# Google Cloud Professional Cloud Network Engineer

## Introduction

A Professional Cloud Network Engineer implements and manages network architectures in the Google Cloud Platform. This individual has at least 1 year of hands-on experience working with Google Cloud Platform and may work on networking or cloud teams with architects who design the infrastructure. By leveraging experience implementing VPCs, hybrid connectivity, network services, and security for established network architectures, this individual ensures successful cloud implementations using the command line interface or the Google Cloud Platform Console.

The Professional Cloud Network Engineer exam assesses your ability to:

- Design, plan, and prototype a GCP Network
- Implement a GCP Virtual Private Cloud (VPC)
- Configure network services

## Course Objective

- Designing, planning, and prototyping a GCP network
- Implementing a GCP Virtual Private Cloud (VPC)
- Configuring network services
- Implementing hybrid interconnectivity
- Implementing network security
- Managing and monitoring network operations
- Optimizing network resources

## Course Outline

**1. Designing, planning, and prototyping a GCP network**

1.1 Designing the overall network architecture. Considerations include:

- Failover and disaster recovery strategy
- Options for high availability
- DNS strategy (e.g., on-premises, Cloud DNS, GSLB)
- Meeting business requirements
- Choosing the appropriate load balancing options
- Optimizing for latency (e.g., MTU size, caches, CDN)
- Understanding how quotas are applied per project and per VPC
- Hybrid connectivity (e.g., Google private access for hybrid connectivity)
- Container networking
- IAM and security
- SaaS, PaaS, and IaaS services
- Micro-segmentation for security purposes (e.g., using metadata, tags)

1.2 Designing a Virtual Private Cloud (VPC). Considerations include:

- CIDR range for subnets
- IP addressing (e.g., static, ephemeral, private)
- Standalone or shared
- Multiple vs. single
- Multi-zone and multi-region

- Peering
- Firewall (e.g., serviceaccount-based, tag-based)
- Routes
- Differences between Google Cloud Networking and other cloud platforms

1.3 Designing a hybrid network. Considerations include:

- Using interconnect (e.g., dedicated vs. partner)
- Peering options (e.g., direct vs. carrier)
- IPsec VPN
- Cloud Router
- Failover and disaster recovery strategy (e.g., building high availability with BGP using cloud router)
- Shared vs. standalone VPC interconnect access
- Cross-organizational access
- Bandwidth

1.4 Designing a container IP addressing plan for Google Kubernetes Engine

**2. Implementing a GCP Virtual Private Cloud (VPC)**

2.1 Configuring VPCs. Considerations include:

- Configuring GCP VPC resources (CIDR range, subnets, firewall rules, etc.)
- Configuring VPC peering
- Creating a shared VPC and explaining how to share subnets with other projects
- Configuring API access (private, public, NAT GW, proxy)
- Configuring VPC flow logs

2.2 Configuring routing. Tasks include:

- Configuring internal static/dynamic routing
- Configuring routing policies using tags and priority
- Configuring NAT (e.g., Cloud NAT, instance-based NAT)

2.3 Configuring and maintaining Google Kubernetes Engine clusters. Considerations include:

- VPC-native clusters using alias IPs
- Clusters with shared VPC
- Private clusters
- Cluster network policy
- Adding authorized networks for cluster master access

2.4 Configuring and managing firewall rules. Considerations include:

- Target network tags and service accounts
- Priority
- Network protocols
- Ingress and egress rules
- Firewall logs

**3. Configuring network services**

3.1 Configuring load balancing. Considerations include:

- Creating backend services
- Firewall and security rules
- HTTP(S) load balancer: including changing URL maps, backend groups, health checks, CDN, and SSL certs
- TCP and SSL proxy load balancers
- Network load balancer
- Internal load balancer
- Session affinity
- Capacity scaling

3.2 Configuring Cloud CDN. Considerations include:

- Enabling and disabling Cloud CDN
- Using cache keys
- Cache invalidation
- Signed URLs

3.3 Configuring and maintaining Cloud DNS. Considerations include:

- Managing zones and records
- Migrating to Cloud DNS
- DNS Security (DNSSEC)
- Global serving with Anycast
- Cloud DNS
- Internal DNS
- Integrating on-premises DNS with GCP

3.4 Enabling other network services. Considerations include:

- Health checks for your instance groups
- Canary (A/B) releases
- Distributing backend instances using regional managed instance groups
- Enabling private API access

**4. Implementing hybrid interconnectivity**

4.1 Configuring interconnect. Considerations include:

- Partner (e.g., layer 2 vs. layer 3 connectivity)
- Virtualizing using VLAN attachments
- Bulk storage uploads

4.2 Configuring a site-to-site IPsec VPN (e.g., route-based, policy-based, dynamic, or static routing).

4.3 Configuring Cloud Router for reliability.

**5. Implementing network security**

5.1 Configuring identity and access management (IAM). Tasks include:

- Viewing account IAM assignments
- Assigning IAM roles to accounts or Google Groups
- Defining custom IAM roles
- Using pre-defined IAM roles (e.g., network admin, network viewer, network user)

5.2 Configuring Cloud Armor policies. Considerations include:

IP-based access control

5.3 Configuring third-party device insertion into VPC using multi-mic (NGFW)

5.4 Managing keys for SSH access

**6. Managing and monitoring network operations**

6.1 Logging and monitoring with Stackdriver or GCP Console

6.2 Managing and maintaining security. Considerations include:

- Firewalls (e.g., cloud-based, private)
- Diagnosing and resolving IAM issues (shared VPC, security/network admin)

6.3 Maintaining and troubleshooting connectivity issues. Considerations include:

- Identifying traffic flow topology (e.g., load balancers, SSL offload, network endpoint groups)

- Draining and redirecting traffic flows
- Cross-connect handoff for interconnecting
- Monitoring ingress and egress traffic using flow logs

- Monitoring firewall logs
- Managing and troubleshooting VPNs
- Troubleshooting Cloud Router BGP peering issues

6.4 Monitoring, maintaining, and troubleshooting latency and traffic flow. Considerations include:

- Network throughput and latency testing
- Routing issues
- Tracing traffic flow

**7. Optimizing network resources**

7.1 Optimizing traffic flow. Considerations include:

- The load balancer and CDN location
- Global vs. regional dynamic routing
- Expanding subnet CIDR ranges in service
- Accommodating workload increases (e.g., autoscaling vs. manual scaling)

7.2 Optimizing for cost and efficiency. Considerations include:

- Cost optimization (Network Service Tiers, Cloud CDN, autoscaler [max instances])
- Automation
- VPN vs. interconnect
- Bandwidth utilization (e.g., kernel sys tuning parameters)

## Prerequisites

Basic understanding of cloud concepts such as virtual machines, containers, and networking

## Recommended Experience

3+ years of industry experience including 1+ years designing and managing solutions using GCP.

## Target Audience

- Software developers who want to build versatile applications on Google Cloud Platform
- People preparing for the Google Cloud Network Engineering exam
- Software Engineers
- Network Engineers
- Routing and Switch Administrators
- Backend Administrators

## Duration

3 days training course