DDANEP CCNA v2 Enterprise Network Lab

A persistent Cisco Modeling Labs implementation

21 nodes	24 links	3 persistent servers

Executive summary

DDANEP designed, implemented and validated a multi-site enterprise learning environment in Cisco Modeling Labs. The project combines campus switching, a routed headquarters core, a branch office, multi-area OSPF, centralized infrastructure services, public and internal web services, and simulated internet access.

The final artifact contains 21 nodes and 24 links. Seven Cisco devices retain extracted startup configurations, while three Ubuntu servers rebuild automatically from embedded cloud-init user-data and network-config files.

This is an independently developed educational environment aligned with CCNA 200-301 v2.0 objectives. It demonstrates engineering workflow and troubleshooting discipline; it is not presented as a production deployment template.

Project objectives

- Build a hierarchical headquarters and branch topology.
- Implement VLAN segmentation and secure unused access ports.
- Configure 802.1Q trunks, LACP EtherChannels and Rapid PVST+.
- Route headquarters and branch networks through multi-area OSPF.
- Centralize DHCP and DNS on an Ubuntu infrastructure server.
- Provide internal and public HTTP/HTTPS services with Nginx.
- Simulate internet connectivity and PAT through an ISP router.
- Preserve the complete environment across clean CML imports.
- Produce a repeatable senior-level implementation and troubleshooting runbook.

Architecture

The headquarters uses two core switches and one access switch. The core pair is connected by Layer 2 and Layer 3 LACP EtherChannels. Headquarters VLANs are advertised through OSPF Area 10, the branch networks through Area 20, and the routed transit links through Area 0.

HQ-R1 originates the enterprise default route and performs PAT toward ISP-R1. ISP-R1 connects the enterprise, a public server network and the CML external connector.

The Linux service roles are:

- HQ-INFRA-SRV1: centralized Dnsmasq DHCP and DNS.
- HQ-WEB-SRV1: internal Nginx HTTP/HTTPS service.
- PUBLIC-WEB-SRV1: public-network Nginx HTTP/HTTPS service.

Persistence engineering

Each Ubuntu server uses two embedded CML configuration files:

- `user-data` installs packages, writes application configuration, creates systemd services and enables services.
- `network-config` assigns the static address, gateway and DNS resolver to `ens2`.

CML presents these files through DataSourceNoCloud. A fresh import therefore reconstructs the server identity, networking and application services without repeating the manual installation.

Validation completed

- LACP member links bundled successfully at Layer 2 and Layer 3.
- Trunks used the approved VLAN list and native VLAN 999.
- Rapid PVST+ produced the intended root and alternate-port behavior.
- OSPF adjacencies reached FULL state across the backbone.
- Inter-area routes appeared as expected at headquarters and the branch.
- Headquarters and branch clients received the correct DHCP leases.
- Internal DNS resolved the DDANEP internal and public service names.
- Internal and public websites returned HTTP and HTTPS `200 OK`.
- The public server reached the internet through the CML external connector.
- NAT/PAT translations were observed on HQ-R1 and ISP-R1.
- A clean import rebuilt the three Ubuntu servers and restored their services.

Troubleshooting lessons

The project reinforced several operational principles:

1. Verify physical and data-link state before investigating routing.
2. Treat the first failed ping as possible ARP convergence and repeat the test.
3. Match trunk encapsulation, native VLAN and allowed VLANs on both ends.
4. Form EtherChannels only after confirming identical member configuration.
5. Distinguish DNS `NXDOMAIN` from `connection refused`; they indicate different failure domains.
6. Wait for `cloud-init status --wait` before judging a freshly imported Ubuntu node.
7. Confirm the active resolver with `resolvectl status`, not only the nameserver list.
8. Generate traffic before expecting NAT translation entries.

9. Save Cisco configurations and extract them only after stopping the lab.

10. Preserve the final YAML with a checksum and a tested recovery copy.

Production qualification

The laboratory intentionally uses visible training credentials and self-signed certificates. A production implementation would also require AAA, SSH keys, restricted management access, trusted PKI, inter-VLAN security policy, FHRP, centralized logging, NTP, monitoring, redundant services and documented recovery objectives.

Project deliverables

- Certified CML YAML topology.
- Senior implementation and troubleshooting runbook.
- SHA-256 integrity manifest.
- Publication-readiness and security qualification notes.

Credit

Concept, design, implementation, testing and documentation: DDANEP.

Cisco and Cisco Modeling Labs are trademarks of their respective owners. This independent educational project is not affiliated with or endorsed by Cisco.

Educational scope	**This independent environment demonstrates repeatable engineering practice aligned with CCNA 200-301 v2.0. Training credentials and self-signed certificates are intentionally non-production values.**