General:

* Another benefit of cloud computing: easier to build infrastructure that’s close to your end user.
* When ping fails, look for security (firewall) issues first.

VPC:

* Subnets are not just public/private, they can serve more specific purposes. You can have a private subnet only for RDS and a public subnet for all EC2 servers, etc.
* Security Group vs NACL, Security can be applied on resource level, NACLs operate on subnet level.
* A common use case of VPC peering is to build inter-network between organizations
* Typically, when you want to integrate your on-premise infrastructure, you want to use a custom VPC.
* Subnets don’t span AZs, but one AZ can have multiple subnets.
* Route table is the one used to make subnets talk to each other. It basically defines: “for any traffic that’s trying to reach the following IP, dump it to target”, e.g. “for 0.0.0.0/0, dump it to IGW”.
* VPC launch wizard allows you to create VPCs based on some standard configurations, and then customise later
* An alternative to IGW is attaching a Virtual Private Gateway (VPG) and a Customer Gateway (CG) (defined in AWS so AWS is aware of it, but ultimately is still connected to a VPG through internet and hardware-based VPN)
* You’re allowed to have an EC2 on a dedicated hardware, within a VPC on a shared tenancy.
* Elastic IP is a randomly generated IPv4 address, and all you must do is to associate it with an EC2 or its primary Network Interface (what is this??). Essentially it is associated with a private IP address, and it is charged until you release that address
* VPC peering is very simple, just start from one VPC and request peering with another VPC. However, there’s no overlapping IP addresses allowed between peering VPCs (You may want to look into how to change configuration if the two VPC were set to use the same IP range).
* Layered security: Resource -> VM FW -> Security Group (customer FW but not VM level) -> NACLs (one per subnet)
* Security Group has limits, up to 100 per VPC, up to 50 lines each, up to 5 attached to each instance.
* By default, instances in the same security group can talk to each other (default rule has the security group itself as source for all traffic)
* Security group only allows target port filtering (e.g. open port 22 to IP range XXX.XXX.XXX.XXX/XX), source filtering only applies at IP level, not port level.
* By default, Security Group deny all inbound until allow, and allow all outbound until allow.
* Two types of VPN: Remote access (everyday VPN), Site to Site connection (e.g. connect corporate datacentre and Branch office, but still go through internet). As long as it goes through internet, it’s not a private connection, it’s a VPN.
* Direct Connect is normally not direct, it’s done through a co-location owned by an AWS partner, the connection from your cold location to the co-location maybe through internet dedicated line or VPN