

Introduction to Cloud Networking

Introduction to Cloud Networking

Key concepts, components, and best-practice guidelines

1. What Is Cloud Networking?

Aspect	Description
Definition	The design, deployment, and management of network services (routing, switching, security, load balancing, etc.) that run on public, private, or hybrid cloud platforms instead of traditional on-premises hardware.
Goal	Deliver scalable, on-demand connectivity and network services to applications and users while reducing capital expense and operational complexity.
Typical Use Cases	- Multi-region web-app deployment - Disaster-recovery and backup traffic - Secure SaaS integration - Edge computing and IoT connectivity - Hybrid-cloud data center extension

2. Core Building Blocks

Component	Cloud-Native Equivalent	Primary Functions
Virtual Private Cloud (VPC) / Virtual Network (VNet)	AWS VPC, Azure VNet, GCP VPC	Isolated IP address space, subnets, routing tables, security boundaries.
Subnets	Public vs. private subnets	Separate workloads (e.g., web tier vs. database tier); control exposure to the internet.
Internet Gateway / NAT Gateway	AWS IGW/NAT, Azure Internet Gateway, GCP Cloud NAT	Enable outbound/inbound traffic for public subnets; provide NAT for private subnets.
Route Tables	Custom routing rules	Direct traffic between subnets, VPN, peered VPCs, and on-premises networks.

Introduction to Cloud Networking

Component	Cloud-Native Equivalent	Primary Functions
Security Groups & Network ACLs	Stateful vs. stateless firewalls	Instance-level (SG) and subnet-level (ACL) traffic filtering.
Load Balancers	ALB/NLB, Azure Load Balancer, GCP Cloud Load Balancing	Distribute traffic across instances, support TLS termination, health checks.
VPN & Direct Connect / ExpressRoute / Cloud Interconnect	Site-to-site IPsec VPN, dedicated private links	Secure, low-latency connectivity between on-premises data centers and the cloud.
Peering & Transit Gateways	VPC Peering, Transit Gateway, Azure Virtual WAN	Inter-VPC communication without traffic traversing the public internet.
DNS Services	Route 53, Azure DNS, Cloud DNS	Authoritative and private DNS zones, health-based routing.
SD-WAN Integration	Cloud-managed WAN overlays	Centralized policy control across multiple branch sites and clouds.

3. Network Topology Patterns

Pattern	Description	Typical Scenario
Single-Region VPC	One VPC with public & private subnets in a single region.	Small web app, low latency, simple compliance.
Multi-Region VPC with Transit Gateway	Central hub (Transit GW) connects spoke VPCs across regions.	Global SaaS, disaster recovery, data locality.
Hybrid Cloud (VPN/Direct Connect)	On-premises network linked via encrypted VPN or dedicated line.	Legacy workloads, data residency, lift-and-shift migrations.
Multi-Cloud Mesh	Peered VPCs/VNets across AWS, Azure, GCP using third-party interconnect or native cloud-exchange services.	Redundancy, vendor-agnostic architecture, workload bursting.
Edge-Centric Architecture	Cloud-based routing + edge locations (CDN, edge compute)	