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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

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.

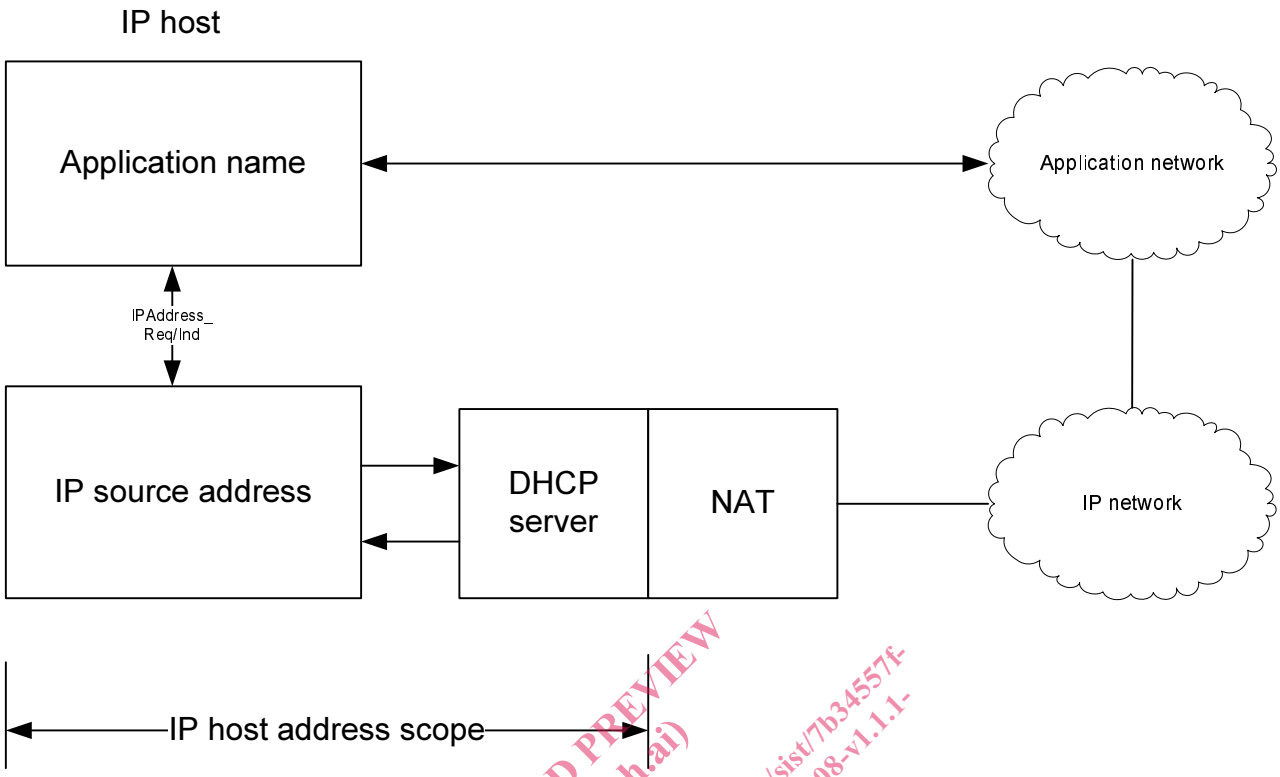

Figure 1: NAT Traversal problem

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.