Network Working Group
Request for Comments: 988

S. E. Deering
Stanford University

July 1986

Host Extensions for IP Multicasting

1. STATUS OF THIS MEMO

This memo specifies the extensions required of a host implementation of the Internet Protocol (IP) to support internetwork multicasting. This specification supersedes that given in RFC-966, and constitutes a proposed protocol standard for IP multicasting in the ARPA-Internet. The reader is directed to RFC-966 for a discussion of the motivation and rationale behind the multicasting extension specified here. Distribution of this memo is unlimited.

2. INTRODUCTION

IP multicasting is defined as the transmission of an IP datagram to a "host group", a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group with the same "best-efforts" reliability as regular unicast IP datagrams, i.e. the datagram is not guaranteed to arrive at all members of the destination group or in the same order relative to other datagrams.

The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group, but membership in a group may be restricted to only those hosts possessing a private access key. A host may be a member of more than one group at a time. A host need not be a member of a group to send datagrams to it.

A host group may be permanent or transient. A permanent group has a well-known, administratively assigned IP address. It is the address, not the membership of the group, that is permanent; at any time a permanent group may have any number of members, even zero. A transient group, on the other hand, is assigned an address dynamically when the group is created, at the request of a host. A transient group ceases to exist, and its address becomes eligible for reassignment, when its membership drops to zero.

The creation of transient groups and the maintenance of group membership information is the responsibility of "multicast agents", entities that reside in internet gateways or other special-purpose hosts. There is at least one multicast agent directly attached to every IP network or subnetwork that supports IP multicasting. A host requests the creation of new groups, and joins or leaves existing groups, by exchanging messages with a neighboring agent.

Multicast agents are also responsible for internetwork delivery of multicast IP datagrams. When sending a multicast IP datagram, a host transmits it to a local network multicast address which identifies all neighboring members of the destination host group. If the group has members on other networks, a multicast agent becomes an additional recipient of the local multicast and relays the datagram to agents on each of those other networks, via the internet gateway system. Finally, the agents on the other networks each transmit the datagram as a local multicast to their own neighboring members of the destination group.

This memo specifies the extensions required of a host IP implementation to support IP multicasting, where a "host" is any internet host or gateway other than those serving as multicast agents. The algorithms and protocols used within and between multicast agents are transparent to non-agent hosts and will be specified in a separate document. This memo also does not specify how local network multicasting is accomplished for all types of network, although it does specify the required service interface to an arbitrary local network and gives an Ethernet specification as an example. Specifications for other types of network will be the subject of future memos.

3. LEVELS OF CONFORMANCE

There are three levels of conformance to this specification:

Level 0: no support for IP multicasting.

There is, at this time, no requirement that all IP implementations support IP multicasting. Level 0 hosts will, in general, be unaffected by multicast activity. The only exception arises on some types of local network, where the presence of level 1 or 2 hosts may cause misdelivery of multicast IP datagrams to level 0 hosts. Such datagrams can easily be identified by the presence of a class D IP address in their destination address field; they should be quietly discarded by hosts that do not support IP multicasting. Class D addresses are defined in section 4 of this memo.

Level 1: support for sending but not receiving multicast IP datagrams.

Level 1 allows a host to partake of some multicast-based services, such as resource location or status reporting, but it does not allow a host to create or join any host groups. An IP implementation may be upgraded from level 0 to level 1 very easily and with little new code. Only sections 4, 5, and 6 of this memo are applicable to level 1 implementations.

Level 2: full support for IP multicasting.

Level 2 allows a host to create, join and leave host groups, as well as send IP datagrams to host groups. It requires implementation of the Internet Group Management Protocol (IGMP) and extension of the IP and local network service interfaces within the host. All of the following sections of this memo are applicable to level 2 implementations.

4. HOST GROUP ADDRESSES

Host groups are identified by class D IP addresses, i.e. those with "1110" as their high-order four bits. The remaining 28 bits are unstructured as far as hosts are concerned. The addresses of well-known, permanent groups are to be published in "Assigned Numbers". Class E IP addresses, i.e. those with "1111" as their high-order four bits, are reserved for future addressing modes.

Appendix II contains some background discussion of several issues related to host group addresses.

5. MODEL OF A HOST IP IMPLEMENTATION

The multicast extensions to a host IP implementation are specified in terms of the layered model illustrated below. In this model, ICMP and (for level 2 hosts) IGMP are considered to be implemented within the IP module, and the mapping of IP addresses to local network addresses is considered to be the responsibility of local network modules. This model is for expository purposes only, and should not be construed as constraining an actual implementation.

```
         |                                                           |
         |                Upper-Layer Protocol Modules               |
         |___________________________________________________________|

      -------------------- IP Service Interface -----------------------
          ___________________________________________________________
         |                             |              |              |
         |                             |     ICMP     |     IGMP     |
         |             IP              |______________|______________|
         |           Module                                          |
         |                                                           |
         |___________________________________________________________|

      --------------- Local Network Service Interface -----------------
          ___________________________________________________________
         |                             |                             |
         |            Local            | IP-to-local address mapping |
         |           Network           |         (e.g. ARP)          |
         |           Modules           |_____________________________|
         |       (e.g. Ethernet)                                     |
         |                                                           |
```

To support level 2 IP multicasting, a host IP implementation must provide three new services: (1) sending multicast IP datagrams, (2) receiving multicast IP datagrams, and (3) managing group membership. Only the first service need be provided in level 1 hosts. Each of these services is described in a separate section, below. For each service, extensions are specified for the IP service interface, the IP module, the local network service interface, and an Ethernet local network module. Extensions to local network modules other than Ethernet are mentioned briefly, but are not specified in detail.

6. SENDING MULTICAST IP DATAGRAMS

6.1. Extensions to the IP Service Interface

No change to the IP service interface is required to support the sending of multicast IP datagrams. An upper-layer protocol module merely specifies an IP host group destination, rather than an individual IP destination, when it invokes the existing "Send IP" operation.

6.2. Extensions to the IP Module

To support the sending of multicast IP datagrams, the IP module must be extended to recognize IP host group addresses when routing outgoing datagrams. Most IP implementations include the following logic:

```
if IP-destination is on the same local network,
   send datagram locally to IP-destination
else
   send datagram locally to GatewayTo(IP-destination)
```

To allow multicast transmissions, the routing logic must be changed to:

```
if IP-destination is on the same local network
or IP-destination is a host group,
   send datagram locally to IP-destination
else
   send datagram locally to GatewayTo(IP-destination)
```

If the sending host is itself a member of the destination group, a copy of the outgoing datagram must be looped-back for local delivery if and only if loopback was requested when the host joined the group (see section 8.1). (This issue does not arise in level 1 implementations.)

On hosts attached to more than one network, each multicast IP datagram must be transmitted via one network interface only, leaving it to the multicast agents to effect delivery to any other required networks.

A host group address should not be placed in the source address field of an outgoing IP datagram. A host group address may be used in a source routing option as the last element only.

It should be noted that a small IP time-to-live (TTL) value can prevent delivery to some members of a destination group. Thus, a large TTL value should be used to reach all members. Conversely, a small TTL value can be used to advantage to reach only "nearby" members of a widely-dispersed group. In clusters of low-delay local area networks, the TTL field acts as a hop limit; thus, one can perform expanding-ring searches by starting with a TTL of 1 and incrementing on each retransmission, up to some limit defined by the diameter of the cluster.

6.3. Extensions to the Local Network Service Interface

No change to the local network service interface is required to support the sending of multicast IP datagrams. The IP module merely specifies an IP host group destination, rather than an individual IP destination, when it invokes the existing "Send Local" operation.

6.4. Extensions to an Ethernet Local Network Module

The Ethernet directly supports the sending of local multicast packets by allowing multicast addresses in the destination field of Ethernet packets. All that is needed to support the sending of multicast IP datagrams is a procedure for mapping IP host group addresses to Ethernet multicast addresses.

An IP host group address is mapped to an Ethernet multicast address by placing the low-order 28-bits of the IP address into the low-order 28 bits of an Ethernet address. The high-order 20 bits of the Ethernet address are set to a well-known value, to be published in "Assigned Numbers".

[At time of publication of this memo, a block of Ethernet multicast addresses with 28 unspecified bits had not yet been obtained from the allocating authority. If such a block of addresses cannot be obtained, an alternative mapping scheme will be specified.]

6.5. Extensions to Local Network Modules other than Ethernet

Other networks that directly support multicasting, such as rings or buses conforming to the IEEE 802.2 standard, can be handled the same way as Ethernet for the purpose of sending multicast IP datagrams. For a network that supports broadcast but not multicast, such as the Experimental Ethernet, all IP host group addresses can be mapped to a single local broadcast address (at the cost of increased overhead on all local hosts). For a point-to-point networks like the ARPANET or a public data network

(X.25), all IP host group addresses might be mapped to the well-known local address of an IP multicast agent; an agent on such a network would take responsibility for completing multicast delivery within the network as well as among networks.

7. RECEIVING MULTICAST IP DATAGRAMS

7.1. Extensions to the IP Service Interface

No change to the IP service interface is required to support the reception of multicast IP datagrams. Incoming multicast IP datagrams are delivered to upper-layer protocol modules using the same "Receive IP" operation as normal, unicast datagrams.

7.2. Extensions to the IP Module

To support the reception of multicast IP datagrams, the IP module must be extended to recognize the addresses of IP host groups to which the host currently belongs, in addition to the host's individual IP address(es). An incoming datagram destined to one of those group addresses is processed exactly the same way as datagrams destined to one of the host's individual addresses. Incoming datagrams destined to groups to which the host does not belong are discarded without generating any error report.

On hosts attached to more than one network, if a datagram arrives via one network interface, destined for a group to which the host belongs only on a different interface, the datagram is quietly discarded. (This should occur only as a result of inadequate multicast address filtering in the local network module.)

An incoming datagram is not rejected for having an IP host group address in its source address field or anywhere in a source routing option.

An ICMP error message (Destination Unreachable, Time Exceeded, Parameter Problem, Source Quench, or Redirect) is never generated in response to a datagram destined to an IP host group.

7.3. Extensions to the Local Network Service Interface

No change to the local network service interface is required to support the reception of multicast IP datagrams. Incoming local network packets, whether multicast or unicast, are delivered to the IP module using the same "Receive Local" operation.

7.4. Extensions to an Ethernet Local Network Module

To support the reception of multicast IP datagrams, an Ethernet module must be able to receive packets addressed to the Ethernet multicast addresses that correspond to the host's IP host group addresses. It is highly desirable to take advantage of any address filtering capabilities that the Ethernet hardware interface may have, so that the host only receives packets that are destined to it.

Unfortunately, many current Ethernet interfaces have a small limit on the number of addresses that the hardware can be configured to recognize. However, an implementation must be capable of listening on an arbitrary number of Ethernet multicast addresses, which may mean "opening up" the address filter to accept all multicast packets during those periods when the number of addresses exceeds the limit of the filter.

For interfaces with inadequate hardware address filtering, it may be desirable (for performance reasons) to perform Ethernet address filtering within the software of the Ethernet module. This is not mandatory, however, because the IP module performs its own filtering based on IP destination addresses.

7.5. Extensions to Local Network Modules other than Ethernet

Other multicast networks, such as IEEE 802.2 networks, can be handled the same way as Ethernet for the purpose of receiving multicast IP datagrams. For pure broadcast networks, such as the Experimental Ethernet, all incoming broadcast packets can be accepted and passed to the IP module for IP-level filtering. On a point-to-point network, multicast IP datagrams will arrive as local network unicasts, so no change to the local network module should be necessary.

8. MANAGING GROUP MEMBERSHIP

8.1. Extensions to the IP Service Interface

To allow upper-layer protocol modules to request that their host create, join, or leave a host group, the IP service interface must be extended to offer the following three new operations:

```
   CreateGroup ( private, loopback )
                             --> outcome, group-address, access-key
```

The CreateGroup operation requests the creation of a new, transient host group, with this host as its only member. The "private" argument specifies if the group is to be private or public. The "loopback" argument specifies whether or not datagrams sent from this host to the group should be delivered locally as well as to other member hosts. The "outcome" result indicates whether the request is granted or denied. If it is granted, a new 32-bit IP host group address is returned, along with a 64-bit access key which is zero for public groups and non-zero for private groups. The request may be denied due to lack of response from a multicast agent, or lack of resources.

```
   JoinGroup ( group-address, access-key, loopback ) --> outcome
```

The JoinGroup operation requests that this host become a member of the host group identified by "group-address", with the specified access key. The "loopback" argument specifies whether or not datagrams sent from this host to the group should be delivered locally as well as to other member hosts. The "outcome" result indicates whether the request is granted or denied. The request may be denied due to lack of response from a multicast agent, lack of resources, an invalid group address, an incorrect access key, or already being a member.

```
   LeaveGroup ( group-address, access-key ) --> outcome
```

The LeaveGroup operation requests that this host give up its membership in the host group identified by "group-address", with the specified access key. The "outcome" result indicates whether the request is granted or denied. The request may be denied due to an invalid group address, an incorrect access key, or not currently being a member.

Each of these operations may take up to a minute or more to complete, depending on the number of IGMP retransmissions performed within the IP module, and time required for a multicast agent to generate a reply. However, typical delays should be on the order of a few seconds.

Besides the LeaveGroup operation, a host loses its membership in a group whenever the host or its IP module crashes, or, in rare circumstances, when a multicast agent revokes its membership. The IP service interface should provide some means of informing an upper-layer module when its membership has been revoked. Membership may be revoked due to lack of resources, deallocation of the group address, or the discovery of another host group using the same group address with a different access key. (See Appendix II for discussion of address recycling issues.)

It is important to observe that IP group membership is per-host, rather than per-process. An IP service interface should not allow multiple processes to invoke JoinGroup operations for the same group as a way of achieving delivery to more than process. The IP module delivers each incoming datagram, whether multicast or unicast, to the single upper-layer protocol module identified by the protocol field in the datagram's IP header; it is an upper-layer issue whether or not to deliver incoming datagrams to more than one process, perhaps using the concept of "process groups" or "shared ports".

8.2. Extensions to the IP Module

Within the IP module, the membership management operations are supported by the Internet Group Management Protocol (IGMP), specified in Appendix I. As well as having messages corresponding to each of the operations specified above, IGMP also specifies a "deadman timer" procedure whereby hosts periodically confirm their memberships with the multicast agents.

The IP module must maintain a data structure listing the IP addresses of all host groups to which the host currently belongs, along with each group's loopback policy, access key, and timer variables. This data structure is used by the IP multicast transmission service to know which outgoing datagrams to loop back, and by the reception service to know which incoming datagrams to accept. The purpose of IGMP and the management interface operations is to maintain this data structure.

On hosts attached to more than one network, each membership is associated with a particular network interface. On such a host the management interface operations above may each require an additional parameter specifying to which interface the create, join, or leave request applies. The group membership data structure must also be extended to associate an interface with each membership. If a host joins the same host group on more than one network interface, it can expect to receive multiple copies of each datagram sent to that group.

8.3. Extensions to the Local Network Service Interface

To allow an IP module to control what packets should be accepted by the local network module, it is necessary to extend the local network service interface with the following two new operations:

```
AcceptAddress ( group-address )

RejectAddress ( group-address )
```

where "group-address" is an IP host group address. The AcceptAddress operation requests the local network module to accept and deliver up subsequently arriving packets destined to the local network address corresponding to "group-address". The RejectAddress operation requests the local network module to stop delivering up packets destined to the local network address corresponding to "group-address".

Any local network module is free to ignore RejectAddress requests, and may deliver up packets destined to more addresses than just those specified in AcceptAddress requests, if it is unable to filter incoming packets adequately.

8.4. Extensions to an Ethernet Local Network Module

An Ethernet module responds to AcceptAddress operations by adding the corresponding Ethernet multicast address to its acceptance filter for incoming packets. A RejectAddress operation causes the corresponding Ethernet address to be dropped from the filter. For Ethernet interfaces with a limit on the number of addresses that can be added to the filter, the Ethernet software module must detect when that threshold is exceeded and open up the filter to accept all multicast packets. It should also detect when the number of addresses drops below the threshold and revert to individual address filtering.

8.5. Extensions to Local Network Modules other than Ethernet

Other multicast networks, such as IEEE 802.2 networks, can be handled the same way as Ethernet for the purpose of controlling address filtering. For a pure broadcast network or a point-to-point network, the AcceptAddress and RejectAddress operations may have no effect; all incoming packets could be passed to the IP module for IP-level filtering.

APPENDIX I. INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)

The Internet Group Management Protocol (IGMP) is used between IP hosts and their immediate neighbor multicast agents to support the creation of transient groups, the addition and deletion of members of a group, and the periodic confirmation of group membership. IGMP is an asymmetric protocol and is specified here from the point of view of a host, rather than a multicast agent.

Like ICMP, IGMP is a integral part of IP. It is required to be implemented in full by all hosts conforming to level 2 of the IP multicasting specification. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. All IGMP messages have the following format:

```
 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      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Identifier                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Group Address                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Access Key                            +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

There are eight types of IGMP message:

1 = Create Group Request
2 = Create Group Reply

3 = Join Group Request
4 = Join Group Reply

5 = Leave Group Request
6 = Leave Group Reply

7 = Confirm Group Request
8 = Confirm Group Reply

Code

In a Create Group Request message, the code field indicates if the new host group is to be public or private:

0 = public
1 = private

In all other Request messages, the code field contains zero.

In a Reply message, the Code field specifies the outcome of the request:

```
0       = request granted
1       = request denied,  no resources
2       = request denied,  invalid code
3       = request denied,  invalid group address
4       = request denied,  invalid access key
5 - 255 = request pending, retry in this many seconds
```

Checksum

The checksum is the 16-bit one's complement of the one's complement sum of the IGMP message starting with the IGMP Type. For computing the checksum, the checksum field should be zero.

Identifier

In a Confirm Group Request message, the identifier field contains zero.

In all other Request messages, the identifier field contains a value to distinguish the request from other requests by the same host.

In a Reply message, the identifier field contains the same value as in the corresponding Request message.

Group Address

In a Create Group Request message, the group address field contains zero.

In all other Request messages, the group address field contains a host group address.

In a Create Group Reply message, the group address field contains either a newly allocated host group address (if the request is granted) or zero (if denied).

In all other Reply messages, the group address field contains the same host group address as in the corresponding Request message.

Access Key

In a Create Group Request message, the access key field contains zero.

In all other Request messages, the access key field contains the access key assigned to the host group identified in the Group Address field (zero for public groups).

In a Create Group Reply message, the access key field contains either a non-zero 64-bit number (if the request for a private group is granted) or zero.

In all other Reply messages, the access key field contains the same access key as in the corresponding Request.

Protocol Rules

Request messages are sent only by hosts. Reply messages are sent only by multicast agents. If a host receives an IGMP message of a type other than the four Reply types specified above, the message is discarded.

A Request message is sent with its IP destination field containing the well-known address of the Multicast Agent Group. The IP time-to-live field is initialized by the sender to 1, in order to limit the scope of the request to immediate neighbor multicast agents only. The IP source address field contains the individual IP address of the sending host.

A Reply message is sent only in response to a Request message. Its IP destination address field contains the individual address of the host that sent the corresponding Request. (A Confirm Group Reply may also be sent to the host group address specified in its corresponding Confirm Group Request.) The IP source address field contains the individual IP address of the replying multicast agent.

When a host sends a new Create Group, Join Group, or Leave Group Request message, it supplies an arbitrary identifier that it has not used within the last T0 seconds. (It is usually sufficient just to increment the identifier for each new request.) The host initializes a timer to T1 seconds and a retransmission counter to zero. If a Reply message with a matching identifier is not received before the timer expires, it is reset to T1 seconds and the retransmission counter is incremented. If the counter is less than N1, the host retransmits the Request message with the same identifier. If the counter equals N1, the host gives up; if the request was to create or join a group, it is deemed to have failed; if the request was to leave a group, it is deemed to have succeeded.

If a "request pending" code is received in a matching reply to a Create Group, Join Group, or Leave Group Request, the timer is reset to the number of seconds specified by the code and the retransmission counter is reset to zero. The new timer value applies to one timeout interval only -- if the timer expires, it is reset to T1 seconds, the counter is incremented, and the request is retransmitted.

The first matching Reply to a Create Group, Join Group, or Leave Group Request containing a "request granted" or "request denied" code determines the outcome of the request. Any subsequent or non-matching Replies are discarded by the host. However, if a host receives an affirmative Create Group Reply or Join Group Reply that neither matches an outstanding Request nor contains the address of a group to which the host belongs, the host should immediately send a Leave Group Request for the unexpected group address.

A "request granted" reply to a Create Group Request implies that, as well as the group being created, the requesting host is granted membership in the group, i.e. there is no need to send a separate Join Group Request.

Confirm Group Request messages must be sent periodically by hosts to inform the neighboring multicast agent(s) of the hosts' continuing membership in the specified groups. If an agent does not receive a Confirm Group Request message for a particular group within an agent-defined interval, it stops delivering datagrams destined to that group.

For each group to which it belongs, a host maintains a confirmation timer and a variable t. The variable t is initialized to T2 seconds. Whenever the host's request to create or join a group is granted, and whenever the host either sends a Confirm Group Request or receives a Confirm Group Reply with a "request granted" code for the group, the host sets the group's timer to a random number uniformly distributed between t and t + T3 seconds. If the host receives a a Confirm Group Reply with a "request pending" code, t is changed to the value of the code and the timer is reset to a random number between the new t and t + T3. The variable t retains its value until another "request pending" code is received. Whenever the timer expires, the host sends a Confirm Group Request.

Even if a host fails to receive Confirm Group Replies to its Requests, it continues to consider itself a member of the group, because it may still be able to receive multicast datagrams from other hosts on the same local network. Only if a host receives a "request denied" code in a Confirm Group Reply does it stop sending Confirm Group Requests and consider its membership to be revoked.

Multicast agents respond to Confirm Group Request messages by sending Confirm Group Reply messages either to the individual sender of the Request or to the host group address specified in the Request. By sending back a Confirm Group Reply to all neighboring members of a group, a multicast agent is able to reset every member's timer with a single packet. The randomization of the timers is intended to cause only the one member whose timer expires first to send a Confirm Group Request, stimulating a Reply to reset all the timers. The use of the "request pending" codes allows the multicast agent to control the rate at which it receives Confirm Group Requests.

Protocol Timing Constants

The following timing constants are specified for IGMP. They are subject to change as a result of operational experience.

T0 = 300 seconds	minimum recycle time for identifiers
T1 = 2 seconds	retrans. interval for Create/Join/Leave Requests
N1 = 5 tries	retrans. limit for Create/Join/Leave Requests
T2 = 15 seconds	initial value for Confirm Request variable t
T3 = 15 seconds	random range for Confirm Request variable t

APPENDIX II. HOST GROUP ADDRESS ISSUES

This appendix is not part of the IP multicasting specification, but provides background discussion of several issues related to IP host group addresses.

Group Address Binding

The binding of IP host group addresses to physical hosts may be considered a generalization of the binding of IP unicast addresses. An IP unicast address is statically bound to a single local network interface on a single IP network. An IP host group address is dynamically bound to a set of local network interfaces on a set of IP networks.

It is important to understand that an IP host group address is NOT bound to a set of IP unicast addresses. The multicast agents do not need to maintain a list of individual members of each host group. For example, a multicast agent attached to an Ethernet need associate only a single Ethernet multicast address with each host group having local members, rather than a list of the members' individual IP or Ethernet addresses.

Group Addresses as Logical Addresses

Host group addresses have been defined specifically for use in the destination address field of multicast IP datagrams. However, the fact that group addresses are location-independent (they are not statically bound to a single network interface) suggests possible uses as more general "logical addresses", both in the source as well as the destination address field of datagrams. For example, a mobile IP host might have a host group address as its only identity, used as the source of datagrams it sends. Whenever the mobile host moved from one network to another, it would join its own group on the new network and depart from the group on the old network. Other hosts communicating with the mobile one would deal only with the group address and would be unaware of, and unaffected by, the changing network location of the mobile host.

Host group addresses cannot, however, be used to solve all problems of internetwork logical addressing, such as delivery to the "nearest" or the "least loaded" network interface of a multi-homed host. Furthermore, there are hazards in using group addresses in the source address field of datagrams when the group actually contains more than one host. For instance, the IP datagram reassembly algorithm relies on every host using a different source address. Also, errors in a datagram sent with a group source address may result in error reports being returned to all members of the group, not just the sender. In view of these hazards, this memo specifies the use of host group addresses only as destinations of datagrams, either in the destination address field or as the last element of a source routing option. However, it is recommended that datagrams with a group source address be accepted without complaint, thereby allowing other implementations to experiment with logical addressing applications of host group addresses.

Recycling of Transient Host Group Addresses

Since host group addresses are of fixed, relatively small size, transient group addresses must be recycled to satisfy continuing requests for creation of new groups. The multicast agents make an effort to ensure that a group has no members anywhere in the internet before allocating its address to a new group. However, under certain conditions of internetwork partitioning and membership migration, it is impossible to guarantee unique allocation of an address without seriously compromising the availability and robustness of host groups. Furthermore, hosts that are unaware that a particular group has ceased to exist may send datagrams to it long after its address has been assigned to a new group. Therefore, hosts should be prepared for the possibility of misdelivery of multicast IP datagrams to unintended hosts, even in private groups. Such misdelivery can only be detected at a level above IP, using higher-level identifiers or authentication tokens. (The access key of a private group might be used in some applications as such an identifier.) Of course, there are other threats to privacy of communication in the internet, besides group address collision, such as untrustworthy gateways or unsecured networks. End-to-end encryption is an effective defense against such threats.