

# Functioning of NAT in Computer Networks

**Ravjot Singh Syal**  
**Research fellow (M.Tech Student),**  
**SGGSWU Fatehgarh Sahib.**

**ABSTRACT-** In this paper the NAT has been implemented & visualized in computer networks. NAT stands for Network Address Translation & is widely used in all types of networks whether wired or wireless. NAT has widely acceptance through all over the world because of its technique of mapping private IP to a public IP address which helps to conserve the limit of IPv4 Addressing. In this Paper it is clearly shown how the NAT helps in communication of network from an ISP to various organizations & further to various computers under it.

**1. INTRODUCTION-** **Lixia Zhang** et al. described the original design of the Internet architecture, each IP address was defined to be globally unique and globally reachable. In contrast, a private IPv4 address is meaningful only within the scope of the local network behind a NAT and, as such, the same private address block can be reused in multiple local networks, as long as those networks do not directly talk to each other. Instead, they communicate with each other and with the rest of Internet through NAT boxes [1]. **Eddie Kohler, Robert Morris, Massimiliano Poletto et al.** represented a a general-purpose toolkit for network address translation in Click, a modular, component-based networking system. Network address translation, or NAT, was designed to allow disparate address realms to communicate. The components of our toolkit can be combined in a variety of ways to implement this task and many others, including some that, super\_cially, have nothing to do with address

translation [2]. **Daryl Johnson, Bruce Hartpence et al.** The use of Network Address Translation (NAT) has greatly expanded in recent years. While originally an address management technique it has often been used for security. However, there are many implementations of NAT that are inherently insecure. Recently investigation into some of these has shown increased potential for security holes in NAT deployments. An understanding of the risks associated with NAT and the basic networking topics supporting a research in this area are critical to an information assurance student [3]. **Sarabjeet Singh Chugh** et al. explained Network Address Translation (NAT) is a method by which Internet Protocol (IP) addresses are translated from one group to another, in a manner transparent to the end users. It translates the source and destination addresses and ports in the Internet Protocol datagram. There are several benefits for using NAT. NAT can be installed without changes to hosts or routers, it allows reuse of globally routable addresses, it facilitates easy migration or addition of new networks and it provides a method to keep private network addresses hidden from the outside world [4]. **Bryan Ford, Pyda Srisuresh** et al. stated that Network Address Translation (NAT) causes well-known difficulties for peer-to-peer (P2P) communication, since the peers involved may not be reachable at any globally valid IP address. Several NAT traversal techniques are

known, but their documentation is slim, and data about their robustness or relative merits is slimmer. This paper documents and analyzes one of the simplest but most robust and practical NAT traversal techniques, commonly known as “hole punching.” Hole punching is moderately well-understood for UDP communication, but we show how it can be reliably used to set up peer-to-peer TCP streams as well. After gathering data on the reliability

of this technique on a wide variety of deployed NATs, we find that about 82% of the NATs tested support hole punching for UDP, and about 64% support hole punching for TCP streams. As NAT vendors become increasingly conscious of the needs of important P2P applications such as Voice over IP and online gaming protocols, support for hole punching is likely to increase in the future. [5]. **SHIUH-PYNG SHIEH, FU-SHEN HO, YU-LUN HUANG, JIA-NING LUO** et al. proposed method for mitigating the address shortage problem in IPv4 is to use network address translators (NATs) to allow address reuse. The basic idea is to transparently map a wide set of private network addresses and corresponding TCP/UDP ports to a small set of globally unique public network addresses and ports. NAT devices provide a way to handle IP address depletion incrementally—without changing hosts and routers—until more long-term approaches like IPv6 can be implemented. Existing Internet security protocols must be re-examined, however, to see how they function within this new network environment [6]. **Ailin Zeng** et al. analyzed computer network security is to integrate resources related to computer network

technology and security system to build a computer network security model. This article start with the current situation of security of computer network and analyze the influential elements of computer network security and security property of computer network to provide references for security property of computer network model [7]. **Anupriya Shrivastava, M A Rizvi** et al. stated Network Security issues are now becoming important as society is moving to digital information age. Data security is the utmost critical component in ensuring safe transmission of information through the internet. It comprises authorization of access to information in a network, controlled by the network administrator. The task of Network security not only requires ensuring the security of end systems but of the entire network. Authentication is one of the primary and most commonly ways of ascertaining and ensuring security in the network. In this paper, an attempt has been made to analyze the various authentication techniques such as Knowledge-based, Token-based and Biometric-based etc. Furthermore, we consider multi-factor authentications by choosing a combination of above techniques and try to compare them [8]. **S. Gopalakrishnan** et al. described Wireless networking is inherently insecure. From jamming to eavesdropping, from man-in-the-middle to spoofing, there are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. However, much of the commonly used security precautions are woefully inadequate [9]. **Jun Bi, Miao Zhang, and Lei**

**Zhao et al.** stated that Detecting network address translation is helpful for network administrators to enhance the network security. Current network address translation detection approaches cannot work effectively in all scenarios. In this paper, a new detection scheme ImNatDet utilizing instant messaging information is presented, a case study based on characters of MSN Messenger is analyzed, and related security issues are discussed. This paper also indicates that characters of instant messaging applications can be used to detect users' privacy information [10]. **Pawan Kr. Chaurasia et al.** underlined how internet users are increased in exponential form. It is very difficult to secure data when two users want to communicate through Internet. When we share information and resources among various users on internet, then networking is required to implement. Today hacking is the major problem with internet user. When user shared information or data then they share the IP address also between two users. It is mandatory to provide strong security on IPV4 address to secure data in the form of XXX.YYY.ZZZ.RRR. IP addresses are binary numbers, which are usually stored in text files. IP address is classified into various classes. IP address is secured on IPV4. A class model is proposed to secured data on internet through IP address. Through RSA algorithm, it is tested and verified, IP address on sender end and receiver end are same during the share of information between two users [11]. **Bhavya Daya et al.** showed Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of

security technology. The internet structure itself allowed for many security threats to occur [12]. **Yinglian Xie, Fang Yu, Kannan Achan Eliot Gillum, Moises Goldszmidt, Ted Wobber** introduced addresses and analyze their dynamics pattern. UDmap is fully automatic, and relies only on application-level server logs that are already available today. We applied UDmap to a month-long Hotmail user-login trace and identified a significant number of dynamic IP addresses – more than 102 million. This suggests that the portion of dynamic IP addresses in the Internet is by no means negligible. In addition, using this information combined with a three-month Hotmail email server log, we were able to establish that 97% of mail servers setup on dynamic IP addresses sent out solely spam emails, likely controlled by zombies [13]. **Jie Shan et al.** investigated the rapid development of computer technology, computer network continues to expand the scope of application with more and more users. Network security gradually attracts people's attention. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security and discusses basic techniques. It proposes effective measures to improve the computer network security [14]. **Sumedha Kaushik, Ankur Singhal et al.** elaborated that Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management



```

Command Prompt
Packet Tracer PC Command Line 1.0
PC>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification
Password:
oxg2#en
Password:
Password:
oxg2#

```

Figure 4: Telnet Protocol

It shows the telnet service that is being used with which a router configuration can be accessed from the remote machine which can be anywhere inside a network & this is a most powerful protocol of a computer network.

**4. Conclusion-** It is concluded that the NAT is the future of the computer networks where we can conserve the IP range of IPv4 addressing. In today's world where we have networks everywhere so implementing NAT inside the Network will help the various organizations as well as the ISP to communicate. Various factors like security, data traffic management, path determination, message delivery etc. can be managed when the NAT will be used along with the routing protocols in the computer network & that will not only increase the efficiency of network but also will make it a robust network.

## References

1. Lixia Zhang, "A Retrospective View of Network Address Translation" IEEE Network September/October 2008, February 9, 2009.
2. Eddie Kohler, Robert Morris, Massimiliano Poletto, "Modular Components for Network Address Translation".
3. Daryl Johnson, Bruce Hartpence, "A Re-examination of network address translation security", Rochester Institute of Technology, RIT Scholar Works 2010.
4. Sarabjeet Singh Chugh, "Impact of Network Address Translation on Router Performance" Thesis for the degree of Master of Science in Electrical Engineering ,2003.
5. Bryan Ford, Pyda Srisuresh, "Peer-to-Peer Communication Across Network Address Translators".
6. SHIUH-PYNG SHIEH, FU-SHEN HO, YU-LUN HUANG AND JIA-NING LUO, "Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP Stack, National Chiao Tung University, Taiwan, and December 2000.
7. Ailin Zeng, "Discussion and research of computer network security", Journal of Chemical and Pharmaceutical Research, 2014, 6(7):780-783, ISSN: 0975-7384 CODEN (USA): JCPRC5.
8. Anupriya Shrivastava, M A Rizvi, "Network Security Analysis Based on Authentication Techniques", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 6, June 2014, pg.11 – 18, ISSN 2320–088X.
9. S. Gopalakrishnan, "A SURVEY OF WIRELESS NETWORK SECURITY", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 1, January 2014, pg.53 – 68, ISSN 2320–088X.
10. Jun Bi, Miao Zhang, and Lei Zhao, "Security Enhancement by Detecting Network Address Translation based on Instant Messaging" Network Research Center Tsinghua University.

11. Pawan Kr. Chaurasia, “International Journal of Advanced Research in Computer Science and Software Engineering”, Volume 4, Issue 5, May 2014 ISSN: 2277 128X.
12. Bhavya Daya, “Network Security: History, Importance, and Future”, University of Florida Department of Electrical and Computer Engineering.
13. Yinglian Xie, Fang Yu, Kannan Achan ,Eliot Gillum, Moises Goldszmidt, Ted Wobber, “How Dynamic are IP Addresses?” Microsoft Research, Silicon Valley, Microsoft Corporation.
14. Jie Shan, “Analysis and research of computer network security”, Journal of Chemical and Pharmaceutical Research, 2014, 6(7):874-877”, ISSN: 0975-7384, CODEN (USA): JCPRC5.
15. Sumedha Kaushik, Ankur Singhal, “International Journal of Advanced Research in Computer Science and Software Engineering” Volume 2, Issue 12, December 2012 ISSN: 2277 128X.