Thesis Title	Filtering Multicast Packet through NAT
Author	Sarathoon Khammakasikit
Faculty	Computer Science, Thammasat University
Thesis Advisor	Thanakorn Sakchaichroenkul Ph.d.
Year Submitted	2007

Abstract

Video conferencing is one of multimedia applications widely seen in today's Internet. In the video conferencing application, a participant initiates a conference session. Then, many other participants located in different networks distributed across the Internet can join the session. During the conference session, each participant can play both sender and receiver roles resulting in many-to-many transmission paradigm. Henceforth, multicast service from either the network layer (IP multicast) or the application layer itself (application-layer multicast) is a great support for the video conferencing application.

This thesis focuses on the problem of video conferencing application with IP multicast service not being able to accompany participants located in some networks. These networks are those placed behind Network Address Translation (NAT) servers to fully utilize blocks of IP addresses assigned to them. This problem is caused by NAT servers dropping any packet with class D IP address, i.e. multicast packet.

To address the problem, we developed a novel module that operates on NAT servers. The new module enhances the capability of NAT servers regarding multicast packets as follows. For an arriving multicast packet originating from a network behind the NAT server (an outgoing multicast packet), our new module causes the NAT server to join the multicast group specified in the packet header. Consequently, the NAT server becomes a part of a multicast distribution tree of the group. The multicast packet can then be forwarded along the distribution tree to other members of the group. For a multicast packet originating from a remote network outside (an incoming multicast

packet), our module verifies whether the NAT server has joined the multicast group specified in the packet's header. If the NAT server is currently a member of the multicast group, our module delivers the multicast packet to the network behind the server. Otherwise, our module drops the multicast packet.

Our experimental results show that the proposed method allows participants located in networks placed behind NAT servers to initiate or join conference sessions. This can be done without requiring any alteration to the existing IP multicast protocol. In addition, NAT servers still provide the same degree of security to the networks behind them. This is achieved by dropping multicast packets originating from remote networks outside if NAT servers are not current members of multicast groups specified in the headers of incoming multicast packets.