

In this lab, you'll learn the Compute Engine Subnetwork model. Subnetwork allows you to create your own network topology as you would in your own on-premise datacenter, so that you can assign specific IP address ranges to groups of machines.

- Differences between legacy network model and subnetwork.
- Learn about regional subnetwork.
- Setup custom subnetworks.

gcloud auth list - list the active account name with this command:

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud auth list
Credentialed Accounts

ACTIVE: *
ACCOUNT: student-00-e909601900c8@qwiklabs.net

To set the active account, run:
$ gcloud config set account `ACCOUNT`
```

list the project ID with this command: gcloud config list project

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud config list project
[core]
project = qwiklabs-gcp-00-f9ef3a2a350a

Your active configuration is: [cloudshell-19240]
```

gcloud config set compute/zone europe-west1-c

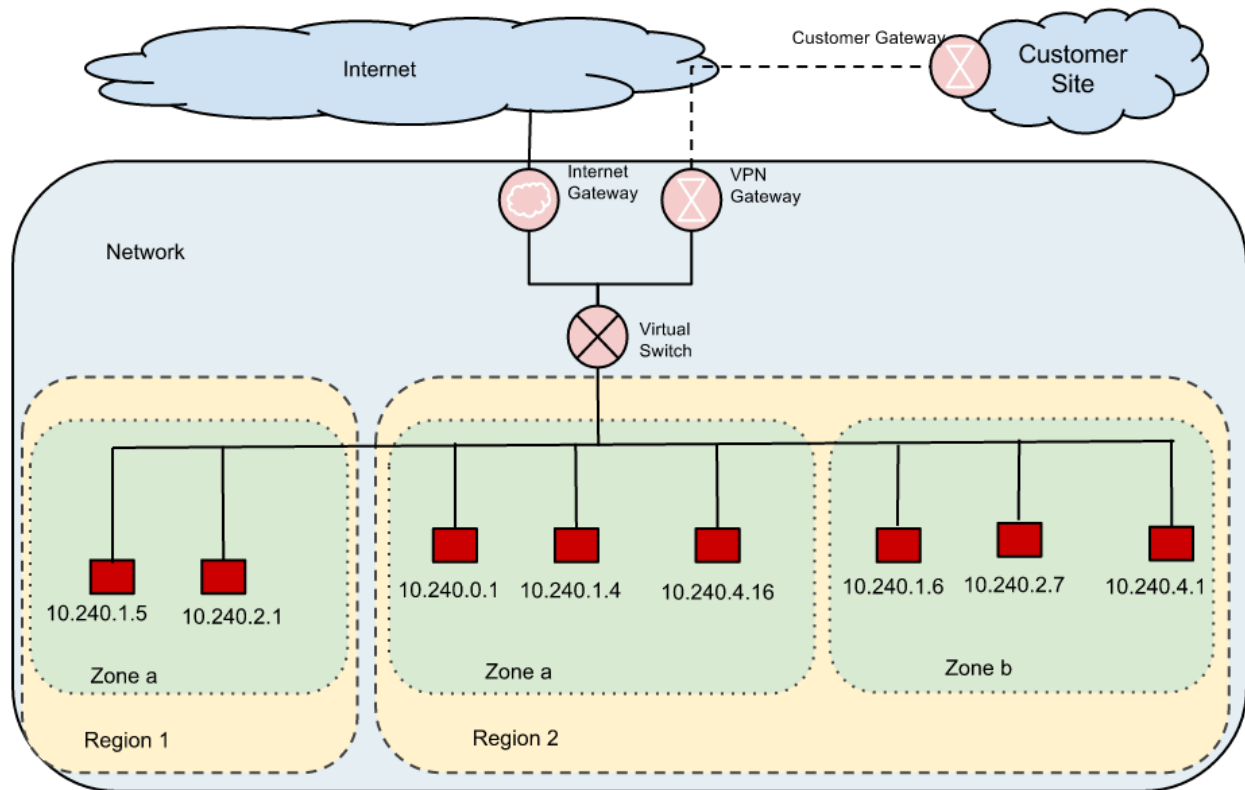
gcloud config set compute/region europe-west1

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud config set compute/zone europe-west1-c
gcloud config set compute/region europe-west1
Updated property [compute/zone].
Updated property [compute/region].
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$
```

Traditionally in Compute Engine, you define a single network IPv4 prefix range for all the virtual machine instances attached to that network, and that network spans all Cloud Platform regions.

Each instance within a network is assigned an IPv4 address from a global network IPv4 range. Instance IP addresses are not grouped by region or zone. One IP address might appear in one region, and its neighbor might be in a different region. Any given range of IPs can be spread across all regions, and the IP addresses of instances created within a region are not necessarily contiguous.

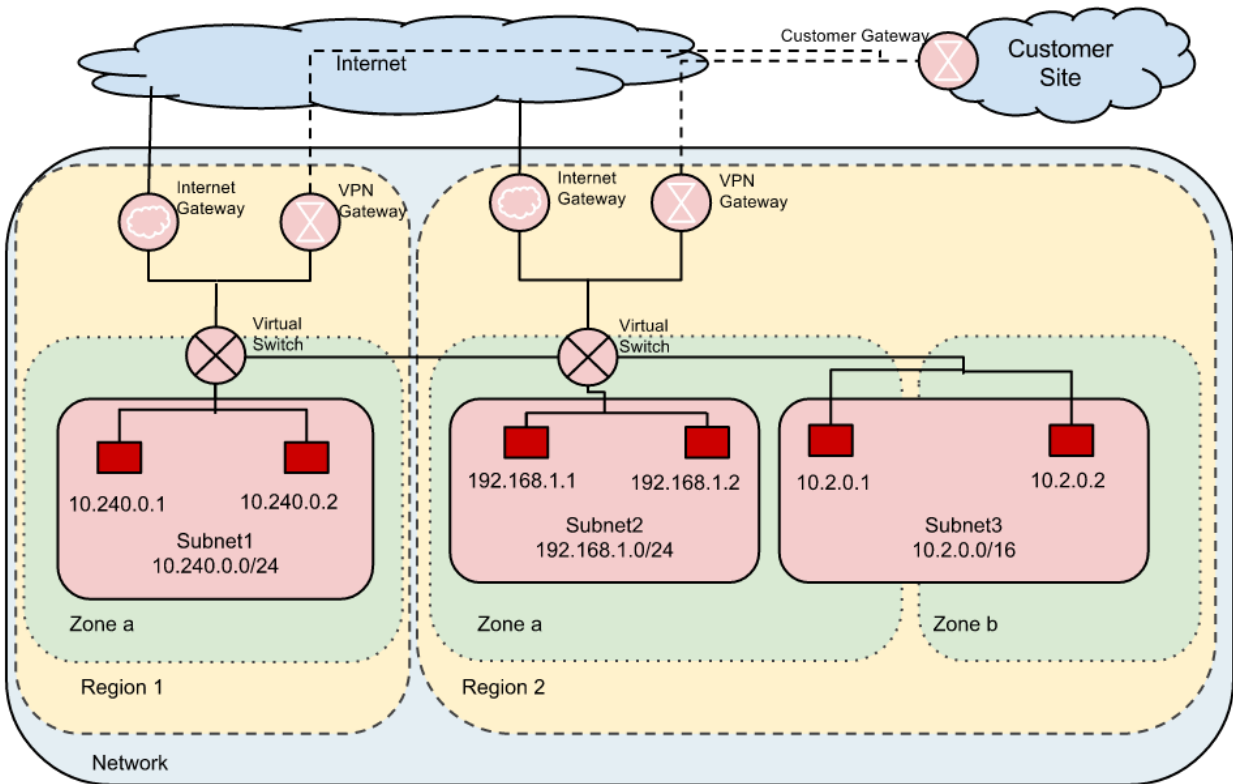
For example, if you have virtual machine instances in two Google Cloud regions, and different zones, each of the instance will be assigned an IP address from the global pool, like this:



As a result, in the legacy network mode, you won't be able to group your instances into different logical subnetworks like you do in your on-premise networks.

Compute Engine now supports creating your own subnetworks, and it's turned on by default for new projects. Read on to learn more.

You can let Google Kubernetes Engine automatically create and manage subnetworks based on region. It can automatically assign a [subnetwork IP prefix range](#) to each region in your network. The instances created in a zone in a specific region in your network get assigned an IP allocated from the regional subnetwork range. This is the default mode for any new Google Cloud projects.



You can see your current network setup two ways, from the Cloud Console, or from command line.

2. In the **VPC Networks** page, select the tab **Subnets in Current Project**.

You will see that your project is already configured with automatic regional subnetworks, and there are different subnetworks created for each of the regions:

VPC network	VPC networks + CREATE VPC NETWORK REFRESH HELP ASSISTANT							
VPC networks	<div> <div>NETWORKS IN CURRENT PROJECT</div> <div>SUBNETS IN CURRENT PROJECT</div> </div> <div>Filter Enter property name or value</div>							
IP addresses	Name	Region	VPC network ↑	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways	Flow logs
Bring your own IP	default	asia-east1	default	10.140.0.0/20	None	None	10.140.0.1	Off
Firewall	default	asia-northeast1	default	10.146.0.0/20	None	None	10.146.0.1	Off
Routes	default	asia-south1	default	10.160.0.0/20	None	None	10.160.0.1	Off
VPC network peering	default	asia-southeast1	default	10.148.0.0/20	None	None	10.148.0.1	Off
Shared VPC	default	australia-southeast1	default	10.152.0.0/20	None	None	10.152.0.1	Off
Serverless VPC access	default	europa-central2	default	10.186.0.0/20	None	None	10.186.0.1	Off
Packet mirroring	default	europa-north1	default	10.166.0.0/20	None	None	10.166.0.1	Off
	default	europa-west1	default	10.132.0.0/20	None	None	10.132.0.1	Off
	default	europa-west2	default	10.154.0.0/20	None	None	10.154.0.1	Off
	default	europa-west3	default	10.156.0.0/20	None	None	10.156.0.1	Off
	default	europa-west4	default	10.164.0.0/20	None	None	10.164.0.1	Off
	default	me-west1	default	10.208.0.0/20	None	None	10.208.0.1	Off

You can get the same information from the console.

4. In Cloud Shell, list existing networks:

gcloud compute networks list

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a) $ gcloud compute networks list
NAME: default
SUBNET_MODE: AUTO
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a) $
```

This shows the default network with the automatic regional subnetwork mode.

5. To see the actual subnetwork ranges, run:

gcloud compute networks subnets list

```
NAME: default
REGION: us-central1
NETWORK: default
RANGE: 10.128.0.0/20
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
.....
```

6. Now, create two different virtual machines, each in a different region:

```
gcloud compute instances create instance-1 --zone us-east1-b
```

```
gcloud compute instances create instance-2 --zone us-central1-c
```

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute instances create instance-1 --zone us-east1-b
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/zones/us-east1-b/instances/instance-1].
NAME: instance-1
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 104.196.182.117
STATUS: RUNNING
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute instances create instance-2 --zone us-central1-c
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/zones/us-central1-c/instances/instance-2].
NAME: instance-2
ZONE: us-central1-c
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.128.0.2
EXTERNAL_IP: 34.133.139.38
STATUS: RUNNING
```

8. Run the following to check their IP addresses - they should belong to the same subnet range for the respective region that the zone belongs to:

```
gcloud compute instances list
```

```

student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute instances list
NAME: instance-2
ZONE: us-central1-c
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.128.0.2
EXTERNAL_IP: 34.133.139.38
STATUS: RUNNING

NAME: instance-1
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 10.142.0.2
EXTERNAL_IP: 104.196.182.117
STATUS: RUNNING

```

Custom Subnetworks allows you to manually define subnetwork IP range for each region in your network. There can be zero, one, or several subnetwork IP ranges created per region for a network. In order to create an instance in a zone, you must have previously created at least one subnetwork in that region. At instance creation time, you will need to specify the subnetwork in the region that the instance IP should be allocated from.

1. Create a new network topology that supports custom subnetworks:

```
gcloud compute networks create custom-network1 --subnet-mode custom
```

```

student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute networks create custom-network1 --subnet-mode custom
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/global/networks/custom-network1].
NAME: custom-network1
SUBNET_MODE: CUSTOM
BGP_ROUTING_MODE: REGIONAL
IPV4_RANGE:
GATEWAY_IPV4:

Instances on this network will not be reachable until firewall rules
are created. As an example, you can allow all internal traffic between
instances as well as SSH, RDP, and ICMP by running:

$ gcloud compute firewall-rules create <FIREWALL_NAME> --network custom-network1 --allow tcp,udp,icmp --source-ranges <IP_RANGE>
$ gcloud compute firewall-rules create <FIREWALL_NAME> --network custom-network1 --allow tcp:22,tcp:3389,icmp

```

2. Next, create a custom subnet in the us-central1 region:

```
gcloud compute networks subnets create subnet-us-central-192 \
```

```
--network custom-network1 \
```

```
--region us-central1 \
```

--range 192.168.1.0/24

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute networks subnets create subnet-us-central-192 \
--network custom-network1 \
--region us-central1 \
--range 192.168.1.0/24
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/regions/us-central1/subnetworks/subnet-us-central-192].
NAME: subnet-us-central-192
REGION: us-central1
NETWORK: custom-network1
RANGE: 192.168.1.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

3. Next, create a custom subnet in the europe-west1 region:

```
gcloud compute networks subnets create subnet-europe-west-192 \
```

--network custom-network1 \

--region europe-west1 \

--range 192.168.5.0/24

```
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute networks subnets create subnet-europe-west-192 \
--network custom-network1 \
--region europe-west1 \
--range 192.168.5.0/24
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/regions/europe-west1/subnetworks/subnet-europe-west-192].
NAME: subnet-europe-west-192
REGION: europe-west1
NETWORK: custom-network1
RANGE: 192.168.5.0/24
STACK_TYPE: IPV4_ONLY
IPV6_ACCESS_TYPE:
INTERNAL_IPV6_PREFIX:
EXTERNAL_IPV6_PREFIX:
```

4. You can then list all of your subnetworks:

```
gcloud compute networks subnets list
```

5. Then you can create instances in the different subnetworks:

```
gcloud compute instances create instance-3 \
```

--zone us-central1-a \

--subnet subnet-us-central-192


```

student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute instances create instance-3 \
--zone us-central1-a \
--subnet subnet-us-central-192
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/zones/us-central1-a/instances/instance-3].
NAME: instance-3
ZONE: us-central1-a
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 192.168.1.2
EXTERNAL_IP: 35.184.26.188
STATUS: RUNNING

```

6. And another one:

```
gcloud compute instances create instance-4 \
```

```
--zone europe-west1-d \
```

```
--subnet subnet-europe-west-192
```

```

STATUS: RUNNING
student_00_e909601900c8@cloudshell:~ (qwiklabs-gcp-00-f9ef3a2a350a)$ gcloud compute instances create instance-4 \
--zone europe-west1-d \
--subnet subnet-europe-west-192
Created [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00-f9ef3a2a350a/zones/europe-west1-d/instances/instance-4].
NAME: instance-4
ZONE: europe-west1-d
MACHINE_TYPE: n1-standard-1
PREEMPTIBLE:
INTERNAL_IP: 192.168.5.2
EXTERNAL_IP: 34.76.80.8
STATUS: RUNNING

```

In the automatic regional network, all virtual machine instances within a network can communicate with each other, because it automatically created firewall rules to open communication between the different regional networks. However, custom subnetworks do not have default firewall rules, so an instance in one custom subnetwork cannot reach an instance in another custom subnetwork.

To allow inter-subnetwork communication, you'll need to create firewall rules. We won't have time to go through this in this lab. But you can learn more about this advanced topic in the [Subnetwork documentation](#).

All virtual machine instances within a network can communicate with each other.

Each subnet in VPC network is associated with a region and not with zone.