对等系统NAT穿越技术研究

谢统义[1,2],黄保华[2]

(1.广西教育学院科研处;2.广西大学计算机与电子信息学院,广西 南宁 530004)

摘 要:计算机和智能手机作为终端进行对等网络通信时,通常是被NAT(network address translator)设备隔离的,阻碍现代智能网络应用的发展。本文对国内外NAT技术原理、NAT基本类型以及各种NAT技术进行分析,详细分析了常用NAT技术的应用环境和体系结构,以及其有效性、稳定性、健壮性、安全性等技术特点,为对等系统NAT穿越技术的研究提供基础。

关键词:NAT;STUN;TURN;穿越

中图分类号:TP393.02 **文献标识码**:A **文章编号**:1006-9410(2014)03-0145-04

0 NAT穿越技术概述

NAT技术在内网与外网间实现IP地址复用是通过IP地址映射来实现的。通过使用较少的公有IP地址映射到数量较多的私有IP的地址,在局域网中使用私有IP地址,从而提高IP地址的利用率。NAT技术能有效的实现TCP(Transmission Control Protocol)协议、UDP(User Datagram Protocol)协议以及ICMP(Internet Control Message Protocol)协议等信息进行透明中继。

1. NAT穿越基本原理

NAT技术使得在IP地址不足的情况下,使内网主机有效的访问外网上的服务。内网使用复用的私有IP地址,这些私有地址只能得到内部网络的认可,而得不到互联网等外网的认可。此时NAT功能相当于路由器的功能,完成代理转发数据包信息,当内网主机要访问互联网必须路由到NAT网关代完成,同样,外网需与内网通信时也由NAT代完成。在NAT规则中,由内网向外网发送的数据包将被映射为合法互联网IP地址,而由外网向内网的数据包中的目的地址将被替换为内网的私有IP地址。NAT在应用中的设备一般安装两块网络接口卡,其中一块对外网与互联网连接,配置合法IP地址;一块对内网与局域网连接,配置为任意网段的私有IP地址,对内的私有地址即为局域网主机的默认网关[1,2]。

在P2P网络应用中,要实现对内网主机的连接就必须对NAT设备穿越,现阶段NAT的穿越方法主要有3种方式:反向连接方式、UDP穿越技术和中转方式。

(1)反向连接技术

反向连接方式的使用范围不大,适用性一般,适用于两个client端连接同一个Server端,而另一台主机直接与互联网相连。

(2)UDP穿越技术

收稿日期:2013年10月20日

基金项目:本文系国家自然科学基金项目 (No. 61262072) 和南宁市科学研究与技术开发计划项目(No. 20125258)成果。

要实现 UDP 穿越技术，要求通信双方能与互联网上某服务器建立 UDP 连接，即可以实现 UDP 数据包发送和接收。服务器能获取客户端节点的有关登录信息，并能通过登录信息的数据包中得到该客户端的公网节点。当该客户端位于公网上时，采用以上方法得到的两个节点的值是相同。

(3)中转方式技术

中转方式是比较简单的一种，具有高可靠性，但服务器负载压力大。此种方式是以 C/S 架构为基础，所有的 Client 都可以连接到对应的 server 端。

2. NAT 的基本类型

现阶段，在 NAT 的分类中主要是根据映射方式的差别来划分，主要有以下 4 种：对称型 NAT (Symmetric NAT)、完全圆锥型 NAT (Full Cone NAT)、受限圆锥型 NAT(Restricted Cone NAT)和端口受限圆锥型 NAT (Port Restricted Cone NAT)。

(1)对称型 NAT

对称型 NAT(Symmetric NAT)，工作原理与前几种有较大差别，其只是完成对同一私网的 IP 地址和端口对同一 IP 地址和端口的连接要求，全都转换到同一外网 IP 地址和端口，但如果主机使用 IP 地址和 Port 的地址对不一样，目的地址也不一样，这时 NAT 的映射也将不一样。也就是只有能够收到 IP 包的外网主机才能够向该内网主机发送回一个数据包。对称型 NAT，只要是源和目的地址不同则分配一个不同的地址映射。

(2)完全圆锥型 NAT

完全圆锥型 NAT(Full Cone NAT)，工作过程是将全部来自内网 IP 地址和端口的每一个连接请求，都转换成同一个外网的 IP 和 Port，公网主机则通过转换后的外网 IP 和 Port 实现通信，实现穿越 NAT 通信。此种方式是简单可行，在实际应用中也比较简单，快速的建立了内网与外网的 IP 地址和端口映射关系，这样也就实现外网与内网通信连接，实现穿越 NAT。

(3)受限圆锥型 NAT

受限圆锥型 NAT (Restricted Cone NAT)，工作原理与完全圆锥型 NAT 基本相同，同样也将全部来自内网所有连接请求，都转到外网的连接。但与完全圆锥型 NAT 工作方式不同的是，只有当内主机之前若是已经向外网的主机发送过信息，外网主机才可以与 NAT 后的主机实现通信。

(4)端口受限圆锥型 NAT

端口受限圆锥型 NAT (Port Restricted Cone NAT)，工作原理与受限圆锥型 NAT 方式基本相同，但限制条件较多。相比前面的类型多了对端口的限制，只有当内部主机曾经向外部某主机曾经发送过信息，外网主机才能与此内网主机建立通信。

3. NAT 穿越技术

目前常用的几种 NAT 穿越技术主要包括：ALG 方式、Full Proxy 方式、MIDCOM 方式、TURN 方式、STUNT 方式以及 ICE 方式。

3.1 ALG 方式

ALG(Application Level Gate)[3]应用层网关穿越技术，这是几种 NAT 穿越技术中使用比较早的方式，是在老式 NAT 穿越技术的扩展。老式的 NAT 或 NAPT 技术针对 IP 报头地址和传输协议报头信息进行修改，报文中可能包含 IP 地址或端口信息的应用层协议(例如 H.323[4]、SIP 协议以及 FTP 协议等)，此时就不用完成地址转换。而 ALG 方式对此进行了改进，它可以对应用层数据进行完整数据的分析，可以有效的完成 IP 地址和端口的转换。

ALG 方式是比较简单一种 NAT 穿越方式，其缺点相对也是比较多。

(1)可扩展性差，当需要增加新的应用需要对硬件进行更新。

(2)ALG 方法需要对数据包进行分析，NAT 负载过重，容易成为网络瓶颈，所以其效率和性能并不高。

(3)在有多层 NAT 中，则每个 NAT 都必须升级改进以支持不同协议 ALG 功能。

(4)安全性不高，在应用中 ALG 不能解密加密后的报文信息，数据传输采用明文传送，存在安全隐患较大。

3.2 Full Proxy 方式

代理技术(Proxy)[5]方式是为解决 ALG 方式需要更改 NAT 硬件设备升级问题所产生的，也是目前运用较多的一种 NAT 穿越技术方案。

Proxy 技术是指通过对私网内用户呼叫的信令和媒体同时做 Relay[6]来实现对 NAT 的穿越。代理方式在网络中部署可以位于私网内部，也可以位于公网和私网边缘或公网上。Proxy 方式用的

是专用的语音和视频的设备，不需要对现有的NAT进行软件扩展,不影响对其他业务的NAT穿越。但是与ALG穿越方式相比Proxy技术在实现NAT穿越时对硬件要求也不高，因此Proxy方式应用范围比较广，在实际应用中Proxy方式会增加了网络信息安全功能、防止终端漫游等。但是，Proxy方式的不足之处是每增加一种新的应用就要进行协议扩展要求，在对媒体和信令同时进行数据通信时,工作效率将受到比较大的影响,有时还会出现延时和丢包可能性。

3.3 MIDCOM 方式

MIDCOM [7](Middle-Box Communications)技术是针对解决ALG和Proxy方式的所出现的问题而出现的方案，解决可扩展性不强和中继转发效率低的问题,由IETF制定。

MIDCOM由两部分构成:MIDCOM Agent和Middle-Box，分别设在代理和具有合法网络地址的服务器上。MIDCOM方式采取的是MIDCOM Agent通过Middle-Box识别H.323报文，进而控制端口的打开或关闭来实现连接，在应用中由Middle-Box转移到MIDCOM Agent上实行透明的转换，从而通过对MIDCOM Agent改进来适应和支持更多的不同的业务。

在网络信息安全上,MIDCOM方式可进行密文和控制信息的传输,安全性相对比较高。但是，在设备扩展上要求现有NAT进行改进以支持MIDCOM协议,所以目前MIDCOM穿越方式的实际应用并不多。

3.4 STUN 穿越方式

STUN [8](Simple Traversal of User Datagram Protocol Through NAT),采用STUN协议,可以简单的实现NAT穿越,并且STUN是一种轻量级协议。STUN协议属于简单的C/S协议,Client向Server发送请求,Server返回Response。

在NAT穿越过程中，首先是内网主机Client通过传输网络协议向STUN server发送请求信息，当STUN server对相关信息进行应答后,应答信息中包含Client端口的IP地址,然后对响应的信息通过NAT返回Client,Client在全部业务请求过程中会将该公网的有关地址信息替换所被响应的信息中,并且告知与其直接相连结点的IP和Port信息,作为NAT内部的IP和Port地址。STUN网络结构示意图如图3-1所示。

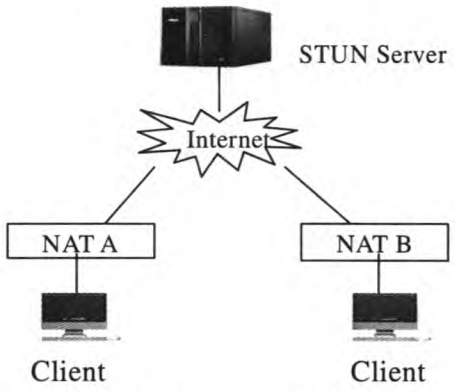

图3-1　STUN结构

Fig.3-1　The structure of STUN

在STUN实际应用中，通常是利用客户端向服务器发送请求(Require)消息和接收响应（Response）消息，通过Response消息获取外部NAT上的映射地址和NAT类型等相关信息,此时在数据包中的有关地址信息就可以直接更改为外部NAT上的地址,而不是私网内客户端的私有网络地址,并且通知目的节点自己的接收IP和Port地址信息。所以数据包在通过NAT时不用修改的，更改数据包报头的相关地址信息即可。

3.5 TURN 穿越方式

TURN（Traversal Using Relay NAT）方式。TURN解决方案的原理与STUN是类似的,TURN采用内网的VOIP终端设备获取直接与互联网相连的TURN Server的IP地址,然后在数据包中更改所需的外网地址。TURN通过有效的控制机制获取内网中VOIP端对外的所接收的IP地址和端口号，当内网Client所发送的信息都通过TURN Server对数据进行Relay中转。这个优点是与STUN相同的，另外TURN可以对对称型NAT网络的穿越,弥补了STUN不能穿越对称型NAT的不足。示意图如图3-2所示。

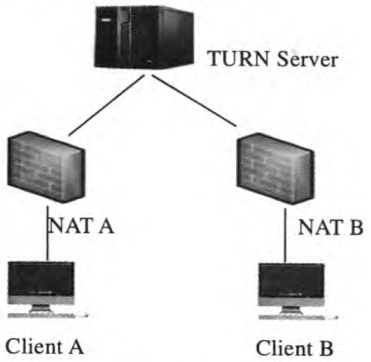

图3-2　TURN结构

Fig.3-2　The structure of TURN

TURN的不足之处是对网络终端有一定的依赖性，TURN客户端必须支持VOIP。另外，全部的数据传输都必须由TURN Server完成转发，这样的结果导致TURN Server负载过重，可能会出现丢包和网络连接延迟等现象。

3.6 ICE穿越方式

ICE [9,10]（Interactive Connectivity Establishment）交互式连通建立方式方式。ICE并不是一种新的技术，ICE是STUN和TURN的综合应用。ICE不需要对STUN、TURN或RSIP进行修改就能实现各种NAT的穿越，并且在穿越非对称型和对称型NAT的过程中是自适应的过程，自动采取比较合适的工作方式进行穿越，能够解决单一使用某种穿越方式所带来的各种缺陷和不足。

4. 总结与展望

本文详细分析了ALG、Full Proxy、MIDCOM、STUN、TURN和ICE协议的原理及实现，通过对其协议的流程分析，明确各种NAT穿越技术的适用范围和优缺点。由于篇幅所限，本文还有许多需要完善之处，对目前最新的ICE解决方案穿透NAT的原理和穿越流程未做详细研究，在今后的工作中，对等系统基础上ICE穿越技术还有很多需要补充，如：通过对ICE协议实现代码的分析，验证了其方案的可行性，分析了ICE协议解决方案的优点和缺点等问题。

参考文献：

[1] 陈亮. 基于改进ICE协议的流媒体穿透NAT的研究[D].华南理工大学，2012.

[2] 马义涛. 基于P2P网络应用的NAT穿越方案的分析与设计[D].上海交通大学，2008.

[3]P.Srisuresh，M.Holdrege.IP Network Address Translator（NAT)Terminology and Considerations [EB/OL]. http://www.ietf.org/rfcs/rfc2663.txt，August 1999/March 2013.

[4]ITU -T Recommendation H.323 -1997 Packet based multimedia communication systems.

[5]杨鑫，沈燕飞，王毅，朱珍民.基于SIP的Android视频通信终端实现[J].计算机工程，2012(07)：220~222+226.

[6]巩文科，赵洁，张继声，黄月珍.基于GPRS的移动监控系统设计与实现 [J]. 计算机安全，2012(03)：21~24.

[7]周野，基于ICE的NAT_FW穿越技术研究与实现[D].哈尔滨理工大学，2009.

[8]J.Rosenberg，J.Weinbergerete. RFC3489STUN -SimpleTraversalof User Datagram Protocol （UDP） Through NAT.Mareh2003.http://Tools.ietf.org/html/rfe3489.

[9]Rosenberg J.RFC5245 Interactive Connectivity Establishment （ICE）：A Protocol for Network Address Translator （NAT） Traversal for Offer/Answer Protocols[S].IETF，2010.

[10]J.Rosenberg，J.Weinberger，C.Huitema，R. Mahy.STUN-Simple Traversal of User Datagram Protocol(UDP)[EB/OL].http://www.faqs.org/rfcs/rfc3489.html，IETF RFC3489 March 2003/March 2013.

（上接第140页）

总的说来，广西大学图书馆在东盟研究专题文献保障方面已经具有良好的基础，形成了初步的特色。要建设研究级的东盟研究文献保障体系，还必须在文献资源建设中制定系统化建设规划和特色化建设策略。

参考文献：

[1]龚亦农.基于硕士学位论文引文分析的文献需求研究——以南京师范大学为例[J].新世纪图书馆，2011(07)：42，44，21.

[2]潘云涛，马峥. 2003年度中国科技论文统计与分析 [M]. 北京：科学技术文献出版社，2005：114.

[3]张桂清.汕头大学研究生学位论文引文分析与研究[J].大学图书情报学刊，2005(02)：84~86.

[4]石晓军等. working paper推进学术研究作用的实证研究[J] 中国软科学，2008(09)：46~53.

[5]何荣利等. 科学引文的聚散性探讨[J].图书馆理论与实践 2000(06)：26~28.

[6]李峰.使用引文分析法考察图书馆文献保障情况 [J].大学图书馆学报，2011(05)：104~107.

作者简介：

林葵(1967-)，女，广西大学图书馆副研究馆员。