ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.5,No.3,January 2009, pp.606-609

E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

UDT 穿透在 P2P 开发平台中的应用

周寅[1],竺伟[2],张鹏[2]

(1.浙江大学 宁波理工学院信息分院,浙江 宁波 315040; 2.宁波科技园区瀑布软件有限公司,浙江 宁波 315040)

摘要:目前众多的 P2P 软件都采用 TCP/UDP 协议的穿透,其中穿透的方式 ALG、MIDCOM、STUN、TURN、FullProxy 等。该文针对这些协议的各种穿透进行了分析和总结,提出了基于 UDT 传输协议的 NAT 穿透。它能够使 P2P 软件在穿透中实现可靠连接和动态设置 QoS。通过在本公司自主开发的 P2P 平台[1]中的应用可以发现 UDT 穿透可以在数据传输中充分的利用有限的带宽。

关键词:UDT;穿透;NAT;可靠连接;Qos 动态设置

中图分类号:TP311 **文献标识码**:A **文章编号**:1009-3044(2009)03-0606-04

UDT Penetration in the P2P Application Development Platform

ZHOU Yin[1], ZHU Wei[2], ZHANG Peng[2]

(1.Ninbo Institute of Technology Zhejiang University,Ninbo 315040,China; 2.Ninbo Science and Technology Park Waterfall Software CO.,Ltd., Ninbo 315040,China)

Abstract: Presently,most of the P2P softwares are using TCP/UDP while penetrate the different NATs in internet.The way of penetration are different,which includeing ALG, MIDCOM,STUN,TURN,FullProxyand so on. We set up a new NAT penetration based on the UDT while analysing and summarizing these kinds of penetrating technology.It can create the reliable connection while penetrate the different NAT and set the QoS dynamically. Through the P2P platform which use the UDT NAT penetration we find it can use the limited bandwidth adequately in the data transmission.

Key words: UDT;penetrate;NAT;reliable connection;dynamical QoS set

1 引言

1.1 NAT 穿透的意义

IP 地址是构成整个网络的基础,根据中国互联网络信息中心(CNNIC)研究表明,全球仅剩 10 亿个可用的 IPv4 地址,IP 地址匮乏早已是一个不争的事实。通过对现有 IP 地址扩展技术的分析得知,IPv6 是解决 IP 地址匮乏的最佳的办法,但是由于现有网络设备以及各种条件的制约,在全国范围内实施 IPv6 架构还需时日。在现有 IP 地址扩展技术里面,网络地址转换技术(NAT)是进行 IP 地址扩展的一项非常流行的技术,它通过私有地址与公共地址之间的转换来使更多的主机上网,现有大部分企业及组织都采用了 NAT 技术来组建自己的网络,但是 NAT 的存在也给网络带来了一定的问题,因为 NAT 只允许内网主动向外建立连接,丢弃任何主动向内的连接,这样就失去了对现在非常流行的端对端网络的全面支持,所以如何顺利高效的实现对 NAT 穿越就显得尤为重要[2]。

1.2 NAT 穿透技术目前的发展现状

目前国内外穿越 NAT 的方法主要包括 ALG[3]方式,MIDCOM[4]方式、STUN[5]方式、TURN[6]方式、FullProxy[7]方式等。这些方法或多或少都有一系列的问题存在,比如目前国内外流行 UDP 穿透技术,这种方式实现起来比较简便,且能穿越除对称型 NAT 之外的所有 NAT 类型,但是 UDP 穿透技术实现互连时,数据丢失的现象比较普遍,而且丢失的情况比想象的还要严重,虽然根据情况的不同多少有些差异,但是一般都有 10%~20%的数据包不能正确地到达目的地。这对于一些对数据安全性要求高的情况就不适合了,现实中很多实际的情况就是在数据传输时,重要与非重要的数据并存,如此高的丢包率显然无法满足要求。

本文在分析这些主流穿越方法的特性后,提出了一种新型的穿越思想:将原有服务器的角色转移到具有公共 IP 地址的 PC 机上,让其实现服务器功能,提供分布式服务,这样就能有效的解决现有穿越方式中普遍存在的服务器瓶颈问题;本文还提出了一种依据地理位置远近进行代理 PC 机的查找的方法,这种方法可以提高代理节点的效率。论文充分地分析了现有的 IP 地址扩展技术及 NAT 穿越技术,并在总结现有 NAT 穿越技术的基础上,给出了新穿越方式的具体设计思路及核心部分的实现,这对目前的 NAT 穿越方式的发展是具有一定的参考价值的。

1.3 UDT 简介

基于 UDP 的数据传输协议(UDP-based Data Transfer Protocol,简称 UDT[8])是一钟互联网数据传输协议。UDT 的主要目的是支持高速广域网上的海量数据传输,而互联网上的标准数据传输协议 TCP 在高带宽长距离网络上性能很差。

顾名思义,UDT 建于 UDP 之上,并引入新的拥塞控制和数据可靠性控制机制。UDT 是面向连接的双向的应用层协议。它同时支持可靠的数据流传输和部分可靠的数据报传输。

本文是利用 UDT 的拥塞控制和数据可靠性控制机制,来实现 UDT 穿透连接在传输中的动态的 QoS 设置和可靠连接的优越特性[9]。

收稿日期:2008-11-25

基金项目:宁波市科技型中小企业技术创新基金项目(项目编号:06C26213311212);宁波市自然科学基金(项目标号,项目编号:200502A4501003);宁波市留学人员科技创新创业资金(项目编号:2005A710013)

作者简介:周寅(1974-),1995 年获得中国科学技术大学少年班和近代物理系学士,1999 年分别获得美国俄亥俄大学物理系和计算机系的物理学硕士学位和计算机系硕士学位,2003 年获得美国俄亥俄大学物理博士学位。主要从事网络应用、P2P 应用研究。

2 相关技术

2.1 ALG方式

应用层网关(ALG)是被设计能识别指定 IP 协议的 NAT 设备或者防火墙。它不是简单地察看包头信息来决定数据包是否可以通过,而是更深层地分析数据包负载内的数据,也就是应用层的数据。

如果一个 NAT 被应用来屏蔽内部 IP 地址,这时 ALG 就需要一个代理,一些防火墙生产厂商把代理结合到 ALG 上越过 NAT。

主要的路由器、防火墙厂商像 Cisco、Checkpoint 都对他们的 NAT 设备/防火墙产品提供 H.323 ALG 升级功能,但市场上很多防火墙还不支持 ALG。

这种解决方案有如下缺点:

1) 由于要分析数据包负载,加重了 NAT 的处理任务,影响网络的运行,形成潜在的网络"瓶颈"。

2) 当配置多级 NAT 设备时,在呼叫路径上的每个 NAT 都必须被升级来支持 ALG 功能。

3) 网上大量 NAT/FW 不具备 ALG 能力,需要更换或升级。

2.2 MIDCOM 方式

中间盒通信(MIDCOM)方式的主要思想是引入实体 MIDCOM 代理,并通过 MIDCOM 协议对 Middlebox 进行控制。这是一种比较有前景的方式,但是目前的 NAT/FW 设备大部分没有 MIDCOM 协议,所以先在应用范围还是相对较小。

2.3 STUN 方式

STUN 是一个轻型协议,它可以使得应用程序发现它和公网之间的 NAT 类型。它也可以使得应用程序知道 NAT 为其分配的公网地址。

STUN 是一个简单的客户端/服务器协议,使用 STUN 协议主要是为了发现 NAT,获得自身绑定的端口。

STUN 绑定请求用来发现存在的 NAT,发现 NAT 映射的公网地址和端口。当客户端接收到 STUN 绑定应答时,比较数据包中的 IP 地址和端口,并和发送请求包的本地 IP 地址和端口进行比较。如果不匹配,说明 STUN 客户端在一个或者多个 NAT 后。对于静态 NAT,STUN 应答中的地址和端口是公网的,公网上的主机可以发送数据包到发送 STUN 请求的应用程序。应用程序只需要侦听 发送请求的地址和端口,就会收到从公网主机向该公网地址和端口发送的数据包。

当然,主机可能不是在静态 NAT 后。事实上,应用程序本身不知道它自己位于哪种 NAT 后。为了判断 NAT 类型,客户端会发送其他的 STUN 绑定请求。客户端发送第二个 STUN 绑定请求,请求会从同样的源地址和端口发往不同的 IP 地址,如果应答数据包中的 IP 地址和端口与第一次应答包中的地址和端口不同,客户端就可以知道其位于对称 NAT 后。为了判断是否是在静态 NAT 后,客户端可以在 STUN 绑定请求中设置标志告诉 STUN 服务器从与接收数据包的 IP 地址 和端口不同的 IP 地址和端口发送应答包。换句话说,客户端在源地址和端口向目的地址发送 STUN 绑定请求,服务器使用地址和端口应答。如果客户端接收到了 该应答,那么它就是在静态 NAT 后。STUN 也可以允许客户端请求服务器从接收请求的地址发送 STUN 应答,但端口是不同的,从而可以发现客户端是在动态 NAT 还是在 PAT 后。STUN 存在的问题如下:

1) 不能建立可靠 UDP 的连接;

2) 不能动态设置 QoS;

3) 能够使得 UDP 数据包穿越 NAT,但是只支持 NAT 类型的子集,特别是 STUN 不支持对称类型的 NAT 穿越,而该类型在很多企业中的应用是很普遍的;

4) STUN 的发现过程基于 NAT 处理 UDP 的方式,可能对某些新型的 NAT 设备是不正确的。当 STUN 服务器不是位于一个公共的地址域时,STUN 不能正常工作。

2.4 TURN 方式

TURN 方式解决 NAT 问题的思路与 STUN 相似,也是私网中的 P2P 节点通过某种机制预先得公网上的服务地址(STUN 方式得到的地址为出口 NAT 上外部地址,TURN 方式得到地址为 TURN Server 上的公网地址),然后在报文净载中所要求的地址信息就直接填写该公网地址。

TURN 的全称为 Traversal Using Relay NAT,即通过 Relay 方式穿越 NAT。TURN 应用模型通过分配 TURN Server 的地址和端口作为私网中 VOIP 终端对外的接受地址和端口,即私网终端发出的报文都要经过 TURN Server 进行 Relay 转发,这种方式除了具有 STUN 方式的优点外,还解决了 STUN 应用无法穿透对称 NAT(Symmetric NAT)以及类似的 Firewall 设备的缺陷,同时 TURN 支持基于 TCP 的应用,如 H323 协议。此外 TURN Server 控制分配地址和端口,能分配 RTP/RTCP 地址对(RTCP 端口号为 RTP 端口号加 1)作为私网终端用户的接受地址,避免了 STUN 方式中出口 NAT 对 RTP/RTCP 地址端口号的任意分配,使得客户端无法收到对端发来的 RTCP 报文 (对端发 RTCP 报文时, 目的端口号缺省按 RTP 端口号加 1 发送)。

TURN 的局限性在于需要终端支持 TURN Client,这一点同 STUN 一样对网络终端有要求。此外,所有报文都必须经过 TURN Server 转发,增大了包的延迟和丢包的可能性。

3 UDT 穿透的具体设计实现

本文提出的 UDT 穿透是通过对现有的穿越方式的研究构思出来的, 参考了 STUN 方式与 TURN 方式的部分思想,并且针对它们所不能解决的服务器服务性能瓶颈问题,提出了自己的服务器分布式方式和物理地址查询方式,很好的解决了现有方式的相关问题。新穿越方式是基于 UDT 协议的,是一种可靠连接的网络协议。

3.1 Peer 注册

每一个作为 Client 的 Peer 都各自相邻的 Proxy Server 处进行注册, 本文采取 UDT 连接方式进行两次注册。具体注册过程的时序图,如图 1 所示。

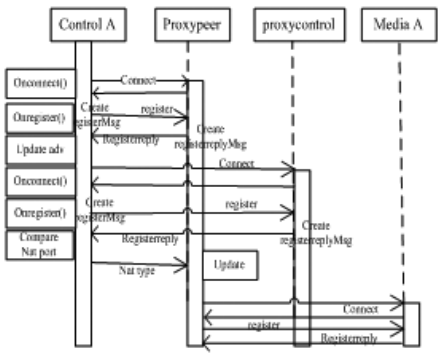

图 1 Peer 的注册时序图

3.2 NAT 端口预测

互联网中存在各种各样的局域网,它们一般都是在各种不同的 NAT 后。如图 2 所示。

目前市场上主要有三种 NAT 端口映射类型:

1) 静态端口映射(Static NAT);

2) 动态端口映射(Pooled NAT);

3) 网络地址端口映射(Port-Level NAT)。

本平台在穿透中,主要是针对动态端口映射和网络地址端口映射两种路由器地进行分析。上一节中 Peer 两次注册的方式,来实现对 NAT 端口的记录和预测。具体过程是:

1) Client Control 在 Proxy Peer 上第一次注册的,Proxy Peer 返回 RegisterReply 消息, 其中包含 Client Control 在 NAT 中对外的 IP 和 Port;

2) Client Control 在 Proxy Control 上进行第二次注册,Proxy Control 同样返回 RegisterReply,里面也包含 Client Control 在 NAT 中对外的 IP 和 Port;

3) Client 对于这两次的 NAT 信息进行比较,如果一样则更新返回回来的 NAT 信息对名片进行更新,同时通知给 Proxy Peer 更新该 Client 名片信息;如果不一样,则根据类型对 NAT 端口进行预测;目前预测主要是针对端口线性变化的 NAT,通过端口递增或递减的 δ 量的预测方式。

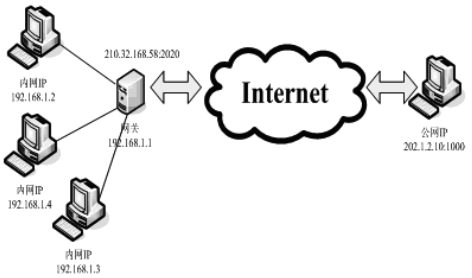

图 2　NAT 映射示意图

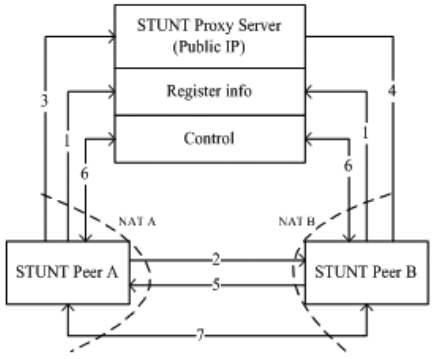

图 3　UDT STUNT 穿透图

3.3 穿透连接

1) Register Advertisement 和 Nat Type

2) Connect PeerB

3) StunConnect Proxy Server

4) Triger PeerB

5) FireBack to Peer A

6) A and B exchange info through the proxy's Control channel

7) Direct Connection between A and B

图 3-3 是本平台采用 UDT 打洞穿透方式示意图,具体的实现主要有以下几个步骤:

1) Client A 通过服务器注册获取自身信息与该 Proxy 上其它用户信息等;

2) Proxy 记录 Client A 的 NAT 后的 IP 地址与端口;

3) Client B 通过 Proxy 注册成功获取自身信息与该 Proxy 上其它用户信息等;

4) Proxy 记录 Client B 的 NAT 后的 IP 地址与端口;

5) Client A 向 Proxy 获取 Client B 的 IP 和 Port;

6) Client A 获得 Client B 的 IP 地址后并发送 UDT 信息到 Client B;

7) Client A 与 Client B 请求失败,信息丢失,此时 Client A 报告 Proxy 要求 Proxy 帮忙对 Client B 进行通知;

8) Proxy 接到此命令后,将 Client A 的 IP 地址发给 Client B,要求它连接;

9) Client B 收到服务器的信息后发送请求到 Client A;

10) 由于此时 Client A NAT 已经存在 Clinet B 的 session, 所以此时 Client A 与 Client B 建立链接成功;

11) Client A 发送消息到 Client B 成功,不经 Proxy 中转。

通过以上的一系列的步骤,ClientA 与 ClientB 实现了直接的通讯, 并在它们之间建立了可动态设置 QoS 的 UDT 可靠连接。

4 实验结果

4.1 实验用例

本用例采用三台 PC,其中一台 Server,两台 Client。此时 Server 只提供数据给一台 Client1, Client2 从 Client1 上去数据。然后通过艾泰 810 实现带宽限制。利用这种方法来测试使用 UDT 穿透的 Client2 在不同带宽下的数据读取情况。

4.2 实验环境

系统硬件:三台 PC ,配置:CPU P4 3.20GHz　480M 内存

路由器: 一个艾泰 810,一个 D-LINK DI704UP

系统软件:windows XP

应用软件:Iperf 测速软件

4.3 实验结果

实验结果如表 1~表 2,图 4~图 6。

表 1　UDT 穿透

带宽(Kbps)	帧大小 (Byte)	传输速率 (Kbps)
30	140	25.7
40	255	46.9
50	298	54.8
78	450	82.8
100	780	143.5
230	1360	250.2
321	1900	349.6
500	2780	511
1000	8000	1472

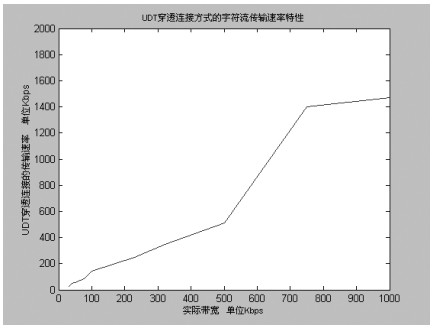

图 4　UDT 穿透方式的传输速率特性图

4.4 测试结论

有上面的图表可以看出 UDT 传输的效率要高于传统的 TCP，而且在带宽大于 50Kbps 的情况下,UDT 的传输速率会大于当前的带宽，充分的利用和扩充了当前的带宽。

表 2 TCP 穿透

带宽(Kbps)	帧大小 (Byte)	传输速率 (Kbps)
30	140	31.1
40	255	48.8
50	298	62.7
78	450	67.2
100	780	125.1
230	1360	165.6
321	1900	230
500	2780	331.2
1000	8000	1361.6

5 结论

该文介绍了一种网络传输的协议以及它在 NAT 穿透领域的应用。提出了 UDT 穿透的几个优点:

1)不需要特殊的硬件来支持,是一种轻型的网络协议;
2)建立了可靠连接;
3)实现了动态的 QoS 设置;
4)能够充分的利用当前的网络带宽。

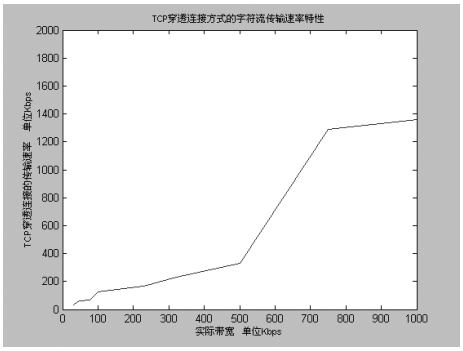

图 5 UDT 穿透方式的传输速率特性图

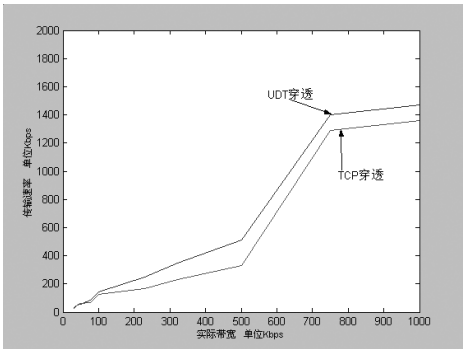

图 6 UDT 穿透和 TCP 穿透传输速率特性比较图

参考文献:

[1] Zhou Y,Chen X,Hua X.Cascade: A P2P Live Media Broadcasting Middleware in Java[C].Iowa City, USA:The Second International Multi-Symposiums on Computer and Computational Sciences,2007.
[2] 张云勇,刘韵洁.基于工 Pv6 的下一代互联网[M].北京:电子工业出版社,2004.
[3] 黄永峰,李建庆.SIP ALG 穿透 NAT 的实现[J].电信快报:网络与通信,2007(2):5-9.
[4] IETF RFC3303,Middlebox Communication(MIDCOM) protocol Semantics[S].
[5] RFC3489,Rosenberg J.STUN-Simple Traversal of User Datagram Protocol(UDP) Through Network Address Translators (NATs)[S].2000.
[6] Rosenberg J,Mahy R,Huitema C.Traversal Using Relay NAT(TURN) draft-rosenberg-midcom-trun-05[Z].2004.
[7] 张巍.基于 Fullproxy 的 H.323 协议穿透 NAT 解决方案[J].电脑知识与技术,2007(24):12-15.
[8] UDT 协议-基于 UDP 的可靠数据传输协议[EB/OL].http://linux.chinaunix.net/bbs/archiver/tid-935314.html.
[9] 王欣,张永军,顾畹仪.一种新的基于认购速率和 QoS 等级的动态带宽分配算法[J].中国电子科学研究院学报,2007(3):250-253.

(上接第 592 页)

通过这种混合机制的加密算法,发送方和接收方只需拥有 ECC 公钥和 ECC 密钥就可以实现对 AES 算法中密钥的管理。其中 ECC 公钥和 ECC 密钥都有 ECC 椭圆曲线加密算法生成。

5 小结

IEEE801.11iWLAN 安全标准在数据安全性机制中使用了 AES 加密算法来实现对网络数据的加解密。AES 作为新一代的数据加密标准,具有高安全性、高性能、高效率等特点,但由于其属于对称密钥加密系统,对加解密的密钥管理较为繁琐,为了解决这一缺陷,可使用 ECC(椭圆曲线加密)算法来加密和管理 AES 的密钥,实现 AES 与 ECC 的混合加密机制,从而达到高效率的密钥管理与高安全性的数据加密,进一步提高 WLAN 的数据安全性能。

参考文献:

[1] 黄智颖,冯新喜,张焕国.高级加密标准 AES 及其实现技巧[J].计算机工程与应用,2002(9):114-115.
[2] Stalings W.密码编码学与网络安全[M].北京:电子工业出版社,2004.
[3] 朱根标,张凤鸣,王金干.基于混合加密算法的网络安全体系构造[J].微电子学与计算机,2005,22(6):33-35.
[4] IEEE Standard 802.11-l 999.IEEE Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part l1:Wireless Medium Access Control(MAC)and Physical Layer(PHY)Specifications[S].New York:IEEE Press,1999.