**Subnet:**

When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting. So, maintenance is easier for smaller networks.

**Uses of Subnetting:**

1. Subnetting helps in organizing the network in an efficient way which helps in expanding the technology for large firms and companies.
2. Subnetting is used for specific staffing structures to reduce traffic and maintain order and efficiency.
3. Subnetting divides domains of the broadcast so that traffic is routed efficiently, which helps in improving network performance.
4. Subnetting is used in increasing [network security](https://www.geeksforgeeks.org/network-security/).

**Advantages of Subnetting**

The advantages of Subnetting are mentioned below:

It provides security to one network from another network. eg) In an Organisation, the code of the Developer department must not be accessed by another department.

It may be possible that a particular subnet might need higher network priority than others. For example, a Sales department needs to host webcasts or video conferences.

In the case of Small networks, maintenance is easy.

**Disadvantages of Subnetting**

The disadvantages of Subnetting are mentioned below:

1. In the case of a single network, only three steps are required to reach a Process i.e Source Host to Destination Network, Destination Network to Destination Host, and then Destination Host to Process.
2. In the case of a Single Network only two IP addresses are wasted to represent Network Id and Broadcast address but in the case of Subnetting two IP addresses are wasted for each Subnet.
3. The cost of the overall Network also increases. Subnetting requires internal routers, Switches, Hubs, Bridges, etc. which are very costly.
4. This platform doesn’t allow me to study efficiently.

### Subnet types

The subnet type is determined by how you configure routing for your subnets. For example:

* **Public subnet** – The subnet has a direct route to an [internet gateway](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html). 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](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat.html) to access the public internet.

# Network ACL:

A network access control list (NACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC. For more information about the differences between security groups and network ACLs.

# What is a Route Table in AWS:

In the AWS ecosystem, a route table is a set of rules, known as routes, that determines where network traffic is directed. Each subnet in your AWS Virtual Private Cloud (VPC) is associated with a route table that controls the traffic flow between subnets. A route table includes details like the Route Table ID and ‘The ID’ of its associated VPC.

## *What does a Route Table do?*

The role of an AWS route table is to direct network traffic based on the destination IP address. Each route in the table specifies a destination (in the form of an IP address or CIDR block) and a target (like an internet gateway (IGW), network interface, or another route table). A local route is a special type of route that enables communication within the VPC.

For example, if you have a subnet with an associated route table that has a route pointing to an internet gateway (IGW), the traffic from that subnet to the internet is allowed. Similarly, traffic from a subnet with a route pointing to a transit gateway is directed to the appropriate network.

## *AWS Route Tables and Security Groups: The Difference*

While both route tables and security groups play essential roles in network traffic management, they serve distinct functions. Security groups, managed through IAM, act as firewalls for EC2 instances, whereas route tables control the routing of network traffic.

It’s critical to understand the difference between route table and Network Access Control Lists (NACL) in AWS, too. While a route table defines rules for routing network traffic, a NACL is a subnet-level firewall controlling traffic in and out of subnets.

## What is a router:

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between [LANs (local area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) and [WANs (wide area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches\*.

**Internet gateways**

Internet gateways provide two-way public connectivity to applications running in AWS Regions and/or in Local Zones.  
In the following diagram, end users access a public-facing application in Local Zone 1. Traffic goes directly to the internet gateway in Local Zone 1 without going through the parent AWS Region. Use this type of connectivity for low-latency use-cases where you want your public-facing applications to be closer to end users than an AWS Region can provide.

