Guide de conception détaillée et exemples de configuration de la politique de chemin explicite SR-TE avec EVPN VPWS, version IOS XR - 7.5.x

Contenu

Introduction

Ce document décrit le guide de conception détaillé avec des descriptions techniques basées sur les exigences des réseaux XYZ et fournit également un modèle de configuration et une configuration de bas niveau pour les exemples d'utilisation de la stratégie de chemin explicite SR-TE (Segment Routing Traffic Engineering) avec un service privé virtuel VPN Ethernet (EVPN) (Virtual Private Wired Service) (VPWS).

1. Informations générales

1.1. Hors portée

Ce document ne couvre pas les exigences des politiques SR-TE centralisées à la demande qui utilisent le contrôleur XTC, EVPN ELAN, etc., mais se concentre uniquement sur les politiques SR-TE pilotées par noeud de tête de réseau avec superposition EVPN VPWS.

1.2. Hypothèse

Le lecteur de ce document doit connaître les concepts d'IP/MPLS et d'Ethernet ainsi que les technologies de routage de segment et d'ingénierie de trafic.

1.3. Champ d'application technique

Le champ d'application technique principal de ce document se limite aux domaines suivants :

- OSPF avec FRR TI-LFA
- Stratégies SR-TE contrôlées par la tête de réseau (distribuées)
- Chemin principal explicite et chemins de basculement dynamiques basés sur IGP
- VPWS EVPN à résidence unique

Les modèles de configuration fournis dans ce document sont appelés Cisco IOS®-XR 7.5.x.

1.4. Résumé du document

Tableau 1 . Sections de document

Type de sujet	Nom du sujet	Numéro de section
Introduction	Informations générales	1
Exigence	Exigences utilisateur	2
Aperçu de la technologie	Routage de segment	3
	Présentation de SR-TE	4
	FRR TI-LFA	5
	Superposition EVPN	6
	BoB et équilibrage de charge	7
Modèles de configuration et exemples de commandes	La solution de conception complète	8
	Exemple de commande Configuration & Show	9

Exigence

2. Exigences utilisateur

2.1. Récapitulatif des besoins

Le fournisseur de services XYZ Networks a besoin de créer un réseau de terrain vert via les périphériques Cisco NCS 5500.

L'objectif est de transporter un flux de données multidiffusion (voix, vidéo) en tant que service sur un réseau de transport de couche 2 avec certaines exigences, dont l'une consiste à concevoir les chemins de trafic à travers le réseau.

Ils ont préféré la SR pour les étiquettes de transport, la SR-TE pour l'ingénierie de trafic et l'EVPN comme superposition pour fournir des étiquettes de service.

2.2. Components Used

L'utilisateur XYZ a convergé sur les routeurs et les cartes de ligne NCS 5500 :

Tableau 2 . Exigences matérielles du projet

Noeuds PE	PID
Châssis	NCS-5504
MPA/LC connectant des noeuds P	NC55-36X100G-A-SE
MPA/LC connectant les noeuds CE	NC55-36X100G-A-SE
Noeuds P	**PID**
Châssis	NCS-5508
MPA/LC connectant d'autres noeuds P	NC55-36X100G-A-SE
MPA/LC connectant les noeuds PE	NC55-36X100G-A-SE

Cette section donne un aperçu des technologies à utiliser avec de brèves descriptions.

Aperçu de la technologie

3. Routage de segment

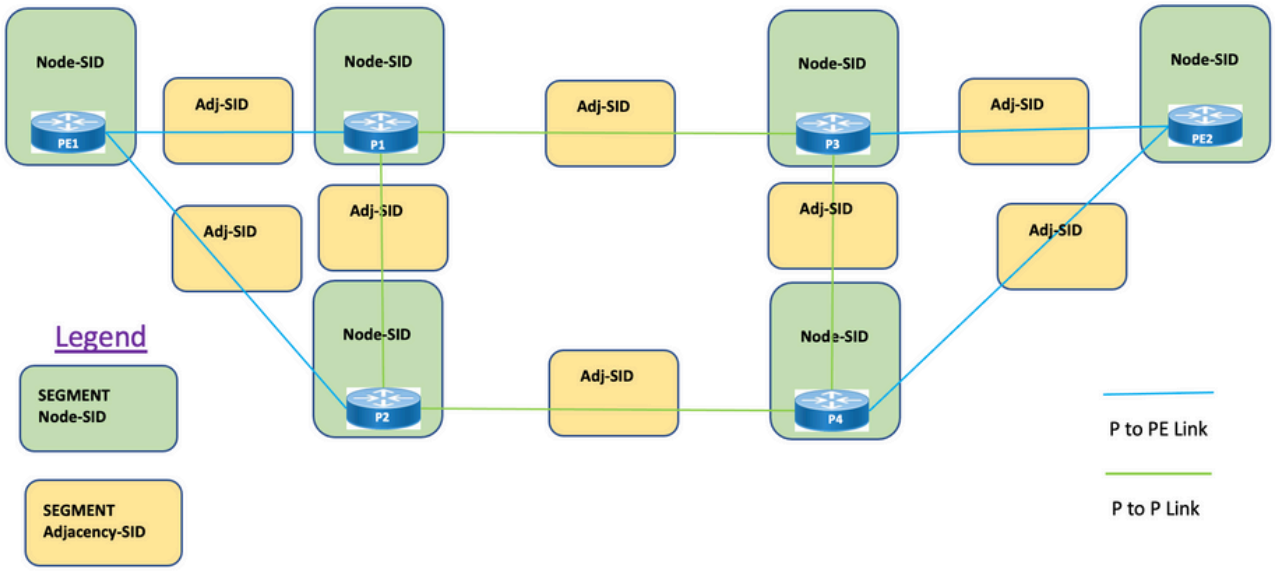
3.1. Qu’est-ce que le routage de segment ?

Le routage de segment est la dernière technologie MPLS avancée qui est en cours de remplacement des protocoles LDP et RSVP-TE traditionnels par l'introduction de la distribution d'étiquettes et de l'ingénierie de trafic sous un même parapluie et pour le faire seulement via les protocoles IGP/BGP à état de liens.

Le routage de segment est une méthode de transmission des paquets sur le réseau basée sur le paradigme de routage source. La source choisit un chemin et l’encode dans l’en-tête du paquet en tant que liste ordonnée de segments. Les segments sont un identificateur pour tout type d'instruction. Par exemple, les segments de topologie identifient le tronçon suivant vers une destination. Chaque segment est identifié par l'ID de segment (SID) qui se compose d'un entier plat non signé de 20 bits.

3.2. Identificateurs de segment

Figure 1. SID de noeud SR et SID de contiguïté



Segments: Le protocole IGP (Interior Gateway Protocol) distribue deux types de segments : Préfixe les segments et les segments de contiguïté. Chaque routeur (noeud) et chaque liaison (contiguïté) ont un identificateur de segment (SID) associé.

SID de préfixe : un segment de préfixe est un segment global, un SID de préfixe est donc globalement unique dans le domaine de routage de segment, comme illustré à la Figure 1. Un SID de préfixe est associé à un préfixe IP. Le SID de préfixe est configuré manuellement à partir de la plage d'étiquettes SRGB (Segment Routing Global Block) et est distribué par IS-IS ou OSPF. Le segment de préfixe dirige le trafic le long du chemin le plus court vers sa destination.

- Utilise le bloc global SR (SRGB)
- SRGB annoncé avec des fonctionnalités de routeur TLV - Dans la configuration, Prefix-SID peut être configuré en tant que valeur absolue ou en tant qu'index
- Dans l'annonce de protocole, Prefix-SID est toujours codé en tant qu'index global unique. L'index représente un décalage par rapport à la base SRGB, la numérotation basée sur zéro, c'est-à-dire 0 est le 1er index. Par exemple, l'index 1 à SID est 16 000 + 1 = 16 001

SID de noeud : un SID de noeud est un type spécial de SID de préfixe qui identifie un noeud spécifique. Il est configuré sous l'interface de bouclage avec l'adresse de bouclage du noeud comme préfixe. Un segment de préfixe est un segment global, de sorte qu'un SID de préfixe est globalement unique dans le domaine de routage de segment.

En d'autres termes, le segment de noeud est un segment de préfixe associé à un préfixe d'hôte qui identifie un noeud.

- Équivalent à un préfixe router-id, qui est un préfixe qui identifie un noeud
- Node-SID est Prefix-SID avec N-flag défini dans l'annonce
- Par défaut, chaque Prefix-SID configuré est un noeud-SID
- 'normal' (c'est-à-dire non-Node-SID) Prefix-SID est configurable pour IS-IS

SID de contiguïté : Un segment de contiguïté est identifié par une étiquette appelée SID de contiguïté, qui représente une contiguïté spécifique, telle qu'une interface de sortie, à un routeur

voisin. Le SID de contiguïté est distribué par IS-IS ou OSPF. Le segment de contiguïté dirige le trafic vers une contiguïté spécifique. Un segment de contiguïté est un segment local, de sorte que le SID de contiguïté est localement unique par rapport à un routeur spécifique.

- Importante localement
- Attribuée automatiquement pour chaque contiguïté
- Toujours encodé comme valeur absolue (c'est-à-dire non indexée)

SID ou BSID de liaison : Il s'agit d'un SID d'importance locale associé à la stratégie SR. Il aide à orienter les paquets dans sa stratégie SR associée. Le segment de liaison est un segment local qui identifie une stratégie SR-TE. Chaque stratégie SR-TE est associée à un ID de segment de liaison (BSID).

Le BSID est une étiquette locale qui est automatiquement allouée pour chaque stratégie SR-TE lorsque la stratégie SR-TE est instanciée. Le BSID peut être utilisé pour diriger le trafic vers la stratégie SR-TE et au-delà des frontières de domaine, ce qui crée des politiques SR-TE inter-domaines de bout en bout transparentes.

4. Présentation de SR-TE

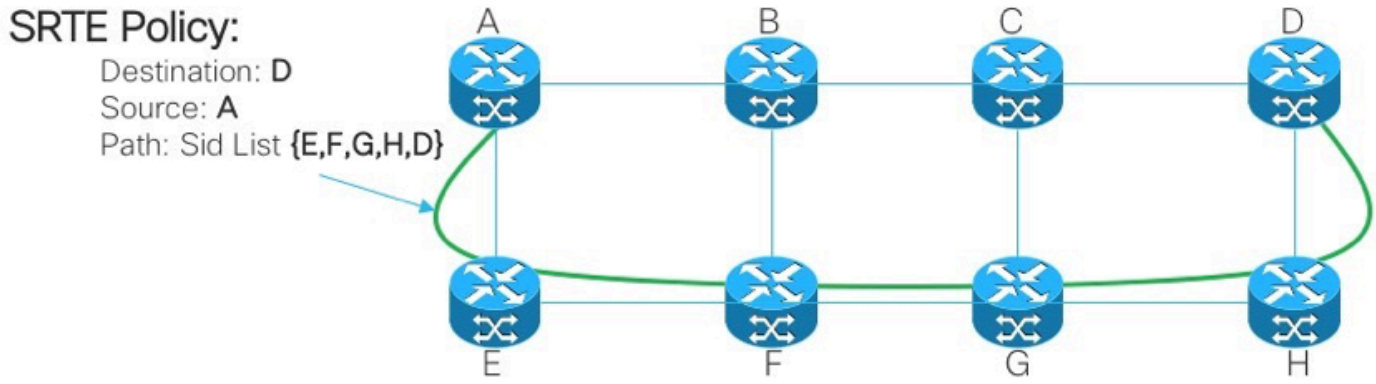
4.1. Qu'est-ce que SR-TE ?

La technologie SR-TE (Segment Routing Traffic Engineering) transforme le mécanisme de routage source simple et sans état de SR en niveau avancé pour programmer et diriger le trafic de données via des chemins prédéfinis qui évitent la congestion et fournissent des chemins alternatifs, tout comme une carte de trafic en direct express.

Ceci est réalisé lorsque vous configurez administrativement des stratégies définies via une combinaison de contraintes diverses qui programment les chemins principal et de sauvegarde de la source aux noeuds de destination. Le contrôleur peut être centralisé (SDN) ou distribué (tête de réseau) selon les besoins du réseau.

Examinons la topologie présentée à la Figure 2. Supposez que le coût des liaisons sont des valeurs par défaut et que le chemin le plus court pour atteindre D à partir de A est A-B-C-D, mais que le chemin à faible latence est A-E-F-G-H-D. L'opérateur peut définir le chemin d'ingénierie de trafic conformément aux exigences (par exemple, Latence) et l'exprimer sous la forme d'une liste d'ID de segment (A, E, F, G, H, D). Contrairement à RSVP-TE, l'état de cette stratégie est maintenu au niveau du routeur A uniquement et non sur l'ensemble des routeurs traversés par les paquets (c'est-à-dire E, F, G et H).

Figure 2. Exemple de chemin défini administrativement par SR-TE



4.2. Stratégie SR-TE

Le routage de segment pour l'ingénierie de trafic (SR-TE) utilise une politique pour diriger le trafic à travers le réseau. Un chemin de stratégie SR-TE est exprimé sous la forme d'une liste de segments qui spécifie le chemin, appelé liste SID (Segment ID). Chaque segment est un chemin de bout en bout de la source à la destination et indique aux routeurs du réseau de suivre le chemin spécifié au lieu de suivre le chemin le plus court calculé par le protocole IGP. Si un paquet est dirigé vers une stratégie SR-TE, la liste SID est poussée sur le paquet par la tête de réseau. Le reste du réseau exécute les instructions intégrées dans la liste SID.

Une stratégie SR-TE est identifiée comme une liste ordonnée (tête de réseau, couleur, point final) :

- Tête de réseau : où la stratégie SR-TE est instanciée
- Couleur : valeur numérique qui fait la distinction entre deux politiques ou plus et les mêmes paires de noeuds (tête de réseau - point de terminaison)
- Point de terminaison : destination de la stratégie SR-TE
- Chaque stratégie SR-TE a une valeur de couleur. Chaque stratégie entre les mêmes paires de noeuds nécessite une valeur de couleur unique.

Une stratégie SR-TE est configurée avec un ou plusieurs chemins candidats qui incluent les chemins principal et de secours.

Par exemple, le chemin principal de la stratégie peut être explicitement défini avec des SID de contiguïté et, en cas de scénario d'échec, le chemin de sauvegarde peut être dynamique et pris en charge par la métrique IGP.

5. FRR TI-LFA

5.1. Aperçu

TI-LFA (Topology Independent loop-free Alternate) est une fonctionnalité qui protège les liaisons, les noeuds et les SRLG. Il est simple à configurer ; seules deux lignes de configuration sont nécessaires pour implémenter une configuration TI-LFA simple dans le routeur. Il ne nécessite aucune modification des protocoles utilisés dans le routeur. Figure 3. La présente le chemin de trafic principal et le chemin de sauvegarde précalculé par TI-LFA pour les scénarios de défaillance de liaison locale et de défaillance de noeud.

Figure 3. Scénario de basculement de liaison LFA TI

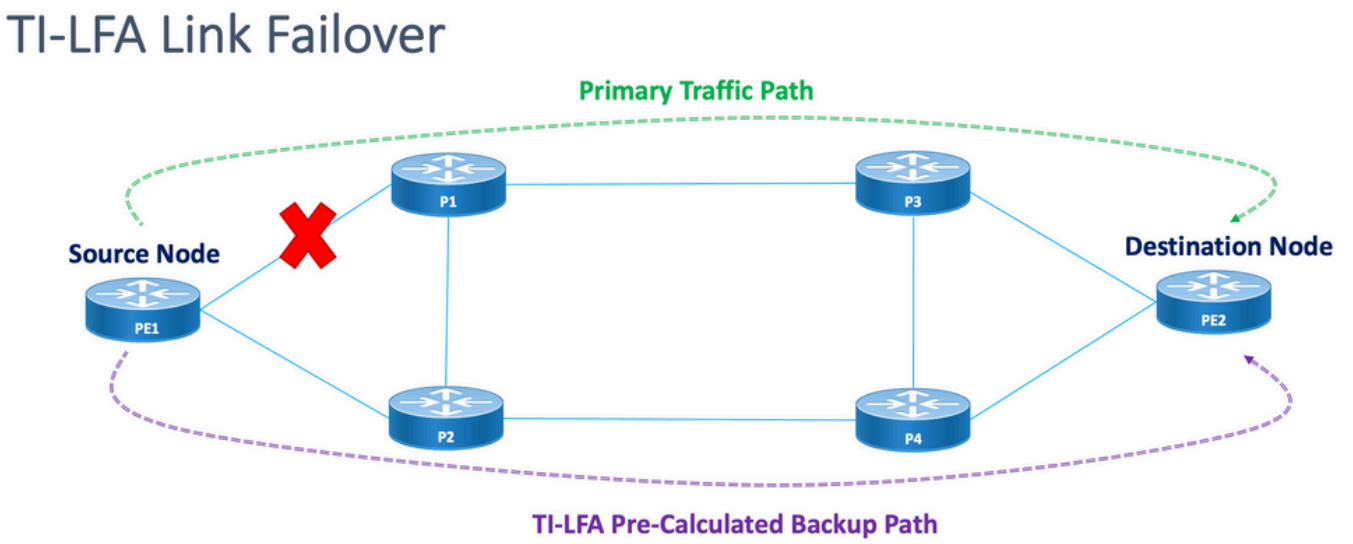
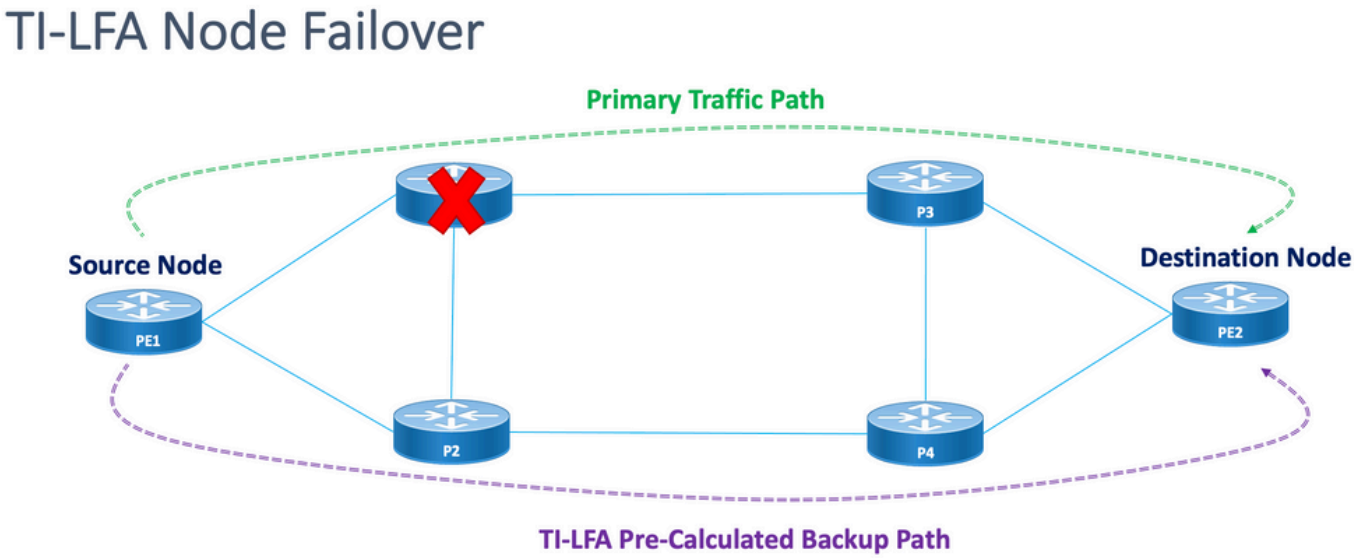


Figure 4. Scénario de basculement de noeud TI LFA



Chaque noeud et chemin protégés possède un chemin de sauvegarde précalculé qui peut être activé rapidement. Le temps de convergence d'un chemin protégé est de 50 millisecondes ou moins. Cela signifie que même les applications les plus sensibles à la latence ou à la perte de paquets peuvent fonctionner sans interruption en cas de défaillance d'un noeud ou d'une liaison. TI-LFA calcule le chemin de sauvegarde et supprime temporairement la liaison ou le noeud protégé de la base de données. Après cela, il calcule d'abord le chemin de sauvegarde avec le chemin le plus court. Cela garantit que le chemin de sauvegarde a le coût métrique le plus faible possible, tout en évitant le chemin protégé. Un tunnel généré par le trafic qui suit le chemin de sauvegarde est utilisé pour le trafic en cas de panne. Une liste d'étiquettes de réparation détermine le chemin des paquets qui ont besoin d'une nouvelle route vers leur destination. Une liste d'étiquettes de réparation est une pile d'étiquettes normale, mais elle n'est utilisée que lorsqu'une défaillance se produit dans la route protégée.

5.2. Impact de la méthode de détection des défaillances sur le FRR

Fast Reroute pour les chemins d'ingénierie de trafic SR-TE est configuré comme un moyen de commuter le trafic en cas de scénarios de basculement du chemin principal aux chemins de

sauvegarde dans un rayon aussi proche que possible de 50 ms. La fonction de réacheminement rapide est configurée sous le protocole IGP (OSPF/ISIS). Le temps de convergence dépend de la méthode par laquelle la détection des défaillances de liaison se produit. Dans le cas d'une coupure de fibre, la détection est immédiate et la possibilité d'obtenir un minimum de 50 ms de convergence est élevée. Cependant, au cas où la détection de défaillance de liaison doit être effectuée par BFD avec un intervalle de 15 ms (multiplicateur x3). Le temps de convergence est généralement supérieur à 50 ms.

5.3. Évitement du micrologiciel avec SR

Les microloops sont de brèves boucles de paquets qui se produisent sur le réseau à la suite d'une modification de topologie (événements de liaison inactive, de liaison active ou de modification de métrique). Les microloops sont provoquées par la convergence non simultanée de différents noeuds du réseau. Si les noeuds convergent et envoient le trafic vers un noeud voisin qui n'a pas encore convergé, le trafic peut être bouclé entre ces deux noeuds, ce qui entraîne la perte de paquets, la gigue et les paquets hors-ordre.

La fonction d'évitement de microloop de routage de segment détecte si les microloops sont éventuellement suivis d'une modification de topologie. Si un noeud calcule qu'une micro-boucle peut se produire sur la nouvelle topologie, il crée un chemin de stratégie SR-TE sans boucle vers la destination à l'aide d'une liste de segments. Une fois le délai de mise à jour RIB expiré, la stratégie SR-TE est remplacée par des chemins de transfert réguliers. Il existe un compteur par défaut pour le délai de mise à jour RIB qui est pris en charge par TI-LFA.

6. Superposition EVPN

EVPN est une technologie initialement conçue pour les services multipoints Ethernet, avec des fonctionnalités avancées de multihébergement, avec l'utilisation de BGP pour distribuer les informations d'accessibilité des adresses MAC sur le réseau MPLS, tout en apportant les mêmes caractéristiques opérationnelles et d'évolutivité des VPN IP aux VPN L2VPN. Aujourd'hui, au-delà des applications DCI et E-LAN, la gamme de solutions EVPN fournit une base commune pour tous les types de services Ethernet, qui inclut E-LINE et E-TREE, ainsi que des scénarios de routage et de pontage de data center. EVPN fournit également des options permettant de combiner les services L2 et L3 dans la même instance.

EVPN est une solution de nouvelle génération qui fournit des services multipoints Ethernet sur des réseaux MPLS. EVPN fonctionne à la différence du VPLS (Virtual Private LAN Service) qui existe et qui permet l'apprentissage MAC basé sur le plan de contrôle BGP dans le coeur. Dans EVPN, les PE qui participent aux instances EVPN apprennent les routes MAC utilisateur dans Control-Plane à l'aide du protocole MP-BGP.

EVPN apporte un certain nombre d'avantages, comme mentionné ci-dessus :

- Redondance par flux et équilibrage de charge
- Provisionnement et fonctionnement simplifiés
- Transfert optimal
- Convergence rapide
- Évolutivité des adresses MAC
- Solutions multifournisseurs dans le cadre de la normalisation IETF

Les adresses MAC apprises sur un périphérique doivent être apprises ou distribuées sur les autres périphériques d'un VLAN. La fonction Apprentissage MAC du logiciel EVPN permet de

distribuer les adresses MAC acquises sur un périphérique aux autres périphériques connectés à un réseau. Les adresses MAC sont apprises à partir des périphériques distants à l'aide du protocole BGP.

Dans ces sections, vous découvrirez certains des avantages et des types de routage d'EVPN en général, puis comprendrez les composants spécifiques à la solution qui sont appliqués à la conception des services réseau XYZ.

6.1. Avantages d'EVPN

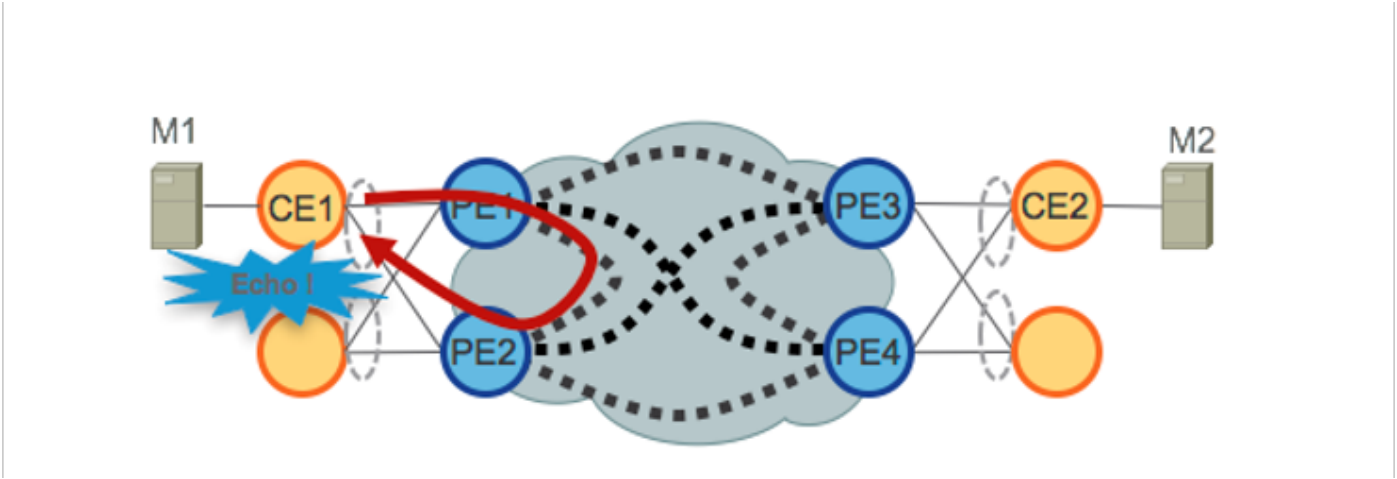
Les réseaux L2VPN et L3VPN fournissent non seulement des services sous un même parapluie de solutions avec l'aide de différents types de route, mais ils résolvent également deux limitations de longue date pour les services Ethernet dans les réseaux des fournisseurs de services :

- Accès Ethernet multirésidence et tout actif
- Réseau du fournisseur de services : intégration au bureau central ou au centre de données

6.1.1 . Accès Ethernet multirésidence et tout actif

La figure illustre la plus grande limitation des solutions multipoints de couche 2 traditionnelles telles que VPLS.

Figure 5. Accès actif EVPN



Lorsque VPLS s'exécute dans le coeur, l'évitement de boucle nécessite que PE1/PE2 et PE3/PE4 fournissent uniquement une redondance active unique vers leurs CE respectifs. Traditionnellement, des techniques telles que mLACP ou les protocoles L2 hérités tels que MST, REP, G.8032, etc. ont été utilisées pour fournir une redondance d'accès actif unique.

La même situation se produit avec Hierarchical-VPLS (H-VPLS), où le noeud d'accès est responsable de fournir un accès H-VPLS mono-actif par un pseudowire en étoile actif et de secours (PW).

Les modèles de redondance d'accès actif ne peuvent pas être déployés car la technologie VPLS n'a pas la capacité d'empêcher les boucles de couche 2 qui dérivent des mécanismes de transfert utilisés dans le coeur de réseau pour certaines catégories de trafic. Le trafic de diffusion, de monodiffusion inconnue et de multidiffusion (BUM) provenant du CE est diffusé dans le coeur du VPLS et est reçu par tous les PE, qui le diffusent à tous les CE connectés. Dans notre exemple,

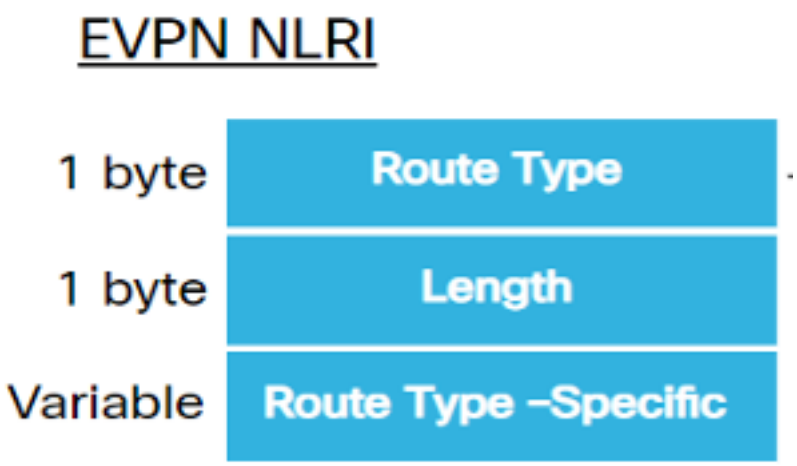
PE1 peut inonder le trafic BUM de CE1 vers le coeur de réseau, et PE2 peut le renvoyer vers CE1 une fois reçu.

EVPN utilise des techniques de plan de contrôle BGP pour résoudre ce problème et active des modèles de redondance d'accès Active-Active pour l'accès Ethernet ou H-EVPN.

6.2. Types de routage EVPN

EVPN définit une nouvelle NLRI BGP qui est utilisée pour transporter toutes les routes EVPN. EVPN NLRI est transporté dans BGP avec l'utilisation d'extensions multiprotocoles avec un AFI de 25 (L2VPN) et un SAFI de 70. L'annonce des fonctionnalités BGP permet de s'assurer que deux haut-parleurs prennent en charge l'EVPN NLRI.

Figure 6. NLRI EVPN



Les types de route EVPN appropriés nécessaires à cette mise en oeuvre sont décrits ici :

6.2.1 . Route Type 1 - Route de découverte automatique Ethernet (AD)

Les routes de découverte automatique Ethernet (AD) sont annoncées par interface EVI et par ESI. Ces routes sont envoyées par ES. Ils portent la liste des EVI qui appartiennent à l'ES. Le champ ESI est défini sur zéro lorsqu'un CE est à résidence unique. Ce type de route est utilisé pour un retrait massif d'adresses MAC, un alias pour l'équilibrage de charge et le filtrage à horizon divisé.

6.2.2 . Route Type 4 - Ethernet Segment Route

Les routes de segment Ethernet permettent la connexion d'un périphérique CE à deux ou deux périphériques PE. La route ES permet de détecter les périphériques PE connectés qui sont connectés au même segment Ethernet, c'est-à-dire la détection de groupe de redondance. Il est également utilisé pour la sélection du redirecteur désigné (DF).

6.3. Connectivité hôte EVPN

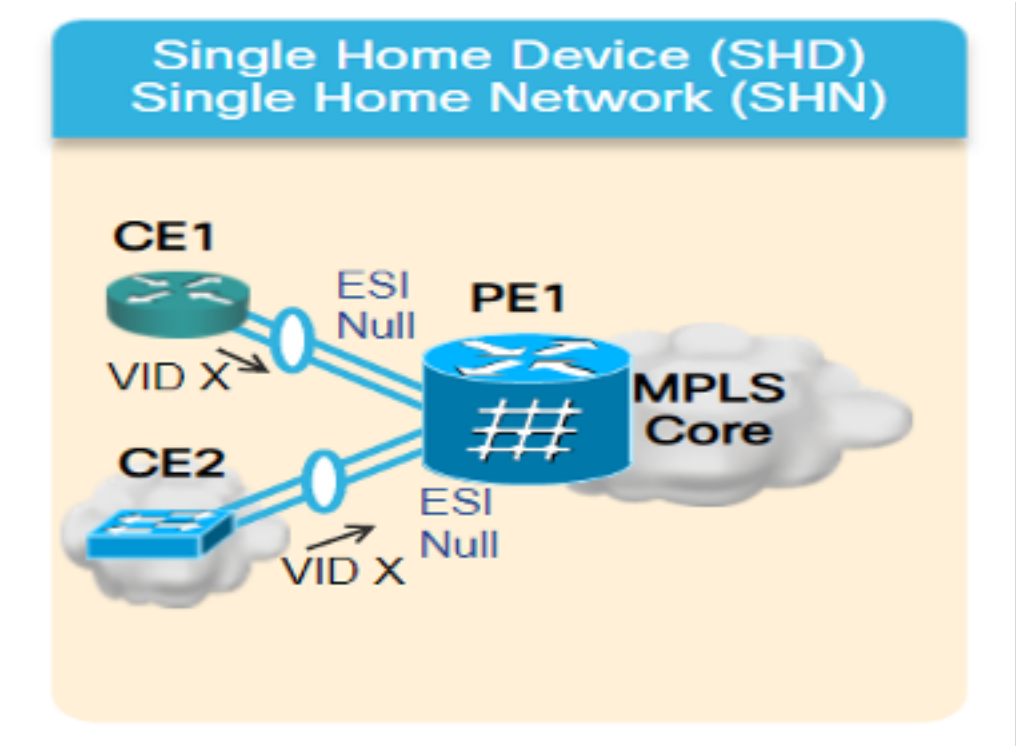
Ces modes EVPN sont pris en charge :

- Liaison unique : permet de connecter un périphérique de périphérie utilisateur (CE) à un périphérique de périphérie fournisseur (PE). Dans cette valeur ESI est nulle pour chaque

liaison PE-CE.

- Multihoming (Multihoming) : permet de connecter un périphérique de périphérie utilisateur (CE) à deux ou plusieurs périphériques de périphérie fournisseur (PE) pour fournir une connectivité redondante. Aucune liaison d'interconnexion n'est requise. Le périphérique PE redondant garantit qu'il n'y a pas de perturbation du trafic en cas de défaillance du réseau. Les types de multihébergement sont les suivants :

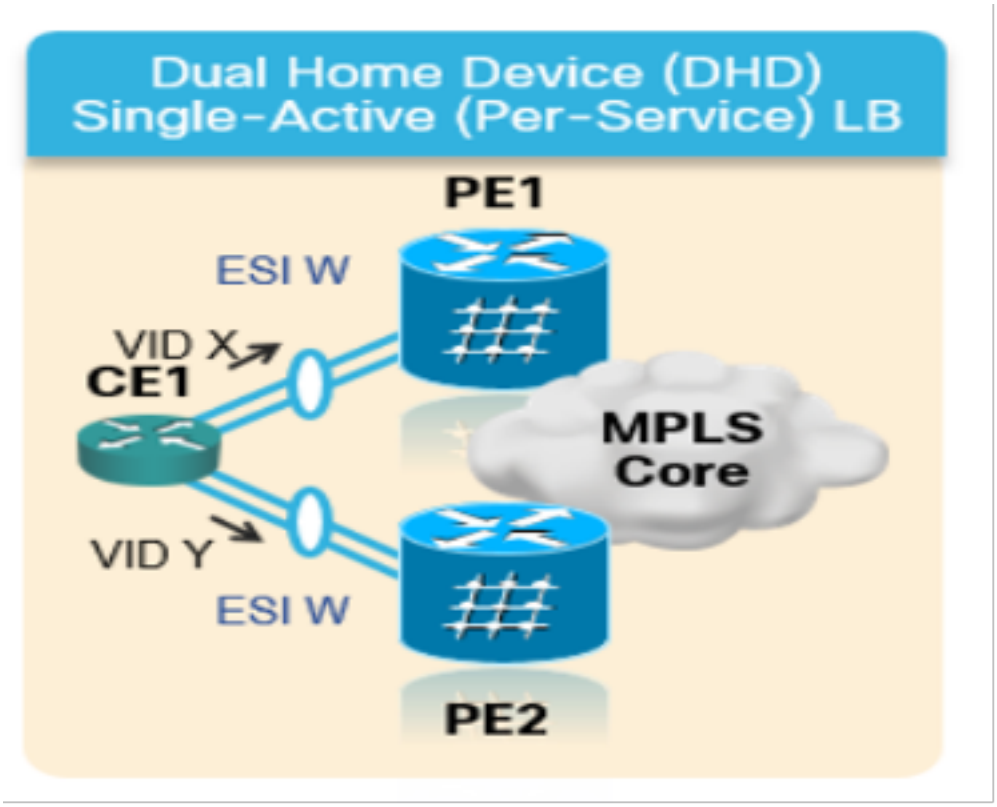
Figure 7. Résidence unique EVPN



Multihoming (Multihébergement) : il s'agit des types de multihoming :

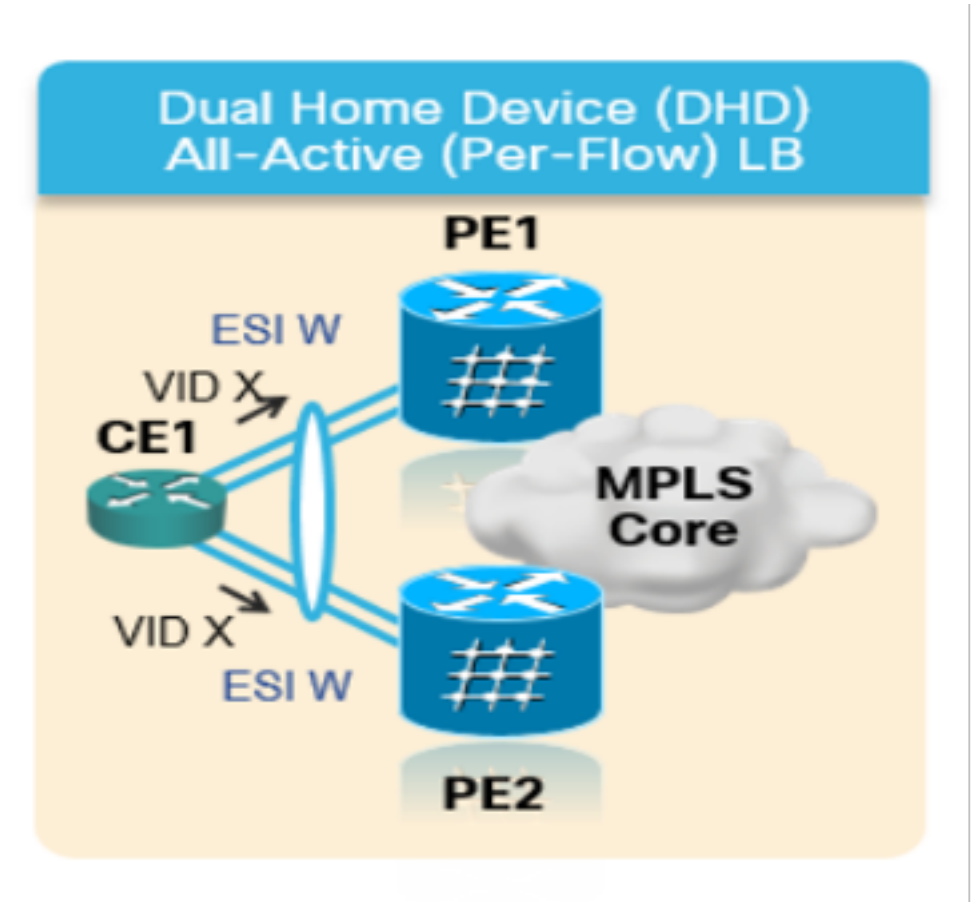
1. Single-Active : en mode single-active, seul un seul PE d'un groupe de PE connecté au segment Ethernet donné est autorisé à transférer le trafic vers et depuis ce segment Ethernet.

Figure 8. EVPN mono-actif



2. Active-Active : en mode actif-actif, tous les PE connectés au segment Ethernet donné sont autorisés à transférer le trafic à destination et en provenance de ce segment Ethernet.

Figure 9. EVPN double actif



7. BoB et équilibrage de charge

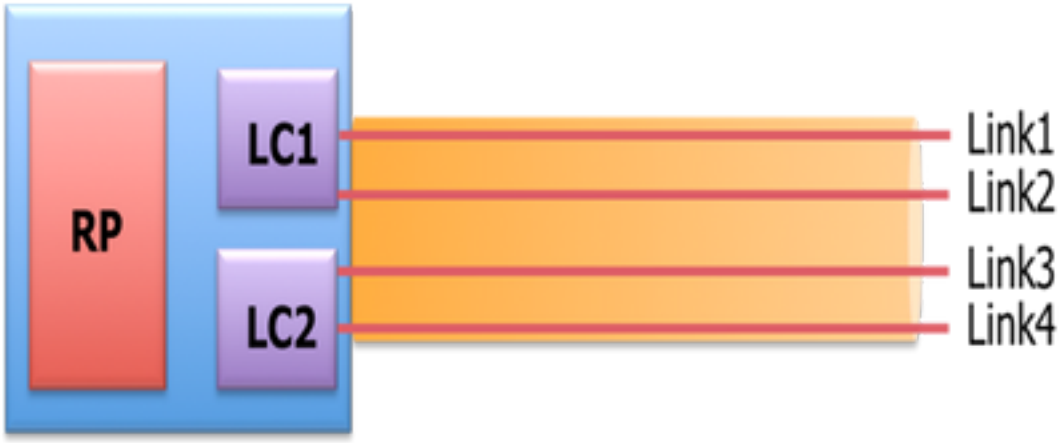
7.1. Offre groupée BFD (BoB)

La détection BFD (Bidirectional Forwarding Detection) permet de détecter les pannes de courte durée et à faible surcharge sur le chemin entre les moteurs de transfert adjacents. Le BFD permet d'utiliser un mécanisme unique pour la détection des pannes sur n'importe quel support et sur n'importe quelle couche de protocole, avec un large éventail de temps de détection et de surcharge. La détection rapide des pannes fournit une réaction immédiate en cas de défaillance d'une liaison ou d'un voisin.

Cela déclencherait l'IGP à commencer à transférer le trafic vers le chemin de sauvegarde déjà calculé avec l'utilisation de FRR (dans le cas d'IGP) et PIC (dans le cas de BGP).

Dans la fonctionnalité BFD Over Bundle (BoB), la session BFD IPv4 s'exécute sur chaque membre actif du bundle.

Figure 10. Diagramme logique BoB



Bundlemgr prend en compte les états BFD, en plus des états L1/L2 qui existent, pour déterminer la convivialité de la liaison de membre. L'état membre de l'offre groupée est fonction de :

État L1 (liaison physique)

État L2 (LACP)

État de couche 3 (BFD)

L'agent BFD fonctionne toujours sur la carte de ligne. Les états BFD des liaisons de membres de l'offre groupée sont consolidés sur RP. Les liaisons membres doivent être connectées dos à dos, sans commutateur L2 entre les deux. La fonctionnalité BoB est configurée dans toutes les interfaces Ethernet d'offre groupée sur le réseau XYZ.

7.2. Équilibrage de charge

Équilibrage de charge ECMP par flux dans le réseau concerné s'étend sur les interfaces Ethernet entre les bundles et les Ethernet intra-bundle (entre les membres physiques d'une interface Bundle). Ceci s'applique à l'ensemble du réseau, de PE à PE (Core Load Balance) et de PE à CE (AC Load-Balance), comme discuté.

7.2.1 . Équilibrage de charge de base avec étiquette FAT

En fonction de la portée du réseau XYZ, vous devez considérer uniquement l'équilibrage de charge ECMP par flux (chemin multiple à coût égal) comme indiqué :

Les routeurs équilibrent généralement la charge du trafic en fonction de l'étiquette la plus basse de la pile d'étiquettes, qui est la même étiquette pour tous les flux d'un pseudocâble donné. Cela peut conduire à un équilibrage de charge asymétrique. Dans ce contexte, le flux fait référence à une séquence de paquets qui ont la même paire source et de destination. Les paquets sont transportés d'un périphérique fournisseur source (PE) vers un périphérique fournisseur de destination.

Le Pseudowire de transport sensible aux flux (FAT PW) permet d'identifier les flux individuels au sein d'un pseudowire et offre aux routeurs la possibilité d'utiliser ces flux pour équilibrer la charge du trafic. Les PW FAT sont utilisés pour équilibrer la charge du trafic dans le coeur de réseau lorsque des chemins ECMP (Equal-Cost Multipaths) sont utilisés. Une étiquette de flux est créée en fonction des flux de paquets indivisibles qui entrent dans un pseudocâble et sont insérés en tant qu'étiquette la plus basse du paquet. Les routeurs peuvent utiliser l'étiquette de flux pour l'équilibrage de charge, ce qui améliore la distribution du trafic sur les chemins ECMP ou les chemins de liaison groupés dans le coeur.

Une étiquette supplémentaire est ajoutée à la pile, appelée étiquette de flux, générée pour chaque flux entrant unique sur le PE. Une étiquette de flux est un identificateur unique qui distingue un flux dans le PW et provient des adresses MAC source et de destination, ainsi que des adresses IP source et de destination. L'étiquette de flux contient la fin du jeu de bits de la pile d'étiquettes (EOS). L'étiquette de flux est insérée après l'étiquette VC et avant le mot de contrôle (le cas échéant). Le PE d'entrée calcule et transfère l'étiquette de flux. La configuration FAT PW active l'étiquette de flux. Le PE de sortie rejette l'étiquette de flux de sorte qu'aucune décision ne soit prise.

7.2.2 . Équilibrage de charge du circuit de connexion

Pour l'équilibrage de charge des membres de l'offre groupée CA, cependant, vous avez besoin d'une approche différente en raison de l'absence de SR-MPLS dans cette section du réseau.

L'équilibrage de charge par flux peut être réalisé ici lorsque des boutons de configuration l2vpn spécifiques sur tous les routeurs PE sont explicitement modifiés. Il peut être défini par adresse MAC SRC/DST ou par adresse IP SRC/DST selon les besoins.

Modèles de configuration et exemples de commandes

8. La solution de conception complète

Cette section traite des détails complets de la conception cousus par tous les composants individuels qui ont été expliqués dans les sections précédentes. Cette section décrit la topologie et le modèle de configuration approprié en référence à Cisco IOS-XR 7.5.x.

8.1. Exigences de bas niveau

Pour le scénario de trafic normal, le flux de trafic est conçu pour se propager toujours entre les terminaisons de service de PE1 et PE3 et entre PE2 et PE4 uniquement. L'objectif principal dans cette situation est de maintenir la disjonction complète du chemin de trafic, comme illustré à la Figure 12.

Le trafic concerné ici serait des flux de multidiffusion encapsulés via la superposition EVPN. À partir des noeuds CE1 et CE2, les flux multidiffusion (voix/vidéo) sont fournis dans lesquels ils peuvent être encapsulés au niveau des noeuds PE1 et PE2 et transportés sur la superposition EVPN L2 vers les noeuds CE3 et CE4 respectivement après avoir été décapsulés au niveau des noeuds PE3 et PE4 respectivement.

Par conséquent, la paire de trafic source-destination est dorénavant considérée comme PE1-PE3 et PE2-PE4 en toutes circonstances, sauf mention contraire. Pour plus de détails sur les exigences, veuillez vous reporter à la sous-section 2.2.

8.2. Résumé de la conception

Pour répondre à ces exigences, OSPF est choisi comme IGP sous-jacent comme souhaité par les réseaux XYZ. Pour diriger le flux de multidiffusion encapsulé à travers la paire de trafic source-destination via le chemin souhaité, SR-TE doit être mis en oeuvre entre les noeuds PE.

Les stratégies SR-TE ont été conçues avec des chemins d'accès IGP explicites et dynamiques.

Les chemins explicites couvrent les éléments suivants :

- Scénario de trafic normal
- Scénario de basculement jusqu'à ce que d'autres options de chemin soient disponibles

Les chemins IGP dynamiques couvrent :

- Chemin de sauvegarde pour scénario de basculement dans lequel les options de chemin alternatif ne sont PAS disponibles

Les fonctionnalités telles que BFD, TI-LFA et Microloop Avoidance sont configurées sous OSPF comme indiqué dans les sous-sections des modèles de configuration.

Pour les scénarios de trafic normaux, le modèle de configuration et d'autres détails sont mentionnés dans la sous-section 8.5.1.

Pour les scénarios de basculement de trafic, le modèle de configuration et d'autres détails sont mentionnés dans la sous-section 8.5.2.

En outre, les exigences telles que l'évitement de microloop et moins de 50 ms de convergence en cas de panne sont également prises en compte.

8.3. Blocs de conception

Cette sous-section présente tous les éléments de conception qui sont ensuite traités en détail dans ces sections.

Présentation générale de la conception (couche 1) :

- La taille de MTU sur le réseau XYZ est fixée à 9216 dans le but de prendre en charge jusqu'à 5 à 6 piles d'étiquettes SR
- 'BFD over Bundle' est mis en oeuvre avec un intervalle de 15 ms pour détecter la coupure de fibre inférieure à 50 ms

Présentation de la conception OSPF/SR-TE :

- **OSPF** comme protocole IGP avec **TI-LFA** configuré pour fournir **FRR** moins de 50 ms de temps de convergence
- **Couche transport** basée sur le **routage de segment** comme plan de transfert et **OSPF** comme protocole de routage
- Dans le réseau XYZ, le chemin explicite **Segment Routing Traffic Engineering** dirige le trafic dans toutes les directions de chemin principal requises. Dans le cas de scénarios de basculement de liaison/noeud, le trafic est routé par un chemin igp dynamique
- L'évitement de microloop et la métrique maximale OSPF font également partie de cette conception

Présentation de la conception BGP/RR :

- Il y a **deux RR** configurés dans un cluster pour fournir une **redondance**
- Le processus XYZ Network, BGP dans chaque PE forme '**IPv4**' et '**L2VPN EVPN**' avec les deux RR séparément

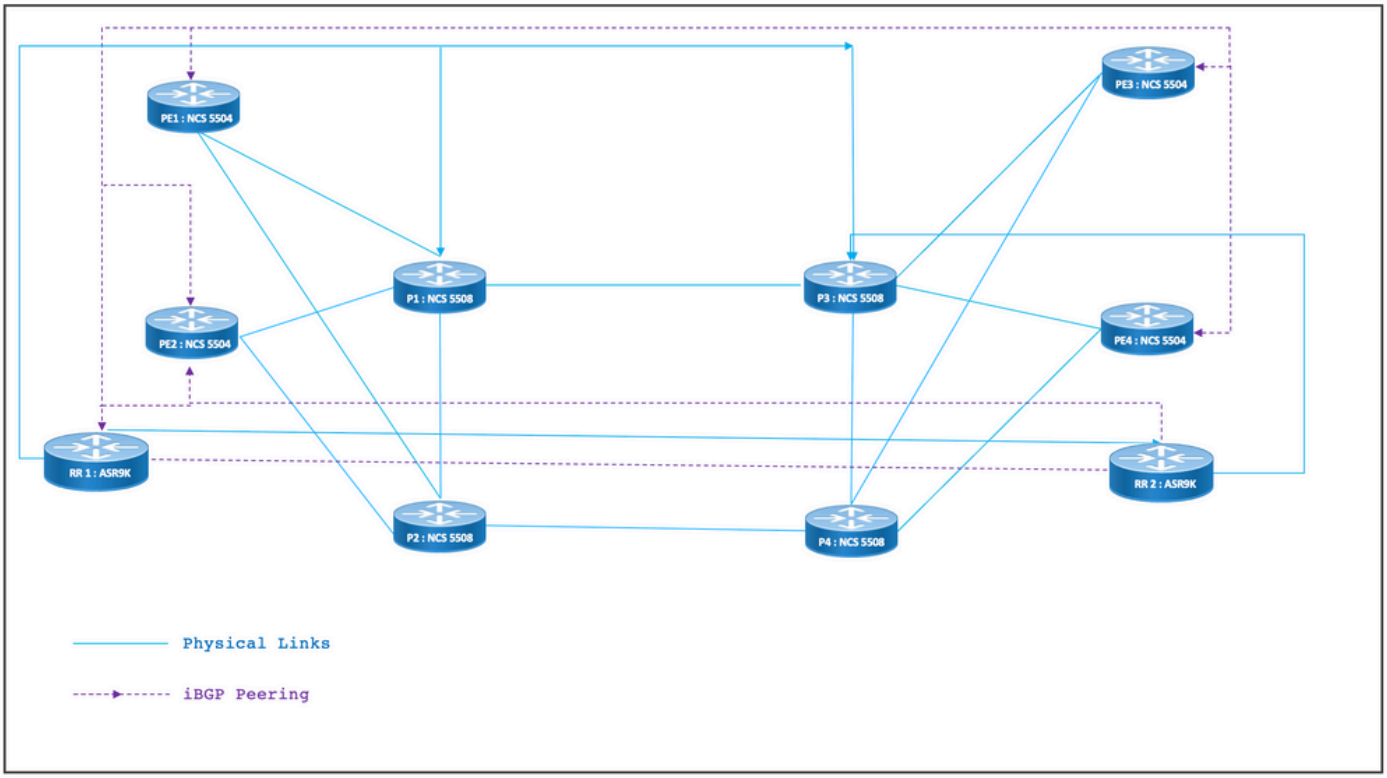
Présentation de la conception des services :

- **Les couches de service** sont construites sur le **plan de contrôle BGP** et l'EVPN point à point de couche 2 (**EVPN-VPWS**)
- Le trafic vidéo de multidiffusion (UDP) est envoyé encapsulé sur les PW point à point EVPN-VPWS
- **L'équilibrage de charge ECMP** est réalisé par la configuration de l'étiquette FAT sous la section EVPN.
- Le service vise à prendre en charge jusqu'à 5 à 6 piles d'étiquettes SR comprenant des étiquettes de transport SR, des étiquettes EVPN et des étiquettes FAT pour l'équilibrage de charge

8.4. Exemple de topologie physique

La topologie physique des réseaux XYZ est représentée dans cette figure. Par souci de simplicité, seuls 4 noeuds PE et 4 noeuds P sont affichés. Il existe deux noeuds RR qui agissent dans des clusters pour fournir une redondance.

Figure 11. Topologie physique



8.5. Détails de la conception de couche 1

Dans la conception générique de couche 1, il existe un bundle Ethernet avec au moins deux liaisons membres par bundle configuré. Pour détecter rapidement les défaillances de liaison, choisissez BFD sur la fonctionnalité Bundle. L'intervalle de temps peut être idéalement varié entre 5 et 15 ms. Cela dépend de la capacité matérielle à se décharger.

Pour plus d'informations sur le BFD, consultez le site https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/73x/b-routing-cg-ncs5500-73x/implementing-bfd.html. Notez que cette fonctionnalité doit être configurée uniquement sous l'interface Ethernet du bundle et qu'il n'est pas nécessaire de la configurer sous IGP. La taille de MTU est fixée à **9216** avec un objectif de prise en charge jusqu'à 5 à 6 SR label-stack.

8.5.1 . Modèles de configuration

Les modèles de configuration BFD over Bundle pour tous les noeuds sont les suivants :

```
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. Présentation de la conception OSPF/SR-TE

Tous les routeurs OSPFv2 du réseau se trouvent dans la zone 0 et le réseau gère donc un seul domaine IGP.

Sous le protocole OSPF du routeur, le routage de segment est activé et les interfaces Ethernet du bundle correspondantes sont configurées. De même, sous Bundle Interfaces, le type de réseau et les paramètres de réacheminement rapide sont activés. Plus important encore, une interface de bouclage est activée en mode passif avec Prefix-SID configuré.

Le protocole OSPF est un protocole à état de liens. Il doit donc être prioritaire d'identifier immédiatement les liaisons descendantes et de créer un chemin de secours. Pour cela, BFD over Bundle sous Bundle Interface et TI-LFA FRR sous OSPF sont configurés, ce qui permet de maintenir le temps de convergence à 50 ms dans le cas de scénarios de découpe de fibre.

Les sous-sections suivantes décrivent en détail les scénarios normaux et de basculement des chemins de trafic :

8.6.1 . Scénario de trafic normal SR-TE

Pour maintenir un chemin principal très strict, les politiques SR-TE doivent être conçues avec des chemins explicites de bout en bout entre les paires de trafic source-destination mentionnées précédemment. En outre, plusieurs chemins de préférence possibles sont nécessaires dans une stratégie SR-TE pour fournir des possibilités de basculement multiples.

Cette figure illustre les détails du réseau utilisateur en fonction des blocs de conception mentionnés dans la sous-section 8.3.

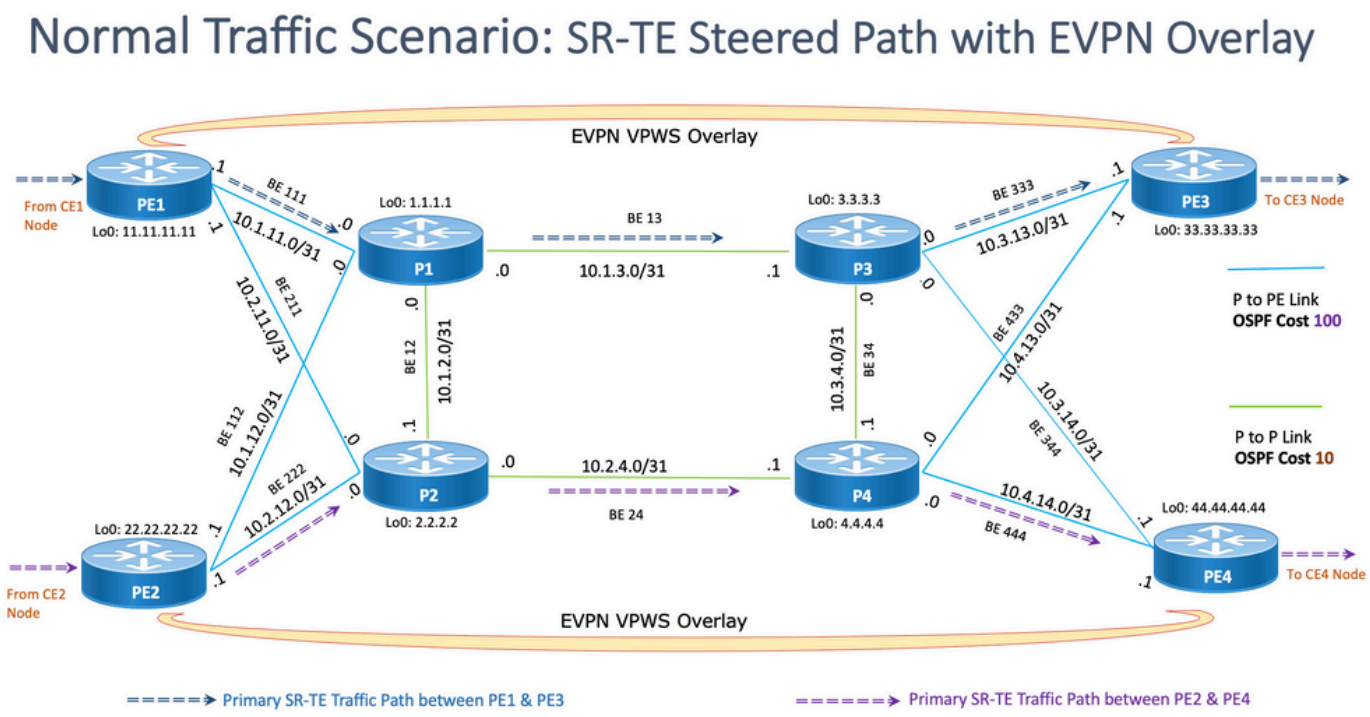
- Liens entre les noeuds PE à P et P à P
- Adresses de bouclage de tous les noeuds
- Adresses d'interface de tous les noeuds
- Direction du chemin de trafic normal dirigé par SR-TE
- Superposition EVPN entre les noeuds PE

Les RR n'ont pas été montrés intentionnellement pour réduire l'encombrement dans la topologie.

Les liaisons entre PE et P ont été marquées en bleu et les liaisons entre P et P ont été marquées en vert. Le coût OSPF des liaisons PE à P est de 100 et le coût des liaisons P à P est de 10.

Le flux de trafic SR-TE principal a été marqué par des flèches bleues entre la paire PE1-PE3 et des flèches violettes entre la paire PE2-PE4.

Figure 12. Détails de la topologie



8.6.1.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés du protocole OSPF/SR-TE pour les noeuds PE1 et PE2, comme indiqué :

```
# 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**: Pour configurer la commande **Source-Address** ” GLOBALEMENT OU sous POLICY. En tant que comportement par défaut, l'adresse source sous la stratégie remplace la commande globale.

La commande d'adresse source sous la configuration de routage de segment comme indiqué est nécessaire dans des scénarios spécifiques où, dans le même PE, comme source de la stratégie SR-TE, nous devons choisir une adresse de bouclage parmi plusieurs ou lorsque ISIS et OSPF s'exécutent tous deux avec des bouclages séparés, et nous devons geler sur l'une de ces adresses. Sinon, dans les scénarios normaux où il n'y a qu'un seul IGP qui fonctionne avec un bouclage unique, alors la configuration de l'adresse source est facultative.

```
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                    Command to distribute OSPF database into SR-TE database
 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: Les commandes source facultatives, SRGB par défaut et SRLB ont été supprimées.

```
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: Dans la solution mentionnée précédemment, les sauts explicites des listes de segments sont basés sur des adresses IP, car comme mentionné ici, la configuration explicite de la stratégie SR-TE de chemin basée sur " **étiquette mpls** " la validation du chemin ne fonctionne pas pour une défaillance de liaison distante dans 7.3.x

En cas d'échec d'une liaison distante, en dehors de la liaison locale d'un noeud PE, le chemin reste valide. Il est conçu et ne peut pas être modifié avant 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 pour scénarios de basculement

Pour comprendre les scénarios de basculement de trafic, il faut examiner de près le trafic du chemin principal dans des conditions de trafic normales, comme indiqué dans le schéma de topologie de la sous-section précédente.

L'objectif principal dans le cas de scénarios de basculement est de maintenir la discontinuité du

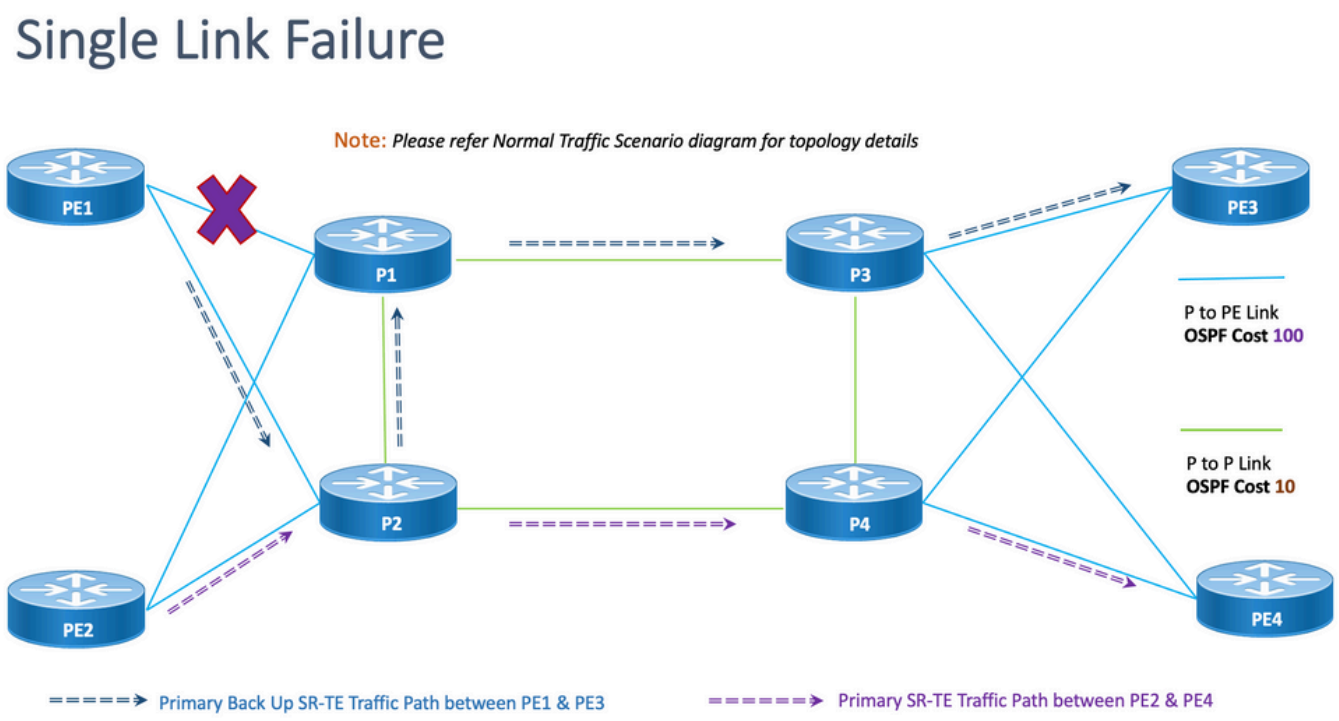
chemin de trafic dans toute la mesure possible, compte tenu de l'infrastructure topologique actuelle. Le réseau XYZ a des exigences strictes pour diriger administrativement le trafic via des noeuds spécifiques dans des chemins de sauvegarde afin de maintenir une séparation maximale entre les paires de noeuds source et de destination. Cette conception permet d'éviter la surcharge des liaisons utilisées et de conserver un minimum de liaisons inutilisées.

Ces sous-sections présentent les différents scénarios de basculement tels que liaison unique, liaison double, noeud unique et noeud double avec le chemin de basculement que le trafic prend pour maintenir une désunion maximale.

8.6.3 . Scénario de basculement de liaison unique

Il s'agit du scénario de défaillance d'une liaison unique où la liaison locale entre PE1 et P1 échoue et où le trafic fait un détour par les noeuds P2 et P1 principaux. Cette opération est administrativement dirigée via la liste de segments <SIDLIST1> qui constitue le chemin de sauvegarde principal entre les noeuds PE1 et PE3.

Figure 13. Scénario de basculement de liaison unique



Disparité : En cas de défaillance d'une liaison unique, le nombre de liaisons communes partagées est égal à zéro (0), comme indiqué dans la topologie précédente.

8.6.3.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés du protocole OSPF/SR-TE pour les noeuds PE1 et PE2, comme indiqué ici :

> **Note**: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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>
```

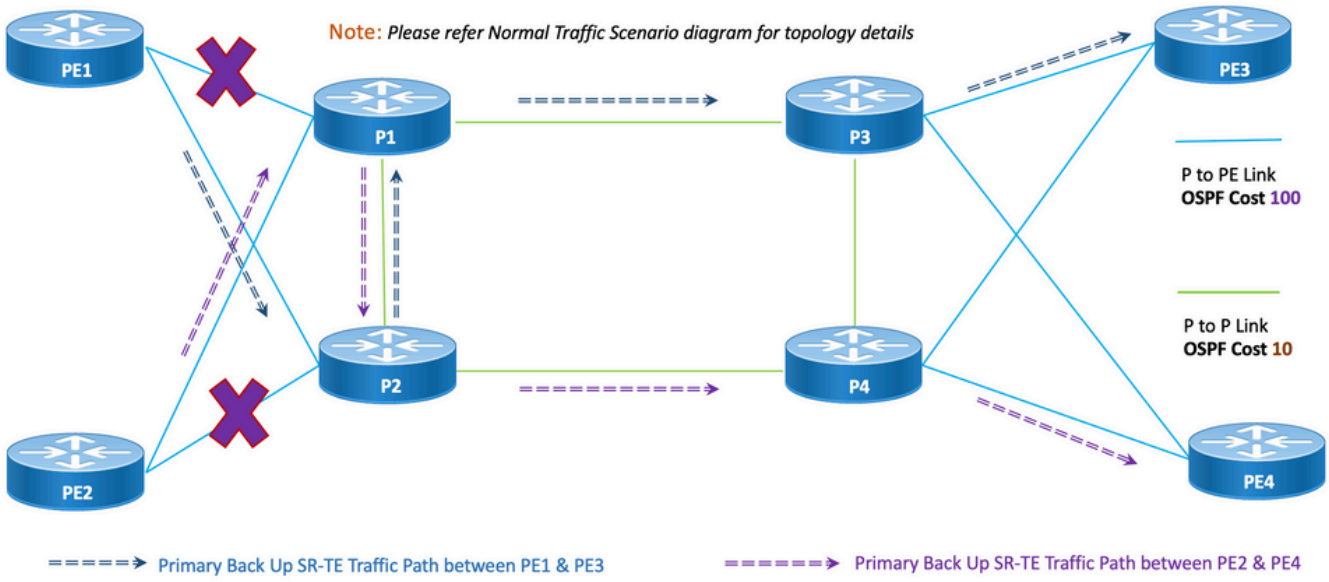
```
    !

   !

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

    explicit segment-list <SIDLIST1>

    !

   !



  !

 !

 !

!
```

8.6.4 . Scénario de basculement de liaison double

Il s'agit du scénario de défaillance de liaison double où la liaison locale entre PE1 et P1 et la liaison locale entre PE2 et P2 échoue. Le trafic en provenance de PE1 fait un détour via les noeuds P2 et P1 principaux et le trafic en provenance de PE2 fait un détour via les noeuds P1 et P2 principaux.

Ils sont gérés par l'administrateur via la liste de segments <SIDLIST2> respective de PE1 et PE2 qui forment les chemins de sauvegarde secondaires entre les noeuds PE1 et PE3 et PE2 et PE4 respectivement.

Figure 14. Scénario de basculement de liaison double



Disparité : En cas de défaillance de liaison double, le nombre de liaisons communes partagées est un (1), comme indiqué dans la topologie mentionnée précédemment.

8.6.4.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés du protocole OSPF/SR-TE pour les noeuds PE1 et PE2, comme indiqué ici :

> **Note**: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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>
     !
    !


   !
  !
```

!

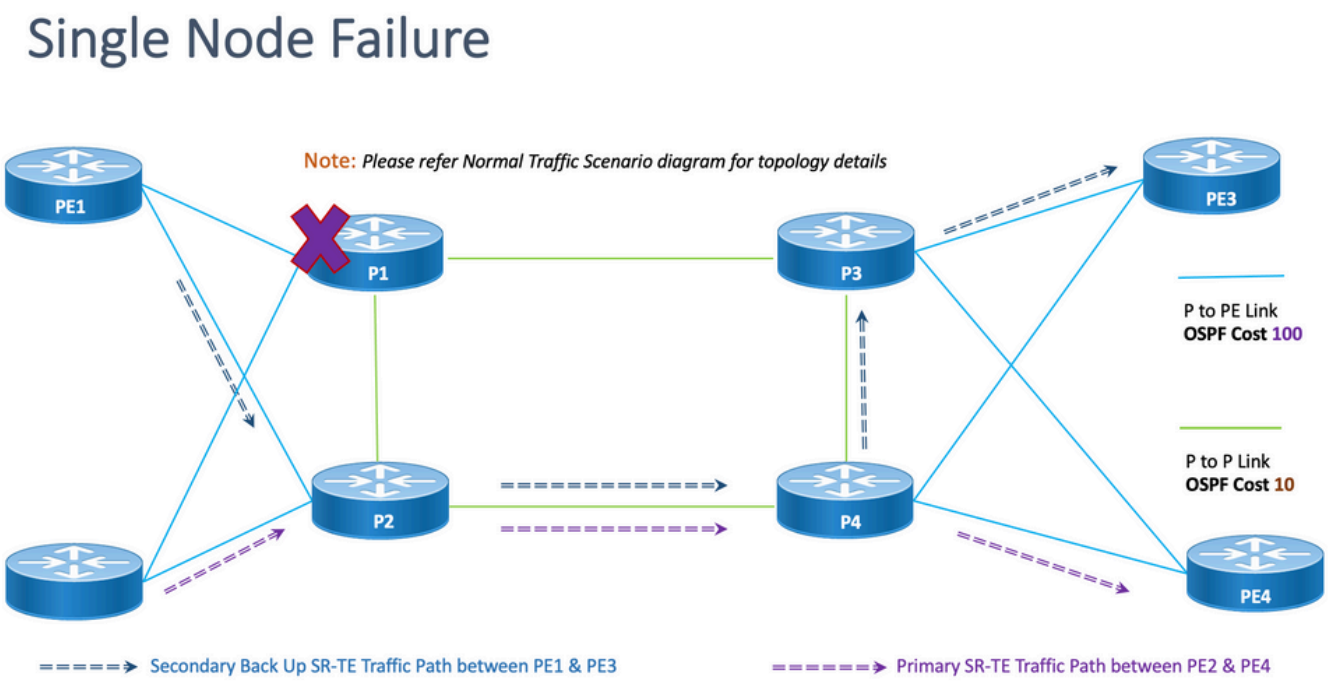
!

8.6.5 . Scénario de basculement de noeud unique

Il s'agit du scénario de défaillance d'un noeud unique où le noeud P1 tombe en panne et où le trafic prend un détour via les noeuds P2 et P4 principaux. Cette opération est administrativement pilotée via la liste de segments <SIDLIST3> qui constitue le chemin de sauvegarde secondaire entre les noeuds PE1 et PE3.

Cependant, le trafic entre PE2 et PE4 reste le même que le chemin principal, comme illustré dans cette topologie.

Figure 15. Scénario de basculement de noeud unique



Disparité : En cas de défaillance d'un noeud unique, le nombre de liaisons communes partagées est un (1), comme indiqué dans la topologie mentionnée précédemment.

8.6.5.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés du protocole OSPF/SR-TE pour les noeuds PE1 et PE2, comme indiqué :

> **Note**: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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>
```

!

!

!

!

!

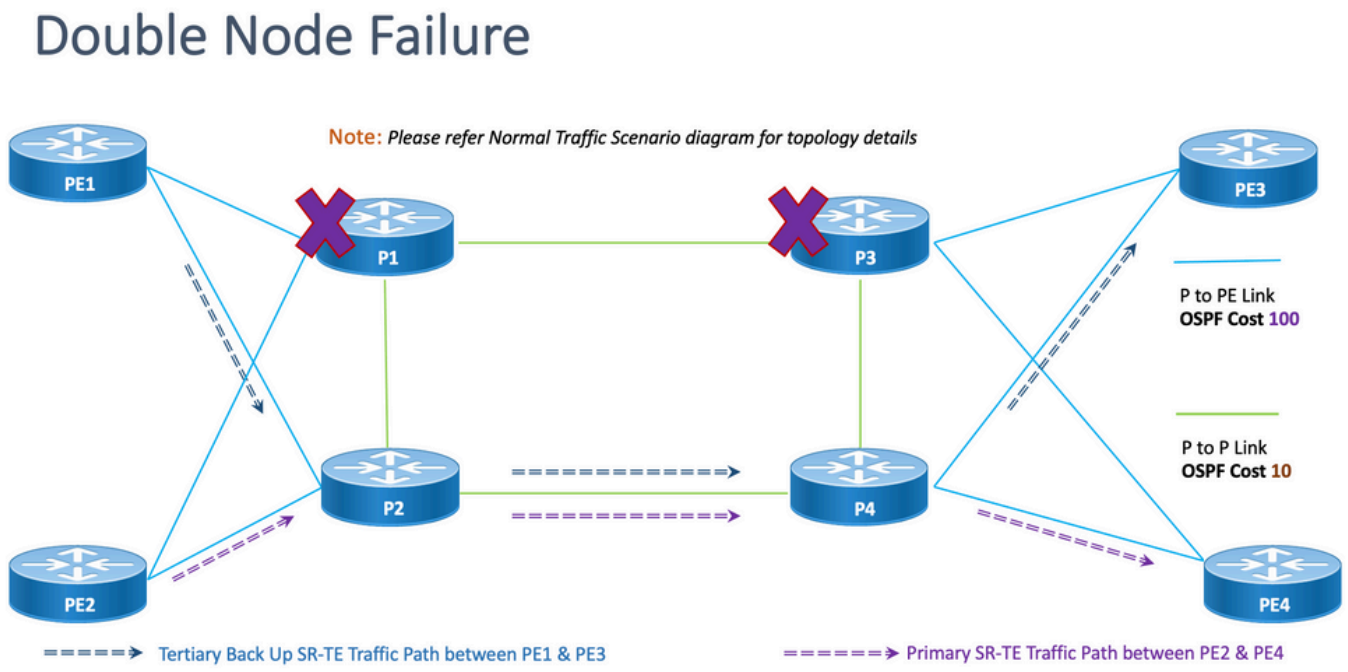
!

8.6.6 . Scénario de basculement de noeud double

Il s'agit du scénario de défaillance de deux noeuds où les noeuds P1 et P3 échouent et où le trafic prend un détour par les noeuds P2 et P4 principaux. Cette opération est administrativement pilotée via la liste de segments <SIDLIST3> qui constitue le chemin de sauvegarde secondaire entre les noeuds PE1 et PE3. Puisque les chemins explicites sont définis uniquement pour les 2 scénarios mentionnés précédemment, ici le chemin IGP dynamique forme le chemin de sauvegarde tertiaire et assume le rôle de routage du trafic via les noeuds P2 et P4.

Cependant, le trafic entre PE2 et PE4 reste le même que le chemin principal, comme illustré dans cette topologie.

Figure 16. Scénario de basculement de noeud double.



Disparité : En cas de défaillance d'un double noeud, le nombre de liaisons communes partagées est un (1), comme indiqué dans cette topologie.

8.6.6.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés du protocole OSPF/SR-TE

pour les noeuds PE1 et PE2, comme indiqué :

> **Note**: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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: Les modèles de configuration OSPF des routeurs PE1 et PE2 sont similaires au scénario 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. Présentation de la conception BGP/RR

Le protocole BGP (Border Gateway Protocol) est le protocole qui prend les décisions de routage principales sur Internet. Il tient à jour une table de réseaux IP ou de préfixes qui désignent l'accessibilité du réseau parmi les systèmes autonomes (AS). Il est décrit comme un protocole à vecteur de chemin. Le protocole BGP n'utilise pas de métriques IGP (Interior Gateway Protocol) traditionnelles, mais prend des décisions de routage en fonction du chemin, des politiques réseau et/ou des ensembles de règles. Pour cette raison, il est plus approprié de l’appeler protocole de capacité de portée qu’un protocole de routage.

MP-BGP peut être utilisé pour propager les préfixes IPv4, IPv6, VPNv4, VPNv6, EVPN et d'état de liens sur le réseau. Ceci est fait avec une configuration de réflecteur de route qui forme les voisins iBGP avec les périphériques Core, d'agrégation, d'accès et SR-PCE.

Grâce au RR, les préfixes appris par BGP sont propagés en interne via iBGP. Les routes BGP ne sont jamais redistribuées dans les IGP. Les réflecteurs de route sont totalement isolés du plan de données et sont dédiés à des fins de plan de contrôle.

8.7.1 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés pour BGP/RR, comme indiqué :

```
# 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 Neighborship with RR
  maximum-prefix <PREFIX> <PERCENT> warning-only
 !
 address-family ipv4 rt-filter
 !

neighbor <RR1-Loopback>          Neighborship with RR1 using the above neighbor group
 use neighbor-group <RR-EVPN>

neighbor <RR2-Loopback>          Neighborship 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 Neighborship with PE
  route-reflector-client
  !
 address-family ipv4 rt-filter
 !



 neighbor <PE1-Loopback>         Neighborship with PE1 using the above neighbor group
 use neighbor-group <PE-EVPN>
```

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

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

8.8. Présentation de la conception des services

Cette sous-section décrit le service de superposition EVPN VPWS, ainsi que la représentation de la pile d'étiquettes prise en charge et des modèles de configuration.

L'EVPN-VPWS est une solution de plan de contrôle BGP pour les services point à point. Il implémente les techniques de signalisation et d'encapsulation qui établissent une instance EVPN entre deux PE. Il peut transférer le trafic d'un réseau à un autre sans recherche MAC. L'utilisation d'EVPN pour VPWS élimine la nécessité de signaler les PW à segment unique et multisegment pour les services Ethernet point à point. La technologie EVPN-VPWS fonctionne sur le coeur IP et MPLS ; le coeur IP prend en charge le coeur BGP et MPLS pour la commutation de paquets entre les points d'extrémité.

8.8.1 . Représentation de la pile d'étiquettes

Le service vise à prendre en charge jusqu'à 5 à 6 étiquettes SR, y compris les étiquettes de transport SR, les étiquettes EVPN et les étiquettes FAT pour l'équilibrage de charge. Il s'agit du nombre maximal d'étiquettes analysées dans les **scénarios normaux** où le trafic passe par un chemin principal explicite :

SID1 ADJ
SID2 ADJ
SID3 ADJ
ÉTIQUETTE
EVPN
ÉTIQUETTE DE
FLUX (S=1)

Il s'agit du nombre maximal d'étiquettes analysées dans les **scénarios de basculement** où le trafic circule via le chemin explicite de sauvegarde ou le chemin de sauvegarde dynamique défini par IGP :

SID1 TI-LFA
SID2 TI-LFA
SID3 TI-LFA
ÉTIQUETTE
EVPN
ÉTIQUETTE DE
FLUX (S=1)

8.8.2 . Modèles de configuration

Cette sous-section contient les modèles de configuration appropriés pour EVPN-VPWS, comme indiqué :

```
# 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>

  !
```

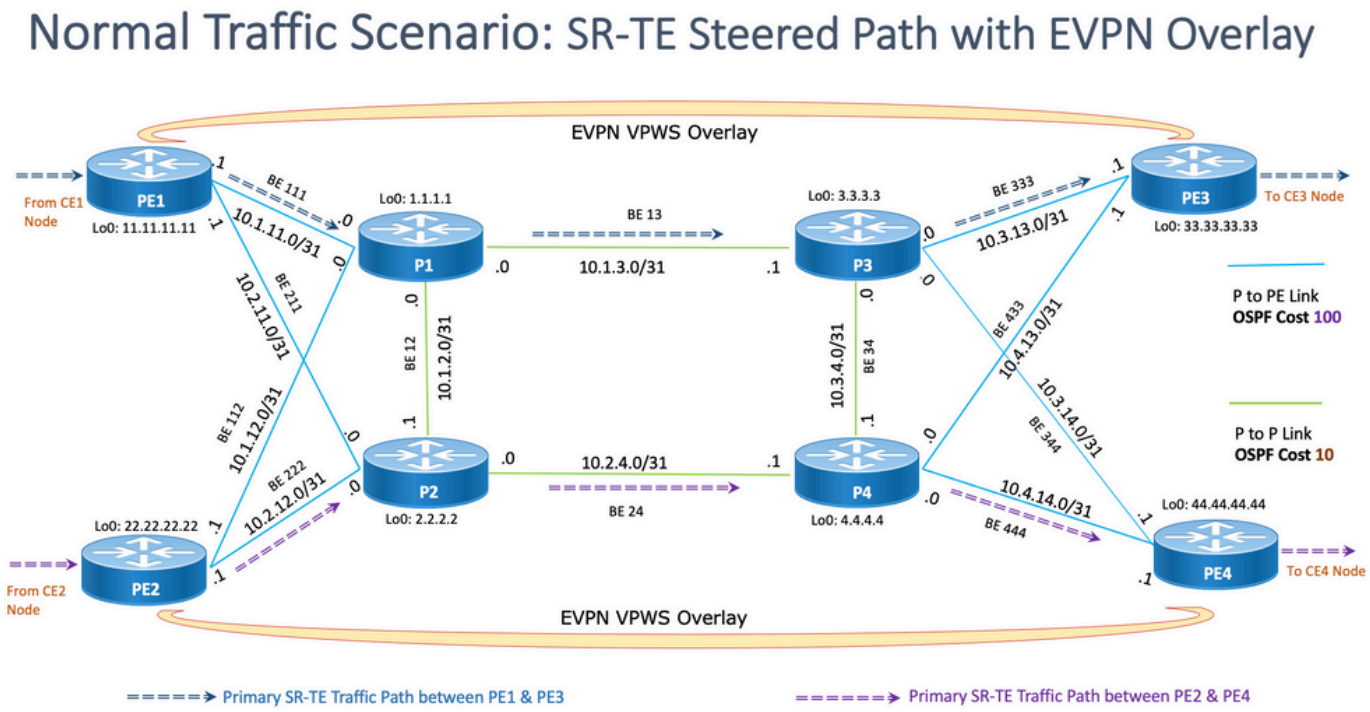
9. Exemples de commandes Configuration et Show

Cette dernière section contient les commandes show et de configuration pertinentes des noeuds

PE pour le scénario de trafic normal uniquement. Ils sont capturés ici en fonction des paramètres donnés dans cette figure comme référence qui aide à comprendre les modèles de configuration expliqués dans les sections précédentes.

9.1. Exemple de configuration sur les noeuds PE

Figure 17. Topologie avec paramètres de configuration.




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

```
#show run router ospf
```

```
router ospf CORE
 distribute link-state                    Command to distribute OSPF database into SR-TE
database
 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                     Command to distribute OSPF database into SR-TE
database
 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. Commandes show pertinentes sur les noeuds 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
```

BGP fonctionne en mode AUTONOME.

```
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
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- 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
- Support et documentation techniques - Cisco Systems