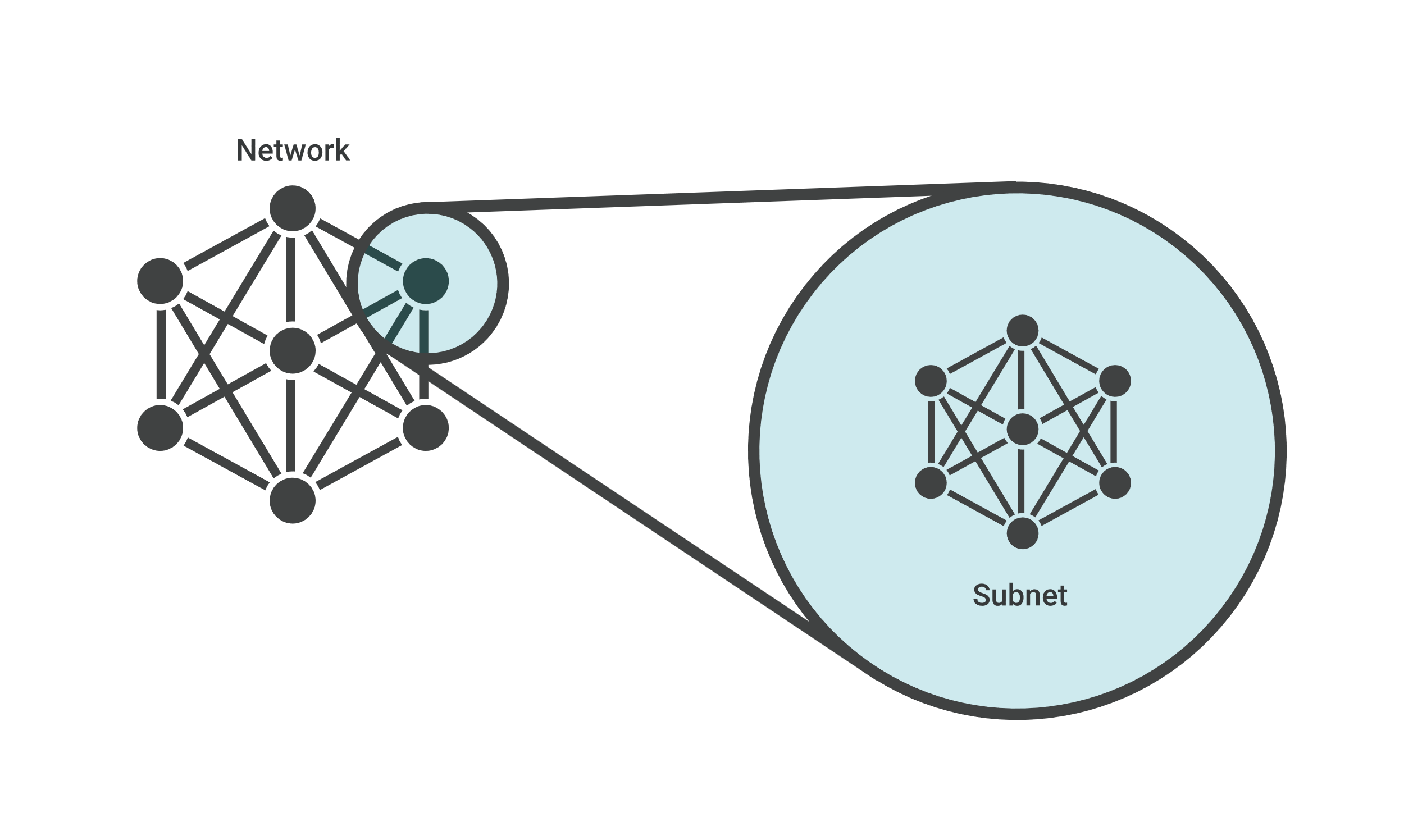
**subnet**

A subnet, or subnetwork, is a [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) to reach its destination.



Imagine Alice puts a letter in the mail that is addressed to Bob, who lives in the town right next to hers. For the letter to reach Bob as quickly as possible, it should be delivered right from Alice's post office to the post office in Bob's town, and then to Bob. If the letter is first sent to a post office hundreds of miles away, Alice's letter could take a lot longer to reach Bob.

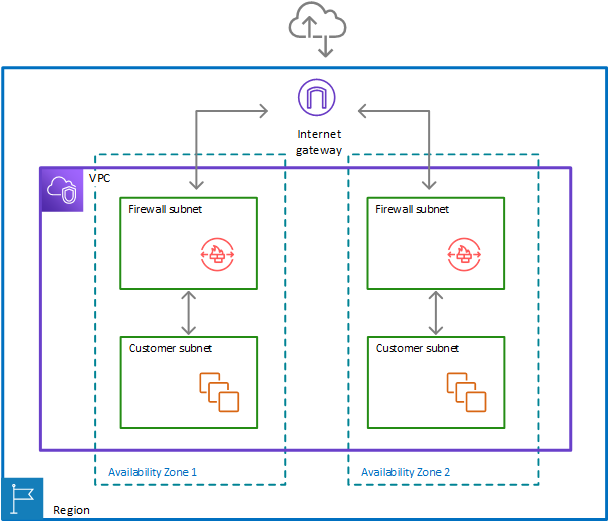
Like the postal service, networks are more efficient when messages travel as directly as possible. When a network receives data packets from another network, it will sort and route those packets by subnet so that the packets do not take an inefficient route to their destination.

**Public subnet vs Private subnet**

Public subnet – The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet. Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the public internet

**Internet Gateway**

An Internet Gateway (IGW) is an AWS component that provides a path for network traffic to travel between a Virtual Private Cloud (VPC) and the public internet. It acts as a bridge between the two networks, enabling inbound and outbound connections from resources within the VPC



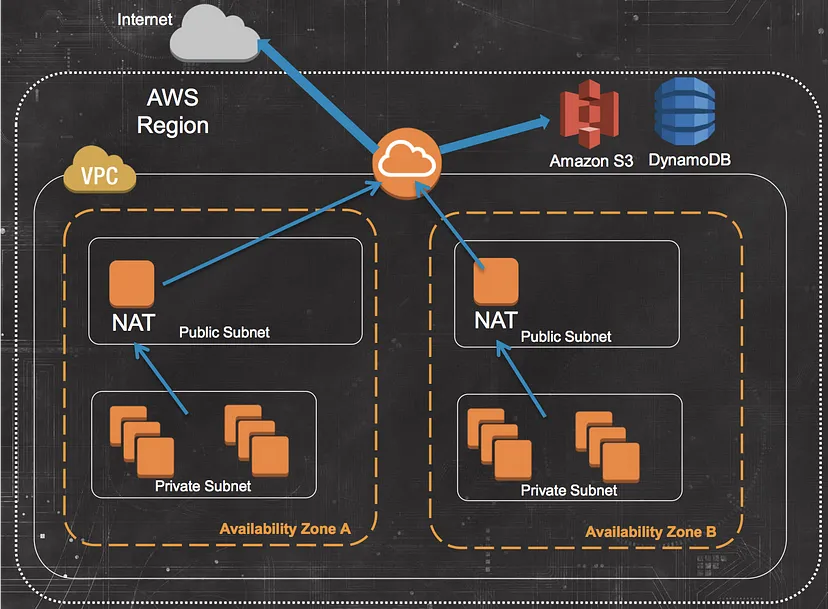
**Nat Gateway**

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

When you create a NAT gateway, you specify one of the following connectivity types:

* **Public** – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.
* **Private** – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

Both private and public NAT gateways map the source private IPv4 address of the instances to the private IPv4 address of the NAT gateway, but in the case of a public NAT gateway, the internet gateway then maps the private IPv4 address of the public NAT Gateway to the Elastic IP address associated with the NAT Gateway. When sending response traffic to the instances, whether it's a public or private NAT gateway, the NAT gateway translates the address back to the original source IP address



**Internet Gateway vs NAT Gateway**

Internet GW allows both inbound and outbound access to the internet whereas the NAT Gateway only allows outbound access. Thus, IgW allows instances with public IPs to access the internet whereas NAT Gateway allows instances with private IPs to access internet.

**Routing Tables**

A *route table* contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

**Route table concepts**

The following are the key concepts for route tables.

* **Main route table**—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
* **Custom route table**—A route table that you create for your VPC.
* **Destination**—The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with the CIDR 172.16.0.0/12.
* **Target**—The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.
* **Route table association**—The association between a route table and a subnet, internet gateway, or virtual private gateway.
* **Subnet route table**—A route table that's associated with a subnet.
* **Local route**—A default route for communication within the VPC.
* **Propagation**—If you've attached a virtual private gateway to your VPC and enable route propagation, we automatically add routes for your VPN connection to your subnet route tables. This means that you don't need to manually add or remove VPN routes. For more information, see [Site-to-Site VPN routing options](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html) in the *Site-to-Site VPN User Guide*.
* **Gateway route table**—A route table that's associated with an internet gateway or virtual private gateway.
* **Edge association**—A route table that you use to route inbound VPC traffic to an appliance. You associate a route table with the internet gateway or virtual private gateway, and specify the network interface of your appliance as the target for VPC traffic.
* **Transit gateway route table**—A route table that's associated with a transit gateway. For more information, see [Transit gateway route tables](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-route-tables.html) in *Amazon VPC Transit Gateways*.
* **Local gateway route table**—A route table that's associated with an Outposts local gateway. For more information, see [Local gateways](https://docs.aws.amazon.com/outposts/latest/userguide/outposts-local-gateways.html) in the *AWS Outposts User Guide*.

