MAC Flush Loop Detection in VPLS

draft-pkwok-l2vpn-vpls-macflush-ld-01

Paul Kwok
Pranjal Dutta

IETF-77

Summary

- First version was presented in IETF-74, San Francisco.
- Addressed comments received in mailing list.

Objectives

- Improve robustness of existing MAC Flush mechanism in RFC 4762.

Problem Statement

- Failure of "split horizon" rule, that provide loop free connectivity among VPLS PE devices in the full mesh may cause loops of MAC flush messages.
- Misconfiguration in dual home H-VPLS redundancy or malfunctioning of dual homing protocols may cause loops of MAC flush messages.
- MAC flush loop may cause Denial of Service or complete failure of the Control Plane.
- Solutions for loop detection and prevention in data plane is out of scope.

Procedure

- Use Path Vector TLV defined in RFC 5036 in MAC Flush messages.
- Path Vector TLV in the context of MAC Flush message contains the list of VPLS PE devices that has propagated the MAC Flush instance.
- On receipt of a MAC Flush with Path Vector TLV, if a VPLS PE device finds its own LSR-ID in the Path Vector List then a loop is detected and the message is dropped.

Procedure

- Supports the notion of max. Path Vector length based on local configuration - to declare loop if MAC flush has traversed number of given VPLS PEs = max Path Vector Length.
- MAC Flush Loop Detection should be turned on in all PE devices within a VPLS Network, else may result in undetected loops.

Next Steps

- WG Status?