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

Internet Draft
Document:draft-ietf-mboned-maccnt-req-06.txt
Intended Status: Informational
Expires: December 22, 2008

June 20, 2008

Requirements for Multicast AAA coordinated between Content Provider(s) and Network Service Provider(s) <draft-ietf-mboned-maccnt-req-06.txt>

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 that Authentication, Accounting and Authorization (AAA) functions are coordinated between Content

Provider(s) and Network Service Provider(s). General requirements for accounting and admission control capabilities including quality-of-service (QoS) related issues are listed. This memo assumes that these capabilities can be realized by functions implemented at edges of a network based on IGMP or MLD. Finally, cases for Content Delivery Services (CDS) are described as application examples which could benefit from multicasting accounting and access control capabilities as described in this memo.

This memo defines requirements related to AAA issues for multi-entity provider models in which the network service provider and content provider cooperate to provide CDS and various related AAA functions for purposes such as protecting and accounting for the access to content and network resources. The requirements are generally not relevant to cases in which there is not a reason to share AAA functions between separate entities.

Table of Contents

1. Introduction

This memo presents general functional requirements related to accounting, access control and admission control issues in IP multicasting networks. A multicast network which fulfills all of these requirements is called a "fully AAA and QoS enabled" IP multicasting network here. Fulfillment of all or some of the requirements will make possible more robust management of IP multicasting networks.

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

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

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

As such, multicasting can be useful to make a network more scalable when a large volume of information needs to be distributed to a large number of receivers. However, multicasting according to current standards (e.g., IGMPv3[1] and MLDv2[2]) has drawbacks compared to unicasting when one applies it to commercial services. Accounting of each user's actions is not possible with multicasting as it is with unicasting. Accounting consists of grasping each user's behavior, when she/he starts/stops to receive a channel, which channel she/he receives, etc.

There are limitations to the application of multicasting in usage models where user-based accounting is necessary, such as is the case with many commercial applications. These limitations have prevented the widespread deployment of multicasting. Development and use of proprietary solutions to address such issues is an alternative to providing standardized solutions. However, non-standard solutions have drawbacks in terms of interoperability or cost of development and maintenance.

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

This memo first describes problems on accounting issues in multicasting. Then the general requirements for this capability including QoS related issues are listed. Finally, application examples which could benefit from multicasting with accounting capabilities are shown.

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. Problem Statement

3.1 Accounting Issues

In unicast communications, the server (information source) can identify the client (information receiver) and only permits connection by an eligible client when this type of access control is necessary. In addition, when necessary, the server can grasp what the client is doing (e.g., connecting to the server, starting reception, what information the client is receiving, terminating reception, disconnecting from the server).

On the other hand, in multicast communication with current standards (e.g., IGMPv3[1] or MLDv2[2]) the server just feeds its information to the multicast router [as in Fig.1]. Then, the multicast router replicates the data to any link which has at least one client requesting the information. In this process, no eligibility check is conducted. Any client can receive information just by requesting it.

It is envisioned that there are many large-scale content distribution applications transferred over IP-based networks that can leverage multicasting technologies to meet their scalability requirements for clients and data volume, and that some of these applications require user-based accounting capabilities similar to available with unicast networks. For example, accounting is needed if one wants to charge for distributed information on a non-flat-fee basis. The current standards do not provide multicasting with authorization or access control capabilities sufficient to meet the requirements of accounting.

```
|--- user ----|------------NSP------------------|-----CP---|

  +--------+
  | user   |\
  +--------+ \
              \+------+    +------+    +------+    +------+
  +--------+   |Multi-|    |Multi-|    |Multi-|    |      |
  | user   |---|cast  |----|cast  |----|cast  |----|Server|
  +--------+   |router|    |router|    |router|    |      |
              /+------+    +------+    +------+    +------+
  +--------+ /
  | user   |/
  +--------+
```

Fig.1 Example network for multicast communication

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

3.2 Relationship with Secure Multicasting (MSEC)

In many cases, content encryption (e.g. MSEC) is an effective method for preventing unauthorized access to original content (in other words, the ability to decode data to return it to its generally usable form.) This memo presents requirements for multicasting networks in the areas of 1) access control to prevent unauthorized usage of network resources (link bandwidth, router's processing power, etc.) , and 2) accounting to grasp user activity in a NSP. The functional requirements do not require content encryption although it might solve some of the content related problems. At this point, it is not yet clear whether encryption would be part of a solution and if so, what other components (if any) would also be required. Multicast streams generally consume large amounts of bandwidth for extended periods of time. Additionally, some multicast streams may have high-priority depending on a NSP's policy. NSP does not want to let ineligible users waste large amounts of bandwidth: for example encryption protects against content viewing but NSP desires protection against DoS attacks of ineligible users wasting network resources, even if it is encrypted. Content encryption and multicast access control should both be able to coexist for more robust security.

3.3 Regarding Access Media and User Separation

The requirements defined in this memo apply to solutions that provide user separation either through physical separation provided by dedicated access media between the user and multicast router (see Fig. 1) or else through logical separation in cases of shared physical access media (e.g. using VLAN). However, IP multicast solutions with shared Layer 2 access media between the user and multicast router and no logical user separation (e.g. Ethernet with shared links and no VLAN) are out of scope of this memo. Nevertheless, some of the requirements in this memo defined for multicasting may also be relevant to multicasting over links without either physical or logical user separation. Therefore in the interest of modularity and flexibility, solutions addressing the requirements of this memo may also take into account application to multicasting without such user separation.

4. General AAA-related Functional Requirements for IP Multicasting

In consideration of the issues presented in section 3, the following requirements have been derived:

(1) User identification

The network should be able to identify each user when they attempt to access the service so that necessary access controlling actions can be applied. Also, it is necessary to identify the user's receiver (e.g. IP address) of each request (e.g., join/leave) for per host tracking purposes.

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.

(2) Issue of Network Resource Protection

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

For comparisons sake, for unicast this issue can be resolved e.g. by using RSVP in some cases.

(2.1) Access control

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.

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

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.

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

If an NSP desires to guarantee a certain level of QoS to CP and the receivers, it is necessary that the NSP be able to control the number of channels delivered from a physical port of an edge router and a switch in cases that there is a limit to the number of packet copies and/or number of channels that can be handled by multicast routers.

For comparisons sake, for unicast this issue can be resolved e.g. by using RSVP in some cases.

(3) User Authentication

The network should be able to authenticate a user.

(4) 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. In the case that the NSP may wish to provide a service based on guaranteed delivery, the NSP would not want to waste its network resources on ineligible users.

(5) Accounting and Billing

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

To assemble such an understanding of 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.

(5.1) How to share user information

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

(6) Notification to Users of the Result of the Join Request

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

(7) Service and Terminal Portability

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

(8) Support of ASM and SSM

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

(9) Admission Control for Join Action

In order to maintain a predefined QoS level, 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.

(10) 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.

(11) 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)

(12) Small Impact on the Existing Products

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

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

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.

(13) Deployable as Alternative to Unicast

IP Multicasting would ideally be available as an alternative to IP unicasting when the "on-demand" nature of unicasting is not required. Therefore interfaces to multicasting should allow for easy integration into CDS systems that support unicasting.

Especially equivalent interfaces for authorization, access control and accounting capabilities should be provided.

(14) Multicast Replication

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

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

5. Application Example and its Specific Requirements

This section shows an application example which could benefit from multicasting. Then, specific functional requirements related to user-based accounting capabilities are derived.

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

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

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

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

5.1.1 Network Model for Multicast Content Delivery Service

As shown in Fig.2, networks for CDS contain three different types of entities: Content Provider (CP), Network Service Provider (NSP), and 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 other entities (i.e., CPs and user clients). A CP provides content to each user through the network of NSPs. NSPs are responsible for delivering the content to user clients, and for controlling the network resources.

```
+-------------+  +-------------+  +-------------+
| CP          |  | CP          |  | CP          |
|          #1 |  |          #2 |  |          #3 |
| +---------+ |  | +---------+ |  | +---------+ |
| | content | |  | | content | |  | | content | |
| | server  | |  | | server  | |  | | server  | |
| +-------+-+ |  | +----+----+ |  | +-+-------+ |
+----------\--+  +------|------+  +--/----------+
            \           |           /
             \          |          / <- network/network
              \         |         /     interface
+------------- \ ------ | ------ / ----+
|               \       |       /      |
|   NSP         +-+-----+-----+-+      |
|               | Provider Edge |      |
|               +-------+-------+      |   +-----------------+
|                       |              |---| Information     |
|                       |              |   | server          |
|             +--+------+---+          |   +-----------------+
|             | User Edge   |          |
|             +--+---+---+--+          |
|               /    |    \            |
+------------- / --- | --- \ ----------+
             /       |      \
            /        |       \ <- user/network interface
           /         |        \
 +---------++  +-----+----+  ++---------+
 |client #a |  |client #b |  |client #c |
 +----------+  +----------+  +----------+
 User A        User B        User C
```

Fig.2 Example of CDS network configuration

The NSP provides the information server for all multicast channels, and a CP gives detailed channel information (e.g., Time table of each channel) to the information server. An end-user client gets the information from the information server. In this model, 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. As such, IP Multicast network should support portability capabilities.

5.1.2 Content Delivery Service Requirements

Below are listed specific requirements to support common business cases/ contractual arrangements for the IP Multicast-based Content Delivery Service.

5.1.2.1 Accounting Requirements

An NSP may have different contractual agreements with various CPs or various legal obligations in different locations. One possible business relationship between a CP and NSP is that of a revenue sharing which could be on a per content/usage-base. A solution should support varied billing and charging methods to satisfy both common legal and business/financial requirements to deploy multicasting services: this requires accurate and near real-time accounting information about the user clients' activity accessing the content services.
The user accessing particular content is represented by the user's activities of joining or leaving the corresponding multicast group/channel (<(*,g)> or (s,g)). In multicast networks, only NSPs can collect joining or leaving activities in real-time through their user edges. The NSPs can transfer the accounting information to related CPs for them to generate user billing information. Existing standard AAA technology may be used to transfer the accounting information.

To match the accounting information with a particular user, the user has to be authenticated. Usually the account information of a user for content access is maintained by the CP. A user may have different user accounts for different CPs.(e.g. user_a@cp#1 and user_b@cp#2) The account is usually in the format of (username, password) so an user can access the content services from anywhere. For example, an user can access the CP from different NSPs.(e.g. a fixed line NSP and a mobile NSP). It should be noted that the user account used for content access can be different from the one used for network access maintained by NSPs.

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

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

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

Any solution addressing the requirements of this memo should consider the Interdomain accounting issues presented in RFC-2975 [3]. It is especially important to consider that the CP and NSP as separate administrative entities can not be assumed to trust one another. The solution should be robust enough to handle packet loss between entity domains and assure for data integrity. In addition any solution should take into consideration common legal or financial requirements requiring confidential archiving of usage data.

5.1.2.2 Authorization Requirements

The NSPs are responsible for delivering content and are generally required to meet certain QoS levels or SLA (service level agreements). For example, video quality is very sensitive to packet loss. So if an NSP --due to limited network resources -- cannot meet quality requirements if it accepts an additional user request, the NSP should reject that user's access request to avoid charging the existing (i.e., already-joined) user for bad services. For example, if an access line is shared by several users, an additional user's join may cause performance degradation for other users. If the incoming user is the first user on a user edge, this will initiate the transmission of data between the provider edge and the user edge and this extra network traffic may cause performance degradation. There may also be policies that do not necessarily give highest priority to the "first-come" users, and these should also be considered.

In order to protect network resources against misuse/malicious access and maintain a QoS level, appropriate admission control function for traffic policing purposes is necessary so that the NSP can accept or reject the request without degrading the QoS beyond the specified level.

5.1.2.3 Authentication Requirements

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

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

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

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

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

This model does not require the following items:

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

- Methods to share user-related information between NSPs and CPs.

```
  +-----------------------------------------------------+
  |              +---------+                            |
  |              | content |                            |
  |              | server  |                            |
  |              +----+----+                            |
  |                   |                                 |
  | CP+NSP    +-------+-------+                         |
  |           | Provider Edge |                         |
  |           +-------+-------+  +--------------------+ |
  |                   |          | Information server | |
  |                   |          +--------------------+ |
  |           +-------------+                           |
  |           | User Edge   |                           |
  |           +--+---+---+--+                           |
  |             /    |    \                             |
  +----------- / --- | --- \ ---------------------------+
              /      |      \
             /       |       \ <- user/network interface
            /        |        \
 +---------++  +-----+----+   ++---------+
 |Client #a |  |client #b |   |client #c |
 +----------+  +----------+   +----------+
   User A    User B     User C
```

Fig.3 Example of CDS network configuration

6. Acknowledgments

The authors of this draft would like to express their appreciation to Pekka Savola of Netcore Ltd., Daniel Alvarez, and Toerless Eckert of Cisco Systems, Sam Sambasivan of AT&T, Sanjay Wadhwa of Juniper, Tom Anschutz and Steven Wright of BellSouth, Nicolai Leymann of T-Systems, Carlos Garcia Braschi of Telefonica Empresas, Marshall Eubanks of Multicast Techno, Stephen Rife of NTT and David Meyer in his 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.

7. IANA Considerations

This memo does not raise any IANA consideration issues.

8. 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.

9. 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.

10. Conclusion

This memo describes general requirements for providing AAA and QoS enabled IP multicasting services. It lists issues related to accounting, authentication, authorization and admission control for multicast content delivery. Content Delivery Services with different business models are cited as the type of application which could benefit from the capabilities of AAA and QoS enabled IP multicasting described in this document.

Normative References

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

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

[3] Aboba B , et. al., "Introduction to Accounting Management", RFC 2975, October 2000.

Authors' Addresses

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

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

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

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

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

Full Copyright Statement

Disclaimer

Intellectual Property

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

Acknowledgement

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