

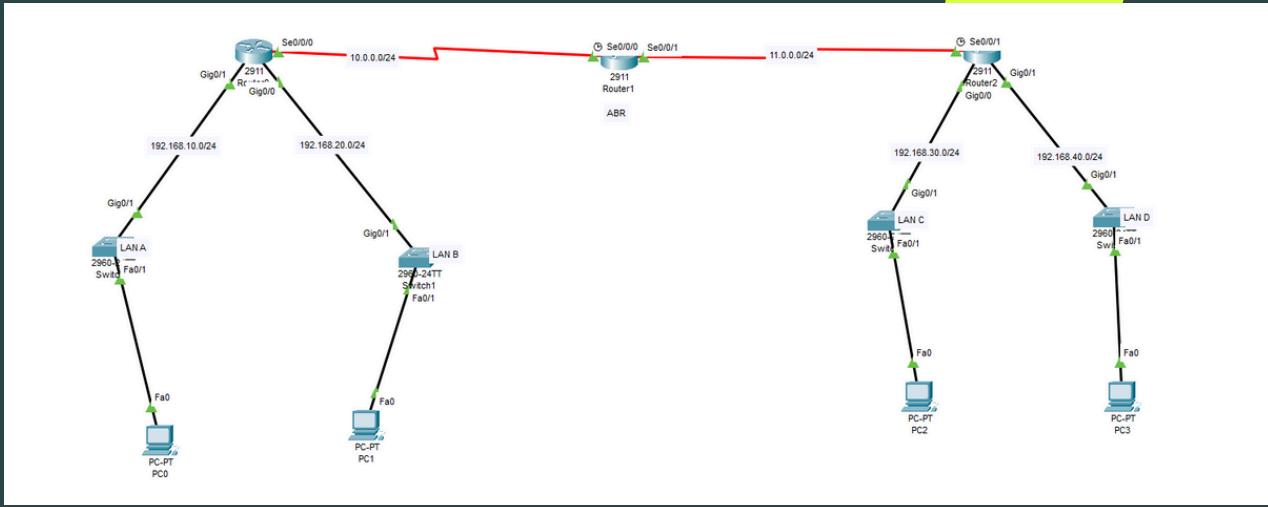
# SECURE WAN CONNECTIVITY

CATEGORY  
NETWORKING

Author: Md Rezvee Parvez

ENVIRONMENT  
CISCO PACKET TRACER





# PROJECT SUMMARY —

Modern enterprise networks require scalable routing mechanisms and strong access control to ensure secure communication across geographically distributed locations. This project focuses on designing and implementing a secure Wide Area Network (WAN) using OSPF (Open Shortest Path First) for dynamic routing and Access Control Lists (ACLs) to enforce traffic segmentation and security policies. The lab simulates a multi-router enterprise WAN where user networks, a head office network, and a management network must communicate securely while preventing unauthorized lateral movement between user segments.



## PROJECT OBJECTIVES

- To design and configure a multi-router WAN topology
- To implement multi-area OSPF for scalable and efficient routing
- To apply standard and extended ACLs to enforce least-privilege access
- To validate routing and security behavior through structured testing

# NETWORK TOPOLOGY OVERVIEW

## TOPOLOGY

- 3 routers connected via serial WAN links
- Four LAN segments, each representing a different functional role
- One Area Border Router (ABR) connecting OSPF Area 0 and Area 1

THIS DESIGN REFLECTS REAL-WORLD ENTERPRISE PRACTICES, WHERE AREA 0 SERVES AS THE BACKBONE AND OTHER AREAS ARE USED TO IMPROVE SCALABILITY AND ROUTING EFFICIENCY.

## IP Addressing Scheme

### WAN LIINKS

Link	OSPF Area	Network
Router 1↔Router 2	Area 0	10.0.0.0/8
Router 2↔Router 3	Area 1	11.0.0.0/8

### LAN LIINKS

LAN	Purpose	Network
LAN A	User Network	192.168.10.0/24
LAN B	Head Office	192.168.20.0/24
LAN C	Branch User Network	192.168.30.0/24
LAN D	Management Network	192.168.40.0/24

# ROUTING IMPLEMENTATION (OSPF)

## KEY FEATURES IMPLEMENTED

- Multi-area OSPF configuration
- Area Border Router (ABR) connecting Area 0 and Area 1
- Dynamic route advertisement of LAN and WAN networks

## VERIFICATION

- show ip ospf neighbor to confirm neighbor adjacency (FULL state)
- show ip route ospf to verify learned routes
- End-to-end connectivity tests across LANs

## WHY EXTENDED ACL USED

- Source IP address
- Destination IP address
- Protocol type

**OSPF  
PROTOCOL**  
Open Shortest  
Path First

## Security Policy Design

- User networks are allowed to access the Head Office network
- Direct communication between user LANs is restricted
- The Management network is allowed unrestricted access
- ICMP is permitted selectively for troubleshooting
- All other traffic is denied by policy

Note: All tests confirmed correct VLAN segmentation and inter-VLAN connectivity.

# ACL AND RULES IMPLEMENTED

## ACL PLACEMENT STRATEGY

- Extended ACLs were applied close to the source networks
- This prevents unauthorized traffic from entering the WAN and conserves bandwidth

## KEY ACL RULES ENFORCED

- Permit user LANs to communicate with the Head Office network
- Deny user-to-user LAN communication (lateral movement prevention)
- Permit ICMP only where explicitly required
- Allow all other essential traffic to avoid disrupting routing operations

## TESTING AND VALIDATION

- OSPF neighbor relationships reached FULL state
- All networks were dynamically learned and reachable as expected

## SECURITY VALIDATION

Controlled ping tests were performed to validate ACL behavior:

Source	Destination	Result
LAN A	LAN B	SUCCESS
LAN A	LAN C	BLOCKED
LAN C	LAN B	SUCCESS
LAN C	LAN A	BLOCKED

# CHALLENGES & OUTCOMES

During testing, ICMP traffic was initially permitted unintentionally due to overly broad ACL rules. This issue was resolved by refining rule order and scoping ICMP permissions to specific destination networks.

## THIS TROUBLESHOOTING STEP REINFORCED THE IMPORTANCE OF:

- ACL rule order (top-down processing)
- Protocol-specific filtering
- Validation through real traffic testing

## LEARNING OUTCOMES

- Designing scalable WAN topologies using multi-area OSPF
- Implementing and troubleshooting extended ACLs
- Applying least-privilege security principles
- Validating network behavior using structured testing

## CONCLUSION

This project successfully demonstrates the implementation of a secure, scalable WAN architecture using OSPF and ACLs. By combining dynamic routing with carefully designed access controls, the network achieves both operational efficiency and strong security segmentation. The project closely mirrors real-world enterprise networking scenarios and serves as a strong portfolio example of routing and security fundamentals.

---

# THANK YOU —

This project demonstrated the successful design and implementation of a secure, scalable WAN using multi-area OSPF for dynamic routing and extended ACLs for traffic segmentation. Proper validation and troubleshooting ensured that routing operated correctly while unauthorized inter-LAN communication was effectively restricted. Overall, the lab reflects real-world enterprise networking practices and reinforces the importance of combining routing efficiency with security controls.

Author: Md Rezvee Parvez

contact me:

rezvx@proton.me <https://www.linkedin.com/in/rezvx>