第32卷 第20期 计 算 机 工 程 2006年10月
Vol.32 № 20 Computer Engineering October 2006
·网络与通信· 文章编号：1000—3428(2006)20—0126—03 文献标识码：A 中图分类号：TP393

IPv6隧道的NAT穿越技术及其在GPRS中的应用

苏 静，张会生
(西北工业大学电子信息学院，西安 710072)

摘 要：随着NGN、3G等IP网络业务的开展，向IPv6过渡的需求越来越迫切。隧道技术是过渡初期最易采用的方式，由于网络中大量NAT设备的存在，隧道技术中的NAT穿越问题是不容忽视的重点。该文通过对现有的普通隧道技术和Teredo隧道技术分析后，从NAT设备后IPv6孤岛接入IPv6网络的角度，提出了实现IPv6网络互联的IPv4 UDP隧道实现方法，并详细说明在园区网和GPRS网络中的应用。

关键词：NAT；Teredo隧道；IPv4 UDP隧道；GPRS

NAT Acrossing Technology in IPv6 Transition and Its Application in GPRS

SU Jing, ZHANG Huisheng
(Electronic Information College, Northwestern Polytechnical University, Xi'an 710072)

【Abstract】With the explosion of the IP network service, such as NGN, 3G, transiting to the IPv6 network is on the agenda. Using tunnels is the most easily method to choose. However, NAT devices in the path will be a big tough thing in the transition to IPv6 network. This paper focuses on how to across the NAT device using IPv4 UDP tunnel after analyzing the normal tunnel mechanism and Teredo tunnel, then produces the application method of fixed network and GPRS network.

【Key words】NAT; Teredo tunnel; IPv4 UDP tunnel; GPRS

大量增加的网络设备使得互联网的规模不断扩大，基于32位地址的IPv4协议显得力不从心，而随着NGN、3G等IP网络业务的开展，对IP承载网在地址容量、网络安全、服务质量和移动性方面有了更高的要求。在现有的IPv4基础网络中，NAT、CIDR等技术虽然缓解了地址短缺的压力，但却破坏了网络层的端到端架构，同时IPv4在移动性、安全性方面也暴露了缺陷。从IPv4向下一代网络协议IPv6的过渡已经提上日程。

隧道技术是向IPv6过渡初期最易采用的一种方法，本文将对其做深入的探讨和研究，并重点研究其中隧道封装数据包的NAT穿越问题。

1 NAT穿越问题

网络地址转换（NAT）技术是为了解决IPv4网络地址空间不足而产生的技术，在IP网络上已经得到了普遍的应用。NAT技术使得一个私有网络可以通过Internet注册IP连接到外部世界，位于inside网络和outside网络中的NAT路由器在发送数据包之前，负责把内部IP翻译成外部合法地址，以达到私网和公网互通。

NAT的技术比较复杂，数据包的传输过程中，根据一定的规则将包头中的地址、端口号进行转变，一般是基于一个转换地址池，并对其中的转换条目设定了一定的老化时间，根据不同的NAT机制，根据转换表做不同的处理，一般的上层传输通道是无法直接穿越NAT设备的。因此，NAT的出现带来的最大问题就是破坏了网络层的端到端架构，目前，也成为向IPv6网络过渡的一个拦路虎。

2 隧道技术分析对比

隧道技术是通过现有的IPv4网络基础设施来连接各个孤立的IPv6网络，IPv6数据包被封装在IPv4包里面进行传输，在隧道的终点进行解封装得到IPv6数据包后再交给相连的IPv6网络。具体方式如图1所示。

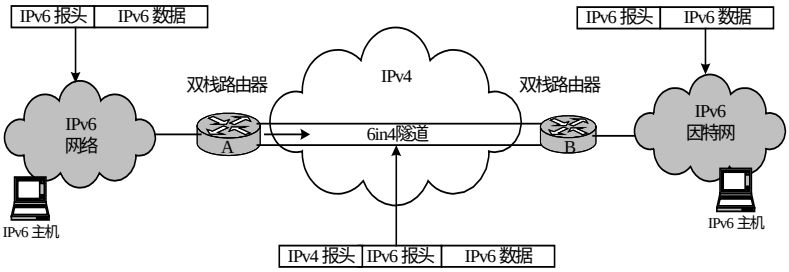

图1 隧道技术的基本机制

RFC2893（Transition Mechanisms for IPv6 Hosts and Routers）中分配给IPv6封装在IPv4中的协议号是41，表示IPv4包里面的上层协议数据是IPv6数据包。协议号为41的报文很可能被防火墙或NAT设备过滤掉，另外，IPv6 in IPv4隧道是无法穿越启用动态端口转换的NAT设备的，因为大多数的NAT设备不具备提供隧道路由的功能。下面对现有的几个隧道方式分析后，在TSP隧道建立协议的基础上提出了一

作者简介：苏 静(1981－)，女，硕士，主研方向：数据通信和网络；张会生，教授

收稿日期：2006-01-15 **E-mail：**susan1022@hotmail.com

种隧道报文顺利通过 NAT 设备的 IPv4 UDP 隧道的方法。

2.1 隧道技术基本方法

如图 1 所示，利用隧道技术连接 IPv6 孤岛和 IPv6 网络的基本思想就是将 IPv6 报文封装在 IPv4 报头中进行传输，以穿越 IPv4 网络，具体实现情况主要有以下两点：

(1)在隧道的入口对 IPv6 报文进行 IPv4 报头的封装，IPv4 报头中的协议字段为 41，Total Length 字段是其中 IPv6 的 Payload 长度加上原 IPv6 头的 40B 再加 IPv4 头的 20B，另外 IPv4 报头的校验和需要重新计算。

(2)在隧道的出口收到的封装好的 IPv6 in IPv4 报文，先判断报文是否经过分段，如果是，就对数据包进行重组，然后去掉 IPv4 报头，更新 IPv6 报头后，查 IPv6 路由，发送至相应的接口 ;如果没有分段，直接去掉隧道封装的 IPv4 报头，进行相应的 IPv6 报文处理。即完成了隧道报文的解封装和 IPv6 报文的路由发送。

这种方法的要求隧道两端的路由器均为双栈路由器，无论是哪种隧道类型，都是在 IPv4 报头中直接封装 IPv6 报文，但这种方法无法穿越路径中的 NAT 设备。

2.2 Teredo 隧道

Teredo 隧道是微软针对 NAT 问题提出的一种隧道方式，为了能够通过路径中的 NAT 设备，IPv6 数据包作为基于 IPv4 的用户数据包协议发送出去。

发送的报文格式有两种格式：Teredo 数据包（含负载）和 Teredo 气泡数据包（不含负载）。在这种隧道机制中，存在 Teredo 客户端、Teredo 服务器、Teredo 中继还有特定于 Teredo 主机的中继，如图 2 所示。

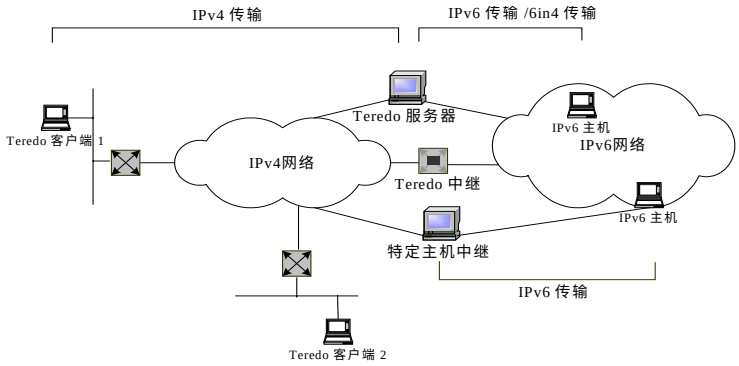

图 2 Teredo 隧道的组网结构

Teredo 的处理过程是，首先对 Terodo 客户端进行初始化，通过定期发送单一的气泡数据包到 Teredo 服务器，刷新相应的 NAT 转换表，在完成很多繁琐的相关初始化设置，并得知相应的 IP 地址和端口号后，Teredo 客户端就可以发送 Teredo 数据包到最近的 Teredo 服务器或中继器，由中继器完成报文的解封装发送到相应的 IPv6 主机。反之，从 IPv6 主机到 Teredo 客户端，也需要相应的初始化设置，发送气泡数据包以建立合适的链路后，再发送数据包进行通信。

Teredo 隧道方法涉及较多的 Teredo 设备，组网和实现都很复杂，且成本高。这种隧道机制是针对单一的 Teredo 客户端的，在 IPv6 开始的初期可能会有一定的应用，但是如果要将整个 IPv6 孤岛连接到 IPv6 网络中，则无法实现。另外它只能作用于 Cone NAT 和受限 NAT，不能作用于对称 NAT。因为对称 NAT 中如图中的 Teredo 客户端访问不同的外网地址会映射不同的外部地址和端口号，这是 Teredo 服务器所不能处理的。

2.3 IPv4 UDP 隧道

通过以上对两种隧道方式的分析发现，普通的隧道封装方式机制简单，但是无法穿越路径中的 NAT 设备，Teredo 隧道方式机制复杂，但致命的缺点是仅针对单一的客户端，没有实现 IPv6 孤岛与 IPv6 网络互联。因此根据 TSP（Tunnel Setup Protocol）隧道建立协议，再结合网络现状，可以从位于 IPv4 网络 NAT 设备后的 IPv6 孤岛开始考虑，如何将其连接到 IPv6 网络，而不是从 IPv6 网络角度考虑，如果路径中有 NAT 设备怎么办。

由于直接从位于 NAT 设备后的 IPv6 孤岛角度考虑，网络路径上必然存在 NAT 设备，因此 TSP 协议中的 NAT 发现处理就可以忽略了，直接从 IPv4 UDP 隧道的建立开始，相应的 TSP sever 的角色也就没有那么重要了，直接将 UDP 隧道的建立交给相连的路由设备即可。

该方案的工作机制是：IPv6 孤岛边界的双栈路由器收到一个发往 IPv6 网络的 IPv6 报文，则对其进行 IPv4 UDP 封装，该报文能够自动穿越 IPv4 网络中的 NAT 设备到达对端的双栈路由器。对端的路由器，也就是隧道出口，将 IPv6 报文解封装出来，送入 IPv6 网络；类似的，如果会话是 IPv6 网络内的主机发起的，则也是同样进行 IPv4 UDP 封装和解封装，实现通信。另外，如果 IPv6 网络中的主机与路径上没有 NAT 设备的 IPv6 孤岛进行通信，则通过其他的隧道（如普通 IPv6 in IPv4 隧道）进行通信，这种情况不在本文考虑范围以内。

这种机制不需要繁琐的初始化过程和过多的网络设备，能够工作于多层 NAT 设备的网络中，适合于园区网，也可以应用于无线分组网络中。下面就具体结合实例分析这种机制的实现方法。

3 固网和 GPRS 网络中的应用

3.1 固网应用

网络 A 是某企业网，通过 NAT 设备连入 IPv4 网络，现在想在企业网内部加入 IPv6 应用，要求能够与 IPv6 网络互联，且不影响原有的 IPv4 业务。

根据上述的机制，需要在企业网中添置一台支持 UDP 封装解封装的双栈路由器，与 NAT 相连后接入 IPv4 网络，相当于在企业的 IPv4 网络内部嵌套了一个 IPv6 孤岛，运行 IPv6 业务。

IPv4 UDP 隧道在固网中的应用见图 3。

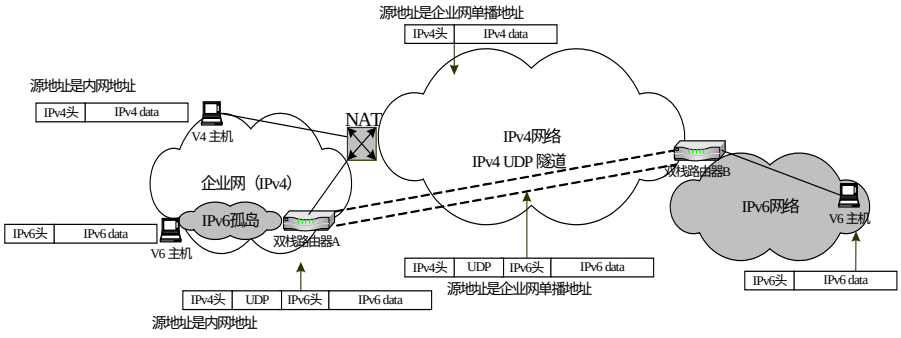

图 3 IPv4 UDP 隧道在固网中的应用

如图 3 所示，原来的企业网通过 NAT 设备连接到 IPv4 网络，企业网内部的 IPv4 主机都配置内部网络地址，当企业网内部要同外部网络通信时，发送源地址是内网地址（如 10.1.1.1）的 IPv4 报文，通过 NAT 转换后，修改 IPv4 源地址，变成外网地址（如 192.1.32.25）发送至 IPv4 网络，当 IPv4 外网主机要访问企业网内部主机时，则发送目的地址为 192.1.32.25 的数据报文，NAT 设备则根据地址和端口号等发送至相应的接口的主机上面，完成通信。

现在企业网内部加入了一批新的 IPv6 主机，要将这个 IPv6 孤岛与 IPv6 网络相连，需要如下的实现过程。

首先 IPv6 孤岛中的主机发送报文到 IPv6 网络。执行如下步骤：

(1)IPv6 主机发送源地址是主机 IPv6 地址，目的地址是要通信的 IPv6 网络中的某个 IPv6 地址的数据报文到双栈路由器 A。

(2)路由器 A 对该报文进行 IPv4 UDP 的封装，封装的 IPv4 的源地址是企业网的私网地址(如 10.1.1.1)，目的地址是 UDP 隧道对端的双栈路由器 B 对应的单播 IPv4 地址（如 206.13.34.10），将该 IPv4 UDP 报文发送到 NAT 设备。

(3)NAT 设备根据 NAT 转换表将私网 IPv4 源地址映射为对应的外网地址（如 192.1.32.25）发送至 IPv4 网络。

(4)该通过 IPv4 UDP 封装和 NAT 转换的 IPv6 报文在 IPv4 网络中传输，无论路径上存在多少 NAT 设备，由于 UDP 报头的关系都能够顺利穿越到达双栈路由器 B。

(5)路由器 B 收到该封装报文，对报文进行解封装，得到原始的 IPv6 报文，发送到 IPv6 网络中。

类似的从 IPv6 网络中的 host 发送 IPv6 报文到企业网内的 IPv6 主机，则由双栈路由器 B 执行 IPv4 UDP 封装，由 NAT 将目的 IPv4 地址进行转换后，发现是 IPv6 主机对应的 IPv4 私网地址，就发送给路由器 A，路由器 A 完成报文解封装后发送给 IPv6 主机，完成数据的传输。

简单地说，在增加了 IPv6 主机后，NAT 设备作为企业网与外网的连接入口的作用没有改变，只是增加了一个双栈路由器 A，将 IPv6 报文转化为 NAT 可识别的 IPv4 UDP 报文，转换后发送。相当于给 NAT 映射表中多增加了条目而已。另外要求对端的双栈路由器 B 能够识别该封装的报文，对其进行解封装后发送到相应的主机。

这种将 IPv6 孤岛连接入 IPv6 网路的方法，简单易行，成本低，组网简单，还能够穿越路径中的 NAT 设备，是一种经济可行的解决方案，很适合一些相对较独立的园区网采用。

3.2 移动网中的应用

在移动网络中，移动终端（Mobile Station, MS）通过接入网络（Receive Access Network, RAN）接入到通用分组无线业务（Generally Packet Radio Service, GPRS）网络，服务支撑节点（Service GPRS Support Node, SGSN）跟踪 MS 的位置，执行移动性管理和接入控制服务，网关支撑节点（Gateway GPRS Support Node, GGSN）则提供 GPRS 网络内部与外部网络的路由和封装，分配 IP 地址，实现与 ISP 网络的互通。MS 接收和发送的 IP 数据报文只对 MS 本身和 GGSN 是可见的，对 SGSN 是透明的。一般 MS 使用的是 IPv4 内网地址，如果该地址是 GGSN 给分配的，就由防火墙充当 NAT 的功能，将地址转化为外网地址，发送给 ISP 网络；如果该地址是 ISP 给分配的，则由 ISP 与 IPv4 网络相接的路由器做 NAT 转换，接入 IPv4 网络。后者更类似与固网的情况，相当于把 ISP 网络、GPRS 网络和 RAN 网络看作一个大的园区网。

如果基于 GPRS 形成 IPv6 孤岛，即图 4 中的 RAN 接入网络中所控制的主机含有 IPv6 地址的 MS，当然，对于 SGSN 来说，与 IPv4 一样是透明的，无法区分。当 IPv6 分组到达 GGSN 时，在 GGSN 与 IPv4 与 IPv6 网络间的双栈路由器 B 间建立一个 IPv4 UDP 隧道，具体在 GGSN 上对 IPv6 数据分组进行 UDP 和 IPv4 封装，IPv4 源地址为 GGSN 或 ISP 所能分配的 IPv4 地址之一，目的地址是对端 IPv6 网络与 IPv4 网络相连所使用的单播 IPv4 地址。封装好的数据包，无论是通过防火墙转换，还是通过路由器 A 转换，都因为含有 UDP 包头而不会被过滤，到达双栈路由器后，将数据进行解封装，就可得到原 IPv6 分组数据，然后根据路由发送到相应的 host。反之，IPv6 网络的 host 要访问 IPv6 地址的 MS，也同样，只是在双栈路由器上完成 IPv4 UDP 封装，在 GGSN 中完成解封装。

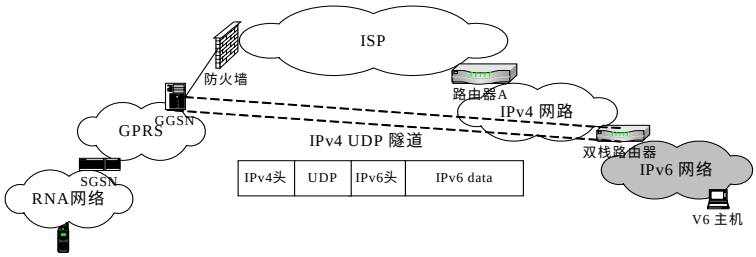

图 4 IPv4 UDP 隧道在移动网中的应用

鉴于 GPRS 网络的特殊性，用这种方法实现 IPv6 孤岛 MS 与 IPv6 网络的互通，对于接入网络层 RAN 不需要做太大的修改，只需在上层对 GGSN 做升级，使其能够支持 IPv4 UDP 封装和解封装，而且这种方式不需要给网络中添置其他服务器设备，就能实现与 IPv6 网络的互通。

4 结束语

在 IPv6 孤岛与 IPv6 网络互联的过程中，对 NAT 的穿越问题是必须解决的问题，使用 IPv4 UDP 隧道能有效解决这个问题，无论是在固网还是无线移动网络，都能够很好地应用。IPv4 UDP 隧道对 NGN 和 3G 业务的顺利开展有着不可忽视的作用，并具有其特定的应用领域。然而，下一代网络的业务发展是多元化的，网络构架也很复杂，要想能够顺利完成平滑过渡还有很长一段路要走。

参考文献

1 Teredo 概述[Z]. http:// www.microsoft.com, 2004-05.

2 Desmeules R. Cisco IPv6网络实现技术[M]. 北京：人民邮电出版社, 2004-01.

3 Blanchet M. IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)[Z]. Internet Draft: draft-blanchet-v6ops-tunnelbroker-tsp-0, 2004-11.