|  |
| --- |
| Skolkovo institute of science and technology |
| Analysis of high performance software NAT design approaches |
| Denis Plotnikov |
|  |
| **June, 2015** |

**Table of Contents**

[**Part 1 NAT OVERVIEW** 2](#_Toc416958414)

[**1. Introduction** 2](#_Toc416958415)

[**2. Background and motivation** 2](#_Toc416958416)

[**2.1 NAT Purpose and Motivation of Using** 2](#_Toc416958417)

[**1.2.2 NAT operation** 3](#_Toc416958418)

[**1.2.3 NAT behavioral requirements** 4](#_Toc416958419)

[**1.2.4 Carrier grade NAT (CG-NAT)** 7](#_Toc416958420)

[**1.3 NAT implementations comparison and analysis** 9](#_Toc416958421)

[**1.3.1 Software NAT** 9](#_Toc416958422)

[**1.3.2 Hardware NAT** 9](#_Toc416958423)

[**1.3.3 Software and hardware NAT comparison** 9](#_Toc416958424)

[**1.3.4 The comparison and analysis results.** 12](#_Toc416958425)

[**1.4 NAT improvements** 12](#_Toc416958426)

[**Part 2. ANALYSIS OF NAT DESIGN APPROACHES** 13](#_Toc416958427)

[**2.1 Overview of high performance design approaches** 13](#_Toc416958428)

[**2.2 Software NAT design exploration** 13](#_Toc416958429)

[**2.2.1 NAT design overview** 13](#_Toc416958430)

[**2.2.3 NAT bottlenecks** 13](#_Toc416958431)

[**2.2.4 How to overcome the bottlenecks** 13](#_Toc416958432)

[**2.3 NAT performance** 13](#_Toc416958433)

[**2.3.1 Performance metrics** 13](#_Toc416958434)

[**2.3.2 Target metric values** 13](#_Toc416958435)

[**2.4 Implementation** 13](#_Toc416958436)

[**Part 3. RESULTS** 13](#_Toc416958437)

[**3.1 Evaluation** 13](#_Toc416958438)

[**3.1.1 Measurement setup** 13](#_Toc416958439)

[**3.1.2 Experimental methodology** 13](#_Toc416958440)

[**3.2 Results discussion** 13](#_Toc416958441)

[**3.3 Conclusion** 13](#_Toc416958442)

[**REFERENCES** 29](#_Toc416958443)

[**Appendix A** 30](#_Toc416958444)

**Part 1 NAT OVERVIEW**

**1. Introduction**

These days each device tends to communicate with the rest of the world over the Internet. The internet is a gigantic data network used IP protocol for nodes identification and consists of big number of sub networks. These sub networks have a way of transparent communication between the nodes inside and outside the sub network. The transparent way is called NAT (*Network Address Translator*). The main its function is changing the source IP address and port number of the packet going from the inner network and changing the destination IP address and port number of coming to the inner network packets. This process is called *address translation.* There is a set of requirements for a NAT which stays the same but has some difference depending on the size of network and the use case.

There are different types of NAT implementations: software and hardware. The software versions of NAT provide all the required functionality but have low performance level. The hardware versions provide full functionality and high performance but usually expensive. Nowadays, when the high performance needed the hardware NATs have no competitors.

This work is focused on finding the way of making a software version of NAT which would have the same performance as a hardware version.

The work organized as follows. Part 1 gives overview of NAT technology and the existing NAT solutions, formulates the requirements to the NAT in terms of functionality and the performance. Part 2 does the software design approach analysis. Part 3 analyzes the results acquired from implementation of the approaches described in part 2, makes a conclusion of what the best approach to use among described is and formulates the conclusion.

**2. Background and motivation**

**2.1 NAT Purpose and Motivation of Using**

NAT was invented as a way of using a single IP address for several network devises. Thus, the main reason of using it is to reduce the number of IP addresses used by a number of network devices. Besides of the main functionality the NAT gives some security benefits like internal network structure hiding while and ability to restrict the access to the outer network of an internal node. Some versions of NAT provide functionality of translating IPv4 address to IPv6 which is helpful when changing provider settings.

This time the number of network devices grows rapidly because personal devises with the Internet access become more popular and more people starts using it every day. Each of those devices needs a network address to communicate through the data network. Presently, the main protocol used in the Internet is IPv4. The problem with IPv4 is that at the time the number of address in the IPv4 reached its limit and the organization affiliated to manage the addresses issues has stopped its free distribution at 2012 **[ref\_ripe\_limit]**.

As the number of IPv4 addresses has reached its limit the addresses are turning into more and more valuable resource and the price of buying or renting it becomes higher and higher which means that more and more network devices will share the one IPv4 address for the Internet accessing [rfc\_6888].

Although, IPv6 seems to be a solution of the lack of IPv4 addresses the process of switching to IPv6 is quite slow. The most likely reason for that is the whole network setting changing necessity as well as a need to remove all legacy network equipment and software which are not compatible with IPv6. This will take a lot of efforts from the Internet providers and they are not ready to put many of them right away because of the investments needed. Instead, they keep working on IPv4 using NATs to reduce the number of “white” IPv4 addresses used.

**1.2.2 NAT operation**

This document is focused in exploring of traditional NAT setup as most frequently used. Although, other NAT setups also have its own application case but they are quite rare in the real world and omitted from the consideration.

The traditional NAT setup [ref\_rfc3022] looks as follows. There are two networks which considered by NAT as *inner* and *outer.* The inner network is the local area network served with NAT. The outer network is the wide area network which can communicate with inner network via the NAT only. There are two main NAT methods Basic NAT and NAPT (Network Address Port Translator). Basic NAT performs IP address translation only (i.e. changing a source IP address of a packet to an IP address allocated to NAT for translation)without changing of port number when NAPT does translation of a tuple {IP, port (TCP/UDP/ICMP)}. These days NAPT method is used mostly and further in this document it is implied when saying NAT.

<here goes the scheme of NAT operation>

NAT operations as follows: a node from inner network sends a packet to a node in the outer network. The packet comes to the NAT. The NAT gets the packet, allocates an IP address and port number for translation. Then, the source IP address and port number stores in the NAT with respect to just allocated IP and port number to perform backwards translation. The packet source IP address and port number is replaced with the allocated tuple and checksums of IP and TCP/UDP/ICMP headers of the packet are recalculated. After that, the packet is sent to the destination node in the outer network. The outer network node receives the packet and sends a replying packet using the tuple of source IP address and porn number from the just received packet as the destination IP address and port number in its packet. The replying packet comes to the NAT. The NAT using the destination address and port number from the replying packet looks for the corresponding tuple of IP address and port number saved previously.

Having found the tuple, the NAT performs destination IP address and port number replacement in the replying packet as well as changing of checksums in IP and TCP/UDP/ICMP packets. Then the replying packet is sent to the node in the inner network which was an originator of connection.

Although, NAT supplies transparency to inner and outer nodes communication (i.e. the nodes know nothing about NAT existing) it has a serious disadvantage. There are a set of application protocols (FTP, DNS, PPTP, H.323, etc.) working onto TCP/UDP that store the connection data (i.e. IP address and port number) inside their packet on the level upper than L4 of ISO model where TCP/UDP works. This fact leads to inconsistency of IP addresses and port numbers in translated by NAT packets where source IP and port number in TCP/IP headers doesn’t match to the source IP and port number in the upper level protocol headers. This problem is solved with ALGs (Application Layer Gateway) working with NAT. There are different protocol specific ALG. Each ALG protocol are able to distinguish and process the packets belongs to the protocol accordingly. This document is not focused on using ALGs in NAT and only core traditional NAT functionality is taken into consideration.

**1.2.3 NAT behavioral requirements**

NAT behavioral requirements for TCP, UDP and ICMP are clearly stated in [ref\_rfc5382], [ref\_rfc4787] and [ref\_rfc5508] respectively. Here the generalized list of NAT behavioral requirements based on mentioned documents is shown.

1. A NAT must have an “Endpoint-Independent mapping” behavior. Endpoint-Independent mapping means that the NAT reuses port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port[ref\_rfc4787]
2. A NAT must support all valid sequences of TCP/UDP/ICMP packets for connections initiated both internally as well as externally when the connection is permitted by the NAT. In addition to handling the TCP 3-way handshake mode of connection initiation, A NAT must handle the TCP simultaneous-open mode of connection initiation
3. If application transparency is most important, it is RECOMMENDED that a NAT have an "Endpoint-Independent Filtering" behavior for TCP. If a more stringent filtering behavior is most important, it is RECOMMENDED that a NAT have an "Address-Dependent Filtering" behavior.

*Endpoint-Independent Filtering* means that 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* means that for receiving 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

1. A NAT must not respond to an unsolicited inbound TCP SYN packet for at least 6 seconds after the packet is received. If during this interval the NAT receives and translates an outbound TCP SYN for the connection the NAT must silently drop the original unsolicited inbound TCP SYN packet. Otherwise, the NAT should send an ICMP Port Unreachable error (Type 3, Code 3) for the original TCP SYN. The NAT must silently drop the original TCP SYN packet if sending a response violates the security policy of the NAT
2. If a NAT cannot determine whether the endpoints of a TCP connection are active, it MAY abandon the session if it has been idle for some time. In such cases, the value of the "established connection idle-timeout" must not be less than 2 hours 4 minutes. The value of the "transitory connection idle-timeout" must not be less than 4 minutes. The value of the NAT idle-timeouts may be configurable.
3. A NAT UDP mapping timer must not expire in less than two minutes, unless the port number is from the well-known port range of 0 -1023. In that case NAT may have shorter UDP mapping timers. The value of the NAT UDP mapping timer MAY be configurable. A default value of five minutes or more for the NAT UDP mapping timer is recommended.
4. A NAT must not have a "Port assignment" behavior of "Port overloading". Another words, the NAT must not always use port preservation even in the case of port collisions
5. It is recommended that a NAT have an "IP address pooling" behavior of "Paired". It means that the NAT use the same external IP address mapping for all sessions associated with the same internal IP address. This requirement is not applicable to NATs that do not support IP address pooling
6. It is recommended that a NAT have a "Port parity preservation" behavior which means that after the NAT processing an even UDP port will be mapped to an even UDP port, and an odd UDP port will be mapped to an odd UDP port.
7. If a NAT includes ALGs it is RECOMMENDED that all of those ALGs (except for FTP) be disabled by default.
8. A NAT must support "hairpinning" for TCP/UDP/ICMP. A NAT's hairpinning behavior must be of type "External source IP address and port". This means that two nodes are behind the same NAT both use for communication to each other different tuples of external IP address and port allocated by NAT
9. Unless explicitly overridden by local policy, a NAT device must permit ICMP Queries and their associated responses, when the Query is initiated from a private host to the external hosts
10. An ICMP Query session timer must not expire in less than 60 seconds. It is recommended that the ICMP Query session timer be made configurable
11. When an ICMP Error packet is received, if the ICMP checksum fails to validate, the NAT should silently drop the ICMP Error packet. If the ICMP checksum is valid, do the following: If the IP checksum of the embedded packet fails to validate, the NAT should silently drop the Error packet; If the embedded packet includes IP options, the NAT device must traverse past the IP options to locate the start of the transport header for the embedded packet; the NAT device should not validate the transport checksum of the embedded packet within an ICMP Error message, even when it is possible to do so; if the ICMP Error payload contains ICMP extensions, the NAT device must exclude the optional zero-padding and the ICMP extensions when evaluating transport checksum for the embedded packet.
12. If a NAT device receives an ICMP Error packet from an external realm, and the NAT device does not have an active mapping for the embedded payload, the NAT should silently drop the ICMP Error packet. If the NAT has active mapping for the embedded payload, then the NAT must do the following prior to forwarding the packet, unless explicitly overridden by local policy: revert the IP and transport headers of the embedded IP packet to their original form, using the matching mapping; leave the ICMP Error type and code unchanged; modify the destination IP address of the outer IP header to be same as the source IP address of the embedded packet after translation.
13. If a NAT device receives an ICMP Error packet from the private realm, and the NAT does not have an active mapping for the embedded payload, the NAT should silently drop the ICMP Error packet. If the NAT has active mapping for the embedded payload, then the NAT must do the following prior to forwarding the packet, unless explicitly overridden by local policy: revert the IP and transport headers of the embedded IP packet to their original form, using the matching mapping;
14. leave the ICMP Error type and code unchanged; if the NAT enforces Basic NAT function, and the NAT has active mapping for the IP address that sent the ICMP Error, translate the source IP address of the ICMP Error packet with the public IP address in the mapping. In all other cases, translate the source IP address of the ICMP Error packet with its own public IP address
15. While processing an ICMP Error packet pertaining to an ICMP Query or Query response message, a NAT device must not refresh or delete the NAT Session that pertains to the embedded payload within the ICMP Error packet.
16. When a NAT device is unable to establish a NAT Session for a new transport-layer (TCP, UDP, ICMP, etc.) flow due to resource constraints or administrative restrictions, the NAT device should send an ICMP destination unreachable message, with a code of 13 (Communication administratively prohibited) to the sender, and drop the original packet.
17. A NAT device MAY implement a policy control that prevents ICMP messages being generated toward certain interface(s).
18. Receipt of any sort of ICMP message MUST NOT terminate the NAT mapping or TCP connection for which the ICMP was generated.

The requirements listed above do not guarantee the compliance of NAT with all application protocols but fulfilling them significantly improves the likelihood of successful processing of any kinds of packets.

**1.2.4 Carrier grade NAT (CG-NAT)**

The NAT supplies the ability to share a single external IP address among several nodes in the external network. Some of internet service providers have started offering this service long before IPv4 address space shortage problem has arisen showing that there is another driven force of using NAT. Each subscriber at the ISP’s network assigned a private address and the NAT, situated at the customer edge, translates traffic between public and private addresses[ref\_frc6888].

Because of scales of ISP’s networks NATs used there have some additional functional and determined performance requirements. The list of NAT functional requirements is added with following points (taken from [ref\_frc6888]) extending the points shown previously in this chapter:

1. The CGN function should not have any limitations on the size or the contiguity of the external address pool. In particular, the CGN function must be configurable with contiguous or non-contiguous external IPv4 address ranges
2. A CGN MUST support limiting the number of external ports (or, equivalently, "identifiers" for ICMP) that are assigned per subscriber. Per-subscriber limits must be configurable by the CGN administrator. Per-subscriber limits may be configurable independently per transport protocol. Additionally, it is recommended that the CGN include administrator-adjustable thresholds to prevent a single subscriber from consuming excessive CPU resources from the CGN (e.g., rate-limit the subscriber's creation of new mappings).
3. A CGN should support limiting the amount of state memory allocated per mapping and per subscriber. This may include limiting the number of sessions, the number of filters, etc., depending on the NAT implementation. Limits should be configurable by the CGN administrator. Additionally, it should be possible to limit the rate at which memory-consuming state elements are allocated.
4. It must be possible to administratively turn off translation for specific destination addresses and/or ports.
5. Once an external port is deallocate, it should not be reallocated to a new mapping until at least 120 seconds have passed, with the exceptions being If the CGN tracks TCP sessions TCP ports MAY be reused immediately. If external ports are statically assigned to internal addresses, the assignment remains constant across state loss, than ports may be reused immediately. If the allocated external ports used address-dependent or address-and-port-dependent filtering before state loss, they may be reused immediately. The length of time and the maximum number of ports in this state must be configurable by the CGN administrator.
6. A CGN must implement a protocol giving subscribers explicit control over NAT mappings. That protocol SHOULD be the Port Control Protocol [RFC6887]
7. CGN implementers should make their equipment manageable. Standards-based management using standards such as "Definitions of Managed Objects for NAT" [RFC4008] is recommended
8. When a CGN is unable to create a dynamic mapping due to resource constraints or administrative restrictions (i.e., quotas): it must drop the original packet; it should send an ICMP Destination Unreachable message with code 1 (Host Unreachable) to the sender; it should send a notification (e.g., SNMP trap) towards a management system (if configured to do so); it must not delete existing mappings in order to "make room" for the new one. (This only applies to normal CGN behavior, not to manual operator intervention.)

The requirements listed above do not guarantee the compliance of NAT with all application protocols and is based on the best practices. Fulfilling the requirements significantly improves the likelihood of successful processing of any kinds of packets while NAT working on the ISP edge.

**1.3 NAT implementations comparison and analysis**

There are two types of NATs available: software and hardware.

**1.3.1 Software NAT**

Software NAT is a program that implements NAT functionality and works on the top of operating system. There are two kinds of software NAT implementation. One is a user program working in the user mode totally like *NAT32 IP Router* [ref\_nat32] or *WinGate* for windows or *IPFilter* for Linux and using the OS resources to access the network. It can be installed or uninstalled by user’s demands. There are commercial versions of this kind of NAT as well as free once.

Another kind of software NAT is a program working in the kernel space like Linux module or is a part of operation system like *ICS* in Windows or *iptables* in Linux. As this kind of NAT distributed along the operation systems it is usually free. Some of UNIX family software NATs have opened source code and are free for changing.

**1.3.2 Hardware NAT**

Hardware NAT is a specialized network device or a feature of specialized network device like firewall or router. These devices usually have their own specific operation system and interfaces for management. The hardware core of hardware NAT device consist of a specific processor designed for fast packet processing as well as associative memory and another chips that increase the performance in specific operations. Hardware NATs are produced by telecommunication producers like Cisco, Juniper and others. These devices have high performance and are expensive.

**1.3.3 Software and hardware NAT comparison**

**Functionality:** As hardware NAT is usually a part of industrial firewall or a router which is used at Internet Services Provider’s or Data Center’s facilities it is equipped with vast functionality where NAT is one of many. The functionality includes firewall, VPN support and crypto security features allowing a customer to have many of needed abilities in one box. Software NAT is often is an integral part of operation system and its functionality is not that advanced because it is usually used for small offices or tiny private networks. Talking about NAT core functionality, both of them provide full support of NAT requirements.

**Performance:** Hardware NAT is specially designed for high performance used the cutting edge hardware for achieving it. In particular, for the performance improvement special memory units are used called CAM (Content-addressable memory a.k.a. associative memory). CAM(TCAM) is extremely fast in tasks of comparing input data against stored data and returning matched data as a result. Although CAM is fast it has low memory capacity and very high price. One unit with capacity of 80Kbytes costs around $180 while hundreds of these units needed in a router working at an ISP’s rack.

Software NAT is installed in commodity computers and has a serious performance limiting factor. As software NAT use OS system as the source of network resources it uses OS system calls to get them and, hence, is limited by the performance of that system calls which means that the NAT is not able to outperform the OS it uses. Thus, the main limiting factor is the network stack used by the operation system. The experiment revealed the packet performance rate for Linux 3.16 kernel around 260 Kpps.

**Upgradability:** The hardware NAT is a set of hardware mounted in some kind of chassis with a piece of specialized software pre-installed which is hardly be compatible with different set of hardware because of technical and vendor limitations. Another thing is that because of the software, controlling the hardware NAT is proprietary and upgrading might be an issue. This makes the only way of upgrading this equipment possible: buying a new software update, support plan, new hardware NAT device from the vendor. Unlike hardware NAT, software NAT can be installed at any system supporting the OS the software NAT specialized. Thus, increasing of performance is possible by updating the hardware where the software NAT installed. As software NAT is just a program than the upgrading/updating could be done by using the same approach as other pieces of software used with paying no attention to the hardware used. This makes the software NAT more flexible in terms of modification and customization.

**Price:** The price of the system implementing NAT functions based on software NAT consists of several parts: price of the computer, price of the OS and the price of software NAT itself. The price of software NAT program was around $2200 (Win gate [ref\_wingate]) for maximum functional version at the time of writing. There are free versions of software NAT working on free OS like iptables on Linux. In that case the price depends on the price of computer used only.

As for hardware NAT the prices are much higher. This is mainly due to pieces of hardware used in producing of such devices but the vendor interests also play a big role. The marked research has been done to evaluate the prices and the results are shown in Figure 1.

For evaluation a set of edge routers was taken produced by three well known telecommunication equipment vendors: HP, Cisco and Juniper. The performance of the NAT mode has not been found and firewall on mode was used as an approximation. The packet processing rate and related price for the set of HP devices seems to be not consistent with the same data for Cisco and Juniper devices. This is could be a consequence of difference in the packet processing rate definition and measuring methodology used by different vendors. When claiming performance, Juniper and Cisco use packet processing rate with firewall turned on. HP doesn’t give any clarification about the mode they used for packet processing rate measuring. The data found for Juniper and Cisco routers shows pretty much the same trend and, thus, it can be considered as trustworthy and showing the current situation on the market.

It is seen from the chart that high performance costs a lot: roughly 15 000 USD for each 1 Mpps which makes buying of the router the matter of capital investments for ISPs.

The data for the chart was collected from the public resources on the Internet. The prices are relevant for Russian market, for other countries prices may vary. The list of model used is in Appendix A.

**1.3.4 The comparison and analysis results.**

The results of comparison are shown in Table 1. The analysis revealed the situation as following. Hardware NAT provides vast functionality and high performance wherein the price is much higher than software NAT provides. The reason for the lower software NAT performance is limited packet processing ability of underlying OS. Also, Hardware NAT is hard to upgrade because of the high cost whereas Software NAT is easily updatable because it is just a program working on top of operation system.

|  |  |  |
| --- | --- | --- |
|  | Hardware NAT | Software NAT |
| Additional functionality | High | Low |
| Performance | High | Low |
| Upgradeability | Low | High |
| Price | High | Low |

**Table 1. Advantages and disadvantages comparison of hardware and software NATs. The advantages marked with red color**

**1.4 NAT improvements**

Based on the analysis, the reasonable improvement would be increasing of performance of the Software NAT. In this case it could significantly increase the number of cases where Software NAT could be used instead of Hardware NAT by that decreasing the amount of necessary investments. In particular, software version of NAT could be applied at ISP’s facilities playing the role of a CG-NAT. If the price of software NAT deploying would be much lower than the price of using hardware NAT at the same place than the development of such a system would worth of efforts.

This work is focused on exploring feasibility and reasonability of software NAT development that could be compared with hardware NAT in performance. Further in this work the name “the software CG-NAT” is used to denote the goal of exploration.

**Part 2. ANALYSIS OF NAT DESIGN APPROACHES**

**2.1 Overview of high performance design approaches**

**2.2 Software NAT design exploration**

**2.2.1 NAT design overview**

**2.2.3 NAT bottlenecks**

**2.2.4 How to overcome the bottlenecks**

**2.3 NAT performance**

**2.3.1 Performance metrics**

**2.3.2 Target metric values**

**2.4 Implementation**

**Part 3. RESULTS**

**3.1 Evaluation**

**3.1.1 Measurement setup**

**3.1.2 Experimental methodology**

**3.2 Results discussion**

**3.3 Conclusion**

**<<<<<<<< THE END SO FAR >>>>>>>>**

<HOW CAN WE DO BETTER>

Algorithmic(data structure) + technology(software/hardware architecture approaches (batching processing, NIC RSS queues, multithreading, “locklessness”, DDIO ) -> consequence DPDK already have all of those so let’s choose it)

…

<THE GOAL OF THIS WORK>

let’s try to make one reducing the price of nat as much as we can

…

**NAT DEVELOPING**

<related works -- how we are going to do attack the problem and what do we need for that – BASICALLY THE INTRO OF THIS PART >

**NAT Performance Metrics**

**CG NAT Target Metric Values**

Based on the sources of information the performance requirements of the NAT device are set following:

* Packet processing rate: 5.5 Mpps
* Concurrent session support: 65.5M (a B-class network with up to 1000 active ports for each node)
* Connection setups rate: 3 Mcsps
* Throughput: 10 Gbps

**NAT Design Approach**

The design process of the NAT system consists of two parts. In the first part the exploration of possible algorithms and data structures are made to choose the one which gives the best performance results. The second part is about choosing of technological approaches which give an answer to the question of how the program have to be structured and what technics have to be used to achieve the target performance.

**NAT testing application**

For choosing the approach of building the NAT the testing application has been made. To simulate the NAT workflow several solutions have been implemented which use different data structures and software organization options. Conditionally the program can be split into 3 parts: measuring part, generation part and simulating part.

***The measuring part*** consists of the environment that performs testing routine and calculates the performance results. The metric produced by this part is cycles per packet. This metric is acquired by using **rdtsc** instruction which reads the internal processor tick counters. The measuring part performs the number of tests set by the user and as an output calculates the average value of cycles per packet achieved and standard deviation of the result.

***The generation part*** generates a packet set to be processed by the simulation part. It imitates uniformly distributed network activity and stores generated packets in a one-dimensional array of structures which is the input to the simulation part. Time of packet set generation isn’t taken into account when calculating the performance of the algorithm.

***The simulation part*** is a core of the testing application and consists of NAT routine. There are several mandatory actions which must be performed by any NAT to actually perform proper packets translations. They are: calculation of the check sum, setting time stamp and saving/acquiring translation information in a NAT lookup data structure. The last point is the main exploration area of this document.

There are several necessary action to be performed by the NAT in order to perform address translation properly besides changing of packet’s IP address and number of TCP/UDP port in the corresponding headers. They are: calculation of the checksum for IP and TCP/UDP headers and storing the timestamp of the particular translation.

The checksum calculation is related to the packet processing. This action should be performed each time when the packet translation occurs and a packet IP and port number changed in order to be consistent with the requirements of the IP[1.4 of ref\_rfc791] and TCP/UDP protocols [1.5 of ref\_rfc793 and rfc\_768].

The storing of the timestamp translation in the NAT translation data structure is necessary and cannot be eliminated because of the Mapping Refresh requirement for NATs [ref\_rfc4787].

For the testing purposes in the NAT testing program the following function implementations are used. For checksum calculation *ip\_fast\_csum()* from Linux kernel is used. For getting/setting the timestamp *gettimeofday()* Linux system call is used. However, some different, faster, source of timestamp data can be used, for example CPU ticks counter which is faster but trickier when connecting it to the physical time. These functions might be potential targets of performance optimization but are out of the scope of this document.

**NAT testing methodology**

In getting metrics values the test setup plays a key role. The values of the metrics are highly dependent on the test methodology.

To get the values of interest the following setup was used. There were packets with mostly unique (more than 99%) tuples of IP and Port number in the packet set. The test routine gave this packet set as an input to the testing NAT routine. The routine processed each packet and change the values of IP, port number and checksums in the packet saving this data at the same packet set. Once all packets processed the routine performed backward translation simulating the response of the node from the outer network to the just translated and transmitted packet. After all packet processing has been done the check for translation correctness was performed.

This testing routine was used in order to simulate the most intensive regime of network working: the nodes of the network are constantly trying to communicate with nodes in the outer network but the NAT device is offline, then the NAT device is switched on and right away starts serving the nodes connection, creating and performing new translations. This routine is more computationally intense that just packet translation because the creating of a new connection costs more than just a packet translating as it includes search for the connection translation data and if it was not found than creating of a new translation entry is done.

This is the worst case scenario of network operating. The kind of testing used, allows getting the fair level of the NAT device performance.

**“Ideal” NAT Performance and Packet Processing Latency**

The most interesting part in the NAT system is the algorithm and data structure for storing the address translation information. In fact, two of the data structures are needed because of the necessity to store two pieces of data for a single address translation. The first one is the data about translation from LAN to WAN and second one is the data about the translation from WAN to LAN. From the first glance it isn’t clear how to organize them well. This issue is explored further in the document.

Before starting the exploration of the NAT translation algorithms and data structures it is essential to estimate the performance of the system which uses the ideal NAT translator. By word “ideal” the zero-time lookup data structure is implied. To get this estimation the bogus data structure has been used which returns deterministic result and requires computation time tends to be zero. Another words, it is a function which cyclically returns the same sequence of results.

In the figure 1 there are some results explaining the cost of one packet processing having the ideal lookup data structure. One packet processing takes around 120 cycles including calculation of checksums and timestamps settings processing. The packet processing routine takes around 40 cycles including processing of the test packet set which could be thought like simulation of packet acquiring from the network interface card queues. Thus, the overall overhead of packet data checksums calculation and timestamp/timeout processing is around 80 cycles.

Based on this data it is possible to claim that than closer the performance of a NAT to “ideal” values than better the NAT setup is. In our case the ideal value is 120 cycles/pkt.

Figure 1. "Ideal" NAT performance

Having this results in mind, the latency value for a single packet processing becomes known. The ***latency*** is 119 cps or 50 ns.

**NAT Bottleneck**

In this chapter the part of NAT system is to be investigated which has the most significant influence on overall NAT performance. Each NAT system should store information in some kind of data structure to be able to retrieve this information when it is necessary. Having in mind that the NAT should be able to support 65.5M unique translations, it is easy to conclude that its lookup data structure have to be able to store 65.5M records and the search process will take a majority of packet processing time because of the size of this data structure. To achieve the target packet processing rate (5.5M pps) it is easy to calculate how many cycles could be spent on a packet. Having a processor working on 2.4GHz frequency we could spend 436 cycles per packet. Hence, our target performance characteristic in cycles per packet is 436.

As it is seen from the Figure 1 the processing time of one packet excluding searching for translation data is a constant. This process is quite fast and can be compared with processors L3 cache miss penalty which is around 100 cycles.

So the first question to investigate is how fast the searching process is and does it really necessary to choose the algorithm and data structure. To answer that question the test has been performed which uses as a lookup data structure a simple linear array with linear search algorithm [ref\_cormen]. This algorithm is known as having O(n) search time and can be a good starting point of performance exploration.

The results of testing the algorithm are shown in Figures 2.1 and 2.2

Figure 2.1 NAT Performance: Linear search in cycles per packet

Figure 2.2 NAT Performance: Linear search in packets per second

Linear search revealed the high linear performance degradation with increasing of the NAT records capacity: at size of 2000 entries the time of a packet processing is 3 times higher than at size of 500 entries and 3 times higher than the target performance.

These results show that the translation data search is a real and quite serious bottleneck of the NAT performance and to solve this problem some effective algorithms and data structures are needed.

**Testing of NAT lookup data structures and algorithms**

The target capacity of the NAT translation information data structure is 65.5M records which makes the NAT data structure space consuming. Having stored IP address and port number for each unique translation, minimum size of the data structure size is 65.5M \* [4 (IP) + 2 (port) + 2(timestamp)] = 524 Mb. The NAT must be able to perform two translations for a single connection: from its inner network to its outer network and vice versa. So, it should have 2 similar data structures to store corresponding translation information. Thus, the amount of memory to be allocated is 2 \* [data structure size] which is 1048 Mb in our case. This amount of memory could be reduced and it is shown in further chapters of this document but nevertheless it is still a big chunk of memory which cannot be placed in the fast CPU cache memory so the solution to be chosen cannot rely on that memory and should take into consideration software construction approaches that could help to eliminate cache misses which could be a key point in the race to the performance.

To find a suitable solution it is worth to look for a data structure which provides better lookup time than O(n) and doesn’t allow significant memory overheads because of the big given amount of data to be stored but leaving acceptable level of data locality[ref\_locality] for reducing of CPU overheads. In particular, this research is focused on the data structures and algorithms with search time equal or less than O(logN) because they significantly reduce the amount of reads from the memory. In our case, using an ideal algorithm with O(logN) search time on 65.5M gives around 26 memory reads. This number is quite theoretical because in the real word CPU needs a number of addition memory reads. The performance of this approach has been got and described in further chapters. Another group of algorithms and data structures is that one which employs hash-based technics. In theory, it could provide with O(1) searching speed. Number 1 here doesn’t mean exactly 1 but a constant number which represents the constant time of getting the requested value. This value can vary greatly depending on algorithm used and its parameters.

**NAT Translation Record Structure**

To store data about each address translation it is necessary to make the following record:

* source packet IP address [4 bytes] – IPv4
* source packet port number [2 bytes]
* IP address assigned by translation [4 bytes] – IPv4
* port number assigned by translation [2 bytes]
* translation timestamp – to calculate timeout [4 bytes]
* some additional service info (L4 protocol, flags) [4 bytes]

The total record size is 20 bytes. As it is needed to perform 2 translations for each connection it is necessary to save 2 records associated with that connection. So the total amount of data to save is 40 bytes per connection. This amount of data can be reduced. The memory reducing technic is described in the following chapters.

**NAT lookup data structures and algorithm choosing**

The following paragraphs show sequential improvement attempts and results achieved.

From now and further in this document the NAT translation lookup data structure is called a NAT table and the translation record is called NAT table entry. The NAT table and the NAT table entry structures and sizes can differ in further described experiments depending on underlying data structure used in each particular experiment.

**Tree-based NAT table**

The simplest data algorithm and data structure with O(logN) search time is a simple binary tree. (ADD SOME EXPLANATION ABOUT WHAT THE BINARY TREE IS AND HOW IT WORKS – IF NEEDED)

Its performance looks potentially promising but it consumes additional memory on tree node linking, in particular, each node uses 3 additional pointers to keep link with its parent node and 2 child nodes (left and right). Each of these links consumes at least 4 bytes of memory (12 in total) which leads to increasing of a NAT table entry size at least to 60%. So the overall memory overhead is more or equal than 60% depending on the CPU architecture and OS used.

The first test was made using two tree-based NAT table. The test results are shown in Figures 3.1 and 3.2

Figure 3.1 NAT performance. Binary tree based NAT table in cycles per packet

Figure 3.2 NAT performance. Binary tree based NAT table in packets per second

This approach has reviled poor performance. With NAT table size of 100 000 entries it spends more than 3.7M cycles/pkt which is ridiculously big number having in mind a target of 436 cycles/pkt. Most likely reasons of the poor performance are unbalanced tree structure and CPU massive cache misses.

Simple binary tree is known with its drawback of data sequence storing dependency. In the worst case, when the inserting values set sorted, the binary tree turns into a linked list. In this case the search time becomes to be equal to O(n) the same as linear search has. Although, this scenario is highly unlikely to happen in the real world it shows the main problem of the simple binary tree: it could be highly unbalanced which means that the depth of one branch can differ of the depth of the other branch in the order of magnitude. Thus, the real search time is somewhere between O(n) and O(logN) depending on data sequence.

Another drawback of binary tree is low spatial locality[ref\_locality]. This happens because of the binary tree node’s creation routine. The binary tree allows storing as many values as needed but, because of that, many memory allocations in different time frames are necessary. Because these allocated chunks of memory could be in the different parts of physical memory the CPU has to load each node in the memory separately instead of loading several of them at a time. As the NAT table size is much larger than a cache, even on a highly advanced CPU with a big cache, only some of the most frequently used nodes stays in the cache. All other nodes are constantly removed and stored again which means that the CPU spends a majority of time on data transferring from the main memory to the cache and vice versa.

To solve the last issue there another test was performed. Despite, it is impossible to guess the network to be processed with NAT in prior, the NAT output data range (IPs and ports) is always known because it is the main resource that NAT uses for packet translation. Hence, as a data structure for backwards NAT translation a one-dimensional array of structures can be used. To access its data the hash-based approach can be used: the destination IP and port can be used to make a key and this key is used to access the data in the array (hash table with open addressing). IP could be thought as a segment number and port could be thought as an offset inside the segment. Having used this simple technic, we can, first, get rid of the second binary tree saving some memory, second, make backwards packet translation cheap because of O(1) searching time. The result of the experiment is shown in Figure 4.

Figure 4.1 Nat Performance. Binary tree-based NAT table for outgoing packets and 1D array for incoming packets in cycles per second. Comparison of basic and red-black binary trees.

Figure 4.2 Nat Performance. Binary tree-based NAT table for outgoing packets and 1D array for incoming packets in packets per second. Comparison of basic and red-black binary trees.

The improvements made have given a remarkable performance increasing about 5700% on 100 000 nodes data set. From the chart it is clearly seen that although this result is quite good but has two serious flaws: The first one is that the performance is still below the desired level of 436 cycles and to fulfill that requirement it is necessary to speed up the lookup in 3.5 times. The second one is that the tree isn’t balanced which means that the search time for different nodes takes different time. To fix that flaw any balanced-tree data structure can be used, for example, a well-known and widely spread red-black tree[ref\_cormen]. The figure 4 shows the results of using red-black tree instead of regular binary tree. The performance improvement that gives red-black tree data structure is around 13% and still 3 times below the desired value.

The results of using tree-based data structures revealed the fact that these group of data structures cannot be used for achieving of the target level of performance. The maximum result they could provide is 3 times slower than needed. For further investigation of the performance more fast data structures should be taken into consideration.

**Hash-based NAT table**

The hash table is a data structure which provides the constant time O(1) of getting the value using a key. The key is produced with by a hash function. The hash function has a deterministic value for a given input.

Figure 5.1 Nat Performance. Hash-based NAT table for outgoing packets and 1D array for incoming packets in cycles per second

Figure 5.2 Nat Performance. Hash-based NAT table for outgoing packets and 1D array for incoming packets in packets per second.

The biggest issue while using a hash table is collisions arising which occur when the hash function produce the same result for any two or more inputs. There are several schemes of this problem resolving. The most frequently used is separate chaining with linked lists. It provides with good performance allowing to use simple (i.e. computationally cheap) hash functions.

For implementing the NAT table modulo division operation was used as the hash function. The NAT table capacity is set to store 1000 translation for each of 65536 nodes of the supported network. As in case of the binary tree exploration, the hash table is used for outgoing packets. For incoming packets the same 1-dimensional array is used. The hash table cell includes supplementary data which includes a link to a corresponding cell in the incoming array for accelerating of new translation creating time. The results of using the hash table are shown in Figure 5. There is a significant performance increasing in comparison with the tree-based NAT tables: it is 4 times faster. Because of the test system limitations it is not seen from the chart what the NAT performance is at the target level of connections number. Although, it is not shown in Figure 2, it is possible to estimate the full load performance, using the essence of the separate chaining linked list hash table and the results of linear search. The worst case scenario search time for this data structure is determined by the maximum length of the linked list associated with the cell calculated by hash function. Thus, changing the devisor value we could adjust the search time. But with changing the value the initial size of the hash table varies: than bigger the devisor that bigger its initial size. How to adjust these values properly is the question out of the scope of this document. The short estimations gave the value of 2^23 for the devisor which means the initial size of the hash table is around 67 Mb and the table maximum size is around 2.5 GB. In these settings the maximum list size is 512 elements and the translation data can be found in around 500 cycles (see Figure 2.). In the Figure 5 the value of 567 cycles is shown at 8M connections, which is very close to the numbers estimated.

This performance value is very close to target one, 37% more that needed, but still doesn’t achieve the desired value.

Further speed up can be gotten using parallelization of the translation process.

**Hash-based parallel NAT table**

All the results described previously in this document were gotten with 1 core at a multicore processor. Almost all modern CPUs offer several cores on a single chip. Thus, using several cores for NAT routine seems to be a promising idea.

When employing multicores technics for software developing there are several issues to aware of which make significant influence on performance speed up.

The first issue is the cache coherence which arises when using shared data structures. Because of a copy of current processing data is stored in a core’s cache, changing the data by one core leads to updating the data in all cores currently use it. This means that the data have to overwritten in some common place of memory and then once again reloaded by other cores. This process is expensive and could cost hundreds of cycles which leads to considerable performance degradation.

The second issue is keeping the data in consistent state which is closely related to using special data structures known as locks. A lock also could be a problem because it makes the cores get access to the data in a sequence manner which can lead to core idling, decreasing the degree of parallelization. In the worst case it can lead to the result when the multicore code works with the same (or even less) performance it single core version.

Trying to avoid these issues the following approach was used. The biggest degree of parallelization can be achieved in case when a process running on core is fully independent from other processes (i.e. isn’t used the shared data). In case of our system this is possible because modern network interface cards provides multiple queues which can be used by different cores in associated manner when a given queue is associated with one and only one core. In this case it can be seen as if a separate NAT process uses a core and a single network card and the amount of network cards installed in the system is more or equal to number of processors.

The approach described is simulated in the test system using ***pthread*** library. Each process shares the same generated packet set but the set is split into parts and this parts associated to each thread so that no process packets reads or writes interfere to other process packets reads or writes. Each thread is a separate NAT with fully independent data structures (i.e NAT tables) which eliminates all the drawbacks described in the previous paragraph but leads to memory overheads. As performance is the priority of this research the memory overhead issues were postponed to the future work.

Figure 6.1 Nat Performance. Parallel hash-based NAT table for outgoing packets and 1D array for incoming packets in cycles per second. Results for different number of simultaneously working cores.

Figure 6.2 Nat Performance. Parallel hash-based NAT table for outgoing packets and 1D array for incoming packets in packets per second. Results for different number of simultaneously working cores.

In figure 6 the results is shown for different number of cores. The experiments were set for 4 threads maximum because the testing system has 4 cores processor and setting experiment with more threads are meaningless because of the maximum number of simultaneously running cores is equal to number of cores available on the CPU chip and the OS scheduling issues, i.e. an operating system spends additional time on context switching and doesn’t give performance boost.

The result shows that in Figure 6 shows that the parallel approach gives the desired results: than more cores are available than grater performance improvement is. Adding of an additional core gives around 30% of performance boost.

The experiment wasn’t very clear because of using the hyper-threaded processor which in fact has only 2 physical cores while OS sees 4. A processor with fully-functional 4 physical cores can give better performance improvement.

**SUMMARY**

Using of parallel hash-tables gives the result which is greater than the target one. This approach is the will be used as a core for developing the NAT application. Further modifications and optimizations of the NAT table structure based on hash-table could be done to improve the currently achieved performance values by using more sophisticated data structures, for example cuckoo hashing, but this is the matter of further research.

**REFERENCES**

[ref\_TT\_ROS\_TEL] file:TT CGNAT 2014\_26\_06v1.doc

[ref\_rfc3022] Traditional IP address translator. https://www.ietf.org/rfc/rfc3022.txt

[ref\_RDP.RU] <http://rdp.ru/>

[ref\_rfc4787] Network Address Translation (NAT) Behavioral Requirements for Unicast UDP <https://tools.ietf.org/html/rfc4787#page-5>

[ref\_rfc5382] NAT Behavioral Requirements for TCP <https://tools.ietf.org/html/rfc5382>

[ref\_rfc5508] NAT Behavioral Requirements for ICMP https://tools.ietf.org/html/rfc5508

[ref\_rfc791] Internet protocol <https://www.ietf.org/rfc/rfc791.txt>

[ref\_rfc793] Transmission Control Protocol <https://www.ietf.org/rfc/rfc793.txt>

[ref\_rfc768] User Datagram Protocol <https://www.ietf.org/rfc/rfc768.txt>

[ref\_cormen] Introduction to algorithms, By [Thomas H. Cormen](http://mitpress.mit.edu/authors/thomas-h-cormen), [Charles E. Leiserson](http://mitpress.mit.edu/authors/charles-e-leiserson), [Ronald L. Rivest](http://mitpress.mit.edu/authors/ronald-l-rivest) and [Clifford Stein](http://mitpress.mit.edu/authors/clifford-stein) ISBN: 978026203384

[ref\_locality] <http://en.wikipedia.org/wiki/Locality_of_referencee>

[ref\_ripe\_limit] <https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion>

[ref\_frc6888] Common Requirements for Carrier-Grade NATs (CGNs) <http://www.rfc-base.org/txt/rfc-6888.txt>

[rfc\_3489] STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) <https://tools.ietf.org/html/rfc3489>

[ref\_nat32] NAT 32 IP Router <http://v2.nat32.com/index.html>

[ref\_cam]<http://www.digikey.com/product-detail/en/EP20K160EBC356-2X/EP20K160EBC356-2X-ND/4160824>

[ref\_wingate] http://www.wingate.com/purchase/wingate/purchase.php

**Appendix A**

**List of router models used for market research**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **brand** | **router model** | **Mpps** | **Price, USD** | **url** |
| hp | MSR2021 | 0.18 | 760 | http://www8.hp.com/ru/ru/products/networking-routers/product-detail.html?oid=5054094#!tab=specs |
| hp | MSR1002-4 | 0.50 | 1100 | http://www8.hp.com/us/en/products/networking-routers/product-detail.html?oid=6288749#!tab=specs |
| hp | MSR2003 | 1.00 | 1700 | http://www8.hp.com/ru/ru/products/networking-routers/product-detail.html?oid=5408900#!tab=specs |
| hp | MSR50-40 | 1.20 | 2500 | http://www8.hp.com/us/en/products/networking-routers/product-detail.html?oid=4199527#!tab=specs |
| hp | MSR3012 | 2.60 | 2700 | http://www8.hp.com/us/en/products/networking-routers/product-detail.html?oid=6288370&jumpid=reg\_r1002\_usen\_c-001\_title\_r0002#!tab=specs |
| hp | MSR3040 | 0.36 | 3200 | http://www8.hp.com/ru/ru/products/networking-routers/product-detail.html?oid=4199541#!tab=specs |
| hp | MSR4060 | 10.00 | 6000 | <http://www8.hp.com/us/en/products/networking-routers/product-detail.html?oid=5408896> |
| cisco | 7301 | 1.00 | 10000 | http://www.cisco.com/web/RU/products/hw/routers/ps352/ps4972/index.html |
| cisco | ASA5515-IPS-K9 | 0.50 | 4800 | http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_accessories/asa5515-ips-k9/ http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-a |
| cisco | ASA 5525-X | 0.70 | 5200 | <http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-b> |
| cisco | ASA 5545-X | 0.90 | 10200 | http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-b |
| cisco | ASA 5555-X | 1.00 | 17000 | <http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-b> |
| cisco | 5585-X SSP10 | 1.10 | 14200 | http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_firewall\_edition\_bundles/asa5585-s10-k9/ |
| cisco | 5585-X SSP20 | 2.00 | 40000 | http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_firewall\_edition\_bundles/asa5585-s20-k8/http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_firewall\_edition\_bundles/asa5585-s20-k8/ |
| cisco | 5585-X SSP40 | 4.00 | 80000 | [http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_firewall\_edition\_bundles/asa5585-s40-k8/](http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c ) |
| cisco | 5585-X SSP60 | 10.00 | 128300 | http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html#~tab-c http://ciscosales.ru/katalog\_produkcii/cisco/mezhsetevye\_ekrany\_i\_fil\_try/cisco\_asa\_5500\_series\_firewall\_edition\_bundles/asa5585-s60-2a-k9/ |
| juniper | SRX240 | 0.20 | 2000 | http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf http://www.srv-trade.ru/catalog/976735833/SRX240H/?gclid=CKXzk-\_4ysMCFYPUcgodBmUALQ |
| juniper | SRX550 | 0.70 | 7900 | http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf |
| juniper | SRX650 | 0.85 | 13000 | http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf |