The Modern LAN: A Story of Switching, Security, and Segmentation

From Chaotic Hubs to Intelligent Fabrics

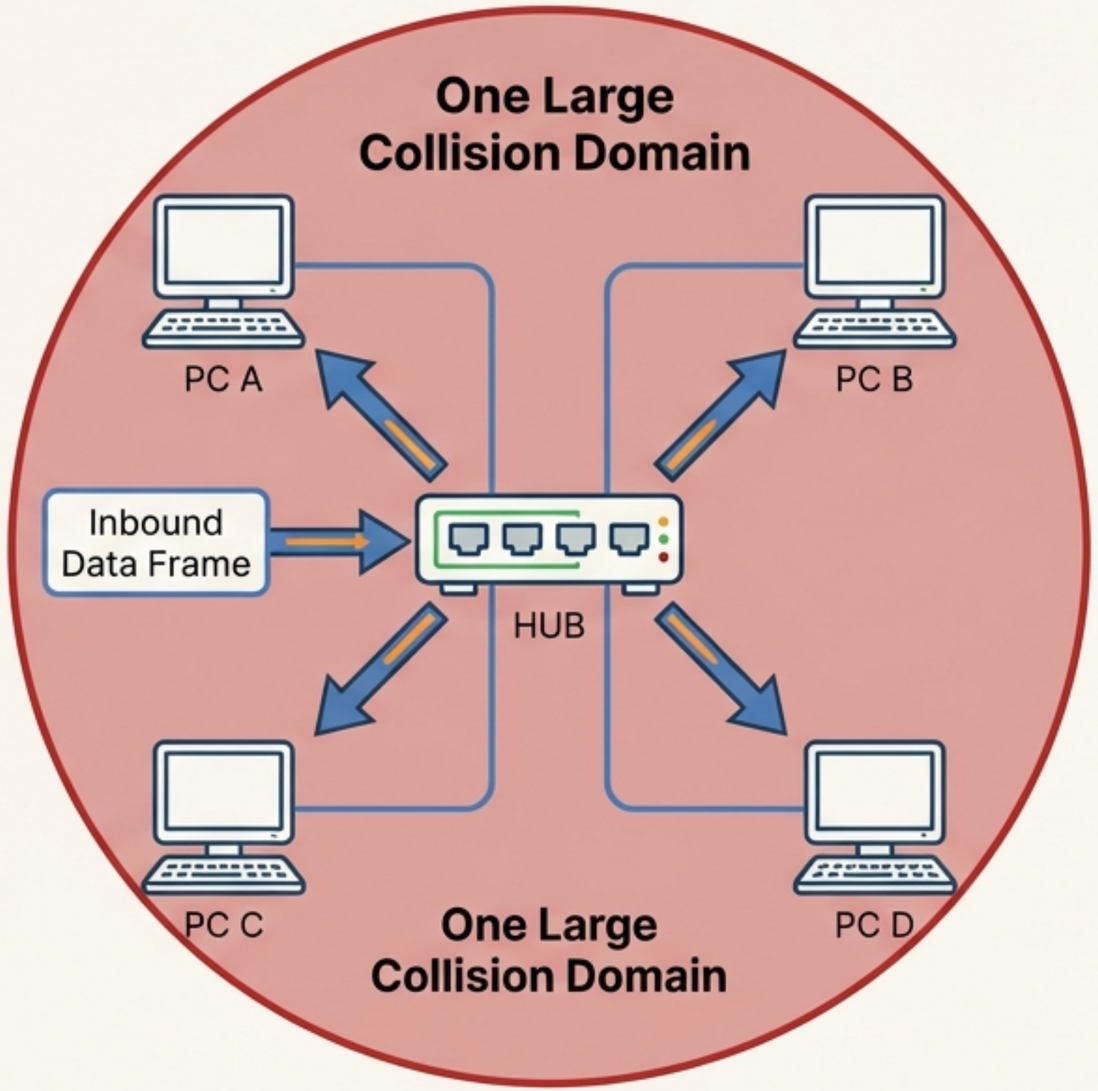
We Begin in Chaos: The Era of the Hub

Key Concept

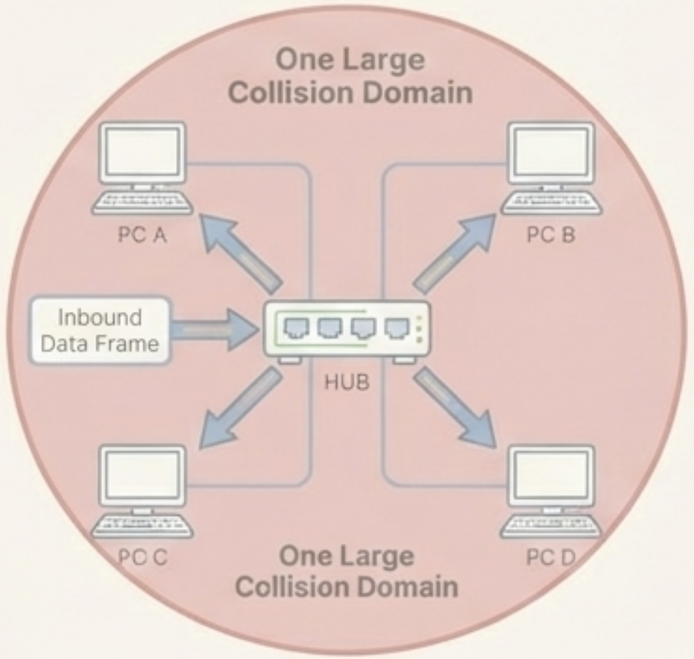
Before switches, networks were built with hubs. A hub operates in a single, large **collision domain**, meaning all devices share the same bandwidth.

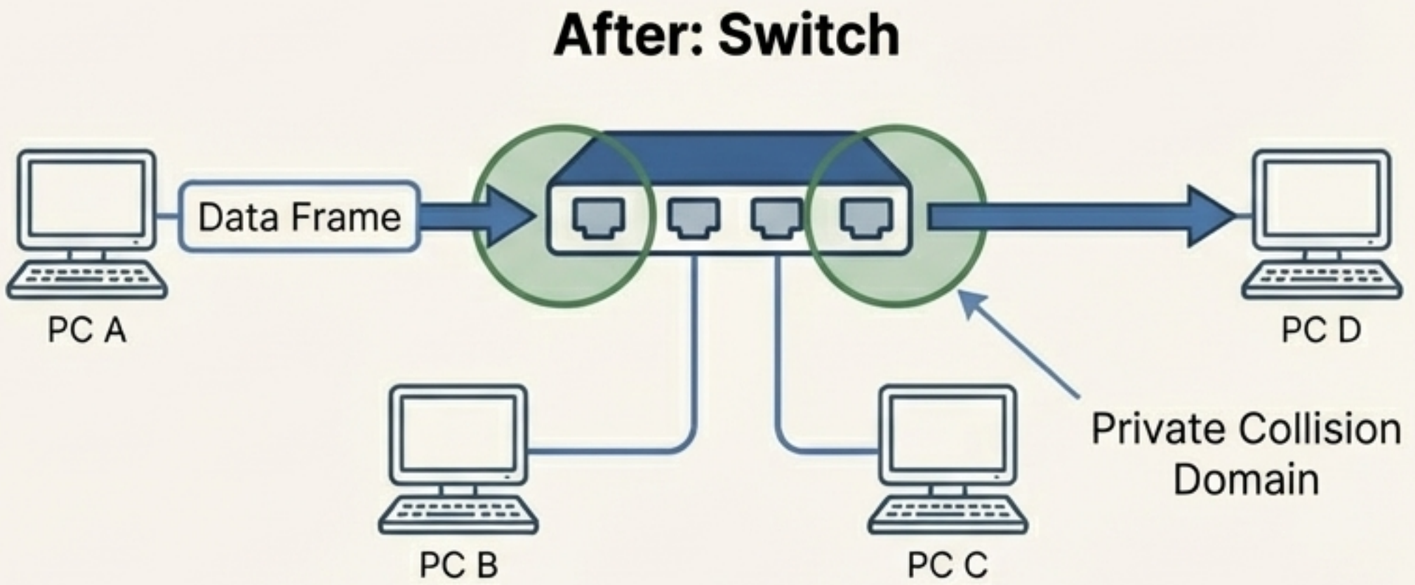
Analogy

A hub-based network is like a noisy party where everyone shouts at once. Every message is sent to every guest, causing interference (collisions) and making meaningful conversation inefficient.



Bringing Order: The Layer 2 Switch





Hardware-based bridging (ASICs)

Purpose-built hardware for high-speed decisions.

Wire speed performance

Operates at the maximum speed of the physical links.

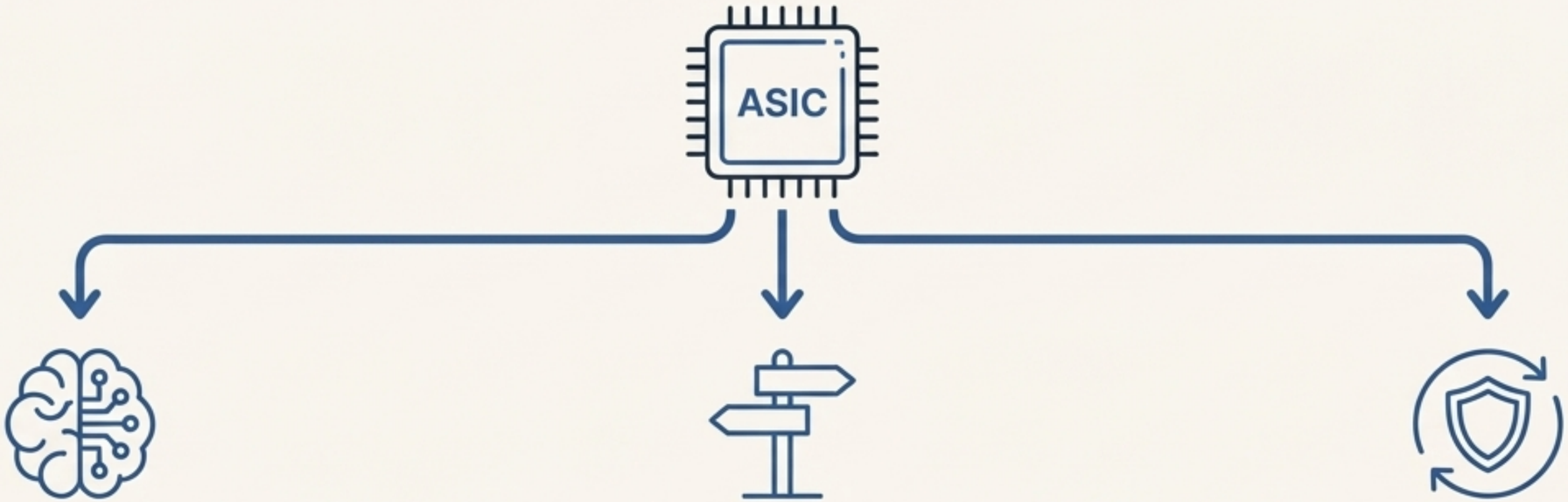
Low latency

Minimal delay in forwarding frames.

A switch is like a building with a smart telephone operator. Instead of shouting, each person makes a private, point-to-point call to their intended recipient. Conversations don’t interfere with each other.

The Three Pillars of a Switch’s Intelligence

A switch isn’t magic; it operates on three distinct functions to create an efficient network.



1. Address Learning

The switch builds a “map” of the network by observing the source MAC address of every frame it receives. This map is stored in a MAC address table (or CAM table).

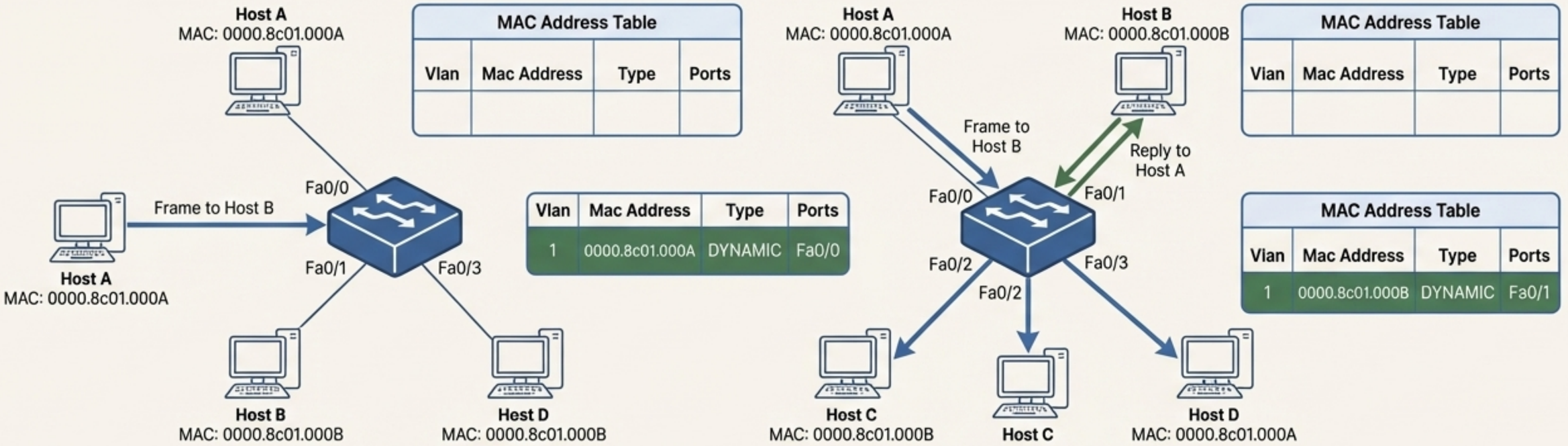
2. Forward/Filter Decisions

Using its MAC address table, the switch intelligently forwards frames only to the port where the destination device is located. If the destination is unknown, it floods the frame.

3. Loop Avoidance

A built-in safety net. If redundant links between switches create a loop, the Spanning Tree Protocol (STP) prevents a catastrophic “broadcast storm” by logically blocking one of the links.

How a Switch Learns the Lay of the Land



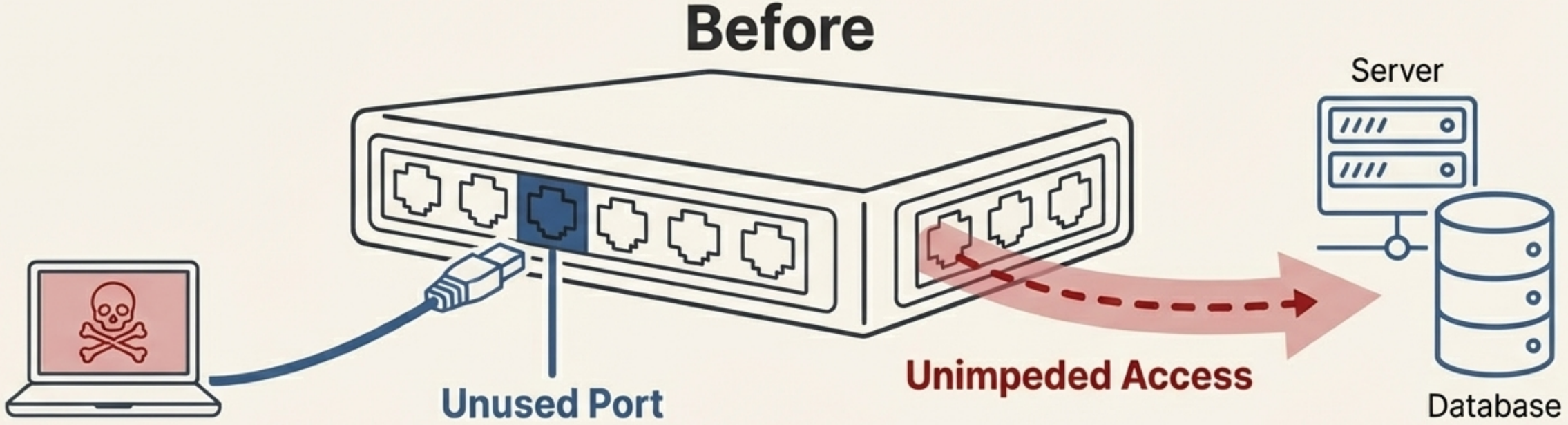
1. Host A sends a frame to Host B. The switch's MAC table is empty.
2. The switch receives the frame, **learns** Host A's MAC, and records its port.
3. Destination for Host B is unknown. The switch **floods** the frame to all other ports.
4. Host B replies. The switch **learns** Host B's MAC and port.

The Result: Now, Host A and Host B can have a point-to-point connection. Future frames between them will be **filtered** and sent directly, not flooded. This is the core of switching efficiency.

```
Switch# show mac address-table
Vlan   Mac Address       Type        Ports
----   --------------    --------    -----
1      0000.8c01.000A    DYNAMIC     Fa0/0
1      0000.8c01.000B    DYNAMIC     Fa0/1
```

The New Vulnerability: The Unsecured Port

The Problem: Our network is fast, but **it's not secure**. By default, anyone can connect a device to an unused switch port and gain immediate access to the network.



"We worry about wireless security, so why wouldn't we demand switch security just as much, if not more?"

Securing the Gates with Port Security

The Solution

Port security acts as a digital bouncer for your switch ports. It restricts port access by MAC address, allowing you to control exactly *who* can connect.

Key Capabilities

- Limit the number of MAC addresses allowed on a port.
- Statically assign specific MACs to a port.
- Automatically learn a limited number of MACs ('sticky').

The Consequences (Violation Modes)

- **Shutdown (Default):** The port is disabled and placed in an 'error-disabled' state. The port light turns amber. *A satisfying option for network admins.*
- **Restrict:** Drops packets from unknown sources and sends a security notification.
- **Protect:** Quietly drops packets from unknown sources without notification.

After

Configuring Your Digital Bouncer

1. Core Configuration Steps

1. **Set Port to Access Mode**: A prerequisite for port security.

```
Switch(config-if)# switchport mode access
```

2. **Enable Port Security**: Activates the feature with defaults (max 1 MAC, shutdown violation).

```
Switch(config-if)# switchport port-security
```

A Powerful, Time-Saving Technique: `mac-address sticky`

Instead of manually typing every MAC address, the `sticky` command tells the switch to automatically learn the first MAC address(es) that connect and 'stick' them to the port as secure entries in the running configuration.

3. Example Configuration

```
Switch(config)# interface Fa0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum
2
Switch(config-if)# switchport port-security mac-
address sticky
```

Explanation: This configuration allows the **first two devices** that connect to `Fa0/3` to be learned and secured. If a **third device** attempts to connect, the port will **shut down**.

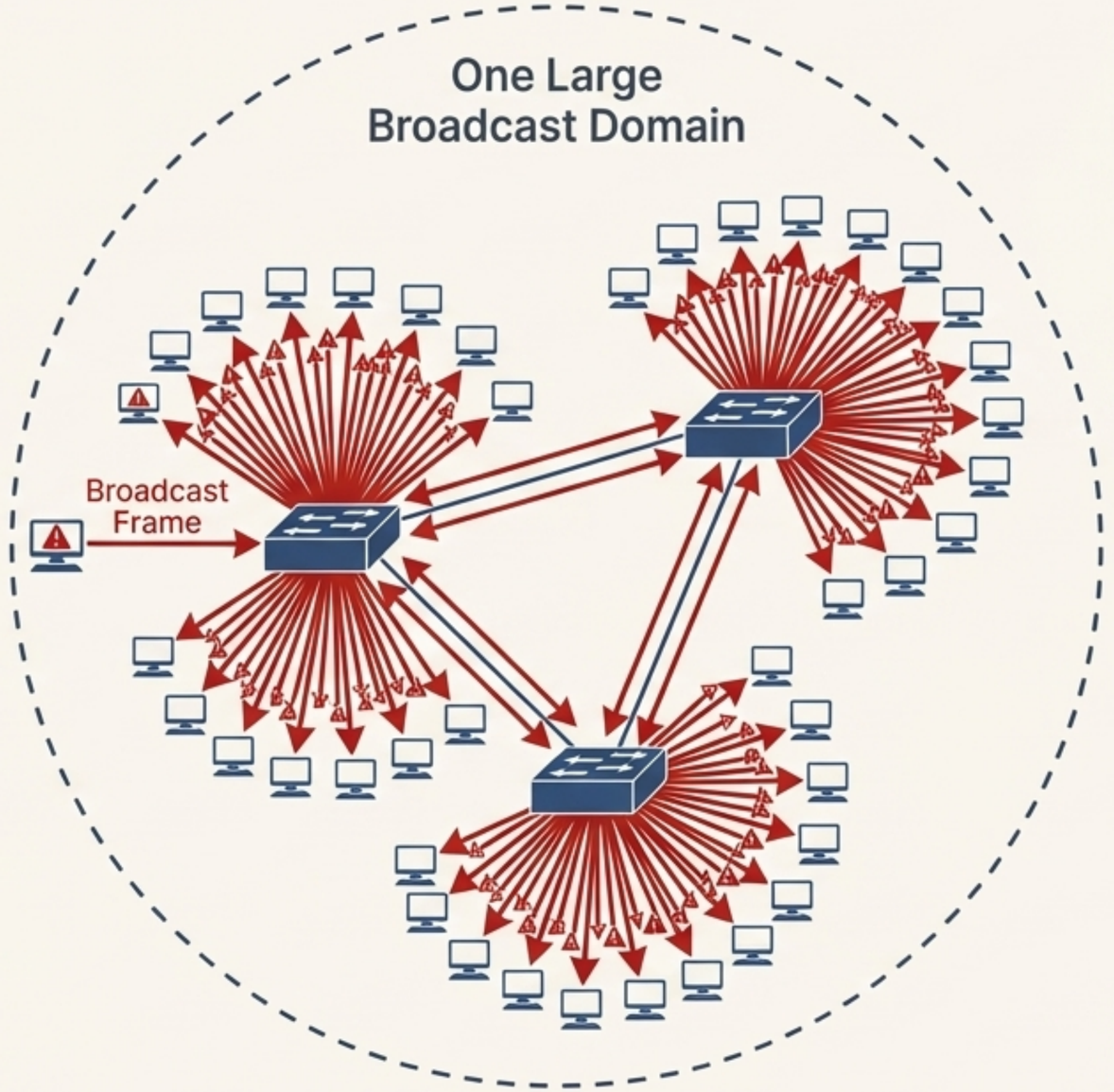
The Crisis of Scale: The Single Broadcast Domain

The Problem

Our switched network is efficient for known unicast traffic, but it is still **one large broadcast domain**. Broadcast frames (e.g., ARP requests) are flooded out of all active ports.

Consequences of Growth

1. **Wasted Bandwidth**: Every device must process every broadcast, even if it's irrelevant.
2. **Security Risks**: All users can see broadcast traffic from all other users by default.
3. **Broadcast Storms**: A single faulty device can create an endless flood of broadcast frames, consuming all available bandwidth and bringing the entire network to a halt.

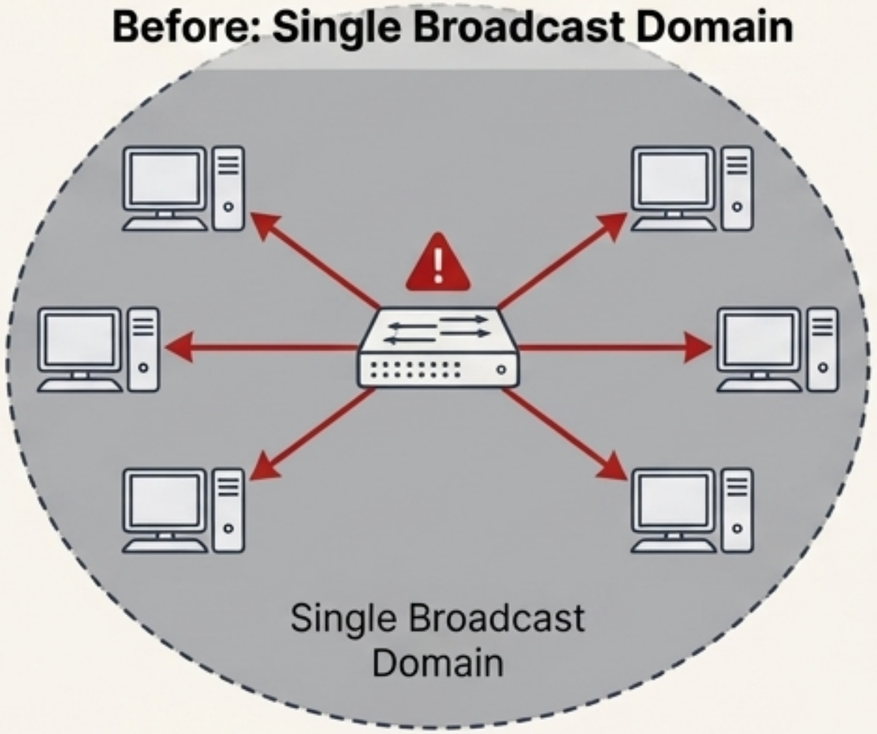


Taming the Storm with Virtual LANs (VLANs)

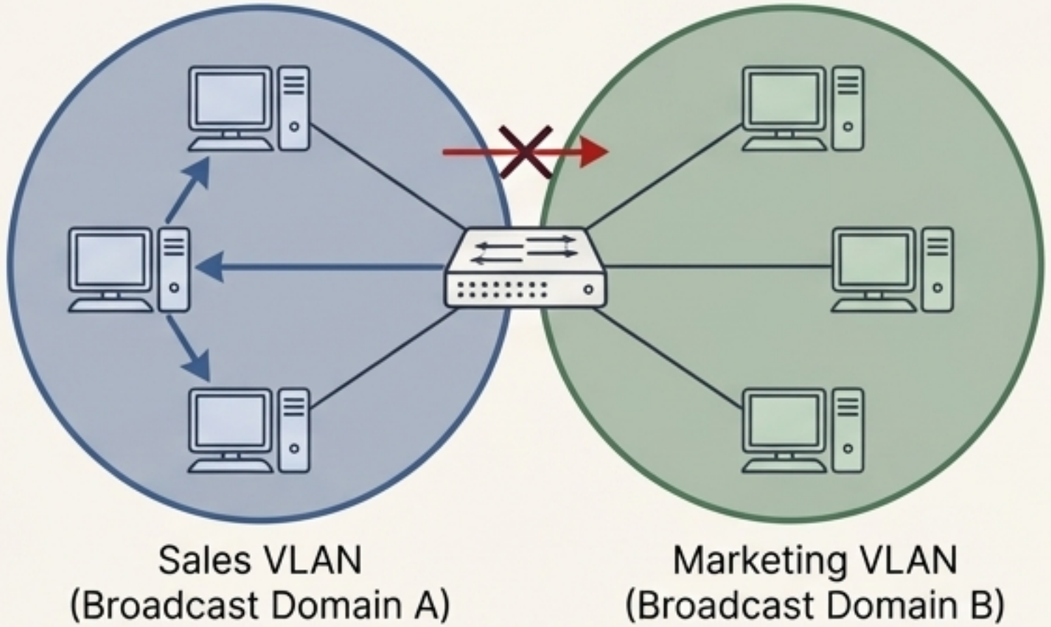
The Solution: A VLAN is a logical grouping of network users and resources. It allows you to take one physical switch and logically carve it into multiple, isolated virtual networks.

The Core Benefit: Each VLAN is its own separate broadcast domain. Broadcasts from a device in one VLAN are only forwarded to other devices in the *same VLAN*.

Before: Single Broadcast Domain



After: Multiple Virtual LANs



Broadcast Control
Shrinks broadcast domains, saving bandwidth and CPU cycles.

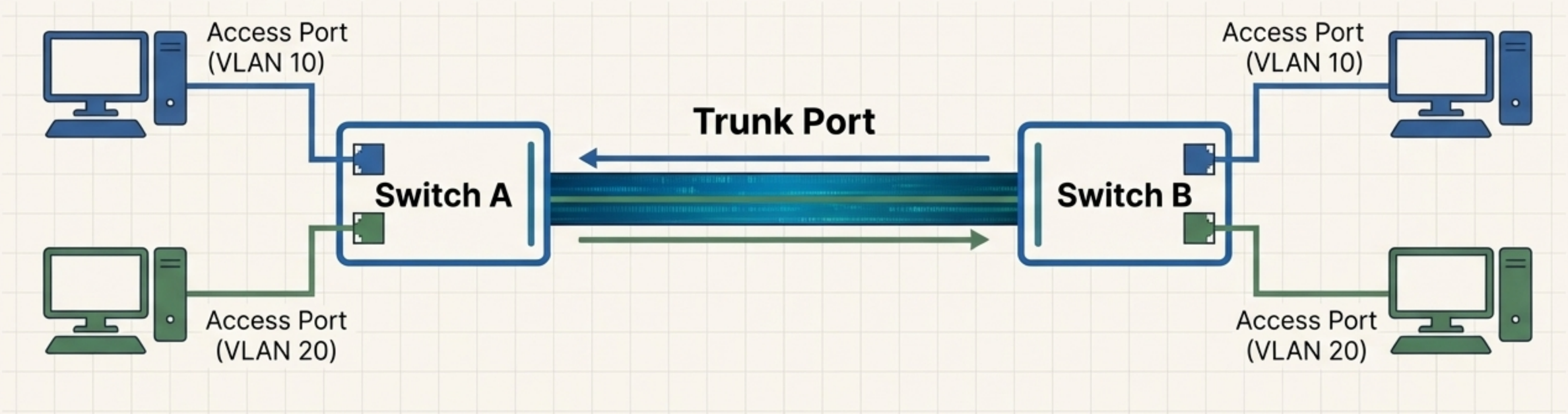
Enhanced Security
Isolates groups of users; traffic cannot pass between VLANs without a router.

Flexibility
Group users by department regardless of their physical location.

Weaving the Fabric: Extending VLANs Across Switches

The Challenge:

VLANs are great on a single switch, but real networks have many. How do we **ensure a user in the Sales VLAN on Switch A can communicate with a user in the Sales VLAN on Switch B?**



1. Access Port

- Belongs to **one** data VLAN.
- Connects to end-user devices (PCs, printers).
- Carries a second, special **Voice VLAN** for IP phones.

2. Trunk Port

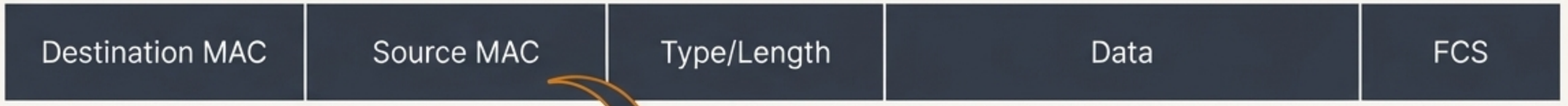
- Belongs to **all** VLANs by default.
- Connects switches to other switches (or routers).
- Acts as a superhighway, carrying traffic for multiple VLANs simultaneously.

The Secret Language of Trunks: 802.1q Frame Tagging

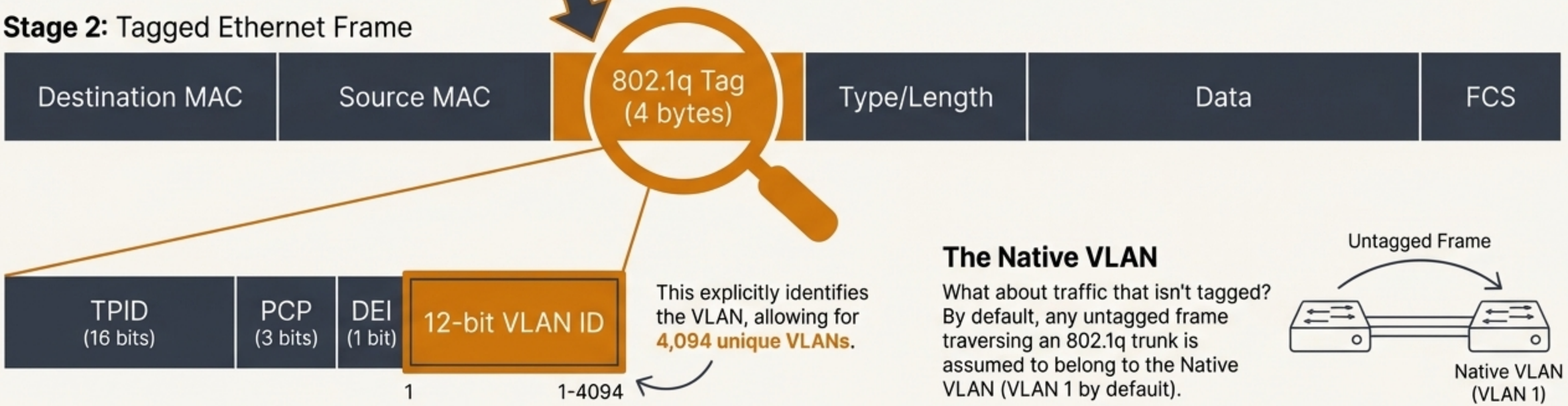
The Question: When a frame from the Sales VLAN (VLAN 10) arrives at Switch B over a trunk link, how does Switch B know it belongs to the Sales VLAN?

The Answer: Frame Tagging. The industry standard IEEE 802.1q protocol inserts a small tag into the Ethernet frame.

Stage 1: Standard Ethernet Frame



Stage 2: Tagged Ethernet Frame



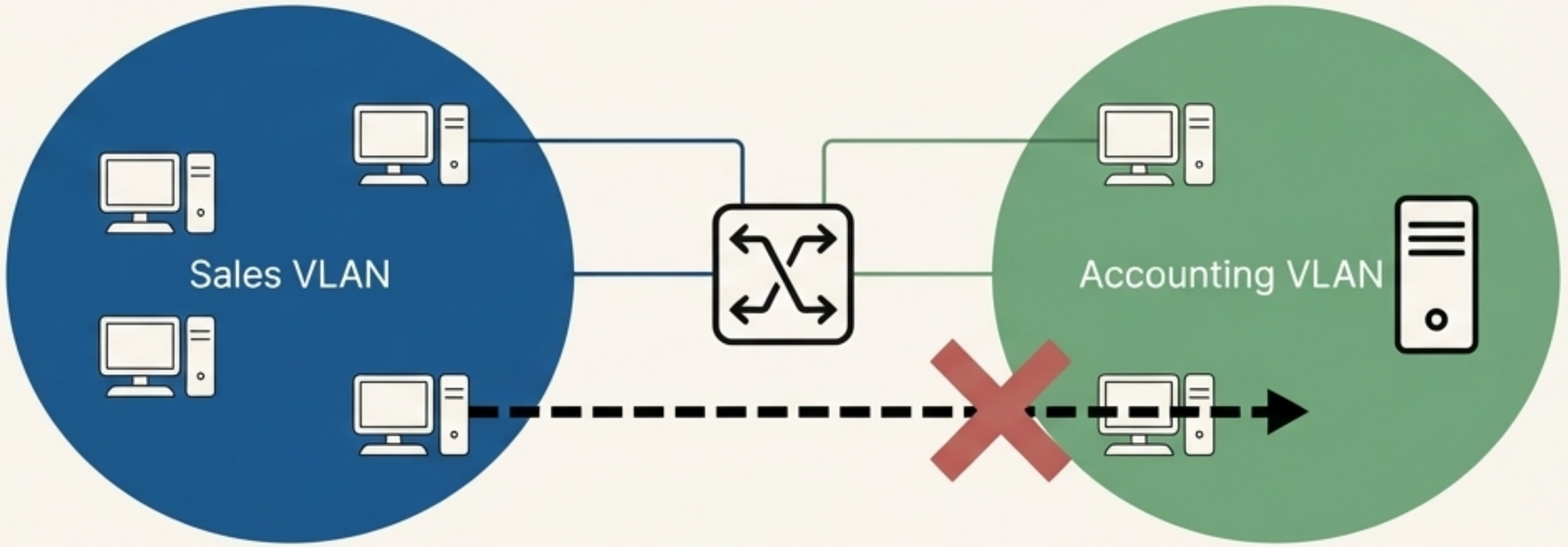
The Native VLAN

What about traffic that isn't tagged? By default, any untagged frame traversing an 802.1q trunk is assumed to belong to the Native VLAN (VLAN 1 by default).

The Final Challenge: Isolation Is Too Good

The New Problem: We have achieved our goal of segmentation. The Sales, Marketing, and Accounting VLANs are secure and isolated broadcast domains.

The Unintended Consequence: The Sales department can no longer access the shared server in the Accounting VLAN. By default, devices in different VLANs cannot communicate.



The Need: We require a controlled, secure way to allow traffic to pass between VLANs. We need a Layer 3 gateway.

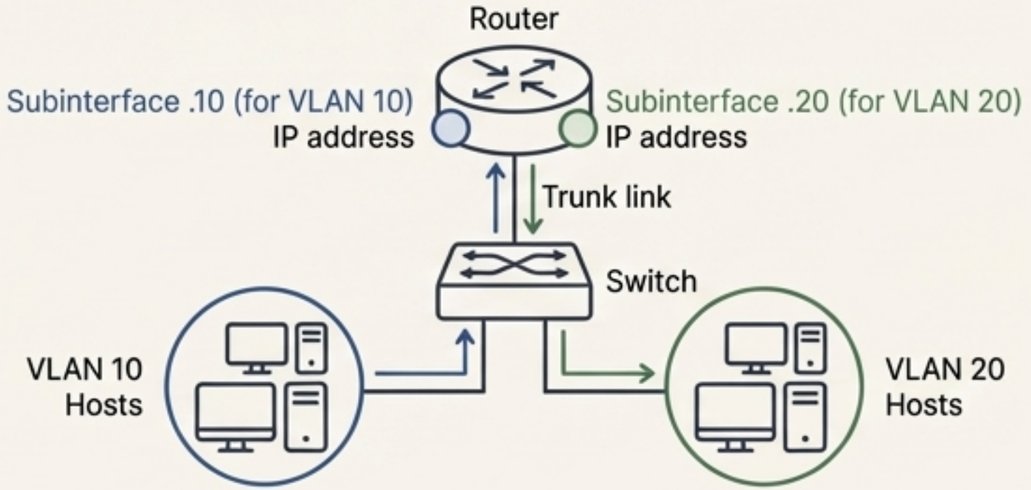
Bridging Worlds with Inter-VLAN Routing

The Solution: A Layer 3 device (a router or multilayer switch) is required to act as a gateway, making decisions based on IP addresses to forward traffic between the separate VLAN subnets.

Method 1: Router-on-a-Stick (ROAS)

Concept: A single physical router interface is connected to a switch trunk port. The router interface is divided into logical subinterfaces, one for each VLAN.

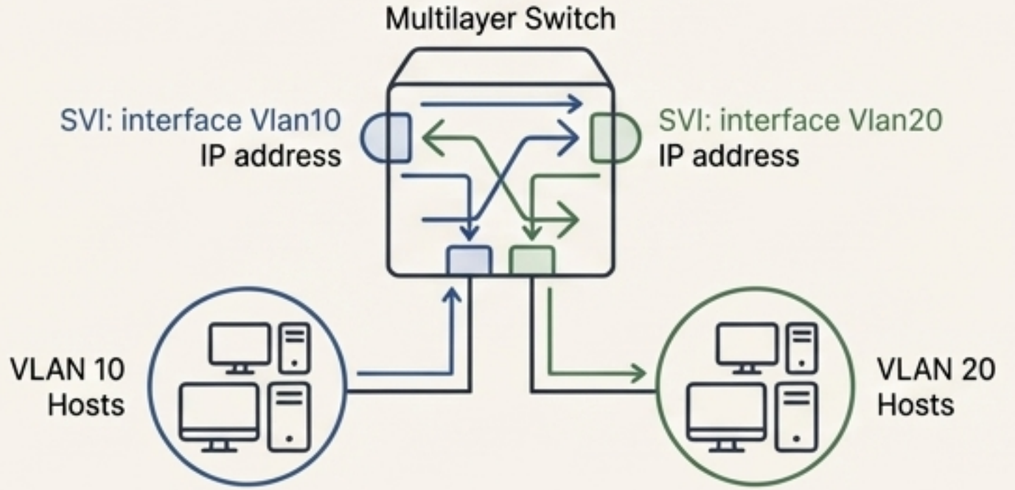
Function: Each subinterface is configured with an IP address in the VLAN's subnet and serves as the default gateway for hosts in that VLAN.



Method 2: Layer 3 Switching (SVI)

Concept: Routing logic is built directly into the switch's backplane. We create a logical Switched Virtual Interface (SVI) for each VLAN.

Function: The SVI (`interface Vlan10`) is a virtual Layer 3 interface that serves as the default gateway for its VLAN.



The Modern LAN: A Cohesive Architecture

The Complete Picture: By combining Layer 2 switching, port security, VLANs, 802.1q trunking, and Inter-VLAN routing, we build a network that is efficient, secure, scalable, and flexible.