Guida dettagliata alla progettazione ed esempi di configurazione della policy SR-TE Explicit-Path con EVPN VPWS, IOS XR release - 7.5.x

Sommario

Introduzione

Questo documento descrive la guida di progettazione dettagliata con descrizioni tecniche basate sui requisiti di XYZ Networks e fornisce anche un modello di configurazione di basso livello e la configurazione per i casi di utilizzo della policy SR-TE (Segment Routing Traffic Engineering) a percorso esplicito con VPN (EVPN) Virtual Private Wired Service (VPWS).

1. Premesse

1.1. Fuori dal campo di applicazione

Questo documento non copre i requisiti delle policy SR-TE 'on-demand' centralizzate che utilizzano il controller XTC, EVPN ELAN e così via, ma si concentra solo sulle policy SR-TE basate sul nodo headend con la sovrapposizione EVPN VPWS.

1.2. Presupposto

Il lettore di questo documento deve conoscere i concetti di IP/MPLS e Ethernet insieme alle tecnologie di routing dei segmenti e progettazione del traffico.

1.3. Ambito tecnico

Il campo di applicazione tecnico principale del presente documento è limitato a:

- OSPF con TI-LFA FRR
- Regole SR-TE controllate (distribuite) dall'headend
- Percorso primario esplicito e percorsi di failover dinamici basati su IGP
- VPWS VPN single-homed

I modelli di configurazione riportati in questo documento sono denominati Cisco IOS®-XR 7.5.x.

1.4. Riepilogo del documento

Tabella 1. Sezioni di documenti

Tipo di argomento	Nome argomento	Numero sezione
Introduzione	Premesse	1
Requisito	Requisiti utente	2
Panoramica della tecnologia	Ciclo dei segmenti	3
	Panoramica di SR-TE	4
	TI-LFA FRR	5
	Sovrapposizione EVPN	6
	BoB e load balancing	7
Modelli di configurazione	La soluzione di progettazione completa	8
Esempi di comandi e	Comandi Di Esempio Per La Configurazione E L'Attivazione Del Comando Show	9

Requisito

2. Requisiti dell'utente

2.1. Sintesi del fabbisogno

Il provider di servizi XYZ Networks ha l'esigenza di creare una rete ecologica sul campo tramite i dispositivi Cisco NCS 5500.

Lo scopo è trasportare un flusso di dati multicast (voce, video) come servizio su una rete di trasporto di layer 2 con determinati requisiti, uno di questi è quello di configurare i percorsi del traffico attraverso la rete.

Hanno preferito SR per le etichette di trasporto, SR-TE per la progettazione del traffico e EVPN come sovrapposizione per fornire le etichette di servizio.

2.2. Componenti usati

L'utente XYZ ha fatto convergere i router e le schede di linea dell'NCS 5500:

Tabella 2. Requisiti hardware del progetto

Nodi PE	PID
Chassis	NCS-5504
MPA/LC che connettono i nodi IP	NC55-36X100G-A-SE
MPA/LC che collegano i nodi CE	NC55-36X100G-A-SE
Nodi IP	PID
Chassis	NCS-5508
MPA/LC che collegano altri nodi IP	NC55-36X100G-A-SE
MPA/LC che connettono nodi	NC55-36X100G-A-

PE	SE

In questa sezione viene fornita una panoramica delle tecnologie da utilizzare con brevi descrizioni.

Panoramica della tecnologia

3. Instradamento dei segmenti

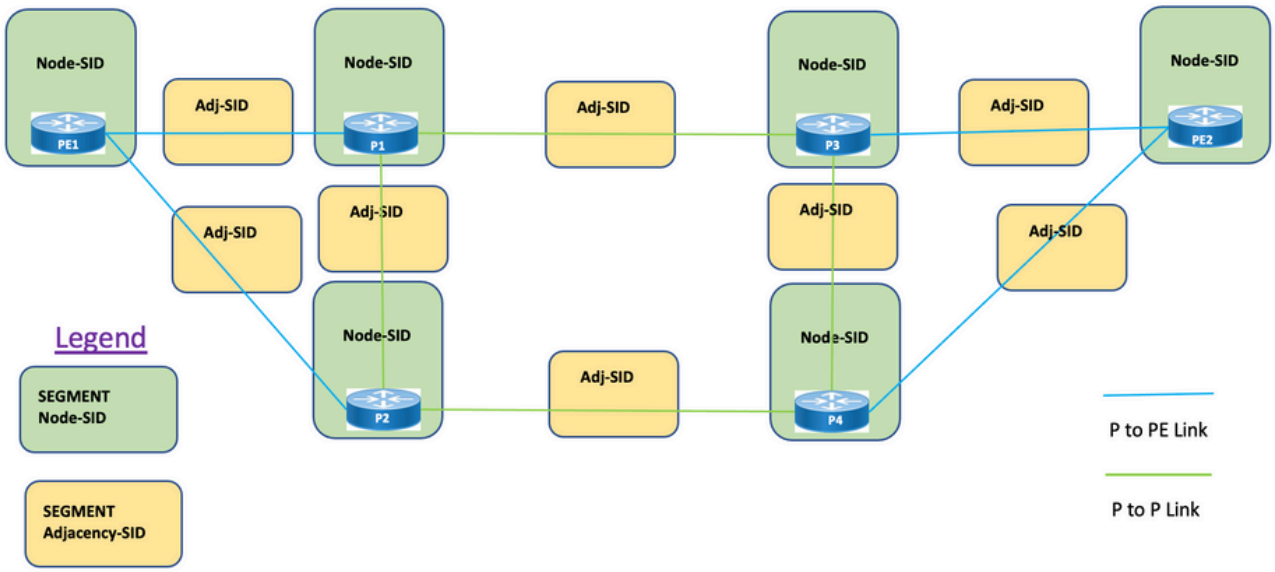
3.1 Che cos'è il ciclo di segmenti?

Il Segment Routing è l'ultima tecnologia MPLS avanzata in fase di sviluppo per sostituire i protocolli LDP e RSVP-TE tradizionali con l'introduzione della distribuzione di etichette e la progettazione del traffico sotto un unico ombrello, e per realizzare questo obiettivo solo tramite i protocolli IGP/BGP allo stato del collegamento.

Il routing dei segmenti è un metodo per inoltrare i pacchetti sulla rete basato sul paradigma di routing di origine. L'origine sceglie un percorso e lo codifica nell'intestazione del pacchetto come un elenco ordinato di segmenti. I segmenti sono un identificatore per qualsiasi tipo di istruzione. Ad esempio, i segmenti della topologia identificano l'hop successivo verso una destinazione. Ciascun segmento è identificato dall'ID segmento (SID), che è costituito da un numero intero a 20 bit senza segno.

3.2. Identificativi dei segmenti

Figura 1. SID nodo SR e SID adiacenti



Segmenti: IGP (Interior Gateway Protocol) distribuisce due tipi di segmenti: segmenti di prefisso e segmenti di adiacenza. A ogni router (nodo) e collegamento (adiacenza) è associato un identificatore di segmento (SID).

SID prefisso: un segmento di prefisso è un segmento globale, quindi un SID prefisso è globalmente univoco all'interno del dominio di routing del segmento, come mostrato nella Figura 1. Un SID di prefisso è associato a un prefisso IP. Il prefisso SID viene configurato manualmente dall'intervallo di etichette SRGB (Segment Routing Global Block) ed è distribuito da IS-IS o OSPF. Il segmento del prefisso indirizza il traffico sul percorso più breve verso la sua destinazione.

- Utilizza il blocco globale SR (SRGB)
- SRGB annunciato con TLV funzionalità router - Nella configurazione, Prefix-SID può essere configurato come valore assoluto o indice
- Nell'annuncio del protocollo, Prefix-SID è sempre codificato come indice univoco globale. L'indice rappresenta un offset dalla base SRGB, numerazione a base zero, ovvero 0 è il primo indice. Ad esempio, indice 1 à SID è 16.000 + 1 = 16.001

SID nodo: un SID nodo è un tipo speciale di SID prefisso che identifica un nodo specifico. Viene configurato nell'interfaccia di loopback con l'indirizzo di loopback del nodo come prefisso. Un segmento di prefisso è un segmento globale, quindi un SID di prefisso è globalmente univoco all'interno del dominio di routing del segmento.

In altre parole, il segmento Node è un segmento Prefix associato a un prefisso host che identifica un nodo.

- Equivale a un prefisso ID router, che identifica un nodo
- Node-SID è Prefix-SID con N-flag impostato nell'annuncio
- Per impostazione predefinita, ogni prefix-SID configurato è un node-SID
- Prefix-SID configurabile come IS-IS in base a 'normal', ovvero senza SID di nodo

SID adiacenza: un segmento adiacente è identificato da un'etichetta denominata SID adiacente, che rappresenta una adiacenza specifica, ad esempio un'interfaccia di uscita, a un router adiacente. Il SID adiacente è distribuito da IS-IS o OSPF. Il segmento adiacente dirige il traffico verso una adiacenza specifica. Poiché un segmento adiacente è un segmento locale, il SID adiacente è univoco a livello locale rispetto a un router specifico.

- Importante a livello locale
- Allocazione automatica per ogni adiacenza
- Sempre codificato come valore assoluto (non indicizzato)

SID di binding o BSID: è un SID significativo a livello locale associato al criterio SR. Aiuta a indirizzare i pacchetti nella relativa policy SR associata. Il segmento di binding è un segmento locale che identifica una politica SR-TE. Ogni criterio SR-TE è associato a un ID segmento di binding (BSID).

Il BSID è un'etichetta locale allocata automaticamente per ogni criterio SR-TE quando viene creata un'istanza del criterio SR-TE. Il BSID può essere utilizzato per indirizzare il traffico nella policy SR-TE e oltre i confini del dominio, creando policy SR-TE end-to-end senza interruzioni.

4. Panoramica di SR-TE

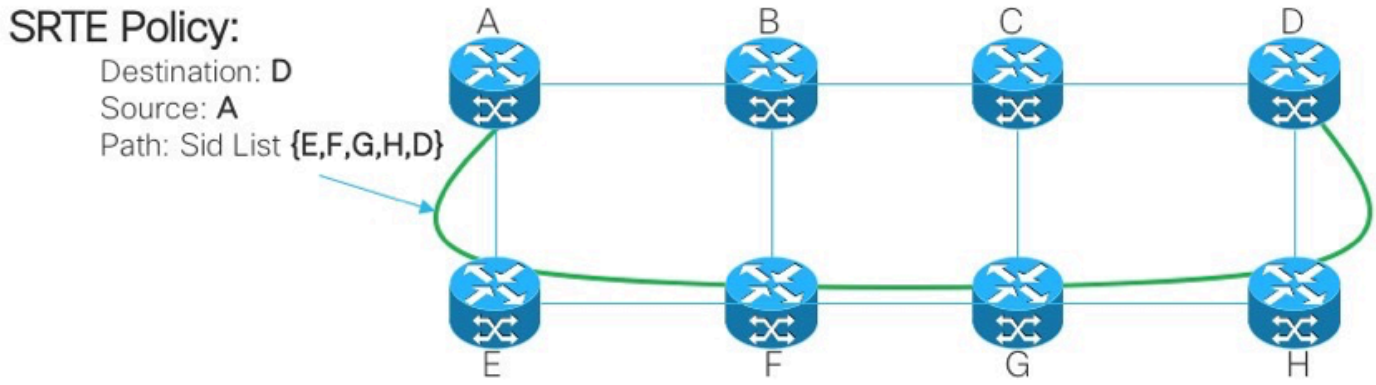
4.1 Che cos'è SR-TE?

La tecnologia SR-TE (Segment Routing Traffic Engineering) trasforma il semplice meccanismo di routing all'origine senza stato della SR a un livello avanzato per programmare e indirizzare il traffico di dati attraverso percorsi predefiniti che evitano la congestione e forniscono percorsi alternativi, proprio come una mappa del traffico live express way.

Ciò si ottiene quando si configurano in modo amministrativo criteri definiti tramite una combinazione di vari vincoli che programmano i percorsi primari e di backup dai nodi di origine a quelli di destinazione. Il controller può essere centralizzato (SDN) o distribuito (headend), a seconda dei requisiti di rete.

Si consideri la topologia illustrata nella Figura 2. Si supponga che il costo dei collegamenti sia un valore predefinito e che il percorso più breve per raggiungere D da A sia A-B-C-D, ma il percorso a bassa latenza sia A-E-F-G-H-D. L'operatore può definire il percorso progettato per il traffico in base al requisito (ad esempio, Latenza) ed esprimerlo sotto forma di elenco di ID dei segmenti (A, E, F, G, H, D). A differenza di RSVP-TE, lo stato di questo criterio viene mantenuto solo sul router A e non sull'intero router attraversato dai pacchetti (ossia E, F, G e H).

Figura 2. Esempio di percorso definito dall'amministratore SR-TE



4.2. Politica SR-TE

Il routing dei segmenti per la progettazione del traffico (SR-TE) utilizza una 'policy' per indirizzare il traffico attraverso la rete. Un percorso dei criteri SR-TE viene espresso come elenco di segmenti che specifica il percorso, denominato elenco ID segmento (SID). Ogni segmento è un percorso end-to-end tra l'origine e la destinazione e indica ai router della rete di seguire il percorso specificato anziché il percorso più breve calcolato dall'IGP. Se un pacchetto viene indirizzato in un criterio SR-TE, l'elenco SID viene indirizzato sul pacchetto dall'headend. Il resto della rete esegue le istruzioni incorporate nell'elenco SID.

Una policy SR-TE viene identificata come un elenco ordinato (headend, colore, end-point):

- Headend - Dove viene creata l'istanza della policy SR-TE

- Colore: valore numerico che distingue due o più criteri rispetto alle stesse coppie di nodi (headend - endpoint).
- Endpoint: la destinazione della policy SR-TE
- Ogni criterio SR-TE ha un valore di colore. Ogni criterio tra le stesse coppie di nodi richiede un valore di colore univoco.

Una regola SR-TE è configurata con uno o più percorsi candidati che includono percorsi primari e di backup.

Ad esempio, il percorso primario del criterio può essere definito in modo esplicito con SID adiacenti e, in caso di scenari di errore, il percorso di backup può essere un percorso dinamico gestito dalla metrica IGP.

5. TI-LFA FRR

5.1. Panoramica

TI-LFA (Topology Independent Loop-Free Alternate) è una funzione che protegge collegamenti, nodi e SRLG. È semplice da configurare; sono necessarie solo due linee di configurazione per implementare una semplice configurazione TI-LFA nel router. Non sono necessarie modifiche ai protocolli esistenti utilizzati nel router. La Figura 3. mostra il percorso del traffico primario e il percorso di backup precalcolato da TI-LFA per scenari di errore del collegamento locale e di errore del nodo.

Figura 3. Scenario di failover collegamento LFA TI

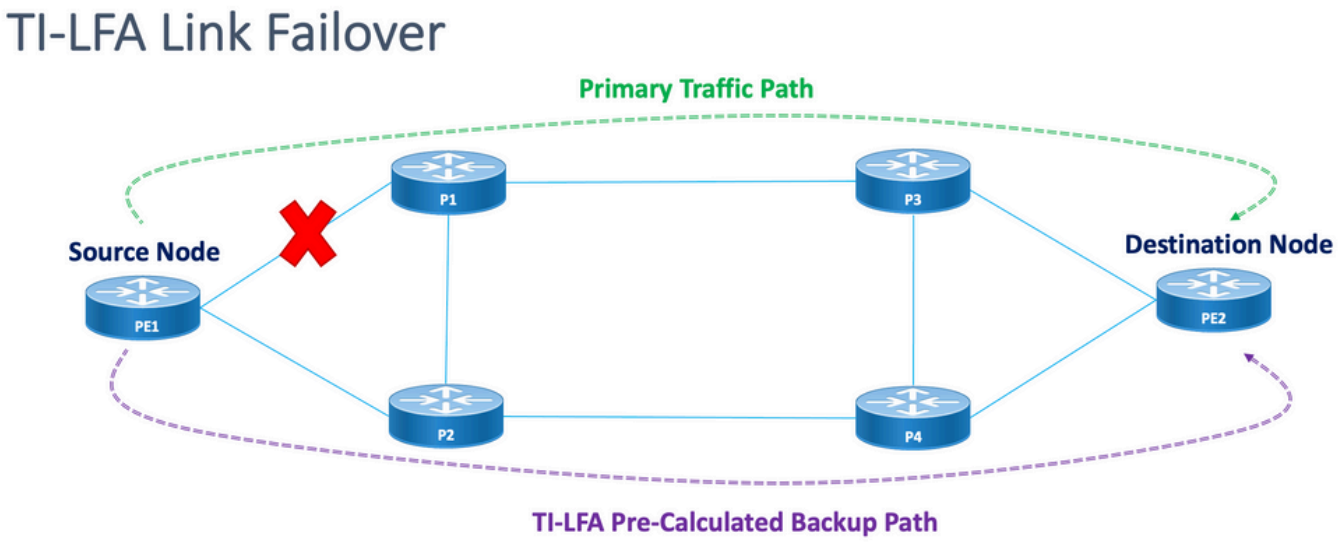
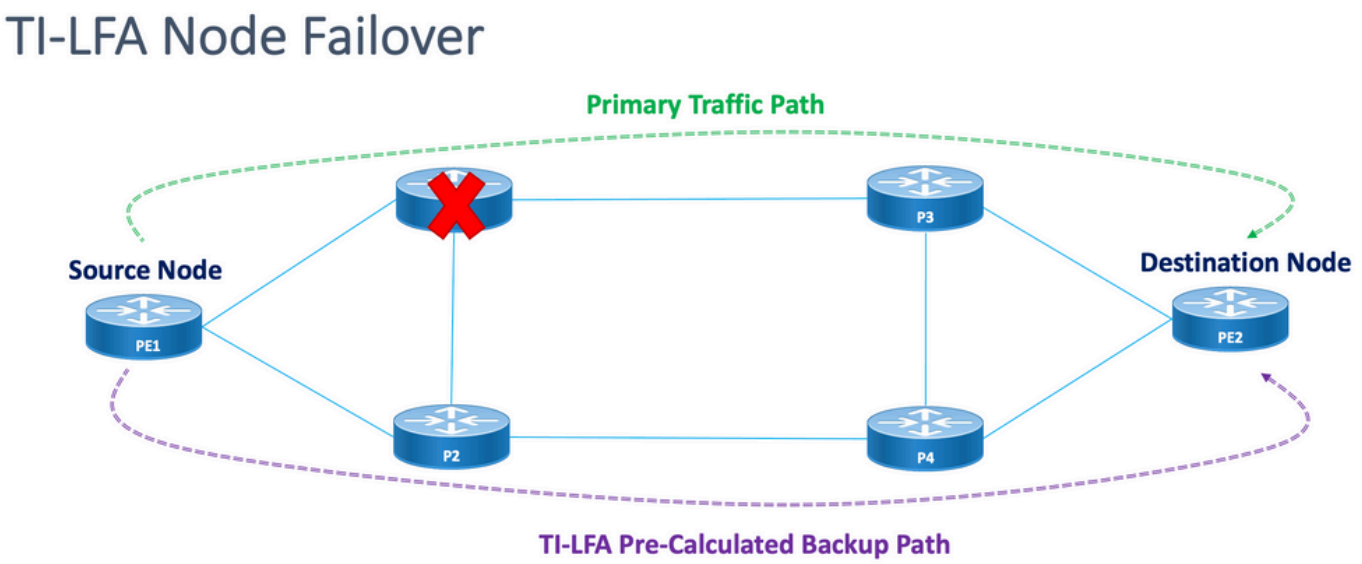


Figura 4. Scenario di failover del nodo TI LFA



Ogni nodo e percorso protetto dispone di un percorso di backup precalcolato che può essere abilitato rapidamente. Il tempo di convergenza per un tracciato protetto è di 50 millisecondi o meno. Ciò significa che anche le applicazioni più sensibili alla latenza o alla perdita di pacchetti possono funzionare senza interruzioni in caso di guasto di un nodo o di un collegamento. TI-LFA calcola il percorso di backup e rimuove temporaneamente il collegamento o il nodo protetto dal database. In seguito, viene calcolato il percorso di backup con il percorso più breve. Ciò garantisce che il percorso di backup abbia il costo metrico più basso possibile e che venga evitato il percorso protetto. In caso di errore, per il traffico viene utilizzato un tunnel progettato per il traffico che segue il percorso di backup. Un elenco di etichette di correzione determina il percorso dei pacchetti che richiedono un nuovo percorso verso la destinazione. Un elenco di etichette di correzione è un normale stack di etichette, ma viene utilizzato solo quando si verifica un errore nel percorso protetto.

5.2. Impatto del metodo di rilevamento degli errori sulle FRR

Fast Reroute for SR-TE traffic-engineered path è configurato come mezzo per commutare il traffico in caso di scenari di failover dal percorso principale ai percorsi di backup entro il più vicino possibile a 50 msec. La funzione fast reroute è configurata con il protocollo IGP (OSPF/ISIS). Il tempo di convergenza dipende dal metodo con cui si verifica il rilevamento degli errori del collegamento. Nel caso di un taglio di fibra, il rilevamento è immediato e la possibilità di ottenere una convergenza inferiore a 50 msec è elevata. Tuttavia, se il rilevamento degli errori del collegamento deve essere eseguito dal BFD con un intervallo di 15 msec (moltiplicatore x3). Il tempo di convergenza è per lo più superiore a 50 msec.

5.3. Prevenzione del microloop con SR

I microloop sono brevi loop di pacchetto che si verificano nella rete dopo una modifica della topologia (eventi di collegamento non attivo, collegamento attivo o modifica metrica). I microloop sono causati dalla convergenza non simultanea di nodi diversi nella rete. Se i nodi convergono e inviano traffico a un nodo adiacente che non ha ancora effettuato la convergenza, è possibile che il traffico tra questi due nodi venga ripetuto, con conseguente perdita, jitter e pacchetti non

ordinati.

La funzione di prevenzione dei microloop di routing dei segmenti rileva se i microloop sono seguiti da una modifica della topologia. Se un nodo calcola che un microloop può verificarsi sulla nuova topologia, crea un percorso di criteri SR-TE senza loop verso la destinazione utilizzando un elenco di segmenti. Dopo la scadenza del timer di ritardo dell'aggiornamento RIB, il criterio SR-TE viene sostituito con percorsi di inoltro regolari. È disponibile un timer predefinito per il ritardo di aggiornamento RIB che viene gestito da TI-LFA.

6. Sovrapposizione EVPN

EVPN è una tecnologia inizialmente progettata per i servizi multipoint Ethernet, con funzionalità di multi-homing avanzate, con l'utilizzo di BGP per distribuire informazioni sulla raggiungibilità dell'indirizzo MAC sulla rete MPLS, mentre offre le stesse caratteristiche operative e di scalabilità delle VPN IP alle VPN L2P. Attualmente, oltre alle applicazioni DCI ed E-LAN, la famiglia di soluzioni EVPN fornisce una base comune per tutti i tipi di servizi Ethernet, che includono E-LINE ed E-TREE, nonché scenari di routing e bridging di centri dati. EVPN offre inoltre opzioni per combinare i servizi L2 e L3 nella stessa istanza.

EVPN è una soluzione di nuova generazione che fornisce servizi multipoint Ethernet su reti MPLS. EVPN opera in contrasto con il servizio VPLS (Virtual Private LAN Service) esistente che consente l'apprendimento MAC basato sul control plane BGP nel core. In EVPN, i PE che partecipano alle istanze EVPN apprendono le route MAC degli utenti in Control-Plane con l'utilizzo del protocollo MP-BGP.

EVPN offre una serie di vantaggi, come indicato:

- Ridondanza per flusso e bilanciamento del carico
- Provisioning e funzionamento semplificati
- Inoltro ottimale
- Convergenza rapida
- Scalabilità degli indirizzi MAC
- Soluzioni multifornitore in base alla standardizzazione IETF

Gli indirizzi MAC appresi su un dispositivo devono essere appresi o distribuiti sugli altri dispositivi di una VLAN. La funzione di apprendimento MAC del software EVPN consente la distribuzione degli indirizzi MAC appresi su un dispositivo agli altri dispositivi collegati a una rete. Gli indirizzi MAC vengono appresi dai dispositivi remoti con l'uso di BGP.

In queste sezioni vengono descritti alcuni dei vantaggi e dei tipi di percorso di EVPN in generale e vengono descritti i componenti specifici della soluzione applicati alla progettazione dei servizi di rete XYZ.

6.1. Vantaggi EVPN

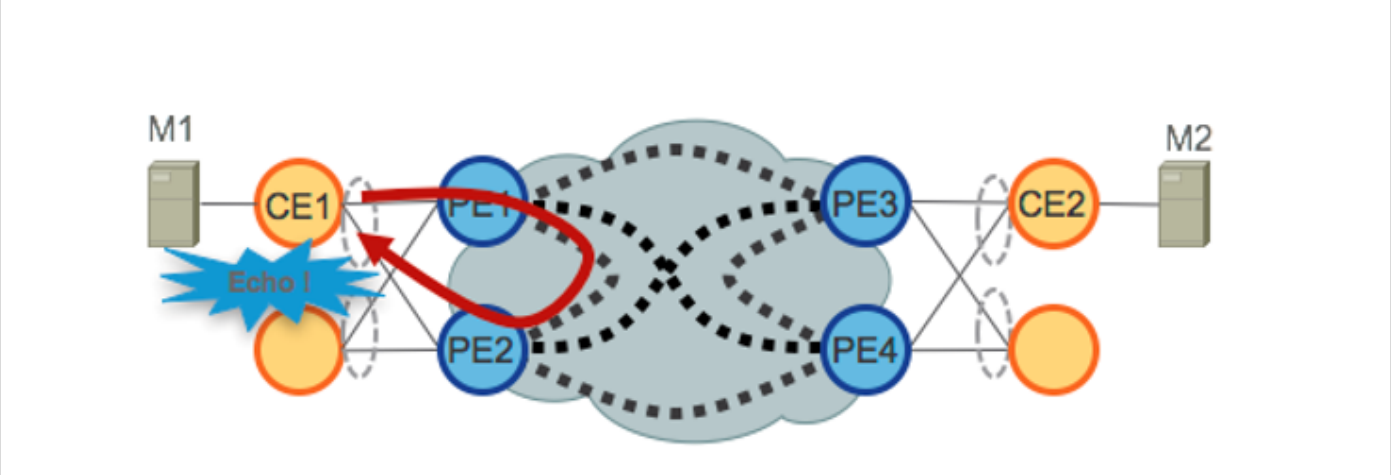
L2VPN e L3VPN non solo forniscono servizi sotto un unico ombrello con l'aiuto di vari tipi di route, ma risolvono due limitazioni di lunga data per i servizi Ethernet nelle reti dei provider di servizi:

- Accesso Ethernet multi-homed e all-active
- Rete di provider di servizi: integrazione con la sede centrale o con il centro dati

6.1.1. Accesso Ethernet multi-homed e all-active

Nella figura viene illustrato il limite massimo delle tradizionali soluzioni L2 Multipoint come VPLS.

Figura 5. Accesso tutti attivi EVPN



Quando VPLS viene eseguito nel core, per evitare il loop è necessario che PE1/PE2 e PE3/PE4 forniscano solo la ridondanza Single-Active verso i rispettivi CE. Tradizionalmente, tecniche come mLACP o i protocolli L2 legacy come MST, REP, G.8032 e così via sono state utilizzate per fornire ridondanza di accesso Single-Active.

La stessa situazione si verifica con Hierarchical-VPLS (H-VPLS), in cui il nodo di accesso è responsabile di fornire l'accesso Single-Active H-VPLS da parte di uno pseudofilo spoke (PW) attivo e di backup.

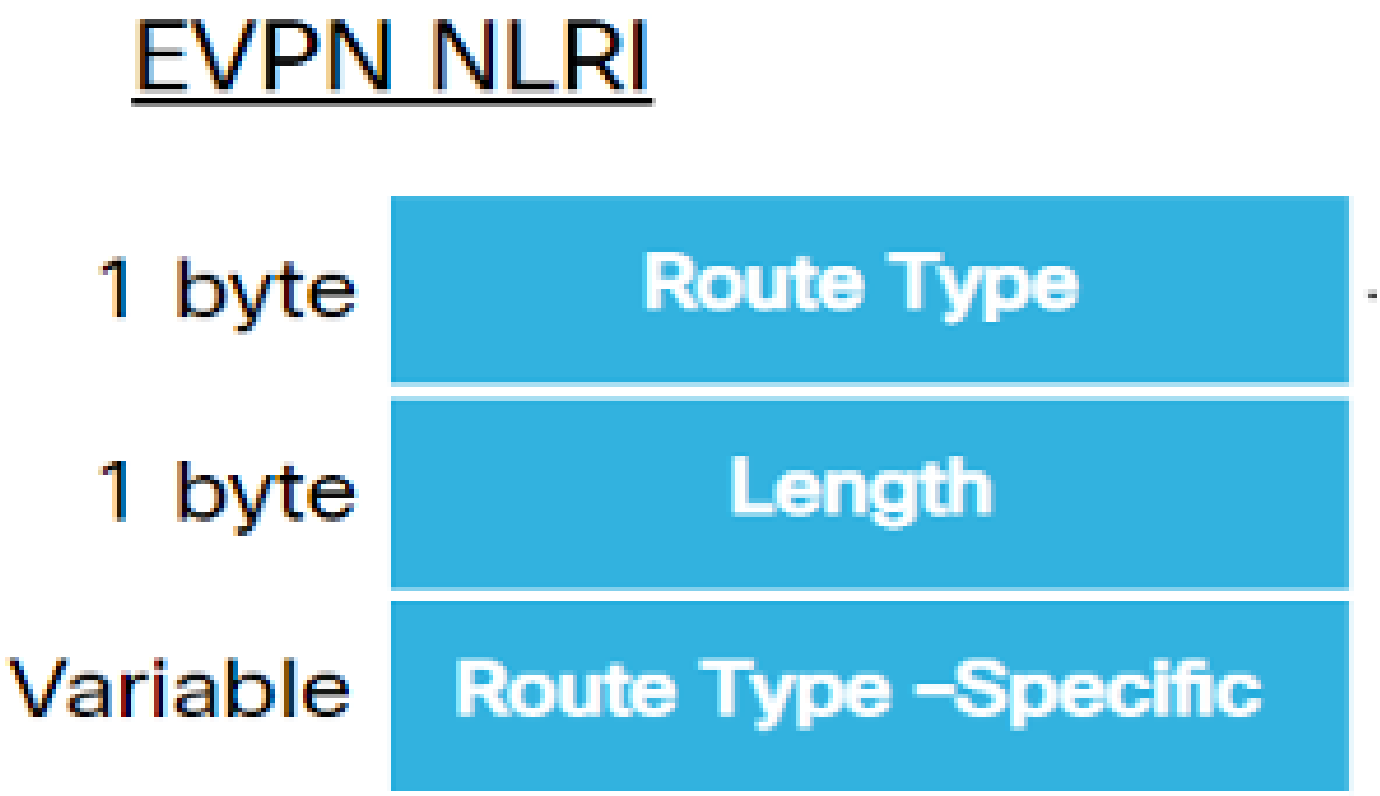
I modelli di ridondanza di accesso completamente attivi non possono essere implementati poiché la tecnologia VPLS non è in grado di impedire loop L2 derivanti dai meccanismi di inoltro utilizzati nel core per determinate categorie di traffico. Il traffico broadcast, unicast sconosciuto e multicast (BUM) proveniente dal CE viene inondato in tutto il core VPLS e viene ricevuto da tutti i PE, che a loro volta lo inondano in tutti i CE collegati. Nell'esempio, PE1 può inondare il traffico BUM da CE1 al core e PE2 può rimandarlo a CE1 quando ricevuto.

EVPN utilizza tecniche Control Plane basate su BGP per risolvere questo problema e abilita modelli di ridondanza di accesso attivo-attivo per l'accesso Ethernet o H-EVPN.

6.2. Tipi di route EVPN

EVPN definisce una nuova NLRI BGP utilizzata per trasportare tutte le route EVPN. EVPN NLRI viene trasportato in BGP con l'uso di estensioni multiprotocollo con un AFI di 25 (L2VPN) e un SAFI di 70. L'annuncio delle funzionalità BGP viene utilizzato per garantire il supporto di EVPN NLRI da parte di due altoparlanti.

Figura 6. EVPN NLRI



I tipi di route EVPN necessari per questa implementazione sono descritti di seguito:

6.2.1. Route di tipo 1 - Ethernet Auto-Discovery (AD) Route

Le route Ethernet Auto-Discovery (AD) vengono pubblicizzate per EVI e per ESI. Queste route vengono inviate per ES. Portano l'elenco delle EVI che appartengono all'ES. Il campo ESI è impostato su zero quando un CE ha una posizione iniziale singola. Questo tipo di route viene utilizzato per il ritiro di massa degli indirizzi MAC, l'aliasing per il bilanciamento del carico e il filtro dell'orizzonte di divisione.

6.2.2. Rotta di tipo 4 - Rotta a segmenti Ethernet

I percorsi dei segmenti Ethernet consentono il collegamento di un dispositivo CE a due dispositivi o PE. Il percorso ES consente il rilevamento di dispositivi PE connessi allo stesso segmento Ethernet, ovvero il rilevamento dei gruppi di ridondanza. Viene inoltre utilizzato per la scelta del server d'inoltro designato (DF, Designed Forwarder).

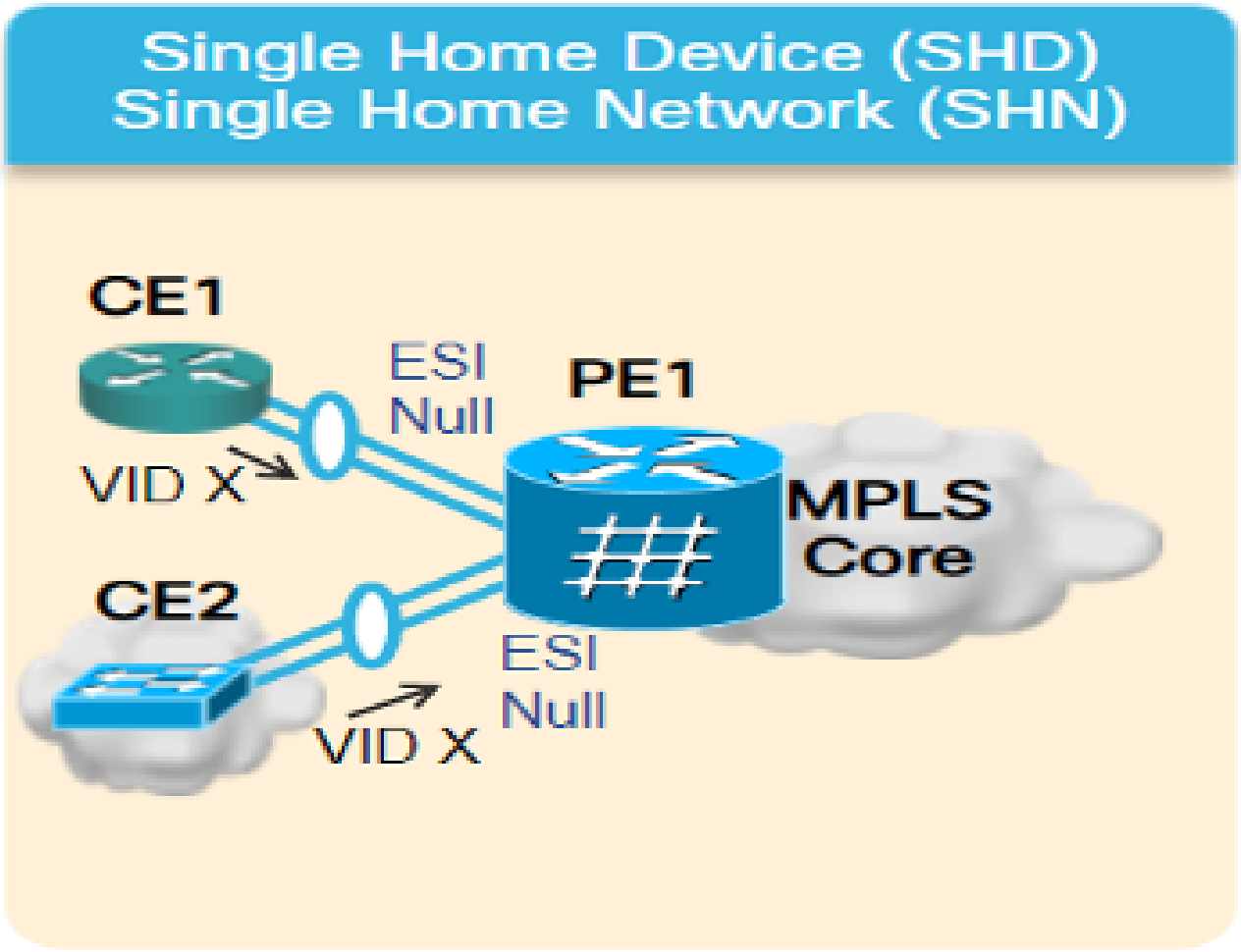
6.3. Connettività host VPN

Sono supportate le seguenti modalità EVPN:

- Single homing - Consente di connettere un dispositivo CE (User Edge) a un dispositivo PE (Provider Edge). In questo valore ESI è null per ogni collegamento PE-CE.
- Multihoming: consente di connettere un dispositivo CE (User Edge) a due o più dispositivi PE (Provider Edge) per fornire connettività ridondante. Non è richiesto alcun collegamento

all'intercalità. Il dispositivo PE ridondante garantisce che non vi siano interruzioni del traffico in caso di guasto della rete. I tipi di multihoming sono:

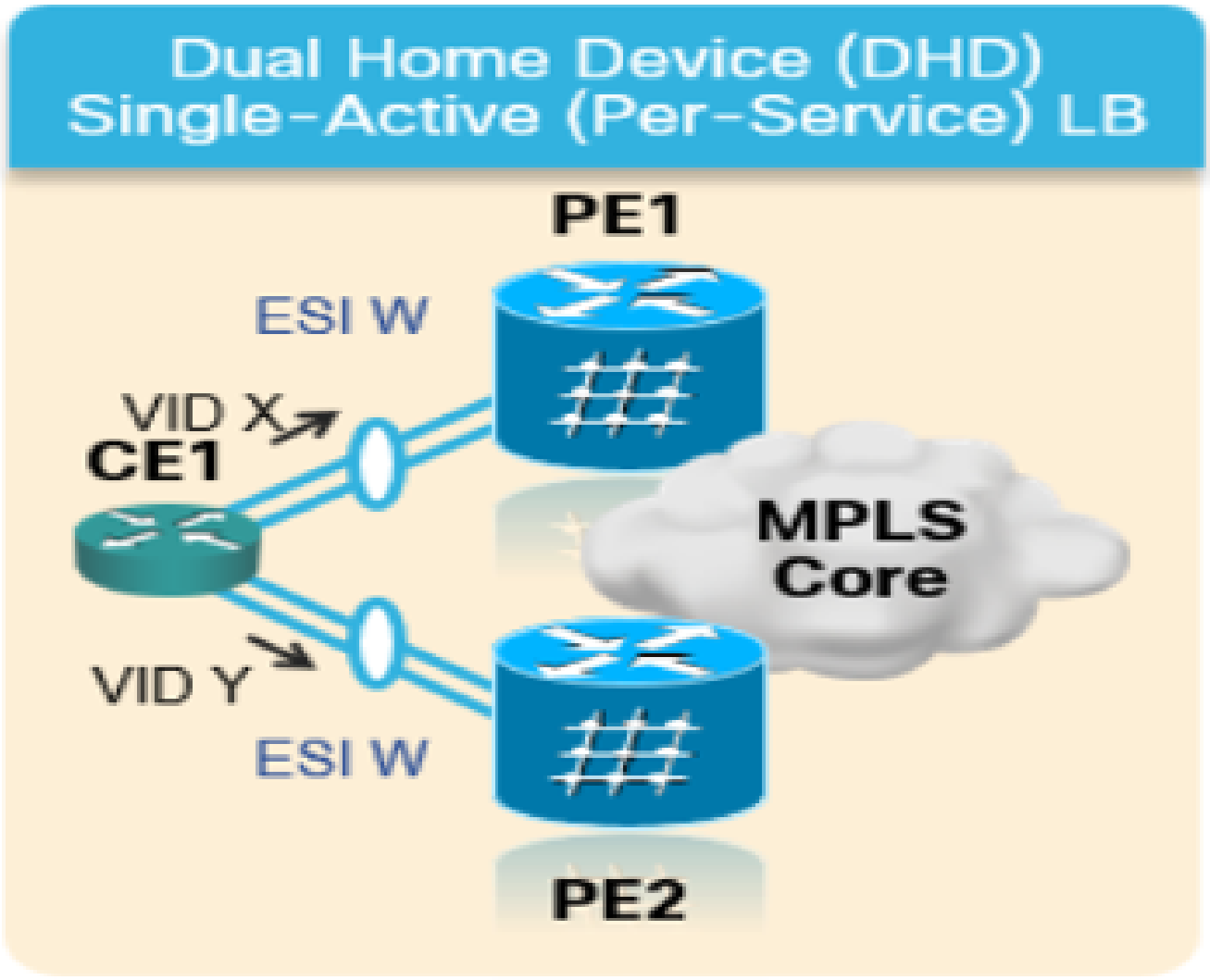
Figura 7. Abitazione singola EVPN



Multihoming - Di seguito sono riportati i tipi di multihoming:

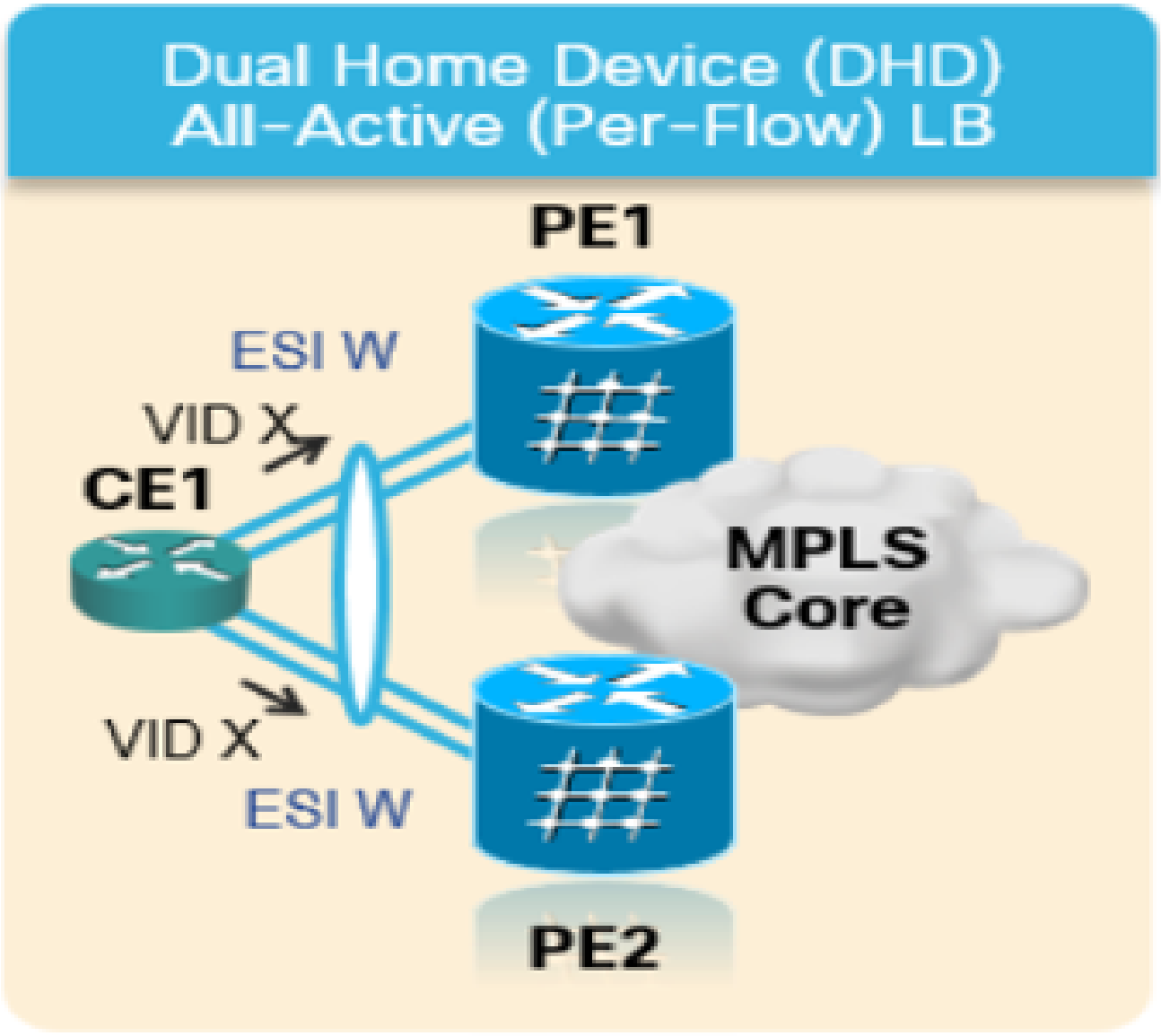
1. Single-Active: in modalità single-active, solo un singolo PE tra un gruppo di PE collegati al segmento Ethernet specifico può inoltrare il traffico da e verso tale segmento Ethernet.

Figura 8. EVPN Single-Active



2. Attivo-Attivo: in modalità attivo-attivo, tutti i PE collegati al segmento Ethernet specifico possono inoltrare il traffico da e verso tale segmento Ethernet.

Figura 9. EVPN Dual Active



7. BoB e bilanciamento del carico

7.1. BFD over Bundle (BoB)

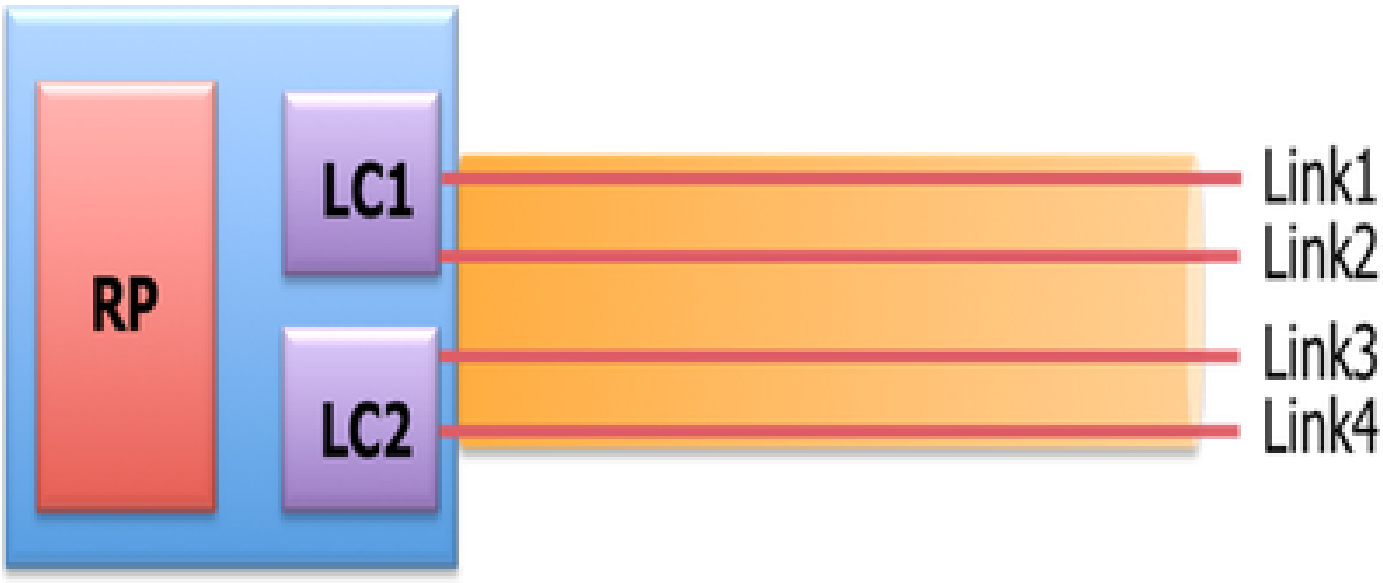
Il rilevamento dell'inoltro bidirezionale (BFD, Bidirectional Forwarding Detection) fornisce un rilevamento a breve durata e a basso sovraccarico degli errori nel percorso tra motori di inoltro adiacenti. Il BFD permette di utilizzare un singolo meccanismo per il rilevamento dei guasti su qualsiasi supporto e a qualsiasi livello di protocollo, con un'ampia gamma di tempi di rilevamento e sovraccarico. Il rilevamento rapido degli errori fornisce una reazione immediata in caso di guasto di un collegamento o di un router adiacente.

In questo modo l'IGP inizierebbe a inoltrare il traffico verso il percorso di backup già calcolato con l'uso di FRR (nel caso di IGP) e PIC (nel caso di BGP).

Nella funzione BFD Over Bundle (BoB), la sessione BFD IPv4 viene eseguita su ciascun membro

del bundle attivo.

Figura 10. Diagramma logico BoB



Bundlemgr considera gli stati BFD, oltre agli stati L1/L2 esistenti, per determinare l'usabilità dei collegamenti tra membri. Lo Stato membro del pacchetto è una funzione di:

Stato L1 (collegamento fisico)

Stato L2 (LACP)

Stato L3 (BFD)

L'agente BFD è ancora in esecuzione sulla scheda di linea. Gli stati BFD dei collegamenti dei membri del bundle sono consolidati su RP. I collegamenti dei membri devono essere collegati in modalità back-to-back, senza alcun switch L2. La funzione BoB è configurata in tutte le interfacce Bundle Ethernet della rete XYZ.

7.2. Bilanciamento del carico

Il load balancing ECMP per flow nella rete interessata si estende sulle interfacce Ethernet tra bundle e sulle reti Ethernet intra-bundle (tra i membri fisici di un'interfaccia Bundle). Questo è applicabile in tutta la rete da PE a PE (Core Load Balance) e da PE a CE (AC Load Balance) come descritto.

7.2.1. Bilanciamento del carico del nucleo con etichetta FAT

Per quanto riguarda l'ambito della rete XYZ, è necessario considerare solo il bilanciamento del carico ECMP (Multipath a costo uguale) per flusso, come indicato di seguito:

In genere, i router bilanciano il carico del traffico in base all'etichetta più in basso nello stack di etichette, che ha la stessa etichetta per tutti i flussi di un determinato pseudofilo. Ciò può portare a un bilanciamento del carico asimmetrico. Il flusso, in questo contesto, si riferisce a una sequenza

di pacchetti che hanno la stessa coppia di origine e destinazione. I pacchetti vengono trasportati da un perimetro del provider di origine (PE) a un perimetro del provider di destinazione (PE).

Lo Pseudowire di trasporto basato sul flusso (FAT PW) consente di identificare i singoli flussi all'interno di uno pseudowire e fornisce ai router la possibilità di utilizzare questi flussi per bilanciare il carico del traffico. I PW FAT vengono utilizzati per bilanciare il carico del traffico nel core quando vengono utilizzati percorsi multipli (ECMP) a costo uguale. Un'etichetta di flusso viene creata in base ai flussi di pacchetti indivisibili che entrano in uno pseudofilo e viene inserita come etichetta più in basso nel pacchetto. I router possono utilizzare l'etichetta di flusso per il bilanciamento del carico, che fornisce una migliore distribuzione del traffico tra i percorsi ECMP o i percorsi basati su link nel core.

Allo stack viene aggiunta un'etichetta aggiuntiva, denominata etichetta di flusso, che viene generata per ogni singolo flusso in ingresso nel file PE. Un'etichetta di flusso è un identificatore univoco che distingue un flusso all'interno del PW e deriva dagli indirizzi MAC di origine e destinazione e dagli indirizzi IP di origine e destinazione. L'etichetta di flusso contiene la fine dell'insieme di bit dello stack di etichette (EOS). L'etichetta di flusso viene inserita dopo l'etichetta VC e prima della parola di controllo (se presente). Il PE in entrata calcola e inoltra l'etichetta di flusso. La configurazione FAT PW abilita l'etichetta di flusso. L'entità PE in uscita ignora l'etichetta di flusso in modo che non vengano prese decisioni.

7.2.2. Bilanciamento del carico del circuito di collegamento

Per il bilanciamento del carico dei membri del bundle AC, tuttavia, è necessario un approccio diverso a causa dell'assenza di SR-MPLS in questa sezione della rete.

In questo caso, il bilanciamento del carico per flusso può essere ottenuto quando i manopole di configurazione l2vpn specifici di tutti i router PE vengono modificati in modo esplicito. Può essere per SRC/DST MAC o SRC/DST IP in base ai requisiti.

Modelli di configurazione Esempi di comandi e

8. La soluzione di progettazione completa

In questa sezione vengono illustrati i dettagli completi del progetto cuciti da tutti i singoli componenti descritti nelle sezioni precedenti. In questa sezione vengono illustrati la topologia e il modello di configurazione appropriato con riferimento a Cisco IOS-XR 7.5.x.

8.1. Requisiti di basso livello

Per lo scenario di traffico normale, il flusso di traffico è progettato per propagarsi sempre tra le terminazioni del servizio di PE1 e PE3 e solo tra PE2 e PE4. In questa situazione, l'obiettivo principale è mantenere la traccia completamente disgiunta, come mostrato nella Figura 12.

Il traffico in questione in questo caso sarebbe costituito da flussi multicast incapsulati attraverso la sovrapposizione EVPN. Dai nodi CE1 e CE2, arrivano i flussi multimediali multicast (voce/video) in cui, può essere incapsulato ai nodi PE1 e PE2 e trasportato attraverso la sovrimpressione EVPN

L2 rispettivamente ai nodi CE3 e CE4 dopo essere stato decapsulato rispettivamente ai nodi PE3 e PE4.

Pertanto, la coppia traffico origine-destinazione viene considerata come PE1-PE3 e PE2-PE4 in tutte le circostanze, a meno che non sia diversamente indicato. Per maggiori informazioni, consultare il paragrafo 2.2.

8.2. Riepilogo del progetto

Per soddisfare tali requisiti, l'opzione OSPF viene scelta come IGP sottostante, a seconda delle esigenze di XYZ Networks. Per indirizzare il flusso multicast incapsulato attraverso la coppia di traffico origine-destinazione attraverso il percorso desiderato, è necessario implementare SR-TE tra i nodi PE.

Le policy SR-TE sono state progettate con percorsi IGP dinamici ed espliciti.

I percorsi espliciti riguardano:

- Scenario di traffico normale
- Scenario di failover fino a quando non sono disponibili opzioni alternative per il percorso

I percorsi IGP dinamici comprendono:

- Percorso di backup per lo scenario di failover in cui NON sono disponibili opzioni alternative per il percorso

Le funzionalità quali BFD, TI-LFA e Microloop Avoidance sono configurate in OSPF come illustrato nelle sottosezioni relative ai modelli di configurazione.

Per gli scenari di traffico normale, il modello di configurazione e altri dettagli sono menzionati nella sottosezione 8.5.1.

Per gli scenari di failover del traffico, il modello di configurazione e altri dettagli sono menzionati nella sottosezione 8.5.2.

Oltre a questi, vengono presi in considerazione anche i requisiti come la prevenzione del microloop e meno di 50 msec di convergenza in caso di scenari di guasto.

8.3. Blocchi di progettazione

Questa sottosezione raccoglie tutti i blocchi di progettazione che vengono successivamente trattati in modo approfondito in queste sezioni.

Panoramica generale della progettazione (livello 1):

- Le dimensioni MTU nell'intera rete XYZ sono fissate su '9216' con l'obiettivo di supportare fino a 5-6 stack di etichette SR
- Il protocollo 'BFD over Bundle' viene implementato con un intervallo di 15 msec per rilevare la fibra tagliata al di sotto dei 50 msec

Panoramica del progetto OSPF/SR-TE:

- OSPF come protocollo IGP con TI-LFA configurato per fornire FRR sotto i 50 msec di tempo di convergenza
- Layer di trasporto basato su Segment Routing come Forwarding Plane e OSPF come protocollo di routing
- In Rete XYZ, il percorso esplicito di Ingegneria del traffico di routing del segmento guida il traffico in tutte le direzioni del percorso principale richieste. In caso di scenari di failover di collegamento/nodo, il traffico viene instradato da un percorso igp dinamico
- Fanno parte di questo progetto anche le tecnologie Microloop Avoidance e OSPF Max-Metric

Panoramica del progetto BGP/RR:

- In un cluster sono configurati due record di risorse per fornire ridondanza
- Il processo BGP, rete XYZ, in ciascun PE forma 'IPv4' e 'L2VPN EVPN' con entrambi gli RR separatamente

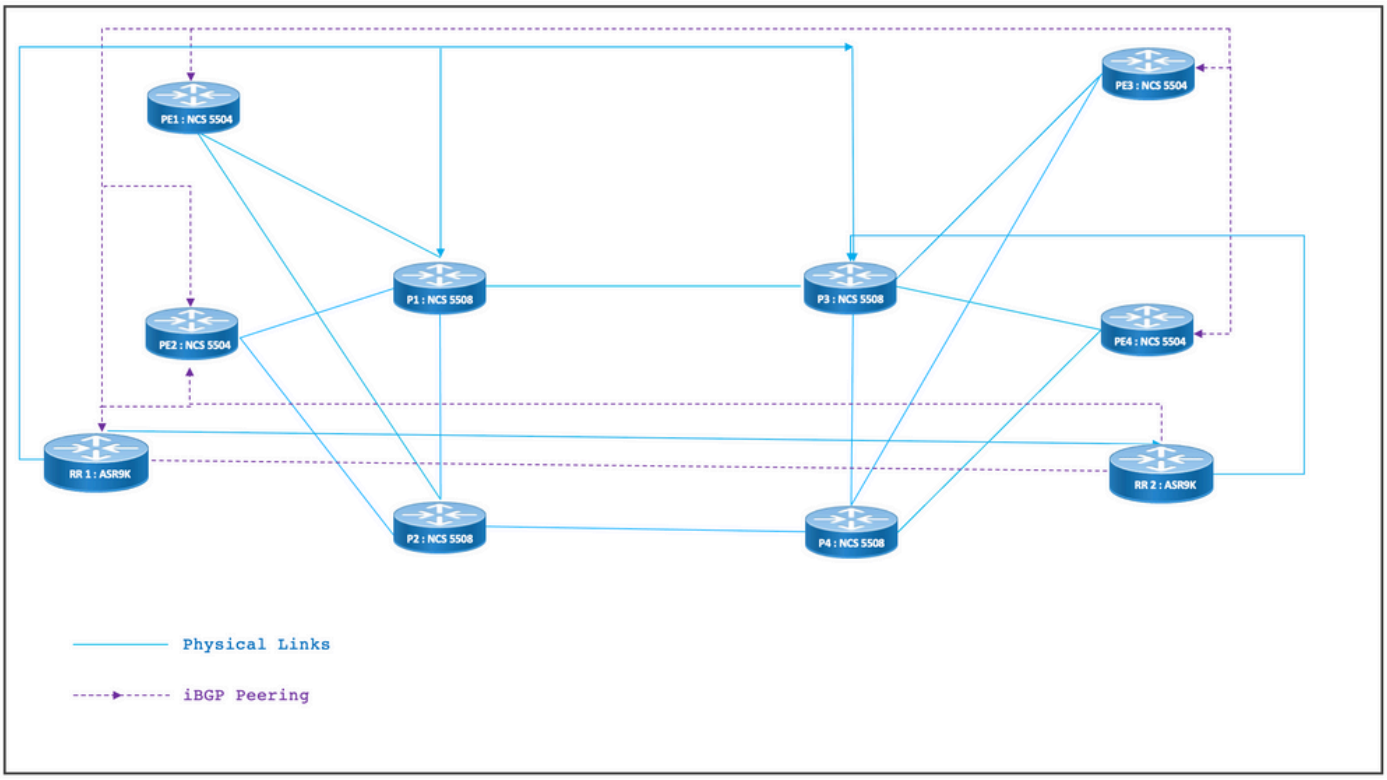
Panoramica della progettazione dei servizi:

- I livelli di servizio sono basati sul Control Plane basato su BGP e sul layer 2 point-to-point EVPN (EVPN-VPWS)
- Il traffico video multicast (UDP) viene inviato incapsulato attraverso i PMW EVPN-VPWS point-to-point
- Il bilanciamento del carico ECMP si ottiene configurando l'etichetta FAT nella sezione EVPN
- Il servizio mira a supportare fino a 5-6 etichette SR che includono etichette per il trasporto SR, etichette EVPN e etichette FAT per il bilanciamento del carico

8.4. Topologia fisica di esempio

La topologia fisica delle reti XYZ è illustrata in questa figura. Per semplicità, vengono mostrati solo 4 nodi PE e 4 P. Sono disponibili due nodi RR che operano in cluster per fornire ridondanza.

Figura 11. Topologia fisica



8.5. Dettagli di progettazione del layer 1

Nel progetto generico di layer 1, è presente un'interfaccia Bundle Ethernet con almeno due collegamenti membri per bundle configurati. Per un rapido rilevamento di errori di collegamento, scegliere BFD sulla funzione Bundle. L'intervallo di tempo può variare in modo ideale tra 5 e 15 msec. Dipende dalla capacità hardware di scaricamento.

Per i dettagli sul BFD, consultare il sito https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/routing/73x/b-routing-cg-ncs5500-73x/implementing-bfd.html. Notare che questa funzione deve essere configurata solo con l'interfaccia Ethernet del bundle e non è richiesta la configurazione con IGP. Le dimensioni MTU sono fissate a 9216 con l'obiettivo di supportare fino a 5-6 stack di etichette SR.

8.5.1. Modelli di configurazione

I modelli di configurazione BFD over Bundle per tutti i nodi sono riportati di seguito:

```
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. Panoramica del progetto OSPF/SR-TE

Tutti i router OSPFv2 della rete si trovano nell'area 0, quindi la rete gestisce un singolo dominio IGP.

Nel router OSPF, il routing dei segmenti è abilitato e le interfacce Bundle Ethernet rilevanti sono configurate. Analogamente, in Interfacce bundle sono attivati il tipo di rete e i parametri di reindirizzamento rapido. L'aspetto più importante è che un'interfaccia di loopback è abilitata in modalità passiva con prefisso-SID configurato.

Poiché OSPF è un protocollo dello stato del collegamento, è necessario identificare immediatamente i collegamenti di downlink e creare un percorso di backup. Per risolvere questo problema, il BFD over Bundle sotto Bundle Interface e TI-LFA FRR sotto OSPF è configurato in modo da mantenere il tempo di convergenza a 50 msec in caso di scenari di taglio della fibra.

Le sezioni secondarie seguenti descrivono in dettaglio gli scenari Normale e Failover dei percorsi di traffico:

8.6.1. Scenario di traffico normale SR-TE

Per mantenere un percorso primario molto rigoroso, le policy SR-TE devono essere progettate con percorsi espliciti end-to-end tra le coppie di traffico origine-destinazione menzionate in precedenza. Inoltre, sono necessari più percorsi di selezione delle preferenze all'interno di una regola SR-TE per fornire il provisioning per più scenari di failover.

La figura mostra i dettagli della rete utente allineati con i blocchi di progettazione menzionati nella sottosezione 8.3.

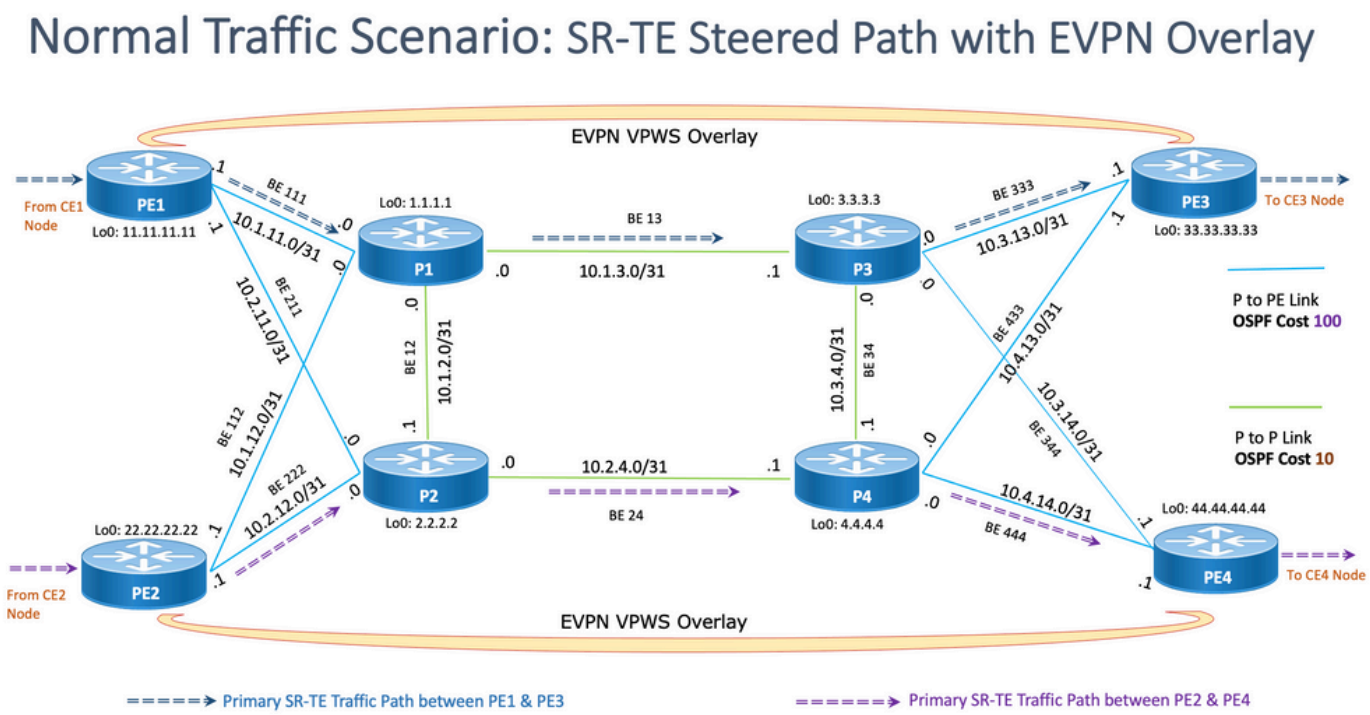
- Collegamenti tra nodi PE e P e nodi P-P
- Indirizzi di loopback di tutti i nodi
- Indirizzi di interfaccia di tutti i nodi
- Direzione del percorso del traffico normale sterzato SR-TE
- Sovrapposizione EVPN tra nodi PE

Non è stata dimostrata l'intenzione di ridurre l'ingombro nella topologia.

I collegamenti tra PE e P sono stati contrassegnati in blu e i collegamenti tra P e P sono stati contrassegnati in verde. Il costo OSPF dei collegamenti PE-to-P è 100 e il costo dei collegamenti P-to-P è 10.

Il flusso di traffico primario SR-TE è stato contrassegnato con frecce blu tra la coppia PE1-PE3 e con frecce viola tra la coppia PE2-PE4.

Figura 12. Dettagli topologia



8.6.1.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione OSPF/SR-TE per i nodi PE1 e PE2 indicati di seguito:

<#root>

 # 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
```

Nota: per configurare il comando Source-Address" globalmente o in criteri. Come comportamento predefinito, l'indirizzo di origine nel criterio sostituisce il comando globale.

Il comando source address nella configurazione di routing del segmento come mostrato è necessario in scenari specifici in cui, nello stesso PE, come origine della policy SR-TE, è necessario scegliere un indirizzo di loopback tra più o quando ISIS e OSPF vengono eseguiti con loopback separati, e occorre bloccarlo su uno di essi. In caso contrario, in scenari normali in cui esiste un solo IGP che viene eseguito con un loopback univoco, la configurazione dell'indirizzo di origine è facoltativa.

<#root>

segment-routing

```
 global-block 16000 23999   ✳Default SRGB Value (Need not be configured). Needs to be configured only i
 local-block 15000 15999    ✳Default SRLB Value (Need not be configured). Needs to be configured only i
 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>
     !
    !


   !
  !
 !
!
```

<#root>

```
# 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
```

Nota: i comandi facoltativi indirizzo di origine, SRGB predefinito e SRLB sono stati rimossi.

<#root>

```
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>
     !
    !


   !
  !
 !
!
```

Nota: nella soluzione sopra menzionata, gli hop espliciti degli elenchi dei segmenti sono

basati sugli indirizzi IP, in quanto, come accennato in questo documento, la configurazione esplicita della policy SR-TE del percorso è basata su "etichetta mpls" e la convalida del percorso non funziona in caso di errore del collegamento remoto nella versione 7.3.x

Se un collegamento remoto, a parte il collegamento locale di un nodo PE, ha esito negativo, il percorso rimane valido. Questa è la versione progettata e non può essere modificata fino a XR 7.5.x

<#root>

```
# 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 per scenari di failover

Per comprendere gli scenari di failover del traffico, è necessario esaminare attentamente il traffico del percorso primario in condizioni di traffico normali, come indicato nel diagramma della topologia della sottosezione precedente.

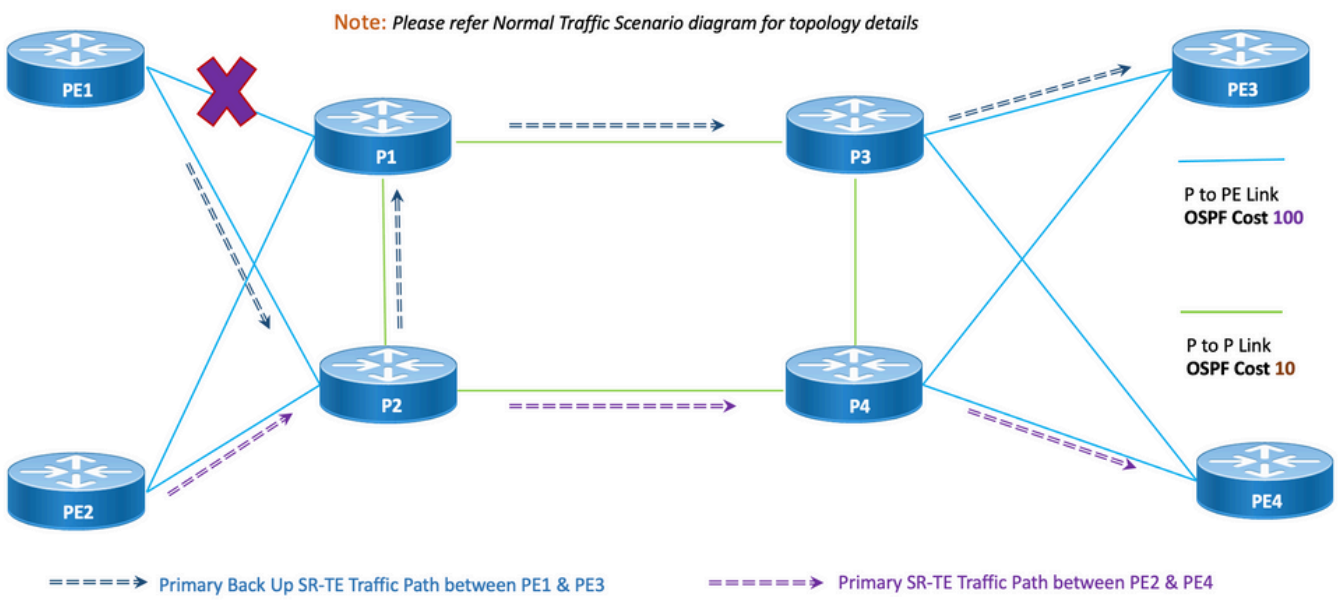
L'obiettivo principale in caso di scenari di failover è mantenere la discontinuità del percorso del traffico il più possibile, data l'infrastruttura della topologia corrente. La rete XYZ ha requisiti molto severi per indirizzare il traffico attraverso nodi specifici nei percorsi di backup in modo da mantenere la massima separazione tra le coppie di nodi di origine e destinazione. Questa progettazione viene eseguita per evitare il sovraccarico dei collegamenti utilizzati e per mantenere un numero minimo di collegamenti inutilizzati.

In queste sottosezioni vengono illustrati i vari scenari di failover, ad esempio collegamento singolo, doppio collegamento, nodo singolo e doppio nodo, con il percorso di failover necessario al traffico per mantenere la massima discontinuità.

8.6.3. Scenario di failover a collegamento singolo

Si tratta dello scenario di errore del collegamento singolo in cui il collegamento locale tra PE1 e P1 si interrompe e il traffico prende una deviazione attraverso i nodi P2 e P1 di base. Questo processo è gestito a livello amministrativo tramite segment-list <SIDLIST1> che costituisce il percorso di backup principale tra i nodi PE1 e PE3

Figura 13. Scenario di failover a collegamento singolo



Disgiunzione: in caso di errore di un singolo collegamento, il numero di collegamenti comuni condivisi è zero (0), come mostrato nella topologia precedente.

8.6.3.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione OSPF/SR-TE pertinenti per i nodi PE1 e PE2 indicati di seguito:

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
# 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>
     !
    !


   !
  !
 !
!
```

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

```
<#root>
# 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

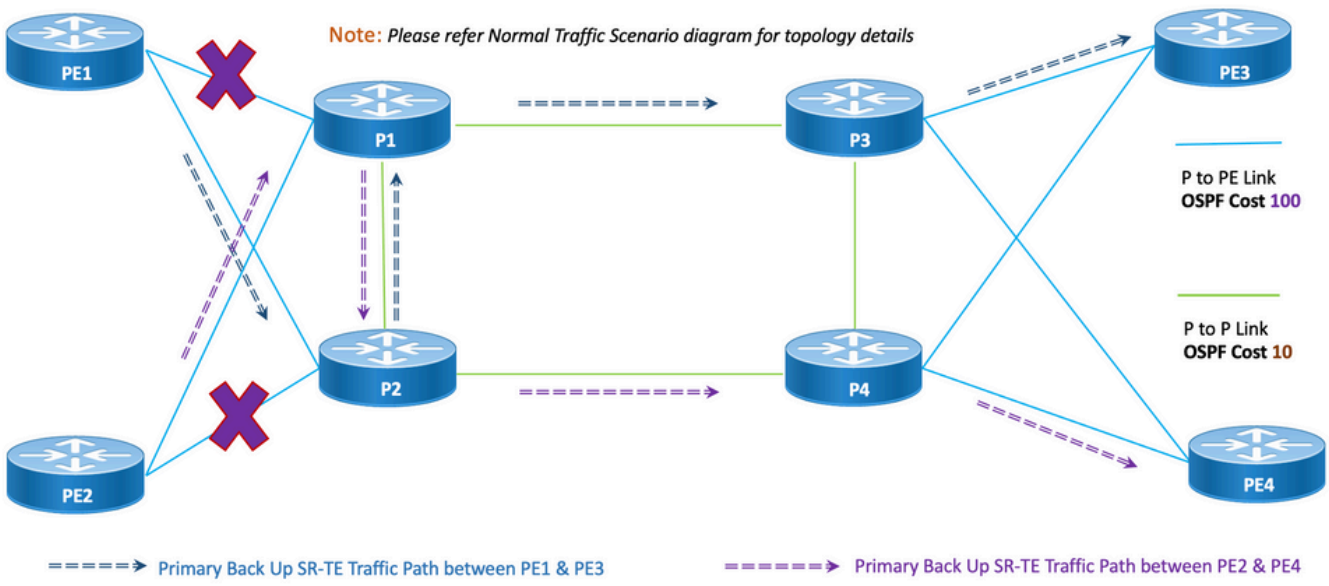
```
     ✳Primary/Normal Path with highest preference
(Active Path for PE2 in this scenario)


     explicit segment-list <SIDLIST1>
     !
    !


   !
  !
 !
!
```

8.6.4. Scenario di failover a doppio collegamento

Si tratta dello scenario di errore del collegamento doppio in cui il collegamento locale tra PE1 e P1 e il collegamento locale tra PE2 e P2 ha esito negativo. Il traffico proveniente da PE1 prende una deviazione attraverso i nodi P2 e P1 core, mentre il traffico proveniente da PE2 prende una deviazione attraverso i nodi P1 e P2 core.

Tali percorsi vengono gestiti a livello amministrativo mediante il rispettivo elenco di segmenti <SIDLIST2> di PE1 e PE2 che costituiscono i percorsi di backup secondari tra i nodi PE1 e PE3 e PE2 e PE4 rispettivamente.

Figura 14. Scenario di failover a doppio collegamento



Disgiunzione: in caso di errore di collegamento doppio, il numero di collegamenti comuni condivisi è uno (1), come mostrato nella topologia sopra indicata.

8.6.4.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione OSPF/SR-TE pertinenti per i nodi PE1 e PE2 indicati di seguito:

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
# 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
  !
 !
!
```

<#root>

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>

!

!

```
   !
  !
 !
!
```

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
# 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

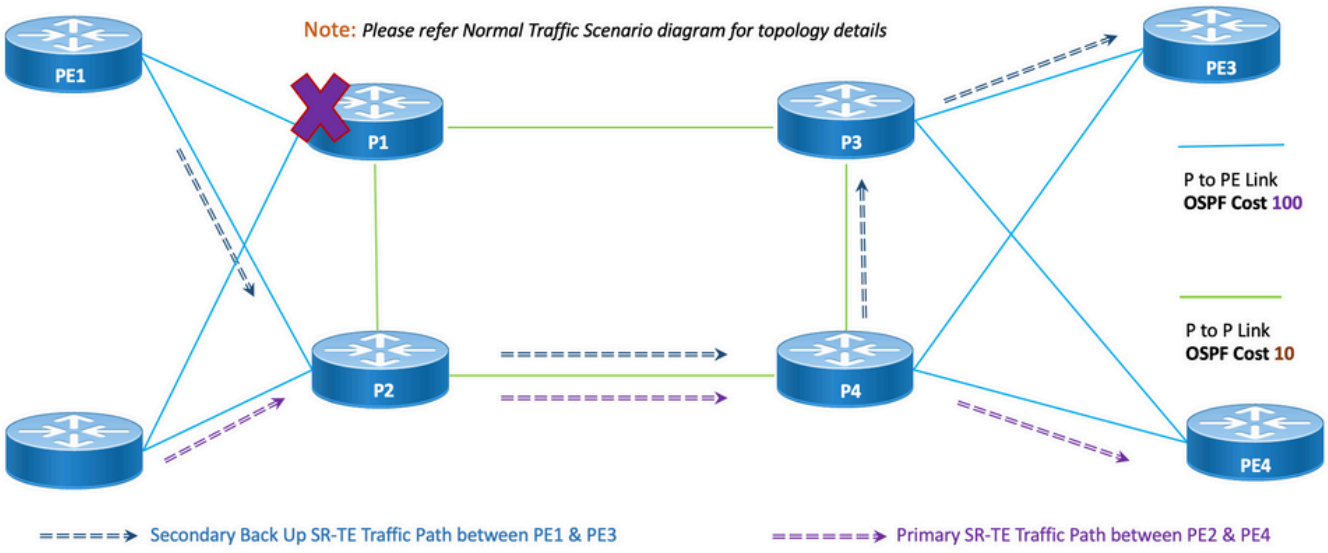
```
     ✳Primary Back Up Path with 2nd highest preference
 (Active Path for PE2 in this scenario)


     explicit segment-list <SIDLIST2>
     !
    !


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



   !
  !
 !
!
```

8.6.5. Scenario di failover a nodo singolo

Si tratta dello scenario di errore di un singolo nodo in cui il nodo P1 si guasta e il traffico prende una deviazione attraverso i nodi P2 e P4 principali. Questo processo viene gestito a livello amministrativo tramite segment-list <SIDLIST3>, che costituisce il percorso di backup secondario tra i nodi PE1 e PE3.

Il traffico tra PE2 e PE4, tuttavia, rimane lo stesso del percorso primario, come mostrato in questa topologia.

Figura 15. Scenario di failover a nodo singolo



Disgiunzione: in caso di errore di un singolo nodo, il numero di collegamenti comuni condivisi è uno (1), come mostrato nella topologia sopra menzionata.

8.6.5.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione OSPF/SR-TE per i nodi PE1 e PE2 indicati di seguito:

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
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>
     !
    !


   !
  !
 !
!
```

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

 # 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)

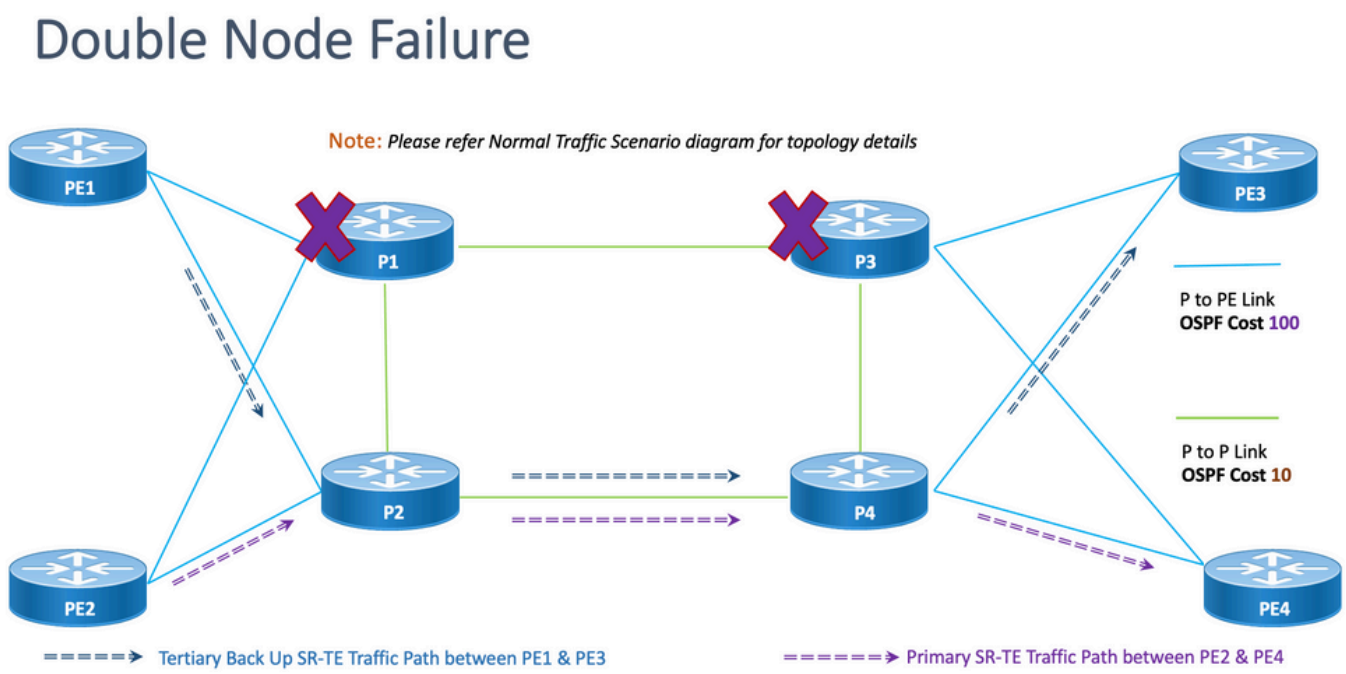
```
     explicit segment-list <SIDLIST1>
      !
     !


    !
   !
  !
!
```

8.6.6. Scenario di failover a doppio nodo

Si tratta dello scenario di errore dei nodi doppi in cui i nodi P1 e P3 si guastano e il traffico prende una deviazione attraverso i nodi P2 e P4 principali. Questo processo viene gestito a livello amministrativo tramite segment-list <SIDLIST3>, che costituisce il percorso di backup secondario tra i nodi PE1 e PE3. Poiché i percorsi espliciti sono definiti solo per i 2 scenari precedentemente menzionati, il percorso IGP dinamico forma il percorso di backup terziario e assume il ruolo di instradamento del traffico attraverso i nodi P2 e P4.

Il traffico tra PE2 e PE4, tuttavia, rimane lo stesso del percorso primario, come mostrato in questa topologia.

Figura 16. Scenario di failover a doppio nodo.



Disgiunzione: in caso di errore di nodo doppio, il numero di collegamenti comuni condivisi è uno (1), come mostrato in questa topologia.

8.6.6.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione OSPF/SR-TE per i nodi PE1 e PE2 indicati di seguito:

✎ Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
# 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>
     !
    !


   !
  !
 !
!
```

Nota: i modelli di configurazione OSPF del router di PE1 e PE2 sono simili allo scenario normale.

<#root>

```
# 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. Panoramica del progetto BGP/RR

Border Gateway Protocol (BGP) è il protocollo che prende le decisioni di routing su Internet. Mantiene una tabella di reti IP o "prefissi" che designano la raggiungibilità della rete tra i sistemi autonomi (AS). È descritto come protocollo vettoriale di percorso. BGP non utilizza le metriche IGP (Interior Gateway Protocol) tradizionali, ma prende le decisioni di routing in base al percorso,

alle policy di rete e/o ai set di regole. Per questo motivo, è più appropriato definire un protocollo di raggiungibilità che un protocollo di routing.

MP-BGP può essere utilizzato per propagare i prefissi IPv4, IPv6, VPNv4, VPN6, EVPN e dello stato del collegamento attraverso la rete. Questa operazione viene eseguita con una configurazione del reflector di route che forma iBGP neighbors con dispositivi Core, di aggregazione, di accesso e SR-PCE.

Tramite RR, i prefissi appresi BGP vengono propagati internamente tramite iBGP. Le route BGP non vengono mai ridistribuite in IGP. I riflettori di instradamento sono totalmente isolati dal piano dati e sono dedicati ai piani di controllo.

8.7.1. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione rilevanti per BGP/RR come mostrato:

<#root>

```
# 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>
```

<#root>

```
# 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. Panoramica della progettazione del servizio

In questa sezione secondaria viene descritto il servizio di overlay di VPN VPWS insieme alla rappresentazione dello stack di etichette supportato e ai modelli di configurazione.

EVPN-VPWS è una soluzione BGP control plane per servizi point-to-point. Implementa le tecniche di segnalazione e incapsulamento che stabiliscono un'istanza EVPN tra una coppia di PE. Consente di inoltrare il traffico da una rete all'altra senza la ricerca MAC. L'uso di EVPN per VPWS elimina la necessità di segnalare PW a segmento singolo e a più segmenti per i servizi

Ethernet point-to-point. La tecnologia EVPN-VPWS funziona sui core IP e MPLS; il core IP supporta i core BGP e MPLS per lo switching dei pacchetti tra gli endpoint.

8.8.1. Rappresentazione dello stack di etichette

Il servizio mira a supportare fino a 5-6 etichette SR, incluse le etichette di trasporto SR, le etichette EVPN e le etichette FAT per il bilanciamento del carico. Il numero massimo analizzato di etichette in Scenari normali in cui il traffico passa attraverso un percorso primario esplicito:

ADJ SID1	
ADJ SID2	
ADJ SID3	
ETICHETTA EVPN	
ETICHETTA FLUSSO (S=1)	

Il numero massimo analizzato di etichette negli scenari di failover in cui il traffico passa attraverso il percorso di backup esplicito o il percorso di backup dinamico definito da IGP:

TI-LFA SID1
TI-LFA SID2
TI-LFA SID3
ETICHETTA EVPN
ETICHETTA FLUSSO (S=1)

8.8.2. Modelli di configurazione

Questa sottosezione contiene i modelli di configurazione rilevanti per EVPN-VPWS, come mostrato:

<#root>

```
# 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 e
  !
 !
 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 EV
  !
 !
 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
```

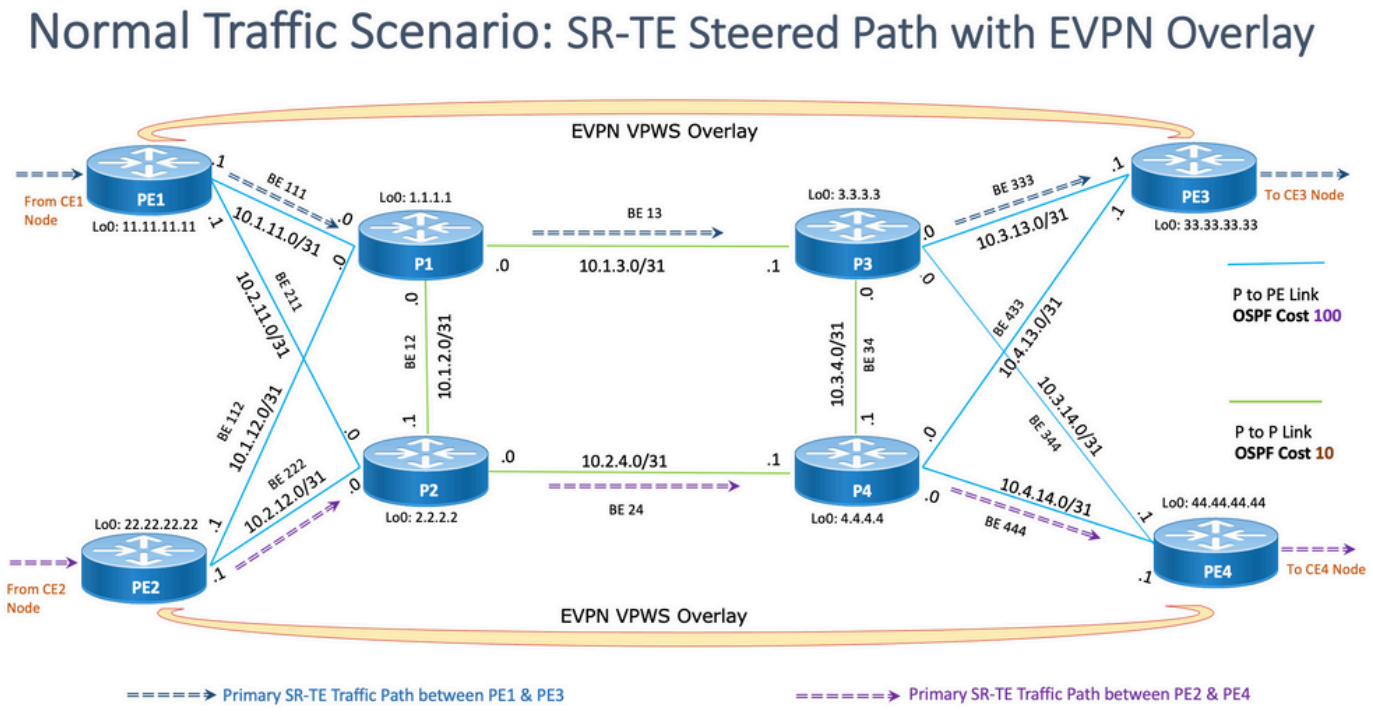
```
    pw-class <PW-Class-Name1>
   !
```

9. Comandi di esempio per la configurazione e la visualizzazione

Questa sezione finale contiene la configurazione rilevante e i comandi show dei nodi PE solo per lo scenario Normal Traffic. Questi vengono acquisiti allineati ai parametri riportati nella figura come riferimento per comprendere meglio i modelli di configurazione descritti nelle sezioni precedenti.

9.1. Configurazione di esempio nei nodi PE

Figura 17. Topologia con parametri di configurazione.



<#root>

```
# 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
  !
 !
```

```
!
```

<#root>

```
#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
     !
    !
   !
  !
 !
!
```

<#root>

 # 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
  !
 !
!
```

<#root>

#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
     !
    !
   !
  !
 !
!
```

<#root>

 # 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
 !
!
```

<#root>

 # 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
 !
!
```

<#root>

 # 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 &
   flow-label static
  !
 !
 interface Bundle-Ether99        ✳Interface Attachment Circuit
  ethernet-segment
   identifier type 0 00.00.00.00.00.00.00.00.00
  !
 !
!
```

<#root>

 # 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 &
   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. Comandi di visualizzazione rilevanti nei nodi PE

<#root>

```
# 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
```

<#root>

 # 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
```

<#root>

 # 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 funziona in modalità STANDALONE.

<#root>

```
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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- 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
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).