# DOCUMENTATION

# Enterprise Inter-VLAN Communication and Dynamic Routing Configuration Using OSPF

## Introduction

The increasing complexity of enterprise networks necessitates solutions for efficient segmentation, dynamic routing, and scalability. This project, "Enterprise Inter-VLAN Communication and Dynamic Routing Configuration Using OSPF," focuses on designing and implementing a network infrastructure that ensures seamless communication between different departments while maintaining scalability and adaptability through dynamic routing.  
  
This documentation provides an in-depth explanation of the network topology, configurations, and protocols implemented to achieve the project's objectives.

## Objectives

1. Implement VLAN Segmentation for Network Efficiency: Configure VLANs for departments (IT, HR, Sales, and Servers) to enhance network segmentation and improve security and manageability.   
2. Enable Inter-VLAN Communication Using Router-on-a-Stick: Configure a router-on-a-stick setup for inter-VLAN routing to allow seamless communication between different VLANs.  
3. Deploy OSPF Protocol for Scalable Dynamic Routing: Configure OSPF across routers to ensure dynamic, scalable routing between VLANs and remote networks, simulating branch connectivity.

## Network Topology Overview

The network design includes:   
- Four main VLANs representing different departments: IT, HR, Sales, and Servers.  
- A core router configured as a router-on-a-stick for inter-VLAN communication.  
- Dynamic routing between VLANs and a branch office simulated using the OSPF protocol.

Key Devices:   
- Cisco 2960 switches for VLAN segmentation.   
- Cisco 2911 routers for inter-VLAN routing and OSPF configuration.   
- PCs and servers for testing connectivity and services such as DHCP, DNS, and web hosting.

## Implementation Details

1. VLAN Configuration   
   - Each department is assigned a unique VLAN ID:   
    - IT: VLAN 10   
    - HR: VLAN 20   
    - Sales: VLAN 30   
    - Servers: VLAN 40   
   - Configure VLANs on the switches using the vlan database command.   
   - Assign specific switch ports to respective VLANs.   
     
   2. Router-on-a-Stick Setup   
   - Configure sub-interfaces on the core router (Router0) for each VLAN:   
    - Example: interface GigabitEthernet0/0.10 for VLAN 10.   
    - Assign IP addresses to subinterfaces to act as default gateways for VLANs.   
   - Enable 802.1Q encapsulation for VLAN tagging.   
     
   3. OSPF Configuration   
   - Enable OSPF on all routers:   
    - Define OSPF process ID and assign network ranges to areas.   
    - Example: router ospf 1 and network 192.168.10.0 0.0.0.255 area 0.   
   - Configure routing between VLANs and a secondary branch router.   
   - Verify OSPF neighbors and routing tables to ensure connectivity.

## Testing and Verification

1. Inter-VLAN Communication: Use ping and traceroute commands from PCs in different VLANs to ensure successful communication.   
  
2. Dynamic Routing Verification:   
 - Check OSPF neighbor relationships using the show ip ospf neighbor command.  
 - Validate the routing table using the show ip route command.   
  
3. Server Connectivity:   
 - Ensure DHCP servers assign IP addresses to PCs correctly.  
 - Verify DNS resolution and access to web servers.

## Results and Observations

1. VLAN segmentation successfully isolated department traffic while allowing inter-VLAN communication.   
2. OSPF dynamically adapted to network changes and routed traffic efficiently between VLANs and the branch network.   
3. All services, including DHCP, DNS, and web hosting, functioned as expected, ensuring end-to-end connectivity.

## Conclusion

The project successfully demonstrated the implementation of inter-VLAN communication and dynamic routing using OSPF. The design provides scalability, efficient network management, and adaptability to future expansion. This setup is ideal for enterprises requiring robust and dynamic network solutions.

## Future Enhancements

1. Integrate firewall rules to enhance network security.   
2. Implement redundancy protocols such as HSRP or VRRP for high availability.  
3. Expand the design to include wireless connectivity and VPN support for remote users.