Tsunemasa Hayashi, NTT
Haixiang He, Nortel
Hiroaki Satou, NTT
Hiroshi Ohta, NTT
Susheela Vaidya, Cisco Systems

Internet Draft
Document:draft-ietf-mboned-maccnt-req-00.txt
Expires: October 15, 2005

April 15, 2005

Accounting, Authentication and Authorization Issues in Well Managed IP Multicasting Services

<draft-ietf-mboned-maccnt-req-00.txt>

Status of this Memo

Copyright Notice

Internet Draft draft-ietf-mboned-maccnt-req-00.txt April, 2005

Abstract

This Internet Draft (I-D) describes problems in the area of accounting and access control for multicasting. General requirements for accounting capabilities including quality-of-service (QoS) related issues are listed. This I-D assumes that these capabilities can be realized by functions implemented at edges of a network based on IGMP or MLD. By such functions, information obtained from edge routers would be logged in a dedicated database. Finally, cases for Content Delivery Services (CDS) are described as application examples which could benefit from multicasting accounting and access control capabilities as described in the I-D. It is proposed that this I-D be used as a starting point for further discussion on these issues.

Table of contents

1. Introduction

The intention of this Internet Draft (I-D) is to initiate a discussion focused on accounting, authentication and authorization issues for "well-managed IP multicasting" services ("well-managed" defined at the end of this introduction). This I-D intends to develop an informational RFC on requirements for "well-managed IP multicasting".

IP multicasting is becoming widely used as a method to save network resources such as bandwidth or CPU processing power of the sender's server for cases where a large volume of information needs to be distributed to a large number of receivers. This trend can be observed both in enterprise use and in broadband services provided by network operator/service providers.

Distance learning within a university and in-house (in-company) sharing of multimedia information are examples of enterprise use. In these examples, sources generate high-bit rate (e.g., 6Mbit/s) streaming information. When the number of receivers becomes large, such systems do not scale well without multicasting.

On the other hand, a Content Delivery Service (CDS) is an example of a broadband service provided by network operators/service providers. Distribution of movies and other video programs to each user are typical services. Each channel requires large bandwidth (e.g., 6Mbit/s) and operator/service providers need to provide many channels to make their service attractive. In addition, the number of receivers is large (e.g., more than a few thousands). The system to provide this service does not scale well without multicasting.

As such, multicasting can be useful to make the network more scalable when a large volume of information needs to be distributed to a large number of receivers. However, multicasting according to

current standards (e.g., IGMPv3[1] and MLDv2[2]) has drawbacks compared to unicasting when one applies it to commercial services. Accounting of each user's actions is not possible with multicasting as it is with unicasting. Accounting consists of grasping each user's behavior, when she/he starts/stops to receive a channel, which channel she/he receives, etc.

IP multicasting can be used to distribute free material efficiently, but there are limitations to multicasting in usage models where usage accounting is necessary, such as many commercial applications. Although multicasting has already been used in several applications, in many cases it is used in such a way that accounting is not necessary. Alternatively, one could develop and use a proprietary solution to address this issue. However, non-standard solutions

have drawbacks in terms of interoperability or cost of development and maintenance.

Without accounting capability in multicasting, information providers desiring accounting capability are forced to use unicasting even when multicasting would otherwise be desirable from a bandwidth/server resource perspective. If multicasting could be used with user-based accounting capabilities, its applicability would be greatly widened.

This I-D first describes problems on accounting issues in multicasting. Then the general requirements for this capability including QoS related issues are listed. This I-D assumes that these capabilities can be realized by functions implemented at edges of a network based on IGMP or MLD. Such functions would record into dedicated database information obtained from edge routers. Finally, application examples which could benefit from multicasting with accounting capabilities are shown. It is proposed that this I-D be used as a starting point for a discussion on these issues.

This I-D will present general functional requirements related to accounting, authentication and authorization issues in IP multicasting networks, and a multicast network which fulfills these requirements will be called a "well managed" IP multicasting network.

2. Definitions and Abbreviations

2.1 Definitions

Authentication: action for identifying a user as a genuine one.

Authorization: action for giving permission for a user to access content or the network.

User-based accounting: actions for grasping each user's behavior, when she/he starts/stops to receive a channel, which channel she/he receives, etc.

2.2 Abbreviations

ASM: Any-Source Multicast

CDS: Content Delivery Service

CP: Content Provider

IGMP: Internet Group Management Protocol

MLD: Multicast Listener Discovery

NSP: Network Service Provider

SSM: Single-Source Multicast

QoS: Quality of Service

3. Problem statement

3.1 Accounting issues

In unicast communications, the server (information source) can identify the client (information receiver) and only permits connection by an eligible client when this type of access control is necessary. In addition, when necessary, the server can grasp

what the client is doing (e.g., connecting to the server, starting reception, what information the client is receiving, terminating reception, disconnecting from the server).

On the other hand, in multicast communication as in Fig.1, the server just feeds its information to the multicast router. Then, the multicast router replicates the information to distribute to the clients. According to current standards (e.g., IGMPv3[1] or MLDv2[2]), the multicast router feeds the replicated information to any link which has at least one client requesting the information. In this process, no eligibility check is conducted. Any client can receive information just by requesting it. In other words, the current standards do not provide multicasting with authorization or access control capabilities sufficient to meet the requirements of accounting.

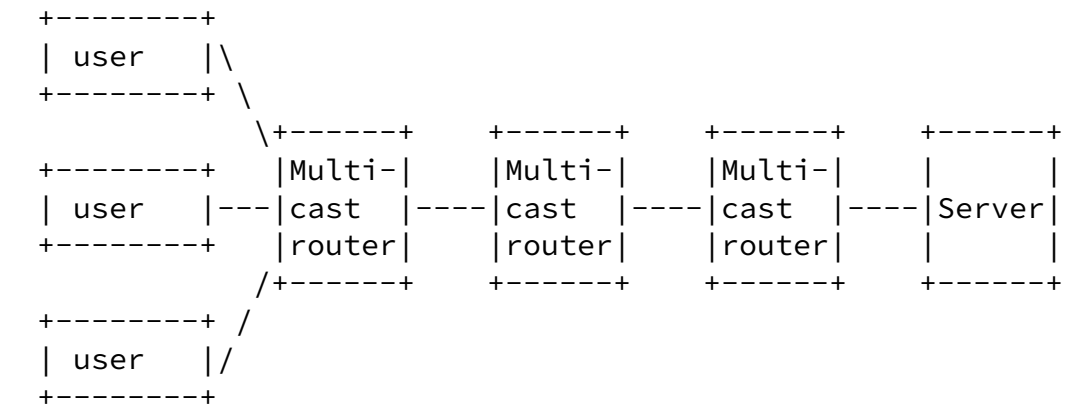


Fig.1 Example network for multicast communication

This is the major reason why multicasting is only used for cases where no user-based accounting capabilities are necessary. However, since more and more information is transferred over IP-based networks and some of these applications may require accounting capabilities, it is easy to envision the requirement of supporting such cases. For example, accounting is needed if one wants to charge for distributed information on a non-flat-fee basis. If the volume of information and number of clients are large, it is beneficial to use multicasting for purposes of network resource efficiency.

As such, the same level of user-based accounting capabilities as provided in unicast networks should be provided in multicast networks.

3.2 Relationship with secure multicasting (MSEC)

In many cases, content encryption (e.g. MSEC) is an effective method for preventing unauthorized access to original content (in other words, the ability to decode data to return it to its generally useable form.) This I-D presents requirements for multicasting networks in the areas of 1) access control to prevent unauthorized access to the network, and 2) accounting to grasp user activity. It is not the intention of this I-D to propose alternatives to encryption. Access control, accounting and encryption are separate technologies. The implementation of any of these technologies does not preclude the use of the others.

4. Functional general requirements for well managed IP multicasting

It seems beneficial to use IGMP or MLD for access controlling in multicast networks. However, from the considerations presented in section 3, there are issues in the following areas:

(1) User identification

The network should be able to identify each user when they attempt to access the service so that necessary access controlling actions can be applied. Also, it is necessary to identify the source (user) of each request (e.g., join/leave) for user accounting purposes.

With current protocols, the sender cannot distinguish which receivers (end hosts) are actually receiving its information with current protocols (IGMP/MLD.) The sender must rely on the

information from the multicasting routers. This can be complicated if the sender and routers are maintained by different entities.

(2) Issue of network resource protection

In order to guarantee certain QoS it is important for network providers to be able to protect their network resources from being wasted, (either maliciously or accidentally).

(2.1) Access control

The network should be able to apply necessary access controlling actions when an eligible user requests. The network should be able to reject any action requested from an ineligible user.

(2.2) Control mechanism to support bandwidth of multicast stream from a physical port of edge router or switch

The network should be able to control the combined bandwidth for all groups both at the physical port of the edge router or switch so that these given physical entities are not overflowed with traffic.

(2.3) Control mechanism of number of groups delivered from a physical port of edge router and switch

In order to enable an NSP to guarantee a certain level of QoS to the CP and the receivers, it is important that the NSP can control the number of groups delivered from a physical port of an edge router and a switch so that the combined bandwidth between content servers and multicast routers can be within the limit.

(3) User authentication

The network should be able to authenticate a user.

(4) User authorization

The network should be able to authorize a user's access to content or a multicast group, so as to meet any demands by a CP to prevent content access by ineligible users. Also, the NSP does not want to waste their network resources on ineligible users. Eligibility can be defined in several ways. The definition of an "eligible user" should be discussed further.

(5) Accounting and billing

In many commercial multicast situations, NSP would like to be able to precisely grasp network resource consumption and CP would like to be able to precisely grasp the content consumption by end-users. Such information might be used for "identifying highly viewed content" for advertising revenue, ratings calculations, programming decisions, etc., as well as billing and auditing purposes. Also content and network providers may wish to provide users with access to their usage history.

To assemble such an understanding of end-user behavior, it is necessary to precisely log information such as who (host/user) is accessing what content at what time (join action) until what time (leave action). The result of the access-control decision (e.g. results of authorization) would also be valuable information. The desired degree of logging precisions would depend on the application used.

Networks need database functions to realize user-based accounting through the accumulation of logs from edge routers.

(5.1) How to share user information

For commercial multicast applications it is important for NSP and CP to be able to share information regarding user's behaviour (as described in (5) in standardized ways.

(6) Notification to users of the result of the join request

It should be possible to provide information to the user about the status of his/her join request(granted/denied/other).

(7) Service and terminal portability

Networks should allow for a user to receive a service from different places and/or with a different terminal device.

(8) Support of ASM and SSM

Both ASM (G), and SSM (S,G) should be supported as multicast models.

(9) Admission control for join action

In order to maintain a predefined QoS level, an edge router should not accept a consequent "join" after a "leave" until the

termination of the stream of the multicast group which was "left". This is essential to protect against e.g., multicast denial of service (DoS) attacks.

(10) Channel Leave Latency

Commercial implementations of IP multicasting are likely to have strict requirements in terms of user experience. Leave latency is the time between when a user sends a signal that he/she wishes to "leave" a group and when the network recognizes the "leave."

Leave latency impacts :

i. Acceptable end-user experience for fast channel surfing.

In an IP-TV application, users are not going to be receptive to slow response time when changing channels.

ii. Resource consumption

With a low "leave latency" network providers could minimize streaming content when there are no audiences.

It is important that any overhead for authentication, authorization, and access-control be minimized at the times of joining and leaving multicast groups so as to achieve join and leave latencies acceptable in terms of user experience. For example this is important in an IP-TV application, because users are not going to be receptive to a slow response time when changing channels.

(11) Scalability

Solutions that are used for well managed IP multicasting should scale enough to support the needs of content providers and network operators.

(12) Small impact on the existing products

Impact on the existing products (e.g., protocols, software, etc.) should be as minimal as possible.

Ideally the NSP should be able to use the same infrastructure (such as access control) to support commercial multicast services for the so called "triple play" services: voice (VoIP), video, and broadband Internet access services.

(13) Deployable as alternative to Unicast

IP Multicasting would ideally be available as an alternative to IP unicasting when the "on-demand" nature of unicasting is not required. Therefore interfaces to multicasting should allow for easy integration into CDS systems that support unicasting. Especially equivalent interfaces for authorization, access control and accounting capabilities should be provided.

(14) Multicast replication
The above requirements should also apply if multicast replication is
being done on an access-node (e.g. DSLAMs or OLTs).

Specific functional requirements for each application can be derived from the above general requirements. An example is shown in the section 5.

5. Application example and its specific requirements

This section shows an application example which could benefit from

multicasting. Then, specific functional requirements related to user-based accounting capabilities are derived.

5.1 IP Multicast-based Content Delivery Service (CDS): CP and NSP are different entities (companies)

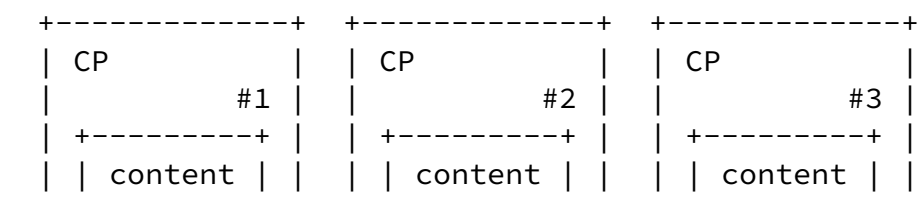
Broadband access networks such as ADSL (Asymmetric Digital Subscriber Line) or FTTH (Fiber to the Home) have been deployed widely in recent years. Content Delivery Service (CDS) is expected to be a major application provided through broadband access networks. Because many services such as television broadcasting require huge bandwidth (e.g., 6Mbit/s) and processing power at content server, IP multicast is used as an efficient delivery mechanism for CDS.

One way to provide high quality CDS is to use closed networks ("walled-garden" model).

This subsection shows an example where CP and NSP are different entities (companies).

5.1.1 Network model for Multicast Content Delivery Service

As shown in Fig.2, networks for CDS contain three different types of entities: Content Provider (CP), Network Service Provider (NSP), and end user clients. An NSP owns the network resources (infrastructure). It accommodates content providers on one side and accommodates end user clients on the other side. NSP provides the network for CDS to two other entities (i.e., CPs and end user clients). A CP provides content to each end-user client through the network of NSPs. NSPs are responsible for delivering the content to end user clients, and for controlling the network resources.



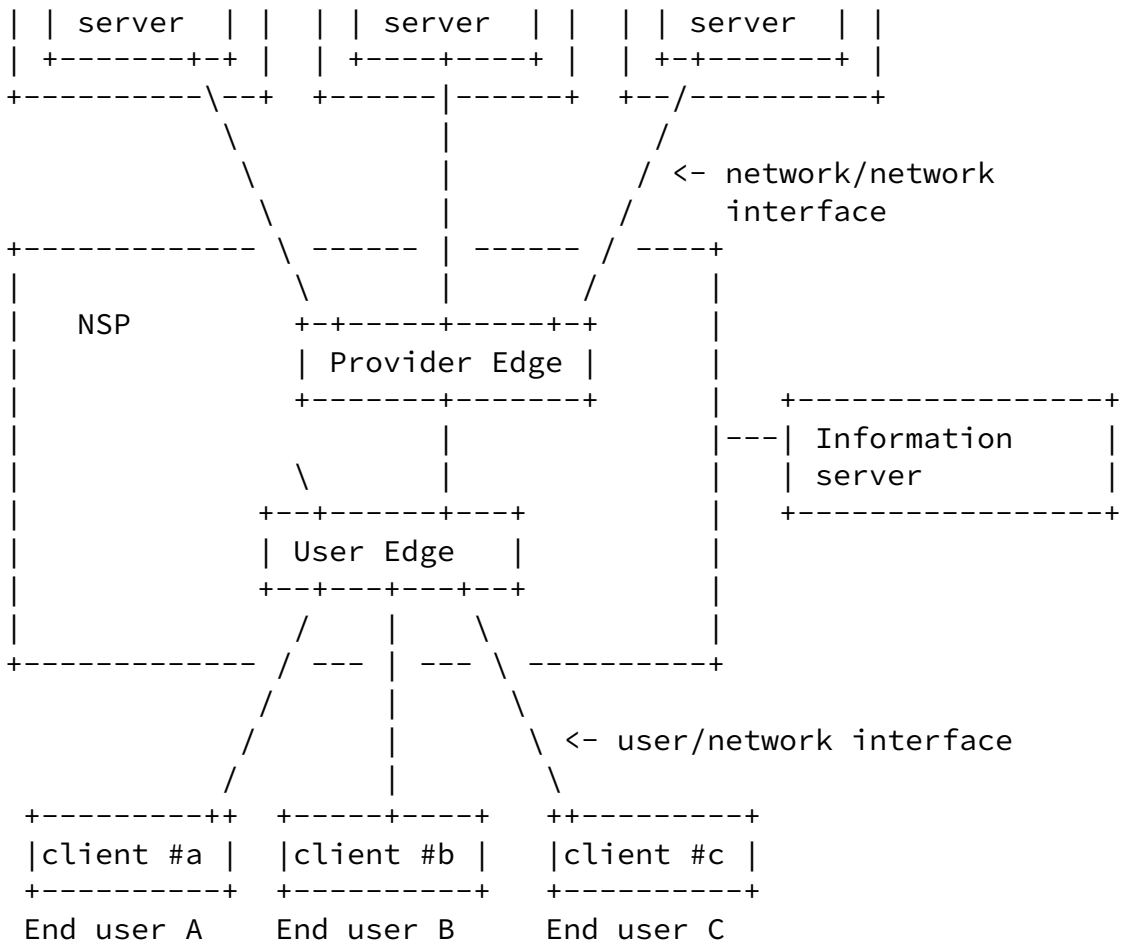


Fig.2 Example of CDS network configuration

The NSP provides the information server for all multicast channels, and a CP gives detailed channel information (e.g., Time table of each channel) to the information server. An end-user client gets the information from the information server. In this model, multicast is used in the NSP's CDS network, and there are two

different contracts. One is the contract between the NSP and the end user which permits the user to access the basic network resources of the NSP. Another contract is between the CP and end user to permit the user to subscribe multicast content. Because the CP and NSP are different entities, and the NSP generally does not allow a CP to control (operate) the network resources of the NSP, user authorization needs to be done by the CP and NSP independently.

Since there is no direct connection to the user/network interface, the CP cannot control the user/network interface. An end user may want to move to another place, or may want to change her/his device (client) anytime without interrupting her/his receiving services. As such, IP Multicast network should support portability capabilities.

5.1.2 Content Delivery Service Requirements

To have a successful business providing multicast, there are some specific requirements for the IP Multicast-based Content Delivery Service.

5.1.2.1 Accounting Requirements

Since the CP and NSP are different business entities, they need to share the profit. Such a profit sharing business relationship requires accurate and near real-time accounting information about the end user clients' activity on accessing the content services. The accounting information should be per content/usage-base to enable varied billing and charging methods.

The user accessing particular content is represented by the user's activities of joining or leaving the corresponding multicast group/channel (<g> or <s,g>). In multicast networks, only NSPs can collect group joining or leaving activities through their last-hop multicast access edge devices in real-time. The NSPs can transfer the accounting information to related CPs for them to generate end user billing information. The normal AAA technology can be used to transfer the accounting information.

To match the accounting information with a particular end-user client, the end-user client has to be authenticated. Usually the account information of an end-user client for content access is maintained by the CP. An end user client may have different user accounts for different CPs. The account is usually in the format of (username, password) so an end user client can access the content services from anywhere. For example, an end user client can access the CP from different NSPs. It should be noted that the user account used for content access can be different from the one used for network access maintained by NSPs.

The NSP-CP model represents a multi-domain AAA environment. There are plural cases of the model depending on the trust relationship between the NSP and CP, and additional service requirements such as a certain QoS level guarantee or service/terminal portability.

A mechanism is necessary to allow a CP and NSP to grasp each user's behavior independently.

Another requirement related to accounting is the ability to notify a user when accounting really starts. When a "free preview" capability is supported, accounting may not start at the same time as the user's joining of the stream.

5.1.2.2 Authorization Requirements

The NSPs are responsible for delivering content and are required to meet certain QoS levels or SLA (service level agreements). For example, video quality is very sensitive to packet loss. So if an NSP cannot meet the quality requirements due to limited network resources if it accepts an additional user request, the NSP should reject that end user's access request to avoid charging the existing (i.e., already joined) user for bad services. For example, if an access line is shared by several users, an additional user's join may cause performance degradation for other users. If the incoming user is the first user on an edge node, this will initiate the transmission of data between the multicast router and the edge node and this extra network traffic may cause performance degradation. There may also be policies that do not necessarily give highest priority to the "first-come" users, and these should also be considered.
In order to protect network resources against misuse/malicious access and maintain a QoS level, appropriate admission control function for traffic policing purposes is necessary so that the NSP can accept or reject the request without degrading the QoS beyond the specified level.

5.1.2.3 Authentication Requirements

There are two different aims of authentication. One is authentication for network access, and another one is for content access. For the first case of authentication, NSP has a AAA server, and for the second case, each CP has a AAA server. In some cases, CPs delegate (outsource) the operation of user authentication to NSPs.

As such, in addition to network access, multicast group access by a user also needs to be authenticated. Content authentication should support the models where:

- authentication for multicast content is outsourced to the NSP.
- authentication for multicast content access is operated by the content provider

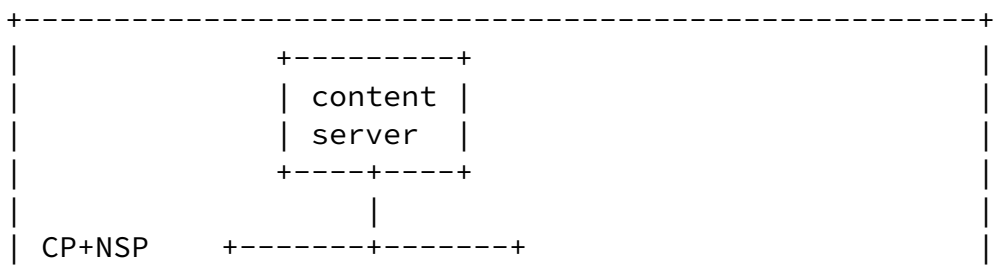
5.2 IP Multicast-based Content Delivery Service (CDS): CP and NSP are the same entities (companies)

Another application example is the case where the content provider (CP) and network service provider (NSP) are the same entity (company) as shown in Fig. 3. In the case that the CP and NSP are the same entity, some of the requirements indicated in 4.1 are not required.

This model does not require the following items:

- Communication method between sender (server) and user (end host). Since they belong to the same company, they can use all the available information.

- Methods to share user-related information between network providers and content providers.



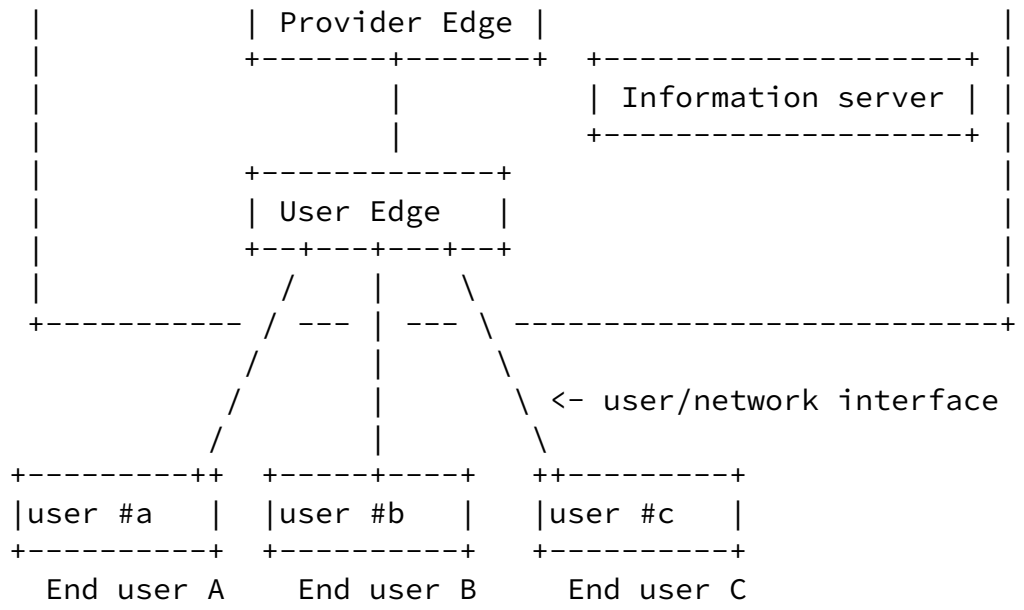


Fig.3 Example of CDS network configuration

6. IANA considerations

This I-D does not raise any IANA consideration issues.

7. Security considerations

Accounting capabilities can be used to enhance the security of multicast networks by excluding ineligible clients from the networks.

8. Conclusion

This I-D describes general requirements for providing "well managed"
IP multicasting services. It lists issues related to accounting, authentication, authorization and admission control for multicast content delivery, with the goal of finding a solution implemented at edges of the network based on IGMP or MLD. This solution likely would assume the existence of a database in the network dedicated to accumulating logs obtained from edge routers. Content Delivery Services with different business models is cited as an application

which could benefit from the capabilities of "well managed" IP multicasting described in this document.
It is proposed that this document be used as a starting point for discussing requirements for "well managed" IP multicasting services.

Normative References

[1] B. Cain, et. al., "Internet Group Management Protocol, Version 3", RFC3376, October 2002.

[2] R. Vida, et. al., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC3810, June 2004.

Authors' Addresses

Tsunemasa Hayashi
NTT Network Innovation Laboratories
1-1 Hikarino'oka, Yokosuka-shi, Kanagawa, 239-0847 Japan
Phone: +81 46 859 8790
Email: hayashi.tsunemasa@lab.ntt.co.jp

Haixiang He
Nortel
600 Technology Park Drive Billerica, MA 01801, USA
Phone: +1 978 288 7482
Email: haixiang@nortel.com

Hiroaki Satou
NTT Network Service Systems Laboratories
3-9-11 Midoricho, Musashino-shi, Tokyo, 180-8585 Japan
Phone: +81 422 59 4683
Email: satou.hiroaki@lab.ntt.co.jp

Hiroshi Ohta
NTT Network Service Systems Laboratories
3-9-11 Midoricho, Musashino-shi, Tokyo, 180-8585 Japan
Phone: +81 422 59 3617
Email: ohta.hiroshi@lab.ntt.co.jp

Susheela Vaidya
Cisco Systems, Inc.
170 W. Tasman Drive San Jose, CA 95134
Phone: +1 408 525 1952
Email: svaidya@cisco.com

Full Copyright Statement

Intellectual Property

this standard. Please address the information to the IETF at ietf ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.