Configuración de Overlay Transport Virtualization con ASR 1000

Contenido

Introducción

Este documento describe las topologías de red Overlay Transport Virtualization (OTV) soportadas en los routers de las series ASR1000 y Catalyst 8300/8500.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASR1000, IOS® XE versión 16.10.1a y posteriores
- Catalyst 8300, IOS® XE versión 17.5.1a y posterior
- Catalyst 8500, IOS® XE versión 17.6.1a y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

ASR1000 es compatible con OTV desde Cisco IOS® XE versión 3.5. El router Catalyst de la serie 8300 comienza a ser compatible con IOS® XE17.5.1a y las rutas Catalyst de la serie 8500 comienzan a ser compatibles con IOS® XE versión 17.6.1a.

OTV proporciona conectividad de capa 2 entre sitios de red remotos mediante routing basado en direcciones MAC y reenvío encapsulado IP (MAC en IP) a través de una red de transporte para proporcionar compatibilidad con aplicaciones que requieren adyacencia de capa 2, como clústeres y virtualización. OTV utiliza un protocolo de plano de control de superposición para aprender y propagar la información de ruteo MAC a través de la red superpuesta. El protocolo de plano de control OTV utiliza mensajes de sistema intermedio a sistema intermedio (IS-IS) para crear adyacencias a sitios remotos y enviar actualizaciones de rutas MAC a sitios remotos. OTV crea adyacencias de capa 2 a sitios remotos en la red superpuesta mediante la detección automática de dispositivos OTV remotos.

Las ventajas de OTV para la extensión de capa 2 incluyen:

- Sin requisito de MPLS
- Sin configuración compleja de Ethernet sobre switching de etiquetas multiprotocolo (EoMPLS) para la malla
- Sin implementación compleja de servicios de LAN privada virtual (VPLS) para extensiones de capa 2
- Aislamiento del árbol de extensión nativo
    - no es necesario configurar explícitamente los filtros de la unidad de protocolo de datos de puente (BPDU)
    - aislamiento predeterminado de los problemas del árbol de extensión en un Data Center determinado
- Aislamiento de inundación de unidifusión desconocida nativa
    - los paquetes MAC de unidifusión desconocidos no se reenvían
    - se permite el soporte para reenvío de unidifusión desconocido por MAC
- Optimización del protocolo de resolución de direcciones (ARP) con el almacenamiento en caché de ARP de OTV
    - reduce el tráfico WAN innecesario
- Aprovisionamiento simplificado del aislamiento del protocolo de redundancia de primer salto

(FHRP)
- Incorporación simplificada de sitios
- Configuración de redundancia simplificada
- Posibilidad de disponer de un "dispositivo de entrega" para las migraciones cuando se requieran servicios temporales

Requirements

Los elementos siguientes son las reglas principales que se deben tener en cuenta al diseñar una implementación de OTV. Si se cumplen estas reglas, el diseño y la implementación se simplifican.

- Una y solo una interfaz se puede utilizar para transmitir el tráfico encapsulado OTV, conocido como la interfaz de unión, para todas las interfaces OTV Overlay configuradas
- Una y solo una interfaz se puede utilizar para configurar las instancias de servicio de L2 del Data Center para la VLAN del sitio OTV y las VLAN extendidas entre los Data Centers para todas las interfaces OTV Overlay configuradas
- Los canales de puerto se pueden utilizar para la redundancia de interfaz y la conexión a switches VSS o VPC y se admiten como la interfaz "única" para la conectividad.
- Todos los routers OTV deben ser contactables a través de la interfaz de unión
- El árbol de extensión se debe configurar en el router OTV que apunta al Data Center
- La indagación y la consulta IGMP deben configurarse para reenviar correctamente el tráfico multidifusión del Data Center
- Un Data Center determinado se puede configurar con 1 o 2 routers OTV. Con dos routers, distribuyen el reenvío de VLAN de manera par/impar según el número de VLAN. Cada router OTV de un Data Center actúa como copia de seguridad del otro.
- Los pares de hosts múltiples deben configurarse con el mismo identificador de sitio OTV
- ASR 1000/Catalyst 8300/Catalyst 8500 y Nexus 7000 pueden participar en la misma red OTV
    - Nexus 7000 no admite fragmentación ni cifrado OTV, por lo que estas funciones no se pueden utilizar en una implementación "híbrida".

Existen ciertos diseños de conectividad adosada compatibles que no cumplen con las reglas establecidas. Aunque estas configuraciones son compatibles, no se recomiendan. Los detalles sobre estos se pueden encontrar en la sección posterior "Caso especial de topología unicast".

No se puede enfatizar lo suficiente que el software OTV actual tiene la restricción de interfaz "uno y solo uno" cuando se configura la unión y las interfaces de acceso L2 para OTV. Una interfaz de canal de puerto se puede utilizar para la redundancia. Se admite la conexión del canal de puerto a Nexus 7000 en un VPC. También se admite una conexión de canal de puerto básica a un solo switch.

Tipos de implementación de OTV

OTV requiere una única interfaz de unión y una única interfaz L2. Cada router OTV puede admitir sólo uno de ellos. OTV también requiere que se configure una VLAN de sitio para que los routers

OTV de hosts múltiples puedan comunicarse entre sí a través de la red local. Incluso los routers OTV de enlace único deben tener configurada la VLAN del sitio OTV. Además, cada sitio o Data Center debe tener configurado un identificador de sitio único. Los routers OTV doblemente conectados deben utilizar el mismo identificador de sitio y poder comunicarse a través de la misma VLAN.

La configuración subsiguiente proporciona la configuración básica necesaria para OTV. Sin embargo, no está completa, ya que se debe agregar la configuración de núcleo de unidifusión o multidifusión. Esas recomendaciones se detallan en las secciones siguientes del presente documento.

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

La configuración de instancia de servicio se utiliza para toda la configuración de interfaz L2 con OTV.

Cada instancia de servicio en la interfaz L2 debe estar asociada con una encapsulación de etiqueta simple o doble específica.

A su vez, cada una de esas instancias de servicio debe estar asociada a un dominio de bridge.

Ese dominio de bridge se utiliza en una instancia de servicio configurada en la interfaz de superposición.

El dominio de bridge es el pegado que enlaza la instancia del servicio de superposición con la instancia del servicio de interfaz L2.

La encapsulación del tráfico en la interfaz superpuesta debe coincidir con la encapsulación del tráfico después de reescribir el ingreso en la interfaz L2.

En el ejemplo, el tráfico que ingresa en la instancia de servicio 99 Gig1/0/1 tiene una sola VLAN 802.1Q de 99 y el dominio de bridge 99. La instancia de servicio correspondiente con el dominio de bridge 99 en la interfaz de superposición también se configura para una sola VLAN 802.1Q de 99. Este caso es el más sencillo.

En el ejemplo, el tráfico que ingresa en la instancia de servicio 98 Gig1/0/1 tiene una VLAN 802.1Q doble de 99 y 1098 y un dominio de bridge 90. La instancia de servicio correspondiente con el dominio de bridge 90 en la interfaz de superposición se configura para una única VLAN 802.1Q de 90. Claramente, no son iguales. El comando rewrite ingress garantiza que las etiquetas se traduzcan correctamente a medida que el tráfico se mueve a través de la interfaz de ingreso. El tráfico que ingresa a la interfaz L2 tiene las VLAN 802.1Q 98/1098 reemplazadas por una sola VLAN de 90. La palabra clave symmetric asegura que el tráfico que egresa de la interfaz L2 tenga la única VLAN 802.1Q de 90 reemplazada por 98/1098.

Cualquier instancia de servicio con varias VLAN 802.1Q ampliadas por OTV debe utilizar el comando rewrite ingress. La encapsulación OTV sólo admite un único identificador de VLAN. Por esa razón, cualquier configuración de VLAN doble en las interfaces L2 se debe reescribir en una sola etiqueta en la instancia de servicio de interfaz de superposición. Esto excluye el soporte para configuraciones VLAN ambiguas.

Para obtener más información sobre la reescritura de etiquetas, consulte este documento: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

En este ejemplo, el dominio de bridge del sitio OTV es 100.

- El dominio de bridge del sitio OTV se configura solamente en la interfaz L2.
- El dominio de puente de sitio OTV nunca debe configurarse en la interfaz de superposición, ya que esto hace que la implementación de OTV sea inestable.
- La VLAN del sitio de OTV debe estar conectada únicamente a los routers OTV y no debe transportar ningún otro tráfico de usuarios/Data Centers.
- La VLAN del sitio OTV debe estar en la misma interfaz física que las VLAN ampliadas OTV.

Multicapa

Un Data Center se puede conectar con un solo host OTV o hasta 2 para obtener redundancia, también conocido como multihome. Multihome se utiliza para la resistencia y el equilibrio de carga. Cuando más de un dispositivo de borde está presente en un sitio y ambos participan en la misma red superpuesta, el sitio se considera multihomed. OTV Multihome divide las VLAN entre los dos routers OTV que pertenecen al mismo sitio de forma par/impar en función del número de VLAN. Un dispositivo de borde se elige como AED para todas las VLAN impares, mientras que el otro router OTV se elige como AED para todas las VLAN pares. Cada AED también es un modo de espera para las VLAN que están activas en el otro router. En caso de falla de link o nodo en

uno de los AED, el AED en espera se activa para todas las VLAN.

Si hay dos ASR 1000 conectados en el mismo Data Center para realizar la funcionalidad de varias unidades, no es necesario un enlace dedicado entre los dos ASR 1000. OTV utiliza la VLAN del sitio OTV que se propaga a través de la interfaz interna y la comunicación a través de la interfaz de unión para determinar qué routers son responsables de las VLAN pares e impares.

Los routers ASR1000 y Nexus 7000 no se pueden mezclar en el mismo Data Center con OTV configurado en ambos routers como copia de seguridad del otro. Las plataformas compatibles (ASR1000 o Nexus 7000) son compatibles con varias casas en un Data Center determinado. Puede tener ASR1000 en un Data Center y Nexus 7000 en otro Data Center. Se ha probado y respaldado la interoperabilidad entre estas dos plataformas. Algunos Data Centers pueden tener varias conexiones, mientras que otros son de una única conexión.

Los pares de routers ASR1000 con varias conexiones deben ejecutar la misma versión del software Cisco IOS® XE.

Si se utiliza Multihome, se recomienda encarecidamente que se active el árbol de extensión en los routers OTV, ya que esto permite que el router OTV envíe una notificación de cambio de topología (TCN) que hace que el dispositivo de switch de L2 adyacente (junto con otros switches en el árbol de extensión) reduzca su temporizador de antigüedad del valor predeterminado a 15 segundos. Esto aumenta en gran medida la convergencia de velocidad cuando hay una falla o recuperación entre el par multihomed. El árbol de expansión se puede habilitar para todas las instancias de servicio configuradas (conectadas a OTV o de otro modo) mediante la adición de la línea subsiguiente a la configuración global.

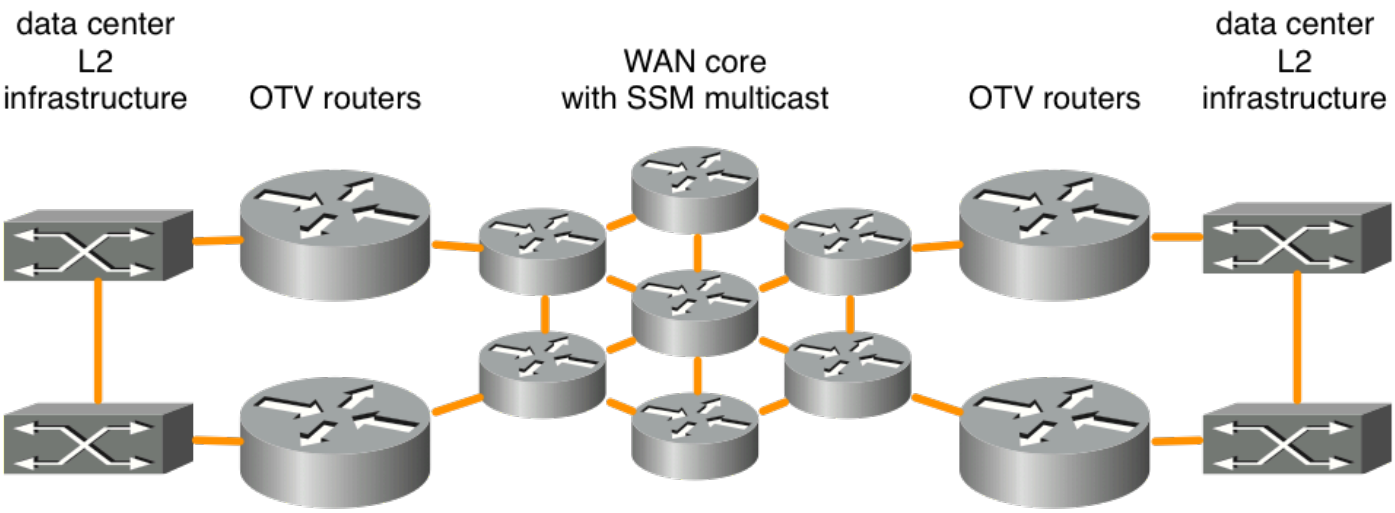
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

No se requiere ninguna configuración específica por vlan o por instancia de servicio.

Núcleo de multidifusión

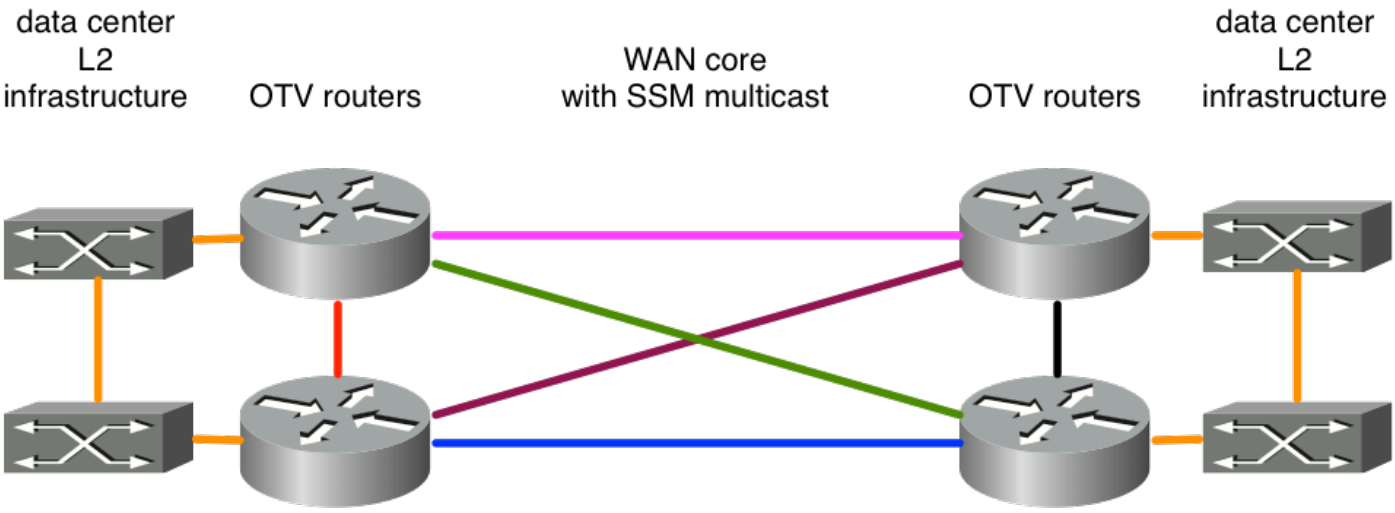
La red multidifusión requiere conectividad de malla completa en toda la WAN. Todos los routers OTV deben estar conectados entre sí a través de la interfaz de unión.

Figura 1. Topología de red de multidifusión admitida



En esta figura se muestra un ejemplo de dos Data Centers conectados a través de un núcleo en malla completa. La multidifusión de origen específico (SSM) y la multidifusión independiente del protocolo (PIM) se ejecutan entre los routers OTV y los routers de núcleo WAN. Se admite cualquier número de routers de núcleo siempre que haya conectividad de malla completa. No existe un requisito explícito de latencia máxima para la conectividad OTV en el núcleo WAN.

Figura 2 Topología de red de multidifusión no admitida



Debido a que ASR1000/OTV espera recibir mensajes de multidifusión en una única interfaz de unión de todos sus pares, por ejemplo, esto resultaría en una implementación de OTV inestable. Supongamos que los links este-oeste en rosa y azul se configuraran como interfaces de unión. Cuando el link rosa fallaba, el router ya no podía recibir actualizaciones de OTV en esa interfaz. Una trayectoria alternativa a través de los links verdes o morados sería inaceptable porque la interfaz de unión está configurada explícitamente. Se deben recibir actualizaciones en esa interfaz. En este momento no se admite el uso de interfaces de loopback como interfaz de unión.

Si los usuarios no son propietarios de su estructura básica, deben asegurarse de que su proveedor de servicios admite la multidifusión en su núcleo y de que puede responder a los mensajes de consulta del protocolo de administración de grupos de Internet (IGMP). OTV en ASR 1000 actúa como host de multidifusión (reenvía mensajes de unión IGMP), no como router de multidifusión a la topología de multidifusión WAN principal.

La red de transporte entre los routers OTV debe admitir el modo disperso de PIM (Cualquier multidifusión de origen [ASM]) para el grupo de multidifusión del proveedor y SSM para el grupo de entrega.

Los núcleos de multidifusión requieren alguna configuración específica en la interfaz de superposición para un grupo de control, así como un rango de grupos de multidifusión de datos que se utilizan para reenviar datos.

```
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
```

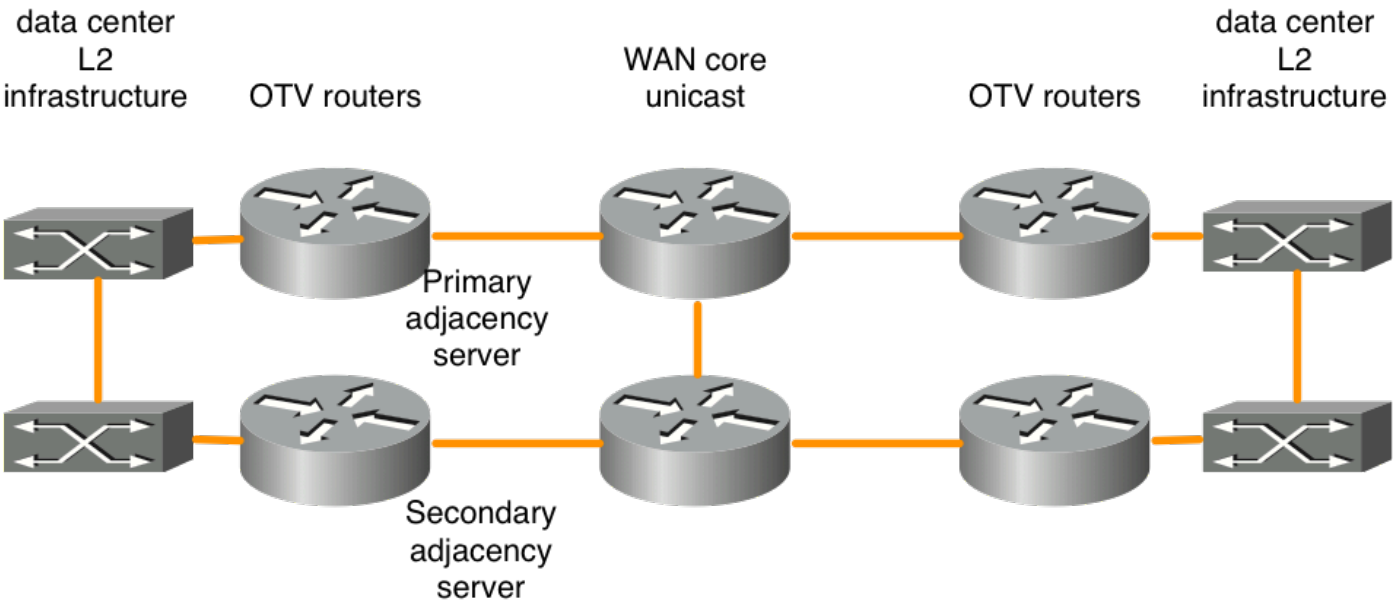
Las implementaciones de OTV de multidifusión requieren que la interfaz de unión se configure como una interfaz pasiva PIM. IGMP se puede configurar para diferentes versiones según sea necesario. La interfaz superpuesta debe tener configurados un grupo de control y un grupo de datos. El grupo de control es un único grupo de multidifusión que se utiliza para la administración de OTV. El grupo de datos es un intervalo de direcciones de multidifusión que se utilizan para transportar datos de usuario entre Data Centers. Si el grupo de datos no está en el espacio IP 232.0.0.0/8, el comando adicional "ip pim ssm range" debe configurarse para incluir el rango requerido por OTV.

La red de transporte entre los routers OTV debe admitir el modo disperso de PIM (cualquier multidifusión de origen [ASM]) para el grupo de multidifusión del proveedor y multidifusión desde un origen específico (SSM) para el grupo de entrega.

Núcleo unidifusión con servidores adyacentes

Cisco IOS® XE 3.9 agregó soporte para OTV con un núcleo de unidifusión. Los núcleos de unidifusión y multidifusión para OTV siguen siendo compatibles con todas las plataformas ASR1000 y las versiones futuras de Cisco IOS® XE 3.9.

Figura 3. Topología de red unidifusión



La función de servidor de adyacencia de OTV permite el transporte solo de unidifusión entre la frontera de OTV. Los routers OTV configurados con el rol de servidor de adyacencia mantienen una lista de todos los routers OTV conocidos. Proporcionan esa lista a todos los routers OTV registrados para que tengan una lista de dispositivos que deben recibir tráfico de difusión y multidifusión replicado.

El plano de control OTV sobre un transporte solo de unidifusión funciona exactamente igual que OTV con núcleo de multidifusión, excepto en que en una red de núcleo de unidifusión, cada dispositivo de extremo OTV necesita crear varias copias de cada paquete de plano de control y unidifusión en cada dispositivo de extremo remoto en la misma superposición lógica.

En la misma línea de pensamiento, cualquier tráfico multidifusión del Data Center se replica en el router OTV local y se envían varias copias a cada uno de los Data Centers remotos. Aunque esto resulta menos eficaz que depender del núcleo WAN para realizar la replicación, no se requiere la configuración y la gestión de la red de multidifusión principal. Si solo hay una pequeña cantidad de tráfico de multidifusión del Data Center o solo hay un pequeño número de ubicaciones de Data Center (cuatro o menos), un núcleo de unidifusión para el reenvío de OTV suele ser la mejor opción. En general, la simplificación operativa del modelo de solo unidifusión hace que la opción de implementación de núcleo de unidifusión sea la preferida en escenarios donde la conectividad de extensión LAN solo se requiere entre cuatro o menos Data Centers. Se recomienda tener al menos dos servidores de adyacencia configurados, uno primario y otro de respaldo. No hay ninguna opción para la configuración del servidor de adyacencia activo/activo.

Los routers OTV deben configurarse según corresponda para identificar y registrar correctamente el servidor de adyacencia apropiado.

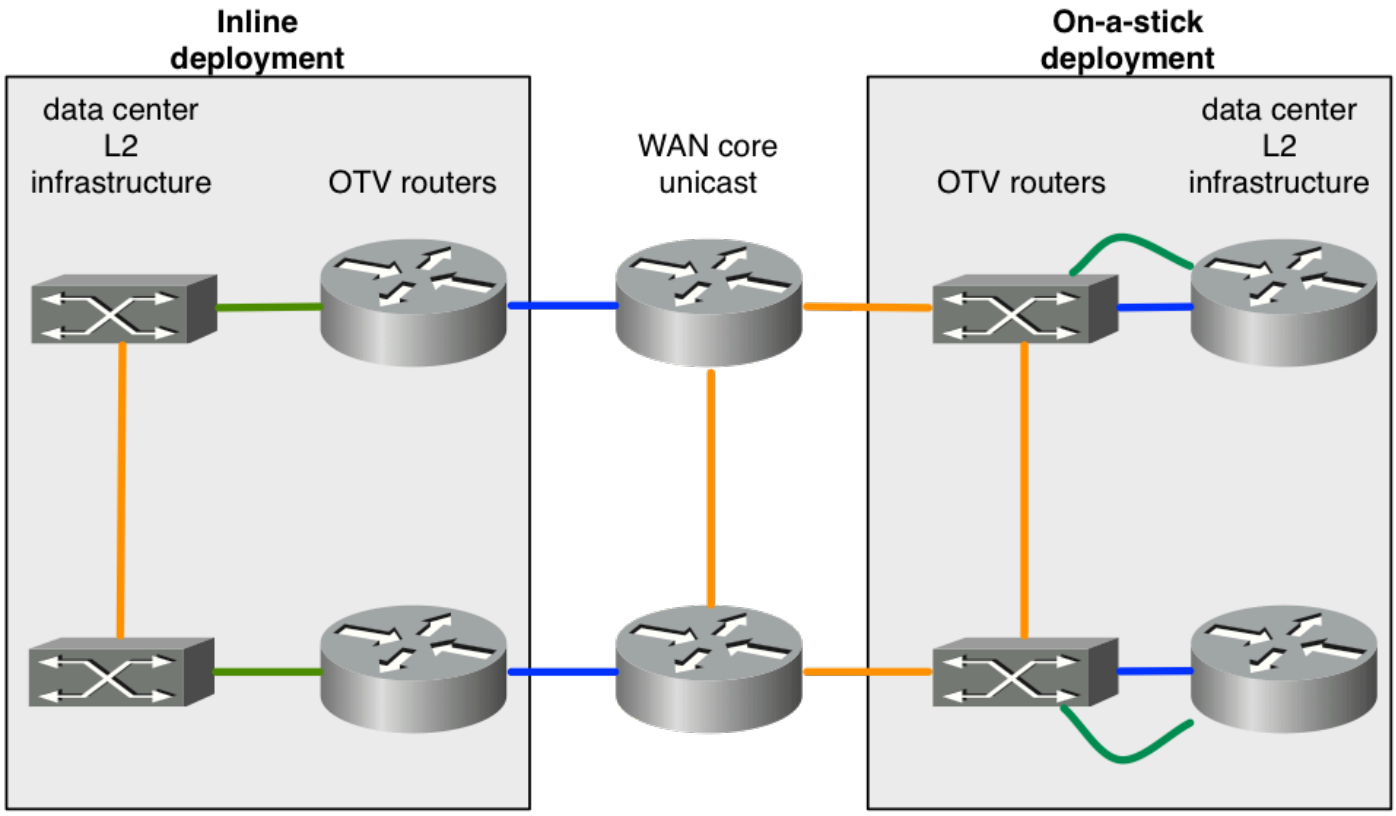
	Servidor de adyacencia principal	Servidor de adyacencia secundario	Otros routers OTV
Dirección IP de interfaz de unión a OTV	10.0.0.1	10.2.2.24	otras direcciones IP
Configuración	interface Overlay 1 otv adjacency-server unicast-only	interface Overlay 1 otv adjacency-server unicast-only otv use-adjacency-server 10.0.0.1 unicast-only	interface Overlay 1 otv use-adjacency-server 10.0.0.1 10.2.2.24 unicast-only

Existen ciertos diseños de conectividad adosada compatibles con el reenvío de OTV de unidifusión que no cumplen las reglas de "malla completa". Aunque estas configuraciones son compatibles, no se recomiendan. Este tipo de implementación es más habitual cuando los Data Centers se conectan mediante fibra oscura. Los detalles de esta opción de configuración se pueden encontrar en la sección posterior "Topología de unidifusión de caso especial".

OTV en un palo frente a en línea

Hay dos modelos para implementar OTV en su Data Center: en un solo sentido y en línea. En los escenarios de diseño presentados anteriormente, los routers OTV estaban alineados entre el Data Center y la red principal del proveedor de servicios. Sin embargo, la adición del router OTV como un dispositivo que no está en la trayectoria de transporte de todo el tráfico podría ser más deseable. A veces, el requisito es no cambiar la topología actual para conectarse al proveedor de servicios a través del equipo actual (por ejemplo, una implementación antigua con un switch Catalyst 6000 o un hardware de switch Nexus que no sea compatible con OTV). Por lo tanto, es preferible implementar OTV en ASR1000 como en un solo dispositivo OTV.

Figura 4 Topología en línea frente a topología "en un solo sentido"



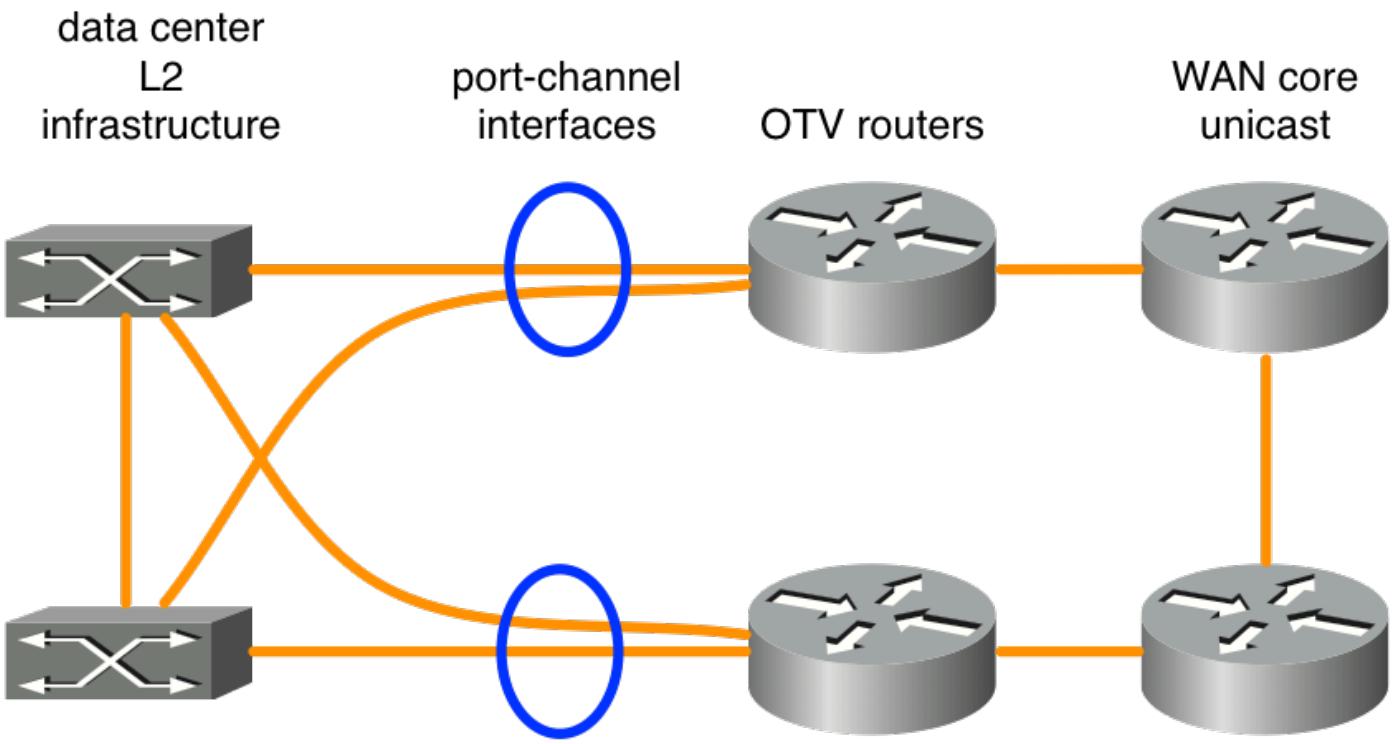
El diagrama muestra los dos modelos de implementación que pueden formar parte de la misma superposición. Los links verdes conectados a los routers OTV se configuran como interfaces de acceso L2 para aceptar el tráfico VLAN. Los links azules conectados a los routers OTV son las interfaces de unión que transportan el tráfico VLAN encapsulado OTV.

Puede ser necesario configurar una función que no sea compatible con OTV. Por ejemplo, OTV y MPLS no se pueden configurar en el mismo cuadro. Como resultado, puede ser una buena opción utilizar ASR1000/OTV en un solo dispositivo y configurar MPLS en el router que se encuentra delante del router OTV.

Canales de puerto para las capas 2 y 3

El código Cisco IOS® XE 3.10 para ASR1000 agregó compatibilidad con la configuración de canal de puerto de capa 2 y capa 3 con OTV. El canal de puerto de capa 2 se puede utilizar como interfaz interna. El canal de puerto debe constar de hasta 4 interfaces físicas. El canal de puerto de capa 3 se puede utilizar como interfaz de unión.

Figura 5. Canales de puerto utilizados para la conectividad L2



El diagrama muestra una situación típica de canal de puerto con dos switches en VSS (Catalyst 6000 Series) o VPC (Nexus 7000 Series). Este tipo de diseño ofrece redundancia con routers OTV duales y conectividad dual con la infraestructura del Data Center. No se requiere ninguna configuración especial para OTV que no sea la configuración básica de canal de puerto si se utiliza VSS o un VPC en un equipo de conmutación L2 adyacente a los routers OTV.

Gateway predeterminado

Por definición, OTV crea la misma subred L3 en varias ubicaciones. Esto requiere algunas consideraciones especiales al rutear el tráfico L3 hacia y desde las VLAN extendidas. El ruteo L3 se puede configurar en los routers OTV mismos o se puede configurar en otros dispositivos conectados a las VLAN extendidas. Además, en cada escenario se pueden implementar protocolos de redundancia de primer salto (FHRP) como el protocolo de redundancia en espera en caliente (HSRP) o el protocolo de redundancia de router virtual (VRRP) para obtener redundancia. HSRP puede ejecutarse de forma local en un Data Center determinado o extenderse entre Data Centers (no es habitual).

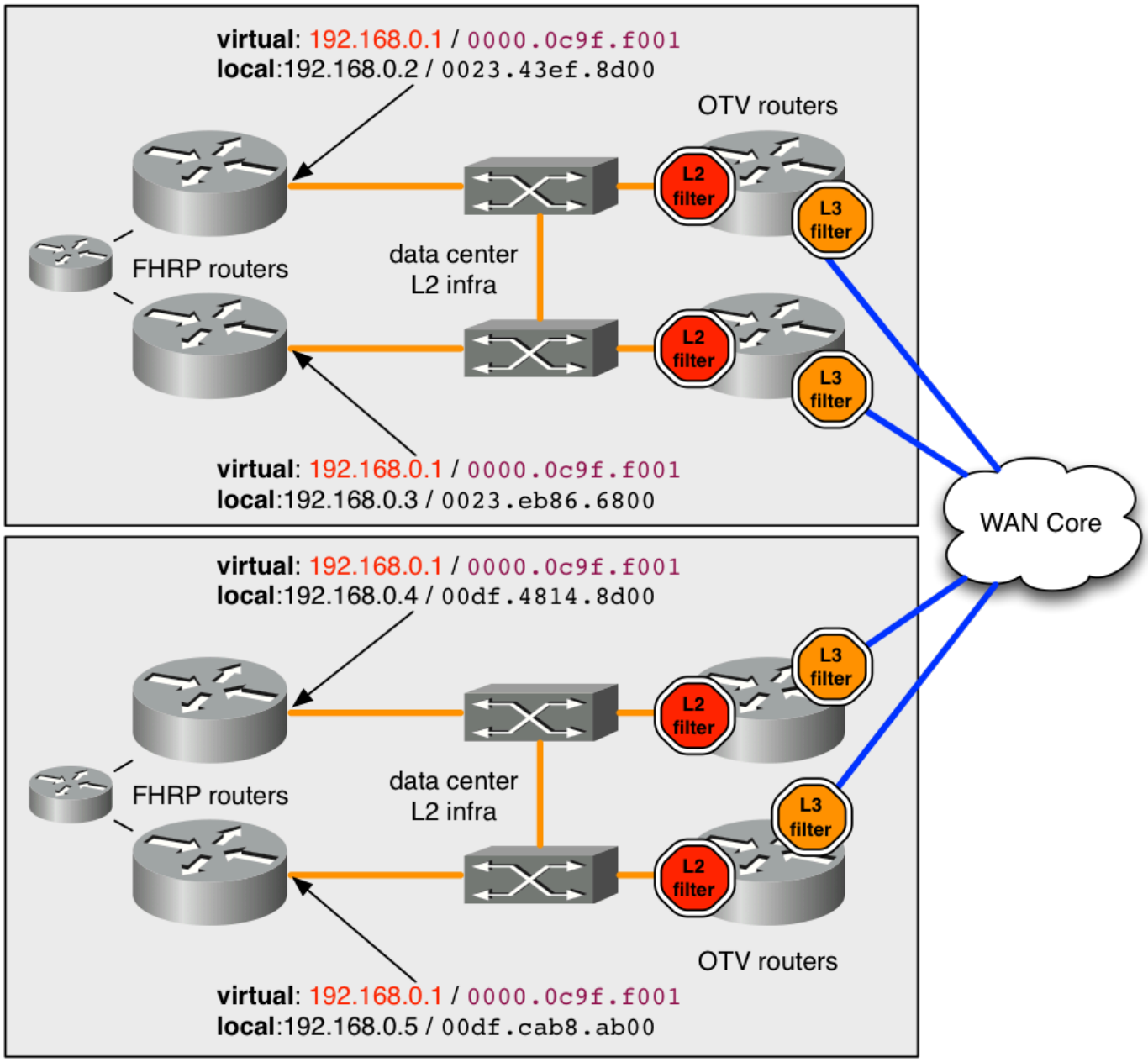
La práctica recomendada para las implementaciones de OTV que utilizan FHRP es que las instancias locales del FHRP se ejecuten en cada Data Center. Estas instancias de FHRP utilizan la misma dirección MAC virtual y la misma dirección IP de modo que, cuando las máquinas virtuales (VM) se mueven entre Data Centers, tienen una conexión ininterrumpida. Si la dirección MAC del router predeterminado cambiara entre Data Centers, las máquinas virtuales no podrían comunicarse fuera de la subred hasta que se agotara el tiempo de espera de la entrada ARP del gateway predeterminado de la máquina virtual.

Para implementar correctamente un FHRP con OTV, es necesario considerar qué tráfico L2 y L3 se debe filtrar y aislar de OTV. En el nivel L2, esto es necesario para evitar que OTV detecte el mismo MAC virtual L2 utilizado por el FHRP en varias ubicaciones. Se requieren filtros en el nivel

L3 para mantener los anuncios HSRP y VRRP aislados en cada Data Center de modo que la elección de activo/receptor/en espera se localice en cada Data Center.

De forma predeterminada, los filtros FHRP se activan cuando se activa OTV. Se puede deshabilitar si el diseño requiere que FHRP se extienda entre Data Centers. El filtrado L2 de direcciones MAC virtuales NO está habilitado de forma predeterminada y debe configurarse manualmente.

figura 6. Ejemplo de implementación recomendada para FHRP



En el ejemplo, la dirección MAC virtual 0000.0c9f.f001 se utiliza para la dirección IP 192.168.0.1 que se aloja en la VLAN extendida para la conectividad fuera de la subred. Al utilizar la misma dirección MAC e IP virtual en ambos Data Centers, un host tiene una conectividad perfecta de la subred cuando transfiere entre Data Centers.

Para mantener la dirección MAC 0000.0c9f.f001 oculta a OTV en varias ubicaciones, se debe implementar un filtro de entrada L2 (parada roja en el diagrama) para la VLAN en cada uno de los

routers OTV que dan servicio a la VLAN. Mediante el filtro ACL, la ACL de filtro configurada en las instancias de servicio L2 para la entrada, todos los paquetes originados en esa MAC se descartan antes de que el proceso OTV en ASR1000 pueda verlos. Por lo tanto, OTV nunca se entera de la MAC y no la anuncia a los Data Centers remotos.

Aquí se proporciona la configuración recomendada para capturar todo el tráfico MAC virtual FHRP conocido/predeterminado.

```
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
```

Esta ACL coincide con los espacios de direcciones MAC conocidos asociados con las versiones 1 y 2 de HSRP, el protocolo de equilibrio de carga de gateway (GLBP) y VRRP (en ese orden). Si la MAC virtual está configurada para utilizar un valor no estándar no basado en el número de grupo FHRP, se debe agregar explícitamente al ejemplo de ACL. La ACL se debe agregar a la instancia de servicio L2 (que se muestra aquí).

```
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
```

También es necesario administrar la comunicación entre los hosts FHRP en el nivel L3. Hay cuatro routers FHRP configurados en una sola subred extendida en el diagrama. Sin algún grado de filtros L3, los cuatro routers se verían entre sí y elegirían un único dispositivo activo y tendrían 3 en varios estados de espera. Por lo tanto, un centro de datos tendría dos routers FHRP locales en espera pero no tendría conectividad L2 con el router activo remoto debido a los filtros L2 anteriormente mencionados.

El resultado deseado es tener un router FHRP activo y uno en espera en cada Data Center. El filtro L2 de entrada descrito anteriormente no detecta este tráfico de elección, ya que el proceso de elección utiliza las direcciones IP y MAC reales del router. De forma predeterminada, la ACL subsiguiente se aplica como salida en la interfaz de superposición. La salida de la interfaz de superposición sería tráfico hacia el núcleo de la WAN. La ACL no aparece en la configuración en ejecución, sin embargo, se puede observar con "show ip access-list". Filtra el tráfico de elección FHRP basado en el número de puerto UDP.

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

La única razón para inhabilitar este filtro sería si desea que todos los routers FHRP en una VLAN participen en la misma elección para el estado activo. Para inhabilitar este filtro, configure "no otv filter-fhrp" en la interfaz de superposición.

Tráfico unicast desconocido

De forma predeterminada, se descarta el tráfico de unidifusión recibido de la LAN por el router OTV destinado a una dirección MAC que no se conoce que existe en una ubicación OTV remota. Este tráfico se conoce como unidifusión desconocida. Esta acción de descarte se dirige al núcleo de la WAN, que limita la cantidad de ancho de banda consumido en la WAN por el tráfico de difusión. La expectativa general es que todos los hosts en la LAN emitan suficiente tráfico de broadcast (ARP, difusiones de protocolo, etc.) que siempre debe ser visto por un router OTV, anunciado y, por lo tanto, "conocido".

Ciertas aplicaciones aprovechan los hosts silenciosos. En una infraestructura de switching normal, esto no es un problema, ya que la transmisión L2 de direcciones MAC de unidifusión desconocidas en la LAN permite que el host silencioso vea el tráfico. Sin embargo, en un entorno OTV, el router OTV bloquea el tráfico entre los Data Centers.

Para compensar esto, se integró una función conocida como Reenvío selectivo de unidifusión en Cisco IOS® XE. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 y todas las versiones posteriores tienen soporte para el reenvío selectivo de unidifusión.

Se configura mediante la adición de un solo comando por dirección MAC en la interfaz de superposición. Por ejemplo:

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

Cualquier tráfico destinado a 0000.0001.0001 debe ser inundado a todos los routers OTV remotos con VLAN 100 en este ejemplo. Esto se puede observar mediante el comando subsiguiente:

<#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
```

Si esa dirección MAC se aprende en un sitio remoto, se debe agregar una entrada a la tabla de reenvío que tenga prioridad sobre la entrada de inundación.

<#root>

OTV_router_1#

show otv route

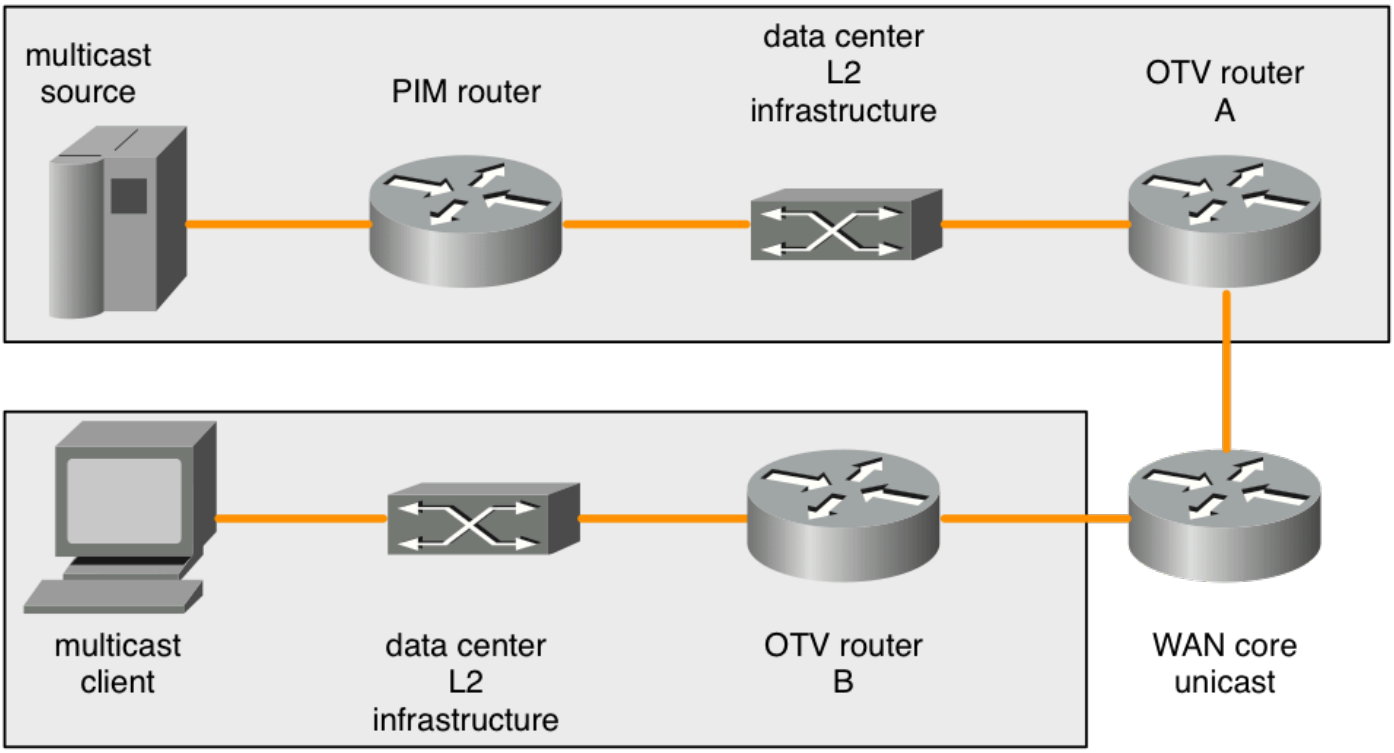
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV    Flood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

Por lo general, se debe configurar una entrada de inundación para una dirección MAC determinada en todos los routers OTV con esa VLAN.

Fuentes de multidifusión remota

ASR1000 que es un router OTV no reenvía solicitudes de unión IGMP multidifusión recibidas de la LAN. El siguiente diagrama detalla la topología donde esto puede ser un problema.

Figura 7 Orígenes de multidifusión remotos



Cuando el cliente de multidifusión envía una unión IGMP de multidifusión, el ASR1000 (router B de OTV) la observa y anuncia interés en el grupo de multidifusión. Los routers OTV remotos (router A OTV) deben reenviar todo el tráfico a ese grupo de multidifusión que vean en su dominio de difusión de L2 local. Sin embargo, el ASR1000 remoto (router A de OTV) no regenera las solicitudes de unión IGMP multidifusión cuando se anuncia el interés en un grupo multidifusión a partir del router OTV del cliente (router B de OTV).

Cuando los orígenes multicast están en el mismo dominio de broadcast L2 que el router OTV, esto no es un problema. El router OTV debe configurarse como solicitante IGMP. Esto aparece en cualquier tráfico multicast presente en el dominio de broadcast L2. Sin embargo, solo una solicitud de unión a PIM haría que un router PIM reenviara un origen de multidifusión desde un dominio de difusión L2 diferente al dominio de difusión L2 en el que se encuentra el router OTV.

La solicitud de unión IGMP remota no se reenvía ni se vuelve a generar. Los routers OTV tampoco son routers PIM. Por lo tanto, las topologías con orígenes de multidifusión que no se encuentran directamente en el dominio de difusión de L2 con el router OTV no tienen forma de informar a los routers PIM que reenvíen el tráfico de origen cuando un cliente remoto esté interesado.

Hay dos soluciones alternativas para este problema.

En primer lugar, se puede implementar un cliente IGMP local en el dominio de difusión L2 conectado al router OTV (router A OTV). Dicho cliente IGMP tendría que suscribirse a cualquier grupo de multidifusión al que se pudieran suscribir los clientes remotos. Esto haría que el router PIM reenviara el tráfico multicast al dominio de broadcast adyacente al router A de OTV. Las consultas IGMP entonces atraerían cualquier tráfico multicast y se enviarían a través de la superposición.

La otra solución sería configurar un "ip igmp static-join" para cualquier grupo al que los clientes

remotos pudieran suscribirse. Esto también haría que el router PIM reenviara el tráfico multicast al dominio de broadcast adyacente al router A de OTV.

Esta limitación es conocida y forma parte de la especificación de diseño. No se considera un bug, sino un límite en la topología soportada en este momento.

Consideraciones de QoS

De forma predeterminada en ASR 1000, el valor TOS del encabezado OTV agregado se copia de los bits 802.1p del paquete L2. Si el paquete L2 no está etiquetado, se utiliza un valor de cero.

Nexus 7000 tiene un comportamiento predeterminado diferente en el software 5.2.1 y las versiones más recientes. Si el comportamiento deseado es copiar el valor TOS de los paquetes internos en el router, la configuración de QoS adicional puede lograrlo. Esto ofrece el mismo comportamiento que el nuevo software Nexus 7000.

La configuración para copiar el valor TOS de L3 de los paquetes L2 en el encabezado más externo del paquete OTV es la siguiente:

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

La configuración proporcionada debe coincidir con el tráfico para varios valores DSCP en el ingreso. La etiqueta qos-group de importancia local se utiliza para marcar internamente ese tráfico durante el tránsito a través del router. En la interfaz de egreso, el grupo de QoS coincide y luego el byte TOS más externo se actualiza en consecuencia.

Consideraciones/fragmentación de MTU de WAN

OTV utiliza esencialmente un encabezado GRE para transportar el tráfico L2 a través de la WAN. Este encabezado GRE tiene un tamaño de 42 bytes. En una implementación de red ideal, el enlace WAN debe tener una unidad de transmisión máxima (MTU) que sea al menos 42 bytes mayor que el paquete más grande que se espera que maneje OTV.

Si la interfaz L2 tiene una MTU de 1500 bytes, la interfaz de unión debe tener una MTU de 1542 bytes o más. Si la interfaz L2 tiene una MTU de 2000 bytes, pero solo se espera que gestione paquetes de hasta 1500 bytes, entonces una MTU WAN de 1542 bytes es suficiente, sin embargo, la adición estándar de 42 a la 2000 sería 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
```

Algunos proveedores de servicios no pueden proporcionar valores de MTU mayores para sus circuitos WAN. En tal caso, ASR1000 puede fragmentar los datos transportados por OTV. Nexus 7000 no tiene esta capacidad. No se admiten redes OTV mixtas ASR1000 y Nexus 7000 con fragmentación habilitada en ASR1000.

La configuración para la fragmentación de OTV es:

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

Es importante que el comando global level se configure antes del comando Overlay interface join-

interface. Si el comando otv join-interface de la interfaz de superposición se configuró primero, quite el comando otv join-interface de la interfaz de superposición, configure el comando otv fragmentation join-interface y, a continuación, vuelva a configurar el comando otv join-interface de la interfaz de superposición.

Cuando la fragmentación OTV no está habilitada, todos los paquetes OTV que transportan datos L2 encapsulados se envían con el bit DF configurado para que no se fragmenten en tránsito. Una vez agregado el comando de fragmentación, el bit DF se establece en 0. Los routers OTV pueden fragmentar el paquete y otros routers pueden fragmentarlo en tránsito.

Hay una cantidad limitada de búferes de reensamblado de paquetes disponibles en las plataformas ASR1000, por lo que cuantos menos fragmentos se recorten en un paquete para la transmisión, mejor. Esto aumenta la eficacia y reduce el consumo general de ancho de banda en la WAN si esto supone un problema. Existen implicaciones de rendimiento para habilitar la fragmentación de OTV. Si existe fragmentación y se espera que se gestione más de 1 Gb/s de tráfico de OTV, se debe investigar más a fondo el rendimiento de OTV.

Topología de unidifusión de caso especial

Las implementaciones de campo para OTV suelen tener conexiones directas de fibra adosada entre los routers OTV de dos Data Centers.

En el caso de topologías de enlace único, se trata de una implementación estándar en la que el tráfico OTV y no OTV comparten la interfaz de unión. No se necesitan consideraciones especiales para esta configuración, por lo que esta sección no se aplica.

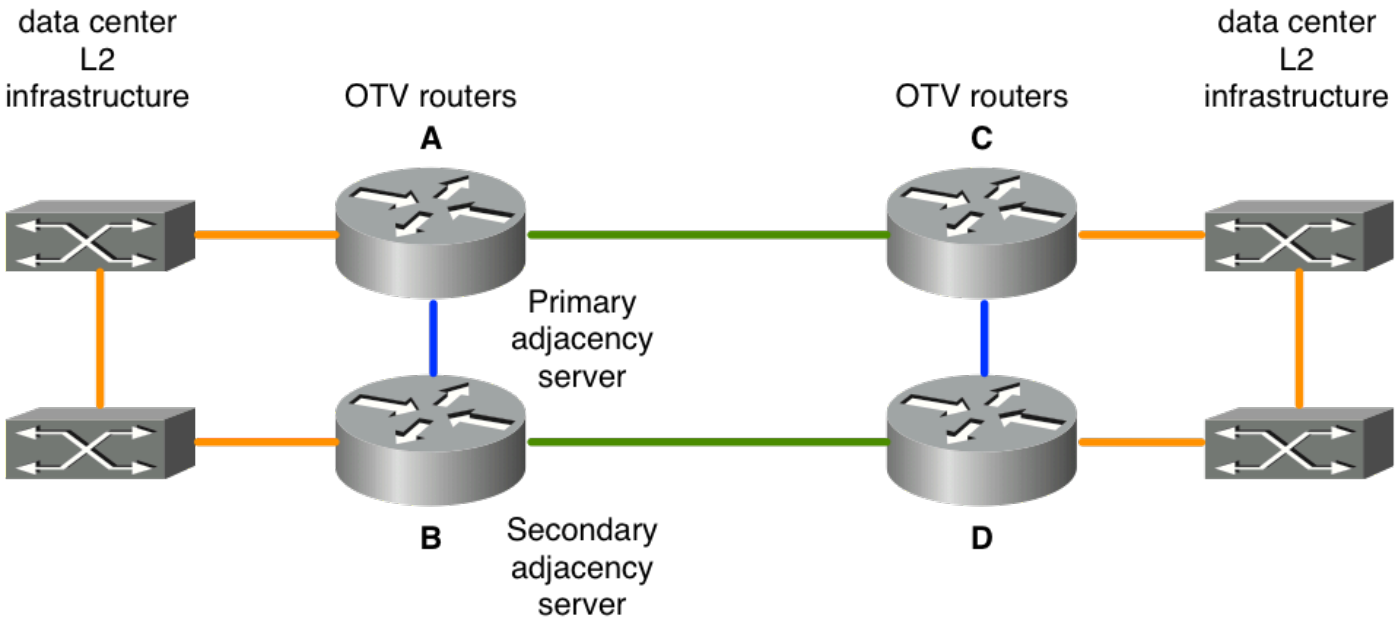
Sin embargo, si la implementación tiene routers OTV de varias conexiones en los dos Data Centers, hay algunas consideraciones especiales. Se requiere configuración adicional.

Si hay más de dos Data Centers involucrados, esta configuración especial no se aplica.

Para el escenario con más de dos Data Centers con routers OTV de uno o varios hosts, se debe utilizar una implementación OTV de unidifusión o multidifusión estándar.

No existe ninguna otra alternativa compatible.

Figura 8 Caso especial de unidifusión



En la topología presentada, los enlaces en verde son los enlaces de fibra oscura entre los dos Data Centers. Estas fibras oscuras están conectadas directamente a los routers OTV. Los links azules entre los routers OTV se utilizan para re-enrutar el tráfico no OTV en caso de falla de los links verdes. Si el link verde superior falla (A a C), el tráfico no OTV que utiliza los routers OTV superiores como su ruta predeterminada se enrutará a través de los links azules norte-sur (A a B y C a D) al link verde aún operativo entre el par de routers OTV inferiores (B a D).

Este reenrutamiento básico del tráfico no funciona para el tráfico de OTV porque la configuración de OTV especifica una interfaz física como interfaz de unión. Si la "interfaz verde" del router A de OTV deja de funcionar, el tráfico de OTV no se puede obtener de una interfaz alternativa del router B de OTV. Además, dado que no hay conectividad completa a través del núcleo WAN, no se puede informar a todos los routers OTV cuando se produce un error. Para evitar este problema, se utiliza la detección de reenvío bidireccional (BFD) junto con la secuencia de comandos integrada del administrador de eventos (EEM).

BFD debe supervisar el enlace WAN entre los pares de routers OTV este-oeste (A/C y B/D). Si se pierde la conexión con el router remoto, la interfaz de superposición de OTV se apaga mediante el script EEM en ese par este-oeste de routers OTV. Esto hace que el router multi-home emparejado asuma el reenvío para todas las VLAN. Cuando BFD detecta que el link se ha recuperado, el script EEM se dispara para volver a habilitar la interfaz de superposición.

Es muy importante que BFD se utilice para detectar fallas de link. Esto se debe a que la interfaz de superposición debe apagarse tanto en el lado "fallido" como en el par este-oeste. Dependiendo del tipo de conectividad proporcionada por el proveedor de servicios, un link físico puede caer (interfaz verde en el router A de OTV) mientras que la interfaz del par horizontal correspondiente del router puede permanecer activa (interfaz verde en el router C de OTV). BFD detecta la falla de cualquiera de las interfaces o cualquier otro problema en tránsito y notifica inmediatamente a ambos pares simultáneamente. Lo mismo se aplica cuando los routers necesitan ser informados del link de recuperación.

La configuración de esta implementación es la misma que la de cualquier otra implementación con la adición de los elementos siguientes:

- Configuración de BFD en la interfaz WAN
- el script EEM subsiguiente
- Identidad OTV ISIS para igualar la distribución VLAN par/impar

La configuración de BFD en la interfaz de unión de OTV está fuera del alcance de este documento. Puede encontrar información sobre cómo configurar BFD en ASR1000 en:

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

Una vez que la detección de fallas BFD esté funcionando correctamente entre los pares de interfaz de unión (links verdes en el diagrama), se debe implementar el script EEM. La secuencia de comandos EEM debe adaptarse a los routers específicos para modificar las interfaces Overlay correctas, así como para supervisar cadenas más exactas en el registro para detectar fallos BFD y recuperación.

```
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 ..."
!
```

Este tipo de implementación también requiere que los pares de router horizontal (A/C y B/D) coincidan en su reenvío de VLAN pares e impares.

Por ejemplo, A y C deben reenviar las VLAN pares mientras que B y D reenvían las VLAN impares en el funcionamiento nominal de estado estable.

La distribución impar / par se determina por el número ordinal de OTV que se puede observar con el comando "show otv site".

El número ordinal entre los dos routers de sitio se determina en función del ID de red de OTV ISIS.

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

El identificador de red OTV ISIS debe configurarse en todos los routers OTV. Se debe tener cuidado cuando se configura el identificador de manera que todos los routers OTV todavía se reconozcan entre sí.

<#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

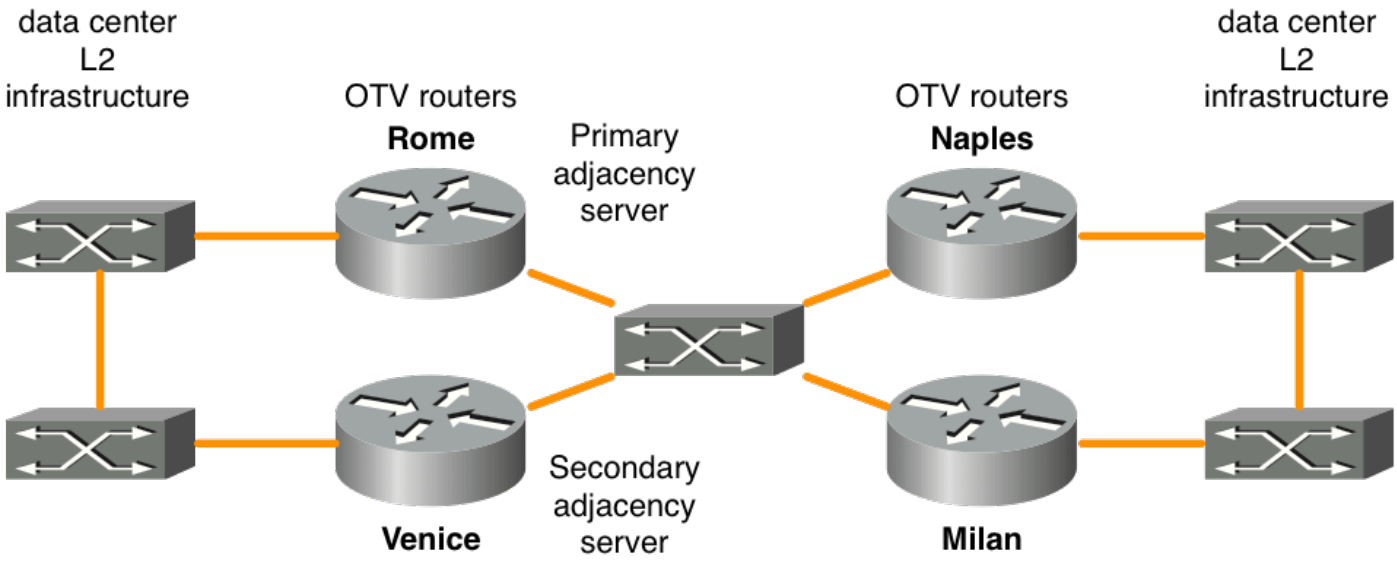
Las partes del identificador en negro deben coincidir en todos los routers OTV que participen en la

superposición. La parte del identificador en rojo se puede modificar. El identificador de red más bajo de un sitio obtiene el número ordinal 0 y, a su vez, reenvía las VLAN pares. El identificador de red más alto de un sitio obtiene el número ordinal 1 y reenvía el número impar de VLAN.

Ejemplos de Configuración

Unidifusión

Figura 9. Ejemplo de configuración de unidifusión



Configuración de Roma:

```
!
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
 !
```

Configuración de Venecia:

```
!
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
 !
```

Configuración de Nápoles:

```
!
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
```

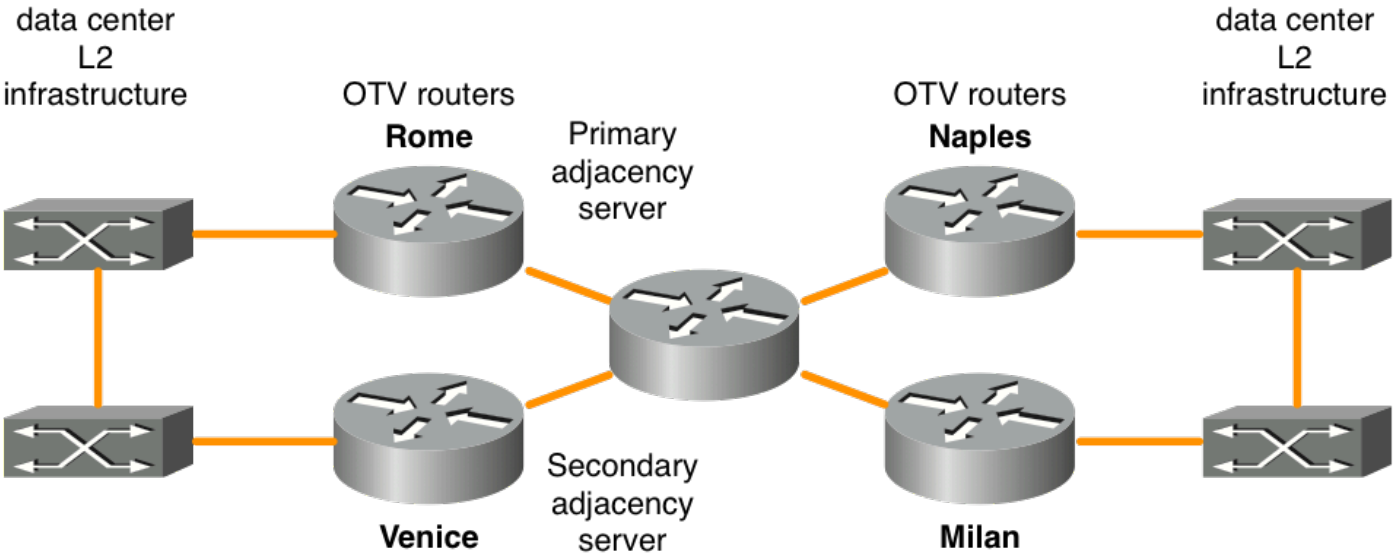
```
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Configuración de Milán:

```
!
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 (multidifusión)

Figura 10. Ejemplo de configuración de multidifusión



Configuración de Roma:

```
!
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
 !
```

Configuración de Venecia:

```
!
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
 !
```

Configuración de Nápoles:

```
!
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
 !
!
```

Configuración de Milán:

```
!
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
 !
!
```

Preguntas Frecuentes

P) ¿Se admiten las VLAN privadas junto con OTV?

R) Sí, se requiere una configuración no especial en OTV. En la configuración de VLAN privada, asegúrese de que los puertos del switch conectados a la interfaz L2 de OTV estén configurados en modo promiscuo.

P) ¿Es compatible OTV con IPSEC crypto?

R) Sí, se admite la configuración de mapa criptográfico en la interfaz de unión. No se requiere ninguna configuración especial para que OTV admita criptografía. Sin embargo, la configuración criptográfica agrega una sobrecarga adicional y esto debe compensarse con el aumento de la MTU de WAN frente a la MTU de LAN. Si esto no es posible, debe requerirse la fragmentación de OTV. El rendimiento de OTV se limita al del hardware IPSEC.

P) ¿MACSEC admite OTV?

R) Sí, ASR1001-X incluye compatibilidad con MACSEC para las interfaces integradas. OTV funciona con MACSEC configurado en las interfaces LAN o WAN. El rendimiento de OTV se limita al del hardware MACSEC.

P) ¿Se puede utilizar una interfaz de loopback como interfaz de unión?

R) No, solo se pueden utilizar interfaces Ethernet, Portchannels o POS como interfaces de unión OTV. La interfaz de unión de loopback de OTV está en la hoja de ruta, pero actualmente no está programada una versión en este momento.

P) ¿Se puede utilizar una interfaz de túnel como interfaz de unión?

R)No, los túneles GRE, los túneles DMVPN o cualquier otro tipo de túnel no se admiten como interfaces de unión. Solo se pueden utilizar interfaces Ethernet, Portchannels o POS como interfaces de unión de OTV.

P) ¿Pueden diferentes interfaces de superposición utilizar diferentes interfaces L2 y/o de unión?

R) Todas las interfaces de superposición deben apuntar a la misma interfaz de unión. Todas las superposiciones deben vincularse a la misma interfaz física para la conectividad de capa 2 con el Data Center.

P) ¿Puede la VLAN del sitio de OTV estar en una interfaz física diferente de las VLAN ampliadas de OTV?

R) La VLAN del sitio OTV y las VLAN extendidas deben estar en la misma interfaz física.

P) ¿Qué conjunto de funciones es necesario para OTV?

R) Se requieren servicios IP avanzados (AIS) o servicios empresariales avanzados (AES) para OTV.

P) ¿Se requiere una licencia independiente para OTV en plataformas de configuración fija?

R) No, siempre y cuando el ASR1000 se ejecute con el nivel de inicio de advipservices o adventerprise configurado, OTV estará disponible.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).