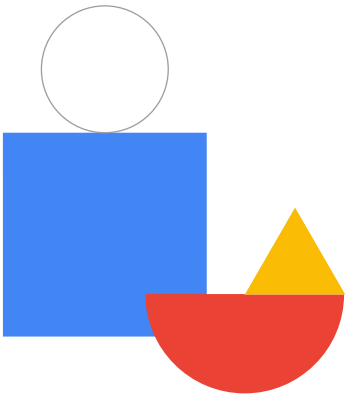
Google Cloud

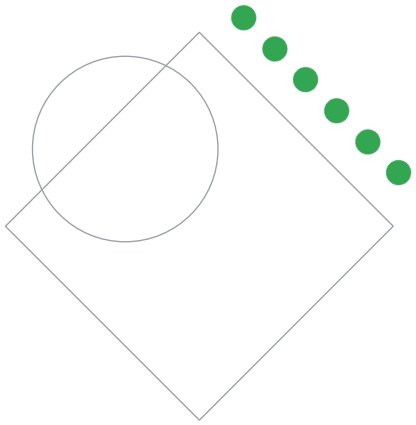


Preparing for Your Professional Cloud Network Engineer Journey

Module 1: Designing and planning a Google Cloud network

Welcome to Module 1: Designing and planning a Google Cloud Network.

Review and study planning

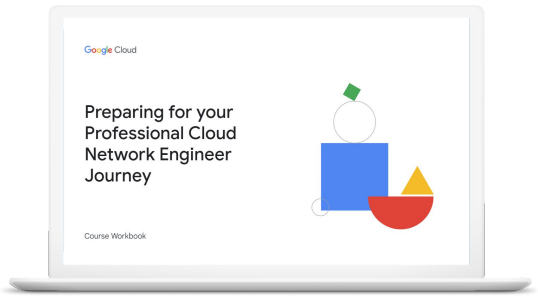


Google Cloud

You'll now review the diagnostic questions and your answers to help you identify what to include in your study plan.

Your study plan:

Designing and planning a Google Cloud network



1.1	Designing an overall network architecture
1.2	Designing Virtual Private Cloud (VPC) networks
1.3	Designing a resilient and performant hybrid and multi-cloud network
1.4	Designing an IP addressing plan for Google Kubernetes Engine

Google Cloud

The diagnostic questions align with these objectives of this exam section. Use the PDF resource that follows to review the questions and how you answered them. Pay specific attention to the rationale for both the correct and incorrect answers. Use the resources detailed under **Where to look** and **Content mapping** to build a study plan that meets your learning needs.

1.1 Designing an overall network architecture (1)

Considerations include:

- Designing for high availability, failover, disaster recovery, and scale
- Designing the DNS topology (e.g., on-premises, Cloud DNS)
- Designing for security and data exfiltration prevention requirements
- Choosing a load balancer for an application
- Designing for hybrid connectivity (e.g., Private Google Access for hybrid connectivity)
- Planning for Google Kubernetes Engine (GKE) networking (e.g., secondary ranges, scale potential based on IP address space, access to GKE control plane)
- Planning Identity and Access Management (IAM) roles including managing IAM roles in a Shared VPC environment

Google Cloud

A Professional Cloud Network Engineer should start the Google Cloud network infrastructure design process with a high-level analysis and plan for the network infrastructure. Some general considerations are listed on the slide, such as high availability, failover, and disaster recovery strategy, DNS strategy, load balancing, etc.

Questions 1 through 3 in this section covered networking fundamentals, using IAM to control access to network resources, and being able to identify networking features in Google Cloud.

To answer these questions, you should be comfortable with all of the considerations listed on this slide and the next.

1.1 Designing an overall network architecture (2)

Considerations include:

- Incorporating micro segmentation for security purposes (e.g., using metadata, tags, service accounts, secure tags)
- Planning for connectivity to managed services (e.g., private services access, Private Service Connect, Serverless VPC Access)
- Differentiating between network tiers (e.g., Premium and Standard)
- Designing for VPC Service Controls

1.1 Diagnostic Question 01 Discussion

You are a network engineer designing a network IP plan and need to select an IP address range to use for a subnet. The subnet will need to host up to 2000 virtual machines, each to be assigned one IP address from the subnet range. It will also need to fit in the network IP range 10.1.0.0/16 and be as small as possible.

What subnet range should you use?

A. 10.1.1.0/24
B. 10.1.240.0/21
C. 10.1.1.0/21
D. 10.1.240.0/20

Google Cloud

Feedback:
A: Incorrect. This range would have a maximum of 255 IP addresses and could not support 2000 virtual machines each having one IP address
*B: Correct! This range will satisfy the requirements. It has 2040 IP addresses and can therefore host 2000 virtual machines with one IP address per machine. It is the smallest range that could host this number of VMs, and it fits within the network range of 10.1.0.0/16
C: Incorrect. This range is invalid; the 3rd byte of the range mask occupies the range.
D: Incorrect. This range has 4080 IP addresses. However, 10.1.240.0/21 can host up to 2040 IP addresses and is therefore a better fit.

Where to look:
Public learning resources such as *The Bits and Bytes of Computer Networking* (https://www.coursera.org/learn/computer-networking)

Summary:
There are networking fundamentals that are common to all environments, cloud or otherwise. A network engineer should have familiarity with such networking fundamentals. For example, a network engineer should be able to select subnet ranges that satisfy requirements such as available IP addresses for assignment and prevent overlap.

1.1 Diagnostic Question 02 Discussion

Cymbal Bank has a network support engineering team which will need access to create or change subnet names, locations, and IP address ranges for some but not all subnetworks of a VPC network in a Google Cloud project. Cymbal Bank uses the principle of least privilege and would like to restrict role usage to Google predefined roles.

Which role should be assigned to this group?

A. The Compute Admin role bound at the project level for the project that owns the VPC network

B. The Compute Network Admin role bound at the project level for the Project that owns the VPC network

C. The Compute Network Admin role bound at the resource level for the subnetworks of the VPC network that will be created or changed by the team

D. The Compute Admin role bound at the resource level for the subnetworks of the VPC network that will be created or changed by the team

Feedback:
A: Incorrect. The Compute Admin role has many extra permissions beyond what is required. Assigning the role at the project level will provide access to all VPC networks and subnetworks. They only need access to some subnetworks of a specific VPC network.
B: Incorrect. Assigning the role at the Project level will provide access to all VPC networks and subnetworks. They only need access to some subnetworks of a specific VPC network.
*C: Correct! The Compute Network Admin role is the minimum predefined role that provides the necessary permissions. Assigning it for just the applicable subnetworks rather than at the project level ensures that it will only apply to those subnetworks - and not all VPC networks and subnetworks in the project.
D: Incorrect. This is incorrect, binding the role at resource level is correct but the Compute Admin role has many extra permissions beyond what is required.

Where to look:
https://cloud.google.com/compute/docs/access/iam#predefinedroles

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M9 Controlling Access to VPC Networks

- On-demand course: **Networking in Google Cloud: Network Security**
  - M2 Controlling Access to VPC Networks

Summary:
There are many predefined Compute Engine roles available in Google Cloud that provide differing levels of access to networking resources. Most roles can be bound at the Organization, Folder, or Project level, and some roles can also be bound at the Resource level. The principles of least privilege and separation of duties should be followed when designing access control policies.

1.1 Diagnostic Question 03 Discussion

You are a network engineer designing a solution for hosting a Cymbal Bank web application in Google Cloud. The application will serve a collection of static and dynamic web resources served over HTTPS to users worldwide. You need to design a solution that maximizes availability while minimizing average user latency.

Which of the following features of Google Cloud networking can you utilize? (Select 2)

A. **Cloud CDN could be used to cache static content resources at edge locations close to end-users, increasing their availability and minimizing their latency.**

B. Cloud NAT could be used to provide outbound connectivity to the internet for resources with only internal IP addresses, thereby increasing their availability.

C. Google Cloud Armor could be used to provide protection against DDoS and injection attacks and thereby minimize solution latency.

D. **An Application Load Balancer with a backend service connected to a set of regional MIGs, distributed over the regions closest to the users, to improve availability and minimize latency.**

E. Network Intelligence Center could be used to provide network insights, enabling the web application to be deployed in a configuration with maximum availability and minimal latency.

Feedback:
*A: Correct! Cloud CDN can be used to cache static content at edge locations. This would help maximize the availability and minimize the average latency for end users accessing those resources.
B: Incorrect. Cloud NAT can be used to provide outbound connectivity to the internet for resources with only internal IP addresses, but this does nothing to increase availability or minimize latency for end users interacting with those resources.
C: Incorrect. Google Cloud Armor can be used to provide protection against DDoS and injection attacks. This can improve solution availability in the presence of such attacks but does nothing to minimize average user latency.
*D: Correct! Using an Application Load Balancer with a backend service connected to a set of regional MIGs distributed over the regions closest to the users would ensure high availability and minimal average user latency for serving dynamic web resources.
E: Incorrect. The Network Intelligence Center has features that can be used to troubleshoot network connectivity and performance issues, but this would be of limited applicability in designing a networking solution for high availability and low latency.

Where to look:
https://cloud.google.com/cdn/docs/overview
https://cloud.google.com/nat/docs/overview
https://cloud.google.com/load-balancing/docs/load-balancing-overview
https://cloud.google.com/armor/docs/cloud-armor-overview
https://cloud.google.com/network-intelligence-center/docs

Content mapping:

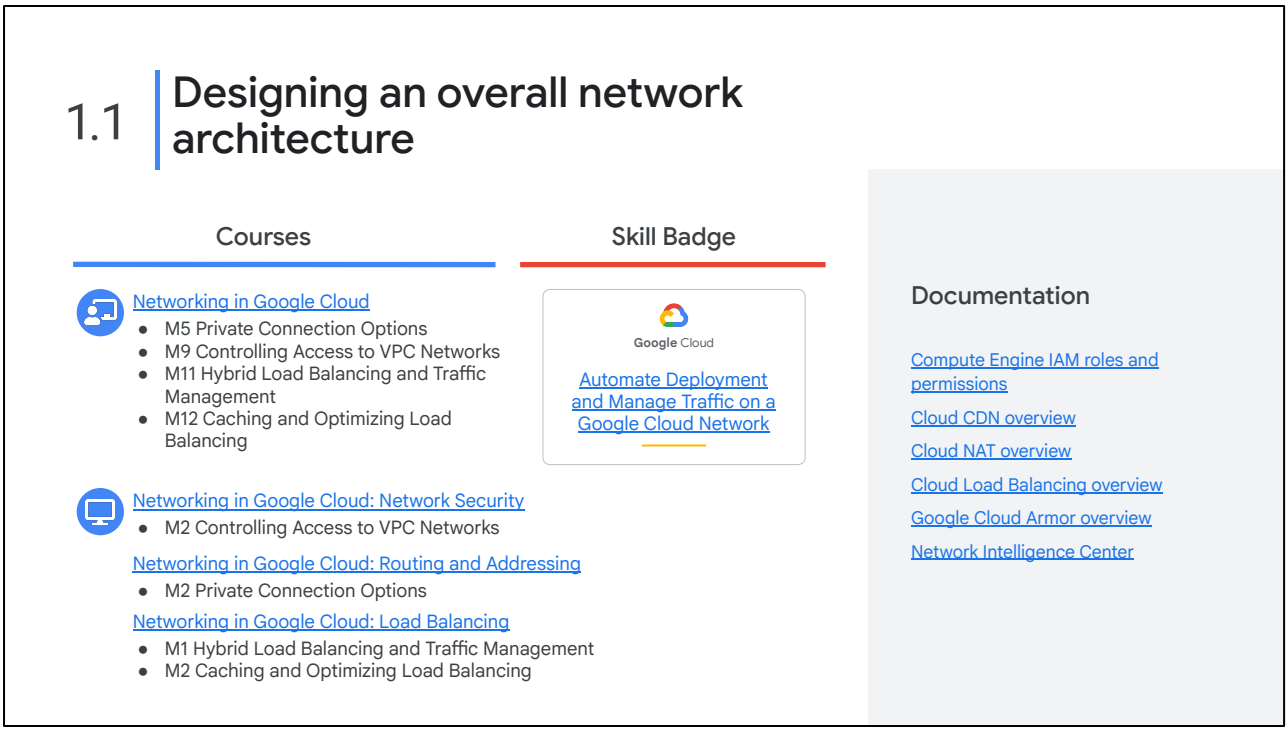
- ILT course: **Networking in Google Cloud**
  - M5 Private Connection Options
  - M11 Hybrid Load Balancing and Traffic Management
  - M12 Caching and Optimizing Load Balancing

- On-demand course: **Networking in Google Cloud: Routing and Addressing**
  - M2 Private Connection Options

- On-demand course: **Networking in Google Cloud: Load Balancing**
  - M1 Hybrid Load Balancing and Traffic Management
  - M2 Caching and Optimizing Load Balancing

- Skill badge: Automate Deployment and Manage Traffic on a Google Cloud Network

Summary:
Google Cloud provides many networking features. Cloud CDN is a content delivery network that caches static resources at Google edge locations around the world. It serves these resources to a large user base with maximal availability and minimal latency. Cloud NAT provides network address translation that enables private/internal IP-only resources to make secure requests to the internet. Google Cloud Armor is a web-application firewall (WAF) providing traffic scanning and filtering.It provides configurable protection against attack traffic including distributed denial of service (DDoS). Cloud Load Balancing provides managed software load balancing in many varieties including full global anycast load balancing to enable delivery traffic to the nearest regional backends using a single IP address. Network Intelligence Center provides several modules, including Network Topology, Connectivity Tests, Performance Dashboard, Firewall Insights, Network Analyzer, and Flow Analyzer. These modules aid in network troubleshooting and performance debugging.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Network Security (On-demand)
Networking in Google Cloud: Routing and Addressing (On-demand)
Networking in Google Cloud: Load Balancing (On-demand)

Automate Deployment and Manage Traffic on a Google Cloud Network (Skill Badge)

https://cloud.google.com/compute/docs/access/iam#predefinedroles
https://cloud.google.com/cdn/docs/overview
https://cloud.google.com/nat/docs/overview
https://cloud.google.com/load-balancing/docs/load-balancing-overview
https://cloud.google.com/armor/docs/cloud-armor-overview
https://cloud.google.com/network-intelligence-center/docs

1.2 Designing Virtual Private Cloud (VPC) networks

Considerations include:

- Choosing the VPC type and quantity (e.g., standalone or Shared VPC, number of VPC environments)
- Determining how the networks connect based on requirements (e.g., VPC Network Peering, VPC Network Peering with Network Connectivity Center, Private Service Connect)
- Planning the IP address management strategy (e.g., subnets, IPv6, bring your own IP (public advertised prefix (PAP) and public delegated prefix (PDP)), Private NAT, non-RFC 1918, managed services)
- Planning for a global or regional network environment
- Planning the firewall strategy (e.g., VPC firewall rules, Cloud Next Generation Firewall, hierarchical firewall rules)
- Planning custom routes (static or policy-based) for third-party device insertion (e.g., network virtual appliance)

Google Cloud

A Professional Network Engineer begins the design and implementation of the Google Cloud networking infrastructure with the VPC(s).

In this section, question 4 covered a general knowledge of Google Cloud VPCs. Question 5 covered VPC connections - to each other and from external networks. Question 6 covered network considerations pertaining to location - such as availability, latency, regions, and zones.

To answer these questions, you should be comfortable with all of the considerations listed on the slide.

1.2 Diagnostic Question 04 Discussion

Cymbal Bank needs to create one or more VPC networks to host their cloud services in 3 regions: Northeastern US, Western Europe, and Southeast Asia. The services require bi-directional inter-regional communication on port 8443. The services receive external internet traffic on port 443.

What is the minimal network topology in Google Cloud that would satisfy these requirements?

A. 3 custom VPC networks, one in each region with one subnet each. The VPC networks all connected with VPC peering with default firewall rules, and custom routes added to support the traffic requirements.

B. 3 custom VPC networks, one in each region with one subnet each. The VPC networks all connected with VPC peering with default routes, and firewall rules added to support the traffic requirements.

C. 1 custom VPC network, with a subnet in each region. The VPC network has the default routes, and the appropriate firewall rules added to support the traffic requirements.

D. 1 custom VPC network, with a subnet in each region. The VPC network has default firewall rules and custom routes added to support the traffic requirements.

Feedback:
A: Incorrect. A single VPC network with 3 subnets is the minimal topology to satisfy these requirements.
B: Incorrect. A single VPC network with 3 subnets is the minimal topology to satisfy these requirements.
*C: Correct! This is the correct minimal topology satisfying the requirements.
D: Incorrect. The traffic requirements can be satisfied with the default routes but would require additional firewall rules.

Where to look:
https://cloud.google.com/vpc/docs/vpc
https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/routes

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M6 Introduction to Network Architecture
  - M7 Network Topologies

- On-demand course: **Networking in Google Cloud: Network Architecture**
  - M1 Introduction to Network Architecture
  - M2 Network Topologies

- Skill badge: Automate Deployment and Manage Traffic on a Google Cloud

- Network

Summary:
VPC networks are global resources in Google Cloud and contain regional subnetworks. Auto VPC networks will have at least one subnet in each Google Cloud region. Custom VPC networks can have subnetworks in only desired regions. Each subnetwork will have at least one primary subnet range and none of the primary or secondary subnet ranges can overlap in a single VPC. Each VPC network has a set of default routes routing the subnet IP ranges of each subnet to that subnet and a route for all other IP addresses to the internet. Other custom routes can also be added. Firewall rules are the primary mechanism for traffic control and can be used to allow or deny traffic matching the configured rule parameters. Firewall rules are evaluated in priority order. The two implicit firewall rules in every VPC - implicit deny all ingress and allow all egress rules- have the lowest priority.

1.2 Diagnostic Question 05 Discussion

Sarah is a network architect responsible for the network design between Cymbal Bank's on-premises network and Google Cloud resources, and also between Cymbal Bank's Google Cloud resources and a partner company's Google Cloud resources. These connections must provide private IP connectivity and support up to 100 Gbps of data exchange with minimum possible latency.

Which options satisfy these requirements? (Select 2)

A. A Shared VPC network connecting Google Cloud resources for Cymbal Bank and the partner company

B. VPC peering between VPC networks for Cymbal Bank and the partner company

C. A Dedicated Interconnect connection between Cymbal Bank's on-premises network and their Google Cloud VPC network

D. A Cloud VPN tunnel between Cymbal Bank's on-premises network and their Google Cloud VPC network

E. 50 Cloud VPN tunnels between Cymbal Bank's on-premises network and their Google Cloud VPC network

Google Cloud

Feedback:
A: Incorrect. A Shared VPC network cannot be used to connect resources across separate organizations.
*B: Correct!. VPC peering allows for private IP connectivity between Google Cloud resources across organizations and is the lowest latency and highest bandwidth option for such connectivity
*C: Correct! Dedicated Interconnect provides private IP connectivity with bandwidths ranging from 10-200 Gbps per interconnect link and has the lowest possible latency.
D: Incorrect. Cloud VPN maximum bandwidth is 3 Gps per tunnel, which is considerably less than the 100 Gbps that is required. Also Cloud VPN has significantly more latency than Cloud Interconnect and Dedicated Interconnect.
E. Incorrect. Cloud VPN maximum bandwidth is 3 Gps per tunnel, 50 tunnels would provide more than the 100 Gbps that is required. However Cloud VPN has significantly more latency than Cloud Interconnect and Dedicated Interconnect.

Where to look:
https://cloud.google.com/vpc/docs/shared-vpc
https://cloud.google.com/vpc/docs/vpc-peering
https://cloud.google.com/network-connectivity/docs/how-to/choose-product

Content mapping:
- ILT course: **Networking in Google Cloud**
  - M2 Sharing VPC Networks
  - M13 Connectivity Options

- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M2 Sharing VPC Networks

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
  - M1 Connectivity Options

Summary:
There are 2 main approaches to connecting resources using private/internal IP communication across projects or VPC networks in Google Cloud. Shared VPC provides a centralized networking model. VPC peering provides a decentralized model. Shared VPC allows resources from multiple projects to be placed in a common VPC network owned by a host project. VPC peering allows VPC networks to be connected within or across projects, or even across organizations.

There are 3 main approaches to connecting resources using private/internal IP communication between on-premises and cloud environments in Google Cloud. Dedicated Interconnect provides the highest bandwidth and lowest latencies, but requires connectivity to and installing a router in a Google Cloud colocation facility. Partner Interconnect provides a variety of sub-10gbps bandwidth options for customers who do not need the full 10 or 100gbps that Dedicated Interconnect provides, and allows meeting Google Cloud Partners in many more locations around the world. Cloud VPN typically provides for lower bandwidths and higher latency, but is relatively inexpensive and quick to set up.

1.2 Diagnostic Question 06 Discussion

You are selecting Google Cloud locations to deploy Google Cloud VMs. You have general requirements to maximize availability and reduce average user latency with a lower priority goal of reducing networking costs. The users served by these VMs will be in Toronto and Montreal. You must deploy workloads requiring instances at 99.5% availability in Toronto and 99.99% availability in Montreal. These instances all exchange a large amount of traffic among themselves.

Which deployment option satisfies these requirements?

A. Deploy instances in multiple zones in the northamerica-northeast1 (Montreal) and northamerica-northeast2 (Toronto) regions.

B. Deploy instances in a single zone in the northamerica-northeast1 (Montreal) and northamerica-northeast2 (Toronto) regions.

C. Deploy instances in a single zone in the northamerica-northeast1 (Montreal) region and multiple zones in the northamerica-northeast2 (Toronto) region.

D. **Deploy instances in multiple zones in the northamerica-northeast1 (Montreal) region and a single zone in the northamerica-northeast2 (Toronto).**

Feedback:
A: Incorrect. This would provide higher than necessary availability in Toronto and increase the networking costs in that region by incurring inter-zone traffic.
B: Incorrect. This would not provide the required availability in Montreal as single-zone deployments would not provide 99.99% availability.
C: Incorrect.This would provide higher than necessary availability in Toronto and increase the networking costs in that region by incurring inter-zone traffic. It would also not provide the required availability in Montreal as single-zone deployments would not provide 99.99% availability.
*D: Correct! This satisfies the availability, latency and cost requirements. It ensures the lowest possible latency for users in Toronto and Montreal. It provides the desired availability (99.5% in Toronto and 99.99% in Montreal). By minimizing inter-zone network traffic, this solution minimizes networking costs.

Where to look:
https://cloud.google.com/about/locations
https://cloud.google.com/compute/docs/regions-zones
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources
https://cloud.google.com/vpc/network-pricing
https://cloud.google.com/compute/sla

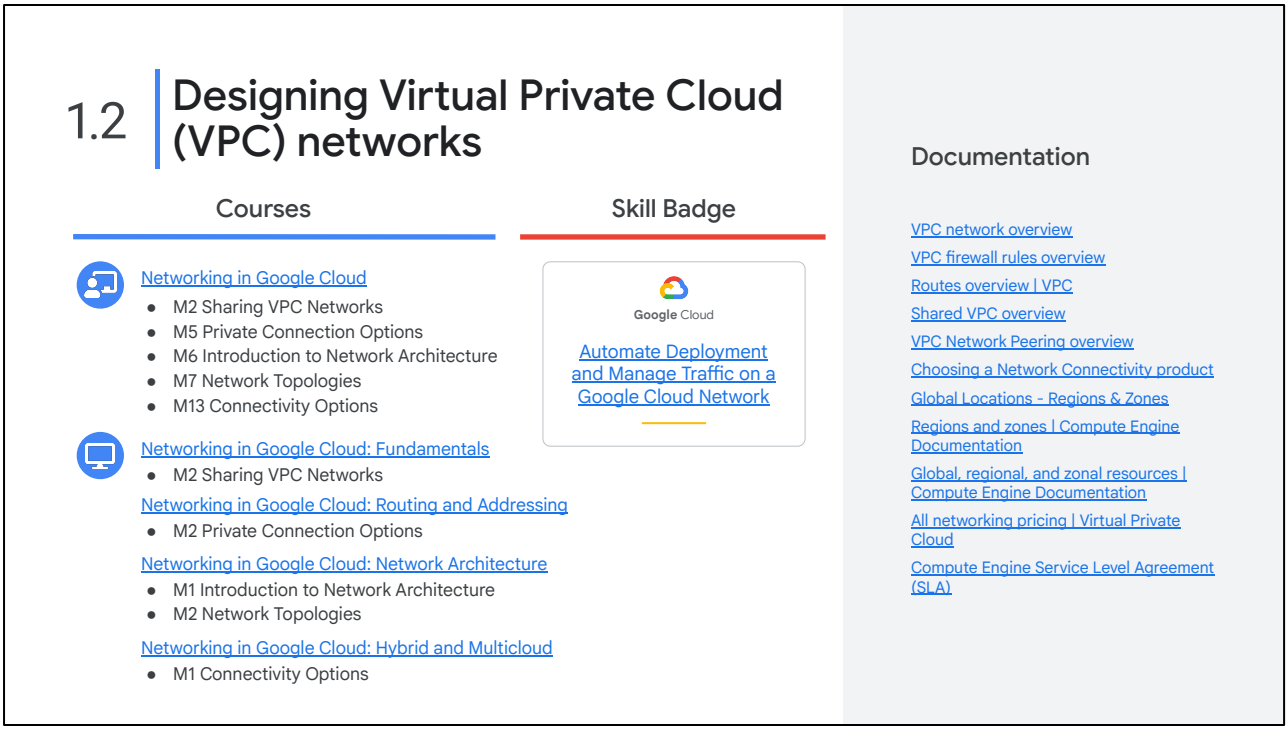
Content mapping:

- ILT course: **Networking in Google Cloud**
  - M5 Private Connection Options

- On-demand course: **Networking in Google Cloud: Routing and Addressing**
  - M2 Private Connection Options

- Skill badge: Automate Deployment and Manage Traffic on a Google Cloud Network

Summary:
Google Cloud offers 3 zones across approximately 30 regions (4 zones in us-central1 in Iowa). Though many capabilities are available across all regions, there are some differences in supported features and capabilities by region. Resources may be zonal, regional, multi-regional, or global with implications for availability, latency, and data residency. Placing replica resources across multiple zones increases availability (protecting against resource and zone failure). Placing replica resources across multiple regions can further increase availability, protect against regional outage, and reduce average latency for users close to those regions.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)
Networking in Google Cloud: Routing and Addressing (On-demand)
Networking in Google Cloud: Network Architecture (On-demand)
Networking in Google Cloud: Hybrid and Multicloud (On-demand)

Automate Deployment and Manage Traffic on a Google Cloud Network (Skill Badge)

https://cloud.google.com/vpc/docs/vpc
https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/routes
https://cloud.google.com/vpc/docs/shared-vpc
https://cloud.google.com/vpc/docs/vpc-peering
https://cloud.google.com/network-connectivity/docs/how-to/choose-product
https://cloud.google.com/about/locations

https://cloud.google.com/compute/docs/regions-zones
https://cloud.google.com/compute/docs/regions-zones/global-regional-zonal-resources
https://cloud.google.com/vpc/network-pricing
https://cloud.google.com/compute/sla

1.3 Designing a resilient and performant hybrid and multi-cloud network (1)

Considerations include:

- Designing for datacenter connectivity including bandwidth constraints (e.g., Dedicated Interconnect, Partner Interconnect, Cloud VPN)
- Designing for multi-cloud connectivity (e.g., Cloud VPN, Cross-Cloud Interconnect)
- Designing for branch office connectivity (e.g., IPSec VPN, SD-WAN appliances)
- Choosing when to use Direct Peering or a Verified Peering Provider
- Designing high-availability and disaster recovery connectivity strategies
- Selecting regional or global dynamic routing mode

Google Cloud

Professional Cloud Network Engineers should also be familiar with the options of connecting on-premise networks or other cloud networks to Google Cloud privately and securely to create hybrid or multi-cloud networks.

In this section, question 7 addressed types and high-level details for VPN, and question 8 covered Partner Interconnect.

To answer these questions, you should be comfortable with all of the considerations listed on this slide and the next.

1.3 Designing a resilient and performant hybrid and multi-cloud network (2)

Considerations include:

- Accessing multiple VPCs from on-premises locations (e.g., Shared VPC, multi-VPC peering and Network Connectivity Center topologies)
- Accessing Google Services and APIs privately from on-premises locations (e.g., Private Service Connect for Google APIs)
- Accessing Google managed services through VPC Network Peering connections (e.g., Private Services Access, Service Networking)
- Designing the IP address space across on-premises locations and cloud environments (e.g., Cloud NAT Private, internal ranges)
- Designing the DNS peering and forwarding strategy (e.g., DNS forwarding path)

1.3 Diagnostic Question 07 Discussion

You are designing a VPN solution to connect Cymbal Bank's on-premises data center to Google Cloud. You have a BGP-capable VPN gateway installed in the data center and require 99.99% availability for the VPN link.

What Cloud VPN configuration meets these requirements while requiring the least setup and maintenance?

A. Classic VPN with route-based static routing
B. Classic VPN with policy-based static routing
C. Classic VPN with Cloud Router and dynamic routing
D. HA VPN with Cloud Router and dynamic routing

Feedback:
A: Incorrect. This configuration does not provide the required availability. It can only provide 99.9% availability. It also requires extra configuration and maintenance for the static routes,compared to dynamic routing with BGP utilizing the Cloud Router.
B: Incorrect. This configuration does not provide the required availability. It can only provide 99.9% availability. It also requires extra configuration and maintenance for the static routes, compared to dynamic routing with BGP utilizing the Cloud Router.
C: Incorrect. This configuration does not provide the required availability. It can only provide 99.9% availability
*D: Correct! This configuration can provide the required availability of 99.99%. It also minimizes setup and maintenance configuration by using dynamic routing,

Where to look:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview

Content mapping:
- ILT course: **Networking in Google Cloud**
  - M14 Cloud VPN

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
  - M2 Cloud VPN

Summary:
There are many configuration options available for Cloud VPN in Google Cloud.

There is Classic VPN which supports both static and dynamic routing when used with the Cloud Router. Classic VPN offers lower availability (99.9%) but can connect to on-premises VPN gateways that don’t support BGP. HA VPN only supports dynamic routing and requires a Cloud Router. Cloud Routers and HA VPN can’t work with on-premises VPN gateways that don’t support BGP. However, HA VPN can offer higher availability (99.99%) and is the Google recommended approach where possible.

1.3 Diagnostic Question 08 Discussion

To reduce latency, you will be replacing an existing Cloud VPN Classic VPN connection. You will connect your organization's on-premises data center to Google Cloud resources in a VPC network with all resources in a single subnet and region using private/internal IP connectivity. The connection will need to support 1.5 Gbps of traffic. Due to cost considerations, you would like to order the option that provides just enough bandwidth and not more but must have significantly lower latency than the existing Cloud VPN connection.

What should you use?

A. A 10 Gbps Dedicated Interconnect connection with one 10 Gbps VLAN attachments

B. A 2 Gbps Dedicated Interconnect connection with one 2 Gbps VLAN attachments

C. A Partner Interconnect connection with 1 or 2 VLAN attachments

D. A Cloud VPN HA VPN connection with Cloud Router

Feedback:
A: This option will not be the lowest cost as it involves purchasing the 10 Gbps connection. Only 1.5 Gbps is required and can be purchased at lower cost through Partner Interconnect.
B: This option is not possible. Dedicated Interconnect connections start at 10 Gbps.
*C: This option will be the most cost effective among the options that would satisfy the requirement to reduce the latency significantly compared to the previous Cloud VPN connection.
D: This option will be inexpensive but would not reduce the latency significantly relative to the Cloud VPN Classic VPN connection.

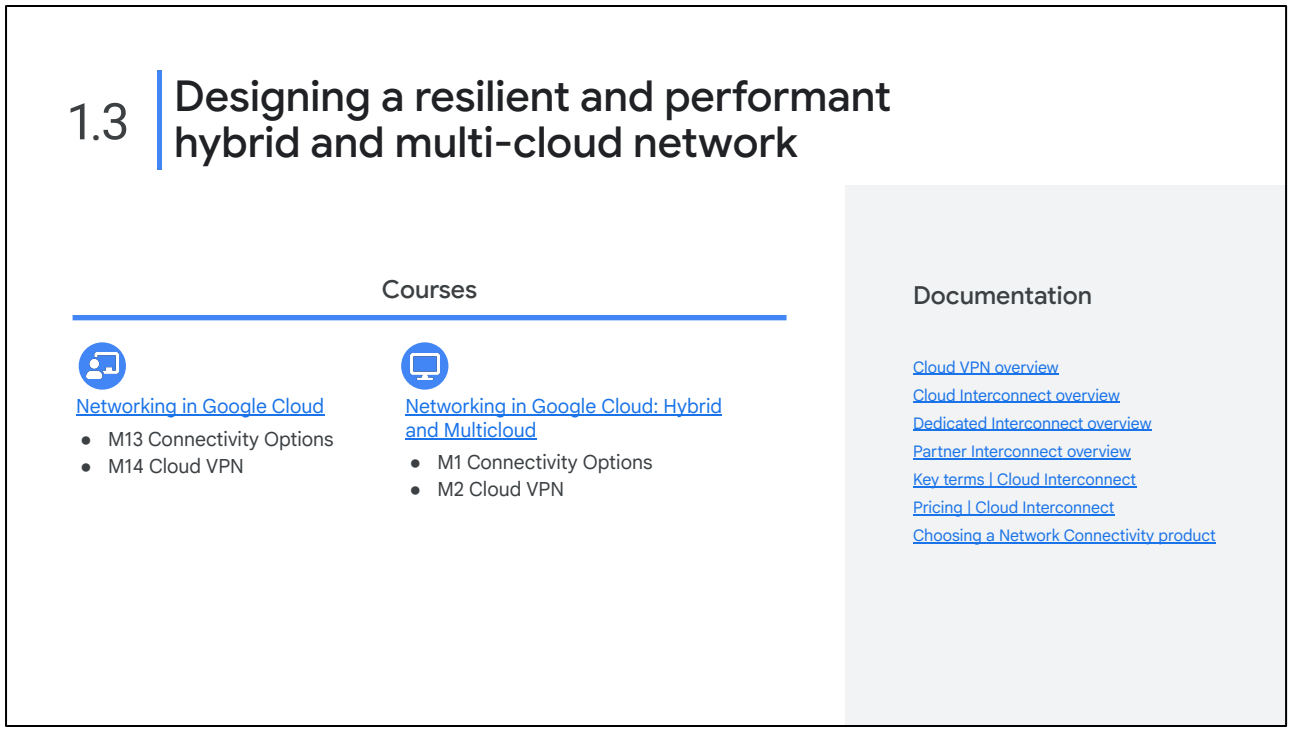
Where to look:
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/terminology
https://cloud.google.com/network-connectivity/docs/interconnect/pricing
https://cloud.google.com/network-connectivity/docs/how-to/choose-product#cloud-interconnect

Content mapping:
- ILT course: **Networking in Google Cloud**

    - M13 Connectivity Options

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
    - M1 Connectivity Options

Summary:
At a high level there are two options for Interconnect: Dedicated Interconnect and Partner Interconnect. Dedicated and Partner Interconnect can provide higher bandwidths and lower latencies. Dedicated Interconnect requires installing a router in a Google co-location facility and requires purchasing at least a 10 Gbps connection. Partner Interconnect can provide lower bandwidths and will be available at more locations from various providers. It can provide connections as low as 50 Mbps, which means it would typically be more cost effective at bandwidths lower than 10 Gbps.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Hybrid and Multicloud (On-demand)

https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/dedicated-overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/terminology
https://cloud.google.com/network-connectivity/docs/interconnect/pricing
https://cloud.google.com/network-connectivity/docs/how-to/choose-product#cloud-interconnect

1.4 Designing an IP addressing plan for Google Kubernetes Engine

Considerations include:

- Choosing between public or private cluster nodes and node pools
- Choosing between public or private control plane endpoints
- Choosing between GKE Autopilot mode or Standard mode
- Planning subnets and alias IPs
- Selecting RFC 1918, non-RFC 1918, and/or privately used public IP (PUPI) addresses
- Planning for IPv6

Google Cloud

A Professional Cloud Network Engineer should be familiar with the IP addressing concerns of Google Kubernetes Engine (GKE), including how pod and service addresses are allocated, how GKE uses subnet primary and secondary IP ranges, and the differences between private and public clusters and control-plane endpoints.

In this section, question 9 explored GKE VPC-native clusters and IP planning. Question 10 explored public vs. private GKE clusters.

To answer these questions, you should be comfortable with all of the considerations listed on the slide.

1.4 Diagnostic Question 09 Discussion

You need to create a GKE cluster, be able to connect to pod IP addresses from your on-premises environment, and control access to pods directly using firewall rules. You will need to support 300 nodes, 30000 pods, and 2000 services.

Which configuration satisfies these requirements?

A. A GKE route-based cluster in a subnet with primary IP range 10.0.240.0/20 and pod IP range of 10.1.0.0/16

B. A GKE route-based cluster in a subnet with primary IP range 10.0.240.0/20 and pod IP range of 10.252.0.0/14

C. A GKE VPC-native cluster in a subnet with primary IP range 10.0.240.0/20, pod IP range of 10.252.0.0/15, and service IP range of 10.0.224.0/20

D. A GKE VPC-native cluster in a subnet with primary IP range 10.0.240.0/20, pod IP range of 10.252.0.0/16, and service IP range of 10.0.224.0/20

Feedback:
A: Incorrect. A route-based GKE cluster will not satisfy the first 2 requirements. Additionally, the pod IP range would not be large enough to support the required number of nodes and pods.
B: Incorrect. A route-based GKE cluster will not satisfy the first 2 requirements
*C: Correct! This option will satisfy all requirements. A VPC-native cluster will satisfy the first 2 requirements and the provided ranges will support the required number of nodes, pods, and services.
D: Incorrect. This option will satisfy the first 2 requirements (being a VPC-native cluster), but the pod IP range will not be sufficient to hold the required number of nodes and pods.

Where to look:
https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters
https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/routes-based-cluster

Content mapping:
Not covered in learning path.

Summary:
With respect to network routing and IP planning, there are two main approaches to deploying GKE: routes-based or VPC-native. VPC-native is the newer and

recommended approach that provides several benefits. It is important to be aware of the subtle differences in how to select the correct IP ranges to use with each type, as well as the supported numbers of resources based on size of the ranges.

1.4 Diagnostic Question 10 Discussion

Cymbal Bank wants to ensure communication from their on-premises data centers to the GKE control plane stays private using internal IP communication and their Dedicated Interconnect links. However, they will need to allow administrators to periodically connect to the cluster control plane from remote internet-accessible locations that don't have access to the on-premises private network. You want to select a configuration and connection approach that will enable these requirements while providing the highest security.

What should you do?

A. Deploy a private GKE cluster with public endpoint access enabled and authorized networks disabled.

B. Deploy a private GKE cluster with public endpoint access enabled and authorized networks enabled. Configure authorized networks for the cluster to include all remote source IP ranges that administrators may connect from.

C. Deploy a private GKE cluster with public endpoint access disabled. Create a VM in the same subnet with only an internal IP address and provide IAP tunnel based SSH access to remote administrators for this VM. Have remote administrators connect via IAP tunnel SSH to this VM when requiring access to the GKE cluster control plane.

D. Deploy a private GKE cluster with public endpoint access disabled. Provide remote administrators IAP tunnel based SSH access to a node in the cluster. Have remote administrators connect via an IAP tunnel SSH to this node when requiring access to the GKE cluster control plane.

Feedback:
A: Incorrect. This option satisfies the requirements; however, it is the least secure option because it provides access to the control plane from any public IP address.
B: Incorrect. This option satisfies the requirements; however, it is not as secure as options C and D because it provides access to the control plane from a set of public IP addresses/ranges.
*C: Correct! This options satisfies the requirements in the most secure way by not providing any public access to the control plane and no private access to the cluster nodes.
D: Incorrect. Though satisfying requirements, this approach is slightly less secure than approach C as it provides direct node access to the remote administrators when only control plane access is required. (Option C only provides access to the control plane without access to the nodes.)

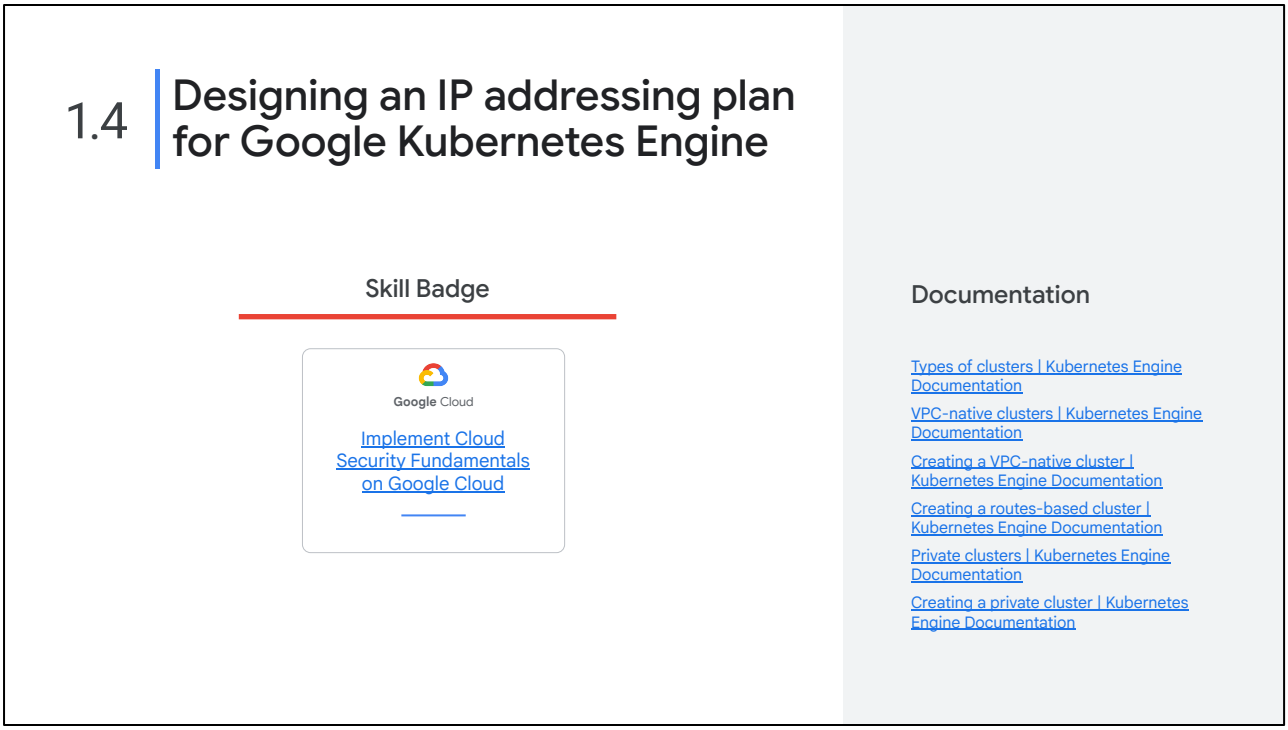
Where to look:
https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept
https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters

Content mapping:
Partial coverage in skill badge: Implement Cloud Security Fundamentals on Google Cloud.

Summary:
Creating GKE private clusters improves security. There are 3 high level configurations

available for private clusters with varying levels of security and ease of access for each:

- Public endpoint access disabled is the most secure. Connectivity to the control plane is not allowed from any client outside the cluster subnet.
- Public endpoint access enabled, authorized networks enabled is the next most secure and provides connectivity to the control plane from only specified public or private IP ranges.
- Public endpoint access enabled, authorized networks disabled provides the least secure and provides the most permissive connectivity allowing access to the public endpoint from any IP address.



Let's take a moment to consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Implement Cloud Security Fundamentals on Google Cloud (Skill badge)

https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters
https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/routes-based-cluster
https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept
https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters