International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Study on Virtual Local Area Network (VLAN) Management

Amar Bahadur Haricharan Jaiswar, Balasubramanian Perumal

Department – Inft, Vesit, Chembur Mumbai - 400074

Abstract : This article consists of the implementation of a VLAN network in the education sector like College & school. The objective is to increase information security & avoiding broadcasting in networks, as well as to improve and optimize user data, and this is achieved through the development and use of different protocols, restrictions, and methods that helped to achieve this purpose. These phases focused on analyzing, developing, and improving the different processes for designing and implementing a VLAN network topology. As a technique, an interview was conducted with the person who handled the college network expressing their opinion on the college's problems under study. Data processing was carried out at a qualitative level using HA SOPHOS XGS 5500 FIREWALL DEVICE and managed switches, which allowed internet access to all students and staff. This information was used to obtain the data for the research work. The result was a slow bandwidth and broadcasting in network with the system they are currently using. In addition, the conclusion obtained was that in view of the existing problems, the experts indicated that the proposal related to the implementation of a VLAN Network would meet the desired expectations, providing security to the information, so they consider it a feasible and appropriate option that would be a great alternative for the improvement of the college.

Keywords: VLAN network, IP address allocation, Information security, Network topology, Inter Switch Link,Top-down methodology.

Introduction : A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.
A LAN is a group of computers or other devices in the same place -- e.g., the same building or campus -- that share the same physical network. A LAN is usually associated with an Ethernet (Layer 2) broadcast domain, which is the set of network devices an Ethernet broadcast packet can reach.
A VLAN allows you to take one physical switch, and break it up into smaller *mini-switches*.
One of the biggest problems of a switch is that Switch creates one large broadcast domain. Let’s consider a typical 48 port switch, A single broadcast generated from one single user in a LAN supported by L2 switch, will be broadcasted in the whole LAN and all other users in the same LAN have to Listen to the same broadcast even though it’s not addressed to them. This will consume the Bandwidth of the network and also the CPU cycle. To solve this problem, we can virtually break this one large broadcast domain into multiple domains. Which means one switch can act as multiple switches. VLAN’s also allow us to provide security by denying access to members of one VLAN to another unless it was authorized. In this paper we will demonstrate how to set up a virtual LAN and communicate among one another by breaking broadcast domains.

Switch Ports :
A Switch has two types of ports in VLAN.
1. Access Ports
2. Trunk Ports

Access Ports:
Ports which connect end Users are called Access ports. Access ports belong to one single VLAN and it carries only traffic of one single VLAN. No control information (TAGS) will be added in the packets flowing through access ports. Any device connected to any switch doesn't know anything about VLANS. It only knows that it belongs to some VLAN. If a switch receives any Packet with TAGS attached, Switch will remove the TAGS before forwarding the packet to the respective device connected on the Access lines. Any physical port can either be an Access port or trunk port.

Trunk Ports:
Trunk ports are used to carry multiple VLAN traffic on a single Link. It's like multiplexing multiple source traffic onto a single line, and how the traffic can be distinguished at the other end. For this we use TAGS. Each VLAN has its own tags which are added to the traffic when the packet leaves the switch trunk port. Figure 1 shows the difference between the normal Ethernet frame and the VLAN encapsulated frame.

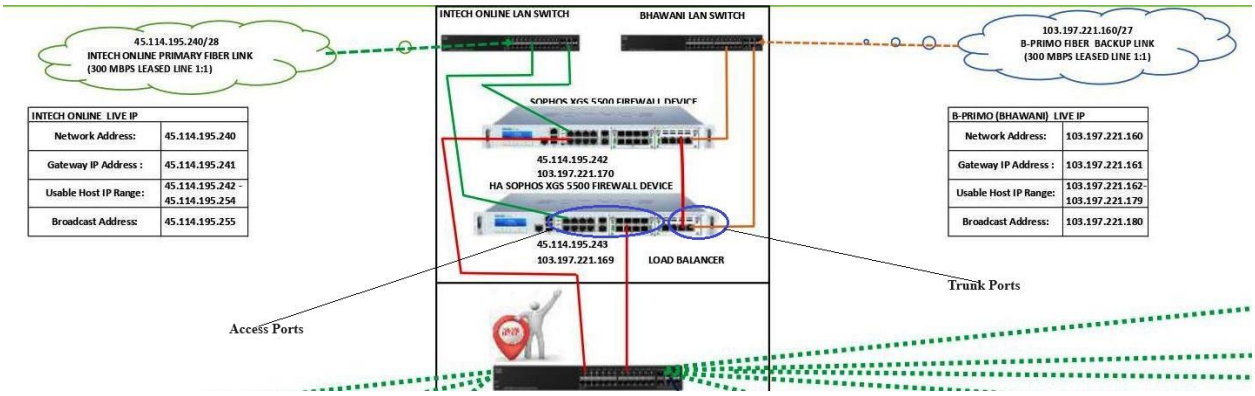

Fig.1

IP address allocation : An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.IP addresses are not random. They are mathematically produced and allocated by the Internet Assigned Numbers Authority (IANA), a division of the Internet Corporation for Assigned Names and Numbers (ICANN).
IP addresses are allocated to each TCP/IP services address on a TCP/IP Internet. Each address is a unique 32-bit (an IPv4 Internet Address) or a unique 128-bit (an IPv6 Internet Address) quantity defining the host's network and the particular host. A host can have more than one IP address if it is connected to more than one network (a so-called multihomed host).
Conclusion : Our aim in VLAN management is to eliminate duplicate IP addresses which have been formed because of routers connected inside a particular VLAN.
When VLAN is created different VLAN ID & VLAN names are created. In our case VLAN ID - I is for Trunk
VLAN ID-2 is for staff
VLAN ID -3 is for student
VLAN ID - 4 is for wifi access.
In this scenario we have multiple Labs where different types of experiments are conducted as a port of academic study work which is the student Lab experiments.

Every computer system is connected to a particular VLAN under LAN connected to ISP.

Some experiments are in VMware, Where VMware software is installed & experiments are performed in this software. Here VMware sometimes acts as a DHCP server who distributes IP of the same range as in particular VLAN, in this case network flooding is created & network traffic is increased. So particular VLAN ID is slowed down gradually & internet connection is slowed down gradually & internet connection is slowed as increase in network traffic. This is a big issue where VLAN ID does not work until the problem of flooding is solved.

Our solution here is to isolate the VLAN first & test for network traffic then connect each lab in the network of VLAN & see for traffic in network, by connecting one by one lab in network we can find out the lab which is crating flooding in network, then we identify particular machine i.e. computer in the network & rectify the issue by disabling DHCP server of the VMware system.

But the above solution is consuming in finding issues created. So we are forced to implement a system where VLAN traffic can be indetried. Then our system will identify real traffic & fake traffic there by solving the issues in a simple way just by monitoring the VLAN management system.