Network Address Translation (NAT) Overview (RFC 3022/2663)

September 3, 2013 | By Andrew Johnson and Chris Yoo (tech@netmanias.com)

Today, NATs are employed by Korean telecom operators in almost all of their access networks except for wired access networks (FTTH, Ethernet, DSL, etc.).

- 3G/LTE network: Large Scale NAT (LSN) installed beyond GGSN/P-GW in the 3G/LTE Core networks. Also called "Carrier Grade NAT (CGN)".
- Wi-Fi Hotspot network: NAT implemented in Wi-Fi Hotspot
- Residential network: NAT implemented in subscribers' APs provided by (leased from) telecom operators, or in APs purchased from open markets (e.g. D-Link's DIR)

All users, including 3G/LTE users, Wi-Fi Hotspot users and home AP users, are assigned a private IP address. Then later when they access the Internet, this address is converted into a public IP address through a NAT.

Using a NAT allows telecom operators to:
(1) save public IP addresses because the NAT converts the private IP addresses assigned to multiple devices into a public address. This allows the devices to use only one public IP address instead of their private IP addresses when accessing the Internet.
(2) prevent any external attack on mobile devices or mobile networks by introducing LSNs on the 3G/LTE network. Enterprises can also protect their internal network from external intrusion/attack by making their addresses private (similar to using firewalls).

Below, NAT-related terms defined in RFC 3022 (Traditional NAT) and RFC 2663 (IP NAT Terminology and Considerations) will be explained.

Terminology

1. TU Ports

Both TCP and UDP header have Source and Destination Port fields. And these ports are collectively called "TU Ports", or "Transport Identifiers". When a device (client) communicates with a server using TCP or UDP, a value from 0 to 1,023 (well-known ports defined by IANA) or from 1,024 to 49,191 (registered ports defined by IANA) is generally used as a value for a TU Destination Port, as set in RFC 1700. For example, HTTP's TCP Destination Port is 80. For a TU Source Port, however, each OS uses a value randomly selected from different ranges defined for each OS (approximately 30,000 ~ 60,000). This type of port is called an "ephemeral port" (see http://en.wikipedia.org/wiki/Ephemeral_port for more information).

2. Public/Global/External Network

Refers to a network which has globally unique IP addresses assigned by the Internet Assigned Numbers Authority (IANA). Therefore, this type of network can route (communicate) across telecom operators' networks around the world. It is commonly called a "public IP network".

3. Private/Local Network

Refers to a network which has IP addresses that are not assigned by IANA. This type of network cannot route through the Internet. It is commonly called a "private IP network".

IANA defines the following three IP blocks for this purpose:

- 10/8, 172.16/12, 192.168/16

4. Session

A session is defined as the set of traffic that is managed as a unit for translation. Each TCP/UDP session is identified by the values of a source IP address, source TU port, destination IP address and destination TU port.

5. Application Level Gateway (ALG)

Some applications have IP address and/or TU port information in their payload (application-specific data that follows TCP/UDP headers). For this reason, some NAT devices have Application Level Gateways (ALGs), which feature an agent that can translate the IP address and/or TU port information stored in payloads (Application awareness inside the NAT). In general, these NATs come with a list of applications supported (e.g. FTP, SIP, RTSP, etc.). Since it is practically impossible for a NAT to support ALGs for all the applications that are being released every day in the market, not many NATs seem to support ALGs.

What is NAT?

Network Address Translation (NAT) is the process of converting a private IP address into a public IP address, and vice versa, to allow a device on a private network to communicate with a public network (Internet).

Traditional NAT would allow hosts within a private network to transparently access hosts in theexternal network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts. (RFC 3022)

Traditionally, **NAT devices** are used to connect an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. (RFC 2663)

Types of NAT

There are two types of NAT defined in RFC 3022/2663: Basic NAT and Network Address Port Translation (NAPT). They both are collectively called "Traditional NAT" although NAPT, aimed at "saving IPv4 addresses", is the most common type of NAT these days. So, when we say NAT, we refer to NAPT in most cases. The NAPT-type operation is now supported by all APs.

Basic Network Address Translation or **Basic NAT** is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation, or **NAPT** is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports.
Together, **these two operations**, referred to as **traditional NAT**, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses. (RFC 3022)

Basic NAT

■ **Definition and Purpose**

Basic NAT is employed in enterprise networks for security purposes (like firewall). It provides a one-to-one translation of IP addresses. This means the same number of public IP addresses as the devices with a private IP address are needed to access the Internet.

> Nodes on private network could be enabled to communicate with external network by dynamically mapping the set of private addresses to a set of globally valid network addresses. (RFC 3022)

■ **Translation Rule**

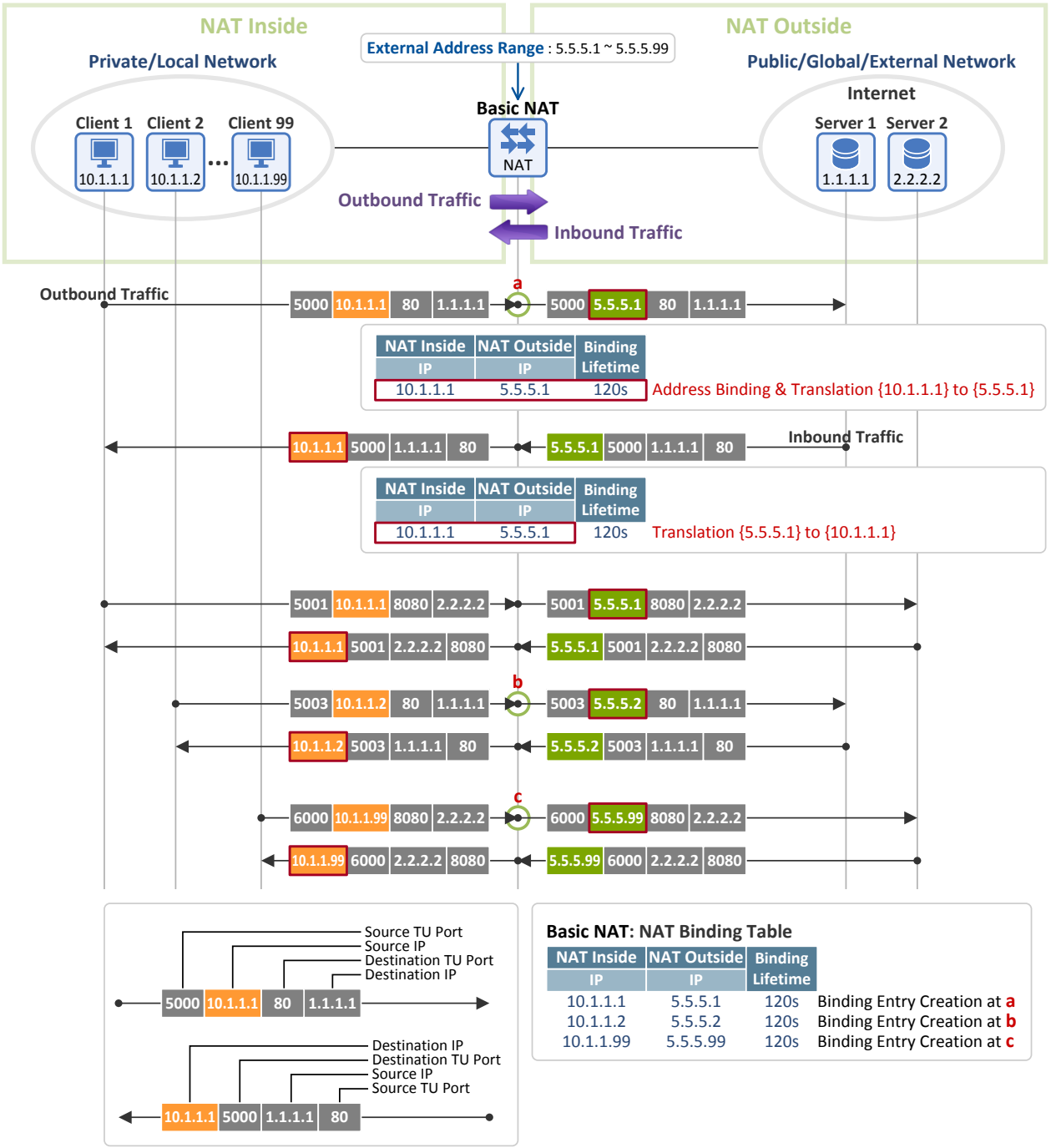
1:1 translation (1 = Public IP, 1 = Private IP)

■ **Mapping**

- Outbound Traffic: Translating a Private Source IP Address to a Public Source IP Address
- Inbound Traffic: Translating a Public Destination IP Address to a Private Destination IP Address

■ **Packet Modification**

Following packet information is replaced during translation:
- Outbound Traffic: Source IP Address, IP Header Checksum
- Inbound Traffic: Destination IP Address, IP Header Checksum



■ Three Translation Phases in a Session

1. Address Binding

A basic NAT binds a Public IP Address to each outbound traffic sent by a device with a Private IP Address (1:1 mapping), and generates a session entry in the NAT binding table.

2. Address Lookup and Translation

- Later when the NAT receives an outbound traffic packet (from a user device to NAT), it translates the Private Source IP Address of the packet to a Public Source IP Address by referring to the binding table, and delivers it on to the Internet.

- When it receives an inbound traffic packet (from the Internet to NAT), it translates the Public Destination IP Address of the packet to the IP address of the user device, i.e. a Private Destination IP Address, by referring to the binding table, and delivers it on to the user device.

3. Address Unbinding

If there is no incoming packet that corresponds to a session entry generated, the NAT deletes the entry from the NAT binding table.

■ **Deployment Example**

Enterprise Network

Network Address Port Translation (NAPT)

■ **Definition and Purpose**

NAPT is employed for saving public IP addresses. It provides a many-to-one translation of IP addresses. That means one public IP address is used when multiple user devices with a private IP address access the Internet.

> Nodes on the private network could be allowed simultaneous access to the external network, using the single registered IP address with the aid of NAPT. (RFC 3022)

■ **Translation Rule**

1:N translation (1 = Public IP, N = Private IP)

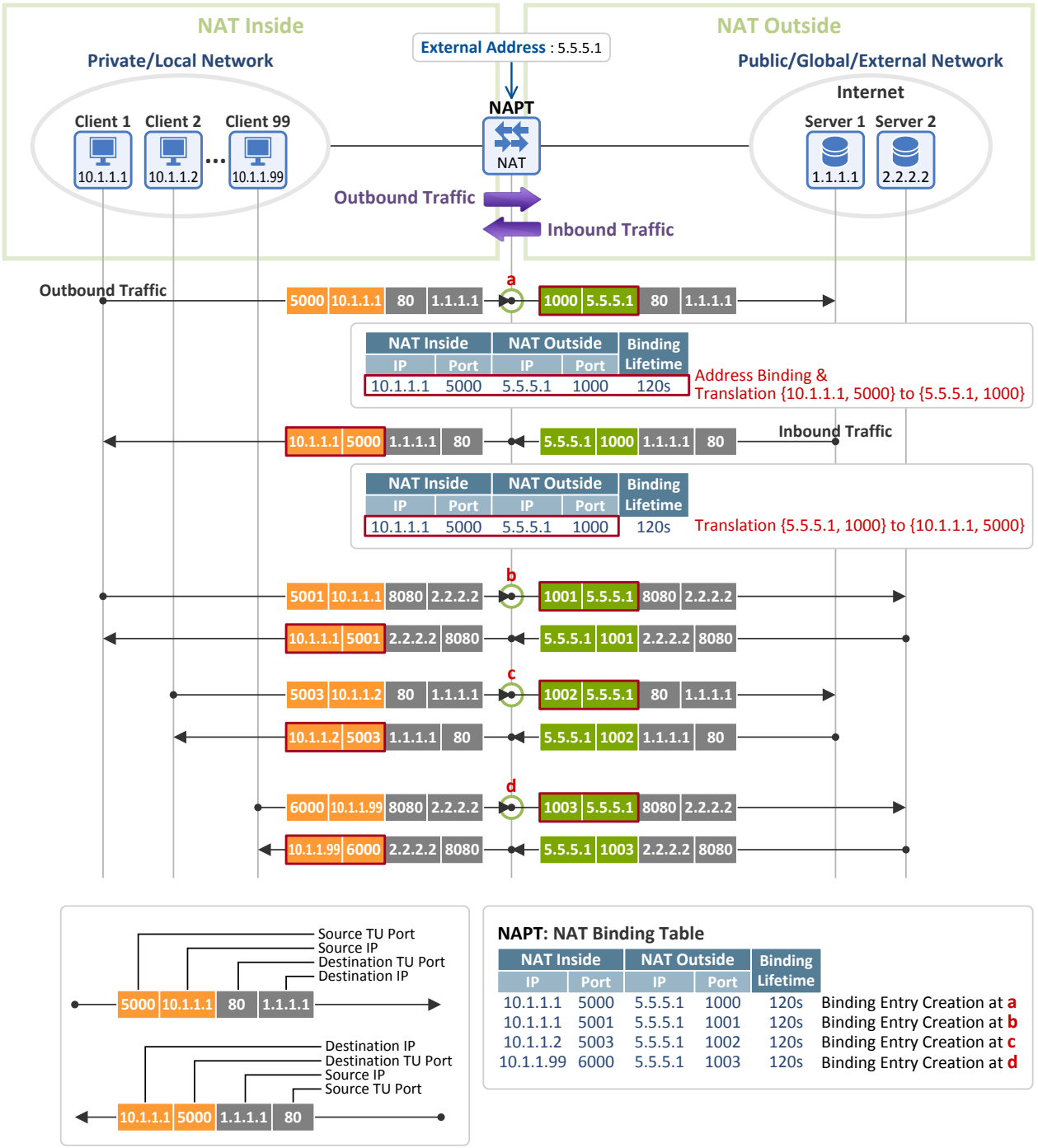
■ **Mapping**

- Outbound Traffic: Translating {Private Source IP Address, Local TU Source Port} tuple to {Public Source IP Address, Registered TU Source Port} tuple
- Inbound Traffic: Translating {Public Destination IP Address, Registered TU Destination Port} tuple to {Private Destination IP Address, Local TU Destination Port}

■ **Packet Modification**

Following packet information is replaced during translation:

- Outbound Traffic: Source IP Address, IP Header Checksum, TU Source Port, TCP/UDP Header Checksum
- Inbound Traffic: Destination IP Address, IP Header Checksum, TU Destination Port, TCP/UDP Header Checksum



■ Three Translation Phases in a Session

1. Address Binding

When a device with a Private IP Address sends an outbound traffic, a NAPT binds a Public IP Address and TU Source Port to the Private IP Address and TU Source Port of the device (1:N mapping). Then the NAPT generates a session entry for the traffic in the NAT binding table.

2. Address Lookup and Translation

- Later when the NAPT receives an outbound traffic packet (from a user device to NAT), it translates the Private Source IP Address and Local TU Source Port of the packet into a Public Source IP Address and Registered TU Source Port by referring to the binding table, and delivers it on to the

Internet (Registered ports refer to the ones assigned by a NAT. A Local TU Source Port is also called an "Internal Port", and a Registered TU Source Port is called an "External Port.).

- When it receives an inbound traffic packet (from the Internet to NAT), it translates the Public Destination IP Address and Registered TU Destination Port of the packet to the IP address and Port values of the user device, i.e. a Private Destination IP Address and Local TU Destination Port, by referring to the binding table, and delivers it on to the user device.

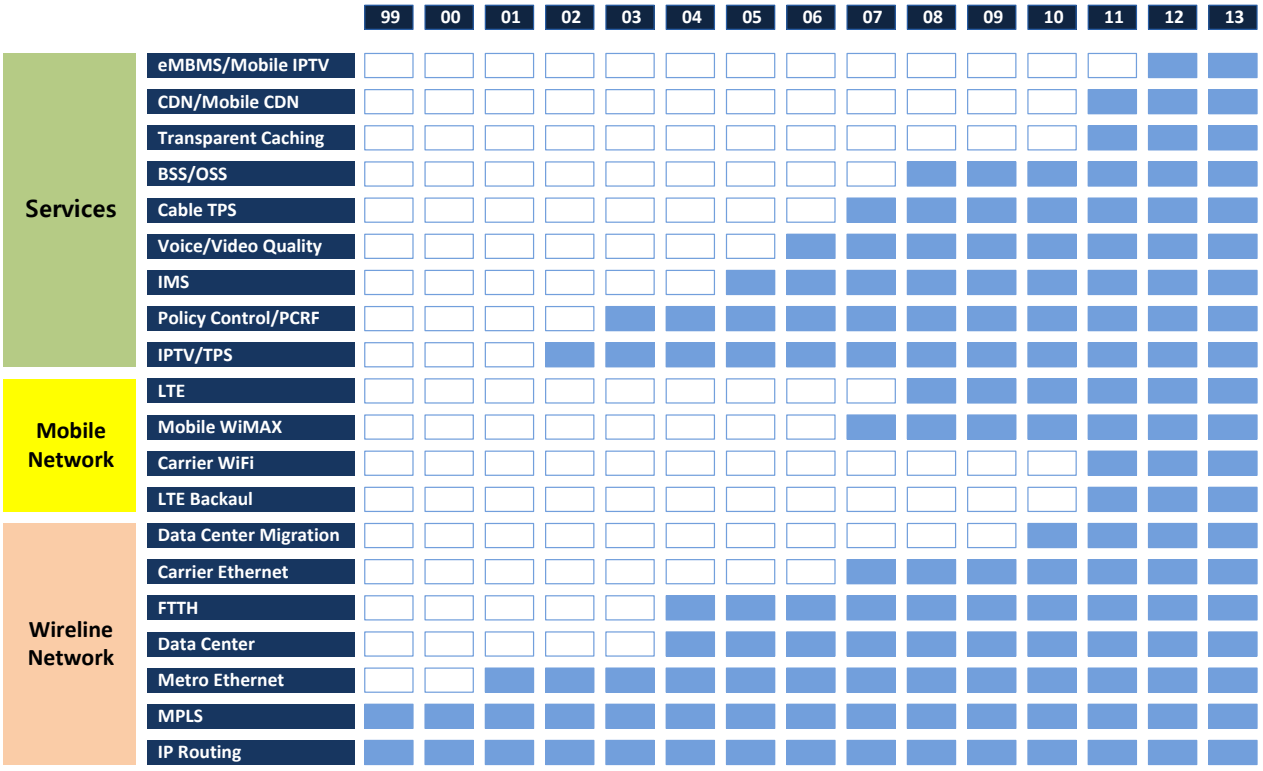
3. Address Unbinding

If there is no incoming packet that corresponds to a session entry generated, the NAPT deletes the entry from the NAT binding table.

■ **Deployment Example**

Wi-Fi Hotspot, SOHO, Home and 3G/LTE LSN

Netmanias Research and Consulting Scope

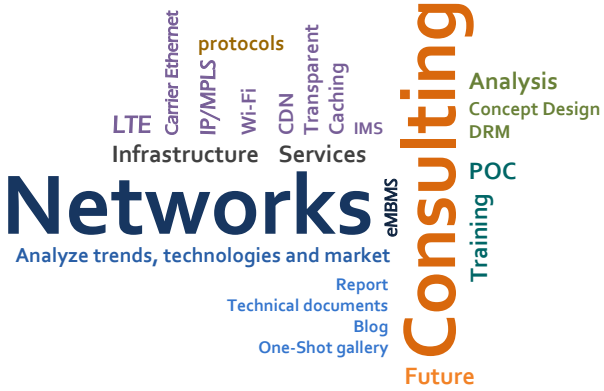


Visit http://www.netmanias.com to view and download more technical documents.

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.