What is VPC & how it worked in cloud –

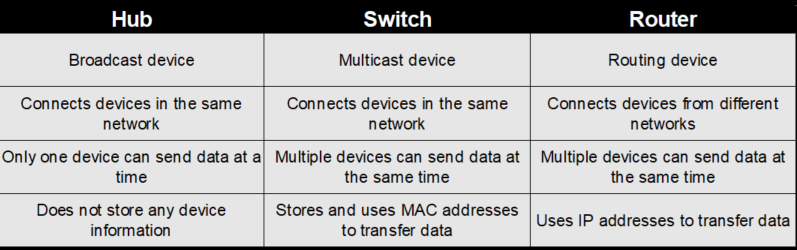
Amazon Virtual Private Cloud (Amazon VPC) **gives you full control over your virtual networking environment, including resource placement, connectivity, and security.** Get started by setting up your VPC in the AWS service console.

* NIC – ENI (Elastic Networking Interface)
* Hub – Repeater –Connecting all networks ---Broadcasting— (Send to everyone in the network)
* Switch – Subnet in cloud –IN AWS cloud Likes 1a/1b/1c----Send to packet for requester only --

Its connections of IPs

* Router- Gateway VPC Router—AWS used

Internet Gateway – Internet



* Operating System /Instance -----In aws Security Group

Firewall ---

* Enterprises Firewall ---NACL (Network Access Control List)
* NAT ---SNAT

DNAT

PAT

* IP Address – IPV4 & IPV6
* Public IP Address & Private IP Address

Its Assign IP with DNS, DHCP as well

This all are working behind the network – **SDN (Software-Defined Networking)**

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network.

* VPC is Regional Service in AWS

Define the IPV4 & IPV6: -

|  |  |
| --- | --- |
| **IPV4** | **IPV6** |
| 32-bit | 128-bit |
| 4-billions | near infinity (unlimited) |
|  |  |

IPV4: - IPV4 having working on 2 types of class

1. Class Full
2. Class less----- <CIDR>

**Class Full**: - The method divides the IP address space for Internet Protocol version 4 (IPv4) into five address classes based on the leading four address bits. Classes A, B, and C provide unicast addresses for networks of three different network sizes.

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **IP Address Range** | **Subnet mask** |  |
| Class A | 1 to 126 | 255.0.0.0 |  |
| Class B | 128 to 191 | 255.255.0.0 |  |
| Class C | 192 to 223 | 255.255.255.0 |  |
| Class D | 224 to 239 |  | *Multicasting* |
| Class E | 240 to 255 |  | *Research/Reserved/Experimental* |

In the IPv4 IP address space, there are five classes: A, B, C, D and E. Each class has a specific range of IP addresses (and ultimately dictates the number of devices you can have on your network). Primarily, class A, B, and C are used by the majority of devices on the Internet. Class D and class E are for special uses.

The list below shows the five available IP classes, along with the number of networks each can support and the maximum number of hosts (devices) that can be on each of those networks. The four octets that make up an IP address are conventionally represented by a.b.c.d - such as 127.10.20.30.

Additionally, information is also provided on private addresses and loop address (used for network troubleshooting).

**Class A Public & Private IP Address Range**

Class A addresses are for networks with large number of total hosts. Class A allows for 126 networks by using the first octet for the network ID. The first bit in this octet, is always zero. The remaining seven bits in this octet complete the network ID. The 24 bits in the remaining three octets represent the hosts ID and allows for approximately 17 million hosts per network. Class A network number values begin at 1 and end at 127.

* Public IP Range: 1.0.0.0 to 127.0.0.0

First octet value range from 1 to 127

* Private IP Range: 10.0.0.0 to 10.255.255.255
* Subnet Mask: 255.0.0.0 (8 bits)
* Number of Networks: 126
* Number of Hosts per Network: 16,777,214--------------------- (224-2). or 256\*256\*256-2

**Class B Public & Private IP Address Range**

Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allows for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

* Public IP Range: 128.0.0.0 to 191.255.0.0

First octet value range from 128 to 191

* Private IP Range: 172.16.0.0 to 172.31.255.255
* Subnet Mask: 255.255.0.0 (16 bits)
* Number of Networks: 16,382
* Number of Hosts per Network: 65,534---------------------------(216-2). or 256\*256-2

**Class C Public & Private IP Address Range**

Class C addresses are used in small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. In a class C IP address, the first three bits of the first octet are always 1 1 0. And the remaining 21 bits of first three octets complete the network ID. The last octet (8 bits) represent the host ID and allows for 254 hosts per network. Class C network number values begins at 192 and end at 223.

* Public IP Range: 192.0.0.0 to 223.255.255.0

First octet value range from 192 to 223

* Private IP Range: 192.168.0.0 to 192.168.255.255
* Special IP Range: 127.0.0.1 to 127.255.255.255
* Subnet Mask: 255.255.255.0 (24 bits)
* Number of Networks: 2,097,150
* Number of Hosts per Network: 254--------------------------- (28-2). or256-2

**Class D IP Address Range**

Class D IP addresses are not allocated to hosts and are used for multicasting. Multicasting allows a single host to send a single stream of data to thousands of hosts across the Internet at the same time. It is often used for audio and video streaming, such as IP-based cable TV networks. Another example is the delivery of real-time stock market data from one source to many brokerage companies.

* Range: 224.0.0.0 to 239.255.255.255

First octet value range from 224 to 239

* Number of Networks: N/A
* Number of Hosts per Network: Multicasting

**Class E IP Address Class**

Class E IP addresses are not allocated to hosts and are not available for general use. These are reserved for research purposes.

* Range: 240.0.0.0 to 255.255.255.255

First octet value range from 240 to 255

* Number of Networks: N/A
* Number of Hosts per Network: Research/Reserved/Experimental

**Private IP Addresses**

Within each network class, there are designated IP address that is reserved specifically for private/internal use only. This IP address cannot be used on Internet-facing devices as that are non-routable. For example, web servers and FTP servers must use non-private IP addresses. However, within your own home or business network, private IP addresses are assigned to your devices (such as workstations, printers, and file servers).

* Class A Private Range: 10.0.0.0 to 10.255.255.255
* Class B Private **APIPA Range: 169.254.0.0 to 169.254.255.255**

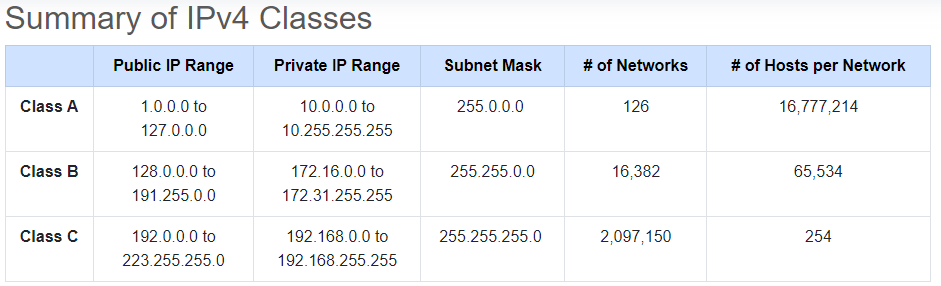
*Automatic Private IP Addressing* (APIPA) is a feature with *Microsoft Windows*-based computers to automatically assign itself an IP address within this range if a *Dynamic Host Configuration Protocol (DHCP) server is not available on the network. A DHCP server is a network device that is responsible for assigning IP addresses to devices on the network.  
  
At your home, your Internet modem or router likely provides this functionality. In your work place, a Microsoft Windows Server, a network firewall, or some other specialized network device* likely provides this functionality for the computer at your work environment.

* Class B Private Range: 172.16.0.0 to 172.31.255.255
* Class C Private Range: 192.168.0.0 to 192.168.255.255

**Special IP Address:** 127.0.0.1 to 127.255.255.255 are network testing addresses (**also referred to as loop-back addresses**). These are virtual IP address, in that they cannot be assigned to a device. Specifically, the IP 127.0.0.1 is often used to troubleshoot network connectivity issues using the [*ping command*](https://www.meridianoutpost.com/resources/articles/command-line/ping.php)*.*

We are only used 1st 3 Class (A, B, C) for device networking and Class D & Class E are used only for multicasting & research development –for experimental

**Summary for IPV4 class which we can used –**



**For more about IPV4 -** [*https://www.meridianoutpost.com/resources/articles/IP-classes.php*](https://www.meridianoutpost.com/resources/articles/IP-classes.php)

**Important Notes: -**

**Class less: - CIDR (Classless Inter-Domain Routing)** is the successor to class-oriented domains for Internet routing, it allows for better allocations of Internet addresses. It combines a number of Class C Internet Protocol (IP) addresses to reduce the burden on routing tables in the Internet.

Classless Inter-Domain Routing (CIDR), also called supernetting, is a way to more flexibly allocate Internet Protocol (IP) addresses by creating unique and more granular identifiers for networks and individual devices. It was introduced in 1993 as an alternative to Internet routers that managed network traffic based on the class of IP addresses and determined subnetworks, for routing, based on IP address class.

The objective of CIDR was to address scalability issues with classful IP addresses which are based on three classes – Class A, Class B, and Class C. Since it is not bound by Class, CIDR can organize IP addresses into subnetworks independent of the value of the addresses themselves. This is referred to as supernetting because CIDR effectively allows the aggregation of multiple subnets into a supernet for network routing. With this alternative to traditional subnetting, it is possible to specify the number of significant bits that make up the routing or networking portion by adding this to the IP address. This not only reduces wasted address space but also provides a flexible way to specify network addresses in routers.

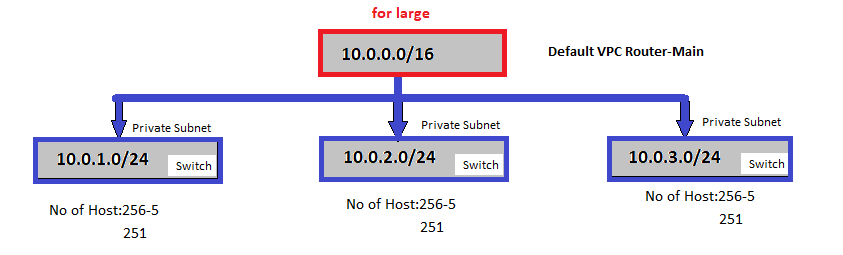
Classless IP addresses, enabled by CIDR, are required when creating a Virtual Private Cloud (VPC) that is logically isolated from other virtual networks. When creating a VPC, a range of IPv4 addresses must be specified in the form of a CIDR.

**VSLM (Variable Subnet Length Mask)**

Variable Length Subnet Mask (VLSM) is a subnet -- **a segmented piece of a larger network -- design strategy where all subnet masks can have varying sizes.** This process of "subnetting subnets" enables network engineers to use multiple masks for different subnets of a single class A, B or C network.

When we create the VPC in AWS, make sure we can take the large network as –If we create the small network it’s very difficult when increase the host or machines.

**Class A: -**

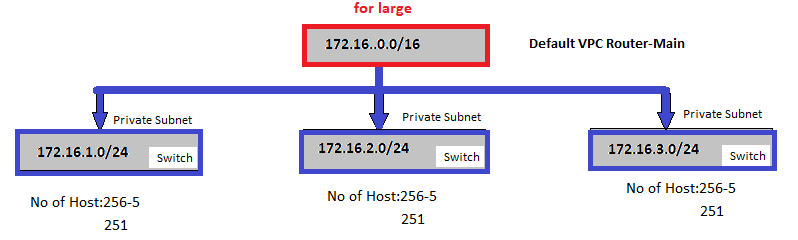


In Normal Switch only 2 IP has been lost in every subnet but in AWS its should 5 IP’s

In AWS Below are the IP’s goes default for every subnet

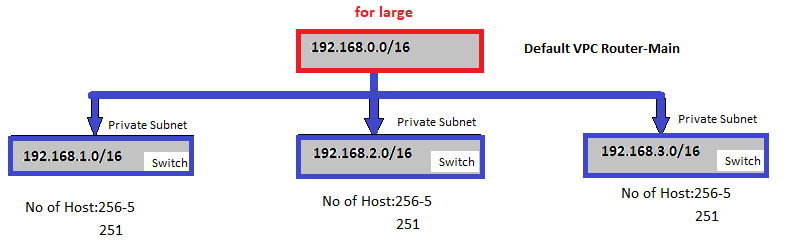
1. 10.0.1.0 For Network Subnet address
2. 10.0.1.1 For Router
3. 10.0.1.2 For DNS/DHCP
4. 10.0.1.3 For Reserve
5. 10.0.1.255 For Broadcasting

**Class B: -**



It’s also same as like Class A 5 IP’s are goes to networking add, Router, DNS/DHCP, Reserve & last for broadcasting except 251 are used.

**Class C: -**



It’s also same as like Class A & Class B 5 IP’s are goes to networking add, Router, DNS/DHCP, Reserve & last for broadcasting except 251 are used.

**VPC – < Isolation >**

VPC is part of a public cloud**, VPCs are logically isolated networks so your data and applications are entirely separate from your provider's other clients.** Access is limited to your resources, unless you grant this. Logical isolation makes a VPC environment inherently more secure.

Isolation provide the more security in flat network.

**Advantages**

1. Network Isolation: - VLAN, VxLan, GRE ----------------Logical splitting of network

-Working on Tunnelling Protocol.

1. Complete Control on network design, subnets & IP Address.
2. Create Private Cloud inside the Public cloud.