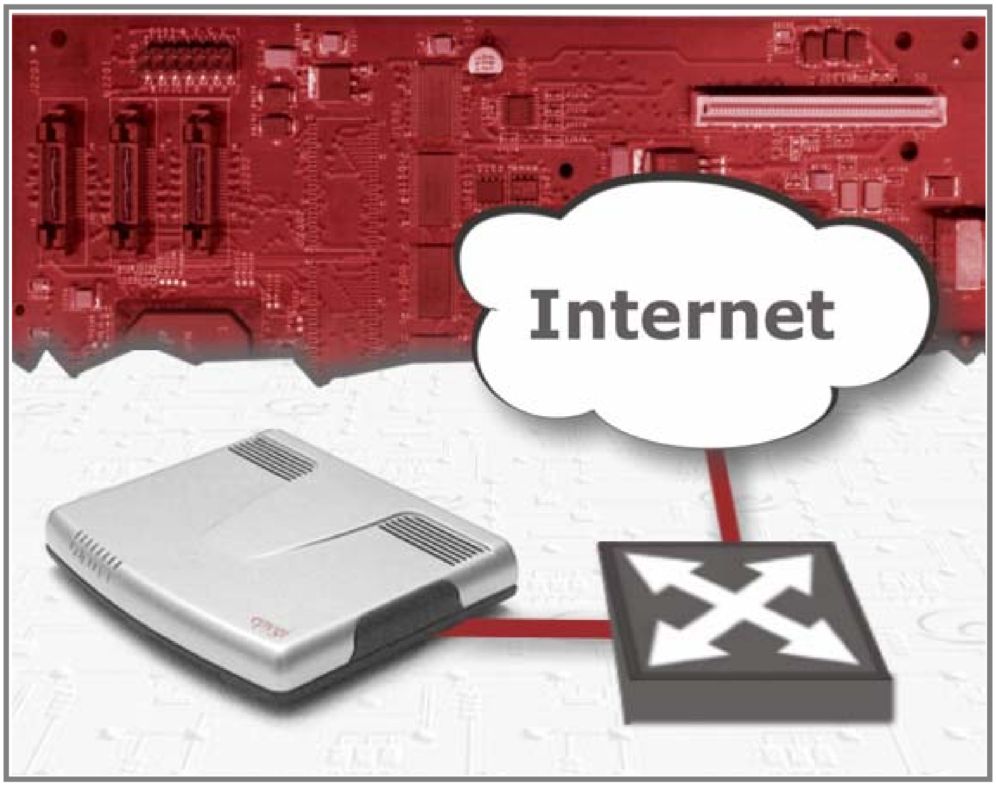
NAT Traversal with Quadro IP PBX



Revision: 2.0

Abstract: This document illustrates different methods of running Quadros behind the NAT.

Table of Contents:

Document Revision History

Revision	Date	Revision	Valid for SW	Valid for models
1.0	14-Jul-05	Initial version	3.1.x	IP PBXs
2.0	24-May-07	Updated	4.1.x	IP PBXs

1 Introduction

NAT is widely used in networks to save IP address space by providing only one IP address for complete companies.

The NAT device (a router with a firewall) will then map the internal and private IP addresses to the single public IP address. And it will use different ports for all the connections to distinguish them (see Figure 1).

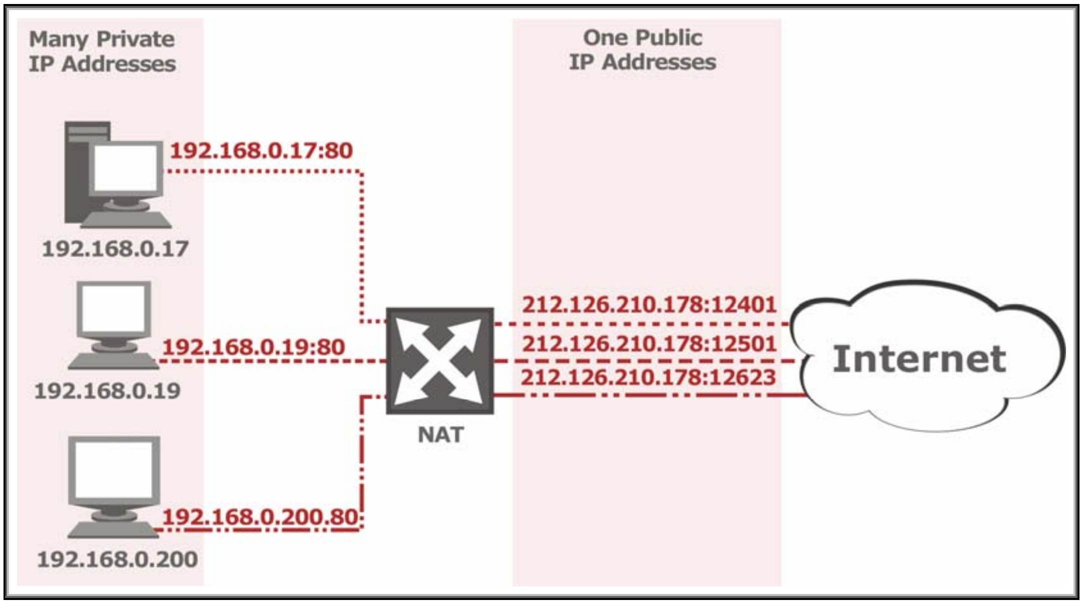


Figure 1

Basically the NAT dynamically creates a table of connections and keeps track of them. Connection like this can only be initiated from inside the NAT. So in addition to saving public IP addresses, the NAT also protects the private LAN from outside attacks.

2 Problems with VoIP and NAT

There are many protocols which are used for VoIP.

- The SIP protocol uses the IP address in some of its fields. Unfortunately the VoIP device will put the private IP address in these protocol fields and the typical NAT will not correct it. For example when using a SIP registrar which is correlating a SIP number with an IP address/port in a database, the registrar will receive the private IP address and will not be able to contact the device (see Figure 2).

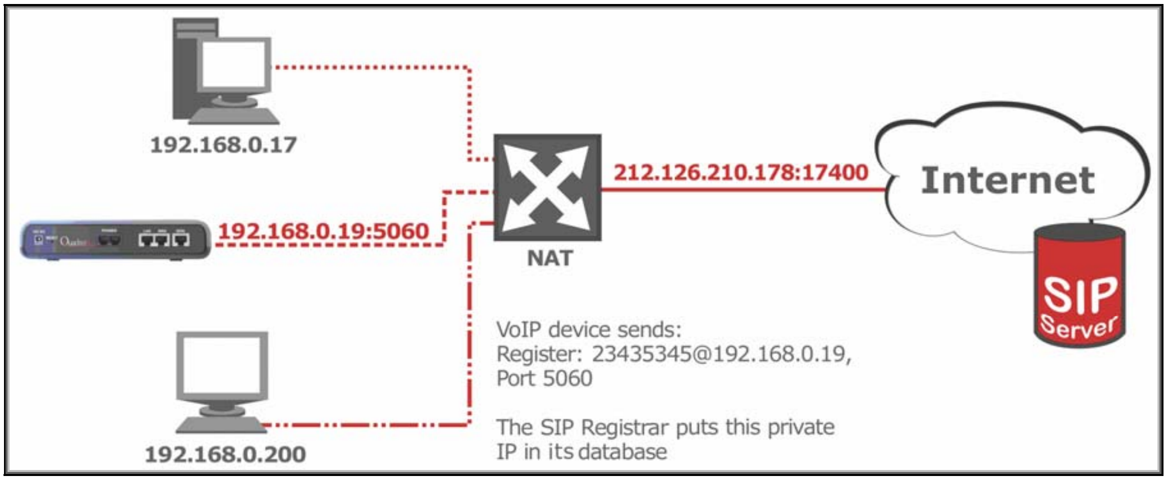


Figure 2

- NAT creates and deletes the connection entries dynamically. It means that after some timeout, all connections are deleted and for example a call from outside would be dropped at the NAT device.
- Even worse is the situation with the RTP streams. They are used to carry the voice. During the call setup the VoIP system will tell the called party the IP address/the port of its own RTP receiver. But in fact the NAT will change the IP and may change the port as well.

Similar but maybe easier-to-solve problems exist for all kinds of services that you want to run behind the NAT. One example is the WEB server.

3 Solutions

To allow Quadros to function behind the NAT router, the following should be executed:

- All Quadros should have different SIP ports.
- All Quadros should have different RTP port ranges which do not overlap.
- The NAT Traversal feature should be enabled on all Quadros (manually or using the STUN).
- Outgoing traffic from the Quadros as well as NATing should be allowed on the routers. And at the same time the source port of the packet should remain unchangeable after NATing (SIP ports and RTP port ranges).
- Incoming traffic through these ports (SIP ports and RTP port ranges) should be allowed on the router to be forwarded to the appropriate Quadro depending on the destination port.

A detailed example is given in Appendix.

As stated above the NAT Traversal feature on the Quadro should be enabled either manually or by using the STUN. Both methods are detailed below.

3.1 Manual NAT traversal

This method requires manual configuration of NAT traversal settings and is the most reliable solution.

1. Log into the Quadro as an administrator.
2. Open the **NAT Traversal Settings** from the menu.
3. Enable NAT Traversal by selecting either the **force** or **automatic** radio buttons.
4. Accordingly in the **SIP Parameters** and **RTP Parameters** tabs select the outside IP address of the NAT device as well as the port and port ranges.

Restrictions:

- As the method requires entering the public IP address of the NAT, it can only work when this IP address is static.

3.2 STUN

The STUN protocol [RFC 3489 - STUN - **S**imple **T**raversal of **U**ser Datagram Protocol (UDP) Through **N**etwork Address Translators (NATs)] allows entities behind a NAT to discover the presence and the type of the NAT and to learn and use the bindings they allocate.

How is the STUN working?

- First of all the STUN requires the existence of a STUN server. There are a couple of free servers in the Internet, as well as EPYGI is offering to its customers to use **stun.epygi.com**. In parallel there are free Linux implementations that can be run without effort on any Linux box that has a public IP address.
- By default the STUN is enabled on all Quadro IP PBXs and uses **stun.epygi.com** as the STUN server.
- To detect the type of the NAT and its outside IP address and ports Quadro sends several packets to the STUN server. The latter analyzes them and reports back the **IP address** and the **Port** the packets were received from. In parallel the STUN server itself will try to send some packets to the Quadro from its second interface. Determining weather the device receives these packets or not will help to find out the type of NAT.

There are several types of NAT. Here is the list of NATs the Quadro may report:

- Open Internet
- Full Cone NAT
- IP Restricted Cone NAT
- Port Restricted Cone NAT
- Symmetric NAT
- Blocked UDP

The result of the NAT detection process can be seen under **System->Status->SIP Registration Status**, below the table of registered extensions.

Please Note: In certain cases the STUN requires no changes on the existing NATs. So by providing SIP and RTP port diversity on Quadros we can secure properly functioning devices. However it is recommended to open incoming and outgoing rules on the router as described above.

3.2.1 Open Internet

If the STUN client on the Quadro detects that the Quadro is connected to the Internet with a public IP address, it will re-check this situation every 5 minutes.
If it is clear that the situation will not change, then the NAT traversal can be switched off or set to automatic in this scenario.

3.2.2 Full Cone NAT

On the Full Cone NAT all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address. This is the simplest NAT and it has some security issues. Any system from outside may send packets to the system behind the NAT by detecting the open port(s).

Method of the Quadro:

- Every 5 minutes the Quadro will check the outside IP address - if changed, the STUN process will start again.
- Every <keepalive> (default 120 sec) time the Quadro will send out UDP packets to the STUN server to keep the SIP and RTP ports open and reserved to the Quadro.
- Every hour a complete rescan will be done.

What will work?

- All types of SIP calls

Restrictions:

- In case you want to place 2 or more Quadros (or other IP phones) behind the router the SIP and RTP ports (port ranges) must not overlap.
- If have more than 2 devices behind the NAT router, these devices will not be able to call to each other. In this case it's recommended to include the local IP addressed into the **NAT Exclusion** Table.

3.2.3 IP Restricted Cone NAT

On IP Restricted Cone NAT all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

Method of the Quadro:

- Every 5 minutes the Quadro will check the outside IP address - if changed, the STUN process will start again.
- Every <keepalive> (default 120 sec) time the Quadro will send out UDP packets to all the SIP servers to keep the port to the SIP servers open.
- Every <keepalive> time the Quadro will send UDP packets to the STUN server to keep the RTP ports reserved for the Quadro.
- Every hour a complete rescan will be done.

What will work?

- SIP calls using a SIP server (only if the SIP server uses the record-route flag, which is the case with the EPYGI SIP server).

Restrictions:

- In addition to the restrictions described for Full Cone NAT, no Quadro to Quadro calls are possible.

3.2.4 Port Restricted Cone NAT

A port restricted cone NAT is like an IP restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

Method of the Quadro:

- Every 5 minutes the Quadro will check the outside IP address - if changed, the STUN process will start again.
- Every <keepalive> (default 120 sec) time the Quadro will send out UDP packets to all the SIP servers to keep the port to the SIP servers open.
- Every <keepalive> time the Quadro will send UDP packets to the STUN server to keep the RTP ports reserved for the Quadro.
- Every hour a complete rescan will be done.

Restrictions:

- The same restrictions described above for Full Cone NAT and IP Restricted Cone NAT.

3.2.5 Symmetric NAT

On the Symmetric NAT all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

Method of the Quadro:

- Just every 5 minutes the outside WAN IP address is rescanned.

What will work?

- Most likely nothing - or signaling but voice only in one way.

3.2.6 Blocked UDP

This may have different reasons:

- The Quadro is installed in a closed private network and can not even reach the STUN server.
- There is a very restrictive firewall which is filtering the UDP reply from the STUN server.

Method of the Quadro:

- The Quadro will retry every 5 minutes.

What will work?

- Most likely nothing - the Quadro may not even be able to determine its outside IP-address.

4 Appendix

Below is an example of Quadros behind the NAT.

Let’s assume that there are 3 Quadros (1, 2, and 3) behind the NAT. To make them fully functional, it is necessary to additionally configure both the NAT and the Quadros.

Separate UDP ports should be dedicated for each Quadro on the NAT. And depending on the ports the Quadros (1, 2, and 3) should be respectively configured.

The configuration steps are detailed below.

1. Assign different SIP and RTP Ports to each of the devices as shown in Table 1.

Quadro Name	IP address	SIP port	RTP Ports
Quadro 1	192.168.0.1	5061	6100 - 6199
Quadro 2	192.168.0.2	5062	6200 – 6299
Quadro 3	192.168.0.3	5063	6300 - 6399

Table 1

2. Allow **incoming** traffic for Quadros as detailed below.
   - Allow all incoming UDP traffic on the NAT from the Internet with port 5061 and port range 6100-6199. Forward the traffic to the Quadro 1 (192.162.0.1).
   - Allow all incoming UDP traffic on the NAT from the Internet with port 5062 and port range 6200-6299. Forward the traffic to the Quadro 2 (192.162.0.2).
   - Allow all incoming UDP traffic on the NAT from the Internet with port 5063 and port range 6300-6399. Forward the traffic to the Quadro 3 (192.162.0.3) as shown in Figure 3.

3. Allow **outgoing** UDP traffic from the Quadros and forward it to Internet retaining the SIP port as detailed below.
   - Allow all outgoing UDP traffic on the NAT with port 5061 and port range 6100-6199 from Quadro 1 (192.162.0.1) and forward it to Internet retaining the SIP port.
   - Allow all outgoing UDP traffic on the NAT with port 5062 and port range 6200-6299 from Quadro 2 (192.162.0.2) and forward it to Internet retaining the SIP port.
   - Allow all outgoing UDP traffic on the NAT with port 5063 and port range 6300-6399 from Quadro 3 (192.162.0.3)and forward it to Internet retaining the SIP port (see Figure 3).

4. Configure **Quadros** as detailed below.
   - Enable NAT Traversal on the Quadros (selecting **force/automatic** radio buttons).
   - Select the **Use STUN** radio button from the **NAT Traversal Settings→SIP Parameters** page.
   - Select the **Use STUN** radio button from the **NAT Traversal Settings→RTP Parameters** page as shown in Figure 3**.**

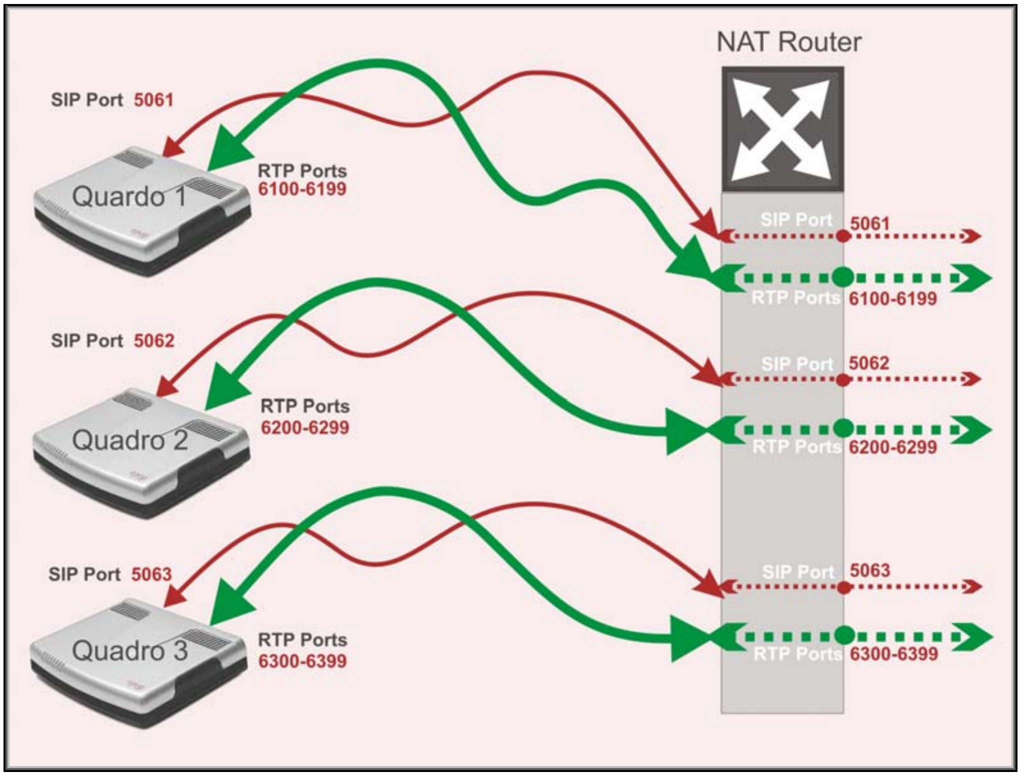


Figure 3