AWS Networking

Cloud Computing

Brenden west

Contents

Learning Outcomes

- Basics of computer networking
- Virtual networking with AWS VPC & Route 53
- Managing security & access control
- Distributed content delivery with AWS CloudFront

Resources

- Cloud Computing: Concepts, Technology, Security, and Architecture - Ch. 5
- AWS Cloud Foundations - module 5
- https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

Networking Basics

- A computer network is 2 or more connected client machines
- A network can be logically partitioned into **subnets**
- Networking requires a device (e.g. router or switch) to enable communications between devices on the network
- Each client machine has a unique **IP address** - a numeric label in decimal format (e.g. 192.0.2.0)
- Each dot-separated number represents 8 bits in **octal** number format (so numbers 0 - 255)
- IP addresses can be **IPv4** (32 bits) or **IPv6** (128 bits)

Networking Basics, cont.

- An IPv6 address is 8 four-item 16-bit groups of letters & numbers
- **CIDR** describes a group of consecutive IP addresses
  - The last number indicates how many bits are fixed
  - Other numbers can vary from 0 to 255
  - e.g. 192.0.2.0/24 - only the last 8 bits can vary, so the IP range is 2^8 or 256 addresses

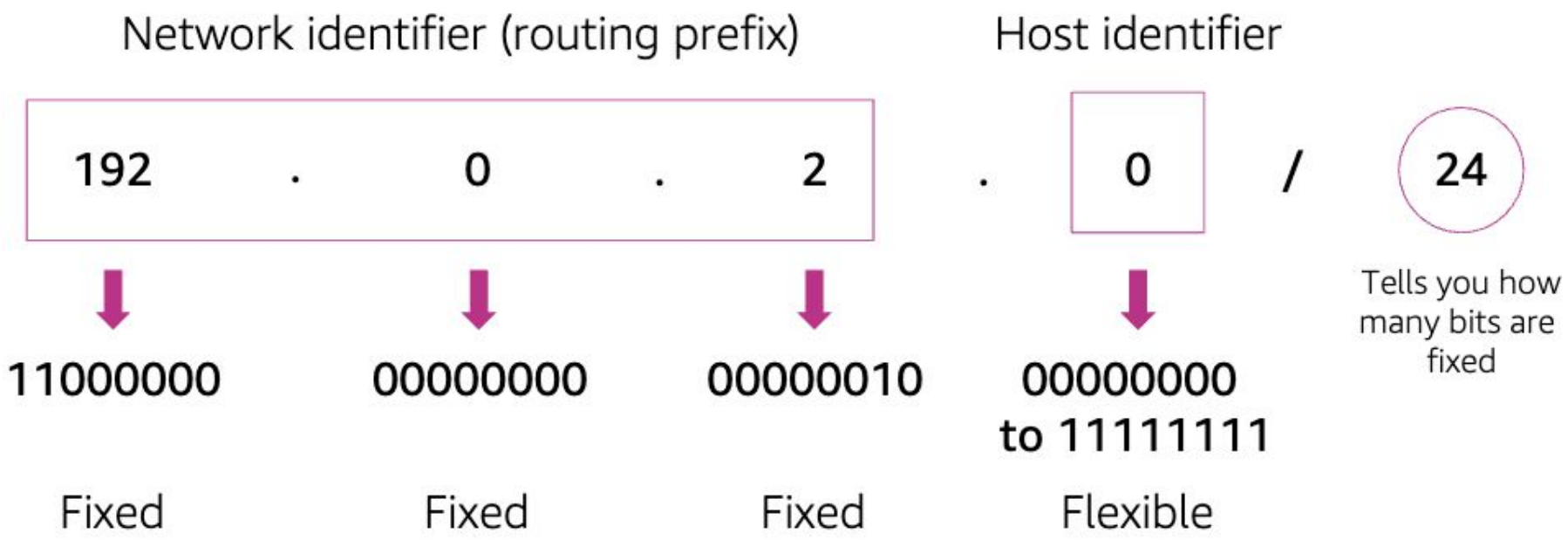
OSI Model

- A conceptual model that describes how data travels over a network.
- Consists of seven layers showing the common protocols and addresses used to send data at each layer.
- Helps explain how communication happens in a virtual private cloud (VPC)

Open Systems Interconnection (OSI) model

Layer	Number	Function	Protocol/Address
Application	7	Means for an application to access a computer network	HTTP(S), FTP, DHCP, LDAP
Presentation	6	• Ensures that the application layer can read the data • 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)

Classless Inter-Domain Routing (CIDR)



Amazon Virtual Private Cloud (VPC)

- Dedicated, logically isolated section of Amazon Cloud where an account's AWS resources are launched
- Belong to a single AWS region. Can span multiple availability zones
- AWS customer can :
  - Select IP address range
  - Divide VPC into one or more subnets
  - Configure route tables
  - Define security groups & network access control lists (ACLs)

Subnets

- A section of a VPC into which resources are grouped based on security or operational needs.
- Belong to a single Availability Zone
- **Public subnet** - contains resources that need to be accessible to the public
- **Private subnet** - contains resources that should be accessed only through the account's private network
- Subnets within a VPC can communicate with each other

VPC IP Addressing

- Creating a VPC involves assigning an IPv4 CIDR block
- Address range can’t be changed
- Each subnet requires its own CIDR block
- Five addresses in each CIDR block are reserved by AWS & unavailable for account use
- Subnet CIDR blocks can’t overlap
- A VPC can’t have duplicate IP addresses
- Optional IPv6 CIDR block can be assigned to a VPC & subnets
- Every instance in the VPC automatically gets a **private** IP address (default network interface)

Public IP address types

- Resource instances can be assigned a public IP address when created, either:
  - Through the subnet's auto-assign public IP address properties
  - Manually through an **Elastic** IP address
- Elastic IP address
  - A static, public IPv4 address
  - Can be associated with any VPC instance or network interface in an account
  - Useful for masking instance failure or moving network interface attributes in a single step
  - May incur additional costs, so important to release if unused

Network Access Control List (ACL)

- VPC component that controls inbound & outbound network traffic for a subnet
- Perform **stateless** packet filtering as packets cross subnet boundary

Route Tables

- Route table contains rules (**route**) that directs network traffic from a subnet
- Each route specifies a **destination** (CIDR block) & a **target**
- Every route table contains a **local** route for communication within the subnet
- VPC automatically has a **main** route table to control routing for any subnets not associated with any other route table
- Each subnet in a VPC must be associated with one, and only one, route table
- Multiple subnets can be associated with a route table

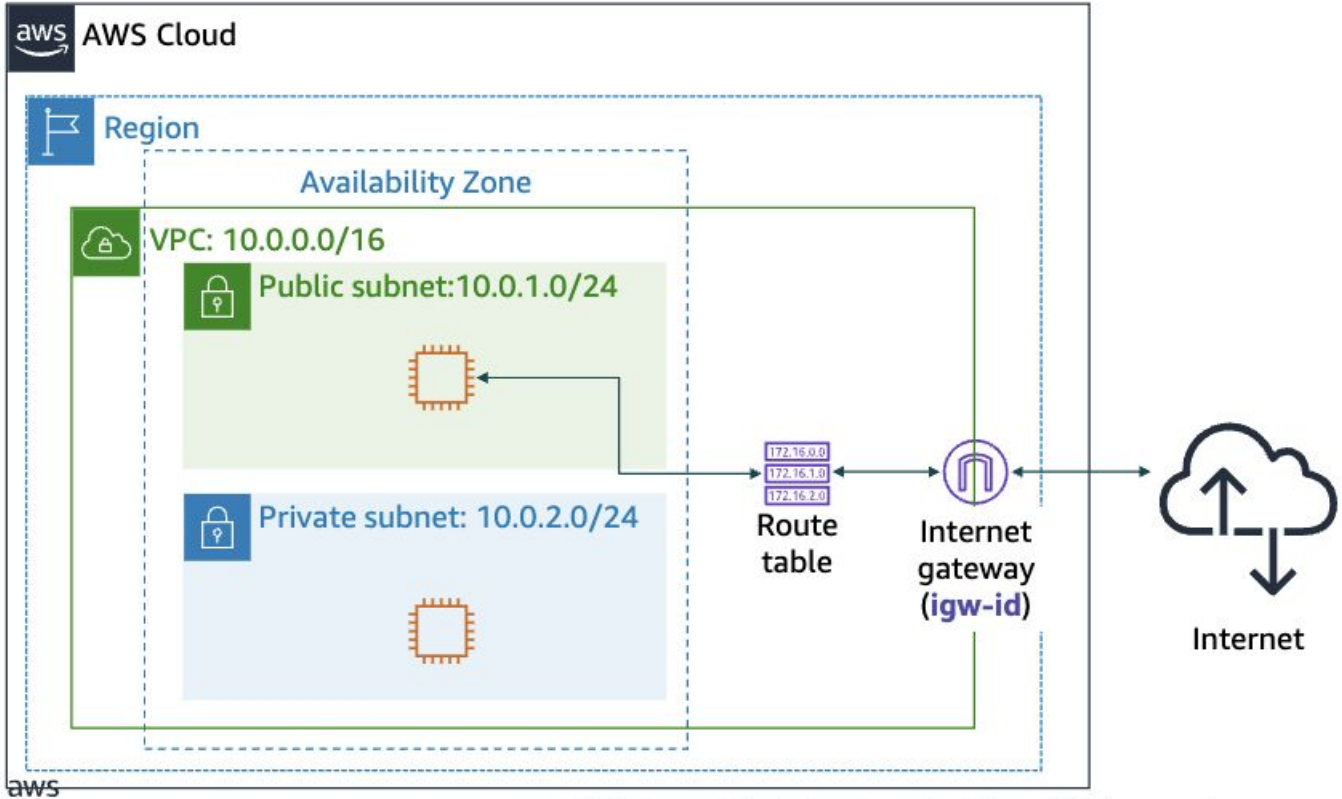
VPC Networking

- **Internet Gateway** - a scalable, redundant, and highly available VPC component that allows communication between VPC instances and the internet.
  - provides a target in VPC route tables for internet routable traffic
  - Performs network address translation for instances that have public IPv4 addresses
- **Network Address Translation** (NAT) gateway - enables instances in a private subnet to connect to internet or other AWS services while preventing inbound internet connections
  - Must reside in a public subnet
  - Must be created with an Elastic IP address

VPC Networking, cont.

- **VPC Sharing** - enables sharing of subnets with other AWS accounts in the same AWS Organization
  - Multiple AWS accounts can create application resources in shared, centrally managed VPCs
  - Allows application owners to offload networking duties while keeping control of resources

Internet gateway



Public Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Amazon Route 53

- Highly available & scalable Domain Name System (DNS)
- Routes end users to internet applications by translating names into numeric IP addresses
- Compliant with IPv4 and IPv6
- Connects to infrastructure running in AWS or outside AWS
- Can register domain names
- Supports a variety of routing policies

Amazon CloudFront

- Fast, global, secure content delivery network (CDN) service
- Global network of **edge locations** and regional **edge caches**
- Self-service model with pay-as-you-go pricing