

# Risoluzione dei problemi relativi a errori di OMP e azioni TLOC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica di OMP](#)

[Scenario di errore EIGRP](#)

[Scenario errore OMP](#)

[Errore diretto](#)

[Errore indiretto](#)

[TLOC-Action](#)

---

## Introduzione

Questo documento descrive la risoluzione dei problemi relativi agli scenari di errore di Overlay Management Protocol (OMP) e le best practice per fornire resilienza della rete in Cisco SD-WAN.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza della soluzione SD-WAN (Software Defined Wide Area Network) di Cisco.

### Componenti usati

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

- Cisco IOS Catalyst SD-WAN Manager aka vManage
- Cisco IOS Catalyst SD-WAN Validator aka vBond
- Cisco IOS Catalyst SD-WAN Controller alias vSmart
- Dispositivi vEdge

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.

# Panoramica di OMP

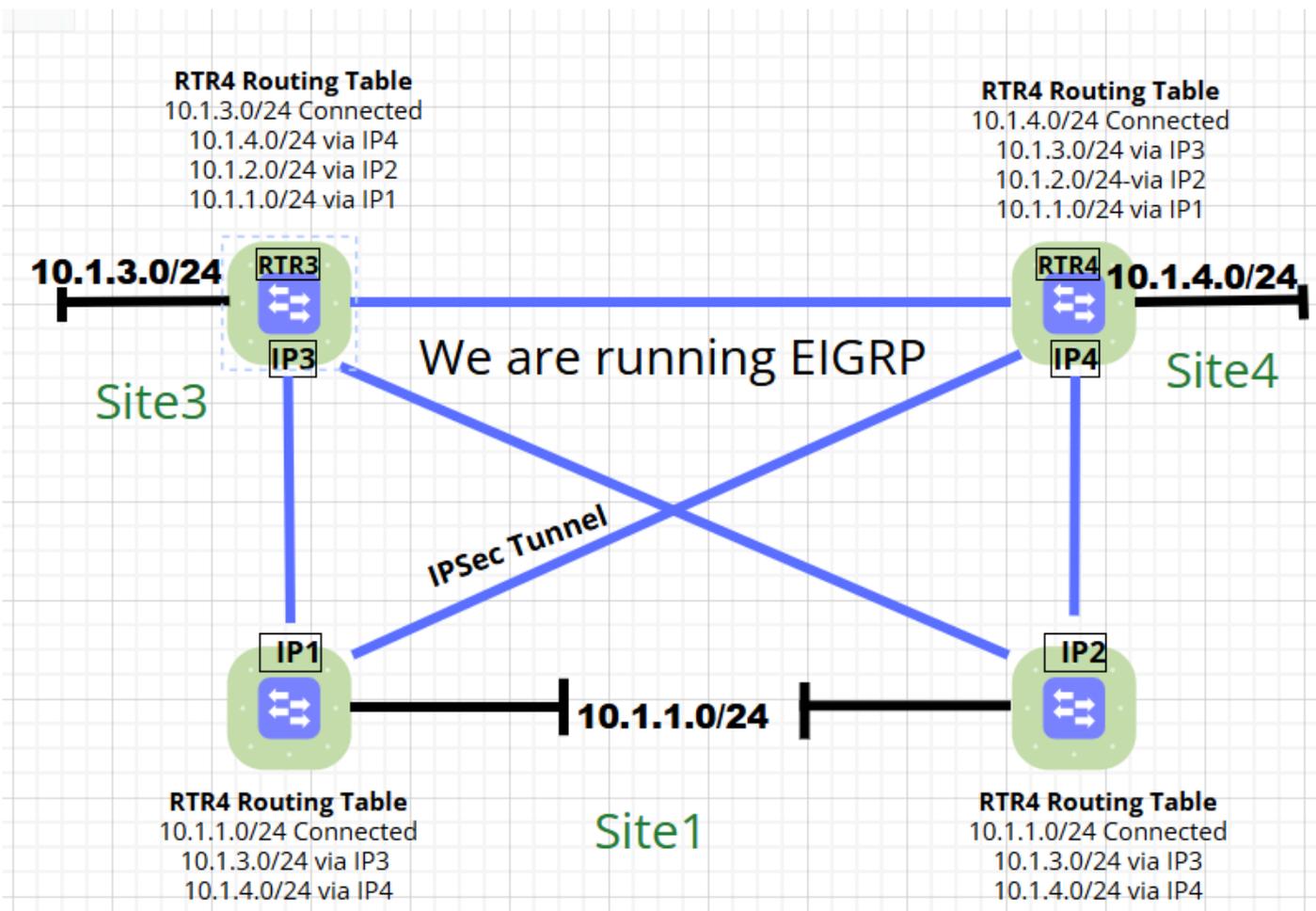
Come è noto, il dispositivo Cisco SD-WAN Edge condivide le route solo con il controller Catalyst SD-WAN. Affinché una route sia valida e installata nella relativa tabella di inoltro:

- Il TLOC (Transport Locator) dell'hop successivo deve essere raggiungibile, ovvero il dispositivo Edge deve avere un percorso valido per il TLOC.
- Il TLOC a cui punta è attivo. Affinché un TLOC sia attivo, è necessario associare a tale TLOC una sessione di inoltro bidirezionale (BFD) attiva. Le sessioni BFD vengono stabilite da ciascun dispositivo che crea una sessione BFD separata con ciascuno dei TLOC remoti. Se una sessione BFD diventa inattiva, il controller Cisco Catalyst SD-WAN rimuove tutte le route OMP che puntano a tale TLOC dalla tabella di inoltro.
- La route OMP deve essere calcolata nel modo migliore.

Sebbene tutte queste affermazioni siano logiche e semplici, esiste una differenza significativa tra OMP e i protocolli di routing tradizionali, ad esempio il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) e OSPF (Open Shortest Path First), durante gli scenari di errore.

## Scenario di errore EIGRP

Nella rete successiva, ci sono tre siti, ossia Sito1, Sito3 e Sito4 con router RTR1/RTR2, RTR3 e RTR4 rispettivamente con una singola connessione WAN. Il protocollo EIGRP di routing tradizionale viene eseguito su IPsec e IP1, IP2, IP3 e IP4 sono gli indirizzi IP dell'interfaccia WAN nelle rispettive posizioni.



La rete deve essere interrotta, per il momento focalizzandosi su RTR3 e RTR4. In RTR3, il percorso per raggiungere il sito 10.1.4.0/24 consiste in un tunnel diretto tra RTR3 e RTR4. Se il tunnel non funziona, come reagisce l'EIGRP in questo caso? Non appena il tunnel diventa inattivo, EIGRP invia una query ai router adiacenti per la rete 10.1.4.0/24 e, in base alle risposte ricevute, la esamina e installa il nuovo percorso per la destinazione nella tabella di routing dopo il calcolo del miglior percorso.

Questa è una spiegazione molto semplice del tradizionale processo di convergenza dei protocolli di routing. Pertanto, i protocolli di routing tradizionali come EIGRP sono in grado di eseguire il ricalcolo della rete:

- Quando il percorso corrente verso una destinazione diventa inattivo
- Quando non esistono successori possibili per una destinazione
- Quando si verifica una modifica della topologia

## Scenario errore OMP

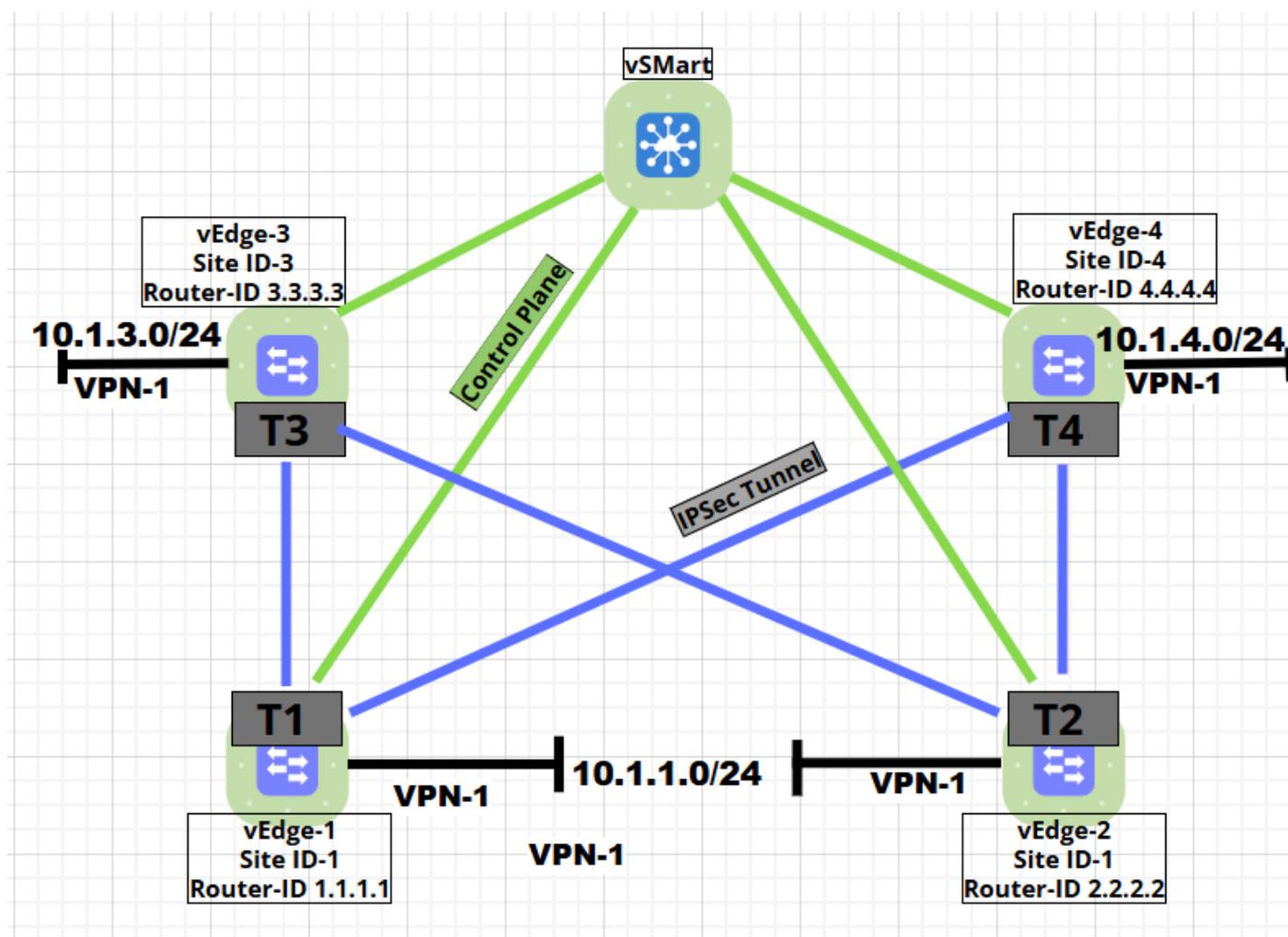
I due scenari di errore per OMP sono illustrati di seguito:

1. Errore diretto
2. Errore indiretto

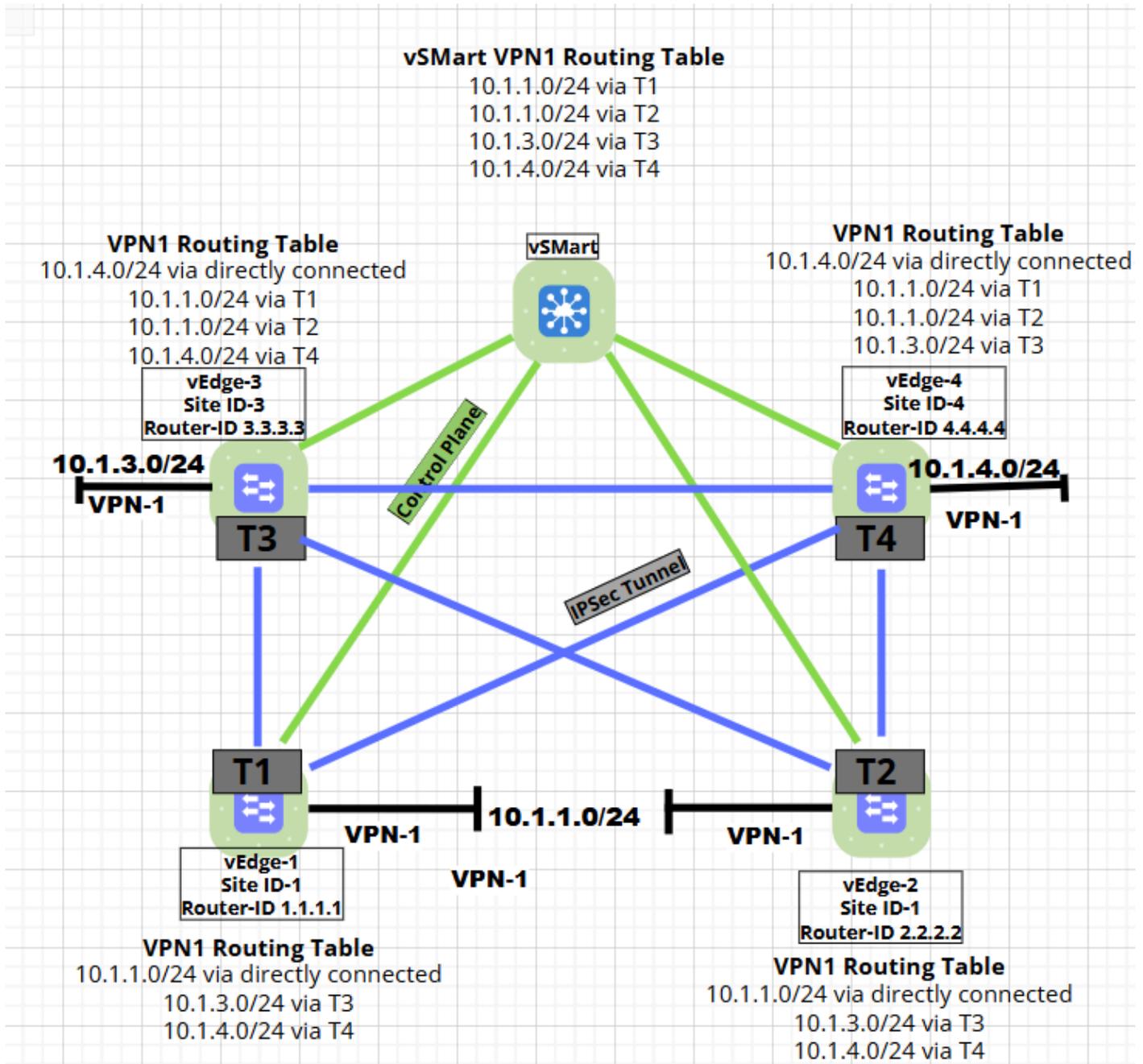
Errore diretto

Nella Topologia successiva, sono presenti tre siti con una singola connessione di trasporto.

Sito	Router	Transport Locator (TLOC)	IP di sistema	Subnet
Site1	vEdge 1	T1	1.1.1.1	10.1.1.0/24
	vEdge 2	T2	2.2.2.2	
Sito-3	vEdge 3	T3	3.3.3.3	10.1.3.0/23
Sito-4	vEdge 4	T4	4.4.4.4	10.1.4.0/24



Si supponga che tutto sia impostato sui valori predefiniti sul controller Catalyst SD-WAN. I dispositivi vEdge condividono le informazioni di routing direttamente con il controller Catalyst SD-WAN e il controller le condivide con tutti i dispositivi vEdge. La topologia seguente mostra la tabella di routing per tutti i router:



Al momento, tutte le sessioni BFD sono attive.

vEdge-DC1# show bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
1.1.1.1	1	up	mpls	mpls	60.1.1.1
2.2.2.2	1	up	mpls	mpls	60.1.1.1
4.4.4.4	2	up	mpls	mpls	60.1.1.1

vEdge-DC1# show omp routes vpn 20 | t

Code:

- C -> chosen
- I -> installed
- Red -> redistributed
- Rej -> rejected

L -> looped  
 R -> resolved  
 S -> stale  
 Ext -> extranet  
 Inv -> invalid  
 Stg -> staged  
 IA -> On-demand inactive  
 U -> TLOC unresolved

VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
20	10.1.1.0/24	2.2.2.2	43	1005	C,I,R	installed	1.1.1.1	
			2.2.2.2	37	1006	C,I,R	installed	
20	10.1.3.0/24	0.0.0.0	66	1005	C,Red,R	installed	3.3.3.3	
20	10.1.4.0/24	2.2.2.2	45	1006	C,I,R	installed	4.4.4.4	

Se la connettività tra vEdge3 e vEdge4 è disabilitata, quando il tunnel si interrompe, anche le sessioni BFD di vEdge3 e vEdge4 si interromperanno. In questo modo le rispettive route verranno contrassegnate come 'Invalid' e 'TLOC Unresolve'. Come si può vedere nell'output successivo:

vEdge3# show bfd sessions

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
1.1.1.1	1	up	mpls	mpls	60.1.1.1
2.2.2.2	1	up	mpls	mpls	60.1.1.1
4.4.4.4	4	down	mpls	mpls	60.1.1.1

vEdge3# show omp routes vpn 20 | t

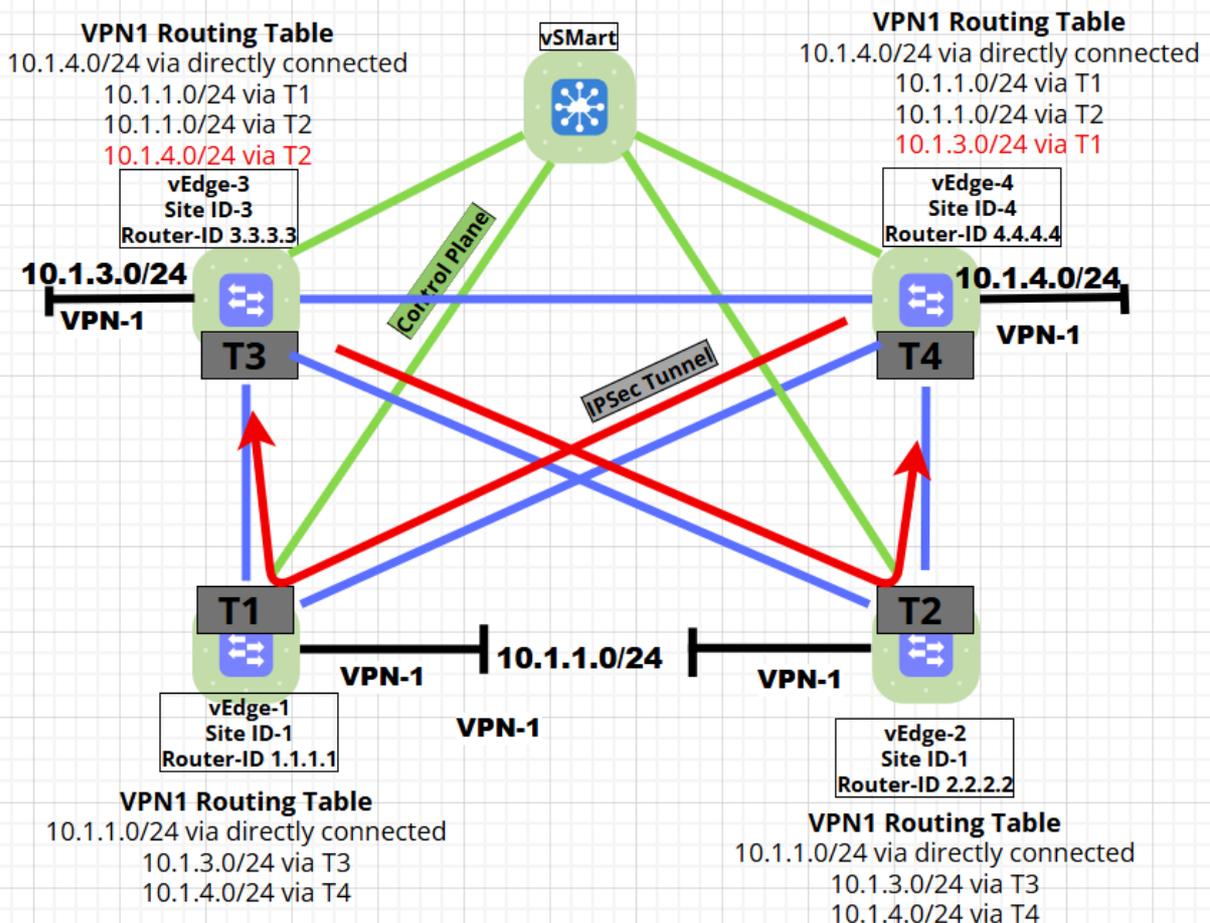
Code:

C -> chosen  
 I -> installed  
 Red -> redistributed  
 Rej -> rejected  
 L -> looped  
 R -> resolved  
 S -> stale  
 Ext -> extranet  
 Inv -> invalid  
 Stg -> staged  
 IA -> On-demand inactive  
 U -> TLOC unresolved

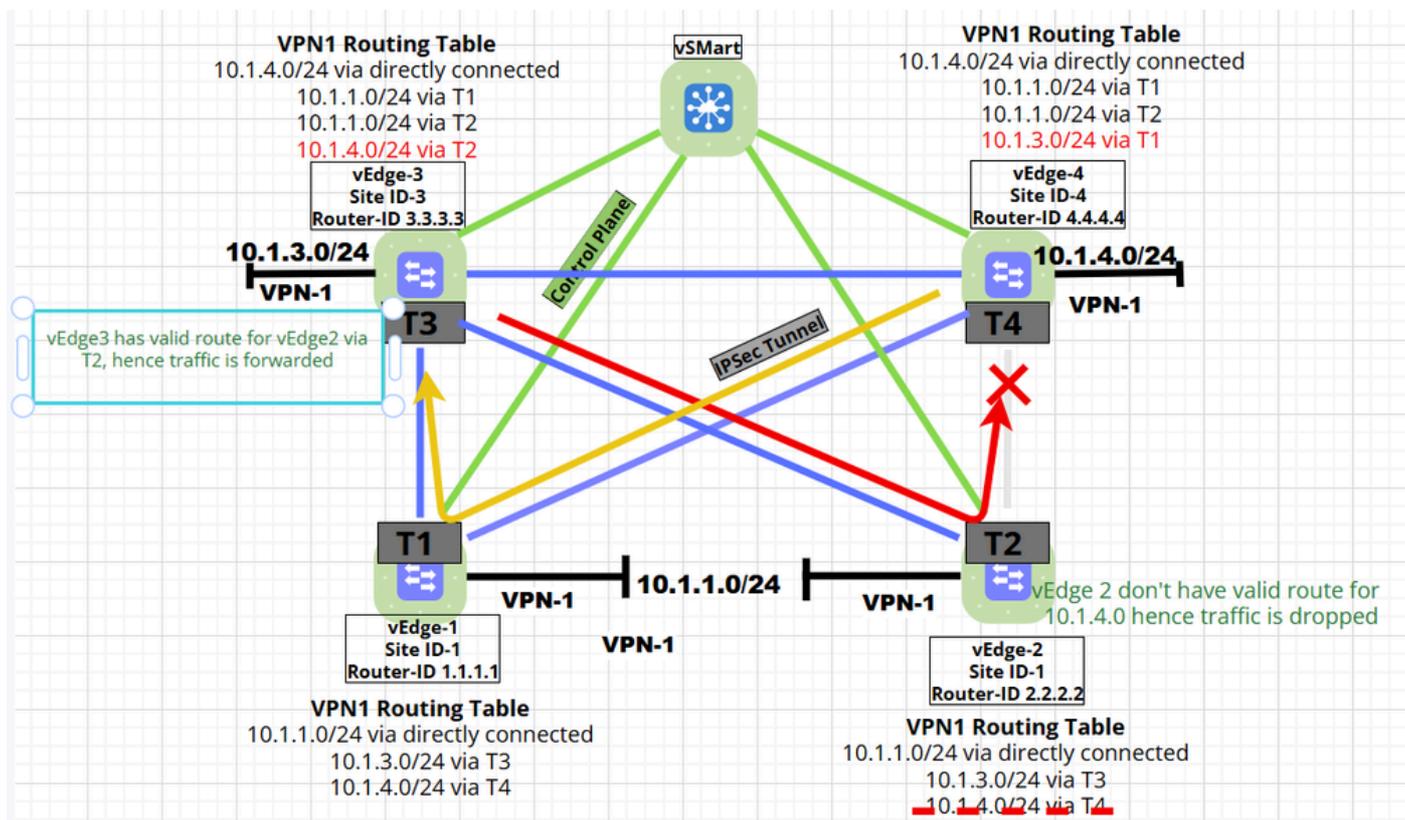
VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP	COLOR
1	10.1.1.0/24	2.2.2.2	43	1005	C,I,R	installed	1.1.1.1	
			2.2.2.2	37	1006	C,I,R	installe	
1	10.1.3.0/24	0.0.0.0	66	1005	C,Red,R	installed	3.3.3.3	
1	10.1.4.0/24	2.2.2.2	45	1006	Inv,U	installed	4.4.4.4	

## Errore indiretto

Per comprendere il concetto di 'errore indiretto', si supponga che i criteri di controllo siano stati definiti in modo da modificare l'hop successivo su vEdge3 per la route 10.1.4.0/24 tramite vEdge2 e che su vEdge4 l'hop successivo per la route 10.1.3.0/24 sia stato modificato in vEdge1. In altre parole, per il traffico tra vEdge 3 e 4, vEdge 2 e 1 sono stati inseriti come hop intermedi. Come si può vedere nel diagramma seguente:



Se si verifica un errore di rete che determina una perdita di connettività tra vEdge2 e vEdge4, mentre il tunnel di sovrapposizione tra T2 e T4 non è attivo, vEdge3 dispone ancora di un percorso valido per 10.1.4.0 tramite T2. Pertanto, invia traffico a vEdge2. vEdge2 non ha un tunnel valido con vEdge4, quindi le route non saranno più attive su di esso, quindi il traffico verrà eliminato.



Sulla base dei registri e dei test precedenti, si può concludere che:

- Con OMP, non è possibile eseguire il rilevamento automatico dei peer di routing e degli hop successivi
- Quando un tunnel diventa inattivo non è necessario ricalcolare la topologia
- Le route OMP a un prefisso di destinazione non cambiano mai quando un tunnel diventa inattivo. L'unico cambiamento che avviene è la raggiungibilità dell'hop successivo, ovvero il TLOC.
- In caso di errore di sovrapposizione diretta, è necessario fornire una ridondanza tunnel con più tunnel alla stessa destinazione.
- Prestare particolare attenzione quando si introducono hop/hop intermedi nel percorso di sovrapposizione e fornire una ridondanza del tunnel per evitare la mancanza di traffico.

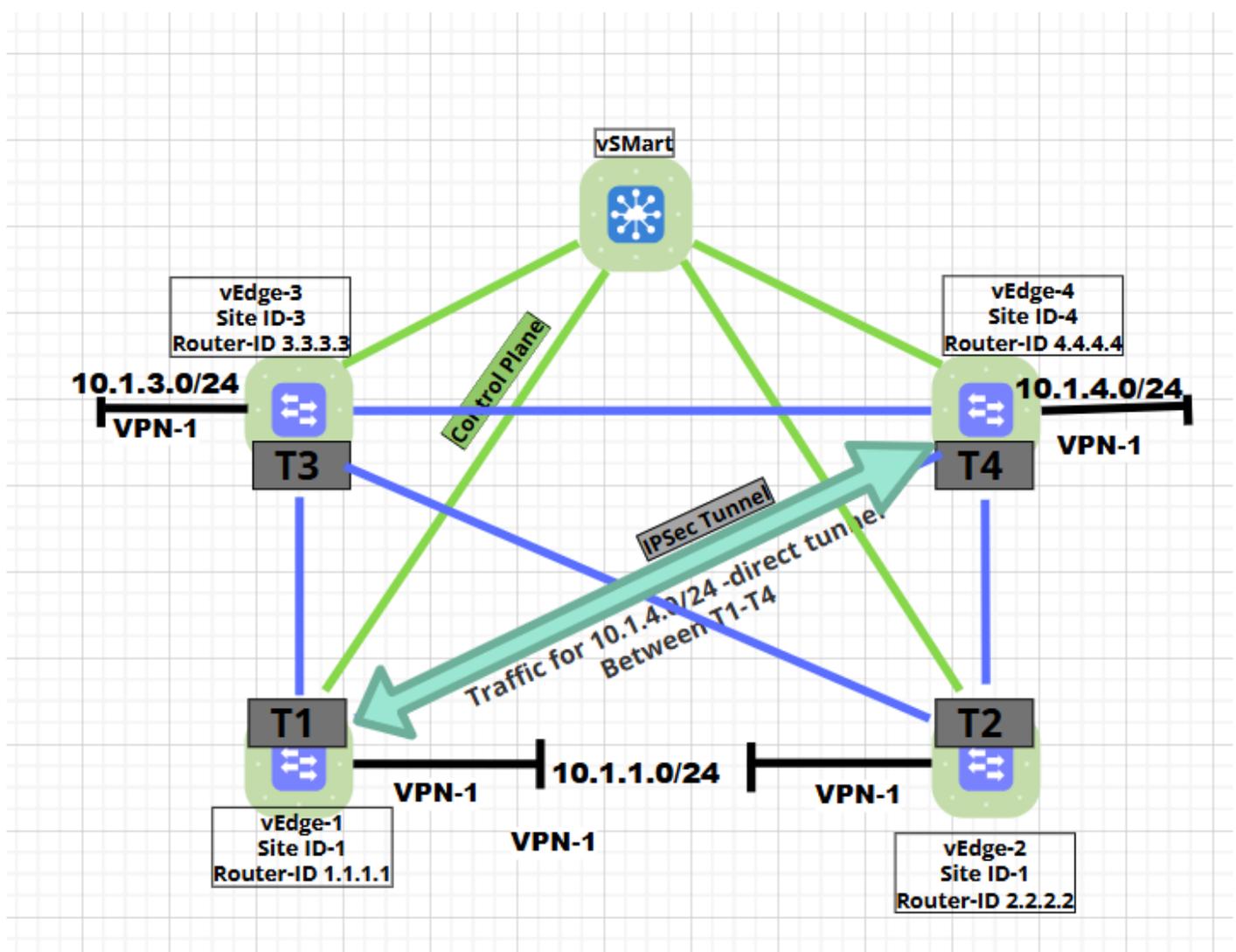
Per impostazione predefinita, OMP non esegue il ricalcolo o la reindirizzamento in caso di errore di sovrapposizione. Per risolvere questo problema, è possibile attivare una funzionalità denominata 'TLOC-Action' tramite una policy di controllo.

## TLOC-Action

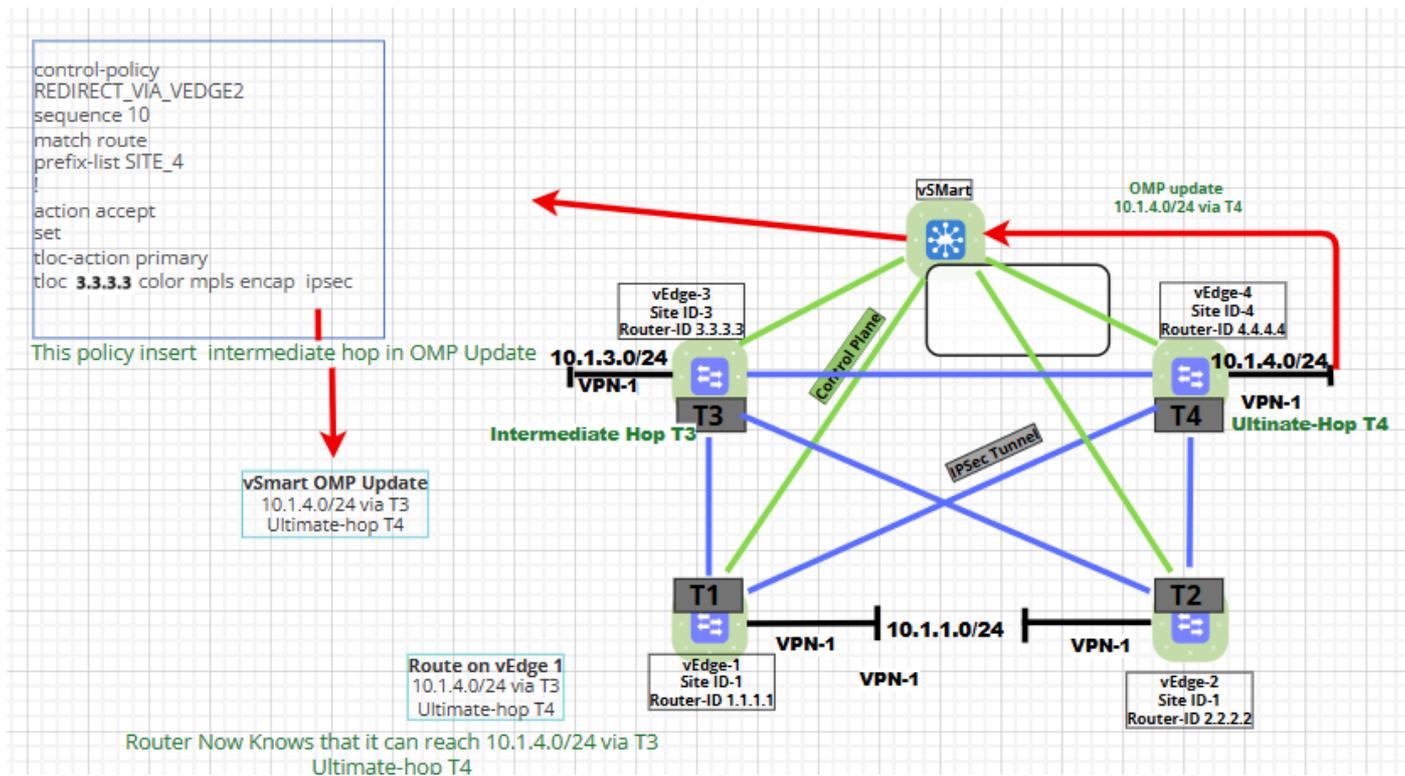
- In Cisco SD-WAN, un'azione TLOC' all'interno di una policy di controllo consente l'inserimento di un hop intermedio (TLOC) da utilizzare per l'inoltro del traffico mantenendo la visibilità sul percorso completo dall'origine alla destinazione. Ciò significa che l'impostazione dell'opzione TLOC action consente al controller Cisco Catalyst SD-WAN di eseguire il tracciamento end-to-end del percorso al dispositivo di destinazione finale. Se il percorso diventa inattivo, il controller informa i router edge della WAN che hanno ricevuto la route OMP.

- Fornisce un percorso di backup in caso di guasto del collegamento primario, migliorando così la resilienza della rete e la tolleranza di errore all'interno della rete overlay SD-WAN. È un modo per controllare il modo in cui il traffico viene instradato attraverso la rete manipolando i TLOC utilizzati per raggiungere una destinazione.
- Quando un'azione TLOC viene definita in un criterio, indica al controller SD-WAN di inserire un TLOC intermedio nel calcolo del percorso, ovvero il traffico verrà indirizzato al percorso di backup specificato prima di raggiungere la destinazione finale, se necessario.
- Ciò è particolarmente utile negli scenari in cui si desidera garantire la connettività anche in caso di interruzione di un collegamento principale, reindirizzando automaticamente il traffico su un percorso diverso (tramite il TLOC specificato).

Per una migliore comprensione della topologia successiva, è opportuno focalizzarsi su vEdge2, vEdge3 e vEdge4. Al momento non è definito alcun criterio e il traffico dati per 10.1.4.0/24 su vEdge3 sta attraversando un tunnel diretto tra T3 e T4.



Per garantire la tolleranza di errore e la resilienza della rete, i criteri di controllo sono configurati per reindirizzare il traffico su un percorso diverso (tramite il TLOC specificato).



- vEdge4 invia l'aggiornamento OMP per la rete 10.1.4.0/24 a connessione diretta con l'hop successivo T4 al controller Catalyst SD-WAN come '10.1.4.0/24 via T4'.
- Questa route corrisponde a un criterio di controllo configurato sul controller SD-WAN e imposta un nuovo TLOC e TLOC-Actions in base al criterio definito, ovvero inserisce il nuovo 'TLOC intermedio'.
- Il controller annuncia il percorso OMP verso vEdge1 con due hop successivi: TLOC intermedio (T3, 3.3.3.3) e TLOC finale (next-hop-T4 del percorso originale). In questo modo vEdge1 è in grado di rilevare che il prefisso di destinazione 10.1.4.0/24 è raggiungibile tramite T2 e T4.

Ora, in base all'azione TLOC definita vEdge1, inoltra il traffico per 10.1.4.0/24. È quindi possibile definire questi quattro tipi di azioni TLOC nella policy del control plane:

1. Strict (impostazione predefinita) - Il parametro 'TLOC-Action strict' definisce il traffico tra vEdge1 e vEdge4 come traffico di tipo T3 (hop intermedio) e il traffico deve diminuire se il tunnel tra vEdge1 e vEdge4 diventa inattivo.
2. Primario - 'TLOC-Action primary' definisce il traffico tra vEdge1 e vEdge4 che passa attraverso l'hop intermedio T3 (3.3.3.3). Se il tunnel di sovrapposizione non funziona, il controller SD-WAN informa vEdge1 e il traffico viene instradato al tunnel diretto verso T4.
3. Backup - Il 'backup TLOC-Action' definisce che il traffico tra vEdge1 e vEdge4 va direttamente al LOC finale (next-hop -T4 del percorso originale) e se il tunnel di sovrapposizione diretta tra vEdge1 e vEdge4 va giù, il controller SD-WAN informa vEdge1 e il traffico passa attraverso l'hop intermedio T3.
4. Equal-Cost Multi-Path (ECMP) - 'TLOC-Action ECMP' specifica che in circostanze normali la comunicazione tra vEdge1 e vEdge4 viene bilanciata dal carico tramite l'hop intermedio T3 e l'hop finale T4.

## 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).