Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Implementing key Technologies in Multicast Environment through IP Multicast

Mayank Sharma
Associate Professor (IT)
Aurora's Engineering College
Bhongir, Andhra Pradesh, India
Mayank_sharma04@yahoo.com

S.Santhi Priya
Assistant Professor (CSE),
Sagar Institute of Technology
Andhra Pradesh, India
santhipriya.sunkara@gmail.com

B.V.S.S.R.S.Sastry*
Aurora's Engineering College
Bhongir, Andhra Pradesh, India
sastry_38@yahoo.com

K. Akshitha
Aurora's Engineering College
Bhongir, Andhra Pradesh, India
koluguri.87@gmail.com

Dr.S.M.Afroz
Professor (CSE)
Nizam's Engineering College
Andhra Pradesh, India

Abstract - IP multicast, method of sending IP datagrams to a group of interested receivers in a single transmission. Some applications require data to be delivered from a sender to multiple receivers. Examples of such applications include audio and video broadcasts, real-time delivery of stock quotes, and teleconferencing applications [1]. In contrast to the one-to-one model of IP unicast, in which data packets are sent from a single source to a single recipient, IP multicast provides a method of efficient many-to-many communication. This concept is becoming increasingly important, both in the Internet and in private networks, for providing services such as multimedia content delivery[2][3]. In this paper we provide various technologies to be implemented in multicast Environment.

Keywords - IP multicast, IGMP, PIM, multicast authority, multicast security

I. INTRODUCTION

Deering proposed IP multicast – an extension to the IP unicast service model for efficient multipoint communication [1]. The multicast service model offered two key benefits: (1) the efficient use of bandwidth for multipoint communication and, (2) the indirection of a group address which allows for network-level rendezvous and service discovery. Deering's proposal triggered an era of research on the implementation and applications of IP multicast.

In terms of actual deployment, this research has had somewhat mixed success. On the one hand, support for multicast is built into virtually every endhost and IP router and the service is often deployed within enterprise networks. However there is little crossprovider global deployment of multicast, and today, fifteen years after Deering's seminal work, the vision of a ubiquitous multicast "dialtone" remains an elusive, if not altogether abandoned, goal.

Theories abound for why this vision was never realized (*e.g.*, [2–4]). Very broadly, most of these can be viewed as questioning the viability of IP multicast on two fronts. The first is its practical *feasibility* given the apparent complexity of deploying and managing multicast at the network layer. The second is the *desirability* of supporting multicast with many questioning whether the demand for multicast applications justified the complexity of its deployment, whether ISPs could effectively charge for the service, the adequacy of alternate solutions, and so forth.

II. OVERVIEW

As far as the heavy traffic and the large number of multicast data receivers are concerned, strict multicast source and user management is required to control the direction and scope of multicast data propagation so as to implement multicast services on IP multicast networks. Otherwise, the deployment of multicast service will not only bring impact on existing IP networks, but also fail to provide expected QoS for users [3][5].

The standard IP multicast protocol defined by IETF does not cover multicast control and management. In combination with the IP network model and IP multicast technologies, the controllable multicast technologies define a control model and a control mechanism for IP multicast services on basis of complete compliance with the standard IP multicast protocol so that multicast services become controllable, manageable, and operable [6][8]. The control mechanism involves technologies such as multicast address allocation, multicast source control, multicast traffic control, multicast receiver control, and multicast security control.

Authentication, authorization, and accounting (AAA) and configurations involved in multicast service control can be integrated into an AAA server and NM server, respectively, or be integrated into a standalone device — multicast management server.

The figure 1 below shows the model for implementing IP multicast technologies:

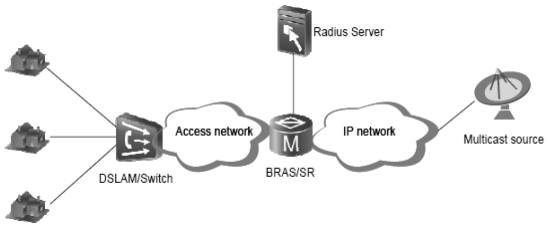

Figure 1: Implementation of IP Multicast

Through NMS or MML, the network administrator can configure necessary parameters related to multicast source authentication, authorization, and traffic control on the router directly connected to the multicast source, and parameters related to receiver authentication, authorization, and traffic control on the access edge device (such as DSLAM) directly connected to receivers or on the network access server (such as BRAS) of receivers.

The edge router directly connected with the multicast source first detects multicast traffic to be sent to the network and then controls the multicast traffic delivery according to the local or remote authentication result [6][7]. The edger router either discards the multicast traffic or forwards it to the network in accordance with the setting of flow control parameters.

The edge access device or the network access server detects that a user sends an IGMP message to the network and controls users joining in the multicast group according to the local or remote authentication. The network access server prevents or restricts users from receiving multicast traffic in accordance with the setting of flow control parameters. The layer 2 switch on the access network suppresses multicast flooding on the layer 2 network and prevents unauthorized users from receiving multicast traffic through IGMP Snooping, IGMP Proxy or other layer 2 multicast control protocols.

The controllable multicast model is built on the one-to-many or many-to-many multicast applications with a limited number of relatively-fixed multicast sources. The model can meet the following requirements:

A. Multicast data delivery, multicast traffic, and destination multicast group address of a multicast source are strictly controlled and recorded.
B. Which multicast groups a receiver joins or leaves is strictly controlled and recorded.
C. User access authentication and user multicast authentication are bound together or separated from each other so as to separate the access control from the service control.
D. A reliable authentication mechanism is provided to prevent fraudulence.
E. Layer 2 switches at the network access layer can suppress multicast flooding on the layer 2 network and isolates receivers to guarantee the security of multicast data.
F. The receiver terminal supports IGMP, and the access device can identify IGMP messages.
G. Smooth connection with existing access devices, authentication devices, and accounting devices can be implemented.

Through the controllable multicast technologies and the control model, network operators can operate, manage, and monitor IP multicast services. Multicast services are usually considered as value-added services. Content providers are usually multicast sources. Network operators construct, maintain, and manage multicast-supporting IP networks, and also manage multicast sources, multicast receivers, and multicast addresses in a centralized way. Content providers and network operators reach an authorization agreement on management and accounting of multicast services [9]. Through the cooperation of the edge access device or network access server, authentication server, and NM server, network operators can implement multicast source control, receiver control, and accounting data collection, guarantee information security, and prevent illegal multicast sources[11]. By monitoring the state, session, members, route, traffic, protocol, topology and geographical location, network operators can plan and balance the whole-network load and services, analyze, diagnose, prevent, and recover network faults[10]. Through address space monitoring, network operators can allocate and manage multicast addresses in a more reasonable way.

III. KEY TECHNOLOGIES

The controllable multicast technologies include multicast address allocation, multicast source control, multicast traffic control, multicast receiver control, and multicast security control.

A. Multicast Address Allocation

In IGMPv1 and IGMPv2, a multicast address Gx uniquely identifies a multicast group, which is referred to as any source multicast (ASM).The receivers of multicast data do not need to know the sender's address, but they must know the multicast address. After sending an IGMP Join (*,Gx) to join the multicast group Gx, users can receive the information flow addressed to the multicast group. In IGMPv3, the combination of multicast address with the multicast source address (Sx,Gx) uniquely identifies a multicast group, which is referred to as source specific multicast (SSM). Currently, the one-to-one and many-to-many multicast applications with a limited number of relatively-fixed multicast sources have a high demand on the IP multicast technologies [13 – 18]. Multicast sources are usually content servers that send multicast information in a relatively-fixed period. Therefore, one or more multicast sources should be statically allocated with one or more fixed multicast addresses to send a specific type of multicast information flows in the commercialized operation of multicast services. For the many-to-many multicast applications that would be used widely in future, multicast sources should also be controllable in aspect of scope and addresses. Network operators manage the allocation and reclaim of multicast addresses in the whole network: They allocate a specific multicast address when a multicast service is requested for creation, and reclaim the multicast address when the service is requested for termination to guarantee no conflicts between various multicast information flows. To support multicast services among different network operators, the Internet Assigned Number Authority (IANA) will pre-allocate some multicast addresses to the network operators to prevent multicast address allocation conflicts among them. For the multicast addresses that can be allocated to users, see figure 2 below:

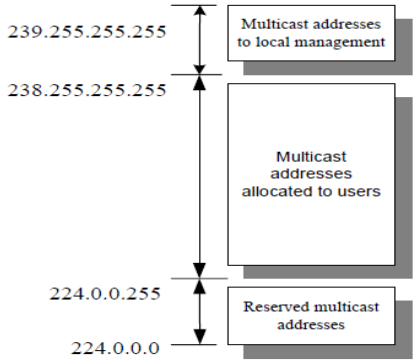

Figure 2: Allocation of Multicast Addresses to users

IETF has presented some suggestive or tentative standards for multicast address dynamic client allocation protocol (MADCAP). However, cross-domain multicast services are currently very few. Therefore, it is recommended that network operators should adopt the static multicast address allocation method in a short term. The manual management of multicast address allocation and reclaim can ensure no multicast address conflict within a domain. With the development of multicast services and the improvement of multicast protocols, MADCAP can be considered in future.

B. Multicast Source Control

Before a multicast service is created, the content provider (namely, multicast source) must submit an application to the network operator to apply for multicast source address, multicast address, bandwidth, priority, and multicast route [12] [15]. After a multicast service is terminated, the content provider must submit an application again, asking the network operator to reclaim the multicast source address, multicast address, bandwidth, priority, and multicast route.

The creation of a multicast service involves the release of the multicast service and the authorization of multicast source. The content provider should prepare the software used for sending and receiving multicast information flows and announce the receiver software to users.

The release of multicast service means releasing the correspondence between the multicast address and the multicast service to users. A multicast service can be released in two ways. One is to use a well-known multicast address to release the correspondence so that hosts can listen to these multicast messages. The other is to release the correspondence to one or more well-known websites so that hosts can query these websites [16]. From the angle of network resource occupation and management, the latter is recommended to release classified, leveled services to users, and also release the receiver software to users to facilitate the maintenance and update of the released service.

The authorization of the multicast source must ensure that only the applied and authorized multicast source can send multicast messages to the network. Two authorization modes are available to multicast sources:

a. *Static Long-Term Authorization:*

After assigning a multicast source address, multicast address, bandwidth, priority, and multicast route, the network administrator configures ACL and CAR on the edge router directly connected with the multicast source through the NMS (or multicast management server) or MML to perform the long-term authorization. The authorization is deleted when the multicast service is terminated. Only local authentication is performed for multicast messages listened to by the edge router.

b. *Dynamic Authentication and Authorization:*

After assigning a multicast source address, multicast address, bandwidth, priority, and multicast route, the network administrator configure these parameters as a multicast source authority list on the authentication server (or multicast management server). The authentication server (or multicast management server) performs remote authentication for the multicast source address and multicast address in multicast messages listened to by the edge router. After authentication, the authentication server (or multicast management server) returns the authentication result to the edge router. The edge router configures ACL and CAR according to the authentication result. Upon detecting that the multicast source stops sending multicast messages, the edge router deletes the authorization result. The authentication, authorization, and accounting information between the edge router and the authentication server (or multicast management server) can be exchanged through RADIUS or a similar protocol.

From the angle of management, the static long-term authorization mode is stable and simple for one-to-many or many-to-many multicast applications with a limited number of relatively fixed multicast resources. By default, multicast source control requires that all edge access devices and edge routers should be forbidden to forward multicast messages from downlinks unless the multicast messages comply with the configured ACL and CAR. When a host sends a multicast message, the first edge router receiving the message will use the ACL and CAR to filter the message. Only the message satisfying the condition is forwarded to the multicast distribution tree.

Multicast route configuration makes multicast data go from the multicast source through the multicast distribution tree to multicast group members. Configuration commands and methods vary with multicast protocols [17]. For multicast services requiring high security, a static multicast distribution tree can be configured so as to strictly control the path, scope, and traffic of multicast messages.

When a multicast source stops sending multicast messages and requests to release the multicast address and the multicast authorization is deleted, the multicast service is terminated.

C. Multicast Traffic Control

In view of the characteristics of heavy traffic and many receivers of multicast data, measures should be adopted to control multicast traffic on the network to avoid impact on the network and unicast services.

The following measures can be adopted:

Configure a priority for multicast messages to enter the network. Use QoS forwarding methods such as DiffServ of the network. Configure ACL and CAR (including multicast identifier and committed rate) on edge routers [11]. Forbid unauthorized multicast messages from being forwarded and restrict the traffic of multicast messages entering the network. Let the edge router shape or discard the data flow according to the service level agreement (SLA) if the actual traffic exceeds the committed rate [19].

In the backbone network, tunneling or MPLS VPN is used to isolate multicast traffic from unicast traffic. Control multicast traffic by restricting the bandwidth of tunnels and VPNs. Control the traffic of inter-domain multicast messages by using the ACL and CAR (where the multicast

address is matched with the egress interface) on edge routers.

In the access network, isolate multicast traffic from unicast traffic by dividing VLANs. In this case, inter-VLAN multicast replication should be supported. Control multicast traffic by limiting port rate and VLAN rate.

Perform resource admission control when users request to join a multicast group. Only the bandwidth agreed between users and network operators, access link bandwidth, and network bandwidth satisfy the requirement of the bandwidth necessary for multicast traffic, the request can be accepted to avoid the situation that the QoS cannot be guaranteed because of the excessive traffic [15]. By limiting the maximum number of multicast groups on the access network, the maximum number of members in a multicast group, and the maximum number of multicast entries on the layer 2/3 network device, the number and size of multicast distribution trees can be restricted to some extent to avoid DoS attacks against multicast devices. If necessary, static multicast distribution trees can be configured.

D. Multicast Receiver Control

Edge access devices or the network access server is responsible for performing local or remote authentication and authorization for users who wish to join a multicast group to control multicast receivers at the network layer and collect accounting data. Multicast services can be put under the unified management of the network operator. Multicast receiver control at the application layer is not discussed in this document.

The following describes the complete process in which a user accesses a multicast service:

a. Access authentication— Authentication performed when a user accesses a network.
b. Service selection — A user selects a multicast service on the WEB page or via the multicast receiver software.
c. Multicast authentication — Authentication performed when a user joins a multicast group.
d. Multicast reception — A user receives and reads multicast information flows via the receiver software.
e. Multicast exit — A user leaves a multicast group.
f. Access exit — A user is disconnected with the network.

There are three access authentication modes: port-based authentication, account-based authentication, and authentication based on account and port. The port-based authentication does not require users to enter any account or password. Three types of account-based authentication are available: PPP authentication, 802.1x authentication, and WEB-based portal authentication. The user access identifier, which can be user account, VLAN ID, physical port, MAC address or binding information, varies with access authentication modes.

No matter whatever the authentication mode is, all network devices responsible for multicast authentication must detect the IGMP Join message originated by users to the network to perform the local or remote authentication at the network layer to determine whether the users can join a multicast group. The network devices also process the IGMP Join message according to the authentication and authorization results. The authentication and authorization of multicast receivers must ensure that only the requested and authorized multicast receivers can receive the traffic of the multicast group over the network [18] [20].

If the multicast authentication succeeds, the IGMP Join message is transparently transmitted or sent to a multicast router via Proxy, or the IGMP Join message is added to a multicast distribution tree through the protocol independent multicast – sparse mode (PIM-SM) after it is terminated. The traffic of the authorized multicast group is forwarded to the user according to the traffic control parameters. As a result, the user becomes a receiver of the multicast group. If the multicast authentication fails, the IGMP Join message is directly discarded or special treatment is given to it.

When detecting that a user sends an IGMP Leave message or learning via the timer that a user leaves a multicast group, the edge access device stops forwarding the traffic of the multicast group to the user [14].

E. Multicast Receiver Authentication and Control Point

As the multicast authentication node varies, two authentication and authorization methods are available to multicast receivers.

a. Multicast authentication on the edge access device:

The edge access device can terminate or transparently transmit IGMP messages via Proxy. When detecting an IGMP Join message from a user, the edge access device performs the local multicast authentication according to the multicast source address, multicast address and user's port number in the IGMP Join message, or originates a remote multicast authentication request to the authentication server (or multicast management server). Based on the authentication result, the edge access device directly controls the forwarding of the traffic of the multicast group to the user to ensure the security of multicast traffic on the access network, without any interaction with the network access server.

b. Multicast Authentication on the Network Access Server:

This method requires that the edge access device can transparently transmit the IGMP Join message of the user to the network access server. When detecting the IGMP Join message from the user, the network access server performs the local multicast authentication according to the multicast source address and multicast address in the IGMP Join message, or originates a remote multicast authentication request to the authentication server (or multicast management server). Based on the authentication result, the network access server controls the forwarding of the traffic of the multicast group to the user and meanwhile actively controls the multicast forwarding behavior of the edge access device to ensure the security of multicast traffic on the access network.

F. Multicast Security Control

On the access network, a layer 2 switching device supports IGMP Snooping or IGMP Proxy, or other layer 2 multicast control protocols to suppress multicast flooding and prevent unauthorized users from receiving multicast traffic. Otherwise, even if multicast authentication and authorization is implemented, unauthorized users may still receive multicast information flows when the access device forwards multicast messages in broadcast mode [12][15].

During multicast authentication, if each VLAN contains more than one user, when processing an IGMP message or detecting a user leaves a multicast group via the timer, the network access server should actively control the multicast forwarding behavior of the edge access device and prevent the edge access device from forwarding multicast traffic to the user who fails multicast authentication. If each VLAN contains multiple user ports, each port should separately maintain the multicast group list to prevent flooding of the

multicast message between ports in the VLAN. To further save network sources occupied by multicast traffic, the edge access device should support inter-VLAN multicast replication. To ensure the validity of multicast authentication, the network access server and layer 2 switching device should be able of detecting fraudulent MAC addresses under different VLANs. To do so, MAC address based authentication and user information binding are required after user authentication [14]. The edge access device must suppress unauthorized multicast messages from users. By default, the edge access device should be forbidden to forward multicast messages from downlinks unless the multicast messages comply with the configured ACL and CAR (including the multicast group identifier and committed rate).

IV. CONCLUSION

By using the controllable multicast technologies, network operators can control multicast in an effective and secure way so that the multicast service becomes operable and manageable. In combination with reasonable user authentication, accounting system, and policies, the multicast service will develop healthily and stably to gradually become an operable, manageable Internet value-added service with a mature value chain system.

V. REFERENCES

[1] Stephen Deering and David Cheriton. Multicast routing in datagram internetworks and extended LANs. ACM Transactions on ComputerSystems, 8(2):85–110, May 1990.

[2] Yang hua Chu, Sanjay Rao, and Hui Zhang. A Case for End System Multicast. In Proceedings of SIGMETRICS 2000, CA, June 2000.

[3] Christophe Diot, Brian Levine, Bryan Lyles, H. Kassem, and D. Balensiefen. Deployment issues for IP multicast service and architecture. IEEE Network Magazine. Special Issue on Multicasting, 2000.

[4] Hugh Holbrook and David Cheriton. Ip multicast channels: Express support for single-source multicast applications. In Proceedings of SIGCOMM ’99, Cambridge, MA, September 1999.

[5] ISC Domain Survey, January 2005.

[6] Craig Labovitz, Abha Ahuja, Abhijit Abose, and Farnam Jahanian. An experimental study of delayed Internet routing convergence. 2000.

[7] Matthew Caesar, Donald Caldwell, Nick Feamster, Jennifer Rexford, Aman Shikh, and Jacobus van der Merwe. Design and Implementation of a Routing Control Platform. In Proc. of NSDI, 2005.

[8] E. Castronova. Network Technology, Markets and the Growth of Synthetic Worlds. In Second Workshop on Network and Systems Support for Games (NetGames). ACM, May 2003.

[9] MMOGCHART. http://www.mmogchart.com , http://terranova.blogs.com/terra nova/2003/10/growth rates of.html.

[10] Blizzard Entertainment. WoW Surpasses 5 Million Customers Worldwide. 2005. http://www.blizzard.com/press/051219.shtml.

[11] N. Sheldon, E. Girard, S. Borg, M. Claypool, and E. Agu. The Effect of Latency on User Performance in Warcraft III. In Second Workshop on Network and Systems Support for Games (NetGames). ACM, May 2003.

[12] J. Pellegrino and C. Dovrolis. Bandwidth Requirement and State Consistency in Three Multiplayer Game Architectures. In Second Workshop on Network and Systems Support for Games (NetGames). ACM, May 2003.

[13] Blizzard Entertainment. World of Warcraft. http://www.blizzard.com.

[14] Synthetic Statehood and the Right to Assemble. http://terranova.blogs.com/2005/02/the right to as.html.

[15] Microsoft IPTV Edition.

[16] Ion Stoica, Dan Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet Indirection Infrastructure. In Proceedings of SIGCOMM, August 2002.

[17] Bryan Ford. Unmanaged Internet Protocol: Taming the edge network management crisis. In HotNets, November 2003.

[18] A. Rowstron, A-M. Kermarrec, M. Castro, and P. Druschel. SCRIBE: A large-scale and decentralized application-level multicast infrastructure. In Proceedings of NGC, London, UK, November 2001.

[19] Hui, Chaintreau, Scott, Gass, Crowcroft, and Diot. Pocket switched networks and the consequences of human mobility in conference environments. In Workshop on Delay Tolerant Networking, 2005.

[20] Kevin Fall. A Delay Tolerant Networking Architecture for Challenged Internets. In Proceedings of SIGCOMM, August 2003.