MPLS Traffic Engineering
Traffic Protection using Fast Re-route (FRR)

Santiago Álvarez
August 2008
MPLS TE Use Cases

Bandwidth Optimization

Strategic

R1
IP/MPLS

R2

R8

Tactical

R1
IP/MPLS

R2

R8

Protection

R1
IP/MPLS

R2

R8

Point-to-Point SLA

R1
IP/MPLS

R2

R8
Traffic Protection Using MPLS TE Fast Re-Route (FRR)

- Subsecond recovery against node/link failures
- Scalable 1:N protection
- Greater protection granularity
- Cost-effective alternative to 1:1 protection
- Bandwidth protection

IP/MPLS

R1
R2
R8

Primary TE LSP
Backup TE LSP
FRR Link Protection Operation

- Requires next-hop (NHOP) backup tunnel
- Point of Local Repair (PLR) swaps label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic rejoins primary
- Restoration time expected under ~50 ms
FRR Node Protection Operation

- Requires next-next-hop (NNHOP) backup tunnel
- Point of Local Repair (PLR) swaps next-hop label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic rejoins primary
- Restoration time depends on failure detection time
Bandwidth Protection

- Backup tunnel with associated bandwidth capacity
- Backup tunnel may or may not actually signal bandwidth
- PLR will decide best backup to protect primary (nhop/nnhop, backup-bw, class-type, node-protection flag)
Configuring FRR (Cisco IOS)

Primary Tunnel

```plaintext
interface Tunnel1
   description FROM-ROUTER-TO-DST1-FRR
   ip unnumbered Loopback0
   tunnel destination 172.16.255.2
   tunnel mode mpls traffic-eng
   tunnel mpls traffic-eng bandwidth 20000
   tunnel mpls traffic-eng path-option 10 dynamic
   tunnel mpls traffic-eng fast-reroute
```

Indicate the desire for local protection during signaling

Backup Tunnel

```plaintext
interface Tunnel1
   description NNHOP-BACKUP
   ip unnumbered Loopback0
   tunnel destination 172.16.255.2
   tunnel mode mpls traffic-eng
   tunnel mpls traffic-eng path-option 10 explicit name PATH1

interface POS1/0/0
   ip address 172.16.192.5 255.255.255.254
   mpls traffic-eng tunnels
   mpls traffic-eng backup-path Tunnel1
   ip rsvp bandwidth
```

Explicitly routed backup to 172.16.255.2 with zero bandwidth

Use Tunnel1 as backup for protected LSPs through POS1/0/0
Configuring FRR (Cisco IOS XR)

Primary Tunnel

```
interface tunnel-te1
description FROM-ROUTER-TO-DST1-FRR
ipv4 unnumbered Loopback0
signalled-bandwidth 30000
destination 172.16.255.2
fast-reroute
path-option 10 dynamic
```

Indicate the desire for local protection during signaling

Backup Tunnel

```
interface tunnel-te1
description NHOP-BACKUP
ipv4 unnumbered Loopback0
destination 172.16.255.130
path-option 10 explicit name PATH1
!
mpls traffic-eng
interface POS0/3/0/0
backup-path tunnel-te 1
!
```

Explicitly routed backup to 172.16.255.130 with zero bandwidth

Use tunnel-te1 as backup for protected LSPs through POS0/3/0/0
AutoTunnel: Primary Tunnels
What’s the Problem?

- FRR can protect TE Traffic
- No protection mechanism for IP or LDP traffic
- How to leverage FRR for all traffic?
- What if protection desired without traffic engineering?
AutoTunnel: Primary Tunnels
What’s the Solution?

Forward all traffic through a one-hop protected primary TE tunnel

- Create protected one-hop tunnels on all TE links
  - Priority 7/7
  - Bandwidth 0
  - Affinity 0x0/0xFFFF
  - Auto-BW OFF
  - Auto-Route ON
  - Fast-Reroute ON
  - Forwarding-Adj OFF
  - Load-Sharing OFF

- Tunnel interfaces not shown on router configuration
- Configure desired backup tunnels (manually or automatically)
AutoTunnel: Primary Tunnels

Why One-Hop Tunnels?

- CSPF and SPF yield same results (absence of tunnel constraints)
- Auto-route forwards all traffic through one-hop tunnel
- Traffic logically mapped to tunnel but no label imposed (imp-null)
- Traffic is forwarded as if no tunnel was in place
Configuring AutoTunnel Primary Tunnels (Cisco IOS)

```bash
mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel primary onehop
mpls traffic-eng auto-tunnel primary tunnel-num min 900 max 999
!
```

- **Enable auto-tunnel primary**
- **Range for tunnel interfaces**
AutoTunnel: Backup Tunnels
What’s the Problem?

- MPLS FRR requires backup tunnels to be preconfigured
- Automation of backup tunnels is desirable
AutoTunnel: Backup Tunnels
What’s the Solution?

Create backup tunnels automatically as needed

- Detect if a primary tunnel requires protection and is not protected
- Verify that a backup tunnel doesn’t already exist
- Compute a backup path to NHOP and NNHOP excluding the protected facility
- Optionally, consider shared risk link groups during backup path computation
- Signal the backup tunnels
AutoTunnel: Backup Tunnels
What’s the Solution? (Cont.)

- Backup tunnels are preconfigured
  - Priority: 7/7
  - Bandwidth: 0
  - Affinity: 0x0/0xFFFF
  - Auto-BW: OFF
  - Auto-Route: OFF
  - Fast-Reroute: OFF
  - Forwarding-Adj: OFF
  - Load-Sharing: OFF

- Backup tunnel interfaces and paths not shown on router configuration
Configuring AutoTunnel Backup Tunnels (Cisco IOS)

- mpls traffic-eng tunnels
- mpls traffic-eng auto-tunnel backup nhop-only
- mpls traffic-eng auto-tunnel backup tunnel-num min 1900 max 1999
- mpls traffic-eng auto-tunnel backup timers removal unused 7200
- mpls traffic-eng auto-tunnel backup srlg exclude preferred

Enable auto-tunnel backup (NHOP tunnels only)

Range for tunnel interfaces

Tear down unused backup tunnels

Consider SRLGs preferably
Shared Risk Link Group (SRLG)

- Some links may share same physical resource (e.g. fiber, conduit)
- AutoTunnel Backup can force or prefer exclusion of SRLG to guarantee diversely routed backup tunnels
- IS-IS and OSPF flood SRLG membership as an additional link attribute
Configuring SRLG (Cisco IOS)

```
mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel backup nhop-only
mpls traffic-eng auto-tunnel backup srlg exclude force
!
interface POS0/1/0
  ip address 172.16.0.0 255.255.255.254
  mpls traffic-eng tunnels
  mpls traffic-eng srlg 15
  mpls traffic-eng srlg 25
  ip rsvp bandwidth
!
interface POS1/0/0
  ip address 172.16.0.2 255.255.255.254
  mpls traffic-eng tunnels
  mpls traffic-eng srlg 25
  ip rsvp bandwidth
!
```
What About Path Protection?

- Primary and backup share head and tail, but diversely routed
- No dynamically computed path diversity
- Expected to result in higher restoration times compared to local protection
- Doubles number of TE LSPs (1:1 protection)
- May be an acceptable solution for restricted topologies (e.g. rings)
P2MP TE LSP Traffic Protection

- No new protocol extensions to support FRR
- Protection requirement applies to all destinations
- P2P LSP as backup tunnel for a sub-LSP
- No changes to label stacking procedure
- Only link protection supported
Inter-Domain TE – Fast Re-route

- Same configuration as single domain scenario
- Support for node-id sub-object required to implement ABR/ASBR node protection
- Node-id helps point of local repair (PLR) detect a merge point (MP)
FRR relies on quick PLR failure detection

Some failures may not produce loss of signal or alarms on a link

BFD provides light-weight neighbor connectivity failure detection
References
Cisco Documentation

- MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

- MPLS Traffic Engineering: BFD-triggered Fast Reroute (FRR)

- MPLS Traffic Engineering (TE)--AutoTunnel Primary and Backup

- MPLS Traffic Engineering: Shared Risk Link Groups (SRLG)
Standards

- Fast Reroute Extensions to RSVP-TE for LSP Tunnels
  http://www.ietf.org/rfc/rfc4090
- Routing Extensions in Support of GMPLS
  http://www.ietf.org/rfc/rfc4202
- OSPF Extensions in Support of GMPLS
  http://www.ietf.org/rfc/rfc4203
- IS-IS Extensions in Support of GMPLS
  http://www.ietf.org/rfc/rfc4205
- Definition of a Record Route Object (RRO) Node-Id Sub-Object
  http://www.ietf.org/rfc/rfc4561