Configurazione della virtualizzazione del trasporto overlay con ASR 1000

Sommario

Introduzione

Questo documento descrive le topologie di rete OTV (Overlay Transport Virtualization) supportate sui router ASR1000 e Catalyst serie 8300/8500.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASR 1000, IOS® XE versione 16.10.1a e successive
- Catalyst 8300, IOS® XE versione 17.5.1a e successive
- Catalyst 8500, IOS® XE versione 17.6.1a e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

ASR 1000 supporta OTV da Cisco IOS® XE release 3.5. Il router Catalyst serie 8300 inizia il supporto con IOS® XE17.5.1a, mentre le route Catalyst serie 8500 iniziano il supporto con IOS® XE versione 17.6.1a.

OTV fornisce la connettività di layer 2 tra siti di rete remoti tramite routing basato su indirizzo MAC e inoltro incapsulato IP (MAC-in-IP) su una rete di trasporto per fornire il supporto per le applicazioni che richiedono l'adiacenza di layer 2, quali cluster e virtualizzazione. OTV utilizza un protocollo del control plane di overlay per apprendere e propagare le informazioni di routing MAC attraverso la rete di overlay. Il protocollo del control plane OTV utilizza messaggi IS-IS (Intermediate-System-to-Intermediate-System) per creare adiacenze ai siti remoti e inviare aggiornamenti della route MAC ai siti remoti. OTV crea adiacenze di layer 2 ai siti remoti sulla rete di sovrapposizione mediante l'individuazione automatica dei dispositivi OTV remoti.

I vantaggi di OTV per l'estensione di layer 2 includono:

- Nessun requisito MPLS
- Nessuna configurazione EoMPLS (Ethernet over Multiprotocol Label Switching) complessa per mesh
- Nessuna distribuzione complessa di VPLS (Virtual Private LAN Services) per le estensioni di layer 2
- Isolamento Spanning-Tree nativo
    - non è necessario configurare esplicitamente i filtri BDPU (Bridge Data Protocol Unit)
    - isolamento predefinito dei problemi di spanning-tree in un data center specifico
- Isolamento flooding unicast nativo sconosciuto
    - pacchetti MAC unicast sconosciuti non inoltrati
    - supporto per inoltro unicast sconosciuto per MAC consentito
- Ottimizzazione Address Resolution Protocol (ARP) con memorizzazione nella cache OTV ARP
    - riduce il traffico WAN non necessario
- Provisioning semplificato dell'isolamento del protocollo FHRP (First Hop Redundancy Protocol)
- Aggiunta semplificata di siti
- Configurazione di ridondanza semplificata

- Possibilità di disporre di un "dispositivo di caduta" per le migrazioni quando sono necessari servizi temporanei

Requisiti

Gli elementi successivi sono le regole principali da tenere presenti quando viene progettata una distribuzione OTV. Se queste regole vengono rispettate, la progettazione e la distribuzione risulteranno semplificate.

- È possibile usare un'unica interfaccia per trasmettere il traffico incapsulato OTV, nota come interfaccia di join, per tutte le interfacce di overlay OTV configurate
- È possibile utilizzare un'unica interfaccia per configurare le istanze del servizio L2 del data center per la VLAN del sito OTV e le VLAN estese tra i data center per tutte le interfacce di overlay OTV configurate
- I canali delle porte possono essere utilizzati per la ridondanza dell'interfaccia e la connessione a switch VSS o VPC e sono supportati come interfaccia "una e una sola" per la connettività.
- Tutti i router OTV devono essere contattabili tramite l'interfaccia di join
- Lo Spanning Tree deve essere configurato sul router OTV che punta al centro dati
- Lo snooping e l'esecuzione di query IGMP devono essere configurati in modo da inoltrare correttamente il traffico multicast del centro dati
- Un data center può essere configurato con 1 o 2 router OTV. Con due router distribuiscono l'inoltro VLAN in modo dispari/pari in base al numero VLAN. Ogni router OTV di un centro dati funge da backup per l'altro.
- Le coppie multihomed devono essere configurate con lo stesso identificatore di sito OTV
- ASR 1000/Catalyst 8300/Catalyst 8500 e Nexus 7000 possono partecipare alla stessa rete OTV
    - Nexus 7000 non supporta la frammentazione OTV o la crittografia, pertanto queste funzionalità non possono essere utilizzate in una distribuzione "ibrida".

Esistono progetti supportati per la connettività back-to-back che non rispettano le regole indicate. Benché queste configurazioni siano supportate, non sono consigliate. Ulteriori informazioni sono disponibili nella sezione successiva "Special case unicast topology".

Non è possibile sottolineare a sufficienza che il software OTV corrente ha la restrizione di un'unica interfaccia quando si configurano le interfacce join e di accesso L2 per OTV. Un'interfaccia di canale porta può essere utilizzata per la ridondanza. È supportata la connessione del canale della porta a Nexus 7000 in un VPC. È inoltre supportata una connessione di base porta-canale a un singolo switch.

Tipi di implementazione OTV

OTV richiede una singola interfaccia join e una singola interfaccia L2. Per ciascun router OTV è possibile supportare uno solo di questi. OTV richiede anche che una VLAN di sito sia configurata in modo che i router OTV multihomed possano comunicare tra loro attraverso la rete locale. La VLAN del sito OTV deve essere configurata anche per i router OTV single-homed. Inoltre,

ciascun sito o centro dati deve disporre di un identificatore di sito univoco configurato. I router OTV dual-homed devono utilizzare lo stesso identificatore di sito ed essere in grado di comunicare sulla stessa VLAN.

La configurazione successiva fornisce la configurazione fondamentale di base necessaria per OTV. Tuttavia, non è completa in quanto è necessario aggiungere la configurazione di base unicast o multicast. Tali elementi sono descritti in dettaglio nelle sezioni successive 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 configurazione dell'istanza del servizio viene utilizzata per tutta la configurazione dell'interfaccia L2 con OTV.

Ogni istanza del servizio sull'interfaccia L2 deve essere associata a un incapsulamento con tag singolo o doppio specifico.

A sua volta, ognuna di queste istanze del servizio deve essere associata a un bridge-domain.

Tale dominio-bridge viene utilizzato in un'istanza del servizio configurata nell'interfaccia Overlay.

Il bridge-domain è l'associazione che collega l'istanza del servizio Overlay all'istanza del servizio interfaccia L2.

L'incapsulamento del traffico sull'interfaccia overlay deve corrispondere all'incapsulamento del traffico dopo la riscrittura in entrata sull'interfaccia L2.

Nell'esempio, il traffico in entrata sull'istanza del servizio Gig1/0/1 99 ha una singola VLAN 802.1Q di 99 e il dominio del bridge 99. Anche l'istanza del servizio corrispondente con il dominio del bridge 99 sull'interfaccia Overlay è configurata per una singola VLAN 802.1Q di 99. Questo caso è il più semplice.

Nell'esempio, il traffico in entrata sull'istanza del servizio Gig1/0/1 98 ha una doppia VLAN 802.1Q di 99 e 1098 e un dominio di bridge 90. L'istanza del servizio corrispondente con il dominio di bridge 90 sull'interfaccia Overlay è configurata per una singola VLAN 802.1Q di 90. Chiaramente, queste non sono le stesse. Il comando rewrite in entrata garantisce la corretta conversione dei tag man mano che il traffico passa attraverso l'interfaccia in entrata. Il traffico che entra nell'interfaccia L2 ha una VLAN 98/1098, 802.1Q, che viene sostituita con una singola VLAN 90. La parola chiave simmetrica garantisce che il traffico che esce dall'interfaccia L2 abbia una singola VLAN 802.1Q di 90 che viene sostituita con 98/1098.

Le istanze del servizio con più VLAN 802.1Q estese da OTV devono usare il comando rewrite in entrata. L'incapsulamento OTV supporta solo un singolo identificatore VLAN. Per questo motivo, ogni configurazione con doppia VLAN sulle interfacce L2 deve essere riscritta su un singolo tag sull'istanza del servizio dell'interfaccia Overlay. Ciò preclude il supporto di configurazioni VLAN ambigue.

Per ulteriori informazioni sulla riscrittura dei tag, vedere questo documento: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-cr-book/ce-m1.html

In questo esempio, il dominio bridge del sito OTV è 100.

- Il dominio bridge di sito OTV è configurato solo sull'interfaccia L2.
- Il dominio bridge del sito OTV non deve mai essere configurato sull'interfaccia Overlay perché ciò rende instabile la distribuzione OTV.
- La VLAN del sito OTV deve essere connessa solo ai router OTV e non trasportare altro traffico del centro dati/utente.
- La VLAN del sito OTV deve trovarsi sulla stessa interfaccia fisica delle VLAN estese OTV.

Multihome

Un centro dati può essere connesso con un singolo host OTV o fino a 2 per la ridondanza, nota anche come multihome. La funzione multihome viene utilizzata per la resilienza e il bilanciamento del carico. Quando in un sito sono presenti più dispositivi periferici ed entrambi partecipano alla stessa rete di sovrapposizione, il sito viene considerato multihomed. OTV Multihome suddivide le VLAN tra i due router OTV che appartengono allo stesso sito in modo dispari/pari in base al numero di VLAN. Un dispositivo periferico viene scelto come AED per tutte le VLAN dispari, mentre l'altro router OTV viene scelto come AED per tutte le VLAN pari. Ciascun AED è inoltre un dispositivo di standby per le VLAN attive sull'altro router. In caso di errore di collegamento o di nodo in uno degli AED, l'AED di standby diventa attivo per tutte le VLAN.

Se due ASR1000 sono connessi nello stesso centro dati per eseguire la funzione multihome, non

è necessario un collegamento dedicato tra i due ASR1000. OTV utilizza la VLAN del sito OTV che viene propagata tramite l'interfaccia interna e comunica tramite l'interfaccia di join per determinare i router responsabili per le VLAN pari e dispari.

Non è possibile combinare ASR1000 e Nexus 7000 nello stesso centro dati con OTV configurato su entrambi i router come backup per l'altro. La funzionalità multihome in un determinato centro dati è supportata per le piattaforme corrispondenti (ASR1000 o Nexus 7000). È possibile avere ASR1000 in un centro dati e Nexus 7000 in un altro centro dati. L'interoperabilità tra queste due piattaforme è stata testata e supportata. Alcuni centri dati possono essere multihomed mentre altri sono single homed.

Le coppie di router ASR1000 multihomed devono eseguire la stessa versione del software Cisco IOS® XE.

Se si usa la modalità multi-home, si consiglia di abilitare lo spanning-tree sui router OTV in quanto ciò permette al router OTV di inviare una notifica di modifica della topologia (TCN). In questo modo, il dispositivo dello switch L2 adiacente (insieme ad altri switch nello spanning-tree) riduce il timer della durata da quello predefinito a 15 secondi. Ciò aumenta notevolmente la convergenza di velocità in caso di guasto o ripristino tra la coppia multihomed. Lo Spanning-Tree può essere abilitato per tutte le istanze del servizio configurate (connesse a OTV o in altro modo) aggiungendo la riga successiva alla configurazione globale.

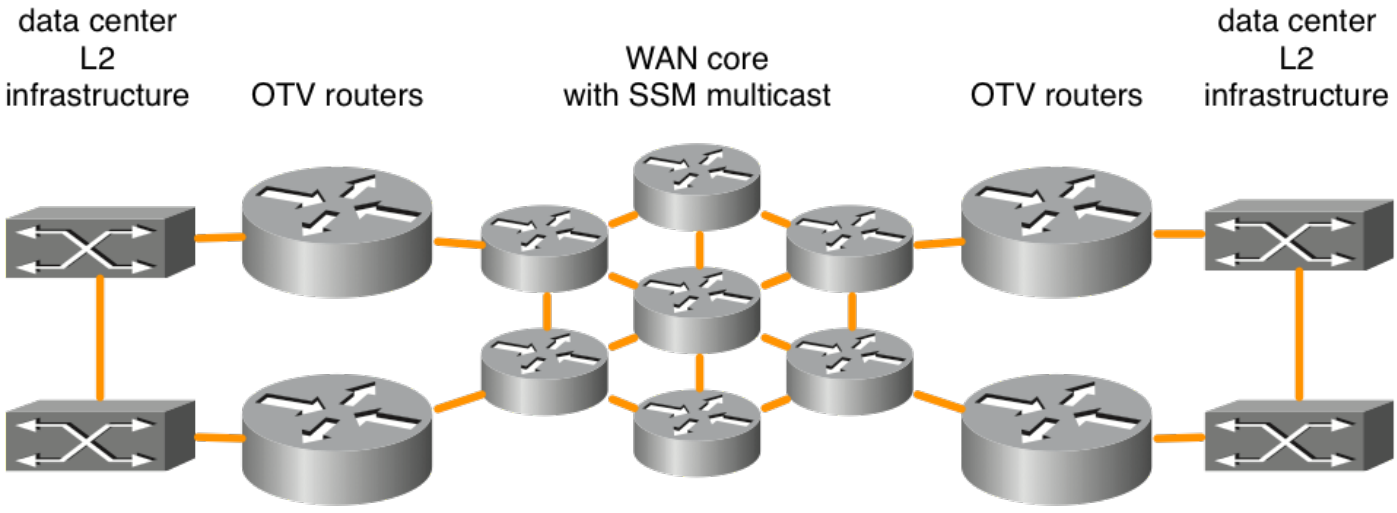
```
spanning-tree mode [ pvst | rapid-pvst | mst ]
```

Non è richiesta alcuna configurazione specifica per vlan o per istanza di servizio.

Multicast Core

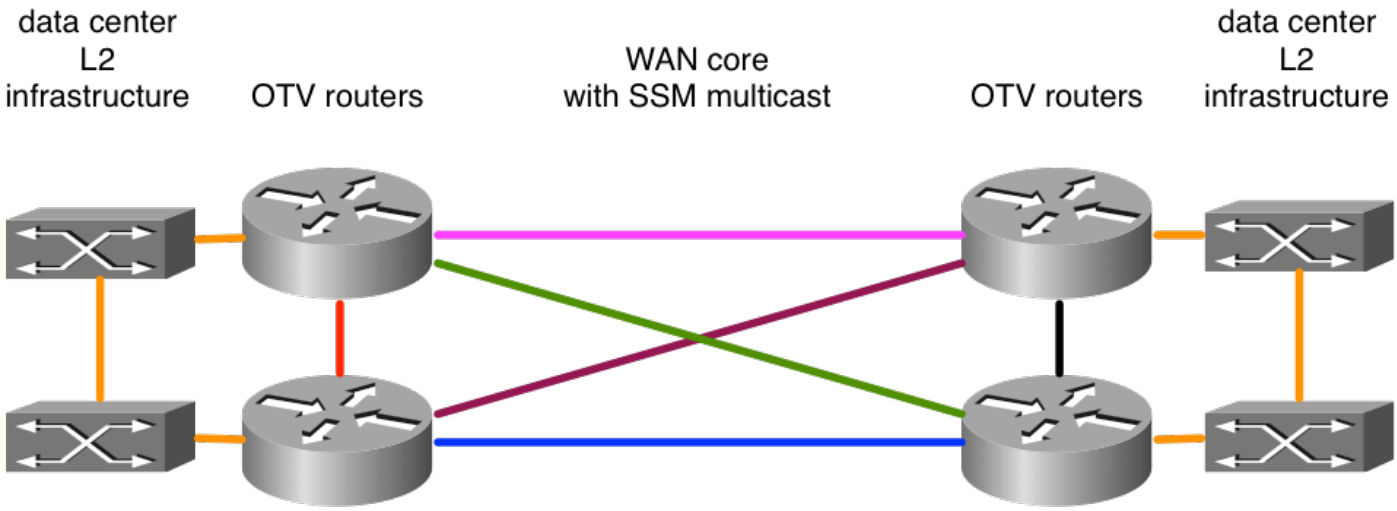
La rete multicast richiede una connettività mesh completa sulla WAN. Tutti i router OTV devono essere connessi tra loro tramite l'interfaccia di join.

Figura 1. Topologia di rete multicast supportata



Nella figura viene illustrato un esempio di due centri dati connessi tramite un core in rete completa. Il protocollo PIM (Source Specific Multicast) viene eseguito tra i router OTV e i router core WAN. È supportato un numero qualsiasi di router principali, a condizione che vi sia una connettività mesh completa. Non esiste alcun requisito esplicito di latenza massima per la connettività OTV nel core WAN.

Figura 2. Topologia di rete multicast non supportata



Poiché ASR1000/OTV si aspetta di ricevere messaggi multicast su un'interfaccia single join da tutti i peer, come nell'esempio, ciò determinerebbe una distribuzione OTV instabile. Si supponga che i collegamenti est-ovest in rosa e blu siano stati configurati come interfacce di join. Quando il collegamento rosa ha esito negativo, il router non sarà più in grado di ricevere gli aggiornamenti OTV su quell'interfaccia. Un percorso alternativo tramite i collegamenti verde o viola non è accettabile perché l'interfaccia di join è configurata in modo esplicito. Gli aggiornamenti devono essere ricevuti su tale interfaccia. L'utilizzo di interfacce di loopback come interfaccia di join non è attualmente supportato.

Se l'utente non è il proprietario della backbone, deve verificare che il provider di servizi supporti il multicast nel nucleo e che possa rispondere ai messaggi di query IGMP (Internet Group Management Protocol). OTV su ASR1000 agisce come host multicast (inoltra messaggi di join IGMP), non come router multicast per la topologia multicast WAN principale.

La rete di trasporto tra i router OTV deve supportare la modalità sparse PIM (Any Source Multicast [ASM]) per il gruppo multicast del provider e SSM per il gruppo di recapito.

I core multicast richiedono una configurazione specifica sull'interfaccia Overlay per un gruppo di controllo, nonché per un intervallo di gruppi multicast di dati utilizzati per l'inoltro dei dati.

```
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
```

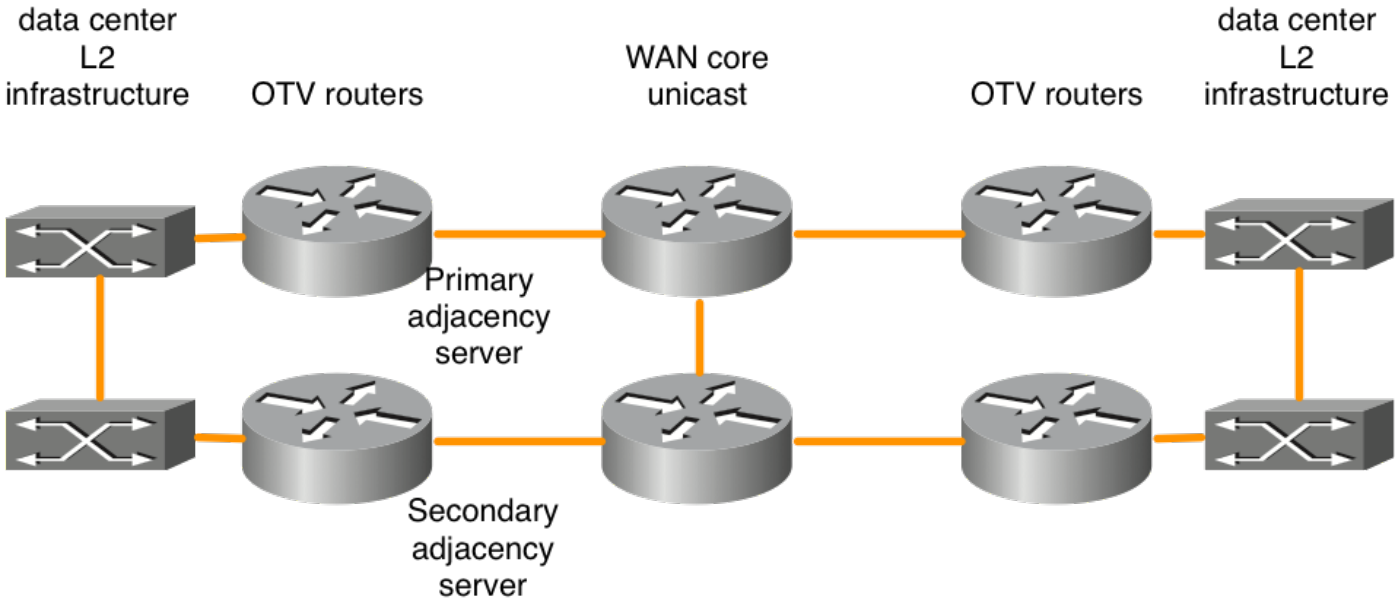
Le distribuzioni OTV multicast richiedono che l'interfaccia di join sia configurata come interfaccia passiva PIM. IGMP può essere configurato per diverse versioni, se necessario. Sull'interfaccia di overlay devono essere configurati un gruppo di controllo e un gruppo di dati. Il gruppo di controllo è un singolo gruppo multicast utilizzato per la gestione OTV. Il gruppo di dati è un intervallo di indirizzi multicast utilizzato per il trasporto di dati utente tra centri dati. Se il gruppo di dati non si trova nello spazio IP 232.0.0.0/8, il comando aggiuntivo "ip pim ssm range" deve essere configurato in modo da includere l'intervallo richiesto da OTV.

La rete di trasporto tra i router OTV deve supportare la modalità sparse PIM (Any Source Multicast [ASM]) per il gruppo multicast del provider e SSM (Source Specific Multicast) per il gruppo di recapito.

Core unicast con server adiacenti

Cisco IOS® XE 3.9 ha aggiunto il supporto per OTV con un core unicast. I core unicast e multicast per OTV continuano ad essere supportati per tutte le piattaforme ASR1000 e le versioni future di Cisco IOS® XE 3.9.

Figura 3. Topologia di rete unicast



La funzionalità server adiacente OTV consente il trasporto solo unicast tra i bordi OTV. I router OTV configurati con il ruolo server adiacente mantengono un elenco di tutti i router OTV noti. Forniscono tale elenco a tutti i router OTV registrati in modo che dispongano di un elenco di dispositivi che devono ricevere traffico broadcast e multicast replicato.

Il control plane OTV su un trasporto solo unicast funziona esattamente allo stesso modo di OTV con core multicast, con la differenza che in una rete unicast-core, ciascun dispositivo OTV edge deve creare più copie di ciascun pacchetto control plane e unicast a ciascun dispositivo remote nella stessa sovrapposizione logica.

Allo stesso modo, qualsiasi traffico multicast proveniente dal data center viene replicato sul router OTV locale e a ognuno dei data center remoti vengono inviate più copie. Anche se questa operazione è meno efficiente che essere subordinata al core WAN per eseguire la replica, la configurazione e la gestione della rete multicast di base non sono necessarie. Se il traffico multicast del centro dati è limitato o se il numero di postazioni del centro dati è ridotto (quattro o meno), un core unicast per l'inoltro OTV rappresenta in genere la scelta migliore. Nel complesso, la semplificazione operativa del modello solo unicast rende l'opzione di installazione dei core unicast preferibile negli scenari in cui la connettività di estensione LAN è richiesta solo tra quattro o meno centri dati. È consigliabile configurare almeno due server adiacenti, uno primario e uno di backup. Non è disponibile un'opzione per la configurazione del server adiacente attivo/attivo.

I router OTV devono essere configurati di conseguenza per identificare e registrare correttamente il server adiacente appropriato.

	Server adiacente primario	Server adiacente secondario	Altri router OTV
Indirizzo IP interfaccia join OTV	10.0.0.1	10.2.2.24	altri indirizzi IP
Configurazione	interface Overlay 1 adiacenza otv-server solo unicast	interface Overlay 1 adiacenza otv-server solo unicast otv use-adiacency-server 10.0.0.1 unicast-only	interface Overlay 1 otv use-adiacency-server 10.0.0.1 10.2.2.24 unicast-only

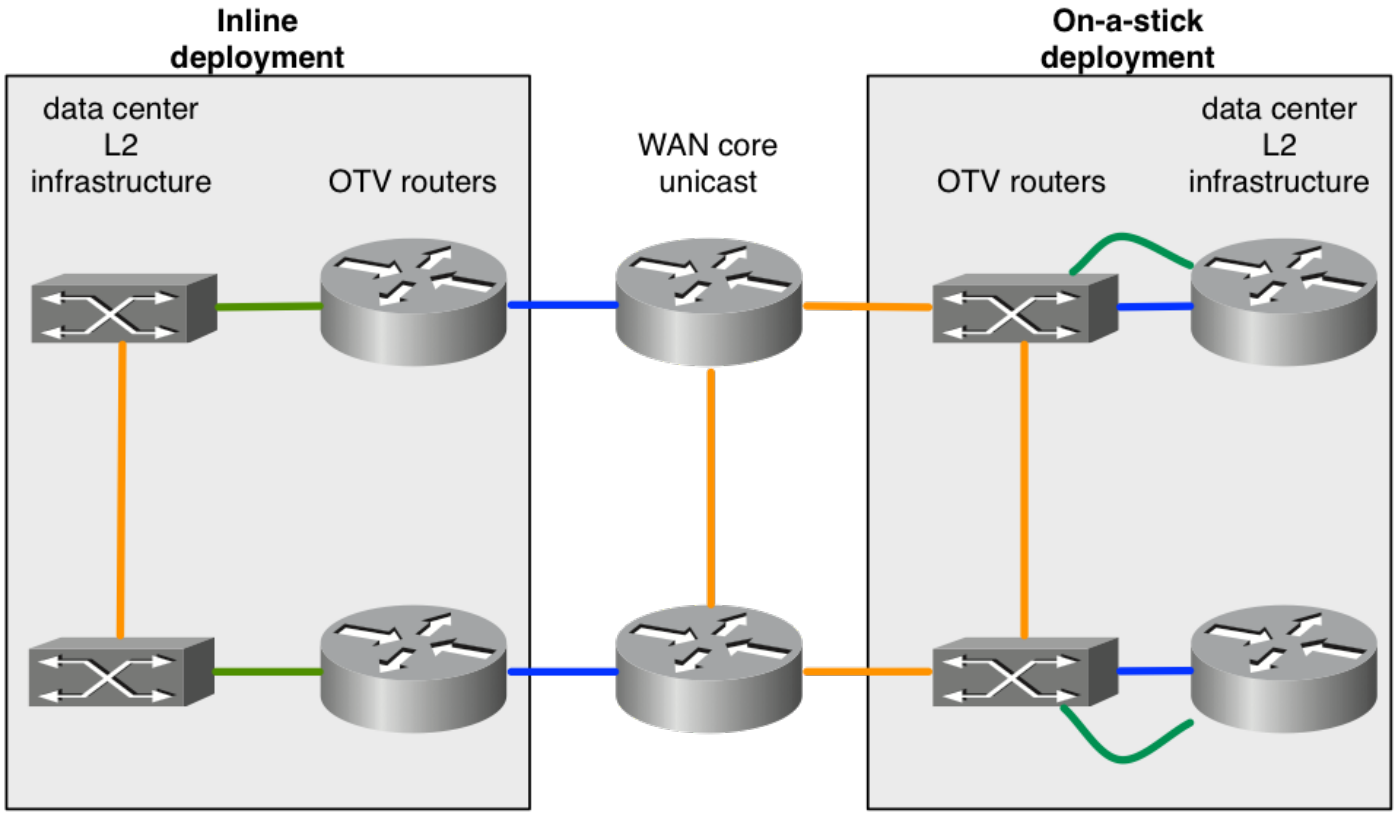
Esistono progetti per la connettività back-to-back supportati con l'inoltro OTV unicast che non rispettano le regole della "rete completa". Sebbene supportate, queste configurazioni non sono consigliate. Questo tipo di installazione è più comune quando i centri dati sono connessi tramite fibra oscura. I dettagli su questa opzione di configurazione sono disponibili nella sezione successiva "Topologia unicast del caso speciale".

OTV su Memory Stick e inline

Esistono due modelli per l'installazione di OTV nel centro dati: su bastoncino e in linea. Negli scenari di progettazione presentati in precedenza, i router OTV erano inline tra il centro dati e la rete principale del provider di servizi. Tuttavia, l'aggiunta del router OTV come accessorio che non si trovi sul percorso di trasporto di tutto il traffico potrebbe essere più auspicabile. A volte è

necessario non modificare la topologia corrente per connettersi al provider di servizi tramite le apparecchiature correnti (ad esempio, un'implementazione in modalità brownfield con lo switch Catalyst 6000 o hardware dello switch Nexus che non supporta OTV). Pertanto, è preferibile implementare OTV su ASR1000 come su un dispositivo stick come un accessorio OTV.

Figura 4. Topologia inline e on-a-stick



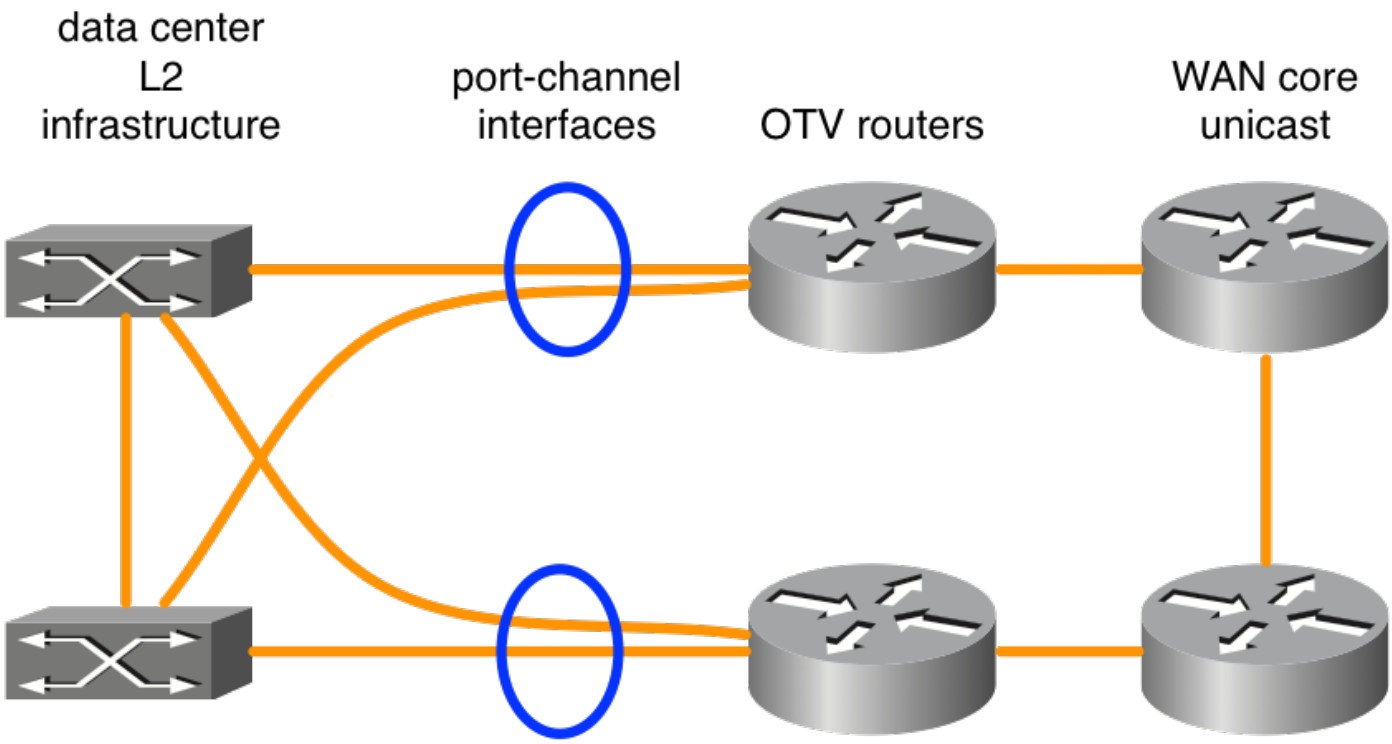
Nel diagramma vengono illustrati i due modelli di distribuzione che possono far parte della stessa sovrapposizione. I collegamenti verdi connessi ai router OTV sono configurati come interfacce di accesso L2 per accettare il traffico VLAN. I collegamenti blu collegati ai router OTV sono le interfacce di join che trasportano il traffico VLAN incapsulato OTV.

Può essere necessario configurare una funzionalità non supportata con OTV. Ad esempio, non è possibile configurare OTV e MPLS nella stessa casella. Di conseguenza, può essere una buona opzione usare ASR1000/OTV su uno stick e configurare MPLS sul router che si trova di fronte al router OTV.

Canali delle porte per layer 2 e layer 3

Il codice Cisco IOS® XE 3.10 per ASR1000 ha aggiunto il supporto per la configurazione del canale della porta di livello 2 e 3 con OTV. Il canale della porta di livello 2 può essere usato come interfaccia interna. Il canale della porta deve essere costituito da un massimo di 4 interfacce fisiche. Il canale della porta di layer 3 può essere utilizzato come interfaccia di join.

Figura 5. Canali delle porte utilizzati per la connettività L2



Il diagramma mostra un tipico scenario di canale porta con due switch in VSS (Catalyst serie 6000) o VPC (Nexus serie 7000). Questo tipo di progettazione offre ridondanza con due router OTV e doppia connettività all'infrastruttura del centro dati. Non è necessaria alcuna configurazione speciale per OTV diversa dalla configurazione base del canale della porta se il VSS o il VPC viene utilizzato su apparecchiature di commutazione L2 adiacenti ai router OTV.

Gateway predefinito

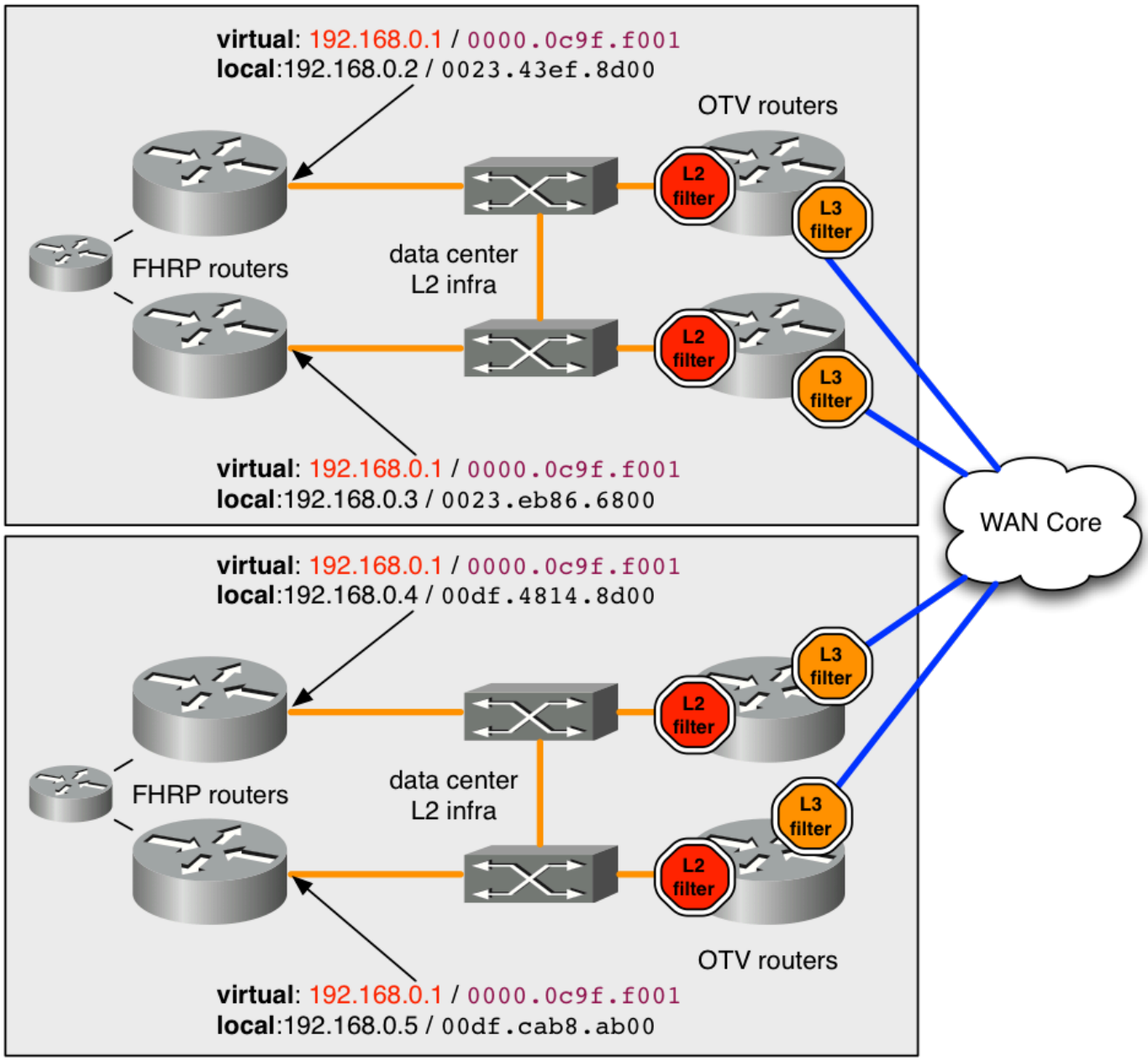
Per definizione, OTV crea la stessa subnet L3 in più posizioni. Ciò richiede alcune considerazioni speciali quando si instrada il traffico L3 da e verso le VLAN estese. Il routing L3 può essere configurato sugli stessi router OTV o su altri dispositivi connessi alle VLAN estese. Inoltre, in ogni scenario è possibile implementare per la ridondanza i protocolli di ridondanza del primo hop (FHRP), ad esempio il protocollo HSRP (Hot Standby Redundancy Protocol) o il protocollo VRRP (Virtual Router Redundancy Protocol). L'HSRP può essere eseguito in locale in un dato centro dati o estendersi tra centri dati diversi (in genere).

La procedura ottimale per le distribuzioni OTV che utilizzano FHRP consiste nell'esecuzione di istanze locali di FHRP in ogni centro dati. Tali istanze di FHRP utilizzano lo stesso indirizzo MAC virtuale e lo stesso indirizzo IP in modo che, quando le macchine virtuali (VM) si spostano tra i centri dati, abbiano una connessione ininterrotta. Se l'indirizzo MAC del router predefinito dovesse passare da un centro dati all'altro, le VM non sarebbero in grado di comunicare al di fuori della subnet fino al timeout della voce ARP del gateway predefinito della VM.

Per distribuire correttamente un FHRP con OTV, è necessario considerare quali traffici L2 e L3 devono essere filtrati e isolati da OTV. Al livello L2, ciò è necessario per impedire a OTV di rilevare lo stesso MAC virtuale L2 utilizzato da FHRP in più posizioni. I filtri sono necessari a livello L3 per mantenere gli annunci HSRP e VRRP isolati in ogni centro dati, in modo che la scelta di attivazione/ascolto/standby sia localizzata in ogni centro dati.

Per impostazione predefinita, i filtri FHRP sono abilitati quando OTV è abilitato. Può essere disattivata se la progettazione richiede l'estensione di FHRP tra centri dati. Il filtro L2 degli indirizzi MAC virtuali NON è abilitato per impostazione predefinita e deve essere configurato manualmente.

figura 6. Esempio di distribuzione consigliata per FHRP



Nell'esempio, l'indirizzo MAC virtuale 0000.0c9f.f001 viene usato per l'indirizzo IP 192.168.0.1 che ospita la VLAN estesa per la connettività della subnet. Utilizzo dello stesso indirizzo MAC e IP virtuale in entrambi i centri dati, un host dispone di connettività senza problemi dalla subnet quando viene trasferito tra i centri dati.

Per mantenere l'indirizzo MAC 0000.0c9f.f001 nascosto da OTV in più posizioni, è necessario distribuire un filtro L2 in entrata (arresto rosso nel diagramma) per la VLAN su ciascuno dei router OTV che gestiscono la VLAN. Con il filtro ACL l'ACL del filtro configurato sulle istanze del servizio L2 per l'entrata, tutti i pacchetti provenienti da tale MAC vengono scartati prima che il processo

OTV su ASR1000 possa vederli. Pertanto, OTV non viene mai a conoscenza dell'indirizzo MAC e non lo annuncia ai centri dati remoti.

La configurazione consigliata per intercettare tutto il traffico MAC virtuale FHRP conosciuto / predefinito è indicato qui.

```
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
```

Questo ACL corrisponde agli spazi di indirizzi MAC conosciuti associati alle versioni 1 e 2 dell'HSRP, al protocollo di bilanciamento del carico del gateway (GLBP) e al protocollo VRRP (in questo ordine). Se l'MAC virtuale è configurato per utilizzare un valore non standard non basato sul numero di gruppo FHRP, deve essere aggiunto esplicitamente all'esempio dell'ACL. È necessario aggiungere l'ACL all'istanza del servizio L2 (mostrato di seguito).

```
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
```

È inoltre necessario gestire la comunicazione tra gli host FHRP anche a livello L3. In un diagramma sono configurati quattro router FHRP su una singola subnet estesa. Senza un certo grado di filtri L3, i quattro router si vedrebbero a vicenda e selezionerebbero un singolo dispositivo attivo e ne avrebbero 3 in vari stati di standby. Pertanto, un centro dati avrebbe due router FHRP in standby locale, ma non avrebbe connettività L2 al router attivo remoto a causa dei filtri L2 discussi in precedenza.

Il risultato desiderato è disporre di un router FHRP attivo e di un router FHRP in standby in ciascun centro dati. Il filtro in entrata L2 descritto in precedenza non intercetta questo traffico di selezione, in quanto il processo di selezione usa gli indirizzi IP e MAC effettivi del router. Per impostazione predefinita, l'ACL successivo viene applicato in uscita sull'interfaccia Overlay. L'uscita per l'interfaccia Overlay sarebbe il traffico verso il core WAN. L'ACL non viene visualizzato nella configurazione corrente, ma è possibile osservarlo con "show ip access-list". Filtra il traffico elettorale FHRP in base al numero di 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
```

L'unico motivo per disabilitare questo filtro è se si desidera che tutti i router FHRP su una VLAN partecipino alla stessa scelta dello stato attivo. Per disabilitare questo filtro, configurare "no otv filter-fhrp" sull'interfaccia Overlay.

Traffico unknown unicast

Per impostazione predefinita, il traffico unicast ricevuto dalla LAN dal router OTV destinato a un indirizzo MAC sconosciuto in una posizione OTV remota viene scartato. Questo traffico è noto come unicast sconosciuto. Questa operazione di drop va verso il core WAN che limita la quantità di larghezza di banda utilizzata sulla WAN dal traffico di broadcast. In genere, tutti gli host della LAN emettono un traffico di broadcast (ARP, trasmissioni di protocollo, ecc.) sufficiente per essere sempre visti da un router OTV, pubblicizzati e quindi "noti".

Alcune applicazioni sfruttano gli host in background. Su una normale infrastruttura di switching questo non è un problema, in quanto la trasmissione L2 di indirizzi MAC unicast sconosciuti sulla LAN consente all'host silenzioso di vedere il traffico. Tuttavia, in un ambiente OTV, il router OTV blocca il traffico tra i centri dati.

Per ovviare a questo problema, Cisco IOS® XE ha integrato una funzione nota come Selective Unicast Forwarding. XE 3.10.6, XE3.13.3, XE 3.14.1, XE3.15 e tutte le versioni successive supportano l'inoltro unicast selettivo.

La configurazione viene effettuata aggiungendo un unico comando per indirizzo MAC sull'interfaccia Overlay. Ad esempio:

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

Nell'esempio, il traffico destinato a 0000.0001.0001 deve essere inondato su tutti i router OTV remoti con VLAN 100. Ciò può essere osservato dal comando seguente:

<#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 l'indirizzo MAC viene appreso in un sito remoto, è necessario aggiungere alla tabella di inoltro una voce che abbia la precedenza sulla voce flood.

<#root>

```
OTV_router_1#
```

show otv route

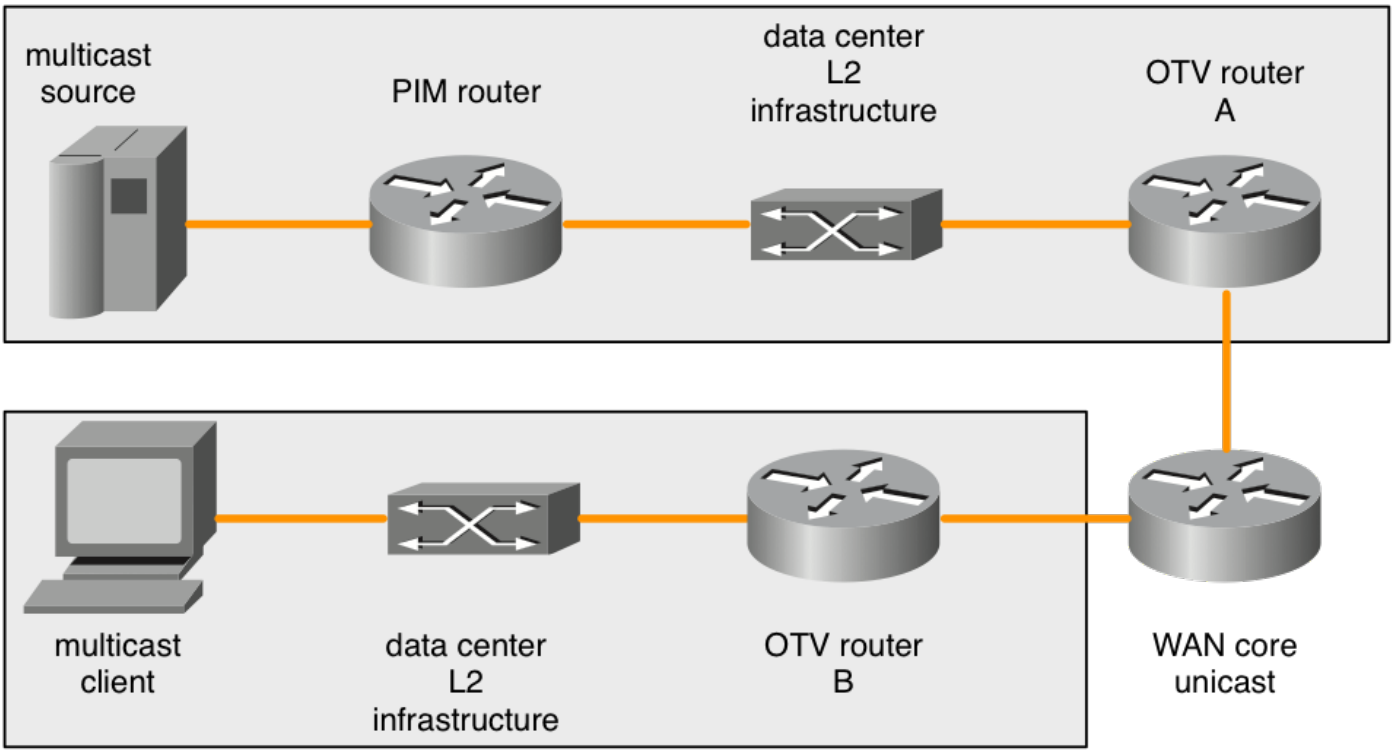
```
Codes: BD - Bridge-Domain, AD - Admin-Distance,SI - Service Instance, * - Backup Route
OTV Unicast MAC Routing Table for Overlay99
 Inst VLAN BD     MAC Address    AD    Owner  Next Hops(s)
-------------------------------------------------------------
 0    100  100    0000.0000.0001 20    OTV  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

In genere, una voce di flooding per un determinato indirizzo MAC deve essere configurata su tutti i router OTV con quella VLAN.

Origini Multicast remote

ASR1000 - Un router OTV non inoltra le richieste di join IGMP multicast ricevute dalla LAN. Il diagramma successivo illustra in dettaglio la topologia in cui può trattarsi di un problema.

Figura 7. Origini multicast remote



Quando un join IGMP multicast viene inviato dal client multicast, ASR1000 (router B OTV) lo osserva e annuncia l'interesse per il gruppo multicast. I router OTV remoti (router OTV A) devono inoltrare tutto il traffico a quel gruppo multicast che vedono sul loro dominio broadcast L2 locale. Tuttavia, ASR1000 (router OTV A) remoto non rigenera le richieste di join IGMP multicast quando l'interesse in un gruppo multicast viene annunciato al router OTV (router B) del client.

Quando le origini multicast si trovano nello stesso dominio di broadcast L2 del router OTV, non si tratta di un problema. Il router OTV deve essere configurato come query IGMP. Questo appare in qualsiasi traffico multicast presente sul dominio di trasmissione L2. Tuttavia, solo una richiesta di unione PIM causerebbe a un router PIM l'inoltro di una fonte multicast da un dominio di trasmissione L2 diverso al dominio di trasmissione L2 su cui è attivo il router OTV.

La richiesta di aggiunta IGMP remota non viene inoltrata o rigenerata. Nemmeno i router OTV sono router PIM. Pertanto, le topologie con origini multicast non direttamente nel dominio di trasmissione L2 con il router OTV non hanno modo di informare i router PIM di inoltrare il traffico di origine quando vi è interesse da parte di un client remoto.

Per risolvere questo problema, sono disponibili due soluzioni.

In primo luogo, è possibile distribuire uno o più client IGMP locali nel dominio di trasmissione L2 collegato al router OTV (router A OTV). Tale client IGMP dovrebbe sottoscrivere qualsiasi gruppo multicast a cui i client remoti potrebbero sottoscrivere. In questo modo, il router PIM inoltra il traffico multicast al dominio di trasmissione adiacente al router A OTV. Le query IGMP richiederebbero quindi qualsiasi traffico multicast e verrebbero inviate attraverso la sovrapposizione.

L'altra soluzione consisterebbe nel configurare un "ip igmp static-join" per tutti i gruppi ai quali i client remoti potrebbero iscriversi. In questo modo, il router PIM inoltra il traffico multicast al dominio di trasmissione adiacente al router A OTV.

Questa limitazione è nota e fa parte della specifica di progettazione. Al momento non viene considerato un bug, ma un limite nella topologia supportata.

Considerazioni QoS

Per impostazione predefinita, su ASR1000, il valore TOS nell'intestazione OTV aggiunta viene copiato dai bit 802.1p del pacchetto L2. Se il pacchetto L2 non ha tag, viene usato il valore zero.

Nexus 7000 ha un comportamento predefinito diverso nel software 5.2.1 e versioni successive. Se il comportamento desiderato è copiare il valore TOS dei pacchetti interni nel router, è possibile ottenere una configurazione QoS aggiuntiva. In questo modo si ottiene lo stesso comportamento del nuovo software Nexus 7000.

La configurazione per copiare il valore TOS L3 dei pacchetti L2 nell'intestazione più esterna del pacchetto OTV è la seguente:

```
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 configurazione fornita deve corrispondere al traffico per i vari valori DSCP in entrata. Il tag

qos-group significativo a livello locale viene usato per contrassegnare internamente il traffico durante il transito attraverso il router. Sull'interfaccia di uscita, il qos-gruppo viene abbinato e quindi il byte TOS più esterno viene aggiornato di conseguenza.

Considerazioni sulla MTU WAN / Frammentazione

OTV utilizza essenzialmente un'intestazione GRE per trasportare il traffico L2 sulla WAN. Questa intestazione GRE ha dimensioni di 42 byte. In una distribuzione di rete ideale, il collegamento WAN deve avere un'unità di trasmissione massima (MTU) che sia almeno 42 byte più grande del pacchetto più grande che OTV dovrebbe gestire.

Se l'interfaccia L2 ha una MTU di 1500 byte, allora l'interfaccia di join deve avere una MTU di 1542 byte o più. Se l'interfaccia L2 ha una MTU di 2000 byte, ma si prevede che gestisca pacchetti fino a 1500 byte, è sufficiente una MTU WAN di 1542 byte, ma l'aggiunta standard di 42 alla 2000 è ideale.

```
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
```

Alcuni provider di servizi non sono in grado di fornire valori MTU più grandi per i circuiti WAN. In questo caso, ASR1000 può eseguire la frammentazione dei dati trasportati da OTV. Nexus 7000 non dispone di questa funzionalità. L'uso combinato di reti ASR1000 e Nexus 7000 OTV con frammentazione abilitata su ASR1000 non è supportato.

La configurazione per la frammentazione OTV è:

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

È importante configurare il comando level prima del comando overlay interface join-interface. Se il comando otv join-interface dell'interfaccia di overlay è stato configurato per primo, rimuovere il

comando otv join-interface dall'interfaccia di overlay, configurare il comando otv fragmentation join-interface e quindi configurare nuovamente il comando otv join-interface dell'interfaccia di overlay.

Quando la frammentazione OTV non è abilitata, tutti i pacchetti OTV che contengono dati L2 incapsulati vengono inviati con il bit DF impostato in modo che non vengano frammentati durante la trasmissione. Dopo aver aggiunto il comando fragmentation, il bit DF è impostato su 0. I router OTV possono frammentare il pacchetto e può essere frammentato da altri router.

Sulle piattaforme ASR1000 è disponibile una quantità limitata di buffer di riassemblaggio dei pacchetti, quindi meno frammenti in un pacchetto devono essere frammentati per una migliore trasmissione. Ciò aumenta l'efficienza e riduce il consumo complessivo di larghezza di banda sulla WAN, se questo è un problema. L'abilitazione della frammentazione OTV comporta alcune implicazioni in termini di prestazioni. Se è presente la frammentazione e ci si aspetta di gestire più di 1 Gb/sec di traffico OTV, è necessario esaminare ulteriormente le prestazioni OTV.

Topologia unicast caso speciale

Le installazioni sul campo per OTV spesso dispongono di connessioni in fibra back-to-back dirette tra i router OTV in due centri dati.

Per le topologie single-homed, questo rende disponibile una distribuzione standard in cui il traffico OTV e non OTV condividono l'interfaccia di join. Questa sezione non è valida in quanto non sono necessarie particolari considerazioni per questa impostazione.

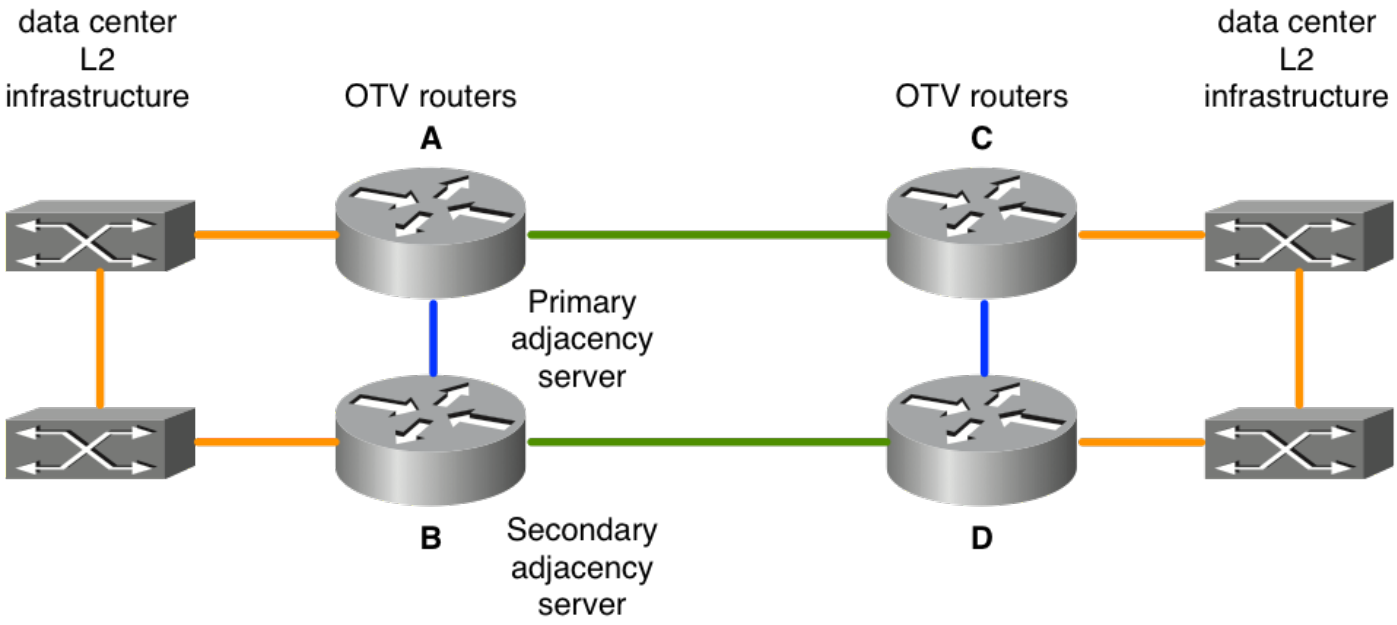
Tuttavia, se l'implementazione dispone di router OTV multihomed nei due centri dati, è necessario tenere presenti alcune considerazioni speciali. È necessaria un'ulteriore configurazione.

Se sono coinvolti più di due data center, questa configurazione speciale non è applicabile.

Per lo scenario con più di due centri dati con router OTV single o multi-homed, è necessario utilizzare una distribuzione OTV unicast o multicast standard.

Non esistono altre alternative supportate.

Figura 8. unicast con case speciali



Nella topologia presentata, i collegamenti in verde sono i collegamenti in fibra scura tra i due centri dati. Queste fibre scure sono collegate direttamente ai router OTV. I collegamenti blu tra i router OTV vengono usati per reindirizzare il traffico non OTV in caso di guasto ai collegamenti verdi. Se il collegamento verde superiore non funziona (A-C), il traffico non OTV che usa i router OTV più in alto come percorso predefinito viene instradato attraverso i collegamenti blu nord-sud (A-B e C-D) al collegamento verde ancora operativo tra la coppia di router OTV più in basso (B-D).

Questo reindirizzamento di base del traffico non funziona per il traffico OTV perché la configurazione OTV specifica un'interfaccia fisica come interfaccia di join. Se l'"interfaccia verde" sul router A OTV si interrompe, il traffico OTV non può essere indirizzato da un'interfaccia alternativa sul router B OTV. Inoltre, poiché non vi è piena connettività tramite il core WAN, tutti i router OTV non possono essere informati in caso di guasto. Per risolvere questo problema, vengono utilizzati il rilevamento dell'inoltro bidirezionale (BFD) e gli script EEM (embedded event manager).

Il BFD deve monitorare il collegamento WAN tra le coppie di router OTV est-ovest (A / C e B / D). Se la connessione al router remoto viene persa, l'interfaccia OTV Overlay viene chiusa tramite lo script EEM su tale coppia di router OTV est-ovest. In questo modo, il router multi-home associato assume l'inoltro per tutte le VLAN. Quando BFD rileva che il collegamento è stato ripristinato, lo script EEM attiva di nuovo l'interfaccia Overlay.

È molto importante utilizzare il BFD per rilevare eventuali errori di collegamento. Questo perché l'interfaccia Overlay deve essere chiusa sia sul lato "guasto" che sulla coppia est-ovest. A seconda del tipo di connettività fornito dal provider di servizi, un collegamento fisico può interrompersi (interfaccia verde sul router A OTV) mentre l'interfaccia della coppia est-ovest corrispondente può rimanere attiva (interfaccia verde sul router C OTV). Il BFD rileva il guasto di entrambe le interfacce o qualsiasi altro problema in transito e avvisa immediatamente entrambe le coppie contemporaneamente. Lo stesso vale quando i router devono essere informati del collegamento di ripristino.

La configurazione per questa distribuzione è la stessa di tutte le altre distribuzioni con l'aggiunta degli elementi seguenti:

- Configurazione BFD sull'interfaccia WAN
- lo script EEM successivo
- Identità ISIS OTV corrispondente alla distribuzione VLAN pari/dispari

La configurazione del BFD sull'interfaccia di join OTV esula dall'ambito di questo documento. Per informazioni su come configurare BFD su ASR1000, visitare:

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

Se il rilevamento degli errori BFD funziona correttamente tra le coppie di interfacce di join (collegamenti verdi nel diagramma), è necessario distribuire lo script EEM. Lo script EEM deve essere personalizzato in base ai router specifici per modificare le interfacce overlay corrette e forse monitorare le stringhe più esatte nel log per rilevare errori BFD e ripristinare dati.

```
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 ..."
!
```

Per questo tipo di implementazione, è necessario anche che le coppie di router est-ovest (A / C e B / D) corrispondano durante l'inoltro di vlan pari e dispari.

Ad esempio, A e C devono inoltrare le VLAN pari mentre B e D inoltrano le VLAN dispari in modalità di funzionamento nominale stazionario.

La distribuzione pari / dispari è determinata dal numero ordinale OTV che può essere osservato con il comando "show otv site".

Il numero ordinale tra i due router di sito viene determinato in base all'ID di rete 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
```

L'identificatore di rete ISIS OTV deve essere configurato su tutti i router OTV. Prestare attenzione quando si configura l'identificatore in modo che tutti i router OTV si riconoscano ancora.

<#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
```

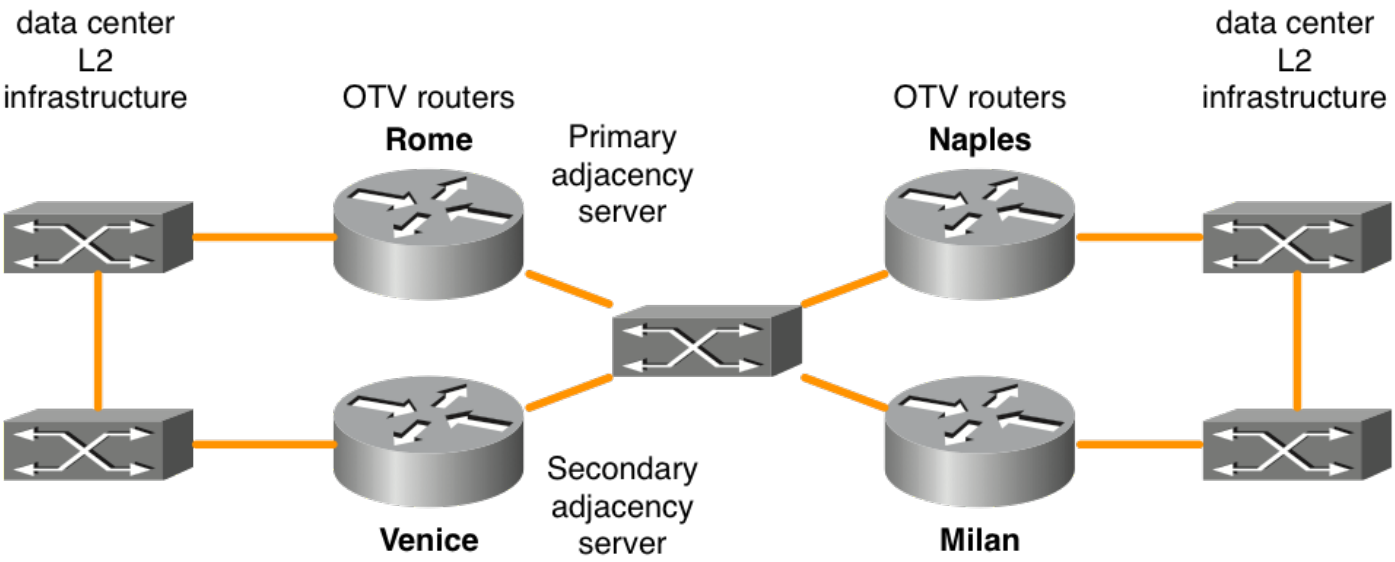
Le parti nere dell'identificatore devono corrispondere su tutti i router OTV che partecipano alla sovrapposizione. È possibile modificare la parte dell'identificatore in rosso. All'identificatore di rete più basso in un sito viene assegnato il numero ordinale 0 e le VLAN con numero pari vengono

quindi inoltrate. L'identificatore di rete più alto di un sito riceve il numero ordinale 1 e inoltra il numero dispari delle VLAN.

Esempi di configurazione

Unicast

Figura 9. Esempio di configurazione unicast



Configurazione 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
 !
```

Configurazione Venezia:

```
!
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
 !
```

Configurazione Napoli:

```
!
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
```

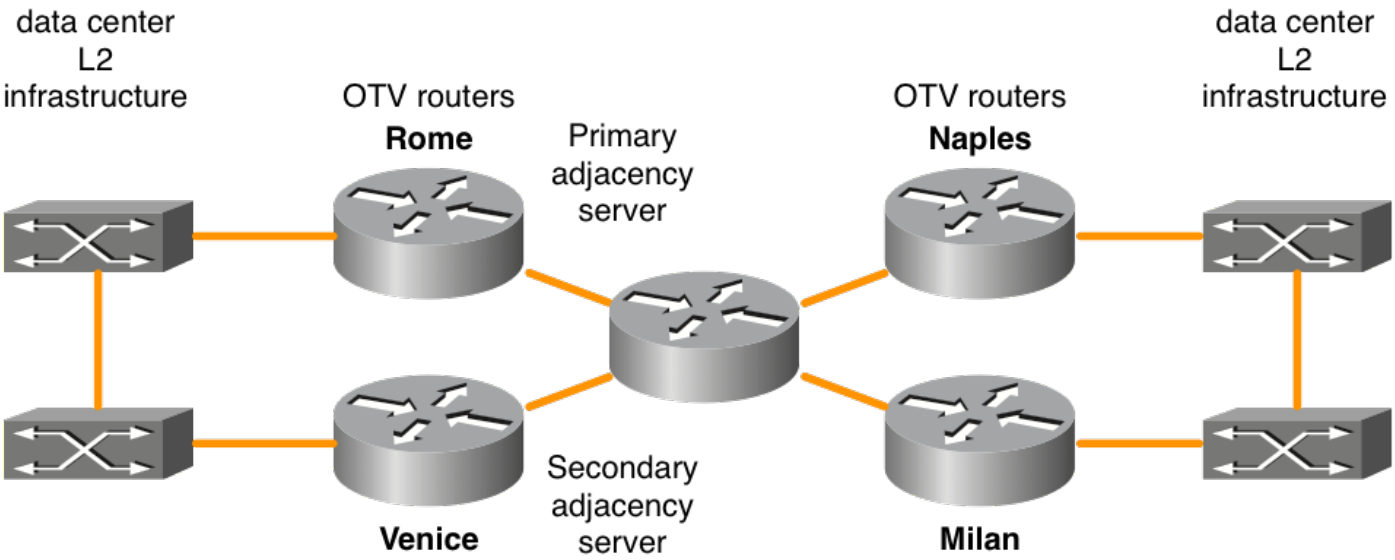
```
 !
!
```

Configurazione Milano:

```
!
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. Esempio di configurazione multicast



Configurazione 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
 !
```

Configurazione Venezia:

```
!
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
 !
```

Configurazione Napoli:

```
!
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
 !
!
```

Configurazione Milano:

```
!
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
 !
!
```

Domande frequenti

Q) Le VLAN private sono supportate in combinazione con OTV?

A) Sì, non è richiesta una configurazione speciale in OTV. Nella configurazione VLAN privata, verificare che le porte dello switch collegate all'interfaccia OTV L2 siano configurate in modalità promiscua.

Q) OTV è supportato con IPSEC crypto?

A) Sì, è supportata la configurazione della mappa crittografica sull'interfaccia di join. Per il supporto della crittografia da parte di OTV, non è necessaria alcuna configurazione speciale. Tuttavia, la configurazione crittografica aggiunge un ulteriore sovraccarico che deve essere compensato dall'aumento della MTU della WAN rispetto alla MTU della LAN. Se ciò non è possibile, è necessario richiedere la frammentazione OTV. Le prestazioni OTV sono limitate a quelle dell'hardware IPSEC.

Q) OTV è supportato da MACSEC?

A) Sì, ASR1001-X include il supporto MACSEC per le interfacce incorporate. OTV funziona con MACSEC configurato sulle interfacce LAN e/o WAN. Le prestazioni OTV sono limitate a quelle dell'hardware MACSEC.

Q) È possibile utilizzare un'interfaccia di loopback come interfaccia di join?

A) No, Solo Ethernet, Portchannel o POS possono essere utilizzati come interfacce di giunzione OTV. L'interfaccia di join di loopback OTV è inclusa nella roadmap, ma al momento non è prevista una release.

Q) È possibile usare un'interfaccia tunnel come interfaccia di join?

A)No, i tunnel GRE, DMVPN o qualsiasi altro tipo di tunnel non sono supportati come interfacce di join. Come interfacce join OTV è possibile utilizzare solo interfacce Ethernet, Portchannel o POS.

Q) Le diverse interfacce Overlay possono utilizzare interfacce L2 e/o join diverse?

A) Tutte le interfacce di sovrapposizione devono puntare alla stessa interfaccia di collegamento. Tutte le sovrapposizioni devono essere collegate alla stessa interfaccia fisica per la connettività L2 verso il centro dati.

Q) La VLAN del sito OTV può essere su un'interfaccia fisica diversa dalle VLAN estese OTV?

A) La VLAN del sito OTV e le VLAN estese devono trovarsi sulla stessa interfaccia fisica.

Q) Quale funzione è richiesta per OTV?

A) Servizi IP avanzati (AIS) o Servizi Enterprise avanzati (AES) sono richiesti per OTV.

Q) È richiesta una licenza separata per OTV su piattaforme a configurazione fissa?

A) No, a condizione che ASR1000 sia eseguito con i servizi di consulenza o con il livello di avvio configurato, è disponibile OTV.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).