

Cisco-Based Enterprise Network Simulation using CML

Project Introduction

This project aims to simulate an enterprise-grade network infrastructure using **Cisco Modeling Labs (CML)** as the primary emulation platform. The objective is to validate critical Layer 2 and Layer 3 technologies in a safe, scalable, and repeatable environment. Automation is introduced using **Ansible** to streamline configuration management and reduce human error. The simulation serves to minimize risks typically associated with physical lab environments and provides practical insights into real-world enterprise network behavior.

Key Technologies Covered:

- MST, EtherChannel, HSRP
 - OSPF, EIGRP, eBGP
 - Ansible-driven automation
-

Lab 1: Layer 2 Redundancy and High Availability

Topology:

A 2-Tier Campus Core design composed of Distribution and Access layers.

Implemented Features:

- VLAN segmentation and trunking between switches
- Switched Virtual Interfaces (SVIs) for inter-VLAN routing
- **MST (Multiple Spanning Tree)** for loop prevention
- **EtherChannel (LACP)** for link aggregation
- **HSRP** for first-hop redundancy

Verification:

- Simulated link and device failure to test HSRP failover
 - MSTP convergence verified via blocking and forwarding port states
-

Lab 2: Multi-Protocol Routing and Edge Connectivity

Focus:

A side-by-side comparison of **OSPF**, **EIGRP**, and **eBGP** behavior in a hybrid routing environment.

Configured Features:

- **Route redistribution** between IGP and BGP
- **Policy-Based Routing (PBR)** for custom forwarding behavior
- **NAT/PAT** for simulated internet access scenarios

Validation Methods:

- Used ping and traceroute to confirm connectivity across paths
 - Adjusted metric/cost values to verify routing decisions and failover behavior
-

Lab 3: Configuration Automation via Ansible**Objective:**

Automate routine configuration tasks across CML devices to improve consistency and deployment speed.

Setup Overview:

- Inventory of CML-hosted **Cisco IOS** devices defined in Ansible
- Developed playbooks for:
 - VLAN and interface provisioning
 - Fetching of device information
 - Basic security features

Execution & Validation:

- Ansible playbooks pushed to live devices
- Logs compared before and after execution to confirm changes
- Verified idempotency and output correctness

Outcome:

Demonstrated the value of using **infrastructure-as-code** practices in network engineering by enabling faster, error-free configuration rollouts.

