Dynamic Distribution of SSM ranges.

Presenter: Stig/Ramakrishnan

Problem Overview

- Snooping switches are unaware of the user configured SSM ranges in the network.
- For SSM operation the (*,G) v2/v3 for SSM ranges need to be ignored.
- If the v2/v3 (*,G) reports for the SSM ranges are accepted then the router will operate in v2 compatible mode for such groups. This can hinder SSM operation.
- This is an avenue for an attacker to deny SSM service.
- https://tools.ietf.org/html/rfc4604 describes the SSM service operations.

"It is important that a router not accept non-source-specific reception requests for an SSM destination address. The rules of [IGMPv3] and [MLDv2] require a router, upon receiving such a membership report, to revert to earlier version compatibility mode for the group in question. If the router were to revert in this situation, it would prevent an IGMPv3-capable host from receiving SSM service for that destination address, thus creating a potential for an attacker to deny SSM service to other hosts on the same link."

- The draft proposes mechanism to learn the user configured SSM ranges.

Proposal in the draft

- The draft https://tools.ietf.org/html/draft-ramki-igmp-ssm-ranges-00 proposes a method to send and learn SSM ranges dynamically.
- A pim hello option extension is proposed to learn the SSM ranges.

Advantages

- SSM operation is not compromised due to version incompatibility for SSM group ranges
- The learning is dynamic and will ensure consistency.