

Mecanismo de convergência de caminho explícito baseado em política SR-TE com proteção de link TI-LFA

Contents

[Introdução](#)

[Detecção de falha de link](#)

[Cenários de convergência detalhados](#)

[Convergência de falha de link - o caminho principal entra no estado inativo](#)

[Reconvergência de falha de link - caminho principal de volta ao estado ativo](#)

[Software usado](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o conceito de convergência com Topology Independent (TI) - Loop-Free Alternative (LFA), que é um recurso altamente focado. Ele detalha o mecanismo de roteamento de segmento (SR - Segment Routing) - convergência de caminho de política de engenharia de tráfego (TE - Traffic Engineering) com proteção TI-LFA como uma base com um diagrama de topologia baseado nos requisitos das redes XYZ.

Detecção de falha de link

Observe que os recursos de convergência de caminho de política SR-TE e TI-LFA são independentes um do outro e funcionam separadamente. No entanto, o recurso TI-LFA é adicionado para fazer uma detecção rápida de falha de caminho de política SR-TE primária e menos de 50 ms de comutação de tráfego para o caminho de backup predefinido sob condições de rede ideais. A política SR-TE funcionaria perfeitamente sem TI-LFA, no entanto, nesse cenário, o número de convergência dependeria apenas do IGP (Interior Gateway Protocol) e seria muito maior que 50 ms.

No cenário de falha de link, nosso objetivo é manter o tempo de convergência o mais baixo possível, o que minimizaria a perda de pacotes durante o evento de inatividade/oscilação do link.

A detecção de evento de link inativo no nó do headend pode ocorrer principalmente por estes métodos:

1. Detecção na Camada Física em caso de links adjacentes quebrados.
2. Detecção por BFD sobre pacote em caso de links remotos quebrados.

No primeiro caso, a detecção é mais rápida e o tempo de convergência é menor que a segunda opção, onde a detecção depende do intervalo BFD/temporizador dead configurado e do ponto de rede exato onde o link foi desativado. No entanto, uma detecção muito rápida não significa necessariamente uma convergência rápida, já que a XYZ Org Network é uma estrutura multicamada com tráfego de serviço completo que cobre vários saltos.

Como a rede da empresa XYZ está contida em um único BGP AS e um único domínio IGP, aqui os caminhos de backup pré-definidos TI-LFA transportam imediatamente o tráfego de failover após uma falha de link em todos os cenários e garantem a perda mínima de pacotes e a cobertura completa do prefixo, independentemente do estado da topologia. Os caminhos primários/secundários definidos pela política SR-TE podem demorar um pouco para convergir devido ao IGP e, por fim, assumir o controle do tráfego de serviço de ponta a ponta através do núcleo, que pode ou não corresponder aos caminhos predefinidos do TI-LFA.

Cenários de convergência detalhados

Para obter mais detalhes, vamos entender o exemplo detalhado aqui que explica o caminho do tráfego com políticas SR-TE e TI-LFA como o mecanismo de convergência da rede da empresa XYZ.

Exemplo de configuração de SR alinhada com os diagramas de topologia:

```
<#root>
```

```
segment-routing
```

```
traffic-eng
```

```
!
```

```
!
```

```
segment-list PrimaryPath1
```

```
index 10 mpls adjacency 10.1.11.0
```

```
--> First Hop (P1 node) of the explicit-path
```

```
index 20 mpls adjacency 10.1.3.1
```

```
-->
```

```
Second Hop (P3 node) of the explicit-path
```

```
index 30 mpls adjacency 10.3.13.1
```

```
--> Third Hop (PE3 node) of the explicit-path
```

```
!
```

```
policy POL1
```

```
source-address ipv4 11.11.11.11
```

```
--> Source Node of the explicit-path
```

color 10 end-point ipv4 33.33.33.33

--> Destination Node of the explicit-path

candidate-paths

preference 100

--> Secondary Path taken care of dynamically by IGP TI-LFA

```
dynamic
metric
type igp
!
```

preference 200

explicit segment-list PrimaryPath1

--> Primary Explicit-Path of the SR-TE policy

```
!
```

Em um cenário normal, o tráfego deve passar de PE1 a PE3 por um dos dois possíveis caminhos candidatos $PE1 > P1 > P3 > PE3$ e $PE1 > P2 > P4 > PE3$ da política SR-TE, o caminho explícito primário conforme configurado pelo administrador com a lista Adjacency (Adj) - Segment Identifier (SID) **10.1.11.0**, **10.1.3.1**, **10.3.13.1** ou o caminho dinâmico secundário conforme determinado pelo IGP em questão. O administrador prefere usar o caminho do candidato principal e somente o fallback para o caminho secundário quando o principal estiver inativo. Assim, um valor de preferência mais alto é atribuído ao caminho do candidato principal, que indica um caminho preferido. Por exemplo, o caminho do candidato principal pode ter uma preferência de **200** e o caminho do candidato secundário tem uma preferência de **100**.

Normal Traffic Scenario: Steered Traffic Path via SR-TE Primary Candidate Path

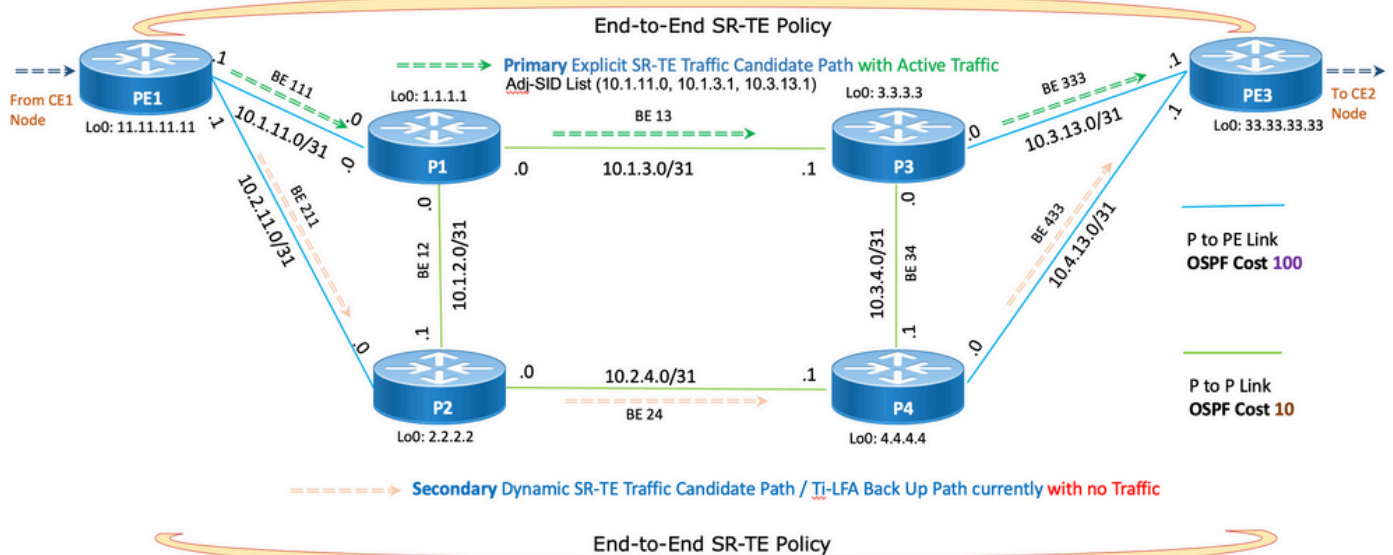


Figura 1: Caminho do candidato principal do cenário de tráfego normal SR-TE

Qualquer caminho candidato é usado quando é válido, e a acessibilidade de seus SIDs constituintes determina o critério de validade.

Quando ambos os caminhos candidatos são válidos e utilizáveis, o ponto inicial PE1 seleciona o caminho de preferência mais alto e instala a lista SID desse 10.1.11.0, 10.1.3.1, 10.3.13.1 caminho em sua tabela de encaminhamento. A qualquer momento, o tráfego de serviço que é direcionado para essa política de SR é enviado apenas no caminho selecionado, qualquer outro caminho candidato dinâmico está inativo.

Um caminho candidato é selecionado quando tem o valor de preferência mais alto entre todos os caminhos candidatos válidos da política SR. O caminho escolhido também é conhecido como o "caminho ativo" da política de SR.

Convergência de falha de link - o caminho principal entra no estado inativo

Em algum momento, uma falha de link pode ocorrer na rede. O link com falha pode ser um link entre dois nós quaisquer, por exemplo, P1 e P3. Assim que a falha for detectada por qualquer meio, conforme descrito no início da seção, a proteção TI-LFA deve garantir que os fluxos de tráfego sejam rapidamente redirecionados para o caminho de proteção TI-LFA, idealmente dentro de 50 ms.

Observe que, nesse cenário, o caminho de backup determinado pelo TI-LFA, como mostrado na Figura 2, é diferente do caminho de política de backup convergente determinado pelo IGP na Figura 3. Isso é bastante normal, pois o caminho de backup TI-LFA é determinado localmente pelo nó de Ponto de Reparo Local (PLR) onde a falha ocorreu, no entanto, o caminho de backup de política SR-TE otimizado é determinado pela convergência IGP pelo nó de headend que mantém as decisões de política SR-TE.

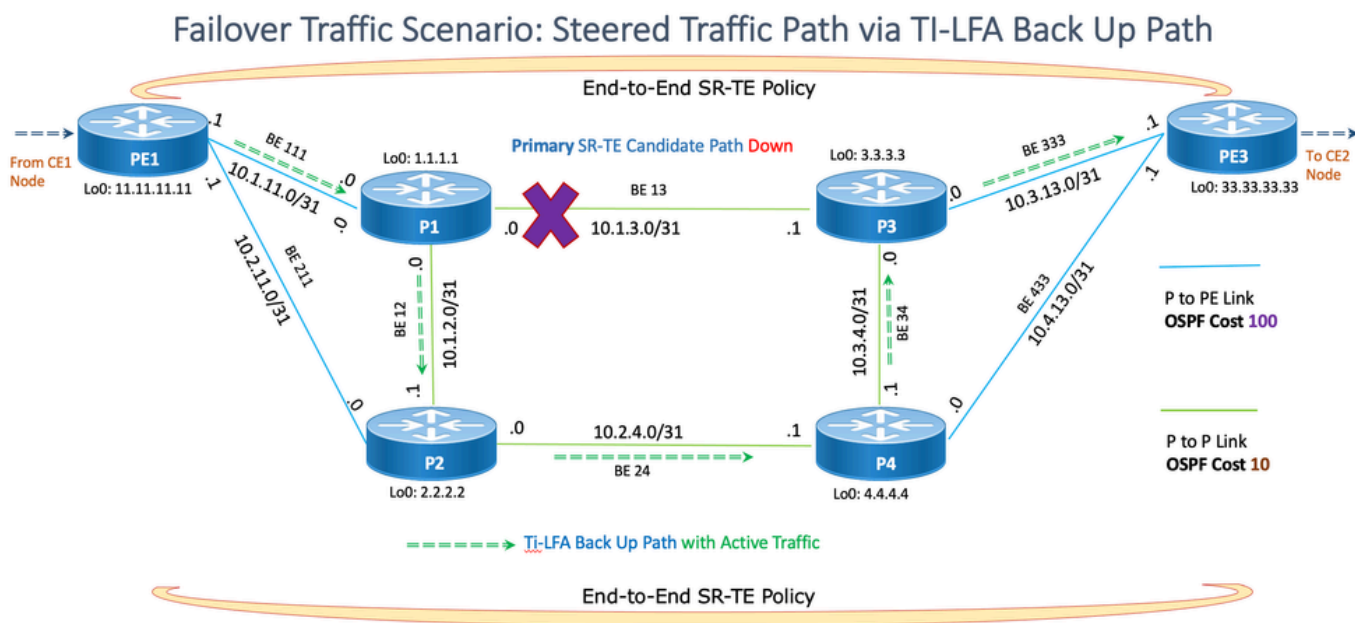


Figura 2: Cenário de tráfego de failover pelo caminho de backup TI-LFA

O tráfego continua a fluir através do caminho de proteção TI-LFA até que, eventualmente, o ponto inicial PE1 aprenda através da inundação de IGP que o SID 10.1.3.1 do link com falha se tornou inválido. Em seguida, o PE1 avalia a validade da lista SID do caminho 10.1.11.0, 10.1.3.1, 10.3.13.1 e a invalida devido à presença do SID inválido 10.1.3.1. Simultaneamente, invalida o caminho candidato e executa novamente o processo de seleção de caminho da política SR-TE. O PE1, subsequentemente, seleciona outro caminho de candidato válido com o próximo valor de preferência mais alto e instala a lista SID 10.2.11.0, 10.2.4.1, 10.4.13.1 do novo caminho de candidato secundário na tabela de encaminhamento. No entanto, esse caminho de candidato secundário é dinâmico por natureza, determinado pelo IGP Open Shortest Path First (OSPF) e não tem controle administrativo. Até essa etapa, o tráfego flui pelo caminho TI-LFA protegido; mas depois disso, ele é direcionado para o caminho secundário recém-preferido da política SR-TE.

Failover Traffic Scenario: Steered Traffic Path via SR-TE Secondary Candidate Path

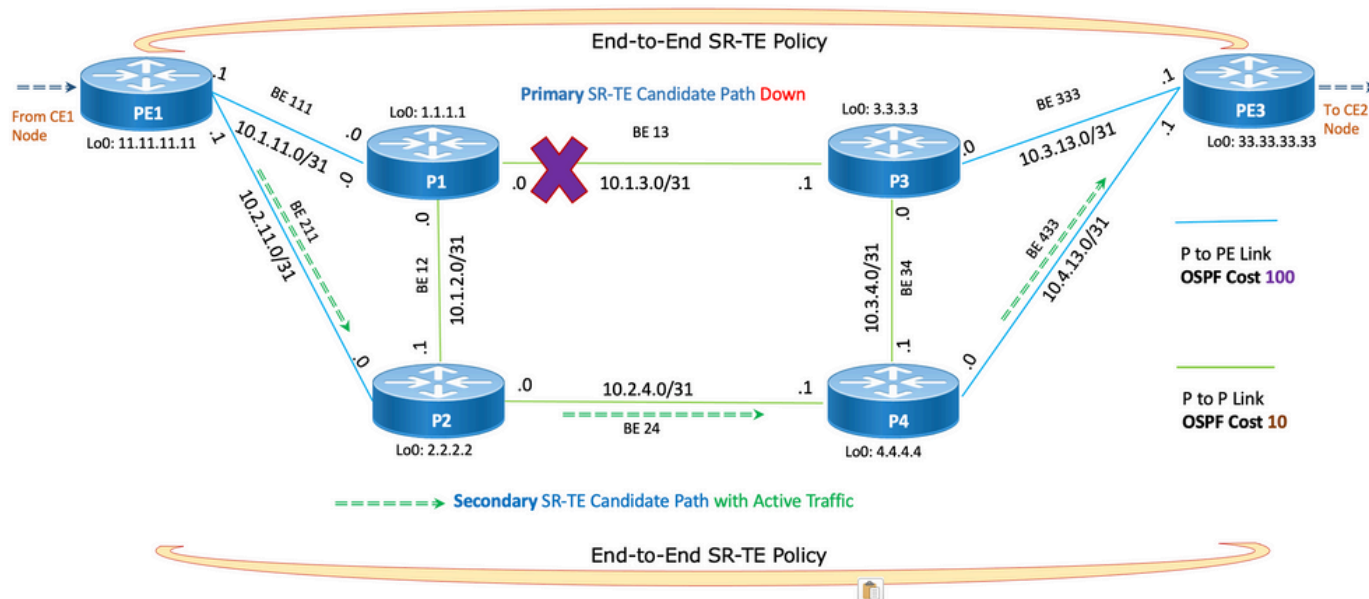


Figura 3: Cenário de tráfego de failover via caminho do candidato secundário SR-TE

Etapas de resumo:

1. No ponto de falha:

- A camada I/BFD sinaliza o caminho principal até a FIB
- A FIB envia ao HW o caminho de backup estabelecido com TI-LFA
- Interrupção de tráfego esperada:
 - Link inativo: aprox. 50 ms
 - Perda de peer de BFD: tempo inativo de BFD + ~50 ms
- A troca de tráfego (peering) do OSPF por link perdido fica inativa

2. Todos os roteadores OSPF no domínio aprendem sobre a perda de SID através da inundação de Link State Advertisement (LSA)

3. No ponto inicial SR-TE PE1:

- Convergências de OSPF
- A lista de SID de caminho principal da política SR-TE é invalidada

- O caminho do candidato principal cai
- A lista de SID do caminho do candidato secundário é validada e torna-se ativa
- O tráfego é enviado por um caminho secundário sem nenhuma perda de tráfego de serviço

Reconvergência de falha de link - caminho principal de volta ao estado ativo

Enquanto isso, quando o link primário com falha é restaurado, o caminho primário original com preferência (200) se torna válido novamente e, assim, o ponto inicial PE1 executa o procedimento de seleção de caminho de política SR-TE, seleciona o caminho de candidato explícito válido com a preferência mais alta e atualiza sua tabela de encaminhamento com a lista de SID do caminho primário original. O tráfego de serviço que é direcionado para essa política SR é enviado no caminho PE1 > P1 > P3 > PE3 original novamente.

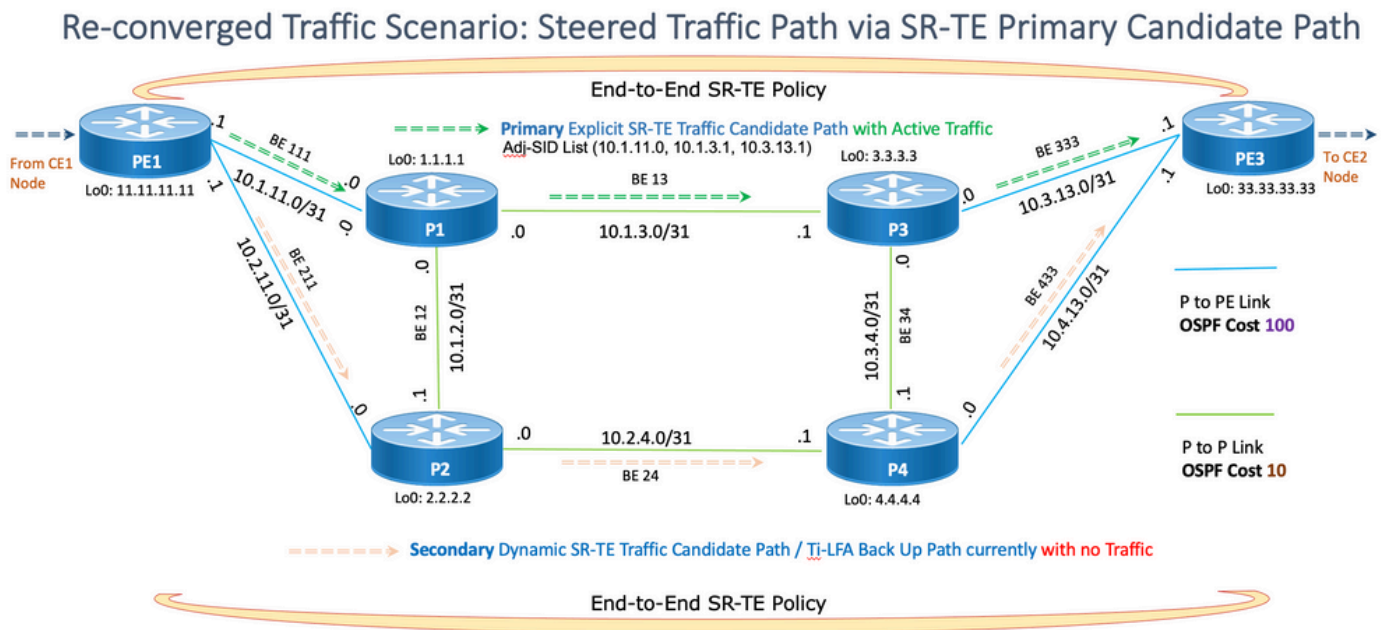
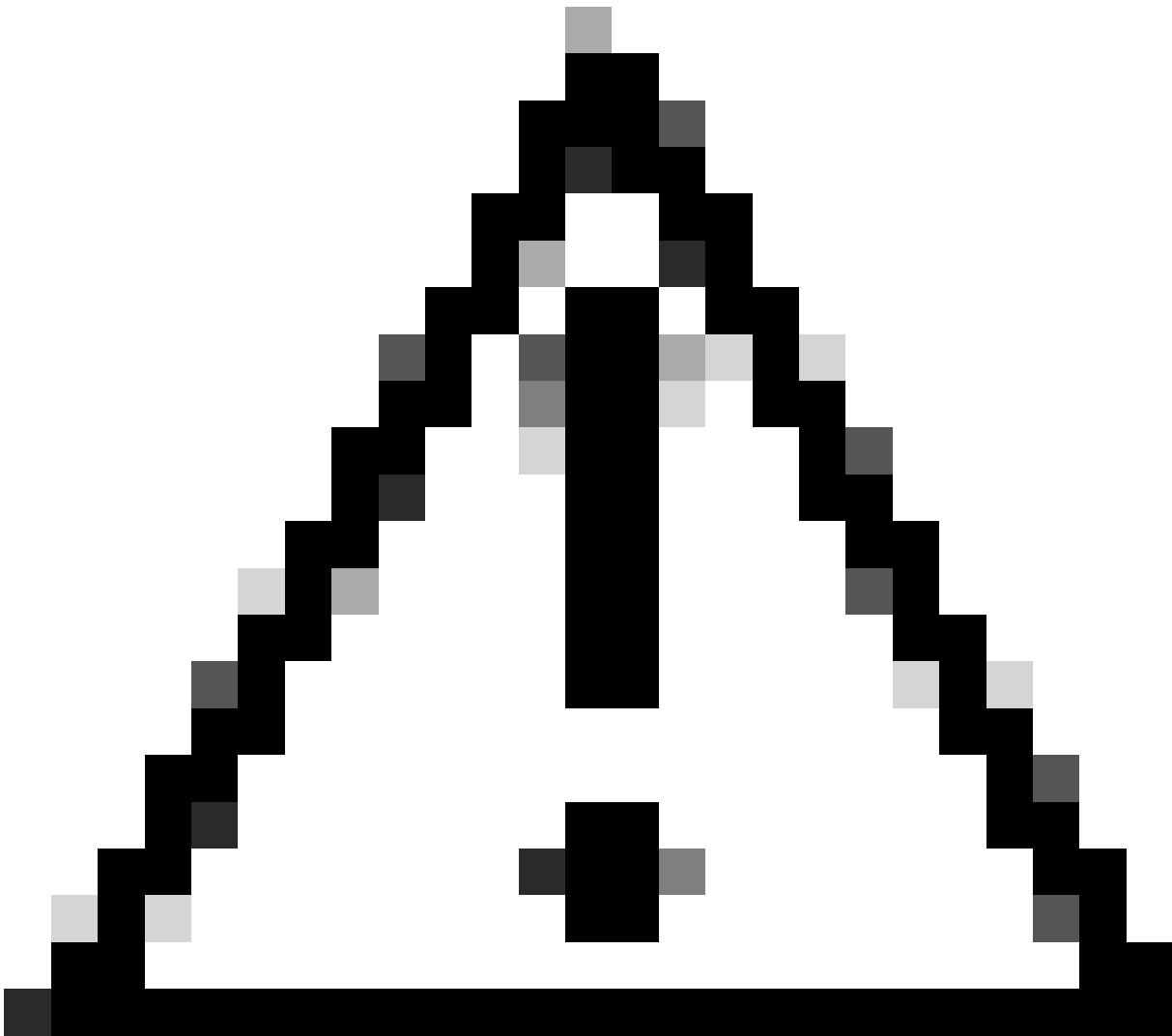


Figura 4: Cenário de tráfego reconvergado

Etapas de resumo:

1. A Camada 1/BFD sinaliza o caminho principal de backup e o OSPF é notificado.
2. O tráfego ainda é encaminhado através do caminho candidato de backup de política SR-TE.
3. Depois de um tempo, a lista SID do caminho principal do candidato da política SR-TE se torna válida por meio da inundação LSA do OSPF.
4. O tráfego é comutado do caminho do candidato de backup da política SR-TE para o caminho do candidato principal da política SR-TE com perda de tráfego zero.

Para concluir, esses cenários fornecem uma explicação teórica do processo de convergência e dos números de convergência ideais; no entanto, você precisa testar os números de convergência reais no laboratório que imitam a rede de produção e a configuração o mais próximo possível e acionam diferentes pontos de falha na rede que podem ser previstos.



Cuidado: observe que este documento explica apenas cenários de Proteção de link, uma vez que a Proteção de nó não funciona com caminhos explícitos de SR-TE se o caminho explícito definido tocar em nós intermediários. Isso ocorre porque o TI-LFA assume cada salto intermediário configurado como o nó de destino e, em caso de falha de qualquer um deles, não é possível resolver o destino final. Essa é uma limitação de tecnologia e não está restrita a nenhuma plataforma ou versão de imagem. A solução para essa limitação foi discutida na Parte 2 deste documento, conforme mencionado na seção Informações Relacionadas.

Software usado

O software usado para testar e validar a solução é o Cisco IOS®XR 7.3.2.

Informações Relacionadas

- Parte 2. [Mecanismo de convergência de caminho explícito baseado em política SR-TE com proteção de nó TI-LFA](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.