International Journal of
Computer & Software Engineering
Research Article Open Access

A Security-tool Free Detection Method of the Inter-vlan Hopping

Shigeo Akashi* and Tomofumi Matsuzawa
Department of Information Sciences, Tokyo University of Science, Noda City, Chiba Prefecture, 278-8510, Japan

Abstract

It is a matter of course that our network has been constructed according to the regulations that there should exist a bijective correspondence between a set of vlans and a set of network segments whose elements are pairwisely separated from each other. For example, in case that there exist the set of two network addresses {192.168.1.0/24, 192.168.2.0/24} and the set of vlans {the vlan 1, the vlan 2}, the network should be configured according to either of the following two regulations:

- Regulation 1: The vlan 1 includes 192.168.1.0/24 only and the vlan 2 includes 192.168.2.0/24 only.
- Regulation 2: The vlan 1 includes 192.168.2.0/24 only and the vlan 2 includes 192.168.1.0/24 only.

This implies that there happpens neither the case that the vlan 1 includes a subset of 192.168.1.0/24 and a subset of 192.168.2.0/24 simultaneously nor the case the vlan 2 also includes a subset of 192.168.1.0/24 and a subset of 192.168.2.0/24 simultaneously and that every network designer follows such regulations as stated above. Actually, it is well known that, if the inter-vlan hopping is brought about, then this network configuration rule cannot work correctly.

In this paper, we discuss the problem asking how the inter-vlan hopping brings about the infromation leakage and the way of detecting the inter-vlan hopping without using security tools.

Publication History:

Received: September 24, 2024
Accepted: October 02, 2024
Published: October 04, 2024

Keywords:

Inter-vlan hopping; Internet; Network structures; ICMP

Introduction

Though it is often said that our communication based on the Internet is often suspended due to unexpected network failure, we cannot tell to what extent our mutual network correspondence can work well, because there are various kinds of causal network misconfigurations. Therefore, we restrict the causal network misconfiguration bringing about information leakeage only to the inter-vlan hopping. Here, we prepare the following classification methods:

Throughout this paper, we assume that a network which is composed of two switches being directly connected with a crossover cable and that both interfaces being directly connected with the both ends of the crossover cable are configured in the trunk mode.

In this paper, we discuss the problem asking how the inter-vlan hopping brings about the infromation leakage, more concretely speaking, the problem asking the way of making some packets stream from one vlan to another one beyond the boundary without using the inter-vlan routing, and the way of detecting the inter-vlan hopping without using security tools.

As for the mathematically basic skills which can be used for analyzing network structure, we can refer to Knuth [?]. As for the foundation of cyber security, we can refer to Santos and Muniz [?], [?]. As for the basic skills which are used to realize the inter-vlan hopping and the contuermeasures against the inter-vlan hopping, we can refer to Zola [?] and Redfox Security [?], respectively. As for the more sophisticated and network skills formulated by Cisco Systems, we can refer to edgeworthriosgooleyhucaby Edgeworth, Garza Rios, Gooley and Hucaby [?].

The case that each vlan includes each switch

First of all, we summarize a method of bringing about the intentional inter-vlan hopping. As for the two interfaces being directly connected to the both ends of the crossover cable stated in the previous section, two native vlans assigned for the them should be strictly different from each other. This illegal configuration due to the native-vlan mismatcing can be applied to the intentional inter-vlan hopping.

In this section, we use the simplest network where the inter-vlan hopping is realized can be illustrated as the following:

Throughout this paper, all the network structures which are used are composed of three routers and two switches, and as the above figure shows, the network segments encircled in blue and the network segments encircled in red are assumed to be occupied by the vlan 1 and by the vlan 2, respectively. and the crossover cable encircled in yellow is configured as the inter-vlan hopping is brought about intentionally,

Especially, in this section, the network structure illustrated in the figure 1.

- Condition 1: The 24^{th} interface belonging to the lefthand side switch and the 24^{th} interface of the righthand side switch are directly connected with the both ends of the crossover cable. It is assumed that the 24^{th} interface of the left-hand side switch and the 24^{th} interface of the right-hand side switch are configured in the trunk mode, the vlan 1 is designated for the native vlan of the left-hand side switch, and the vlan 2 is designated for the native vlan of the right-hand side switch.

***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: Akashi S, Matsuzawa T (2024) A Security-tool Free Detection Method of the Inter-vlan Hopping. Int J Comput Softw Eng 9: 189. doi: https://doi.org/10.15344/2456-4451/2024/189

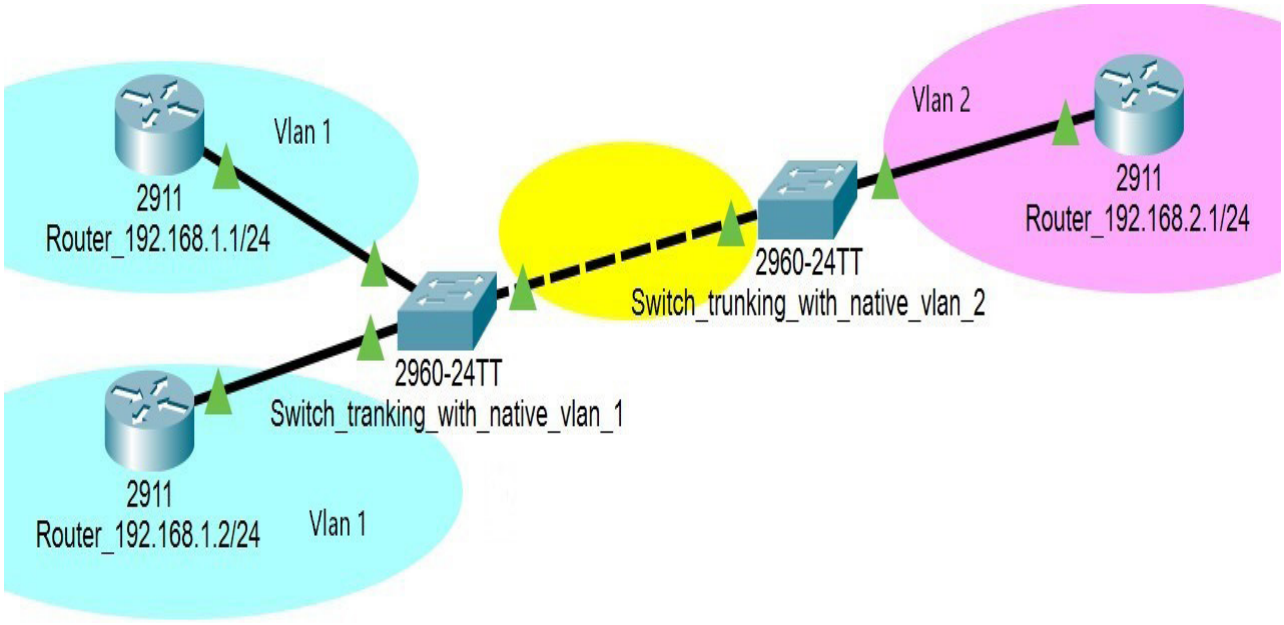

Figure 1: The case that each vlan occupies each switch.

- Condition 2: The router, which is provided with the IP address 192.168.1.1/24 and included by the vlan 1, is directly connected to the first interface of the lefthand side switch and situated on the left-hand and upper area.
- Condition 3: The router, which is provided with the IP address 192.168.2.1/24 and included by the vlan 2, is directly connected to the first interface of the righthand side switch and situated on the right-hand and upper area.
- Condition 4-1: The router which is provided with the IP address 192.168.1.2/24 is directly connected to aninterface of the left-hand side switch belonging to the vlan 1 and situated on the left-hand and lower area

It is a matter of course that the connection between the left-hand side switch and the right-hand side one brings about intentional native-vlan-mismatching, and eventually, resulting in the inter-vlan hopping, because the native vlan for which the left-hand side switch is designated is strictly different from the native one for which the righthand side switch is designated..

Under the conditions stated as above, we discuss the problem asking if the ICMP echo-requests which are issued in the broadcast way are reachable, and the problem asking if the ICMP echo-replies can be issued. Under the conditions stated above, we can obtain the following:

These table 1, table 2 and table 3 show that the packets whose destinaiton IP address is 192.168.1.255/24 can reach not only the lefthand side router but the right-hand side one beyond the left-hand and the right-hand side switches. This phenomenon, which is called

ICMP echo request	ICMP echo reply
can reach 192.168.2.1/24	cannot be issued
can reach 192.168.1.2/24	can be issued

Table 1: ICMP echo request broadcast by 192.168.1.1/24.

ICMP echo request	ICMP echo reply
can reach 192.168.1.1/24	cannot be issued
can reach 192.168.1.2/24	cannot be issued

Table 2: ICMP echo request broadcast by 192.168.2.1/24.

ICMP echo request	ICMP echo reply
can reach 192.168.1.1/24	can be issued
can reach 192.168.2.1/24	cannot be issued

Table 3: ICMP echo request broadcast by 192.168.1.2/24.

the inter-vlan hopping, means that any broadcast packets commuting in the inside of the network segment 192.168.1.0/24 are leaking into the other network segment 192.168.2.0/24.

The case that multiple vlans share one switch with each other in legitimate way

In this section, we use almost the same network structure as shown in the previous section, which can be illustrated in figure 2:

As we see in the previous section, the network structure illustrated as above satisfies the following conditions:

- Conditions 1, Condition 2 and Condition 3: The same conditions as the corresponding ones stated in Section 2.
- Condition 4-2: The router which is provided with the IP address 192.168.2.2/24 is directly connected to an interface of the left-hand side switch belonging to the vlan 2 and situated on the left-hand and lower area.

As the above figure shows, while all the interfaces of the right-hand side switch is included by the vlan 2, some interfaces of the left-hand side switch are included by the vlan 1 and the other interfaces are

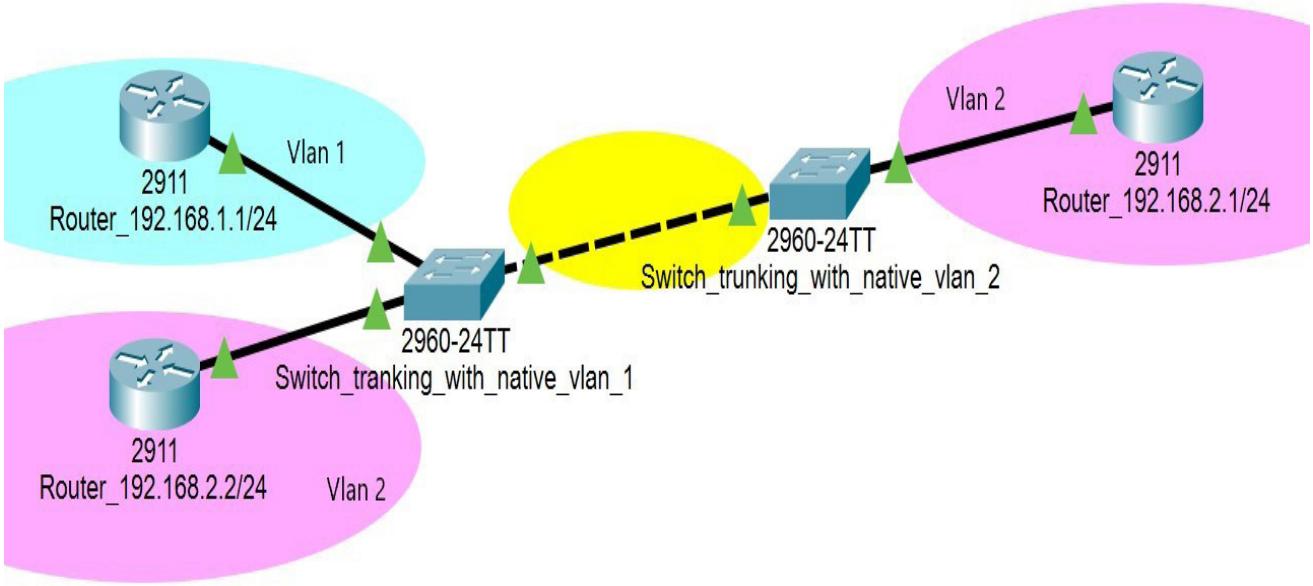

Figure 2: The case that two vlans sharing the left-hand side switch in legitimate way.

included by the vlan2, and there exists a bijective correspondence between the set of all network segments {192.168.1.0/24, 192.168.2.0/24} and the set of all vlans {*thevlan*1, *thevlan*2}, because the vlan 1 includes the network address 192.168.1.0/24 only and the vlan 2 includes the network address 192.168.2.0/24 only.

In this subsection, under the conditions stated in Section 3, we discuss the problem asking if the ICMP echo-requests which are issued in the broadcast way are reachable, and the problem asking if the ICMP echo-replies can be issued. Under the conditions stated above, we can obtain the following table 4, table 5 and table 6:

ICMP echo request	ICMP echo reply
can reach 192.168.2.1/24	cannot be issued
cannot reach 192.168.2.2/24	cannot be issued

Table 4: ICMP echo request broadcast by 192.168.1.1/24.

ICMP echo request	ICMP echo reply
can reach 192.168.1.1/24	cannot be issued
cannot reach 192.168.2.2/24	cannot be issued

Table 5: ICMP echo request broadcast by 192.168.2.1/24.

ICMP echo request	ICMP echo reply
cannot reach 192.168.1.1/24	cannot be issued
can reach 192.168.2.1/24	cannot be issued

Table 6: ICMP echo request broadcast by 192.168.2.2/24

The case that multiple vlans share one switch with each other in illegitimate way.

In the previous section, we see that, if the inter-vlan hopping works effectively, there does not exist any sustainable mutual unicast correspondence. Therefore, in this section, we discuss a solution enabling the mutual and sustainable correspondence to be realized. Firstly, we can compare the former two assumptions, which are discussed in the previous sections, with the latter one assumption, which is expected to be discussed in this section, as the following:

- As for the left-hand side switch, it is assumed that the vlan 1 occupies the left-hand side switch. Moreover, all the interfaces, except the interface being configured in trunk mode, are connected to two routers which are provided with the IP addresses, one of which is 192.168.1.1/24 and the other of which is 192.168.1.2/24. As for the right-hand side switch, it is assumed that the right-hand side switch is connected to the router which is provided with the IP address 192.168.2.1/24.
- As for the left-hand side switch, it is assumed that the vlan 1 and the vlan 2 share the left-hand side switch with each other. Moreover, an interface belonging to the vlan 1 and another interface belonging to the vlan 2 are connected to the router which is provided with the IP address 192.168.1.1/24 and 192.168.2.2/24, respectively. As for the rihgt-hand side switch, the same assumtions as above are held.
- As for the left-hand side switch, it is assumed that the vlan 1 and the vlan 2 share the left-hand side switch with each other. Moreover, an interface belonging to the vlan 1 and another interface belonging to the vlan 1 are connected to the router which is provided with the IP address 192.168.1.1/24 and 192.168.2.2/24, respectively. As for the rihgt-hand side switch, the same assumtions as above are held.

In this section, we use almost the same network as shown in the previous section whose construction can be illustrated in figure 3:

Especially, in this section, the network structure illustrated as above satisfies the following conditions:

- Condition 1, Condition 2 and Condition 3: The same conditions as the corresponding ones stated in Section 2.

- Condition 4-3: The router which is provided with IP address 192.168.2.2/24 is directly connected to an interface of the left-hand side switch belonging to the vlan 1 and situated on the left-hand and lower area.

As the figure 2 shows, while whole part of the righthand side switch is included by the vlan 2, some part of the left-hand side switch is included by the vlan 1 and the other part is included by the vlan2, and there does not exist any bijective correspondence between the set of all network segments {192.168.1.0/24, 192.168.2.0/24} and the set of all vlans {thevlan1, thevlan2}, because the vlan 1 includes the network address 192.168.1.0/24 and 192.168.2.0/24 while the vlan 2 includes the network address 192.168.2.0/24 only.

In this subsection, under the conditions stated in Section 4, we discuss the problem asking if the ICMP echo-requests which are issued in the broadcast way are reachable, and the problem asking if the ICMP echo-replies can be issued. Under the conditions stated above, we can obtain in Table 7, Table 8 and Table 9 :

ICMP echo request	ICMP echo reply
can reach 192.168.2.1/24	cannot be issued
can reach 192.168.2.2/24	cannot be issued

Table 7: ICMP echo request broadcast by 192.168.1.1/24.

ICMP echo request	ICMP echo reply
can reach 192.168.1.1/24	cannot be issued
can reach 192.168.2.2/24	can be issued

Table 8: ICMP echo request broadcast by 192.168.2.1/24.

ICMP echo request	ICMP echo reply
can reach 192.168.1.1/24	cannot be issued
can reach 192.168.2.1/24	cannot be issued

Table 9: ICMP echo request broadcast by 192.168.2.2/24.

It is a matter of course that the mutual correspondence holds successfully between the left-hand side router and the right-hand side one for which the IP addresses 192.168.2.2/24 and 192.168.2.1/24 are provided, respectively, because both routers are included by the vlan 1.

How to detect of the existence of the inter-vlan hopping

If we compare all the tables presented in Section 3 with all the tables presented in Section 4, then we can obtain a method of discriminating the case that the inter-vlan hopping happens from the case that it does not happen according to the following steps:

- Step 1: As Figure 2 shows, we confirm that, though the left-hand side router being included by the vlan 2, for which the IP address 192.168.2.2/24 is provided, issues several ICMP echo-requests whose destination IP address is 192.168.2.255, it cannot receive any ICMP echo-reply.
- After we have finished following Step 1, we change the holder of the left-hand side router used in Step 1 from the vlan 2 to the vlan 1 without changing its IP address.
- Step 3: As Figure 3 shows, if the inter-vlan hopping happens, then we can observe that the left-hand side router being included by the vlan 1, for which the IP address 192.168.2.2/24 is provided, can receive several ICMP echo-replies according as it issues several ICMP echo requests whose destination IP address is 192.168.2.255. The content of the ICMP echo-reply can be illustrated in Figure 4:

As Figure 4 shows, the ARP table recording the bijiective correspondence between the set of two IP addresses and the set of two MAC addresses is commonly used between the left-hand side router and the right-hand side one. These phenomena prove that the inter-vlan hopping has brought about unicast correspondence under the conditions stated in Section 4, which cannot be observed under the conditions stated in Section 3. This is the reason why the appearance of unicast correspondence can be applied to the detection of the inter-vlan hopping.

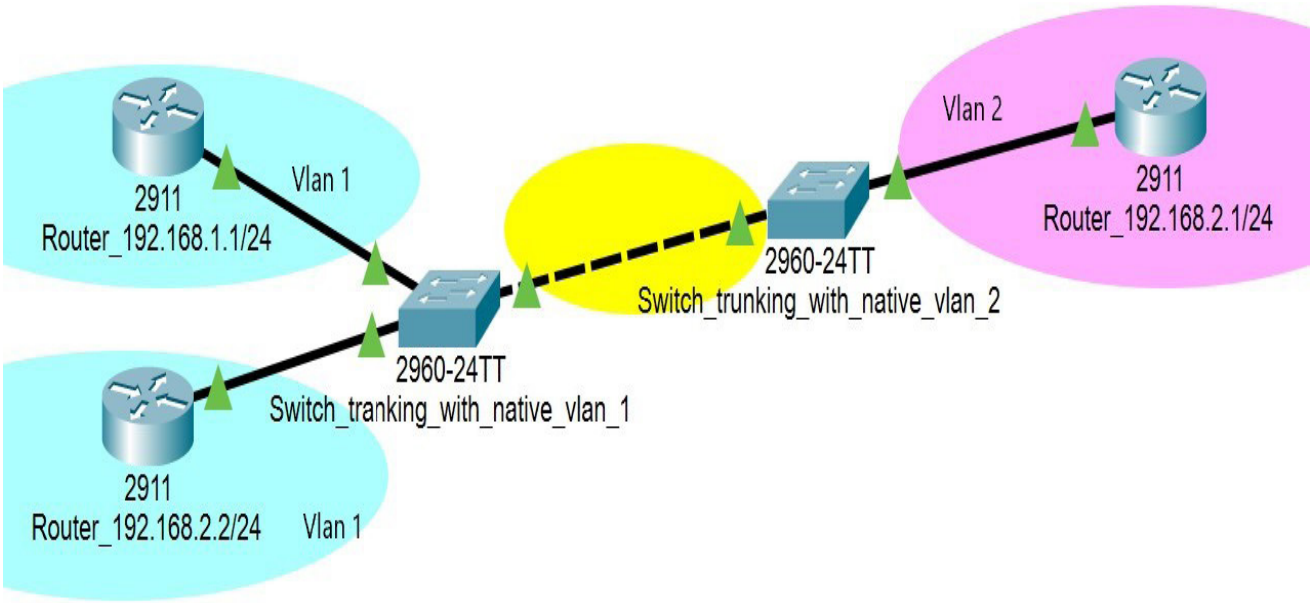

Figure 3: The case that two vlans sharing the left-hand side switch in illegitimate way.

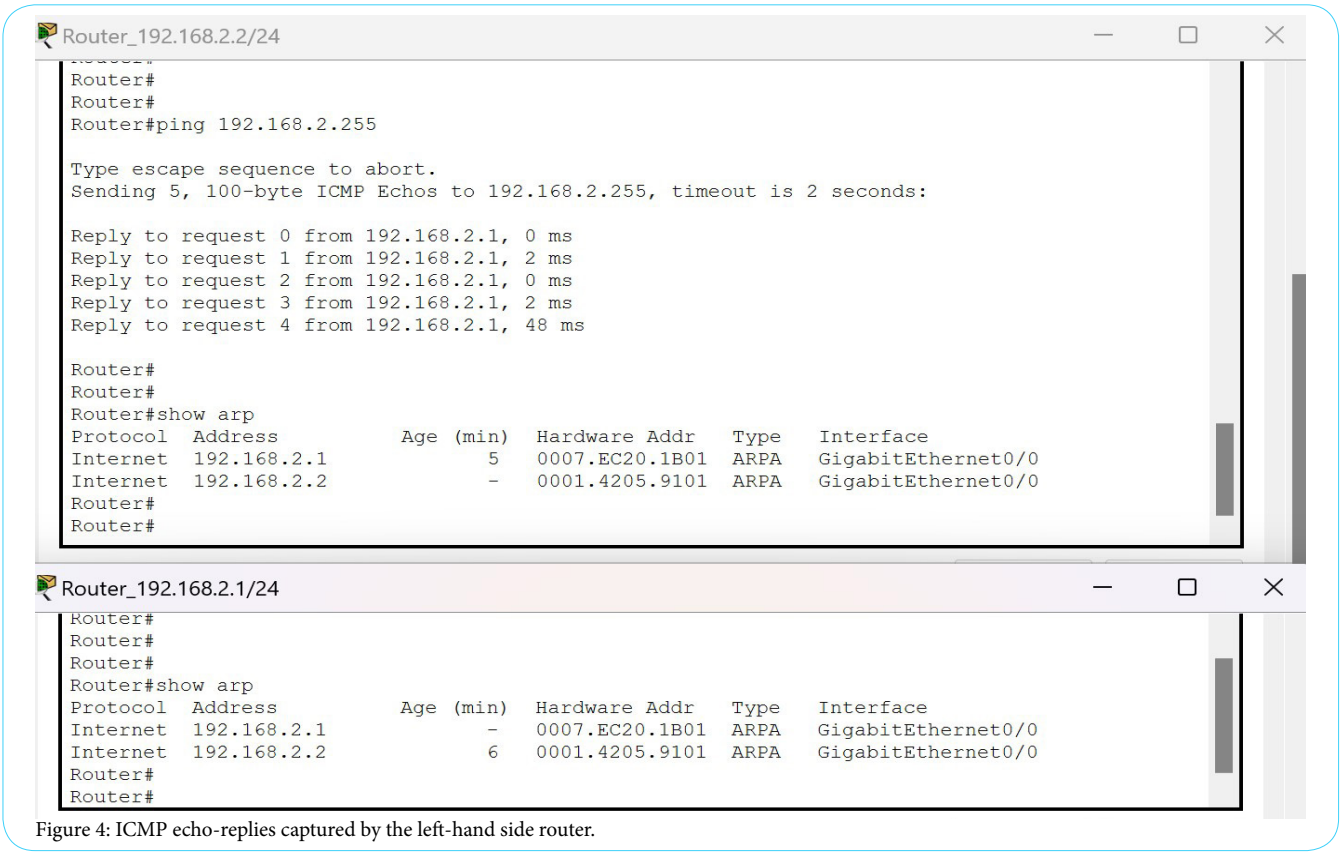

Figure 4: ICMP echo-replies captured by the left-hand side router.

Competing Interests

The author declare that he has no competing interests.

References

1. Santos O and Muniz (2017) CCNA Cyber Ops Secfnd 210-250, Cisco Press, Indianapolis, 1st edition, ISBN-13: 978-1-58714-703-5, ISBN-10: 1-58714-703-2.
2. Santos O and Muniz J (2017) CCNA Cyber Ops, Secops 210-255 Official Cert Guide, Cisco Press, Indianapolis, 1st edition, ISBN-13: 978-1-58714-703-6, ISBN-10: 1-58714-703-3.
3. Knuth DE (1973) The Art of Computer Programming, Addison-Wesley Publishing Company, Massachusetts, 2nd edition.
4. Zola A, Virtual Local Area Network Hopping, TechTarget Security,
5. Redfox Security, VLAN Hopping Attack,
6. Edgeworth B, Garza Rios R, Gooley J, Hucaby D (2020) CCNP and CCIE Enterprise Core, Encor 350-401 Official Cert Guide, Cisco Press, ISBN-13:978-1-58714-523-0, ISBN-10: 1-58714-523-5.