estos STUN/TURN Server

7·3·3·5345

1 Willkommen zum estos STUN/TURN Server

Direkte Audio/Video-Kommunikation ist ein wichtiger Bestandteil moderner Zusammenarbeit geworden.

Um dies technisch effizient umsetzen zu können und gleichzeitig dabei interne Netzwerke sicher zu halten, müssen Rahmenbedingungen eingehalten werden, die es auf den ersten Blick schwierig machen, eine direkte Kommunikation über Netzwerkgrenzen hinaus zu etablieren.

In privaten IPv4 Netzwerken wird zur Erhöhung der Sicherheit oft ein NAT-Router eingesetzt, der es einem externen Computer erschwert bzw. unmöglich macht, einen internen Client ohne Aufforderung zu kontaktieren.

Leider werden hierdurch auch die für die effiziente Audio/Video-Kommunikation notwendigen Verbindungen gesperrt.

Um diese und ähnliche, eigentlich gewünschten Verbindungen dennoch herstellen zu können, wurden Techniken entwickelt, die es ohne Verminderung der Sicherheit erlauben Audio/Video-Kommunikation zu betreiben. Zu diesen Techniken gehören STUN und TURN, die mit dem estos STUN/TURN Server umgesetzt werden.

Der estos STUN/TURN Server besteht aus folgenden Komponenten:

- Dem estos STUN/TURN Server
- Dem Installations- und Konfigurationsprogramm
- Der Onlinehilfe

Das Konfigurationsprogramm und die Onlinehilfe sind jederzeit über das Startmenü verfügbar.

1.1 Kapitelübersicht

Im Kapitel Funktionsweise werden verwendete Begriffe und Einsatzszenarien rund um STUN und TURN beschrieben.

Der Abschnitt Voraussetzungen beschreibt die Systemvoraussetzungen, welche für die Installation und den Betrieb des Dienstes notwendig sind.

Im Kapitel Installation und Konfiguration wird die Installation und die nötige Konfiguration beschrieben.

Das Kapitel Informationen über den estos STUN/TURN Server beschreibt, wie Sie bei technischen Anliegen und Fragen Unterstützung erhalten.

2 Voraussetzungen

Für den Betrieb des estos STUN/TURN Servers müssen folgende Voraussetzungen erfüllt sein:

- **Betriebssystem**
  Der Dienst kann auf folgenden Betriebssystemen installiert werden:
  - Windows® 8.1
  - Windows® 10
  - Windows® 11
  - Windows Server® 2012
  - Windows Server® 2012 R2
  - Windows Server® 2016
  - Windows Server® 2019
  - Windows Server® 2022

- **TCP/IP-Protokollunterstützung mit entsprechender Anbindung an das Internet**
  Durch die Funktion eines TURN-Servers, Media-Streams zu terminieren und weiterzuleiten, sind die Anforderungen an die Netzwerkanbindung entsprechend der Anzahl und des Typs der gleichzeitig unterstützten Verbindungen auszulegen:
  Ein VideoChat benötigt zwischen 300kbit/s bis 2,3 Mbit/s pro Richtung.
  Ein AudioChat benötigt typisch 45 kbit/s pro Richtung.

3 Funktionsweise

Der estos STUN/TURN Server ist als Systemdienst implementiert, welcher die STUN- und TURN-Server Funktionalität zur Verfügung stellt.

Im Folgenden wird kurz beschrieben was ein STUN-/TURN-Dienst macht und welche Probleme er bei der Audio/Video Kommunikation zwischen zwei Clients beseitigt. Anschliessend werden noch die Hauptanwendungsfälle aufgezeichnet.

Diese Beschreibung soll dazu dienen ein grundlegendes Verständnis für die Thematik zu vermitteln und geht nicht auf genauere Details ein.

3.1 Beteiligte Komponenten und Begriffe

NAT - Network Address Translation (RFC 2663)
NAT beschreibt die Umsetzung des "internen" IPv4-Adressraums eines LAN zu "externen" IPv4-Adressen (und Ports) im Internet. Das trägt zur Sicherheit des internen Netzes bei, da von aussen kein direkter, ungewünschter Zugriff auf interne Adressen erfolgen kann.

Ein NAT Device ist z.B. ein Router, der ein LAN mit dem Internet verbindet.

Symmetric NAT
Zusätzlich zum normalen NAT merken sich diese Router nicht nur die interne Client Adresse, sondern auch die von ihm angesprochene Zieladresse und lässt Daten nur von dieser in das interne Netz gelangen. Ein anderes Ziel kann also keine Daten an den internen Client senden, selbst wenn die IP-Adressen (und Ports) bekannt wären. Für eine Audio/Video Kommunikation ist in diesem Fall nur in Verbindung mit einem TURN-Server möglich.

NAT Traversal
"NAT Traversal" bezeichnet Techniken zum Aufbau und Halten von Verbindungen über NAT-Umsetzungsstellen hinweg. Zu diesen Techniken gehören STUN und TURN.

STUN - Session Traversal Utilities for NAT (RFC5389)
Dieses Protokoll ermöglicht es einem Client in einem LAN, seine eigene, öffentliche IPv4-Adresse zu ermitteln.

Der rufende Client im LAN kann auf diese Weise dem angerufenen Client ausserhalb des LAN mitteilen, welche IPv4-Adresse (und Portnummer) verwendet werden kann um eine direkte Kommunikation mit ihm zu ermöglichen ("Peer-to-Peer" Verbindung).

TURN - Traversal Using Relays around NAT (RFC5766)
Ein Server im Internet, der das TURN-Protokoll implementiert, ermöglicht es zwei Clients, Daten ohne eine direkte Verbindung auszutauschen ("Relay Server"). Dies wird notwendig, wenn es keine Möglichkeit gibt, eine direkte Client-zu-Client-Verbindung aufzubauen.

ICE - Interactive Connectivity Establishment (RFC5245)
Zwei Clients können die mit Hilfe von STUN und TURN ermittelten Verbindungsinformationen (und andere Daten) mit Hilfe des ICE Protokolls austauschen. Die Übermittlung der Informationen muß dabei über einen eigenen Dienst erfolgen, einen sog. "Signaling Server". Dieser Dienst muß von beiden Clients erreichbar sein.

Das Zusammenstellen einer ICE Informationen, sog. ICE Kandidaten, erfolgt durch beide Clients. Dazu sammeln beide die verschiedene Kandidaten (mögliche Protokolle und dazugehörende IP-Adressen mit Ports) aus ihrem LAN heraus ein. Die beiden Clients tauschen diese Kandidaten anschliessend über die Signaling Server aus und versuchen daraufhin, den jeweils anderen mit Hilfe des passendsten Kandidaten zu erreichen.

Signaling Server
Signaling Server dienen zum indirekten Austausch von Daten zwischen zwei Clients. Dies kann ein Dienst sein, der von beiden Clients erreichbar ist (z.B. ein UCServer in einem Netzwerk) oder auch mehrere Dienste die mittels Federation miteinander verbunden sind (z.B. zwei UCServer zweier Firmen, die eine XMPP Federation eingegangen sind).

3.2 Anwendungsfälle

Im Folgenden werden die Hauptanwendungsfälle der STUN/TURN-Dienste etwas ausführlicher gezeigt.

Direkte Kommunikation ist möglich (kein STUN/TURN-Dienst notwendig)

Damit Client A die Medienströme von Client B empfangen kann, muß Client A zunächst Client B seine Kontaktdaten (IP-Adresse und Port) mitteilen. Dies geschieht in der Regel über einen Signaling-Server, zu dem beide Clients eine Verbindung haben. Solange sich beide Clients im gleichen LAN befinden ist dies problemlos möglich. Abb. 1 verdeutlicht dies. In Schritt 1 sendet Client A seine IP-Adresse und Port über den Signaling Server an Client B. Daraufhin kann Client B in Schritt 2 damit beginnen einen Medienstrom an Client A zu senden.

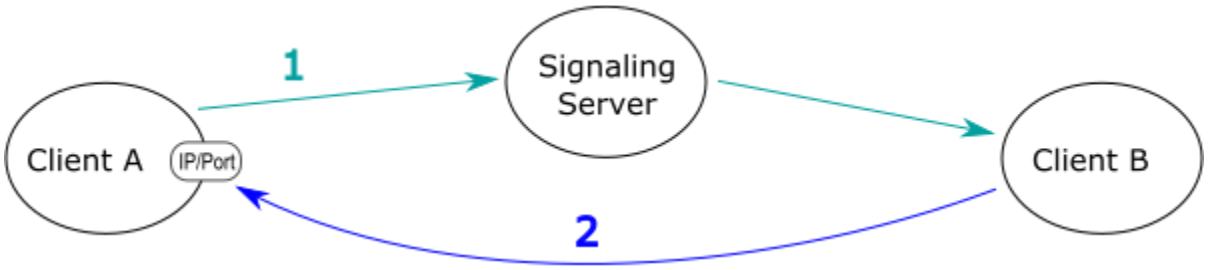

Abb. 1: Client A ist direkt erreichbar. Client B kann den Medienstrom direkt an Client A senden.

Ein Client befindet sich hinter einem NAT-Router

Befinden sich Client A und Client B in verschiedenen LANs, die durch einen NAT-Router getrennt sind, wird das obige Szenario fehlschlagen. Da Client A nicht weiß, dass er gegenüber Client B mit der öffentlichen IP-Adresse und Port des NAT-Routers erscheint, würde Client A in Schritt 1 seine lokale IP-Adresse und Port an Client B signalisieren. Da diese Adresse aber für Client B nicht erreichbar ist, schlägt das senden des Medienstroms (Schritt 2) fehl (siehe Abb. 2).

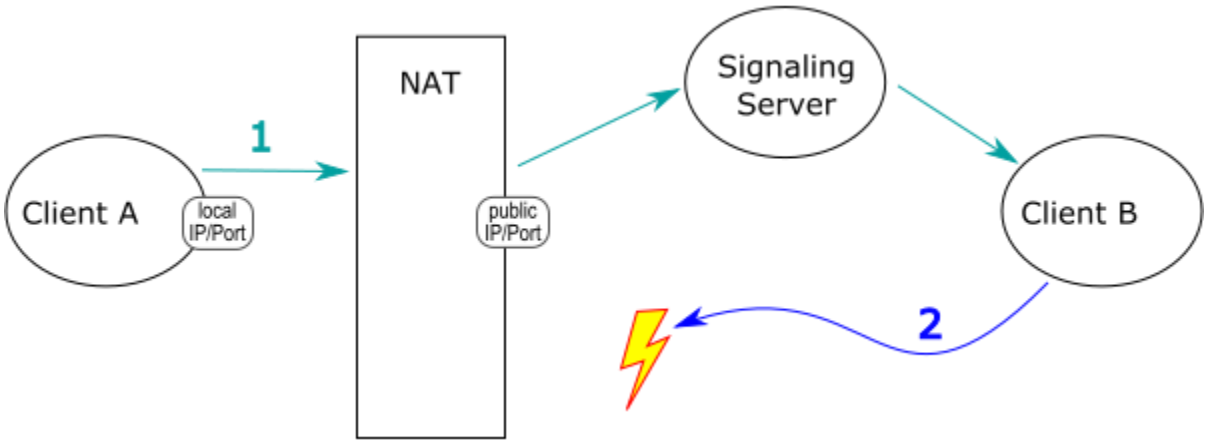

Abb. 2: Erfolgloser Verbindungsaufbau über einen NAT-Router hinweg.

Das Nichterreichbarkeitsproblem kann mit Hilfe eines STUN-Servers gelöst werden wie in Abb. 3 dargestellt. Mit Hilfe des STUN-Servers kann Client A in Schritt 1 seine öffentliche IP-Adresse und Port ermitteln. Diese kann er dann in Schritt 2 an Client B übermitteln woraufhin dieser seinen Medienstrom an die öffentlich erreichbare Adresse des NAT-Routers senden kann. Der NAT-Router leitet den Medienstrom dann an Client A weiter.

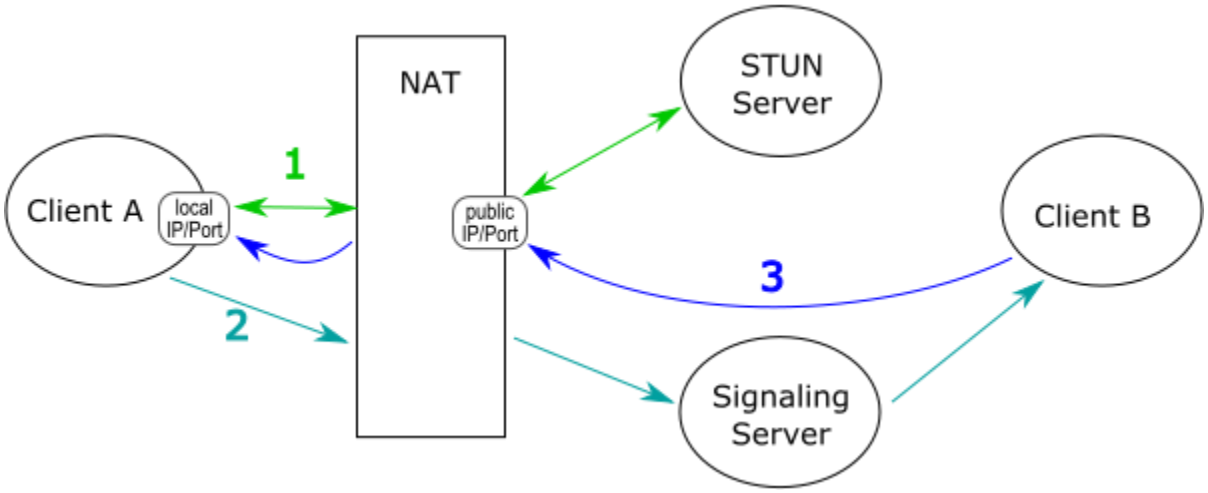

Abb. 3: Erfolgreiche Kommunikation unter Zuhilfenahme eines STUN-Servers.

Mindestens ein Client kann von aussen gar nicht erreicht werden (Symmetric NAT-Router)

Die vorherige Lösung funktioniert allerdings nicht für alle NAT Ausprägungen. Es gibt eine Klasse von NATs, die sog. "Symmetric NAT", die nicht nur einen öffentlichen Port für einen LAN Client A öffnen, sondern für auch jede einzelne Verbindung nach aussen. Das hat zur Folge, dass Client A zwar nach wie vor seine öffentliche IP-Adresse/Port vom STUN-Server abfragen kann, diese wären dann aber für Verbindungen mit Client B nicht gültig.

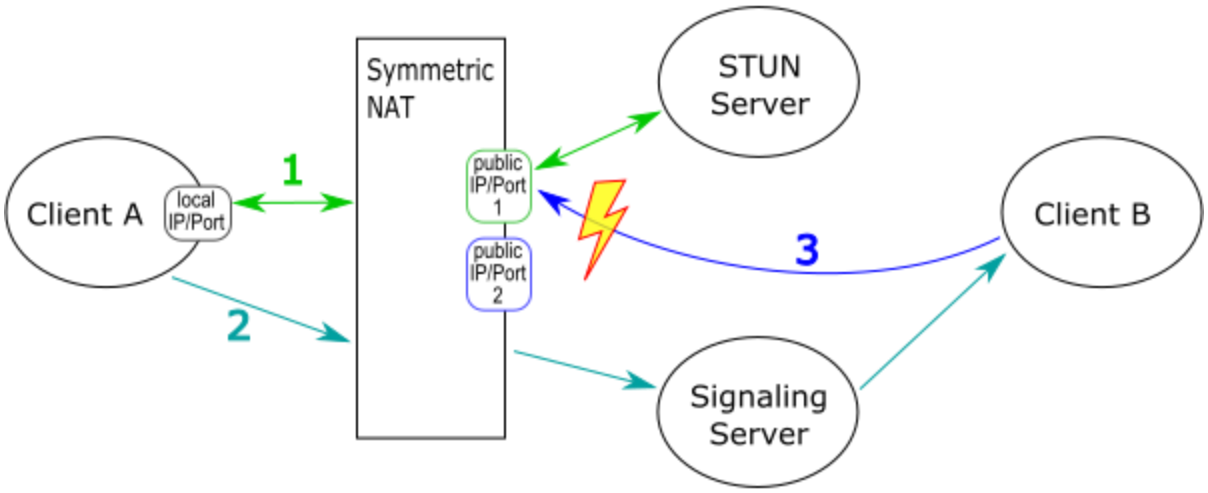

Abb. 4: Erfolgloser Kommunikationsversuch über ein "Symmetric NAT".

Da der korrekte öffentliche Port über den STUN-Server nicht ermittelt werden kann, schlägt das Senden eines Medienstroms von Client B fehl.

Um dieses Problem mit dem "Symmetric NAT" zu lösen, benötigt man einen TURN-Server (siehe Abb. 5). Sobald Client A feststellt, dass direkte und STUN Verbindungen nicht möglich sind (Schritt 1), kann er Client B über den Signaling-Server mitteilen, dass er eine Verbindung zu einen gemeinsam bekannten TURN-Server

(Schritt 2) aufbauen soll. In Schritt 3 haben beide Clients eine Verbindung zum TURN Server und können darüber nun Daten austauschen.

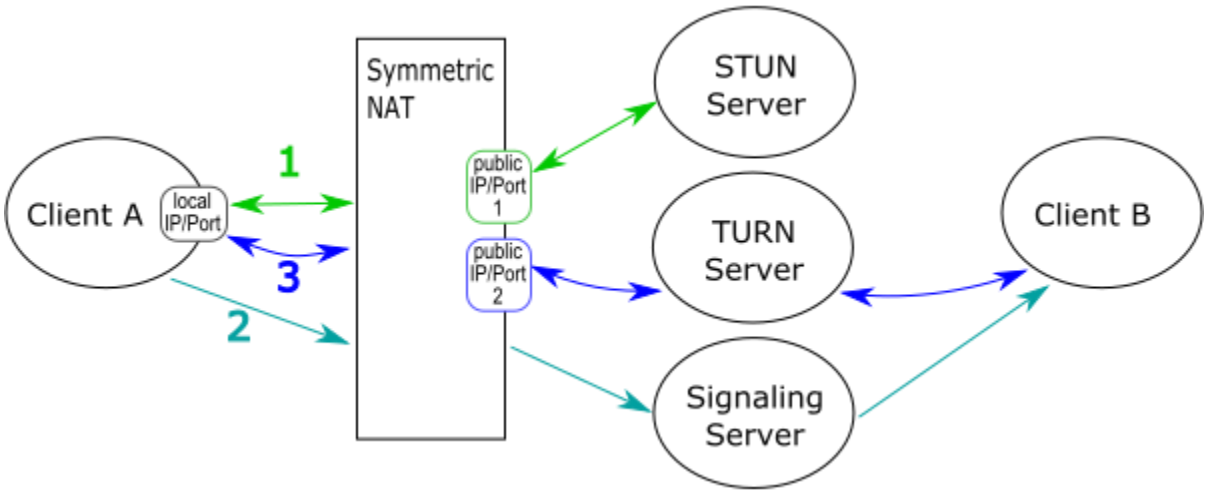

Abb. 5: Erfolgreicher Kommunikationsversuch über ein "Symmetric NAT" durch Nutzung eines TURN-Servers.

Da die Nutzdaten bei dieser Lösung direkt über den TURN-Server fließen hat ein TURN-Server insbesondere bei mehreren parallelen Verbindungen sehr hohe Anforderungen an die Bandbreite zu erfüllen. Deshalb wird diese Lösung nur dann gewählt, wenn es keine andere Möglichkeit für eine Datenübertragung gibt.

4 Installation und Konfiguration

4.1 Installation

Die Installation und Einrichtung eines estos STUN/TURN Servers wird einfach durch Doppelklick auf das Installationspaket gestartet.Damit startet der Installationsassistent, der durch die Installation des Dienstes auf dem Computer führt.

Anschließend startet der Konfigurationsassistent, der durch die einzelnen, notwendigen Einrichtungsschritte führt. Danach ist der Dienst einsatzbereit.

4.2 Konfiguration

Für den Betrieb des estos STUN/TURN Servers sind einige Einstellungen notwendig. Um diese Einstellungen vorzunehmen wird das Administrationsprogramm des estos STUN/TURN Servers verwendet.

4.2.1 Allgemein

Damit Clients Anfragen an den Dienst stellen können muss eine Netzwerkschnittstelle eingerichtet werden.

IP Adresse
Konfigurieren Sie das IP-Interface, über welches die Dienste für die Clients erreichbar sind.

Port
Voreinstellung für den Port ist 3478.

4.2.2 TURN Konfiguration

Passwort
Da der Transfer der Mediadaten zwischen den Clients eine hohe Bandbreitenanforderungen an die Schnittstelle stellt, ist der Zugriff durch ein Passwort geschützt. Dieses muss im UCServer ebenfalls eingegeben werden.

4.2.3 Diagnose

In diesem Dialog kann der Dienst beendet und gestartet werden. Es wird der aktuelle Status des Dienstes angezeigt.

Außerdem können hier die Log-Dateien zur Diagnose von Problemen konfiguriert werden.

Status
Mit den entsprechenden Schaltflächen kann der Dienst gestartet und beendet werden. Ist der STUN/TURN Server gestoppt, wird ein im Fehlerfall vorhandener Fehlercode ausgegeben.

Logging

- **Log Level**
  Stellen Sie hier ein, ob der Dienst Log-Dateien schreiben soll.
- **Maximale Größe einer Log-Datei**
  Es werden mehrere Log-Dateien geschrieben. Jede Log-Datei wird zyklisch neu angelegt, wenn die hier eingestellte Größe überschritten ist.

- **Log-Dateipfad**
  In diesem Verzeichnis werden die Log-Dateien abgelegt. Beachten Sie, dass der Dienst entsprechende Schreibrechte in diesem Verzeichnis benötigt.
- **Log-Dateien löschen**
  Die im Log-Dateipfad liegenden Log-Dateien werden gelöscht. Dies kann nur bei gestartetem STUN/TURN Server ausgeführt werden.
- **Log-Dateien bereitstellen**
  Die im Log-Dateipfad liegenden Log-Dateien werden in eine ZIP-Datei gepackt. In einem Dialog können Sie den Speicherort und den Dateinamen bestimmen.

Info
Hier werden allgemeine Informationen (z.B. Version) zum Dienst angezeigt.

5 Informationen über den estos STUN/TURN Server

Der estos STUN/TURN Server ist ein Produkt der estos GmbH.

Produkt Updates finden Sie unter https://www.estos.de/

Häufig gestellte Fragen und Antworten, sowie Support erhalten Sie unter https://support.estos.de