Fehlerbehebung: OMP-Fehler und TLOC-Aktion

Inhalt

Einleitung

In diesem Dokument werden Fehlerbehebungsszenarien für das Overlay Management Protocol (OMP) und Best Practices zur Gewährleistung der Netzwerkausfallsicherheit im Cisco SD-WAN beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco Software Defined Wide Area Network (SD-WAN)-Lösung verfügen.

Verwendete Komponenten

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

- Cisco IOS Catalyst SD-WAN Manager, auch vManage genannt
- Cisco IOS Catalyst SD-WAN Validator (vBond)
- Cisco IOS Catalyst SD-WAN Controller (vSmart)
- vEdge-Geräte

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

OMP im Überblick

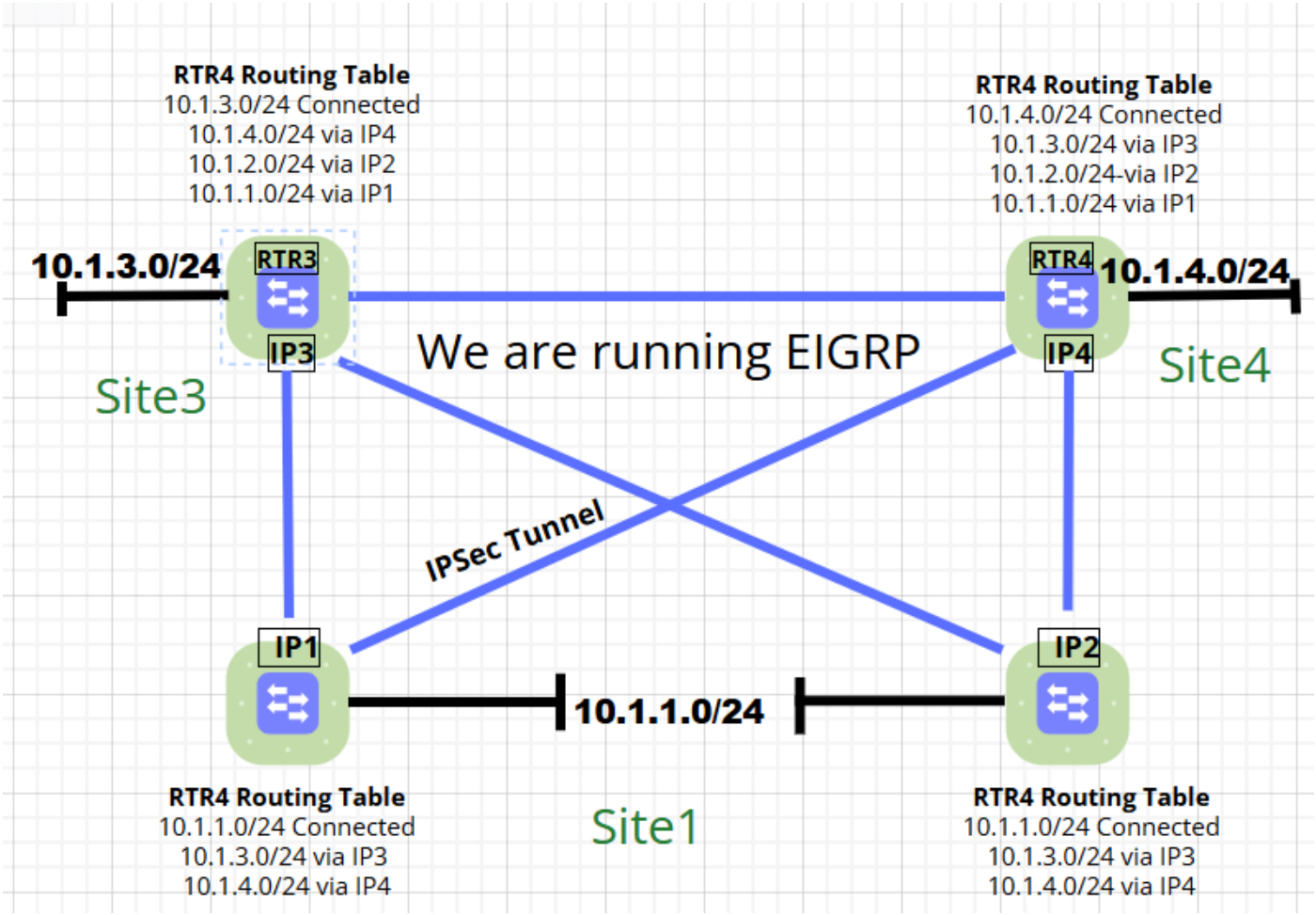
Wie Sie wissen, gibt das Cisco SD-WAN Edge-Gerät die Routen nur für den Catalyst SD-WAN-Controller frei. Damit eine Route gültig ist und in ihrer Weiterleitungstabelle installiert wird:

- Der Next Hop Transport Locator (TLOC) muss erreichbar sein, d. h. das Edge-Gerät muss über eine gültige Route für den TLOC verfügen.
- Der TLOC, auf den er zeigt, ist aktiv. Damit ein TLOC aktiv ist, muss diesem TLOC eine aktive BFD-Sitzung (Bidirectional Forwarding) zugeordnet werden. BFD-Sitzungen werden von jedem Gerät eingerichtet, das eine separate BFD-Sitzung mit jedem der Remote-TLOCs erstellt. Wenn eine BFD-Sitzung inaktiv wird, entfernt der Cisco Catalyst SD-WAN Controller alle OMP-Routen, die auf diesen TLOC verweisen, aus der Weiterleitungstabelle.
- Die OMP-Route muss am besten berechnet werden.

Obwohl alle diese Anweisungen logisch und direkt sind, gibt es einen signifikanten Unterschied zwischen OMP und herkömmlichen Routing-Protokollen wie Enhanced Interior Gateway Routing Protocol (EIGRP) und Open Shortest Path First (OSPF) während Ausfallszenarien.

EIGRP-Fehlerszenario

Im nächsten Netzwerk gibt es drei Standorte, nämlich Site1, Site3 und Site4 mit den Routern RTR1/RTR2, RTR3 und RTR4 mit jeweils einer WAN-Verbindung. Das traditionelle Routing-Protokoll EIGRP wird über IPSec ausgeführt, und IP1, IP2, IP3 und IP4 sind die IP-Adressen der WAN-Schnittstelle an den jeweiligen Standorten.



Das Netzwerk muss defekt sein, wobei der Schwerpunkt vorerst auf RTR3 und RTR4 liegt. Auf RTR3 erfolgt die Route zum 10.1.4.0/24 über einen direkten Tunnel zwischen RTR3-RTR4. Wie reagiert EIGRP in diesem Fall, wenn der Tunnel ausfällt? Sobald der Tunnel ausfällt, wird EIGRP ausgeführt und eine Abfrage an benachbarte Router für das Netzwerk 10.1.4.0/24 gesendet. Basierend auf den erhaltenen Antworten wird das Netzwerk überprüft und der neue Pfad für das Ziel in der Routing-Tabelle installiert, um den besten Pfad zu berechnen.

Dies ist eine sehr einfache Erklärung des herkömmlichen Konvergenzprozesses für Routing-Protokolle. Herkömmliche Routing-Protokolle wie EIGRP können daher eine Neuberechnung des Netzwerks vornehmen:

- Wenn die aktuelle Route zu einem Ziel ausfällt
- Wenn es keine praktikablen Nachfolger für ein Ziel gibt
- Bei Topologieänderungen

OMP-Fehlerszenario

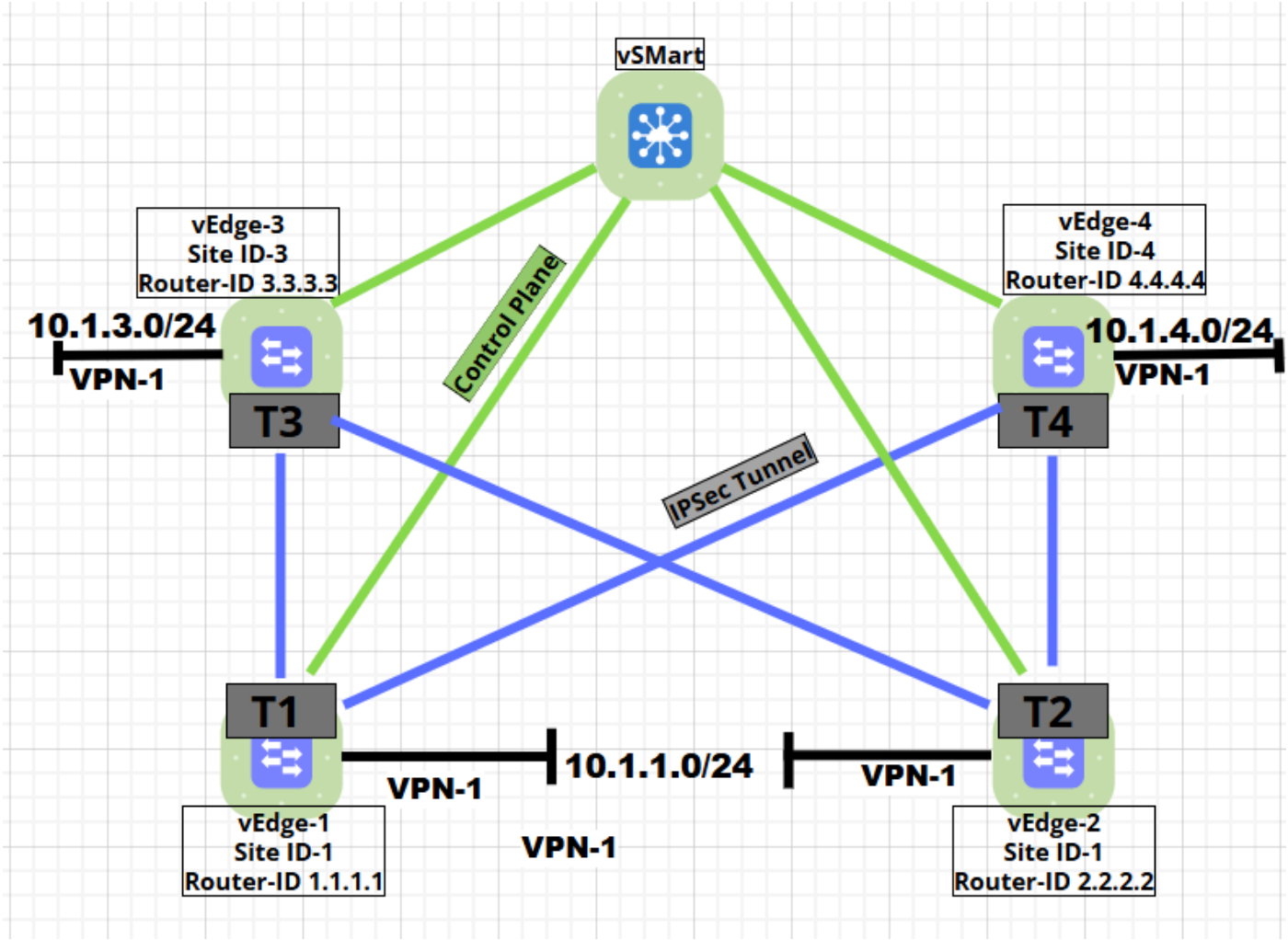
Die beiden Fehlerszenarien für OMP werden hier erläutert:

1. Direkter Ausfall
2. Indirekter Fehler

Direkter Ausfall

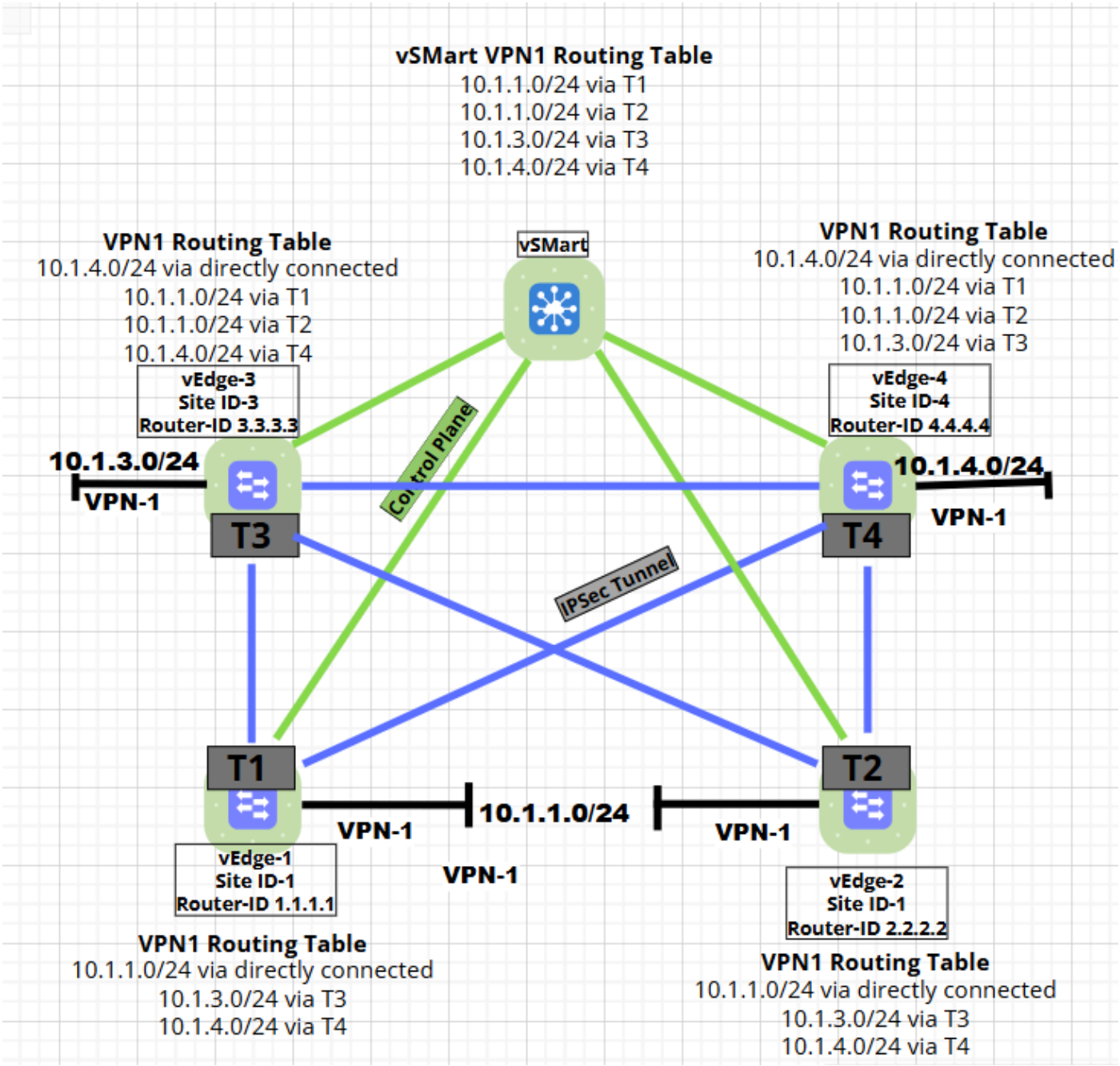
In der nächsten Topologie gibt es drei Standorte mit einer Transportverbindung.

Standort	Router	Transport Locator (TLOC)	System-IP	Subnetz
SIte1	vEdge 1 vEdge 2	T1 T2	1.1.1.1 2.2.2.2	10.1.1.0/24
Standort-3	vEdge 3	T3	3.3.3.3	10.1.3.0/23
Standort-4	vEdge 4	T4	4.4.4.4	10.1.4.0/24



Angenommen, auf dem Catalyst SD-WAN-Controller ist alles auf die Standardeinstellung gesetzt. Die vEdge-Geräte geben die Routing-Informationen direkt an den Catalyst SD-WAN-Controller

weiter, und der Controller teilt sie mit allen vEdge-Geräten. Die nächste Topologie zeigt die Routing-Tabelle für alle Router:



Derzeit sind alle BFD-Sitzungen aktiv.

```
vEdge-DC1# show bfd sessions
                                       SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID  STATE       COLOR            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

                                        PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER    ID     LABEL    STATUS    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
```

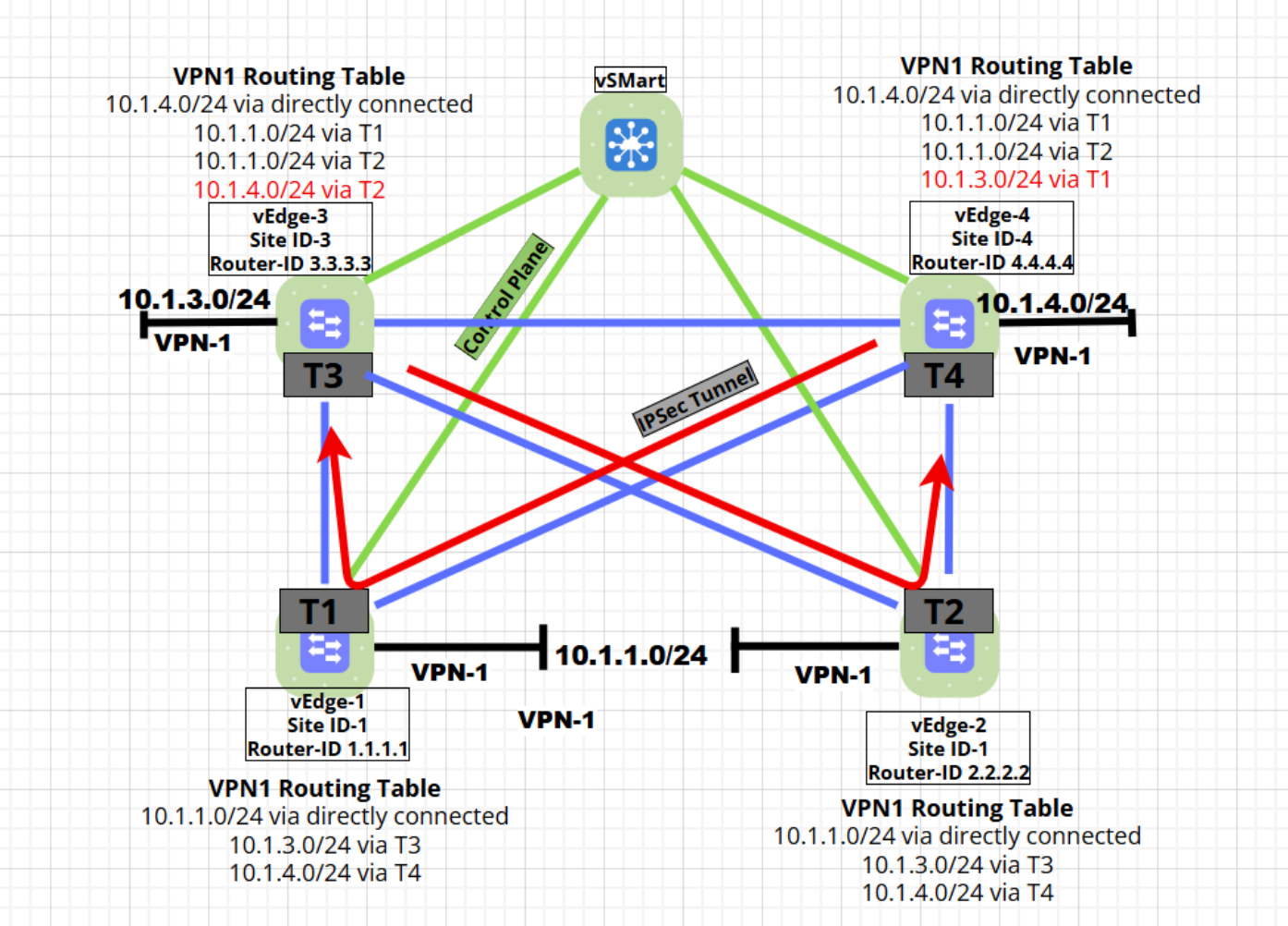
Wenn die Verbindung zwischen vEdge3 und vEdge4 deaktiviert ist, werden bei einem Tunnelausfall auch die BFD-Sitzungen von vEdge3 und vEdge4 deaktiviert. Dies veranlasst sie, die jeweiligen Routen als 'Ungültig' und 'TLOC Unaufgelöst' zu markieren. Das können Sie in der nächsten Ausgabe sehen:

```
vEdge3# show bfd sessions
                                    SOURCE TLOC      REMOTE TLOC
SYSTEM IP        SITE ID  STATE     COLOR            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

                                        PATH                      ATTRIBUTE
VPN    PREFIX              FROM PEER    ID     LABEL    STATUS    TYPE       TLOC IP          COLOR
-------------------------------------------------------------------------------------------------------
1     10.1.1.0/24          2.2.2.2       43     1005       C,I,R                installed       1.1
                                       2.2.2.2          37     1006       C,I,R                installe
```

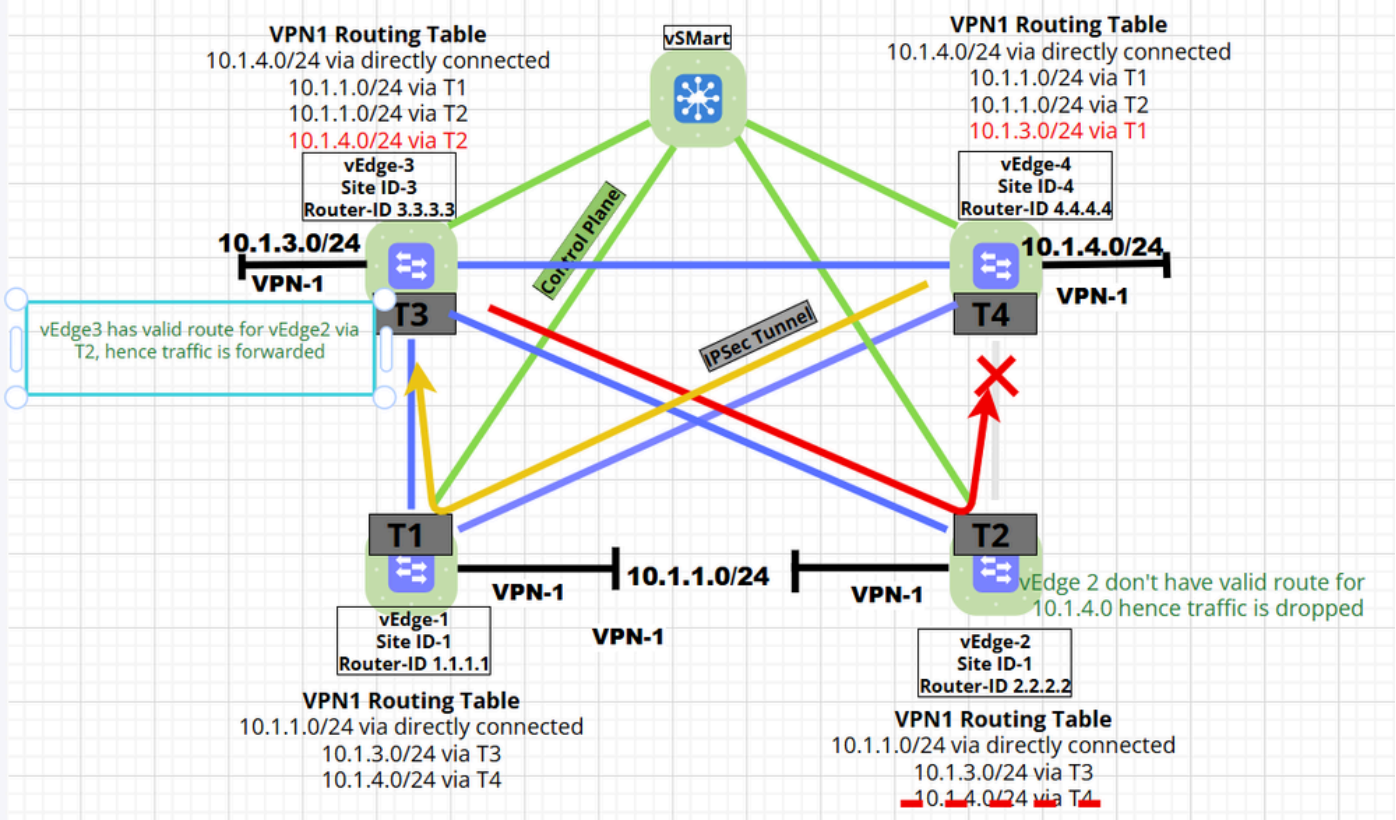
```
1     10.1.3.0/24          0.0.0.0          66      1005        C,Red,R           installed       3.3.3.
1      10.1.4.0/24         2.2.2.2          45      1006        Inv,U               installed       4.4
```

Indirekter Fehler

Um den Begriff "indirekter Fehler" zu verstehen, gehen Sie davon aus, dass die Kontrollrichtlinie so definiert ist, dass der nächste Hop auf vEdge3 für die Route 10.1.4.0/24 über vEdge2 geändert wird, und auf vEdge4 wird der nächste Hop für 10.1.3.0/24 in vEdge1 geändert. Mit anderen Worten: Für den Datenverkehr zwischen vEdge 3 und 4 wurden vEdge 2 und 1 als Zwischen-Hops eingefügt. Dies wird im folgenden Diagramm veranschaulicht:



Bei einem Netzwerkausfall, der zu einem Verbindungsverlust zwischen vEdge2 und vEdge4 führt, während der Overlay-Tunnel zwischen T2-T4 ausfällt, verfügt vEdge3 über eine gültige Route für 10.1.4.0 über T2. Daher wird Datenverkehr an vEdge2 gesendet. vEdge2 verfügt nicht über einen gültigen Tunnel mit vEdge4, daher sind Routen auf dem Tunnel nicht mehr aktiv, wodurch der Datenverkehr verworfen wird.



Auf der Grundlage früherer Protokolle und Tests kann der Schluss gezogen werden, dass

- Mit OMP gibt es keine automatische Erkennung von Routing-Peers und Next-Hops.
- Beim Ausfall eines Tunnels findet keine Neuberechnung der Topologie statt
- Die OMP-Routen zu einem Zielpräfix ändern sich nie, wenn ein Tunnel ausfällt. Die einzige Änderung, die eintritt, ist die Erreichbarkeit des nächsten Hop, also der TLOC.
- Bei einem Ausfall des direkten Overlays muss eine Tunnel-Redundanz mit mehreren Tunneln zum gleichen Ziel bereitgestellt werden.
- Bei der Einführung von Hop/Hops als Zwischenstufe in den Overlay-Pfad ist besondere Vorsicht geboten, und es muss für Tunnelredundanz gesorgt werden, um ein Verkehrsdefizit zu vermeiden.

Jetzt wissen Sie, dass OMP standardmäßig keine Neuberechnung oder Umleitung bei Overlay-Fehlern vornimmt. Um dieses Problem zu beheben, können Sie eine Funktion namens 'TLOC-Action' über eine Kontrollrichtlinie aktivieren.

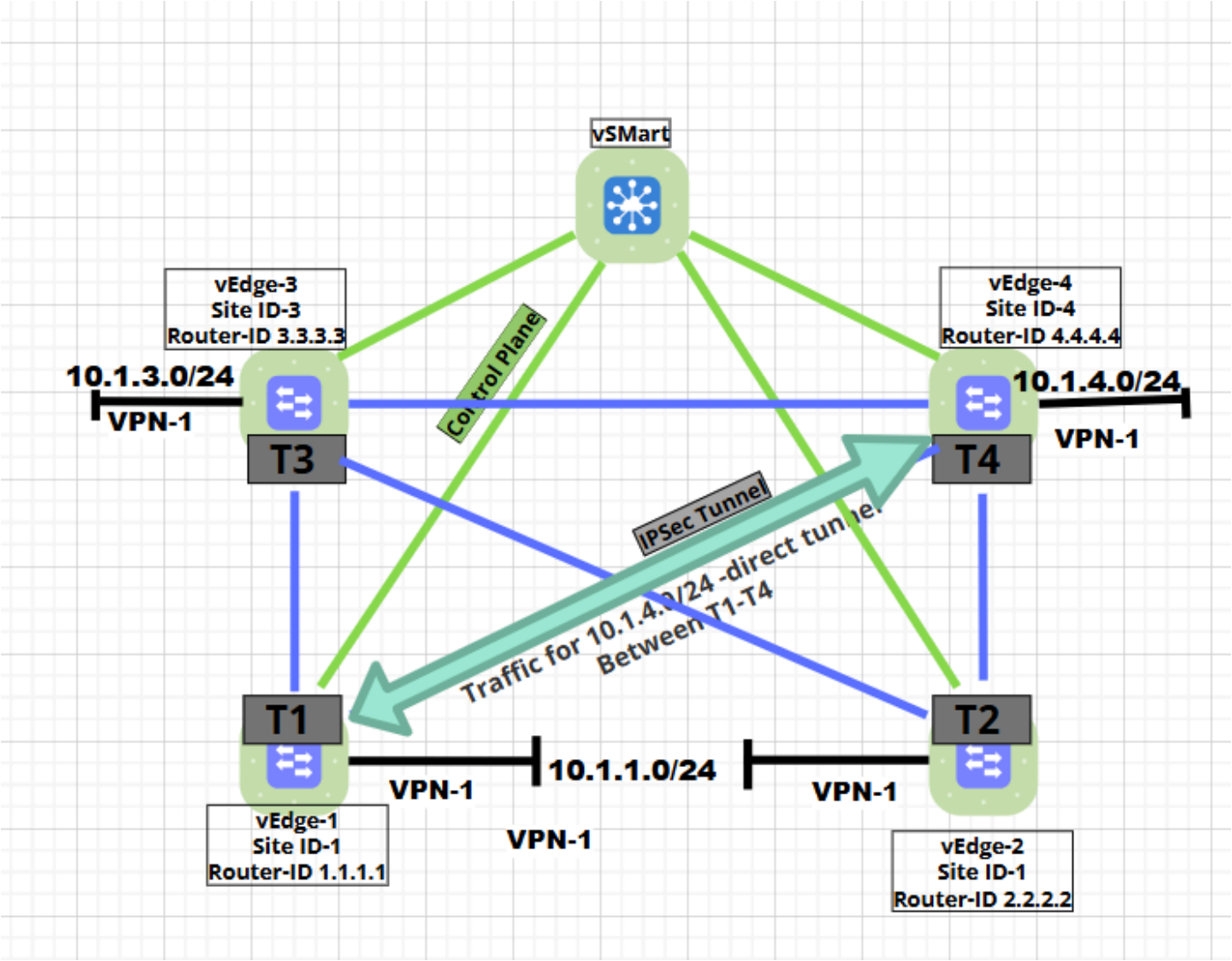
TLOC-Aktion

- In Cisco SD-WAN ermöglicht eine "TLOC Action" innerhalb einer Kontrollrichtlinie die Einfügung eines Intermediate Hop (TLOC), der für die Weiterleitung des Datenverkehrs verwendet werden kann, während der vollständige Pfad von der Quelle bis zum Ziel transparent bleibt. Das bedeutet, dass der Cisco Catalyst SD-WAN Controller durch Festlegen der Option "TLOC action" den Pfad zum endgültigen Zielgerät vollständig nachverfolgen kann. Wenn dieser Pfad ausfällt, informiert der Controller die WAN-Edge-Router, die diese OMP-Route empfangen haben.
- Es bietet einen Backup-Pfad für den Fall eines Ausfalls der primären Verbindung und

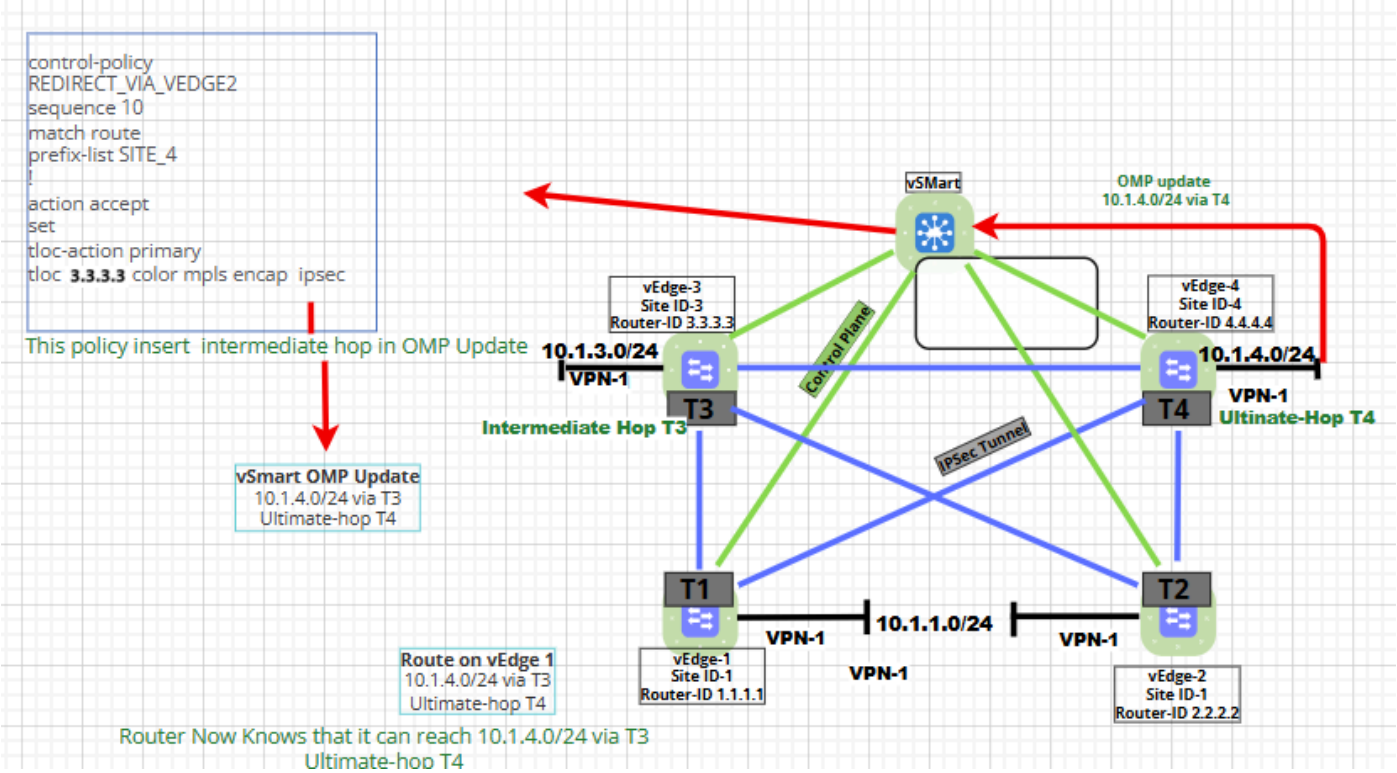
verbessert so die Ausfallsicherheit des Netzwerks und die Fehlertoleranz innerhalb des SD-WAN-Overlay-Netzwerks. Mit diesem Parameter kann gesteuert werden, wie der Datenverkehr durch das Netzwerk geleitet wird, indem die zum Erreichen eines Ziels verwendeten TLOCs geändert werden.

- Wenn eine TLOC-Aktion in einer Richtlinie definiert wird, weist sie den SD-WAN-Controller an, einen Zwischen-TLOC in die Routenberechnung einzufügen. Der Datenverkehr wird also zuerst an diesen angegebenen Backup-Standort geleitet, bevor er gegebenenfalls das endgültige Ziel erreicht.
- Dies ist besonders in Szenarien nützlich, in denen Sie die Konnektivität auch dann sicherstellen möchten, wenn eine primäre Verbindung ausfällt, indem der Datenverkehr automatisch über einen anderen Pfad (über das angegebene TLOC) umgeleitet wird.

Bei der nächsten Topologie konzentrieren wir uns auf vEdge2, vEdge3 und vEdge4, um ein besseres Verständnis zu erhalten. Derzeit ist keine Richtlinie definiert, und der Datenverkehr für 10.1.4.0/24 auf vEdge3 wird über einen direkten Tunnel zwischen T3 und T4 übertragen.



Um Fehlertoleranz und Netzwerkausfallsicherheit zu gewährleisten, wird die Steuerungsrichtlinie so konfiguriert, dass der Datenverkehr über einen anderen Pfad (über das angegebene TLOC) umgeleitet wird.



- vEdge4 sendet OMP-Update für sein direkt verbundenes Netzwerk 10.1.4.0/24 mit Next-Hop T4 an den Catalyst SD-WAN-Controller mit der Bezeichnung "10.1.4.0/24 via T4".
- Diese Route stimmt mit einer auf dem SD-WAN-Controller konfigurierten Steuerungsrichtlinie überein und legt neue TLOC- und TLOC-Aktionen gemäß der darauf definierten Richtlinie fest, d. h., sie fügt die neue 'Zwischen-TLOC' ein.
- Der Controller kündigt die OMP-Route dem vEdge1 jetzt mit zwei Next-Hops an - intermediärer TLOC (T3, 3.3.3.3) und ultimativer TLOC (Next-Hop-T4 der ursprünglichen Route). Dadurch erhält vEdge1 die Intelligenz, dass das Zielpräfix 10.1.4.0/24 über T2 und T4 erreichbar ist.

Basierend auf der definierten TLOC-Aktion vEdge1 wird der Datenverkehr für 10.1.4.0/24 weitergeleitet. Sie können daher die folgenden vier Typen von TLOC-Aktionen in der Kontrollebenen-Richtlinie definieren:

1. Strict (Standard) - Die "TLOC-Action strict" definiert, dass der Datenverkehr zwischen vEdge1 und vEdge4 über T3 (Intermediate Hop) erfolgen muss und fallen muss, wenn der Tunnel zwischen vEdge1 und vEdge4 ausfällt.
2. Primär - Die "TLOC-Aktion Primär" definiert, dass der Datenverkehr zwischen vEdge1 und vEdge4 über den Zwischenhop T3 (3.3.3.3) läuft. Wenn dieser Overlay-Tunnel ausfällt, informiert der SD-WAN-Controller vEdge1 und den Datenverkehr, der über den Direkttunnel nach T4 geleitet wird.
3. Sicherung - Die "TLOC-Action-Sicherung" definiert, dass der Datenverkehr zwischen vEdge1 und vEdge4 direkt an die ultimative LOC (Next-Hop -T4 der ursprünglichen Route) geht. Wenn der direkte Overlay-Tunnel zwischen vEdge1 und vEdge4 ausfällt, informiert der SD-WAN-Controller vEdge1 und den Datenverkehr über Intermediate Hop T3.
4. Equal-Cost Multi-Path (ECMP) - Die "TLOC-Action ECMP" legt fest, dass die Kommunikation zwischen vEdge1 und vEdge4 unter normalen Umständen durch den Zwischen-Hop T3 und den Ultimate-Hop T4 ein Lastenausgleich erhält.

Informationen zu dieser Übersetzung

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