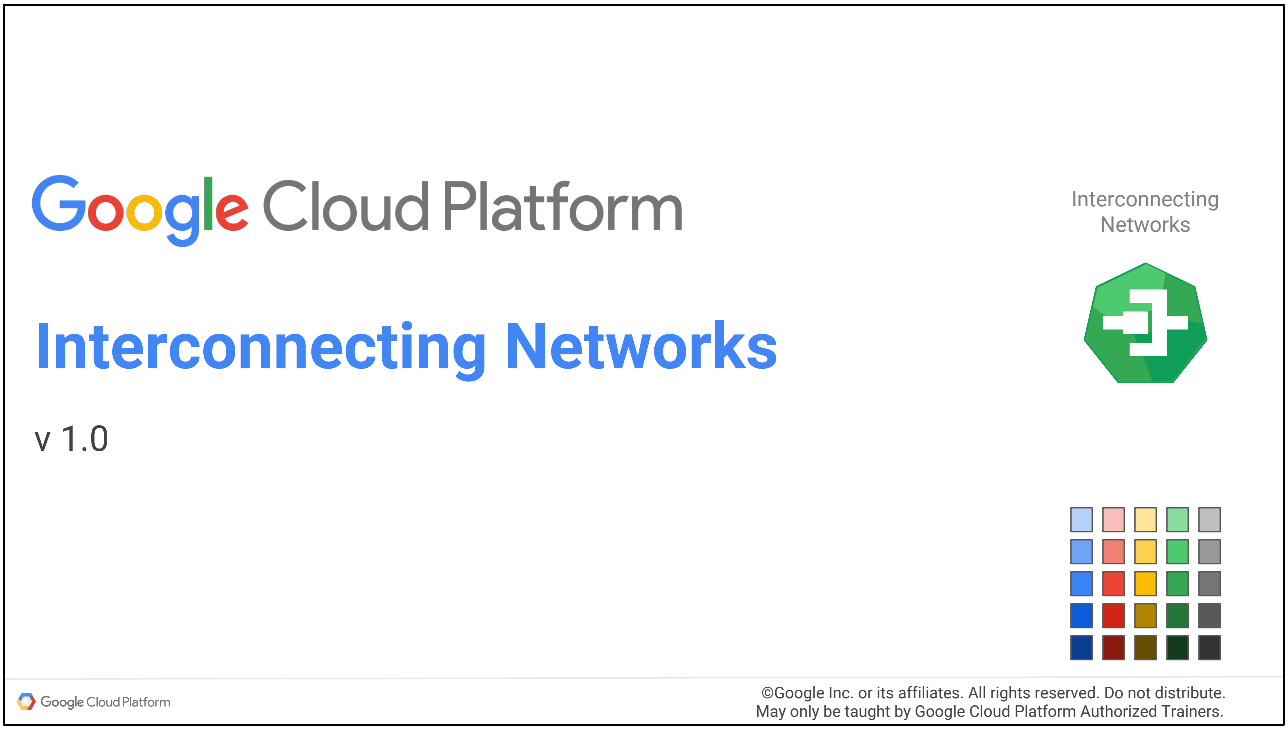


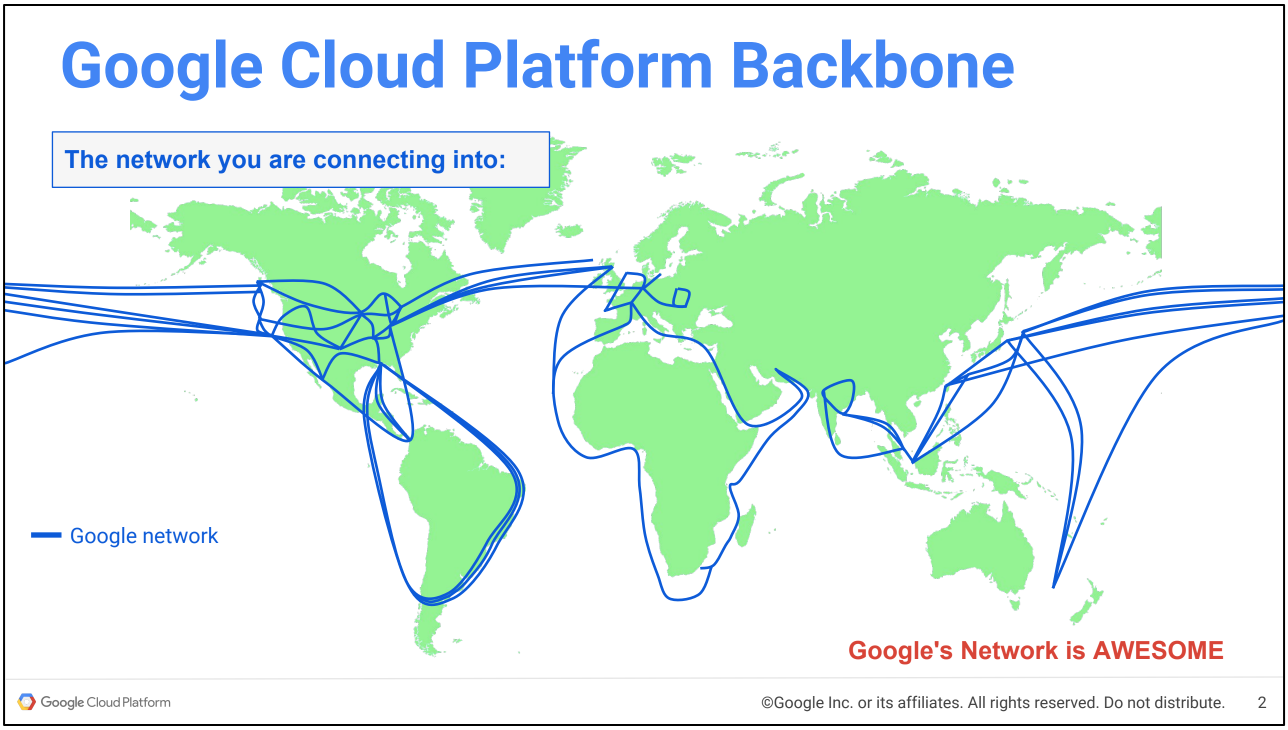
Google Cloud Platform

Interconnecting Networks

v 1.0

Interconnecting Networks

Google Cloud Platform



Google Cloud Platform Backbone

The network you are connecting into:

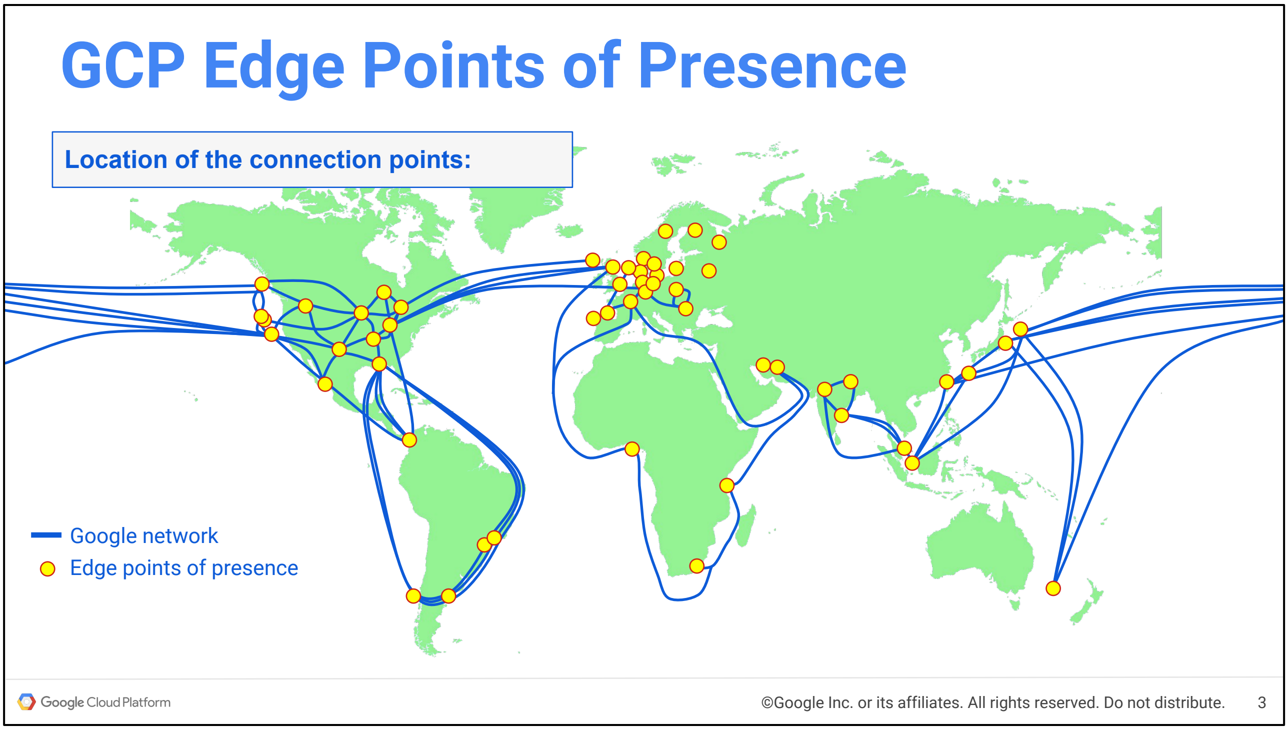
▬ Google network

Google's Network is AWESOME

Google Cloud Platform

A global network.
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/

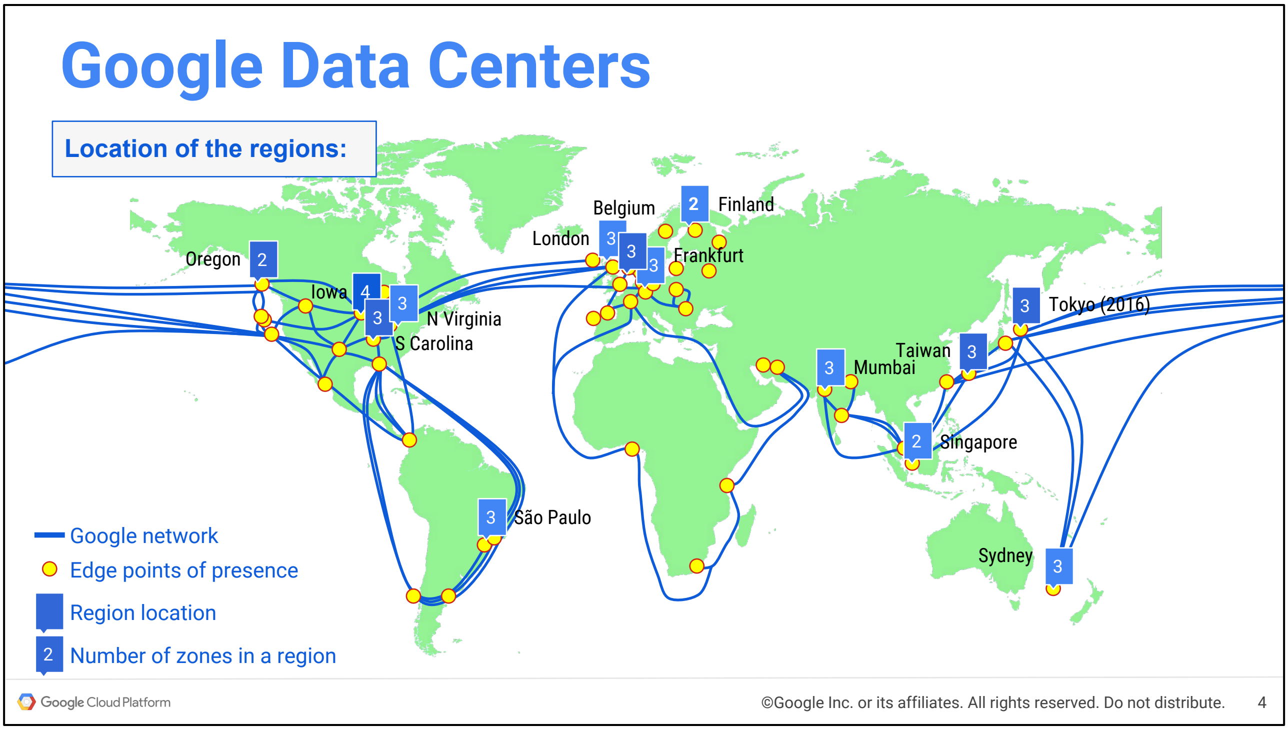


GCP Edge Points of Presence

Location of the connection points:

Google Cloud Platform

https://peeringdb.com/asn/15169



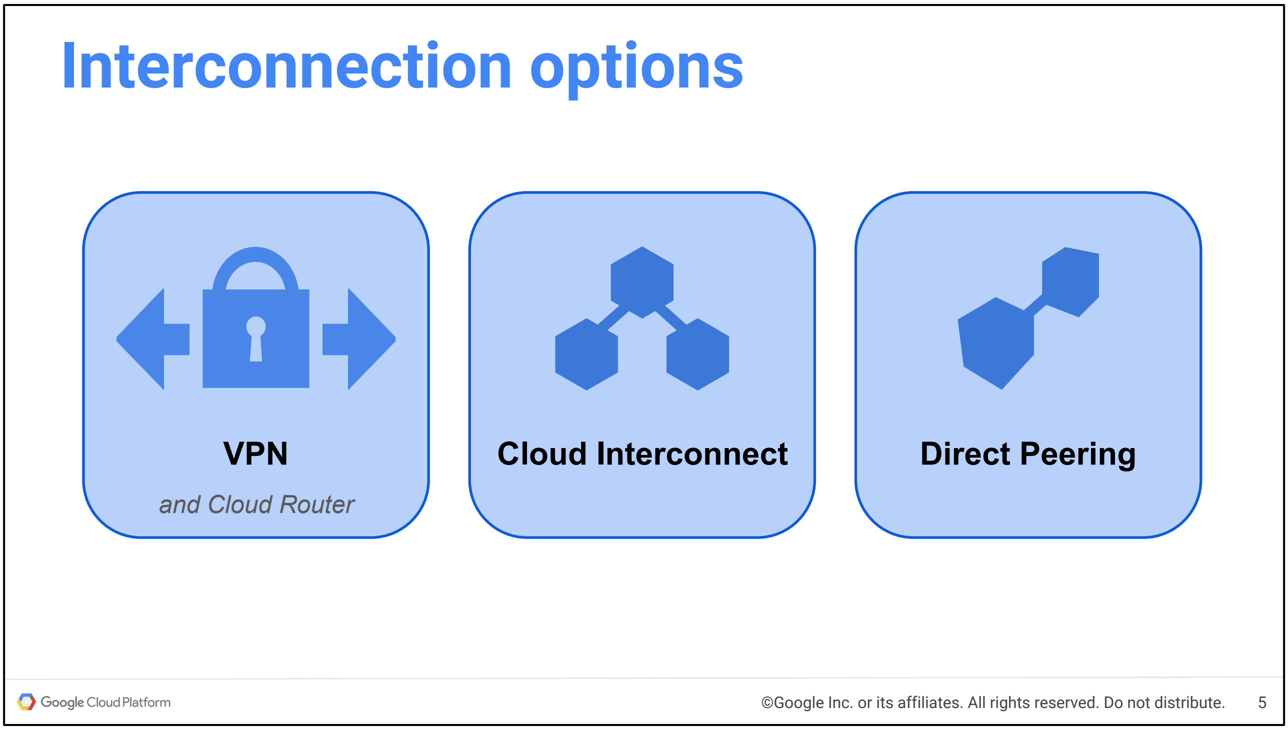
Google Data Centers

Location of the regions:

- ▬ Google network
- ● Edge points of presence
- ▮ Region location
- 2 Number of zones in a region

Google Cloud Platform

Existing and announced regions.
https://cloud.google.com/compute/docs/regions-zones/regions-zones



Interconnection options

VPN

and Cloud Router

Cloud Interconnect

Direct Peering

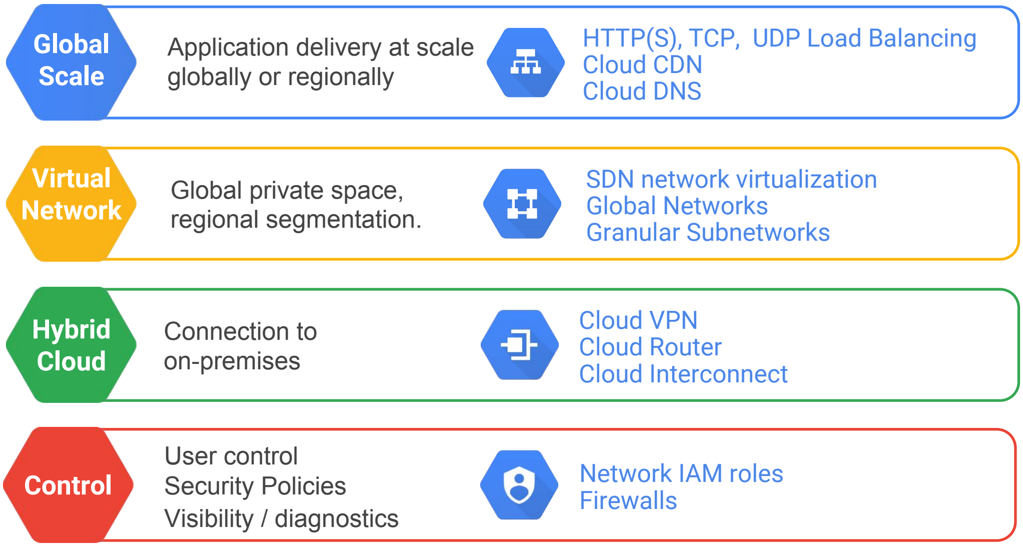
Google Cloud Platform

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

Google Cloud Networking



Global Scale

Application delivery at scale globally or regionally

HTTP(S), 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

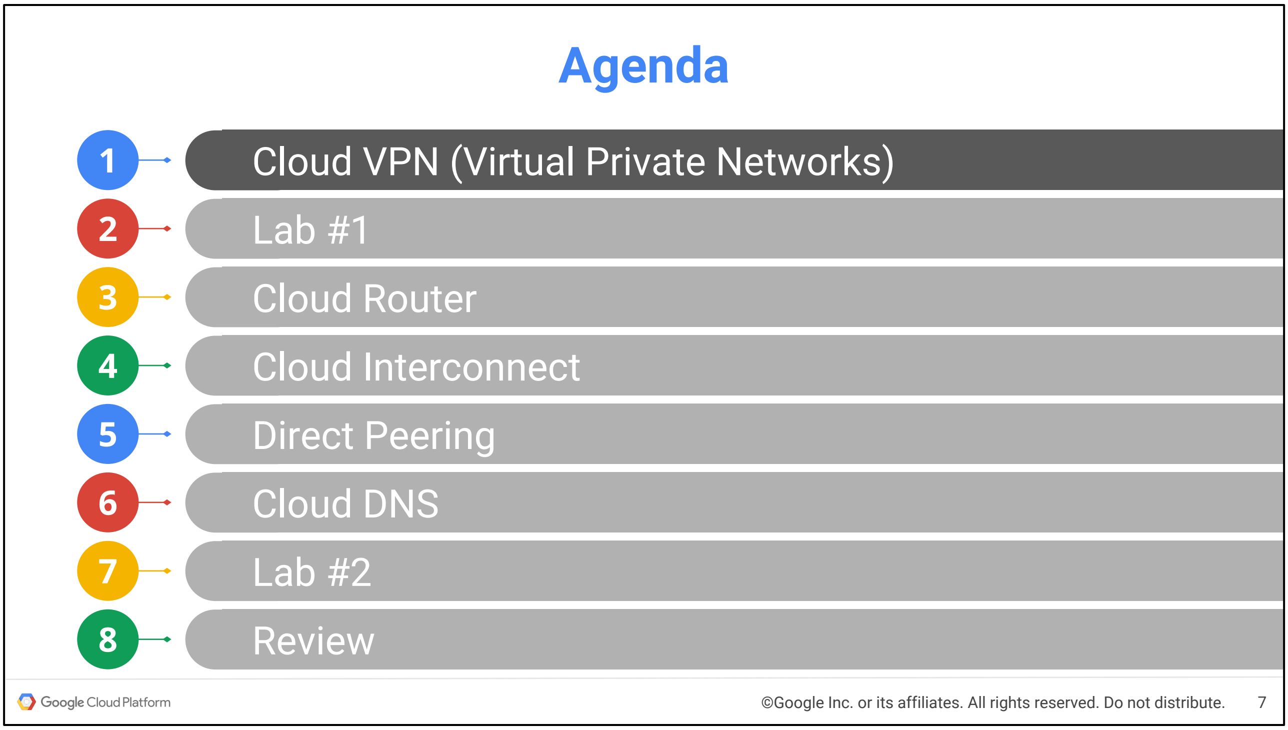
Cloud VPN
Cloud Router
Cloud Interconnect

Control

User control
Security Policies
Visibility / diagnostics

Network IAM roles
Firewalls

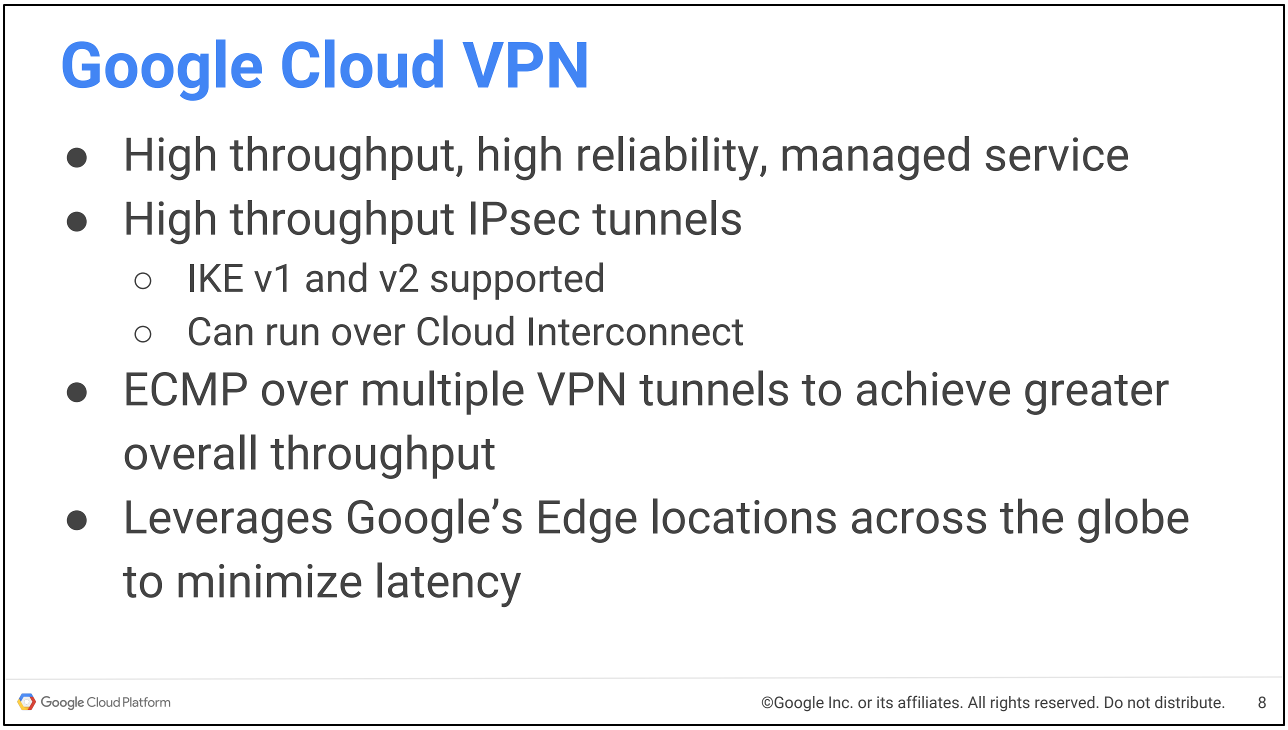
Google Cloud Platform



Agenda

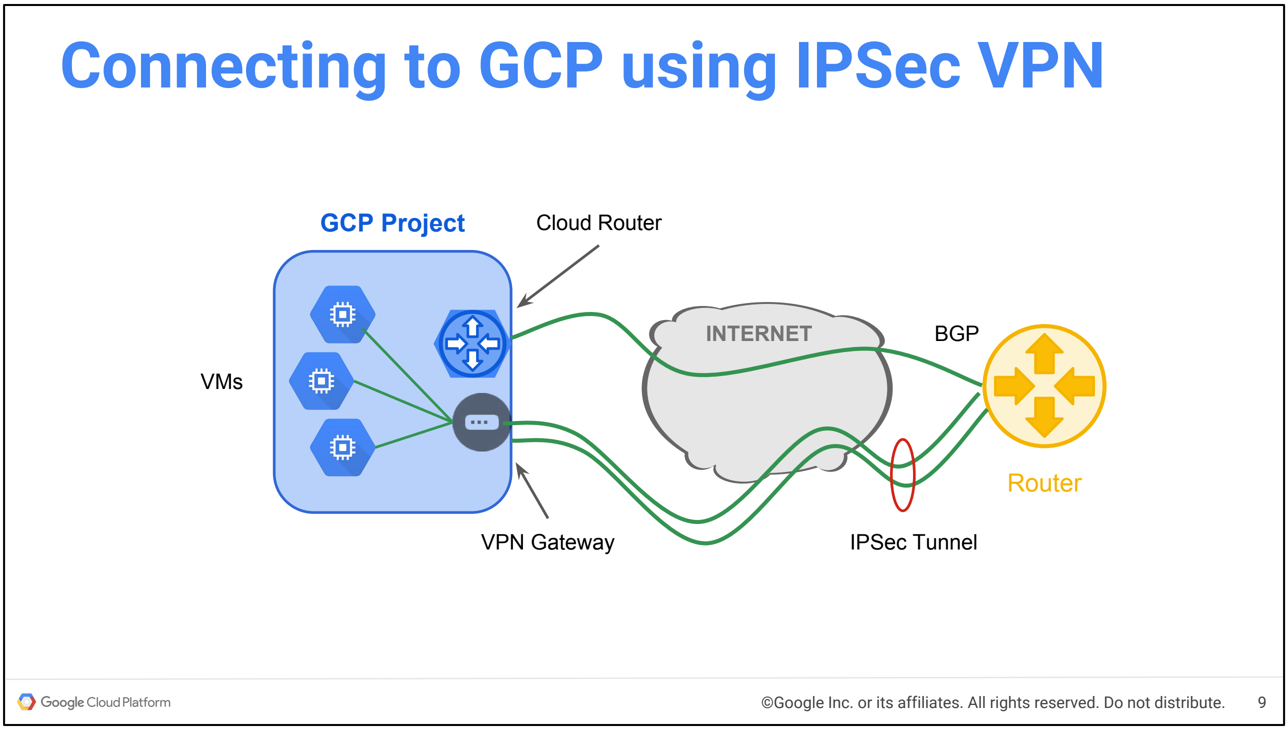
1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review

Google Cloud Platform



Google Cloud VPN

- 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



Connecting to GCP using IPSec VPN

GCP Project

Cloud Router

VMs

INTERNET

BGP

Router

VPN Gateway

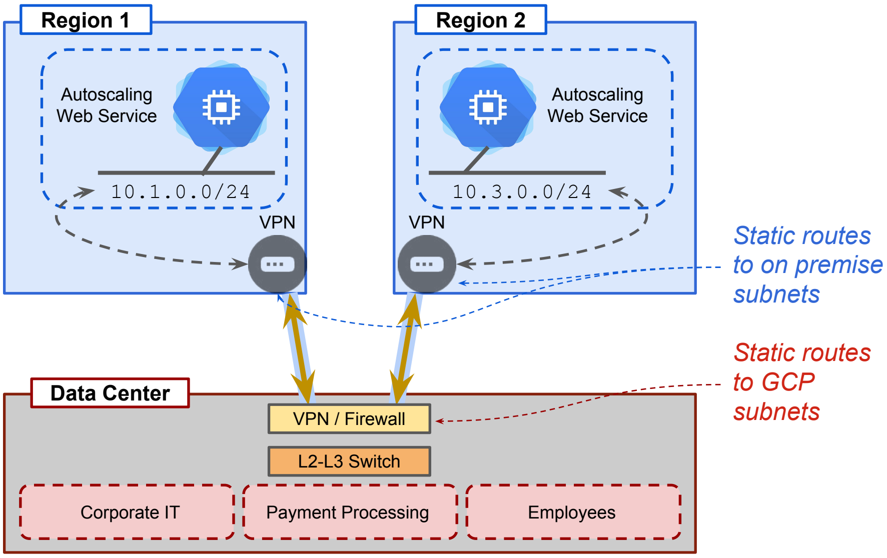
IPSec Tunnel

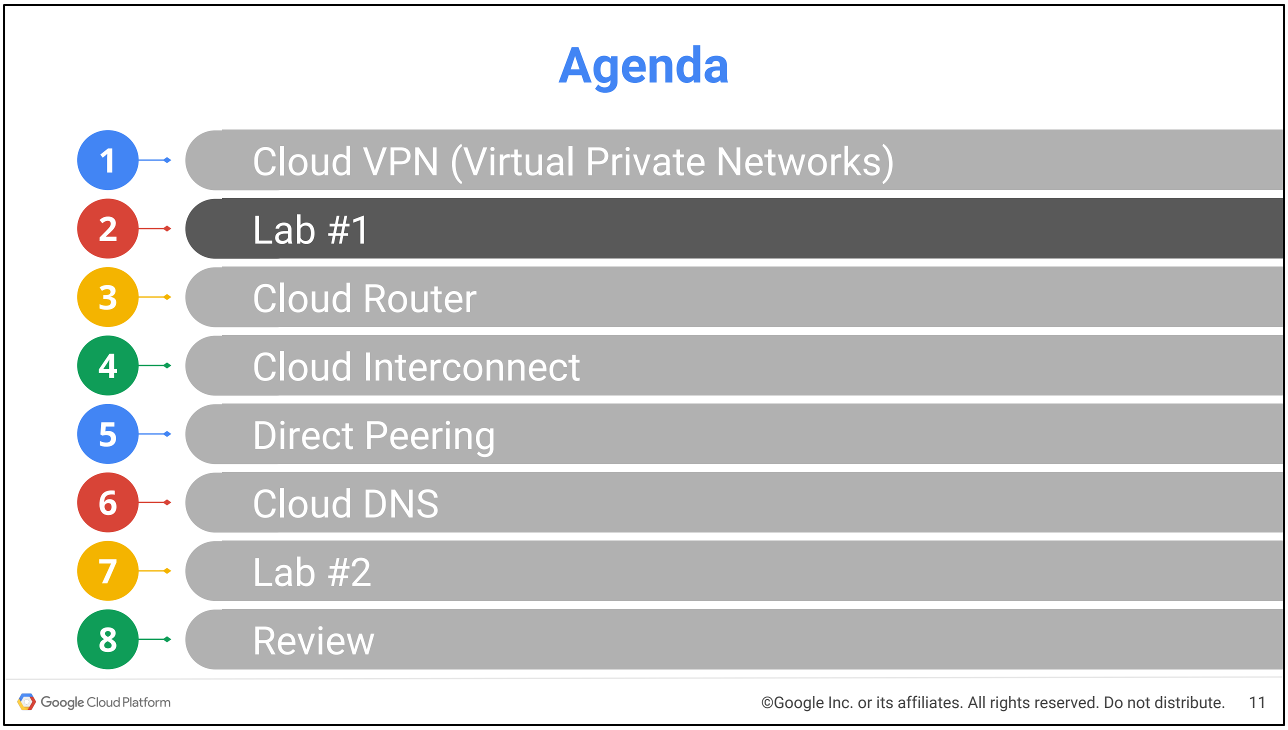
Google Cloud Platform

- Supports private addressing (RFC1918) in an on premise to GCP project network
- A separate instance of Cloud Router/VPN Gateway is required in each region
- BGP only advertises routes in local subnet
- Required for authenticated and encrypted traffic over unsecured links
- ~3Gbps per tunnel - multiple tunnels with ECMP can increase aggregate throughput
- Guides for 3rd Party devices are available at: https://cloud.google.com/compute/docs/vpn/interop-guides

Cloud VPN with static routes

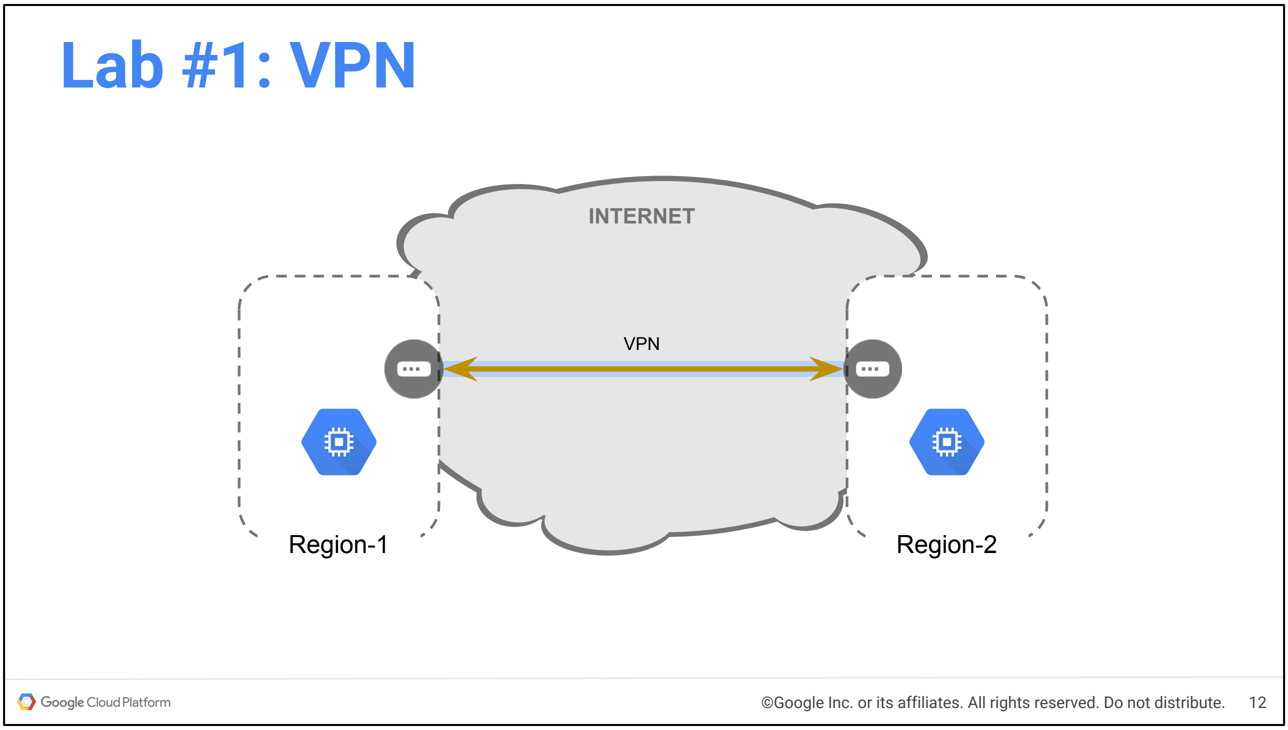
- Public IP on both peers
- Global or Regional
- 1.5 Gbps throughput
- Secret password
- Scale horizontally through parallel tunnels





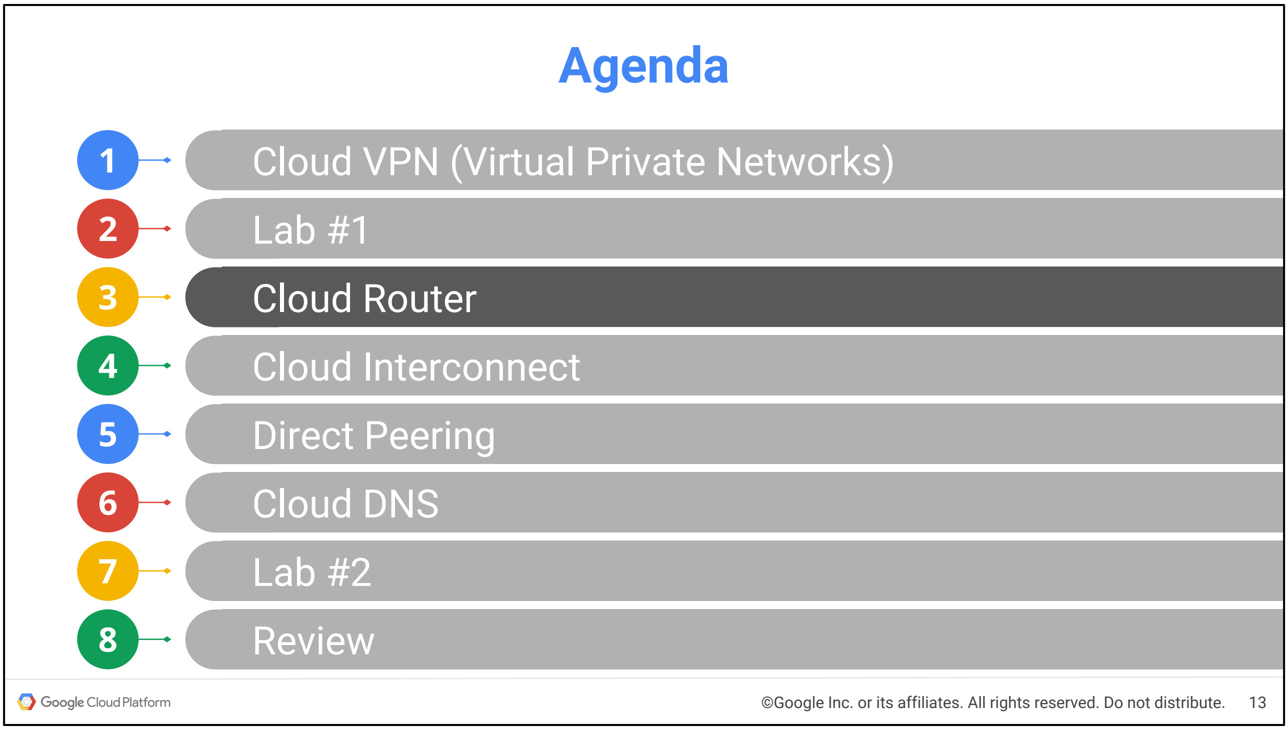
Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review



Lab #1: VPN

08-1 Virtual Private Networks (VPN)



Agenda

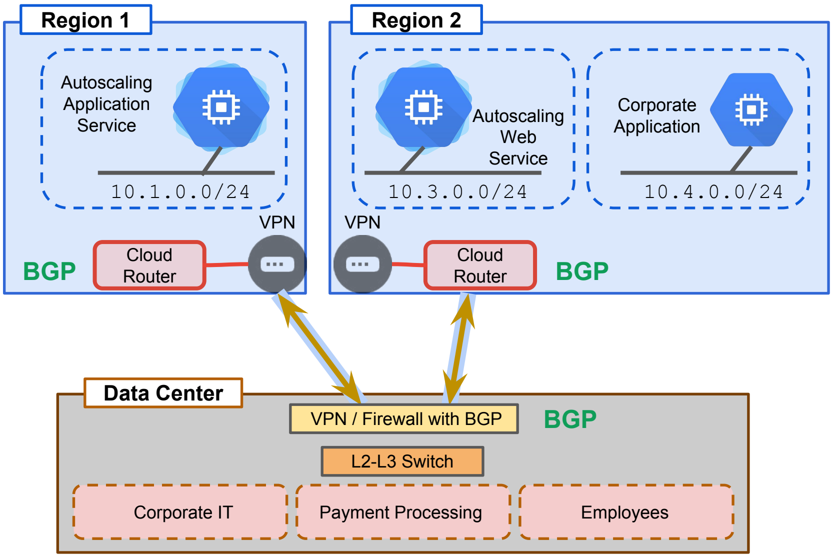
1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. **Cloud Router**
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review

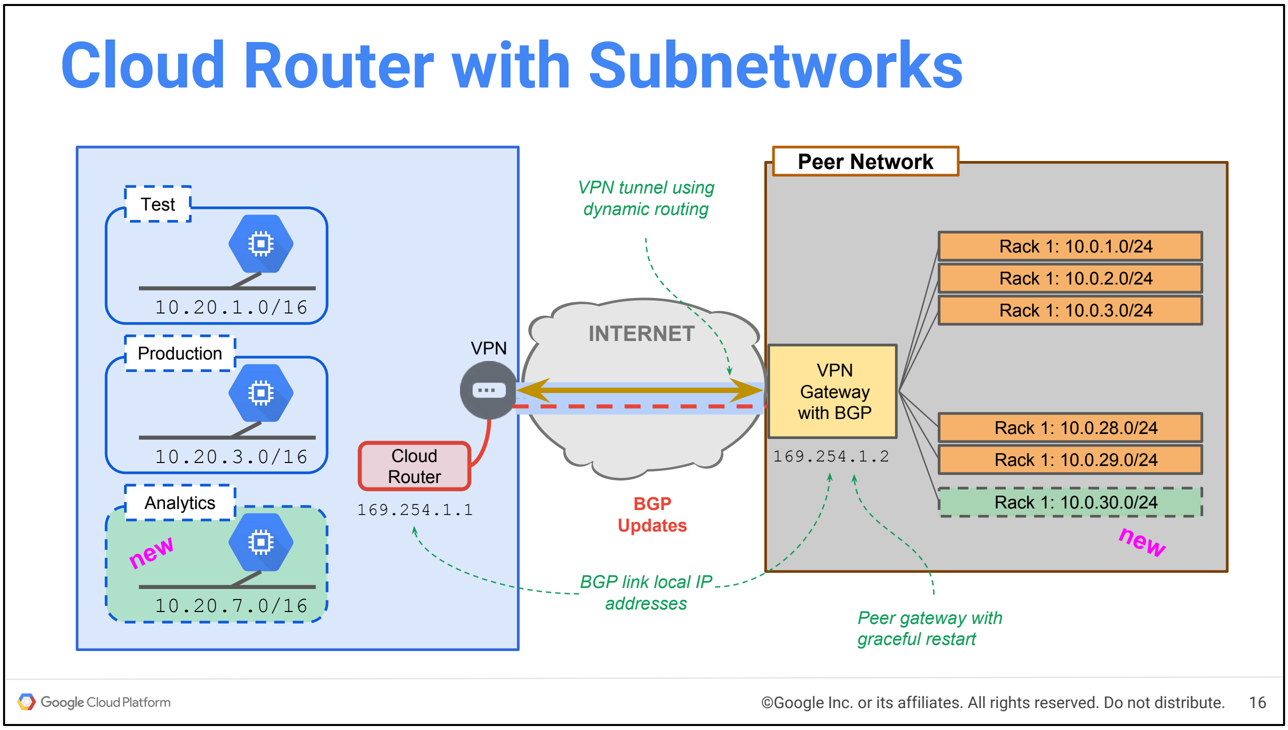
Cloud Router

- 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

Test

10.20.1.0/16

Production

10.20.3.0/16

Analytics

new

10.20.7.0/16

VPN

Cloud Router

169.254.1.1

VPN tunnel using dynamic routing

INTERNET

BGP Updates

BGP link local IP addresses

Peer Network

VPN Gateway with BGP

169.254.1.2

Rack 1: 10.0.1.0/24

Rack 1: 10.0.2.0/24

Rack 1: 10.0.3.0/24

Rack 1: 10.0.28.0/24

Rack 1: 10.0.29.0/24

Rack 1: 10.0.30.0/24

new

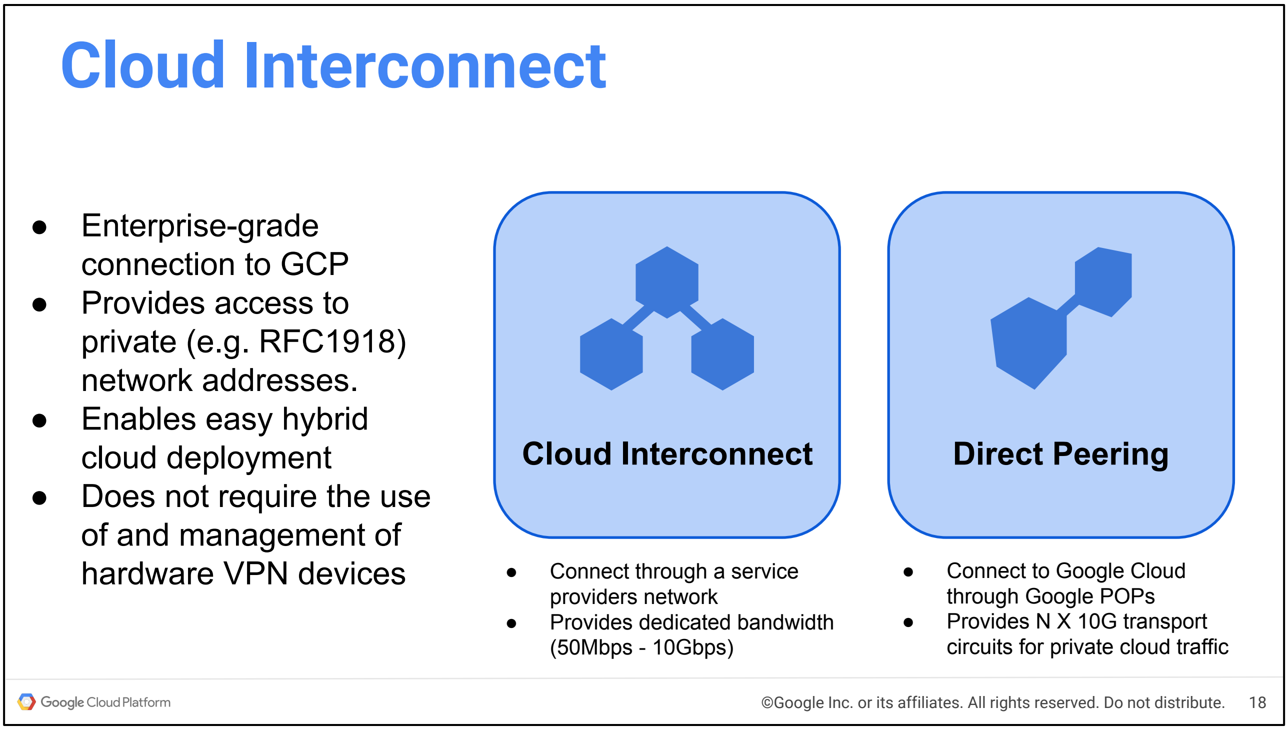
Peer gateway with graceful restart

Google Cloud Platform

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

Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review



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)

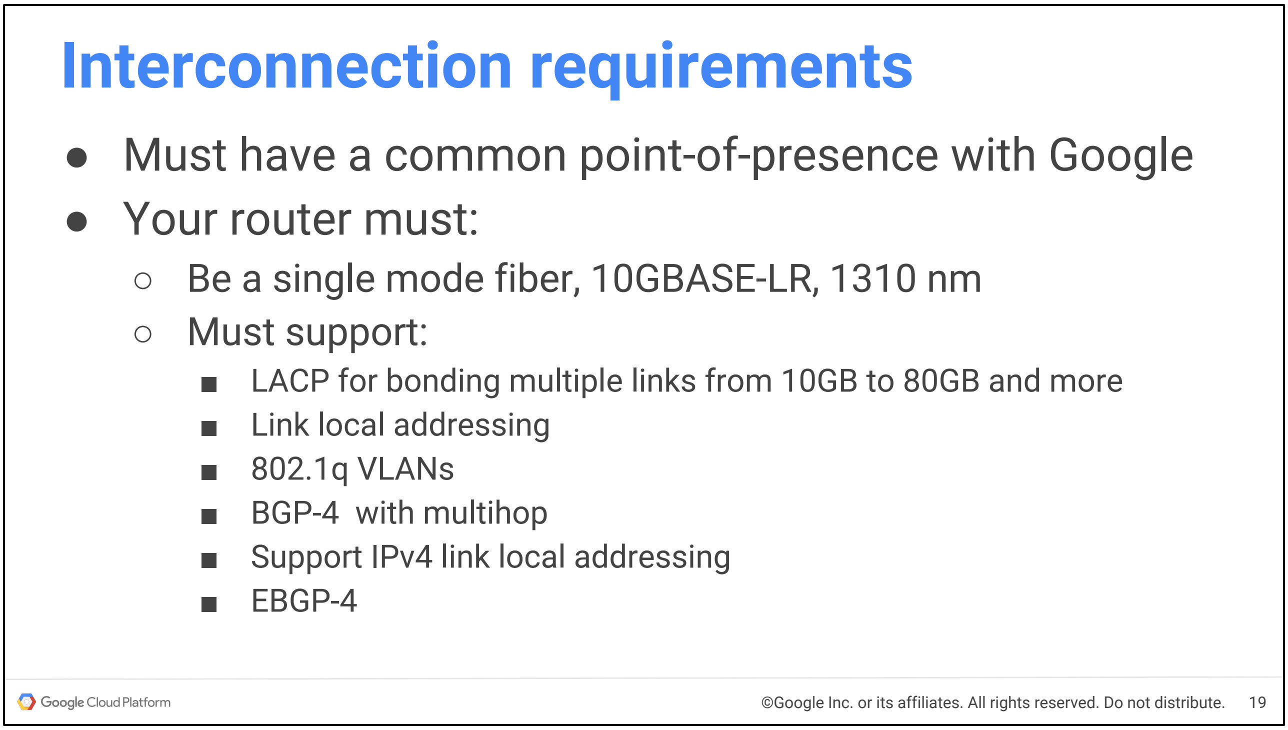
Direct Peering

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

Google Cloud Platform

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

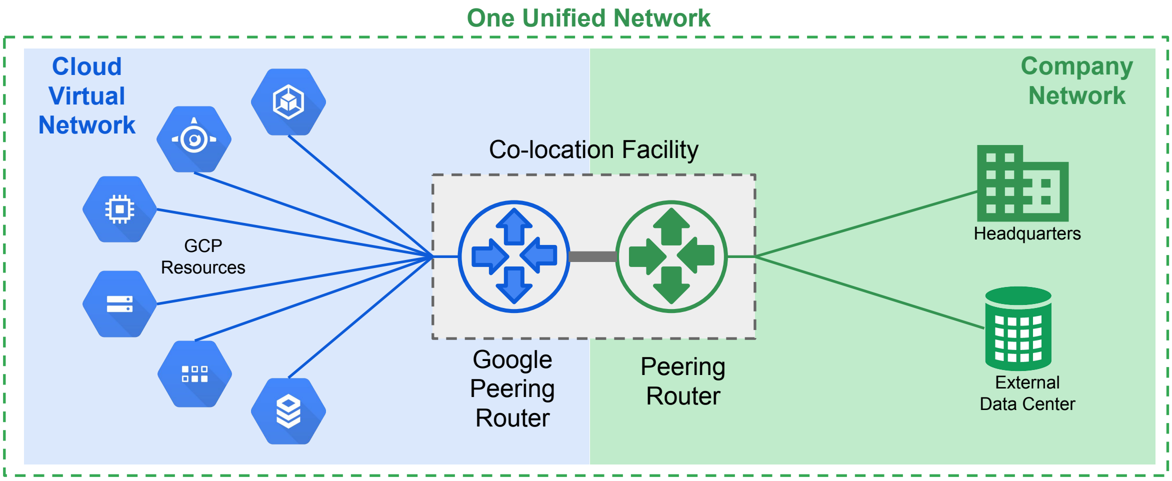


Interconnection requirements

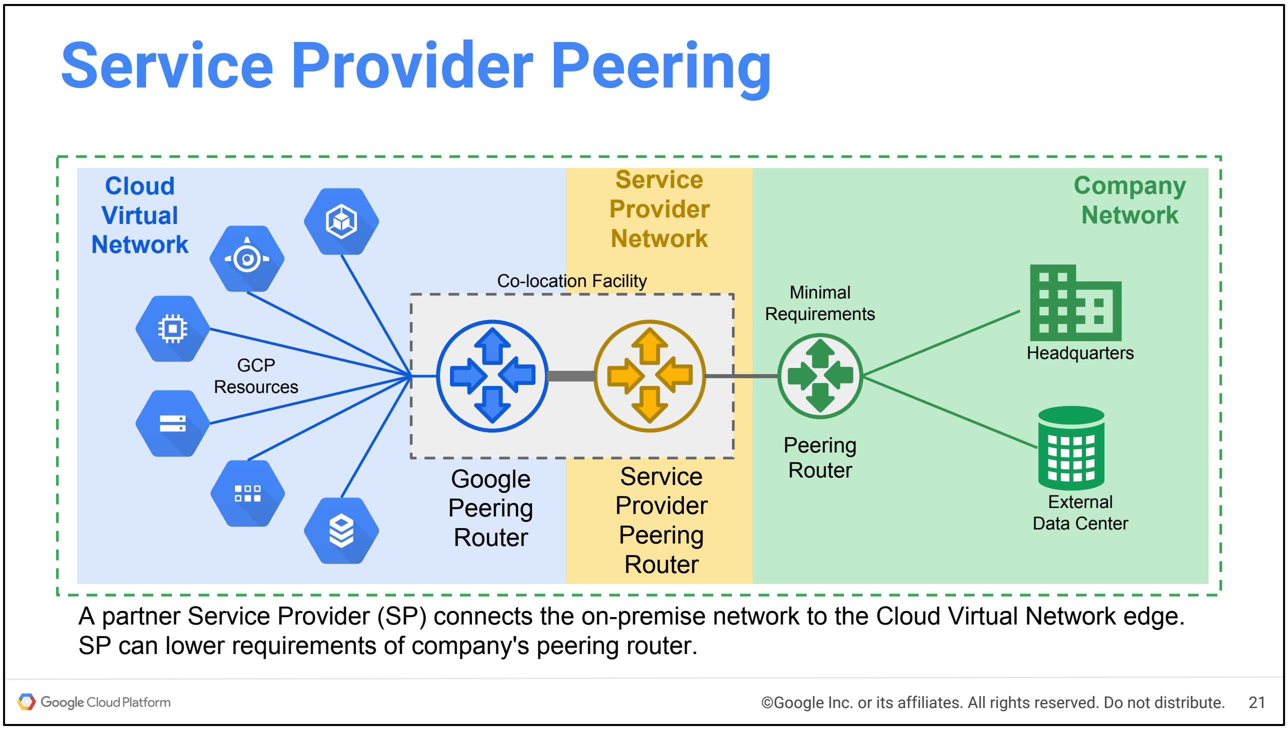
- Must have a common point-of-presence with Google
- Your router must:
  - Be a single mode fiber, 10GBASE-LR, 1310 nm
  - Must support:
    - LACP for bonding multiple links from 10GB to 80GB and more
    - Link local addressing
    - 802.1q VLANs
    - BGP-4 with multihop
    - Support IPv4 link local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

Google Cloud Platform

Direct Peering



Direct physical connection between an on-premise network and the Cloud Virtual Network edge. Extends your private network into your cloud network.

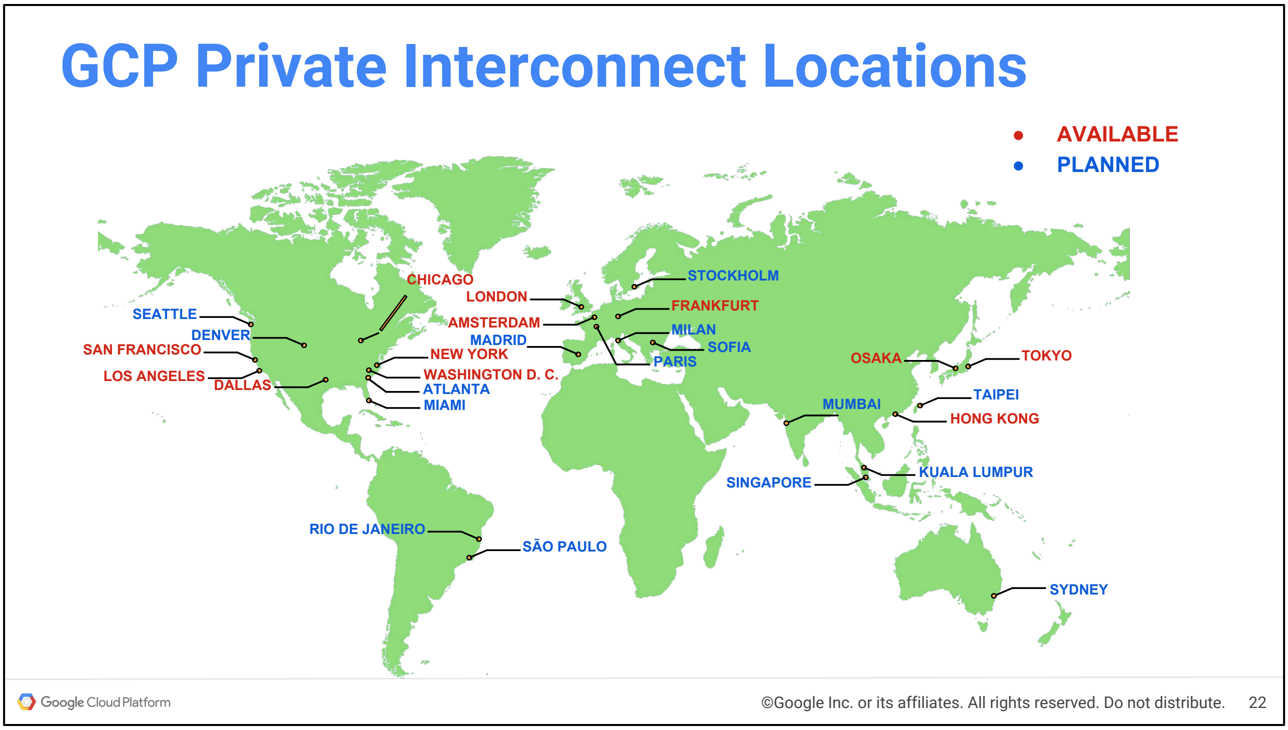


Service Provider Peering

A partner Service Provider (SP) connects the on-premise network to the Cloud Virtual Network edge.
SP can lower requirements of company's peering router.

Google Cloud Platform

For example, the company network might only need to have an Ethernet



GCP Private Interconnect Locations

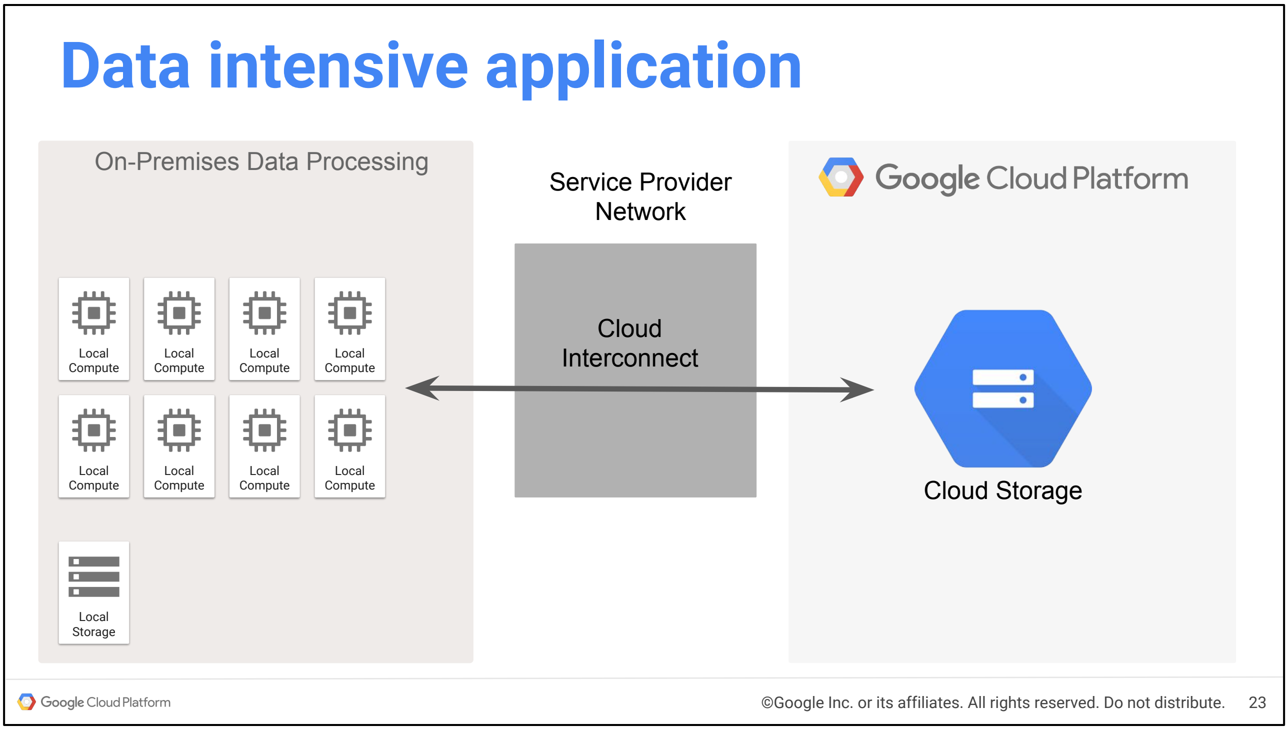
● AVAILABLE

● PLANNED

Google Cloud Platform

©Google Inc. or its affiliates. All rights reserved. Do not distribute. 22

The map comes from Google's presentation style guide: https://docs.google.com/presentation/d/13F3QCHra3T2n3m3QE-ZIcWytMzw8kwWLH90HQvwsJYU/edit#slide=id.g899806071_0_24



Data intensive application

On-Premises Data Processing

Local Compute

Local Compute

Local Compute

Local Compute

Local Compute

Local Compute

Local Compute

Local Compute

Local Storage

Service Provider Network

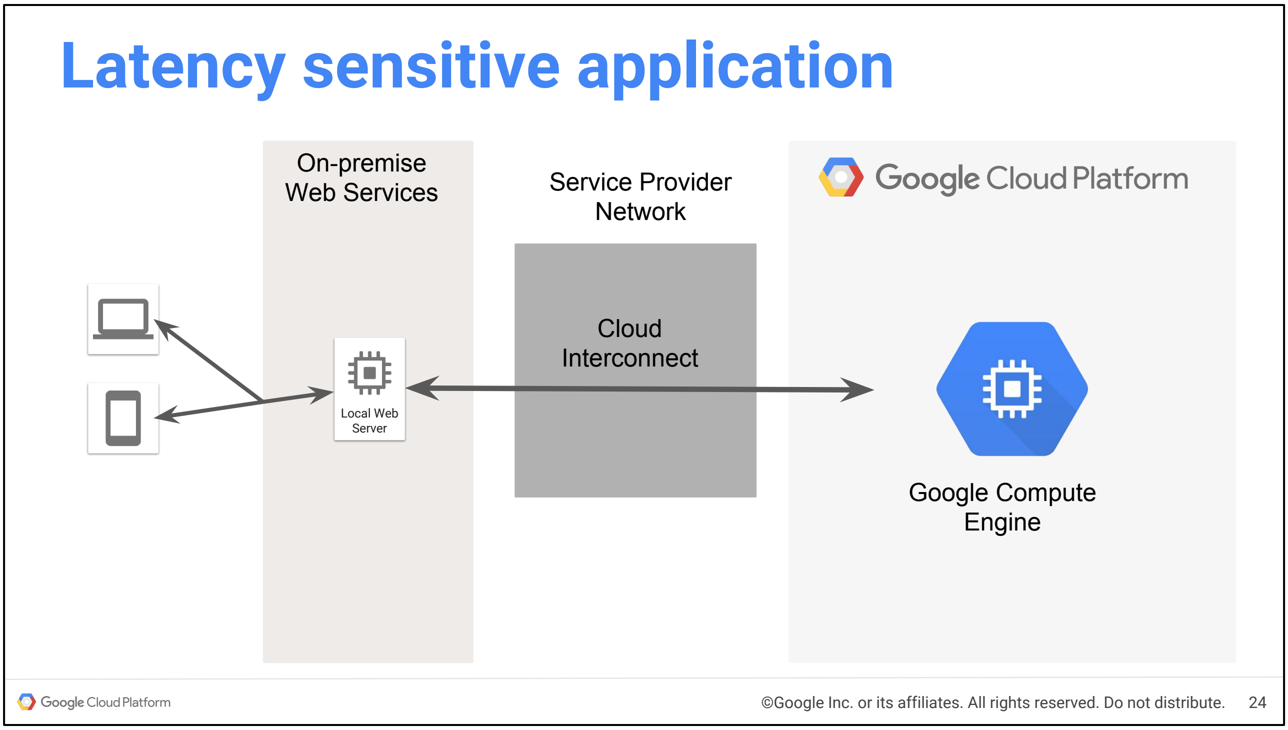
Cloud Interconnect

Google Cloud Platform

Cloud Storage

Google Cloud Platform

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



Latency sensitive application

On-premise Web Services

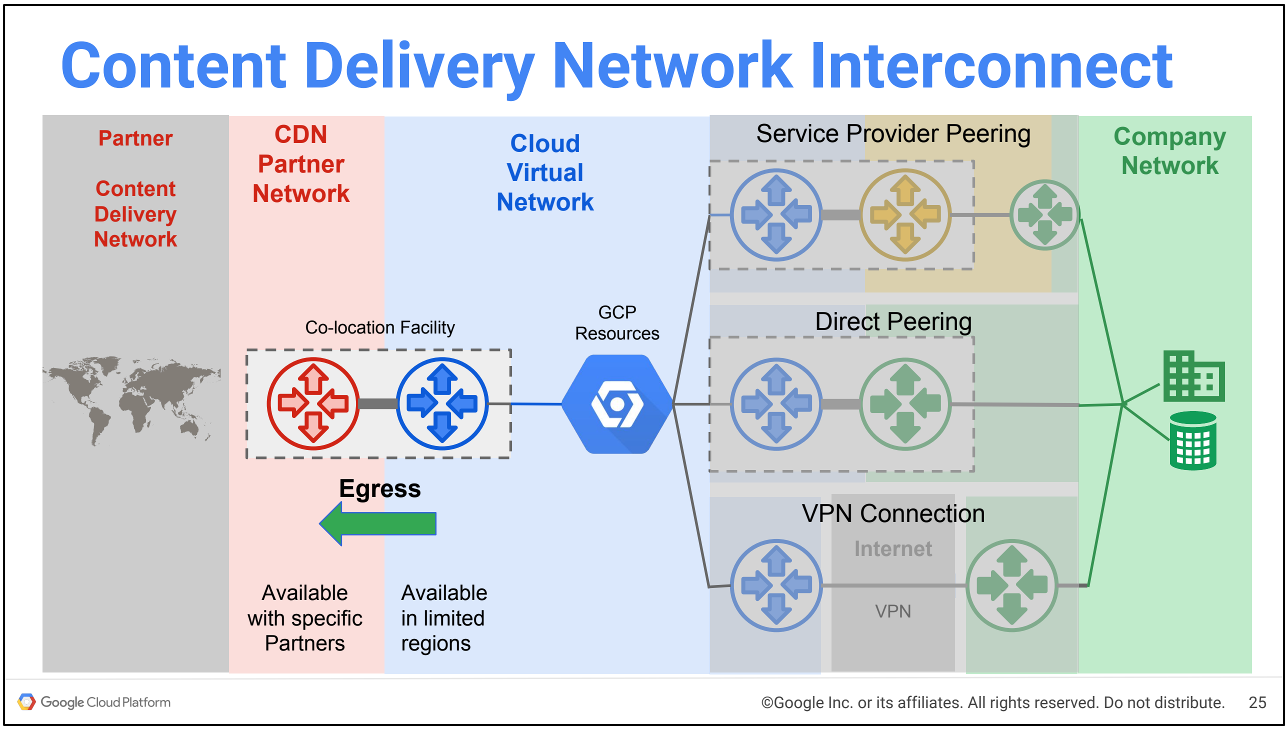
Service Provider Network

Google Cloud Platform

Cloud Interconnect

Google Compute Engine

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



Content Delivery Network Interconnect

Partner

Content Delivery Network

CDN Partner Network

Cloud Virtual Network

Service Provider Peering

Company Network

Co-location Facility

GCP Resources

Direct Peering

Egress

VPN Connection

Internet

VPN

Available with specific Partners

Available in limited regions

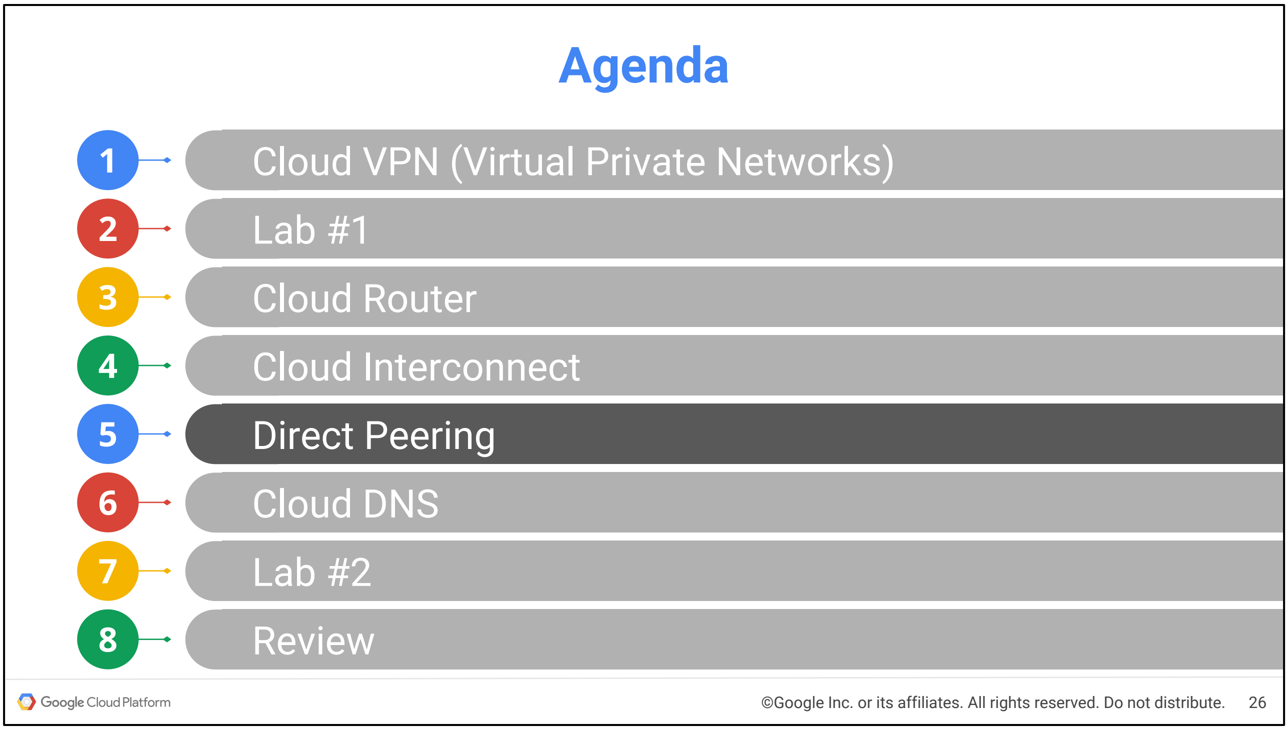
Google Cloud Platform

https://cloud.google.com/interconnect/cdn-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

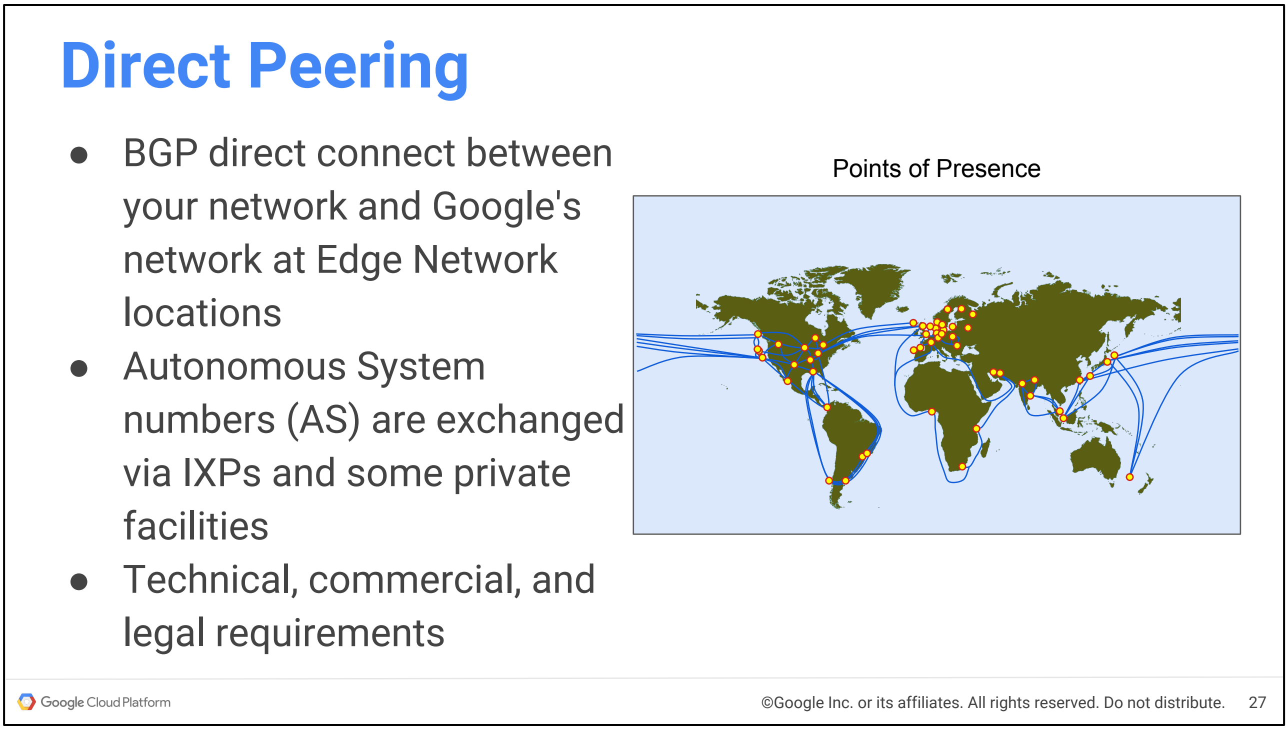
CDN Interconnect is about Egress from the Cloud Virtual Network. Select CDN Partner Providers have direct egress capability to access their global Content Delivery Network. Note that Google has its own Content Delivery Network service. However, if you choose to use a different CDN provider, we have a 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



Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review



Direct Peering

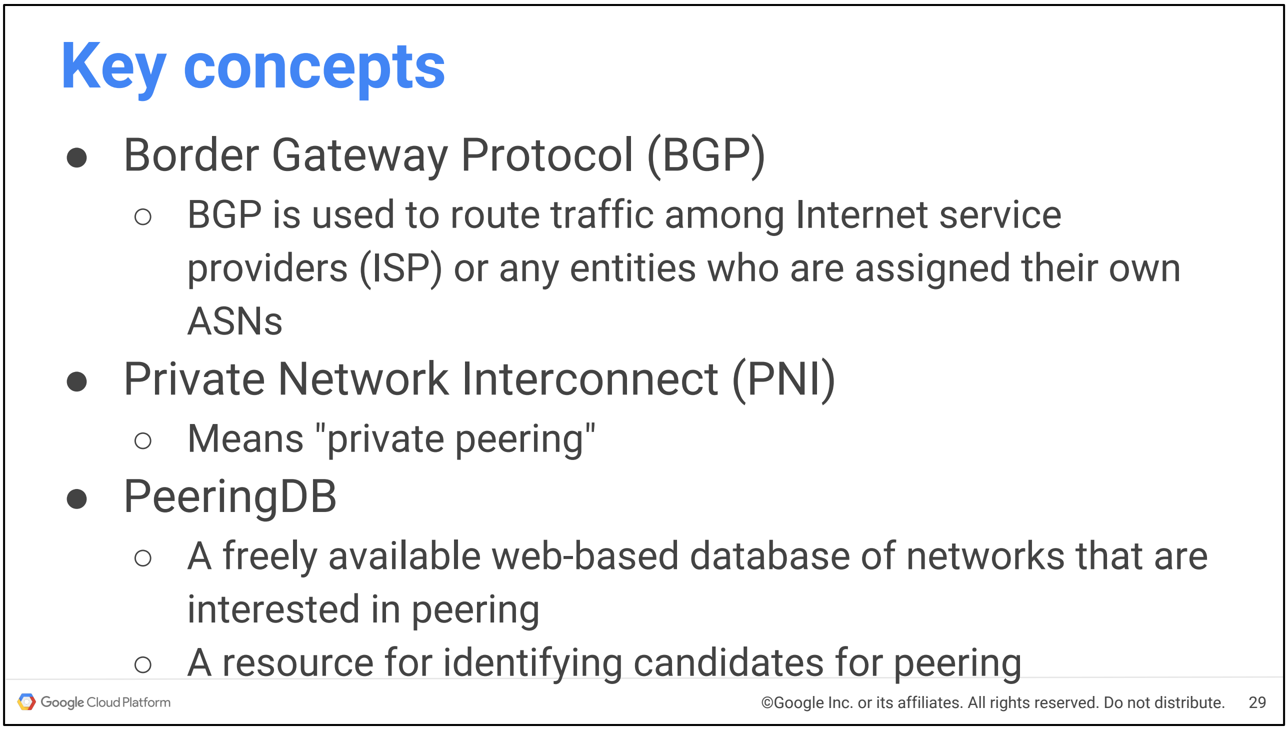
- BGP direct connect between your network and Google's network at Edge Network locations
- Autonomous System numbers (AS) are exchanged via IXPs and some private facilities
- Technical, commercial, and legal requirements

Points of Presence

Our Edge point of presence (PoPs) are where we connect Google's network to the rest of the internet via peering. We are 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.

Autonomous System (AS)

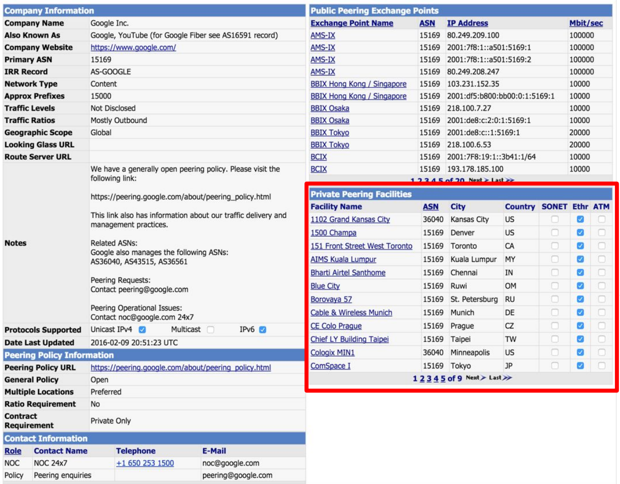
- AS represents a collection of Internet Protocol (IP) routing prefixes under the control of an administrative entity representing one or more network operators
- ASN refers to AS number, which is allocated by Internet Assigned Numbers Authority (IANA)
- A business entity with an assigned ASN generally 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	
Company Name	Google Inc.
Also Known As	Google, YouTube (for Google Fiber see AS16591 record)
Company Website	https://www.google.com/
Primary ASN	15169
IRR Record	AS-GOOGLE
Network Type	Content
Approx Prefixes	15000
Traffic Levels	Not Disclosed
Traffic Ratios	Mostly Outbound
Geographic Scope	Global
Looking Glass URL	
Route Server URL	
Notes	We have a generally open peering policy. Please visit the following link: https://peering.google.com/about/peering_policy.html This link also has information about our traffic delivery and management practices. Related ASNs: Google also manages the following ASNs: AS36040, AS43515, AS36561 Peering Requests: Contact peering@google.com Peering Operational Issues: Contact noc@google.com 24x7
Protocols Supported	Unicast IPv4 ☑ Multicast □ IPv6 ☑
Date Last Updated	2016-02-09 20:51:23 UTC

Peering Policy Information	
Peering Policy URL	https://peering.google.com/about/peering_policy.html
General Policy	Open
Multiple Locations	Preferred
Ratio Requirement	No
Contract Requirement	Private Only

Contact Information

Role	Contact Name	Telephone	E-Mail
NOC	NOC 24x7	+1 650 253 1500	noc@google.com
Policy	Peering enquiries		peering@google.com

Public Peering Exchange Points

Exchange Point Name	ASN	IP Address	Mbit/sec
AMS-IX	15169	80.249.209.100	100000
AMS-IX	15169	2001:7f8:1::a501:5169:1	100000
AMS-IX	15169	2001:7f8:1::a501:5169:2	100000
AMS-IX	15169	80.249.208.247	100000
BBIX Hong Kong / Singapore	15169	103.231.152.35	10000
BBIX Hong Kong / Singapore	15169	2001:df5:b800:bb00:0:1:5169:1	10000
BBIX Osaka	15169	218.100.7.27	10000
BBIX Osaka	15169	2001:de8:c:2:0:1:5169:1	10000
BBIX Tokyo	15169	2001:de8:c::1:5169:1	20000
BBIX Tokyo	15169	218.100.6.53	20000
BCIX	15169	2001:7F8:19:1::3b41:1/64	10000
BCIX	15169	193.178.185.100	10000

1 2 3 4 5 of 20 Next > Last >>

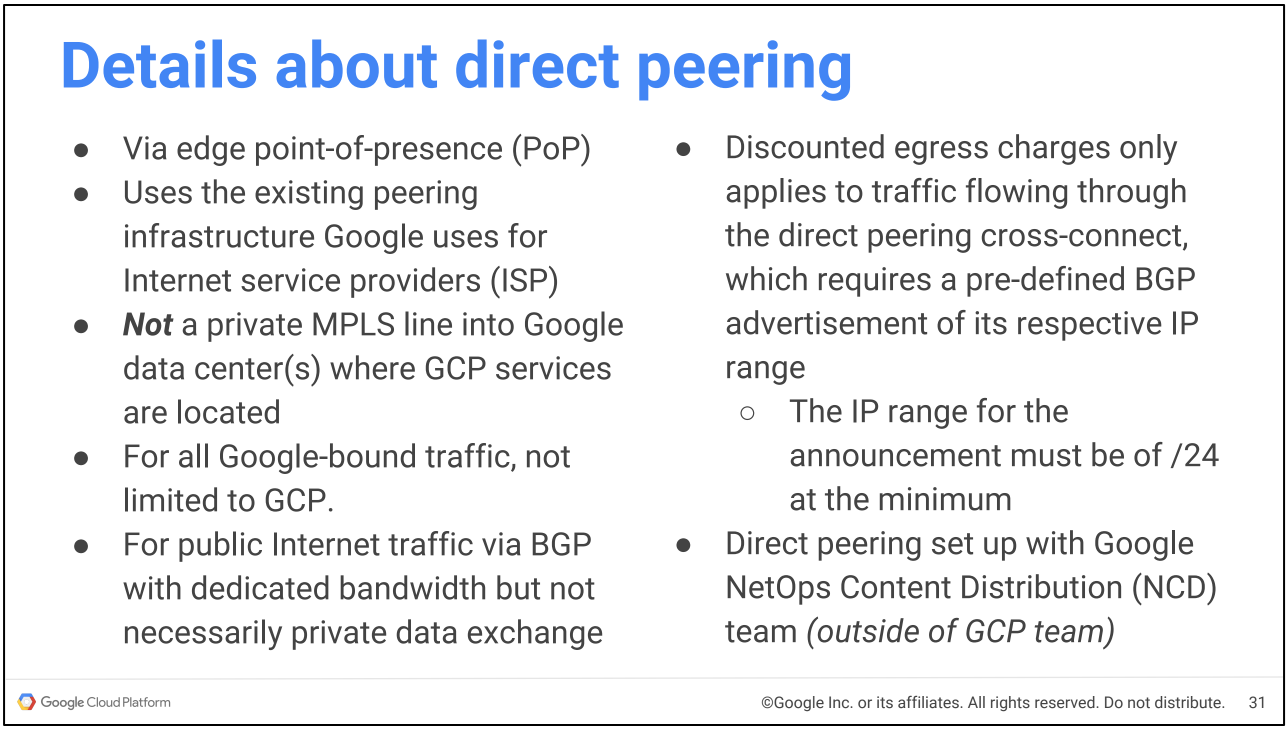
Private Peering Facilities

Facility Name	ASN	City	Country	SONET	Ethr	ATM
1102 Grand Kansas City	36040	Kansas City	US	□	☑	□
1500 Champa	15169	Denver	US	□	☑	□
151 Front Street West Toronto	15169	Toronto	CA	□	☑	□
AIMS Kuala Lumpur	15169	Kuala Lumpur	MY	□	☑	□
Bharti Airtel Santhome	15169	Chennai	IN	□	☑	□
Blue City	15169	Ruwi	OM	□	☑	□
Borovaya 57	15169	St. Petersburg	RU	□	☑	□
Cable & Wireless Munich	15169	Munich	DE	□	☑	□
CE Colo Prague	15169	Prague	CZ	□	☑	□
Chief LY Building Taipei	15169	Taipei	TW	□	☑	□
Cologix MIN1	36040	Minneapolis	US	□	☑	□
ComSpace I	15169	Tokyo	JP	□	☑	□

1 2 3 4 5 of 9 Next > Last >>

Peering locations

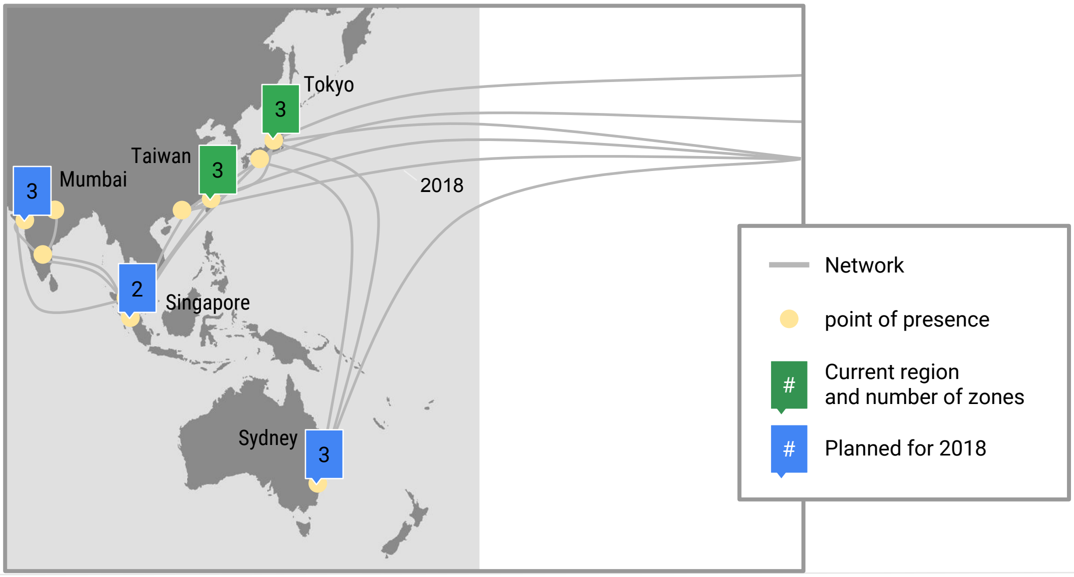
https://www.peeringdb.com/view.php?asn=15169

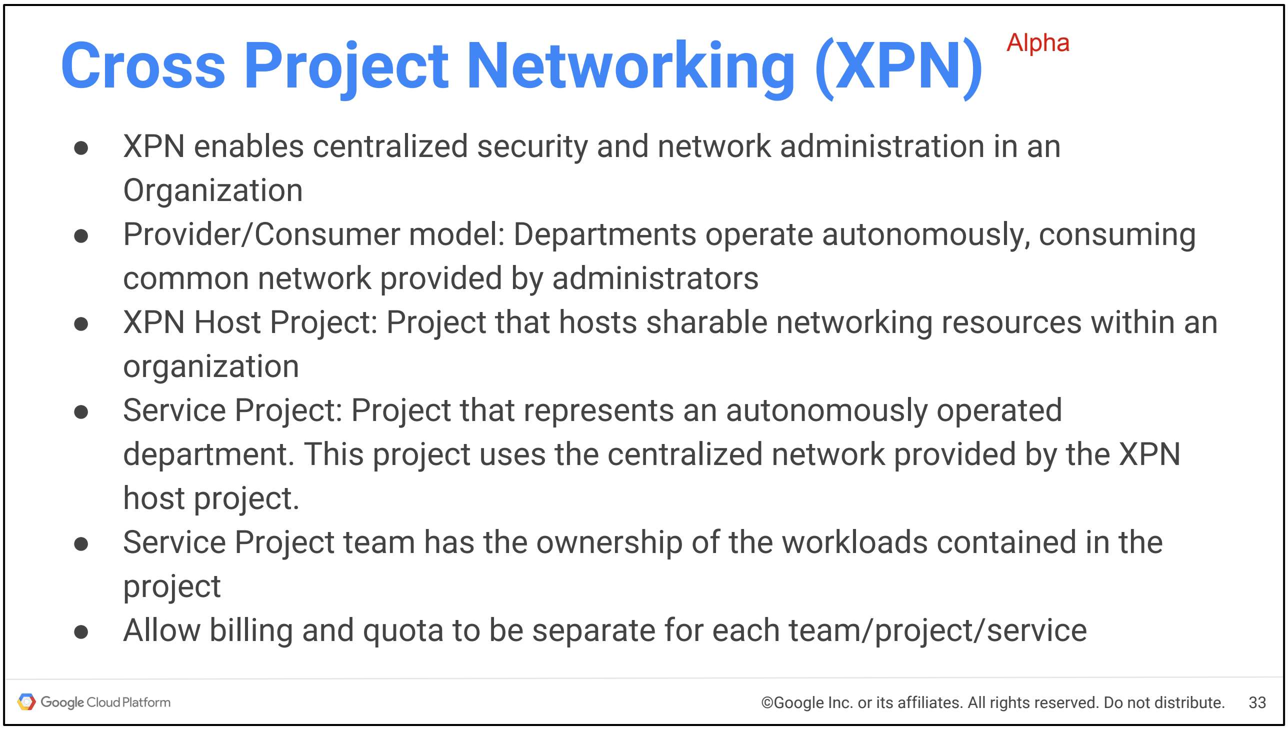


Details about direct peering

- 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 center(s) 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 applies 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)*

GCP in the Pacific (details)





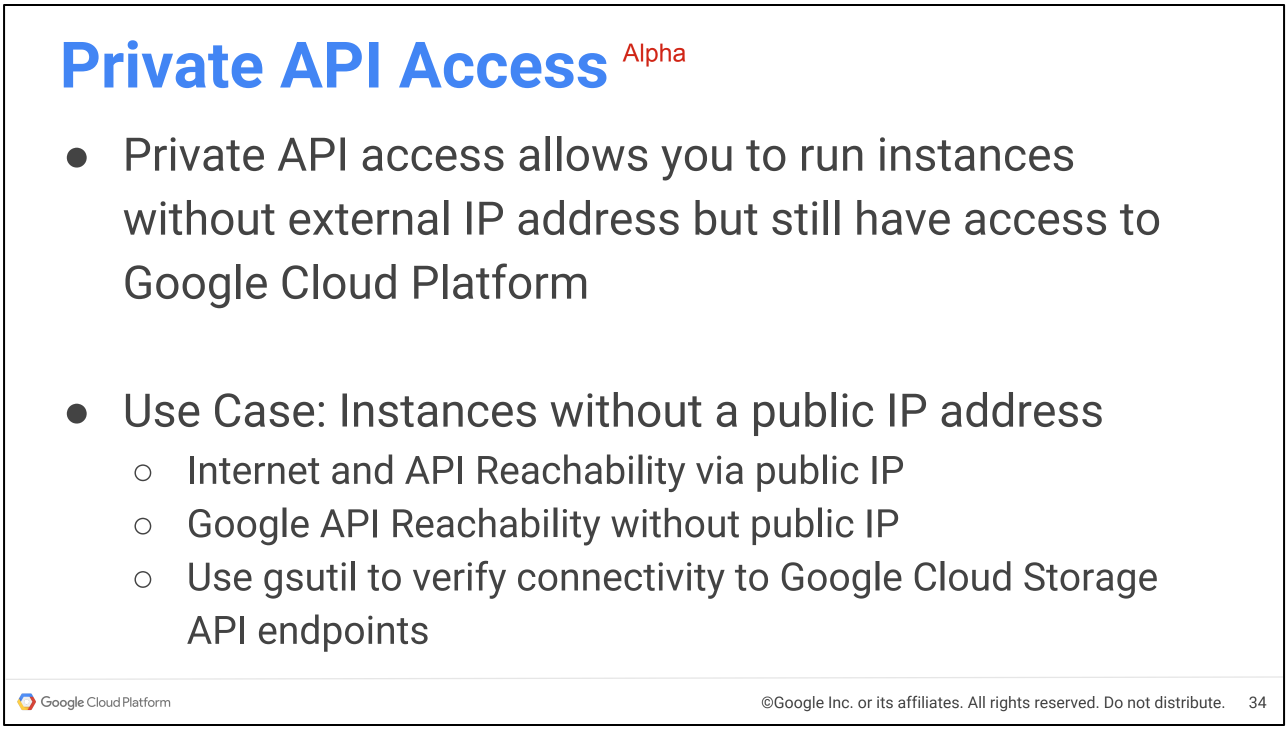
Cross Project Networking (XPN)

Alpha

- XPN enables centralized security and network administration in an Organization
- Provider/Consumer model: Departments operate autonomously, consuming common network provided by administrators
- XPN Host Project: Project that hosts sharable networking resources within an organization
- Service Project: Project that represents an autonomously operated department. This project uses the centralized network provided by the XPN host project.
- Service Project team has the ownership of the workloads contained in the project
- Allow billing and quota to be separate for each team/project/service

Google Cloud Platform

XPN provides a centralized model for networking administration. This means central administration, control, and governance over network resources. In contrast to Network Peering, XPN resources are deployed in service projects and are consumers of the shared network. Enterprises with centralized networking and security operations with gravitate towards XPN based on central governance.



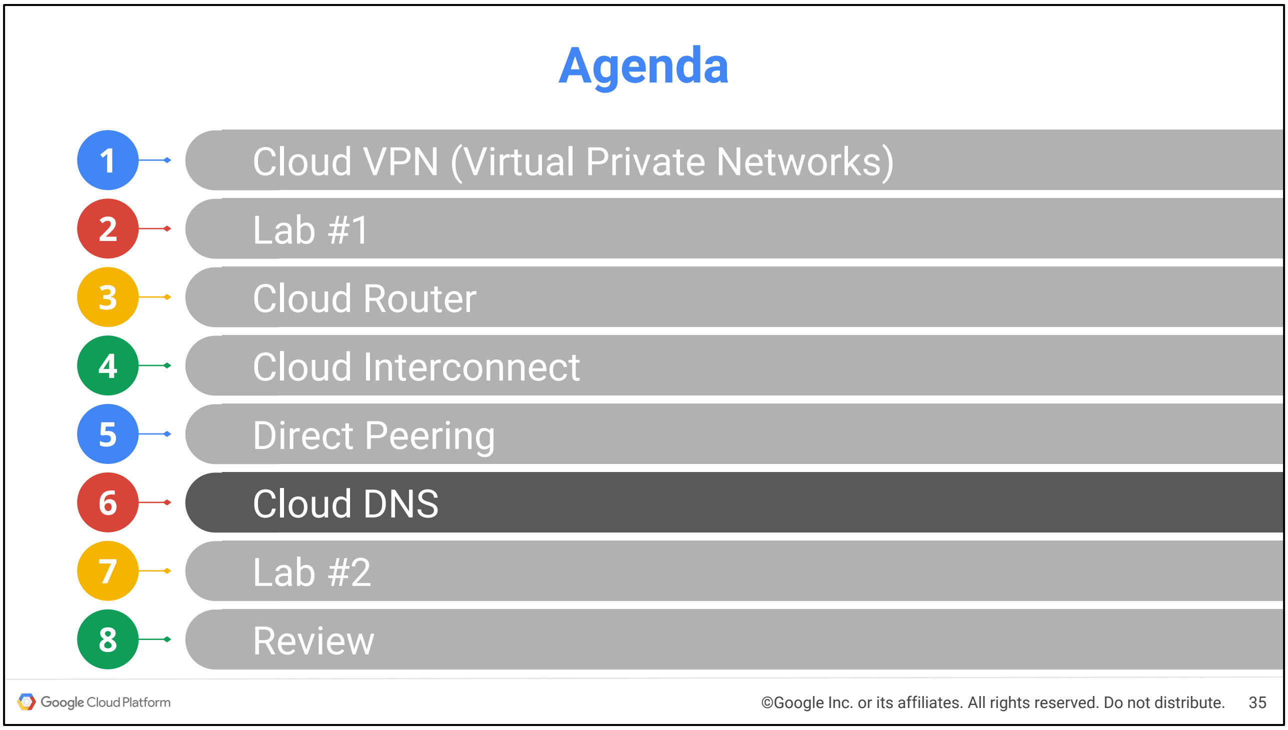
Private API Access Alpha

- Private API access allows you to run instances without external IP address but still have access to Google Cloud Platform

- Use Case: Instances without a public IP address
  - Internet and API Reachability via public IP
  - Google API Reachability without public IP
  - Use gsutil to verify connectivity to Google Cloud Storage API endpoints

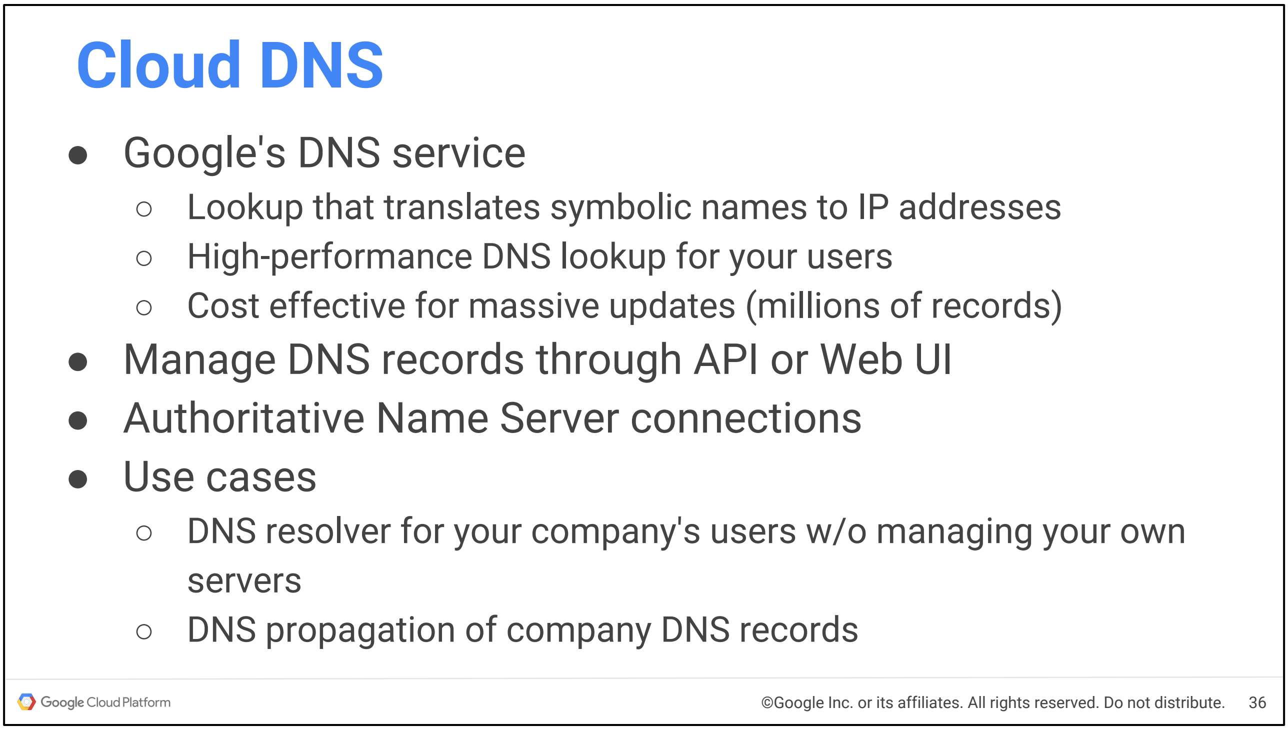
Google Cloud Platform

Private API access allows you to run instances without external IP address but still have access to Google Cloud Platform



Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. **Cloud DNS**
7. Lab #2
8. Review

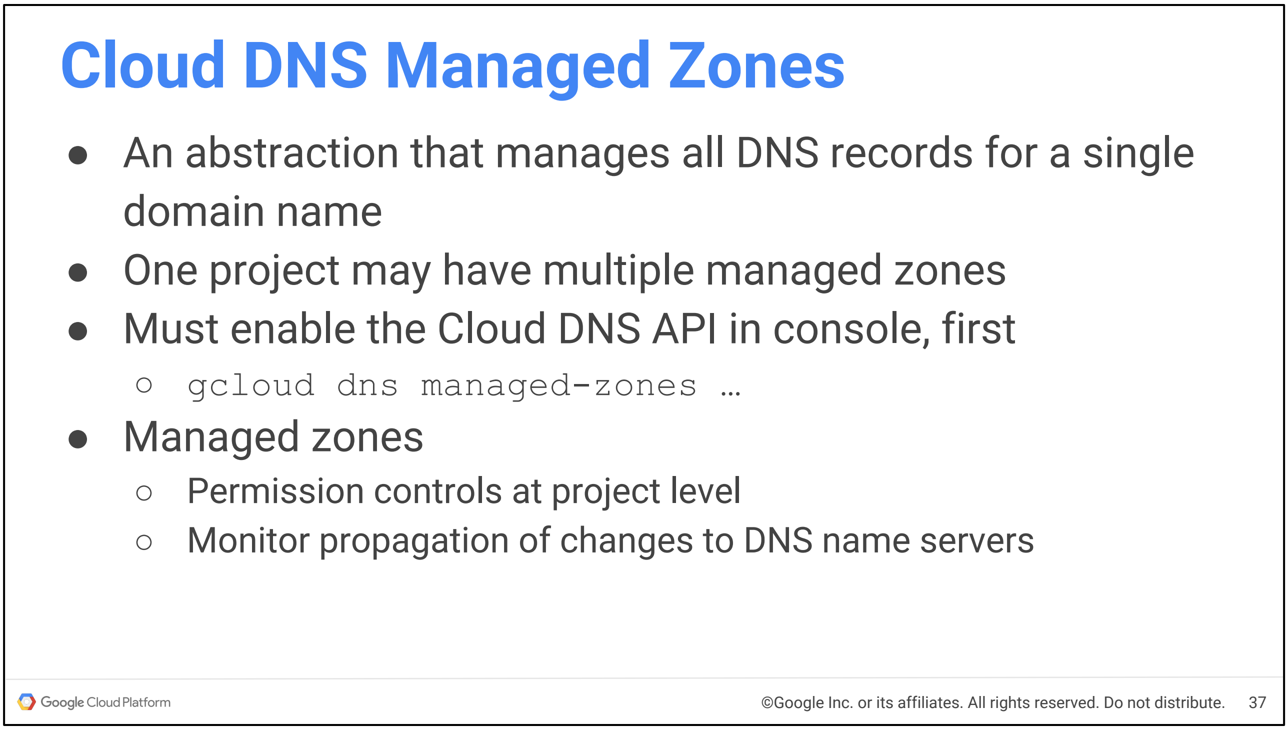


Cloud DNS

- 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
- Authoritative Name Server connections
- Use cases
  - DNS resolver for your company's users w/o managing your own servers
  - DNS propagation of company DNS records

Google Cloud Platform

Domain Name Service (DNS)

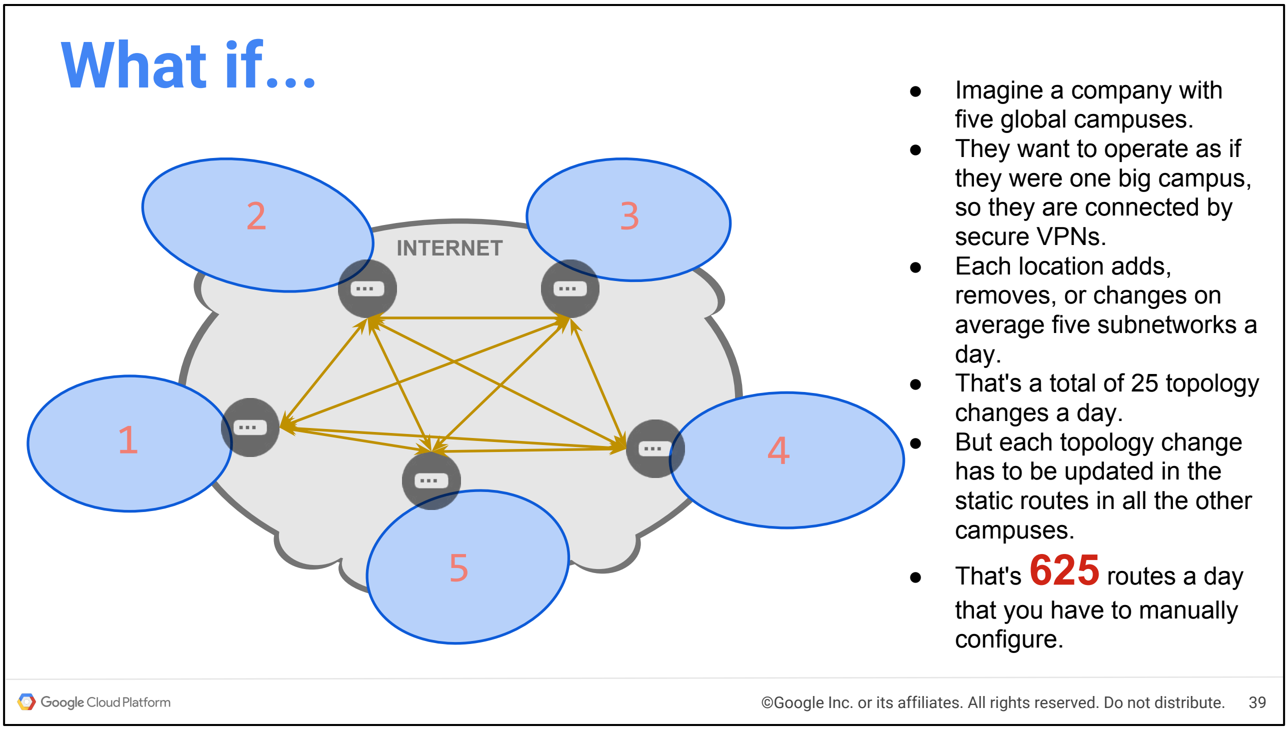


Cloud DNS Managed Zones

- 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 console, first
  - `gcloud dns managed-zones …`
- Managed zones
  - Permission controls at project level
  - Monitor propagation of changes to DNS name servers

Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. **Lab #2**
8. Review

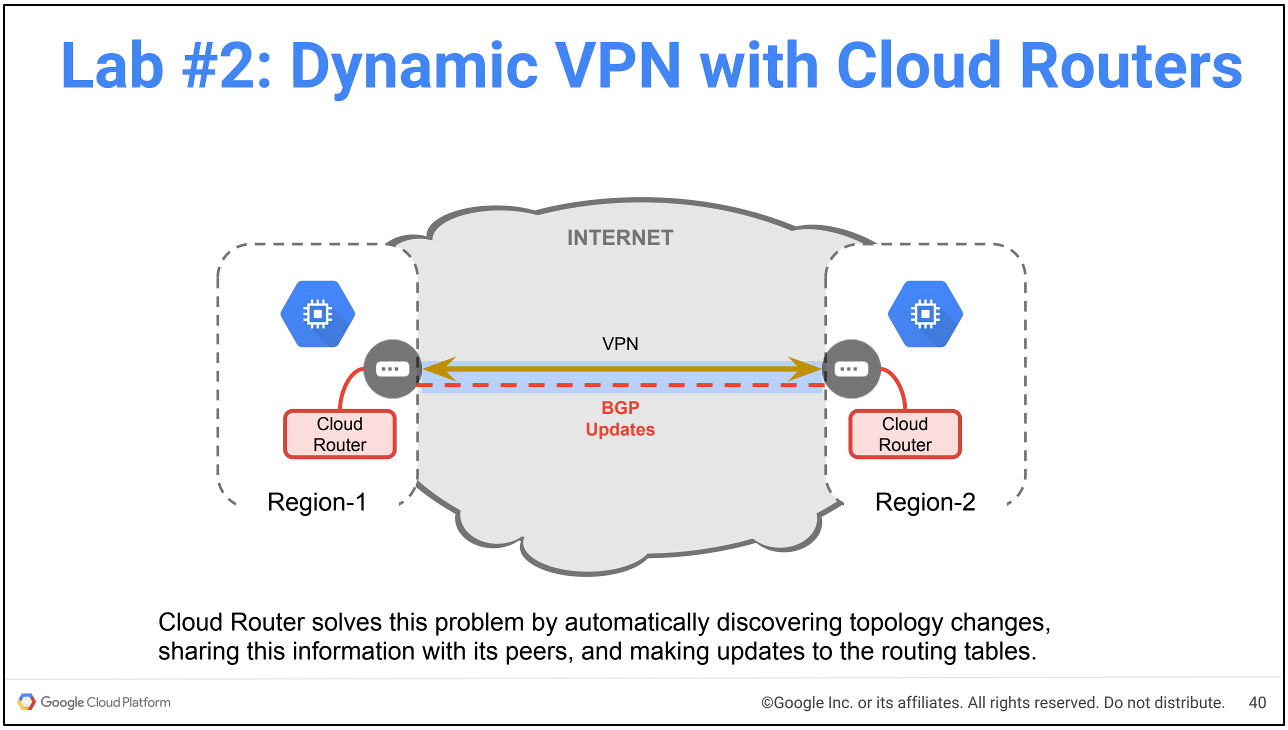


What if...

- Imagine a company with five global campuses.
- They want to operate as if they were one big campus, so they are connected by secure VPNs.
- Each location adds, removes, or changes on average five subnetworks a day.
- That's a total of 25 topology changes a day.
- But each topology change has to be updated in the static routes in all the other campuses.
- That's **625** routes a day that you have to manually configure.

Google Cloud Platform

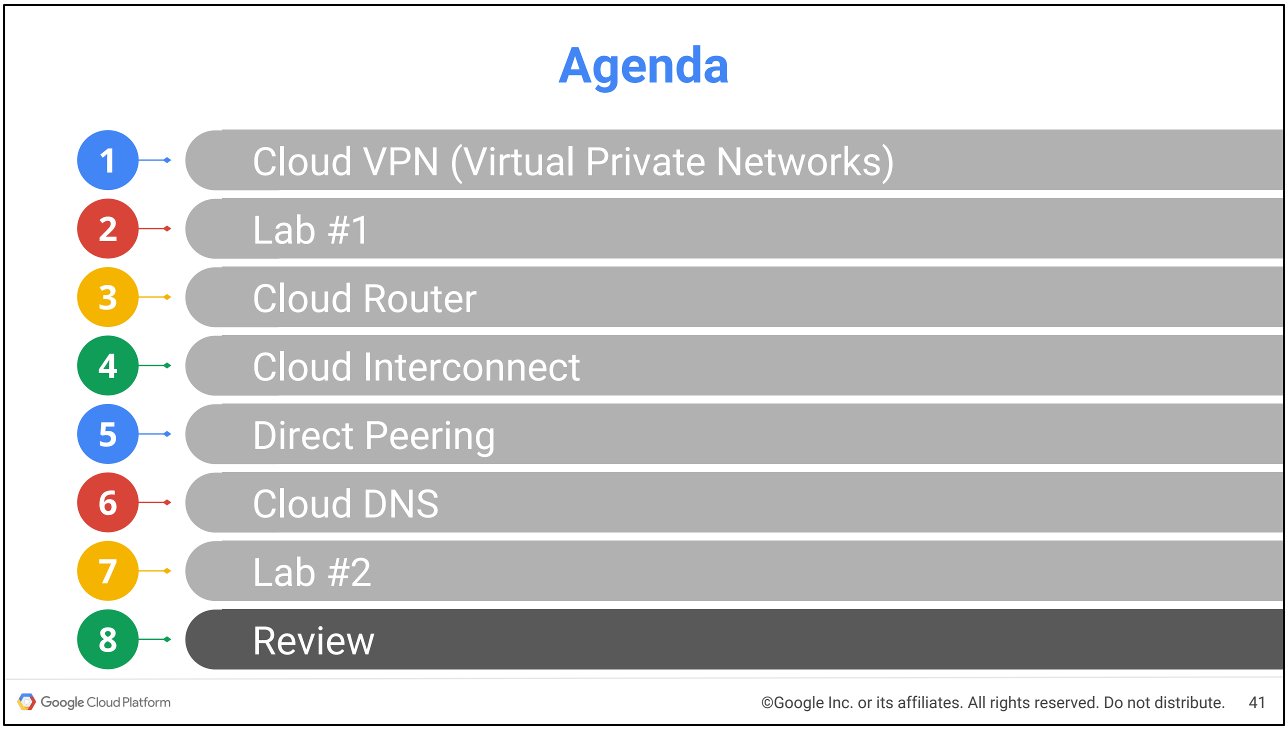
625 x 365 = 228,125 static route commands per year.



Lab #2: Dynamic VPN with Cloud Routers

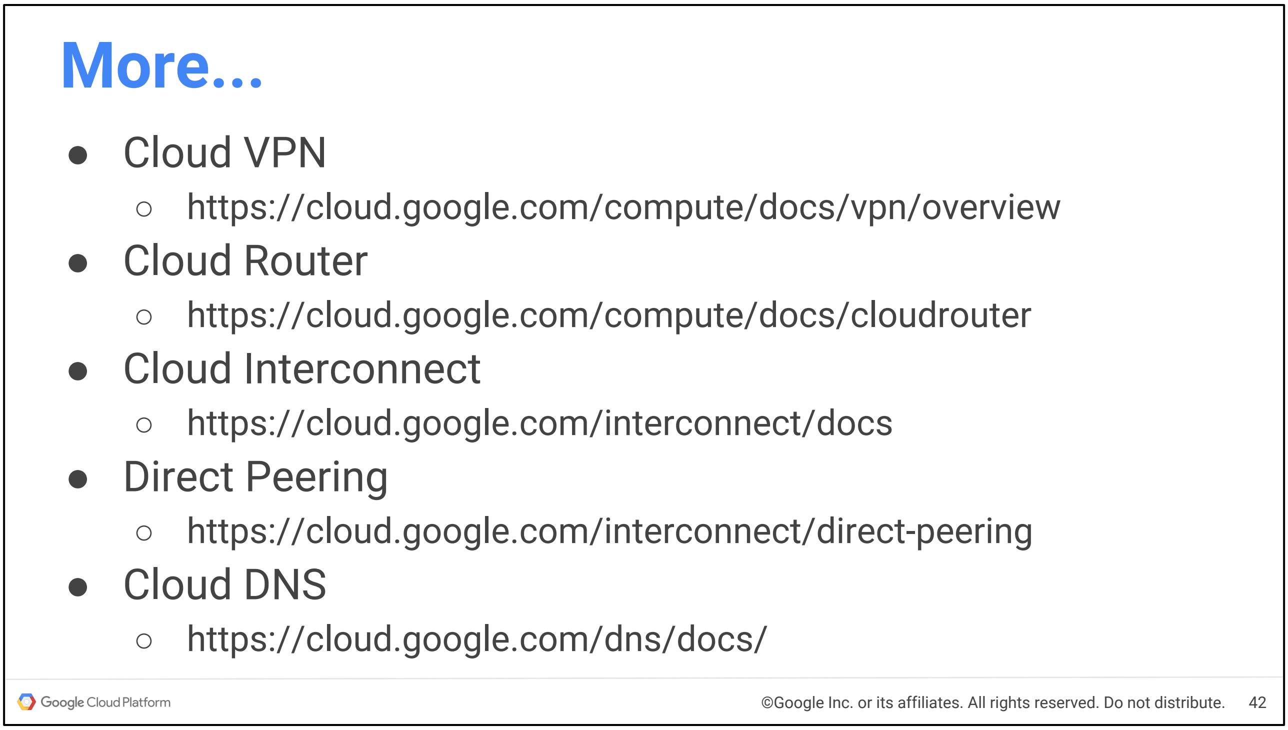
Cloud Router solves this problem by automatically discovering topology changes, sharing this information with its peers, and making updates to the routing tables.

08-2 Dynamic VPN with Cloud Routers



Agenda

1. Cloud VPN (Virtual Private Networks)
2. Lab #1
3. Cloud Router
4. Cloud Interconnect
5. Direct Peering
6. Cloud DNS
7. Lab #2
8. Review



More...

- 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/

Google Cloud Platform

More to learn on this subject. Here are some suggestions and links.

cloud.google.com