9. VPN, VLAN, I2P

VPN

A VPN, or Virtual Private Network, is a technology that creates a secure and encrypted connection over a less secure network, such as the Internet. It allows users to send and receive data as if their devices were directly connected to a private network.

Key features of a VPN include:

1. **Privacy and Anonymity**: By masking the user's IP address, a VPN helps protect their identity and online activities from being tracked by websites, ISPs, or government entities.
2. **Security**: VPNs encrypt data, making it difficult for hackers to intercept and read information, especially on public Wi-Fi networks.
3. **Access to Restricted Content**: VPNs can help users bypass geo-restrictions and access content that may be blocked in their region, such as streaming services or websites.
4. **Remote Access**: VPNs enable remote workers to securely connect to their company's internal network from anywhere, ensuring that sensitive data remains protected.

SSL VPN:

An SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses SSL or its successor, TLS (Transport Layer Security), to provide secure remote access to a network. Unlike traditional VPNs that often require specialized client software, SSL VPNs can typically be **accessed through a standard web browser**, making them more user-friendly and easier to deploy.

- **Definition**: A Secure Sockets Layer Virtual Private Network (SSL VPN) uses SSL/TLS protocols to secure internet connections for remote access to private networks.
- **Security**: Employs SSL/TLS encryption to protect data during transmission, ensuring confidentiality and integrity.
- **Access Control**: Provides granular permissions, allowing administrators to specify user access to resources based on roles and credentials.
- **Clientless Access**: Supports web-based access, enabling users to connect without installing additional software.

Use Cases:

- **Remote Work**: Employees can securely access company resources from remote locations.
- **Secure Browsing**: Users can protect their online activities when using public Wi-Fi networks.
- **Access to Internal Applications**: Organizations can provide secure access to internal applications without exposing them directly to the internet.

VLAN

A VLAN, or **Virtual Local Area Network**, is a logical grouping of devices within a physical network that allows them to communicate as if they are on the same local network, regardless of their actual physical location. VLANs are used to segment networks for improved performance, security, and management.
Generally, layer 3 devices.

> VLANs, or Virtual Local Area Networks, are a technology used to segment a physical network into multiple logical networks

Using VLANs to group endpoints also enables administrators to group devices for purely administrative, nontechnical purposes.

> VLAN 1 can't talk VLAN 2 even both are on 1 switch
> we can **create vlan as much we want** because its on logical based managed by software. limitation of 4096 vlans as far as i remember

The purpose of a VLAN

Network engineers use VLANs for multiple reasons, including the following:

- to improve performance
- to tighten security
- to ease administration

HOW VLAN WORKS ?

A VLAN (Virtual Local Area Network) is identified by a VLAN ID on network switches, allowing each port to be assigned one or more VLAN IDs. If no VLAN ID is assigned, the port defaults to a standard VLAN. Each VLAN provides data-link access to all hosts connected to its configured ports.

VLAN IDs are translated into VLAN tags, which are 12-bit fields in the Ethernet frame headers, allowing for up to 4,096 VLANs per switching domain, as defined by the IEEE 802.1Q standard. When an Ethernet frame is received without a VLAN tag, the switch adds one based on the port's VLAN ID (static VLAN) or the device's ID/type of traffic (dynamic VLAN).

Switches forward tagged frames to the appropriate media access control addresses, only to ports associated with the VLAN. Broadcast, unknown unicast, and multicast traffic are sent to all ports within the VLAN. Trunk links between switches carry traffic for all VLANs in use, and the VLAN tag is removed before the frame reaches its destination device.

The Spanning Tree Protocol (STP) ensures a loop-free topology among switches in each Layer 2 domain, with options for per-VLAN STP instances or multi-instance STP to optimize performance across similar topologies.

Types of VLANs:

1. **Data VLAN**: Used for user data traffic, allowing devices to communicate within the same VLAN.
2. **Voice VLAN**: Specifically designed for voice traffic, ensuring quality of service (QoS) for VoIP (Voice over Internet Protocol) communications.
3. **Management VLAN**: Used for network management traffic, allowing administrators to manage network devices securely.
4. **Native VLAN**: The default VLAN for untagged traffic on a trunk port, which is used to carry traffic from multiple VLANs.

Use Cases:

- **Enterprise Networks**: VLANs are commonly used in corporate environments to separate departments, such as HR, finance, and IT, enhancing security and performance.
- **Educational Institutions**: Schools and universities can use VLANs to separate student, faculty, and administrative networks.
- **Data Centers**: VLANs help manage traffic and resources efficiently in data center environments.

I2P

Invisible internet project (I2P) based on P2P.
Its more sure than TOR as it is decentralized.

P2P Peer to Peer (P2P)

Peer-to-peer (P2P) is a decentralized communication model in which computers or devices in a network share resources and information directly with each other, without the need for a central server or authority.
In a P2P network, each computer or device can function both as a client and a server. This means that each device is both a consumer and a provider of resources, such as processing power, bandwidth, storage, and content. This allows P2P networks to scale efficiently, since each device contributes to the network's overall capabilities.
P2P networks are commonly used for file sharing, messaging, and other forms of decentralized communication. Examples of P2P networks include BitTorrent, Gnutella, and Napster.