A Vulnerability of Dynamic Network Address Translation to Denial-of-Service Attacks

Shigeo Akashi*
Yao Tong*
akashi@is.noda.tus.ac.jp
6320519@ed.tus.ac.jp
Department of Informaiton Sciences, Faculty of Science and Technology,
Tokyo University of Science
Noda City, Chiba Prefecture, JAPAM

ABSTRACT

It is well known that Network Address Translation plays not only an important role as the soltion to the IPv4 Depletion problem but also another important one as the enhancement of network security. Actually, it sometimes happens that some newly born network skills are not always compatible with other ready-constructed network ones.

In this paper, we point out that the simulutaneous use of network routing and Network Address Translation may bring about an unexpected network traffic congestion. Exactly speaking. in the former half of this paper, we point out the fact that, if we apply dynamic routing together with static one simultaneously, another type of network traffic congestion, which resembles what is brought about by the routing loop, may happen spontaneously, and in the latter half of this paper, we discuss the problem asking if this network traffic congestion can be brought about not only spontaneously but also intentionally for preventing malicious cyber attackers from using this phenomenon intentionally.

CCS CONCEPTS

• **Computer systems organization** → **Network security**; • **Networks** → **Network types**; *Network reliability*; • **Social and professional topics**;

KEYWORDS

Denial of service attacks, Packet oscillation, Inside static network address translation, Inside dynamic network address translation, Inside local IP address, Inside global IP address, Outside global IP address

ACM Reference Format:
Shigeo Akashi and Yao Tong. 2021. A Vulnerability of Dynamic Network Address Translation to Denial-of-Service Attacks. In *2021 4th International Conference on Data Science and Information Technology (DSIT 2021), July 23–25, 2021, Shanghai, China.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3478905.3478950

*Both authors contributed equally to this research.

DSIT 2021, July 23–25, 2021, Shanghai, China

ACM ISBN 978-1-4503-9024-8/21/07…$15.00
https://doi.org/10.1145/3478905.3478950

1 INTRODUCTION

The modern dynamic routing protocols such as OSPF, EIGRP and RIP have been succeeding in protecting our network infrastructures from traffic congestions which are brought about by routing loops. Actually, it sometimes happens that the network traffic has been suspended by a large number of packets streaming upward and downward simultaneously on the links connecting between the Internet and the gateway routers being in charge of autonomous systems. Though many network administrators are apt to regard these network traffic congestions as spontaneous ones which are brought about by the shortage of the allocated bandwidths, we cannot always confirm that all the network traffic congestions are brought about spontaneously. In other words, it may be possible that some of network traffic congestions are brought about intentionally.

In the first part of this paper, we introduce classification of cyber attacks from the various kinds of network theoretic viewpoints. It is well known that there are two ways of developing new malicious network skills which can be applied to committing new cybercrimes, one of which is finding security halls already existing in the modern network and the other of which is combining network skills with other ones to produce new hybrid cyber attacks. Therefore, it seems to be important that we clarify mutual relations among several cyber attacks and we specify the network skills which have been abused for committing these attacks. The authors confide that such classification leads us to the systematization of the cyber attacks and the specification of network skills can contribute to preventing authenticated network users from potential cyber attacks before they happen, In the second part of this paper, we introduce the fact that there exist the phenomena that some packets can commute spontaneously on a bottlenecked link between one end and the other one, until their TTLs expire, These phenomena can be called packet oscillations, and in the third part of this paper, we discuss the problem asking if the modern dynamic routing protocols can prevent these packet oscillations. Since it is well known that almost all cyber attacks can be classified into two cases, namely the case consisting of the attacks realized from remote network segments and the case consisting of the attacks realized from local network segments, and it is also well known that the former case is more difficult than the latter one to be realized. In final part of this paper, we discuss some relations between static NAT and dynamic NAT.

Throughout this paper, all the simulation models are implemented with Cisco Packet Tracer to which we can refer to [1].

2 CLASSIFICATION OF NETWORK ADDRESS TRANSLATION

Network address translation, which is abbreviated to NAT, is defined as a method of constructing mappings on a set of local IP addresses into a set of global IP addresses. According to the difference between the mappings being one-to-one correspondencees and the mappings being many-to-one correspondences, they are called basic NAT and Network Address Port Translation, respectively, While both translations, with which network routing devices are equipped, are implemented, these devices such as routers and L3-switches continue to exchange the local IP addresses assigned for the packets being forwarded across these devices for the corresponding global IP addresses. Exactly speaking, the roles being play by NAT can be summerized as the following:

Role 1. Solution to the IPv4 depletion problem,
Role 2. Concealing the IPv4 addresses.

As stated above, the roles being played by NAT have very useful effects on the packet transmission over the Internet in varous ways. Concretely speaking, while Role 1 contributes to the IPv4 Depletion Problem, Role 2 contributes to enhancing the network security. In the sequel, it is shown that Role 2 is not compatible with solutions to the Network Traffic Congestion Problem.

3 RELATIONS OF ICMP PACKET TRANSMISSION TO INSIDE NAT

The problem asking wheter or not mutual communications between two network devices hold successfully should be discussed carefully, because we have to discuss the problem deciding which of two become the packet sender or the packet receiver. For example, om case of the bidirectional ICMP packet transmission between two network devices being directly connected to each other, we have to assign each of two roles, namely the ICMP echo-request packet sender and the ICMP echo-reply packet sender, to each of these network devices.

In this section, we show that whether the bidirectional communications hold or not changes according to the way of choosing which NAT is used, inside static NAT or inside dynamic one. If we apply inside static NAT, the results of bidirectonal packet trnsmission can be summarized as the following:

Table 1: Application of inside static NAT

Direction of ICMP packets	Echo-request	Echo-reply
Inside local → Outside global	Success	-
Outside global → Inside local	-	Success
Outside global → Inside global	Success	-
Inside global → Outside global	-	Success
Outside global → Inside local	Failure	-
Inside local → Outside global	-	-

If we apply inside dynamic NAT, the results of bidirectonal packet trnsmission can be summarized as the following:

Table 2: Application of inside dynamic NAT

Direction of ICMP packets	Echo-request	Echo-reply
Inside local → Outside global	Success	-
Outside global → Inside local	-	Success
Outside global → Inside global	Failure	-
Inside global → Outside global	-	-
Outside global → Inside local	Failure	-
Inside local → Outside global	-	-

As for some other types of dynamic routing falsifidcation, we can refer to [5–7] and [8].

4 DIFFERENCE BETWEEN ROOTING LOOPS AND PACKET OSCILLATIONS

The modern dynamic routing protoclos are constructed so as to prevent such abnormal packet streamings as routing loops and packet oscillation. In this section is based on both the summary of the cyber troubles and the mathematical aspects of the network traffic flows, which have been used for the realization of cybercrimes. As for the former part, we can refer to [2] and [3], and as for the latter part, as we can refer to the famous textbook [4].

In this section, we illustrate the topological difference between the routing loops and packet oscillations. presented by two figures, namely the figure showing the flow of packets streaming around clockwise on the loop composed of three routers collored with the red arrow and the figure showing the flow of packets commuting between the both ends of the link located on the left-hand side colored with two black arrows. Two examples of the routing loop amd that of the packet oscillation can be illustrated respectiveluy, as the following:

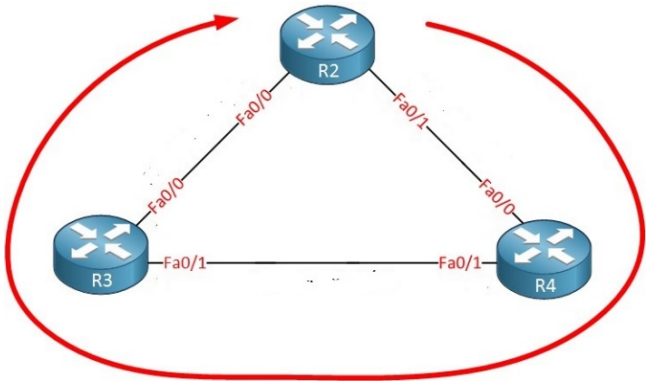

Figure 1: An 0rbit designed with routing loops :.

5 SERVER TARGETING DOS ATTACKS AND BOTTLENECKED LINK TARGETING DOS ATTACKS

Till the previous sections, it is assumed that the cyber attackers executing DoS attacks target servers or PCs. In this section, we discuss the problem asking if there is another cyber attacks which can

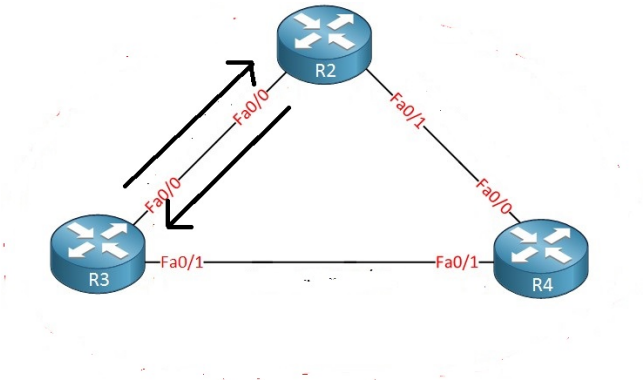

Figure 2: An 0rbit designed with packet oscillations :.

bring about the network traffic congestions in the way of targeting any other network devices than PCs and servers. Exactly speaking, intentional network traffic congestions can be classified according to a difference in the destinations which the cyber attackers target. Here, we assume that the topological relations among the cyber attackers, the servers suffering from attacks and the Internet are illustrated as the following:

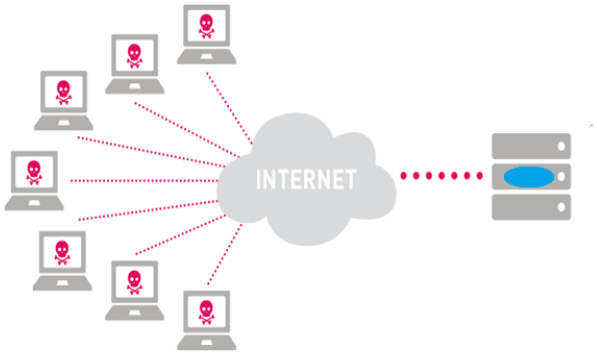

Figure 3: Server targeting DoS attacks.

In Figure 3, it is shown that the seven cyber attackers give offence to one of three servers. Though only one server, which is encircled in blue, suffers from network traffic congestion happening on the interface of this server, the other two servers can continue to offer their service through the Internet.

On the contrary, in Figure 4, it is shown that the seven cyber attackers give offence to the bottlenecked link, which is encircled in green, connecting between the group of all three servers and the Internet. Therefore, the network segment in which all three servers exist has been isolated from the Internet, and eventually, none of these servers can continue to offer their service to the clients through the Internet.

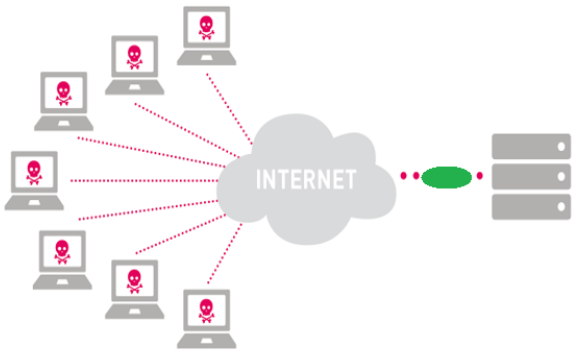

Figure 4: Bottlenecked link targeting DoS attacks.

6 AN EXAMPLE OF THE SIMPLEST ARTIFICIAL PACKET OSCILLATION

In this section, we show that the network traffic congestions which are brought about with routing loops and those which are brought about with packet oscillations are different from each other if we apply simultaneously combined use of dynamic routing with static one to network construction.

For example, the links connecting default gateways and the entrances into the internet service providers must be configured with static routing, and all the network segments located behind the default gateways must be configured with dynamic routing. This configuration necessarily requires all the network administrators to the use the dynamic routing protocols combined with static routing protocols simultaneously.

Though it is hardly possible to construct network segments on which packets commute on condition that the networks are constructed with dynamic routing protocols only, the simultaneously combined use of dynamic routing with static one brings about the packet oscillations as stated below. The simplest network structure on which intentional packet oscillations may happen is illustrated as the following:

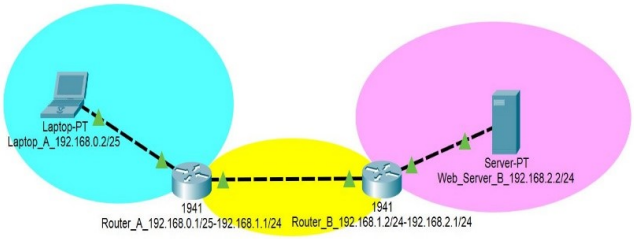

Figure 5: The simplest artificial packet oscillation.

In Figure 5, it is illustrated that Laptop-A with its IP address 192.168.0.2/24, which is located on the left-hand side and encircled in blue, visits Web-Server-B with its IP address 192.168.2.2/24, which is located on the right-hand side and encircled in red, through the

network segment with its network address 192.168.1.0/24, which is located in the central part and encircled in yellow, Exactly speaking, the network structure composed of the four network devices are configured as the following:

- Router-A is designated as the default gateway for Laptop-A and is configured with the default-route forwarding any other packets than what belongs to 192.168.2.0/24.
- Router-B is designated as the default gateway for Web-Server-B and is configured with the static route forwarding all packets which is bound for the destinations belongs to 192.168.0.0/24.

Under the assumptions as stated above, the routing path for the ICMP packets originating in Web-Server-B, which are bound for Laptop-A, can be recorded as the following:

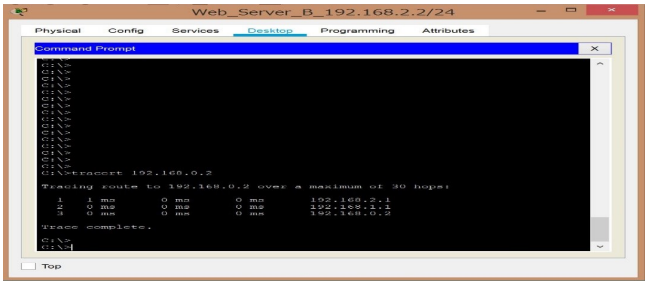

Figure 6: Normal ICMP packet transmission.

Here, when we send some other ICMP packets which are bound for a non-existing PC for which 192.168.0.129 is assumed to be assigned, we can obtain the following:

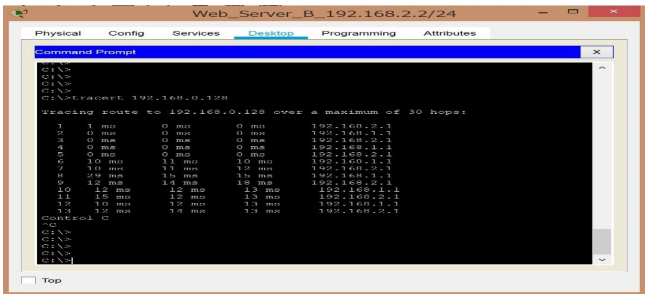

Figure 7: Sending ICMP packets bound for a non-existing network.

In Figure 7, we can see the packet oscillation in the form of endless commutation between the gateway router of Laptop-A and that of Web-Server-B. The reason why such a phenomenon has happened can be clarified by the following:

- Step 1. Web-Server-B sends an ICMP packet whose final destination IP address is 192.168.0.129 to Router-B.
- Step 2. Router-B forwards the ICMP packets to Router-A, because the routing table of Router-B confirms that 192.168.0.129 belongs to 192.168.0.0/24.
- Step 3. After the ICMP packets has reached Router-A, this router tries to compare 192.168.0.129 with its network addresses which have been regitered with its routing table and finds that 192.168.0.129 belongs to neither 192.168.0.0/25 nor 192.168.1.0/24.
- Step 4. According to the default route configured in the routing table of Router-A, the ICMP packet whose final destination IP address is 192.168.0.129 is forwarded back to Router-B. Therefore, the ICMP packet results in getting back to Router-B again, and eventually, this ICMP packet commutes between Router-A and Router-B, until the Time-To-Live assigned for the packet expires. .

If Web-Server-B sends another ICMP packet whose final destination IP address is 192.168.0.126 to Router-B, then another phenomenon which is different from what has happened as stated above. Since there does not exist any PC for which 192.168.0.126 is assigned, the ICMP packet cannot reach anywhere. But the routing path for the ICMP packet whose destination IP address is 192.168.0.129 is different from that for the ICMP packet whose destination IP address is 192.168,0.127, which can be seen as the following:

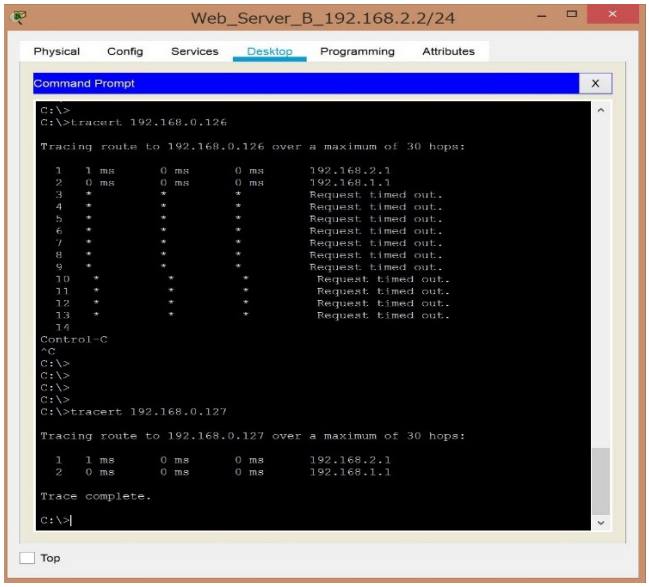

Figure 8: Sending ICMP packet bound for an non-existing PC.

The comparison of Figure 7 with Figure 8 clarifies that the difference between the routing path followed by a packet whose destination IP address is neither assigned for any PC nor contained in any network address, and the routing path followed by a packet whose destination IP address is not assigned for any PC but included in a certain network address. More exactly speaking, while Figure 7 proves that there does not exist the network segment for which 192.168.0.128/25 is assigned, Figure 8 proves that there exists the network segment for which 192.168.0.0/25 is assigned, and the response shown in Figure 8 informing of the success in sending the ICMP packet whose destination IP address is 192.168.1.127 proves that this IP address is the broadcast one of 192.168.0.0/25. These results tell us that the difference enables cyber attackers located on remote network segments to investigate the correspondence between the

network segments and the network addresses for which these segments are assigned from outside beyond the gateway routers. As for the protection against Distributed DoS attacks, we can refer to [9] and [10].

7 INTENTIONAL PACKET OSCILLATION UNDER THE NETWORKS EQUIPPED WITH NAT

In this section, we discuss the problem asking if the packet oscillations can be brought about on the bottlenecked links which are equipped with NAT, because almost all modern internet service providers connect themselves to the gateway routers of their clients' networks which are equipped with NAT. Since it is a matter of course that the bidirectional ICMP packet transmissions originating in the PCs located in the inside network segments, we restrict application of NAT to the inside one, and moreover, we restrict the bidirectional ICMP packet transmissions to those which are originating in the servers located in the outside network segments. As for the case of inside static NAT, the results can be summarized as the following:

Table 3: Application of inside static NAT

Direction of ICMP packets	Echo-request	Echo-reply
Outside global address → Inside global address in use	Success	-
Inside global address in use → Outside global address	-	Success
Outside global address → Inside global address not in use	Failure	-
Inside global address not in use → Outside global address	-	Packet oscillation

As for the case of inside dynamic NAT, the results can be summarized as the following:

Table 4: Application of inside dynamic NAT

Direction of ICMP packets	Echo-request	Echo-reply
Outside global address → Inside global address in use	Success	-
Inside global address in use → Outside global address	-	Pacet oscillation
Outside global address → Inside global address not in use	Failure	-
Inside global address not in use → Outside global address	-	Packet oscillation

The comparison of the former table with the latter one shows that the difference of inside static NAT from inside dynamic NAT. As for some relations betweenDDos attacks and NAT, we can refer to [11].

8 CONCLUSIONS

While the packets whose destionations addresses have been registered with the router in the way of static NAT can be forwarded into the inside networks from outside, the packets whose destination addresses have been registered with the router in the way of dynamic NAT cannot only be forwarded into the inside networks but send back to another router bring about packet oscillation.

REFERENCES

[1] Cisco Networking Academy. 2019. Cisco Packet Tracer: Network Simulation Tool built by Cisco, version 8.0.1. https://www.netacad.com/ja/courses/packet-tracer

[2] O. Santos and J. Muniz. 2017. CCNA Cyber Ops Secfnd 210-250 (1st ed.). Cisco Press. Indianapolis.

[3] O. Santos and J. Muniz. 2017. CCNA Cyber Ops Secops 210-255 (1st ed.). Cisco Press. Indianapolis.

[4] Donald E. Knuth. 1997. The Art of Computer Programming, Vol. 1: Fundamental Algorithms (3rd. ed.). Addison Wesley Longman Publishing Co., Inc.

[5] S. Akashi and Y. Tong. 2019. Classification of DHCP Spoofing and Effectiveness of DHCP Snooping. In Proceedings on 2018 International Conference on Advances in Computer Technology, Information Science and Communication. 233-238. ISBN:978-989-758-357-5

[6] S. Akashi and Y. Tong. 2019. A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping: To what extent can DHCP snooping protect clients from the cyberattack based on DHCP spoofing. DSIT 2019: Proceedings of the 2019 2nd International Conference on Data Science and Information TechnologyJuly 2019, pp 267–272. https://doi.org/10.1145/3352411.3356103

[7] S. Akashi and Y. Tong. 2020. Numerical Estimation of Network Traffic Failure Based on Probabilistic Approximation Methods: To what extent the network traffic failure can be predicted? CCRIS 2020: 2020 International Conference on Control, Robotics and Intelligent SystemOctober 2020, pp 213–217. https://doi.org/10.1145/3437802.3437838

[8] S. Akashi and Y. Tong. 2019. E-mail spoofing based on the datalink layers and its application to e-mail aggregation systems: is it possible to make good use of e-mail spoofing? AISS '19: Proceedings of the International Conference on Advanced Information Science and SystemNovember 2019, Article No.: 26, pp 1–5. https://doi.org/10.1145/3373477.3373503

[9] G. Loukas, G. Oke. 2010. Protection Against Denial of Service Attacks: A Survey. Comput. J. 53, 7(2010), 1020–1037. doi:10.1093/comjnl/bxp078

[10] Y. Chen; K. Hwang, Y-K Kwok. 2005. Filtering of shrew DDoS attacks in frequency domain. The IEEE Conference on Local Computer Networks 30th Anniversary. Lecture Notes in Computer Science, Vol. 70. Springer-Verlag, Berlin. 8-8. doi:10.1109/LCN.2005.70. ISBN 978-0-7695-2421-4

[11] U. Ben-Porat, A. Bremler-Barr and H. Levy. 2013. Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. IEEE Transactions on Computers. Vol. 62. 5(2013). 1031-1043. doi:10.1109/TC.2012.49, ISSN 0018-9340