

mboned
Internet-Draft
Intended status: Informational
Expires: February 25, 2011

T. Hayashi,
H. Satou,
H. Ohta
NTT
H.He
Nortel
S. Vaidya
Cisco Systems, Inc.
August 24, 2010

Requirements for Multicast AAA coordinated between Content Provider(s)
and Network Service Provider(s)
draft-ietf-mboned-macnt-req-10

Abstract

This memo presents requirements in the area of accounting and access control for IP multicasting. The scope of the requirements is limited to cases where Authentication, Accounting and Authorization (AAA) functions are coordinated between Content Provider(s) and Network Service Provider(s).

In order to describe the new requirements of a multi-entity Content Deliver System(CDS) using multicast, the memo presents three basic business models: 1) the Content Provider and the Network Provider are the same entity, 2) the Content Provider(s) and the Network Provider(s) are separate entities and users are not directly billed, and 3) the Content Provider(s) and the Network Provider(s) are separate entities and users are billed based on content consumption or subscriptions. The requirements of these three models are listed and evaluated as to which aspects are already supported by existing technologies and which aspects are not.

General requirements for accounting and admission control capabilities including quality-of-service (QoS) related issues are listed and the constituent logical functional components are presented.

This memo assumes that the capabilities can be realized by integrating AAA functionalities with a multicast CDS system, with IGMP/MLD at the edge of the network.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on February 25, 2011.

1. Introduction

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 the content server(s), IP multicast is used as an efficient delivery mechanism for CDS.

A single entity may design and be responsible for a system that covers the various common high-level requirements of a multicasting CDS such as 1) content serving, 2) the infrastructure to multicast it, 3) network and content access control mechanisms. For cases in which the business model includes the direct billing of users, the single provider of both content and network services has sufficient data in its control to bill users based on their content consumption. Furthermore it is possible to tie access to the network and QoS based on a user's contract status. Therefore current technologies support the single entity case.

Often, however, the content provision and network provision roles are

split between separate entities. Commonly, Content Providers (CP) do not build and maintain their own multicast network infrastructure as this is not their primary business area. Instead, CPs often purchase transport and management services from network service providers. This memo lists the requirements of a business model in which the NSP provides CDS using multicast as one such contractible service.

The direct revenue source for the multiple entity provider is a defining aspect of the business model which often has implications on requirements for the technologies that support the system. There are cases such as the the advertising-based model where billing end-users is not done and therefore accounting of content consumption can be anonymous and/or in aggregate. In these cases the requirements of the business model for accounting for billing purposes are already supported by existing technologies. However, the NSP can not guarantee high quality transmission on a per-content basis with existing technologies.

There is also the business model in which the individual user of multicastrated contents is the source of revenue for both consumed content and network resources. In this model the NSP wants to receive the appropriate fees for multicast services and the NSP undertakes collecting bills as a proxy for the CPs. The NSP may provide high quality service by admission control. Current standards do not fully support this model and this memo will list the requirements which need to be supported.

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.

Eligible user: Users may be eligible (permitted) to access resources because of the attributes they have (e.g., delivery may require possession of the correct password or digital certificate), their equipment has (e.g., content may only be eligible to players that can decode H.264 or 3GPP streams), their access network has (e.g., HDTV content may only be eligible to users with 10 Mbps or faster access line), or because of where they are in network topology (e.g., HDTV content may not be eligible for users across congested links) or in actual geography (e.g., content may only be licensed for distribution to certain countries), and, of course, a mix of attributes may be required

for eligibility or ineligibility.

User: In this document user refers to a requester and a recipient of multicast data, termed a viewer in CDS.

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

AAA: Authentication, Accounting and Authorization

ASM: Any-Source Multicast

CDS: Content Delivery Service

CP: Content Provider

IGMP: Internet Group Management Protocol

MLD: Multicast Listener Discovery

NSP: Network Service Provider

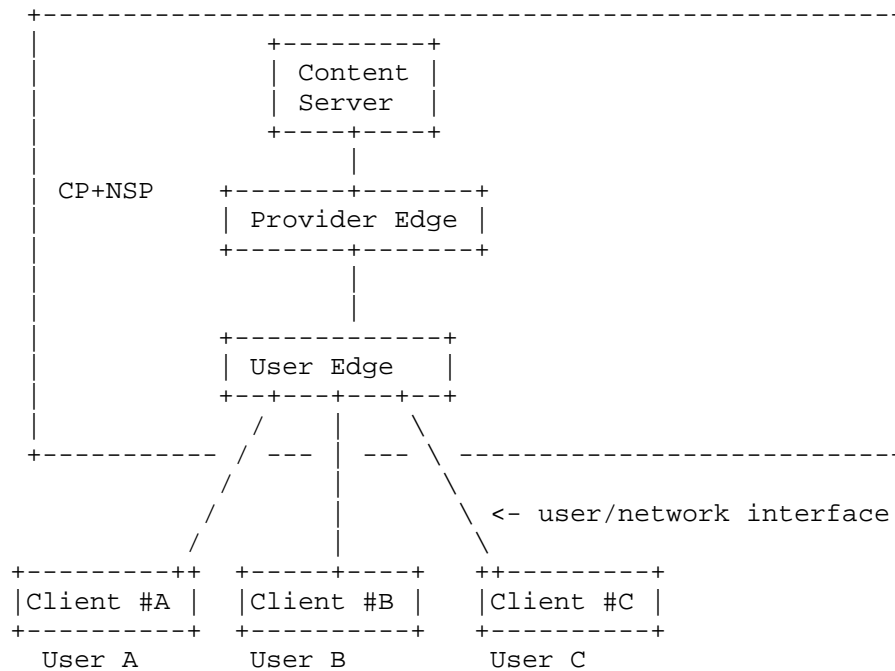
SSM: Source Specific Multicast

QoS: Quality of Service

3. Current Business Models

3.1. Single entity model where CP and NSP are the same entity

One existing business model is that of a single entity responsible for both content and network service provision which bills its users based on content provision. (See figure below.)



Example of CDS network configuration

Figure 1

In this model the network can query a content-policy-enabled AAA server within its own domain at the time a user requests content. The network can provide the AAA server with information such as user identity, device identity, the requested content (channel), geographic information, method of network connection, etc. that might be required for the content provision authorization decision. It is therefore possible to configure a network to deny network access based on the content policy decision.

In this model there are no issues of mapping user identities between different entity domains. The provider has access to the information on which user accessed from which point on what device. Furthermore as network provider they can record not only when a user joined or left a certain channel, but also if packets were actually delivered. Moreover, there are no inter-entity security and privacy concerns between the CP and NSP.

The single entity network service and content provider also knows the content schedules for various channels. This is important not only

for time and content-sensitive authorization decisions but also for providing meaningful billing details to end users.

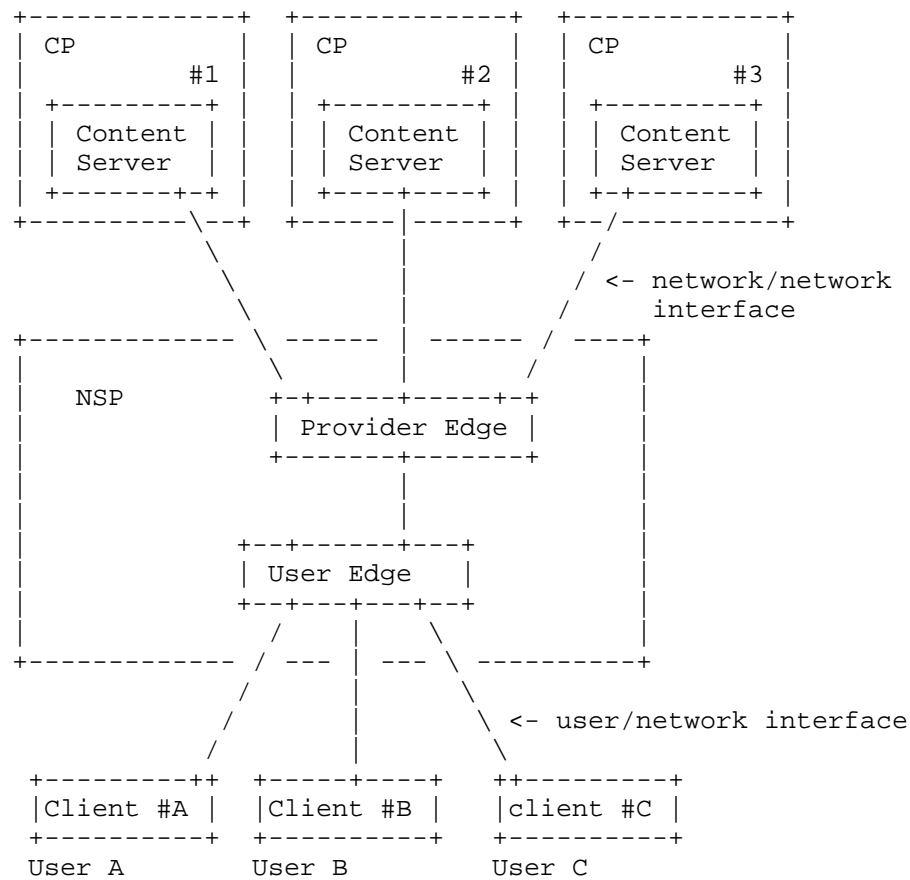
3.2. Multiple entity model without direct content-based billing

An additional model for delivering contents over a CDS is the advertising-based model where billing end-users is not done. In this model the four different roles may be filled by separate entities: Content Provider (CP), Network Service Provider (NSP), user clients, and advertising sponsors. In the general case of this business model, insofar as the advertiser does not require user-based metrics the accounting of content consumption can be anonymous and/or in aggregate and can be off-line from the multicast-with-AAA CDS system itself. Therefore this model does not require any new standards to provide user-based accounting for a multi-entity CDS using multicast with AAA. (Providing this data in near real-time and inline would entail further requirements which can be dealt with in a separate memo if necessary.)

A more complex version of this business model is conceivable in which a CP may require a user to enter into a subscription contract, even when the user does not get billed for content consumption. For example, a CP may value individual data because it allows it to supply the advertisers with rich, user-segmented data and charge a higher premium. In that case the requirements of the next section "CDS with direct billing of the end user" are generally applicable because of the need to link the user data which the CP has to the actual viewing (or stream downloading) data that the NSP has.

4. Proposed Model: Multity-entity CDS

In this model the networks for CDS contain three different types of entities: Content Provider (CP), Network Service Provider (NSP), and user clients. An NSP owns the network resources (infrastructure). It accommodates content providers on one side and accommodates user clients on the other side. NSP provides the network for CDS to two entities (i.e., CPs and user clients). A CP provides content to each user through the network of NSPs and charges users for content. NSPs are responsible for delivering the content to user clients, and for controlling the network resources. A NSP charges a user or a CP for network usage. A NSP may charge users for content as a proxy of the CP.



Example of CDS network configuration

Figure 2

The CP provides detailed channel information (e.g., Time table of each channel) to the information server which is either managed by the NSP or CP. An end-user client gets the information from the information server. In this model, multicasting is used in the NSP's CDS network, and there are two different contracts. One is the contract between the NSP and the user which permits the user to access the basic network resources of the NSP. Another contract is between the CP and user to permit the user to subscribe to 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. A user may want to move to another place, or may want to change her/his device (client) any time without interrupting her/his reception of services.

4.1. Information Required by Entities to Support the Proposed Business Model

User identification and Authentication:

The network should be able to identify and authenticate each user when they attempt to access the service requesting content. This user identification is required for:

- authorization for content consumption eligibility

- user tracking for billing based on actual content consumption and network resource usage

With current protocols (IGMP/MLD), the sender cannot distinguish which receivers (end hosts) are actually receiving the information. 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. Furthermore, the current user associated with receiver must be identified.

User Authorization:

The network, at its option, 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.

Sharing Programming data:

NSP needs a mechanism to receive channel programming data from the CP in order to provide the information to the user at channel selection time and also for somehow logging or recording what programming content has been streamed to the user. In some cases the CP may contract the NSP to bill the user as a proxy for the CP. In this case there needs to be a mechanism for supplying the user-based viewing history with human-meaningful channel data to the end-user.

Content usage information by user:

For billing and auditing purposes the CP needs the NSP to provide it with detailed per-user usage behavior indicating what content was consumed from when to when. There needs to be a mechanism to

supply the user-based viewing history from the NSP to the CP. If the CP is selling on an on-demand model, or tiered subscription basis or supplies some sort of online account statement this history needs to be fed back to the CP in near real-time. To assemble such data on 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.

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). Such information can be used to give meaningful feedback to the user.

5. Admission Control for Multicasting

In order to guarantee certain QoS it is important for network providers (at their option) to be able to protect their network resources from being wasted, (either maliciously or accidentally). The NSP should be able to apply appropriate access controlling actions based on user eligibility status:

The network should be able to apply necessary access controlling actions when an eligible user requests an action (such as a join or a leave.)

The network should be able to reject any action requested from an ineligible user.

In order to maintain a predefined QoS level, depending on the NSP's policy, a user edge should be able to control the number of streams it serves to a user, and total bandwidth consumed to that user. For example if the number of streams being served to a certain user has reached the limit defined by the NSP's policy, then the user edge should not accept a subsequent "join" until one of the existing streams is terminated. Similarly, if the NSP is controlling by per-user bandwidth consumption, then a subsequent "join" should not be accepted if delivery of the requested stream would push the consumed bandwidth over the NSP policy-defined limit.

The network may need to control the combined bandwidth for all channels at the physical port of the edge router or switch so that these given physical entities are not overflowed with traffic. This entails being able to control the number of channels delivered, the

bandwidth for each channel and the combined bandwidth for all channels.

6. Reauthorization/ deauthorization requirements

A mechanism for periodic reauthorization of users who have already joined a channel stream should be supported. The reauthorization could be an authorization check based on the NSP's eligibility requirements and/or could involve the NSP querying the CP for reauthorization of a user.

A mechanism for deauthorization should be supported for cases in which a user is deemed ineligible by the NSP and/or CP at the time of a reauthorization check. If a NSP revokes authorization for the network for a user it should force a leave, and record details of the leave (including the time and reason for the forced leave.) If a CP revokes authorization to content for a user the CP signals to the NSP to cease streaming to that user. An example usage case for deauthorizing a user is one where a user has a subscription or has paid for a certain amount of content and has reached that limit. In some models, it is conceivable that a CP could communicate the parameters for de-authorization to the NSP at the time of the original join's authorization so as to make NSP->CP reauthorization requests unnecessary.

7. Performance requirements

Channel Join Latency and Leave Latency

Commercial implementations of IP multicasting are likely to have strict requirements in terms of user experience. Join latency is the time between when a user sends a "join" request and when the requested data streaming first reaches the user. Leave latency is the time between when a user sends a "leave" signal and when the network stops streaming to the user. Leave and Join latencies impact the acceptable user experience for fast channel surfing. In an IP-TV application, users are not going to be receptive to a slow response time when changing channels. If there are policies for controlling the number of simultaneous streams a user may access then channel surfing will be determined by the join and leave latencies. Furthermore, leave affects 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 channels 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.

8. Concomitant requirements

Scalability

Solutions that are used for AAA and QoS enabled IP multicasting should scale enough to support the needs of content providers and network operators. NSP's multicast access and QoS policies should be manageable for large scale users. (e.g. millions of users, thousands of edge-routers)

Service and Terminal Portability:

Depending on the service, networks should allow for a user to receive a service from different places and/or with a different terminal device.

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.

Support of ASM and SSM

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

Support for Tunneled Multicast

The AAA requirements specified in this document should apply to both end-to-end native multicast and to tunnel-enabled multicast, such as AMT multicast: [I-D.ietf-mboned-auto-multicast]

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. When a CP requires the NSP to provide a level of QoS

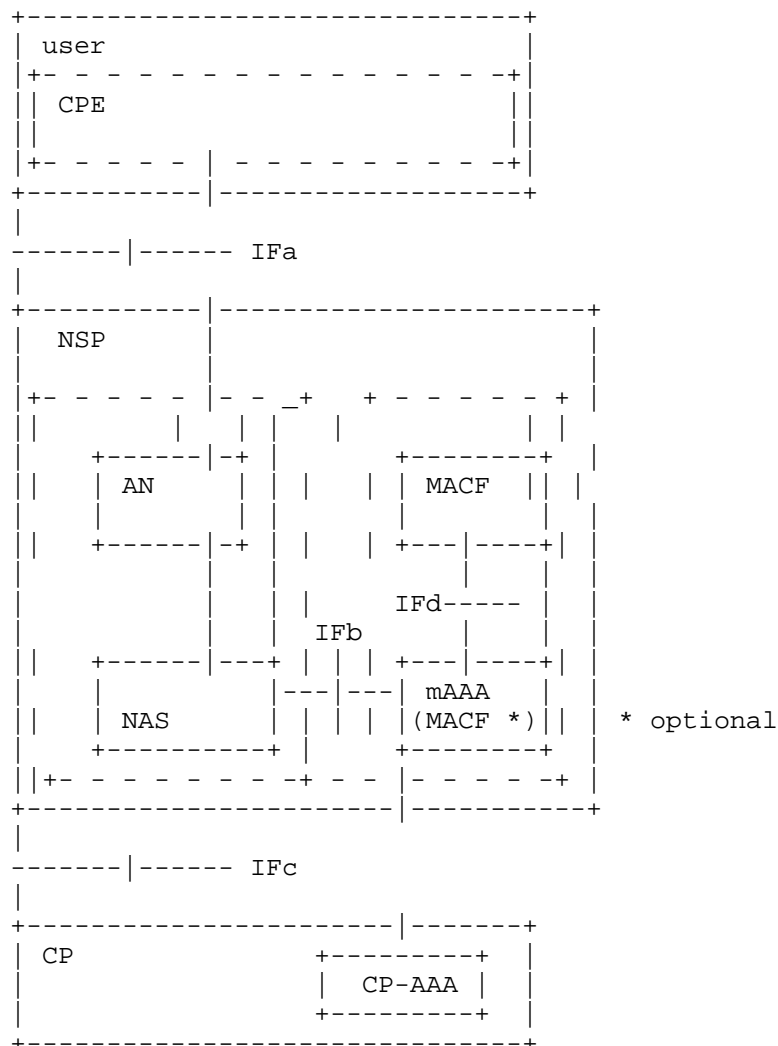
surpassing "best effort" delivery or to provide special services (e.g., to limited users with specific attributes), certain parameters of the CDS may be defined by a contractual relation between the NSP and the CP. However, just as for best-effort unicast, multicast allows for content sourced by CPs without a contractual relation with the NSP. Therefore, solutions addressing the requirements defined in this memo should not make obsolete multicasting that does not include AAA features. NSPs may offer tiered services, with higher QoS, accounting, authentication, etc., depending on contractual relation with the CPs. It is therefore important that Multicast AAA and QoS functions be as modular and flexible as possible.

Multicast Replication

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

9. Constituent Logical Functional Components

Below is a diagram of a AAA enabled multicasting network, including the logical components within the various entities.



AAA enabled multicasting network with admission control

Figure 3

The user entity includes the CPE (Customer Premise Equipment) which connects the receiver (s).

The NSP (Network Service Provider) includes the transport system and a logical element for multicast AAA functionality. The TS (transport system) is comprised of the access node and NAS (Network Access Server) An AN (Access Node) may be connected directly to mAAA or a

NAS relays AAA information between an AN and a mAAA. Descriptions of AN and its interfaces are out of the scope for this memo. The multicast AAA function may be provided by a mAAA which may include the function that downloads Join access control lists to the NAS (this function is referred to as the conditional access policy control function.)

Interface between mAAA and NAS

The interface between mAAA and the NAS is labeled IFb in Figure 3. Over IFb the NAS sends an access request to the NSP-mAAA and the mAAA replies. The mAAA may push conditional access policy to the NAS.

CP-AAA

The content provider may have its own AAA server which has the authority over access policy for its contents.

Interface between user and NSP

The interface between the user and the NSP is labeled IFa in Figure 3. Over IFa the user makes a multicasting request to the NSP. The NSP may in return forward multicast traffic depending on the NSP and CP's policy decisions.

Interface between NSP and CP

The interface between the NSP and CP is labeled IFc. Over IFc the NSP requests to the CP-AAA for access to contents and the CP replies. CP may also send conditional access policy over this interface for AAA-proxying.

The NSP may also include a component that provides network resource management (e.g. QoS management), as described in section 5, "Admission Control for Multicasting". Resource management and admission control is provided by MACF (Multicast Admission Control Function). This means that, before replying to the user's multicast request, the mAAA queries the MACF for a network resource access decision over the interface IFd. The MACF is responsible for allocating network resources for forwarding multicast traffic. MACF also receives Leave information from NAS so that MACF releases corresponding reserved resources.

10. Acknowledgments

The authors of this draft would like to express their appreciation to Christian Jacquenet of France Telecom whose contributions to the "AAA

Framework for Multicasting" [draft-ietf-mboned-multiaaaa-framework] largely influenced this draft; Pekka Savola of Netcore Ltd.; Daniel Alvarez, and Toerless Eckert of Cisco Systems; Sam Sambasivan of AT&T; Sanjay Wadhwa, Greg Shepherd, and Leonard Giuliano of Juniper; Tom Anschutz and Steven Wright of BellSouth; Nicolai Leymann of T-Systems; Bill Atwood of Concordia University; Carlos Garcia Braschi of Telefonica Empresas; Mark Altom, Andy Huang, Tom Imburgia, Han Nguyen, Doug Nortz of ATT Labs; Marshall Eubanks in his role as mboned WG chair; Ron Bonica in his role as Director as the Operations and Management Area; Stephen Rife of Digital Garage and David Meyer in his former role as mboned WG chair as well as their thanks to the participants of the MBONED WG in general.

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

11. IANA Considerations

This memo does not raise any IANA consideration issues.

12. Security Considerations

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

These requirements are not meant to address encryption issues. Any solution meeting these requirements should allow for the implementation of encryption such as MSEC on the multicast data.

13. Privacy considerations

Any solution which meets these requirements should weigh the benefits of user-based accounting with the privacy considerations of the user. For example solutions are encouraged when applicable to consider encryption of the content data between the content provider and the user in such a way that the Network Provider does not know the contents of the channel.

14. Conclusion

This memo describes general requirements for providing AAA and QoS enabled IP multicasting services in multi-entity models. A few models are evaluated with regard to their support by current technologies. The "multi-entity CDS with direct billing of the end

user" model is presented and requirements for information sharing between entities and requirements for admission control to enable guaranteeing of QoS are derived. Performance requirements and concomitant requirements are also presented.

15. References

15.1. Normative References

- [RFC2975] Aboba, B., Arkko, J., and D. Harrington, "Introduction to Accounting Management", RFC 2975, October 2000.
- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

15.2. Informative References

- [I-D.ietf-mboned-auto-multicast]
Thaler, D., Talwar, M., Aggarwal, A., Vicisano, L., and T. Pusateri, "Automatic IP Multicast Without Explicit Tunnels (AMT)", draft-ietf-mboned-auto-multicast-09 (work in progress), June 2008.

Authors' Addresses

Tsunemasa Hayashi
Nippon Telegraph and Telephone Corporation
1-1 Hikarino'oka
Yokosuka-shi, Kanagawa 239-0847
Japan

Phone: +81 46 859 8790
Email: hayashi.tsunemasa@lab.ntt.co.jp

Hiroaki Satou
Nippon Telegraph and Telephone Corporation
3-9-11 Midoricho
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 4683
Email: satou.hiroaki@lab.ntt.co.jp

Hiroshi Ohta
Nippon Telegraph and Telephone Corporation
3-9-11 Midoricho
Musashino-shi, Tokyo 180-8585
Japan

Phone: +81 422 59 3617
Email: ohta.hiroshi@lab.ntt.co.jp

Haixiang He
Nortel
600 Technology Park Drive
Billerica, MA 01801
USA

Phone: +1 978 288 7482
Email: haixiang@nortel.com

Susheela Vaidya
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408 525 1952
Email: svaidya@cisco.com

Copyright and License Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

