Network Working Group   S. Deering, Editor
Request for Comments: 1256   Xerox PARC
                                                        September 1991

                     ICMP Router Discovery Messages

Status of this Memo

   This RFC specifies an IAB standards track protocol for the Internet
   community, and requests discussion and suggestions for improvements.
   Please refer to the current edition of the "IAB Official Protocol
   Standards" for the standardization state and status of this protocol.
   This document is a product of the IETF Router Discovery Working
   Group. Distribution of this memo is unlimited.

Abstract

   This document specifies an extension of the Internet Control Message
   Protocol (ICMP) to enable hosts attached to multicast or broadcast
   networks to discover the IP addresses of their neighboring routers.

Table of Contents

1. Terminology

   The following terms have a precise meaning when used in this
   document:

   system   a device that implements the Internet Protocol, IP [9].

   router   a system that forwards IP datagrams, as specified

in [2]. This does not include systems that, though
capable of IP forwarding, have that capability turned
off. Nor does it include systems that do IP forwarding
only insofar as required to obey IP Source Route
options.

host   any system that is not a router.

multicast   unless otherwise qualified, means the use of either IP
              multicast [4] or IP broadcast [6] service.

link   a communication facility or medium over which systems
              can communicate at the link layer, i.e., the protocol
              layer immediately below IP. The term "physical
              network" has sometimes been used (imprecisely) for
              this. Examples of links are LANs (possibly bridged to
              other LANs), wide-area store-and-forward networks,
              satellite channels, and point-to-point links.

multicast link
              a link over which IP multicast or IP broadcast service
              is supported. This includes broadcast media such as
              LANs and satellite channels, single point-to-point
              links, and some store-and-forward networks such as SMDS
              networks [8].

interface   a system's attachment point to a link. It is possible
              (though unusual) for a system to have more than one
              interface to the same link. Interfaces are uniquely
              identified by IP unicast addresses; a single interface
              may have more than one such address.

multicast interface
              an interface to a multicast link, that is, an interface
              to a link over which IP multicast or IP broadcast
              service is supported.

subnet   either a single subnet of a subnetted IP network [7] or
              a single non-subnetted IP network, i.e., the entity
              identified by an IP address logically ANDed with its
              assigned subnet mask. More than one subnet may exist
              on the same link.

neighboring   having an IP address belonging to the same subnet.

2. Protocol Overview

   Before a host can send IP datagrams beyond its directly-attached
   subnet, it must discover the address of at least one operational
   router on that subnet. Typically, this is accomplished by reading a
   list of one or more router addresses from a (possibly remote)
   configuration file at startup time. On multicast links, some hosts
   also discover router addresses by listening to routing protocol
   traffic. Both of these methods have serious drawbacks: configuration
   files must be maintained manually -- a significant administrative
   burden -- and are unable to track dynamic changes in router
   availability; eavesdropping on routing traffic requires that hosts
   recognize the particular routing protocols in use, which vary from
   subnet to subnet and which are subject to change at any time. This
   document specifies an alternative router discovery method using a
   pair of ICMP [10] messages, for use on multicast links. It
   eliminates the need for manual configuration of router addresses and
   is independent of any specific routing protocol.

   The ICMP router discovery messages are called "Router Advertisements"
   and "Router Solicitations". Each router periodically multicasts a
   Router Advertisement from each of its multicast interfaces,
   announcing the IP address(es) of that interface. Hosts discover the
   addresses of their neighboring routers simply by listening for
   advertisements. When a host attached to a multicast link starts up,
   it may multicast a Router Solicitation to ask for immediate
   advertisements, rather than waiting for the next periodic ones to
   arrive; if (and only if) no advertisements are forthcoming, the host
   may retransmit the solicitation a small number of times, but then
   must desist from sending any more solicitations. Any routers that
   subsequently start up, or that were not discovered because of packet
   loss or temporary link partitioning, are eventually discovered by
   reception of their periodic (unsolicited) advertisements. (Links
   that suffer high packet loss rates or frequent partitioning are
   accommodated by increasing the rate of advertisements, rather than
   increasing the number of solicitations that hosts are permitted to
   send.)

   The router discovery messages do not constitute a routing protocol:
   they enable hosts to discover the existence of neighboring routers,
   but not which router is best to reach a particular destination. If a
   host chooses a poor first-hop router for a particular destination, it
   should receive an ICMP Redirect from that router, identifying a
   better one.

   A Router Advertisement includes a "preference level" for each
   advertised router address. When a host must choose a default router
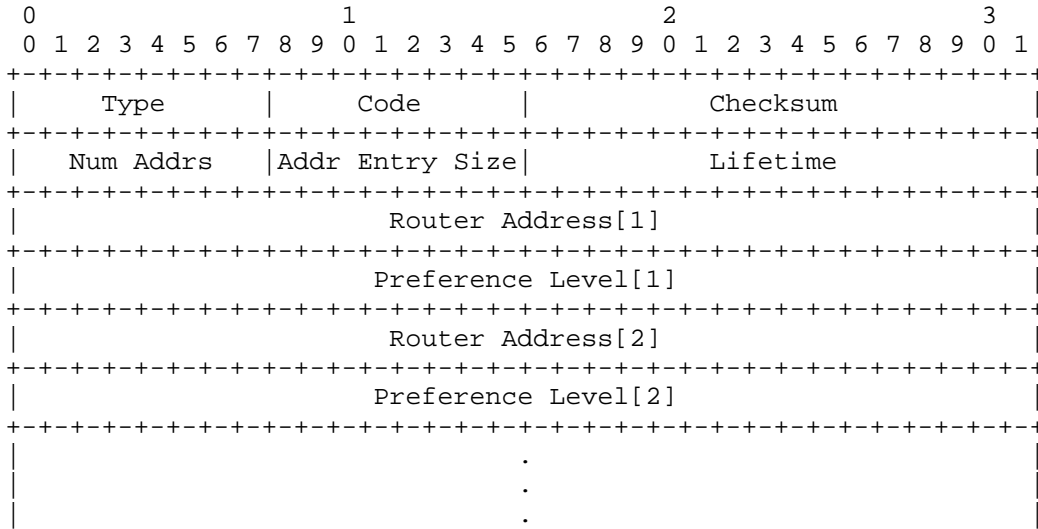   address (i.e., when, for a particular destination, the host has not

been redirected or configured to use a specific router address), it
is expected to choose from those router addresses that have the
highest preference level (see Section 3.3.1 in the Host Requirements
-- Communication Layers RFC [1]). A network administrator can
configure router address preference levels to encourage or discourage
the use of particular routers as default routers.

A Router Advertisement also includes a "lifetime" field, specifying
the maximum length of time that the advertised addresses are to be
considered as valid router addresses by hosts, in the absence of
further advertisements. This is used to ensure that hosts eventually
forget about routers that fail, become unreachable, or stop acting as
routers.

The default advertising rate is once every 7 to 10 minutes, and the
default lifetime is 30 minutes. This means that, using the default
values, the advertisements are not sufficient as a mechanism for
"black hole" detection, i.e., detection of failure of the first hop
of an active path -- ideally, black holes should be detected quickly
enough to switch to another router before any transport connections
or higher-layer sessions time out. It is assumed that hosts already
have mechanisms for black hole detection, as required by [1]. Hosts
cannot depend on Router Advertisements for this purpose, since they
may be unavailable or administratively disabled on any particular
link or from any particular router. Therefore, the default
advertising rate and lifetime values were chosen simply to make the
load imposed on links and hosts by the periodic multicast
advertisements negligible, even when there are many routers present.
However, a network administrator who wishes to employ advertisements
as a supplemental black hole detection mechanism is free to configure
smaller values.

3. Message Formats

    ICMP Router Advertisement Message

```
        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            |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |   Num Addrs   |Addr Entry Size|            Lifetime           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Router Address[1]                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                      Preference Level[1]                      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                       Router Address[2]                       |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                      Preference Level[2]                      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                               .                               |
       |                               .                               |
       |                               .                               |
```

    IP Fields:

        Source Address   An IP address belonging to the interface
                               from which this message is sent.

        Destination Address   The configured AdvertisementAddress or the
                               IP address of a neighboring host.

        Time-to-Live   1 if the Destination Address is an IP
                               multicast address; at least 1 otherwise.

    ICMP Fields:

        Type   9

        Code   0

        Checksum   The 16-bit one's complement of the one's
                               complement sum of the ICMP message, start-
                               ing with the ICMP Type. For computing the
                               checksum, the Checksum field is set to 0.

      Num Addrs   The number of router addresses advertised
                            in this message.

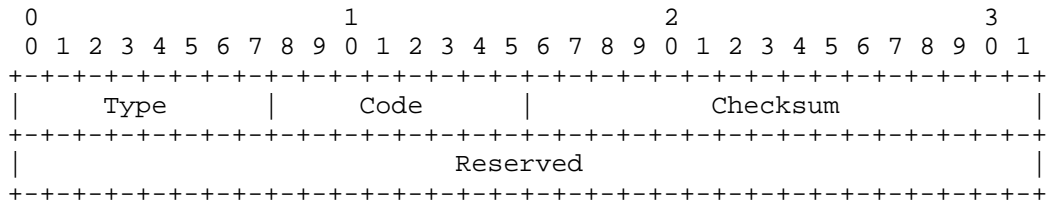   Addr Entry Size   The number of 32-bit words of information
                            per each router address (2, in the version
                            of the protocol described here).

      Lifetime   The maximum number of seconds that the
                            router addresses may be considered valid.

      Router Address[i],   The sending router's IP address(es) on the
       i = 1..Num Addrs   interface from which this message is sent.

      Preference Level[i], The preferability of each Router Address[i]
       i = 1..Num Addrs   as a default router address, relative to
                            other router addresses on the same subnet.
                            A signed, twos-complement value; higher
                            values mean more preferable.

   ICMP Router Solicitation Message

       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 |
      +-+
      | Reserved |
      +-+

   IP Fields:

      Source Address   An IP address belonging to the interface
                            from which this message is sent, or 0.

      Destination Address   The configured SolicitationAddress.

      Time-to-Live   1 if the Destination Address is an IP
                            multicast address; at least 1 otherwise.

   ICMP Fields:

      Type   10

      Code   0

        Checksum   The 16-bit one's complement of the one's
                                  complement sum of the ICMP message, start-
                                  ing with the ICMP Type. For computing the
                                  checksum, the Checksum field is set to 0.

        Reserved   Sent as 0; ignored on reception.

4. Router Specification

4.1. Router Configuration Variables

   A router that implements the ICMP router discovery messages must
   allow for the following variables to be configured by system
   management; default values are specified so as to make it unnecessary
   to configure any of these variables in many cases.

   For each multicast interface:

   AdvertisementAddress
                  The IP destination address to be used for multicast
                  Router Advertisements sent from the interface. The
                  only permissible values are the all-systems multicast
                  address, 224.0.0.1, or the limited-broadcast address,
                  255.255.255.255. (The all-systems address is preferred
                  wherever possible, i.e., on any link where all
                  listening hosts support IP multicast.)

                  Default: 224.0.0.1 if the router supports IP multicast
                  on the interface, else 255.255.255.255

   MaxAdvertisementInterval
                  The maximum time allowed between sending multicast
                  Router Advertisements from the interface, in seconds.
                  Must be no less than 4 seconds and no greater than 1800
                  seconds.

                  Default: 600 seconds

   MinAdvertisementInterval
                  The minimum time allowed between sending unsolicited
                  multicast Router Advertisements from the interface, in
                  seconds. Must be no less than 3 seconds and no greater
                  than MaxAdvertisementInterval.

                  Default: 0.75 * MaxAdvertisementInterval

AdvertisementLifetime
            The value to be placed in the Lifetime field of Router
            Advertisements sent from the interface, in seconds.
            Must be no less than MaxAdvertisementInterval and no
            greater than 9000 seconds.

            Default: 3 * MaxAdvertisementInterval

For each of the router's IP addresses on its multicast interfaces:

Advertise
            A flag indicating whether or not the address is to be
            advertised.

            Default: TRUE

PreferenceLevel
            The preferability of the address as a default router
            address, relative to other router addresses on the same
            subnet. A 32-bit, signed, twos-complement integer,
            with higher values meaning more preferable. The
            minimum value (hex 80000000) is used to indicate that
            the address, even though it may be advertised, is not
            to be used by neighboring hosts as a default router
            address.

            Default: 0

The case in which it is useful to configure an address with a
preference level of hex 80000000 (rather than simply setting its
Advertise flag to FALSE) is when advertisements are being used for
"black hole" detection, as mentioned in Section 2. In particular, a
router that is to be used to reach only specific IP destinations
could advertise its address with a preference level of hex 80000000
(so that neighboring hosts will not use it as a default router for
reaching arbitrary IP destinations) and a non-zero lifetime (so that
neighboring hosts that have been redirected or configured to use it
can detect its failure by timing out the reception of its
advertisements).

It has been suggested that, when the preference level of an address
has not been explicitly configured, a router could set it according
to the metric of the router's "default route" (if it has one), rather
than defaulting it to zero as suggested above. Thus, a router with a
better metric for its default route would advertise a higher
preference level for its address. (Note that routing metrics that
are encoded such that "lower is better" would have to be inverted

before being used as preference levels in Router Advertisement
messages.) Such a strategy might reduce the amount of ICMP Redirect
traffic on some links by making it more likely that a host's first
choice router for reaching an arbitrary destination is also the best
choice. On the other hand, Redirect traffic is rarely a significant
load on a link, and there are some cases where such a strategy would
result in more Redirect traffic, not less (for example, on links from
which the most frequently chosen destinations are best reached via
routers other than the one with the best default route). This
document makes no recommendation concerning this issue, and
implementors are free to try such a strategy, as long as they also
support static configuration of preference levels as specified above.

4.2. Message Validation by Routers

A router must silently discard any received Router Solicitation
messages that do not satisfy the following validity checks:

   - IP Source Address is either 0 or the address of a neighbor
     (i.e., an address that matches one of the router's own
     addresses on the arrival interface, under the subnet mask
     associated with that address.)

   - ICMP Checksum is valid.

   - ICMP Code is 0.

   - ICMP length (derived from the IP length) is 8 or more
     octets.

The contents of the ICMP Reserved field, and of any octets beyond the
first 8, are ignored. Future, backward-compatible changes to the
protocol may specify the contents of the Reserved field or of
additional octets at the end of the message; backward-incompatible
changes may use different Code values.

A solicitation that passes the validity checks is called a "valid
solicitation".

A router may silently discard any received Router Advertisement
messages. Any other action on reception of such messages by a router
(for example, as part of a "peer discovery" process) is beyond the
scope of this document.

4.3. Router Behavior

The router joins the all-routers IP multicast group (224.0.0.2) on
all interfaces on which the router supports IP multicast.

The term "advertising interface" refers to any functioning and
enabled multicast interface that has at least one IP address whose
configured Advertise flag is TRUE. From each advertising interface,
the router transmits periodic, multicast Router Advertisements,
containing the following values:

   - In the destination address field of the IP header: the
     interface's configured AdvertisementAddress.

   - In the Lifetime field: the interface's configured
     AdvertisementLifetime.

   - In the Router Address[i] and Preference Level[i] fields:
     all of the interface's addresses whose Advertise flags are
     TRUE, along with their corresponding PreferenceLevel
     values. (In the unlikely event that not all addresses fit
     in a single advertisement, as constrained by the MTU of the
     link, multiple advertisements are sent, with each except
     the last containing as many addresses as can fit.)

The advertisements are not strictly periodic: the interval between
subsequent transmissions is randomized to reduce the probability of
synchronization with the advertisements from other routers on the
same link. This is done by maintaining a separate transmission
interval timer for each advertising interface. Each time a multicast
advertisement is sent from an interface, that interface's timer is
reset to a uniformly-distributed random value between the interface's
configured MinAdvertisementInterval and MaxAdvertisementInterval;
expiration of the timer causes the next advertisement to be sent from
the interface, and a new random value to be chosen. (It is
recommended that routers include some unique value, such as one of
their IP or link-layer addresses, in the seed used to initialize
their pseudo-random number generators. Although the randomization
range is configured in units of seconds, the actual randomly-chosen
values should not be in units of whole seconds, but rather in units
of the highest available timer resolution.)

For the first few advertisements sent from an interface (up to
MAX_INITIAL_ADVERTISEMENTS), if the randomly chosen interval is
greater than MAX_INITIAL_ADVERT_INTERVAL, the timer should be set to
MAX_INITIAL_ADVERT_INTERVAL instead. Using this smaller interval for
the initial advertisements increases the likelihood of a router being
discovered quickly when it first becomes available, in the presence
of possible packet loss.

In addition to the periodic, unsolicited advertisements, a router
sends advertisements in response to valid solicitations received on
any of its advertising interfaces. A router may choose to unicast

the response directly to the soliciting host's address (if it is not
zero), or multicast it to the interface's configured
AdvertisementAddress; in the latter case, the interface's interval
timer is reset to a new random value, as with unsolicited
advertisements. A unicast response may be delayed, and a multicast
response must be delayed, for a small random interval not greater
than MAX_RESPONSE_DELAY, in order to prevent synchronization with
other responding routers, and to allow multiple, closely-spaced
solicitations to be answered with a single multicast advertisement.

If a router receives a solicitation sent to an IP broadcast address,
on an interface whose configured AdvertisementAddress is an IP
multicast address, the router may send its response to the IP
broadcast address instead of the configured IP multicast address.
Such an event indicates a configuration inconsistency, and should be
logged for possible corrective action by the network administrator.

It should be noted that an interface may become an advertising
interface at times other than system startup, as a result of recovery
from an interface failure or through actions of system management
such as:

   - enabling the interface, if it had been administratively
     disabled and it has one or more addresses whose Advertise
     flag is TRUE, or

   - enabling IP forwarding capability (i.e., changing the
     system from being a host to being a router), when the
     interface has one or more addresses whose Advertise flag is
     TRUE, or

   - setting the Advertise flag of one or more of the
     interface's addresses to TRUE (or adding a new address with
     a TRUE Advertise flag), when previously the interface had
     no address whose Advertise flag was TRUE.

In such cases, the router must commence transmission of periodic
advertisements on the new advertising interface, limiting the first few
advertisements to intervals no greater than MAX_INITIAL_ADVERT_INTERVAL.
In the case of a host becoming a router, the system must also join the
all-routers IP multicast group on all interfaces on which the router
supports IP multicast (whether or not they are advertising interfaces).

An interface may also cease to be an advertising interface, through
actions of system management such as:

   - administratively disabling the interface,

          - shutting down the system, or disabling the IP forwarding
            capability (i.e., changing the system from being a router
            to being a host), or

          - setting the Advertise flags of all of the interface's
            addresses to FALSE.

   In such cases, it is recommended (but not required) that the router
   transmit a final multicast advertisement on the interface, identical
   to its previous transmission but with a Lifetime field of zero.   In
   the case of a router becoming a host, the system must also depart
   from the all-routers IP multicast group on all interfaces on which
   the router supports IP multicast (whether or not they had been
   advertising interfaces).

   When the Advertise flag of one or more of an interface's addresses
   are set to FALSE by system management, but there remain other
   addresses on that interface whose Advertise flags are TRUE, it is
   recommended that the router send a single multicast advertisement
   containing only those address whose Advertise flags were set to
   FALSE, with a Lifetime field of zero.

5. Host Specification

5.1. Host Configuration Variables

   A host that implements the ICMP router discovery messages must allow
   for the following variables to be configured by system management;
   default values are specified so as to make it unnecessary to
   configure any of these variables in many cases.

   For each multicast interface:

   PerformRouterDiscovery
               A flag indicating whether or not the host is to perform
               ICMP router discovery on the interface.

               Default: TRUE

   SolicitationAddress
               The IP destination address to be used for sending
               Router Solicitations from the interface.   The only
               permissible values are the all-routers multicast
               address, 224.0.0.2, or the limited-broadcast address,
               255.255.255.255.   (The all-routers address is preferred
               wherever possible, i.e., on any link where all
               advertising routers support IP multicast.)

                    Default: 224.0.0.2 if the host supports IP multicast on
                    the interface, else 255.255.255.255

   The Host Requirements -- Communication Layers RFC [1], Section
   3.3.1.6, specifies that each host implementation must support a
   configurable list of default router addresses. The purpose of the
   ICMP router discovery messages is to eliminate the need to configure
   that list in hosts attached to multicast links. On non-multicast
   links, and on multicast links for which ICMP router discovery is not
   (yet) supported by the routers or is administratively disabled, it
   will continue to be necessary to configure the default router list in
   each host. Each entry in the list contains (at least) the following
   configurable variables:

   RouterAddress
                    An IP address of a default router.

                    Default: (none)

   PreferenceLevel
                    The preferability of the RouterAddress as a default
                    router address, relative to other router addresses on
                    the same subnet. The Host Requirements RFC does not
                    specify how this value is to be encoded; to allow the
                    preference level to be conveyed in a Router
                    Advertisement or configured by system management, it is
                    here specified that it be encoded as a 32-bit, signed,
                    twos-complement integer, with higher values meaning
                    more preferable. The minimum value (hex 80000000) is
                    reserved to mean that the address is not to be used as
                    a default router address, i.e., it is to be used only
                    for specific IP destinations, of which the host has
                    been informed by ICMP Redirect or configuration.

                    Default: 0

5.2. Message Validation by Hosts

   A host must silently discard any received Router Advertisement
   messages that do not satisfy the following validity checks:

      - ICMP Checksum is valid.

      - ICMP Code is 0.

      - ICMP Num Addrs is greater than or equal to 1.

      - ICMP Addr Entry Size is greater than or equal to 2.

          - ICMP length (derived from the IP length) is greater than or
            equal to 8 + (Num Addrs * Addr Entry Size * 4) octets.

     The contents of any additional words of per-address information
     (i.e., other than the Router Address and Preference Level fields),
     and the contents of any octets beyond the first 8 + (Num Addrs * Addr
     Entry Size * 4) octets, are ignored. Future, backward-compatible
     changes to the protocol may specify additional per-address
     information words, or additional octets at the end of the message;
     backward-incompatible changes may use different Code values.

     An advertisement that passes the validity checks is called a "valid
     advertisement".

     A host must silently discard any received Router Solicitation
     messages.

5.3. Host Behavior

     On any interface on which the host supports IP multicast, the host
     will be a member of the all-systems IP multicast group (224.0.0.1).
     This occurs automatically, as specified in [4]; no explicit action is
     required on the part of the router discovery protocol implementation.

     A host never sends a Router Advertisement message.

     A host silently discards any Router Advertisement message that
     arrives on an interface for which the host's configured
     PerformRouterDiscovery flag is FALSE, and it never sends a Router
     Solicitation on such an interface.

     A host cannot process an advertisement until it has determined its
     own IP address(es) and subnet mask(s) for the interface on which the
     advertisement is received. (On some links, a host may be able to use
     some combination of BOOTP [3], RARP [5], or ICMP Address Mask
     messages [7] to discover its own address and mask.) While waiting to
     learn the address and mask of an interface, a host may save any valid
     advertisements received on that interface for later processing; this
     allows router discovery and address/mask discovery to proceed in
     parallel.

     To process an advertisement, a host scans the list of router
     addresses contained in it. It ignores any non-neighboring addresses,
     i.e., addresses that do not match one of the host's own addresses on
     the arrival interface, under the subnet mask associated with that
     address. For each neighboring address, the host does the following:

        - If the address is not already present in the host's default

router list, a new entry is added to the list, containing
the address along with its accompanying preference level
and a timer initialized to the Lifetime value from the
advertisement.

- If the address is already present in the host's default
  router list as a result of a previously-received
  advertisement, its preference level is updated and its
  timer is reset to the values in the newly-received
  advertisement.

- If the address is already present in the host's default
  router list as a result of system configuration, no change
  is made to its preference level; there is no timer
  associated with a configured address. (Note that any
  router addresses acquired from the "Gateway" subfield of
  the vendor extensions field of a BOOTP packet [11] are
  considered to be configured addresses; they are assigned
  the default preference level of zero, and they do not have
  an associated timer. Note further that any address found
  in the "giaddr" field of a BOOTP packet [3] identifies a
  BOOTP forwarder which is not necessarily an IP router; such
  an address should not be installed in the host's default
  router list.)

Whenever the timer expires in any entry that was created as a result
of a received advertisement, that entry is discarded.

To limit the storage needed for the default router list, a host may
choose not to store all of the router addresses discovered via
advertisements. If so, the host should discard those addresses with
lower preference levels in favor of those with higher levels. It is
desirable to retain more than one default router address in the list
so that, if the current choice of default router is discovered to be
down, the host may immediately choose another default router, without
having to wait for the next advertisement to arrive.

Any router address advertised with a preference level of hex 80000000
is not to be used by the host as default router address; such an
address may be omitted from the default router list, unless its timer
is being use as a "black-hole" detection mechanism, as discussed in
Section 4.1.

It should be understood that preference levels learned from
advertisements do not affect any of the host's cached route entries.
For example, if the host has been redirected to use a particular
router address to reach a specific IP destination, it continues to
use that router address for that destination, even if it discovers

another router address with a higher preference level. Preference
levels influence the choice of router only for an IP destination for
which there is no cached or configured route, or whose cached route
points to a router that is subsequently discovered to be dead or
unreachable.

A host is permitted (but not required) to transmit up to
MAX_SOLICITATIONS Router Solicitation messages from any of its
multicast interfaces after any of the following events:

   - The interface is initialized at system startup time.

   - The interface is reinitialized after a temporary interface
     failure or after being temporarily disabled by system
     management.

   - The system changes from being a router to being a host, by
     having its IP forwarding capability turned off by system
     management.

   - The PerformRouterDiscovery flag for the interface is
     changed from FALSE to TRUE by system management.

The IP destination address of the solicitations is the configured
SolicitationAddress for the interface. The IP source address may
contain zero if the host has not yet determined an address for the
interface; otherwise it contains one of the interface's addresses.

If a host does choose to send a solicitation after one of the above
events, it should delay that transmission for a random amount of time
between 0 and MAX_SOLICITATION_DELAY. This serves to alleviate
congestion when many hosts start up on a link at the same time, such
as might happen after recovery from a power failure. (It is
recommended that hosts include some unique value, such as one of
their IP or link-layer addresses, in the seed used to initialize
their pseudo-random number generators. Although the randomization
range is specified in units of seconds, the actual randomly-chosen
value should not be in units of whole seconds, but rather in units of
the highest available timer resolution.)

A host may also choose to further postpone its solicitations,
subsequent to one of the above events, until the first time it needs
to use a default router.

Upon receiving a valid advertisement containing at least one
neighboring address whose preference level is other than hex
80000000, subsequent to one of the above events, the host must desist
from sending any solicitations on that interface (even if none have

been sent yet), until the next time one of the above events occurs.
The small number of retransmissions of a solicitation, which are
permitted if no such advertisement is received, should be sent at
intervals of SOLICITATION_INTERVAL seconds, without randomization.

6. Protocol Constants

   Router constants:

        MAX_INITIAL_ADVERT_INTERVAL   16 seconds

        MAX_INITIAL_ADVERTISEMENTS   3 transmissions

        MAX_RESPONSE_DELAY   2 seconds

   Host constants:

        MAX_SOLICITATION_DELAY   1 second

        SOLICITATION_INTERVAL   3 seconds

        MAX_SOLICITATIONS   3 transmissions

   Additional protocol constants are defined with the message formats in
   Section 3, and with the router and host configuration variables in
   Sections 4.1 and 5.1.

   All protocol constants are subject to change in future revisions of
   the protocol.

7. Security Considerations

   This extension of ICMP makes it possible for any system attached to a
   link to masquerade as a default router for hosts attached to that
   link. Any traffic sent to such an imposter is vulnerable to
   eavesdropping, to denial of forwarding service, and to modification
   by insertion, deletion, or alteration of packets. It should be noted
   that, on most multicast or broadcast links on which this protocol is
   expected to operate, eavesdropping is already possible by any system
   attached to the link, and the Address Resolution Protocol (ARP) used
   on those links offers a similar opportunity for service denial and
   message stream modification. For environments where those threats
   are deemed unacceptable, there are configuration variables to disable
   dynamic router discovery by hosts.

   The Router Advertisement message format is defined so as to allow
   additional information to be added to the message in a backward-
   compatible manner. One possible use of that capability is to add

digital signatures or some other form of authentication information
to the advertisements, to enable hosts to verify their authenticity.
This is FOR FURTHER STUDY.

References

   [1] Braden, R., Editor, "Requirements for Internet Hosts --
       Communication Layers", RFC 1122, USC/Information Sciences
       Institute, October 1989.

   [2] Braden, R., and J. Postel, "Requirements for Internet Gateways",
       RFC 1009, USC/Information Sciences Institute, June 1987.

   [3] Croft, B, and J. Gilmore, "Bootstrap Protocol (BOOTP)", RFC 951,
       Stanford and SUN Microsystems, September 1985.

   [4] Deering, S., "Host Extensions for IP Multicasting", RFC 1112,
       Stanford University, August 1989.

   [5] Finlayson, R., Mann, T., Mogul J., and M. Theimer, "A Reverse
       Address Resolution Protocol", RFC 903, Stanford University, June
       1984.

   [6] Mogul, J., "Broadcasting Internet Datagrams", RFC 919, Stanford
       University, October 1984.

   [7] Mogul J., and J. Postel, "Internet Standard Subnetting
       Procedure", RFC 950, USC/Information Sciences Institute, August
       1985.

   [8] Piscitello D., and J. Lawrence, "Transmission of IP datagrams
       over the SMDS Service", RFC 1209, Bell Communications Research,
       March, 1991.

   [9] Postel, J., "Internet Protocol - DARPA Internet Program Protocol
       Specification", RFC 791, DARPA, September 1981.

  [10] Postel, J., "Internet Control Message Protocol - DARPA Internet
       Program Protocol Specification", RFC 792, USC/Information
       Sciences Institute, September 1981.

  [11] Reynolds, J., "BOOTP Vendor Information Extensions", RFC 1084,
       USC/Information Sciences Institute, December 1988.

Author's Address

        Stephen E. Deering
        Xerox Palo Alto Research Center
        3333 Coyote Hill Road
        Palo Alto, CA 94304

        Phone: (415) 494-4839

        EMail: deering@xerox.com

        Or send comments to gw-discovery@gregorio.stanford.edu.