Requirements for IP Multicast Session Announcement
draft-ietf-mboned-session-announcement-req-03

Abstract

The Session Announcement Protocol (SAP) [2] was used to announce
information for all available IP multicast sessions to the
prospective receiver in an experimental network. It is easy to use,
but not scalable and difficult to control the SAP message
transmission in a wide area network. This document describes the
issues and the requirements for multicast session announcement in the
global Internet.

Status of this Memo

Copyright Notice

Table of Contents

[1]. **Introduction**

   IP multicast session or channel information is described with the
   Session Description Protocol (SDP) [3] syntax or written in a
   metafile.

   The Session Announcement Protocol (SAP) [2] was used to announce
   information for all available multicast sessions to the prospective
   receiver in the experimental MBone. In a SAP announcement procedure,
   the entire session information must be periodically transmitted and
   all active session descriptions must be continuously refreshed. If
   ever a session is no longer announced, its description eventually
   times out and is deleted from the available session list. This is a
   major property of a "soft-state" protocol.

   SAP enables to keep the session information active and refresh it,
   and builds robust and fault-tolerant systems. However, it requires
   the periodic message transmission (i.e. message flooding) that may
   cause major overheads or overloads. Although this strategy keeps the
   implementation simple, it rises costs and further reduces its
   scalability.

   Another issue is closely related to a security or policy management.
   As with the above issue, it is difficult to control a data sender or
   a receiver and the amount of traffic or the data distribution area
   even with existing scoping techniques.

   This document explains the issues SAP and other systems have raised
   and clarifies the requirements that should fulfill an ideal session
   announcement system. This document describes work originally
   published by Asaeda and Roca in IEICE Transactions on Information and
   Systems [6].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL
NOT","SHOULD", "SHOULD NOT", "RECOMMENDED","MAY", and "OPTIONAL" in
this document are to be interpreted as described in RFC 2119 [1].

3. Potential Problems in SAP

3.1. Announcement Interval vs. Latency

   SAP improves the robustness and data consistency in front of packet
   losses by transmitting each message several times. However,
   transmitting a large number of active multicast session information
   in a flooding manner may cause major overheads. The solution defined
   in [2] is the time period between repetitions of an announcement.
   This period is chosen such that the total bandwidth used by all
   announcements on a single SAP group remains below a preconfigured
   limit, and the bandwidth limit should be assumed to be 4000 bits per
   second, if not specified.

   However, this solution largely increases the latency experienced by
   end users especially when the number of sessions increases. In its
   definition, since the minimum interval of SAP message transmission is
   200 seconds, end users experience a minimum waiting time of 200
   seconds to obtain the entire session list, irrespective of the number
   of observed multicast sessions, message size of multicast session
   information, and bandwidth SAP uses. Let us assume the average
   message size of a single multicast session information is about 300
   bytes. When there are more than 500 active multicast sessions, an
   interval time of each session announcement becomes greater than 200
   seconds and the average announcement interval increases accordingly.
   For instance, if 2000 multicast sessions are active in the Internet,
   each session announcement interval is between 800 seconds and 1600
   seconds. In this case, if some SAP message is lost, users may need
   to wait 1600 seconds for the next announcement as maximum.

   Obviously, it is possible to make the announcement interval shorter
   by changing the SAP configuration on a sender side and provide
   shorter latency for the sender-receiver communication. However, it
   makes the total amount of SAP messages transmitted larger and may
   increase the probability of creating congestions.

3.2. Difficulties in Scope Definition

   Multicast data senders or network administrators may want to define
   an area where data packets sent within a session will be confined.
   This area is called "scope area". An end user who belongs to the
   scope area can receive the session data.

   When IP multicast was initially deployed in the MBone, the Time-To-
   Live (TTL) field of the IP header was used to control the
   distribution of multicast traffic. A multicast router configured
   with a TTL threshold drops any multicast packet in which the TTL
   falls below the threshold. For instance, a router at the boundary of

   an organization configures the threshold to 32, which denotes an
   "organization" scope boundary.

   The drawbacks of this "TTL scoping" are: 1) the senders must be
   sufficiently aware of the network topology to determine the TTL value
   to use, and 2) complex scope areas cannot be defined (e.g., between
   overlapped areas). Especially the first point becomes big obstacles
   for general end users to precisely set up the data distribution area.
   TTL scoping, which only defines a rough granularity, does not provide
   a complete solution.

   The "administratively scoped IP multicast" approach [4] provides
   clear and simple semantics such as scope boundaries are associated to
   multicast addresses. With IPv4, packets addressed to the
   administratively scoped multicast address range 239/8 (i.e. from
   239.0.0.0 to 239.255.255.255) cannot cross the configured
   administrative boundaries. Since scoped addresses are defined
   locally, the same multicast address can be used in different non-
   overlapping areas. Oppositely, an administrator can define multiple
   areas overlap by dividing the administratively scoped address range,
   which is not possible with TTL scoping.

   However, administrative scoping has several major limitations. An
   administrator may want to partition the scope area to disjoint areas
   on a per receiver basis, or he may want to limit data distribution
   according to the transmission rate or the content category of each
   session, or he may want to use the data sender's address as a keyword
   to set up the scope. Note that the latter aspect is nowadays
   feasible since Source-Specific Multicast (SSM) [5] requires that a
   join request specifies both the multicast and source addresses.

   SSM highlights another contradiction in the administrative scoping
   approach: the address range dedicated to SSM, 232/8 with IPv4, cannot
   cover the address range dedicated to administrative scoping, 239/8.
   Although the problem can be solved by defining yet another SSM
   specific administrative scoping address range, defining a new
   addressing architecture requires modifying application, end host, and
   router implementations or configurations. Hence, using multicast
   addresses to define a scope is not a complete solution either.

3.3. ASM Dependency

   SAP relies on the ASM model, since every SAP instance can send
   announcements in the SAP announcement group. For instance, to
   receive SAP announcement messages for the global scope IPv4 multicast
   sessions, all prospective receivers must join session 224.2.127.254
   (without specifying any source address). This is another major
   limitation of SAP since some Internet Service Providers (ISPs) may

want to provide only SSM multicast routing. It is known that a
versatile announcement protocol should not rely on any specific
routing architecture.

Moreover, this communication model is subject to a Denial-of-Service
attack. If malicious hosts flood high bandwidth stream to this
global announcement address, 224.2.127.254, then all prospective
receivers including multicast routers listening SAP messages take in
the stream and their networks may be corrupted or destroyed.

4. **Lack of Sender and Receiver Control in Announcement**

   Network administrators or service providers may want to define
   approved senders and restrict multicast data transmissions or
   announcement only from them. However, in a spontaneous announcement
   protocol, it is impossible to allow to send announcement messages
   only from approved senders or make non-approved senders stop sending
   announcement messages.

   In addition, it is difficult to hide multicast session information
   announced by an announcement protocol from non-approved receivers if
   they are inside the scoped network. For instance, SAP messages might
   be encrypted to prevent non-authorized client from reading them.
   However, it adds more complexity to SAP by combining with additional
   key sharing mechanism.

   Conceptually, it is difficult to disallow non-approved data receivers
   to receive session information announced by an announcement protocol,
   if the announcement data is flooded to their network. It is the
   basic concept that IP multicast requires scoping configuration to
   address this issue. However, defining a fine-grained scope areas
   with using TTL or a multicast address range is a big challenge as
   described in Section 3.2.

5. **Potential Problems in Central Server Model**

   Emails, RSS (Rich Site Summary or Really Simple Syndication), and the
   Web are the alternative ways of conveying session descriptions.
   These applications are of wide use and can be used to carry many
   kinds of information. However, to provide a multicast announcement
   function, these approaches would have to rely on a central server or
   a central management system. This server-based approach reduces
   flexibility of fine-grained user and session management.

   Session announcement should be decided by data senders or
   administrators policy, such as scoping policy [4], or content-level
   or user-level access control, to define "who can access which
   contents". Defining and applying such site-local policy or user
   management would be very difficult or impossible on a single server
   in the global Internet. This condition contradicts the requirements
   experienced in the traditional MBone and expected in current or
   future use.

   In addition, emails and the RSS feed are implemented with a
   "subscription model". The subscription model requires end users to
   know the address of service providers and have subscribed to the
   services for getting session information prior to receiving the
   contents information. This condition is not reasonable for session
   announcement, because end users do not always know potential data
   senders.

   Finally, server-based systems may require a large amount of
   operational costs or cause scalability problems for the fine-grained
   user and session management and session announcement, especially when
   the systems need to support a large number of users and contents
   information.

6. **Potential Problems in Discovery Model**

   Session information discovery is another possible approach to
   retrieve session information. Currently, there are information
   discovery systems largely deployed in the Internet. However, an
   information discovery system usually adopts crawling method to
   discover information. If an information discovery system is used for
   session information discovery, it not only causes a number of traffic
   but also takes time for gathering all available session information
   in the entire Internet or updating the collected session information.
   This is a drawback for searching the available IP multicast session
   information, because many of IP multicast sessions are possibly
   launched and terminated highly dynamically.

   Another issue resided in an information discovery system is that it
   is difficult to enable a scoping function on it, as each site-local
   operator or administrator does not control the service, especially
   when the system is implemented with the server-based approach as
   described in Section 5.

7. **Requirements**

   According to the analyses aforementioned, the requirements for IP
   multicast session announcement are defined as follows;

   o Information consistency: Information consistency, which warrants
      that end users have a consistent view of session announcement, is
      of major importance.

   o Low information update latency: IP multicast session would be
      fully dynamic. The list of sessions should be updated rapidly
      after the creation, modification, or removal of the session
      information.

   o Low bandwidth consumption: IP multicast session announcement
      should effectively consume the network bandwidth so that it does
      not affect other communications or services.

   o Scalability: Session announcement can be used by a large number of
      end users spread throughout the Internet, and can manage a very
      large number of sessions.

   o High availability: The scheme must be robust in front of host/link
      failures and packet losses. This can be fulfilled either by
      transmitting messages periodically or by keeping track of failures
      and recovering them.

   o Scope control: Scope control is required to preserve bandwidth
      resources and offer a certain level of confidentiality in IP
      multicast communication.

   o Sender control: Administrators must be able to allow to announce
      multicast sessions only from approved multicast senders.

   o User access control: Administrators or data senders must be able
      to configure approved multicast data receivers. They must be able
      to filter out malicious users.

   o No dependency on a routing architecture: The session announcement
      scheme must accommodate (or be independent of) any kind of
      multicast routing protocol or communication model.

   o Security consideration: In order to provide secure multicast
      communication, session announcement should have a function that
      enables to encrypt session information and distribute it to only
      the legitimate users.

8. References

8.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to indicate requirement
     levels", RFC 2119, March 1997.

[2] Handley, M., Perkins, C., and E. Whelan, "Session Announcement
     Protocol", RFC 2974, October 2000.

[3] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session
     Description Protocol", RFC 4566, July 2006.

[4] Mayer, D., "Administratively scoped IP multicast", RFC 2365,
     July 1998.

[5] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP",
     RFC 4607, August 2006.

8.2. Informative References

[6] Asaeda, H. and V. Roca, "Policy and Scope Management for
     Multicast Channel Announcement", IEICE Trans. on Information and
     Systems, Vol.E88-D, No.7, pp.1638-1645, July 2005.

Authors' Addresses

    Hitoshi Asaeda
    Keio University
    Graduate School of Media and Governance
    5322 Endo
    Fujisawa, Kanagawa 252-8520
    Japan

    Email: asaeda@wide.ad.jp
    URI: http://www.sfc.wide.ad.jp/~asaeda/

    Vincent Roca
    INRIA
    Planete Research Team
    655, Avenue de l'Europe
    Montbonnot - Saint Martin, Saint Ismier 38334
    France

    Email: vincent.roca@inrialpes.fr
    URI: http://planete.inrialpes.fr/~roca/