Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 639528, 9 pages
doi:10.1155/2008/639528

Research Article

NAT Traversing Solutions for SIP Applications

Whai-En Chen,[1] Ya-Lin Huang,[2] and Han-Chieh Chao[1,3,4]

[1] *Institute of Computer Science and Information Engineering, National I-Lan University, I-Lan 260, Taiwan*
[2] *Department of Computer Science, National Chiao Tung University, Hsinchu 300, Taiwan*
[3] *Department of Electronic Engineering, National I-Lan University, I-Lan 260, Taiwan*
[4] *Department of Electrical Engineering, National Dong Hwa University, Hualien 974, Taiwan*

Correspondence should be addressed to Han-Chieh Chao, hcc@niu.edu.tw

Received 2 January 2008; Accepted 2 March 2008

Recommended by Jong Hyuk Park

Session Initiation Protocol (SIP) has been proposed for multimedia services and wide-area connectivity in smart home environments (SHEs). An important issue for SIP deployment in SHEs is network address translator (NAT) traversing. SIP and Real-time Transport Protocol (RTP) packets are delivered between an SHE (i.e., private IP network) and Internet (i.e., a public IP network) through an NAT function of a home gateway, and the NAT translates the IP/transport layer address and port number but leaves the application layer content unchanged. This results in inconsistency between the IP addresses/port numbers in the IP/transport layers and those in the SIP layer. To resolve this issue, we describe six solutions including static route, UPnP, STUN, ICE, ALG, and SBC. Then we compare these solutions in terms of smart home appliance (SHA) modification, scope of NATs supported, multilayer NAT traversal, ease of configuration, security issue, and time complexities.

1. INTRODUCTION

Smart home appliances (SHAs) including information appliances and multimedia appliances have rapidly deployed in smart home environments (SHEs). These SHAs are interconnected with each other through various access technologies such as radio links, power lines, and Ethernet cables [1]. To provide wide-area connectivity and multimedia services, many SHAs adopt Session Initiation Protocol (SIP) [2] as their signaling protocol and Real-time Transport Protocol (RTP) as multimedia transport protocol. For example, SIP Voice over IP (VoIP) phones, video conference devices, video door phones, IPTV, and health monitoring systems are proposed in [3–7]. The SHAs connect to Internet devices through a home gateway (HG), which is equipped with firewall to provide security and network address translator (NAT) to solve IP shortage problem. However, NAT blocks the requests from Internet and the multimedia initialized by application layer protocols (e.g., SIP). To demonstrate the NAT traversing problem, this paper utilizes VoIP as an example since VoIP is an always-on service and can be used to evaluate both SIP and RTP sessions traversing over NAT.

In SIP-based VoIP, user agents (UAs) are the IP network endpoints just like telephones in the SHEs. UAs send/receive SIP messages to create, modify, and terminate multimedia sessions. SIP utilizes IP addresses/port numbers as location information in the SIP messages. Therefore, it cannot work correctly when a UA resides in a private network (i.e., SHE) behind a network address translator [8]. This issue referred to as SIP/RTP NAT traversing problem is described as follows.

Figure 1(b) shows the NAT configuration in an SHE. In this figure, an SHE (i.e., private network) connects to Internet (i.e., the public IP network) through an NAT (i.e., home gateway). The private IP addresses 192.168.0.0/24 are assigned to the hosts in the private IP network. The IP address of the public network interface card (NIC) for the NAT is 140.113.131.88.

Consider the communications between a host UA1 in the smart home environment (i.e., private IP network) and another host UA2 in Internet. Since a packet from UA1 (with the source IP address/port 192.168.0.111:5060) cannot be routed in Internet, the NAT replaces the source IP address of the packet by that of the NAT (i.e., 140.113.131.88) and changes the source port (i.e., 5060) to an unused port 10080 in the NAT. The mapping between the private IP address/port and the public IP address/port is stored in the NAT's mapping table (Figure 1(a)). When the NAT receives

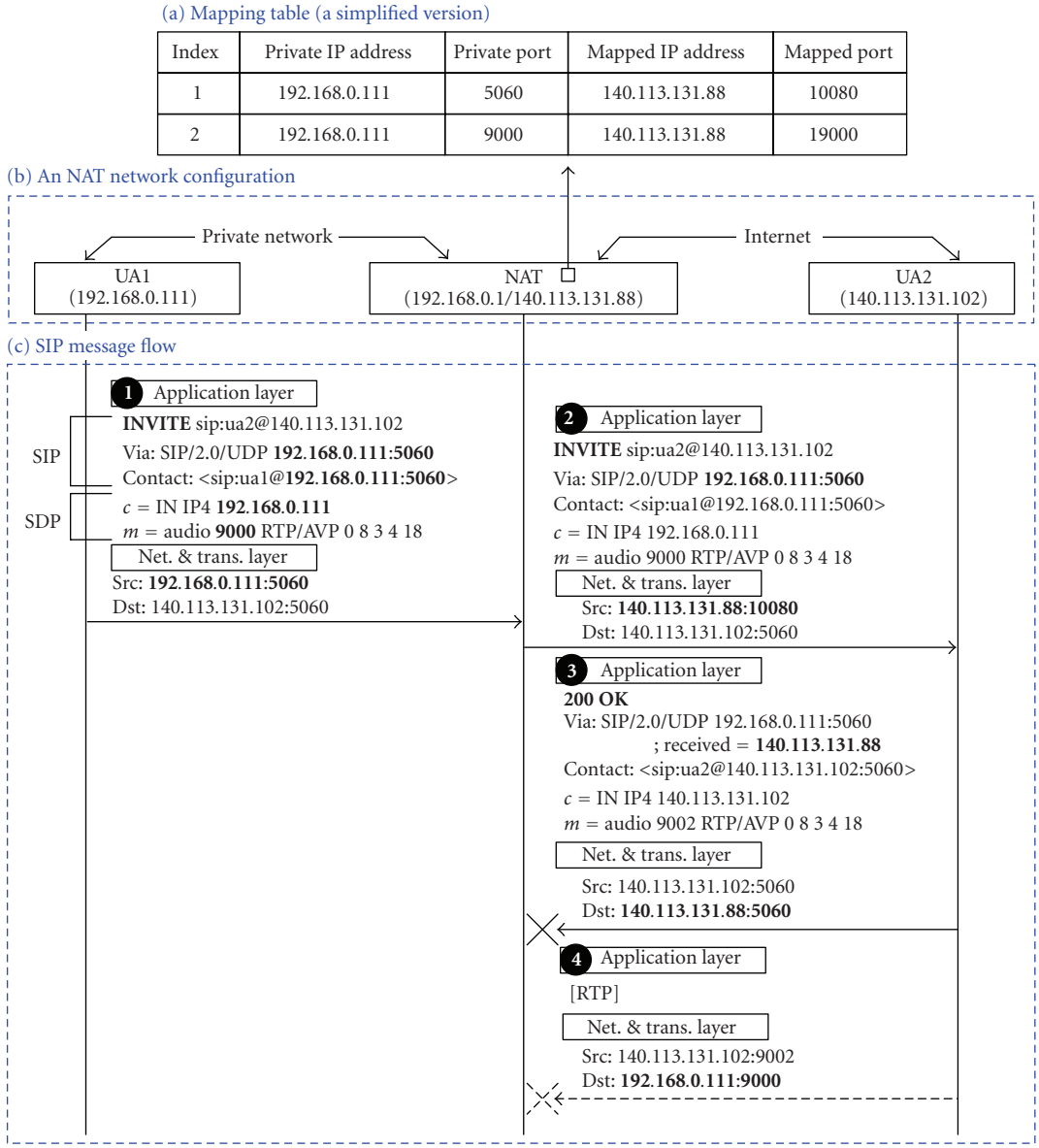

Figure 1: SIP message flow with standard NAT mechanism.

a packet from UA2 (with the destination IP address/port 140.113.131.88:10080), it retrieves the mapping table to translate the IP address/port to 192.168.0.111:5060 and sends the packet to UA1. The above NAT mechanism only translates the *IP information* (i.e., the IP address and the port number) at the network and the transport layers. It does not translate the IP information carried in the content of an SIP message. Therefore, the application-layer IP information is not consistent when the SIP message traverses the NAT. This issue is further elaborated as follows. Several header fields in an SIP message contain IP information related to SIP message delivery. For example,

(i) the *Via* header field indicates the SIP nodes visited by an SIP request so far; the reverse direction of the path should be followed to route the responses for this request,

(ii) the *Contact* header field indicates the address where the other party can send subsequent requests.

Two Session Description Protocol (SDP) fields in the SIP body provide IP information for media sessions [9].

(i) The IP address for the connection is provided in the *c* field.

(ii) The port number for the media information is provided in the *m* field.

Figure 1(c) illustrates SIP message delivery between UA1 and UA2 through the standard NAT. Suppose that UA1 sends an SIP INVITE message (Figure 1(1)) to UA2. In this message, both the *Via* and the *Contact* header fields contain UA1's IP address 192.168.0.111 and port 5060. For the RTP media session, 192.168.0.111 and 9000 are recorded in the *c* and the *m* fields, respectively. This message is carried by an IP

packet with the source IP address/port 192.168.0.111:5060. At the NAT, the source IP address/port of the packet is translated to 140.113.131.88:10080 (Figure 1(2)). However, the application layer content (i.e., the SIP message) is left unchanged.

Upon receipt of the INVITE message, UA2 creates a 200 OK message where the *Via* header field (i.e., 192.168.0.111:5060) is copied from the INVITE message. Then UA2 adds the *received* parameter with the value 140.113.131.88 to the *Via* header field. UA2 replies the 200 OK message by using the address and the port number in the *Via* header field (Figure 1(3)). Since 5060 is not a correct port number in the NAT's mapping table, this message cannot be delivered to the destination (i.e., UA1). Also, the RTP packets will be delivered to 192.168.0.111:9000 (Figure 1(4)) as designated by the *c* and the *m* fields in the INVITE message. Consequently, the destination is unreachable from the public IP network for this SIP call.

The SIP/RTP NAT traversing issue can be resolved by two approaches. In the *SHA-based* solution, the application layer IP information translation is performed at the SHAs. In the *server-based* solution, the translation is performed at a server in the public IP network. Note that in the SHA-based solution, the SHA may still need to interact with a server to obtain the IP information mappings.

Examples for SHA-based solutions include Static Route [10], Universal Plug and Play (UPnP) [11], Simple Traversal of UDP through NATs (STUN) [12], STUN Relay Usage [13], Interactive Connectivity Establishment (ICE) [14], and Realm Specific IP (RSIP) [15]. Examples for server-based solutions include Application Layer Gateway (ALG) [16], Session Border Controller (SBC) [17, 18], and midcom [19]. This article focuses on several widely SIP/RTP NAT traversing solutions used in SHEs, and shows their tradeoffs.

2. STATIC ROUTE

In Static Route [10], the application layer address translation is performed at the SHA (i.e., an SIP UA) in a smart home environment (i.e., private IP network), and the standard NAT is used to translate the IP-layer address. Both the SHA and the NAT need to configure an SIP mapping (e.g., entry 1 in Figure 1(a)) and an RTP mapping (e.g., entry 2 in Figure 1(a)). If the SHA is engaged in multiple media streams (e.g., audio plus video), extra RTP mappings are required.

Figure 2 illustrates SIP message delivery between UA1 (in the private IP network) and UA2 (in the public IP network) based on Static Route. The IP address settings for UA1, UA2, and the NAT are the same as those in Figure 1. Initially, the SIP mapping and the RTP mapping are configured in both UA1 and the NAT.

Whenever UA1 sends an INVITE message to the UA2 (Figure 2(1)), the message is carried by an IP packet with the source IP address/port 192.168.0.111:5060. The IP address/port reserved for the media session is 192.168.0.111:9000. The private IP information is not shown in the application layer content. Instead, through the mapping table in UA1, the private IP address/port is replaced by the public IP address/port 140.113.131.88:10080, which are filled in both the *Via* and the *Contact* header fields. Also, the public IP address/port 140.113.131.88:19000 for RTP are filled in the *c* and the *m* fields, respectively. At the NAT, the source IP address/port of the packet is translated from 192.168.0.111:5060 to 140.113.131.88:10080 (Figure 2(2)). The application layer content is left unchanged.

Upon receipt of the INVITE message, UA2 replies a 200 OK message (Figure 2(3)). The *Via* header field (i.e., 140.113.131.88:10080) in the INVITE message (Figure 2(2)) is copied to the 200 OK message as the destination of the message. Then the 200 OK message is sent to the NAT. When the NAT receives the 200 OK message, it retrieves the mapping table, translates the destination IP address/port from 140.113.131.88:10080 to 192.168.0.111:5060, and sends the packet to UA1 (Figure 2(4)).

The ACK message (with 140.113.131.88:10080 in the *Via* and the *Contact* header fields) is delivered to UA2 (Figure 2(5) and (6)) just like the INVITE message. The RTP packets from UA1 to UA2 are delivered to 140.113.131.102:9002 (Figure 2(7)) as designated by the *c* and the *m* fields in the 200 OK message (Figure 2(4)). At the NAT, the source IP addresses/ports of these packets are translated from 192.168.0.111:9000 to 140.113.131.88:19000. These packets are then sent to UA2 (Figure 2(8)). For the RTP media data sent from UA2 to UA1 (Figure 2(9)), they are carried by IP packets with destination IP address/port 140.113.131.88:19000. This destination IP information is specified in the *c* and the *m* fields in the INVITE message (Figure 2(2)). Upon receipt of the RTP packets, the NAT translates the destination IP address/port from 140.113.131.88:19000 to 192.168.0.111:9000 and sends the packets to UA1 (Figure 2(10)).

3. UNIVERSAL PLUG AND PLAY (UPnP)

Manual configuration of Static Route can be automated by Universal Plug and Play (UPnP) [11]. UPnP is a network protocol for automatic discovery and configuration when a certain device (i.e., an UPnP client) is online. Therefore, IP information mappings in both the UA and the NAT can be automatically established by the UPnP protocol. Then all SIP/RTP packets traverse over the NAT with the same procedure described in Section 2.

An UPnP system typically consists of several UPnP clients and an Internet Gateway Device (IGD). In the SHE, a smart home appliance is an UPnP client and a home gateway plays the role as an IGD. The IGD joins in the multicast group 239.255.255.250 and listens on port 1900 for the requests issued by the UPnP clients. The UPnP messages are exchanged through the Hypertext Transfer Protocol (HTTP).

Figure 3 illustrates how the mapping in entry 1 of Figure 1(a) is established by the UPnP messages exchanged between UA1 (an UPnP client) and the NAT (i.e., home gateway). The IP address settings for UA1 and the NAT are the same as those in Figure 1. The message flow in Figure 3 is described as follows.

Step 1. When UA1 is online, it sends an UPnP multicast M-SEARCH request (with the destination IP address/port