IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA ITB7319
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

Chapter XVIII

IP Multicast: Inter Domain, Routing, Security and Address Allocation

Antonio F. Gómez-Skarmeta, University of Murcia, Spain
Pedro M. Ruiz, University Carlos III of Madrid, Spain
Angel L. Mateo-Martínez, University of Murcia, Spain

INTRODUCTION

Without doubt, multicast communication as a means for one-to-many or many-to-many delivery of data has become a hot topic in multimedia environments. A lot of people are interested in multicast: the research community, standards groups and Internet Service Providers (ISP) among them.

Although IP multicast is a very good solution for Internetworking multimedia in many-to-many communications, there are still issues that have not been completely solved. Protocols are still evolving and new protocols are constantly coming up to solve these issues because that is the only way for making multicast become a true Internet service.

The main goal of this chapter is to describe the evolution of IP multicast from the obsolete MBone (Multicast Backbone) and intra-domain multicast routing to the actual inter-domain multicast routing scheme. We will pay special attention to the challenges and problems that need to be solved, the problems that have been solved and the way they were solved. We will make a complete picture of the state of the art explaining the idea behind each protocol and how all those protocols work together.

Some of the topics that we will discuss broadly are related to address allocation, security and authentication, scope control and so on. We will explain our view of the problems, the work that has been made worldwide on these issues and also the developments that we have made in order to solve some of these problems. We will give some results and recommendations.

This chapter appears in the book, Multimedia Networking: Technology, Management and Applications by Syed Mahbubur Rahman.

Authentication

With the current IP multicast model, there is no way to control who can join to a certain multicast group or even who can send datagrams addressed to a certain multicast group. Nowadays there is only one proposal in the draft "IGMP Extensions for IP Multicast Sender and Receiver Authentication," written by N. Ishikawa from the NTT Information Centre. We have developed a system for controlling accesses to IP multicast networks based on this work. We are planning to integrate our system with the current ideas expressed in the IGMPv3 protocol that is being defined these days.

Scope Control

Another drawback that the current IP multicast model shows is related to the scope control. In the same way that you cannot control who accesses to IP multicast networks, is not possible to limit the scope of the sent datagrams. The system we have developed also covers this issue by adding some ideas to Ishikawa's proposal.

Without solving these problems, it is not possible to become IP multicast in a true Internet service because malicious users could conspire to clog your network and you cannot do anything. This makes ISPs think twice before offering this service to their customers.

Address Allocation

Another problem that arises when deploying IP multicast to the whole Internet is related to address allocation. The current model is based on sdr and the fact that if there is not an announced session using a certain multicast group, then there is nobody using that group.

Nevertheless, IP multicast evolution based on inter-domain routing protocols makes this solution obsolete, and a more dynamic and robust solution is needed, which should be integrated with this new multicast routing models; so MASC, GLOP and AAP are been proposed to solve this problem.

Then we will present some conclusions, future work and future research opportunities for people working in the deployment of IP multicast.

BACKGROUND

There are various ways to provide interactive multimedia services with real-time requirements. The first solution we can use is ISDN, as the great variety of H.320 videoconference systems over this kind of switched network shows. H.320 is not just a unique standard, but a set of standards covering topics such as audio and video formats, data transmission or control signalling.

Although H.320 is a good solution to remote videoconferencing, it has some drawbacks. The first one is the fact that it does not use the Internet "standard" for communicating remote sites, so you need an extra and independent tool to access the service. Nowadays the Web browser is thought to be the killer application for accessing Internet services, so this is not a friendly solution.

H.323 is very close to H.320. Actually, protocols and formats defined and used in H.323 are very similar (if not the same) to that ones used with H.320. The main difference between these two protocols is their objective. While H.320 was designed for digital switched network based on 64 kpbs channels, H.323 was designed to be used over datagram networks with unguaranteed bandwidth. So H.323 can be used in low bandwidth environments.