Modue_5 :Network Design Concepts

Introduction to VLAN, VPN.

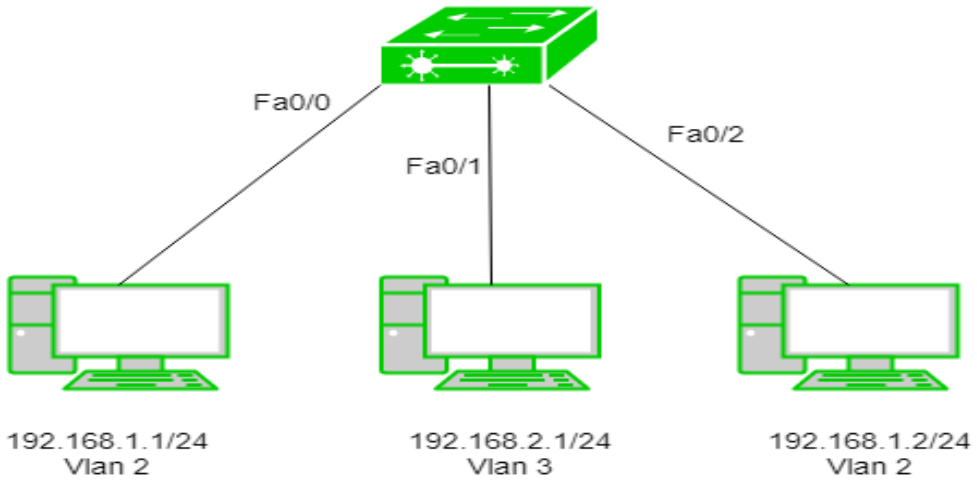
Virtual LAN (VLAN)

Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter Vlan routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

LAN ranges:

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1:** It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.
- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094:** This is the extended range of Vlan.



VLANs offer several features and benefits, including:

- **Improved network security:** VLANs can be used to separate network traffic and limit access to specific network resources. This improves security by preventing unauthorized access to sensitive data and network resources.
- **Better network performance:** By segregating network traffic into smaller logical networks, VLANs can reduce the amount of broadcast traffic and improve network performance.
- **Simplified network management:** VLANs allow network administrators to group devices together logically, rather than physically, which can simplify network management tasks such as configuration, troubleshooting, and maintenance.
- **Flexibility:** VLANs can be configured dynamically, allowing network administrators to quickly and easily adjust network configurations as needed.
- **Cost savings:** VLANs can help reduce hardware costs by allowing multiple virtual networks to share a single physical network infrastructure.
- **Scalability:** VLANs can be used to segment a network into smaller, more manageable groups as the network grows in size and complexity.

Some of the key features of VLANs include:

- **VLAN tagging:** VLAN tagging is a way to identify and distinguish VLAN traffic from other network traffic. This is typically done by adding a VLAN tag to the Ethernet frame header.
- **VLAN membership:** VLAN membership determines which devices are assigned to which VLANs. Devices can be assigned to VLANs based on port, MAC address, or other criteria.
- **VLAN trunking:** VLAN trunking allows multiple VLANs to be carried over a single physical link. This is typically done using a protocol such as IEEE 802.1Q.

- **VLAN management:** VLAN management involves configuring and managing VLANs, including assigning devices to VLANs, configuring VLAN tags, and configuring VLAN trunking.

Types of connections in VLAN –

There are three ways to connect devices on a VLAN, the type of connections are based on the connected devices i.e. whether they are VLAN-aware(A device that understands VLAN formats and VLAN membership) or VLAN-unaware(A device that doesn't understand VLAN format and VLAN membership).

1. **Trunk Link –**
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access link –**
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames on the access link must be untagged.
3. **Hybrid link –**
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

Advantages –

- **Performance –**
  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups –**
  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.

- **Security –**

  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.

- **Flexibility –**

  VLAN provide flexibility to add, remove the number of host we want.

- **Cost reduction –**

  VLANs can be used to create broadcast domains which eliminate the need for expensive routers.

  By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

Disadvantages of VLAN

1. **Complexity:** VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.
2. **Limited scalability:** VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.
3. **Limited security**: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.
4. **Limited interoperability**: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.
5. **Limited mobility**: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.
6. **Cost:** Implementing and maintaining VLANs can be costly, especially if specialized hardware or software is required.

7. **Limited visibility:** VLANs can make it more difficult to monitor and troubleshoot network issues, as traffic is isolated in different segments.

Real-Time Applications of VLAN

Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:

1. **Voice over IP (VoIP)** : VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.
2. **Video Conferencing** : VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.
3. **Remote Access** : VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users from the rest of the network.
4. **Cloud Backup and Recovery** : VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.
5. **Gaming** : VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.
6. **IoT** : VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion.

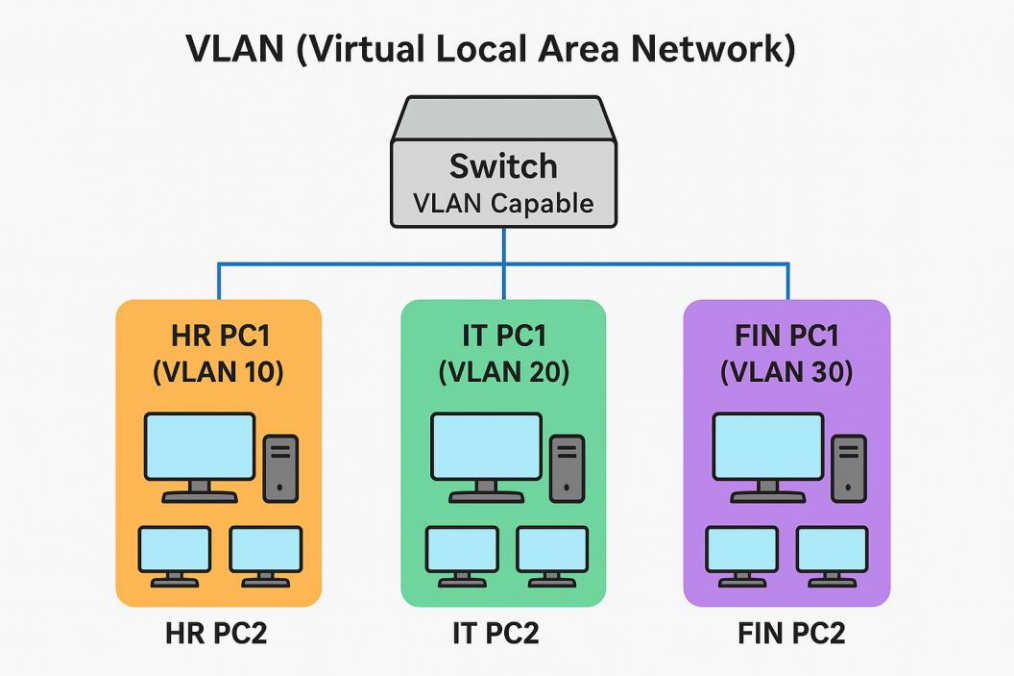
VPN in Computer Networks

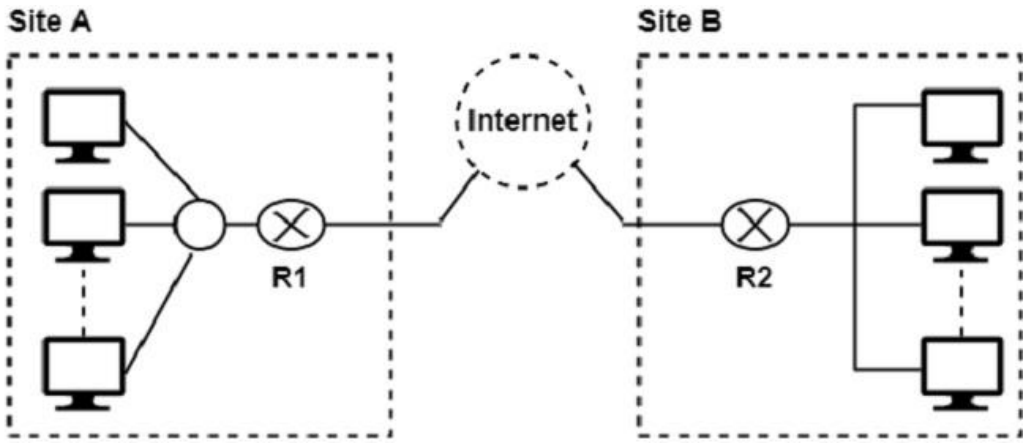
What is VPN in Computer Networks?

A **VPN (Virtual Private Network)** is a powerful tool that enhances **online privacy**, protects sensitive data, and enables secure access to the internet. In today's interconnected world, **online privacy** and **data security** are more important than ever. One of the best ways to protect yourself and enhance your internet experience is by using a **VPN (Virtual Private Network)**. Whether you're looking to **secure your data**, **bypass geo-restrictions**, or simply want to **maintain your anonymity online**, a VPN is an invaluable tool.

VPN Connection Diagram

A VPN connection is shown in the figure below





In this figure, Routers R1 and R2 use VPN technology to guarantee privacy for the organization.

What Is a VPN?

A **VPN (Virtual Private Network)** is a technology that creates a secure, encrypted connection between your device and the internet. It essentially acts as a private tunnel for your internet traffic, preventing hackers, ISPs, and even governments from monitoring your activities. When

using a VPN, your **IP address** is masked, and your online actions are routed through a remote server, making it harder to track your online activity.

Key Benefits of Using a VPN:

1. **Privacy Protection**: A VPN hides your IP address, ensuring that your browsing habits and activities remain private.
2. **Security on Public Networks**: Public Wi-Fi networks are often insecure, but a VPN encrypts your connection, making it safer to browse the internet on networks like those in cafes or airports.
3. **Bypass Geo-restrictions**: A VPN allows you to access content that may be blocked in certain regions (such as streaming platforms, social media sites, etc.).
4. **Prevent Data Throttling**: Some ISPs throttle your connection speed when you stream or play games. A VPN can bypass this, allowing for faster internet speeds.
5. **Accessing Remote Work Resources**: A VPN enables secure access to private networks, making it ideal for businesses and remote workers.

How Does a VPN Work?

A VPN works by creating an encrypted tunnel between your device and a remote server. Here's the process simplified:

1. **Connection Establishment**: When you activate a VPN on your device, it connects to a server operated by the VPN provider.
2. **Encryption**: The VPN encrypts your data (information, files, web traffic) so that it's unreadable to anyone trying to intercept it, whether it's a hacker on the same Wi-Fi network or an entity trying to monitor your browsing.
3. **Traffic Redirection**: Your device's internet traffic is routed through the VPN server, which can be located in any country. This makes it appear as though you're browsing from the server's location, masking your actual IP address.
4. **Decryption**: Once your data reaches the VPN server, it is decrypted and sent to the destination (such as a website, app, or service). Any response from the server is then sent back to you through the encrypted tunnel.

This **end-to-end encryption** ensures that your sensitive data stays private and your location remains anonymous.

Types of VPN

VPNs come in various types, each catering to different needs, from individual privacy to enterprise-level solutions. Below are the main types of VPNs:

1. Remote Access VPN

A **Remote Access VPN** allows individual users to connect to a network remotely, such as accessing work files from home. It's ideal for people who need secure access to a private network from anywhere.

2. Site-to-Site VPN

A **Site-to-Site VPN** is used to connect two networks, often used by businesses with multiple office locations. It securely links two private networks over the internet, enabling employees to access resources from both locations.

3. Mobile VPN

A **Mobile VPN** is designed for mobile devices like smartphones and tablets. It ensures stable connections even when switching between different networks (such as from Wi-Fi to mobile data) and is used in industries like healthcare and logistics where users need continuous access while moving.

4. MPLS VPN (Multiprotocol Label Switching)

An **MPLS VPN** is used mainly by large businesses and enterprise networks. It routes data between different locations through an efficient network that prioritizes data traffic. It's often more complex and provides more scalability compared to traditional VPNs.

5. PPTP VPN (Point-to-Point Tunneling Protocol)

PPTP is one of the oldest VPN protocols and is known for being fast but less secure compared to others. It is rarely used in modern systems due to its vulnerabilities, but it's still available on some legacy systems.

6. L2TP/IPsec VPN (Layer 2 Tunneling Protocol with IPsec)

L2TP combined with **IPsec** offers more security than PPTP. It uses encryption to secure data, making it a popular option for users who need a reliable, moderately secure connection.

7. OpenVPN

OpenVPN is a highly secure, open-source VPN protocol known for its flexibility and strength in encryption. It's often used for custom VPN setups and is highly configurable, making it a popular choice for advanced users.

8. IKEv2/IPsec VPN (Internet Key Exchange version 2)

IKEv2 is a fast, stable, and secure VPN protocol that works well on mobile devices. It automatically reconnects when the device switches between networks, providing continuous service without interruptions.

Differences Between VPN And VLAN

Parameter of Comparison	VLAN	VPN
Full Form	Virtual Local Area Network (VLAN)	Virtual Private Network (VPN)
Types	Type of VLAN: 1. Port-based VLAN 2. Protocol-based VLAN 3. MAC-based VLAN	Type of VPN: 1. Remote Access VPN 2. Site-to-Site VPN
Kind of service	VLANs are the kind of subnetworks	VPNs are the technology a service

Take help of	**VLANs use virtual LANs to segment traffic**	**VPN uses encryption to create a virtual private network**
Purpose	**Help in connecting multiple devices that are separated by distance**	**Help in connecting authorization personals**
hierarchical structure	**VLAN is a subset of the VPN**	**VPN is a superset of VLAN**
Definition	**use to consolidate(or strong) devices that are separated, into a single Broadcast Domain**	**use to transmit secure data**
Tunnel/channel	**VLAN does not use any kind of tunnel**	**VPN uses a virtual tunnel for secure connection**
Security	**less secure as compared to VPN**	**more secure**
Price	**VLANs are cheap**	**VPNs are expensive**

Efficiency	**VLAN is less efficient as compared to the VPN**	**VPN increases the efficiency**

Similarities Between VPN And VLAN

Despite being so many differences between VLAN and VPN, there are multiple similarities between them,

- **In terms of network scalability both VPN and VLAN allow multiple institutes and corporates to maintain their webbing more effectively.**
- **VPN and VLAN both can be used to enhance privacy or security by encrypting the network traffic.**
- **VPN and VLAN can be used to improve network security.**
- **As far as route traffic is concerned both VPN and VLAN use IP addresses.**
- **Within the physical network layer VPN and VLAN both are used to create independent virtual networks.**
- **Both are used in saving the cost of the different institutes and corporate by reducing the need for physical network components**