



SD-WAN and SASE Training Course: Overlay Design, Zero Trust Access and MPLS Migration



SD-WAN and SASE Training Course: Overlay Design, Zero Trust Access and MPLS Migration

Introduction:

SD-WAN and SASE training on overlay design, zero trust access and MPLS migration is a 1-week course for network architects, security architects and WAN service owners that ends with an SD-WAN and SASE Migration Roadmap. Multi-site organisations still backhaul branch and remote-user traffic through costly private circuits and central security stacks, so cloud applications run slowly and access policy differs between sites. Nominees already run enterprise WANs or perimeter security, and each day is taught through case studies on realistic branch estates. CoreConcept Training Center delivers this SD-WAN and SASE course.

Course Objectives:

- Assess an existing hub-and-spoke WAN and remote-access estate against cloud traffic patterns, branch growth and circuit spend to build the business case for change
- Design an SD-WAN overlay with edge, gateway, orchestrator and controller roles, topology choices and segmentation using MEF 70 service attributes
- Specify application-aware routing policies, path quality thresholds and underlay transport mixes of broadband, cellular and private circuits for each site tier
- Select and sequence Security Service Edge functions such as ZTNA, secure web gateway, CASB and FWaaS against NIST SP 800-207 zero trust tenets
- Plan a phased exit from MPLS with pilot sites, coexistence routing, cutover waves and rollback criteria
- Define a converged network and security operating model with policy ownership, service levels and provider governance for SASE

Target Audience:

- Network architects responsible for the design of enterprise WAN topology, branch connectivity and data centre interconnection
 - Security architects responsible for remote access, web and cloud application protection and zero trust strategy
 - WAN service owners responsible for carrier contracts, circuit renewals and branch connectivity service levels
 - Infrastructure leads responsible for multi-site rollouts, branch standardisation and transformation budgets
 - Technical procurement and vendor managers responsible for evaluating managed SD-WAN and SASE offers
-

Course Outline:

Day 1: WAN Modernisation Drivers and Current-State Assessment

- Hub-and-Spoke Backhaul Limits for Cloud and SaaS Traffic
- SD-WAN, SSE and SASE Definitions and Market Architecture Models
- Branch Estate Inventory with Site Tiers and Application Profiles
- Circuit Spend and Contract Renewal Baseline Worksheet
- Current-State WAN Assessment Scorecard and Gap Register

Day 2: SD-WAN Overlay Architecture and MEF 70 Service Model

- MEF 70 Service Attributes for Overlay Connectivity and Policy
- Edge, Gateway, Orchestrator and Controller Role Placement
- Full-Mesh, Regional Hub and Cloud On-Ramp Topology Options
- IPsec Tunnel Fabric, Key Rotation and Overlay Segmentation Design
- Zero-Touch Provisioning Workflow for New Branch Edge Devices

Day 3: Application-Aware Routing, Underlay Selection and Branch Design

- Deep Packet Inspection Application Classification and Policy Groups
- Loss, Latency and Jitter Thresholds for Dynamic Path Steering
- Forward Error Correction and Packet Duplication for Real-Time Voice
- Broadband, Cellular and Private Circuit Underlay Mix by Site Tier
- Branch Edge High Availability and Last-Mile Diversity Patterns

Day 4: SASE Security Services, Zero Trust Access and Migration Risk

- NIST SP 800-207 Policy Decision and Enforcement Points Applied
- ZTNA Application Connectors Replacing Full-Tunnel Remote Access
- Secure Web Gateway and TLS Inspection Exemption Rules
- CASB Inline and API Modes for Sanctioned SaaS Control
- Single-Vendor Versus Dual-Vendor SASE Selection Criteria Matrix

Day 5: Case Study Building an SD-WAN and SASE Migration Roadmap

- Case Organisation Site Tiering and Target Overlay Blueprint
 - Case Pilot Site Selection and MPLS Coexistence Routing Plan
 - Cutover Wave Schedule with Rollback Criteria and Acceptance Tests
 - NetSecOps Operating Model with RACI and Provider Service Levels
 - SD-WAN and SASE Migration Roadmap Completion and Panel Review
-

Skills You Will Gain:

- WAN Transformation Business Case
- Overlay Topology Design
- Application Path Policy Engineering
- Underlay Transport Selection
- Zero Trust Access Architecture
- SSE Service Evaluation
- Phased Cutover Planning
- NetSecOps Governance

Why Attend This Course:

- Hand the infrastructure director and the architecture board an SD-WAN and SASE Migration Roadmap with site tiers, target overlay, security services and cutover waves
- Choose between single-vendor and dual-vendor SASE, and between full and partial MPLS exit, on documented criteria
- Avoid application outages, user disruption and overlapping contracts caused by unplanned cutovers and poorly sized underlay links
- Share site tiering templates, path policy tables and cutover acceptance tests with the engineers who run the rollout

Conclusion:

Back at work, the participant hands the SD-WAN and SASE Migration Roadmap to the infrastructure director, the security lead and procurement, who use it to approve the target overlay, the security service model and the first pilot sites before tendering. Operations teams take its path policy tables and operating model as the starting point for rollout. After the pilot wave, the unit should compare application performance, circuit spend and remote-access incidents with the baseline, then adjust site tiers, path thresholds and the remaining cutover waves.

Frequently Asked Questions FAQ:

What should participants know before an SD-WAN and SASE training course?

Participants should already understand IP routing, VPN tunnels and basic firewall policy, and have worked on an enterprise WAN or remote-access service. A site list, circuit inventory or application list from their own organisation makes the case work more useful.

How does an SD-WAN and SASE course differ from a carrier MPLS backbone design course?

This course designs the enterprise side: overlays across mixed transports, application path policy, zero trust access and the exit from private circuits. A carrier backbone course designs the provider core itself, with interior routing, label switching and traffic engineering.

Does SASE replace SD-WAN or the branch firewall?

No. SASE combines SD-WAN for connectivity with cloud-delivered security services such as ZTNA, secure web gateway, CASB and FWaaS. Many organisations keep an edge firewall function at larger sites while moving web, SaaS and remote-access inspection to the security service edge.

What do participants take back from the SD-WAN and SASE training course?

Participants take back an SD-WAN and SASE Migration Roadmap with site tiers, a target overlay blueprint, path policy tables, a security service selection matrix, cutover waves with rollback criteria and an operating model, ready to adapt to their own estate.
