Gap Analysis in IP Multicast Dissemination

Hitoshi Asaeda[1] and Bill Manning[2]

[1] Graduate School of Media and Governance
Keio University
5322 Endo, Fujisawa
252-8520 Kanagawa, Japan
asaeda@wide.ad.jp
[2] Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, CA 90292
bmanning@karoshi.com

Abstract. IP multicast is advantageous for high quality streaming applications and future needs in the Internet. However, it is generally recognized that IP multicast requires significant routing coordination and configuration, and hence its routing protocols are non-scalable. Recently, Source-Specific Multicast (SSM) has been standardized and proposed as the deployable IP multicast communication architecture. SSM basically works for the one-to-many communication, and eliminates many of the complexities the traditional many-to-many multicast communication has. While SSM gives advantages for the IP multicast deployment, there is still a gap between what is reported as the state-of-the-art in the literature and what could be implemented in practice.

In this paper, we analyze the deployment barriers SSM creates, and consider how we can ease some of the barriers. To define the possible approaches, we discuss the functions SSM requires, and the necessary components network operators and application developers need to know for fulfilling the demand.

Keywords: IP multicast, SSM, multicast deployment.

1 Introduction

IP multicast is designed to distribute data to a large number of receivers in the Internet. It is advantageous for high quality streaming applications and envisioned future needs in the Internet. In contrast, although there is much research work related to IP multicast technologies and most router vendors already support basic IP multicast routing protocols, IP multicast has not fully deployed in the Internet yet. One of the main reasons is that it is generally recognized that IP multicast requires significant routing coordination and configuration, and hence its routing protocols are fairly complex and non-scalable, and network administrators and application developers believe that IP multicast requires additional maintenance and operational costs.

S. Fdida and K. Sugiura (Eds.): AINTEC 2007, LNCS 4866, pp. 199–212, 2007.

Recently, Source-Specific Multicast (SSM) [1] has been proposed as the deployable IP multicast communication architecture. SSM basically works for the one-to-many communication in which a single data sender transmits data to multiple receivers, and eliminates many of the complexities the traditional many-to-many multicast communication has. Moreover, IP multicast technology has been rapidly increasing in perceived importance and growing due to the emergence of IPTV services (in the broad sense) these days. SSM ideally fits an IPTV's communication style, and the IP multicast deployment should have been accelerated. However, the situation was not drastically changed. One of the reasons is that the alternative approaches like Application Layer Multicast [12] or P2P multicast can work well in the current Internet without requiring significant protocol change. But the fundamental point is that, regarding the IP multicast and SSM deployment, there is still a big gap between what is reported as the state-of-the-art in the literature and what could be implemented in practice.

In this paper, we analyze some of the deployment barriers SSM creates, and discuss how we can ease the barriers and grow SSM use. To define the possible approaches, we discuss the functions SSM requires, and the necessary components network operators and application programmers need to know for fulfilling the demand. In fact, there are many alternative approaches, like ALM and overlay multicast [13], that support data distribution to multiple receivers without using IP multicast. Knowing these technologies is important, but showing the future direction toward the IP multicast deployment is the main aim of this paper, and the discussions related to these alternative approaches are out of scope of this paper.

The remainder of this paper is organized as follows: Section 2 briefly explains the SSM architecture and its functions. In this section, we describe the advantages of SSM and the required protocols to make the SSM communication viable in operations. Obsolete protocols that are not used in SSM networks are also mentioned to contrast prior multicast efforts. By showing the statistical trends measured in the target networks, most applications used in the Internet would be able to work on SSM only multicast networks. Section 3 analyzes the gap between the SSM deployment scenarios or strategies and the unsolved issues remaining in the SSM architecture. Note that some issues are very broad and are not completely solved with the current stage. This paper clarifies the points we need to discuss and gives the first steps toward the future solution. Section 4 concludes the discussions and describes the points as the future work.

2 Source-Specific Multicast

2.1 Concepts

Multicast communication has run into barriers to its wide-scale deployment. Mainly, these barriers are rooted in the problem of building efficient multicast

routing trees for dynamic group memberships [16]. More precisely, a PIM-SM protocol [2] provides many-to-many communication by using a Rendezvous Point router (RP) and maintaining a shared-tree called a Rendezvous Point Tree (RPT). After PIM routers construct an RPT, they discover the source address whose data is transmitted along the RPT, and switch to the optimal source-rooted Shortest-Path Tree (SPT). Since the routing states between RPT and SPT may be frequently changed, the router procedures require complex algorithms and do not scale well. In addition, in order for an RP to notify information about active sources in a local PIM domain to other domains, Multicast Source Discovery Protocol (MSDP) [3] cooperates with PIM-SM. MSDP provides a mechanism to connect multiple PIM domains by managing multiple RPs in the entire Internet, yet it introduces extra message handling and burden in routers.

On the other hand, in a one-to-many communication environment, each receiver can notify interesting source address(es) with group address to the upstream router on the same LAN as group membership information upon request. In this communication architecture called Source-Specific Multicast (SSM) [1], a multicast data receiver specifies both source and group addresses for his join or leave request. The collaborative effort with source and multicast address specification eliminates the source address discovery procedure from multicast routing protocols. Furthermore, in this communication, a multicast router can eliminate the process of coordinating and maintaining a shared-tree because it can directly construct a source-based tree from its initial protocol phase. At the protocol level, PIM-SM working on SSM solely maintains an explicit source-based SPT. As the result, an RP can be eliminated from any PIM domains in this communication, and hence the scalability problem (mainly caused by RP-to-group mapping) is effectively reduced from the multicast routing protocol.

2.2 Protocols

The multicast protocol architecture works with a common set, including a data sender, a data receiver, and a multicast router. Host-to-router communication is provided by the Internet Group Management Protocol (IGMP) for IPv4 and Multicast Listener Discovery (MLD) for IPv6. When a data receiver wants to join or leave multicast sessions, it notifies the multicast group address by sending an IGMP/MLD join or leave message to the upstream multicast router.

In an SSM environment, a data receiver must send an IGMP/MLD join or leave message that specifies the source address(es), as well as the multicast address, referred to as (S,G) join/leave message to its upstream router. This host-side extension to send a join or leave message with the pair of interesting source and group addresses is done using IGMP version 3 (IGMPv3) [5] for IPv4 and MLD version 2 (MLDv2) [6] for IPv6.

As well, it is indispensable that every receiver site router must support IGMPv3 and MLDv2 protocols in order to recognize the (S,G) join/leave messages sent from the data receivers. Since SSM is a subset of a PIM-SM routing

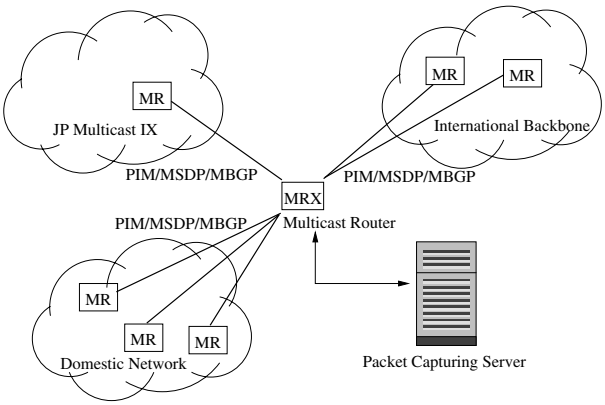

Fig. 1. Network and server configuration

protocol, it is not necessary for PIM-SM to add special functions to support SSM. Oppositely, there are unused protocols or router functions that are not necessary to be used in the SSM communication. Since an RP is not used in SSM, clearly MSDP is not needed if the network works with an SSM only network.

2.3 Statistical Trends

We obtained experimental data through our operational experience and analyzed the statistical trends in international multicast backbones using the following measurements to understand the current situation and future needs of IP multicast services [16].

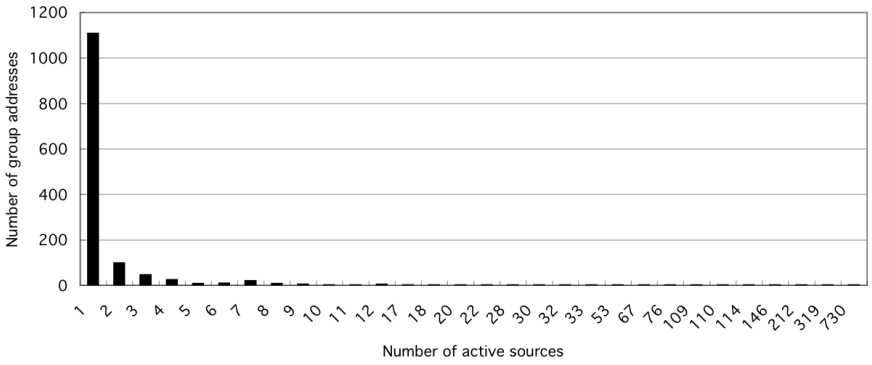

Fig. 2. Number of active data sources per multicast session

Figure 1 shows the topology of the target networks. The Japanese multicast backbone is known as "JP Multicast IX", which was previously established for

multicast data exchange over MBone. The "Domestic Network" is a network to which the WIDE project [27] and other Japanese research communities are connecting. The "International Backbone" is the connection to Abilene [28] via TransPAC [29]. Our multicast router (MRX – Juniper M20 with JUNOS 5.7) was connected to six multicast routers (MRs) using Gigabit Ethernet interfaces. These routers used PIM-SM, MSDP, and MBGP [4] to exchange each routing information required for IPv4 multicast routing. The "Packet Capturing Server" was a PC (Dell PowerEdge 2650 with FreeBSD 5.1) equipped with 2 GB memory and 160 GB hard-disk. It was used to collect routing information from our multicast router MRX. It ran a program that logged into the router to extract the MSDP and MBGP routing information at eight-hour intervals from Feb. 28 to Mar. 13, 2004.

From the extracted data, distribution of the number of senders per group was obtained. Figure 2 shows that more than 90% of the multicast sessions were categorized as one-to-many communication, in which a data sender is only one node in a multicast session and the number of the data receivers is many, although the network infrastructure supported traditional many-to-many communication, in which both of data receivers and data senders are potentially many. This fact indicates that currently many-to-many communication is not widely used from the viewpoint of multicast service providers. In other words, one-to-many communication does not interfere with the steady deployment of IP multicast, and hence we believe there should be no problem in replacing the many-to-many communication with the one-to-many communication in IP multicast. In fact, a few multicast sessions were advertised from a large number of senders (e.g. 212, 319, and 730). Yet, they were used for the multicast session announcement by the SAP [15] protocol, which requires multicast data senders send announcement messages to the corresponding multicast addresses.

3 Gap Analysis

3.1 Operational Considerations

Network operations have not embraced IP multicast in any of its forms outside of what might be considered a single broadcast domain. This may be due to the fact that multicast inherits many of the same attributes of its predecessor, broadcast. In essence, multicast "floods" a network with a packet that must be replicated so as to reach all the nodes in a group. This behavior leads to the first operational consideration; Router design. All known routers are designed and optimized to handle unicast packet forwarding. The upshot of this implementation choice is that the multicast handling is pushed to high-overhead systems, usually in general purpose CPU and software. As a result, network operators find multicast processing to be slower than unicast and to consume more infrastructure resources in the form of CPU cycles and memory consumption. In fact, SSM routers need to maintain the routing entries that are composed of complete source-group address pairs (known as "channels" as explained in the next section) in their routing tables. Since it is currently impossible to aggregate

the routing entries, network operators may concern that SSM much consumes router memory and does not improve the deployment condition.

A second consideration is that by its design, multicast does not have the functional equivalent of an External Gateway Protocol (EGP) like the unicast Boarder Gateway Protocol (BGP) [19]. For operators, this means that multicast must be artificially constrained or allowed by packet filtering or access controls at the unicast policy edges, where one network interconnects to another. Each of these considerations may be considered a gap in the roadmap to effective, wide-scale deployment of IP multicast or even SSM. Neither is further considered in this paper.

Lack of effective monitoring tools also limits the IP multicast deployment activities on an operator side. While lightweight multicast monitoring tools, like mtrace2 [20] and ssmping [21], have been recently proposed in the IETF MBONED working group, these tools may be too simple and difficult to satisfy to monitor any kind of situation.

3.2 Multicast Address Assignment

According to an IP multicast addressing architecture, a transient multicast address is dynamically assigned to a multicast session for its entire duration. Traditionally, there had been issues how the multicast address is uniquely assigned in the entire Internet and proposals to address the issues [30,31]. Yet, these proposals require that hosts (or applications) access to the address allocation servers that are well coordinated in the entire networks, where this requirement is difficult to be implemented with scalable manners.

Instead, GLOP [24] and EGLOP [25] for IPv4, and unicast-prefix-based IPv6 multicast addresses [26] have been commonly used. GLOP is the standard definition that describes an experimental policy for use of the IPv4 multicast address range by mapping 16 bits of Autonomous System (AS) number into the middle two octets of 233/8 to be uniquely assigned to that ASN. While this technique is simple and successfully used, the assignments are inefficient because of the cases in which users do not have its own AS or have ASN longer than 16 bits. Therefore EGLOP can be used as the extension of GLOP. In the absence of an assigned ASN, the sites then use private ASN. Unicast-prefix-based IPv6 multicast addresses is straightforward, since the source address prefix is inserted (embedded) in the IPv6 multicast address (FF3x::/32, where "x" is any valid scope value) used by the source.

SSM solves the addressing problem, because a "channel" is identified not only by the group address but also by the source address (i.e. (S,G) pair). Since the unique channel is composed of both the multicast address and the source address, the multicast address does not longer have to be globally unique. Hence, in SSM, multicast address allocation is not a global issue but rather a local decision (e.g. by an Internet Service Provider's policy).

However, SSM highlights another contradiction in the IPv4 addressing schema. SSM addresses are allocated in the special SSM range of 232/8 for IPv4. This means that the SSM sources cannot interoperate with GLOP/EGLOP

addressed targets. Of course, it is not disallowed to create a multicast channel with non-SSM address range, network administrators or application developers may confuse or conflict in their thoughts.

3.3 Session Information Announcement

Due to the multicast addressing schema, a multicast data receiver needs to resolve a multicast address of the session whenever he joins the session. However, a traditional multicast session and address announcement architecture does not support access control methods to provide the session information including data sender address only to the legitimate members, and hence any user can get multicast session information by accessing a public session directory, e.g., *sdr*.

There would be two possible solutions to resolve a multicast address: one is the use of an address discovery mechanism, and the other relies on an address announcement model. The former model can use the Session Invitation Protocol (SIP) [14] and the later model can use the Session Announcement Protocol (SAP) [15]. In SIP environment, since the inviter must know the unicast addresses of all possible participants beforehand, it is not suited to large multicast sessions. On the other hand, SAP multicasts session information to keep all the session directory instances synchronized. However, such periodic session announcement to whole network not only brings a scalability problem, and is not appropriate to limit the user access nor to bring the privacy and secrecy of a user, in order to advertise private sessions only to the legitimate user.

SAP has several major limitations including scalability problem as explained in [17]. The biggest issue here is that SAP relies on the many-to-many multicast communication 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 clients must join session 224.2.127.254 [15] (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. We believe that a versatile announcement protocol must not rely on any specific routing architecture. the user would get only the available session information individually, and moreover the network administrator or the data sender can avoid bogus join request.

One of the possible idea is to use a distribute session directory system, like Channel Reflector [18]. It aims to provide a concrete implementation that enables the announcement of multicast session parameters. It could handle current and future needs, in particular when considering the scalability in terms of session announcements, the need for policy and scope control mechanisms, and the support of any group communication system, including SSM scheme.

3.4 Multicast Security

We know that security threats against IP multicast would have a catastrophic effect on IP multicast deployment in the Internet. For the clarification, IP

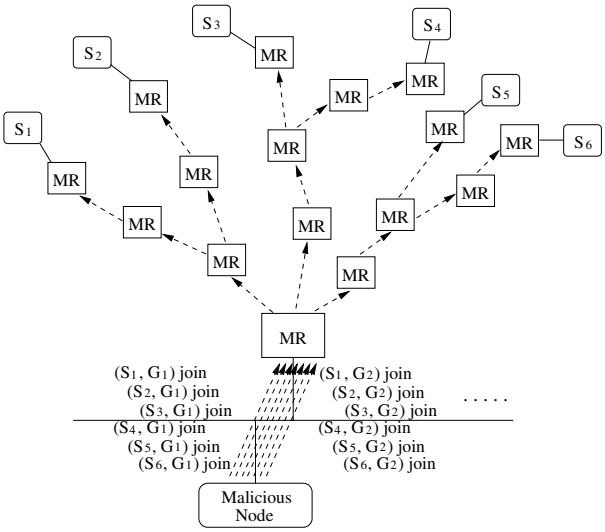

Fig. 3. Receiver-based attack

multicast security should be categorized into three points; (1) infrastructure protection, (2) contents protection, and (3) privacy. In this section, we mainly discuss infrastructure protection, and introduce some activities for contents protection. Privacy issue is skipped as the future issue.

Regarding the infrastructure protection, as described by Savola et al. of the IETF MBONED working group document [32], the security threats are categorized into "source-based" and "receiver-based" attacks. In short, the former is a DoS attack against the multicast networks, in which data is sent to numerous and random group addresses, and the latter is a DoS attack against multicast routers, in which innumerable IGMP/MLD joins are sent from a client.

In terms of multicast routing stability, source-based attacks are very serious. Generally, the data sender will keep streaming data even if there is no data receiver for the data. To make things worse, multicast routers, including first-hop routers, do not recognize or cannot reject these packets. In fact, MSDP has caused When a data sender starts sending data, the RP in the sender's PIM domain forwards Source Active (SA) messages to each MSDP neighbor router (peer), and the SA messages are forwarded hop-by-hop. SA messages used in MSDP are easily flooded throughout the PIM domains. This situation has induced denial-of-service (DoS) attacks, like *Ramen Worm* [22] and *Sapphire* [23]. These DoS attacks presumed on the MSDP architecture and overwhelmed the multicast infrastructure. However, these kinds of attacks do not affect SSM, in which the first-hop router can discard multicast data packets that do not have a corresponding routing entry.

On the contrary, SSM is not robust against receiver-based attack. In the many-to-many communication, a PIM-SM router initially constructs an RPT in order

to find available sources for requested multicast address, and switches to each SPT for active sources. This behavior implies that a PIM-SM router working with the many-to-many communication model does not voluntarily construct a *non-active* SPT.

On the other hand, an SSM capable router constructs an SPT with no shared tree coordination. Thus, even if a host triggers invalid or unavailable (S,G) joins, the upstream router starts establishing all SPTs with no intellectual decision (Figure 3). This attack not only largely increases the router's routing table size and its memory by an unlimited number of malicious (S,G) joins, but also affects a large number of multicast routers along the invalid routing paths in the entire Internet. What is worse is that these multicast routers cannot recognize the original router that is attacked and cannot stop the attack itself. By using some timer mechanism to monitor the data flow, it would be possible to prune unavailable (S,G) entries from the routing table. But it is neither a great deal of the solution for tens of thousands of bogus requests.

In summary, because there is no channel validation mechanism in a router side working in the SSM communication, SPT coordination triggered by (S,G) join request may bring another security concern. In addition, current IGMPv3 and MLDv2 do not have a standard mechanism to validate requested joins. It is necessary to propose some mechanism that recognizes and notifies valid join requests to these protocols or routers.

Regarding contents protection, the IETF MSEC working group has been working to standardize protocols by which only legitimate members will have access to contents. The major issues focused on the MSEC working group are related to the group key management architecture [33] and has proposed corresponding protocols [34,35]. These architecture and protocols are necessary components, but more appropriate security model should implement the access control mechanism by the session announcement level. As the beneficial approach, the multicast session announcement scheme is included in the multicast security architecture that authenticates and authorizes legitimate users before giving the session information. Securing the session directory architecture provides security at each level of interaction with users; thus it guarantees privacy and secrecy for any members who join to multicast sessions.

3.5 Filter-Mode Operation

IGMPv3 and MLDv2 implement INCLUDE and EXCLUDE filter-modes that are introduced to support the source filtering function, as well as a source address specification function. If a host wants to receive from specific sources, it sends an IGMPv3 or MLDv2 report with specifying the source addresses and the filter-mode set to INCLUDE. If the host does not want to receive from sources, it sends a report with specifying the source addresses and filter-mode set to EXCLUDE.

The INCLUDE and EXCLUDE filter-modes are also defined in a multicast router to process the IGMPv3 or MLDv2 reports. When a multicast router receives the report messages from its downstream hosts, it forwards the corresponding multicast traffic by managing requested group and source addresses.

The INCLUDE filter-mode is necessary to support SSM by specifying interesting source addresses. However, practical applications do not use EXCLUDE mode to block sources very often, because a user or application usually wants to specify desired source addresses, not undesired source addresses. Even if a user wants to explicitly refuse traffic from some sources in a group, when other users in the same shared network have an interest in these sources, the corresponding multicast traffic is forwarded to the network.

There is a proposal of the simplified versions of IGMPv3 and MLDv2, named Lightweight IGMPv3 (LW-IGMPv3) and Lightweight MLDv2 (LW-MLDv2) [8], in which EXCLUDE filter-mode is eliminated. Not only are LW-IGMPv3 and LW-MLDv2 compatible with the standard IGMPv3 and MLDv2, but also the protocol operations made by data receiver hosts and routers or switches (performing IGMPv3/MLDv2 snooping) are simplified in the lightweight protocol, and complicated operations are hence effectively reduced. Since LW-IGMPv3 and LW-MLDv2 are fully compatible with the full version of these protocols (i.e., the standard IGMPv3 and MLDv2), hosts or routers that have implemented the full version do not need to implement or modify anything to cooperate with LW-IGMPv3/LW-MLDv2 hosts or routers.

In fact, the aim of LW-IGMPv3 and LW-MLDv2 is not only for contributing to the implementation or reducing the memory size on a host. One of the big advantages is that it highly reduces the processing cost on upstream routers by eliminating the EXCLUDE filter-mode operations. If both INCLUDE and EXCLUDE filter-mode operations are supported in the networks, the routers need to maintain all source addresses joined from end hosts. Even if an SPT is well coordinated by (S,G) joins given by SSM-capable receivers, the routers need to refresh (and re-generate) some or all of the corresponding routing paths including the RPT whenever the downstream host requests EXLUDE filter-mode join. According to this unwilling scenario, LW-IGMPv3 and LW-MLDv2 that disable EXCLUDE filter-mode operations are further encouraged to grow SSM only networks.

3.6 Application Development

When a multicast application requests a new (S,G) join, it uses embedded Application Program Interfaces (APIs) to control socket operations. For the SSM communication, Multicast Source Filtering (MSF) APIs for `setsockopt()`, `getsockopt()` and `ioctl()` are defined [7]. These APIs are classified to the "IPv4 MSF API" and the "Protocol-Independent MSF API". In an IPv6 application, the Protocol-Independent MSF API is used.

As another taxonomy, the "Basic API" and the "Advanced API" are available to provide independent usage for each API. The Basic API uses `setsockopt()` and `getsockopt()` functions and can minimize changes needed in existing multicast application source code to add the source address filtering operations. The following example shows a part of a multicast application, which uses the Basic API of the IPv4 MSF API.

Usage-1: IPv4 Basic MSF API

```
bcopy(&in_grp, &ims.imr_multiaddr, sizeof(in_grp));
bcopy(&in_src, &ims.imr_sourceaddr, sizeof(in_src));

if (setsockopt(socket, IPPROTO_IP, IP_ADD_SOURCE_MEMBERSHIP,
    (char *)&ims, sizeof(ims)) < 0)
        perror("cannot listen group");
```

This application first copies the multicast address (`in_grp`) to `ims.imr_multiaddr` and a source address (`in_src`) to `ims.imr_sourceaddr` respectively. And then it calls `setsockopt()` function with `IP_ADD_SOURCE_MEMBERSHIP` operation defined as the Basic API for the `INCLUDE` (S,G) join request.

The example using Protocol-Independent MSF API for IPv6 is as follows:

Usage-2: IPv6 (Protocol Independent) Basic MSF API

```
bcopy(&grp, &gsr.gsr_group, grp.sin6_len);
bcopy(&src, &gsr.gsr_source, src.sin6_len);

if (setsockopt(socket, IPPROTO_IPV6, MCAST_JOIN_SOURCE_GROUP,
    (char *)&gsr, sizeof(gsr)) < 0)
        perror("cannot listen group");
```

As shown above, it is easy to adapt MSF APIs to existing applications. The biggest concern is to recognize which APIs can be used on your OS. For instance, Windows XP only supports IPv4 MSF API, and Windows Vista supports both IPv4 and Protocol-Independent MSF APIs (i.e. Basic APIs), but non of them supports Advanced APIs. The latest Linux supports all MSF APIs in definition. Current BSD OSes and MacOS X do not officially support any MSF API, while we have provided LW-IGMPv3 and LW-MLDv2 kernel patches [9,10], which supports Basic APIs. According to this scenario, cross platform compatibility is sacrificed because of incompatible APIs, and therefore, application developers who need to support various OSes should insert procedures to check whether the OSes support SSM and which API can be used in the source codes.

We definitively need the guideline mentioning the newly developed applications should use either `IP_ADD_SOURCE_MEMBERSHIP` or `MCAST_JOIN_SOURCE_GROUP`, because these commands are supported by both IGMPv3/MLDv2 and LW-IGMPv3/LW-MLDv2 implementations, and simply request the SSM communication by invoking INCLUDE mode (S,G) join. And also, using `IP_BLOCK_SOURCE` and `MCAST_BLOCK_SOURCE` on an IGMPv3/MLDv2 capable host is harmful, because these commands invoke EXCLUDE filter-mode operations and request to construct an RPT to the upstream routers as described in Section 3.5.

4 Conclusions and Future Work

Source-Specific Multicast (SSM) is designed as the deployable IP multicast communication architecture, and the demands of IP multicast technology have been rapidly increasing in perceived importance and growing these days. However, it still requires operational functions and application development manners for its smooth deployment. In this paper, we analyze the deployment barriers resided in IP multicast or SSM deployment, and consider how we can ease some of the barriers. We also discuss the functions SSM requires, and the necessary components network operators and application developers need to know for fulfilling the demand.

As well as addressing remaining issues aforementioned in this paper, we would like to propose much robust routing technology that creates robust routing paths. There has been recently proposing various ways to fulfill the demand like [36], and we believe it is the indispensable research topic.

Multicast AAA should be separately discussed from multicast security. Although the IETF MBONED working group has been trying to standardize AAA frameworks for common multicast services, providing the scalability and combining group key management architecture sec:msec are vital. We definitively need the concrete implementations and must verify the integrated behavior.

As another issue, multicast Quality-of-Service (QoS) is also the sensitive requirement especially for service providers who want to make accounting to their customers. It is a challenge to guarantee the contents quality at a reasonable level, and it would be the hot research topic for the Internet communities.

References

1. Holbrook, H., Cain, B.: Source-Specific Multicast for IP. RFC4607, August (2006)
2. Fenner, B., Handley, M., Holbrook, H., Kouvelas, I.: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). RFC4601 (August 2006)
3. Fenner, B., Meyer, D.: Multicast Source Discovery Protocol (MSDP), RFC3618 (October 2003)
4. Bates, T., Chandra, R., Katz, D., Rekhter, Y.: Multiprotocol Extensions for BGP-4, RFC2283 (February 1998)
5. Cain, B., Deering, S., Kouvelas, I., Fenner, B., Thyagarajan, A.: Internet Group Management Protocol, Version 3. RFC3376 (October 2002)
6. Vida, R., Costa, L.: Multicast Listener Discovery Version 2 (MLDv2) for IPv6, RFC3810 (June 2004)
7. Thaler, D., Fenner, B., Quinn, B.: Socket Interface Extensions for Multicast Source Filters, RFC3678 (January 2004)
8. Liu, H., Cao, W., Asaeda, H.: Lightweight IGMPv3 and MLDv2 Protocols. Internet Draft (work in progress), draft-ietf-mboned-lightweight-igmpv3-mldv2-01.txt (June 2007)
9. LW-IGMPv3 Host-side Implementation for NetBSD, `http://www.sfc.wide.ad.jp/~asaeda/LW-IGMPv3`

10. LW-MLDv2 Host-side Implementation for NetBSD, http://www.sfc.wide.ad.jp/~asaeda/LW-MLDv2
11. Casner, S., Deering, S.: First IETF Internet Audiocast. ACM SIGCOMM Computer Communication Review 22(3), 92–97 (1992)
12. El-Sayed, A., Roca, V., Mathy, L.: A Survey of Protocols for an Alternative Group Communication Service. IEEE Network 17(1), 46–51 (2003)
13. Wang, W., Helder, D., Jamin, S., Zhang, L.: Overlay Optimizations for End-host Multicast. In: NGC 2002. Proc. Int'l Workshop on Networked Group Communication, pp. 154–161 (October 2002)
14. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol, RFC3261 (June 2002)
15. Handley, M., Perkins, C., Whelan, E.: Session Announcement Protocol, RFC2974 (October 2000)
16. Asaeda, H., Suzuki, S., Kobayashi, K., Murai, J.: Architecture for IP Multicast Deployment: Challenges and Practice. IEICE Trans. on Communications E89-B(4), 1044–1051 (2006)
17. Asaeda, H., Roca, V.: Policy and Scope Management for Multicast Channel Announcement. IEICE Trans. on Information and Systems E88-D(7), 1638–1645 (2005)
18. Asaeda, H., Pokavanich, W., Yamamoto, S.: Channel Reflector: An Interdomain Channel Directory System. IEICE Trans. on Communications E89-B(10), 2860–2867 (2006)
19. Rekhter, Y., Li, T.: A Border Gateway Protocol 4 (BGP-4), RFC1771 (March 1995)
20. Asaeda, H., Jinmei, T., Fenner, B., Casner, S.: Mtrace Version 2: Traceroute Facility for IP Multicast. Internet Draft (work in progress), draft-asaeda-mboned-mtrace-v2-00.txt (July 2007)
21. Venaas, S., Santos, H.: ssmping Protocol. Internet Draft (work in progress), draft-ietf-mboned-ssmping-01.txt (July 2007)
22. Rajvaidya, P., Ramachandran, K., Almeroth, K.: Detection and Deflection of DoS Attacks Against the Multicast Source Discovery Protocol. In: Proc. IEEE INFOCOM 2003 (March 2003)
23. Rajvaidya, P., Ramachandran, K., Almeroth, K.: Managing and Securing the Global Multicast Infrastructure. Journal of Network and Systems Management (JNSM) 12(3), 297–326 (2004)
24. Meyer, D., Lothberg, P.: GLOP Addressing in 233/8, RFC3180 (September 2001)
25. Meyer, D.: Extended Assignments in 233/8, RFC3138 (June 2001)
26. Haberman, B., Thaler, D.: Unicast-Prefix-based IPv6 Multicast Addresses, RFC3306 (August 2002)
27. The WIDE Project, http://www.wide.ad.jp/
28. Abilene Backbone Network, http://abilene.internet2.edu/
29. The TransPAC2 Project, http://www.transpac.org/
30. Hanna, S., Patel, B., Shah, M.: Multicast Address Dynamic Client Allocation Protocol (MADCAP), RFC2730 (December 1999)
31. Radoslavov, P., Estrin, D., Govindan, R., Handley, M., Kumar, S., Thaler, D.: The Multicast Address-Set Claim (MASC) Protocol. RFC2909 (September 2000)
32. Savola, P., Lehtonen, R., Meyer, D.: Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements, RFC4609 (October 2006)

33. Baugher, M., Canetti, R., Dondeti, L., Lindholm, F.: Multicast Security (MSEC) Group Key Management Architecture, RFC4046 (April 2005)
34. Baugher, M., Weis, B., Hardjono, T., Harney, H.: The Group Domain of Interpretation, RFC3547 (July 2003)
35. Arkko, J., Carrara, E., Lindholm, F., Naslund, M., Norrman, K.: MIKEY: Multimedia Internet KEYing, RFC3830 (August 2004)
36. Arberg, P.: High availability multicast delivery in IPTV networks, http://www.nanog.org/mtg-0706/arberg.html