Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/10548
DOI URL: http://dx.doi.org/10.21474/IJAR01/10548

RESEARCH ARTICLE

IMPLEMENTATION OF VLAN AND INTER VLAN IN CORPORATE NETWORKS

Mrs. M. Sudha[1], Aishwaran K.[2], Arun A.[2], Jagadesh T.[2] and Japus Nelson[2]

1. Associate Professor, Department of ECE, Paavai Engineering College, Namakkal, Tamilnadu, India-637018.
2. WUG Students, Depaetment of ECE, Paavai Engineering College, Namakkal, Tamilnadu, India-637018.

Manuscript Info

Manuscript History
Received: 20 December 2019
Final Accepted: 22 January 2020
Published: February 2020

Abstract

The most of the organization uses computer network and it increases data due to the development of internet and computerizations which enable for file download, browsing internet and also make their work easier by sharing their files and folders. When no. of systems increases in computer network and it generates the heavy traffic and creates collision thus reduces network performance as well as the security. The overhead information increases due to broadcasting concepts and The traffic over the network address space utilization cannot be controlled by installing more routers or by increasing the size of the routing tables. Every system has given a unique IP address consisting of 32 bits specified in dotted decimal notation. To overcome from these issues we are using subnetting. The basic purpose of subnetting is to control the traffic over the networks and dividing one network into many smaller networks. An IP address consists of network number and host number therefore subnetting is dividing the network number part classes into pieces. In subnetting bits are borrowed from host ID part to the network ID part. It has network number, subnet number and host number. In this project subnetting improve the network performance and security and other parameters in the network for excellent communication.

Introduction:-

Local Area Network (LAN) is built with the help of network switches which by default creates a single flat network with large broadcast domain. The increase in the number of devices on LAN becomes paramount as we populate the network with more switches and workstations. Since most workstations tend to be loaded with existing operating system, it results in unavoidable broadcasts being sent occasionally on the network. Unfortunately, each host on such network cannot escape from the effects generated by such uncontrollable broadcast which decreases network performance. Security is never guaranteed in the above network infrastructure since all users are able to see all devices on local area network. In the case of Ebonyi University network having critical file servers, organizational databases and other confidential information, this would mean that everyone would have network access to these resources and naturally, they are prone to different attacks. To effectively regent such situations from operational network we need to restrict access by implementing Virtual Private Network (VLAN) which segments the existing network into different work groups.

Corresponding Author:- Mrs. M. Sudha
Address:- Associate Professor, Department of ECE, Paavai Engineering College, Namakkal, Tamilnadu, India-637018.

VLAN:
A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch. When you create VLANs, you're given the ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to service different sub- networks. A VLAN is treated as its own subnet or broadcast domain, meaning that any frames broadcast from Ebonyi State University Database Admin can only be switched between the ports logically grouped within the same Admin VLAN thereby restricting access from any other network groups within the University. By default, hosts in a specific VLAN can't communicate with hosts that are members of another VLAN. This concept of grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design and increase performance. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise- level networks today use the concept of virtual LANs. Therefore, in the absence of VLANs technology, a switch considers every its LAN ports to be in the same broadcast domain. VLAN design and implementation in Ebonyi State University can create lots of benefits. Here's a short list of ways VLANs simplify network management.

Flat Network Structure:
A flat network is a computer network design approach. The aim of the structure is to reduce cost, maintenance and administration. Flat network structures are designed in order to reduce the number of routers and switches on a computer network, Instead of separate devices connected to multiple switches, The Flat structure network connects all the devices to a single switch.

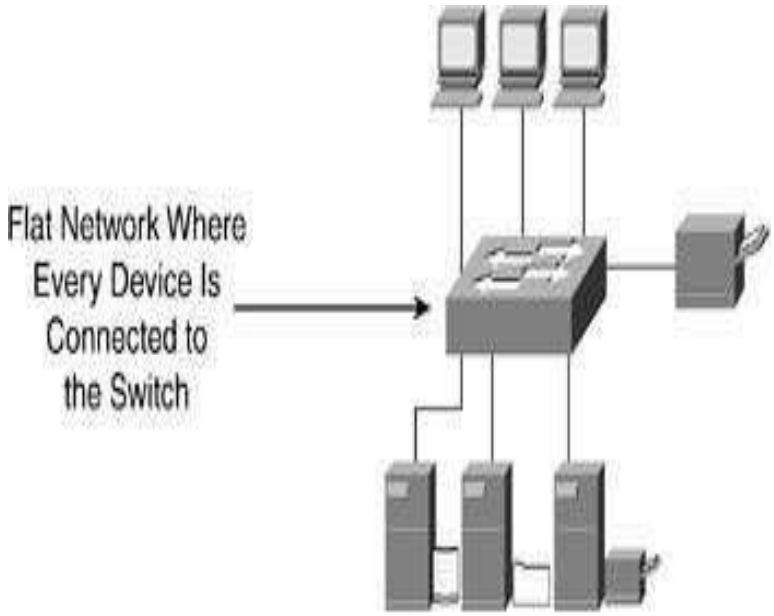

Figure1:- Flat Network Structure.

VLAN Network:
VLANs are used to simplify the network management. Network adds, moves, and changes can be achieved very easily by configuring a port into its appropriate VLAN. It provides high level of security to a group of users, where the group of users can be put into its own VLAN, so, the users which is outside of the VLAN cannot communicate with that particular group of users.

Classified into two:
Static VLANs:
These VLANs are created by network administrator, where the network administrator provides more security to VLANs. VLAN will always maintain any switch port that is assigned to it, unless one change in the port VLAN MEMBERSHIPS VLAN memberships is which assign manually. Static VLANs are very easy to set up, and

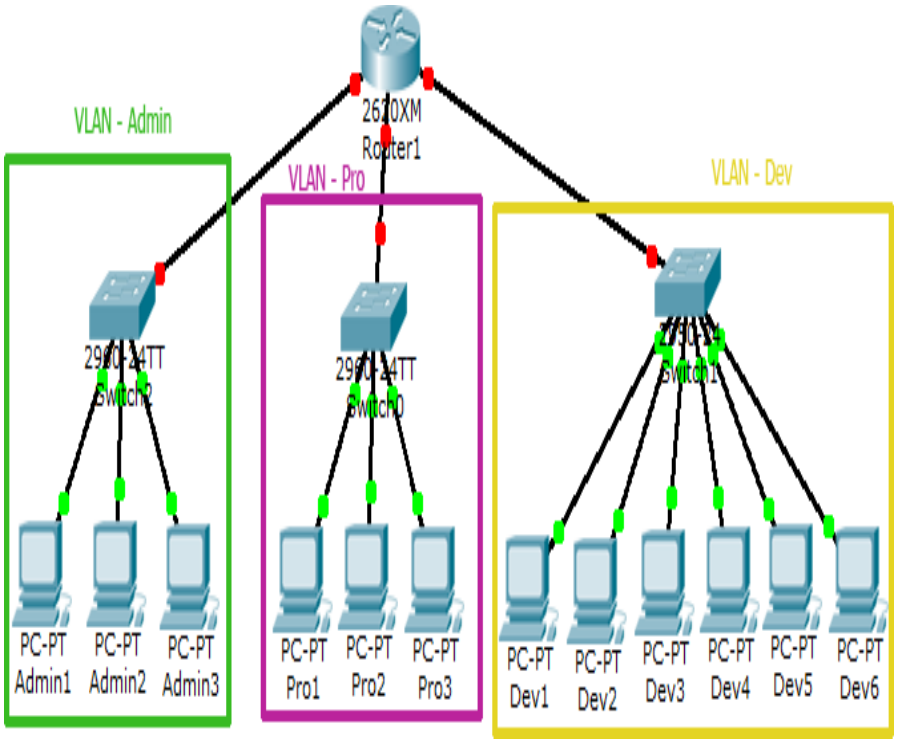

Figure2:- VLAN Network.

If there is any change in the host, then a manual update us required. Larger networks that requires more updates regarding VLAN are not possible statically, so it is routed to dynamic VLANs.

Dynamic VLANs:

Dynamic VLANs uses software for assigning the VLANs automatically, and it is based on the hardware address (MAC), protocols and applications. For example, In a centralized VLAN management application software, If a MAC address has entered into it, If you are attaching it to an unassigned switch port, The VLAN management database will be searching the hardware address regarding to the MAC address, and It will assign and configure that switch port to the correct VLAN. At initial level, it is very tough to setup a database.

Identifying Vlans:

A switch port is an interface that is associated with the physical port, where the switch port can belong to one VLANs or all VLANs. The ports of the VLAN can be configured manually. If the switch port is an access port, then it is one VLAN. If it is a trunk port, then it is all VLAN. To set the switch port mode, Dynamic Trunking Protocol will be operating on a per-port basis. It is possible by neglecting the port at the other end of the link. There are two different types of links in switched network:

Access ports:

Access link connection is that, where the switch port is connected with a device that has a standardized Ethernet NIC. It understands only IEEE 802.3 or Ethernet II frames. Access port can be assigned only with the single VLAN.

Vlan Identification:-

VLAN Identification is that, switches can track all the frames that are travelling in a switched network. In this way, switches identify which frames belong to which VLANs. This method is also called as frame Identification method. In this method each frame can be assigned a user ID. There are more trunking methods.

Inter-Switch link (ISL):

This protocol primarily is used for the ethernet media. That is, it is only used in fast ethernet and gigabit ethernet links only. It is a versatile routing method and it can used as switch port, router interface and server interface cards to trunk a server. ISL is the pathway where the VLAN information is tagged onto a ethernet frame. Switches can identify the

VLAN membership of a frame; it is possible only if the tagging information allows the VLANs to be multiplexed over the trunk through ISL.

IEEE802.1Q:
It is the standard created by IEEE for frame tagging. In order to identify a VLAN, IEEE802.1Q inserts a field into the frame. If you've to trunk between the cisco switched link and a different band of switch, then you've to use 802.1Q for the trunk to work. The basic purpose of these two trunking methods is to provide inter- switch VLAN communication.

Routing between Vlans:
Each VLAN has their own subnet and broadcast domain, where the frames which are broadcasted onto the networks can be switched only between the ports within the same VLAN, and it can communicate freely. VLANs create network partitioning and separation at the layer2 of the OSI. A layer 3 device is necessary in order to create communication between the host or any other IP addressable devices and the VLANs. A router can be used which has an interface or a router that supports ISL OR 802.1Q routing.

Advantages of using Vlans:
Cost and time reduction: It can reduce the migration cost of stations moving from one group to another. It takes more time for physical reconfiguration, and the process is more costly. It is very easier and also very quicker to move it by using software, instead of moving the stations from one to another.

Security: The network cannot be used by third party user easily.

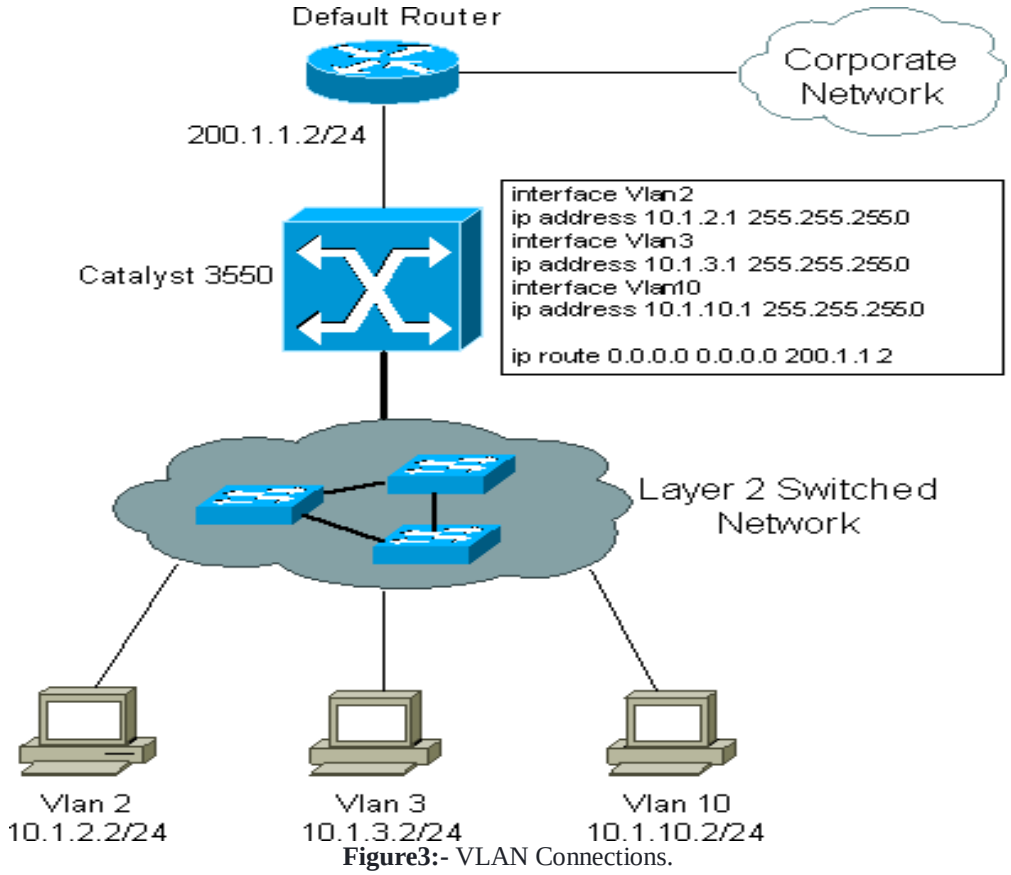

Figure3:- VLAN Connections.

References:-

1. Ahmed Abdelhalim, "IP/MPLS-Based VPNs Layer-3 vs. Layer-2", Foundry Networks, Inc. June 2003.
2. Ankur Dumka, IEEE paper on " MPLS VPN using IPv4 Ankur Dumka, IEEE paper on "layer 3 services implementation on different routers".

3. Cisco "MPLS VPN Technology" Chris Metz "The Latest in VPNs: Part II" published by the IEEE Computer Society May 2004.
4. Dr. Hosein F. Badran, "Service Provider Networking Infrastructures with MPLS" in Sixth IEEE Symposium on Computers and Communications (ISCC'01) July 05, 2001.
5. E. Rosen, Y. Rekhter, "BGP/MPLS VPNs" RFC 2547, March 1999.
6. Francesco Palmieri, "Evaluating MPLS VPN against traditional approaches", Eighth IEEE Symposium on Computers and Communications (ISCC'03), June 30, 2003.
7. M. El Hachimi, M.-A Breton, and M. Bennani, "Efficient QoS Implementation for MPLS VPN", International Conference on Advanced Information Networking and Applications, pp. 259-263,March 2008.
8. R. Pulley: "Implementing VPNs Using MPLS", Proceedings of MPLS Forum 2000, 2000.
9. S. Previdi: "Introduction to MPLS-BGP-VPN", Proceedings of MPLS Forum 2000, 2000.
10. M.Sudha, J.Sundarrajan " Energy Efficient Conservation Routing Technology for WSN with node mobility"Middle East Journal of Scientific Research,Vol.24,Issue 1,pp:103-112,2016,ISSN : 1990-92.