72nd IETF, July 2008, Dublin

Requirements for IP Multicast Session Announcement in the Internet

draft-asaeda-mboned-session-announcement-req-00

Hitoshi Asaeda (Keio University)
Kazuhiro Mishima (Keio University)
Vincent Roca (INRIA)

Motivation

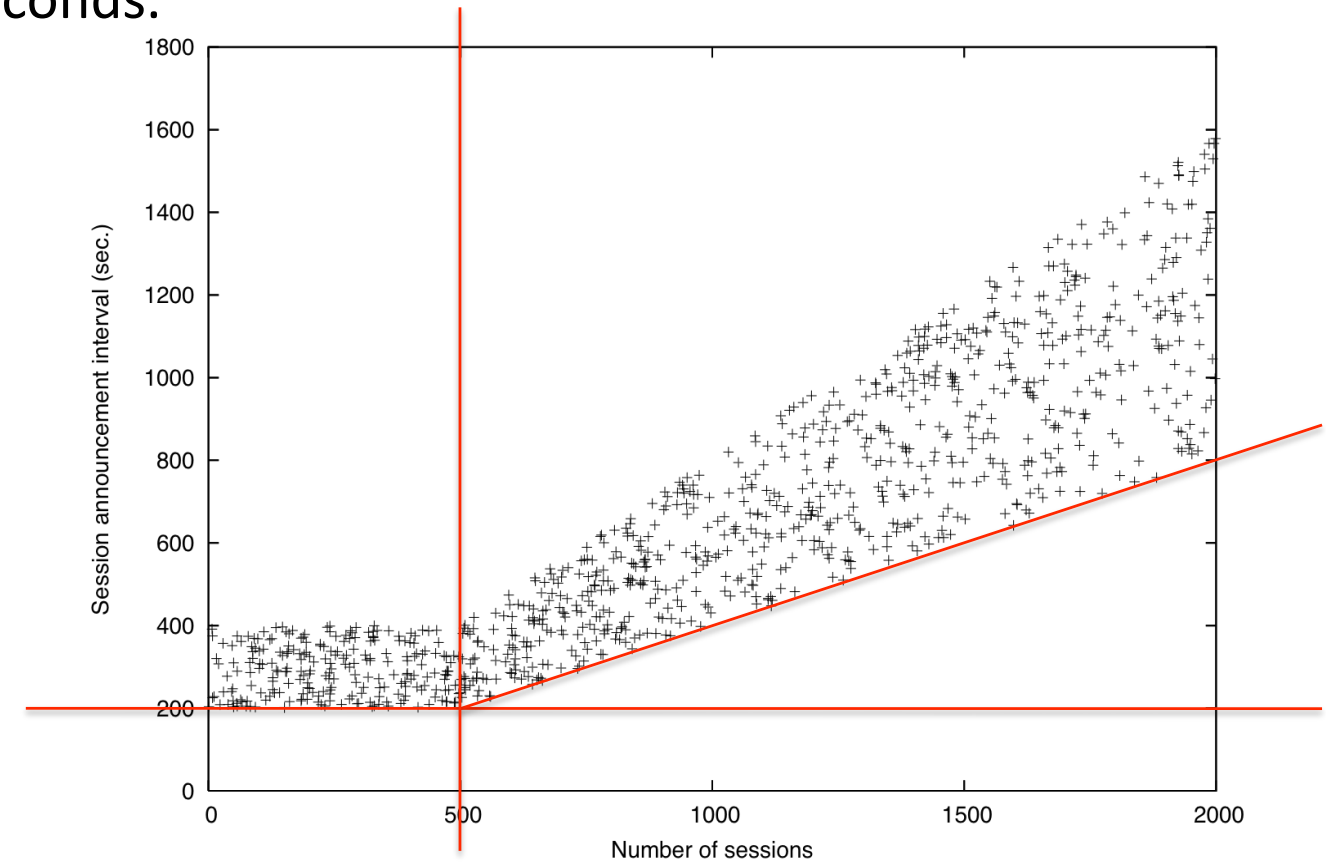
- Clarify the issues SAP has, and show the requirements for IP multicast session announcement protocols/procedures
- No protocol definition in this draft
  - Another draft will be proposed in a future if gain a consensus

Session Announcement Requirements

- Abstract
  - The Session Announcement Protocol (SAP) was used to announce information for all available multicast sessions to the prospective receiver in an experimental network. It is useful and easy to use, but difficult to control the SAP message transmission in a wide area network. This document describes the several major limitations SAP has and the requirements for multicast session announcement in the global Internet.

Announcement Interval vs. Latency

- Periodical non-reliable SAP message transmission needs to keep interval, but it gives longer latency [RFC2974]
  - E.g., if 2,000 multicast sessions are active in the Internet, each session announcement interval is set between 800 and 1600 seconds.



Difficulties in Scope Definition

- TTL scoping
  - Difficult to control traffic
  - Impossible to manage complex network topologies
    - E.g. between overlapped area
- Administrative scoping
  - Still difficult to manage complex network topologies
  - Impossible to overlap SSM address range (232/8) and 239/8
    - Possible to define SSM administrative scope range (already defined in some place?), but defining yet another address range might be troublesome or make users confuse

Communication Dependency

- SAP relies on ASM
  - All prospective receivers must join 224.2.127.254 without specifying any source address
    - Does not work “SSM-only” network
- Weak for DoS
  - If malicious hosts flood high bandwidth stream to 224.2.127.254, all prospective receivers and multicast routers listening SAP messages take in the stream and their networks may be corrupted or destroyed.

Lack of Sender and Receiver Control

- Sender control
  - Difficult to configure approved senders only who can send SAP messages or non-approved senders who are disabled to send SAP messages
- Receiver control
  - Difficult to hide multicast session information announced by SAP from non-approved receivers if they are inside the scoped network
  - Difficult to encrypt SAP messages to prevent non authorized client from reading them
    - Because it adds more complexity to SAP by combining with a key sharing mechanism.

Requirements

- Information consistency
- Low information update latency
- Low bandwidth consumption
- Scalability
- High availability
- Scope control
- No dependency on a routing architecture
- Sender and receiver control

Next Steps

- Revise the draft
  - Need more inputs and detail for the requirements
- Move forward
  - WG item?