CLOUD BEGINNER 2 DAYS

Cloud Networking and Cloud-Infra Deep Dive Fast Track

Build a strong foundation in hands-on cloud networking skills, from architecture fundamentals to troubleshooting common connectivity issues. Learn how to design secure networks, validate routing and access, and build confidence in real-world production networking scenarios.

Why Cloud Networking Fast Track?

Reduce downtime

Faster diagnosis and fewer misconfigurations in routing, firewall rules, and load balancers.

Accelerate migrations

Teams build correct network foundations faster and avoid rework.

Improve security posture

Better public/private segmentation and least privilege network access.

Operate with confidence

Practical troubleshooting skills for the most common production failures.

What you'll be able to do

- Understand essential cloud networking concepts including CIDR, subnetting, routing, and traffic flows.
- Build a secure VPC/VNet with public and private subnets and correct route table behavior.
- Implement safe internet access patterns using internet gateways and NAT gateways.
- Apply network security boundaries using security groups/NSGs and NACL concepts with least privilege rules.
- Deploy and validate load balancing using L4/L7 patterns and health checks.
- Configure DNS records and validate resolution and connectivity.
- Implement private connectivity to managed services using private endpoints or service endpoints.
- Troubleshoot common cloud networking incidents using a structured checklist.

Who this is for

- Cloud Engineers DevOps Engineers
- SRE and Platform Engineers
- Network Engineers moving to cloud
- Solution Architects (hands-on foundation)
- Backend engineers owning cloud deployments

Curriculum

01 Cloud Networking Essentials (CIDR, Subnetting, Routing, Traffic Flows)

- CIDR fundamentals and IP addressing in cloud networks
- Subnetting basics (splitting address space for tiers and zones)
- Routing concepts (route tables, next hop behavior)
- North-south vs east-west traffic flows in real architectures
- **Hands-on:** Lab: Design CIDR and subnet plan for a 3-tier application with public and private subnets

02 Build a Secure VPC/VNet (Public and Private Subnets + Route Tables)

- VPC/VNet building blocks (address space, subnets, network interfaces)
- Public vs private subnet design and placement strategy
- Route table association and correct route behavior
- Multi-AZ / multi-zone design basics for availability
- **Hands-on:** Lab: Build a VPC/VNet with public and private subnets and validate routes

03 Safe Internet Access Patterns (IGW + NAT Gateway)

- Internet gateway concepts and inbound/outbound behavior
- NAT gateway patterns for private subnet egress
- Secure egress strategy (what should be allowed and why)
- Common misconfigurations that break internet access
- **Hands-on:** Lab: Enable outbound internet for private workloads using NAT and validate connectivity

04 Network Security Boundaries (Security Groups/NSGs + NACL Concepts)

- Security groups/NSGs as stateful firewalls (inbound/outbound rules)
- Least privilege rule design (restrict sources, ports, and protocols)
- NACL concepts as stateless subnet boundary controls
- Tiered security model for web/app/db subnets
- **Hands-on:** Lab: Implement least privilege SG/NSG rules and validate allowed vs blocked traffic

05 Load Balancing Patterns (L4/L7 + Health Checks)

- L4 vs L7 load balancers and selection criteria
- External vs internal load balancing patterns
- Health check fundamentals and common causes of unhealthy targets
- Routing basics (host/path routing for L7 concepts)
- **Hands-on:** Lab: Deploy a load balancer, configure health checks, and validate traffic distribution

06 DNS Configuration and Validation (Resolution + Connectivity)

- DNS fundamentals (records, TTL, resolution path)
- Common record types (A/AAAA, CNAME) and when to use each
- Troubleshooting DNS issues (DNS works but no connectivity patterns)
- Private DNS concepts for internal services (intro)
- **Hands-on:** Lab: Create DNS records and validate resolution and end-to-end connectivity

07 Private Connectivity to Managed Services (Private Endpoints / Service Endpoints)

- Why private connectivity matters (reduce exposure, compliance, security)
- Private endpoints concepts (private access to managed services)
- Service endpoints concepts (subnet-level service access)
- Private DNS resolution for private connectivity
- **Hands-on:** Lab: Implement private connectivity to a managed service and validate private DNS + access

08 Incident Troubleshooting Checklist (Real Cloud Networking Scenarios)

- Structured troubleshooting flow (scope, isolate, validate, fix)
- No internet access checklist (routes, NAT/IGW, SG/NSG, NACL, DNS)
- Unreachable service checklist (LB health checks, security rules, routing)
- DNS but no connectivity checklist (firewall, routing, endpoints)
- **Hands-on:** Lab: Solve incident simulations (broken NAT, blocked ports, unhealthy targets, DNS mismatch) using the checklist