

# Virtual Networking

## Overview

In this lab you build and explore a complex GCP network structure. In most labs you choose the regions and zones where objects are located; however, this lab is prescriptive about the network layout. The lab systematically highlights the differences between placing instances in a variety of network locations and depending on the instances relative location, how you establish communications between virtual machines.

## Objectives

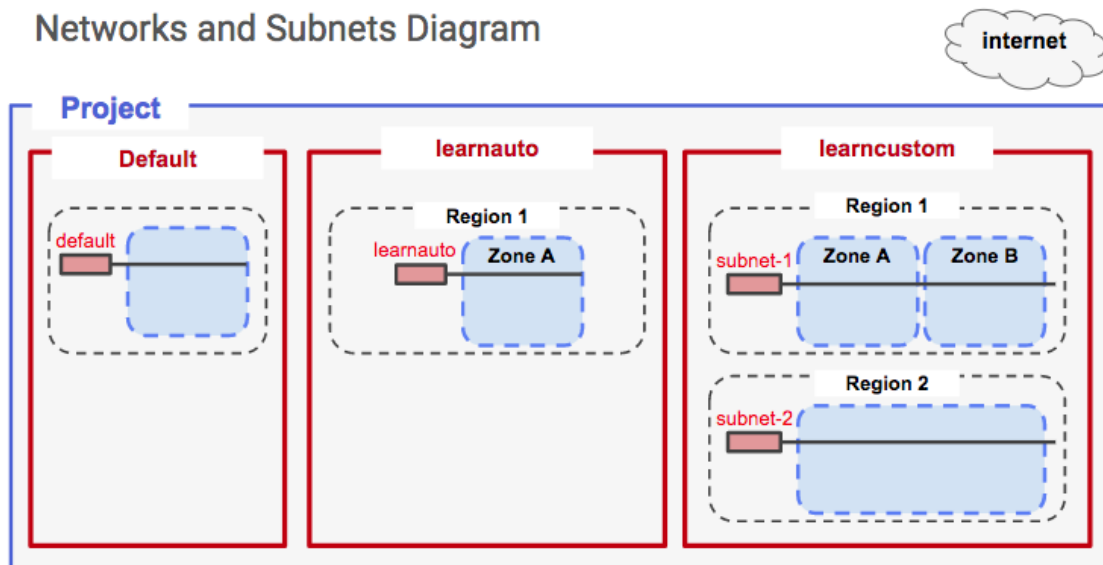
In this lab, you learn how to perform the following tasks:

- Create an auto-mode network, a custom-mode network, and associated subnetworks
- Compare connectivity in the various types of networks
- Create routes and firewall rules using IP addresses and tags to enable connectivity
- Convert an auto-mode network to a custom-mode network
- Create, expand, and delete subnetworks

Here is a preview of the lab activities and the networks you will create:

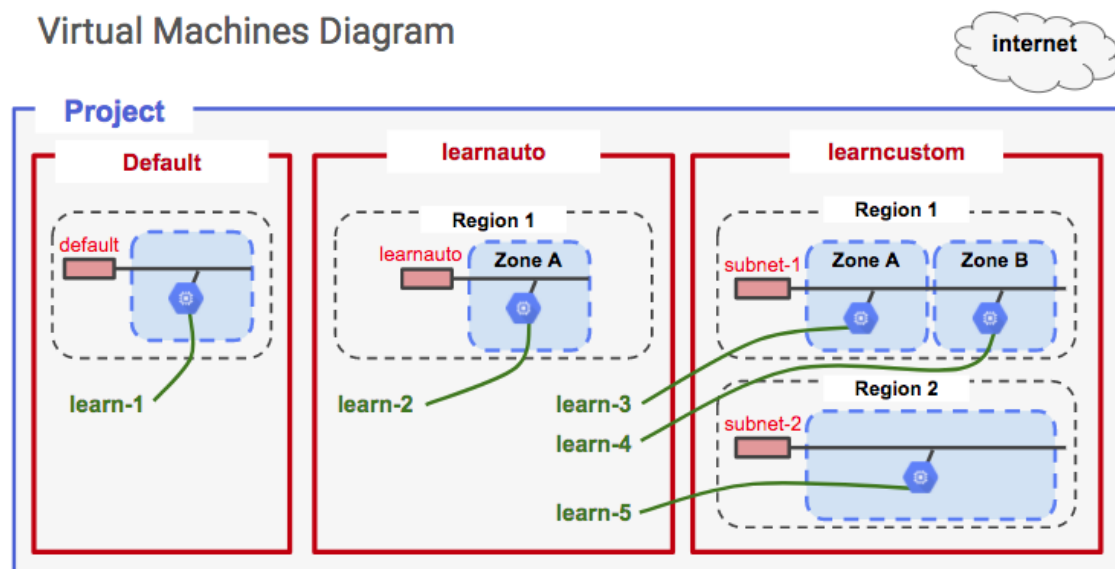
## Task 1: Create the network topology

### Networks and Subnets Diagram



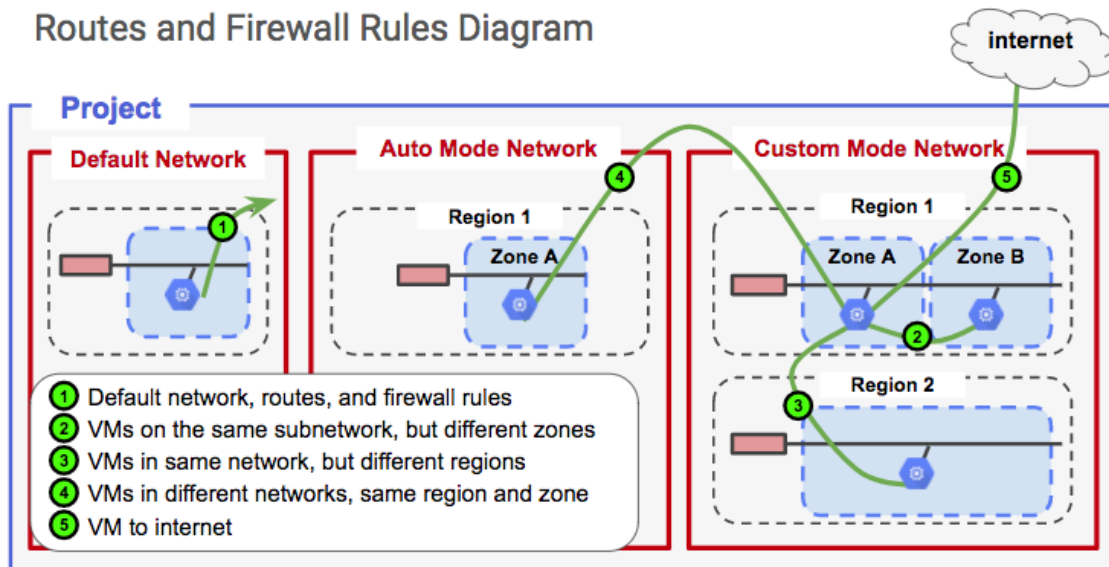
## Task 2: Create the VM instances

### Virtual Machines Diagram



## Task 3: Work with routes and firewall rules

## Routes and Firewall Rules Diagram



The scoping and connectivity relationships between zones, regions, networks, and subnets are different from networking in other public clouds.

You have been provided with a project in Qwiklabs. The project ID is a unique name across all Google Cloud projects. It is referred to later in this lab as `PROJECT_ID`.

Note: In most labs in this class, you choose any region and any zone for the purposes of the lab. In this lab, you are given specific regions and zones because you will construct and explore very specific networking relationships.

### What you'll need

To complete this lab, you'll need:

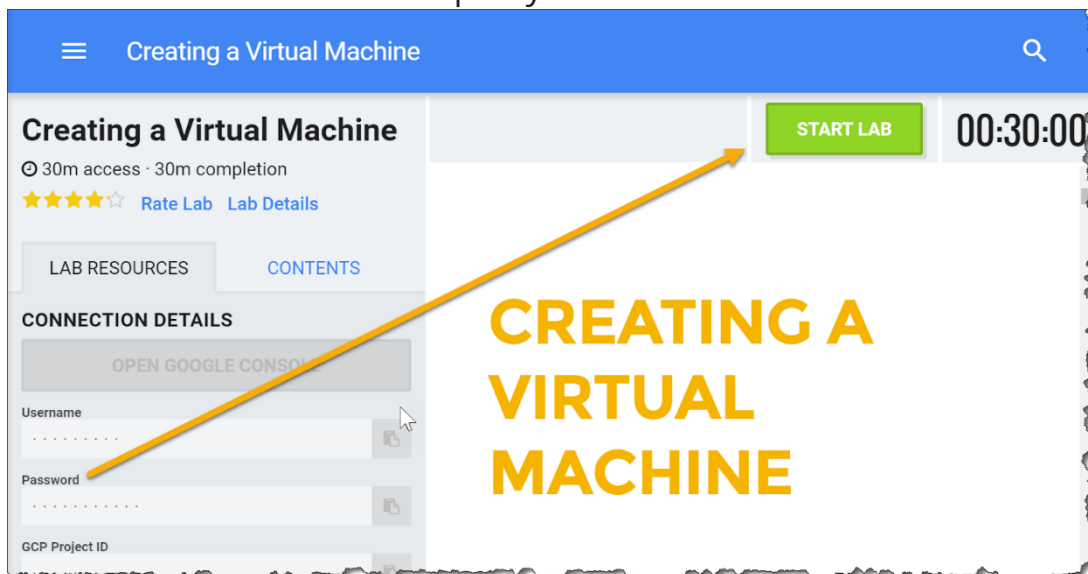
- Access to a standard internet browser (Chrome browser recommended).
- Time. Note the lab's **Completion** time in Qwiklabs, which is an estimate of the time it should take to complete all steps. Plan your schedule so you have time to complete the lab. Once you start the lab, you will not be able to pause and return later (you begin at step 1 every time you start a lab).
- You do NOT need a Google Cloud Platform account or project. An account, project and associated resources are provided to you as part of this lab.
- If you already have your own GCP account, make sure you do not use it for this lab.

- If your lab prompts you to log into the console, **use only the student account provided to you by the lab**. This prevents you from incurring charges for lab activities in your personal GCP account.  
Use a new Incognito window (Chrome) or another browser for the Qwiklabs session. Alternatively, you can log out of all other Google / Gmail accounts before beginning the labs.



## Start your lab

When you are ready, click **Start Lab**. You can track your lab's progress with the status bar at the top of your screen.

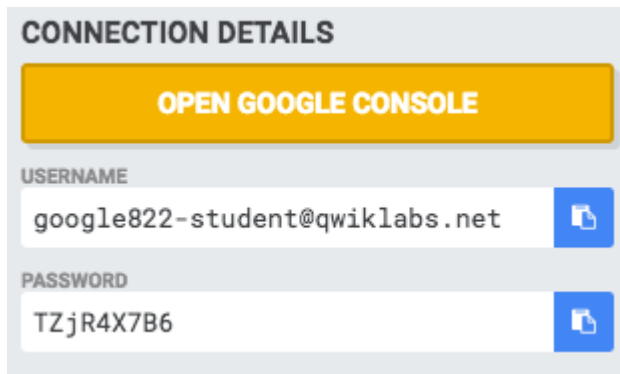


**Important:** What is happening during this time?

Your lab is spinning up GCP resources for you behind the scenes, including an account, a project, resources within the project, and permission for you to control the resources you will need to run the lab. This means that instead of spending time manually setting up a project and building resources from scratch as part of your lab, you can begin learning more quickly.

## Find Your Lab's GCP Username and Password

To access the resources and console for this lab, locate the Connection Details panel in Qwiklabs. Here you will find the account ID and password for the account you will use to log in to the Google Cloud Platform:



If your lab provides other resource identifiers or connection-related information, it will appear on this panel as well.

## Task 1: Create the network topology

### Explore the default network

The default network is created automatically for you with each new project. The default network layout is not ideal for managing resources. The main benefit is that it is a fast way to get a project set up and running. The default network is great for prototyping solutions and for training purposes.

1. In the Google Cloud Platform (GCP) Console, on the **Navigation** menu () , click **VPC network > VPC networks**.

Notice the default network. It was created automatically for you with a subnetwork in each region.

Example:

asia-east1 | default | 10.140.0.0/20 | 10.140.0.1

For more information, see:

IP Addresses: <https://cloud.google.com/compute/docs/ip-addresses/>

Subnets and CIDR ranges: [https://cloud.google.com/compute/docs/alias-ip/#subnets\\_and\\_cidr\\_ranges](https://cloud.google.com/compute/docs/alias-ip/#subnets_and_cidr_ranges)

2. In the left pane, click **Routes**.

Notice that a route was created for each subnetwork, and one global route was created to enable traffic to the internet.

## Create an auto-mode network and subnets

1. In the left pane, click **VPC networks**.
2. Click **Create VPC network**.
3. Specify the following:

Property	Value (type value or select option as specified)
Name	learnauto
Description	Learn about auto-mode networks
Subnet creation mode	Automatic

When you click **Automatic**, the list of subnetworks to be created is automatically displayed.

4. For **Firewall rules**, select all listed firewall rules.
5. At the bottom of the page are two links labeled **Equivalent REST** or **command line**. Click **REST** to see POST commands for API programming automation of this process.
6. Click **Close**.
7. Click **command line** to see commands you could use for automation of this process. You could use these commands to create the network by clicking RUN IN CLOUD SHELL—but *don't do it*.

Note: These commands tend to include options that are not required. They may not work in a bash script without being altered. Don't rely on them. You should consider these more of a suggestion. If you need to

automate with scripts, plan to craft your own commands from examples in the documentation.

8. Click **Close**.
9. Click **Create**.
10. Click **REFRESH** occasionally until the networks are created and appear in the list.

## Explore the auto-mode network

1. In the left pane, click **Routes**.

Notice that a route has been created for each subnetwork, and one route was created to enable traffic from anywhere, including the internet. Traffic is delivered via the most specific matching route: traffic intended for any of the listed subnets gets delivered via virtual network to the host. These routes take precedence over the route that matches all traffic.

2. Click **Destination IP ranges** to sort the list of routes.

Notice that there is an identical subnetwork and route in the learnauto network as there is in the default network. It is possible to have VMs with duplicate Internal IP addresses in the two networks.

3. In the left pane, click **Firewall rules**.

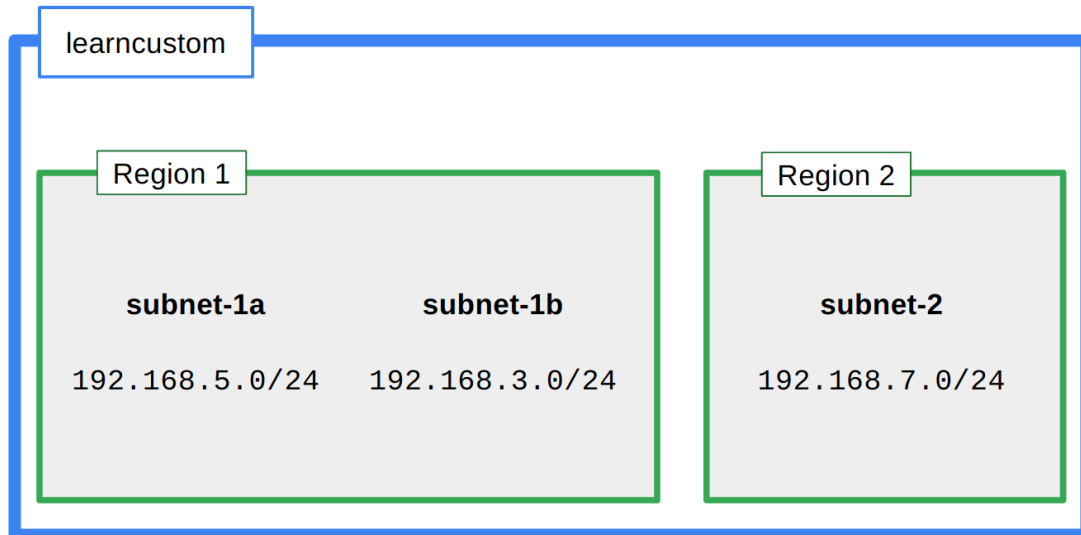
Verify that firewall rules were created for the learnauto network and its subnetworks.

If you delete your default network, you can always recreate it as an auto network using the name "Default."

## Create a custom-mode network

In this subtask, you create a custom-mode network named **learncustom** with three subnetworks:

- **(subnet-1a)** 192.168.5.0/24
- **(subnet-1b)** 192.168.3.0/24, in the same region
- **(subnet-2)** 192.168.7.0/24 in a different region



1. In the left pane, click **VPC networks**.
2. Click **Create VPC network**.
3. Specify the following:

Property	Value (type value or select option as specified)
Name	learncustom
Description	Learn about custom networks
Subnet creation mode	Custom

Use the dialog to add three subnets as follows.

4. For the first subnet, specify the following:

Property	Value (type value or select option as specified)
Name	subnet-1a
Region	us-east1
IP address range	192.168.5.0/24

5. Click **Add subnet**.



6. For the second subnet, specify the following:

Property	Value (type value or select option as specified)
Name	subnet-1b
Region	us-east1
IP address range	192.168.3.0/24

7. Click **Add subnet**.

8. For the third subnet, specify the following:

Property	Value (type value or select option as specified)
Name	subnet-2
Region	us-west1
IP address range	192.168.7.0/24

9. Click **Create**.

## Explore the routes and firewall rules

Did creating the custom network automatically create routes?

1. In the left pane, click **Routes**.
2. Click **Network** in the table header to sort by network name. Routes should be displayed for each subnetwork.

Did creating the custom network automatically create firewall rules?

3. In the left pane, click **Firewall rules**.
4. Click **Network** in the table header to sort by network name. No default firewall rules were created for the custom network. You will have to manually add default rules in the next step.

## Create firewall rules for the learncustom network

Notice that for the other networks, the default network and the learnauto network, GCP automatically created default firewall rules allowing SSH traffic (tcp:22), icmp traffic, and rdp (tcp:3389) traffic for Windows VMs.

Add a firewall rule to provide the same access for the learncustom network.

1. Click **Create firewall rule**.
2. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	<b>allow-ssh-icmp-rdp-learncustom</b>
Network	<b>learncustom</b>
Target tags	<b>allow-defaults</b>
Source IP ranges	<b>0.0.0.0/0</b>
Protocols and ports	<b>Specified protocols and ports</b>

3. For **tcp**, specify ports **22** and **3389**.
4. Specify the **icmp** protocol.

Make sure that the source filter address includes the final "/0". If you specify 0.0.0.0 instead of 0.0.0.0/0, the filter defaults to 0.0.0.0/32, which is an exact host address that doesn't exist.

5. Click **Create**.

## Create firewall rules for the learncustom network

In this subtask, you attempt to modify the network by adding a subnet with an overlapping address range but in a different region. What do you predict will happen?

1. In the left pane, click **VPC networks**.
2. Click **learncustom**.
3. Click **Add subnet**.
4. Specify the following, leaving all other values with their defaults:

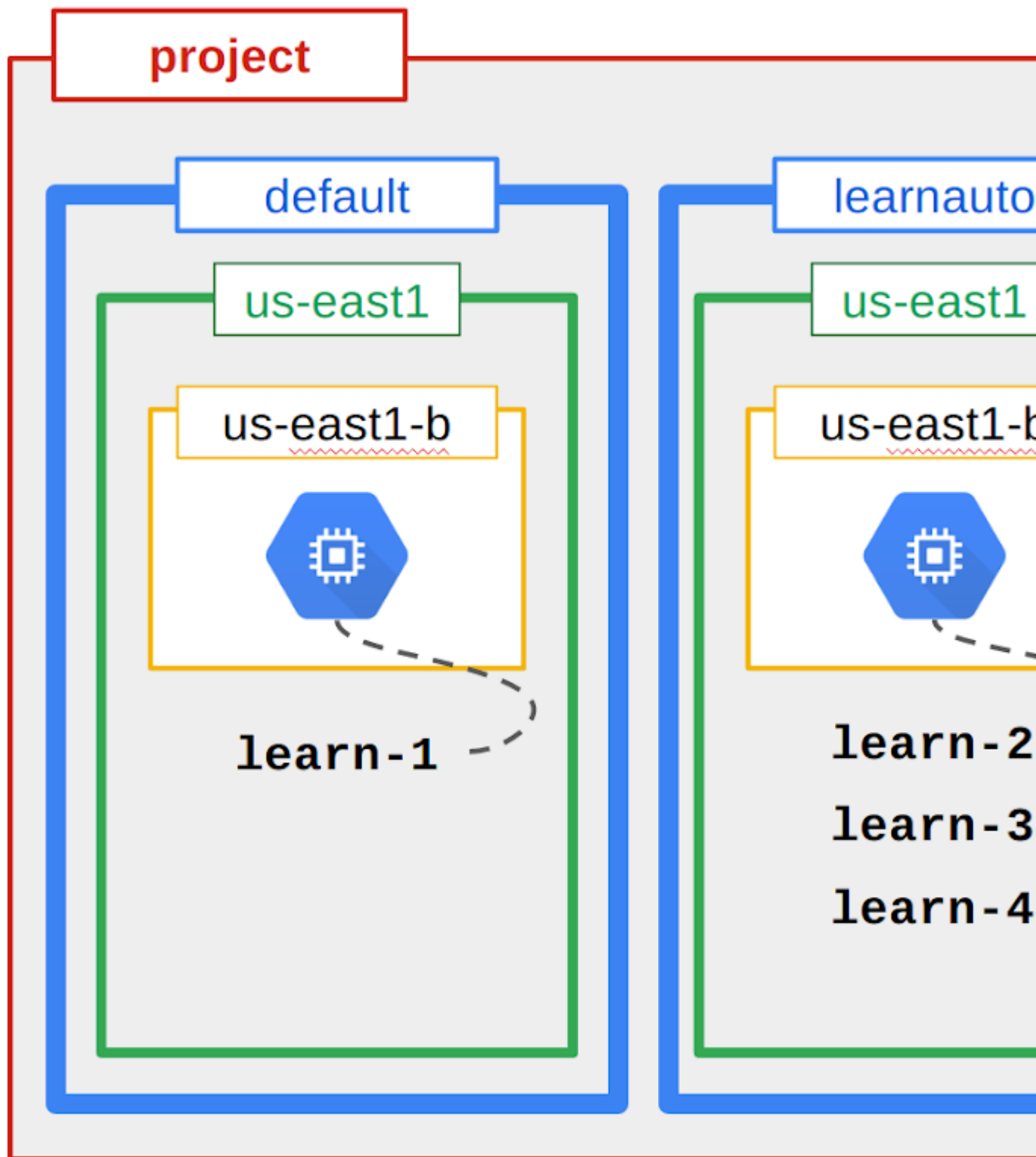
Property	Value (type value or select option as specified)
Name	subnet-3
Region	europe-west1
IP address range	192.168.5.0/24

The IP address range label is displayed in red with the following error message: "This IP address range overlaps with a subnet you already added. Enter an address range that doesn't overlap."

5. Click **CANCEL**.

## Task 2: Create the VM instances


To explore the Cloud Virtual Network, you create five micro VMs in different locations in the network. You will not install any additional software on them. They will not run any applications. You will just use them to explore the connectivity across the topologies in the network.



Name	Network	Region	Zone
learn-1	default	us-east1	us-east1-b

learn-2	learnauto	us-east1	us-east1-b
learn-3	learncustom	us-east1	us-east1-b
learn-4	learncustom	us-east1	us-east1-c
learn-5	learncustom	us-west1	us-west1-a

## Create the learn-1 VM

1. On the **Navigation menu** () , click **Compute Engine > VM instances**.
2. Click **Create**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
<b>Name</b>	<b>learn-1</b>
<b>Region</b>	<b>us-east1</b>
<b>Zone</b>	<b>us-east1-b</b>
<b>Machine type</b>	<b>micro (1 shared vCPU)</b>

4. Click **Management, security, disks, networking, sole tenancy** to access the advanced options.
5. Click **Networking**. The default network interface should already be selected.
6. Click **Create**.

## Create the learn-2 VM

1. Click **Create instance**.
2. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
----------	---

<b>Name</b>	<b>learn-2</b>
<b>Region</b>	<b>us-east1</b>
<b>Zone</b>	<b>us-east1-b</b>
<b>Machine type</b>	<b>micro (1 shared vCPU)</b>

3. Click **Management, security, disks, networking, sole tenancy** to access the advanced options.
4. Click **Networking**.
5. Click the pencil icon to edit **Network interfaces**.
6. Specify the following, and leave the remaining settings as their defaults:

<b>Property</b>	<b>Value</b> (type value or select option as specified)
<b>Network</b>	<b>learnauto</b>
<b>Subnetwork</b>	<b>learnauto</b>

7. Click **Done**.
8. Click **Create**.

## Create the learn-3 VM

1. Click **Create instance**.
2. Specify the following, and leave the remaining settings as their defaults:

<b>Property</b>	<b>Value</b> (type value or select option as specified)
<b>Name</b>	<b>learn-3</b>
<b>Region</b>	<b>us-east1</b>
<b>Zone</b>	<b>us-east1-b</b>
<b>Machine type</b>	<b>micro (1 shared vCPU)</b>

3. Click **Management, security, disks, networking, sole tenancy** to access the advanced options.
4. Click **Networking**.
5. Click the pencil icon to edit **Network interfaces**.
6. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Network	learncustom
Subnetwork	subnet-1a

7. Click **Done**.
8. Click **Create**.

## Create the learn-4 VM

1. Click **Create instance**.
2. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	learn-4
Region	us-east1
Zone	us-east1-c
Machine type	micro (1 shared vCPU)

3. Click **Management, security, disks, networking, sole tenancy** to access the advanced options.
4. Click **Networking**.
5. Click the pencil icon to edit **Network interfaces**.
6. Specify the following, and leave the remaining settings as their defaults:

Property	Value
----------	-------

	(type value or select option as specified)
<b>Network</b>	<b>learncustom</b>
<b>Subnetwork</b>	<b>subnet-1b</b>

7. Click **Done**.
8. Click **Create**.

## Create the learn-5 VM

1. Click **Create instance**.
2. Specify the following, and leave the remaining settings as their defaults:

<b>Property</b>	<b>Value</b> (type value or select option as specified)
<b>Name</b>	<b>learn-5</b>
<b>Region</b>	<b>us-west1</b>
<b>Zone</b>	<b>us-west1-a</b>
<b>Machine type</b>	<b>micro (1 shared vCPU)</b>

3. Click **Management, security, disks, networking, sole tenancy** to access the advanced options.
4. Click **Networking**.
5. Click the pencil icon to edit **Network interfaces**.
6. Specify the following, and leave the remaining settings as their defaults:

<b>Property</b>	<b>Value</b> (type value or select option as specified)
<b>Network</b>	<b>learncustom</b>
<b>Subnetwork</b>	<b>subnet-2</b>

7. Click **Done**.
8. Click **Create**.



## Verify that all the test VMs are running

1. On the **VM instances** page, verify that all 5 instances are running.

## Task 3: Work with routes and firewall rules

In this task, you connect via SSH to the VMs and use ping to test connectivity between VMs. This helps you understand how the Cloud Virtual Network topology behaves.

Google Cloud Platform (GCP) Virtual Private Cloud (VPC) networks have an internal DNS service that allows you to use instance names instead of instance IP addresses to refer to Compute Engine virtual machine (VM) instances.

Each instance has a metadata server that also acts as a DNS resolver for that instance. DNS lookups are performed for instance names. The metadata server itself stores all DNS information for the local network and queries Google's public DNS servers for any addresses outside of the local network.

An instance is not aware of any external IP address assigned to it. Instead, the network stores a lookup table that matches external IP addresses with the internal IP addresses of the relevant instances.

To break out of the ping command at any time, press **Ctrl+C**.

### ping from learn-1 and learn-2

1. On the **VM instances** page, for **learn-1**, click **SSH**.
2. Run the following command:

```
ping learn-1
```

Notice how DNS translates for you. This should execute and display no packet loss.

3. Now try to reach learn-2:

```
ping learn-2
```

Can you explain why this fails?

It is because DNS is scoped to network. The VM learn-2 is not in the default network where learn-1 is located. So the symbolic name can't be translated.

Locate the internal IP address and the external IP address for learn-2.

4. Try to ping learn-2's internal IP address:

```
ping <learn-2's internal IP>
```

Did this work?

In a few cases you may try to ping the internal IP of the other machine and it succeeds! Do you know why this would be the case?

Because ... the internal IP of the machine you are using could be the same as the internal IP of the VM in the other network. In this case, the ping would succeed because you are actually pinging your own local VM's interface, not the one on the other VM in the other network. You can't ping an internal IP address that exists in a separate network than your own.

When you create a new auto-mode network, the IP ranges will be identical to the ranges in the default network. The first address in the range is always reserved for the gateway address. So it is actually likely that the first VM in a zone will have the same address as the first VM in the corresponding zone in another network.

If it didn't work... learn-1 is in the default network and learn-2 is in the learnauto network. Even though both VMs are located in the same region, us-east1, and in the same zone, us-east-1b, they cannot communicate over internal IP.

5. Try to ping learn-2's external IP address:

```
ping <learn-2's external IP>
```

This works.

## traceroute from learn-1

1. From the learn-1 SSH terminal, install traceroute:

```
sudo apt-get install traceroute
```

2. Verify that traceroute is working by tracing the route to a public website:

```
sudo traceroute google.com -I
```

Did it work? Yes.

3. Now use traceroute to find the path to learn-2's external IP:

```
sudo traceroute <learn-2's external IP> -I
```

## ping to learn-3

You already know that learn-3 is in a different network from learn-1, so the internal IP for learn-3 will not be reachable.

1. Try to ping learn-3's external IP address:


```
ping <learn-3's external IP>
```

2. Press **Ctrl+C** to stop the command.


Why didn't this work? You were able to reach learn-2's external IP; why not learn-3's?

Recall that learn-2 is in an auto-mode network, so firewall rules were automatically created that enabled ingress traffic to reach its external IP. However, learn-3 is in a custom-mode network, and no firewall rules were established. You created a firewall rule to permit access.

Take another look at that firewall rule.

3. In the GCP Console, on the **Navigation menu** () , click **VPC network > Firewall rules**.

Notice that the default firewall rules were established to apply to all targets. You created the firewall rule with tighter security. It will only permit traffic to VMs that have the Target tag *allow-defaults*.

4. On the **Navigation menu** () , click **Compute Engine > VM instances**.
5. Click **learn-3** to access details about the VM.
6. Click **edit**.
7. For **Network tags**, type **allow-defaults**
8. Click **Save**.
9. Return to the SSH terminal for **learn-1** (or reconnect if needed).

10. Try again to ping learn-3's external IP address:

```
ping <learn-3's external IP>
```

The firewall rule and network tags can take time to take effect; if the last step didn't work, wait a few minutes and try again.

## Edit the firewall rule

You already know that learn-3 is in a different network from learn-1, so the internal IP for learn-3 will not be reachable.

1. Open an SSH terminal to **learn-3**.
2. Try the following:


```
ping learn-4
ping learn-5
sudo apt-get install traceroute
sudo traceroute learn-5 -I
```

Can you explain all the behaviors?

DNS translation works for both learn-4 and learn-5 because all of these VMs are in the same network as learn-3, the learncustom network. Pinging the IP addresses will work after the firewall rules have been added.

3. In the GCP Console, in the left pane, click **VM instances**.
4. Try to connect via SSH to learn-4.

The firewall rule for the learncustom network only delivers traffic to VMs with the target tag allow-defaults.

5. In the GCP Console, on the **Navigation menu** () , click **VPC network > Firewall rules**.
6. Click **allow-ssh-icmp-rdp-learncustom** to access the firewall rule details.
7. Click **Edit**.
8. For **Targets**, click **All instances in the network**.
9. Click **Save**.
10. Try the commands again:

```
ping learn-4
ping learn-5
sudo apt-get install traceroute
sudo traceroute learn-5 -I
```

Everything should work this time.

11. Verify that you can now connect via SSH to learn-4.

## Convert an auto-mode network to a custom-mode network

In this section, you convert an auto-mode network to a custom-mode network to gain more fine-grained control over the subnetworks.

A new policy for network learnauto will be implemented. There will no longer be assets in us-central1 region. New projects instead shift planned assets from us-central1 to a new subnetwork in us-east1 region named *new-useast*.

To implement the policy, you delete the learnauto us-central1 subnetwork and create the new subnetwork in us-east1 to allow for the work that was originally planned for the us-central1 region.

1. In the GCP Console, in the left pane, click **VPC networks**.
2. Click **learnauto** to view network details.

Notice that there is no option to select the subnets. You can only delete the entire network.

You can't delete the subnetwork because this network is an auto-mode network. You will have to convert it to a custom-mode network to gain the ability to delete the subnetwork.

3. Return to the **VPC networks** page.
4. For **learnauto**, in the **Mode** column, switch from **Auto** to **Custom**.
5. In the confirmation dialog, click **OK**.

## Delete the learnauto subnet and create a new subnet

1. Click **learnauto** to view network details.
2. Click **learnauto** for the **us-central1** subnet.
3. Click **Delete subnet**.
4. In the confirmation dialog, click **Delete**.

Reflecting the new tighter policies, the new subnetwork is CIDR /26. How many VMs can that support?  $2^6 = 64$  addresses, minus broadcast, subnet, and gateway = 61 VMs.

5. Return to the **VPC networks** page and click **learnauto** to return to the network details.
6. Click **Add subnet**.

7. Specify the following, and leave the remaining settings as their defaults:

Property	Value (type value or select option as specified)
Name	new-useast
Region	us-east1
IP address range	10.133.5.0/26


8. Click **Add**.

## Expand a subnet

The projects in the new-useast subnet have been a success; however, the original range of /26 was too restrictive. Expand the subnet to support at least 500 VMs.

1. In the left pane, click **VPC networks**.
2. Click **learnauto** to view network details.
3. On the **Google Cloud Platform** menu, click **Activate Google Cloud**



**Shell** (  ) to open Cloud Shell. If prompted, click **Start Cloud Shell**.



4. To increase the address range, run the following command:

```
gcloud compute networks subnets \  
expand-ip-range new-useast \  
--prefix-length 23 \  
--region us-east1
```

5. When prompted, type **Y** to continue.
6. There is no refresh button on the **VPC network details** page to see the result; in the left pane, click **VPC networks**.
7. Click **Refresh** until you see that the range has expanded.

## Delete resources that are no longer needed

If you end the lab now, the lab infrastructure will clean up and delete all the resources. However, in this section, you delete objects so that you can explore the dependent relationship in deleting. Objects must be deleted in a specific order. Before you can delete networks and subnets, you must delete all VMs and firewall rules.

1. On the **Navigation menu** () , click **Compute Engine > VM instances**.
2. Select all the VMs, and then click **Delete**.
3. In the confirmation dialog, click **Delete**.
4. On the **Navigation menu** () , click **VPC network> Firewall rules**.
5. Delete all firewall rules that are part of the **learnauto** and **learncustom** networks.
6. In the left pane, click **VPC networks**.
7. Click **learncustom** to view network details.
8. Click **Delete VPC network**.
9. In the confirmation dialog, click **Delete**.
10. Repeat steps 7–9 for the **learnauto** network.

Do **not** delete the Default network.

## Review the delete project procedure

You do not have the IAM role necessary to delete the project. The following steps illustrate what the activity would look like if you could perform it.

However, if you were to delete the project, the process would look like this:

1. In the Console, navigate to **Navigation menu > IAM & admin > Settings**.
2. Click **Delete Project**.
3. To shut down the project, you would need to type in the Project ID and click **Shut down**.

## Task 4: Review

In this lab you created networks and subnetworks of many different varieties, started VMs in each location, and then explored the network relationship between them.

## Cleanup

1. In the **Cloud Platform Console**, sign out of the Google account.
2. Close the browser tab.

Last Updated: 2018-09-24

## End your lab

When you have completed your lab, click **End Lab**. Qwiklabs removes the resources you've used and cleans the account for you.

You will be given an opportunity to rate the lab experience. Select the applicable number of stars, type a comment, and then click **Submit**.

The number of stars indicates the following:

- 1 star = Very dissatisfied
- 2 stars = Dissatisfied
- 3 stars = Neutral
- 4 stars = Satisfied
- 5 stars = Very satisfied

You can close the dialog box if you don't want to provide feedback.

For feedback, suggestions, or corrections, please use the **Support** tab.

©2018 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.