本文翻译者：　　weicq2000

RFC 4861　　IPv6 邻居发现

(2007 年 9 月)

摘要

本文件规定了 IPv6 邻居发现(Neighbor Discovery, ND)协议。在同一链路上的 IPv6 节点使用 Neighbor Discovery，发现彼此的存在，确定彼此的链路层地址，发现路由器，以及维护通向激活状态邻居的路径的可达性信息。

目录

第 1 章　介绍

本标准定义了 IPv6 邻居发现(ND)协议。节点(主机或路由器)使用 ND，可以确定已知驻留在其附着的链路上的邻居们的链路层地址，快速清除已经变得无效的缓存值。主机也使用 ND 发现临近的、愿意代表它们转发分组的路由器。最后，节点使用此协议主动跟踪哪一个邻居可通达，哪一个邻居不可通达，以及侦听邻居们改变的链路层地址。当路由器或到路由器的路径出现故障时，主机主动搜索正常运行的替代者。

除非规定了其他情况(在特定链路类型上运行 IP 的文件中讨论)，本文件适用所有链路类型。然而，因为 ND 的一些服务使用链路层多播，在某些链路类型(例如，非广播多址(Non-Broadcast Multi-Access, NBMA)链路)上，可能规定使用其他协议或机制来实现这些服务(在特定链路类型上运行 IP 的文件中讨论)。本文件中描述的服务不直接依靠多播，例如 Redirects、下一跳确定、Neighbor Unreachability Detection 等。可以认为这些服务按照本文件中的规定提供。如何在 NBMA 链路上使用 ND 的细节在[IPv6-NBMA]中介绍。此外，[IPv6-3GPP]和[IPv6-CELL]讨论了本协议在蜂窝链路上的应用，它们是 NBMA 链路的例子。

第 2 章　术语

2-1　一般术语

- IP- IPv6 (Internet Protocol Version 6)：

  术语 IPv4 和 IPv6 仅用于必须避免混淆情况。

- ICMP(Internet Control Message Protocol)：

  术语 ICMPv4 和 ICMPv6 仅用于必须避免混淆情况。

- 节点(node)：

  执行 IP 协议的设备。

- 路由器(router)：

  一个节点，转发不是显示寻址到自己的 IP 分组。

- 主机(host)：

  任何不是路由器的节点。

- 上层(upper layer)：

  紧挨着下面的 IP 层的协议层。例如传输协议 TCP 和 UDP、控制协议 ICMP、路由协议 OSPF，以及被在 IP 上“隧道化”(即，被封装进 IP)的互联网络层(或低层)协议，例如 IPX、AppleTalk 或 IP 自身。

- 链路(link)：

  通信设施或媒介，是紧挨着上面的 IP 层的协议层，节点能够在其上的链路层通信。例如以太网(简单或桥接)、PPP 链路、X.25、帧中继、ATM 网络，以及互联网络层(或高层)“隧道”，例如 IPv4 或 IPv6 自身之上的隧道。

- 接口(interface)：

节点附着到链路的点。

- 邻居(neighbors)：
  附着在相同链路的节点们。
- 地址(address)：一个接口或一组接口的 IP 层标识符。
- 任播地址(anycast address)：
  一组接口的标识符(典型属于不同节点)。发送到任播地址的分组被交付给由那个地址标识的一组接口之一(交付给“最近”的一个接口，按照路由协议的距离度量)。参阅[ADDR-ARCH]。注意，任播地址在语义上与单播地址不能区分。于是，发送分组到任播地址的节点通常不知道任播地址正在被使用。本文件的其余部分，在节点没有意识到单播地址实际上是任播地址的情况，把单播地址也看作是任播地址。
- 前缀(prefix)：
  由地址的一些起始比特构成的比特串。
- 链路层地址(link-layer address)：
  接口的链路层标识符。例如以太网链路的 IEEE802 地址。
- on-link：
  一个地址。该地址分配给特定链路上的接口。如果满足下述条件，节点认为地址是 on-link：
  - 该地址由链路的多个前缀之一覆盖(例如，由Prefix Information选项中on-link标记标识)，或
  - 邻近路由器规定该地址为Redirect消息的目标，或
  - 收到针对该(目标)地址的Neighbor Advertisement消息，或
  - 从该地址收到任何Neighbor Discovery消息。
- off-link：
  与“on-link”相反；它也是一个地址，该地址没有分配给特定链路上的任何接口。
- 最长前缀匹配(longest prefix match)：
  在覆盖目标地址的一组前缀中确定一个前缀的处理。如果前缀中的所有比特匹配目标地址的最左边比特，目标地址由该前缀覆盖。当多个前缀覆盖一个地址时，最长前缀是那个匹配的前缀。
- 可达性(reachability)：
  在任何情况下通向邻居的单向“转发”路径正在正常运行。尤其是，是否发送到邻居的分组正在达到邻居的 IP 层，以及正在被接收 IP 层适当处理。对于邻近路由器，可达性意味着由节点的 IP 层发送的分组被交付到该路由器的 IP 层，并且该路由器的确正在转发分组(即，它被配置为路由器，而不是主机)。对于主机，可达性意味着由节点的 IP 层发送的分组正在交付到邻居主机的 IP 层。
- 分组(packet)：
  IP 首部加上净荷。
- 链路 MTU(link MTU)：
  最大传输单元，即，以字节为单位的最大分组尺寸，它能在链路上用一个传输单元传送。
- 目标(target)：
  一个地址，该地址的地址解析信息正在被搜索；或者是在进行重定向操作时新的第一跳地址。
- 代理(proxy)：
  代表另一个节点响应 Neighbor Discovery 询问消息的节点。代表已经 off-link 的移动节点的路由器实际上是该移动节点的代理。
- ICMP 目的地不可达指示(ICMP destination unreachable indication)：

返回到分组原始发送者的出错指示。该分组由于在[ICMPv6]中描述的原因不能被交付。如果发生出错的节点不是分组的原始节点，产生 ICMP 出错消息。如果发生出错的节点是分组的原始节点，实际上不要求产生和发送一个 ICMP 出错分组到此原始节点，只要通过适当机制通知上层发送者即可(例如，来自过程呼叫返回值)。然而应注意，在某些情况下，按一般出错处理程序：取出违规分组，生成 ICMP 出错消息，接着交付该消息(在本地)，返回出错到发送者更为方便。

- 随机延时(random delay)：

发送消息时，有时必须延时一个随机时间发送，这可减少多个节点在同一时刻一起发送的可能，也可防止节点间长期同步周期发送[SYNC]。当需要随机分量时，节点以这样一种方法计算实际延时：计算出的延时为均匀分布随机值，该值在规定的最小延时时间和最大延时时间之间。实现者必须确保求出的随机量粒度和计时器解析度足够高，使得多个节点延时相同时间的概率较小。

- 随机延时种子(random delay seed)：

如果计算随机延时量时使用伪随机数发生器，此发生器在使用前应当用唯一的种子初始化。注意，单独使用接口标识符做种子是不够的，因为接口标识符不总是唯一的。为了降低重复接口标识符引起使用相同种子的概率，计算种子应当采用变化的输入源(例如，机械量)，这些输入源很可能是不同的，即使在相同的“匣子”内。例如，将接口标识符与 CPU 系列号合起来做种子。关于随机化和随机数发生器的更多信息参阅[RAND]。

2-2　链路类型

不同链路层有不同特性。与 Neighbor Discovery 有关的链路特性是：

- 多播能力(multicast capable)：

一条链路，它在链路层上支持一种本地机制，发送分组到所有邻居(即，广播)，或所有邻居的一个子集。

- 点对点(point-to-point)：

一条链路，它仅连接两个接口。假定点对点链路有多播能力和链路本地地址。

- 非广播多址(non-broadcast multi-access, NBMA)：

一条链路，有多于两个接口附着到它，但是该链路不支持多播或广播的本地形式(例如，X.25、ATM、帧中继等)。注意，预期所有链路类型(包括 NBMA)为需要多播的应用提供多播服务(例如，使用多播服务器)。然而，需要研究的是：是否 ND 应当使用这种功能，或为 ND 提供等效多播能力的替代机制。

- 共享介质(shared media)：

一条链路，它允许众多节点间直接通信，但是附着在共享介质上的节点们按这样一种方法配置：对于所有 on-link 目的地，它们没有完整的前缀消息。即，在 IP 层，在同一链路上的节点们或许不知道它们彼此是邻居；默认情况，它们通过路由器通信。例如大型公共数据网络，如 SMDS 和 B-ISDN。也称为“大型云”。参阅[SH-MEDIA]。

- 可变MTU(variable MTU)：

一条链路，它没有公认的MTU(例如，EEE 802.5令牌环)。许多链路(例如，以太网)有由链路层协议或由特定的文件定义的标准MTU，描述如何在链路层上运行IP。

- 非对称可达性(asymmetric reachability)：

一条链路，在那里，非折返可达性，和/或非传递可达性是正常操作的一部分。(非折返可达性意味着分组可从A到B的，但是分组不能从B到A。非传递可达性意味着分组可从A到B，并且分组可从B到C，但是分组不能从A到C。)许多无线链路具有这种性质。

2-3　地址

ND 使用大量不同地址，它们在[ADDR-ARCH]中定义，包括：

- 所有节点多播地址(all-nodes multicast address)：

  到所有节点的链路本地范围地址，FF02::1。

- 所有路由器多播地址(all-routers multicast address)：

  到所有路由器的链路本地范围地址，FF02::2。

- 请求-节点多播地址(solicited-node multicast address)：

  链路本地范围多播地址，它作为请求的目标地址的函数经计算得到，参见[ADDR-ARCH]。借助于此函数，仅在最高有效位不同(例如，由于与不同提供者关联的多个前缀)的 IP 地址，被映射到相同的请求-节点地址，于是减少了节点在链路层必须加入的多播地址数目。

- 链路本地地址(link-local address)：

  仅有链路范围的单播地址，用于连通邻居们。所有路由器上的接口必须有链路本地地址。此外，[ADDRCONF]也要求主机上的接口有链路本地地址。

- 未指定地址(unspecified address)：

  保留地址值，它表示没有这个地址(例如，地址未知)。它决不能用于目的地地址，但是可用于源地址，如果发送者(还)不知道它自己的地址(例如，在无状态地址自动配置期间验证地址没有被使用时[ADDRCONF])。未指定地址的值为 0:0:0:0:0:0:0:0。

注意，对于源和目的地地址的范围，本标准没有严格遵循[ADDR-SEL]中的一致性要求。有可能在一些情况下，主机使用的源地址的范围比IPv6首部中目的地地址的范围更大。

2-4　要求

本文中使用的关键词MUST、MUST NOT、REQUIRED、SHALL、SHALL NOT、SHOUT、SHOUT NOT、RECOMMENDED、MAY和OPTIONAL，其含义参阅[KEYWORDS]。

本文件也使用了描述协议行为的内部概念性变量，以及实现中必须允许系统管理者改变的外部变量。本文件举例特殊变量名称，它们的值如何改变，以及它们的设置如何影响协议行为

来演示协议行为。不要求实现中和这里完全一样的使用它们，只要其外部行为与本文件描述的一致即可。

第 3 章　协议综述

本文件解决了一系列与附着到同一链路的节点间互动有关的问题。定义了解决下述每个问题的机制。

路由器发现(Router Discovery:)：主机如何查找驻留在其附着的链路上的路由器。

前缀发现(Prefix Discovery)：主机如何发现地址前缀集合，这些地址前缀定义了哪个目的地是附着链路的 on-link。(节点使用前缀把驻留在 on-link 的目的地，和需要通过路由器才能到达的目的地相区别。)

参数发现(Parameter Discovery)：节点如何学习到放置在发出分组中的链路参数(例如链路 MTU)或互联网参数(例如跳数限制值)。

地址自动配置(Address Autoconfiguration)：介绍了一种机制，该机制是允许节点以无状态方式配置接口地址所需要的。无状态地址自动配置参阅[ADDRCONF]。

地址解析(Address resolution)：当仅给定目的地的 IP 地址时，节点如何决定一个 on-link 目的地(例如，一个邻居)的链路层地址。

下一跳确定(Next-hop determination)：映射 IP 目的地地址为邻居 IP 地址的算法，到该目

的地的流量应当被发送到该邻居。下一跳可以是路由器或目的地自身。

邻居不可达检测(Neighbor Unreachability Detection)：节点如何确定邻居不再可达。如果邻居被用作路由器，其不可达时需要尝试替代默认路由器。对于路由器和主机，可以再次执行地址解析。

重复地址检测(Duplicate Address Detection)：节点如何确定在任何情况下它希望使用的地址已经由另一个节点使用。

重定向(Redirect:)：路由器如何通知主机，有到达特定目的地的较好第一跳节点。

ND 定义了 5 个不同的 ICMP 分组类型：Router Solicitation 和 Router Advertisement 消息，Neighbor Solicitation 和 Neighbor Advertisements 消息，以及 Redirect message 消息。这些消息服务于下述目的：

Router Solicitation：当接口使能后，主机可以发出 Router Solicitations，要求路由器立即生成 Router Advertisements，而不是在它们的下一个规定时间生成。

Router Advertisement：路由器周期地用此消息通告它们的存在及各种链路参数和互联网参数，或响应 Router Solicitation 消息。Router Advertisements 包括前缀，这些前缀用于确定是否另一个地址共享相同链路(on-link 确认)和/或地址配置，建议的跳数限制值，等等。

Neighbor Solicitation：由节点发送，以便确定邻居的链路层地址，或者通过缓存的链路层地址验证邻居仍然可达。Neighbor Solicitations也用于Duplicate Address Detection。

Neighbor Advertisement：响应Neighbor Solicitation消息。节点也可以发送非请求的Neighbor Advertisements，通知链路层地址改变。

Redirect：由路由器使用，用于通知主机有到目的地的较好的第一跳。

在有多播能力的链路上，每个路由器周期多播Router Advertisement分组，宣告自己的存在。主机从所有路由器收到Router Advertisements后，建立默认路由器列表。路由器足够频繁地发出Router Advertisements，主机们在几分钟内便可得知路由器们的存在，但是还没有频繁到足以依靠通告的缺乏就可检测到路由器出故障；独立的Neighbor Unreachability Detection算法提供失败检测。

Router Advertisements包含用于on-link确定和/或自动地址配置的前缀列表；与前缀关联的标记规定特定前缀的预期使用。主机使用通告的on-link前缀去建立和维护一个列表，该列表用于确定何时分组的目的地是on-link或超出路由器范围。注意，目的地能够是on-link，即使它没有被任何通告的on-link前缀覆盖。在此情况，路由器能够发送Redirect，通知发送者目的地是邻居。

Router Advertisements(和每个前缀标记)允许路由器通知主机如何执行Address Autoconfiguration。例如，路由器能够规定是否主机应当使用DHCPv6和/或自动(无状态)地址配置。

Router Advertisement消息也包含互联网参数，例如主机在发出分组中使用的跳数限制，以及可选的链路参数，例如链路MTU。这有利于关键参数的集中管理，这些关键参数能够在路由器上设置并自动传播给所有附着的主机。

节点通过多播Neighbor Solicitation(它要求目标节点返回自己的链路层地址)完成地址解析。Neighbor Solicitation消息被多播到目标地址的请求-节点多播地址。此目标用单播Neighbor Advertisement消息返回它自己的链路层地址。一对请求-响应分组，对于解析相互链路层地址的初始者和目标来说是足够的；初始者在Neighbor Solicitation中包括它的链路层地址。

Neighbor Solicitation消息也能够用于确定是否多于一个节点已经被分配了相同的单播地址。针对Duplicate Address Detection的Neighbor Solicitation消息的使用参阅[ADDRCONF]。

Neighbor Unreachability Detection检测出故障的邻居，或检测通向邻居的转发路径有故障。为做到此，要求肯定确认，即，发送到邻居的分组们实际上正在抵达那个邻居，并正由那个邻居的IP层正常处理。Neighbor Unreachability Detection用于从两个源进行确认。如果可能，上层协议对连接正在处于“转发过程”中提供一个肯定的确认，即，认为先前发送的数据已经被正确交付(例如，最近收到新的确认)。当不能通过这样的“暗示”获得肯定确认时，节点发送单播Neighbor Solicitation消息，该消息请求Neighbor Advertisements作为来自下一跳的可达性确认。这减少了不必要的网络流量，试探消息仅发送到节点正在主动发送分组去的邻居。

除了处理上述一般问题外，Neighbor Discovery也处理下述情况：

链路层地址改变：知道自己的链路层地址已经改变的节点能够多播若干(非请求)Neighbor Advertisement分组到所有节点，快速更新缓存的、已经变得无效的链路层地址。注意，发送非请求通告仅仅是一个性能增强(即，非可靠)。Neighbor Unreachability Detection算法才能确保所有节点将可靠地发现新地址，尽管延时或许有点长。

入境负载均衡：拥有重复接口的节点或许希望在同一链路上跨多个网络的接口间，对输入分组的接收进行负载均衡。这样的节点有多个分配给同一个接口的链路层地址。例如，单一网络驱动器能够代表多个网络接口卡，作为有多个链路层地址的单一逻辑接口。

通过允许路由器忽略来自Router Advertisement分组的源链路层地址，Neighbor Discovery允许路由器为寻址到它自己的流量执行负载均衡，借此强迫邻居们使用Neighbor Solicitation消息去学习路由器们的链路层地址。接着返回的Neighbor Advertisement消息能够包括链路层地址，这些地址根据发出请求者的不同而不同。本标准没有定义允许主机对输入分组进行负载均衡的机制。参阅[LD-SHRE]。

任播地址：任播地址标识一组提供等效服务的节点之一，在同一链路上的多个节点可被配置认可相同的任播地址。通过使节点们盼望接收多个相同目标的Neighbor Advertisements，Neighbor Discovery处理任播。所有任播地址的通告被标记为非替代(non-Override)通告。非替代通告是这样的通告，它不能更新或取代由另一个通告发送的信息。这些通告稍后将在讨论Neighbor通告消息内容时介绍。这引发在潜在的多个通告中应当使用哪一个的判决规则。

代理通告：愿意代表一个目标地址(该地址不能响应Neighbor Solicitations)接收分组的节点能够发布非替代Neighbor Advertisements。代理通告由MIPv6归属地代理使用，用于当移动节点移动到off-link时保护移动节点的地址。然而，它不能作为一个处理节点的常规机制，例如不能执行本协议。

3-1　与IPv4的比较

IPv6的 Neighbor Discovery协议对应于IPv4的Address Resolution Protocol [ARP]，ICMP Router Discovery [RDISC]和ICMP Redirect [ICMPv4]的组合。在IPv4中对Neighbor Unreachability Detection没有形成一致的协议和机制，虽然Hosts Requirements [HR-CL]文件为Dead Gateway Detection(难对付的Neighbor Unreachability Detection套件的子集)规定了一些可能的算法。

相对上述IPv4协议组，Neighbor Discovery协议有多方面改善：

Router Discovery是基础协议集的一部分；不需要主机“窥探”路由协议。

Router Advertisements携带链路层地址；解析路由器的链路层地址不需要附加分组交换。

Router Advertisements携带链路的前缀；不需要有独立的配置“网络掩码”机制。

Router Advertisements使能地址自动配置。

路由器能够为主机通告链路上使用的MTU，确保所有节点在缺乏约定的MTU的链路上使用相同的MTU值。

地址解析多播被“扩展”到超过1.6千万(2^{24})个多播地址，极大地减少了在节点上而不是在目标上的地址-解析-相关中断。此外，非IPv6机将完全不会被中断。

重定向包含了新第一跳的链路层地址；一旦接收到重定向，不需要独立的地址解析。多个前缀能够被关联到同一个链路。默认情况，主机从Router Advertisements中学习到所有on-link前缀。然而，路由器可以被配置成忽略来自Router Advertisements的某些或所有前缀。在这些情况，主机假定目的地是off-link并发送流量到路由器。接着一个路由器能够发布适当的重定向。

与IPv4不同，IPv6重定向的接收者假定新的下一跳是on-link。在IPv4，按照链路的网络掩码，主机忽略规定下一跳不是on-link的重定向。IPv6重定向机制类似在[SH-MEDIA]中描述的XRedirect功能。可以期望IPv6重定向机制将用于非广播和非共享媒介链路上，在那里要求节点知道所有on-link目的地的前缀是不现实的或不可能的。

Neighbor Unreachability Detection是基础部分，它在很大程度上改善了存在失效路由器，部分链路有故障或隔离的链路，或节点改变它们的链路层地址等情况下分组交付的茁壮性。例如，移动节点能够在不丢失任何连接(由于过期的ARP缓存)情况下移到off-link。

与ARP不同，Neighbor Discovery检测半程链路(half-link)故障(使用Neighbor Unreachability Detection)并避免发送流量到不能实现双向连接的邻居。与IPv4中的Router Discovery不同，Router Advertisement消息不包含优先权字段。处理不同“稳定性”的路由器不需要优先权字段；Neighbor Unreachability Detection将检测出有故障的路由器，并转换到正常工作的路由器。

链路本地地址唯一标识路由器，它的使用(对于Router Advertisement消息和Redirect消息)使得在为了应用新的全球前缀而进行站点重新编码的事件中，主机有可能维持与路由器的关联。

通过设置Hop Limit为255，Neighbor Discovery不受off-link发送者(该发送者偶然地或故意地发送ND消息)的影响。在IPv4中，off-link发送者既能够发送ICMP Redirects消息又能够发送Router Advertisement消息。

在ICMP层设置地址解析使得协议比ARP更加介质-独立，并使得有可能使用适当的常规IP层认证机制和安全机制。

3-2　支持的链路类型

Neighbor Discovery支持不同特性的链路。面对多种链路特性，本文件仅完整规范了ND协议机制的一个子集：

点对点：Neighbor Discovery处理这类链路就像处理多播链路一样。(多播能够很容易地在点对点链路上提供，接口可分配链路本地地址。)

多播：Neighbor Discovery在多播使能链路上的操作正如本文件所述。

非广播多路访问(non-broadcast multiple access, NBMA)：Redirect、Neighbor Unreachability Detection和下一跳确定的实现如本文所述。本文件没有规定地址解析，以及在NBMA链路上交付Router Solicitations和Router Advertisements的机制。注意，如果主机支持默认路由器列表人工配置，主机能够从Redirect消息中动态获得它们邻居的链路层地址。

共享介质：在[SH-MEDIA] 中XRedirect 消息之后塑造了Redirect消息，以便简化本协议在共享介质链路上的使用。

本标准没有涉及仅与路由器有关的共享介质问题，诸如：

路由器们如何在共享介质链路上交换可达性信息？

路由器如何确定主机的链路层地址？为解决此路由器需要发送重定向消息到该主机。

路由器如何确定它是接收分组的第一跳路由器？

本协议被扩展(通过定义新的选项)后，将来可能提出其他解决方案。

可变MTU：Neighbor Discovery允许路由器为链路规定MTU，接着所有节点使用该MTU。链路上的所有节点必须使用相同的MTU(或Maximum Receive Unit)，以便多播能够正常

工作。否则，当多播时，发送者(它或许不知道哪个节点将接收分组)不能确定所有接收者都能处理的最小分组尺寸(或Maximum Receive Unit)。

非对称可达性：Neighbor Discovery检测是否没有对称可达性；节点避免连接到不能支持对称连接的邻居的路径上。

Neighbor Unreachability Detection将标识出这类半链路，节点将忍住不使用它们。估计本协议在将来会被扩展，以便在缺乏折转的、可迁移的连接环境中寻找适用的路径。

3-3 安全的Neighbor Discovery消息

各种功能都需要Neighbor Discovery消息。几种功能设计用来使主机能确定地址的所有权，或在链路层地址和IP地址间映射。与Neighbor Discovery相关的弱点在第11-1讨论。对于安全的Neighbor Discovery的通用解决方案超出本标准的范围，在[SEND]讨论。然而，第11-2节说明了如何及在哪些限制下IPsec Authentication Header (AH)或Encapsulating Security Payload (ESP)能够用来保证Neighbor Discovery的安全。

第4章 消息格式

本章介绍本标准中使用的所有消息的格式。

4-1 Router Solicitation消息格式

主机发送Router Solicitations以便督促路由器尽快生成Router Advertisements。Router Solicitation消息格式如图1所示。

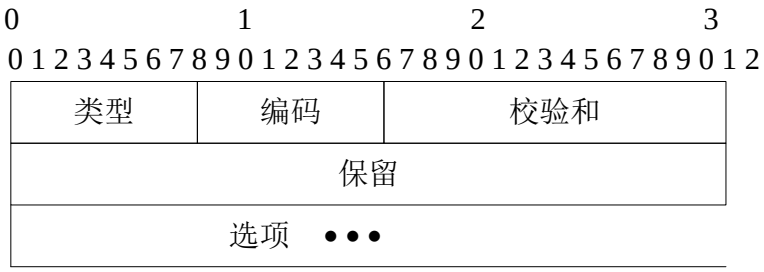

图1 Router Solicitation消息格式

IP字段：

Source Address

分配给发送接口的IP地址，或未指定地址，如果没有分配地址给发送接口。

Destination Address

典型为所有路由器多播地址。

Hop Limit

255

ICMP字段：

Type

133

Code

0

Checksum

ICMP校验和，参阅[ICMPv6]。

Reserved

此字段不使用。它必须由发送者初始化为0，接收者必须忽略它。

合法选项：

源链路层地址

发送者的链路层地址，如果知道。如果Source Address是未指定地址，必须不包括在内。否则，有地址的链路层上应当包括源链路层地址。

本协议的将来版本或许定义新的选项类型。接收者必须静默忽略任何它们不能识别的选项并继续处理消息。

4-2 Router Advertisement消息格式

路由器周期地发出Router Advertisement消息，或因响应Router Solicitations而发送Router Advertisement消息。Router Advertisement消息格式如图2所示。

图2 Router Advertisement消息格式

IP字段：

Source Address

必须是分配给该接口的链路本地地址，从该接口此消息被发送出去。

Destination Address

典型为引起Router Solicitation的Source Address，或所有节点的多播地址。

Hop Limit

255

ICMP字段：

Type

134

Code

0

Checksum

ICMP校验和，参阅[ICMPv6]。

Cur Hop Limit

8位无符号整数。默认值应当放置在发出IP分组的IP首部的Hop Count字段中。取0值意味着未(由该路由器)规定。

M

1位“管理地址配置”标记。当置1时，它指出地址可通过Dynamic Host Configuration协议获得[DHCPv6]。

如果M标记置1，O标记为冗余，可以忽略，因为DHCPv6将返回所有可用配置信息。

O

1位“其他配置”标记。当置1时，它指出其他配置信息可通过DHCPv6获得。例如，这类信息包括DNS相关信息或关于网络内其他服务器的信息。

注意，如果既没有M标记也没有O标记被置1，这指出没有信息可通过DHCPv6获得。

Reserved

6位未使用字段。它必须由发送者初始化为0，接收者必须忽略它。

Router Lifetime

16位无符号整数。与默认路由器关联的生存期，以秒为单位。最大值18.2小时。取0值的Lifetime指出路由器不是默认路由器并且不应当出现在默认路由器列表中。Router Lifetime仅适用于作为默认路由器的路由器应用；对包括在其他消息字段或选项中的信息不适用。需要对它们的信息规定时间限制的选项有它们自己的生存期字段。

Reachable Time(可到达时间)

32位无符号整数。此时间以毫秒计，在收到可达性确认后节点假定该邻居是可到达的。它由Neighbor Unreachability Detection算法使用(参阅第7-3节)。此值为0意味着没有(由此路由器) 作出规定。

Retrans Timer(重新传输计时器)

32位无符号整数。重发的Neighbor Solicitation消息间隔时间，以毫秒计。由地址解析和Neighbor Unreachability Detection算法使用(参阅第7-2节和第7-3节)。此值为0意味着没有(由此路由器)作出规定。

可能的选项：

源链路层地址

发出Router Advertisement的接口的链路层地址。仅在有地址的链路层上使用。路由器可以忽略此选项，以便能够使入境负载跨多个链路层地址共享。

MTU

在有可变MTU的链路上应当按此发送流量(正如在描述特定链路类型上如何运行IP的文件中规定的)。可以按此在其他链路上发送流量。

Prefix Information

这些选项规定了前缀，这些前缀是on-link的，和/或被用于地址自动配置。路由器应当包括所有它的on-link前缀(链路本地前缀除外)，所以多归属第主机有完整的前缀信息，这些前缀是关于主机们附着的链路的on-link目的地的。如果缺乏完整信息，当发送流量到它的邻居们时，多归属地主机或许不能够选择正

确的出接口。

本协议的将来版本或许定义新的选项类型。接收者必须静默忽略任何它们不能识别的选项，并继续处理消息。

4-3 Neighbor Solicitation消息格式

节点发送Neighbor Solicitations消息，请求目标节点的链路层地址，同时也提供它们自己的链路层地址给目标节点。当节点需要解析地址时，多播发送Neighbor Solicitations消息；当节点搜索以便验证邻居的可达性时，单播发送Neighbor Solicitations消息。Neighbor Solicitation消息格式如图3所示。

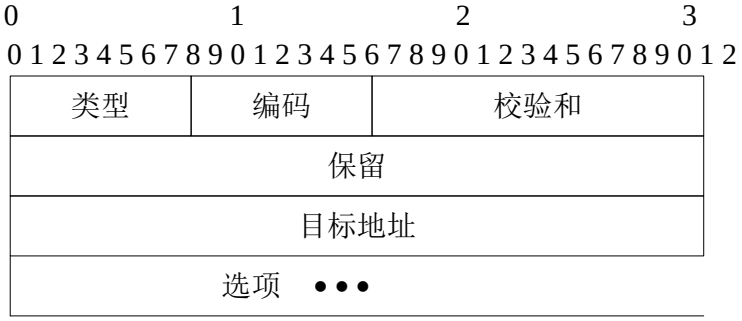

图3 Neighbor Solicitation消息格式

IP字段：

Source Address

或者是分配给发送此消息的接口的地址，或者是(如果Duplicate Address Detection在执行中 [ADDRCONF])未指定地址。

Destination Address

或者是与目标地址相对应的请求-节点多播地址，或者是目标地址。

Hop Limit

255

ICMP字段：

Type

135

Code

0

Checksum

ICMP校验和。参阅[ICMPv6]。

Reserved

此字段不使用。它必须由发送者初始化为0，接收者必须忽略它。

Target Address

请求的目标的IP地址。它必须不是多播地址。

可能的选项：

源链路层地址

发送者的链路层地址。当源IP地址是未指定地址时必须不包括此选项。其他情况，在有地址的链路层上，此选项必须包括在多播请求中和应当包括在单播请求中。

本协议的将来版本或许定义新的选项类型。接收者必须静默忽略任何它们不能识别

的选项，并继续处理消息。

4-4　Neighbor Advertisement消息格式

节点发送Neighbor Advertisements以响应Neighbor Solicitations，发送非请求Neighbor Advertisements以便(非可靠)快速传播新信息。Neighbor Advertisement消息格式如图4所示。

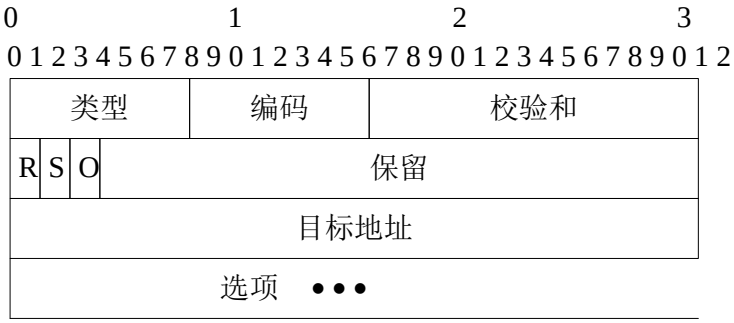

图4　Neighbor Advertisement消息格式

IP字段：

Source Address

分配给发送此通告的接口的地址。

Destination Address

对于请求的通告，是引起Neighbor Solicitation 的Source Address，或者如果此请求的Source Address是未指定地址，是所有节点的多播地址。对于非请求通告，典型为所有节点的多播地址。

Hop Limit

255

ICMP字段：

Type

136

Code

0

Checksum

ICMP校验和，参阅[ICMPv6]。

R

路由器标记。当置1时，R位指出发送者是路由器。R位由Neighbor Unreachability Detection使用，用于检测改变为主机的路由器。

S

请求标记。当置1时，S位指出通告被发送以响应来自目的地地址的Neighbor Solicitation。S位用作Neighbor Unreachability Detection的可达性确认。在多播通告和非请求单播通告中它必须不置1。

O

替代标记。当置1时，O位指出通告应当替代现存的缓存条目并更新缓存的链路层地址。当它没有置1时通告将不更新缓存的链路层地址，尽管通告将更新现存的Neighbor Cache条目，对于该条目没有链路层地址是已知的。在针对任播地址的请求通告中，以及在请求的前缀通告中它不能被置1。在其他请求通告中和在非请求通告中它应当被置1。

Reserved

29位未使用字段。它必须由发送者初始化为0，接收者必须忽略它。

Target Address

对于请求的通告，是在Neighbor Solicitation消息(该消息催促这个通告)中的Target Address字段。对于非请求通告，是其链路层地址已经改变的地址。Target Address必须不是多播地址。

可能的选项：

目标链路层地址

目标的链路层地址，即，通告发送者。当响应多播请求时，在有地址的链路层上必须包括此选项。当响应单播Neighbor Solicitation时应当包括此选项。

当对端节点由于没有缓存条目从而不能返回一个Neighbor Advertisements消息时，为了避免无休止的Neighbor Solicitation“递归”，对于多播请求必须包括此选项。当响应单播请求时，可忽略此选项，因为请求的发送者有正确的链路层地址；其他情况，此选项不能在第一位置发送单播请求。然而，在此情况，包括链路层地址仅增加了少许开销，却消除了潜在的竞争条件，那里在收到对先前的请求的响应之前，发送者删除缓存的链路层地址。

本协议的将来版本或许定义新的选项类型。接收者必须静默忽略任何它们不能识别的选项，并继续处理消息。

4-5　Redirect消息格式

发送Redirect分组的路由器通知主机，在前往目的地的路径上有一个较好的第一跳节点。主机能够被重定向到较好的第一跳路由器，但是也能够用重定向通知目的地事实上是邻居。后者由设置ICMP Target Address等于ICMP Destination Address实现。Redirect消息格式如图5所示。

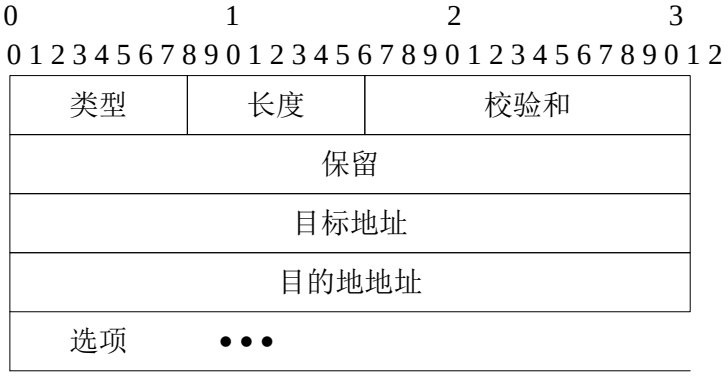

图5　Redirect消息格式

IP字段：

Source Address

必须是分配给发送此消息的接口的链路本地地址。

Destination Address

触发此重定向分组的Source Address。

Hop Limit

255

ICMP字段：

Type

137

Code

0

Checksum

ICMP校验和。参阅[ICMPv6]。

Reserved

此字段未使用。它必须由发送者初始化为0，接收者必须忽略它。

Target Address

一个IP地址，它是针对ICMP Destination Address的较好的第一跳。当目标是实际通信端点时，即，目的地是邻居，Target Address字段必须包括与ICMP Destination Address字段相同的值。其他情况，目标是较好的第一跳路由器并且Target Address必须是该路由器的链路本地地址，以便主机能够唯一地识别路由器。

Destination Address

重定向到目标的目的地的IP地址。

可能的选项：

目标链路层地址

该目标的链路层地址。应当包括它(如果知道)在内。注意，在NBMA链路上，主机们或许根据Redirect消息中Target Link-Layer Address选项的存在，作为确定邻居们的链路层地址的方法。在此情况，此选项必须包括在Redirect消息中。

Redirected Header

不造成重定向分组超过在[IPv6]中规定的最小MTU情况下，尽可能多地触发发送Redirect的IP分组。

4-6　选项格式

Neighbor Discovery消息包括0个或多个选项，它们中的一些或许多次出现在相同的消息中。当需要时选项应当被填充，以确保它们可在(它们的)自然的64位边界结束。所有选项格式如图6所示。

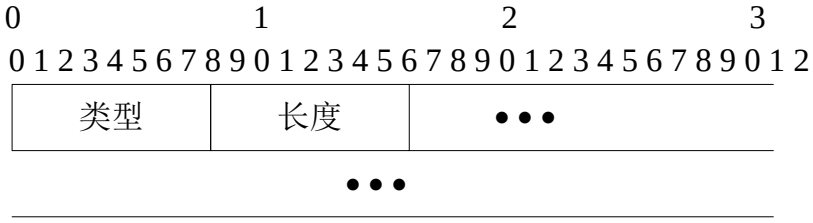

图6　选项格式

字段：

Type

8位选项类型标识符。在本文件中定义的选项是：

Option Name	Type
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3

Redirected Header 4

MTU 5

Length

8位无符号整数。选项的长度(包括类型字段和长度字段)以8字节为单位计算。值0无效。注意，节点必须静默抛弃包含长度值为0的选项的ND分组。

4-6-1 源/目标链路层地址

源/目标链路层地址的格式如图7所示。

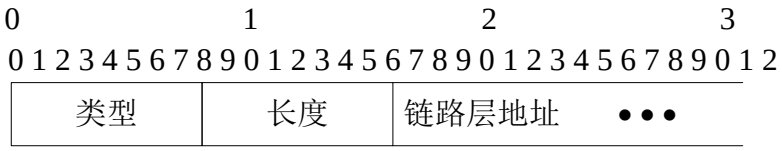

图7 源/目标链路层地址格式

字段：

Type

1为Source Link-layer Address。

2 为Target Link-layer Address。

Length

选项的长度(包括类型字段和长度字段)以8字节为单位计算。例如，IEEE802地址的长度是1[IPv6-ETHER]。

Link-Layer Address

可变长度的链路层地址。

此字段的内容和形式(包括字节和比特顺序)一般由描述IPv6在不同链路层上如何运行的特定文件中规定。例如，[IPv6-ETHER]。

描述

Source Link-Layer Address选项包括分组发送者的链路层地址。它应用在Neighbor Solicitation、Router Solicitation和Router Advertisement分组中。

Target Link-Layer Address选项包含目标的链路层地址。它应用在Neighbor Advertisement和Redirect分组中。

对于其他Neighbor Discovery消息，这些选项必须被静默忽略。

4-6-2 前缀信息

前缀信息格式如图8所示。

图8　前缀信息格式

字段：

Type

3

Length

4

Prefix Length

8位无符号整数。在合法前缀中领先比特的数目。其值范围是0到128。前缀长度字段为on-link确定提供必须的信息(当与前缀信息选项中L标记相结合时)。它也帮助实现地址自动配置，如[ADDRCONF]所述，对此存在更多关于前缀长度的限制。

L

1位on-link标记。当置1时，指出此前缀可用于on-link确定。当没有置1时，通告对此前缀的on-link或off-link性质没有说明。换句话讲，如果L标记没有置1，主机不能推断出从该前缀引申出的地址是off-link。即，主机不能更新先前关于地址是on-link的指示。

A

1位自动地址配置标记。当置1时，指出此前缀可用于无状态地址自动配置，如[ADDRCONF]所述。

Reserved1

6位未使用字段。必须被发送者初始化为0，接收者必须忽略它。

Valid Lifetime

32位无符号整数。时间长度以秒为单位(相对于分组被发送的时间)，在此时间内此前缀对于on-link确定来说是合法的。全1比特值(0xffffffff)表示无限。Valid Lifetime也由[ADDRCONF]使用。

Preferred Lifetime

32位无符号整数。时间长度以秒为单位(相对于分组被发送的时间)。在此时间内经无状态地址自动配置，根据此前缀生成的地址保有优先权[ADDRCONF]。全1比特值(0xffffffff)表示无限。参阅[ADDRCONF]。

注意，此字段的值不能超过Valid Lifetime字段的值，以避免优先的地址不再合法。

Reserved2

此字段未使用。它必须被发送者初始化为0，接收者必须忽略它。

Prefix

IP地址或IP地址的前缀。Prefix Length字段包含此前缀中有效领先比特的数目。在前缀中，在前缀长度之后的这些位被保留，并且必须被发送者初始化为0，接收者必须忽略它们。路由器不应当发送链路本地前缀的前缀选项，主机应当忽略这种前缀选项。

描述

Prefix Information选项为主机提供on-link前缀，和为Address Autoconfiguration提供前缀。Prefix Information选项出现在Router Advertisement分组中，其他消息必须对其静默忽略。

4-6-3 重定向首部

重定向首部格式如图9所示。

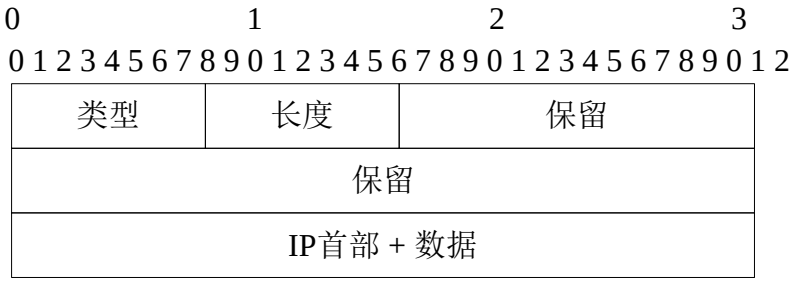

图9 重定向首部格式

字段：

Type

4

Length

此选项的长度，以8字节为单位。

Reserved

这些字段未使用。它们必须被发送者初始化为0，接收者必须忽略它们。

IP首部 + 数据

原始分组被截短，以便确保重定向消息大小不超过IPv6要求的最小MTU，如[IPv6]中所述。

描述

Redirected Header首部在Redirect消息中使用，包括全部或部分被重定向的分组。其他Neighbor Discovery消息必须静默忽略此选项。

4-6-4 MTU

MTU格式如图10所示。

图10 MTU格式

字段：

Type

5

Length

1

Reserved

此字段未使用。它必须被发送者初始化为0，接收者必须忽略它。

MTU

32位无符号整数。是为此链路推荐的MTU。

描述

MTU选项在Router Advertisement消息中使用，以便确保链路上的所有节点使用相同的MTU值，主要用在节点可能不知道链路MTU的情况。

其他Neighbor Discovery消息必须静默忽略此选项。

在将不同介质技术桥接在一起的配置中，最大支持的MTU在各段网络之间可以不同。如果网桥不生成ICMP Packet Too Big消息，通信节点们将不能在每个邻居基础上，使用Path MTU去动态确定适当的MTU。在这些情况，路由器们能够被配置使用MTU选项来规定被所有网段支持的最大MTU值。

第5章　主机概念模型

本章描述可能的数据结构组织概念模型，该模型是主机(在一定程度上包括路由器)在与邻居节点交互时将维护的模型。该模型用于更方便地说明Neighbor Discovery协议应当如何行为。本文件不强制实现中遵循这个模型，只要它们的外在表现与本文件描述的一致即可。

此模型仅关注与Neighbor Discovery直接相关的主机行为。尤其是，它本身不关注诸如源地址选择，或在多归属地主机上选择离境接口等问题。

5-1　概念性数据结构

主机需要维护下述每个接口信息：

Neighbor Cache

一组单个邻居(最近有流量发送到这些邻居)条目。涉及邻居的on-link单播IP地址的条目被加密。这些条目包括这样的信息：邻居的链路层地址、指出邻居是主机还是路由器的标记(即本文件中的IsRouter)、等待完成地址解析的任何排队分组的指示符，等等。Neighbor Cache条目也包括Neighbor Unreachability Detection算法使用的信息，包括可达性状态，未回答探测数目，以及规划的下一次Neighbor Unreachability Detection事件发生时间。

Destination Cache

一组关于最近有流量发送去的目的地的条目。Destination Cache既包括on-link目的地也包括off-link目的地，并且提供间接进入Neighbor Cache的平台；Destination Cache映射了到下一跳邻居的IP地址的目的地IP地址。此缓存用从Redirect消息中学习到的信息更新。实现中可发现，在Destination Cache条目中存储不直接与Neighbor Discovery相关的附加信息是方便的，这些信息诸如Path MTU (PMTU)和由传输协议维护的往返定时器。

Prefix List

定义了一组on-link地址的前缀列表。Prefix List条目根据在Router

Advertisements中收到的信息生成。每个条目有关联的失效计时器值(从此通告中抽取)，用于当前缀变得无效时终止前缀。特殊的“无限”计时器值规定前缀永远保持有效，除非在后续通告中收到一个新的(有限)值。

链路本地前缀被认为是在这样的前缀列表上，该列表具有无限失效计时器，无论是否路由器正在通告针对该列表的前缀。收到的Router Advertisements不应当修改链路本地前缀的失效计时器。

Default Router List

路由器列表，分组将发送到这些路由器。路由器列表条目指向Neighbor Cache中的条目；比起其可达性受到怀疑的路由器，选择默认路由器的算法偏爱已知它们是可达的路由器。每个条目也有一个关联的失效计时器值(从Router Advertisements中取得)，用于检测不再被通告的条目。

注意，上述概念性数据结构可使用各种技术实现。一种针对所有上述数据结构的可能实现是使用单一最长匹配路由表。无论具体怎样实现，关键是路由器的Neighbor Cache条目由所有使用那个路由器的Destination Cache条目共享，从而避免冗余的Neighbor Unreachability Detection探测。

也要注意，其他协议(例如MIPv6)或许添加附加概念性数据结构。实现是自由的，可以以任何喜欢的方法实现这样的数据结构。例如，实现中能够融合所有概念性数据结构成为单一路由表。

Neighbor Cache包含由Neighbor Unreachability Detection算法维护的信息。关键信息是邻居的可达状态，它是5个可能值之一。下述定义是非正式的；精确定义参阅第7-3-2节。

INCOMPLETE(未完成的)

地址解析在进行中，邻居的链路层地址还没有被确定。

REACHABLE(可到达的)

粗略讲，已知邻居最近(几十秒前)是可达的。

STALE(陈旧的)

邻居不再被认为是可达的，但是直到流量发送给该邻居时，不应当尝试改变它的可达性。

DELAY(延时)

邻居不再被认为是可达的，最近流量已经发送到该邻居。然而，不立即探测该邻居的可达性，延时一段时间发送探测消息，以便给上层协议一个机会提供可达性确认。

PROBE(探测)

邻居不再被认为是可达的，并且发送了单播Neighbor Solicitation探测消息以便验证可达性。

5-2 概念性发送算法

当发送分组到目的地时，节点使用Destination Cache、Prefix List和Default Router List的组合，以便确定适当下一跳的IP地址，这里的操作称为“下一跳确定”。一旦获得下一跳的IP地址，则针对那个邻居的链路层信息查询Neighbor Cache。

针对给定单播目的地的下一跳确定操作如下所述。发送者依据Prefix List执行最长前缀匹配以便确定该分组的目的地是on-link还是off-link。如果目的地是on-link，下一跳地址与分组的目的地地址相同。否则，发送者根据Default Router List选择一个路由器(遵循第6-3-6节描述的规则)。

出于效率原因，下一跳确定不按每个被发送的分组执行。取而代之，下一跳确定计算的结果被保存在Destination Cache中(它也包含从Redirect消息中学习到的更新)。当发送节点有

分组发送时，发送节点首先检查Destination Cache。如果没有针对该目的地的条目存在，下一跳确定被激活，生成一个Destination Cache条目。

一旦获得下一跳节点的IP地址，发送者针对那个邻居的链路层信息查阅Neighbor Cache。如果没有条目存在，发送者生成一个条目，设置该条目的状态为INCOMPLETE，初始Address Resolution，接着排队地址解析暂未完成的数据分组。对于多播使能接口，Address Resolution由发送Neighbor Solicitation消息然后等待Neighbor Advertisement消息构成。当收到Neighbor Advertisement响应后，链路层地址被输入到Neighbor Cache条目中，排队的分组被发送出去。此地址解析机制在第7-2节详细描述。

对于多播分组，下一跳总是(多播)目的地地址并且被认为是on-link。IP多播地址已经给定情况下确定链路层地址的过程，可参阅论述在特定链路类型(例如[IPv6-ETHER])上运行IP的文献。

每当发送单播分组时访问一次Neighbor Cache条目，发送者按照Neighbor Unreachability Detection算法(参阅第7-3节)检验Neighbor Unreachability Detection的相关信息。此不可达检验或许导致发送者发送单播Neighbor Solicitation去验证该邻居仍然是可到的。

流量首次发送到目的地时，进行下一跳确定。只要到那个目的地的后续通信成功进行，Destination Cache条目继续被使用。如果通过Neighbor Unreachability Detection算法确定，通信在某点停止，下一跳确定或许需要重新执行。例如，通过出故障路由器的流量应当被交换到正常工作的路由器。同理，很可能重新路由目的地为移动节点的流量到“移动性代理”。注意，当节点重做下一跳确定时，不需要抛弃完整的Destination Cache条目。事实上，保留像PMTU和环回计时器值这样的缓存信息通常是有益的，PMTU和环回计时器值或许也被保存在Destination Cache条目中。

路由器和多归属地主机有多个接口。本文件余下部分假定所有发送的和接收的Neighbor Discovery消息涉及上下文相关的接口。例如，当响应Router Solicitation时，相应的Router Advertisement是在接收上述请求的接口上发送出的。

5-3　垃圾收集和超时要求

上述概念性数据结构使用不同机制抛弃潜在的陈旧或无用信息。

从正确性的角度，无需周期清除Destination Cache条目和Neighbor Cache条目。虽然陈旧信息能够无限期地潜在保存在缓存中，Neighbor Unreachability Detection算法确保陈旧信息被迅速清除，如果实际上在使用该算法的话。

为了限制对Destination Cache条目和Neighbor Cache条目的存储需求，节点或许需要收集陈旧的条目。然而，必须小心，以便确保总有充足的空间保存正在使用的活跃条目。如果条目被抛弃接着被快速重新建立，小容量的缓存或许导致过量的Neighbor Discovery消息。收集不使用的条目，可以采取仅收回在一段时间内(例如，10分钟或更长)已经不使用的条目的最近最少使用(Least Recently Used, LRU)策略。

节点应当在Default Router List和Prefix List中保留条目，直到它们的生存期到期。然而，如果节点的存储器不够用，节点可以收集未到期的条目。如果不是所有路由器都列在Default Router list上，节点应当在Default Router List中至少保留两个条目(多于两个更可取)，以便维持off-link目的地的茁壮连接。

当从Prefix List中删除条目时，不需要从Destination Cache或Neighbor Cache中清除任何条目。Neighbor Unreachability Detection将在这些缓存中高效清除任何已经变为失效的条目。然而，当从Default Router List中删除条目时，在Destination Cache中搜索那个路由器的任何条目必须再次执行下一跳确定，以便选择一个新的默认路由器。

第6章　路由器和前缀发现

本章描述与Neighbor Discovery的Router Discovery部分有关的路由器行为和主机行为。Router Discovery用于找出临近路由器，以及学习前缀和与无状态地址自动配置有关的配置参数。Prefix Discovery是一个过程，通过此过程主机了解了驻留在on-link的IP地址范围，并且可不经路由器直接到达。路由器发送Router Advertisements指出是否该发送者愿意作默认路由器。Router Advertisements也包括Prefix Information选项，该选项列出标识on-link IP地址的前缀集合。

Stateless Address Autoconfiguration也必须获得作为配置地址一部分的子网前缀。虽然用于地址自动配置的前缀在逻辑上不同于用于on-link确定的前缀，自动配置信息是在Router Discovery消息中捎带的，以便减少网络流量。的确，通过在Prefix Information选项中规定适当标记，相同前缀能够用于通告on-link确定，也能用于通告地址自动配置。关于如何处理自动配置信息的详细内容参阅[ADDRCONF]。

6-1　消息合法性检测

6-1-1　Router Solicitation消息的合法性检测

主机必须静默抛弃任何收到Router Solicitation消息。

路由器必须静默抛弃任何收到的，不能满足所有下述合法性检验的Router Solicitation消息：

- IP Hop Limit 字段值为 255，即，分组可能不能由路由器转发。
- ICMP 校验和合法。
- ICMP 编码是 0。
- ICMP 长度(从 IP 长度引出)是 8 字节或更多字节。
- 所有包括的选项的长度大于0。
- 如果IP源地址是未指定地址，在消息中不存在源链路层地址。

Reserved字段的内容，以及任何不能识别的选项的内容，必须忽略。将来，协议的后向兼容改变可能规定Reserved字段的内容，也可能添加新的选项；后向不兼容改变或许使用不同Code值。

任何已定义的、没有规定由Router Solicitation消息使用的选项的内容必须忽略，分组处理照常进行。唯一经过定义的、可能出现的选项是Source Link-Layer Address选项。

通过合法性检验的请求称为“合法请求”。

6-1-2　Router Advertisement消息的合法性检测

节点必须静默抛弃任何收到的、不能满足所有下述合法性检验的Router Advertisement：

- IP Source Address是链路本地地址。路由器必须使用它们的链路本地地址作为Router Advertisement消息和Redirect消息的源，以便主机能够唯一地识别路由器。
- IP Hop Limit字段的值为255，即，分组可能不能由路由器转发。
- ICMP校验和是合法的。
- ICMP Code是0。
- ICMP 长度(从 IP 长度引出)是 16 字节或更多字节。
- 所有包括的选项的长度大于0。

Reserved字段的内容，以及任何不能识别的选项的内容，必须忽略。将来，协议的后向兼容改变可能规定Reserved字段的内容，也可能添加新的选项；后向不兼容改变或许使用不同Code值。

任何已定义的、没有规定由Router Advertisement消息使用的选项的内容必须忽略，分组处理照常进行。仅有的经过定义的选项是Source Link-Layer Address选项、Prefix Information

选项和MTU选项。

通过合法性检验的通告称为“合法通告”。

6-2 路由器规范

6-2-1 路由器配置变量

路由器必须允许通过系统管理配置下述概念性变量。特定的变量名称仅用于演示目的，实现中不要求使用它们，只要外在行为与本文件描述的一致即可。规定了默认值以便简化常规配置。

下面列出的某些变量的默认值可以由特定文件替代，这些特定文件描述IPv6如何在不同链路层上运行。本规则简化了Neighbor Discovery在具有很大性能差异的不同链路类型上的配置。

对于每个接口：

IsRouter

一个标记，指出是否在此接口上使能了路由功能。在接口上使能路由暗示路由器能够转发分组到此接口，或接收从此接口来的分组。

默认值：FALSE

AdvSendAdvertisements

一个标记，指出在任何情况下路由器都定期发送Router Advertisements，以及响应Router Solicitations。

默认值：FALSE

注意，AdvSendAdvertisements的默认值必须是FALSE，以便节点不能偶然充当路由器，除非它被系统管理显式配置，能够发送Router Advertisements。

MaxRtrAdvInterval

接口连续发送非请求多播Router Advertisements，相邻两个Advertisements间允许的最大时间间隔，以秒为单位。必须不短于4秒，不长于1800秒。

默认值：600秒

MinRtrAdvInterval

接口连续发送非请求多播Router Advertisements，相邻两个Advertisements间允许的最小时间间隔，以秒为单位。必须不短于3秒，不长于0.75× MaxRtrAdvInterval秒。

默认值：0.33× MaxRtrAdvInterval秒，如果 MaxRtrAdvInterval >= 9秒；否则，默认值是MaxRtrAdvInterval。

AdvManagedFlag

放置在Router Advertisement中“Managed address configuration”标记字段内的TRUE/FALSE值。参阅[ADDRCONF]。

默认值：FALSE

AdvOtherConfigFlag

放置在Router Advertisement中“Other configuration”标记字段内的TRUE/FALSE值。参阅[ADDRCONF]。

默认值：FALSE

AdvLinkMTU

放置在路由器发送的MTU选项中的值。值为0指出没有发送MTU选项。

默认值：0

AdvReachableTime

放置在路由器发送的Router Advertisement消息中Reachable Time字段内的值。值为0表示未(由此路由器)指定。必须不大于3,600,000毫秒(1小时)。

默认值：0

AdvRetransTimer

放置在路由器发送的Router Advertisement消息中Retrans Timer字段内的值。值为0表示未(由此路由器)指定。

默认值：0

AdvCurHopLimit

放置在路由器发送的Router Advertisement消息中Cur Hop Limit字段内的默认值。应当设置此值为互联网目前范围。值为0表示未(由此路由器)指定。

默认值：由“Assigned Numbers”[ASSIGNED]中规定，在实现时有效。

AdvDefaultLifetime

放置在该接口发送的Router Advertisements的Router Lifetime字段内的值。必须或者是0，或者是MaxRtrAdvInterval和9000秒之间。值为0指出该路由器不是默认路由器。这些限制可以由描述IPv6如何在不同链路层上运行的特定文件替代。例如，在点对点链路中，对端可以有另一端设备的数目和状态的充足信息，所以仅需发送较少次数的通告。

默认值：3× MaxRtrAdvInterval

AdvPrefixList

放置在该接口发送的Router Advertisement消息中Prefix Information选项内的前缀列表。

默认值：路由器使用路由协议通告的所有前缀，对于发送通告的接口而言，这些前缀是on-link。在通告的前缀列表中不能包括链路本地前缀。

每个前缀有一个关联的：

AdvValidLifetime

放置在Prefix Information选项中Valid Lifetime内的值，以秒为单位。全1值(0xffffffff)表示无限。实现中也可以用两种方法规定AdvValidLifetime：

- 按真实时间衰减的时间，即，取值 1 将导致在规定的将来时刻有值为 0 的 Lifetime，或者
- 固定时间，在连续的通告中保持不变。

默认值：259200 秒(30 天)，固定(即，在连续的通告中保持不变)。

AdvOnLinkFlag

放置在Prefix Information选项中on-link标记(L位)字段内的值。

默认值：TRUE

无状态地址自动配置[ADDRCONF]定义了与每个前缀关联的附加信息：

AdvPreferredLifetime

放置在Prefix Information选项中Preferred Lifetime内的值，以秒为单位。全1值(0xffffffff)表示无限。关于此值如何使用参阅[ADDRCONF]。实现中也可以允许用两种方法规定AdvPreferredLifetime：

- 实时衰减的时间，即，取值 1 将导致在规定的将来时刻有一个值为 0 的 Lifetime，或者
- 固定时间，在连续的通告中保持不变。

默认值：604800秒(7天)，固定(即，在连续的通告中保持不变)。此值

必须不大于AdvValidLifetime。

AdvAutonomousFlag

放置在Prefix Information选项中Autonomous Flag字段内的值。参阅[ADDRCONF]。

默认值：TRUE

上述变量包含了放置在发出Router Advertisement消息中的信息。主机使用收到的信息初始化一系列类似的变量，这些变量控制它们的外在行为(参阅第6-3-2节)。这些主机变量中的一些(例如，CurHopLimit、RetransTimer和ReachableTime)适用于所有节点，包括路由器。实践中，这些变量实际上可以不出现在路由器上，因为它们的内容能够从上面描述的变量中引申出来。然而，外在的路由器行为必须与基于这些变量的主机的行为相同。尤其是，这包括ReachableTime值的偶然随机化，如第6-3-2节所述。

协议常数在第10章定义。

6-2-2 成为通告接口

术语“通告接口(advertising interface)”指这样的任何使能接口，它有至少一个分配给它的单播IP地址，它的对应AdvSendAdvertisements标记为TRUE。路由器必须不在任何不是通告接口的接口上发送Router Advertisements。

接口可以方便地变成通告接口，而不一定在系统启动时。例如：

- 在使能接口上改变AdvSendAdvertisements标记，从FALSE变为TRUE，或者
- 如果它已经被管理上关闭，通过管理使能该接口，并且它的AdvSendAdvertisements标记改变为TRUE，或者，
- 使能IP转发能力(即，将系统从是一个主机变为是一个路由器)，当接口的AdvSendAdvertisements标记是TRUE时。

路由器必须在通告接口上添加all-routers多播地址。路由器们响应发送到all-routers地址的Router Solicitations，并检验由邻居路由器发送的Router Advertisements的一致性。

6-2-3 Router Advertisement消息内容

在路由器的通告接口上，除了发送请求的Router Advertisements外，路由器也周期发送。发出的Router Advertisements具有下述与第4-2节给出的消息格式相一致的值：

- 在Router Lifetime字段中：接口配置为AdvDefaultLifetime。
- 在M和O标记中：接口分别配置为AdvManagedFlag和AdvOtherConfigFlag。
- 在Cur Hop Limit字段中：接口配置为CurHopLimit。
- 在Reachable Time字段中：接口配置为AdvReachableTime。
- 在Retrans Timer字段中：接口配置为AdvRetransTimer。
- 在选项中：
  - Source Link-Layer Address选项：发送接口的链路层地址。可以忽略此选项，以便促进在重复接口上的入境负载均衡。
  - MTU选项：接口配置为AdvLinkMTU值，如果此值为非0。如果AdvLinkMTU是0，MTU选项不发送。
  - Prefix Information选项：每个前缀有一个Prefix Information选项，这些前缀在AdvPrefixList中列出，采用根据AdvPrefixList条目中的信息设置选项字段，如下所示：
    - 在“on-link”标记中：条目是AdvOnLinkFlag。
    - 在Valid Lifetime字段中：条目是AdvValidLifetime。
    - 在“Autonomous address configuration”标记中：条目是AdvAutonomousFlag。

** 在Preferred Lifetime字段中：条目是AdvPreferredLifetime。

路由器或许希望发送不通告它自己是默认路由器的Router Advertisements。例如，路由器或许为无状态地址自动配置通告前缀，同时不希望转发分组。这个路由器在发出的通告中设置Router Lifetime字段为0。

路由器在发送非请求Router Advertisements 时可以选择不包括某些或全部选项。例如，如果前缀生存期比AdvDefaultLifetime长很多，每隔几个通告包括这些前缀生存期也就足够了。然而，当响应Router Solicitation或发送前几个初始非请求通告时，路由器应当包括所有选项，以便在系统初始化期间能够快速传播所有信息(例如，前缀)。

如果包括所有选项会使通告大小超过链路MTU，可以发送多个通告，每个通告包括这些选项的一个子集。

6-2-4 发送Unsolicited Router Advertisements

主机在任何时刻必须不发送Router Advertisement消息。

Unsolicited Router Advertisements不严格周期发送：相继发送间的间隔是随机的，以便减少与来自同一链路上其他路由器的通告发生同步的概率[SYNC]。每个通告接口有它自己的计时器。每当多播通告从接口发送出去时，计时器总是被重新设置为一个均匀分布的随机值，该值取值范围在该接口已经配置的MinRtrAdvInterval和MaxRtrAdvInterval之间；计时器到期引起下一个通告发送，并且选择新的随机值。

接口变成通告接口后，对于前几个通告(最多MAX_INITIAL_RTR _ADVERTISEMENTS)，如果随机选择的间隔大于MAX_INITIAL_RTR_ADVERT _INTERVAL，计时器应当被设置为MAX_INITIAL_RTR_ADVERT_INTERVAL。如果有分组丢失可能，初始通告使用较小的间隔，可增加路由器首次变得可用时被迅速发现的可能性。

包含在Router Advertisements中的信息可以通过系统管理操作改变。例如，改变通告的前缀的生存期，添加新的前缀，使路由器停止是一个路由器(即，从是一个路由器转变为是一个主机)，等等。在这些情况，路由器可以发送最多MAX_INITIAL_RTR_ ADVERTISEMENTS次非请求通告，遵循的规则和接口变成通告接口时遵循的规则相同。

6-2-5 停止是一个通告接口

通过下述系统管理操作，可停止接口的通告接口身份：

- 改变使能接口的AdvSendAdvertisements标记，从TRUE变为FALSE，或者
- 从管理上关闭该接口，或
- 关闭系统。

在这些处理中，路由器应当在具有Router Lifetime字段值为0的接口上发送一个或多个(但不超过MAX_FINAL_RTR_ADVERTISEMENTS个)最终的多播Router Advertisements。在路由器变成主机情况，系统也应当使该路由器上所有支持IP多播的接口，脱离all-routers IP多播组(无论它们是否已经是通告接口)。此外，“主机”必须确保后续从该接口发送的Neighbor Advertisement消息将Router标记设置为0。

注意，系统管理可以关闭路由器的IP转发能力(即，改变系统，从是一个路由器改变到是一个主机)，这不一定暗示此路由器的接口已停止是通告接口。在这些情况，后续Router Advertisements必须设置Router Lifetime字段为0。

6-2-6 处理Router Solicitations

主机必须静默抛弃任何收到的Router Solicitation消息。

除了发送周期的、非请求的通告外，路由器还发送响应合法请求(在通告接口上收到的)

的通告。路由器可以选择直接单播响应到发出请求的主机的地址(如果该请求的源地址不是非请求地址)，但是通常情况是多播此响应到all-nodes组。在后者，接口的间隔计时器被重新设置为新的随机值，好像非请求通告刚刚被发送(参阅第6-2-4节)。

所有情况中，为响应Router Solicitation 而发送的Router Advertisements必须延时一个随机时间，其时间值范围在0到MAX_RA_DELAY_TIME秒之间。(如果发送单一通告响应多个请求，延时相对于第一个请求。)此外，连续发送Router Advertisements到all-nodes多播地址的速率，必须限定在每MIN_DELAY_BETWEEN_RAS秒不得多于一个通告。

路由器可以按如下处理Router Solicitations：

- 一旦收到Router Solicitation，计算范围在0到AX_RA_DELAY_TIME内的随机延时。如果计算出的值对应的时间迟于规定的下一个多播Router Advertisement发送时间，忽略此随机延时，按先前规定的时间发送此通告。
- 如果在最后MIN_DELAY_BETWEEN_RAS秒内，路由器发送了多播Router Advertisement (请求的或非请求的)，规定通告在这样的时间发送，该时间对应MIN_DELAY_BETWEEN_RAS加上发送前一个通告后的随机值。这确保多播Router Advertisements的发送速率是受限的。
- 否则，规定以随机值给定的时间发送Router Advertisement。

注意，准予路由器比由MinRtrAdvInterval配置变量指出的更频繁地发送多播Router Advertisements，只要更频繁地通告是响应Router Solicitations。然而，在所有情况，必须不能比MinRtrAdvInterval指出的更频繁地发送非请求多播通告。

如果Router Solicitations中Source Address是未指定地址，那么Router Solicitations必须不更新该路由器的Neighbor Cache；带有适当源地址的请求按如下所述更新Neighbor Cache。如果路由器已经有该请求发送者的Neighbor Cache条目，该请求包含Source Link-Layer Address选项，并且接收的链路层地址不同于已经在该缓存中的地址，那么该链路层地址应当用适当的Neighbor Cache条目更新，并且它的可达性状态也必须设置为STALE。如果不存在现存的该请求的发送者的Neighbor Cache条目，路由器生成一个，安装该链路层地址，并设置它的可达性状态为STALE，如第7-3-3节所述。如果不存在现存的Neighbor Cache条目，并且没有Source Link-Layer Address选项出现在该请求中，路由器可以用或者一个多播，或者一个单播路由器通告进行响应。在任何情况下Source Link-Layer Address选项是提供的，如果该请求的发送者的Neighbor Cache条目存在(或者被生成)，该条目的IsRouter标记必须被设置为FALSE。

6-2-7 Router Advertisement一致性

路由器应当检查由其他路由器发送的合法Router Advertisements，验证路由器们正在链路上通告一致的信息。检测到的不一致性指出一个或多个路由器或许被错误配置，应当由系统或网络管理记录在案。需检验信息的最小集包括：

- Cur Hop Limit值(除了未规定的0值，其他的不一致性应当由系统或网络管理记录在案)。
- M标记或O标记的值。
- Reachable Time值(除了未规定的0值)。
- Retrans Timer值(除了未规定的0值)。
- MTU选项内的值。
- 同一前缀的Preferred Lifetime和Valid Lifetime。如果AdvPreferredLifetime和/或AdvValidLifetime实时递减，如第6-2-1节所述，那么生存期们的比较不能比较Router Advertisement中多个字段的内容，而必须是前缀分别变得过时和不合法的时刻的比较。由于链路传播延时和路由器间潜在的拙劣同步时钟，这样的比较应当允许稍微时间不齐。

注意，通告不同前缀设置对于不同路由器来讲不是一个错误。同样，一些路由器或许留下一些字段未指定，即，字段值为0，而其他路由器规定了值。出错日志应当限制冲突信息，这些冲突信息引起主机们根据收到的每一个通告，一次接一次地交换收到的值。

任何由路由器执行的接收Router Advertisement消息的其他操作超出本文件范围。

6-2-8 链路本地地址改变

路由器上的链路本地地址几乎不应当改变，如果有的话。收到Neighbor Discovery消息的节点使用源地址标识发送者。如果来自同一路由器的多播分组包括不同源地址，节点将假定它们来自不同路由器，导致不希望的行为。例如，节点将忽略被认为由不是目前第一跳路由器的路由器发送的Redirect消息。于是，由特定路由器发送的Router Advertisements中使用的源地址必须等同于当重定向到那个路由器时，Redirect消息中的目标地址。

使用链路本地地址唯一标识链路上的路由器的优点是，标识路由器的地址，当站点重新编码时不会改变。

如果路由器改变了它的接口之一的链路本地地址，它应当将这个改变通知主机们。路由器应当以旧的链路本地地址，多播几个Router Lifetime字段取值为0的Router Advertisements，也应当以新的链路本地地址多播几个Router Advertisements。这样做的综合影响与接口停止充当通告接口，另一个接口开始成为通告接口类似。

6-3 主机规范

6-3-1 主机概念性变量

无。

6-3-2 主机变量

除了第5-1节定义的数据结构以外，主机维护某些与Neighbor-Discovery相关的变量。具体使用的变量名称仅用于演示目的，不要求实现中选用它们，只要它的外在行为与本文件描述的一致即可。

这些变量有默认值，这些默认值被在Router Advertisement消息中收到的信息替代。当链路上没有路由器，或当所有收到的Router Advertisements剩下一个特定的未指定值时，使用默认值。

本规范中的默认值可以被描述IP如何在不同链路层上运行的具体文件替代。此项规则允许Neighbor Discovery在有很宽性能特征变化的链路上运行。

对于每个接口：

LinkMTU

该链路的MTU。

默认值：在描述IPv6如何在特定链路层上运行的具体文件(例如[IPv6-ETHER])中定义。

CurHopLimit

发送IP分组时使用的默认跳数限制。

默认值：在[ASSIGNED]的“Assigned Numbers”中规定的值，该值在实现中有效。

BaseReachableTime

计算随机ReachableTime值时使用的基础值。

默认值：REACHABLE_TIME毫秒。

ReachableTime

收到可达性确认后认为该邻居是可通达的时间。

此值应当是均匀分布随机值，取值范围在MIN_RANDOM_FACTOR到MAX_RANDOM_FACTOR乘以BaseReachableTime毫秒之间。当BaseReachableTime改变(由于Router Advertisements)或至少每两、三个小时即使没有收到Router Advertisements，应当计算新的随机值。

RetransTimer

当解析地址或当探测邻居的可达性时，重复向邻居发送Neighbor Solicitation消息的间隔时间。

默认值：RETRANS_TIMER毫秒。

6-3-3 接口初始化

主机在所有多播使能接口上加入all-nodes多播地址。

6-3-4 处理接收的Router Advertisements

当有多个路由器时，由所有路由器收集的已通告信息或许是单Router Advertisement中包含的信息的超集。此外，也可以通过其它动态方法(例如DHCPv6)获得信息。主机接收所有收到信息的并集；收到Router Advertisement不应使在前一个通告中收到的或来自另一个源的所有信息失效。然而，当收到特定参数信息(例如，链路MTU)或选项(例如，在特定前缀上的Lifetime)，这些参数信息不同于较早收到的信息，并且该参数/选项只能有一个值时，认为最近收到的信息更具权威性。

Router Advertisement字段(例如，Cur Hop Limit、Reachable Time和Retrans Timer)可以包含一个值，该值表示该字段为未指定。在此情况，参数应当被忽略，主机应当继续使用无论什么它正在使用的值。尤其是，主机必须不能把未指定值理解为是改回到第一次收到Router Advertisement前使用的默认值。此规则阻止当一个路由器通告变量的特定值，但是其他路由器通告该变量的未指定值时，主机不停地改变内部变量。

一旦收到合法的Router Advertisement，主机抽取分组的源地址，并进行如下操作：

- 如果地址在主机的 Default Router List 中不存在，并且通告的 Router Lifetime 为非 0，在该列表中生成新的条目，并根据该通告的 Router Lifetime 字段初始化它的未生效计时器值。
- 如果地址已经存在于主机的 Default Router List 中，而且是作为上次收到通告的结果，重新设置它的未生效计时器的值为在最近收到的通告中的 Router Lifetime 的值。
- 如果在主机的 Default Router List 中地址已经存在，并且接收的 Router Lifetime 值为 0，按第 6-3-5 节所述立即关断该条目。

为了限制 Default Router List 需要存储的信息量，主机可以选择不存储经通告发现的所有路由器地址。然而，主机必须保留至少两个路由器地址，并且应当保留更多。无论何时到目的地的通信出现故障，进行默认路由器选择。于是，该列表上路由器越多，越有可能快速发现替代工作路由器(例如，不必等到下一个通告到来)。

如果收到的 Cur Hop Limit 值是非 0，主机应当设置它自己的 CurHopLimit 变量为此接收的值。

如果收到的 Reachable Time 值为非 0，主机应当设置它自己的 BaseReachableTime 变量为此接收的值。如果新值不同于先前的值，主机应当重新计算新的随机 ReachableTime 值。ReachableTime 是作为范围从 MIN_RANDOM_FACTOR 到 MAX_RANDOM_FACTOR 乘以 BaseReachableTime 的均匀分布随机值而计算得到的。使用随机量降低了各 Neighbor Unreachability Detection 消息相互同步发送的可能性。

在大多数情况，已通告的 Reachable Time 值在相继发送的 Router Advertisements 中是相

同的，并且主机的 BaseReachableTime 很少改变。在这些情况，实现应当确保至少每二、三小时重新计算一次新的随机值。

如果收到的值是非 0，RetransTimer 变量的值应当从 Retrans Timer 字段拷贝来。

从 Router Advertisement 消息的固定部分抽取信息后，通告被扫描以考察选项的合法性。如果通告包含 Source Link-Layer Address 选项，链路层地址应当被记录在针对该路由器的 Neighbor Cache 条目中(如果需要生成一个条目)，并且 Neighbor Cache 条目中 IsRouter 标记必须被设置为 TRUE。如果不包括 Source Link-Layer Address，但是对应的 Neighbor Cache 条目存在，它的 IsRouter 标记必须被设置为 TRUE。IsRouter 标记由 Neighbor Unreachability Detection 使用，用于确定路由器何时改变为主机(即，不再能够转发分组)。如果生成了路由器的 Neighbor Cache，它的可达性状态必须被设置为 STALE，如第 7-3-3 节所述。如果缓存条目已经存在并被用于不同链路层地址更新，可达性状态也必须设置为 STALE。如果 MTU 选项存在，主机应当拷贝该选项的值到 LinkMTU，只要该值大于或等于最小链路 MTU[IPv6]，并且不超过在特定链路类型文件(例如，[IPv6-ETHER])中规定的最大 LinkMTU 值。

有“on-link”(L)标记置 1 的 Prefix Information 选项指出标识地址范围的前缀，这些地址应当被认为是 on-link。然而，注意，带有 on-link 标记置 0 的 Prefix Information 选项不传送有关 on-link 确定的信息，并且必须不能认为这表示由该前缀覆盖的地址是 off-link。消除先前 on-link 指示的唯一方法是用 L 比特置 1 和 Lifetime 置 0 通告那个前缀。当发送分组到一个地址，对于该地址的 on-link 状态没有已知信息时，默认行为(参阅第 5-2 节)是转发该分组到默认路由器；接收带有“on-link”(L)标记置 0 的 Prefix Information 选项不改变此行为。地址被看作是 on-link 的原因在第 2-1 节“on-link”定义中作了说明。带有 on-link 标记置 0 的前缀通常有自主标记设置，并由[ADDRCONF]使用。

对于每个带有 on-link 标记置 1 的 Prefix Information 选项，主机进行如下操作：

- 如果前缀是链路本地前缀，静默忽略 Prefix Information 选项。
- 如果前缀还没有出现在 Prefix List 中，并且 Prefix Information 选项的 Valid Lifetime 字段为非 0，生成该前缀的新条目并初始化该前缀的未生效计时器的值为 Prefix Information 选项中的 Valid Lifetime。
- 如果前缀已经出现在主机的 Prefix List 中，作为先前接收的通告的结果。重新设置该前缀的未生效计时器的值为 Prefix Information 选项中的 Valid Lifetime。如果新的 Lifetime 值为 0，立即终止该前缀(参阅第 6-3-5 节)。
- 如果 Prefix Information 选项的 Valid Lifetime 字段是 0，并且前缀没有出现在主机的 Prefix List 中，静默忽略该选项。

无状态地址自动配置[ADDRCONF]，在某些环境中，可以使用较大的前缀 Valid Lifetime，或者完全忽略它以便阻止特定的拒绝服务攻击。然而，因为目标在 on-link 前缀列表的上述拒绝服务的影响不是灾难性的(主机能够发送分组到默认路由器和接收重定向，而不是直接发送分组到邻居)，Neighbor Discovery 协议没有强制对前缀生存期值进行这样的检验。类似，出于地址配置考虑，[ADDRCONF]或许对前缀长度强制实行某些限制。因此，前缀或许被主机中[ADDRCONF]的实现拒绝。然而，当把其他标记一起组合到前缀选项中时，对于 on-link 确定，前缀长度仍然合法。

注意：实现中可以选择分开处理前缀的 on-link 方面和前缀的无状态地址自动配置方面，例如将每个合法 Router Advertisement 消息的副本既传递到“on-link”功能，又传递到“addrconf""功能。接着每个功能能够在设置了适当标记的前缀上独立操作。

6-3-5 终止前缀和默认路由器

无论何时 Prefix List 条目的未生效计时器到期，抛弃该条目。然而，现存的 Destination

Cache 条目不需要更新。如果可达性问题与现存 Neighbor Cache 条目一起出现，Neighbor Unreachability Detection 将执行任何需要的复原。

无论何时在 Default Router List 中条目的 Lifetime 到期，抛弃该条目。当从 Default Router list 中删除一个路由器时，节点必须用这样的方法升级 Destination Cache，即对使用该路由器的所有条目再一次执行下一跳确定，而不是继续发送流量到该(删除的)路由器。

6-3-6 默认路由器选择

选择路由器的算法部分取决于无论怎样路由器已知是可达的。关于节点如何保持对邻居可达性状态跟踪的详细描述参阅第 7-3 节。在下一跳确定期间当针对 off-link 目的地的 Destination Cache 条目不存在时，引发选择默认路由器的算法；或者当经由现存路由器的通信出失败时，引发选择默认路由器的算法。在正常条件下，首次发送流量到目的地时触发路由器选择，后续到该目的地的流量使用相同的路由器，正如在 Destination Cache 模任何 Destination Cache 的改变(该改变由 Redirect 消息引起)指出的。

从 Default Router List 中选择路由器的策略如下：

1）是可达的或可能是可达的(即，除了 INCOMPLETE 状态外的任何状态)路由器应当优先于其可达性是未知的或存疑的路由器(即，处于 INCOMPLETE 状态，或没有该路由器的 Neighbor Cache 条目存在)。当有多个同等条件路由器存在时，默认路由器选择的进一步实现在[LD-SHRE]中讨论。

2）当该表上没有已知路由器是可达的或可能可达的时，应当用一种循环方式选择路由器，所以对默认路由器的其次要求不再返回到同一路由器，直到所有其他路由器已经被选过。此选择方法中，循环通过路由器列表确保了所有可用路由器被 Neighbor Unreachability Detection 算法主动探测到。对默认路由器的要求是和发送分组到该路由器连在一起的，通过此，将探测被选择路由器的可达性。

6-3-7 发送 Router Solicitations

接口使能后，主机或许不愿意等待下一个非请求 Router Advertisement，以便找出默认路由器或学习到前缀。为了较快获得 Router Advertisements，主机会发送直到 MAX_RTR_SOLICITATIONS 次 Router Solicitation 消息，每次发送至少相隔 RTR_SOLICITATION_ INTERVAL 秒。Router Solicitations 可以在下述任何事件之后发送：

- 接口在系统启动时被初始化。
- 在接口暂时失败之后或暂时被系统管理关闭之后接口被重新初始化。
- 通过系统管理将系统的 IP 转发能力改变，使系统从是一个路由器变为是一个主机。
- 主机首次附着到链路。
- 主机脱离网络一些时间后，再次附着到链路。

主机发送 Router Solicitations 到 all-routers 多播地址。IP 源地址被设置为或者是接口的单播地址之一，或者是未指定地址。如果 IP 源地址不是未指定地址，Source Link-Layer Address 选项应当被设置为该主机的链路层地址。

主机发送初始请求前，它应当延时一个随机时间量发送，该量取值范围是 0 到 MAX_RTR_SOLICITATION_DELAY。这用于减轻链路上很多主机在同一时刻启动导致的拥塞，这种情况可能在电源故障恢复后发生。如果因接口被(再次)打开(例如，作为 Duplicate Address Detection 的一部分[ADDRCONF])，主机已经执行了一个随机延时，发送第一个 Router Solicitation 消息前不需要再次延时。

在某些情况，如果需要，随机延时可以忽略。例如，使用[MIPv6]的移动节点，移动到新的链路，需要尽可能快地发现这样的移动，以便最小化由于它的拓扑位置改变导致的分组

丢失数量。在 MIPv6 中 Router Solicitations 为移动检测提供了有用的工具，因为 Router Solicitations 允许移动节点决定移动到新链路。因此，如果移动节点收到指示移动可能已经发生的链路层信息，它可以立即发送 Router Solicitation，没有随机延时。上述指示的强度应当依据链路层暗示的必然性水平，由该移动节点的实现评估，然而这超出本标准的范围。注意，不适当使用此机制(例如，基于弱的或瞬时的指示)或许导致 Router Solicitation 风暴。此外，使用此机制的大量移动节点同时移动能够导致大量请求同时发送。

一旦主机发送了 Router Solicitation，并收到带有非 0 Router Lifetime 的合法 Router Advertisement，主机必须停止在那个接口发送附加的请求，直到下一次上述事件之一发生。然而，在发送请求之前已收到通告的情况，主机应当发送至少一个请求。对请求的通告的响应可以包含比非请求的通告更多的信息。

如果主机发送了 MAX_RTR_SOLICITATIONS 次请求，在发送最后一个请求之后已经等待了 MAX_RTR_SOLICITATION_DELAY 秒，没有收到 Router Advertisements，主机推断在链路上没有基于[ADDRCONF]用途的路由器。然而，主机继续接收并处理 Router Advertisements 消息直到最终路由器出现在链路上。

第 7 章　地址解析和 Neighbor Unreachability Detection

本章描述与 Neighbor Solicitation 消息和 Neighbor Advertisement 消息有关的功能，包括对地址解析和 Neighbor Unreachability Detection 算法的讨论。

Neighbor Solicitation 消息和 Neighbor Advertisement 消息也用于 Duplicate Address Detection，如[ADDRCONF]所述。尤其是，Duplicate Address Detection 发送 Neighbor Solicitation 消息，该消息带有目标为它自己的“临时”地址的未指定源地址。这样的消息触发已经使用了该地址的节点，用指出该地址正在使用的多播 Neighbor Advertisement 作为响应。

7-1　消息合法性检测

7-1-1　Neighbor Solicitations 的合法性检测

节点如果收到不满足下述所有合法性检验的 Neighbor Solicitation 消息，必须将其静默抛弃：

- IP Hop Limit 字段值为 255，即，分组可能不能被路由器转发。
- ICMP 校验和合法。
- ICMP Code 为 0。
- ICMP 长度(由 IP 长度引申出)是 24 字节或更多字节。
- Target Address 不是多播地址。
- 所有包括的选项的长度大于 0。
- 如果 IP 源地址是未指定地址，IP 目的地地址是请求的节点的多播地址。
- 如果 IP 源地址是未指定地址，在该消息中不存在源链路层地址。

必须忽略 Reserved 字段的内容，以及任何不能识别的选项。将来，与本协议后向兼容的改变或许规定 Reserved 字段的内容或添加新的选项；后向不兼容的改变或许使用不同的 Code 值。

任何定义的、没有规定由 Neighbor Solicitation 消息使用的选项的内容必须被忽略，分组正常处理。可能出现的唯一已定义选项是 Source Link-Layer Address 选项。

通过此合法性检验的 Neighbor Solicitation 被称为“合法请求”。

7-1-2　Neighbor Advertisements 的合法性检测

节点如果收到不满足下述所有合法性检验的任何 Neighbor Advertisement 消息，必须将其静默抛弃：

- IP Hop Limit 字段值为 255，即，分组可能不能被路由器转发。
- ICMP 校验和合法。
- ICMP Code 为 0。
- ICMP 长度(由 IP 长度引申出)是 24 字节或更多字节。
- Target Address 不是多播地址。
- 如果 IP 目的地地址是多播地址，Solicited 标记是 0。
- 所有包括的选项的长度大于 0。

必须忽略 Reserved 字段的内容，以及任何不能识别的选项。将来，与本协议后向兼容的改变或许规定 Reserved 字段的内容或添加新的选项；后向不兼容的改变或许使用不同的 Code 值。

任何已定义的、没有规定由 Neighbor Advertisement 消息使用的选项的内容必须被忽略，分组处理正常进行。可能出现的唯一已定义选项是 Target Link-Layer Address 选项。

通过了合法性检验的 Neighbor Advertisements 被称为“合法通告”。

7-2 地址解析

地址解析是一种处理，通过地址解析节点可确定仅给出其IP地址的邻居的链路层地址。地址解析仅对被确定是on-link的地址进行，发送者不知道这些地址相应的链路层地址(参阅第5-2节)。地址解析绝不能对多播地址进行。

主机可能收到不包括链路层地址选项的请求消息、路由器通告消息、或Redirect消息。这些消息必须不生成或不更新邻居缓存条目，除非根据IsRouter标记，如第6-3-4节和第7-2-5节所述。如果针对这样消息的源地址的Neighbor Cache条目不存在，在开始与那个地址的单播通信前要求先进行Address Resolution。这特别适合对请求的单播响应，那里为完成通告传递需要一个附加分组交换。

7-2-1 接口初始化

当使能有多播能力的接口时，节点必须在那个接口上加入 all-nodes 多播地址，以及相应于分配给该接口的每一个 IP 地址的请求-节点(solicited-node)多播地址。

分配给一个接口的地址集合可随时改变。可能添加新的地址，删除旧的地址[ADDRCONF]。在这些情况，节点必须分别加入和去除相应于新的地址和旧的地址的请求-节点多播地址。使用 Multicast Listener Discovery，例如[MLD]或[MLDv2]协议，加入该请求-节点多播地址。注意，多个单播地址可以映射成同一个请求-节点多播地址；在相应于那个多播地址的所有分配的地址已经被删除前，节点必须不能去除请求-节点多播组。

7-2-2 发送 Neighbor Solicitations

当节点想发送单播分组到某个邻居，但没有该邻居的链路层地址时，它执行地址解析。对于有多播能力的接口，这要求生成处于 INCOMPLETE 状态的 Neighbor Cache 条目，并发送目标为该邻居的 Neighbor Solicitation 消息。请求被发送到对应于目标地址的请求-节点多播地址。

如果引起请求的分组的源地址与分配给该出接口的地址相同，那个地址应当被放置在该出请求的 IP Source Address 中。否则，应当使用分配给该接口的地址中的任何一个。如果可能，使用引起请求的分组的源地址，以便确保 Neighbor Solicitation 的接收者在它的 Neighbor Cache 中设置此 IP 地址，该 IP 地址极有可能被用于属于引起请求的分组的“连接”的后续

返回流量。

如果该请求正在发送到请求-节点多播地址，发送者必须包括它的链路层地址(如果它有)作为 Source Link-Layer Address 选项。否则，发送者应当包括它自己的链路层地址(如果它有)作为 Source Link-Layer Address 选项。要求在多播请求中包括源链路层地址，可以给目标一个地址，发送者能够发送 Neighbor Advertisement 到该地址。对于单播请求，实现可以忽略 Source Link-Layer Address 选项。这里假定如果发送者在它的缓存中有对端的链路层地址，存在很高概率的是对端在其缓存中也有发送者的一个条目。因此，对端不需要发送。

当等待地址解析完成时，对于每一个邻居，发送者必须保留一个小的等待地址解析完成的分组队列。然而，针对每个邻居的排队分组数目应当限制在较小值。当队列溢出时，新来的应当取代最早进入的。一旦地址解析完成，节点发送任何排队分组。

当等待响应时，发送者应当重复发送 Neighbor Solicitation 消息，几乎每 RetransTimer 毫秒发送一次，甚至在没有附加流量需要发送到该邻居时也应如此。重复发送必须是速率受限的，每个邻居，每 RetransTimer 毫秒最多 1 个请求。

如果在 MAX_MULTICAST_SOLICIT 次请求后，没有收到 Neighbor Advertisement，地址解析失败。对于每个排队等待地址解析的分组，发送者必须返回代码为 3(地址不可达)的 ICMP 目的地不可达指示。

7-2-3 Neighbor Solicitations 接收

不满足下述任何要求的合法 Neighbor Solicitation 必须被静默抛弃：

- Target Address 是分配给接收接口的“合法”单播或任播地址[ADDRCONF]，
- Target Address 是单播或任播地址，节点正在为该地址提供前缀服务，或
- Target Address 是“临时”地址，在该地址上 Duplicate Address Detection 正在执行[ADDRCONF]。

如果 Target Address 是临时的，应当按照[ADDRCONF]描述的处理 Neighbor Solicitation。否则，适用下述描述。如果 Source Address 不是未指定地址，以及在链路层有地址，请求包括 Source Link-Layer Address 选项，那么接收者应当生成或更新该请求的 IP Source Address 的 Neighbor Cache 条目。如果条目不存在，节点应当生成一个新的条目，并设置它的可达性状态为 STALE，如第 7-3-3 节规定的。如果条目已经存在，并且缓存的链路层地址不同于收到的 Source Link-Layer 选项中的值，缓存的地址应当被收到的地址取代，并且该条目的可达性状态必须设置为 STALE。

如果生成了 Neighbor Cache 条目，IsRouter 标记应当设置为 FALSE。这将是这样的情况：因为 Neighbor Solicitation 消息没有包括在任何情况下发送者都是路由器的指示，即使 Neighbor Solicitation 是由路由器发送的。在发送者是路由器情况，后续 Neighbor Advertisement 消息或 Router Advertisement 消息将设置正确的 IsRouter 值。如果一个 Neighbor Cache 条目已经存在，它的 IsRouter 标记必须不被修改。

如果 Source Address 是未指定地址，节点必须不生成或更新 Neighbor Cache 条目。

在对 Neighbor Cache 的任何更新之后，节点发送 Neighbor Advertisement 响应，如下一节所述。

7-2-4 发送 Solicited Neighbor Advertisements

节点发送 Neighbor Advertisement，以便响应目标为节点的已分配地址之一的合法 Neighbor Solicitation。通告的 Target Address 拷贝自请求的 Target Address。如果请求的 IP Destination Address 不是多播地址，Target Link-Layer Address 选项可以被忽略；邻近节点的缓存值必须已经是目前值，以便使请求能够被接收。如果请求的 IP Destination Address 是一

个多播地址，通告中必须被包括 Target Link-Layer 选项。此外，如果节点是路由器，它必须设置 Router flag 为 1；否则，它必须设置该标记为 0。

如果 Target Address 或者是任播地址，或者是节点正在为其提供前缀服务的单播地址，或者没有包括 Target Link-Layer Address 选项，Override 标记应当设置为 0。否则，Override 标记置 1。Override 标记的适当设置确保节点对非前缀通告提供优先权，甚至当在前缀通告之后收到，同时也确保任播地址的第一个通告“成功”。

如果请求的源是未指定地址，节点必须设置 Solicited 标记为 0 并多播该通告到 all-nodes 地址。否则，节点必须设置 Solicited 标记为 1 并单播该通告到该请求的 Source Address。如果 Target Address 是任播地址，发送者应当延时一个随机时间(随机时间取值范围在 0 到 MAX_ANYCAST_DELAY_TIME 秒之间)发送响应。

因为单播 Neighbor Solicitations 不要求包括 Source Link-Layer Address，发送请求的 Neighbor Advertisement 的节点在它的 Neighbor Cache 中没有该邻居的相应的链路层地址是可能的。在此情况，节点将第一次必须使用 Neighbor Discovery 去确定它的邻居的链路层地址(即，发出多播 Neighbor Solicitation)。

7-2-5 Neighbor Advertisements 的接收

当收到合法 Neighbor Advertisement 时(或者请求的，或者非请求的)，针对此目标条目搜索 Neighbor Cache。如果没有条目存在，该通告应当被静默抛弃。条目不存在也不需要生成，因为接收者明显还没有初始化任何与该目标的通信。

一旦加载了适当的 Neighbor Cache 条目，规定采取的具体操作取决于 Neighbor Cache 条目的状态，在通告中的标记，以及实际提供的链路层地址。

如果收到通告时，目标的 Neighbor Cache 条目处于 INCOMPLETE 状态，一或两个事情发生。如果链路层有地址并且不包括 Target Link-Layer Address 选项，接收节点应当静默抛弃收到的通告。否则，接收节点执行下述步骤：

- 它在 Neighbor Cache 条目中记录下此链路层地址。
- 如果通告的 Solicited 标记置 1，条目的状态被设置为 REACHABLE；否则，被设置为 STALE。
- 它基于收到的通告中的 Router 标记，在缓存条目中设置 IsRouter 标记。
- 它发送任何目的地为该邻居的、等待地址解析完成的排队分组。

注意，如果该条目处于 INCOMPLETE 状态，忽略 Override 标记。

如果当收到通告时，目标的 Neighbor Cache 条目处于除了 INCOMPLETE 外的任何状态，采取下述行动：

1、如果 Override 标记被清零，并且提供的链路层地址不同于在缓存中的地址，那么采取以下两个行动之一：

a、如果条目的状态是 REACHABLE，设置它为 STALE，但是不用任何其他方法更新该条目。

b、否则，此收到的通告应当被忽略并且必须不更新该缓存。

2、如果 Override 标记置 1，或提供的链路层地址与在缓存中的地址相同，或没有提供 Target Link-Layer Address 选项，此接收的通告必须按如下更新 Neighbor Cache 条目：

- 在 Target Link-Layer Address 选项中的链路层地址必须被插入到该缓存中(如果该链路层地址被提供，并且不同于已经记录的地址)。
- 如果 Solicited 标记置 1，该条目的状态必须被设置为 REACHABLE。如果 Solicited 标记置 0 并且链路层地址被用不同的地址更新，此状态必须被设置为 STALE。否则，该条目的状态保持不变。

如果通告是对 Neighbor Solicitation 的响应，该通告的 Solicited 标记仅应当被置 1。因

为 Neighbor Unreachability Detection Solicitations 被发送到该缓存的链路层地址，收到请求的通告标志着转发路径正在工作。然而，收到非请求通告，可能指示邻居有紧急信息宣布(例如，改变了链路层地址)。如果此紧急信息指出节点目前使用的某个东西已经改变了，当节点发送下一个分组时，节点应当检验(新)路径的可达性。对于没有改变缓存内容的非请求通告不需要更新状态。

- 在缓存条目中的 IsRouter 标记必须基于收到通告中的 Router 标记设置。在由于这个更新导致的 IsRouter 标记从 TRUE 改变到 FALSE 情况，节点必须从 Default Router List 中删除此路由器，并为使用那个邻居作为路由器的所有目的地更新 Destination Cache 条目，如第 7-3-3 节所规定的。这对于检测被用作路由器的节点何时由于被配置成主机而停止转发分组是需要的。

上述规则确保当 Neighbor Advertisement 在先(即，Override 标记置 1)时更新缓存，或者是当 Neighbor Advertisement 表示相同的链路层地址，且该地址目前记录在缓存中时更新缓存。如果不属于上述应用中的任何一种，通过改变该缓存条目中的状态，该通告催促进一步的 Neighbor Unreachability Detection(如果它不是已经在进行中)。

7-2-6 发送 Unsolicited Neighbor Advertisements

某些情况下节点或许能够确定它的链路层地址已经改变(例如，接口卡的热插拔)，希望尽快通知它的邻居们链路层地址发生改变。在此情况，节点可以发送最多 MAX_NEIGHBOR_ADVERTISEMENT 次非请求 Neighbor Advertisement 消息到 all-nodes 多播地址。这些通告之间必须相隔至少 RetransTimer 秒。

在非请求通告中 Target Address 字段被设置为接口的 IP 地址，Target Link-Layer Address 选项用新的链路层地址填充。Solicited 标记必须设置为 0，以便避免干扰 Neighbor Unreachability Detection 算法。如果节点是路由器，它必须设置 Router 标记为 1；否则，它必须设置 Router 标记为 0。Override 标记可以被设置为 0 或 1。在每一种情况下，相邻节点将立即改变它们的 Target Address 的 Neighbor Cache 条目的状态为 STALE，督促相邻节点们检验路径的可达性。如果 Override 标记置 1，相邻节点们将在它们的缓存中设置新的链路层地址。否则，它们将忽略新的链路层地址，选择探测此缓存的地址。

接口分配了多个 IP 地址的节点可以为每个地址多播独立的 Neighbor Advertisement。在此情况，在发送每个通告之间节点应当引入一个小的延时，以便减小由于拥塞导致通告丢失的概率。

代理可以多播 Neighbor Advertisements，当代理的链路层地址改变或当代理被配置(由系统管理或其他机制)为地址的代理时。如果有多个节点正在为相同的地址集合提供代理服务，这些代理应当提供一种机制，该机制阻止多个代理为任何一个地址多播通告，以便减少产生过分多播流量的风险。这是对需要使用 Neighbor Advertisements 代理的其他协议的要求。节点执行代理通告的一个例子是在[MIPv6]中规定的归属地代理。

同样，属于任播地址的节点可以为该任播地址多播非请求 Neighbor Advertisements，当该节点的链路层地址改变时。

注意，因为非请求 Neighbor Advertisements 不能可靠更新在所有节点中的缓存(通告或许不被所有节点接收)，非请求 Neighbor Advertisements 应当仅被看作在大多数邻居中快速更新缓存的性能最佳化。Neighbor Unreachability Detection 算法确保所有节点获得可通达的链路层地址，尽管延时或许稍微长一些。

7-2-7 任播 Neighbor Advertisements

从 Neighbor Discovery 的角度，多数情况任播地址仅被看作是单播地址。因为任播地址

在句法上与单播地址相同，在任播地址上执行地址解析或 Neighbor Unreachability Detection 的节点，对待任播地址就好像它是一个单播地址一样。不需要特殊的处理。

当节点的接口被分配了任播地址时，节点对待任播地址完全像对待单播地址一样，但有两点除外。第一，为响应 Neighbor Solicitation 而发送的 Neighbor Advertisements 应当延时一个随机时间，该时间取值范围从 0 到 MAX_ANYCAST_DELAY_TIME，以便减少网络拥塞的概率。第二，在 Neighbor Advertisements 中的 Override 标记应当被设置为 0，所以当多个通告抵达时，使用第一个接收的通告，而不是使用最后收到的通告。

与采用单播地址时一样，Neighbor Unreachability Detection 确保节点快速检测出何时目前绑定的任播地址变得不合法。

7-2-8 代理 Neighbor Advertisements

在限定的环境下，路由器可以代理一个或多个其他节点，即，通过 Neighbor Advertisements，路由器指出愿意接收不显示寻址到它自己的分组。例如，路由器或许代表移动到 off-link 的移动节点接收分组。由代理使用的这些机制基本上与采用任播地址的机制相同。

代理必须加入非请求-节点多播地址，这个(这些)地址对应于接受代理的节点的 IP 地址。这应当使用多播监听发现协议(例如[MLD]或[MLDv2])实现。

所有非请求代理的 Neighbor Advertisement 消息必须将 Override 标记置 0。这确保如果节点自己在链路上，它的 Neighbor Advertisement(带有置 1 的 Override 标记)将优先于从代理处收到的任何通告。代理可以发送带有 Override 标记置 1 的非请求通告，如第 7-2-6 节所述，但是这样做或许引起此代理通告废止由节点自己生成的合法条目。

最后，当发送响应 Neighbor Solicitation 的代理通告时，发送者应当延时一个随机时间发送它的响应，该时间取值从 0 到 MAX_ANYCAST_DELAY_TIME 秒，以避免几个代理同时发送的多个响应从而出现碰撞。然而，在某些情况(例如，MIPv6)，那里仅有一个代理，这类延时是不需要的。

7-3 Neighbor Unreachability Detection

到邻居或经过邻居的通信会在任何时刻，因无数种原因而失败，包括硬件故障，接口卡热插拔，等等。如果目的地不对，不可能恢复，通信将失败。另一方面，如果失败的原因是路径，恢复通信是可能的。于是，节点积极跟踪它正在发送的分组要抵达的节点的可达性“状态”。

Neighbor Unreachability Detection 用于主机和相邻节点间的所有路径，包括主机到主机通信，主机到路由器通信和路由器到主机通信。Neighbor Unreachability Detection 也可用于路由器之间，但是如果相同的机制存在(例如作为路由协议的一部分)，对此不作要求。

当到邻居的路径出现故障时，具体的恢复程序依赖于邻居如何被使用。例如，如果邻居是最终目的地，应当再次执行地址解析。然而，如果邻居是路由器，尝试交换到另一个路由器是适当的。发生的特定恢复包括在下一跳确定中；Neighbor Unreachability Detection，通过删除一个 Neighbor Cache 条目，指出需要下一跳确定。

Neighbor Unreachability Detection 的执行，仅针对向其发送单播分组的邻居(即这些邻居接收单播分组)；当发送到多播地址时不使用 Neighbor Unreachability Detection。

7-3-1 可达性确认

如果节点最近已经收到一个确认，该确认表明最近发送到某个邻居的分组已经由该邻居的 IP 层接收，该邻居被认为是可达的。收集肯定确认有两种方法：来自上层协议的暗示，

这些暗示指出连接正处于“转发中”，或正在接收作为 Neighbor Solicitation 消息的响应的 Neighbor Advertisement 消息。

如果来自远端对端的分组正在抵达，如果发送到那个对端的最新分组实际上正在抵达对端，连接处于“转发中”。例如，在 TCP 中，收到(新)确认指出先前发送的数据已抵达对端。同样，新数据(非重复)的到来指出较早的确认正在被交付给远端对端。如果分组正在抵达对端，分组也必然正在抵达发送者的下一跳邻居；于是，“转发中”是一个确认，它指出下一跳邻居是可达的。对于 off-link 目的地，转发中暗示第一跳路由器是可达到。当有可能时，这个上层信息应当使用。

在某些情况(例如，基于UDP的协议和转发分组到主机的路由器)，这类可达性信息不容易从上层协议获得。当没有暗示可以利用而节点正在发送分组到邻居时，节点使用单播 Neighbor Solicitation消息主动探测该邻居，以检验转发路径是否仍然工作正常。

收到请求的 Neighbor Advertisement 可视为可达性确认，因为带有 Solicited 标记置 1 的通告仅在响应 Neighbor Solicitation 时发送。其他 Neighbor Discovery 消息的接收，例如 Router Advertisements 和带有 Solicited 标记置 0 的 Neighbor Advertisement，不能被看作是可达性确认。收到非请求消息仅确认从发送者到接收节点的单向路径。比较起来，Neighbor Unreachability Detection 要求节点从它的角度，持续跟踪到邻居的转发路径的可达性，不是从邻居的角度。注意，收到请求的通告指出路径双向可通达。该请求必然已经到达该邻居，并引起该邻居生成一个通告。同样，收到通告指出从发送者到接收者的路径是通达的。然而，后者的事实仅接收者知道；通告的发送者没有直接方法知道它发送的通告实际上已抵达邻居。从 Neighbor Unreachability Detection 的角度，仅对转发路径的可达性感兴趣。

7-3-2 Neighbor Cache 条目状态

Neighbor Cache 条目可处于以下 5 种状态之一：

INCOMPLETE

关于该条目的地址解析正在被执行。具体来说，Neighbor Solicitation 已经发送到目标的请求-节点多播地址，但是相应的 Neighbor Advertisement 还没有收到。

REACHABLE

在最后的 ReachableTime 毫秒内收到肯定确认，该确认指出到邻居的转发路径正常运行。在 REACHABLE 状态期间，发送分组时不发生特定操作。

STALE

自从收到最后一个表示转发路径正常运行的肯定确认后，超过 ReachableTime 毫秒时间已经过去。在 STALE 状态期间，直到分组被发送为止没有操作发生。进入 STALE 状态，依赖于收到非请求 Neighbor Discovery 消息，该消息更新了缓存的链路层地址。收到这样的消息不能确认可达性，进入 STALE 状态确保可达性被迅速检验，如果该条目实际上正在被使用。然而，直到该条目实际被使用为止可达性实际上没有被检验。

DELAY

自从收到最后一个表明转发路径正常运行的肯定确认，超过 ReachableTime 毫秒时间已经过去，并且在最后 DELAY_FIRST_PROBE_TIME 秒内发送了分组。如果在进入 DELAY 状态后的 DELAY_FIRST_PROBE_TIME 秒内没有收到可达性确认，发送 Neighbor Solicitation 并改变状态到 PROBE。

DELAY 状态是一种优化，它适用于在下述场景给上层协议一些附加时间，以便提供可达性确认。这些场景是指，由于最近流量缺乏，自最近的确认以来 ReachableTime 毫秒时间已经过去。没有这个优化，在流量间歇之后，当打开

TCP 连接时会进行初始化探测，即使随后的三次握手几乎立即提供可达性确认。

PROBE

通过每RetransTimer毫秒重复发送Neighbor Solicitations直到收到可达性确认，来主动地搜索可达性确认。

7-3-3　节点行为

采用发送分组到邻居，Neighbor Unreachability Detection 以并联方式运行。当重申邻居的可达性时，节点继续使用缓存的链路层地址发送分组到那个邻居。如果没有流量发送到邻居，也就没有发送探测。

当节点需要对邻近地址执行地址解析时，它用 INCOMPLETE 状态生成条目，并初始化地址解析，如第 7-2 节所述。如果地址解析失败，会删除该条目，因而到那个邻居的后续流量将再次引起下一跳确定过程。这里引起下一跳确定可确保寻找替代默认路由器。

当收到可达性确认时(或者通过上层设备，或者通过请求的 Neighbor Advertisement)，条目状态改变到 REACHABLE。一个例外是上层设备对处于 INCOMPLETE 状态的条目没有影响(例如，没有缓存链路层地址情况)。

自从收到最后一个对于某个邻居的可达性确认以来 ReachableTime 毫秒时间已经过去，Neighbor Cache 条目的状态从 REACHABLE 改变到 STALE。

注意：实现中可以考虑推迟从 REACHABLE 到 STALE 的改变，直到分组被发送到该邻居，即，不需要有与 ReachableTime 到期关联的清晰的超时事件。

第一次节点发送分组到邻居(该邻居的条目是 STALE)时，发送者改变该状态为 DELAY，并设置一个在 DELAY_FIRST_PROBE_TIME 秒期满的计时器。如果该计时器到期此条目仍然处于 DELAY 状态，该条目的状态改变到 PROBE。如果收到可达性确认，此条目的状态改变到 REACHABLE。

一旦进入 PROBE 状态，节点使用缓存的链路层地址发送单播 Neighbor Solicitation 消息到该邻居。当在 PROBE 状态时，节点每 RetransTimer 毫秒重发一次 Neighbor Solicitation 消息，直到获得可达性确认。即使没有附加分组需要发送到该邻居，也将重复发送探测。如果在等待RetransTimer毫秒后，发送了 MAX_UNICAST_SOLICIT 次请求之后，没有收到响应，停止重发并且应当删除该条目。到那个邻居的后续流量将重新生成该条目并再次执行地址解析。

注意，所有 Neighbor Solicitations 对于每个邻居而言是发送速率受限的。节点必须不能比每 RetransTimer 毫秒 1 次更频繁地发送 Neighbor Solicitations 到同一邻居。

当出现收到分组而不是收到请求的Neighbor Advertisements (即，Router Solicitations、Router Advertisements、Redirects和Neighbor Solicitations)的结果时，Neighbor Cache条目进入STALE状态。这些分组包含发送者的链路层地址，或者是，在Redirect情况，包含重定向目标的链路层地址。然而，收到这些链路层地址不能证实到那个节点的转发方向路径是畅通的。安排新生成的处于STALE状态的Neighbor Cache条目(对应该条目的链路层地址是已知的)，可提供迅速检测到路径故障的保证。此外，由于收到上述消息之一，应当修改缓存的链路层地址，状态也应当被设置为STALE，以便提供快速验证：到新的链路层地址的路径工作正常。

为了适时检测到路由器从是路由器转变为是主机(例如，如果路由器的 IP 转发能力被系统关断)，节点必须将所有接收到的 Neighbor Advertisement 消息中的 Router 标记字段与在 Neighbor Cache 条目中记录的 IsRouter 标记比较。当节点检测到邻居已经从是路由器转变为是主机时，节点必须从 Default Router List 中删除那个路由器，并更新 Destination Cache，如

第 6-3-5 节所述。注意，即使 Destination Cache 条目正在使用一个路由器(例如，主机被重定向到它)，该路由器或许并没有列示在 Default Router List 中。在此情况，所有与该(前)路由器有关的 Destination Cache 条目，在使用前必须再次执行下一跳确定。

在某些情况，链路-特定信息或许指出到邻居的路径已经出故障(例如，重新设置了虚电路)。在此情况，链路-特定信息可以用于在执行 Neighbor Unreachability Detection 前清除 Neighbor Cache 条目。然而，链路-特定信息必须不用于确认邻居的可达性；这样的信息不提供相邻 IP 层之间的端到端确认。

第 8 章　重定向功能

本章描述与 Redirect 消息的发送和处理有关的功能。Redirect 消息由路由器发送，以便针对具体的目的地重定向主机到较好的第一跳路由器，或通知主机某个目的地事实上是邻居(即，on-link)。后者通过使 ICMP Target Address 等于 ICMP Destination Address 实现。路由器必须能够确定它的每个邻近路由器的链路本地地址，以便确保通过邻近路由器的链路本地地址，Redirect 消息中的目标地址可以标识邻近路由器。对于静态路由，这个要求暗示应当规定使用下一跳路由器的链路本地地址为该路由器的地址。对于动态路由，这个要求暗示所有 IPv6 路由协议必须以某种方式交换邻近路由器的链路本地地址。

8-1　Redirect 消息的合法性检测

主机必须静默抛弃收到的任何不能满足下述所有合法性检验的 Redirect 分组：

- IP Source Address 是链路本地地址。路由器必须使用它们的链路本地地址作为 Router Advertisement 消息和 Redirect 消息的源，以便主机能够唯一地识别路由器。
- IP Hop Limit 字段值为 255，即，分组可能不能被路由器转发。
- ICMP 校验和合法。
- ICMP Code 为 0。
- ICMP 长度(从 IP 长度引出)是 40 字节或更多字节。
- Redirect 的 IP 源地址与规定的 ICMP Destination Address 的目前第一跳路由器相同。
- 重定向消息中 ICMP Destination Address 字段不包括多播地址。
- ICMP Target Address 或者是链路本地地址(当重定向到路由器时)，或者是与 ICMP Destination Address 相同(当重定向到 on-link 目的地)。
- 所有包括的选项的长度大于 0。

Reserved 字段的内容以及任何不能识别的选项必须被忽略。将来，与本协议后向兼容的改变或许规定 Reserved 字段的内容或添加新的选项；后向不兼容的改变或许使用不同的 Code 值。

任何已定义的、没有规定由 Redirect 消息使用的选项的内容必须被忽略，分组处理正常进行。唯一经过定义，有可能出现的选项是 Target Link-Layer Address 选项和 Redirected Header 选项。

主机必须不仅仅因为重定向的 Target Address 没有被链路的前缀之一覆盖，就认为重定向无效。Redirect 消息在语义上的含义是 Target Address 为 on-link。
通过合法性检验的重定向成为“合法的重定向”。

8-2　路由器规范

路由器应当发送重定向消息，遵守速率限制，无论何时它都转发不是显示寻址到它自己的分组(即，分组不是源路由通过该路由器)：

- 分组的 Source Address 字段标识邻居，并且

- 路由器确定(采用的方法超出本规范)较好的第一跳节点驻留在同一链路上，作为正在被转发的分组的 Destination Address 的发送节点，并且
- 该分组的 Destination Address 不是多播地址。

发送的重定向分组包括(消息格式与第 4-5 节给出的一致)：

- 在 Target Address 字段中：到该目的地的后续分组应当被发送到的地址。如果此目的地是路由器，必须使用路由器的链路层地址。如果目标是主机，目标地址字段必须被设置为与 Destination Address 字段相同的值。
- 在 Destination Address 字段中：产生 IP 分组的目的地地址。
- 在这些选项中：
  - Target Link-Layer Address 选项：目标的链路层地址，如果知道。
  - 重定向首部：像能够适合没有超过支持 IPv6 要求的最小 MTU(如在[IPv6]中规定)的重定向分组一样多的转发分组。

路由器必须限制发送 Redirect 消息的速率，以便限制当源端没有正确响应 Redirects，或源端选择忽略未授权的 Redirect 消息时，由 Redirect 消息引起的带宽和处理成本。更多关于 ICMP 出错消息速率限制的细节可在[ICMPv6]中发现。

路由器必须不依据收到 Redirect 来更新它的路由表。

8-3　主机规范

收到合法重定向的主机应当按照后续流量将要被发送到的特定目标，更新它的 Destination Cache。如果那个目的地的 Destination Cache 条目不存在，实现中应当生成这个条目。

如果重定向包括 Target Link-Layer Address 选项，主机或者生成或者更新此目标的 Neighbor Cache 条目。在两种情况，缓存的链路层地址是从 Target Link-Layer Address 选项中拷贝来的。如果生成了该目标的 Neighbor Cache 条目，它的可达性状态必须设置为 STALE，如第 7-3-3 节所述。如果缓存条目已经存在并且它被用不同的链路层地址更新，它的可达性状态也必须被设置为 STALE。如果链路层地址与缓存中已经存在的地址相同，该缓存条目的状态保持不变。

如果 Target Addresses 和 Destination Addresses 相同，主机必须把 Target 看作是 on-link。如果 Target Address 与 Destination Address 不同，对于该目标地址，主机必须设置 IsRouter 为 TRUE。然而，如果 Target Addresses 和 Destination Addresses 相同，还不能够可靠地确定该 Target Address 是否是路由器。因此，新生成的 Neighbor Cache 条目应当设置 IsRouter 标记为 FALSE，而现存的缓存条目应当保留标记不变。如果 Target 是路由器，后续 Neighbor Advertisement 消息或 Router Advertisement 消息将相应地更新 IsRouter。

重定向消息适用于所有正在被发送到给定的目的地的流。即，一旦收到 Destination Address 的 Redirect，所有到那个地址的条目应当被更新到使用规定的下一跳，无论 Flow Label 字段的内容如何，Flow Label 字段出现在 Redirected Header 选项中。

主机必须不发送 Redirect 消息。

第 9 章　扩展-选项处理

选项为编码的变量长度字段提供了一种机制，这些字段或许在同一个分组中出现多次，或者信息可能在所有分组中不出现。对于 ND 的将来版本，选项与能用于添加功能。

为了确保将来的扩展能与目前的实现共处，所有节点必须静默忽略接收的 ND 分组中任何它们不能识别的选项，并继续处理分组。节点必须能够识别本文件中规定的所有选项。节点必须不能仅因为 ND 消息包含不能识别的选项就忽略合法选项。

目前对选项集合的处理原则是：接收者能够相互独立地处理同一分组中的多个选项。为了维护这些性质，将来的选项应当遵循下述简单规则：

选项必须不依赖于任何其他选项的存在或不存在。选项的语义应当仅依赖于 ND 分组固定部分中的信息，以及选项自身中包含的信息。

遵循上述规则有下述获益：

1）接收者们能够相互独立地处理选项。例如，实现能够选择在用户-空间操作中处理包含在 Router Advertisement 消息中的 Prefix Information 选项，虽然按照惯例在同一消息中的链路层地址选项由内核处理。

2）如果选项的数目过多，引起分组超过链路 MTU，可由多个分组携带选项的子集，不需要在语义上有任何改动。

3）发送者可以在不同分组中发送选项的一个子集。例如，如果前缀的 Valid Lifetime 和 Preferred Lifetime 足够长，发送者或许不需要在每个 Router Advertisement 中包括 Prefix Information 选项。此外，不同的路由器或许发送不同的选项集合。于是，接收者必须不能因在具体分组中缺少某个选项而采取任何关联的操作。本协议规定接收者仅应当根据计时器的期满，以及根据在分组中收到的信息采取行动。

在 Neighbor Discovery 分组中的选项能够以任何次序出现；接收者必须准备独立于它们的次序处理它们。也存在消息中相同选项多次出现的情况(例如，Prefix Information 选项)。如果在 Router Advertisement 包括的选项数目引起通告的大小超过链路 MTU，路由器能够发送多个独立的通告，每个包括该选项的一个子集。

在 Redirected Header 选项中包括的数据量必须受到限制，以便该整个重定向分组不超过支持 IPv6 要求的最小 MTU(参阅[IPv6])。

所有选项都是 8 字节倍数长度，这确保可使用无需任何“填充”项的算法。定义选项中的字段(以及在 ND 分组中的字段)在它们的自然边界对齐(例如，16 位字段在 16 位边界对齐)，有 128 位 IP 地址/前缀的例外，它们对齐在 64 位边界上。链路层地址字段包含未译码字节串；它在 8 位边界上对齐。

包括 IP 首部的 ND 分组的大小被限制为链路 MTU。当添加选项到 ND 分组中时，节点必须注意分组不能超过此链路 MTU。

本协议将来版本可以定义新的选项类型。接收者必须静默忽略任何它们不能识别的选项，并继续处理消息。

第 10 章　协议常数

路由器常数：

MAX_INITIAL_RTR_ADVERT_INTERVAL	16秒
MAX_INITIAL_RTR_ADVERTISEMENTS	3次发送
MAX_FINAL_RTR_ADVERTISEMENTS	3次发送
MIN_DELAY_BETWEEN_RAS	3秒
MAX_RA_DELAY_TIME	0.5秒

主机常数：

MAX_RTR_SOLICITATION_DELAY	1秒
RTR_SOLICITATION_INTERVAL	4秒
MAX_RTR_SOLICITATIONS	3 次发送

节点常数：

MAX_MULTICAST_SOLICIT	3次发送
MAX_UNICAST_SOLICIT	3次发送

MAX_ANYCAST_DELAY_TIME	1秒
MAX_NEIGHBOR_ADVERTISEMENT	3 次发送
REACHABLE_TIME	30,000毫秒
RETRANS_TIMER	1,000毫秒
DELAY_FIRST_PROBE_TIME	5秒
MIN_RANDOM_FACTOR	.5
MAX_RANDOM_FACTOR	1.5

附加的协议常数采用第 4 章中的消息格式定义。

所有协议常数服从本协议将来版本中的改变。

本规范中的常数可以由描述 IPv6 如何在不同链路层上运行的文件替代。本规则允许 ND 在具有很宽性能特征变化范围的链路上运行。

第 11 章　安全考虑

ND 易遭受这样的攻击，该攻击能够使 IP 分组流动到不希望位置。这类攻击能够用于引起拒绝服务，而且能让节点截获和选择性地修改分组的目的地为其他节点。本章详述与 ND 消息相关的主要威胁，和能够减轻这些威胁的可能安全机制。

11-1　威胁分析

本节讨论与 ND 相关的主要威胁。更为详细的分析参阅[PSREQ]。针对本协议弱点的攻击主要有：

- 拒绝服务(DoS)攻击。
- 地址欺骗攻击。
- 路由器欺骗攻击。

下述是拒绝服务攻击的一个例子。在链路上能够用任意 IP 源地址发送分组的节点，既能通告它自己为默认路由器，也能发送“伪造的”Router Advertisement 消息，这些伪造的消息可以立即终止所有其他默认路由器，以及所有 on-link 前缀。入侵者通过发送出多个 Router Advertisements 即可实现此。

在针对每个合法路由器的 Router Advertisements 中，将另一个路由器的地址设置为源地址，Router Lifetime 字段设置为 0，所有前缀的 Preferred lifetimes 和 Valid lifetimes 设置为 0。这样一个攻击引起所有分组，无论是 on-link 目的地还是 off-link 目的地，都被发送到该流氓路由器。接着那个路由器能够有选择的检验、修改或抛弃所有在该链路上发送的分组。只要流氓路由器用一个 R 比特置 1 的 Neighbor Advertisement 有礼貌地回答 NDU 的探测，Neighbor Unreachability Detection (NUD)将不检测这样的黑洞。

对于任何主机类似的攻击可能是，在另一个主机上通过阻止该主机使用[ADDRCONF]配置地址，发动 DoS 攻击。本协议不允许主机验证是否 Neighbor Advertisement 的发送者是包括在该消息中的 IP 地址的真正拥有者。

Redirect 攻击也可通过任何主机实现，以便泛洪牺牲者或盗取它的流量。主机能够发送 Neighbor Advertisement(对请求进行响应)，该 Neighbor Advertisement 中包含主机的 IP 地址，和牺牲者的链路层地址，以便用不希望的流量泛洪该牺牲者。作为替代，该主机能够发送 Neighbor Advertisement，该 Neighbor Advertisement 包括牺牲者的 IP 地址，和主机自己的链路层地址，以便在发送者的目的地缓存中重写一个现存的条目，借此强迫发送者转发牺牲者的所有流量到自己。

重定向的信任模式与 IPv4 相同。仅当从同一路由器(该路由器目前正在被用于那个目的地)接收时，重定向才被接受。如果主机已经被重定向到另一个节点(即，目的地是 on-link)，

没有办法阻止目标发布另一个重定向到某个其他目的地。然而，这个暴露不比主机被重定向以前更糟；目标主机，一旦被破坏，总能够充当隐藏的路由器向其他地方转发流量。

本协议没有包括确定哪一个邻居被授权发送特定类型消息的机制(例如，Router Advertisements)；任何邻居，甚至是有认证情况下，能够发送 Router Advertisement 消息，因此能够引起拒绝服务。此外，任何邻居能够发送代理 Neighbor Advertisements，以及非请求 Neighbor Advertisements 作为潜在的拒绝服务攻击。

许多链路层也容易受到不同的拒绝服务攻击，例如在 CSMA/CD(Carrier Sense Multiple Access with Collision Detection)网络中连续占用链路(例如，通过紧密地背对背发送分组或坚持说在链路上有碰撞信号)，或用某个别的源 MAC 地址的起始分组来混淆，例如，以太网交换。另一方面，本章讨论的许多威胁不太有效，或不存在，在点对点链路上，或蜂窝链路上，那里主机仅与一个邻居，即默认路由器，共享链路。

11-2　安全的 Neighbor Discovery 消息

通过忽略从 off-link 发送者收到的 ND 分组，本协议减少了在缺少认证情况下对上述威胁的暴露。所有收到分组的 Hop Limit 字段被验证包含 255，最大逻辑值。因为路由器在所有它们转发的分组上减少了 Hop Limit，包含 Hop Limit 值为 255 的收到的分组必然来自邻居。

对 ND 的加密安全机制超出本文件范围，在[SEND]中定义。作为替代，IPsec 能够用于 IP 层认证[IPv6-SA]。Internet Key Exchange (IKE)不适合生成动态安全联盟，安全联盟能够用于安全地址解析或邻居请求消息，参阅[ICMPIKE]。

在某些情况，使用静态配置的安全联盟是可以接受的，该安全联盟使用[IPv6-AUTH]或[IPv6-ESP]保护 ND 消息。然而，需要注意到是，静态配置的安全联盟是不可测量的(尤其是使用多播链路时)，因此仅适用于已知主机的小型网络。在任何情况，如果使用[IPv6-AUTH]或[IPv6-ESP]，出于认证目的，必须验证 ND 分组。不能通过认证验证的分组必须被静默抛弃。

第 12 章　重新编码考虑

ND 协议与 IPv6 Address Autoconfiguration [ADDRCONF]一起提供了协助重新编码机制：引入新的前缀和地址，使旧的前缀和地址无效并被删除。

这些机制的茁壮性，依赖于链路上采用及时方式接收 Router Advertisement 消息的所有节点。然而，在连续的时间周期内主机可能关机，或变为不可达(即，项目结束后计算机被关机数月)。在这类情况中保存茁壮的重编码是可能的，但是对多长时间必须通告一次前缀要做一些限制。

下面试举一例。例子中初始通告中指明的前缀生存期为 2 个月，但是 8 月 1 日决定，由于 9 月 1 日要重新编码，该前缀需要被废弃和删除。为实现此，可如下操作，将前面通告的生存期改为到 8 月 1 日后 1 周为止，因为生存期的截止期提前了，生存期缩短，直到 9 月 1 日发出的通告指出前缀的生存期为 0。

关键是，如果一个或多个节点在 9 月 1 日前开通与链路的连接，它们或许仍然认为前缀是合法的，因为它们收到的最后一个生存期是 2 个月。于是，如果节点在 7 月 31 日开通，它认为直到 9 月 30 日前缀都有效。如果那个节点在 9 月 30 日前又关机，它或许继续使用旧的前缀。强迫节点停止使用先前通告的、有长生存期的前缀的唯一方法，是使那个节点收到一个针对那个前缀的通告，在此通告中说明该前缀的生存期已经缩短。此例中的解决办法比较简单：连续发出前缀生存期值为 0 的通告，从 9 月 1 日直到 10 月 1 日。

一般来说，为了减轻节点又连接到链路对茁壮性的影响，重要的是持续跟踪下去，一直

到将来某个时刻链路上任何节点都能视一个特定前缀为合法为止。其次必须通告该前缀的生存期值为 0，直到将来的那个时刻。对于所有 Router Advertisements，“将来的那个时刻”简单讲是通告发送时间的最大值，加上包括在通告内的该前缀生存期。

上述分析体现了使用无限期生存期的重要意义。如果发出的通告中前缀的生存期为无限，并且之后需要对那个前缀重新编码，连续通告那个前缀的生存期永远为 0 是令人不愉快的。于是，或者不使用无限生存期，或者对节点在它被再次关机前能有多长时间连接到链路上必须有一个限制。然而不清楚网络管理者如何能够强制执行一个限制，这个限制是指主机(如笔记本电脑)被连接到链路多长时间。

网络管理者应当严肃对待使用相对短的生存期(即，仅几周)。虽然短生存期也可以使用，使用长生存期有助于确保茁壮性，实际中，没有适当行使职责的路由器的支持主机将不能通信。适当行使职责的路由器将发送包含适当(和目前)前缀的 Router Advertisements。没有行使职责路由器支持的连网主机很可能遇到比仅缺乏合法前缀和地址更严重的问题。

上述讨论没有区别优先的生存期和合法的生存期。从实际考虑，跟踪合法生存期更合理一些，因为优先的生存期不会超过合法的生存期。

第 13 章　IANA 考虑

本文件不要求分配任何新的 ICMPv6 类型或代码。然而，现存 ICMPv6 类型已经被更新到本文件，取代了 RFC2461。ICMPv6 类型/代码的分配程序在[ICMPv6]第 6 章介绍。

本文件继续使用由 RFC2461 引入的下述 ICMPv6 消息类型，这些消息类型已经由 IANA 分配：

消息名称	ICMPv6 类型
Router Solicitation	133
Router Advertisement	134
Neighbor Solicitation	135
Neighbor Advertisement	136
Redirect	137

本文件继续使用由 RFC2461 引入的下述下述 Neighbor Discovery 选项类型，这些选项类型已经由 IANA 分配：

选项名称	类型
Source Link-Layer Address	1
Target Link-Layer Address	2
Prefix Information	3
Redirected Header	4
MTU	5

Neighbor Discovery 选项类型的分配过程如下：

1、IANA 会根据 IETF RFC 出版物，分配和永久注册新的选项类型。这适合所有 RFC 类型，包括标准历程、信息、和试验状态，它们来源于 IETF 并已经获得 IESG 批准出版。

2、获得工作组一致同意和区域执行官批准后，IETF 工作组可以向 IANA 申请可回收的 Neighbor Discovery 选项类型分配。IANA 将分配的选项类型标记为“将来可回收的”。

当 RFC 被出版，成为文本化的协议(如 1、中定义的)，“将来可回收的”标记将被删除。这将使分配永久化，并更新 IANA 网站上的说明。

当分配了 85%的选项类型值时，IETF 将检查标记为“将来可收回的”的分配情况，并通知 IANA 一些标记应当收回，重新分配。

3、来自 IETF 外的请求新选项类型值分配，仅通过 IETF 文件出版物方式提出，参考上述 1、。

也要注意，出版的文件如“RFC Editor contributions” [RFC3667]不被认为是 IETF 文件。

14. 参考文献

14-1 标准类参考文献

[ADDR-ARCH] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[ICMPv6] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

14-2 信息类参考文献

[ADDRCONF] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[ADDR-SEL] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[ARP] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[ASSIGNED] Reynolds, J., Ed., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[DHCPv6] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[HR-CL] Braden, R., Ed., "Requirements for Internet Hosts -Communication Layers", STD 3, RFC 1122, October 1989.

[ICMPIKE] Arkko, J., "Effects of ICMPv6 on IKE", Work in Progress, March 2003.

[ICMPv4] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[IPv6-3GPP] Wasserman, M., Ed., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[IPv6-CELL] Arkko, J., Kuijpers, G., Soliman, H., Loughney, J., and J. Wiljakka, "Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts", RFC 3316, April 2003.

[IPv6-ETHER] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[IPv6-SA] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[IPv6-AUTH] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[IPv6-ESP] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[IPv6-NBMA] Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, January 1999.

[LD-SHRE] Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, November 2005.

[MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[MLD] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[MLDv2] Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[PSREQ] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RAND] Eastlake, D., 3rd, Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RDISC] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[RFC3667] Bradner, S., "IETF Rights in Contributions", RFC 3667, February 2004.

[RTSEL] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[SH-MEDIA] Braden, B., Postel, J., and Y. Rekhter, "Internet Architecture Extensions for Shared Media", RFC 1620, May 1994.

[SEND] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[SYNC] S. Floyd, V. Jacobson, "The Synchronization of Periodic Routing Messages", IEEE/ACM Transactions on Networking, April 1994. ftp://ftp.ee.lbl.gov/papers/sync_94.ps.Z

附录 A 多归属地主机

当 ND 由有多个接口的主机使用时，存在许多复杂的问题。本附录不打算定义关于 ND 的多归属地主机操作。相反，仅指出需要进一步研究的问题。鼓励人们使用各种方法试验在多归属地主机上使用 ND，并报告他们的经验。有关此的进一步讨论参阅[RTSEL]。

如果多归属地主机在所有它的接口上收到 Router Advertisements，它将(或许)针对驻留在每个链路上的地址学习 on-link 前缀。然而，当分组必须经路由器发送时，选择“错误的”路由器会导致次优化或非运行路径。如下问题需要考虑：

1）为使路由器发送重定向，必须确定正在转发的分组源于邻居。对此的标准检测是将分组的源地址与收到该分组的接口相关的 on-link 前缀的列表相比较。然而，如果发送分组的主机是多归属地主机，它使用的源地址或许属于某个接口，而该接口不是发送分组的接口。在此情况，路由器将不发送重定向，很可能选择次最佳路由。为了被重定向，发送主机必须总是在对应于发出分组的源地址的接口发出分组。注意，如不使用多归属地主机不会出现此问题；这些主机仅有一个接口。涉及此内容的进一步讨论参阅 RFC1122 第 3-3-4-2 节。

2）如果选择的第一跳路由器没有到该目的地的路由，该路由器将不能传递分组。然而，通过在其他接口上的路由器，该目的地可以通达。ND 不应用于这种场景；这在非多归属

地情况中不会出现。

3）即使第一跳路由器没有到目的地的路由，经另一个接口或许有较好的路由。多归属地主机检测这种情况的机制不存在。

如果多归属地主机不能在它的一个或多个接口上收到 Router Advertisements，它将不知道(在无配置信息时)在涉及到的接口上哪些目的地是 on-link。这会出现问题：如果在一些接口，但不是在所有接口上收到 Router Advertisements，多归属地主机仅能选择在已经收到 Router Advertisements 的接口上发出分组。然而，这里的关键假定是：在那些其他接口上的路由器们将能够路由分组到最终目的地，甚至当那些目的地驻留在发送者连接到的子网上，但是没有 on-link 前缀信息。如果此假定为 FALSE，通信将失败。即使假定成立，分组将通过次最佳路径传送。

附录 B　将来的扩展

将来的可能扩展有：

- 使用动态计时器能够适应宽范围可变延时的链路。然而，测量往返时间需要确认和序列号，以便用触发此通告的实际 Neighbor Solicitation 匹配收到的 Neighbor Advertisements。希望试验这类装置的实现者，能够通过定义携带必要信息的新选项，用后向兼容的方法完成此。节点不理解该选项可简单忽略它。
- 增加简化链路上操作的能力，目前的操作要求主机向地址解析服务器注册。例如，这将使路由器们要求主机定期向它们发送非请求通告。使用在 Router Advertisements 中发送的新选项，能够实现此增加。
- 对于将非对称的和不可转移的可达性看作是正常操作一部分的链路，添加附加程序。这类程序或许允许主机和路由器发现可使用的路径，例如，无线链路。

附录 C　可达性状态的状态机

本附录归纳第 7-2 节和第 7-3 节描述的规则。本文件不要求实现中遵循此模型，只要它们的外部行为与此文件中介绍的一致即可。

当执行地址解析和 Neighbor Unreachability Detection 时，下述状态转换适用于使用的概念性模型。

状态	事件	操作	新状态
-	分组发送。	生成条目。 发送多播 NS。 启动重发计时器	INCOMPLETE
INCOMPLETE	重发超时， 少于 N 次重发。	重发 NS 启动重发计时器	INCOMPLETE
INCOMPLETE	重发超时， N 或更多次重发。	抛弃条目 发送 ICMP 出错	-
INCOMPLETE	NA，Solicited=0， Override=any	记录链路层地址。 发送排队分组。	STALE
INCOMPLETE	NA，Solicited=1， Override=any	记录链路层地址。 发送排队分组。	REACHABLE
INCOMPLETE	NA，Solicited=any， Override=any，无 链路层地址	更新 IsRouter 标记内容	不改变
-	NS，RS，重定向	-	-

	无链路层地址		
!INCOMPLETE	NA，Solicited=1，Override=0，与缓存相同的链路层地址。	-	REACHABLE
!INCOMPLETE	NA，Solicited=any，Override=any，无链路层地址	更新 IsRouter 标记内容。	不改变
REACHABLE	NA，Solicited=1，Override=0，与缓存不同的链路层地址。	-	STALE
STALE,PROBE 或 DELAY	NA，Solicited=1，Override=0，与缓存不同的链路层地址。	-	不改变
!INCOMPLETE	NA，Solicited=1，Override=1	记录链路层地址(如果不同)。	REACHABLE
!INCOMPLETE	NA，Solicited=0，Override=0	-	不改变
!INCOMPLETE	NA，Solicited=0，Override=1，与缓存相同的链路层地址	-	不改变
!INCOMPLETE	NA，Solicited=0，Override=1，与缓存不同的链路层地址。	记录链路层地址	STALE
!INCOMPLETE	上层可达性确认	-	REANHABLE
REACHABLE	超时，自可达性确认以来多于 N 秒。	-	STALE
STALE	发送分组	启动延时计时器	DELAY
DELAY	延时超时	发送单播 NS 探针 启动重发计时器	PROBE
PROBE	重发超时，少于 N 次重发。	重发 NS	PROBE
PROBE	重发超时，N 或更多次重发。	抛弃条目	-

接收非请求信息而不是 Neighbor Advertisement 消息的状态转换用于分组源(例如，Neighbor Solicitation 消息、Router Solicitation 消息和 Router Advertisement 消息)，或者用于目标地址(例如，Redirect 消息)，如下所示：

状态	事件	操作	新状态
-	NS, RS, RA, 重定向	生成条目。	STALE
INCOMPLETE	NS, RS, RA, 重定向	记录链路层地址。 发送排队分组。	STALE

!INCOMPLETE	NS, RS, RA, 重定向与缓存不同的链路层地址	更新链路层地址	STALE
INCOMPLETE	NS, RS 无链路层地址	-	不改变
!INCOMPLETE	NS, RS, RA, 重定向与缓存相同的链路层地址	-	不改变

附录 D　IsRouter 规则小结

本附录归纳维护 IsRouter 标记的规则，正如本文件介绍的。

这些规则的背景是 ND 消息(隐含或显示)包括标识发送者(或者 Target Address)在任何情况下是主机或是路由器的信息。使用下述假定：

- 隐含假定 Router Advertisement 的发送者是路由器。
- Neighbor Solicitation 消息不包括(无论是隐含还是显示)验明发送者的标识。主机和路由器都发送 Neighbor Solicitation 消息。
- Neighbor Advertisement 消息包含显示的“IsRouter 标记”，即 R 比特。
- 当目标不同于被重定向的分组中的目的地地址时，重定向的目标隐含假定是路由器。这一假定很自然，因为预期节点会朝向目的地转发分组。
- 当该目标与目的地相同时，重定向目标不携带任何主机与路由器对应信息。所有已知的是目的地(即，目标)是 on-link，但是它可能是主机或路由器。

设置IsRouter标记的规则基于上述信息内容。如果ND消息包括显示的或隐含的信息，此消息的接收将更新IsRouter标记。但是当ND消息中没有主机与路由器对应信息时，此消息的接收必须不改变IsRouter状态。当消息的接收引起生成Neighbor Cache条目时，本文件规定IsRouter标记设置为FALSE。当节点错误地把主机当作路由器时，与其他情况相比，会出现更大的混乱。在这类情况，后续Neighbor Advertisement消息或Router Advertisement消息将设置正确的IsRouter值。

附录 E　实现问题

E-1　可达性确认

Neighbor Unreachability Detection 要求显示确认转发路径正在正常运行。为了避免对 Neighbor Solicitation 探测消息的需要，上层协议应当提供这样的指示，当这样做成本较小时。可靠的面向连接协议(例如 TCP)通常能够意识到转发路径正在正常工作。例如，当 TCP 发送(或接收)数据时，它更新它的窗口序列号，设置和清零重发计时器，等等。指出转发路径工作正常的具体场景包括：

- 收到对先前没有获得确认的序列号(例如，数据)的确认，指出在该数据被发送的时刻转发路径在正常工作。
- 完成初始化三次握手是上述规则的特例；虽然在握手期间没有数据发送，从序列号的角度 SYN 标记被看作是数据。这既适用于主动打开的 SYN+ACK，也适用于在被动打开的对端上的那个分组的 ACK。
- 收到新数据(即，数据先前没有收到)表示，发送确认时刻转发路径是畅通的，该时刻先于对端的允许发送新数据的发送窗口。

为了最小化 TCP 层和 IP 层间交流可达性信息的开销，实现中或许希望限制向 IP 层发送可达性确认的速率。一种方法是每几个分组检查一次可达性。例如，如果实现中每个连接仅有一个往返计时器，可采取每个往返时间内更新一次可达性信息。对于那些在控制块内缓存 Destination Cache 条目的做法，一旦 TCP 分组已经被解复用到它对应的控制块，可以直接更新 Neighbor Cache 条目(即，无需代价高昂的查询)。对于其他的实现，有可能在提交给

IP 的下一个分组上捎带上可达性确认。这里假定，当在扩展的时间周期内无分组发送到 IP 时，该实现可防止捎带的确认变得陈旧。

TCP 也必须避免认为“陈旧的”信息指出了目前的可达性。例如，窗口打开后 30 分钟收到的新数据不能形成目前路径畅通的确认；它仅指出 30 分钟前对端开始窗口更新，即，在那个时刻路径是畅通的。实现也必须考虑发送 TCP 零窗口探测，即使路径中断和对端没有开始窗口更新。

对于基于 UDP 的应用(Remote Procedure Call (RPC)、DNS)，当收到响应分组时使客户端发送可达性确认相对较为简单。服务器生成这样的确认比较困难，在某些情况下是不可能的，因为没有流控制，即，服务器不能确定是否收到的请求指出前一个响应已到达客户端。注意，实现不能使用否定的上层通告作为 Neighbor Unreachability Detection 算法的替代。否定的通告(例如，当存在过量重发时来自 TCP)可作为一个暗示，暗示来自数据发送者的转发路径或许不通。但是它不能检测何时来自数据接收者的路径不通，导致没有一个确认分组到达发送者。

附录 F　对 RFC2461 的改变

- 删除了作为保护消息或作为使收到的消息合法化的一部分而撰写的对 IPsec AH 和 ESP 的介绍。
- 添加了第 3-3 节。
- 更新了第 11 章，增加更多对威胁、IPsec 限制和 SEND 使用的介绍。
- 基于 RFC4942 删除了第 5-2 节中 on-link 假设，“IPv6 Neighbor Discovery On-Link Assumption Considered Harmful”。
- 在第 4-2 节澄清了 Router Lifetime 字段的定义。
- 更新了第 4-6-2 节和第 6-2-1 节中的文本，指出优先的生存期必须不大于合法生存期。
- 删除了对有状态配置的介绍，增加了对 DHCPv6 的介绍。
- 在第 6-2-1 节添加了 IsRouter 标记定义，允许混合主机/路由器行为。
- 在切换期间发送 RS 前，允许移动节点不添加随机延时。
- 在前缀选项中更新了前缀长度定义。
- 在介绍中更新了 NBMA 链路的可用性，增加了对 3GPP RFCs 的考虑。
- 澄清负载平衡仅适用于路由器。
- 说明了当收到没有 Source Link-Layer Address Option (SLLAO)的 Router Solicitation 时，路由器如何行为。
- 澄清了针对 CurHopLimit 的不一致性检验仅适用于非 0 值。
- 为了便于理解重新编排了第 7-2-5 节，并描述了在 INCOMPLETE 状态下收到 NA 时的处理。
- 在第 7-2 节澄清了关于一旦收到没有 SLLAO 的消息时，节点应当如何行动。
- 增加了新的 IANA 节。
- 增加了各方面的撰稿人。

致谢

The authors of RFC 2461 would like to acknowledge the contributions of the IPV6 working group and, in particular, (in alphabetical order) Ran Atkinson, Jim Bound, Scott Bradner, Alex Conta, Stephen Deering, Richard Draves, Francis Dupont, Robert Elz, Robert Gilligan, Robert Hinden, Tatuya Jinmei, Allison Mankin, Dan McDonald, Charles Perkins, Matt Thomas, and Susan Thomson.

The editor of this document (Hesham Soliman) would like to thank the IPV6 working group for the numerous contributions to this revision --in particular (in alphabetical order), Greg Daley, Elwyn Davies, Ralph Droms, Brian Haberman, Bob Hinden, Tatuya Jinmei, Pekka Savola, Fred Templin, and Christian Vogt.

撰写人通讯录
Thomas Narten
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709-2195
USA
Phone: +1 919 254 7798
EMail: narten@us.ibm.com

Erik Nordmark
Sun Microsystems, Inc.
17 Network Circle
Menlo Park, CA 94025
USA
Phone: +1 650 786 2921
Fax: +1 650 786 5896
EMail: erik.nordmark@sun.com

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine
Madison Heights, Michigan 48071
USA
EMail: william.allen.simpson@gmail.com

Hesham Soliman
Elevate Technologies
EMail: hesham@elevatemobile.com

版权声明
Copyright (C) The IETF Trust (2007).
This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.
This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

知识产权

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.