VPN vs VLAN

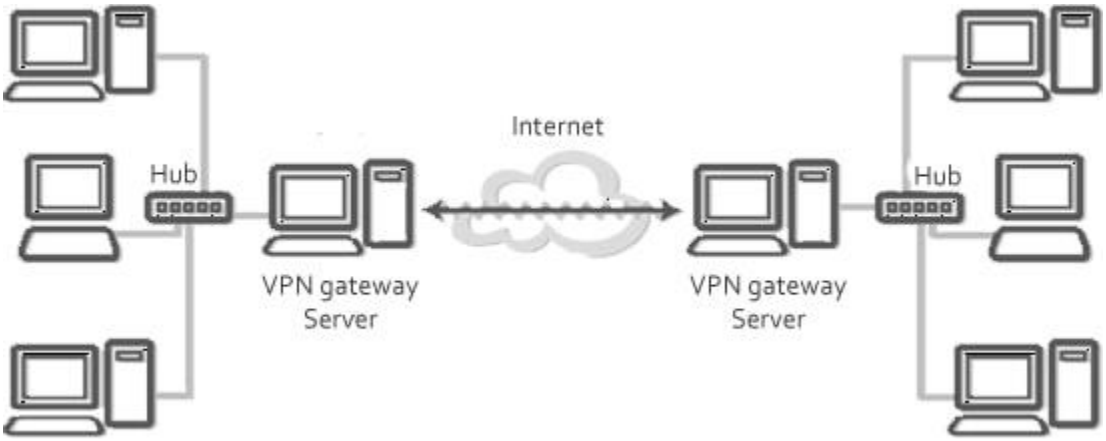
A Local area network is defined as a network of computers that is located in the same area and this means that when a user broadcasts any information on the LAN, the broadcast is received by every user on the LAN. But the only issue with LAN is that if two people send information at the same time, there will be a collision that occurs and the data that is transmitted will be lost. The area where the data is broadcast is called the broadcast domain but everyone on the LAN has to be in the same area. It is here that VLAN or Virtual LAN allows the network manager to effectively segment a LAN into diverse broadcast domains and it is not essential for the workstations to be physically located together. Users can be on different floors of the same building or even in different buildings.

Understanding VLAN

With companies increasing their means of communication between employees, the networks have also grown over the years. Unsecured networks mean unauthorized people gaining access to confidential information. It is for this reason that companies are more concerned about the security mechanism and malicious attacks.

VLANs (Virtual Local Area Networks) are a logical group of networking devices, workstations, and servers that are connected to the same physical LAN, regardless of how they are geographically distributed. A VLAN enables several networks to communicate with each other in a simulated environment as if they are on a single LAN and sharing a single broadcast as well as multicast domain.

Organizations implement VLANs because of their security, scalability, and not to mention, ease of network management. The implementation and functionality of VLANs is made possible via higher-end switches. The main purpose of a VLAN is to enhance the network performance or apply suitable security features.



What is VPN?

VPN or Virtual Private Network can be defined as a secured means of connecting to the private network through a public network that is not very much safe. Usually the data that is sent through unsecure public network is not encrypted for security and there is a high possibility that the data can be easily accessed and misused. Organizations that are concerned about the safety of their data take a VPN connection so that they can share the data and other network resources with people located in remote areas. A VPN connection reduces the network cost of an organization and removes the need of having leased lines to connect organization's network in various locations.

Difference between a VLAN and VPN?

- A VLAN helps to group workstations that are not within the same locations into the same broadcast domain and VPN is related to remote access to the network of a company.
- VLAN is a subcategory of VPN and VPN is a means of creating a secured network for safe data transmission.
- A VLAN is basically a means to logically segregate networks without physically segregating them with various switches. A VPN is used to connect two points in a secured and encrypted tunnel.
- A VPN saves the data from prying eyes while in transit and no one on the net can capture the packets and read the data. VLAN does not involve any encryption technique but it is only used to slice up your logical network into different sections for the purpose of management and security.
- VLAN is generally used when it is necessary for a person to connect with someone whom you cannot connect from outside the VLAN. It requires a

special permission before access. VPN is used to communicate in a secured manner in an unsecured environment.

Summary

Both VPN and VLAN are extended communications across multiple business options with secured and fast connections. Organizations that are looking for smaller networks over their existing bigger networks and want to securely access remote company networks can use VLAN and VPN. They have different functions and help in managing the connections and providing a safe environment for data transfer.