基于 UDP 交换路由的 NAT 互联技术研究*)

张建伟[1,2] 蔡增玉[2] 郭云飞[1] 贺 蕾[2]
(信息工程大学国家数字交换系统工程技术研究中心 郑州 450002)[1]
(郑州轻工业学院计算机与通信工程学院 郑州 450002)[2]

摘 要 在对 NAT 互联技术的深入研究基础上,提出了一种基于 UDP 交换路由器的 NAT 互联技术,对其中的信息格式和工作流程进行了深入研究,并通过使用 SIP 协议的例子对其进行了详细论述和分析。新方案克服了 TURN 存在的 TURN 服务器瓶颈问题,能够提高穿越的效率以及改进实际部署的可行性。同时,本方案采用了 RID,SID 和 DID 来确定对等会话端的位置,这是身份标识和路由标识分离的一种体现,能很好地解决向下一代网络过渡过程中 NAT 设备的有效性问题。

关键词 UDP 交换,路由,NAT 互联,NAT 穿越

Research on NAT Interconnection Based on UDP Switch Router

ZHANG Jian-wei[1,2] CAI Zeng-yu[2] GUO Yun-fei[1] HE Lei[2]
(National Digital Switching System Engineering & Technological Research Center, Information Engineering University, Zhengzhou 450002, China)[1]
(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)[2]

Abstract A new NAT Interconnection method based on UDP switch router has been presented. Firstly, the paper gives the message format using and protocol operation. Then, an example using SIP protocol has been discussed and analyzed in detail. The new method avoids the bottle-neck of TURN protocol on TURN server, and can improve the efficiency of communication between NATs. On the other hand, using of RID, SID and DID is the application of separating router identifier and session identifier, so our method can resolve the validity of NAT equipment during the transition to NGN.

Keywords UDP switch, Router, NAT interconnection, NAT traversal

1 引言

随着互联网的普及,连接在互联网上的计算机越来越多,人们开始意识到 IP 地址资源匮乏的问题。为了满足人们对 IP 地址资源的需求,产生了网络地址转换(NAT)技术[1]。NAT 通过端口映射技术,使得私网中的结点不需要一个真正可寻址的 IP 地址也能访问 Internet。NAT 的出现,一定程度上缓解了对 Internet 地址空间的需求。但是,私网结点必须先主动建立与 Internet 服务器端的连接,两者才能正常通讯,反方向的连接建立请求则是不允许的。为此,人们对如何穿越 NAT 进行了大量研究,并取得了一系列研究成果,如 AIG[2],MIDCOM[3],STUN[4] 和 TURN[5] 等,但是仍存在许多问题。

本文在对 STUN,TURN 协议草案进行深入研究与分析的基础上,提出了一种基于 UDP 交换路由器的 NAT 的互联解决方案,与现有的 STUN 和 TURN 相比,新方案利用 UDP 交换路由器而不需要专用的服务器,能够提高穿越的效率以及改进实际部署的可行性。

2 NAT 互联技术

为了实现 NAT 穿越,出现了 ALG,MIDCOM,STUN 和 TURN 等技术。其中 STUN 和 TURN 是典型的基于 UDP 实现 NAT 互联的技术,下面简单介绍它们的原理和存在的问题。

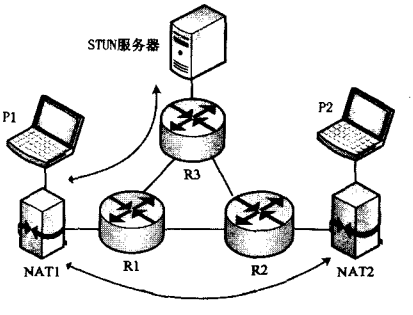

图 1 STUN 原理图

STUN 的运行原理如图 1 所示[4]。P1 要求与 P2 通信,首先,P1 从 STUN 服务器获得它的 NAT 地址,并将该地址发送到同等节点 P2;然后,P2 发送信息给 P1 的 NAT 地址。STUN 方式最大的优点是无需现有 NAT 设备做任何改动,但是 STUN 不支持 TCP 连接的穿越,因此不支持 H. 323 等应用协议,也不支持对称 NAT 的穿越。但是在安全性要求较高的企业网中,出口 NAT 通常是对称 NAT 类型,这就限制了 STUN 的应用范围[6]。

图 2 给出了一个 TURN 运行实例[5]。P1 要求与 P2 通信,在 P1 和 P2 间的任一通信都需要在 TURN 服务器中进行转播。除了具有 STUN 方式的优点外,TURN 还支持基于

*)本文得到国家 973 重点基础研究发展规划(2007CB307100)资助。**张建伟** 博士研究生,副教授,主要研究方向为下一代网络与信息安全;**蔡增玉** 助教,主要研究方向为智能规划与下一代网络;**郭云飞** 教授,博士生导师,主要研究方向为下一代网络关键技术;**贺 蕾** 助教。

TCP的应用，解决了STUN应用无法穿透对称NAT设备的缺陷。其缺点是：内网对外网的发送的所有数据包都必须通过TURN Server转发，这样增大了包的延迟，同时丢包率也会升高，会对通信速度产生影响。另外，在TURN客户端数量很大的时候，TURN Server可能成为系统的瓶颈[6]。

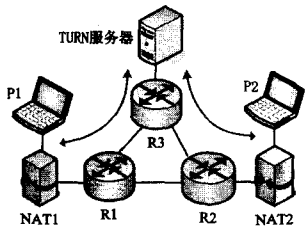

图2 TURN原理图

本文针对STUN，TURN互联方式存在的问题，通过对使用UDP交换路由器来实现NAT互联。使用UDP作为传输层的协议，主要是因为几乎所有的NAT设备很好地支持UDP，并且UDP编程比ICMP要相对容易。

3 基于UDP交换路由的NAT互联

3.1 信息格式

UDP数据包主要包括PING，PONG，OPEN，ACK，SHUT和DATA六类，各种数据包的信息格式如图3，信息类型在UDP报头后的CMD字段中说明。除了DATA信息外，其他的信息包括一个序列号，它是请求和响应的联合，例如PING/PONG，OPEN/ACK。其中表示通信节点位置和身份的信息有：RID（Router Identifier，路由标识）是支持UDP交换的路由器的IP地址；SID（Session Identifier，会话标识）是一个路由器中的特定的交换会话标识；DID（Direction Identifier，方向标识）指示DATA信息来自哪个对等节点，DID-self被用来发起PING和OPEN的主动节点使用，DID-peer被被动节点使用。

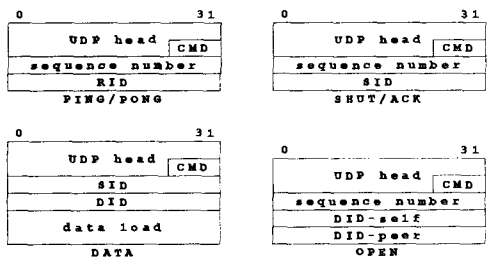

图3 信息格式

3.2 工作流程

基于UDP交换路由的NAT的互联解决方案，克服了STUN和TURN的缺点，利用UDP交换路由技术和应用层的协议，不需要专用的服务器，可实现NAT高效互联。其工作流程主要包含以下五个步骤：

（1）通信发起端获得对等端的NAT地址

任何的节点发送探测信息之前，必须得到对等端的NAT地址。如何得到对等端的NAT地址，在该协议中并没有规定，可以自主选择相应的方式来实现。

（2）获得交换路由地址

得到对等端的NAT地址后，发起端向对等端的NAT地址发送PING信息，UDP数据包的源端口和目标端口都是默认端口号。如果发起端在非活动状态（没有收到任何路由器的响应），这个消息的RID将全为0，表示任何支持UDP交换的路由器可以用一个PONG来响应该PING信息；如果发起端处于活动状态（已经从一些路由器得到了响应），该消息的RID为交换路由器的IP地址，只有交换路由器需要用PONG来响应该消息。为了减少活动状态到非活动状态的转化时间，发起端可以同时发送全0RID和非0RID，这样可以保证当原来的交换路由器不可用时，该传送可以被快速地转化到一个新的可用路由器。当发起端收到带着有效RID的PONG消息并且没有旧的交换路由器时，发起端得到交换路由器。

（3）建立通信会话

发起端发送OPEN消息到交换路由器，OPEN消息的目标IP地址是发送端收到的有效RID，目标UDP端口是默认端口，含有DID-self和DID-peer，用来区分是从发起端到对等端，还是从对等端到发起端。P1发送数据以后，从发起端发出的数据带有DID-self，而从对等端发出的数据带有DID-peer。如果交换路由器同意来自发起端的申请，该路由器将发送一个包含SID的ACK消息，SID用来索引发起端和对等端之间的交换会话。当发起端从来自交换路由器的ACK报文中得到SID后，发起端必须向对等端发送带有SID和DID的INFO消息，INFO消息先被送到SIP服务器，接着被转发到对等端，这样对等端就得到了SID和DID。建立会话后，每个节点即使没有实际通信任务也必须持续地发送空的DATA报文，也就是保持一个单向数据流。

（4）通信开始

交换路由器在收到含有RID目标IP地址、目标UDP端口为默认端口，并且CMD field为DATA的UDP报文时，使用SID作为交换路由表的索引。当在交换路由表中找到有效出口的时候，交换路由器用DID字段比较来输入参数DID-self和DID-peed来确定转发方向，并进行转发。

（5）通信结束，关闭会话

任意一个通信节点要结束通信，可以发送SHUT报文到交换路由器，路由器清理路由表中相关的记录后，向对等节点发送一个SHUT报文。交换路由器也在每个路由表项上保持一个计时器，如果任何一个对等节点在该时间内没有发送数据，则关闭该会话。

4 实例设计分析：使用SIP协议

4.1 网络拓扑结构

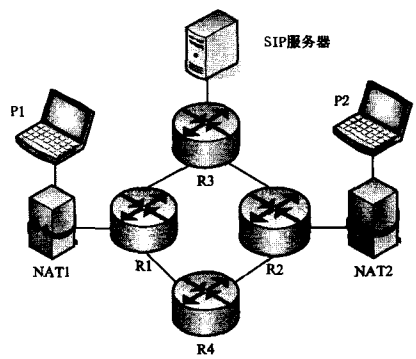

图4 网络模型

在此通过对一个NAT互联网络模型的通信过程的描述，来说明基于UDP交换路由的NAT互联的原理。网络模

型拓扑结构如图 4 所示，其中 R4 是一个支持 UDP 交换的路由器，如果路由是从 NAT2 开始，依次经过 R2，R4，R1 到达 NAT1，那么 P2 到 P1 的通信可以在没有转发服务器的情况下，以常规的单播路由算法实现。

4.2 通信实现细节

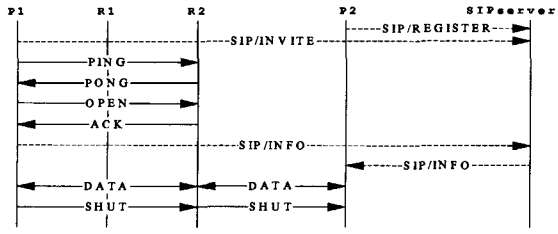

图 5 通信实现流程

现在来详细讨论图 4 所示网络中实现节点 P1 和节点 P2 通信的过程(图 5 所示)，主要分为下面几个步骤：

(1) 节点 A 得到对等端节点 B 的 NAT 地址

本文以 SIP 中的注册方式来实现 NAT 地址注册，通信节点 P1 和节点 P2 通过向公共服务器发送注册信息来注册它的 NAT 地址。为了使一个节点得到它的对等节点的 NAT 地址，引进了一个新的经由参数：paddr。当节点 P1 发送 INTVITE 报文初始化呼叫时，它把 paddr 参数加入到经过链中，经过链指示 SIP 服务器相应一个 NAT 地址或者只公布被叫 IP 地址的可达性。例如：

```
INVITE sip:100@20.1.2.3 SIP/2.0
Via:SIP/2.0/UDP 10.3.4.5;paddr
From:<sip:200@20.1.2.3>
To:<sip:200@20.1.2.3>
Call-ID:321253
CSeq:1 INVITE
```

当 SIP 服务器收到一个带 via-paddr 参数的 INVITE 报文时，它把被叫部分的 NAT 地址放入相应消息中，发给节点 P1。例如：

```
SIP/2.0 200 OK
Via:SIP/2.0/UDP 10.3.4.5;paddr=30.7.8.9
From:<sip:100@20.1.2.3>
To:<sip:200@20.1.2.3>
Call-ID:321253
CSeq:1 INVITE
```

当节点 P1 从来自交换路由器的 ACK 报文中得到 SID 之后，节点 P1 通过在 SIP INFO 信息向节点 P2 发送 SID 和 DID，在 SIP INFO 信息中引入了内容类型：application/x-udp-switch，例如：

```
INFO sip:100@20.1.2.3 SIP/2.0
Via:SIP/2.0/UDP 10.3.4.5
From:<sip:100@20.1.2.3>
To:<sip:200@20.1.2.3>
Call-ID:321253
CSeq:5 INFO
Content-Length:20
Content-Type:application/X-udp-switch
SID=927741
DID=538874
```

INFO 报文首先被送到 SIP 服务器，接着被转发到节点 P2。由于 Internet 中的非对称路由，节点 P2 必须自己完成 PING 和 OPEN 过程，节点 P1 和节点 P2 的交换路由器可能不同。例如在图 4 中，如果从 NAT2 到 NAT1 的路由是 R2⇒R4⇒R1，而从 NAT1 到 NAT2 的路由是 R1⇒R3⇒R2，其中 R3 和 R4 是支持 UDP 交换的路由器，因此从 P1 到 P2 通信要由 R3 交换，而从 P2 到 P1 通信要由 R4 来交换。

(2) 通信节点得到自己的交换路由标识

节点 P1 得到节点 P2 的 NAT 地址之后，节点 P1 向节点 P2 的 NAT 地址发送 PING 信息，UDP 数据报的源端口和目标端口都是 56789(假设在发送和接收端都使用 56789 作为默认端口号)。假设节点 P1 在非活动状态，这个消息的 RID 将全为 0；交换路由器 R1 收到节点 P1 的 PING 信息后，向节点 P1 发送带着一个有效 RID 的 PONG 消息作为响应；节点 P1 把 R1 地址作为路由地址。由于 Internet 中的非对称路由，因此节点 P2 必须自己完成 PING 和 OPEN 过程。节点 P1 和节点 P2 使用的交换路由器可能不同。

(3) 建立会话

节点 P1 发送 OPEN 消息到 R1 上，目标 IP 地址是该有效 RID，目标 UDP 端口是 56789。OPEN 消息中含有 DID-self 和 DID-peer，用来区分是从 P1 到 P2 还是从 P2 到 P1。以后，从 P1 发出的数据带有 DID-self，而从 P2 发出的数据带有 DID-peer。如果交换路由器同意来自节点 P1 的申请，该路由器将发送一个包含 SID 的 ACK 消息，SID 用来索引 P1 和 P2 之间的交换会话。交换路由器 R1 处理消息的过程如下：

```
    void RusForwadData(msg)
{
  u_int32_t SID=msg.SID;
  if (Rustab[SID].flag==VALID){
    if (msg.DID==RusTab[SDI].DIDself){
      msg.SrcAddr=RID;
      msg.SrcPort=56789;
      msg.DstAddr=Rustab[SID].Addrpeer;
      msg.DstPort=RusTab[SID].Portpeer;
    } else
    if (msg.DID==Rustab[SID].DIDpeer){
      msg.SrcAddr=RID;
      msg.SrcPort=56789;
      msg.DstAddr=Rustab[SID].Addrpeer;
      msg.DstPort=RusTab[SID].Portpeer;
    } else
      returen;
    send(msg);
  }}
```

上面的伪代码显示一个数据消息在 UDP 交换路由器的处理过程，交换路由器在收到含有 RID 目标 IP 地址、目标 UDP 端口为 56789，并且 CMD field 为 DATA 的 UDP 报文时，调用该函数。

(4) 通信开始

节点 P1 和节点 P2 建立会话后，两者开始通信，传送的数据不需要应用服务器参与。

(5) 关闭会话

如果节点 P1 或者 P2 想关闭该交换会话，它们中的任意一个可以发送 SHUT 报文到交换路由器，路由器清理路由表中相关的记录后，向对等节点发送一个 SHUT 报文。交换路由器也在 R1 和 R2 对应路由表项上保持一个计时器，如果任何一个对等节点在该时间内没有发送数据，则关闭该会话。

说明：在本例中以 SIP 中的注册方式来实现，即每一个节点通过向公共服务器发送注册信息来注册它的 NAT 地址。在通信过程中用到 SIP 协议的步骤情况主要有：

(1) P2 发送 REGISTER 报文到 SIP 服务器发布它的 NAT 地址；

(2) P1 通过发送带地址参数的 INVITE 信息从 SIP 服务器得到 P2 的 NAT 地址；

(3) P1 通过 INFO 发送 SID 和 DID-peer 到 SIP 服务器，以便 P2 可以找到 P1；

(4) SIP 服务器转发 INFO 到 P2，以使 P2 能在以后的交换中使用 SID 和 DID-peer。

结束语 本文提出了一种基于 UDP 交换路由器的 NAT

互联技术。通过在普通路由器的IP路由进程中增加少量的附加处理，新方案克服了STUN存在的不足，能使传递给路由器的所有通信都不需要服务器转播，因此能显著地减少网络通信开销，也避免了出现STUN服务器的瓶颈问题。另外，该方案中采用了RID和SID之间的映射来确定对等会话端的位置，SID和DID确定会话及其转发方向，是身份标识和路由标识分离的一种体现，能很好地解决向下一代网络过渡过程中NAT设备的有效性问题。

参考文献

[1] Egevang K, Francis P. The IP network address translator (NAT) [S]. RFC1631, May 1994

[2] Biggs B. A SIP application level gateway for network address translation[S]. IEFF issues, March 2000

[3] Srisuresh P, Kuthan J, Rosenberg J. Middlebox communication a-rchitecture and framework [S]. RFC3303, August 2002

[4] Rosenberg J, Weinberger J, Huitema C, et al. STUN - simple traversal of user datagram protocol (UDP) through network address translators (NATs) [S]. RFC3489, March 2003

[5] Rosenberg J, Mahy R, Huitema C. Traversal using relay NAT (TURN) [EB/OL]. http://draft-rosenberg-midcom-turn-08, September 2005

[6] 白伟华，李吉桂. NAT技术及其穿越方案研究[J]. 计算机科学，2005，32(8)：44-45

[7] Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol [S]. RFC3261, June 2002

[8] 陈晓铭，吴中福，等. 基于ICE方式H.323信令穿越Symmetric NAT技术研究 [J]. 计算机科学，2006，33(8)：82-85

(上接第47页)

仿真结果表明，无论是场景1(图6)还是场景2(图7)，采用本文提出的基于效用的呼叫接纳控制与流量均衡策略时，网络的总效用都是最大的。不是基于效用的或者没有流量均衡的呼叫接纳控制策略都会使网络的总效用降低，而采用既不基于效用又不含流量均衡的简单的呼叫接纳控制策略时，网络的总效用是最低的。

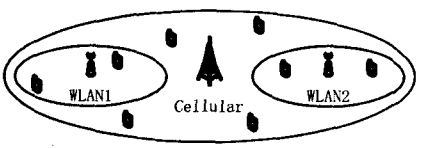

图5 仿真中的小区结构

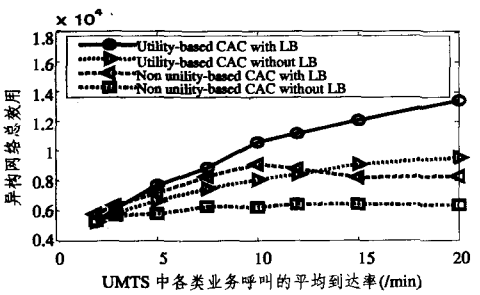

图6 场景1下的异构网络总效用对比

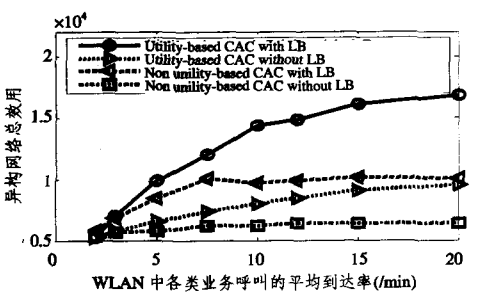

图7 场景2下的异构网络总效用对比

结束语 本文提出了一种基于效用的呼叫接纳控制及流量均衡策略，该策略利用物理层和链路层反馈的参数对两种网络性能的分析与预测，并结合应用层对各类业务定义的效用函数，利用跨层信息进行决策，从而达到最佳的呼叫接纳控制和流量均衡的效果。效用函数的引入保证了各类业务都能获得一定的满意度，而在下层对网络性能的分析与预测保证了所采取策略的准确性，在此基础上的流量均衡策略也避免了两种网络的负载差别过大而带来总收益的损失，仿真结果表明本文提出的策略可以使异构无线网络中所有呼叫的效用总和最大。

参考文献

[1] Song Wei, Zhuang Weihua, Cheng Yu. Load balancing for cellular/WLAN integrated networks [J]. IEEE Network, 2007, 21 (1): 27-33

[2] SKEHILL R, BARRY M, KENT W, et al. The common RRM approach to admission control for converged heterogeneous wireless networks [J]. IEEE Wireless Communications, 2007, 14 (2): 48-56

[3] MURRY K, PESCH D. Call Admission and Handover in Heterogeneous Wireless Networks [J]. IEEE Internet Computing, 2007, 11 (2): 44-52

[4] Chen Bin Bin, Chan M C. Resource Management in Heterogeneous Wireless Networks with Overlapping Coverage [C]. Comsware'06, Jan. 2006: 1-10

[5] FALOWO O E, CHAN H A. Joint Call Admission Control for Next Generation Wireless Network [C]// Canadian Conference on Electrical and Computer Engineering. May 2006: 1151-1154

[6] Ning Guqin, ZHU Guangxi, Peng Liexin, et al. Load Balancing Based on Traffic Selection in Heterogeneous Overlapping Cellular Networks [C]// The First IEEE and IFIP International Conference in Central Asia on Internet, Sept. 2005: 26-29

[7] Yu Fei, KRISHNAMURTHY V. Optimal Joint Session Admission Control in Integrated WLAN and CDMA Cellular Networks with Vertical Handoff [J]. IEEE Transactions on Mobile Computing, 2007, 6 (1): 126-139

[8] CHATTERJEE M, Lin Haitao, DAS S K. Rate Allocation and Admission Control for Differentiated Services in CDMA Data Networks [J]. IEEE Transactions on Mobile Computing, 2007, 6 (2): 179-191

[9] 陈明欣，朱光喜，刘干. WLAN中基于效用的呼叫接纳控制策略. 电子学报(录用待发)，2008