MERCURY

Enterprise SD-WAN Architecture, Design, and Implementation Training Course

31 May – 4 June 2027
Barcelona (Spain)



Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

MERCURY

Enterprise SD-WAN Architecture, Design, and Implementation Training Course

Ref: 28_1082096 **Date:** 31 May – 4 June 2027 **Location:** Barcelona (Spain) **Fees:** 6200 Euro

The Enterprise SD-WAN Architecture, Design, and Implementation Training Course is a one-week professional course for network engineers, infrastructure architects, and technical operations specialists responsible for deploying software-defined wide area network fabrics. Working through control plane designs, underlay transports, and policy orchestration, you build an Enterprise SD-WAN Architecture and Deployment Blueprint. This course is delivered by Mercury Training Center to establish resilient enterprise network connectivity.

About This Course

Legacy wide area networks struggle with rigid multiprotocol label switching contracts, cloud application latency, and complex branch security management. To follow this course, you must already manage enterprise routing protocols, configure virtual private networks, and administer firewall policies at work. Through hands-on design models and traffic orchestration scenarios, you master scalable multi-transport network migration.

Who It Is For

- Professionals responsible for architecting multi-transport enterprise connectivity across cloud and branch data environments
- Professionals responsible for deploying centralized control planes, routing policies, and secure edge appliance configurations
- Professionals responsible for integrating wide area transport security with cloud access gateways and threat defenses
- Professionals responsible for monitoring application performance metrics and troubleshooting software-defined transport failovers

This course is not for entry-level desktop support technicians seeking introductory cabling and local area network basics, nor is it for application programmers requiring custom software development frameworks.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Competencies You Will Build

- Fabric Architecture Design: Defining decoupled control, management, and data plane topologies across distributed hybrid edge sites.
- Underlay Transport Integration: Aggregating private multiprotocol label switching, broadband internet, and cellular connections under standard service attributes.
- Centralized Policy Orchestration: Engineering application-aware routing rules, traffic steering thresholds, and localized data forwarding policies.
- Transport Security Enforcement: Aligning secure network access, data plane segmentation, and intrusion protection with statutory network controls.
- Branch Edge Provisioning: Streamlining zero-touch edge onboarding workflows, cryptographic authentication, and equipment compliance verification.
- Application Performance Monitoring: Tracking jitter, packet loss, and latency metrics to enforce stringent service level agreements.

What You Will Be Able to Do

By the end of the course you will be able to:

- From enterprise connectivity requirements, construct a multi-site SD-WAN topology separating control, data, and management plane functions.
- Given diverse carrier circuits, map underlay transports into standardized overlay tunnels conforming to MEF 70.2 service attributes.
- Using centralized controller platforms, configure application-aware routing policies to steer mission-critical traffic past transport degradation.
- From regulatory security baselines, design network segmentation and threat inspection matching NCA ECC-2:2024 control subdomain 2-5 requirements.
- Given hardware onboarding schedules, establish edge equipment staging and validation workflows fulfilling CST Type Approval prerequisites.
- Using synthetic telemetry and application quality metrics, diagnose transit path faults and optimize direct internet breakout routes.

Course Content

Day 1: Principles of Enterprise SD-WAN Architecture

- Decoupled Control, Data, Management, and Orchestration Planes in Modern SD-WAN
- Underlay Connectivity Services and Performance Metrics Defined by MEF 70.2
- Controller Topologies, High Availability Clustering, and Secure Discovery Protocols
- Zero-Touch Provisioning Workflows and Cryptographic Identity Certificates
- Overlay Management Protocol Operation and Routing Table Distribution Mechanics

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

Day 2: Underlay Connectivity and Transport Design

- Hybrid Transport Design Combining Private Circuits, Public Broadband, and Cellular Links
- Bidirectional Forwarding Detection and Overlay Tunnel Path Health Monitoring
- Direct Internet Access Architecture and Local Cloud Application Breakout Policies
- Transport Staging Requirements and CST Type Approval Verification via SABER Platform
- Carrier Service Level Agreements and Application Quality of Experience Metrics

Day 3: Centralized Traffic Engineering and Policy Frameworks

- Application Identification Engine Configuration and Deep Packet Inspection Rules
- Application-Aware Routing Policies Based on Latency, Jitter, and Packet Loss Thresholds
- Centralized Data Policies and Localized Control Policies for Traffic Forwarding
- Security Policy Framework Alignment Spanning SD-WAN and SASE Under MEF 95
- Multicast Routing Topologies and Quality of Service Queuing Schedules across Overlays

Day 4: Network Security, Segmentation, and Statutory Compliance

- End-to-End Enterprise Segmentation across Virtual Private Network Topologies
- Edge Security Integration Featuring Intrusion Prevention and Secure Web Gateways
- Network Security Implementation Aligned with NCA ECC-2:2024 Subdomain 2-5 Controls
- Distributed Denial of Service Protection Integration Under Clause 2-5-3-9
- Cryptographic Key Lifecycle and In-Transit Data Protection Under Subdomain 2-8

Day 5: Fabric Implementation and Blueprint Finalization

- Exercise on Multi-Tenant Controller Staging and High Availability Failover Validation
- Exercise on Direct Internet Breakout Policy Deployment and Application Traffic Steering
- Exercise on Branch Edge Provisioning and Cryptographic Trust Verification
- Exercise on Network Segmentation Auditing Against Statutory Cybersecurity Frameworks
- Finalization of the Enterprise SD-WAN Architecture and Deployment Blueprint

Case Studies and Exercises

These suggested activities provide practical application of technical network architecture across diverse sectors:

- Case study: A commercial retail group where you architect direct internet breakout and application-aware routing across hundreds of distributed store branches.
- Case study: A healthcare provider where you segment clinical imaging, patient telemetry, and guest traffic to satisfy strict network security controls.
- Exercise: A financial enterprise scenario where you map encrypted overlay tunnels across hybrid multiprotocol label switching and internet transports.
- Exercise: An edge device onboarding workflow where you validate hardware conformity schedules and equipment type approval submission records.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

What You Take Back

The Enterprise SD-WAN Architecture and Deployment Blueprint equips you to plan, commission, and optimize wide area network fabrics during your first month back at work. You will use it to validate controller designs, standardize edge provisioning, and verify regulatory network compliance across enterprise branch locations.

- Detailed controller architecture schema with high availability clustering and transport interface maps
- Application-aware traffic steering matrix with quantitative delay, loss, and jitter thresholds
- Edge appliance provisioning checklist incorporating equipment type approval and staging milestones
- Cybersecurity control alignment workbook mapping overlay segments to network security standards

Quick Answers FAQ

What background is required before attending the Enterprise SD-WAN Architecture, Design, and Implementation Training Course?

You need practical experience administering enterprise IP networks, configuring dynamic routing protocols such as BGP and OSPF, and managing site-to-site IPsec virtual private networks. Prior experience with command-line interface device configuration and enterprise firewall rules will help you complete policy design exercises effectively.

How does this course differ from conventional router configuration training?

Conventional routing courses concentrate on box-by-box interface management, localized routing metrics, and individual device command sets. This course addresses software-defined fabric orchestration, centralized control plane architecture, automated edge onboarding, and cross-carrier policy enforcement across entire wide area network environments.

Why are organizations replacing legacy WAN architectures with SD-WAN?

Organizations adopt software-defined wide area networking to aggregate diverse transport providers, lower private line costs, improve direct access to cloud workloads, and enforce uniform security policies dynamically without requiring manual reconfigurations across distributed branch locations.

What work product do you take back from this training?

You return with the Enterprise SD-WAN Architecture and Deployment Blueprint, complete with controller topology specifications, traffic steering matrices, equipment onboarding checklists, and regulatory security control mappings ready for immediate enterprise implementation.

Dubai - UAE: +971 4 450 5697
Istanbul - Türkiye: +90 539 599 1206
Amman - Jordan: +962 79 712 3347

For Your Manager

This course develops the practical capability to architect, migrate, and govern software-defined wide area network fabrics across hybrid enterprise infrastructures. The participant returns with a completed Enterprise SD-WAN Architecture and Deployment Blueprint, which provides direct technical utility when retiring obsolete carrier circuits, establishing resilient application routing policies, and fulfilling mandatory statutory network cybersecurity controls across branch facilities.