第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·网络与通信· 文章编号：1000—3428(2008)17—0108—03 文献标识码：A 中图分类号：TP393.03

支持动态选路的NAT-PT机制

陆海洲，王振兴，程之年，耿楠楠
(解放军信息工程大学信息工程学院，郑州 450002)

摘 要：孤立的多个NAT-PT无法为会话提供较短的路径，NAT-PT发生故障会导致经过该NAT-PT的会话中断和IPv4地址的浪费。该文提出一种支持动态选路的NAT-PT机制，通过NAT-PT间的伪路由发布和信息共享，使多个NAT-PT协同工作，互为同步/友好NAT-PT，为报文提供动态选路支持，实现报文路径的优化和故障NAT-PT负载的实时迁移。

关键词：NAT-PT机制；拓扑局限性；动态选路；信息共享；伪路由

NAT-PT Mechanism Supporting Dynamic Routing

LU Hai-zhou, WANG Zhen-xing, CHENG Zhi-nian, GENG Nan-nan
(Information Engineering College, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 Multiple isolated Network Address Translation Protocol Translation(NAT-PT) can not offer shorter path for a session, and all sessions via one NAT-PT may be broken and the IPv4 addresses may be wasted when NAT-PT failing. A Dynamic Routing NAT-PT(DRN) mechanism is presented to coordinate multiple NAT-PT working. With the pseudo route information which is broadcasted by DRN and shared information among NAT-PTs, NAT-PT becomes synchronous/friendly NAT-PT each other and achieves dynamic routing. A more appropriate NAT-PT is chosen to make path length of a session shorter and the load of a failure NAT-PT can be moved to a working one automatically.

【Key words】 Network Address Translation Protocol Translation(NAT-PT) mechanism; topology limitation; dynamic routing; information sharing; pseudo-route

1 概述

NAT-PT[1](Network Address Translation Protocol Translation)是一种协议翻译机制，用来实现过渡时期纯IPv6网络和纯IPv4网络之间的通信。NAT-PT在网络边界进行网络地址转换和协议翻译，实现IPv6和IPv4之间的透明路由，无须对现有的网络设备和结构做改动，也不要求IPv4和IPv6主机做任何特殊配置，即可实现纯IPv6和纯IPv4之间的通信，大大降低了IPv6和IPv4共存与过渡的成本。目前主流路由器(如CISCO)均开始支持NAT-PT。但NAT-PT模型存在拓扑局限性，即限制会话的所有报文在选路时必须经过同一个NAT-PT，这会引起2个严重问题：(1)NAT-PT失效后将导致现有会话中断，即使存在多个NAT-PT，其他NAT-PT也无法实现功能替代，不能充分利用已有资源，闲置了宝贵的IPv4地址；(2)由于缺乏路由信息和相应的地址绑定信息，无法选择恰当的NAT-PT使会话路径较短。

通过深入研究，发现NAT-PT存在拓扑局限性的2个主要原因为：路由信息无法穿越IPv6/IPv4边界和NAT-PT存在信息封闭。IPv4和IPv6作为2个不同的IP层协议，其路由信息无法进行交互。即使双栈路由器之间在IPv4域中的路径比IPv6中的长，IPv4报文也只能通过IPv4网络到达目的地。NAT-PT虽然能够转换报文使其穿越网络边界，但是不处理任何路由协议信息。目前NAT-PT模型也没有考虑多个NAT-PT互通的问题，NAT-PT作为一个独立的翻译器发挥作用，相互间不交换信息，因此，经某个NAT-PT建立的会话无法通过其他NAT-PT进行转换。

随着IPv6和IPv4间通信量的增大，如果各个NAT-PT仍然独立工作，通信的选路性能将无法得到满足，因此，需要一种实现多个NAT-PT协同工作的机制。使用孤立的多个NAT-PT，即使在域名解析阶段采用NAT-PT轮询来保证成功解析域名并建立会话，依然无法避免NAT-PT失效时引起的会话中断，不能为会话选择较短路径。VAPTR系统[2]虽并联了多个NAT-PT，但只提高了单NAT-PT的性能，从IPv4和IPv6网络来看，VAPTR系统依然是单NAT-PT。NAT-PT簇[3]和DAPTC[4]利用DNS-ALG在多个NAT-PT上调度会话，解决了单NAT-PT存在的负载过重问题。但是会话建立后，其地址绑定信息只存在于一个NAT-PT中，NAT-PT间没有交互，退化为单NAT-PT。目前尚未见到关于NAT-PT动态路由研究的文献。

本文提出一种支持动态选路的NAT-PT机制——DRN(Dynamic Routing NAT-PT)，在多个NAT-PT间共享地址信息和发布伪路由，使多个NAT-PT协同工作。为每个NAT-PT提供至少2个同步NAT-PT，避免因NAT-PT失效引起的通信中断和资源浪费，实现故障NAT-PT负载的实时迁移，并发布友好NAT-PT的伪路由信息以协助报文动态选路，为穿越NAT-PT的报文选择较短的路径。

2 DRN机制

DRN用来解决多个NAT-PT协同工作的问题，每个NAT-PT可以有不同的实现，只要符合RFC2766规范，并实现与DRN间的接口，就可以通过DRN协调工作。

首先定义2个术语，其他基本术语见文献[1]。

(1)同步NAT-PT。对于2个NAT-PT：N_1和N_2，如果N_1

作者简介：陆海洲(1980－)，男，硕士，主研方向：网络互联，网络信息安全；王振兴，教授、博士、博士生导师；程之年、耿楠楠，硕士

收稿日期：2008-03-10 **E-mail：**luhk213@yahoo.com.cn

通告了 N_2 的伪路由，保存并同步更新 N_2 的地址状态和绑定信息，则称 N_1 为 N_2 的同步 NAT-PT。

(2)友好 NAT-PT。如果 N_1 仅通告关于 N_2 的伪路由，而不同步更新 N_2 的相关信息，并只在需要转换 N_2 的会话报文时才请求相应的信息，则称 N_1 为 N_2 的友好 NAT-PT。

N_1 是 N_2 的同步/友好 NAT-PT 并不代表 N_2 一定是 N_1 的同步/友好 NAT-PT，即两者不一定是对称的。

2.1 DRN 基本原理

DRN 环境如图 1 所示。NAT-PT$_1$ 和 NAT-PT$_2$ 分别连接 IPv6 和 IPv4 网络，为各自所连的网络实现透明路由，有各自的 DNS 服务器、IPv4 地址池、IPv6 前缀 PREFIX::/96 等。NS 为 NAT-PT 服务器，保存活跃 NAT-PT 的地址信息，并检测可达性。

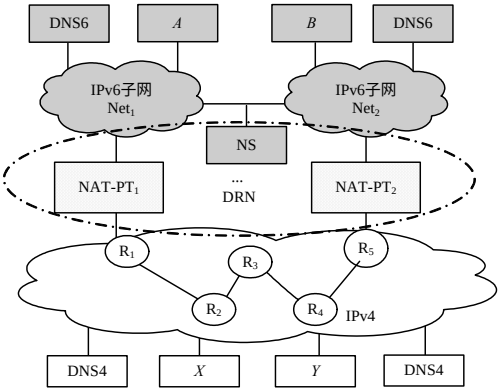

图 1 DRN 示意图

DRN 功能的实现基于以下 4 个条件：

(1)NAT-PT 间 IPv6 互通。考虑到发展趋势和 IPv6 所具有的优点，这里假定 NAT-PT 间通过 IPv6 相连。

(2)NAT-PT 发现。该机制使 NAT-PT 能够找到其他 NAT-PT，这是发布伪路由和共享信息的基础。

(3)伪路由发布。借鉴路由协议[5]将多个路由器连接起来并为报文动态选路的工作原理，DRN 使用伪路由将多个 NAT-PT 连接起来，将一种网络的路由信息转换为伪路由发布到另一种网络，实现跨网络的路径优化。

(4)信息共享。NAT-PT 在会话初始阶段为 IPv6 绑定 IPv4 地址时，需要知道地址状态信息，对经过的会话报文进行协议翻译时，需要知道该会话的地址绑定信息，信息共享使 NAT-PT 可以转换其他 NAT-PT 的报文。

2.2 NAT-PT 发现

NAT-PT 须手动配置 NS 的地址，启动后在 NS 中注册基本信息，然后获取其他 NAT-PT 的信息。NS 需要维护一个列表以保存活跃 NAT-PT 的信息，列表内容为(NAT-PT, IPv6 地址, IPv4 地址, 域名)。

每个活跃的 NAT-PT 在列表中都有一个表项，IPv6/IPv4 地址是 NAT-PT 在 2 种网络上接口的对应 IP 地址，当某个地址不存在或不可用时，使用域名进行查询。

2.3 伪路由发布

发布伪路由使报文可以选择较短的路径穿越 NAT-PT，到达目的节点。伪路由使得 IPv4 网络可以被 IPv6 节点视为 NAT-PT 间虚拟的 IPv6 路径，反之亦然。

NAT-PT 获得其他节点的地址信息后，使用报文交换计算出跳数(距离)信息。请求对方发送一个报文，数据内容填上发送时设置的初始跳数，收到该报文后，用报文内容里的数值 H_s 减去 IP 头中的跳数 H_n 得到经过的跳数 H_{ij}，然后利用关系公式确立关系：

$$R_{ij}=\begin{cases} S & h_{ij}=\min\{H\} \\ S & Num(\min\{H\})<2,\ =\min\{H-\min\{H\}\} \\ F & \text{otherwise} \end{cases} \tag{1}$$

其中，R_{ij} 为 NAT-PT$_i$ 和 NAT-PT$_j$ 之间的关系；S 表示同步关系；F 表示友好关系；h_{ij} 为 NAT-PT$_i$ 和 NAT-PT$_j$ 之间的跳数；H 为 NAT-PT$_i$ 到其他 NAT-PT 之间所有跳数的集合；$Num(h)$ 表示跳数为 h 的 NAT-PT 个数。

式(1)选择跳数最小的 NAT-PT 作为同步 NAT-PT，如果跳数小于 2，则添加跳数次小的 NAT-PT 作为同步 NAT-PT，保证每一个 NAT-PT 至少有 2 个同步关系的 NAT-PT，其他跳数的 NAT-PT 则作为友好 NAT-PT。

伪路由跳数计算公式为

$$T'=T+W \tag{2}$$

其中，T 为 2 个 NAT-PT 间的实际跳数；W 为一个大于 0 的整数值，表示经过本 NAT-PT 访问其他 NAT-PT 所连网络产生的跳数代价，需要根据具体情况进行设置，以调节 2 条路由的优先级；T'为伪路由跳数。NAT-PT 需要在 IPv4 和 IPv6 2 个域中分别计算伪路由。

2.4 信息共享

同步 NAT-PT 和友好 NAT-PT 共享的信息内容是不同的。同步 NAT-PT 共享基本信息、地址状态信息和地址绑定信息，友好 NAT-PT 只共享基本信息。NAT-PT 维护 3 个表来保存这些信息：基本信息表，地址状态表和地址绑定表[6]，表项内容分别为(NAT-PT, IPv4 地址池, 96 bit 路由前缀, 跳数, 关系)、(IPv4 地址, 绑定地址, 状态)、(IPv4 地址, IPv4 端口, IPv6 地址, IPv6 端口, 转换地址, 转换端口)，分别用来保存发现的 NAT-PT 的基本信息、IPv4 地址池中地址的状态和会话的地址绑定信息。

由于地址状态表和地址绑定表是随会话的建立和结束而变化的，因此同步 NAT-PT 需要及时更新共享信息。借鉴路由协议 RIPng 的更新机制，DRN 采用周期更新和触发更新相结合的更新方法。周期更新是指每过一个时间段 T 后，向同步关系的 NAT-PT 发送地址状态信息和地址绑定信息。触发更新是指 NAT-PT 地址信息改变后立即将更新的表项发送给同步 NAT-PT。

NAT-PT 的基本信息通常是不会改变的，因此，基本信息表不需要周期更新，仅在发生变化时产生一个触发更新。

3 DRN 工作过程

NAT-PT 启动后，通过发现机制与其他 NAT-PT 建立连接；计算相隔跳数，生成伪路由信息并传递给路由协议；根据信息共享策略交换信息。下面举例说明。

假设 DRN 包含一个 NAT-PT 服务器(NS)和 4 个 NAT-PT(记为 N_1~N_4)，其初始信息如表 1 所示。

表 1 NAT-PT 详细配置

	IPv4 地址	IPv6 地址	IPv4 地址池	路由前缀	DNS 地址映射		NS 地址
N_1	1.1.1.1	3FFE:1::1	1.1.1.0/24	3FFE:1::/96	1.1.1.2	3FFE:1::2	3FFE:5::5
N_2	2.2.2.1	3FFE:2::1	2.2.2.0/24	3FFE:2::/96	2.2.2.2	3FFE:2::2	3FFE:5::5
N_3	3.3.3.1	3FFE:3::1	3.3.3.0/24	3FFE:3::/96	3.3.3.2	3FFE:3::2	3FFE:5::5
N_4	4.4.4.1	3FFE:4::1	4.4.4.0/24	3FFE:4::/96	4.4.4.2	3FFE:4::2	3FFE:5::5

NAT-PT 之间的跳数如图 2 所示，其中，左下方为 IPv4

中的跳数，右上方(阴影部分)为 IPv6 中的跳数。

	N_1	N_2	N_3	N_4
N_1	/	0	1	2
N_2	4	/	2	1
N_3	4	4	/	1
N_4	5	5	4	/

图 2　NAT-PT 间跳数信息

假定 N_2, N_3, N_4 已正常工作，N_1 启动后的工作过程如下：

(1)初始化。启动后从本机获得基本配置信息，初始化基本信息表、地址状态表和地址绑定表，将静态映射地址加入地址绑定表。

(2)获取 NAT-PT 列表。与 NS 建立连接，注册基本信息，并获取其他 NAT-PT 地址列表，如表 2 所示。

表 2　NAT-PT 地址列表

	N_2	N_3	N_4
IPv6 地址	3FFE:2::1	3FFE:3::1	3FFE:4::1
IPv4 地址	2.2.2.1	3.3.3.1	4.4.4.1
域名	N2.lab.edu	N3.lab.edu	N4.lab.edu

(3)计算伪路由。其他 NAT-PT 利用式(2)和表 2 分别计算 IPv4 和 IPv6 中到 N_1 的伪路由，设所有 NAT-PT 对 IPv4 和 IPv6 的跳数代价分别为 W_4=1, W_6=3，结果如图 3 所示，其中，左下方为 IPv4；右上方为 IPv6。

	N_1	N_2	N_3	N_4
N_1	/	3	4	5
N_2	5	/	5	4
N_3	5	5	/	4
N_4	6	6	5	/

图 3　NAT-PT 间伪路由跳数

N_2, N_3, N_4 根据 N_1 的地址信息和伪路由跳数生成伪路由信息添加到路由协议中，并分别在两边网络中扩散。由于 IPv6 伪路由跳数用于生成 IPv4 伪路由，因此此时 IPv6 作为 IPv4 的虚拟路径。IPv4 伪路由同理。

(4)根据式(1)确定 N_1 与其他 NAT-PT 的关系，结果如表 3 所示。

表 3　N_1 与其他 NAT-PT 的关系

	N_2	N_3	N_4
IPv6	*S*	*S*	*F*
IPv4	*S*	*S*	*F*

(5)信息共享。依据不同的关系和更新策略，周期更新或触发更新相应的信息。

N_2 和 N_3 作为 N_1 的同步 NAT-PT，始终可利用 N_1 的 IPv4 地址建立会话并为会话选路。而 N_4 作为 N_1 的友好 NAT-PT，在 N_1 工作正常时，可以为当前已建立的会话选路，但不能建立新的会话，当 N_1 发生故障后，N_4 无法从 N_1 处获取信息，不再有任何作用。

下面举例说明 NAT-PT 不同状态时报文动态选路的过程。设图 1 中的纯 IPv4 节点 *X* 与纯 IPv6 节点 *A* 建立了会话，*X* 连接到路由器 R_2。N_1 与 N_2, N_3, N_4 的地址信息、伪路由信息及其关系如上。

在 N_1 正常工作时，R_2 关于 N_1 的伪路由跳数大于 N_1 的真实路由跳数，因此，会根据真实路由信息更新路由表并为报文选路，这时 *X* 经 R_2 到 N_1 只有 2 跳，会话报文经过 R_2 和 R_1 到达 N_1。

当 N_1 发生故障后，R_1 与 N_1 间路由变为不可达，进而 R_2 知道与 N_2 路由不可达。根据伪路由机制，N_2 关于 N_1 需 3 跳可达的伪路由信息通过路由协议进行传播，R_2 获知 R_3 经过 5 跳可到 N_1，于是更新关于 N_1 的路由信息：通过 R_3 到 N_1 需 6 跳，并将会话的所有报文转发到 R_3。

4　DRN 功能分析及需求

DRN 可优化穿越 NAT-PT 的会话的路径，避免 NAT-PT 失效时的通信中断和 IPv4 地址的浪费，并能在某种程度上缓解 NAT-PT 负载过重的问题。

DRN 中的伪路由机制使穿越 IPv6/IPv4 网络边界的报文不必通过特定的 NAT-PT，而是可以通过路由机制动态选择 NAT-PT，从而优化了 IPv6 和 IPv4 间会话的路径长度，发挥了多 NAT-PT 的优势，这是其他模型无法实现的。

DRN 中同步 NAT-PT 在功能上相当于备用 NAT-PT，一个 NAT-PT 失效后，同步 NAT-PT 可以转换失效 NAT-PT 会话的报文，并能够使用失效 NAT-PT 的 IPv4 地址池和路由前缀建立新的会话，使 NAT-PT 不再是单一失效点。

在多个 NAT-PT 之间进行大粒度的负载均衡时，伪路由变化时间间隔长，对整个路由影响不大，可以通过 DRN 在多个 NAT-PT 上实现负载均衡。但如果通过动态改变伪路由实现在多个 NAT-PT 间进行小粒度的负载均衡，则会导致路由变化过于频繁，容易引起路由振荡。

当 NAT-PT 规模很大或 NAT-PT 不属于同一个管理域时，为了提高 DRN 的可管理性，需要对 NAT-PT 进行级联。可将 NAT-PT 按管理域、地理位置或其他标准划分为多个 NAT-PT 域，然后通过域中的 NAT-PT 服务器进行级联。不同域的 NAT-PT 均为友好关系，只共享基本信息。

NS 需要检测已注册的 NAT-PT 是否在线，如果没有响应，则从活跃列表中删除。NS 是单一失效点，需要冗余备份。

NAT-PT 之间以及与 NS 间交互的信息属于关键信息，一旦泄漏，将使 NAT-PT 面临攻击和滥用的威胁，因此，需要使用加密认证技术(如 IPSec)保护这些信息的安全。

5　结束语

本文提出的 DRN 机制通过 NAT-PT 间的伪路由发布和信息共享，使多个 NAT-PT 协同工作，不仅可为报文提供动态选路支持，优化 IPv6 网络与 IPv4 网络间会话的路径长度，而且在 NAT-PT 发生故障时，可将其负载实时迁移到其他同步 NAT-PT 上，避免会话的中断。DRN 是一种协调多个 NAT-PT 共同工作的机制，可结合其他单 NAT-PT 改进方法，提高 NAT-PT 的性能。在下一步工作中，需要设计 DRN 与 NAT-PT 间的接口，实现 DRN 中的具体协议(如 NAT-PT 发现、伪路由发布和信息共享)，以及研究 DRN 对路由的影响等。

参考文献

[1] Tsirtsis G, Srisuresh P. Network Address Translation: Protocol Translation(NAT-PT)[S]. RFC 2766. 2000.

[2] 叶润国, 冯彦君, 吴　宇, 等. NAT-PT 可扩展性和可靠性问题研究[J]. 微电子学与计算机, 2004, 21(4): 19-24.

[3] 肖辽亮. NAT-PT 簇负载平衡的设计与实现[J]. 计算机技术与发展, 2006, 16(3): 80-82.

[4] Feng Yanjun, Ye Runguo, Song Chuck, et al. Load Balance and Fault Tolerance in NAT-PT[J]. IEEE/ACM Transactions on Networking, 2003, 11(12): 1957-1961.

[5] 张宏科, 苏　伟. IPv6 路由协议栈原理与技术[M]. 北京: 北京邮电大学出版社, 2006.

[6] 曾立安, 程朝挥, 凌　力. 一个加强的 NAT-PT 模型[J]. 软件学报, 2003, 14(12): 2037-2044.