综合 UDP 打洞与 Http 代理的 SIP 穿越 NAT 方案

周 敏[1],余慕春[2],黄维丰[3]
(1. 南京航空航天大学 计算机科学与技术学院,江苏 南京 210016;
2. 南京航空航天大学 航空宇航学院,江苏 南京 210016;
3. 中兴通讯有限公司 中兴网信科技有限公司,江苏 南京 210012)

摘 要:软交换是下一代网络中的核心技术,SIP 协议作为下一代网络最重要的协议之一,已经被广泛应用于 VoIP 系统中。SIP 协议无法支持 SIP 信令和媒体流的 NAT 穿越,从而限制了其在广域网上的应用和发展。虽然目前解决 NAT 穿越的方案已经很多,但都存在着一定的局限性。文中详细解释了 NAT 对 SIP 通信的影响,介绍了 UDP 打洞技术的基本原理,介绍了 UDP 打洞技术穿越锥形 NAT 的流程,以及 Http 代理网关方式穿越各种 NAT 的流程。文中通过比较各种 NAT 穿越方案的优缺点,提出一种综合 UDP 打洞与 Http 代理网关的 NAT 穿越方案。经过论证与实验,证明了该方案的可行性。

关键词:初始会话协议;NAT;UDP 打洞;STUN;Http 隧道
中图分类号:TN915 **文献标识码**:A **文章编号**:1673-629X(2014)08-0147-05
doi:10.3969/j.issn.1673-629X.2014.08.034

Solution of NAT Traversal in SIP Integrated UDP Hole Punching and Http Proxy

ZHOU Min[1], YU Mu-chun[2], HUANG Wei-feng[3]
(1. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China;
2. College of Aerospace Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China;
3. ZTEICT, ZTE Corporation, Nanjing 210012, China)

Abstract: Soft switch is the core technology of next generation network. SIP protocol as one of the most important protocols in the next generation network, has been widely used in VoIP systems. SIP protocol can't support SIP signaling and media stream through NAT, which limits its application and development in the WAN. Although there are many NAT traversal solutions, every solution has limitations. In this paper, explain the impact of NAT on the SIP communication in detail, introduce the basic principle of UDP hole punching technology, the process of using UDP hole punching through the cone NAT and using the Http proxy gateway through various NAT. Compared the advantages and disadvantages of various NAT traversal solutions, present a NAT traversal solution which integrates UDP hole punching and Http proxy gateway technology. After the argument and experiment, it proves the scheme is feasibile.

Key words: SIP; NAT; UDP hole punching; STUN; Http tunnel

0 引 言

SIP[1](Session Initiation Protocol)是一个应用层的信令控制协议,用于创建、修改和释放一个或者多个参与者的会话。基于分组的多媒体通信系统的 SIP 协议已经被广泛应用于 IP 电话和视频会议中。由于 IP 地址紧缺以及网络安全等原因,企业网和驻地网基本上都采用了 NAT[2](Network Address Translator)技术,使得企业内部可以共用一个或若干个有效的公网 IP 地址连接到公网中。然而,NAT 设备工作在网络层和传输层,NAT 只能对报文中网络层和传输层的信息做修改,而无法修改应用层中携带的内网地址信息,SIP 客户端和 SIP 服务器根据 SIP 信令中的相关 IP 地址进行寻址,内网 IP 地址是一个不可路由的 IP 地址,

收稿日期:2013-10-11 **修回日期**:2014-01-16 **网络出版时间**:2014-05-21
基金项目:江苏省研究生培养创新工程项目(CXLX13_134)
作者简介:周 敏(1989-),男,硕士研究生,研究方向为人工智能。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140524.2149.012.html

最终导致寻址不正确,从而媒体通道无法建立。

目前,解决 SIP 穿越 NAT 的方案主要有 STUN[3](Simple Traversal of UDP through NAT)、TURN(Traversal Using Relay NAT)、MIDCOM(Middlebox Communication)、SBC(Session Border Controller)、ALG(Application Level Gateway)、Http 代理等,但以上方案各有优缺点,都存在一定的局限性。在下一代 NGN 网络的部署中,应当尽可能保留运营商和用户现有的设备,尽量不更换目前已经广泛部署在网络中的各种设备。MIDCOM、ALG 方案需要升级 NAT 设备和防火墙策略,作为 VoIP 网络电话供应商去升级客户企业网络的 NAT 是不切实际的,尤其对于一些保密严格的单位,更不可能允许其他单位修改 NAT 设置,因此不能满足需求。STUN、TURN、SBC、Http 代理模式方案都可以不更改企业网 NAT 就能实现 SIP 的 NAT 穿越,有利于保护企业的投资和隐私,有利于促进 VoIP 网络的广泛部署。TURN、SBC、Http 代理模式方案都是通过 Relay 方式实现 SIP 媒体流的 NAT 的穿越。其中,TURN 和 SBC 只能以 UDP 方式实现 SIP 穿越 NAT,一些限制比较严格的企业网络的 NAT 不允许 UDP 方式传输数据,甚至只允许 TCP 报文通过 80 或 443 端口传输数据,因此,TURN 和 SBC 无法穿越这种企业网络的 NAT。

文中综合考虑各种穿越方案的优缺点,利用 STUN 技术实现 NAT 的类型判断,提出一种综合 UDP 打洞技术[4]和 Http 代理模式的 NAT 穿越新方案,是一种可以穿越各种 NAT 及其防火墙的综合解决方案。该方案以不需要对 NAT 升级改造为前提,实现了对各类 NAT 及其防火墙的穿越。

1 NAT 对 SIP 通信的影响

使用 NAT 技术时,同一个内网的终端之间可以正常通讯,但内网与外网终端之间进行 SIP 通信时就会出现问题[5]。首先,外网终端无法呼叫内网终端;其次,内网终端呼叫外网终端时 SIP 信令可以传输成功,但内网终端却不能收到外网终端发送的媒体报文,内网客户端不能听到外网客户端的语音,但外网客户端能听到内网客户端的语音,即电话单通。这是因为路由设备只能把报文发送到具有可路由的 IP 地址的终端处,由于相同内网的 IP 地址也是可路由的,所以位于 NAT 后的终端之间可以相互发起呼叫,然而内网终端的 IP 地址是私有的,对外网来说又是不可路由的,因此 NAT 后的终端不能接收到位于 NAT 之外的终端的呼叫。

下文分别对内网呼叫外网和外网呼叫内网两种情况进行详细讨论[6-7]。

1.1 内网终端 A 呼叫外网终端 B

如图 1 所示,内网终端 A 以私有地址(192.168.1.10)通过代理服务器 SA 在重定向服务器上完成注册,外网终端 B 以外网地址(200.100.50.25)通过代理服务器 SB 在重定向服务器上完成注册。内网终端 A 发送的 Invite 消息中携带的 SDP[8](Session Description Protocol,会话描述协议)包含了自身的 IP 地址(192.168.1.10)和接收媒体流的端口,该消息通过 NAT 设备之后发往代理服务器 SA,代理服务器 SA 向重定向服务器转发 Invite,重定向服务器响应的 302 报文中包含了用户 B 的代理服务器 SB 的位置,代理服务器 SA 将 Invite 报文发给代理服务器 SB,代理服务器 SB 再将 Invite 报文发给外网用户 B。

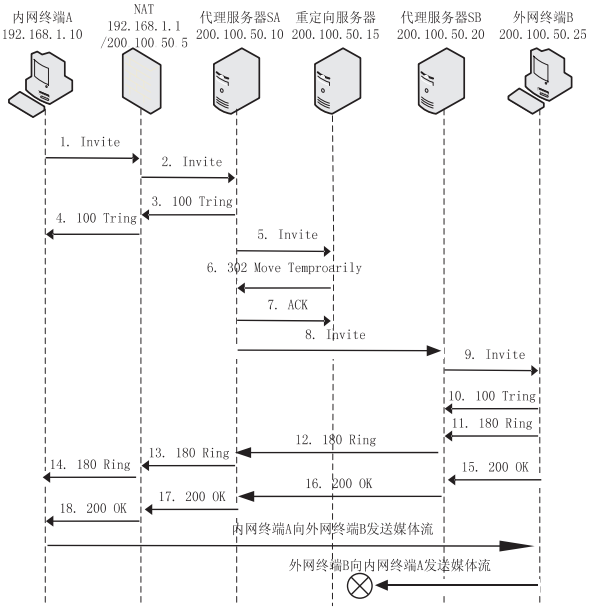

图 1 内网终端 A 呼叫外网终端 B 的流程图

然后,外网用户 B 向内网终端发送 180 报文和 200 OK 报文,呼叫建立,但是媒体通道并没有完全建立,外网终端 B 发送的 200 OK 报文中所携带的媒体连接 IP 地址是公网的,而内网终端发送给外网终端的 Invite 报文中携带的媒体链接的 IP 地址是局域网内部地址,所以外网终端 B 可以收到内网终端 A 发来的媒体数据,但是外网终端 B 不能成功发送媒体数据到内网终端 A,产生电话单通现象。

1.2 外网终端 B 呼叫内网终端 A

如图 2 所示,当外网终端 B 向内网终端 A 发起呼叫时,由于内网终端 A 在重定向服务器上注册的是内网地址,所以按照图 2 中的流程,当代理服务器 A 向重定向服务器查询内网终端 A 的地址时,得到的是内网地址(192.168.1.10),代理服务器 A 转发该 Invite 报文时,由于该地址在公网上是不可路由的,最终该消息将会被代理服务器 A 丢弃,代理服务器 B 不能得到正确响应,于是此次呼叫因目的地址不可达或超时而无

法建立。

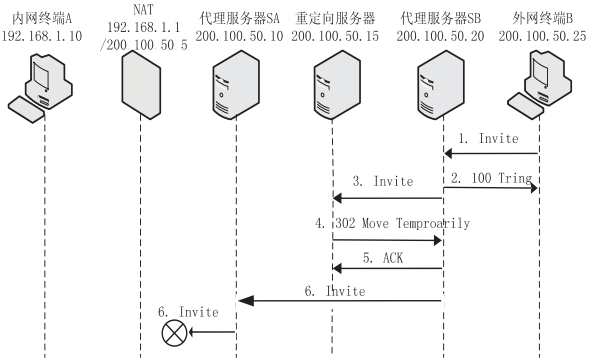

图 2　外网终端 B 呼叫内网终端 A 流程图

2　STUN 技术

STUN 技术可以让客户终端发现自己是否处于 NAT 之后的内网中,并能判定出 NAT 的类型,还能获得内网终端在 NAT 上映射到公网的 IP 地址和端口号。STUN 体系由三个部分组成,STUN Client,NAT 和 STUN Server。STUN Client 通过多次给 STUN Server 发送不同类型请求消息,并根据 STUN Server 的返回消息判定出自己的 IP 地址是不是内网私有地址,如果是内网私有地址则能判断出所经过的 NAT 类型,同时获得 NAT 分配给它的公网 IP 和端口号。STUN Server 的工作是根据 STUN Client 的请求类型返回不同的处理消息[9]。STUN 技术判断 NAT 类型的具体流程参见 RFC 3489[3],文中不再敖述。STUN 技术把 NAT 分为如下几种类型:

2.1　完全锥形 NAT(Full Cone)

完全锥形 NAT 把所有来源于同一个内网私有地址和端口的请求,都映射到同一个外部公网地址和端口。并且,任何外网终端可以通过向映射得到的 NAT 上的外部地址和端口发送数据包,从而将数据包发送到该内部终端。

2.2　受限锥形 NAT(Restricted Cone)

受限锥形 NAT 把所有来源于同一个内网私有地址和端口的请求,都映射到同一个外部公网地址和端口。但是,只有当该内部终端曾经给某个外部终端发送过数据包时,这个外部终端才能够向该内部终端发送数据包,否则 NAT 将丢弃外部终端发来的数据包。

2.3　端口受限锥形 NAT(Port Restricted Cone)

类似于受限锥形 NAT,但限制更加严格。只有当内部终端曾经给某个外部终端的某个特定端口发送过数据包时,这个外部终端才能用这个特定端口向该内部终端发送数据包。

2.4　对称 NAT(Symmetric)

对称 NAT 的限制是最严格的。所有来自于同一个内部终端地址和端口并且要发送到某个特定终端地址和端口的请求将被映射到同一个外部地址和端口。如果同一个内部终端从同一端口上发送了一个数据包,但是目的地址和端口不同,那么将被映射到不同的端口。并且,只有曾经收到内部终端发送的数据包的外部终端才能向该内部终端发送数据包[10]。

3　UDP 协议穿越 NAT 的原理

UDP 穿越 NAT 的方法主要有 Relay 方式、反向连接方式和 UDP 打洞方式。Relay 方式需要服务器中转,反向连接方式是 UDP 打洞方式的一种特例。

3.1　Relay 方式

Relay 实现原理为位于 NAT 之后的两个终端,通过 UDP 方式连接到一个拥有公网 IP 地址的服务器上。两个终端间的通讯由服务器来中转完成。这种方式的优点是安全可靠,实现起来也很简单。但是这种方式效率较低,消耗了服务器的处理能力和网络带宽,同时增加了终端之间的数据传输时间,服务器处理能力有限的时候很容易产生瓶颈。TURN 和 SBC 方案都是通过 Relay 方式实现 SIP 穿越 NAT。

3.2　反向连接方式

终端 A 在 NAT 后面,另一个终端 B 拥有合法公网 IP 地址。终端 B 主动向终端 A 发送连接请求失败后,终端 B 通过服务器 S 来中转一个请求到终端 A,让终端 A 发出一个反向的连接请求到终端 B。终端 A 在收到服务器 S 的要求后,主动发起一个到终端 B 的公网 IP 地址和端口号上 UDP 连接。通过这种“反向连接”的方式,终端 A 与终端 B 就可以相互建立连接了。这种“反向连接”方式只能用于通讯中的一方在 NAT 的后面,如果通讯双方都在 NAT 后面,那么“反向连接”方式就行不通了。

3.3　UDP 打洞方式

通过 UDP 打洞技术可以使处于 NAT 之后的两个终端间直接建立双向 UDP 连接。UDP 打洞技术只能穿越锥型 NAT,但无法穿越对称型 NAT。

如图 3 所示,有两台分别处于各自的内网中的终端:A 和 B;A 处于锥形 NAT 设备 N_1 之后,B 处于锥形 NAT 设备 N_2 之后;S 是一个拥有公网唯一 IP 地址的公共服务器,可以把上述所说的 STUN Server 作为此处的 S 服务器。按照下面三个步骤可以实现 UDP 打洞方式穿越 NAT:

(1)A 和 B 分别向 S 发送 UDP 报文;报文经过 NAT 设备 N_1 和 N_2 将被分别分配临时的外部端口号。

(2)S 将 N_1 和 N_2 的 IP 地址和分配的端口号分别传回给 A 和 B。

(3)A 和 B 通过对方映射在 NAT 设备上的端口直接联系对方。例如,N_1 和 N_2 都是端口限制型 NAT,A

在 N_1 上映射的 IP 地址和端口为 $N_1:port_1$，B 在 N_2 上映射的 IP 地址和端口为 $N_2:port_2$。A 要发送数据到 B，A 直接发送数据到 $N_2:port_2$，数据到达 B 所处网络 NAT 设备 N_2 时，由于 N_2 是端口限制型 NAT，A 发送的数据将被阻止进入。同时，B 也向 A 发送报文，B 直接发送数据到 $N_1:port_1$，B 发送的数据到达 A 所处网络 NAT 设备 N_1 时，由于 A 曾经给 B 发送过数据，B 发送的数据将被 N_1 转发给 A。同理，A 再向 B 发送数据也能被 N_2 转发给 B。至此，A 与 B 之间的 UDP 连接建立成功。由于端口限制锥形 NAT 是锥形 NAT 中限制最严格的，因此对于其他类型的锥形 NAT 也可以用上述方法实现 NAT 穿越。

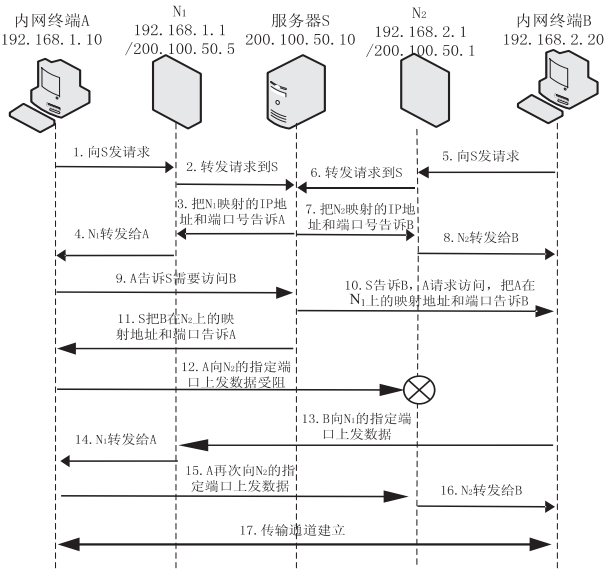

图 3 UDP 打洞流程图

4 综合 UDP 打洞与 Http 代理的穿越方案

UDP 打洞技术可以实现对锥形 NAT 的穿越，使得两个 NAT 之后的终端之间可以直接通讯，但不能用于对称型 NAT 和 UDP 报文受阻的 NAT 穿越。Http 代理方式可以实现对称型 NAT 和 UDP 报文受阻的 NAT 的穿越，即使是只允许 Http 传输的 NAT 也可以实现穿越。结合上述两种穿越方式，对于锥形 NAT 之后的客户端使用 UDP 打洞方式实现，对于对称型 NAT 或者 UDP 报文受阻的 NAT 穿越使用 Http 代理方式，可以实现对所有常见 NAT 和防火墙的穿越。

4.1 UDP 打洞技术穿越处理

内网客户端登陆时，与公网的 STUN Server 交互，最终判别出客户端所在网络的 NAT 类型。如果客户端处于锥形 NAT 之后，则使用 UDP 打洞技术实现 NAT 穿越。具体步骤如下：

1）SIP 信令传输通道建立过程：内网客户端首先用本地收发 SIP 信令的端口向处于公网上的 STUN Server 发送请求报文，STUN Server 在响应报文中告知客户端在 NAT 上映射的 IP 地址和端口号。客户端将发送的 SIP 报文中的本地地址和端口号替换为发送 SIP 信令报文的端口在 NAT 上映射的 IP 地址和端口号。由于客户端首先给 SIP Proxy 发送了 SIP 报文，后期 SIP Proxy 向客户端发送的 SIP 报文也可以直接通过 NAT 到达客户端。为了使客户端在 NAT 上映射的端口保持不变，客户端定期向 SIP Proxy 发送 PUBLISH 报文[11]。至此，SIP 信令传输通道就建立成功了。

2）RTP 和 RTCP 传输通道建立过程：客户端分别用 RTP 和 RTCP 的收发端口向 STUN Server 发送请求，分别得到客户端收发 RTP 和 RTCP 的端口在 NAT 上映射的端口号。客户端发送含有 SDP 描述的 SIP 报文时，将 SDP 中的 c 字段的连接地址替换为 NAT 的 IP 地址，将 SDP 中的 m 字段中的端口号替换为客户端收发 RTP 报文端口在 NAT 上映射的端口。在 SDP 描述中添加‘a=rtcp:’字段，指定 RTCP 接收的端口号为客户端收发 RTCP 端口在 NAT 上映射的端口号（例如：‘a=rtcp:12345’）。通过 SDP 描述将 NAT 上映射的 RTP 和 RTCP 的 IP 地址、端口号告诉会话的另一终端，同样会话的另一终端也会通过 SIP 中的 SDP 描述告知本地客户端在其 NAT 上映射的媒体连接地址和端口号。两个客户端之间通过 3.3 中介绍的 UDP 打洞技术实现媒体数据的 NAT 穿越。

4.2 Http 代理方式穿越处理

4.2.1 Http 代理方式穿越原理

Http 代理穿越 NAT 方式是利用 Http 隧道[12-13]绕过防火墙端口屏蔽的穿越方式。一般的防火墙上都开放了 80 和 443 端口，按照 Http 协议规定的方式在 Http 信令的应用协议数据单元中携带 SIP 信令和媒体数据，且不需要再添加其他的 NAT 规则，因而不会对客户所在的企业网络安全有所影响。

实现 Http 隧道的方式主要有两种：利用 SSL[14]（Secure Socket Layer，安全套接层）的 443 端口和 Http 的 80 端口。根据 SSL 协议，通过 443 端口传输的数据报都是被加密的信息，经过的 NAT 是无法破解的，因而所有的数据都可以从 443 端口透明穿过。通过 443 端口建立两条 TCP 连接，分别连接信令代理服务器和媒体代理服务器可以实现 SIP 电话穿越 NAT。但基于安全的原因，一些企业会关闭 443 端口，以防止黑客解密通过 443 端口传输的数据流进行入侵或攻击。根据 Http 协议，形成 Http 隧道通过 80 端口，穿透 NAT 进行通讯。

首先，SIP 信令代理服务器（下文简称信令代理）开启对 TCP 的 80 端口和 UDP 的 5060 端口的监听。然后，内网终端通过与信令代理的 80 端口建立一条 Http 隧道，即可实现 SIP 信令的双向通讯。

客户端向信令代理发送 SIP 信令报文之前,先把报文中的 VIA、Contact、Route 等字段中的内网本地地址和端口号分别替换为信令代理的 IP 地址和信令代理监听的 UDP 侧端口。信令代理对于 SIP 信令报文的处理主要可以分为 Register 报文处理和 Invite 报文处理。

4.2.2　Register 信令处理主要流程

1)监听 TCP 的 80 端口并接受内网客户端 TCP 连接。保存 TCP 连接的 Socket 句柄,NAT 的 IP 地址和端口,设置信令通道连接状态为等待接收 Register 信令请求。

2)收到内网客户端发来的 Register 信令。解析信令,记录客户端软号码;更新信令通道链路状态为等待注册成功状态,添加 Socket 句柄与软号码关联表。

3)收到 SIP Proxy 发来的 Register 的 200 OK 报文。解析报文,查找 Socket 与软号码关联表,通过对应的 Socket 句柄将报文转发至内网客户端。

4.2.3　Invite 报文处理主要流程

对于 Invite 报文的流程可以分为四种情况:内网呼叫外网、外网呼叫内网、内网呼叫同一个内网、内网呼叫其他内网。对于内网呼叫其他内网的流程可以分解成内网呼叫外网和外网呼叫内网两个流程,因此文中将不再对内网呼叫其他内网的流程进行介绍。

1)内网客户端呼叫外网客户端。

(1)信令代理 TCP 的 80 端口收到内网已注册成功的客户端发送的 Invite 请求信令。解析信令,记录主叫软号码,被叫软号码,Call-ID。

(2)在通话记录表中查找该 Call-ID,如果找不到,添加一条通话记录,并通知媒体代理服务器分配一条媒体链路,获得分配的媒体代理网关的 IP、TCP 端口和 UDP 端口,记录到通话记录表中;如果找到,则使用查找到的通话记录信息。

(3)Invite 报文的 SDP 修改。将 SDP 的 c 字段中 IP 替换为分配到的媒体代理服务器 IP,将 m 字段中的端口号替换为分配到的媒体代理服务器 UDP 端口。将处理后的 Invite 报文转发给 SIP Proxy。

(4)信令代理 UDP 的 5060 端口收到 SIP Proxy 发来的 Invite 响应报文。从 SDP 报文中获得被叫方接收和发送媒体信息的 IP 和 UDP 端口号,记录到对应的通话记录信息中。媒体修改报文中的 SDP 描述,将 c 字段中 IP 替换为媒体代理网关 IP,将 m 字段中的端口号换成媒体代理网关的 TCP 端口(80 或 443 端口)。通知媒体代理服务器被叫方接收和发送媒体流的 IP 地址和端口号。将处理后的报文通过对应的 TCP 端的 Socket 转发给客户端。

2)外网客户端呼叫内网客户端。

(1)信令代理的 UDP 的 5060 端口收到 SIP Proxy 发送的 Invite 报文。判断被叫客户端已经在该信令代理注册成功,记录主叫软号码,被叫软号码,Call-ID。

(2)在通话记录表中查找该 Call-ID,如果找不到,添加一条通话记录,并通知媒体代理服务器分配一条媒体链路,获得分配的媒体代理网关的 IP、TCP 端口和 UDP 端口,记录到通话记录表中;如果找到,则使用查找到的通话记录信息。

(3)Invite 报文的 SDP 修改。将 SDP 的 c 字段中 IP 替换为分配到的媒体代理服务器 IP,将 m 字段中的端口号替换为分配到的媒体代理服务器 TCP 端口(80 或者 443)。将处理后的 Invite 报文通过对应的 TCP 端的 Socket 转发给客户端。

(4)信令代理 TCP 的 80 端口收到内网客户端发来的 Invite 响应报文。媒体修改报文中的 SDP 描述,将 c 字段中 IP 替换为媒体代理网关 IP,将 m 字段中的端口号换成媒体代理网关分配的 UDP 端口。将处理后的 Invite 的响应报文转发给 SIP Proxy。

3)呼叫同一个内网的客户端。

(1)信令代理 TCP 的 80 端口收到内网已注册成功的客户端发送的 Invite 请求信令。解析信令,记录主叫软号码,被叫软号码,Call-ID。

(2)通过主叫软号码和被叫软号码在信令通道记录表中查找内网客户端记录,判断两个终端处于同一个内网中(NAT 的 IP 地址相同或者其他策略判断)。对于处在同一个内网的终端之间的呼叫,信令代理服务器不需要在通话记录表中添加记录,也不需要分配媒体链路,直接转发 Invite 报文到 SIP Proxy。

(3)信令代理 UDP 的 5060 端口收到 SIP Proxy 发来的 Invite 响应报文。同样,信令代理根据主被叫软号码判断出是内网呼叫内网,根据主叫软号码查询 TCP 链路的 Socket,将 Invite 响应报文通过对应的 TCP 端的 Socket 转发给客户端。

5　测　试

按照上述方案,在中兴通讯与若干个小型企业网络之间进行通话测试,中兴通讯的 NAT 类型是 UDP 受阻的,其他几个公司的 NAT 类型涵盖了完全锥形 NAT、限制型锥形 NAT、端口限制型锥形 NAT、对称型 NAT 和 UDP 受阻 NAT 五种类型。测试结果发现通过 Http 代理模式中转的通话没有明显的延迟的增加,各个公司之间都可以正常通话,实现了对各类 NAT 的穿越。结合 UDP 打洞技术可以降低 Http 代理模式的服务器负载,Http 代理模式可以穿越限制严格的 NAT,结合 UDP 打洞和 Http 代理模式的穿越方案是可行的。

(下转第 156 页)

(1)对物理链路的影响;

(2)采集到数据泄密所可能造成的影响。如:IP 卡类业务的用户和密码泄漏。

对于第一个问题,一方面系统采用的镜像或旁路的方式,均是电信号复制后的供给信令采集设备,不会对原电路电平信号造成损失;另一方面,镜像或旁路只有接收线路,不会发生向被镜像或旁路发送信号的情况。从上述两个方面可保证跨接采集数据不会影响到现网信令链路的安全。

对于第二个问题,可分为两种情况。如果该卡类业务的密码不经过 INAP 传送,而是直接以 DTMF 或 FSK 的方式在话路传送的不会存在用户信息和密码泄露的问题。如果卡类业务的用户信息、密码等用 INAP 传送,那么可能被信令采集设备采集到,对于此问题系统设计了以下解决办法:

(1)在信令采集硬件上直接屏蔽对 INAP 消息的采集,仅采集漏话业务需要的 ISUP、TUP 和 MAP 消息;

(2)双方签订数据保密协议。

下一步工作,针对中等规模、大规模业务交换中心一并接入形成统一的漏话提醒业务系统以及系统的整体扩容升级做深入的研究。

参考文献:

[1] 张志英. 漏话提醒业务在移动通信中的应用[D]. 南京:南京邮电大学,2012.

[2] 张慧嫦,李力卡,陈庆年. CDMA 网络漏话提醒业务的优化与实现[J]. 移动通信,2012(Z1):142-146.

[3] 王兆爱. 基于 CTI 技术的漏话业务平台的设计与实现[D]. 北京:北京邮电大学,2007.

[4] 沈 巍. 基于 ICE 技术的漏话提醒业务系统[J]. 电脑与电信,2011(7):66-67.

[5] 张 旻,李网灿. "来电宝"--一种新型的短消息增值业务[J]. 江苏通信技术,2004,20(5):46-48.

[6] Wilson D R. Signaling system No. 7, IS-41 and cellular telephony networking[J]. Proceedings of the IEEE, 1992, 80(4):644-652.

[7] ITU2T. Signaling system No. 7 protocol tests[R]. [s. l.]:[s. n.],1993.

[8] BELLCORE. Signaling Transfer Point (STP) generic requirements[R]. [s. l.]:[s. n.],1996.

[9] BELLCORE. Specification of signaling system number 7[R]. [s. l.]:[s. n.],1998.

[10] 夏 雷,李 青,李东亮,等. CDMA 网络移动交换机系统间短消息寻呼技术研究及应用[J]. 电信科学,2012,28(5):37-42.

[11] 钟延辉,傅 彦,陈安龙,等. 基于抽样的垃圾短信过滤方法[J]. 计算机应用研究,2009,26(3):933-935.

[12] 胡日勒,蔡 洁,钟义信. 短信过滤系统设计分析[J]. 计算机应用研究,2008,25(8):2557-2560.

[13] 沈 冰,陈向东,黄馨竹. 基于 J2ME 技术的短信智能回复系统的设计与实现[J]. 计算机应用研究,2007,24(12):263-265.

[14] 杨 云,冯 亚. GSM 网络优化中接通率的分析[J]. 计算机工程与科学,2010,32(10):20-22.

(上接第 151 页)

6 结束语

文中根据现有的 SIP 穿越技术,结合对 SIP 协议的深入研究,采用 UDP 打洞与 Http 代理相结合的方法,提出了一种支持 SIP 穿越各类 NAT 的解决方案。该方案无需对 NAT 设备做任何改动。实验结果证明,基于 UDP 打洞与 Http 代理相结合的 SIP 穿越 NAT 的解决方案具有很强的可行性,对 VoIP 网络的发展有一定的促进作用。

参考文献:

[1] Rosenberg J. SIP:Session Initiation Protocol[S]. RFC 3261, 2002.

[2] Egevang K, Francis P. The IP Network Address Translator (NAT)[S]. RFC 1631,1994.

[3] Rosenberg J, Weinberger J, Huitema C, et al. STUN-Simple traversal of User Datagram Protocol (UDP) through Network Address Translators (NATs)[S]. RFC 3489,2003.

[4] Ford B, Srisuresh P, Kegel D. Peer-to-Peer (P2P) communication across middleboxes[S]. 2003.

[5] 邓 勇,屈玉贵,赵保华,等. 一种 SIP 穿越 NAT 的解决方案[J]. 小型微型计算机系统,2007,28(5):769-773.

[6] 张慧敏. SIP 穿越 NAT/防火墙的研究与实现[D]. 武汉:华中科技大学,2006.

[7] 徐静华. VoIP 中 NAT 穿越解决方案的设计与实现[D]. 武汉:华中科技大学,2005.

[8] Handley M, Jacobson V. SDP: Session Description Protocol [S]. RFC 2327,1998.

[9] 郭常清. 针对 SIP 的 STUN 解决方案的设计与实现[J]. 科学技术与工程,2006,6(11):1556-1560.

[10] 史永林,潘 进. STUN 技术深入分析[J]. 电脑知识与技术:学术交流,2006(8):71-72.

[11] Niemi A. Session Initiation Protocol (SIP) extension for event state publication[S]. RFC 3903,2004.

[12] 黄伟峰. HTTP Tunnel 技术在 VoIP 系统中的实现[J]. 微型电脑应用,2004,20(2):43-45.

[13] 韩 风,施 寅. Http 隧道在穿越 NAT/防火墙技术中的应用[J]. 计算机技术与发展,2006,16(5):163-165.

[14] Dierks T, Rescorla E. The Transport Layer Security (TLS) protocol, version 1.1[S]. RFC 4346,2006.