# Future and Techniques of Implementing Security in VLAN

Jazeb Akram
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Nabeela Akram
University of the Punjab, Lahore, Pakistan.

Saqib Mamoon
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Sheraz Ali
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

Nouman Naseer
University of the Punjab, Jhelum Campus, Jhelum, Pakistan.

**Abstract – The goal of this paper is to highlight different exposure techniques and challenges on VLAN and describing methods of employing the features provided by VLAN postures. We will first introduce the VLAN need in today's world and then we will conclude with the sketch of ongoing problems with desire solution and overall security techniques (Spanning Tree Protection, Enabling MAC Flooding Defense, Enabling Cisco Discovery Protocol (CDP) Protection, VLAN Hopping Defense, Dynamic Port Configuration, Double Tagging And Safe Implementation Process) with respect to different attacks on which VLAN security could be compromised.**

**Index Terms – VLAN; Security techniques; Future;**

## 1. INTRODUCTION

VLAN are group of Computers/ Devices on different Local Area Networks that have the ability to communicante with each other in one network or with devices on other networks as if they were all on the same physical LAN. It manage and configured through software. Due to many Exploit techniques used by attackers now a days, our systems that are operates in VLAN at risk. So if the attacker find out the Vulnerability state of our system then our networks may suffer different exposures. So, we must have to implement different Security Postures in our Virtual Local Area Networks in order to protect our networks from loss of data and information. This paper will focus on techniques that can be use to increase the security of VLAN as well as it will also discuss the future of VLAN. Firstly, we will discuss different security techniques and at the end we will present why these techniques are important for the future of VLAN.

## 2. VLAN SECURITY

In Every System Security [5] is top priority. VLANs manage each possess its own attack surface. There are many type of VLAN Security implementation techniques [2] the Core ones are listed below.

- Physical Security
- Password Protection
- Individual Role-based Access Control
- VLAN Pruning
- Spanning Tree Protection
- Enabling MAC Flooding Defense
- Enabling Cisco Discovery Protocol (CDP) Protection
- VLAN Hopping Defense
- Dynamic Port Configuration
- Double Tagging
- Safe Implementation Process

### 2.1. Physical Security

The first step in securing a switch is usually constraining physical accessibility. Make sure it is behind a locked door. On no account need to unauthorized men and women gain physical entry to this or maybe any other structure equipment.

### 2.2. Password Protection

Under no circumstances must remote control or perhaps local accessibility to be password-free. For example, configure protected layer (SSH) or perhaps Telnet ports for password-only access. Additionally, access must confirmed to the tasks carried out through everyone with top management responsibilities.

2.3. Individual Role Based Access Control

Today in many companies, giving some employee privileged [1] access to the switch means giving entire access to. No matter what role, each person with access is fully able to do almost any operational job on the device. It is no way a good idea. As a substitute, configure this each end user have unique login id and security password according to its job for accessing devices. Furthermore, defining privilege levels on the user's role in switch [4] administration A maximum of a couple facilitators (people from top administration) should have entire access to. Finally, configure secure password encryption.

In addition, giving privilege access controls, make sure accountability is properly configured and integrated according to your log management processes. Only authenticated user can have the access to changes the Accounting tracks. System must know who do what, who are trying to create hole in the security. Most of attacks happened in VLANs due to poor switch configuration. So if we assigns privilege to our System, we can create Secure Configuration for VLANs.

2.4. VLAN Pruning

Permit just applicable VLANs make use of every single trunk. Once you learn there is reason for a broadband packet from VLAN. Like, if packet go to specific trunk, stop the item.

2.5. Spanning Tree Protection

In Spanning Tree Attack, attack worked as Spanning Tree [8]. Spanning Tree Protocol (STP) maintain on Layer 2. In STP communication being held on BPDUs (Bridge Protocol Data Units) in a simple manner.. The attacker transmit BPDUs which can made a change in Root bridge and as a result create a denial of Service attacks on the network that rapidly become a commonplace threat condition. The attacker can also see the frames that he shouldn't. There are two tools to prevent this attack.

- brconfig
- macof.

On these tools we need to divide the attack on two different switches. Or we can disable STP, but then introducing loops would be another source of attack.

2.6. Enabling MAC Flooding Defense

A typical VLAN invasion is a CAM table overflow. As Q-switch CAM desk consists of port/MAC address/VLAN tasks. A packet without unique address information in the table causes the switch to perform an ARP broadcast to determine the port through which to send the packet. If the address table fills up, however, all incoming packets are sent out all ports: regardless of VLAN assignment. This essentially turns the switch into a hub.

An attacker will try to exploits this vulnerability by sending maximum number of con MAC addresses to the switch continuously, creating the CAM table (see Figure 1-1). Programs like DSNIFF provide this capability. So, the switch replaces actual entries with one from the continuous flow of attack packets. Once the switch begins flooding packets out all ports, the attacker can get the data or take advantage of the opportunity and spoof one or more MAC addresses. That ARP spoofing makes it possible for the particular attacker to maintain several gain after the flooding attack ends.

Figure 1 - 1: MAC Flooding Attack

If we want to counter MAC [6] flooding then we should implement one or more port security steps [2]:

- Use 802.1x to force packet filtering.
- On each port bind MAC address manually.
- Make the switch to learn the first *n* MAC addresses appearing on each port, and cause the switch to write them to the running configuration.

Once port security is enabled, a port receiving a packet with an unknown MAC address blocks the address or shuts down the port; the administrator determines what happens during port security configuration.

2.7. Enabling Cisco Discovery Protocol (CDP) Protection

Cisco Discovery Protocol [7] is very helpful when we need to chat between different Cisco devices. But CDP is unauthenticated. Besides its benefit of gathering information. CDP is also a piece of cake for an attacker. Like sometime in CDP that worked on Cisco devices run out of memory and crash, when attacker send hundreds of CDP packets on it. We can prevent this attack by disabling CDP or being very selective in its use in security sensitive environments.

2.8. VLAN Hopping Defense

VLAN hopping is technique representing any unauthorized VLAN access that uses one VLAN or trunk to access data on another. Dynamic port configuration and double tagging are the most common VLAN hopping attack vectors.

### 2.9. Dynamic Port Configuration

Q-switches often provide dynamic port configuration. This allows a switch to either configure a port as a trunk port or as an access port. An access port is any non-trunk port in a VLAN set. In reality, the Dynamic Trunking Protocol (DTP) is designed specifically for this. If one Q-switch sends a Dynamic Trunking Request to another Q-switch, a trunk is significantly created on the relevant port. That's great if not maliciously used.

An attacker using Dynamic Trunking Request can easily gain access to all VLAN traffic. First a laptop or desktop is attached to a switch port. Any open port in the organization will satisfy. Spoofing a Q-switch, the attacker might sends a DTP request to the target Q-switch that he want to attack. The target grants the request and configures the attacker's port as a trunk only If dynamic port configuration is enabled, All VLAN traffic destined for trunk output from the switch now also flows to the attacker's computer and attacker will extracts our data in mints.

Preventing this attack requires two simple steps:

I. Ensure that all Unused VLAN connect with unused ports.
II. Manually configure trunk ports.

### 2.10. Double Tagging

Double tagging technique operates on DTP. The attacker sends a packet with two VLAN tags over a malicious trunk on the way on which a MAC flooding attacker would. As shown in Figure 1-2, the first Q-switch strips the VLAN 10 tag and sends the packet to next. The second switch sees the packet as belonging to VLAN 20 and sends it to all next appropriate ports. The defense is to not use DTP and initially to set all switch ports to access ports on all edge switches.

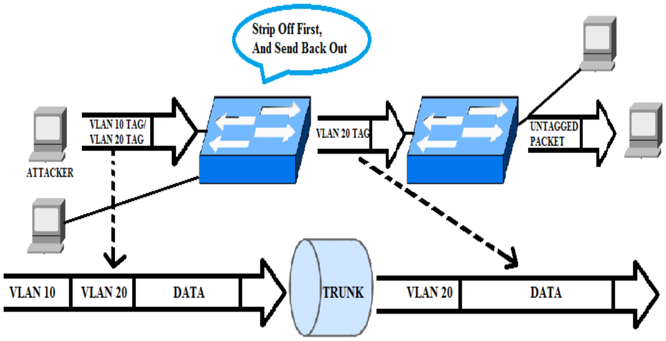

Figure 1 – 2:Double-Tagging

### 2.11. Safe Implementation Process

Implementation plan is a plan that provides architecture-specific segmentation and safe switch operation. The process consists of following,

1 First of all configure all ports as access ports and then Configure switch security (Control physical access, Create role-based user accounts, Restrict telnet ports to account- and, password-only access, Enable port security). Configure trunks and Configure VTP/MVRP (recommended to shut it off) after that Create VLANs and Assign an IP address range to each VLAN.

2 Assign ports to VLANs according to their IP address (recommended for most static wired networks), MAC address, port assignment, by dynamic assignment (recommended for most wireless networks and shared switch port networks), protocols, and by applications.

3 Remove all data VLANs from the native VLAN and Assign unused, connected ports to an unused VLAN.

4 Configure inter-VLAN routing.

5 Create and apply L2 ACLs and VACLs and then Create and apply L3 ACLs.

## 3. FUTURE OF VLAN

The Future [3] of Virtual Local Area Network (VLAN) is wide open to companies which operates on wide scale to small Companies. The VLAN will help reduction of traffic, increase security, cost effective (traveling expanses while communicating other department in different cities) and make it easier for the IT department to manage better security and Management in the organization. Many companies have Installed VLAN into their networks. This cost-effective solution offer a way of secure communicate with decreasing the surplus on the network. Companies cost decreased due to VLAN because now their employee don't have to travel to other cities which have different departments. They form a network and communicate with rest of the departments using VLAN. The future of VLAN will grow bright, as now a days companies are focusing on cost effective ways and forming a VLAN is in the best interest of companies. Of course there will be some initial cost establishing VLAN but it is in the best interest of Companies future. The MAC-based protocol will be going to implement on wider scale because it tends to be more protected and secure of sharing different resources on different virtual local Area networks. We will see different styles of VLAN in future due to the fastest innovations of new hardware, software, technologies etc.

## 4. CONCLUSION

In Future Companies having the Secure VLAN technology installed in their organization will be gaining a greater competitive advantage on those companies which don't established VLAN yet. But the key focus would be designing those Virtual Local Area Networks that could have the full mechanism of secure access instead of unsecure VLANs.

## REFERENCES

[1] Tom Olzaq "VLAN network segmentation and security chapter 5" April 18 2012.

[2] IEEE. (2002). IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. New York, NY: The Insitute of Electrical and Electronics Engineers.

[3] McDonald, B. (2007, March). EPON Deployment Challenges: Now and in the Future. In National Fiber Optic Engineers Conference (p. JWA96). Optical Society of America.

[4] Seifert, R., & Edwards, J. (2008). The All-New Switch Book. Indianapolis: Wiley Publishing, Inc.

[5] Rooney, S., Hörtnagl, C., & Krause, J. (1999). Automatic VLAN creation based on on-line measurement. ACM SIGCOMM Computer Communication Review, 29(3), 50-57.

[6] Sailer, R., Jaeger, T., Valdez, E., Caceres, R., Perez, R., Berger, S., ... & Van Doorn, L. (2005, December). Building a MAC-based security architecture for the Xen open-source hypervisor. In Computer security applications conference, 21st Annual (pp. 10-pp). IEEE.

[7] Rouiller, S. A. (2006). Virtual LAN Security: weaknesses and countermeasures. Available at uploads. askapache.com/2006/12/vlan-security-3. pdf.

Author

**Jazeb Akram**

Researcher, Freelancer.