Hiroaki Satou, NTT

Internet Draft **Hiroshi Ohta, NTT**

Expires: May 17, **Christian Jacquenet, France Telecom**

2008

Tsunemasa Hayashi, NTT

Haixiang He, Nortel Networks

November 19, 2007

AAA Framework for Multicasting

<draft-ietf-mboned-multiaaa-framework-05.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 May 17, 2008.

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-05.txt, "Requirements for Multicast AAA coordinated between Content Provider(s) and Network Service Provider(s)" 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

MACF: Multicast 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:

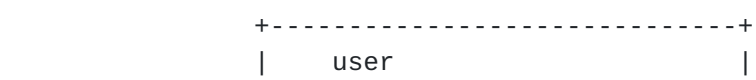
-Need for user tracking and billing capabilities
-Need for QoS control such as resource management and admission control
-Need for conditional content access control satisfactory to the requirements of the CP
-Methods for sharing information between the NSP and CP to make the above two possible

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 Entities4.1 Framework for multicast AAA

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



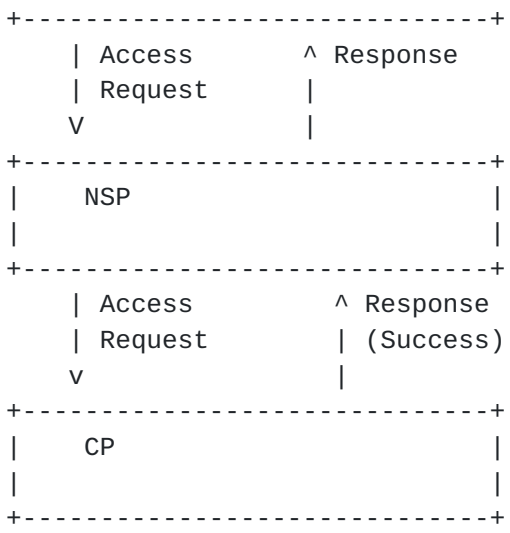


Figure 1

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 a single NSP (e.g. NSP may provide connections to multiple CPs to provide a wide selection of content categories.) 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.

The user should send an Access-Request to the selected NSP with enough information not only for authentication by the

CP but also for CP selection and admission control by the NSP.

When an NSP receives an Access-Request from a user, the NSP selects the appropriate CP for the received Access-Request and relays the content request. As the NSP is responsible for managing its network resources, the NSP may perform admission control.The NSP will allow access to the network and contents conditional to both the CP's content authorization result and the NSPs network availability. That is, the NSP starts multicast flow only when it has both 1) received an accept response from the CP and 2) determined that the network resources (e.g. bandwidth) are sufficient to serve the multicast channel. When neither of these conditions are met, the NSP does not start the requested multicast channel. When the NSP already knows that network resources are insufficient or there is a network failure, the NSP may choose to not relay the Access-Request to the CP. The NSP is also responsible for relaying the Response message from the CP to the user whether the user is eligible to receive content (in response to the corresponding Access-Request from the user to the CP.) In cases that the NSP does not start multicast 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 Access-Request relayed by the NSP. The CP authenticates the NSP s identity and makes an authorization decision regarding the NSP s eligibility to provide users access to its contents. 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 responds to the NSP regarding the relayed Access-Request. 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 reasons for rejection to the user.

4.1.2 Multiple CPs are connected to a single NSP

The user subscribes to a single NSP which provides multicasting of channels 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, when the user selects content, the CP is automatically selected.

The user should send an Access-Request 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 A single CP is connected to multiple NSPs

A user subscribes to multiple NSPs but a single CP in this usage case. A user selects the NSP when the user requests content but the CP is fixed. The user should send an Access-Request 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 an Access-Request from a user, NSP relays it 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 NSP and CP in this scenario. The user should send an Access-Request to the NSP with 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 they may have for 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 CP itself. A NSP identifies a user by a user ID assigned by NSP itself. The user IDs are only meaningful in 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 a specific CP. A user sends an Access-Request 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 relay the CP-assigned user ID from the user to the CP. A NSP should not send a CP-assigned user ID to any CP except the one which assigned it and should not relay it 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 sends an Access-Request to a NSP, the NSP-assigned user ID may be indicated in it so that the NSP can identify the user. The NSP should not relay 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 specific accounting issues for multicasting. A (S,G) should be recorded as a channel identifier. The last hop devices, such as a IGMP or MLD router and a IGMP or MLD proxy, notify a (S,G) to AAA function in the NSP. The (S,G) information should be notified to the CP as part of the accounting log.

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

A NSP records accounting stop triggered by not only user requested Leave but also timeout of a multicast state or 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.

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 finer estimation of the time spent for delivering the content in the event 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, 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 needs to know traffic parameters of a multicast channel for admission control. The traffic parameter information may be either indicated by the user or CP within the access request and responses, or otherwise shared between the NSP and CP outside the access-request message mechanism:

- A user may declare traffic parameters for each Access-Request.
- 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.
- 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 basis.

A NSPs 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 case, 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. The user has permission to receive multicast channel at that time. 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 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 reauthenticate. 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 content without interruption.
When re-authentication fails, the NSP should stop the multicast channel and record accounting stop.

5. Network Connection Model and Functional Components

Section 3.1 introduces the high-level AAA framework for multicasting. This section provides more details 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.

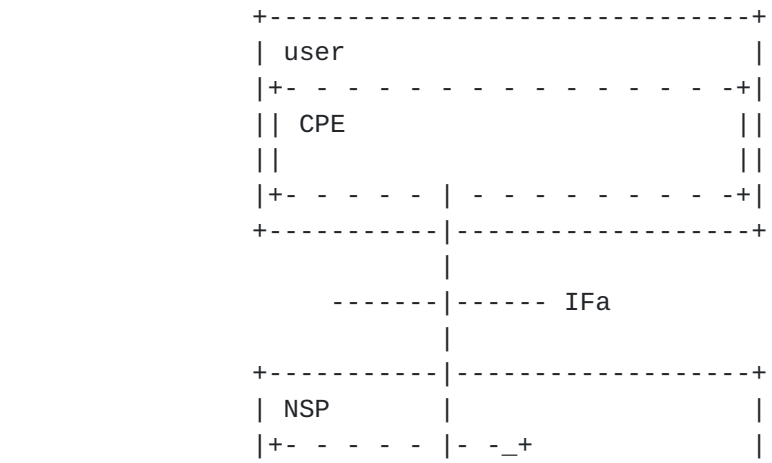
In this model, as described in section 3.1, the relationship between NSP and CP can be 1:1, 1:N or M:N. Users may connect to multiple networks, and networks have multiple users.

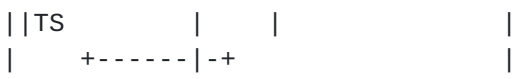
5.2 Constituent Logical Functional Components of the fully enabled AAA Framework

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.

AAA enabled framework (basic model)




||TS
|
|
|
+------|-+
|

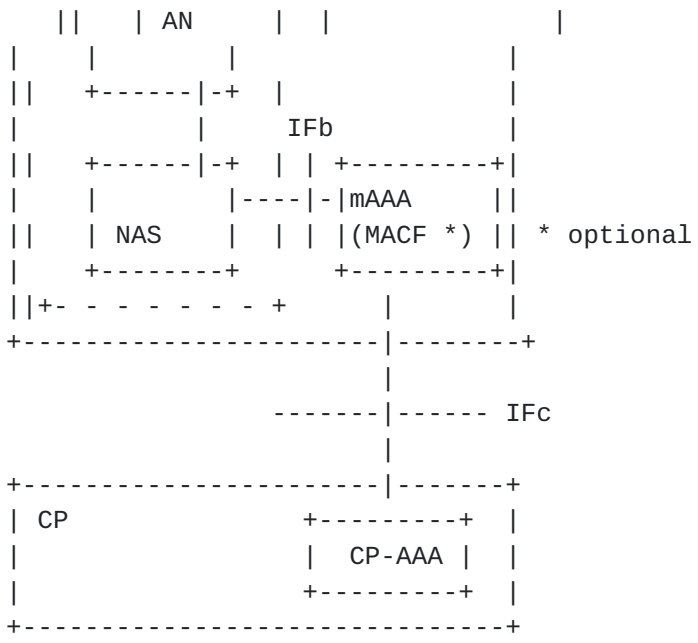


Figure 2

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) An AN 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 scope for this memo. The multicast AAA function may be provided by a multicast AAA server (mAAA) which may include the function by which the access policy is downloaded to the NAS (Multicast access control function.) The interface between mAAA and the 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 within the context of proxying multicast AAA messagescaching.

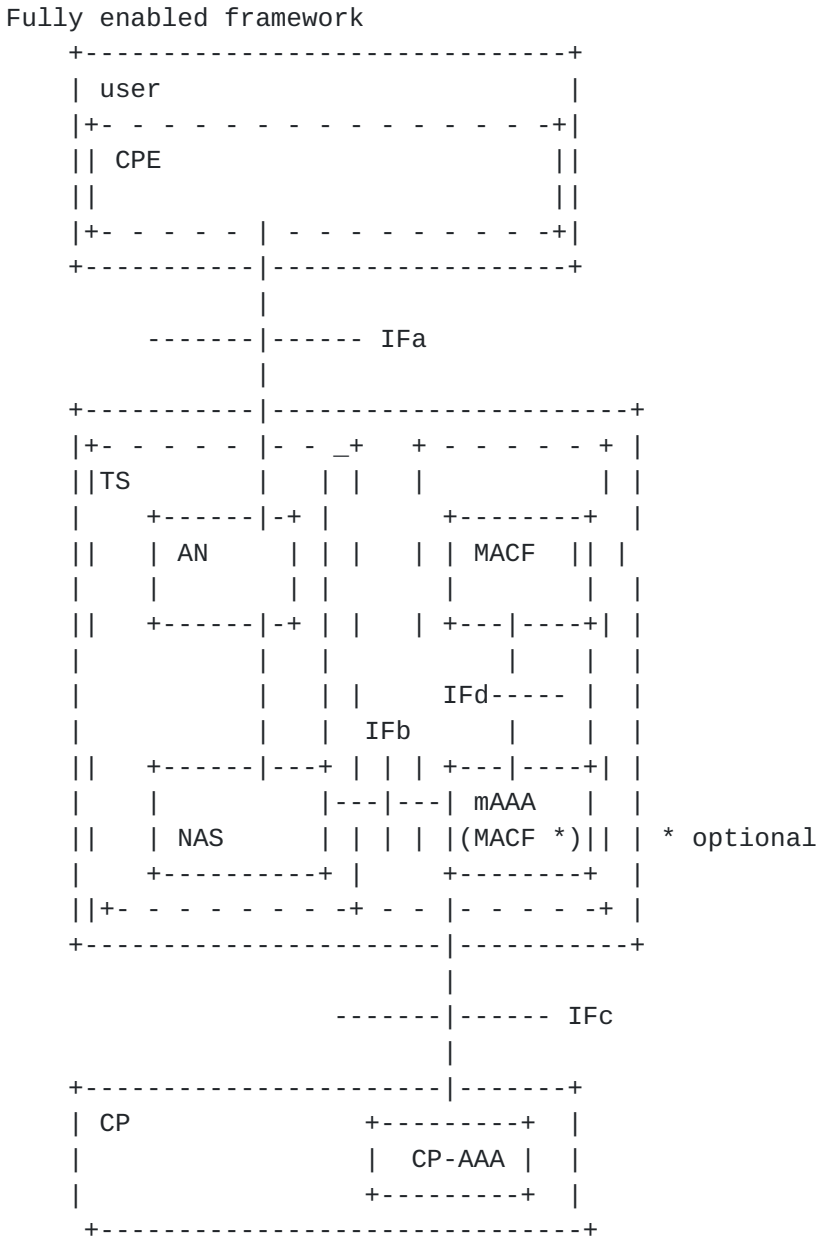


Figure 3

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 MACF (multicast admission control function). 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 multicast traffic. To provide MACF with the relevant network resource

availability information, NAS notifies MACF via mAAA that sending multicast traffic has ceased.

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. An 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. 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.)

Normative References

[1] Hayashi, et. al., Requirements for Multicast AAA coordinated between Content Provider(s) and Network Service Provider(s)", draft-ietf-mboned-maccnt-req-05.txt, September 2007, 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 R&D
4, rue du Clos Courtel -
- BP 91226
35512 Cesson-Sévign ECedex, France
Phone: +33 2 99 12 49 40
Email: christian.jacquenet@orange-ftgroup.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 May 17, 2008.

Acknowledgement

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