Configurar a virtualização de transporte de sobreposição com ASR 1000

Contents

Introdução

Este documento descreve as topologias de rede Overlay Transport Virtualization (OTV) suportadas nos roteadores das séries ASR1000 e Catalyst 8300/8500.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASR1000, IOS® XE versão 16.10.1a e posteriores
- Catalyst 8300, IOS® XE versão 17.5.1a e posteriores
- Catalyst 8500, IOS® XE versão 17.6.1a e posteriores

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O ASR1000 suporta OTV desde o Cisco IOS® XE Release 3.5. O roteador da série Catalyst 8300 começa o suporte com IOS® XE17.5.1a e as rotas da série Catalyst 8500 começam o suporte com IOS® XE versão 17.6.1a.

O OTV fornece conectividade de Camada 2 entre locais de rede remotos por roteamento baseado em endereço MAC e encaminhamento encapsulado por IP (MAC-in-IP) através de uma rede de transporte para fornecer suporte a aplicativos que exigem adjacência de Camada 2, como clusters e virtualização. O OTV usa um protocolo de plano de controle de sobreposição para aprender e propagar informações de roteamento MAC através da rede de sobreposição. O protocolo de plano de controle OTV usa mensagens IS-IS (Intermediate-System-to-Intermediate-System) para criar adjacências para sites remotos e enviar atualizações de rotas MAC para sites remotos. O OTV cria adjacências de Camada 2 para sites remotos na rede de sobreposição pela descoberta automática de dispositivos OTV remotos.

Os benefícios do OTV para a extensão da Camada 2 incluem:

- Sem requisito de MPLS
- Nenhuma configuração complexa de Ethernet sobre Multiprotocol Label Switching (EoMPLS) para malha
- Nenhuma implantação complexa de VPLS (Virtual Private LAN Services) para extensões de camada 2
- Isolamento de spanning tree nativo
    - não há necessidade de configurar explicitamente os filtros da unidade de protocolo de dados de bridge (BPDU)
    - isolamento padrão de problemas de spanning-tree para um determinado data center
- Isolamento de inundação de unicast desconhecido nativo
    - pacotes MAC unicast desconhecidos não são encaminhados
    - é permitido suporte para encaminhamento unicast desconhecido por MAC
- Otimização do Address Resolution Protocol (ARP) com o cache ARP OTV
    - reduz o tráfego de WAN desnecessário
- Provisionamento simplificado do isolamento do First Hop Redundancy Protocol (FHRP)
- Adição simplificada de locais
- Configuração de redundância simplificada
- Capacidade de ter um "dispositivo de drop-in" para migrações quando serviços temporários

são necessários

Requisitos

Os itens subsequentes são as regras principais a serem lembradas quando uma implantação de OTV é projetada. Se essas regras forem seguidas, o projeto e a implantação serão otimizados.

- Uma e somente uma interface pode ser usada para transmitir o tráfego encapsulado de OTV, conhecido como a interface de junção, para todas as interfaces de sobreposição de OTV configuradas
- Uma e somente uma interface pode ser usada para configurar as instâncias de serviço L2 do data center para a VLAN do local OTV e as VLANs estendidas entre os data centers para todas as interfaces de sobreposição OTV configuradas
- Os canais de porta podem ser usados para redundância de interface e conexão com switches VSS ou VPC e são suportados como a interface "única" para conectividade.
- Todos os roteadores OTV devem ser contatáveis através da interface de junção
- A árvore de abrangência deve ser configurada no roteador OTV que aponta para o data center
- O snooping e a consulta de IGMP devem ser configurados para encaminhar corretamente o tráfego de multicast do data center
- Um determinado data center pode ser configurado com 1 ou 2 roteadores OTV. Com dois roteadores, eles distribuem o encaminhamento de VLAN de forma ímpar/par com base no número da VLAN. Cada roteador OTV em um data center atua como um backup para o outro.
- Pares multihomed devem ser configurados com o mesmo identificador de site OTV
- O ASR1000/Catalyst 8300/Catalyst 8500 e o Nexus 7000 podem participar da mesma rede OTV
    - O Nexus 7000 não suporta fragmentação ou criptografia OTV, portanto esses recursos não podem ser usados em uma implantação "híbrida".

Há determinados projetos de conectividade back-to-back suportados que não seguem as regras declaradas. Embora essas configurações sejam suportadas, elas não são recomendadas. Detalhes sobre isso podem ser encontrados na seção posterior "Topologia unicast de caso especial".

Não é possível enfatizar suficientemente que o software OTV atual tem a restrição de interface "um e apenas um" ao configurar as interfaces de junção e de acesso L2 para OTV. Uma interface de canal de porta pode ser usada para redundância. A conexão do canal de porta para o Nexus 7000s em um VPC é suportada. Uma conexão port-channel básica para um único switch também é suportada.

Tipos de Implementação OTV

O OTV requer uma única interface de junção e uma única interface L2. Um e apenas um de cada um deles pode ser suportado por roteador OTV. O OTV também exige que uma VLAN de local seja configurada para que os roteadores OTV multihomed possam se comunicar entre si através

da rede local. Até mesmo os roteadores OTV single-homed devem ter a VLAN do local OTV configurada. Além disso, cada local ou data center deve ter um identificador de local exclusivo configurado. Os roteadores OTV dual-homed devem usar o mesmo identificador de site e ser capazes de se comunicar pela mesma VLAN.

A configuração subsequente fornece a configuração básica fundamental necessária para OTV. No entanto, ela não está completa, pois a configuração de núcleo unicast ou multicast deve ser adicionada. Eles são detalhados nas seções subsequentes deste 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
```

A configuração da instância de serviço é usada para todas as configurações de interface L2 com OTV.

Cada instância de serviço na interface L2 deve ser associada a um encapsulamento específico com uma ou duas marcas.

Por sua vez, cada uma dessas instâncias de serviço deve ser associada a um domínio de bridge.

Esse domínio de ponte é usado em uma instância de serviço configurada na interface de Sobreposição.

O domínio de ponte é a cola que vincula a instância do serviço de Sobreposição à instância do serviço de interface L2.

O encapsulamento do tráfego na interface de sobreposição deve corresponder ao encapsulamento do tráfego após o ingresso de regravação na interface L2.

No exemplo, o tráfego que entra na instância de serviço 99 Gig1/0/1 tem uma única VLAN 802.1Q de 99 e domínio de ponte 99. A instância de serviço correspondente com domínio de ponte 99 na interface de Sobreposição também é configurada para uma única VLAN 802.1Q de 99. Esse caso é o mais simples.

No exemplo, o tráfego que entra na instância de serviço Gig1/0/1 98 tem uma VLAN 802.1Q dupla de 99 e 1098 e domínio de bridge 90. A instância de serviço correspondente com domínio de bridge 90 na interface Overlay é configurada para uma única VLAN 802.1Q de 90. Claramente, elas não são iguais. O comando rewrite ingress garante que as marcas sejam convertidas corretamente à medida que o tráfego se move pela interface de entrada. O tráfego que entra na interface L2 tem as VLANs 802.1Q 98/1098 substituídas por uma única VLAN 90. A palavra-chave simétrica garante que o tráfego que sai da interface L2 tenha a VLAN 802.1Q única 90 substituída por 98/1098.

Qualquer instância de serviço com várias VLANs 802.1Q estendidas por OTV deve usar o comando rewrite ingress. O encapsulamento OTV suporta apenas um único identificador de VLAN. Por esse motivo, qualquer configuração de VLAN dupla nas interfaces L2 deve ser regravada em uma única marca na instância do serviço de interface de Sobreposição. Isso impede o suporte para configurações VLAN ambíguas.

Para obter mais detalhes sobre a regravação de marcas, consulte este documento: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

Neste exemplo, o domínio de ponte do site OTV é 100.

- O domínio de ponte do site OTV é configurado somente na interface L2.
- O domínio de ponte do site OTV nunca deve ser configurado na interface Overlay, pois isso torna a implantação de OTV instável.
- A VLAN do local OTV deve ser conectada somente aos roteadores OTV e não deve transportar nenhum outro tráfego de usuário/data center.
- A VLAN do local OTV deve estar na mesma interface física que as VLANs estendidas OTV.

Multihome

Um data center pode ser conectado com um único host OTV ou até 2 para redundância, também conhecido como Multihome. Multihome é usado para resiliência e balanceamento de carga. Quando mais de um dispositivo de borda está presente em um local e ambos participam da mesma rede de sobreposição, o local é considerado multihomed. O OTV Multihome divide as VLANs entre os dois roteadores OTV que pertencem ao mesmo local de forma ímpar/par com base no número da VLAN. Um dispositivo de borda é eleito como o AED para todas as VLANs ímpares, enquanto o outro roteador OTV é eleito como o AED para todas as VLANs pares. Cada AED também é um standby para as VLANs que estão ativas no outro roteador. Em caso de falha de link ou nó em um dos AEDs, o AED em standby se torna ativo para todas as VLANs.

Se dois ASR1000s estiverem conectados no mesmo data center para fazer Multihome, não

haverá necessidade de um link dedicado entre os dois ASR1000s. O OTV usa a VLAN do local OTV que é propagada através da interface interna e da comunicação através da interface de junção para determinar quais roteadores são responsáveis por VLANs pares e ímpares.

Os ASR1000s e Nexus 7000s não podem ser misturados no mesmo data center com OTV configurado em ambos os roteadores como backup para o outro. Multihome em um determinado data center é suportado para plataformas correspondentes (ASR1000 ou Nexus 7000). Você pode ter ASR1000s em um data center e Nexus 7000s em outro. A interoperabilidade entre essas duas plataformas foi testada e suportada. Alguns data centers podem ser multihomed, enquanto outros são single homed.

Os pares de roteadores ASR1000 multihomed devem executar a mesma versão do software Cisco IOS® XE.

Se o Multihome for usado, é altamente recomendável que o spanning-tree esteja ativado nos roteadores OTV, pois isso permite que o roteador OTV envie uma notificação de alteração de topologia (TCN) que faz com que o dispositivo de switch L2 adjacente (juntamente com outros switches na spanning-tree) reduza seu temporizador de idade do padrão para 15 segundos. Isso aumenta muito a convergência de velocidade quando há uma falha ou recuperação entre o par multihomed. A árvore de abrangência pode ser ativada para todas as instâncias de serviço configuradas (conectadas ao OTV ou de outra forma) pela adição da linha subsequente à configuração global.

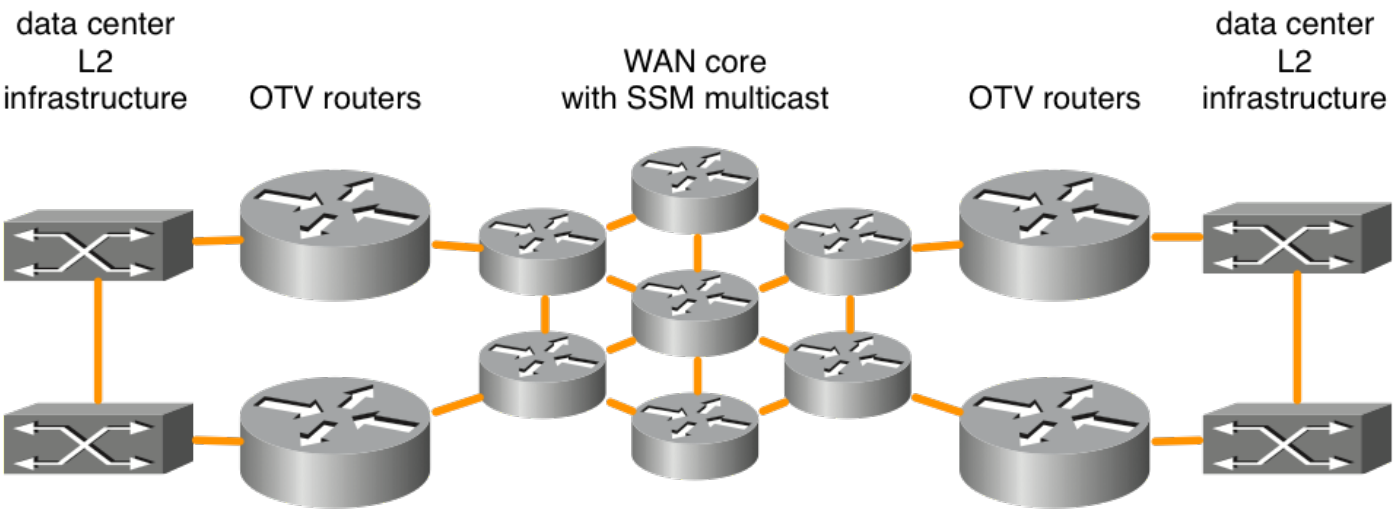
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

Nenhuma configuração específica por vlan ou por instância de serviço é necessária.

Núcleo Multicast

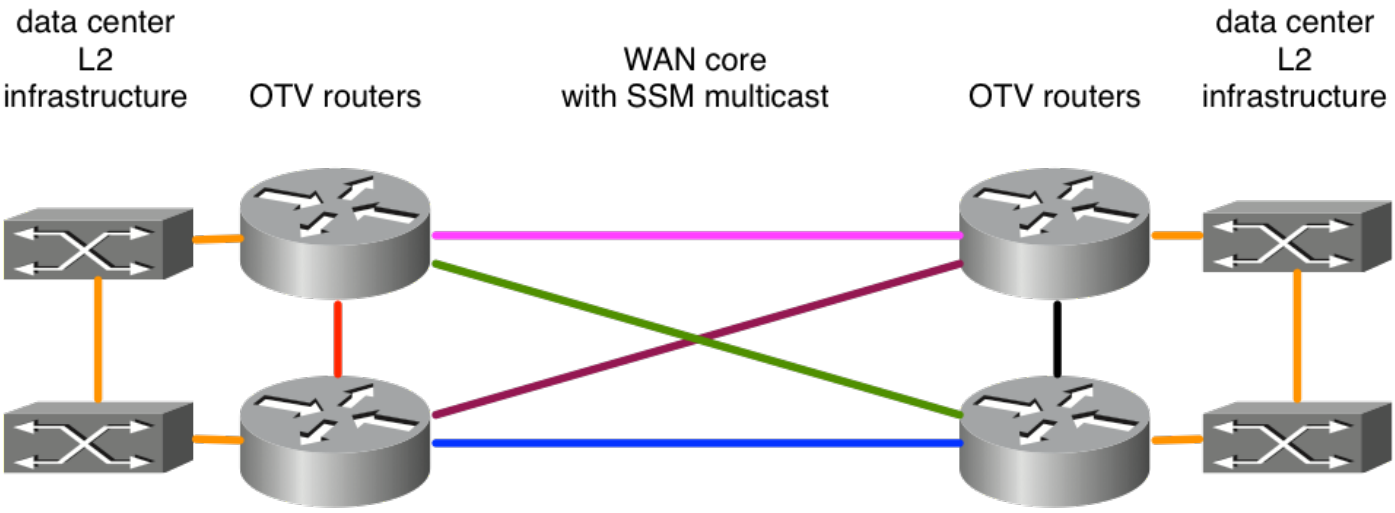
A rede multicast exige conectividade de malha completa através da WAN. Todos os roteadores OTV precisam estar conectados através da interface de junção.

Figura 1. Topologia de rede multicast suportada



Esta figura mostra um exemplo de dois data centers que estão conectados através de um núcleo em malha completa. O Protocol Independent Multicast (PIM) do Source Specific Multicast (SSM) é executado entre os roteadores OTV e os roteadores de núcleo da WAN. Qualquer número de roteadores de núcleo é suportado desde que haja conectividade de malha completa. Não há nenhum requisito explícito de latência máxima para a conectividade OTV no núcleo da WAN.

Figura 2. Topologia de rede multicast sem suporte



Como o ASR1000/OTV espera receber mensagens multicast em uma única interface de junção de todos os seus peers, por exemplo, isso resultaria em uma implantação de OTV instável. Suponha que os links leste-oeste em rosa e azul foram configurados como interfaces de junção. Quando o link rosa falhar, o roteador não poderá mais receber atualizações de OTV nessa interface. Um caminho alternativo através dos links verdes ou roxos seria inaceitável porque a interface de junção está configurada explicitamente. As atualizações devem ser recebidas nessa interface. No momento, não há suporte para o uso de interfaces Loopback como a interface de junção.

Se os usuários não possuírem seu backbone, eles deverão se certificar de que seu provedor de serviços suporta multicast em seu núcleo, e o provedor de serviços pode responder a mensagens de consulta do Internet Group Management Protocol (IGMP). O OTV no ASR1000 atua como host multicast (encaminha mensagens de junção IGMP), não como um roteador multicast para a

topologia de multicast da WAN central.

A rede de transporte entre os roteadores OTV deve suportar o modo esparso de PIM (Any Source Multicast [ASM]) para o grupo multicast do provedor e SSM para o grupo de entrega.

Os núcleos multicast exigem alguma configuração específica na interface Overlay para um grupo de controle, bem como uma gama de grupos multicast de dados que são usados para encaminhar dados.

```
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
```

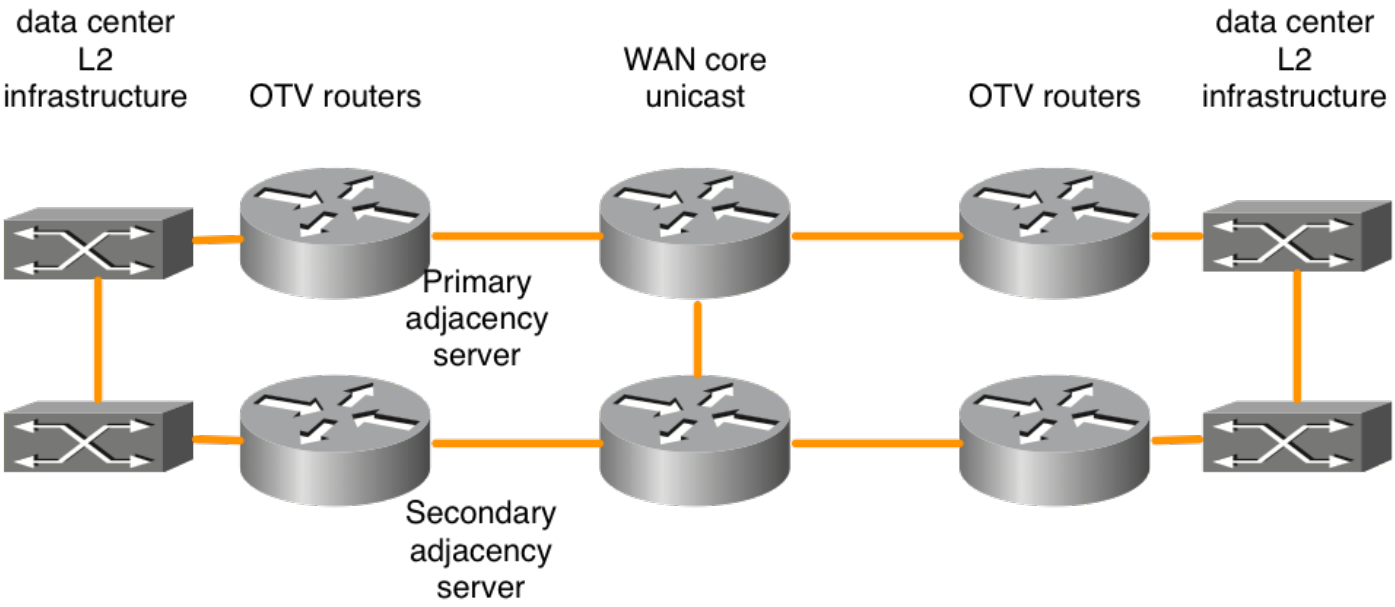
As implantações de OTV multicast exigem que a interface de junção seja configurada como uma interface passiva PIM. O IGMP pode ser configurado para diferentes versões conforme necessário. A interface de sobreposição deve ter grupos de controle e de dados configurados. O grupo de controle é um único grupo multicast usado para gerenciamento de OTV. O grupo de dados é um intervalo de endereços multicast usados para transportar dados de usuários entre data centers. Se o grupo de dados não estiver no espaço IP 232.0.0.0/8, o comando adicional "ip pim ssm range" deverá ser configurado para incluir o intervalo exigido pelo OTV.

A rede de transporte entre os roteadores OTV deve suportar o modo esparso de PIM (Any Source Multicast [ASM]) para o grupo multicast do provedor e Source Specific Multicast (SSM) para o grupo de entrega.

Núcleo Unicast com Servidores Adjacentes

O Cisco IOS® XE 3.9 adicionou suporte para OTV com um núcleo unicast. Os núcleos unicast e multicast para OTV continuam a ser suportados para todas as plataformas ASR1000 e versões futuras do Cisco IOS® XE 3.9.

Figura 3. Topologia de rede Unicast



O recurso OTV Adjacency Server permite o transporte somente unicast entre a borda OTV. Os roteadores OTV configurados com a função de servidor de adjacência mantêm uma lista de todos os roteadores OTV conhecidos. Eles fornecem essa lista a todos os roteadores OTV registrados para que tenham uma lista de dispositivos que devem receber tráfego de broadcast e multicast replicado.

O plano de controle OTV sobre um transporte somente unicast funciona exatamente da mesma maneira que o OTV com núcleo multicast, exceto que em uma rede de núcleo unicast, cada dispositivo de borda OTV precisa criar várias cópias de cada pacote de plano de controle e enviá-las por unicast para cada dispositivo de borda remoto na mesma sobreposição lógica.

Na mesma linha de raciocínio, qualquer tráfego multicast do data center é replicado no roteador OTV local e várias cópias são enviadas a cada um dos data centers remotos. Embora isso seja menos eficiente do que ser contingente no núcleo da WAN para fazer a replicação, a configuração e o gerenciamento da rede multicast do núcleo não são necessários. Se houver apenas uma pequena quantidade de tráfego multicast de data center ou apenas um pequeno número de locais de data center (quatro ou menos), um núcleo unicast para encaminhamento OTV é geralmente a melhor opção. No geral, a simplificação operacional do modelo somente unicast torna a opção de implantação do núcleo unicast preferida em cenários onde a conectividade de extensão de LAN é necessária apenas entre quatro ou menos data centers. É recomendável ter pelo menos dois servidores de adjacência configurados, um principal e um de backup. Não há uma opção para a configuração do servidor de adjacência ativo/ativo.

Os roteadores OTV devem ser configurados de acordo para identificar e registrar adequadamente com o servidor de adjacência apropriado.

	Servidor de adjacência primário	Servidor de adjacência secundário	Outros roteadores OTV
Endereço IP da	10.0.0.1	10.2.2.24	outros endereços IP

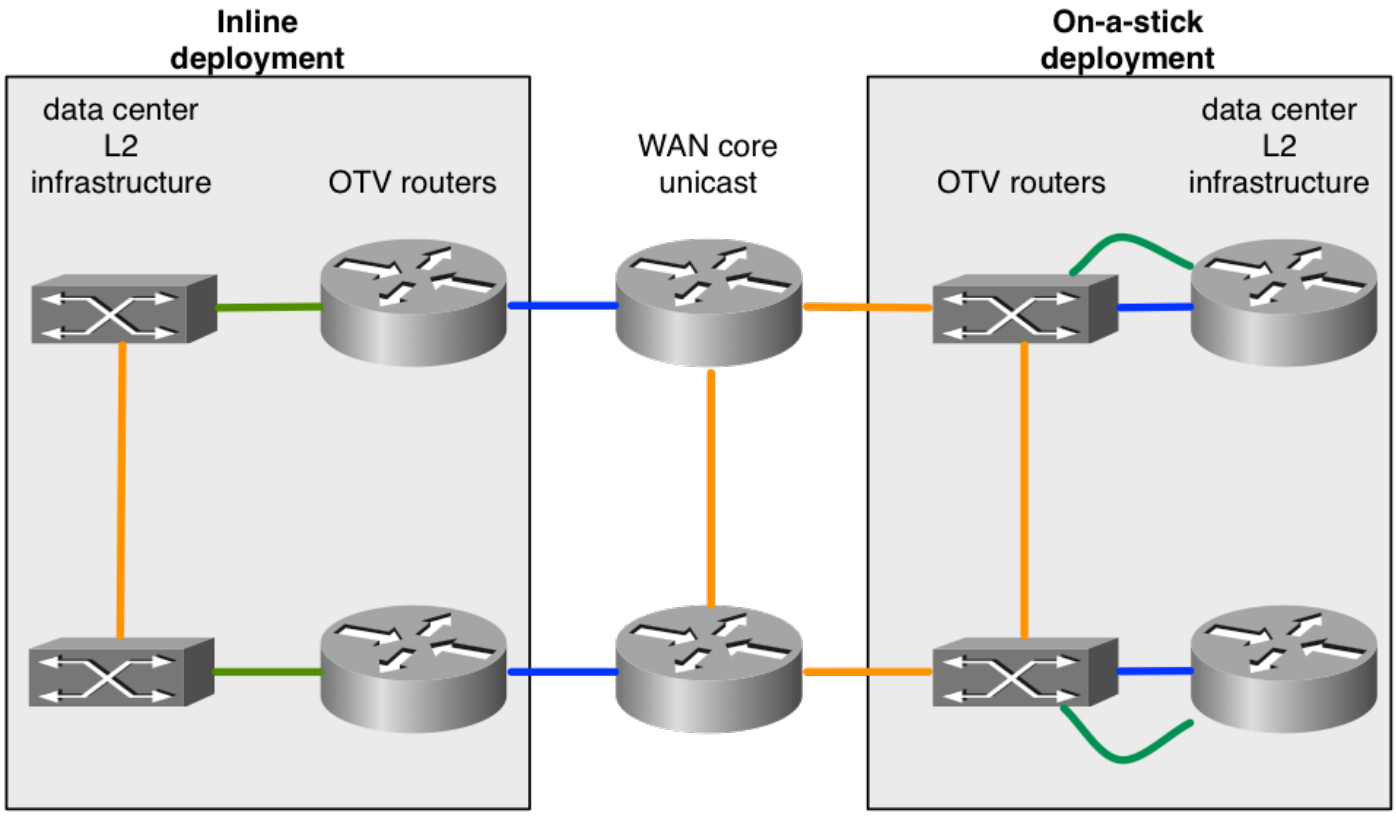
	Servidor de adjacência primário	Servidor de adjacência secundário	Outros roteadores OTV
interface de ingresso OTV			
Configuração	interface Overlay 1 otv adjacency-server unicast-only	interface Overlay 1 otv adjacency-server unicast-only otv use-adjacency-server 10.0.0.1 unicast-only	interface Overlay 1 otv use-adjacency-server 10.0.0.1 10.2.2.24 unicast-only

Há certos designs para conectividade back-to-back que são suportados com encaminhamento de OTV unicast que não seguem as regras de "malha completa". Embora essas configurações sejam suportadas, elas não são recomendadas. Esse tipo de implantação é mais comum quando os data centers estão conectados por fibra escura. Detalhes sobre essa opção de configuração podem ser encontrados na seção posterior "Topologia unicast de caso especial".

OTV em um bastão versus em linha

Há dois modelos para implantar o OTV em seu data center: em um stick e em linha. Nos cenários de projeto apresentados anteriormente, os roteadores OTV estavam em linha entre o data center e a rede central do provedor de serviços. No entanto, a adição do roteador OTV como um dispositivo que não está no caminho de transporte de todo o tráfego poderia ser mais desejável. Às vezes, o requisito é não alterar a topologia atual para conectar-se ao provedor de serviços por meio do equipamento atual (por exemplo, uma implantação em áreas industriais com switch Catalyst 6000 ou hardware de switch Nexus que não suporte OTV). Portanto, é preferível implantar OTV no ASR1000 como um dispositivo OTV.

Figura 4. Topologia em linha versus on-a-stick



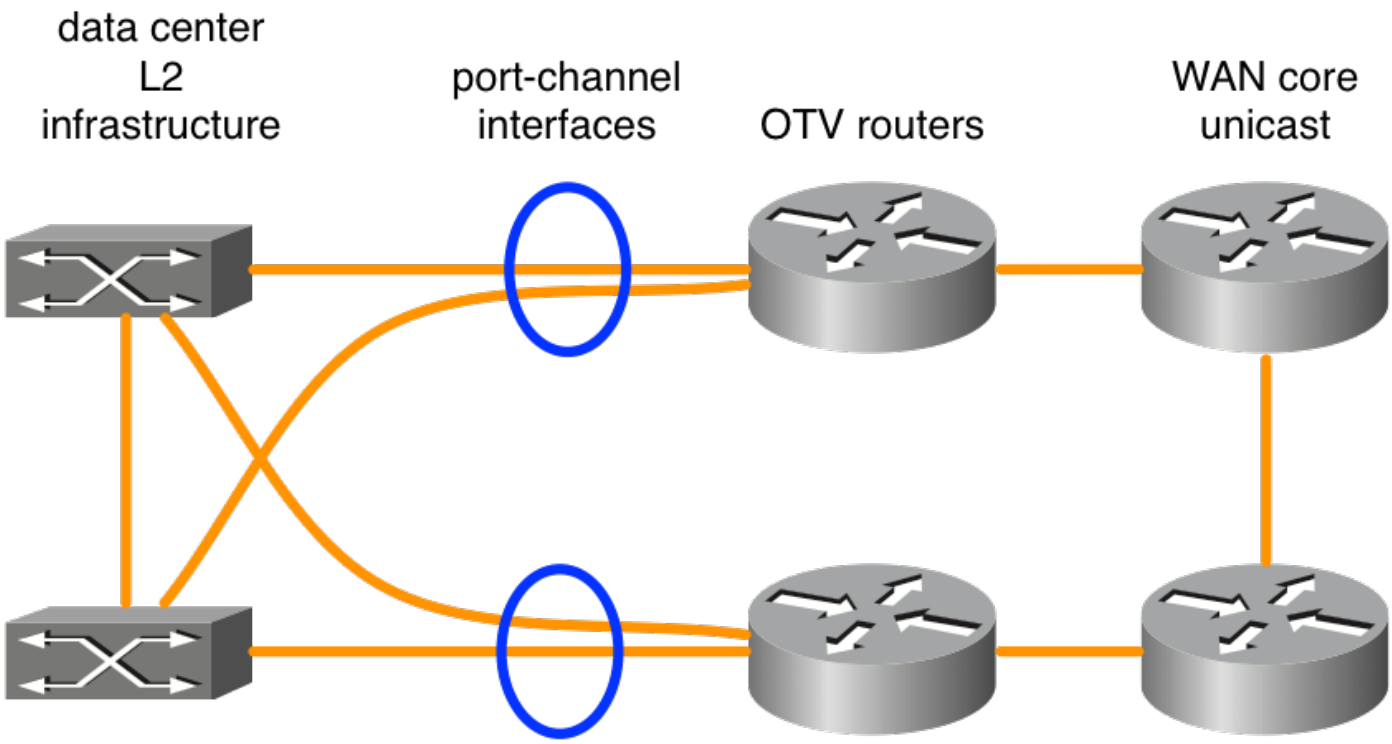
O diagrama demonstra os dois modelos de implantação que podem fazer parte da mesma sobreposição. Os links verdes conectados aos roteadores OTV são configurados como interfaces de acesso L2 para aceitar tráfego VLAN. Os links azuis conectados aos roteadores OTV são as interfaces de junção que transportam o tráfego VLAN encapsulado OTV.

Pode ser necessário configurar um recurso que não seja suportado com OTV. Por exemplo, OTV e MPLS não podem ser configurados na mesma caixa. Como resultado, pode ser uma boa opção usar ASR1000/OTV em um stick e configurar MPLS no roteador que fica na frente do roteador OTV.

Canais de porta para Camada 2 e Camada 3

O código do Cisco IOS® XE 3.10 para ASR1000 adicionou suporte à configuração de canal de porta da camada 2 e da camada 3 com OTV. O canal de porta da camada 2 pode ser usado como a interface interna. O canal de porta deve consistir em até 4 interfaces físicas. O canal de porta da camada 3 pode ser usado como a interface de junção.

Figura 5. Canais de porta usados para conectividade L2



O diagrama mostra um cenário típico de canal de porta com dois switches em VSS (série Catalyst 6000) ou VPC (série Nexus 7000). Esse tipo de design oferece redundância com roteadores OTV duplos e conectividade dupla para a infraestrutura do data center. Nenhuma configuração especial para OTV além da configuração básica de canal de porta é necessária se VSS ou VPC for usado em equipamentos de switching L2 adjacentes aos roteadores OTV.

Gateway padrão

Por definição, o OTV cria a mesma sub-rede L3 em vários locais. Isso exige algumas considerações especiais ao rotear o tráfego de L3 de e para as VLANs estendidas. O roteamento L3 pode ser configurado nos próprios roteadores OTV ou pode ser configurado em outros dispositivos conectados às VLANs estendidas. Além disso, em cada cenário, os protocolos de redundância de primeiro salto (FHRP), como o Hot Standby Redundancy Protocol (HSRP) ou o Virtual Router Redundancy Protocol (VRRP), podem ser implantados para fins de redundância. O HSRP pode ser executado localmente em um determinado data center ou pode se estender entre data centers (não típico).

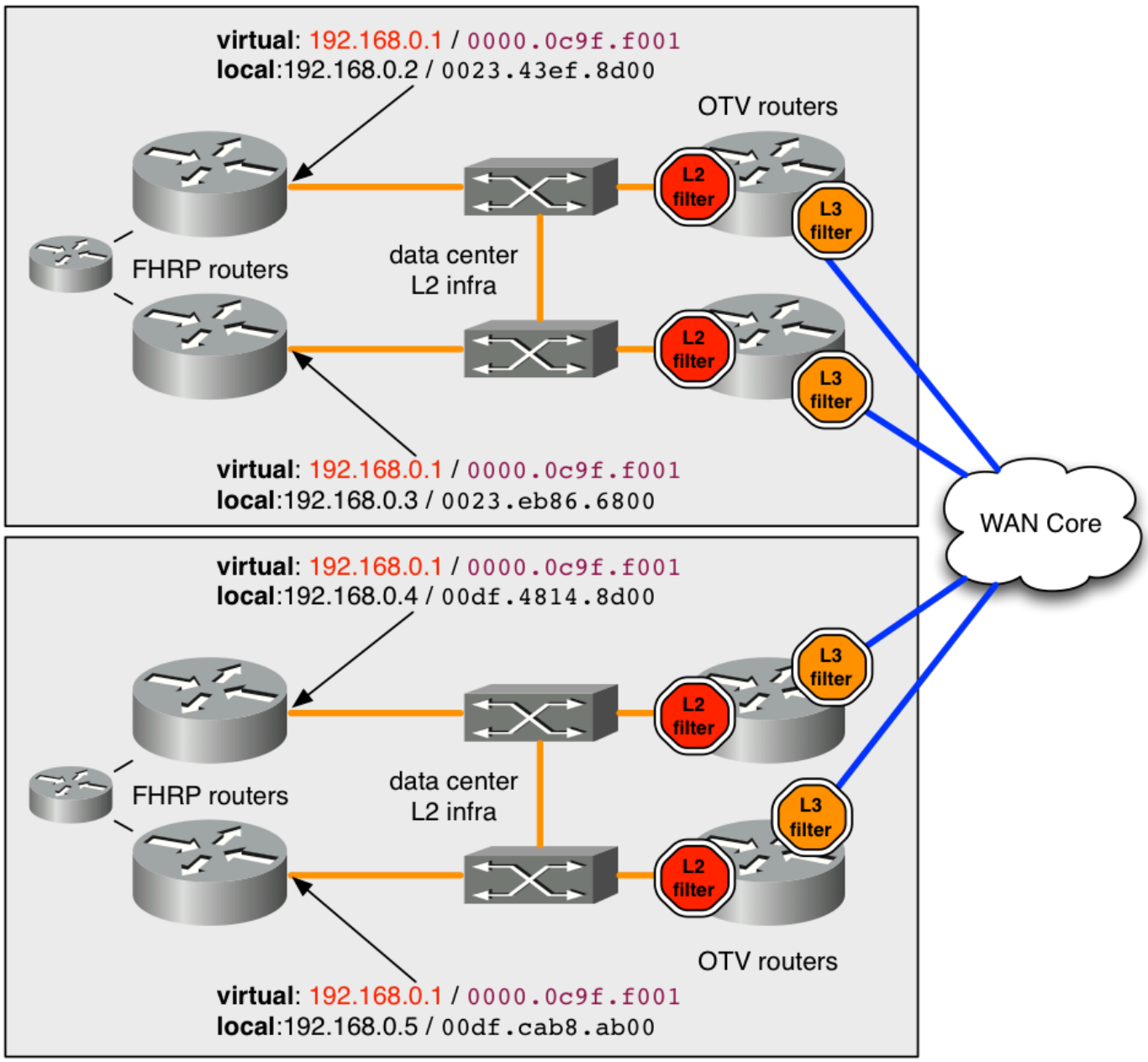
A prática recomendada para implantações de OTV que utilizam FHRP é ter instâncias locais do FHRP em execução em cada data center. Essas instâncias de FHRP utilizam o mesmo endereço MAC virtual e endereço IP para que, quando as máquinas virtuais (VMs) se moverem entre os data centers, elas tenham uma conexão ininterrupta. Se o endereço MAC do roteador padrão mudasse entre os data centers, as VMs não seriam capazes de se comunicar fora da sub-rede até que a entrada ARP do gateway padrão da VM atingisse o tempo limite.

Para implantar corretamente um FHRP com OTV, é necessário considerar qual tráfego L2 e L3 deve ser filtrado e isolado do OTV. No nível L2, isso é necessário para manter o OTV fora de vista direta do mesmo MAC virtual L2 usado pelo FHRP em vários locais. Os filtros são necessários no nível L3 para manter os anúncios de HSRP e VRRP isolados em cada data center, de modo que

a escolha ativa/de escuta/espera seja localizada em cada data center.

Por padrão, os filtros de FHRP são ativados quando o OTV é ativado. Ele pode ser desativado se o design exigir que o FHRP seja estendido entre os data centers. A filtragem L2 de endereços MAC virtuais NÃO é habilitada por padrão e deve ser configurada manualmente.

figura 6. Exemplo de implantação recomendada para FHRP



No exemplo, o endereço MAC virtual 0000.0c9f.f001 é usado para o endereço IP 192.168.0.1 que hospeda na VLAN estendida para conectividade fora da sub-rede. Com o uso do mesmo MAC virtual e IP em ambos os data centers, um host tem conectividade contínua fora da sub-rede quando transfere entre os data centers.

Para manter o endereço MAC 0000.0c9f.f001 oculto do OTV em vários locais, um filtro L2 de entrada (parada vermelha no diagrama) deve ser implantado para a VLAN em cada um dos roteadores OTV , que atendem à VLAN. Pelo filtro de ACL, a ACL de filtro configurada nas instâncias de serviço L2 para entrada, todos os pacotes originados desse MAC são descartados

antes que o processo OTV no ASR1000 possa vê-los. Assim, o OTV nunca aprende sobre o MAC e não o anuncia aos data centers remotos.

A configuração recomendada para capturar todo o tráfego MAC virtual FHRP conhecido/padrão é fornecida aqui.

```
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
```

Essa ACL corresponde aos espaços de endereço MAC bem conhecidos associados às versões 1 e 2 do HSRP, ao Gateway Load Balancing Protocol (GLBP) e ao VRRP (nessa ordem) . Se o MAC virtual for configurado para usar um valor fora do padrão não baseado no número de grupo FHRP, ele deverá ser explicitamente adicionado ao exemplo da ACL. A ACL deve ser adicionada à instância do serviço L2 (mostrada aqui).

```
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
```

Também é necessário gerenciar a comunicação entre os hosts FHRP no nível L3. Há quatro roteadores FHRP configurados em uma única sub-rede estendida no diagrama. Sem um certo grau de Filtros L3, os quatro roteadores se veriam e elegeriam um único dispositivo ativo e teriam 3 em vários estados de standby. Assim, um data center teria dois roteadores FHRP em standby local, mas não teria conectividade de L2 com o roteador ativo remoto devido aos Filtros de L2 discutidos anteriormente.

O resultado desejado é ter um roteador FHRP ativo e um roteador FHRP em standby em cada data center. O filtro de entrada L2 discutido anteriormente não detecta esse tráfego de eleição, já que o processo de eleição usa os endereços IP e MAC reais do roteador. Por padrão, a ACL subsequente é aplicada como saída na interface de Sobreposição. A saída para a interface de sobreposição seria o tráfego em direção ao núcleo da WAN. A ACL não aparece na configuração de execução, no entanto, ela pode ser observada com "show ip access-list". Ele filtra o tráfego de eleição de FHRP com base no número da porta 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
```

A única razão para desabilitar esse filtro seria se você quisesse que todos os roteadores FHRP em uma VLAN participassem da mesma eleição para status ativo. Para desabilitar esse filtro, configure "no otv filter-fhrp" na interface de Sobreposição.

Tráfego de unicast desconhecido

Por padrão, o tráfego unicast recebido da LAN pelo roteador OTV destinado a um endereço MAC que não existe em um local OTV remoto é descartado. Esse tráfego é conhecido como unicast desconhecido. Essa ação de queda vai em direção ao núcleo da WAN que limita a quantidade de largura de banda consumida na WAN pelo tráfego de broadcast. A expectativa geral é que todos os hosts na LAN emitam tráfego de broadcast suficiente (ARPs, broadcasts de protocolo, etc.) que sempre deve ser visto por um roteador OTV, anunciado e, portanto, "conhecido".

Determinados aplicativos aproveitam os hosts silenciosos. Em uma infraestrutura de switching normal, isso não é um problema, pois a transmissão L2 de endereços MAC unicast desconhecidos na LAN permite que o host silencioso veja o tráfego. No entanto, em um ambiente OTV, o roteador OTV bloqueia o tráfego entre os data centers.

Para compensar isso, um recurso conhecido como Encaminhamento Unicast Seletivo foi integrado ao Cisco IOS® XE. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 e todas as versões depois têm suporte para encaminhamento unicast seletivo.

Ele é configurado pela adição de um único comando por endereço MAC na interface de sobreposição. Por exemplo:

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

Qualquer tráfego destinado a 0000.0001.0001 deve ser enviado a todos os roteadores OTV remotos com VLAN 100 neste exemplo. Isso pode ser observado pelo comando subsequente:

<#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
```

Se esse endereço MAC for aprendido em um local remoto, uma entrada deverá ser adicionada à tabela de encaminhamento que tem precedência sobre a entrada de inundação.

<#root>

```
OTV_router_1#
```

show otv route

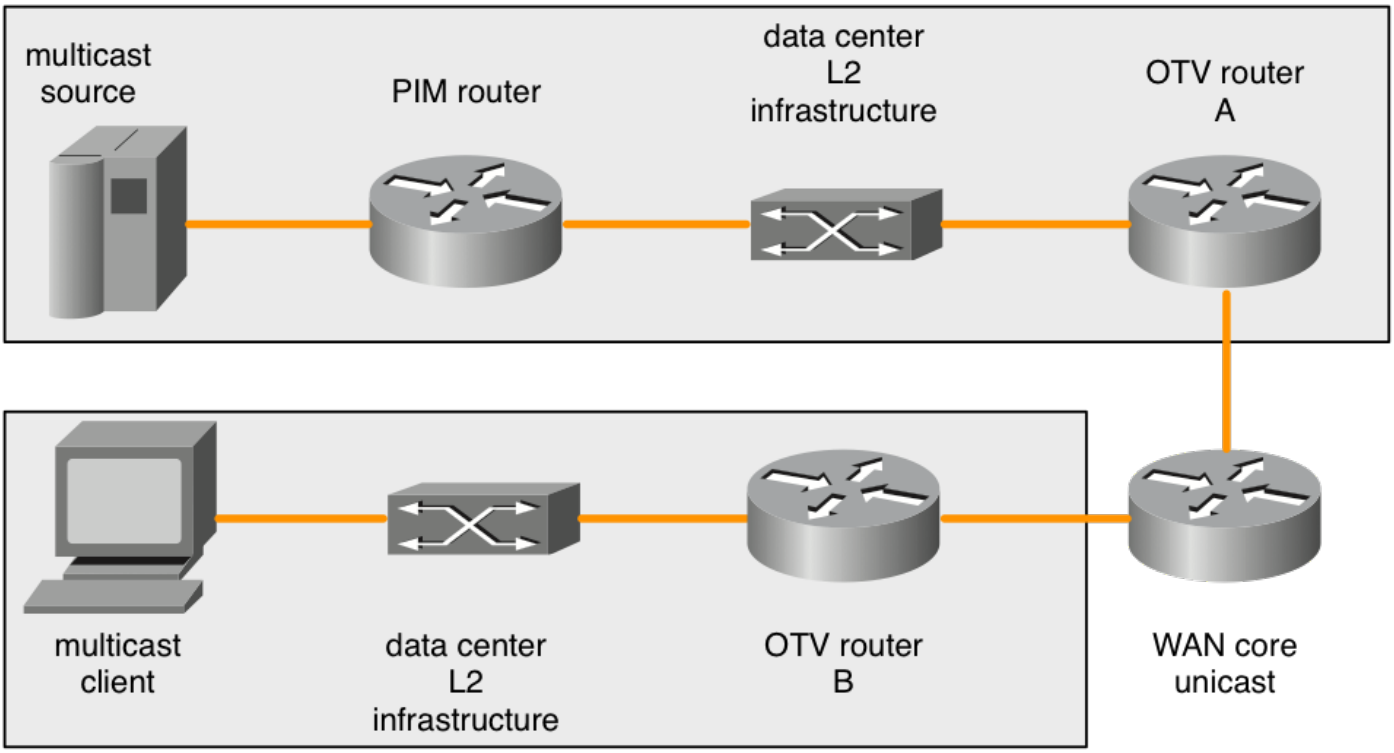
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-------------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV  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

Geralmente, uma entrada de inundação para um determinado endereço MAC deve ser configurada em todos os roteadores OTV com essa VLAN.

Origens de Multicast Remoto

O ASR1000 indica que um roteador OTV não encaminha solicitações de junção IGMP multicast recebidas da LAN. O diagrama subsequente detalha a topologia onde isso pode ser um problema.

Figura 7. Origens de multicast remoto



Quando uma junção IGMP multicast é enviada pelo cliente multicast, o ASR1000 (roteador B OTV) a observa e anuncia o interesse no grupo multicast. Os roteadores OTV remotos (roteador A OTV) devem encaminhar todo o tráfego para esse grupo multicast que eles veem em seu domínio de broadcast L2 local. O ASR1000 remoto (roteador A OTV), no entanto, não regenera as solicitações de junção de IGMP multicast quando o interesse em um grupo multicast é anunciado do roteador OTV do cliente (roteador B OTV).

Quando as origens de multicast estão no mesmo domínio de broadcast L2 que o roteador OTV, isso não é um problema. O roteador OTV deve ser configurado como um consultante IGMP. Isso aparece em qualquer tráfego multicast presente no domínio de broadcast L2. No entanto, apenas uma solicitação de junção PIM faria com que um roteador PIM encaminhasse uma origem de multicast de um domínio de broadcast L2 diferente para o domínio de broadcast L2 em que o roteador OTV está.

A solicitação de junção IGMP remota não é encaminhada ou gerada novamente. Os roteadores OTV também não são roteadores PIM. Portanto, as topologias com origens de multicast não diretamente no domínio de broadcast L2 com o roteador OTV não têm como informar os roteadores PIM para encaminhar o tráfego de origem quando há interesse por um cliente remoto.

Há duas soluções para esse problema.

Primeiro, um cliente IGMP local pode ser implantado no domínio de broadcast L2 conectado ao roteador OTV (roteador A OTV). Esse cliente IGMP teria que se inscrever em qualquer grupo multicast no qual os clientes remotos pudessem se inscrever. Isso faria com que o roteador PIM encaminhasse o tráfego multicast para o domínio de broadcast adjacente ao roteador A do OTV. As consultas de IGMP seriam desenhadas em qualquer tráfego de multicast e seriam enviadas através da sobreposição.

A outra solução seria configurar uma "ip igmp static-join" para quaisquer grupos nos quais os

clientes remotos possam se inscrever. Isso também faria com que o roteador PIM encaminhasse o tráfego multicast para o domínio de broadcast adjacente ao roteador A do OTV.

Essa limitação é conhecida e faz parte da especificação do projeto. No momento, não é considerado um bug, mas um limite na topologia suportada.

Configurações de QoS

Por padrão no ASR1000, o valor TOS no cabeçalho OTV adicionado é copiado dos bits 802.1p do pacote L2. Se o pacote L2 não estiver marcado, o valor zero será usado.

O Nexus 7000 tem um comportamento padrão diferente no software 5.2.1 e mais recente. Se o comportamento desejado for copiar o valor TOS dos pacotes internos para o roteador, uma configuração adicional de QoS pode conseguir isso. Isso gera o mesmo comportamento do software Nexus 7000 mais recente.

A configuração para copiar o valor de TOS de L3 dos pacotes de L2 no cabeçalho mais externo do pacote de OTV é a subsequente:

```
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
```

A configuração fornecida deve corresponder ao tráfego para vários valores de DSCP no ingresso. A tag qos-group localmente significativa é usada para marcar internamente esse tráfego durante o trânsito pelo roteador. Na interface de saída, o qos-group é correspondido e o byte TOS mais externo é atualizado de acordo.

Considerações/Fragmentação de WAN MTU

O OTV usa basicamente um cabeçalho GRE para transportar o tráfego L2 através da WAN. Esse cabeçalho GRE tem 42 bytes de tamanho. Em uma implantação de rede ideal, o link de WAN deve ter uma unidade de transmissão máxima (MTU) que seja pelo menos 42 bytes maior que o maior pacote que o OTV deve tratar.

Se a interface L2 tiver uma MTU de 1500 bytes, a interface de junção deverá ter uma MTU de 1542 bytes ou mais. Se a interface L2 tiver uma MTU de 2000 bytes, mas só tiver a expectativa de lidar com pacotes de até 1500 bytes, então uma MTU de WAN de 1542 bytes será suficiente; no entanto, a adição padrão de 42 ao 2000 seria 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
```

Alguns provedores de serviços não conseguem fornecer valores de MTU maiores para seus circuitos de WAN. Se esse for o caso, o ASR1000 pode executar a fragmentação dos dados transportados do OTV. O Nexus 7000 não tem esse recurso. Não há suporte para redes OTV Mistas ASR1000 e Nexus 7000 com fragmentação habilitada no ASR1000.

A configuração para fragmentação de OTV é:

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

É importante que o comando global level seja configurado antes do comando Overlay interface

join-interface. Se o comando otv join-interface da interface de Sobreposição tiver sido configurado primeiro, remova o comando otv join-interface da interface de Sobreposição, configure o comando otv fragmentation join-interface e, em seguida, configure o comando otv join-interface da interface de Sobreposição novamente.

Quando a fragmentação de OTV não está habilitada, todos os pacotes de OTV que transportam dados L2 encapsulados são enviados com o bit DF definido para que não sejam fragmentados em trânsito. Depois que o comando fragmentation é adicionado, o bit DF é definido como 0. Os próprios roteadores OTV podem fragmentar o pacote e ele pode ser fragmentado em trânsito por outros roteadores.

Há uma quantidade limitada de buffers de remontagem de pacotes disponíveis nas plataformas ASR1000, portanto, quanto menos fragmentos um pacote precisar ser cortado para melhor transmissão. Isso aumenta a eficiência e diminui o consumo geral de largura de banda na WAN, se isso for um problema. Há implicações de desempenho para habilitar a fragmentação de OTV. Se a fragmentação estiver presente e houver a expectativa de que mais de 1 Gb/s de tráfego OTV seja processado, o desempenho de OTV deve ser investigado mais a fundo.

Topologia Unicast de Caso Especial

As implantações de campo para OTV frequentemente têm conexões diretas de fibra back-to-back entre os roteadores OTV em dois data centers.

Para topologias single homed, isso cria uma implantação padrão em que o tráfego OTV e não OTV compartilham a interface de junção. Nenhuma consideração especial é necessária para esta configuração, portanto esta seção não se aplica.

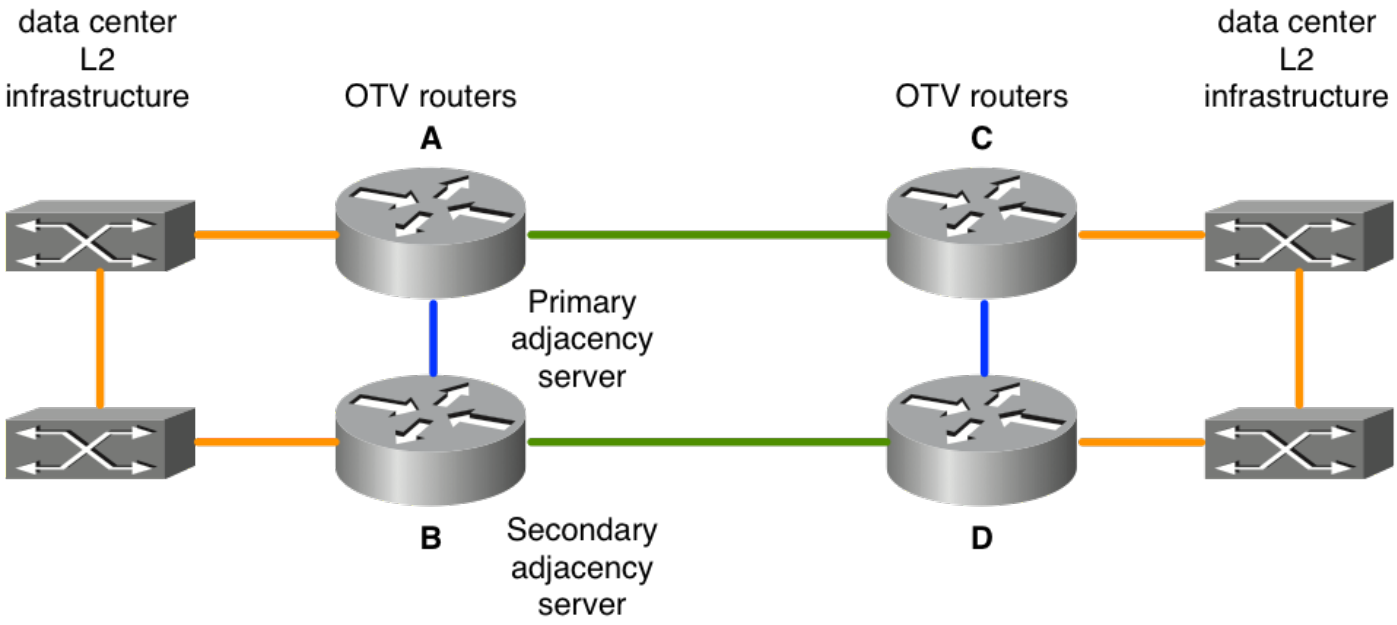
No entanto, se a implantação tiver roteadores OTV multihomed nos dois data centers, há algumas considerações especiais. É necessária uma configuração adicional.

Se mais de dois data centers estiverem envolvidos, esta configuração especial não se aplica.

Para o cenário com mais de dois data centers com roteadores OTV single ou multi-homed, deve ser usada uma implantação de OTV unicast ou multicast padrão.

Não há outra alternativa compatível.

Figura 8. Caso especial unicast



Na topologia apresentada, os links em verde são os links de fibra escura entre os dois data centers. Essas fibras escuras estão diretamente conectadas aos roteadores OTV. Os links azuis entre os roteadores OTV são usados para redirecionar o tráfego não OTV em caso de falha dos links verdes. Se o link verde superior falhar (A a C), o tráfego não OTV que usa os roteadores OTV mais superiores como sua rota padrão será roteado através dos links azuis norte-sul (A a B e C a D) para o link verde ainda operacional entre o par de roteadores OTV inferior (B a D).

Esse novo roteamento básico de tráfego não funciona para o tráfego OTV porque a configuração de OTV especifica uma interface física como a interface de junção. Se a "interface verde" no roteador A de OTV for desativada, o tráfego de OTV não poderá ser originado de uma interface alternativa do roteador B de OTV. Além disso, como não há conectividade total através do núcleo da WAN, todos os roteadores OTV não poderão ser informados quando houver uma falha. Para contornar esse problema, a detecção de encaminhamento bidirecional (BFD), juntamente com o script do gerenciador de eventos incorporado (EEM), é usada.

O BFD deve monitorar o link de WAN entre os pares de roteadores OTV leste-oeste (A/C e B/D). Se a conexão com o roteador remoto for perdida, a interface OTV Overlay será desativada através do script EEM nesse par de roteadores OTV leste-oeste. Isso faz com que o roteador multi-home pareado assuma o encaminhamento para todas as VLANs. Quando o BFD detecta que o link foi recuperado, o script EEM é acionado para reativar a interface de Sobreposição.

É muito importante que o BFD seja usado para detectar falhas de link. Isso ocorre porque a interface de sobreposição precisa ser desligada tanto no lado "com falha" quanto no par leste-oeste. Que depende do tipo de conectividade fornecido pelo provedor de serviços, um link físico pode ficar inativo (interface verde no roteador A do OTV), enquanto a interface do roteador correspondente do par leste-oeste pode permanecer ativa (interface verde no roteador C do OTV). O BFD detecta falhas de interface ou qualquer outro problema em trânsito e notifica imediatamente os dois pares simultaneamente. O mesmo se aplica quando os roteadores precisam ser informados sobre o link de recuperação.

A configuração para esta implantação é a mesma de qualquer outra implantação com a adição dos itens subsequentes:

- Configuração BFD na interface WAN
- o script EEM subsequente
- Identidade ISIS OTV para corresponder a distribuição de VLAN par/ímpar

A configuração de BFD na interface de junção OTV está além do escopo deste documento. Informações sobre como configurar o BFD no ASR1000 podem ser encontradas em:

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

Quando a detecção de falha de BFD estiver operacional corretamente entre os pares de interface de junção (links verdes no diagrama), o script EEM deverá ser implantado. O script EEM deve ser ajustado aos roteadores específicos para modificar as interfaces Overlay corretas, bem como talvez monitorar as strings mais exatas no registro para falha e recuperação de BFD.

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

Esse tipo de implantação também exige que os pares de roteadores leste-oeste (A/C e B/D) correspondam em seu encaminhamento de vlans ímpares e pares.

Por exemplo, A e C devem encaminhar VLANs pares, enquanto B e D encaminham VLANs ímpares em operação nominal em estado estacionário.

A distribuição ímpar/par é determinada pelo número ordinal OTV que pode ser observado pelo comando "show otv site".

O número ordinal entre os dois roteadores do local é determinado com base no ID de rede ISIS OTV.

```
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
```

O identificador de rede ISIS OTV deve ser configurado em todos os roteadores OTV. Deve-se tomar cuidado ao configurar o identificador de modo que todos os roteadores OTV ainda se reconheçam.

<#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

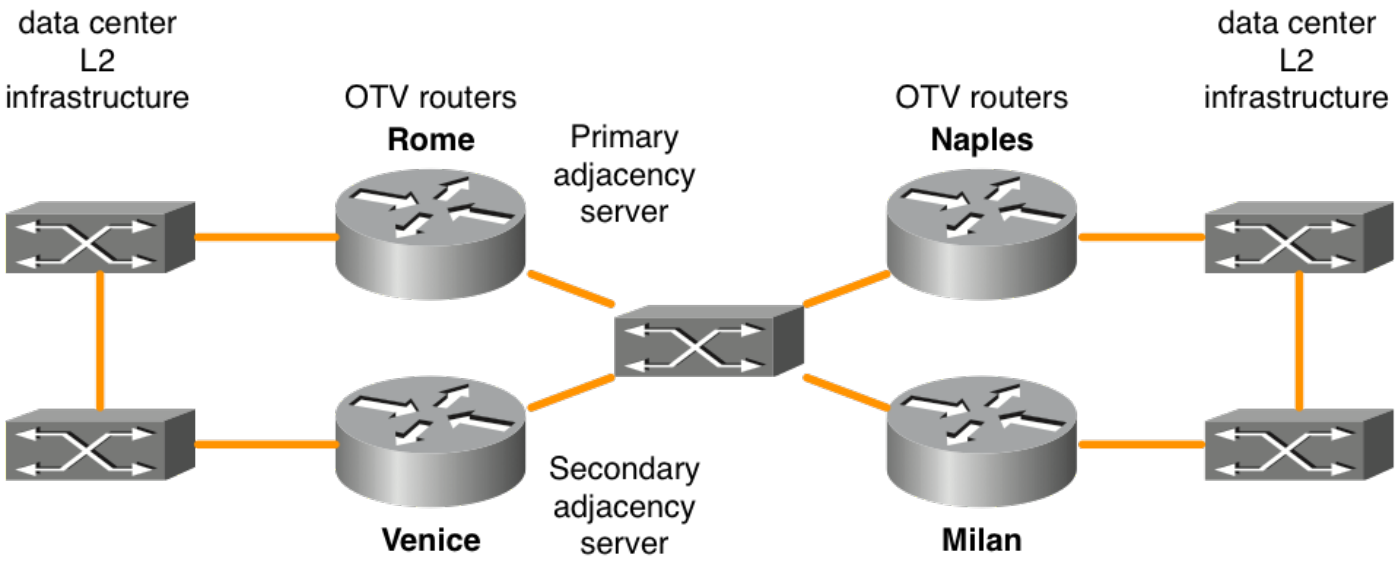
As partes do identificador em preto devem corresponder em todos os roteadores OTV que

participam da sobreposição. A parte do identificador em vermelho pode ser modificada. O identificador de rede mais baixo em um local obtém o número ordinal 0 e, por sua vez, encaminha as VLANs com número par. O identificador de rede mais alto em um local obtém o número ordinal 1 e encaminha as VLANs de número ímpar.

Exemplos de configuração

Unicast

Figura 9. Exemplo de configuração unicast



Configuração Rome:

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

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

Configuração de Veneza:

```
!
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
 !
```

Configuração 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
 !
```

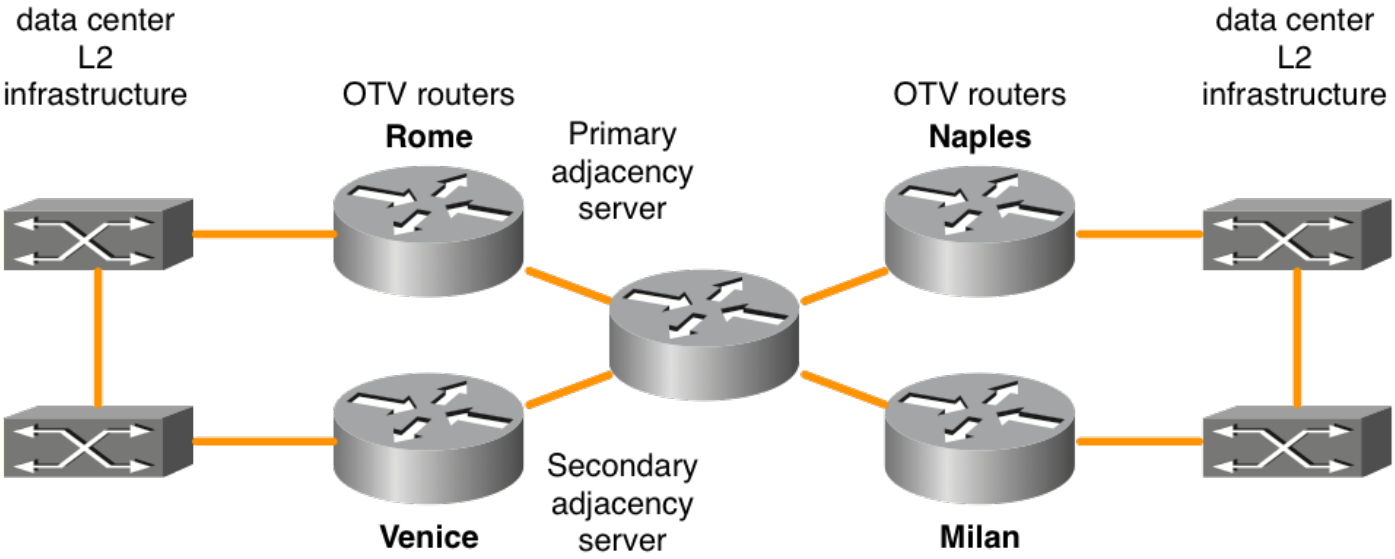
```
 service instance 101 ethernet
  encapsulation dot1q 101
  bridge-domain 101
 !
!
```

Configuração do Milan:

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

Multicast

Figura 10. Exemplo de configuração multicast



Configuração Rome:

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

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

Configuração de Veneza:

```
!
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
 !
```

Configuração 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
 !
!
```

Configuração do Milan:

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

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

Perguntas mais freqüentes

P) As VLANs privadas são suportadas em conjunto com o OTV?

A) Sim, Não é necessária uma configuração especial no OTV. Na configuração de VLAN privada, verifique se as portas do switch conectadas à interface L2 do OTV estão configuradas no modo promíscuo.

P) O OTV é compatível com a criptografia IPSEC?

A) Sim, a configuração de mapa de criptografia na interface de junção é suportada. Nenhuma configuração especial é necessária para que o OTV ofereça suporte à criptografia. No entanto, a configuração criptografada adiciona mais sobrecarga e isso deve ser compensado pelo aumento do MTU da WAN versus o MTU da LAN. Se isso não for possível, a fragmentação de OTV deve ser necessária. O desempenho de OTV é limitado ao do hardware IPSEC.

P) O OTV é compatível com o MACSEC?

A) Sim, o ASR1001-X inclui suporte MACSEC para as interfaces integradas. O OTV funciona com o MACSEC configurado nas interfaces LAN e/ou WAN. O desempenho do OTV é limitado ao do hardware MACSEC.

P) Uma interface de loopback pode ser usada como a interface de junção?

A) Não, somente interfaces Ethernet, Portchannels ou POS podem ser usadas como interfaces de junção OTV. A interface de junção de loopback de OTV está no roteiro, mas não está programada para uma versão no momento.

P) Uma interface de túnel pode ser usada como a interface de junção?

R) Não, túneis GRE, túneis DMVPN ou qualquer outro tipo de túnel não são suportados como interfaces de junção. Somente interfaces Ethernet, Portchannels ou POS podem ser usadas como interfaces de junção OTV.

P) Interfaces de sobreposição diferentes podem usar interfaces L2 e/ou de junção diferentes?

A) Todas as interfaces de sobreposição devem apontar para a mesma interface de junção. Todas as sobreposições devem ser vinculadas à mesma interface física para conectividade L2 em direção ao data center.

P) A VLAN do local OTV pode estar em uma interface física diferente das VLANs estendidas OTV?

A) A VLAN do local OTV e as VLANs estendidas devem estar na mesma interface física.

P) Que conjunto de recursos é necessário para OTV?

A) Advanced IP Services (AIS) ou Advanced Enterprise Services (AES) é necessário para OTV.

P) É necessária uma licença separada para OTV em plataformas de configuração fixa?

R) Não, enquanto o ASR1000 for executado com serviços de consultoria ou nível de inicialização adventerprise configurado, o OTV estará disponível.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.