mboned   T. Hayashi
Internet-Draft   NTT Network Innovation
Intended status: Informational   Laboratories
Expires: February 5, 2010   H. He
                                                       Nortel
                                                     H. Satou
                                                      H. Ohta
                                  NTT Network Service Systems
                                                 Laboratories
                                                 C. Jacquenet
                                               France Telecom
                                               August 4, 2009

AAA and Admission Control Framework for Multicasting
draft-ietf-mboned-multiaaa-framework-10

Status of this Memo

   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/1id-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 5, 2010.

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
users (if not authenticate, especially within the context of
enforcing electronic payment schemes) and to retrieve statistical
information for accounting purposes, as far as content and network
usage are concerned. 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 "Requirements for
Accounting, Authentication and Authorization in Well Managed IP
Multicasting Services" [I-D.ietf-mboned-maccnt-req]. The memo
provides a basic AAA enabled model as well as an extended fully
enabled model with resource and admission control coordination.

Table of Contents

1. Introduction

1.1. Purpose and Background

   IP multicasting is designed to serve cases of group communication
   schemes of any kind, such as one-to-many (case of TV broadcasting
   services for example) or many-to- many (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 Multicast Admission
   Control Function (MACF) with multicast Authorization.

   Specifically, this framework addresses the requirements presented in
   "Requirements for Multicast AAA coordinated between Content
   Provider(s) and Network Service Provider(s)" which describes the
   requirements in CDN services using IP multicast. 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. [I-D.mboned-maccnt- req]

Detailed requirements are presented in "Requirements for Accounting,
Authentication and Authorization in Well Managed IP Multicasting
Services" [I-D.ietf-mboned-maccnt-req]. 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 an authenticated user is fully entitled to access a
set of services.

Join: Signaling mechanism used by receivers to indicate they want
to access a multicast group and receive the corresponding traffic.

Leave: Signaling mechanism used by receivers to indicate they want to leave a multicast group and not receive the corresponding traffic anymore.

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:

AAA: Authentication.Authorization.and Accounting

ACL: Access Control List

AN: Access Node

CDN: Content Delivery Network

CDS: Content Delivery Services

CP: Content Provider

CP-AAA: Authentication, Authorization, and Accounting functions used by a Content Provider

CPE: Customer Premise Equipment

ID: Identifier

IF: network interface

mAAA: Authentication, Authorization, and Accounting functions activated in multicast-enabled environments

MACF: Multicast Admission Control Function

NAS: Network Access Server (RFC2881)

NSP: Network Service Provider

        NSP-mAAA: Authentication, Authorization, and Accounting functions
        used by a Network Service provider

        QoS: Quality of Service

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. Commonly, Content
    Providers (CP) do not build and maintain their own multicast network
    infrastructure as this is not their primary business area. CP often
    purchase transport and management services from network service
    providers instead. Similarly Network Service Providers (NSP) may not
    make their business in providing content. [I-D.mboned- maccnt-req]
    provides more detail of the multiple versus single-entity Content
    Delivery Service (CDS) network models.

    In the usage model where a single NSP provides multicast services to
    multiple CPs, the following general requirements from [I-D.ietf-
    mboned-maccnt-req] apply:

        Need for user tracking and billing capabilities

        Need for QoS control such as resource management and admission
        control

        Need for conditional multicast 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 then 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](#). **AAA Framework in Multicast-Enabled Environments**

   A general high-level framework is depicted in Figure 1.

```
            +-------------------------------+
            |     user                      |
            |                               |
            +-------------------------------+
                          |
                          |
                          |
            +-------------------------------+
            |     NSP                       |
            |                               |
            +-------------------------------+
                          |
                          |
                          |
            +-------------------------------+
            |     CP                        |
            |                               |
            +-------------------------------+
```
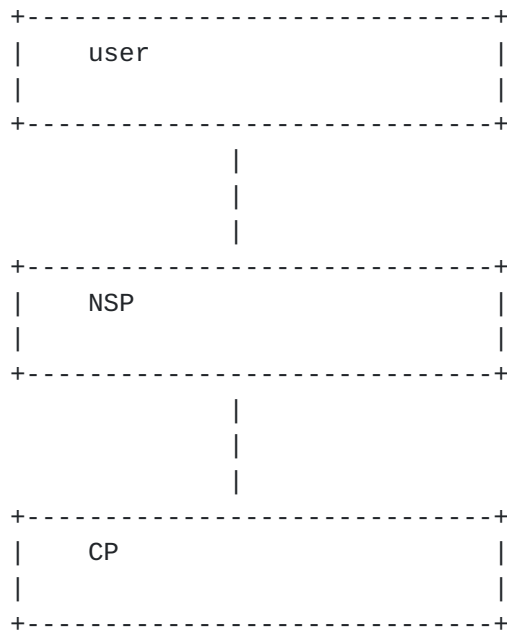
   Figure 1: High-level AAA framework in Multicast-Enabled Environments

                            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 (one-to-one
   model), but multiple CPs can be connected to a single NSP (e.g. NSP
   may provide connections to multiple CPs to provide a wide selection
   of content categories: one-to-many model) It is also possible for a
   single CP to be connected to multiple NSP networks (e.g. network
   selection). Furthermore it is possible that the NSP and CP could be
   the same entity. A NSP and CP authenticate and authorize each other
   when they establish connectivity. Below the general case of multiple
   NSPs with multiple CPs is explained. Then, the various combinations
   of single and multiple CPs and NSPs are described in relation to the
   general case.

[4.1.1](#). **Multiple CPs are connected to multiple NSPs**

   The user subscribes to multiple NSPs and multiple CPs in this usage
   case. The user 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 by a set top box or a mobile NSP by a mobile
phone. In some usage cases it is possible that the NSP used by a
certain user will not always be the same. For example a user may
have contracted with more than one NSP: one for fixed line access and
another for mobile roaming access.

The content may be associated with (or managed by) a specific CP. In
this case, when the user selects content, the CP is automatically
selected.

Requests for multicast sent by the user to a selected NSP should
include enough information not only for authentication by the CP but
also for CP selection and admission control by the NSP.

When an NSP receives a request for multicast from a user, the NSP
requests the appropriate CP to make sure that the user is entitled to
access the corresponding content As the NSP is responsible for
managing its network resources, the NSP may perform admission
control.The NSP will allow access to the multicast service, depending
on both the response sent by the CP and the availability of resources
operated by the NSP. That is, the NSP will forward multicast traffic
towards the user only when the NSP has 1) made sure the user is
entitled to access the network resources operated by the NSP, 2)
received a confirmation from the CP that the user is entitled to
access the content and (possibly) 3) determined that the network
resources (e.g. bandwidth) are sufficient to deliver the multicast
traffic to the user with the relevant level of quality. When neither
of the first two conditions are met, the NSP will not forward
multicast traffic to the user. Condition #3 may also be a
showstopper. When the NSP already knows that network resources are
insufficient or there is a network failure, the NSP may choose to not
request the CP about the user's ability to retrieve content. The NSP
is also responsible for notifiying the user whether he/she is
eligible to receive content depending on the response sent by the CP.
In cases where the NSP does not start multicasting because of its own
network issues (e.g. lack of network resources or network failure),
the NSP notifies the user with a reason for rejecting the request.

A CP receives an inquiry from the NSP. The CP authenticates the
NSP's identity and makes an authorization decision regarding the
user's eligibility to access the requested contents. The CP is
responsible for the authentication and authorization of users so that
they can access the content managed by the CP. The CP notifies the
NSP accordingly. 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 about the reason. It is up to the
NSP to relay or translate the reasons for rejection to the user.

A CP may delegate AAA responsibility to a NSP. 'AAA proxy in NSP' is
described in 4.7 for this case.

As defined in [I-D.ietf-mboned-maccnt-req], the CP may require the
retrieval of accounting information related to the access of its
content.

4.1.2. Multiple CPs are connected to a single NSP

The user subscribes to a single NSP which provides multicasting from
multiple CPs in this usage case. In this case the user does not
select an NSP. The user selects a CP when the user requests content.
The content may be associated with (or managed by) the specific CP,
so that when the user selects content, the CP is automatically
selected.

The user should send a request for multicast to the specific NSP with
enough information not only for authentication by the CP but also for
CP selection and admission control by the NSP.

The role of the NSP is the same as that described in 4.1.1.

The role of a CP is the same as that described in 4.1.1.

4.1.3. Multiple CPs are connected to a single NSP

In this usage case, a user subscribes to multiple NSPs but only a
single CP. A user selects the NSP when the user requests multicast
but the CP is fixed. The user should send a request for multicast to
the selected NSP with enough information not only for authentication
by the CP but also for admission control by the NSP.

The role of the NSP is similar to the description in 4.1.1, with the
exception that when a NSP receives a request from a user, NSP makes
an inquiry to the CP without CP selection.

The role of the CP is the same as that described in 4.1.1.

4.1.4. A single CP is connected to single NSP

In this case, a user subscribes to only one NSP and one CP. The user
does not select a NSP and CP in this scenario. Requests for
multicast sent by the user to a selected NSP should include enough
information not only for authentication by the CP but also for
admission control by the NSP.

The role for the NSP is the same as 4.1.3 The role of the CP is the
same as the description in 4.1.1.

The NSP and CP could be the same entity. In this case, the roles of
the NSP and CP may be combined.

4.2. User ID

Users may hold multiple user IDs: IDs which have been separately
assigned for each subscription to various NSPs and CPs. The NSPs and
CPs manage the user IDs for their respective domains. A CP
identifies a user by a user ID assigned by the CP itself. A NSP
identifies a user by a user ID assigned by the NSP itself. The user
IDs are only meaningful within the context of each domain. Users may
hold multiple user IDs which have been separately assigned for each
subscription they may have for various NSPs and CPs.

4.2.1. CP-assigned user ID

CPs assign user IDs to their users. The user may have more than one
CP-assigned user ID per specific CP. A user requests multicast to a
NSP, the CP-assigned user ID should be indicated so that the CP can
identify the user requesting content access. A NSP should notify the
CP- assigned user ID to the CP. A NSP should not share a CP-
assigned user ID with any CP except the one which assigned it and
should not relay it at all if there is no appropriate CP that
assigned the user ID.

4.2.2. NSP-assigned user ID

NSPs assign user IDs to their users. A user may have more than one
NSP-assigned user ID per a specific NSP. A user requests for
multicast to a NSP, the NSP-assigned user ID may be indicated in the
request so that the NSP can identify the user. The NSP should not
inform the NSP- assigned user ID to the CP for security reasons. The
NSP may identify the multicast-access user by other methods than the
NSP-assigned userID, e.g. by the access port.

The actual mapping rules for NSP-assigned user IDs with CP- user
assigned IDs in account logs is a matter for the providers and out of
the scope of this framework.

4.3. Accounting

There are some accounting issues specific to multicasting. An (S,G)
should be recorded as a channel identifier. The last hop device,
such as an IGMP or MLD router or an IGMP or MLD proxy, notifies the
NSP's mAAA function of the (S,G) channel identifier. The NSP should
notify the CP of the (S,G) information in the accounting report
messages.

A NSP records an accounting start corresponding to only the first
Join for a specific user-access session. A NSP should not treat a
"Join" response to a Query as the accounting start.

A NSP records an accounting stop triggered by any of the following:
1) a user requested Leave, 2) a timeout of a multicast state or 3) a
re-authentication failure. A NSP may also record an accounting stop
due to network availability reasons such as failure. The NSP logs
the reason for each accounting stop.

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 multicast, in the event that users disconnect
without sending leave messages.

There are two levels of accounting report messaging. Messages in
Accounting level 1 include a channel identifier, a user identifier,
and the accounting start and stop time information. Accounting level
2 includes all information of Level 1, plus traffic volume
information.

QoS class is an optional item for each accounting level. Whether to
send, and at what interval to send intermittent log information is
optional for both levels. CP and NSPs may also agree to include
additional option information in accounting messages of either level.

The level of account report messaging between the NSP and CP may be
either configured statically or can be dynamically requested by the
CP in its response to the Access-Request relayed by the NSP to the
CP. The determination of the actual level of report messaging is
configured by the NSP at the NAS.

In case of very fast channel changes, the amount of items logged by
the NSP could become high. In order to reduce the number of report
messages sent to the CP, the NSP can consolidate multiple sets of
accounting information inside a single accounting report message.

4.4. Access Control and CP selection by NSP

When a NSP receives an access request from a user, the NSP determines
to which CP the request is to be directed. The NSP may select a CP
based on CP-assigned userID with CP domain name or channel identifier
(S,G). The user should include in the request sufficient information
for CP selection.

4.5. Admission Control Information by NSP

   After authorizing a user request, the NSP may have further conditions
   for determining its admission control decision.

   The NSP receives parameters (such as QoS class, required bandwidth,
   burst-size, etc.) of multicast traffic. Such parameters serve as
   information to be considered in the admission control decision. The
   traffic parameters can be communicated as follows:

      A CP may notify a mapping between the channel identifier (S,G) and
      traffic parameters in the Response message when the CP authorizes
      an access request. Such parameters may include required
      bandwidth, burst-size, QoS class downgrade policy, etc.

      A user may indicate in the Request willingness to accept QoS class
      downgrade to best-effort streaming.

      The NSP may maintain a mapping between channel identifier (S,G)
      and traffic parameters in advance, for example pre-configured by
      agreement between the CP and NSP on a per channel (S,G) basis.

   The ultimate admission decision is made by the NSP based on required
   traffic parameters of the requested, and available resources. In a
   case that it cannot guarantee the required network resources for the
   requested multicast traffic, streaming the requested multicast
   traffic as best-effort is optional. The user may indicate in his/her
   Access Request whether he/she will accept best-effort grade streaming
   if guaranteed class is not available. The CP's preference for
   accepting downgrading to best-effort streaming may be either
   configured statically or can be dynamically requested by the CP in
   its response to the Access-Request relayed by the NSP to the CP. In
   the case that it cannot be offered a guaranteed QoS stream, the NSP
   may decide either to decline admission or to stream the requested
   multicast traffic as best-effort. The NSP should not stream best-
   effort traffic if either the user or CP has indicated against best-
   effort provision.

   A NSP's admission control may manage integrated network resources for
   unicast usage, such as VoIP or unicast streaming, and multicast
   usage. Alternatively, it may manage network resources separately for
   unicast and multicast usage. In either ease, AAA and admission
   control framework for multicast usage is independent of unicast
   admission control.

   Such QoS measurement and policy mechanisms themselves depend on NSP
   policies and are out of the scope of this memo.

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. AAA proxy in NSP

   A NSP may act as AAA proxy of a CP based upon an agreement between
   the NSP and the CP. The AAA proxy 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 proxying is implemented, the NSP may receive authorization
   conditions from a CP in advance and statically hold them, or a CP may
   send them dynamically in the Response message. In either case, the
   user has permission to receive multicast traffic and therefore the
   NSP starts the multicasting without querying the CP.

   The CP may send unsolicited requests to the NSP to refresh or change
   the permissions for a user for specific group(s) or channel(s).

   When a user is receiving multicast traffic while 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-
   authenticate. In such a case, the user will have to send the Access-
   Request. In the case that the user still has permission to the
   content, they should be able to continue to receive the multicast
   traffic without interruption.

   When re-authentication fails, the NSP should stop the multicast
   traffic and record accounting stop.

5. Network Connection Model and Functional Components

   Section 3.1 introduced 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**

```
            +------------------------------+
            |     receiver                 |
            |                              |
            +------------------------------+
                 |                ^ Response
                 | Request        |
                 V                |
            +------------------------------+
            |     NSP's network            |
            |                              |
            +------------------------------+
                 |                ^ Response
                 | Request        | (Success)
                 V                |
            +------------------------------+
            |     CP's network             |
            |                              |
            +------------------------------+
```
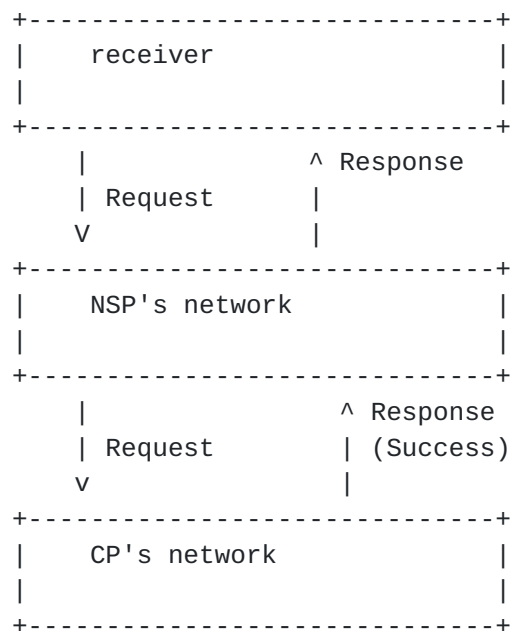
                Figure 2: Basic Connection Model

                          Figure 2

   In the simple case represented in Figure 1 the NSP is the sole entity
   providing network resources including network access to the multicast
   receiver. First a receiver sends a request for multicast (e.g. an
   IGMP Report message) to an NSP which may then forward a mAAA request
   towards the appropriate CP for authentication and authorization
   purposes. The receiver gets information about a given multicast
   group (*,G) or channel (S,G) corresponding to the content beforehand
   for generating the request. The CP responds with either "success" or
   "failure". If "success", the NSP grants access to the receiver and
   forwards multicast traffic accordingly.

   In this model the receiver selects the NSP to which the Join request
   will be sent. Based on this request the NSP selects an appropriate
   CP to which it forwards the corresponding mAAA request. The CP
   responds to the NSP's m AAA request: it may not respond to another
   NSP in regards to the request.

   In this model, as described in section 4.1, the relationship between
   NSP and CP can be one-to-one, one-to- many or many-to-many.
   Receivers may connect to multiple networks.

5.2. **Constituent Logical Functional Components of the fully enabled AAA
     Framework**

   Requirements for "fully AAA and QoS enabled" IP multicasting networks
   were defined in MACCNT-REQ-draft. To allow for levels of enablement,
   this memo defines two models within the framework: "AAA enabled"
   multicasting and "Fully enabled AAA" multicasting which means "AAA
   enabled" with added admission control 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.

```
                +------------------------------+
                | user                         |
                |+- - - - - - - - - - - - - -+|
                || CPE                       ||
                ||                           ||
                |+- - - - - | - - - - - - - -+|
                +----------|-----------------+
                           |
                    -------|------ IFa
                           |
                +----------|-----------------+
                | NSP      |                 |
                |+- - - - -|- -_+            |
                ||TS       |    |            |
                |     +------|-+             |
                ||   | AN    | |             |
                |    |       |---------+     |
                ||   +------|-+ |       |    |
                |          |    IFb    |     |
                ||   +------|-+ | | +---------+|
                |    |        |----|-|mAAA     ||
                ||   | NAS    | | | |(MACF *) || * optional
                |    +--------+     +---------+|
                ||+- - - - - - - +   |        |
                +----------------------|-------+
                                       |
                                -------|------ IFc
                                       |
                +----------------------|-------+
                | CP              +---------+  |
                |                 | CP-AAA |  |
                |                 +---------+  |
                +------------------------------+
```
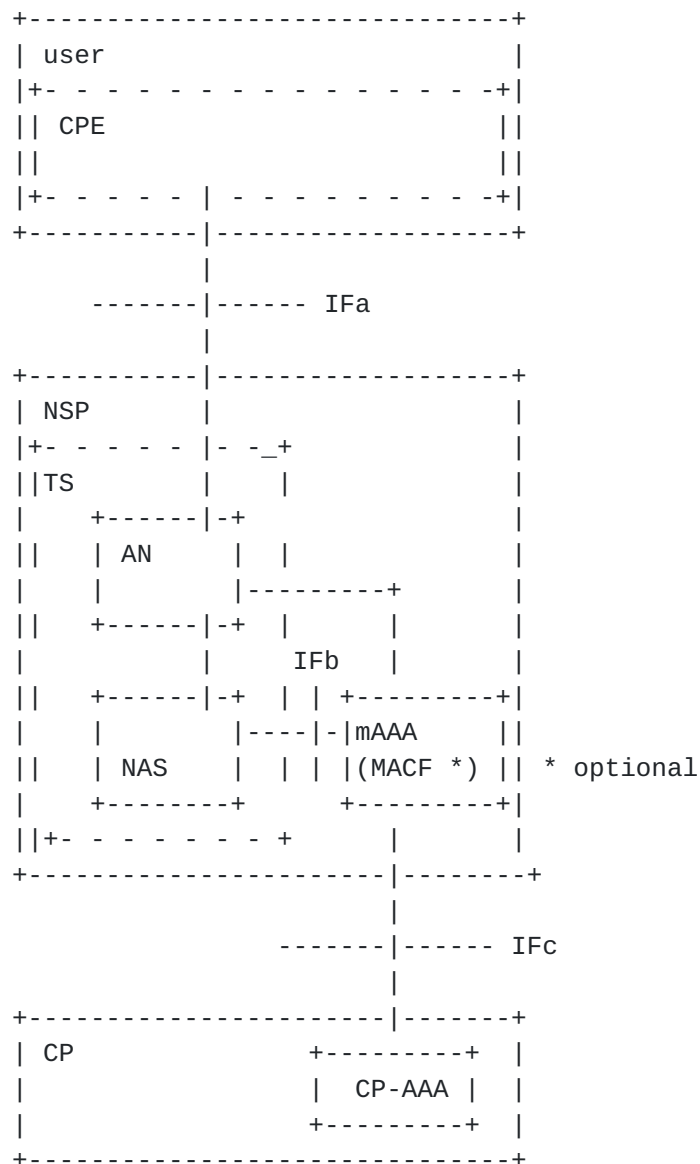
                 Figure 3: AAA enabled framework (basic model)

                                 Figure 3

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

   The NSP (Network Service Provider) in the basic model 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 conditional
access policy control function.)

Interface between mAAA and NAS

The interface between mAAA and the NAS is labeled IFb in Figure 2.
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.

```
        +-------------------------------+
        | user                          |
        |+- - - - - - - - - - - - - -+|
        || CPE                        ||
        ||                            ||
        |+- - - - - | - - - - - - - -+|
        +----------|------------------+
                   |
           -------|------ IFa
                   |
        +----------|---------------------+
        |+- - - - - |- - _+   + - - - - - + |
        ||        |  | |   |          | |
        |    +------|-+ |         +--------+  |
        ||   | AN     | | |   | | MACF  || |
        |    |        | | |       |      | |  |
        ||   +------|-+ | |   | +---|----+| |
        |            |   |       |     | |  |
        |            |   | |     IFd-----  | |
        |            |   | IFb       |    | |  |
        ||   +------|---+ | | | +---|----+| |
        |    |        |---|---| mAAA   | |  |
        ||   | NAS     | | | | |(MACF *)|| | | * optional
        |    +----------+ |     +--------+  |
        ||+- - - - - - - -+ - - |- - - - -+ |
        +----------------------|-----------+
                               |
               -------|------ IFc
                               |
        +----------------------|-------+
        | CP               +---------+  |
        |                  | CP-AAA |  |
        |                  +---------+  |
        +------------------------------+
```

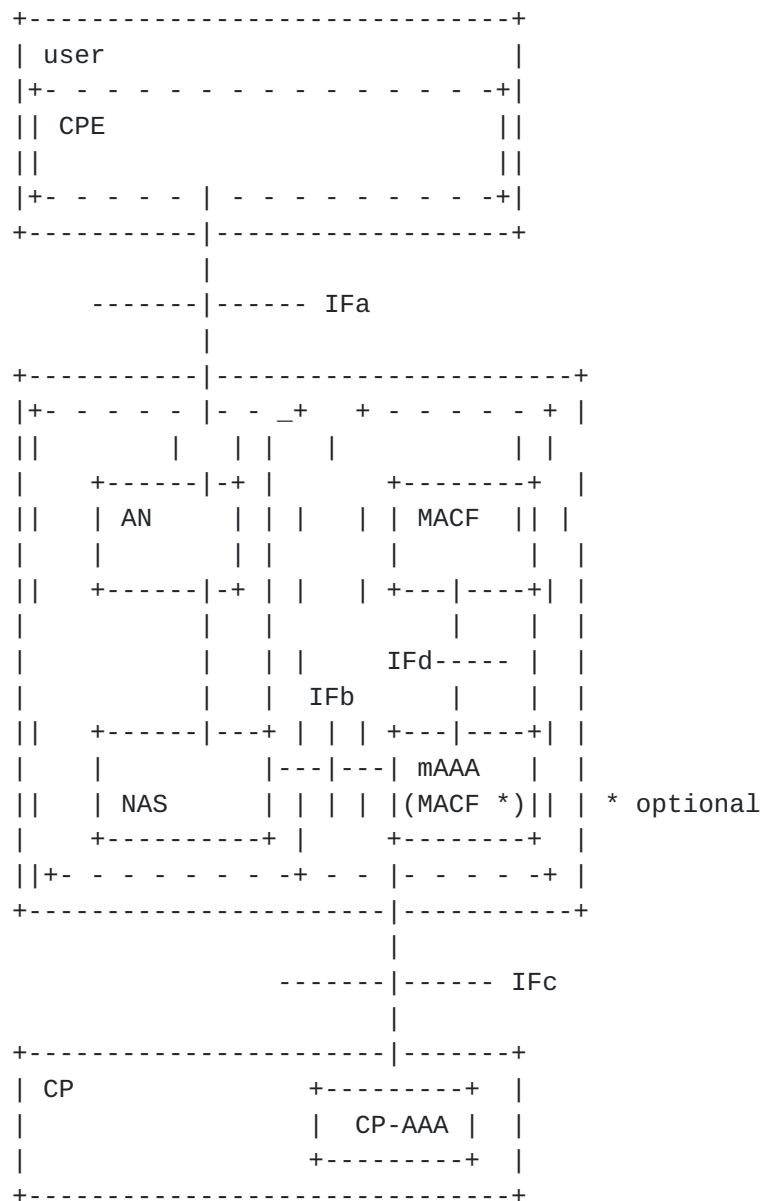   Figure 4: Fully enabled framework

                        Figure 4

   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 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.

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

   The user information related to authentication with the CP and the
   information related to user accounting shared between the NSP and 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. Further work should be done to specify the
   interfaces between the user and NSP, NAS and mAAA, mAAA and MACF and
   NSP-mAAA and CP-AAA (presented in 5.2.)

9. Normative References

   [I-D.ietf-ancp-framework]
              Ooghe, S., Voigt, N., Platnic, M., Haag, T., and S.
              Wadhwa, "Framework and Requirements for an Access Node
              Control Mechanism in Broadband Multi-Service Networks",
              draft-ietf-ancp-framework-11 (work in progress),
              July 2009.

   [I-D.ietf-mboned-maccnt-req]
              Hayashi, T., He, H., Satou, H., Ohta, H., and S. Vaidya,
              "Requirements for Multicast AAA coordinated between
              Content Provider(s) and Network Service Provider(s)",
              draft-ietf-mboned-maccnt-req-08 (work in progress),
              July 2009.

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

Christian Jacquenet
France Telecom
3, avenue Francois Chateau
CS 36901, Rennes Cedex 95134
France

Phone: +33 2 99 87 61 92
Email: christian.jacquenet@orange-ftgroup.com