Comprensione di LFA e Remote LFA IP Fast Reroute

Sommario

Introduzione

In questo documento viene descritto come IP Fast Reroute (FRR) fornisce metodi di recupero rapidi nelle reti LDP (Label Distribution Protocol).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

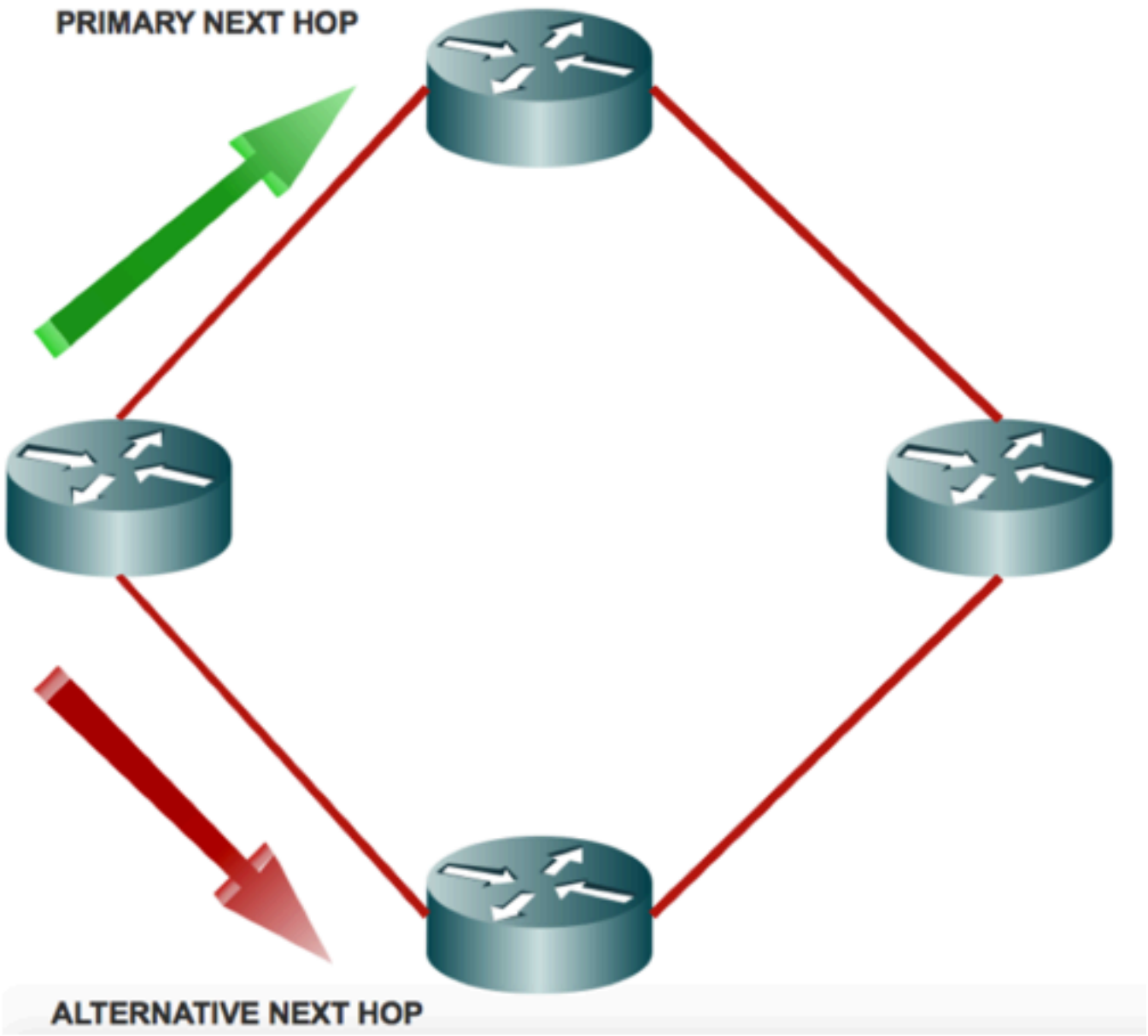
Premesse

L'implementazione è molto più semplice. Il protocollo LFA (Loop Free Alternate) è simile al protocollo MPLS (Multiprotocol Label Switching) FRR, ad esempio, preinstalla l'hop successivo di backup sul piano di inoltro. Le LFA non introducono estensioni del protocollo e possono essere implementate per router, il che la rende un'opzione molto interessante.

Informazioni su MPLS

Opzioni FRR:

La funzione LFA (Loop Free Alternate) FRR pre-calcola un percorso alternativo privo di loop e si installa nella posizione di inoltro. LFA viene calcolato in base alla route in uguaglianza.



LFA:

Disuguaglianza 1: D(N,D) < D(N,S) + D(S,D)

Percorso privo di loop perché il percorso migliore non è un router locale. Il traffico inviato al backup dell'hop successivo non viene rinviato al server.

Percorso downstream:

Disuguaglianza 2: D(N,D) < D(S,D)

Il router adiacente è più vicino alla destinazione del router locale. L'assenza di loop è garantita

anche in caso di più errori (se tutti i percorsi di riparazione sono a valle).

Protezione dei nodi:

Disuguaglianza 3: D(N,D) < D(N,E) + D(E,D) Il percorso N verso D non deve passare per E.

La distanza tra il nodo N e il prefisso attraverso l'hop successivo primario è strettamente maggiore della distanza ottimale tra il nodo N e il prefisso.

Protezione collegamento senza loop per collegamento broadcast:

Disuguaglianza 4: D(N,D) < D(N,PN) + D(PN,D)

Il collegamento da S a N non deve essere lo stesso del collegamento protetto.

Il collegamento da N a D non deve essere lo stesso del collegamento protetto.

Vantaggi di LFA e rLFA:

- Configurazione semplificata
- Protezione collegamenti e nodi
- Protezione collegamenti e percorsi
- percorsi LFA
- Supporto per IP e LDP
- LFA FRR è supportato con Equal Cost Multipath (ECMO)

Svantaggi delle ZLS e delle ZLS:

- LDP deve essere abilitato ovunque
- LDP destinazione abilitata ovunque
- Non sono supportati altri meccanismi di tunnel oltre a MPLS
- Il nodo PQ protegge solo il collegamento e non il nodo
- I calcoli del nodo PQ vengono eseguiti solo se sono presenti percorsi non protetti per i prefissi da proteggere
- Una sessione LDP di destinazione al nodo PQ viene creata solo se non ne esiste ancora una
- Nessuna LFA remota per collegamento

LFA (Remote LFA):

LFA non fornisce una copertura completa ed è molto dipendente dalla topologia. Il motivo è semplice: ad esempio, in molti casi per eseguire il backup dell'hop successivo, il percorso migliore passa attraverso il router e calcola il backup dell'hop successivo.

Per risolvere il problema, è possibile trovare un router che si trovi a più di un hop di distanza dal router che esegue i calcoli, da cui il traffico viene inoltrato alla destinazione che non attraversa il collegamento in cui si è verificato l'errore, e quindi eseguire il tunnel del pacchetto verso tale router.

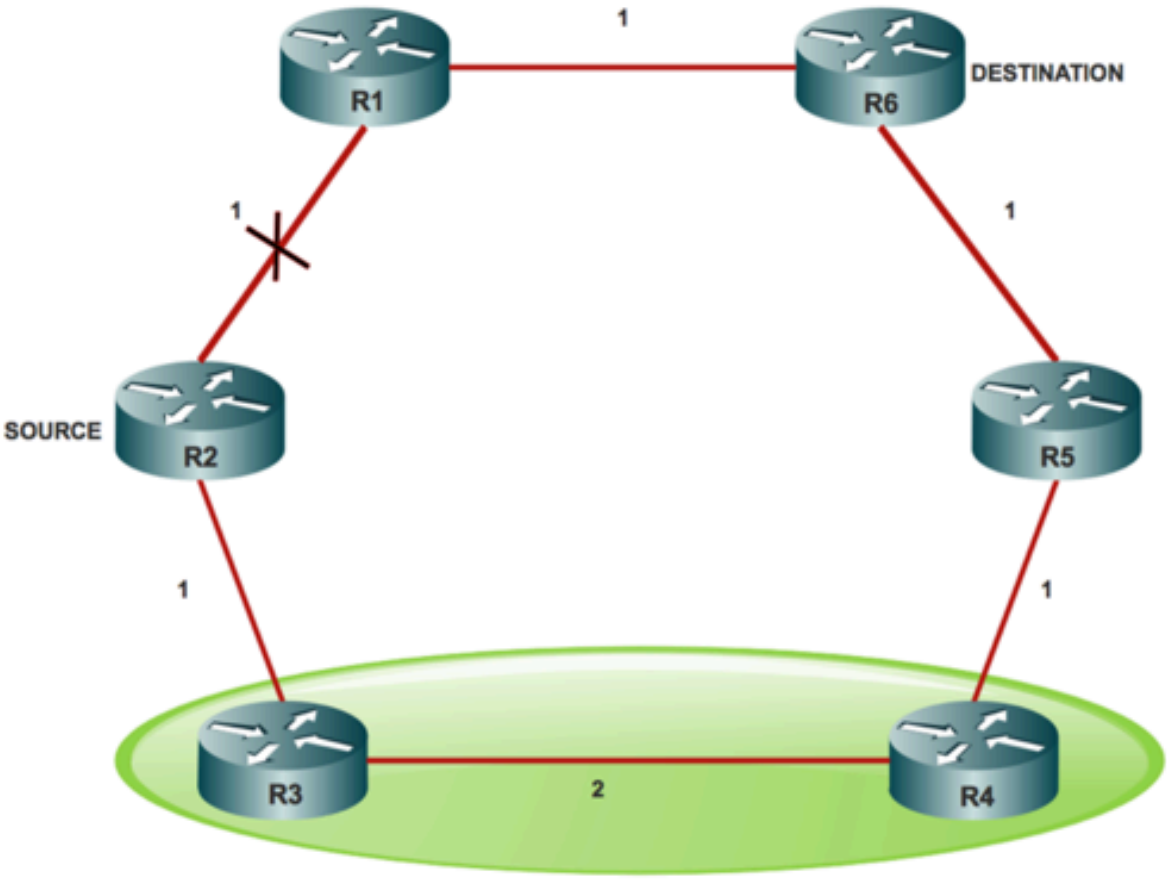
Questi tipi di percorsi di ripristino multi-hop sono più complessi dei percorsi di ripristino single-hop in quanto sono necessari calcoli per determinare se un percorso esiste (per iniziare) e quindi un meccanismo per inviare il pacchetto a tale hop.

Osservare un punto di presenza (POP) con untopologia degli anelli secondo la struttura degli

anelli citata.

R3 non soddisfa la disuguaglianza # 1 (3 < 1 + 2). Quindi il miglior percorso per R3 è attraverso il collegamento fallito.

Se si trova un nodo dal quale il traffico viene inoltrato alla destinazione che non attraversano il collegamento non riuscito e lo invia a tale nodo, è possibile ottenere FRR che non causa un loop.



Spazio P:

Lo spazio P di un router in relazione a un collegamento protetto è l'insieme di router raggiungibili da quel router specifico con l'uso dei percorsi più brevi pre-convergenza, senza alcuno di questi percorsi, che attraversano quel collegamento protetto.

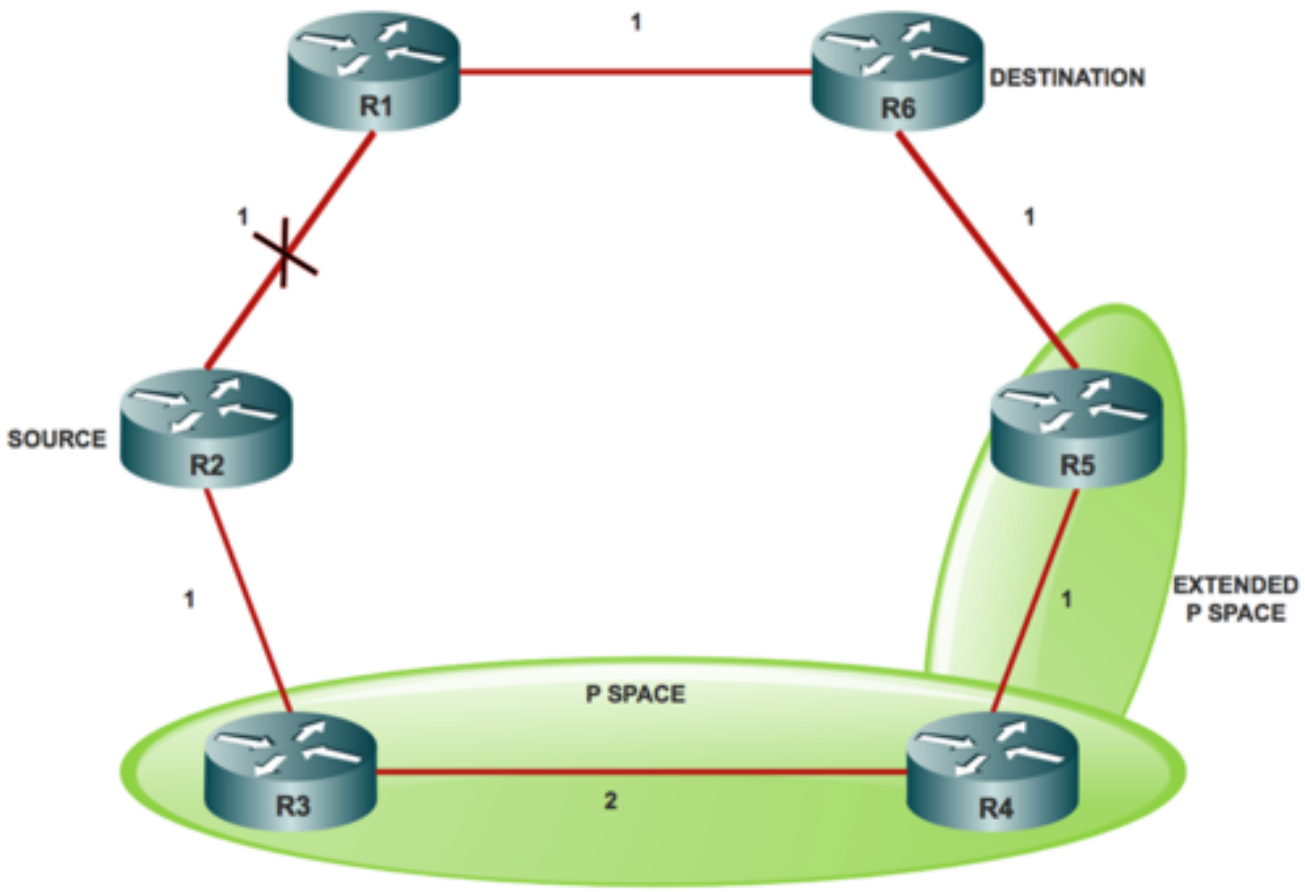
P-Space è un insieme di router che R2 (origine) può raggiungere senza l'uso del collegamento R2 (S) - R1, che è il nodo R3 (P-Space) e R4 (P-Space).

Spazio P esteso:

Lo spazio P esteso del router che protegge rispetto al collegamento protetto è l'unione dello spazio P dei vicini in quel set di vicini, rispetto al collegamento protetto, che lo rende l'unione degli spazi P dei vicini in quel set di vicini rispetto al collegamento protetto.

Lo spazio P esteso contiene i router che sono R2 - router adiacente diretto, R3 - raggiungibili

senza l'uso del collegamento R2 - R1 che è un nodo R4 e R5. Il punto dietro lo spazio P esteso è che aiuta ad aumentare la copertura.



Spazio Q:

Lo spazio Q di un router rispetto a un collegamento protetto è il set di router da cui quel router specifico può essere raggiunto senza alcun percorso (che include gli split ECMP) e attraversa quel collegamento protetto.

Q-Space contiene i router che normalmente raggiungono R6 senza l'uso del collegamento R2 (S) R1, che è costituito dai nodi R1, R5 e R4.

Nodo PQ:

Un router che è sia P-Space esteso che Q-Space è un nodo PQ.

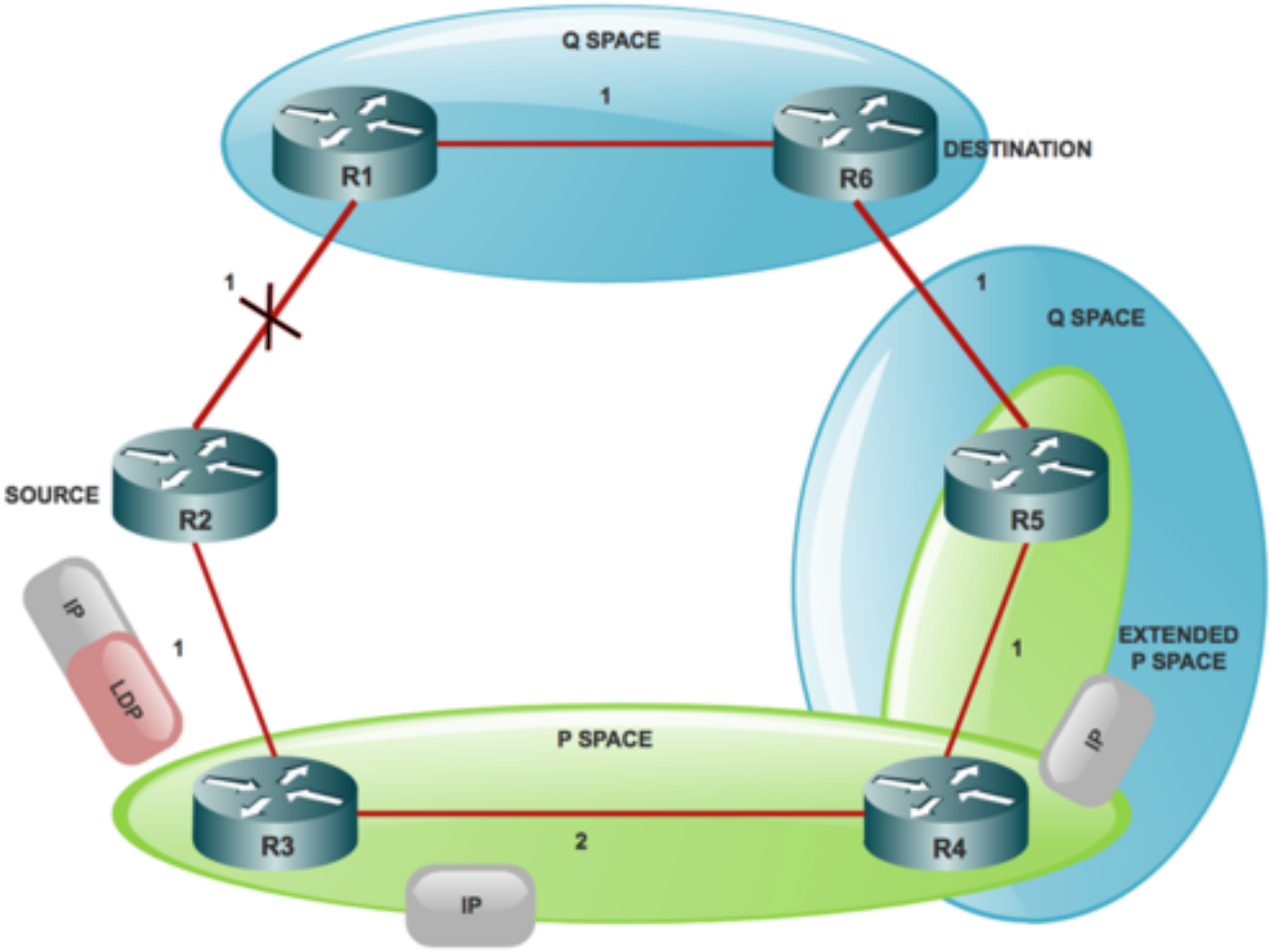
Qualsiasi router che sia un nodo PQ può essere un candidato LFA remoto. Il router candidato a cui R2 (S) può inviare il pacchetto, lo inoltra alla destinazione e non attraversa il collegamento di R2(S) R1. In questo caso, R4 e R5 sono i nodi PQ e sono considerati candidati LFA remoti per R2 (S).

Sono disponibili diversi modi per eseguire il tunnel del traffico, ad esempio IPinIP, GRE e LDP. Tuttavia, la forma più comune di implementazione è il tunnel LDP.

In caso di protezione del traffico IP:

Se si protegge il traffico IP, R2 (s) spinge un'etichetta LDP sopra il pacchetto IP per raggiungere R4 (si supponga R2 (S) picchetto R4) come nodo LFA remoto. Quando R3 riceve il pacchetto, lo

inoltra a R4 come pacchetto IP normale a causa del normale comportamento del PHP. Quando R4 riceve il pacchetto destinato a R6 (D), inoltra il pacchetto a monte verso il nodo R5.

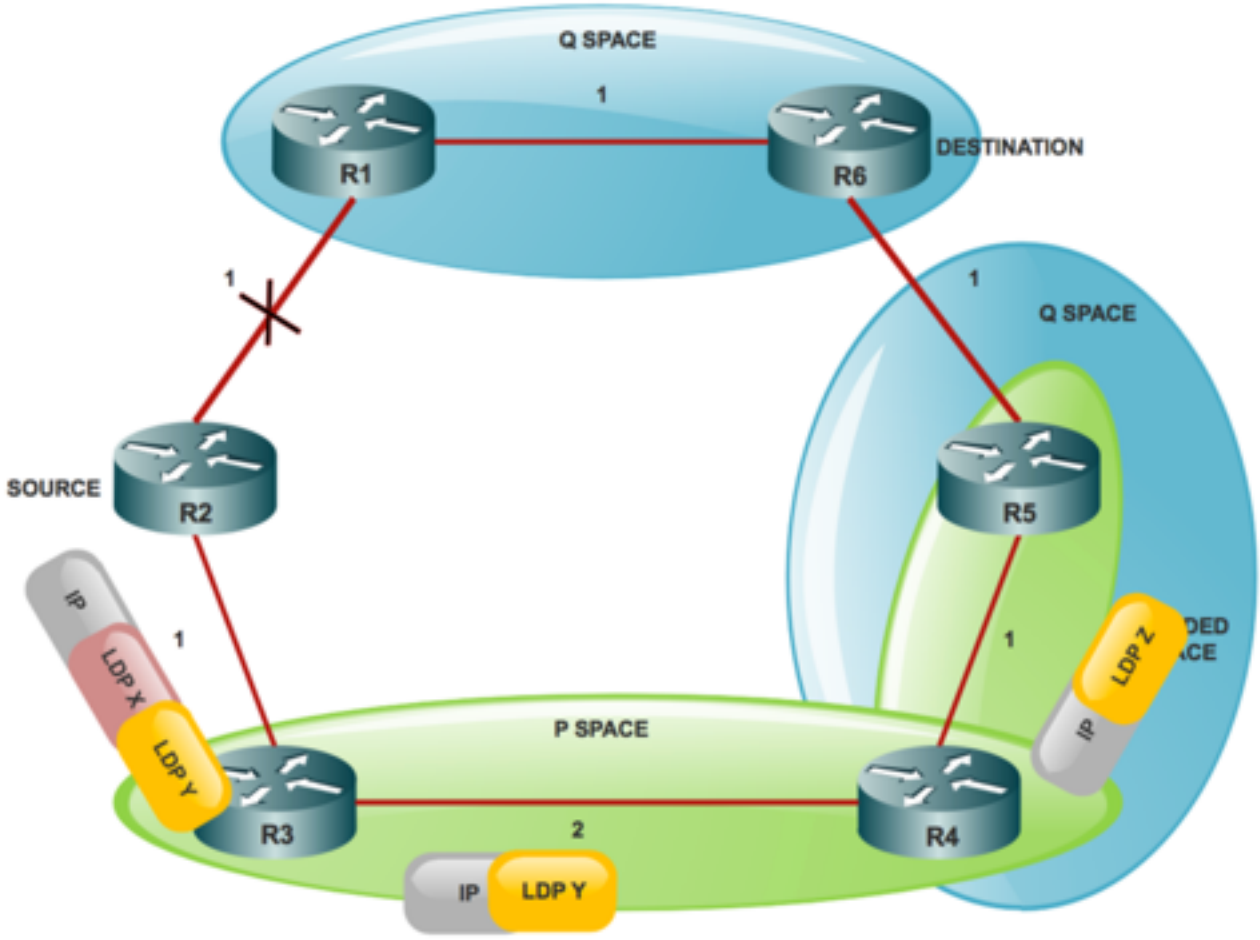


In caso di protezione del traffico LDP:

In questo caso R2(S) utilizza uno stack costituito da due etichette LDP.

Etichetta LDP esterna x, è l'etichetta per raggiungere R4 e etichetta LDP interna Y, è l'etichetta per raggiungere R6 (D) da R4.

Ora la domanda è: come fa R2 (S) a sapere che R4 usa l'etichetta LDP Y per inviare traffico verso R6(D)? Affinché il nodo di protezione conosca l'etichetta utilizzata da un nodo PQ per inoltrare la destinazione (D), è necessario stabilire una sessione LDP di destinazione con unPQ per ottenere il mapping FEC-etichetta. È pertanto necessario abilitare le sessioni TLDP in tutti i nodi per Remote LFA.

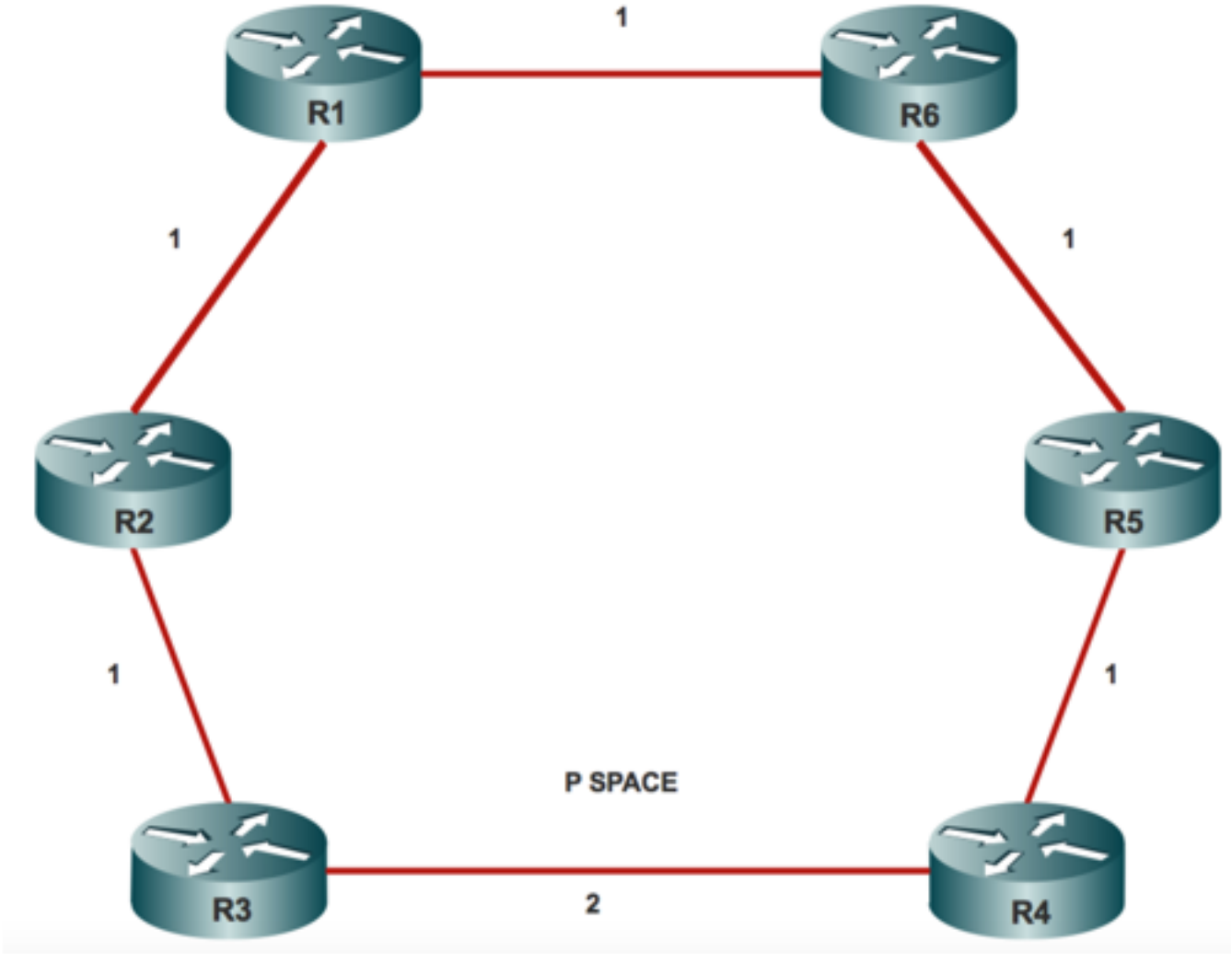


Vantaggi di rLFA rispetto a LFA:

- rLFA migliora la copertura LFA nella topologia ad anello e a maglia scarsa
- Migliora la coerenza quando viene selezionato l'endpoint del tunnel remoto
- Possibilità di lavorare con RSVP con un sovraccarico operativo e di calcolo molto ridotto
- L'RSVP può essere utilizzato per integrare LFA/eLFA e viceversa
- Se utilizzato in combinazione con MPLS LDP, non è necessario un protocollo aggiuntivo nel control plane
- Il piano dati per MPLS utilizza lo stack di etichette per eseguire il tunnel dei pacchetti al nodo PQ
- Il traffico passa alla destinazione e non torna all'origine o attraversa il collegamento protetto

Configurazione

Esempio di rete



Configurazioni

Dettagli del laboratorio per proteggere il traffico LDP:

Configurazione 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
```

Configurazione obbligatoria MPLS:

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per visualizzare i tunnel LFA remoti per l'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 - Per tunnel LFA remoti:

```
  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
```

Per controllare la programmazione Cisco IOS per un determinato prefisso, eseguire la 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
```

In questo output è possibile visualizzare rispettivamente le etichette primaria e di backup [17|17]. Il percorso di riparazione passa attraverso un tunnel LFA remoto. Non è necessario proteggere tutti i prefissi utilizzando un tunnel LFA remoto. In base alla possibilità di loop, la logica LFA sceglie di passare al normale percorso di backup o a un percorso di backup con tunneling.

```
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 10.0.0.81/32

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
```

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

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).