# Module 5: Networking and Content Delivery

Thursday, September 11, 2025 7:35 AM

## *A. Learning Outcomes (LOs):*

- Recognize the basics of networking
- Describe virtual networking in the cloud with Amazon VPC
- Label a network diagram
- Design a basic VPC architecture.
- Indicate the steps to build a VPC
- Identify security groups
- Create your own VPC and add additional components to it to produce a customized network.
- Identify the fundamentals of Amazon Route S3
- Recognize the benefits of Amazon CloudFront.

## *B. Networking Basics*

- Networking requires a networking device such as a router or a switch.
- IP addresses (decimal to binary):
  + IPv4 (32-bit address): 192.0.2.0
  + IPv6 (128-bit address): 2600:1f18:22ba:8c00:a05e:a5ba:00FF
- Careless Inter-Domain Routing (CIDR): 192.0.2.0
  + 192.0.2 is fixed
  + 0 is Flexible
  + /24 tells how many bits are fixed

| *Layer* | *Number* | *Function* | *Protocol/Address* |
|---|---|---|---|
| Application | 7 | Means for an application to access a computer network | HTTP(S), FTP, DHCP, LADP |
| Presentation | 6 | - Ensure that the application layer can read the data<br>- Encryption | ASCI, ICA |
| Session | 5 | Enables orderly exchange of data | NetBIOS, RPC |
| Transport | 4 | Provides protocols to support host-to-host communication | TCP, UDP |
| Network | 3 | Routing and packet forwarding (routers) | IP |
| Data link | 2 | Transfer data in the same LAN network (hubs and switches) | MAC |
| Physical | 1 | Transmission and reception of raw bitstreams over a physical medium | Signals (1s and 0s) |

## *C. Amazon VPC*

- Enables you to provision a ***logically isolated*** section of the AWS Cloud where you can launch the AWS resources in a virtual network that you define
- Gives you **control over yout virtual networking resources including**:
  **+ Selection of IP address range**
  **+ Creation of subnets**
  **+ Configuration of route tables and network gateways**
- Enables to customize the network configuration for your VPC
- Enables yo use multiple layers of security
- VPCs:
  + **Logically isolated** from other VPCs
  + **Dedicated** to user AWS ccount
  + Belong to a single **AWS Region** and can span multiple Availability Zones
- Subnets:
  + **Range of IP addresse**s that divide a VPC
  + Belong to a single **Availability Zone**
  **+** Classified as **public** or **private**
- IP addressing:

+ When creating a VPC, assigning it to an **IPv4 CIDR block (range of private IPv4 addresses)**
+ **Cannot change the address range** after creating the VPC
+ The **larges**t IPv4 CIDR size is **/16**
+ The **smallest** IPv4 CIDR block size is **/28**
+ IPb6 is also supported (with a different block size limit)
+ CIDR blocks of subnets **cannot overlap**

- Reserved IP addresses:

Scenario: A VPC wit an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.

| ***IP addresses for CIDE Block 10.0.0.0/24*** | ***Rserved 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 |
| 10.0.0.4 | Network broadcast address |

- Public IP address types:
  + **Public IPv4 address:**
    * Manually assigned through an Elastic IP address
    * Automatically assigned through the auto-assign public IP address settings at the subnet level
  + **Elastic IP address:**
    * Associated with an AWS account
    * Can be allocated and remapped anytime
    * Additonal costs might apply
- Elastic network interface:
  + An elastic network interface is a virtual network interface that can attract to an instance and detach from the instance, and attach to another instance to redirect network traffic.
  + It's attributes follow when it is reattached to a new instance
  + Each instance in your VPC has a default network interface that is assigned a private IPv4 address form the IPv4 address range of user VPC.
- Route tables and routes:
  + A route table contains a set of rules (or routes) that you can configure to direct network traffic from the subnet.
  + Each route specifies a destination and a target.
  + By default, every route table contains a local route for communication within the VPC
  + Each subnet must be associated wirh a route table (at most one).

## *D. VPC Networking*

***- Internet gateways serves two purposes:***
  + Provide a target in the VPC route tables for internet traffic
  + Perform network address translation for instances that were assigned public IPv4 addresses
- VPC peering: User can connect VPCs in own AWS account, between AWS accouns, or between AWS Regions
- Restrictions:
  + IP spaces cannot overlap
  + Transitive peering is not supported
  + Can only have one peering resources between the same two VPCs
- Two types of endpoints:
  + **Gateway** endpoints (Amazon S3 and Amazon Dynamo DB)
  + **Interface** endpoints (powered by AWS PrivateLink)

***E. VPC Security:*** There are two VPC firewalls including security groips and network access control lists (network ACLs)

- Security groups:
  + Security groups have ruiles to manage instance traffic.
  + Default security groups are sealed shut to inbound traffic. We need to define rules.
  + Security froups are stateful. The outbound traffic is always allowed.

- Network accessm control lists (Netwrok ACLs):
  + A network ACL has separate inbound and outbound rules, and eahc rule can either allow or deny traffic.
  + Default network ACLs allow all inbound and outbound IPv4 traffic.
  + Network ACLs are stateless
- Security groups versus Network ACLs:

| ***Attribute*** | ***Security groups*** | ***Network ACLs*** |
|---|---|---|
| Scope | Instance level | Subnet level |
| Supported Rules | Allow rules only | Allow and deny rules |
| Scale | Stateful (return traffic is automatically allowed, regardless of rules) | Stateless (reutrn traffic must be explicity allowed by rules) |
| Order of Rules | All rules are evaluated before decision to allow traffic | Rules are evaluated in number order before decision to allow traffic. |

## *F. Amazon Route 53*

- Amazon Route 53 is  a highly available and scalable Domain Name System (DNS) web service
- It is used to route end users to internet applications by translating names into numeric IP addresss that computers use to connect to each other.
- It is fully compliant with Ipv4 and Ipv6
- Connects user rerquests to infrastructure running in AWS and also outside of AWS
- It is used to check the health of the resources.
- Features traffic flow
- Enables to register domain names.
- Amazon Route 53 supported routing:
  + Simple routing: Use in single server environments
  + Weighted routing: Assign weights to resource record sets to specify the frequency
  + Latency routing: Help improve global applications
  + Geolocation routing: Route traffic based on location of users.
  + Geopromixity routing: Route traffic based on location of resources
  + Fallover routing: Fall over to a backup site if primary site becomes unreachable.
  + Multivalue answer routing: Respons to DNS queries with up tp eight healthy records selected at random.
- Amazon Route S3 DNS failover: Improve the availability of applications that run on AWS by
  + Configuring backup and failover scenarios for own application
  + Enabling highly available multi-region architectures on AWS
  + Creating health checks

## *G. CloudFront*

- Amazon CloudFront:
  + Fast, global, and secure DNS service
  + Global netowrk of edge locations and Regional edge cahces
  + Self-service model
  + Pay-as-you-go pricing