This document contains instructions for configuring alias IP addresses and alias IP ranges using the Google Cloud Console and `gcloud` command line tool. Please review the Alias IP overview (/vpc/docs/alias-ip/) page before executing these commands.

- The per network limits (/vpc/docs/quota#per_network) describe the maximum number of secondary ranges that you can define for each subnet.
- You cannot add *and* remove secondary ranges at the same time. Adding and removing must be done as separate steps.
- CIDR expansion is not supported for secondary ranges.

- Alias IP ranges are supported on all VM network interfaces. Routing is configured automatically for alias IP ranges on the primary network interface, but not secondary interfaces. If you have Multiple Network Interfaces (/vpc/docs/multiple-interfaces-concepts), you have to configure policy routing (/vpc/docs/create-use-multiple-interfaces#configuring_policy_routing) for the additional interfaces.
- A VM instance virtual interface can have up to 10 alias IP ranges assigned to it.
- Alias IP ranges can be added or deleted, but they can't be updated.
- If you remove an alias IP range from one VM and assign it to another VM, it might take up to a minute for the transfer to complete.
- Firewall source tags are not supported for alias IP addresses. This means that when you configure source tags in firewall rules, the source tags match the VM primary IP address, but not the alias IP addresses. Use source ranges to allow or deny ingress traffic from alias IP addresses.
- Internal DNS resolves a VM name to its primary IP. Additional names for alias IPs are not configured automatically, but may be added manually.

- A VPC network can have up to 7000 alias IP ranges across all VMs.
- Adding or removing a large number of alias IP ranges at the same time can take a long time. For example, it may take up to 10 minutes to add or delete 7000 alias IP ranges.
- Auto mode VPC networks cannot be deleted if secondary subnet ranges are present.
- In a static route, the next-hop IP address must be the primary IP address of the VM. Alias IP addresses are not supported as next-hop IP addresses.
- IPv6 addresses are not supported.
- Alias IP ranges are only supported in VPC networks, not legacy networks. To determine your network type, list your networks. VPC networks have a mode of `custom` or `auto`. Legacy networks have a mode of `legacy`.

VM alias IP ranges must be assigned from a range owned by the subnet that the VM is in. All subnets have a primary range, which is the standard range of internal IP addresses that defines the subnet. A subnet may also have one or more secondary IP ranges of internal IP addresses. You can assign alias IP ranges from either the primary or secondary ranges of the subnet.

You must give each secondary range a name that is unique for the subnet. When assigning an alias IP range to a VM, the secondary range name tells GCP from which subnet range to assign the alias IPs.

All ranges, both primary and secondary, must be unique across all subnets in the VPC network and in any networks attached via VPC Network Peering, VPN, or Interconnect.

This section shows you how to create a subnet with a secondary range, add a secondary range to an existing subnet, or remove a secondary range from a subnet. Once your subnet has the range you want to use, see the VM instance commands (#vm-instance-commands) for instructions on assigning a range to a VM.

This command assumes you have a VPC network already. If you do not, create one (/vpc/docs/using-vpc).

This command is the same whether you're creating a subnet for the VM's primary interface or one of the secondary interfaces (/vpc/docs/multiple-interfaces-concepts).

Using a secondary range for alias IP allocation allows you to separate the IP space for services hosted in the VM, making it easier to create firewall rules that allow access only to the services running on the VM and block access to the VM's primary IP address.

This procedure assumes you have a subnet that you want to use, but you need to add one or more secondary ranges.

Using a secondary range for alias IP allocation makes it easier to create firewall rules that allow access to the services running on a VM, but not to the VM's primary IP address.

These commands show how to create an instance with an alias IP range, add one or more alias IP ranges to an existing VM instance, or remove one or more ranges from an existing VM instance.

Use this procedure if you want to assign an alias IP range from the primary range of the subnet. The range you choose must not already be in use, even in part, by any other resource on the VPC network.

Use this procedure if you want the instance's primary interface and alias IP addresses to be in the same range.

Use this procedure if you want to assign an alias IP range taken from a secondary range of the subnet. Keeping the alias IP ranges separate from the primary range of the subnet makes it easier to create firewall rules that allow access to the services running on a VM, but not to the VM's primary IP address.

This example creates two networks, each with one subnet, and a VM with interfaces in both networks. If you already have two VPC networks, you can skip to the "create VM instance" step.

You can add an alias IP range to a running instance.

You can add more alias IP ranges to an existing instance or remove one or more ranges.

1. Verify that the network is a VPC network. Alias IPs are not supported on legacy networks.

   The network `MODE` should be "auto" or "custom".

2. If a subnet range name is specified, verify the following:

   - the subnet has a secondary range with the corresponding name
   - the requested alias IP range is inside this secondary range or, if using netmask, is smaller than the primary range.

3. If subnet range name is not specified, verify that the requested alias IP range is inside the primary subnet range or, if using netmask, is smaller than the primary range.

1. Verify firewall rules.

   a. List all firewall-rules:

   b. Verify that traffic to and from alias IP is allowed.

★ **Note:** source service account and source tags will only expand to primary network IPs of matching instances.

c. If necessary, add firewall rules to allow pinging alias IP:

2. Ensure that the VM recognizes the IP alias ranges as being local. On Linux distributions such as Debian, this can typically be done as follows.

   a. Connect to the instance (/compute/docs/instances/connecting-to-instance) and run this command:

   The output should contain the following:

   b. Ensure that `ip_alias = true` in `/etc/default/instance_configs.cfg`. If you have to change this, you must also restart the routing daemon:

   c. If local route is not present, configure it using this command:

Secondary IP ranges are not listed as regular subnets. In order to show that the subnet secondary IP range has been created, use the `gcloud compute networks subnets describe` command.

1. Create a subnet.

2. List your subnets.

3. Get details on a subnet to see the secondary ranges.

When creating a VM, if you get an error saying that the secondary range does not exist, ensure the following:

- That the subnet has a secondary range with the specified name.
- That you are creating your VM within the subnet that has the secondary range.

You can see this error by running the following commands:

1. Create a subnet with a secondary range.

2. Create an instance in another network, such as the default network, rather than in the newly created subnet.

3. Try to assign an alias IP range from the subnet created in step 1. The command will fail because the secondary range is in a different subnet than the instance.

4. Create another instance, this one with its interface in the subnet created in step 1.

5. Add an alias IP range to the interface. This time the command succeeds because the interface and the secondary range are in the same subnet.

Adding and removing subnetwork secondary IP ranges in the same command is not currently supported. The gcloud commands to add and remove secondary ranges will preserve the existing

ranges that are not modified.

To add and remove ranges, run the two commands separately.

To see more details for this command, use `gcloud compute networks subnets update --help`.

Adding and removing VM alias IP ranges in the same request is currently not supported.

The `gcloud` command to update alias IP ranges does NOT preserve the existing ranges, so omitting a range is treated as a request to delete that range.

For example, if the current VM has alias range `10.9.27.0/24` and the new requested range is `/24`, running the command to request the `/24` will be rejected as it is interpreted as removing `10.9.27.0/24` and adding `/24`. The existing range must be explicitly removed before you can add the new range.

Example:

1. Create alias IP range.

2. Try to add `/24` without specifying the existing range. An error results.

3. Update the VM to have no alias IP range.

4. Add the new alias IP range.

To see more details for this command, use `gcloud compute instances network-interfaces update --help`.

Firewall source service account and source tags only expand to primary network IPs of matching instances and do not apply to alias IPs of matching instances. So, a firewall rule based on source tags will not affect traffic from an instance alias IP address. Alias IP addresses can be added to firewall rules as source or destination ranges.

See Troubleshooting for multiple interfaces (/vpc/docs/create-use-multiple-interfaces).

On Kubernetes clusters, the `ALIAS_IP_RANGE` local route conflicts with and disables `cbr0` causing Pods to lose network connectivity.

As such this route is disabled on GKE's Container-Optimized OS images.

Users wishing to use Alias IPs on self-managed clusters using Google Cloud provided images may need to take steps exclude this route.

Symptoms:

- If this conflict arises, Kubernetes Pods will have no network access

- A packet capture on the Linux bridge device (`tcpdump -ni cbr arp`) run while the pods attempt to raise outbound connections will show the pods ARPing for their gateway's MAC address. The gateway, `cbr0`, does not issue an ARP response despite being up.
- `ip route show table local` shows `ALIAS_IP_RANGE` on `eth0`

Fix:

- Set `ip_forwarding_daemon = false` in `/etc/default/instance_configs.cfg` on the affected nodes. This prevents the route from being reinstalled after deletion
- Restart the IP forwarding daemon: `service google-ip-forwarding-daemon restart`
- Manually delete existing route: `sudo ip route del local ALIAS_IP_RANGE dev eth0`

- Read more about instances (/compute/docs/instances/)