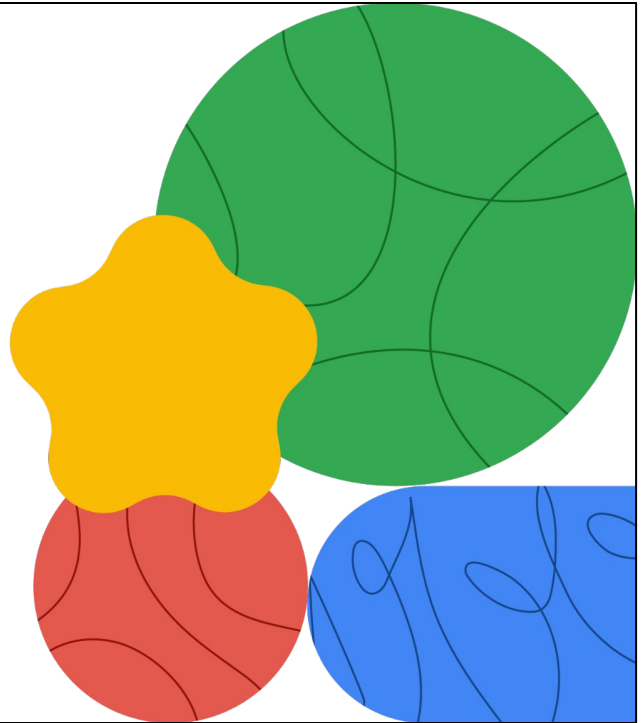



Networking in Google Cloud

Module 13:
Connectivity options



Welcome to Connectivity options, module



Today's agenda



- | | |
|----|--------------------------|
| 01 | Connection options |
| 02 | Dedicated Interconnect |
| 03 | Partner Interconnect |
| 04 | Cross-Cloud Interconnect |
| 05 | Quiz |

In this module, you will receive a brief overview of Cloud Interconnect and Cloud VPN. You then learn about the three types of Cloud Interconnect: Dedicated Interconnect, Partner Interconnect, and Cross-Cloud Interconnect. You also learn about how they can be useful and also how to set them up. At the end of the module, there is a short quiz to check your understanding of what you learned.

Cloud Interconnect and Cloud VPN

- ✓ Cloud Interconnect provides a fast connection to the Google network.
- ✓ Google offers three different Cloud Interconnect products.
 - To connect at a colocation facility, use Dedicated Interconnect.
 - To connect through a supported service provider, use Partner Interconnect.
 - To connect to other cloud providers directly, use Cross-Cloud Interconnect.
- ✓ Google also offers Cloud VPN, which can be used over the internet for lower bandwidth needs.

Cloud Interconnect provides fast connection to Google's network. Google offers two different Cloud Interconnect products; choose a product based on your situation and your needs.

When you can physically connect to the Google network at a colocation facility, use Dedicated Interconnect. When you cannot connect to the Google network at a colocation facility but can connect through a service provider, use Partner Interconnect. When you want to connect to other cloud providers directly, use Cross-Cloud Interconnect.

Google Cloud also offers Cloud VPN. Cloud VPN can be useful when you have lower bandwidth needs or when you must encrypt data in transit.

In this module, you will learn more about the three types of Cloud Interconnect.

Comparison of connection options

Connection	Provides	Capacity	Requirements	Access Type
VPN tunnel	Encrypted tunnel to VPC networks through the public internet	1.5–3 Gbps per tunnel	Remote VPN gateway	Internal IP addresses
Dedicated Interconnect	Dedicated, direct connection to VPC networks	10 Gbps or 100 Gbps per link	Connection in colocation facility	
Partner Interconnect	Dedicated bandwidth, connection to VPC network through a service provider	50 Mbps – 50 Gbps per connection	Supported Service Provider with Google Cloud connectivity	
Cross-Cloud Interconnect	Dedicated physical connection between Google VPC and other cloud service provider network	10 Gbps or 100 Gbps per connection	Primary and redundant ports (Google Cloud and remote cloud service provider)	

Let's compare these connection options. All these options provide internal IP address access between resources in your on-premises network and in your VPC network. The main differences are the connection capacity and the requirements for using a service.

The IPsec VPN tunnels that Cloud VPN offers have a capacity of 1.5 Gbps to 3 Gbps per tunnel. The tunnels connect to a VPN device in your on-premises network. The 1.5 Gbps capacity applies to traffic that traverses the public internet, and the 3 Gbps capacity applies to traffic that is traversing a direct peering link. If you want to scale this capacity, you can configure multiple tunnels.


Dedicated Interconnect has a capacity of 10 Gbps or 100 Gbps per link and requires you to have a connection in a Google-supported colocation facility. You can have up to eight links to achieve multiples of 10 Gbps, or up to two links to achieve multiples of 200 Gbps, but 10 Gbps is the minimum capacity.

Partner Interconnect has a capacity of 50 Mbps to 50 Gbps per connection, and requirements depend on the service provider.


Dedicated Interconnect and Partner Interconnect do not encrypt data in transit. Secure data in transit at the application layer using TLS, for example.

Cross-Cloud Interconnect enables you to establish high-bandwidth dedicated connectivity between Google Cloud and another cloud service provider. Cross-Cloud

Interconnect connections are available in two sizes: 10 Gbps or 100 Gbps.



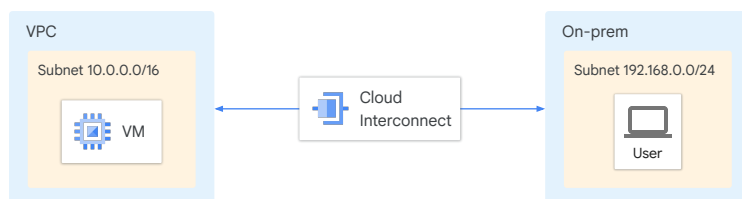
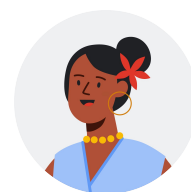
Today's agenda



- 01 Connection options
- 02 **Dedicated Interconnect**
- 03 Partner Interconnect
- 04 Cross-Cloud Interconnect
- 05 Quiz

Next, let's discuss Dedicated Interconnect.

Use case: Faster and optimal data migration



- ✓ Dedicated, high performance connection with fiber ports
- ✓ Secure with option for data encryption through IPsec or MACsec.

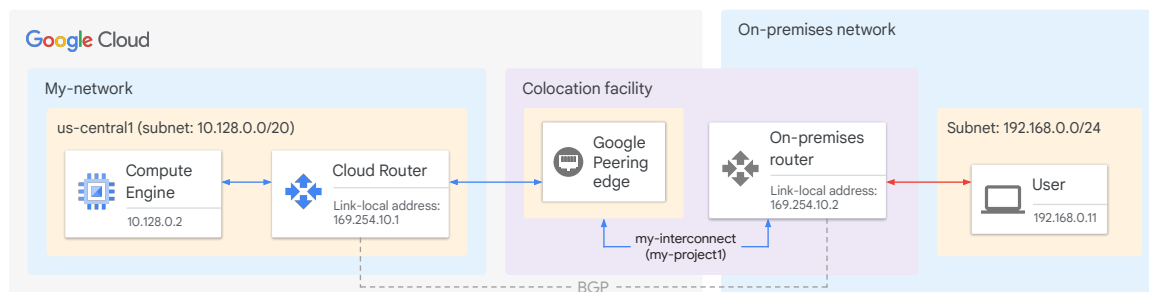
Dedicated Interconnect to migrate data to Google Cloud

Sam, a network engineer at Cymbal Corporation, is tasked with migrating mission-critical workloads to Google Cloud. Sam won't migrate the entire on-prem to Google and it makes sense to migrate a portion of the workload. These workloads require the highest levels of performance and reliability, with minimal latency and jitter. Currently, Sam is considering using the public internet for the connection, but concerns about security and reliability remain. A VPN connection over the internet is not the top choice, as the Public internet is not most performant and overhead of VPN on packets can impact performance.

Sam needs a solution that guarantees consistent, high-performance connectivity with fiber ports between Cymbal's on-premises network and Google Cloud. The solution must offer dedicated bandwidth, ensuring that mission-critical workloads have the resources they need to function flawlessly. Additionally, Sami requires the solution to be highly secure, with the option to enable robust data encryption and isolation from public internet traffic. Thus a dedicated interconnect option checks all his requirements.

Dedicated Interconnect provides direct physical connections

Dedicated Interconnect provides direct physical connections between your on-premises network and the Google network.



Google Cloud

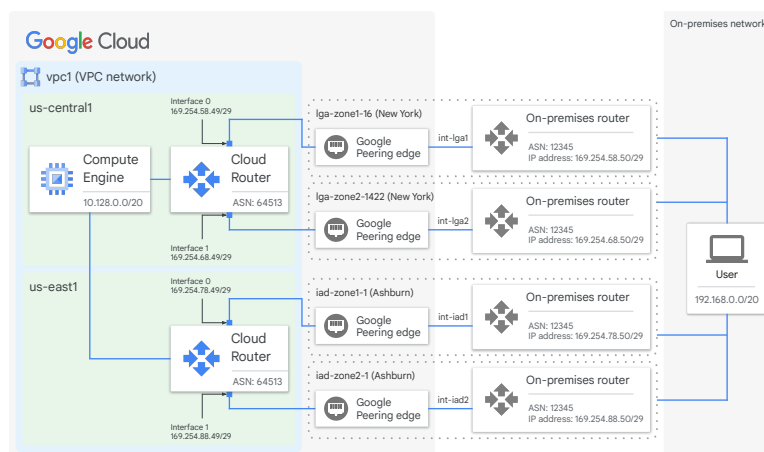
Dedicated Interconnect provides direct physical connections between your on-premises network and the Google network. Dedicated Interconnect enables you to transfer large amounts of data between networks, which can be more cost-effective than purchasing additional bandwidth over the public internet.

Upon establishing a VLAN attachment, it is linked with a Cloud Router. This Cloud Router initiates a BGP session for both the VLAN attachment and its corresponding on-premises peer router. Through this BGP session, the Cloud Router receives routes advertised by the on-premises router. These routes are then integrated into your VPC network as custom dynamic routes. Simultaneously, the Cloud Router advertises routes for Google Cloud resources to the on-premises peer router, ensuring bi-directional route exchange.

High availability with peering edge placement

To achieve 99.99% high availability, consider the following:

- Create at least 4 Interconnect connections, 2 in each metropolitan areas.
- In a metro, place 2 connections in different edge availability domains (metro availability zones).
- Deploy a minimum of 2 Cloud Routers across at least 2 regions



Google Cloud

In order to provide redundancy, create at least 4 Interconnect connections, 2 in each metropolitan areas.

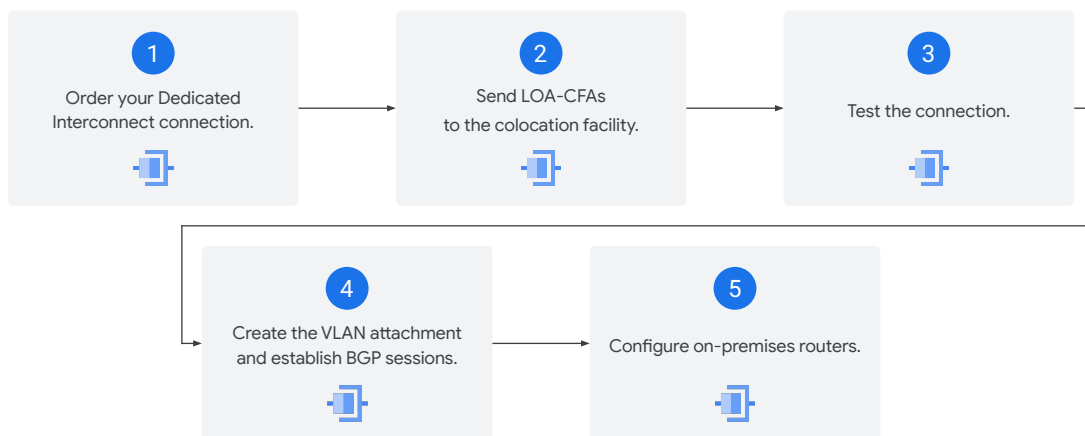
Placing a Dedicated Interconnect connection in more than one domain in a metropolitan area provides redundancy. The domains provide isolation during scheduled maintenance, which means that two domains in the same metropolitan area are not down for maintenance at the same time. If you have a Dedicated Interconnect connection defined in each of the two domains, scheduled maintenance can only affect a single connection at any given time.

A minimum of two Cloud Routers should be deployed across at least two separate Google Cloud regions. This is essential even if all your virtual machine (VM) instances are located within a single region. In the event of a region-wide disruption, Google Cloud can redirect traffic through the unaffected region to ensure continued access to your VMs. Each Cloud Router must be linked to a pair of Dedicated Interconnect connections situated within the same metropolitan area.

In the example shown on the slide, network configuration features four Dedicated Interconnect connections distributed across two separate metropolitan areas and distinct edge availability domains: lga-zone1-16, lga-zone2-1422, iad-zone1-1, and iad-zone2-1. Each region (us-central1 and us-east1) houses a Cloud Router within the vpc1 network, with each router maintaining its own independent Border Gateway Protocol (BGP) session.

For a complete list of colocation facilities and edge availability zones, see [All colocation facilities](#) in the Google Cloud documentation. Note that the documentation also refers to an edge availability zone as an Interconnect location name.

Create a Dedicated Interconnect connection



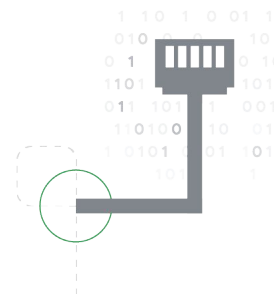
To create a Dedicated Interconnect connection, follow these steps:

1. Order your connection; you can do this within Google Cloud. Next, Google sends you a LOA-CFA—that is, a Letter of Authorization and Connecting Facility Assignment. The LOA-CFA identifies the connection ports that Google has assigned for your Dedicated Interconnect connection. The LOA-CFA also grants permission for a vendor in a colocation facility to connect to them.
2. Send LOA-CFAs to the colocation facility, so they can complete your connection setup. Your vendor will let you know when this setup is complete.
3. Test the connection. Google sends you automated emails with configuration information for two different tests. First, Google sends an IP address configuration to test light levels on every circuit in a Dedicated Interconnect connection. After those tests pass, Google sends the final IP address configuration to test the IP connectivity of each connection. Apply these configurations to your Cloud Routers so that Google can confirm connectivity. After all tests have passed, your Dedicated Interconnect connection is ready to use.
4. Create VLAN attachments and establish BGP sessions. You can do this using the Google Cloud console.
5. Configure the on-premises routers to establish a BGP session with your Cloud

1. Router. To configure your on-premises router, use the VLAN ID, interface IP address, and peering IP address provided by the VLAN attachment.


Connection bandwidth and circuits

- A Dedicated Interconnect connection consists of one or more fiber circuits.
- The circuits in a connection can be 10 Gbps or 100 Gbps, but not both.
- A connection can have one of the following maximum capacities:
 - Eight 10-Gbps circuits (80 Gbps total)
 - Two 100-Gbps circuits (200 Gbps total)




Next, let's talk about your connection bandwidth. You can purchase bandwidth as one or more circuits. Each circuit can be either 10 Gbps or 100 Gbps, but not both. You cannot have different types of circuits in the same connection.

A connection can have a maximum of eight 10-Gbps circuits, or two 100-Gbps circuits. Therefore, the maximum connection capacity is either 80 Gbps or 200 Gbps, depending on which type of circuit you choose.



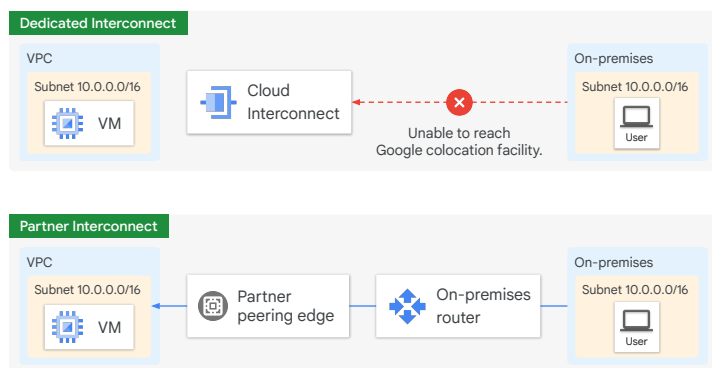
Today's agenda



- 01 Connection options
- 02 Dedicated Interconnect
- 03 [Partner Interconnect](#)
- 04 Cross-Cloud Interconnect
- 05 Quiz

Next, let's discuss Partner Interconnect, starting with a use case.

Use case: Connect from a partner location of your choice



High bandwidth, low latency connectivity even without a nearby colocation facility.



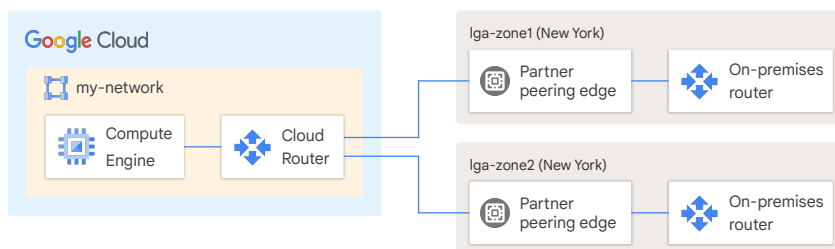
Uses the partner's underlying infrastructure to connect to Google Cloud.

Ken, a network engineer at Cymbal Corporation, is tasked with connecting Cymbal's geographically remote data center to Google Cloud. However, the data center's location doesn't have access to a Dedicated Interconnect colocation facility, making a direct connection impossible.

Solution: Ken requires a solution that offers high bandwidth, low latency, and dedicated connectivity to Google Cloud, even without a nearby colocation facility. A set up that Uses the partner's underlying infrastructure to connect to Google Cloud. Additionally, the solution needs to be secure and reliable, providing robust data protection and ensuring seamless operations. Thus, Partner Interconnect seems to be an excellent fit.

Partner Interconnect

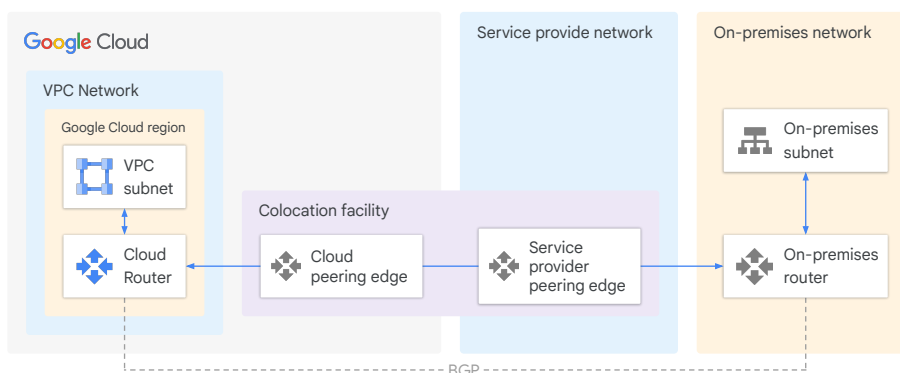
- Partner Interconnect is similar to Dedicated Interconnect.
- The physical connection is made through a supported service provider.



Partner Interconnect is similar to Dedicated Interconnect. Dedicated Interconnect and Partner Interconnect have technical feature parity.

However, the physical connection for Dedicated Interconnect is made through a supported service provider. Let's look at a few more differences on the next slide.

Partner Interconnect provides connectivity through a supported service provider



Google Cloud

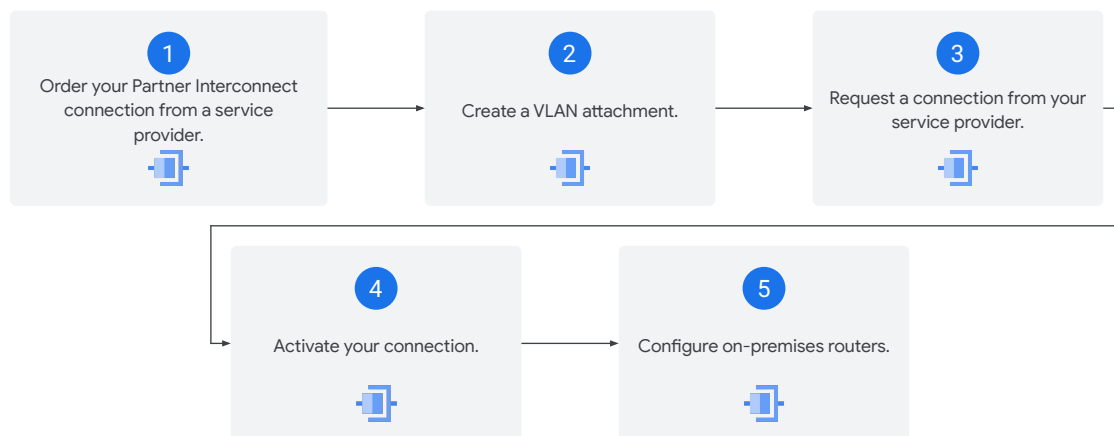
Partner Interconnect provides connectivity between your on-premises network and your VPC network through a supported service provider. If your data center is in a physical location that can't reach a Dedicated Interconnect colocation facility, Partner Interconnect is a good option. If your data needs don't warrant using Dedicated Interconnect, consider using Partner Interconnect. Work with a supported service provider to connect your VPC and on-premises networks.

Consider placing the Partner Interconnect connection in multiple edge availability domains for redundancy.

For a full list of service providers, see *Supported service providers* in the Google Cloud documentation at

<https://cloud.google.com/interconnect/docs/concepts/service-providers>.

Create a Partner Interconnect connection



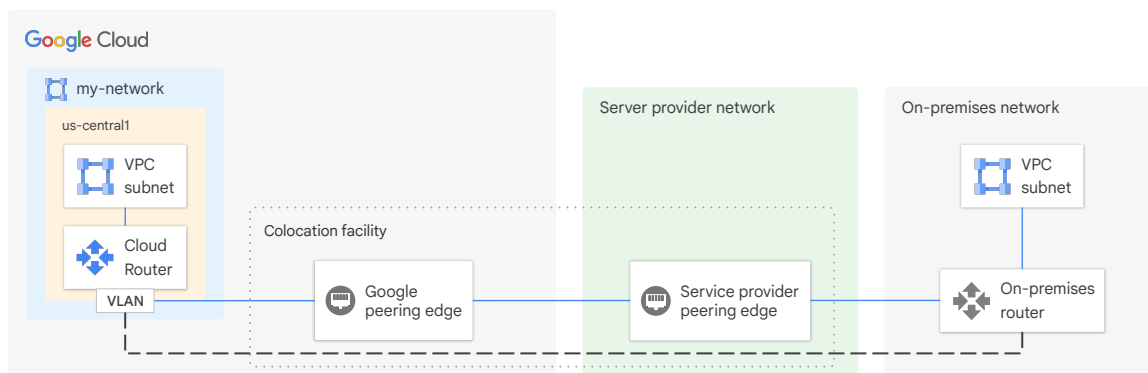
To create a Partner Interconnect connection, follow these steps:

1. Order your connection from a supported service provider. For a list of service providers in your area, see [Supported service providers](#) in the Google Cloud documentation. The service provider will then provide the connectivity needed to create a VLAN attachment.
2. Create a VLAN attachment, which creates a pairing key. The pairing key is unique and lets a service provider identify and connect to the associated Cloud Router. The service provider uses this key to finish configuring your VLAN attachment.
3. Request a connection from your service provider. Submit the pairing key and other connection details, such as the connection capacity and location. Your service provider configures your connection; they must confirm that they can serve your requested capacity. When the configuration is complete, you'll receive an email.
4. In the VLAN attachment, activate your connection. After the connection is activated, it can start passing traffic.
5. Configure the on-premises routers to establish a BGP session with your Cloud Router. To configure your on-premises routers, use the VLAN ID, interface IP address, and peering IP address provided by the VLAN attachment.

Layer 2 connections

For each VLAN attachment, configure and establish a BGP session between your Cloud Routers and on-premises routers.

— Data plane
- - - BGP session



Google Cloud

For Layer 2 connections, traffic passes through the service provider network to reach the VPC network or on-premises network. BGP is configured between the on-premises router and a Cloud Router in the VPC network, as shown in the graphic.

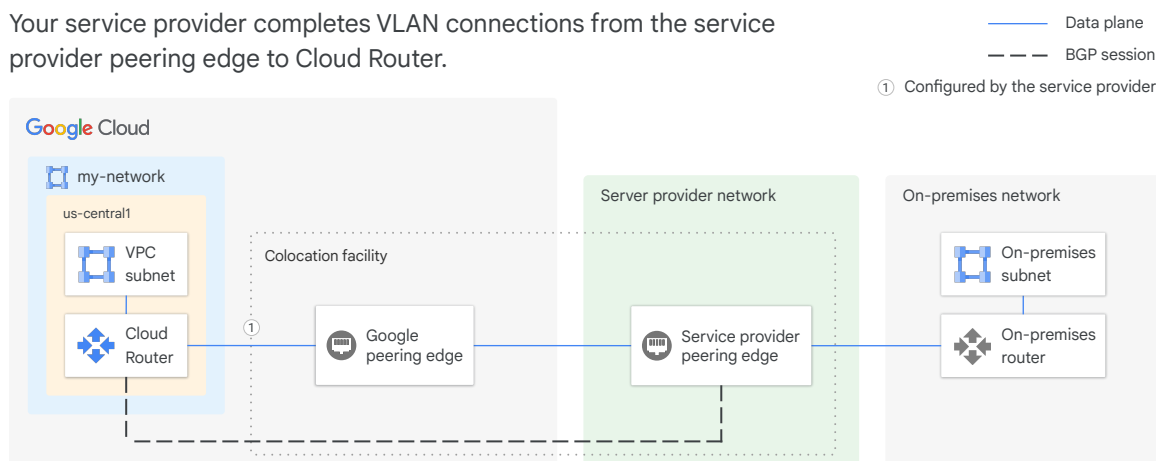
For Layer 2 connections, you must configure and establish a BGP session between your Cloud Routers and on-premises routers. When you configure Cloud Router, you configure VLAN (virtual local area network) attachments. Each VLAN attachment is a logical connection between your on-premises network and a single region in your VPC network.

When creating a VLAN attachment, specify a Cloud Router in the region that contains the subnets that you want to reach. The VLAN attachment automatically allocates a VLAN ID and BGP peering IP addresses. Use that information to configure your on-premises router and establish a BGP session with your Cloud Router.

For Partner Interconnect, the VLAN attachment uses a connection that your service provider sets up and manages. The service provider completes the circuit.

Layer 3 connections

Your service provider completes VLAN connections from the service provider peering edge to Cloud Router.



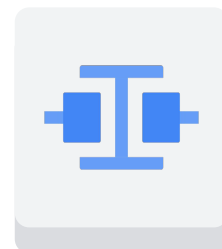
For Layer 3 connections, traffic is passed to the service provider network. Their network then routes the traffic to the correct destination, either to the on-premises network or to the VPC network. Connectivity between the on-premises network and the service provider network depends on the service provider. For example, the service provider might request that you establish a BGP session with them or configure a static default route to their network.

For Layer 3 connections, your service provider establishes a BGP session between your Cloud Routers and their on-premises routers for each VLAN attachment. You don't need to configure BGP on your local router. Google and your service provider automatically set the correct BGP configurations.

Partner Interconnect recommendations

Use Partner Interconnect when you:

- 01 Cannot physically connect from a facility where Google has a presence.
- 02 Need to procure a connection quickly.
- 03 Have lower bandwidth needs (50 Mbps - 50 Gbps).



Dedicated Interconnect and Partner Interconnect have technical feature parity. The biggest difference is where you interconnect; from a Google colocation facility or from a partner facility. However, there are some other points to consider.

Use Partner Interconnect when you cannot physically connect from a colocation facility where Google has presence, but can use a partner colocation facility.

Partner Interconnect can be procured quickly. The physical configuration already exists at the service provider, so there's less infrastructure to set up.

Partner Interconnect also is sufficient to support bandwidth needs less than 50 Gbps. A Partner Interconnect connection can be scaled based on the number and capacity of your VLAN attachments; thus, the smallest connection is 50 Mbps. If you need less than 50 Mbps, consider using Cloud VPN.

Partner Interconnect recommendations

Use Partner Interconnect when you:

- Cannot physically connect from a facility where Google has a presence.
- Need to procure a connection quickly.
- Have lower bandwidth needs (50 Mbps - 50 Gbps).




Dedicated Interconnect and Partner Interconnect have technical feature parity. The biggest difference is where you interconnect; from a Google colocation facility or from a partner facility. However, there are some other points to consider.


Use Partner Interconnect when you cannot physically connect from a colocation facility where Google has presence, but can use a partner colocation facility.

Partner Interconnect can be procured quickly. The physical configuration already exists at the service provider, so there's less infrastructure to set up.

Partner Interconnect also is sufficient to support bandwidth needs less than 50 Gbps. A Partner Interconnect connection can be scaled based on the number and capacity of your VLAN attachments; thus, the smallest connection is 50 Mbps. If you need less than 50 Mbps, consider using Cloud VPN.



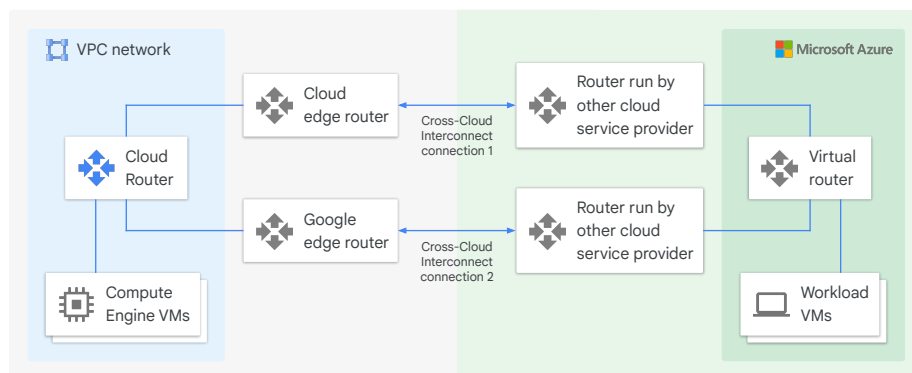
Today's agenda



- | | |
|----|--|
| 01 | Connection options |
| 02 | Dedicated Interconnect |
| 03 | Partner Interconnect |
| 04 | Cross-Cloud Interconnect |
| 05 | Quiz |

This module will delve into Google Cloud's Cross-Cloud Interconnect, a solution designed to provide private, high-bandwidth connections between Google Cloud and other cloud providers, enabling an integrated multi-cloud environment. Let's start with a usecase.

Use case: Connect from another cloud provider to Google Cloud



Rob, a network engineer at Cymbal Corporation, is tasked with managing the hybrid cloud environment for Cymbal, which spans Google Cloud and Microsoft Azure. As Cymbal's workload grows, Rob needs a solution to seamlessly connect the two cloud platforms and ensure consistent performance and security across both environments.

Solution: Cross Cloud Interconnect is an excellent fit as it offers dedicated, high-bandwidth connectivity between Google Cloud and Microsoft Azure. This would enable them to efficiently transfer data between the two platforms and eliminate the latency and bandwidth limitations associated with public internet connections. Additionally, Rob requires the solution to be secure and reliable, providing strong data encryption and redundancy to guarantee business continuity.

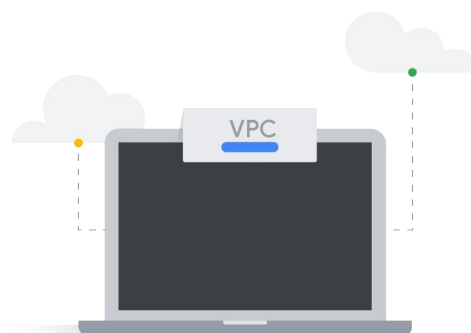
Use Cross-Cloud Interconnect to connect to a network hosted by another cloud service provider

01 Amazon Web Services (AWS)

02 Microsoft Azure

03 Oracle Cloud Infrastructure (OCI)

04 Alibaba Cloud



Google Cloud

With Cross-Cloud Interconnect, Google provisions a dedicated physical connection between the Google network and that of another supported cloud service provider. Google currently supports Amazon Web Services (AWS), Microsoft Azure, Oracle Cloud Infrastructure (OCI), and Alibaba Cloud for use with Cross-Cloud Interconnect. You can use this connection to peer your Google Virtual Private Cloud (VPC) network with your network that's hosted by the cloud service provider.

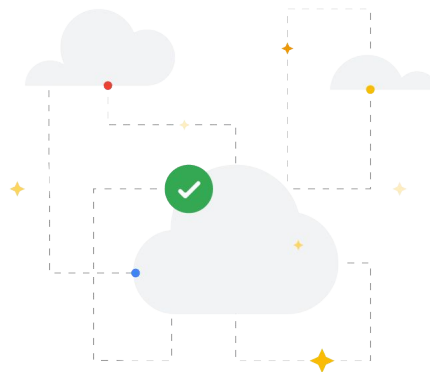
You identify supported locations where you want Google to place your connections. Then you purchase primary and redundant Cross-Cloud Interconnect ports. You also buy primary and redundant ports from your cloud service provider. After provisioning the connection, Google supports the connection up to the point where it reaches the network of your other cloud service provider. Google does not guarantee uptime from the other cloud service provider and cannot create a support ticket on your behalf.

Benefits of using Cross-Cloud Interconnect

01 Integrated multicloud strategy

02 Reduced complexity

03 Site-to-site data transfer



Google Cloud

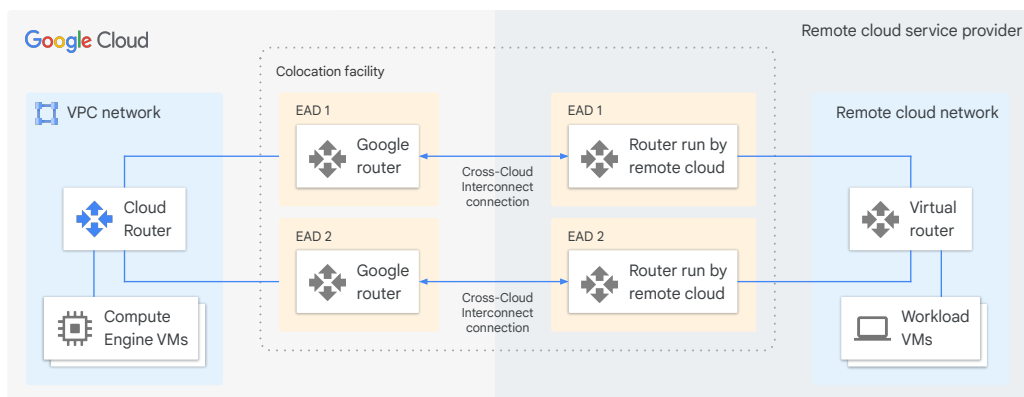
Cross-Cloud Interconnect supports the adoption of an integrated multicloud strategy. Adopting a multicloud architecture lets you:

- Avoid being locked in with a single vendor.
- Store data in one cloud while hosting business logic in another.
- Avoid downtime if one cloud has an outage.
- Use a second cloud for disaster recovery.
- Maximize business insights by analyzing data in multiple clouds.

Without Cross-Cloud Interconnect, the options for setting up connectivity are limited, and all are relatively complex. When you use Cross-Cloud Interconnect, you don't have to deploy your own hardware, and you eliminate the need to work with third parties.

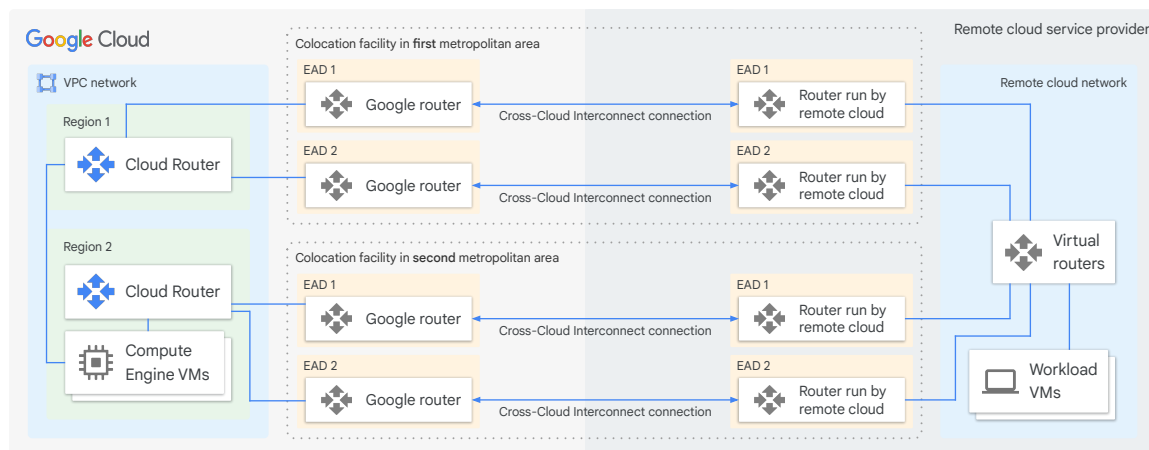
You can use Cross-Cloud Interconnect as part of a site-to-site data transfer strategy. Site-to-site data transfer is a feature of Network Connectivity Center that lets you use the Google network as a wide area network (WAN). Network Connectivity Center is discussed later.

Cross-Cloud Interconnect minimum requirement (99.9% availability)



The Cloud Interconnect SLA requires you to have, minimally, two connections: each in a different edge availability domain (EAD) of a metropolitan area. This approach gives you 99.9% availability.

High availability configuration (99.99%)



Google Cloud

In order to achieve high availability for critical applications, you should configure two pairs of connections. Each pair must be in a different metropolitan area. Within each metropolitan area, you must use two different edge availability domains. This approach gives you 99.99% availability.

Cross-Cloud Interconnect connections are available in two sizes: 10 Gbps or 100 Gbps.

For more information, see [Cross-Cloud Interconnect Overview](#).

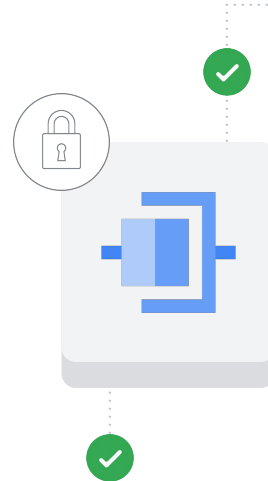
MACsec for Cloud Interconnect

MACsec for Cloud Interconnect helps you secure traffic on Cloud Interconnect connections.

MACsec encrypts traffic like this:

- On **Dedicated Interconnect**—between Google's peering edge router and an on-premises router.
- On **Partner Interconnect**—between Google's peering edge router and the service provider's peering edge router.
- On **Cross Cloud Interconnect** - Between Google's peering edge router and router run by remote cloud.

MACsec for Cloud Interconnect doesn't provide encryption in transit within Google. For stronger security, use MACsec with other network security protocols.



Google Cloud

MACsec for Cloud Interconnect helps you secure traffic on Cloud Interconnect connections, specifically between your on-premises router and Google's edge routers.

- MACsec encrypts traffic on Dedicated Interconnect between Google's peering edge router and an on-premises router.
- MACsec encrypts traffic on Partner Interconnect between Google's peering edge router and the service provider's peering edge router.
- MACsec encrypts traffic on Cross Cloud Interconnect between Google's peering edge router and router run by remote cloud.

MACsec for Cloud Interconnect doesn't provide encryption in transit within Google. For stronger security, we recommend that you use MACsec with other network security protocols, such as IP Security (IPsec) and Transport Layer Security (TLS).

Let's ask Gemini



Which should I use, Cloud VPN or Cloud Interconnect? Please provide details supporting the use of each according to their respective strengths.



List the steps to generate a report on the past week's performance of my Cloud Interconnect link, including bandwidth utilization, latency, and packet loss.

You decide to connect the network that you created to your on-premises network. Use Gemini to help you understand what options are available:

“Which should I use, Cloud VPN or Cloud Interconnect? Please provide details supporting the use of each according to their respective strengths.”

Another useful prompt is “List the steps to generate a report on the past week's performance of my Cloud Interconnect link, including bandwidth utilization, latency, and packet loss.”

Let's ask Gemini



Which should I use, Cloud VPN or Cloud Interconnect? Please provide details supporting the use of each according to their respective strengths.




The best choice for connecting your on-premises network to Google Cloud depends on your specific needs and requirements. Here is a comparison of Cloud VPN and Cloud Interconnect to help you make a decision.

Feature	Cloud VPN	Cloud Interconnect
Connection type	Point-to-point	Dedicated
Bandwidth	Up to 10 Gbps	Up to 100 Gbps


...

*Gemini responses may vary

Shown on slide is the response to the first prompt.
Gemini will provide a comparison table that covers the various feature differences between Cloud VPN and Cloud Interconnect.



Today's agenda



- 01 Connection options
- 02 Dedicated Interconnect
- 03 Partner Interconnect
- 04 Cross-Cloud Interconnect
- 05 [Quiz](#)

Quiz | Question 1

Question

Which Google Cloud Interconnect option requires the customer to provide their own routing equipment and establish a Border Gateway Protocol (BGP) session with Google's edge network?

- A. Cross-Cloud Interconnect
- B. Network Connectivity Center
- C. Dedicated Interconnect
- D. Partner Interconnect

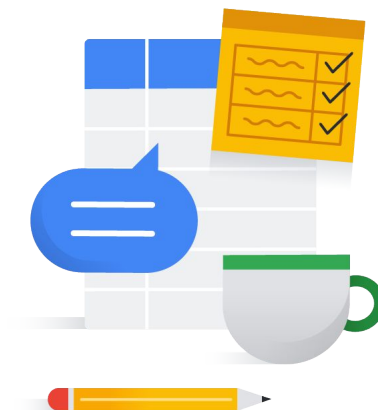
Quiz | Question 2

Question

Your company is located in a city where Google Cloud does not have a Dedicated Interconnect location, but you need a private connection to your Google Cloud Virtual Private Cloud (VPC). Which Cloud Interconnect option is most suitable for this scenario?

- A. Dedicated Interconnect
- B. Network Connectivity Center
- C. Carrier Peering
- D. Partner Interconnect

Debrief



In this module, we began by comparing the available options for hybrid connectivity with your Google Cloud network: Direct Interconnect, Partner Interconnect, Cross-Cloud Interconnect, and Cloud VPN.

You learned how to set up Direct Interconnect, Partner Interconnect and Cross-Cloud Interconnect. We also discussed conditions to consider.



THANK YOU

