第 XII 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 12 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 published academic papers and submitted Internet-Drafts to the IETF. We also have been maintaining and promoting IP multicast capable networks in the global Internet. The following chapters introduce the contributions and the primary outputs.

第 2 章 Gap Analysis in IP Multicast Dissemination

IP multicast 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.

Recently, Source-Specific Multicast (SSM)[61] 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 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 [12], we therefore analyzed 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.

第 3 章　Analysis of FEC Function for Real-Time DV Streaming

Due to the widespread dissemination of high speed DSL and FTTH, real-time streaming applications have been commonly used in the Internet. However, it is impossible to preclude the possibility of data transmission delay and packet loss for the real-time applications on the best-effort Internet.

As a high quality real-time streaming applications, Digital Video Transport System (DVTS)[86, 126] contributes to end users to play with the DV transmission over IP, because it simply uses general consumer products which support a DV format, and does not require any professional equipment. However, DVTS consumes 30 Mbps for its transmission and requires high speed networks for the DV transmission. Since the current Internet is heterogeneous and does not guarantee the Quality of Service (QoS), end users must take into account network congestion that causes the disruption of video and audio upon its use.

For keeping a stable streaming quality, we proposed a mechanism that a sender adds redundant data to its steam, and a receiver detects and corrects errors being happened during transmission without the need to ask the sender for additional data. As its typical component, we investigated a “Forward Error Correction (FEC)” mechanism[19, 129] on DV streaming that keeps a stable quality. We then study the relation between the network bandwidth and FEC recovery rate upon data transmission in a congested network, and the relation between the receiver’s play quality and FEC calculation cost. Our experimental results[104] show that the FEC function can provide the best possible streaming quality, without leading the further disruption of video and audio irrespective of the available network bandwidth.

To investigate FEC effectiveness for making an adaptive system using frame rate control and FEC rate control, we implemented static FEC using Reed-Solomon Code with DVTS. The characteristic of Reed-Solomon Code is that processing speed is fast, and consumed bandwidth is large. To utilize FEC function, a sender adds redundant packets with FEC encode module, while a receiver recovers loss packets with FEC decode module by using redundant packets according to need.

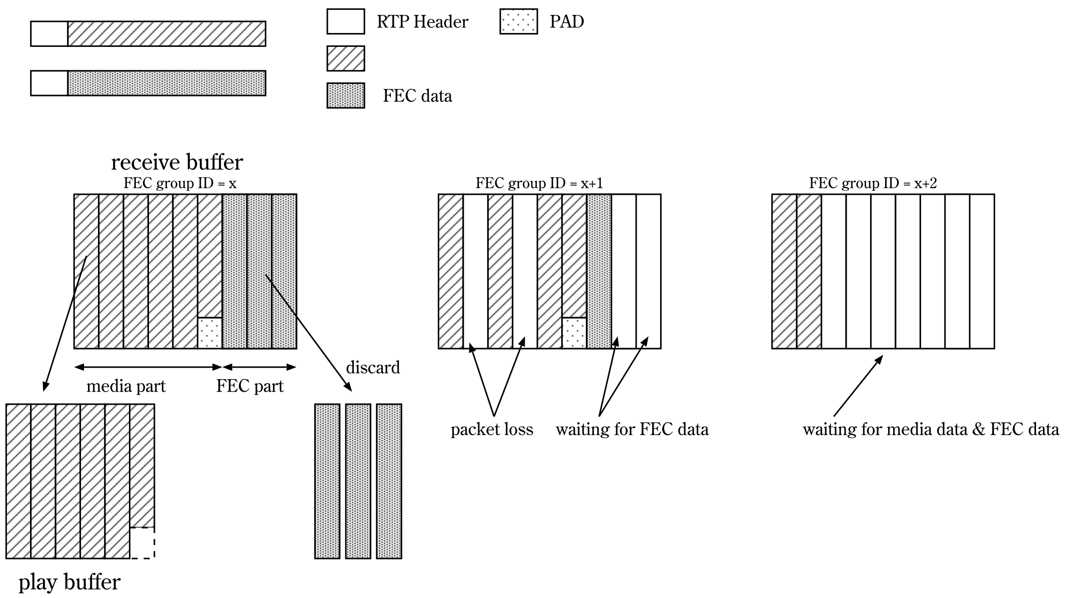

Fig. 3.1. FEC decode management

Figure 3.1 shows how a receiver decodes FEC. When a receiver gets the all DV/RTP packets which belong to the same group, redundant packets are thrown and DV/RTP packets are stocked with the play buffer. A receiver recovers the packet if packet loss is observed and redundant packet is encoded. If it is impossible to recover lost packets due to exceeding packet loss limit, a receiver throws redundant packets and stocks DV/RTP packets with the play buffer.

第 4 章 IPv4/v6 Dual Stack HD Live Streaming in SIGCOMM 2007

ACM SIGCOMM is the primary conference in the communication and computer networking. It was held at Kyoto in August, 2007. The WIDE Project hosted this conference, and we provided the Internet connectivity for participants and live streaming for the online participants.

In this chapter, we introduce the experience of the world wide IP multicast live streaming in SIGCOMM 2007 at Kyoto. This activity was presented at the Fall Internet2 member meeting[63]. At first, we present the world wide academic network topology that enables Inter-domain IP multicast, and show the actual listeners map and AS path tree. We then explain the operational problems we encountered and the solutions we provided.

4.1 Network Topology

Primarily, the WIDE Project connected to IPv6 multicast network via M6bone which is an experimental IPv6 multicast backbone using IP over IPv6 tunnel. After this experiment, WIDE has (AS2500) provided both IPv4 and IPv6 world wide native multicast connectivities via APAN-JP (AS7660).

Figure 4.1 shows the world wide inter-domain multicast topology map. Most of the transit backbone ASes have multiple AS-Paths, and hence the world wide multicast network is redundant.

4.2 Operational Problems

Although multicast source operators want to recognize how many nodes and which ASes have been listening, it is generally difficult to make a real-time monitoring or gathering the information of the active IP multicast listeners. We hence tried to use the other way to gather the listeners' information.

Figure 4.2 shows address family IPv6 multicast BGP table in UNINETT (AS224) AS border router connected to NORDNET (AS8362). WIDE (AS2500) was appeared in this table.

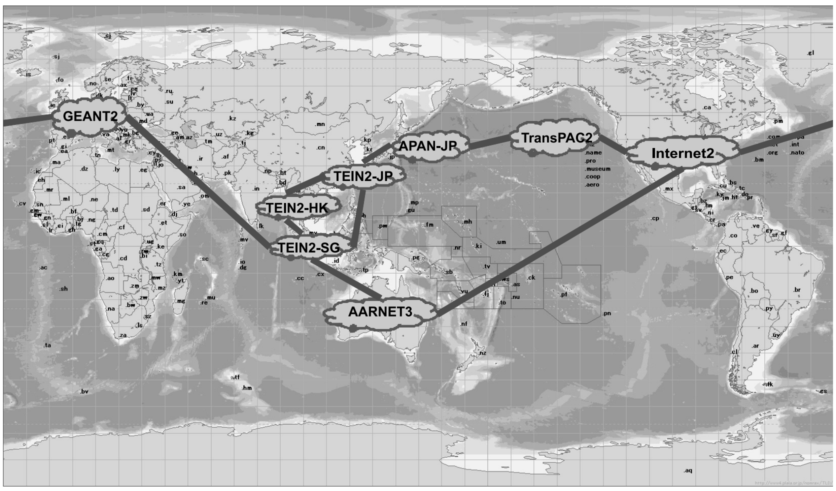

Fig. 4.1. World Wide IDMR Topology MAP

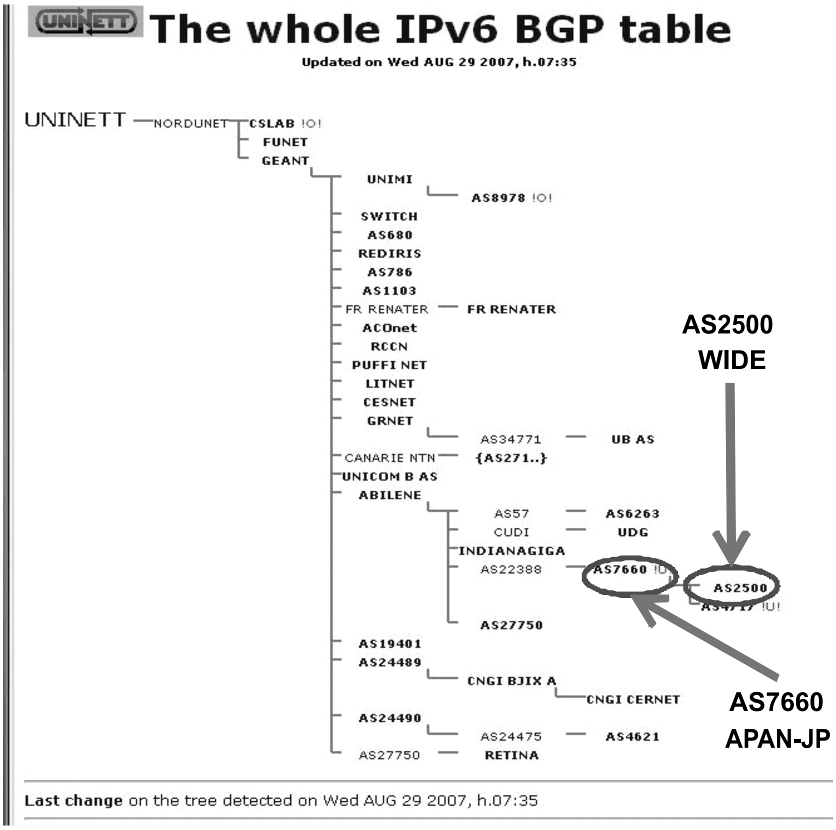

Fig. 4.2. IPv6 Multicast BGP Table

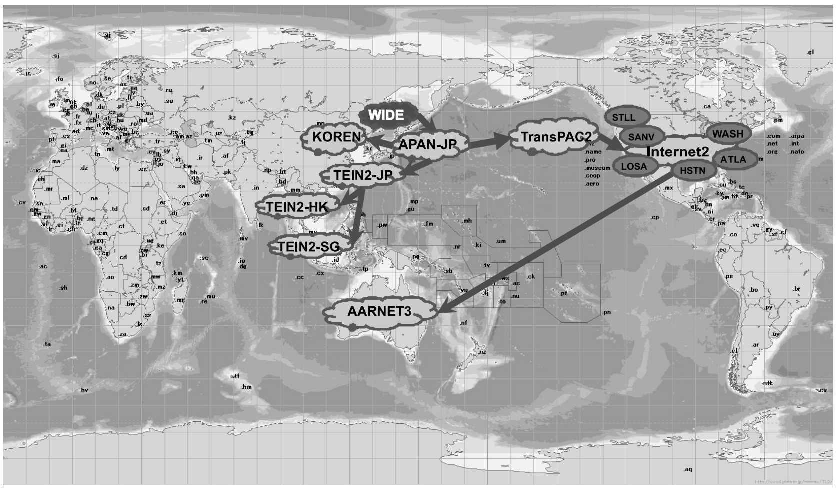

Fig. 4.3. Confirmed Listener AS in IPv4

We also used “Router Looking Grass” in APAN-JP, Geant2, and Abilene to clarify articulate the listening leaf AS. Router Looking Grass is a router command proxy that provides executing authority via Web interface. Figure 4.3 and 4.4 show the listener ASes for IPv4 and IPv6 respectively. These figures were created based on the information of multicast routing tables provided by Router Looking Grasses.

In our experiences, tools for monitoring IP multicast routing paths and listeners are highly required to make the IP multicast deployment, in order that multicast source operators check the traffic conditions. We as well as setting up

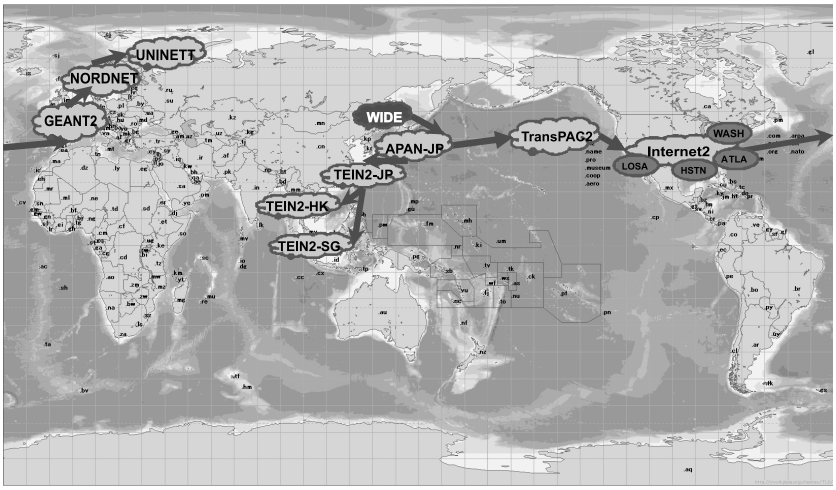

Fig. 4.4. Confirmed Listener AS in IPv6

ssmping and web proxy to check network connectivity, we will study and develop a mechanism to check IP multicast listeners in the next step.

第 5 章　Contributions for the IETF

5.1 Lightweight IGMPv3 and MLDv2 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.

IGMP version 3 (IGMPv3) and MLD version 2 (MLDv2) implement source filtering capabilities that are not supported by their earlier versions, IGMPv1, IGMPv2 and MLDv1. An IGMPv3 or MLDv2 capable host can tell its upstream router which group it would like to join by specifying which sources it does or does not intend to receive multicast traffic from. IGMPv3 and MLDv2 add the capability for a multicast router to 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 SSM[61] 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)[96]. LW-IGMPv3 and LW-MLDv2 support both ASM 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).

5.2 Mtrace Version 2

Lack of effective monitoring tools limits the IP multicast deployment activities on an operator side. 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.

第 6 章　Conclusion

M6bone Working Group 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.