# Scalable Network Expansion & Change Control

## Objective

This lab simulates controlled enterprise network expansion within a routed multi-site topology while preserving routing stability and enforcing scoped security policy. The implementation includes migration of HQ to Router-on-a-Stick (ROAS) architecture, introduction of a new branch growth segment, dynamic EIGRP route advertisement updates, and structured ACL enforcement to protect critical server infrastructure without disrupting permitted traffic flows.

## Topology Overview

- HQ VLAN 10 (Users) – 10.10.10.0/24
- HQ VLAN 40 (Servers) – 10.10.40.0/24
- Branch LAN – 10.10.20.0/24
- Branch Growth LAN – 10.10.30.0/24
- Transit WAN Links – 10.0.12.0/30, 10.0.23.0/30
- Dynamic Routing Protocol – EIGRP AS 100

The topology maintains full Layer 3 segmentation between sites while enabling controlled inter-site communication via dynamic routing.

## Implementation

### HQ Migration to Router-on-a-Stick (ROAS)

- Configured 802.1Q trunk between SW1-HQ and R1-HQ
- Implemented router subinterfaces for VLAN 10 and VLAN 40
- Assigned dedicated server gateway for VLAN 40
- Relocated SRV-1 to 10.10.40.100 within isolated server segment

This migration preserved inter-VLAN routing functionality while improving segmentation and scalability.

### Branch Growth Deployment

- Introduced new LAN segment: 10.10.30.0/24
- Advertised network via EIGRP AS 100
- Verified route propagation across R1–R2–R3
- Confirmed routing table consistency and absence of convergence disruption

This migration preserved inter-VLAN routing functionality while improving segmentation and scalability.

### Access Control Policy Enforcement

Configured extended ACL on R3 to restrict branch-to-server access:

- Deny: 10.10.20.0/24 to 10.10.40.100
- Permit: All other traffic

ACL applied inbound on source-facing interface (R3 G0/0) to enforce policy closest to origin.

During validation, an order-of-operations issue (permit above deny) was identified and corrected. The ACL was reordered to ensure the deny statement is evaluated before the general permit.

Enforcement verified using:

- Controlled ping testing (expected deny behavior)
- Positive traffic validation for permitted flows
- ACL hit counter monitoring to confirm rule engagement

## Validation Evidence

- Verified EIGRP route propagation for VLAN 40 and Branch Growth networks across R1–R2–R3.
- Confirmed permitted end-to-end connectivity remained intact post-change.
- Validated targeted denial (10.10.20.0/24 to 10.10.40.100) using controlled tests and ACL hit counters.
- Ensured routing stability and absence of unintended traffic disruption following implementation.

## Key Technical Concepts Demonstrated

- Implemented VLAN segmentation and inter-VLAN routing via Router-on-a-Stick (802.1Q trunking + subinterfaces).
- Integrated dynamic routing updates with EIGRP and validated convergence across a multi-router topology.
- Designed and corrected extended ACL sequencing to enforce precise traffic policy.
- Applied structured change control with impact validation through routing and traffic analysis.