+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 06/08/2026

Sign up

Cisco ENARSI Certification Training

3 days (21 hours)

Overview

The Cisco CCNP 300-410 ENARSI training course prepares you to troubleshoot and optimize enterprise networks based on OSPF, EIGRP, BGP, redistribution, and VPN. It focuses on real-world scenarios: routing incidents, instability, loops, connectivity loss, and degraded performance.

You will learn to quickly isolate root causes, validate hypotheses using IOS commands, and apply safe fixes in production. The approach emphasizes methodology: collection, analysis, action plan, verification, and documentation.

The training centers on troubleshooting workshops and guided demos (multi-protocol topologies, failure scenarios, log captures). Deliverables: diagnostic checklists, procedure templates, and reusable reference configurations.

Objectives

- Diagnose IPv4/IPv6 routing issues on IOS.
- Troubleshoot OSPF (adjacencies, LSAs, convergence) and EIGRP.
- Analyze and resolve BGP incidents (peering, attributes, policies).
- Implement and validate route redistribution and filtering.
- Resolve issues related to VPNs and WAN connectivity.

Target Audience

- Network administrators
- N2/N3 support engineers
- Operations/production engineers
- Network consultants

Prerequisites

- Solid foundation in IP routing and subnetting
- Operational knowledge of OSPF, EIGRP, and BGP
- Understanding of ACLs, NAT, and VRFs
- Practical experience with IOS commands (show, debug, logs)

Technical prerequisites

- Lab tool: CML, EVE-NG, or GNS3
- SSH client (Terminal, PuTTY) and text editor

Curriculum for our Cisco Certified Network Professional 300-410 ENARSI training

[Day 1 - Morning]

Architecture and preparation for advanced troubleshooting (ENARSI)

- Review of core/distribution/access roles and their impact on troubleshooting
- Reading and using tables: ARP, MAC, CEF, routing
- Diagnostic methodology: hypotheses, testing, validation, rollback
- IOS XE tools: show, debug, logging, SPAN/ERSPAN
- Hands-on workshop: Implementing a diagnostic plan and gathering clues for a simulated incident.

[Day 1 - Afternoon]

Advanced routing: EIGRP (troubleshooting and optimization)

- EIGRP adjacencies: K-values, timers, authentication, MTU, and causes of flapping
- Optimization: stub, summarization, variance, leak-map
- Filtering and control: distribute-list, prefix-list, route-map
- Convergence analysis: DUAL, feasible successor, stuck-in-active
- Hands-on Workshop: Diagnosing a loss of adjacency and correcting an EIGRP redistribution.

[Day 2 - Morning]

Advanced Routing: OSPF (multi-area and troubleshooting)

- OSPF neighbor states and checks: area-id, network type, DR/BDR, MTU, auth
- Multi-area design: backbone, ABR, area types (stub, NSSA)
- LSA and LSDB: reading, propagation, causes of inconsistencies

- Optimization: summarization, passive-interface, timers, SPF/LSA throttling
- Hands-on workshop: Troubleshooting an NSSA area issue and restoring route visibility.

[Day 2 - Afternoon]

BGP for the enterprise: eBGP/iBGP, policies, and troubleshooting

- Session establishment: states, TCP/179, TTL, update-source, multihop
- Attributes and route selection: local-pref, AS-path, MED, communities
- Route control: prefix-list, route-map, inbound/outbound filtering
- Stability and scalability: next-hop-self, route-reflector (principles), dampening (concepts)
- Hands-on workshop: Correct a BGP policy (route-map) blocking prefixes and validate the best path.

[Day 3 - Morning]

VPNs and tunnels: GRE, IPsec, and DMVPN (troubleshooting)

- GRE: encapsulation, MTU/MSS, keepalive, and fragmentation symptoms
- IPsec: IKEv2 phases, proposals, transform sets, PFS, and causes of failure
- DMVPN: NHRP, mGRE, spoke-to-spoke, and key checks
- Targeted debugging tools: crypto session, ipsec sa, ikev2 sa, nhrp
- Hands-on workshop: Diagnosing a downed DMVPN tunnel (NHRP/IKE/IPsec) and restoring traffic.

[Day 3 - Afternoon]

Services and security: redistribution, ACL, QoS, and end-to-end validation

- Redistribution: loops, tags, metrics, and control via route-map
- ACLs and filtering: order, implicit deny, critical items to check (ICMP, routing)
- QoS: classification/marking, LLQ, shaping/policing, and impacts on voice
- End-to-End Validation: application tests, extended traceroute, captures, and log correlation
- Hands-on workshop: Fixing a redistribution loop and applying simple QoS validated by measurements.

Target Audience

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Entry-level assessment

The assessment conducted at the start of the training program complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.