Akashi et al., Int J Comput Softw Eng 2023, 8: 185
https://doi.org/10.15344/2456-4451/2023/185

International Journal of
Computer & Software Engineering

Research Article Open Access

On Compound Attacks Composed of Man-in-the-middle Attacks and Smurf Spoofing

Yao Tong and Shigeo Akashi*

Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan

Abstract

Nowadays there are various kinds of cyber attacks threatening the Internet and there has never been such an age when every cyber incident response team is making effort in developing countermeasures against cyber attacks. Actually, almost all cyber incident response teams develop each countermeasure against each cyber attack on case-by-case basis.

In this paper, if we take smurf attacks and man-in-the-iddle attacks as an example of two cyber attacks which are different from each other, then a simultaneous use of them happens to have a maliciously synergistic effect on the networking system which cannot be prevented by DHCP snooping.

Publication History:

Received: April 27, 2023
Accepted: May 08, 2023
Published: May 10, 2023

Keywords:

Smurf spoofing, Man-in-the-middle attack, DHCP spoofing, DHCP snooping

Introduction

Nowadays there are various kinds of cyber attacks threatening the Internet and there has never been such an age when the Internet plays so important roles as today. Unfortunately, the more skillful and sophisticated the contemporary network skills are, the more vulnerable both the wide and the local area networks are to the cyber attacks. Exactly speaking, as for the vulnerability accompanying the contemporary network skills, they can be classified into the following two cases:

- Inevitable vulnerability: The vulnerability accompanying network skils which cannot be removed from the contemporary network skills, because we have some adverse side effects on the Internet unless the network skills are used.
- Non-inevitable vulnerability: The vulnerability which can be removed from the contemporary network skills without causing any other side-effects on the Internet.

It is a matter of courese that the cyber attacks based on the inevitable vulnerability is more dangerous than the cyber attacks based on the non-inebvitable one. Moreover, as for the distance between the cyber attackers and the victims, they can be clssified into the following two cases:

- Remote attacks: The attack which is made possible by the cyber attackers who are far from the victimes.
- Local attacks: The attack which is made possible by the cyber attackers who are near the victimes.

It is a matter of course that the cyber attacks originating in remote area where the cyber attackers exist is more difficult than the cyber attacks originating in local area where the victims exist [1]. There are some other network theoretic points of view which can be regarded as criteria which can indicate how dangerous and malicious cyber attacks are. If we apply these two classifications to smurf spoofing and man-in-the-middle attack, then we can represent a maliciously synergistic effect as the following:

cyber attacks	remote or local	inevitable or non-inevitable
smurf spoofings only	remote	non-inevitable
man-in-the-middle attacks only	remote	non-inevitable
simultaneous use of smurf spoofings and man-in-the-middle attacks	remote	inevitable

Table 1: Smurf attacks and man-in-the-middle attacks cyber.

In this paper, we discuss smurf spoofings and man-in-the-middle attacks as examples of two cyber attacks which are different from each other, and clarify a malicously synergistic effect on the Internet, which is brought about by a simultaneous use of them.

Network Topology Where Man-in-the-middle Attack Happens

In this section, we show an example illustrating smurf spoofings and man-in-the-middle attacks which can be deployed in the following network:

In the above figure, we can find two network areas encircled in blue and in red, respectively. These two network areas are connected to each other by way of Switch-boundary. A DHCP client which is named as DHCP-client-laptop-192.168.0.1, is located in the right-hand side of the blue-colored network area, while a DHCP server combining a gateway router with a DHCP server simultaneously and being named as DHCP-authenticated-router-192.168.0.254, is alocated in the left-hand side of the blue-colored network area. Moreover, two routers

***Corresponding Author:** Prof. Shigeo Akashi, Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan, E-mail: akashi@is.noda.tus.ac.jp

Citation: Tong Y, Akashi S (2023) On Compound Attacks Composed of Man-in-the-middle Attacks and Smurf Spoofing. Int J Comput Softw Eng 8: 185. doi: https://doi.org/10.15344/2456-4451/2023/185

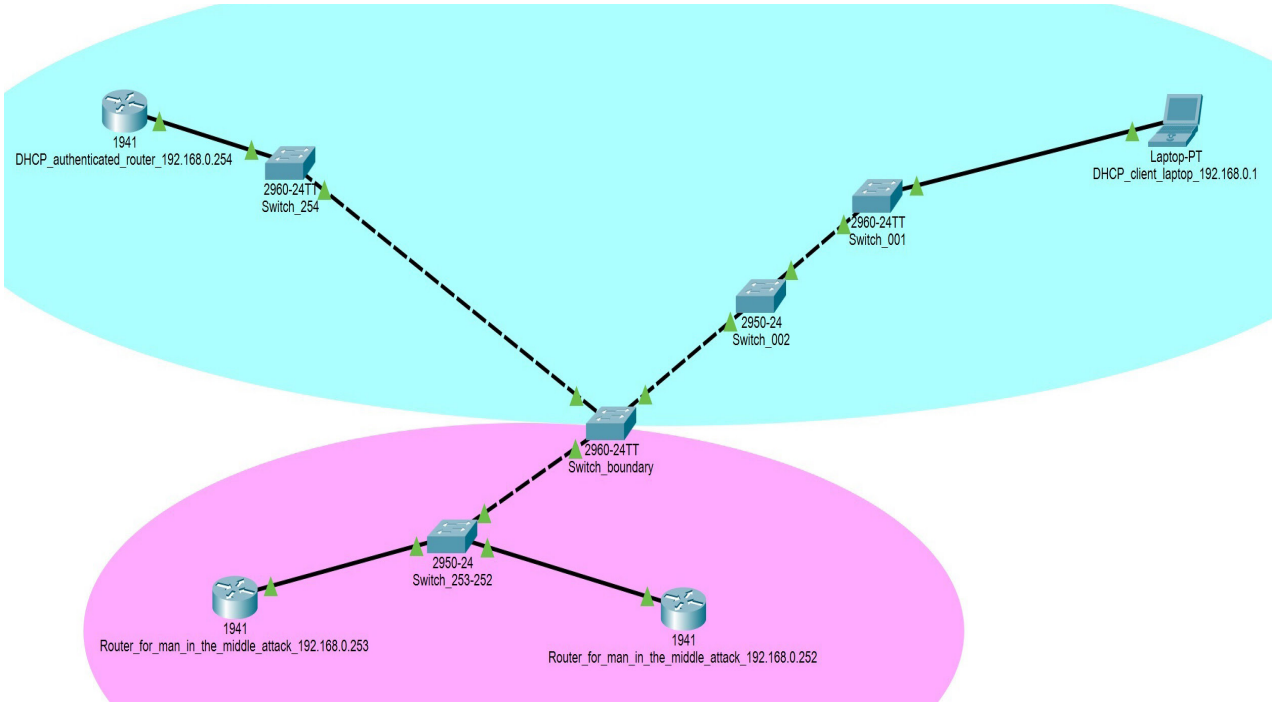

Figure 1: The simplest structure for deploying smurf spoofings and man-in-the-middle attacks.

following the procedure for the man-in-the-middle attacks and being named as Router-for-man-in-the-middle-attack-192.168.0.253 and Router-for-manin- the-middle-attack-192.168.0.252, respectively, are located in the left-hand side and the right-hand side of the pink-colored network area.

Proposed Solution

In figure 1, we can find two network areas encircled in blue and in red, respectively. These two network areas are connected to each other by way of Switch-boundary. A DHCP client which is named as DHCP-client-laptop-192.168.0.1, is located in the right-hand side of the blue-colored network area, while a DHCP server combining a gateway router with a DHCP server simultaneously and being named as DHCP-authenticated-router-192.168.0.254, is alocated in the left-hand side of the blue-colored network area. Moreover, two routers following the procedure for the man-in-the-middle attacks and being named as Router-for-man-in-the-middle-attack-192.168.0.253 and Router-for-manin-the-middle-attack-192.168.0.252,respectively, are located in the left-hand side and the right-hand side of the pink-colored network area [2].

Throughout this paper, since the role of attacking on the blue-colored netowrk, which Routerfor-man-in-the-middle-attack-192.168.0.252 plays is almost the same as Router-for-man-in-the-middleattack-192.168.0.253 does, we discuss the cyber attacks played by Router-for-man-in-the-middle-attack-192.168.0.253 only.

Under the above network circumstances, the IP address of the interface of DHCP-client-laptop-192.168.0.1 is assumed to be assigned by DHCP-authenticated-router-192.168.0.254. Since DHCP transactions commuting betwen DHCP-client-laptop-192.168.0.1 and DHCP-authenticated-router-192.168.0.254 must pass through Switch-boundary, two cyber attackers, namely Router-for-man-in-the-middle-attack-192.168.0.253 and Router-for-man-in-the-middle-attack-192.168.0.252, is also assumed to connect themselves to Switch-boundary, and the distance bwtween DHCP-authenticated-router-192.168.0.254 and DHCP-client-laptop-192.168.0.1 can be characterized by the total number of the switches existing on the shortest route connecting between them and is equal to four. Moreover, the distance between DHCPauthenticated- router-192.168.0.254 and Router-for-man-in-the-middle-attack-192.168.0.253, which is exactly equal to the distance between DHCP-authenticated-router-192.168.0.254 and Router-for-manin- the-middle-attack-192.168.0.252, can be characterized by the total number of the switches existing on the shortest route connecting between them and is equal to three. Under the above network circumstances, the interface of DHCP-authenticated-router-192.168.0.254 and the interface of Routerfor-man-in-the-middle-attack-192.168.0.253 are configured as figure 2:

The figure 2 shows that both the IP address and the MAC address which are assigned for the interface of DHCP-authenticated-router-192.168.0.254 is 192.168.0.254 and 0005.5ec7.3e01, respectively.

The above figure shows that both the IP address and the MAC address which are assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 is 192.168.0.253 and 00d0.58a1.0001, respectively.

While the attacker is allowed to share neither IP address nor MAC address which has already assigned for the interfaces of some other authenticated routers, the IP address which is assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 can be changed intentionally from 192.168.0.253 to 192.168.0.254 for a very short period of time, even though the MAC address which is assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253 can never be changed anytime [3].

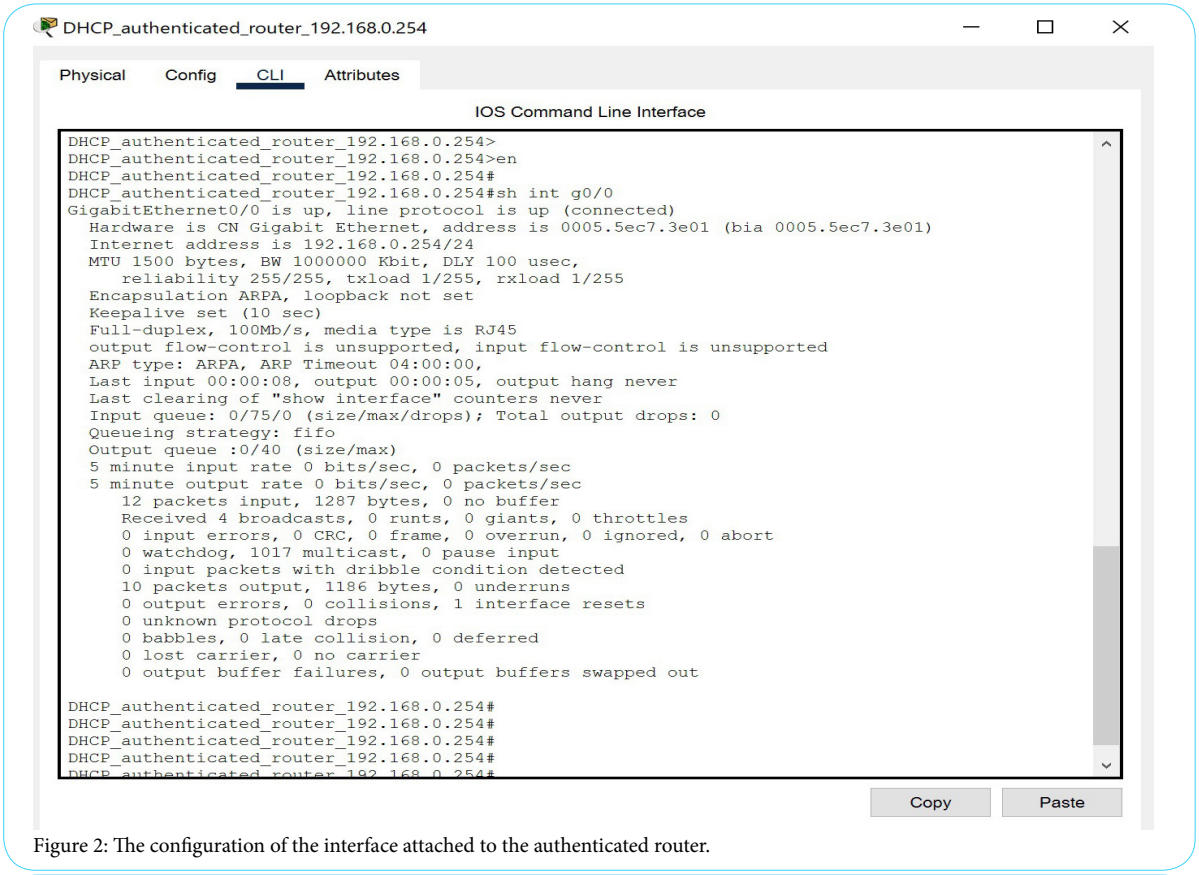

Figure 2: The configuration of the interface attached to the authenticated router.

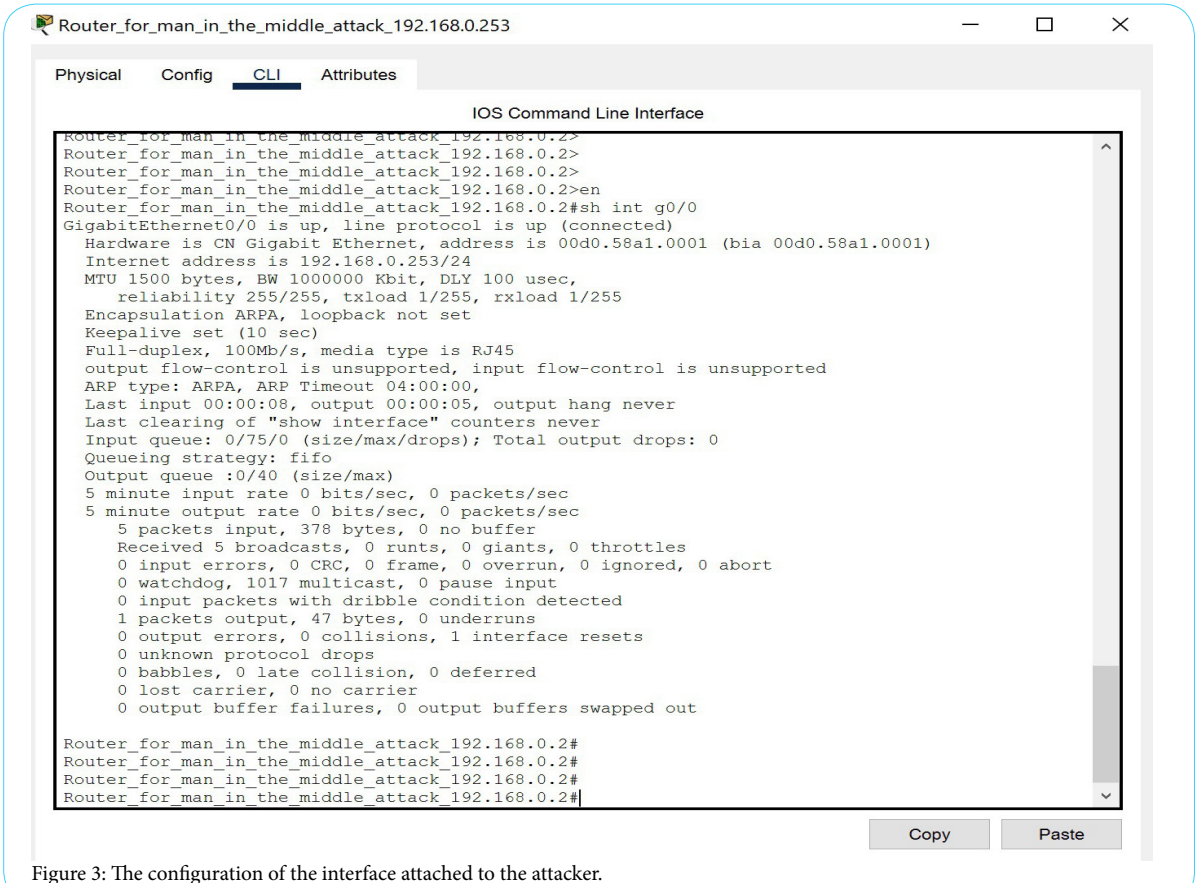

Figure 3: The configuration of the interface attached to the attacker.

Smurf spoofings

Throughout this section, we use the network topology which has been introduced in the previous section and discuss the smurf spoofing which is carried out by Router-for-man-in-the-middle-attack-192.168.0.253 only [4].

Now the smurf spoofing is composed of the following two stages, that is, the first stage is prepared for listeing by Router-for-man-in-the-middle-attack-192.168.0.253 and the second stage is prepared for captureing by this attacker, respectively.

The first stage exists for Router-for-man-in-the-middle-attack-192.168.0.253 to listen to broadcast packets commuting betwen DHCP-client-laptop-192.168.0.1 and DHCP-authenticated-router-192.168.0.254, and the sequential packet streaming being monitored by Router-for-man-in-the-middle-attack-192.168.0.253, which includes DHCP transactions originating in DHCP-authenticated-router-192.168.0.254 can be illustrated as the following (Figure 4):

- Before the falsified packet is sent, the IP address assigned for DHCP-authenticated-router-192.168.0.254 corresponds to the MAC address assigned for the interface of DHCP-authenticated-router-192.168.0.254.
- After the falsified packet has been sent, the IP address assigned for DHCP-authenticated-router-192.168.0.254 corresponds to the MAC address assigned for the interface of Router-for-man-inthe-middle-attack-192.168.0.253.

Here, the difference between the ARP table of DHCP-client-laptop-192.168.0.1 before the smurf spoofing and the ARP table after the smurf soofing can be illustrated as figure 5 [5]:

In the figure 5, the ARP table DHCP-client-laptop-192.168.0.1 shows that the smurf spoofing which has been carried out by Router-for-man-in-the-middle-attack-192.168.0.253 has made the correspondence of the IP address assigned for the interface of DHCP-authenticated-router-192.168.0.254 to be changed from 0005.5ec7.3e01 to 00d0.58a1.0001, the former half of which is assigned for the MAC address of the interface of DHCP-authenticated-router-192.168.0.254 and the latter half of which is assigned for the MAC address of the interface of Router-for-man-in-the-middle-attack-192.168.0.253.

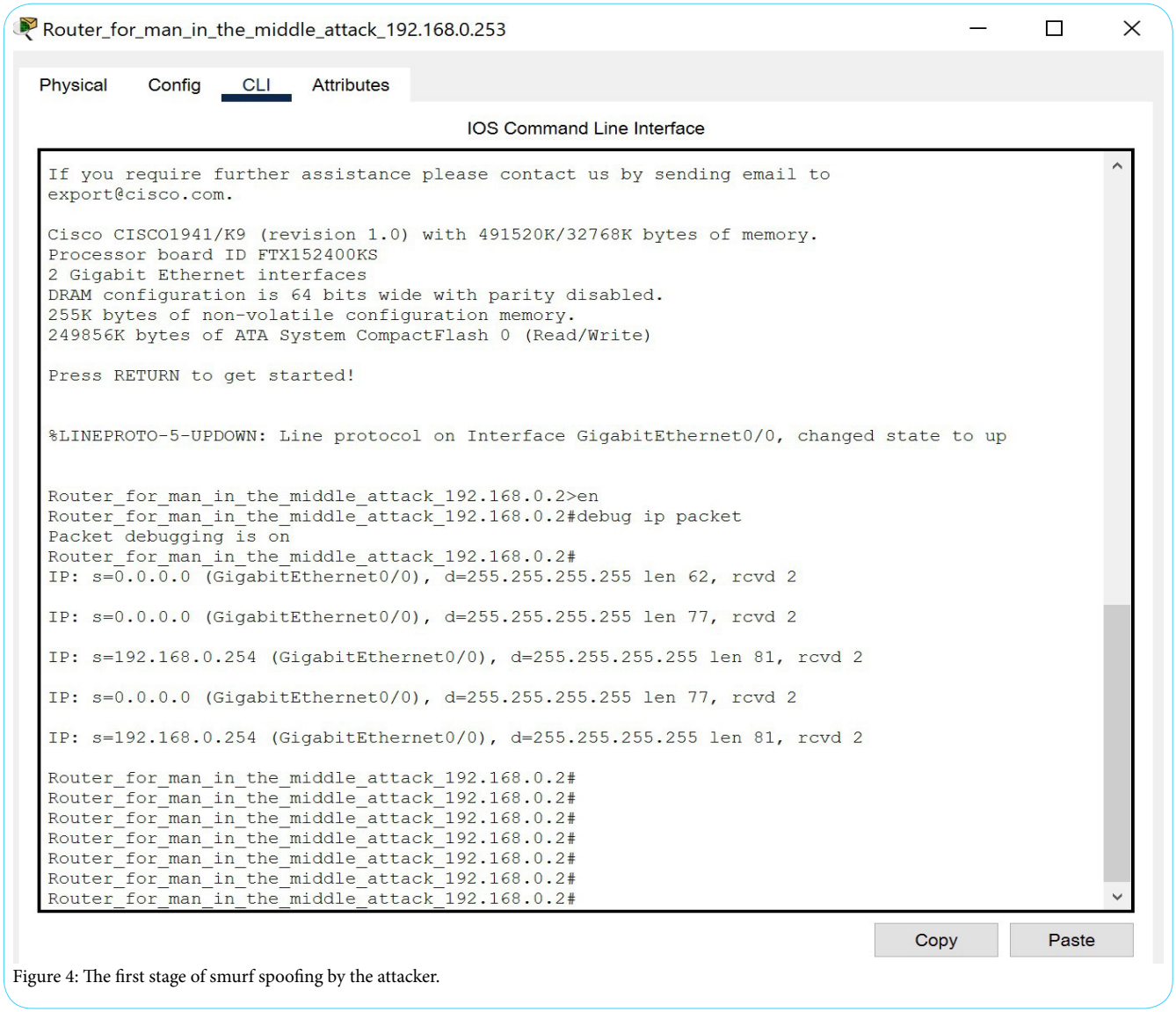

Figure 4: The first stage of smurf spoofing by the attacker.

Citation: Tong Y, Akashi S (2023) On Compound Attacks Composed of Man-in-the-middle Attacks and Smurf Spoofing. Int J Comput Softw Eng 8: 185. doi: https://doi.org/10.15344/2456-4451/2023/185

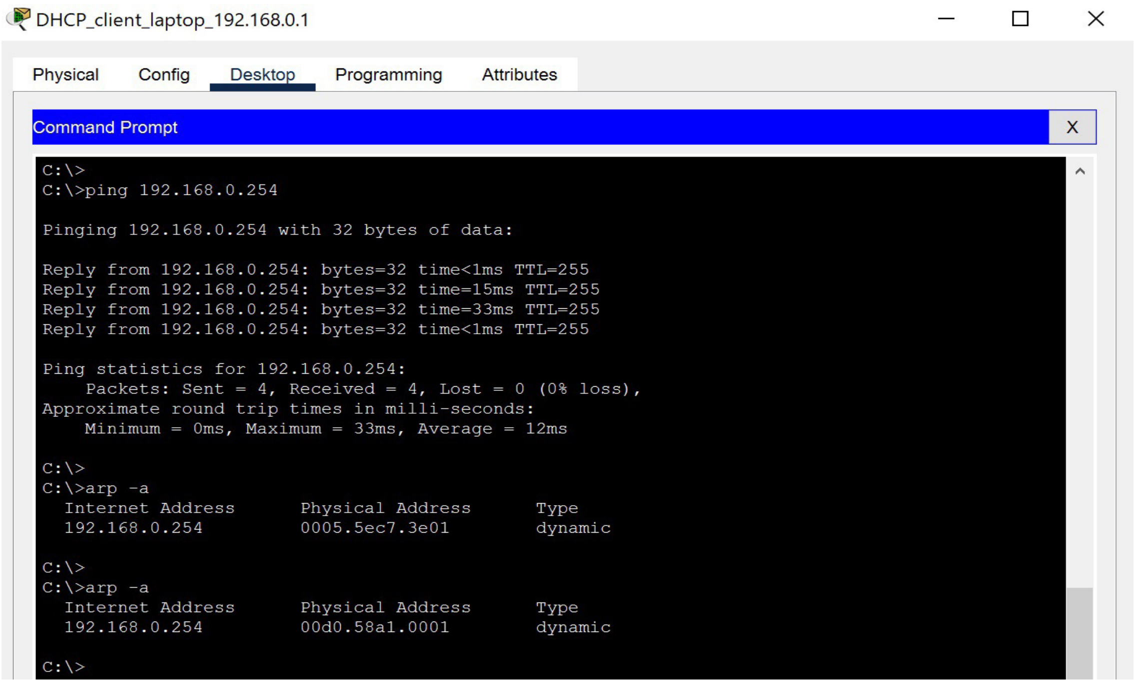

Figure 5: The difference of the ARP table of the victim before and after the attack.

Figure 6: The performance of the attacker under arp spoofing.

Smurf-spoofing-aided man-in-the-middle Attacks

In this section, we show that a simultaneous use of smurf spoofings and man-in-the-middle attacks brings about a maliciously unexpected synergistic effect. Here, if we assume that the smurf spoofings have been intentionally carried out by Router-for-man-in-the-middle-attack-192.168.0.253 and that the MACaddress table of DHCP-client-laptop-192.168.0.1 has come to contain the malicious correspondence between the IP address assigned for the interface of DHCP-authenticated-router-192.168.0.254 and the MAC address assigned for the interface of Router-for-man-in-the-middle-attack-192.168.0.253, then, by way of Switch-boundary, any packet whose source IP address and destination IP address is 192.168.0.1 and 192.168.0.254 turns to be bound for Router-for-man-in-the-middle-attack-192.168.0.253 as its final destination. Therefore, if Router-for-man-in-the-middle-attack-192.168.0.253 configures the following default route:

Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.254

in its routing table, then the packet having stopped by Router-for-man-in-the-middle-attack-192.168.0.253 halfway on the optimal route connecting between DHCP-authenticated-router-192.168.0.254 and DHCPclient-laptop-192.168.0.1 results in being forwarded to DHCP-authenticated-router-192.168.0.254. Unfortunately, this round trip route constructed maliciously by the smurf spoofing can be recognized neither DHCP-authenticated-router-192.168.0.254 nor DHCP-client-laptop-192.168.0.1.

Here the the sequential progress, which are monitored by Router-for-man-in-the-middle-attack-192.168.0.253 can be illustrated as Figure 6:

Conclusions

A large part of the comtemporary networking systems provide authenticated network clients with IP addresses and other information which are required for the authenticated clients' connecting to the Internet according to Dynamic Host Configuration Protocol. Therefore, if man-in-the middle-attacks are based on DHCP spoofings, then DHCP snooping can completely prevent the network clients from the cyber attacks being carried out DHCP spoofers. Actually, as we have seen, a simultaneous use of the man-in-the-middle attacks and the smurf spoofings cannot be prevented by DHCP snooping, because the man-in-the-middle attackers who are combined with smurf spoofers do not play a malicious role of the DHCP spoofers.

Such man-in-the-the middle attacks based on smurf spoofings as stated in this paper cannot capture any packets originating in the authenticated gateway routes and being bound for the authenticated metwork clients. Therefore, if the attackers want to the packets originating in the gateway routers and being bound for the network clients, then some other attackers such as Router-for-man-in-the-middleattack-192.168.0.252 in Figure 1 should play this role.

Competing Interests

The author declare that he has no competing interests.

References

1. A Cisco Guide to Defending Against Distributed Denial of Service Attacks, September, 2019.
2. Santos O, Muniz J (2017) CCNA Cyber Ops Secfnd 210-250, Cisco Press, Indianapolis, 1st edition,
3. Santos O, Muniz J (2017) CCNA Cyber Ops Secfnd 210-255, Cisco Press, Indianapolis, 1st edition,
4. Knuth DE (1973) The Art of Computer Programming, Addison-Wesley Publishing Company, Massachusetts, 2nd edition, 1973.
5. Kumar S (2007) Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet, Proceedings of International Conference on Internet Monitoring and Protection.