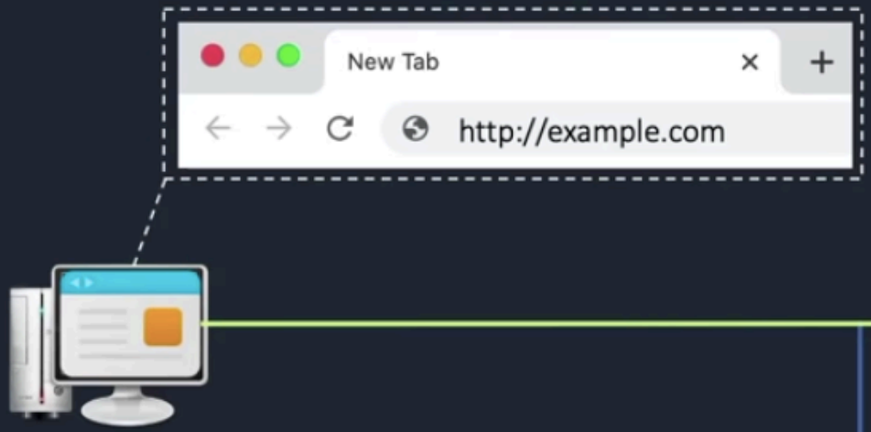
What is an IPv4 address?

IP addresses are the addresses computers use to communicate



52.134.26.12

Web Server

Connection is made using **IP address**

What's the **IP address** for example.com?

Name	Type	Value
example.com	A	52.134.26.12
test.com	A	137.10.47.51

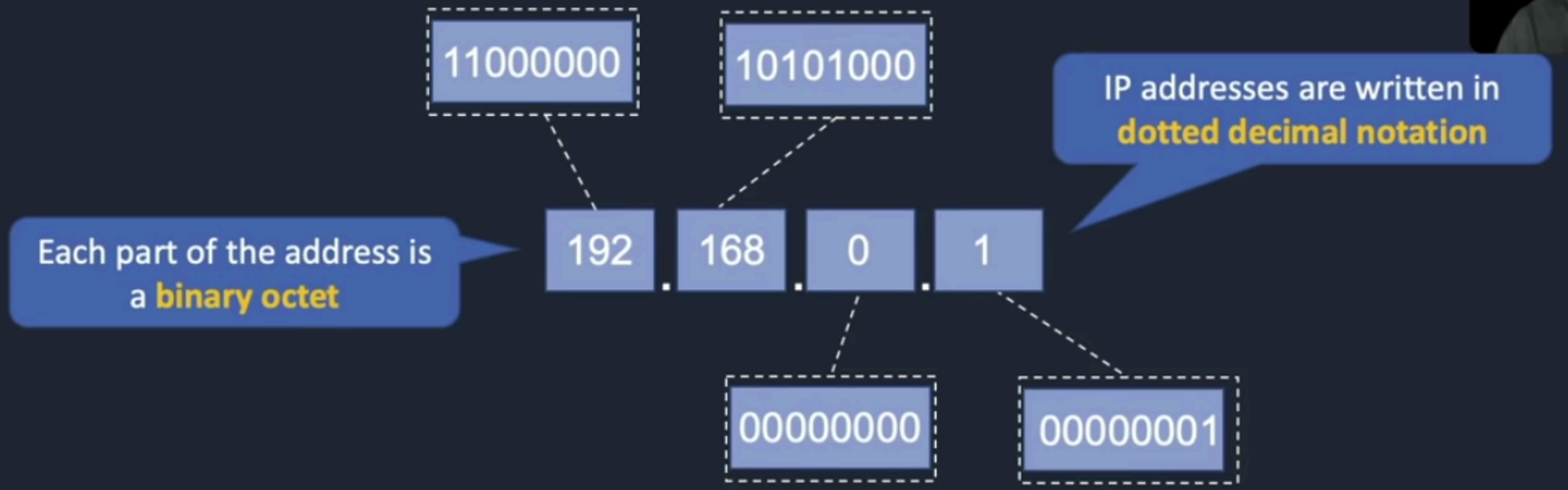
DNS Zone File

DNS Server

DigitalCloud TRAINING

SUBSCRIBE

Structure of an IPv4 Address



Most significant bit ⟶

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

⟵ Least significant bit

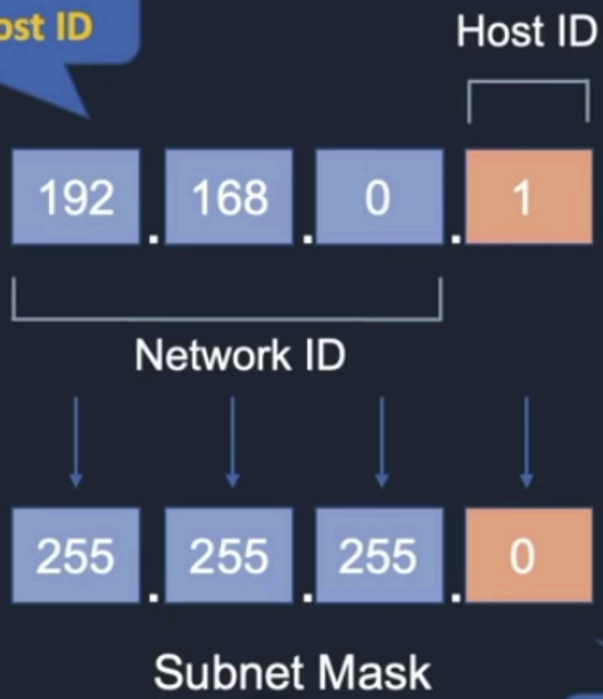
Binary Values

DigitalCloud TRAINING

SUBSCRIBE

Networks and Hosts

An IPv4 address has a **network** and **host ID**



The **subnet mask** is used to define the **network** and **host ID**

DigitalCloud TRAINING

SUBSCRIBE

Networks and Hosts

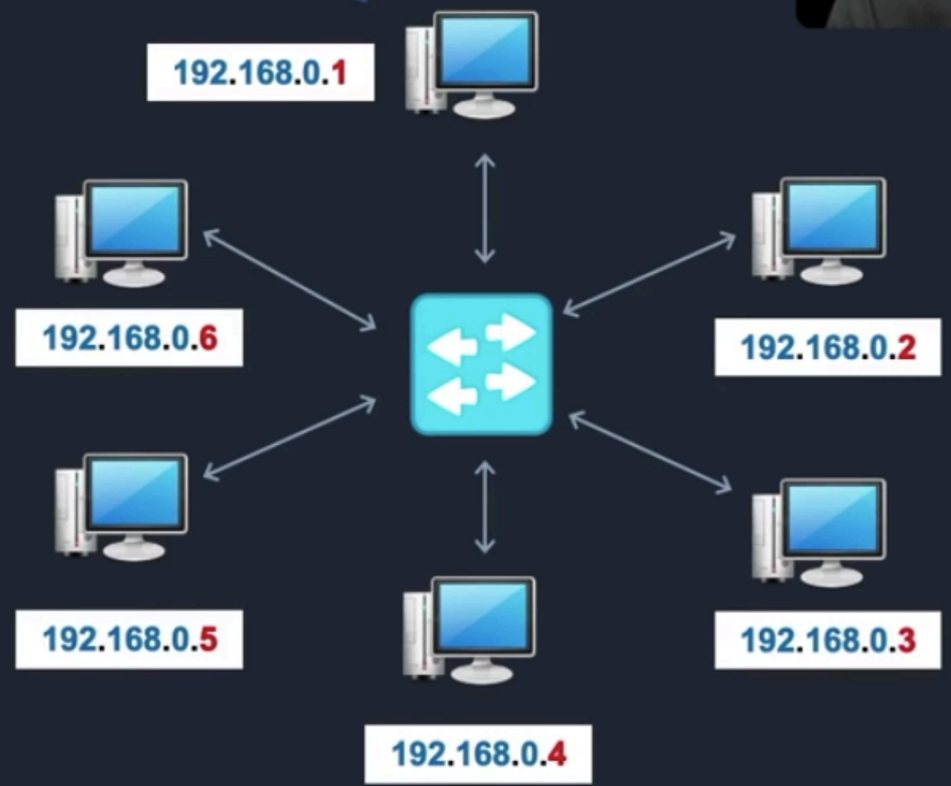
Network	192	168	0	0
Subnet Mask	255	255	255	0

24 bits

192.168.0.0/24

A network and subnet mask can also be written in this format

All computers share the same network ID and have a unique host ID



DigitalCloud TRAINING

SUBSCRIBE

Classes of IPv4 Address

Class A	10	0	0	0
	255	0	0	0
Class B	172	16	0	0
	255	255	0	0
Class C	192	168	0	0
	255	255	255	0

First assignable address = 10.0.0.1
Last assignable address = 10.255.255.254
Total networks = 126
Usable addresses per network = 16,777,214

First assignable address = 172.16.0.1
Last assignable address = 172.16.255.254
Total networks = 16,382
Usable addresses per network = 65,534

First assignable address = 192.168.0.1
Last assignable address = 192.168.0.254
Total networks = 2,097,150
Usable addresses per network = 254

DigitalCloud TRAINING

Private IP Address Ranges

10	0	0	0	→	10	255	255	255
172	16	0	0	→	172	32	255	255
192	168	0	0	→	192	168	0	255

These addresses are reserved for **private use** according to IETF RFC-1918

DigitalCloud TRAINING

SUBSCRIBE

Classless Interdomain Routing (CIDR)

Network	192	168	0	0	
/24 Subnet Mask	255	255	255	0	8 host bits = 254 addresses
/16 Subnet Mask	255	255	0	0	16 host bits = 65,534 addresses
/20 Subnet Mask	255	255	0	0	12 host bits = 4094 addresses

First Address	Last Address
192.168.0.1	192.168.0.254

First Address	Last Address
192.168.0.1	192.168.255.254

First Address	Last Address
192.168.0.1	192.168.15.254

Classless Interdomain Routing (CIDR) uses **variable length subnets masks** (VLSM)

DigitalCloud TRAINING

SUBSCRIBE

Amazon Virtual Private Cloud (VPC)

A **VPC** is a logically isolated portion of the AWS cloud within a region

Region

VPC

Availability Zone

Public subnet

EC2 Instance

Subnets are created within **AZs**

The **VPC router** takes care of routing within the VPC and outside of the VPC

Router

Internet gateway

Availability Zone

Private subnet

EC2 Instance

You can launch **EC2 instances** into your VPC subnets

An **Internet Gateway** is attached to a VPC and used to connect to the Internet

Main Route Table

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

The **route table** is used to configure the VPC router

DigitalCloud TRAINING

Amazon VPC

Each **VPC** has a different block of IP addresses

CIDR stands for Classless Interdomain Routing

Region

VPC

CIDR 10.0.0.0/16

Availability Zone

Public subnet

10.0.0.0/24

Private subnet

10.0.2.0/24

Availability Zone

Public subnet

10.0.1.0/24

Private subnet

10.0.3.0/24

VPC

CIDR 10.1.0.0/16

Availability Zone

Public subnet

10.1.0.0/24

Private subnet

10.1.3.0/24

Availability Zone

Public subnet

10.1.2.0/24

Private subnet

10.1.4.0/24

Each subnet has a block of **IP addresses** from the CIDR block

You can create **multiple VPCs** within each region

DigitalCloud TRAINING

Amazon VPC Components

VPC Component	What it is
Virtual Private Cloud (VPC)	A logically isolated virtual network in the AWS cloud
Subnet	A segment of a VPC's IP address range where you can place groups of isolated resources
Internet Gateway/Egress-only Internet Gateway	The Amazon VPC side of a connection to the public Internet for IPv4/IPv6
Router	Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets
Peering Connection	Direct connection between two VPCs
VPC Endpoints	Private connection to public AWS services
NAT Instance	Enables Internet access for EC2 instances in private subnets managed by you)
NAT Gateway	Enables Internet access for EC2 instances in private subnets (managed by AWS)
Virtual Private Gateway	The Amazon VPC side of a Virtual Private Network (VPN) connection
Customer Gateway	Customer side of a VPN connection
AWS Direct Connect	High speed, high bandwidth, private network connection from customer to aws
Security Group	Instance-level firewall
Network ACL	Subnet-level firewall

Amazon VPC Core Knowledge

- A virtual private cloud (VPC) is a virtual network dedicated to your AWS account
- Analogous to having your own data center inside AWS
- It is logically isolated from other virtual networks in the AWS Cloud
- Provides complete control over the virtual networking environment including selection of IP ranges, creation of subnets, and configuration of route tables and gateways
- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC

Amazon VPC Core Knowledge

- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16
- A VPC spans all the Availability Zones in the region
- You have full control over who has access to the AWS resources inside your VPC
- By default you can create up to 5 VPCs per region
- A default VPC is created in each region with a subnet in each AZ

Defining VPC CIDR Blocks

DigitalCloud TRAINING

SUBSCRIBE

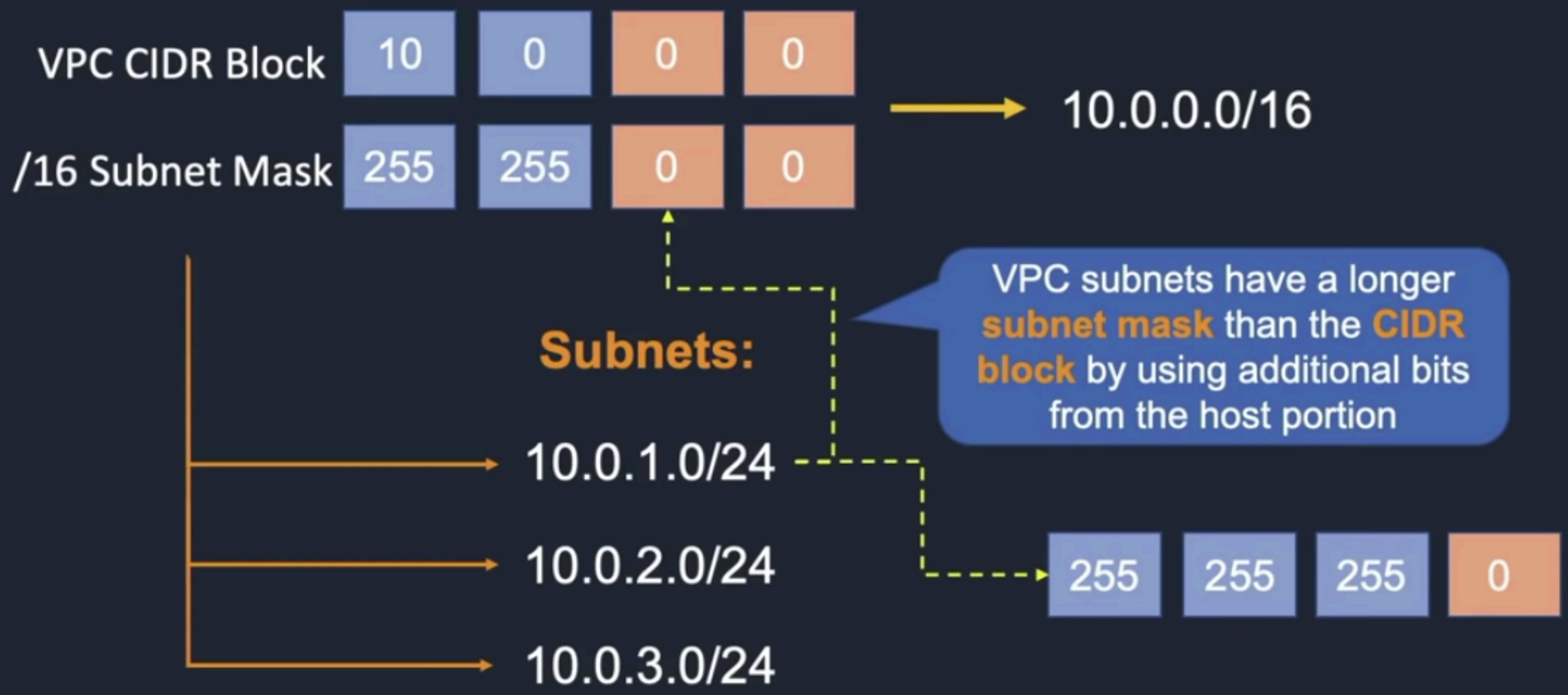
Rules and Guidelines

- CIDR block size can be between /16 and /28
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC
- You cannot increase or decrease the size of an existing CIDR block
- The first four and last IP address are not available for use
- AWS recommend you use CIDR blocks from the RFC 1918 ranges:

RFC 1918 Range	Example CIDR Block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20

DigitalCloud TRAINING

VPC CIDR Blocks and Subnets



DigitalCloud TRAINING

SUBSCRIBE

Additional Considerations

- Ensure you have enough networks and hosts
- **Bigger CIDR blocks** are typically better (more flexibility)
- **Smaller subnets** are OK for most use cases
- Consider deploying application tiers per subnet
- Split your HA resources across subnets in different AZs
- VPC Peering requires non-overlapping CIDR blocks
  - This is across all VPCs in all Regions / accounts you want to connect
- **Avoid overlapping CIDR blocks** as much as possible!

Example VPC CIDR Block and Subnets

VPC CIDR Block	10	0	0	0
/16 Subnet Mask	255	255	0	0

Subnet Name	IPv4 CIDR block	Availability Zone	Route Table	Auto-assign Public IP v4
private-1a	10.0.0.0/24	us-east-1a	Private-RT	No
private-1b	10.0.1.0/24	us-east-1b	Private-RT	No
private-1c	10.0.2.0/24	us-east-1c	Private-RT	No
public-1a	10.0.3.0/24	us-east-1a	MAIN	Yes
public-1b	10.0.4.0/24	us-east-1b	MAIN	Yes
public-1c	10.0.5.0/24	us-east-1c	MAIN	Yes

IPv4 Subnet Creator

About this tool

Enter base network

Network Address 10.0.0.0 Subnet Mask 255.255.0.0 (/16) [65536

Enter required no. of subnets or hosts

No. of subnets

Max subnets: 65536, all /32s

No. of hosts 254

Max hosts: 65536

CREATE

Network Tools

Other tools which you may like

IPv4 Address Planner IPv6 Address Planner IPv6 Tools
Cisco Config Comparison Tool Cisco Routing Table Comparison Tool

Network: 10.0.0.0/16

Summary of created subnets	
Total subnets	256 (8 bits)
Total IPs per subnet	256 (8 bits)
Subnet/Network Mask	255.255.255.0
Wildcard/Host Mask	0.0.0.255

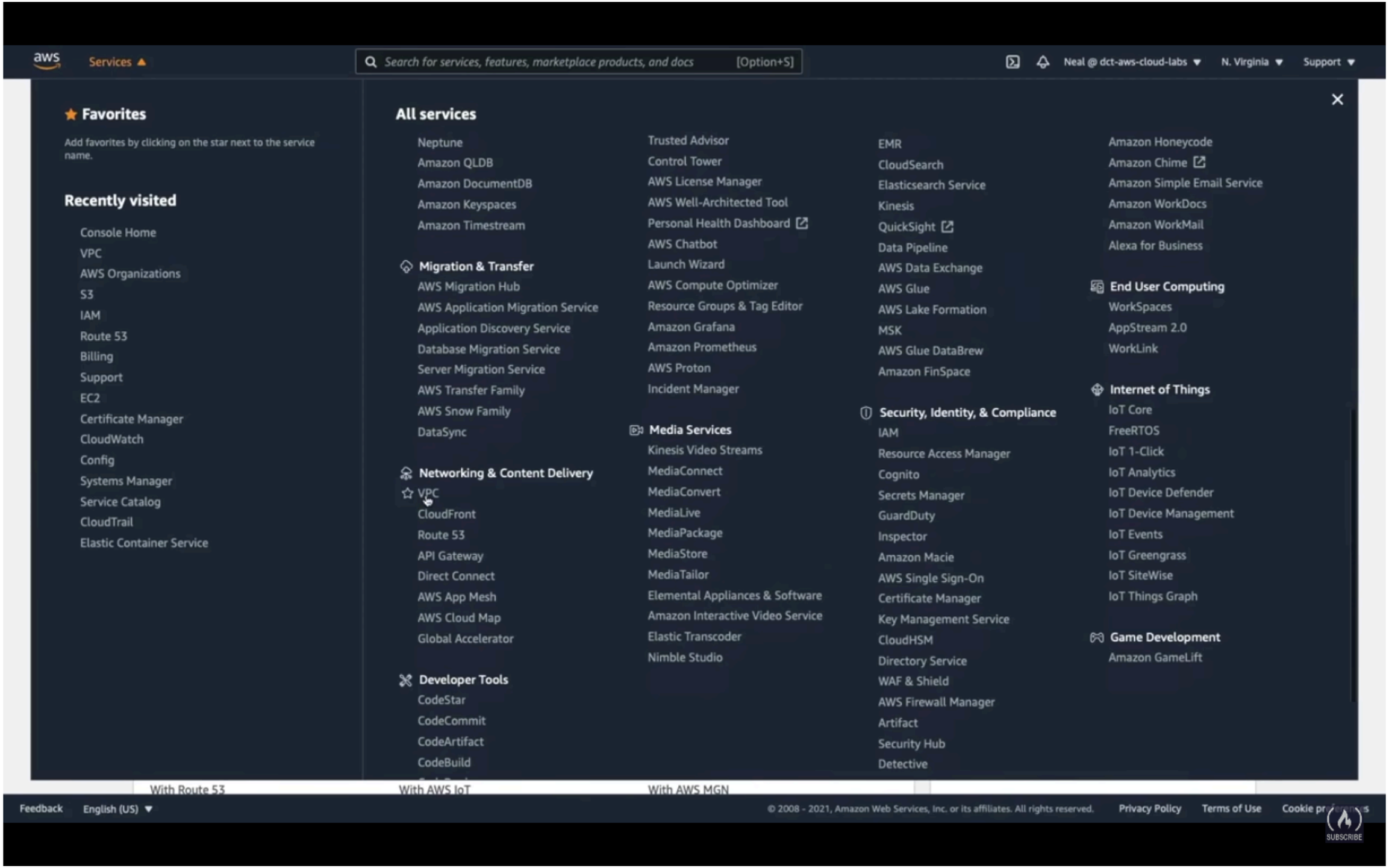
Showing first 1024 subnets only. Total subnets: 256

237	10.0.237.0/24	10.0.237.1	10.0.237.254	10.0.237.255	254
238	10.0.238.0/24	10.0.238.1	10.0.238.254	10.0.238.255	254
239	10.0.239.0/24	10.0.239.1	10.0.239.254	10.0.239.255	254
240	10.0.240.0/24	10.0.240.1	10.0.240.254	10.0.240.255	254
241	10.0.241.0/24	10.0.241.1	10.0.241.254	10.0.241.255	254
242	10.0.242.0/24	10.0.242.1	10.0.242.254	10.0.242.255	254
243	10.0.243.0/24	10.0.243.1	10.0.243.254	10.0.243.255	254
244	10.0.244.0/24	10.0.244.1	10.0.244.254	10.0.244.255	254
245	10.0.245.0/24	10.0.245.1	10.0.245.254	10.0.245.255	254
246	10.0.246.0/24	10.0.246.1	10.0.246.254	10.0.246.255	254
247	10.0.247.0/24	10.0.247.1	10.0.247.254	10.0.247.255	254
248	10.0.248.0/24	10.0.248.1	10.0.248.254	10.0.248.255	254
249	10.0.249.0/24	10.0.249.1	10.0.249.254	10.0.249.255	254
250	10.0.250.0/24	10.0.250.1	10.0.250.254	10.0.250.255	254
251	10.0.251.0/24	10.0.251.1	10.0.251.254	10.0.251.255	254
252	10.0.252.0/24	10.0.252.1	10.0.252.254	10.0.252.255	254
253	10.0.253.0/24	10.0.253.1	10.0.253.254	10.0.253.255	254
254	10.0.254.0/24	10.0.254.1	10.0.254.254	10.0.254.255	254
255	10.0.255.0/24	10.0.255.1	10.0.255.254	10.0.255.255	254

VPC Wizard

DigitalCloud TRAINING

SUBSCRIBE


aws
Services
Search for services, features, marketplace products, and docs [Option+S]
Neal @ dct-aws-cloud-labs
N. Virginia
Support
Favorites
Add favorites by clicking on the star next to the service name.
Recently visited
Console Home
VPC
AWS Organizations
S3
IAM
Route 53
Billing
Support
EC2
Certificate Manager
CloudWatch
Config
Systems Manager
Service Catalog
CloudTrail
Elastic Container Service
All services
Neptune
Amazon QLDB
Amazon DocumentDB
Amazon Keyspaces
Amazon Timestream
Migration & Transfer
AWS Migration Hub
AWS Application Migration Service
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer Family
AWS Snow Family
DataSync
Networking & Content Delivery
VPC
CloudFront
Route 53
API Gateway
Direct Connect
AWS App Mesh
AWS Cloud Map
Global Accelerator
Developer Tools
CodeStar
CodeCommit
CodeArtifact
CodeBuild
Trusted Advisor
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard
AWS Chatbot
Launch Wizard
AWS Compute Optimizer
Resource Groups & Tag Editor
Amazon Grafana
Amazon Prometheus
AWS Proton
Incident Manager
Media Services
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage
MediaStore
MediaTailor
Elemental Appliances & Software
Amazon Interactive Video Service
Elastic Transcoder
Nimble Studio
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Data Exchange
AWS Glue
AWS Lake Formation
MSK
AWS Glue DataBrew
Amazon FinSpace
Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
AWS Firewall Manager
Artifact
Security Hub
Detective
Amazon Honeycode
Amazon Chime
Amazon Simple Email Service
Amazon WorkDocs
Amazon WorkMail
Alexa for Business
End User Computing
WorkSpaces
AppStream 2.0
WorkLink
Internet of Things
IoT Core
FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise
IoT Things Graph
Game Development
Amazon GameLift
With Route 53
With AWS IoT
With AWS MGN
Feedback
English (US)
© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
SUBSCRIBE