CLOUD INTERMEDIATE 3 DAYS

Cloud Networking and Cloud-Infra Deep Dive Bootcamp

Build a strong foundation in production-grade cloud networking, from secure design to automation and real troubleshooting. Learn how to implement private connectivity, control traffic flows, and resolve real-world incident scenarios across enterprise cloud architectures.

Why Cloud Networking?

Fewer production outages

Many cloud incidents are caused by network misconfigurations; training reduces downtime.

Lower cloud costs

Better designs avoid unnecessary NAT/LB usage and support efficient scaling.

Better security and reduced attack surface

Proper subnet design and private connectivity prevent unintended exposure.

Enterprise architecture readiness

Hub-spoke, private endpoints, and controlled ingress are standard enterprise patterns.

Faster cloud migrations

Teams can migrate workloads confidently with correct connectivity and routing.

What you'll be able to do

- Understand cloud networking fundamentals and how they map to real infrastructure and traffic flows.
- Design secure and scalable cloud network architectures using VPC/VNet, subnets, routing, NAT, and internet gateways.
- Explain ingress and egress traffic flows and implement safe internet connectivity patterns.
- Apply network-layer security boundaries using security groups/NSGs and NACL concepts with least privilege rules.
- Implement private connectivity patterns including private endpoints, service endpoints, and private DNS resolution.
- Understand load balancer types and selection criteria (L4 vs L7, internal vs external) with health checks.
- Troubleshoot production networking issues such as no internet access, unreachable services, DNS-but-no-connectivity, and blocked traffic.
- Build reference architectures for 3-tier web apps and microservices and understand hybrid connectivity concepts.
- Understand cloud infra building blocks (compute, storage, identity, routing, monitoring basics) and how they integrate with networks.
- Automate network provisioning and changes using Terraform with safe plan/apply workflows.

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 Fundamentals (How Traffic Really Flows)

- Core networking concepts refresher (CIDR, IPs, ports, protocols)
- DNS fundamentals and how name resolution impacts connectivity
- Routing basics (route tables, next hop behavior)
- How cloud networking maps to real traffic flows (client → LB → app → DB)
- **Hands-on:** Activity: Trace request flow for a 3-tier application and identify network touchpoints

02 Cloud Network Architecture Design (VPC/VNet + Subnets + Routing)

- VPC/VNet building blocks (address space, subnets, isolation)
- Subnet design strategy (public vs private subnets)
- Route tables and routing patterns (east-west vs north-south)
- High availability patterns (multi-AZ / multi-zone subnet layout)
- **Hands-on:** Lab: Design a VPC/VNet with public and private subnets and validate routing intent

03 Ingress and Egress Patterns (Safe Internet Connectivity)

- Ingress flow patterns (internet → load balancer → application)
- Egress flow patterns (app → internet for updates/APIs)
- Internet gateways and egress control concepts
- NAT gateways and when to use them for private subnets
- **Hands-on:** Lab: Configure NAT-based outbound internet for private workloads with controlled access

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

- Security groups/NSGs fundamentals (stateful firewall behavior)
- Least privilege rule design (only required ports, restricted sources)
- NACL concepts (stateless rules, subnet boundary controls)
- Common mistakes (overly open inbound, wide egress, wrong direction rules)
- **Hands-on:** Lab: Implement SG/NSG rules for web, app, and database tiers using least privilege

05 Private Connectivity Patterns (Private Endpoints + Service Endpoints + Private DNS)

- Why private access matters for compliance and reduced exposure
- Private endpoints concept (private connectivity to managed services)
- Service endpoints concept (controlled service access from subnets)
- Private DNS resolution patterns and split-horizon DNS concept
- **Hands-on:** Lab: Enable private access to a managed service and validate DNS resolution + connectivity

06 Load Balancers Deep Dive (L4 vs L7, Internal vs External)

- L4 vs L7 load balancer selection (TCP vs HTTP routing)
- External vs internal load balancers and common use cases
- Health checks and why they impact availability
- Sticky sessions, path routing, and TLS termination concepts
- **Hands-on:** Lab: Deploy an external LB for a web tier and an internal LB for app-tier services

07 Troubleshooting Production Networking Issues (Real Scenarios)

- No internet access troubleshooting (IGW/NAT/routes/DNS)
- Unreachable services debugging (SG/NSG/NACL, wrong ports, wrong subnets)
- DNS works but no connectivity (routing or firewall issue patterns)
- Blocked traffic debugging with flow logs and connectivity tests
- **Hands-on:** Lab: Resolve failure scenarios (blocked inbound, broken egress, DNS mismatch, wrong routing)

08 Reference Architectures (3-Tier Apps, Microservices, Hybrid Connectivity Concepts)

- 3-tier reference architecture (web, app, database) and subnet placement
- Microservices networking patterns (service-to-service, internal routing)
- Hybrid connectivity overview (VPN, Direct Connect/ExpressRoute concepts)
- Network segmentation and environment separation (dev/stage/prod)
- **Hands-on:** Workshop: Design reference architectures for 3-tier and microservices with secure boundaries

09 Cloud Infrastructure Building Blocks and Network Integration

- Compute placement and network interfaces (public/private IP behavior)
- Storage access patterns (public endpoints vs private access)
- Identity and access basics that impact networking (IAM/RBAC + service identity)
- Monitoring basics for networks (logs, metrics, health checks)
- **Hands-on:** Activity: Map infra components into a network diagram with trust boundaries

10 Network Provisioning and Change Automation with Terraform

- Terraform basics for networks (VPC/VNet, subnets, route tables)
- Safe plan/apply workflow and environment separation
- Reusable modules and consistent naming conventions
- Change control practices (review, approvals, drift awareness)
- **Hands-on:** Lab: Provision a full network stack with Terraform and validate routes, NAT, and security rules