

A person in a dark suit and tie is holding a tablet. Overlaid on the image is a complex digital network diagram with nodes and connecting lines. Some nodes are labeled with terms like 'PLATFORM', 'APPLICATION', and 'INFRASTRUCTURE'. The background is a blurred image of a server rack with glowing blue lights.

# Google Cloud Platform Networking Fundamentals

Understanding GCP Networking Services



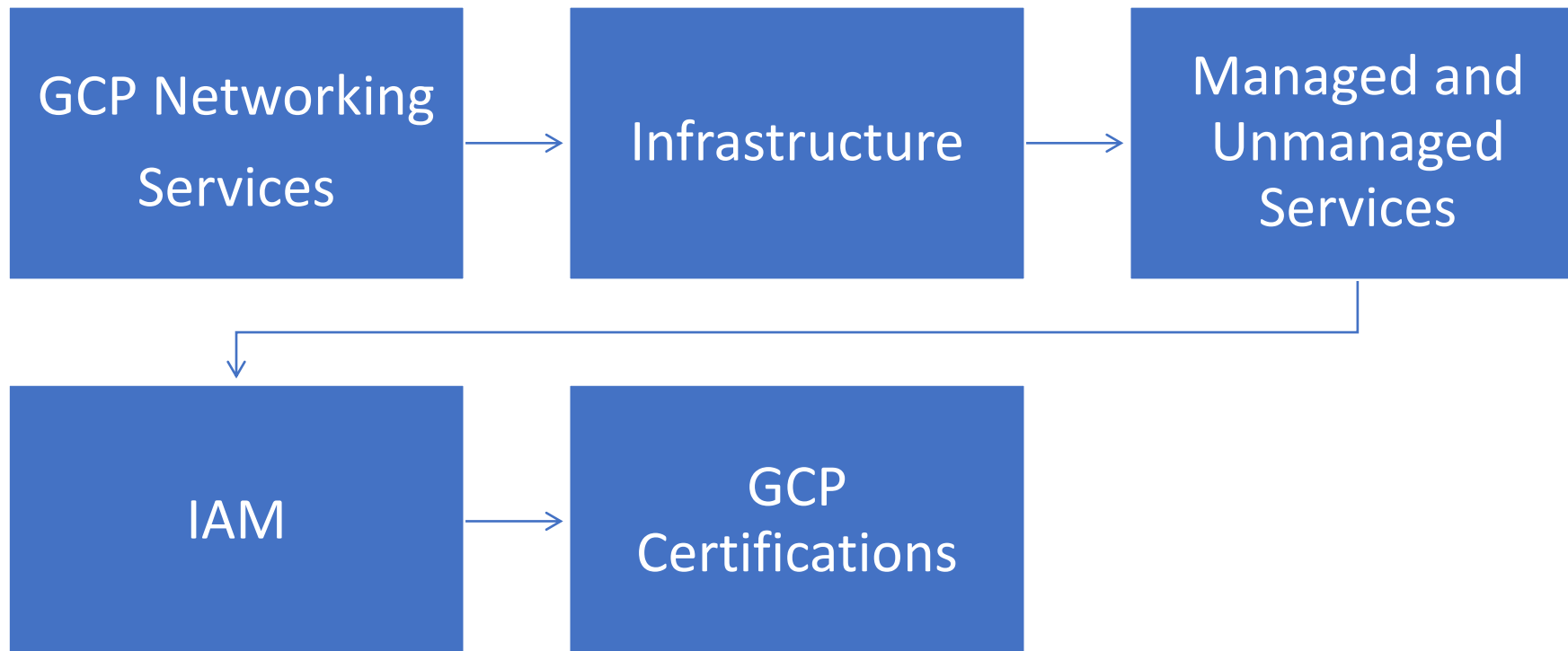
# Instructor Introduction

- Joseph Holbrook
  - Consulting Cloud/Blockchain Solutions Architect/Trainer/Speaker out of Jacksonville, FL
  - Certified Blockchain Solutions Architect (CBSA)
  - Certified Blockchain Expert (CBE)
  - Certified Bitcoin Professional (CBP)
  - Certified Blockchain Developer Hyperledger (CBDH)
  - Certified Corda Developer
  - Certified Google Cloud Platform Cloud Architect
  - Certified AWS Solutions Architect
  - Brocade Distinguished Architect (BDA) 2013
  - EMC Proven Professional – Expert – Cloud (EMCCE)
  - Published Course Author on Pearson Safari, Udemy, LinkedIn Learning
  - Author “Architecting Enterprise Blockchain Solutions” – Wiley Oct. 2019
  - Prior US Navy Veteran

# Course Overview

Google Cloud Platform  
Networking Fundamentals

# Course Overview



# Prerequisites





GCP has really powerful capabilities for cloud networking.

Lets proceed  
& talk about these capabilities.

# Networking Tiers

Google Cloud Platform

Networking Fundamentals

# Why Choose Google Cloud?

## ***Standard Tier or Premium Tier?***

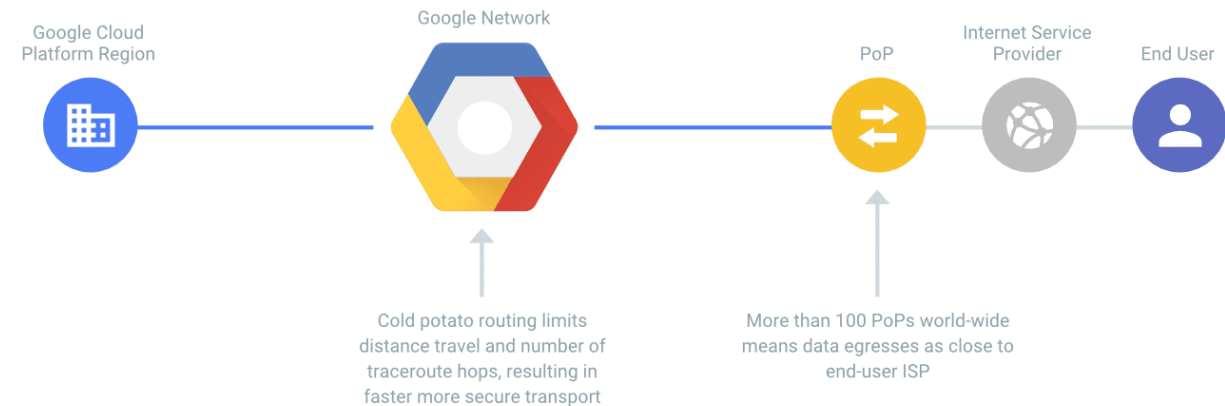
- Premium tier delivers traffic over Google's well-provisioned, low latency, highly reliable global network.
- Redundancy is paramount (three independent paths) (N+2 redundancy) between any two locations on the Google network.
- Standard tier delivers network quality comparable to that of other major public clouds. (Uses standard ISPs)



# Why Choose Google Cloud?

## Standard Tier or Premium Tier?

- Premium tier delivers traffic over Google's well-provisioned, low latency, highly reliable global network.



GCP Premium Tier

<https://cloud.google.com/blog/products/gcp/introducing-network-service-tiers-your-cloud-network-your-way>

# Networking Infrastructure

Google Cloud Platform

Networking Fundamentals

# Why Choose Google Cloud?



Why GCP? [Lets](#) Discuss



Google has the most powerful infrastructure and owns most of it.



Datacenters



Fiber Backbones

<https://peering.google.com/#/>



Submarine lines

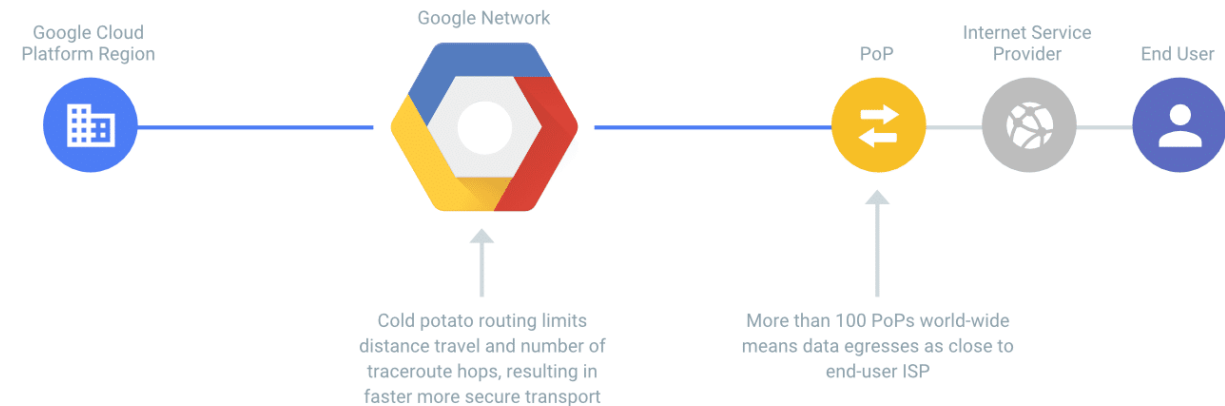


Points of Presence

# Why Choose Google Cloud?

## Standard Tier or Premium Tier?

- Premium tier delivers traffic over Google's well-provisioned, low latency, highly reliable global network.



GCP Premium Tier

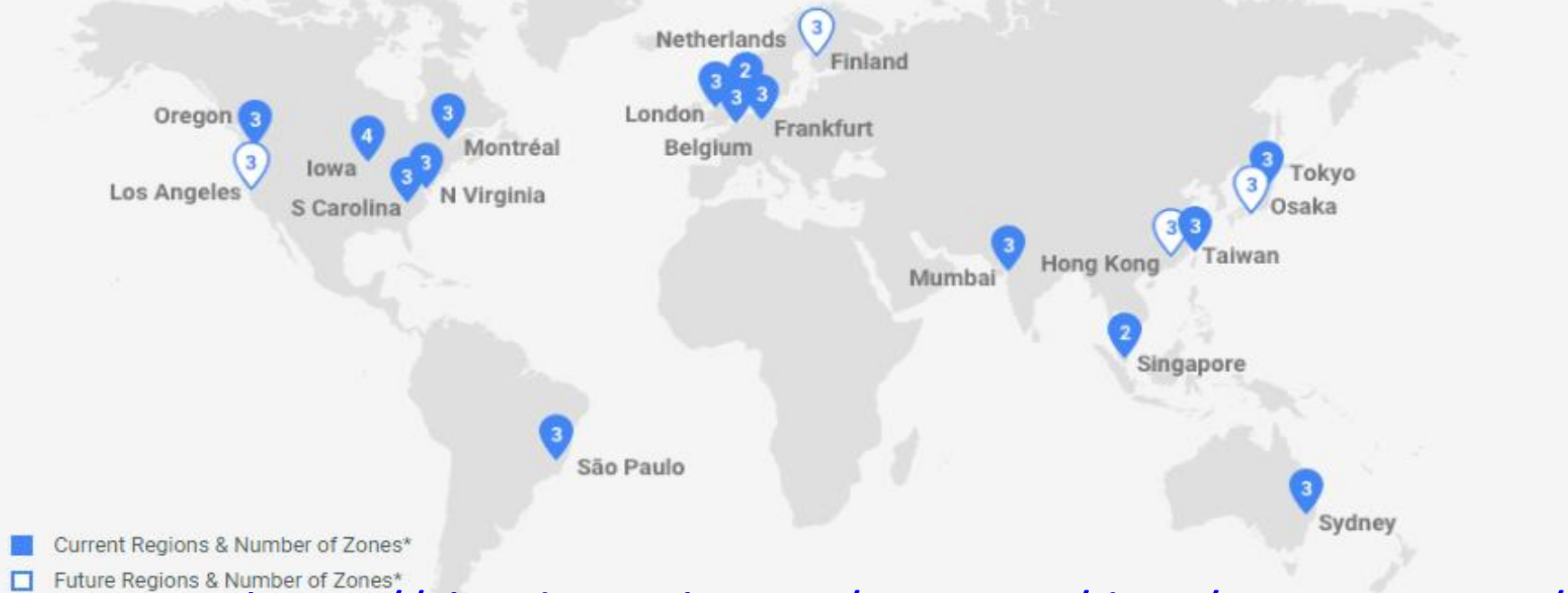
<https://cloud.google.com/blog/products/gcp/introducing-network-service-tiers-your-cloud-network-your-way>

# Networking Infrastructure

Regions

Network

GCP Has a growing number of zones and regions.



<https://cloud.google.com/compute/docs/regions-zones/>

\* While some regions may launch with 2 zones, all regions are planned for a minimum of 3 zones.

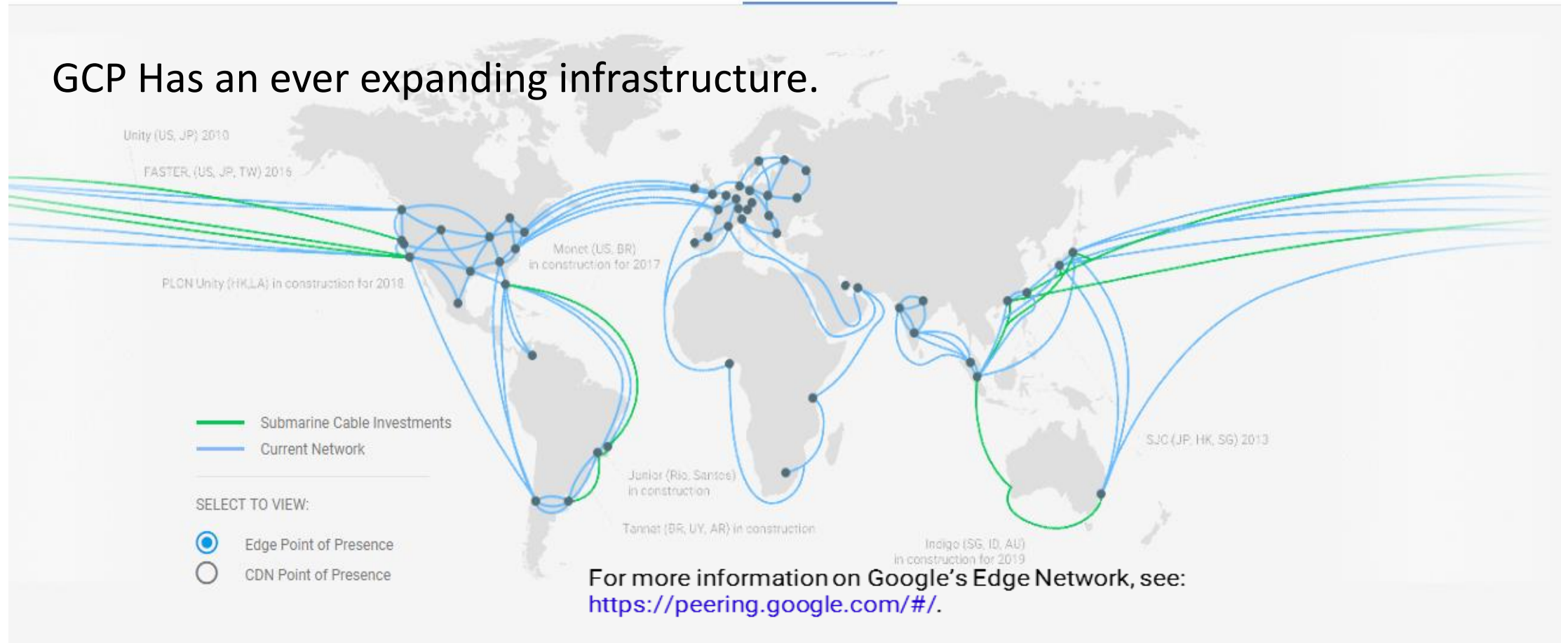


# Why Choose Google Cloud?

Regions

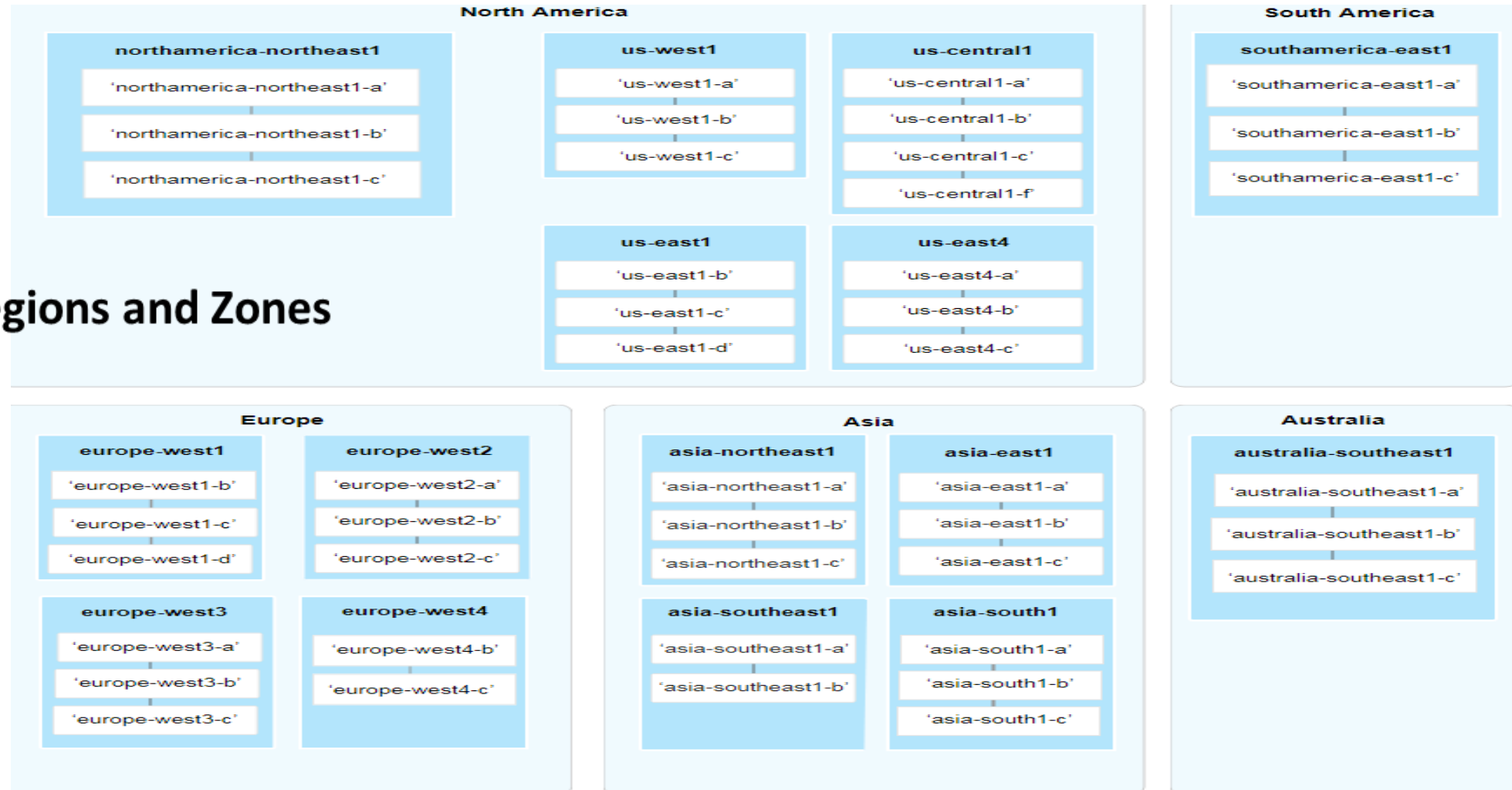
Network

GCP Has an ever expanding infrastructure.



# Networking Infrastructure

## Regions and Zones



# Why Choose Google Cloud?

## Lets Review

- Google has the most powerful infrastructure and owns it
- Submarine Lines
- Datacenters
- Google has a Premium network tier that allows customers to deliver traffic over Google's well-provisioned, low latency, highly reliable global network.

# Infrastructure, Regions and Zones

Google Cloud Platform

GCP Networking Fundamentals

# GCP Networking Fundamentals

	AWS	GCP
Regions	Global Infrastructure	Regions and Zones
Abstracted data center	Availability Zone	Zone
Edge caching	CloudFront	Cloud CDN(App Engine, Cloud Storage)



# GCP Networking Fundamentals

Lets Compare Terms and numbers

	AWS	GCP
Backbones	-	- Different View
Datacenters	region and availability zone (AZ)	region and zone
Edge Locations	CloudFront (75+)	Cloud CDN and Cloud Interconnect (110+)

# GCP Networking Fundamentals

Lets Compare Terms and numbers

Concept	AWS	GCP	Notes
Cluster of DC Services	Region (20)	Region (18)	GovCloud in progress with GCP....
Abstracted DC	Availability Zone (60)	Zone(55)	* Does not include locales that are not online
Edge Caching	POP (Cloudfront)	POP(CDN, Other Services)	<i>Cloud Platform's POPs connect to data centers through Google-owned fiber.</i>
Total Services	220 +	70+	

# GCP Networking Fundamentals

Google Cloud Platform resources are organized by Regions and Zones.

Regions – Collection of Zones

- Specific location to run resources

- Connected by Googles global and meshed backbone

Zones – Isolated deployment areas in a region.

- Resource can be zonal, regional or multi regional

# GCP Networking Fundamentals

## Regions and Zones

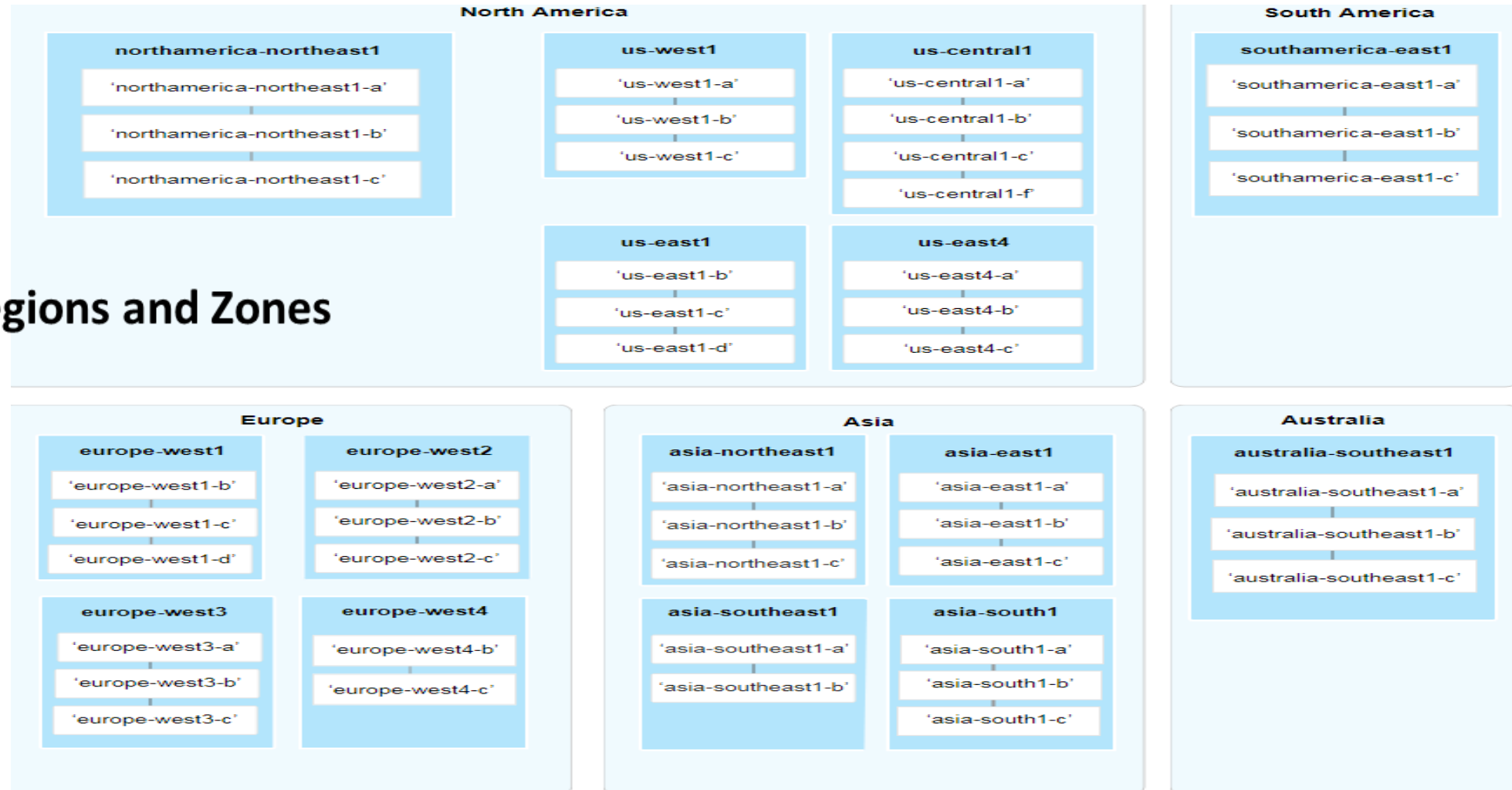
Zones have high-bandwidth, low-latency network connections to other zones in the same region.

Note that there could be bandwidth costs between regions and zones.

Google recommends deploying applications across multiple zones and multiple regions.  
MZ + MR

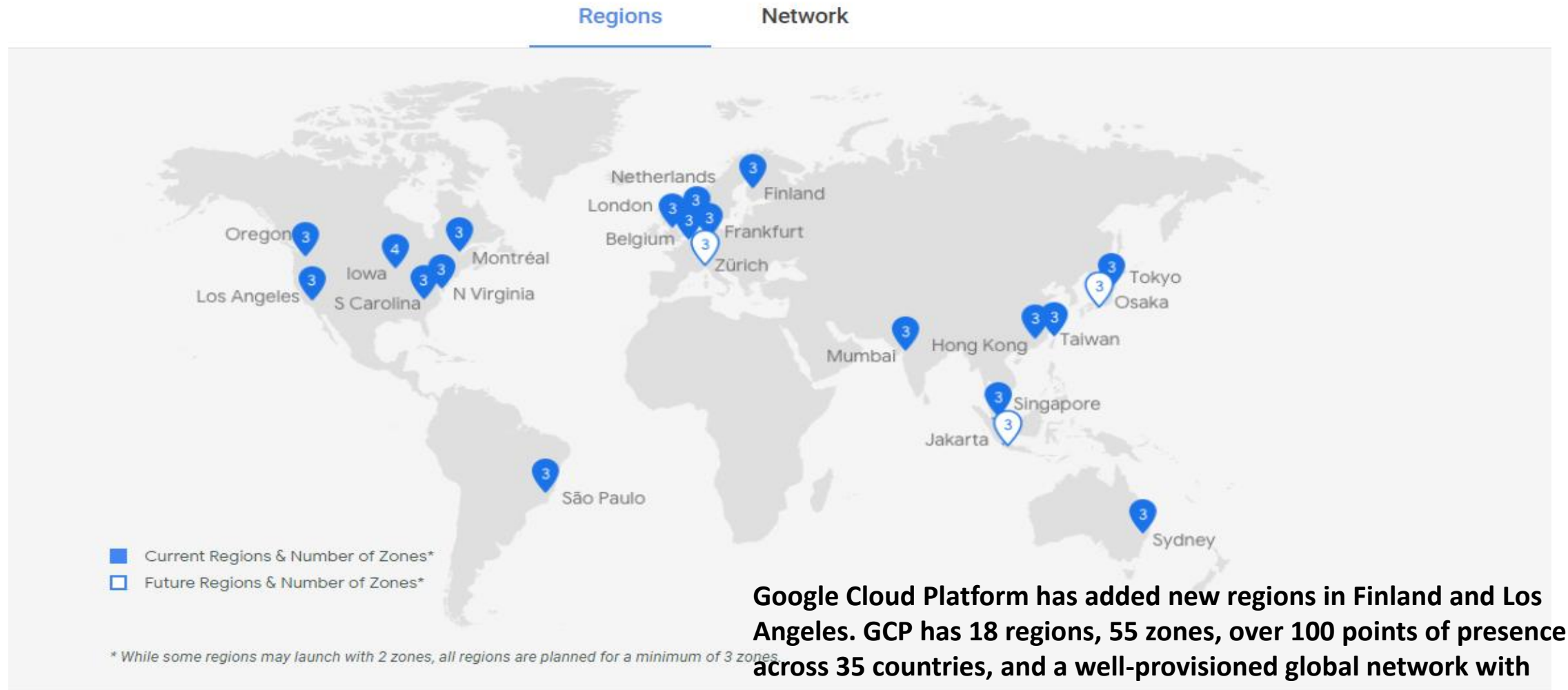
# GCP Networking Fundamentals

## Regions and Zones





# GCP Networking Fundamentals



# Org. Hierarchy and Projects

Google Cloud Platform

GCP Networking Fundamentals

# GCP Networking Fundamentals

## Projects in GCP

# GCP Networking Fundamentals

## Projects



A Project facilitates organization of services and objects and also use this method of segmentation for billing and accounting.



Each Google Cloud Platform project has:



A project name, which you provide.



A project ID, which you can provide or GCP can provide for you.(It is your App ID)



A project number, which GCP provides.

# GCP Networking Fundamentals

## Projects

Use	Use a project to:
Track	Track resource and quota usage.
Billing	Enable billing.
Manage	Manage permissions and credentials.
Enable	Enable services and APIs



# GCP Networking Fundamentals

## Projects



### Project info

Project name

My Python Hello World

Project ID

my-python-hello-world-191118

Project number

452326268329

## Projects

**A Project facilitates organization of services and objects and also use this method of segmentation for billing and accounting.**



[Go to project settings](#)

# GCP Networking Fundamentals



Folders are also introduced when you use Cloud IAM.



The Cloud IAM Folders feature lets you assign policies to resources at a level of granularity you choose.



The resources in a folder can share IAM policies

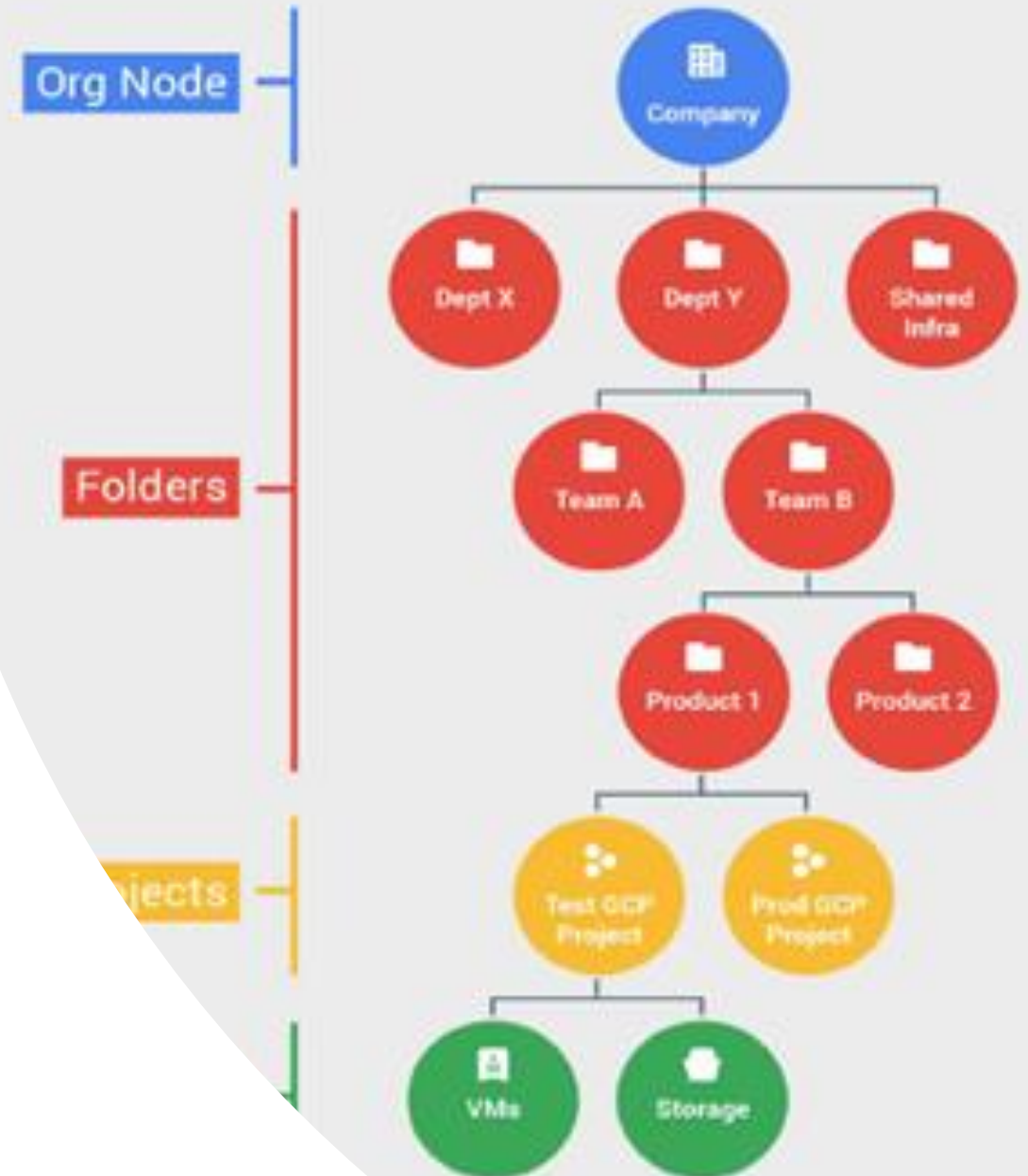


Google Cloud IAM is comparable to AWS Directory Service

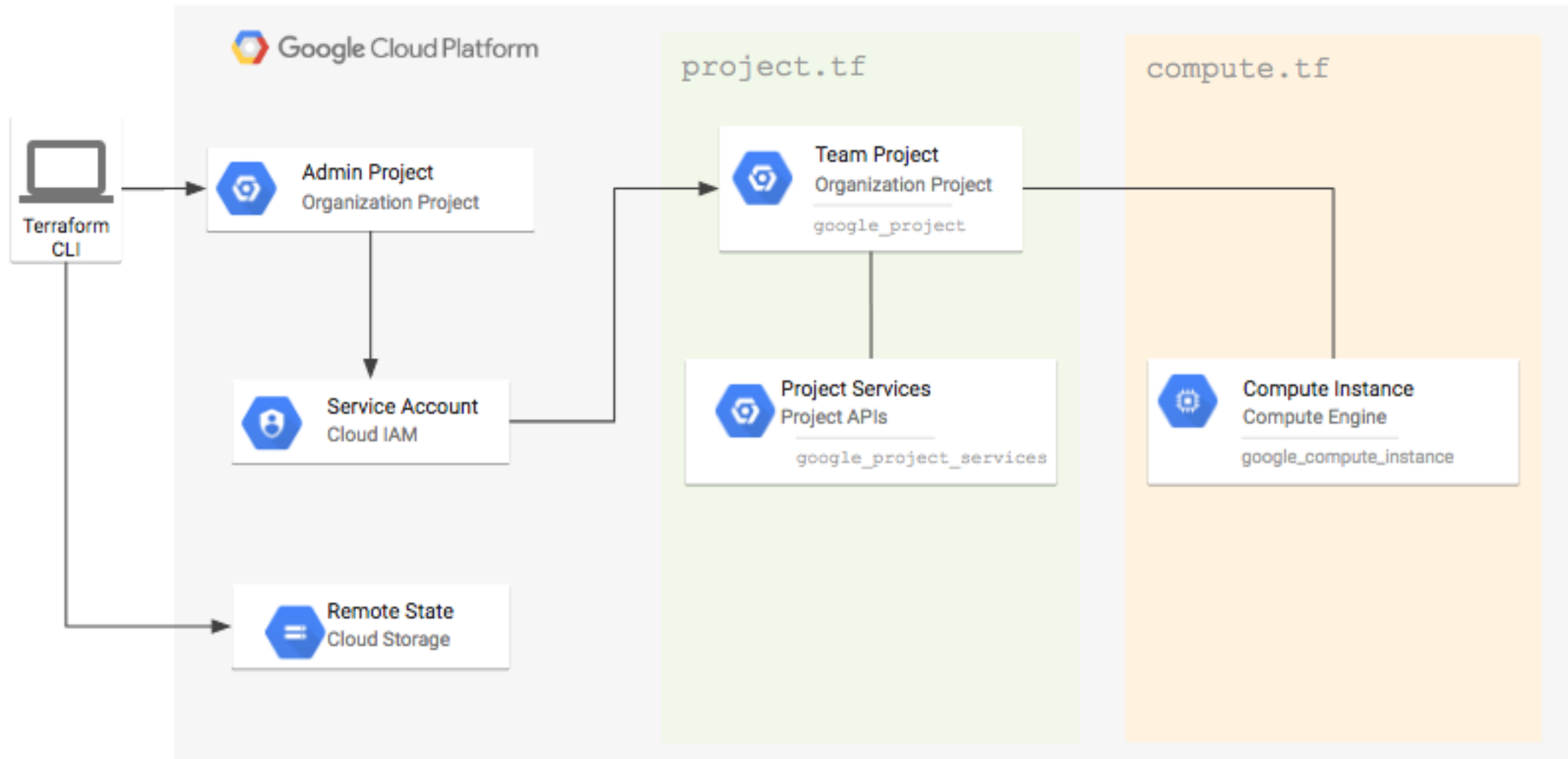
# Projects and Hierarchy

GCP Has the following Hierarchy.

- Organizations
- Folders
- Projects
- Resources



# Projects and Hierarchy





# Projects and Hierarchy

- An Organization resource is available for G Suite and Cloud Identity customers.
- Link your org domain to GCP.
- Think of an Organization as a hierarchy.
- Set access control and configuration settings at the organization or project level
- Billing accounts, projects, and resources are not deleted when an employee leaves the company. Follows corporate lifecycle.

# Projects and Hierarchy

---

GCP accounts can be associated to a G Suite domain or Gmail user account.

This is useful since it can follow a lifecycle with Gmail. If you delete the user, all billing accounts, projects and resources are deleted. (Follow the user)

With GSuite this works different. Billing accounts, projects, and resources follow the company life cycle. (Follow the company organization)

# GCP Networking Fundamentals

*Projects – Notes*

- Google Cloud Platform APIs interact with project-based resources
- Example: disk resources act as data storage for a server
- Resources are either global, regional, or zone-based
  - - Global resources can be used by any other resource, in any region/zone, in the same project
  - - Regional resources can only be used resources in the same region
  - - Zonal resources can only be used resources in the same zone

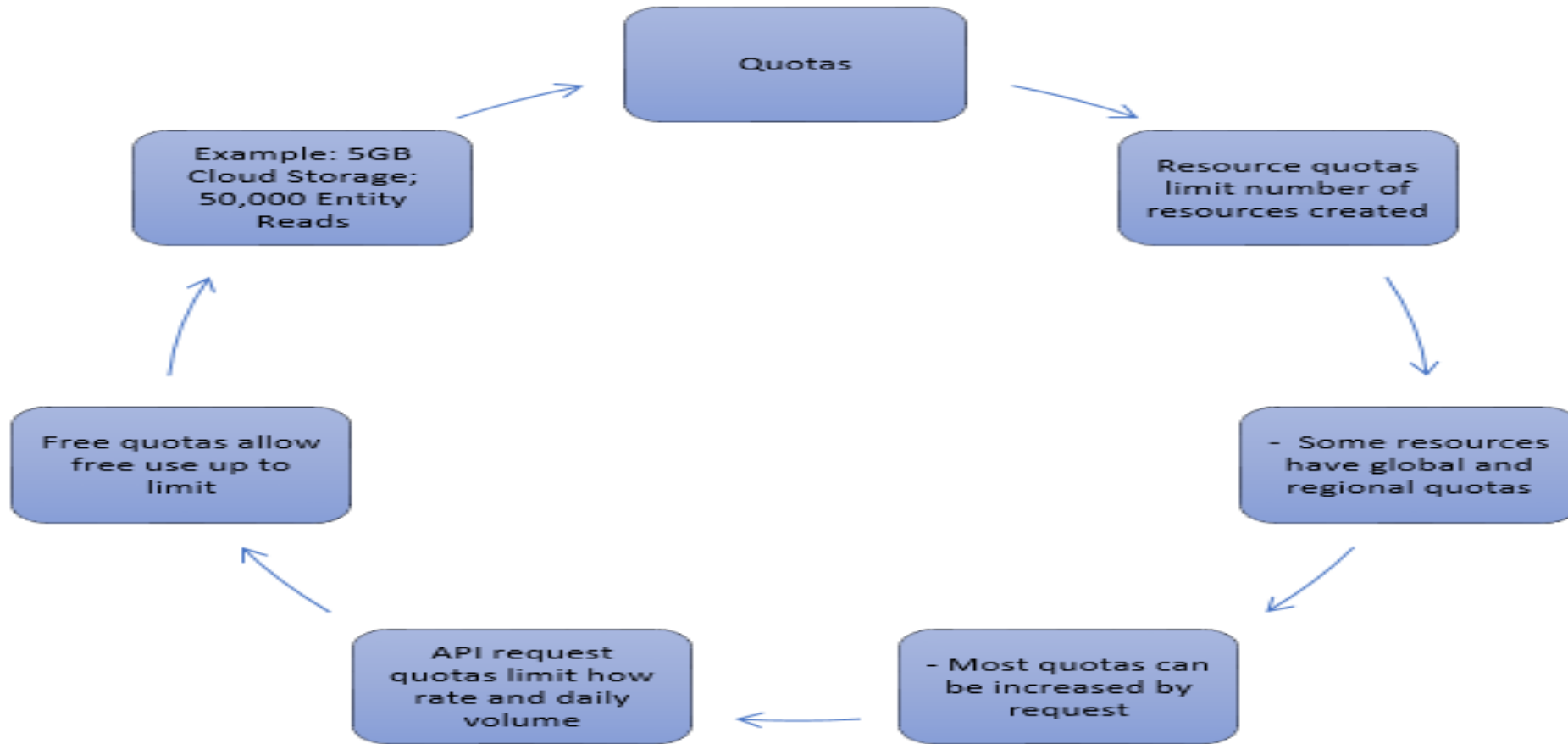


# Gsuite

- - In GCP all you have to do to allow an outside user is to add their Gmail or Gsuite user account to a project
- Add a Gsuite domain as a user and create what is really an admin domain.
- The organization is linked to your G Suite domain.
- - All billing accounts, projects, and resources created by domain members belong to the organization instead of users who create them.



# GCP Networking Fundamentals



# Networking Overview

Google Cloud Platform

Networking Fundamentals



Network Investments by GCP are impressive



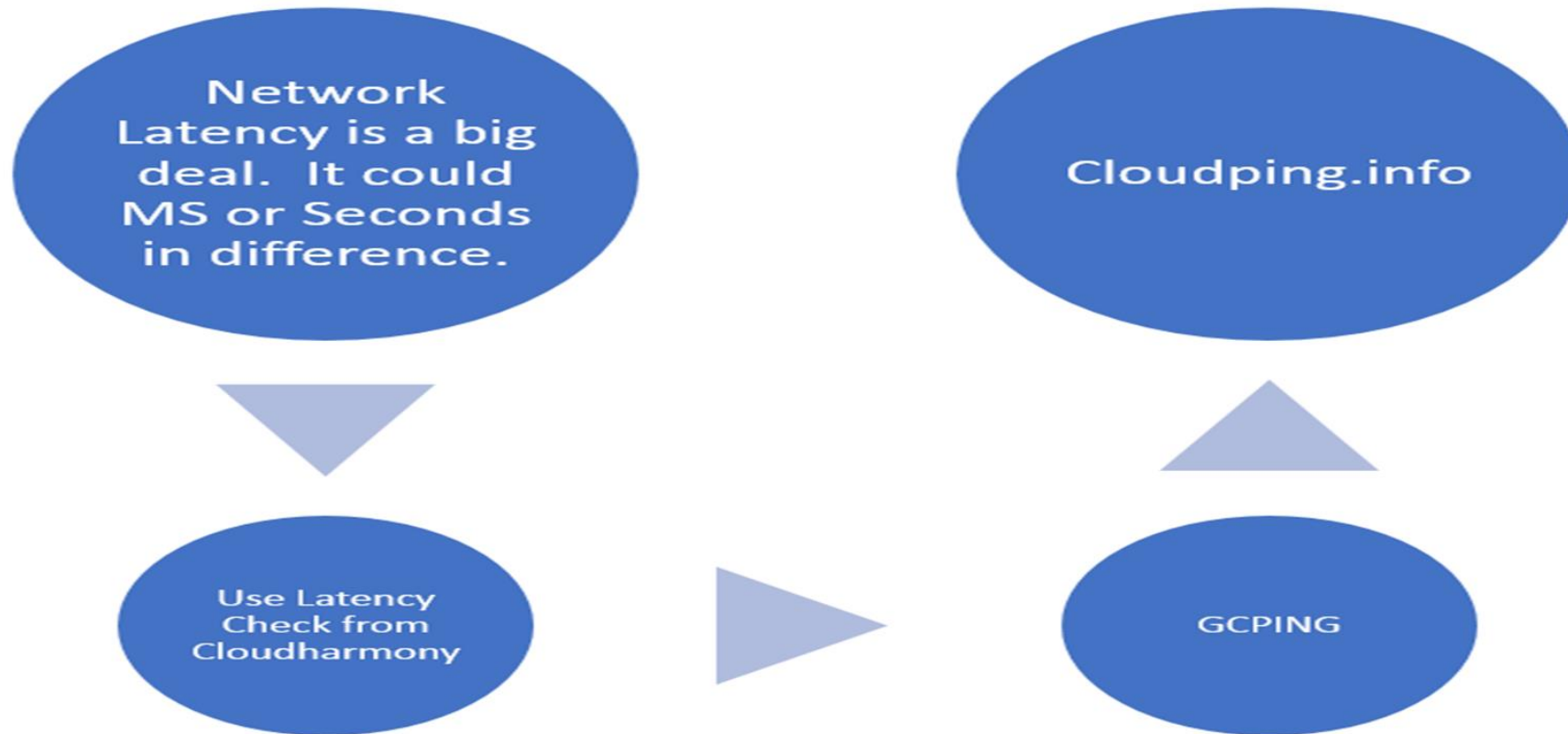
Google Network speed up to 10Tbps of the cable's total 60Tbps bandwidth. JPN – USA



Over Googles private network and not the internet!!!

# GCP Networking Fundamentals

# GCP Networking Fundamentals



# GCP Networking Fundamentals



Google launched the first of any cloud providers network tier service.



Standard Tier - It delivers outbound traffic from GCP to the internet over transit (ISP) networks



Premium Tier - served over Googles low latency and reliable network. (N+2)

# GCP Networking Fundamentals

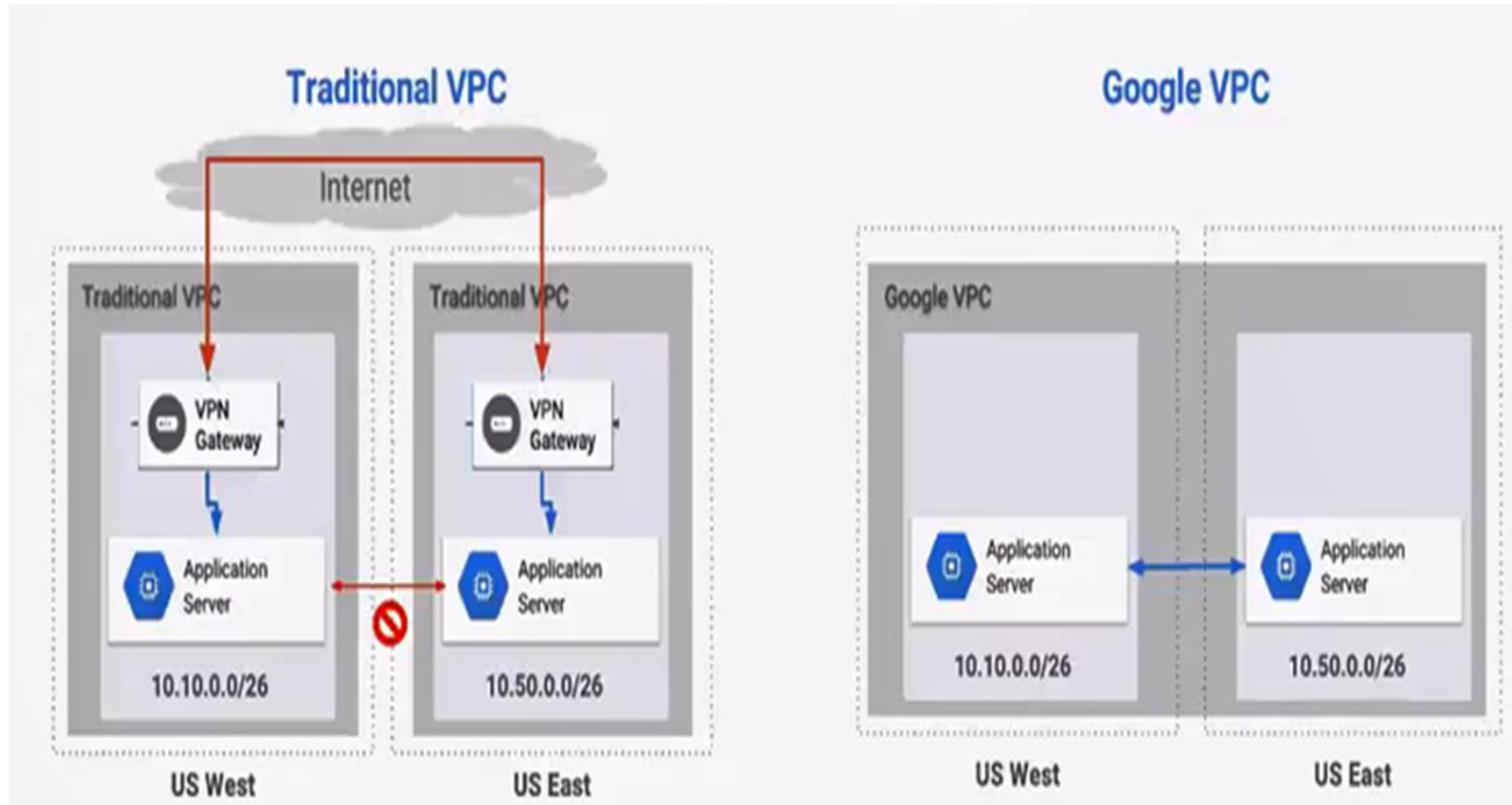
Solutions	GCP	AWS
VPC	VPC	VPC
DNS	Cloud DNS	Route 53
CDN	Cloud CDN	CloudFront
Interconnect	Cloud Interconnect	Direct Connect
Load Balancing	Cloud Load Balancing	Elastic Load Balancing
Tiering	Network Service Tier	N/A

# GCP Networking Fundamentals

	<b>Cloud Scale Services and Comparing to AWS VM Networking</b>	
	GCP offers global networks	
	GCP offers regional subnetting	
	GCP offers a default internet gateway which does not require peering.	
	GCP VMS in Compute Engine are more global.	
	AWS VMS in EC2 are more isolated.	

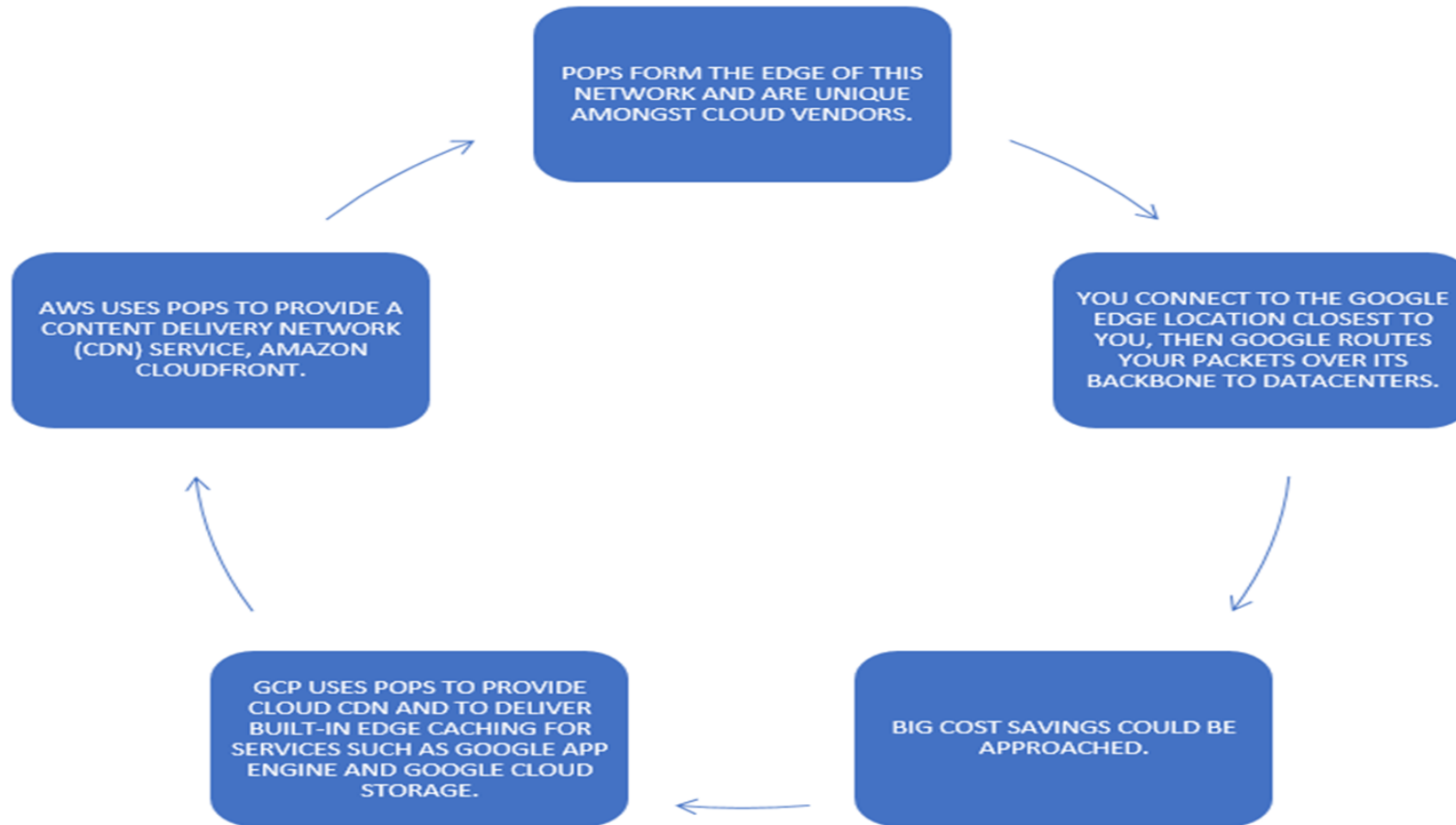
# GCP Networking Fundamentals

<https://cloud.google.com/vpc/docs/vpc>





# GCP Networking Fundamentals



# GCP Networking Fundamentals

---

Networking is Global in GCP

---

Three Types of Networks

---

1. Default

---

2. Custom

---

3. Auto

---

Below are Important Notes about networking

---

Has no IP Range, global and spans regions

---

Contains Subnetworks

---

Use networks to isolate systems.

# GCP Networking Fundamentals

## Networking Services – IP Addressing

Internal IP Addresses

Attached from subnet range to VMS by DHCP

Renewed every 24HRs

VM Name and the IP is registered with DNS

External IP Addresses

Assigned from Pool (Ephemeral)

Reserved (Static)

VM does not know address but it is mapped to internal IP.

# GCP Networking Fundamentals

## Internal IP Addresses DNS Resolution

### DNS Notes

Each instance has a hostname that can be resolved to an internal IP address

- Hostname is the same as the instance name

- FQDN is [hostname].c.[project-id].internal

- Example: guestbook-test.c.guestbook-151617.internal

Name resolution is handled by internal DNS resolver

# Virtual Private Cloud (VPC)

# GCP Networking Fundamentals

What is a VPC

A Virtual Private Cloud (VPC) is a GLOBAL private isolated virtual network partition that provides managed networking functionality for your Google Cloud Platform (GCP) resources

Sandbox

# GCP Networking Fundamentals

Google Cloud Platform

My Python Hello World

VPC network

VPC networks

External IP addresses

Firewall rules

Routes

VPC network peering

Shared VPC

VPC networks

CREATE VPC NETWORK

REFRESH

Name	Region	Subnets	Mode	IP addresses ranges	Gateways	Firewall Rules	Global dynamic routing
default		15	Auto			6	Off
	us-central1	default		10.128.0.0/20	10.128.0.1		
	europa-west1	default		10.132.0.0/20	10.132.0.1		
	us-west1	default		10.138.0.0/20	10.138.0.1		
	asia-east1	default		10.140.0.0/20	10.140.0.1		
	us-east1	default		10.142.0.0/20	10.142.0.1		
	asia-northeast1	default		10.146.0.0/20	10.146.0.1		
	asia-southeast1	default		10.148.0.0/20	10.148.0.1		
	us-east4	default		10.150.0.0/20	10.150.0.1		
	australia-southeast1	default		10.152.0.0/20	10.152.0.1		
	europa-west2	default		10.154.0.0/20	10.154.0.1		
	europa-west3	default		10.156.0.0/20	10.156.0.1		
	southamerica-east1	default		10.158.0.0/20	10.158.0.1		
	asia-south1	default		10.160.0.0/20	10.160.0.1		
	northamerica-northeast1	default		10.162.0.0/20	10.162.0.1		
	europa-west4	default		10.164.0.0/20	10.164.0.1		

# GCP Networking Fundamentals

A VPC supports  
your enterprise  
with

Global  
Communications  
Space

Compute or GCP  
Services

Shared VPC

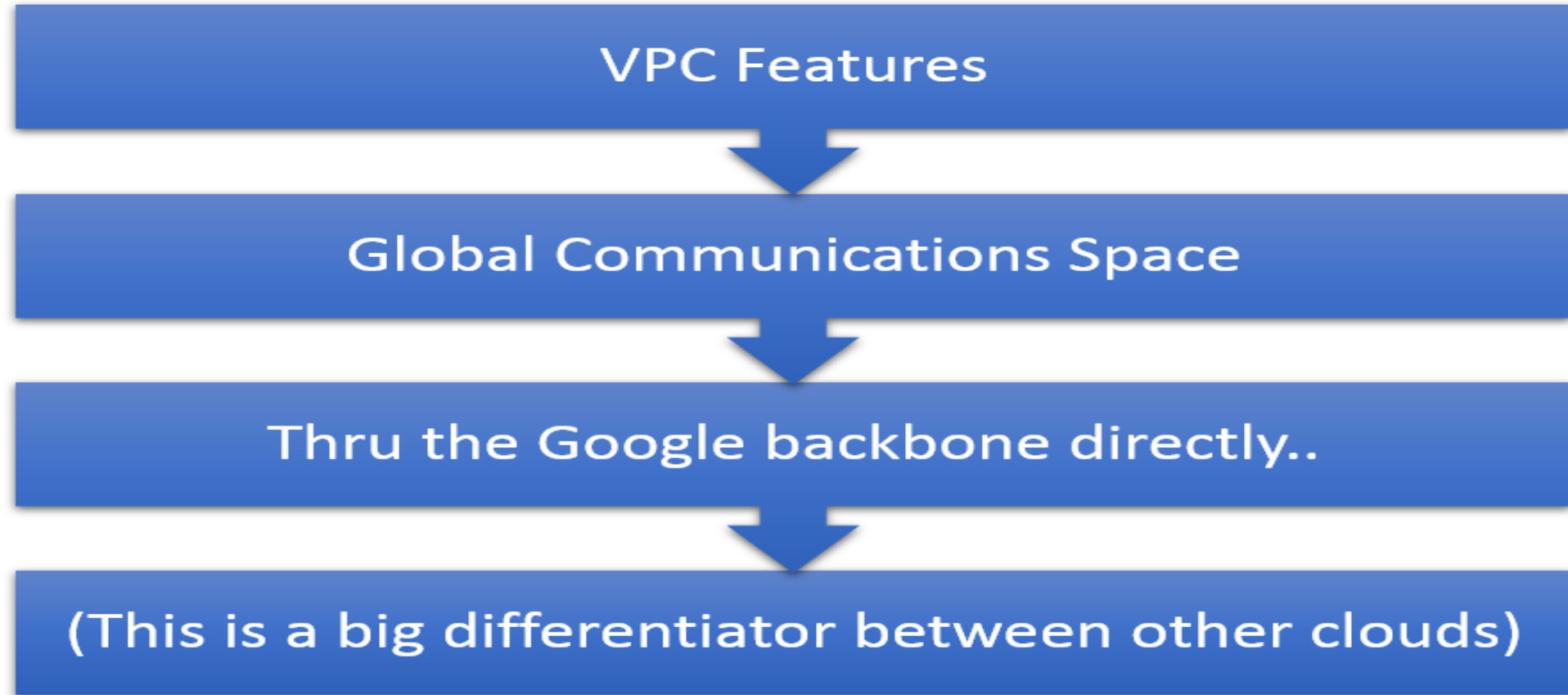
Hybrid Support

Private Peering

Two Types (Auto  
& Custom)



# GCP Networking Fundamentals



<https://cloud.google.com/vpc/docs/vpc>

# GCP Networking Fundamentals

## VPC Modes

### Auto Mode

- VPC Network is created with one subnet from each region is automatically created within it
- Uses predefined IP Range
- Adds new regions automatically with subnets
- Can add manually

### Custom Mode

- Custom Config
- VPC Network is created (no subnets are created automatically)
- Uses your custom IP Range
- You have control and add subnets as required.

# GCP Networking Fundamentals



VPC Peering



Can add manually Google Cloud Platform (GCP)  
Virtual Private Cloud (VPC)



Network Peering allows  
private RFC1918 connectivity across two VPC  
networks regardless of whether or not they  
belong to the same project or the same  
organization

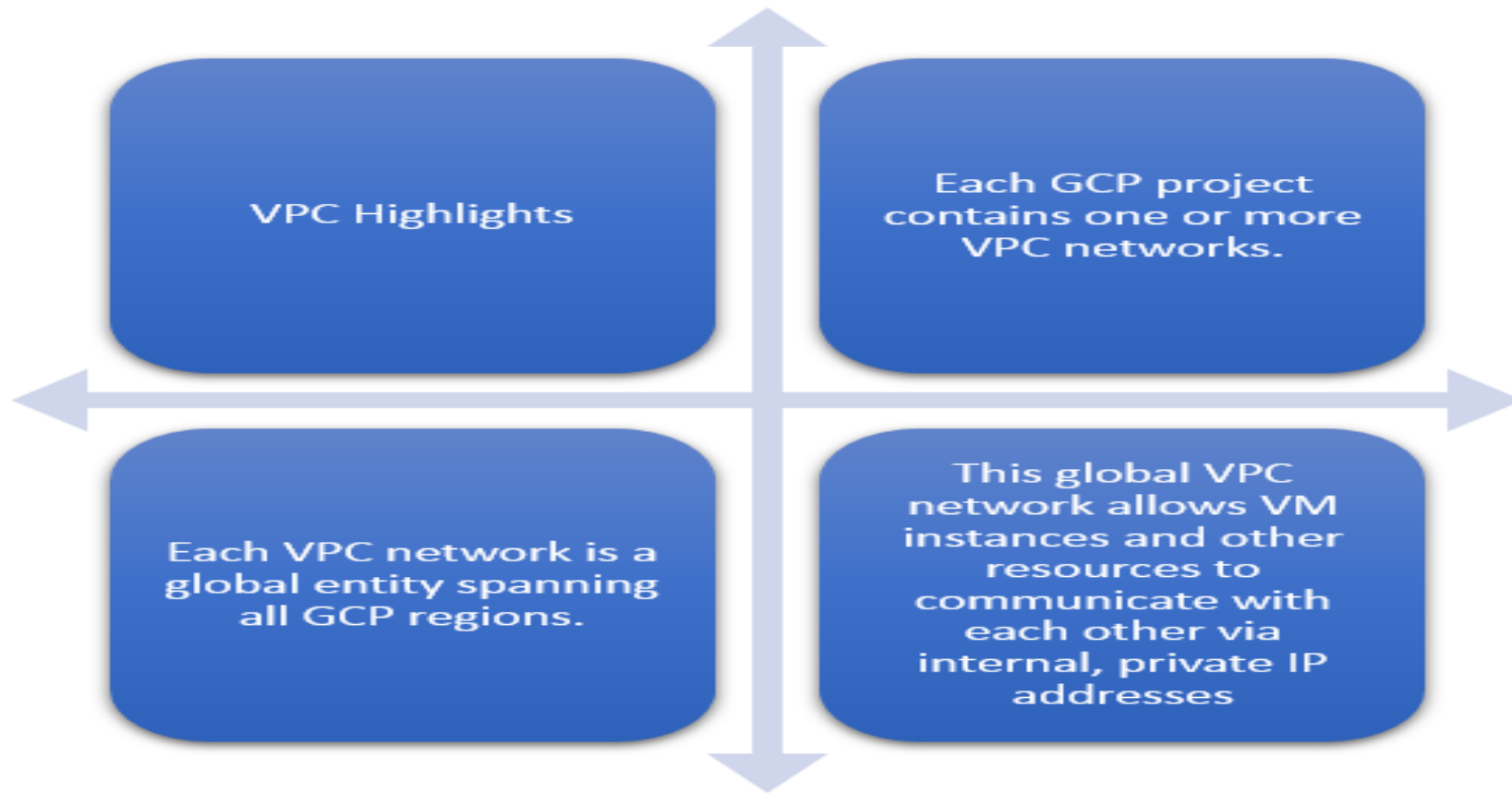
# GCP Networking Fundamentals

## VPC Peering Use Cases

Organizations with several network administrative domains.

Organizations that want to peer with other organizations.

# GCP Networking Fundamentals

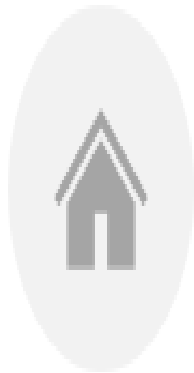


# GCP Networking Fundamentals

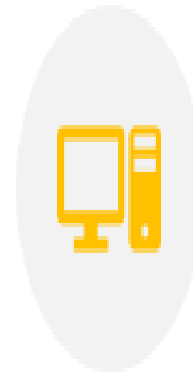
## Global, regional, and zonal resources



- Global resources include preconfigured disk images, disk snapshots and networks.



- Regional resources include static external IP addresses.



- Zonal resources include VM instances, their types, and disks.

# Cloud VPN

Google Cloud Platform  
Networking Fundamentals

# GCP Networking Fundamentals

<https://cloud.google.com/vpn/docs/concepts/overview>



Virtual Private Network (VPN)



Google Cloud VPN securely connects your on-premises network to your Google Cloud Platform (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection.



Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway.



Protects your data as it travels over the Internet.



Cloud VPN only supports IPsec gateway-to-gateway scenarios. You must have a dedicated physical or virtual IPsec VPN gateway on the client side.



# GCP Networking Fundamentals



Cloud VPN Features



High throughput, high reliability, managed service



High throughput IPsec tunnels



- IKE v1 and v2 supported



- Can run over Cloud Interconnect

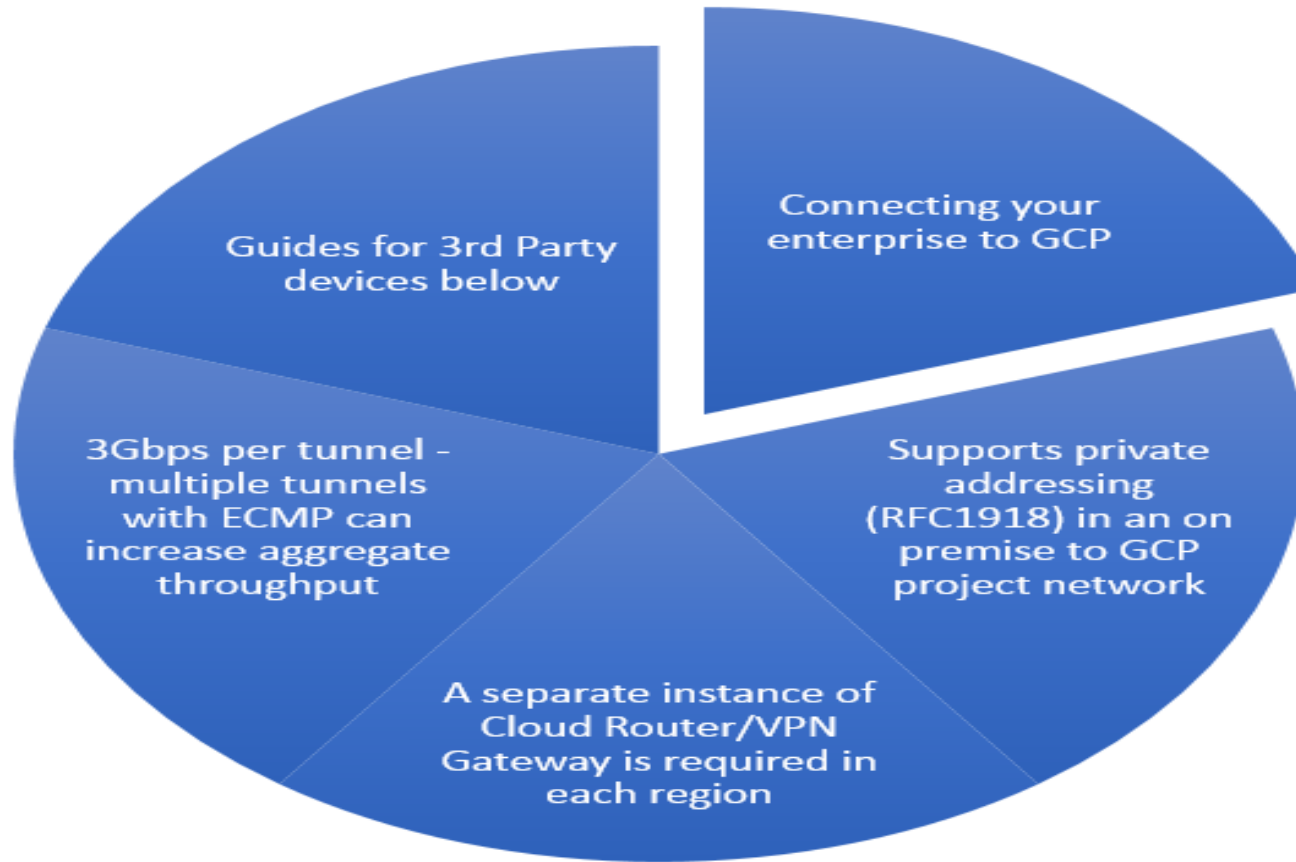


ECMP over multiple VPN tunnels to achieve greater overall throughput



Leverages Google's Edge locations across the globe to minimize latency

# GCP Networking Fundamentals



<https://cloud.google.com/compute/docs/vpn/interop-guides>

# GCP Networking Fundamentals



Connecting to GCP Static Routes



*With static routing, updating the tunnel requires the addition of static routes to Google Cloud Platform and restarting the VPN tunnel to include the new subnet.*



Some points to know for Exam..



Public IP on both peers



Global or Regional



1.5 Gbps throughput



Secret password



Scale horizontally through parallel tunnels

# GCP Networking Fundamentals

## VPC and VPNs - Connecting

Depending on your VPC network and how many regions you want to connect, the initial procedure is somewhat different.

### Several Options to consider

1. Simple setup
2. Auto mode VPC network using only the gateway subnet
3. Auto mode VPC network using more than one subnet
4. Custom Network VPN
5. Legacy Networks

[https://cloud.google.com/vpn/docs/concepts/overview#vpn\\_diagram](https://cloud.google.com/vpn/docs/concepts/overview#vpn_diagram)

# Hybrid Connectivity

# Cloud Interconnect

# GCP Networking Fundamentals



Cloud Interconnect



GCP has a interconnect (AWS Directconnect) called Cloud Interconnect to extend your data center network into your Google Cloud projects.



IPSec VPN



Direct access to RFC1918 IPs in your VPC (SLA)



Partner Interconnect

# GCP Networking Fundamentals

## Cloud/Partner Interconnect

- 10 Gbps connections for Cloud Interconnect (Up to 10Gbps connections for a max of 80Mbps)
- 50Mbps minimum for Partner Interconnect and scale to partner support
- Use your own VPN Solution or application level
- <https://cloud.google.com/hybrid-connectivity/>





# Peering

# GCP Networking Fundamentals



VPC Peering



Can add manually Google Cloud Platform (GCP)  
Virtual Private Cloud (VPC)



Network Peering allows  
private RFC1918 connectivity across two VPC  
networks regardless of whether or not they  
belong to the same project or the same  
organization

# GCP Networking Fundamentals

## VPC Peering Use Cases

Organizations with several network administrative domains.

Organizations that want to peer with other organizations.

# GCP Networking Fundamentals

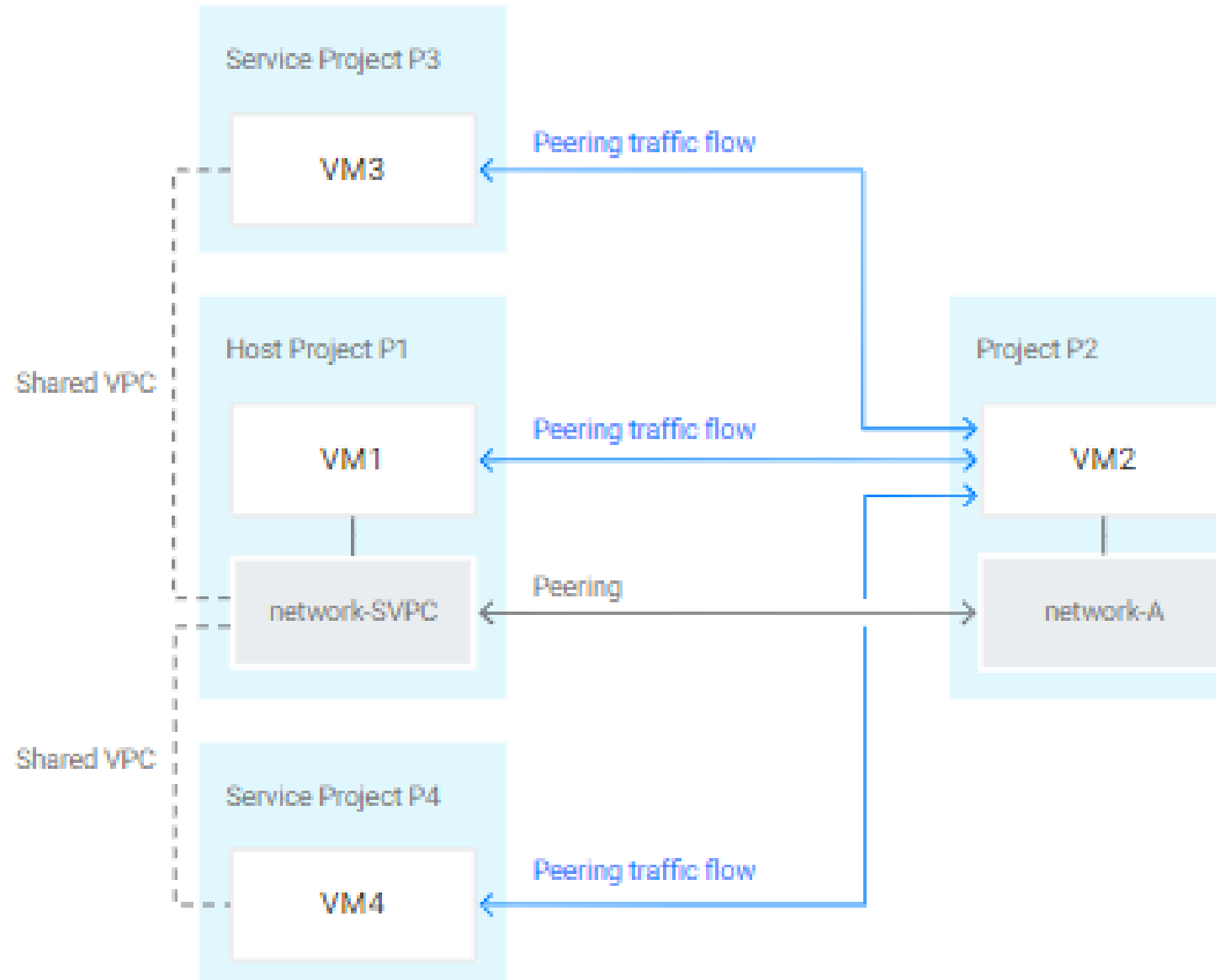
- VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks:
  - 1. Network Latency
  - 2. Network Security
  - 3. Network Cost

<https://cloud.google.com/vpc/docs/vpc-peering>

# GCP Networking Fundamentals

Peering works with:

- Compute Engine
- App Engine (Flexible)
- GKE



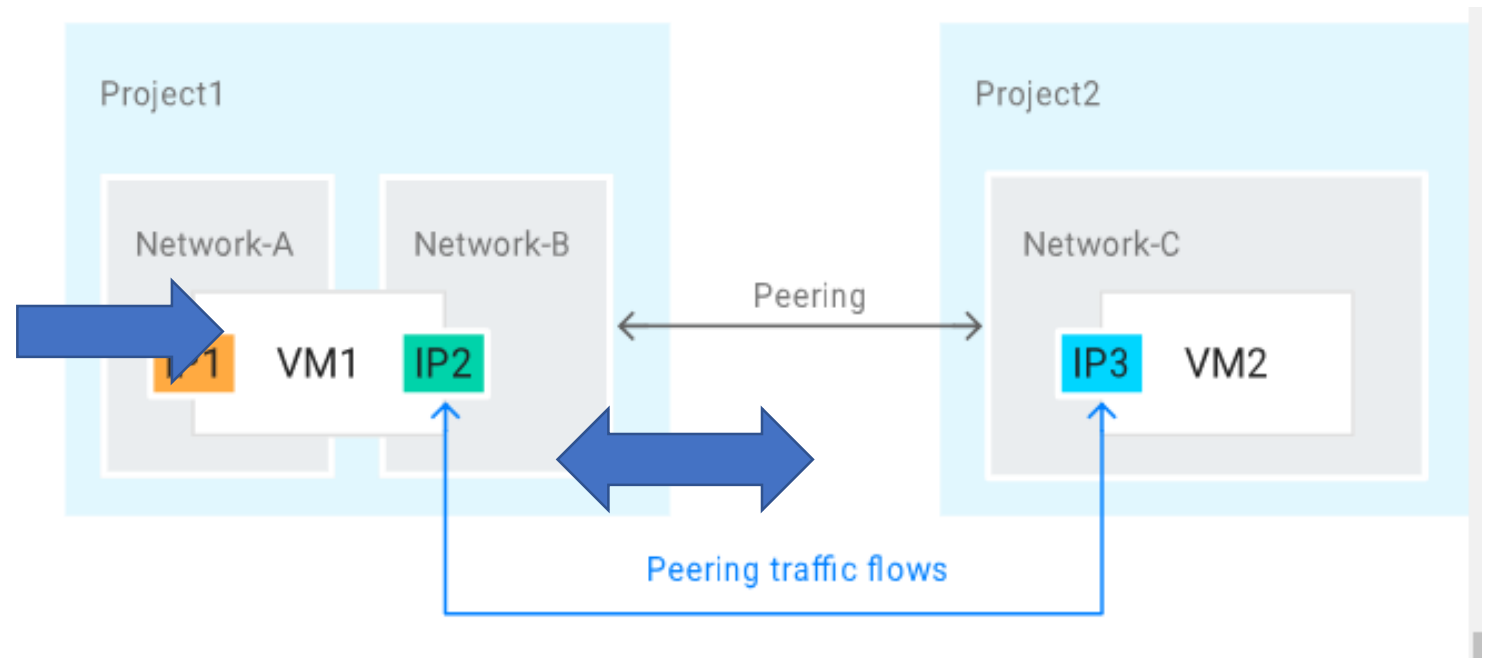
# GCP Networking Fundamentals

## Properties

- Peered VPC networks remain administratively separate. Routes, firewalls, VPNs, and other traffic management tools are administered and applied separately in each of the VPC networks.
- Each side of a peering association is set up independently. Peering will be active only when the configuration from both sides matches
- A given VPC network can peer with multiple VPC networks

# GCP Networking Fundamentals

- Shared VPC
- VPC Network Peering allows peering with a Shared VPC.
- A shared VPC host project is a project that allows other projects to use one of its networks.



# Cloud CDN

Google Cloud Platform  
Networking Fundamentals



# GCP Networking Fundamentals

- Google Cloud CDN leverages Google's globally distributed edge caches to accelerate content delivery for websites and applications served out of Google Compute Engine.
- Cloud CDN lowers network latency, offloads origins, and reduces serving costs.
- Enable with a checkbox

# GCP Networking Fundamentals

- Google Cloud features built-in edge caching in its points of presence for some services
- For Example. Cloud Storage and App Engine and thus you may not need to implement other CDN products
- CDN works with GCP Load Balancing
- Cloud Storage bucket mapping
- Supports Custom Domains (HTTPS)

# GCP Networking Fundamentals

---

- Content delivery network (CDN) peering provides a connection between your resources in the cloud and a CDN provider by way of network edge locations.
- Google provides CDN peering for several CDN providers through its CDN Interconnect service.
- Amazon only provides CDN peering for its own CDN service, Amazon CloudFront.

# Load Balancing

Google Cloud Platform

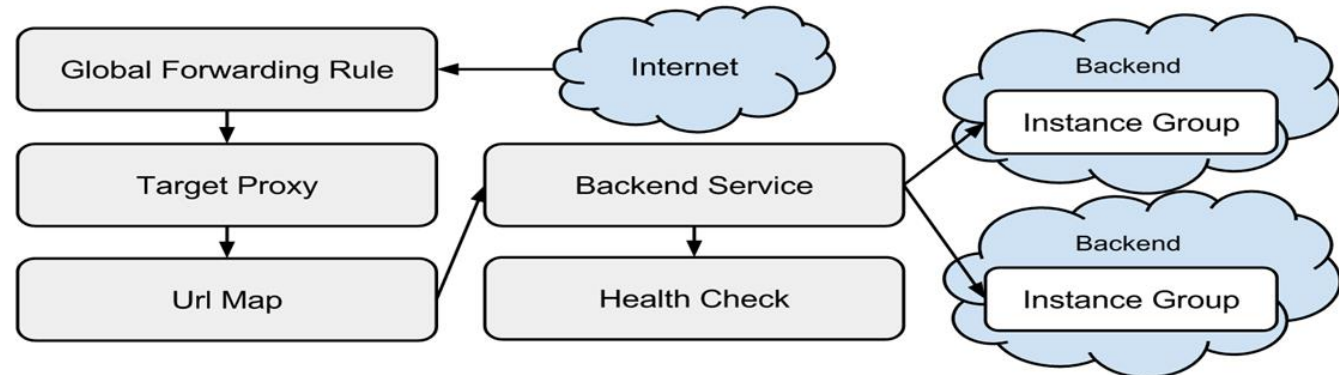
Networking Fundamentals

# GCP Networking Fundamentals

AWS and GCP approach load balancing very differently.

- AWS is manual service and is VPC bound
- GCP is a managed service and is global.

Lets discuss more in detail

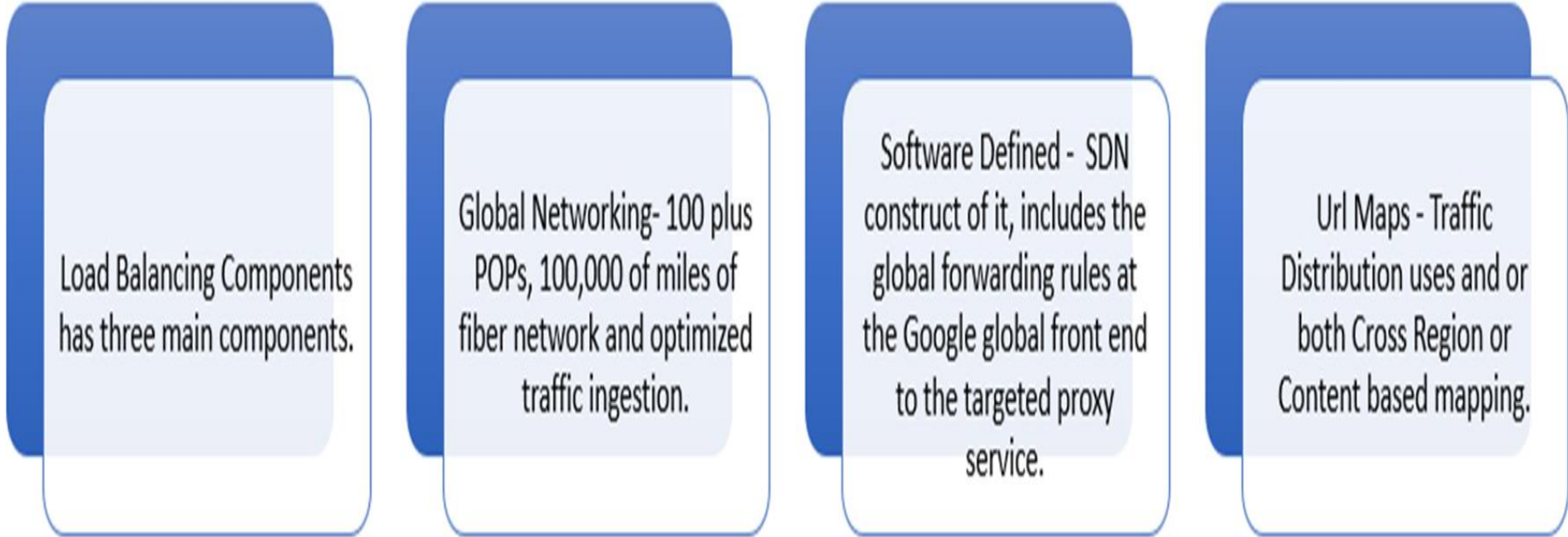


# GCP Networking Fundamentals

	AWS	GCP
Service	Elastic Load Balancer	Compute Engine
Network load balancing	Yes	Yes
Static IP	No	Yes
Content	No	Yes
Cross Region	No	Yes
Scaling Pattern	Linear	Real Time
Locality	Regional	Global

# GCP Networking Fundamentals

Load Balancing Components has three main components.



Load Balancing Components  
has three main components.

Global Networking- 100 plus  
POPs, 100,000 of miles of  
fiber network and optimized  
traffic ingestion.

Software Defined - SDN  
construct of it, includes the  
global forwarding rules at  
the Google global front end  
to the targeted proxy  
service.

Url Maps - Traffic  
Distribution uses and or  
both Cross Region or  
Content based mapping.

# GCP Networking Fundamentals

Load Balancing

Types of Load Balancing

- Network Load Balancing

- HTTPS Load Balancing

- Cross-Region Load Balancing

- Content-based Load Balancing

- Cloud SSL Proxy



# GCP Networking Fundamentals

Network Load Balancing in GCP is a Managed Service and deployed globally.

- Network load balancing distributes incoming traffic across multiple instances
  - Supports non-HTTP(S) protocols (TCP/UDP)
  - Can be used for HTTPS traffic when you want to terminate connection on your instances (not at HTTPS load balancer)
- Supports autoscaling with managed instance groups

<https://cloud.google.com/compute/docs/load-balancing/network/>

# GCP Networking Fundamentals

Network Load  
Balancing

Forwarding  
rules consist of...

Name

Region

IP Address  
(regional, not  
global)

IP Protocol (TCP,  
UDP; AH, ESP,  
ICMP, SCTP)

Ports

Target-pool or  
target-instance



# GCP Networking Fundamentals

## Network Load Balancing

- Target pools consist of...
- Name
- Description
- Region
- Instances (must all be in same region as target pool)
- SessionAffinity (NONE, CLIENT\_IP\_PROT, CLIENT\_IP)
- BackupPool
- FailoverRatio

# GCP Networking Fundamentals

HTTP(S) Load Balancing



HTTP(S) Load Balancing distributes HTTP(S) traffic among instance groups based on proximity to user or URL or both



Autoscalers can be attached to HTTP(S)load balancers

<https://cloud.google.com/compute/docs/load-balancing/network/>

# GCP Networking Fundamentals

HTTP(S) Load  
Balancing

HTTP(S) The  
following resources  
comprise a load  
balancer

Global Forwarding  
Rule

Target Proxy (w SSL  
certificate resource  
for HTTPS proxy)

URL map

Backend Service  
and Backends

Health Check

The load balancer  
leverages  
additional  
resources

Global IP Address  
(ephemeral or  
static)

One or more  
Instance Groups

# GCP Networking Fundamentals

## Global Forwarding

- A global forwarding rule provides a single global IP address for an application
- The rule routes traffic by IP address, port, and protocol to an HTTP or HTTPS target proxy
- A global forwarding rule can only forward to a single port
- Global forwarding rules can only be used by an HTTP(S) load balancer

<https://cloud.google.com/compute/docs/load-balancing/http/global-forwarding-rules>

# GCP Networking Fundamentals

Target proxies route incoming HTTP(requests) based on URL maps and backend service configurations

- HTTPS target proxy terminates client SSL session
- HTTPS target proxies require configured SSL certificate resources

<https://cloud.google.com/compute/docs/load-balancing/http/target-proxies>

# GCP Networking Fundamentals

Backend services

A health check  
capacity

Session affinity  
settings

One or more  
backends

A backend  
comprises

An instance group  
(managed or  
unmanaged)

A balancing mode  
(CPU utilization or  
Rate in  
request/second)

A capacity scaler  
(ceiling % of  
CPU/Rate targets)

A backend service  
can have up to 500  
endpoints per zone



# GCP Networking Fundamentals

- Connection draining delays the termination of an instance until remaining connections are closed
  - New connections to the instance are prevented
  - Instance preserves existing sessions until they end OR a designate timeout is reached (1 to 3600 seconds)
    - Minimizes interruption for users
- Connection draining is triggered when an instance is removed from an instance group
  - Manual removal, resizing, autoscaling

<https://cloud.google.com/compute/docs/load-balancing/enabling-connection-draining>

# GCP Networking Fundamentals

## Why Cloud SSL Proxy

### Cloud SSL proxy alt type of load balancing

- non-HTTP(S) traffic

- Performs global load balancing, routing clients to the closest instance with capacity

### Cloud SSL proxy advantages

- Intelligent routing

- Reduced CPI load on instances

- Certificate management

- Security patching



# GCP Networking Fundamentals

## Cross Region Load Balancing

- HTTP/HTTPS only
- Cross-region using a single global IP address
- Requests routed to the closest region
- Automatically reroutes to next closest once capacity is reached
- Eliminates need for DNS-based load balancing



# GCP Networking Fundamentals

## Content Based Load Balancing

- HTTP/HTTPS only
- Create multiple backend services to handle content types
- Add path rules to backend services
  - - /video for video services
  - - /static for static content
- Configure different instance types for different content types

# Instance Groups

Google Cloud Architect Exam Bootcamp

# GCP Networking Fundamentals

**Instance Groups** are Managed Groups of VMs

Three Types

1. Unmanaged
2. Managed Instance Group (Zonal)
3. Managed Instance Group (Regional)

**Unmanaged instance groups contain dissimilar instances and wont.**

- Autoscaling
- Rolling updates
- Instance creation using instance templates

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances>

Google Cloud Architect Exam Bootcamp

# Auto Scaling

# GCP Networking Fundamentals

## Autoscaling

- Part of the Compute Engine API
- Used to automatically scale number of instances in a managed instance group based on workload
- Create one autoscaler per managed instance group
- Autoscalers can be used with zone-based managed instance groups or regional managed instance groups
- Fast typically ~ 1 min windows

[https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance-groups#provisioning\\_your\\_autoscaler\\_configuration](https://cloud.google.com/compute/docs/instance-groups/distributing-instances-with-regional-instance-groups#provisioning_your_autoscaler_configuration)



# IAM

Google Cloud Architect Exam Bootcamp

# GCP Networking Fundamentals

	AWS	GCP
Users/Groups	Individual Accounts and Groups	Individual Accounts but need Google account
Outside of Cloud Users	No	Yes
Policy	Yes, is considered a document that lists permissions. Attached to a user or group	A list of bindings that binds members to a role. Attached to a resources
Role Stages	No	Yes
API	Yes	No, provides a URI for http requests.
Environments	Yes, link them (Cross Account)	Done via projects

# GCP Networking Fundamentals

- Manage projects and IAM services using Google Cloud Platform API calls. URIs are relative to <https://iam.googleapis.com>.
- Google Cloud Platform provides the Key Management Service (KMS) to manage encryption keys. KMS provides AES 256 standard encryption.
- IAM and Audit Logging features that allow Google Cloud Platform users to manage and monitor permissions of an individual key.
- IAM service policy consists of a list of members bound to roles.
- A Role is a collection of permissions that is assigned to a user, group or service account.

# GCP Networking Fundamentals

---

Identity and Access Management (IAM)

---

Cloud IAM, you grant access to members. Members can be of following types:

---

Google account

---

Service account

---

Google group

---

G Suite domain

---

Cloud Identity domain

# GCP Networking Fundamentals

---

A large number of projects can become unwieldy to manage at scale. This is why IAM includes the concept of an Organization Node.

---

The Organization Node sits above Projects and is your company's root node for Google Cloud resources.

---

Gsuite, when you enable the Organization Node, any project created by users in your domain will automatically belong to your Organization Node

---

The account with Organization Owner role is empowered to modify all projects within the organization.

---

Changes to the organization must occur through Google Sales.

---

# GCP Networking Fundamentals



**IAM ORG NODES**



**USE YOUR OWN  
AUTHENTICATION  
MECHANISM AND MANAGE  
YOUR OWN CREDENTIALS**



**FEDERATE YOUR IDENTITIES  
TO GOOGLE CLOUD  
PLATFORM**



**USERS DO NOT HAVE TO  
LOGIN A SECOND TIME TO  
ACCESS CLOUD PLATFORM  
RESOURCES**

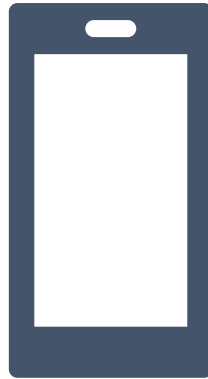


**REVOKE ACCESS TO CLOUD  
PLATFORM USING YOUR  
EXISTING CREDENTIAL  
MANAGEMENT**



**GOOGLE APPS DIRECTORY  
SYNC INTEGRATES WITH  
LDAP**

# GCP Networking Fundamentals



## Roles

# GCP Cloud Architect Overview

---

There are three types of roles in GCP Cloud IAM:

---

**Primitive roles:** The original roles available in the Google Cloud Platform Console. These are the Owner, Editor, and Viewer roles. Still assigned by default to projects. Primitive roles are quite broad.

---

**Curated roles:** Curated roles are new IAM roles that give finer-grained access control than the primitive roles

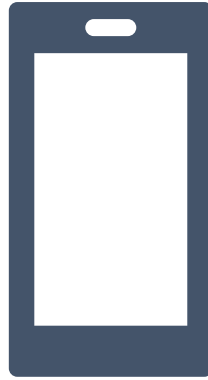
---

**Custom Roles** - provide granular access according to a user-specified list of permissions

---



# GCP Cloud Architect Overview



## **Service Accounts**

# GCP Cloud Architect Overview



GCP Service Accounts



A service account is an identity for your programs to use to authenticate and gain access to GCP APIs. (Server to Server)



Service accounts authenticate applications running on your virtual machine instances to other GCP services.



Each service account is associated with a key pair, which is managed by GCP. It is used for service-to-service authentication within GCP.



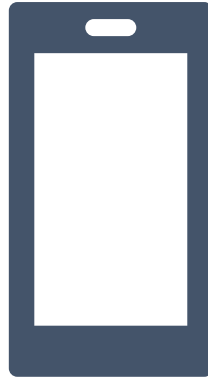
Google rotates the keys daily.

# GCP Cloud Architect Overview

- By default, all projects come with the Compute Engine default service account.
- When you start a new instance using gcloud, the default service account is enabled on that instance.
- Apart from the default service account, all projects come with a Google APIs service account, identifiable using the email:

`{project-number}@cloudservices.gserviceaccount.com`

# GCP Cloud Architect Overview



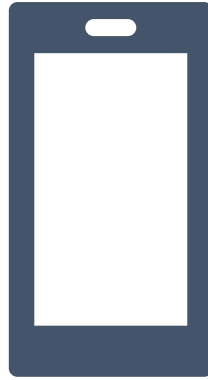
## **App Engine Permissions**

# GCP Cloud Architect Overview

Role Name	Role Title	Description	Resource Type
<code>roles/appengine.appAdmin</code>	App Engine Admin	Read/Write/Modify access to all application configuration and settings.	Project
<code>roles/appengine.serviceAdmin</code>	App Engine Service Admin	Read-only access to all application configuration and settings. Write access to module-level and version-level settings. Cannot deploy a new version.	Project
<code>roles/appengine.deployer</code>	App Engine Deployer	Read-only access to all application configuration and settings. Write access only to create a new version; cannot modify existing versions other than deleting versions that are not receiving traffic.	Project
<code>roles/appengine.appViewer</code>	App Engine Viewer	Read-only access to all application configuration and settings.	Project
<code>roles/appengine.codeViewer</code>	App Engine Code Viewer	Read-only access to all application configuration, settings, and deployed source code.	Project

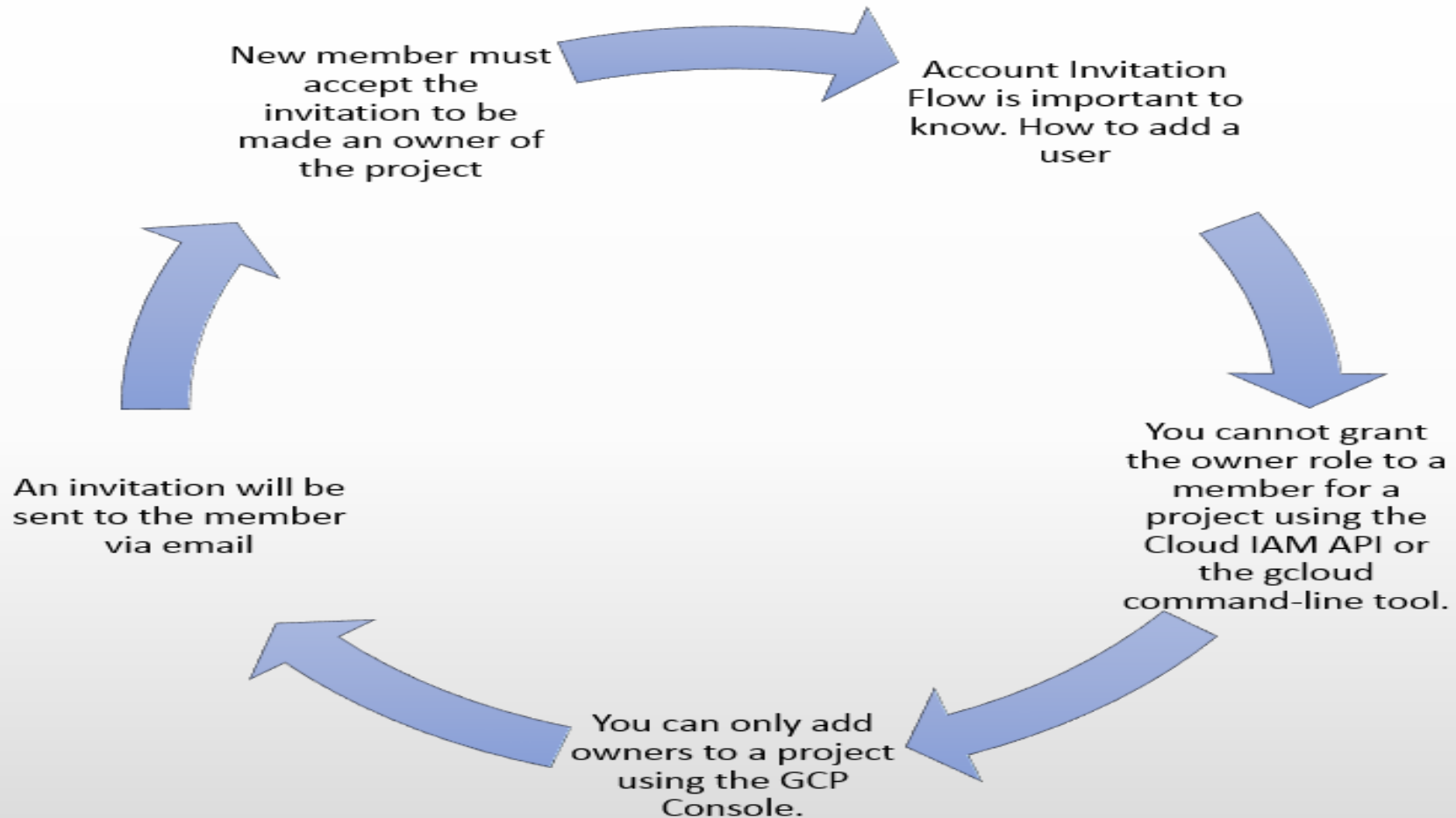
<https://cloud.google.com/iam/docs/understanding-roles>

# GCP Cloud Architect Overview



## **Access Invitation Workflow**

# GCP Cloud Architect Overview



<https://cloud.google.com/iam/docs/understanding-roles>

# GCDS

Google Cloud Architect Exam Bootcamp



# GCP Networking Fundamentals



Google Cloud Directory Sync



GSuite Admin can automatically add, modify, and delete users, groups, and non employee contacts to synchronize the data in a GSuite domain with an LDAP directory server or MS Active Directory.



The data in the LDAP directory server is never modified or compromised. (one way update)

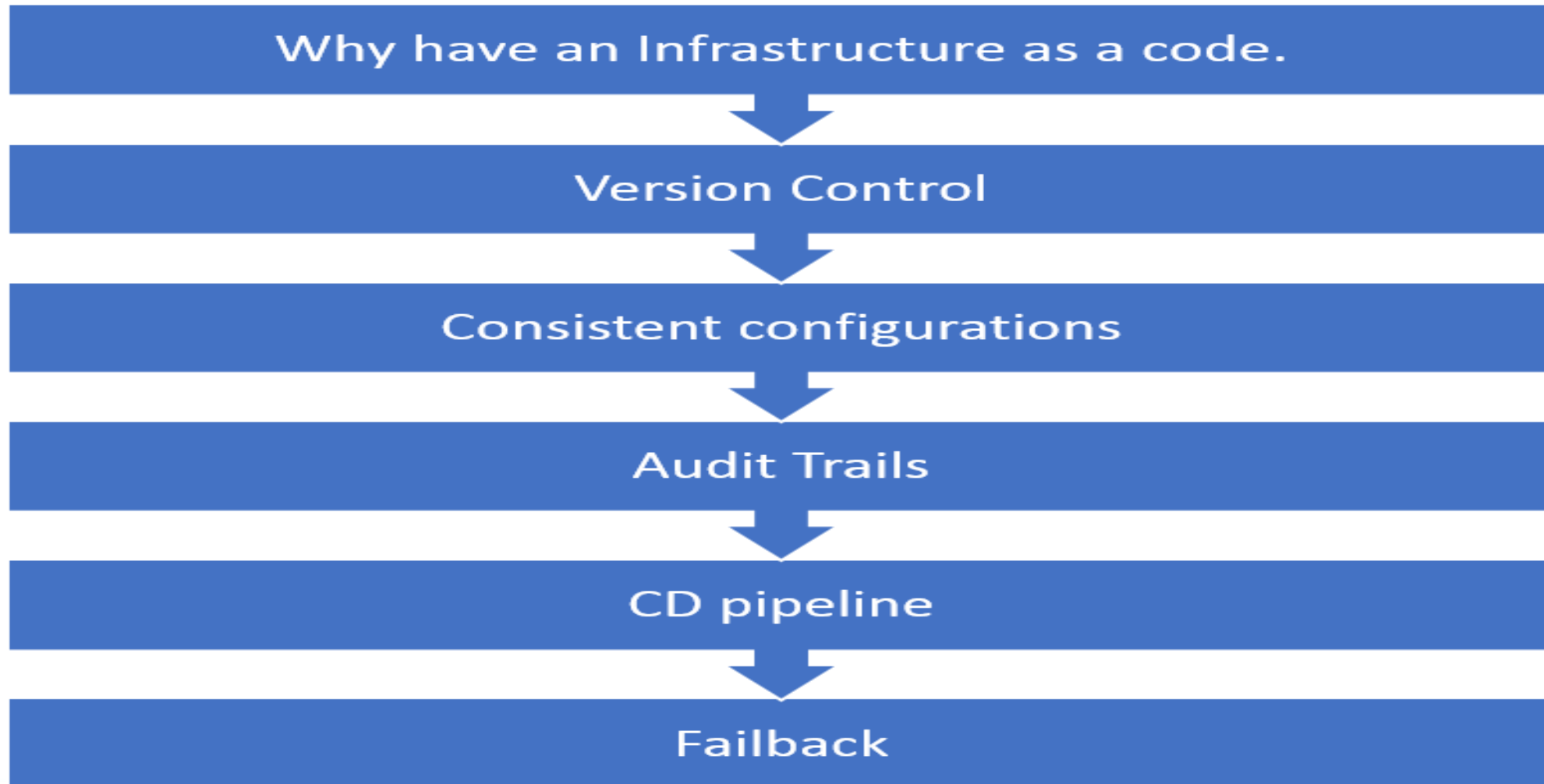


GCDS is a secure tool that help keep track of users and groups.

# Infrastructure as Code

Google Cloud Architect Exam Bootcamp

# GCP Networking Fundamentals



# GCP Networking Fundamentals

Deploying infrastructure

	AWS	GCP
Infrastructure Tool	CloudFormation	Deployment Manager
Resources	Stack	Files, templates and schemas
Syntax	JSON, YAML	YAML, Jinja, Python
Reuse	Nested Stacks	Templates
Scope	Regional	Global

# GCP Networking Fundamentals

## ***Deployment Manager***

- Deployment Manager is an infrastructure deployment service that automates the creation and management of Google Cloud Platform resources for you.
- Declarative format (Schema Files)– yaml
- Python or Jinja2(Templates)

<https://cloud.google.com/deployment-manager/>

# GCP Networking Fundamentals

## ***Cloud Marketplace***

- Cloud Launcher has been rebranded to Cloud Marketplace
- Same purpose as AWS Marketplace
- Allows you to deploy ready made templates from GCP and partners.

# GCP Certifications

Google Cloud Architect Exam Bootcamp

# GCP Cloud Architect Overview

Google has a growing portfolio of Cloud Certifications.

- Associate Cloud Engineer
- Professional Cloud Architect
- Professional Data Engineer
- Professional Cloud Developer
- G Suite Certs (2)
- Professional Cloud Network Engineer
- Professional Cloud Security Engineer



Certification Page

<https://cloud.google.com/certification/>



# Course Closeout

Google Cloud Architect Exam Bootcamp

# Resources

- Google Cloud Platform <https://cloud.google.com/>
- GCP Console <https://console.cloud.google.com/>
- GCP Storage <https://cloud.google.com/products/storage/>
- Documentation <https://cloud.google.com/docs/>
- Pricing <https://cloud.google.com/pricing/>
- Free Tier <https://cloud.google.com/free/>
- Code Labs <https://codelabs.developers.google.com/>
- Qwiklabs <https://qwiklabs.com/dashboard>
- Stackoverflow <https://stackoverflow.com/>

# Resources

- Google Site Reliability Book

<https://landing.google.com/sre/book/index.html> (Ebook)

<https://www.safaribooksonline.com/library/view/the-site-reliability/9781492029496/> (Ebook)

- <https://amzn.to/2JDDJ6p> (Amazon)

- GCP Diagram Templates

<https://cloud.google.com/icons/>

- GCP to AWS Services

<https://cloud.google.com/free/docs/map-aws-google-cloud-platform>

# Resources

- Kinsta Blogpost

<https://kinsta.com/blog/google-cloud-hosting/>

- Rightscale Pricing Comparison

<https://www.rightscale.com/blog/cloud-cost-analysis/aws-reserved-instances-vs-google-committed-use-discounts>

# Thank you

Thank you for Joining

- I wish you luck on learning more about the Google Cloud Platform

Connecting

Feel free to connect with me

- LinkedIn
- Youtube
- Steemit
- Myblockchainexperts.net

A large, stylized graphic of the words 'thank you!' in a lowercase, rounded font. The letters are filled with a vibrant rainbow gradient, transitioning from yellow on the left, through green, blue, red, and orange, to a bright yellow on the right. The exclamation mark is also filled with the same gradient. The text is set against a white background.