第 XIV 部

IP マルチキャストに関する
運用・応用アプリケーション開発

第 14 部
IP マルチキャストに関する運用・応用アプリケーション開発

第 1 章 Introduction

Multimedia streaming has been one of the most popular applications in the Internet. To provide high quality multimedia streaming content to a large number of Internet users, a quality adaptation mechanism for streaming applications and defining operational conditions to deploy IPv4/v6 multicast in the Internet are necessary for distributing the future media in the Internet. M6bone Working Group in the WIDE Project has been focusing on multimedia streaming applications and IPv4/IPv6 multicast deployment in the Internet.

We have been maintaining and promoting IP multicast capable networks in the global Internet. We also submitted Internet-Drafts to the IETF. The following sections introduce the contributions and the primary outputs.

第 2 章 Inter-AS IPv6 Multicast Streaming in CanalAVIST ICT Forum

CanalAVIST is a part of the ASEAN Virtual Institute of Science and Technology (AVIST) and the ASEAN Science and Technology Research and Education Network Alliance (ASTRENA) under ASEAN Committee for Science and Technology to provide channels for seamless education, teaching, training, conferencing, lectures, talks through ASEAN countries for ASEAN researchers and students.

2.1 Network Topology

CanalAVIST ICT Forum was streaming talks from various sites. This forum was designed as multiple venues, and we used IPv6 Multicast to provide many to many communication.

The following are the designated venues for CanalAVIST ICT Forum. The network topology was star topology centering on TEIN2-SG (AS24490), and individual venues were on TEIN2, APAN, AARNET, CERNET2, KOREN, UniNET, ThaiREN, SingaREN and WIDE.

- Australia: NICTA Seminar Room, Bay 15 Ground Floor, Australian Technology Park
- China: Lecture Hall, Main Building, Tsinghua University, Beijing
- Indonesia: LPM Studio, Gedung TVST 2nd floor, Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
- Japan: Shochoshitsu, Delta Building, Keio University/SFC, Fujisawa, Japan
- Korea: 1102 New Millennium Hall, Konkuk University, 1 Hwayang-dong, Gwangjin-Gu, Seoul Korea
- Malaysia: MYREN Network Operation Center, MSC Innovation Centre, 1st Floor East Wing, Enterprise 1, Jalan Teknorat 3 63000 Cyberjaya
- Singapore: School of Computing, COM1 Building, Video Conference Room #02-13
- Thailand: UniNet Auditorium, 3rd Floor Meeting Room, Commission on Higher Education Building
- Vietnam: NACESTI, Hanoi, Vietnam

2.2 Operational Problems

Although multicast operators want to recognize the delivering path and topology. Basically, Inter-AS IPv6 Multicast is operated by MBGP to control the MRIB route. MBGP also provides

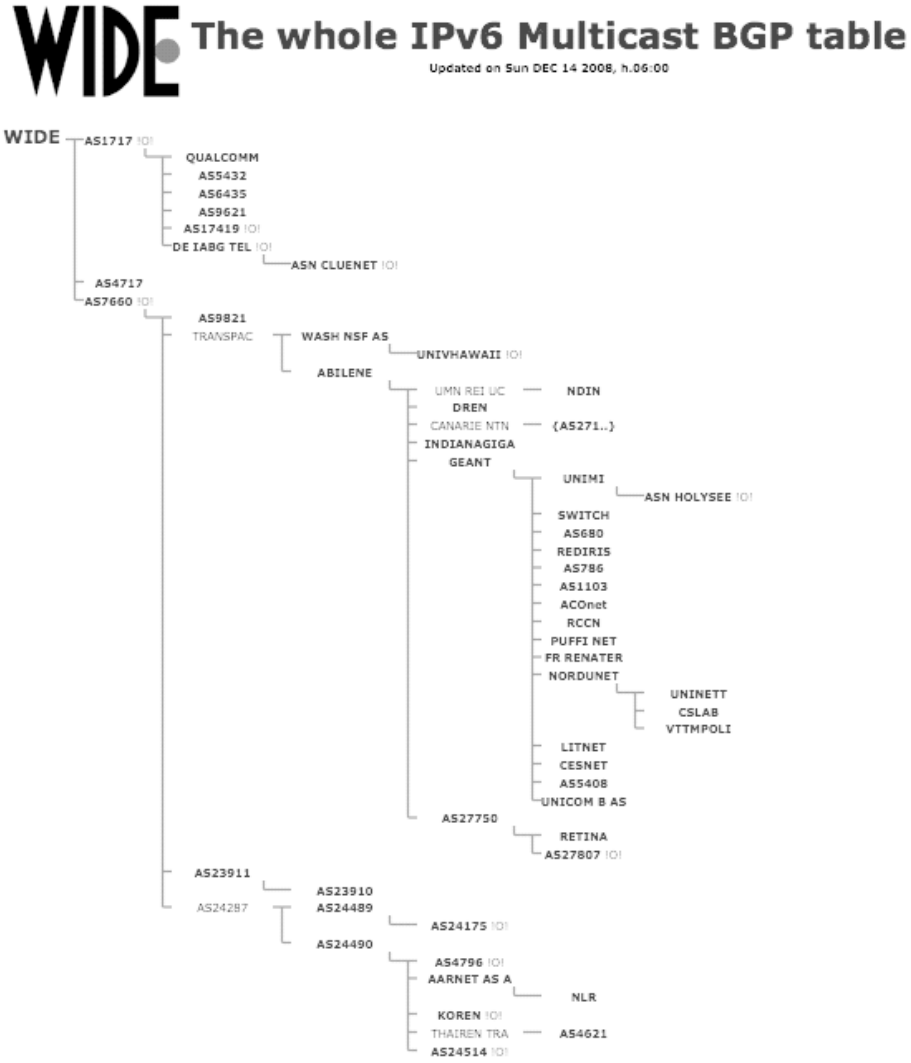

Fig. 2.1. Inter-AS Topology using MBGP table

AS-Path information to the operators, Inter-AS topology is shown in the MBGP table. Figure 2.1 shows inter-AS MRIB routes on WIDE which was generated by MBGP table.

However, there are few routers which don't support MBGP in this forum's network. Therefore we have to configure the static MRIB routes, and it made us to monitor the Inter-AS topology.

In our experience, tools for monitoring IPv6 Multicast paths is highly required to make the IPv6 Multicast deployment. We will study and develop a mechanism to check the inter-AS topology and connectivity in Multicast.

第 3 章　Contributions for the IETF

3.1 Lightweight IGMPv3 and MLDv2 Protocols

An IP multicast protocol architecture requires host-and-router communication, in order for multicast router to maintain active multicast routing tree. The Internet Group Management Protocol (IGMP) for IPv4 and the Multicast Listener Discovery (MLD) for IPv6 are the standard protocols for the host-and-router communication. 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.

IGMP version 3 (IGMPv3) and MLD version 2 (MLDv2) implement source filtering capabilities. An IGMPv3 or MLDv2 capable host can send IGMPv3/MLDv2 messages to its upstream router to notify which multicast channels the host wants to subscribe and unsubscribe. An IGMPv3 or MLDv2 capable router then can learn sources which are of interest or which are of not interested for a particular multicast address.

The multicast filter-mode improves the ability of the multicast receiver to express its desires. It is useful to support one-to-many multicast communications known as SSM[67] by specifying interesting source addresses with INCLUDE mode. 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. It is generally unnecessary to support the filtering function that blocks sources.

We proposed simplified versions of IGMPv3 and MLDv2, named Lightweight IGMPv3 and Lightweight MLDv2 (or LW-IGMPv3 and LW-MLDv2)[105]. LW-IGMPv3 and LW-MLDv2 support both traditional many-to-many communications and SSM communications without a filtering function that blocks sources. Not only are they compatible with the standard IGMPv3 and MLDv2, but also the protocol operations made by hosts and routers or switches (performing IGMPv3/MLDv2 snooping) are simplified to reduce the complicated operations. LW-IGMPv3 and LW-MLDv2 are fully compatible with the full version of these protocols (i.e., the standard IGMPv3 and MLDv2).

LW-IGMPv3 and LW-MLDv2 protocol specification has been accepted as the IETF MBONED working group draft, and at the end of this year, Working Group Last Call was invoked. Hopefully, this protocol specification will become an RFC with Best Current Practice (BCP) status in 2009.

3.2 Mtrace Version 2

From operator's perspective, lack of effective monitoring tools limits the IP multicast deployment activities. To monitor unicast routing path, the unicast traceroute program has been used to trace a path from one machine to another. The key mechanism for unicast traceroute is the ICMP TTL exceeded message, which is specifically precluded as a response to multicast packets. On the other hand, the multicast traceroute facility that allows the tracing of an IP multicast routing paths is not standardized but needed. We specified the new multicast traceroute facility to be implemented in multicast routers and accessed by diagnostic programs. The new multicast traceroute, mtrace version 2 or mtrace2[11], can provide additional information about packet rates and losses that the unicast traceroute cannot, and generally requires fewer packets to be sent.

The proposed draft supports both IPv4 and IPv6 multicast traceroute facility. The protocol design, concept, and program behavior are same between IPv4 and IPv6 mtrace2. Mtrace2 messages are carried on UDP, whereas the packet formats of IPv4 and IPv6 mtrace2 are different (but similar) because of the different address family.

We have been enhancing the mtrace2 functions to make it fully worthful. One of the major changes of the latest version is that the current mtrace2 encodes TLV fields in mtrace2 messages. For instance, mtrace2 response can encode not only Mtrace2 Standard Response Block, which includes common router's information, but also Mtrace2 Augmented Response Block, which includes extended vendor or protocol specific information. This is useful for future's extension.

Mtrace2 specification has been accepted as the IETF MBONED working group draft. Its intended status is Proposed Standard RFC.

3.3 Security and Reliable Multicast Transport Protocols

Since IP multicast usually works with non-reliable UDP, creating reliability with multicast data transmission is the requirement for current and future needs. One of the simplest method to recover packet loss is Ack-based (Acknowledgement-based) or NAck-based (Negative Acknowledgement-based) data retransmission. However, to give robustness from loss of transmitted multicast data, a large number of data retransmission will not only waste network resources but also lead additional security concerns.

We clarify the issues how multicast security should be considered to deploy IP multicast services in the global Internet and enable realiable multicast transmission in [3]. This document describes general security considerations for the IETF Reliable Multicast Transport (RMT) working group set of building blocks and protocols. The purpose of this document is to provide a consolidated security discussion and provide a basis for further discussions and potential resolution of any significant security issues that may exist in the current set of RMT standards.

This draft has been accepted as the IETF RMT working group draft. Its intended status is Informational RFC.

第 4 章　Conclusion

M6bone WG has been working for IP multicast deployment and conducted various research towards its further use. In this year, we studied advanced research topics and had operational experience in the global native multicast networks. Protocol standardization is also our important task for fulfilling the future demand. Our future work would improve current research solutions and much relate to the fundamental issues being required in various multimedia streaming services including future Internet TV. Since multicast security is also an important topic in order to provide the concrete applications and services in the Internet, we will investigate the related issues and give the feasible solutions. Providing IP multicast stability and robustness should be also convinced in our future work.