IEICE TRANS. COMMUN., VOL.E89–B, NO.4 APRIL 2006

INVITED PAPER *Special Section on Internet Technology VI*

Architecture for IP Multicast Deployment: Challenges and Practice

Hitoshi ASAEDA[†a)], ***Member***, **Shinsuke SUZUKI**[††], **Katsushi KOBAYASHI**[†††], ***Nonmembers***, ***and*** **Jun MURAI**[†], ***Member***

SUMMARY IP multicast technology is highly advantageous for various applications and future needs in the Internet. Yet, it is generally recognized that the IP multicast routing protocol is fairly complex and non-scalable and requires additional maintenance and operational cost to network administrators. Although there has been much research related to IP multicast and most router vendors already support basic IP multicast routing protocols, there is still a big gap between what is reported as the state-of-the-art in the literature from what is implemented in practice. In this paper, we clarify the complexities of traditional multicast communication and describe possible solutions using the one-to-many multicast communication model called Source-Specific Multicast (SSM). We explain this communication model and the corresponding routing architecture and examine the statistics obtained for the number of multicast routing entries in our backbone router, which is connected to the international backbone. We also introduce our international collaboration activities that are contributing to the deployment and promotion of IP multicast services in the Internet.

key words: *IP multicast, Source-Specific Multicast, multicast statistics, M6Bone*

1. Introduction

IP multicast saves processing resources at the data sender and saves network bandwidth because only one copy of each data packet is sent over physical links to an unlimited number of receivers. In addition, it enables data to be transferred more quickly to a large number of receivers than with the repeated unicast model because all copies are delivered in parallel by the network.

The properties of multicast communication are defined as having a *high probability* and a *short delay* in transmitting data to multiple receivers. More specifically, the ratio of successful delivery of multicast packets should remain high enough to allow for the recovery of lost or damaged packets by end-to-end protocols. Additionally, short delays are an important property of many multicast applications, since delivery delays of multicast packets in wide-area networks are usually longer due to the greater geographic extent.

Therefore, optimizing multicast routes is essential for minimizing delays. Multicast routing protocols used in the Internet must be designed to support wide-area routing – a reasonable optimal path must be established between multicast data senders and receivers. Some essential requirements are *scalability*, *simplicity*, and *independence* of the protocols.

Unfortunately, in addition to the benefits offered by multicast routing protocols, there are more complexities than in unicast routing protocols. The major concerns relate to the following difficulties:

- Reverse Path Forwarding
  A multicast router registers not only source and destination addresses but also incoming interface and outgoing interface(s) for each data stream. Such information is needed for the Reverse Path Forwarding (RPF) mechanism to effectively avoid multicast routing loops. However, RPF requires more information than a unicast routing protocol, and multicast routers increase the performance costs and number of required resources.
- Aggregation of routing entries
  Aggregation of unicast routing entries is a widely used and indispensable operation. It is achieved by carefully assigning unicast addresses. However, multicast addresses do not have any network topological dependency, which makes it currently impossible to aggregate multicast routing information upon their exchange.

Understanding the characteristics of multicast routing protocols is needed to create a manageable communication environment and to design a multicast routing protocol that harmonizes with the philosophy of the unicast routing concept. Classifying routing protocol as either "*intra-domain*" or "*inter-domain*" is a fundamental approach. According to the current situation, Protocol Independent Multicast – Sparse Mode (PIM-SM) [1] is the most widely used multicast routing protocol, and many router vendors now support this routing protocol. Nevertheless, it has not yet been widely deployed in the Internet. One of the main reasons is that PIM-SM does not fulfill every requirement of an inter-domain routing protocol we could expect.

In this paper, we discuss current IP multicast routing protocols and technologies, including the Source-Specific Multicast (SSM) [2] architecture, which has recently been recognized as the most feasible multicast communication model for use in the Internet. To understand the situation of IP multicast deployment in the Internet, we investigate experimental data obtained through our operational experi-

Manuscript received October 3, 2005.
Manuscript revised November 22, 2005.
[†]The authors are with Keio University, Fujisawa-shi, 252-8520 Japan.
[††]The author is with ALAXALA Networks Corporation, Kawasaki-shi, 212-0058 Japan.
[†††]The author is with NICT, Koganei-shi, 184-8795 Japan.
a) E-mail: asaeda@sfc.wide.ad.jp
DOI: 10.1093/ietcom/e89–b.4.1044

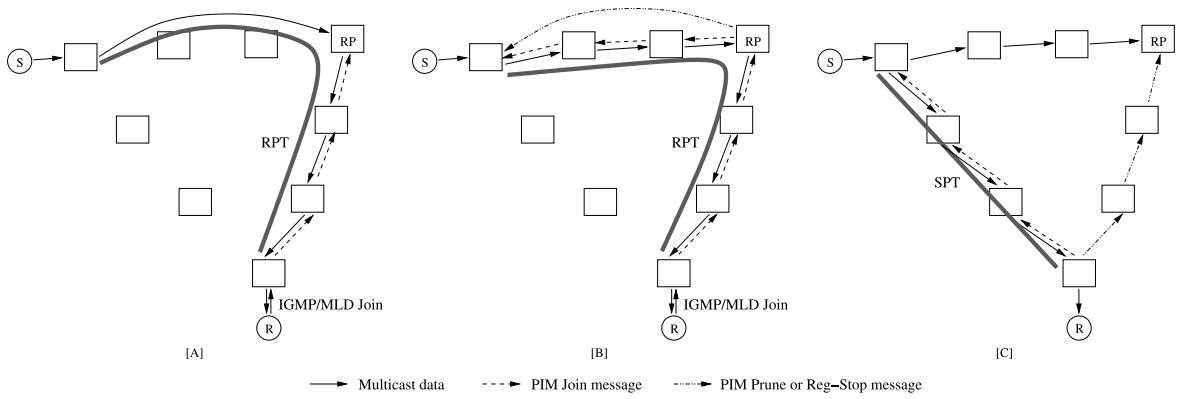

Fig. 1 Establishment of [A], [B] Rendezvous Point Tree (RPT) and [C] Shortest-Path Tree (SPT).

ence. We then introduce MONACO project [3], which is an international collaboration organized by the WIDE project [4] and French M6Bone [5] coordinators to promote future research and further deployment of IP multicast services.

2. Multicast Routing Protocols Used in the Internet

2.1 Protocol Independent Multicast – Sparse Mode (PIM-SM)

The Protocol Independent Multicast – Sparse Mode (PIM-SM) [1] routing protocol is an explicit-join type protocol, which is suitable when multicast receivers are sparse in a wide-area with many hop counts. This multicast routing protocol builds a shared tree called Rendezvous Point Tree (RPT) rooted at a Rendezvous Point router (RP) per group prefix, and then switches the routing tree to a Shortest-Path Tree (SPT) to efficiently forward the data.

Figure 1[A] shows the establishment of a shared tree. When a multicast receiver expresses its interest in receiving multicast data by sending the Internet Group Management Protocol (IGMP) [6], [7] (over IPv4) or Multicast Listener Discovery (MLD) [8], [9] (over IPv6) control messages, a PIM Designated Router (DR) on the receiver's LAN sends a PIM join message to the upstream router toward the RP for the corresponding multicast group G. This message called PIM (*,G) join message travels hop-by-hop toward the RP for the group, and at each router along the path, the multicast tree state for group G is instantiated. When a multicast data sender starts sending data destined for a multicast group, the PIM router on the sender's LAN (i.e. the first-hop router) encapsulates the data and unicasts it to the RP as PIM Register packets. The RP receives the packets, decapsulates them, and then forwards the data to each receiver. After the RP recognizes the sender's address S in the PIM Register packets, it sends a PIM (S,G) join message hop-by-hop toward S to initiate a native multicast route between S and the RP (Fig. 1[B]). Spontaneously the RP sends PIM Register-Stop messages to the first-hop router to get it to stop sending PIM Register packets.

Even though an RPT is used to multicast the data to the receivers, it does not always follow the optimal forwarding path. For many receivers, the route via the RP might involve a detour from the shortest path between the source and the receiver. Consequently, the receiver site router (i.e. the last-hop router) needs to initiate a transfer from the RPT to the source-specific Shortest-Path Tree (SPT) by issuing a PIM (S,G) join message toward S, to enable the data packets to flow smoothly to the receiver. The establishment of an SPT is shown in Fig. 1[C]. Superfluous routing paths, which are part of the RPT, are released by sending PIM prune messages after the SPT is established, while the routing path between S and the RP is kept to send the data to the remaining receivers using the RPT and to new receivers that will use the RPT. Note that there are several tradeoffs involved in using an RPT and an SPT as described by Wei and Estrin [10].

PIM-SM was originally designed for use in wide-areas in which multicast receivers are sparsely distributed. However, it is categorized as an *intra-domain* multicast routing protocol, and not an *inter-domain* multicast routing protocol, because it does not meet the requirements for use in the global Internet. The following problems in particular might be of concern in its routing architecture:

- Traffic concentration
  Multicast data and PIM join/prune messages must go through an RP until or unless an SPT is established. This traffic concentration reduces the protocol scalability and affects heavy loads on an RP if there is a large amount of transmitted data.
- Third-party resource dependency
  When an RPT is used, the RP might be far from the sources or the receivers, which might degrade the quality of the received data due to packet loss or delay on the link between the RP and the senders or the receivers whereas the shortest path between each sender and receiver could be in good condition.
- Bootstrap scalability
  PIM-SM can set up a bootstrap router (BSR) and an RP using a dynamic selection mechanism. With this mechanism, candidate RPs (which may become backup RPs) periodically unicast their availability to the BSR, and the BSR periodically announces the candidate RPs ad-

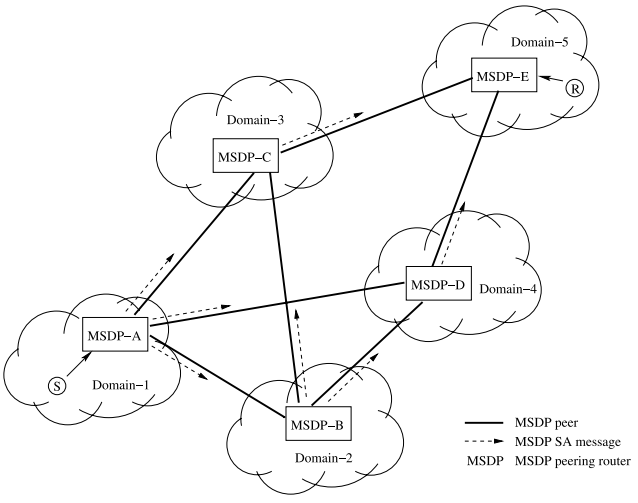

Fig. 2 MSDP peering networks.

dresses in a bootstrap message flooded hop-by-hop throughout the entire network. Exchanging a large number of protocol messages could consume network and router resources or introduce protocol latency.

Based on these observations, PIM-SM does not perfectly fulfill the requirements for a large-scale routing protocol by itself. Multicast Source Discovery Protocol (MSDP) along with another function enables the PIM-SM routing protocol to work as an inter-domain multicast routing protocol.

2.2 Multicast Source Discovery Protocol (MSDP)

All the concerning points thus far are due to the difficulties of RP management in wide-area networks. According to the idea of dividing wide-area networks into several smaller and more manageable-sized networks called PIM domains, independent RP(s) can be located in each PIM domain and data traffic on each RP can be dispersed. Accordingly, third-party dependency is reduced, and bootstrap messages are also easily transmitted within a smaller PIM domain.

In the PIM-SM model, an RP must know all data sender addresses for any particular group prior to RPT construction. In a condition having multiple PIM domains, however, a data sender's first-hop PIM router forwards the data only to its local RP and other RPs cannot find the sender's address. Finally the RPT cannot be created along with multiple PIM domains, and a receiver site Designated Router (DR) located in a different domain cannot join the RPT. In order for an RP to notify information about active sources in a local PIM domain to other domains, Multicast Source Discovery Protocol (MSDP) [11] cooperates with PIM-SM.

MSDP provides a mechanism to connect multiple PIM domains. Each candidate RP in a PIM domain works as an MSDP router and forms an MSDP peering relationship with the candidate RPs in the other domains (Fig. 2). The peering relationship is made up of a TCP connection to exchange information and discover multicast sources in other

FF7 (12)	scope (4)	0YZZ (16)	Network Prefix (64)	Group ID (32)

RPaddress for the group = P::Y, where P = (Network Prefix)::/Z Z

Fig. 3 Embedding RP address in IPv6 multicast address.

domains. When a data sender starts sending data, the RP in the sender's PIM domain forwards Source Active (SA) messages to each MSDP peering router, and the SA messages are forwarded hop-by-hop. Then, if the multicast sources are of interest to a PIM domain that has receivers, an RPT (and later an SPT) is normally established.

While combining PIM-SM with MSDP can provide a functional solution built primarily on existing protocols, the MSDP protocol is more likely to provide a short-term solution. Its biggest weakness is that the time scales for changing the active source indications might be very short; sources can come and go arbitrarily, so the information exchange rate can potentially be quite high. In addition, SA messages are easily flooded throughout the PIM domains. This situation has induced denial-of-service (DoS) attacks, like *Ramen Worm* [12] and *Sapphire* [13]. These DoS attacks presumed on the MSDP architecture and overwhelmed the multicast infrastructure. Actually, this is the reason that MSDP has not been defined for an IPv6 multicast communication environment, and to solve this problem, an alternative embedded-RP mechanism has been proposed [14].

2.3 Embedded-RP for IPv6 Multicast

To get a PIM-SM router to cooperate with multiple RPs, we can adopt the approach given by an embedded-RP [14] mechanism for IPv6 multicast, which is invented by an IPv6 multicast addressing architecture and mitigates the difficulties in managing RP-to-group mapping.

This mechanism assumes that every IPv6 multicast address is in the format defined in Fig. 3. Since the IPv6 multicast address always includes an RP address, all data packets and PIM join or prune messages are transferred to the corresponding RP. For example, if the group address is ff7e:0530:2001:db8:1234:5678::8000, its corresponding RP address is 2001:db8:1234::5. Each PIM router implicitly calculates an RP address when it receives a PIM (*,G) join message and forwards the message toward the embedded RP address.

The embedded-RP mechanism is simple enough, and PIM-SM routers do not need any external mechanisms to synchronize their RP-to-group mapping with other routers. However, the embedded-RP mechanism must be completely deployed in the Internet; all PIM routers must understand the embedded-RP mechanism and forward all multicast data packets and PIM join or prune messages to the appropriate RPs. In other words, if there is a PIM router that does not support the embedded-RP mechanism, it does not extract an expected RP address from a PIM join or prune message and hence cannot properly construct an RPT. This means that we cannot allow step-by-step implementation of this mech-

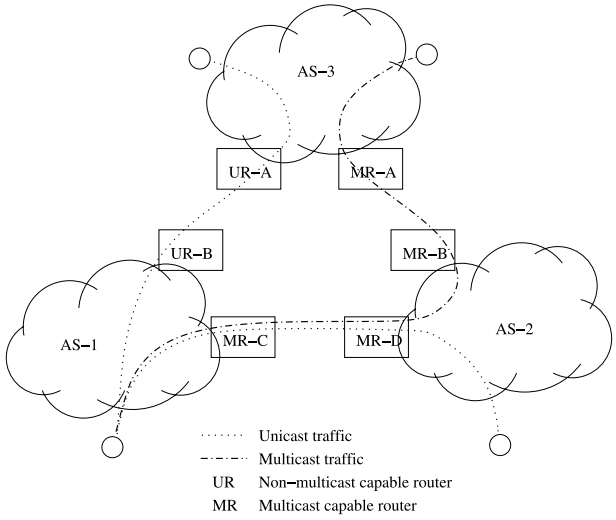

Fig. 4 Policy-based multicast routing path controlled by MBGP.

anism, and such situation might become another deployment barrier.

We also need to be aware that the procedures for maintaining an RPT and switching to an SPT are still necessary, even with an embedded-RP mechanism. This requirement is fundamental for the multicast routing tree construction, while the embedded-RP mechanism can escape from threats seen on the MSDP architecture.

2.4 Multiprotocol Extensions for BGP-4 (MBGP)

The PIM protocol does not exchange routing tables between neighbor PIM routers. It only acts to construct a multicast routing tree with the neighbor routers by sending messages that include a joined or pruned incoming interface address and by receiving messages that include a joined or pruned outgoing interface addresses for the corresponding multicast packets. The PIM protocol uses underlying topology so called Multicast Routing Information Base (MRIB). MRIB is used to determine the next-hop router to which a PIM join/prune message is sent. In other words, MRIB gives reverse path information (see Sect. 1) and indicates the path to which a multicast data packet is forwarded.

Regular unicast routing tables can be used for MRIB. However, network administrators might want to distinguish unicast and multicast routing policies, especially in an inter-domain routing environment. Multiprotocol extensions for BGP-4 (MBGP) [15] adds the capability to enable a multicast routing policy throughout the Internet. It allows the use of a multicast routing topology, which is different from the unicast routing topology, thus giving network administrators control over their networks and resources. MBGP is often combined with PIM-SM to provide the functions needed to cope with an inter-domain multicast.

MBGP defines a network and exchanges the prefix with adjacent MBGP networks. Its network boundaries are generally equivalent to the definition of the Autonomous System (AS) boundaries. Here, to simplify the configuration, the PIM domain defined by MSDP can also correspond to the MBGP network.

In the example shown in Fig. 4, backbone routers connect each of the three ASes. Some of them only support unicast (UR), and others support multicast (MR). Among URs, BGP [16] is used for unicast routing exchange. For MRs, BGP and MBGP can be used for unicast RIB and MRIB constructions. These combinations make it possible to distinguish unicast and multicast data flow as shown in the figure.

3. Source-Specific Multicast (SSM)

3.1 Concept of SSM

Multicast communication has run into significant barriers to its wide-scale deployment. Mainly, these barriers are rooted in the problem of building efficient multicast routing trees for dynamic group memberships. More precisely, the PIM-SM protocol provides many-to-many communication by using a Rendezvous Point router (RP) and maintaining a Rendezvous Point Tree (RPT). Both of constructing the RPT and switching to an optimal source-rooted Shortest-Path Tree require complex routing algorithms. Managing multiple RPs in the Internet further impedes deployment because the additional routing functions introduce extra complexity.

Such complexity of multicast routing tree coordination has caused attention to be focused on the traditional many-to-many multicast communication called Any-Source Multicast (ASM). ASM was designed so that *any* kind of multicast application can work well over it. However, supporting *any* kind of application may be too ambitious in our sense.

With regard to widely used multicast applications like live streaming or the contents distribution style applications used in the Internet, the one-to-many or few-to-many communication model, in which the data sender is only one node or a few nodes in a multicast session and the number of the data receivers is many, is usually sufficient. When we consider one-to-many or few-to-many communication, we can assume that multicast data receivers know the address of each data sender, as well as the multicast address, prior to sending the join requests. In this case, 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. This collaborative effort eliminates the source address discovery procedure from multicast routing protocols, which is the key reason of problems caused by MSDP, as described in the previous section. Furthermore, in this communication, a multicast router can eliminate the process of coordinating and maintaining a shared tree because it can directly construct an SPT from its initial protocol phase. In other words, 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. As can be seen in the example shown in Fig. 1, in this commu-

nication, there is no [A] or [B] state, and only an SPT in the [C] state exists.

This one-to-many or few-to-many multicast communication model is called Source-Specific Multicast (SSM) [2], because the data receivers specify source and group addresses for their join or leave requests. SSM solely maintains an explicit source-based routing tree; in an SSM communication environment, each receiver site DR only coordinates the appropriate SPTs toward each data sender. An SSM communication model would better facilitate multicast service deployment in the Internet.

3.2 SSM Adaptation to Current Environment

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 ASM environment, a data receiver sends an IGMP/MLD join or leave message that only indicates the multicast address referred to as a (*,G) join/leave message. On the other hand, 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 an (S,G) join/leave message to its DR.

To realize SSM communication, host-side extension is required to send a join or leave message including the pair of interesting source and group addresses. At the protocol level, this extension is done using IGMP version 3 (IGMPv3) [7] for IPv4 and MLD version 2 (MLDv2) [9] for IPv6. As well, it is indispensable that every receiver site DR must support these protocols in order to translate the (S,G) join/leave messages sent from the data receivers. Either or both of the IGMPv3 and MLDv2 protocol implementations are provided in the major OSes and applications [17], and most router vendors support them as well. We therefore hope that many Internet users will be eager to start or move forward to the SSM communication model in the near future.

3.3 Consideration of Security Threats

We know that security threats against IP multicast would have a catastrophic effect on IP multicast deployment in the Internet, as described by Savola et al. of the IETF MBONED working group document [18]. They categorized the security threats into receiver-based and source-based attacks. In short, the former is a DoS attack against multicast routers, in which innumerable IGMP/MLD joins are sent from a client, and the latter is a DoS attack against the entire multicast network, in which data is sent to numerous and random group addresses.

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, because the sender does not (or cannot) trace the active data receivers. To make things worse, multicast routers, including first-hop routers, do not recognize or reject bogus packets, and this is the main reason for the problems mentioned in Sect. 2.2.

However, these kinds of attacks are specific to ASM and do not affect SSM, in which the first-hop router can discard multicast data packets that do not have a corresponding routing entry. While more discussions about security considerations regarding SSM are needed, we expect there will be fewer source-based attacks in SSM communication.

4. Case Study and New Project

4.1 Analysis of Statistical Trend

We analyzed the statistical trends in the international multicast backbone using the following measurements to understand the current situation and future needs of IP multicast services.

Figure 5 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 [4] and other Japanese research communities are connecting. The “International Backbone” is the connection to Abilene [19] via TransPAC [20]. 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 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

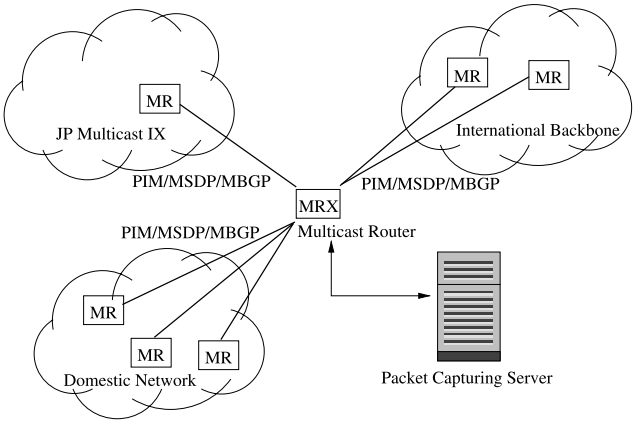

Fig. 5 Network and server configuration.

†Note that IGMP/MLD join and leave are with different protocol messages from PIM join and prune.

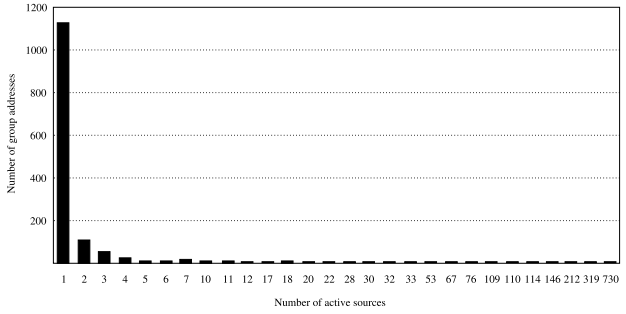

Fig. 6 Number of active data sources per multicast session.

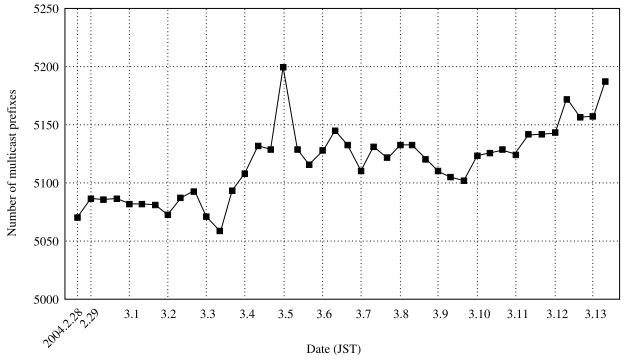

Fig. 7 Number of advertised multicast address prefixes (i.e. MRIB).

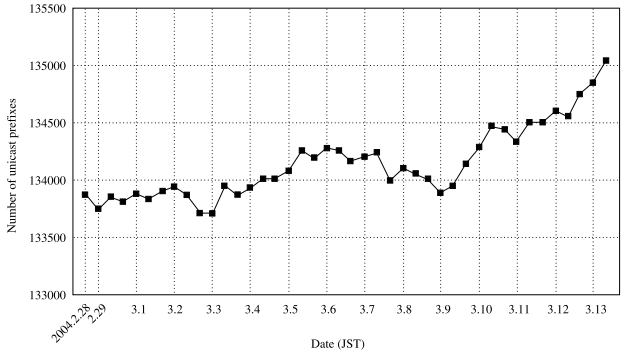

Fig. 8 Number of advertised unicast address prefixes (i.e. unicast RIB).

MSDP, MBGP and BGP routing information at eight-hour intervals from Feb. 28 to March 13, 2004.

From the extracted data, the following information was obtained: (1) distribution of the number of senders per group (Fig. 6), (2) chronological trends of IPv4 multicast RIB entries (Fig. 7), and (3) chronological trends of IPv4 unicast RIB entries (Fig. 8).

Figure 6 shows that more than 90% of the multicast sessions were categorized as one-to-many communication, although the network infrastructure supported many-to-many communication. This fact indicates that ASM is not mandatory from the viewpoint of multicast service providers. In other words, SSM does not interfere with the steady deployment of IP multicast, and there should be no problem in replacing ASM with SSM. Although a few multicast sessions were advertised from a large number of senders (e.g. 212, 319, and 730), we believe that they were used for the multicast session announcement by the SAP [21] protocol, which requires multicast data senders send announcement messages to the corresponding multicast addresses.

Figure 7 and Fig. 8 show the number of MRIB entries and unicast RIB entries measured on our multicast router[†]. From these figures, we can predict the current status and future possibilities of IP multicast deployment, because the number of MRIB entries could become one of the fundamental indicators. Actually, the rate of increase in multicast RIB entries was about 2.0%, whereas that of unicast RIB entries was about 1.4% during our measurement period. From these observations, it is clear that the popularity of MRIB has been increasing for a long time, as well as unicast RIB. Note that a network would be unstable, even though routes appear to be advertised stably, because a small fluctuation of routes might cause significant network instability [22]. We would therefore need distributed measurements and micro observations to accurately determine the stability of end-to-end reachability, instead of only retrieving the MRIB or RIB trends from a single router.

As an additional consideration, we also analyzed the traffic and the number of advertised routing entries on the multicast network. In fact, only about 0.5% of the total MRIB entries were advertised and only about 0.1% of the multicast data were sent from JP Multicast IX and Domestic Network (graphs omitted). These results are not cause for optimism for IP multicast deployment in Japan. Consequently, we are openly encouraging some form of action to resolve these difficulties, and we hope the collaboration described in the next section will contribute to it.

4.2 MONACO Project

In an effort to promote IP multicast deployment and update researchers on multicast technologies, it would be highly advantageous to publicize attractive multicast services to the various Internet communities through demonstrations. The WIDE project and the French M6Bone [5] coordinators have initiated a project called "IP multicast deployment and international collaboration (MONACO)" [3] to encourage IP (especially IPv6) multicast deployment in the Internet. As part of this collaboration, we have initially established IPv6 multicast connections between France and Japan, in addition to the worldwide M6Bone.

This effort has increased our operational experiences and improved protocol analysis and traffic and performance measurements. In the next step, various aspects would be given by monitoring multicast routing exchange on these global site routers. We are also planning to test various IP multicast services over the networks to identify any missing components so that we can expand its usage.

[†]Each advertised routing entry had a different prefix length. Therefore we only compared the trends from these figures.

We found that sharing technical information among the collaborating members to be highly beneficial – it has improved our technical backgrounds and created a greater impact. The MONACO members exchange information on various topics and work towards a multilateral solution using the unique approaches and insights of each member. Therefore open discussions on potential research topics and problems and encouraging idea exchange or brainstorming sessions are absolutely essential to ensure the success of this collaboration. Furthermore, developing and evaluating protocols or applications contributes to IP multicast deployment. Promoting our deliverables – research reports, softwares, and services – to the Internet communities is vital. We hope this collaboration will trigger the actual use of IP multicast in the Internet accordingly.

5. Conclusion

IP multicast provides various advantages for meeting current and future Internet needs. This encouraged us to investigate the problems with existing multicast architecture and propose possible and feasible solutions that will help promote its deployment. In this document, we summarized the difficulties of traditional ASM multicast communication and the benefits of SSM communication.

We discussed the characteristics of multicast routing protocols and an SSM communication model with use of IGMPv3 and MLDv2. To investigate and clarify the current situation in IP multicast deployment, we also measured the number of available sessions and multicast routing entries in our backbone router.

To further contribute to IP multicast deployment, we introduced our international collaboration called MONACO. A future report will describe the activities and experiences we obtain from this collaboration and our efforts to promote feasible applications and services for use in the Internet.

Acknowledgements

This paper describes research supported by the Asia Grid Initiative project funded by MEXT, Japan. We are sincerely grateful to the WIDE project members and the MONACO members for their comments that helped us improve the presentation of our ideas.

References

[1] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol independent multicast – Sparse mode (PIM-SM): Protocol specification (revised)," Internet Draft - work in progress, draft-ietf-pim-sm-v2-new-11.txt, Oct. 2004.
[2] S. Bhattacharyya, "An overview of source-specific multicast (SSM)," RFC3569, July 2003.
[3] "MONACO: IP multicast deployment and international collaboration," http://www.sfc.wide.ad.jp/monaco/
[4] "WIDE project," http://www.wide.ad.jp/
[5] "M6Bone—IPv6 multicast network," http://www.m6bone.net/
[6] W. Fenner, "Internet group management protocol, version 2," RFC2236, Nov. 1997.
[7] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajan, "Internet group management protocol, version 3," RFC3376, May 2002.
[8] S. Deering, W. Fenner, and B. Haberman, "Multicast listener discovery (MLD) for IPv6," RFC2710, Oct. 1999.
[9] R. Vida and L. Costa, "Multicast listener discovery version 2 (MLDv2) for IPv6," RFC3810, June 2004.
[10] L. Wei and D. Estrin, "A comparison of multicast trees and algorithms," Technical Report USC-CS-93-560, University of Southern California, Sept. 1993.
[11] B. Fenner and D. Meyer, "Multicast source discovery protocol (MSDP)," RFC3618, Oct. 2003.
[12] P. Rajvaidya, K. Ramachandran, and K. Almeroth, "Detection and deflection of DoS attacks against the multicast source discovery protocol," UCSB Technical Report, July 2002.
[13] P. Rajvaidya, K. Ramachandran, and K. Almeroth, "Managing and securing the global multicast infrastructure," J. Network and Systems Management (JNSM), vol.12, no.3, pp.297–326, Sept. 2004.
[14] P. Savola and B. Haberman, "Embedding the rendezvous point (RP) address in an IPv6 multicast address," RFC3956, Nov. 2004.
[15] T. Bates, R. Chandra, D. Katz, and Y. Rekhter, "Multiprotocol extensions for BGP-4," RFC2283, Feb. 1998.
[16] Y. Rekhter and T. Li, "A border gateway protocol 4 (BGP-4)," RFC1771, March 1995.
[17] H. Asaeda, "Design and analysis of IGMPv3 and MLDv2 host-side protocol implementations," IEICE Trans. Inf. & Syst., vol.E87-D, no.12, pp.2602–2609, Dec. 2004.
[18] P. Savola, R. Lehtonen, and D. Meyer, "PIM-SM multicast routing security issues and enhancements," Internet Draft - work in progress, draft-ietf-mboned-mroutesec-04.txt, Oct. 2004.
[19] "Abilene backbone network," http://abilene.internet2.edu/
[20] "The transPAC2 project," http://www.transpac.org/
[21] M. Handley, C. Perkins, and E. Whelan, "Session announcement protocol," RFC2974, Oct. 2000.
[22] C. Labovitz, A. Ahuja, and F. Jahanian, "Experimental study of internet stability and backbone failures," Proc. FTCS-29, p.278, June 1999.

Hitoshi Asaeda received B.E. in Science and Technology from Keio Univ. in 1991. From 1991 to 2001, he was with IBM Japan, Ltd. From 2001, he was a research engineer specialist in the INRIA Sophia Antipolis research unit, France. Since 2005, he is an assistant professor of Graduate School of Media and Governance, Keio Univ. His research interests are IP multicast routing architecture and its deployment including implementations of the corresponding kernel and user code. He is a member of IEEE, IPSJ and WIDE project.

Shinsuke Suzuki joined Hitachi, Ltd. in 1997 and has working in ALAXALA Networks Corporation since May 2005. He has been working on the development of IPv6 routing protocols (especially multicast-related protocols) and the deployment of IPv6. He is also a core member of KAME Project since 2000, and a network operator in various IPv6 and multicast networks (WIDE Project, Interop2005 Tokyo, etc).

Katsushi Kobayashi received his B.E., M.E., and Ph.D. degrees in Electro-Communications Engineering, The University of Electro-Communications, Japan in 1987, 1989, and 1994 respectively. During 1994–1998, he was the research associate of Information Processing Center, The University of Electro-Communications. He joined the Communications Research Laboratory (CRL), Japan in 1998. He is currently the leader of Internet Architecture Group at The National Institute of Information and Communications Technology (NICT), Japan.

Jun Murai received M.E. and Ph.D. in Computer Science from Keio Univ. in 1981 and 1987 respectively. He is currently Vice-President, Keio Univ., where he is a professor in the faculty of Environmental Information. In 1984, he developed the Japan University UNIX Network (JUNET), and in 1988 established the WIDE project of which he continues to serve as the General Chairperson. He is President of the Japan Network Information Center (JPNIC), a former member of the Board of Trustees of the Internet Society and a former board director of the Internet Corporation for Assigned Names and Numbers (ICANN).