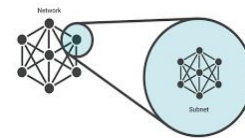# EXPLORE | DIGITAL SKILLS

Networking and Content Delivery

Train Overview

This train will explore the **basics of networking**, how **networking** works **with AWS**, and understand the use of **Domain Name System** and **Content Delivery Network services.**

Basics of Networking	➢ What is networking? ➢ How do computers communicate? ➢ Information on IP Addresses

Networking with AWS	➢ Why should I use Amazon VPC? ➢ The main components of Amazon VPC ➢ Amazon VPC security

DNS and CDN services	➢ What is a Domain Name System service? ➢ Amazon Route 53 ➢ What is a Content Delivery Network? ➢ Amazon CloudFront

Networking Basics

The Fundamentals of Networking in AWS

DNS Service and Content Delivery with AWS

Conclusion

What is networking?

A computer network, also known as a data network, is a **group** of **computing devices linked** to each other. This enables **communication** between the devices, allowing the sharing of data, resources and applications. **Networking** is the whole process of creating and using computer networks.

Computer Network Types

There are many different types of computer networks, the main ones being:
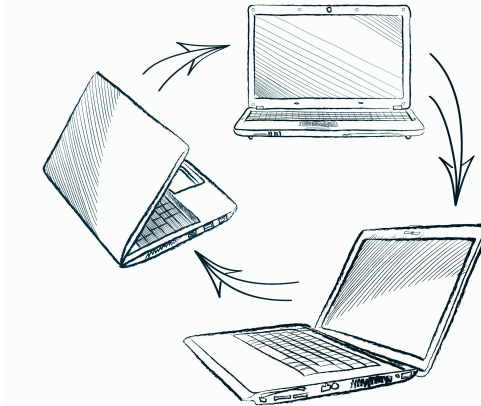
LAN = local area network
PAN = personal area network
MAN = metropolitan area network
WAN = wide area network

Another common network is a VPN. A **virtual private network** (VPN) connects remote users or sites together over an encrypted public connection.

For more information read **here**.

Computer Network Components

A computer network has both hardware and software components.

Hardware Components are servers, clients, peers, transmission media and connecting devices such as routers and gateways.

Software Components are networking operating systems and protocol suites. Common protocol suites are OSI and TCP/IP models.

For a more in depth explanation read here.

How do computers communicate?

The following components are required for computers to communicate:

All over the world, computers are connected via the **internet**.

→

The internet is a vast network that allows people to **communicate** from anywhere in the world.

→

Communication is possible as long as devices have an **internet connection**.

→

TCP/IP

Each device connected to the internet has a **unique identifier** and follows the ***TCP/IP protocol.**

→

The *TCP/IP protocol is a set of **standardized rules** for communication over the internet.

→

The unique identifier for each device is the **IP Address**.

*Transmission Control Protocol/Internet Protocol

Information on IP Addresses

There are two different versions for an IP address, **IPv4** and **IPv6**. Each one of these versions has its own **format** and **size**. IPv6 addresses will be used more in the future as IPv4 addresses will run out.

Format and size of IP addresses		

IPv4

- ★ A set of **4** numbers.
- ★ Numbers are separated by dots.
- ★ Each number has a *range of **0** to **255**.
- ★ Each number represents a maximum of **8** bits.
- ★ The total size of the address is **32** bits.

IPv4 address in dotted-decimal notation

172 . 16 . 254 . 1

↓ ↓ ↓ ↓

10101100 .00010000 .11111110 .00000001

8 bits

32 bits (4 bytes)
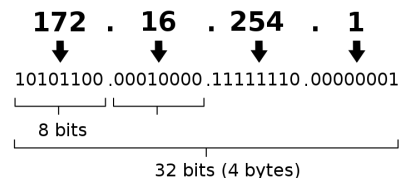
IPv6

- ★ A set of **8** groupings.
- ★ Groups are separated by colons.
- ★ Each group has **4** letters and numbers, ranging from **0** to **ffff**.
- ★ Each group represents a maximum of **16** bits.
- ★ The total size of the address is **128** bits.

IPv6 address

2001: 0db8 : 3902 : 00c2 : 0000 : 0000 : 0000 : fe04

∨ ∨ ∨

16 bits   16 bits

128 bits

*Some **IP address ranges** are reserved for specific purposes or **subnet** classes.
 A subnet is a smaller network of computers connected to a larger network and it makes routing more efficient.

EXPLORE || DIGITAL SKILLS

Why should I use Amazon VPC?

Amazon Virtual Private Cloud (VPC) allows you to create a virtual isolated network in the cloud.
In this network space you can define how your network and resources are exposed to the internet.
You will also have complete control over IP address ranges, subnets, route tables and network gateways.

Benefits of using Amazon VPC		
	Secure	• AWS VPC security groups and network ACLS act as firewalls. • You can configure rules for inbound and outbound traffic. • You can enable access control with an VPC endpoint.
	Simple	• An Amazon VPC can easily be created in the AWS Management Console or AWS CLI. • The Amazon VPC console wizard provides multiple options to create a VPC, you can select one suitable to your needs and customize it. • All components of the VPC are automatically created by the VPC wizard.
	Customisable	• Configure the Amazon VPC to fit your specific needs. • Choose your IP Address range and create your own subnet. • Configure route tables to available gateways.

EXPLORE | DIGITAL SKILLS
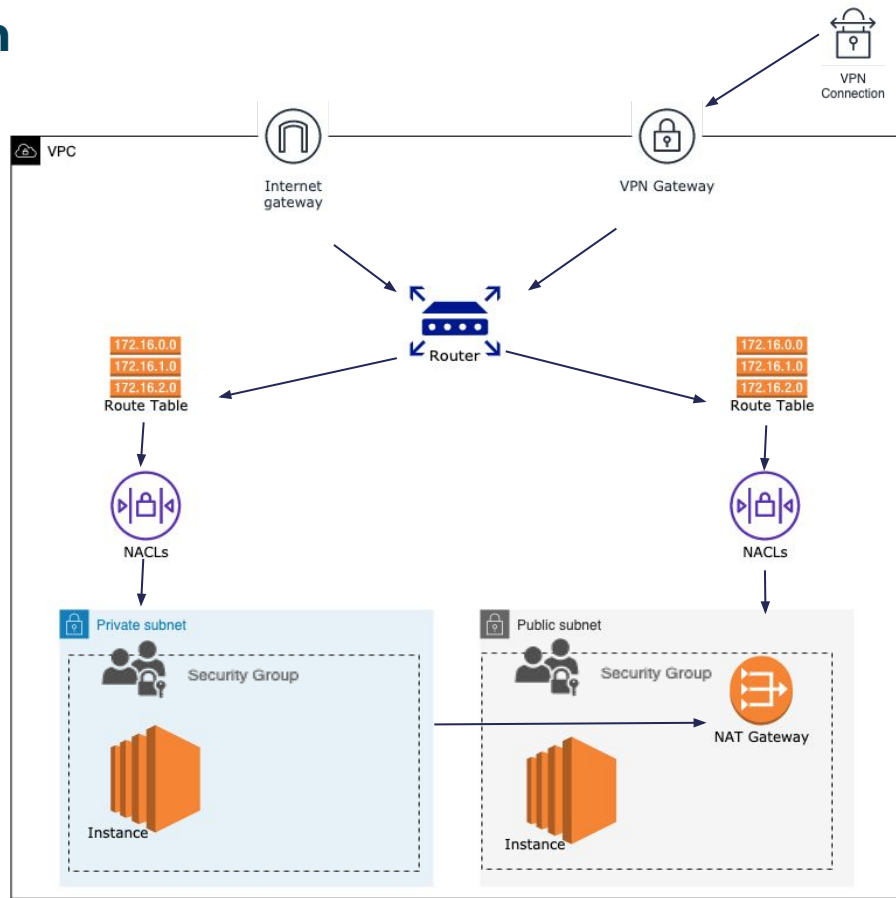
Amazon VPC ~ Architecture Diagram

An **architecture diagram** is a visual representation of the cloud services used for an application, and how they connect to each other. Here is an example of an architecture diagram, making up the main **components of an Amazon VPC**.

In the next part of this train you will learn:

- ❖ The difference between a public and private **Subnet**.
- ❖ How an **Internet** and **NAT gateway** allows or prevents traffic from the outside world.
- ❖ How a **Route table** controls traffic flow.
- ❖ How the security of a VPC is managed by **NACLs** and **Security Groups**.
- ❖ The reason for a **VPN connection** and **VPN gateway**.

More detail on how an architecture diagram works will be covered in one of the trains to follow.
Explore here for architecture diagram tools and toolkits.

VPN Connection

VPC

Internet gateway

VPN Gateway

172.16.0.0
172.16.1.0
172.16.2.0
Route Table

Router

172.16.0.0
172.16.1.0
172.16.2.0
Route Table

NACLs

NACLs

Private subnet

Security Group

Instance

Public subnet

Security Group

NAT Gateway

Instance

EXPLORE DIGITAL SKILLS
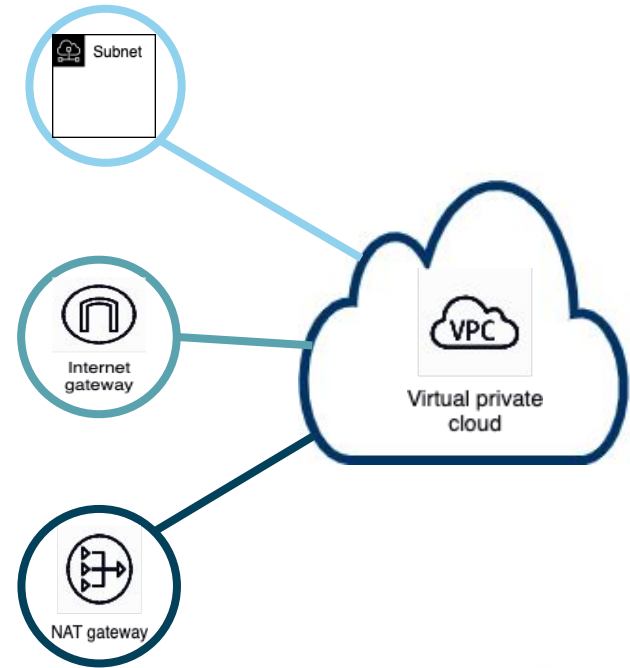
1) The main components of Amazon VPC

When setting up your Amazon VPC it is important to consider each of the following components and set it up accordingly. The first few components to consider: **Subnets**, an **Internet gateway** and a **NAT gateway**.

- Create separate **subnets** for different purposes.
- **Public** subnet - visible to the outside world - attach a public IP address.
- **Private** subnet - not publicly available - backend information you do not want visible.
- A subnet can only be defined in one **availability zone.**

- An **internet gateway** allows access to and from the outside world.
- It does not have an IP address and is **managed by AWS**.
- If you need to access your *AWS resources from anywhere they have to be in a public subnet, with a **route** defined to the internet gateway.

- Create a **NAT gateway** for AWS resources that can't be visible, but requires access to the outside world.
- Select the subnet for the gateway and **AWS will manage** the rest.
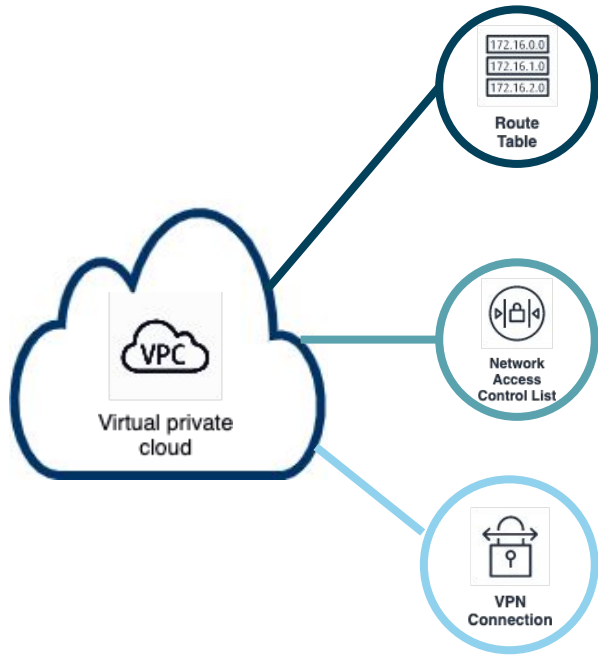- It **allows outbound** traffic but **limits inbound** access.

*Consider AWS resources to be a virtual machines/instances in this scenario.

2) The main components of Amazon VPC

The other components to consider are **Route Tables**, **Network Access Control Lists** and a **VPN Connection**.

All six components cannot be changed once your Amazon VPC is set up.

- For **access** to resources or networks **outside** your VPC **routing** is required.
- Traffic is routed through the **internet** or **NAT gateway**.
- **Route tables** control the flow of traffic and are connected to each of your subnets.

- **Network Access Control Lists (NACLs)** are for security in your VPC.
- It **limits inbound** and **outbound traffic** to specific instances or destinations.
- This allows for a **secure infrastructure** and protection against attacks.

- Use a **VPN Connection** to connect your on-premise infrastructure and VPC. A **VPN Gateway** allows traffic from a VPN Connection into your VPC.

EXPLORE DIGITAL SKILLS

Amazon VPC Security

There are two methods of securing virtual networks with AWS: **Security Groups** and **Network Access Control Lists (NACLs)**. These methods function as a **firewall** to protect your network and automatically get created with default settings upon the configuration of a VPC, but they have some **differences**.

Security Groups

NACLs

Security Groups	NACLs
A security group provides a set of inbound and outbound rules that controls traffic to and from EC2 **instances**.	A NACL controls traffic to and from a **subnet** based on a set of inbound and outbound rules.
Each security group can be applied to one or more instances and across subnets.	Each NACLS can be applied to one or more subnet, but each subnet can only have one NACL.
A VPC can be protected with security groups alone, but it is best practice to use security groups and NACLs.	Traffic entering a network is first filtered by NACLs, and then by security groups.

Rules in a security group and NACL can be added or removed, but security group and NACL can never be deleted.

EXPLORE | DIGITAL SKILLS

What is a DNS service?

Websites and computing devices communicate with IP addresses, but when a user visits a website the domain name is typed into the browser. The domain name used needs to be mapped to its IP address to access the website or target server. A **Domain Name System (DNS) service** is required to perform this mapping.

For the domain name to IP Address mapping, four different **DNS servers** are queried. All of this happens extremely fast.

The Four DNS Servers
1) Resolving Name Server
2) Root Name Server
3) TLD Name Server
4) Authoritative Name Server

Have a look at **this video** for an explanation of the role of each DNS server.

Amazon Route 53

Amazon Route 53 is a cloud-based DNS web service with high availability and scalability.

Services offered by Amazon Route 53

	Domain Registration	▪ A new domain can be **registered** by using the Amazon Route 53 console. ▪ A **¹hosted zone** is created when registering a domain. ▪ **Fees charged**: There is an annual charge for domain registration and a monthly fee for the hosted zone.
	DNS Routing	▪ This is a **cost-effective** way for businesses to connect end-users to their internet applications by translating domain names into IP addresses. ▪ The IP address: **²**216.58.211.110 is translated to "www.google.com"
	Health Checks	▪ Route 53 sends **automated requests** to a resource to ensure that the web server that deals with user requests are available and fully functioning. ▪ **Different health checks** can be performed by specifying the following values: - IP address/domain name of the web server that needs monitoring. - The request interval / frequency of requests. - Protocol: HTTP, HTTPS or TCP. - Failure threshold.

¹A hosted zone is a container for records, and records contain information about how you want to route traffic for a specific domain. **²**The IP address will change based on time and location. Use "nslookup google.com" from your command prompt to see the current IP address for the site.

The benefits of using Amazon Route 53

Highly Available, Reliable & Flexible

❖ **Amazon Route 53 Traffic Flow** re-routes traffic if an application endpoint is unavailable.
❖ **Multiple traffic policies** can be defined and edited in the Route 53 console, AWS SDKs or the Route 53 API.

Simple & Fast

❖ Configure **DNS settings** in the AWS Management Console or the AWS API.
❖ Use the **self-service sign-up**.
❖ Users will be automatically routed to the **best location** based on network conditions.

Cost-effective

❖ **Only pay** for resources being **used**:
 - Number of queries answered per domain.
 - Hosted zones.
 - Traffic flows and health checks.
❖ **No** minimum usage commitments or up-front payments.

Secure

❖ Grant unique credentials and permissions to users by integrating with AWS IAM.

Scalable

❖ **Automatic scaling** to handle large query volumes.

Use with other services

❖ Designed to work with other AWS features and offerings.
❖ Provides a **hybrid cloud solution** by connecting with your on-premise networks.

Read more here on Amazon Route 53 features.

What is a Content Delivery Network?

A **Content Delivery Network (CDN)** is required to minimise delays in loading content on web pages.
A **CDN** is a geographically distributed platform of servers that reduces the distance between the server and the user. The **benefits** of using a CDN:

Faster Website	**Reduced Costs**	**Increased Content Availability**	**Improved Security**

A CDN allows for the quick transfer of internet content:
 	
  - HTML pages
  - Javascript files
  - Images
  - Videos
	A CDN reduces website hosting costs by ***caching** the data and making use of other optimisations.
	
	Read here how it is done.
		The functionality of a website can be interrupted by increased traffic and hardware failures. The distributed servers of a CDN reduces/removes these interruptions.	A CDN with DDos mitigation can cope with sudden traffic increases and protect web pages from a variety of attacks.

*In computing, a **cache** is a high-speed data storage layer that stores a subset of data, typically transient in nature, so that future requests for that data are served up faster than is possible by accessing the data's primary storage location.

Amazon CloudFront

Amazon CloudFront is a CDN service with low latency and high transfer speeds.

Amazon CloudFront Key Features

Global Edge Network	Security	Availability	Metrics & Logging	Cost Effective
CloudFront delivers content through **edge locations** - a worldwide network of data centers. There are 215 edge locations across 46 countries.	The following AWS services work together to provide a **security layer** against attacks: - Amazon CloudFront - AWS Shield - AWS WAF - Amazon Route 53	CloudFront uses *Origin Shield to reduce traffic and increase **availability** to applications. Origin failover is used to serve backup content when the original is unavailable.	CloudFront and CloudWatch are integrated, and **automated metrics** are published in the CloudFront console. Requests from distributions are logged as: - Standard logs - Real-time logs	CloudFront offers **pay-as-go pricing** with no upfront fees. A one-year commitment offers up to 30% **discount**. **Free** data transfers between AWS services.

*Origin Shield, a centralized caching layer that helps increase your cache hit ratio to reduce the load on your origin.
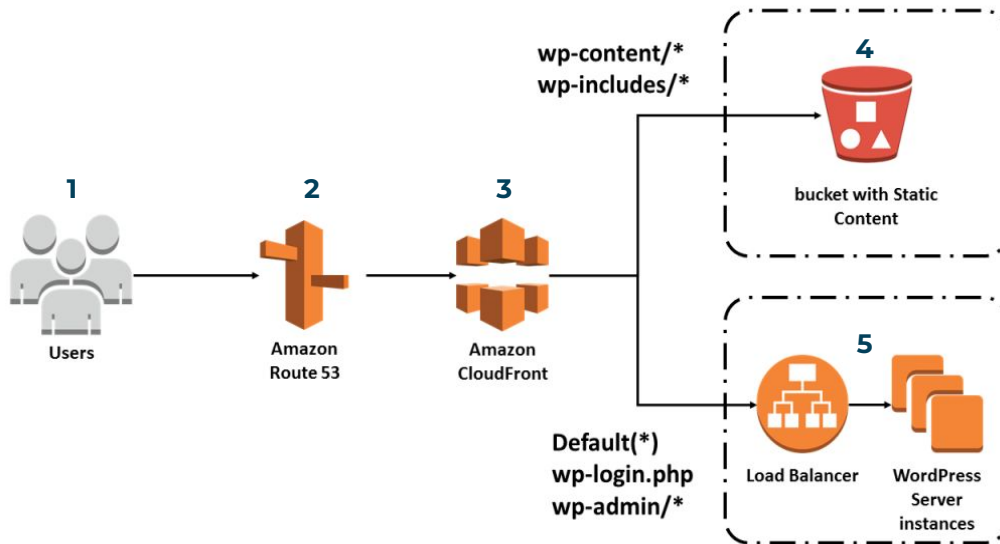
EXPLORE DIGITAL SKILLS

Use Case ~ Route 53 and CloudFront

A user wants to create their own website using WordPress.

Architecture Diagram

wp-content/*
wp-includes/*

4

bucket with Static
Content

1

Users

2

Amazon
Route 53

3

Amazon
CloudFront

Default(*)
wp-login.php
wp-admin/*

5

Load Balancer

WordPress
Server
instances

[How to Accelerate Your WordPress Site with Amazon CloudFront](#)

1) A **user** types "www.your-wordpress-site.com" into the bowser.

2) Amazon's DNS service, **Amazon Route 53**, translates this domain name into the IP address to direct the user to the correct location.

3) **Amazon CloudFront** directs the user traffic.

4) If the content requested is static (cached), the user will be directed to the **bucket**.

5) Otherwise, the user is directed to the nearest edge location to access your **website**.

Networking Basics

The Fundamentals of Networking in AWS

DNS Service and Content Delivery with AWS

Conclusion

Conclusion

This train covered a high-level explanation of the following learning objectives:

Networking Basics

A computer network is a group of computing devices linked together, enabling communication through an internet connection. Each computing device has a unique identifier known as an IP address.

Networking with AWS

Amazon VPC is an isolated virtual network in the cloud. The components of a VPC are subnets, internet gateway, NAT gateway, Route tables, NACLs and a VPN connection. The VPC is made secure by the use of security groups and NACLs.

Domain Name System

A Domain Name System (DNS) maps domain names (website URLs) to an IP address. **Amazon Route 53** offers a DNS service. This service is useful for domain registration, DNS routing and health checks.

Content Delivery Network

A Content Delivery Network (CDN) reduces the delay on a website by shortening the distance between a user and a server. **Amazon CloudFront** offers a CDN service. This service uses edge locations to deliver content with low latency and high speed.

EXPLORE DIGITAL SKILLS

Additional Resources

AWS Networking and Content Delivery is extremely powerful. It is important to deepen your understanding on this topic by referencing the following resources:

SETTING UP A AMAZON VPC:
- ❖ Amazon VPC Fundamentals - Part I
- ❖ Amazon VPC Fundamentals - Part II

PRICING:
- ❖ Amazon VPC
- ❖ Amazon Route 53
- ❖ Amazon CloudFront

NETWORKING AND CONTENT DELIVERY
- ❖ Networking and Content Delivery on AWS
- ❖ What does AWS Networking Services Offer?
- ❖ A complete guide to networking