A Retrospective View of Network Address Translation

IEEE Network • September/October 2008
Authors:
Lixia Zhang, University of California, Los Angeles
Speaker: Yu-Chan Lin
Outline

• Abstract
• Introduction
• How a NAT Works
• The Planned Solution
• Why NATs Succeeded
• The Other Side of the NAT
• Why the Opportunity of Standardizing NAT Was Missed

2010/6/30
Abstract

• Their ubiquitous adoption was not promoted by design or planning but by the continued growth of the Internet, which places an ever-increasing demand not only on IP address space but also on other functional requirements that network address translation is perceived to facilitate. This article presents a personal perspective on the history of NATs, their pros and cons in a retrospective light, and the lessons we can learn from the NAT experience.
Introduction

• A network address translator (NAT) commonly refers to a box that interconnects a local network to the public Internet.
• The same private address block can be reused in multiple local networks, as long as those networks do not directly talk to each other.
• NAT traversal solutions, such as simple traversal of UDP through NAT, traversal using relay NAT and Teredo, to name a few.
How a NAT Works
How a NAT Works (cont.)

• In the process of changing the IP address carried in the IP header of each passing packet, a NAT box also must recalculate the IP header checksum.

• Major benefit - one can connect a large number of hosts to the global Internet by using a single public IP address.
How a NAT Works (cont.)

- A number of drawbacks
  - changed the end-to-end communication model of the Internet architecture in a fundamental way.
  - if the NAT box crashes, it could lose all the existing state, and the data exchange between all of the internal and external hosts must be restarted.
A Recall of the History of NATs

• RFC 1287 also discussed pointed to a direction similar to current NATs:

  – Replace the 32-bit field with a field of the same size but with a different meaning. Instead of being globally unique, it would be unique only within some smaller region. Gateways on the boundary would rewrite the address as the packet crossed the boundary.
A Recall of the History of NATs (cont.)

- RFC 1335, published shortly after RFC 1287, provided a more elaborate description of the use of internal IP addresses (i.e., private IP addresses) as a solution to IP address exhaustion.

- Although these RFCs can be considered forerunners in the development of NAT, as explained later, for various reasons the IETF did not take action to standardize NAT.
A Recall of the History of NATs (cont.)

• The explosive growth underlined the urgency to take action toward solving both the routing scalability and the address shortage problems.

• The IETF took several follow-up steps, which eventually led to the launch of the IPng development effort.
The Planned Solution

• Short Term Solution
  – Classless inter-domain routing, or CIDR, was proposed as a short term solution. CIDR removed the class boundaries embedded in the IP address structure, thus enabling more efficient address allocation, which helped extend the lifetime of IP address space.
    • 120.101.10.X / 255.255.255.0
    • 120.101.10.X /24
Why NATs Succeeded

• The first recognized NAT advantages were stated in RFC 1918:
  – With the described scheme many large enterprises will need only a relatively small block of addresses from the globally unique IP address space. The Internet at large benefits through conservation of globally unique address space, which will effectively lengthen the lifetime of the IP address space. The enterprises benefit from the increased flexibility provided by a relatively large private address space.
Why NATs Succeeded (cont.)

• Anyone can use a large block of private IP addresses — up to 16 million without asking for permission — and then connect to the rest of the Internet by using only a single public IP address.
Why NATs Succeeded (cont.)

• NATs can be unilaterally deployed by any end site without any coordination by anybody else.

• The major gains from deploying a NAT were realized on day one, whereas its potential drawbacks were revealed only slowly and recently.
The Other Side of the NAT

• In most networks, the majority of the traffic is confined to its local area networks.

• The number of machines that act as Internet servers, that is, run programs waiting to be called by machines in other networks, is often limited and certainly much smaller than the total number of machines.
The Other Side of the NAT (cont.)

• The use of these machines is primarily limited to their local environment. They also can be used as clients such as ftp and telnet to access other machines.

• For security reasons, many large organizations, such as banks, government departments, military institutions, and some companies, allow only a very limited number of their machines to have access to the global Internet.
The Other Side of the NAT (cont.)

• Client-server to a peer-to-peer model, meaning that any host may call any other host.

• In addition to the change of application patterns, a few other problems also arise due to the use of non-unique, private IP addresses with NATs.
Why the Opportunity of Standardizing NAT Was Missed

• The feasibility of designing and deploying a brand new IP was misjudged, as were the time and effort required for such an undertaking.

• Yet another factor was that given that network address translation could be deployed unilaterally by a single party alone, there was not an apparent need for standardization.
Why the Opportunity of Standardizing NAT Was Missed (cont.)

• NAT deployment was widely rolled out, and the absence of a standard led to a number of different behaviors among various NAT products.

• IPSec、SAP、SIP

IPSec: IP Securely    SAP: Session Announcement Protocol
SIP: Session Initiation Protocol
Looking Back and Looking Forward

• The original IP design clearly defined an IP address as being globally unique and globally reachable and as identifying an attachment point to the Internet.

• Last, but not least, I believe it is important to understand that successful network architectures can and should change over time. All new systems start small. Once successful, they grow larger, often by multiple orders of magnitude as is the case of the Internet.
Thank you.

****************************

Q & A