Introduction, Course Objective

A Professional Cloud Network Engineer implements and manages network architectures in Google Cloud. This individual may work on networking or cloud teams with architects who design cloud infrastructure. The Cloud Network Engineer uses the Google Cloud Console and/or command line interface, and leverages experience with network services, application and container networking, hybrid and multi-cloud connectivity, implementing VPCs, and security for established network architectures to ensure successful cloud implementations.

The Professional Cloud Network Engineer exam assesses your ability to:
Design, plan, and prototype a Google Cloud network
Implement Virtual Private Cloud (VPC) instances
Configure network services
Implement hybrid interconnectivity
Manage, monitor, and optimize network operations

Target Audience

IT Infrastructure Engineer/Admin
IT Professionals
Cloud Network Engineer
Google Cloud Platform Network Engineer
Network Professional
Network Support Engineer
Network Admin
System Engineer
GCP Product Pre-sales engineer

Course Pre-Requisites

- Basic Cloud Computing Knowledge
- Basic Networking related experience
- Network infrastructure management
- System server related experience.
- Computer Networking Components
- OSI References Model
- TCP/IP Protocols
- IP Addressing, VLSM
- VPN, VPC, Load balancer,
- Firewall, NAT

Professional Cloud Network Engineer

Class No	Module Details	Duration
Module Name: Designing, planning, and prototyping a Google Cloud network		
01	• Virtualization and Cloud Computing Concept • GCP resource Hierarchy • Zone, Region concept • Networking concept • System Administration concept • Linux OS concept Lab: Virtulalbox, GCP Resource Hierarchy	2 Hours
02	• Cloud Identity • Designing an overall network architecture. • High availability, failover, and disaster recovery strategies • DNS strategy (e.g., on-premises, Cloud DNS) • Security and data exfiltration requirements Lab: Cloud identity	2 Hours
03	• IP addressing (VLSM subnetting) • Load balancing concept • Applying quotas per project and per VPC • Hybrid connectivity concept (e.g., Google private access for hybrid connectivity) Lab: Subnetting and LB	2 Hours
04	• IAM (Identity & Access Management) • Container networking concept • SaaS, PaaS, and IaaS services concept • Micro segmentation for security purposes (e.g., using metadata, tags, service accounts) Lab: IAM, Project Quota	2 Hours
Module Name: Designing Virtual Private Cloud (VPC) instances		
05	• IP address management and bring your own IP (BYOIP) • Standalone vs. Shared VPC • Multiple vs. single, Regional vs. multi-regional • VPC Network Peering Lab: VPC	2 Hours
06	• Firewalls (e.g., service account-based, tag-based)	2 Hours

	• Custom routes • Using managed services (e.g., Cloud SQL, Memorystore) • Third-party device insertion (NGFW) into VPC using multi-NIC and internal load balancer as a next hop or equal-cost multi-path (ECMP) routes Lab: Firewall	
Module Name: Designing a hybrid and multi-cloud network		
07	• Dedicated Interconnect vs. Partner Interconnect • Multi-cloud connectivity • Direct Peering • IPsec VPN • Failover and disaster recovery strategy • Regional vs. global VPC routing mode Lab: Hybrid Connectivity	2 Hours
08	• Accessing multiple VPCs from on-premises locations (e.g., Shared VPC, multi-VPC peering topologies) • Bandwidth and constraints provided by hybrid connectivity solutions • Accessing Google Services/APIs privately from on-premises locations • IP address management across on-premises locations and cloud • DNS peering and forwarding Lab: Hybrid Connectivity	2 Hours
Module Name: Designing an IP addressing plan for Google Kubernetes Engine		
09	• GKE • Public and private cluster nodes concept • Control plane public vs. private endpoints concept • Subnets and alias IPs for GKE • RFC 1918, non-RFC 1918, & privately used public IP (PUPI) address options Lab: GKE	2 Hours
Module Name: Implementing Virtual Private Cloud (VPC) instances		
10	• Google Cloud VPC resources (instance and other services) (e.g., networks, subnets, firewall rules) • VPC Network Peering • Creating a Shared VPC network and sharing subnets with other projects Lab: VPC Resources	2 Hours

11	• Configuring API access to Google services (e.g., Private Google Access, public interfaces) • Expanding VPC subnet ranges after creation • Static vs. dynamic routing • Global vs. regional dynamic routing • Routing policies using tags and priority • Internal load balancer as a next hop • Custom route import/export over VPC Network Peering Lab: Routing	2 Hours
12	• Configuring and maintaining Google Kubernetes Engine clusters. Considerations include: • VPC-native clusters using alias IPs • Clusters with Shared VPC • Creating Kubernetes Network Policies • Private clusters and private control plane endpoints • Adding authorized networks for cluster control plane endpoints • Configuring and managing firewall rules. Considerations include: • Target network tags and service accounts • Rule priority • Network protocols • Ingress and egress rules • Firewall rule logging • Firewall Insights • Hierarchical firewalls Lab: VPC and Firewall	2 Hours
13	• Implementing VPC Service Controls. Considerations include: • Creating and configuring access levels and service perimeters • VPC accessible services • Perimeter bridges • Audit logging • Dry run mode Lab: VPC Service Controls	2 Hours
	Module Name: Configuring network services	
14	• Configuring load balancing. Considerations include: • Backend services and network endpoint groups (NEGs) • Firewall rules to allow traffic and health checks to backend services • Health checks for backend services and target instance groups • Configuring backends and backend services with balancing method (e.g., RPS, CPU, Custom), session affinity, and capacity scaling/scaler Lab: Load Balancer	2 Hours

15	• TCP and SSL proxy load balancers • Load balancers (e.g., External TCP/UDP Network Load Balancing, Internal TCP/UDP Load Balancing, External HTTP(S) Load Balancing, Internal HTTP(S) Load Balancing) • Protocol forwarding • Accommodating workload increases using autoscaling vs. manual scaling Lab: Load Balancer	2 Hours
16	• Configuring Google Cloud Armor policies. Considerations include: • Security policies • Web application firewall (WAF) rules (e.g., SQL injection, cross-site scripting, remote file inclusion) • Attaching security policies to load balancer backends • Configuring Cloud CDN. Considerations include: • Enabling and disabling • Cloud CDN • Cache keysInvalidating cached objects • Signed URLs • Custom origins Lab: WAF and CDN	2 Hours
17	• Configuring and maintaining Cloud DNS. Considerations include: • Managing zones and records • Migrating to Cloud DNS • DNS Security Extensions (DNSSEC) • Forwarding and DNS server policies • Integrating on-premises DNS with Google Cloud • Split-horizon DNS • DNS peering • Private DNS logging Lab: DNS	2 Hours
18	• Configuring Cloud NAT. Considerations include: • Addressing, Port allocations • Customizing timeouts, Logging and monitoring • Restrictions per organization policy constraints • Configuring network packet inspection. Considerations include: • Packet Mirroring in single and multi-VPC topologies • Capturing relevant traffic using Packet Mirroring source and traffic filters • Routing and inspecting inter-VPC traffic using multi-NIC VMs (e.g., next-generation firewall appliances) • Configuring an internal load balancer as a next hop for highly available multi-NIC VM routing • Lab: NAT	2 Hours

	Module Name: Implementing hybrid interconnectivity	
19	• Configuring Cloud Interconnect. Considerations include: • Dedicated Interconnect connections and VLAN attachments • Partner Interconnect connections and VLAN attachments • Configuring a site-to-site IPsec VPN. Considerations include: • High availability VPN (dynamic routing) • Classic VPN (e.g., route-based routing, policy-based routing) • Configuring Cloud Router. Considerations include: • Border Gateway Protocol (BGP) attributes (e.g., ASN, route priority/MED, link-local addresses) • Custom route advertisements via BGP • Deploying reliable and redundant Cloud Routers • Lab: VLAN, BGP, VPN	2 Hours
	Module Name: Managing, monitoring, and optimizing network operations	
20	• Logging and monitoring with Google Cloud's operations suite. Considerations include: • Reviewing logs for networking components (e.g., VPN, Cloud Router, VPC Service Controls) • Monitoring networking components (e.g., VPN, Cloud Interconnect connections and interconnect attachments, Cloud Router, load balancers, Google Cloud Armor, Cloud NAT) • Managing and maintaining security. Considerations include: • Firewalls (e.g., cloud-based, private) • Diagnosing and resolving IAM issues (e.g., Shared VPC, security/network admin) • Lab: Monitoring and Troubleshooting	2 Hours
21	• Maintaining and troubleshooting connectivity issues. • Draining and redirecting traffic flows with HTTP(S) Load Balancing • Monitoring ingress and egress traffic using VPC Flow Logs • Monitoring firewall logs and Firewall Insights • Managing and troubleshooting VPNs • Troubleshooting Cloud Router BGP peering issues • Monitoring, maintaining, and troubleshooting latency and traffic flow. Considerations include: • Testing network throughput and latency, Diagnosing routing issues • Using Network Intelligence Center to visualize topology, test connectivity, and monitor performance Lab: Troubleshooting	2 Hours
22	Summary with Exam preparation Tips	1 Hour
	Total Course Length	43 Hours