# NAT Traversal at the DTAG VoIP Platforms

Deutsche Telekom Technik GmbH

# Version 1.02

Sachstand 30.04.2015

Schutzklasse Extern

Dokumententyp

Persönliche Unterlage von ……………………………………………… ……………………..

(Vorname, Nachname) (Unterschrift)

Impressum

|  |  |  |
| --- | --- | --- |
| Herausgeber | | |
| Deutsche Telekom Technik GmbH  Fixed Mobile Engineering Deutschland Heinrich-Hertz-Str. 3-7 64295 Darmstadt | | |
|  |  |  |
| Autor | Inhaltlich geprüft von | Freigegeben von |
|  |  |  |
|  |  |  |
|  |  |  |
| Kurzinfo | | |
| Beschreibung des High Level Designs im Rahmen einer Machbarkeitsuntersuchung des Projektes Plattformsteuerung 3.0 und Basis für das Detailed Design. Das High Level Design behandelt die Möglichkeit einer Architektur der Plattformsteuerung ohne Mainframe und mit einer eigenen Datenbank für Session-Kontexte. | | |

# Mitarbeiterverweise

Die vorliegende Arbeitsunterlage gilt innerhalb der benannten Verantwortungsbereiche Deutschen TelekomTechnik GmbH und wurde gemeinsam mit den nachfolgend aufgeführten Expertinnen/Experten aus den an der Produktion beteiligten Bereichen erstellt und abgestimmt.

|  |  |
| --- | --- |
| **Name** | **Email** |
| Beck, Wolfgang | BeckW@telekom.de |
|  |  |
|  |  |
|  |  |

Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Stand | Bearbeiter | Änderungen / Kommentar |
| 0.5 | 29.2.2016 | Wolfgang Beck | Basisversion |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. SIP Trunk support on GK-Platform
   1. SIP Trunk is used to connect Voice over IP communication systems of business customers to the “User-to-network” interface of the GK-Platform. It integrates everything from data, the internet and voice services into a single line and suits the needs of a small businesses as well as of large corporations.
   2. In the context of SIP-Connect-Standards, GK-Platform, as a part of SIP-Service-Provider of the public network infrastructure, offer the connection of the telephone communication systems to the public telephone network, PSTN or NGN.
2. Configuration of the CPE-parameter NAT\_MODE on the CPE-Environments

CPE Environment’s configuration of the customer’s SIP- PBX may be customized. These specific characteristics of the CPE-Environment include also the configuration of the parameter NAT\_MODE. The NAT\_MODE parameter describes which configuration of NAT/PAT shell be implemented on the customer equipment. Also define the behavior of the customer’s infrastructure related to the traversing the SIP requests.

On customer’s infrastructure can be configured next modes of NAT:

* 0-No translation required;
* 1- NAT-Traversal according to the TAS-Proxy-Method (e.g. recognition of private addresses in contact, SDP);
* 272 - NAT Traversal with translation of Source Port and Source IP Address;
* 544 - NAT Traversal with IP Address and Port translation of initially used source address.

The default behavior is 272 mode.

These settings have an influence on how the GK-Contacts shell be treated during the registration as well as how the initial SIP requests and subsequent requests within the dialog shell be delivered/traversed.

This section describes a different realizations of NAT, depending on which type of NAT/PAT the IP Gateway (the router) provides.

* 1. Symmetric NAT

This is a very restricted method of Address and Port Translation, which means that new mapping for each different connection has to be made. That means 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 but 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 packet back to the internal host.

* 1. 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.

* 1. Restricted Cone

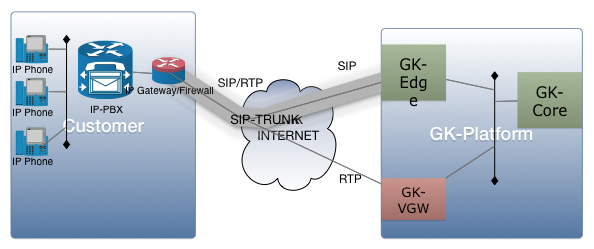
All requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

* 1. Port-Restricted-Cone NAT

In this type of NAT 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.

1. SIP-Trunk Topology in GK-TAS Environment

This section describes a different realizations of NAT, depending on which type of NAT/PAT the IP Gateway (the router) provides. The most common topology in the Business Customer’s Access (GK) is presented on the following figure:



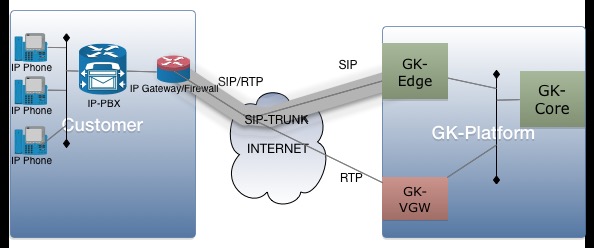


Figure 3.

On the CPE side there are next components installed:

* SIP-PBX (IP-PBX);
* SIP- phones as an End-user equipment;
* IP-Gateway (IP-Access-Gateway/Router) at the point of IP connection to the Internet.

On the Service Provider side is GK-Platform. GK-Edge and GK-VGWs components are dedicated to accept the SIP signalization and RTP stream respectively.

1. NAT-Traversal Scenarios in GK-TAS Environments

The NGN provides functionalities to support PBXs using different types of NAT with e.g. a private IP-address for SIP-Header and –body without using e.g. STUN. In some scenarios will be necessary to use a protocol such a STUN (TURN/ICE?) that combined with NGN functionalities can provide a complete media traversal solution for NATs.

STUN is a lightweight tool kit and protocol that provides details of the external IP address/port combination used by the NAT device to represent the internal entity on the public facing side of NATs.

Traversal of SIP through existing NATs can be divided into two discrete problem areas: getting the SIP signaling across NATs and enabling media as specified by SDP in a SIP offer/answer exchange to flow between endpoints.

This section of the document includes detailed NAT traversal scenarios for both SIP signaling and the associated media in the environment of GK-TAS.

* 1. Scenario 1- NAT profile 1

The system under test is UNI-Interface@GK\_TAS

NAT profile: 1 - NAT-Traversal according to the TAS-Proxy-Method (e.g. recognition of private addresses in contact, SDP);

IP-PBX is behind NAT in the range of private IP addresses.

TCP is used as a Transport Protocol.

VIA header field of the PBX’s REGISTER request contains a private IP address and fixed listening port;

CONTACT header field of the PBX’s REGISTER request contains a private IP address and fixed listening port;

* + 1. PBX initiates the session
       1. PBX initiates the session without using STUN (Outgoing call)

When using a TCP, SIP has an inherent mechanism that results in SIP responses reusing the connection that was created/used for the corresponding transactional request.

Call established

* + - 1. PBX initiates the session using STUN

Call establisshed

* + 1. Receiving session invitation (Incoming call)
       1. Receiving session invitation without using STUN (Incoming call)

Not established

* + - 1. Receiving session invitation using STUN (Incoming call)

Not established

* 1. Scenario 2- NAT profile 227

272 - NAT Traversal with translation of Source Port and Source IP Address is used on CPE

* + 1. PBX initiates the session (Outgoing call)
       1. PBX initiates the session without using STUN (Outgoing call)

This scenario is an example of how GK-Platform deal with Symmetric NAT. In general, traversing signaling is not a problem as traversing of media stream /SDP packets.

The outgoing request from PBX opens a pinhole in the NAT. Using TCP as a transport protocol keep-alive mechanism is provided to keep NAT bindings alive. The GK-Edge (SIP Proxy) would normally respond to the port available in the SIP 'Via' header. The SIP Proxy honors the 'rport' parameter in the SIP 'Via' header and routes the response to the port from which it was sent. The exact functionality for this method of response traversal is called 'Symmetric Response'.

On receiving an incoming request to a SIP Address-Of-Record (AOR), a GK-Edge (proxy/registrar) routes to the associated flow created by the registration and thus a route through NATs. The initial

The problem is to establish RTP media stream. SDP-body always includes the private IP address and initial port number. Knowing that NAT operates on 3th layer of TCP/IP Model and the changes of the IP address are only made in IP header, the data – where SDP is to be carried, shell be unchanged. That means GK-VGW shell send the data only to the IP address and port known from SDP-body header field.

The result of this scenario is that call

call established without voice

* + - 1. PBX initiates the session using STUN (Outgoing call)

d This is achieved by multiplexing a ping-pong mechanism over the SIP signaling connection (STUN for UDP and CRLF/operating system keepalive for reliable transports like TCP).

call established with voice succesfully

* + 1. Receiving session invitation
       1. Receiving session invitation without using STUN (Incoming call)

call established without voice

* + - 1. Receiving session invitation using STUN (Incoming call)

call established with voice succesfully

* 1. Scenario 3 –NAT Profile 554

544 - NAT Traversal with IP Address and Port translation of initially used source address.

* + 1. PBX initiates the session
       1. PBX initiates the session without using STUN (Outgoing call)
       2. PBX initiates the session using STUN
    2. Receiving session invitation
       1. Receiving session invitation without using STUN (Incoming call)
       2. Receiving session invitation using STUN (Incoming call)

1. NAT Traversal Principles

The following section describes what the platform expects of IP PBXs behind NAT firewalls.

* 1. The platform ignores IP addresses and port numbers contained in SIP/SDP messages

This behavior avoids certain attack scenarios , allows the platform to deal with broken SIP implementations, and uncooperative NATs.

As NAT firewall behavior cannot reliably determined, the platform always assumes symmetric NAT.

User agents MUST use the same IP address for SIP signaling and RTP/RTCP.

User Agents MUST send at least three RTP packets or unauthenticated STUN connectivity checks per m-line towards the platform after receiving an SDP answer.

The initial answer send by a user agent must never contain a port number of zero or ‘sendonly’ attributes.

**Rationale**: The NAT or Firewall in the customers LAN will not allow incoming UDP packets from the WAN unless it has seen UDP in the reverse direction.

The platform will use the source port of the first RTP/UDP packet as destination port for RTP packets targeted at the user agent. As UDP packets may get lost, the user agent must send three packets.

Refer to informational RfC 7362 for details.

* 1. User Agents must support symmetric RTP, RTCP
  2. User Agents must refresh NAT bindings

When no RTP packets are sent or received, the user agent must refresh the NAT bindings. This should be done using unauthenticated STUN connectivity checks with the same source and destination IP address and port number an RTP packet for this stream would use.

* 1. The platform does not alter the Contact URL

For incoming requests, the request URL will be the URL the IP PBX sent in its REGISTER request Contact URL.

* 1. The platform does not alter IP addresses and port numbers in the topmost Via

The IP address and port number contained in the topmost Via header in a request sent from the IP PBX to the platform will not be altered in topmost Via header of the SIP response sent from the platform to the IP PBX .

* 1. SIP over TLS

The IP PBX MUST establish a TLS session to the platform. The platform will use this session for all SIP messages towards the IP PBX. TCP Keepalives are the preferred method to refresh the NAT binding.

* 1. SIP over TCP

See 1.6

* 1. SIP over UDP

The platform may add a ‘received’ parameter to the topmost Via header. If the IP PBX sends a request with an rport parameter in its topmost Via header, the platform will fill out the rport parameter in the corresponding SIP response.