

Introduction aux Adresses IP

Coucou tout le monde ! Voici un petit récap de ce qu'on a appris en cours sur les Adresses IP

- Qu'est-ce qu'une Adresse IP ? ☐☐
- Comment Fonctionnent les Adresses IP ? ☐☐
- Le masque de sous-réseau (netmask) ☐☐
- Serveurs DHCP (Dynamic Host Configuration Protocol) ☐☐
- Serveurs DNS (Domain Name System) ☐☐
- Le Modèle OSI (Open Systems Interconnection) ☐☐

Qu'est-ce qu'une Adresse IP



Une adresse IP est un numéro unique attribué à chaque appareil connecté à un réseau informatique utilisant le protocole IP (Internet Protocol) pour communiquer, C'est un peu comme un numéro de téléphone unique pour chaque machine Il en existe deux types d'adresses IP :

1. IPv4 :

- C'est le format le plus courant, il est composé de 4 groupes de nombres (allant de 0 à 255) séparés par des points. Par exemple : **192.168.0.1**.

Il existe 4,294,967,296 possibilités différentes pour une adresse IPv4 (Ce nombre inclut toutes les adresses possibles, y compris celles qui sont réservées pour des usages spéciaux et d'autres adresses spéciales qui ne sont pas attribuées pour une utilisation publique sur internet)

2. IPv6 :

- C'est une version plus récente pour répondre à la pénurie d'adresses IPv4. Elle utilise une combinaison de 32 chiffres et lettres, offrant un nombre quasi illimité d'adresses. Par exemple : **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.

Il y'a plusieurs moyens de savoir son IP actuelle, voici un exemple pour chaque système d'exploitation :

Windows

1. Utiliser l'invite de commandes :

- Appuyez sur **Windows + R** pour ouvrir la boîte de dialogue Exécuter.
- Tapez **cmd** et appuyez sur **Entrée** pour ouvrir l'invite de commandes.
- Dans l'invite de commandes, tapez **ipconfig** et appuyez sur **Entrée**.
- Cherchez la section "Carte Ethernet" ou "Carte sans fil" pour trouver votre adresse IP.

2. Via les Paramètres :

- Allez dans **Paramètres > Réseau et Internet**.
- Sélectionnez votre réseau (Wi-Fi ou Ethernet).
- Faites défiler jusqu'à "Propriétés" pour trouver les détails de votre IP.

macOS

1. Via les Préférences Système :

- Cliquez sur l'icône Apple dans le coin supérieur gauche et choisissez **Préférences Système**.
- Cliquez sur **Réseau**.
- Sélectionnez le réseau actif (Wi-Fi ou Ethernet) sur la gauche.
- Votre adresse IP s'affichera sur la droite.

2. Utiliser le Terminal :

- Ouvrez le Terminal (trouvable via Spotlight ou dans le dossier Applications > Utilitaires).
- Tapez **ifconfig** et appuyez sur **Entrée**.
- Cherchez **inet** sous les sections **en0** (Ethernet) ou **en1** (Wi-Fi) pour votre adresse IP.

Linux

1. Utiliser le Terminal :

- Ouvrez le terminal.
- Tapez **hostname -I** et appuyez sur **Entrée** pour une méthode rapide.
- Ou tapez **ifconfig** (vous devrez peut-être installer **net-tools** si la commande n'est pas disponible).
- Cherchez **inet** pour trouver votre adresse IP dans les informations affichées.

2. Via les Paramètres Réseau :

- Allez dans les paramètres réseau via l'interface graphique de votre distribution.
- Sélectionnez le réseau auquel vous êtes connecté.
- Regardez les détails du réseau pour trouver l'adresse IP.


Comment Fonctionnent les Adresses IP ?

<https://www.youtube.com/embed/Oc7Ts8tVjyE?si=ihH4a3IDxyK1sU1J>

Lorsque vous voulez accéder à Internet, votre appareil (ordinateur, téléphone, tablette etc.) est assigné à une adresse IP, soit par votre réseau domestique soit directement par votre fournisseur d'accès internet (FAI). Cette adresse est conçue pour permettre à votre appareil de communiquer avec d'autres appareils sur Internet, de la même manière qu'un numéro de téléphone vous permet de communiquer avec d'autres téléphones. Il se doit d'être unique, vous n'aimeriez pas envoyer un message à votre patron alors que vous vouliez l'envoyer à votre ami, cela fonctionne de la même manière.

Dans un Réseau Local (comme votre maison ou bureau) :

Les appareils reçoivent des adresses IP privées, généralement attribuées par le routeur (votre box Internet à la maison). Ces adresses ne sont pas routables sur Internet et servent uniquement à la communication interne au réseau.

 Dans les réseaux informatiques, certaines plages d'adresses IP sont réservées pour un usage privé. Ces adresses ne sont pas routables sur Internet, ce qui signifie qu'elles ne sont pas destinées à être utilisées sur le réseau public mondial. Au lieu de cela, elles sont utilisées dans les réseaux locaux (comme les réseaux domestiques, d'entreprise, ou d'écoles). Voici les trois plages principales d'adresses IP privées définies par les standards IPv4 :

Plage 10.0.0.0 à 10.255.255.255 :

Cette plage permet un très grand nombre d'adresses IP privées (environ 16 millions). Elle est souvent utilisée dans de grands réseaux, comme ceux des entreprises ou des universités.

Plage 172.16.0.0 à 172.31.255.255 :

Cette plage offre environ 1 million d'adresses IP privées. Elle est couramment utilisée dans les réseaux de taille moyenne. Cela comprend 16 blocs de réseaux distincts (de 172.16.0.0 à

172.31.0.0).

Plage 192.168.0.0 à 192.168.255.255 :

Cette plage est la plus utilisée dans les réseaux domestiques et les petits bureaux. Elle fournit jusqu'à 65,536 adresses IP privées

“ Pour qu'un appareil avec une adresse IP privée communique avec Internet, il utilise un processus appelé NAT (Network Address Translation) sur un routeur. Le NAT traduit l'adresse IP privée en une adresse IP publique pour la communication sur Internet, et vice versa pour les réponses entrantes.

Sur Internet :

Votre routeur utilise une adresse IP publique attribuée par votre fournisseur d'accès Internet (FAI). Cette adresse est visible sur Internet et permet à vos appareils de communiquer avec les autres appareils dans le “Monde extérieur” (WAN : Wide Area Network)

Adresses Dynamiques et Statiques

Dynamique :

La plupart des appareils reçoivent des adresses IP dynamiques qui peuvent changer à chaque connexion au réseau. Tout ça est géré par le DHCP (Dynamic Host Configuration Protocol) de votre routeur.

Statique :

Certains appareils nécessitent une adresse IP statique qui ne doit pas changer sinon certaines applications risquent de mal fonctionner (comme des serveurs, des imprimantes en réseau, etc.) Il faut paramétrer manuellement sur le routeur ces adresses statiques et elles seront toujours assignées pour cet appareil en particulier.

Le masque de sous-réseau (netmask)

<https://www.youtube.com/embed/3Scbl-D5rpM>

Chaque adresse IP est composée de deux parties : l'identifiant du réseau et l'identifiant de l'hôte (vos appareils). Le masque de sous-réseau aide à déterminer où se termine la partie réseau et où commence la partie hôte dans une adresse IP.

Comment fonctionne un masque de sous réseau ?

Le format du masque de sous réseau est exprimé en termes d'adresses IP avec des nombres allant de 0 à 255, tout comme une adresse IP standard. Par exemple un masque de sous-réseau commun pour les réseaux domestiques est 255.255.255.0

Classes d'adresses	Bits utilisés pour le masque de sous-réseau				Notation décimale
Classe A	1111 1111	0000 0000	0000 0000	0000 0000	
Classe B	1111 1111	1111 1111	0000 0000	0000 0000	
Classe C	1111 1111	1111 1111	1111 1111	0000 0000	

Dans l'adresse IP, les bits correspondant à **255** dans le masque de sous-réseau représentent la partie réseau, tandis que les bits correspondants à **0** représentent la partie hôte. Par exemple avec un masque de **255.255.255.0** et une adresse IP comme **192.168.1.15**, la partie réseau est **192.168.1** et la partie hôte est **15**

En modifiant le masque de sous-réseau, un réseau peut être divisé en plusieurs sous-réseaux plus petits. Cela peut permettre une meilleure organisation, une meilleure sécurité ou bien une utilisation plus efficace des adresses IP.

□□□□ Imaginez un réseau comme un grand immeuble avec plein d'appartements (les adresses IP). Au départ, avec le masque de sous-réseau 255.255.255.0, notre immeuble a une seule grande section pouvant accueillir 254 appartements (ou appareils), numérotés de 192.168.1.1 à 192.168.1.254.

Maintenant, si nous changeons le masque de sous-réseau en 255.255.255.128, c'est comme si nous construisions un mur au milieu de l'immeuble, créant ainsi deux sections plus petites :

Première Section (Sous-réseau 1) :

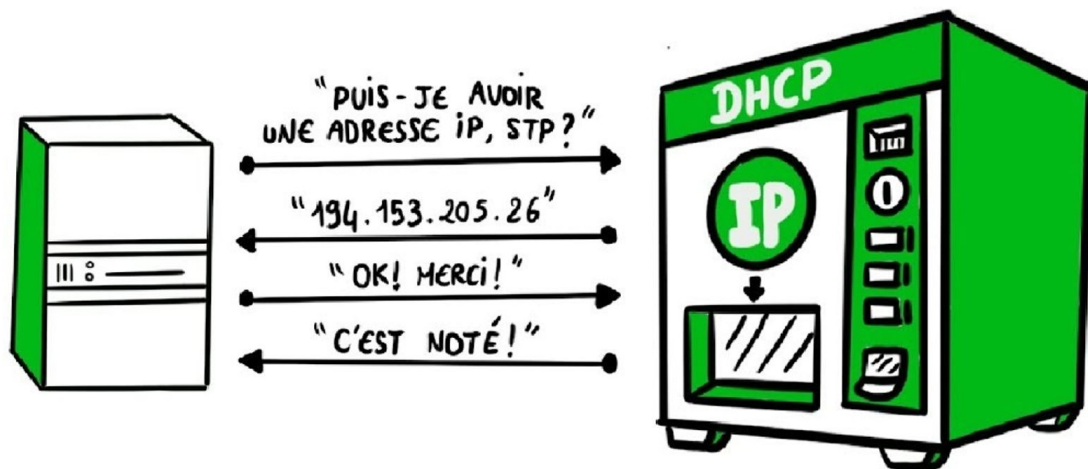
Elle a maintenant des appartements numérotés de 192.168.1.1 à 192.168.1.126. Donc, elle peut accueillir 126 appareils différents.

Deuxième Section (Sous-réseau 2) :

Elle a des appartements numérotés de 192.168.1.129 à 192.168.1.254, pouvant aussi accueillir 126 appareils différents.

En faisant ce changement de masque, nous avons divisé un grand réseau en deux plus petits, facilitant ainsi la gestion et l'organisation du réseau, un peu comme diviser un grand bureau en deux départements plus petits pour une meilleure organisation.

Serveurs DHCP (Dynamic Host Configuration Protocol)



Le serveur DHCP joue un rôle crucial dans l'attribution des adresses IP au sein des réseaux locaux (comme le réseau de votre maison ou bien celui de votre entreprise).

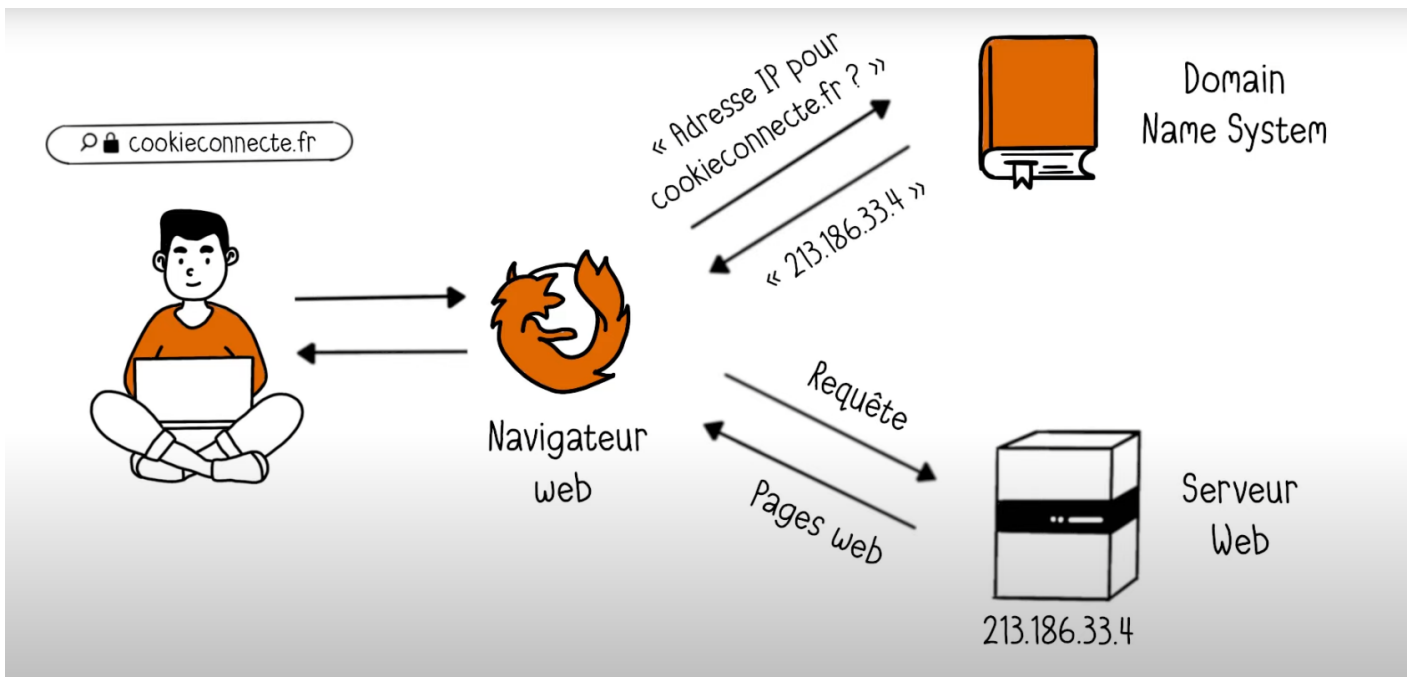
- **Attribution d'Adresses IP :**

- Lorsqu'un appareil se connecte à un réseau, il envoie une requête au serveur DHCP. Le serveur sélectionne alors une adresse IP disponible dans sa gamme d'adresses et l'attribue à l'appareil pour une durée déterminée (bail DHCP).

- **Simplification de la Gestion Réseau :**

- Sans DHCP, les adresses IP devraient être attribuées manuellement, ce qui serait vachement peu pratique et source d'erreurs dans les grands réseaux. Le DHCP assure une gestion automatique et efficace des adresses IP, réduisant les conflits d'adresses et simplifiant l'administration réseau.

Serveurs DNS (Domain Name System) ☐☐



Le DNS est souvent comparé à un annuaire téléphonique pour Internet. Les serveurs DNS sont très importants pour convertir les noms de domaine faciles à retenir (comme www.google.com) en adresses IP numériques que les ordinateurs peuvent comprendre et utiliser pour la communication.

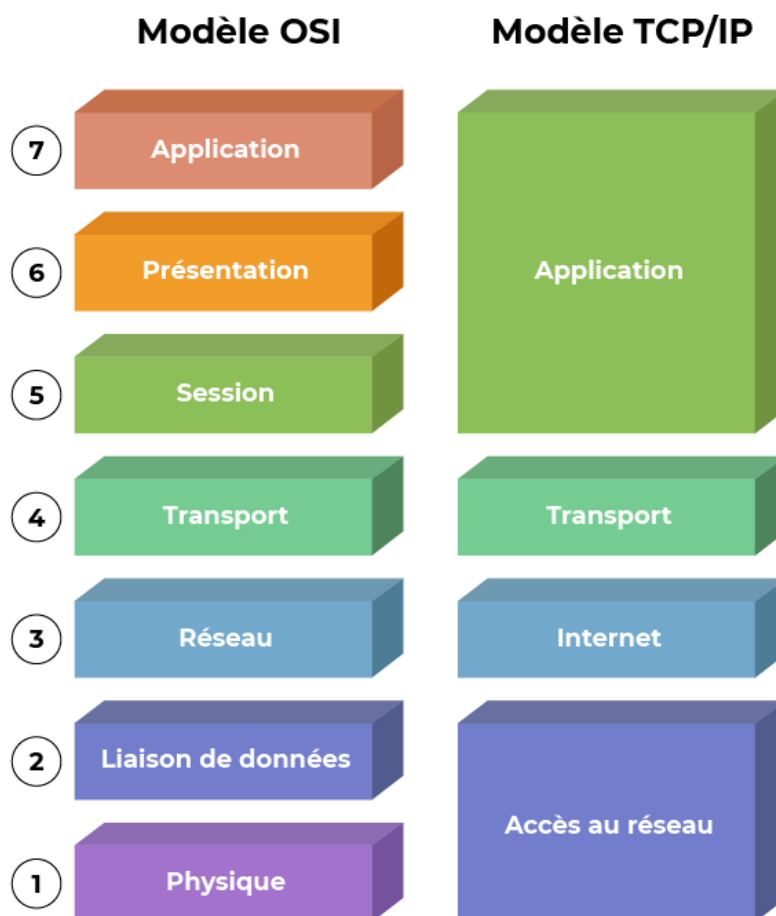
- **Fonctionnement :**

- Lorsque vous tapez une adresse web dans votre navigateur, votre appareil demande au serveur DNS de traduire ce nom en adresse IP. Le serveur DNS consulte sa base de données pour trouver l'adresse IP correspondante et la renvoie à votre appareil pour établir la connexion. C'est en fait une sorte de gros annuaire de l'internet

☐☐☐☐ Les serveurs DNS sont organisés en une structure hiérarchique. Si un serveur DNS local (fichier hosts) ne connaît pas l'adresse IP d'un domaine, il demande à un serveur DNS de niveau supérieur (celui du FAI ou bien entré manuellement), et ainsi de suite, jusqu'à obtenir la réponse

Le Modèle OSI (Open Systems Interconnection) ☐☐

<https://www.youtube.com/embed/26jazyc7VNk>



Le modèle OSI est une façon d'expliquer comment les réseaux informatiques fonctionnent. Il divise le processus en 7 étapes, ou "couches", chacune ayant son propre rôle dans la communication entre les ordinateurs. Voici une explication simplifiée de chaque couche :

1. Couche Physique :

- Elle s'occupe de la transmission physique des données (sous forme de signaux électriques, lumineux ou radio) à travers les câbles, fibres optiques, etc.

“ C’est comme si vous écriviez une lettre que vous souhaiteriez envoyer à quelqu’un

2. **Couche de Liaison de Données :**

- Gère la transmission des données entre deux appareils directement connectés et s'occupe des adresses physiques (adresses MAC).

“ Imaginez que vous écrivez sur votre enveloppe, pour être certain que votre lettre arrive à destination et qu’elle n’arrive pas chez quelqu’un d’autre ou soit perdue et que vous mettiez la lettre dans cette enveloppe

3. **Couche Réseau :**

- Responsable du routage des paquets de données à travers différents réseaux (utilise les adresses IP).

“ C’est comme si vous mettiez maintenant cette enveloppe dans la boîte à lettre du facteur.

4. **Couche Transport :**

- Assure la transmission fiable des données d'un point à un autre (gestion des erreurs, contrôle de flux, etc.).

“ Le facteur vient relever le courrier et se charge que le destinataire reçoive bien votre lettre le plus rapidement possible, il fait donc transporter la lettre avec le moyen de transport le plus rapide et le plus adapté

5. **Couche Session :**

- Gère les sessions de communication entre les applications (ouverture, gestion, fermeture de sessions).

“ Cette couche se charge que vous puissiez bien communiquer entre vous, en laissant la possibilité de vous répondre par “lettres” si besoin

6. **Couche Présentation :**

- Traduit les données entre les formats utilisés par les applications et le réseau (cryptage, compression, etc.).

Cette couche fais en sorte de traduire votre lettre dans la langue du correspondant pour être sûr et certain qu'il va bien comprendre le contenu de la lettre

7. **Couche Application :**

- Niveau le plus proche de l'utilisateur, où se trouvent les applications de réseau comme les navigateurs web, les clients de messagerie, etc.

“ Ca y'est ! Votre destinataire a reçu la lettre

Le Modèle TCP/IP

Le modèle TCP/IP est plus pratique et couramment utilisé pour la communication sur Internet. Il est plus simplifié que le modèle OSI et se compose de quatre couches :

1. **Couche d'Accès Réseau :**

- Équivalente aux deux premières couches de l'OSI. Elle gère la transmission physique et l'accès au média réseau.

2. **Couche Internet :**

- Similaire à la couche Réseau de l'OSI. Elle s'occupe du routage des paquets de données à travers divers réseaux.

3. **Couche Transport :**

- Comme dans OSI, elle s'assure que les données sont transmises de manière fiable et ordonnée.

4. **Couche Application :**

- Fusionne les trois dernières couches de l'OSI. Cette couche est responsable des applications qui accèdent au réseau.

En résumé, le modèle OSI aide à comprendre en détail comment les réseaux fonctionnent, mais c'est le modèle TCP/IP qui est le plus utilisé, surtout pour Internet. Ces modèles rendent le processus complexe des réseaux plus simple à comprendre et à gérer.