AETA AUDIO SYSTEMS

# Successful AoIP connections with AAS codecs

## 1. Introduction : object and general principles

Setting up a link via an IP network between audio codecs is not (yet ?) as simple as via the ISDN. There are numerous reasons for that: newness of technologies, diversity of network environments and organizations, sometimes too lack of coordination between broadcast and network technicians…

Therefore configuring codecs and network equipment may be tricky sometimes, but it is often made easier for AETA AUDIO SYSTEMS codecs, thanks to the use of the SIP protocol.

This document describes techniques to apply in order to overcome the usual obstacles. Although not pretending to be exhaustive, the list of cases here should cover most situations. The most classical issues are related to:

- The presence of a NAT router on the network path between the codecs.
- The presence of a firewall on this path.

*Refer to the glossary at the end of the document for more details on some acronyms used.*

For a fast access, essential information is highlighted in red like this paragraph.

It is always important to have available the information regarding the network organisation and to be allowed to access the devices which need to be configured. Hence we highly recommend to involve the persons empowered for such tasks.

## 2. Links via a private network

### *2.1. Local area network*

No special problem should be met within a LAN. The only critical point is setting the IP addressing on each codec.

The simplest case is when a DHCP server is available on the network, also called “dynamic” addressing situation. In the reverse case of “static” addressing, at least the IP address and the sub-network mask must be configured on each codec. Depending on the organization, it may be necessary to program as well the default gateway address and/or the DNS address.

A link can be set from a « calling » codec towards the other codec:

- Select the desired coding algorithm ;
- Enter the IP address of the other codec, then launch the call (“green phone” key). If using a SIP proxy server, instead of an IP address the SIP identifier (or URI) of the destination will have to be used.

There is no need to prepare the other codec beforehand, and the procedure is quite similar to a telephone call.

The operation is also possible with codecs from other manufacturers, provided that they comply with the Tech3326 EBU recommendation (also known as “N/ACIP” recommendation). *However you should check for specific settings or preparation possibly needed on such devices.*

### *2.2. Wide area network*

A wide area network covers a wider geographic range, and the network topology most probably includes routers on the path between the codecs to be linked. However, usually there is not much difference with a local area network.

*Note: using a VPN leads to just the same case; the operation is identical as far as the codecs are concerned.*

## 3. Links through a public network (Internet)

If each of the units has got a "direct" access to Internet with a public address, we are in the same situation as the previous one, functionally speaking (private WAN). The addressing scheme is normally static, as DHCP can rarely be used on a public access. In fact, this situation is very seldom met in the field!

First, the Internet access is usually protected by a firewall which will, as a principle, block *a priori* the desired connection. In such case exceptions (to the firewall security rules) must be created, that will allow this connection; this has to be done by the person in charge of the network management.

Most often, on one access if not both, the codec accesses the Internet via a NAT router. This router shares Internet access, with one or a few public addresses, among the equipment on the LAN. On this LAN the devices get local private addresses, and the router carries out an IP *address translation*. Note that:

- As an example, a consumer ADSL modem-router is almost always a NAT router, sharing a single public IP address between the devices connected to the router.
- It is just the same on a 3G/3G+ mobile IP access ; the terminals (phones or computers) access the Internet via NAT routing.
- NAT routing is often included in the firewall features; in fact NAT routing somewhat participates to the protection against direct attacks from the outside.

NAT routing is an obstacle to transmission with UDP, mainly for two reasons:

- It does not allow unsolicited data to come in from the outside network. In other words, data input is accepted on a port as an answer to a request from the local network, but an external agent cannot directly initiate the transmission of a packet.
- The terminal units on the LAN only know their private local address. On the other hand, agents implementing the SIP protocol have to communicate to each other the addresses and ports to be used for the media exchanges. Because of the NAT routing, agents do not get the real public addresses, which leads to failure of the session setup attempts.

We are now looking at various methods used to overcome these obstacles.

## 3.1. NAT and use of the STUN server

The STUN protocol is a method which is often successful[1] in helping the agents to discover their public address even when they are « hidden » behind a NAT router. Here is the operation principle:

- A STUN server is used, which is accessible over the Internet ;
- The address of this server is programmed into the agent (i.e. the audio codec in our topic);
- The agent queries the server and discovers its public IP address and port number, as seen from outside of the NAT router and LAN;
- This addressing information is then used by the agent for negotiating and setting up a media session.

The STUN server address is programmable in the html page of a Scoop 4+ or Scoopy+. Besides, one can also find in the menu (keypad and display on the front of the unit) an activate/disable (on/off) selection, available without having to clear the server address.

The are many public STUN servers available on the Internet ; here are a few examples, valid at the time of writing:

| Domain name | Numeric address |
|---|---|
| stun.xten.com | 75.101.138.128 |
| stun.ekiga.net | 75.101.138.128 |
| stun.sipgate.net | 217.10.79.2 |
| stun.ippi.com | 208.73.210.27 |
| stun.sipphone.com | 198.65.166.165 |

**Examples of STUN servers**

*It is advisable to check that the server is operative. A list of servers can also be found on the support page of our web site http://www.aeta-audio.com.*

## 3.2. Standard NAT router

Situation: codec A behind a NAT router with no specific programming
*(a codec accessing Internet via a mobile network is almost always in such situation)*
We also assume that the other codec (B) is accessible with a public address.

Once codec A is configured for using a STUN server:

- codec A can initiate a connection to (call) codec B
- codec B cannot call codec A

| Advantages | Drawbacks |
|---|---|
| Configuration is relatively simple | B cannot call A |
| No change is needed on the router | |
| Several codecs can be set behind the NAT router | |
| Method suitable for mobile network access | |

[1] Although not with so called « symmetric » NAT routers

## 3.3. NAT router with DMZ

Situation: codec A behind a NAT router and placed in « DMZ ».
We also assume that the other codec (B) is accessible with a public address.

Once codec A is configured for using a STUN server:

- codec A can initiate a connection to (call) codec B
- codec B can call codec A, using the public address of the NAT router

| Advantages | Drawbacks |
|---|---|
| Each codec can set up a session | Need to configure the router |
| A is nearly equivalent to a codec with a direct public access | Only one codec can be set up in this way on a LAN |
| | A is exposed to external attacks |
| | The DMZ may be already reserved for other network equipment |
| | Method not possible for a mobile network access |

## 3.4. NAT router with port forwarding

Situation: codec A behind a NAT router and configuration of the router to forward to A the necessary ports.
We also assume that the other codec (B) is accessible with a public address.

Port forwarding to be set on the router:

- UDP 5060 (=SIP port)
- UDP 5004 (RTP port) and 5005 (RTCP port)[1]

Once codec A is configured for using a STUN server:

- codec A can initiate a connection to (call) codec B
- codec B can call codec A, using the public address of the NAT router

| Advantages | Drawbacks |
|---|---|
| Each codec can set up a session | Need to configure the router |
| A is nearly equivalent to a codec with a direct public access | Only one codec can be set up in this way on a LAN |
| | Method not possible for a mobile network access |

[1] For Scoop4+ versions before 1.32, ports 9000 and 9001 respectively

### 3.5. Use of a SIP server

In addition to the numerous features it brings along, using a SIP proxy server is a very powerful method to solve the issues related to NAT routers, because most SIP proxies are capable to detect the presence of NAT routers and/or deal appropriately with their traversal.

If a SIP server is available, and once the codecs are registered on this server:

- Any registered codec can call another registered[1] codec, regardless whether there is or not a NAT router on the path.
- The identifier (SIP URI) is stable and does not depend on the location of the called agent ("mobility" feature).

It is possible either to use a public server on the Internet, or to install a private server accessible via the Internet.

| Advantages | Drawbacks |
|---|---|
| Each codec can initiate a session<br>Each codec can receive calls | Installation may not be easy (private server) |
| Identification is simple and location/time-wise stable | Reliability of server questionable (public server) |
| Security : a private proxy can be linked with a firewall | |
| Also works with symmetric NAT routers | |
| Interoperation with telephony over IP | |
| Method suitable for mobile network access | |

[1] Depending on the access control policy, a server may accept « outgoing » calls to third party domains, or accept « incoming » calls from non registered agents.

AETA AUDIO SYSTEMS

## 4. Summary and reminder of essential rules

The table below sums up the situations where a link can be set up (not using a SIP proxy server) and reminds the needed specific settings :

| | Codec A access | Possible calls | Codec B access | Notes |
|---|---|---|---|---|
| 1 | LAN | ⇒ ⇐ | LAN (same) | |
| 2 | Private WAN | ⇒ ⇐ | Private WAN | |
| 3 | Internet direct | ⇒ ⇐ | Internet direct | |
| 4 | NAT | ⇒ | Internet direct | STUN needed for A |
| 5 | NAT + DMZ | ⇒ ⇐ | Internet direct | STUN needed for A |
| 6 | NAT + port forwarding | ⇒ ⇐ | Internet direct | STUN needed for A<br>UDP ports 5004, 5005, 5060 |
| 7 | NAT | ⇒ | NAT + DMZ | STUN needed for A and B |
| 8 | NAT + DMZ | ⇒ ⇐ | NAT + DMZ | STUN needed for A and B |
| 9 | NAT + port forwarding | ⇒ ⇐ | NAT + DMZ | STUN needed for A and B<br>UDP ports 5004, 5005, 5060 |
| 10 | NAT | ⇒ | NAT + forwarding | STUN needed for A and B |
| 11 | NAT + DMZ | ⇒ ⇐ | NAT + forwarding | STUN needed for A and B |
| 12 | NAT + port forwarding | ⇒ ⇐ | NAT + forwarding | STUN needed for A and B<br>UDP ports 5004, 5005, 5060 |

**Basic rule: Codec behind a NAT router => use a STUN server.**
This allows the codec to set up outgoing calls. This is *not sufficient* to be accessible to connection requests from the outside.

**Mobile network access without SIP server or VPN => use a STUN server**

**NAT + DMZ or NAT + forwarding => incoming calls are possible.**
**Incoming calls are not possible behind a NAT router without either such change or a SIP proxy.**

**SIP server => maximum versatility, at the expense of some initial effort (for installation)**
Important note: contrary to a common but wrong belief, the SIP protocol (always used by AAS codecs) *does not impose the use of a SIP* ***server***. Codecs can set up point-to-point links using this protocol in the above described conditions. When no SIP *registrar* is involved, the identifiers are simply the IP addresses of the codecs.

# 5. Glossary

| Term or abbreviation | Meaning |
|---|---|
| AoIP | *Audio over IP*, audio via an IP protocol network |
| DMZ | Zone, sub-network or specific IP address which escapes the firewall rules and is directly « visible » from outside the local area network. |
| DNS | *Domain Name Server*. Carries out the resolution of symbolic names into numeric addresses. |
| NAT | *Network Address Translation*. A NAT router is typically used to share one or a few public IP addresses for a private sub-network. |
| SIP | *Session Initiation Protocol,* protocol used for signalling multimedia communication sessions (audio in the context of this document) |
| STUN | *Simple Traversal of UDP through NATs,* protocol allowing a client behind a NAT router to discover its public IP address. |
| URI | *Uniform Resource Identifier,* identifier of a SIP "agent" (terminal implementing the SIP protocol to set up a link) |