

中华人民共和国通信行业标准

YD/T 2168-2010

IPv6 技术要求 ——IPv6 反向邻居发现协议

Technique requirement of IPv6: Extensions to IPv6 neighbor
discovery for inverse discovery specification

(IETF RFC 3122: 2001,
Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification, NEQ)

2010-12-29 发布

2011-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 缩略语.....1

4 反向邻居发现消息.....1

 4.1 反向邻居发现请求消息.....1

 4.2 反向邻居发现通告消息.....2

5 反向邻居发现协议选项格式.....3

6 反向邻居发现协议操作.....5

 6.1 发送方节点处理.....5

 6.2 接收节点处理.....5

 6.3 消息确认.....5

7 安全问题.....6

前 言

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. YD/T 1341-2005 IPv6 基本协议——IPv6 协议 (IETF RFC2460:1998, MOD)
2. YD/T 1915-2009 IPv6 技术要求——移动 IPv6 快速切换
3. YD/T 2168-2010 IPv6 技术要求——IPv6 反向邻居发现协议 (IETF RFC3122:2001, NEQ)
4. YD/T 2169-2010 IPv6 技术要求——IPv6 路径最大传输单元发现协议 (IETF RFC1981:1996, NEQ)
5. YD/T 2170-2010 IPv6 技术要求——IPv6 路由器重编号协议 (IETF RFC2984:2000, NEQ)
6. IPv6 技术要求——IPv6 动态主机配置协议
7. IPv6 技术要求——支持计算机移动部分
8. YD/T 1442-2006 IPv6 网络技术要求——地址、过渡及服务质量
9. YD/T 1343-2005 IPv6 邻居发现协议——基于 IPv6 的邻居发现协议 (IETF RFC2461:1998, MOD)
10. IPv6 邻居发现安全性技术要求
11. YD/T 1344-2005 IPv6 地址结构协议——IPv6 无状态地址自动配置
12. YD/T 1612-2007 IPv4 网络向 IPv6 网络过渡中的互联互通技术要求
13. YD/T 2029-2009 基于软线技术的互联网 IPv6 过渡技术框架
14. YD/T 1635-2007 IPv6 网络技术要求——面向网络地址翻译 (NAT) 用户的 IPv6 隧道技术
15. YD/T 1656-2007 采用边界网关协议多协议扩展 (BGP-MP) 的基于 IPv6 骨干网的 IPv4 网络互联 (4 over 6) 技术要求

本标准对应于 IETF RFC3122 (2001 年英文版)《IPv6 反向邻居发现协议》。本标准与 IETF RFC3122 (2001 年英文版)的一致性程度为非等效。主要差异如下：

- 根据 GB/T1 系列要求和汉语习惯进行了结构和格式的修改；
- 本标准删除了 IETF RFC3122 (2001) 中有关帧中继技术的附录 A 以及相关参考引用文件；
- 本标准的第 4 章、第 5 章、第 6 章、第 7 章分别与 IETF RFC3122 (2001) 的第 2 章、第 3 章、第 4 章、第 5 章保持一致。

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：工业和信息化部电信研究院、华为技术有限公司、杭州华三通信技术有限公司。

本标准主要起草人：毕立波、卜 哲、陈国义、万晓兰。

IPv6 技术要求——IPv6 反向邻居发现协议

1 范围

本标准规定了 IPv6 反向邻居发现 (IND) 协议，主要包括 IPv6 反向邻居发现协议的消息、选项的格式以及协议的具体执行过程。

本标准适用于支持 IPv6 协议的网络设备。

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。

YD/T 1343-2005	IPv6 邻居发现协议——基于 IPv6 的邻居发现协议 (IETF RFC2461:1998, MOD)
IETF RFC2401 (1998)	IP 的安全架构
IETF RFC2402 (1998)	IP 验证头
IETF RFC2406 (1998)	IP 封装安全协议

3 缩略语

下列缩略语适用于本标准。

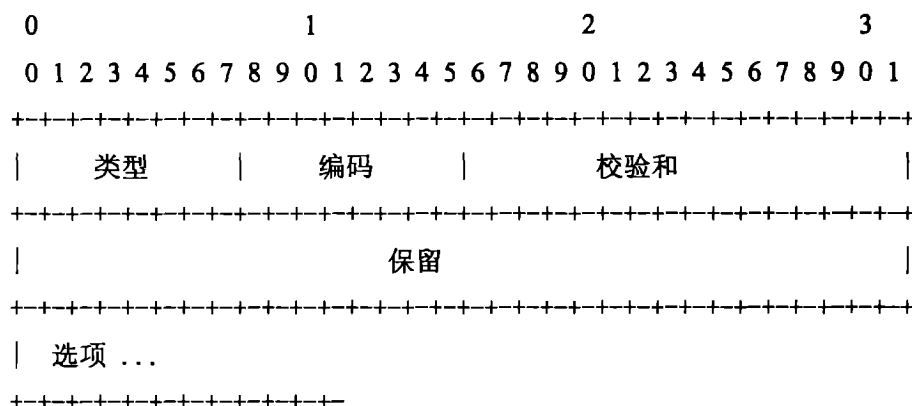
ICMP	Internet Control Message Protocol	Internet 控制消息协议
IND	Inverse Neighbor Discovery	反向邻居发现
IP	Internet protocol	互联网协议
IPv6	Internet protocol version 6	互联网协议第 6 版
MTU	Maximum Transmission Unit	最大传输单元
ND	Neighbor Discovery	邻居发现协议

4 反向邻居发现消息

反向邻居发现消息包括下面的两个消息。

4.1 反向邻居发现请求消息

一个节点发送一个反向邻居发现请求消息，以请求与目标节点链路层地址相对应的 IPv6 地址，同时也把本地节点的链路层地址提供给目标节点。因为目标节点的 IPv6 地址未知，所以反向邻居发现请求消息通过全节点组播地址方式被发送到 IPv6 网络的所有节点上。但从链路层上看，反向邻居发现请求是直接发送给目标节点的，因为该目标节点的链路层地址已知。



a) IP 头字段的规定

- 1) 源地址：发送这个消息的接口的IPv6地址；
- 2) 目的地址：IPv6全节点的组播地址，具体地址是FF02::1；
- 3) 跳数限制：255；
- 4) 认证头：如果发送、接收端之间存在IP认证头的安全关联，发送端应包含这个头字段。

b) ICMPv6 头字段的规定

- 1) 类型：141；
- 2) 编码：0；
- 3) 校验和：ICMP校验和；
- 4) 保留：没有使用这个字段，发送方应把它初始化为0，接收方应忽略它。

c) 应具备的选项

发送节点应在请求消息中发送下述选项：

- 1) 源链路层地址：发送者的链路层地址；
- 2) 目标链路层地址：目标节点的链路层地址。

d) 其他有效选项的规定

发送节点可以选择性地在请求消息中增加下面的选项：

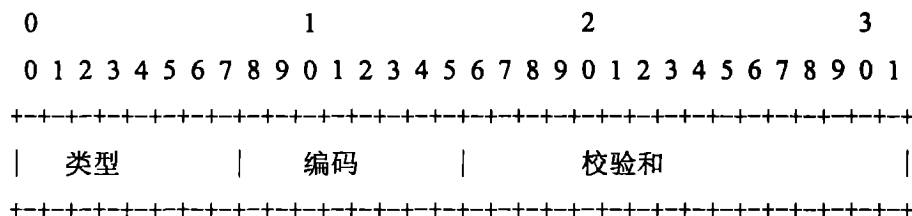
- 1) 源地址列表：由源链路层地址所标识的接口的一个或者多个IPv6地址的列表（在第5章中定义了这个选项）；

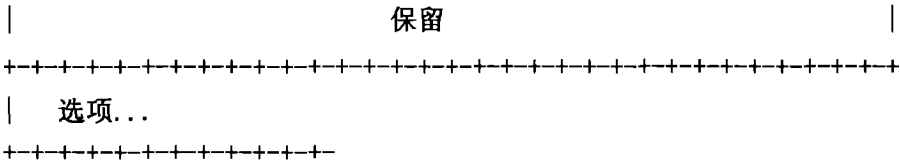
- 2) MTU：这条链路配置的MTU。

本协议的未來版本可能增加其他的选项类型。接收方应忽略它们不能识别的任何选项并且继续处理该消息。

4.2 反向邻居发现通告消息

一个节点发送反向邻居发现通告消息来应答反向邻居发现请求消息。





- a) IP 头字段的规定
- 1) 源地址：发送通告消息的接口的地址；
 - 2) 目的地址：发送反向发现邻居请求的源地址；
 - 3) 跳数限制：255；
 - 4) 认证头：如果发送、接收端之间存在IP认证头的安全关联，发送端应包含这个头字段。

- b) ICMPv6 头字段的规定
- 1) 类型：142；
 - 2) 编码：0；
 - 3) 校验和：ICMP校验和；
 - 4) 保留：32bit保留字段，发送方应把它初始化为0，接收方应忽略它；

c) 应具备选项的规定

发送方应在通告消息中发送下面的选项：

- 1) 源链路层地址：发送方的链路层地址；
- 2) 目标链路层地址：目标节点的链路层地址，即通告消息的发送方链路层地址；
- 3) 目标地址列表：目的链路层地址所对应接口的一个或多个IPv6地址，该目的链路层地址是触发通告消息的请求消息所请求的链路层地址（在第5节中定义了这个选项）；

d) 其他有效的选项

发送接点可以选择在通告消息中增加下面的选项：

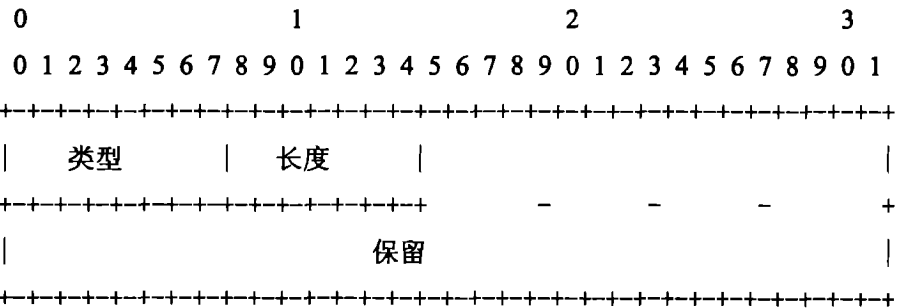
MTU：为这条链路配置的MTU。

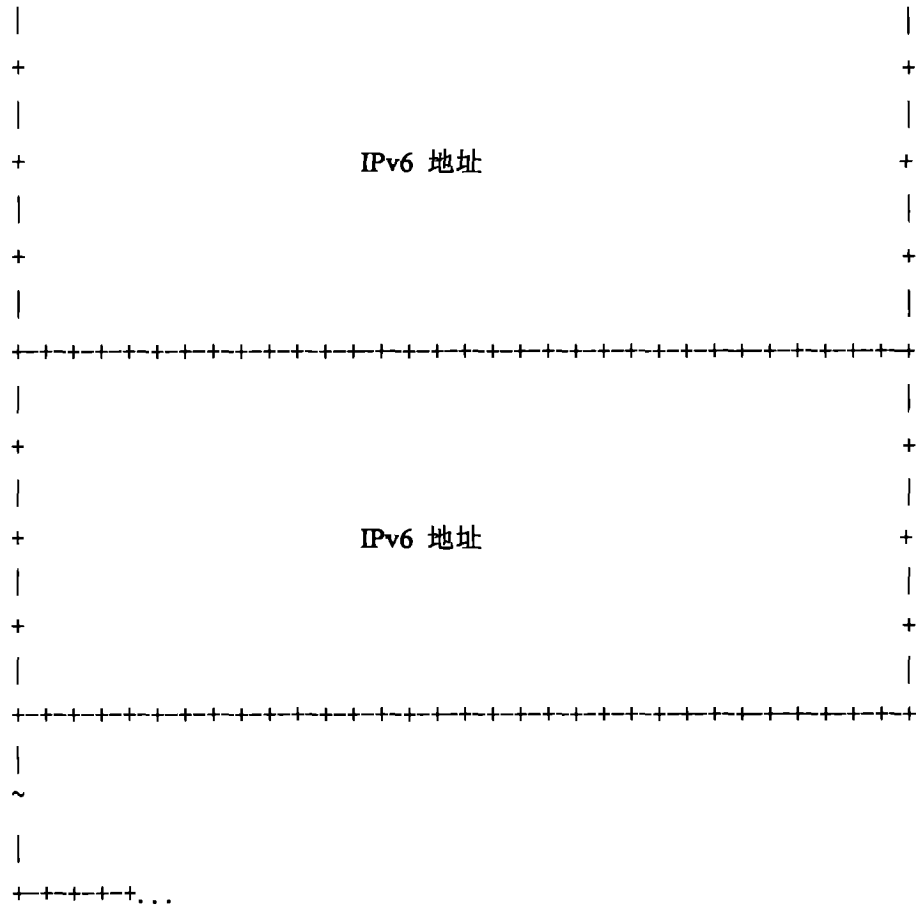
这个协议的将来版本可以增加其他的选项类型，接收方端应忽略它无法识别的选项并且不能因此终止处理该消息。

5 反向邻居发现协议选项格式

反向邻居发现消息中不仅可以包括 IPv6 邻居发现协议定义的选项，而且也包括反向邻居发现协议定义的特定选项：源地址列表以及目标地址列表。

源地址列表和目标地址列表选项是具有下面字段的 TLV 选项（类型、长度、可变长度字段），YD/T 1343-2005 的 6.6 节规定了 TLV 选项）：





IPv6 反向邻居发现协议规定选项的字段如下：

a) 类型：9 表示源地址列表，10 表示目标地址列表，具体数值可以从分配给 IPv6 邻居发现协议使用的数值集合中选取；

b) 长度：选项的长度（包括 TLV 字段），8 字节为一个单位。最短的长度值为 3，表示了一个 IPv6 地址的长度；

c) 预留字段：没有使用这个字段。发送方应把它初始化为 0，接收方应忽略它；

d) IPv6 地址：接口的一个或者多个 IPv6 地址。

源地址列表是由源链路层地址所标识的接口的一系列 IPv6 地址。

目标地址列表是由目标链路层地址所标识的接口的一系列 IPv6 地址。

列表中地址“ n ”的数量基于选项的长度进行计算： $n = (\text{长度} - 1) / 2$ (长度是 8 字节组的数量)。

源地址列表应对应于一个 IND 请求消息。因此如果一个接口的所有 IPv6 地址都不适合一个消息，则选项就不能包含一个完整的列表。节点应该信赖包含完整的 IPv6 地址列表的 IND 通告消息。

目标地址列表应该是一系列由目标链路层地址所标识接口的 IPv6 地址。如果一条 IND 通告消息中不包含目的地址列表，那么这条 IND 通告消息后的通告消息应该包含有目标链路地址所标识接口的 IPv6 地址列表，其他字段应该相同。

注：IND 机制的范围限制在 IPv6 地址发现，即提供地址映射信息。因此，它与节点如何使用通告的 IPv6 地址无关，而且 IND 机制中的地址列表应该兼容各种类型的源、目的 IPv6 地址。比如应能兼容手工配置、自动配置的地址，以及临时、单播、组播的 IPv6 地址。此外 IND 实现中的地址列表中一定不能包含重复的 IPv6 地址。

6 反向邻居发现协议操作

反向邻居发现协议的操作基本上和邻居发现协议一样：一个目标 IP 地址的请求者在接口上发送请求消息，目标节点应答一个包含请求信息的通告消息。通过反向邻居发现协议学习到的信息以及和接口相关 IPv6 地址可能存储在邻居发现缓存中。

6.1 发送方节点处理

一个请求节点按照规定的格式形成一个反向邻居发现协议请求消息，进行特定的链路层封装并且直接发送到目标节点。虽然目的 IP 地址是所有节点的组播地址，但是只把消息发送到目的节点上。反向邻居发现协议报文中关键字段是源 IP 地址、源链路层地址、目标链路层地址以及 MTU，可以为连接设置最优的 MTU 值。

在等待应答的时候，发送方应该根据重发超时机制在所预置时间的计时器过期后再次发送 IND 请求消息，即使没有到达目的节点流量的情况下，也应该执行重发。

如果发送了邻居发现协议规定的最大数量的请求消息后，仍然没有收到 IND 通告，那么反向地址解析失败。如果需要由上层协议发送请求，那么底层发送模块应通过某种机制将错误通告给上层（如从呼叫过程中返回一个数值）。

6.2 接收节点处理

6.2.1 处理反向邻居请求消息

对于每个 IND 请求，接收节点应该根据对应的链路层源、目标地址以及来自 IND 请求消息的 IPv6 源地址来构建正确的 IND 通告消息进行应答。

如果一个节点利用从 IND 消息学习到的信息来更新邻居发现缓存，接收到 IND 请求消息的节点应该把发送节点的 IPv6 地址与链路层地址进行关联，即将接收到的请求消息中的源 IP 地址以及源链路层地址添加到邻居发现缓存中，从而可以在 ND 请求中使用。

因为接口可能具有多个 IPv6 地址，因此应答 IND 请求的节点应该在 IND 通告消息中的目标地址列表项中包含一个或者多个 IPv6 地址，这些 IPv6 地址对应由请求消息中目标链路层地址字段标识的接口。这个列表中的 IPv6 地址不能重复。

6.2.2 处理反向邻居通告消息

如果一个节点将 IND 消息中学习到的信息更新邻居发现缓存，接收到 IND 通告消息的节点应该把应答节点的 IPv6 地址/链路层地址进行关联，即把来自 IND 通告消息中目标地址列表中的 IPv6 地址以及源链路层地址更新到邻居发现缓存中，从而可能用于 ND 通告。

6.3 消息确认

通过如下方式来确认有效的反向邻居发现消息。

6.3.1 反向邻居发现请求的确认

反向邻居请求消息应满足下列所有有效性检查条件，否则将被节点丢弃：

- a) IP 跳数限制字段的值为 255，即消息不能被路由器转发过去；
- b) 如果消息包含一个 IP 认证头，那么消息认证应为正确；
- c) ICMP 校验和有效；
- d) ICMP 编码为 0；
- e) ICMP 长度（从 IP 长度得到）不低于 24 字节；

- f) 目标链路层地址是一个必选项而且应出现；
- g) 源链路层地址是一个必选项而且应出现；
- h) 所含选项的长度大于 0。

应忽略预留字段的内容以及任何无法识别选项。未来向后兼容的协议可能会定义预留字段的内容或者增加新的选项，后向兼容的变化可能会采用不同的编码值。

应忽略任何反向邻居发现协议中没有使用的邻居发现定义的相关内容，并且不影响节点正常处理报文。非必选项中，只有 MTU 选项可能出现。

通过有效性检查的反向邻居请求才是有效 IND 请求消息。

6.3.2 反向邻居发现通告的验证

反向邻居通告消息应满足下列所有有效性检查条件，否则将被节点丢弃：

- a) IP 跳数限制字段的值为 255，即消息不能被路由器转发过；
- b) 如果消息包含一个 IP 认证头，那么消息认证正确；
- c) ICMP 校验和有效；
- d) ICMP 编码为 0；
- e) ICMP 长度（来自 IP 长度）不小于 48 个字节；
- f) 有源链路层地址选项；
- g) 有目标链路层地址选项；
- h) 有目标地址列表选项；
- i) 目标地址列表选项的长度至少为 3；
- j) 所含的选项长度都大于 0。

应忽略预留字段的内容以及任何无法识别选项。未来向后兼容的协议可能会定义预留字段的内容或者增加新的选项，后向兼容的变化可能会采用不同的编码值。

应忽略任何反向邻居发现协议中没有使用的邻居发现协议定义的相关内容，并且不影响节点正常处理报文。非必选项中，只有 MTU 选项可能出现。

通过有效性检查的反向邻居通告才是有效的 IND 通告消息。

7 安全问题

与在帧中继网络这样的点到点虚电路上应用反向邻居发现协议情况相似，IND 消息不太容易受到这条点到点连接上节点所发起攻击的影响，如广播连接的情况。

和邻居发现协议一样，在缺少认证的情况下，反向邻居发现协议通过忽略来自非连接路径节点的 IND 消息来降低暴露给非连接路径上节点的威胁。由于路由器要降低由它们转发分组的跳数限制，因此反向邻居发现协议要求验证所有接收到消息报文中的跳数限制字段是否都是最大长度值 255，这样能够保证消息来自于一个邻居节点。

反向邻居发现协议消息交互可以通过 IP 认证头来进行认证。如果源、目的节点之间存在使用 IP 认证的安全关联，那么节点在发送反向邻居发现协议消息时应包含认证头。可以通过手动方式或一些密钥管理协议的操作来生成安全关联。

应验证在反向邻居发现协议消息中的认证头，没有验证通过的消息不应丢弃。

在帧中继网络中，为了避免 IP 安全认证验证失效，接收节点在完成 IP 安全处理以后，应去处理帧

中继特别规定的包含 DLCI 格式的源链路层地址选项的 ND 请求消息。

系统管理者可以配置一个节点来忽略任何没有通过认证头或者封装安全载荷验证的反向邻居发现消息。支持反向邻居发现协议的交换机缺省处理未认证的消息。

IETF RFC2401、IETF RFC2402 以及 IETF RFC2406 描述了有关机密性问题。
