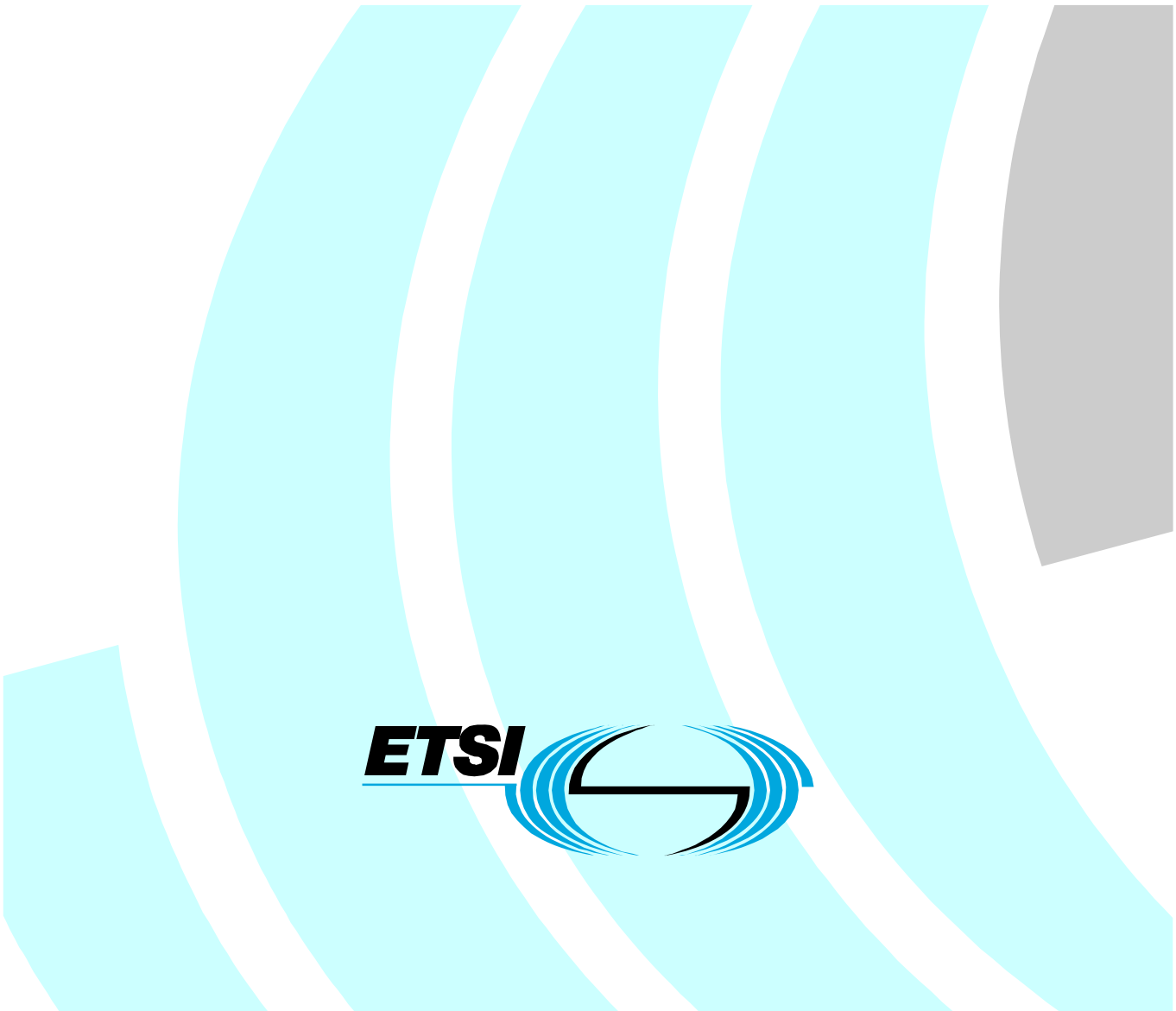
ETSI TR 187 008 V1.1.1 (2008-03)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report



Reference
DTR/TISPAN-07022-NGN

Keywords
report, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 4
Foreword 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8
4 NAT and firewall traversal considerations 8
4.1 Rationale for NAT Traversal study in the NGN 8
4.2 NAT Background 10
4.3 Types of NAT/Firewall Devices 10
4.3.1 NAT types 10
4.3.2 Filtering Behaviour 11
5 Reference architecture for NGN R2 12
6 Requirements and objectives for NGN R2 NAT-T 14
6.1 Objectives for NAT-T in NGN-R2 14
6.2 Requirements for use of NAT-T in NGN-R2 14
7 Existing NAT traversal methods documented in TISPAN R1 and 3GPP specifications 15
7.1 IMS-ALG in TISPAN R1 15
7.1.1 IMS-ALG with signalling not encrypted 15
7.1.2 IMS-ALG with encrypted signalling 16
7.2 ICE and outbound in TS 123 228 17
8 Feasibility, applicability, limitations of existing NAT traversal methods documented in TISPAN R1 and 3GPP specifications 18
8.1 Open issues with the NGN R1 approach for NAT traversal 18
8.1.1 Unidirectional RTP traffic 18
8.1.2 TCP connections initiated externally 19
8.1.3 Signalling traffic 19
8.1.4 Non IMS applications 19
8.1.5 Convergence with other standards 19
8.2 IPSec in presence of NAT 20
8.3 IMS ALG 20
8.3.1 Feasibility 20
8.3.2 Applicability 21
8.3.3 Limitations 21
8.4 ICE for media 22
8.4.1 Feasibility 22
8.4.2 Applicability 22
8.4.3 Limitations 23
8.5 Outbound for signalling 23
8.5.1 Feasibility 23
8.5.2 Applicability 24
8.6 UE ALG 25
9 Solutions for NAT traversal in NGN R2 25
9.1 NAT traversal for signalling 25
9.2 NAT traversal for media 26
Annex A: TVRA Summary for the NAT-T methods recommended in the present document 27
History 28

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document gives the results of a NAT traversal feasibility study for the NGN in TISPAN.

The term NAT Traversal is used to describe the problem of establishing connections between hosts where the IP address and port of the host is modified by a Network Address Translation (NAT) entity placed at some addressing boundary in the NGN. The term NAT in the present document refers to Network Address Port Translation (NAPT) in addition to NAT, where NAPT devices translate port numbers in addition to IP addresses. The study also considers the impact where the NAT device exhibits characteristics associated with firewalls. The document describes:

- Requirements for NGN R2 and open issues with the NGN R1 approach for NAT traversal.
- Reference architecture for NGN R2.
- Existing NAT traversal methods.
- Feasibility/applicability/limitations of those methods to solve the identified issues for NGN applications/services in an NGN environment; analysis of the potential impacts to other TISPAN documents.
- Scenarios for NAT traversal in NGN R2 (residential networks).
- The security problems associated with NAT and NAT Traversal.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

Not applicable.

2.2 Informative references

[1] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

[2] ETSI TS 102 558: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Requirements Catalogue".

[3] ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)".

[4] ETSI TS 183 017: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol Specification".

[5] ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN CNG Architecture and Interfaces and Reference Points".

[6] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements - Release 2".

[7] ETSI TS 123 228 "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[8] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[9] ETSI TS 124 229 "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[10] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".

[11] IETF RFC 1122: "Requirements for Internet Hosts - Communication Layers".

[12] IETF RFC 1631: "The IP Network Address Translator (NAT)".

[13] IETF RFC 1918: "Address Allocation for Private Internets".

[14] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".

[15] IETF RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[16] IETF RFC 3327: "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts".

[17] IETF RFC 3489: "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)".

[18] IETF RFC 3550: "RTP: A Transport Protocol for Real-Time Applications".

[19] IETF RFC 3605: "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".

[20] IETF RFC 3715: "IPSec-Network Address Translation (NAT) Compatibility Requirements".

[21] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[22] IETF RFC 4302: "IP Authentication Header".

[23] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[24] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[25] IETF RFC 4787: "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP".

[26] Draft-ietf-behave-rfc3489bis-13: "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", November 2007.

[27] Draft-ietf-mmusic-ice-19: "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", October 29, 2007.

[28] Draft-ietf-behave-turn-05: "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)", November 15, 2007.

[29] Draft-ietf-sip-outbound-11: "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)", November 10, 2007.

[30] Draft-ietf-sip-gruu-15: "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", October 11, 2007.

[31] Draft-ietf-avt-rtp-no-op-04: "A No-Op Payload Format for RTP", May 21, 2007.

[32] Draft-ietf-behave-nat-behavior-discovery-02: "NAT Behavior Discovery Using STUN", November 17 2007.

[33] IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".

[34] IETF RFC 3261: "SIP: Session Initiation Protocol".

[35] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis - Release 2".

[36] IETF RFC 4961: "Symmetric RTP / RTP Control Protocol (RTCP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Network Address Translation (NAT): method by which IP addresses are mapped from one realm to another in order to provide transparent routing to hosts

NOTE: NAT devices are used to connect address domains with private (unregistered) addresses to public domains with globally unique (registered) addresses.

NAT Traversal (NAT-T): method to establish connections between hosts in IP networks which use NAT devices (either locally or remotely) to modify their local IP address

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Application Function
AH	Authentication Header
ALG	Application Level Gateway
AVP	Attribute-Value Pair
BGF	Border Gateway Function
ESP	Encrypted Secure Payload
FQDN	Fully Qualified Domain Name
ICE	Interactive Connectivity Establishment
IKE	Internet Key Exchange
IMS	IP Multimedia System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IVR	Interactive Voice Response
NAPT	Network Address Port Translation
NAT	Network Address Translation
NAT-T	Network Address Translation Traversal
NGN	Next Generation Network
P-CSCF	Proxy Call Session Control Function
PSTN	Public Switched Telephone Network
RACS	Resource Admission Control Subsystem
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SDI	Session Description Information
SDP	Session Description Protocol
SPDF	Service-based Policy Decision Function
SIP	Session Initiation Protocol
STUN	Simple Traversal of UDP through NAT
TCP	Transport Control Protocol
TE	Terminal Equipment
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	User Equipment
VAD	Voice Activity Detection

4 NAT and firewall traversal considerations

4.1 Rationale for NAT Traversal study in the NGN

The model of IP assumes a single global address space where every host is reachable from all other hosts, in other words there is only one address space and it is public. In many implementations however a single address in the global address space is shared by multiple hosts, thus presenting both public and private IP address spaces. In order to ensure the reachability of the hosts in the private address domain from hosts in the global address domain a border device providing Network Address Translation (NAT) is used to map public to private addresses. However many protocols work on the assumption that the host address is globally unique and publish such addresses. Figure 1 illustrates the problem space by showing the restricted scope of the IP address with respect to the scope of the application name.

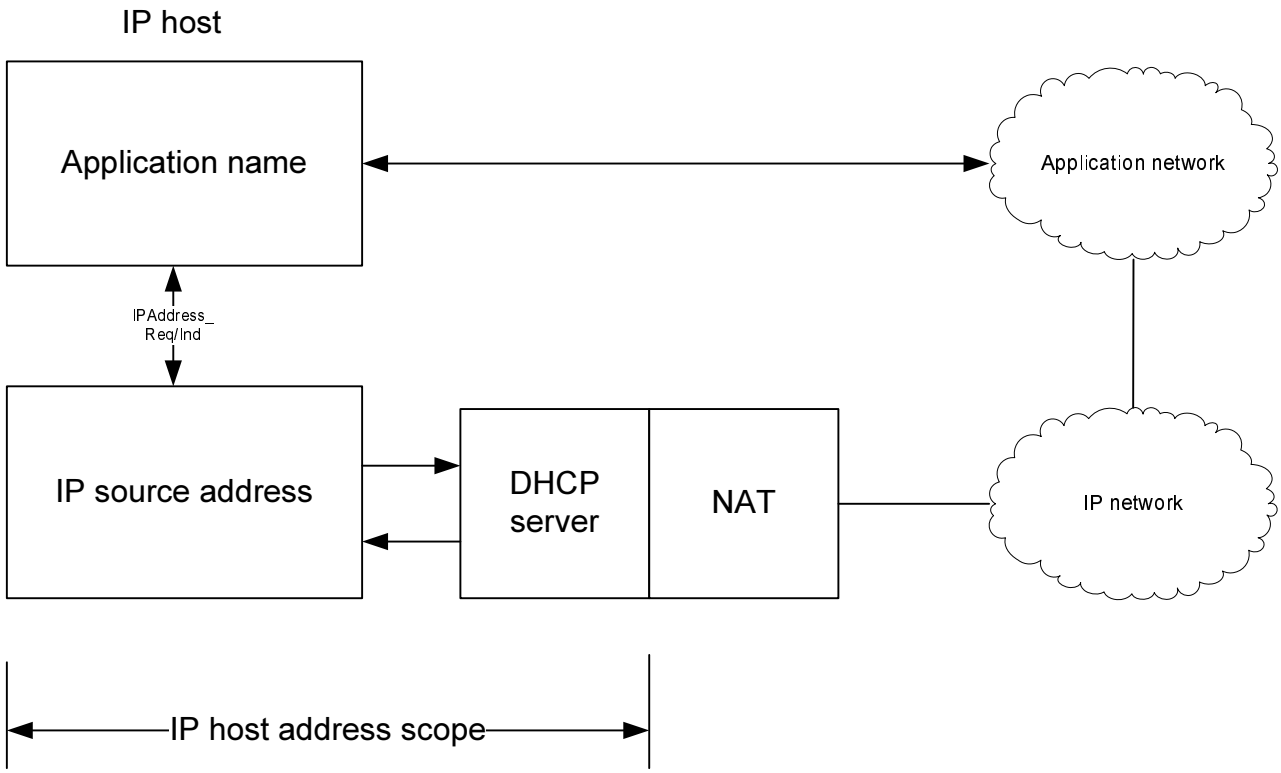


Figure 1: NAT Traversal problem

When an application uses the Host IP Address in establishing a session with an application network outside the scope of host's IP address then any use of that IP address by the application network is invalid.

NAT traversal is a term used to describe the problem of establishing connections between hosts in private IP networks which use NAT devices (either locally or remotely) to mask their local IP address (i.e. the IP address assigned in the private IP network) whilst giving themselves global connectivity by sharing the public IP address of the gateway to the global IP network.

The techniques used to solve the NAT Traversal problem are of three main types:

- NAT traversal protocols and techniques based on NAT behaviour

NOTE: NAT behaviour is not fully specified so such protocols and techniques are not universally applicable.

EXAMPLE 1: STUN and STUN usages (ICE, Outbound); STUN; TURN.

- NAT traversal based on NAT control

EXAMPLE 2: MIDCOM; ALG.

- NAT traversal combining several techniques

EXAMPLE 3: ICE.

The result of NAT Traversal is that the source-address presented by an application protocol (e.g. SIP) is valid in the application domain for the presented name without requiring that the application name be a Fully Qualified Domain Name (FQDN) and without relying on resolution protocols to determine the address associated with a name.

4.2 NAT Background

Network Address Translators (NATs) translate addresses between one IP addressing "realm" and another. This mapping is most commonly done between a private address space using addresses set aside for that purpose described in RFC 1918 [13] and a public address space. This mapping is commonly referred to as a NAT binding as the NAT has bound together the tuple of PrivateIPAddress:Port to the tuple of PublicIPAddress:Port to allow the subsequent response packets from the external endpoint to be forwarded to the proper internal host. The term NAT in the present document also refers to Network Address Port Translation (NAPT) devices which also translate port addresses in order to reduce the number of public addresses used on the public address side of the NAT.

In addition to address translation, NAT devices also exhibit firewall characteristics. In other words, they block traffic coming across the NAT (from "outside" to "inside" the NAT/Firewall device) based on certain filtering rules.

4.3 Types of NAT/Firewall Devices

Functionally NAT includes the following operations:

- Address binding.
- Address lookup and translation.
- Address unbinding.

In addition the NAT device must modify the IP header by recalculation of checksums and the means to do this are described in clause 3.3 of RFC 1631 [12].

4.3.1 NAT types

The terms "Full Cone", "Restricted Cone", "Port Restricted Cone" and "Symmetric" are used in RFC 3489 [17] to describe the behavior of different types of NATs for UDP.

Full Cone: A full cone NAT is one where 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.

Restricted Cone: A restricted cone NAT is one where 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.

Port Restricted Cone: A port restricted cone NAT is like a 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.

Symmetric: A symmetric NAT is one where 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.

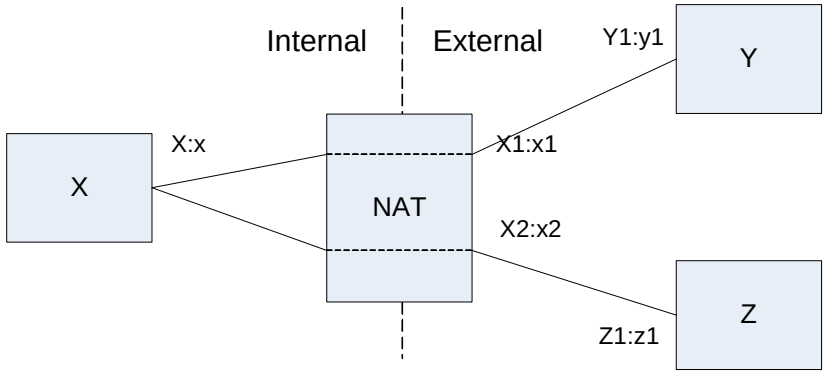
However, this terminology has resulted in some confusion since it combines both address mapping (NAT) behavior and security (firewall) behavior within a single definition. The present document uses the definitions from RFC 4787 [25] and from the Internet Draft NAT Behavior Discovery Using STUN [32].

Endpoint Independent Mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port.

Address Dependent Mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address, regardless of the external port. If the packets are sent to a different external IP address, the mapping will be different.

Address and Port Dependent Mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external address and port. If packets are sent to a different IP address and/or port, then a different mapping will be used.

This address mapping behavior is described in table 1 with respect to the configuration given in figure 2.



X = Host X
X.x = Internal Address:Port tuple of host X
Xn:xn = External Address:port tuple presented by NAT for host X
Y, Z = Hosts that host X is communicating with
Yn:yn = Address:port tuple visible to the NAT for host Y
Zn:zn = Address:port tuple visible to the NAT for host Z

Figure 2: Types of NATs (Address Mapping)

In figure 2, address X:x inside the NAT is translated to address X1:x1 when communicating with host Y outside the NAT. The same address X:x translates to X2:x2 when communicating with Y2:y2.

Table 1: Types of NATs (Address Mapping)

Type of NAT	Mapping Description
Endpoint Independent Mapping	X1:x1 always equals X2:x2
Address Dependent mapping	X1:x1 equals X2:x2 only if Y1 equals Z1
Address and Port Dependent Mapping	X1:x1 equals X2:x2 only if Y1:y1 equals Z1:z1
NOTE: For small NATs (e.g. residential NATs), a single public IP address is normally assigned as the external IP address (i.e., X1 = X2). However, larger NATs will assign the external IP address from a pool of available IP addresses.	

4.3.2 Filtering Behaviour

Filtering behavior in RFC 4787 [25] is described in terms of similar categories to those used in defining NAT behavior described in clause 4.3.1.

Endpoint Independent Filtering:

sending packets from the internal side of the NAT to any external IP address is sufficient to allow any packets back to the internal endpoint.

Address Dependent Filtering:

in order to receive packets from a specific external endpoint, it is necessary for the internal endpoint to send packets first to that specific external endpoint's IP address.

Address and Port Dependent Filtering:

receiving packets from a specific external endpoint, it is necessary for the internal endpoint to send packets first to that external endpoint's IP address and port.

Table 2 describes this filtering behavior in terms of the examples shown in figure 1.

Table 2: Types of Filtering Behavior

Type of NAT	Filtering Example
Endpoint Independent Filtering	Packets sent from X:x to Y1:y1 will enable packets from Y1:y1 or Y2:y2 to be received.
Address Dependent Filtering	Packets sent from X:x to Y1:y1 will enable packets to be received from Y1:z for any port z but will not allow packets to be received from any other IP address.
Address and Port Dependent Filtering	Packets sent from X:x to Y1:y1 will only allow packets to be sent from Y1:y1 to X:x.

5 Reference architecture for NGN R2

In the NGN there is no exclusive home for the NAT and NAT-T services. NAT-T services exist in a number of forms within the NGN standards suite from both TISPAN and 3GPP. Instances of NGN NAT-T services are found with IMS-ALG combined with RACS [1], and the use of STUN usages ICE and SIP-Outbound in 3GPP's IMS [7].

NOTE 1: The STUN usages in 3GPP are intended for specific application technologies and have not been defined for general use.

A NAT service, and the associated NAT-T service, is provided within RACS as defined in ES 282 003 [1]. In particular between the AF and SPDF using the DIAMETER protocol NAT-T is controlled by means of the Attribute Value Pairs (AVP) indicated in TS 183 017 [4] and copied here for convenience.

QUOTE: Based on local configuration data, the AF determines that address translation needs to occur on the user plane (e.g. a BGF on the media path performs NAPT, IP version interworking or hosted NAPT procedures), upon receipt of Session Description Information (SDI) pointing towards the endpoint served by the AF (e.g. for IMS, in case the P-CSCF receives an SDP offer sent by the served UE), the AF shall include the Binding-Information AVP with the Input-List AVP … If required (e.g. the received SDI is sent by a served endpoint with hosted-NAPT configuration), the AF may also include the Latching-Indication AVP set to "LATCH".

There is no direct link between the BGF and the AF hence the requirement for NAT-T in RACS to be invoked from local configuration data. However the specific use of IMS-ALG, ICE or SIP-Outbound may provide a means to automate the provision of the local configuration data.

NOTE 2: The RACS scenario for control of NAT and NAT-T is based on presence of NATc in the C-BGF as shown in the reference architecture of figure 3.

The primary result of NAT-T methods is the receipt by the local UE of an address that is valid in the signalling and media plane. This is termed by STUN [26] as a "Reflexive Transport Address", i.e. the address seen by the STUN server and returned to the STUN client.

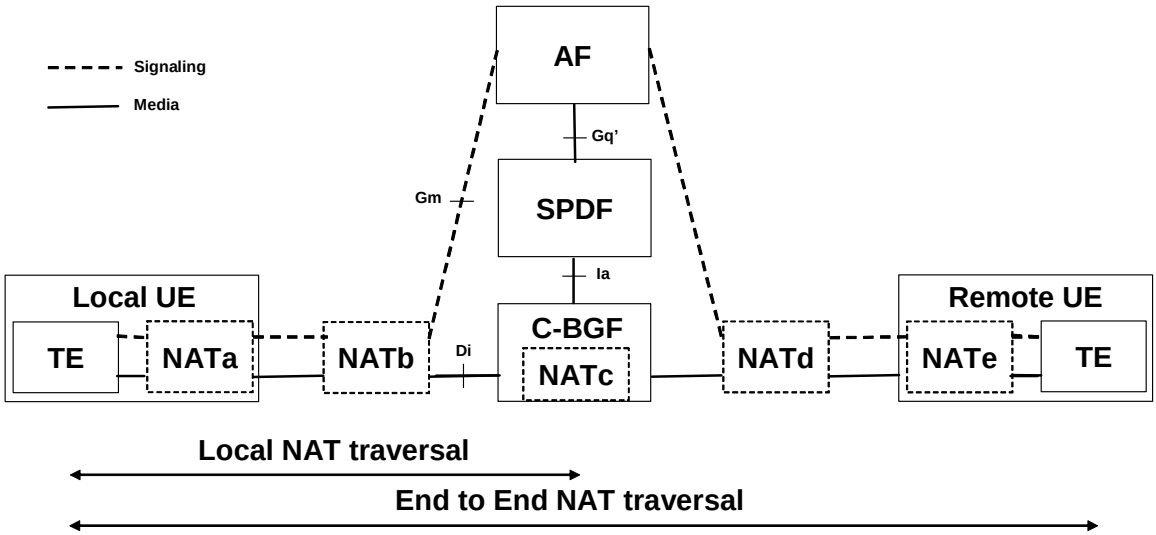


Figure 3: Reference architecture for NGN R2

The reference architecture is composed of the following functional entities:

- The local UE includes a TE and zero or more NAT referenced NATa. The local TE may be involved with NAT traversal. NAT in the UE may not be controlled by the TE.

NOTE 3: Each NAT in the UE may be associated to an ALG (not shown on figure 3), in which case it becomes invisible to the network.

- Zero or more Access Provider NAT referenced NATb, located between the local UE and the C-BGF involved in local NAT traversal. These NAT may not be in the same administrative domain as the AF, SPDF and C-BGF shown in the reference architecture and are not under the control of the AF. One example is a wholesale Access Network Provider which supports NAT to deploy an internal IP address plan.
  ES 282 003 [1], clause 5.2.3.3.1 describes the main C-BGF functions. It indicates in a note that static forwarding functions may be inserted in the IP path, and that the operators shall be the ones to decide on the presence of NAT in their respective networks.

- AF, SPDF and C-BGF involved in NAT traversal with the local TE. An additional NAT referenced NATc may be located in the C-BGF and act upon IP packets carrying media flows.

- Zero or more remote operator NAT referenced NATd, located between the C-BGF involved in local NAT traversal, and the remote UE. This includes NAT that may be included at network boundaries (in an I-BGF) and in the C-BGF serving the remote UE as well as any additional NAT that may be found in the remote access network. These NAT are not under the control of the AF serving the local UE but may be controlled by other network entities. For example, the NAT in the I-BGF is under the control of an IBCF, via an SPDF.

- The remote UE includes a TE and zero or more NAT referenced NATe.

NOTE 4: Local NAT traversal describes the functions in the IP CAN and/or the TE to traverse one or more local NATs in the UE and/or the Access Network. An example of local NAT traversal method is Hosted NAT defined in TISPAN R1 with NAT traversal functions hosted in P-CSCF and C-BGF.

NOTE 5: End-to-End NAT traversal describes the functions between the local and the remote TE to solve the NAT traversal issues which are not addressed by local NAT traversal (i.e. unidirectional media traffic).

NOTE 6: In the transit network, IBCF, SPDF and I-BGF provide a NAT function located between the C-BGF and the remote UE in the reference model. The I-BGF translates the IP transport addresses. The ALG in IBCF translates the IP addresses inside the SIP application level signalling messages, and should not require NAT traversal functions from other Functional Entities.

NOTE 7: In case of discrepancies between this clause and the RACS specification ES 282 003 [1] , the latter document takes precedence.

6 Requirements and objectives for NGN R2 NAT-T

6.1 Objectives for NAT-T in NGN-R2

The following security objectives apply to the NGN-R2 use of NAT Traversal:

- OBJ1: The application of NAT Traversal should not degrade the security (i.e. confidentiality, integrity, availability) of the NGN.
- OBJ2: The application of NAT Traversal should not restrict the communications capability of the NGN.
- OBJ3: The presence of NAT devices in the communications path should be detected.

6.2 Requirements for use of NAT-T in NGN-R2

The following list contains the general requirements for NAT Traversal:

- TISPAN NGN R2 NAT traversal shall support the traversal of the following type of NATs behaviour between the UE and the IMS Core Network:
  - Endpoint Independent Mapping.
  - Address Dependent Mapping.
  - Address and Port Dependent Mapping.
- TISPAN NGN R2 NAT traversal shall support the following type of filtering behavior between the UE and the IMS Core Network:
  - Endpoint Independent Filtering.
  - Address Independent Filtering.
  - Address and Port Dependent Filtering.
- TISPAN NGN R2 NAT traversal shall support both inbound and outbound requests to and from UEs through one or more NAT device(s).
- TISPAN NGN R2 NAT traversal shall support uni-directional and bi-directional RTP traffic.
- TISPAN NGN R2 NAT traversal shall support TCP connections initiated externally and internally.
- TISPAN NGN R2 NAT traversal shall support residential networks.
- TISPAN NGN R2 NAT traversal shall support IP v4.
- TISPAN NGN R2 NAT traversal shall support IP v6.
- TISPAN NGN R2 NAT traversal shall support unicast traffic.
- TISPAN NGN R2 NAT traversal should minimize the number of messages that are transmitted solely for NAT traversal.
- TISPAN NGN R2 NAT traversal shall support multiple UEs (on one or more devices) behind a single NAT.
- TISPAN NGN R2 NAT traversal should minimize additional session setup delay.
- TISPAN NGN R2 NAT traversal shall support the traversal for IMS.
- TISPAN NGN R2 NAT traversal shall support SIP signalling encrypted with IPsec.
- TISPAN NGN R2 NAT traversal shall take into account the scalability, complexity and compatibility with other relevant NGN requirements.

- Any solution recommended for NAT traversal shall not impact the inherent ability of TLS to operate across NAT.

The following NAT traversal requirements are For Further Study:

- TISPAN NGN R2 NAT traversal shall support corporate networks.
- TISPAN NGN R2 NAT traversal shall support multicast traffic.
- TISPAN NGN R2 NAT traversal shall support the traversal for non IMS applications including IP TV and PSTN/ISDN emulation.

7 Existing NAT traversal methods documented in TISPAN R1 and 3GPP specifications

NOTE 1: WLAN specification TS 133 234 [10] with IRAP is for Further Study.

NOTE 2: NAT traversal solutions for signalling and media in 3GPP are largely independent.

7.1 IMS-ALG in TISPAN R1

7.1.1 IMS-ALG with signalling not encrypted

NAT traversal for TISPAN R1 access when signalling is not encrypted is specified in ES 282 003[1] and follows the IMS-ALG and IMS Access Gateway model described in TS 123 228 [7], annex G.

This clause summarizes the reference model for the access and the high level functions in the different Functional Entities for the access and interconnection.

The reference model of TS 123 228 [7] is shown in figure 4.

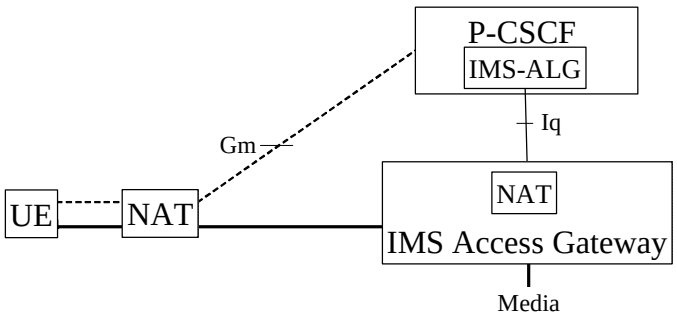


Figure 4: 3GPP Reference model for IMS ALG and IMS Access Gateway model

When applied to the TISPAN R1 architecture the C-BGF plays the role of the IMS Access Gateway. Moreover, the Iq reference point does not exist as a direct reference point: information flows between the P-CSCF and the NAT crosses the SPDF. See TS 182 006 [3] for more details.

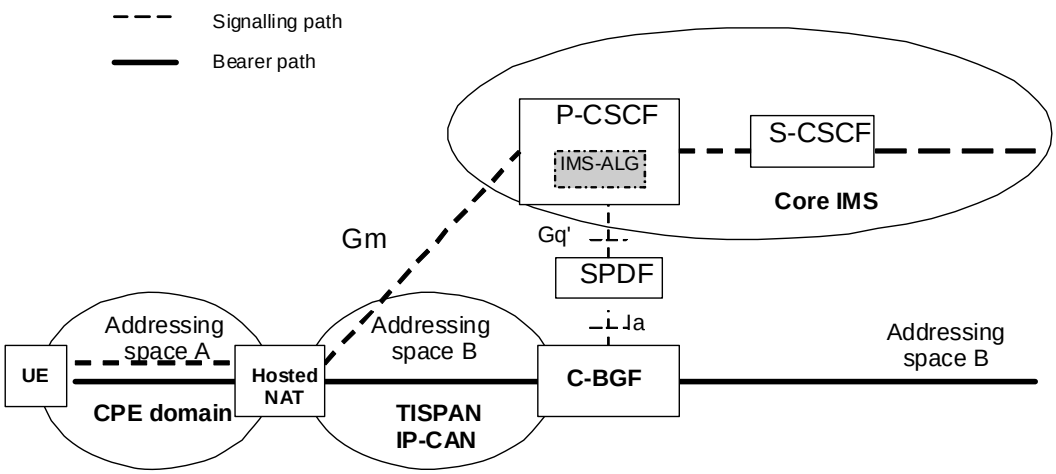


Figure 5: TISPAN Reference model for IMS ALG and IMS Access Gateway model

Functions of the UE

No UE NAT traversal functions are required.

Functions of the P-CSCF

1) Recognize that the UE is behind a NAT.

2) Request the IMS Access Gateway/C-BGF to initiate media latching, in order to retrieve the remote source address of the media received from the UE.

3) Control the IMS Access Gateway/C-BGF with an ALG to request transport addresses for each media flow, as described in TS 124 229 [9], annex F. The interactions between the ALG function in the P-CSCF and the NAT in the C-BGF are performed via the SPDF.

4) Modify the SDP with the addresses allocated by the IMS Access Gateway/C-BGF.

NOTE: There is no method currently defined to keep the UE NAT binding and firewall pinhole open.

Functions of the C-BGF

The C-BGF allocates and releases transport addresses according to the request coming from the IMS_ALG function of the P-CSCF. It ensures proper forwarding/binding of media packets coming from or going to the UE.

Address latching determines the address on which the C-BGF listens for media on the local IP address/port the C-BGF has reserved for the remote UE as requested from SPDF. When media is received the C-BGF stores the IP address/port value from where the media was received (IP address/port of the entity providing the NAT functionality), and uses that information when forwarding media towards the UE. The NAT providing entity then forwards the media to the actual IP address/port of the UE.

7.1.2 IMS-ALG with encrypted signalling

A procedure to enable NAT traversal for signalling messages encrypted with IPsec is specified in TS 133 203 [8], annex M.

The IPsec Security Association between the UE and the P-CSCF requires that the UE and the P-CSCF know the source and destination transport address information. Therefore the UE must know if it is located behind a UE NAT.

If the UE in not located behind a NAT, the IPsec transport mode shall be applied. It minimizes the length of the header. If the UE is located behind a NAT, the IPsec encapsulation tunnel mode shall be applied.

The method selected by TS 133 203 [8] to determine if the UE is located behind a NAT, is integrated inside the SIP registration procedure. The first Register message and the corresponding response are unprotected to setup the security mode with the P-CSCF. When the P-CSCF receives the first Register message, if the source IP address of the IP packet header is different from the address contained in the top-most Via header, the P-CSCF concludes that the UE is located behind a NAT device. It indicates in the Register response 4XX Auth-Challenge that the UDP encapsulation tunnel mode will be selected for the next SIP signalling messages, and provides the public IP address and port number in the received and rport parameters of the via header.

The second register message is protected with IPsec encapsulation tunnel mode. The UE populates the contact and Via headers to contain the UE public IP address or FQDN, and the protected server port value bound to the security association.

The IPsec transport mode has a keep-alive mechanism which keeps the NAT binding and firewall pinhole open.

Address Latching and SDP rewriting by the P-CSCF (i.e. TS 124 229 [9], clause F.3) are identical to the non-encrypted case.

7.2 ICE and outbound in TS 123 228

ICE (Interactive Connectivity Establishment) [27] defines a method for media traversal of NAT devices using SDP offer/answer. It makes use of STUN [26], and allows the UEs to discover, create and verify mutual connectivity.

Outbound [29] defines a method for signalling traversal of NAT devices. Outbound defines a method for User Agents, registrars, and proxy servers that allow requests to be delivered on existing connections established by the User Agent. It also defines keep alive behaviors needed to keep NAT bindings open and detect that a flow between the User Agent and the proxy server or registrar fails. It defines a limited STUN server in the registrar or proxy server to enable the User Agent to know if is located behind a NAT and provide the public IP address and port number associated to the signalling traffic.

NAT traversal with ICE and outbound is specified in TS 123 228 [7], annex G, ICE and outbound model.

Outbound with signalling encryption is specified in TS 124 229 [9], annex K.

This clause summarizes the reference model and the high level functions in the different Functional Entities.

The reference model is shown in figure 6.

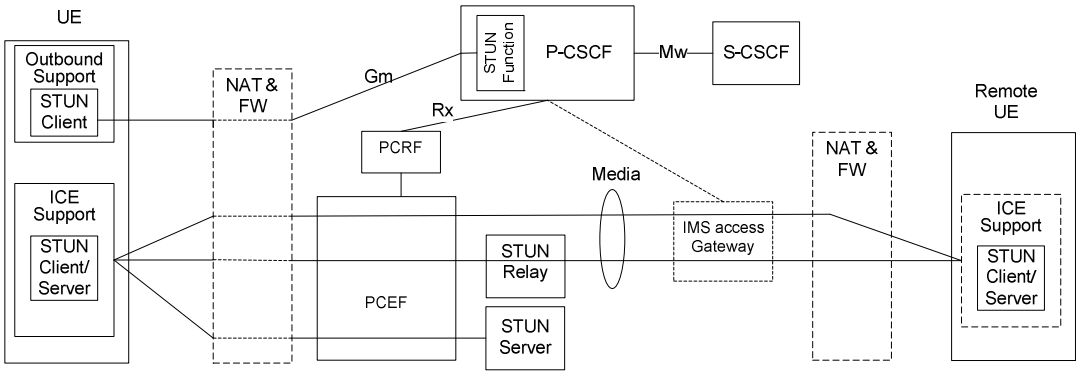


Figure 6: Reference model for ICE and Outbound

Functions of the UE

The UE is responsible for managing the overall NAT traversal process and for invoking the various protocol mechanisms to implement the NAT traversal approach. The following functions shall be performed by the UE:

- STUN relay server and STUN server discovery.
- Maintaining of NAT bindings for media to insure inbound media packets are allowed to traverse the NAT device, and for signalling through the use of a keep-alive mechanism to insure media and inbound signalling packets are allowed to traverse the NAT device.

- Gathering candidate addresses for media communications (locally assigned, server reflexive and relay).
- Advertising the candidate addresses in a special SDP attribute (a=candidate) along with the active transport address in the m/c lines of the SDP.
- Perform connectivity checks on the candidate addresses in order to select a suitable address for communications.

Functions of the UE NAT

There is no requirement in the UE NAT.

Functions of the STUN Relay Server

The STUN relay server and associated signalling requirements are documented in Internet Draft draft-behave-turn [28] and its use is detailed in Internet Draft draft-ietf-mmusic-ice [27]. No additional requirements are placed on this server.

Functions of the STUN Server

The STUN server and associated signalling requirements are documented in Internet Draft draft-ietf-behave-rfc3489bis [26] and its use is detailed in Internet Draft draft-ietf-mmusic-ice [27]. No additional requirements are placed on this server.

Functions of the P-CSCF

When supporting Outbound, the P-CSCF's primary role in NAT traversal is to ensure that requests and responses occur across a flow for which there is an existing NAT binding. The following functions shall be performed by the P-CSCF:

- Ensure that inbound dialog initiating requests can be forwarded to the UE on a flow for which there is an existing NAT binding.
- Ensure that all responses to the UE including those from mid-dialog requests are sent to the same source IP Address and Port which the request was received from.
- Implement a limited STUN server functionality to support the STUN keep-alive usage as defined in Internet Draft draft-ietf-sip-outbound [29] which is used by the UE to maintain the NAT bindings.
- Transmit signalling packets from the same port on which it expects to receive signalling packets.

Functions of the S-CSCF

When supporting Outbound, the S-CSCF shall be responsible for indicating to the UE that Outbound procedures are supported.

During registration the S-CSCF shall store all contact information provided by the UE to allow the S-CSCF to unambiguously determine which registration to update on re-Registration attempts.

8 Feasibility, applicability, limitations of existing NAT traversal methods documented in TISPAN R1 and 3GPP specifications

NOTE: NAT traversal for signalling and NAT traversal for media are considered separately. The solutions to address NAT traversal for signalling and NAT traversal for media do not influence each other.

8.1 Open issues with the NGN R1 approach for NAT traversal

8.1.1 Unidirectional RTP traffic

Where a NAT between the TE and C-BGF is deployed with Address and Port Dependent filtering the UE NAT blocks any return path RTP traffic.

A NAT between the TE and C-BGF with Address Dependent filtering will block the receiving RTP traffic if there is no other traffic between IP addresses used by the C-BGF and the UE.

The following applications generate unidirectional RTP traffic for a period of time.

- Early media defines a method where the Terminal Equipment receives unidirectional media before a particular session is accepted by the called user. Typical examples of early media generated by the called user are ringing tone and announcements from IVR and Call Centers. This function is available in the PSTN today.
- Push To Talk Service uses a half duplex type of communication.
- Compression algorithms with Voice Activity Detection stop sending RTP during period of inactive speech. Simple VAD schemes update the noise level periodically (e.g. 5 Hz to 30 Hz). More complex algorithms analyse the input signal and transmit only when a significant change in ambient noise character is detected, and may stop sending RTP during a larger period than the NAT binding timeout.
- The media stream can be "put on hold" using the SDP "sendonly" or "inactive" attributes as defined in RFC 3264 [15].
- Some RTP payload formats, such as the payload format for text conversation may send packets so infrequently that the interval exceeds the NAT binding timeout.
- At any time, applications with unidirectional RTP traffic may appear in the market. Streaming media is one example. It would be a very strong limitation if TISPAN could not deploy them.

8.1.2 TCP connections initiated externally

Some non IMS applications (i.e. gaming or peer-to-peer) initiate external TCP connections. For all such applications, a UE NAT with Address and Port Dependent filtering block the establishment of a TCP session. A UE NAT with Address Dependent filtering blocks the establishment of a TCP session if there is no other traffic between IP addresses used by the C-BGF and the UE.

Whereas a workaround for this exists in which the UE NAT accepts incoming TCP SYN to the external IP address, this approach violates the requirements for internet hosts defined in RFC 1122 [11] and as such is defined as a security risk that should not be propagated in the NGN.

8.1.3 Signalling traffic

The hosted NAT traversal method shall ensure that any NAT device timeouts associated with NAT binding and firewall pinholes do not expire. When there is no SIP session activity, the only signalling traffic which crosses the NAT device is the SIP registration.. There is no method defined to maintain the NAT binding and keep the firewall pinholes open when IPsec is not employed. A number of proprietary methods have been implemented but have not been analyzed from a security perspective.

8.1.4 Non IMS applications

Requirements for NAT-Traversal for non IMS applications have not been addressed by the TISPAN R1 document suite.

NOTE: The requirements for non IMS applications are for further study.

8.1.5 Convergence with other standards

TS 123 228 [7], annex G specifies several NAT traversal methods to support a wide variety of customer premise NATs that are not under the control of the network operator. This includes the method described in TISPAN R1 specifications as well as additional methods based on STUN and ICE.

8.2 IPSec in presence of NAT

The IPSec architecture is specified in RFC 4301 [21] and detail capabilities of IPSec are defined for each of AH in RFC 4302 [22], ESP in RFC 4303 [23], IKE in RFC 4306 [24] and the requirements in general are catalogued in TS 102 558 [2]. The presence of a NAT may make it difficult for the IPSec implementation to satisfy the requirements of IPSec. The problem of using IPSec in the presence of NATs is discussed in RFC 3715 [20] although it is noted that the specific problems introduced by the latest version of IPSec are not addressed by RFC 3715 (as RFC 3715 pre-dates RFC 4301).

RFC 3715 identifies 3 classes of incompatibilities between IPSec and NAT:

- Intrinsic problems arising from the NAT definition in RFC 3022 [14].
- Implementation weaknesses in NAT.
- NAT-T assistance.

A summary of the intrinsic problems in NAT are given below:

- AH address integrity check failure
  - AH incorporates the original IP source and destination addresses in the keyed message integrity check hence any NAT device that modifies the address fields invalidates the message integrity check. If the integrity check fails the receiving host shall discard the received packet (see RQ_002_2058 in TS 102 558 [2]).
- IKE address failure for SA identification.

NOTE: The use of IPsec in IMS as defined in TS 133 203 [8] uses a 3GPP profile of the IPsec suite, which does not use IKE. The security issues analysis is for further study.

8.3 IMS ALG

8.3.1 Feasibility

Figure 7 shows the IMS ALG reference model.

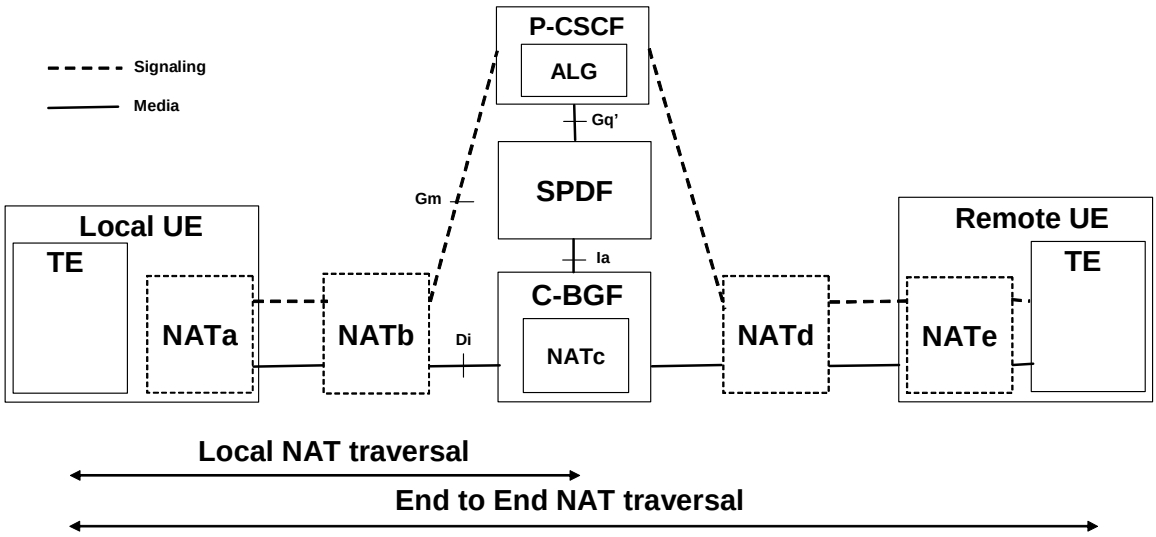


Figure 7: Reference model for IMS ALG

The P-CSCF handles the ALG function defined in TISPAN R1.

The C-BGF handles the NAT functions controlled by the P-CSCF ALG and the address latching function defined in TISPAN R1. Address latching corresponds to determining the address on which the C-BGF listens for media on the local IP address/port the C-BGF has reserved for the local UE as requested from SPDF. When media is received the C-BGF stores the IP address/port value from where the media was received (IP address/port of the entity providing the NATa or NATb functionality), and uses that information when forwarding media towards the UE. The NATa or NATb providing entity then forwards the media to the actual IP address/port of the TE.

8.3.2 Applicability

IMS ALG meets the following requirements for IMS applications:

- Support the traversal of the following type of NATs: Endpoint Independent Mapping, Port Independent Mapping, Address and Port Dependent Mapping, and the following type of filtering behaviour: Endpoint Independent Filtering, Port Independent Filtering, Address and Port Dependent Filtering, between the TE and the IMS Core Network.
- Support both inbound and outbound requests to and from TEs through one or more NAT device(s).
- Support bi-directional RTP traffic.
- Support TCP traffic initiated by the local TE.
- Support IP v4 and v6.
- Support unicast.
- Support multiple TEs (on one or more devices) behind a single NAT. IMS ALG does not have dependency on the number of TEs behind a single NAT.
- Support SIP signalling encrypted with IPsec.

8.3.3 Limitations

IMS ALG with address latching has the following limitations:

- There is no method to support uni-directional RTP traffic in TISPAN R1 when one or more local NAT do not support an ALG. To resolve this problem, the TE may send an empty (no payload) RTP packet with a payload type of 20 as a keepalive.

NOTE: This method complies with TS 124 229 [9], clause K.5.2.1 which states: "UEs that do not implement the ICE procedures as defined in draft-ietf-mmusic-ice [27] should implement the keepalive procedures defined in draft-ietf-mmusic-ice [27]. In the case where keepalives are required and the other end does not support ICE (such that STUN cannot be used for a keepalive), the UE shall send an empty (no payload) RTP packet with a payload type of 20 as a keepalive as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from table 5 of RFC 3551 [33] shall be used".

- The address latching function which is needed when one or more local NAT do not support an ALG requires that C-BGF receives an RTP packet from the local TE to set the NAT binding. The TE cannot received media RTP packets as long as it has not sent at least one RTP packet and creates a media cut-through delay. The transmission of empty RTP keep-alive packets by the TE at the beginning of the send or send/receive mode solves this problem.

- There is no method defined in TISPAN R1 to keep the NAT binding and firewall pinholes open for signalling traffic when IPsec is not employed.

EXAMPLE 1: Define a registration timer in the P-CSCF for the TEs behind a NAT or firewall. This timer must be smaller than twice the smallest local NAT binding and firewall timers. To minimize the number of SIP Register messages between the P-CSCF and the S-CSCF, the P-CSCF may forward the minimum number of SIP Register messages required by the S-CSCF registration timer.

EXAMPLE 2: Introduce a STUN keep-alive function from the TE to the SIP port of the P-CSCF. This complies with TS 123 228 [7], clause G.5.3.1 where it is stated: "The STUN keep-alive function, for SIP signalling, can also be implemented as a standalone function, without ICE and Outbound".

- IMS ALG does not support multicast. The requirements for multicast NAT traversal is for further study.
- The solution assumes symmetric RTP and RTCP as described in RFC 4961 [36].

8.4 ICE for media

8.4.1 Feasibility

Figure 8 shows the adaptation of 3GPP ICE to NGN R2 NAT reference model.

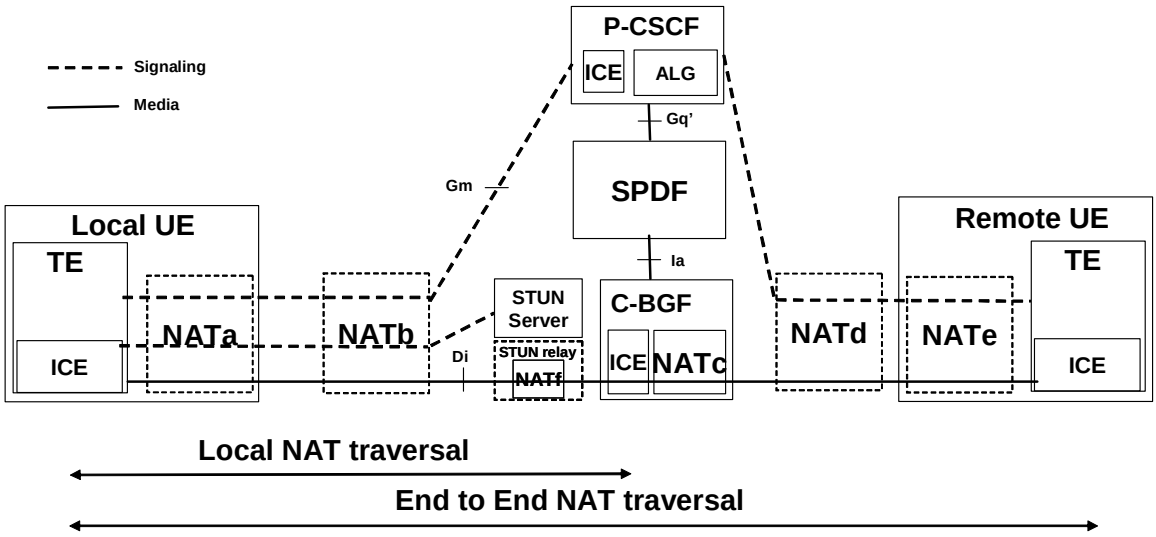


Figure 8: Reference model for ICE

The TE ICE function handles TE STUN client and Server functions, and allows the TE to discover, create, verify, and maintain media connectivity with the local C-BGF.

The P-CSCF handles the ALG function defined in TISPAN R1, and the control of ICE agent in C-BGF. The P-CSCF does not initiate the media latching procedures defined in TISPAN R1 and replaced by STUN and ICE.

The SPDF handles the adaptation of Gq' and Ia to support the H.248.50 package on NAT traversal.

The STUN Server handles the STUN Server functions documented in [1] and [2].

The STUN Relay handles the TURN functions documented in [28]. It includes a NAT function referenced NATf.

The C-BGF handles the NAT functions controlled by the P-CSCF ALG defined in TISPAN R1, and an ICE agent which replaces the address latching function inside C-BGF.

8.4.2 Applicability

ICE meets the following requirements for IMS applications:

- Support the traversal of the following type of NATs: Endpoint Independent Mapping, Port Independent Mapping, Address and Port Dependent Mapping, and the following type of filtering behaviour: Endpoint Independent Filtering, Port Independent Filtering, Address and Port Dependent Filtering, between the TE and the IMS Core Network.

- Support uni-directional and bi-directional RTP traffic: ICE establishes and maintain the media connectivity between the UE independently of RTP transmission. It enables to receive unidirectional RTP traffic for every application which generates unidirectional RTP traffic for a period of time (i.e. early media, push to talk, call on hold, etc.).

NOTE: Unidirectional traffic is not supported as such but converted to bidirectional traffic by generating ICE-specific traffic in the opposite direction.

- Support IP v4 and v6. ICE works with both IP v4 and v6.
- Support unicast.
- Support multiple TEs (on one or more devices) behind a single NAT. ICE does not have dependency on the number of TEs behind a single NAT.

8.4.3 Limitations

ICE has the following limitations:

- ICE does not apply end-to-end between the peer TEs in a TISPAN IMS configuration. The media connectivity is verified with a STUN Binding request and response exchanged between the ICE agents. In a TISPAN IMS residential configuration, the P-CSCF handles an ALG function. The P-CSCF modifies the default destination for media (contained in the m and c lines of SDP). In the case he C-BGF and P-CSCF do not handle an ICE function, the TE would detect an ICE mismatch, and ICE processing would abort.

NOTE: This limitation does not apply in a configuration where the AF does not handle an ALG function.

- The control of ICE agent inside C-BGF impacts P-CSCF, SPDF, Gq' and Ia reference points. The Ia reference point must support the H.248.50 package on NAT traversal under definition in ITU.
- A UE NAT with Address and Port Dependent mapping requires at least 2 NAT in the Access Network: the STUN Relay and the C-BGF NAT.
- ICE [27] only defines UDP. However, extensibility is provided to allow for future transport protocols to be used with ICE, such as TCP.
- ICE does not support multicast. The requirements for multicast NAT traversal should be refined.
- The NAT in the STUN relay and the NAT in the C-BGF provide redundant functionality.

8.5 Outbound for signalling

8.5.1 Feasibility

Figure 9 shows the adaptation of 3GPP Outbound to the NGN R2 NAT reference model.

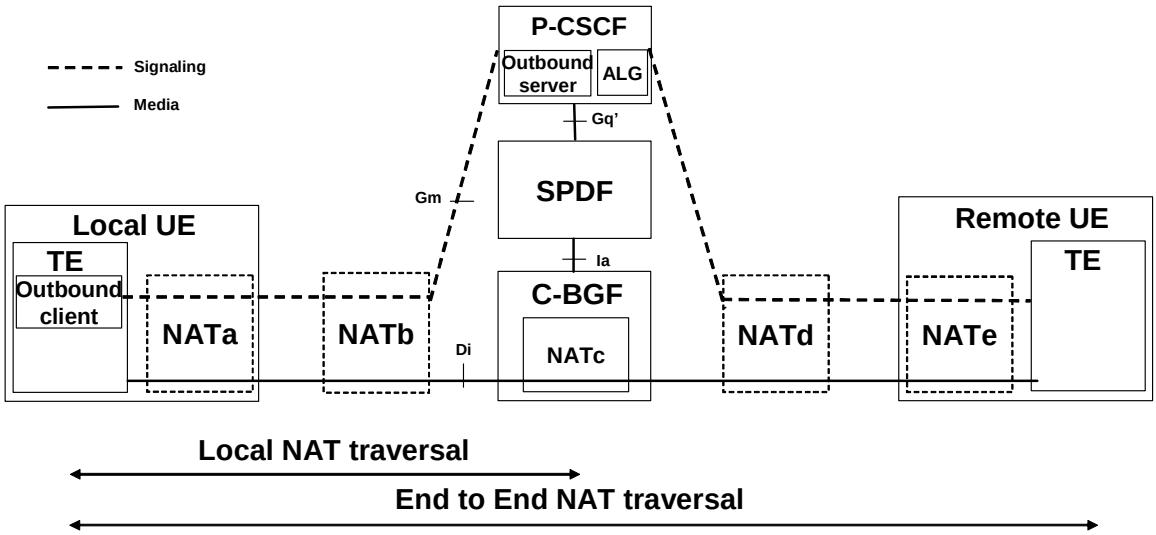


Figure 9: Reference model for Outbound

The TE Outbound client function handles the Outbound STUN client functions for signalling traversal of NAT devices.

The P-CSCF handles the Outbound STUN server functions for signalling traversal of NAT devices. It also handles the ALG function defined in TISPAN R1.

8.5.2 Applicability

Outbound meet the following requirements for IMS applications:

- Support the traversal of the following type of NATs: Endpoint Independent Mapping, Port Independent Mapping, Address and Port Dependent Mapping, and the following type of filtering behaviour: Endpoint Independent Filtering, Port Independent Filtering, Address and Port Dependent Filtering, between the TE and the IMS Core Network.
- Support both inbound and outbound requests to and from TEs through one or more NAT device(s).
- Support IP v4 and v6. Outbound works with both IP v4 and v6.
- Minimize SIP messages to maintain the NAT bindings. Outbound does not rely on SIP messages to maintain the NAT bindings.
- Support multiple TEs (on one or more devices) behind a single NAT. Outbound do not have dependency on the number of TEs behind a single NAT.
- Support SIP signalling encrypted with IPsec. Outbound uses the SIP Register method to know if the TE is located behind a NAT, and provides the public IP address and port number for SIP signalling received by P-CSCF.
- The support of Outbound adds reliability to the signalling connections established by the TE, specifically when the TE is connected to multiple hosts that provide registrar and proxy functionality for that domain. The benefits of Outbound should be evaluated for business trunking scenarios.

Outbound has the following limitations:

- Outbound requires that the transport used at Registration (UDP or TCP) must be used for all subsequent messages. When the UE has registered with UDP, the P-CSCF cannot send a large message to the UE requiring TCP as transport according to RFC 3261 [34]. It needs to be evaluated whether this limitation is significant in a TISPAN environment.

8.6 UE ALG

An Application Level Gateway (ALG) function associated to the NAT in the UE is one of the NAT traversal methods applicable without any impact on the NGN architecture. It is not explicitly described in TISPAN R1. In TISPAN R2, the Customer Gateway Architecture defined in TS 185 003 [5] identifies a SIP Proxy/B2BUA component which may act as an ALG.

The UE NAT translates the IP transport addresses between the internal and the external address realms, and the embedded ALG translates the IP addresses inside the application level signalling messages.

This method has the following limitations:

- It is not applicable when the signalling is encrypted by the TE since the ALG cannot inspect and change the application level signalling messages.
- This ALG requires an understanding of the application level signalling messages which need to be translated inside the UE. It may require an update of the ALG when the signalling protocol evolves.

9 Solutions for NAT traversal in NGN R2

The objective of this clause is to document NAT traversal solutions for residential access extending and complementing those defined in TISPAN R2.

Solutions for supporting NAT traversal in the following scenarios are for further study:

- RACS R2 wholesale with NAT provided by the Access Network operator.
- Business trunking.
- IPTV with dedicated subsystem and RTSP signalling.

9.1 NAT traversal for signalling

In addition to the procedures defined for TISPAN R1, the following methods may be introduced to keep the NAT binding and firewall pinholes open for signalling traffic when one or more NAT located between the TE and the P-CSCF is not associated to an ALG, when IPsec according to TS 133 203 [8], annex M is not employed:

- A registration timer shall be provisioned in the P-CSCF for the TEs behind a NAT or firewall. To minimize the number of SIP Register messages between the P-CSCF and the S-CSCF, the P-CSCF may forward the minimum number of SIP Register messages required by the S-CSCF registration timer. This method is controlled by the P-CSCF, and has the benefit to be transparent to the TE.
- Outbound keep alive mechanisms for NAT binding may be sent by the TE to the SIP port of the P-CSCF. This method is controlled by the TE. It may be complementary to the first one in case the P-CSCF does not provision the appropriate registration timer for the TE.

NOTE 1: Outbound defines three keepalive mechanisms for the NAT binding:

- CR/LF (exchange of carriage return/line feed messages).
- TCP keepalive messages.
- STUN messages.

NOTE 2: The time between keep alive messages should be smaller than the value of the NAT timeout for the transport protocol. For UDP, many NATs have a timeout as low as 30 seconds. Issues such as battery consumption might motivate longer NAT timeout values.

NOTE 3: The reason for selecting this method is that it resolves the identified issues with minimum changes to TISPAN R1 functions. Outbound adds reliability to the signalling connections established by the TE when the TE is connected to multiple hosts that provide registrar and proxy functionality for that domain. However, this configuration does not apply for IMS residential services.

9.2 NAT traversal for media

In addition to the procedures defined for TISPAN R1, the following methods are introduced to keep the NAT binding and firewall pinholes open with uni-directional RTP traffic when one or more NAT located between the TE and the C-BGF is not associated to an ALG:

- The TE may send keepalives for each media session. These keepalives may be sent regardless of whether the media session is currently inactive, sendonly, recvonly or sendrecv. The keepalive message may be an empty (no payload) RTP packet with a payload type of 20.

NOTE: The reason for selecting this method is that it resolves the identified issues with minimum changes to TISPAN R1 functions. The support of ICE in a TISPAN IMS residential configuration has major impacts in P-CSCF, SPDF, C-BGF, Gq', and Ia. It introduces a STUN Server, and a STUN Relay which adds a NAT on the media path when the UE NAT supports Address and Port Dependent mapping.

Annex A:
TVRA Summary for the NAT-T methods recommended in the present document

NOTE: The TVRA analysis is moved to WI 07030, TR 187 002, TISPAN NGN Security - Threat, Vulnerability and Risk Analysis - Release 2 [35].

History

Document history		
V1.1.1	March 2008	Publication