International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V68I12P103

Volume 68 Issue 12, 11-14, December 2020

Original Article

A Network Architecture for secure traffic management for the Internet of Things using Virtual Local Area Network

Deepak Tomar
Northwest Missouri State University, Maryville, USA. Visa Inc, USA

Received Date: 14 October2020
Revised Date: 22 November2020
Accepted Date: 24 November 2020

Abstract - *Computer networks that connect devices in the local areas such as office buildings, warehouses, and campuses are often refer as Local area networks. LAN could be just one building having devices connected using the switch or a hub. WLAN is a wireless computer network that links multiple devices. Two important key components that also need to be discussed are routers and switches. A network switch is a hardware that connects devices using packet switching to receive and send data whereas a router is a network gateway that transfers data packets across the network. This article is an attempt to explain what is VLAN, how it works, and different types of VLAN and their roles to secure traffic for the internet of things.*

Keywords - *LAN (Local Area Network), VLAN (Virtual Local Area Network), Computer Networks, OSI (Open Systems Interconnection) model, Switches, Routers, IoT (Internet of Things), IEEE standards*

I.INTRODUCTION

Internet of things is simply everything connected over the internet or local network. It allows devices to connect and be a part of a network. It is mainly about information and the data transferring across the devices connected over a private network or internet. IoT allows devices on closed private internet connections to communicate with others. It allows devices to communicate not only within close silos but across different networking types and creates a much more connected world.

Now comes the essential part which is security. There are many aspects to many applications regarding security, ranging from secured networks, and securing data.

Although I have been surprised in my experience working with security implementation that despite common misconception, main security threats arise not from networking layers and operating systems, but from applications themselves. Keys areas will be secure your email, sign-on, web, and mobile-based application. Last but not the last, securing your network is very essential.

Since these devices and the applications running on each of these devices can be vulnerable to security threats, it may be worth considering building an entirely separate network segment. It may not be practical in-home, small office worth looking at the VLAN concepts and applying to handle traffic and security it.

A. Definitions

Collision Domain: "In Ethernet, the network area within which frames that have collided are propagated. Repeaters and hubs propagate collisions; LAN switches, bridges and routers do not." (Homan, 1998)

Broadcast Domain: "The set of all devices that will receive broadcast frames originating from any device within the set. Broadcast domains can be bounded by VLANs in a stand-alone environment. In an internetworking environment, they are typically bounded by routers because routers do not forward broadcast frames." (Homan, 1998)

Local Area Network (LAN): "High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters)." (Homan, 1998)

Virtual Local Area Network (VLAN): "Virtual LANs (VLANs) can be viewed as a group of devices on different physical LAN segments which can communicate with each other as if they were all on the same physical LAN segment." (Homan, 1998)

B. Technical Background

The legacy way of connecting devices is LAN particularly if the area is relatively small. The issue with the LAN is that all the computers/devices connected to a local area network get the same packet that could have been just destined for a particular computer. Another issue is the collision. When one or more computer is sending the data at the same time on the same path, package may get collided and devices need to wait until the collision is resolved.

When we want to have a collision domain comprising devices from different collision domains, then we have two ways of doing it. The first one is physically separating those devices from the current collision domains and connecting them to form a separate collision domain. This method needs lots of work to be done. The other option is using the Virtual LAN. Not only to form separate logical collision domains Virtual LANs can also be used to form separate broadcast domains. (Varadarajan S)

II. Why VLAN

A. Hardware can be expensive

In a LAN hub, switches are used to connect devices and the hardware can be costly. Different network segments will need routers, switches, and ethernet. Implementation of physical segments can be very complex and introduces latency. Hardware cost reduces significantly because of the elimination of some of the network hardware components mainly routers.

B. Advantages of VLAN

As we don't use routers in VLANs most of the time we have several advantages which include the following

1) Performance: In a network that includes lots of traffic and a lot of broadcasts and multicast messages VLANs reduce the number of devices that packet has to be sent and through which we can reduce the network traffic and can increase the performance of the network.

2) Formation of Virtual Groups: In these days we have projects for some time in which those particular people will be interacting more and need to be formed a group. So, with VLAN formation of that group (Virtual) is very easy as we physically don't need to move the devices.

3) Simplified Administration: "Seventy percent of network costs are a result of adds, moves, and changes of users in the network". VLANs reduce the adds, moves and changes to the network as routers need not be reconfigured if the group is moved within a particular VLAN.

4) Reduced cost: As the number of routers used in VLANs is very less the cost of the network is considerably reduced.

5) Security: The number of devices a particular packet is sent is very limited though the security of the network is increased. (Varadarajan S)

III. HOW VLAN WORKS

There are two things to be done in VLAN when a packet arrives at any bridge. The first thing is the bridge must identify from which particular VLAN that packet arrived and to which devices that particular VLAN must be transmitted. Identifying to which VLAN a packet belongs is called tagging and sending those packets to destinations is done using the filtering database.

IV. TYPES OF VLAN

The VLAN has got its different terms like types of VLAN and the types of connection for technology and the terminology respectively. Here in this section, the five main technologies are defined which states the types of how VLAN can be configured. The type of VLAN is completely different from the types of connection which are discussed in the next heading. The VLAN has five main types in which it can be configured. This is setting the membership profile at the cantered Switch in a broadcast domain. It mainly helps in configuring the VLAN. (Varadarajan S)

There is a discussion of each of the types of the VLAN and their pros, cons, and also the cases when which one of these should apply.

A. Layer 1 - VLAN

The first type of VLAN is Layer 1-VLAN. It is concerned with the ports. Suppose we have 5 different port types and two VLAN to be configured then we distinguish both VLAN as per the port number. For example, one VLAN is configured for port number 1,2,3,4, and another one using port number 5. The disadvantage is that it does not support user mobility. Hence if the user needs to make a move to some other place then VLAN needs to be reconfigured and the design issues become necessarily be affected.

B. Layer 2 – VLAN (Membership by MAC)

This type of VLAN pertains to the Mac address. Here there is no problem like we had in layer 1-VLAN. Since because the Mac address forms the part of the workstation so no reconfiguration is required in case if the workstation gets displaced to a new place. But there are cases when this condition loses its effect. For instance, in the case of the laptop where Mac addresses are associated with the docking station, not with the machine. Another problem comes when we try to implement the VLAN with tons of machines then it is not possible to assign the Mac address in the beginning.

C. Layer 2 – VLAN (Membership by Protocol)

The. This type of VLAN is configured with the type of protocol used. Suppose any application running with the IP protocol then we can configure the network following this IP protocol. For instance, VLAN 1 for IP and VLAN 2 for IPX.

D. Layer 3 - VLAN

This type of membership considers IP address subnet. It should not be confused with the network routing, since over here IP address is used for mapping. There is one disadvantage associated with this type, which is because it takes a longer time to transfer the packet across the network. Hence as compared to Mac address, it is very slow.

E. Higher Layer VLAN

The membership profile for the device is set as per the applications employed. For instance, telnet application on one VLAN and the FTP on another. (Varadarajan S)

V. TYPES OF CONNECTION

Before talking about the connections, it is important to look into the devices for VLAN. There are two types of devices. These are VLAN aware and the VLAN unaware. The VLAN aware device is that which follows the VLAN format and understands the VLAN membership. There are three types of terminology by which VLAN is formed. (Varadarajan S)

A. Trunk Link

This Trunk is something like a branch of a tree covered with bark. The trunk connection can also be observed in this way. All the devices included in the trunk should be the VLAN aware and the frames used should be tagged frames.

B. Access Link

In this type of connection, VLAN unaware device is connected to a part of the VLAN aware bridge. A bridge is something that consists of the workstations and the devices. Here the VLAN unaware device can a LAN segment with the number of the VLAN unaware workstation or it can be several LAN segments consisting of the many VLAN unaware devices.

C. Hybrid Link

The third one is the combination of both VLAN aware and the VLAN unaware devices. It can have both types of tagged and untagged frames but either one should be used at one time. It cannot have a combination of both. (Varadarajan S)

VI. VLAN STANDARD - IEEE 802.1Q

This standard sets the member profiles on the centrally managed switch. According to the standards the VLAN operates at the data link layer but when it is implemented, appears to be the third layer of the OSI model which is the Open system Interconnection Model. It is important to note that this standard defines only layer1 VLAN and layer 2 VLAN, though others are allowed but not defined in it. (Varadarajan S)

VII. LIMITATIONS

VLAN also has some limitations like broadcast, device, and port limitations which are as follows. The very first disadvantage is the broadcast and the limitation of the device. It is because of the use of the router to manage the routing of the VLAN but if the number of the VLAN to be configured is large then it is required to use many routers and that increases the cost. (VLAN Information)

Since the users on the same VLAN are connected and access the same information simultaneously then there is a threat for the virus to spread and harm the systems. If one of the users gets affected then there is the probability that the entire user on a single VLAN will be affected by it. Because of the requirements for the latest and fast technology, there is a need to expand the network. For this purpose, a greater number of the switches and the router are required and this increases the cost. The communication between the VLAN also becomes one of the disadvantages as we cannot connect directly to two different VLAN so we have to manage the user information somewhere and this is no easy task to do.

VIII. PLANNING AND MAINTAINING

Getting technology and implementing it can be an easy undertaking but the maintenance might not be comfortable. The planning and maintenance involve some issues like what kind of membership should a VLAN use. How to create VLAN groups etc.

Planning addresses traffic and network performance. This can be done by collecting the statistics which is a detailed traffic information statement about the breakdown of the intra and the inter-VLAN packets. Also involves the breakdown of those packets which get dropped by the application. By using this statistic, we can know about the network behavior and react as per the previous cases. This information is essential to make the network performing efficiently.

There are also some other ways to plan a network. For example, by inducing a dynamic VLAN membership registration process which in turn provides a more flexible network. We can also define policies, a class of services, priorities for switches, and also across the links.

The network can be maintained in three ways. These are manual, semi-automated, and fully automated. In the manual method, the network administrator configures filters, labels, and the parameter in each device manually. The semi-automated way has the option to automate the initial steps and then for all the other subsequent changes and the moves, there is the choice of both either manual or automated mode. The fully automated step feeds the constraints while VLAN is configured and if any workstation attempts to join then it depends on the norms and the other criteria set by the administrator. (Long, Leung, Deng)

IX. SECURITY

The security issues come with a poor configuration and its security gains can be obtained with a simple configuration. The Security can be attained by closing off all the highly sensitive users in one VLAN segment group and the outside user cannot communicate with the inside user. (Overview of Routing)

We can divide the broadcast domain into as small as possible groups and attaint the high security. “VLAN's can also be used to set up firewalls, restrict access, and send any intrusion alerts to the administrator.” (VLAN – Virtual)

X. IoT DEVICES ON THEIR VLAN

Primarily security, the IoT devices can be very weak in security. To keep things simple, there can be almost as VLANs as we want but most WIFI access points will have a limited number of networks that they create. A separate WIFI network for each VLAN will also be needed. Having a segregated network will prevent hackers to control all the devices in the network. If a particular VLAN network is comprised, other segments will still be protected. Of course, devices on different network segments are allowed to communicate with each other, we still need firewall rules. There are possible to set these rules so that one IoT VLAN cannot access everything on the main VLAN.

The Internet of Things may be unsecured, and it might be an easy target for a hacker, but with a properly designed network, we can massively reduce the impact of what a compromised device can do. We probably can’t make IOT secure, but we can stop it from stealing your data, and utilizing the concept of VLAN and creating separate traffic on segregated segments can prevent the complete network from getting comprised.

XI. CONCLUSION

In VLAN, it appears that all the devices are on the same connection but in reality, they are not. They are placed at different locations. VLAN is said to be good for medium and small size companies. VLAN helps in cost reduction. It improves network performance and provides better security between different VLAN segments. Users can be put in different segments and do not see information shared from another segment. VLANs can be used to separate different types of traffics between different users onto their protected networks. VLANs through the wired method are referred to as VLANs through the wired. VLANs can also support the wireless network. With a wireless VLAN, you have a separate network that exists within your wireless LAN. A wireless VLAN has the added benefit of being able to segment wireless traffic into groups, keeping certain types of traffic separate from others. Overall, VLAN provides better control and management.

That said, as there are limitations and many consumer routers offer just one guest network and I don't think that's enough. For example, having one Wi-Fi network for devices that need to see other devices, one for actual guests or visitors and another for IoT devices.

REFERENCES

[1] Homan, C. VLAN Information. Retrieved April 8, 2007, from http://net21.ucdavis.edu/newvlan.htm#benefits, (1998, October 29).

[2] Long, X., Leung, H., Deng, Y. Planning, and Managing LAN., http://209.85.165.104/search?q=cache:jYnbP6Ig_rMJ:www.andrew.cmu.edu/user/xlong/vlan_report.ps+Feature+of+VLAN&hl=en&ct=clnk&cd=6&gl=us, (2000, January 28). Retrieved April 6, (2007)

[3] Overview of Routing Between Virtual LANs, from http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1710/1710scg/vlanrt.htm#34095, Retrieved April 4, (2007).

[4] Varadarajan, S. Virtual Local Area Networks. http://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.htm#WhyVLAN Retrieved April 4, (2007).

[5] Deepak Tomar, TQM, ISO 9000, Six Sigma and CMMI Project Management in Business and Technology. Retrieved from http://article.sapub.org/10.5923.j.se.20200901.01.html

[6] VLAN – Virtual Local Area Networks. (2006). Retrieved April 7, 2007,from http://www.simulationexams.com/tutorials/ccna/vlan/vlans.htm

[7] Zheng, X. (2006, February 28). The Advantages and Disadvantages of VLAN. Retrieved April 5, 2007, from http://www.supinfoprojects.com/en/2006/vlan_a_d/conclusion/