NAT 技术及其穿越方案研究

白伟华[1,2] 李吉桂[1]

(华南师范大学计算机科学系 广州 510631)[1] (肇庆学院计算机科学系 肇庆 626040)[2]

摘 要 NAT 技术被广泛应用到各个领域,但在应用中要注意如何解决 NAT 的穿越问题。本文介绍了 NAT 技术和 NAT 穿越问题,并用例子说明了在应用中实现 NAT 穿越所遇到的问题,最后分析了可实现 NAT 穿越的解决方案和方案的局限性。

关键词 NAT,NAT 穿越,STUN,TURN

The Technology of NAT and the Research of its Traverse Solutions

BAI Wei-Hua LI Ji-Gui

(Dep. of Computer Science, South China Normal University, Guangzhou510631)[1] (Dep. of computer science, Zhaoqing college, zhaoqing 626040)[2]

Abstract The technology of NAT has been widely used in many domains, but the problem, how to solve the problem of NAT traverse, must be adverted in the application. This paper introduces the technology of NAT and the problem of NAT traverse, and shows the problem that would be met in the application for NAT traverse with a example, and analyzes the solutions and its limitation which can be used to realize NAT traverse at present in the last.

Keywords NAT, NAT traverse, STUN, TURN

1 什么是 NAT 技术

NAT[1](Network Address Translation 网络地址转换)是一个 IETF 标准,它可以将局域网中的内部地址节点翻译成合法的 IP 地址在 Internet 上使用(即把 IP 包内的地址域用合法的 IP 地址来替换),或者把一个 IP 地址转换成某个局域网节点的地址,从而可以帮助网络超越地址的限制,合理地安排网络中公有 Internet 地址和私有 IP 地址的使用。使用这种通过地址转换访问不同网段信息的 NAT 技术,专用网络上的多台 PC(使用专用地址段,例如 10.0.x.x、192.168.x.x、172.x.x.x)共享单个、全局路由的 IPv4 地址,减少了所需的 IPv4 地址,如图 1 所示。NAT 与防火墙或代理服务器不同,通常 NAT 功能会被集成到路由器、防火墙、单独的 NAT 设备中。

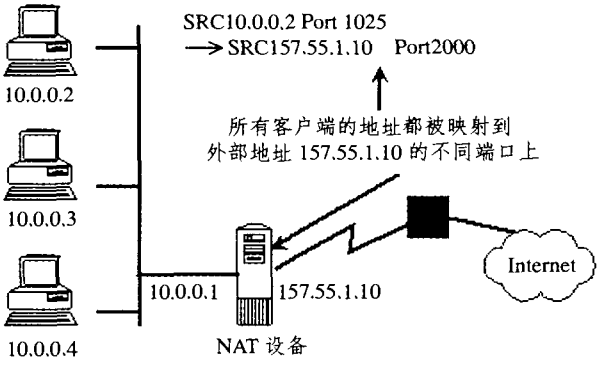

图 1 使用 NAT 设备进行 Internet 通信

2 NAT 穿越及其在应用中的问题

NAT 的作用是:客户机将能在全球 Internet 上与专用 IP 地址进行通讯,而应用程序或客户机却无需做任何额外的工作。这意味着应用程序不必调用额外的 API,客户机也不必执行附加的配置。但是,并非所有网络应用程序都使用能与 NAT 协同工作的协议。解决 NAT 问题已经成为业界的一项重要任务,"NAT 穿越"对于解决由 NAT 引起的连接问题是一种较为全面的解决方案。

"NAT 穿越"是这样一组功能:它允许网络应用程序能明确自己位于 NAT 设备的后面,获得外部 IP 地址,并将端口映射配置为将 NAT 外部端口的数据包转发给应用程序所用的内部端口,而所有这些都是自动完成的,因此用户不必手动配置端口映射或其他类似的方面。虽然"NAT 穿越"可以解决一些 NAT 问题,但它不是万能药,不能解决所有问题。"NAT 穿越"在应用时也会带来一些问题。

以下通过一个例子说明 NAT 在应用中带来的 NAT 穿越问题,如图 2 所示。

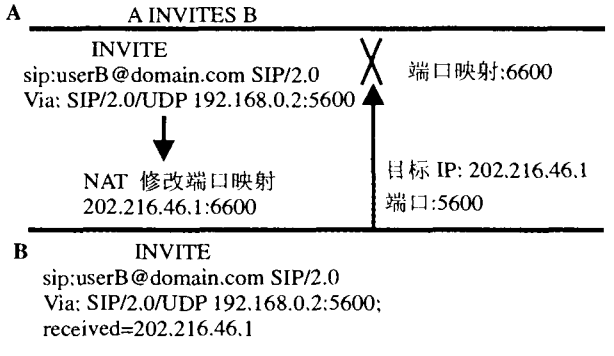

图 2 问题举例

1)内网节点 A 向在外部 Internet 的 B 发出邀请即 A INVITES B—INVITE sip:userB@domain.com SIP/2.0 Via:SIP/2.0/UDP 192.168.0.2:5600;

2)该信息通过 NAT 后源地址和端口被改写为:202.216.46.1:6600,B 接收到该信息—INVITE sip:userB@domain.com SIP/2.0 Via:SIP/2.0/UDP 10.1.1.1:4540;re-

白伟华 硕士研究生,主要研究方向:计算机网络、电子商务。李吉桂 教授,硕士生导师,主要研究方向:计算机网络、电子商务、多媒体技术。

ceived=68.44.20.1;但在接收到的信息中 Via 部分地址依然为:192.168.0.2:5600,B 直接往该地址和端口 192.168.0.2:5600 发回复信息;

3)由 B 发的回复数据包被发送到源地址以及 Via 中所提供的端口,即被发送到 202.216.46.1:5600 中。然而地址映像在 NAT 中记录为 202.216.46.1:6600,由于端口(Port)不一致,故该数据包将被 NAT 过滤掉。

3 实现 NAT 穿越的解决方案

为了实现 NAT 穿越,最早出现了将 ALG[2] 放到 NAT 中,即网络地址转换/应用层网关(NAT/ALG)方式去解决 NAT 穿越问题。这个方式是最简单的一种 NAT 穿越解决方案,但是该方式可扩展性不强,每增加一种应用都需要对相应的 ALG 设备进行升级;使得 NAT 设备的负担更加繁重,跟不上速度太块的 Client,每一个应用都需要单独的实现,影响 NAT 穿越的效率和性能;对于在用中的大量 NAT 的升级改造工作非常困难。

与 NAT/ALG 不同的是,MIDCOM[2](the Middlebox Communications protocol 中间合协议)的框架结构是采用可信的第三方(MIDCOMAgent)对 Middlebox(NAT/FW)进行控制的机制,应用业务识别的智能也由 Middlebox 转移到外部的 MIDCOM Agent 上,因此应用协议对 Middlebox 是透明的。MIDCOM 技术的优势在于可扩展性强,新增应用只需对 MIDCOM Agent 进行扩展,而不会导致 MIDBOX 重新升级。随着 MIDCOM 协议的不断成熟和发展,该方式将获得越来越多的应用前景。

代理(Proxy)技术[2]也是目前比较流行的一种 NAT 穿越解决方案。代理方式在网络中部署的位置也比较灵活,既可以应用于私网内部,也可以应用于公网和私网边缘或公网,无需现有 NAT 做任何改动,可采用普通的设备。然而,使用代理技术时每增加一种新的应用就需要对代理设备进行协议扩展。此外,代理设备需同时对信令和媒体进行中继转发,工作效率和转发速度会受影响,而且还不可避免地增加了数据包的时延和丢包可能性。

3.1 使用 STUN 方式解决 NAT 穿越问题

STUN[3](Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)),即 UDP 对 NAT 的简单穿越方式。在这种方式中,它必须包括 STUN Client——可以是运行在用户终端的系统上,如用户的计算机,也可以是运行在网络设备中,相当于一个应用程序;STUN Server——用以接收和回复 STUN Client,通常放置在公共网络中。使用 STUN 无需对现有 NAT 设备做任何改动。

STUN 应用模型如图 3 所示。STUN Client 先向 NAT 外的 STUN Server 以 UDP 数据包的形式发送请求 STUN 消息。当在公网上的 STUN Server 收到该请求消息后,STUN Server 回复响应消息,并将请求消息的源端口放在该响应消息中,即 STUN Client 通过 NAT 后被映像的外部端口。接着响应消息穿越 NAT 发送到 STUN Client,STUN Client 检查响应消息数据包,并获得其在 NAT 上对应的外部地址,然后将该外部地址填入以后呼叫协议的 UDP 负载中告知通讯端,以后通讯时的 RTP 接收地址和端口为 NAT 对外的地址和端口。通过上述过程,STUN 协议可以在相应的 NAT 上预先建立媒体流的 NAT 映像表项,这样使得媒体流可顺利穿越 NAT。

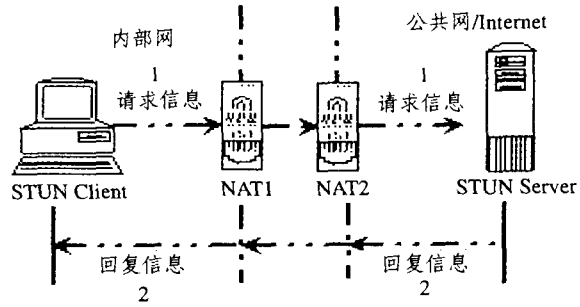

图 3 STUN 应用模型

STUN 方式最大的优点是无需现有 NAT 设备做任何改动。由于实际应用中,已有大量的 NAT,而且这些 NAT 并不支持 VoIP 的应用,若采用 STUN 方式无需改动 NAT,这是其最大的优势,同时 STUN 方式可在多个 NAT 串联的网络环境中使用,但 MIDCOM 方式则无法实现对多级 NAT 的有效控制。但是 STUN 不支持 TCP 连接的穿越,因此不支持 H323 应用协议。STUN 方式不支持 NGN 业务对防火墙的穿越,不支持对对称 NAT(Symmetric NAT)类型的穿越。而在安全性要求较高的企业网中,出口 NAT 通常是对称 NAT 类型;这就是 STUN 的局限性。

3.2 使用 TURN 方式解决 NAT 穿越问题

TURN[4](Traversal Using Relay NAT),即通过 Relay 方式穿越 NAT。TURN 与 STUN 在结构上和实现过程上都相类似,同样也包括了内网的 TURN Client 和公共网的 TURN Server。

TURN 应用模型如图 4 所示。TURN 的实现过程类似于 STUN,不同的是 STUN 方式获得的地址是 NAT 转换后对外的 IP 地址和端口,TURN 方式获得的地址是 TURN Server 的 IP 地址和端口,即 STUN 在给用户的数据包中填写的是 NAT 转换后的 IP 地址和端口,而 TURN 则是使用 TURN Server 的 IP 地址和端口发给用户,作为内网与外网节点通讯的 IP 地址和端口。

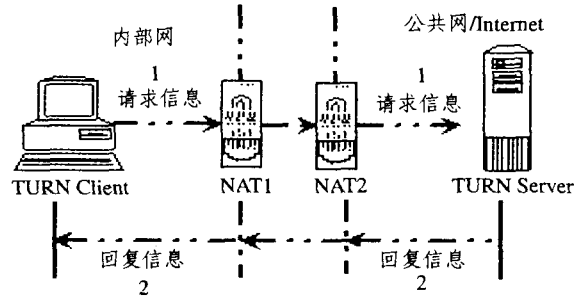

图 4 TURN 应用模型

由此可知,TURN 方式由于在对称 NAT 不会产生新的地址映像,从而可顺利实现对称 NAT 穿越,TURN 解决了 STUN 中不能实现对称 NAT 穿越和不支持对防火墙设备穿越的缺点,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

(下转第 222 页)

$(mt), prob'(\Sigma(mt)))\rightarrow C'$，其中：$\Sigma(mt)=Y_{t\in T}A_1(t)\ Y_{t\in T}A_2(t)\ Y_{t\in T}A_3(t)$，

$A_1(t)=Y_{(s\in LS(t))\cap(s\in C)}exit(s)$，

$A_2(t)=action(t)$，

$A_3(t)=Y_{(S\in AS(t))\cap(s\in C')}entry(s)$，

$prob'(\Sigma(mt)=ProbEv(t)\times\sum_{t\in T}(ProbCond(t))$

6)转到2)，直到所有的事件 $e\in EventS$ 都遍历完毕，得到 C 对应的迁移集合 MT^C

7)添加转移 $mt=(C1,\Sigma(mt),proc'(\Sigma(mt)))\rightarrow C2$，其中：

$C1=C2=C;\Sigma(mt)=\bigcup s\in Cdo(S)$，$\Sigma(mt)$代表在 C 中的 do 动作集合，$prob'(\Sigma(mt))=1$。将迁移 mt 加入迁移集合 MT^C。

8)将迁移集合 MT^C 中的所有迁移 mt 上的概率 $prob'(\Sigma(mt))$进行归一化得到 $prob(\Sigma(mt))$

9)转到1)，直到所有的状态 C 都遍历完毕。

图4是由扩展的UML状态图3转换而来的使用模型。

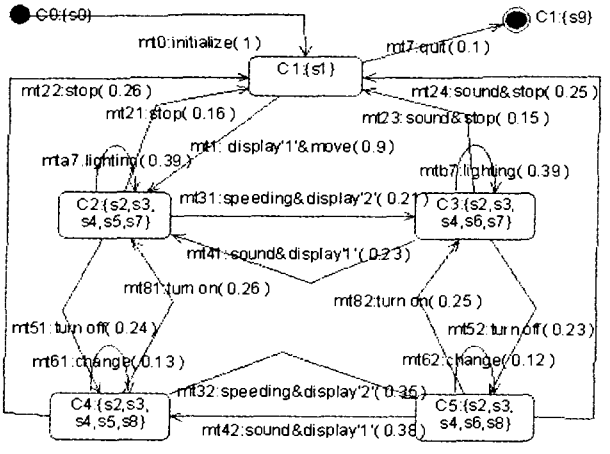

图4 GoForward用案导出的使用模型

5.2 集成系统使用模型的算法

输入：系统的用案集合，对应的使用模型集合

1)取下一个用案 U，取得用案 U 在成功执行后系统进入的状态 $U.PostCond$

2)任取一个用案 U'，$U'\neq U$，取得用案 U' 前置条件集合 $U'.PreCond$

3)如果 $U.PostCond=U'.PreCond$，则将 U 导出的使用模型 $UsageModel^U$ 的结束状态 F 和 U' 导出的使用模型 $UsageModel^{U'}$ 的初始状态 S_0 合并。

4)转到步骤1)，直到所有用案遍历完毕。

6 测试用例的生成与执行

测试用例的生成依赖于测试所使用的模型。利用使用模型，最小覆盖和随机测试用例可由CASE工具[9]自动生成。模型覆盖测试确保了在随机测试开始之前模型的最低功能，而随机测试为投入运行时的可靠性评估提供了依据。

测试用例的执行，应首先构建系统的仿真激励环境，每个仿真脚本(simulation script)对应与使用模型中不同的迁移；然后把测试用例集合翻译为测试脚本(test script)。测试用例的执行就是测试脚本的执行过程。

结束语 本文将UML模型和统计测试有机地结合起来，提出了一种基于UML模型的统计测试方法，通过从UML导出使用模型解决了统计测试中使用模型建立困难的问题。本文首次给出了从用案和状态图模型导出并集成使用模型的形式化算法。该方法增强了统计测试的可行性、可测试性，并降低了对软件系统，尤其是复杂系统进行统计测试的难度。本文正在进行的、以及今后的工作主要在于：

(1) 通过扩展RationalRose，将本文方法软件化，构建基于UML模型的统计测试CASE工具平台。

(2) 在UML模型中扩展时间限制，增加对实时软件测试的支持。

(3) 进一步扩展UML模型，增加对分布式软件计测试的支持。

参 考 文 献

1 颜炯，王戟，陈火旺. 基于模型的软件测试综述. 计算机科学，2004，31(2)

2 Briand L, Labiche Y. A UML-Based Approach to Sysyem Testing: [Carleton University TR SCR-01-01-Version 2]. 2002

3 Riebisch M, Philippow I, et al. UML-Based Statistical Test Case generation. LNCS 2591, Springer, 2003

4 Chevalley P, Thevenod-Fosse P. An Empirical Evaluation of Statistical Testing Designed from UML State Diagrams: the Flight Guidance System Case Study. IEEE. 1071-9458/01, 2001

5 Basanieri F , Bertolino A. A Practical Approach to UML-Based Derivation of Integration Tests. In: Proc. 4th Intl. Software Quality Week Europe, Brussels, Nov. 2000. 20～24

6 Yan Jiong, Wang Ji, Chen Huo Wang. Deriving Software Statistical Testing Model from UML Model. In: Proc. of the Third Intl. Conf. on Quality Software, QSIC03, 2003

7 Kim Y G, Hong H S, Bae D H, et al. Test cases generation from UML state diagrams. IEEE Proc-softw, Aug. 1999, 146(4)

8 Hubner M, Philippow I, et al. Statistical Usage Testing Based on UML. IEEE, 2003

9 Prowell S J. Jumbl. A Tool for Model-Based Statistical Testing. In: Proc. of the 36th Hawaii Intl. Conf. on System Sciences (HICSS03), 2003

(上接第45页)

省按RTP端口号加1发送)。但是，使用TURN方式时，内网对外网的所有数据包都必须通过TURN Server转发，这样TURN Server负担就比较重，增大了包的延迟，效率会降低，同时丢包率也升高了。

结束语 虽然NAT技术已经被广泛应用到各个领域，但在使用NAT技术时解决NAT穿越是个不可避免的问题，我们必须先要清楚知道NAT技术使用的环境、所用的NAT的类型，然后使用适合自己网络环境的NAT穿越方案。

参 考 文 献

1 Srisuresh P, et al. IP Network Address Translator(NAT) Terminology and Considerations [S]. RFC 2663, IETF issue, Aug. 1999

2 严军. NGN网络业务NAT穿透技术探讨[S]. 通信世界网，总第133期 http://www.cww.net.cn/cwwservice/Weekly/Article.asp? SpecialId=163&SpecialRowId=302&Id=8567

3 Takeda Y. Symmetric NAT Traversal using STUN. draft-takeda-symmetric-nat-traversal-00 (work in progress), June 2003

4 Rosenberg J , et al. Traversal Using Relay NAT(TURN). draft-rosenberg-midcom-turn-05 (work in progress), July 2004