FAST RE-ROUTE
TECHNIQUES AND SOLUTIONS

AZHAR SAYEED
asayeed@cisco.com
Agenda

• A Quick Re-Cap on MPLS FRR
• Advanced FRR Methods
• Fast Re-Route without MPLS
• Conclusions
Protection

- Temporary mechanism to minimize packet loss during a failure
- Pre-provisioned protection tunnels that carry traffic when a protected link or node goes down
- FRR protects against LINK FAILURE
  - For example, Fibre cut, Carrier Loss, ADM failure
- FRR protects against NODE FAILURE
  - For example, power failure, hardware crash, maintenance
- Protection against CONDUIT FAILURE (SRLG)
  - Conduit may carry multiple fibres, don’t want to protect C1:F1 with C1:F2
Categories of Fast Reroute Protection

• Local or facility based protection
  - Link protection
  - Node protection
    Protect a piece of the network (node or link)
    1:N scalability
    Fast failure recovery due to local repair

• Path protection
  Protects individual tunnels
  1:1 scalability
MPLS TE FRR Local Repair

- MPLS TE FRR BYPASS make use of nested LSPs (stack of labels)

**Convergence Time**
FRR LSPs: $O(50\text{ms})$
Non FRR LSPs: $O(s)$

**Fast Reroutable LSPs**

**NON Fast Reroutable LSPs Are Rerouted Using Restoration**
MPLS TE Fast Reroute—Key Principle

The Path messages are sent onto the backup tunnel to refresh the downstream states.
MPLS TE Protection/Restoration Schemes

- **Link/Node failure detection**
- **Link** failure detection
  - On POS, link failure detection is handled by Sonet/SDH alarms
    - On Receive side: LOS/LOF/LAIS
    - On Transmit side: LRD
    - Very fast.
- **Node** failure detection is a more difficult problem
  - Node hardware failure => Link failure
  - Software failure… Keepalive scheme (IGP, BFD)
- **Protection time**
  - Link and Node protection are very similar
  - Protection times are commonly linear to number of protected items
  - One nationwide provider gets ~35ms of loss
  - Possible to achieve less than 10ms loss
Node Protection

• Node protection still has the same convergence properties as link protection
• Deciding where to place your backup tunnels is a much harder problem to solve on a large-scale
• For small-scale protection, link may be better
• Auto creation of backup tunnels can help with this
• Configuration is identical to link protection, except where you terminate the backup tunnel (NNHop vs. NHop)
Agenda

• A Quick Re-Cap on MPLS FRR
• Advanced FRR Methods
• Fast Re-Route without MPLS
• Conclusions
Shared Risk Link Group

- Each link in turn passes through a conduit/cable.
- Several links can share the same conduit/cable—If the conduit is broken then several links can be broken.
- All links in the conduit/cable share the same risk (SRLG).
- On each link, the set of SRLGs the link belongs to is configured.
- SRLG information is flooded by the IGP.
- The topology, resources information along with the SRLG membership are stored in the TE database.
- Each node computes the backup path excluding the link and SRLG it is trying to protect.
On each LSR, one single command allows to automatically configure the set of NHOP and/or NNHOP backup tunnels:

```
[no] mpls traffic-eng auto-tunnel backup srlg exclude {force | preferred }
```

“force” indicates that no backup tunnel must be created if the SRLG diversity constraint cannot be satisfied.

“Preferred”: if no SRLG diverse path can be found the constraint is dynamically relaxed.

**Example with NHOP:**

For each link (with an IGP adjacency):

- If there is no Fast Reroute TE LSP traversing the link, do nothing.
- If there is at least one Fast reroutable TE LSP traversing the link, then compute an SRLG diverse path for the NHOP backup tunnel and establish the NHOP backup tunnel.
Example with NNHOP:

For next-next hop neighbor:

If there is no Fast Reroute TE LSP traversing the segment, do nothing

If there is at least one Fast Reroutable TE LSP traversing the segment, then compute an SRLG diverse path for the NNHOP backup tunnel and establish the NNHOP backup tunnel

Notes:

- Each SRLG change membership signalled via the IGP automatically triggers a backup tunnels reoptimization/re-evaluation

- In case of double failures, the SRLG diversity constraint relaxation may still allow to protect against interface failure or single link failure
MPLS TE Fast Reroute to Protect ASBR-ASBR Link and ABR/ASBR Node Failures

- Backup tunnel selection in a multi-AS domains environment

- draft-ietf-mpls-nodeid-subobject-01 defines a new sub-object called the “node-id” sub-object carried within the Resv message that unambiguously identifies the router-ID

Backup tunnel selection may not be possible??
Protecting Bandwidth During Failures

• Bandwidth protection mechanisms is required:
  For some types of traffic
  Not all the traffic types require bandwidth protection
  Ex: Voice, AToM traffics typically require bandwidth protection
  In some networks
  Not all the networks require bandwidth protection

• Backup tunnels can share bandwidth if we operate under the single failure assumption
Bandwidth Protection

Protected LSP + BW Protection Requested

Protected tunnel signalled with bandwidth protection (SESSION-ATTRIBUTES or FAST-REROUTE object)

Protected tunnel locally repaired onto bypass tunnel

Path Error (Tunnel Locally repaired) sent by the PLR

Link/node Failure

Bandwidth protection during failure

Path Error

Backup Tunnel

TE LSP reoptimized (with Make before Break) and set of backup tunnel recomputed
Bandwidth Sharing

- Objectives
- For each LSR, find a set of backup tunnels (to the NHOP for link P and NNHOP for Node P) with capacity constraints,
- Two backup tunnels protecting the same facility cannot share bandwidth,
- Two backup tunnel protecting independent facilities can share bandwidth (as they are not simultaneously active under the assumption of single failure)
Various MPLS TE/FRR Deployments Models

- If MPLS TE is required for FRR only, two possible deployment models:
Agenda

• A Quick Re-Cap on MPLS FRR
• Advanced FRR Methods
• Fast Re-Route without MPLS
• Conclusions
What About Just IP Networks?

• Not all SPs/Enterprise customers are running MPLS TE/FRR
• Some are only running LDP
• Many Enterprise customers are only running IP network (No MPLS at all)
• Can we build a solution to provide link/node protection in such cases?
FRR in IP Networks

• Same failure detection mechanisms can be leveraged
• Traffic can be quickly re-routed onto a “backup path” upon link or node failures
• The notion of back up path may be different (when compared to MPLS TE/FRR)
Challenges

- No concept of explicit routing in IP tunnels (Tunnel pinning)
- Difficult to place an IP tunnel to a downstream node that excludes the node/link to be protected
- The aim is to find a node downstream that will not send the traffic back to given node avoiding loops (or micro-loops)
IP FRR

Notes:
Packets cannot be tunneled to R3, R7 or R1
They need to be tunneled to R5
Since each node has the entire IGP database
Each node can compute the node to which traffic can be tunneled for a given downstream prefix
Establish a tunnel to the downstream node
Send the traffic upon detecting a failure

Shortest paths
From – To
R1 – R6 : R1, R2, R4, R5, R6
R2 – R6 : R2, R4, R5, R6
R3 – R6 : R3, R2, R4, R5, R6
R7 – R6 : R7, R3, R2, R4, R5, R6
The Key

• **Finding the right node to which traffic is tunneled**

  Concept of F and G space

  F Space—A set of routers reachable from a specific router without transiting the failed component

  G Space—A set of routers from which a specific router can be reached without transiting the failed component

• **It is could be**

  One node in the network

  Or many nodes in the network (We choose any one in that case)

  A pair of nodes—One in each partitioned graph between which traffic must be further tunneled (Directed Forwarding)

• **IETF draft**—draft-bryant-ipfrr-tunnels-01.txt
IP FRR

Notes:
Packets cannot be tunneled to R3, R7 or R1
They need to be tunneled to R5
Since each node has the entire IGP database
Each node can compute the node to which traffic can be tunneled for a given downstream prefix
Establish a tunnel to the downstream node
Send the traffic upon detecting a failure

Shortest paths
From – To
R1 – R6 : R1, R2, R4, R5, R6
R2 – R6 : R2, R4, R5, R6
R3 – R6 : R3, R2, R4, R5, R6
R7 – R6 : R7, R3, R2, R4, R5, R6
Conclusion

• If the goal is to provide sub second convergence use IGP fast convergence
  Convergence tuning and incremental SPF
• If the goal is to provide sub 100ms convergence then:
  • MPLS Traffic Engineering Fast Reroute
    Fast recovery using local protection
    A wide scope of recovery: link/node/SRLG
    in a scalable manner (BYPASS makes use of label stacking limiting
    the number of backup tunnels)
    with stability... something crucial in large networks (fast local rerouting
    followed by the head-end reoptimization)
• IP FRR—For just IP networks
  Nice technique to re-route traffic during failures
  Uses the same detection techniques (LOS, BFD etc)
  Intelligence built into the routers (no hardware hacks or protocol changes)
THANK YOU!