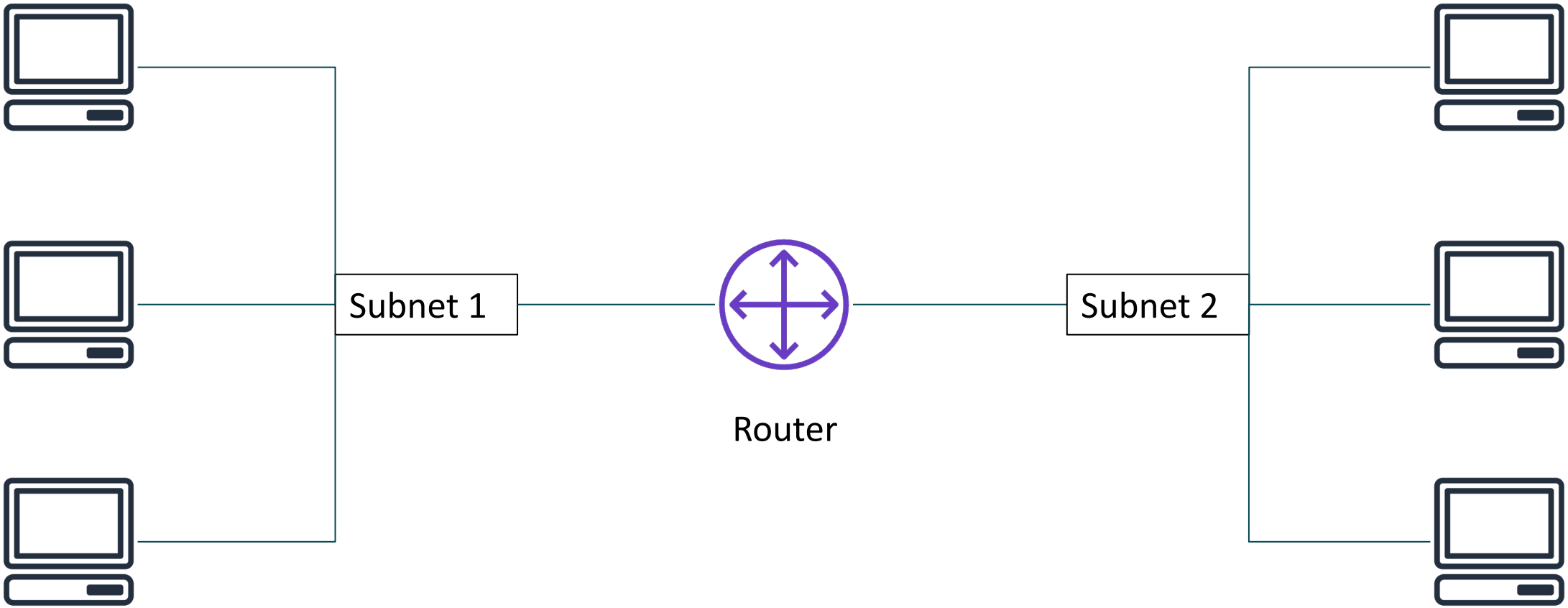
Module 5: Networking and Content Delivery

AWS Academy Cloud Foundations

Networks

→ Public and Private Cloud IaaS model allows you to customize your network



IP addresses

IPv4 addr are 32-bit and uses 4-octets and is represented as a positive integer

192 . 0 . 2 . 0

11000000 00000000 00000010 00000000

IPv4 and IPv6 addresses

-> IPv6 addr are 128-bit and uses 8-hextets (16-bit) and is represented as 4-nibbles or hexadecimal

IPv4 (32-bit) address: 192.0.2.0

IPv6 (128-bit) address: 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

Classless Inter-Domain Routing (CIDR)

→ the subnet mask or prefix length is used to identify the Network and Host portions of an IP address

Network identifier (routing prefix)				Host identifier		
192	. 0	. 2	.	0	/	24
11000000	00000000	00000010		00000000 to 11111111		Tells you how many bits are fixed
Fixed	Fixed	Fixed		Flexible		

Open Systems Interconnection (OSI) model

OSI is a generic model for comms
→ TCP/IP is the model we use for our computers

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)

Network Services

Section 2: Amazon VPC

Module 5: Networking and Content Delivery

Amazon VPC

→ Each account in the cloud is logically separated and isolated from other accounts

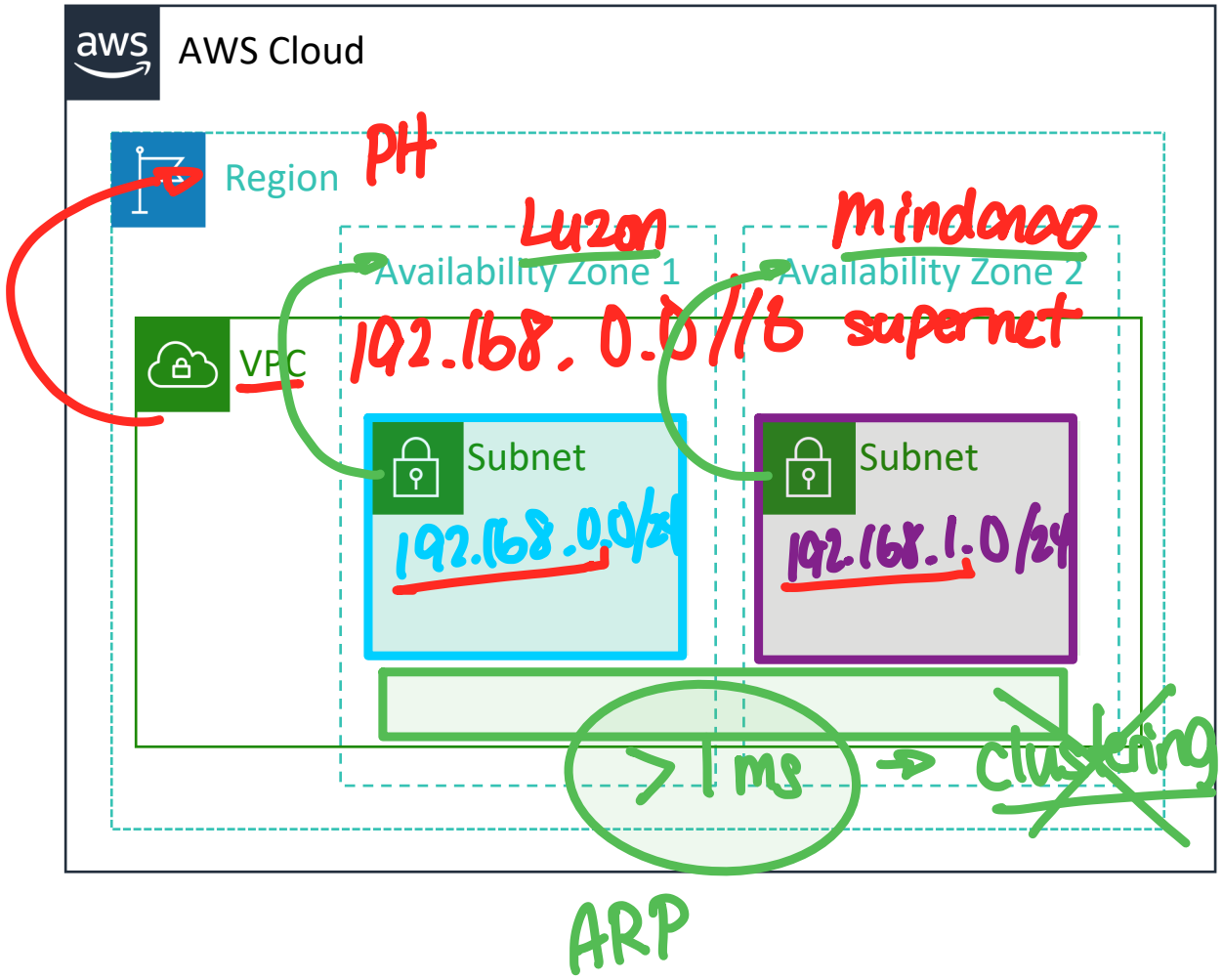
Amazon VPC

- Enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define
- Gives you control over your virtual networking resources, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways
- Enables you to customize the network configuration for your VPC
- Enables you to use multiple layers of security

for laas

VPCs and subnets

- VPCs:
  - Logically isolated from other VPCs
  - Dedicated to your AWS account
  - Belong to a single AWS Region and can span multiple Availability Zones
- Subnets: → network segments
  - Range of IP addresses that divide a VPC
  - Belong to a single Availability Zone
  - Classified as public or private



IP addressing

→ You choose the size of your Private Network

- When you create a VPC, you assign it to an IPv4 CIDR block (range of private IPv4 addresses).
- You cannot change the address range after you create the VPC.
- The largest IPv4 CIDR block size is /16.
- The smallest IPv4 CIDR block size is /28.
- IPv6 is also supported (with a different block size limit).
- CIDR blocks of subnets cannot overlap.

VPC

→ larger = more addr for your machines

x.x.x.x/16 or 65,536 addresses (max)

to

x.x.x.x/28 or 16 addresses (min)

→ smaller = less addr

Host bits

netbits host

PL

net bits

32bit −/16 = 2^16 = 65k

32bit −/28 = 2^4 = 16 addr

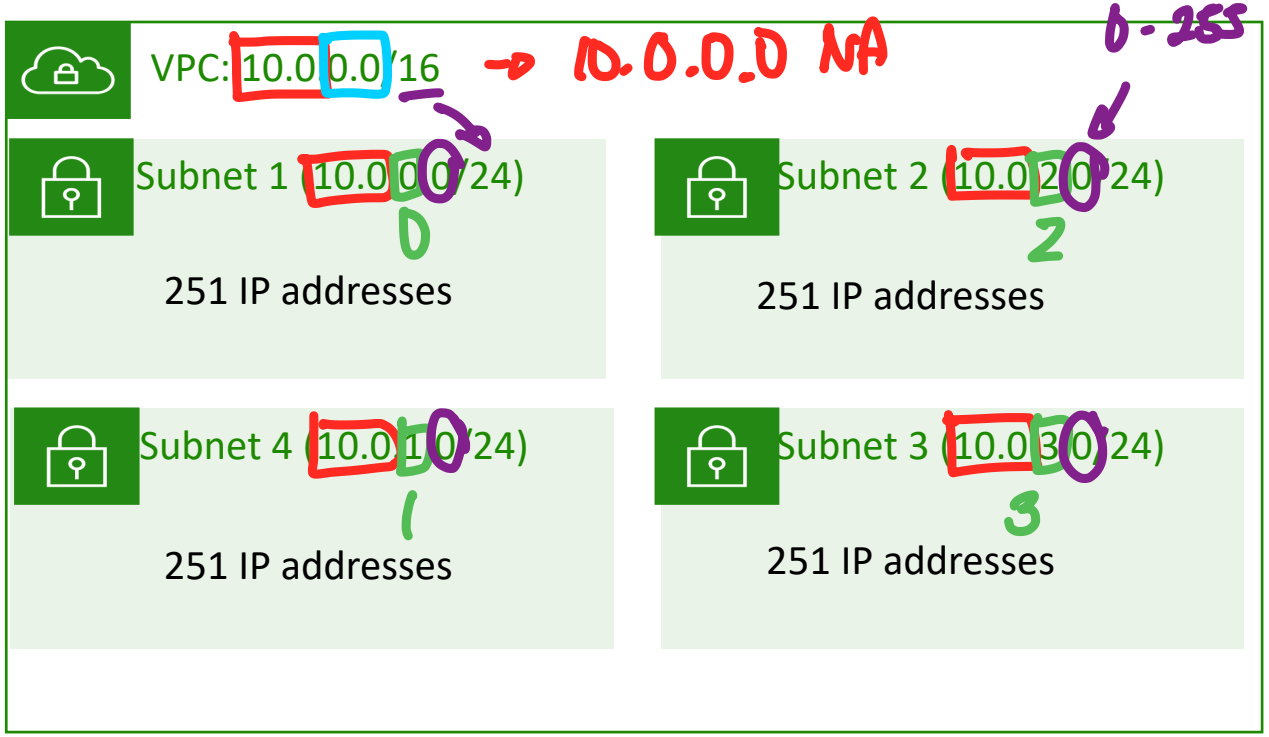
Reserved IP addresses

→ You need to consider an allowance for reserved addresses when you decide on a block

Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.

4 - 254 usable

0 - 255



IP Addresses for CIDR block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

Public IP address types → Public Cloud = Internet Access

Public IPv4 address temporary

- Manually assigned through an Elastic IP address
- Automatically assigned through the auto-assign public IP address settings at the subnet level

→ addr can change if you reboot your server or turn it off

Instance

no Public Service

Elastic IP address

- Associated with an AWS account
- Can be allocated and remapped anytime
- Additional costs might apply

→ addr is semi-permanent but you pay for a reservation cost if you use it or not

Account

✓ Public Service

Route tables and routes → used by the Network Services to route traffic between networks

- A route table contains a set of rules (or routes) that you can configure to direct network traffic from your subnet.
- Each route specifies a destination and a target.
- By default, every route table contains a local route for communication within the VPC.
- Each subnet must be associated with a route table (at most one).

Main (Default) Route Table

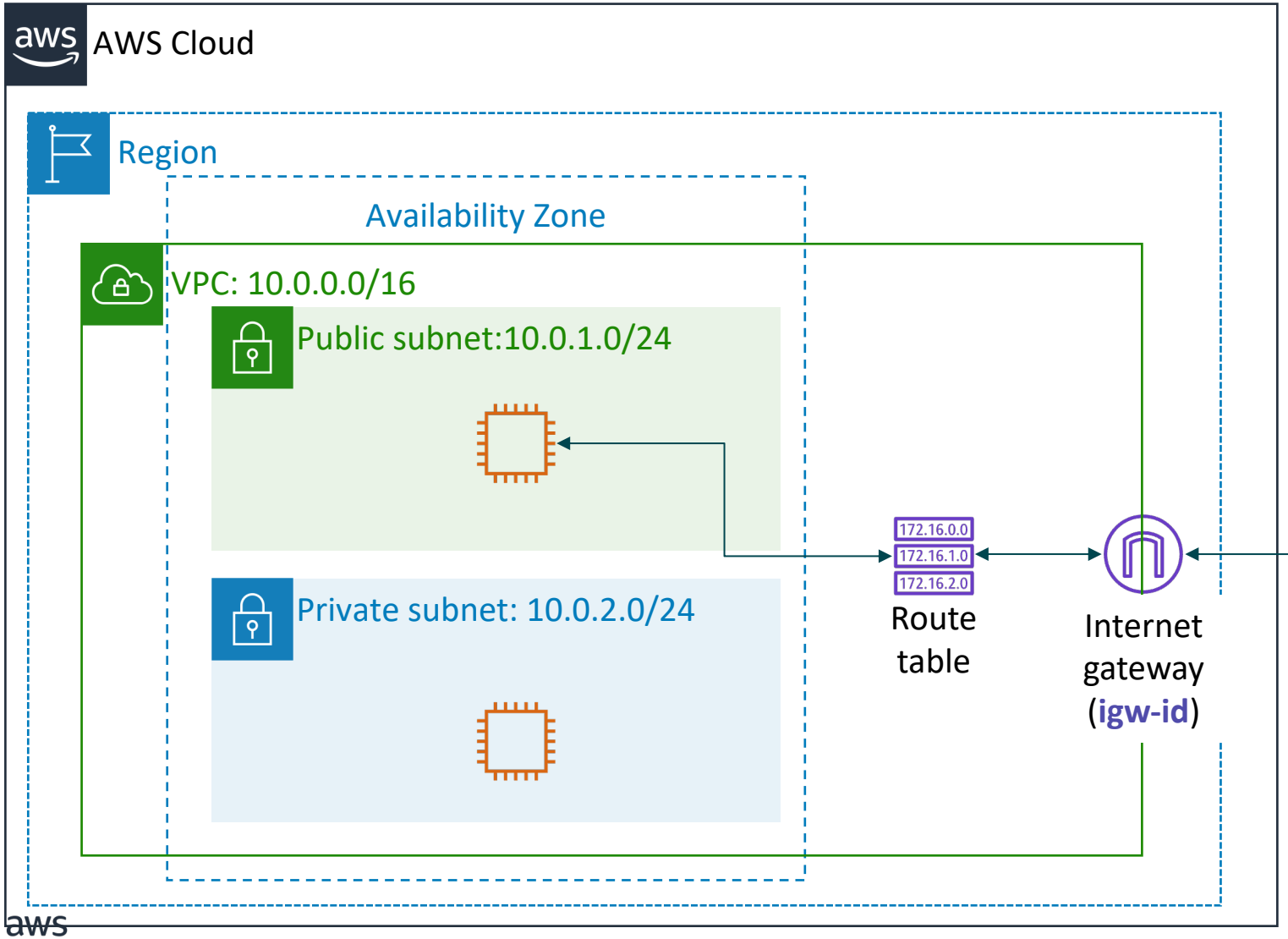
Destination	Target
10.0.0.0/16	local

VPC CIDR block

Section 3: VPC networking

Module 5: Networking and Content Delivery

Internet gateway



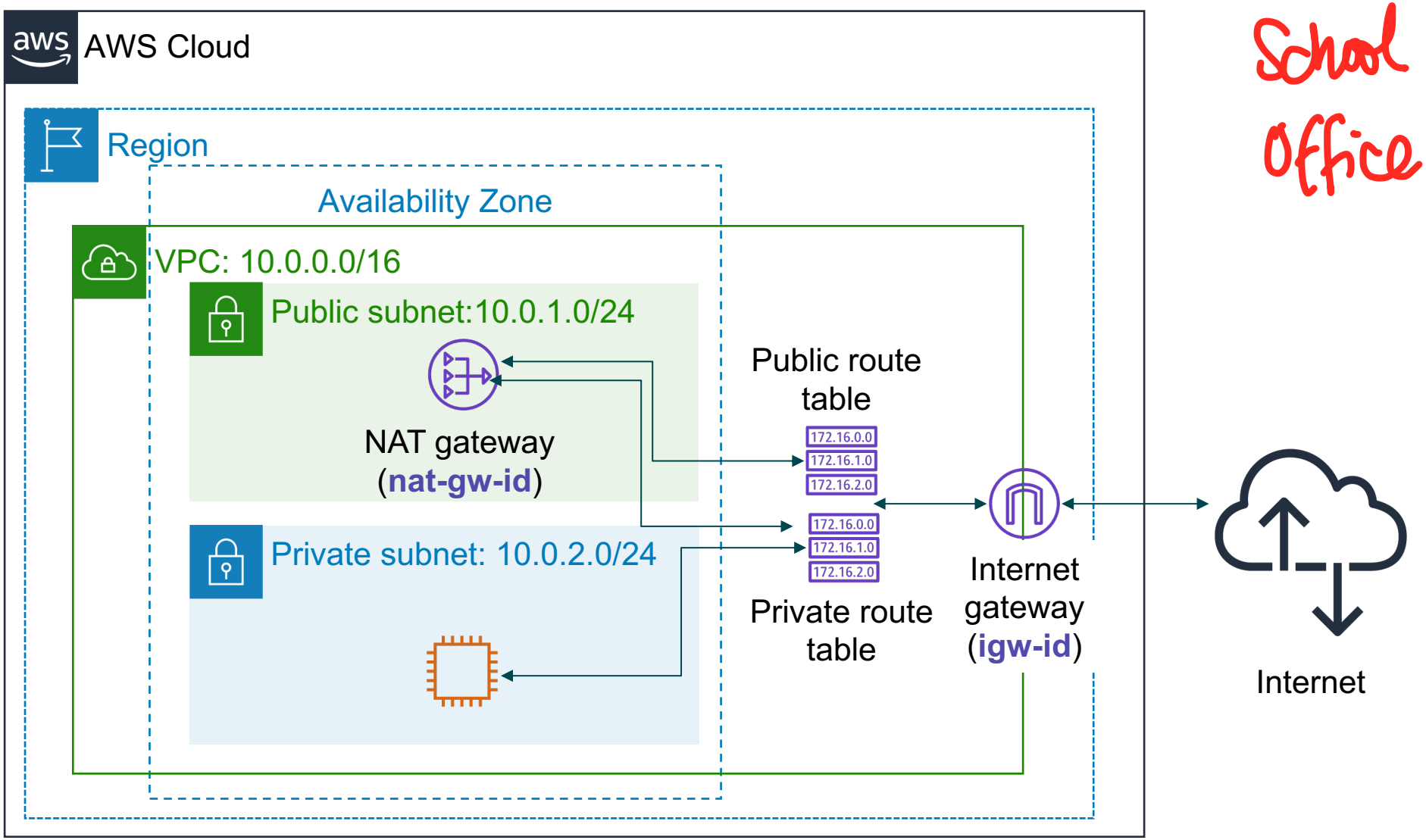
Public Subnet Route Table

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

any IP

Network address translation (NAT) gateway

Private
House
School
Office
→ Public



Public Subnet Route Table

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

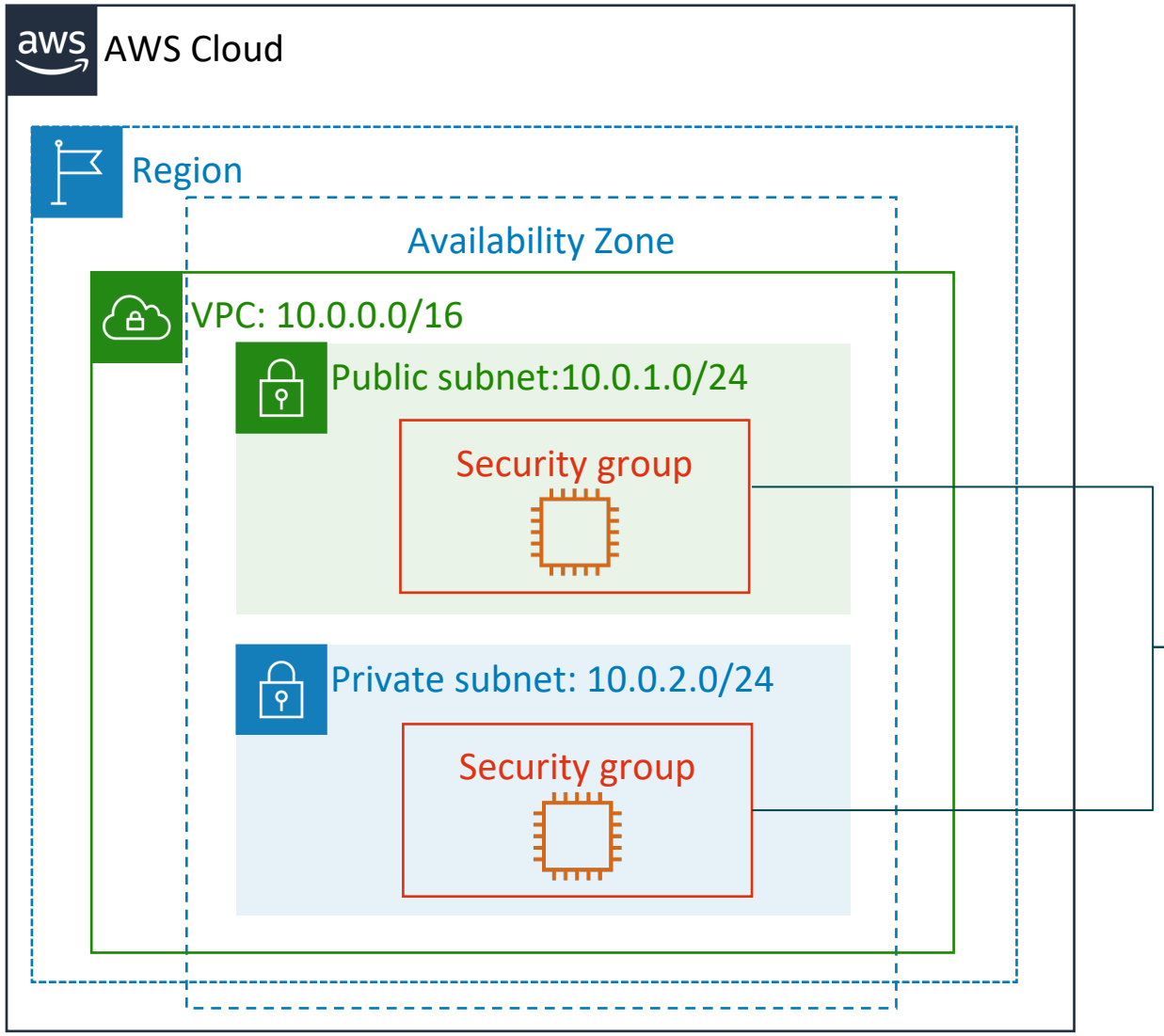
Private Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Section 4: VPC security

Module 5: Networking and Content Delivery

Security groups (1 of 2)



Host-based FW

Security groups act at the instance level.

↳ Compute/resource

Security groups (2 of 2)

origin comes from outside

- Security groups have rules that control inbound and outbound instance traffic.
- Default security groups deny all inbound traffic and allow all outbound traffic.
- Security groups are stateful. → looks at the src of the msg

Inbound			
Source	**Protocol**	**Port Range**	**Description**
sg-*xxxxxxxx*	All	All	Allow inbound traffic from network interfaces assigned to the same security group.

Outbound			
Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

Custom security group examples

default deny

- You can **specify allow** rules, but not deny rules.
- **All rules are evaluated** before the decision to allow traffic.

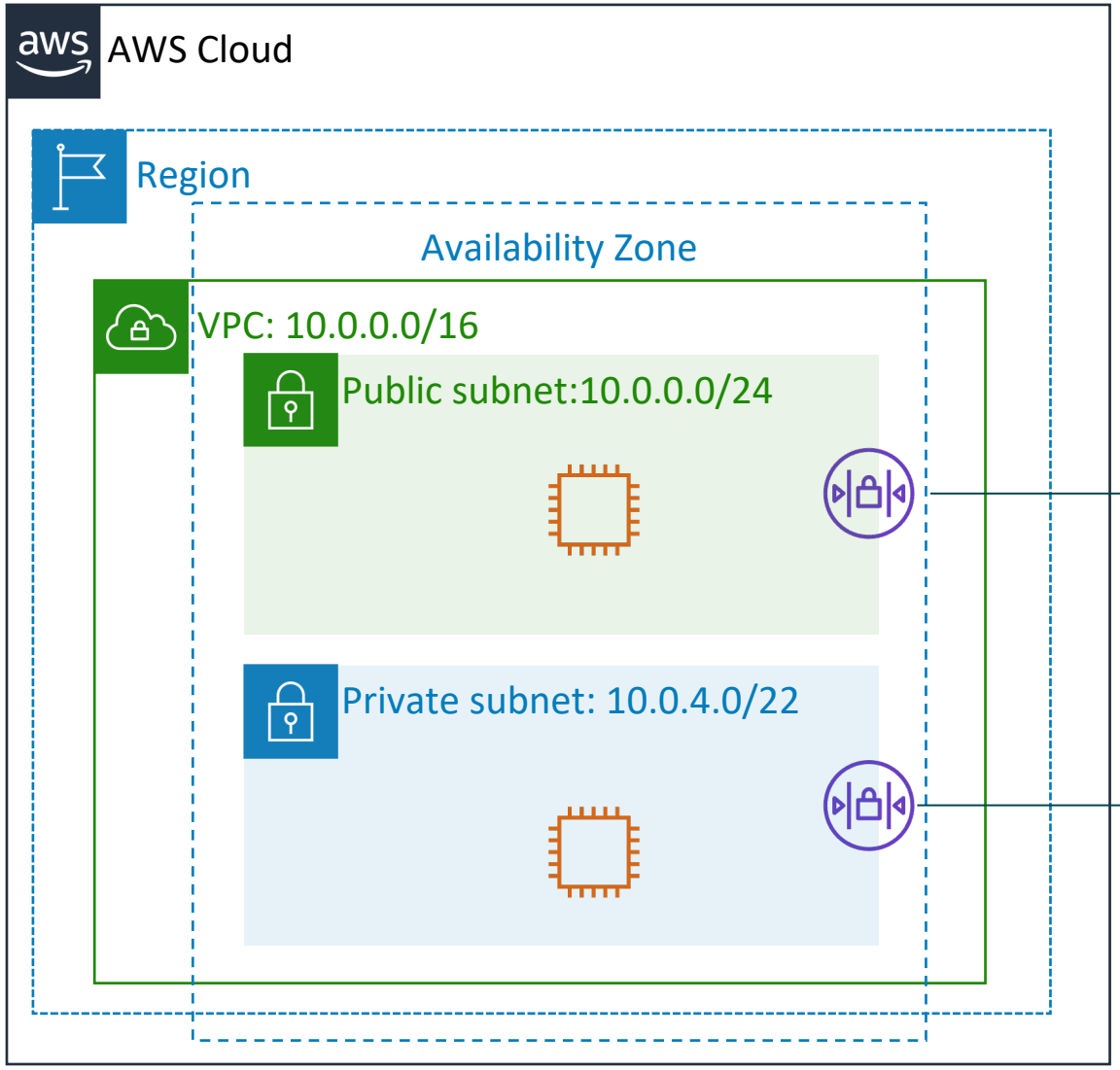
Inbound			
Source	**Protocol**	**Port Range**	**Description**
Any IP 0.0.0.0/0 Internet	TCP	80	Allow inbound HTTP access from all IPv4 addresses
Any IP 0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
Your network's public IPv4 address range House/office IP	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)

web

remote access

Outbound			
Destination	Protocol	Port Range	Description
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group

Network access control lists (network ACLs 1 of 2)



network Firewalls

Network ACLs act at the **subnet level**.

Network access control lists (network ACLs 2 of 2)

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Default network ACLs allow all inbound and outbound IPv4 traffic.
- Network ACLs are stateless.

Inbound					
Rule	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	**Type**	**Protocol**	**Port Range**	**Destination**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Custom network ACLs examples

- **Custom** network ACLs **deny** all inbound and outbound traffic until you add rules.
- You can specify **both allow and deny** rules.
- Rules are evaluated in number order, starting with the **lowest number**.

Inbound					
Rule	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Web
config/access
Any IP
House/office IP

Outbound					
Rule	**Type**	**Protocol**	**Port Range**	**Destination**	**Allow/Deny**
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Any

Security groups versus network ACLs

Attribute	Security Groups	Network ACLs
Scope	Instance level Host-based FW	Subnet level Net FW
Supported Rules	Allow rules only Deny by defaut	Allow and deny rules
State	Stateful (return traffic is automatically allowed, regardless of rules)	Stateless (return traffic must be explicitly allowed by rules)
Order of Rules	All rules are evaluated before decision to allow traffic	Rules are evaluated in number order before decision to allow traffic

DNS

Section 5: Amazon Route 53

Module 5: Networking and Content Delivery

name → address

Amazon Route 53 → port num of DNS

Amazon Route 53

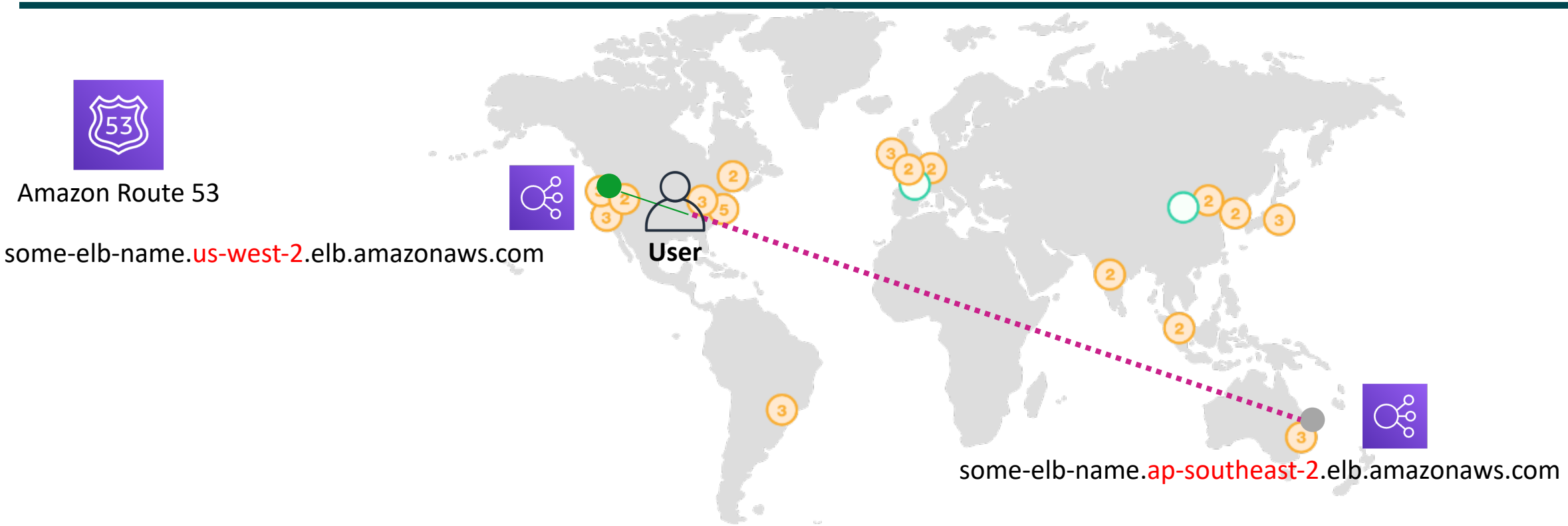
- Is a highly available and scalable Domain Name System (DNS) web service
- Is used to route end users to internet applications by translating names (like *www.example.com*) into numeric IP addresses (like *192.0.2.1*) that computers use to connect to each other
- Is fully compliant with IPv4 and IPv6
- Connects user requests to infrastructure running in AWS and also outside of AWS
- Is used to check the health of your resources
- Features traffic flow
- Enables you to register domain names

Amazon Route 53 supported routing

- Simple routing – Use in single-server environments
- Weighted round robin routing – Assign weights to resource record sets to specify the frequency

  multi-server
- Latency routing – Help improve your global applications
- Geolocation routing – Route traffic based on location of your users
- Geoproximity routing – Route traffic based on location of your resources
- Failover routing – Fail over to a backup site if your primary site becomes unreachable
- Multivalue answer routing – Respond to DNS queries with up to eight healthy records selected at random

Use case: Multi-region deployment



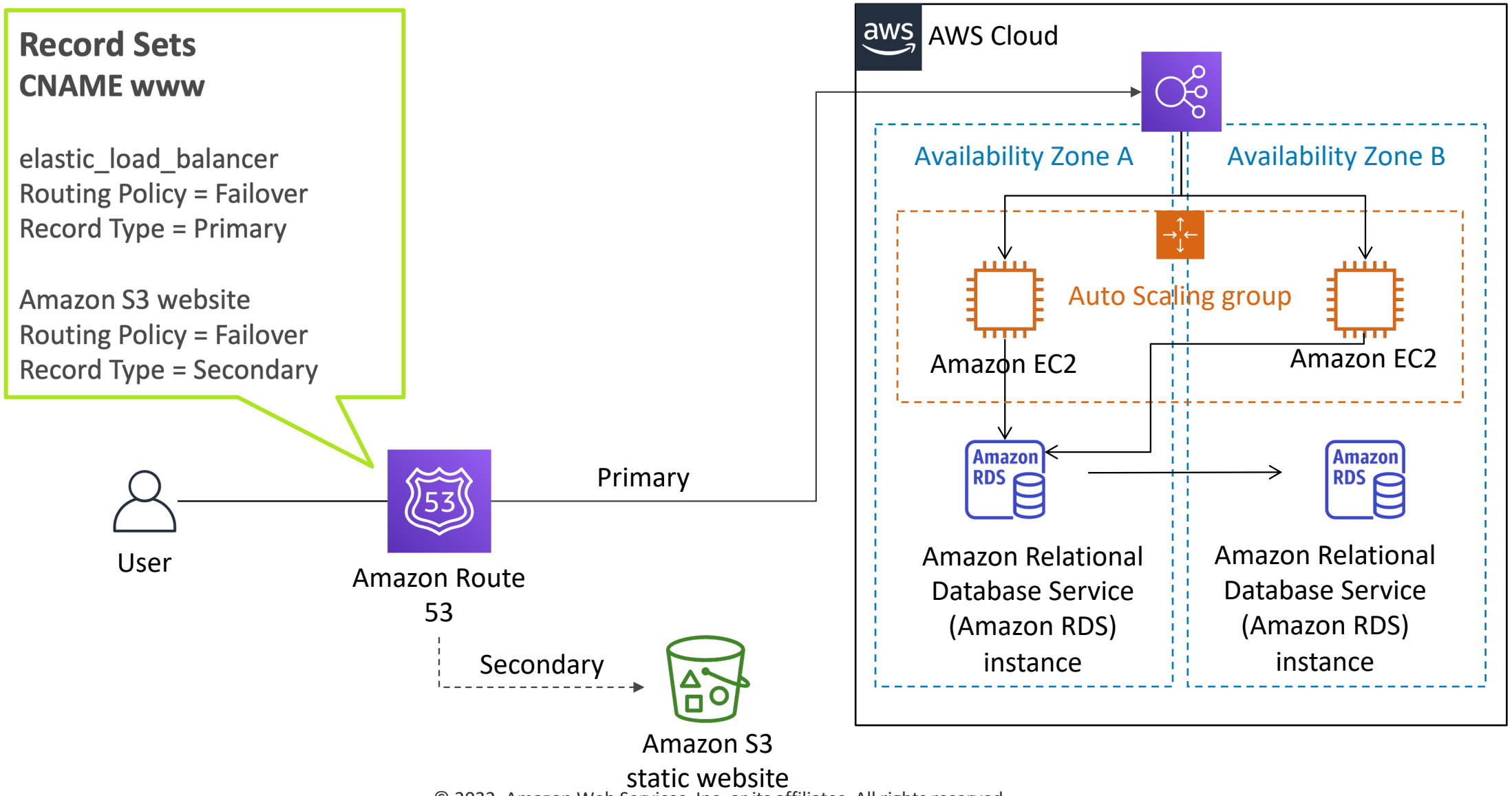
Name	Type	Value
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

Amazon Route 53 DNS failover

Improve the availability of your applications that run on AWS by:

- Configuring backup and failover scenarios for your own applications
- Enabling highly available multi-region architectures on AWS
- Creating health checks

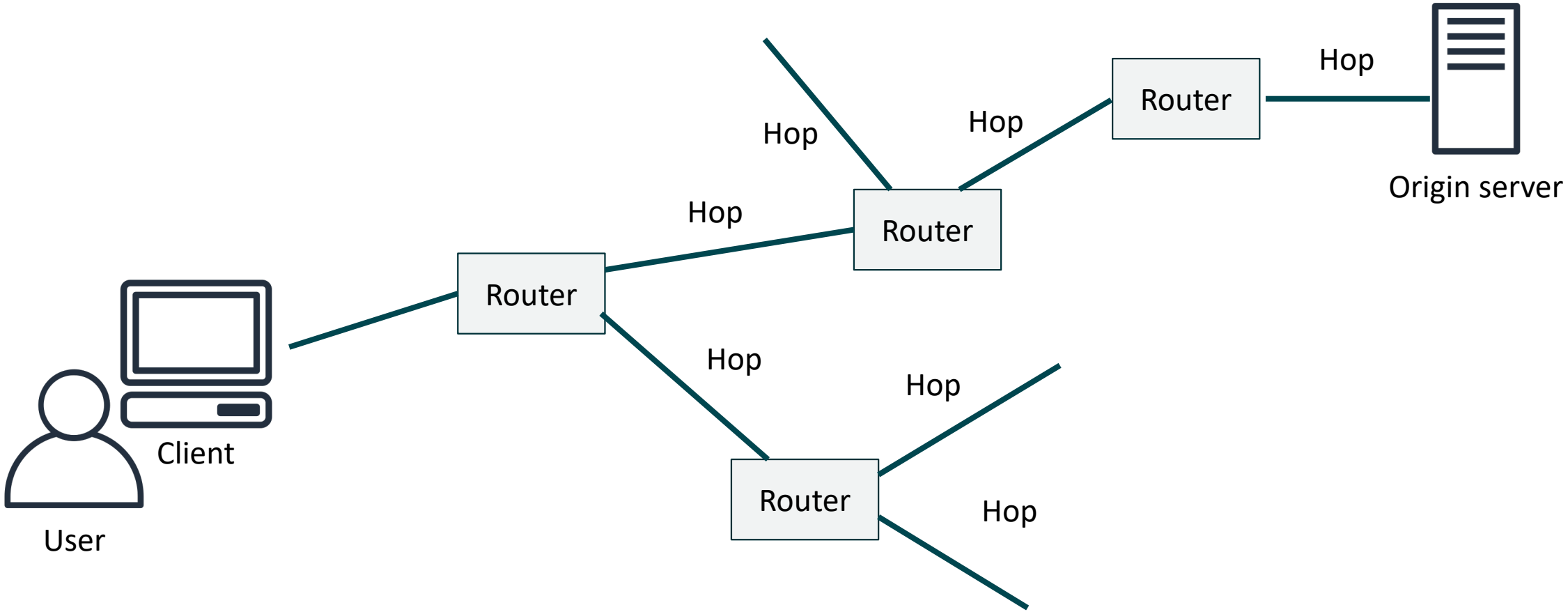
DNS failover for a multi-tiered web application



Section 6: Amazon CloudFront

Module 5: Networking and Content Delivery

Content delivery and network latency

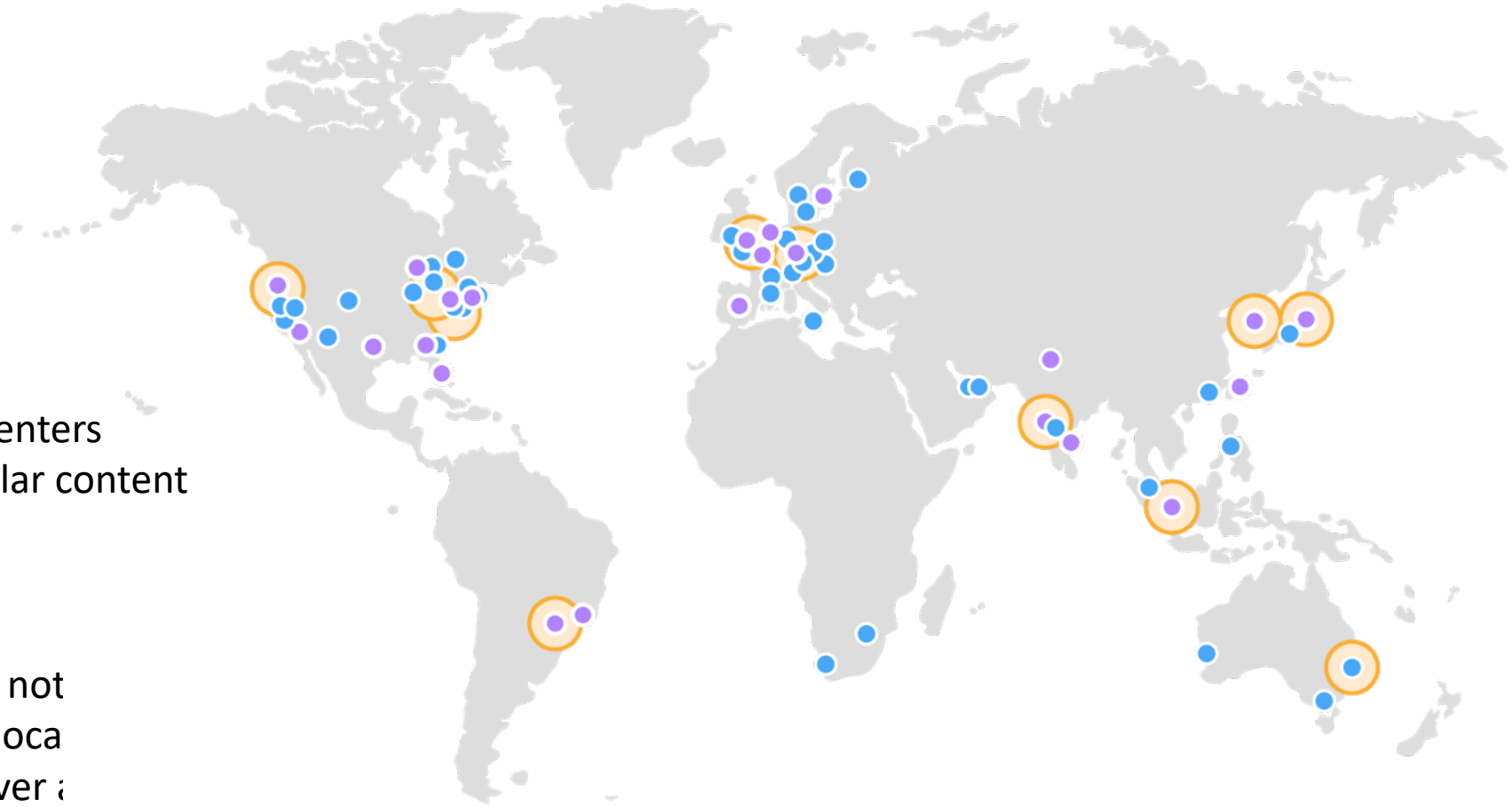


Content delivery network (CDN)

- Is a globally distributed system of caching servers
- Caches copies of commonly requested files (static content)
- Delivers a local copy of the requested content from a nearby cache edge or Point of Presence
- Accelerates delivery of dynamic content
- Improves application performance and scaling

Amazon CloudFront infrastructure

- Edge locations
- Multiple edge locations
- Regional edge caches



- **Edge locations –** Network of data centers that CloudFront uses to serve popular content quickly to customers.

- **Regional edge cache –** CloudFront location that caches content that is not popular enough to stay at an edge loca It is located between the origin server a the global edge location.

Amazon CloudFront benefits

- Fast and global
- Security at the edge
- Highly programmable
- Deeply integrated with AWS
- Cost-effective