

Guia de Design Detalhado e Exemplos de Configuração da Política de Caminho Explícito SR-TE com EVPN VPWS, IOS XR Release - 7.5.x

Contents

[Introduction](#)

[1. Informações gerais](#)

[1.1. Fora do âmbito](#)

[1.2. Pressuposto](#)

[1.3. Âmbito técnico](#)

[1.4. Resumo do documento](#)

[Requisitos](#)

[2. Requisitos do usuário](#)

[2.1. Resumo dos requisitos](#)

[2.2. Componentes utilizados](#)

[Resumo da tecnologia](#)

[3. Roteamento de Segmento](#)

[3.1. O que é roteamento de segmento?](#)

[3.2. Identificadores de segmentos](#)

[4. Visão geral do SR-TE](#)

[4.1. O que é SR-TE?](#)

[4.2. Política SR-TE](#)

[5. RRF TI-LFA](#)

[5.1. Panorâmica](#)

[5.2. Impacto do método de detecção de anomalias na RRF](#)

[5.3. Prevenção de microlaço com SR](#)

[6. Sobreposição de EVPN](#)

[6.1. Benefícios do EVPN](#)

[6.1.1. Acesso Ethernet multilocal e totalmente ativo](#)

[6.2. Tipos de rota EVPN](#)

[6.2.1. Tipo de rota 1 - Rota de descoberta automática \(AD\) de Ethernet](#)

[6.2.2. Tipo de rota 4 - rota de segmento Ethernet](#)

[6.3. Conectividade do host EVPN](#)

[7. Balanceamento de carga e BoB](#)

[7.1. BFD sobre o pacote \(BoB\)](#)

[7.2. Balanceamento de carga](#)

[7.2.1. Balanceamento de carga do núcleo com rótulo FAT](#)

[7.2.2. Balanceamento de carga do circuito de ligação](#)

[Modelos de configuração e exemplos de comandos](#)

[8. A solução de projeto completa](#)

- [8.1. Requisitos de baixo nível](#)
 - [8.2. Resumo do projeto](#)
 - [8.3. Elementos de projeto](#)
 - [8.4. Exemplo de topologia física](#)
 - [8.5. Detalhes do projeto da camada 1](#)
 - [8.5.1. Modelos de configuração](#)
 - [8.6. Visão Geral do Projeto OSPF/SR-TE](#)
 - [8.6.1. Cenário de tráfego normal SR-TE](#)
 - [8.6.1.1. Modelos de configuração](#)
 - [8.6.2. SR-TE para cenários de failover](#)
 - [8.6.3. Cenário de failover de link único](#)
 - [8.6.3.1. Modelos de configuração](#)
 - [8.6.4. Cenário de failover de link duplo](#)
 - [8.6.4.1. Modelos de configuração](#)
 - [8.6.5. Cenário de failover de nó único](#)
 - [8.6.5.1. Modelos de configuração](#)
 - [8.6.6. Cenário de failover de nó duplo](#)
 - [8.6.6.1. Modelos de configuração](#)
 - [8.7. Visão geral do projeto BGP/RR](#)
 - [8.7.1. Modelos de configuração](#)
 - [8.8. Visão geral do design do serviço](#)
 - [8.8.1. Representação da pilha de rótulos](#)
 - [8.8.2. Modelos de configuração](#)
 - [9. Configuração de Exemplo e Comandos Show](#)
 - [9.1. Exemplo de configuração em nós PE](#)
 - [9.1. Comandos show relevantes nos nós PE](#)
- [Troubleshoot](#)
- [Informações Relacionadas](#)

Introduction

Este documento descreve o guia de projeto detalhado com descrições técnicas baseadas nos requisitos das redes XYZ e também fornece um modelo de configuração de baixo nível e configuração para os casos de uso de Política de caminho explícito de Engenharia de tráfego de roteamento de segmento (SR-TE - Segment Routing Traffic Engineering) com VPN Ethernet (EVPN - Virtual Private Wired Service) (VPWS - Virtual Private Wired Service).

1. Informações gerais

1.1. Fora do âmbito

Este documento não cobre os requisitos de políticas SR-TE "sob demanda" centralizadas que usam o controlador XTC, EVPN ELAN e assim por diante, mas focaliza apenas as políticas SR-TE orientadas por nó de fim de cabeçalho com sobreposição EVPN VPWS.

1.2. Pressuposto

O leitor deste documento deve estar familiarizado com os conceitos de IP/MPLS e Ethernet juntamente com as tecnologias de roteamento de segmento e engenharia de tráfego.

1.3. Âmbito técnico

O escopo técnico principal deste documento está limitado a:

- OSPF com TI-LFA FRR
- Políticas SR-TE controladas pelo headend (distribuídas)
- Caminho primário explícito e caminhos de failover baseados em IGP dinâmico
- EVPN VPWS single-homed

Os modelos de configuração fornecidos neste documento são chamados de Cisco IOS®-XR 7.5.x.

1.4. Resumo do documento

Tabela 1. Seções do documento

Tipo de tópico	Nome do tópico	Número da seção
Introduction	Informações de Apoio	1
Requisitos	Requisitos do usuário	2
	Roteamento de segmento	3
	Visão geral do SR-TE	4
Resumo da tecnologia	TI-LFA FRR	5
	Sobreposição de EVPN	6
	Balanceamento de carga e BoB	7
Modelos de configuração e exemplos de comandos	A solução de design completa	8
	Exemplo de configuração e comandos show	9

Requisitos

2. Requisitos do usuário

2.1. Resumo dos requisitos

O provedor de serviços XYZ Networks tem um requisito para criar uma rede de campo verde através de dispositivos Cisco NCS 5500.

A finalidade é transportar um fluxo de dados multicast (voz, vídeo) como um serviço através de uma rede de transporte da camada 2 com determinados requisitos, um deles é projetar os caminhos de tráfego através da rede.

Eles preferiram SR para rótulos de transporte, SR-TE para engenharia de tráfego e EVPN como uma sobreposição para fornecer rótulos de serviço.

2.2. Componentes utilizados

O usuário XYZ convergiu nos roteadores e nas placas de linha do NCS 5500:

Tabela 2. Requisitos de hardware do projeto

Nós PE	PIDs
Chassi	NCS-5504
MPA/LCs conectando nós P	NC55-36X100G-A-SE
MPA/LCs conectando nós CE	NC55-36X100G-A-SE
Nós P	PIDs
Chassi	NCS-5508
MPA/LCs conectando outros nós P	NC55-36X100G-A-SE
MPA/LCs conectando nós PE	NC55-36X100G-A-SE

Esta seção apresenta uma visão geral das tecnologias a serem usadas com descrições breves.

Resumo da tecnologia

3. Roteamento de Segmento

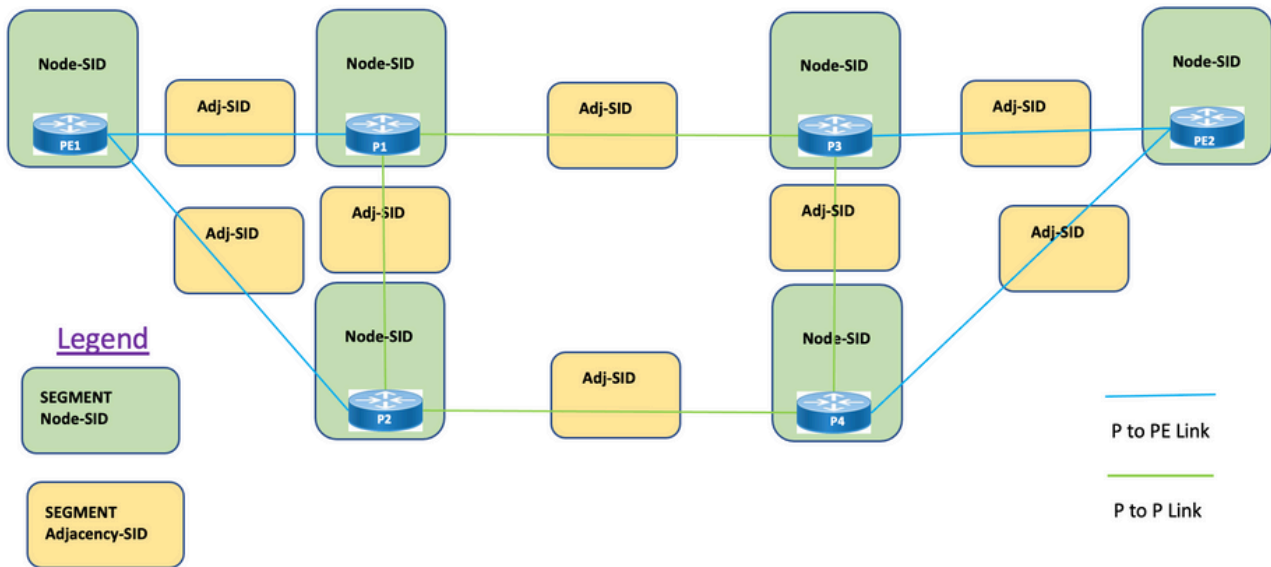
3.1. O que é roteamento de segmento?

O roteamento de segmento é a mais recente tecnologia avançada de MPLS que está no processo para substituir os protocolos LDP e RSVP-TE tradicionais pela introdução da distribuição de rótulo e engenharia de tráfego sob um único guarda-chuva e para fazer isso acontecer apenas através de protocolos IGP/BGP link-state.

O roteamento de segmentos é um método para encaminhar pacotes na rede com base no paradigma de roteamento de origem. A origem escolhe um caminho e o codifica no cabeçalho do pacote como uma lista ordenada de segmentos. Os segmentos são um identificador para qualquer tipo de instrução. Por exemplo, os segmentos de topologia identificam o próximo salto para um destino. Cada segmento é identificado pelo ID do segmento (SID) que consiste em um inteiro de 20 bits simples e sem sinal.

3.2. Identificadores de segmentos

Figura 1. SIDs de Nó SR e SIDs de Adjacência



Segmentos: O Interior Gateway Protocol (IGP) distribui dois tipos de segmentos: Segmentos de prefixo e segmentos de adjacência. Cada roteador (nó) e cada link (adjacência) tem um identificador de segmento (SID) associado.

SID de prefixo: um segmento de prefixo é um segmento global, portanto, um SID de prefixo é globalmente exclusivo dentro do domínio de roteamento de segmento, conforme ilustrado na Figura 1. Um SID de prefixo é associado a um prefixo IP. O SID do prefixo é configurado manualmente a partir do intervalo de rótulos do bloco global de roteamento de segmentos (SRGB) e é distribuído pelo IS-IS ou OSPF. O segmento de prefixo orienta o tráfego ao longo do caminho mais curto até seu destino.

- Usa Bloco Global SR (SRGB)
- SRGB anunciado com TLV de recursos do roteador - na configuração, o Prefix-SID pode ser configurado como um valor absoluto ou um índice
- No anúncio do protocolo, Prefix-SID é sempre codificado como um índice globalmente exclusivo. O índice representa um deslocamento da base SRGB, numeração baseada em zero, ou seja, 0 é o 1º índice. Por exemplo, o índice 1 à SID é $16.000 + 1 = 16.001$

SID do nó: Um SID de nó é um tipo especial de SID de prefixo que identifica um nó específico. Ele é configurado na interface de loopback com o endereço de loopback do nó como o prefixo. Um segmento de prefixo é um segmento global, portanto um SID de prefixo é globalmente exclusivo dentro do domínio de roteamento de segmento.

Em outras palavras, o segmento Nó é um segmento de Prefixo associado a um prefixo de host que identifica um nó.

- Equivalente a um prefixo router-id, que é um prefixo que identifica um nó
- Node-SID é Prefix-SID com N-flag definido no anúncio
- Por padrão, cada SID de prefixo configurado é um SID de nó
- 'regular' (isto é, não-Node-SID) Prefix-SID é configurável para IS-IS

SID de adjacência: Um segmento de adjacência é identificado por um rótulo chamado SID de

adjacência, que representa uma adjacência específica, como uma interface de saída, para um roteador vizinho. O SID de adjacência é distribuído por IS-IS ou OSPF. O segmento de adjacência direciona o tráfego para uma adjacência específica. Um segmento de adjacência é um segmento local, portanto, o SID de adjacência é localmente exclusivo em relação a um roteador específico.

- Localmente significativo
- Alocado automaticamente para cada adjacência
- Sempre codificado como um valor absoluto (ou seja, não indexado)

SID ou BSID de vinculação: É um SID localmente significativo associado à Política SR. Ajuda a direcionar pacotes para sua política SR associada. O segmento de ligação é um segmento local que identifica uma política SR-TE. Cada política SR-TE é associada a um ID de segmento de ligação (BSID).

O BSID é um rótulo local que é alocado automaticamente para cada política SR-TE quando a política SR-TE é instanciada. O BSID pode ser usado para direcionar o tráfego para a política SR-TE e entre fronteiras de domínio, o que cria políticas SR-TE interdomínio de ponta a ponta contínuas.

4. Visão geral do SR-TE

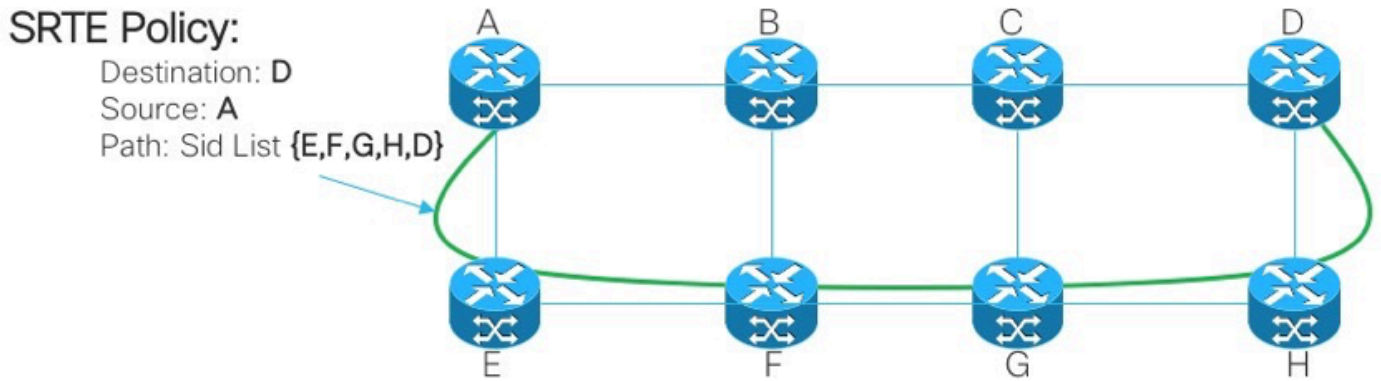
4.1. O que é SR-TE?

O Segment Routing Traffic Engineering (SR-TE) transforma o mecanismo de roteamento de origem simples e stateless do SR em um nível avançado para programar e orientar o tráfego de dados através de caminhos predefinidos que evitam congestionamentos e fornecem caminhos alternativos, assim como um mapa de tráfego de via expressa.

Isso é obtido quando você configura administrativamente as políticas definidas por meio de uma combinação de várias restrições que programam os caminhos principal e de backup dos nós de origem para destino. O controlador pode ser centralizado (SDN) ou distribuído (headend), o que depende do requisito de rede.

Vamos considerar a topologia apresentada na Figura 2. Suponha que o custo dos links sejam valores padrão e que o caminho mais curto para alcançar D de A seja A-B-C-D, mas o caminho de latência baixa seja A-E-F-G-H-D. O operador pode definir o caminho projetado pelo tráfego conforme o requisito (por exemplo, Latência) e expressá-lo na forma de uma lista de ID de segmento - (A, E, F, G, H, D). Diferentemente do RSVP-TE, o estado dessa política é mantido somente no roteador A e não nos roteadores inteiros pelos quais os pacotes passam (isto é, E, F, G e H).

Figura 2. Exemplo de caminho definido administrativamente pelo SR-TE



4.2. Política SR-TE

O roteamento de segmento para engenharia de tráfego (SR-TE) usa uma 'política' para orientar o tráfego através da rede. Um caminho de política SR-TE é expresso como uma lista de segmentos que especifica o caminho, chamada de lista de ID de segmento (SID). Cada segmento é um caminho de ponta a ponta da origem até o destino e instrui os roteadores na rede a seguir o caminho especificado em vez de seguir o caminho mais curto calculado pelo IGP. Se um pacote for direcionado para uma política SR-TE, a lista SID será enviada no pacote pelo headend. O restante da rede executa as instruções incorporadas na lista de SID.

Uma política SR-TE é identificada como uma lista ordenada (head-end, cor, end-point):

- Head-end - onde a política SR-TE é instanciada
- Cor - Um valor numérico que distingue entre duas ou mais políticas para os mesmos pares de nós (Head-end - Endpoint)
- Ponto final - o destino da política SR-TE
- Cada política SR-TE tem um valor de cor. Cada política entre os mesmos pares de nós requer um valor de cor exclusivo.

Uma política SR-TE é configurada com um ou mais caminhos candidatos que incluem caminhos principais e de backup.

Por exemplo, o caminho principal da política pode ser explicitamente definido com os SIDs de adjacência e, em caso de cenários de falha, o caminho de backup pode ser dinâmico, tomado pela métrica IGP.

5. RRF TI-LFA

5.1. Panorâmica

A Topologia Independent Loop-Free Alternative (TI-LFA) é um recurso que protege links, nós e SRLGs. É simples de configurar; são necessárias apenas duas linhas de configuração para implementar uma configuração TI-LFA simples no roteador. Ele não exige nenhuma alteração nos protocolos que existem usados no roteador. A Figura 3 mostra o caminho de tráfego principal e o caminho de backup pré-calculado pelo TI-LFA para cenários de falha de link local e falha de nó.

Figura 3. Cenário de failover do link LFA do TI

TI-LFA Link Failover

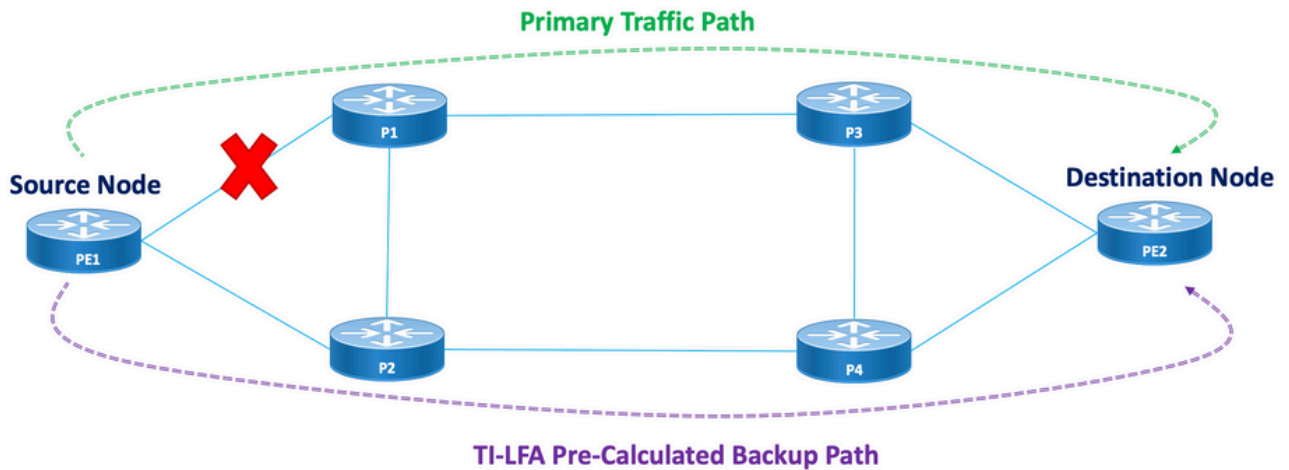
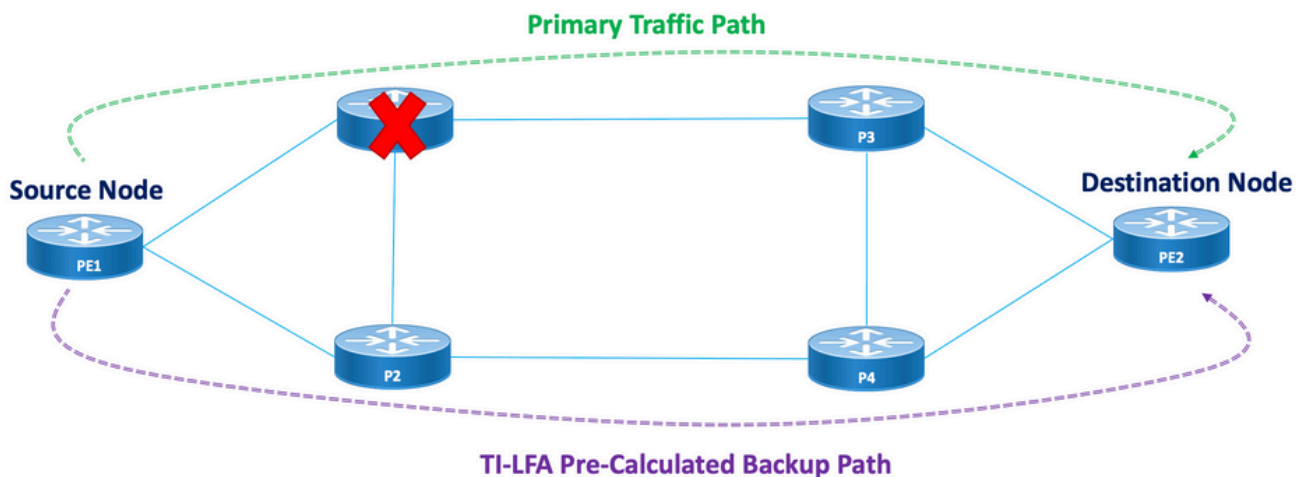


Figura 4. Cenário de failover do nó LFA do TI

TI-LFA Node Failover



Cada nó e caminho protegido tem um caminho de backup pré-calculado que pode ser ativado rapidamente. O tempo de convergência de um caminho protegido é de 50 milissegundos ou menos. Isso significa que até mesmo os aplicativos com maior sensibilidade à perda de latência ou de pacotes podem funcionar sem interrupções caso um nó ou um link falhe. O TI-LFA calcula o caminho de backup e remove temporariamente o link ou nó protegido do banco de dados. Depois disso, ele calcula o caminho de backup com o caminho mais curto primeiro. Isso garante que o caminho de backup tenha o menor custo de métrica possível enquanto evita o caminho protegido. Um túnel de engenharia de tráfego que segue o caminho de backup é usado para tráfego se ocorrer uma falha. Uma lista de rótulos de reparo determina o caminho para os pacotes que precisam de uma nova rota para seu destino. Uma lista de rótulos de reparo é uma pilha de rótulos normal, mas só é usada quando ocorre uma falha na rota protegida.

5.2. Impacto do método de detecção de anomalias na RRF

O Fast Reroute para caminhos com engenharia de tráfego SR-TE é configurado como um meio de comutar o tráfego no caso de situações de failover do caminho principal para caminhos de backup dentro de 50 ms, o mais próximo possível. O recurso de redirecionamento rápido é

configurado no protocolo IGP (OSPF/ISIS). O tempo de convergência depende do método pelo qual ocorre a detecção de falha do link. No caso de um corte de fibra, a detecção é imediata e a possibilidade de obter uma convergência abaixo de 50 ms é alta. No entanto, caso a detecção de falha do link tenha que ser feita pelo BFD com um intervalo de 15 ms (multiplicador x3). O tempo de convergência é maior que 50 ms.

5.3. Prevenção de microloop com SR

Os microloops são pequenos loops de pacote que ocorrem na rede que segue uma alteração de topologia (eventos de link inativo, link ativo ou alteração de métrica). Os microloops são causados pela convergência não simultânea de nós diferentes na rede. Se os nós convergirem e enviarem o tráfego para um nó vizinho que ainda não convergiu, o tráfego pode ser colocado em loop entre esses dois nós, o que resulta em perda de pacotes, instabilidade e pacotes fora de ordem.

O recurso Segment Routing Microloop Avoidance detecta se os microloops são possivelmente seguidos por uma alteração de topologia. Se um nó computa que um microloop pode ocorrer na nova topologia, o nó cria um caminho de política SR-TE sem loops para o destino com o uso de uma lista de segmentos. Depois que o temporizador de retardo de atualização RIB expira, a política SR-TE é substituída por caminhos de encaminhamento regulares. Há um temporizador padrão para o atraso de atualização RIB que é atendido pelo TI-LFA.

6. Sobreposição de EVPN

O EVPN é uma tecnologia projetada inicialmente para serviços multiponto Ethernet, com recursos avançados de multihoming, com o uso do BGP para distribuir informações de alcançabilidade de endereço MAC através da rede MPLS, enquanto traz as mesmas características operacionais e de escala de VPNs IP para L2VPNs. Hoje, além dos aplicativos DCI e E-LAN, a família de soluções EVPN fornece uma base comum para todos os tipos de serviços Ethernet, que inclui E-LINE e E-TREE, bem como cenários de roteamento e bridging de data center. O EVPN também oferece opções para combinar serviços L2 e L3 na mesma instância.

O EVPN é uma solução de última geração que fornece serviços multiponto Ethernet sobre redes MPLS. O EVPN opera em contraste com o Virtual Private LAN Service (VPLS) que existe, o que permite o aprendizado de MAC baseado em plano de controle BGP no núcleo. No EVPN, os PEs que participam das instâncias do EVPN aprendem as rotas MAC do usuário no plano de controle com o uso do protocolo MP-BGP.

O EVPN traz vários benefícios como mencionado:

- Redundância por fluxo e balanceamento de carga
- Provisionamento e operação simplificados
- Encaminhamento ideal
- Convergência rápida
- Escalabilidade de endereço MAC
- Soluções de vários fornecedores sob padronização IETF

Os endereços MAC aprendidos em um dispositivo precisam ser aprendidos ou distribuídos em outros dispositivos em uma VLAN. O recurso Aprendizado MAC do Software EVPN permite a distribuição dos endereços MAC aprendidos em um dispositivo para os outros dispositivos conectados a uma rede. Os endereços MAC são aprendidos dos dispositivos remotos com o uso do BGP.

Nestas seções, você aprenderá sobre alguns dos benefícios e tipos de rota do EVPN em geral e, em seguida, entenderá os componentes específicos da solução que são aplicados ao projeto dos serviços de rede XYZ.

6.1. Benefícios do EVPN

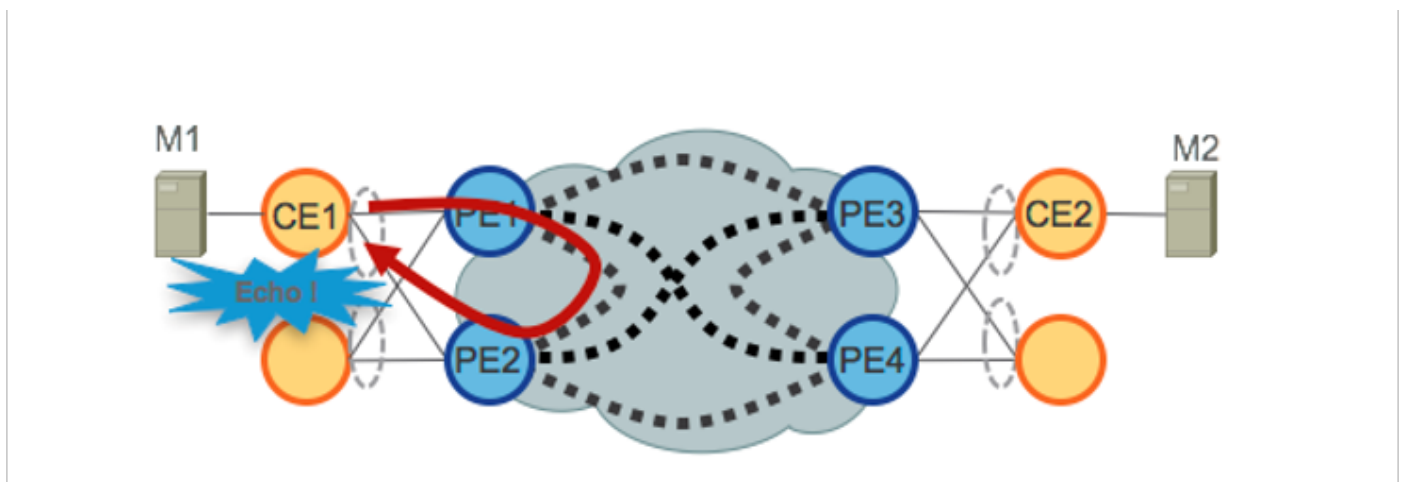
O L2VPN e o L3VPN não apenas fornecem serviços sob um único guarda-chuva de soluções com a ajuda de vários tipos de rotas, as EVPNs resolvem duas limitações de longa data para serviços Ethernet em redes de provedores de serviços:

- Acesso Ethernet multilocal e totalmente ativo
- Rede do provedor de serviços—integração com o escritório central ou com o data center

6.1.1. Acesso Ethernet multilocal e totalmente ativo

A figura demonstra a maior limitação das soluções L2 Multipoint tradicionais, como VPLS.

Figura 5. Acesso All-Active EVPN



Quando o VPLS é executado no núcleo, a prevenção de loop exige que PE1/PE2 e PE3/PE4 forneçam apenas redundância de Atividade Única para seus respectivos CEs. Tradicionalmente, técnicas como mLACP ou protocolos L2 legados, como MST, REP, G.8032, etc., eram usadas para fornecer redundância de acesso Single-Ativo.

A mesma situação ocorre com o Hierarchical-VPLS (H-VPLS), em que o nó de acesso é responsável por fornecer acesso de H-VPLS de Atividade Única por pseudofio de spoke ativo e de backup (PW).

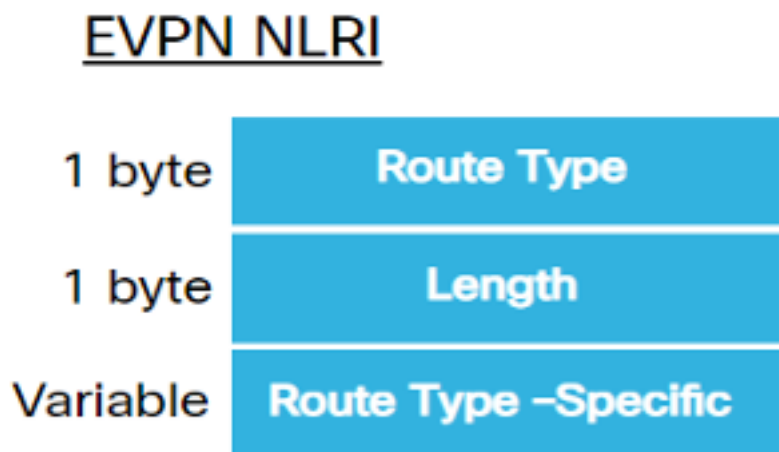
Os modelos de redundância de acesso totalmente ativo não são implantáveis, pois a tecnologia VPLS não tem a capacidade de impedir loops L2 que derivam dos mecanismos de encaminhamento empregados no núcleo para determinadas categorias de tráfego. O tráfego de broadcast, unicast desconhecido e multicast (BUM) originado do CE é inundado por todo o núcleo VPLS e é recebido por todos os PEs, que, por sua vez, o inundam para todos os CEs conectados. Em nosso exemplo, PE1 pode inundar o tráfego de BUM de CE1 para o núcleo e PE2 pode enviá-lo de volta para CE1 quando recebido.

O EVPN usa técnicas de plano de controle baseadas em BGP para resolver esse problema e permite modelos de redundância de acesso ativo-ativo para acesso Ethernet ou H-EVPN.

6.2. Tipos de rota EVPN

O EVPN define um novo BGP NLRI que é usado para transportar todas as rotas EVPN. O NLRI de EVPN é transportado no BGP com o uso de extensões multiprotocolo com um AFI de 25 (L2VPN) e um SAFI de 70. O anúncio de capacidades do BGP é usado para garantir que dois alto-falantes suportem o NLRI de EVPN.

Figura 6. NLRI da EVPN



Os tipos de rota EVPN relevantes necessários para esta implementação são descritos aqui:

6.2.1. Tipo de rota 1 - Rota de descoberta automática (AD) de Ethernet

As rotas de descoberta automática Ethernet (AD) são anunciadas por EVI e por ESI. Essas rotas são enviadas por ES. Eles carregam a lista de EVIs que pertencem ao ES. O campo ESI é definido como zero quando um CE é single-homed. Esse tipo de rota é usado para uma retirada em massa de endereços MAC, aliasing para balanceamento de carga e Filtragem Split Horizon.

6.2.2. Tipo de rota 4 - rota de segmento Ethernet

As rotas de segmento Ethernet permitem a conexão de um dispositivo CE a dois ou PE dispositivos. A rota ES permite a descoberta de dispositivos PE conectados ao mesmo segmento Ethernet, ou seja, descoberta de grupo de redundância. Ela também é usada para a eleição do encaminhador designado (DF).

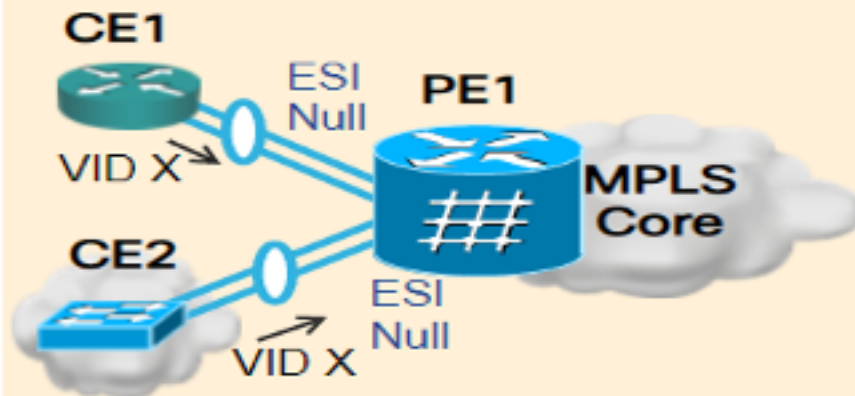
6.3. Conectividade do host EVPN

Estes modos EVPN são suportados:

- Single homing - Isso permite que você conecte um dispositivo de borda do usuário (CE) a um dispositivo de borda do provedor (PE). Neste ESI, o valor é nulo para cada link PE-CE.
- Multihoming - Isso permite que você conecte um dispositivo de borda do usuário (CE) a dois ou mais dispositivos de borda do provedor (PE) para fornecer conectividade redundante. Nenhum link Interchassis é necessário. O dispositivo PE redundante garante que não haja interrupção de tráfego quando houver uma falha de rede. Os tipos de multihoming são:

Figura 7. EVPN Single Homing

Single Home Device (SHD) Single Home Network (SHN)

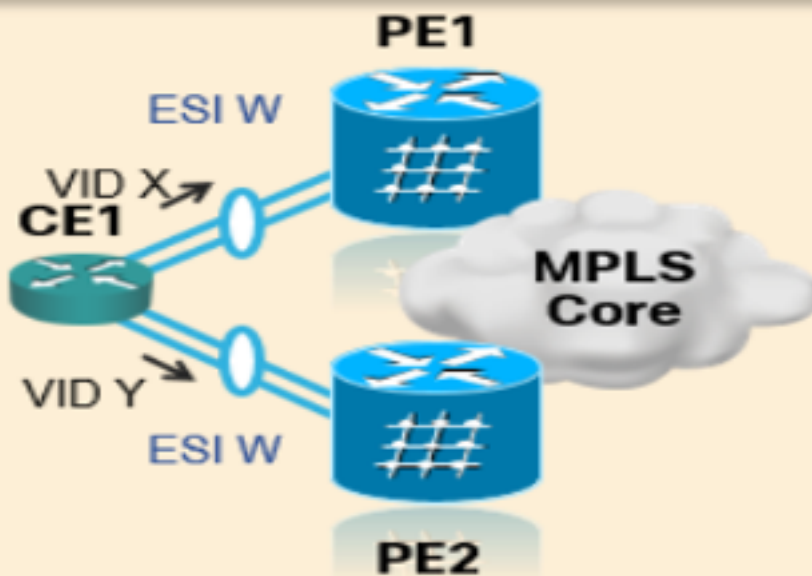


Multihoming - Estes são os tipos de multihoming:

1. Único-Ativo - Em um modo único-ativo, apenas um único PE entre um grupo de PEs conectados ao Segmento Ethernet específico tem permissão para encaminhar o tráfego de e para esse Segmento Ethernet.

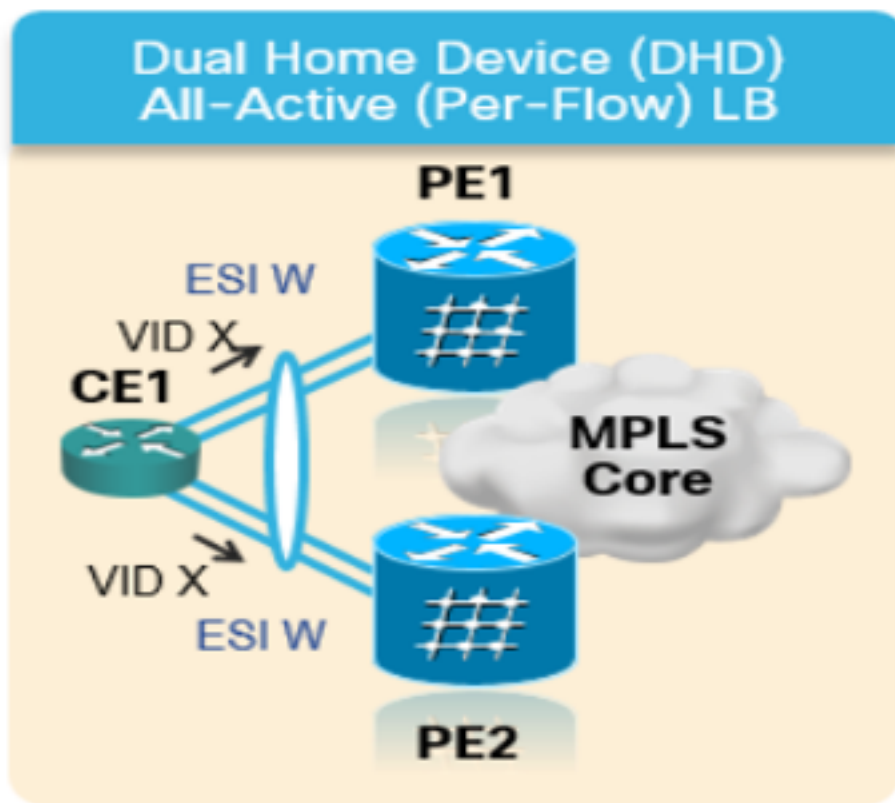
Figura 8. EVPN Single-Ativo

Dual Home Device (DHD) Single-Active (Per-Service) LB



2. Ativo-Ativo - No modo ativo-ativo, todos os PEs conectados a um Segmento Ethernet específico têm permissão para encaminhar tráfego de e para esse Segmento Ethernet.

Figura 9. EVPN Dual Active



7. Balanceamento de carga e BoB

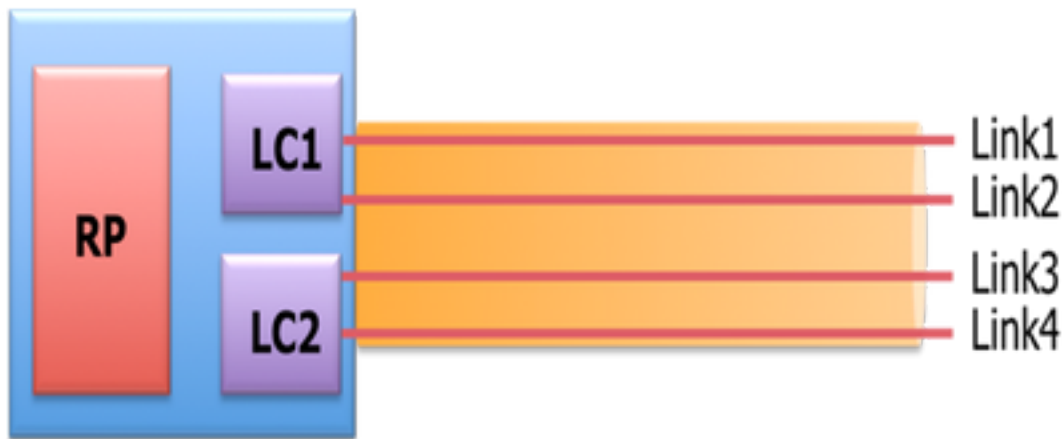
7.1. BFD sobre o pacote (BoB)

A Detecção de Encaminhamento Bidirecional (BFD - Bidirectional Forwarding Detection) fornece detecção de falhas de baixa sobrecarga e curta duração no caminho entre mecanismos de encaminhamento adjacentes. O BFD permite que um único mecanismo seja usado para detecção de falhas em qualquer meio físico e em qualquer camada de protocolo, com uma ampla gama de tempos de detecção e sobrecarga. A detecção rápida de falhas fornece uma reação imediata à falha no caso de um link ou vizinho com falha.

Isso acionaria o IGP para começar a encaminhar o tráfego para o caminho de backup já calculado com o uso de FRR (no caso do IGP) e PIC (no caso do BGP).

No recurso BFD Over Bundle (BoB), a sessão BFD IPv4 é executada em cada membro ativo do pacote.

Figura 10. Diagrama Lógico da BoB



O Bundlemgr considera os estados BFD, além dos estados L1/L2 existentes, para determinar a usabilidade do link do membro. O Estado-Membro do pacote é uma função de:

Estado L1 (link físico)

Estado L2 (LACP)

Estado L3 (BFD)

O agente BFD ainda é executado na placa de linha. Os estados BFD dos enlaces de membros do pacote são consolidados no RP. Os links membros devem ser conectados back-to-back, sem qualquer switch L2 no meio. O recurso BoB é configurado em todas as interfaces Bundle Ethernet na rede XYZ.

7.2. Balanceamento de carga

O balanceamento de carga ECMP por fluxo na rede em questão abrange as interfaces Ethernet entre pacotes e as ethernets entre pacotes (entre membros físicos de uma interface de pacote). Isso é aplicável em toda a rede de PE para PE (Balanceamento de carga do núcleo), bem como de PE para CE (Balanceamento de carga CA), conforme discutido.

7.2.1. Balanceamento de carga do núcleo com rótulo FAT

De acordo com o escopo da rede XYZ, você deve considerar apenas o balanceamento de carga ECMP (multicaminho de custo igual) por fluxo como mencionado:

Os roteadores normalmente fazem o balanceamento de carga do tráfego com base no rótulo mais baixo na pilha de rótulos, que é o mesmo rótulo para todos os fluxos em um determinado pseudofio. Isso pode levar ao balanceamento de carga assimétrico. O fluxo, nesse contexto, se refere a uma sequência de pacotes que têm o mesmo par origem e destino. Os pacotes são transportados de uma extremidade de provedor de origem (PE) para uma extremidade de provedor de destino PE.

O Flow-Aware Transport Pseudowire (FAT PW) oferece a capacidade de identificar fluxos individuais dentro de um pseudofio e fornece aos roteadores a capacidade de usar esses fluxos para balancear a carga do tráfego. Os PWs FAT são usados para balancear a carga do tráfego no núcleo quando são usados ECMP (Equal-Cost Multipaths, vários caminhos de custo igual). Um rótulo de fluxo é criado com base em fluxos de pacotes indivisíveis que entram em um pseudofio e é inserido como o rótulo mais baixo no pacote. Os roteadores podem usar o rótulo de fluxo para

balanceamento de carga, que fornece uma melhor distribuição de tráfego através de caminhos ECMP ou caminhos de link agrupados no núcleo.

Um rótulo extra é adicionado à pilha, chamado de rótulo de fluxo, que é gerado para cada fluxo de entrada exclusivo no PE. Um rótulo de fluxo é um identificador exclusivo que distingue um fluxo no PW e é derivado dos endereços MAC origem e destino e dos endereços IP origem e destino. O rótulo de fluxo contém o final do conjunto de bits da pilha de rótulos (EOS). A etiqueta de fluxo é inserida depois da etiqueta VC e antes da palavra de controle (se houver). O PE de entrada calcula e encaminha o rótulo de fluxo. A configuração FAT PW ativa o rótulo de fluxo. O PE de saída descarta o rótulo de fluxo para que nenhuma decisão seja tomada.

7.2.2. Balanceamento de carga do circuito de ligação

No entanto, para o balanceamento de carga dos membros do pacote CA, você precisa de uma abordagem diferente devido à ausência de SR-MPLS nesta seção da rede.

O balanceamento de carga por fluxo aqui pode ser obtido quando botões específicos de configuração l2vpn em todos os roteadores PE são ajustados explicitamente. Pode ser por MAC SRC/DST ou IP SRC/DST conforme o requisito.

Modelos de configuração e exemplos de comandos

8. A solução de projeto completa

Esta seção discute os detalhes completos do projeto ajustados por todos os diferentes componentes individuais que foram explicados em seções anteriores. Esta seção descreve a topologia e o modelo de configuração relevante com referência ao Cisco IOS-XR 7.5.x.

8.1. Requisitos de baixo nível

Para o cenário de tráfego normal, o fluxo de tráfego é projetado para se propagar sempre entre as terminações de serviço de PE1 e PE3 e somente entre PE2 e PE4. O objetivo principal nessa situação é manter o caminho de tráfego totalmente desarticulado, como mostrado na Figura 12.

O tráfego em questão aqui seria de fluxos multicast encapsulados através da sobreposição de EVPN. A partir dos nós CE1 e CE2, os fluxos de mídia multicast (voz/vídeo) chegam e podem ser encapsulados nos nós PE1 e PE2 e transportados pela sobreposição EVPN L2 para os nós CE3 e CE4 respectivamente depois de serem desencapsulados nos nós PE3 e PE4 respectivamente.

Portanto, o par de tráfego origem-destino é considerado como PE1-PE3 e PE2-PE4 de agora em diante em todas as circunstâncias, a menos que seja mencionado de outra forma. Para obter os detalhes do requisito, consulte a [subseção 2.2](#).

8.2. Resumo do projeto

Para atender aos requisitos, o OSPF é escolhido como IGP subjacente, conforme desejado pelas redes XYZ. Para direcionar o fluxo multicast encapsulado através do par de tráfego origem-destino através do caminho desejado, o SR-TE precisa ser implementado entre nós PE.

As políticas SR-TE foram projetadas com caminhos IGP explícitos e dinâmicos.

Os caminhos explícitos abrangem:

- Cenário de tráfego normal
- Cenário de failover até que opções de caminho alternativo estejam disponíveis

Os Caminhos IGP Dinâmicos abrangem:

- Caminho de Backup para Cenário de Failover em que opções de caminho alternativo **NÃO** estão disponíveis

Os recursos como BFD, TI-LFA e Prevenção de Microloop são configurados no OSPF, conforme mostrado nas subseções dos modelos de configuração.

Para cenários de tráfego normal, o modelo de configuração e outros detalhes são mencionados na subseção 8.5.1.

Para cenários de failover de tráfego, o modelo de configuração e outros detalhes são mencionados na subseção 8.5.2.

Além disso, os requisitos como a prevenção de microloop e menos de 50 ms de convergência em caso de cenários de falha também são tratados.

8.3. Elementos de projeto

Esta subseção captura todos os blocos de design que são posteriormente abordados minuciosamente nessas seções.

Visão geral do projeto (Camada 1):

- O tamanho da MTU na rede XYZ é fixado em '9216' com o objetivo de suportar até 5 a 6 pilhas de rótulos SR
- O 'BFD over Bundle' é implementado com um intervalo de 15 ms para detectar cortes de fibra inferiores a 50 ms

Visão geral do design do OSPF/SR-TE:

- **OSPF** como protocolo IGP com **TI-LFA** configurado para fornecer **FRR** abaixo de 50 ms de tempo de convergência
- **Camada de Transporte** baseada no **Roteamento de Segmento** como Plano de Encaminhamento e no **OSPF** como o **protocolo de roteamento**
- Na rede XYZ, o caminho explícito da **engenharia de tráfego de roteamento de segmento** orienta o tráfego em todas as direções do caminho principal necessárias. No caso de cenários de failover de link/nó, o tráfego é roteado por um caminho igp dinâmico
- A Prevenção de Microloop e a Métrica Máxima do OSPF também fazem parte desse projeto

Visão geral do design de BGP/RR:

- Há **dois RRs** configurados em um cluster para fornecer **redundância**
- A rede XYZ, o processo BGP em cada PE forma o peering 'IPv4' e 'L2VPN EVPN' com ambos os RRs separadamente

Visão geral do design do serviço:

- **As camadas de serviço** são criadas sobre o **plano de controle baseado em BGP** e o **EVPN**

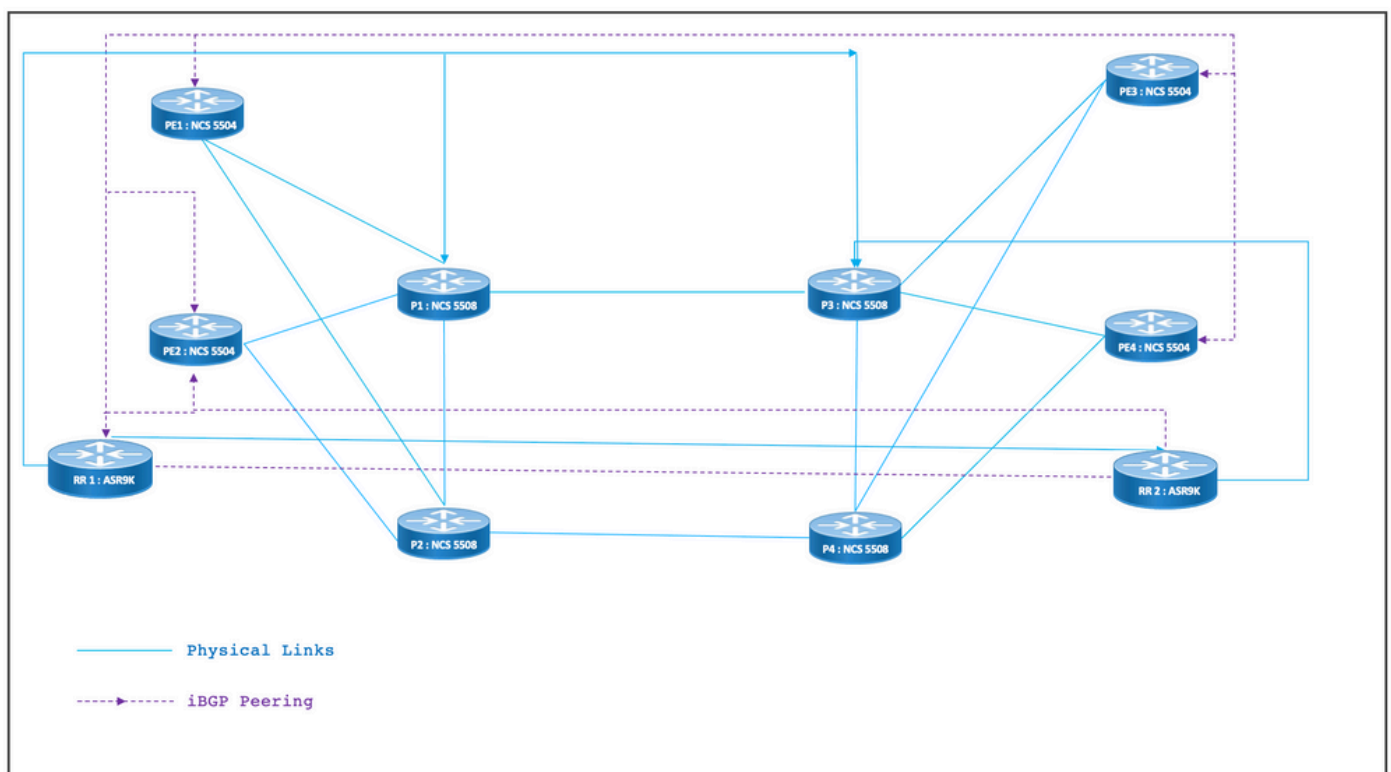
ponto a ponto da camada 2 (EVPN-VPWS)

- O tráfego de vídeo multicast (UDP) é enviado encapsulado através dos PWs EVPN-VPWS ponto a ponto
- O **balanceamento de carga ECMP** é obtido pela configuração do rótulo FAT na seção EVPN
- O serviço tem como objetivo suportar até 5 a 6 pilhas de rótulos SR que incluem rótulos de transporte SR, rótulos EVPN e rótulos FAT para balanceamento de carga

8.4. Exemplo de topologia física

A topologia física das redes XYZ é descrita nesta figura. Por uma questão de simplicidade, apenas 4 nós PE e 4 P são mostrados. Há dois nós RR que atuam em clusters para fornecer redundância.

Figura 11. Topologia Física



8.5. Detalhes do projeto da camada 1

No projeto genérico da camada 1, há um pacote Ethernet com pelo menos dois links membros por pacote configurado. Para a detecção rápida de falhas de link, escolha BFD em vez do recurso Pacote. O intervalo de tempo pode variar idealmente entre 5 e 15 ms. Depende da capacidade de descarregamento do hardware.

Para obter detalhes sobre o BFD, consulte

<https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/73x/b-routing-cg-ncs5500-73x/implementing-bfd.html>. Observe que esse recurso deve ser configurado somente na interface Bundle Ethernet e não é necessário configurá-lo no IGP. O tamanho da MTU é fixo em 9216 com o objetivo de suportar até 5 a 6 pilhas de rótulos SR.

8.5.1. Modelos de configuração

Os modelos de configuração de BFD sobre pacote para todos os nós são mostrados aqui:

```
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. Visão Geral do Projeto OSPF/SR-TE

Todos os roteadores OSPFv2 na rede estão na área 0 e, portanto, a rede trata de um único domínio IGP.

No OSPF do roteador, o roteamento de segmentos é ativado e as interfaces relevantes do pacote Ethernet são configuradas. Da mesma forma, em Bundle Interfaces, os parâmetros de tipo de rede e redirecionamento rápido são ativados. O mais importante é que uma Interface de Loopback está ativada no modo passivo com o Prefix-SID configurado.

O OSPF é um protocolo link-state, portanto, deve ser uma prioridade para identificar imediatamente os downlinks e criar um caminho de backup é necessário. Para cuidar disso, o BFD sobre o pacote na interface do pacote e o TI-LFA FRR no OSPF são configurados, o que mantém o tempo de convergência em 50 ms no caso de cenários de corte de fibra.

Estas subseções descrevem os cenários normal e de failover dos caminhos de tráfego em detalhes:

8.6.1. Cenário de tráfego normal SR-TE

Para manter um caminho primário muito estrito, as políticas SR-TE devem ser projetadas com caminhos explícitos de ponta a ponta entre os pares de tráfego de origem-destino mencionados anteriormente. Além disso, são necessários vários caminhos candidatos de preferência em uma política SR-TE para fornecer provisão para vários cenários de failover.

Esta figura representa os detalhes da rede do usuário em alinhamento com os blocos de design mencionados na [subseção 8.3](#).

- Links entre nós PE para P e P para P
- Endereços de Loopback de todos os nós
- Endereços de interface de todos os nós

- Direção do caminho de tráfego normal direcionado por SR-TE
- Sobreposição de EVPN entre nós PE

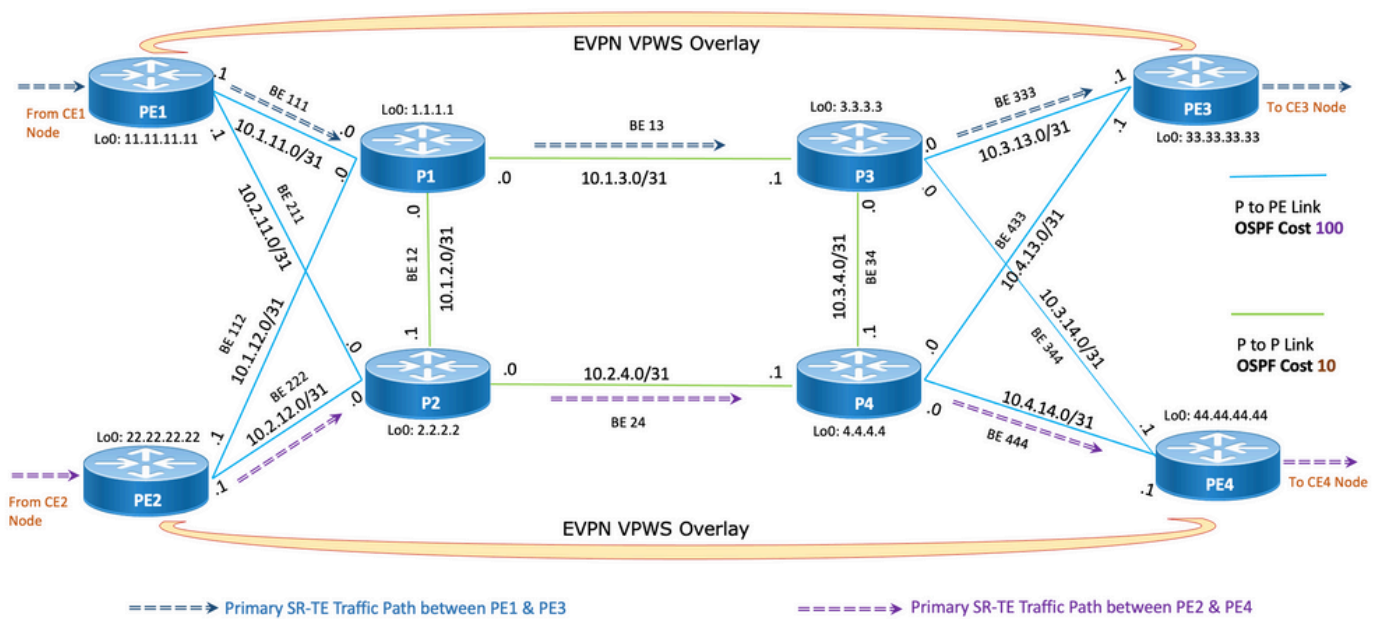
Os RRs não foram mostrados intencionalmente para reduzir a aglomeração na topologia.

Os links entre PE e P foram marcados com azul e os links entre P e P foram marcados com cor verde. O custo OSPF de links PE-para-P é 100 e o custo de links P-para-P é 10.

O fluxo de tráfego SR-TE primário foi marcado com setas azuis entre o par PE1-PE3 e com setas violetas entre o par PE2-PE4.

Figura 12. Detalhes da Topologia

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



8.6.1.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes do OSPF/SR-TE para os nós PE1 e PE2 conforme fornecido:

PE1 Node: OSPF & SR-TE configs

router ospf CORE

```

nsr
distribute 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

```

Note: Para configurar o comando **Source-Address**" GLOBALLY OU em POLICY. Como comportamento padrão, o endereço de origem na política substitui o comando global.

O comando source address na configuração de roteamento de segmento conforme mostrado é necessário em cenários específicos onde, no mesmo PE, como origem da política SR-TE, precisamos escolher um endereço de loopback entre vários ou quando ISIS e OSPF são executados com loopbacks separados, e precisamos congelar em um deles. Caso contrário, em cenários normais, em que há apenas um IGP executado com um loopback exclusivo, a configuração do endereço de origem é opcional.

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

```

Note: Os comandos opcional **source address**, **default SRGB** e **SRLB** foram removidos.

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>
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

Note: Na solução mencionada anteriormente, os saltos explícitos das listas de segmentos

são baseados em endereços IP, já que, como mencionado aqui, a configuração da política SR-TE de caminho explícito baseada no "rótulo mpls" a validação de caminho não funciona para a falha de link remoto na 7.3.x

No caso de qualquer link remoto, além do link local de um nó PE, falhar, o caminho permanecerá válido. Ele é projetado e não pode ser modificado até o XR 7.5.x

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 para cenários de failover

Para entender os cenários de failover de tráfego, é necessário examinar atentamente o tráfego do caminho principal sob condições de tráfego normais, conforme mencionado no diagrama de topologia na subseção anterior.

O objetivo principal em caso de cenários de failover é manter a disjunção do caminho de tráfego na extensão máxima possível, dada a infraestrutura de topologia atual. A rede XYZ tem requisitos rigorosos para administrativamente orientar o tráfego através de nós específicos em caminhos de backup, de modo a manter a separação máxima entre os pares de nós origem-destino. Esse design é feito para evitar que os links usados fiquem sobrecarregados e para manter o mínimo de links não usados.

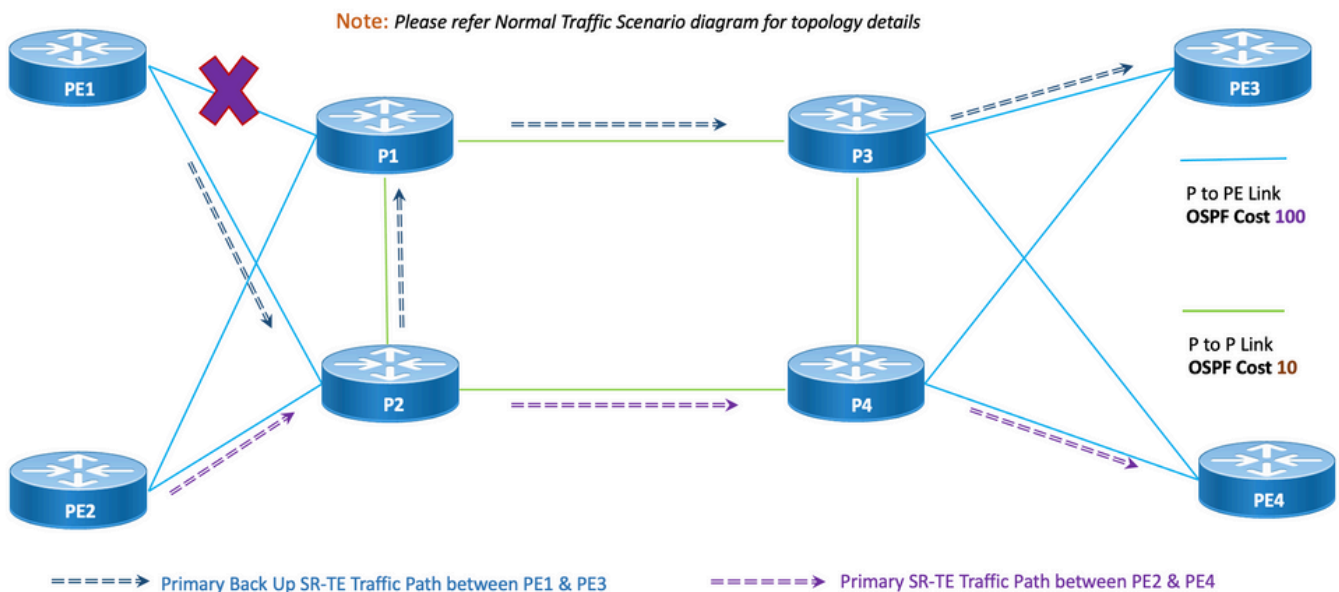
Estas subseções mostram os vários cenários de failover como link único, link duplo, nó único e nó duplo com o caminho de failover que o tráfego usa para manter a máxima disjunção.

8.6.3. Cenário de failover de link único

Este é o cenário de falha de link único onde o link local entre PE1 e P1 falha e o tráfego faz um desvio através dos nós P2 e P1 do núcleo. Ele é administrativamente orientado por meio da lista de segmentos <SIDLIST1>, que forma o caminho de backup principal entre os nós PE1 e PE3

Figura 13. Cenário de failover de link único

Single Link Failure



Desarticulação: Para falha de link único, o número de links comuns compartilhados é zero (0), como mostrado na topologia anterior.

8.6.3.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes do OSPF/SR-TE para os nós PE1 e PE2, conforme indicado aqui:

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
# 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
```

```
!
```

```
!
```

```
!
```

```
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>
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
# 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>

!

!

!

!

!

```

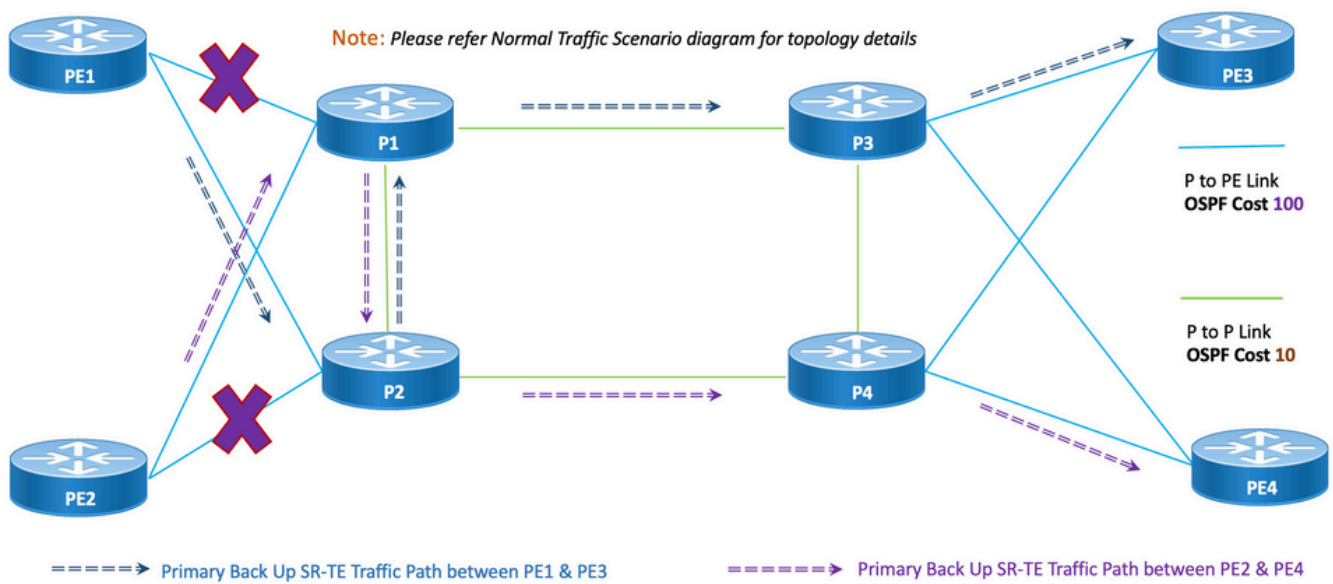
8.6.4. Cenário de failover de link duplo

Este é o cenário de falha de link duplo onde o link local entre PE1 e P1 e o link local entre PE2 e P2 falham. O tráfego de PE1 faz um desvio através dos nós P2 e P1 do núcleo e o tráfego de PE2 faz um desvio através dos nós P1 e P2 do núcleo.

Eles são administrativamente orientados através da respectiva lista de segmentos <SIDLIST2> de PE1 e PE2 que formam os caminhos de backup secundários entre os nós PE1 e PE3 e PE2 e PE4, respectivamente.

Figura 14. Cenário de failover de link duplo

Double Link Failure



Desarticulação: Para falha de link duplo, o número de links comuns compartilhados é um (1), como mostrado na topologia mencionada anteriormente.

8.6.4.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes do OSPF/SR-TE para os nós PE1 e PE2, conforme indicado aqui:

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
# 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>
!
!

!
!
!
!

```

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

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>

!

!

!

!
```

!

!

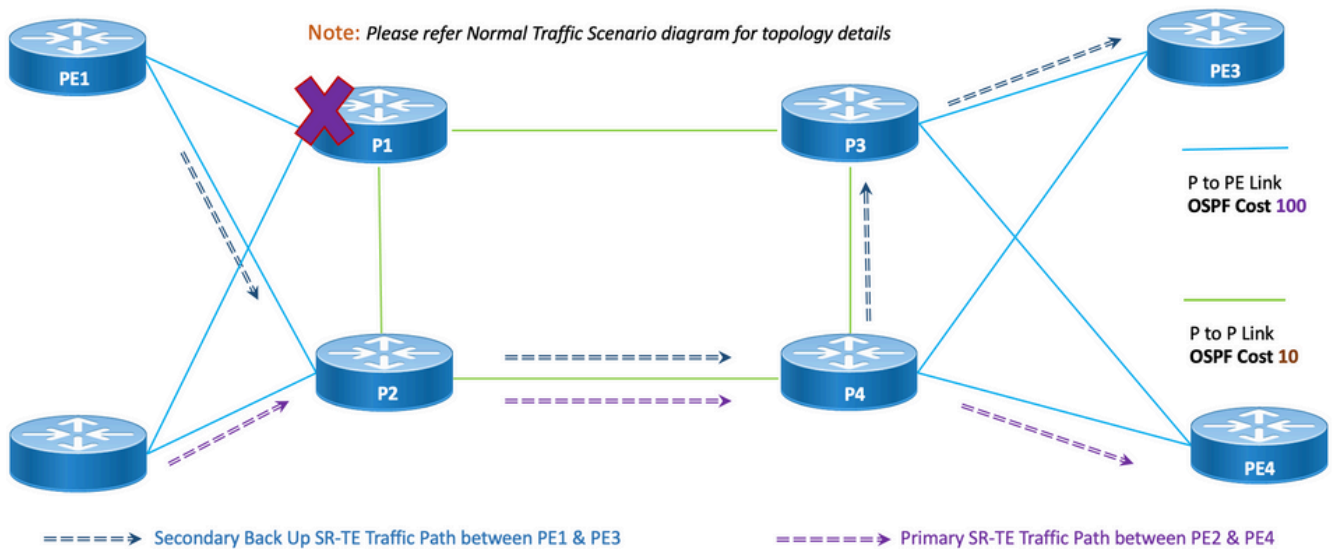
8.6.5. Cenário de failover de nó único

Este é o cenário de falha de nó único onde o nó P1 falha e o tráfego faz um desvio através dos nós P2 e P4 do núcleo. Ele é administrativamente orientado por meio da lista de segmentos <SIDLIST3>, que forma o caminho de backup secundário entre os nós PE1 e PE3.

O tráfego entre PE2 e PE4, no entanto, permanece o mesmo que o caminho principal como mostrado nesta topologia.

Figura 15. Cenário de failover de nó único

Single Node Failure



Desarticulação: Para falhas de nó único, o número de links comuns compartilhados é um (1), como mostrado na topologia mencionada anteriormente.

8.6.5.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes do OSPF/SR-TE para os nós PE1 e PE2 conforme fornecido:

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
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>
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
# 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>
!

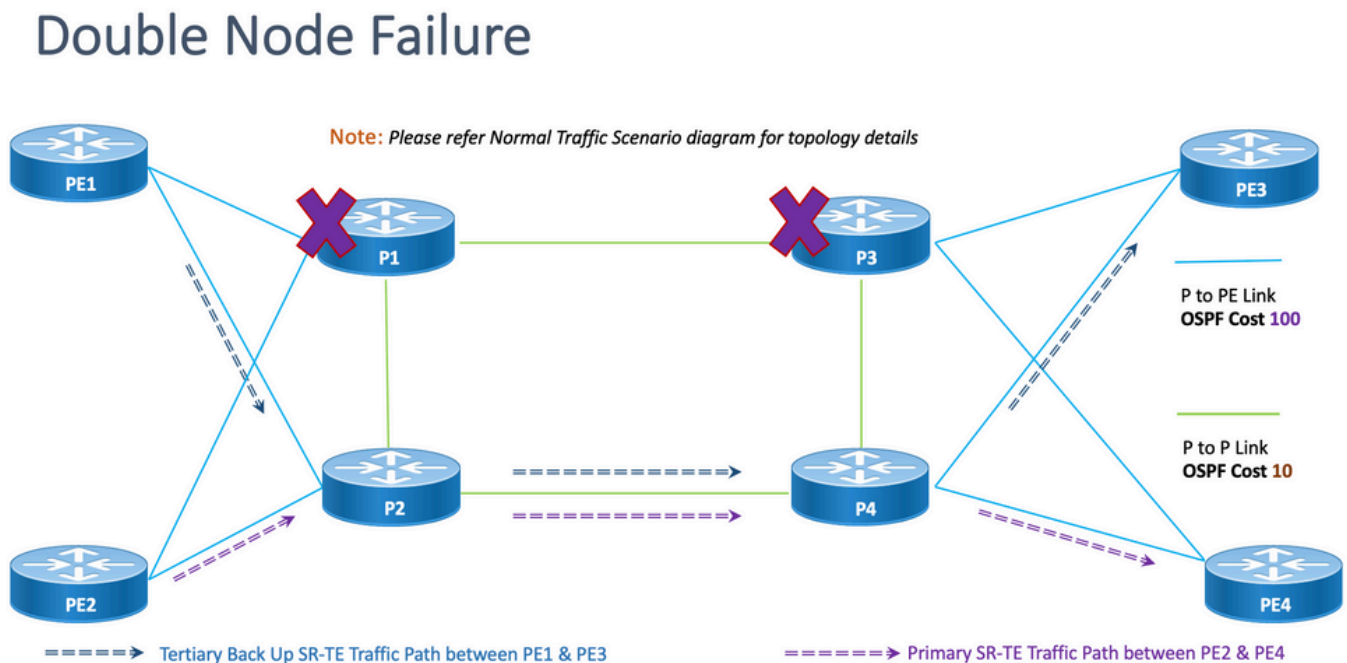
```

8.6.6. Cenário de failover de nó duplo

Este é o cenário de falha de nó duplo onde os nós P1 e P3 falham e o tráfego faz um desvio através dos nós P2 e P4 do núcleo. Ele é administrativamente orientado por meio da lista de segmentos <SIDLIST3>, que forma o caminho de backup secundário entre os nós PE1 e PE3. Como os caminhos explícitos são definidos apenas para os dois cenários mencionados anteriormente, aqui o caminho IGP dinâmico forma o caminho de backup terciário e assume a função de rotear o tráfego através dos nós P2 e P4.

O tráfego entre PE2 e PE4, no entanto, permanece o mesmo que o caminho principal como mostrado nesta topologia.

Figura 16. Cenário de Failover de Nó Duplo.



Desarticulação: Para falha de nó duplo, o número de links comuns compartilhados é um (1), como mostrado nesta topologia.

8.6.6.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes do OSPF/SR-TE para os nós PE1 e PE2 conforme fornecido:

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```
# 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)

  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

explicit segment-list <SIDLIST1>

!

!

!

!

!

!

!

```

Note: Os modelos de configuração do OSPF do roteador de PE1 e PE2 são semelhantes ao cenário normal.

```

# 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>

!
!

!
!
!
!

```

8.7. Visão geral do projeto BGP/RR

O BGP (Border Gateway Protocol) é o protocolo que toma as principais decisões de roteamento na Internet. Ele mantém uma tabela de redes IP ou "prefixos" que designam a alcançabilidade de rede entre sistemas autônomos (AS). É descrito como um protocolo de vetor de caminho. O BGP não usa métricas tradicionais do Interior Gateway Protocol (IGP), mas toma decisões de roteamento com base no caminho, nas políticas de rede e/ou nos conjuntos de regras. Por esse motivo, é mais apropriado denominá-lo como um protocolo de alcance do que como um protocolo de roteamento.

O MP-BGP pode ser usado para propagar prefixos de IPv4, IPv6, VPNv4, VPNv6, EVPN e Link-state pela rede. Isso é feito com uma configuração de refletor de rota que forma vizinhos iBGP com dispositivos de núcleo, agregação, acesso e dispositivos SR-PCE.

Através do RR, os prefixos aprendidos do BGP são propagados internamente através do iBGP. As rotas BGP nunca são redistribuídas em IGP. Os refletores de rota são totalmente isolados do plano de dados e dedicados para fins do plano de controle.

8.7.1. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes para BGP/RR como mostrado:

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. Visão geral do design do serviço

Esta subseção descreve o serviço de sobreposição de EVPN VPWS junto com a representação da pilha de rótulos suportada e os modelos de configuração.

O EVPN-VPWS é uma solução de plano de controle BGP para serviços ponto a ponto. Ele implementa as técnicas de sinalização e encapsulamento que estabelecem uma instância de EVPN entre um par de PEs. Ele tem a capacidade de encaminhar tráfego de uma rede para outra sem consulta MAC. O uso de EVPN para VPWS elimina a necessidade de sinalização de PWs de segmento único e de vários segmentos para serviços Ethernet ponto a ponto. A tecnologia EVPN-VPWS funciona no núcleo IP e MPLS; o núcleo IP suporta os núcleos BGP e MPLS para comutar pacotes entre os pontos finais.

8.8.1. Representação da pilha de rótulos

O serviço tem como objetivo suportar até 5 a 6 rótulos de pilha SR incluindo rótulos de transporte SR, rótulos EVPN e rótulos FAT para balanceamento de carga. Este é o número máximo de rótulos analisados em **Cenários Normais** onde o tráfego flui por um Caminho Primário Explícito:

```
ADJ SID1  
ADJ SID2  
ADJ SID3  
RÓTULO EVPN  
RÓTULO DO  
FLUXO (S=1)
```

Este é o número máximo de rótulos analisados nos **cenários de failover** em que o tráfego flui pelo caminho explícito de backup ou pelo caminho de backup dinâmico definido pelo IGP:

```
TI-LFA SID1  
TI-LFA SID2  
TI-LFA SID3  
RÓTULO EVPN  
RÓTULO DO  
FLUXO (S=1)
```

8.8.2. Modelos de configuração

Esta subseção contém os modelos de configuração relevantes para EVPN-VPWS, conforme mostrado:

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

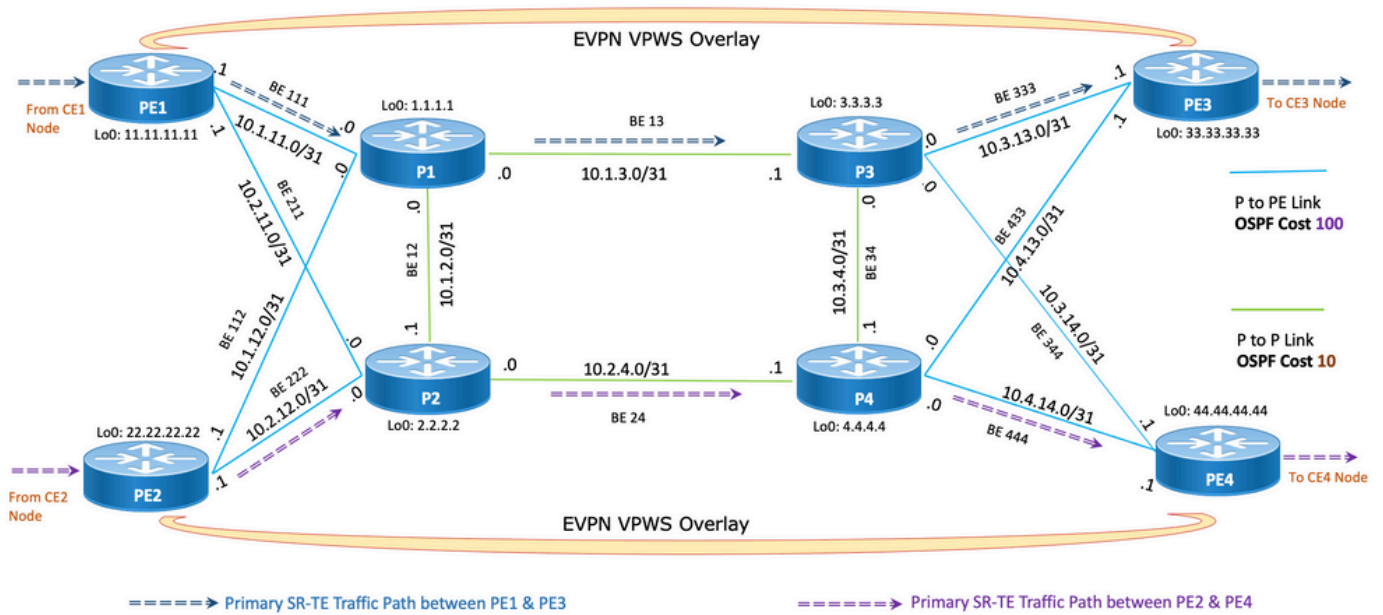
```
evpn
```

```
evi <EVI-ID>      Ethernet Virtual Identifier
```

```
bgp
```


Figura 17. Topologia com parâmetros de configuração.

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



PE1 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 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. Comandos show relevantes nos nós PE

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

O BGP opera no modo STANDALONE.

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

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- <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>
- [Suporte Técnico e Documentação - Cisco Systems](#)