

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 5, 2011

B. Fenner
AT&T Labs--Research
B. Haberman
Johns Hopkins University Applied
Physics Lab
H. Holbrook
Arastra, Inc.
I. Kouvelas
S. Venaas
cisco Systems
March 4, 2011

Multicast Source Notification of Interest Protocol (MSNIP)
draft-ietf-magma-msnip-06.txt

Abstract

This document discusses the Multicast Source Interest Notification Protocol (MSNIP). MSNIP is an extension to IGMPv3 and MLDv2 that provides membership notification services for sources of multicast traffic operating within the SSM destination address range.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 5, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

Internet-Draft

MSNIP

March 2011

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Routing Protocol Support	4
3.	Service Interface for Requesting Membership Notification . . .	5
3.1.	Application Operation	6
4.	MSNIP Managed Address Range Negotiation	7
4.1.	Router Coordination	7
4.1.1.	MSNIP Operation Option	7
4.1.2.	SSM Range Option	8
4.2.	Managed Range Discovery by Source Systems	8
5.	Requesting and Receiving Notifications	10
5.1.	Host Interest Solicitation	10
5.2.	Router Receiver Membership Reports	11
6.	Application Notification	13
7.	Router Processing	15
8.	Message Formats	17
8.1.	Host Interest Solicitation Message	17
8.2.	Receiver Membership Report Message	18
8.3.	IPv4 Header Fields	19
8.4.	IPv6 Header Fields	19
9.	Constants Timers and Default Values	20
10.	Possible Optimisations	21
10.1.	Suppressing HIS Messages	21
10.2.	Host Stack Filtering	21
10.3.	Responding to Unexpected IGMP Queries	21
10.4.	Host and Router Startup	22
11.	Inter-operation with IGMP / MLD Proxying	23
12.	Security Considerations	24
12.1.	Receiver Membership Report Attacks	24
12.2.	Host Interest Solicitation Attacks	24
12.3.	MSNIP Managed Range Discovery	25
13.	IANA Considerations	26
14.	Acknowledgements	27
15.	References	28

15.1	Normative References	28
15.2	Informative References	28
Appendix A	Extending MSNIP to Any-Source Multicast	30
A.1	Extending MSNIP to ASM with PIM-SM	30
	Authors' Addresses	32

[1](#). Introduction

The Multicast Source Notification of Interest Protocol (MSNIP) is an extension to version 3 of the Internet Group Membership Protocol (IGMPv3 [[RFC3376](#)]) and version 2 of the Multicast Listener Discovery Protocol (MLDv2 [[RFC3810](#)]). MSNIP operates between multicast sources and their first-hop routers to provide information on the presence of receivers to the source systems. Using the services offered by MSNIP an application on an IP system wishing to source multicast data can register to be notified when receivers join and leave the session. This enables multicast sources to avoid the work of transmitting packets onto their first-hop link when there are no joined receivers.

A common scenario where MSNIP may be useful is one where there is a multicast server offering a large pool of potential flows that map onto separate multicast destination addresses but receivers exist only for a small subset of the flows. If the source were to continuously transmit data for all the flows that could potentially have receivers, significant resources would be wasted in the system itself as well as the first-hop link and first-hop router. Using a higher level control protocol to determine the existence of receivers for particular flows may not be practical as there may be many potential receivers in each active session.

Information on which multicast destination addresses have receivers for a particular sender is typically available to the multicast routing protocol on the first hop router for a source. MSNIP uses this information to notify the application in the sending system of when it should start or stop transmitting. This is achieved without any destination address specific state on the first-hop router for potential sources without receivers.

[2.](#) Routing Protocol Support

For reasons described in this section, MSNIP only supports transmission control for applications that use multicast destination addresses that are routed using Source Specific Multicast (SSM). See [Appendix A](#) for information on how MSNIP potentially can be extended to also work with Any-Source Multicast (ASM).

Many currently deployed multicast routing protocols require data from an active source to be propagated past the first-hop router before information on the existence of receivers becomes available on the first-hop. In addition, such protocols require that this activity is repeated periodically to maintain source liveness state on remote routers. All dense-mode protocols fall under this category as well as sparse-mode protocols that use shared trees for source discovery (such as PIM-SM [[RFC4601](#)]). In order to provide receiver interest notification for such protocols, the default mode of operation would require that the source IP system periodically transmits on all potential destination addresses and the first-hop routers prune the traffic back. Such a flood-and-prune behavior on the first-hop link significantly diminishes the benefits of managing source transmission.

In contrast, with source-specific sparse-mode protocols such as PIM-SSM [[RFC4601](#)]) availability of receiver membership information on the first-hop routers is independent of data transmission. Such protocols use an external mechanism for source discovery (like source-specific IGMPv3 membership reports) to build source-specific multicast trees.

Clearly these two classes of routing protocols require different handling for the problem MSNIP is trying to solve. In addition the second type covers the majority of applications that MSNIP is targeted at. MSNIP avoids the extra complication in supporting routing protocols that require a flood and prune behavior.

[3.](#) Service Interface for Requesting Membership Notification

Applications within an IP system that wish to source multicast packets and are interested in being notified on the existence of receivers must register with the IP layer of the system. MSNIP requires that within the IP system, there is (at least conceptually) a service interface that can be used to register with the IP layer for such notifications. Dual stack systems supporting both IPv4 and IPv6 need to provide separate service interfaces for each protocol.

A system's IPv4 or IPv6 service interface must support the following operation or any logical equivalent:

IPMulticastSourceRegister (socket, source-address, multicast-address)

IPMulticastSourceDeregister (socket, source-address, multicast-address)

In addition the application must provide the following interface for receiving notifications from the IP system:

IPMulticastSourceStart (socket, source-address, multicast-address)

IPMulticastSourceStop (socket, source-address, multicast-address)

where:

socket: is an implementation-specific parameter used to distinguish amongst different requesting entities (e.g., programs or processes) within the system; the socket parameter of BSD UNIX system calls is a specific example.

source-address: is the IP unicast source address that the application wishes to use in transmitting data to the specified multicast address. The specified address must be one of the IP addresses associated with the network interfaces of the IP system. Note that an interface in an IP system may be associated with more than one IP address. An implementation may allow a special "unspecified" value to be passed as the source-address parameter, in which case the request would apply to the "primary" IP address of the "primary" or "default" interface of the system (perhaps established by system configuration). If transmission to the same multicast address is desired using more than one source IP address, IPMulticastSourceRegister must be invoked separately for each desired source address.

multicast-address: is the IP multicast destination address to which the request pertains. If the application wishes to transmit data to more than one multicast addresses for a given source address, IPMulticastSourceRegister must be invoked separately for each desired multicast address.

[3.1.](#) Application Operation

Applications wishing to use MSNIP to control their multicast data transmission to destination G from source address S operate as follows.

Initially the application contacts the IP system to obtain the socket handle for use on all subsequent interactions. The application invokes IPMulticastSourceRegister for the desired S and G and then

waits without transmitting any packets for the IP system to notify that receivers for the session exist.

If and when the IP system notifies the application that receivers exist using the `IPMulticastSourceStart` call, the application may start transmitting data. After the application has been notified to send, if all receivers for the session leave, the IP system will notify the application using the `IPMulticastSourceStop` call. At this point the application should stop transmitting data until it is notified again that receivers have joined through another `IPMulticastSourceStart` call.

When the application no longer wishes to transmit data it should invoke the `IPMulticastSourceDeregister` call to let the IP system know that it is no longer interested in notifications for this source and destination. The `IPMulticastSourceDeregister` call should be implicit in the teardown of the associated socket state.

[4.](#) MSNIP Managed Address Range Negotiation

With current multicast deployment in the Internet, different multicast routing protocols coexist and operate under separate parts of the multicast address space. Multicast routers are consistently configured with information that maps specific multicast address ranges to multicast routing protocols. Part of this configuration describes the subset of the address space that is used by source-

specific multicast (SSM) [[RFC5771](#)]. As described in [section 2](#), MSNIP only tries to control application transmission within the SSM address range.

It is desirable for applications within an IP system that supports MSNIP to have a consistent service interface for multicast transmission that does not require the application to be aware of the SSM address range. MSNIP supports this by allowing applications to use the service interface described in [section 3](#) for multicast destination addresses that are outside its operating range. When an application registers for notifications for a destination address that is not managed by MSNIP it is immediately notified to start transmitting. This is equivalent to the default behavior of IP multicast without MSNIP support which forces multicast applications to assume that there are multicast receivers present in the network.

[4.1.](#) Router Coordination

In order for MSNIP to operate on a shared link where two or more multicast routers may be present, all the multicast routers must be MSNIP-capable and have an identical configuration for the SSM address range. MSNIP enforces these requirements by using two new options for IPv4 in the Multicast Router Discovery protocol [[RFC4286](#)] and one new option for IPv6 in the Neighbor Discovery / ICMPv6 protocol [[RFC4861](#)].

[4.1.1.](#) MSNIP Operation Option

A multicast router advertises that it is participating in MSNIP using the MSNIP Operation option in either the Multicast Router Discovery protocol for IPv4 or the Neighbor Discovery / ICMPv6 protocol for IPv6. This option MUST be included in all router advertisement messages of a router that is configured for MSNIP. The format of the option is as follows:


```

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      Padding      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Padding                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type: The type field is set to WW (TBD by IANA) for IPv4 and ZZ (TBD by IANA) for IPv6.

Length: The length field is set to 0 for IPv4 and 1 for IPv6.

Padding: The six extra bytes of padding are only present in IPv6 and are required to bring the size of the option up to the eight octet boundary. The value of the padding bytes must be set to zero on transmission and ignored on receipt.

A multicast router uses received Multicast Router Advertisement and Neighbor Discovery / ICMPv6 messages to determine if all live neighbor multicast routers on each interface are participating in MSNIP. When a router advertisement message not containing an MSNIP option is received by a router participating in MSNIP, the mis-configuration SHOULD be logged to the operator in a rate-limited manner.

If even one multicast router on a link does not have MSNIP capability then ALL routers on that link MUST be configured to not provide MSNIP services and to not advertise the MSNIP Operation option.

4.1.2. SSM Range Option

The SSM Range Multicast Router Discovery option advertises the IPv4 SSM Range with which the router is configured. The option is defined in [[I-D.ietf-magma-mrdssm](#)]. This option is only valid in IPv4. The SSM range for IPv6 is well defined for all valid scopes [[RFC3306](#)] and a mechanism to allow additional ranges to operate in SSM mode on a per-link bases is not required.

4.2. Managed Range Discovery by Source Systems

When an application in an IP system uses the MSNIP service interface to register for notification, the IP system must behave differently depending on whether or not the destination address for which the application registered is operating under SSM (and is being managed by MSNIP). For SSM channels, the IP system should only instruct the application to transmit when there are receivers for the multicast destination. For non-SSM destination addresses the IP system will

not be able to determine if there are receivers and should immediately instruct the application to transmit. In addition, an MSNIP-capable IP system must be able to detect if there are multicast routers on its connected links and if they support MSNIP operation. If no multicast routers are present or if the multicast routers are not MSNIP-capable then the IP system MUST default to flooding and immediately instruct applications to transmit.

An IP system controls transmission behavior under the different possible conditions by adapting its definition of the MSNIP-managed multicast destination address range:

- o On a link with multicast routers operating the MSNIP protocol the IP system MUST use the SSM multicast destination address range as the MSNIP-managed range. IPv4 systems MUST use the contents of the SSM Range option in received Multicast Router Advertisement messages [[I-D.ietf-magma-mrdssm](#)] to discover the configured SSM range. SSM range discovery is not needed in IPv6 where the SSM destination address range is fixed.
- o On a link not connected to a multicast routed infrastructure or on a link with multicast routers that do not support MSNIP operation, the IP system MUST use an empty range as its MSNIP-managed range. This forces applications transmitting to any multicast destination address to default to flooding thus providing backward compatibility.

As described in [Section 4.1.1](#), an IP system can determine the status of a link and distinguish between the above two cases through the reception of IPv4 Multicast Router Advertisement and Neighbor Discovery / ICMPv6 messages.

Internet-Draft

MSNIP

March 2011

[5.](#) Requesting and Receiving Notifications

Like IGMP, MSNIP is an asymmetric protocol specifying different behavior for systems wishing to source traffic and for multicast routers. Host IP systems multicast Host Interest Solicitation messages to register for notification with their first-hop routers. Routers unicast Router Receiver Membership Reports to IP systems to notify them of the arrival of the first or departure of the last receiver for a session. Note that a system may perform at the same time both of the above functions. An example is a router that wishes to source traffic.

[5.1.](#) Host Interest Solicitation

Source systems that wish to be managed by MSNIP periodically transmit a Host Interest Solicitation message. This message is multicast with a multicast destination address of ALL_IGMPv3_ROUTERS (224.0.0.22) or ALL_MLDv2_ROUTERS (FF02::16) and is transmitted every [Interest Solicitation Interval] seconds. The Host Interest Solicitation message contains a holdtime which is set to [Interest Solicitation Holdtime] and instructs the multicast first-hop routers to maintain MSNIP state for this IP system for the specified period. Systems with multiple interfaces or multiple IP addresses per interface must originate separate Host Interest Solicitation messages from each of their IP addresses that they wish to have managed by MSNIP. In practice a system with more than one IP address is treated by MSNIP as multiple IP systems.

When an IP system first comes up it transmits [Robustness Variable] Host Interest Solicitation messages spaced by [Initial Interest Solicitation Interval] seconds.

All MSNIP capable routers that receive a Host Interest Solicitation message from an IP system, maintain a system interest record of the form:

(IP system address, holdtime timer)

Each time a Host Interest Solicitation message is received from the

IP system, the holdtime timer is reset to the holdtime in the received message. In addition the router may respond to the solicitation message with a Receiver Membership Report message described in [Section 5.2](#). The message contains a TRANSMIT record for each of the multicast destination addresses within the MSNIP-managed range for which the routing protocol indicates there are receivers for this source system.

The holdtime timer of a record counts down to zero. When the

holdtime timer of a specific system interest record expires, the record is deleted.

[5.2](#). Router Receiver Membership Reports

Receiver Membership Report messages are used by routers to communicate the receiver membership status of particular multicast destination addresses to a specific IP system. Each message contains a list of transmission control records of either TRANSMIT or HOLD type that instruct a system to respectively start or stop sending traffic on this link to the specified multicast destination address. Receiver Membership Report messages are unicast to the target system.

In addition to reports sent in response to Host Interest Solicitation messages, routers send unsolicited Receiver Membership Reports to IP systems when the receiver membership status reported by the multicast routing protocol changes for a specific source and multicast destination. Such reports are only sent if the multicast destination address is managed by MSNIP and the router has a system interest record created by a previously received Host Interest Solicitation message with an IP system address equal to the source address. If the source / destination pair satisfy these conditions then [Robustness Variable] Receiver Membership Reports are sent out spaced by [Unsolicited Membership Report Interval] seconds. If the membership status changes again for the same destination address and source system while transmission of Receiver Membership Reports is still pending then the pending report messages are canceled and a new set of [Robustness Variable] messages indicating the new state are scheduled.

When an IP system receives a Receiver Membership Report message, for each of the TRANSMIT records listed in the message, it creates or

updates a transmission record of the form:

(router address, source address, multicast address, holdtime timer)

The router address is obtained from the source address of the IP header of the received message. The source address is obtained from the destination address of the IP header of the received message. The multicast address is obtained from the information in the TRANSMIT record. The holdtime timer is set to the value of the holdtime field in the received Receiver Membership Report message.

For each HOLD record present in the message, the system deletes the matching previously created transmission record from its state.

The holdtime timer of a record counts down to zero. When the

holdtime timer of a specific transmission record expires, the record is deleted.

Note that creation and deletion of transmission records in an IP system's state may cause local applications to be notified to start and stop transmitting data (see [Section 6](#)).

6. Application Notification

This section describes the relation between protocol events and notifications to source applications within an IP system. The state machine below is specific to each source address of the IP system and each multicast destination address. The initial state is the No Info state.

In tabular form, the state-machine is:

Event	Previous State		
	No Info	Hold	Transmit
New Register	- Start new	-	- Start new

Start Manage	-> Hold Stop ALL registered	-	-
Stop Manage	-	-> No Info Stop ALL registered	-> No Info
Recv TRANSMIT	-	-> Transmit Start ALL registered	-
Recv last HOLD or timeout	-	-	-> Hold Stop ALL registered

The events in the state machine above have the following meaning:

New register: A new application has registered through a call to `IPMulticastSourceRegister` for this S and G.

Start manage: We received an SSM Range option in an MRD packet on the interface that S belongs to that changed the status of G from a non-managed to a MSNIP-managed destination address. The SSM Range option is only valid in IPv4.

Stop manage: We received an SSM Range option in an MRD packet on the interface that S belongs to that changed the status of G from a MSNIP-managed to a non-managed destination address or the mapping state that caused this destination address to be managed expired. The SSM Range option is only valid in IPv4.

Receive TRANSMIT: We received a Receiver Membership Report with S as the IP destination address that contains a TRANSMIT record for G.

Receive last HOLD or timeout: We either received a Receiver

Membership Report with S as the IP destination address that contains a HOLD record for G or the holdtime timer in a transmission record for S and G expired and there are no other transmission records for S and G. This means that the last router that was reporting receivers no longer does so and there are no routers left wishing to receive traffic from this S to destination address G.

The state machine actions have the following meaning:

Start new: Send an IPMulticastSourceStart notification to the application that just registered for this S and G.

Start ALL registered: Send an IPMulticastSourceStart notification to all applications that are registered for this S and G.

Stop ALL registered: Send an IPMulticastSourceStop notification to all applications that are registered for this S and G.

[7.](#) Router Processing

This section describes the per-source system tracking state machine operated by each first-hop router. The initial state is No Info.

In tabular form, the state-machine is:

Event	Previous State	
	Not tracking	Tracking
Receive HIS	-> Tracking Set HT to message holdtime; Send ALL existing TRANSMITs	- Set HT to message holdtime; Send ALL existing TRANSMITs
HIS timeout	-	-> Not tracking
Receivers for new destination G	-	- Send TRANSMIT for G
Receivers of G leave	-	- Send HOLD for G

The events in the state machine above have the following meaning:

Receive HIS: The router has received a Host Interest Solicitation from S.

HIS timeout: The holdtime timer (HT) in the host interest record associated with S has expired.

Receivers for new destination G: The routing protocol has informed MSNIP that it now has receivers for the MSNIP-managed destination address G and source IP system S.

Receivers of G leave: The routing protocol has informed MSNIP that all receivers for the MSNIP-managed destination address G and source IP system S have left the channel.

The state machine actions have the following meaning:

Set HT to message holdtime: The holdtime timer in the host interest record associated with S is restarted to the value of the holdtime field in the received Host Interest Solicitation message.

Send ALL existing TRANSMITs: The router builds and transmits Receiver Membership Reports to S that contain a TRANSMIT record for each of the MSNIP-managed destination addresses that have receivers for S.

Send TRANSMIT for G: The router builds and transmits a Receiver Membership Report to S that contains a TRANSMIT record for the destination address G.

Send HOLD for G: The router builds and transmits a Receiver Membership Report to S that contains a HOLD record for the destination address G.

Internet-Draft

MSNIP

March 2011

8. Message Formats

The following packet formats are valid for both IPv4 and IPv6. IP version-specific values will be explicitly defined.

There are two message types of concern to the MSNIP protocol described in this document:

Type Number (hex)	Message Name
0xXX	Host Interest Solicitation
0xYY	Receiver Membership Report

Both the Host Interest Solicitation message and the Receiver Membership Report message MUST not be forwarded by routers (see [Section 12](#)). The Router Alert option [[RFC2113](#)] [[RFC2711](#)] MUST be included in the packet by the router or host IP system transmitting the message. Routers receiving Host Interest Solicitation messages and IP systems receiving Receiver Membership Reports MUST not process a received MSNIP message if the Router Alert option is not present.

8.1. Host Interest Solicitation Message

A Host Interest Solicitation message is periodically multicast by MSNIP capable systems to declare interest in Receiver Membership Reports from multicast routers on the link. The Host Interest Solicitation message is multicast with a destination address of ALL_IGMPv3_ROUTERS (224.0.0.22) or ALL_MLDv2_ROUTERS (FF02::16).

0	1	2	3
0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9	0 1
Type	Reserved	Checksum	
Holdtime			

Type: The type field is set to YY (to be assigned by IANA as an IGMP type for IPv4 and an ICMPv6 type for IPv6).

Dest Count: The number of multicast destination address records present in this message.

Checksum: In IPv4, the Checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). In IPv6, the Checksum is the standard ICMPv6 checksum, covering the entire MLDv2 message plus a "pseudo-header" of IPv6 header fields [[RFC4443](#)]. For computing the checksum, the Checksum field is set to zero. When receiving packets, the checksum MUST be verified before processing a packet.

Fenner, et al.

Expires September 5, 2011

[Page 18]

Internet-Draft

MSNIP

March 2011

Holdtime: The amount of time in seconds that the target host must keep alive the transmission record state created or updated by the TRANSMIT records in this report. The router originating the Receiver Membership Report sets this field to the current value of the holdtime timer in the system interest record corresponding to the target host. As a result Receiver Membership Reports sent in response to the reception of a Host Interest Solicitation message have their holdtime set to the value of the holdtime field in the received HIS message.

Reserved: Transmitted as zero. Ignored upon receipt.

Record-Type-1: The type of the first transmission control record in this message. Valid values are:

Record Type	Description	Value
TRANSMIT	Request to start transmitting to destination	1
HOLD	Request to stop transmitting to destination	2

Record-Reserved-1: Transmitted as zero. Ignored upon receipt.

Destination-Address-1: The multicast destination address of the

first record in the message.

[8.3.](#) IPv4 Header Fields

Like all IGMP messages, MSNIP messages are encapsulated in IPv4 datagrams, with an IP protocol number of 2. MSNIP messages can be identified from other IGMP messages by the message types listed in [Section 8](#). Every MSNIP message described in this document is sent with an IP Time-to-Live of 1, and carries an IP Router Alert option [[RFC2113](#)] in its IP header.

[8.4.](#) IPv6 Header Fields

MLD messages are a sub-protocol of the Internet Control Message Protocol (ICMPv6 [[RFC4443](#)]). MSNIP messages are identified in IPv6 packets by the combination of a preceding Next Header value of 58 and by the MLD message types listed in [Section 8](#). All MSNIP messages described in this document are sent with a link-local IPv6 Source Address (or the unspecified address, if a valid link-local address is not available), an IPv6 Hop Limit of 1, and an IPv6 Router Alert option [[RFC2711](#)] in a Hop-by-hop Options header.

[9.](#) Constants Timers and Default Values

Robustness Variable: The Robustness Variable allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the Robustness Variable may be increased. MSNIP is robust to (Robustness Variable - 1) packet losses. The Robustness Variable MUST NOT be zero, and SHOULD NOT be one. Default: 2

Interest Solicitation Interval: The interval used by MSNIP capable systems between transmissions of Host Interest Solicitation messages. Default: 60 secs

Interest Solicitation Holdtime: The interval inserted in Host Interest Solicitation messages by systems to instruct routers how long they should maintain system interest state for. This MUST be ((the Robustness Variable) times (the Interest Solicitation Interval) plus (one second)).

Initial Interest Solicitation Interval: The interval used by

systems to send out the initial Host Interest Solicitation messages when they first come up. Default: 1 second.

Unsolicited Membership Report Interval: The interval used by routers to send out a set of Membership Report messages when the receiver membership changes for a specific system. Default: 1 second.

[10.](#) Possible Optimisations

[10.1.](#) Suppressing HIS Messages

A possible optimisation for MSNIP is to suppress the transmission of Host Interest Solicitation messages from the source address of an IP system for which no local application has registered interest. In addition to conserving bandwidth, not transmitting HIS messages prevents remote receivers for groups with no matching source application from creating transmission record state in the host system.

[10.2.](#) Host Stack Filtering

Legacy applications that have not been coded with MSNIP support can still be prevented from wasting first-hop link bandwidth by filtering transmitted packets at the operating system level. Even though such applications will not register for MSNIP notifications with the host operating system, if the OS is MSNIP-capable and the application is transmitting data to an MSNIP-managed group for which there are no transmit records, the OS can safely filter the packets and not transmit them on the wire.

A problem with the filtering approach is that it cannot be combined with the HIS message suppression optimisation (see [Section 10.1](#)). If there are no registered applications in the system and HIS messages are being suppressed then the first-hop routers will not send any Receiver Membership Reports to the system. As a result, knowledge of receiver membership from the presence of transmit records for groups operated by legacy applications will not exist. It therefore becomes unsafe to filter packets from legacy applications.

[10.3.](#) Responding to Unexpected IGMP Queries

Under steady state the router side of the IGMP protocol elects a single router on each link that is responsible for issuing IGMP Queries. Routers other than the acting IGMP querier will send an IGMP Query only if they restart and have no IGMP querier election state or if the active Querier crashes and a new election takes place.

MSNIP can take advantage of this mechanism to quickly populate the host interest records of a new router starting up. When the router comes up it will issue an IGMP Query in an attempt to be elected as a Querier. MSNIP-capable hosts will notice that the sender of the Query is not the acting Querier. They can use this trigger to respond with Host Interest Solicitation Messages (with transmission randomised over a small interval) to quickly bring the new router up-

to-date.

[10.4.](#) Host and Router Startup

When a host operating system is restarted there may be applications

that are started as part of the initialisation process and want to source IPv4 multicast traffic. It is possible for the applications to register through MSNIP with the IP subsystem and to start transmitting multicast data before the host receives the MSNIP-managed range definition through the SSM Range option of the Multicast Router Discovery protocol.

This temporary flooding can be avoided if the host OS holds off notifying MSNIP-capable applications that they can transmit until it receives an MRD advertisement and learns the SSM configuration for the network. This behaviour has the drawback that it is not compatible with legacy networks with no MRD deployment. In such a network the host OS has to be able to determine after a configurable period that MRD is not enabled and hence all multicast applications wishing to source traffic should be notified to transmit. A good default value for this period is the MAX_RESPONSE_DELAY of the Multicast Router Discovery protocol [[RFC4286](#)].

Late router startup is harder to deal with. Hosts that start up before the multicast router may time out waiting for an MRD advertisement and instruct all MSNIP-capable multicast source applications to transmit data. One way to work around this problem is to configure the host OS to wait forever for an MRD advertisement before instructing MSNIP applications to transmit.

11. Inter-operation with IGMP / MLD Proxying

MSNIP is intended for use on networks with multicast servers offering a large number of potential sessions. Although unlikely, it is possible to deploy such a server behind an IGMP / MLD Proxy [[RFC4605](#)]. If the proxy is not MSNIP-aware and does not implement the extensions described below then sources behind the proxy will default to flooding.

If a device performing IGMP / MLD Proxying wishes to proxy MSNIP, it MUST forward MSNIP Host Interest Solicitation messages that are received on downstream interfaces to its upstream interface. No special treatment is required for MSNIP Receiver Membership Reports as they are unicast to the target host.

In addition to the forwarding of MSNIP messages, an IGMP proxy MUST operate the Multicast Router Discovery protocol [[RFC4286](#)] on all its downstream interfaces and advertise the MSNIP capability option ([Section 4.1.1](#)) and SSM address range option ([Section 4.1.2](#)). The MSNIP capability option should be advertised on downstream interfaces only if it is included in MRD messages received on the upstream interface. The address range to be included in the SSM Range option MUST be determined by MRD and IGMP messages received on the upstream interface of the proxy according to the rules in [Section 4.2](#).

In addition to the forwarding of MSNIP messages, an MLD proxy MUST operate the IPv6 Neighbour Discovery protocol. The MSNIP capability option should be advertised on downstream interfaces when it is included in IPv6 Neighbour Discovery messages received on the upstream interface.

Internet-Draft

MSNIP

March 2011

12. Security Considerations

We consider the ramifications of a forged message of each type. As described in [\[RFC3376\]](#) and [\[RFC3810\]](#), IPSEC AH can be used to authenticate IGMP and MLD messages if desired.

12.1. Receiver Membership Report Attacks

A DoS attack on a host could be staged through forged Receiver Membership Report messages. The attacker can send a large number of reports, each with a large number of TRANSMIT records and a holdtime field set to a large value. The host will have to store and maintain the transmission records specified in all of those reports for the duration of the holdtime. This would consume both memory and CPU cycles in the host.

Forged Receiver Membership Report messages from the local network can be easily traced. There are three measures necessary to defend against externally forged reports:

- o Routers SHOULD NOT forward Receiver Membership Reports. This is easier for a router to accomplish if the report carries the Router-Alert option.
- o Hosts SHOULD ignore Receiver Membership Reports without the Router-Alert option.

Note that a remote attack through the multicast routing protocol is possible. A remote site can originate join state for a large number of groups that will propagate through MSNIP to the target source host. Such attacks are considered a more significant problem for the routers involved and are left up to the routing protocol security.

HOLD records in forged Receiver Membership Report messages are not a significant threat as hosts track the individual interests of each first-hop router separately. Only by forging the source address of the report message so that it appears to have originated from a real first-hop router can the attacker cause the source to stop transmitting to a group that has valid receivers. Such forged messages can be detected by the router itself.

12.2. Host Interest Solicitation Attacks

Forged Host Interest Solicitation messages can have two effects:

- o When non-existent source addresses are used the solicitation messages can create unwanted host record state on attached routers for the duration of the holdtime specified in the message.

- o When a source address corresponding to an existing host is used in the forged HIS message, receipt of the message by attached routers will cause them to transmit Receiver Membership Reports messages for all MSNIP-managed multicast destination addresses with receivers for the target host. Although no additional state will be created in routers or hosts from this attack, bandwidth and CPU is wasted in both the first-hop routers and the target host.

Just like for the Receiver Membership Report message, attacks using the Host Interest Solicitation message can be reduced by requiring the use of the Router-Alert option on the message.

[12.3.](#) MSNIP Managed Range Discovery

As discussed in [[I-D.ietf-magma-mrdssm](#)] it is possible for directly connected systems to send forged Multicast Router Advertisement messages containing the SSM Range Discovery option. As the SSM Range Discovery option determines the MSNIP-managed range under IPv4, such forged messages can temporarily replace the managed range map with incorrect information in receiving hosts. An incorrect mapping can have two effects:

- o Applications using a multicast destination address within the real SSM range that have no valid receivers can be tricked into thinking that their chosen destination address is no longer an SSM address and will therefore start transmitting data.
- o Applications using group addresses outside the valid SSM range can be tricked into thinking that they are using an SSM destination address and therefore prevented from transmitting data.

The Multicast Router Discovery SSM Range Option specification suggests that a router receiving a Multicast Router Advertisement with an inconsistent SSM Range Option log the event to the operator. Such logging will enable tracking of this type of attack.

[13.](#) IANA Considerations

This document introduces the following new types and options that require allocation by IANA:

- o Two new IGMP messages for Host Interest Solicitation and Receiver Membership Report. Each of these messages requires a new IGMP type value to be assigned by IANA [[IGMPREG](#)].
- o The new MSNIP Operation option for the Multicast Router Discovery protocol. This option requires a new MRD type value to be assigned by IANA.
- o The new MSNIP Operation option for the Neighbour Discovery / ICMPv6 protocol. This option requires a new NDP / ICMPv6 type value to be assigned by IANA.

[14.](#) Acknowledgements

The authors would like to thank Dave Thaler, Jon Crowcroft, Toerless Eckert, Haixiang He, Pekka Savola and Karen Kimball for their contribution to this specification.

[15.](#) References

[15.1.](#) Normative References

- [I-D.ietf-magma-mrdssm]
Kouvelas, I., "Multicast Router Discovery SSM Range Option", [draft-ietf-magma-mrdssm-03](#) (work in progress), June 2003.
- [RFC2113] Katz, D., "IP Router Alert Option", [RFC 2113](#), February 1997.
- [RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", [RFC 2711](#), October 1999.

- [RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", [RFC 3376](#), October 2002.
- [RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", [RFC 3810](#), June 2004.
- [RFC4286] Haberman, B. and J. Martin, "Multicast Router Discovery", [RFC 4286](#), December 2005.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [RFC 4443](#), March 2006.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.

[15.2.](#) Informative References

- [IGMPREG] IANA, "IGMP Type Numbers", IGMP TYPE NUMBERS - per [RFC3228](#), [BCP57](#) <http://www.iana.org/assignments/igmp-type-numbers>, June 2005.
- [RFC3306] Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", [RFC 3306](#), August 2002.
- [RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", [RFC 4601](#), August 2006.
- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick,

"Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", [RFC 4605](#), August 2006.

- [RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", [BCP 51](#), [RFC 5771](#), March 2010.

[Appendix A](#). Extending MSNIP to Any-Source Multicast

This document defines MSNIP only for use with SSM. As noted in [Section 2](#) many currently deployed multicast routing protocols require data from an active source to be propagated past the first-hop router before information on the existence of receivers becomes available on the first-hop. We will specify in [Appendix A.1](#) how MSNIP can be extended to work for ASM when PIM-SM [[RFC4601](#)]) is used.

Whether MSNIP can be used for ASM depends on the multicast routing protocols used. There may be different protocols used for different group addresses. Rather than requiring a host to know for which ASM groups MSNIP can be used, we suggest that the host can use it for all ASM groups. If the first-hop router is unable to determine whether there are receivers or not, it can tell the source that there are receivers present anyway. The host will then start sending and the behavior will be as if MSNIP is not used. If MSNIP is extended to ASM, one should consider adding a flag to the MSNIP Operation Option [Section 4.1.1](#), or creating a new option for use with IPv4 in the Multicast Router Discovery protocol [[RFC4286](#)] and Neighbor Discovery / ICMPv6 protocol [[RFC4861](#)], in order to announced the router capability to the hosts.

[A.1](#). Extending MSNIP to ASM with PIM-SM

When PIM-SM [[RFC4601](#)] is used to provide ASM service, a first-hop router will generally not know if there are receivers for a group until it starts receiving data from an active source. Until the source becomes active, receivers simply join the shared tree for the group. This allows the Rendezvous-Point (RP) for the group to learn that receivers are present. Next when a source becomes active, a first-hop router (the Designated Router (DR)) will be responsible for sending PIM register messages to the the RP. If there are receivers present, the RP and/or last-hop routers will join the Shortest Path Tree (SPT) towards the source. This will result in at least one first-hop router learning that a source exists. The last part is similar to when using PIM-SM for SSM. With SSM a last-hop router immediately joins the Shortest Path Tree (SPT).

MSNIP can be extended to ASM with PIM-SM as follows:

- o Host Interest Solicitation Message ([Section 8.1](#)) need to be extended to include a list of groups that the host is interested in receiving membership reports for.
- o When a Designated Router (DR) receives a Host Interest Solicitation Message with source address S containing a group G, it will periodically send PIM Null-Register messages to the RP for

Internet-Draft

MSNIP

March 2011

(S,G). This is done instead of the data PIM Register messages the DR would use if the source did not use MSNIP. Per the DR register state machine in [section 4.4.1 of \[RFC4601\]](#), one can immediately send a Null-Register and then move to Prune state as if a Register-Stop was received. When the Register-Stop timer expires, send a Null-Register as usual. But then, rather than setting the Register-Stop timer to Register_Probe_Time, transition directly to Prune state as if a Register-Stop was received again. By periodically receiving the (S,G) registers, the RP will know that a source exists, and will join the SPT towards the source if it has receivers. Just like SSM, a first-hop routers will then receive an SPT join for (S,G) and learn that there are receivers. It can then inform the source. If the first-hop router has (*,G)-state, e.g., local interest or it is part of the shared tree, but has not yet got an (S,G) olist, it must immediately inform the source.

One benefit with this approach, is that PIM data registers can be avoided.

Internet-Draft

MSNIP

March 2011

Authors' Addresses

Bill Fenner
AT&T Labs--Research
1 River Oaks Place
San Jose, CA 95134
USA

Email: fenner@research.att.com

Brian Haberman
Johns Hopkins University Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723-6099
USA

Email: brian@innovationslab.net

Hugh Holbrook
Arastra, Inc.
P.O. Box 10905
Palo Alto, CA 94303
USA

Email: holbrook@arastra.com

Isidor Kouvelas
cisco Systems
Tasman Drive
San Jose, CA 95134
USA

Email: kouvelas@cisco.com

Stig Venaas
cisco Systems
Tasman Drive
San Jose, CA 95134
USA

Email: stig@cisco.com