estos STUN/TURN Server

7.1.7.4336

1 Welcome to estos STUN/TURN Server

Direct audio/video communication has become an important component of modern collaboration.

To implement this in a technically efficient way while keeping internal networks secure, framework conditions must be adhered to which at first glance make it difficult to establish direct communication across network boundaries.

A NAT router, which often makes in difficult or impossible for an external computer to contact with an internal client without a request, is often used in private IP4 networks to increase security.

Unfortunately, this also blocks the connections necessary for efficient audio/video communications.

In order to produce these desired compounds, these techniques include STUN and TURN, which are implemented in the estos STUN/TURN Server.

estos STUN/TURN Server consists of the following components:

- The estos STUN/TURN Server
- The Installation- und Configurationprogram
- The Online Help

The configuration program and online help is always available via the Start Menu.

1.1 Chapter Overview

Terms and scenarios for use involving STUN and TURN will be described in the Functionality section.

The Requirements section describes the system requirements necessary for installing and running the service.

The chapter Installation and Configuration specifies the recommended installation procedure and configuration options.

The chapter information describes about the estos STUN/TURN Server how to obtain support for technical questions and concerns.

2 Requirements

For the operation of the estos STUN/TURN Server the following requirements must be met:

- **Operating system**
  The service can be installed on the following operating systems:
    - Windows® 8.1
    - Windows® 10
    - Windows Server® 2012
    - Windows Server® 2012 R2
    - Windows Server® 2016
    - Windows Server® 2019

- **TCP / IP protocol support with the corresponding connectivity to the Internet**
  Because of a TURN server's function of terminating and forwarding media streams, network connection requirements must be geared to the number and type of connections which are simultaneously supported:
  An single VideoChat requires between 300kbit/s and 2,3 Mbit/s per direction.
  An single AudioChat requires typically 45 kbit/s per direction.

3 Operating Mode

The estos STUN/TURN Server is implemented as system service which provides STUN- und TURN-Server functionality.

The following briefly describes what a STUN/TURN service is and which problems can be solved with it in the audio/video communication environment. Subsequently, the main use cases are being described.

This description is intended to give a basic understanding of the subject without going too much into detail.

3.1 Components and terms

NAT - Network Address Translation (RFC 2663)
NAT describes the translation of "internal" IPv4 address space on the LAN to "external" IPv4 addresses (and ports) on the Internet. This increases the security of the internal network, by preventing direct, unwanted access to internal addresses from outside.

A NAT device is e.g. a router connecting a LAN to the Internet.

Symmetric NAT
In addition to a normal NAT router, these routers will not only track internal client addresses, but also destination addresses contacted by you and permit data from these addresses only to enter the internal network. A third party Client cannot send data to the internal client, even if the IP addresses (and ports) were known. In this scenario audio/video communication is only possible by using a TURN server.

NAT Traversal
NAT Traversal refers to techniques for setting up and maintaining connections through a devices implementing NAT. These techniques include STUN and TURN.

STUN stands for Session Traversal Utilities for NAT (see RFC5389)
This protocol makes identification of a client behind a NAT device possible through its public IP address.

The client on the LAN making the call can then provide its IP address (and port number) to the client to be called, in order to make direct communication (a peer-to-peer connection) possible.

TURN means Traversal Using Relays around NAT (see RFC5766)
A server in the Internet which implements the TURN protocol makes it possible for two clients to exchange data without a direct connection ("relay server"). This must be done if it is not possible for a client-to-client connection to be established.

ICE means Interactive Connectivity Establishment (see RFC5245)
With the help of STUN and TURN, two clients can exchange the connection information (and other data) detected with the help of the ICE protocol. The information must be transmitted using an internal service (a so-called signaling server). This service must be accessible from both clients.

Both clients will be collected ICE information, so-called ICE candidates. For this purpose, both clients will collect various candidates (potential protocols and the associated IP addresses with ports) from their LANs. The two clients then exchange these candidates over signaling servers then attempt to reach the other client by using the most appropriate candidate.

Signaling Server
Signaling Server are used for indirect exchange of data between two clients. This may be a service that is accessible from both clients (eg a UCServer in a network) or more services, which are interconnected by federation (eg two UCServer of two companies which have established a XMPP Federation).

3.2 Use cases

In the following the main use cases of STUN/TURN services are described in more detail.

Direct communication is possible (STUN & TURN services are not needed)

To receive media streams from Client B, Client A has to send his contact information (IP address and port) to Client B. This is usually done via a signaling server to which both clients must have a connection. As long as both clients are in the same LAN, direct communication is not a problem. Fig. 1 clarifies this situation. In Step 1, Client A will send its IP address and port to Client B using the signaling server. In Step 2, Client B can begin sending a media stream to Client A.

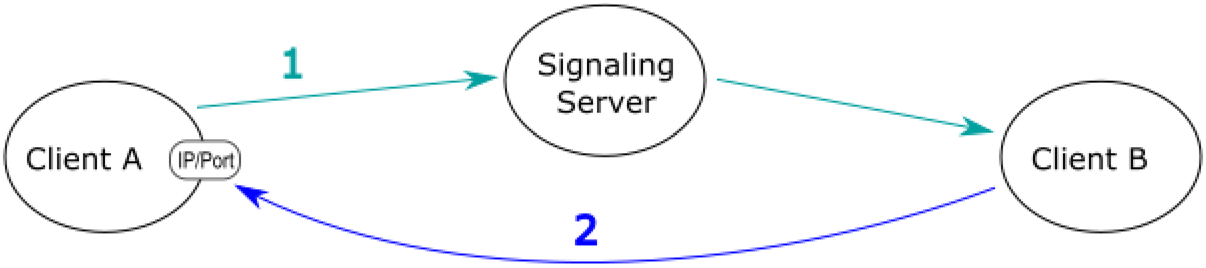

Fig. 1: A client is directly accessible. Client B can send the media stream directly to client A.

One client is behind a NAT router

If both Client A and Client B are in different LANs and separated by a NAT router, the scenario above will fail. Because Client A does not know that it should use the public IP address and port for the NAT router for transferring to Client B, Client will tell Client B to use the local IP address and port. Because that address is not accessible for Client B, transferring the media stream will fail in Step 2 (see Fig. 2).

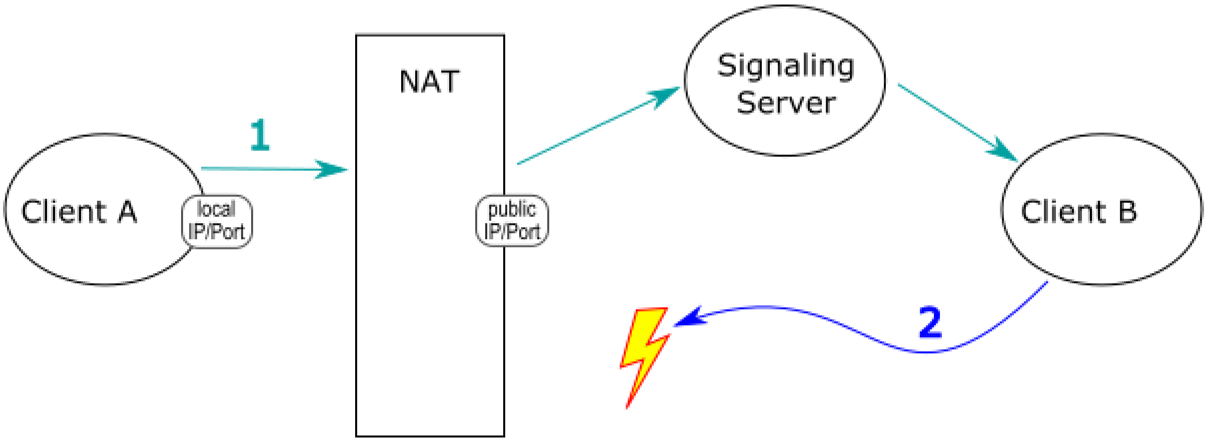

Fig. 2: Unsuccessful connection setup through a NAT router.

The non-accessibility problem can be solved by using a STUN server as shown in Fig. 3. With the help of the STUN server, Client A can determine its public IP address & port in Step 1. It can then transmit the correct information to Client B, which can then send its media stream to the public IP address of the NAT router. The NAT router will then forward the media stream to Client A.

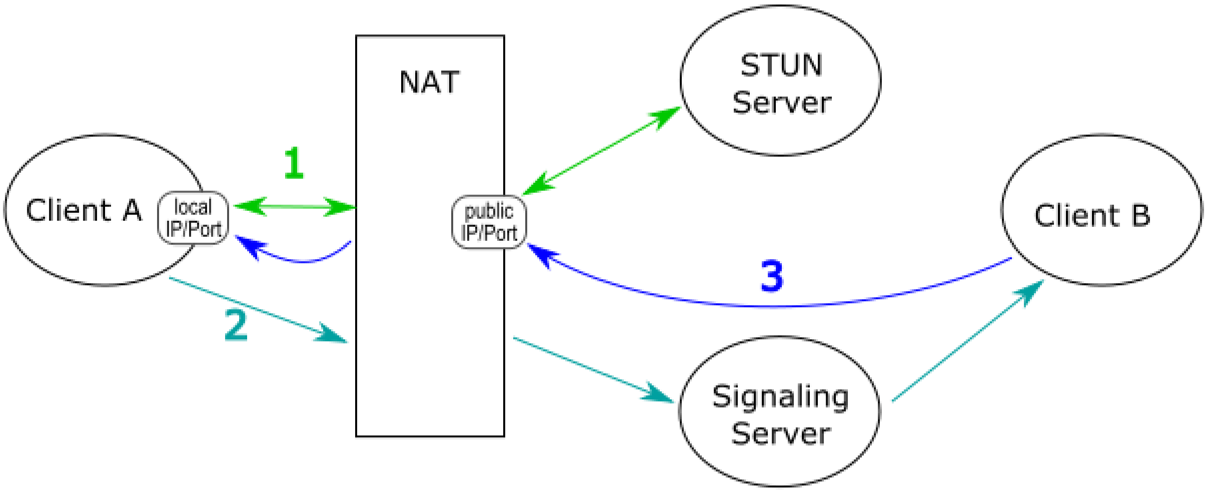

Fig. 3: Successful communication with the help of a STUN server

At least one client cannot be reached from outside the network (symmetric NAT router).

The previous solution will not work for all NAT implementations. There is a class of NAT systems, indicated by the term symmetric NAT, which open a port not just for one LAN Client A, but rather open a port for each individual connection. As a consequence, Client A can still request its public IP address & port from the STUN server, which would be invalid for connections with Client B.

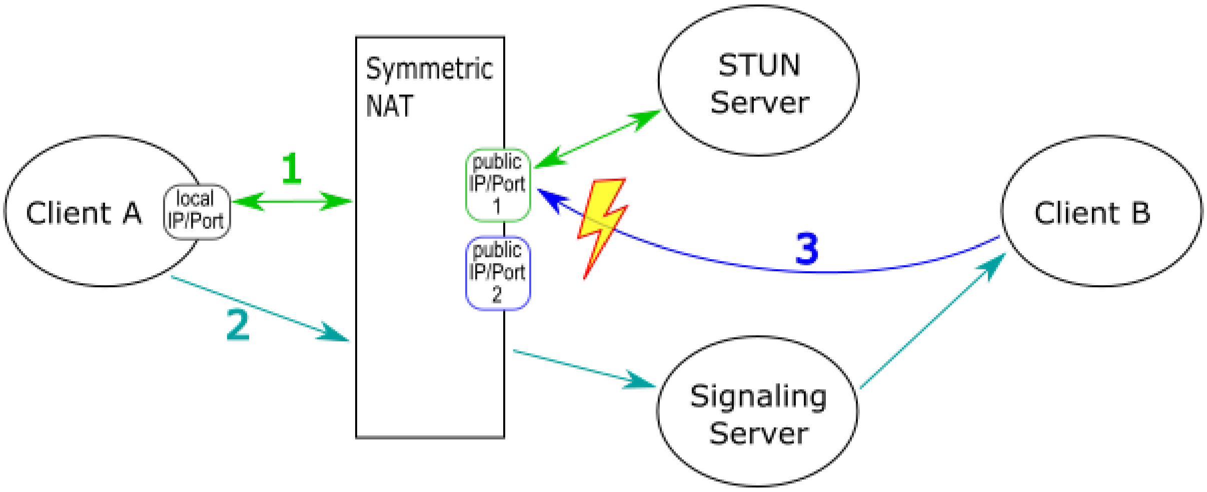

Fig. 4: Unsuccessful communication attempt through a symmetric NAT setup

Because the correct public port cannot be determined from the STUN server, sending the media stream from Client B will fail.

In order to solve the problem with the a "Symmetric NAT", a TURN server is needed (see Fig. 5). Once Client A determines that direct and STUN connections are not possible (step 1), he may notify Client B via the Signaling Server about a common known TURN server (step 2). In step 3, both clients are connected through the TURN server and are able to communicate.

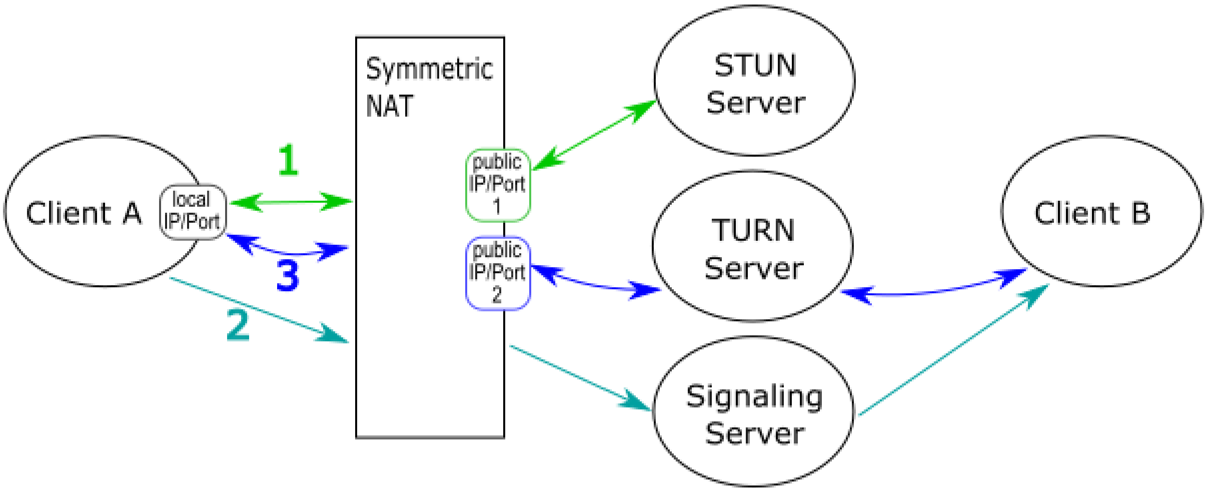

Fig. 5: Successful communication attempt via a "symmetric NAT", using a TURN server.

Because the useful data will be transferred directly through the TURN server, a TURN server must fulfill very high demands with regard to bandwidth, in particular given multiple parallel connections. For this reason, this solution will only be chosen when there are no other options for transferring data.

4 Installation and configuration

4.1 Installation

The installation and setup of estos STUN/TURN Server will be started simply by double-clicking on the installation package. Doing so will start the installation wizard, which will then execute the installation of the service on the computer.

The configuration wizard, which will perform the steps individually necessary for setup, will be started afterwards. The service can be used afterwards.

4.2 Configuration

Several settings will be required for operation of estos STUN/TURN Server. estos STUN/TURN Server's administration program will be used to make these settings.

4.2.1 General

That clients are able to request the service a network interface must be set up.

IP Address
Configure the IP interface through which services can be accessed by clients.

Port
Default setting for the port is 3478.

4.2.2 TURN Configuration

Password
Because transferring media data between clients will place high bandwidth demands on the interface, access is protected by a password. This password must also be entered in UCServer.

4.2.3 Diagnose

The service can be stopped and started in this dialog. It shows its current status.

Configuration of the logging to help diagnose problems.

State
Buttons to start and stop the service. If the STUN/TURN Server is terminated unexpected, an error code will be displayed.

Logging

- **Log Level**
  Sets whether debug information is written into the log files.
- **Maximun size of a log file.**
  There are several log files written. Each log file is cyclically re-created when the size set here is exceeded.
- **Log Directory**
  The log files are stored in this directory . Note that the service requires appropriate write permissions.

- **Delete Log Files**
  Log files in the log directory will be deleted. This is available only while the STUN/TURN Server is running.
- **Provide Log Files**
  Log files in the log directory will be packed into a ZIP-file. The location and name of the ZIP-file can be set in a dialog.

Info

General Service Information

5 Info about estos STUN/TURN Server

The estos STUN/TURN Server is a product of estos GmbH.

You will find product updates at https://www.estos.de/

Frequently asked questions and answers and also support are available at https://support.estos.de