# VLANs and VPNs

Prepared By
Dr. Islam Zakaria

# Introduction

- **What is a LAN?**
  - A LAN (Local Area Network) is a network that connects computers and devices within a limited geographic area, such as a single building, office, school, or home.
  - a LAN is the fundamental building block of networking, creating a small, fast, and private network for a localized group of users.
- **Problems in traditional LANs:**
  - **Broadcast storms.**
  - **Lack of security.**
  - **Network congestion.**
  - **Every device sees every broadcast**

# Virtual Local Area Network (VLAN)

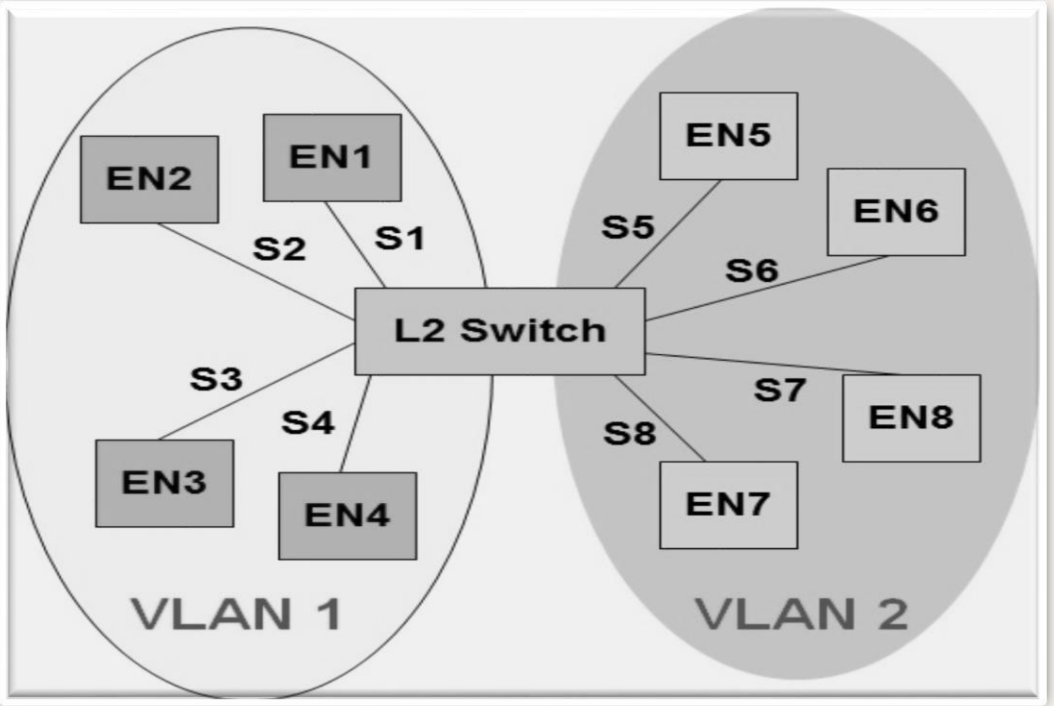
- **Definition**
  - **A VLAN is a logical segmentation of a physical network into multiple, distinct broadcast domains.**
  - Logical grouping of devices regardless of physical location
  - Devices in different VLANs behave as if on different LANs
  - Each VLAN is typically a unique IP subnet.
- **VLANs solve the traditional LAN issues by allowing a single physical switch or network to be logically partitioned into multiple separate broadcast domains.**
- **How VLANs Solve These Problems?**
  - **Broadcast Control:** Each VLAN is its **own broadcast domain**, meaning a broadcast frame sent within VLAN "A" **cannot be forwarded** to devices in VLAN "B". This **significantly reduces broadcast traffic and improves network efficiency**.

# VLAN (Cont.)

- **Security:** VLANs provide **traffic isolation**. Devices in one VLAN cannot directly communicate with devices in another VLAN without going through a **router** (a layer 3 device), which enforces security policies and filtering.
- **Flexibility and Grouping:** Users can be grouped by **function** (e.g., Accounting VLAN) or **application** regardless of their physical location. A user can plug into any port on the network, and as long as that port is configured for the correct VLAN, they belong to the correct logical network.

# VLAN Types

- There are four main different methods of assigning devices to VLANs, moving from the most common to the more specialized.
  - **Port-based VLAN (most common)**
  - **MAC-based VLAN**
  - **Protocol-based VLAN**
  - **Voice VLAN**



# Port-Based VLAN (Static VLAN)

- **The Most Common Method:** This is the default and by far the most widely used type of VLAN, comprising about 90% of all implementations.
- **How it Works:** VLAN membership is **statically configured on the switch port itself**. It doesn't matter what device you plug into the port; it will be a member of the VLAN assigned to that port.
- **Technical Mechanism:**
  - The network administrator **manually configures** each switch port to be an Access Port and assigns it to a specific **VLAN ID** (e.g., switchport mode access, switchport access vlan 10).
  - When a device sends a frame into an **access port**, the switch internally "**tags**" that frame with the configured **VLAN ID**.
  - All frames **leaving** that port towards the device have the **VLAN tag removed**.

# Port-Based VLAN (Cont.)

- **Example:**
  - **Ports 1 - 12** on a switch are configured for **VLAN 10** (**Student-Lab**).
  - **Ports 13 - 24** are configured for **VLAN 20** (**Faculty**).
  - If a student plugs their laptop into **Port 5**, it is in the **Student-Lab VLAN**.
  - If a professor accidentally plugs into **Port 5**, their computer is also in the **Student-Lab VLAN** and may be unable to access faculty resources.
- **Advantages:**
  - **Simple & Easy to Manage:** Very straightforward to configure and troubleshoot.
  - **High Security:** Since membership is tied to a physical port, users cannot change their VLAN by spoofing a MAC address.
- **Disadvantages:**
  - **Inflexible for Mobility:** If a user moves to a different part of the building, a network administrator must manually reconfigure the new switch port for their correct VLAN.

# MAC-Based VLAN

- **How it Works:** VLAN membership is based on the **unique MAC address (Layer 2 address) of the device's network interface card**. The physical switch port a device uses becomes irrelevant.
- **Technical Mechanism:**
  - The administrator creates a **lookup table on the switch that maps specific MAC addresses to specific VLANs**.
  - When a device is plugged into a switch port (which must be configured for this feature), **the switch sees the source MAC address of the first frame**.
  - The switch **consults** its **table** and **dynamically assigns the port to the appropriate VLAN for that MAC address**.

# MAC-Based VLAN (Cont.)

- **Example:**
  - A professor's research laptop with MAC address **AA:BB:CC:11:22:33** is mapped to **VLAN 200** (**Faculty-Research**).
  - A student's personal laptop with MAC address **DD:EE:FF:44:55:66** is mapped to **VLAN 100** (**Student-Lab**).
  - If the professor **unplugs** their **research laptop** from their office and **plugs** it into a port in a lecture hall or a **student lab**, the switch will **automatically** place that port into **VLAN 200**. The professor maintains full access to the **research network** and **servers** from that new location, **without any need for a network administrator to reconfigure the switch**.

# MAC-Based VLAN (Cont.)

- **Advantages:**
  - **Excellent Mobility:** Users and devices can move freely without requiring switch reconfiguration.
  - **Centralized Policy:** Security policy is tied to the device, not the location.
- **Disadvantages:**
  - **High Administrative Overhead:** Initially, you must record the MAC address of every device and configure them all on the switch. This is a massive task in a large network.
  - **Doesn't work well with DHCP:** (**Each VLAN is typically a unique IP subnet**) If a device gets a new IP address after moving, it might not be in the correct IP subnet for its new, mobility-based VLAN, causing connectivity issues. This requires a special DHCP helper configuration.

# Protocol-Based VLAN

- **How it Works:**

  VLAN membership is based on the **protocol type** found in the **Layer 3 header** of the frame (e.g., **IPv4**, **IPv6**, **IPX**, **AppleTalk**). **This is a much less common method today**.

- **Technical Mechanism:**
  - The switch is configured to inspect the "**EtherType**" field of the incoming frame.
  - If the frame contains an **IPv4** packet (**EtherType 0x0800**), it's assigned to one VLAN.
  - If the frame contains an **IPv6** packet (**EtherType 0x86DD**), it's assigned to a different VLAN.

# Protocol-Based VLAN (Cont.)

- **Example:**

  In a transitional network, you might have put all **legacy IPX traffic** on **VLAN 50** to **isolate** it, while keeping modern **IPv4 traffic on VLAN 1**.

- **Advantages:**
  - **Traffic Isolation by Protocol:** Good for separating older or non-internet types of network data.

- **Disadvantages :**
  - **Old-fashioned/No longer necessary:** Standard internet protocols (IP) are used everywhere, so this specific separation method isn't needed anymore.
  - **Complexity:** Adds processing overhead on the switch and complicates configuration for little modern benefit.

# Voice VLAN

- This is **NOT a separate type** of membership, but **a specialized feature that works with Port-Based VLANs**.
- This concept has a specialized configuration used for **Voice over IP (VoIP) phones and their attached computers**.
- This configuration allows a **single physical switch port to carry traffic for two separate logical networks (VLANs) simultaneously, while keeping them properly isolated**.
- **The IP phone acts as a small, managed Layer 2 device (a simple switch)**.

# Voice VLAN (Cont.)

- **The Problem:**
  - An **IP phone** is a device that often has **two connections**: **one to the switch and one to a user's PC**.
  - We want the **voice traffic to be on a separate VLAN** (**for QoS and security**) than the **data traffic** from the PC.
- **The Solution: A Hybrid Port**
  - The switch port is configured to behave as an **Access Port for the PC and a Trunk Port for the IP Phone**.

# Voice VLAN (Cont.)

- **Technical Mechanism:**
  - The administrator configures a **Voice VLAN on the switch port** (e.g., **switchport voice VLAN 200**).
  - The port's default Access VLAN is for the PC (e.g., **switchport access VLAN 10**).
  - The **IP phone**, which is a "**smart**" device, **tags its own voice traffic with the Voice VLAN ID (VLAN 200) before sending it to the switch**.
  - **The PC sends untagged data traffic, which the switch places on the Access VLAN (VLAN 10)**.
  - **The switch port accepts both, treating the voice frames as tagged and the data frames as untagged**.

| Device Originating Traffic | Path Taken | Traffic Type & VLAN ID |
|---|---|---|
| **User's PC** | PC ➡ Phone ➡ Switch | **Untagged Data**<br>(Assigned to VLAN 10 by the switch) |
| **IP Phone** | Phone ➡ Switch | **Tagged Voice**<br>(Tagged with VLAN 200 by the phone) |

# Voice VLAN (Cont.)

- **Example:**
  - A professor's office has **one network jack** connected to their **IP phone**, and their **PC is plugged into the phone**.
- **The switch port is configured with:**
  - Switchport **access vlan 10** (**Faculty Data VLAN**)
  - Switchport **voice vlan 200** (**Voice VLAN**)
  - The PC's web traffic travels on VLAN 10. The professor's phone call travels, with high priority, on VLAN 200.
- **Advantages:**
  - **Simplified Cabling:** Only one cable run per office is needed.
  - **Automatic QoS:** Switches can automatically give priority to traffic from the Voice VLAN, ensuring call quality.

# Comparison of Different VLAN Methods

| VLAN Type | Membership Based On | Advantages | Disadvantages | Suitable For |
|---|---|---|---|---|
| **Port-Based** | Physical Switch Port | Simple, Secure, Easy to manage | Inflexible for user mobility | Most common scenario; fixed workstations |
| **MAC-Based** | Device's MAC Address | Great for device mobility | High admin overhead; complex initial setup | Hospitals (mobile equipment), guest networks |
| **Protocol-Based** | Layer 3 Protocol (e.g., IP) | Isolates legacy traffic | Largely obsolete; complex | Legacy networks (rarely used today) |
| **Voice VLAN** | A feature, not a type | Simplifies wiring; enables QoS | Requires compatible IP phones | Any environment with IP telephony |

# VLAN ID and Range

- **Standard VLAN Range:**
  - **Source:** The **12-bit** VLAN ID field in the **802.1Q** (IEEE standard for VLAN tagging) tag allows for **4096** values (**0-4095**).
  - **Usable Range: VLANs 2-1001** are the normal range for everyday use.

| VLAN ID | Meaning |
| --- | --- |
| **0** | Priority-tagged frame (QoS only) |
| **1** | The default native VLAN |
| **2 – 1001** | Standard user-defined VLANs |
| **1002 – 1005** | Reserved for older technologies like FDDI and Token Ring |
| **1006 – 4094** | Extended range user-defined VLANs |
| **4095** | Used or specific internal diagnostic, control, or management functions |

# Access Ports vs. Trunk Ports

## Access Port (The "End-User" Port)

- **Purpose:** **Connects to a single end device** (e.g., computer, printer, IP phone, server).
- **VLANs:** Carries traffic for **only one VLAN**.
- **Tagging:** **Forwards traffic untagged**. The switch adds/removes the VLAN tag internally.
- **When to Use:** **For any port where an end-user device is plugged in**.

## Trunk Port (The "Inter-Switch" Port)

- **Purpose:** **Connects network devices** (e.g., switch-to-switch, switch-to-router, switch-to-firewall).
- **VLANs:** Carries traffic for **multiple VLANs simultaneously**.
- **Tagging:** Forwards traffic with **802.1Q tags**. The VLAN tags are preserved so the receiving device knows which VLAN the frame belongs to.
- **When to Use:** **For links between switches and routers to allow multiple VLANs to cross the network.**

# Access Ports vs. Trunk Ports (Cont.)

| Feature | Access Port | Trunk Port |
|---|---|---|
| **Purpose** | Connects end devices | Connects network devices |
| **VLAN Traffic** | One VLAN | Many VLANs |
| **802.1Q Tagging** | Untagged | Tagged |
| **Typical Use** | User PC, Printer, Server | Switch-to-Switch, Switch-to-Router |

# Inter-VLAN Routing: The Essential Bridge Between VLANs

- **The Core Problem: VLANs Create Isolation**
  - **VLANs are Separate Broadcast Domains:** By design, a VLAN is an **isolated Layer 2 network**. Broadcasts, multicasts, and unknown unicasts are contained within a single VLAN.
  - **No Direct Communication:** A device in **VLAN 10 cannot** send a frame directly to a device in **VLAN 20 through a switch alone**. **The switch will not forward the frame across VLAN boundaries**.
- **The Solution: A Layer 3 Device is Required**
  - To allow communication between VLANs, you need a device that can make decisions based on IP addresses (Layer 3), a router or a Layer 3 switch.
- **The Two Primary Methods**
  - **Router-on-a-Stick** (Traditional)
  - **Layer 3 Switch** (Modern)

# Router-on-a-Stick (Traditional)

- **Concept:** A single physical router interface is used to route between multiple VLANs. It's called "on-a-stick" because one link handles all the inter-VLAN traffic.
- **How it Works:**
  1. **Trunk Link:** The router is connected to a switch via **a single trunk link** that carries all VLANs.
  2. **Subinterfaces:** The physical router interface is logically **divided into multiple virtual subinterfaces** (e.g., **G0/0.10**, **G0/0.20**).
  3. **VLAN Assignment:** Each **subinterface is assigned to a specific VLAN** and **given an IP address that serves as the default gateway for that VLAN's devices**.

# Router-on-a-Stick (Cont.)

4. **The Routing Process:**
    1. A **PC in VLAN 10** sends a packet to a **PC in VLAN 20**. It sends the packet to its **default gateway** (**the VLAN 10 subinterface on the router**).
    2. The switch **tags** the frame with **VLAN 10** and sends it over the **trunk** to the router.
    3. The router receives the frame on **subinterface G0/0.10**, remove the **VLAN tag**, and routes the packet.
    4. The router sees the **destination** is in the **VLAN 20 subnet**, so it **forwards** the packet out **subinterface G0/0.20**.
    5. The router **re-tags** the frame with **VLAN 20** and sends it back down the **trunk** to the switch.
    6. The switch **forwards** the frame to the **destination** PC in **VLAN 20**.

- ❑ **Advantages: Cost-effective (uses only one router port)**.
- ❑ **Disadvantages: Can become a bottleneck because all inter-VLAN traffic must traverse a single physical link.**

# Layer 3 Switch (The Modern, High-Performance Method)

- **Concept:** **A switch that has a router built into its hardware. It can perform both switching (within a VLAN) and routing (between VLANs) at wire speed**.
- **How it Works:**
  1. **Switched Virtual Interfaces (SVIs):** Instead of physical subinterfaces, you create **logical Layer 3 interfaces for each VLAN** (e.g., **interface vlan 10**, **interface vlan 20**).
  2. **Default Gateway:** **Each SVI is assigned an IP address**, **which becomes the default gateway for that VLAN**.

# Layer 3 Switch (The Modern, High-Performance Method)

3. **The Routing Process:**
   - A PC in **VLAN 10** sends a packet to a PC in **VLAN 20**. It sends the packet to its **default gateway** (**the SVI for VLAN 10 on the switch**).
   - The traffic arrives at the switch. Instead of being **sent out** a physical port to a router, it is handled **internally**.
   - The switch's routing engine processes the packet and **determines the exit point is the SVI for VLAN 20**.
   - The packet is immediately forwarded out the correct switch port to the destination PC in **VLAN 20**.

- **Advantages:** **Extremely fast because routing is done in hardware. No single point of bottleneck**.
- **Disadvantages:** **More expensive than a standard Layer 2 switch**.

# Router-on-a-Stick VS Layer 3 Switch

| Feature | Router-on-a-Stick | Layer 3 Switch |
|---|---|---|
| **Device Used** | External Router | Layer 3 Switch (Switch + Router) |
| **Interface Type** | Subinterfaces on a single physical port | Switched Virtual Interfaces (SVIs) |
| **Performance** | Lower (Can be a bottleneck) | Very High (Hardware-based) |
| **Cost** | Lower (Uses existing router) | Higher |
| **Use Case** | Smaller networks, low traffic | Modern enterprise networks, high traffic |

# VPN

# Virtual Private Network (VPN)

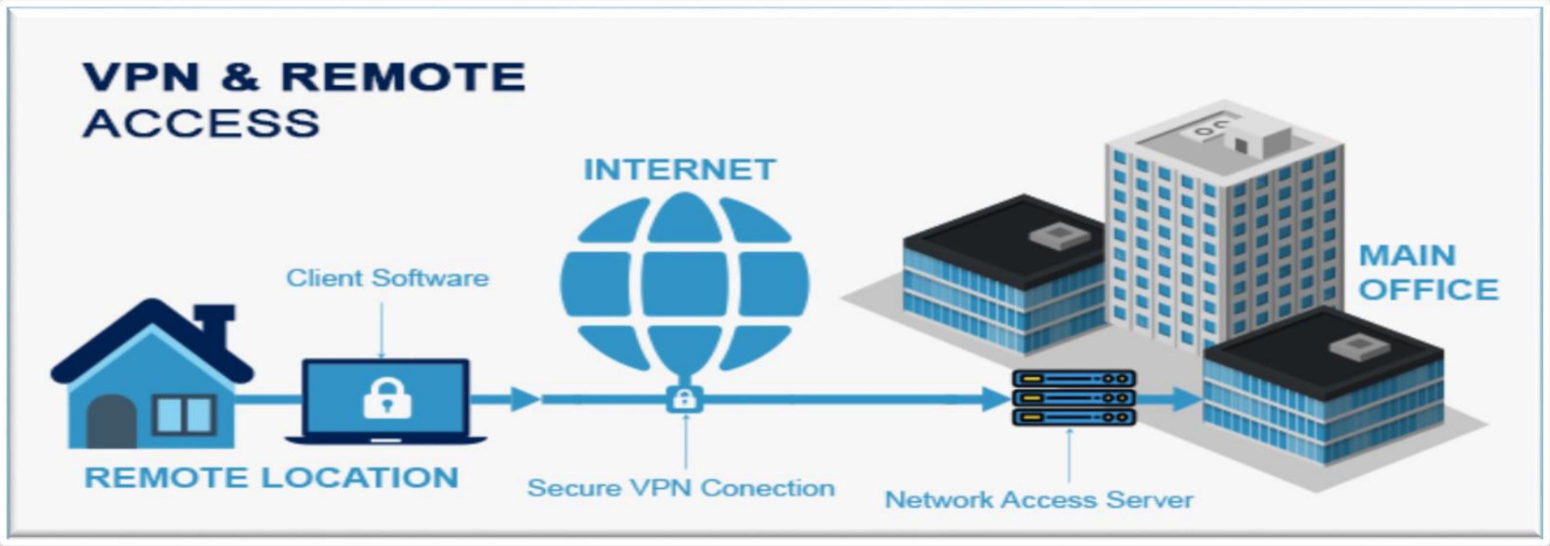
- **VPN is Provides the following:**
  - **Secure Tunnel:** It creates a private, secure communication path (**a "tunnel"**) over a **public, insecure network** like the Internet.
  - **Encryption is Key:** All data sent through this tunnel is **encrypted**, making it **unreadable** to anyone who **intercepts** it, thus **preventing eavesdropping**.
  - **Logical Connection:** It allows devices to behave as if they are **on the same local physical network**, even when they are physically far apart.
  - **Core Purpose:** To provide **secure remote access for users and securely connect separate networks over the internet**.

# VPN Types

- There are two main types of VPNs based on their architecture and use case, such as:
  - Remote Access VPN (Or Client-to-Site VPN)
  - Site-to-Site VPN

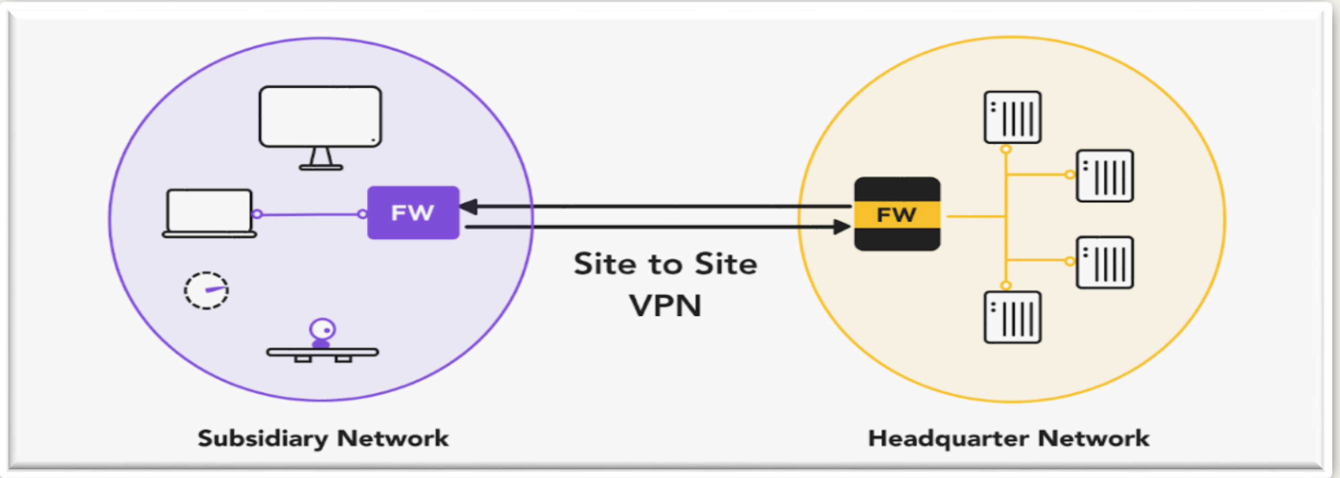
# Remote Access VPN

- **Purpose:** Allows a single user to connect to a remote network from anywhere.
- **How it works:** The user runs VPN client software on their device (laptop, phone). Once connected, their device acts as if it's physically inside the office network.
- **Example:** An employee working from home uses a VPN client to access their company's internal file servers and applications.



# Site-to-Site VPN

- **Purpose:** Connects two entire networks together over the internet.
- **How it works:** Uses VPN-capable routers or firewalls at each location (e.g., Headquarters and Branch Office). The devices create a permanent secure link between the two sites.
- **Example:** A bank's branch office connects to its main data center, allowing any computer at the branch to securely use resources at the main center.



# VPN Core Mechanisms

- **The core mechanisms of a Virtual Private Network (VPN) are Tunneling**, **Encapsulation**, **Encryption**, and **Authentication**. These processes work together to establish a secure, private, virtual link over a public network, like the internet.

1) **Tunneling**

   - **Tunneling** is the process of creating a secure, logical pathway, the "tunnel“, through the public internet.
   - **Process:** A VPN protocol (like WireGuard, OpenVPN, or IPsec) establishes a **persistent, virtual connection between your device** (the VPN client) and **the VPN server**.
   - **Function:** **This tunnel routes all your internet traffic through the VPN server**, **hiding your real IP address and location behind the server's IP**.
   - **Result:** **All your data appears to originate from the VPN server's location**, **making the public network function like a private, dedicated link**.

# VPN Core Mechanisms

## 2) Encapsulation (The Wrapper)

- **Encapsulation** is how the data is **wrapped** to travel through the tunnel.
- **Process:** Your original data packet (**which includes the data, destination IP, and your source IP**) is taken and **wrapped** inside another header that contains the **VPN server's IP address as the destination**.
- **Function:** This new **outer** packet acts as the envelope. Your Internet Service Provider (ISP) and other observers can **only** see the outer header (the VPN server's address) and **cannot** read the **inner**, original packet's contents or destination.
- **Result:** The original, **private packet is hidden**, allowing it to traverse the public internet securely to the VPN server, which is the only system that knows how to **unwrap** it.

# VPN Core Mechanisms

## 3) Encryption (The Code)

- **Encryption** is the process that scrambles the data, rendering it unreadable to anyone who intercepts the encapsulated packet. This is the most critical mechanism for privacy.
- **Process:** The VPN client uses a cryptographic algorithm (like AES-256) and a secret key to transform the readable data (plaintext) into an unreadable format (ciphertext).
- **Function:** This scrambling happens before encapsulation and transmission. The VPN server possesses the corresponding key to decrypt (unscramble) the data upon arrival.
- **Encryption Types:**
  - **Symmetric Encryption:** Uses the same single key for both encryption and decryption (e.g., AES). This is used for the bulk data transfer due to its speed.
  - **Asymmetric Encryption:** Uses a pair of public and private keys (e.g., RSA). This is typically used only during the initial secure "handshake" to securely exchange the much faster symmetric key.

# VPN Core Mechanisms

## 4) Authentication (The Verification)

- **Authentication** is the mechanism used to **verify** the **identities of both the client and the server before** the **secure tunnel is fully established**.
- **Process:** Before establishing the tunnel, the client and server exchange **credentials** or **digital certificates** to prove they are who they claim to be.
- **Function:** This **prevents unauthorized** devices or **malicious actors** from joining the **private** network or **impersonating** the VPN service.
- **Result:** **Guarantees** that the data is sent to the **legitimate VPN server** and that only **authorized users are establishing the connection**.

# VPN Core Mechanisms

- **How They Work Together: When you connect to your office VPN:**
  1. **Authentication:** Your laptop and the company VPN server first verify each other's identity.
  2. **Encryption:** They agree on a secret key to use for scrambling the data.
  3. **Encapsulation:** For every packet you send, your laptop:
  4. **Encrypts** the original, private packet.
  5. **Wraps** this encrypted data inside a new, outer packet addressed to the VPN server.
  6. **Tunneling:** This new packet is sent through the pre-established logical tunnel over the public internet.

# Any Questions