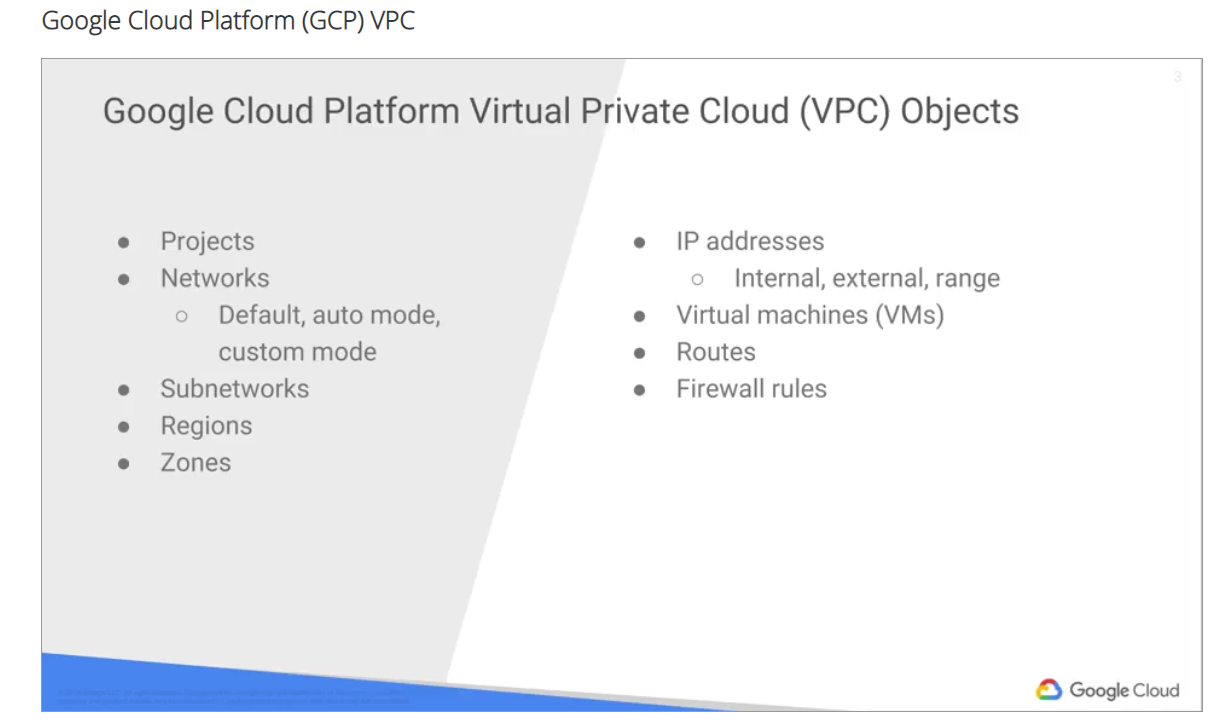
Module two: Virtual Networks.

GCP uses a software-defined network that is built on a global fiber infrastructure that makes GCP one of the largest and fastest networks. Thinking about resources as services rather than as hardware, will help you understand the options that are available and their behavior. For example, a persistent disk isn't really a physical device. It's a service that you acquire and use over a network. So, a good understanding of GCP begins with a solid understanding of how GCP has implemented networking.

In this module, we will start by introducing Virtual Private Cloud, or VPC, which is Google's managed networking functionality for your Cloud Platform resources. Then, we are going to dissect networking into its fundamental components which are **projects, networks, subnetworks, IP addresses, routes and rules along with billing**.

Next, you will explore GCP's network structure in a lab by creating networks and subnetworks of many different varieties and exploring the network relationships between them.

After that, we will look at common network designs like a bastion host isolation which you will get to implement in a lab.



With Google Cloud Platform VPC, you can provision your GCP resources, connect them to each other and isolate them from one another in a virtual private cloud. You can also define fine-grained networking policies within GCP, and between GCP and on premises or other public clouds.

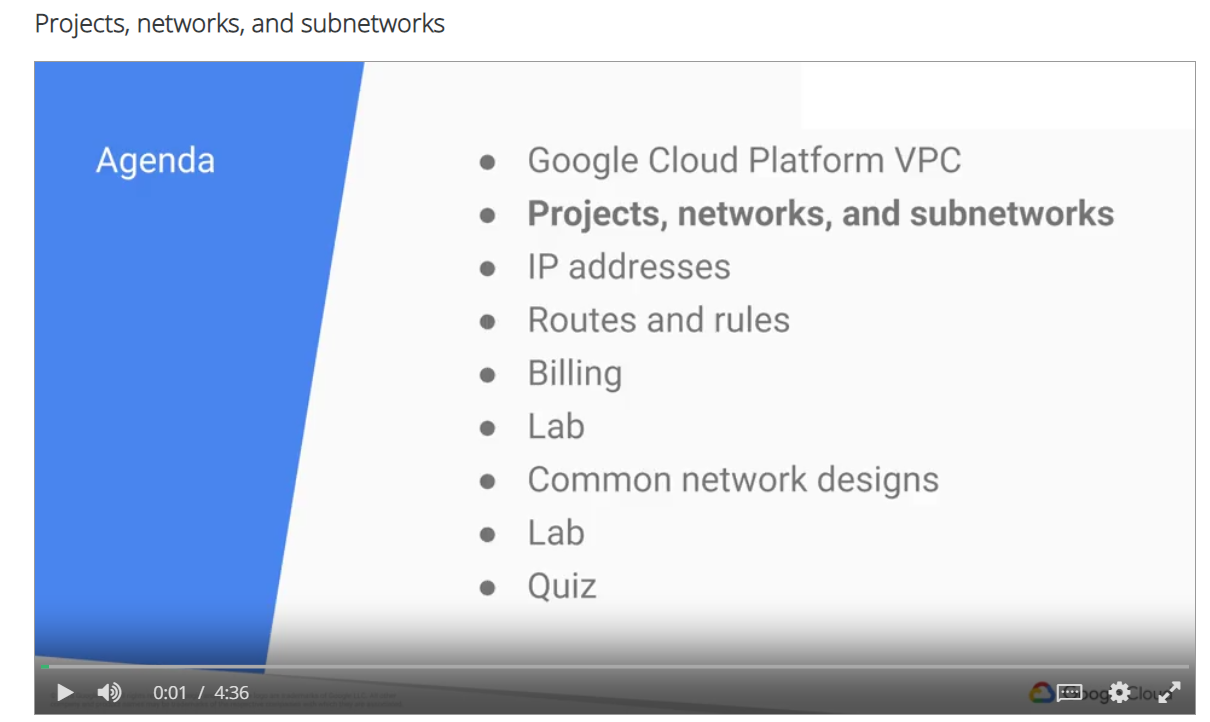
Essentially, VPC is a comprehensive set of Google-managed networking objects that we will explore in detail throughout this module.

* Projects are going to encompass every single service that you utilize.
* Networks come in three different flavors: default, auto mode and custom mode.
* Subnetworks allow you to divide or segregate your environment.
* Regions and zones represent Google's data centers and they provide continuous data protection and high availability.
* VPC provides IP addresses for internal and external use along with granular IP address range selections. As for virtual machines, in this module, we'll focus on configuring a VM from a networking perspective.

In the next module, we'll go deeper into how to setup and configure virtual machines.

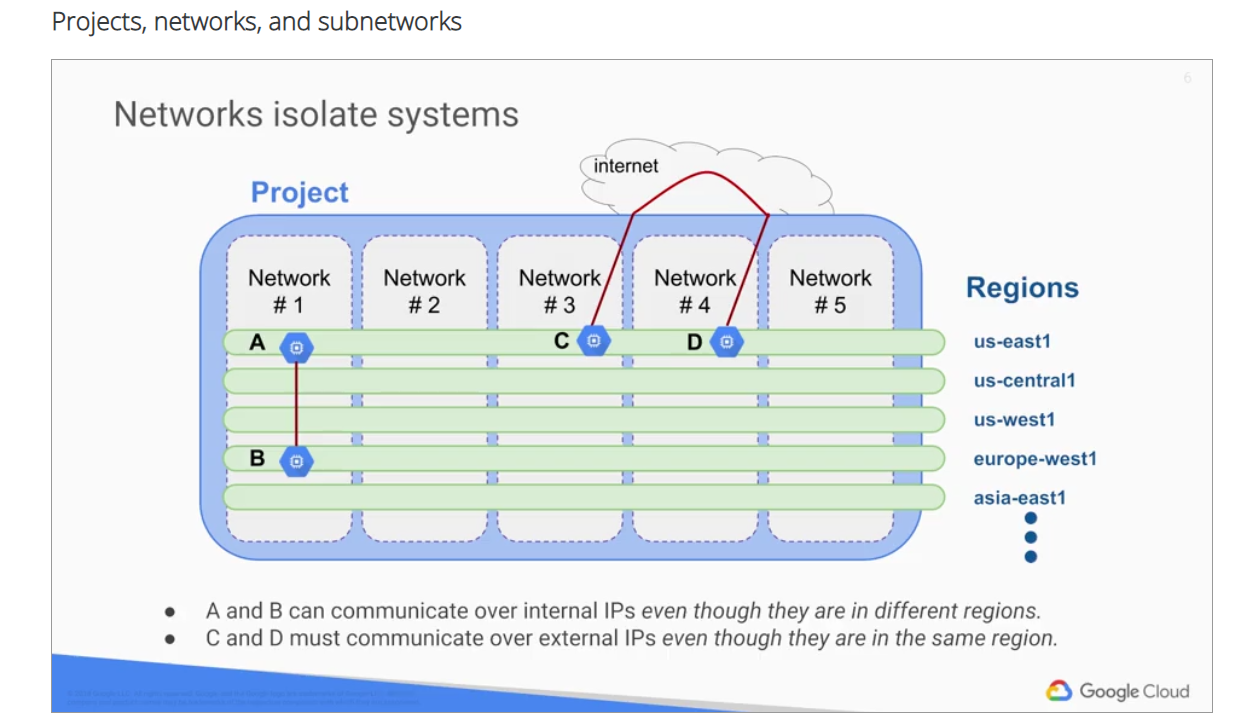
Finally, we'll conclude with routes and firewalls.

IP forwarding, protocol forwarding, load balancing, cloud DNS and VPN tunnels are built on top of these objects and are covered separately in a later course.

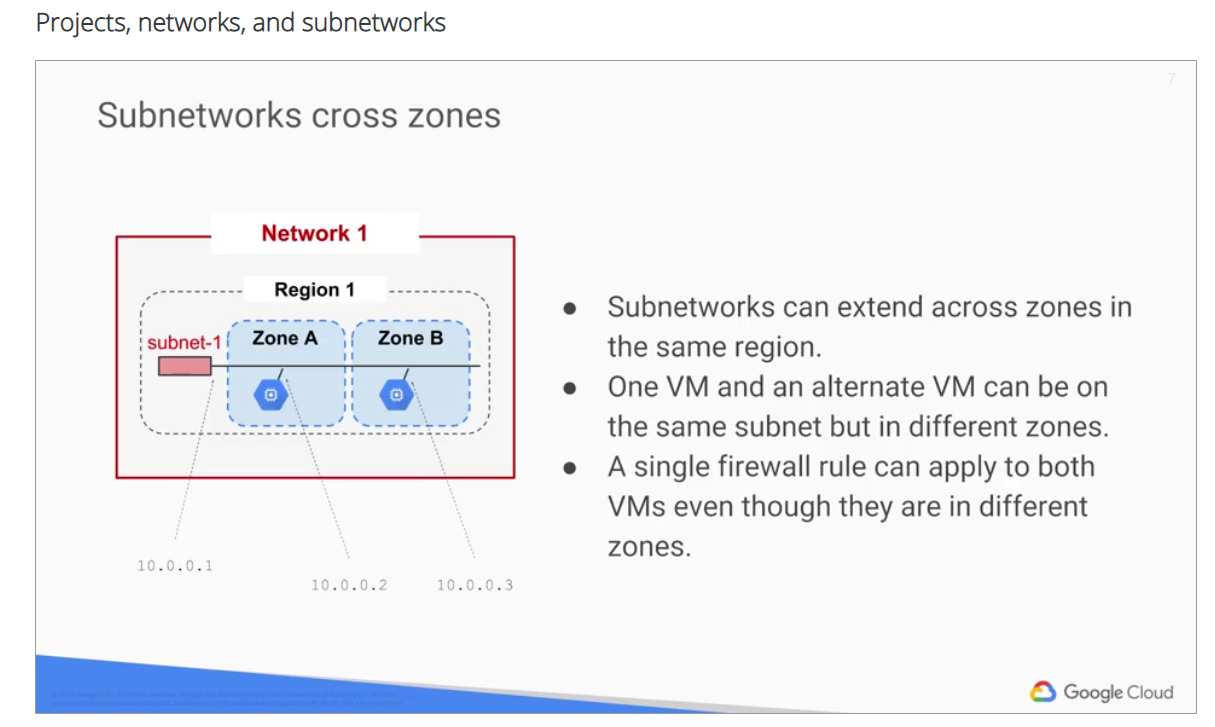


Let's start by looking at projects, networks, and subnetworks.

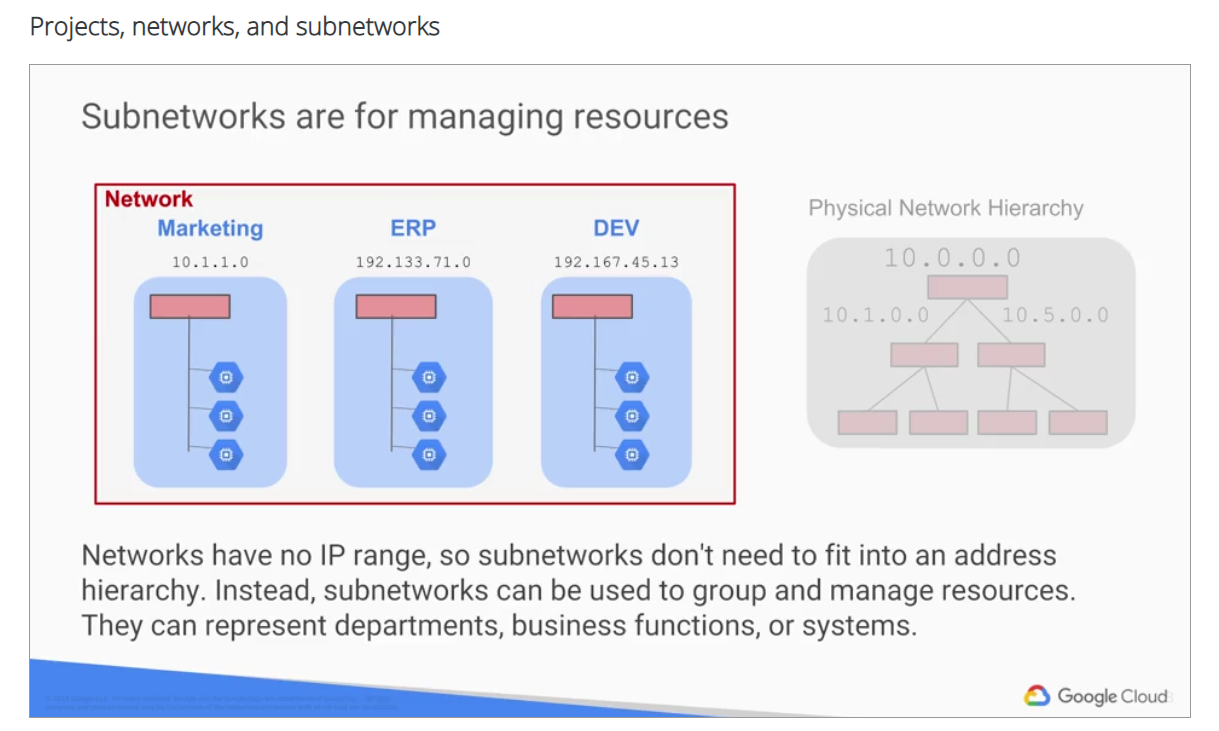
* projects as the key organizer of infrastructure resources.
  + a project associates objects and services with billing.
  + what's unique is the fact that projects actually contain entire networks, up to five networks per project to be exact.
  + A network :
    - Has no IP address ranges,
    - Is global, spanning all available regions across the world.
    - Contains subnetworks.
    - Can be of type **default**, **auto mode**, and **custom mode**. While an auto mode network can be converted to a custom mode network, a custom mode network cannot be converted to anything else. Essentially, once custom always custom.



Let's look an example of how networks can isolate systems in GCP. On this slide we have an example of a project that contains five networks. All of these networks span multiple regions across the world as you can see on the right hand side. Each network contains separate virtual machines. Since VMs A and B are on the same network, Network one, they can communicate over internal IP addresses, even though they're in different regions. Essentially, your virtual machines, even if they exist in different locations across the world, take advantage of Google's global fibre network. Those virtual machines are going to appear as though they're sitting in the same rack when it comes to a Network Configuration Protocol. VMs C and D on the other hand, are not in the same network. Therefore, these VMs must communicate over external IPs, even though they're in the same region. The traffic between VMs C and D isn't actually touching the Internet, but is going through the Google Edge routers which has different billing and security ramifications that we're going to explore.



To better understand the slide, let me define regions and zones. A region is a specific geographical location where you can run your resources. Each region has one or more zones. For example, the US Central One region denotes a region in the central United States that has zones US Central 1A, US Central 1B, US Central 1C, and US Central 1F. For an up-to-date list of GCP regions and zones, please refer to the online documentation, as new regions and zones are constantly added. This slide has a region, Region one, with two zones, Zone A, and Zone B. Subnetworks can extend across zones within the same region such as subnet-1. The subnet is simply an IP address range, so you can carve up IP addresses within that range. Notice that the first address in the range 10.0.0.1 is reserved for the router address. The last address in the range, 10.0.0.255, is reserved for the broadcast address. Even though the two virtual machines in this example are across different zones, they will still communicate with each other using the same subnet IP address. Essentially, a single firewall rule will apply to both VMs even though they are in different zones.



In an on-premises environment, you might design subnetworks in the traditional way that is based on the stacks of routers or switches within your environment. Essentially, a top-down hierarchy, as you can see on the right hand side, where you have a master network 10.0, and you've carved it up into your core switches and core routers specifically into 10.1 and 10.5. Each of these might represent different environments such as marketing, ERP, or development. In GCP, you just simply set up a network, and you create multiple subnets for marketing, ERP and development. As you can see, networks do not have IP ranges. So, subnetworks don't need to fit into an address hierarchy. While subnetworks can be used to manage resources, there are other ways of managing resources like Cloud IAM, labels, tags, and managed instance groups. These are covered throughout the different courses of this specialization.