Configuring for Registration
and NAT Traversal with
Smart ATA®

Copyright © Commetrex
2018

This section should probably be named “*Configuring Smart ATA for Registration and NAT Traversal in North America*” since handling NAT happens to be regional. The US has been assigned 20 times the addresses than has China, causing ISPs in China to handle dynamic NAT quite a bit differently than they do in the US. This, then, affects the way we traverse NAT. For example, although STUN is frequently used in China, it’s rarely needed in North America.

And it’s much easier to handle NAT in Smart ATA if you understand how the device does it. For this reason, the next section is a NAT tutorial. We recommend you give it a read, but skip it if you’ve fully up to speed.

# Fix for SIP Devices Behind a NATed Device

## Background

Network Address Translation (NAT) allows a routing device to alter IP address in the IP header to translate private LAN addresses to routable public addresses and vice versa.

– A NAT Example

In Figure 1-1– A NAT Example, a LAN-connected entity (“behind” the NAT) has an IP address of 192.168.16.22. The routing device is configured to perform NAT (it includes Domain Name Server (DNS)). It changes the source IP address of outbound messages to 64.12.145.14, the routable/public IP address of the router/gateway.

However, some higher-level (application-layer) protocols, such as Session Initiation Protocol (SIP) and Session Description Protocol (SDP) include IP address information in the body of the message. These IP addresses are usually unchanged by NAT, resulting in an inability of the correspondent (external) SIP entity to send information back to the NATed device since the local-LAN device typically uses the IP address given to it by the DNS server, in this case 192.168.16.22.

– SIP with NAT

In Figure 1-2 – SIP with NAT, the IP address of the From field inside the SIP message is unchanged and has an address that is unreachable from the external network.

## Problem Description

The problems with making SIP calls through a routing device with NAT can best be seen by looking at traces.

 – SIP Call Example with NAT

In Figure 1-3 – SIP Call Example with NAT, the IP address in the SDP body of the message is left unchanged. The problem with this scenario is that when the SIP peer/receiver tries to send RTP packets to the address in the message (192.168.16.22) no RTP flows since this is the wrong (unreachable) address.

The previous problem can be solved if the routing device supports Application Layer Gateway (ALG) with SIP. With ALG, the IP addresses inside the SIP messages (including the SDP) are also changed.

– SIP Call Example With NAT and ALG

Figure 1-4 – SIP Call Example with NAT and ALG shows how the routing device correctly changes the IP address in the SDP, allowing the receiver to send the SDP packets to the correct address. The routing device will then forward the packets to the 192.168.16.22 device.

ALG works for voice and G.711 pass-through fax calls since the ALG function is setup to handle VoIP. However, FoIP with T.38 is another story. For T.38 calls, the routing device does not correctly alter the messages related to reINVITES to T.38.

– SIP Call Example (T.38)

In Figure 1-5 – SIP Call Example (T.38), everything is correct until the 200 OK response from 192.168.16.22 to the T.38 Re-Invite. The routing device is not T.38 aware, so it incorrectly alters the SDP body of the message.

## Solution

The solution to the problem of making SIP-based FoIP calls with T.38 support from behind a NAT routing device is to turn off ALG and configure Smart ATA with the IP address that the external network should use to communicate with it. (The Smart ATA User Manual calls this the “NAT IP Address.”) Then, the correspondent SIP UA client can fill in the SIP message and SDP body with that IP address. This is shown in Figure 1-6 – SIP Example With Fix. But how does the device obtain the external address assigned by the NAT? Read on.

 – SIP Example With Fix


## Implementation

If it’s on a LAN, by default Smart ATA obtains its LAN IP address via DHCP and fills it in on the Network configuration page. (You can override the default on that page by using the drop-down to select Static or PPPoE.) But to answer the question regarding learning the external address, you should not need to know the NAT IP (public) Address since it is obtained by the ATA during the SIP registration. The Registrar populates the “Via” field in the INVITE contact header with the ATA’s From address.

To correctly configure the ATA for operation behind a NAT device, go to Advanced>>System and make sure Dynamic NAT is selected at the top of the screen and NAT IP Address/External Network IP Address radio button is selected, rather than the Local/Internal IP Address.

Now go to Advanced>>SIP, and make sure that NAT IP Address is selected for “Contact field in register” and “Via field.”

# GUI Configuration

The balance of this guide will walk through each GUI screen involved in registration and NAT traversal.

**Basic>>**

* 1. **Network**
	Usually, a device’s IP LAN address is obtained dynamically. Therefore, “Obtain an IP address automatically” in “Setup” and “DNS server” “Obtained Automatically” radio button are usually selected. STUN should be disabled. In the US, where our IP addresses are usually static, there is usually no need for STUN since the ATA obtains its address during SIP registration as explained above.
	2. **SIP**

This is where you enter your ITSP-provided credentials. The terminology is not universal, so don’t get frustrated. Enter the Registrar Server’s address here, and the Proxy Server, if provided. The Registrar Server may be an IP address or a domain name (Assuming you chose DNS on the Network page (above)). Include the Port Number, if provided.
User Name: This should be your domain name that will be used in SIP INVITE messages.

* 1. **FoIP**

This has nothing to do with registration, but as long as we’re on the Basic tab, let’s look at FoIP. If your provider supports T.38, select it here. It you don’t want to use T.38, select G.711 pass-through. (Don’t select both.) T.38 sessions begin in G.711 mode and then will either reINVITE if receiving, or accept a reINVITE if sending, provided the reINVITE arrives in time, otherwise, it will be rejected by Smart FoIP®.

**Routing>>**

Routing has nothing to do with registering either, but while you’re here, check to make sure that any routing rules shown are what you want.

**Advanced>>**

* 1. **System**

Here is where you select Dynamic NAT and External Network IP Address for “External Network IP Address.” (The External Network IP Address is extracted from the registrar’s Via contact header.)

* 1. **SIP**

|  |  |
| --- | --- |
| **SIP**Check “Always Honor SIP Contact Field”. (We don’t know why this Port for sending response  | Using received port to send response Using 5060  |
| Contact field in REGISTER  | External Network IP Address LAN IP address  |
| Domain name in REGISTER  | Domain name Subdomain name  |
| Via field  | External Network IP Address LAN IP address  |
| *To* header field  | Subdomain name Outbound proxy  |
| *Call-ID* header field  | Hostname Internal Network IP Address  |
| Obtain called party number from  | *Request Line* field *To* field  |
| Calling party number in call transfer  | Originating number Forwarding number  |
| Do not validate Via  |  |
| Re-register on INVITE failure  |  |
|  |
| Selecting the receiving port for response  | Use the receiving port of proxy Use the sending port of proxy  |
| Always honor proxy  |  |

# Using Smart ATA with Commetrex’ BladeWare

Many organizations that are adding fax servers are reluctant to invest in PSTN-specific systems, electing to acquire FoIP servers based on BladeWare, even though they are not quite ready to move to an all-IP system. For these applications where the port requirements are low (2-8 ports), Smart ATA can be used as an affordable interim PSTN interface since it is available in configurations with two-eight office trunks, making it an IP-PSTN gateway. This means that IP traffic can be routed to and from the FXO/office trunks through the ATA to the fax server.

Configure the routing rules as follows:

1. On the ATA's web interface, go to routing>>routing table.
2. Click on help at the bottom of the page.
3. Read the intro, then go to #9, Routing calls to PSTN.
4. Click “return” at the bottom of the page.
5. Enter the following:
IP X ROUTE FXO 1-2/R
This causes calls from the IP network/BladeWare to be routed to line ports 1 and 2 in round-robin order
6. For the reverse direction:
FXO[1-2] X ROUTE IP <ip\_address\_or\_domain\_name>:<port\_num>
This causes FXO calls to be routed to BladeWare at the specified address.
7. Click the Submit button.

Section 2.4.2 of the Smart ATA manual gives additional information.