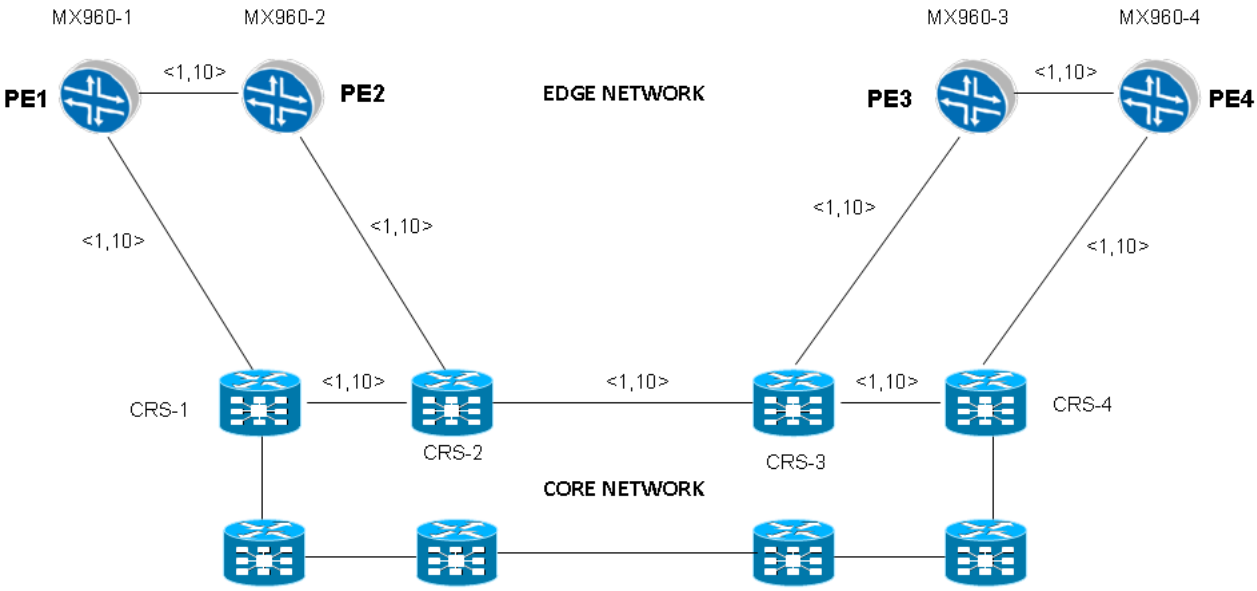
Il documento mette in evidenza uno studio ed ipotesi di flusso di traffico all'interno di una struttura backbone MPLS-IP in considerazione di parametri quali:

- metrica IT
- CSPF
- RSVP
- metodi di protezione su base:
  - link-protection
  - node-protection

Il design del backbone preso in considerazione presenta router MX960 Juniper come PE (Provider Edge) e CRS Cisco come P (router di transito)



<1,10> = metric IT = 1 ; bandwidth = 10

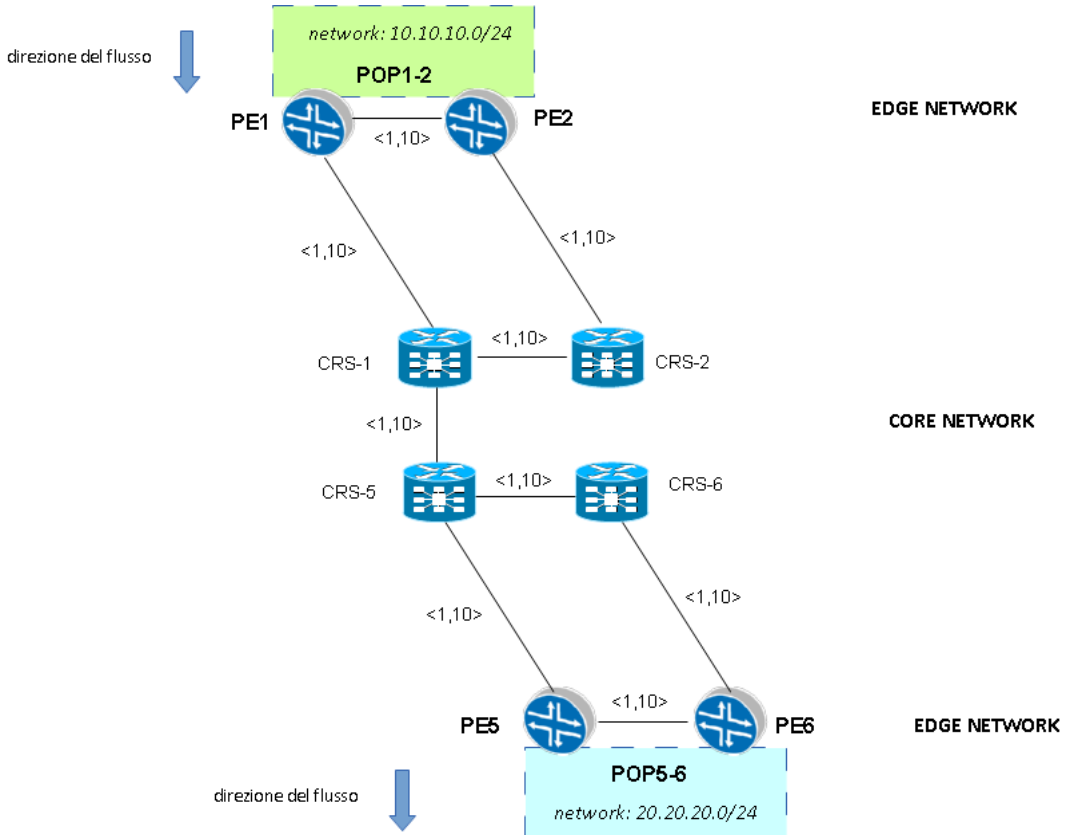
- EDGE: MX960 JUNIPER Networks con ruolo di router PE sorgente e destinazione di flussi di traffico
- CORE: CRS CISCO System con ruolo di router di transito.

Considerazioni a livello fisico:

- costo (metrica IT) è data dalla seguente configurazione:
  - interfaccia di collegamento link = TenGigEth = 10 Gbit/s
  - **auto-cost** reference bandwith 100000 = reference bandwith = 100000 Mbit = 100.000.000.000 / 10.000.000.000 = cost = 10

- metrica IGP = metrica IT
- la banda per ciascun link backbone è identica = 10 Gbit/s
- nel grafo con il parametro <1,10> si intende metrica = 1 , BW = 10 (10 Gbit/s)

ipotesi: flusso di traffico da POP 1-2 e POP 5-6 (come da diagramma seguente)



Considerazioni:

- la banda di 10 Gbit/s omogenea per tutto il backbone dovrebbe garantire qualunque richiesta da parte del flusso di traffico sorgente in termini di banda disponibile e/o altri parametri che possono influenzare il suo instradamento; per parametri si intendono ad es. banda equivalente, priorità, recupero in caso di guasto, qos, etc...
- Nel nostro caso i parametri che prenderemo in considerazione sono metrica IT e banda disponibile.
- i tunnel TE sono in configurazione dinamica (algoritmo CSPF constrained shortest path first)

Caratteristiche di funzionamento dell'algoritmo CSPF:

- obiettivo principale è la selezione di un solo path tra nodo sorgente e nodo destinazione
- viene applicato dal nodo di ingresso del flusso di traffico su base metrica IT minima e massimo valore di banda disponibile
- eliminazione dalla topologia di rete i collegamenti che non soddisfano i vincoli (ad esempio il vincolo di banda); nel nostro caso però abbiamo supposto che una banda = 10 Gbit/s riesca a soddisfare il vincolo.

Altra nota importante da sottolineare è che se entrambi i router MX960 operassero contemporaneamente ci troveremmo ad avere due LSP indipendenti tra loro (i nodi sorgente del tunnel IT sarebbero diversi) secondo questo schema:

in cui entrambi i tunnel TE sarebbero interessati al trasporto del flusso di traffico.

Si evince che per ogni coppia di router MX960 IDC uno solo ha il ruolo di primario mentre l'altro ha ruolo di router secondario (backup)

Per convenzione in questo documento si ipotizza:

- MX960-1 : router primario
- MX960-2 : router secondario

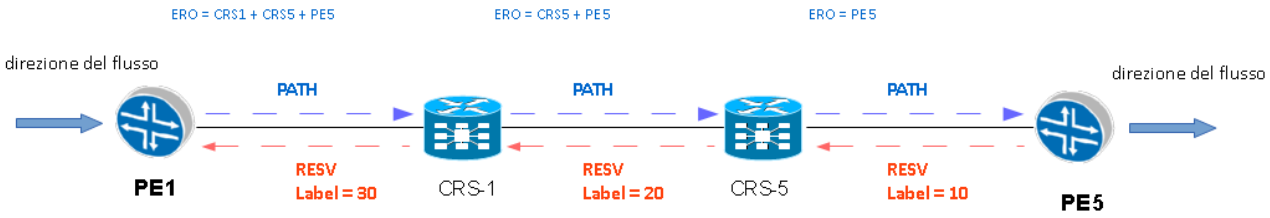
Il percorso selezionato dall'algoritmo on-line CSPF è il primo LSP [PE1 → CRS1 → CRS5 → PE2]; tutti gli altri percorsi avrebbero metrica IT maggiore rispetto a 30.

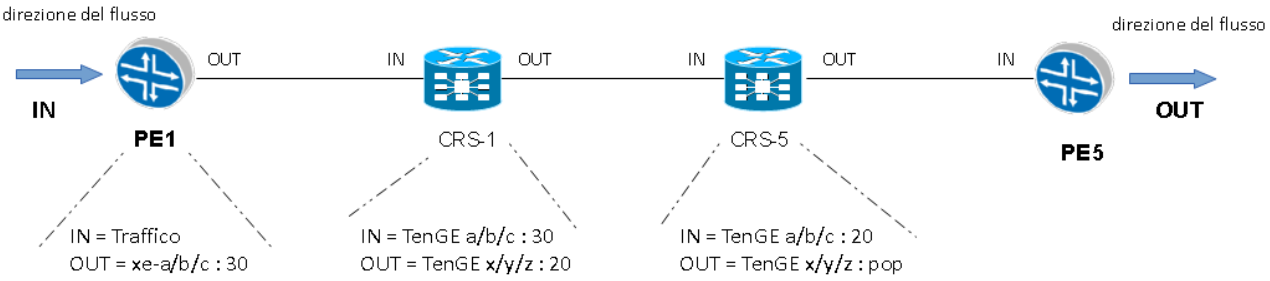
Segnalazione: RSVP TE

Le principali caratteristiche funzionali sono:

- prenotazione di banda unidirezionale tra sorgente e destinazione per un determinato flusso di traffico
- soft state signaling: continui rinfreschi su stati di prenotazione per un certo periodo di tempo, scaduto il quale viene cancellato
- la prenotazione di banda avviene attraverso messaggi di segnalazione Path e Reservation State, di cui

1. PATH STATE: relativo al processo di instradamento
2. RESV STATE: relativo al processo di prenotazione della banda





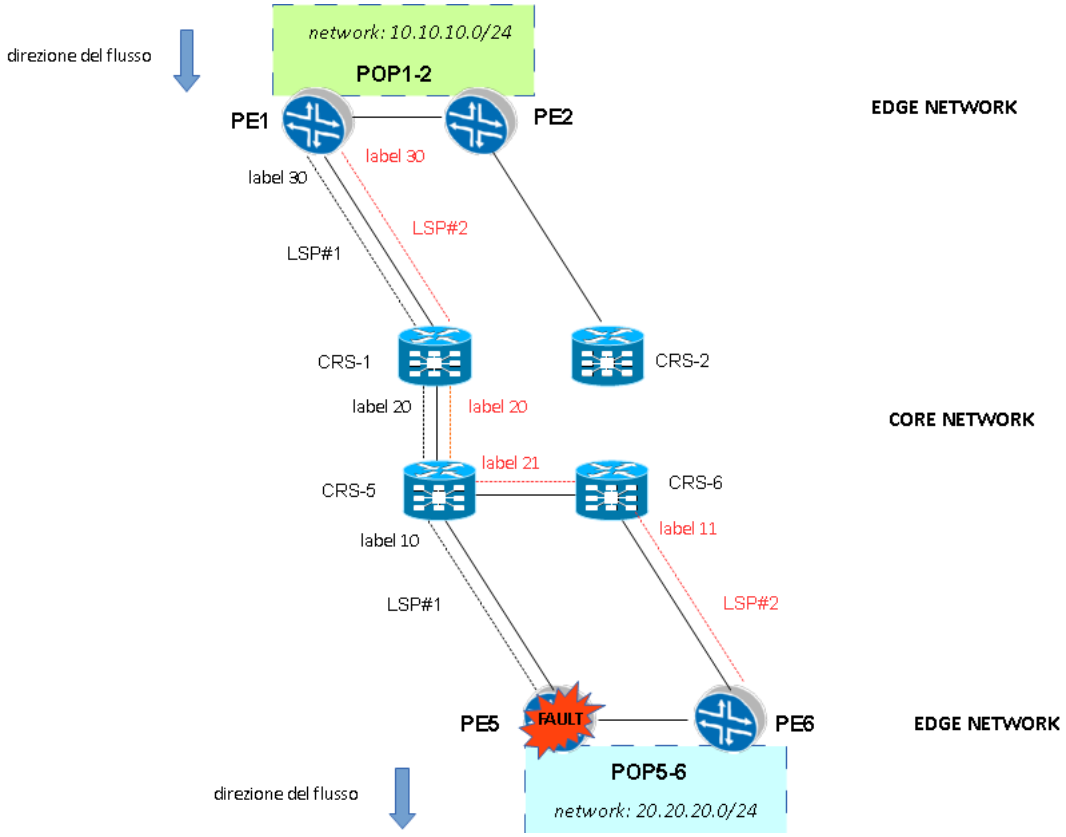
ipotesi: Link e Node Protection

Eventuali fault a livello di link e nodi è bene prevederli, e nel caso del flusso di traffico tra il POP1-2 ed il POP 5-6, potrebbero verificarsi i seguenti fault:

- PE5 : caso di node protection
- link di collegamento PE5 ↔ CRS5 : caso di link protection
- CRS5: caso di node protection
- link di collegamento CRS5 ↔ CRS1 : caso di link protection
- CRS1 : caso di node protection
- link di collegamento CRS1 ↔ PE1 : caso di link protection

vediamo di analizzarli uno per uno.

1) Fault: PE5 node protection



Configurazione PE1:

```
edit protocol ospf
 set traffic-engineering
!
edit
 protocol
 rsvp set
 interface
 all
!
edit protocol mpls
!
 set label-switched-path POP12_to_POP56
 set < loopback-PE5>
 set primary PE5-primary
 set strict
```

```
set label-switched-path POP12_to_POP56_backup
set <loopback-PE6>
set secondary PE6-secondary
set loose
!
```

Il Nodo PE5 è in fault:

- il router di backup PE6 diventa active (attraverso un meccanismo di ridondanza come vrrp)
- al momento dell'evento riparte una nuova segnalazione RSVP per ristabilire un LSP#2 di backup per raggiungere la destinazione, pertanto il PE1 (POP1-2) invia una nuova sequenza di "path label request", a questa richiesta risponde il PE6 router che ha conoscenza della destinazione in oggetto (20.20.20.0) con dei pacchetti "resv - label"
- appena il PE1 riceve il pacchetto "resv" instaura il secondo LSP di backup.
- Il node CRS5 commuta la label da 10 a 21 e direziona il traffico verso il nodo CRS6, il quale farà un'operazione di pop ed inoltra il traffico verso il nodo di destinazione

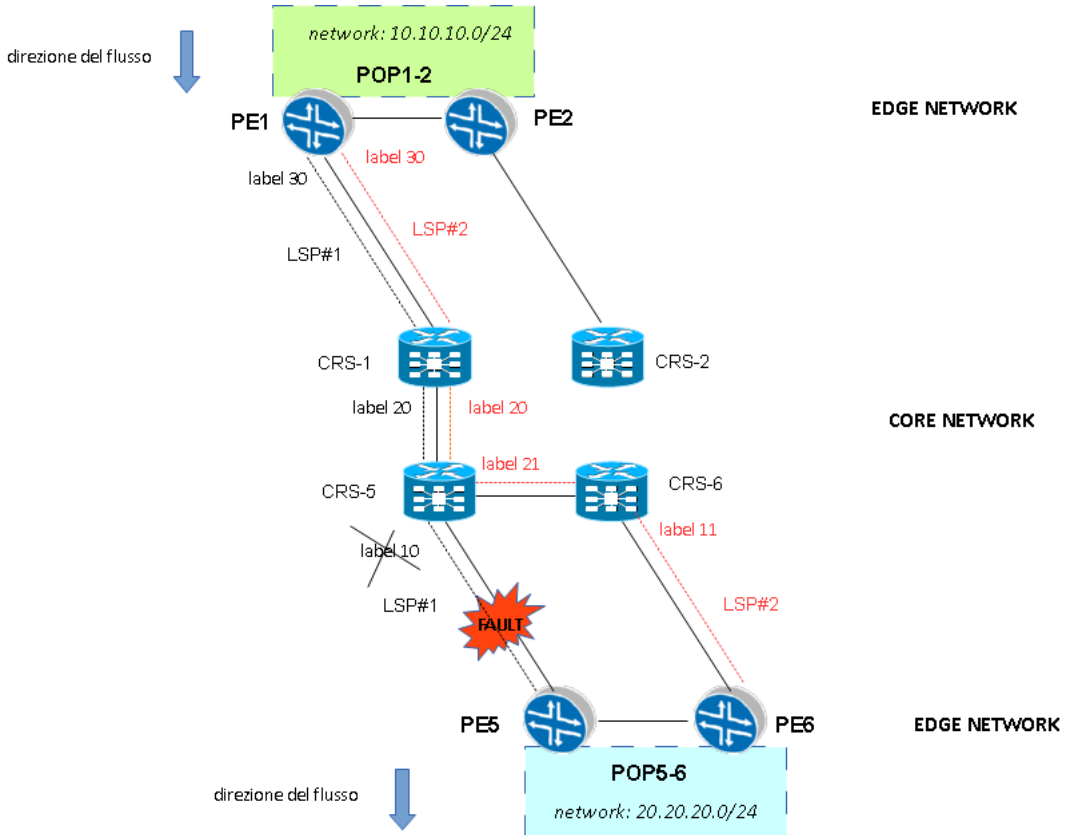
Tempi di convergenza: tempi del fast-reroute dell'ordine di msec.

A livello di Core nessuna configurazione di tunnel TE è necessaria.

A livello di Edge, sulla configurazione del tunnel dinamico in modalità strict va aggiunto il comando fastreroute e sull'interfaccia di output il comando link-protection.

Appena il fault si ripristina, LSP#1 viene ristabilito in quanto a metrica migliore (minor hop)

2) Fault: Link Protection (PE5 – CRS5)



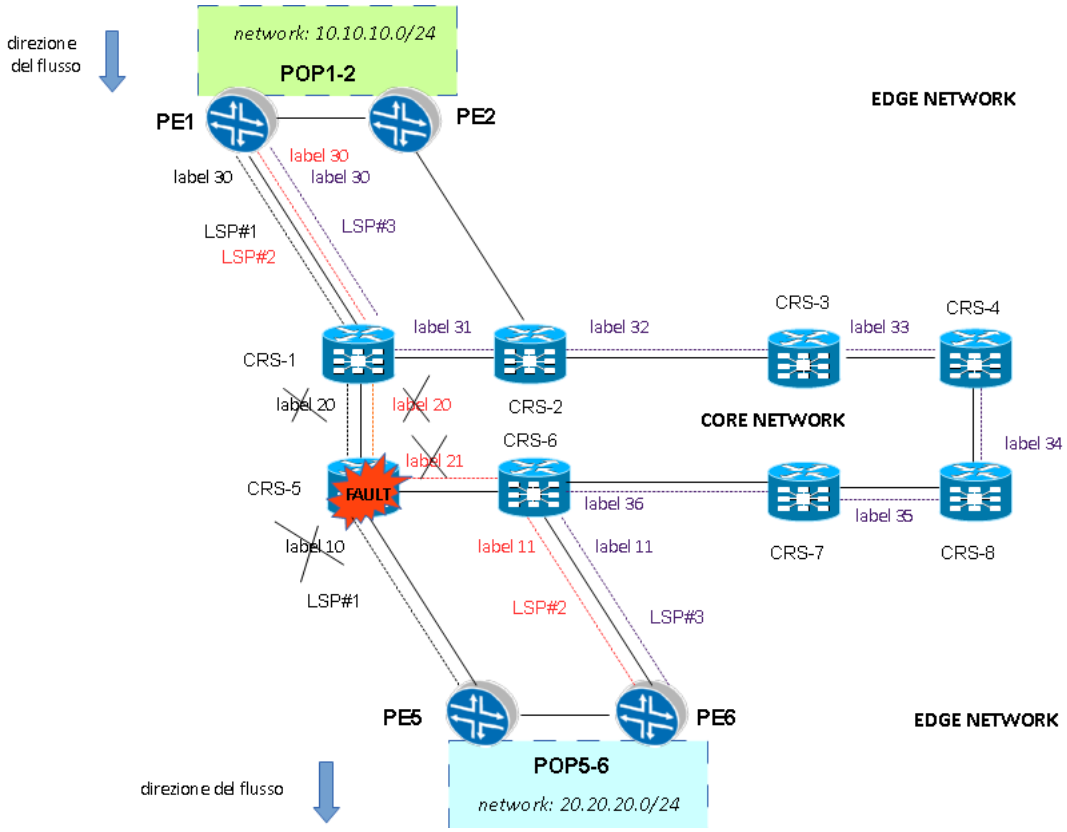
- il nodo PE5, attraverso un meccanismo di convergenza (vrrp) con tracciamento della sua interfaccia di output si accorge del fault sul proprio link e con un decremento della sua priority vrrp rende attivo il nodo PE6
- la modalità di ricalcolo LSP#2 di backup è identica alla prima ipotesi.

Tempi di convergenza: tempi del fast-reroute dell'ordine di msec.

A livello di Core nessuna configurazione di tunnel TE è necessaria.

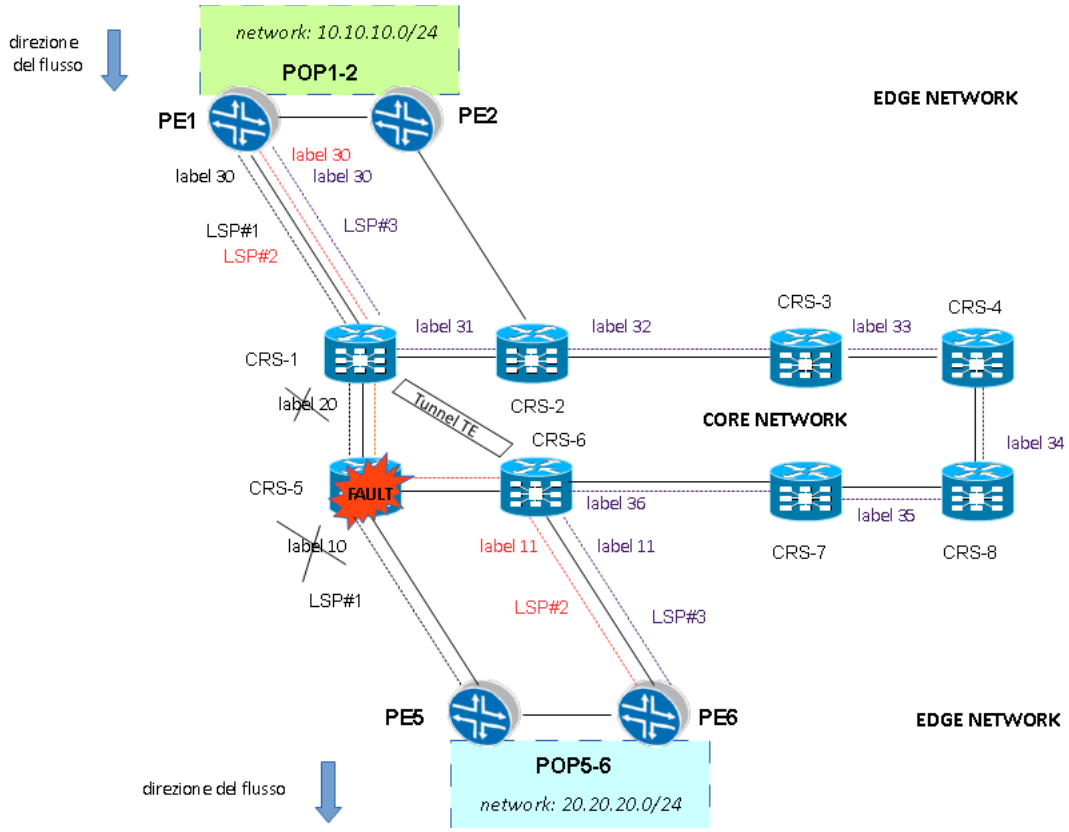
Appena il fault si ripristina, LSP#1 viene ristabilito in quanto a metrica migliore (minor hop)

3) Fault: Node Protection (CRS5)



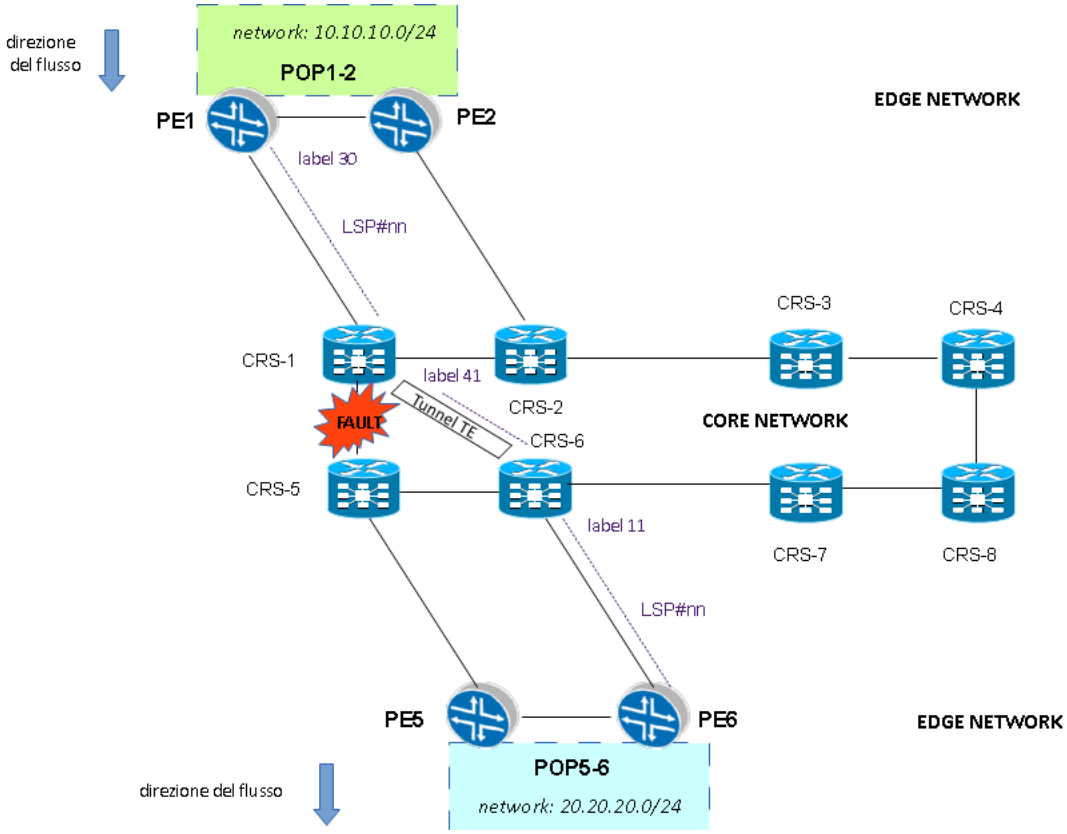
- il nodo PE5, attraverso un meccanismo di convergenza (vrrp) con tracciamento della sua interfaccia di output si accorge del fault sul proprio link del nodo CRS5 e con un decremento della sua priority vrrp rende attivo il nodo PE6;
- anche il link di collegamento CRS5 ↔ CRS1 è interessato al faul del nodo di RM-INV;
- Gli LSP di prima vengono interrotti ed una nuova segnalazione RSVP è necessaria per stabilire un nuovo LSP#3 di backup;
- un'ulteriore ridondanza può essere considerata, pensando di configurare sul nodo di backbone adiacente (CRS1) al PE1 sorgente di traffico, un tunnel TE verso il nodo di backbone non adiacente (in questo caso il nodo CRS6); la segnalazione CR-LDP per TE presente nei router CRS cisco di backbone prevede la possibilità di stabilire sessioni multi-hop tra LDP peer non adiacenti. (RSVP TE è permesso via RRO record- route)

Nel successivo grafo la rappresentazione di un tunnel multi-hop ldp tra CRS routers:




```
CRS1:
!
interface tunnel-te1
description Tunnel FRR link CRS1-5
ipv4 unnumbered Loopback0
destination < loopback CRS5> path-option 10 dynamic
!
interface tunnel-te2
description Tunnel FRR link CRS1-6
ipv4 unnumbered Loopback0
destination < loopback CRS6> path-option 10 dynamic
!
mpls traffic-eng
 interface TenGigE0/0/0/0
 traffic-eng
 tunnels backup-path tunnel-te2
 interface TenGigE0/2/0/0
 traffic-eng
 tunnels backup-path tunnel-te1
```

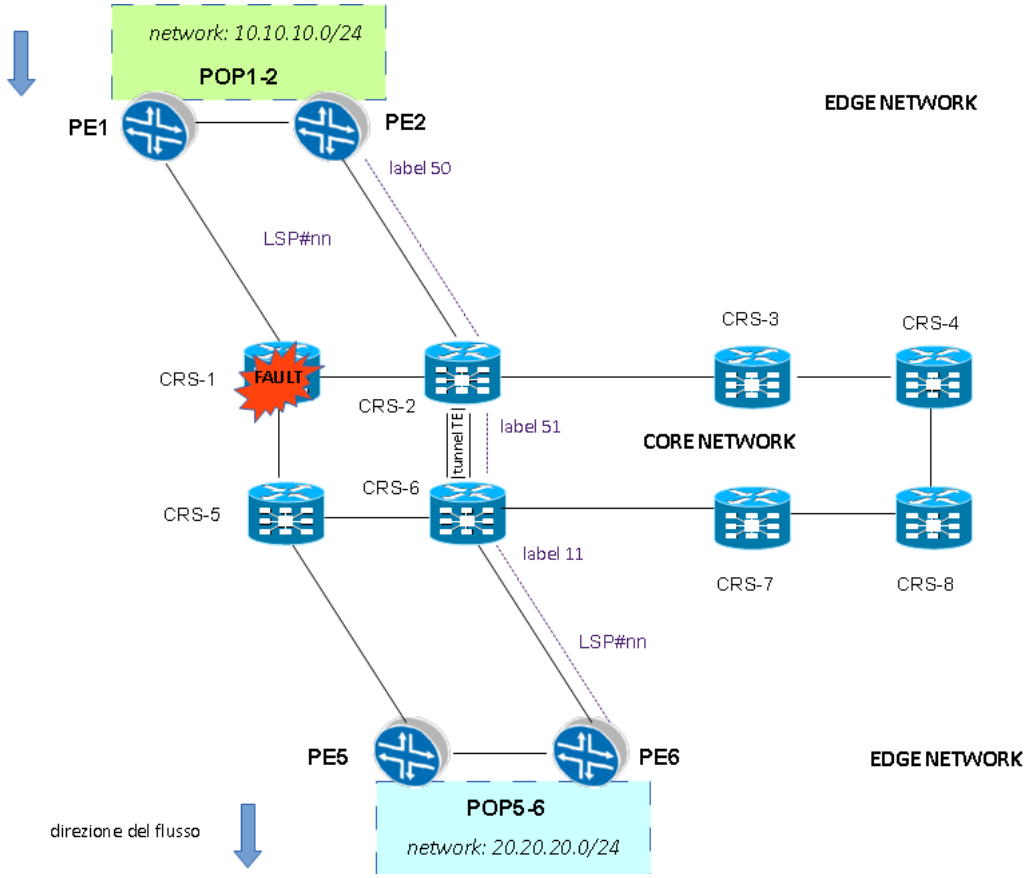
4) Fault: Link Protection Node (CRS5 – CRS1)



Il path LSP#nn stabilito via RSVP è quello evidenziato in figura.
Il tunnel TE tra CRS ha sta stessa funzione vista in precedenza.

5) Fault: Node Protection (CRS1)

Il path LSP#nn stabilito via RSVP è quello evidenziato in figura.



Il path LSP#nn stabilito via RSVP è quello evidenziato in figura.
Il tunnel TE tra CRS ha sta stessa funzione vista in precedenza.

Conclusioni:

- *i tunnel LSP tra PE vengono realizzati dinamicamente via CSPF – RSVP TE*
- *i tunnel TE a livello di Core può essere considerata una configurazione di questo tipo:*

- tunnel-te primario verso il nodo NON adiacente del POP di backbone a lui connesso
- tunnel-te secondario verso il nodo adiacente sempre del POP di backbone a lui connesso
- *mpls-ldp multi-hop abilitato*