



# Le protocole TCP/IP

## Présenter par:

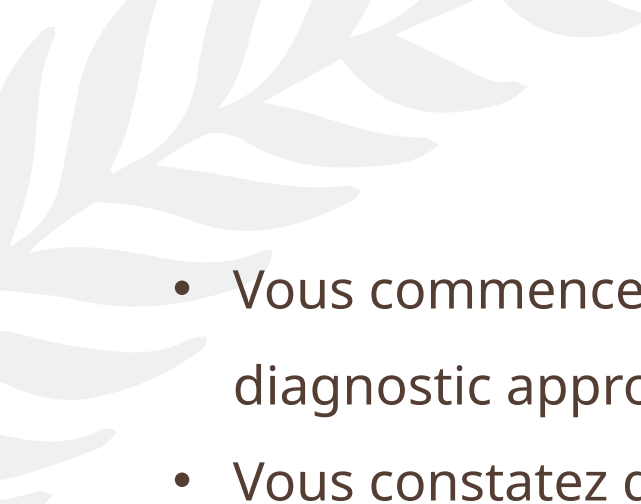
Allali Ouissal  
Salma Zribah  
Othman Benmalek  
Karroum Abdelaziz  
Mosadaq Aymane

## Encadré par:

Mr Abdellaoui Arbi

# Situation Problème

Supposons que vous travaillez dans une entreprise où les employés utilisent des ordinateurs pour accéder à Internet. Vous recevez des plaintes de la part de certains employés qui se plaignent que leurs ordinateurs ne peuvent pas accéder à certains sites Web.

- 
- Vous commencez par vérifier la connectivité réseau en utilisant les outils de diagnostic appropriés.
  - Vous constatez que les ordinateurs qui ont des problèmes d'accès à Internet ne peuvent pas atteindre le serveur DNS de l'entreprise.
  - Après avoir vérifié la configuration du serveur DNS, vous constatez qu'il y a une erreur de configuration qui empêche les ordinateurs de se connecter correctement.
  - Vous modifiez la configuration du serveur DNS pour corriger l'erreur et vous vous assurez que tous les ordinateurs ont la bonne adresse IP pour le serveur DNS.
  - Vous vérifiez ensuite que les ordinateurs peuvent maintenant atteindre le serveur DNS et accéder aux sites Web qu'ils souhaitent.



# Plan

Introduction

1

---

Couche Liaison

2

---

Couche Réseau

3

---

Couche Transport

4

---

Couche Application

5

---

Conclusion

6

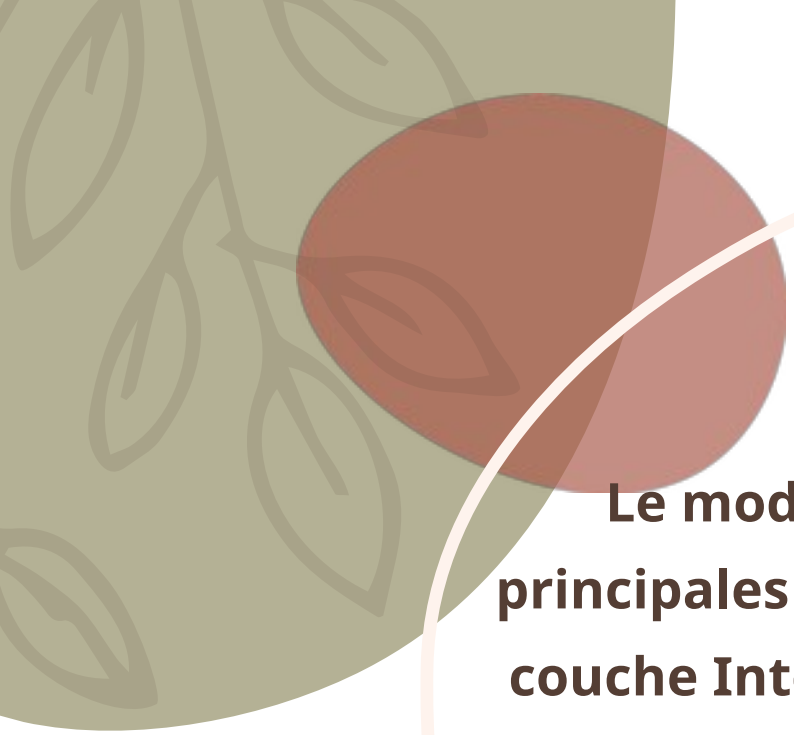
# C'est quoi un protocole ?

Un protocole est ensemble de règles qui définit comment se produit une communication dans un réseau .



# INTRODUCTION

**Le modèle TCP/IP, également connu sous le nom de modèle de référence TCP/IP, est un modèle de communication en réseau qui définit les normes pour la transmission de données entre des ordinateurs sur un réseau. Il est largement utilisé dans le monde entier pour la communication sur Internet et d'autres réseaux informatiques.**



**Le modèle TCP/IP est composé de quatre couches principales : la couche application, la couche transport, la couche Internet et la couche liaison de données. Chaque couche est responsable de fonctions spécifiques et utilise des protocoles de communication pour transmettre des données entre les ordinateurs.**

# La raison pour la quelle on a changé le modèle OSI par TCP/IP

**Le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) sont tous deux des modèles de référence utilisés pour décrire la communication entre ordinateurs.**

**La principale raison pour laquelle le modèle TCP/IP est aujourd'hui plus largement utilisé que le modèle OSI est qu'il est plus simple et plus facile à implémenter. Le modèle TCP/IP a été conçu pour être utilisé sur des réseaux hétérogènes (c'est-à-dire des réseaux comprenant différents types d'ordinateurs et de systèmes d'exploitation), ce qui le rend plus adaptable et plus pratique pour la plupart des applications.**



**En outre, le modèle TCP/IP a été largement adopté par l'industrie informatique et est aujourd'hui considéré comme le modèle de référence standard pour la communication sur Internet. Il est également devenu le modèle de référence pour de nombreux protocoles de communication, tels que HTTP (utilisé pour les pages web) et SMTP (utilisé pour le courrier électronique).**

Cliquez sur l'icône pou



The background features a large, dark brown organic shape on the left, a muted olive green shape on the top right, and a white shape on the bottom right. Faint, stylized foliage is visible in the top left corner, and thin, flowing lines in light brown and white cross the bottom right area.

# 1. Couche Liaison

# Définition

----La couche de liaison de données est la deuxième couche dans le modèle TCP/IP, elle est divisées en deux sous-couche :

**\*La sous-couche LLC(Logical Link Control)** : responsable de la gestion de control des flux, du contrôle d'erreur et l'établissement de la liaison entre les différents périphériques.

**\*la sous- couche MAC (Media AccessControl)** : responsable de la gestion de l'accès au support de transmission (par exemple, le cable Ethernet, Wi-Fi)

Cette couche a pour objectif de gérer la transmission de données entre les différents nœuds d'un réseau local (LAN). Parmi leurs fonctionnalités :

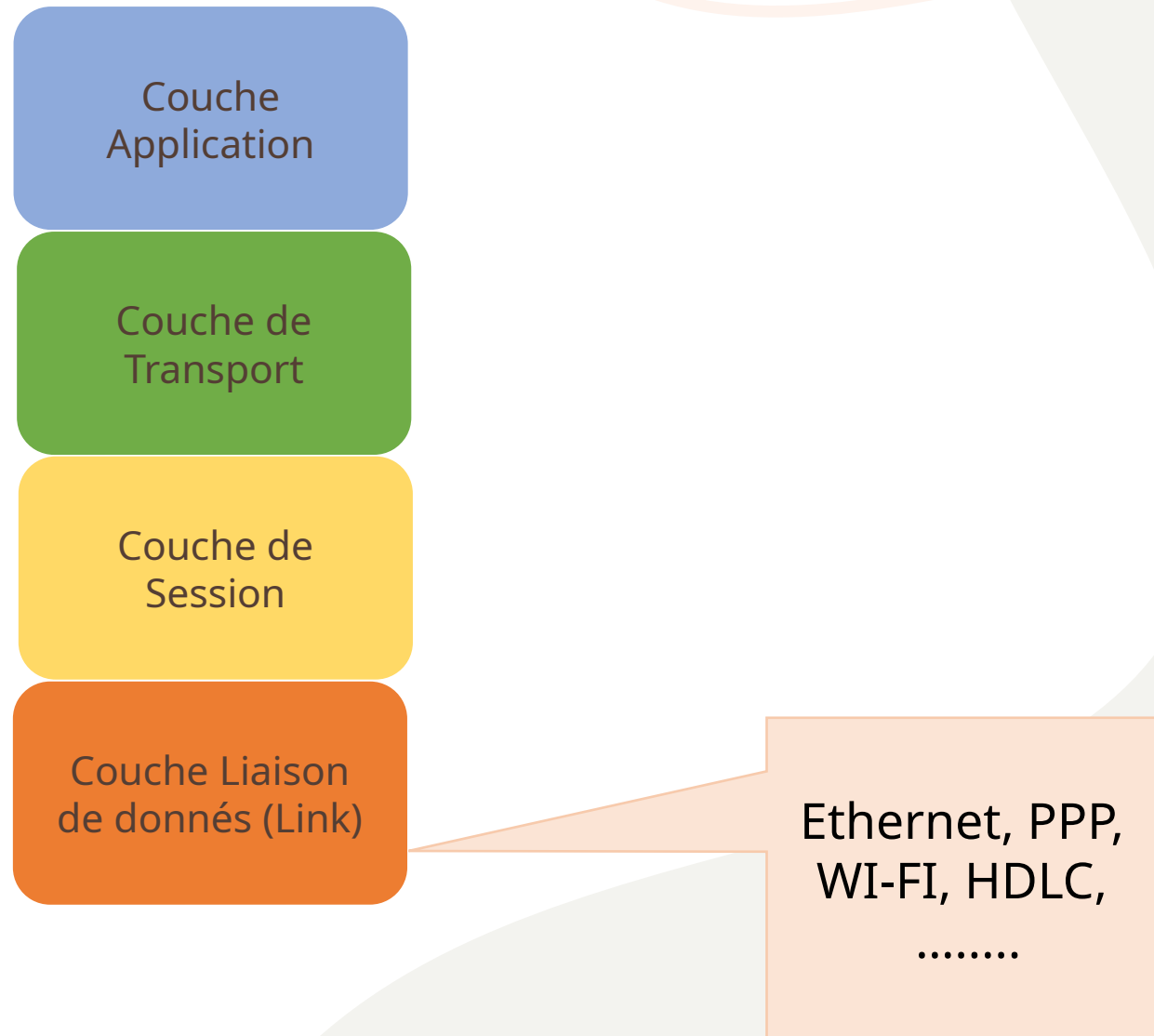
- Encapsulation des données de la couche réseau dans des trames ou des paquets qui peuvent être transmis sur le support de transmission physique.

- Gestion du flux de données pour éviter la saturation du support de transmission

- Contrôle d'accès au support de transmission pour éviter les collisions de données

- Détection et correction d'erreurs de transmission pour garantir l'intégralité des données transmises.

- Elle est responsable de l'adressage physique, qui permet de différencier les nœuds sur un réseau en utilisant des adresses MAC (Media Access Control) uniques.



# \*\*\*\*\*Le protocole Ethernet\*\*\*\*\*

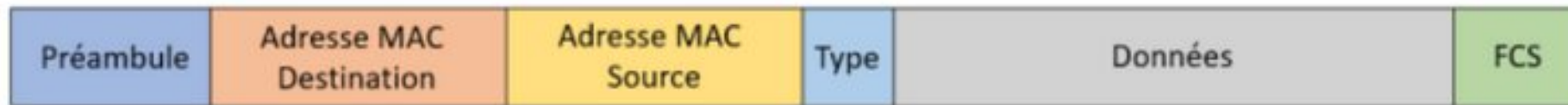
**Ethernet** : C'est un protocole de réseau local (LAN) qui utilise une méthode de transmission de données en mode paquet. Il est utilisé pour connecter des ordinateurs et des périphériques sur un même réseau local. Ethernet est le protocole le plus couramment utilisé pour les réseaux filaires.

la mise en **réseau filaire** traduit par des câbles RJ45 qui relie des équipements comme des PC, imprimantes.

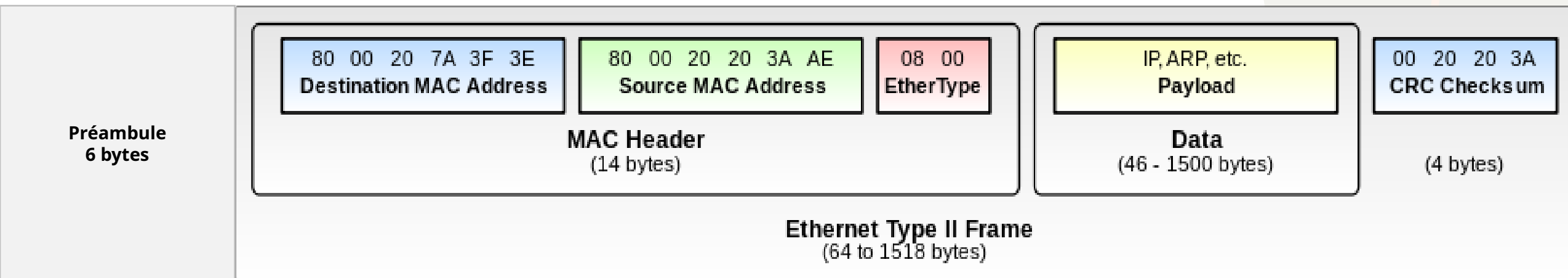
# Le Principe de protocole Ethernet :

Le fonctionnement du protocole Ethernet est basé sur la transmission de **frames** de données entre les équipement connectés au réseau. Les trames Ethernet sont constituées de plusieurs parties, y compris une en tête et un corps de données.

## Trame Ethernet



# La structure d'une trame Ethernet :





Les différentes parties qui composent une trame Ethernet :

- **Préambule** : une séquence de 7 Octets (56 bits) qui sert à synchroniser les horloges des dispositifs.
- **Un En-tête (MAC)** : composées de 14 octets, et qui contient :
  - L'Adresse MAC de destination (6 octets).
  - L'Adresse MAC Source (6 octets)
- **Type de protocole** : un champs de 2 octets(16 bits) qui indique le type de protocole encapsulé dans la trame (Type de données encapsulée/taille de la trame ) .

## Le champs Ether peut prendre les valeurs suivantes :

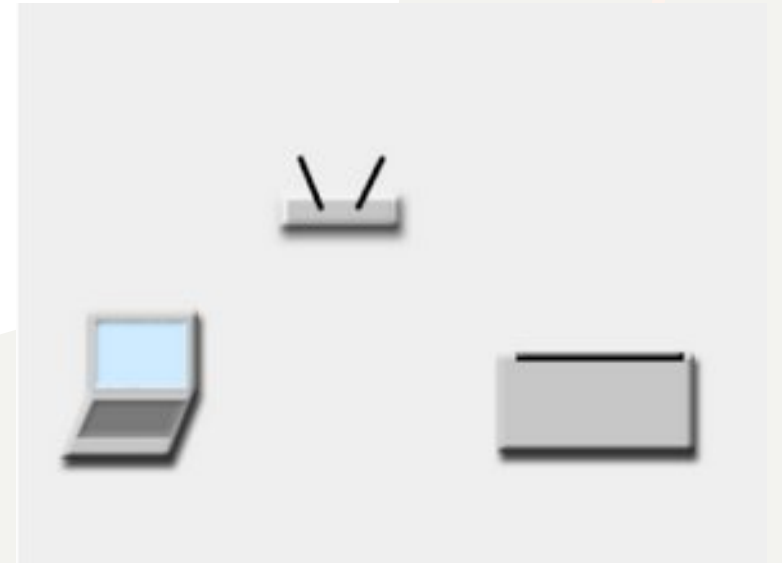
Type	utilisation
0x0800	IPv4, DoD Internet
0x0801	X.75 Internet
0x0802	NBS Internet
0x0803	ECMA Internet
0x0804	ChaosNet
0x0805	X.25 niveau 3
0x0806	ARP
0x0807	XNS
0x86DD	IPv6

- **Données** : la charge utile de la trame, qui contient les informations envoyées entre les dispositifs. La longueur de ce champ peut varier de 46 à 1500 octets.
- **FCS** : Un champ de 4 octets (32 bits) qui contient un code de redondance cyclique (CRC) qui permet de détecter les erreurs de transmission.

Donc la longueur total de la trame Ethernet et généralement comprise entre 64 et 1518 bytes.

## \*\*\*\*\*Le Protocole Wi-Fi\*\*\*\*\*

Le protocole Wi-Fi(Wireless Fidelity) est un protocole de communication sans fil basé sur les normes IEEE 802.11 qui permet la communication entre des dispositifs électroniques sans utiliser de câbles. Le protocole Wi-Fi utilise des ondes radio pour transmettre des données entre des dispositifs tels que les ordinateurs, des smartphones, des tablettes, des routeurs et des points d'accès.



Wireless Standard	Frequency Band	Wireless Rate
802.11a	5GHz	54 Mbps
802.11b	2.4GHz	11 Mbps
802.11g	2.4GHz	54 Mbps
802.11n	2.4GHz & 5GHz	Up to 600 Mbps
802.11ac	5GHz	Up to 6.93 Gbps
802.11ax	2.4GHz & 5GHz	Up to 9.6 Gbps

## \*\*\*\*\*Le Protocole PPP\*\*\*\*\*

Point-to-Point Protocol (PPP, protocole point à point) est un protocole de transport pour l'Internet, décrit par le standard **RFC 1661**, fortement basé sur HDLC, qui permet d'établir une connexion entre deux hôtes sur une **liaison point à point**. Il fait partie de la couche liaison de données (couche 2) du modèle OSI.

Les fonctionnalités d'authentification est assurée par les protocoles PAP ou CHAP. Il est capable d'agrégier les liaisons grâce à PPP Multi Link (MLPPP). Enfin, il permet de créer des connexions point à point par sur-encapsulation sur une technologie partagée comme Ethernet (PPPoE).

## Noté bien :

Le protocole HDLC (High-level Data Link Control) est un protocole de liaison de données utilisé pour la transmission de données sur des réseaux de télécommunication. Il est largement utilisé dans les réseaux de communication de données tels que les réseaux WAN (Wide Area Networks) et les réseaux de commutation de paquets.

## ***PPP s'appuie sur trois composants :***

L'encapsulation des datagrammes.

Le contrôle de la liaison avec LCP (Link Control Protocol).

Le contrôle de la couche réseau avec NCP (Network Control Protocol).

## ***Le protocole PPP permet une meilleure gestion des liaisons par rapport à HDLC car :***

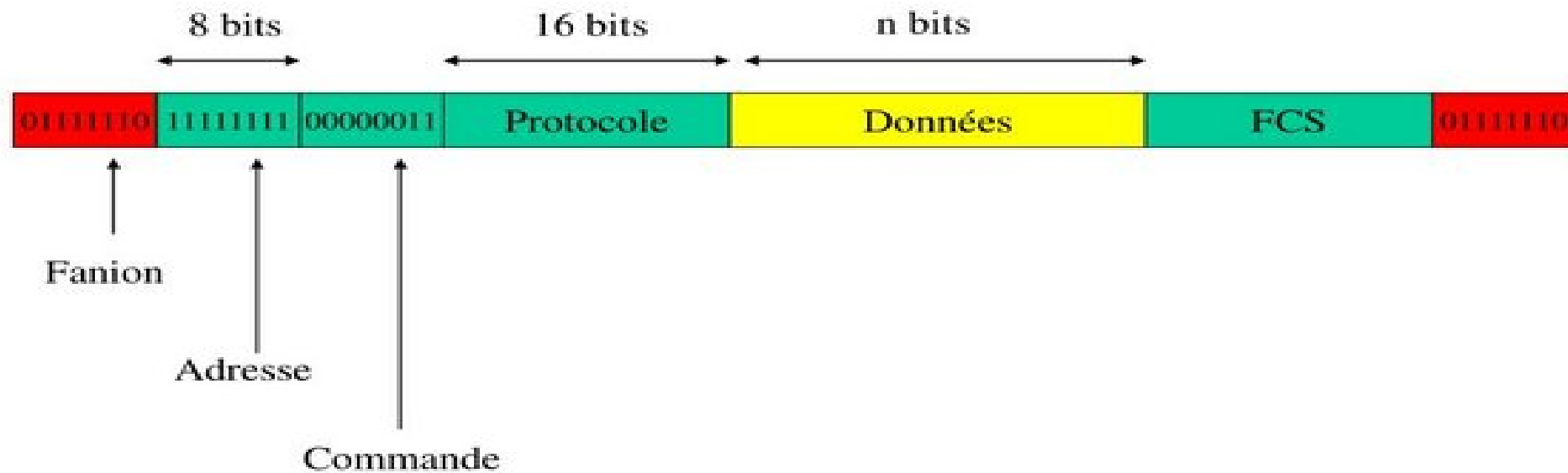
Il prend en charge des mécanismes d'authentification, comme PAP ou CHAP.

Il permet l'agrégation de lien (on parle de PPP Multilink).

Il permet la compression des données



# Format des trames PPP



## Protocole point à point

Protocole de liaison de données commun pour les réseaux étendus

Trame						
Nom du champ	Indicateur	Adresse	Contrôle	Protocole	Données	FCS
Taille	1 octet	1 octet	1 octet	2 octets	variable	2 ou 4 octets

**Indicateur** : octet unique qui indique le début ou la fin d'une trame. L'indicateur est constitué de la séquence binaire 01111110.

**Adresse** : octet unique qui contient l'adresse de diffusion PPP standard. PPP n'attribue pas d'adresses de station individuelles.

**Contrôle** : octet unique composé de la séquence binaire 00000011, qui appelle la transmission des données utilisateur dans une trame non séquencée.

**Protocole** : deux octets qui identifient le protocole encapsulé dans le champ de données de la trame. Les valeurs les plus à jour du champ de protocole sont spécifiées dans les documents RFC les récents des numéros attribués.

**Données** : zéro ou plusieurs octets contenant le datagramme du protocole précisé dans le champ de protocole.

**Séquence de contrôle de trame (FCS)** : normalement, 16 bits (2 octets). En vertu d'un accord précédent, les mises en oeuvre PPP adoptées peuvent utiliser une séquence de contrôle de trame 32 bits (4 octets) pour une détection améliorée des erreurs.

## ---les sous protocoles de PPP :

Le protocole PPP est constituée par des sous protocole :

### **LCP**

Le sous-protocole LCP (Link Control Protocol) ne s'occupe que paramètres de couche 2 :

- Détection de boucle : transmission d'un nombre magique

- Détection d'erreur avec LQM Link-Quality Monitoring

- Support Multilink : répartition de charge sur plusieurs liaisons

- Authentication : PAP ou CHAP

## ***NCP***

Network Control Protocols (NCP) est une catégorie de protocole qui négocie des paramètres de couche 3 pour son propre compte comme par exemple :

CDPCP

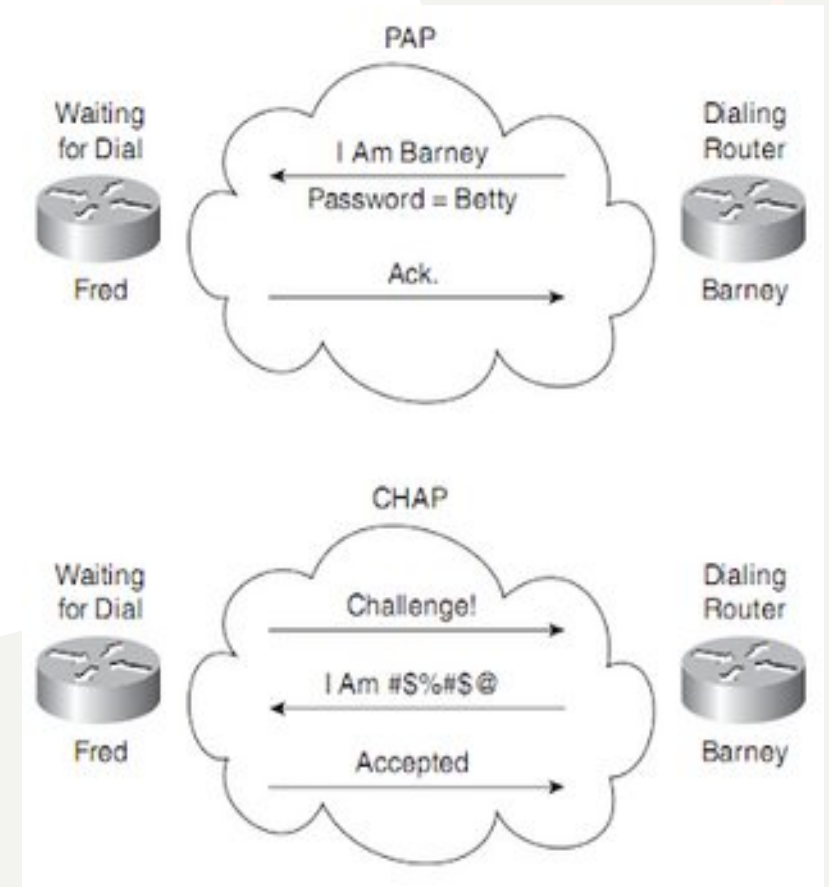
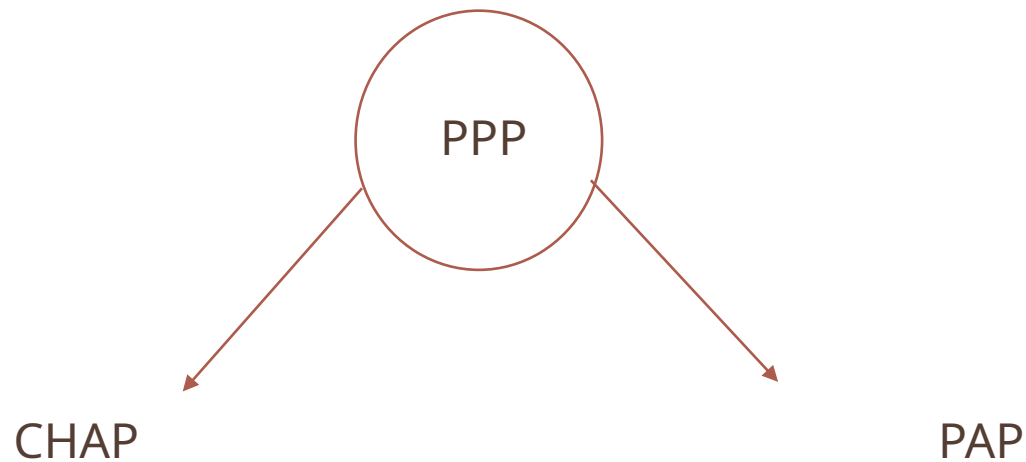
IPCP

--- l'authentification PPP :

**Définition :**

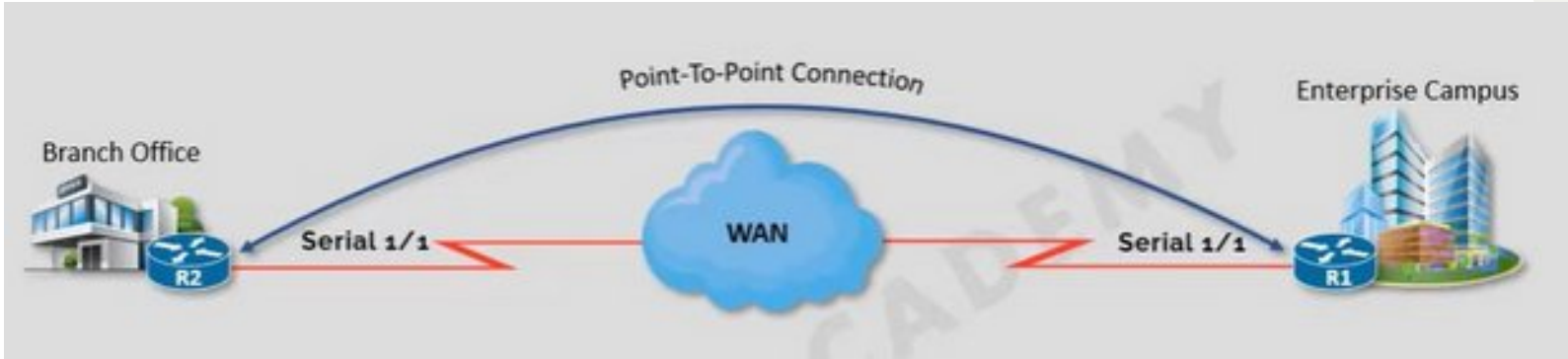
**L'authentification PPP** est une méthode utilisée pour vérifier l'identité de l'utilisateur qui se connecte au réseau.

On a deux méthodes de s'authentification :



# Authentication PPP PAP

Password Authentication Protocol (PAP) est un protocole d'authentification pour PPP. Les données d'authentification sont transmises en texte clair sur le réseau ce qui le rend par conséquent non sécurisé



User Name : R2, Password : Cisco123

User Name	Password
R2	Cisco123

-----  
----->

Accept or Reject

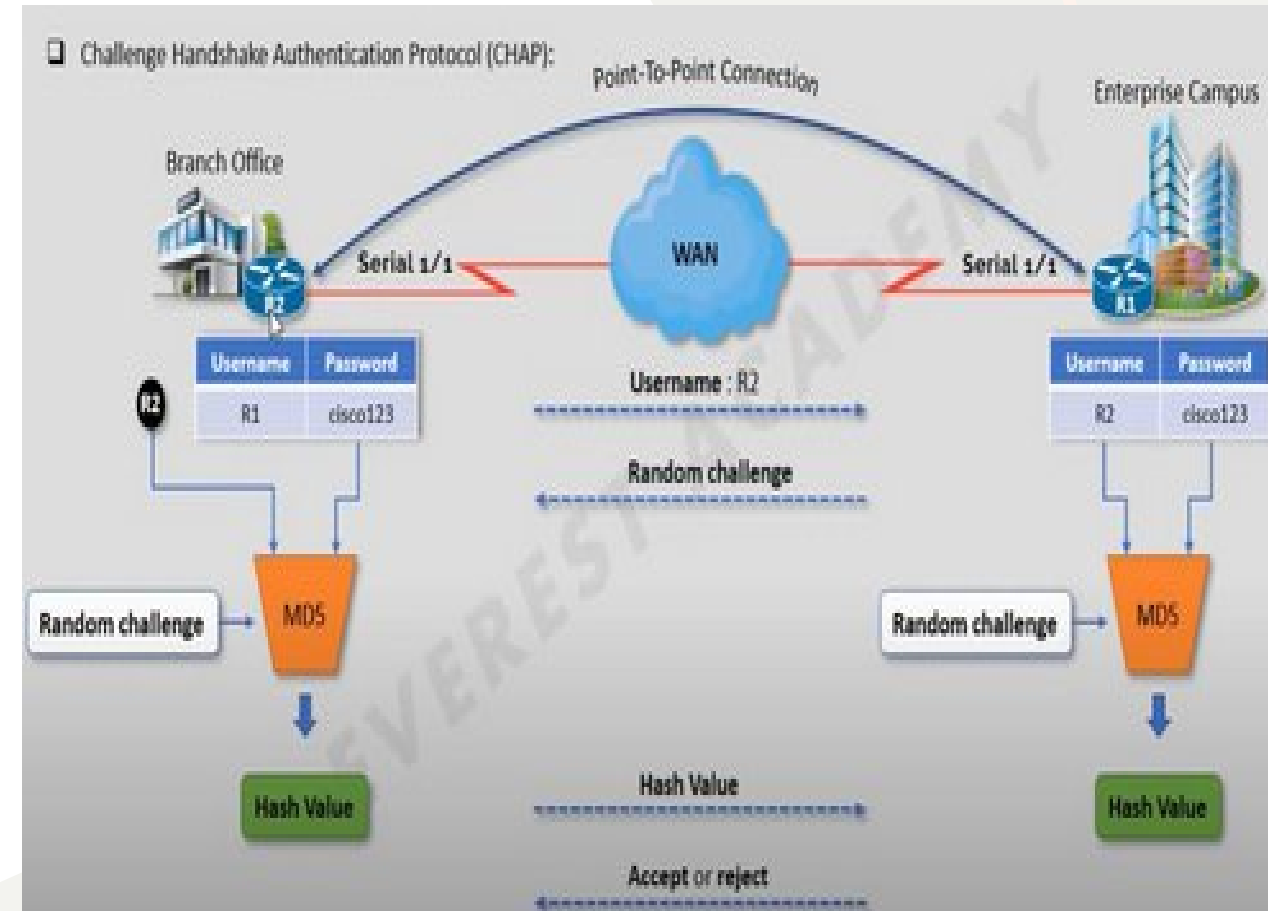
□-----  
-----

## Configuration PAP :

- Le client envoie une demande de connexion au serveur distant.
- Le serveur distant envoie une demande d'authentification au client.
- Le client répond avec un nom d'utilisateur et un mot de passe valides.
- Le serveur vérifie les informations d'authentification et, si elles sont correctes, autorise la connexion.
- La connexion est établie et les données peuvent être échangées entre le client et le serveur.

## Authentication PPP CHAP

Challenge Handshake Authentication Protocol (CHAP) est un protocole d'authentification pour PPP à base de challenge, ce qui le rend bien plus sûr que son pendant PAP. Ce protocole est défini dans la [RFC 1994](#). Il est aussi utilisé par le protocole iSCSI afin qu'Initiator et Target iSCSI s'authentifient éventuellement mutuellement





## Configuration CHAP :

- Le client envoie une demande de connexion au serveur distant.
- Le serveur distant envoie une demande de challenge au client.
- Le client répond avec une valeur de réponse chiffrée.
- Le serveur vérifie la valeur de réponse pour s'assurer que l'utilisateur est authentifié.

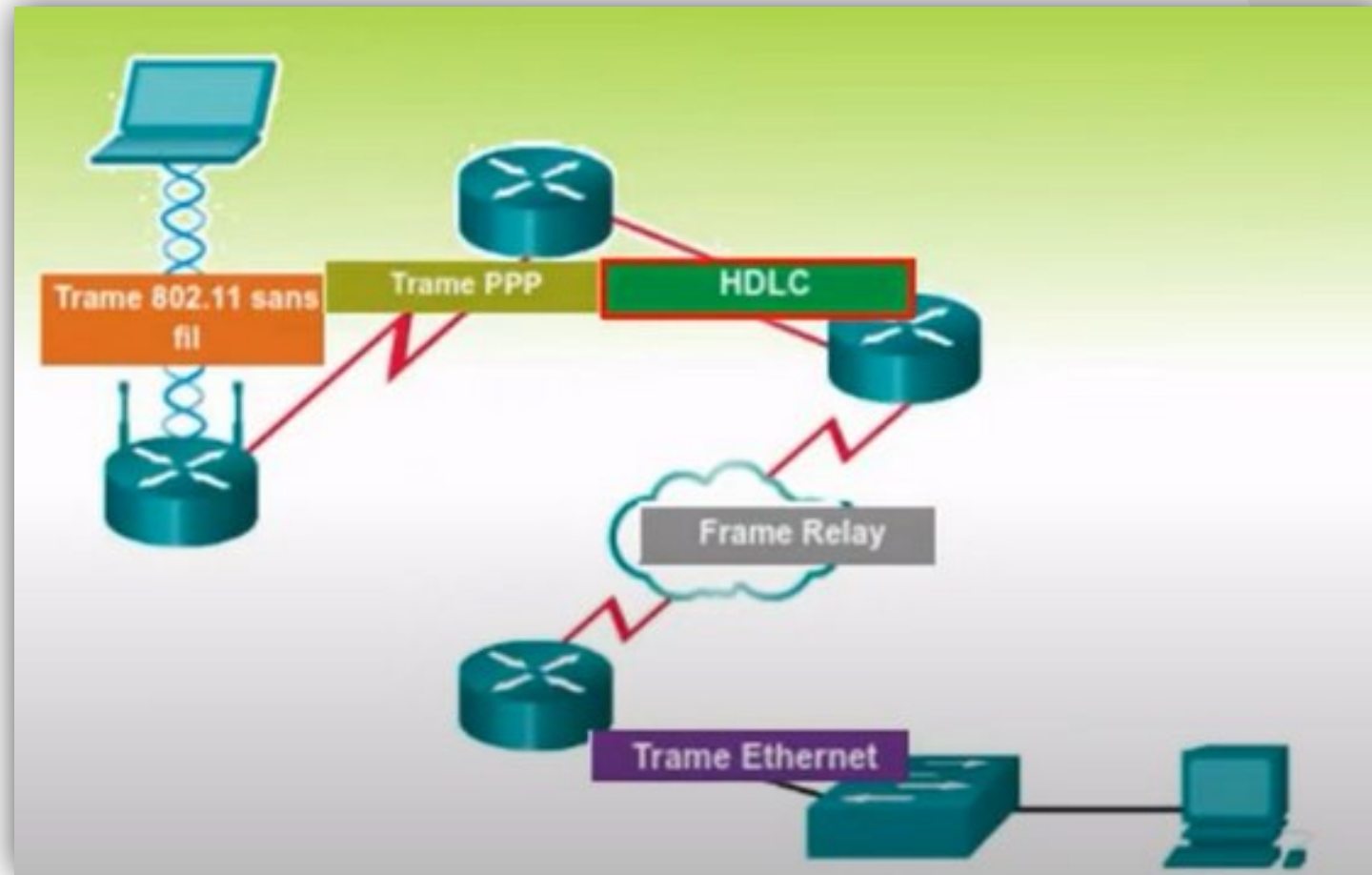
Si la valeur de réponse est valide, le serveur autorise la connexion.

- La connexion est établie et les données peuvent être échangées entre le client et le serveur.

### Noté bien

MD5 : Le MD5 (Message Digest 5) est une fonction de hachage cryptographique utilisée dans le protocole de challenge-authentication protocol (CHAP).

En résumé :



The background features a large, dark brown organic shape on the left containing the text. To its right is a large, muted olive-green organic shape. In the top-left corner, there are stylized, light grey foliage elements. At the bottom, thin, light orange wavy lines cross the frame.

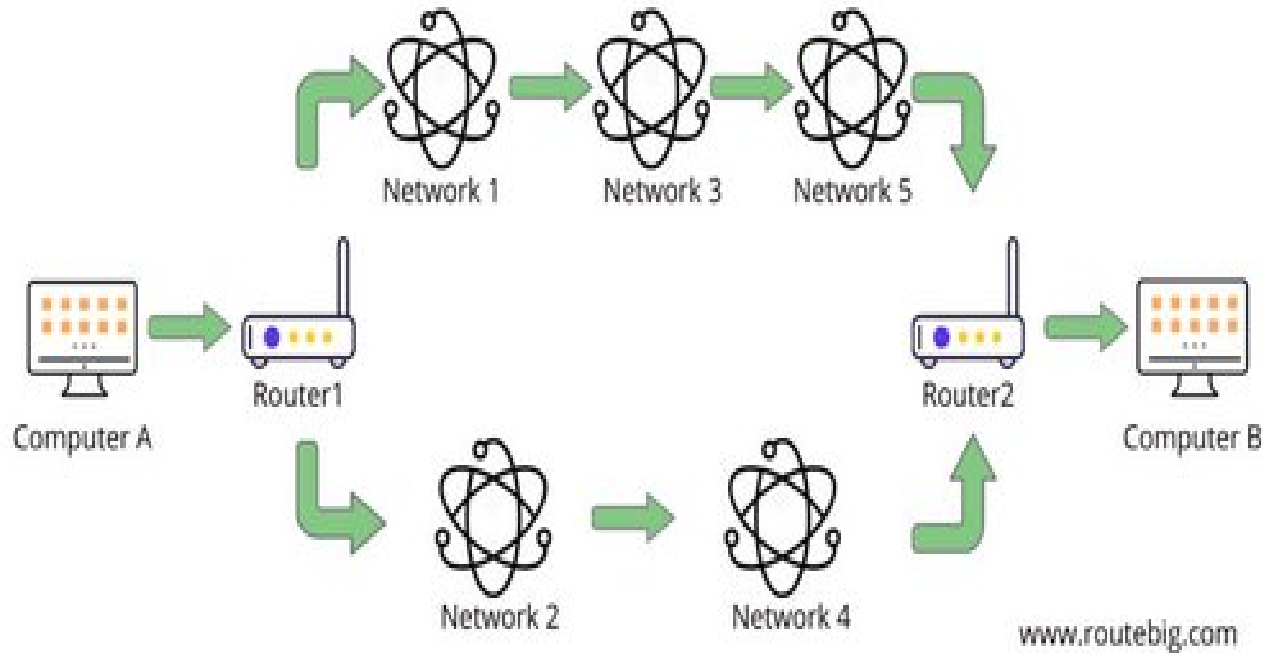
## 2. Couche Réseau

## Définition de la couche réseau :


La couche de réseau est la troisième couche du modèle TCP/IP. Elle est responsable de l'acheminement des paquets de données à travers les réseaux en utilisant des adresses IP. Elle utilise le protocole IP pour diriger les paquets vers leur destination en utilisant des routeurs et des tables de routage.

# Mots clés de la couche :

## What is Routing



- Routage : Le routage est le processus par lequel les paquets de données sont acheminés à travers les réseaux pour atteindre leur destination. Les routeurs sont des dispositifs qui effectuent cette fonction en utilisant des tables de routage pour déterminer le chemin optimal à suivre pour chaque paquet.



2. Fragmentation : Les paquets de données peuvent être fragmentés en plusieurs morceaux pour être transmis à travers des réseaux ayant une taille maximale de paquet différente.

Le protocole qui responsable de la fragmentation est le protocole IP.

# Protocoles :

❖ **IP (Internet Protocol)** : est un protocole qui est responsable de l'acheminement des paquets de données à travers les réseaux en utilisant des adresses IP. Le protocole IP est utilisé pour transmettre des datagrammes, qui sont des unités de données contenant des informations telles que l'adresse IP de la source et de la destination, ainsi que le numéro de séquence pour permettre la réassemblage des fragments.

## IP fixe et dynamique :

-Une **adresse IP dynamique** est une adresse IP qui peut changer à chaque fois que l'appareil se connecte à un réseau. Elle est attribuée par un serveur DHCP (Dynamic Host Configuration Protocol) qui gère les adresses IP disponibles sur un réseau et les assigne aux différents appareils qui y sont connectés.

Lorsqu'un appareil se connecte à un réseau, il envoie une demande de configuration au serveur DHCP, qui lui attribue une adresse IP dynamique pour une durée limitée. Cette durée est appelée bail et peut être renouvelée automatiquement si l'appareil reste connecté au

Les adresses IP dynamiques sont utilisées pour économiser les adresses IP disponibles sur un réseau et permettre à un grand nombre d'appareils de se connecter en utilisant un nombre limité d'adresses IP. Cependant, cela peut rendre plus difficile l'accès à un appareil spécifique depuis Internet, car l'adresse IP peut changer à chaque fois que l'appareil se connecte au réseau.

Les fournisseurs d'accès Internet (FAI) utilisent souvent des adresses IP dynamiques pour leurs clients résidentiels, car cela leur permet de gérer plus efficacement l'utilisation des adresses IP disponibles et de réduire les coûts d'infrastructure réseau.

## Adresse Fixe :

Une adresse IP fixe est une adresse IP qui est assignée de manière permanente à un appareil sur un réseau. Contrairement à une adresse IP dynamique, qui peut changer chaque fois que l'appareil se connecte au réseau, une adresse IP fixe reste constante, ce qui permet aux autres appareils et utilisateurs de se connecter à cet appareil de manière fiable et constante.

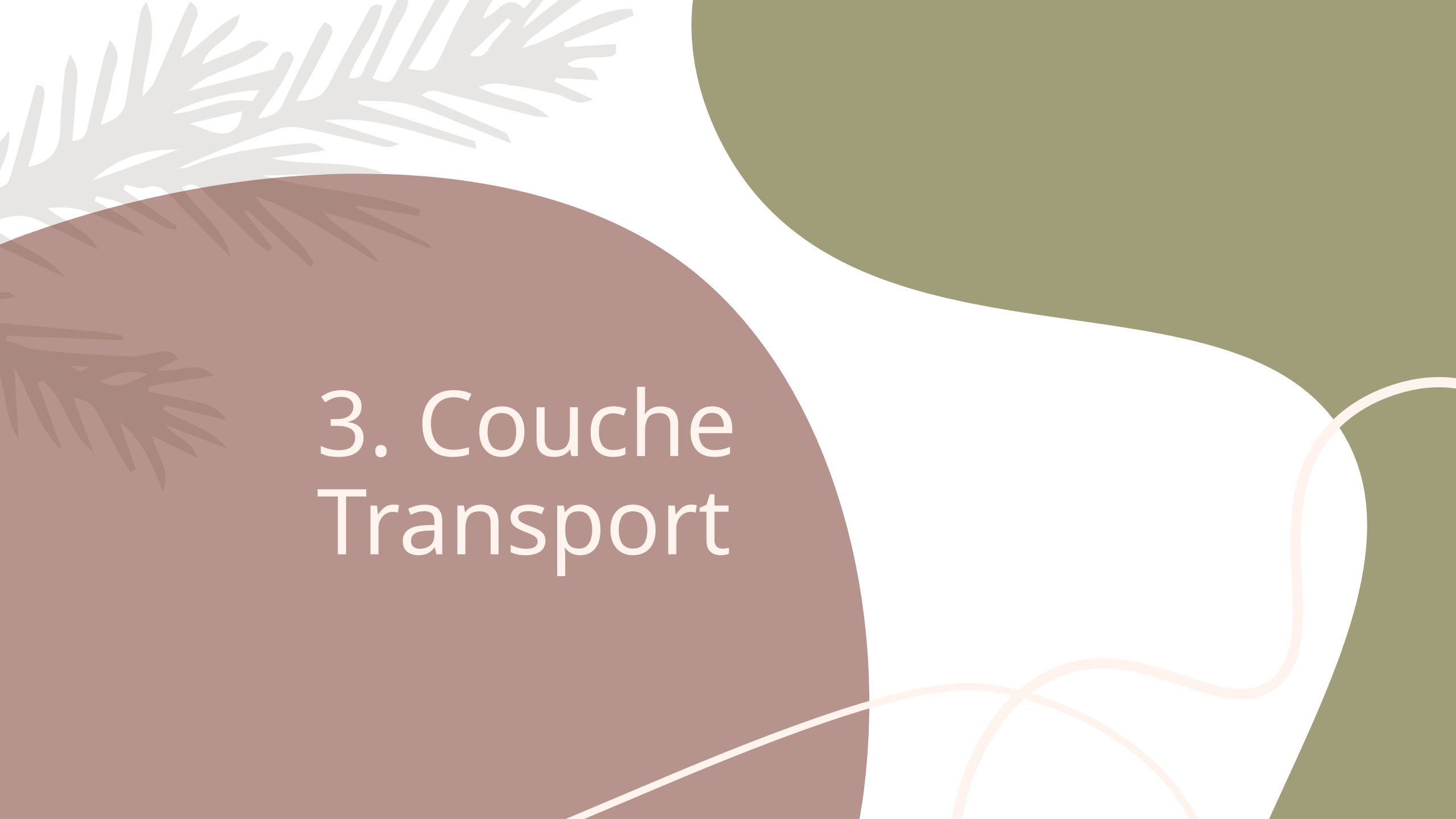
Les adresses IP fixes sont souvent utilisées pour les serveurs web, les serveurs de messagerie électronique, les caméras de surveillance, les routeurs, les imprimantes réseau et d'autres périphériques réseau qui doivent être accessibles en permanence.



L'avantage principal d'une adresse IP fixe est qu'elle permet aux autres appareils et utilisateurs de se connecter à un appareil spécifique sur un réseau de manière constante et fiable. Cela peut être important pour les entreprises, les organisations ou les particuliers qui ont besoin d'un accès constant à des ressources réseau spécifiques.

Cependant, l'utilisation d'adresses IP fixes peut également présenter des inconvénients, notamment la possibilité d'être ciblé par des attaques informatiques, la nécessité de configurer manuellement les adresses IP sur chaque appareil et la limitation du nombre d'adresses IP disponibles sur un réseau.

- ❖ **ARP (Address Resolution Protocol)** est un protocole de la couche liaison de données du modèle TCP/IP. Il est utilisé pour résoudre les adresses MAC (Media Access Control) en adresses IP. Lorsque les hôtes communiquent sur un réseau local, ils utilisent des adresses MAC pour identifier les autres hôtes, tandis que les adresses IP sont utilisées pour les communications à travers les réseaux. L'ARP permet donc de faire correspondre les adresses IP aux adresses MAC correspondantes.
- ❖ **ICMP (Internet Control Message Protocol)** est un protocole de la couche de réseau du modèle TCP/IP. Il est utilisé pour envoyer des messages d'erreur et de contrôle à d'autres équipements réseau, tels que des routeurs. Les messages ICMP peuvent être utilisés pour signaler des erreurs de transmission, des pannes de réseau, des congestions, etc. par exemple, le message ICMP "ping" est utilisé pour tester la connectivité entre deux hôtes en envoyant un message ICMP echo-request et en attendant une réponse ICMP

The background features a large, dark brown organic shape on the left containing the text. To its right is a large, muted olive-green shape. In the top left corner, there are stylized, light grey foliage elements. At the bottom, thin, light orange wavy lines cross the frame.

## 3. Couche Transport

# Définition

La couche de transport du modèle TCP/IP est responsable de la communication de bout en bout entre les applications. Elle fournit des services de transport de données fiables et sans erreur entre les machines de source et de destination.

Plus précisément, la couche de transport est chargée de segmenter les données en unités plus petites appelées segments, d'ajouter des en-têtes de contrôle pour assurer la fiabilité de la transmission, de gérer le flux de données et de fournir des mécanismes de contrôle de congestion pour éviter la surcharge du réseau.

# Les protocoles de la couche

Parmi les protocoles de transport les plus couramment utilisés dans le modèle TCP/IP sont TCP et UDP et SCTP.

## *Le protocole TCP :*

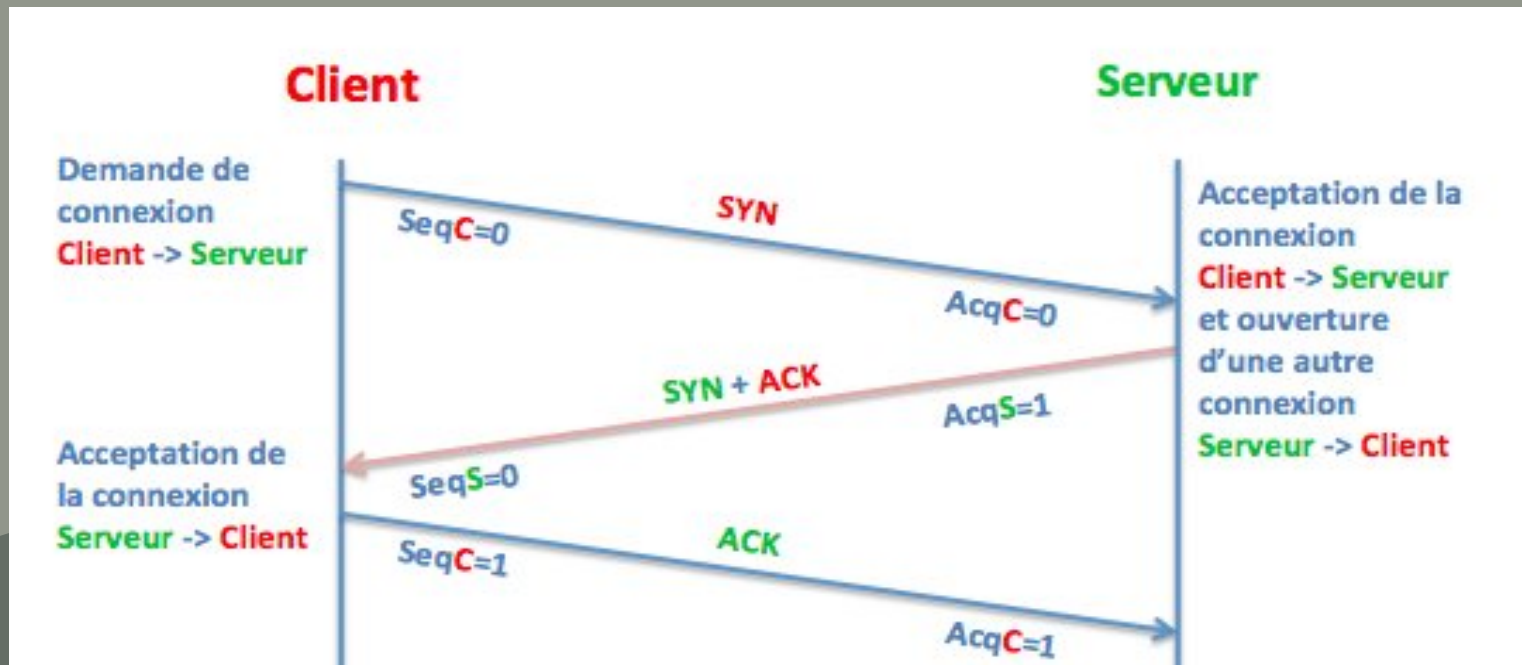
Le TCP, pour Transmission Control Protocol, ou littéralement protocole de contrôle de transmissions en français, développé au début des années 1970, désigne un protocole de transmission utilisé sur les réseaux IP.

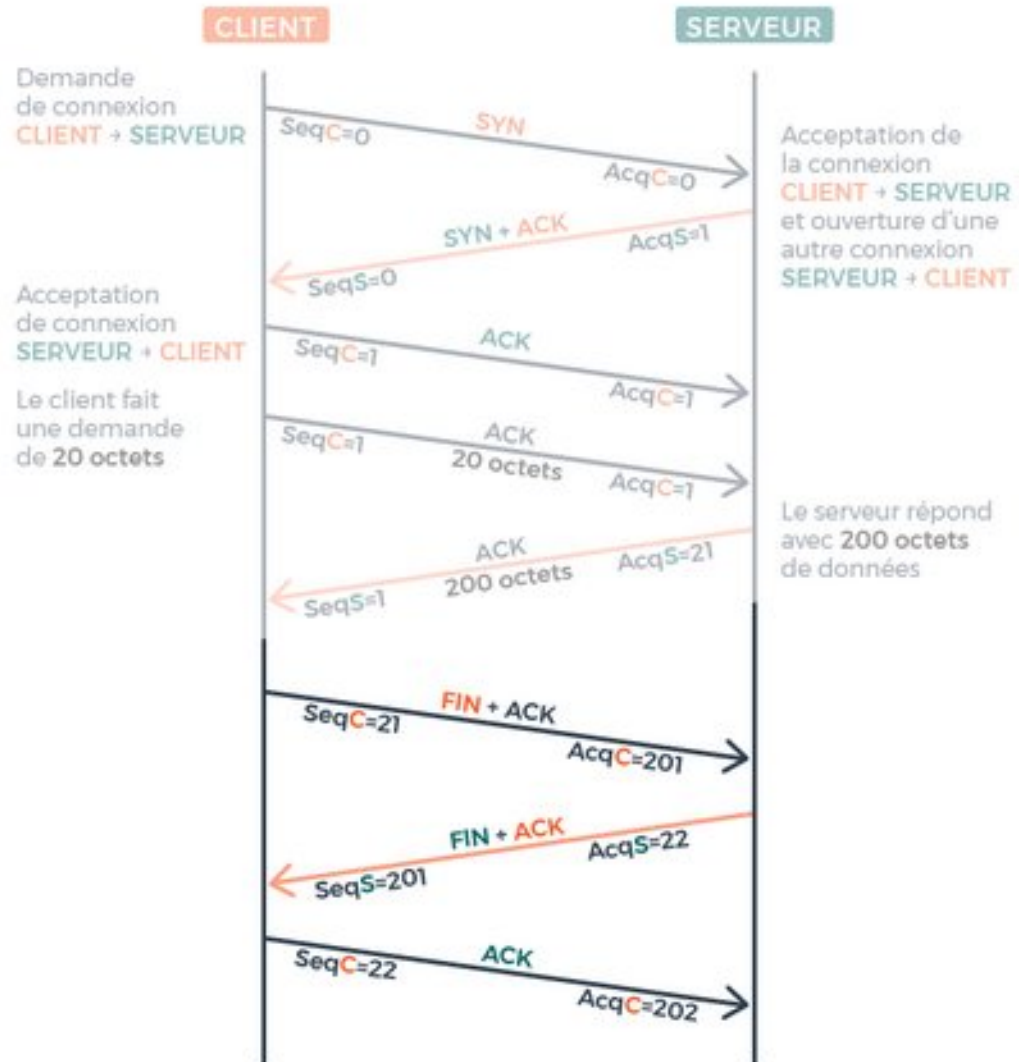
Il est basé sur un fonctionnement en trois temps. Il établit d'abord une connexion, transfère ensuite les données, et met enfin un terme à la connexion. Toutes ces opérations sont réalisées dans un environnement sécurisé et fiable.

# Le fonctionnement de TCP

Le principe de fonctionnement de TCP repose sur l'établissement d'une **connexion à trois voies** entre les **machines source** et **destination** avant que les données ne soient transmises. Cette connexion utilise une technique de **synchronisation** appelée "**handshake à trois voies**", qui permet aux deux machines de se mettre d'accord sur les paramètres de la connexion, tels que les **numéros de séquence** et **d'acquittement**, les **options de transfert de données** et les **fenêtres de transmission**.

Une fois que la connexion est établie, les données sont transmises en **segments**, chaque segment étant **numéroté** et accompagné d'un **accusé de réception (ACK)** qui indique à la machine source que le segment a été reçu correctement par la machine destination. Si un segment est perdu ou corrompu en cours de route, TCP demande sa réémission à la machine source. En outre, TCP utilise des mécanismes de contrôle de flux et de congestion pour éviter la surcharge du réseau et garantir une transmission fluide et efficace des données.





Lorsque la transmission des données est terminée, la connexion est **fermée** à l'aide d'un "**handshake à quatre voies**", qui permet aux deux machines de **confirmer** la fin de la communication et de **libérer** les ressources réseau utilisées par la connexion.



## *Le protocole UDP :*

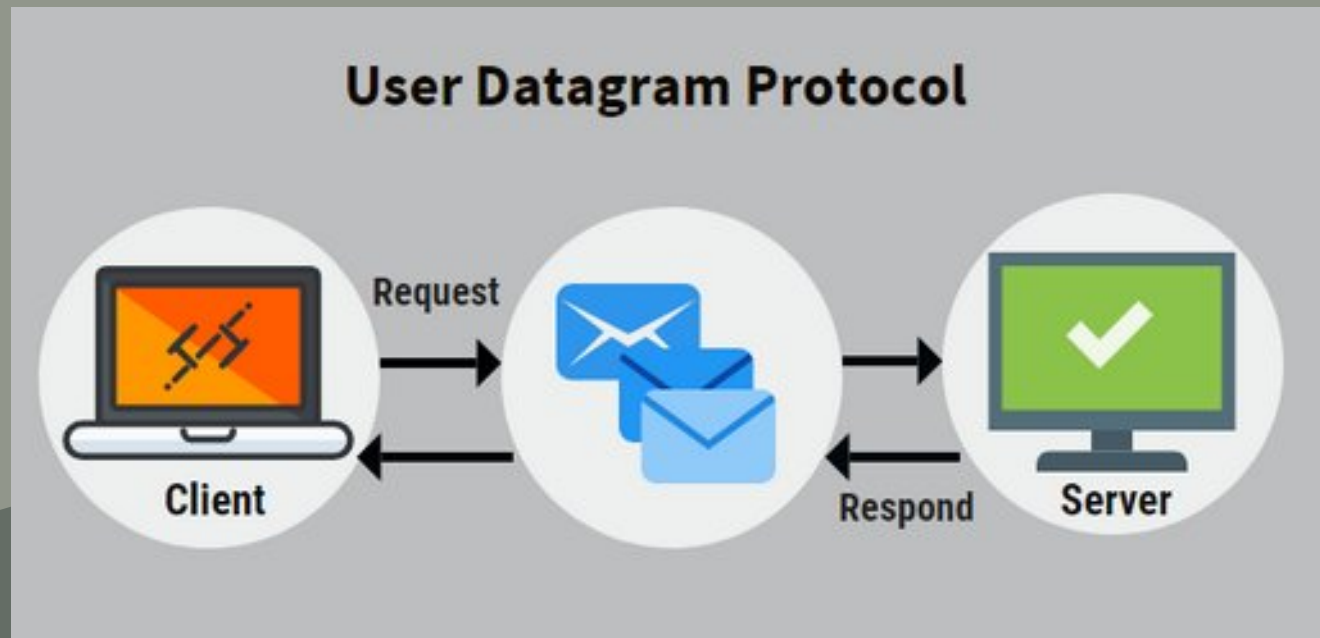
Le UDP pour User Datagram Protocol, est un protocole permettant l'envoi sans connexion de datagrammes (paquets de données) dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP.

Contrairement à TCP, UDP est un protocole non orienté connexion qui ne garantit pas la fiabilité de la transmission. Il est souvent utilisé pour les applications où la rapidité et l'efficacité sont plus importantes que la fiabilité de la transmission.

# Le fonctionnement de UDP

Le principe de fonctionnement d'UDP est simple. Lorsqu'un paquet de données est envoyé, il est divisé en datagrammes, chacun étant transmis individuellement et sans qu'il y ait d'établissement préalable d'une connexion. Chaque datagramme est accompagné d'un numéro de port source et de destination, qui permettent aux machines de savoir à quelle application destinataire le datagramme doit être transmis.

UDP ne fournit pas de mécanismes de contrôle de flux, de congestion ou de retransmission des datagrammes perdus ou corrompus. Cela signifie qu'il est possible que des datagrammes soient perdus en cours de route, ou qu'ils arrivent dans le désordre ou en double à la destination. Pour ces raisons, UDP est souvent utilisé pour les applications telles que les jeux en ligne, la diffusion de vidéos en temps réel ou la communication vocale sur IP, où la vitesse de transmission est plus importante que la fiabilité.



## *Le protocole SCTP :*

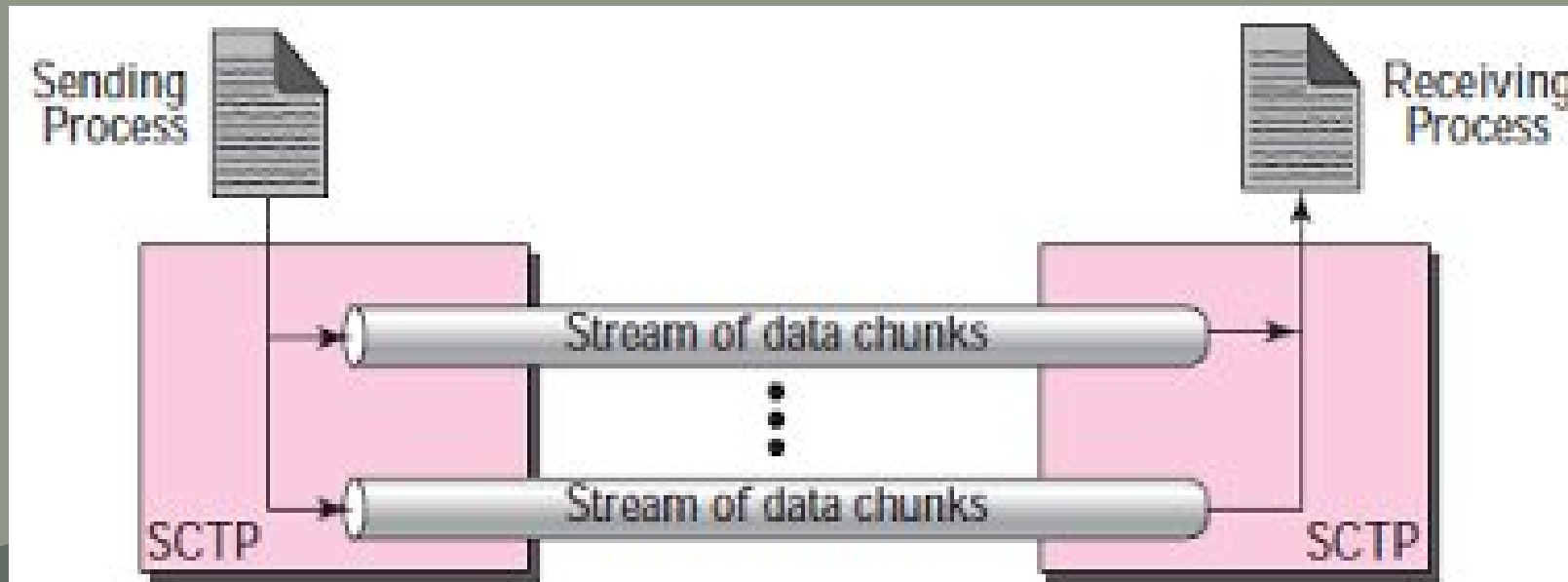
SCTP (Stream Control Transmission Protocol) est un protocole de transport de la couche de transport du modèle TCP/IP. Il a été développé pour fournir une alternative à TCP et à UDP, offrant une transmission fiable et efficace des données tout en étant mieux adapté aux applications modernes telles que la voix sur IP (VoIP) et les communications temps réel.


## fonctionnement de SCTP :

Le principe de fonctionnement de SCTP est similaire à celui de TCP, avec l'établissement d'une connexion à quatre voies entre les machines source et destination. Cependant, SCTP divise les données en plusieurs flux indépendants qui peuvent être transmis simultanément, ce qui permet d'optimiser la transmission des données pour les applications à plusieurs flux, comme la voix sur IP.

SCTP utilise également des mécanismes de contrôle de flux et de congestion pour éviter la surcharge du réseau et garantir une transmission fluide et efficace des données. En outre, SCTP dispose de fonctionnalités supplémentaires telles que la détection d'erreurs et la retransmission des données manquantes, qui offrent une fiabilité accrue par rapport à UDP.

SCTP est également capable de gérer des connexions multiples entre les mêmes machines source et destination, ce qui est particulièrement utile pour les applications de tolérance aux pannes ou de haute disponibilité. SCTP peut également être utilisé avec des mécanismes de sécurité tels que le chiffrement et l'authentification pour une transmission sécurisée des données.



The background features a large, dark brown organic shape on the left containing the text. To its right is a large, muted olive-green shape. In the top left corner, there are stylized, light grey foliage elements. At the bottom, thin, light orange wavy lines cross the frame.

## 4. Couche Application

# Définition

La couche applicative du modèle OSI est la couche supérieure responsable de l'interaction entre l'application et le réseau sous-jacent. Dans le modèle TCP/IP, la couche applicative est la couche la plus élevée et est responsable des protocoles de communication entre les applications sur les ordinateurs. Cette couche inclut des protocoles tels que HTTP, DNS et FTP.



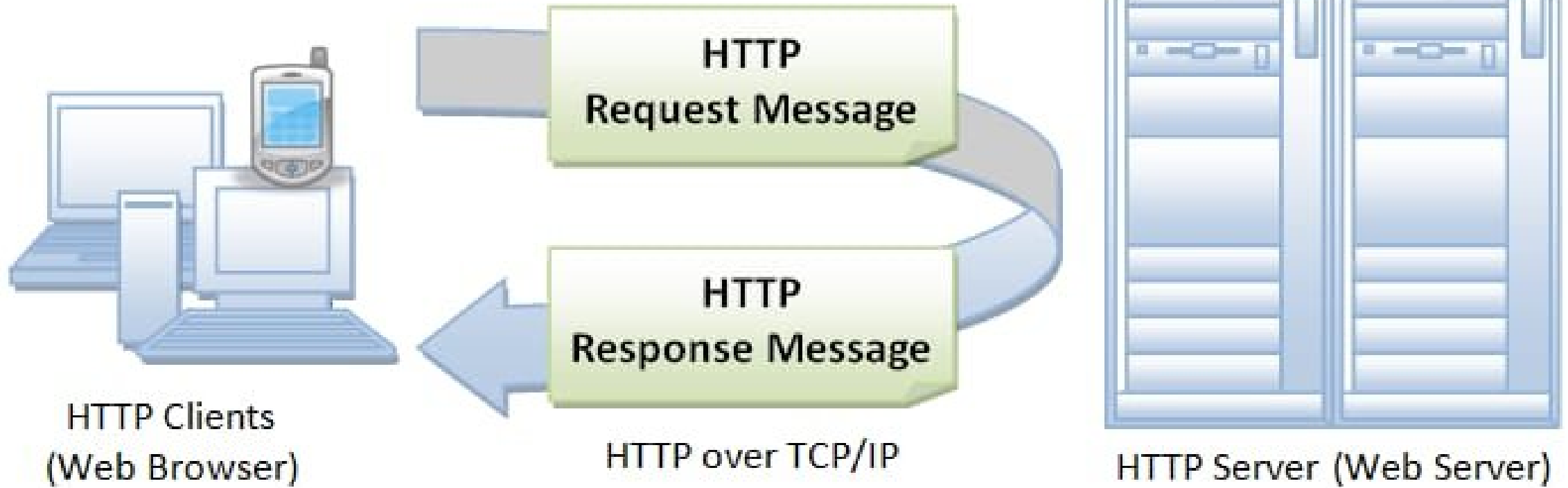
# HTTP

Le protocole HTTP (Hypertext Transfer Protocol) est le protocole le plus couramment utilisé sur le Web pour transférer des données hypertexte, telles que des pages Web, entre les serveurs Web et les navigateurs Web. Il utilise le port 80 pour communiquer. Le principe de fonctionnement du protocole HTTP est le suivant :

Le navigateur envoie une requête HTTP au serveur Web pour récupérer la page demandée.

Le serveur Web envoie une réponse HTTP contenant la page demandée.

Le navigateur affiche la page à l'utilisateur.



# DNS

Le protocole DNS (Domain Name System) est un protocole utilisé pour résoudre les noms de domaine en adresses IP. Il permet aux utilisateurs d'accéder à des sites Web en utilisant des noms de domaine facilement mémorisables plutôt que des adresses IP numériques. Les serveurs DNS conservent une base de données de noms de domaine et de leurs adresses IP correspondantes. Le principe de fonctionnement du protocole DNS est le suivant :

Le navigateur envoie une requête DNS pour résoudre le nom de domaine en adresse IP.

Les serveurs DNS recherchent le nom de domaine dans leur base de données et renvoient l'adresse IP correspondante.

Le navigateur utilise l'adresse IP pour se connecter au serveur Web et récupérer la page demandée.

# FTP


Le protocole FTP (File Transfer Protocol) est utilisé pour transférer des fichiers entre des ordinateurs sur un réseau. Il utilise le port 21 pour les commandes de contrôle et le port 20 pour les données de fichier. Il permet aux utilisateurs de télécharger et de téléverser des fichiers sur des serveurs FTP. Le principe de fonctionnement du protocole FTP est le suivant :

- Le client FTP se connecte au serveur FTP en utilisant le protocole FTP.

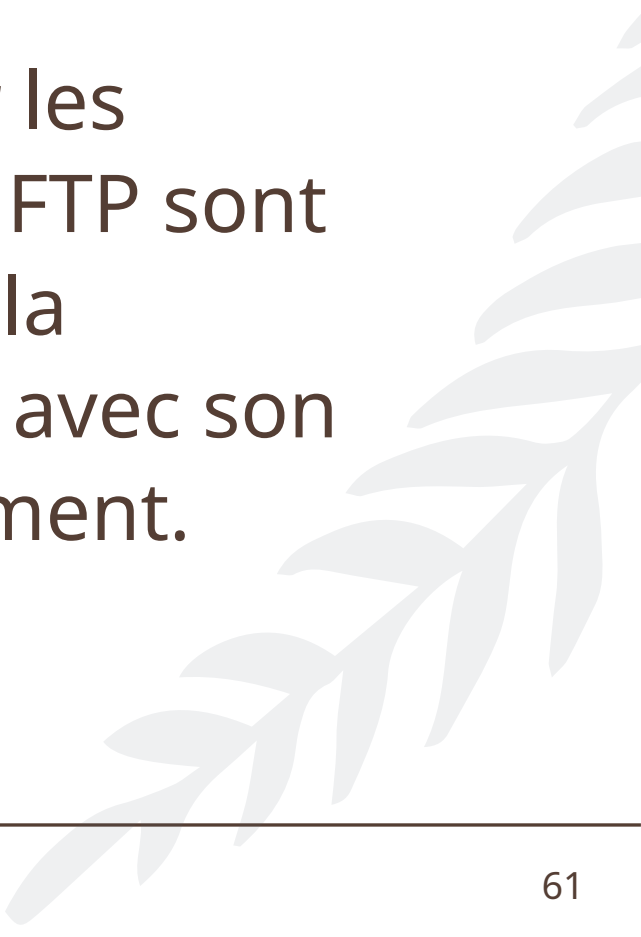
- Le client envoie une commande pour transférer un fichier.

- Le serveur répond avec une confirmation ou une erreur.

- Si la commande est confirmée, les données du fichier sont transférées sur le port 20.



En résumé, la couche applicative du modèle OSI et du modèle TCP/IP est essentielle pour la communication entre les applications sur les ordinateurs. Les protocoles HTTP, DNS et FTP sont des exemples de protocoles utilisés pour la communication sur cette couche, chacun avec son propre objectif et principe de fonctionnement.



# CONCLUSION

le modèle TCP/IP est un outil clé pour les professionnels de l'informatique et les utilisateurs d'Internet pour faciliter la communication efficace entre les périphériques connectés, et pour permettre le développement de nouvelles technologies de communication.



**Merci pour  
votre  
attention**