Module 5 : Networking & Content Delivery

Topics

- Networking basics
- Amazon VPC
- VPC networking
- VPC Security
- Amazon Route 53
- Amazon Cloudfront

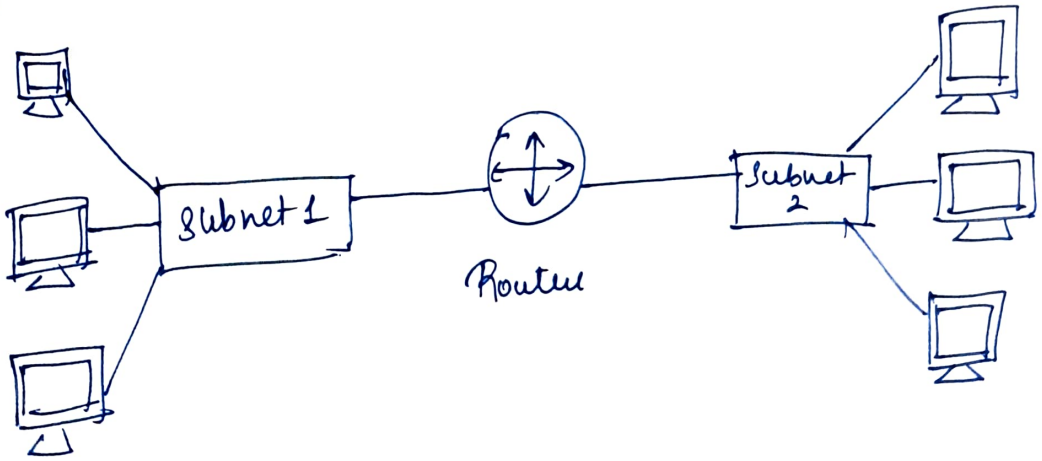
(Amazon VPC, VPC networking, VPC Security) → for Networking

(Amazon Route 53, Amazon Cloudfront) → for content delivery & distribution

---

(I) Networking Basics

- A computer is two or machines that are connected together, in order to communicate.
- A network can be logically partitioned into Subnets.
- Networking requires a networking device such as a router or a switch. this connects all the machines together & enables communication b/w them.



→ IP addresses

- Each machine in a network has a unique Internet Protocol assigned to it.

- IP address: it is a unique number assigned to a machine, in order to identify it uniquely.
  (similar to a phone number — unique)

- IP number is expressed as 4 decimal numbers, seperated by dots. Machines convert that decimal number to binary number format in order to use it.

Ex

192 . 0 . 2 . 0

↓ ↓ ↓ ↓

11000000 00000000 00000010 00000000

Here each of the 4 seperated numbers of address represent a maximum of 8 bits, i.e., they can be anything in range (0 – 255)

Combined total of 4 numbers of IP address is 32 bits, (in binary format)

- A 32-bit IP address is called an IPv4 address.
- IPv6 address also exists & use 128 bits. Thus they can accomodate more user devices & were invented to compensate for IPV4 address's short supply.

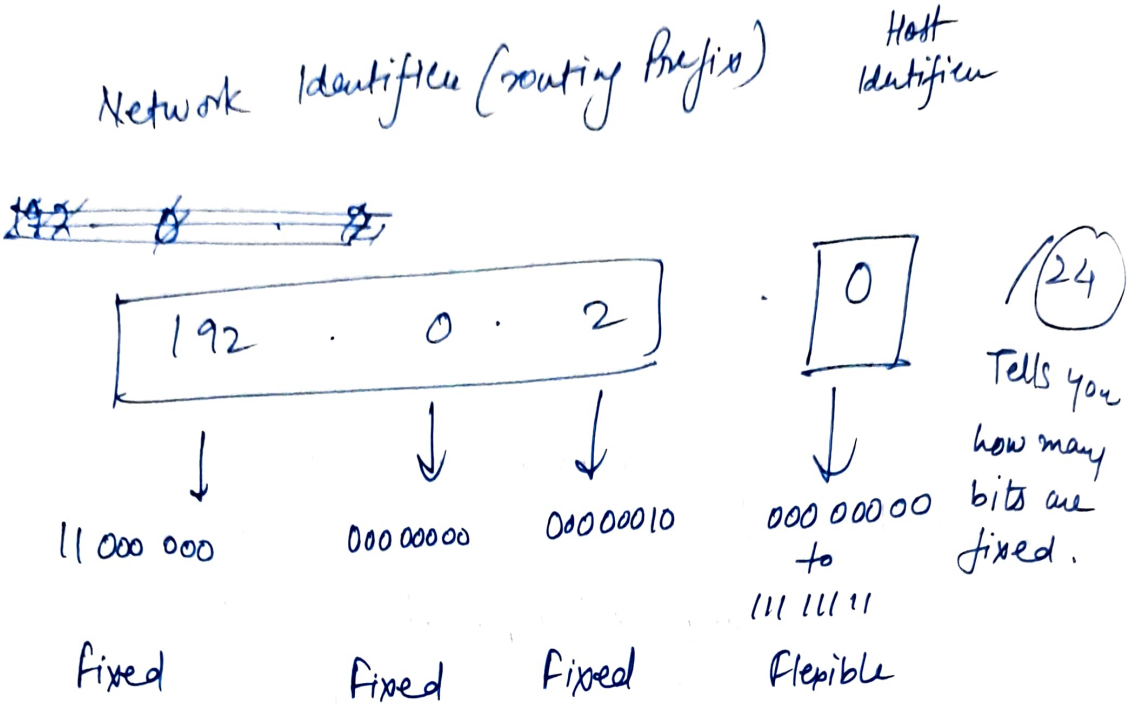
↳ IPv6 address compose of-

2600 : 1f18 : 22ba : 8c00 : ba86 : a05e : a5ba : 00ff

8 groups of 4 letters/numbers each, seperated by colons (:)

↳ Each seperated group represent 16 bits. ∴ each group can be from 0 to ffff.

→ Classless Inter-Domain Routing (CIDR)



- CIDR is a common method to describe networks & groups of IP addresses.
- A CIDR address is expressed as an IP address which is the first address of the network. It's followed by a '/' character.
- The '/' character tells us that how many bits of the routing prefix must be steady & allocated for the network identifier. The bits that aren't fixed are allowed to change.
- CIDR is used to describe IP addresses consecutive to each other.

Ex: here, CIDR address is 192.0.2.0/24
the last no. 24 tells us that first 24 bits must be fixed. & last 8 bits are flexible ∴ 256 IP addresses are available

i.e. 192.0.2.0 to 192.0.2.255

→ OSI Model

Def: The OSI model is a conceptual model that is used to explain data as it travels over a network.

- It has 7 layers & shows common protocols & addresses that are used to send data at each layer.

Eg Hubs & Switches — work at layer 2 i.e. data link layer.

Routers — Layer 3 i.e. network layer.

Layer	No.	Function	Protocol / Address
Application	7	Means for an app^n to access computer network	HTTP(S), FTP, DHCP, LDAP
Presentation	6	- Ensures that the App^n layer can read the data - Encryption	ASCII, ICA
Session	5	Enables orderly exchange of data	NetBIOS, RPC
Transport	4	Provides protocols to support host-to-host comm^n.	TCP, UDP
Network	3	Routing & Packet forwarding (Routers)	IP
Data Link	2	Transfer Data in the same LAN network (hubs & switches)	MAC
Physical	1	Transmission & reception of raw bitstreams over a physical medium	Signals (1s & 0s)

(II) Amazon VPC

Def: Amazon Virtual Private Cloud (VPC) is a service that lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network you define.

→ It gives you control over your virtual networking resources including:-

- Selection of IP address range (can use both IPv4 & IPv6 in VPC for secure access to apps & resources)
- Creation of subnets
- Configuration of route tables & network gateways.

→ Enables you to customize the network configuration for your VPC. (Ex) Subdivide VPC into subnets & create a public subnet for your web servers that can access the public internet).

→ Enables you to use multiple layers of security (like security groups & Network ACLs)

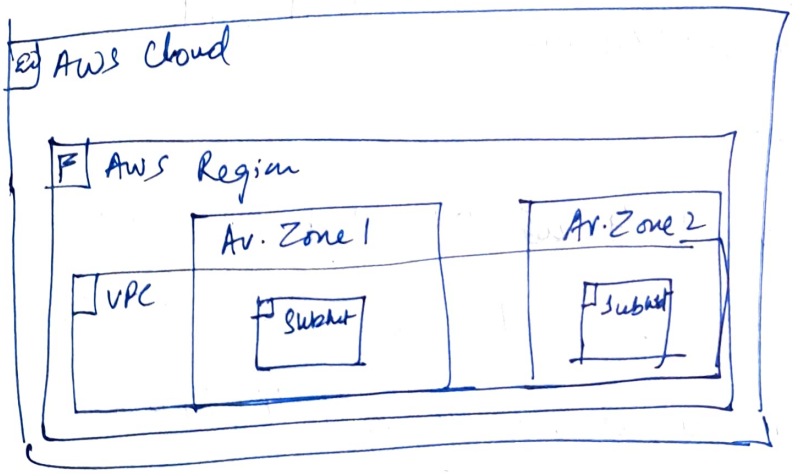
→ VPC & Subnets

VPC:

- Logically isolated from other VPCs.
- Dedicated to your AWS account
- Belong to a single AWS region & can span multiple Av. Zones.
-

Subnets:

- Range of IP addresses that divide a VPC.
- Belong to a sing AV. Zone
- classified as Public / Private



→ IP addressing

- ~~addr~~
- When you create a VPC, you assign it to an IPv4 CIDR block (Range of private IPv4 addresses)
- You cannot change the address range after you create the VPC.

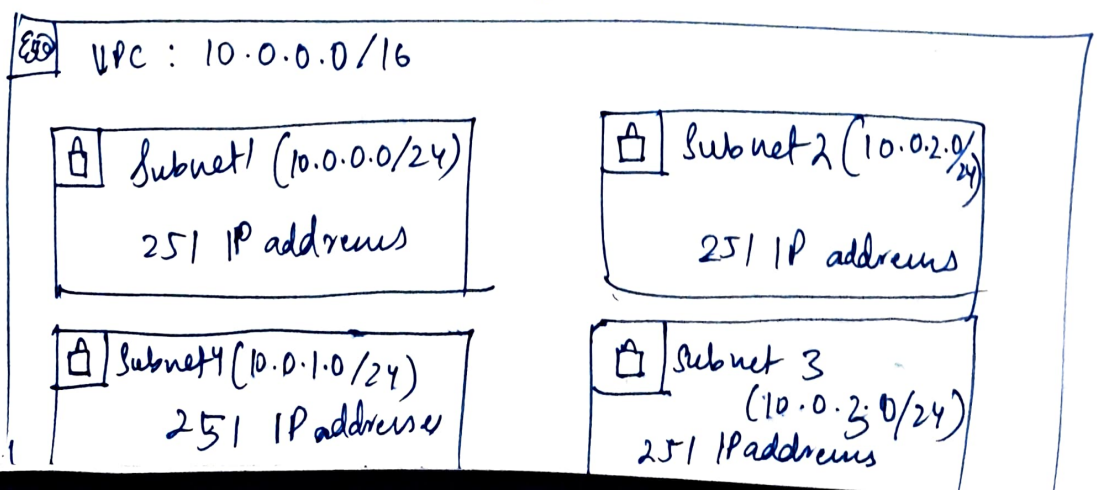
- The largest IPv4 CIDR block size is /16.
- The smallest IPv4 CIDR block size is /28.
- IPv6 is also supported (with a different block size limit)
- CIDR blocks of subnet cannot overlap

> x.x.x.x/16 or 65,536 addresses (map) to x.x.x.x/28 or 16 addresses (min)

→ Reserved IP Addresses

- for each CIDR block that you specify, AWS reserves 5 IP addresses within that block & we can't use them.

Ex: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total of IP addresses. the VPC has 4 equal-sized subnets. Only 251 IP address are available for use by each subnets.



IP addresses for CIDR block 10.0.0.0/24	Reserved for
10.0.0.0	Network Address
10.0.0.1	Internal Communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future Use
10.0.0.255	Network broadcast address

Public IP address types

→ When you create a VPC, every VM in that VPC gets a private IP address automatically.

→ We can also request a Public IP address to be assigned to a VM when creating the instance by modifying VPC's autoassign Public IP address properties.

→ Elastic IP address : Its a static public IPv4 address. You can associate an elastic IP address with any instance or network interface for any VPC in your account.

(Benefit of Using elas. IP with network interface : One instance → move all the IP addresses from one Network to another in case of failure.

with elastic IP address you can mask the failure of an instance by rapidly remapping the address to another instance in your VPC.

Public IPv4 address	Elastic IPv4 address
• Manually assigned through an elastic IP address • Automatically assigned through the auto-assign public IP address settings at subnet level.	• Associated with an AWS account • Can be allocated & remapped anytime • Additional costs might apply.

→ Elastic Network Interface

- A virtual network interface that you can:
  - Attach to an instance
  - Detach from the instance & attach to another instance to redirect network traffic
- Its attributes follow when it is reattached to a new instance.
- Each instance in your VPC has a default network interface (also called primary network interface.) that is assigned a private IPv4 address from the IPv4 address range of your VPC.

→ Route Tables & Routes

- A route table contains a set of rules (called routes) that you can configure to direct network traffic to/from your subnet.
- Each route specifies a destination & a target.
- By default, every route table contains a local route for communication within VPC.
- Each subnet must be associated with a route table (atmost one)

↳ main (Default) Route table

Destination	Target
10.0.0.0/16	local

→ VPC CIDR Block.

(III) VPC networking

→ Internet Gateway

↳ Def: It is a scalable redundant & highly available VPC component that allows Communication b/w instances in your VPC & the public internet.

↳ It serve 2 purposes:

1.) to provide a target in your VPC route tables for internet traffic

2.) to perform network address translation for instances that were assigned public IPv4 addresses.

↳ To make a subnet public attach an internet gateway to your VPC & add a route entry to the route table associated with the subnet.

→ Network Address Translation (NAT) gateway

↳ It enables instances in a private subnet to connect to internet & other AWS services, but it prevents the internet gateway from initiating a connec^{n} with those instances.

↳ To create a NAT Gateway :-

- You must specify the public subnet in which NAT Gateway should live.
- You must also specify an elastic IP address to associate with the NAT gateway when you create it

↳ After creating the NAT Gateway, update the route table that is associated with one or more of your private subnets to point internet-bound traffic to NAT Gateway.

[Hence, private subnet instances will be able to communicate with the internet.]

(Can also use NAT instance directly but not recommended)

→ VPC Sharing (b/w 2 subnets)

↳ Enables customers to share subnets with other AWS accounts in the same organization.

→ VPC Peering (b/w 2 VPCs)

↳ A VPC peering connection enables you to privately route traffic between 2 VPCs.

↳ Can connect VPCs in your own AWS Account, b/w AWS accounts, or b/w AWS regions.

↳ Restrictions:

- IP spaces cannot overlap
- Transitive peering not supported
- You can only have one peering resource b/w the same two VPCs.

Route Table for VPC A

Destination	Target
10.0.0.0/16	local
10.30.0.0/16	pcx-id

Route Table for VPC B

Destination	Target
10.30.0.0/16	local
10.0.0.0/16	pcx-id

AWS Site-to-Site VPN

↳ By default VPC created cannot directly connect to your remote network.

↳ You must attach a virtual private Gateway to VPC, creating a customer table, updating security group rules, creating AWS site to site VPN connection & configuring routes to pass through the VPN connection. traffic through

---

AWS Direct Connect

when the data center is located far away from AWS region, we can use AWS Direct Connect to not hamper the network performance.

Def: AWS Direct Connect enables you to establish a dedicated private connection b/w your network & one of the direct-connect locations. This connection (private) can increase bandwidth, throughput, & provide a more consistent network experience than internet-based conn's or VPN

↳ Uses Open Standard 802.1q virtual LAN.

→ VPC Endpoints

When you need to connect VPC resources to Aws regional services like Amazon S3 & Dynamo DB Then we use VPC Endpoint

Def : A virtual device that helps privately connect your VPC to the supported Aws services

VPC Endpoints

Gateway
(Amazon S3 & Dynamo DB)

Specify as a target in your route table for traffic destined to S3 or Dynamo DB.

Interface
(Powered by AWS PrivateLink)

→ Aws Transit Gateway

to connect 100s of VPCs together, Aws Transit Gateway can be used instead.

→ VPC Security

VPC firewall options → Security Groups
→ Network ACLs.

1.) Security Groups

- It acts as virtual firewall that controlls inbound & outbound traffic to & from your instance.
- Acts at Instance level & can assign each instance in VPC to diff set of Sec. Groups.
- Have rules to manage instance traffic
- Default Security groups are sealed shut to inbound traffic. We need to define rules.
- Security groups are stateful. The outbound traffic is always allowed

2.) Network ACLs

- It works at subnet level & control traffic In & out of subnet.
- Each subnet in your VPC must be associated with a Network ACL.

- A network ACL has separate inbound & outbound rules, & each rule can either allow or deny traffic.
- Default network ACLs allow all inbound & outbound IPv4 traffic.
- Network ACLs are Stateless
  ↳ i.e. no info about a request is maintained after the request is process

→ Sec. Group v/s Network ACLs

Attribute	Security Groups	Network ACLs
Scope	Instance level	Subnet level
Supported Rules	Allow rules only	Allow & deny rules
State	Stateful (return traffic is automatically allowed regardless of rules)	Stateless (return traffic must explicitly be allowed by rules
Order of Rules	All rules are evaluated before decision to allow traffic	Rules are evaluated in no. order before to allow traffic.

(V) Route 53

→ Domain Name System

→ DNS Resolution

It is the process of translating an internal name to the corresponding IP address.

↳ Acts like a phonebook where names are replaced with IP addresses

→ Amazon Route 53

- Its a highly available & scalable DNS web service
- Used to route end users to Internet App^h's by translating names like (www.example.com) to numeric IP addresses (like 192.0.2.1) that computers use to connect to each other.
- fully compliant with IPv4 & IPv6.
- Connects user requests to infrastructure running in AWS & also outside AWS.
- Used to check health of your resources.
- Features traffic flow.
- Enables you to register domain names

Route 53

→ Supported Routing :-

1.) Simple Routing – Use in single server environments

2.) Weighted Routing – Assign weights to resource record sets to specify the freq.

3.) Latency Routing – Help improve your global Applications

4.) Geolocation Routing – Routing traffic based on location of your users.

5.) GeoProximity Routing – Route traffic based on location of your resources

6.) Failover Routing – Fail over to a backup site if your primary site becomes unreachable.

7.) multivalue answer Routing – Respond to DNS queries with upto 8 healthy records selected at random.

→ Amazon Cloudfront

→ when ~~requesting~~ on a browsing a website, your request is routed through different networks. The origin server stores the original version of data that's in high density. The distance in customer & server significantly affects network performance.

∴ we need a content delivery network.

Amazon Cloudfront is a fast content Delivery service (CDN) that securely delivers data to customers at high transfer speeds. ~~It also provides~~

- Global network of edge locations & regional caches.
- Self service model
- Pay-as-you-go Pricing

Edge locations

Network of data centers that cloudfront uses to serve popular content quickly to customers.

Regional edge caches

Cloudfront location that caches content ~~that's~~ not popular enough to stay at edge locations.