Google Cloud Platform (GCP) Virtual Private Cloud (VPC) Network Peering allows private RFC 1918 (https://tools.ietf.org/html/rfc1918) connectivity across two VPC networks regardless of whether or not they belong to the same project or the same organization.

For details on VPC Network Peering, see the VPC Network Peering Overview (/vpc/docs/vpc-peering).

Before you begin, you must have the name of the VPC network to which you will peer with. If that network is located in another project, you must also have the project ID of that project.

A peering **configuration** establishes the *intent* to connect to another VPC network. Your network and the other network are not connected until each one has a peering configuration for the other. After the other network has a corresponding configuration to peer with your network, the peering state changes to `ACTIVE` in both networks, and they are connected. If there's no matching peering configuration in the other network, the peering state remains `INACTIVE`, indicating that your network is not connected to the other one.

Once connected, the two networks always exchange subnet routes (/vpc/docs/routes#subnet-routes). You can optionally import both static and dynamic custom routes (/vpc/docs/routes#custom-routes) from a peered network if it has been configured to export them. For more information, see importing and exporting custom routes (/vpc/docs/vpc-peering#importing-exporting-routes).

Update an existing VPC Network Peering connection to change whether your VPC network exports or imports custom routes to or from the peer VPC network.

You network imports custom routes only if the peer network is also exporting custom routes, and the peer network receives custom routes only if it imports them.

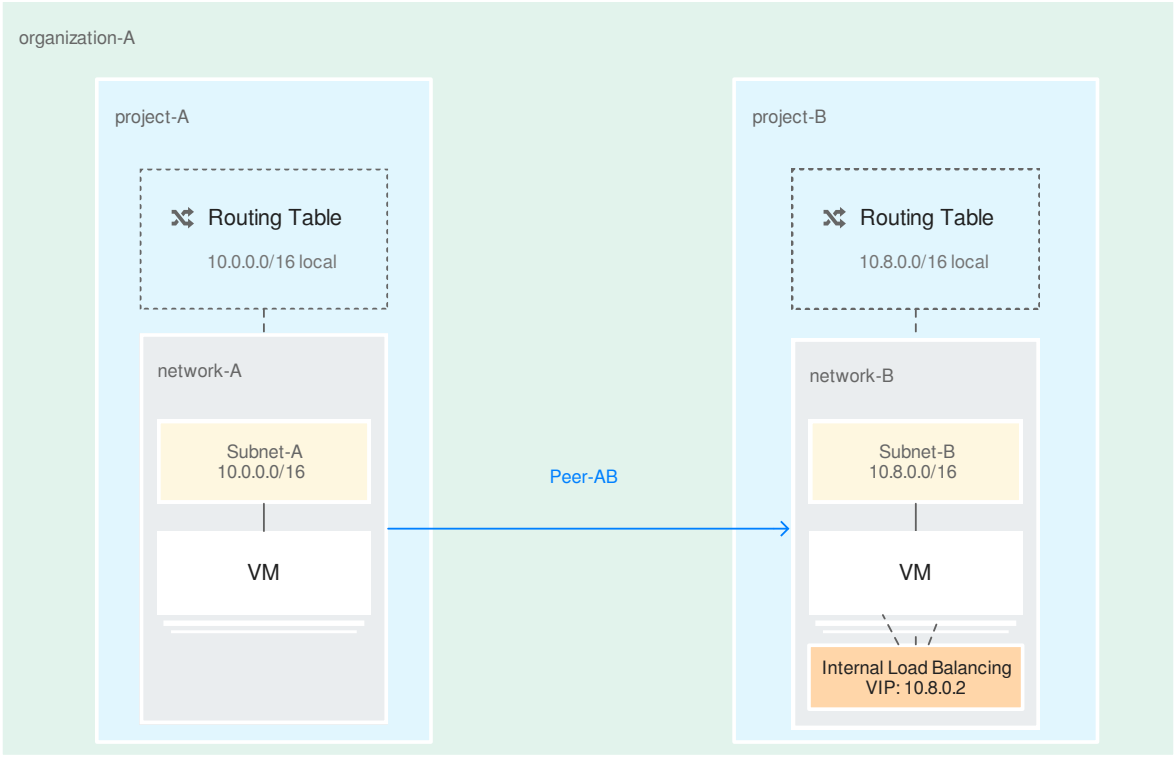
List existing peering connections to view their status and whether they're importing or exporting custom routes.

List the routes that your VPC network is importing from or exporting to a peered VPC network. For exported routes, you can check whether a peer network is accepting or rejecting your custom routes. For imported routes, you can check whether your network is accepting or rejecting custom routes from a peer network.

You or a network administrator for the peer VPC network can delete a peering configuration. When a peering configuration has been deleted, the peering *connection* switches to `INACTIVE` in the other network, and all routes shared among the networks are removed.

Consider an organization `organization-a` which needs VPC Network Peering to be established between `network-a` in `project-a` and `network-b` in `project-b`. In order for VPC Network Peering to be established successfully, administrators of `network-a` and `network-b` must separately configure the peering association.

A user with appropriate IAM permissions in `project-a` configures `network-a` to peer with `network-b`. For example, users with the roles/editor (/iam/docs/understanding-roles#primitive_role_definitions) or roles/compute.networkAdmin (/iam/docs/understanding-roles#compute-engine-roles) role can configure peering.



(/vpc/images/peering/network-peering-01.svg)

Peering from network-a to network-b (click to enlarge)

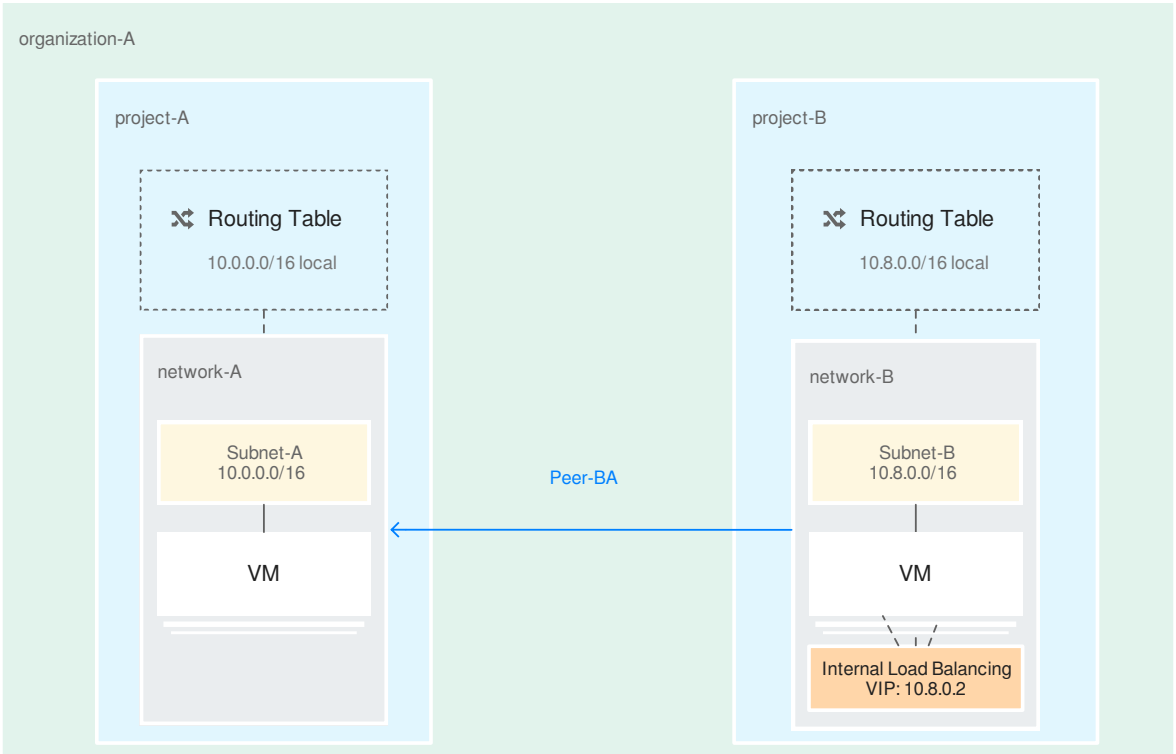
Before you begin, you will need the project IDs and network names of the networks you want to peer.

At this point, the peering state remains `INACTIVE` because there is no matching configuration in `network-b` in `project-b`.

When the peering state becomes `ACTIVE`, VPC Network Peering automatically exchanges subnet routes. Google Cloud also exchanges custom routes (static routes and dynamic routes) by importing or exporting them over the peering connection. Both networks must be configured to exchange custom routes before they are shared. For more information, see Importing and exporting custom routes (/vpc/docs/vpc-peering#importing-exporting-routes).

To see the current peering state, view the peering connection:

A NetworkAdmin (/iam/docs/understanding-roles#predefined_roles), or a user with appropriate IAM permissions, in `project-b` must configure the matching configuration from `network-b` to `network-a` in order for the peering to become `ACTIVE` on both ends.

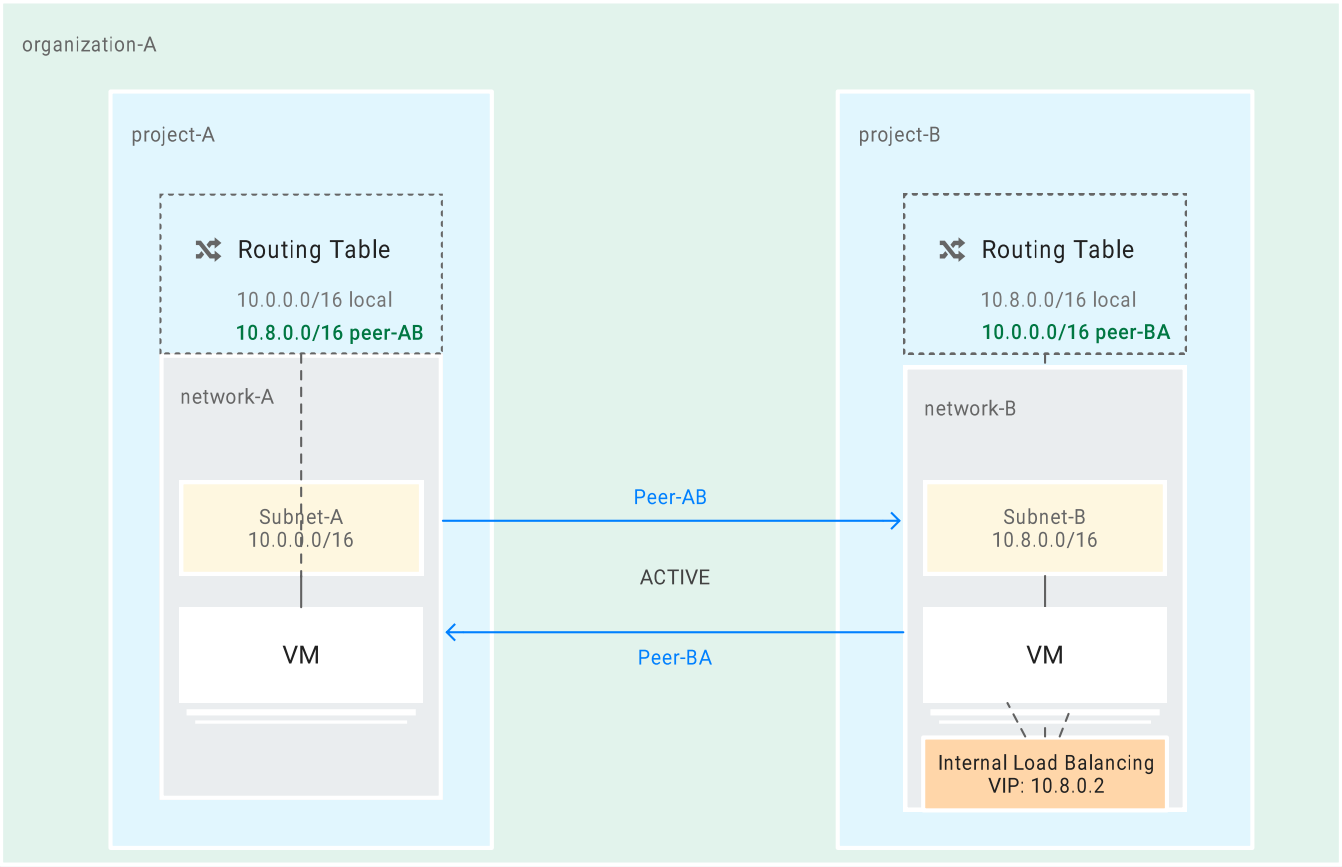


(/vpc/images/peering/network-peering-02.svg)

Peering from network-a to network-b (click to enlarge)

As soon as the peering moves to an `ACTIVE` state, subnet routes and custom routes are exchanged. The following traffic flows are set up:

- Between VM instances in the peered networks: Full mesh connectivity.
- From VM instances in one network to Internal TCP/UDP Load Balancing endpoints in the peered network



(/vpc/images/peering/network-peering-03.svg)

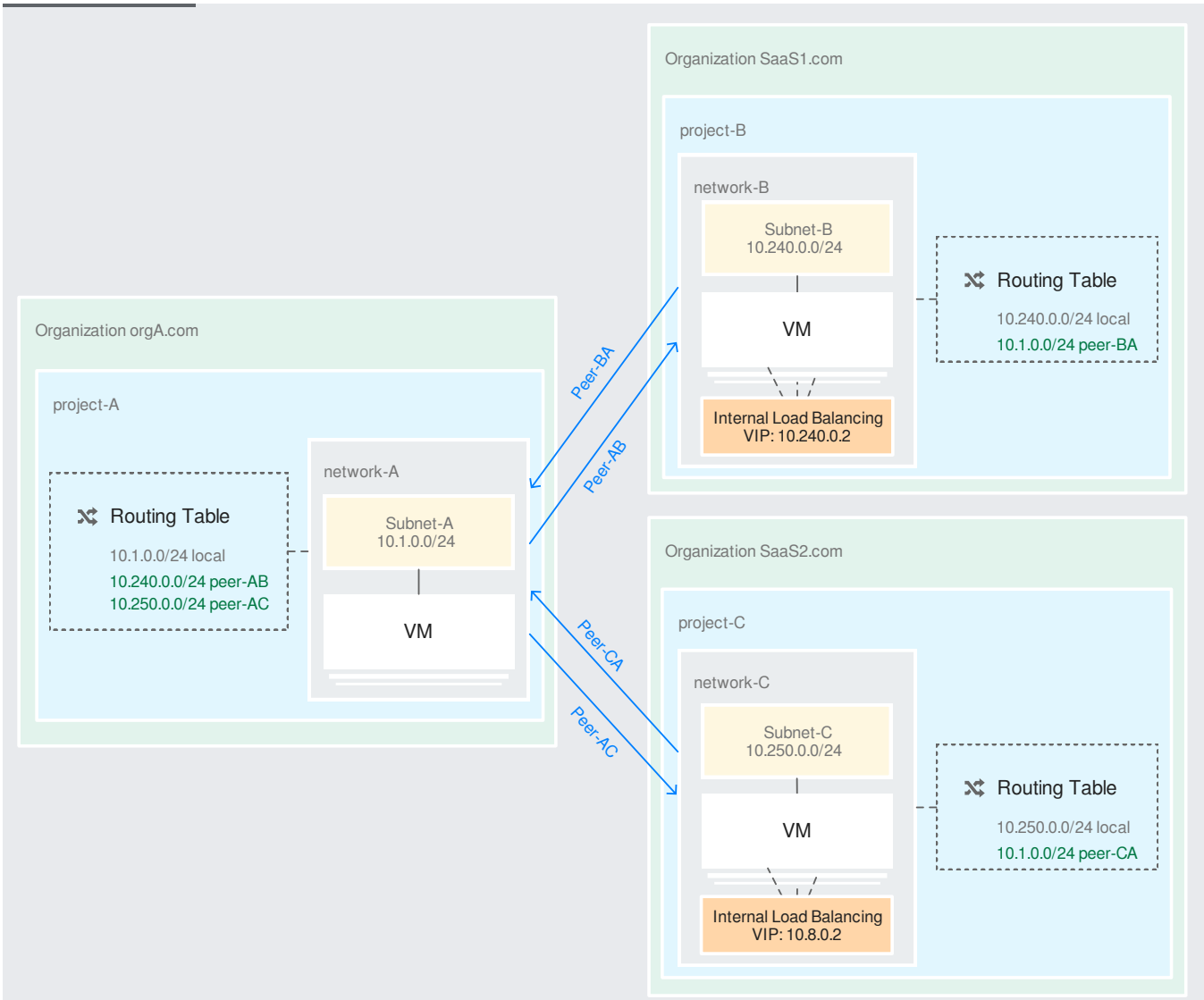
Peering ACTIVE (click to enlarge)

The routes to peered network CIDR prefixes are now visible across the VPC network peers. These routes are implicit routes that generated for active peering connections. They don't have corresponding route resources. The following procedure shows routes for all VPC networks for `project-a`.

Consider the scenario in which VM instances in `network-a` need to access services from two different external organizations: `SaaS1` and `SaaS2`. To access both using only internal (private, RFC 1918) IP addresses, two peering connections are required:

- `network-a` peers with `network-b`, which is in `SaaS1`
- `network-a` peers with `network-c`, which is in `SaaS2`

With VPC Network Peering, it doesn't matter that that `network-b` and `network-c` are in different projects and different organizations.



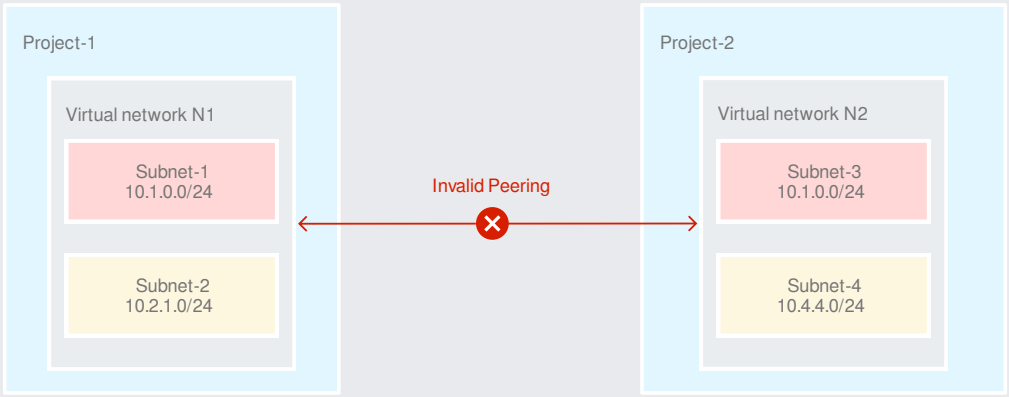
(/vpc/images/peering/network-peering-04.svg)

Cross-organization peering (click to enlarge)

To create this setup, simply create two different peering sessions.

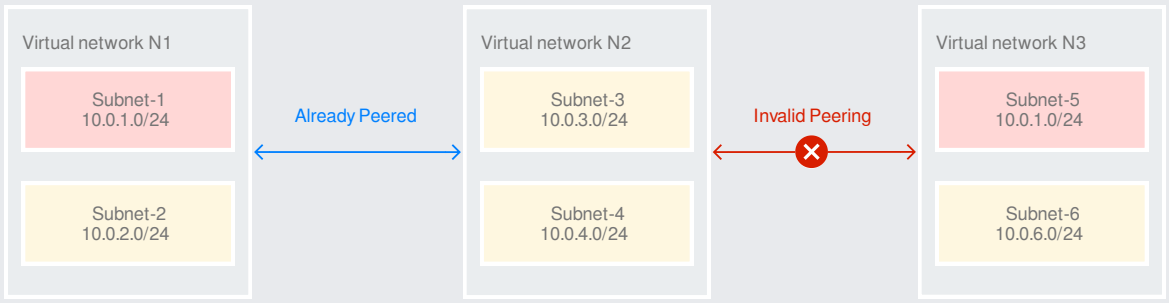
No subnet IP range can overlap with another subnet IP range in a peered VPC network.

At the time of peering, GCP checks to see if there are any subnets with overlapping IP ranges between the two VPC networks or any of their peered networks. If there is an overlap, peering is not established. Since a full mesh connectivity is created between VM instances, subnets in the peered VPC networks can't have overlapping IP ranges as this would cause routing issues.



(/vpc/images/peering/network-peering-11.svg)
Overlapping subnet IP ranges between two peers (click to enlarge)

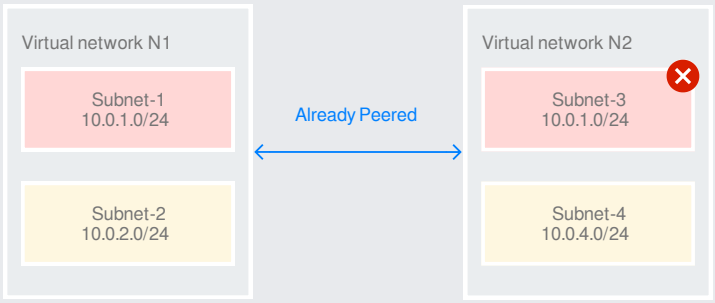
If there were any subnets with overlapping IP ranges between peers of a given VPC network, it would cause a routing conflict. For example, suppose VPC network N1 has already peered with VPC network N2, then VPC network N3 tries to peer with N2. This is an invalid peering because N3 has a subnet Subnet_5 whose IP range overlaps with Subnet_1 in network N1.



(/vpc/images/peering/network-peering-12.svg)
Overlapping subnet IP ranges with three peers (click to enlarge)

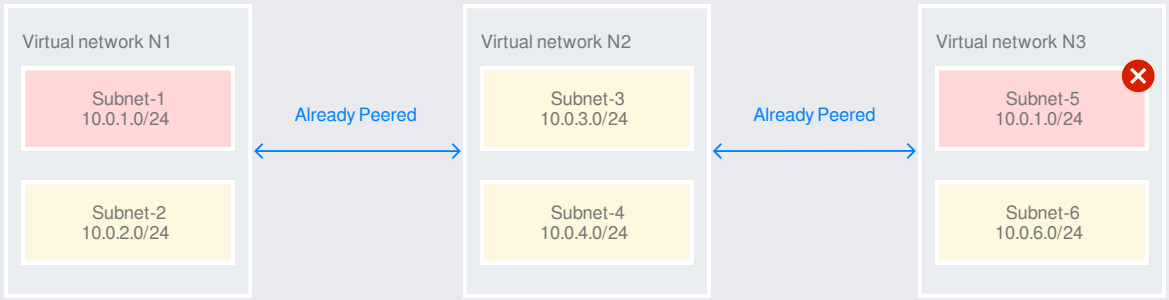
When a VPC subnet is created or a subnet IP range is expanded, GCP performs a check to make sure the new subnet range does not overlap with IP ranges of subnets in the same VPC network

or in directly peered VPC networks. If it does, the creation or expansion action fails. For example, when a new subnet subnet_3 is created in network N2 in the following figure, the IP ranges must not overlap with the IP ranges defined in the directly peered network N1.



(/vpc/images/peering/network-peering-13.svg)
Subnet creation check (click to enlarge)

GCP also ensures that no overlapping subnet IP ranges are allowed across VPC networks that have a peered network in common. If it does, the creation or expansion action fails. For example, when a new subnet subnet_5 is created in network N3 in the following figure, the IP ranges must not overlap with the IP ranges defined in directly peered network N2, or with network N1, because N1 is already peered with N2.



(/vpc/images/peering/network-peering-14.svg)
Subnet creation check with three peers (click to enlarge)

Legacy Networks are networks that do not have subnets. Legacy networks cannot peer with any other networks and are not supported in VPC Network Peering.

Compute Engine internal DNS names created in a network are not accessible to peered networks. The IP address of the VM should be used to reach the VM instances in peered network.

You cannot use a tag or service account from one peered network in the other peered network.

VPC Network Peering with GKE (/kubernetes-engine/) is supported when used with IP Aliases (/kubernetes-engine/docs/ip-aliases) and custom routes (/vpc/docs/vpc-peering#importing-exporting-routes). Kubernetes Services, if exposed via Internal TCP/UDP Load Balancing (/kubernetes-engine/docs/internal-load-balancing), and Pod IPs are reachable across VPC networks.

See VPC Network Peering limits (/vpc/docs/quota#vpc-peering).

Q: My peering connection is set up, but I am not able to reach peer VMs or internal load balancers.

After the peering connection is ACTIVE, it may take up to a minute for all the traffic flows to be set up between the peered VPC networks. This time depends on the size of the VPC networks that are peering. If you have just set up the peering connection, please wait up to a minute and try again. Also, ensure that there are no firewall rules blocking access to/from peer VPC network subnet CIDRs.

Q: When I try to set up the peering connection, I get an error that another peering operation is in progress.

In order to avoid contention with routing updates and the like, GCP allows only one peering-related activity at a time across peered networks. For example, if you set up peering with one network and immediately try to set up another, all the tasks from the first peering may not have completed. It may take up to a minute for all tasks to complete. Alternatively, your existing network peer may be adding an internal load balancer or VM, both of which affect what is reachable between networks. In most cases, you should wait a minute or two and retry the peering operation.

Q: When I try to delete a VPC network with `ACTIVE` peerings, I get an error.

Before you can delete a VPC network (/vpc/docs/using-vpc#deleting_a_network), you must first delete all peering configurations in the network. See deleting a VPC network peering connection (#deleting-peer).

Q: Can you peer VPC networks that have subnets with overlapping primary or secondary IP ranges?

No. You can only peer VPC networks whose subnets have unique primary and secondary subnet IP ranges (/vpc/docs/vpc#manually_created_subnet_ip_ranges).

Q: How do I make sure new subnets I create in my VPC network will not have subnet IP ranges that conflict with subnets or routes in peer networks?

Before creating new subnets, you can list the routes from peering connections (#list-peer-routes). Make sure you do not use any of their destinations as either primary or secondary IP ranges when you create new subnets in your VPC network.

Q: I have a VPC network that is peered with another VPC network. I want to create a subnet in my VPC network. How do I create this subnet so that it does not overlap with my peer's peer subnets?

At this time, there is no command that helps you to find this. Please ask the admin of the peered network to find out what subnet routes are already in that network.

Q: Are there any security or privacy concerns with VPC peering?

After peering is set up, each VPC network knows the subnet ranges of the other network. In addition, each peer VPC network is able to send and receive traffic from the all VMs in the other network unless firewall rules are in place to prevent it. Other than that, peered networks do not have visibility into each other.

Q: How do I determine if there are any requests from other VPC networks to connect to my VPC network using VPC Network Peering?

There is no way to list any peering requests for your VPC network. You can only see the peering configurations that you have created.

VPC Network Peering requires that both your network and another network create a peering *configuration* to one another before a connection can be established. Even if a network administrator for another VPC network creates a peering configuration to your network, no peering *connection* will be created unless you create a peering configuration to that network.

Q: How do I make routes in a peer network available to an on-premises network connected to my VPC network using Cloud VPN or Cloud Interconnect?

VPC Network Peering does not support transitive routing; that is, imported routes from other networks are not automatically advertised by Cloud Routers in your VPC network. However, you can use custom IP range advertisements (/router/docs/how-to/advertising-custom-ip) from Cloud Routers in your VPC network to share routes to destinations in the peer network.

For Cloud VPN tunnels using static routing, you must configure static routes to the peer network's destination ranges in your on-premises network.

Q: Why are custom routes not exchanged between peered networks?

First, list the routes from your peering connections (#list-peer-routes). If you don't see routes to destinations that you expect, check the following:

- List peering connections (#list-peer-connections). Find the network with the desired destination ranges, and ensure that its peering state is `ACTIVE`. If the peering connection is `INACTIVE`, a peering configuration for your network does not exist in the other network. If you don't manage the other network, you'll need to coordinate with a network administrator who does.
- Update the peering configuration (#updating_a_peering_connection) in your network so that it is configured to import custom routes from the other network. Ensure that the other network has been configured to export its custom routes.

Q: Why is traffic destined for a peer network being dropped?

First, list peering connections (#list-peer-connections) to make sure your network is still connected to the other one. If the peering state is `INACTIVE`, a peering configuration for your network does

not exist in the other network. If you don't manage the other network, you'll need to contact a network administrator who does.

Next, list routes from peer connections (#list-peer-routes). You can only import as many routes as are allowed by the VPC Network Peering limits (/vpc/docs/quota#vpc-peering).

Q: Why is traffic being sent to an unexpected next hop?

Review the routing order (/vpc/docs/routes#routeselection) to see if another route was chosen instead.

Q: Why can't my VPC network peer with a particular VPC network?

If you cannot create a peering configuration with certain VPC networks, an organization policy might be constraining the VPC networks that your network can peer with. In the organization policy, add the network to the list of allowed peers or contact your organization administrator. For more information, refer to the `constraints/compute.restrictVpcPeering` (/resource-manager/docs/organization-policy/org-policy-constraints) constraint.

- See the Routes (/vpc/docs/routes) overview for more information on VPC routing.
- For limits related to VPC Network Peering, see VPC Network Peering limits (/vpc/docs/quota).
- See Using an internal TCP/UDP load balancer as a next hop (/load-balancing/docs/internal/ilb-next-hop-overview) for information on how to use an internal TCP/UDP load balancer as the next hop for a custom static route.