doi:10.3969/j.issn.1000-436x.2014.z1.027

非对称的 IPv6 地址翻译技术的实现与分析

张宇烜[1]，闫岫[1]，徐希炜[2]
(1. 北京邮电大学 信息网络中心，北京 100876；2. 潍坊职业学院，山东 潍坊 261041)

摘 要：非对称的 IPv6 地址翻译方法可以对任意长度前缀的 IPv6 地址进行透明地翻译。通过使用 Netfilter 框架实现非对称 IPv6 地址翻译技术，对该翻译方法做了定性和定量的分析。在局域网，通过对比不同环境中地址翻译的效率和局域网中可容纳的主机数量规模，给出了在实际环境中运用此技术的相关建议。

关键词：IPv6；网络地址转换；IPv6 网络前缀翻译
中图分类号：TP393.2 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0141-05

Implementation and analysis of PANET

ZHANG Yu-xuan[1], YAN Shen[1], XU Xi-wei[2]
(1.Network Information Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Weifang Vocational College, Weifang 261041, China)

Abstract: Partial-state asymmetric NAT (PANAT) could translate any prefixes of IPv6 address seamlessly. With the implementation of PANAT method by using Netfilter framework, it does both the quantitative research and qualitative research for PANET. Some suggestions are given for using PANET in the real environment though comparison of the translation efficiency and the hosts scales.

Key words: IPv6; network address translation; IPv6 network prefix translation

1 引言

全球互联网正在经历从 IPv4 至 IPv6 的过渡，IPv4 私有地址到 IPv4 公有地址的地址转换技术（NAT44）曾被用以应对 IP 地址短缺的问题。虽然 IPv6 提供了足够的地址空间，解决了 IPv4 地址不足的问题。但是 IPv6 地址转换技术仍然拥有技术应用的价值。现阶段，IPv6 地址空间的分配和使用仍然受制于运营商。但是 IPv6 地址在满足可用性的同时，还需要具有健壮性和易用性。在这个背景下，地址翻译技术（NAT）有天然的优势。RFC5902 中指出，地址翻译技术可以防止重编码，有效解决私有网络的多宿主问题，同时还有安全保障[1]。通过与应用层网关(ALG)、防火墙等技术的结合，NAT 技术可以提供隐藏网络拓扑、追踪可疑流量等功能。

IETF 提出 RFC6296[2]作为 IPv6 地址翻译的解决方案。RFC6296 描述了一种无状态的 IPv6 地址前缀翻译方法。该方案在不同 IPv6 前缀之间互相转换，以达到无状态透明的 IPv6 地址前缀转换，保证了 IPv6 地址的 1:1 翻译。然而，RFC6296 对于地址前缀长度有要求与限制，只能实现前缀等长的 IPv6 地址之间的转换，不能对任意 IPv6 地址执行翻译，并且 RFC6296 翻译方案不能为网络提供相关的安全保障机制。

这种背景下，文献[3]提出了一种半状态非对称的任意 IPv6 前缀地址翻译方案(PANAT)，用以实现一种在不同前缀长度的 IPv6 地址之间互相转换的地址翻译方案。相比于 RFC6296，PANAT 通过减少翻译过程中的存储记录，压缩存储表项，实现了任意前缀长度的 IPv6 地址空间的翻译和转换。同

收稿日期：2014-10-14
基金项目：国防科技重大专项——移动互联网 IPv6 应用示范基金资助项目(2012ZX03002016-002)
Foundation Item: The National Science and Technology Majar Project “Mobile Internet IPv6 Application Trial (FDD)” (2012ZX03002016-002)

时，PANAT 避免了重新计算伪头，保证在转换过程中转换地址对传输层和应用层透明。通过算法设计，PANAT 可以兼容 RFC62697。本文对 PANAT 方法进行了具体的实现，在真实环境中，对于常用前缀进行了随机地址翻译实验，评估了在不同条件下 PANAT 部署对于 IPv6 地址空间的要求，给出了不同前缀长度在 PANAT 翻译方法中可使用的主机数量上限。

2 非对称地址翻译方案的实现

PANAT 方案基于 Linux 内核中的 Netfilter[4]组件开发，可完成任意前缀长度的 IPv6 地址的转换与翻译。当安装完成后，PANAT 作为内核模块，在 Linux 内核网络栈中运行。PANAT 方案是基于 HOOK 模型来处理数据分组的。

HOOK 的数据分组处理模型属于 Netfilter 架构。Netfilter 在网络协议栈的关键位置定义了 5 个 HOOK 处理点，利用 HOOK 处理模型，开发者可以快速开发自定义的网络处理模块。PANAT 方案通过 HOOK 模型，在数据分组被路由前后，完成 IPv6 地址的检查和翻译。PANAT 的整体工作流程如图 1 所示。

在载入翻译模块前，可以通过手动配置对转换前缀进行修改。当模块载入 Linux 内核时，通过对前缀变量的初始化和系统函数注册，翻译模块拥有了相关的处理数据分组的权限。模块可以对网卡上的所有数据分组进行过滤和翻译操作。

当数据分组从内网进入转换网关时，翻译模块首先查找数据库，当发现流量目的地址为内网地址时，数据分组正常路由，翻译模块不执行翻译算法。当目的地址为外网地址时，翻译模块对目的地址进行地址翻译，将翻译特征记录数据库后进行正常路由。当用 IPv6 数据分组从外部网络进入转换网关时，翻译模块检查数据分组的目的地址。通过查找数据库，当且仅当存在唯一特征值时，翻译模块恢复相关的原始地址信息，恢复目的地址，完成地址翻译。当报文从内网向外网发送，如果数据库查找失败，则意味着出现重复翻译地址的现象，模块发出相关地址重复消息，通知内网主机修改自身的网络地址。同时模块丢弃数据分组，向管理员报告错误。当报文从外网向内网发送时，如果数据库查找失败，模块直接丢弃数据分组，向管理员报告错误。

此外，还利用 PANAT 方案中校验和不变的特

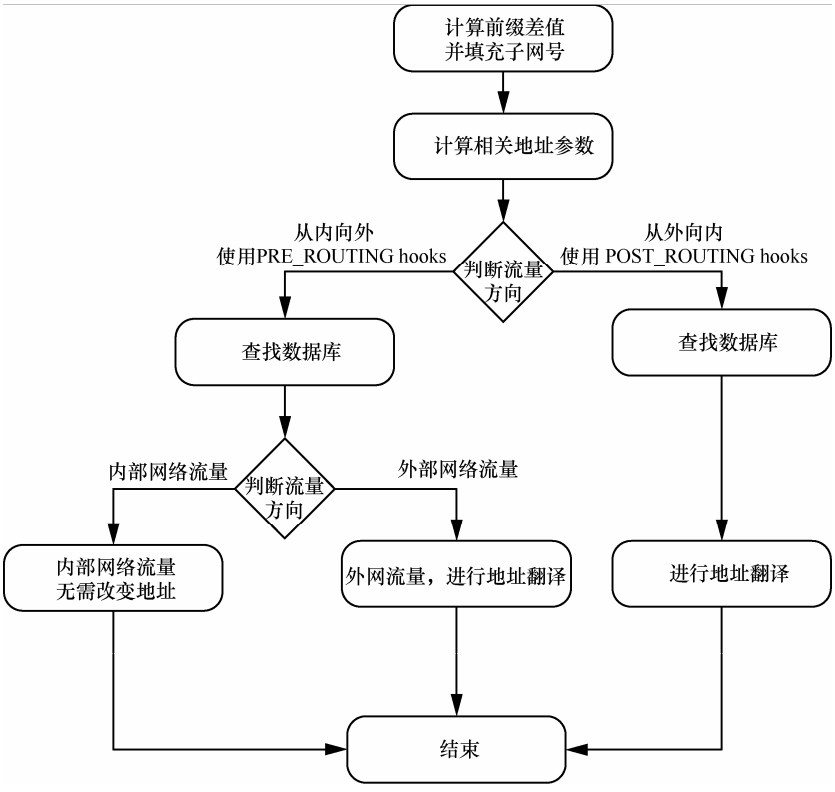


图 1 翻译模块的工作流程

性，实现了 ALG，为此方案增加安全功能。翻译模块能够对特定的网络端口号过滤。ALG 的实现使模块在执行地址翻译功能的同时对数据进行过滤和控制，保障了网络安全。应用层安全网关实现，如下所示。

ALG 数据分组处理流程
输入：数据报文
输出：路由指令
1) 开始
2)　　解析数据分组,取得端口号
3)　　Switch(端口号)：
4)　　case 知名端口号：
5)　　根据事先配置进行路由，输出路由
6)　　case 自定义端口号：
7)　　根据管理员规则，输出路由。
　　当发现可疑流量，进行端口和地址识别，报告管理员
8)　　default：
9)　　根据黑名单机制或白名单机制进行数据分组过滤
10) 结束

因为在翻译过程需要消耗大量的系统资源，对出口网关造成较大的运行负荷。因此翻译模块做了进一步的优化处理。例如，消除翻译过程中的重复计算，利用红黑树等数据结构实现了自定义的键值数据库。通过这些优化，整个地址转换程序可以更高效地完成地址的转化和匹配，最大程度保证了程序的性能。

3　测试与分析

通过对 PANAT 模块的测试，对 PANAT 方案进行了定性和定量的分析。测试环境使用 CentOS 系统，系统版本是 6.4。测试拓扑如图 2 所示。

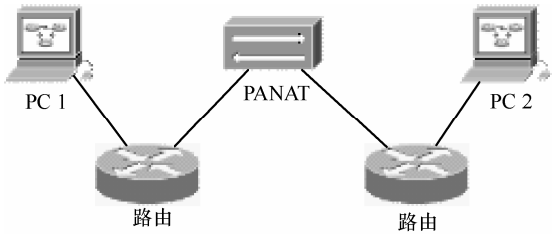


图 2　测试环境拓扑

通过对某一前缀子网空间内的所有地址进行翻译，发现 PANAT 翻译方案中存在一个重复周期。假设使用 fe80::/96 作为内网 IPv6 前缀，使用 2001:db8::/112 作为外网 IPv6 前缀。通过翻译模块，每一个内网地址均生成一个对应的新的外网 IPv6 地址。从 fe80::0 到 fe80::f:ffff 的非对称地址翻译结果如图 3 所示。横轴标识了内网地址空间，纵轴标识了被翻译后的地址。

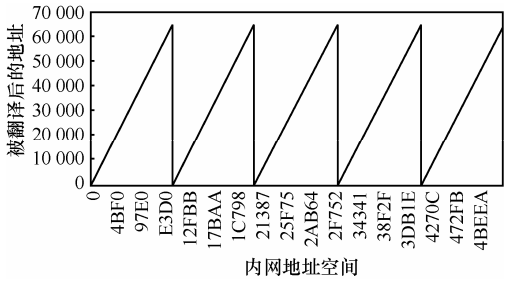


图 3　PANAT 翻译周期

从图 3 中可以发现，PANAT 翻译方案存在一个重复的周期。在一个重复周期内，翻译地址空间内没有重复地址翻译的现象。在不同重复周期间，不同内网地址有可能会被翻译为同一个外网地址，造成地址翻译失败。经过测算，图 3 中的翻译重复周期是 65 535，重复周期的数目与外网地址空间的大小相等。因此，可以推断在 PANAT 翻译方案中，存在一个重复周期，周期的大小与前缀长度较长的 IPv6 地址空间的大小相同，重复周期的大小与地址翻译方案中的可用地址数目大小相等。若非对称翻译方案中 2 个前缀长度的差值为 N，则重复周期的个数为 2^N。

根据上面的实验数据，随机选取了一些有代表性的前缀长度，使用非对称地址翻译方案，通过对比翻译前后的地址，对随机状态下地址空间中可用地址数目进行了测试。统计结果如表 1 所示。

从表 1 中可以发现，在随机状态下，实际可用的地址空间数目远小于理论值。究其原因，一次 PANAT 翻译过程中存在一个重复周期。在重复周期等于或大于可用地址空间数目的情况下，非连续的随机地址从一个大 IPv6 地址空间被映射到一个小的 IPv6 地址空间。由于地址空间大小不同，地址数目不同，可能会出现地址翻译碰撞的现象。因此在 PANAT 方案中，随机状态下的地址冲突概率明显增大，实际可用地址空间大大减小，且可用地址的利用率随着地址空间的增大而减小。

表 1　随机状态下不同前缀长度下的可用地址数目

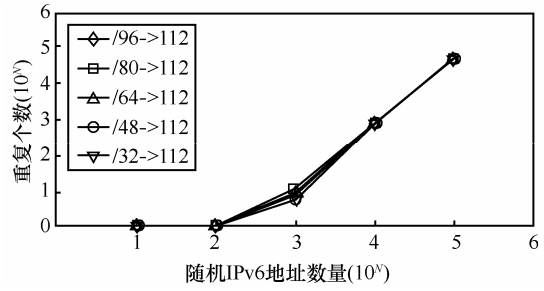
翻译后的前缀长度	翻译前的前缀长度	可用无重复地址个数
/112	/96	500
	/80	500
	/64	500
	/48	500
	/32	500
/96	/80	100 000
	/64	100 000
	/48	100 000
	/32	100 000
/80	/64	30 000 000
	/48	30 000 000
	/32	30 000 000
/64	/48	>100 000 000
	/32	>100 000 000
/48	/32	>100 000 000

图 4 显示了不同的内网地址被翻译到同一个外网前缀的重复地址数量的曲线。以图 4(a)为例，发现可用重复地址的数目呈线性增长，与图 3 中的地址增长规律保持一致。另一方面，从图 4 中可以看出，翻译地址的重复数目与翻译前的地址没有直接关系，翻译过程中的地址空间的实际可用地址数目取决于前缀长度较长的 IPv6 地址。最后，随着待翻译地址空间的增长，可用空间数目呈指数型增长。

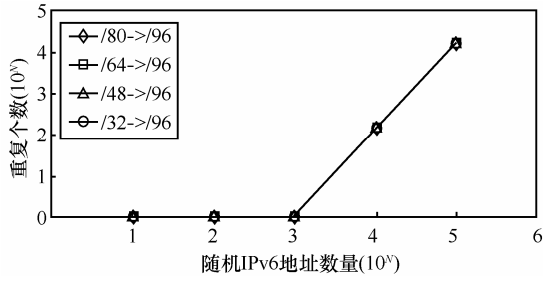
综上所述，实际部署 PANAT 的过程中，用户应注意以下两点。首先，在地址空间的选择上，应尽可能选择连续的地址空间，从而降低地址碰撞的次数。其次应尽可能使用较大地址空间以减少地址重复的数目。

4　结束语

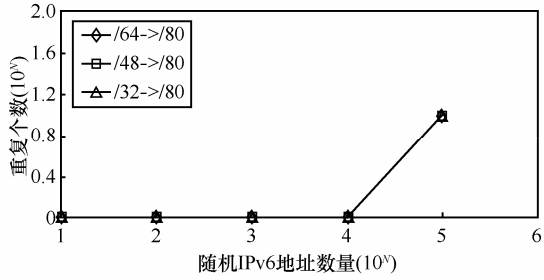
本文对 PANAT 进行了实现，评估了 PANAT 方



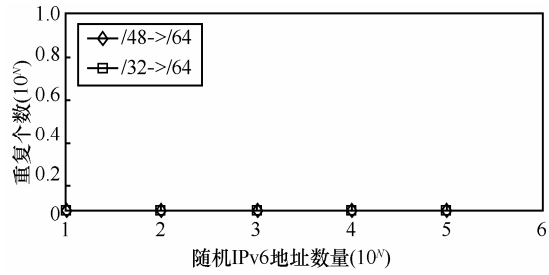
(a) /112 的翻译重复曲线



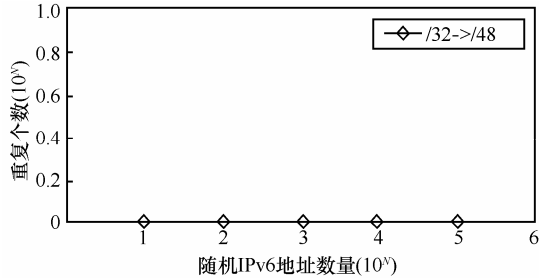
(b) /96 的翻译重复曲线



(c) /80 的翻译重复曲线



(d) /64 的翻译重复曲线



(e) /48 的翻译重复曲线

图 4　翻译重复曲线

案在翻译实施过程中重复地址的特性。实验表明，PANAT 方法在翻译过程中存在一个翻译地址的重复周期。在随机条件下，重复周期的出现使方案的实际可用地址空间大大减小。最后本文给出了在 PANAT 的实际部署过程中的相关建议。

对于今后的工作，通过继续完善 ALG 功能，使模块具有更好的安全特性，能够加强对流量的控制。同时，对于现有 PANAT 方案不能完全处理地址重复地址的问题，可以通过计算二次校验和与地址重复检测机制来进行进一步降低地址碰撞的概率。

参考文献：

[1] THALER D, ZIUHANG L, LEBOVITZ G. IAB Thoughts on IPv6 Network Address Translation[S]. IETF, RFC5092, 2010.

[2] WASSERMAN P S M, BAKER F. Cisco Systems, IPv6-to-IPv6 Network Prefix Translation[S]. IETF RFC 6296, 2011.

[3] YAN S, ZHAO Q, HUANG X H, *et al*. Partial-state asymmetric NAT: universal and asymmetric IPv6 address mapping[A]. The 15th Communication Technology (ICCT)[C]. 2013.

[4] ENGELHARDT J, BOULIANE N. Writing netfilter modules[EB/OL]. http://inai.de/documents/Netfilter_Modules.pdf, 2012.

作者简介：

张宇烜（1989-），男，甘肃兰州人，北京邮电大学硕士生，主要研究方向为下一代互联网络和 IPv6。

闫岫（1987-），男，北京人，北京邮电大学博士生，主要研究方向为分布式移动性管理。

徐希炜（1979），男，山东潍坊人，潍坊职业学院讲师，主要研究方向为计算机网络技术及应用。