VLAN LAB DESCRIPTION

This lab demonstrates how **Virtual Local Area Networks (VLANs)** are used to logically segment a network and how **inter-VLAN routing** allows communication between those VLANs using a router. The setup follows the **router-on-a-stick** approach, which is commonly used in small to medium networks.

Network Topology Overview

The network consists of:

- **One Cisco 2911 router**
- **One Cisco 2960 switch**
- **Six end devices (PCs)** grouped into three departments

Each department is placed in its own VLAN to improve **security, performance, and traffic management**.

VLAN Structure and IP Addressing

Three VLANs are configured on the switch, each representing a department:

VLAN 10 – IT Department

- Network: 192.168.10.0/24
- Devices:
    - PC1: 192.168.10.2
    - PC2: 192.168.10.3

VLAN 20 – Admin Department

- Network: 192.168.20.0/24
- Devices:
    - PC3: 192.168.20.2
    - PC4: 192.168.20.3

VLAN 30 – Sales Department

- Network: 192.168.30.0/24
- Devices:

  - PC5: 192.168.30.2
  - PC6: 192.168.30.3

Each VLAN is treated as a **separate broadcast domain**, meaning devices in different VLANs cannot communicate directly without a routing device.

Switch Configuration and VLAN Assignment

The Cisco 2960 switch is responsible for:

- Creating VLANs
- Assigning access ports to the correct VLAN
- Forwarding tagged VLAN traffic to the router

Ports connected to end devices are configured as **access ports**, while the port connecting the switch to the router is configured as a **trunk port** to carry traffic for multiple VLANs simultaneously.

Inter-VLAN Routing (Router-on-a-Stick)

Inter-VLAN routing is enabled using a **single physical router interface** divided into multiple **subinterfaces**. Each subinterface corresponds to a VLAN and acts as the **default gateway** for that VLAN.

On the router:

- One physical interface connects to the switch
- Subinterfaces are created (e.g. Gig0/0.10, Gig0/0.20, Gig0/0.30)
- Each subinterface is configured with:
  - encapsulation dot1Q for VLAN tagging
  - An IP address to serve as the VLAN gateway

This allows the router to receive tagged frames from the switch, route them between VLANs, and send them back appropriately.

Traffic Flow Explanation

When a device in one VLAN sends traffic to a device in another VLAN:

1. The PC sends the packet to its **default gateway** (router subinterface)
2. The switch forwards the frame over the **trunk link** to the router

3. The router routes the packet to the destination VLAN
4. The packet is sent back through the trunk to the switch
5. The switch forwards the frame to the destination PC

This process enables controlled communication between VLANs while maintaining logical separation.

Protocols Used

- **IEEE 802.1Q** – VLAN tagging on trunk links
- **IPv4** – logical addressing
- **Inter-VLAN Routing** – routing between VLANs via subinterfaces
- **ICMP** – connectivity testing using ping

Key Commands Used and Their Purpose

On the Switch:

- vlan – create VLANs
- name – label VLANs by department
- switchport mode access – configure access ports
- switchport access vlan – assign ports to VLANs
- switchport mode trunk – enable trunking to the router
- show vlan brief – verify VLAN configuration

On the Router:

- interface g0/0.x – create subinterfaces
- encapsulation dot1Q – enable VLAN tagging
- ip address – assign gateway IPs
- no shutdown – activate interfaces
- show ip interface brief – verify subinterface status