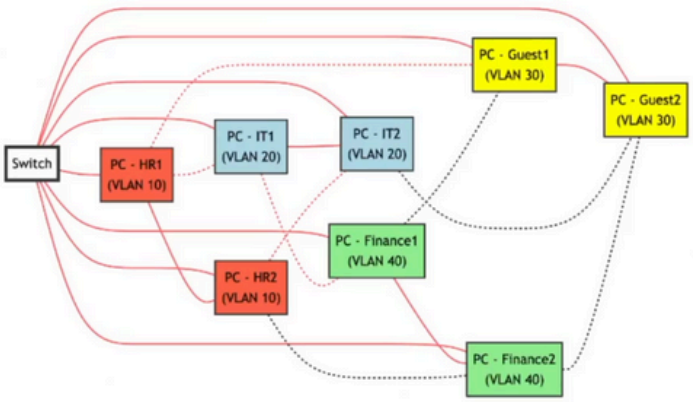
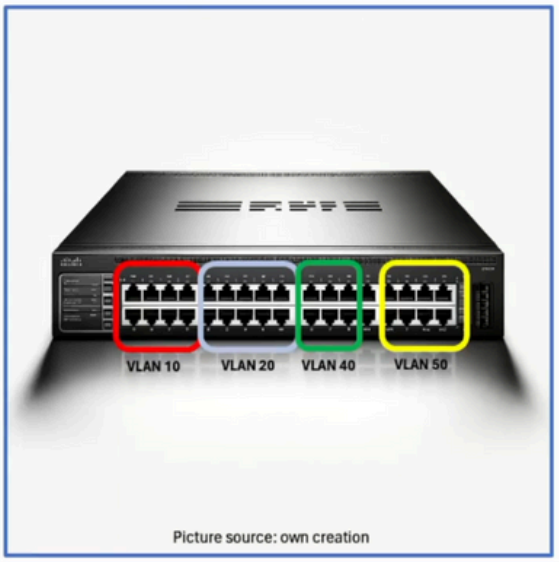
VLAN

VLAN (Virtual Local Area Network) is a technology that allows network administrators to segment a physical network into multiple logical networks, enabling them to isolate traffic for different user groups, departments, or types of traffic within the same physical infrastructure.

This segmentation enhances security by limiting broadcast domains, reducing the potential for eavesdropping, and containing network-based attacks within a single segment. Additionally, VLANs enforce access control policies more effectively by segregating sensitive data and systems, thus playing a crucial role in implementing a layered security strategy and improving overall network management and performance.

VLAN

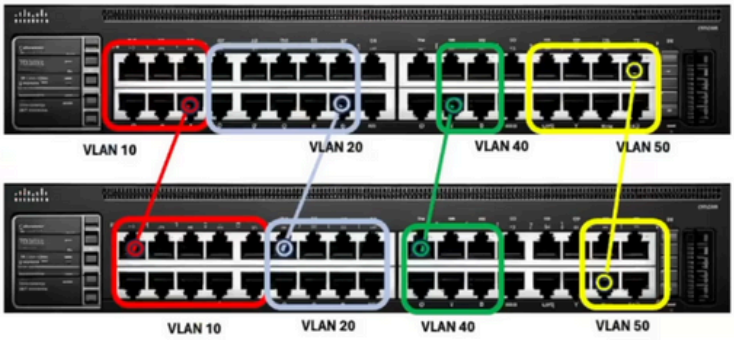




Picture source: own creation

VLAN

Trunk ports



Picture source: own creation

VLAN

- **Default VLAN**: The base configuration grouping all ports into a single VLAN (usually VLAN 1), responsible for network traffic control.
- **Native VLAN:** Allows untagged frame traffic from untagged ports, used for compatibility with other networks, typically left unused to collect unauthorized traffic.
- **Management VLAN:** Provides access to switch management, should be separate from the default VLAN to secure management ports from network users.
- **Voice VLAN:** Supports VoIP traffic with higher priority and bandwidth requirements, configured specifically for VoIP functions.
- **Data VLAN:** Handles the majority of network traffic from users and devices, with options for individual or collective security measures.