die Overlay-Schnittstelle angewendet. Der Ausgang für die Overlay-Schnittstelle ist der Datenverkehr zum WAN-Core. Die ACL wird in der aktuellen

Konfiguration nicht angezeigt, kann jedoch mit "show ip access-list" beobachtet werden. Es filtert den FHRP-Auswahldatenverkehr basierend auf der UDP-Portnummer.

```
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
```

Dieser Filter sollte nur deaktiviert werden, wenn alle FHRP-Router in einem VLAN an derselben Auswahl für den aktiven Status teilnehmen sollen. Um diesen Filter zu deaktivieren, konfigurieren Sie "no otv filter-fhrp" auf der Overlay-Schnittstelle.

Unbekannter Unicast-Datenverkehr

Standardmäßig wird Unicast-Datenverkehr, der vom OTV-Router vom LAN empfangen wird und für eine MAC-Adresse bestimmt ist, die an einem entfernten OTV-Standort unbekannt ist, verworfen. Dieser Datenverkehr wird als unbekannter Unicast bezeichnet. Diese Drop-Aktion wird auf den WAN-Core angewendet, der die vom Broadcast-Datenverkehr im WAN verbrauchte Bandbreite begrenzt. Die allgemeine Erwartung ist, dass alle Hosts im LAN ausreichend Broadcast-Datenverkehr (ARPs, Protokoll-Broadcasts usw.) ausgeben, der immer von einem OTV-Router zu sehen ist, gemeldet wird und somit "bekannt" ist.

Bestimmte Anwendungen nutzen Silent Hosts. Bei einer normalen Switching-Infrastruktur ist dies kein Problem, da L2-Broadcasting von unbekannten Unicast-MAC-Adressen im LAN dem unbeaufsichtigten Host ermöglicht, den Datenverkehr zu sehen. In einer OTV-Umgebung blockiert der OTV-Router jedoch den Datenverkehr zwischen den Rechenzentren.

Um dies zu kompensieren, wurde eine Funktion namens Selective Unicast Forwarding in Cisco IOS® XE integriert. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 und alle Versionen nach haben Unterstützung für selektive Unicast-Weiterleitung.

Die Konfiguration erfolgt durch Hinzufügen eines einzelnen Befehls pro MAC-Adresse auf der Overlay-Schnittstelle. Beispiele:

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

In diesem Beispiel muss jeglicher Datenverkehr, der für 0000.0001.0001 bestimmt ist, an alle Remote-OTV-Router mit VLAN 100 geleitet werden. Dies kann durch den folgenden Befehl beobachtet werden:

<#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
```

Wenn diese MAC-Adresse an einem Remote-Standort abgerufen wird, muss der Weiterleitungstabelle ein Eintrag hinzugefügt werden, der Vorrang vor dem Flood-Eintrag hat.

<#root>

OTV_router_1#

show otv route

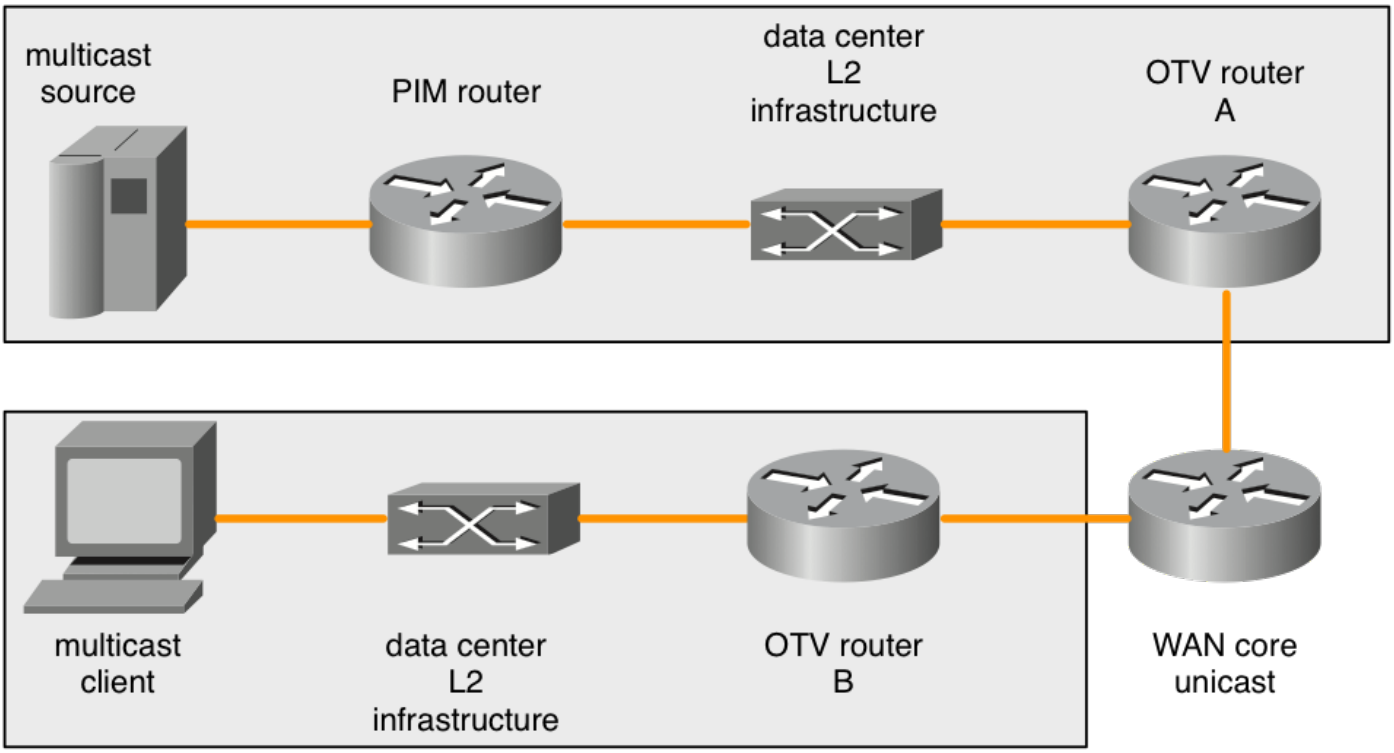
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-----------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood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

Im Allgemeinen muss ein Flooding-Eintrag für eine bestimmte MAC-Adresse auf allen OTV-Routern mit diesem VLAN konfiguriert werden.

Remote-Multicast-Quellen

Der ASR1000 leitet von einem OTV-Router keine Multicast-IGMP-Join-Anforderungen weiter, die vom LAN empfangen wurden. Das nachfolgende Diagramm zeigt die Topologie, in der dieses Problem auftreten kann.

Abbildung 7: Remote-Multicast-Quellen



Wenn ein Multicast-IGMP-Join vom Multicast-Client gesendet wird, wird dieser vom ASR1000 (OTV-Router B) überwacht und das Interesse an der Multicast-Gruppe angekündigt. Die Remote-OTV-Router (OTV-Router A) müssen den Datenverkehr an die Multicast-Gruppe weiterleiten, die in ihrer lokalen L2-Broadcast-Domäne angezeigt wird. Der Remote-ASR1000 (OTV-Router A) generiert die Multicast-IGMP-Join-Anforderungen jedoch nicht neu, wenn das Interesse an einer Multicast-Gruppe vom OTV-Router des Clients (OTV-Router B) angekündigt wird.

Wenn sich Multicast-Quellen in derselben L2-Broadcast-Domäne wie der OTV-Router befinden, ist dies kein Problem. Der OTV-Router muss als IGMP Querier konfiguriert werden. Dieser wird in jedem Multicast-Verkehr angezeigt, der in der L2-Broadcast-Domäne vorhanden ist. Allerdings würde nur eine PIM-Join-Anforderung einen PIM-Router dazu veranlassen, eine Multicast-Quelle von einer anderen L2-Broadcast-Domäne an die L2-Broadcast-Domäne weiterzuleiten, in der sich der OTV-Router befindet.

Die Remote-IGMP-Beitrittsanfrage wird nicht weitergeleitet oder neu generiert. Auch OTV-Router sind keine PIM-Router. Topologien mit Multicast-Quellen, die sich nicht direkt in der L2-Broadcast-Domäne mit dem OTV-Router befinden, können daher keine Informationen von PIM-Routern einholen, um Quelldatenverkehr weiterzuleiten, wenn ein entfernter Client Interesse daran hat.

Es gibt zwei Problemumgehungen.

Zunächst können lokale IGMP-Clients in der L2-Broadcast-Domäne bereitgestellt werden, die mit dem OTV-Router (OTV-Router A) verbunden ist. Dieser IGMP-Client muss alle Multicast-Gruppen abonnieren, die Remote-Clients abonnieren können. Dies würde dazu führen, dass der PIM-Router den Multicast-Verkehr an die Broadcast-Domäne neben dem OTV-Router A weiterleitet. Die IGMP-Abfragen würden dann beliebigen Multicast-Datenverkehr aufnehmen und über das Overlay gesendet.

Die andere Lösung wäre, einen "ip igmp static-join" für alle Gruppen zu konfigurieren, die Remote-Clients möglicherweise abonnieren können. Dies würde auch dazu führen, dass der PIM-Router den Multicast-Verkehr an die Broadcast-Domäne neben dem OTV-Router A weiterleitet.

Diese Einschränkung ist bekannt und Teil der Konstruktionsspezifikation. Es wird derzeit nicht als Bug angesehen, sondern als Grenzwert in der unterstützten Topologie.

Überlegungen zur QoS

Standardmäßig wird der TOS-Wert im hinzugefügten OTV-Header des ASR1000 aus den 802.1p-Bits des L2-Pakets kopiert. Wenn das L2-Paket nicht gekennzeichnet ist, wird der Wert 0 verwendet.

Der Nexus 7000 hat ein anderes Standardverhalten als der Nexus 7000 (ab Version 5.2.1). Wenn das gewünschte Verhalten darin besteht, den TOS-Wert der inneren Pakete in den äußeren zu kopieren, kann dies durch eine zusätzliche QoS-Konfiguration erreicht werden. Dies entspricht dem Verhalten der neueren Nexus 7000-Software.

Die Konfiguration zum Kopieren des L2-Pakete-L3-TOS-Werts in den äußersten Header des OTV-Pakets ist nachfolgend festgelegt:

```
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
```

Die bereitgestellte Konfiguration muss mit dem Datenverkehr für verschiedene DSCP-Werte beim Eingang übereinstimmen. Das lokal relevante QoS-Gruppen-Tag wird verwendet, um diesen Datenverkehr während der Übertragung durch den Router intern zu markieren. An der Ausgangsschnittstelle wird die QoS-Gruppe zugeordnet, und anschließend wird das äußerste TOS-Byte entsprechend aktualisiert.

Überlegungen zur WAN-MTU/Fragmentierung

OTV verwendet im Wesentlichen einen GRE-Header, um L2-Datenverkehr über das WAN zu transportieren. Dieser GRE-Header hat eine Größe von 42 Byte. In einer idealen Netzwerkbereitstellung muss die WAN-Verbindung eine Maximum Transmission Unit (MTU) aufweisen, die mindestens 42 Byte größer ist als das größte Paket, das OTV voraussichtlich verarbeiten wird.

Wenn die L2-Schnittstelle eine MTU von 1500 Byte hat, muss die Join-Schnittstelle eine MTU von 1542 Byte oder mehr haben. Wenn die L2-Schnittstelle eine MTU von 2.000 Byte hat, aber nur Pakete mit einer Größe von 1.500 Byte verarbeiten soll, dann ist eine WAN-MTU von 1.542 Byte ausreichend. Die standardmäßige Hinzufügung von 42 Byte zu 2.000 wäre jedoch ideal.

```
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
```

Einige Service Provider sind nicht in der Lage, höhere MTU-Werte für ihre WAN-Schaltkreise bereitzustellen. Ist dies der Fall, kann der ASR1000 eine Fragmentierung der über OTV übertragenen Daten durchführen. Nexus 7000 bietet diese Funktion nicht. Gemischte ASR1000- und Nexus 7000-OTV-Netzwerke mit aktivierter Fragmentierung auf dem ASR1000 werden nicht unterstützt.

Die Konfiguration für die OTV-Fragmentierung ist wie folgt:

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

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

Es ist wichtig, dass der Befehl auf globaler Ebene vor dem Befehl "Overlay interface join-interface" konfiguriert wird. Wenn der Befehl otv join-interface der Overlay-Schnittstelle zuerst konfiguriert wurde, entfernen Sie den Befehl otv join-interface von der Overlay-Schnittstelle, konfigurieren Sie den Befehl otv fragmentation join-interface, und konfigurieren Sie den Befehl otv join-interface der Overlay-Schnittstelle erneut.

Wenn die OTV-Fragmentierung nicht aktiviert ist, werden alle OTV-Pakete, die gekapselte L2-Daten enthalten, mit festgelegtem DF-Bit gesendet, sodass sie bei der Übertragung nicht fragmentiert werden. Sobald der Fragmentierungsbefehl hinzugefügt wurde, wird das DF-Bit auf 0 gesetzt. Die OTV-Router selbst können das Paket fragmentieren und es kann bei der Übertragung durch andere Router fragmentiert werden.

Die ASR1000-Plattformen verfügen nur über eine begrenzte Anzahl an Puffern für die Paketzusammenfügung. Je weniger Fragmente ein Paket für die Übertragung zerlegt, desto besser. Dies erhöht die Effizienz und verringert die Bandbreitennutzung im gesamten WAN, falls dies ein Problem darstellt. Die OTV-Fragmentierung kann sich negativ auf die Leistung auswirken. Wenn eine Fragmentierung vorliegt und davon ausgegangen wird, dass mehr als 1 Gb/s OTV-Datenverkehr verarbeitet werden soll, muss die OTV-Leistung weiter untersucht werden.

Spezialfall Unicast-Topologie

Außenstellenbereitstellungen für OTV verfügen häufig über direkte Back-to-Back-Glasfaserverbindungen zwischen den OTV-Routern in zwei Rechenzentren.

Für Single-Homed-Topologien ist dies eine Standardbereitstellung, bei der OTV- und Nicht-OTV-Datenverkehr die Join-Schnittstelle gemeinsam nutzen. Für diese Konfiguration sind keine besonderen Überlegungen erforderlich, daher gilt dieser Abschnitt nicht.

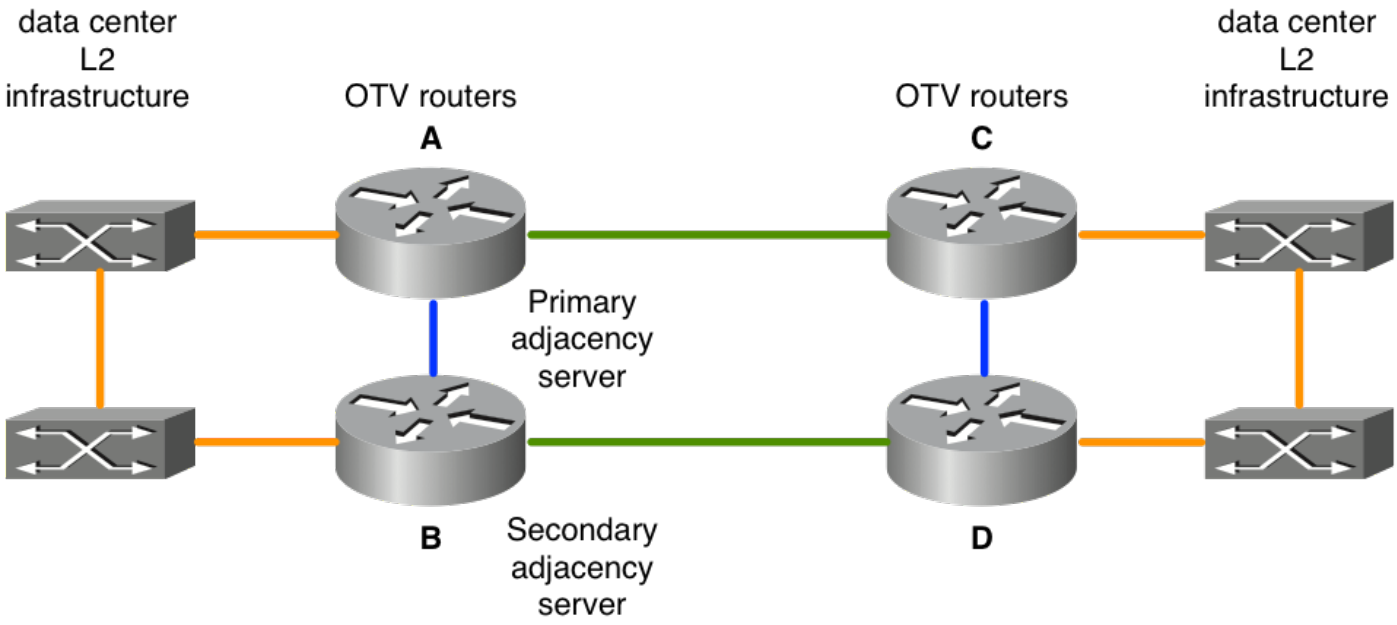
Wenn die Bereitstellung jedoch über Multihomed-OTV-Router in den beiden Rechenzentren verfügt, müssen einige besondere Überlegungen angestellt werden. Eine zusätzliche Konfiguration ist erforderlich.

Bei mehr als zwei Rechenzentren gilt diese Sonderkonfiguration nicht.

Bei einem Szenario mit mehr als zwei Rechenzentren mit einem oder mehreren OTV-Routern muss eine standardmäßige Unicast- oder Multicast-OTV-Bereitstellung verwendet werden.

Es gibt keine andere unterstützte Alternative.

Abbildung 8: Sonderfall Unicast



In der dargestellten Topologie sind die Verbindungen in Grün die Dark Fiber-Verbindungen zwischen den beiden Rechenzentren. Diese Dark Fiber werden direkt an die OTV-Router angeschlossen. Die blauen Verbindungen zwischen den OTV-Routern werden verwendet, um Nicht-OTV-Datenverkehr umzuleiten, wenn die grünen Verbindungen ausfallen. Wenn die obere grüne Verbindung ausfällt (A bis C), wird Nicht-OTV-Datenverkehr, der die obersten OTV-Router als Standardroute verwendet, über die Nord-Süd-Blau-Verbindungen (A bis B und C bis D) an die noch funktionsfähige grüne Verbindung zwischen dem unteren OTV-Routerpaar (B bis D) weitergeleitet.

Diese grundlegende Umleitung des Datenverkehrs funktioniert nicht für den OTV-Datenverkehr, da in der OTV-Konfiguration eine physische Schnittstelle als Join-Schnittstelle angegeben ist. Wenn die "grüne Schnittstelle" des OTV-Routers A ausfällt, kann der OTV-Datenverkehr nicht von einem alternativen OTV-Schnittstellenrouter B bezogen werden. Da keine vollständige Konnektivität über den WAN-Core besteht, können darüber hinaus nicht alle OTV-Router über einen Ausfall informiert werden. Um dieses Problem zu umgehen, wird die bidirektionale Weiterleitungserkennung (BFD) zusammen mit Embedded Event Manager (EEM)-Scripting verwendet.

BFD muss die WAN-Verbindung zwischen den Ost-West-OTV-Routerpaaren (A/C und B/D) überwachen. Wenn die Verbindung zum Remote-Router unterbrochen wird, wird die OTV-Overlay-Schnittstelle über das EEM-Script auf diesem Ost-West-Paar von OTV-Routern heruntergefahren. Dadurch übernimmt der gepaarte Router mit mehreren Heimnetzwerken die Weiterleitung für alle VLANs. Wenn BFD erkennt, dass die Verbindung wiederhergestellt wurde, löst das EEM-Skript die erneute Aktivierung der Overlay-Schnittstelle aus.

Es ist sehr wichtig, dass BFD zum Erkennen von Verbindungsausfällen verwendet wird. Der Grund hierfür ist, dass die Overlay-Schnittstelle sowohl auf der "ausgefallenen" Seite als auch auf der Ost-West-Verbindung heruntergefahren werden muss. Je nach Art der vom Service Provider bereitgestellten Verbindung kann eine physische Verbindung ausfallen (grüne Schnittstelle auf OTV-Router A), während die entsprechende Ost-West-Router-Schnittstelle in Betrieb bleiben kann (grüne Schnittstelle auf OTV-Router C). BFD erkennt einen Ausfall einer Schnittstelle oder ein

anderes Problem bei der Übertragung und benachrichtigt beide Paare sofort gleichzeitig. Dasselbe gilt, wenn die Router über die Wiederherstellungsverbindung informiert werden müssen.

Die Konfiguration für diese Bereitstellung ist mit der Konfiguration für alle anderen Bereitstellungen identisch, wobei die folgenden Elemente hinzugefügt werden:

- BFD-Konfiguration an der WAN-Schnittstelle
- das nachfolgende EEM-Skript
- OTV-ISIS-Identität zur Übereinstimmung mit gerader/ungerader VLAN-Verteilung

Die Konfiguration von BFD auf der OTV-Join-Schnittstelle wird in diesem Dokument nicht behandelt. Informationen zur BFD-Konfiguration auf dem ASR1000 finden Sie unter:

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

Sobald die BFD-Ausfallerkennung zwischen den Join-Schnittstellenpaaren (grüne Links im Diagramm) ordnungsgemäß funktioniert, muss das EEM-Skript bereitgestellt werden. Das EEM-Skript muss auf die jeweiligen Router zugeschnitten werden, um die richtigen Overlay-Schnittstellen zu ändern und möglicherweise genauere Strings im Protokoll auf BFD-Fehler und Wiederherstellung zu überwachen.

```
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 ..."
!
```

Bei dieser Art der Bereitstellung müssen auch die Ost-West-Routerpaare (A/C und B/D) bei der Weiterleitung ungerader und gerader VLANs übereinstimmen.

Beispielsweise müssen A und C gerade VLANs weiterleiten, während B und D ungerade VLANs im Dauerbetrieb weiterleiten.

Die ungerade/gerade Verteilung wird durch die OTV-Ordnungszahl bestimmt, die mit dem Befehl "show otv site" angezeigt werden kann.

Die Ordnungszahl zwischen den beiden Standort-Routern wird auf Basis der OTV-ISIS-Netz-ID bestimmt.

```
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
```

Die OTV-ISIS-Netzkennung muss auf allen OTV-Routern konfiguriert werden. Bei der Konfiguration der Kennung muss darauf geachtet werden, dass sich alle OTV-Router immer noch gegenseitig erkennen.

<#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

.

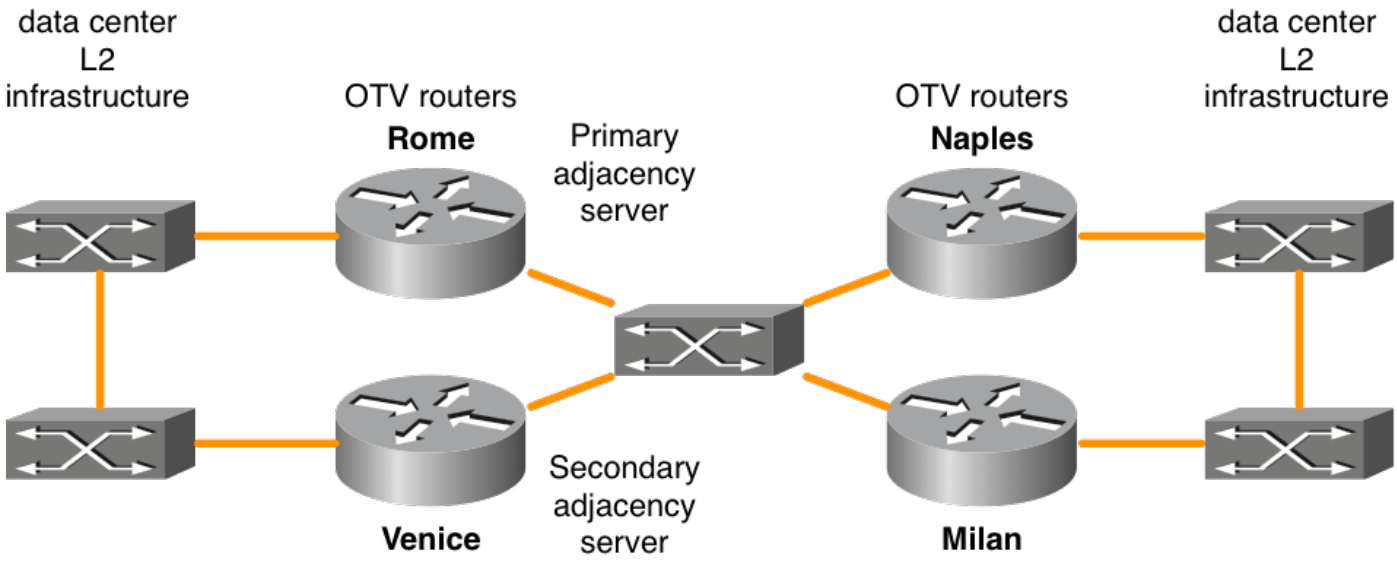
00

Die schwarzen Teile der Kennung müssen mit allen OTV-Routern übereinstimmen, die am Overlay beteiligt sind. Der rot markierte Teil der Kennung kann geändert werden. Die niedrigste Netzwerkkennung an einem Standort erhält die Ordnungszahl 0 und leitet die geraden VLANs weiter. Die höchste Netzwerkkennung eines Standorts erhält die Ordnungszahl 1 und leitet die ungeraden Zahlen an die VLANs weiter.

Konfigurationsbeispiele

Unicast

Abbildung 9: Unicast-Konfigurationsbeispiel



Konfiguration in Rom:

```
!
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
 !
```

Konfiguration von Venedig:

```
!
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
 !
```

Konfiguration von Neapel:

```
!
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
 !
!
```

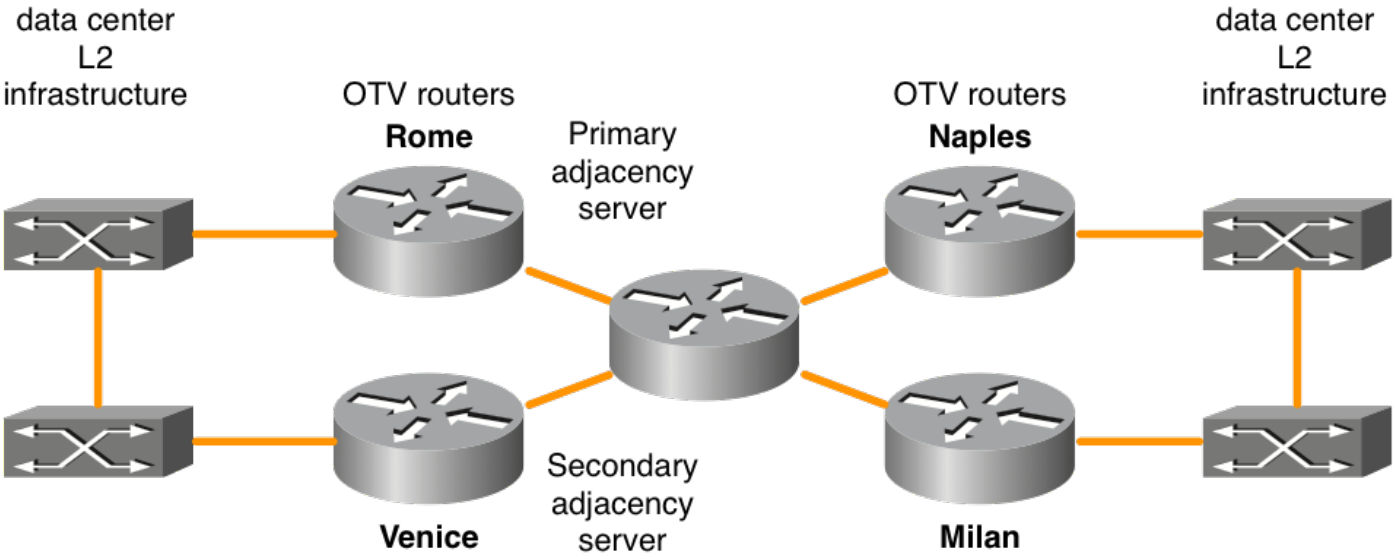
Mailand-Konfiguration:

```
!
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

Abbildung 10: Multicast-Konfigurationsbeispiel



Konfiguration in Rom:

```
!
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
 !
```

Konfiguration von Venedig:

```
!
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
 !
```

Konfiguration von Neapel:

```
!
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
 !
!
```

Mailand-Konfiguration:

```
!
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
 !
!
```

Häufig gestellte Fragen

Frage: Werden private VLANs in Verbindung mit OTV unterstützt?

A) Ja, in OTV ist keine spezielle Konfiguration erforderlich. Stellen Sie in der privaten VLAN-Konfiguration sicher, dass die mit der OTV-L2-Schnittstelle verbundenen Switch-Ports im Promiscuous-Modus konfiguriert sind.

F) Wird OTV mit IPSEC crypto unterstützt?

Antwort: Ja, die Crypto-Map-Konfiguration auf der Join-Schnittstelle wird unterstützt. Für die Unterstützung von Crypto ist keine spezielle Konfiguration für OTV erforderlich. Durch die Verschlüsselungskonfiguration entsteht jedoch zusätzlicher Overhead, der durch die Erhöhung der WAN-MTU im Vergleich zur LAN-MTU kompensiert werden muss. Wenn dies nicht möglich ist, muss eine OTV-Fragmentierung erforderlich sein. Die OTV-Leistung ist auf die der IPSEC-Hardware beschränkt.

Frage: Wird OTV von MACSEC unterstützt?

Antwort: Ja, ASR1001-X bietet MACSEC-Unterstützung für die integrierten Schnittstellen. OTV funktioniert mit MACSEC, das auf den LAN- und/oder WAN-Schnittstellen konfiguriert wurde. Die OTV-Leistung ist auf die der MACSEC-Hardware beschränkt.

Frage: Kann eine Loopback-Schnittstelle als Join-Schnittstelle verwendet werden?

Antwort: Nein, nur Ethernet-, Port-Channels oder POS-Schnittstellen können als OTV-Join-Schnittstellen verwendet werden. Die OTV-Loopback-Join-Schnittstelle ist in der Roadmap vorgesehen, ihre Einführung ist jedoch derzeit noch nicht geplant.

F) Kann eine Tunnelschnittstelle als Join-Schnittstelle verwendet werden?

Antwort: Nein, GRE-Tunnel, DMVPN-Tunnel oder andere Tunneltypen werden als Join-Schnittstellen nicht unterstützt. Nur Ethernet-, Port-Channels oder POS-Schnittstellen können als OTV-Join-Schnittstellen verwendet werden.

F) Können verschiedene Overlay-Schnittstellen unterschiedliche L2- und/oder Join-Schnittstellen verwenden?

Antwort: Alle Overlay-Schnittstellen müssen auf dieselbe Join-Schnittstelle verweisen. Alle Overlays müssen mit der gleichen physischen Schnittstelle verbunden sein, damit L2-Verbindungen zum Rechenzentrum möglich sind.

Frage: Kann sich das VLAN des OTV-Standorts auf einer anderen physischen Schnittstelle befinden als die erweiterten OTV-VLANs?

Antwort: Das VLAN des OTV-Standorts und die erweiterten VLANs müssen sich auf derselben physischen Schnittstelle befinden.

Frage: Welcher Funktionssatz ist für OTV erforderlich?

Antwort: Advanced IP Services (AIS) oder Advanced Enterprise Services (AES) sind für OTV erforderlich.

Frage: Ist für OTV auf festkonfigurierten Plattformen eine separate Lizenz erforderlich?

Antwort: Nein. Solange der ASR1000 mit advipservices oder konfiguriertem adventerprise Boot-Level ausgeführt wird, ist OTV verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.