

Entender o redirecionamento rápido de IP LFA e LFA remoto

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Entender o MPLS](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como o IP Fast Reroute (FRR) fornece métodos de recuperação rápida em redes baseadas no Label Distribution Protocol (LDP).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

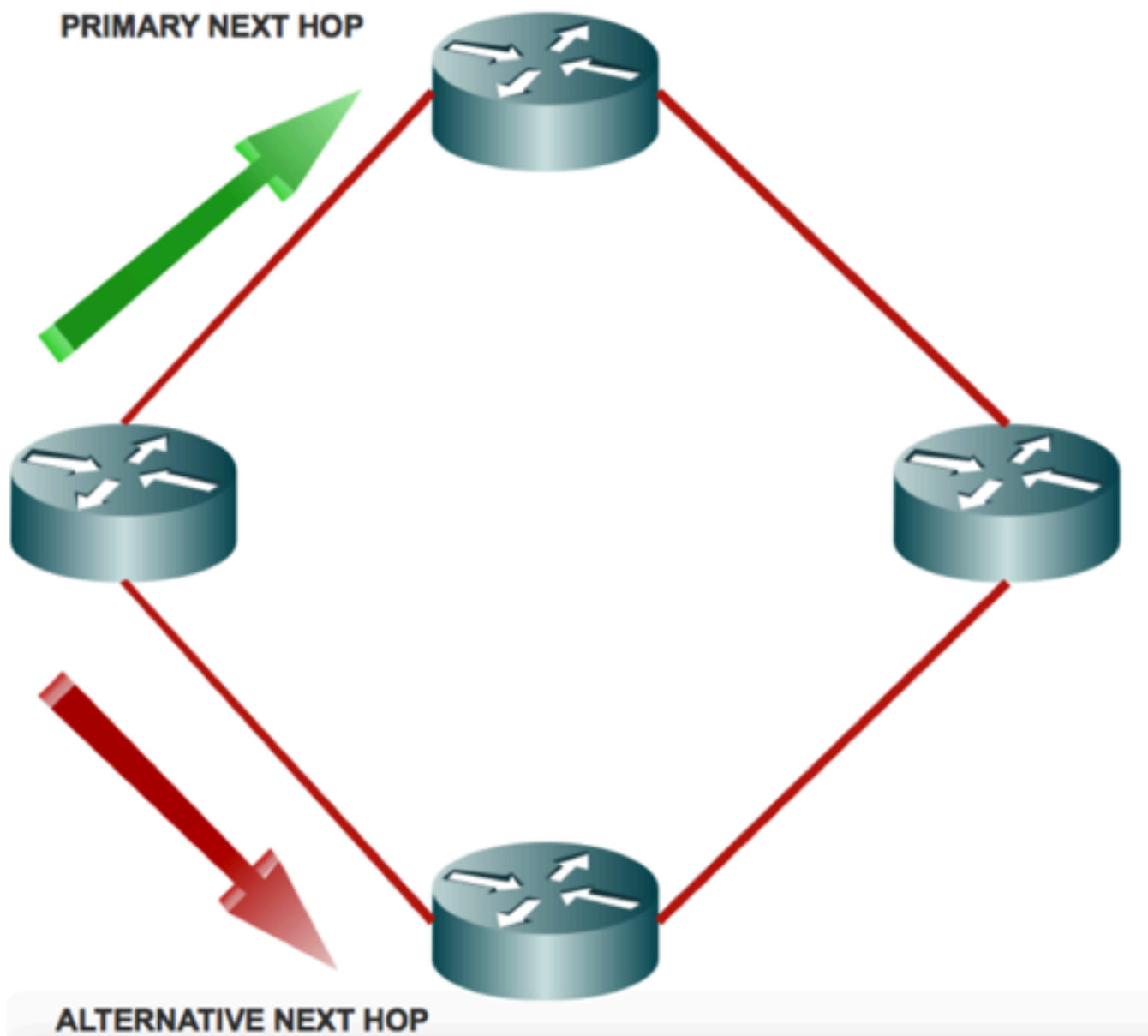
Informações de Apoio

Isso é muito mais simples de implementar. O Loop Free Alternate (LFA) é semelhante ao Multiprotocol Label Switching (MPLS) FRR, por exemplo, pré-instala o próximo salto de backup no plano de encaminhamento. As LFAs não introduzem extensões de protocolo e podem ser implementadas por roteador, o que as torna uma opção muito atraente.

Entender o MPLS

Opções de FRR:

O FRR de circuito alternativo (LFA - Loop Free Alternate) pré-computa um caminho alternativo sem loops e o instala no local de encaminhamento. O LFA é calculado com base na rota em igualdade.



LFA:

Desigualdade 1: $D(N,D) < D(N,S) + D(S,D)$

O caminho está livre de loops porque N melhor caminho não é através do roteador local. O tráfego enviado para o próximo salto de backup não é enviado de volta para S.

Caminho downstream:

Desigualdade 2: $D(N,D) < D(S,D)$

O roteador vizinho está mais próximo do destino do que o roteador local. A ausência de loops é garantida mesmo com várias falhas (se todos os caminhos de reparo forem caminhos downstream).

Proteção de nós:

Desigualdade 3: $D(N,D) < D(N,E) + D(E,D)$ N caminho para D não deve passar por E.

A distância do nó N ao prefixo através do próximo salto principal é estritamente maior que a distância ideal do nó N ao prefixo.

Proteção de link livre de loop para link de transmissão:

Desigualdade 4: $D(N,D) < D(N,PN) + D(PN,D)$

O link de S para N não deve ser o mesmo que o link protegido.

O link de N a D não deve ser o mesmo que o link protegido.

Vantagens do LFA e do rLFA:

- Configuração simplificada
- Proteção de link e nó
- Proteção de enlace e caminho
- Caminhos LFA
- Suporte para IP e LDP
- O LFA FRR é suportado com Equal Cost Multipath (ECMO)

Desvantagens do LFA e do rLFA:

- O LDP deve ser habilitado em todos os lugares
- LDP de destino habilitado em todos os lugares
- Nenhum outro mecanismo de túnel além do MPLS é suportado
- O nó PQ protege apenas o link e não o nó
- Os cálculos de nó PQ só são executados se houver caminhos desprotegidos para Prefixos protegíveis
- Uma sessão LDP de destino para o Nó PQ é criada somente se ainda não houver nenhuma saída
- Sem LFA remoto para cada link

LFA remoto (rLFA):

O LFA não oferece cobertura total e depende muito da topologia. O motivo é simples, por exemplo, em muitos casos, para fazer backup do próximo salto, o melhor caminho passa pelo roteador e calcula o próximo salto de backup.

Esse problema pode ser resolvido se você puder encontrar um roteador que esteja a mais de um salto de distância do roteador que calcula, a partir do qual o tráfego é encaminhado para o destino que não atravessa o link com falha e, em seguida, você pode encapsular o pacote para esse roteador.

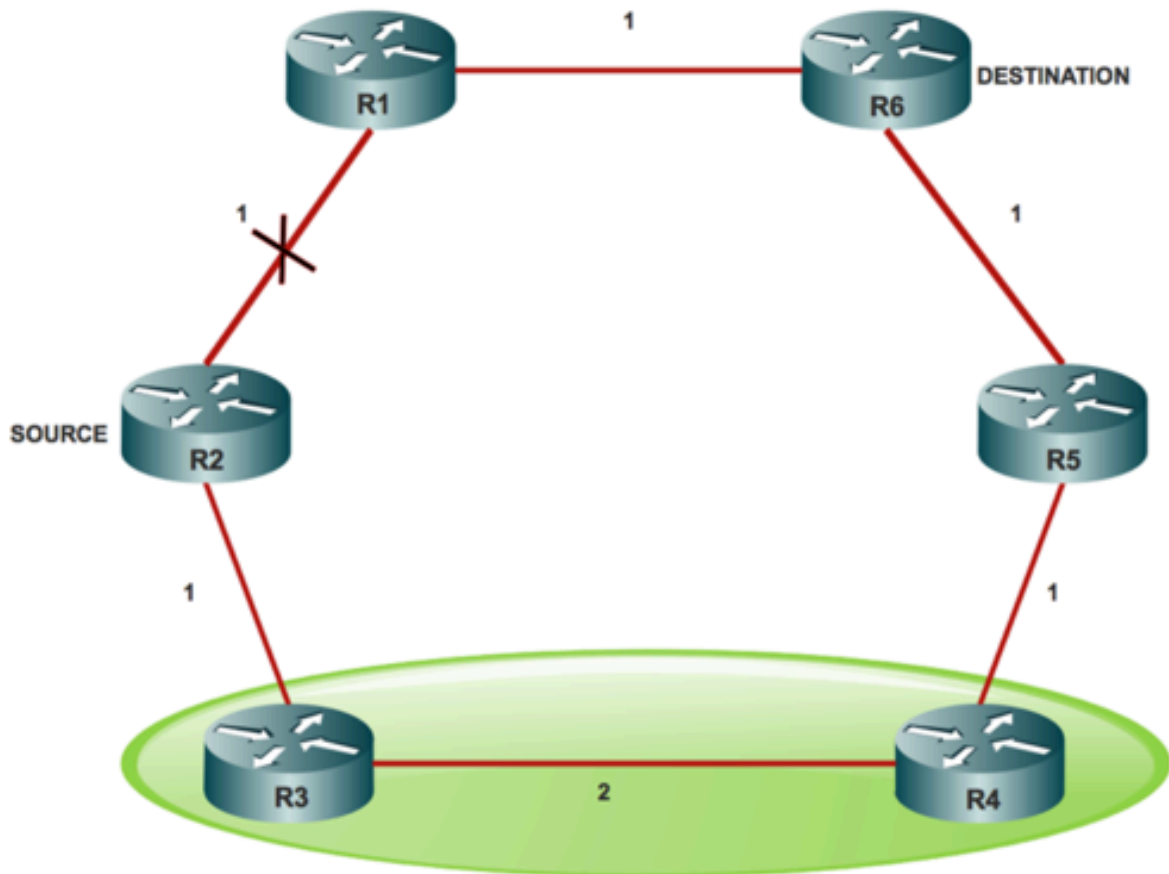
Esses tipos de caminhos de reparo multi-hop são mais complicados que os caminhos de reparo de salto único, pois são necessários cálculos para determinar se um caminho sai (para começar)

e depois um mecanismo para enviar o pacote a esse salto.

Examine um Point of Presence (POP) com uma topologia em anel de acordo com a estrutura em anel mencionada.

R3 não atende à desigualdade # 1 ($3 < 1 + 2$). Portanto, o melhor caminho de R3 é através do link com falha.

Se você encontrar um nó do qual o tráfego é encaminhado para o destino que não atravessa o link com falha e o envia para esse nó, então você pode obter o FRR que não causa um loop.



Espaço P:

O P-Space de um roteador em relação a um link protegido é o conjunto de roteadores alcançáveis a partir desse roteador específico com o uso dos caminhos mais curtos de pré-convergência, sem nenhum desses caminhos, que transita esse link protegido.

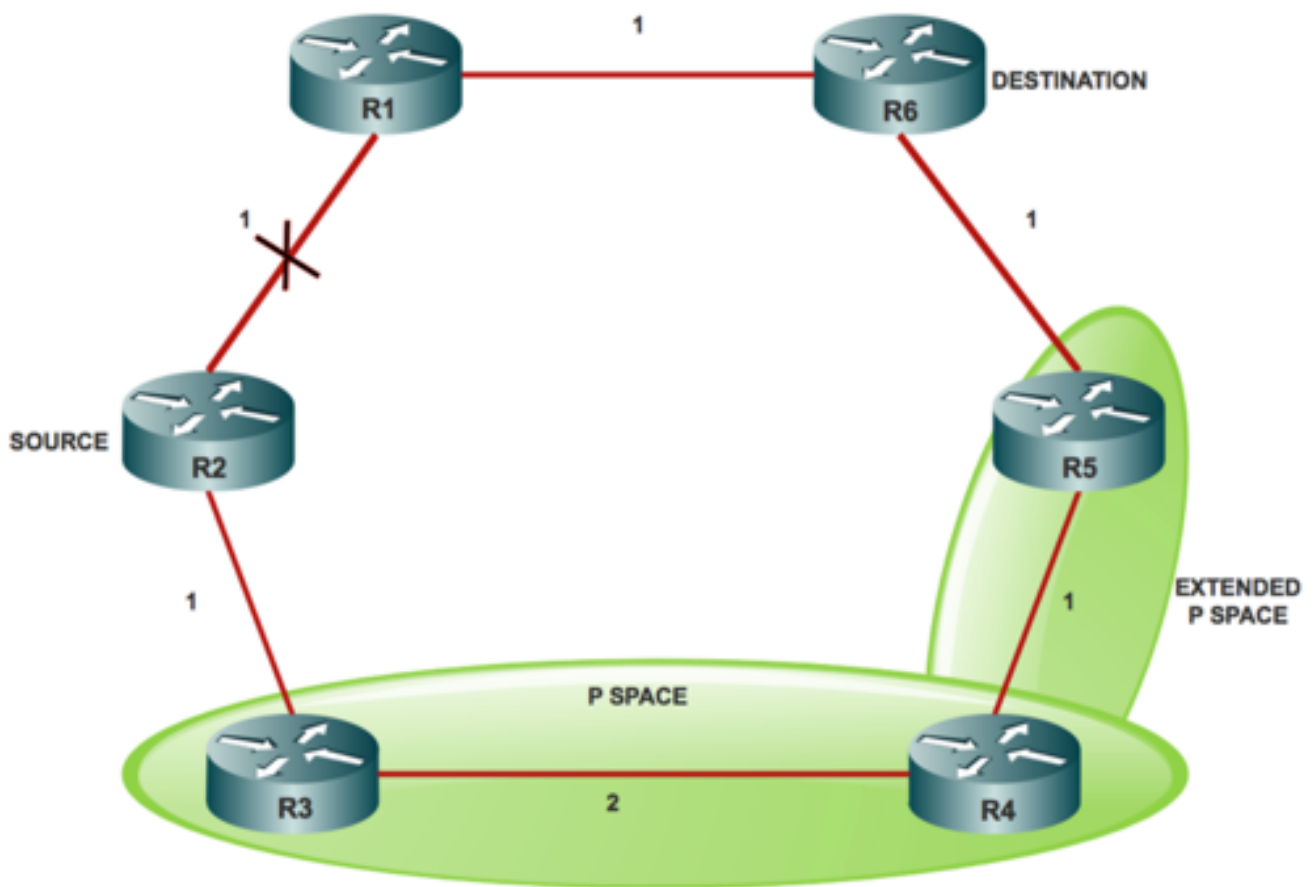
O P-Space é um conjunto de roteadores que o R2 (origem) pode acessar sem o uso do link R2 (S) - R1, que são os nós R3 (P-Space) e R4 (P-Space).

Espaço IP estendido:

O P-Space estendido do roteador que protege em relação ao link protegido é a união do P-Space dos vizinhos nesse conjunto de vizinhos, em relação ao link protegido, o que o torna a união dos

P-Spaces dos vizinhos nesse conjunto de vizinhos em relação ao link protegido.

O P-Space Estendido contém os roteadores que são R2 - vizinho direto, R3 - podem alcançar sem o uso do link R2 - R1, que é o nó R4 e R5. O ponto atrás do Espaço IP estendido é que ele ajuda a aumentar a cobertura.



|

Q-Espaço:

Q-Espaço de um roteador em relação a um link protegido é o conjunto de roteadores a partir do qual esse roteador específico que pode ser acessado sem nenhum caminho (que inclui divisões de ECMP) transita por esse link protegido.

O Q-Space contém os roteadores que normalmente acessam R6 sem o uso do link R1 de R2 (S), que são os nós R1, R5 e R4.

Nó PQ:

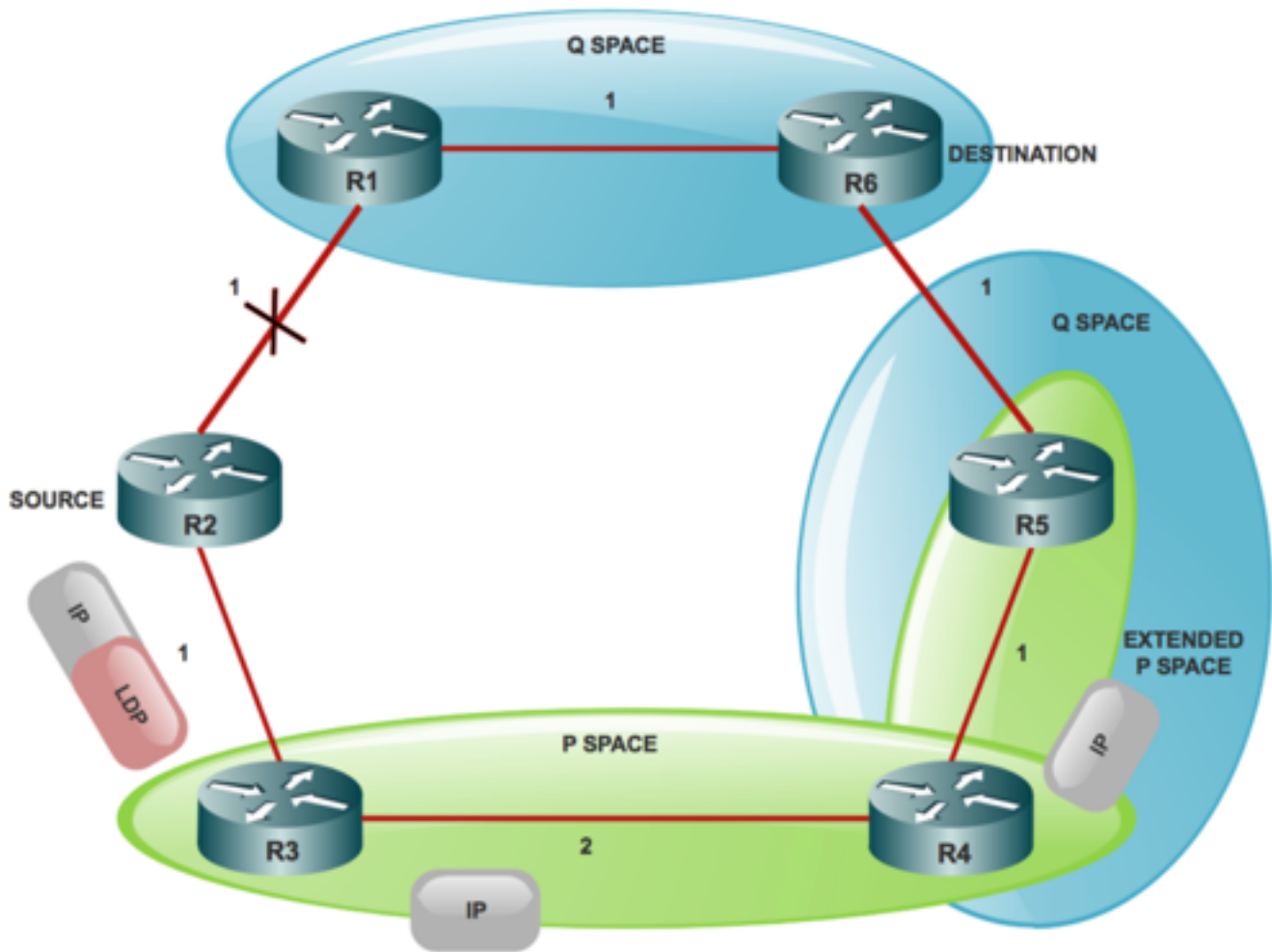
Um roteador que seja P-Space Estendido e Q-Space é um nó PQ.

Qualquer roteador que seja um nó PQ pode ser um candidato LFA remoto. O roteador candidato para o qual R2 (S) pode enviar o pacote, encaminha o pacote para o destino e não atravessa o link R2(S) R1. Nesse caso, R4 e R5 são os nós PQ e são considerados candidatos LFA remotos para R2 (S).

Há várias maneiras de criar um túnel para o tráfego, como IPinIP, GRE e LDP. No entanto, a forma mais comum de implementação é o túnel LDP.

Em caso de proteção de tráfego IP:

Se você proteger o tráfego IP, o R2 (s) enviará um rótulo LDP na parte superior do pacote IP para acessar R4 (suponha que o R2 (S) ataca o R4) como um nó LFA remoto. Quando R3 recebe o pacote, ele o encaminha para R4 como um pacote IP simples devido ao comportamento normal do PHP. Quando R4 recebe o pacote destinado a R6 (D), ele encaminha o pacote upstream para o nó R5.

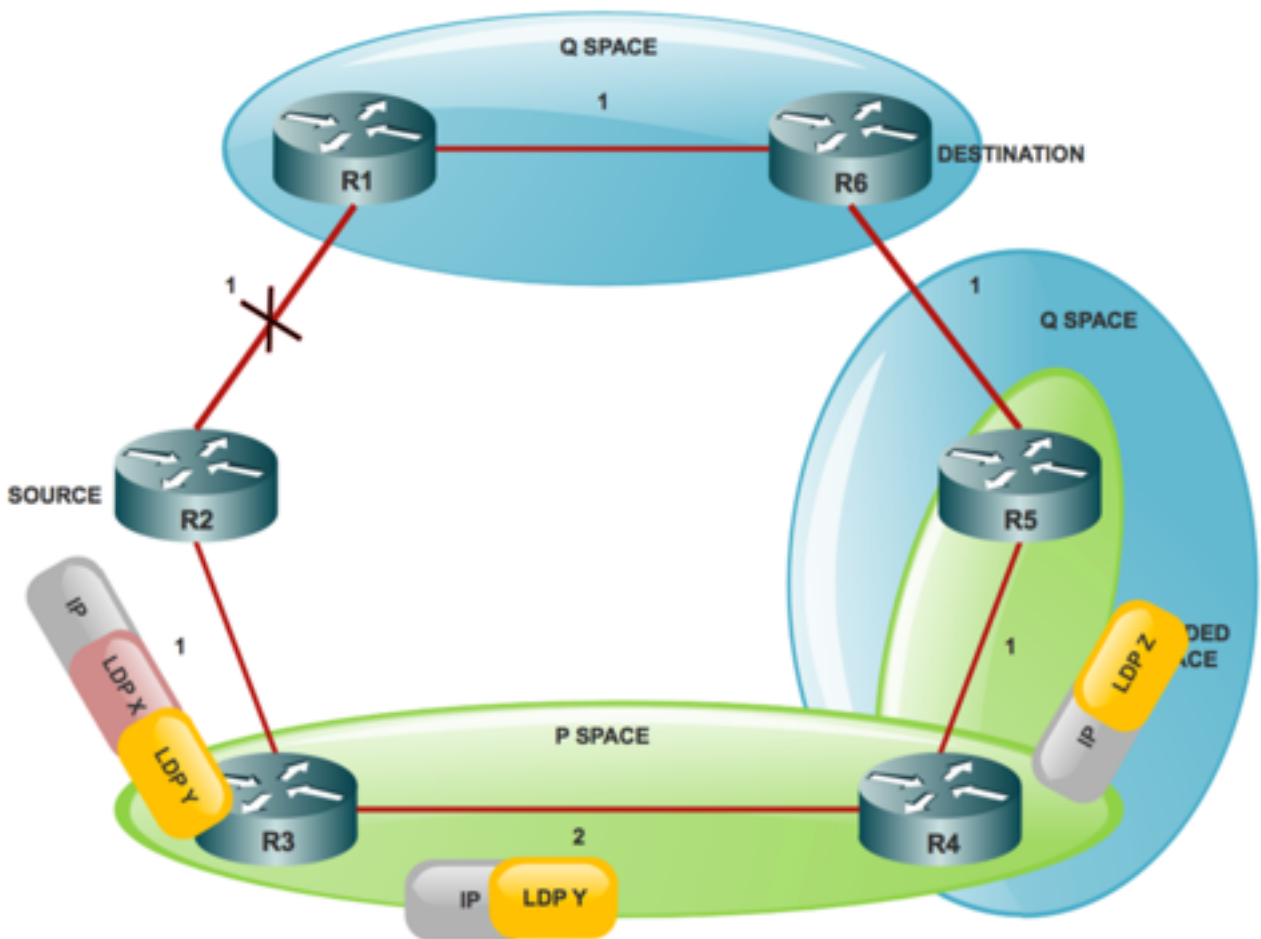


No caso de proteção de tráfego LDP:

Nesse caso, uma pilha que consiste em dois rótulos LDP é usada por R2(S).

O rótulo LDP externo x, é o rótulo para acessar R4 e o rótulo LDP interno Y, é o rótulo para acessar R6 (D) de R4.

Agora a pergunta é: como o R2 (S) sabe que o R4 usa o rótulo LDP Y para enviar tráfego para o R6(D). Para que o nó protetor para nó saiba qual rótulo um nó PQ usa para encaminhar o destino (D), ele deve estabelecer uma sessão LDP direcionada com umNó PQ para fazer com que o FEC rotule o mapeamento. Portanto, você sabe que as sessões TLDP devem ser ativadas em todos os nós para o LFA remoto.

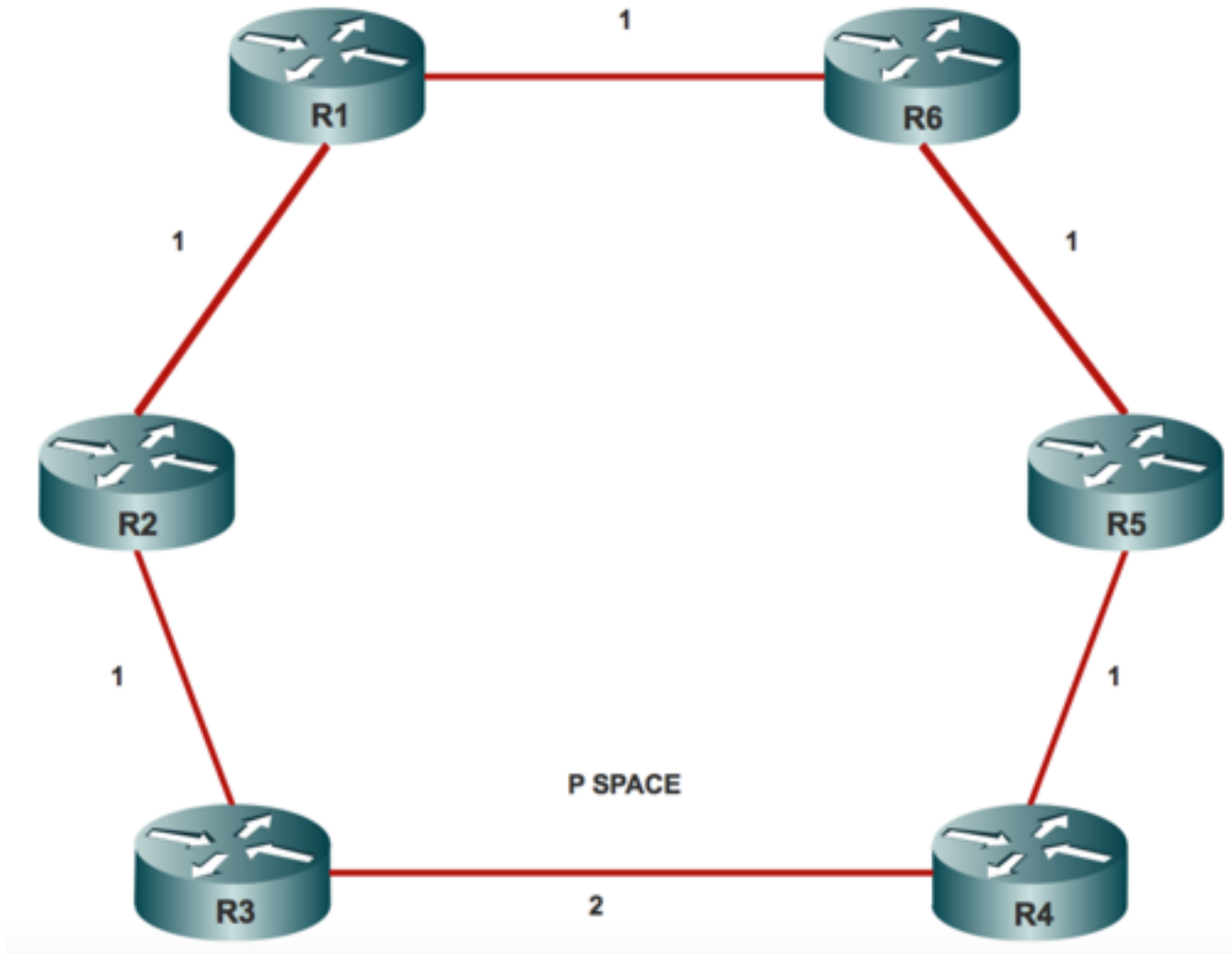


Benefícios do rLFA em relação ao LFA:

- O rLFA melhora a cobertura do LFA em anel e topologia mal engrenada
- Aumenta a consistência quando o ponto final do túnel remoto é selecionado
- Pode trabalhar com RSVP com pouquíssima sobrecarga operacional e computacional
- O RSVP pode ser usado para complementar o LFA/eLFA e vice-versa
- Quando usado em conjunto com o LDP MPLS, não há necessidade de protocolo adicional no plano de controle
- O plano de dados para MPLS usa a pilha de rótulos para criar um túnel dos pacotes para o nó PQ a partir daí
- O tráfego flui para o destino e não retorna à origem ou atravessa o link protegido

Configurar

Diagrama de Rede



Configurações

Detalhes do laboratório para proteger o tráfego LDP:

Configuração do ISIS:

```
router isis 20
net 20.0000.0000.0005.00
is-type level-1
metric-style wide level-1
fast-reroute per-prefix level-1 route-map LFA >>>>>>>>>> rLFA Configuration
fast-reroute remote-lfa level-1 mpls-ldp >>>>>>>>>>>>>>>> rLFA Configuration
mpls ldp autoconfig level-1
```

Configuração obrigatória de MPLS:

```
mpls ldp explicit-null
fast-reroute remote-lfa level-1 mpls-ldp
mpls ldp router-id Loopback0
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para exibir os túneis LFA remotos para ISIS:

```
R1#show isis fast-reroute remote-lfa tunnels
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
```

```
No time source, *11:28:59.528 UTC Wed Jan 3 2018
```

Tag 20 - Túneis RRF Remote-LFA:

```
MPLS-Remote-Lfa1: use Gi2/0, nexthop 10.3.4.4, end point 10.0.0.5
```

```
MPLS-Remote-Lfa2: use Gi3/0, nexthop 10.3.3.3, end point 10.0.0.5
```

Para verificar a programação do Cisco IOS para um determinado prefixo, execute o CLI:

```
R1#show ip cef 10.0.0.5
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
```

```
No time source, *11:32:04.857 UTC Wed Jan 3 2018
```

```
10.0.0.4/32
```

```
  nexthop 10.31.32.32 GigabitEthernet3/0 label [17|17]
```

```
    repair: attached-nexthop 10.3.4.4 GigabitEthernet2
```

```
  nexthop 10.3.4.4 GigabitEthernet2/0 label [17|17]
```

```
    repair: attached-nexthop 10.3.3.3 GigabitEthernet3
```

Nesta saída, você pode ver os rótulos principal e de backup [17|17] respectivamente. O caminho de reparo passa por um túnel LFA remoto. Não é necessário que todos os prefixos sejam protegidos com o uso de um túnel LFA remoto. Com base na possibilidade de looping, a lógica LFA escolhe passar por um caminho de backup normal ou um caminho de backup em túnel.

```
R1#show ip route repair-paths 10.0.0.8
```

```
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
```

```
No time source, *11:39:07.467 UTC Wed Jan 3 2018
```

```
Routing entry for 10.0.0.8/32
```

```
Known via "isis", distance 115, metric 30, type level-1
```

```
  Redistributing via isis 20
```

```
  Last update from 10.3.4.4 on GigabitEthernet2/0, 1d12h ago
```

```
  Routing Descriptor Blocks:
```

```
    * 10.3.4.4, from 10.10.0.81, 1d12h ago, via GigabitEthernet2/0
```

```
      Route metric is 30, traffic share count is 1
```

```
      Repair Path: 10.10.0.42, via MPLS-Remote-Lfa2
```

```
    [RPR]10.0.0.4, from 10.0.0.8, 1d12h ago, via MPLS-Remote-Lfa2
```

```
      Route metric is 20, traffic share count is 1
```

Troubleshoot

No momento, não há informações específicas de solução de problemas disponíveis para essa configuração.

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.