Internet Engineering Task Force
INTERNET-DRAFT

Expire: May, 2002

Haixiang He, Nortel Networks
Brad Cain, Cereva Networks
Thomas Hardjono, Verisign
November, 2001

Upload Authentication Information Using IGMPv3

<draft-he-magma-igmpv3-auth-00.txt>

Status of this Memo

Abstract

This document describes the changes of Internet Group Management Protocol(IGMP) version 3 that enable a host to upload the authentication information to its neighboring multicast routers.

1. Introduction

The Internet Group Management Protocol (IGMP) [1, 2, 3] is used in IPv4 environment to communicate IP multicast group membership subscriptions from a host to its neighboring multicast routers.

The current multicast model allows any host to join the multicast group by issuing IGMP join message. In some scenarios such as

security attack protection, a host's IGMP requests needs to be authenticated before a router triggers the multicast routing protocol. In some other scenarios such as group access control, a host needs to be authorized before it can receive the multicast traffic. Some solutions to these problems require a host to provide authentication information such as access token [4, 5] accompanying its IGMP requests. They also require the host's neighboring routers to periodically query for authentication information and authenticate those IGMP requests before taking related actions about IGMP requests.

This document defines the necessary changes of IGMPv3 to support the use of IGMP to communicate the authentication information, in particular access token.

2. Solution Goal, Approach, and Rationale

The IGMP state records maintained by a multicast router are used to trigger the multicast routing protocol that will cause the multicast traffic being delivered to that router. They are also used to forward the traffic downstream. The goal of a solution that protects the multicast router is to protect the IGMP state records.

To achieve this goal, the IGMP requests should be authenticated. One approach is to require authentication information such as access token accompanying an IGMP request. Once a router receives the request, it will use the authentication information to authenticate the request. And according to the authentication results, it will take appropriate actions to update the IGMP state records.

One simple and easy solution is to authenticate every IGMP request. In another word, this solution requires authentication information accompanying every IGMP request. This solution has some disadvantages. Authentication information is not needed if an IGMP request does not cause any change of the IGMP state records. So the extra authentication information is a waste of the bandwidth usage of network and it is also an extra burden of the host's processing power.

One the router side, there is also some cost of providing authentication. The cost maybe very high. So authentication should be minimized. In some circumstances, it may be tolerable to update the timers associated with the IGMP state records that have already been created without authenticating those IGMP requests for a certain period of time. A solution should provide a router with an option of when to use the authentication.

Based on the rationale above, this document proposes two new IGMPv3 authentication messages, Authentication Query and Authentication Report. These two new message coexist with the current IGMPv3 messages. A host uses the normal IGMPv3 report message to report its interest. When it receives an authentication query, it will reply an authentication report. Besides the normal IGMPv3 query, a router also sends authentication query in some conditions described in section 5.

3. Authentication Message Formats

The new Authentication Messages follow the requirements for normal IGMP message specified in IGMPv3 document [3]. There are two Authentication Messages:

Type Number (hex)	Message Name
0x31	Authentication Membership Query
0x32	Authentication Membership Report

3.1. Authentication Membership Query

The Authentication Membership Queries are sent by multicast router. The format is the same as IGMPv3 query except that the message type field is 0x31 instead of 0x11.

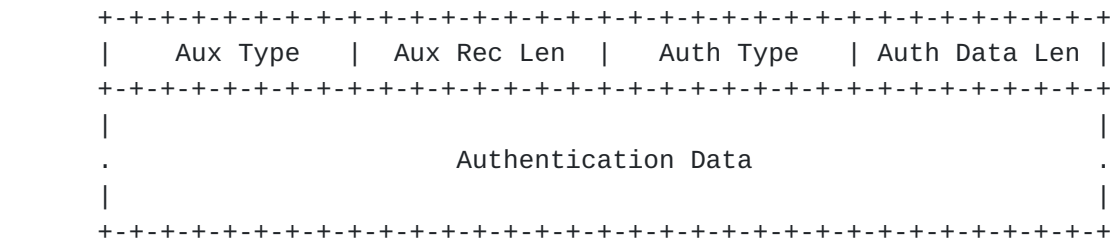
There are also three variants of the Authentication Query message: General Authentication Query, Group-Specific Authentication Query, Group-and-Source-Specific Authentication Query. In a General Authentication Query, both the Group Address field and the Number of Sources (N) field are zero. In a Group-Specific Authentication Query, the Group Address field contains the multicast address of interest, and the Number of Sources (N) field contains zero. In a Group-and-Source-Specific Authentication Query, the Group Address field contains the multicast address of interest, and the Source Address [i] fields contain the source address(es) of interest.

3.2. Authentication Membership Report

The Authentication Membership Reports are sent by IP systems. Besides the message type field which is 0x32 and the changes in Group Record, the format is the same as IGMPv3 report message.

The new Group Record has the following internal format:

where each Auxiliary Data Record has the following internal format:



3.2.1. Aux Type

The Aux Type field unambiguously specifies the type of the Auxiliary Data. This document only specifies one type of Auxiliary Data: Authentication Information, Aux Type = 0x01.

3.2.2. Aux Rec Len

The Aux Rec Len field contains the length of the Auxiliary Data Record, in the units of 32-bits words. The length of the Auxiliary Data Record is not fixed. Besides the Aux Type and Aux Rec Len fields, the rest of the record is interpreted according to the value of the Aux Type field, Authentication Information in this document.

3.2.3. Auth Type

The Auth Type field indicates the authentication mechanism being used.

3.2.4 Auth Data Len

The Auth Data Len field contains the length of the useful Authentication Data.

3.2.5. Authentication Data

The Authentication Data field contains the authentication information as well as extra padding that makes the whole Auxiliary record into the units of 32-bits words.

3.2.6. Record Type

There are only two types of Group Records that may be included in an Authentication Report message. They are all "Current-State Record" as specified in IGMPv3 document. An Authentication Report is only sent by a system in response to an Authentication Query.

4. Host Behavior

A host takes the same actions as described in IGMPv3 document in response to the event: a change of the interface reception state, caused by a local invocation of IPMulticastListen.

A host will receive only General Query, General Authentication Query, Group Specific Authentication Query, Group-and-Source Specific Authentication Query. If all multicast routers in the same networks support this document, a host should not receive Group Specific Query, Group-and-Source Specific Query as described in section 5.

To schedule a response to an Authentication Query, the system must maintain one more state in addition to the three states it has already maintained as described in IGMPv3 document. The new state is:

- A timer per interface for scheduling responses to General Authentication Queries. This timer is identified as Authentication Interface Timer to differentiate itself from interface timer used for scheduling response to General Queries.

The group timer and the source-list are now used to schedule responses to Group Specific Authentication Queries and Group-and-Source Specific Queries. The interface timer is still used to schedule responses to General Queries.

The rules used to determine if a Report needs to be scheduled and the type of Report to schedule are the same as in IGMPv3 document except a few changes. First, new rules are added to process General Authentication Queries. These rules are the same as rules used to process General Queries. Second, rules used process Group Specific and Group-and-Source Specific Queries are instead used to process Group Specific and Group-and-Source Specific Authentication Queries.

When the interface timer expires, a normal Report message is sent. When the Authentication Interface Timer expires, an Authentication Report message is sent. Except the authentication information, this message contains the same information as the normal Report message used to response the General Queries. When the group timer expires, an Authentication Report message is sent. Except the authentication information, the message contains the same information as the normal Report message used to response the Group Specific and Group-and-Source Specific Queries.

5. Router Behavior

Multicast routers maintain the same IGMP group membership state as specified in IGMPv3. They also follow the IGMPv3 Source-Specific forwarding rules. To protect the IGMP state records, routers maintain extra authentication state and there are few changes about the router behavior.

5.1. IGMP Authentication State Maintained by Multicast Routers

Multicast routers maintain a set of authentication state records per attached networks. Each authentication state record conceptually is of the form:

(multicast address, authentication timer)

for group specific authentication state record or of the form:

(multicast address, source address, authentication timer)

for group-and-source specific authentication state record.

Records are created when multicast routers send Authentication Query. And their authentication timers are set to the Last Member Authentication Query Interval (LMAQI). A record is deleted when the authentication timer time out or when an authentication current-state record is received that contains the record's multicast address (and source address in scenarios) before timer time out.

5.2. IGMP Queries

Multicast routers use 4 types of queries: General Query, General Authentication Query, Group Specific Authentication Query, and Group-and-Source Specific Authentication Query. They SHOULD not send Group Specific Query and Group-and-Source Specific Query.

Multicast routers still send General Queries periodically to request group membership information. These queries are used to refresh the group membership state of the systems on attached networks.

Multicast routers also send General Authentication Queries periodically to request group membership information as well as its associated authentication information. These queries are also used to refresh the group membership state. The interval between two General Authentication Queries SHOULD be larger than the interval between two General Queries. When sending a General Authentication Query, routers also create a group specific authentication state record with only multicast address for each IGMP state record. And the record's non zero timers including group and source timers are set to LMAQI.

Multicast routers send Group Specific Authentication Queries when a group record needs to be created, when a group's filter-mode needs to be changed from INCLUDE to EXCLUDE, or when a system is leaving the group. A group specific authentication state record is created using the group record's multicast address.

Multicast routers send Group-and-Source Specific Authentication Queries when traffic from a new source record is needed or a system expresses interest in not receiving traffic from particular sources. A group-and-source specific authentication state record is created using the group record's multicast and source addresses.

5.3. Action on Reception of Reports

If all hosts in a network support this documents, multicast routers SHOULD receive Membership Reports with Current-State records and State-Change records as well as Authentication Membership Reports with only Current-State records.

5.3.1. Reception of Current-State Records

When receiving Current-State records, a router updates the related timers. If a new group state record needs to be created or the group record's filter mode needs to be changed from INCLUDE to EXCLUDE, a router sends a Group Specific Authentication Query. If traffic from a new source is needed, a router sends a Group-and-Source Specific Authentication Query.

The table below describes the modified actions upon reception of Current-State Records. The notation 'AQ(G)" is used to describe a Group Specific Authentication Query to G. The notation 'AQ(G,A)' is used to describe a Group-and-Source Specific Query to G with source-list A. Every time a router send an AQ(G) or AQ(G,A), it creates related authentication state records.

Router State	Report Rec'd	New Router State	Actions
INCLUDE (A)	IS_IN (B)	INCLUDE (A)	(A*B)=GMI Send AQ(G,B-A)
INCLUDE (A)	IS_EX (B)	INCLUDE (A)	Send AQ(G)
EXCLUDE (X,Y)	IS_IN (A)	EXCLUDE (X+(A-Y),Y)	(A-Y)=GMI Send AQ(G,A*Y)
EXCLUDE (X,Y)	IS_EX (A)	EXCLUDE (A-Y,Y)	Send AQ(G,Y-A) (A-X-Y)=GMI Delete (X-A) Group Timer=GMI

5.3.2. Reception of State-Change Records

When receiving State-Change records, a router updates its records and may change its state to reflect the new desired membership state of the network. If some sources are requested to be no longer forwarded to a group, a router sends a Group-and-Source Specific Authentication Query to query sources. It lowers the source timers for those sources to Last Member Query Interval (LMQI). Similarly, when a router sends Group Specific Authentication Query, it lowers the group timer for that group to LMQI.

Also if a new group state record needs to be created or the group record's filter mode needs to be changed from INCLUDE to EXCLUDE, a router sends a Group Specific Authentication Query. If traffic from a new source is needed, a router sends a Group-and-Source Specific Authentication Query.

The table below describes the modified actions upon reception of State-Change Records.

Router State	Report Rec'd	New Router State	Actions
INCLUDE (A)	ALLOW (B)	INCLUDE (A)	(B*A)=GMI Send AQ(G,B-A)
INCLUDE (A)	BLOCK (B)	INCLUDE (A)	Send AQ(G,A*B) (A*B)=LMQI
INCLUDE (A)	TO_EX (B)	INCLUDE (A)	Send AQ(G)
INCLUDE (A)	TO_IN (B)	INCLUDE (A)	(A*B)=GMI Send AQ(G,A-B) (A-B)=LMQI Send AQ(G,B-A)
EXCLUDE (X,Y)	ALLOW (A)	EXCLUDE (X+(A-Y),Y)	(A-Y)=GMI Send AQ(G,A*Y)
EXCLUDE (X,Y)	BLOCK (A)	EXCLUDE (X+(A-Y),Y)	(A-X-Y)=Group Timer Send AQ(G,A-Y)
EXCLUDE (X,Y)	TO_EX (A)	EXCLUDE (A-Y,Y)	Send AQ(G,Y-A) (A-X-Y)=Group Timer Delete (X-A) Send AQ(G,A-Y) Group Timer=GMI

EXCLUDE (X,Y)	TO_IN (A)	EXCLUDE (X+(A-Y),Y)	(A-Y)=GMI Send AQ(G,A*Y) Send AQ(G,X-A) (X-A)=LMQI Send AQ(G) Group Timer=LMQI

5.3.3. Reception of Authentication Current-State Records

When receiving Authentication Current-State records, a router triggers the authentication module through the authentication APIs described in section 7. For each record that is authenticated, the related IGMP state record is updated.

When updating the IGMP state records, a router takes the same actions as the actions a normal IGMP router takes upon reception of Current-State records. The same table is used.

Router State	Report Rec'd	New Router State	Actions
INCLUDE (A)	IS_IN (B)	INCLUDE (A+B)	(B)=GMI
INCLUDE (A)	IS_EX (B)	EXCLUDE (A*B,B-A)	(B-A)=0 Delete (A-B) Group Timer=GMI
EXCLUDE (X,Y)	IS_IN (A)	EXCLUDE (X+A,Y-A)	(A)=GMI
EXCLUDE (X,Y)	IS_EX (A)	EXCLUDE (A-Y,Y*A)	(A-X-Y)=GMI Delete (X-A) Delete (Y-A) Group Timer=GMI

6. Group-and-Source Specific Authentication Information

In some scenarios especially in SSM [6,7], Group-and-Source Specific authentication information is required. Without changing the format and interpretation of the current IGMPv3 report, a group record with a single source address has to be used to upload Group-and-Source Specific authentication information.

But this method does not apply to a group if the group's filter mode is EXCLUDE since a record whose record type is MODE_IS_EXCLUDE cannot be split into multiple records.

7. The API for Authenticating IGMP Requests

Within a router, there is an Application Programming Interface or API that is used by the IGMP module to authenticate the IGMP requests. The API must support the following operation or any logical equivalent:

```
bool IGMPAllowed(multicast-address, source-list, auth record)
```

where the "auth record" contains the authentication information that is in the IGMP request.

8. New Timer

This document introduces one new timer. It is configurable.

8.1. Authentication Query Interval

The Authentication Query Interval is the interval between General Authentication Queries. Default: 300 seconds.

The Authentication Query Interval should be larger than Query Interval since authentication is more expensive and should be used less.

References

[1] Deering, S., "Host Extension for IP Multicasting", RFC 1112, August 1989.
[2] Fenner, W., "Internet Group Management Protocol, Version2", RFC 2236, November 1997.
[3] Cain, B., Deering, S., Fenner, W., Kouvelas, I., Thyagarajan, A., "Internet Group Management Protocol, Version 3", Internet-Draft, January 2001.
[4] He, H., Hardjono, T., and Cain, B., "Simple Multicast Receiver Access Control", Internet-Draft, work in progress.
[5] Hardjono, T. and Cain, B., "Key Establishment for IGMP Authentication in IP Multicast", IEEE European Conference on Universal Multiservice Networks (ECUMN), CERF, Colmar, France, September 2000.
[6] Holbrook, H., and Cain, B., "Using IGMPv3 For Source-Specific Multicast", draft-holbrook-idmr-igmpv3-ssm-01.txt, March 2001.
[7] Holbrook, H., and Cain, B., "Source-Specific Multicast for IP", Internet-Draft, work in Progress.

Author's Address:

Haixiang He
Nortel Networks
600 Technology Park Drive
Billerica, MA 01821
Phone: 978-288-7482
Email: haixiang@nortelnetworks.com

Brad Cain
Cereva Networks
Email: bcain@cereva.com

Thomas Hardjono
Verisign
401 Edgewater Place, Suite 208
Wakefield, MA 01880
Email: thardjono@verisign.com