



Google Certified

# Associate Cloud Engineer

Batch-2011 | Moon International Karachi Pakistan

khawarhere@gmail.com

# Lesson Plan

## 7. VPC: Networking

### 7.1. OSI Layers

### 7.2. Routing

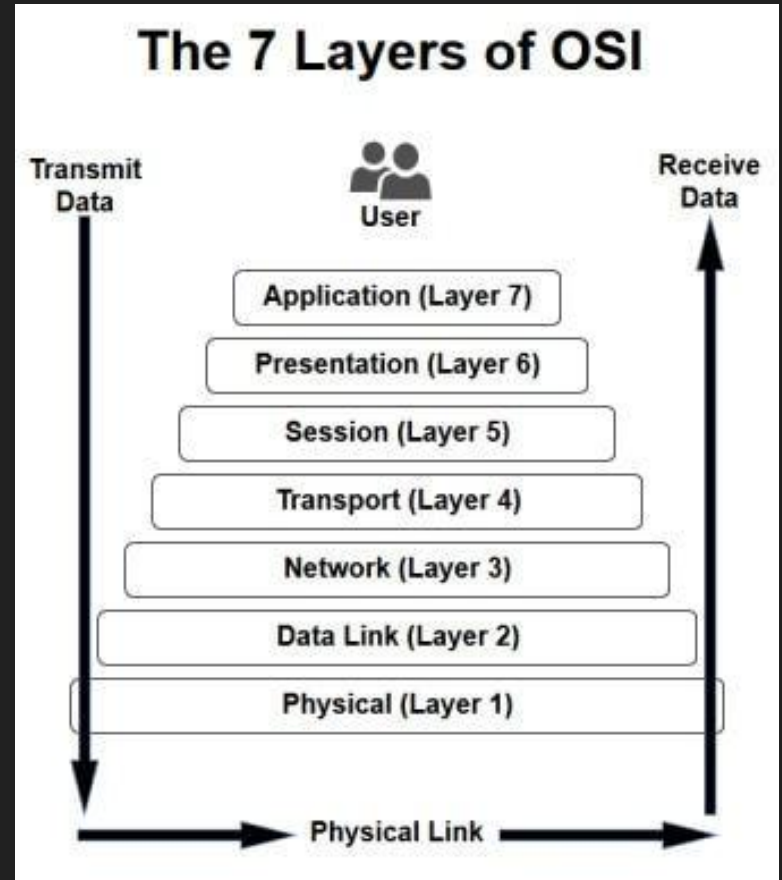
#### 7.2.1. Delivery schemes

#### 7.2.2. Google Network (Premium Routing)

### 7.3. VPC

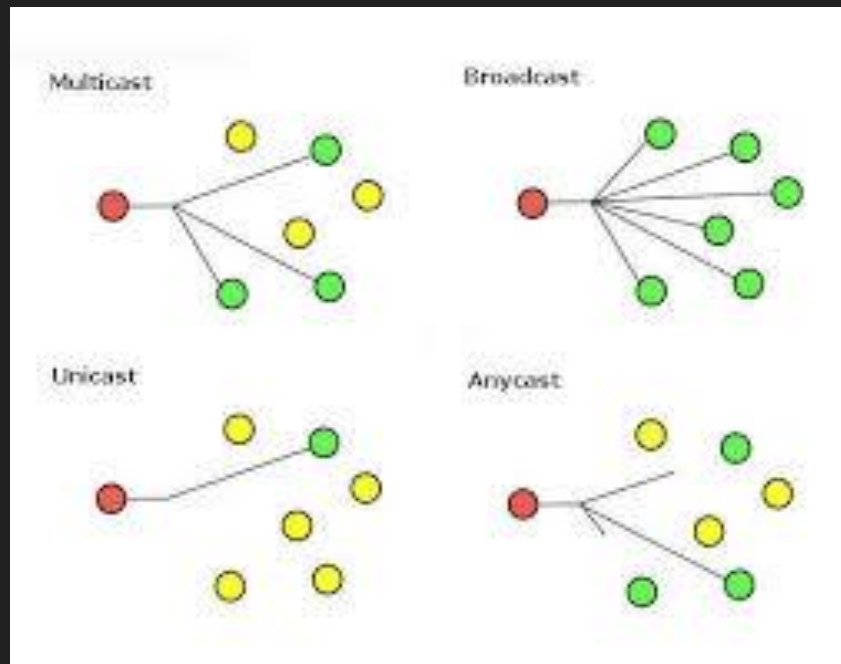
# 7.1 OSI Layers

The [7 Layers](#) of the OSI Model



## 7.2.1 Routing | Delivery schemes

- Delivery schemes
  - **unicast**: delivers a message to a single specific node
  - There is only one unique device in the world that can handle this.
  - **anycast**: delivers a message to any one out of a group of nodes, typically the one nearest to the source
  - Multiple devices, send it to any of them



## 7.2.2 Routing | Google Network

- Premium
  - Cool potato
  - Latency reduction
- Standard
  - Hot potato

## 7.2.2 Routing | Google Network | Animation

Premium

Standard

## 7.2 Routing | Load Balancing

- Separate from auto scaling
- Internal and External LB
- LB on layer 7 and layer 4

## 7.3 VPC

- Virtual Private Cloud: are global
- Software Defined Networking (SDN)
- Not just resource to resource, also outside and peers.
- Subnets: are regional
- Routes: are global, next hop
- Firewall: global, restrictive inbound and permissive outbound



## 7.3.1 VPC | Auto-Mode

Auto vs Custom is all about how subnets are created.

Subnet create mode is persistent not just a onetime.

In Auto-mode VPC's will get net subnets added automatically.

IP Address ranges are tied to subnets

No VPC level address range.

1. Open cloud console
  - a. VPC network
2. Create VPC Network
  - a. Subnet Creation mode: Automatic
  - b. name: my-vpc-auto
  - c. firewall rules: turn on all 4
  - d. Dynamic routing mode : Regional

## 7.3.2 VPC | Custom-Mode

A subnet or subnetwork is not the same thing as a (VPC) network. Networks and subnets (subnetworks) are different types of objects in GCP.

When a custom mode network is created, no subnets are automatically created.

This type of network provides you with complete control over its subnets and IP ranges. You decide which subnets to create, in regions.

1. Open cloud console
  - a. VPC network
2. Delete previous (auto and default) VPC(s)
3. Create VPC Network
  - a. Subnet Creation mode: Custom
  - b. name: my-vpc-custom
  - c. subnet: iowa
  - d. IP address range: 192.168.0.0/24
  - e. create

## 7.3.3 VPC | Custom-Mode | Create IAM

Multiple service accounts may have in single role

When Google will update primitive roles, it will not effect our custom role.

1. Open cloud console
  - a. IAM & admin > Role
2. Filter
  - a. Title:\*writer
  - b. Select:
    - i. Logs Writer
    - ii. Monitoring Metric Writer
  - c. Create Role From Selection
    - i. Title: Developer Team
    - ii. ID:DevelopmentTeam
    - iii. Create

## 7.3.4 VPC | Custom-Mode | Service Account

A service account is a special type of Google account intended to represent a non-human user that needs to authenticate and be authorized to access data in Google APIs.

1. Open cloud console
  - a. IAM & admin > Service Accounts
  - b. Create Service Account
    - i. name: devops-sa
    - ii. Create
    - iii. Role:Custom > Developer Team
    - iv. Continue
    - v. Done

## 7.3.5 VPC | Custom-Mode | Instance Template

An instance template is a resource that you can use to create VM instances and managed instance groups

1. Open cloud console
  - a. Compute Engine> Instance Template
  - b. Create Instance Template
    - i. name: frontend-it
    - ii. Machine type: f1-micro
    - iii. Service account: devops-sa
    - iv. Network: my-vpc-custom
    - v. Subnet: iowa-subnet
    - vi. create

## 7.3.6 VPC | Custom-Mode | Instance Group

An instance group is a collection of virtual machine (VM) instances that you can manage as a single entity.

**Managed instance groups:** let you operate apps on multiple identical VMs

**Unmanaged instance groups:** let you load balance across a fleet of VMs that you manage yourself.

1. Open cloud console
  - a. Compute Engine> Instance Group
  - b. Create Instance Group
    - i. Name: frontend-ig
    - ii. Location: multiple zones
    - iii. region: us-central1
    - iv. instance template: frontend-it
    - v. Minimum number of instances: 2
    - vi. Maximum number of instances: 3
    - vii. create

## 7.3.7 VPC | Custom-Mode | Firewall Rule

`ping -c 3 <IP>`

Will not ping

After creating firewall rule, ping again.

1. Open cloud console
  - a. Compute Engine> Instance Group
  - b. Enter into Instance Group (frontend-ig)
    - i. Copy external IP, ping via cloud shell
  - c. VPC Network> my-vpc-custom
  - d. Firewall rules> Add firewall rule
    - i. Name: allow-incoming-to-frontend-fwr
    - ii. Direction of traffic: Ingress
    - iii. Action to mach: Allow
    - iv. Target: serviceAccount>devops-sa
    - v. Source IP ranges: 0.0.0.0/0
    - vi. Protocols>Other: icmp

## 7.3.8 VPC | Custom-Mode | SSH Rule

SSH using cloud shell

Will not SSH

Edit any instance and add tag

“open-ssh-tag”

After creating firewall rule, SSH again.

1. Open cloud console
  - a. Compute Engine> Instance Group
  - b. Enter into Instance Group (frontend-ig)
    - i. Try to ssh (It will fail)
  - c. VPC > Firewall Rules>Add Fwr
    - i. Name: open-ssh-by-tag-fwr
    - ii. Target tag: open-ssh-tag
  - d. Edit Instance Group (frontend-ig)
    - i. Auto scaling: off
    - ii. Number of instances: 0