VPN and VLAN

UNIT 2

What is a VPN?

- A VPN or Virtual Private Network creates a private network connection between devices through the internet.

- VPNs are used to safely and anonymously transmit data over public networks.

- They work by masking user IP addresses and encrypting data so it's unreadable by anyone not authorized to receive it.

What is a VPN used for?

VPN services are mainly used to safely send data over the internet. The three main **functions** of VPNs are:

1. Privacy

- Without a virtual private network, your **personal data** like **passwords**, **credit card** information, and **browsing history** can be recorded and sold by third parties. VPNs use encryption to keep this confidential information private, especially when connecting over **public wi-fi** networks.

2. Anonymity

- Your **IP address** contains **information** about your **location** and **browsing activity**. All websites on the Internet track this data using **cookies** and similar technology. They can identify you whenever you visit them. A VPN connection hides your IP address so that you remain anonymous on the Internet.

3. Security

- A VPN service uses **cryptography** to protect your internet connection from unauthorized access. It can also act as a **shut-down mechanism**, terminating pre-selected programs in case of suspicious internet activity. This decreases the likelihood of data being compromised. These features allow companies to give remote access to authorized users over their business networks.

How does a VPN work?

A VPN connection redirects data packets from your machine to another remote server before sending them to third parties over the internet. Key principles behind VPN technology include:

- **Tunneling protocol**
- **Encryption**

How does a VPN work?

Tunneling protocol

- A virtual private network essentially creates a **secure data tunnel** between your **local machine and another VPN server** at a location that is thousands of miles away. When you go online, this VPN server becomes the source of all your data. Your Internet Service Provider (ISP) and other third parties can no longer see the contents of your internet traffic.

Encryption

- VPN protocols like **IPSec** scramble your data before sending them through the data tunnel. IPsec is a **protocol suite** for securing Internet Protocol (IP) communications by **authenticating and encrypting each IP packet** of a data stream. The VPN service acts as a filter, making your data unreadable at one end and only decoding it at the other — this prevents personal data misuse, even if your network connection were to be compromised. Network traffic is no longer vulnerable to attack, and your internet connection is secure.

Why should you use a VPN?

- **For safe public internet access**
- **For keeping your search history private**
- **For accessing streaming services globally**
- **For protecting your identity**

How to set up a VPN?

There are two common ways to access VPN services for individuals:

1. Use a VPN provider

- You can choose a **VPN service** that can be **accessed** either from your **browser** or by **downloading an app or software** to your device. These are **subscription-based** services that typically charge on a per device basis. Hence they can be quite **expensive** to set up. Also, each device needs to be configured individually.

2. Use a VPN router

- This involves either purchasing a **router with a VPN connection pre-installed** or **installing VPN software** yourself on your home router. The advantage of this approach is that every device accessing the internet via this router gets protected automatically.

How to choose the best VPN provider?

1. Logging policies

- The best VPN providers have **minimal or no-logging policies** to **prevent data breaches** from their end.

2. Updated software

- The best VPN connections use the **latest tunneling protocol**. **OpenVPN** protocol provides more robust security than others. It is open-source software that is compatible with all major operating systems.

3. Bandwidth limit

- All services have **data usage limitations**. You will need to choose a VPN provider that meets your data needs within budget.

4. VPN server locations

- You have to ensure that your VPN provider has a server located in the country where you require private internet access.

How do businesses use VPNs?

There are three main ways that businesses use a VPN:

1. **Site to site VPN**

A site-to-site VPN acts as an **internal private network for companies** with **multiple geographically separated locations.** It seamlessly and securely **connects different intranets**, allowing employees to share resources between different internal networks.

2. Client VPN or open VPN (Remote Access VPN)

In Client VPN, the **network administrator** is responsible for **setting up and configuring the VPN** service. The configuration file is then **distributed to the clients**, or end-users, who need access. The client can then establish a VPN connection from their local computer or mobile device to the company network.

3. SSL VPN

Secure Sockets Layer Virtual Private Network (SSL VPN) provides secure **remote access** via a **web portal and an SSL-secured tunnel** between a private device and the office network.

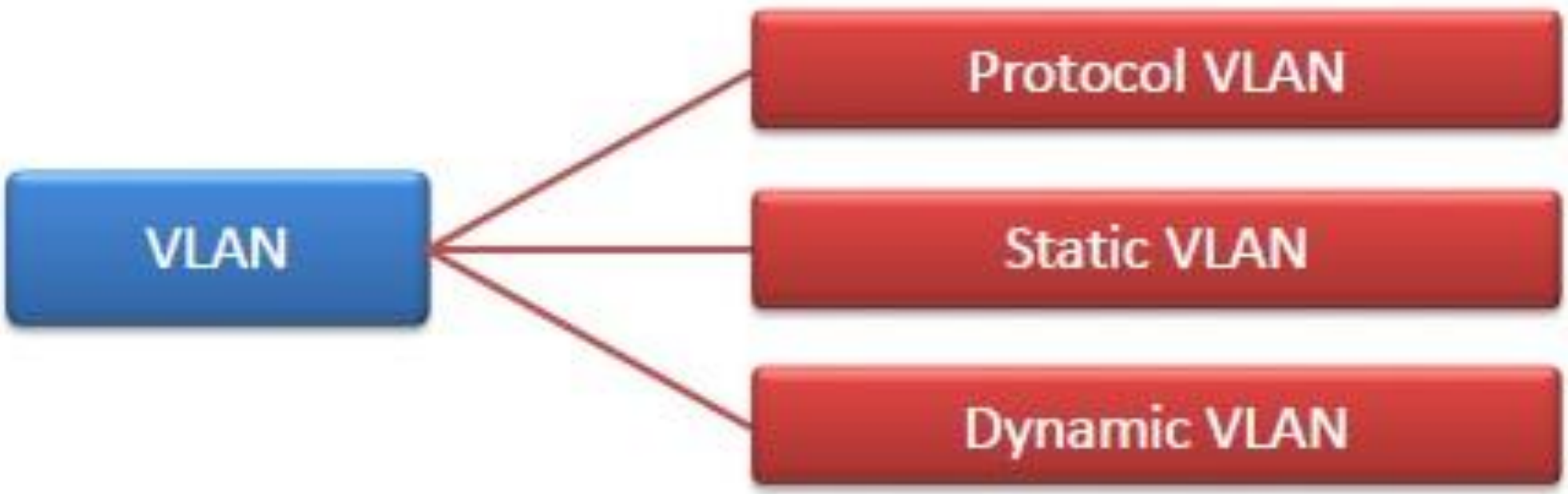
Virtual LAN (VLAN)

- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.

- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges.

- This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Types of VLANs



Types of VLANs

- **Protocol VLAN** – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames that come to it based upon the traffic protocols.

- **Port-based VLAN** – This is also called **static VLAN**. Here, the network administrator assigns the ports on the switch/bridge to form a virtual network.

- **Dynamic VLAN** – Here, the network administrator simply defines network membership according to device characteristics.

Application/Purpose of VLAN

- VLAN is used when you have **200+ devices** on your LAN.
- It is helpful when you have a **lot of traffic** on a LAN.
- VLAN is ideal when a group of users need **more security** or being slow down by many broadcasts.
- It is used when users are not on one broadcast domain.
- Make a single switch into multiple switches.

- Difference b/w LAN and VLAN
- Adv. & Disadv. Of VLAN