Abstract

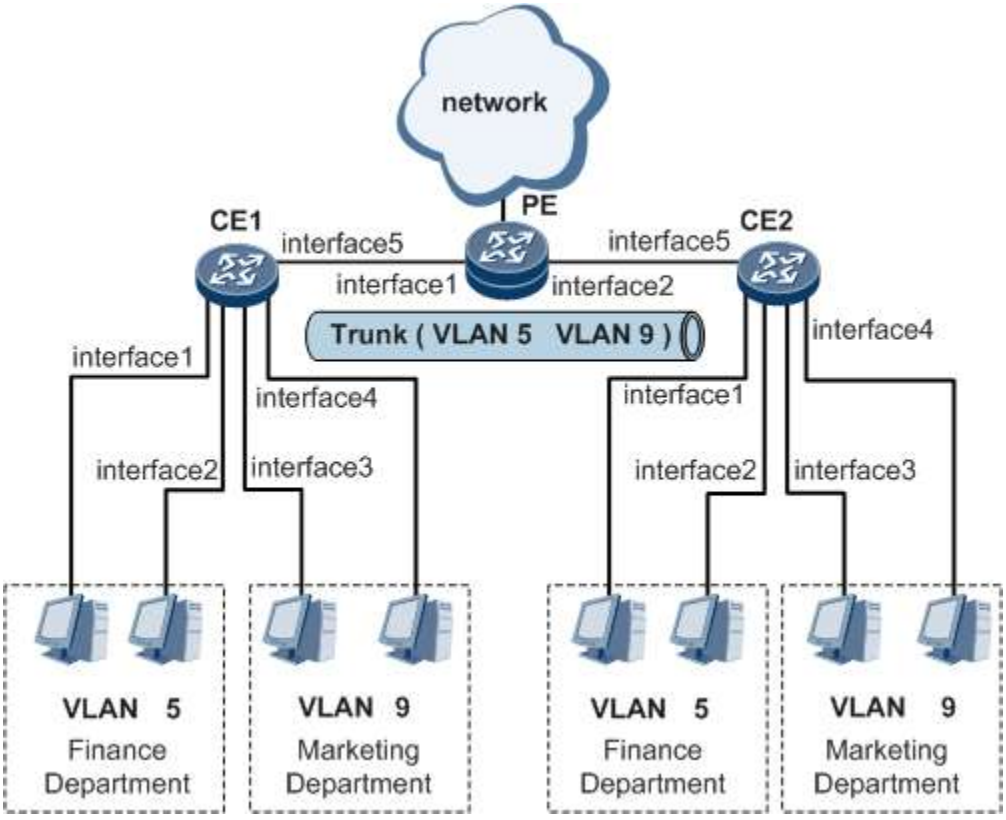
VLANs or Virtual Local Area Networks are devices in classification that move in the same broadcasting domain. On VLANs, categorization is commonly done by group interfaces that have to move in one broadcast domain while others move into other domains, wherein an Ethernet-based LAN network, each VLAN has a subset on the switch ports which may span as many switches required based on the subnet devices, each being recognized with the domain of broadcast or from subnet masks. Such that, each VLAN only provide data that belongs to the same VLAN regardless of ports they are all connected to and regardless of many networks being attached to a device.

Each VLAN can connect the domain it has to connect even if the switch they both are connecting to isn't the same. While a VLAN can be customized to take more than one LAN and each number can be used to identify the VLAN that has a valid range from 1-4094. Regardless of network dissimilarity, if the VLAN structure has the same numbers, they will connect. The common difference between LAN and VLAN would be that in LAN, each device receives a network packet while in VLAN, the network packet is sent, but only to one broadcast domain instead of many [1].

Introduction

VLANs are virtual networks that connect that connects the different physical local devices over a LAN connection under a definitive port, and can't communicate outside of it. A LAN, whereas, is a collection of computers that communicates with each other over a server wired or wirelessly in the same region. VLANs are important because they enhance data transfer and their rates by grouping the required LANs to be receiving the broadcast moved for a specified position in a large network.

More VLANs could be supported with more than one more network switch in Layer 2 (data link) which is applying the subnet masks. A broadcast domain is always linked to a VLAN for verification and data transferring, and in this, one or more network switches are usually used [2].



What is VLAN? Source [3]

Standard VLANs and VLAN Tagging

A type of IEEE standard of 802.1Q is the industry standard is VLAN tags in the ethernet networks where these tags are made up of 4bytes of data, or a 32-bit representation of 802.1Q frame. The hardcoded value for this is 0x8100 which takes like 16 bits of the first 32 bits of data, where the data packets belong to the 802.1Q VLAN. The range of these numbers is from 1 to 4094 which is stored in the final 12-bits of data. There are several kinds of VLAN for management practices:

- Native LAN

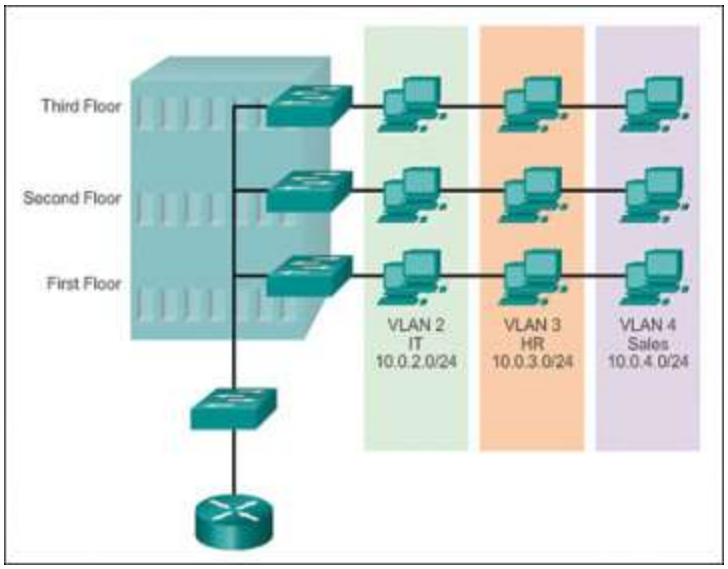
  Each untagged VLAN device will draw its attention to the Native LAN. All the packets by default will move to it and the Native LAN could be 1, 24, or however the administrators want to choose.

- Management VLAN

  It is a VLAN that the administrators of the networks can remotely connect and utilize elsewhere in the management to prevent others from interfering with the network [4].

Switch ports are the interfaces that are allocated to one or more VLANs that allow the devices to properly manage the groups based on the department each VLAN belongs to and transfers data to those systems connecting the VLAN by establishing rules for how each group can interact with the other and in what way.

Each group may vary based on the rules set for them that is, one of the VLAN connections having a set of computers can see the printer connection, but computers outside that reside outside of the connection cannot because they are from a different connection of LAN. Another example would be that the computers within the trading department cannot access or send messages to the banking department because they are two different systems.



How VLAN works? Source [5]

All computers are connected with a switch port that is configured on the same VLAN ID, having the same data connection being passed within a VLAN, such that, others outside of the VLAN cannot access the said VLAN connection. The VLAN is a 12-bit field of ethernet header which allows domains to have around 4096 VLANs with 802.1Q that defines the VLAN tagging which is called Dot1Q.

When untagged frames are received from some hosts, the 802.1Q appends a VLAN tag for representation and such that the data on the interface header becomes hidden for the other ports when moving towards its destination. The tags are used by the VLANs to identify which VLAN the packet came from and to which VLAN it should be forwarded and with that, each is sent to the required target and when the destination is reached, the VLAN tag is removed.

In terms of a trunk setup that can be used to deliver each frame across ports with the help of tags and VLAN ID under a single port that is linked with other VLANs as well. The 802.1Q tagging checks the port and with the trunk configuration enabled, the messages will be sent to the proper destinations. Ethernet packets that are not tagged properly will be sent to the default VLAN which is configured by the network administrator at that time.

A VLAN Enabled switch will look after the VLAN Tag when sending a data packet to other connections and authorize them with those tags if packets are coming from an untagged interface.

The frames are forwarded to the host port having the mac address to the destination and is transmitted through the VLAN ports. In the case of unknown responders, the frame learns its position and does not share future frames with that host.

Two methods to keep the tables for forwarding the switches up to date are either by starting with the forward entries and later deleting those entries or either by changing the topology at some point to reduce the forwarding when the table refreshes. The STP (Spanning Tree Protocol) is a protocol that is used for creating a loop-free topology among Layer 2 domains such that if the topology comes across several VLANs, a single STP can look for its VLAN in a MISTP (Multi-instance STP) and decrease the overhead of Layer 2 topologies. It does so by creating a spanning tree that checks for the connections being forwarded to it and this STP makes the linked part active forward until a failure occurs in another section [2].

Characteristics

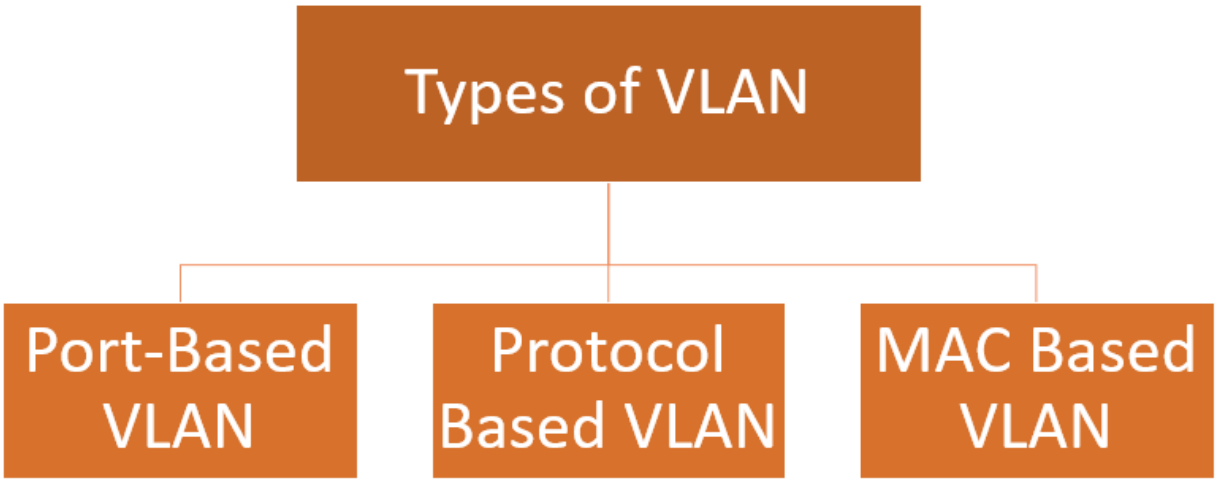
These are the essential characteristics of a VLAN:

- Regardless of dissimilarity in the networks, VLANs allow and form a gateway where devices can be grouped and formed that of a cluster.
- VLANs minimize the security vulnerabilities by only allowing the hosts to connect having the same VLAN ID.
- This also expands the requirement of using more broadcast domains since others are already grouped in a LAN.
- Traffic can be pooled as well, meaning the congestion alleviate since each VLAN has a different functioning LAN.
- VLAN can be shared across other switches and a VLAN trunk could also be formed.
- Changing the users on a VLAN is simpler in terms of commands.
- The data can be transferred to other LANs safely without some hazel of sharing sensitive data across the broadcast [6].
- Ports on a VLAN can utilize the full bandwidth provided to it instead of sharing it with others whereas the relocation of the terminal is simpler.

- It is more flexible because it divides users by groups and departments instead of their locations.
- Since VLANs are in groups, sensitive data by each department can also be secured.
- Creating the database and identifying other addresses normally takes a lot of work and time and VLAN does the trick [7].

Types

VLANs also come in their variety and has many types:



Types of VLAN. Source [6]

Protocol VLAN

Traffic routing under the protocol that, depending upon the protocol, switches will forward the traffic and data packets. This type of VLAN handles the data using protocols that are used to filter those messages that don't have a tag. Layer-3 protocol on the other hand is used to identify the frame in the VLAN hosts. Compatible with a variety of VLANs, it is mostly IP based strategy which is impractical.

Port-Based VLAN

Static VLAN

A network administrator allocating the ports of a network switch and identifying through the port position is called Static VLAN. These VLANs are joined on a LAN together and a switch port may be manually assigned as the other ports while all devices belong to the same broadcast domain.

Dynamic VLAN

Enabling a network administrator to determine the host on the network based on the attribute instead of the location of the port is called dynamic VLAN.

MAC VLAN

A MAC VLAN allows the traffic to be identified based on the source address of the packet being received by setting a map item over the MAC table of the VLAN table. The data packets are transmitted based on the VLAN ID provided by the network administrator and then classifies based on the address the packet has come from which is the mac address. All ports are shared in the switch so a table configuration is made [6].

Ranges

These are some of the important ranges present in a VLAN

Range	Description
VLAN 0-4095	Reserved VLAN, which cannot be seen or used.
VLAN 1	This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used.
VLAN 2-1001	It is a normal VLAN range. You can create, edit, and delete it.
VLAN 1002-1005	These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN.

VLAN 1006-4094	It is an extended range of VLANs [8].

Reason to Use VLAN (Virtual Local Area Network)?

There are many reasons why a business should go for a VLAN connection. Some of the following reason includes.

- Providing increased performance in the transfer of data and segregation of networks based on groups that lessen the administrative checks.
- VLANs saves money as they just need switches and would not require routers if there is no need of transferring data outside of the VLAN. It additionally can handle data at increased loads because switches have enough slots and grouping can be done accordingly which is done via the router, which would have cost tons with more departments there would have been.
- VLANs eliminate the need for information to be passed through a router and connect devices over the network which lessens the network latency.
- VLANs are more flexible for network solutions because they allocate ports based on the subnet criteria, allowing VLAN to be changed regardless of which port is being used. VLAN would work even if the switches are different or are on different buildings.
- VLAN additionally reduces the administrative work because of its managed service providers, isolation of LAN segments, and automatically blocking access to a certain set of users [9].

Advantages of VLAN

Here are some of the benefits of VLANs:

- Admittaturs normally were required to adjust the networks which now is managed by VLAN through grouping and security procedures.
- Solves the issue of broadcasting and reduces the size of domains on the broadcast.
- Allows you to add additional security layers and makes device management easier.
- Allows logical grouping of devices instead of port location and act on their network.
- Allows segmentation of department based on VLAN ID.
- Helps in creating a better geographic structure for large and growing companies.
- Reduces network latency and increases data transfer rate.
- Sensitive Data can't be viewed by others
- Hosts can be kept separate with the help of VLAN
- Does not require any additional cabling and saves cost.
- Reduces the number of devices in the topology and makes physical device management less complex.
- Has operational advantages of changing the IP subnet of the users.

Disadvantages of VLAN

These are some of the drawbacks of VLAN:

- A packet can leak from a VLAN and can be sent to another.
- Any injected packet can cause cyber attacks like SQL Injection, XSS scripting and MITM.
- A single threat such as a trojan can spread through the whole VLAN network.
- Large loads of networks require routers to control the workload.
- VLANs cannot transfer data to other VLANs [6].

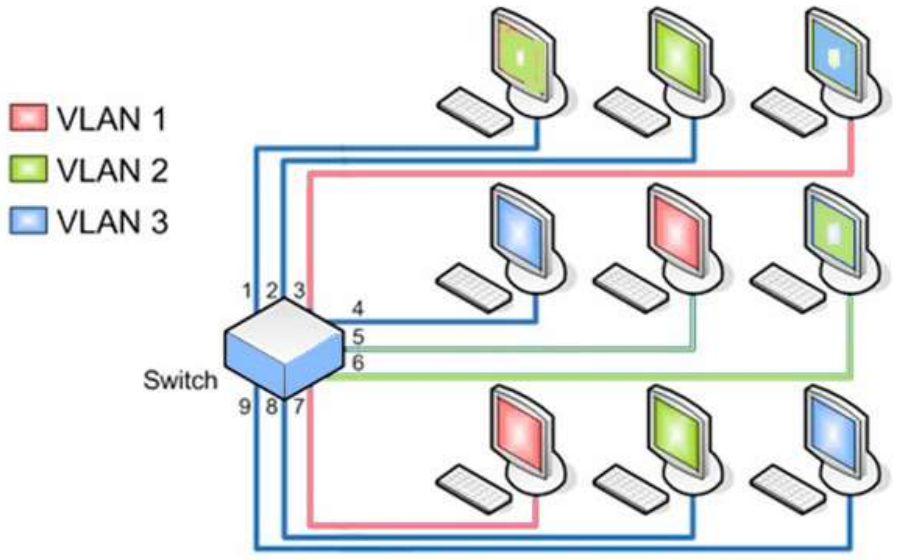
Chapter 2

Literature Review

VLAN

VLANs or Virtual Local Area Networks are subnetworks that are collections of different hosts that are being used over distinct LANs. While any computer or host that are using the same network for communication, can be wireless or wired, under the same geographical area is said to be called Local Area Network or LAN.

VLANs make things easier for the network administrators and are cost-effective because it reduces the workload of setting up different devices and provide a better network connective speed, which used to be just LANs connected with the routers to establish a communication path with the different networks and requiring more cables. VLANs removed that and created a good network infrastructure that is secure and nowadays is often set up by large firms [10].



Source taken from [11].

Another reason why virtual local area networks (VLANs) are essential is that they may aid in improving the overall performance of a network by grouping together devices that interact the most. A further benefit of VLANs is that they increase the security of bigger networks by giving a greater degree of control over which devices have access to one another. Because they are based on logical connections rather than physical connections, virtual local area networks (VLANs) tend to be more adaptable.

In order to deploy subnets at Layer 2 (data link), one or more network switches must support many independent VLANs on the same physical network. A broadcast domain is connected with a virtual local area network (VLAN). It is normally made up of one or more network switches, depending on the situation.

Types of Business VLANs

There are five VLANs where any VLAN would a type of one that is listed below:

Management VLAN

VLANs that are set up separately for the management is one of the best practices that should be applied when setting up VLANs. Such VLAN is commonly used for logging the details, monitoring the traffic, setting up SNMP, and doing more management related tasks. A benefit of this is that under high traffic of users over the network, it can still operate properly.

Data VLAN

Data VLANs are commonly known as VLANs for the users whose network design is based solely on the departments within the organization. Based on which group is which, a VLAN can be made for that department's use and groups can be made based on the organization.

Voice VLAN

Firms or businesses that use Voice over IP network (VoIP) usually have a separate VLAN for such purposes since they are separate, the data transmission rate would be great, ensuring the VoIP

quality over the network. The bandwidth is either fixed by the network administrator or is preserved by default.

Default VLAN

Default VLAN is a port where all the ports over a network device refer to or are switched to when they are not in use. They are typically assigned to port 1, however, it should be kept some other port instead of 1 for security reasons.

Native VLAN

Native VLANs are the ones that manage the untagged traffic that will be in check by the trunk port to verify and send data ahead to the host over which it is sent to or for over the LAN network. The access point where the data is being sent from can be wired or wireless [12].

Why Should We Use It?

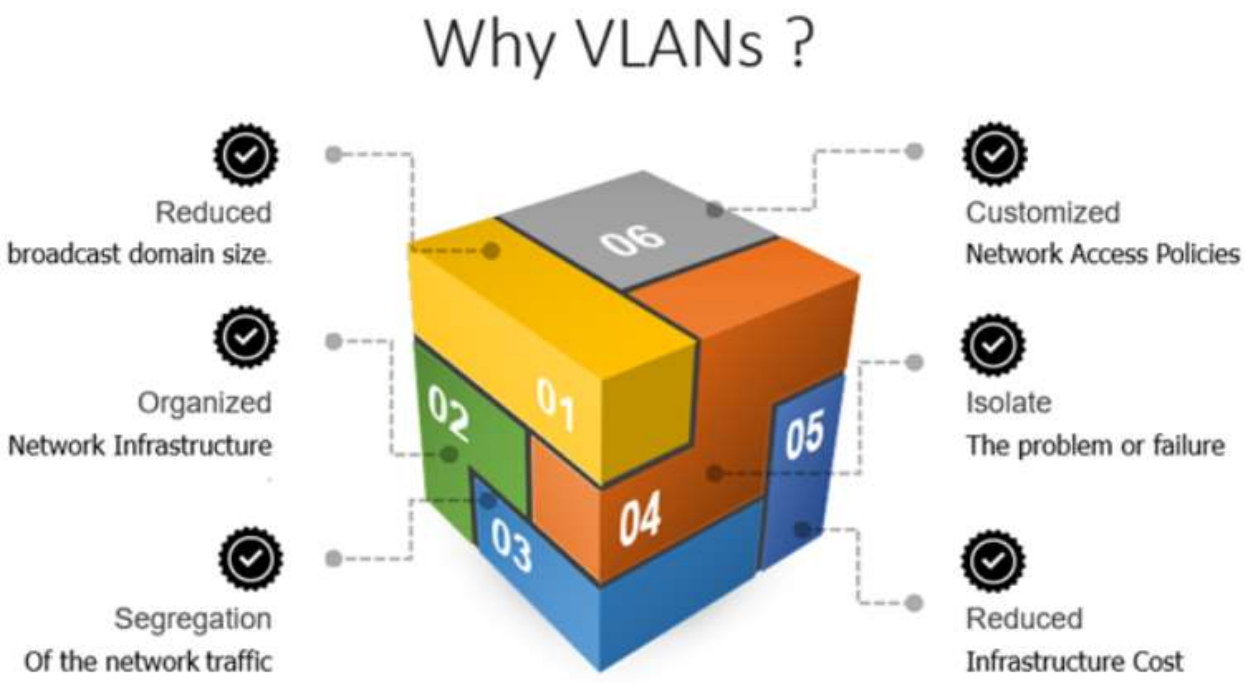


Image source taken from [13].

There are many reasons why VLANs should be used instead of LAN networks.

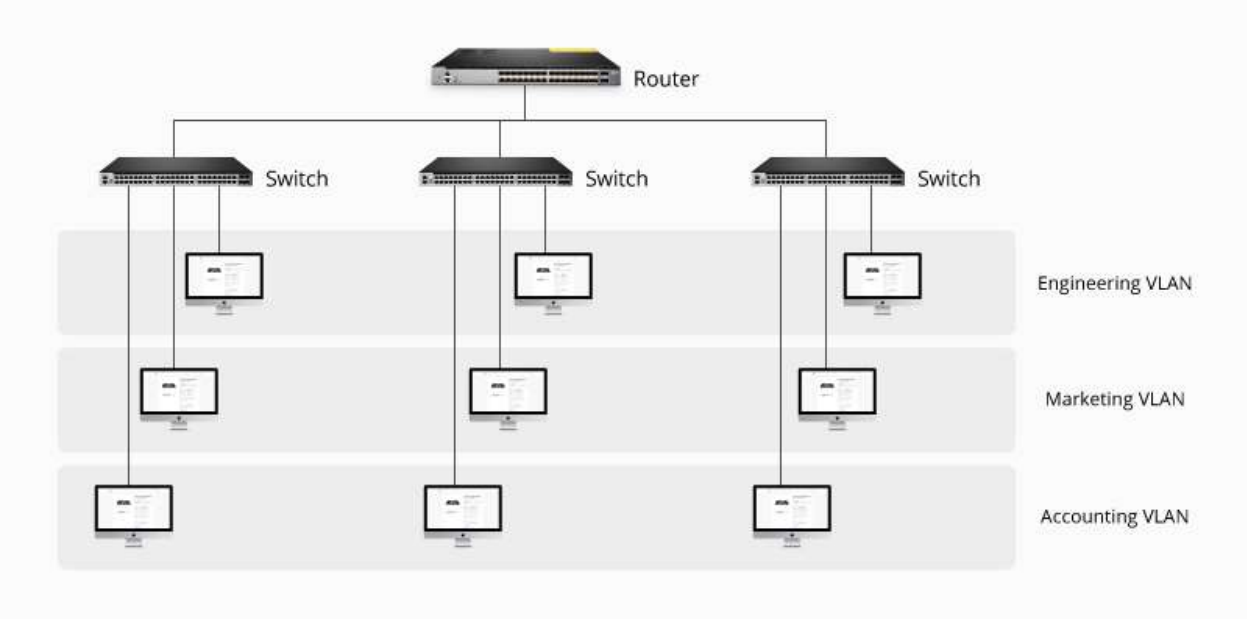
Performance

Network traffic usually has a large amount of traffic in large organizations and huge data flow is being broadcasted or multicasted. VLAN creates proper pathways and stops sending the data where it isn't required or is unrelated to, saving a lot of data and bandwidth and increasing the performance of the operation being commenced.

During the times of routers, it usually required more processing power for the incoming traffic and then it is used to send the data traffic ahead. However, VLAN doesn't require much processing power since it filters the required traffic and only sends where it is needed, creating broadcast domains through switches which decreases the latency that could've been caused when using routers as bandwidth would have been limited by the processing under heavy traffic.

Virtual Groups/Departments

Nowadays, it is common for a business to be cross-functional and there are many different kinds of departments in a company where the common contains sales, marketing, research, accounting, and HR development departments. Such departments are formed by time and communication between each is required to be private. VLAN does the trick and creates a virtual environment where the departments are grouped as one and unless trunking is done, only members of a department, regardless of location, can contact each other. Any host outside of the VLAN won't be able to contact the insiders.



The source is taken from [14]

Simplified Administration

Most of the cost from the administration of the network comes from adding, removing, changing the users over a network. Whenever a user is moved or finds a location change, it requires complete changing of configuration over the ports, creating a new address station, and routers are also required to be modified based on the change. To fix this all, VLAN steps in with a simplified plan that is to directly modify the user or shift them accordingly or change them by forwarding the user to a different VLAN or simply setting up aliases.

Reduced Cost

VLANs normally create broadcast domains that are helpful for data forwarding and communication and what is more that it doesn't require any need for routers so buying expensive routers is off the list.

Security

Under a LAN connection, data can be easily broadcasted over the network with many hosts in it, and sensitive data can also be shared within it regardless. However, to fix this, VLAN comes with a

filtering option that filters users or hosts accordingly based on their VLAN and verifies them if data should be sent to a host or not. VLANs also can be used to restrict access, set stronger firewalls, control broadcasts, or even inform the network administration in case of an intrusion [15, 12].

What Are the Benefits?

These are some of the keen benefits that VLAN comes with:

Troubleshooting

When VLANs are set up in network infrastructure, it makes troubleshooting a lot easier and faster. It is simpler since it doesn't require the strain to check if there's an issue with the router if there's an issue with the wire, is the sender having issues in their backend or not, or was it just the receiver who has some technical difficulties? VLANs isolates users based on the groups meaning only a certain set of users are required to be dealt with instead of the whole network.

Efficient Quality of Service

VLANs are efficient and they manage the user traffic better than a LAN network because they can verify and send data based on the results of filtration and verification. In short, users in the sending/receiving point will experience a surge of increase in network performance when they shift to VLAN from LANs. Networks will also get fewer latency issues, making it faster to operate with increased efficiency for critical applications that requires constant data flow even during high traffic [12].

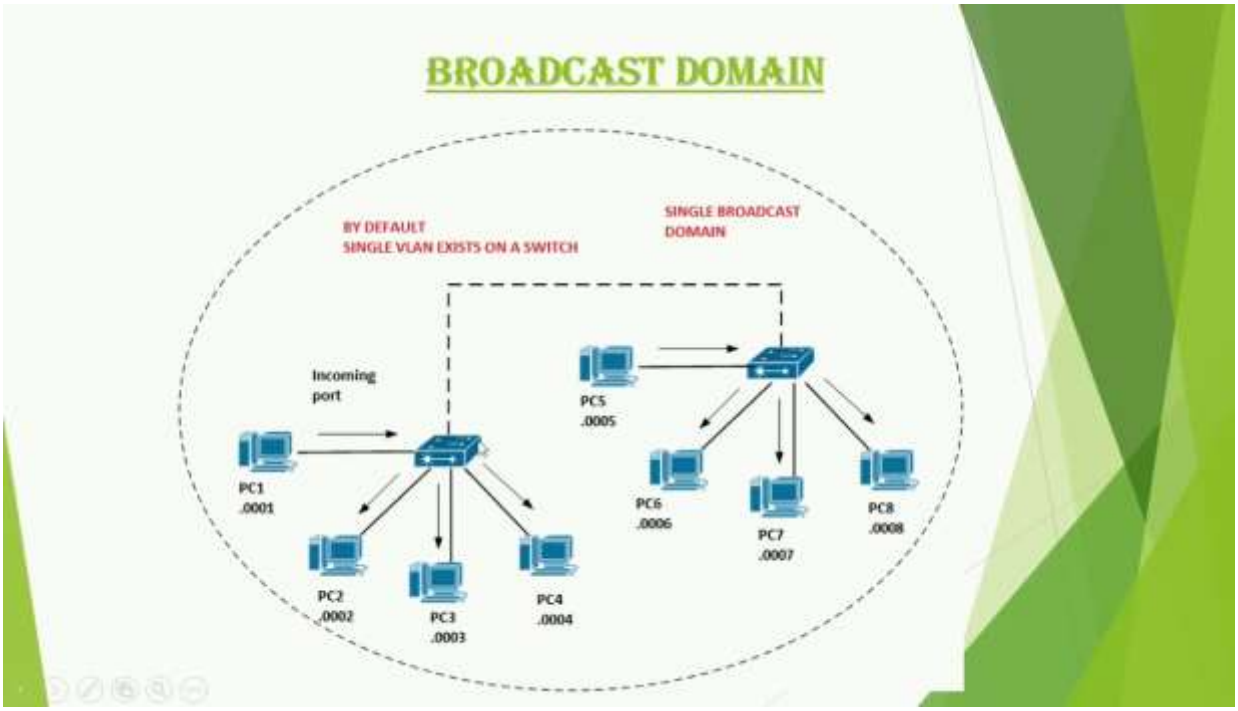
Logical Groups

VLANs enable a firm to create logical sectors or groups based on the department over a different network or LAN. Users who have been required to move from one floor to another, however, keeping their same job would mean having relocation occurred. With VLANs, only the membership of the VLAN port is required to be changed and matched with the VLAN group they were in before and the connection will be established.

Broadcasts

VLAN reduces the requirement of having routers and uses broadcast for the traffic because, during the transfer of data within the broadcast domains, the data traffic is reduced significantly. Flooding packets are limited to the ports such that data goes to where it is needed and stops the unnecessary flow of transfer.

The end-stations over VLANs prevent the broadcast to be received by the hosts that are not intended for them and if a router is not connected between the LANs, VLAN may not be able to communicate with the other VLAN based on the situation [16].



The source of the image is taken from [17]

How does it Work?

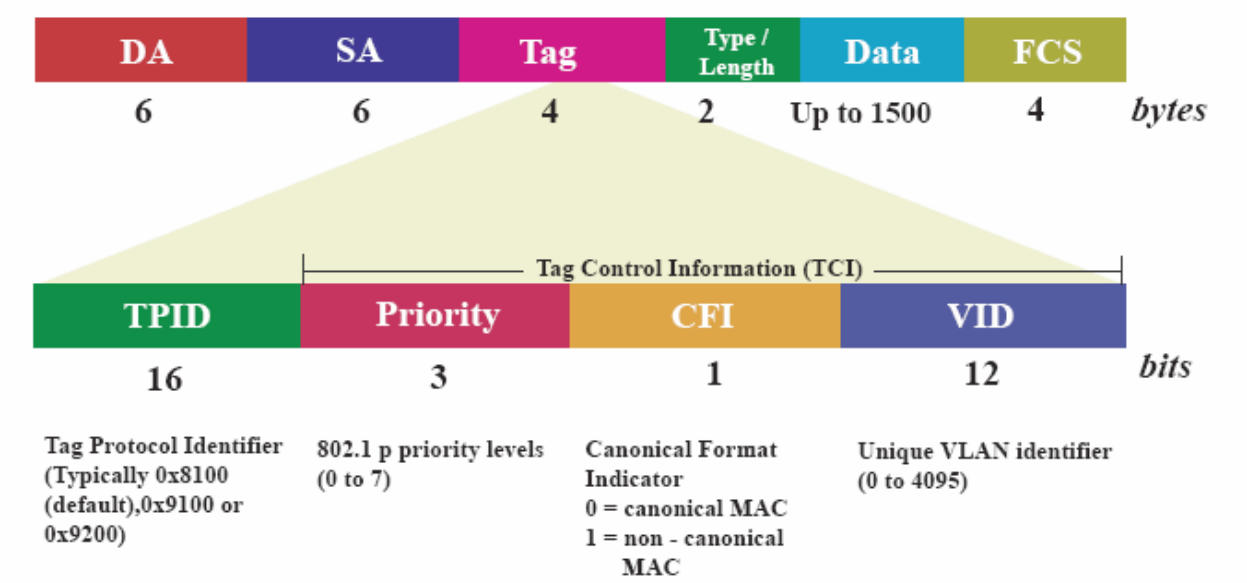
VLANs are created on switches that have ports and can be assigned to many logical groups based on the department and have a different port for each. Rules can be established based on which host is in which department and a system that which group are allowed to contact or communicate with the other group. These VLANs have special accessibility ranging from simple to complex based on the firm requirements, such that as an example of simple design is that there are hosts within

VLAN 10 and they have the access to the printer on the second floor of the firm, while others outside this VLAN cannot use or see the printer in their network. Some complex structuring also includes that the banking departments cannot interact with the trading department.

802.1Q Tagging Standard

Every VLAN gives access to the data links for all of the hosts that are connected with the ports available on the switch with the configuration of a VLAN ID, where a VLAN tag is a 12-bit code for Ethernet headers, providing support up to 4,096 VLANs broadcast domains. It is a tagging standard for VLANs in IEEE which is also known as the Institute of Electrical and Electronics Engineers 802.1Q, usually called Dot1Q.

When it comes to frames that are not tagged yet when coming from a host, the VLAN tags are attached to the header within the link under the 802.1Q format which is recognized by other VLAN for verification that stumbles upon when it reaches its destination. The VLAN uses these tags to separate the VLAN traffic for the ones only given access to it which is forwarded towards the VLAN configuration. Trunks are links for the VLANs which act as a switch handle for more than one VLAN, and for each VLAN, the tag is separated for recognition. However, when the message reaches its destination, the VLAN tag is removed from the frame and is transmitted as a message to the device/host.



The source of the image is taken from [18].

More than two VLANs can be configured over a single port with configuring the trunk that each frame that is being sent by the port is to be tagged with a VLAN ID. The device that is receiving the frame is also required to support the 802.1Q standard of tagging to be able to receive frames and transmit data, in addition to the configuration done over the trunk port as it will be where the tags will be checked and verified. Any untagged ethernet frame would normally move to the default VLAN, configured by the network administrator.

When VLAN receives any frame from an untagged ethernet, it will automatically set it to the tag it is coming from, obtained from the interface the message came, and assign it accordingly. The frame is then forwarded to checking over the trunk ports which checks the host destination it is trying to reach based on the MAC address it has received from the user.

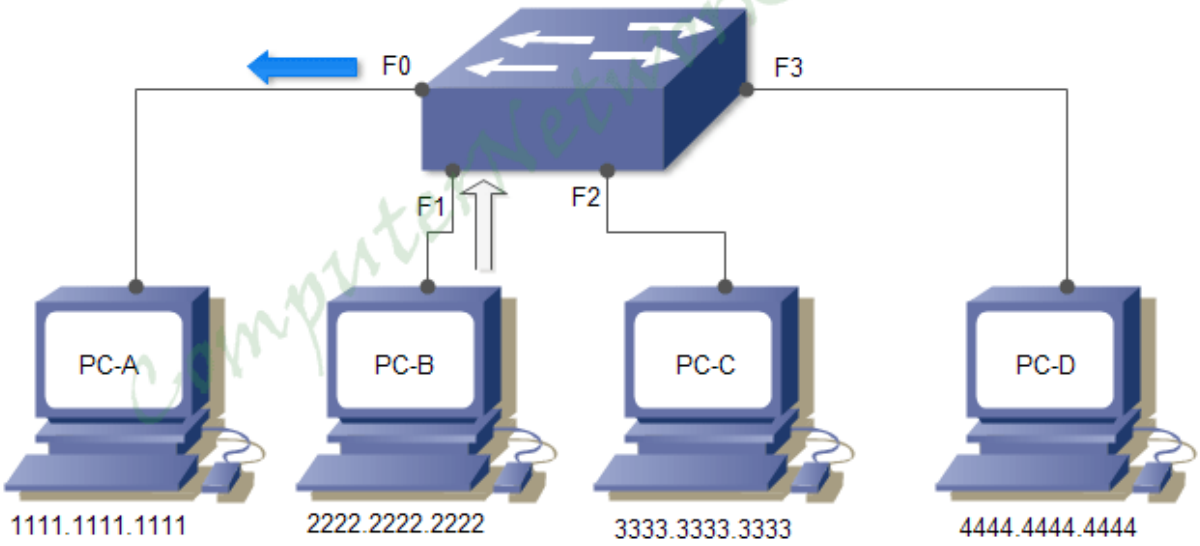
Any unknown casts did to broadcast channel or the multicast which is being forwarded to every port present within the VLAN, and any unknown host replies to that unicast frame switches automatically learn its coordinates and the location from which the message was sent from the host not belonging to the VLAN, and blocks it to prevent flooding of frames.

Switch Forwarding Tables

These tables are forwarding mechanism which is made up to date based on two mechanisms that work in a certain way to update the tables. The first way is that any change that is occurred within the topology would cause a refresh in the forwarding table. Another method is by removing all of the entries present in the table at a certain configurable time.

CAM Table

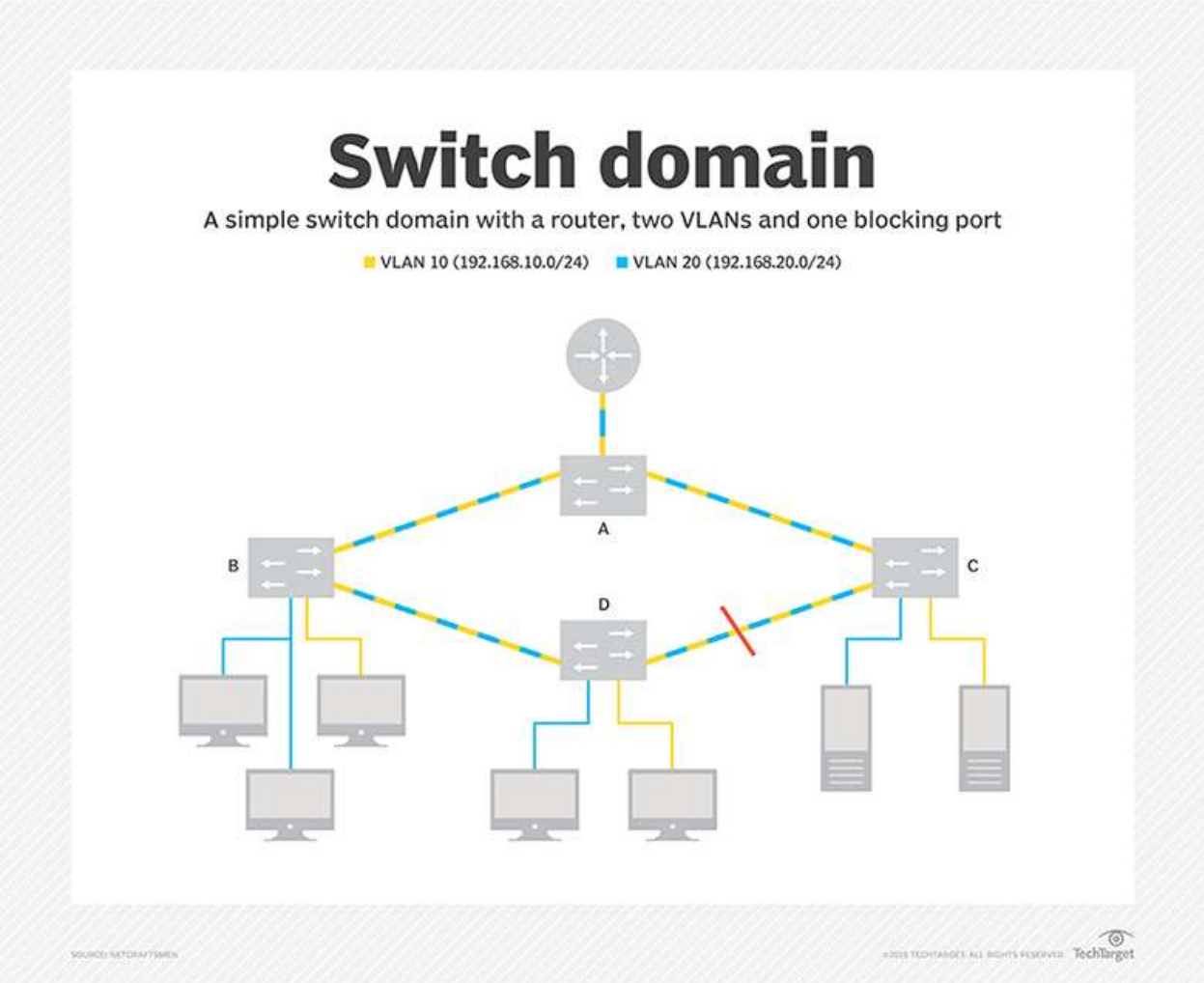
Source MAC Address	Port Number
1111.1111.1111	F0
2222.2222.2222	F1



The source is taken from [19].

Spanning Tree Protocol (STP)

The STP or Spanning Tree Protocol are used for creating topologies that are loop-free for layer 2 domains in a switch. To reduce the STP overhead for multiple requests from STP instances generated from a VLAN, Layer 2 or Multi-instance STPs are used which decrease the STP overhead. The STP blocks all kinds of messages or links that can create forwarding loops, spanning a tree from a root switch. The block would make some of the links inaccessible because the path is active for the forwarding.



The source is taken from [20].

The figure above shows how four switches can be used with two VLANs to create a switch domain. The topology, as shown in the figure, can be seen as a tree topology where the switches are connected in a ring topology. The STP would cause one of the ports to go into a blocked state creating no forwarding loops. The ports connecting switches C and D are blocked, can be seen with a red bar intersecting the port line of C and D switches. The link connecting the router and the switch are trunking the VLANs 10 and 20 respectively and is allowing the hosts to communicate VLAN 10 with VLAN 20 and vice versa. The router is set up with an IPv4 subnet to provide a connection between the two VLANs.

Vulnerabilities & Securities Solutions

These are some of the vulnerabilities that VLANs has and productive counter-measure are also aligned with it to create a proper solution for the errors and issues that could be caused by it and how they can be prevented.

CAM Table Overflow/Media Access Control (MAC) Attack

Issue

Attackers attempts to compromise the CAM table, which is responsible for storing MAC addresses and VLAN attributes for physical ports. Because CAM tables are always the same size, they are a prime target for attack. Method to attack this would be to fill the tables with data and watch the results made from it. MAC entries are generated as soon as the attacker connects to a physical port. When the CAM database is completely in use or is filled, any traffic that does not include a CAM record is routed out on all VLAN ports.

Solution

Depending upon the switches, the attack can be diminished by:

- Specifying the MAC addresses that are permitted to interface with the physical port
- Setting a limit on the number of MAC addresses allowed on a port.

Upon finding an invalid MAC address, the MAC address can be barred from using the service or the port can be closed. This thwarts the assault and doesn't allow the CAM table to be filled. Close the port, even if it means using more harsh measures, since something strange is undoubtedly taking on there.

The ARP Attack

Issue

ARP was developed before the issue of security became a key point in the world. As a consequence, this approach is predicated on the assumption that everyone is nice and that replies are real. When a host broadcasts an ARP request, it expects to get a response from just one other host. The same is true for hosts broadcasting their existence through an ARP. Other hosts think

the host is informing true information and accept its assertions. This is effective until a malicious host appears. If a host broadcasts ARP requests, indicating that it has the IP address of the default gateway, which is 10.3.2.1. PCs, routers, and other hosts will store the ARP requests generated by the host, to use them in future conversations. A consequence of this is that any genuine host traffic will be rerouted via the malicious host. After that, the data is sent to the default gateway by the attacker. Attackers may observe outgoing traffic, but not incoming traffic, because of this vulnerability. Now, on the LAN, the attacker must broadcast the target host's address to cause the default gateway to pass incoming packets to itself before forwarding them to the victim. It is now able to view all incoming and outgoing data.

Solution

Because an attacker has the potential to damage the whole LAN if there is no VLAN in place, VLANs assist to mitigate this threat. Another alternative is to use Private VLANs to compel hosts to only communicate with the default gateway, however, this is not always practical in practice.

VLAN/Switch Spoofing Attack.

Issue

To connect the two routers, a VLAN trunk has been created having VLAN 5, 10, and 15. Using tagging and trunking methods, a malicious site tries to establish a connection to router 1 in the role of another router (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, VLAN Trunking Protocol). If the attacker is successful, he or she will be able to see all VLAN traffic and communicate with hosts on any VLAN.

Solution

This attack vector should be avoided at all costs, and organisations should make certain that ports that are not meant to be trunks are set as access ports.

Double Tagging/Double Encapsulation VLAN Hopping Attack

Issue

Nowadays the systems are configured to prevent switch spoofing from occurring to increase the network infrastructure security. The exploit is done by producing a packet that has two 802.1Q VLAN headers. This is done by the first router, which then sends the header to the second router. Router 2 removes the second header from the packet and passes it to the next router. This vulnerability just broadcasts a single packet, however, it grants access to hosts that shouldn't have access to that packet. It only works if the trunk's native VLAN is the same as the attacker's native VLAN.

Solution

To defend against this attack, turn off auto-trunking and give a unique VLAN ID to each trunk port on your network. VLAN 1 should be avoided at all costs for trunking or default VLANs.

VLAN Management Policy Server/VLAN Query Protocol (VMPS/VQP) Attacks

Issue

This is an attack that has fewer chances to occur due to its requirement of having VMPS. Cisco, whose protocol this is, is moving toward 802.1X to provide the same functionality as the administrative resources, which this attack creates a load over the resources. If VMPS is implemented, it will enable VLANs to be allocated based on the MAC address of the host, that is stored within the database. With this, VQP, which is an unauthenticated protocol that makes use of UDP (User Datagram Protocol) allows the attacker to control the data as he/she likes since they have control over the whole thing. The lack of authentication makes it very simple to impersonate hosts and join a VLAN that you are not authorised to join.

Solution

Network monitoring, sending VQP queries out of band, and deactivating the protocol are all approaches for mitigating the problem.

CDP (Cisco Discovery Protocol) Attack

Issue

CDP is a feature that enables Cisco devices to connect and to build up the network infrastructure. It is also a feature that allows sharing of information over cisco devices. However, any kind of data which is being sent, such as IP addresses, router types, and software versions are among the sensitive data that is written in the readable format of the text that if obtained by an attacker, can allow them to easily create impersonation of devices to spread more threats. Because it is unauthenticated, it may be seen by an attacker who is sniffing the network.

Solution

The best course of action is to turn off CDP. CDP, on the other hand, can make the network function more smoothly and keep sensitive data that can be taken out from users, out of the way if it is kept separate from the user ports.

Multicast Brute-Force (MBF) Attack

Issue

A multicast brute-force attack searches for defects in the switch software that may be exploited. The attackers try to exploit the vulnerabilities of the switch by bombarding it with multicast frames such that the switch can be in the control of the attacker. In this scenario, the switch receives a large amount of multicast traffic over Layer 2 that would make the multicast traffic "behave inappropriately." If the switches are unable to manage all the frames, the multicast traffic can leak into other VLANs if the method to link the VLANs and routers is routing. The exploit hence takes complete advantage of the failure of the switch that wasn’t able to handle all of the multicast packets properly and thus could leak the multicast packets into other VLANs, affecting them. Even if it sounds theoretical or hypothetical because of how the attack works, especially considering the current times. This attack has worked in the past times and such that it is a vector type attack.

Solution

It is recommended that the switch contains all frames inside its broadcast domain to avoid such an attack. Switches, on the other hand, have historically failed to counteract this attack vector.

Random Frame-Stress Attack

Issue

This attack is similar to "Fuzzing," however it occurs at the second layer. A vast number of packets are generated with different fields and random data in each field, however, it leaves the only constants being the source and destination addresses. The main interest of the attacker is how much the software would copy the values that are completely random in the switch.

Solution

Although this attack should normally be unsuccessful, however, there are weaknesses or bugs in the system which enables unintended access to other VLANs or could be the start of the infamous denial of service (DOS) attacks.

PVLAN Attack

Issue

PVLANs are used to divide host groups at the second layer. For example, a DMZ may have web servers that are accessible to the public as well as a secure file transfer protocol (sFTP) server for field staff. The use of PVLANs will prohibit these servers from communicating with one another. However, PVLANs only prevent an infected web server from infecting an sFTP server at the layer 2 levels. PVLANs are not intended to protect layer 3 attacks. An attacker would build a frame with the router's MAC address as the source and his or her own MAC address as the destination. The IP address of the intended victim is included inside Layer 3. The switch will transport this frame to the router since it has the same MAC address as the router. The frame will then be sent to the victim by the router. This attack consists only of sending packets. The return frames will be addressed appropriately and blocked as a result of the blocking.

Solution

By preventing IP addresses on the main LAN from talking with one another, the right ACLs (Access Control Lists) on the router may assist reduce the impact of an attack. Because the attacker cannot access servers on PVLAN 1 from PVLAN 2, the switch is limited to only allowing communication between servers on PVLAN 1.

STP (Secondary Targeting Protocol) Attacks

Issues

STP is used to prevent networks from being looped. Bridge Protocol Data Units (BPDUs) are basic packets that include no information about the bridge protocol. BPDUs are used to identify a switch as the Root Bridge, which is responsible for determining network traffic routing. The process of identifying the Root Bridge may take up to 30 seconds in such an exchange. The attacker has two options. Routinely transmitting Topology Change Notification (TCN) messages causes the system's current network knowledge to be disrupted, resulting in the renegotiation of the Root Bridge. The Root Bridge may also be used as an alternate method of transmission. Once this is completed, the attacker will be able to examine any packets he/she wants.

Regardless of the scope and diversity of VLAN risks, they can all be efficiently mitigated by using appropriate network administration, network architecture, and modern security technology, security updates and more ways. Organizations should not be discouraged with the threats and should adopt the utilization of the VLANs as the VLANs ensures that they are properly deployed to reduce the risks which the organization may find later in the future if no VLAN is set up [21].

References

[1] Study-CCNA, "What is a VLAN?," Study CCNA, 2016. [Online]. Available: https://study-ccna.com/what-is-a-vlan/. [Accessed 2021].

[2] T. Slattery and NetCraftsmen, "VLAN (virtual LAN)," TechTarget, 2018. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/virtual-LAN. [Accessed 2021].

[3] Huawei, "VLAN Configuration," Huawei, 2020. [Online]. Available: https://support.huawei.com/enterprise/br/doc/EDOC1100143177/903e9ea3/vlan-configuration. [Accessed 2021].

[4] Bradley Mitchell, "What Is a Virtual LAN (VLAN)?," Lifewire, 05 June 2021. [Online]. Available: https://www.lifewire.com/virtual-local-area-network-817357. [Accessed 2021].

[5] Cisco Press, "Cisco Networking Academy Switched Networks Companion Guide: VLANs," CISCO, 2014. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=2208697&seqNum=4. [Accessed 2021].

[6] L. Williams, "What is VLAN? Types, Advantages, Example," Guru99, October 2021. [Online]. Available: https://www.guru99.com/vlan-definition-types-advantages.html. [Accessed 2021].

[7] D. Thakur, "Virtual LAN (VLAN) – What is Virtual LAN? Characteristics of VLAN.," E-Computer Notes, 2015. [Online]. Available: https://ecomputernotes.com/computernetworkingnotes/communication-networks/virtual-lan. [Accessed 2021].

[8] S. Sharma, "Virtual LAN (VLAN)," Geeks for Geeks, 2018. [Online]. Available: https://www.geeksforgeeks.org/virtual-lan-vlan/. [Accessed 2021].

[9] N-able, "How VLAN Works," N-Able, 2019. [Online]. Available: https://www.n-able.com/blog/what-are-vlans. [Accessed 2021].

[10] Terry Slattery, "VLAN (virtual LAN)," TechTarget, 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/virtual-LAN. [Accessed 2021].

[11] Mania, "VLAN design and IP addressing What are the fundamentals?," Informatique Mania, 2020. [Online]. Available: https://www.informatique-mania.com/en/linternet/adressage-ip-vlans-design/. [Accessed 2020].

[12] Jim Herbst, "VLANs: 5 Types and Benefits," Summit 360, 2017. [Online]. Available: https://www.summit360.com/2017/08/30/vlans-types-benefits/. [Accessed 2021].

[13] Netsguru, "Tag: VLAN and its Benefits," Netsguru, 2021. [Online]. Available: http://netsguru.com/tag/vlan-and-its-benefits/. [Accessed 2021].

[14] Irving, "VLAN: How Does It Change Your Network Management?," FS Community, 2021. [Online]. Available: https://community.fs.com/blog/vlan-how-does-it-change-your-network-management.html. [Accessed 2021].

[15] Network QnA, "Benefits of VLANs," Network Interview QnA, 2018. [Online]. Available: https://www.cse.wustl.edu/~jain/cis788-97/ftp/virtual_lans/index.html. [Accessed 2021].

[16] NetApp, "Advantages of VLANs," NetApp, 2014. [Online]. Available: https://library.netapp.com/ecmdocs/ECMP1401193/html/GUID-C9DA920B-F414-4017-8DD1-D77D7FD3CC8C.html. [Accessed 2021].

[17] V. Prasad, "Broadcast Domains and VLANS," Youtube, 2017. [Online]. Available: https://www.youtube.com/watch?v=DFd8h0g2rR0. [Accessed 2021].

[18] Will Spencer, "802.1Q," Tech-FAQ, 2019. [Online]. Available: https://www.tech-faq.com/8021q.html. [Accessed 2021].

[19] Computer Netowrking Notes, "How Switches Forward Frames Explained," Computer Netowrking Notes, 2019. [Online]. Available: https://www.computernetworkingnotes.com/ccna-study-guide/how-switches-forward-frames-explained.html. [Accessed 2021].

[20] Terry Slattery, "VLAN (virtual LAN)," Tech Target, 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/virtual-LAN. [Accessed 2021].

[21] Redscan Team, "Ten top threats to VLAN security," Redscan , 2021. [Online]. Available: https://www.redscan.com/news/ten-top-threats-to-vlan-security/. [Accessed 2021].