Advanced AWS Workshop

Instructor: Govind Kumar

Date: 16-May-2025 | Time: 9:00 PM - 11:30 PM IST

VPC Fundamentals

Learn about AWS Virtual Private Cloud and its core networking components.

Security & Connectivity

Master VPC security groups, NACLs, and connectivity options for your cloud resources.

Network Architecture

Design resilient and secure network architectures using AWS VPC.

Virtual Private Cloud in AWS

What is a VPC?

A logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Key Features of Amazon VPC

Complete Network Control

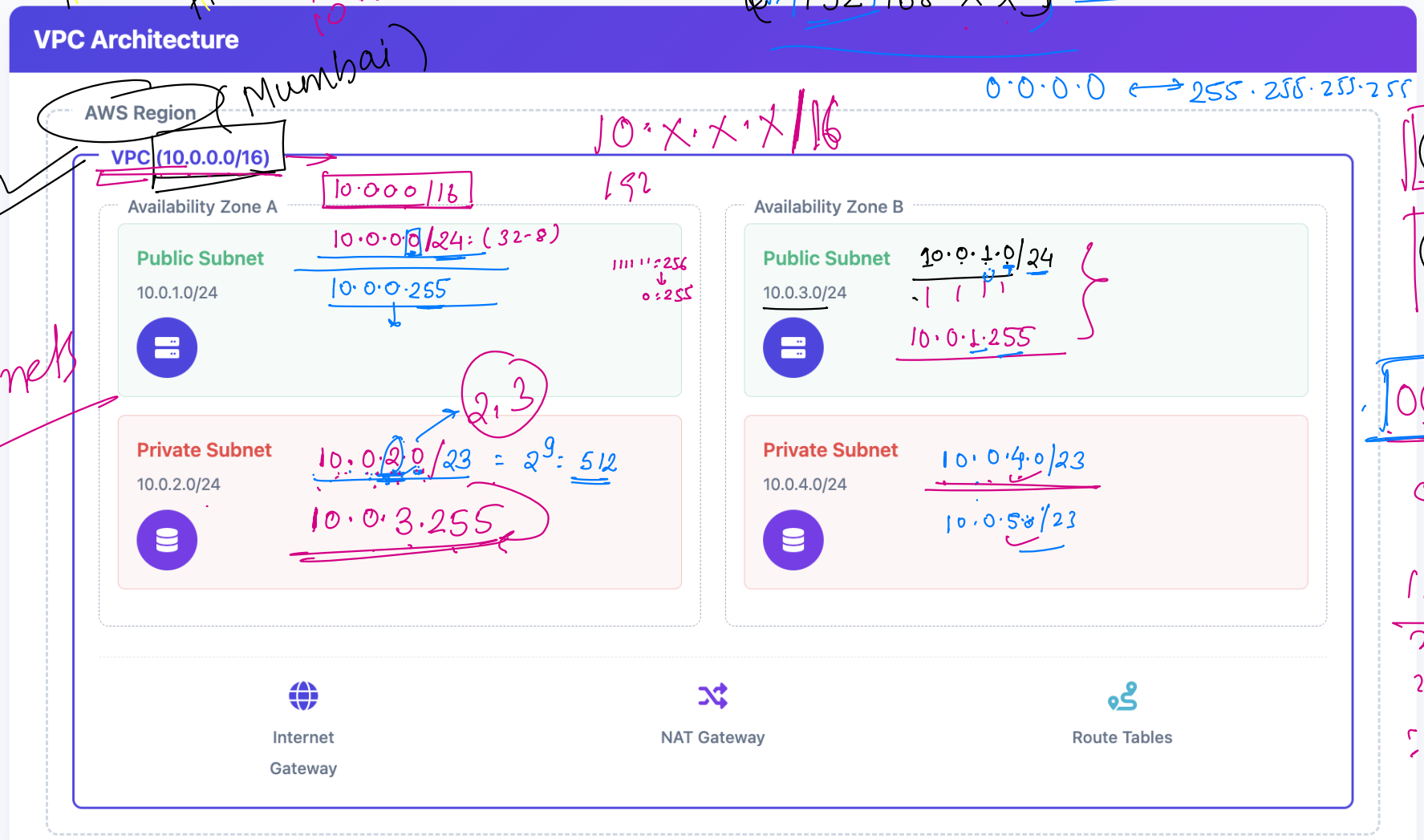
Configure your VPC's IP address range, create subnets, and configure route tables and network gateways.

Enhanced Security

Security groups and network ACLs allow you to filter inbound and outbound traffic to your instances.

Connectivity Options

Connect your VPC to your corporate data center, other VPCs, or directly to the internet.


VPC Architecture
AWS Region
Mumbai
VPC (10.0.0.0/16)
Availability Zone A
Public Subnet
10.0.1.0/24
Private Subnet
10.0.2.0/24
Availability Zone B
Public Subnet
10.0.3.0/24
Private Subnet
10.0.4.0/24
Internet Gateway
NAT Gateway
Route Tables

10.0.0.0/16 : 2^{16} = Hosts

Network Add' | Host Addr

16 on AWS

32 - 16 = 16 = 2^{16}

/27 → 2^5

32 - 27 = 5

VPC1 { 10.0.0.0/16 = 10.0.255.255

10.1.0.0/16 = 10.1.255.255

10.255.0.0/16 .. 10.255.255.25 }

VPC-0

VPC2

VPC-255

10.0.0.0/16

↓

255.0.0

192.168.0.0/16 → 192.168.255.255

172.31.0.0/16 → 172.31.255.255

Subnets

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet.

- Public subnets have direct route to Internet Gateway
- Private subnets have no direct route to Internet Gateway
- Each subnet must reside entirely within one Availability Zone

Internet Gateway

An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

- Provides a target in your VPC route tables for internet-routable traffic
- Performs network address translation for instances with public IPs

NAT Gateway

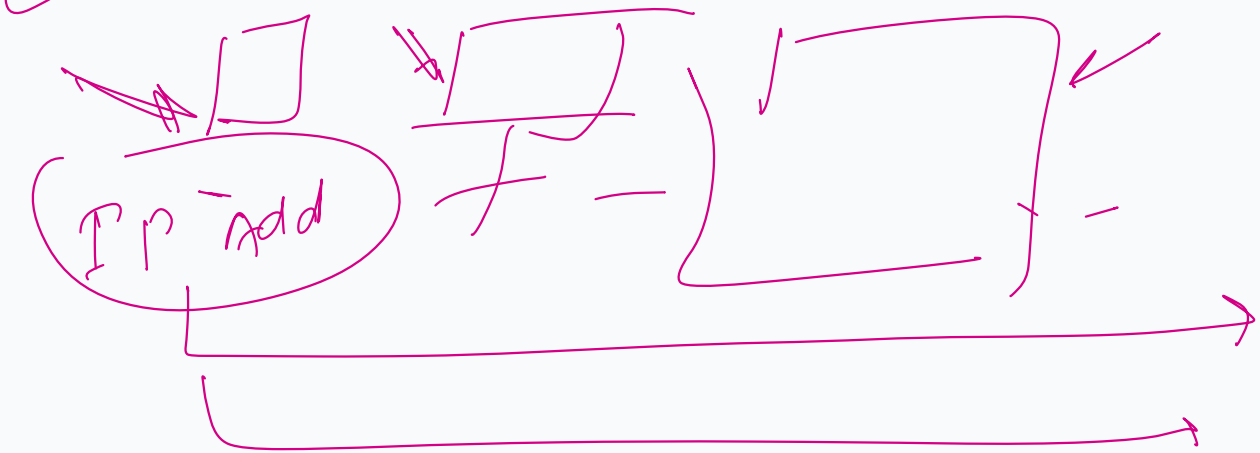
A NAT Gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances.

- Managed by AWS, highly available within an AZ
- Requires an Elastic IP address
- Supports up to 5 Gbps of bandwidth

Route Tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed.

- Each subnet must be associated with a route table
- A subnet can only be associated with one route table at a time



VPC Security

Securing Your VPC

AWS provides multiple layers of security for your VPC resources.

Security Groups vs. Network ACLs

AWS VPC provides two features that you can use to increase security in your VPC: security groups and network access control lists (ACLs).

Feature	Security Groups	Network ACLs
Level of operation	Instance level	Subnet level
State	Stateful (return traffic automatically allowed)	Stateless (return traffic must be explicitly allowed)
Rule evaluation	All rules are evaluated before deciding to allow traffic	Rules are evaluated in order (lowest to highest)
Default behavior	Deny all inbound, allow all outbound	Allow all inbound, allow all outbound
Rule types	Allow rules only	Allow and deny rules

VPC Connectivity Options

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | Direct Connect | Transit Gateway

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.

- Direct network route between two VPCs
- No gateway or VPN connection required
- No single point of failure or bandwidth bottleneck
- Traffic stays on the AWS global network

VPC Connectivity Options

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | **AWS VPN** | Direct Connect | Transit Gateway

AWS VPN

AWS Virtual Private Network (VPN) solutions establish secure connections between your on-premises networks, remote offices, client devices, and the AWS global network.

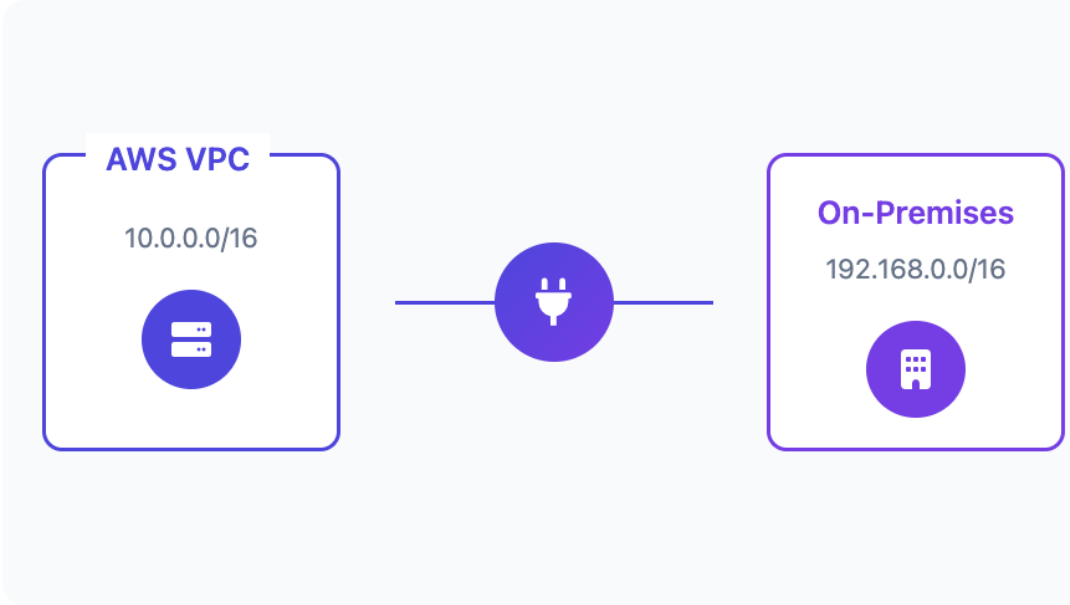
- Site-to-Site VPN connects on-premises to AWS
- Client VPN connects remote users to AWS
- Encrypted connection over the internet
- Supports IPsec protocol

VPC Connectivity Options

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | **Direct Connect** | Transit Gateway



AWS Direct Connect

AWS Direct Connect is a cloud service that establishes a dedicated network connection from your premises to AWS, providing consistent network performance and reducing bandwidth costs.

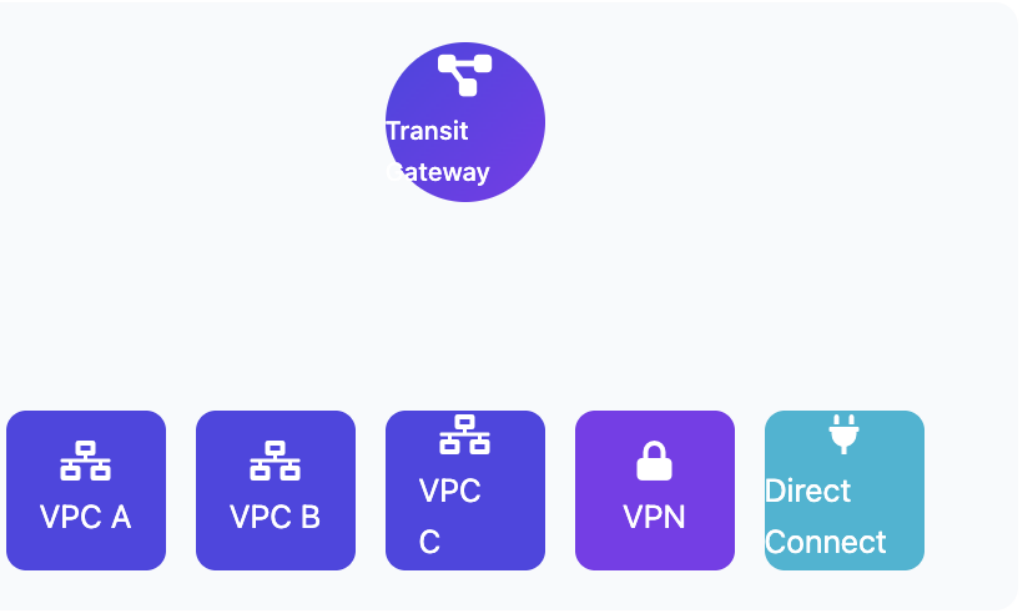
- Dedicated private connection
- Reduced network costs
- Consistent network performance
- Compatible with all AWS services

VPC Connectivity Options

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | Direct Connect | **Transit Gateway**



AWS Transit Gateway

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

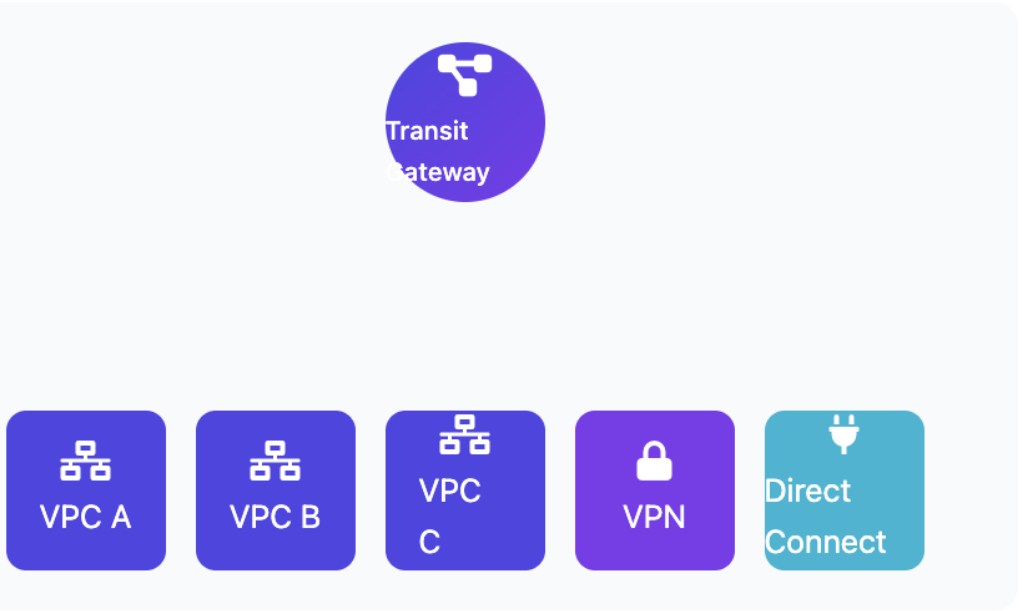
- Hub-and-spoke connectivity model
- Simplifies network architecture
- Centralized control and management
- Supports thousands of connections

VPC Connectivity Options

Connecting VPCs and On-Premises Networks

AWS offers multiple options to connect your VPC to other networks.

VPC Peering | AWS VPN | Direct Connect | **Transit Gateway**



AWS Transit Gateway

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

- Hub-and-spoke connectivity model
- Simplifies network architecture
- Centralized control and management
- Supports thousands of connections