

# Interconnecting Networks

## Elastic Cloud Infrastructure: Scaling and Automation

CLOUD VPN, CLOUD ROUTER, CLOUD INTERCONNECT, DIRECT PEERING, CLOUD DNS



VIRTUAL PRIVATE NETWORKS (VPN)



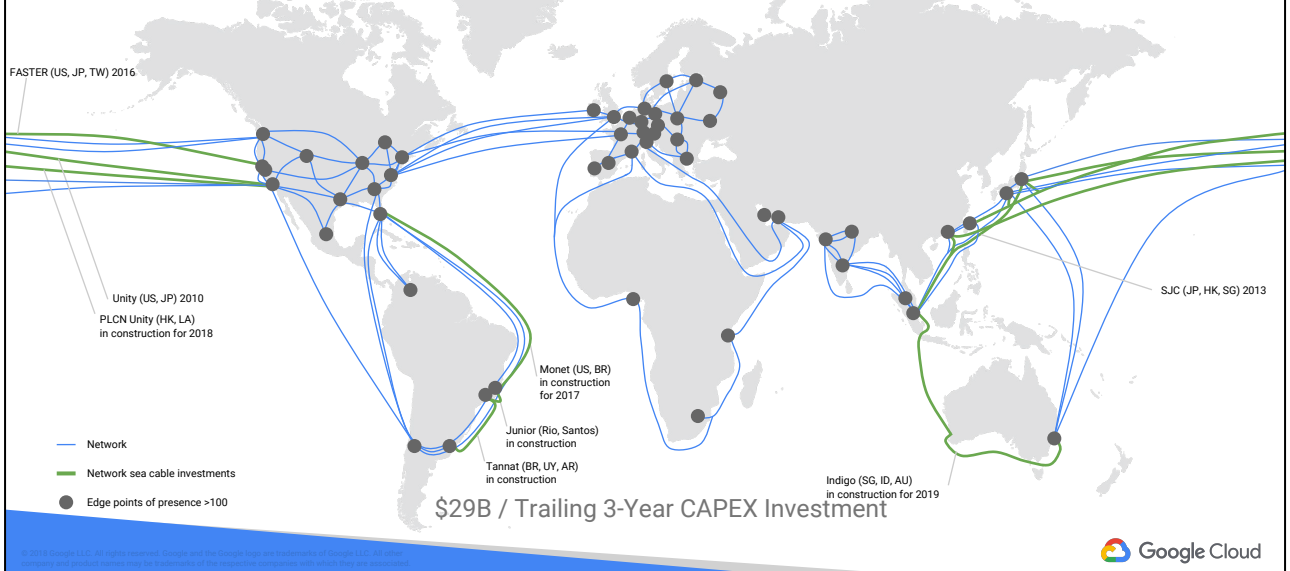
Google Cloud

Last modified 2018-01-29

© 2018 Google LLC. All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.

## Google Cloud Network

Google Cloud's well-provisioned global network is composed of hundreds of thousands of miles of fiber optic cable and seven submarine cable investments.



A global network in 14 regions and 39 zones in 2017. Not only for performance, but also to meet customer regulatory or policy requirements.

Thousands of miles of fiber.  
Four owned undersea cables.

Google's networking infrastructure:

<https://techcrunch.com/2015/08/18/how-googles-networking-infrastructure-has-evolved-over-the-last-10-years/>

# Google Cloud Platform Regions

GCP is adding 10 new regions in 2017/2018



For more information, see:

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

# Google Cloud networking

## Global Scale

Application delivery at scale globally or regionally



HTTPS, TCP, UDP Load Balancing  
Cloud CDN  
Cloud DNS

## Virtual Network

Global private space, regional segmentation



SDN network virtualization  
Global Networks  
Granular Subnetworks

## Hybrid Cloud

Connection to on-premises



Cloud VPN  
Cloud Router  
Cloud Interconnect

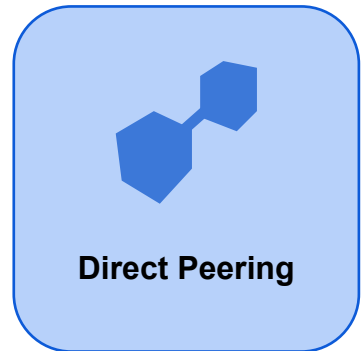
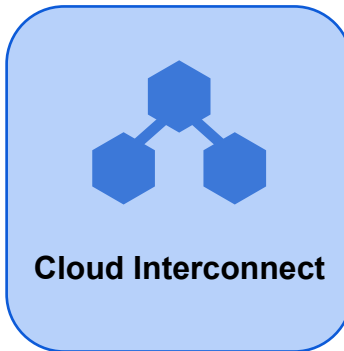
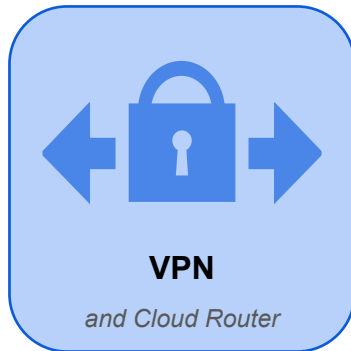
## Control

User control  
Security policies  
Visibility/diagnostics



Network IAM roles  
Firewalls

## Interconnection options



### Direct Peering

Private enterprise-grade connection for hybrid cloud workloads

### Carrier Interconnect

Enterprise-grade connection through service provider partners

### VPN

Secure multi-Gbps connection over VPN tunnels

## Agenda

- **Cloud Virtual Private Networks (VPN)**
- Lab
- Cloud Router
- Cloud Interconnect
- External Peering
- Cloud DNS
- Quiz

## Google Cloud VPN

- Securely connects your on-premises network to your GCP VPC network
- Traffic traveling between the two networks is protected as it travels over the internet:
  - Encrypted by one VPN gateway
  - Decrypted by the other VPN gateway
- SLA of 99.9% service availability
- Supports site-to-site VPN
- Supports:
  - Static routes
  - Dynamic routes (Cloud Router)
- Supports IKEv1 and IKEv2 using a shared secret
- Uses ESP in tunnel mode with authentication

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. This protects your data as it travels over the internet.

- Cloud VPN provides an SLA of 99.9% service availability.
- Cloud VPN supports site-to-site VPN. You can have multiple tunnels to a single VPN gateway.
- Cloud VPN supports both static routes and dynamic routes (via Cloud Router) for managing traffic between your instances and your existing infrastructure.
- Cloud VPN supports both IKEv1 and IKEv2 using a shared secret (IKE pre-shared key).
- Cloud VPN uses ESP in Tunnel mode with authentication. Cloud VPN does not support AH or ESP in Transport mode.

For more information, see:

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

IPsec: <https://wikipedia.org/wiki/IPsec>

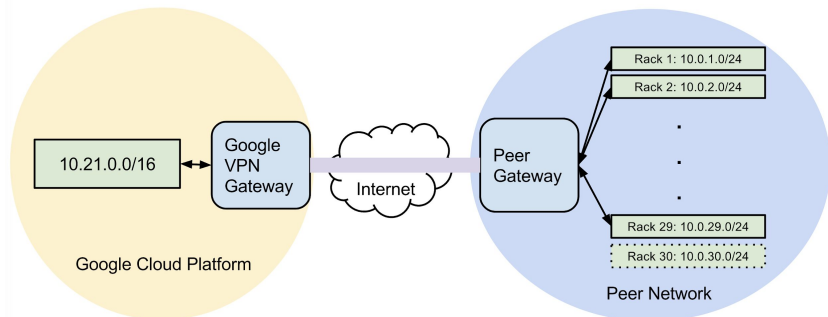
VPN: [https://wikipedia.org/wiki/Virtual\\_private\\_network](https://wikipedia.org/wiki/Virtual_private_network)

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

## VPN with static routes

With static routing, updating the tunnel requires:

- The addition of static routes to GCP.
- Restarting the VPN tunnel to include the new subnet.



The diagram shows the example topology using a VPN tunnel to connect a Google Cloud network and 29 subnets (one per rack) in the on-premises network. In the diagram, a new subnet is being added (10.0.30.0/24).

For more information, see:

<https://cloud.google.com/vpn/docs/how-to/creating-vpns>



## Agenda

- Cloud Virtual Private Networks (VPN)
- **Lab**
- Cloud Router
- Cloud Interconnect
- External Peering
- Cloud DNS
- Quiz

# Lab: Virtual private networks (VPN)

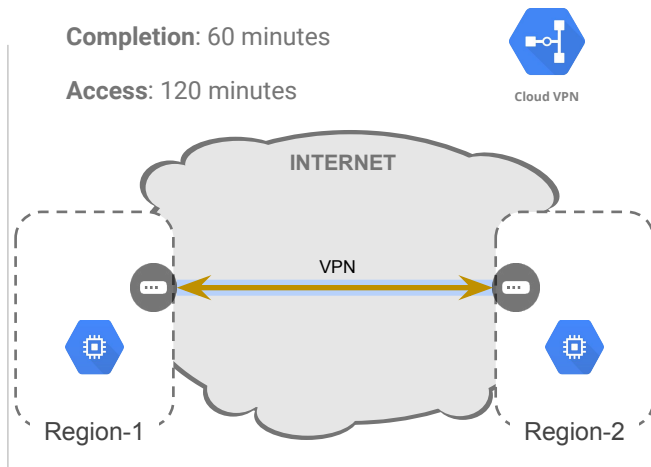
## Objectives

In this lab, you learn how to perform the following tasks:

- Create two custom networks and associated subnetwork
- Create VPN gateways in each network
- Establish static routes to enable the gateways to pass traffic
- Configure static routes to pass traffic to the VPN gateway
- Establish firewall rules to enable ICMP and SSH traffic

**Completion:** 60 minutes

**Access:** 120 minutes



## Lab review

In this lab you learned how to:

- Set up virtual private networking (VPN) between two subnets in different regions.
- Perform most of the configuration from the command line.
- Configure VPN using the GCP Console; many of the steps are automated.

*One purpose of this lab is to show you how to configure VPN manually, so that you will better understand what the GCP Console does automatically. This can help in troubleshooting a configuration.*

## Agenda

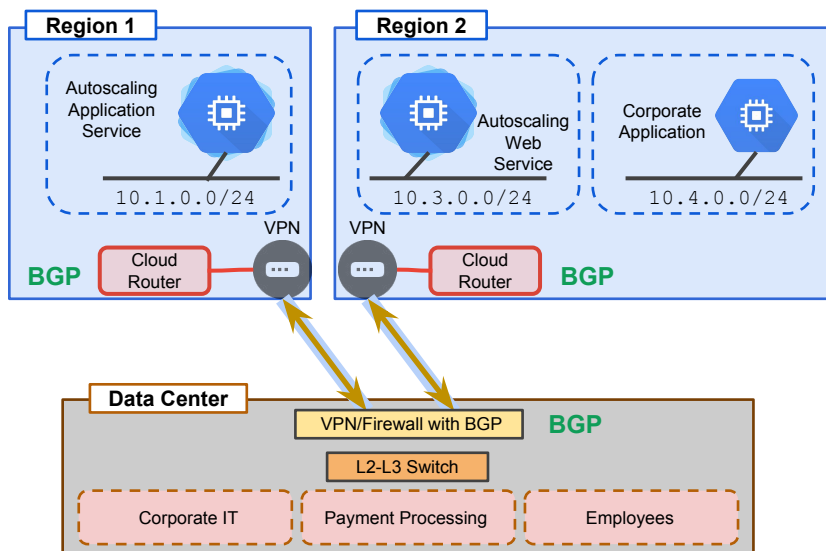
- Cloud Virtual Private Networks (VPN)
- Lab
- **Cloud Router**
- Cloud Interconnect
- External Peering
- Cloud DNS
- Quiz

## Cloud Router

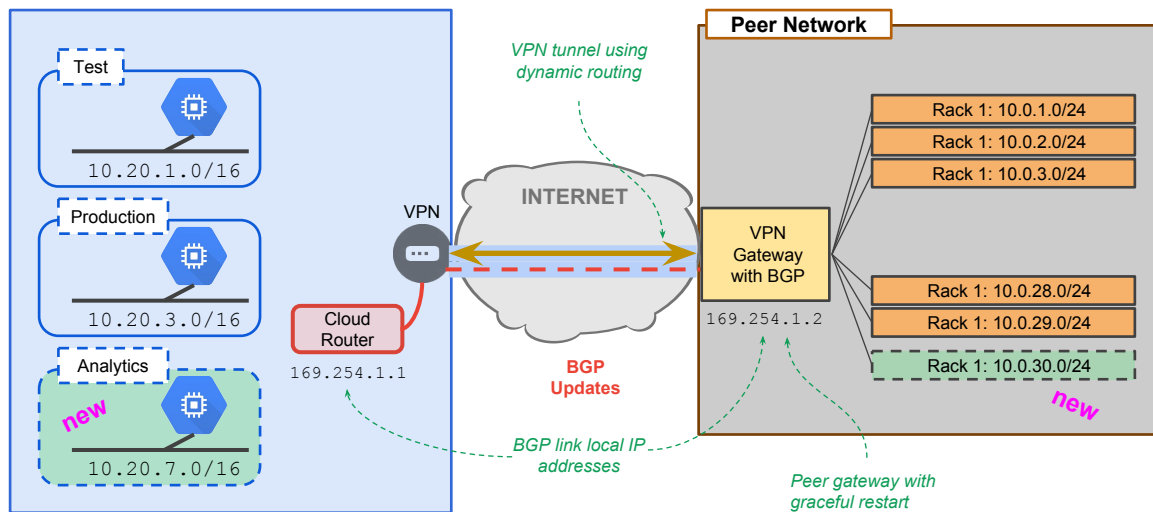
- Provides BGP routing
  - Dynamically discovers and advertises routes
- Supports graceful restart
- Supports ECMP
- Primary/Backup tunnels for failover
  - MED
  - AS Path length
  - AS Prepend

## Dynamic routing with Cloud Router

- One Cloud Router in each region
- Peers with BGP router on-premises
- Advertise all subnets of the region
- Link-local IPs for BGP
- Private ASN on GCP
- Private or Public ASN on-premises



## Cloud Router with subnetworks



BGP peers establish adjacency on private network 169.254.1.0.  
 New subnets in GCP or in Peer network are discovered and shared, enabling connectivity between the two peers for both entire networks.

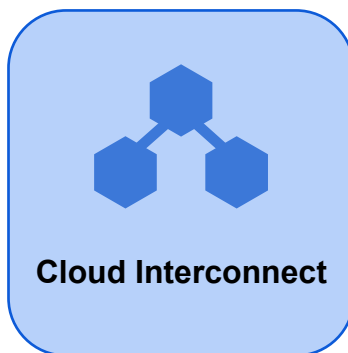
## Agenda

- Cloud Virtual Private Networks (VPN)
- Lab
- Cloud Router
- **Cloud Interconnect**
- External Peering
- Cloud DNS
- Quiz



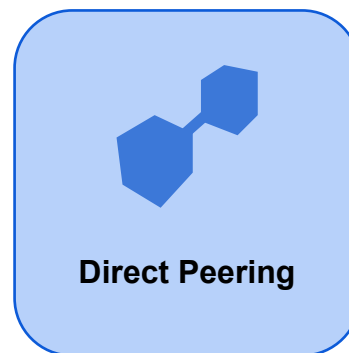
## Cloud Interconnect

- Enterprise-grade connection to GCP
- Provides access to private (e.g., RFC1918) network addresses
- Enables easy hybrid cloud deployment
- Does not require the use of and management of hardware VPN devices



**Cloud Interconnect**

- Connect through a service providers network
- Provides dedicated bandwidth (50Mbps – 10Gbps)



**Direct Peering**

- Connect to Google Cloud through Google POPs
- Provides N X 10G transport circuits for private cloud traffic

For more information, see: <https://cloud.google.com/interconnect/docs>

- Arranged through Cloud Interconnect Service Providers
  - <https://cloud.google.com/interconnect/docs>
  - No Google SLA; SLA only through service provider
  - Service Provider network security (not Google end-to-end)
- Benefits of Cloud Interconnect
  - Higher availability
  - Lower latency
  - Lower cost for data-intensive applications

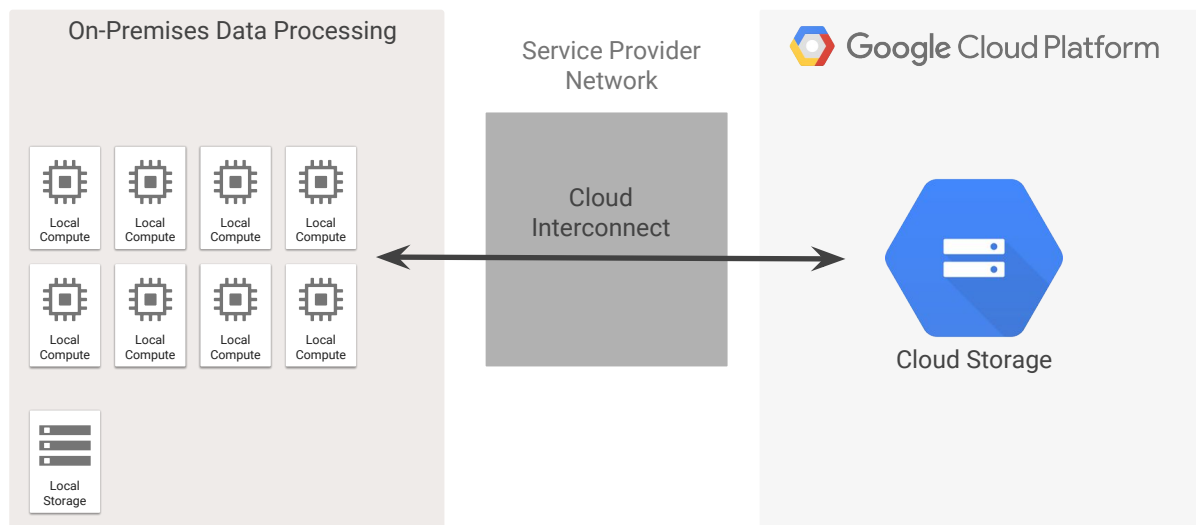
## Dedicated interconnect considerations

- Must have a common point of presence with Google
- Your router must:
  - Be a single-mode fiber, 10GBASE-LR, 1310 nm
  - Must support:
    - LACP for bonding multiple links from 10 GB to 80 GB and more
    - Link local addressing
    - 802.1q VLANs
    - BGP-4 with multihop
    - Support IPv4 link local addressing
    - EBGP-4

For more information, see:

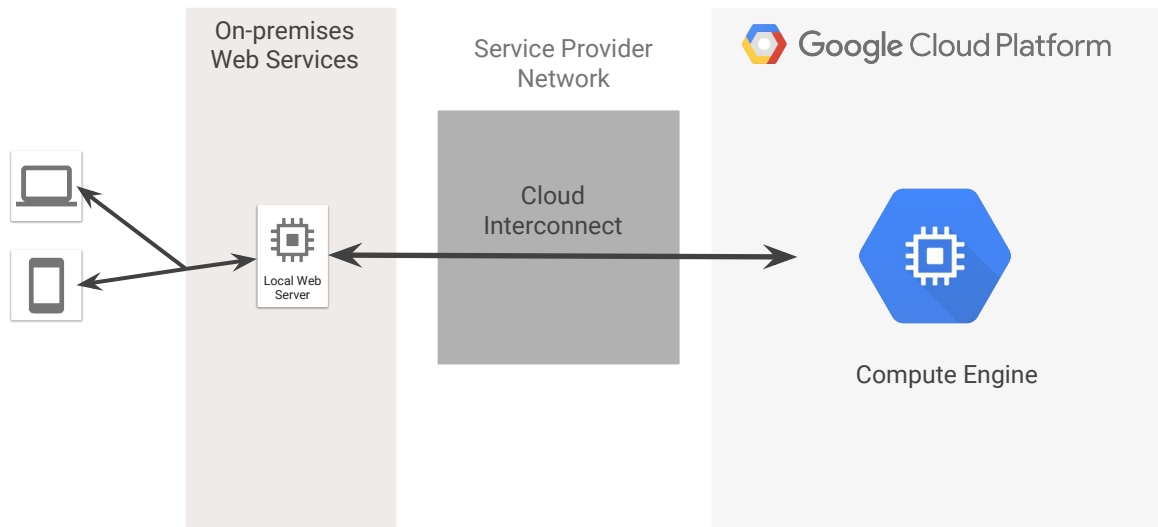
<https://cloud.google.com/interconnect/docs/details/dedicated#benefits>

## Data-intensive application



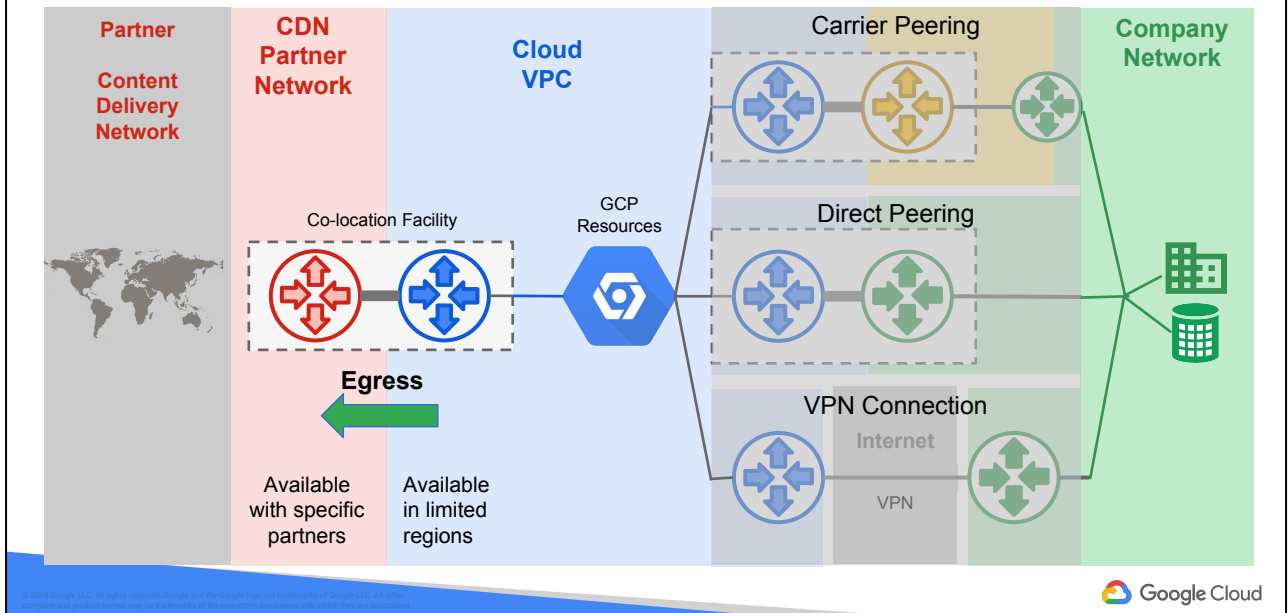
Massive data in cloud storage is being pulled/pushed to the on-premises computers for data processing. In this case, Cloud Interconnect provides lower latency, lower costs for some transfers, and higher reliability (depending on the service provider's SLAs).

## Latency-sensitive application



User uploads video that is transmitted to Compute Engine for flexible compute capacity. The video is processed and returned to the web server and to the user. In this case, Cloud Interconnect is used primarily to reduce the round-trip latency.

## Content Delivery Network Interconnect



- Use case: data stored or processed in GCP, and hosted on the provider's CDN service, that is frequently updated from GCP
- Cloud Interconnect egress region-to-region pricing

CDN Interconnect is about egress from the VPC. Select CDN Partner Providers have direct egress capability to access their global Content Delivery Network. Note that Google has its own Content Delivery Network service. However, if you use a different CDN provider, Google has a partnering relationship with some with which an egress interconnect has been established. You may benefit by lower rates or lower latency to the CDN partner's services.

- Specific CDN Partners
- Specific limited regions and/or locations

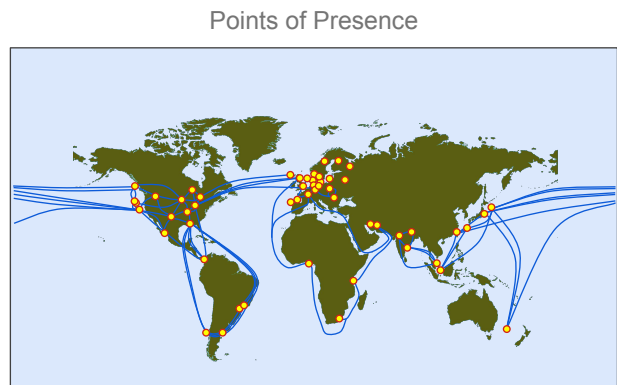
For more information, see: <https://cloud.google.com/interconnect/cdn-interconnect>

## Agenda

- Cloud Virtual Private Networks (VPN)
- Lab
- Cloud Router
- Cloud Interconnect
- **External Peering**
- Cloud DNS
- Quiz

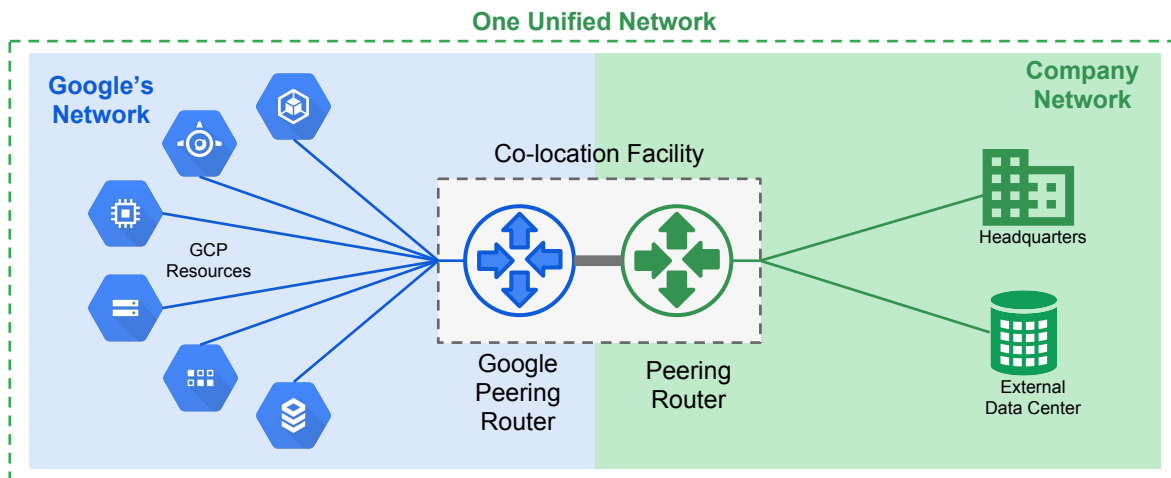
## Direct peering

- BGP direct connect between your network and Google's network at Edge Network locations
- Autonomous System numbers (AS) are exchanged via IXPs and some private facilities
- Technical, commercial, and legal requirements



Google edge points of presence (PoPs) are where Google's network is connected to the rest of the internet via peering. Google is present on over 90 internet exchanges and at over 100 interconnection facilities around the world. LB and CDN at 80+ of these POPs. 42ms latency (median) and 140ms 90p.

## Direct peering



- Direct physical connection between an on-premise network and Google's network at any of 70+ locations in 33 countries around the world.
- Extends your private network into your cloud network.

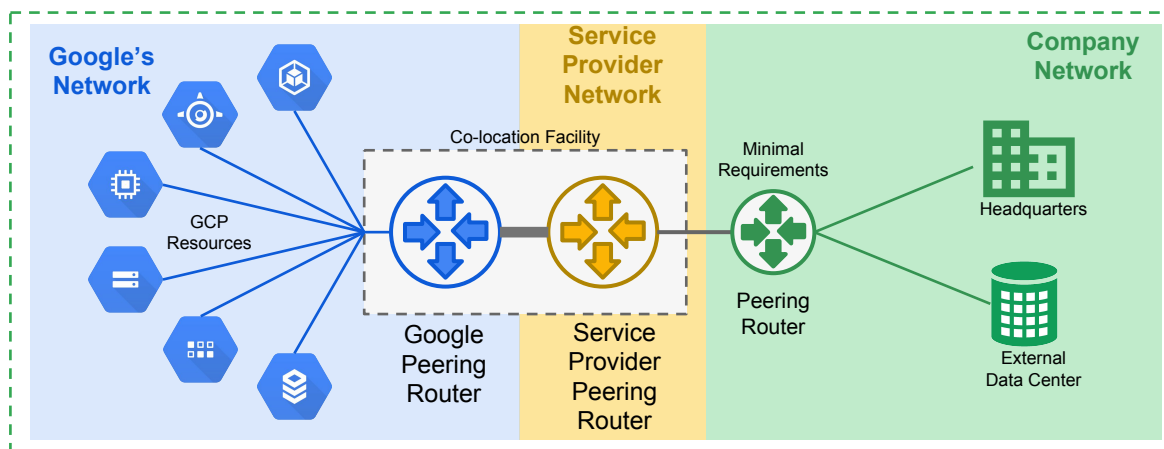
Google allows you to establish a direct peering connection between your business network and Google's. With this connection you can exchange internet traffic between your network and Google's at one of their broad-reaching edge network locations. Direct peering with Google is done by exchanging BGP routes between Google and the peering entity. After a direct peering connection is in place, you can use it to reach all of Google's services, including the full suite of Google Cloud Platform products.

For more information, see:

<https://cloud.google.com/interconnect/docs/how-to/direct-peering>



## Carrier peering



- You can obtain enterprise-grade network services that connect your infrastructure to Google by using a service provider
- You can get connections with higher availability and lower latency, using one or more links.

For more information, see:

<https://cloud.google.com/interconnect/docs/how-to/carrier-peering>

## Autonomous System (AS)

- AS represents a collection of Internet Protocol (IP) routing prefixes under the control of an administrative entity representing one or more network operators
- ASN refers to AS number, which is allocated by Internet Assigned Numbers Authority (IANA)
- A business entity with an assigned ASN generally implies that that entity owns one or more blocks of IP addresses
- Google's ASN is 15169

## Key concepts

- Border Gateway Protocol (BGP)
  - BGP is used to route traffic among internet service providers (ISP) or any entities who are assigned their own ASNs
- Private Network Interconnect (PNI)
  - Means "private peering"
- PeeringDB
  - A freely available web-based database of networks that are interested in peering
  - A resource for identifying candidates for peering

# Peering locations for ASN=15169

Company Information				Public Peering Exchange Points				
Company Name	Google Inc.			Exchange Point Name	ASN	IP Address	Mbit/sec	
Also Known As	Google, YouTube (for Google Fiber see AS16591 record)			AMS-IX	15169	80.249.209.100	100000	
Company Website	<a href="https://www.google.com/">https://www.google.com/</a>			AMS-IX	2001:7f8:1:a001:5169:1		100000	
Primary ASN	15169			AMS-IX	2001:7f8:1:a001:5169:2		100000	
IRR Record	AS-GOOGLE			AMS-IX	15169	80.249.208.247	100000	
Network Type	Content			BBIX Hong Kong / Singapore	15169	103.231.152.35	10000	
Asynux Prefixes	15000			BBIX Hong Kong / Singapore	15169	2001:df8:8000:8a00:0:1:5169:1	10000	
Traffic Levels	Not Disclosed			BBIX Osaka	15169	218.100.7.27	10000	
Traffic Ratios	Mostly Outbound			BBIX Osaka	2001:df8:c:2:0:1:5169:1		10000	
Geographic Scope	Global			BBIX Tokyo	15169	2001:df8:c:1:5169:1	20000	
Looking Glass URL				BBIX Tokyo	15169	218.100.6.53	20000	
Route Server URL				BCIX	2001:7f8:19:1:3041:1/64		10000	
				BCIX	15169	193.178.185.100	10000	
1 2 3 4 5 of 9 Next > Last >>								
We have a generally open peering policy. Please visit the following link: <a href="https://peering.google.com/about/peering_policy.html">https://peering.google.com/about/peering_policy.html</a>								
This link also has information about our traffic delivery and management practices.								
Notes								
Related ASNs: AS36400, AS43515, AS36561								
Peering Requests: Contact <a href="mailto:peering@google.com">peering@google.com</a>								
Peering Operational Issues: Contact <a href="mailto:net@google.com">net@google.com</a> 24x7								
Protocols Supported Unicast IPv4 IPv6 Multicast IPv6								
Date Last Updated 2016-02-09 20:51:23 UTC								
Peering Policy URL <a href="https://peering.google.com/about/peering_policy.html">https://peering.google.com/about/peering_policy.html</a>								
General Policy Open								
Multiple Locations Preferred								
Ratio Requirement Contract Requirement								
Private Only								
Contact Information								
Role	Contact Name	Telephone	E-Mail					
NOC	NOC 24x7	+1 650 253 1500	<a href="mailto:net@google.com">net@google.com</a>					
Policy	Peering enquiries		<a href="mailto:peering@google.com">peering@google.com</a>					

Peering locations

<https://www.peeringdb.com/view.php?asn=15169>



For more information, see: <https://www.peeringdb.com/view.php?asn=15169>

## Details about direct peering

- Via edge point of presence (PoP)
- Uses the existing peering infrastructure Google uses for internet service providers (ISP)
- **Not** a private MPLS line into Google data centers where GCP services are located
- For all Google-bound traffic, not limited to GCP
- For public internet traffic via BGP with dedicated bandwidth but not necessarily private data exchange
- Discounted egress charges only apply to traffic flowing through the direct peering cross-connect, which requires a pre-defined BGP advertisement of its respective IP range
  - The IP range for the announcement must be of /24 at the minimum
- Direct peering set up with Google NetOps Content Distribution (NCD) team (*outside of GCP team*)

## Share GCP VPC networks across projects in your cloud organization using Shared VPC

Shared VPC allows:

- Creation of a VPC network of RFC1918 IP spaces that associated projects can use
- Project admins to create VMs in the shared VPC network spaces
- Network and security admins to create VPNs and firewall rules usable by the projects in the VPC network
- Policies to be applied and enforced easily across a cloud organization

In large organizations, you may need to put different departments or different applications into different projects for purposes of separating budgeting, access control, and so on. With Shared VPC, cloud organization administrators can give multiple projects permission to use a single, shared VPC network and corresponding networking resources.

Shared VPC allows for the creation of a VPC network of RFC1918 IP spaces that associated projects can use. With Shared VPC, you can allow project admins to create VMs in the shared VPC network spaces and allow network and security admins to create VPNs and firewall rules that are usable by the projects in the VPC network. Shared VPC makes it easy to apply and enforce consistent policies across a cloud organization.

For more information, see:

Shared VPC Concepts:

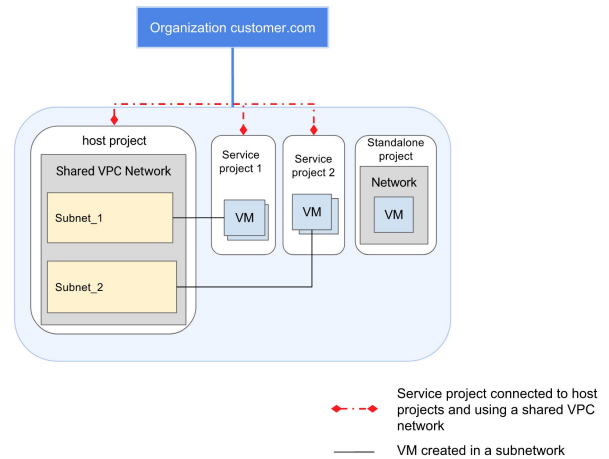
[https://cloud.google.com/vpc/docs/shared-vpc#concepts\\_and\\_terminology](https://cloud.google.com/vpc/docs/shared-vpc#concepts_and_terminology)

Shared VPC: <https://cloud.google.com/vpc/docs/shared-vpc>

RFC1918: <https://tools.ietf.org/html/rfc1918>

## Shared VPC overview

- Make a VPC network shareable across several projects in your cloud organization
- Host the VPC network in a shared VPC host project



The diagram shows a host project sharing its VPC network with two service projects. It is sharing Subnet\_1 with one project and Subnet\_2 with another project. The Standalone project has not been designated a service project, so it can't share resources with the host project.

For more information, see:

[https://cloud.google.com/vpc/docs/shared-vpc#shared\\_vpc\\_host\\_project\\_and\\_service\\_project\\_associations](https://cloud.google.com/vpc/docs/shared-vpc#shared_vpc_host_project_and_service_project_associations)

## Connect two VPC networks regardless of shared projects/organizations using VPC Network Peering

VPC Network Peering allows you to:

- Build SaaS ecosystems in GCP
  - Make services available privately across different VPC networks in and across organizations
  - Have workloads communicate in private RFC1918 space

VPC Network Peering is useful for organizations:

- With several network administrative domains
- That want to peer with other organizations



## VPC Network Peering advantages

VPC Network Peering provides the following advantages over using external IP addresses or VPNs to connect networks:

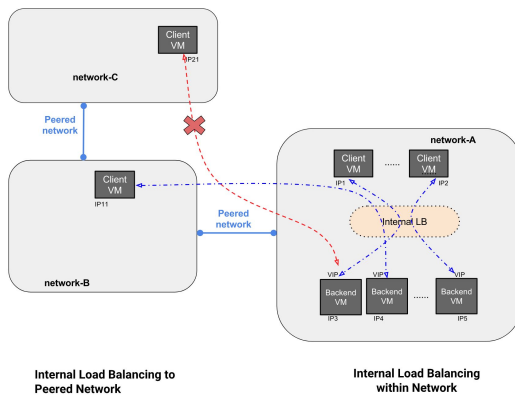
- Network latency
- Network security
- Network cost

VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

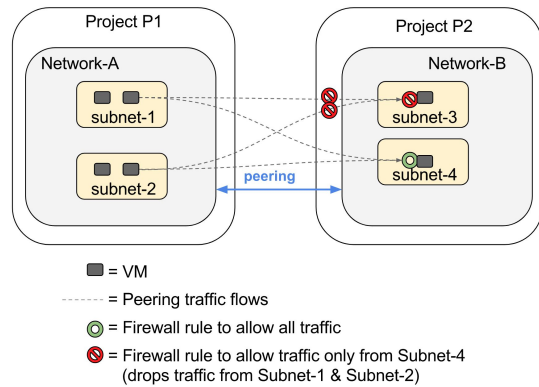
- **Network latency:** Public IP networking suffers higher latency than private networking.
- **Network security:** Service owners do not need to have their services exposed to the public internet and deal with its associated risks.
- **Network cost:** GCP charges egress bandwidth pricing for networks that use external IPs to communicate, even if the traffic is within the same zone. However, if the networks are peered, they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

## VPC Network Peering scenarios

## Internal Load Balancing



## Firewall

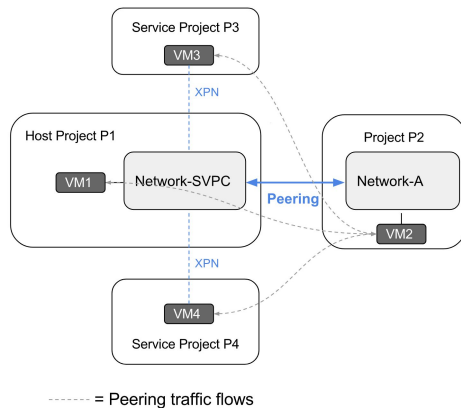


The Internal Load Balancing diagram shows how VM instances in network-B access the load balanced backends in network-A. The Internal Load Balancing configuration from network-A is automatically applied to network-B in this case. Internal Load Balancing services are available to clients in directly peered networks only. That is, in the case that network-B peers with network-C, the Internal load-balanced backends in network-A will not be reachable from clients in network-C.

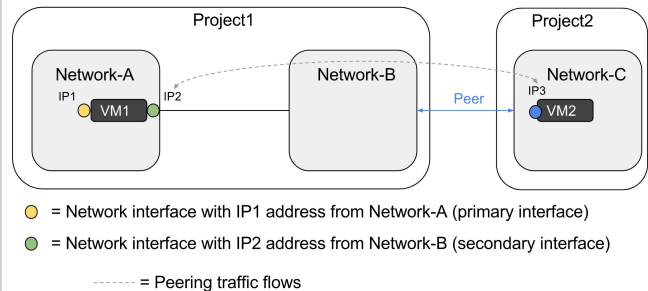
If you have peering between your VPC network and another VPC network, you may want to block traffic to a given set of VM instances or Internal Load Balancing endpoints. You must use firewall rules to do this because there is no way to exclude certain VM instances or Internal load balancers from the peering. If you want to disallow communication with certain VM instances or Internal load balancers, you can install ingress firewall rules on the network you want to block the communication to. The diagram shows how you could create a firewall rule to allow all traffic from subnets 1 and 2 in Network-A to subnet 4 in Network-B and deny traffic from subnets 1 and 2 in Network-A to subnet 3 in Network-B.

## VPC Network Peering scenarios

### Shared VPC



### Multiple Network Interfaces per instance



VPC Network Peering allows peering with a Shared VPC. As discussed earlier, a shared VPC host project allows other projects to use one of its networks. In the Shared VPC diagram, Network-SVPC is in a shared VPC network in host project P1. Service projects P3 and P4 are able to attach VM instances to Network-SVPC peers with Network-A. This results in the following:

- VM instances in shared VPC service projects that are using the Network-SVPC (VM3 and VM4) have private, internal IP connectivity with any endpoints associated to Network-A.
- VM instances associated to network-A will have private, internal IP connectivity with any endpoints associated to Network-SVPC, regardless of whether they live in the host project or a service project.

You can set up VPC Network Peering between two shared VPC networks.

An instance can have multiple network interfaces, one each in different VPC networks, which is shown in the Multiple Network Interfaces per instance diagram. In the diagram, VM1 has a network interface in both network-A and network-B. Network-B is peered with another Network-C. IP3 can send traffic to IP2 because IP2 is in Network-B, and Network-B routes are automatically propagated to Network-C when the two networks are peered. For IP2 to send traffic to IP3, you'd have to configure policy routing for the IP2 interface. Flows for IP1 are not installed in Network-C, so Network-C cannot access IP1.

For more information, see:

Multiple Network Interfaces:

<https://cloud.google.com/vpc/docs/multiple-interfaces-concepts>

Configure Policy Routing:

[https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#configuring\\_policy\\_routing](https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#configuring_policy_routing)

Using VPC Network Peering: <https://cloud.google.com/vpc/docs/using-vpc-peering>

## Private Google access

- Enables virtual machine instances on a subnetwork to reach Google APIs and services using an internal IP address instead of an external IP address
- Allows VMs without internet access to reach Google services

Private Google access enables virtual machine (VM) instances on a subnetwork to reach Google APIs and services using an internal IP address instead of an external IP address. External IP addresses are routable and reachable over the internet. Internal (private) IP addresses are internal to Google Cloud Platform and are not routable or reachable over the internet. You can use Private Google access to allow VMs without internet access to reach Google services.

The services that can be reached include, but are not limited to, the following:

- Cloud Spanner
- Google Cloud BigQuery
- Google Cloud Bigtable
- Google Cloud Dataproc
- Google Cloud Datastore
- Google Cloud Pub/Sub
- Google Cloud Storage

Private Google access does not apply to Google Cloud SQL. You do not get private connectivity to Cloud SQL when you use Private Google access.

For more information, see:

Private Google Access: <https://cloud.google.com/vpc/docs/private-google-access>

Google Cloud and Developer APIs: <https://developers.google.com/apis-explorer/#p/>

Configure Private Google Access:

<https://cloud.google.com/compute/docs/private-google-access/configure-private-google-access>

Configuring IP Addresses:

<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address>

## Agenda

- Cloud Virtual Private Networks (VPN)
- Lab
- Cloud Router
- Cloud Interconnect
- External Peering
- **Cloud DNS**
- Quiz

## Cloud DNS

- Google's DNS service
  - Lookup that translates symbolic names to IP addresses
  - High-performance DNS lookup for your users
  - Cost-effective for massive updates (millions of records)
- Manage DNS records through API or web UI
- Request routed to the nearest location, reducing latency
- Use cases
  - DNS resolver for your company's users w/o managing your own servers
  - DNS propagation of company DNS records

Requests are automatically routed to the nearest location, reducing latency and improving authoritative name lookup performance for your users.

For more information, see: <https://cloud.google.com/dns/overview>



## Cloud DNS managed zones

- An abstraction that manages all DNS records for a single domain name
- One project may have multiple managed zones
- Must enable the Cloud DNS API in GCP Console first
  - `gcloud dns managed-zones ...`
- Managed zones
  - Permission controls at project level
  - Monitor propagation of changes to DNS name servers

For more information, see: <https://cloud.google.com/dns/zones/>

## Agenda

- Cloud Virtual Private Networks (VPN)
- Lab
- Cloud Router
- Cloud Interconnect
- External Peering
- Cloud DNS
- **Quiz**

## More resources

Cloud VPN

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

Cloud Router

<https://cloud.google.com/compute/docs/cloudrouter>

Cloud Interconnect

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

Direct Peering

<https://cloud.google.com/interconnect/direct-peering>

Cloud DNS

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



© 2018 Google LLC. All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.