

Detaillierter Designleitfaden und Konfigurationsbeispiele für die SR-TE Explicit-Path-Richtlinie mit EVPN VPWS, IOS XR, Version 7.5.x

Inhalt

[Einleitung](#)

[1. Hintergrundinformationen](#)

[1.1. Außerhalb des Zuständigkeitsbereichs](#)

[1.2. Annahme](#)

[1.3. Technischer Umfang](#)

[1.4. Dokumentübersicht](#)

[Anforderung](#)

[2. Benutzeranforderungen](#)

[2.1. Anforderungsübersicht](#)

[2.2. Verwendete Komponenten](#)

[Technologieüberblick](#)

[3. Segmentweiterleitung](#)

[3.1. Was ist Segment-Routing?](#)

[3.2. Segment-Bezeichner](#)

[4. SR-TE - Übersicht](#)

[4.1. Was ist SR-TE?](#)

[4.2. SR-TE-Richtlinie](#)

[5. TI-LFA FRR](#)

[5.1. Überblick](#)

[5.2. Fehlererkennungsmethode Auswirkungen auf FRR](#)

[5.3. Mikroschleifenvermeidung mit SR](#)

[6. EVPN-Overlay](#)

[6.1. EVPN-Vorteile](#)

[6.1.1. Multi-Homed- und All-Active-Ethernet-Zugriff](#)

[6.2. EVPN-Routentypen](#)

[6.2.1. Routentyp 1 - Ethernet Auto Discovery \(AD\)-Route](#)

[6.2.2. Routentyp 4 - Ethernet-Segment-Route](#)

[6.3. EVPN-Hostverbindungen](#)

[7. BoB und Lastenausgleich](#)

[7.1. BFD über Paket \(BoB\)](#)

[7.2. Lastenausgleich](#)

[7.2.1. Core-Lastenausgleich mit FAT-Label](#)

[7.2.2. Lastenausgleich für Anhang](#)

[Konfigurationsvorlagen und Befehlsbeispiele](#)

[8. Die komplette Designlösung](#)

- [8.1. Low-Level-Anforderungen](#)
 - [8.2. Zusammenfassung des Designs](#)
 - [8.3. Design-Blöcke](#)
 - [8.4. Beispiel für physische Topologie](#)
 - [8.5. Layer-1-Design details](#)
 - [8.5.1. Konfigurationsvorlagen](#)
 - [8.6. Übersicht über das OSPF/SR-TE-Design](#)
 - [8.6.1. SR-TE Szenario für normalen Datenverkehr](#)
 - [8.6.1.1. Konfigurationsvorlagen](#)
 - [8.6.2. SR-TE für Failover-Szenarien](#)
 - [8.6.3. Szenario für Single-Link-Failover](#)
 - [8.6.3.1. Konfigurationsvorlagen](#)
 - [8.6.4. Failover-Szenario für doppelte Verbindung](#)
 - [8.6.4.1. Konfigurationsvorlagen](#)
 - [8.6.5. Failover-Szenario für einen Knoten](#)
 - [8.6.5.1. Konfigurationsvorlagen](#)
 - [8.6.6. Failover-Szenario mit doppeltem Knoten](#)
 - [8.6.6.1. Konfigurationsvorlagen](#)
 - [8.7. BGP/RR-Designübersicht](#)
 - [8.7.1. Konfigurationsvorlagen](#)
 - [8.8. Überblick über das Servicekondesign](#)
 - [8.8.1. Label Stack-Darstellung](#)
 - [8.8.2. Konfigurationsvorlagen](#)
 - [9. Beispielkonfiguration und Anzeigen von Befehlen](#)
 - [9.1. Beispielkonfiguration an PE-Knoten](#)
 - [9.1. Relevante Show-Befehle an PE-Knoten](#)
- [Fehlerbehebung](#)
- [Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt den detaillierten Designleitfaden mit technischen Beschreibungen, die auf den Anforderungen von Netzwerken von XYZ basieren. Darüber hinaus bietet es eine Konfigurationsvorlage und -konfiguration auf niedriger Ebene für Anwendungsfälle von Explicit-Path-Richtlinie für das Segment Routing Traffic Engineering (SR-TE) mit Ethernet VPN (EVPN) Virtual Private Wired Service (VPWS).

1. Hintergrundinformationen

1.1. Außerhalb des Zuständigkeitsbereichs

Dieses Dokument behandelt nicht die Anforderungen zentralisierter "On-Demand"-SR-TE-Richtlinien, die XTC-Controller, EVPN-ELAN usw. verwenden, sondern konzentriert sich nur auf die SR-TE-Richtlinien für Headend-Knoten mit EVPN VPWS-Overlay.

1.2. Annahme

Der Leser dieses Dokuments muss mit den Konzepten von IP/MPLS und Ethernet sowie mit Segmentrouting- und Traffic Engineering-Technologien vertraut sein.

1.3. Technischer Umfang

Der technische Anwendungsbereich dieses Dokuments ist auf Folgendes beschränkt:

- OSPF mit TI-LFA FRR
- Über Headend (verteilt) gesteuerte SR-TE-Richtlinien
- Explicit Primary Path und Dynamic IGP-basierte Failover Paths
- Single-Homed EVPN VPWS

Die in diesem Dokument aufgeführten Konfigurationsvorlagen werden als Cisco IOS®-XR 7.5.x bezeichnet.

1.4. Dokumentübersicht

Tabelle 1. Dokumentabschnitte

Thementyp	Themenname	Abschnittsnummer
Einleitung	Hintergrundinformationen	1
Anforderung	Benutzeranforderungen	2
	Segmentweiterleitung	3
	SR-TE - Übersicht	4
Technologieüberblick	TI-LFA FRR	5
	EVPN-Overlay	6
	BoB und Lastenausgleich	7
Konfigurationsvorlagen und Befehlsbeispiele	Die komplette Designlösung	8
	Beispielkonfiguration & Anzeigen von Befehlen	9

Anforderung

2. Benutzeranforderungen

2.1. Anforderungsübersicht

Der Service Provider XYZ Networks muss über Cisco NCS 5500-Geräte ein "Green Field Network" aufbauen.

Der Zweck besteht darin, einen Multicast-Datenstrom (Sprache, Video) als Service über ein Layer-2-Transportnetzwerk mit bestimmten Anforderungen zu übertragen. Dazu gehört unter anderem die Entwicklung der Datenverkehrspfade im Netzwerk.

Sie bevorzugen SR für Transportetiketten, SR-TE für Traffic Engineering und EVPN als Overlay zur Bereitstellung von Service-Labels.

2.2. Verwendete Komponenten

Der Benutzer XYZ hat auf den NCS 5500-Routern und Line Cards konvergiert:

Tabelle 2. Hardware-Anforderungen des Projekts

PE-Knoten	PIDs
Gehäuse	NCS 5504
MPA/LCs zum Anschluss von P-Knoten	NC55-36X100G-A-SE
MPA/LCs zur Verbindung von CE-Knoten	NC55-36X100G-A-SE
P-Knoten	PIDs
Gehäuse	NCS 5508
MPA/LCs zur Verbindung anderer P-Knoten	NC55-36X100G-A-SE
MPA/LCs zur Verbindung von PE-Knoten	NC55-36X100G-A-SE

Dieser Abschnitt gibt einen Überblick über die zu verwendenden Technologien sowie kurze Beschreibungen.

Technologieüberblick

3. Segmentweiterleitung

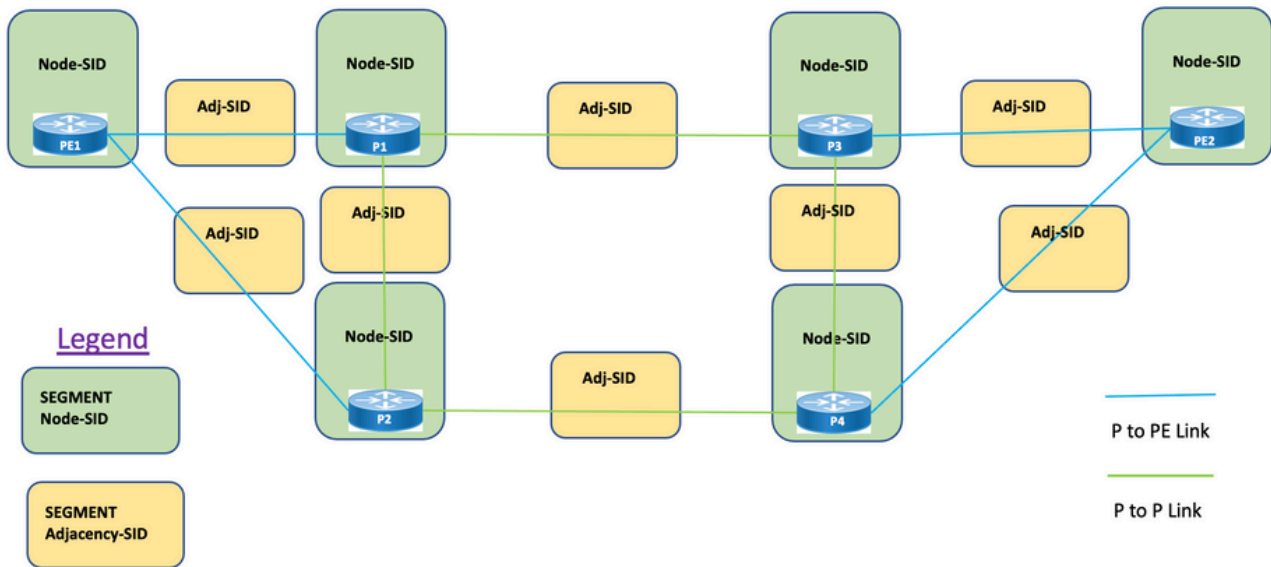
3.1. Was ist Segment-Routing?

Segment Routing ist die neueste erweiterte MPLS-Technologie, die derzeit die herkömmlichen Protokolle LDP und RSVP-TE durch die Einführung von Label Distribution und Traffic Engineering unter einem Dach ersetzt und diese nur über IGP/BGP-Protokolle mit Linkstatus ermöglicht.

Segmentrouting ist eine Methode, um Pakete basierend auf dem Quell-Routing-Paradigma im Netzwerk weiterzuleiten. Die Quelle wählt einen Pfad aus und kodiert ihn im Paket-Header als geordnete Liste von Segmenten. Segmente sind ein Bezeichner für jede Art von Anweisung. Topologiesegmente identifizieren beispielsweise den nächsten Hop zu einem Ziel. Jedes Segment wird durch die Segment-ID (SID) identifiziert, die aus einer vorzeichenlosen 20-Bit-Ganzzahl besteht.

3.2. Segment-Bezeichner

Abbildung 1. SR-Knoten-SIDs und Adjacency-SIDs



Segmente: Interior Gateway Protocol (IGP) verteilt zwei Arten von Segmenten: Präfixsegmente und Adjazenzsegmente. Jeder Router (Knoten) und jede Verbindung (Adjacency) verfügt über eine zugeordnete Segment-ID (SID).

Prefix SID: Ein Präfixsegment ist ein globales Segment, sodass eine Präfix-SID in der Segment-Routing-Domäne global eindeutig ist (siehe Abbildung 1). Eine Präfix-SID ist mit einem IP-Präfix verknüpft. Die Präfix-SID wird manuell aus dem Label-Bereich des globalen Segment-Routing-Blocks (SRGB) konfiguriert und durch IS-IS oder OSPF verteilt. Das Präfixsegment leitet den Datenverkehr über den kürzesten Pfad zum Ziel.

- Verwendet SR Global Block (SRGB)
- SRGB mit Routerfunktionen TLV angegeben - In der Konfiguration kann die Präfix-SID als absoluter Wert oder Index konfiguriert werden.
- Im Protokoll-Advertisement wird Prefix-SID immer als global eindeutiger Index kodiert. Der Index steht für einen Offset von der SRGB-Basis, d. h. 0 ist der 1. Index. Index 1 à SID beispielsweise ist $16.000 + 1 = 16.001$

Knoten-SID: Eine Knoten-SID ist ein spezieller Typ von Präfix-SID, der einen bestimmten Knoten identifiziert. Sie wird unter der Loopback-Schnittstelle mit der Loopback-Adresse des Knotens als Präfix konfiguriert. Ein Präfixsegment ist ein globales Segment, sodass eine Präfix-SID innerhalb der Segment-Routing-Domäne global eindeutig ist.

Mit anderen Worten ist das Knotensegment ein Präfixsegment, das einem Hostpräfix zugeordnet ist, das einen Knoten identifiziert.

- Entspricht einem Router-ID-Präfix, das ein Präfix ist, das einen Knoten identifiziert
- Knoten-SID ist Präfix-SID, wobei N-Flag in der Werbung festgelegt ist.
- Standardmäßig ist jede konfigurierte Prefix-SID eine Knoten-SID.
- 'Reguläres' (d. h. kein Knoten-SID) Präfix-SID kann für IS-IS konfiguriert werden.

Adjacency-SID: Ein Adjacency-Segment wird durch ein Label mit der Bezeichnung Adjacency SID identifiziert, das eine bestimmte Adjacency darstellt, z. B. eine Egress-Schnittstelle, mit einem

benachbarten Router. Die Adjacency-SID wird durch IS-IS oder OSPF verteilt. Das Adjacency-Segment leitet den Datenverkehr an eine bestimmte Adjacency weiter. Ein Adjacency-Segment ist ein lokales Segment, sodass die Adjacency-SID lokal eindeutig ist, bezogen auf einen bestimmten Router.

- Lokal von Bedeutung
- Automatische Zuweisung für jede Adjacency
- Immer als absoluter (d. h. nicht indizierter) Wert codiert

Bindende SID oder BSID: Hierbei handelt es sich um eine lokal relevante SID, die mit SR Policy verknüpft ist. Es hilft, Pakete in die zugehörige SR-Richtlinie zu leiten. Das Bindungssegment ist ein lokales Segment, das eine SR-TE-Richtlinie identifiziert. Jede SR-TE-Richtlinie ist einer Binding Segment ID (BSID) zugeordnet.

Die BSID ist eine lokale Bezeichnung, die automatisch jeder SR-TE-Richtlinie zugewiesen wird, wenn die SR-TE-Richtlinie instanziiert wird. BSID kann verwendet werden, um den Datenverkehr in die SR-TE-Richtlinie und über Domänengrenzen hinweg zu leiten, wodurch nahtlose End-to-End-SR-TE-Richtlinien zwischen den Domänen erstellt werden.

4. SR-TE - Übersicht

4.1. Was ist SR-TE?

Mit Segment Routing Traffic Engineering (SR-TE) wird der einfache Stateless Source Routing-Mechanismus des SR auf eine erweiterte Ebene umgestellt, um den Datenverkehr über vordefinierte Pfade zu programmieren und zu steuern, um Überlastungen zu vermeiden und alternative Pfade bereitzustellen, genau wie eine Express-Live-Datenverkehrsübersicht.

Dies wird erreicht, wenn Sie Richtlinien administrativ konfigurieren, die durch eine Kombination verschiedener Einschränkungen definiert sind, die sowohl die primären als auch die Backup-Pfade von den Quell- bis zu den Ziel-Knoten programmieren. Der Controller kann zentralisiert (SDN) oder verteilt (Headend) werden, je nach Netzwerkanforderungen.

Betrachten wir nun die in Abbildung 2 dargestellte Topologie. Angenommen, die Kosten der Verbindungen sind Standardwerte, und der kürzeste Pfad zum Erreichen von D von A ist A-B-C-D, aber der Pfad mit niedriger Latenz ist A-E-F-G-H-D. Der Operator kann den datenverkehrstechnischen Pfad gemäß Anforderung definieren (z. B. Latenz) und ihn in Form einer Segment-ID-Liste ausdrücken (A, E, F, G, H, D). Im Gegensatz zu RSVP-TE wird der Status dieser Richtlinie nur auf Router A und nicht auf den gesamten Routern beibehalten, die die Pakete durchlaufen (d. h. E, F, G und H).

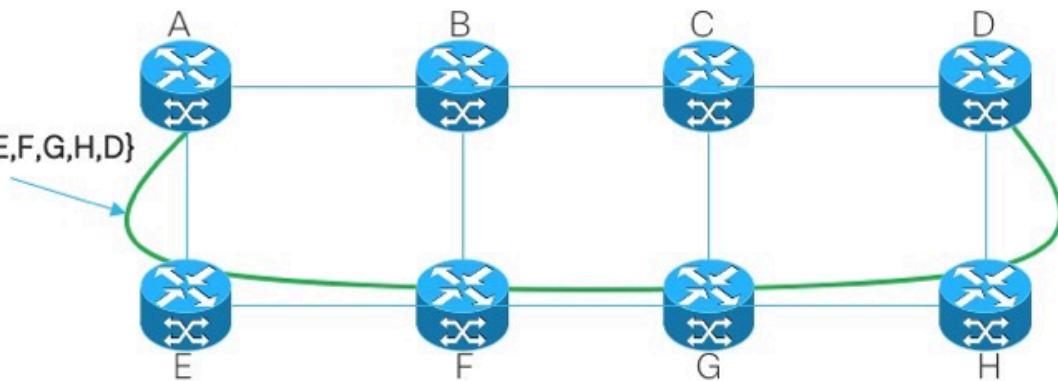
Abbildung 2. Beispiel eines administrativ definierten SR-TE-Pfads

SRTE Policy:

Destination: D

Source: A

Path: Sid List {E,F,G,H,D}



4.2. SR-TE-Richtlinie

Das Segment-Routing für das Traffic-Engineering (SR-TE) nutzt eine "Richtlinie", um den Datenverkehr durch das Netzwerk zu leiten. Ein SR-TE-Richtlinienpfad wird als eine Liste von Segmenten ausgedrückt, die den Pfad angibt, die als Segment-ID (SID)-Liste bezeichnet wird. Jedes Segment ist ein End-to-End-Pfad von der Quelle zum Ziel und weist die Router im Netzwerk an, den angegebenen Pfad zu befolgen, anstatt den kürzesten, vom IGP berechneten Pfad zu verwenden. Wenn ein Paket in eine SR-TE-Richtlinie geleitet wird, wird die SID-Liste vom Headend auf das Paket übertragen. Der Rest des Netzwerks führt die in der SID-Liste eingebetteten Anweisungen aus.

Eine SR-TE-Richtlinie wird als geordnete Liste identifiziert (Headend, Farbe, Endpunkt):

- Head-End: Hier wird die SR-TE-Richtlinie instanziiert.
- Farbe: Ein numerischer Wert, der zwischen zwei oder mehr Richtlinien für dieselben Knotenpaare unterteilt (Head-End - Endpoint).
- Endpunkt: Das Ziel der SR-TE-Richtlinie
- Jede SR-TE-Richtlinie hat einen Farbwert. Jede Richtlinie zwischen denselben Knotenpaaren erfordert einen eindeutigen Farbwert.

Eine SR-TE-Richtlinie wird mit einem oder mehreren potenziellen Pfaden konfiguriert, die primäre und Backup-Pfade beinhalten.

Der primäre Pfad der Richtlinie kann beispielsweise explizit mit Adjacency-SIDs definiert werden, und bei Ausfallszenarien kann der Backup-Pfad ein dynamischer Pfad sein, der von der IGP-Metrik übernommen wird.

5. TI-LFA FRR

5.1. Überblick

Topologieunabhängiges schleifenfreies Alternativmodell (TI-LFA) ist eine Funktion, die Links, Knoten und SRLGs schützt. Die Konfiguration ist einfach. Es sind nur zwei Konfigurationslinien erforderlich, um eine einfache TI-LFA-Konfiguration in den Router zu implementieren. Es sind keine Änderungen an den Protokollen erforderlich, die im Router verwendet werden. Abbildung 3: zeigt den primären Datenverkehrspfad und den vorberechneten Backup-Pfad durch TI-LFA für Szenarien für lokale Verbindungsausfälle und Knotenausfälle.

Abbildung 3: TI LFA Link Failover-Szenario

TI-LFA Link Failover

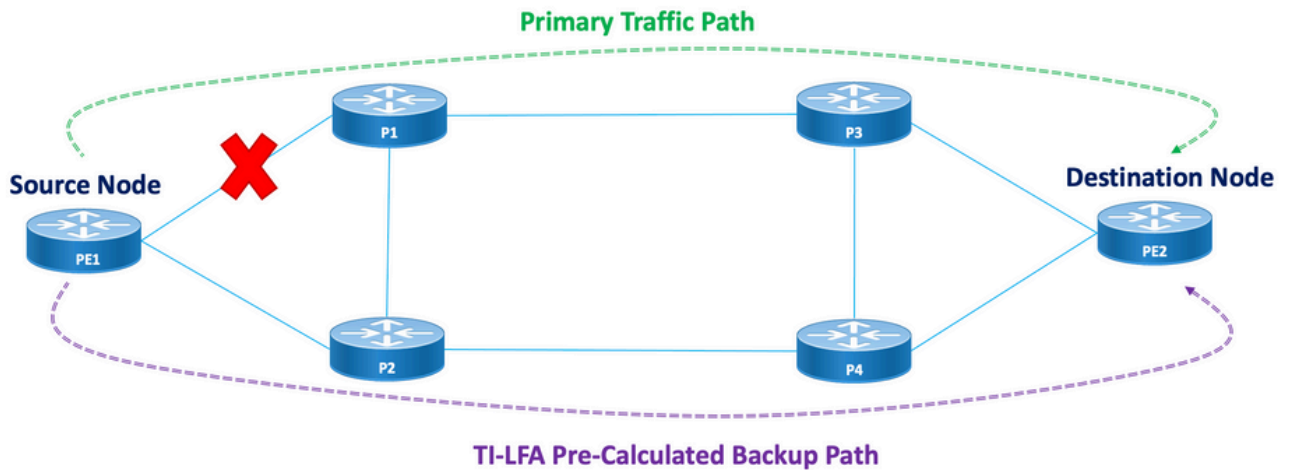
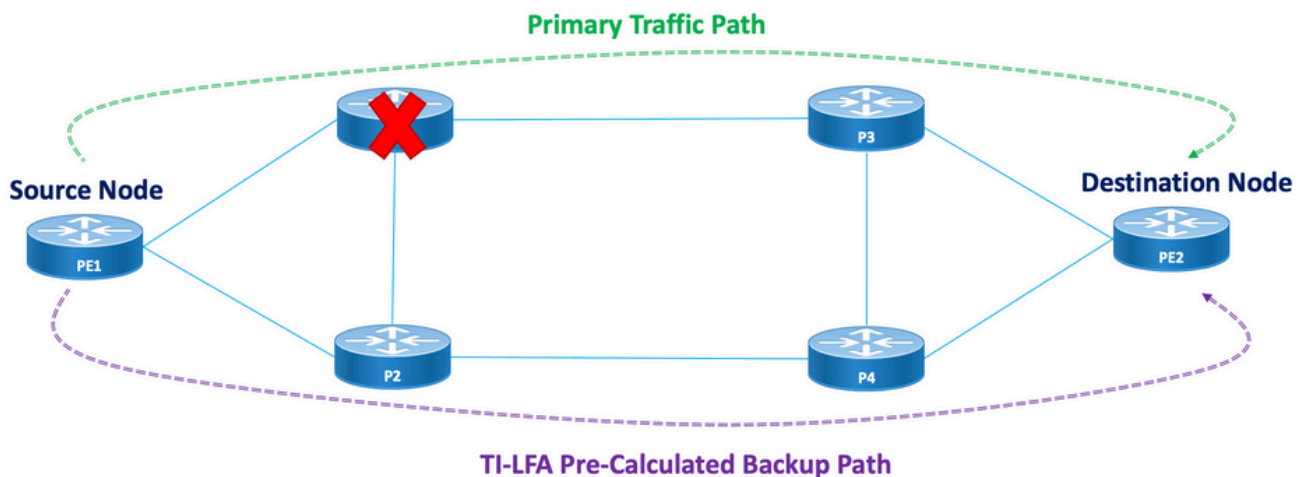


Abbildung 4: TI LFA Node Failover-Szenario

TI-LFA Node Failover



Jeder geschützte Knoten und Pfad verfügt über einen vorab berechneten Backup-Pfad, der schnell aktiviert werden kann. Die Konvergenzzeit für einen geschützten Pfad beträgt maximal 50 Millisekunden. Dies bedeutet, dass selbst die latenzanfälligsten oder bei Paketverlusten empfindlichsten Anwendungen bei Ausfall eines Knotens oder einer Verbindung ohne Unterbrechungen arbeiten können. TI-LFA berechnet den Sicherungspfad und entfernt den geschützten Link oder Knoten vorübergehend aus der Datenbank. Danach berechnet es den Backup-Pfad mit dem kürzesten Pfad zuerst. Dadurch wird sichergestellt, dass der Sicherungspfad die geringstmöglichen metrischen Kosten aufweist, während der geschützte Pfad vermieden wird. Ein verkehrstechnisch entwickelter Tunnel, der dem Sicherungspfad folgt, wird bei einem Ausfall für den Datenverkehr verwendet. Eine Repair Label-Liste bestimmt den Pfad für die Pakete, die eine neue Route zum Ziel benötigen. Eine Repair Label-Liste ist ein normaler Label-Stack, der jedoch nur verwendet wird, wenn in der geschützten Route ein Fehler auftritt.

5.2. Fehlererkennungsmethode Auswirkungen auf FRR

Fast Reroute für datenverkehrstechnisch gesteuerte SR-TE-Pfade wird als Mittel zur Umleitung des Datenverkehrs konfiguriert, wenn Failover-Szenarien vom primären Pfad zu Backup-Pfaden

innerhalb von möglichst 50 ms auftreten. Die schnelle Umleitung wird unter dem IGP (OSPF/ISIS)-Protokoll konfiguriert. Die Konvergenzzeit hängt von der Methode ab, mit der die Erkennung von Verbindungsausfällen erfolgt. Bei einem Glasfaserausfall ist die Erkennung sofort erfolgt und die Konvergenzzeit von unter 50 ms hoch. Falls die Erkennung von Verbindungsausfällen jedoch von BFD mit einem Intervall von 15 ms (multiplier x3) durchgeführt werden muss. Die Konvergenzzeit beträgt meistens mehr als 50 ms.

5.3. Mikroschleifenvermeidung mit SR

Mikroschleifen sind kurze Paketschleifen, die im Netzwerk auftreten und auf eine Topologieänderung (Ereignisse bei Verbindungsabbruch, Verbindungsaufbau oder metrischen Änderungen) folgen. Mikroschleifen werden durch die nicht gleichzeitige Konvergenz verschiedener Knoten im Netzwerk verursacht. Wenn Knoten konvergieren und Datenverkehr an einen Nachbarknoten senden, der noch nicht konvergiert ist, kann Datenverkehr zwischen diesen beiden Knoten hin- und hergeschleift werden, was Paketverluste, Jitter und Out-of-Order-Pakete zur Folge hat.

Die Funktion zur Vermeidung von Segment-Routing-Mikroschleifen erkennt, ob auf Mikroschleifen möglicherweise eine Topologieänderung folgt. Wenn ein Knoten berechnet, dass eine Mikroschleife in der neuen Topologie auftreten kann, erstellt der Knoten unter Verwendung einer Liste von Segmenten einen schleifenfreien SR-TE-Richtlinienpfad zum Ziel. Nach Ablauf des Zeitgebers für die RIB-Aktualisierungsverzögerung wird die SR-TE-Richtlinie durch reguläre Weiterleitungspfade ersetzt. Für die RIB-Aktualisierungsverzögerung gibt es einen Standard-Timer, der von TI-LFA übernommen wird.

6. EVPN-Overlay

EVPN ist eine Technologie, die ursprünglich für Ethernet-Multipoint-Services entwickelt wurde und erweiterte Multi-Homing-Funktionen bietet. BGP wird zur Verteilung von Informationen zur Erreichbarkeit von MAC-Adressen über das MPLS-Netzwerk verwendet. Gleichzeitig werden L2VPNs die gleichen Betriebs- und Skalierungsmerkmale wie IP-VPNs zugewiesen. Neben DCI- und E-LAN-Anwendungen bietet die EVPN-Lösungsfamilie heute eine gemeinsame Grundlage für alle Ethernet-Service-Typen, einschließlich E-LINE und E-TREE, sowie Routing- und Bridging-Szenarien für Rechenzentren. EVPN bietet außerdem Optionen zur Kombination von L2- und L3-Services in derselben Instanz.

EVPN ist eine Lösung der nächsten Generation, die Ethernet-Multipoint-Services über MPLS-Netzwerke bereitstellt. EVPN wird im Gegensatz zum vorhandenen Virtual Private LAN Service (VPLS) ausgeführt, der das BGP-basierte MAC-Learning auf Kontrollebene im Core ermöglicht. In EVPN erfassen PEs, die an den EVPN-Instanzen teilnehmen, mithilfe des MP-BGP-Protokolls MAC-Routen von Benutzern auf Kontrollebene.

EVPN bietet eine Reihe von Vorteilen:

- Redundanz pro Datenfluss und Lastenausgleich
- Vereinfachte Bereitstellung und Bedienung
- Optimale Weiterleitung
- Schnelle Konvergenz
- Skalierbarkeit von MAC-Adressen
- Lösungen verschiedener Anbieter im Rahmen der IETF-Standardisierung

Die auf einem Gerät erfassten MAC-Adressen müssen abgerufen oder auf die anderen Geräte in

einem VLAN verteilt werden. Die EVPN Software MAC Learning-Funktion ermöglicht die Verteilung der auf einem Gerät erfassten MAC-Adressen auf die anderen Geräte, die mit einem Netzwerk verbunden sind. Die MAC-Adressen werden mithilfe von BGP von den Remote-Geräten abgerufen.

In diesen Abschnitten erfahren Sie mehr über einige der Vorteile und Routing-Typen von EVPN im Allgemeinen und lernen anschließend die lösungsspezifischen Komponenten kennen, die auf das Design von Netzwerkservices von XYZ angewendet werden.

6.1. EVPN-Vorteile

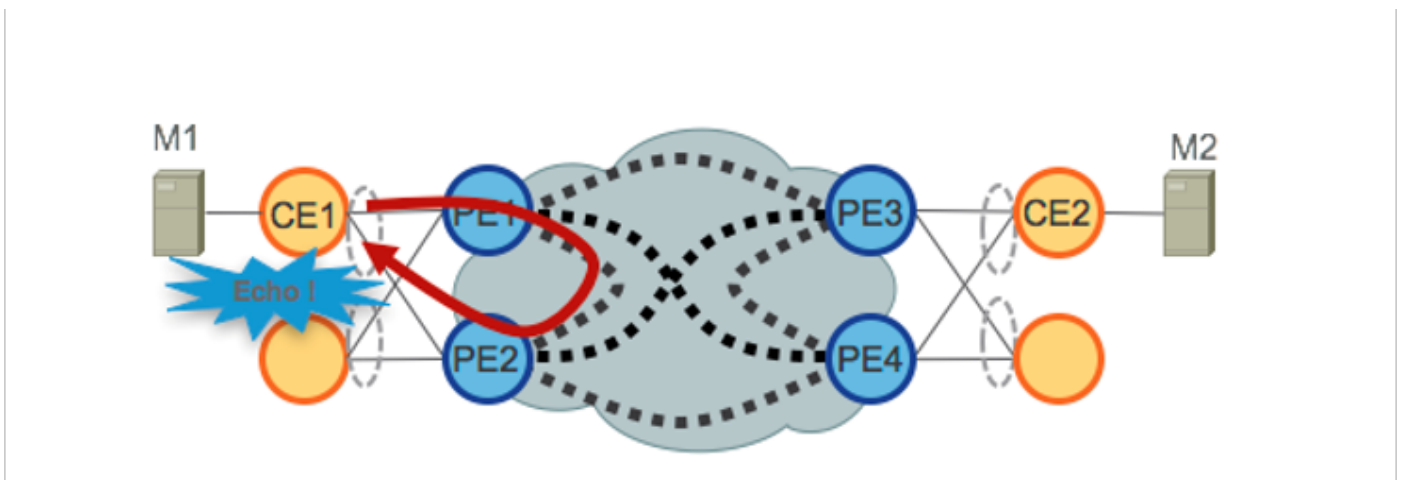
L2VPN und L3VPN bieten nicht nur Services unter einem Lösungsumfang, sondern auch verschiedene Routenarten. EVPNs lösen zwei langjährige Beschränkungen für Ethernet-Services in Service Provider Networks:

- Multi-Homed- und All-Active-Ethernet-Zugriff
- Service Provider Network - Integration in die Zentrale oder das Rechenzentrum

6.1.1. Multi-Homed- und All-Active-Ethernet-Zugriff

Die Abbildung zeigt die größte Einschränkung herkömmlicher L2-Multipoint-Lösungen wie VPLS.

Abbildung 5: EVPN-Zugriff für alle aktiven Benutzer



Wenn VPLS im Core ausgeführt wird, erfordert die Vermeidung von Schleifen, dass PE1/PE2 und PE3/PE4 nur Single-Active-Redundanz für ihre jeweiligen CEs bereitstellen. Bisher wurden Techniken wie mLACP oder Legacy-L2-Protokolle wie MST, REP, G.8032 usw. verwendet, um Redundanz für den Single-Active-Zugriff bereitzustellen.

Dasselbe gilt für Hierarchical-VPLS (H-VPLS), bei dem der Access-Knoten für die Bereitstellung des Single-Active H-VPLS-Zugriffs über Active und Backup Spoke Pseudowire (PW) verantwortlich ist.

Modelle für die reine Zugriffsredundanz können nicht bereitgestellt werden, da die VPLS-Technologie keine Möglichkeit bietet, L2-Schleifen zu verhindern, die von den Weiterleitungsmechanismen im Core für bestimmte Datenverkehrskategorien abgeleitet werden. Broadcast-, Unknown-Unicast- und Multicast (BUM)-Datenverkehr, der vom CE stammt, wird im gesamten VPLS-Core überflutet und von allen PEs empfangen. Dieser wiederum wird an alle

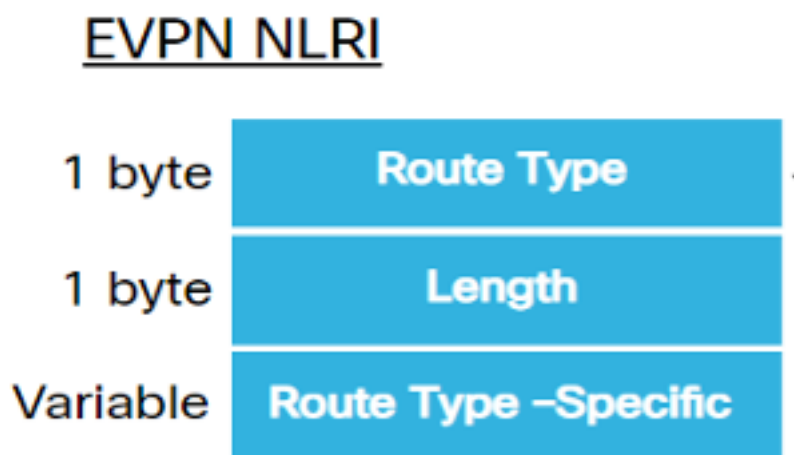
angeschlossenen CEs übertragen. In unserem Beispiel kann PE1 den BUM-Datenverkehr von CE1 zum Core überfluten, und PE2 kann ihn nach dem Empfang an CE1 zurücksenden.

EVPN nutzt BGP-basierte Kontrollebenen-Techniken, um dieses Problem zu beheben, und ermöglicht Active-Active-Access-Redundanzmodelle für Ethernet- oder H-EVPN-Zugriff.

6.2. EVPN-Routentypen

EVPN definiert einen neuen BGP NLRI, der für die Übertragung aller EVPN-Routen verwendet wird. EVPN NLRI wird im BGP mit Multiprotokoll-Erweiterungen mit einem AFI von 25 (L2VPN) und einem SAFI von 70 übertragen. BGP-Funktionen sorgen dafür, dass zwei Lautsprecher EVPN NLRI unterstützen.

Abbildung 6: EVPN NLRI



Die für diese Implementierung erforderlichen EVPN-Routentypen werden hier beschrieben:

6.2.1. Routentyp 1 - Ethernet Auto Discovery (AD)-Route

Die Ethernet Auto-Discovery-Routen (AD) werden pro EVI und pro ESI-Basis angekündigt. Diese Routen werden pro ES gesendet. Sie führen die Liste der EVIs, die zum ES gehören. Das ESI-Feld ist auf null festgelegt, wenn ein CE Single-Homed ist. Dieser Routentyp wird für die Massenentnahme von MAC-Adressen, Aliasing für den Lastenausgleich und Split Horizon Filtering verwendet.

6.2.2. Routentyp 4 - Ethernet-Segment-Route

Ethernet-Segment-Routen ermöglichen die Verbindung eines CE-Geräts mit zwei oder PE-Geräten. Die ES-Route ermöglicht die Erkennung angeschlossener PE-Geräte, die mit demselben Ethernet-Segment verbunden sind, d. h. die Erkennung von Redundanzgruppen. Sie wird auch für die Auswahl des designierten Forwarder (DF) verwendet.

6.3. EVPN-Hostverbindungen

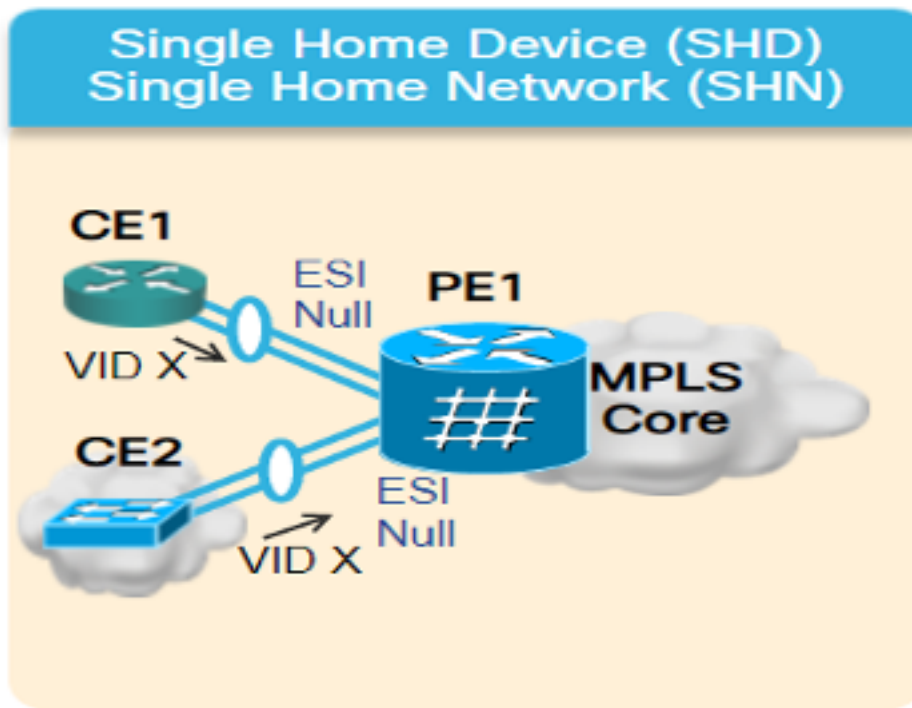
Diese EVPN-Modi werden unterstützt:

- Single Homing (Einzelhoming) - Dadurch können Sie ein Benutzer-Edge (CE)-Gerät mit

einem Provider Edge (PE)-Gerät verbinden. In diesem ESI-Wert ist null für jede PE-CE-Verbindung.

- Multihoming - Dadurch können Sie ein Benutzer-Edge-Gerät (User Edge, CE) mit zwei oder mehr Provider Edge (PE)-Geräten verbinden, um eine redundante Konnektivität bereitzustellen. Es ist keine Interchassis-Verbindung erforderlich. Das redundante PE-Gerät stellt sicher, dass bei einem Netzwerkausfall kein Datenverkehr unterbrochen wird. Die Multihoming-Typen sind:

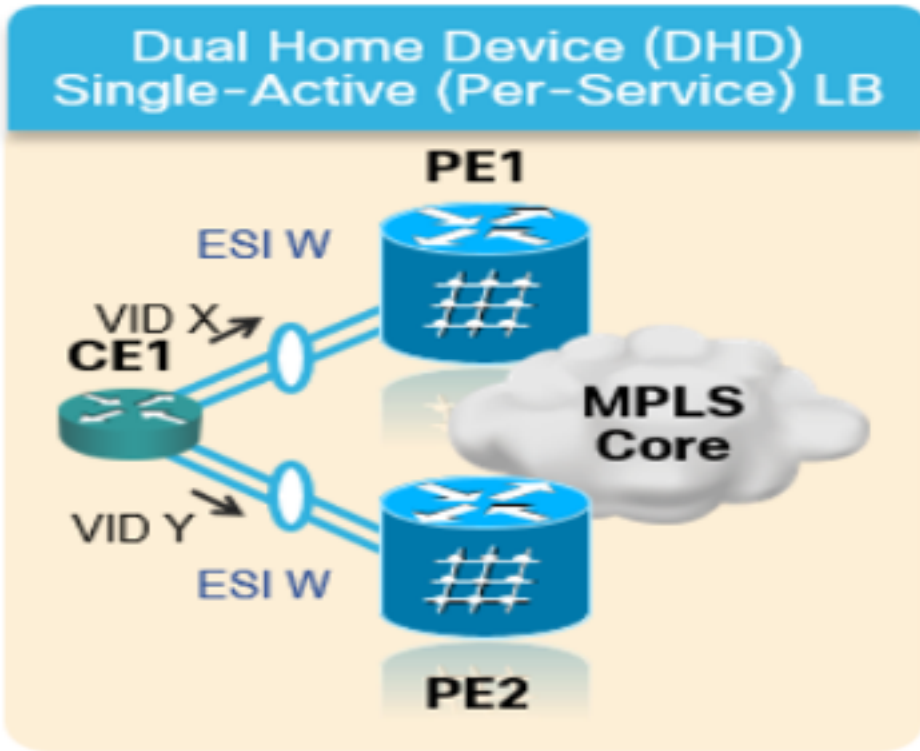
Abbildung 7: EVPN Single Homing



Multihoming - Dies sind die Arten von Multihoming:

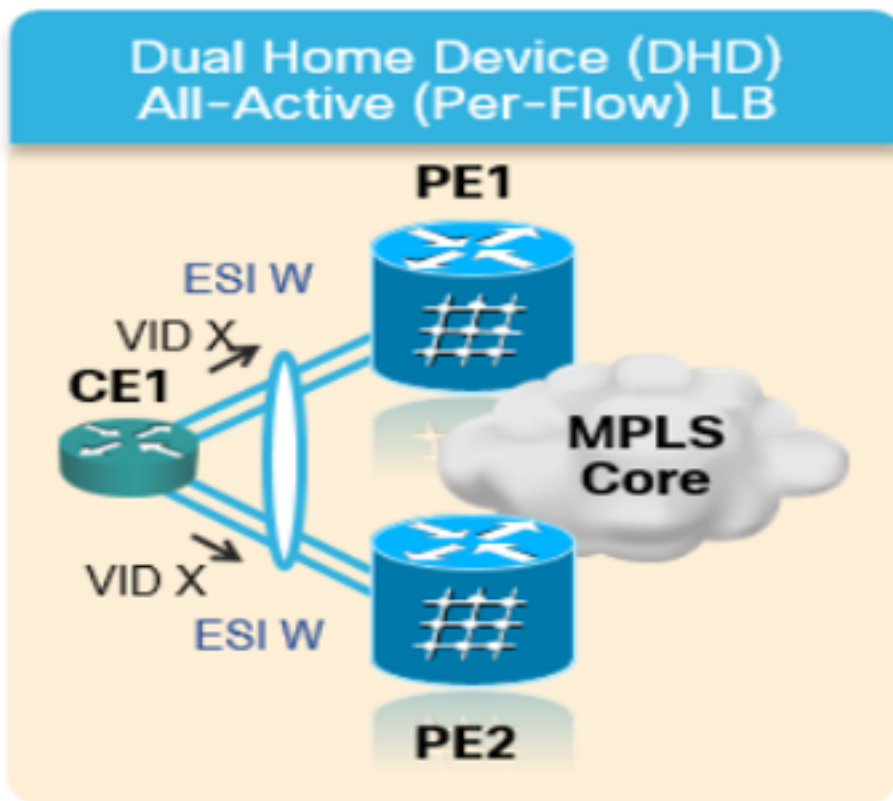
1. Single-Active - In einem Single-Active-Modus ist es nur einem PE einer Gruppe von PEs gestattet, Datenverkehr an und von diesem Ethernet-Segment weiterzuleiten.

Abbildung 8: EVPN Single-Active



2. Aktiv-Aktiv - Im Aktiv-Aktiv-Modus können alle PEs, die an das jeweilige Ethernet-Segment angeschlossen sind, Datenverkehr an dieses und aus diesem Ethernet-Segment weiterleiten.

Abbildung 9: EVPN Dual Active



7. BoB und Lastenausgleich

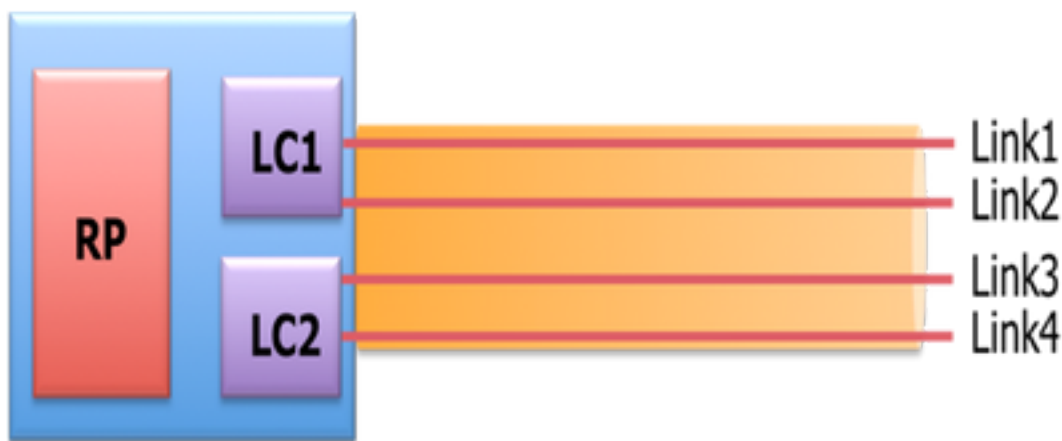
7.1. BFD über Paket (BoB)

Bidirectional Forwarding Detection (BFD) ermöglicht die Erkennung von Ausfällen im Pfad zwischen benachbarten Forwarding-Engines mit geringem Overhead und kurzer Dauer. Mit BFD kann ein einziger Mechanismus für die Fehlererkennung auf allen Medien und auf allen Protokollebenen mit einer Vielzahl von Erkennungszeiten und Overhead verwendet werden. Die schnelle Fehlererkennung bietet eine sofortige Reaktion auf einen Ausfall bei einem fehlerhaften Link oder Nachbarn.

Dies würde das IGP dazu veranlassen, den Datenverkehr an den Backup-Pfad weiterzuleiten, der bereits mit der Verwendung von FRR (im Fall von IGP) und PIC (im Fall von BGP) berechnet wurde.

Bei der BFD Over Bundle (BoB)-Funktion wird die IPv4 BFD-Sitzung für jedes aktive Paketmitglied ausgeführt.

Abbildung 10: BoB - Logisches Diagramm



Bundlemgr berücksichtigt neben den vorhandenen L1/L2-Zuständen auch BFD-Zustände, um die Verwendbarkeit der Mitgliedsverbindung zu bestimmen. Der Bundle-Mitgliedsstaat ist in der Funktion:

L1-Status (physische Verbindung)

L2-Status (LACP)

L3-Status (BFD)

BFD Agent wird weiterhin auf der Linecard ausgeführt. BFD-Zustände von Bündelverbindungen werden auf dem RP konsolidiert. Die Member-Links müssen Back-to-Back verbunden werden, ohne dass zwischen den L2-Switches hin- und hergeschaltet werden müssen. Die BoB-Funktion wird in allen Ethernet-Paketschnittstellen des Netzwerks XYZ konfiguriert.

7.2. Lastenausgleich

Der ECMP-Lastenausgleich für jeden Datenfluss im betroffenen Netzwerk erstreckt sich über mehrere Ethernet-Schnittstellen zwischen Paketen und Ethernet-Intra-Bündeln (zwischen physischen Elementen einer Paketschnittstelle). Dies gilt für das gesamte Netzwerk vom PE zum PE (Core Load Balance) sowie von PE zu CE (AC Load Balancing) wie bereits erläutert.

7.2.1. Core-Lastenausgleich mit FAT-Label

Entsprechend dem Umfang des Netzwerks von XYZ müssen Sie nur den ECMP-Lastenausgleich (Equal Cost Multipath) pro Datenfluss berücksichtigen, wie bereits erwähnt:

Router leiten den Datenverkehr in der Regel auf Basis des einfachsten Labels im Label-Stack aus, das für alle Datenflüsse in einem bestimmten Pseudowire identisch ist. Dies kann zu einem asymmetrischen Lastenausgleich führen. Der Fluss bezieht sich in diesem Kontext auf eine Sequenz von Paketen, die dasselbe Quell- und Zielpaar haben. Die Pakete werden von einem Quell-Provider-Edge (PE) zu einem Edge-PE des Ziellanbieters übertragen.

Flow-Aware Transport Pseudowire (FAT PW) ermöglicht die Identifizierung einzelner Datenflüsse innerhalb eines Pseudowire und ermöglicht Routern die Nutzung dieser Datenflüsse zum Lastenausgleich des Datenverkehrs. FAT-PWs werden zum Lastenausgleich des Datenverkehrs im Core verwendet, wenn ECMP (Equal-Cost Multipath) verwendet wird. Ein Flow-Label wird basierend auf unteilbaren Paketflüssen erstellt, die ein Pseudowire eingeben und als das untere Label in das Paket eingefügt wird. Router können das Flow-Label für den Lastenausgleich verwenden, um eine bessere Verteilung des Datenverkehrs auf ECMP-Pfade oder verbindungsgebündelte Pfade im Core zu ermöglichen.

Dem Stack wird ein zusätzliches Label, das so genannte Flow-Label, hinzugefügt, das für jeden einzelnen eingehenden Datenfluss im PE generiert wird. Ein Flow-Label ist ein eindeutiger Bezeichner, der einen Fluss innerhalb des PW unterscheidet und von Quell- und Ziel-MAC-Adressen sowie Quell- und Ziel-IP-Adressen abgeleitet ist. Das Flow-Label enthält den End-of-Label-Stapelsatz (EOS). Das Fließlabel wird nach dem VC Label und vor dem Kontrollwort eingefügt (falls vorhanden). Der Eingangs-PE berechnet und leitet das Flow-Label weiter. Die FAT-PW-Konfiguration aktiviert die Flow-Bezeichnung. Der Egress-PE verwirft das Flow-Label, sodass keine Entscheidungen getroffen werden.

7.2.2. Lastenausgleich für Anhang

Für den Lastenausgleich von AC-Paketmitgliedern ist jedoch ein anderer Ansatz erforderlich, da in diesem Abschnitt des Netzwerks kein SR-MPLS vorhanden ist.

Der Lastenausgleich pro Datenstrom kann hier erreicht werden, wenn spezifische L2VPN-Konfigurationseinstellungen für alle PE-Router explizit angepasst werden. Sie kann je nach Anforderung per SRC/DST MAC- oder SRC/DST-IP erfolgen.

Konfigurationsvorlagen und Befehlsbeispiele

8. Die komplette Designlösung

In diesem Abschnitt werden die vollständigen Designdetails erläutert, die von allen einzelnen Komponenten zusammengefügt wurden, die in früheren Abschnitten erläutert wurden. In diesem Abschnitt werden die Topologie und die entsprechende Konfigurationsvorlage mit Bezug auf Cisco IOS-XR 7.5.x dargestellt.

8.1. Low-Level-Anforderungen

Im normalen Datenverkehrsszenario wird der Datenverkehrsfluss immer zwischen den

Dienstterminierungen von PE1 und PE3 und nur zwischen PE2 und PE4 propagiert. In dieser Situation besteht das Hauptziel darin, den Datenverkehrspfad vollständig voneinander zu trennen (siehe Abbildung 12).

Der betroffene Datenverkehr hier würde gekapselte Multicast-Datenflüsse durch das EVPN-Overlay übertragen. Von CE1- und CE2-Knoten kommen die Multicast-Media-Streams (Sprache/Video) hinzu, die an den PE1- und PE2-Knoten gekapselt und über das EVPN L2-Overlay an CE3- bzw. CE4-Knoten transportiert werden können, nachdem sie an den PE3- bzw. PE4-Knoten entkapselt werden.

Daher wird das Quell-Ziel-Datenverkehrspaar künftig unter allen Umständen als PE1-PE3 und PE2-PE4 angesehen, sofern nichts anderes angegeben wird. Einzelheiten zu den Anforderungen finden Sie in [Unterabschnitt 2.2.](#)

8.2. Zusammenfassung des Designs

Um die Anforderungen zu erfüllen, wird OSPF entsprechend den Anforderungen von XYZ Networks als Underlay IGP ausgewählt. Um den gekapselten Multicast-Stream über das Quell-Ziel-Datenverkehrspaar über den gewünschten Pfad zu leiten, muss SR-TE zwischen PE-Knoten implementiert werden.

Die SR-TE-Richtlinien wurden mit Explicit-Path und dynamischen IGP-Pfaden konzipiert.

Die expliziten Pfade umfassen:

- Normales Datenverkehrsszenario
- Failover-Szenario, bis alternative Pfadoptionen verfügbar sind

Die dynamischen IGP-Pfade umfassen:

- Backup-Pfad für das Failover-Szenario, bei dem keine alternativen Pfadoptionen verfügbar sind

Funktionen wie BFD, TI-LFA und Microloop Avoidance werden unter OSPF konfiguriert, wie in den Unterabschnitten mit Konfigurationsvorlagen gezeigt.

Für normale Datenverkehrsszenarien werden die Konfigurationsvorlage und andere Details in Abschnitt 8.5.1 erwähnt.

Für Datenverkehrs-Failover-Szenarien werden die Konfigurationsvorlage und andere Details in Abschnitt 8.5.2 erwähnt.

Abgesehen davon werden auch die Anforderungen wie Mikroschleifenvermeidung und Konvergenz von weniger als 50 ms im Falle von Ausfallszenarien berücksichtigt.

8.3. Design-Blöcke

In diesem Unterabschnitt werden alle Designblöcke erfasst, die in diesen Abschnitten ausführlich behandelt werden.

Übersicht über das allgemeine Design (Layer 1):

- Die MTU-Größe im gesamten Netzwerk von XYZ ist auf "9216" festgelegt, um bis zu 5 bis 6

SR-Label-Stacks zu unterstützen.

- 'BFD over Bundle' wird mit einem Intervall von 15 ms implementiert, um Glasfaserkabel unter 50 ms zu erkennen.

Übersicht über das OSPF/SR-TE-Design:

- **OSPF** als IGP-Protokoll mit **TI-LFA**, konfiguriert für **FRR** von weniger als 50 ms Konvergenzzeit
- **Transportschicht** basierend auf **Segment Routing** als Weiterleitungsebene und **OSPF** als Routing-Protokoll
- Im Netzwerk XYZ leitet der explizite Pfad **Segment Routing Traffic Engineering** den Datenverkehr in alle erforderlichen primären Pfadrichtungen. Bei Link-/Knoten-Failover-Szenarien wird der Datenverkehr über einen dynamischen IGP-Pfad geleitet.
- Die Vermeidung von Mikroschleifen und die OSPF-Max-Metric sind ebenfalls Teil dieses Designs.

BGP/RR-Design im Überblick:

- In einem Cluster sind **zwei RRs** konfiguriert, um **Redundanz** bereitzustellen.
- Der BGP-Prozess für das Netzwerk XYZ in jedem PE besteht aus "**IPv4**" und "**L2VPN EVPN**"-Peering mit beiden RRs getrennt

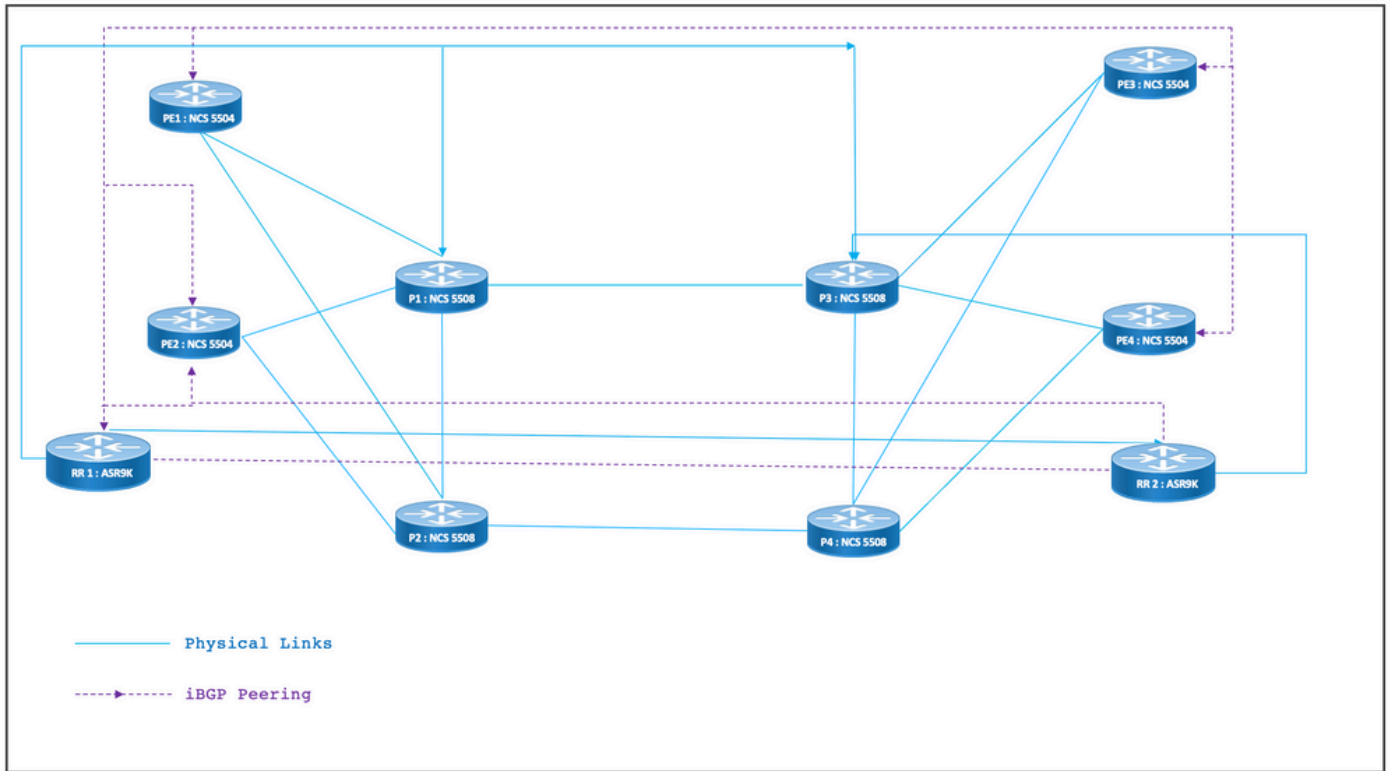
Überblick über das Service-Design:

- **Service-Layer** basieren auf der **BGP-basierten Kontrollebene** und Layer-2-Point-to-Point-EVPN (**EVPN-VPWS**).
- Der Multicast-Videodatenverkehr (UDP) wird über die Point-to-Point-EVPN-VPWS-PWs gekapselt.
- **ECMP-Lastenausgleich** wird durch Konfiguration des FAT-Labels im EVPN-Abschnitt erreicht
- Der Service unterstützt bis zu 5 bis 6 SR Label-Stacks, die SR-Transportlabels, EVPN-Labels und FAT-Labels für den Lastenausgleich enthalten.

8.4. Beispiel für physische Topologie

Die physische Topologie von Netzwerken XYZ ist in dieser Abbildung dargestellt. Aus Gründen der Einfachheit werden nur 4 PE- und 4 P-Knoten angezeigt. Es gibt zwei RR-Knoten, die in Clustern arbeiten, um Redundanz zu gewährleisten.

Abbildung 11: Physische Topologie



8.5. Layer-1-Designdetails

Im generischen Layer-1-Design gibt es ein Paket-Ethernet mit mindestens zwei Mitgliedsverbindungen pro konfiguriertem Paket. Um Verbindungsausfälle schnell zu erkennen, wählen Sie BFD anstelle der Paketfunktion aus. Das Zeitintervall kann im Idealfall zwischen 5 und 15 ms variieren. Dies hängt von der Fähigkeit zur Auslagerung der Hardware ab.

Weitere Informationen zu BFD finden Sie unter

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/73x/b-routing-cg-ncs5500-73x/implementing-bfd.html>. Beachten Sie, dass diese Funktion nur unter der Ethernet-

Paketschnittstelle konfiguriert werden muss und nicht unter IGP konfiguriert werden muss. Die MTU-Größe ist auf **9216** festgelegt, um bis zu 5 bis 6 SR-Label-Stacks zu unterstützen.

8.5.1. Konfigurationsvorlagen

Die BFD-over-Bundle-Konfigurationsvorlagen für alle Knoten sind hier dargestellt:

```
interface Bundle-Ether <Intf-Number>

bfd address-family ipv4 timers start 60

bfd address-family ipv4 timers nbr-unconfig 60

bfd address-family ipv4 multiplier 3

bfd address-family ipv4 destination <Connected-Intf-IP>

bfd address-family ipv4 fast-detect

bfd address-family ipv4 minimum-interval <Time in msec>

mtu <Value as per requirement>
```

```
ipv4 address <Intf IP> <Subnet Mask>>
```

```
bundle minimum-active links 1
```

!

8.6. Übersicht über das OSPF/SR-TE-Design

Alle OSPFv2-Router im Netzwerk befinden sich in Bereich 0, sodass das Netzwerk eine einzige IGP-Domäne behandelt.

Unter Router-OSPF ist Segment-Routing aktiviert, und relevante Paket-Ethernet-Schnittstellen werden konfiguriert. Ebenso sind unter "Bundle Interfaces" der Netzwerktyp und schnelle Umleitungsparameter aktiviert. Am wichtigsten ist, dass eine Loopback-Schnittstelle im passiven Modus aktiviert ist, wobei Prefix-SID konfiguriert ist.

OSPF ist ein Link-State-Protokoll. Daher muss es eine Priorität sein, die Downlinks sofort zu identifizieren und einen Backup-Pfad zu erstellen. Um dies zu gewährleisten, wird BFD over Bundle unter Bundle Interface (Bundle-Schnittstelle) und TI-LFA FRR unter OSPF konfiguriert, wodurch die Konvergenzzeit bei Szenarien mit Glasfaserentrennungen von 50 ms erhalten bleibt.

In diesen Unterabschnitten werden die Szenarien für normale Datenverkehrspfade und Failover-Szenarien detailliert dargestellt:

8.6.1. SR-TE Szenario für normalen Datenverkehr

Um einen sehr strengen primären Pfad beizubehalten, sind SR-TE-Richtlinien mit expliziten End-to-End-Pfaden zwischen den zuvor erwähnten Quell-Ziel-Datenverkehrspaaren zu entwerfen. Darüber hinaus sind in einer SR-TE-Richtlinie mehrere bevorzugte potenzielle Pfade erforderlich, um die Bereitstellung mehrerer Failover-Szenarien zu ermöglichen.

Diese Abbildung zeigt die Details des Benutzernetzwerks in Übereinstimmung mit den in [Unterabschnitt 8.3](#) genannten Design-Bausteinen.

- Verbindungen zwischen PE- und P-zu-P-Knoten
- Loopback-Adressen aller Knoten
- Schnittstellenadressen aller Knoten
- Richtung des regulären SR-TE-Datenverkehrspfads
- EVPN-Overlay zwischen PE-Knoten

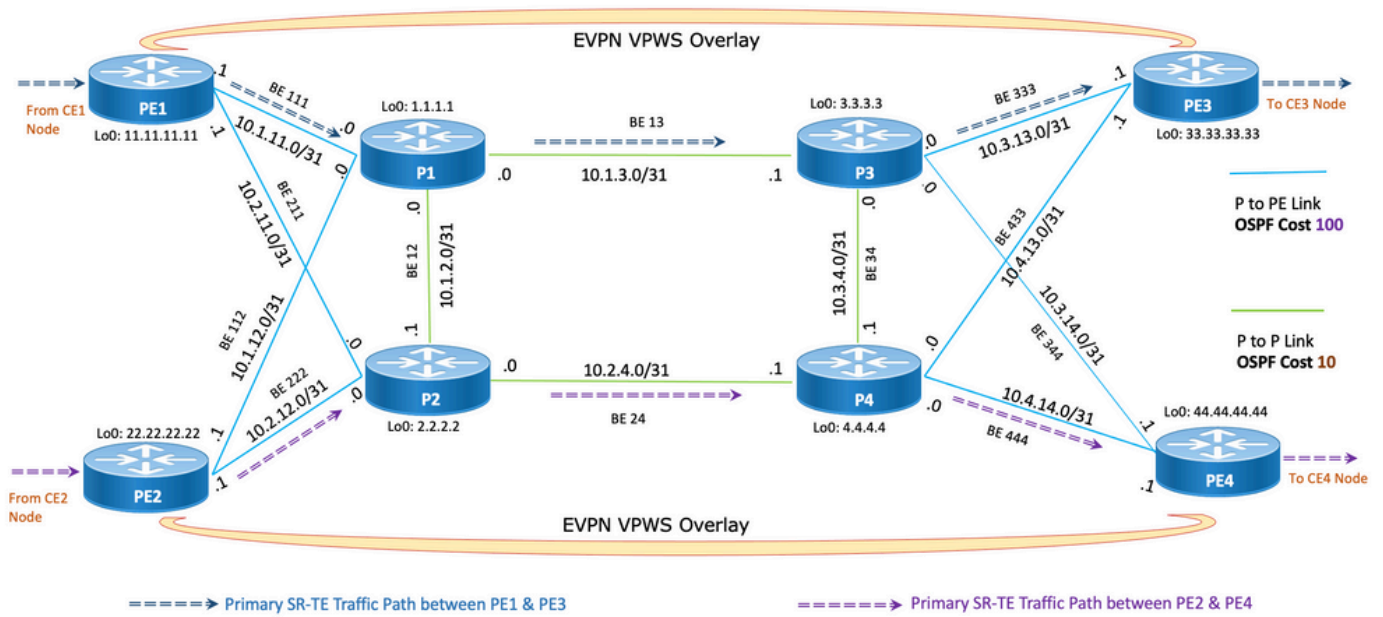
Die RRs wurden nicht absichtlich eingesetzt, um die Übersichtlichkeit in der Topologie zu reduzieren.

Die Verbindungen zwischen PE und P sind blau markiert, und die Verbindungen zwischen P und P sind grün markiert. Die OSPF-Kosten für PE-to-P-Verbindungen betragen 100 und die Kosten für P-P-Verbindungen 10.

Der primäre SR-TE-Datenverkehrsfluss wurde zwischen dem PE1-PE3-Paar mit blauen Pfeilen markiert und mit violetten Pfeilen zwischen dem PE2-PE4-Paar markiert.

Abbildung 12: Topologiedetails

Normal Traffic Scenario: SR-TE Steered Path with EVPN Overlay



8.6.1.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die entsprechenden Konfigurationsvorlagen für OSPF/SR-TE für PE1- und PE2-Knoten wie folgt:

PE1 Node: OSPF & SR-TE configs

router ospf CORE

```

nsr
distributed link-state          Command to distribute OSPF database into SR-TE database
log adjacency changes
router-id <Router-ID-PE1>     OSPF Router-ID
segment-routing mpls
nsf cisco
microloop avoidance segment-routing Command to enable microloop avoidance with TI-LFA
area 0
interface Bundle-Ether<Intf-Number> OSPF PE to P Link
cost 100                        OSPF PE to P Metric
authentication keychain <Key-Chain> Command to enable OSPF Authentication per link
network point-to-point
    
```

```

fast-reroute per-prefix          Commands to enable TI-LFA

fast-reroute per-prefix ti-lfa enable

fast-reroute per-prefix tiebreaker node-protecting index <Index-Value>

prefix-suppression

!

interface Loopback <Loopback-ID-PE1>

passive enable

prefix-sid index <SID-Index-Number1>    OSPF Loopback Prefix SID

```

Anmerkung: So konfigurieren Sie den Befehl **Source-Address**" entweder GLOBAL ODER unter RICHTLINIE. Als Standardverhalten ersetzt die Quelladresse unter Richtlinie den globalen Befehl.

Der Befehl "source address" unter der Segmentrouting-Konfiguration wird in bestimmten Szenarien benötigt, in denen im selben PE, als Quelle der SR-TE-Richtlinie, eine Loopback-Adresse unter mehreren oder wenn sowohl ISIS als auch OSPF mit separaten Loopbacks ausgeführt werden müssen, und in einem dieser Szenarien einfrieren muss. Andernfalls ist in normalen Szenarien, in denen nur ein IGP mit einem eindeutigen Loopback ausgeführt wird, die Konfiguration der Quelladresse optional.

segment-routing

```

global-block 16000 23999    Default SRGB Value (Need not be configured). Needs to be configured
only if non-default value is assigned

```

```

local-block 15000 15999    Default SRLB Value (Need not be configured). Needs to be configured
only if non-default value is assigned

```

```

traffic-eng

```

candidate-paths

```

all

```

```

source-address ipv4

```

Configure SR-TE source address as OSPF loopback (Global Option)

```

!
```

```

!
```

```

segment-list name <SIDLIST1>    Primary/Normal Path SID-LIST1

index <Index ID> mpls adjacency <Remote-IP-Address-Link1>

index <Index ID> mpls adjacency <Remote-IP-Address-Link2>

index <Index ID> mpls adjacency <Remote-IP-Address-Link3>

```

```

!
segment-list name <SIDLIST2>      Primary Back Up Path SID-LIST2
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
!
segment-list name <SIDLIST3>      Secondary Back Up Path SID-LIST3
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
!
policy <Pol-Name1>
source-address ipv4

    Configure SR-TE source address as OSPF loopback (Policy Specific Option)
color <Color-ID> end-point ipv4 <Destn-PE3>
candidate-paths
preference 50      Tertiary Back Up Path with least preference
dynamic
metric
    type igp
!
!
!
preference 100    Secondary Back Up Path with 3rd highest preference
explicit segment-list <SIDLIST3>
!
!
preference 150    Primary Back Up Path with 2nd highest preference
explicit segment-list <SIDLIST2>
!
!

```

preference 200 Primary/Normal Path with highest preference (**Active Path for PE1 in this scenario**)

```
explicit segment-list <SIDLIST1>
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

PE2 Node: OSPF & SR-TE configs

router ospf CORE

```
nsr
```

```
distribute link-state database Command to distribute OSPF database into SR-TE
```

```
log adjacency changes
```

```
router-id <Router-ID-PE2> OSPF Router-ID
```

```
segment-routing mpls
```

```
nsf cisco
```

```
microloop avoidance segment-routing Command to enable microloop avoidance with TI-LFA
```

```
area 0
```

```
interface Bundle-Ether<Intf-Number> OSPF PE to P Link
```

```
cost 100 OSPF PE to P Metric
```

```
authentication keychain <Key-Chain> Command to enable OSPF Authentication per link
```

```
network point-to-point
```

```
fast-reroute per-prefix Commands to enable TI-LFA
```

```
fast-reroute per-prefix ti-lfa enable
```

```
fast-reroute per-prefix tiebreaker node-protecting index <Index-Value>
```

```
prefix-suppression
```

```
!
```

```
interface Loopback <Loopback-ID-PE2>
```

```
passive enable
```

```
prefix-sid index <SID-Index-Number2> OSPF Loopback Prefix SID
```

Anmerkung: Die optionalen **Quelladressen-, Standard-SRGB-** und **SRLB-**Befehle wurden entfernt.

segment-routing

```
traffic-eng
```

```
!
```

```
!
```

```
segment-list name <SIDLIST1> Primary/Normal Path SID-LIST1
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link1>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
```

```
!
```

```
segment-list name <SIDLIST2> Primary Back Up Path SID-LIST2
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
segment-list name <SIDLIST3> Secondary Back Up Path SID-LIST3
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
policy <Pol-Name1>
```

```
source-address ipv4
```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```
color <Color-ID> end-point ipv4 <Destn-PE4>
```

```
candidate-paths
```

```
preference 50 Tertiary Back Up Path with least preference
```

```
dynamic
```



```

metric

type igp

!

!

!

preference 100      Secondary Back Up Path with 3rd highest preference

explicit segment-list <SIDLIST3>

!

!

preference 150      Primary Back Up Path with 2nd highest preference

explicit segment-list <SIDLIST2>

!

!

preference 200      Primary/Normal Path with highest preference (Active Path for PE2 in this
scenario)

explicit segment-list <SIDLIST1>

!

!

!

!

!

```

Anmerkung: In der zuvor erwähnten Lösung basieren die expliziten Hops der Segmentlisten auf IP-Adressen, da, wie hier erwähnt, die explizite Richtlinienkonfiguration für den Pfad SR-TE auf der Grundlage von "**mpls label**" die Pfadvalidierung bei Ausfall von Remote-Verbindungen in 7.3.x nicht funktioniert

Falls eine Remote-Verbindung außer der lokalen Verbindung eines PE-Knotens ausfällt, bleibt der Pfad gültig. Diese Version ist so konzipiert und kann erst ab XR 7.5.x geändert werden.

PE Node: SR-TE configs

```

router ospf <Process-Name>

  address-family ipv4 unicast

  area 0

  interface <Core BE Intf1>

  adjacency-sid absolute <Adj-SID1>

  interface <Core BE Intf2>

  adjacency-sid absolute < Adj-SID2>

  interface <Core BE Intf3>

  adjacency-sid absolute < Adj-SID3>

segment-routing

  traffic-eng

  policy <Pol-Name1>

  color <Color-ID> end-point ipv4 <Destn-PE>

  candidate-paths

  preference 10

  explicit segment-list <SIDLIST1>

  !

  preference 20

  dynamic

  metric

  type igp

  !

segment-list name <SIDLIST1>

  index 10 mpls label <Adj-SID-Link1>

  index 20 mpls label <Adj-SID-Link2>

  index 30 mpls label <Adj-SID-Link3>

```

8.6.2. SR-TE für Failover-Szenarien

Um die Szenarien für den Datenverkehr-Failover zu verstehen, muss der primäre Pfadverkehr unter normalen Verkehrsbedingungen genau geprüft werden, wie im Topologiediagramm im vorherigen Unterabschnitt beschrieben.

Das Hauptziel bei Failover-Szenarien besteht darin, die Uneinheitlichkeit des Datenverkehrspfads

im Rahmen der aktuellen Topologieinfrastruktur so weit wie möglich zu halten. Das Netzwerk XYZ unterliegt strengen Anforderungen, um den Datenverkehr administrativ durch bestimmte Knoten in Backup-Pfaden zu leiten, um eine maximale Trennung zwischen den Quell-Ziel-Knotenpaaren zu gewährleisten. Dieses Design soll verhindern, dass die verwendeten Links überlastet werden und dass nur ungenutzte Links verwendet werden.

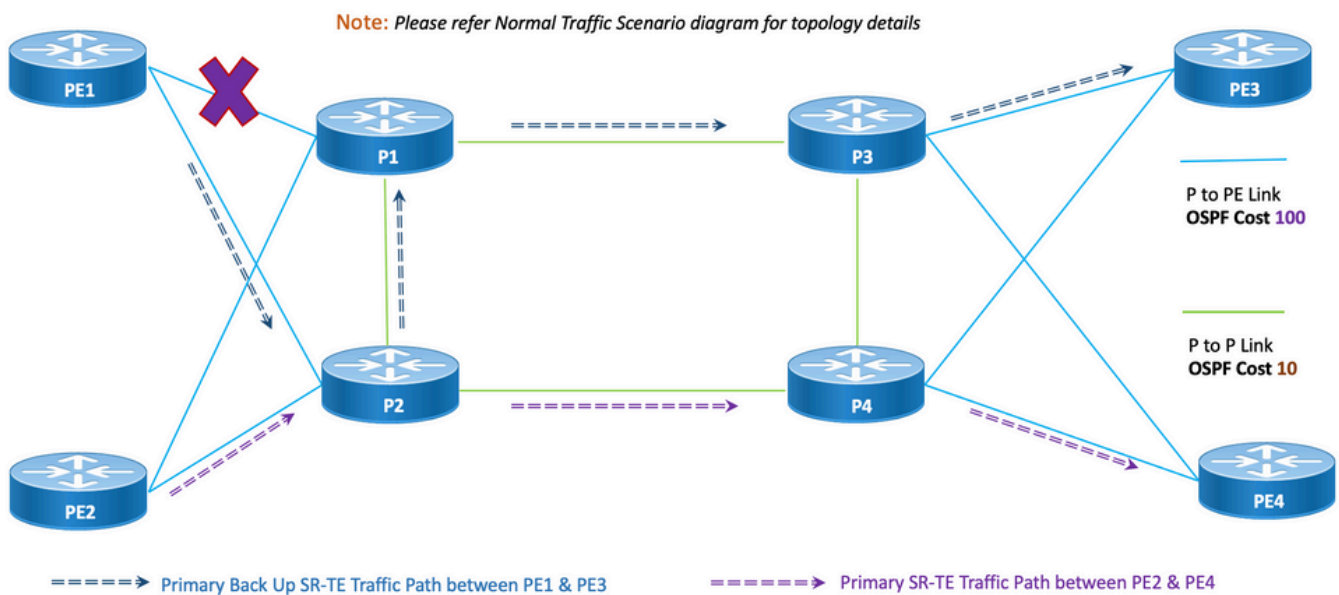
In diesen Unterabschnitten werden die verschiedenen Failover-Szenarien wie Single Link (eine Verbindung), Double Link (eine Verbindung), Single Node (ein Knoten) und Double Node (zwei Knoten) mit dem Failover-Pfad dargestellt, den der Datenverkehr benötigt, um maximale Uneinheitlichkeit zu gewährleisten.

8.6.3. Szenario für Single-Link-Failover

Hierbei handelt es sich um das Szenario eines Verbindungsausfalls, bei dem die lokale Verbindung zwischen PE1 und P1 ausfällt und der Datenverkehr einen Umweg über die Core-P2- und P1-Knoten durchläuft. Diese wird administrativ über die Segmentliste <SIDLIST1> gesteuert, die den primären Backup-Pfad zwischen PE1- und PE3-Knoten bildet.

Abbildung 13: Szenario für Single-Link-Failover

Single Link Failure



Uneinheitlichkeit: Bei Ausfall einer Verbindung beträgt die Anzahl der gemeinsam genutzten Verbindungen null (0), wie in der vorherigen Topologie gezeigt.

8.6.3.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die relevanten Konfigurationsvorlagen für OSPF/SR-TE für PE1- und PE2-Knoten wie folgt:

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

PE1 Node: OSPF & SR-TE configs

segment-routing

traffic-eng

!

!

segment-list name <SIDLIST1> Primary/Normal Path SID-LIST1

index <Index ID> mpls adjacency <Remote-IP-Address-Link1>

index <Index ID> mpls adjacency <Remote-IP-Address-Link2>

index <Index ID> mpls adjacency <Remote-IP-Address-Link3>

!

segment-list name <SIDLIST2> Primary Back Up Path SID-LIST2

index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

segment-list name <SIDLIST3> Secondary Back Up Path SID-LIST3

index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

policy <Pol-Name1>

source-address ipv4

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

color <Color-ID> end-point ipv4 <Destn-PE3>

candidate-paths

preference 50 Tertiary Back Up Path with least preference

dynamic

metric

type igp


```

index <Index ID> mpls adjacency <Remote-IP-Address-Link2>

index <Index ID> mpls adjacency <Remote-IP-Address-Link3>

!

segment-list name <SIDLIST2>      Primary Back Up Path SID-LIST2

index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

segment-list name <SIDLIST3>      Secondary Back Up Path SID-LIST3

index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

policy <Pol-Name1>

source-address ipv4

```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```

color <Color-ID> end-point ipv4 <Destn-PE4>

candidate-paths

preference 50      Tertiary Back Up Path with least preference

dynamic

metric

type igp

!

!

!

preference 100    Secondary Back Up Path with 3rd highest preference

explicit segment-list <SIDLIST3>

!

!

preference 150    Primary Back Up Path with 2nd highest preference

explicit segment-list <SIDLIST2>

```

```
!  
!  
preference 200    Primary/Normal Path with highest preference (Active Path for PE2 in this  
scenario)  
  
    explicit segment-list <SIDLIST1>  
  
!  
!  
  
!  
!  
!  
!  
!
```

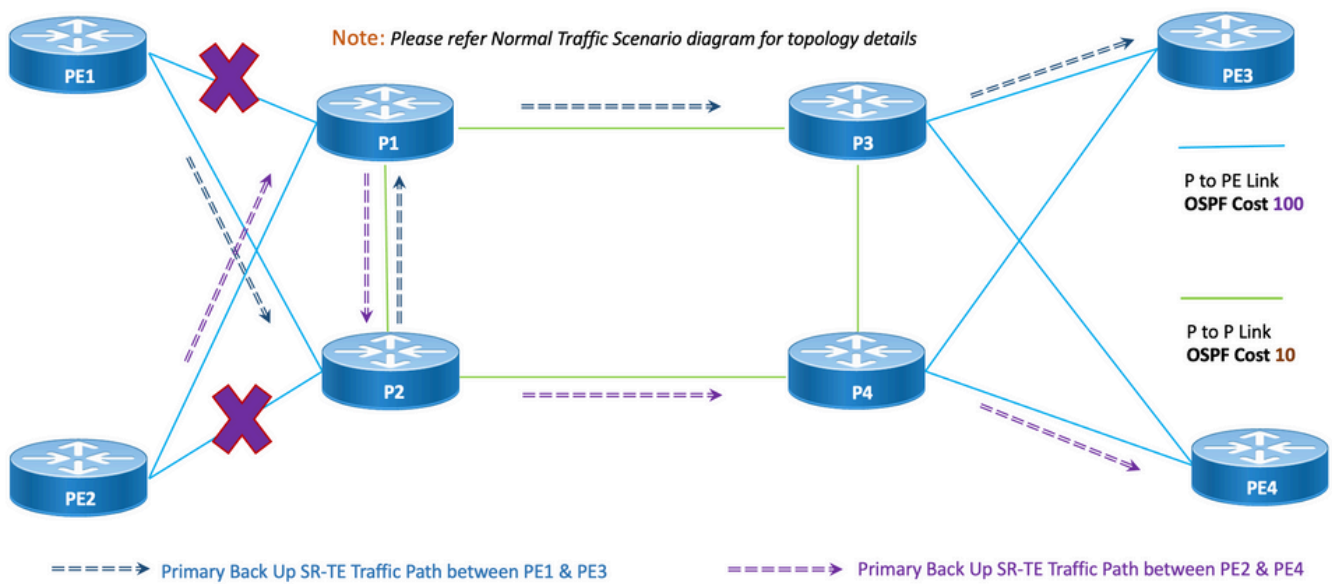
8.6.4. Failover-Szenario für doppelte Verbindung

Dies ist das Szenario eines doppelten Verbindungsausfalls, bei dem die lokale Verbindung zwischen PE1 und P1 und der lokalen Verbindung zwischen PE2 und P2 ausfällt. Der Datenverkehr von PE1 erfolgt über die Core-P2- und P1-Knoten, und der Datenverkehr von PE2 erfolgt über die Core-P1- und P2-Knoten.

Diese werden administrativ über die jeweilige Segmentliste <SIDLIST2> von PE1 und PE2 gesteuert, die die sekundären Backup-Pfade zwischen PE1- und PE3- bzw. PE2- bzw. PE4-Knoten bilden.

Abbildung 14: Failover-Szenario für doppelte Verbindung

Double Link Failure



Uneinheitlichkeit: Bei einem Ausfall einer doppelten Verbindung wird eine (1) gemeinsame Verbindung verwendet, wie in der oben genannten Topologie gezeigt.

8.6.4.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die relevanten Konfigurationsvorlagen für OSPF/SR-TE für PE1- und PE2-Knoten wie folgt:

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

```
# PE1 Node: OSPF & SR-TE configs
```

```
#show run router ospf
```

```
router ospf CORE
```

```
  distribute link-state
```

```
  log adjacency changes
```

```
  router-id 11.11.11.11
```

```
  segment-routing mpls
```

```
  microloop avoidance segment-routing
```

```
  area 0
```

```
  interface Bundle-Ether11
```



```
cost 100

authentication keychain XYZ-CONT-PE1

network point-to-point

fast-reroute per-prefix

fast-reroute per-prefix ti-lfa enable

fast-reroute per-prefix tiebreaker node-protecting index 200

prefix-suppression

!

interface Bundle-Ether12

cost 100

authentication keychain XYZ-CONT-PE1

network point-to-point

fast-reroute per-prefix

fast-reroute per-prefix ti-lfa enable

fast-reroute per-prefix tiebreaker node-protecting index 200

prefix-suppression

!

interface Loopback0

passive enable

prefix-sid index 11

!

!
```

segment-routing

```
traffic-eng

!

!

segment-list name <SIDLIST1> Primary/Normal Path SID-LIST1

index <Index ID> mpls adjacency <Remote-IP-Address-Link1>

index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
```

```
!
```

```
segment-list name <SIDLIST2> Primary Back Up Path SID-LIST2
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
segment-list name <SIDLIST3> Secondary Back Up Path SID-LIST3
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
policy <Pol-Name1>
```

```
source-address ipv4
```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```
color <Color-ID> end-point ipv4 <Destn-PE3>
```

```
candidate-paths
```

```
preference 50 Tertiary Back Up Path with least preference
```

```
dynamic
```

```
metric
```

```
type igp
```

```
!
```

```
!
```

```
!
```

```
preference 100 Secondary Back Up Path with 3rd highest preference
```

```
explicit segment-list <SIDLIST3>
```

```
!
```

```
!
```

```
preference 150 Primary Back Up Path with 2nd highest preference (Active Path for PE1 in this scenario)
```

```
explicit segment-list <SIDLIST2>
```

```

!
!
preference 200    Primary/Normal Path with highest preference
explicit segment-list <SIDLIST1>
!
!
!
!
!
!
!
!
!

```

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

PE2 Node: OSPF & SR-TE configs

segment-routing

traffic-eng

```

!
!
segment-list name <SIDLIST1>    Primary/Normal Path SID-LIST1
    index <Index ID> mpls adjacency <Remote-IP-Address-Link1>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
!
segment-list name <SIDLIST2>    Primary Back Up Path SID-LIST2
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
!
segment-list name <SIDLIST3>    Secondary Back Up Path SID-LIST3
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

```

```

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

policy <Pol-Name1>

source-address ipv4

        Configure SR-TE source address as OSPF loopback (Policy Specific Option)

color <Color-ID> end-point ipv4 <Destn-PE4>

candidate-paths

preference 50      Tertiary Back Up Path with least preference

dynamic

metric

type igp

!

!

!

preference 100    Secondary Back Up Path with 3rd highest preference

explicit segment-list <SIDLIST3>

!

!

preference 150    Primary Back Up Path with 2nd highest preference (Active Path for PE2 in this scenario)

explicit segment-list <SIDLIST2>

!

!

preference 200    Primary/Normal Path with highest preference

explicit segment-list <SIDLIST1>

!

!

!

!

```

!

!

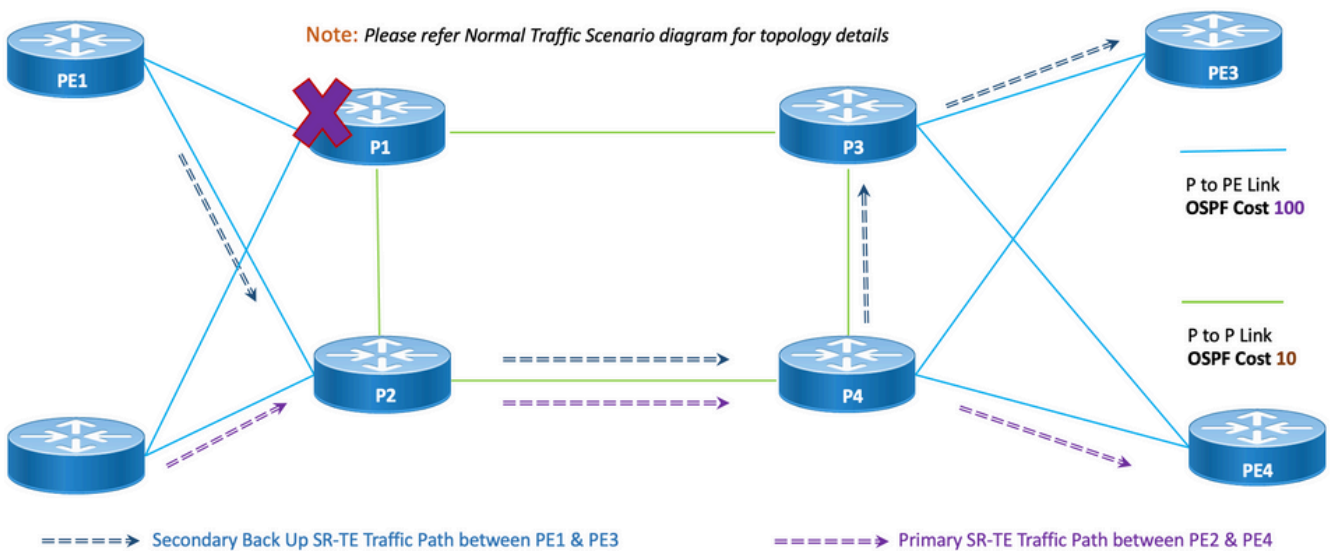
8.6.5. Failover-Szenario für einen Knoten

Dies ist das Szenario eines Knotenausfalls, bei dem der Knoten P1 ausfällt und der Datenverkehr einen Umweg über die Core-P2- und P4-Knoten zurücklegt. Diese wird administrativ über die Segmentliste <SIDLIST3> gesteuert, die den sekundären Backup-Pfad zwischen PE1- und PE3-Knoten bildet.

Der Datenverkehr zwischen PE2 und PE4 bleibt jedoch der gleiche wie der primäre Pfad, der in dieser Topologie gezeigt wird.

Abbildung 15: Failover-Szenario für einen Knoten

Single Node Failure



Uneinheitlichkeit: Bei Ausfall eines Knotens ist die Anzahl der gemeinsam genutzten Verbindungen eine (1), wie in der oben genannten Topologie gezeigt.

8.6.5.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die entsprechenden Konfigurationsvorlagen für OSPF/SR-TE für PE1- und PE2-Knoten wie folgt:

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

segment-routing

traffic-eng

```

!
!
segment-list name <SIDLIST1>      Primary/Normal Path SID-LIST1
    index <Index ID> mpls adjacency <Remote-IP-Address-Link1>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
!
segment-list name <SIDLIST2>      Primary Back Up Path SID-LIST2
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
!
segment-list name <SIDLIST3>      Secondary Back Up Path SID-LIST3
    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
!
policy <Pol-Name1>
    source-address ipv4

```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```

color <Color-ID> end-point ipv4 <Destn-PE3>
candidate-paths
    preference 50      Tertiary Back Up Path with least preference
dynamic
metric
    type igp
!
!
!
preference 100      Secondary Back Up Path with 3rd highest preference (Active Path for PE1 in this scenario)

```

```

explicit segment-list <SIDLIST3>

!

!

preference 150    Primary Back Up Path with 2nd highest preference

explicit segment-list <SIDLIST2>

!

!

preference 200    Primary/Normal Path with highest preference

explicit segment-list <SIDLIST1>

!

!

!

!

!

!

!

!

!

```

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

PE2 Node: OSPF & SR-TE configs

segment-routing

```

traffic-eng

!

!

segment-list name <SIDLIST1>    Primary/Normal Path SID-LIST1

    index <Index ID> mpls adjacency <Remote-IP-Address-Link1>

    index <Index ID> mpls adjacency <Remote-IP-Address-Link2>

    index <Index ID> mpls adjacency <Remote-IP-Address-Link3>

!

segment-list name <SIDLIST2>    Primary Back Up Path SID-LIST2

    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

```

```

index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

segment-list name <SIDLIST3>      Secondary Back Up Path SID-LIST3

    index <Index ID> mpls adjacency <Remote-IP-Address-Link4>

    index <Index ID> mpls adjacency <Remote-IP-Address-Link5>

    index <Index ID> mpls adjacency <Remote-IP-Address-Link6>

!

policy <Pol-Name1>

source-address ipv4

        Configure SR-TE source address as OSPF loopback (Policy Specific Option)

color <Color-ID> end-point ipv4 <Destn-PE4>

candidate-paths

preference 50      Tertiary Back Up Path with least preference

dynamic

metric

    type igp

!

!

!

preference 100    Secondary Back Up Path with 3rd highest preference

explicit segment-list <SIDLIST3>

!

!

preference 150    Primary Back Up Path with 2nd highest preference

explicit segment-list <SIDLIST2>

!

!

preference 200    Primary/Normal Path with highest preference (Active Path for PE2 in this scenario)

explicit segment-list <SIDLIST1>

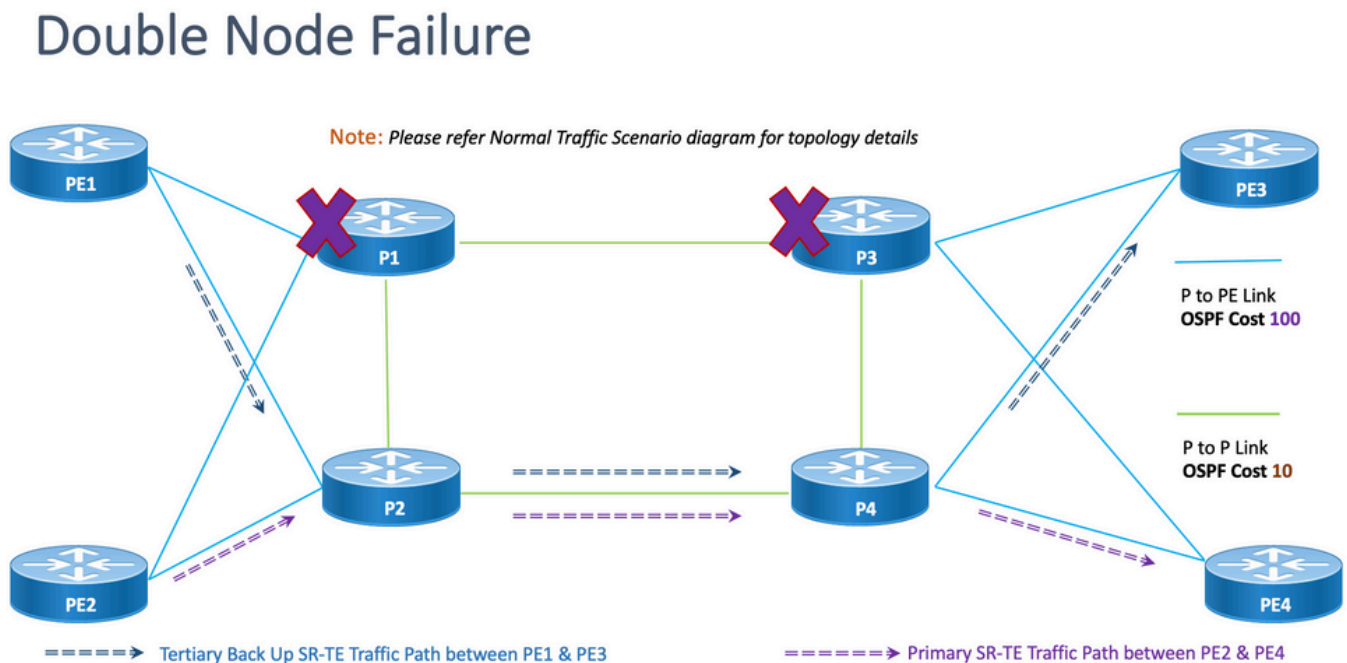
```


8.6.6. Failover-Szenario mit doppeltem Knoten

Dies ist das Szenario eines doppelten Knotenausfalls, bei dem die Knoten P1 und P3 ausfallen und der Datenverkehr einen Umweg über die P2- und P4-Core-Knoten zurücklegt. Diese wird administrativ über die Segmentliste <SIDLIST3> gesteuert, die den sekundären Backup-Pfad zwischen PE1- und PE3-Knoten bildet. Da die expliziten Pfade nur für die zuvor genannten beiden Szenarien definiert sind, bildet der dynamische IGP-Pfad hier den tertiären Backup-Pfad und übernimmt die Rolle des Routings des Datenverkehrs über die P2- und P4-Knoten.

Der Datenverkehr zwischen PE2 und PE4 bleibt jedoch der gleiche wie der primäre Pfad, der in dieser Topologie gezeigt wird.

Abbildung 16: Failover-Szenario mit doppeltem Knoten



Uneinheitlichkeit: Bei Ausfall eines doppelten Knotens beträgt die Anzahl der gemeinsam genutzten Verbindungen 1 (1), wie in dieser Topologie gezeigt.

8.6.6.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die entsprechenden Konfigurationsvorlagen für OSPF/SR-TE für

PE1- und PE2-Knoten wie folgt:

Anmerkung: Die OSPF-Konfigurationsvorlagen für PE1 und PE2 des Routers ähneln dem normalen Szenario.

```
# PE1 Node: OSPF & SR-TE configs
segment-routing
```

```
traffic-eng
```

```
!
```

```
!
```

```
segment-list name <SIDLIST1> Primary/Normal Path SID-LIST1
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link1>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
```

```
!
```

```
segment-list name <SIDLIST2> Primary Back Up Path SID-LIST2
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
segment-list name <SIDLIST3> Secondary Back Up Path SID-LIST3
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

```
!
```

```
policy <Pol-Name1>
```

```
source-address ipv4
```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```
color <Color-ID> end-point ipv4 <Destn-PE3>
```

```
candidate-paths
```

```
preference 50 Tertiary Back Up Path with least preference (Active Path for PE1 in this scenario -
```

```
Policy chooses Least Cost IGP Back Up Path in absence of Valid Explicit Path)
```



```
index <Index ID> mpls adjacency <Remote-IP-Address-Link1>
index <Index ID> mpls adjacency <Remote-IP-Address-Link2>
index <Index ID> mpls adjacency <Remote-IP-Address-Link3>
```

!

```
segment-list name <SIDLIST2>      Primary Back Up Path SID-LIST2
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

!

```
segment-list name <SIDLIST3>      Secondary Back Up Path SID-LIST3
```

```
index <Index ID> mpls adjacency <Remote-IP-Address-Link4>
index <Index ID> mpls adjacency <Remote-IP-Address-Link5>
index <Index ID> mpls adjacency <Remote-IP-Address-Link6>
```

!

```
policy <Pol-Name1>
```

```
source-address ipv4
```

Configure SR-TE source address as OSPF loopback (Policy Specific Option)

```
color <Color-ID> end-point ipv4 <Destn-PE4>
```

```
candidate-paths
```

```
preference 50      Tertiary Back Up Path with least preference
```

```
dynamic
```

```
metric
```

```
type igp
```

!

!

!

```
preference 100    Secondary Back Up Path with 3rd highest preference
```

```
explicit segment-list <SIDLIST3>
```

!

!

```
preference 150    Primary Back Up Path with 2nd highest preference
```

```

explicit segment-list <SIDLIST2>

!

!

preference 200    Primary/Normal Path with highest preference (Active Path for PE2 in this scenario)

explicit segment-list <SIDLIST1>

!

!

!

!

!

!

```

8.7. BGP/RR-Designübersicht

Border Gateway Protocol (BGP) ist das Protokoll, das grundlegende Routing-Entscheidungen im Internet trifft. Es verwaltet eine Tabelle mit IP-Netzwerken oder "Präfixen", die die Netzwerkerreichbarkeit unter autonomen Systemen (AS) bestimmen. Sie wird als Pfadvektor-Protokoll beschrieben. BGP verwendet keine herkömmlichen IGP-Metriken (Interior Gateway Protocol), trifft jedoch Routing-Entscheidungen auf der Grundlage von Pfad, Netzwerkrichtlinien und/oder Regelsätzen. Aus diesem Grund wird es eher als Reach-ability-Protokoll und nicht als Routing-Protokoll bezeichnet.

MP-BGP kann verwendet werden, um IPv4-, IPv6-, VPNv4-, VPNv6-, EVPN- und Link-State-Präfixe über das Netzwerk zu propagieren. Dies erfolgt über eine Routen-Reflektor-Konfiguration, die iBGP-Nachbarn mit Core-, Aggregations-, Access-Devices und SR-PCE-Geräten bildet.

Über den RR werden vom BGP bezogene Präfixe intern über iBGP propagiert. BGP-Routen werden nie in IGP neu verteilt. Die Routen-Reflektoren sind vollständig von der Datenebene isoliert und dienen der Kontrollebene.

8.7.1. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die entsprechenden Konfigurationsvorlagen für BGP/RR wie folgt:

PE Node: Relevant BGP configs

```

router bgp <PE-ASN>

address-family l2vpn evpn

!

```

```

neighbor-group <RR-EVPN>           Neighbor group of Route Reflector (RR)

remote-as <RR-ASN>

update-source <PE-Self-Loopback>

!

address-family l2vpn evpn          AF L2VPN EVPN Neighborhood with RR

maximum-prefix <PREFIX> <PERCENT> warning-only

!

address-family ipv4 rt-filter

!

neighbor <RR1-Loopback>            Neighborhood with RR1 using the above neighbor group

use neighbor-group <RR-EVPN>

neighbor <RR2-Loopback>            Neighborhood with RR2 using the above neighbor group

use neighbor-group <RR-EVPN>

# RR Nodes: Relevant BGP configs

router bgp <RR-ASN>

address-family l2vpn evpn

!

neighbor-group <PE-EVPN>           Neighbor group of Provider Edge (PE)

remote-as <PE-ASN>

update-source <RR-Self-Loopback>

!

address-family l2vpn evpn          AF L2VPN EVPN Neighborhood with PE

route-reflector-client

!

address-family ipv4 rt-filter

!

neighbor <PE1-Loopback>            Neighborhood with PE1 using the above neighbor group

use neighbor-group <PE-EVPN>

```

```
neighbor <PE2-Loopback>      Neighborhood with PE2 using the above neighbor group
```

```
use neighbor-group <PE-EVPN>
```

8.8. Überblick über das Servicekondesign

Dieser Unterabschnitt beschreibt den EVPN VPWS Overlay Service zusammen mit der Darstellung des unterstützten Label-Stacks und der Konfigurationsvorlagen.

EVPN-VPWS ist eine BGP-Kontrollebenenlösung für Point-to-Point-Services. Es implementiert die Signalisierungs- und Kapselungstechniken, die eine EVPN-Instanz zwischen einem Paar von PEs erstellen. Es kann Datenverkehr ohne MAC-Suche von einem Netzwerk an ein anderes weiterleiten. Die Verwendung von EVPN für VPWS macht die Signalisierung von PWs mit einem Segment und mehreren Segmenten für Punkt-zu-Punkt-Ethernet-Services überflüssig. Die EVPN-VPWS-Technologie arbeitet mit IP- und MPLS-Core. Der IP-Core unterstützt BGP- und MPLS-Core für das Switching von Paketen zwischen den Endpunkten.

8.8.1. Label Stack-Darstellung

Der Service unterstützt bis zu 5 bis 6 SR Label-Stacks, darunter SR Transport Label, EVPN Labels und FAT Labels für den Lastenausgleich. Dies ist die analysierte maximale Anzahl von Labels in **Normal Scenarios**, bei denen der Datenverkehr durch einen expliziten primären Pfad fließt:

```
ADJ SID1  
ADJ SID2  
ADJ SID3  
EVPN-ETIKETT  
FLUSSETIKETT  
(S=1)
```

Dies ist die analysierte maximale Anzahl von Labels in **Failover-Szenarien**, bei denen der Datenverkehr über Backup Explicit Path oder einen vom IGP definierten dynamischen Backup-Pfad fließt:

```
TI-LFA SID1  
TI-LFA SID2  
TI-LFA SID3  
EVPN-ETIKETT  
FLUSSETIKETT  
(S=1)
```

8.8.2. Konfigurationsvorlagen

Dieser Unterabschnitt enthält die entsprechenden Konfigurationsvorlagen für EVPN-VPWS, wie hier gezeigt:

```
# PE Node: EVPN configs
```

```
evpn
```

```

evi <EVI-ID>          Ethernet Virtual Identifier

bgp

  rd <RD-Value>

  route-target import <RT-Value>

  route-target export <RT-Value>

!

load-balancing

  flow-label static   Generates bottom-most label (S=1) for load balancing between intra & inter
BE end-to-end

!

!

interface <AC-Interface>

l2vpn

  pw-class <PW-Class-Name1>

  encapsulation mpls

  preferred-path sr-te policy <Pol-Name1>          Attaching SR-TE policy as the traffic path
of EVPN

!

!

xconnect group <Group-Name>

p2p <P2P-Name>

  interface <AC-Subinterface>                      EVPN Attachment Circuit Interface towards CE

  neighbor evpn evi <EVI-ID> service <Service-ID> Service ID defined should match at both the
end PEs

  pw-class <PW-Class-Name1>

!

```

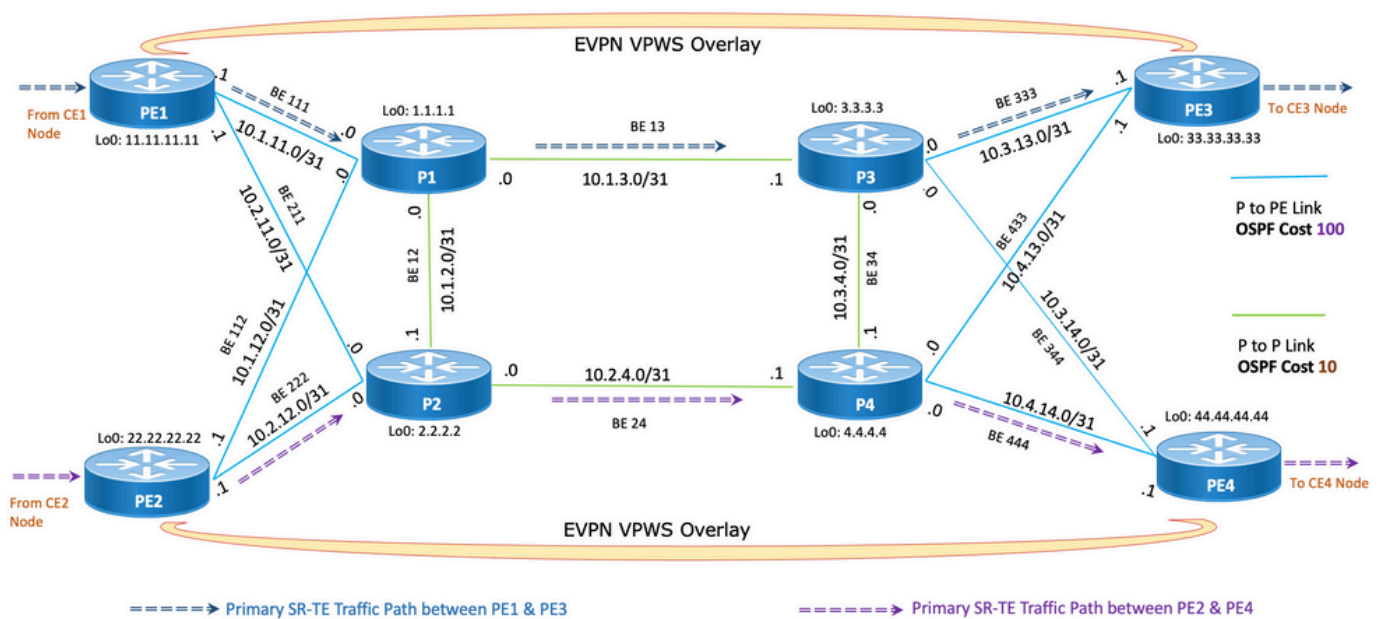
9. Beispielkonfiguration und Anzeigen von Befehlen

Dieser letzte Abschnitt enthält die relevante Konfiguration und die Befehle der PE-Knoten nur für das normale Datenverkehrsszenario. Diese werden hier erfasst, abgestimmt auf die in dieser Abbildung angegebenen Parameter als Referenz, die das Verständnis der in den vorherigen Abschnitten beschriebenen Konfigurationsvorlagen erleichtert.

9.1. Beispielkonfiguration an PE-Knoten

Abbildung 17: Topologie mit Konfigurationsparametern.

Normal Traffic Scenario: SR-TE Steered Path with EVPN Overlay



PE1 Node: OSPF & SR-TE Config

#show run router ospf

router ospf CORE

distributed link-state
database

Command to distribute OSPF database into SR-TE

log adjacency changes

router-id 11.11.11.11

OSPF Router ID

segment-routing mpls

microloop avoidance segment-routing

Command to enable microloop avoidance with TI-LFA

area 0

interface Bundle-Ether111

OSPF PE to P Link

cost 100

OSPF PE to P Metric

authentication keychain XYZ-CONT-PE1

Command to enable OSPF Authentication per link

network point-to-point

```
fast-reroute per-prefix                Commands to enable TI-LFA

fast-reroute per-prefix ti-lfa enable

fast-reroute per-prefix tiebreaker node-protecting index 200

prefix-suppression

!

interface Bundle-Ether211

cost 100

authentication keychain XYZ-CONT-PE1

network point-to-point

fast-reroute per-prefix

fast-reroute per-prefix ti-lfa enable

fast-reroute per-prefix tiebreaker node-protecting index 200

prefix-suppression

!

interface Loopback0

passive enable

prefix-sid index 11                    OSPF Loopback Prefix SID

!

!

!

#show run segment-routing

Sat Apr 16 23:22:42.727 UTC

segment-routing

traffic-eng

segment-list PrimaryPath                Primary/Normal Path

index 10 mpls adjacency 10.1.11.0

index 20 mpls adjacency 10.1.3.1

index 30 mpls adjacency 10.3.13.1

!

segment-list PrimaryBackUpPath          Primary Back Up Path

index 10 mpls adjacency 10.2.11.0

index 20 mpls adjacency 10.1.2.0
```

```
index 30 mpls adjacency 10.1.3.1
!
segment-list SecondaryBackUpPath          Secondary Back Up Path
index 10 mpls adjacency 10.2.11.0
index 20 mpls adjacency 10.2.4.1
index 30 mpls adjacency 10.3.4.0
!
policy SR-TE_POLICY_PE1-to-PE3          SR-TE Policy Towards PE3
color 10 end-point ipv4 33.33.33.33     SR-TE Policy End-Point PE3 Loopback
candidate-paths
preference 50                            Tertiary Back Up Dynamic IGP Path with 4th highest preference
dynamic
metric
type igp
!
!
!
preference 100                           Secondary Back Up Path with 3rd highest preference
explicit segment-list SecondaryBackUpPath
!
!
preference 150                           Primary Back Up Path with 2nd highest preference
explicit segment-list PrimaryBackUpPath
!
!
preference 200                           Primary and Active Path with highest preference
explicit segment-list PrimaryPath
!
!
!
!
!
```

!

PE2 Node: OSPF & SR-TE Config

#show run router ospf

router ospf CORE

```

distribute link-state database          Command to distribute OSPF database into SR-TE
log adjacency changes
router-id 22.22.22.22                   OSPF Router ID
segment-routing mpls
microloop avoidance segment-routing     Command to enable microloop avoidance with TI-LFA
area 0
interface Bundle-Ether112               OSPF PE to P Link
  cost 100                               OSPF PE to P Metric
  authentication keychain XYZ-CONT-PE2
  network point-to-point
  fast-reroute per-prefix                Commands to enable TI-LFA
  fast-reroute per-prefix ti-lfa enable
  fast-reroute per-prefix tiebreaker node-protecting index 200
  prefix-suppression
!
interface Bundle-Ether222
  cost 100
  authentication keychain XYZ-CONT-PE2   Command to enable OSPF Authentication per link
  network point-to-point
  fast-reroute per-prefix                Commands to enable TI-LFA
  fast-reroute per-prefix ti-lfa enable
  fast-reroute per-prefix tiebreaker node-protecting index 200
  prefix-suppression
!
```

```
interface Loopback0
  passive enable
  prefix-sid index 22          OSPF Loopback Prefix SID
!
!
!
```

#show run segment-routing

Sat Apr 16 23:22:42.727 UTC

segment-routing

```
traffic-eng
segment-list PrimaryPath      Primary/Normal Path
  index 10 mpls adjacency 10.2.12.0
  index 20 mpls adjacency 10.2.4.1
  index 30 mpls adjacency 10.4.14.1
!
segment-list PrimaryBackUpPath  Primary Back Up Path
  index 10 mpls adjacency 10.1.12.0
  index 20 mpls adjacency 10.1.2.1
  index 30 mpls adjacency 10.2.4.1
!
segment-list SecondaryBackUpPath  Secondary Back Up Path
  index 10 mpls adjacency 10.1.12.0
  index 20 mpls adjacency 10.1.3.1
  index 30 mpls adjacency 10.3.4.1
!
policy SR-TE_POLICY_PE2-to-PE4    SR-TE Policy Towards PE4
  color 10 end-point ipv4 44.44.44.44  SR-TE Policy End-Point PE4 Loopback
  candidate-paths
    preference 50                  Tertiary Back Up Dynamic IGP Path with 4th highest preference
    dynamic
    metric
```

```
type igp
!
!
!
preference 100           Secondary Back Up Path with 3rd highest preference
explicit segment-list SecondaryBackUpPath
!
!
preference 150          Primary Back Up Path with 2nd highest preference
explicit segment-list PrimaryBackUpPath
!
!
preference 200          Primary and Active Path with highest preference
explicit segment-list PrimaryPath
!
!
!
!
!
!
!
# PE1 Node: BGP Config
```

```
#show run router bgp
```

```
router bgp 64848
```

```
bgp router-id 11.11.11.11      BGP Router-ID
```

```
address-family l2vpn evpn
```

```
!
```

```
neighbor-group RR-EVPN
```

```
remote-as 64848
```

```
update-source Loopback0
```

```
address-family l2vpn evpn      BGP AF L2VPN EVPN
!
!
neighbor 10.10.10.10          Neighbor Route Reflector
use neighbor-group RR-EVPN
!
!
```

PE2 Node: BGP Config

#show run router bgp

router bgp 64848

```
bgp router-id 22.22.22.22     BGP Router-ID
address-family l2vpn evpn
!
neighbor-group RR-EVPN
remote-as 64848
update-source Loopback0
address-family l2vpn evpn     BGP AF L2VPN EVPN
!
!
neighbor 10.10.10.10          Neighbor Route Reflector
use neighbor-group RR-EVPN
!
!
```

PE1 Node: EVPN-VPWS Config

evpn

```
evi 100                       Ethernet Virtual Identifier
bgp
```

```
rd 11:11

route-target import 100:100

route-target export 100:100

!

load-balancing          Generates bottom-most label (S=1) for load balancing between
intra & inter BE end-to-end

flow-label static

!

!

interface Bundle-Ether99      Interface Attachment Circuit

ethernet-segment

identifier type 0 00.00.00.00.00.00.00.00.00

!

!

!
```

PE2 Node: EVPN-VPWS Config

evpn

```
evi 100          Ethernet Virtual Identifier

bgp

rd 11:11

route-target import 100:100

route-target export 100:100

!

load-balancing          Generates bottom-most label (S=1) for load balancing between
intra & inter BE end-to-end

flow-label static

!

!

interface Bundle-Ether99      Interface Attachment Circuit

ethernet-segment

identifier type 0 00.00.00.00.00.00.00.00.00
```


!
!
!

9.1. Relevante Show-Befehle an PE-Knoten

PE1 Node: SR-TE Show Command

#show segment-routing traffic-eng policy

Sat Apr 16 23:35:32.731 UTC

SR-TE policy database

Color: 10, End-point: 33.33.33.33

Name: srte_c_10_ep_33.33.33.33

Status:

Admin: up Operational: up for 00:12:54 (since Apr 16 23:22:38.278)

Candidate-paths:

Preference: 200 (configuration) **(active)** Active Path (Path in use)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list PrimaryPath **(valid)** Only the Active Path shows valid

Weight: 1, Metric Type: TE

24007 [Adjacency-SID, 10.1.11.0 - 10.1.11.1]

24007 [Adjacency-SID, 10.1.3.0 - 10.1.3.1]

24005 [Adjacency-SID, 10.3.13.0 - 10.3.13.1]

Preference: 150 (configuration)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list PrimaryBackUpPath (invalid) All inactive paths show invalid

Weight: 1, Metric Type: TE

Preference: 100 (configuration)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list SecondaryBackUpPath (invalid)

Weight: 1, Metric Type: TE

Preference: 50 (configuration)

All inactive paths show invalid

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Dynamic (invalid)

Metric Type: IGP, Path Accumulated Metric: 0

Attributes:

Binding SID: 24020

Forward Class: Not Configured

Steering labeled-services disabled: no

Steering BGP disabled: no

IPv6 caps enable: yes

Invalidation drop enabled: no

PE2 Node: SR-TE Show Command

#show segment-routing traffic-eng policy

Sat Apr 16 23:35:32.731 UTC

SR-TE policy database

Color: 10, End-point: 44.44.44.44

Name: srte_c_10_ep_44.44.44.44

Status:

Admin: up Operational: up for 00:12:54 (since Apr 16 23:22:38.278)

Candidate-paths:

Preference: 200 (configuration) (**active**) Active Path (Path in use)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list PrimaryPath (**valid**) Only the Active Path shows valid

Weight: 1, Metric Type: TE

24007 [Adjacency-SID, 10.2.12.0 - 10.2.12.1]

24007 [Adjacency-SID, 10.2.4.0 - 10.2.4.1]

24005 [Adjacency-SID, 10.4.14.0 - 10.4.14.1]

Preference: 150 (configuration)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list PrimaryBackUpPath (invalid) All inactive paths show invalid

Weight: 1, Metric Type: TE

Preference: 100 (configuration)

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Explicit: segment-list SecondaryBackUpPath (invalid)

Weight: 1, Metric Type: TE

Preference: 50 (configuration)

All inactive paths show invalid

Name: SR-TE_POLICY_PE1-to-PE3

Requested BSID: dynamic

Protection Type: protected-preferred

Maximum SID Depth: 12

Dynamic (invalid)

Metric Type: IGP, Path Accumulated Metric: 0

Attributes:

Binding SID: 24020

Forward Class: Not Configured

Steering labeled-services disabled: no

Steering BGP disabled: no

IPv6 caps enable: yes

Invalidation drop enabled: no

PE1 Node: BGP Show Command

#show bgp l2vpn evpn summary

Sun Apr 17 07:16:23.574 UTC

Address Family: L2VPN EVPN

BGP router identifier 11.11.11.11, local AS number 64848

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0x0 RD version: 0

BGP main routing table version 25

BGP NSR Initial initsync version 1 (Reached)

BGP NSR/ISSU Sync-Group versions 25/0

BGP scan interval 60 secs

BGP is operating in STANDALONE mode.

Process	RcvTblVer	bRIB/RIB	LabelVer	ImportVer	SendTblVer	StandbyVer
Speaker	25	25	25	25	25	25

Neighbor	Spk	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	St/PfxRcd
10.10.10.10	0	64848	9500	9484	25	0	0	5d16h	1

PE2 Node: BGP Show Command

#show bgp l2vpn evpn summary

Sun Apr 17 07:16:23.574 UTC

Address Family: L2VPN EVPN

BGP router identifier 22.22.22.22, local AS number 64848

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0x0 RD version: 0

BGP main routing table version 25

BGP NSR Initial initsync version 1 (Reached)

BGP NSR/ISSU Sync-Group versions 25/0

BGP scan interval 60 secs

BGP wird im STANDALONE-Modus betrieben.

Process	RcvTblVer	bRIB/RIB	LabelVer	ImportVer	SendTblVer	StandbyVer
Speaker	25	25	25	25	25	25

Neighbor	Spk	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	St/PfxRcd
10.10.10.10	0	64848	9500	9484	25	0	0	5d16h	1

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/segment-routing/configuration/guide/b-segment-routing-cg-asr9000-75x/about-segment-routing.html>
- <https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-5/lxvpn/configuration/guide/b-l2vpn-cg-asr9000-75x/evpn-features.html>
- [Technischer Support und Dokumentation für Cisco Systeme](#)