# NAT Behavioral Requirements, as Defined by the IETF (RFC 4787) - Part 3. Deterministic Properties

**October 10, 2013 | By Netmanias (tech@netmanias.com)**

This is the last post on RFC 4787.

## 4. Application Level Gateway

For information about Application Level Gateways (ALGs), please click here.

**RFC 4787 Recommendation (REQ-10)**: To eliminate interference with UNSAF NAT traversal mechanisms and allow integrity protection of UDP communications, NAT ALGs for UDP-based protocols SHOULD be turned off

What does this recommendation mean? ALGs, if not fully supported, may only interfere with NAT Traversal. So turn it off!!

## 5. Deterministic Properties

■ **Non-Deterministic NAT**

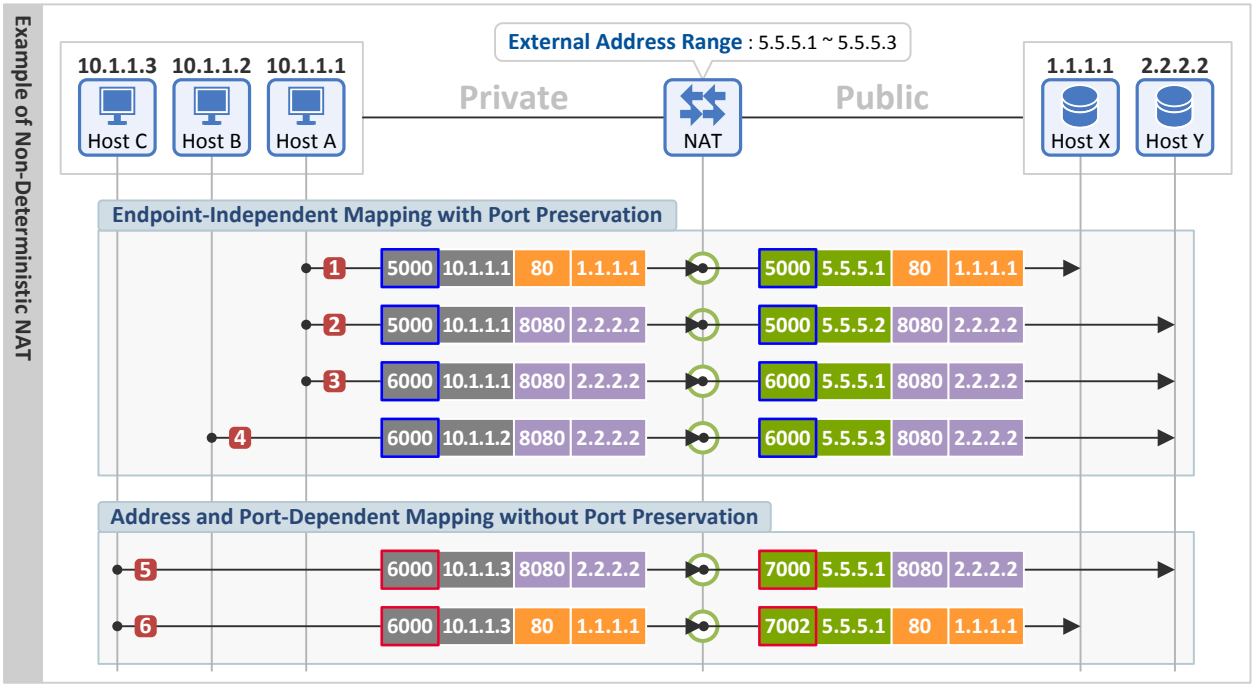
A NAT that changes its Mapping or Filtering Behavior in particular circumstances (see the example below) is called a "Non-Deterministic NAT". One example of these NATs presented in RFC 4787 is described below.

NATs usually implement "Endpoint-Independent Mapping with Port Preservation".
So, in the figure below, the NAT allocates the same External Port (5000) to both packets [1] and [2] that Host A is sending to Host X and Host Y (Endpoint-Independent Mapping). It also allocates 5000, the Internal Port number, to the External Port (Port Preservation).
Next, Host A and Host B send Host Y a packet ([3] and [4], respectively). At this time both packets use 6000 for their Internal Port number. Since the NAT has sufficient IP addresses available in its External Address Pool, it can stick with Port Preservation.

Later when Host C sends Host Y a packet [5] which has 6000 as its Internal Port number as Host B did, the NAT realizes that i) the Internal Port of 6000 has already been allocated to the previous packet destined to the same External Endpoint, and ii) there is no more external address available, and thus it cannot

stick with Port Preservation any more. So, it switches to "Address and Port-Dependent Mapping without Port Preservation".

Then the packet that Host C sends to Host Y (i.e. packet [5]) will inevitably have an External Port (7000) that is different from its Internal Port (6000). Thus, No Port Preservation here! Furthermore, it also becomes inevitable for the packet [6] that Host C sends to Host X to have an External Port (7002) that is different from the External Port (7000) of the packet [5] that Host C sent to Host Y (Address and Port-Dependent Mapping).




■ **Deterministic NAT**

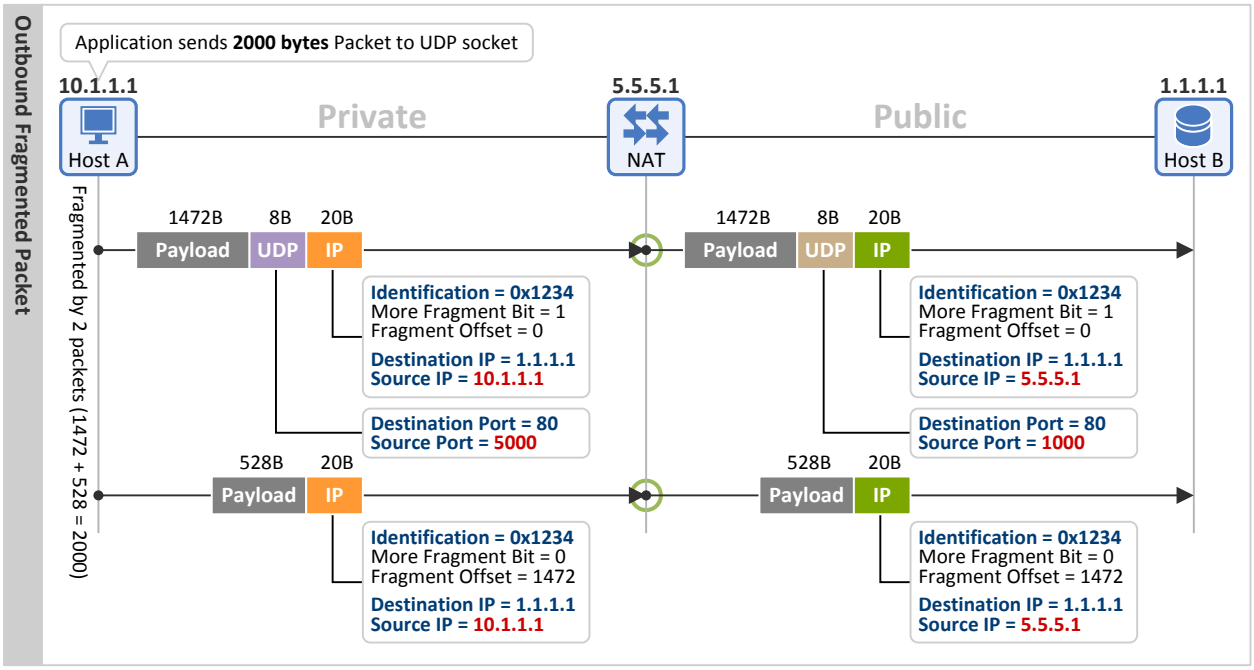
A NAT that never changes its Mapping or Filtering Behavior in any circumstances is called a "Deterministic NAT".

> **RFC 4787 Recommendation (REQ-11)**: A NAT MUST have deterministic behavior, i.e., it MUST NOT change the NAT translation or the Filtering Behavior at any point in time, or under any particular conditions

## 6. Fragmentation of Outgoing Packets

The maximum transmission size of an outbound packet sent by a TCP/UDP application in a host is limited based on the size of the specified IP Maximum Transmission Unit (MTU). In case the lower layer of IP (L2 layer) is Ethernet, the IP MTU is 1500 byte (except for Jumbo Frame). So, if, as in the figure below, a UDP application sends a 2,000-byte packet, the NAT fragments the packet into two smaller ones - the first one with both IP and UDP headers, and the second one with an IP header only.

For this reason, it is important at this time for the NAT to be able to identify fragmented packets by referring to MF (More Fragment) and Fragmentation Offset fields in the IP header of the packets. For the second packet with no UDP header, the NAT should be able to identify sessions by referring the Identification field (0x1234) of the IP header, and replace the Internal Address (10.1.1.1) with the External Address (5.5.5.1) for the packet. If the NAT can't do these, no communication will be allowed (Obviously, these seem too basic. The IETF didn't even bother to include them in its RFC 4787).




Packet fragmentation occurs not only in hosts (devices or servers), but also in generic routers and NATs (NATs can be considered as routers in that their packet delivery is also based on the destination IP address of packets.

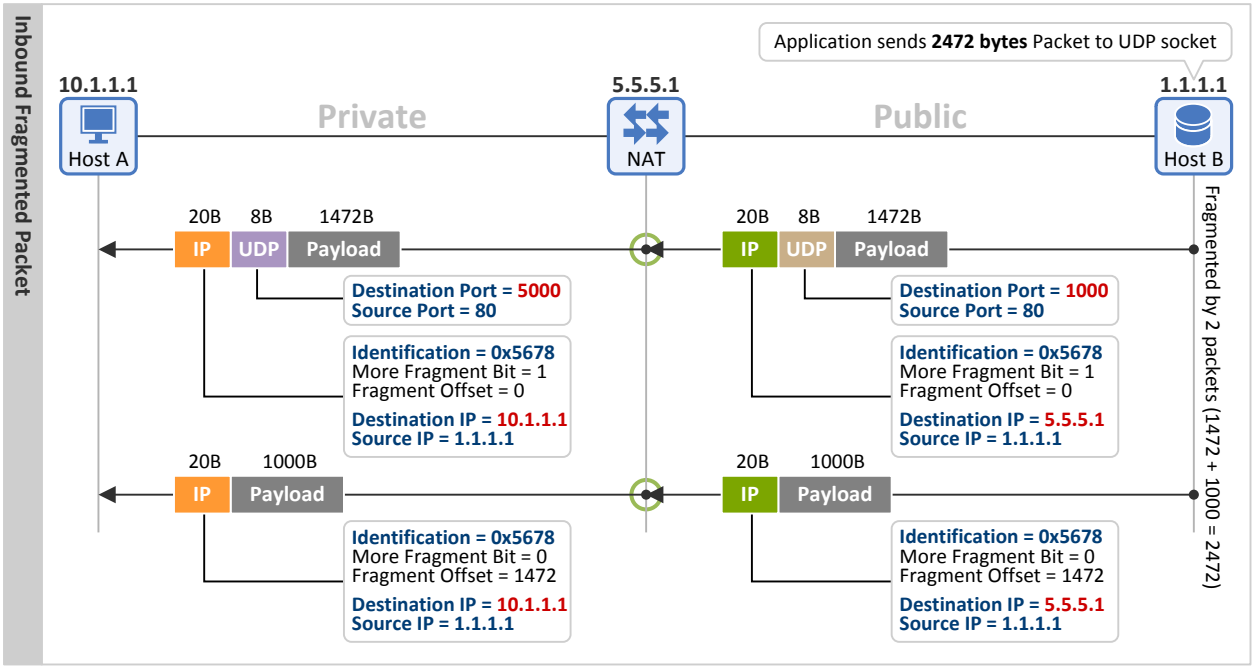
Today, almost all link layers are Ethernet, and besides the MTU size on a Wi-Fi network is 1,500 bytes (with Windows). Therefore, NATs rarely perform packet fragmentation in deed. However, RFC 4787 still recommends NATs send an ICMP message as follows in case needed:

> **RFC 4787 Recommendation (REQ-13)**: If the packet received on an internal IP address has DF=1, the NAT MUST send back an ICMP message "Fragmentation needed and DF set" to the host, as described in [RFC0792]
>
> a) If the packet has DF=0, the NAT MUST fragment the packet and SHOULD send the fragments in order

## 7. Receiving Fragmented Packets

Packet fragmentation is triggered not only by an Internal Endpoint as described above, but also by an External Host (e.g. Host B in the figure below). In case of external host-triggered fragmentation, the same

requirements in Section 6 must be met as well. For the fragmented packet with no UDP header, the NAT should be able to identify sessions by referring the Identification field of the IP header, and replace the received External Address with the Internal Address for the packet.




The following two types of NAT behavior are mentioned in RFC 4787 for such case:

■ **Received Fragments Ordered**

A NAT can translate the address/port of fragmented packets and forward them to Internal Endpoints only when the packets are received in an order that they are fragmented.

■ **Received Fragment Out of Order**

A NAT can translate the address/port of fragmented packets and forward them to Internal Endpoints even when the packets are not received in an order that they are fragmented (e.g. in case an External Endpoint sent packets in order of Fragment Packet 1, 2 and 3, but the NAT receives them in order of Fragment Packet 1, 3 and 2).

**RFC 4787 Recommendation (REQ-14)**: A NAT MUST support receiving in-order and out-of-order fragments, so it MUST have "Received Fragment Out of Order" behavior

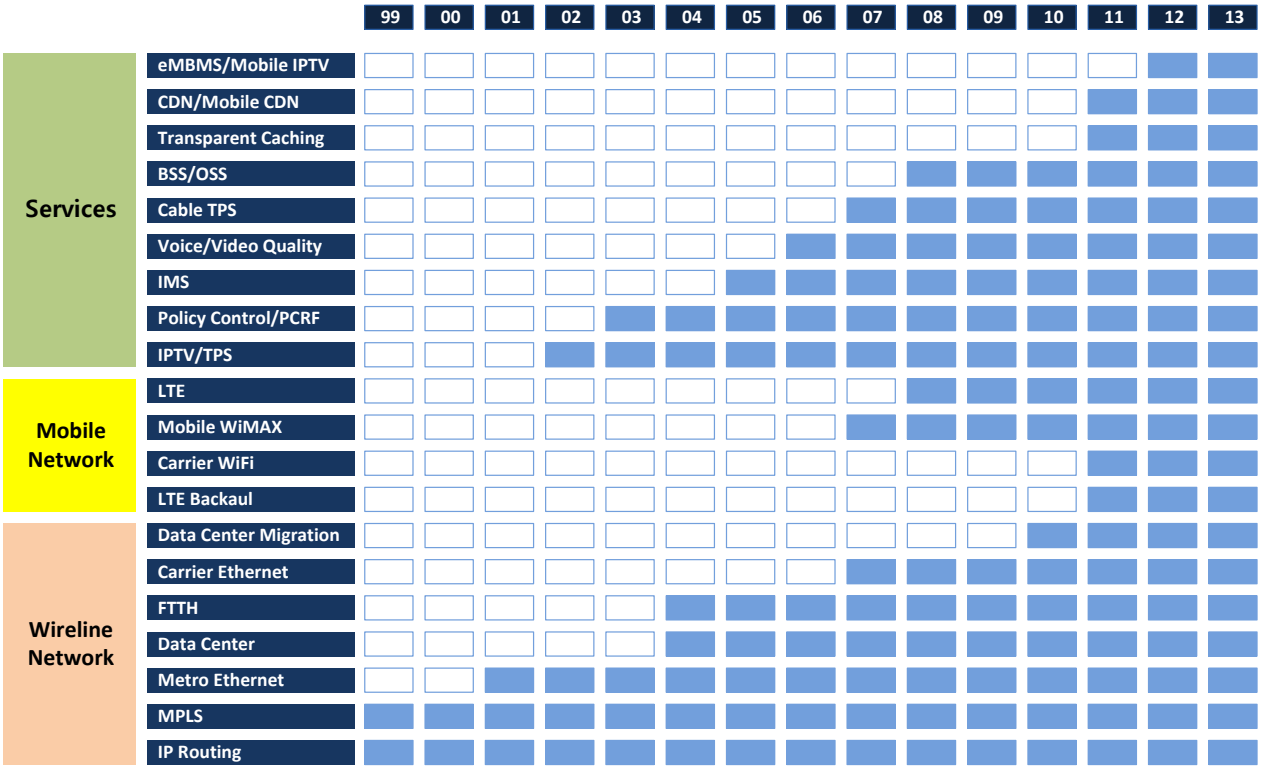
We have reviewed the "NAT Behavioral Requirements for Unicast UDP" as presented in RFC 4787 through three of our posts so far.

You don't get to read an RFC document THIS thoroughly very often. Anyway, after close examination of the document, you may agree with me in that:

i) it could have been much easier and simpler to establish standards for different types of NATs only if NAT behavior had been standardized by the IETF earlier, i.e. before NATs were actually introduced in the market.

ii) it is unfortunate that APs provided by telecom operators or in open markets are not compliant with the foregoing standards because the standards are originally designed for NAT traversal (i.e. for P2P applications of which packets must pass through a NAT). According to our test on APs from Cisco-Linksys, ipTIME and a telecom operator, all APs used Endpoint-Independent Mapping + Address and Port-Dependent Filtering Behavior.

## Netmanias Research and Consulting Scope

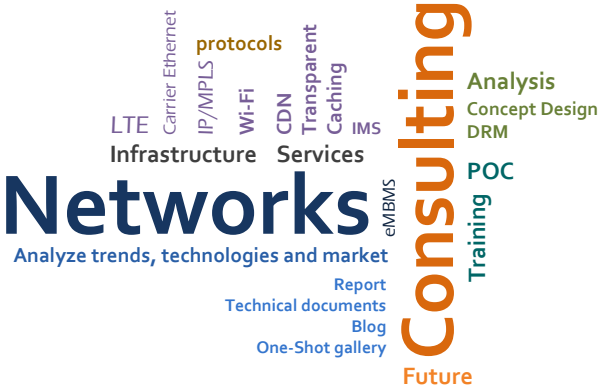



**Visit http://www.netmanias.com to view and download more technical documents.**

We design the future

We design the future

We design the future




**About NMC Consulting Group (www.netmanias.com)**

NMC Consulting Group is an advanced and professional network consulting company, specializing in IP network areas (e.g., FTTH, Metro Ethernet and IP/MPLS), service areas (e.g., IPTV, IMS and CDN), and wireless network areas (e.g., Mobile WiMAX, LTE and Wi-Fi) since 2002.