Atharva Yadav
Roll No. 127
Batch : s23

1. Explain in detail VLAN

VLAN stands for Virtual Local Area Network. It's a method of logically segmenting a single physical network into multiple distinct virtual networks. These virtual networks operate as if they are physically independent, even though they may share the same physical infrastructure. VLANs offer several benefits, including increased security, improved network performance, and simplified network management.

Purpose:

- VLANs are primarily used to improve network performance, security, and scalability.
- They allow network administrators to logically group devices together based on factors such as department, function, or security requirements, regardless of their physical location.

How VLANs Work:

- VLANs are created by assigning ports on network switches to specific VLANs.
- Switches use a process called VLAN tagging to identify which VLAN a packet belongs to. This tagging adds a small piece of extra information to the Ethernet frame, indicating the VLAN membership of the packet.
- When a switch receives a packet, it examines the VLAN tag and forwards the packet only to the ports assigned to the same VLAN as the source of the packet.

Benefits:

- *Improved Security*: VLANs can enhance network security by isolating sensitive data or critical systems from other parts of the network. For example, finance department computers can be placed on a separate VLAN to prevent access from other departments.
- *Better Performance*: By segregating network traffic, VLANs can reduce broadcast traffic and congestion, leading to improved overall network performance.

2.

a. HTTP (Hypertext Transfer Protocol): HTTP is the foundation of data communication on the World Wide Web. It defines how messages are formatted and transmitted, enabling web browsers to retrieve and display web pages. HTTP operates on a client-server model, facilitating the exchange of hypertext documents.

b. SNTP (Simple Network Time Protocol): SNTP is a simplified version of NTP (Network Time Protocol) used for synchronizing the time of networked devices. It ensures accurate timekeeping by synchronizing devices' clocks to a reference time source over a network, vital for tasks such as logging and security protocols.

c. FTP (File Transfer Protocol): FTP is a standard network protocol for transferring files between a client and a server on a computer network. It offers a straightforward method for uploading, downloading, and managing files across the internet. FTP operates on a client-server architecture with control and data connections.

d. DNS (Domain Name System): DNS translates domain names to IP addresses, facilitating human-readable web addresses. It functions as the internet's address book, mapping domain names like example.com to their corresponding IP addresses. DNS operates in a distributed hierarchical system, translating domain names into IP addresses and vice versa.

e. SNMP (Simple Network Management Protocol): SNMP is an internet standard protocol for collecting and organizing information about managed devices on IP networks. It enables network administrators to monitor network performance, detect and resolve issues, and manage network devices such as routers, switches, and servers remotely.