Extensions to RSVP-TE for LSP Ingress Local Protection

draft-ietf-teas-rsvp-ingress-protection

Huaimo Chen, Raveendra Torvi
Ning So, Autumn Liu, Yimin Shen
Tarek Saad, Fengman Xu
Mehmet Toy, Lei Liu
Renwei Li, Quintin Zhao
Zhenbin Li, Boris Zhang, Markus Jork
3 failure cases (combinations) below:

1. Ingress PE1 fails
2. Link PE1-PE2 fails
3. Link CE1-PE1 fails

Ingress Protection behaviors for 2 modes:

1) Source Detects Ingress Failure
2) Backup & Source Detect Ingress Failure
Source (CE1) quickly detects ingress (PE1) failure and switches traffic to backup ingress (PE2).

Backup Ingress (PE2) always ready to import traffic into backup LSP, reliably detects ingress failure, sends Path as needed.

1. Ingress PE1 fails
2. CE1 quickly detects failure by BFD, switches traffic to PE2
3. PE2 imports traffic into backup LSP
4. Traffic merged into primary LSP at P1
5. PE2 reliably detects PE1 failure by IGP/routing, sends/refreshes PATH as needed
Source (CE1) quickly detects ingress (PE1) failure and switches traffic to backup ingress (PE2) for backup LSP.

Backup Ingress (PE2) always ready to import traffic into backup LSP, reliably detects ingress failure, sends Path as needed.

1. Link PE2-PE1 fails

2. CE1 continues sending traffic to PE1, sending traffic through primary LSP

3. PE2 reliably detects PE1 not fail, not send/refresh PATH
Source Detects Failure (3/3)

Source (CE1) quickly detects ingress (PE1) failure and switches traffic to backup ingress (PE2). Backup Ingress (PE2) always ready to import traffic into backup LSP, reliably detects ingress failure, sends Path as needed.

1. Link CE1-PE1 fails
2. CE1 quickly detects failure by BFD and switches traffic to PE2
3. PE2 imports traffic into backup LSP
4. Traffic merged into primary LSP at P1
5. PE2 reliably detects PE1 not fail, not send/refresh PATH
Backup and Source Detect Failure (1/3)

Backup ingress (PE2) and source (CE1) detect ingress (PE1) failure and control the traffic delivery concurrently (CE1 switches traffic when detecting failure, PE2 imports traffic into backup LSP when detecting failure).

1. Ingress PE1 fails

2. CE1 detects it by BFD-1, switches traffic to PE2

2. PE2 detects it by BFD-2, imports traffic into backup LSP to P1

3. Traffic merged into primary LSP at P1
Backup and Source Detect Failure (2/3)

Backup ingress (PE2) and source (CE1) detect ingress (PE1) failure and control the traffic delivery concurrently (CE1 switches traffic when detecting failure, PE2 imports traffic into backup LSP when detecting failure).

1. Link PE1—PE2 fails

2. CE1 continues sending traffic to PE1, importing traffic to primary LSP

2. PE2 detects it by BFD-2 and imports traffic from CE1 into backup LSP, but no traffic from CE1
Backup and Source Detect Failure (3/3)

Backup ingress (PE2) and source (CE1) detect ingress (PE1) failure and control the traffic delivery concurrently (CE1 switches traffic when detecting failure, PE2 imports traffic into backup LSP when detecting failure)

1. **Link PE1—PE2 fails**

2. **CE1 detects it by BFD-1, switches traffic to PE2**

2. **PE2 does not detect it. Traffic gets lost. (May use multi-hop BFD PE2--PE1--CE1, or CE1 can tell link failure from node failure)**
Summary

Presented:

Ingress protection behaviors for two modes

1) **Source Detects Ingress Failure:** works for all cases

2) **Backup and Source Detect:** may not work for some cases if cannot tell link failure from node failure or no multi-hop BFD X border
Next Step

• Welcome comments