



# Amazon VPC-1



CLARUSWAY  
WAY TO REINVENT YOURSELF

## Table of Contents



- ▶ Introduction to VPC
- ▶ VPC Basic Components

CLARUSWAY  
WAY TO REINVENT YOURSELF



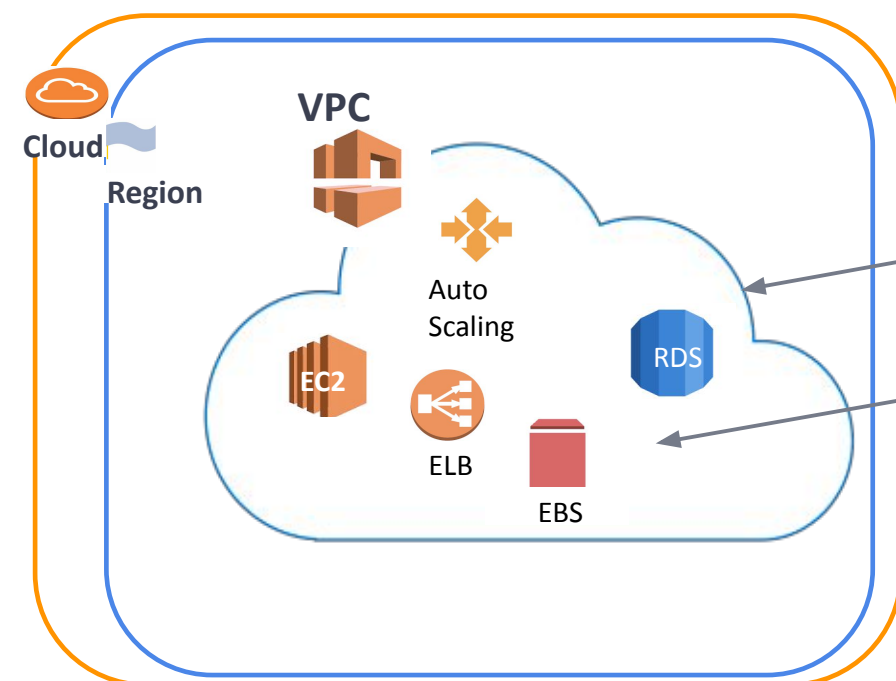
1

# Introduction to VPC

## Introduction to VPC



### What is VPC?



Amazon Virtual Private Cloud (Amazon VPC) is a **logically isolated area** of the AWS cloud where you can **launch AWS resources in a virtual network** that you define.

## 2

# VPC Basic Components

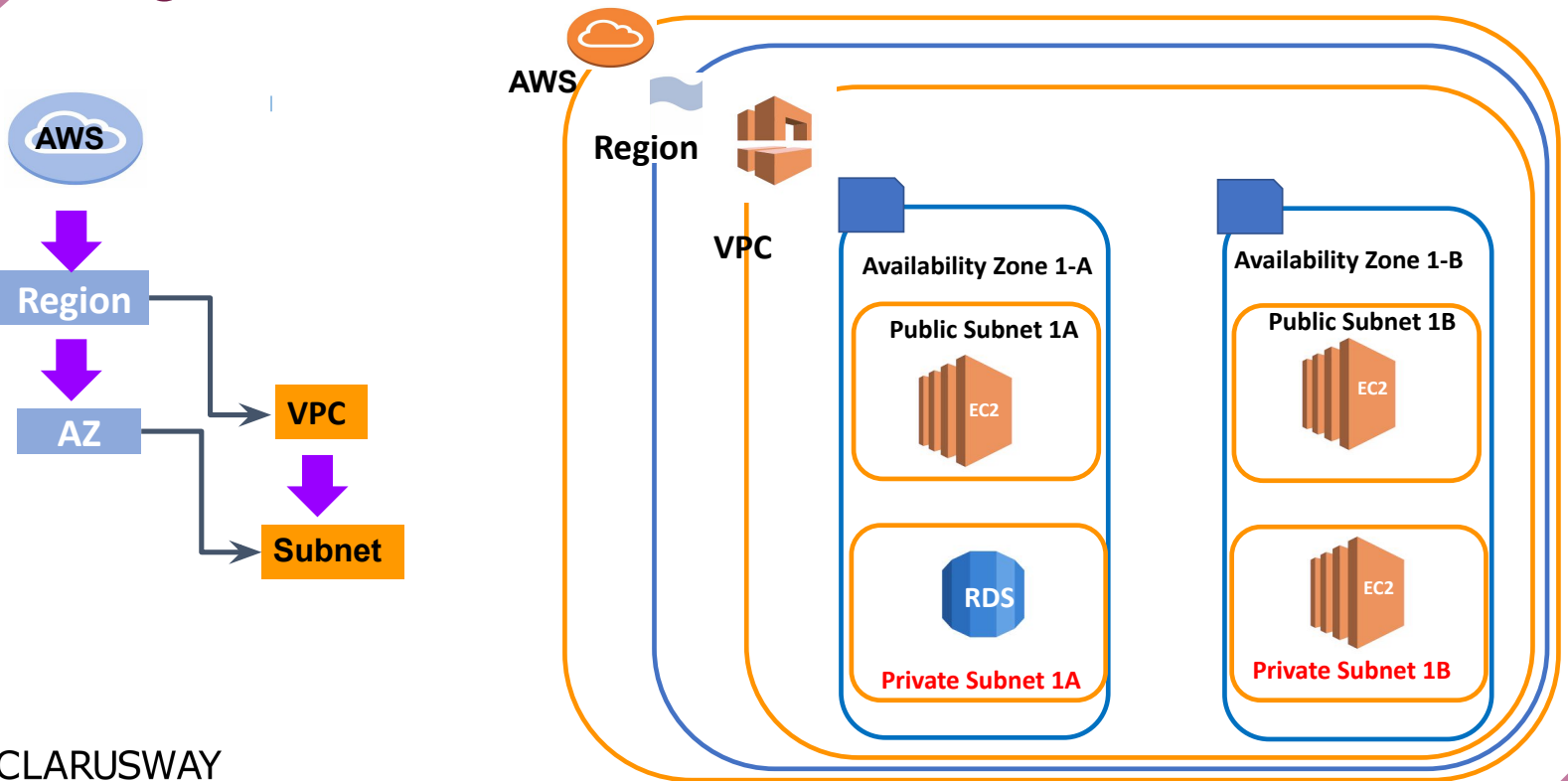
CLARUSWAY  
WAY TO REINVENT YOURSELF

## VPC Basic Components

- VPC Region (AZ)
- VPC Subnets
- VPC CIDR
- Internet Gateway
- Route Table
- Security Group and Network ACL



# Region, VPC, AZ and Subnets



7

## VPC CIDR



10.0.0.0/16

Block Size

10.0.0.0/16 = 65,536 IPs in Range

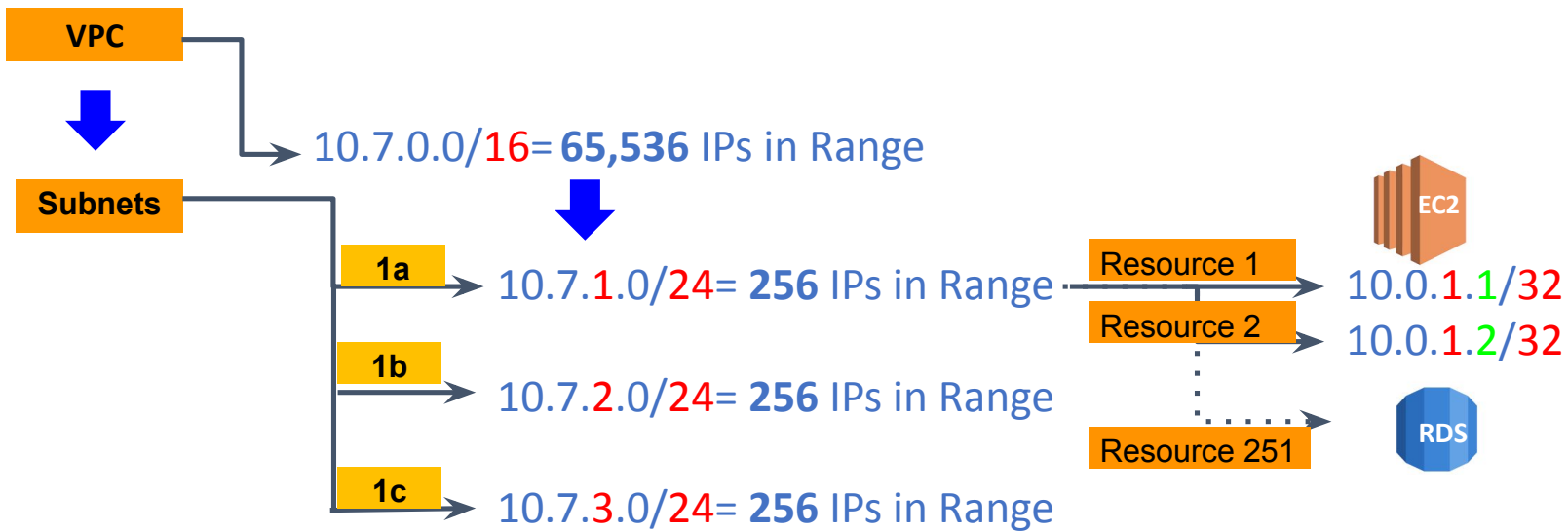
10.0.1.0/24 = 256 IPs in Range

10.0.1.0/32 = 1 IP in Range

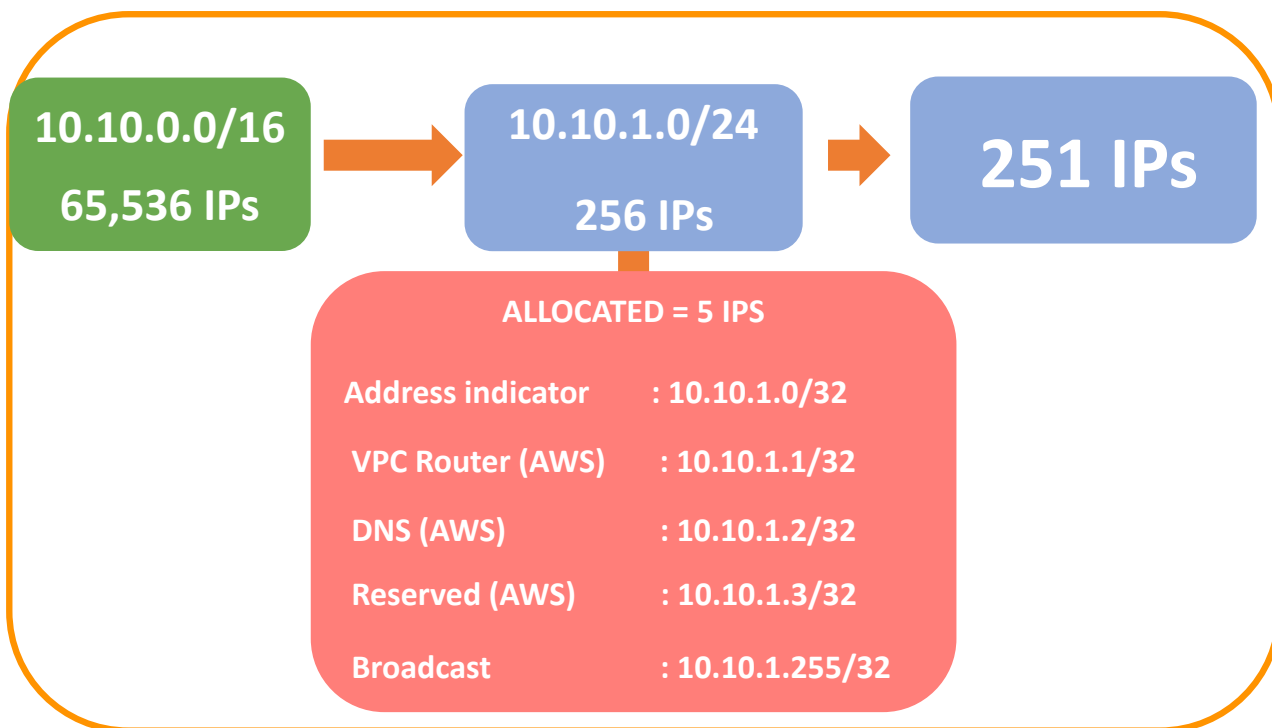
- CIDR refers to Classless Inter-Domain Routing.
- It is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks.
- As the Size Block/Netmask (/16,24,32) increases, the number of IP located in CIDR Block decreases.

8

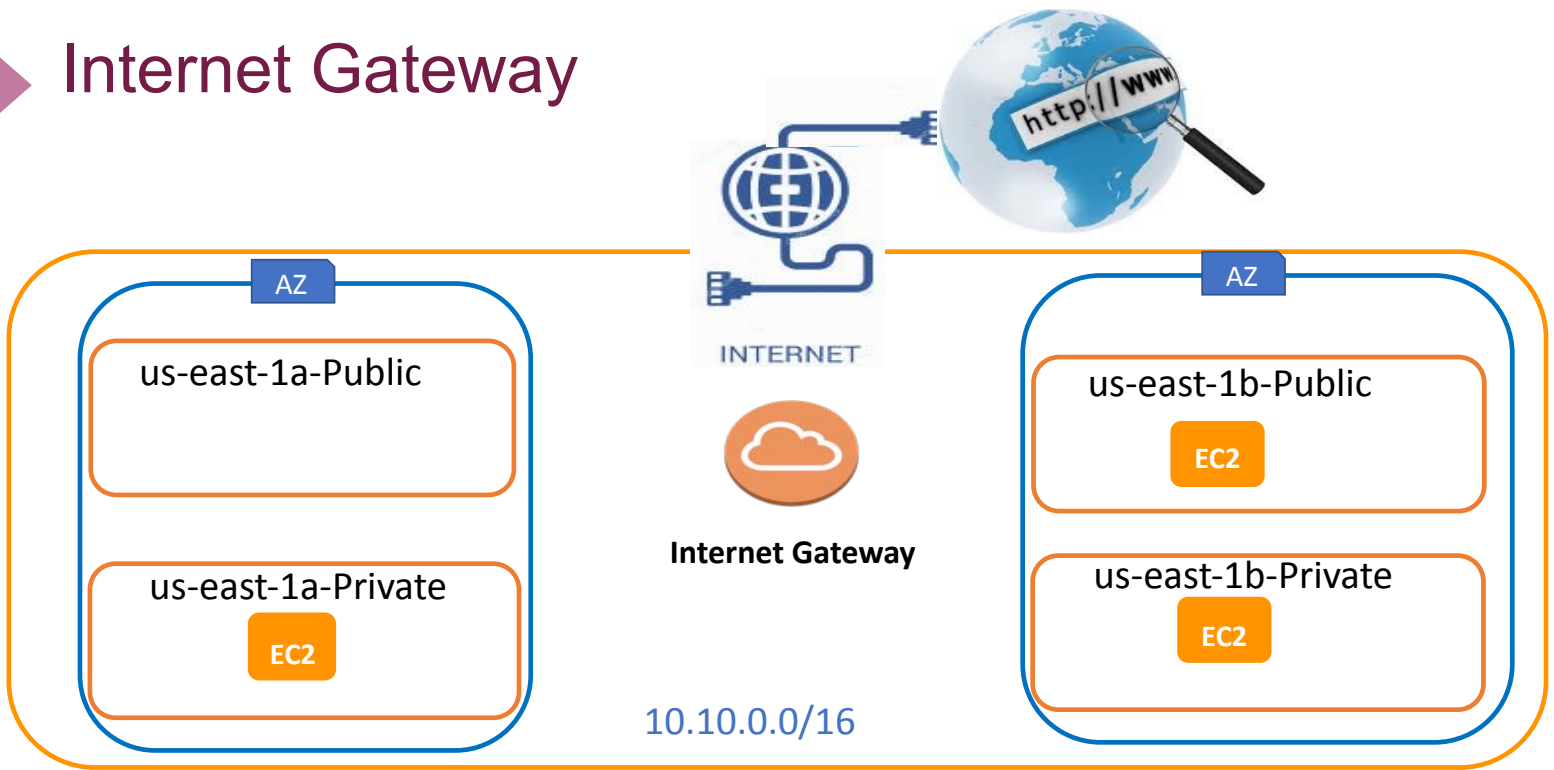
## VPC CIDR



## VPC CIDR



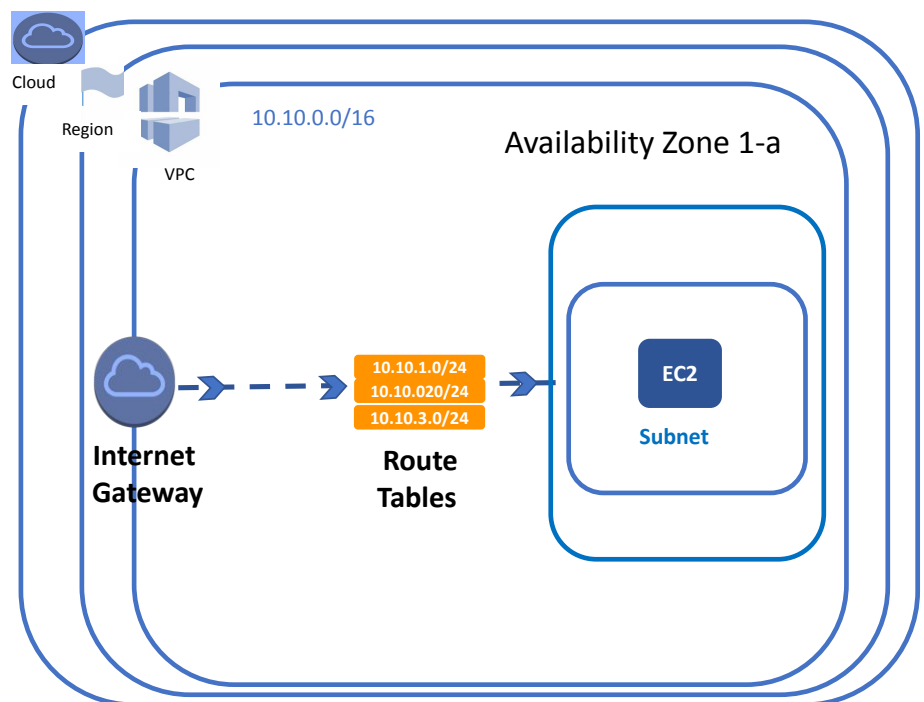
# Internet Gateway



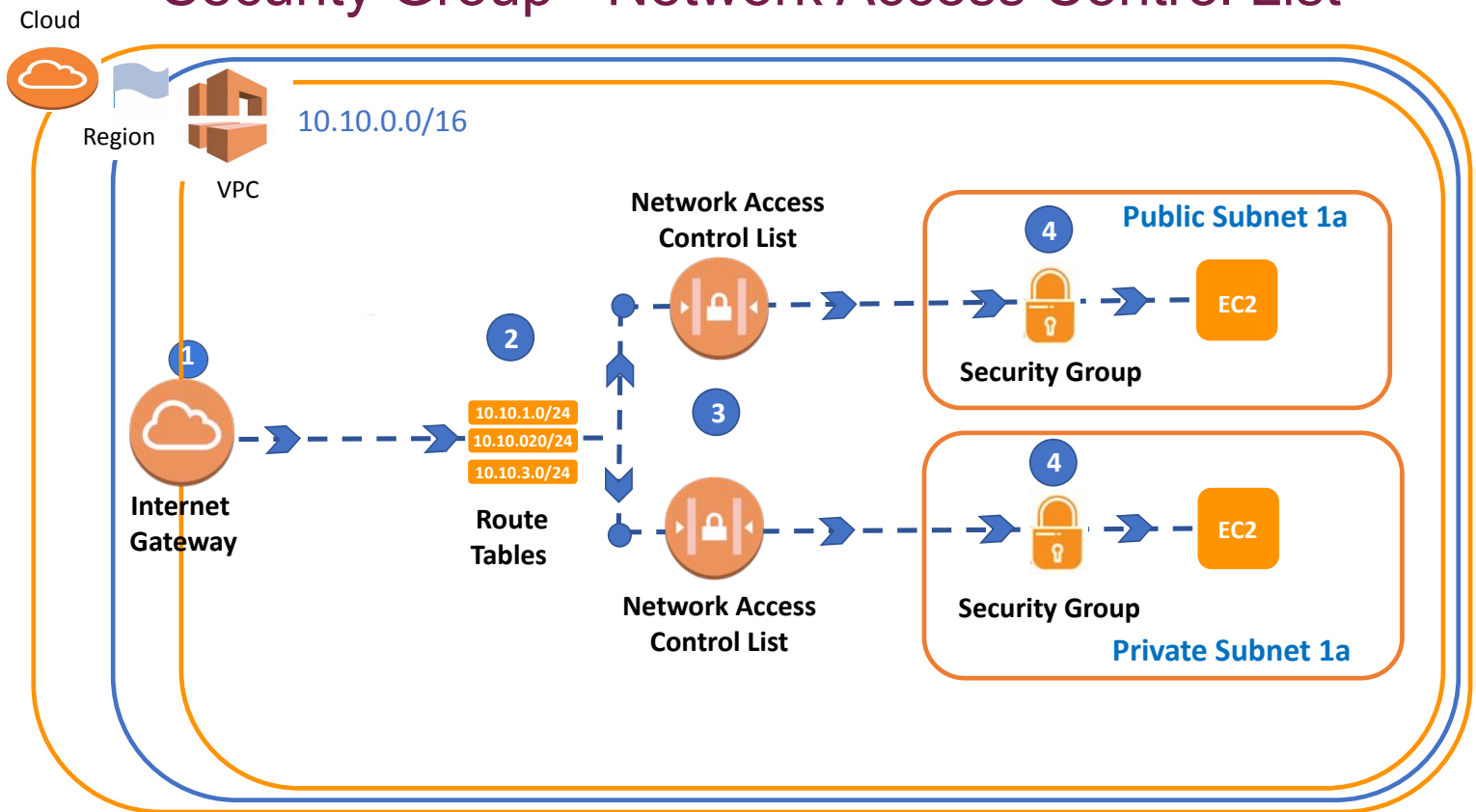
- **Internet Gateway** is a VPC component that provides communication between resources in your VPC and the internet.

# Route Table

- **Route Table** is a set of rules, that is used to determine where VPC traffic is directed.



# Security Group - Network Access Control List





## Network ACLs & Security Groups



- Network ACLs are **subnet-based security components**.
- It controls the traffic in and out of subnets.

- Security Groups are instance-based **security** components,
- They are used for determining which traffic will access the instance.

- Instance in subnet is affected by rules of both Security Groups and Network ACLs

Security Group		Network Access Control List
		
<b>Rules</b>	It supports only <b>Allow Rules</b>	It supports <b>both Allow and Deny</b> rules
<b>Default by AWS</b>	By default, <b>inbound</b> rules are <b>Denied</b> , <b>outbound</b> rules are <b>Allow</b>	By default, all the rules are <b>Allowed</b>
<b>* Newly Created by User</b>	By default, <b>inbound</b> rules are <b>Denied</b> , <b>outbound</b> rules are <b>Allow</b>	By default, all the rules are <b>Denied*</b> until you add rules.
<b>Add Rule</b>	You need to add the rule which you'll <b>Allow</b>	You need to add the rule which you can <b>either Allow or Deny it</b> .
<b>Stateful/Stateless</b>	It is a <b>Stateful</b> means that any changes made in the inbound rule will be automatically reflected in the outbound rule	It is a <b>Stateless</b> means that any changes made in the inbound rule will not reflect the outbound rule
<b>Association</b>	<ol style="list-style-type: none"> <li>1. It is <b>instance-based</b></li> <li>2. Instances can associate with <b>more than one</b> Security Groups</li> </ol>	<ol style="list-style-type: none"> <li>1. It is <b>subnet-based</b></li> <li>2. Subnets can <b>associate with only one</b> Network ACL</li> </ol>



# THANKS!

## Any questions?

