Journal of Alasmarya University: Basic and Applied Sciences
Volume (5) Issue 1 (June 2020)

مجلة الجامعة الأسمرية: العلوم الأساسية والتطبيقية

المجلد (5) العدد 1 (يونيو 2020)

COMPARATIVE STUDY OF THE IMPACT OF DOS ATTACKS ON LANS USING VLANS

Omran Ali Bentaher[1] ،Hadya S. Hawedi[*2] ،Kaled E. I. Abodhir[3]

[1]Higher institute of technology and science, Zliten, Libya
[2]Faculty of Information Technology, Alasmarya Islamic University Zliten, Libya
[3]Faculty of Science, Alasmarya Islamic University, Zliten, Libya

[*]hadia20008@asmarya.edu.ly

Abstract

The separation of critical services from noncritical services can occur on layer two broadcast domain. Separation could involve the isolation of broadcast or collision domains through Virtual Local Area Networks VLANs. This helps reduce the risk of Address Resolution Protocol ARP storms during heavy scanning events or denial of service attacks DoS. The major threat on the network is DoS attacks which use the broadcast storm flooding as TCP syn flood to engage the servers. This paper demonstrate how VLANs could be used to reduce the impact of DoS attacks on the servers. The simulation was carried out using Cisco Packet Tracer 6.0.1. Two scenarios were presented, first one showed flooding the server before VLANs and second scenario showed how VLANs could reduce flooding the servers so using VLANs reduce the impact of DoS attacks as mentioned in scenario two.

Keywords: VLAN, DoS, Broadcast, LAN, Trunk

ISSN: 2706-9524 (Print) ISSN: 2706-9532 (Online)

Introduction

A local area network LAN is a group of computers linked in a limited geographic area to communicate with each other through wired or wireless connections and share resources such as printers and network storage [1,2]. However, there is a problem with the LAN when multiple network groups within an entity need different rates of protection and access, this issue of segregation can be solved by physically separating different network groups in the network. However, there is a problem with the LAN when multiple network groups within an entity need different rates of protection and access, this issue of segregation can be solved by physically separating different network groups in the network. Furthermore, this method is not cost-effective and is increasingly difficult to handle as the network increases in size, thereby preventing network scalability [3]. When we fill the network with more switches and workstations, the rise in the number of devices on LAN is becoming paramount. Because most workstations tend to be fitted with an existing operating system, unavoidable broadcasts are periodically sent over the network. Sadly, each host on such a network can't avoid the consequences of such uncontrollable broadcast that decreases network performance [4]. Service denial Attacks DoS has affected servers because it sends vast amounts of useless packets to overwhelm servers [5]. In addition the network performance can be a factor in an organization's productivity and its reputation for delivering as promised one of the contributing technologies to excellent network performance is the separation of large broadcast domains into smaller ones with VLANs [6,7]. Smaller broadcast domains restrict the number of devices involved in broadcasting, and reduce the impact of DoS attacks. ARP storm is an deliberately generated situation of assault by an intruder from inside the local network. The attacker keeps creating broadcast packets in the ARP packet storm, with IP addresses within a subnet range or even IP addresses that are not present in the local subset. The aim of this attack could be for the attacker to create a DoS [8].

Virtual Local Area Network VLAN

A VLAN is a sub network logically isolated from an IP. VLANs allow for the existence of multiple IP networks and subnets on the same switched network. For example, on the same VLAN a network with three computers will communicate, each one must have an IP address and a subnet mask compatible with that VLAN [9]. The switch must be programmed with

VLAN, and the VLAN must be allocated to each port in the VLAN. An access port is called a transfer port with a singular VLAN mounted on it. Devices on two different networks and sub networks will communicate via a router, whether VLANs are used or not. You don't need VLANs on a switched network to have many networks and subnets, but there are definite advantages to using VLANs [10]. A VLAN enables a network administrator to build groups of logically networked devices which behave as though they are on their own independent network, even though they share a common infrastructure with other VLANs. While configuring a VLAN, you can call it to reflect the users' primary function for that VLAN, for instance, all student computers in a college can be configured in the Student VLAN. Using VLANs you can logically segment switched networks based on functions, departments, or project teams. These VLANs allow the network administrator to implement access and security policies to particular groups of users. For example, the faculty but not the students can be allowed access to e-learning management servers for developing online course materials [11,12].

VLAN advantages

Security groups that have sensitive data are separated from the rest of the network, reducing the chances of breaching confidential information.
Cost reduction cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.
Scalability of adding, transferring and changing networks is accomplished with low cost and less effort by simply configuring a transfer port into the segmented VLANs and assigning clients to the various VLANs.
Broadcast storm mitigation that separates a network into VLANs decreases the number of devices that could be involved in a broadcast storm. LAN segmentation avoids the transmission of a broadcast storm over the entire network.
Easy Troubleshooting administrators can more quickly track the VLANs' activities. Network problems can then be easily tracked, detected and rectified.
Integrity segmenting the network integrity splits a physical switch and removes hosts that are not supposed to be accessing each other. This means data are not corrupted as processed [13].

Types of VLANs

Today there is essentially one way of implementing VLANs port based VLANs. A port based VLAN is associated with a port called an access VLAN. However in the network there are a number of terms for VLANs. Some terms define the type of network traffic they carry and others define a specific function a VLAN performs. The following describes common VLAN terminology:

Data VLAN A data VLAN may be used and configured to bear on the user-generated traffic. It will not involve a VLAN that holds voice or traffic control. Distinguishing voice traffic and traffic control from data traffic is standard practice. Often it's referred to as a VLAN for users. These VLANs are designed for the separation of the network into user groups or system groups [14].

Default VLAN when the default configuration is loaded at the initial boot up, all the ports of a switch become a part of the default VLAN. These switch ports that are now part of default VLAN, in fact they are part of the same broadcast domain. It means any device connected to any switch port is allowed to communicate with other devices on other switch ports. VLAN 1 is considered as default VLAN for Cisco switches.

Native VLAN a native VLAN is defined to an 802.1Q trunk port which considered as the links between switches to provide the traffic transmission associated with more than a VLAN. It supports traffic coming from many VLANs, as well as traffic that does not come from a VLAN, which considered as tagged and untagged traffic, respectively. The trunk port (802.1Q) places untagged traffic on the default VLAN 1 which is known as native VLAN. **Native VLAN** a native VLAN is known as an 802.1Q trunk port which was considered to be the interconnections between switches to provide the transmission of traffic associated with more than one VLAN. This embraces traffic coming from several VLANs, as well as traffic not coming from a VLAN, which is respectively called tagged and untagged traffic. The trunk port (802.1Q) places traffic untagged on the default VLAN 1 known as native VLAN. To preserve backward compatibility with untagged traffic common to legacy LAN scenarios, Native VLANs are specified. Configuring the native VLAN as an unused VLAN, distinct from VLAN 1 and other VLANs is a best practice. As a fixed VLAN it can be dedicated to serving the native VLAN role for all trunk ports in the switched domain [15].

Management VLAN a management VLAN is any VLAN you configure to access the management capabilities of a switch. VLAN 1 would serve as

the management VLAN if you did not proactively define a unique VLAN to serve as the management VLAN. You assign the management VLAN an IP address and subnet mask. A switch can be managed via HTTP, Telnet, SSH, or SNMP. Since the out of the box configuration of a Cisco switch has VLAN 1 as the default VLAN, you see that VLAN 1 would be a bad choice as the management VLAN, you wouldn't want an arbitrary user connecting to a switch to default to the management VLAN. Recall that you configured the management VLAN as VLAN 99 in the basic switch concepts and configuration.

Voice VLAN it is easy to appreciate why a separate VLAN is needed to support Voice over IP (VoIP) [16]. Imagine you are receiving an emergency call and suddenly the quality of the transmission degrades so much you cannot understand what the caller is saying. VoIP traffic requires:-

Assured bandwidth to ensure voice quality.

Transmission priority over other types of network traffic.

Ability to be routed around congested areas on the network.

Delay of less than 150 milliseconds across the network [17].

VLAN Switch Port Modes

When you configure a VLAN you must assign it a number ID and you can optionally give it a name. The purpose of VLAN implementations is to judiciously associate ports with particular VLANs. You configure the port to forward a frame to a specific VLAN. You can configure a port belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the VLANs to which it can belong. A port can be configured to support these VLAN types:

Static VLAN Ports on a switch are manually assigned to a VLAN. Static VLANs are configured using the Cisco CLI. This can also be accomplished with GUI management applications, such as the Cisco Network Assistant. However, a convenient feature of the CLI is that if you assign an interface to a VLAN that does not exist, the new VLAN is created for you.

Dynamic VLAN This mode is not widely used in production networks. However, it's useful to know what a dynamic VLAN is. A dynamic port VLAN membership is configured using a special server called a VLAN Membership Policy Server (VMPS). With the VMPS, you assign switch

ports to VLANs dynamically, based on the source MAC address of the device connected to the port [18]. The benefit comes when you move a host from a port on one switch in the network to a port on another switch in the network the switch dynamically assigns the new port to the proper VLAN for that host [17].

VLAN Trunking

A trunk is a point-to - point connection between one or more Ethernet switch interfaces, such as a router or a switch, and another network unit. Ethernet trunks carry the multiple VLAN traffic over a single connection. A VLAN trunk enables you to spread the VLANs over a whole network. Cisco supports IEEE 802.1Q for the Fast Ethernet and Gigabit Ethernet interfaces to manage trunks. A VLAN trunk does not belong to a single VLAN but instead is a connection between switches and routers for VLANs. In standard topology there must be a separate connection for each subnet except for the VLAN trunk that you are used to see between two switches. In order to communicate between the subnets, each must have its own connection and leave a few fewer ports to assign to end-user devices. Every time a new subnetwork is deemed to need a new connection for each switch in the network when configuring a trunk, we need a single physical connection to link the subnet [19].

Implementations and Results

- before VLAN

In this section a network topology has been designed to demonstrate the information technology college network which has three departments named as student , lecturers and employees . There are three clients for each part. Cisco packet tracer has been used as shown in the figure 1.

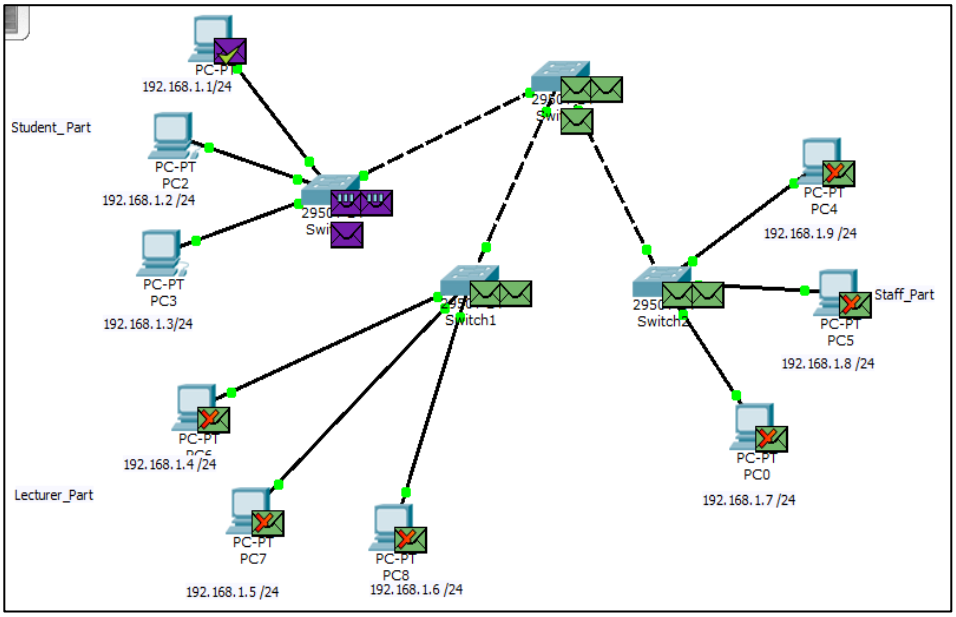

Figure 1: Network topology before VLAN

When a switch receives a broadcast frame from one of its ports, it sends the frame out all other ports on the switch. In the figure1, the entire network is configured in the same subnet, 192.168.1.0/24. As a result, when the PC1 sends out a broadcast frame the switches send that broadcast frame out all of their ports it means that the entire workstations receive them and this happens with all other clients if want to do so. As shown in previous figure there is unnecessary traffic on the network will occur. In figure2 the client_1 pinged 192.168.1.255 using command line interface so all the clients received the message.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.7: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.9: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=28ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.7: bytes=32 time=25ms TTL=128
Reply from 192.168.1.8: bytes=32 time=26ms TTL=128
Reply from 192.168.1.9: bytes=32 time=25ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.7: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.8: bytes=32 time=0ms TTL=128
Reply from 192.168.1.9: bytes=32 time=26ms TTL=128
Reply from 192.168.1.4: bytes=32 time=25ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.8: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.9: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.7: bytes=32 time=26ms TTL=128

Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 32, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Figure 2: Broadcast ping

Impact of Denial of services attacks on the network

Suppose that if there is an attacker wants to flood the server on the network using TCP syn flood one type of denial of service attacks[20] compromising that there is no segmentation on the network. In next figure the attacker flooded the server using its IP address as source and the broadcast IP address of the network as a destination IP address means that all the client would replay to the server at a time. Imagine if there are thousands of clients in the network responding to the victim so it would not be available to the legitimate clients any more as its resources overwhelmed and that is what the attacker looking for [21].

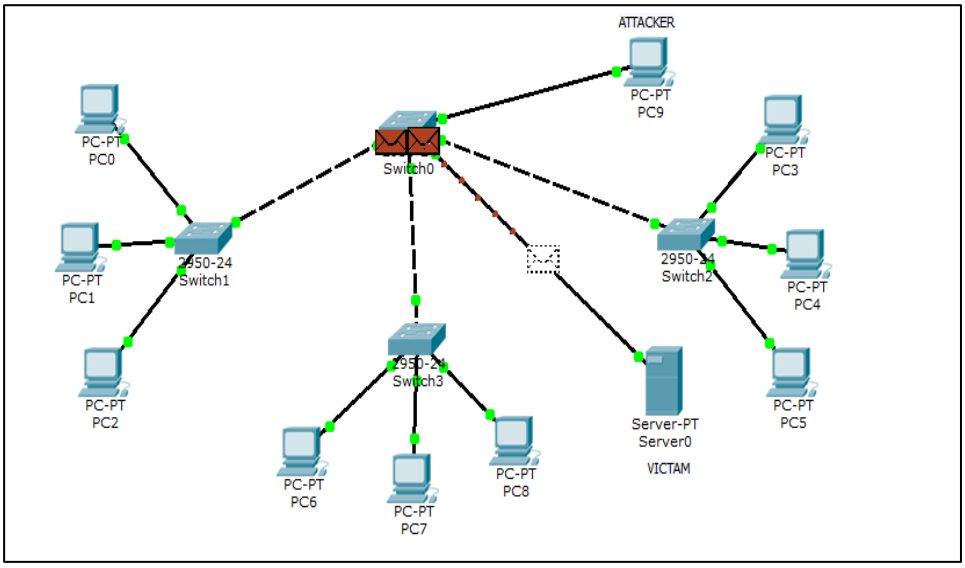

Figure 3: Attacker Flooded the Victim before VLANs

After VLAN

The network was segmented in to three VLANS using Command Line Interface CLI to configure the switches. The VLANS are Student as VLAN 10, Lecturer as VLAN 20 and Employees as VLAN 30 as follow:

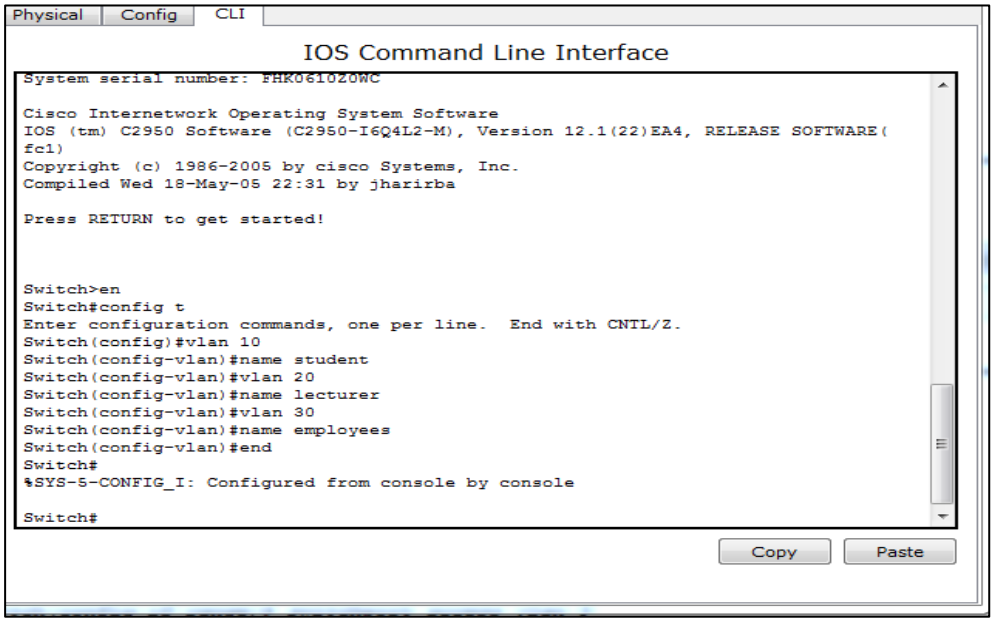

Figure 4: VLAN Configuration

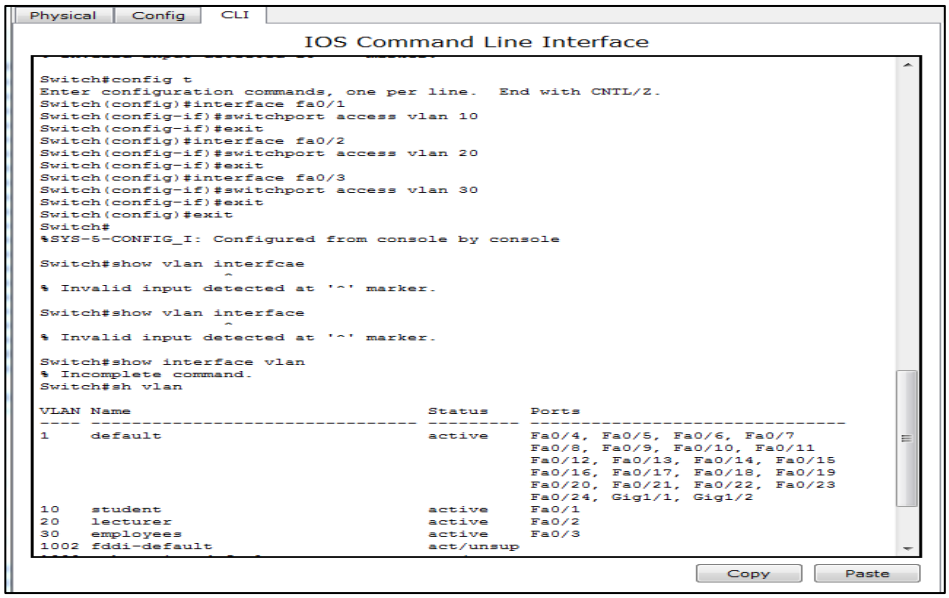

Figure5 : Assign ports to VLANs

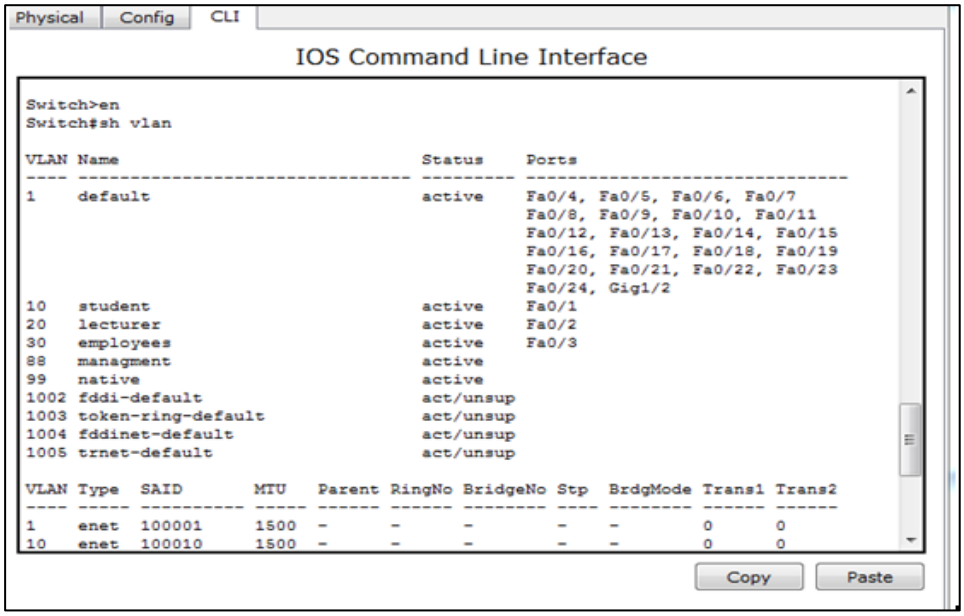

Figure 6: Final VLANs status of the switch

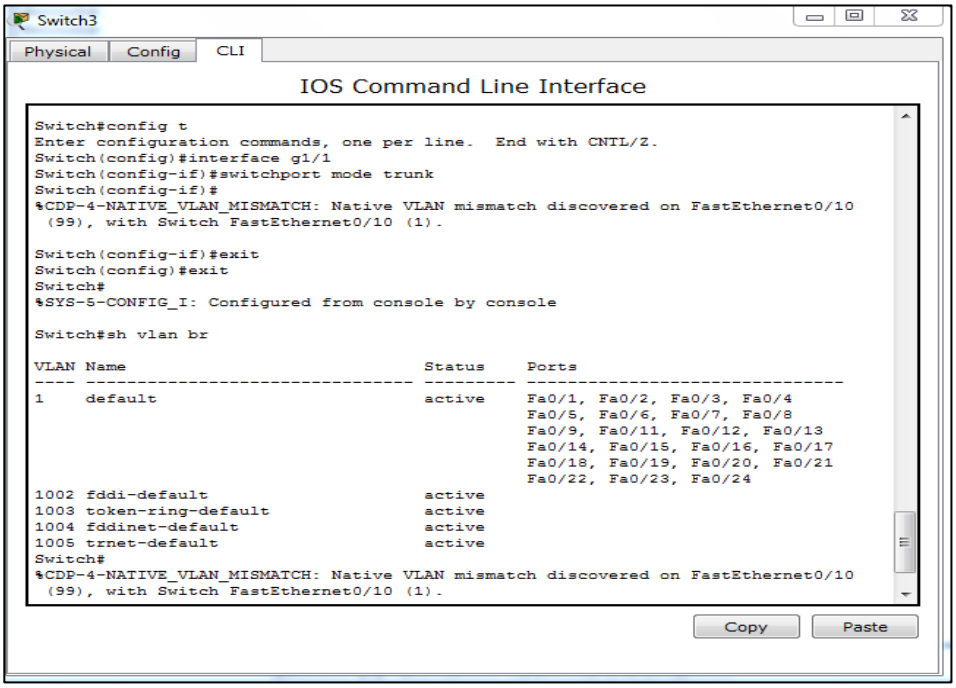

Figure 7: Trunking of Interfaces

Using VLANs to decrease the effect of DoS attacks.

As shown in figures 8,9,10 the network was segmented. The attacker PC_1, in VLAN 10 wanted to flood the server so only the PCs on the VLAN10 would response to the victim, which means reduce the broadcast storm so the server would not be affected as the number of clients minimized due to segmentation.

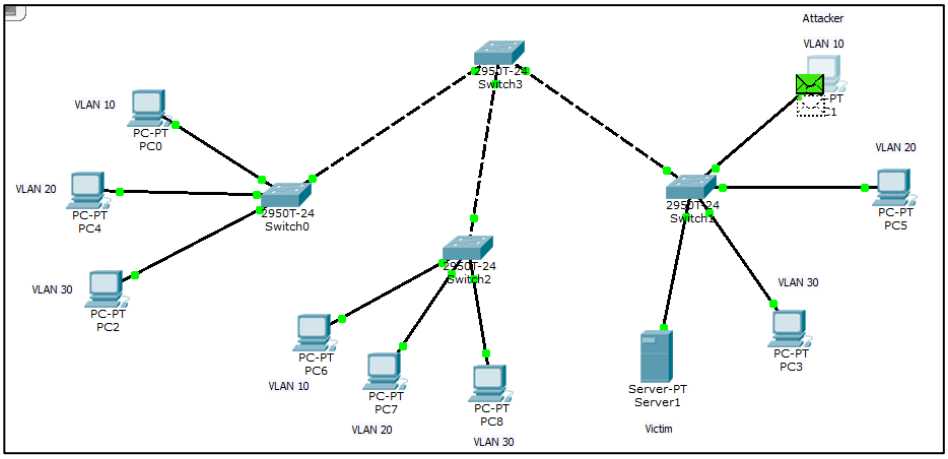

Figure 8: Attacker flooding the server

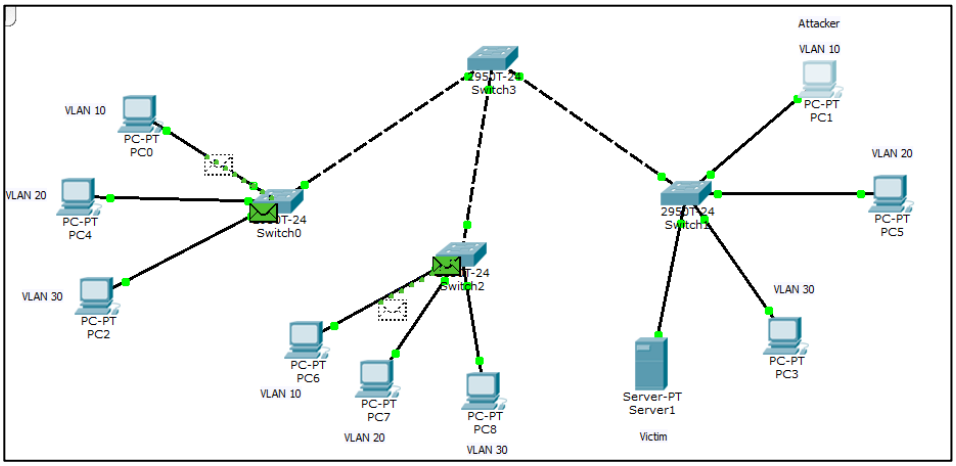

Figure 9: Useless packets sent to VLAN10

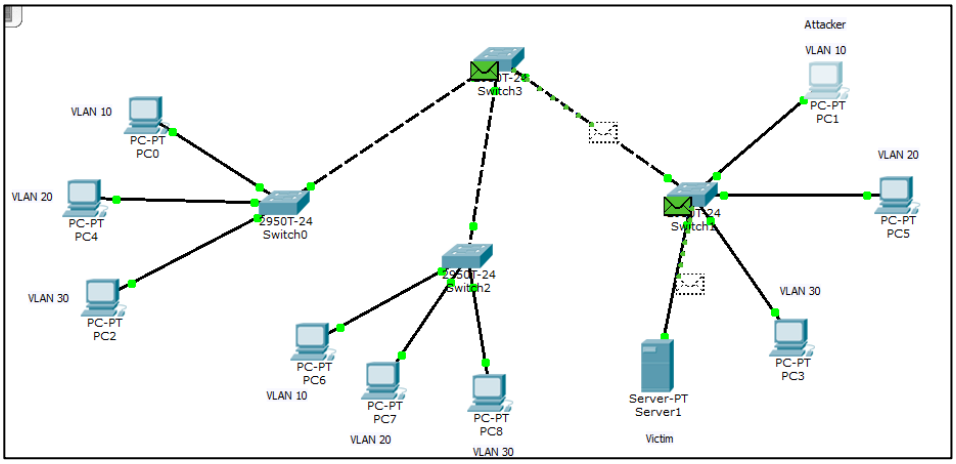

Figure 10: PCs on VLAN10 only reply to the victim

Conclusion

Broadcast storm is a big challenge in local area network especially when the number of hosts grows up frequently. The network was segmented in to three sub networks using VLAN techniques to minimize the broadcast traffic in a network that leads to denial of services attacks. The implementation demonstrated that the broadcast traffics divided in to three broadcasts. In this paper, we can conclude that utilization of VLANs can surely reduce the impact of DoS attacks. Two scenarios were implemented the first one before using VLANs and the second one after using VLANs. Based on the implementations the scenario two showed that utilizing VLANs reduce the impact of the DoS attacks.

References

[1] A. Hameed and A. N. Mian, "Finding efficient VLAN topology for better broadcast containment," in *2012 Third International Conference on The Network of the Future (NOF)*, 2012, pp. 1–6.

[2] V. Pavani, I. L. Chandrika, and A. R. Krishna, "Local Area Network (LAN) Technologies," *Int. J. Innov. Technol. Explor. Eng. IJITEE Vol.*, vol. 1.

[3] I. A. Alimi and A. O. Mufutau, "Enhancement of network performance of an enterprises network with VLAN," *Am. J. Mob. Syst. Appl. Serv.*, vol. 1, no. 2, pp. 82–93, 2015.

[4] A. C. Odi, N. E. Nwogbaga, and N. O. Chukwuka, "The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University," *Int. J. Sci. Res.*, no. 7, pp. 2608–2615, 2015.

[5] H. S. Hawedi, O. A. Bentaher, and K. E. Abodhir, "Using Access Control List against Denial of service attacks."

[6] A. M. H. Nur, "Performance Analysis of LAN and VLAN Using Soft Computing Techniques," *IOSR J. Electron. Commun. Eng.*, vol. 9, no. 6, pp. 10–16, 2014.

[7] M. Baykara and R. DAŞ, "SoftSwitch: a centralized honeypot-based security approach using software-defined switching for secure management of VLAN networks," *Turk. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 5, pp. 3309–3325, 2019.

[8] S. Vidya and R. Bhaskaran, "ARP storm detection and prevention measures," *Int. J. Comput. Sci. Issues IJCSI*, vol. 8, no. 2, p. 456, 2011.

[9] M. B. Lehocine and M. Batouche, "Flexibility of managing VLAN filtering and segmentation in SDN networks," in *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, 2017, pp. 1–6.

[10] M. S. Islam, M. J. Hossain, and M. H. Kabir, "Virtualization of Campus LAN and analyzing traffic issues of these VLANs," *Int. J. Sci. Eng. Res.*, vol. 5, no. 1, 2014.

[11] V.-G. Nguyen and Y.-H. Kim, "SDN-Based Enterprise and Campus Networks: A Case of VLAN Management.," *J. Inf. Process. Syst.*, vol. 12, no. 3, 2016.

[12] S. E. Ul Haq and S. Parveen, "IMPLEMENTATION OF NETWORK ARCHITECTURE, ITS SECURITY AND PERFORMANCE ANALYSIS OF VLAN.," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 7, 2017.

[13] A. Mehdizadeha, K. Suinggia, M. Mohammadpoorb, and H. Haruna, "Virtual Local Area Network (VLAN): Segmentation and Security," in *The Third International Conference on Computing Technology and Information Management (ICCTIM2017)*, 2017, pp. 78–89.

[14] M. Yu, J. Rexford, X. Sun, S. Rao, and N. Feamster, "A survey of virtual LAN usage in campus networks," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 98–103, 2011.

[15] D. A. Aziz, "The Importance of VLANs and Trunk Links in Network Communication Areas."

[16] E. A. Blake, "Network security: VoIP security on data network--a guide," in *Proceedings of the 4th annual conference on Information security curriculum development*, 2007, pp. 1–7.

[17] N. H. Prasad, B. K. Reddy, B. Amarnath, and M. Puthanial, "Intervlan Routing and Various Configurations on Vlan in a Network using Cisco Packet Tracer," *Int. J. Innov. Res. Sci. Technol.*, vol. 2, no. 11, pp. 749–758, 2016.

[18] S. A. Rouiller, "Virtual LAN Security: weaknesses and countermeasures," *Available Uploads Askapache Com200612vlan-Secur.-3 Pdf*, 2003.

[19] R. O. Verma and S. S. Shriramwar, "Security Optimization of VTP Model in an Enterprise VLAN," *IJECCE*, vol. 4, no. 3, pp. 950–954, 2013.

[20] D. J. Jingle and E. B. Rajsingh, "Defending IP spoofing attack and TCP SYN flooding attack in next generation multi-hop wireless networks," *Int. J. Inf. Netw. Secur.*, vol. 2, no. 2, p. 160, 2013.

[21] Prabhakaran Abraham Ali Ahmad Milad and Mustafa Almahdi Algaet, "Performance and Efficient allocation of Virtual Internet Protocol addressing in Next Generation Network Environment," *Aust. J. Basic Appl.*

Sci., vol. 7(7), no. 827–832, pp. 827–832, 2013, [Online]. Available: http://ajbasweb.com/old/ajbas/2013/may/827-832.pdf.

دراسة مقارنة لتأثير هجمات الحرمان من الخدمة DoS على الشبكات المحليةLANs بأستخدام الشبكات الافتراضية VLANs

عمران علي بن طاهر ، هدية سليمان هويدي ، خالد احميد ابوظهير

الملخص

يمكن أن يحدث فصل الخدمات الحرجة عن الخدمات غير الحرجة في مجال الارسال في الطبقة الثانية ويمكن أن ينطوي الفصل على عزل مجالات الارسال أو التصادم من خلال الشبكات الافتراضية . يساعد هذا على تقليل مخاطر كثرة ارسال ARP بروتوكول خلال أحداث المسح الضخمة أو هجمات الحرمان من الخدمة DoS . التهديد الرئيسي على الشبكة هو هجمات الحرمان من الخدمة التي تستخدم كثرة الارسال مثل استخدام الفيضان المتزامن TCP لإشغال الخوادم. توضح هذه الورقة كيف يمكن استخدام شبكات VLAN لتقليل تأثير هجمات DoS على الخوادم. تم تنفيذ الجانب العملي المحاكاة باستخدام برنامج Cisco Packet Tracer 6.0.1. حيث تم تصميم عدد اثنان سيناريو ، أولهما إظهار إغراق الخادم قبل استخدام شبكات VLAN ، والسيناريو الثاني كيف يمكن لشبكات VLAN التقليل من تأثير هجمات الحرمان من الخدمة على الخوادم لذا فإن استخدام الشبكات الافتراضية يقلل من تأثير هجمات الحرمان من الخدمة .