Hiroaki Satou, NTT
Internet Draft **Hiroshi Ohta, NTT**
Expires: Jan 10, 2008 **Christian Jacquenet, France Telecom**
Intended status: Informational Tsunemasa Hayashi, NTT
Haixiang He, Nortel Networks

July 9, 2007

AAA Framework for Multicasting
<draft-ietf-mboned-multiaaa-framework-04.txt>

Status of this Memo

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

This Internet-Draft will expire on January 10, 2008.

Copyright Notice

Abstract

IP multicast-based services, such as TV broadcasting or videoconferencing raise the issue of making sure that potential customers are fully entitled to access the corresponding contents. There is indeed a need for service and content providers to identify (if not authenticate, especially within the context of enforcing electronic payment schemes) and to invoice such customers in a reliable and efficient manner. This memo describes the framework for specifying the Authorization, Authentication and Accounting (AAA) capabilities that could be activated within the context of the deployment and the operation of IP multicast-based services. This framework addresses the requirements presented in draft-ietf-mboned-maccnt-req-04.txt, "Requirements for Accounting, Authentication and Authorization in Well Managed IP Multicasting Services". The memo provides a basic AAA enabled model as well as an extended fully enabled model with resource and admission control coordination.

1. Introduction

1.1 Purpose and Background

IP multicasting is designed to serve cases of group communication schemes of any kind, such as 1-to-n (case of TV broadcasting services for example) or n-to-p (case of videoconferencing services, for example).

In these environments, IP multicast provides a better resource optimization than using a unicast transmission scheme, where data need to be replicated as many times as there are receivers. Activation of IP multicast capabilities in networks yields the establishment and the maintenance of multicast distribution trees that are receiver-initiated by nature: multicast-formatted data are forwarded to receivers who explicitly request them.

IP multicast-based services, such as TV broadcasting or videoconferencing raise the issue of making sure that potential customers are fully entitled to access the corresponding contents.
There is indeed a need for service and content providers to identify (if not authenticate, especially within the context of enforcing electronic payment schemes) and to invoice such customers in a reliable and efficient manner.
Solutions should consider a wide range of possible content delivery applications: content delivered over the multicast network may include video, audio, images, games, software and information such as financial data, etc.

This memo describes a framework for specifying the Authorization, Authentication and Accounting (AAA) capabilities that could be activated within the context of the deployment and the operation of IP multicast-based services. This memo also describes a framework to realize high-quality multicast transport using a Resource and Admission Control System (RACS) with multicast Authorization.
Specifically, this framework addresses the requirements presented in draft-ietf-mboned-maccnt-req-04.txt, "Requirements for Accounting, Authentication and Authorization in Well Managed IP Multicasting Services" MACCNT-REQ-draft describes the requirements in CDN services using IP multicast[1]. The requirements are derived from:

- need for user tracking and billing capabilities
- need for network access control to satisfy the requirements of the Network Service Provider (NSP) and/or content access control to satisfy the requirements of the Content Provider (CP)

- methods for sharing information between the network service provider and content provider to make it possible to fulfill the above two requirements.

Detailed requirements are presented in MACCNT-REQ-draft. These requirements include mechanisms for recording end-user requests and provider responses for content-delivery, sharing user information (possibly anonymously depending on the trust model) between content provider and network service provider, and protecting resources through the prevention of network and content access by unauthorized users, as well as other AAA related requirements.

The purpose of this memo is to provide a generalized framework for specifying multicast-inferred AAA capabilities that can meet these requirements. This framework is to provide a basis for future work of investigating the applicability of existing AAA protocols to provide these AAA capabilities in IP multicast specific context and/or if deemed necessary, the refining or defining of protocols to provide these capabilities.

2. Definitions and Abbreviations

2.1 Definitions

For the purpose of this memo the following definitions apply:

Accounting: The set of capabilities that allow the retrieval of a set of statistical data that can be defined on a per customer and/or a per service basis, within the context of the deployment of multicast-based services. Such data are retrieved for billing purposes, and can be retrieved on a regular basis or upon unsolicited requests. Such data include (but are not necessarily limited to) the volume of multicast-formatted data that have been forwarded to the receiver over a given period of time, the volume of multicast-formatted data that have been exchanged between a receiver (or set of) and a given source over a given period of time (e.g. the duration of a multicast session), etc.

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

Authorization: The set of capabilities that need to be activated to make sure a given requesting customer is (1)

what he claims to be (identification purposes), and (2) is fully entitled to access a set of services (authentication purposes).

Receiver: an end-host or end-client which receives content. A receiver may be identified by a network ID such as MAC address or IP address.

User: a human with a user account. A user may possibly use multiple reception devices. Multiple users may use the same reception device.

Note: The definition of a receiver (device) and a user (human) should not be confused.

2.2 Abbreviations

For the purpose of this draft the following abbreviations apply:

ACL: Access Control List

AN: Access Node

CAPCF: Conditional Access Policy Control Function

CDN: Content Delivery Network

CDS: Content Delivery Services

CP: Content Provider

CPE: Customer Premise Equipment

mRACF: Multicast Resource and Admission Control Function

NSP: Network Service Provider

TS: Transport System

3. Common use models and network architecture implications

In some cases a single entity may design and be responsible for a system that covers the various common high-level requirements of a multicasting system such as 1) content serving, 2) the infrastructure to multicast it, 3) network and content access control mechanisms. In many cases however the content provision and network provision roles

are divided between separate entities. The MACCNT-REQ-

draft provides more detail of the multiple versus single entity CDS network models.

As such it should not be assumed that the entity responsible for the multicasting structure and the entity responsible for content serving are the same. Indeed because the infrastructure for multicasting is expensive and many content holders are not likely to be competent at building and maintaining complicated infrastructures necessary for multicasting, many content holders would prefer to purchase transport and management services from a network service provider and thus share the infrastructure costs with other content holders.

Similarly network service providers in many cases do not specialize in providing content and are unlikely to build and maintain such a resource-intensive system without a certain level of demand from content holders.

The use model of a single NSP providing multicasting services to multiple CPs the following general requirements from MACCNT-REQ-draft apply:

-Need for user tracking and billing capabilities
-Need for QoS control such as resource management and admission control
-Need for conditional content access control satisfactory to the requirements of the CP
-Methods for sharing information between the NSP and CP to make the above two possible

When the NSP and CP are the same single entity the general requirements are as follows.

-Need for user tracking and user-billing capabilities
-Need for access control and/or content protection at level the entity deems appropriate

4. Framework and Roles of Entities

4.1 Framework for multicast AAA

A general high-level framework can be represented as follows.

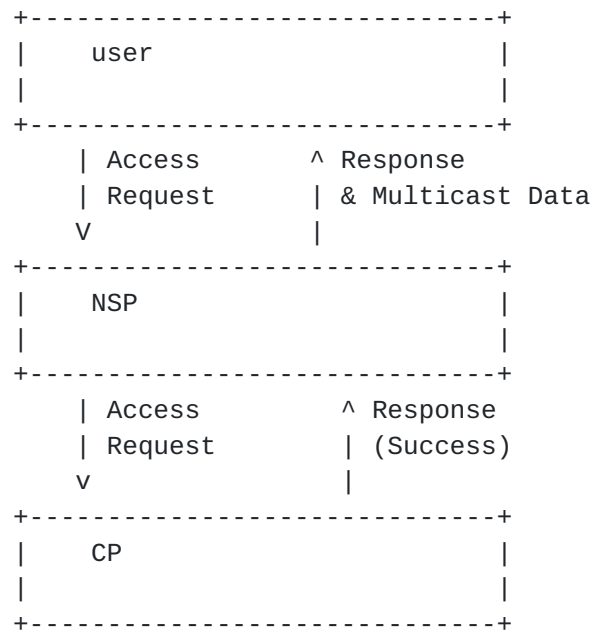

Figure 1

For the sake of simplicity, the above diagram portrays a case where there is a single NSP entity and a single CP entity, but multiple CPs can be connected to the same NSP. It is also possible for the same CP to be connected to multiple NSP networks (e.g. network selection). In other words the relationship of NSP:CP can be described as 1:1, 1:N or M:N. Furthermore it is possible that the NSP and CP could be the same entity.

Description of Roles:

The user (or the user's device) selects a CP and a NSP when the user requests content. The NSP may be automatically selected by a user terminal: e.g. a fixed line NSP for STB or a mobile NSP for mobile phone. In some usage cases it is possible that the NSP used by the user terminal will not always be the same. For example a user may have contracted with different NSPs for fixed line or mobile roaming access.

The CP is responsible for Authentication and Authorization of users' access to content that the CP manages. The CP hopes to collect accounting information related to the access of their content. The CP may choose to authenticate and authorize NSPs which are eligible to provide users access to its contents. When the CP cannot (e.g. error or resource issues) or decides not (e.g. policy issues) to deliver content, the CP is responsible for notifying the NSP of the reason. It is up to the NSP how to relay or translate the messages to the user.

The NSP is responsible for managing its network resources. The NSP may perform admission control. It is also responsible for relaying the AAA messages from the CP whether the user is eligible to receive content (authentication by proxy), and the NSP's relevant AAA server will allow access to the network and contents conditional to both the CP AAA server's content authorization result and the NSPs network utilization authorization result. In certain cases the CP and NSP may have a contractual relationship in which the NSP is authorized to make the content authorization decision based on mutually predetermined criteria: in such cases the NSP-AAA may also make the content authorization decision without querying the CP-AAA. When the NSP cannot or decides not to multicast to users, the NSP may notify the users of the reason. It is recommended that the NSP notify eligible users of the reason for not multicasting content when it is due network or content unavailability, for example. The NSP may choose not to notify ineligible users of the reason for any case.

4.2 Multiple User IDs

Users may hold multiple user IDs: IDs which have been separately assigned for each subscription they may have for various NSPs and CPs. The NSPs and CPs control the user IDs for their respective domains. The user IDs are only meaningful in the context of each domain.

When the user wants to access content, the user registers the corresponding user ID (including its CP domain information) with a request for content, etc: web authentication is one possible method.

Each CP may identify users by the user IDs that it has issued to them.

Terminal portability can be realized if the NSP authenticates a user using a NSP-assigned user ID. A NSP-assigned user ID is an access-line independent unique ID assigned to users which allows user identification from any access point within the network and possibly roaming to other networks. This allows the user to access the content from various network access points.

The NSP and CP do not need to know the corresponding user

id for the same user in the other provider's domain, and it

is not necessary that there is a one to one relationship. It is quite possible for one person to hold multiple user ids for the same provider.

The actual mapping rules for NSPs and CPs to map user IDs with the IDs in other provider domains is a matter for the providers. A solution should provide an API between the providers to flexibly support various mapping methods.

4.3 Accounting

MACCNT-REQ-draft defines requirements for Accounting and Billing. These include the requirement for the NSP to log user behavior such as the join action and the leave action, as well as the result of the access-control decision. (MACCNT-REQ-draft, 4.5) MACCNT-REQ-draft also specifies that there should be a standardized way to sharing with the CP the user behavior and content reception information which the NSP is logging.(MACCNT-REQ-draft, 4.5.1) Standardization of the logs or messages to share content usage information is important to support a single NSP sharing accounting information with multiple CPs or a single CP receiving from multiple NSPs.

In order to provide the granularity of user-behavior and actual content reception information as specified in MACCNT-REQ-draft, the NSP should not manage multicast states on a subnet basis, but on a user basis (see in MACCNT-REQ-draft, 4.1 "User identification") because the NSP needs to be able to notify the CP of a user's start and stop times for accounting purposes. This means that the NSP sends to the CP AAA an indication for Join and Leave on a user basis. User-based multicast state management is equivalent to explicit membership tracking in RFC3376 and per-host tracking in RFC3810.

This framework specifies an accounting API provided by the NSP and accessed by the CP to allow for sharing user-behavior and content-reception information between the NSP AAA and CP AAA. This accounting API should be configurable to allow the CP to request only the logging information it actually requires. Such an API would allow for realtime accounting information sharing by the NSP to the CP. When logging information is shared through the accounting API, it is important that the CP be able to match the user as described in the database operated by the NSP to the user as described in the database operated by the CP.

The NSP requires the capability to log both user and host information for each join and leave, indicating the

corresponding multicast source for each action. When either a CP source stops sending, or the NSP stops multicasting, in an unsolicited manner, there is also a need to notify the AAA servers accordingly about the users who are impacted by this event.

Also, intermittent logs between the join and leave would allow for finer diagnostics and therefore could serve useful in billing discrepancies, and provide for a better estimation of the time span that content was multicasted in the even that users disconnect without sending leave messages.

4.4 Access Control and CP selection by NSP

When a NSP receives an access request from a user, it is necessary for the NSP to determine to which CP the request is to be directed. It is necessary for the NSP to ensure that it is not spoofed by an inappropriate CP or user.

4.5 API for Admission Control Information by NSP

After authorizing a user request, the NSP may have further conditions for determining its admission control decision. MACCNT-REQ-draft defines requirements for providing the network capability to conduct admission control based on the network bandwidth usage status and bandwidth management policy. (MACCNT-REQ-draft, 4.2.2, 4.2.3 & 4.9) Such QoS measurement and policy mechanisms themselves are out of the scope of this memo. However the NSP's AAA Server should be provided with an Admission control API that allows for interfacing so that additional conditions can be added to the admission control decision.

4.6 Access Control and Distinguishing of Users by CP

The user ID and authentication information are forwarded transparently by the NSP so that the CP can distinguish the user, as well as authenticate and authorize the request.

4.7 Caching of AAA results

An NSP should be able to cache AAA results based upon an agreement between the NSP and a CP. The AAA cache would store information about permissions of a specific user to

receive multicast data from specified channel(s) up to specified expiration date(s) and time(s).
If such caching is implemented, a method must exist for the CP to communicate this permission information to the NSP. The NSP refers to the AAA cache and if the cache indicates that the user has permission to receive multicast data from a specific channel at that time, the NSP may forward the data without querying the CP.

It should be possible for a CP to send unsolicited requests to the NSP to refresh or change the permissions for a user for specific channel(s).

When a user is receiving multicast content and the permission is about to expire, the NSP may send a notification to the user client that his session is about to expire, and that he will need to re-connect. The user will have to reestablish a connection. In the case that the user still has permission to the content, they should be able to continue to receive the content without interruption.

5. Network Connection Model and Functional Components

Section 3.1 introduces the high-level AAA framework for multicasting. This section provides more detail on the network connection model and constituent functional components.

5.1 Basic Connection Model

In the simple case represented in Figure 1 the NSP is the sole entity providing network resources including network access to the User. First a user that requests content sends an Access request to an NSP which then forwards it on to the appropriate CP for Authentication and Authorization purposes. The CP responds with either "success" or "failure". If "success", the NSP may forward a success response and stream multicast data to the user.

In this model the user selects the NSP to which to send its content request. Based on this request the NSP selects an appropriate CP to which it forwards the request. The CP responds to the NSP's request: it may not respond to another NSP in regards to the request.

In this model, as described in section 3.1, the

relationship between NSP and CP can be 1:1, 1:N or M:N.

Users may connect to multiple networks, and networks have multiple users.

5.2 Constituent Logical Functional Components of the fully enabled AAA Framework

MACCNT-REQ-draft defined requirements for "well managed" multicasting which this memo calls "AAA enabled" multicasting. "Fully enabled AAA" multicasting in this memo means "AAA enabled" with added QoS functions.

Section 3.1 introduces the high-level AAA framework for multicasting. Below is a diagram of a AAA enabled multicasting network with AAA, including the logical components within the various entities.

AAA enabled framework (basic model)

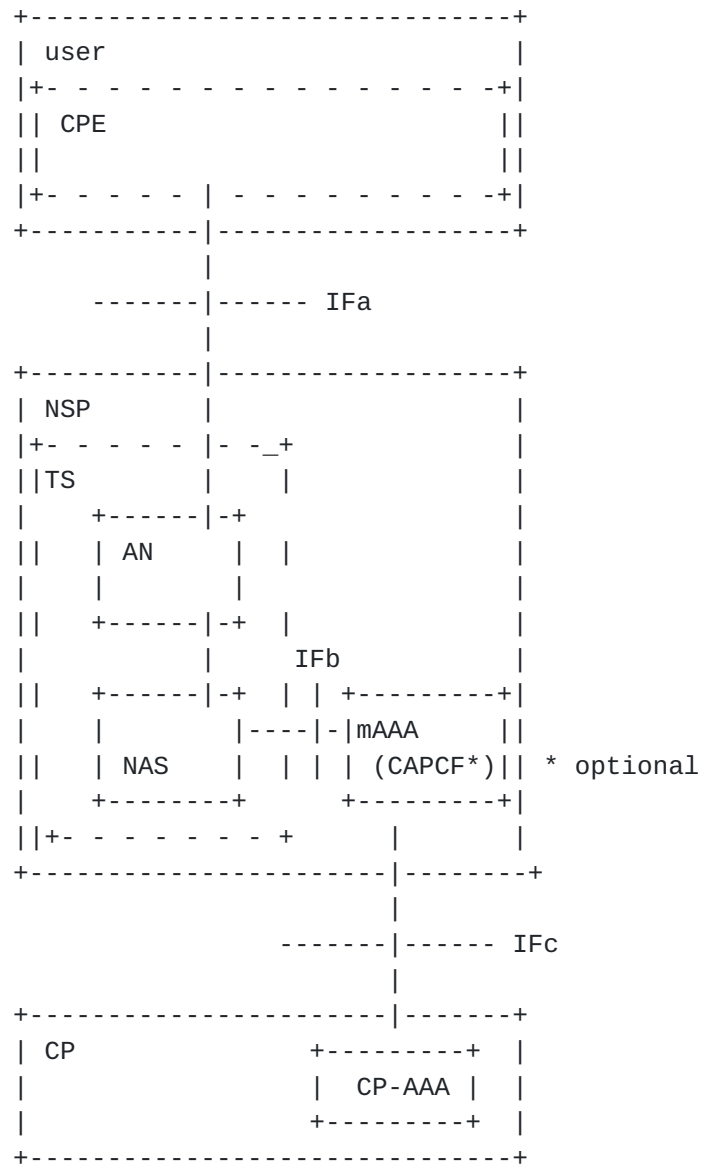

Figure 2

The user entity includes the CPE (Customer Premise Equipment) which includes the user host(s) and optionally a multicast proxy (not shown in the Figure 2.)

The NSP (Network Service Provider) in the basic model includes the transport system and a logical element for multicast AAA functionality. The transport system is comprised of the access node and NAS (network access server.) Descriptions of AN and its interfaces are out of scope for this memo. The multicast AAA function may be provided by a multicast AAA server (mAAA) which may include a function by which the access policy is downloaded to the NAS (conditional access policy control function.) The interface between mAAA and NAS is labeled IFb in Figure 2. Over IFb the NAS makes an access request to the NSP-mAAA and the mAAA replies. The mAAA may push conditional access policy to the NAS.

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

The interface between the user and the NSP is labeled IFa in Figure 2. Over IFa the user makes a multicasting request to the NSP. The NSP may in reply send multicast traffic depending on the NSP and CP's policy decisions.

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-caching.

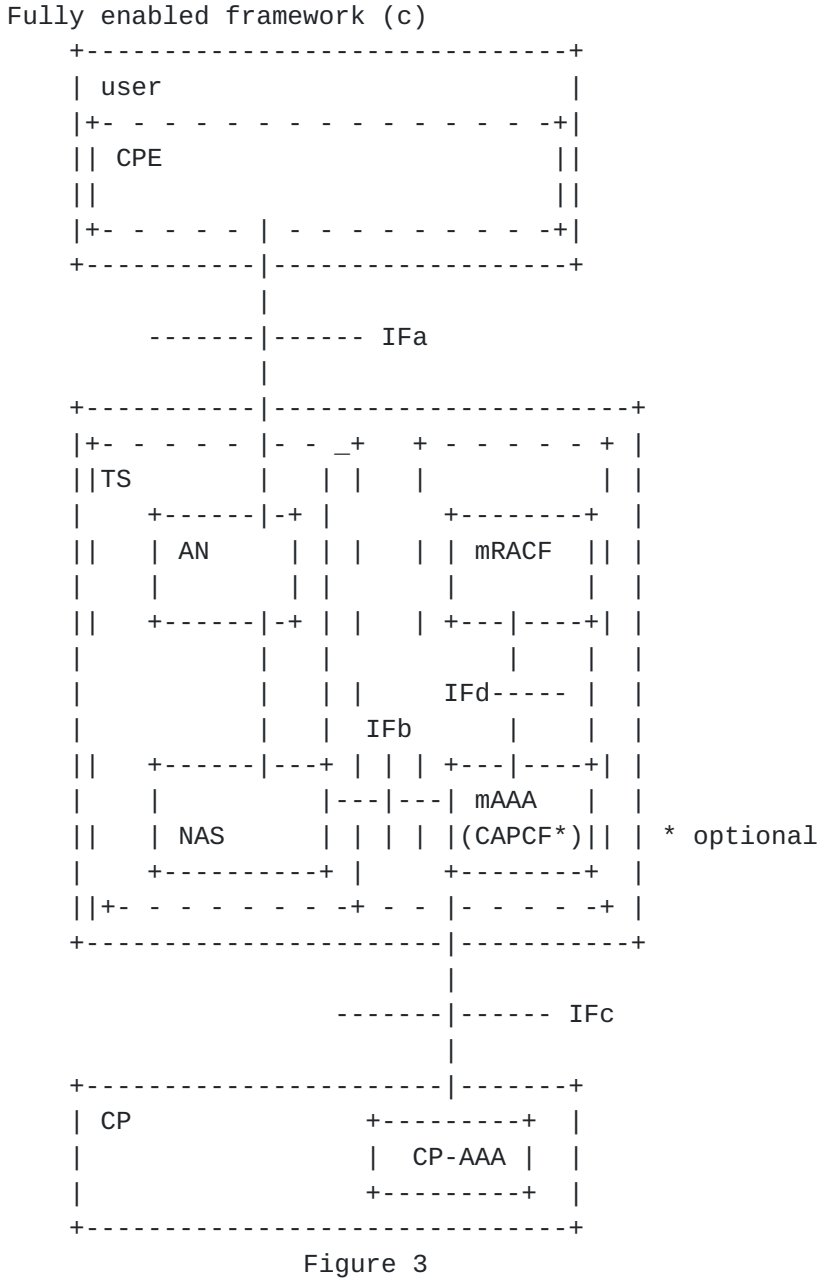

Figure 3

In the fully enabled model the NSP also includes a component that provides network resource management (e.g. QoS management), as described in section 3.4, "Network Resource Management by NSP". In the fully enabled model (Figure 3) resource management and admission control is provided by mRACF (multicast resource and admission control function.) This means that mRACF and Authorization portion of mAAA comprise RACS. Before replying to the user's multicast request the mAAA queries the mRACF for a network

resource access decision over the interface IFd. The mRACF is responsible for allocating network resources for multicast traffic. So that mRACF has the necessary network resource

availability information, NAS notifies mRACF via mAAA of the stopping of multicast traffic.

5.3 Modularity of the framework

In the interest of flexibility, this framework is modular so that it is possible that partially enabled versions of the models are supported. A AAA-enabled version provides AAA functionality without Network Resource management. A Network-Resource-Management-enabled (QoS-enabled) version provides Network Resource management without AAA functionality. Similarly, the possibility of one or more layers of transit provision between an NSP and CP is in the interest of modularity and extendibility.

6. IANA considerations

This memo does not raise any IANA consideration issues.

7. Security considerations

Refer to section 3.3. Also the user information related to authentication with the CP must be protected in some way. Otherwise, this memo does not raise any new security issues which are not already addressed by the original protocols. Enhancement of multicast access control capabilities should enhance security performance.

8. Conclusion

This memo provides a generalized framework for solution standards to meet the requirements presented in MACCNT-REQ-draft. Further work should be done to specify the interfaces between the user and NSP, NAS and mAAA, mAAA and mRACF and NSP-mAAA and CP-AAA (presented in 5.2.)

Normative References

[1] Hayashi, et. al., "Accounting, Authentication and Authorization Issues in Well Managed IP Multicasting Services", draft-ietf-mboned-maccnt-req-04.txt, February 2006, Work in Progress.

[2] RFC-3810, Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", June 2004.

[3] RFC-3376, Cain B., et.al., "Internet Group Management Protocol, Version 3", October 2002.

Authors' Addresses

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

Christian Jacquenet
France Telecom
3, avenue Francois Chateau
CS 36901, 35069 Rennes Cedex, France
Phone: +33 2 99 87 63 31
Email: christian.jacquenet@francetelecom.com

Tsunemasa Hayashi
NTT Network Innovation Laboratories
1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847
Japan
Phone: +81 46 859 8790
Email: tsunemasa@gmail.com

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

Comments

Comments are solicited and should be addressed to the mboned working group's mailing list at mboned@lists.uoregon.edu_and/or the authors.

Full Copyright Statement

Intellectual Property

Expiration

This Internet-Draft will expire on January 10, 2008.

Acknowledgement

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