CHAPTER 5

ICMPv6

The ICMPv6 (Internet Control Message Protocol version 6)[1] is an integral part of the IPv6 architecture[2] and must be completely supported by all IPv6 implementations. ICMPv6 combines functions previously subdivided among different protocols, such as ICMP (Internet Control Message Protocol version 4)[3], IGMP (Internet Group Membership Protocol)[4], and ARP (Address Resolution Protocol)[5], and it introduces some simplifications by eliminating obsolete types of messages no longer in use.

In this chapter, we will analyze the protocol's main characteristics and the packet's format, while a more thorough discussion about Neighbor Discovery problems is deferred until Chapter 6.

5.1 Protocol Overview

ICMPv6 (in the following text called *ICMP* for the sake of brevity) is a multipurpose protocol; for example, it is used for reporting errors encountered in processing packets, performing diagnostics, performing Neighbor Discovery, and reporting multicast memberships. For this reason, ICMP messages are subdivided into two classes: *error messages* and *information messages*.

ICMP messages are transported within an IPv6 packet in which extension headers can also be present (see Section 3.2). An ICMP message is identified by a value of 58 in the Next Header field of the IPv6 header or of the preceding Header (see Table 3-2).

5.2 Packets Format

ICMPv6 packets have the format shown in Figure 5-1.

The 8-bit *Type* field indicates the type of the message. If the high-order bit has value zero (values in the range from 0 to 127), it is an error message; if the high-order bit has value 1 (values in the range from 128 to 255), it is an information message. A list of currently defined message types is shown in Table 5-1.

The 8-bit *Code* field content depends on the message type, and it is used to create an additional level of message granularity.

The *Checksum* field is used to detect errors in the ICMP message and in part of the IPv6 message.

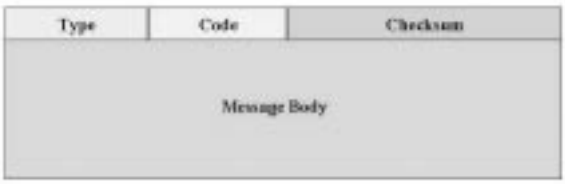

Figure 5-1
Format of an ICMPv6 message

Table 5-1

Types of ICMP messages

Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

5.3 ICMP Message Transmission

A node that forwards an ICMP message has to determine both the source and the destination IPv6 addresses for the ICMP message. Particular care must be put into the choice of the source address. If a node has more than one unicast address, it must choose the source address of the message as follows:

- If the message is a response to a message sent to one of the node unicast addresses, the Source Address of the reply must be that same address.
- If the message is a response to a message sent to a multicast or anycast group to which the node belongs, the Source Address of the reply must be a unicast address belonging to the interface on which the multicast or anycast packet was received.
- If the message is a response to a message sent to an address that does not belong to the node, the Source Address should be the unicast address belonging to the node that will be the most helpful in

checking the error (for example, the unicast address belonging to the interface on which the packet forwarding failed).

- In other cases, the node routing tables must be examined (see Section 2.6) to determine which interface will be used to transmit the message to its destination, and the unicast address belonging to that interface must be used as the Source Address of the message.

When an ICMP node receives a packet, it must undertake actions that depend on the type of message. A more detailed discussion is beyond the aim of this book. Refer to Section A.3 in Appendix A for an excerpt from RFC 1885 [1] dealing with this subject.

Moreover, the ICMP protocol must limit the number of error messages sent to the same destination to avoid network overloading. For example, if a node continues to forward erroneous packets, ICMP will signal the error to the first packet and then do so periodically, with a fixed minimum period or with a fixed network maximum load.

An ICMP error message must never be sent in response to another ICMP error message.

5.4 Error Messages

ICMPv6 error messages are similar to ICMPv4 error messages. They belong to four categories: Destination Unreachable, Packet Too Big, Time Exceeded, and Parameter Problems. We will analyze them further in the following subsections.

5.4.1 Destination Unreachable

The *Destination Unreachable* message, which is illustrated in Figure 5-2, is generated when the network must discard an IPv6 packet because the destination is unreachable. The IPv6 destination address of the ICMP packet is therefore the source address of the discarded packet.

The *Type* field value is 1.

The *Code* field can assume values reported in Table 5-2.

The *Unused* field, of course, is not used; it is initialized to zero during the transmission and ignored on reception.

The first part of the IPv6 packet that caused the generation of the ICMP packet follows. Because being able to transmit the ICMP packet on

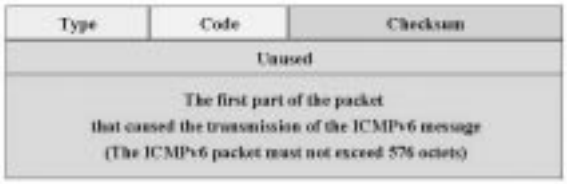

Figure 5-2
Destination Unreachable message

any link must be possible (see Section 3.3), the packet must not exceed 576 octets (the IPv6 header and eventual extension headers included).

This type of message can be generated either by a router or by a destination node that cannot deliver the message; the router or node is therefore forced to discard the message. A packet is dropped without generating a message of this type only when the network is congested; generating ICMP messages will make the congestion worse.

The reasons for the failure in delivering a packet are as follow:

- *No route to destination:* A router cannot find a matching entry for the destination address in its routing table, and therefore it doesn't know on which interface to retransmit the packet.
- *Communication with destination administratively prohibited:* The message is dropped by a firewall—that is, by a router that contains a set of rules that forbid some communications.
- *Not a neighbor:* The message contains a Routing header, the next destination address has the Strict / Loose bit equal to Strict, and the next destination address doesn't belong to any of the router links (it is not a neighbor).
- *Address unreachable:* The destination address is unreachable for other reasons—for example, for an interface error or for the inability to compute the link layer address of the destination node.
- *Port unreachable:* The packet reached the destination node, but the layer 4 protocol (for example, UDP) to which the packet should be delivered (the port) is unreachable.

5.4.2 Packet Too Big

The *Packet Too Big* message, which is illustrated in Figure 5-3, is generated when the network must discard an IPv6 packet because its size exceeds the MTU of the outgoing link. The information contained in the ICMP packet is used as part of the Path MTU Discovery procedure. The

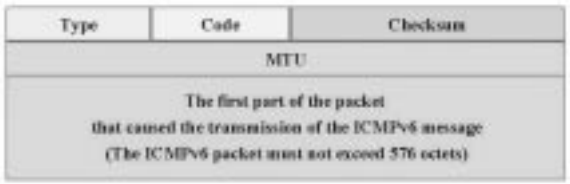

Figure 5-3
Packet Too Big message

Table 5-2
Destination Unreachable: Code

Code	Meaning
0	No route to destination
1	Communication with destination administratively prohibited
2	Not a neighbor
3	Address unreachable
4	Port unreachable

IPv6 destination address of the ICMP packet is therefore the source address of the dropped packet.

The *Type* field has value 2.

The *Code* field always has value zero.

The 32-bit *MTU* field indicates the MTU of the link on which transmitting the packet was impossible.

The first part of the IPv6 packet that caused the ICMP packet follows. Because being able to transmit the ICMP packet on any link must be possible (see Section 3.3), the packet must not exceed 576 octets (the IPv6 header and eventual extension headers included).

5.4.3 Time Exceeded

The *Time Exceeded* message, which is illustrated in Figure 5-4, is generated when a router must discard an IPv6 packet because its Hop Limit field (see Section 3.1.6) is zero or decrements to zero. This message indicates that either a routing loop or an initial Hop Limit value is too small. Another reason is the impossibility to reassemble a fragmented packet within the allowed time limit. The IPv6 destination address of the ICMP packet is therefore the source address of the dropped packet.

The *Type* field has value 3.

The *Code* field can have the values reported in Table 5-3.

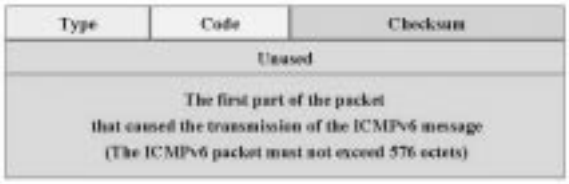

Figure 5-4
Time Exceeded message

Table 5-3
Time Exceeded: Code field values

Code	Meaning
0	Hop limit exceeded in transit
1	Fragment reassembly time exceeded

The *Unused* field is unused for all code values, and it must be initialized to zero by the sender and ignored by the receiver.

The first part of the IPv6 packet that caused the ICMP packet follows. Because being able to transmit the ICMP packet on any link must be possible (see Section 3.3), the packet must not exceed 576 octets (the IPv6 header and eventual extension headers included).

5.4.4 Parameter Problems

The *Parameter Problem* message, which is illustrated in Figure 5-5, is generated when an IPv6 node must discard a packet because it detects problems in a field of the IPv6 header or of an extension header. The IPv6 destination address of the ICMP packet is therefore the source address of the dropped packet.

The *Type* field has value 4.

The *Code* field can have the three values reported in Table 5-4.

The *Pointer* field identifies the octet in the original message where the error was detected.

The first part of the IPv6 packet that caused the ICMP packet follows. Because being able to transmit the ICMP packet on any link must be possible (see Section 3.3), the packet must not exceed 576 octets (the IPv6 header and eventual extension headers included).

The following three errors can be detected:

- *Erroneous header field:* A field in a header holding an illegal value has been detected.

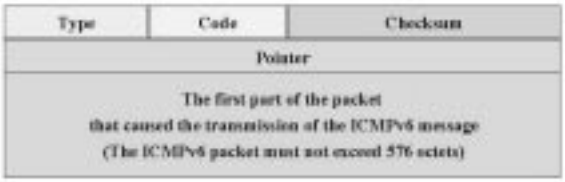

Figure 5-5
Parameter Problem message

- *Unrecognized Next Header*: A Next Header is unrecognized for the IPv6 implementation present on the node.
- *Unrecognized IPv6 option*: The packet holds an unrecognized option (see Section 3.2.2) for the IPv6 implementation present on the node.

5.5 Informational Messages

A second type of ICMP message is the informational message. These messages are subdivided into three groups: diagnostic messages, messages for the management of multicast groups, and Neighbor Discovery messages.

5.5.1 Echo Request Message

The *Echo Request* message and its corresponding *Echo Reply* message are ICMP diagnostic messages. In particular, these two messages are used to implement the `ping` diagnostic application that allows us to test whether a destination is reachable. The format of these two messages is the same, as illustrated in Figure 5-6. The IPv6 destination address can be any valid IPv6 address.

The *Type* field has value 129.

The *Code* field has value zero.

The *Identifier* field is an identifier used to set a relationship between Echo Request and Echo Reply messages. It can also be set to zero.

The *Sequence Number* field is a sequence number used to set a relationship between Echo Request and Echo Reply messages. It can also be set to zero.

The *Data* field contains zero or more octets of data arbitrarily generated by the diagnostic procedure.

Table 5-4

Parameter Problem: Code field values

Code	Meaning
0	Erroneous header field
1	Unrecognized Next Header
2	Unrecognized IPv6 option

5.5.2 Echo Reply Message

Every IPv6 node must implement an ICMP Echo reply function that receives Echo requests and sends corresponding Echo replies, whose format is illustrated in Figure 5-6. The IPv6 destination address is set equal to the IPv6 source address of the Echo Request message.

The *Type* field has value 129.

The *Code* field has value zero.

The *Identifier* field is copied from the field of the same name in the Echo Request message.

The *Sequence Number* field is copied from the field of the same name in the Echo Request message.

The *Data* field is copied from the field of the same name in the Echo Request message.

An example of this type of packet is shown in Section B.2 in Appendix B.

5.5.3 Group Membership Messages

ICMP Group Membership messages are used to convey information about multicast group membership from nodes to their neighboring routers (connected on the same link). Their format is illustrated in Figure 5-7.

The IPv6 destination address values change in function for the different types of messages:

- In a *Group Membership Query* message, the destination address is equal to the multicast address of the group being queried or equal to the link local All-Nodes (FF02::1, see Section 4.8.1) multicast address.
- In a *Group Membership Report* or *Group Membership Reduction* message, the destination address is equal to the multicast address of the group being reported or terminated.

Figure 5-6
Echo Request and Echo Reply messages

Figure 5-7
Group Membership message

The IPv6 header *Hop Limit* field is set to 1 (packets are exchanged only between adjacent nodes).

The *Type* field assumes values 130 (Group Membership Query), 131 (Group Membership Report), or 132 (Group Membership Reduction).

The *Code* field has value zero.

The *Maximum Response Delay* field expresses a value in milliseconds. In Group Membership Query messages, this field indicates the maximum time that the responding Report messages can be delayed. In Group Membership Report or Group Membership Reduction messages, this field is initialized to zero by the sender and ignored by the receiver.

The *Unused* field is unused and must be initialized to zero by the sender and ignored by the receiver.

5.5.4 Router Solicitation Message

ICMP messages that will be introduced from this point to the end of the chapter are messages of Neighbor Discovery type (specified by RFC 1970[6]). We discussed the need and use of these types of messages in Section 2.8. In this section, we will analyze formats of different messages in more detail.

IPv6 nodes transmit *Router Solicitation* messages (see Figure 5-8) to prompt routers to generate Router Advertisements immediately.

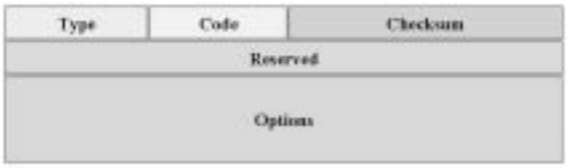

Figure 5-8
Router Solicitation message format

The source address of a Router Solicitation message is either the unicast address of the interface from which the message is sent or, if this address doesn't exist, the unspecified address. The destination address is typically the All-Router (FF02::2) multicast group.

The *Hop Limit* field of the IPv6 header is set to 255. This setting is a form of protection against attack from hackers. In fact, routers verify that this field has value 255, and if not, they discard the packet. A hacker could never forward a message with the Hop Limit equal to 255 from outside the LAN because the router will decrement it by one. Only packets really generated on the LAN can have a Hop Limit equal to 255.

The *Priority* field of the IPv6 header is set to 15.

The *Type* field is equal to 133.

The *Code* field is equal to zero.

The *Reserved* field is unused; it must be initialized to zero during transmission and ignored on reception.

In the *Options* field can appear the option carrying the layer 2 (link layer) address of the source node, if known (see Section 5.5.10).

An example of this kind of packet is shown in Section B.5 of Appendix B.

5.5.5 Router Advertisement Message

Routers send out Router Advertisement messages periodically or in response to Router Solicitation messages. The format of *Router Advertisement* messages is illustrated in Figure 5-9.

The IPv6 source address is set equal to the link local address of the interface from which the message is sent, and the destination address is equal either to the address of the node that solicited the message or to the All-Node multicast address (FF02::1).

The *Hop Limit* field of the IPv6 header is set to 255 (see Section 5.5.4).

The *Priority* field of the IPv6 header is set to 15.

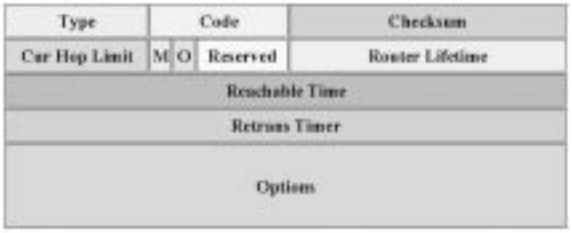

Figure 5-9
Router Advertisement message format

The *Type* field is equal to 134.

The *Code* field is equal to zero.

The 8-bit *Cur Hop Limit* field specifies, to nodes that receive the Advertisement, the default value for the Hop Limit field of the IPv6 header to be used during packet transmission. A value of zero means that the sender's router doesn't suggest any default.

The 1-bit *M* (Managed address configuration) field, when set, indicates to nodes that receive the Advertisement that they must use the stateful protocol (see Section 6.7.3) for address autoconfiguration in addition to the stateless address autoconfiguration.

The 1-bit *O* (Other Stateful configuration) field, when set, indicates to nodes that receive the Advertisement that they must use the stateful autoconfiguration protocol for additional information.

The *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 16-bit *Router Lifetime* field contains the period of time in seconds for which the router can be used as the default router by receiving nodes. If this field is equal to zero, the router cannot be used as the default router.

The 32-bit *Reachable Time* field contains the time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. This parameter is used by the Neighbor Unreachability Detection algorithm (see Section 6.6).

The 32-bit *Retrans Timer* field contains the time, in milliseconds, between retransmitted Neighbor Solicitation messages. It is used by address resolution and Neighbor Unreachability Detection algorithms.

The following options can be present in the *Options* field:

- The option that specifies the layer 2 (link layer) address of the source node, if known (see Section 5.5.10).
- The option that specifies the link MTU (see Section 5.5.13).

- The Prefix Information option that specifies prefixes to be used for the address autoconfiguration (see Section 5.5.11). A router should include all its on-link prefixes (except the link local prefix) so that multihomed hosts will correctly autoconfigure themselves.

An example of this type of packet is shown in Section B.6 of Appendix B.

5.5.6 Neighbor Solicitation Message

IPv6 nodes transmit *Neighbor Solicitation* messages (see Figure 5-10) to request link layer addresses of Target nodes, while also providing the Target with its own link layer address. Neighbor Solicitation messages are sent to multicast addresses (see Section 4.8.1) when a node needs to resolve an address (from IPv6 to link layer) or to unicast addresses when a node seeks to verify the reachability of a neighbor.

The source address of a Neighbor Solicitation message is either the unicast address of the interface that transmits the message or, during the Duplicate Address Detection procedure (see Section 6.7.4), the unspecified address.

The *Hop Limit* field of the IPv6 header is set to 255 (see Section 5.5.4).

The *Priority* field of the IPv6 header is set to 15.

The *Type* field is equal to 135.

The *Code* field is equal to zero.

The *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 128-bit *Target Address* field specifies the Target node address—that is, the IPv6 address of the node to which the Neighbor Solicitation message is sent.

In the *Options* field can be present the option that specifies the link layer address of the source, if known (see Section 5.5.10).

An example of this type of packet is shown in Section B.7 of Appendix B.

Figure 5-10
Format of the Neighbor Solicitation message

5.5.7 Neighbor Advertisement Message

When the state of a node changes, it forwards a Neighbor Advertisement message (see Figure 5-11) to propagate modifications quickly and in response to a Neighbor Solicitation message.

The source IPv6 address field is set equal to the address of the interface from which the message is sent, and the destination address is equal either to the address of the node that solicited the message or to the All-Node (FF02::1) multicast address.

The *Hop Limit* field of the IPv6 header is set equal to 255 (see Section 5.5.4).

The *Priority* field of the IPv6 header is set equal to 15.

The *Type* field is set equal to 136.

The *Code* field is equal to zero.

The 1-bit *R* (Router flag) field indicates, if set, that the source node is a router.

The 1-bit *S* (Solicited flag) field indicates, if set, that the message has been sent as a reply to a Neighbor Solicitation message.

The 1-bit *O* (Override flag) field indicates, when set, that the message should update the cached link layer address.

The 29-bit *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 128-bit *Target Address* field specifies, for solicited advertisements, the address of the node that prompted this advertisement. For unsolicited advertisements, this field specifies the IPv6 address whose link layer address has changed.

The *Options* field can contain the option specifying the Target Link Layer Address—that is, the link layer address of the node that sent the Neighbor Advertisement (see Section 5.5.10).

An example of this type of packet is shown in Section B.8 of Appendix B.

5.5.8 Redirect Message

Routers transmit *Redirect* messages to inform other nodes of a better first hop toward a destination. Hosts can be redirected to another router connected to the same link, but more commonly to another neighbor (this can be obtained by setting the Redirect message Target Address field and the

Figure 5-11
Format of the Neighbor Advertisement message

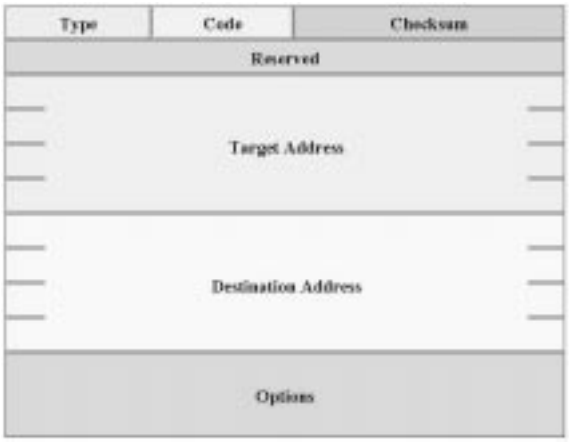

Figure 5-12
Format of the Redirect message

Destination Address field to the same value). The format of the Redirect message is illustrated in Figure 5-12.

The IPv6 source address field is equal to the link local address of the interface from which the message is sent, and the destination address is equal to the source address of the packet that caused the Redirect message.

The *Hop Limit* field of the IPv6 header is set equal to 255 (see Section 5.5.4).

The *Priority* field of the IPv6 header is set equal to 15.

The *Type* field is equal to 137.

The *Code* field is equal to zero.

The *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 128-bit *Target Address* field contains, for solicited messages, the address of the node that solicited the response. When the Target Address is the endpoint of a communication—that is, the destination is a neighbor—the Target Address field must contain the same value as the Destination Address field. Otherwise, the Target Address is the link local address of a better first hop router toward the destination.

The 128-bit *Destination Address* contains the IPv6 address of the destination that is redirected to the Target Address.

In the *Options* field, the following options can appear:

- The option containing the link layer address of the Target Address, if known (see Section 5.5.10).
- The Redirect header—that is, the option containing the initial part of the packet that caused the Redirect message, truncated so that the ICMP packet doesn't exceed 576 octets (see Section 5.5.12).

5.5.9 Options Format

Neighbor Discovery messages can include zero, one, or more options. Some options can appear multiple times in the same message. All options have the general format illustrated in Figure 5-13.

The 8-bit *Type* field specifies the option type, coded as described in Table 5-5.

The 8-bit *Length* field specifies the option length in units of 8 octets. The value zero is invalid, so nodes that receive a Neighbor Discovery packet that contains an option with length zero must discard it.

5.5.10 Source/Target Link Layer Address Option

Type 1 (*Source Link Layer Address*) and type 2 (*Target Link Layer Address*) options have an identical format; they are illustrated in Figure 5-14.

The link layer address is a layer 2 address with variable length. The minimum length (Length = 1) reserves 48 bits for the link layer address; this length is ideal to transport the MAC address on LANs.

Figure 5-13
Options format

Table 5-5
Type field possible values

Type	Option Name
1	Source Link Layer Address
2	Target Link Layer Address
3	Prefix Information
4	Redirect Header
5	MTU

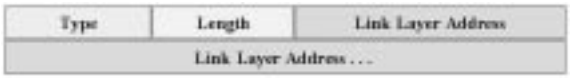

Figure 5-14
Format of Source / Target Link Layer Address option

The Source Link Layer Address option contains the link layer address of the sender of the packet. This option is used in Router Solicitation, Router Advertisement, and Neighbor Solicitation messages.

The Target Link Layer Address contains the link layer address of the target. This option is used in Neighbor Advertisement and Redirect messages.

5.5.11 Prefix Information Option

The *Prefix Information* option provide hosts with on-link prefixes for address autoconfiguration. The format of the Prefix Information option is illustrated in Figure 5-15.

The 8-bit *Prefix Length* field contains the prefix length. Valid values range from 0 to 128.

The 1-bit *L* (on-Link flag) field indicates, if set, that the prefix can be used for on-link determination—that is, all addresses belonging to that prefix are on the link. When this field is not set, some addresses can be on-link and others off-link (outside the link).

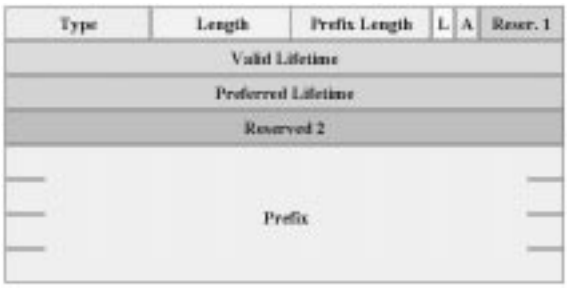

Figure 5-15
Format of the Prefix Information option

The 1-bit *A* (Autonomous address configuration flag) field indicates, if set, that the prefix can be used for autonomous address configuration.

The 6-bit *Reser. 1* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 32-bit *Valid Lifetime* field contains the number of seconds that the address generated from the prefix via stateless autoconfiguration remains valid. The hexadecimal value FFFFFFFF represents infinity.

The 32-bit *Preferred Lifetime* field contains the number of seconds that an address generated from the prefix via stateless autoconfiguration remains preferred. The hexadecimal value FFFFFFFF represents infinity.

The 32-bit *Reserved 2* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 128-bit *Prefix* field contains an IPv6 address or a prefix of an IPv6 address. Only first Prefix Length bits are significant, so others must be ignored and initialized to zero.

5.5.12 Redirect Header Option

The *Redirect Header* option is used in ICMP Redirect packets to contain the first part of the message that caused the request of redirection. The Redirect Header option format is shown in Figure 5-16.

The 48-bit *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The *IP header + data* field contains the packet that generated the redirect message. The original packet is truncated to ensure that the size of the redirect message does not exceed 576 octets.

Figure 5-16
Format of the Redirect Header option

Figure 5-17
Format of the MTU option

5.5.13 MTU Option

The *MTU* option is used in Router Advertisement messages to ensure that, on links with variable MTU values, all nodes use the same MTU value. The format of the MTU option is illustrated in Figure 5-17.

The 16-bit *Reserved* field is unused; it must be initialized to zero by the sender and ignored by the receiver.

The 32-bit *Maximum Transmission Unit* (MTU) field contains the recommended MTU for the link.

REFERENCES

[1]A. Conta, S. Deering, RFC 1885: Internet Control Message Protocol (ICMPv6), December 1995.

[2]S. Deering, R. Hinden, RFC 1883: Internet Protocol, Version 6 (IPv6) Specification, December 1995.

[3]J. Postel, *RFC 792: Internet Control Message Protocol*, September 1981.

[4]S.E. Deering, *RFC 1112: Host extensions for IP multicasting*, August 1989.

[5]D.C. Plummer, *RFC 826: Ethernet Address Resolution Protocol: On converting network protocol addresses to 48 bit Ethernet address for transmission on Ethernet hardware*, November 1982.

[6]T. Narten, E. Nordmark, W. Simpson, *RFC 1970: Neighbor Discovery for IP Version 6 (IPv6)*, August 1996.