

中华人民共和国通信行业标准

YD/T 1343-2005

IPv6 邻居发现协议—— 基于 IPv6 的邻居发现协议

Technical specification for neighbor discovery protocol in IPv6

2005-05-11 发布

2005-11-01 实施

中华人民共和国信息产业部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语	2
4 缩略语	4
5 概述	4
6 消息格式	7
6.1 路由器请求消息格式	7
6.2 路由器通告消息格式	8
6.3 邻居请求消息格式	9
6.4 邻居通告消息格式	10
6.5 重定向消息格式	11
6.6 选项格式	12
7 主机模型	15
7.1 数据结构	15
7.2 发送算法	16
7.3 垃圾收集和超时要求	17
8 路由器和前缀发现	17
8.1 消息有效性验证	17
8.2 路由器要求	18
8.3 主机要求	23
9 地址解析和邻居不可达检测	27
9.1 消息有效性	27
9.2 地址解析	28
9.3 邻居不可达性检测	31
10 重定向功能	34
10.1 验证重定向消息	34
10.2 路由器要求	34
10.3 主机要求	35
11 选项处理	35
12 协议常数	36
13 安全性考虑	37
14 重编号的考虑	37

前 言

本标准修改采用 IETF 的 RFC 2461 (1998), 主要差异如下:

1. 按照 GB 1(2000)系列的要求对标准格式进行了修改;
2. 本标准的第 1、2、3、4 章按照 GB 1(2000)系列要求编写, 第 5、6、7、8、9、10、11、12、13、14 章分别等同于 RFC 2461 的第 3、4、5、6、7、8、9、10、11、12 章;

3. RFC 2461 的附录 A、B、C、D、E、F 的内容未在本标准。

本标准是“IPv6 协议”系列标准之一, 该系列标准预计的结构及名称如下:

1. 《IPv6 基本协议——IPv6 协议》
2. 《IP v6 技术要求——支持计算机移动部分》
3. 《IPv6 技术要求——地址、过渡及服务质量》
4. 《IPv6 地址结构协议——IPv6 无状态地址自动配置》
5. 《IPv6 邻居发现协议——基于 IPv6 的邻居发现协议》
6. 《IPv6 协议一致性测试方法》

本标准由中国通信标准化协会提出并归口。

本标准起草单位: 信息产业部电信研究院

本标准主要起草人: 袁 琦 刘 治 李春安 阚志刚 杜和青

IPv6 邻居发现协议——

基于 IPv6 的邻居发现协议

1 范围

本标准规定了IPv6的邻居发现协议，包括路由器和前缀发现、地址解析和邻居不可达检测、重定向等功能要求。本标准规定的功能不直接依赖于组播。

本标准适用于非特殊规定下的链路类型。本标准不适用于在非广播多连接（NBMA）链路上使用的邻居发现机制。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 0768 (1980)	用户数据包协议
IETF RFC 0791 (1981)	互联网协议
IETF RFC 0792 (1981)	互联网控制消息协议
IETF RFC 0793 (1981)	传输控制协议
IETF RFC 0826 (1982)	以太网地址解释协议（ARP）
IETF RFC 0905 (1984)	ISO 传输协议规范 ISO DP 8073
IETF RFC 1191 (1990)	路径 MTU 发现
IETF RFC 1256 (1991)	ICMP 路由器发现消息
IETF RFC 1519 (1993)	无类域间路由（CIDR）：地址分配和聚合策略
IETF RFC 1546 (1993)	主机泛播服务
IETF RFC 1584 (1994)	OSPF 的组播扩展
IETF RFC 1586 (1994)	在帧中继网络运行 OSPF 的要求
IETF RFC 1587 (1994)	OSPF 的 NSSA 选项
IETF RFC 1620 (1994)	在共享媒体上的因特网结构扩展
IETF RFC 1700 (1994)	被分配的号码
IETF RFC 1745 (1994)	基于 IP OSPF 交互的 BGP4/IDRP
IETF RFC 1771 (1995)	边界网关协议 4（BGP4）
IETF RFC 1793 (1995)	OSPF 外部属性 LSA
IETF RFC 1981 (1998)	IPv6 路径 MTU 发现
IETF RFC 2119 (1997)	RFC 中用来指出所需级别的密词组
IETF RFC 2233 (1997)	使用 SMIPv2 的接口组 MIB

IETF RFC 2328 (1998)	OSPF2 开放式最短路径优先 (版本 2)
IETF RFC 2373 (1998)	IPv6 地址结构
IETF RFC 2401 (1998)	因特网协议的安全体系
IETF RFC 2402 (1998)	IP 认证头
IETF RFC 2406 (1998)	IP 封装安全净荷
IETF RFC 2460 (1998)	IPv6 协议
IETF RFC 2461 (1998)	IPv6 邻居发现协议
IETF RFC 2462 (1998)	IPv6 地址自动配置
IETF RFC 2463 (1998)	IPv6 互联网控制消息协议
IETF RFC 2464 (1998)	IPv6 数据包在以太网网络上的传输

3 术语

下列术语和定义适用于本标准。

3.1

节点 node

实现 IP 协议的设备, 包括主机和路由器。

3.2

泛播地址 anycast address

一组接口的标识符(一般属于不同节点)。发送到泛播地址的数据包会发送到由这个地址标识的一个接口(根据路由协议的距离量度为最近的一个接口)。

3.3

前缀 prefix

由地址的初始比特位构成的比特串。

3.4

在连接 on-link

分配给特定链路上接口的地址, 如果满足下列条件, 节点认为地址是在连接:

- 它被一个链路前缀覆盖;
- 邻居路由指定地址为重定向消息的目标;
- 接收(目标)地址的邻居通告消息;
- 接收来自地址的邻居发现消息。

3.5

非连接 offlink

在连接的反义词。没有分配给特定链路上任何接口的地址。

3.6

最长前缀匹配 longest prefix match

确定前缀集合中哪个前缀覆盖目标地址的过程。如果前缀的比特位和目标地址的比特位从左最大匹

配，前缀就覆盖这个目标地址，当多个前缀覆盖一个地址时，具有最长前缀的地址将得到匹配。

3.7

可达性 reachability

到达邻居的单向转发路径是否工作正常，发送给邻居的包是否到达邻居的 IP 层，是否被接收的 IP 层正确处理。对于邻居路由器，可达性是指节点的 IP 层发送的包发送到路由器的 IP 层，并且路由器确实转发了数据包（即它配置为路由器而不是主机）；对于主机，可达性是指节点的 IP 层发送的包发送到邻居主机的 IP 层。

3.8

链路 MTU link MTU

最大传输单元，即在链路上一次所能传输的最大数据包大小（以字节为单位）。

3.9

目标地址 target

地址解析所解析出的地址，或重定向时新的第一跳地址。

3.10

代理 proxy

代表另一个节点而响应邻居发现查询消息的路由器。当移动节点离开 off-link 状态时，就为移动节点作代理。

3.11

ICMP 目的地不可达指示 ICMP destination unreachable indication

返回到原始发送者的出错指示。如果某节点发生错误，而不是初始发送包的节点发生错误，则产生一个 ICMP 错误消息。如果出错发生在发送节点，并通知了上层发送者，不要求向源发送一个 ICMP 错误消息。

3.12

随机时延 random delay

当发送消息时，为了防止多个节点同时传输，或者防止周期性的传送消息而造成与其他节点同步，需要把一个传输延迟一段时间。随机时延在最小和最大时延值之间呈均匀分布。

3.13

非对称可达性 asymmetric reachability

非自反或非传递可达性的链路。非自反可达性是指数据包能从 A 到 B，但不能从 B 到 A；非传递可达性是指数据包能从 A 到 B，从 B 到 C，但数据包不能从 A 到 C。许多无线链路具有这种特性。

3.14

全部节点组播地址 all-nodes multicast address

到达所有节点的本地链路范围地址：FF02::1。

3.15

全部路由器组播地址 all-routers multicast address

到达所有路由器的本地链路范围地址：FF02::1。

3.16

请求节点组播地址 solicited-node multicast address

链路本地范围的组播地址。

3.17

链路本地地址 link-local address

用于到达邻居，仅有链路范围的单播地址；路由器的所有接口必须有本地链路地址，主机的接口也要求有本地链路地址。

3.18

未规定的地址 unspecified address

保留的地址值，表示没有地址（例如，地址未知）；不能用作目的地地址，如果发送者不知道自己的地址，可以用作源地址（例如，在地址自动配置期间没有使用地址）。未规定的地址值为 0:0:0:0:0:0:0:0。

4 缩略语

下列缩略语适用于本标准。

AH	Authentication Header	认证头
ARP	Address Resolution Protocol	地址解析协议
AS	Autonomous System	自治系统
ESP	Encapsulating Security Payload	封装安全载荷
ICMP	Internet Control Message Protocol	互联网控制消息协议
IP	Internet Protocol	互联网协议
IPv4	Internet Protocol v4	互联网协议版本 4
IPv6	Internet Protocol v6	互联网协议版本 6
MTU	Maximum Transmission Unit	最大传输单元
NBMA	NonBroadcast MultiAccess	非广播多连接
ND	Neighbour Discovery	邻居发现
TCP	Transmission Control Protocol	传输控制协议
PMTU	Path Maximum Transmission Unit	最大传输单元

5 概述

节点（主机和路由器）使用邻居发现来确定相连链路上邻居的链路层地址，并迅速删除无效的缓存值。主机也使用邻居发现来寻找进行包转发的邻居路由器。另外，节点使用邻居发现机制，可以主动跟踪哪些邻居是可达的，或者是不可达的，并检测改变的链路层地址。当路由器或到达路由器的路径发生故障时，主机主动寻找正在工作的另一个路由器或另一条路径。

IPv6的邻居发现协议和IPv4的ARP、ICMP路由器发现和ICMP重定向相对应，在IPv4中没有相应的邻居不可达检测机制和协议。

邻居发现支持的链路类型有：点到点、组播、NBMA、共享介质、可变MTU和不对称可达性。

邻居发现机制具有以下功能。

（1）路由器发现：主机怎样定位相连链路上的路由器。

（2）前缀发现：主机怎样发现一组地址前缀，这些前缀定义了哪些目的地在相连链路上是在连接的

(on-link)。

(3) 参数发现: 节点怎样了解发送接口的链路参数 (如链路 MTU) 或网络参数 (如跳数限制值)。

(4) 地址自动配置: 节点怎样自动配置接口的地址。

(5) 地址解析: 在给出目的地 IP 地址的情况下, 节点怎样确定在连接 (on-link) 目的地 (例如, 邻居) 的链路层地址。

(6) 下一跳确定: 将目的地 IP 地址映射成邻居 IP 地址的算法, 下一跳可以是路由器或目的地。

(7) 邻居不可达检测: 节点怎样确定邻居不可达, 如果邻居是路由器, 可以使用默认路由器。如果邻居既是路由器也是主机, 需要再执行地址解析。

(8) 重复地址检测: 节点怎样确定将要使用的地址没有被另一个节点正在使用。

(9) 重定向: 路由器怎样通知主机到达目的地的最佳下一跳。

邻居发现定义了 5 种不同的 ICMP 包类型: 路由器请求、路由器通告消息、邻居请求、邻居通告消息和重定向消息。

(1) 路由器请求

当接口工作时, 主机立即发送路由器请求消息, 要求路由器产生路由器通告消息, 而不必等待下一个预定时间。

(2) 路由器通告

路由器周期性地通告它的存在以及配置的链路和网络参数, 或者对路由器请求消息作出响应。路由器通告消息包含在连接 (on-link) 确定、地址配置的前缀和跳数限制值等。

路由器发现是基本协议的一部分, 主机不必探测路由协议。

在组播链路上, 每个路由器周期地组播路由通告包, 来通告它的可用性。主机从所有路由器接收路由器通告, 建立默认路由器列表。路由器频繁地产生路由器通告, 以使主机在几分钟内了解到它的可用性, 也可单独使用邻居不可达检测算法进行故障检测。

路由器通告包含用作在连接 (on-link) 确定和/或地址配置的前缀列表, 以及表明特定前缀用途的前缀标志位。主机使用通告的在连接 (on-link) 前缀建立和维护列表, 列表用来决定包的目的地是在连接 (on-link) 还是在路由器外。即使目的地不包含在被通告的在连接 (on-link) 前缀中, 目的地也可以是在连接 (on-link)。在这种情况下路由器发送重定向消息, 来通知发送者目的地是一个邻居。

路由器通告允许路由器通知主机如何执行地址配置。例如, 路由器能指示主机是使用状态地址配置, 还是使用无状态地址配置。

路由通告消息包含网络参数, 例如, 主机的发送接口使用的跳数限制值等, 包含可选的链路参数, 如链路 MTU。这样可有利于集中管理这些设置在路由器上的重要参数, 并能自动传送到所有相连的主机上。

路由器通告含有链路层地址, 不需要另外的包交换来解析路由器的链路层地址; 含有链路前缀, 不需要单独的机制配置掩码。

路由器通告链路上主机使用的 MTU, 保证链路上所有节点使用相同的 MTU 值。

(3) 邻居请求

节点发送邻居请求消息来确定邻居的链路层地址, 或者验证邻居通过缓存的链路层地址仍然可达, 邻居请求消息也可用于重复地址检测。

节点通过组播邻居请求消息完成地址解析，邻居请求消息要求目标节点返回它的链路层地址。邻居请求消息组播到目标节点的请求节点组播地址，目标通过单播邻居通告消息返回链路层地址。发起者的邻居请求消息中包含链路层地址。

邻居请求消息也可以用来确定多个节点是否分配了相同的单播地址。重复地址检测的邻居请求消息在地址自动配置中规定。

(4) 邻居通告

邻居请求消息的响应，节点也可以发送非请求邻居通告来指示链路层地址的变化。

邻居不可达检测可以检测邻居或邻居前向路径发生的故障，这样就要求确认发送给邻居的包到达了那个邻居且正在被 IP 层进行处理。邻居不可达检测使用两种方法进行确认：一种是上层协议提供“连接正在处理”的确认，即先前发送的数据认为是正确发送（例如，最近收到新的确认）；另一种是节点发送单播邻居请求消息，请求的邻居通告消息作为下一跳的可达性确认。为了减少不必要的网络流量，探测消息仅发送到邻居。

在路由器故障或链路层地址改变的链路和节点故障的情况下，邻居不可达检测是提高包传送能力的一部分，例如，由于 ARP 缓存无效，移动节点没有失去任何连接而离开非连接。不像 ARP，邻居发现检测半链路的故障，避免发送流量到失去双向连接的邻居。

路由器通告消息不包含优先权字段，不必处理稳定性不同的路由器。邻居不可达检测将检测失效的路由器，并切换到工作的路由器。

(5) 重定向

路由器用于通知主机到达目的地的最佳下一跳。

重定向包含新第一跳的链路层地址，单独的地址解析不必接收重定向。

多个前缀可以和同一链路有关，默认情况下，主机从路由通告获得所有在连接（on-link）前缀。但路由器可以配置成忽略路由器通告中的某些或所有前缀，在这种情况下，主机认为目的地是非连接，并发送流量到路由器，然后路由器发布合适的重定向。

IPv6 重定向的接收认为下一跳是在连接。在 IPv4 中，根据链路的网络掩码指示下一跳不是在连接，主机忽略重定向。IPv6 重定向机制和共享介质的重定向机制类似。在非广播和共享媒介链路中节点可能知道在连接目的地的所有前缀。

邻居发现也可以处理下列情况。

(1) 链路层地址改变

如果节点得知自己的链路层地址改变，就会组播邻居通告包到所有节点，迅速更新无效的缓存链路层地址。发送非请求通告消息仅能提高可靠性（例如，在不可靠时）。邻居不可达检测算法保证所有节点可以可靠地发现新地址，时延可能会比较长。

(2) 入口负载均衡

在接收来自相同链路上多个网络接口的数据包时需要负载均衡。这个节点在相同接口分配了多个链路层地址，例如，单个的网络驱动程序可以把多个网络接口卡表示为具有多个链路层地址的逻辑接口。负载均衡允许路由器省略路由器通告包中的源链路层地址，强制邻居使用邻居请求消息了解路由器的链路层地址。根据不同的请求消息发送者，返回的邻居通告消息包含不同的链路层地址。

(3) 泛播地址

泛播地址用于标识提供同样服务的一组节点，可以配置相同链路上的多个节点能够识别相同的泛播地址。通过节点接收对于相同目标的多个邻居通告，邻居发现来处理泛播。所有的泛播地址的通告标记为 non-override 的通告，这样可以使使用特定的规则来确定应该使用哪个通告。

(4) 代理通告

如果目标地址不能响应邻居请求，愿意代表该目标地址接收包的路由器会发布 non-override 的邻居通告。目前没有规定代理的使用，代理通告可以处理离开非连接（off-link）的移动节点，但不能作为通用的机制来处理节点。

使用链路本地地址惟一标识路由器（对于路由器通告和重定向消息），主机能在站点重编号且使用新的全球前缀时保持路由器联系。

邻居发现使用的跳数限制等于 255，可以防止非连接发送者故意发送邻居发现消息。在 IPv4 中发送者既发送重定向消息，也发送路由器通告消息。

6 消息格式

6.1 路由器请求消息格式

为了使路由器迅速产生路由器通告，主机发送路由器请求消息，路由器请求消息格式如图 1 所示。

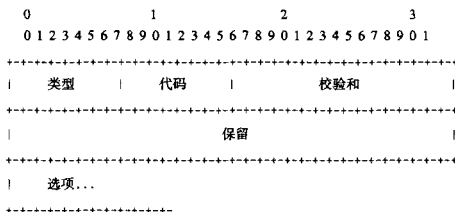


图 1 路由器请求消息格式

图 1 中：

(1) IP 域

源地址：分配给发送接口的 IP 地址，当发送接口没有分配地址时，可以是未规定的地址。

目的地址：全部路由器组播地址（Multicast Address）。

跳数限制：255。

认证头：如果在发送方和目的地址之间存在 IP 认证头的安全联盟（Security Association），发送方的消息中必须包含这个字段。

(2) ICMP 域

类型：133。

代码：0。

校验和：[ICMPv6]中的 ICMP 校验和。

保留：这个字段未使用。发送方必须初始化为 0，同时接收方必须忽略。

(3) 有效选项

源链路层地址：在已知的情况下就是发送方的链路层地址，不包括未规定的源地址。否则它应在链

路层上有地址。

本标准的将来版本会定义新的选项类型，因此接收者必须能忽略不能识别的选项，继续处理消息。

6.2 路由器通告消息格式

路由器周期性地发送路由器通告消息，或者对路由器请求作出响应，路由器通告消息格式如图 2 所示。

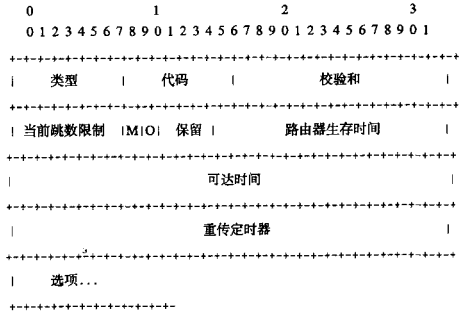


图 2 路由器通告消息格式

图 2 中：

(1) IP 域

源地址：必须是分配给消息发送接口的本地链路地址。

目的地址：激活路由器请求的源地址或全部节点组播地址。

跳数限制：255。

认证头：如果在发送方和目的地址之间存在 IP 认证头的安全联盟，发送方的消息中必须包含这个字头。

(2) ICMP 域：

类型：134。

代码：0。

校验和：[ICMPv6]中的 ICMP 校验和。

当前跳数限制：8 位无符号整数。缺省值应当位于发送的 IP 包头的跳数限制字段。值为 0 表示未规定（本路由器）。

M：1 比特的“管理地址配置”标志位。当置 1 时，主机使用无状态地址自动配置以外，还使用管理（状态）协议进行地址自动配置。

O：1 比特“其他状态配置”标志位。当置 1 时，主机使用管理（状态）协议对其他（非地址）信息进行自动配置。

保留：6 比特未使用字段。发送方必须初始化为“0”，接收方必须忽略。

路由器生存时间：16 位无符号整数。生存时间与缺省路由器有关，以秒为单位。最大值为 18.2h。0 值表示不是缺省路由器，不应该出现在缺省路由器列表中。路由器生存时间仅适用于缺省路由器，不适用于包含在其他消息字段或选项中的信息。信息中需要时间限制的选项包含生存时间字段。

可达时间：32 位无符号整数。以毫秒为单位，节点在收到可达确认后认为邻居是可达的时间。用于邻居不可达检测算法。值为 0 时表示未规定（本路由器）。

重传定时器：32 位无符号整数。以毫秒为单位，重传邻居请求消息之间的时间间隔。用于地址解析

和邻居不可达检测算法。值为 0 时表示未规定（本路由器）。

(3) 可能的选项

源链路层地址：发送路由器通告的接口链路层地址。只用于有地址的链路层。路由器可以忽略这项选项，以便能够在穿过多个链路层地址时使用负载分配。

MTU: 在具有可变 MTU 的链路上发送, 在其他链路上也可发送。

前缀信息：这些选项规定了链路上的前缀，和/或者用于地址自动配置。路由器应当包含所有链路上的前缀（除了本地链路前缀），这样多穴主机具有相连链路的在连接地址全部的前缀信息。如果信息不全，多穴主机将不能选择正确的接口来发送流量到邻居。

本标准的将来版本会定义新的选项类型，因此接收者必须能忽略无法识别的选项，继续处理消息。

6.3 邻居请求消息格式

节点发送邻居请求来请求目标节点的链路层地址，同时也向目标提供自身的链路层地址。邻居请求在节点处理地址时是多点传送的，在节点对邻居的可达性进行校验时是单点传送的。邻居请求消息格式如图 3 所示。



图 3 邻居请求消息格式

图 3 中:

(1) IP 域

源地址：发送消息的接口所分配的地址，或者（如果正在进行多个地址检测[ADDRCONF]）是未规定的地址。

目的地址：目标地址相应的请求节点组播地址或是目标地址。

跳数限制: 255。

认证头：如果在发送方和目的地址之间存在 IP 认证头的安全联盟，那么发送方应当包含这个字头。

(2) ICMP 域

类型: 135。

代码: 0。

校验和: [ICMPv6]中的 ICMP 校验和。

保留：这个字段未使用。发送方必须初始化为 0，同时接收方必须忽略。

目标地址：所请求的目标 IP 地址。它不能是组播地址。

(3) 可能的选项

源链路层地址：发送方的链路层地址。如果源 IP 地址是未规定的地址，不能包括这个选项。否则在有地址的链路层上组播请求必须包含这个选项，单播请求也应当包含。

本标准的将来版本会定义新的选项类型，因此接收者必须能忽略不能识别的选项，继续处理消息。

6.4 邻居通告消息格式

节点通过发送邻居通告消息来回应邻居请求消息, 并且发送非请求邻居通告消息, 以便迅速地传达新信息(非可靠地)。邻居通告消息格式如图 4 所示。



图 4 邻居通告消息格式

图4中:

(1) IP 域

源地址：分配给发送通告接口的地址。

目的地址：对于请求通告，目的地址指调用邻居请求的源地址，或者如果请求的源地址是未规定的地址，目的地址是指全部节点组播地址。对于非请求通告消息，即指全部节点组播地址。

跳数限制: 255。

认证头:如果在发送方和目的地址之间的 IP 认证头中存在安全联盟,那么发送方应当包含这个字头。

(2) ICMP 域

类型: 136。

代码: 0。

校验和: [ICMPv6]中的 ICMP 校验和。

R: 路由器标志位。设置为 1 时, R 位表示发送方为路由器。邻居不可达检测使用 R 位来检测路由器到主机的改变。

S：请求标志位。设置为 1 时，S 位表示从目的地址发送的通告消息，作为对邻居请求的响应。S 位用来作为邻居可达检测的可达性确认。在组播通告或非请求单播通告中不能设置这一项。

O: override 标志。设置为 1 时, O 位表示通告应当替换已存在的缓存表项, 更新缓存的链路层地址。未设置时, 通告不能更新缓存的链路层地址, 虽然它会更新链路层地址未知的邻居缓存表项。在泛播地址的请求通告和非请求通告中不应设置这一项。在其他请求通告和非请求通告中应该设置这一项。

保留：29 比特未使用的字段。发送方必须初始化为 0，接收方必须忽略。

目标地址：对于请求通告，邻居请求消息中的目标地址字段。对于非请求通告，就是发生改变的链路层地址。目标地址不能是组播地址。

(3) 可能的选项

目标链路层地址：目标的链路层地址，例如，通告的发送方。当响应组播请求时，这项选项必须包含在有地址的链路层中。当响应单播邻居请求时也应当包括本选项。

当对等节点没有返回邻居通告消息的缓存表项时，为了避免邻居请求的无穷递归，对于组播请求必须包括这个选项。当响应单播请求时，因为请求的发送方有正确的链路层地址，可以省略此选项；否则不能首先发送单播请求。这种情况下包括链路层地址不会增加开销，在收到先前请求的响应前发送者会删除缓存的链路层地址。

本标准的将来版本会定义新的选项类型，因此接收者必须能忽略不能识别的选项，继续处理消息。

6.5 重定向消息格式

路由器发送重定向包来通知到目的地路径上更佳下一跳节点。主机可被重定向到更佳下一跳路由器，但重定向也可通知目的地（实际上是邻居）。后者可通过把 ICMP 目标地址设置成 ICMP 目的地址来完成。定向消息格式如图 5 所示。

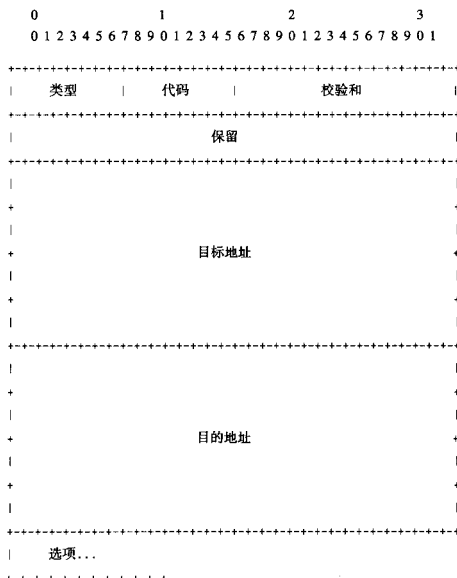


图5 重定向消息格式

图 5 中:

(1) IP 域

源地址: 分配给发送消息接口的本地链路地址。

目的地址: 触发重定向的数据包的源地址。

跳数限制: 255。

认证头: 如果在发送方和目的地址之间的 IP 认证头中存在安全联盟, 发送方应当包含这个字头。

(2) ICMP 域

类型: 137。

代码: 0。

校验和: [ICMPv6]中的 ICMP 校验和。

保留: 这个字段未使用。发送方必须初始化为 0, 接收方必须忽略。

目标地址: 到达 ICMP 目的地址的更佳下一跳的 IP 地址。若目标是通信的终点, 例如, 目的地是邻居, 目标地址字段必须包含和 ICMP 目的地址字段相同的值。否则目标是更佳下一跳路由器, 目标地址必须是路由器的本地链路地址, 以便主机能惟一地识别路由器。

目的地址: 重定向到目标的目的 IP 地址。

(3) 可能的选项

目标链路层地址: 目标的链路层地址应当包括这个选项 (如果已知)。注意, 在 NBMA 链路上, 主机可以根据重定向消息中存在的目标链路层地址选项, 来决定邻居的链路层地址。这时重定向消息必须包括这个选项。

重定向头: 重定向包的长度不超过 1280 字节时, 触发发送重定向的 IP 包的数量不受限制 (尽可能多)。

6.6 选项格式

邻居发现消息包括 0 及更多的选项, 一些选项可能会在同一个消息中出现多次。所有选项的格式如图 6 所示。

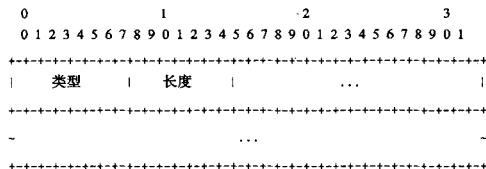


图 6 选项格式

图6中:

类型: 8 比特, 选项类型标识符。具体定义见表 1。

表 1 选项类型定义

选项名称	类型
源链路层地址	1
目的链路层地址	2
前缀信息	3
重定向头	4
MTU	5

长度：8位无符号整数。选项的长度（包括类型和长度字段）以8字节为单位。0值是无效的。节点必须自动丢弃包含了长度为0的选项的数据包。

6.6.1 源/目的链路层地址

源/目的链路层地址格式如图7所示。

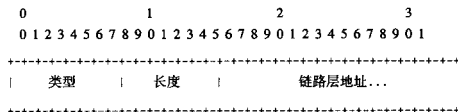


图 7 源/目的链路层地址格式

图7中

类型：1 为源链路层地址；

2 为目标链路层地址。

长度：选项的长度（包括类型和长度字段）以 8 字节为单位。例如，IEEE 802 的地址长度为 1。

链路层地址：长度可变的链路层地址。这个字段的内容和格式（包括 byte 和 bit 排序）在 IPv6 怎样在不同链路层上运行的文档中规定。

说明：源链路层地址选项包含数据包的发送方的链路层地址。可用于邻居请求包、路由器请求包和路由器通告数据包。目标链路层地址选项包含目标的链路层地址。可用于邻居通告包和重定向数据包。这些选项对于其他邻居发现消息必须忽略。

6.6.2 前綴信息

前缀信息格式如图8所示。

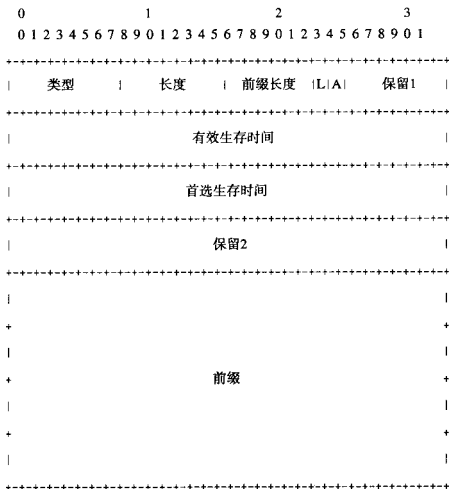


图 8 前缀信息格式

6.6.4 MTU

MTU 格式如图 10 所示。



图 10 MTU 格式

图 10 中：

类型：5。

长度：1。

保留：这个字段未使用。发送方必须初始化为 0，接收方必须忽略。

MTU：32 位无符号整数。链路的推荐 MTU 值。

说明： MTU 选项用于路由器通告消息中，当不知道链路的 MTU 值时，保证链路上所有节点使用相同的 MTU 值。这个选项必须被其他邻居发现消息忽略。

对于用不同种类技术桥接的配置，每段所能支持的最大 MTU 可以不同。如果桥没有产生“ICMP 包太大”的消息，通信节点就无法使用寻径 MTU (Path MTU) 动态地对单个邻居动态决定 MTU 的大小。在这种情况下，路由器使用 MTU 选项来规定所有段支持的最大 MTU 值。

7 主机模型

本节描述了主机（某些程度上指路由器）在与邻居节点的交互过程中需要维护的数据结构模型。只要其外部行为同本标准的描述一致，本标准不强制要求具体的实现遵循这个模型。

该模型只涉及到同邻居发现有直接关系的主机行为，不涉及例如像在多穴主机中源地址和发送接口的选择。

7.1 数据结构

主机需要为每一接口维护以下信息。

邻居缓存：一组有关最近收到数据流的邻居表项。表项为邻居的在连接单播 IP 地址提供信息，它包括：其链路层地址、指示邻居是路由器还是主机的标志位、指向任何排队等待完成地址解析数据包的指针等。

一个邻居缓存表项还包括由邻居不达检测算法所使用的信息，例如，可达状态、探测无应答的次数以及下一次邻居不达检测发生的时间。

目的地缓存：一组有关最近收到数据流的目的地节点表项。目的地缓存包括“在连接 (on-link)”和“非连接 (off-link)”目的地，并在其中提供一定程度的间接寻址；目的地缓存把目的地 IP 地址映射到下一跳邻居的 IP 地址。该缓存通过重定向消息进行信息更新。如果在目的地缓存表项中存储与邻居发现没有直接关系的附加信息，例如，路径 MTU (PMTU) 以及由传输协议设定的往返时间 (RRT)，则执行时会更加方便。

前缀列表：规定一组“在连接 (on-link)”地址的前缀组成的列表。前缀列表表项产生于路由器通告接

收到的信息。每一个表项都有一个相关的失效计时器值（由通告信息确定），它用于在前缀失效时废弃这些前缀。特殊的“无限”计时器值规定前缀永久有效，除非在后续通告中收到了一个新的（有限）值。

本地链路（link-local）前缀位于带有限失效计时器的前缀列表，而不管路由器是否正在向其通告前缀。接收的路由器通告不应该修改本地链路前缀的失效计时器。

缺省路由器列表：接收数据包的路由器列表。路由器列表的表项指向邻居缓存中相应的表项；缺省路由器的选择算法是，选择那些已知可达的路由器，而不选择可达性还不确定的路由器。每一个表项还有一个相关的失效计时器值（从路由器通告信息中得到），它的作用是删除不再通告的表项。

上述数据结构可以用不同的方法实现。一种实现方法是对所有数据结构使用单个最长匹配路由表。不管采用那种特定的实现方法，为了防止重复性的邻居不可达检测，路由器的邻居缓存表项可以由使用该路由器的所有目的地缓存表项共享。

其他协议（例如，移动 IPv6 协议）可能会增加另外的数据结构。这种数据结构的实现方法可以任选，例如，可以把所有的数据结构合并成单个路由表。

邻居缓存包含有邻居不可达检测算法维护的信息。邻居可达性状态是最关键的信息，它的取值是下列的 5 个值之一。

不完全（Incomplete）：正在进行地址解析，邻居的链路层地址还没确定。

可达性（Reachable）：邻居在最近处于可达状态（在小于 10s 以前）。

失效（Stale）：在数据流发送给该邻居以前邻居是不可达的，并无法验证其可达性。

延迟（Delay）：邻居不再是可达的，同时数据流在最近已经发送给邻居，但不立即对该邻居进行探测，而在一个短时延后发送探测信息，这样就可以为上层协议提供可达性确认。

探测（Probe）：邻居不再是可达的，同时发送单播邻居请求探测以验证可达性。

7.2 发送算法

当向目的地发送数据包时，节点采用目的地缓存，前缀列表和缺省路由器列表中的综合信息来确定适当的下一跳 IP 地址。这个操作称为“下一跳确定”。如果下一跳的 IP 地址确定后，邻居缓存就可用于协商有关那个邻居的链路层信息。

对给定的单播目的地地址进行下一跳确定的操作步骤如下：发送方用最长前缀匹配法来与该前缀列表进行匹配，以确定该数据包的目的地地址是“在连接”还是“非连接”。如果目的地地址“在连接”，则下一跳地址同数据包的目的地地址一致，否则发送方从路由器缺省列表中选定一个路由器。如果缺省路由器列表是空的，则发送方认为目的地“在连接”。

出于效率的考虑，不是对每一个发送的数据包都执行下一跳的确定，而是把下一跳确定计算的结果存放在目的地缓存中（也包含从重定向信息得到的更新）。当发送节点有待发送数据包时，它首先检查目的地缓存。如果不存在目的地的表项，则激活下一跳确定来创建一条新的目的地缓存表项。

如果知道了下一跳节点的 IP 地址，发送方就检查邻居缓存中有关邻居的链路层信息。如果没有表项存在，发送方就创建一条，并设置其状态为“不完全”，同时启动地址解析，然后对没有完成地址解析的数据包进行排队。对具有组播功能的接口来说，地址解析的过程是发送一个邻居请求信息，以及等待一个邻居通告。当收到一个邻居通告应答时，链路层地址被记录在邻居缓存中，同时发送排队的数据包。

对于组播数据包下一跳就是目的地地址，并认为处于“在连接”。IP 组播地址对应链路层地址的确定过程不在本标准中描述。

在传输单播数据包期间每次读取邻居发现缓存的表项，发送方根据邻居不可达性检测的算法检查邻居不可达性检测的相关信息，但不可达性检测会使发送方发出单播邻居请求，以验证该邻居还是可达的。

数据流第一次送往目的地时就执行下一跳确定的操作。随后该目的地如果仍能正常通信，目的地缓存的表项就可以继续使用。如果邻居不可达算法决定在这一点终止通信，则需要重新执行下一跳确定，例如，故障路由器的流量应该切换到正常工作的路由器，流向移动节点的数据流可能要重新路由到“移动代理”。

当节点重做下一跳确定时，不需要丢弃整个目的地缓存的表项，其中 PMTU 和往返计时器值的信息是很有用的。

路由器和多穴主机有多个接口。本标准假定所有的邻居发现信息通过相应的接口发送和接收，例如，当应答一个路由请求时，通过收到路由请求的接口送出对应的路由器通告。

7.3 垃圾收集和超时要求

上述的数据结构采用不同的机制来清除无效信息。

不需要周期性地清除目的地和邻居缓存表项。如果无效信息潜在的驻留在缓存中，并正在使用，邻居不可达性检测算法就会立刻清除它。

因为目的地和邻居缓存的存储空间是有限的，节点需要对旧表项进行垃圾收集，并要考虑有足够的空间来保存工作中的活动表项。如果表项被快速清除和重建，则小的缓存可能会导致邻居发现消息的溢出。基于 LRU 的策略是指恢复在一定时间内没有被使用过的表项（例如，10min 或大于 10min），它也适用于垃圾收集这些表项。

节点应该在缺省路由器列表和前缀列表中保留表项直到其生存期结束。如果存储容量小，节点可以预先对表项进行垃圾收集。如果不是所有的路由器都记录在路由器列表上，为了对“非连接”目的地保持健壮性连接，节点应该在缺省路由器列表中至少保存两项表项。当前缀列表中删除一个表项时，不需要从目的地或邻居缓存中清除所有的表项。邻居不可达性检测将有效地清除缓存中无效的表项。当从缺省路由器列表中删除一个表项时，所有经过这个路由器的目的地缓存表项必须再执行下一跳确定的操作，以选择一个新的缺省路由器。

8 路由器和前缀发现

本节叙述与邻居发现中路由器发现有关的路由器和主机的行为。路由器发现用于定位寻找邻居路由器，并获取与地址自动配置相关的前缀和配置参数。通过前缀发现的过程，主机获取驻留“在连接”的 IP 地址范围，并能直接获得而不需要经过一个路由器。路由器发出路由器通告，指示该发送方是否愿意为缺省路由器。路由器通告还包括前缀信息选项，这些选项列出了一组确认“在连接”IP 地址的前缀。

无状态地址自动配置必须获得作为配置地址的子网前缀。尽管这些用于地址自动配置的前缀在逻辑上区别于那些用于“在连接”确定的前缀，但是自动配置信息附在路由器发现消息上可以减少网络的流量。实际上，可以采用在前缀消息选项中规定标志位的方法，为“在连接”确定和地址自动配置通告同样的前缀。

8.1 消息有效性验证

8.1.1 路由器请求消息的有效性验证

主机必须无条件丢弃收到的任何路由器请求消息。

路由器必须无条件丢弃不满足以下有效性检查的路由器请求消息：

- IP 跳限数为值 255，即该数据包不能再被路由器转发；
- 如果消息包含一个 IP 认证标头，该消息认证正确；
- ICMP 校验和有效；
- ICMP 代码值为 0；
- ICMP 长度（从 IP 头长度字段中获取） ≥ 8 字节；
- 所有包含的选项长度 >0 ；
- 如果 IP 源地址不是规定的地址，在消息中没有源链路层地址选项。

必须忽略保留域和任何非确认选项中的内容。将来协议向后兼容进行修改时，可以规定保留域的内容或增加新的选项，也可以采用不同的码值。

必须忽略路由器请求消息中没有规定使用但定义了选项内容，其数据包的处理同正常的处理方式。惟一可能定义的选项是源链路层地址选项。

通过有效性检测的请求称为“有效性请求”。

8.1.2 路由器通告消息的有效性

节点必须无条件地丢弃不满足以下有效性检验的路由器通告消息：

- IP 源地址是本地链路地址。路由器必须把其本地链路地址作为路由器通告和重定向消息的源地址，这样主机才能惟一识别路由器。
- IP 跳限数为 255，该数据包不能再被路由器转发。
- 如果消息包含一个 IP 认证标头，该消息认证正确。
- ICMP 校验和有效。
- ICMP 代码值为 0。
- ICMP 长度（从 IP 头长度字段中获取） ≥ 16 字节。
- 所有包括的选项长度 >0 。

必须忽略保留域和任何非确认选项中的内容。将来协议向后兼容进行修改时，可以规定保留域的内容或增加新的选项，也可以采用不同的码值。

必须忽略路由器请求消息中没有规定使用但定义了选项内容，其数据包的处理同正常的处理方式。可能定义的选项是源链路层地址选项、前缀信息和 MTU 选项。

通过有效性检验的通告称为“有效性通告”。

8.2 路由器要求

8.2.1 路由器配置变量

路由器必须允许系统管理员能够配置以下参数。这里特定的参数仅仅起到说明的作用，具体实现并不要求使用这些参数，只要路由器的外部行为与文档中的描述一致即可。为了简化配置，给出了这些参数的缺省值。

IP 如何工作在不同的链路层的文档中描述的值优于本标准所定义的缺省值。这条规则简化了邻居发现在性能特征不同的链路的配置过程。

- (1) 对于每一个组播接口有下列变量

AdvSendAdvertisements

该标志用来指出路由器是否周期性地发送路由器通告消息和响应路由器请求消息。

缺省值: FALSE。

注意: 这个参数的缺省值必须设置成 FALSE, 除非它被系统管理员有意地配置, 否则节点不会作为路由器来发送路由器通告消息。

MaxRtrAdvInterval

接口发送非请求组播路由器通告消息的最大间隔时间, 不能 $<4s$ 也不能 $>1800s$ 。

缺省值: 600s

MinRtrAdvInterval

接口发送非请求组播路由器通告消息的最小间隔时间, 不能 $<3s$ 也不能 $>0.75 * \text{MinRtrAdvInterval}$ 秒。

缺省值: $0.33 * \text{MaxRtrAdvInterval}$ 秒

AdvManagedFlag

路由器通告消息中的“可管理地址配置”标志位, 值为 TRUE/FALSE。

缺省值: FALSE。

AdvOtherConfigFlag

路由器通告消息中的“其他状态配置”标志位, 值为 TRUE/FALSE。

缺省值: FALSE。

AdvLinkMTU

路由器发送的 MTU 选项值, 值 0 表示不发送 MTU。

缺省值: 0。

AdvReachableTime

路由器通告消息中“可达时间”字段的值, 值 0 表示不规定, 必须 $>3\ 600\ 000ms$ (1h)。

缺省值: 0。

AdvRetransTimer

路由器通告消息中“重传定时器”字段的值, 值 0 表示不规定。

缺省值: 0。

AdvCurHopLimit

路由器通告消息中“当前跳数限制”字段的缺省值, 设置成因特网当前的最大跳数, 值 0 表示不规定 (路由器)。

缺省值: 由 RFC [ASSIGNED]中规定的值。

AdvDefaultLifetime

路由器通告消息中“路由器生存期”字段的缺省值, 以秒为单位。必须设置为 0 值或者介于 MaxRtrAdvInterval 和 9000s 之间的值。值 0 表示这个路由器不能用作缺省的路由器。

缺省值: $3 * \text{MaxRtrAdvInterval}$ 。

AdvPrefixList

路由器通告消息中“前缀信息”选项的前缀列表。

缺省值: 路由器通过路由协议通告某个接口“在连接”的所有前缀, 通告消息通过这个接口发送。

本地链路前缀不应该包括在通告前缀列表中。

(2) 每个前缀有下列相关内容

AdvValidLifetime

前缀信息选项中“有效生存期”的值，以秒为单位。全 1 值 (0xFFFFFFFF) 表示无穷。实现中必须允许以下列两种方式设置 AdvValidLifetime 的值。

- 实时递减的时间，在某个特定的时间，生存期可以递减为 0 值。
- 在后续通告消息中设定的时间值保持不变。

缺省值：2 592 000s (30 天) 或固定值 (在后续通告消息中设定的时间值保持不变)。

AdvOnLinkFlag

前缀信息选项中“在连接” (“L-bit”) 标志位的值。

缺省值：TRUE。

(3) 在“自动地址发现”协议中定义了与每个前缀相关的其他信息

AdvPreferredLifetime

前缀信息选项中“首选生存期”的值，以秒为单位。全 1 值 (0xFFFFFFFF) 表示无穷。实现中必须允许以下列两种方式设置 AdvPreferredLifetime 的值。

- 实时递减的时间，在某个特定的时间，生存期可以递减为 0 值。
- 在后续通告消息中设定的时间值保持不变。

缺省值：604 800s (7 天) 或固定值 (在后续通告消息中设定的时间值保持不变)。

AdvAutonomousFlag

前缀信息选项中“自治标志”字段的值。

缺省值：TRUE。

以上这些参数中包含的信息放在路由器通告消息中。主机使用接收的信息来初始化一些参数。某些主机的参数 (如 CurHopLimit、RetransTimer 和 ReachableTime) 可以用于所有节点 (包括路由器)。由于这些参数的值能够通过上述的参数得到，所以这些参数不可以出现在路由器上。但对于这些参数路由器的外部行为必须与主机的行为一致，尤其包含 ReachableTime 值的随机性。

8.2.2 成为通告接口

“通告接口”指具有任何功能并且具有组播功能的接口，这个接口至少被分配一个单播 IP 地址，并且它的“AdvSendAdvertisements”标志位的值为 TRUE。路由器不能通过非通告接口来发送路由器通告消息。

除了在系统启动时，接口可以在任何时候变成通告接口。例如：

- 改变接口的“AdvSendAdvertisements”标志字段值为 TRUE。
- 系统管理来配置这个接口为通告接口，“AdvSendAdvertisements”标志字段值为 TRUE，或者，
- 设置主机具有 IP 转发功能 (如把主机设置成路由器)，接口的“AdvSendAdvertisements”标志字段值为 TRUE。

路由器必须在通告接口上加入路由器的组播地址。路由器响应发向路由器地址的路由器请求消息，并且检验相邻路由器发送的路由器通告消息的一致性。

8.2.3 路由器通告消息的内容

路由器通过通告接口周期性发送路由器通告消息，也发送请求的路由器通告消息。发送的路由器通

告消息会设置以下的值。

- 路由器生存期字段（Router Lifetime）：接口配置的 AdvDefaultLifetime。
- M 和 O 标志：接口配置的 AdvManagedFlag 和 AdvOtherConfigFlag。
- 当前跳数限制字段（Current Hop Limit）：接口配置的 CurHopLimit。
- 可达时间字段（Reachable Time）：接口配置的 AdvReachableTime。
- 重传定时器字段：接口配置的 AdvRetransTimer。
- 选项中的内容：

源链路地址选项：发送接口的数据链路层地址。为了有助于对重复的接口进行有限范围内的负载均衡，这个选项可以省略。

MTU 选项：如果 AdvLinkMTU 值不为 0，那么接口可以配置 AdvLinkMTU；否则将不发送 MTU 选项。

前缀信息选项：AdvPrefixList 中所列的每个前缀所使用的前缀信息选项，是按 AdvPrefixList 表项的信息来设置。

- “on-link” 标志位：该表项的 AdvOnLinkFlag。
- 有效生存期字段：该表项的 AdvValidLifetime。
- 自动地址配置标志位：该表项的 AdvAutonomousFlag。
- 首选生存期字段：该表项的 AdvPreferredLifetime。

路由器可以发送路由器通告消息，而不通告自己为缺省路由器。例如，路由器在地址自动配置通告前缀信息，但不转发数据包时，路由器会把发送的通告消息的路由器生存期字段设置成 0。

路由器在发送非请求路由器通告消息时，可以选择不包括部分或全部选项。例如，如果前缀的生存期远远大于 AdvDefaultLifetime 值，那么每几个通告消息里包含这些选项就足够了。然而，当响应路由器请求消息或者发送前面几个非请求的通告消息时，路由器应该包含全部的选项，从而这些前缀信息在系统初始化阶段可以迅速地传播。

如果通告消息中包含全部选项而使消息长度超过链路 MTU，那么可以发送多个通告消息，在每个消息中包含这些选项的子集。

8.2.4 发送非请求的路由器通告消息

在任何时候主机都不能发送路由器通告消息。

非请求的路由器通告消息不是严格周期性的：后续消息发送之间的时间间隔可以是随机的，这样可以减少在相同链路上与其他路由器发送的通告消息同步的概率。每个通告接口有自己的定时器。当组播通告消息从接口发送出去时，定时器的值将被重置成平均分布的随机值，这个值介于接口可配置的 MinRtrAdvInterval 与 MaxRtrAdvInterval 之间；当定时器到期的时候将发送下一个通告消息，并且重新选择新的随机值。

对于从某个通告接口上发送的前几个通告消息，如果随机发送间隔值大于 MAX_INITIAL_RTR_ADVERT_INTERVAL，那么定时器值应该设置成 MAX_INITIAL_RTR_ADVERT_INTERVAL。在可能丢包的情况下，为初始的通告消息使用较小的发送间隔会增加路由器被发现可用的可能性。

路由器通告消息中包含的信息可以通过系统管理而改变。例如，通告前缀的生存期会变化，会加入新的前缀，路由器可能停止路由功能（即从路由器变成主机）。在这种情况下，路由器最多发送

MAX_INITIAL_RTR_ADVERTISEMENTS 个非请求通告消息，遵循与接口变成通告接口时相同的规则。

8.2.5 停止成为通告接口

接口通过以下系统管理可以停止成为通告接口：

- 把接口的 AdvSendAdvertisements 标志位的值从 TRUE 改变为 FALSE；
- 禁止接口的功能；
- 关闭系统。

在这种情况下，路由器应该在这个接口上发送一个或多个（不超过 MAX_FINAL_RTR_ADVERTISEMENTS）最终的组播路由器通告消息，并且路由器生存期字段值设置为 0。在路由器变成主机的情况下，系统应该离开所有组播接口上 IP 组播组。另外，主机必须确保这个接口发送的后续邻居发现消息中“Router”标志位为 0。

注意，系统管理可以终止路由器的 IP 转发功能（即路由器变成主机），但这并不是指路由器接口不是通告接口。在这种情况下，后续的路由器通告消息必须设置路由器生存期字段值为 0。

8.2.6 处理路由器请求消息

主机必须无条件丢弃收到的任何路由器请求消息。

为了响应在通告接口接收到的合法请求消息，除了发送周期性的、非请求的通告消息以外，路由器还要发送通告消息。路由器可以选择单播方式直接响应请求主机的地址（如果请求消息的源地址不是未规定的地址），但通常的方法是路由器向所有节点组播组响应。在后面这种情况下，接口的间隔定时器重置成新的随机值，类似于刚发送一个非请求通告消息。

在任何情况下响应路由器请求消息的通告消息必须延迟一个随机时间后发送，这个随机时间介于 0 和 MAX_RA_DELAY_TIME 秒之间（如果发送单个通告以响应多个请求，延迟与第一个请求有关）。另外，发送到所有节点组播地址的后续通告消息的发送频率必须每 MIN_DELAY_BETWEEN_RAS 内不能大于 1 次。

路由器可以按照如下的过程处理路由器请求消息：

— 接收到路由器请求消息之后，在 0 和 MAX_RA_DELAY_TIME 之间计算出一个随机延迟值。如果计算出的值所对应的时间晚于下一个组播路由器通告消息原定的发送时间，那么就忽略这个随机值，并且按照原定的时间发送通告消息。

— 如果路由器在最后的 MIN_DELAY_BETWEEN_RAS 秒内发送了一个组播路由器通告消息（请求的或非请求的），在上一个通告消息发送之后，确定待发送的通告消息时间，该时间是对应于 MIN_DELAY_BETWEEN_RAS 的时间加上这个随机值。这能够保证组播路由器通告的发送频率在规定时间内。

— 否则，以给定的随机时间来调度路由器通告消息的发送。

允许路由器发送比 MinRtrAdvInterval 配置参数中更多的组播路由器通告消息，只要这些通告消息是用来响应路由器请求消息的即可。但在任何情况下非请求组播通告消息的发送次数不能大于 MinRtrAdvInterval 的值。

如果路由器请求消息中的源地址是未规定的地址，那么这个消息不能更新路由器的邻居缓存；具有正确源地址的请求消息按照如下方式更新路由器的邻居缓存。如果路由器的邻居缓存中已经存在请求发送者的缓存项，请求消息中包含源链路层地址选项并且接收到的链路层地址不同于缓存中的地址，那么

应该更新邻居缓存项中的链路层地址，并且可达性状态必须设置成“STALE”。如果路由器的邻居缓存中没有请求者的缓存项，路由器就按照 7.3.3 小节所述创建一个新的缓存项，配置链路层地址，并设置可达性状态为“STALE”。无论是否提供源链路地址选项，如果邻居请求者的缓存项存在，那么此项的 IsRouter 标志位必须设置成 FALSE。

8.2.7 路由器通告消息的一致性

路由器应该能够检测其他路由器发送的路由器通告消息的有效性，并且能够验证路由器正在链路上发送一致的信息。检测到不一致信息表明一个或多个路由器配置错误，系统或网络管理应该表明这些信息。检测的信息最少应该包括：

- 当前跳数限制值（未规定的值 0 除外）；
- M 或者 O 标志的值；
- 可达时间值（未规定的值 0 除外）；
- 重传定时器的值（未规定的值 0 除外）；
- MTU 选项中的值；
- 同一个前缀的首选和有效的生存期，如果 AdvPreferredLifetime 和/或 AdvValidLifetime 按照所指定的实时时间递减，那么生存期不能与路由器通告消息中的字段比较，但是必须分别与前缀将变为无效的时间比较。由于链路传播延迟和路由器间时钟同步的不精确性，这种比较应该允许有时间误差。

不同的路由器通告有不同的前缀集合并不是错误的。另外，一些路由器会对某些字段不作规定，即 0 值，而其他的路由器会规定这些值。错误日志应该约束主机从一个值转向另外值的冲突。

接收路由器通告消息时路由器的其他行为不在本标准的范围内。

8.2.8 改变本地链路地址

路由器本地链路地址应该很少发生变化。如果发生变化，接收邻居发现消息的节点使用源地址来识别发送者。如果从相同的路由器来的多个数据包中包含不同的源地址，节点会认为它们来自不同的路由器。例如，节点忽略重定向消息，认为这个消息是某个路由器发送的，而不是当前第一跳路由器发送的。这样当重定向到那个路由器时，由某个特定的路由器发送的路由器通告消息的源地址必须与重定向消息的目的地址一致。

在链路上使用链路本地地址来惟一地识别路由器，即当一个站点重编号时，路由器了解到的地址不会发生变化。

如果路由器在它的某个接口改变链路本地地址，它应该把这种变化通知到主机。路由器应该从以前的链路本地地址组播一些路由器通告消息，消息中的路由器生存期字段设置为 0，并且也从新的链路本地地址组播一些路由器通告消息。作用应该与终止通告接口的情况相同，与成为通告接口的情况不同。

8.3 主机要求

8.3.1 主机配置变量

本节无内容。

8.3.2 主机变量

主机除了定义的数据结构之外，还维护某些与邻居发现的有关变量。这些变量名在协议实现上没有要求，只要求它的外部行为与本标准描述的内容一致。

这些变量具有缺省值，从路由器通告消息中收到的信息优于变量的缺省值。当链路上没有路由器时

或所有收到的路由器通告中的值未规定，便使用缺省值。

本标准中定义的缺省值可以由描述在不同的链路层之上的 IP 操作的特定文档中的定义所替换。

IP 如何工作在不同的链路层的文档中描述的值优于本标准所定义的缺省值。本标准允许邻居发现工作在不同性能特征的链路层上。

对每个接口：

LinkMTU 链路的 MTU。

缺省值：IPv6 在不同的链路层上如何工作的标准中定义（如[IPv6-ETHER]）。

CurHopLimit 当发送（unicast）IP 数据包时所使用跳数限制的缺省值。

缺省值：在“分配的号码（Assigned Numbers）”RFC [ASSIGNED] 中定义。

BaseReachableTime 用于计算随机可达时间的基准值。

缺省值：REACHABLE_TIME 毫秒。

ReachableTime 在收到可达性确认后，邻居在这段时间内被认为是可达。

此值应该为 MIN_RANDOM_FACTOR 和 MAX_RANDOM_FACTOR 之间平均分布的随机值乘以 BaseReachableTime。当 BaseReachableTime 变化时（由于路由器通告），应该计算一个新的随机值；即使没有收到路由器通告，至少每几小时也应计算新的随机值。

RetransTimer 当解析地址或检测邻居可达性时，重传邻居请求消息到邻居的时间间隔。缺省值：RETRANS_TIMER 毫秒。

8.3.3 接口初始化

主机在所有具有组播功能的接口上加入所有节点组播地址组。

8.3.4 处理接收的路由器通告

当存在多个路由器时，由所有路由器共同通告的信息可以是单个路由器通告包含的信息的一个超集。信息也可以通过其他的动态方法获得，例如，状态自动配置协议。主机接受所有接收的信息，路由器通告的接收不能使先前收到的或从其他源收到的通告信息失效。当收到某一特定的参数信息（例如链路 MTU）或选项（如某一特定前缀上的生存期）与先前收到的信息不同，并且参数/选项仅有一个值，那么最近收到的信息被认为是具有最高优先级。

一些路由器通告消息中的字段（例如，当前跳数限制、可达时间和重传定时器）可以包含未规定的值，此时这些参数可以忽略，主机应该继续使用过去的值。尤其主机不能把未规定的值作为在第一个路由器通告收到以前的缺省值。当路由器通告某一特定值，其他路由器通告未规定值时，可防止主机改变内部的变量值。

当收到有效的路由器通告消息时，主机提取数据包的源地址，并做如下操作：

— 如果地址不在主机的缺省路由器列表中，并且通告的路由器生存期为非零，则在缺省路由器的列表创建一个新的表项，并且以通告的路由器生存期字段中的值来初始化无效定时器值。

— 如果地址已经作为先前收到的通告的结果存在于主机的缺省路由器列表中，则重置无效定时器值为最新收到通告中的路由器生存期值。

— 如果地址已经存在于主机的缺省路由器列表中并且收到的路由器生存期值是零，则该项立即指明超时。

为限制缺省路由器列表的存储容量，主机可以选择不存储由通告发现的路由器地址。但主机必须保

持至少两个路由器地址并应该保持更多的路由器地址。当目的地的通信失败时，应完成缺省路由器的选择。路由器列表中的路由器越多，越能更快地找到可选的工作路由器（例如，不必等待下一个通告到达）。

如果收到的当前跳数限制值为非零，主机应该设置它的当前跳数限制变量为收到的当前跳数限制的值。

如果收到基准可达时间值为非零，主机应该设置它的 BaseReachableTime 为收到的基准可达时间的值。

如果新数值不同于先前的值，主机应该重新计算一个随机的 ReachableTime 值作为可达时间。可达时间的计算是在 MIN_RANDOM_FACTOR 和 MAX_RANDOM_FACTOR 之间平均分布的一个随机数。用随机数来消除相邻路由器同时发送不可达发现消息的可能性。

在大多数情形下，连续路由器通告中通告的可达时间值是相同的，并且主机的 BaseReachableTime 很少改变。在这种情况下，协议的实现应确保至少每隔几小时重新计算随机值。

如果收到的 RetransTimer 值为非零，重传计时器变量应该从 RetransTimer 计时器字段中拷贝得到。

从路由器通告消息中固定部分提取信息以后，则对通告消息中有效选项进行扫描。如果通告消息包含源链路层地址选项，此链路层地址应该被表项在路由器的邻居缓存表项中（如果必要的话，生成一个新项）并且邻居缓存项的 IsRouter 标志必须设置为 TRUE。如果没有包含链路层源地址，但是有相应的邻居缓存项存在，则此邻居缓存项的 IsRouter 标志必须被设置为 TRUE。IsRouter 标志可被邻居不可达检测用于确定路由器何时变为主机（即不再有转发数据包功能）。如果为路由器创建了邻居缓存项，则此邻居缓存项状态必须设置为 STALE。

如果缓存项已经存在，并且被更新为不同的链路层地址，则其可达性状态必须设置为 STALE。

如果存在 MTU 选项，只要此 MTU 的值大于或等于最小链路 MTU [IPv6] 并且不超过链路类型特定文档中所定义的 LinkMTU 缺省值，主机应该拷贝选项的值作为 LinkMTU 的值。

“on-link”（在连接）标志置位的前缀信息选项确定地址范围，这些地址被认为是连接的。然而“on-link”标志置为零的前缀信息选项不表达任何有关在连接决定的信息，并且不能解释为前缀覆盖的地址为非连接。取消先前的在连接标识的惟一方法是通告 L-bit 置位和生存期为零的前缀。当数据包发送到其在连接状态信息未知的地址时，数据包就转发给缺省路由器；接收到在连接（L）标志为零的标志前缀信息选项时，操作不变。地址被认为在连接地址的原因在连接定义中说明。on-link 标志置为零的前缀通常把 autonomous 标志位置位并被地址自动配置使用。

对每个 on-link 标志置位的前缀信息选项，主机执行以下操作：

- 如果前缀是本地链路前缀，忽略此前缀信息选项。
 - 如果前缀不在前缀列表中，并且前缀信息选项的有效生存期字段是非零，为此前缀创建一个新项，并把无效计时器初始化为前缀信息选项中的有效生存期值。
 - 如果前缀作为收到以前通告的结果已经存在于主机的前缀列表中，重置无效计时器值为前缀信息选项中的有效生存期值。如果新的生存期值是零，立即使前缀超时。
 - 如果前缀信息选项的有效生存期字段是零，并且前缀不存在于主机的前缀列表中，则忽略此选项。
- 无状态地址自动配置在某些情况下可以延长前缀的有效生存期或完全忽略它，以防止拒绝服务攻击。由于对链路前缀列表的拒绝服务攻击的效果不是灾难性的（主机发送数据包到缺省路由器，并接收重定向消息而不是直接发送数据包到邻居），所以邻居发现协议不对前缀生存期值进行检查。

注意，在协议具体实现的处理中，可选择不同于前缀地址自动配置的方式，而单独地处理前缀在连接方面的特性，如传送有效路由器通告消息到在连接和地址配置功能中去。每个功能能对标志置位的前缀进行独立地操作。

8.3.5 前缀和缺省路由器超时

只要前缀列表中的无效计时器到期，那么此项便被丢弃。已存在的目的地缓存表项不需要更新。如果已存在的邻居缓存表项引起可达性问题，邻居不可达检测协议将执行任何必要的恢复。

无论何时缺省路由器列表中表项的生存期到期，此项便被丢弃。当从缺省路由器列表中删除路由器时，节点必须用如下方法更新目的地缓存，即所有使用该路由器的缓存表项重新确定下一个跳，而不是继续发送数据到该（已删除的）路由器。

8.3.6 缺省路由器选择

选择路由器的算法部分取决于路由器是否为可达。节点还应跟踪邻居的可达性状态。当 off_link 目的地的没有目的地缓存表项存在或通过路由器的通信失败，在决定下一跳期间使用缺省路由器选择的算法。在正常情况下，当数据首次被发往目的地时，路由器被选定为缺省路由器，随后发往同一目的地的数据使用目的地缓存中指定的相同路由器，任何目的地缓存的变化将引发重定向消息。

从缺省路由器列表中选择路由器的策略如下：

1) 可达或可能可达的路由器（除不完全（IMCOMPLETE）以外的任何状态）应该优先于其可达性是未知的或可疑的路由器（处于不完全状态，或不存在此路由器的邻居缓存表项）。当路由器处于工作状态时，如果它总能返回可达或可能可达的路由器，协议实现可以选择返回相同路由器或以轮询的方式循环使用路由器列表中的路由器。

2) 当列表中没有路由器可达或可能可达时，路由器应以轮询的循环方式选定，以便使随后对缺省路由器的请求返回不同的路由器，直到选定所有其他的路由器。

在这种情况下循环路由器列表可确保邻居不可达检测算法探测到所有的可用路由器，共同完成对缺省路由器的请求和发送数据包到路由器，同时会对选定的路由器进行可达性探测。

3) 如果缺省路由器列表是空，所有目的地是在连接。

8.3.7 发送路由器请求消息

当接口被激活时，主机可以不必等待下一个非请求路由器通告来确定缺省路由器或获得前缀。为了快速获得路由器通告，主机应该发送 MAX_RTR_SOLICITATIONS 次路由器请求消息，每个消息间隔最少是 RTR_SOLICITATION_INTERVAL 秒。路由器请求可以在下列任何事件发生以后发送：

- 系统启动时接口初始化。
- 一个暂时的接口失败或由系统管理暂时设置为无效后，接口重新初始化。
- 系统管理关闭 IP 转发功能，系统从路由器变为主机。
- 主机初次连接到链路上。
- 主机在离开链路一段时间后重新连接到链路上。

主机发送路由器请求到全部路由器多播地址组。IP 源地址被设置为接口的单播地址或未规定的地址。如果 IP 源地址不是未规定的地址，则源链路层地址选项应该设置为主机的链路层地址。

在主机发送初始请求之前，它应该延迟一段时间再发送，此时间为 0 和 MAX_RTR_SOLICITATION_DELAY 之间的随机数。当许多主机在链路上同时启动时，可以起到减少拥塞的作用，例如，掉电恢复后可能发生

这种现象。如果接口被（再）激活后，主机已经执行了随机延迟（如作为重复地址检测的一部分），则没有必要在发送第一个路由器请求消息之前再执行延迟。

如果主机发送路由器请求并收到路由器生存期为非零的有效路由器通告，主机必须停止从此接口发送另外的请求，直到上面所述的事件之一再次发生。而且在发送路由器请求之前收到路由器通告的情况下，主机应该至少发送一次路由器请求。

非请求路由器通告可以是不完全的；请求的通告应该包含完全的信息。

如果主机发送了 MAX_RTR_SOLICITATIONS 次请求，并在发送了最后一个请求之后等待了 MAX_RTR_SOLICITATION_DELAY 秒，仍接收不到路由器通告，那么主机推断链路上不存在用于地址配置[ADDRCONF]的路由器。当路由器出现在链路上时，主机继续接收并处理路由器通告消息。

9 地址解析和邻居不可达检测

本节描述了与邻居请求和邻居通告消息相关的功能，并且包括了对地址解析及邻居不可达算法的描述。

根据地址自动配置中的规定，邻居请求和通告消息可用于重复地址检测。特别地，重复地址检测能够向它自己的临时地址发送带有不确定源地址的邻居请求消息，这个消息会触发节点使用这个地址来应答组播邻居通告消息，指出这个地址正在被使用。

9.1 消息有效性

9.1.1 邻居请求有效性

节点必须丢弃收到的任何不满足以下有效性检查的邻居请求消息：

- IP 跳数限制值是 255，也就是说路由器可能不能够转发这个包。
- 如果消息包含了 IP 认证头，此消息成功验证。
- ICMP 校验和正确。
- ICMP 代码值为 0。
- ICMP 长度是 24 或更大。
- 目的地地址不是组播地址。
- 所有包括的选项长度>0。
- 如果 IP 源地址是未规定的地址，IP 目的地是节点请求组播地址。
- 如果 IP 源地址是未规定的地址，消息中没有链路层源地址选项。

保留域和任何不可识别的可选项的内容必须忽略。将来协议中对向后兼容的修改必须指定预留域或新增可选项的内容；向后不兼容的修改可以采用不同的代码值。

任何已经定义的选项中的内容，如果没有被指定用于邻居请求消息中，那么这些内容必须忽略，但这个包必须按正常方式处理。可能出现在包中的惟一定义了选项是链路层源地址选项。

通过有效性检查的邻居请求称作有效请求。

9.1.2 邻居通告消息的有效性

节点必须丢弃收到的任何不满足以下所有有效性检查的邻居通告消息：

- IP 跳数限制域值是 255，也就是说这个包可能不能够被路由器转发。
- 如果此消息包含了一个 IP 验证头，此消息成功验证。

- ICMP 奇偶校验正确。
- ICMP 代码为零。
- 从 IP 长度得到的 ICMP 长度是 24 或更大。
- 目的地址不是一个组播地址。
- 如果 IP 目的地址是一个组播地址，请求标志位为 0。
- 所有包括的可选项长度>0。

必须忽略保留域和任何非确认选项中的内容。将来协议向后兼容进行修改时，可以规定保留域的内容或增加新的选项，也可以采用不同的码值。

必须忽略邻居通告消息中没有规定使用但定义的选项内容，其数据包的处理同正常的处理方式。可能定义的选项是目的地链路层地址选项。

通过有效性检查的邻居通告称作有效通告。

9.2 地址解析

地址解析是节点在给定 IP 地址的情况下决定其邻居链路层地址的过程。只对决定成为“在连接”的地址进行地址解析，并且发送端不知道相应的链路层地址。对组播地址决不执行地址解析。

9.2.1 接口初始化

当具有组播功能的接口激活后，节点必须加入这个接口的全部节点组播地址组，并加入每个接口 IP 地址相应的节点请求组播地址组。

分配给接口的地址在一段时间后会发生变化。新地址会增加，旧地址会删除。在这种情况下，节点必须分别加入和离开相应于新旧地址的节点请求组播地址。由于多个单播地址会映射成相同的节点请求组播地址，因此节点必须删除所有组播地址相应的地址后，才离开节点请求组播组。

9.2.2 发送邻居请求

当节点向邻居发送一个单播包，但又不知道邻居的链路层地址时，节点会执行地址解析。对具有组播能力的接口，在不完全（INCOMPLETE）状态时地址解析将产生邻居缓存表项，并且给该邻居发送邻居请求消息。请求消息发送给对应于目的地址的节点请求组播地址。

如果提出请求的包源地址与分配给发送端口地址中的地址相同，该地址应该位于发出请求的 IP 源地址中，否则应该使用分配给该接口的地址。在可能的情况下使用提示包的源地址，可保证邻居请求的接受方把 IP 地址加入其邻居缓存中，在随后返回的提示包流中可能使用此 IP 地址。

如果请求被发送给节点请求组播地址，发送端必须把链路层地址（如果有的话）包括在链路层源地址可选项中，否则发送端应该把链路层地址（如果有的话）包括在链路层源地址可选项中。在组播请求中需要包含链路层源地址，并分配给对端一个地址，就可以向该地址发送邻居通告。对单播请求，实现可以省略链路层源地址选项。如果发送端缓存中有对等节点的链路层地址，很可能在对等节点的缓存中也有存在发送节点的表项。因此，包不需要发送。

在等待地址解析完成的过程中，对于每个邻居发送端必须维护一个小的包队列，这个包队列等待地址解析的完成。此队列必须至少能容纳一个包，并且可以容纳多个包。但每个邻居包队列中的数量必须限定到一个小的值。当队列溢出时，新到达的包应该替换旧的表项。当地址解析完成时，节点应发送队列中的任何包。

在等待地址解析的回应消息时，即使没有额外的流量到达邻居，发送端应该以大约 RetransTimer 毫

秒间隔重传邻居请求消息。重传必须有频度限制，对每个邻居在 RetransTimer 毫秒间隔后最多发出一个请求消息。

如果等待 MAX_MULTICAST_SOLICIT 时间后，仍没收到邻居通告，说明地址解析失败。对于排队等待地址解析的每个包，发送端必须返回一个目的地不可达的 ICMP 提示包，其代码为 3。

9.2.3 收到邻居请求

不满足以下任何要求的有效邻居请求必须丢弃。

- 目的地址是分配给接收接口的有效单播地址或者泛播地址。
- 目的地址是用于节点提供代理服务的单播地址。
- 目的地址是执行重复地址检测的临时地址。

如果目的地址是临时的，邻居请求应按地址自动配置所述处理。否则按以下过程处理。如果源地址不是未规定的地址，但有链路层的地址，且请求包含了链路层源地址选项，那么接收端应为请求消息的 IP 源地址产生或更新邻居缓存表项。如果缓存项不存在，节点应产生新的一项，并且把可达状态设置为 STALE。如果缓存中此项已存在，且缓存的链路层地址与收到的链路层地址不同，那么缓存的地址应被新收到的地址所替代，并且该项的可达状态必须设为 STALE。

如果邻居缓存表项已经生成，IsRouter 标志应置为 FALSE。因为邻居请求消息没有包含发送者是否是路由器的指示，如果路由器发送了邻居请求，情况也相同。在发送端是路由器的情况下，后续的邻居通告或路由通告消息将会设置正确的 IsRouter 值。如果邻居缓存表项已经存在，不能修改其 IsRouter 标志。

如果源地址是未规定的地址，节点不能产生或更新邻居缓存表项。

对邻居缓存操作更新后，节点将按下节所述发送邻居通告响应。

9.2.4 发送请求的邻居通告

节点发送邻居通告到节点地址中的一个地址，作为对有效邻居请求的响应。该通告的目标地址是从请求消息的目标地址中拷贝过来的。如果请求消息的 IP 目的地址不是组播地址，那么可省略链路层目标地址选项；邻居节点的缓存值必须是最近收到的请求的值。如果请求消息的 IP 目的地址是组播地址，那么通告必须包括链路层目标地址选项。另外，如果节点是路由器，必须把 Router 标志设为 1，否则设为 0。

如果目标地址是泛播地址，或者是该节点用于提供代理服务的单播地址，或者不包括链路层目标地址选项，那么 Override 标志应设为 0，否则 Override 设为 1。Override 标志的正确设置可保证节点对非代理通告作出优先选择，即使收到代理通告，也可保证第一个泛播地址通告优先。

如果请求的源地址是未规定的地址，节点必须把请求标志设为 0，并把此通告消息按组播方式发送给所有节点地址。否则节点必须把请求标志设为 1，并把通告消息按单播方式发送给请求的源地址。

如果目的地址是泛播地址，发送端应延迟介于 0 ~ MAX_ANYCAST_DELAY_TIME 秒间的随机时间发送响应。

由于单播邻居请求不需要包括源链路层地址，有可能发送请求邻居通告的节点在其邻居缓存中没有相应的链路层地址。在这种情况下，节点要首先使用邻居发现来确定邻居的链路层地址（即发送组播邻居请求）。

9.2.5 接收邻居通告

当接收到有效的邻居通告（请求或者非请求）时，就在缓存中搜索目的地表项。如果没有表项存在，则删除该通告。不必重建不存在的表项，因为接收方没有启动与目的地的通信。

如果已经定位了合适的邻居发现表项，进行何种操作取决于邻居缓存器表项的状态，以及所提供的通告标志和实际的链路层地址。

当收到通告时，如果目的地的邻居缓存处于不完全状态，那么采取以下两种方式中的一种来处理。如果存在链路层地址，但没有包含目标链路层地址选项，则接收节点应该无条件地丢弃收到的通告，否则接收节点完成下列操作步骤：

- 在邻居缓存中表项链路层地址。
- 如果通告请求标志位置位，该项的状态置位可达，否则置位失效。
- 根据收到通告中 Router 标志位，设置缓存表项中的 IsRouter 标志位。
- 发送所有排队等待邻居地址解析的数据包。

如果缓存表项处于不完全状态，忽略 Override 标志位。

当收到通告时，目标的邻居缓存处于不是 INCOMPLETE 的任何其他状态，处理会相当复杂。如果 Override 标志位清零，且提供的链路层地址与缓存中的地址不同，那么按以下两种方式中的一种处理：如果表项的状态位为 REACHABLE，则置为 STALE，但并不用其他方式更新缓存；否则应该忽略收到的通告，并且不能更新该缓存。如果 Override 标志位置位，或者 Override 标志位清零同时提供的链路层地址与缓存中相同，或者没有提供目标表链路层地址，那么收到的通告必须按如下步骤更新邻居缓存项：

- 目标链路层地址选项中的链路层地址必须插入到缓存中（如果已提供地址并且与表项的地址不同）。
- 如果请求标志置位，表项的状态必须置为可达。如果请求标志清零，并且链路层地址被更新为不同的地址，那么缓存状态必须置为失效。否则表项的状态保持不变。

如果通告响应邻居请求，通告的请求标志应置位。由于邻居不可达检测请求是发送给缓存中的链路层地址，所以收到请求通告表明转发功能在起作用。然而收到非请求通告说明邻居有紧急的信息通告（如改变了链路层地址）。如果紧急信息显示改变来自正使用的节点，则当发送下一个包时节点应该验证（新）路径的可达性。不必更新缓存内容不变的非请求通告状态。

— 必须根据收到通告中 Router 标志，置位缓存表项中的 IsRouter 标志。在 IsRouter 标志从 TRUE 更新为 FALSE 的情况下，节点必须从路由器列表中删除该路由器，用该邻居作为路由器来更新所有目的地的目的地缓存表项。当作为路由器的节点配置为主机而停止转发包时，需要进行检测。

当邻居通告优先（即 Override 标志置位），或邻居通告指向与当前在缓存表项中相同的链路层地址时，上述规则保证了缓存的更新。如果上述情况没有发生，则通告通过改变缓存表项中的状态来发起以后的邻居不可达性检测（如果邻居不可达性检测还没有进行）。

9.2.6 发送非请求的邻居通告

在某些情况下节点可确定其链路层地址的改变（如热插入接口卡），并期望迅速把新的链路层地址通知给邻居。在这种情况下，节点可以最多发送 MAX_NEIGHBOR_ADVERTISEMENT 个非请求邻居通告消息到所有组播节点地址。这些通告之间的间隔至少有 RetransTimer 秒。

非请求通告的目标地址字段设为接口的 IP 地址，并且在目标链路层地址选项中填写新的链路层地址。为了避免干扰邻居不可达检测算法，Solicited 标志必须设为零。如果节点是路由器，它必须把 Router

标志置位，否则清零。Override 标志可以置为 1 或 0。在任何一种情况下，相邻节点将立即改变目的地址缓存的状态为失效，同时使它们验证路径的可达性。如果 Override 标志置为 1，相邻节点将在缓存中表项新的链路层地址，否则它们将忽略新的链路层地址，而选择探测缓存地址。

如果一个接口分配多个 IP 地址，节点可为每个地址分别组播邻居通告。在这种情况下，为了减少通告由于堵塞而丢失的概率，节点应该在发送每个通告之间引入一个小的延迟。

当代理的链路层地址改变，或者它配置（系统管理或其他机制）为一地址的代理，那么该代理可组播邻居通告。为了减少组播流量过多，如果存在多个为同一地址集提供代理服务的节点，那么这些代理应该提供一种机制来防止多个代理为任何一个地址组播通告。

此外，当节点的链路层地址改变时，属于泛播地址的节点可为泛播地址组播非请求邻居通告。

由于非请求通告并不是可靠地更新所有节点的缓存（不是所有的节点都能收到通告），它们仅仅被看作是一种性能优化，迅速地更新多数邻居缓存。尽管延迟可能会稍微长一点，但邻居不可达检测算法可保证所有的节点得到可达的链路层地址。

9.2.7 泛播邻居通告

从邻居发现的角度看，泛播地址的处理在大多数场合与单播地址的处理相同。因为泛播地址在语法规则上与单播地址一样，节点在对泛播地址执行地址解析或邻居不可达性检测时，处理方式与单播地址相同，不需要特殊处理。

除两种情况外，接口分配有泛播地址的节点，其处理泛播地址的方式和单播地址相同。第一种情况是，为了减少网络堵塞，响应邻居请求的邻居通告应该延迟一段介于 0 和 MAX_ANYCAST_DELAY_TIME 之间的随机时间。另一种情况是由于 Override 标志置为 0，因此，当收到多个通告时应采用第一个通告而不是最新收到的通告。

由于存在单播地址，当泛播地址的当前绑定失效时，邻居不可达检测保证节点快速检测泛播地址。

9.2.8 代理邻居通告

路由器可以作为一个或多个节点作代理，通过邻居通告来指示它愿意接收不是明确发向它的数据包。例如，路由器可以为离开“非连接”（Off-Link）的移动节点接收数据包。代理采用的机制与用于泛播地址的机制相同。

代理必须加入请求节点多播地址组，该地址组对应于代理节点的 IP 地址。

所有请求代理邻居通告消息必须把 Override 标志置为 0。如果节点在链路上，其邻居通告（Override 标志置为 1）将优先于任何从代理收到的通告。

代理可发送 Override 标志置为 1 的通告，但可能引起代理通告覆盖由节点创建的有效缓存。

最后，当发送响应邻居请求的代理通告时，发送端应延迟响应一段时间，延迟的时间介于 0 和 MAX_ANYCAST_DELAY_TIME 秒之间随机值。

9.3 邻居不可达性检测

任何时候通过邻居或到达邻居的通信，会因各种原因而中断，包括硬件故障、接口卡的热插入等。如果目的地失效，则恢复是不可能的，通信失败。如果路径失效，则恢复是可能的。因此节点应该主动地跟踪数据包发向邻居的可达性状态。

主机与邻居节点之间所有路径都应进行邻居不可达性检测，包括主机到主机、主机到路由器以及路由器到主机之间的通信。邻居不可达性检测也可用于路由器之间，但不要求使用相等的机制，例如，作

为路由协议的一部分。

当到邻居的路径失效时，应根据邻居的使用情况而采用特定的恢复程序。例如，如果邻居是最终目的地，应该重新进行地址解析。如果邻居是路由器，那么应切换到另一个路由器。在确定下一跳时包含了特定的恢复程序。通过删除邻居缓存表项，邻居不可达检测会提示需要进行下一跳确定。

只对发向邻居的单播包执行邻居不可达性检测；如果目的地是组播地址，则不进行检测。

9.3.1 可达性确认

如果节点最近收到确认，IP 层已经收到邻居最近发送出的数据包，那么该邻居是可达的。有两种方法支持这种确认：从上层协议来的提示，说明连接正在“转发进行中”，或者收到了应答邻居请求消息的邻居通告消息。

只有当最近发出的数据包真正到达了对方节点，从远端收到的数据包才能到达，连接才会处于“转发进行中”。例如，在 TCP 中收到一个（新的）确认表明以前发送的数据已到达对端，新（非重复的）的数据到达表明先前的确认信息已发送到远端。如果数据包到达对端，它们必须到达发送端的下一跳邻居；因此“转发进行中”是对下一个邻居可达的确认。对离开链路的目的地，“转发进行中”表示第一跳路由器是可达的。当上层信息可用时应利用上层信息。

在某些情况下（如基于 UDP 的协议和路由器向主机转发数据包），可达性信息可能不容易从上层协议得到。当无提示可用并且节点正向邻居发送数据包时，为了验证转发路径是否在工作，节点可以用单播邻居请求消息主动探查邻居。

由于发送请求标志位置位的通告消息来应答邻居请求，因此收到邻居请求通告消息可作为对可达性的确认。收到请求标志位为 0 的其他邻居发现消息，例如，路由器通告和邻居通告，不能认为是可达性确认消息。收到非请求消息仅仅确认了从发送端到接收节点的单向路径。相反，邻居不可达检测要求节点自己，而不是从邻居的方面来跟踪到邻居的转发路径状态信息。收到请求通告表明路径正在双向工作。请求必须已经到达邻居，提示它产生邻居通告消息。同样收到通告表明从发送端到接收端的单向路径正在工作。只有接收端知道后一种情况。通告的发送端不能直接知道它发送的通告实际已到达邻居，而邻居不可达性检测只关心转发路径的可达性。

9.3.2 邻居缓存表项状态

邻居发现的缓存器表项有以下 5 种状态：

INCOMPLETE（不完全）

正在执行对该表项的地址解析。尤其是邻居请求已经送往目的地的请求节点组播地址，但是还没有收到相应的邻居通告。

REACHABLE（可达性）

在最后 **ReachableTime** 微秒内收到正确的确认，邻居的转发路径工作正常。在可达状态期间，当发送数据包时不能发生特定的动作。

STALE（失效）

在收到邻居转发路径工作正常的正确确认后，经过了大于 **ReachableTime** 微秒的时间。在 **STALE** 状态期间，当发送数据包时不能发生特定的动作。在接收用于更新缓存链路层地址的非请求邻居发现消息时，进入 **STALE** 状态。收到消息并不能确认可达性，如果正在使用该表项，进入 **STALE** 状态可保证可达性迅速得到验证，直到该表项被使用时可达性才能得到验证。

DELAY (延迟)

在收到邻居转发路径工作正常的正确确认, 在最后的 DELAY_FIRST_PROBE_TIME 秒内发送了数据包后, 经过了大于 ReachableTime 毫秒的时间。如果在进入 DELAY 状态 DELAY_FIRST_PROBE_TIME 秒内没有收到可达性确认, 则发送邻居请求并把状态改为探测。

DELAY 状态的优点是上层协议提供了额外的时间来进行可达性确认, 在这种情况下由于缺少数据流, 最后的确认以后经历了 ReachableTime 微秒。如果没有这个优点, 即使 3 次握手会立刻提供可达性确认, 在数据流停止后打开的 TCP 连接可能会启动探测。

PROBE (探测)

在可达性确认收到以前, 重发邻居请求每隔 RetransTimer 微秒主动地寻找一次可达性确认。

9.3.3 节点行为

邻居不可达性检测与向邻居发送数据包同时进行。在邻居可达性确认期间, 节点继续向使用缓存链路层地址的邻居发送数据包。如果没有数据流向邻居, 则不发送检测。

当节点需要对邻居地址进行地址解析时, 它在 INCOMPLETE 状态创建一个表项, 并启动地址解析。如果地址解析失败, 该表项应该删除, 这样流向该邻居的后续数据流就可以再次激活下一跳确定程序。在节点上激活下一跳确定可保证使用替换的缺省路由器。

当收到可达性确认(通过上层设备或者请求的邻居通告)时, 表项的状态改为 REACHABLE。例外的是在 INCOMPLETE 状态, 上层设备对表项没有影响(例如, 没有缓存链路层地址)。

在收到邻居最后的可达性确认后经过 ReachableTime 微秒时, 邻居缓存表项状态 REACHABLE 改为 STALE。(注: 在数据包发向邻居以前, 状态从 REACHABLE 改为 STALE 的具体执行会有不同, 即不必设置与 ReachableTime 过期相关的时间溢出表项。)

节点第一次向表项状态为 STALE 的邻居发送数据包时, 发送方把状态改为 DELAY, 并把计时器的溢出时间设置为 DELAY_FIRST_PROBE_TIME 秒。如果计时器过期时表项还处于 DELAY 状态, 那么表项的状态改为 PROBE。如果收到了可达性确认, 那么表项的状态改为 REACHABLE。

在进入 PROBE 时, 节点向使用缓存链路层地址的邻居发送单播邻居请求消息。在状态处于 PROBE 期间, 节点每隔 RetransTimer 微秒重复发送邻居请求消息, 直到收到可达性确认。如果没有额外的数据包发给邻居, 重发探测。在发送 MAX_UNICAST_SOLICIT 请求后, 等待了 RetransTimer 微秒, 没有收到应答, 那么停止重送, 并且删除表项。发往邻居的后续流会重新创建一个表项, 并再次进行地址解析。

所有邻居请求的发送速率对每个邻居是有限制的。节点向同一个邻居发送邻居请求的频率不能超过 RetransTimer 微秒/次。

由于收到数据包而不是收到请求邻居通告(例如, 路由器请求、路由器通告、重定向和邻居请求)而创建邻居缓存表项时, 该表项状态就进入失效。这些数据包包含有发送方的链路层地址, 或者在重定向时的重定向目的地地址。接收到了这些链路层地址并不能确认通向该节点的转发路径是可达的。在失效状态为已知的链路层地址设置新创建的邻居缓存表项, 就能保证快速检测到路径的故障。另外, 由于接收到了上述消息, 如果缓存的链路层地址得到修改, 状态应该设置为失效, 以快速验证通向新的链路层地址的路径是正常工作的。

为了检测路由器的功能从路由器切换到主机的情况(例如, 系统管理关掉了 IP 转发功能), 主机必须把在所有收到的邻居通告消息中的路由器标志字段与在邻居缓存表项中的 IsRouter 标志相比较。当节

点检测到节点已经从路由器变成了主机，那么节点必须从缺省路由器列表中删除该路由器，并更新目的地缓存。如果目的地缓存表项正在使用该路由器（例如，主机向它重定向），它可以不列入缺省路由器列表。在这种情况下，所有以该（前）路由器为参照的目的地缓存表项在使用表项以前必须再次执行下一跳确定。

在某些情况下，与连接有关的信息可表明指向邻居的路径已经失效（例如，重新设置虚拟电路）。在这种情况下，在进行邻居可达检测以前，与连接有关的信息可用于清除邻居缓存的表项。但与连接有关的信息不能用于确认邻居的可达性；该信息不提供在相邻 IP 层之间端到端的确认。

10 重定向功能

本节叙述发送和处理重定向消息相关的功能。

由路由器发送重定向消息，为特定的目的地把主机重定向到更好的第一跳路由器，或者通知主机目的地实际上是邻居（即 on-link）。后者完成的方法是让 ICMP 目标地址与 ICMP 目的地址相同。

路由器必须能够确定每个邻居路由器的本地链路（link-local）地址，以保证重定向消息里的目标地址根据本地链路地址来识别邻居路由器。对于静态路由意味着下一跳路由器地址应该用路由器的本地链路地址来指定。对于动态路由意味着所有 IPv6 路由协议必须在某种程度上与相邻路由器交换本地链路地址。

10.1 验证重定向消息

如果收到的重定向消息不满足以下有效性检验，则主机必须丢弃：

- IP 源地址是本地链路地址。路由器必须在路由器通告和重定向消息中采用其本地链路地址作为源地址，这样主机能够惟一标识路由器。
- IP 跳数限定字段值为 255，即路由器不能转发数据包。
- 如果该消息中包括 IP 认证报头，消息验证正确。
- ICMP 检验有效。
- ICMP 码为 0。
- ICMP 长度（从 IP 长度得出） ≥ 40 字节。
- 重定向的 IP 源地址就是指定的 ICMP 目的地址的第一跳路由器。
- 在重定向消息中 ICMP 目的地址域不包含组播地址。
- ICMP 目标地址（在重定向指向路由器时）为本地链路地址，或（在重定向指向在连接 on-link 目的地时）与 ICMP 目的地址相同。
- 所有包括的选项长度 > 0 。

必须忽略保留域和任何非确认选项中的内容。将来协议向后兼容进行修改时，可以规定保留域的内容或增加新的选项，也可以采用不同的码值。

必须忽略路由器请求消息中没有规定使用但定义了选项内容，其数据包的处理同正常的处理方式。可能定义的选项是目标链路层地址选项和重定向头选项。

通过有效性验证的重定向称为“有效重定向”。

10.2 路由器要求

由于受到速率的限定，当路由器转发没有明确指定发向自己的数据包（即数据包源路由列表没有包括

该路由器)时, 路由器应该发送重定向消息:

- 数据包的源地址标识邻居;
- 路由器确定下一跳节点和到达转发包目的地地址的发送节点在同一链路上;
- 数据包的目的地址不是组播地址。

传送的重定向数据包所包含的格式为:

— 目标地址字段: 到达目的地的数据包应该发送到该地址。如果目标是路由器, 则必须采用该路由器的本地链路地址。如果目标是主机, 则目标地址域的值必须与目的地地址域相同。

— 目的地地址字段: IP 数据包的目的地地址。

— 选项:

- 目标链路层地址选项: 如果已知, 为目标链路层地址。
- 重定向头: 重定向数据包的长度不超过 1280 字节, 转发的数据包数量不限。

在源端没有正确应答重定向消息, 或者源端选择忽略没有被验证的重定向消息的情况下, 为了节省频带和处理的费用, 路由器必须限定发送重定向消息的速率。

在收到重定向消息时, 路由器不能更新路由表。

10.3 主机要求

主机收到有效的重定向消息后, 应该相应地更新其目的地缓存, 这样后续数据流就发向规定的目标。如果目的地缓存中没有该目的地的表项, 则创建一个这样的表项。

如果重定向包含有目标链路层地址选项, 则主机为该目标创建或更新邻居缓存的表项。在这两种情况下, 缓存的链路层地址从目标链路层地址选项中复制。如果为该目标创建了邻居缓存表项, 则可达性状态置于失效。如果缓存表项已经存在, 并且用不同的链路层地址进行了更新, 则可达性状态必须置于失效。如果链路层地址与已在缓存中的相同, 缓存表项状态保持不变。

如果目标和目的地地址相同, 主机必须把目标作为“在连接”来处理。如果目标地址与目的地地址不相同, 则主机必须把目标的 IsRouter 设为 TRUE 状态。如果目标和目的地地址相同, 但不能可靠地确定该目标地址是否是路由器。所以最新创建的邻居缓存表项应该把 IsRouter 设置为 FALSE, 而现有的缓存表项应该保持标志不变。如果目标是路由器, 则后续的邻居发现通告或路由器通告消息将相应地更新 IsRouter。

重定向消息应用于所有正在被发向给定目的地的数据流。在收到对目的地地址重定向消息时, 为了使用指定的下一跳, 对该地址的所有目的地缓存表项应该进行更新, 而不必考虑在重定向包头选项中出现流标签内容。

主机可以有配置开关, 该开关可以使主机忽略没有 IP 认证报头的重定向消息。

主机不能发送重定向消息。

11 选项处理

选项提供了对可变长度字段、在相同的包里出现多次的字段或不出现在所有包里的信息进行编码的机制, 也可以使用选项来增加额外的功能。

为了使 ND 将来的扩展能兼容目前的版本, 所有节点必须忽略接收的 ND 包中不被识别的选项。本标准规定的所有选项必须能够识别。节点不能因为 ND 消息包含不识别的选项而忽略有效的选项。

目前的选项定义接收者能在相同的包里独立地处理多个选项，将来的选项应该遵守下列规则：

选项不必依赖任何其他选项的存在或不存在。选项的语义应该仅依赖 ND 包固定部分的消息以及包含在选项里的信息。

如果遵守上述规则，那么：

1) 接收者能够独立处理选项，例如，实现可以选择在用户侧处理路由器通告消息内的前缀信息选项，而相同消息的链路层地址选项在内核里由路由进行处理。

2) 如果选项的数目使包的大小超过了链路的 MTU，多个包可以含有选项的子集，但不发生语义的变化。

3) 发送者可以发送不同包的选项子集。例如，如果前缀的有效性和首选生存期很高，在每个路由器通告中不必包含前缀信息选项。另外，不同的路由器可以发送不同的选项集合。接收者的动作不必和特定数据包内选项的存在相关联。本标准规定接收者应该根据定时器的超时和数据包内接收的信息来动作。

邻居发现的选项可以以任何顺序出现，接收者的处理与顺序无关，消息中也可以有多个相同选项（如前缀信息选项）。

如果路由器通告中包含选项的数目使通告的大小超过了链路 MTU，路由器可以发送包含选项子集的多个通告。

重定向头选项包含的数据数量必须限制，整个重定向包不能超过 1280 字节。

所有选项是 8 字节的整数倍，在没有填充选项时可确保字段排列整齐。除了 128 比特的 IP 地址/前缀按照 64 比特的边界排列外，定义的选项字段按照边界的自然大小排列（16 比特的边界安排 16 比特的字段）。链路层地址字段包含连续的字节串，它按照 8 比特的边界进行排列。

包含 IP 头的 ND 包大小限制了链路 MTU（至少 1280 字节）。当 ND 包中加入选项，节点不能超过链路 MTU。

协议的将来版本会定义新的选项类型。接收者必须能忽略它们不识别的任何选项，继续处理消息。

12 协议常数

路由器常数：

MAX_INITIAL_RTR_ADVERT_INTERVAL	16s
MAX_INITIAL_RTR_ADVERTISEMENTS	3 transmissions
MAX_FINAL_RTR_ADVERTISEMENTS	3 transmissions
MIN_DELAY_BETWEEN_RAS	3s
MAX_RA_DELAY_TIME	5s

主机常数：

MAX_RTR_SOLICITATION_DELAY	1s
RTR_SOLICITATION_INTERVAL	4s
MAX_RTR_SOLICITATIONS	3 transmissions

节点常数：

MAX_MULTICAST_SOLICIT	3 transmissions
-----------------------	-----------------

MAX_UNICAST_SOLICIT	3 transmissions
MAX_ANYCAST_DELAY_TIME	1s
MAX_NEIGHBOR_ADVERTISEMENT	3 transmissions
REACHABLE_TIME	30 000ms
RETRANS_TIMER	1 000 ms
DELAY_FIRST_PROBE_TIME	5s
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

其他协议常数在消息格式中定义。所有的协议常数随着协议版本的更新会发生改变。

13 安全性考虑

邻居发现很容易受到攻击，使 IP 包发送到不期望的目的地。这种攻击易引起拒绝服务，也会使节点截取和修改到达其他节点的数据包。

在没有认证的情况下，忽略接收来自非连接发送者的 ND 包可减少这种攻击。所有收到的包的跳数限制字段为 255（最大值）。路由器每次转发包时会减少跳数限制值，因此包含 255 值的数据包是由邻居发出。

拒绝服务攻击的例子是链路上以任意 IP 源地址发送包的节点可以通告自己为默认路由器，也可以发送使默认路由和在连接前缀超时的伪路由器通告消息。入侵者会通过发送多个路由器通告，对合法路由器进行服务攻击，其中消息的源地址设置为另一个路由器，路由器生存期设置为 0，所有前缀的选择和有效生存期设置 0。这种攻击会使所有包到达不正确的路由器，可是在连接或非连接的目的地。路由器然后有选择地检查、修改或丢弃链路上发送的包。如果不合法路由器用 R 比特设置为 1 的邻居通告回答了邻居不可达探测，邻居不可达检测就不能检测到这种黑洞。

许多链路层也容易受到这种攻击，例如，连续占用 CSMA/CD 网络的链路（如背对背发送数据包或者认为链路上信号冲突），或发起其他源地址的包使设备（如以太网交换机）工作混乱。重定向的模型和 IPv4 相同。仅当从相同路由器接收数据包时，使用重定向。如果主机重定向到另一个节点（如目的地是非连接），无法阻止目标发布另一个重定向到其他目的地。如果目标主机被破坏，就会充当隐藏路由器来转发流量。

本标准不能确定哪个邻居有权发送特定类型的消息（如路由器通告）。任何邻居即使在认证的情况下，发送路由器通告消息也会引起拒绝服务，并且任何邻居发送代理邻居通告和非请求邻居通告会引起潜在的拒绝服务。

邻居发现协议数据包交换使用 AH 进行认证。如果使用的安全联盟存在目的地址，发送邻居发现数据包时节点应该包括认证头。通过手工配置或密钥管理协议可以创建安全联盟。

邻居发现数据包的认证头必须验证其正确性，必须忽略认证不正确的包。

系统管理员可以配置节点，并忽略使用未使用 AH 或 ESP 进行认证的邻居发现消息。

14 重编号的考虑

邻居发现协议和 IPv6 地址自动配置相结合可以提供重编号机制——引入新的前缀和地址，删除旧的前缀和地址。

这种机制的健壮性是基于链路上所有的节点能实时地接收路由器通告消息，但主机在一段长时间里有可能处于关机或不可达的状态，这种情况下可以进行重编号，但对通告的前缀长度必须有所限制。

考虑下面的一个例子，前缀初始通告的生存期为两个月，如果9月1号前缀需要重编号，在8月1号时就要确定前缀是否需要删除。因此可以在8月1号时开始减少通告生存期为1周，当接近截止期时，生存期渐渐缩短，直到9月1号时前缀通告的生存期为0。如果在9月1号之前一个或多个节点从链路上离开，如果它上次接收的生存期是两个月，这些节点仍然认为前缀是有效的。如果在7月31号移去节点，节点认为前缀的有效期至9月30号。如果节点在9月30号前返回到链路上，它可以继续使用旧的前缀。强制节点停止使用已经通告长生存期前缀的方法是使节点接收一个生存期改变了的前缀通告，例如：从9月1号到10月1号，以生存期为0的前缀进行通告。

通常，为了保证离开链路节点的健壮性，链路上的任何节点都应长期跟踪前缀的有效期，直到将来的某一刻，然后前缀的生存期才通告为0。这个时间应是最大值，等于发送通告的时间加上通告包含的前缀生存期。

上述使用的都是有限生存期。如果前缀通告的是有限生存期，以后的前缀需要重编号。一般不希望继续通告生存期为0的前缀，因此应该避免使用有限的生存期，或必须限制节点回到链路前离开链路的时间。

网络管理员应考虑使用相对短的生存期（例如，不超过几周），使用长的生存期有利于保证健壮性，但路由器不正常工作时主机不能通信。这种路由器将发送包含适当前缀的路由器通告。连接到路由器不工作的网络上的主机会比没有有效前缀和地址的主机存在更多的问题。

对于首选和有效生存期不作区分。因为首选生存期不超过有效生存期，实际上只需要跟踪有效生存期。
