Multi-Instances ISIS Extension

draft-ietf-isis-mi-08.txt

Stefano Previdi (sprevidi@cisco.com)
Les Ginsberg (ginsberg@cisco.com)
Dave Ward (wardd@cisco.com)
Mike Shand (imc.shand@googlemail.com)
Abhay Roy (akr@cisco.com)

85th IETF, Atlanta, November 2012

MI-ISIS Introduction

- Allows separate ISIS instances to share nodes and links
- Allows routing and non-routing info to be conveyed and stored in separate/isolated LSDB flooding schemes
- Full Topology isolation
  - Ships in the night approach
- Mechanism used to mark packets with instance membership
  - IID TLV
  - Mark all packets: IIH, [C|P]SNP, LSP

MI-ISIS
Changes since V6

RFC 5120 NOT supported within a non-zero instance

Security Related Clarification

Now approved as a draft standard

MT(RFC 5120)/MI

Description	MT	MI
Instance	Standard Instance (#0) only	Non-zero Instances
Adjacencies	Shared by all topologies	Instance specific
Hellos	M-topologies TLV(229) advertises MTIDs supported on a link	IID-TLV advertises ITIDs supported on a link
Update Process	One LSPDB advertises all MTIDs	Each IID/ITID has a unique LSPDB
LSPs	Topology specific TLVs for: IS-Neighbors (TLV 222) IP Reachability (TLV 235) IPv6 Reachability (TLV 237) (in addition to standard TLVs (22, 135, 236))	MT TLVs forbidden Standard TLVs used

RFC 5120 Support within MI

Not supported…

Was always discouraged – but now forbidden.

Would require advertising in hellos the MTIDs supported within a given IID/ITID which is not defined

LSP Purges

Section 7 (Security)

"Use of the extensions defined here with authentication as defined in [RFC5304] or [RFC5310] will result in the discarding of purges by legacy systems which are in strict conformance with either of those RFCs. To avoid this issue an MI-RTR MAY omit the IID-TLV in purges for the standard instance (IID #0) until such time as all ISs in the network have been upgraded to support [RFC6232]."

Text was from earlier version where IID #0 was allowed in PDUs associated with standard instance. As that is prohibited the above text was removed.

Security Discussion

Base Protocol Authentication scopes:

- Circuit (IIHs)
- Area (L1 SNPs, LSPs)
- Domain (L2 SNPs, LSPs)

MI adds:

- Area/IID/ITID (L1 SNPs, LSPs)
- Domain/IID/ITID (L2 SNPs, LSPs)

Authentication procedures unchanged

Next Steps

We’re DONE. ☺

Backup Slides

(from presentation at 83rd IETF in Paris)

Interoperability on LANs

- Use of dedicated per level multicast address for non-zero IID
  Prevent interoperability issues
- Hide MI-ISIS packets to non-MI capable routers
- MI routers MUST discard packets if:
  - The destination multicast address is AllL1IS or AllL2IS and the PDU contains an IID TLV with non-zero value
  - The destination multicast address is one of the two new addresses and the PDU contains an IID TLV with a zero value or has no IID TLV

Instance Identifier

- Assign to each ISIS packet an instance Identifier
  - IIHs, LSPs, SNPs
- Instance is identified through new TLV
  - IID TLV (TBA)
  - IID ==> ISIS Instance
  - IID TLV is 16-bits number
- Single IID TLV on each ISIS packet

Instance Identifier

- IID TLV allows a router to distinguish among ISIS packets when running multiple ISIS instances
  - Upon reception, packets are forwarded to the corresponding instance
  - Routers establish adjacencies if sharing same IID
- How to distinguish/discriminate among data packets once routing schemes/trees have been computed is out of the scope of this document.

MI-ISIS

- Slightly different approach than the one taken by Multi-topologies ISIS
  - No shared fate other than the link
  - Separate flooding, LSDBs, Adjacency table, …
- IID TLV _must_ be unique per ISIS packet
  - Requires packet analysis in order to enforce the rule
  - Probably more work to do prior to accept reject each packet

IID and ITID

- Before version 5:
  - If more than one IID is configured on a given link, multiple adjacencies will be established, one per instance
  - Means: more than one adjacency even on p2p links
- Version 5 introduces the capability of having multiple topologies within the same instance
  - Two levels: instance and topology
  - Separate LSDB per topology
  - Separate Update process per topology
  - ITID: Instance Topology Identifier
- Advantages: two levels of hierarchy:
  - Instance and Topology
  - Still independent flooding and LSDBs

MI-ISIS

- Version 6:
  - Re-defines ITID to 16 bits
    - Requirement: ability to map ITID to VLAN-ID