Extensions to RSVP-TE for P2MP LSP

Ingress/Egress Local Protection

draft-chen-mpls-p2mp-ingress-protection
draft-chen-mpls-p2mp-egress-protection

Huaimo Chen (huaimochen@huawei.com)
Ning So (Ning.So@verizonbusiness.com)
Contents

- Issues in Existing P2MP LSP Ingress & Egress Protection
- **Proposed P2MP LSP Ingress & Egress Local Protection**
- Advantages of P2MP LSP Ingress and Egress Local Protection

- It can be used for P2P LSP Ingress/Egress Protection accordingly
Details in Existing P2MP LSP Ingress & Egress Protections

➢ No standards for LSP Ingress/Egress Local Protection

➢ To provide E2E P2MP LSP protection, a current way (detail in next page)

◆ Redundant Root and Every Leaf

◆ Create two P2MP LSPs from root to leaves, carry the same data at same time.

◆ For each leaf, create a P2P LSP from the leaf to root and configure BFD with it

◆ Run iBGP on every leaf node and use P2P LSP as its next hop

◆ When BFD detects P2P LSP failure, BGP withdraws route to root and this makes the receiver switch to another leaf to get the data.
Details in Existing P2MP LSP Ingress & Egress Protections (Cont)

1. Double leaves
2. Two P2MP LSP carry data
3. P2P LSP (leaf→root) with BFD
4. P2P LSP as NH to SA, export route for SA to receiver
5. Receiver selects a leaf accordingly

- Redundant Root and Every Leaf
- Two P2MP LSPs from root to leaves, carrying the same data at same time.
- For each leaf, a P2P LSP from leaf to root with BFD
- BGP on every leaf & use P2P LSP as its next hop
- When BFD detects P2P LSP failure, BGP withdraws route to SA and this makes the receiver switch to another leaf to get the data.
Issues in Existing P2MP LSP Ingress & Egress Protections

- Not Scalable
- Consume lots of resource
  - Reserve/use double bandwidth
- Not reliable
  - The failure of reverse P2P LSP from leaf to root does not mean the failure of its corresponding P2MP sub-LSP from root to leaf
- Speed of Global Recovery
  - Depends on convergence of IGP and BGP
- Difficult to configure and maintain
  - For each P2MP LSP branch/sub-LSP,
    - need configure a reverse P2P LSP from leaf to root with BFD
    - P2P LSP with BFD is used to detect failure of its corresponding P2MP sub-LSP
The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

P2MP LSP Ingress Local Protection

local protection for ingress failure

Multicast Source

P2MP

PE1

PE2

PE3

PE4

PE5

PE6

CE1

CE2

CE3

CE4

CE5

CE6

P2MP LSP

Backup LSP

Connect of backup group

• Primary ingress PE5 fails:
  • Traffic to backup tunnel
  • Traffic merged into P2MP LSP

Multicast Receiver

Animated Multicast Receiver

RPF Check

Data

Data

Connect of backup group
When primary egress PE1 fails,
- Traffic to backup tunnel to PE2 (backup egress)
- Traffic delivered to CE1 from PE2
P2MP LSP Ingress & Egress Local Protection

Existing scenario: double root and every leaf
Create two global P2MP LSP from each root to leaves, carrying data at same time

One P2MP LSP for all: Every part (ingress & egress) is locally protected
- Big resource saving (e.g., no double bw resv)
- Faster failure recovery: local protection speed
Advantages of P2MP LSP Ingress and Egress Local Protection

- All parts of P2MP LSP are locally protected
- Only one P2MP LSP is used to implement an E2E protection
  - Normally two P2MP LSPs are used
- Big saving on resource: 50% bandwidth saving
  - No need to reserve/use double bandwidth
- Faster recovery
  - Speed of local protection recovery
  - Flow recovery within 50ms when a failure happens
- Easier to operate
Next Step

- Welcome comments
- Request to make it into a working group document