AWS VPC and Networking In Depth

Build, secure, and troubleshoot Amazon VPCs from the ground up with 20+ real-world hands-on labs and production-ready architectures.

DevOps Instructor: Roberto Lopez • 5 sections • 51 lessons • 16.75h total

View this course online Browse all courses

About this course

Most AWS networking courses explain concepts in isolation and leave you guessing when it's time to design a real architecture. You end up with security groups that don't talk to each other, route tables that silently black-hole traffic, and NAT Gateways in the wrong subnet. This course fixes that. You'll work through the actual decision-making process behind VPC design, starting with CIDR planning and subnet layout, then layering in gateways, security controls, peering, endpoints, and hybrid connectivity.

Each section pairs focused explanations with hands-on exercises you build in your own AWS account. You'll configure multi-AZ VPCs from scratch, peer VPCs across regions, set up Site-to-Site VPN and Transit Gateway, harden environments with Security Groups, NACLs, and Flow Logs, and automate everything with CloudFormation and Terraform. By the end, you'll have the practical skills to design, deploy, and troubleshoot production VPC architectures confidently.

Course curriculum

Foundations of AWS Networking

- What Is a VPC and Why It Matters in Cloud Architecture (12m)
  Understand the role of a VPC as your private network boundary inside AWS. We'll cover how VPCs relate to regions, accounts, and real-world deployment patterns.
- AWS Global Infrastructure: Regions, Availability Zones, and Edge Locations (15m)
  Walk through the physical and logical structure of AWS infrastructure. Learn how Regions and Availability Zones directly influence VPC and subnet design.
- IP Addressing in AWS: IPv4, IPv6, and CIDR Block Planning (22m)
  Step-by-step guide to calculating CIDR ranges, understanding address space overlap issues, and planning IPv4 and IPv6 blocks that scale with your architecture.
- Subnetting Basics for VPC Design (18m)
  Break down a CIDR block into usable subnets. Includes real examples of sizing subnets for web, application, and database tiers.
- Setting Up Your AWS Account and Navigating the VPC Dashboard (12m)
  Walk through the AWS console, VPC dashboard layout, and key settings you should configure before building anything.
- Hands-On: Creating Your First VPC with a Custom CIDR Block (25m)
  Create a VPC from scratch using both the console and CLI. Choose a CIDR block, verify it doesn't conflict with existing resources, and confirm provisioning.
- Hands-On: Planning CIDR Ranges for a Multi-Tier Architecture (20m)
  Real case study where you plan and validate CIDR blocks for a three-tier application across two Availability Zones. Includes a reusable planning template.

Subnets, Gateways, and Basic Connectivity

- Public vs. Private Subnets: When and Why to Use Each (15m)
  Understand the difference between public and private subnets at the routing level, not just the name. We'll cover the design rules that guide placement of each resource type.
- Designing Multi-AZ Subnet Layouts for Resilience (18m)
  Learn how to spread subnets across Availability Zones for fault tolerance. Includes a reference architecture for a typical three-tier, two-AZ layout.
- Internet Gateway: Attach, Detach, and Route Configuration (14m)
  Step-by-step guide to creating and attaching an Internet Gateway, then wiring it into route tables so public subnets can reach the internet.
- Route Tables: How AWS Directs Traffic Between Subnets (16m)
  Understand route table evaluation, longest-prefix matching, and how to associate route tables with specific subnets. Covers common misconfigurations.
- NAT Gateway: Managed Outbound Internet for Private Subnets (14m)
  Set up a NAT Gateway in a public subnet and configure routing so private subnets can download updates and call external APIs without being exposed.

- NAT Instances: When They Still Make Sense and How to Configure Them (12m)
  Compare NAT Gateways to NAT Instances. Learn when a NAT Instance saves cost and how to deploy one with proper failover scripts.
- Elastic IPs: Allocation, Association, and Billing Considerations (10m)
  Understand Elastic IP lifecycle, billing rules for unattached addresses, and how they interact with NAT Gateways and EC2 instances.
- Hands-On: Build a Multi-AZ VPC with Public and Private Subnets (30m)
  Full lab where you create a VPC spanning two Availability Zones, configure four subnets, attach an Internet Gateway, and set up route tables correctly.
- Hands-On: Deploy EC2 Instances and Verify Internet Access and Isolation (25m)
  Launch EC2 instances into public and private subnets. Test SSH access, ping external hosts, and confirm private instances cannot be reached from the internet.
- Hands-On: Configure NAT Gateway for Private Subnet Outbound Access (20m)
  Add a NAT Gateway to your architecture and verify that private subnet instances can reach external services for package updates and API calls.

Security, Access Control, and Traffic Flow

- Security Groups Explained: Stateful Filtering and Rule Logic (18m)
  Deep dive into how Security Groups evaluate traffic. Understand stateful behavior, implicit deny, and how multiple Security Groups stack on a single resource.
- Network ACLs: Stateless Rules and Subnet-Level Protection (16m)
  Learn how NACLs process rules in order, why you must define both inbound and outbound allow rules, and how numbered rules affect evaluation.
- Security Groups vs. NACLs: Choosing the Right Layer for Each Rule (14m)
  Problem-solving session comparing both tools side by side. Includes a decision framework for when to use Security Groups, NACLs, or both together.
- Inbound and Outbound Rule Design Best Practices (15m)
  Learn practical patterns for structuring rules: least-privilege defaults, port-based grouping, and how to reference other Security Groups as sources.
- VPC Flow Logs: Capture, Store, and Analyze Traffic Data (20m)
  Enable Flow Logs at the VPC, subnet, or ENI level. Send them to CloudWatch Logs or S3 and understand the fields in each log record.
- Analyzing Flow Logs in CloudWatch and Athena for Troubleshooting (22m)
  Run queries against Flow Log data to find rejected connections, unusual traffic patterns, and misconfigured rules. Includes common query templates.
- Bastion Hosts and SSH Jump Boxes for Secure Private Access (16m)
  Set up a hardened bastion host in a public subnet to SSH into private instances. Covers key-based auth, session manager as an alternative, and access logging.
- IAM Policies for VPC Resource Management and Least-Privilege Access (18m)
  Write IAM policies that control who can create, modify, or delete VPC resources. Includes example policies for networking admins, developers, and auditors.

- Hands-On: Harden a VPC with Layered Security Groups, NACLs, and Flow Logs (35m)
  Full lab applying Security Groups at the instance level and NACLs at the subnet level, then enabling Flow Logs and querying them in CloudWatch to verify the rules work.

VPC Peering, Endpoints, and Hybrid Connectivity

- VPC Peering: Same-Region Setup and Route Configuration (18m)
  Create a VPC peering connection between two VPCs in the same region. Configure route tables in both VPCs and verify connectivity with ping and curl.
- Cross-Region VPC Peering: Latency, Routing, and Limitations (15m)
  Extend peering across AWS Regions. Learn about DNS resolution settings, non-overlapping CIDR requirements, and transitive routing limitations.
- AWS PrivateLink: How It Differs from Peering and When to Use It (14m)
  Understand when PrivateLink is a better choice than peering, especially for accessing services across accounts or organizations without exposing network paths.
- Gateway Endpoints: S3 and DynamoDB Without Public Internet (16m)
  Create Gateway Endpoints for S3 and DynamoDB. Learn how they add route table entries and keep traffic on the AWS backbone at no extra cost.
- Interface Endpoints: Accessing AWS Services via Private IP (18m)
  Deploy Interface Endpoints (PrivateLink-powered) for services like SQS, SNS, and CloudWatch. Covers DNS configuration and security group attachment.
- AWS Direct Connect: Dedicated Network Links from On-Premises (20m)
  Walk through Direct Connect architecture, virtual interfaces (public and private), and how it reduces latency and data transfer costs for hybrid setups.
- Site-to-Site VPN: Concepts, Components, and Configuration (22m)
  Set up a VPN connection between a simulated on-premises network and your VPC. Covers Customer Gateway, Virtual Private Gateway, and tunnel configuration.
- AWS Transit Gateway: Hub-and-Spoke Networking for Multiple VPCs (24m)
  Learn how Transit Gateway simplifies routing between many VPCs and on-premises networks. Covers route tables, attachments, and route propagation.
- AWS Client VPN: Remote User Access to VPC Resources (16m)
  Deploy a Client VPN endpoint so individual users can connect to VPC resources securely. Covers authentication options and split-tunnel vs. full-tunnel.
- Hands-On: Peer Two VPCs and Verify Cross-VPC Communication (25m)
  Lab creating peering between two VPCs, updating route tables, enabling DNS resolution, and testing connectivity between EC2 instances in each VPC.
- Hands-On: Create S3 and DynamoDB Gateway Endpoints (20m)
  Configure Gateway Endpoints, attach them to route tables, set endpoint policies, and test S3 access from a private subnet with no NAT Gateway.
- Hands-On: Configure Transit Gateway with Route Propagation (30m)
  Build a Transit Gateway, attach three VPCs, configure route propagation, and verify full mesh connectivity. Includes a troubleshooting checklist.

Advanced VPC Design, Automation, and Troubleshooting

- Multi-Account Networking with AWS Organizations and RAM (22m)
  Understand how to design networks that span multiple AWS accounts. Use AWS Organizations for structure and RAM to share networking resources.
- Sharing VPC Subnets Across Accounts with Resource Access Manager (18m)
  Step-by-step guide to sharing subnets from a central networking account. Covers ownership, permissions, and how shared subnets appear in member accounts.
- Custom Route Tables: Advanced Routing Scenarios (16m)
  Design route tables for complex architectures: asymmetric routing, service insertion points, and routing traffic through inspection VPCs.
- Egress-Only Internet Gateway for IPv6 Traffic Control (14m)
  Configure egress-only Internet Gateways so IPv6-enabled instances can initiate outbound connections but cannot be reached from the internet.
- Application Load Balancer Placement and Subnet Design (20m)
  Learn how ALBs interact with subnets, security groups, and target groups. Covers multi-AZ placement, internal vs. internet-facing, and health check routing.
- Network Load Balancer: Low-Latency Routing Inside Your VPC (18m)
  Deploy NLBs for TCP/UDP traffic. Compare with ALBs, understand static IP behavior, and configure cross-zone load balancing.
- VPC Architecture for High Availability and Fault Tolerance (22m)
  Design patterns for resilient VPC architectures: multi-AZ redundancy, failover routing, and avoiding single points of failure in networking components.
- Infrastructure as Code for VPCs with AWS CloudFormation (25m)
  Write a CloudFormation template that builds a complete VPC with subnets, route tables, gateways, and security groups. Covers parameterization and stack updates.
- Building VPC Infrastructure with Terraform (25m)
  Create the same VPC architecture using Terraform. Covers modules, state management, and how Terraform handles resource dependencies for networking.
- Troubleshooting Connectivity: Reachability Analyzer (20m)
  Use AWS Reachability Analyzer to trace paths between a source and destination. Learn to read the analysis results and identify blocking components.
- Network Access Analyzer and Identifying Common Misconfigurations (18m)
  Run Network Access Analyzer to find unintended network access in your VPC. Covers common misconfigurations like overly permissive NACLs and missing routes.
- Hands-On: Build a Production-Grade Multi-Tier VPC with IaC (40m)
  Full lab using CloudFormation or Terraform to deploy a multi-AZ VPC with public and private subnets, NAT Gateways, ALB, security groups, and VPC endpoints.
- Hands-On: End-to-End Troubleshooting Lab with Simulated Failures (35m)
  Work through a series of broken VPC configurations. Use Reachability Analyzer, Flow Logs, and route table inspection to diagnose and fix each issue.

Discover our blog

Learn more with free articles written by our professors and guest experts.

Latest article: **Flight Attendant Preparation: What to Study Before You Apply**

Visit the blog All courses This course