组织：中国互动出版网（http://www.china-pub.com/）
RFC 文档中文翻译计划（http://www.china-pub.com/compters/emook/aboutemook.htm）
E-mail：ouyang@china-pub.com
译者：许少君（china_dubing　　sjxu general@263.net）
译文发布时间：2002-11-26

Network Working Group　　S. Thomson
Request for Comments: 2462　　Bellcore
Obsoletes: 1971　　T. Narten
Category: Standards Track　　IBM
December 1998

IPV6无状态地址自动配置

(IPv6 Stateless Address Autoconfiguration)

关于本文的说明

这个文档说明了一个为 Internet通讯的 Internet标准跟踪协议，而且它的改进希望得到讨论和建议。请参考 "Internet 正式协议标准 " (标准 1) 的当前版本来得到本协议的标准化陈述．本文的分发不受限制．

版权声明

摘要

本文档详细说明了在 IPv6 下，一台主机决定如何自动配置它的接口的具体步骤。自动配置的步骤包括了创建一个本地地址，验证它在链路上的唯一性，决定哪些信息是自动配置的(地址，其它信息，或两者兼有)。对于地址而言，还必须决定它是通过无状态(自动配置)机制，还是通过状态(自动配置)机制来获取，或两者兼有。本文档定义了通过无状态自动配置获取本地链路地址、本地站点地址和全球(唯一)地址的过程，以及地址冲突检测过程。状态自动配置协议的细节不属于本文档的范围。

目录

1.简介：

本文档详细说明了在 IPv6 下，一台主机决定如何自动配置它的接口的具体步骤。自动配置的步骤包括了创建一个本地地址，验证它在链路上的唯一性，决定哪些信息是自动配置的(地址，其它信息，或两者兼有)。对于地址而言，还必须决定它是通过无状态(自动配置)机制，还是通过状态(自动配置)机制来获取，或两者兼有。本文档定义了通过无状态自动配置获取本地链路地址、本地站点地址和全球(唯一)地址的过程，以及地址冲突检测过程。有状态自动配置协议的细节不属于本文档的范围。

IPv6 同时定义了无状态与状态自动配置机制。无状态自动配置不需要对主机进行任何手动的配置，对路由器的配置也是最少的(如果有的话)，也不需要任何额外的服务器。无状态机制可以使主机把本地信息同路由器发出的通告消息结合来产生一个地址。路由器通告一个前缀，这个前缀用以标识关联到链路的子网，而主机则产生一个“ 接口标识符 ”，这个“ 接口标识符 ”在本子网上唯一地标识了该接口。主机地址就是这两部分的结合。如果没有路由器，主机只能产生本地链路地址。但是本地链路地址已经足以让主机与本地链路上的其它节点通信了。

在状态自动配置模型里，主机通过一台(DHCP)服务器获取它的接口地址和其它配置参数信息。(DHCP)服务器负责维护地址数据库，以跟踪哪些地址已经被指派给哪些主机了。状态自动配置允许主机从(DHCP)服务器获取地址和其它配置信息。无状态自动配置和状态自动配置互补不足。譬如，一台主机可以用无状态自动配置来配置它的地址，然后再通过状态自动配置来获取其它的配置信息。IPv6 下的状态自动配置还没有形成 RFC，是将来的一个工作主题，DHCPv6。

无状态自动配置用在不太关心主机的确切地址的站点上，只须地址唯一且可以被正确路由即可。而状态自动配置则用在需要比较严格的控制地址分配的站点。无状态和状态自动配置可以同时运用。站点管理员通过设置路由器通告消息里的相关字段，可以指定使用何种自动配置类型。(详见[DISCOVERY])

一个接口租用 IPv6 地址一段固定长度(可能是无限长)的时间。每个地址都有一个相关联的生命周期显示它将被绑定到某个接口上多久。当生命周期到了，这个地址的绑定将失效，这时这个地址可能被重新指派给网络上其它的接口。为了适当地处理地址绑定的过期，一个地址被指派到某个接口上时，经历了两个阶段。最初，一个地址是“ 优先 ”(preferred)的，意味着它可以被用于任何通信而不受限制。然后，一个地址可以变成“ 否决 ”(deprecated)的，以预期它的当前绑定即将失效。处于被“ 否决 ”状态时，使用这个地址是不被提倡的，虽然并不严格禁止。新的通讯(例如打开一个新的 TCP 连接)应该尽可能使用“ 优先 ”的地址。一个被否决的地址只应该被用于那些无法在不造成服务中断的情况下转换到另一个地址，同时又不希望中断服务的应用程序上。

为确保所有被配置的地址在给定的链路上是唯一的，节点在把地址指派给接口之前，都要运行地址冲突检测算法。所有的地址分配都执行地址冲突检测算法，不管它是无状态自动配置还是状态自动配置分配的。

本文档说明的自动配置过程只应用于主机而非路由器。路由器必须通过其它手段进行配置，因为主机自动配置使用了路由器通告的信息。不过，本文档描述的机制也可以用于路由器产生本地链路地址。另外，在所有的地址被分配到接口之前,路由器还必须通过本文档中描述的地址冲突检测过程。

第二节提供了本文档中使用到的一些定义和术语。第三节描述了当前自动配置过程的设计目标。第四节是协议的概览。第五节则详细描述了协议的细节。

2 术语

IP – 网际协议版本 6。术语 IPv4 只用于上下文不能清楚分辨的地方以避免歧义。

节点(Node) – 实现 IP 的一个设备。

路由器(router) – 一个转发 IP 包的节点，这些 IP 包的目的地不是该节点。

主机(host) – 任何不是路由器的节点。

上层(upper layer) – 紧挨着 IP 的上一个协议层。例如传输协议 TCP 和 UDP，控制协议 ICMP，路由协议 OSPF，以及被“隧道封装”的网际或更低层协议如 IPX，AppleTalk,或 IP 协议本身。

链路(link) – 一个通讯设备或媒体，通过它，节点能在链路层上相互通讯，链路层是紧挨着 IP 的下一个协议层。例如以太网，PPP 连接，X.25，帧中断，或 ATM 网络，以网际(或更高)的协议层“隧道”，譬如通过 IPv4 或 IPv6 本身的隧道。

接口(interface) – 一个节点连接到链路的部件。

包(packet) – 一个 IP 头紧跟着净荷(有效负载)。

地址(address) – 一个用于接口的 IP 层的标识符

单播地址(unicast address) – 单个接口的一个标识符。被送到一个单播地址的包被传送到被这个地址所标识的接口上。

组播地址(multicast address) – 一组接口(通常属于不同的节点)的标识符。一个被送到该地址的包，会被传送到被该地址所标识的所有接口上。

任意点播地址(anycast address) –一组接口(通常属于不同的节点)的标识符。一个被送到该地址的包，将被送到被该地址所标识的一个接口上(最“近”的一个接口，“近”是根据具体路由协议的距离测量来算的)。详见[ADDR-ARCH]

被请求节点的多播地址(solicited-node multicast address) – 被发送邻居请求消息的一个多播地址，在[DISCOVERY]里有计算该地址的具体算法。

链路层地址(link-layer address) – 接口的链路层标识符。例如以太网的 IEEE802 地址和 ISDN 链路的 E.164 地址。

本地链路地址(link-local address) – 一个工作仅在本地链路范围内有效的地址(address)，可以用来与连接在同一链路上的邻居节点通讯。所有的接口都有一个本地链路的单播地址。

本地站点地址(site-local address) – 一个有效范围限于本地站点的地址。

全球地址(global address) – 一个无范围限制的地址(全球有效)。

通讯(communication) – 节点间要求过程中每个节点的地址保持不变的包交换，例如 TCP 连接或 UDP 请求-应答。

试探地址(tentative address) – 一个还未指派给接口，正被验证(在本链路上)唯一性的地址。一般来说，不认为试探地址已经被指派给接口。接口若收到发往试探地址的包，会丢弃它，除非这个包是地址冲突检测的邻居发现包，用于验证该试探地址的唯一性的。

优先地址(preferred address) – 指派给接口的一个地址，可以不受限制地被上层协议使用。优先地址可以被用于从接口上发送(或接收)的包的源(或目的)地址。

否决地址(deprecated address) – 指派给接口的一个地址，不提倡使用它，但也没有严格禁止它的使用。一个否决地址不应该被用于新的通讯的源地址，但发往或发自否决地址的的包还是如常处理。否决地址在切换到优先地址有困难的上层(协议)活动中可能被继续用做源地址(例如一个已存在的 TCP 连接)。

有效地址(valid address) – 一个优先或否决地址。一个有效地址可以以包的源或目的地址出现，网际路由系统应该将发往有效地址的包传送给它们想到达的接收方。

无效地址(invalid address) – 没被指派给任何接口的地址。一个有效地址当它的有效生命周期终止时，它就变成一个无效地址。无效地址不应该做为包的源或目的地址出现。当它做为包的源地址时，接收方无法回应，当做为目的地址时，路由器无法转发。

优先生命周期(preferred lifetime) – 一个有效地址做为优先地址的时间，即直到被否决的时间。当该时间到了，地址变成否决地址。

有效生命周期(valid lifetime) – 地址有效的时间，即直到地址失效的时间。该时间必须大于或等于优先生命周期。该时间到了，地址就变成无效。

接口标识符(interface identifier) – 用于接口的，由具体链路决定的标识符，它在每个链路上应该是唯一的。无状态地址自动配置组合接口标识符和前缀以形成一个地址。从地址自动配置的角度来看，一个接口标识符是一个已知长度的位串。接口标识符的确切长度以及它如何产生有另外单独的特定链路类型文档来定义。这些文档涉及了在特定链路类型上进行 IP 传输的各种问题(例如[IPv6-ETHER])。

在许多情况下，接口标识符和接口的链路层地址是一样的。

3. 设计目标

无状态自动配置的设计有如下几个需要达到的目标：

- 每台机器在联入网络时不需要任何的手动配置。因此，需要一种机制能让主机为它的每个接口获取或创建具有唯一性的地址。地址自动配置的前提假设是每个接口都能提供一个唯一的标识符(即一个“ 接口标识符 ”)。最简单的情况，一个接口标识符就是接口的链路层地址。一个接口标识符和一个前缀就可以组成一个地址。
- 由一组连接到同一链路上的机器组成的小型站点不需要有状态服务器(DHCP)或路由器就可以相互通讯。
- 一个由多个网络和路由器组成的大型站点应该可以不需要状态地址配置服务器。为了产生一个本地站点地址或全球地址，主机必须知道一个“ 前缀 ”，这个前缀标识了该主机所连接到的子网。路由器周期性地产生路由通告，通告里有一些选项列出了链路上活跃(可用)的前缀。
- 地址配置必须提供机制，以方便地对站点机器的进行重编号。例如，当一个站点换了一家新的网络服务提供商时，也许就需要对它的所有节点重新编号。重编号通过租赁地址给接口和多个地址指派给同一接口即可实现。租赁周期提供了淡出机制，站点可以逐渐地淡出旧的(子网)前缀。多个地址分配给同一接口提供了一个过渡时期，以使新地址和正在淡出的旧地址可以同时工作。
- 系统管理员要能指定是用无状态自动配置，还是状态自动配置，或者两者同时使用。路由通告里有相应的标志字段以指定主机用何种机制(进行配置)。

4. 协议概览

本小节提供了一个接口自动配置所需典型步骤的概览。只有在一个具有组播能力的链路上自动配置能生效。在一个具有组播能力的接口被启用时，自动配置开始执行，例如当一个系统启动。节点(包括主机和路由)的自动配置过程先为接口产生了一个本地链路地址。将接口标识符追加在“ 众所周知 ”的本地链路前缀就形成了一个本地链路地址。

但这个本地链路地址现在还只是一个“ 试探 ”地址，在把它指派给接口之前，节点还要

先验证该地址是否已经被本地链路上的其它节点所使用。具体一点说，它会发送一个邻居请求消息包，以这个“试探”地址为目标地址。如果另一个节点已经在使用这个地址，它会回应一个邻居通告表示如此。如果另一个节点也在尝试使用一样的地址，它也会发送一样的邻居请求包，即以试探地址为包的目标地址。请求被(重新)发送的次数以及连续发送请求之间的时间间隔和具体链路有关，也可以由系统管理设定。

如果一个节点检测到它的本地链路试探地址已经被其它节点所用，自动配置就会停止，这时需要手动对接口进行配置。为了简化这种情况的处理，必须提供这样的可能：管理员可以提供一个备选的接口标识符，当地址冲突时，自动配置机制会选用这个行备选(可能唯一)的接口标识符(以形成地址)。否则，就要手动配置本地链路地址和其它(本地站点或全球)地址。

节点如果确定它的本地链路试探地址是唯一的(没被其它节点所用)，它就把它指派给接口。这时，这个节点就具备了在 IP 层上与邻居节点进行连接的能力。接下来要讲的自动配置步骤就只适用于主机，路由器的(自动)配置不在本文档的范围之内。

下一个阶段，自动配置涉及获取路由通告，或确定没有路由器存在。如果路由器存在，它们会发送路由通告，指定主机要用何种自动配置。如果没有路由器，就应该启用状态自动配置。

路由器周期性地发送路由通告，但是两个连续的路由通告之间的时延通常不是一台执行自动配置的主机所愿望等待的。为了尽快得到路由通告，主机发送一个或多个路由请求给“所有路由”组播群。路由通告包含了两个标志字段，表示主机应执行何种状态配置。“管理地址配置”(managed address configuration)字段表示主机是否要用状态自动配置获取地址。“其它状态配置”(other stateful configuration)字段还表示主机是否使用状态自动配置获取其它信息(除地址外)。

路由通告也包含零或多个的前缀信息选项，用于无状态地址自动配置产生本地站点和全球地址。值得注意的是，路由通告中的无状态和状态地址自动配置字段是被分别单独处理的，也就是主机可以同时使用无状态和状态地址自动配置。一个前缀信息的选项字段，“自治地址配置标志”(autonomous address-configuration flag)，表示这个前缀信息选项是否用于无状态自动配置。如果是，该选项里的其它包含了子网前缀及生命周期值被用于形成地址，生命周期值显示了由这个前缀所创建的地址保持优先和有效的时间。

路由器是周期性地产生路由通告的，主机会持续地收到新的通告。主机以如上所述的方式处理每个通告所包含的信息，添加和刷新从以前的通告里获取的信息。

安全起见，所有地址在被指派给接口前都应该先验证它们的唯一性。对于无状态自动配置中地址的创建来说，地址的唯一性基本上取决于地址中由接口标识符形成的那部分。所以，

如果一个节点已经验证了它本地链路地址的唯一性，其余也是从一样的接口标识符创建的地址就不需要再进行验证了。相反的，如果所有的地址是手动配置或通过状态地址自动配置获取的地址，就需要分别进行验证唯一性。为适应有些觉得地址冲突检测不必要的站点，地址冲突检测也可以被禁用，通过对一个每接口配置字段的设置来实现。

为加速自动配置过程，主机一边产生本地链路地址(并验证它的唯一性)，一边等待路由通告。因为路由器对路由请求的回应可能会有几秒的延迟，这样如果串行处理这两个步骤，则完成自动配置的总时间加起来会明显地比较长。

4.1 站点重编号

地址租赁提供了一种机制，使被指派给接口的地址可以在一定时间内失效，这方便了站点重编号。目前上层协议如 TCP 还不支持在打开的连接上改变端点地址。如果一个端点地址变成无效，则在该地址上打开的连接马上中断，所有到该地址的通讯也都会失败。即使用 UDP 做传输协议的应用程序，通常在一个包交换过程中地址也不能变动。

将有效地址分为优先和否决地址两种，可以让上层知道一个有效地址很快要变成无效，再继续使用这个地址进行通讯，若在通讯结束前有效生命周期终止，通讯将会失败。为了避免这种情况，高层协议应使用优先地址(假设该地址的作用范围足够)以便在通讯过程中，地址仍然有效的可能性比较大。适当的前缀生命周期由系统管理员来设定，以尽量减小重编号时通讯失败带来的影响。地址处于否决状态的时间应该足够长，以使大部分(如果没办法做到全部的话)通讯能够在旧地址失效前顺利转换到新的地址上来。

给定一个目标地址或可能其它的限制，IP 层应该能够提供一种方法使上层(包括应用程序)能选择最为适当的源地址。在开始通讯之前，应用程序可以自己选定源地址或不指定地址，让 IP 上层使用 IP 层提供的机制来替它选择一个适当的地址。

具体的地址选择规则不在本文档的讨论范围中。

5. 协议规范详述

自动配置是基于每个有组播功能的接口执行的。对多穴主机，自动配置是独立地在每个接口上进行的。自动配置主要是用于主机，但有两个例外。路由器也应该按下面将要列出的步骤来产生本地链路地址。另外路由器在把地址指派给一个接口前，都要进行地址冲突检测。

5.1 节点配置变量

一个节点必须允许系统管理对每个接口设置如下变量，这些变量都是与自动配置相关的：

DupAddrDetectTransmits

在对一个试探地址进行地址冲突检测时，持续发送的邻居请求消息的数目。0 表示不对试探地址进行地址冲突检测，1 表示只发一个邻居请求消息。

默认值：1，但可能不同的链路类型会有不一样的值，这可由其它关于在特定链路类型上进行 IP 传输的文档所指定。(例如[IPv6-ETHER])

自动配置还假设另一个变量 RetransTimer 是存在的，这个变量在[DISCOVERY]里有详细定义。RetransTimer 指定了进行地址冲突检测时，连续发送两个邻居请求传输之间的延时，以及发送完最后一个邻居请求后，节点等待多久才结束地址冲突检测过程。

5.2 自动配置相关变量

主机保持(maintain)了一些和自动配置相关的数据结构与标志。下面，我们提出几个概念上的变量，并指出它们在自动配置过程中是如何被运用的。具体的变量仅供示范，具体实现不一定要有这些变量，只要客观上的行为和下面描述的一致就可以。

本地链路地址的形成和地址冲突检测之外，路由器是如何(自动)配置它们的接口不在本文档的讨论范围之内。

主机基于每接口，保持(maintain)了下列一些变量：

ManagedFlag　拷贝自最近一次收到的路由通告里的 M 标志字段。这个标志变量表示主机是否使用状态自动配置机制。初始值为 FALSE(即使用无状态自动配置)。

OtherConfigFlag　拷贝自最近一次收到的路由通告里的 O 标志字段。这个标志变量表示是否使用状态自动配置机制来获取除地址外的其它信息。初始值为 FALSE。

另外，当 ManagedFlag 为 TRUE 时，OtherConfigFlag 的值则相应地应该为 TRUE。因为主机只通过状态地址自动配置获取地址，而不接收其它信息，这是一种有效的配置。

主机同时也保持了一张地址与对应生命周期的列表。列表里包括了自动配置和手动配置的所有地址。

5.3 本地链路地址的创建

当一个接口启用时，节点就为它生成一个本地链路地址。一个接口的启用可能发生于下列一些事件之后：

- 接口在系统启动时被初始化
- 接口在暂时性地失效或被系统暂时禁用后，重新初始化
- 接口刚接入到链路上
- 接口在出于管理目的禁用后又重新启用

一个本地链路地址由众所周知的本地链路前缀 FE80::0 和接口标识符组合而成。假如接口标识任为 N 个比特位长，则，用它来替代本地链路前缀的最右边的 N 个 0 比特位。如果接口标识符长于 118 比特位，自动配置失败，需要手动配置。典型的接口标识符是 64 比特位长，是基于 EUI-64 标识符的。EUI-64 标识符的描述详见[ADDR-ARCH]。

一个本地链路地址的优先和有效生命周期是无限的，它永不超时。

5.4 地址冲突检测

如果一个接口的 DupAddrDetectTransmits 变量大于 0，在指派单播地址之前要执行地址冲突检测。不管是从状态还是无状态自动配置，或是从手动配置获得的单播地址，都要进行地址冲突检测，除了以下几种情况：

- 任意点播地址不需要进行地址冲突检测
- 每个单播地址都应该测试其唯一性。但是，当使用无状态地址自动配置时，如果我们假设子网前缀的分配正确的话，那么地址的唯一性只取决于接口标识符(就是说，接口的所有地址是从同一个标识符产生而来的，它们的唯一性是一样的，要么全部都不冲突，要么全部冲突)。因此，对于由同一接口标识符形成的一组地址而言，只要检查本地链路地址的唯一性就足够了。在这种情况下，本地链路地址必须检测其唯一性，一旦它的唯一性得到验证，具体实现时可以选择忽略从同一接口标识符派生而来的其它地址的唯一性检测。

地址冲突检测使用了如下描述的邻居请求与通告消息。如果检测过程中发现地址冲突，

地址就不能被指派给接口。如果这个地址是从一个接口标识符派生出来的，就必须指派一个新的标识符给这个接口，否则这个接口所有的地址必须手动配置。值得注意的是，这个检测冲突的方法并不是完全可靠的，地址重复依然可能存在(例如，地址冲突检测的时候，链路被隔离成几段)。

一个未完成地址冲突检测过程的地址称为“试探”性的，直到检测过程的结束。一般而言，试探地址不被认为已经指派给接口。这意味着接口接收邻居请求和通告消息，这些消息里，目标地址就是试探地址，对这些消息包采取和其它正常(目标地址为接口地址之一)的包不一样的处理过程。其它送往试探地址(目的地址为试探地址)的包必须被无声无息地丢弃。

在指派地址前先进行地址冲突检测是为了避免同一时间内，多个不同的节点使用一样的地址。如果在一个节点在地址冲突检测的同时使用这个地址，而此时另一节点已经在使用这个地址，那执行地址冲突检测的这个节点将会错误地处理本来是送往另一个节点的通信数据，从而可能造成不良的后果，如重置一个已经打开的 TCP 连接。

接下来的小节描述了一个节点验证地址唯一性的具体测试。如果发送完 DupAddrDetectTransmits 次的邻居请求，又等待了 RetransTimer 毫秒，没有检测到地址有重复(冲突)，这个地址就被认为具有唯一性。这时就可以把地址指派给接口。

5.4.1 消息验证

节点必须悄悄地丢弃任何未通过有效性检查的邻居请求或通告消息(详见[DISCOVERY])。通过有效性检查的请求或通告消息被称为有效请求或有效通告。

5.4.2 发送邻居请求消息

一个接口在发送邻居请求前，接口必须加入“所有节点”(all-nodes)组播地址和被请求节点的多播地址(solicited-node multicast address)。前者确保节点能接收到其它节点发来的邻居通告(表明地址已被使用，有冲突)；后者确保两个都在尝试使用同一个地址(也即同时在验证这个地址的唯一性)的节点可以检测到对方的存在。

检查地址时，节点发送了 DupAddrDetectTransmits 个邻居请求，每个发送之间间隔了 RetransTimer 毫秒。请求的目标地址就设置成被检查的地址，其 IP 源地址设成未指定，IP 目的地址设成目标地址的被请求节点的多播地址(solicited-node multicast address)。

如果邻居请求是接口(重新)初始化后发送的第一个包，应在一个延迟之后才发送，这个延迟是在 0 到 MAX_RTR_SOLICITATION_DELAY 之间的一个随机延迟(详见[DISCOVERY])。这是出于减轻拥塞的目的，特别是当停电又来电后，许多在同一链路上的

节点同时启动时。这样做也有助于避免由多于一个节点尝试请求使用同一个地址时带来的竞争情况(race condition)。为提高地址冲突检测算法的健壮性，接口在延迟发送邻居请求时，仍然必须接收并处理发送给“所有节点”组播地址或试探地址的被请求节点的多播地址(solicited-node multicast address of the tentative address)的数据报。

5.4.3 接收邻居请求消息

当接口接收到一个有效的邻居请求消息时，节点的行为取决于请求消息里的目标地址是否是试探地址。如果目标地址不是试探地址(即它是已经指派给接收接口的地址)，请求的处理依照[DISCOVERY]里的描述。如果目标地址是试探地址，源地址是一个单播地址，那这个请求的发送者在对目标地址进行地址解析，这样的请求忽略不处理。否则，按如下描述进行处理。在任何情况下，节点都不应该回复一个试探地址的邻居请求。

如果邻居请求的源地址未指定，表明这个请求是从一个正在进行地址冲突检测的节点发出来的。如果这个请求是从另一个节点发出的，这个试探地址就是重复的(有冲突)，不应该被使用。如果这个请求是从节点自向发出的(因为节点回返组播包)，那并不表示有地址冲突。

实现者要注意：很多接口允许上层协议有选择地启用和禁用组播包的回返，从而使得地址冲突检测工作不正常。附录 A 有进一步的阐述。

下面的测试列出了什么情形下试探地址是不唯一的：

- 如果在发送某个试探地址的邻居请求前就收到这个试探地址的邻居请求，则这个地址就是重复(冲突)的。这种情形一般发生在当两个节点同时在运行地址冲突检测时，但发送请求的时间不一样(例如在发送请求前选择的随机延迟不一样)。
- 如果收到邻居请求的实际数目超过了根据回返定义应该收到的数目(例如接口不允许回返包，但却收到了一个或多个的请求)，试探地址是重复(冲突)的。这种情形一般发生在当两个节点同时在运行地址冲突检测时，而且发送请求的时间几乎一样。

5.4.4 接收邻居通告消息

接口收到一个有效的邻居通告消息时，节点的行为取决于目标地址是试探地址或是本接口的单播或任意点地址之一。如果目标地址是已经指派给接口的地址，请求的处理根据[DISCOVERY]里的描述进行。如果目标地址是试探地址，那这个试探地址就是重复的(因为本接口已经在使用了，其它接口不应使用，否则有冲突)。

5.4.5 地址冲突检测失败

一个试探地址如果经过检测，确定是重复的，它就不应该指派给接口，节点必须记录一个系统管理错误。如果这个地址是一个由接口标识符形成的本地链路地址，这个接口应该被禁用。

5.5 全球和本地站点地址的创建

全球和本地站点地址由一定长度的前缀和接口标识符形成的。前缀从路由通告里的前缀信息选项里获取。在本小节详述的全球和本地站点地址，以及其它的参数配置，都必须是本地可配置的。但是下面描述的过程应当默认启用：

5.5.1 请求路由通告

路由通告周期性地被送往“ 所有节点 ”组播地址。主机可以发送路由请求，以更快地获取一个路由通告。(详见[DISCOVERY])

5.5.2 无路由通告的情形

如果一个链路上没有路由器，主机必须尝试用状态自动配置去获取地址和其它配置信息。具体实现可以提供禁用状态自动配置启动的选项，但默认值应该是可以启动(状态自动配置)的。从自动配置的角度来看，如果在发送了一些路由请求后，还是没有收到任何路由通告，就认为链路上没有路由器。

5.5.3 路由通告处理

当收到一个有效的路由通告时，主机把通告里的 M 标志位拷到 ManagedFlag 变量里。如果 ManagedFlag 变量从 FALSE 变为 TRUE 时，主机还没有运行状态自动配置协议，主机应启用状态地址自动配置协议以请求地址信息及其它信息。如果是从 TRUE 变为 FALSE，则主机继续运行状态地址自动配置，也就是说这个变化没带来任何影响。如果 ManagedFlag 值没有变化就无需特别的动作。特别要说的是，如果之前的通告已经使主机运行了状态地址自动配置，那主机就不能(因此次通告)再次调用状态自动配置。

通告的 O 标志位也是类似地处理方式。主机把 O 标志位拷到 OtherConfigFlag 变量里。如果 OtherConfigFlag 的值从 FLASE 变为 TRUE，主机应调用状态自动配置以请求配置信息

(不包括地址信息，若 ManagedFlag 为 FALSE)。如果是从 TRUE 变为 FALSE，则主机继续运行状态地址自动配置协议，即没有改变。如果值不变，则无需特别的动作。特别要说的是，如果之前的通告已经使主机运行了状态地址自动配置，那主机就不能(因此次通告)再次调用状态自动配置。

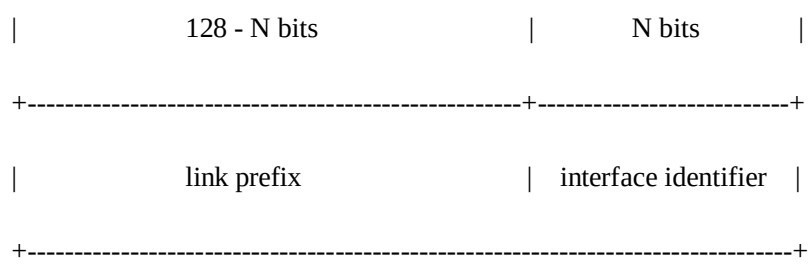
对于路由通告里的每一个前缀信息选项：

a) 如果自治标志没有设置就忽略这个前缀信息选项。

b) 如果是本地链路前缀，也忽略这个前缀信息选项。

c) 如果优先生命周期比有效生命周期来得大，忽略这个前缀信息选项。这种情况节点可以记录一个系统管理错误到日志里。

d) 如果前缀和本地地址列表里的都不一样，有效生命周期不为 0，则产生一个地址，并把它加入到本地地址列表里。地址的产生如下所示:



如果前缀长度和接口标识符长度加起来不等于 128 位的话，这个前缀信息选项必须被忽略。具体实现时，可以记录一个系统管理错误到日志里。系统管理员有责任确保路由通告里的前缀长度与本地链路类型决定的接口标识符长度是协调的(即加起来刚好 128 位)。典型的接口标识符是基于 EUI-64 标识符的，64 比特位长。

如果地址成功形成，主机把它加入到指派给接口的地址列表中，从前缀信息选项里获取并初始化它的优先和有效生命周期。

e) 如果通告里的前缀和主机自动配置的地址(通过无状态或状态自动配置获取的地址)的列表里的某个地址匹配，具体的动作取决于通告里的有效生命周期值，以及和这个已经被自动配置的地址关联的生命周期(下面讨论中我们称这个值为 StoredLifetime)：

1) 如果接收到的通告里的生命周期大于两个小时或比 StoredLifetime 大，就更新相应地址的生命周期。

2) 如果 StoredLifetime 小于或等于两个小时，且接收到的通告里的生命周期小于或等于 StoredLifetime，则忽略它，除非这个路由通告是通过认证的(例如，通过 IPSec[RFC2402])。如果路由通告是通过认证的，就要把 StoredLifetime 设成能通告里的生命周期值。

3) 否则，把 StoredLifetime 的值设成两个小时。

上面的规则解决了拒绝服务攻击，这种攻击通过发送一些伪造的通告，通告里前缀信息带有一个很小的有效生命周期。没有上面的规则，一个未认证过的通告带着伪造的存有极短生命周期值的前缀信息，可以使所有节点的地址提前过期。上面的规则确保了合法的通告(周期性发送的)可以在短的生命周期生效前将其“撤消”。

5.5.4 地址生命周期终止

当优先生命周期终止里，优先地址变为否决地址。一个否决地址应该可以在一个已存在的通讯里用做源地址。如果有一个可选的非否决的地址可以用，而且这个地址又拥有足够的作用范围的话，否决地址不应该用在新建立的通讯里。IP 和上层协议(例如 TCP，UDP)必须继续接收目标为否决地址的数据报，因为否决地址仍然还是接口的一个有效地址。具体的实现可以防止任何新的通讯使用否决地址，但系统管理必须有能力禁用这个功能，这个功能也必须是默认被禁用的。

当有效生命周期终止时，地址(和它与接口的关联)变成无效。一个无效的地址不能被用于流出的通讯的源地址，也不能被接收方识别成一个目标地址。

5.6 配置一致性

主机可能同时从无状态和状态自动配置获取地址信息，因为无状态和状态自动配置可以同时启用。同样的，其它的参数信息如最大传输单元(MTU)大小和跳极限(hop limit)也可能同时从路由通告和状态自动配置协议获得。如果同一参数信息由多个不同的渠道获得，这个参数的值必须是一致的。然而，这个值如果不一致，也不认为是致命的错误。主机综合接收所有从无状态和状态协议中获取的所有信息。如果从不同渠道获得的信息不一致，最新得到的值将优先于更早前得到的值。

6. 安全考虑

无状态地址自动配置允许一台主机接入网络，配置地址，开始和其它节点通讯。而这一切甚至都无需注册或经本地站点认证。这方便了未经授权的用户接入和使用网络，但同时也给因特网的体系结构带来内在的隐患。物理接入网络的节点可以产生一个地址(用一些特别的技术)来提供连接性。

地址冲突检测的使用为拒绝服务攻击提供了可能性。任意节点都可以回复一个试探地址的邻居请求，导致其它节点认为这个地址是重复的，进而放弃使用这个地址。这样的攻击类似于涉及邻居发现消息欺骗的攻击，可以通过要求邻居发现消息包认证来解决。

7. 参考文献

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

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

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

[RFC1112] Deering, S., "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989.

[ADDR-ARCH] Hinden, R. and S. Deering, "Internet Protocol Version (IPv6) Addressing Architecture", RFC 2373, July 1998

[DHCPv6] Bound, J. and C. Perkins, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", Work in Progress.

[DISCOVERY] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

8. 致谢与作者的联系地址

Acknowledgements

The authors would like to thank the members of both the IPNG and ADDRCONF working groups for their input. In particular, thanks to Jim Bound, Steve Deering, Richard Draves, and Erik Nordmark. Thanks also goes to John Gilmore for alerting the WG of the "0 Lifetime Prefix Advertisement" denial of service attack vulnerability; this document incorporates changes that address this vulnerability.

AUTHORS' ADDRESSES

Susan Thomson
Bellcore
445 South Street
Morristown, NJ 07960
USA

Phone: +1 201-829-4514
EMail: set@thumper.bellcore.com

Thomas Narten
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709-2195
USA

Phone: +1 919 254 7798
EMail: narten@raleigh.ibm.com

9. 附录 A: 回返抑制 &地址冲突检测

决定一个接收到的一个组播请求是回返给发送者的或确实是从其它节点发送过来的，是与具体实现有关的。当两个连接到同一链路上的接口碰巧有一样的标识符和链路层地址，麻烦就出现了：它们会几乎同时发送内容一模一样的包(例如做为地址冲突检测消息一部分的某个试探地址的邻居请求)。如果接收方接收到这样的包，它无法只是简单地通过比较包的内容(内容是一样的)来判断包是回返的或是从其它节点发过来的。在这种特殊情况下，没有必要确切地知道包是回返的还是其它节点发送过来的。如果节点发到比它自身发送的还要多的请求，那这个请求所对应的试探地址是重复的。但是，情况并不是那么简单直接的。

IPv4 组播规范[RFC1112]建议接口要提供上层协议禁止一些包的本地传送，这些包是发送到自己也是成员之一的组播群的包。一些应用程序知道在同一主机上不会有组播群的其它成员，就抑制回返，防止主机不得不接收(并丢弃)它们自己发出去的包。一个简单直接的实

现是在硬件层上(如果硬件支持的话)禁用回返，由软件回返数据包(如果被请求)。在硬件本身抑制回返的接口上，运行地址冲突检测的节点只是简单地计算接收到某个试探地址的邻居请求，和预料的数目比较。如果不相符，试探地址就是重复的。

然而，有些硬件无法抑制回返，这些情况下，通过软件过滤不需要的回返，一种可能的方法是丢弃任何链路层源地址和接收接口(链路层)地址一样的包。不幸的是，这种判定标准会导致所有从使用相同链路层地址的其它节点发来的包被丢弃。地址冲突检测在以这种方式过滤接收包的接口上会失败：

o 如果执行地址冲突检测的节点丢弃它链路层源地址和接收接口链路层地址一样的包，那它也会丢弃从使用相同链路层源地址的其它节点上发过来的包，包括邻居通告和邻居请求消息。而这两种消息可是地址冲突检测正常工作所必须的。在执行地址冲突检测时，暂时地禁用回返的软件抑制，可以避免这个问题。

o 如果已经在使用一个特定 ip 的节点丢弃了链路层源地址与本地接收接口链路层地址一样的包，那它也会丢弃与地址冲突检测相关的，由其它使用相同链路层地址的节点发出的邻居请求消息。这样的后果是地址冲突检测会失败，其它节点会配置一个不唯一的地址。这样的情况只有当回返的软件抑制被永远禁用才可能避免，因为一般不可能知道什么时候其它节点要执行地址冲突检测。

因此，在两个接口使用一样的链路层地址的情况下，为了正确执行地址冲突检测，具体实现必须好好了解一下接口的组播回返规定。接口也不能只因为包的链路层源地址和接收接口的链路层源地址一样就丢弃它。

10. 附录 B 自 RFC1971以来的改变

o 改变文档，用“ 接口标识符 ”替代“ 接口令牌 ”，以和其它的 IPv6 文档保持一致。

o 澄清了否决地址的定义，以阐明继续使用否决地址发送和接收(数据包)是没问题的。

o 改写了小节 5.4，使之更明晰(没有实质的变动)。

o 在小节 5.5.3 里，对路由通告的处理添加了一些规则，以解决当带有极短的生命周期的前缀信息被通告时所潜在的拒绝服务攻击。

o 澄清了小节 5.5.4 里的措辞，以阐明所有上层协议必须处理(即发送和接收)送往否决地址的数据报。

11. 完整的版权声明

11. Full Copyright Statement