
VPC

Networking

- Network is the connection between two or more machines to communicate with each other.
- Network components are :

  NIC (Network Interface Card) :

  It is a computer hardware component that connects a computer to a computer network.
  Each NIC will have a unique MAC address to avoid conflicts between same NIC adapters.
  We represent these by the word “eth” or “ens”.

  Media : It is a medium via which two different computer’s NIC card will be connected.

  Topology : Design in which the computers in the network will be connected to each other.

  Protocol : Defines rules and conventions for communications between network devices.

  Ip Addresses : An internet Protocol address is a numerical label assigned to each device connected to a computer network for communication

- Ports : 0 to 65535

Networking

- TCP/IP : Transmission Control Protocol
  - It is connected oriented
  - TCP acknowledgement will be sent/received
  - Slow communication
  - Eg : HTTP, HTTPS

- UPD : User Datagram Protocol
  - It is connectionless
  - No aknowledgements
  - Faster communications.
  - Eg : DNS

Networking

- IP ADDRESS :
- First IP Address : 0.0.0.0
- Last IP Address : 255.255.255.255

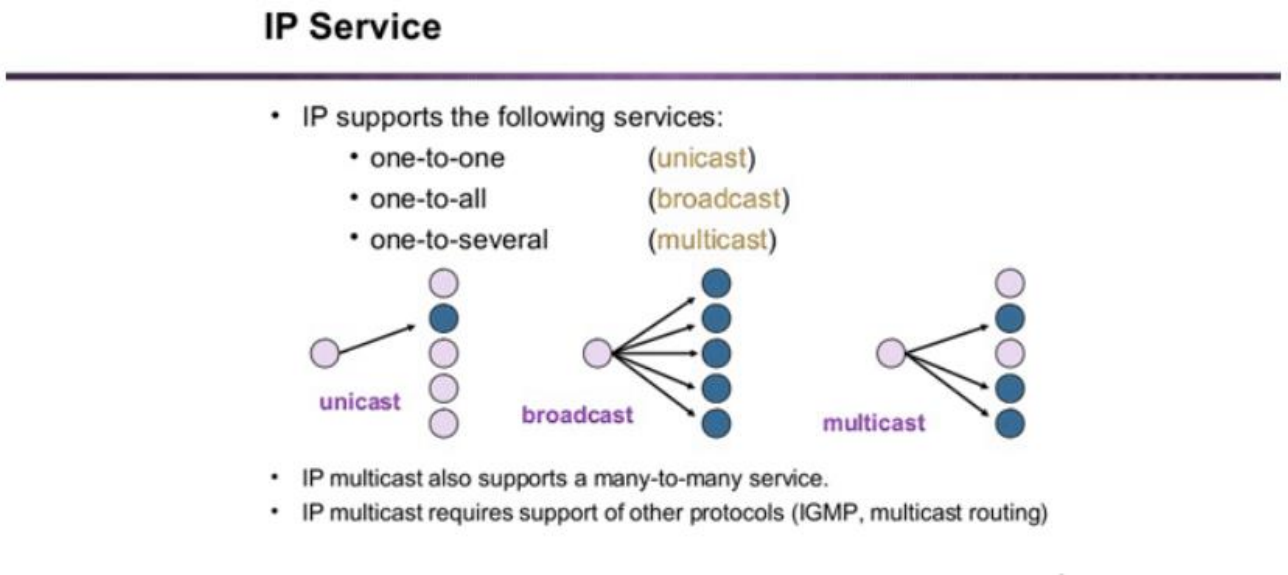
It is called IPV4.
Here the values are converted into binaries.
It is of 32 bits.
IPV6 is of 128 bits and contains alphanumeric values.

- IP Address range is divided into 5 classes :

Class	Left-most Bit	Starting IP Address	Last IP Address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Networking

- Data is transported over a network by three simple methods :



Networking

Unicast :

1. Traffic is sent from one host to another. A replica of each packet in the data stream goes to every host that requests it.

2. The implementation of unicast applications is a bit easy as they use well-established IP protocols; however, they are particularly incompetent when there is a need for many-to-many communications. However, this type of transmission is ineffective in terms of both network and server resources as it equally presents obvious scalability issues.

3. This is a one-to-one connection between the client and the server. Unicast uses IP provision techniques such as TCP (transmission control protocol) and UDP (user datagram protocol), which are session-based protocols

Networking

Broadcast :

Here, traffic streams from a single point to all possible endpoints within reach on the network, which is generally a LAN. This is the easiest technique to ensure traffic reaches its destinations.

This mode is mainly utilized by television networks for video and audio distribution. Even if the television network is a cable television (CATV) system, the source signal reaches all possible destinations, which is the key reason that some channels' content is scrambled. Broadcasting is not practicable on the public Internet due to the massive amount of unnecessary data that would continually reach each user's device, the complications and impact of scrambling, and related privacy issues.

Networking

Multicast :

In this method traffic recline between the boundaries of unicast (one point to one destination) and broadcast (one point to all destinations). And multicast is a “one source to many destinations” way of traffic distribution, which means that only the destinations that openly point to their requisite to accept the data from a specific source to receive the traffic stream.

On an IP network, destinations (i.e. clients) do not regularly communicate straight to sources (i.e. servers), because the routers between source and destination must be able to regulate the topology of the network from unicast or multicast side to avoid disordered routing traffic. Multicast routers replicate packets received on one input interface and send the replicas out on multiple output interfaces.

In the multicast model, the source and destinations are almost every time “Host” and not “Routers”.

Networking

Loopback Address :

- A loopback address is a special IP address, 127.0.0.1, reserved for use in testing network cards.
- This IP address corresponds to the software loopback interface of the network card, which does not have hardware associated with it, and does not require a physical connection to a network.
- The loopback address allows for a reliable method of testing the functionality of an Ethernet card and its drivers and software without a physical network.
- It also allows information technology professionals to test IP software without worrying about broken or corrupted drivers or hardware.
- To test a network card using the loopback address, you can use the TCP/IP utility Ping.
- Just open the command prompt and type ping 127.0.0.1

Networking

CIDR:

Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices. The IP addresses allow particular information packets to be sent to specific computers.

CIDR IP addresses consist of two groups of numbers, which are also referred to as groups of bits. The most important of these groups is the network address, and it is used to identify a network or a sub-network (subnet). The lesser of the bit groups is the host identifier. The host identifier is used to determine which host or device on the network should receive incoming information packets.

According to the CIDR standard, the first part of an IP address is a prefix, which identifies the network. The prefix is followed by the host identifier so that information packets can be sent to particular computers within the network. With the classful routing system, individual networks were either limited to 256 host identifiers or overburdened with 65,536 identifiers. For many network enterprises, 256 identifiers were not enough and 65,536 were too burdensome to be used efficiently.

Networking

Subnet:

A **subnetwork** or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses

A **subnet mask** is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs.
The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.
It ranges from 0 – 32

Calculation of IP Address based upon subnet mask :
https://www.calculator.net/ip-subnet-calculator.html

Count IP Address based subnet mask value : https://cidr.xyz/

Networking

Public IP:

A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a private IP that remains hidden when you connect to the internet through your router's public IP.

Private IP :

A private IP address is the address your network router assigns to your device. Each device within the same network is assigned a unique private IP address (sometimes called a private network address) — this is how devices on the same internal network talk to each other.

Networking

Internet Gateway:

An **internet gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic.

Bastian Host/Jump server:

A **bastion host** is a special-purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.

Route Table:

A **route table** is used to connect IG to subnet.

Networking

DHCP:

A **DHCP** Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

Tenancy:

Tenancy defines how EC2 instances are distributed across physical hardware and affects pricing.
There are three tenancy options available:

Shared (default) — Multiple AWS accounts may share the same physical hardware.

Dedicated Instance (dedicated) — Your instance runs on single-tenant hardware.

Dedicated Host (host) — Your instance runs on a physical server with EC2 instance capacity fully dedicated to your use, an isolated server with configurations that you can control.

Networking

Reserved IP addresses by AWS:

In any range, the 0^{th}, 1^{st}, 2^{nd}, 3^{rd}, and 255^{th} are reserved by AWS.
For example, in the range 10.0.0.0/24 , the reserved ones are :

10.0.0.0 = Network address
10.0.0.1 = Reserved by AWS for VPC Router
10.0.0.2 = Reserved by AWS for IP address for DNS server.
10.0.0.3 = Reserved by AWS for future use.
10.0.0.255 = Reserved for broadcast. VPC do not support broadcast, still it is reserved.

NAT:

Network address translation is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device

VPC : Virtual Private Cloud

Security Group:

A security group acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.

Network ACL:

A network access control list (ACL) 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.

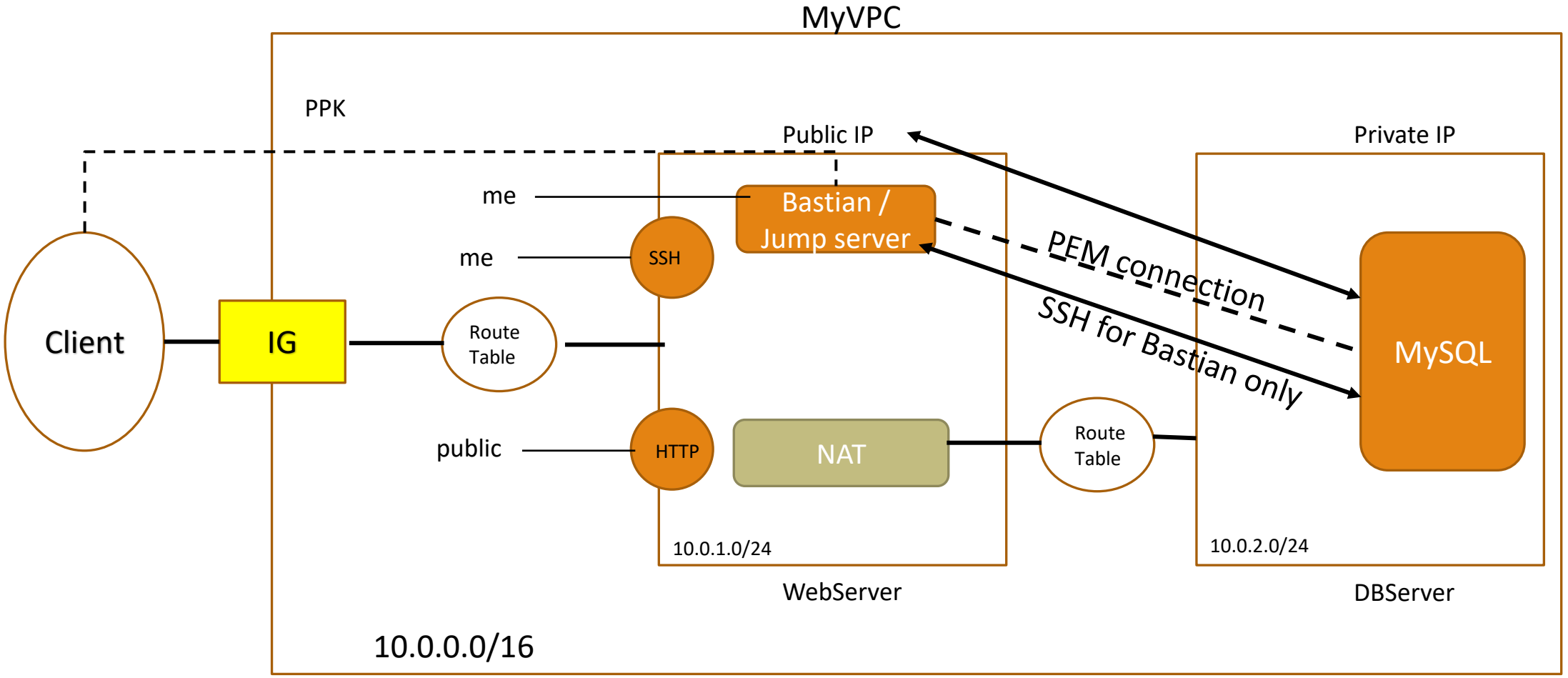
Networking

Comparison of Security Groups and Network ACLs

The following table summarizes the basic differences between security groups and network ACLs.

Security Group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so you don't have to rely on someone specifying the security group)

VPC Example


MyVPC
PPK
Public IP
Private IP
me
Bastian /
Jump server
me
SSH
PEM connection
SSH for Bastian only
Client
IG
Route
Table
MySQL
public
HTTP
NAT
Route
Table
10.0.1.0/24
10.0.2.0/24
WebServer
DBServer
10.0.0.0/16

Hands On 1

1. Create one VPC of name MyVPC
2. Provide the IP range 10.0.0.0/16
3. Select tenancy as “Dedicated”.
4. Create 2 subnets : 10.0.2.0/24 and 10.0.1.0/24 (make it as public)
5. To enable subnet as public :
   Select Subnet
   Go to Actions
   Select “Modify auto assign IP settings”
   Check, “Enable auto assign public IP4 address”
6. Create an Internet Gateway
7. Attach IG to VPC
8. Create a Route Table (will be created by default)
9. Attach Route Table to Subnet (that is public) --- > Subnet Associations by selecting Route Table instance
10. Attach Route Table to IG ---- > Select Routes by selecting Route Table instance, give target as IG and destination as 0.0.0.0/0

Hands On 1

11. Launch 2 EC2 instances –1 in public subnet(SSH- MyIP, HTTP – 80 to all)
2nd one is private with below Security Group details :

12. Give the following lines in option (for public subnet only) :

```
#!/bin/bash
sudo su
yum update -y
yum install httpd -y
systemctl start httpd.service
systemctl enable httpd.service
echo "Hello from $(hostname -f)" > /var/www/html/index.html
```

Hands On 1

13. Try to access the 2 Ec2 instances (won't be able to connect to private EC2 as SSH 22 port is off).
14. Open another EC2 instance as Bastian Server (with default VPC and public IP as subnet) with Security Group port as SSH to MyIP.
15. Add Bastian port also as inbound to private subnet DB. Edit Security group of DB and add SSH to Private IP address of Bastian EC2
16. Open Bastian Server. Connect to DB from Bastian server. So it is a connection between from 1 Linux EC2 to another Linux EC2.
17. Need to place DB server's pem file to Bastian server.
    Login to Bastian EC2 and put the Connect details of DB server using :
    chmod 600 "mydb.pem"
    ssh -i "mydb.pem" ec2-user@.....