Solutions for NAT traversal in SIP Environment

Basics - NAT in SIP

Network Address Translation (NAT) is a big problem for SIP, because both the SIP signalling and the media uses UDP to transport their information.

The reason for introducing NAT was the shortage of public addresses available on the Internet. Therefore, users started to share one IP address through a NAT gateway in a private network. Typically, addresses in the private network have the form 192.168.x.x or 10.x.x.x.

When a phone sends a packet from a private network to a public network, the NAT gateway allocates a port for this new “connection” and patches the IP packet according to this port. Looking at the IP transport layer of the packet, the recipient of the message thinks it came from that port on the NAT gateway. However, because SIP uses explicit addressing in the SIP contents (and that address has priority in SIP), the response to that packet will not find the right way.

The same problem occurs when the phone wants to invite a person for a call. In the invitation message, it needs to put the IP address and the port where it expects the media to go to. If it puts in its private address here, the media will not find its way from the public Internet to the phone.

Firewalls use this mechanism to filter traffic entering and leaving a zone. Often, this is combined with NAT.

There are different approaches to solving this problem:

- Use a SIP-aware NAT router
- Set up a static route in the NAT gateway
- Use STUN to measure out ports

INTERTEX IX66 - SIP-Aware NAT Router

With the increasing acceptance of SIP as a standard protocol and its needs, more and more network equipment becomes “SIP aware”. That means, if a SIP packet passes a NAT gateway, the gateway will inspect it and make the necessary patches to the packet. It allocates ports for the media and puts the right addresses into the SIP address.

This solution is recommended in environments where there is sufficient number of subscribers in the private network. There are “Application Layer Gateways” available to solve this problem (like the snom 4S SIP NAT gateway), which are installed on the firewall or on the NAT gateway computer. Some gateway vendors offer special add-ons to their standard firmware that make their equipment SIP-aware. Some advanced DSL routers include this ALG in their standard configuration.

When you use a SIP-aware router, you should make sure that every SIP message goes to the NAT gateway directly. There are several ways of doing this, depending on the equipment you are using in the private network.

For this mode, NAT detection should be set to “Off” or “Automatic” with the STUN server field empty (this is the default). The fields “dynamic RTP port start”, “dynamic RTP port end”, “Network identity” and “Network port” should be left empty and “Local SIP port” should be set to default.

If all messages are to go over the NAT gateway, you can set the outbound proxy to the address and port of the private NAT gateway. This address takes the format of a SIP URL. If there is no initial “sip:”, the phone will complete the URL according to the rules for the SIP URL. Valid examples for this field include “192.168.0.1”, “192.168.0.1:5062”, “nat.company.com” and “sip:nat@company.com:5065”. In this case you should set the “Treat as initial route” field to “Address”, so that no additional headers are inserted into the SIP messages.

Especially where there are several phones located within the same NAT, you might want to avoid all traffic going through the NAT gateway. In such cases, we recommend setting up a SIP proxy (like the snom 4S SIP proxy) in the private network and pointing all traffic to this proxy. It will then take care of the traffic leaving the NAT and redirect the packets to the NAT gateway itself.

STUN Solution

Setting up the NAT router is impossible in many cases, and new equipment may be too expensive. For these environments, “Simple Traversal of UDP Through NATs” (STUN) has been defined in the SIP environment (see draft-rosenberg-midcom-stun-01.txt).

STUN uses a server located in the public Internet. The phone sends a test message to the server and receives in the response which IP address and port the server received. The client may ask the STUN server to send the packet back from a different location. In this way the client can determine the type of NAT present. You can use the snom 4S STUN server for this.

To set up a phone for STUN, set the NAT detection to “Automatic” and enter the address of the STUN server in the field “STUN server”. The field must have the format hostname [:port], a valid **STUN SERVER is “130.149.31.19:5062”**, other format examples are “mycompany.com”, “stun.mycompany.com:1234”.

SNOM STUN SERVER -For eval use only-	**130.149.31.19:5062**

When you use STUN, the fields “dynamic RTP port start”, “dynamic RTP port end”, “Network identity” and “Network port” should all be left empty and the “Local SIP port” field should be default.

Static Route – Firewall Configuration

Setting up a static route on the NAT gateway is the most powerful, but also most complicated way of setting up the phone in a NAT environment. For this mode, NAT detection should be set to “Static”.

There are a couple of settings available for the static route:

- Dynamic RTP port start, end: The range of ports that are used by the phone for media including start and excluding the end port.
- Network identity (hostname, port): The phone will insert the inserted name as hostname and port into the SIP messages. The values must match the router set-up.
- Local SIP port: With this flag you can decide whether the phone uses the standard port (5060) or the port provided in the network identity as local port. If the router is not able to translate ports, you must use network port.

On the router, you need to set up one UDP port for the SIP traffic and several ports for the RTP (media) traffic. Try to set up at least ten ports for RTP, so that the probability of a port conflict is not too high.

Make sure that the settings on the phone are exactly the same as those on the router. This is very important because otherwise the service will be unreliable and frustrating.

Changing these settings requires a reboot of the phone.

Decision-making matrix

Scenario	**Best Solution**
Home user with old DSL router:	STUN
Experienced home userFirewall:	Static Route Use software ALG
Small office:	Use advanced SIP aware router (IX66)
Phone on public Internet:	Automatic NAT or NAT detection off
Phone only used in private network:	NAT detection off