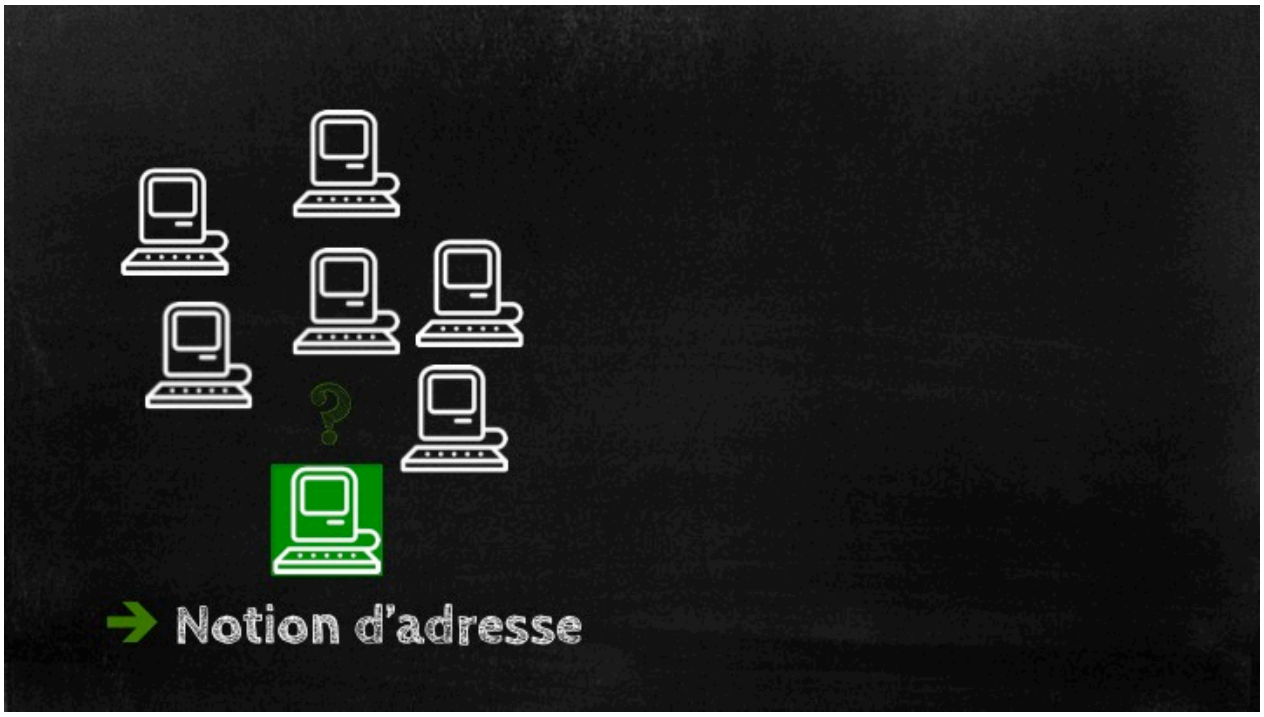
Semaine 4 : le protocole IP

Séance 1 : l'adressage

Introduction

Au cours de cette séance, nous allons parler de l'adresse. Vous avez déjà parlé de la notion d'adresse avec Laurent Toutain dans la première semaine, quand vous avez parlé de l'adresse postale qui permet de désigner une personne dans le réseau de La Poste. Nous pouvons continuer cette analogie, elle rend bien compte de ce qu'est une adresse dans le réseau. L'adresse désigne un équipement dans le réseau de façon unique.

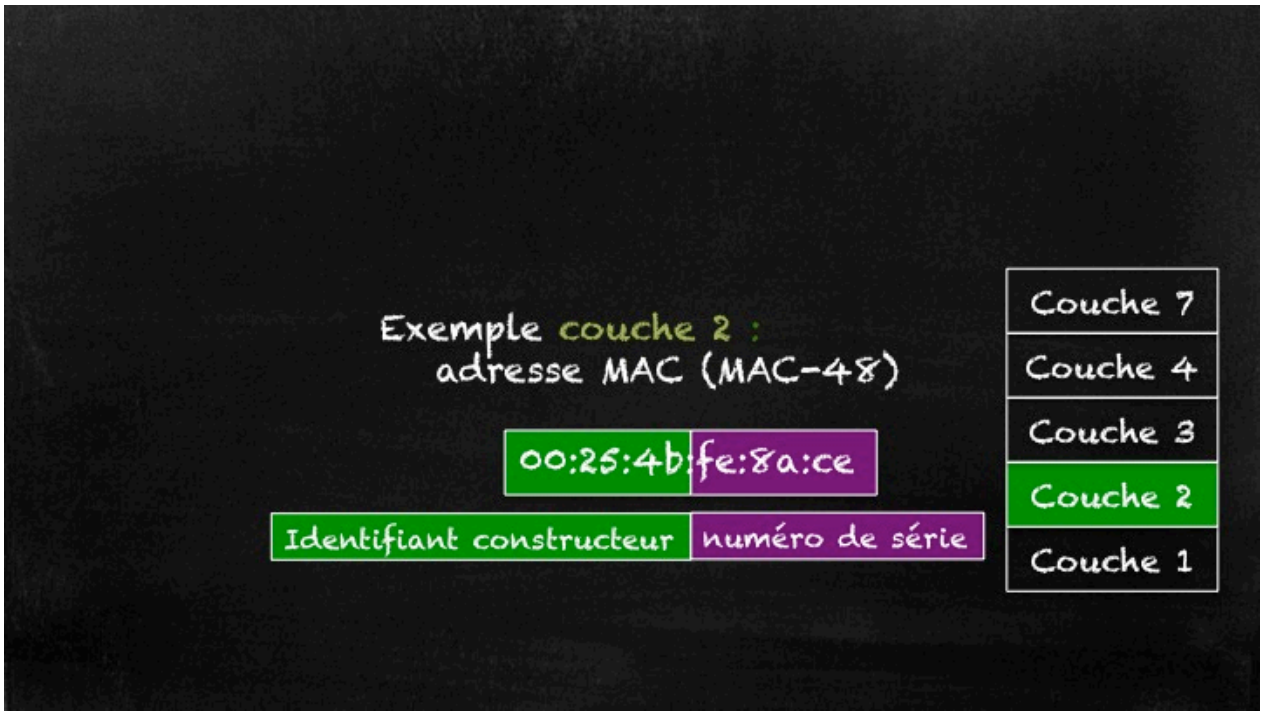
On peut commencer par se poser la question : quand a t on besoin d'une adresse ? Dans un premier cas, on peut connecter deux machines par un câble. Dans ce cas, l'adresse est inutile car quand une machine envoie un paquet, le destinataire est forcément de l'autre côté du câble.



En revanche, on aura besoin de la notion d'adresse quand il y aura plusieurs machines sur le réseau où qu'on utilisera un médium à diffusion. Dans ces cas là, cette adresse va nous permettre soit de désigner l'interlocuteur, soit de savoir où il se trouve.

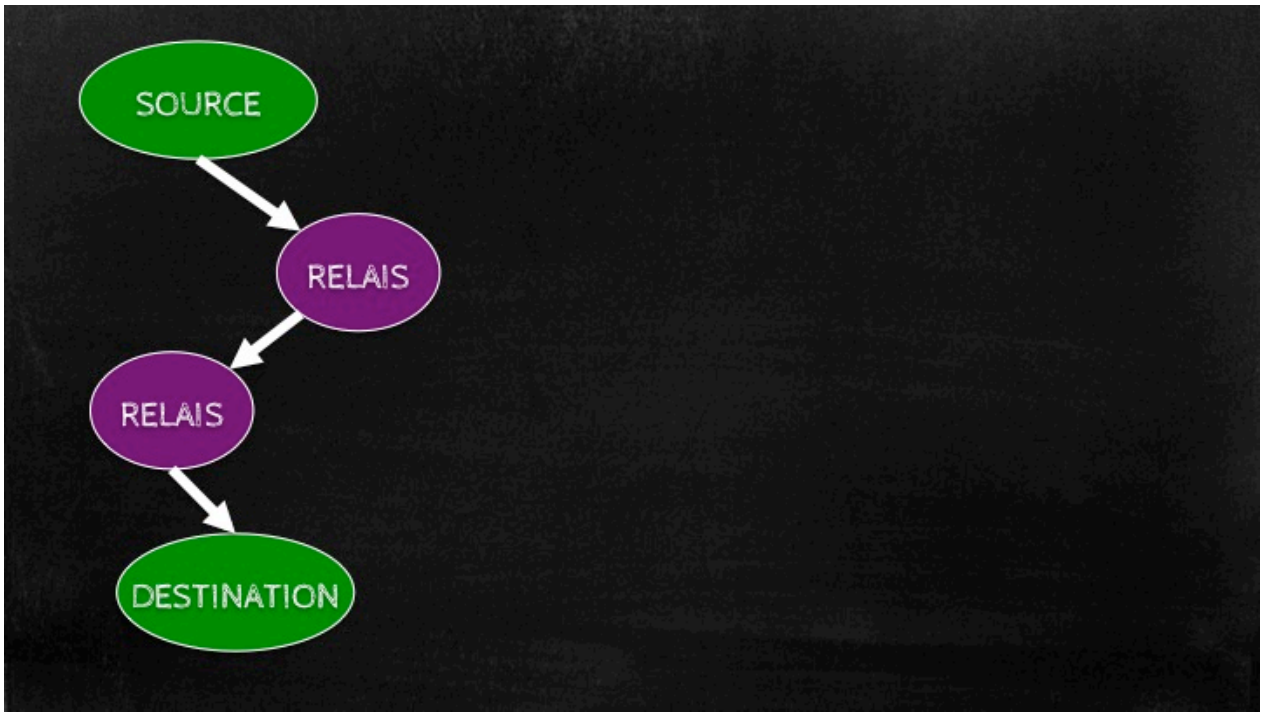
Maintenant nous allons regarder la notion d'adresse dans différents protocoles existants et en particulier, nous allons reprendre le modèle de référence OSI que vous avez vu précédemment.

On verra que la notion d'adresse va apparaître dans différentes couches de ce modèle de référence ;

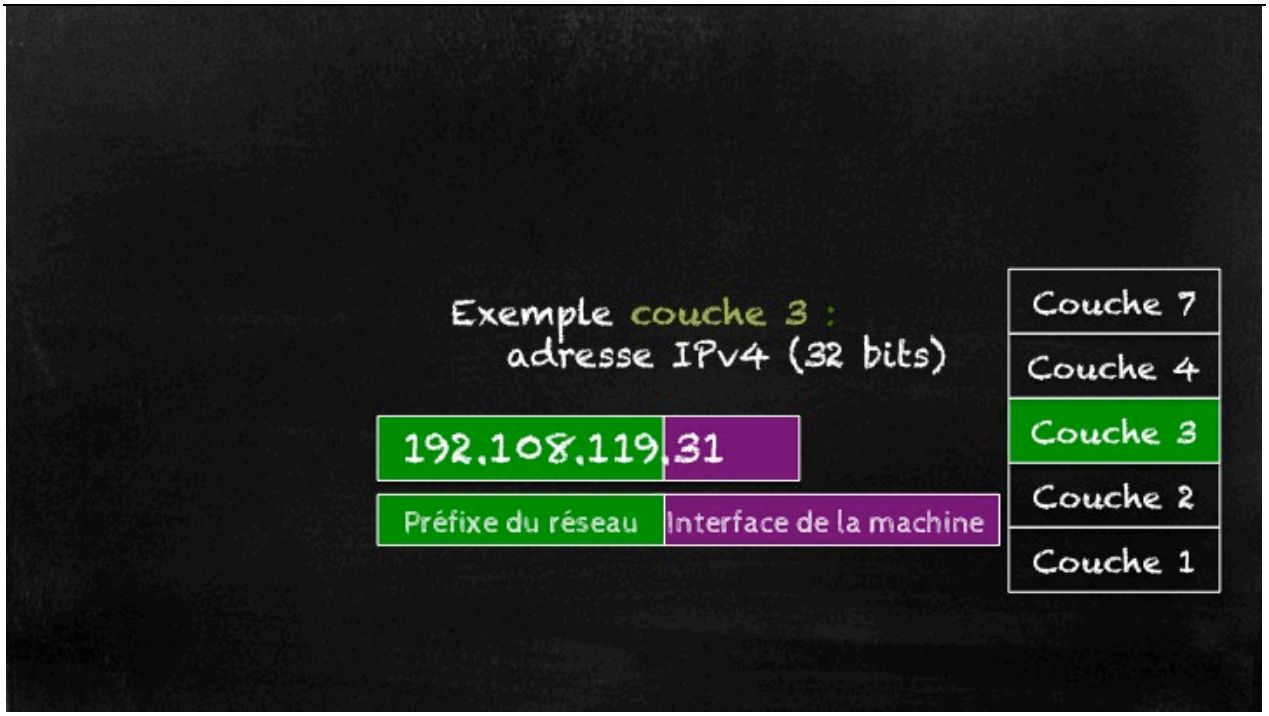


Commençons par le bas du modèle. Au niveau de la couche 2, on trouve l'adresse MAC. Cette adresse permet de désigner une interface réseau de façon unique dans le monde. Cette interface a été fabriquée par un constructeur qui va apparaître dans l'adresse MAC.

Cette adresse fait 48 bits, elle est donc sur 6 octets, et peut être divisée en 2 avec les trois premiers octets qui représentent l'identité du constructeur de la carte réseau. Les trois derniers octets constituent un numéro de série chez ce constructeur pour la carte en question. Si on regardait l'adresse MAC de mon interface réseau, vous verriez que les trois premiers octets correspondent à 00:25:4b et en cherchant sur les documentations qui sont libres sur Internet, vous pourriez voir que le constructeur est Apple.

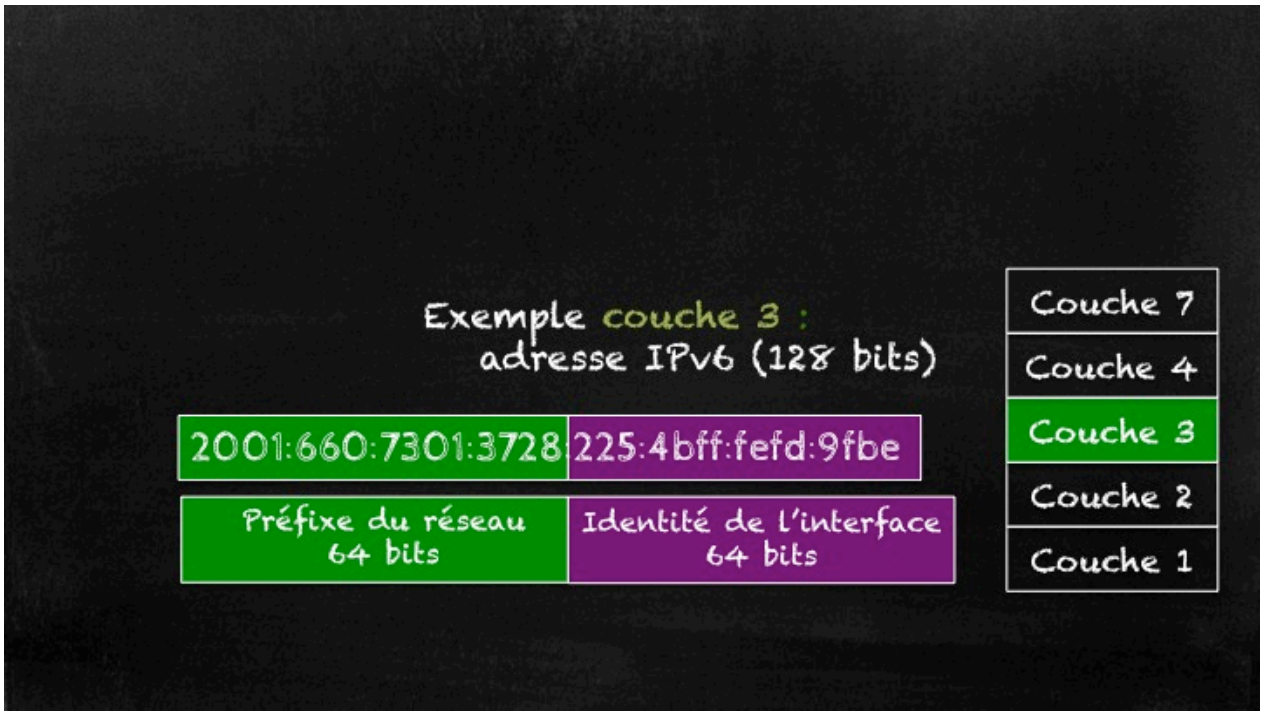


Regardons l'adresse au niveau de la couche 3. Ici, elle prend toute son importance car c'est la couche qui va introduire des relais intermédiaires pour acheminer l'information vers la destination. L'adresse va prendre différentes formes selon le protocole que l'on utilise.

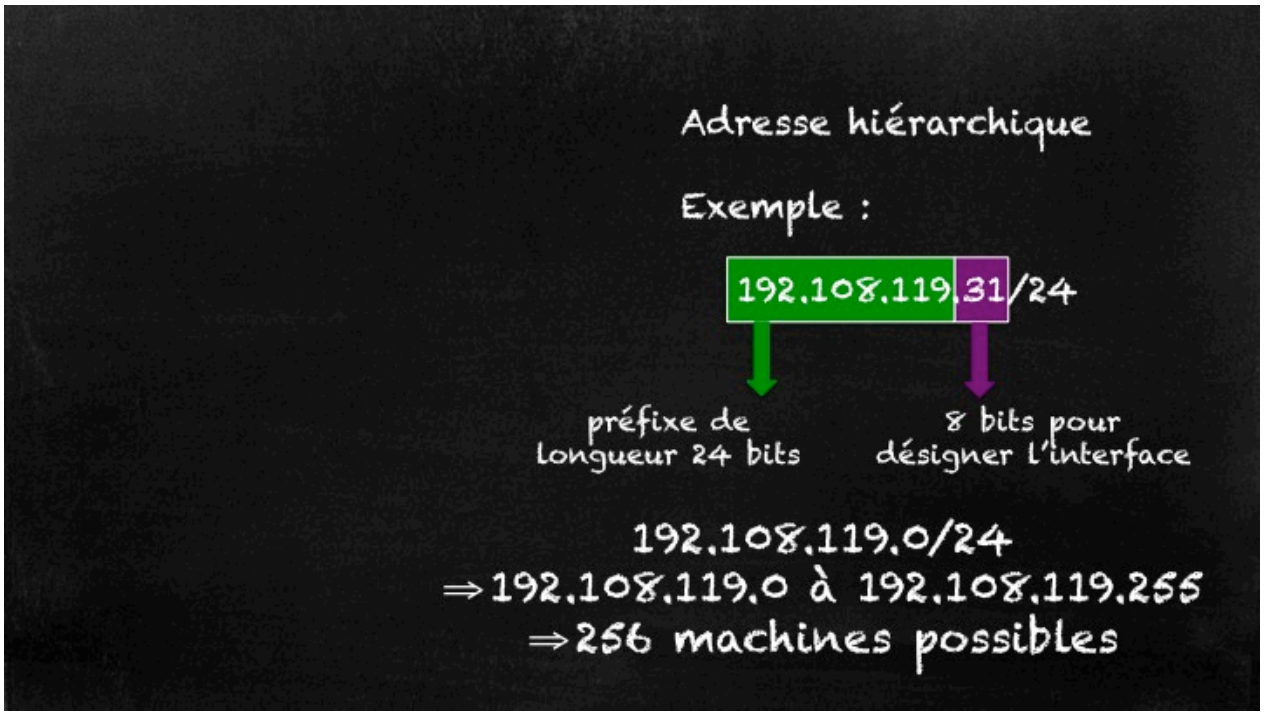


Prenons par exemple IPv4. L'adresse IPv4 fait 32 bits et si on regarde sa structure, on verra que la première partie est constituée d'un préfixe, de longueur variable (ici 24 bits), qui désigne le

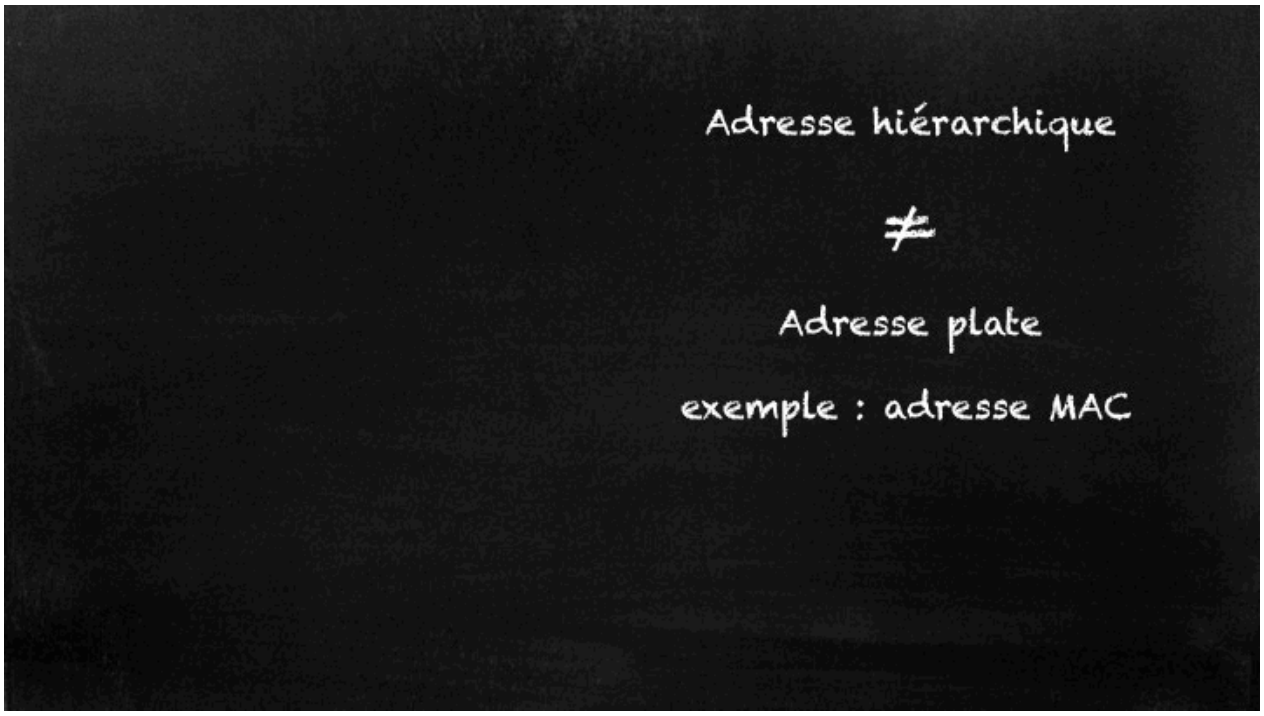
réseau sur lequel se trouve la machine. Le reste de l'adresse désigne l'interface de la machine sur ce réseau.



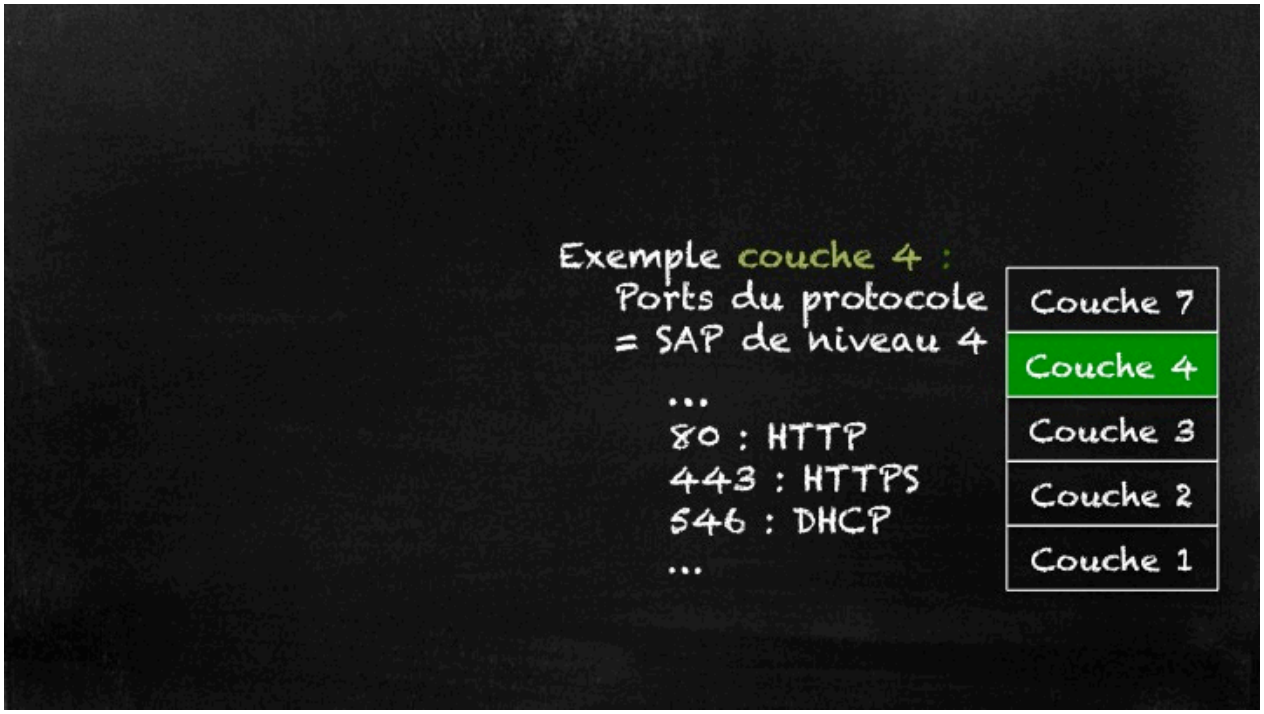
Prenons maintenant l'exemple d'IPv6. L'adresse fait 128 bits. On retrouve, en première partie, le préfixe du réseau puis 64 bits pour désigner l'interface de la machine sur le réseau.



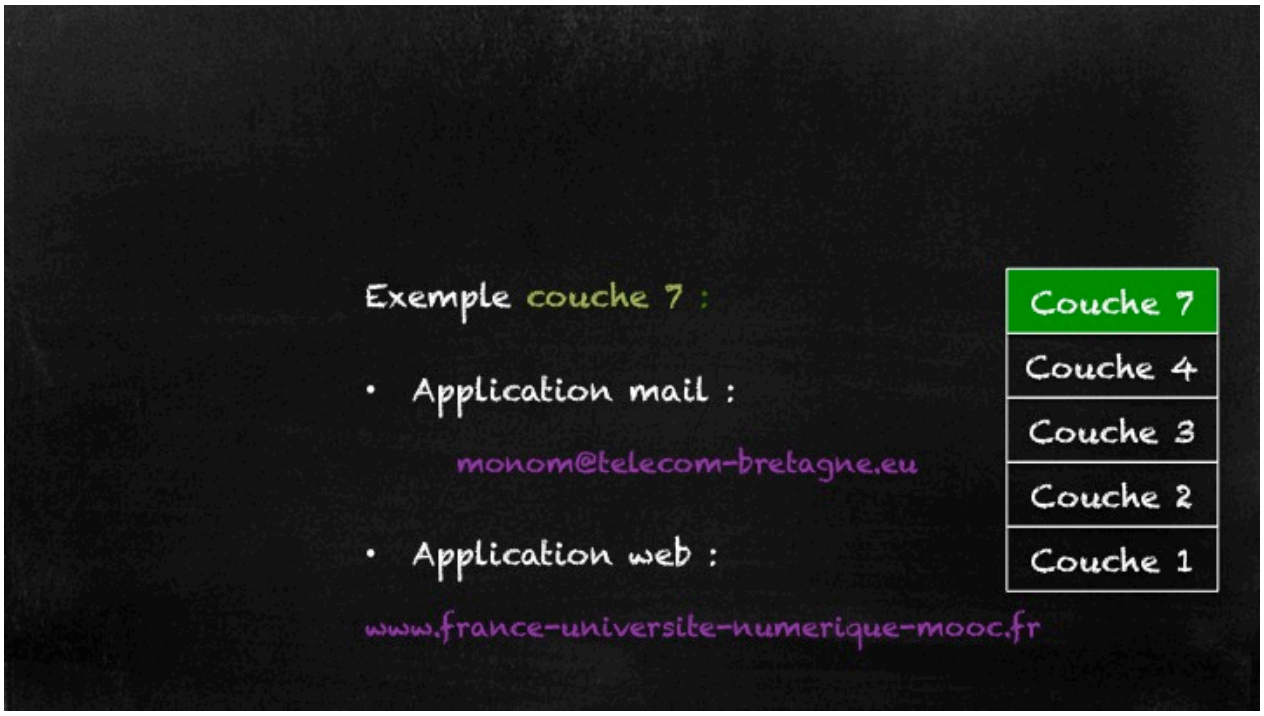
Dans ces deux cas, on peut dire que l'adresse est hiérarchique. En effet, une partie désigne le préfixe du réseau, et donc un ensemble de machines que l'on peut joindre.



Par contraste, on peut comparer avec l'adresse MAC est dite plate puisqu'elle ne désigne qu'une seule machine. En effet, s'adresser à plusieurs adresses MAC ne permet pas de définir un groupe d'utilisateurs particulier.



Dans la couche 4, on peut aussi parler d'adresse si on considère les ports qui désignent le protocole utilisé dans le niveau 4.



Au niveau 7 la forme de l'adresse dépend de l'application considérée.

Premier exemple : le mail. Quand vous écrivez un mail à quelqu'un, pour le désigner vous utilisez son adresse mail.

Second exemple : la consultation de page web. Vous désignez la page que vous souhaitez regarder en donnant on URL, ce qui correspond à son adresse pour l'application.

En résumé

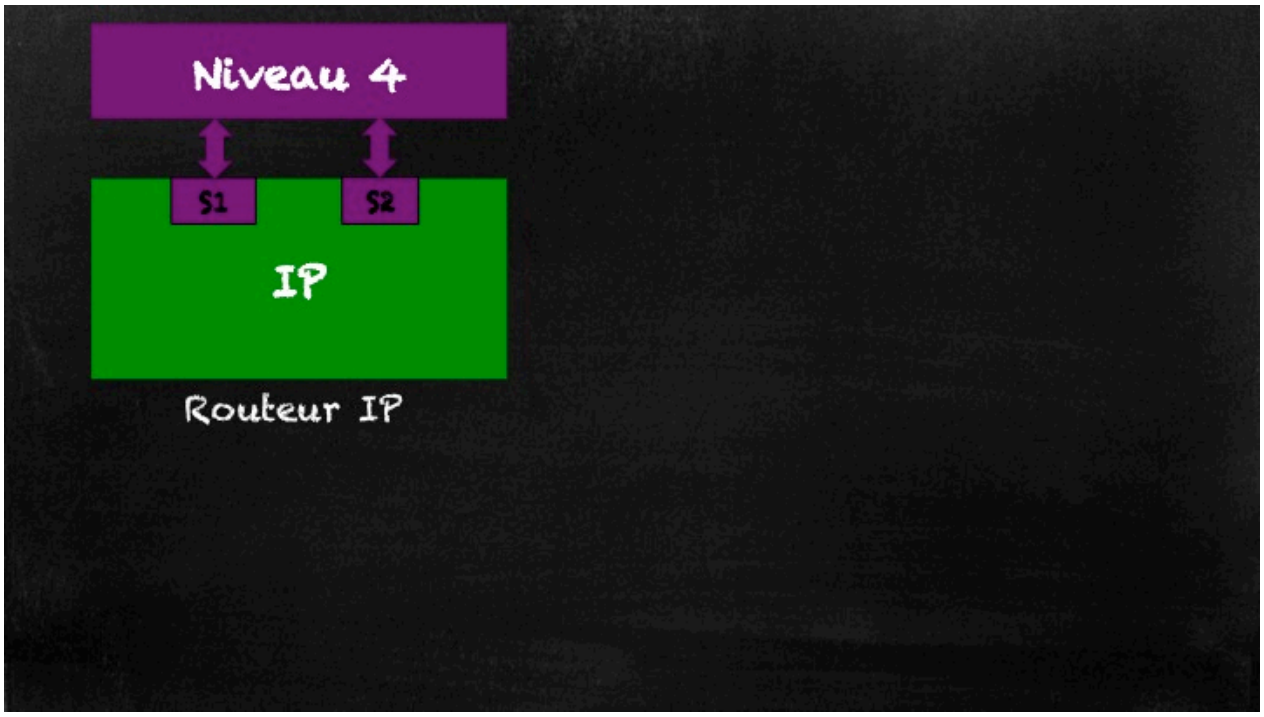
Dans cette séance, nous avons vu la notion d'adresse. Nous avons dit que la notion d'adresse désigne de façon unique une adresse ou une interface sur le réseau. Nous avons vu que l'adresse va prendre différentes formes selon le protocole que l'on va utiliser. Nous avons également vu que l'adresse peut être à la fois la désignation de l'identité d'une machine ou de sa localisation, voire les deux. Nous avons également parlé d'adresse plate ou d'adresse hiérarchique selon le fait que l'on puisse adresser un groupe de machines ou non sur le réseau.

Séance 2 : le protocole IP

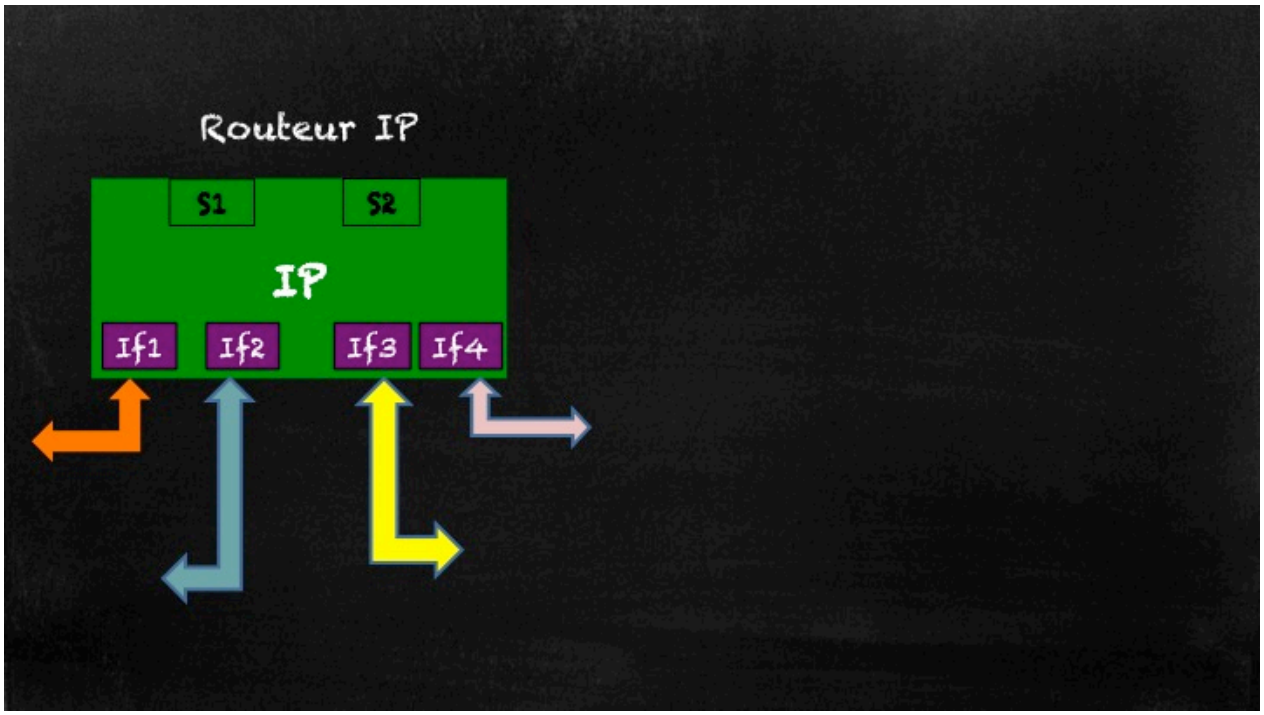
Introduction

Dans l'Internet, les communications sont acheminées grâce au protocole de niveau 3 IP : Internet Protocol. Nous allons voir son fonctionnement dans la séance d'aujourd'hui.

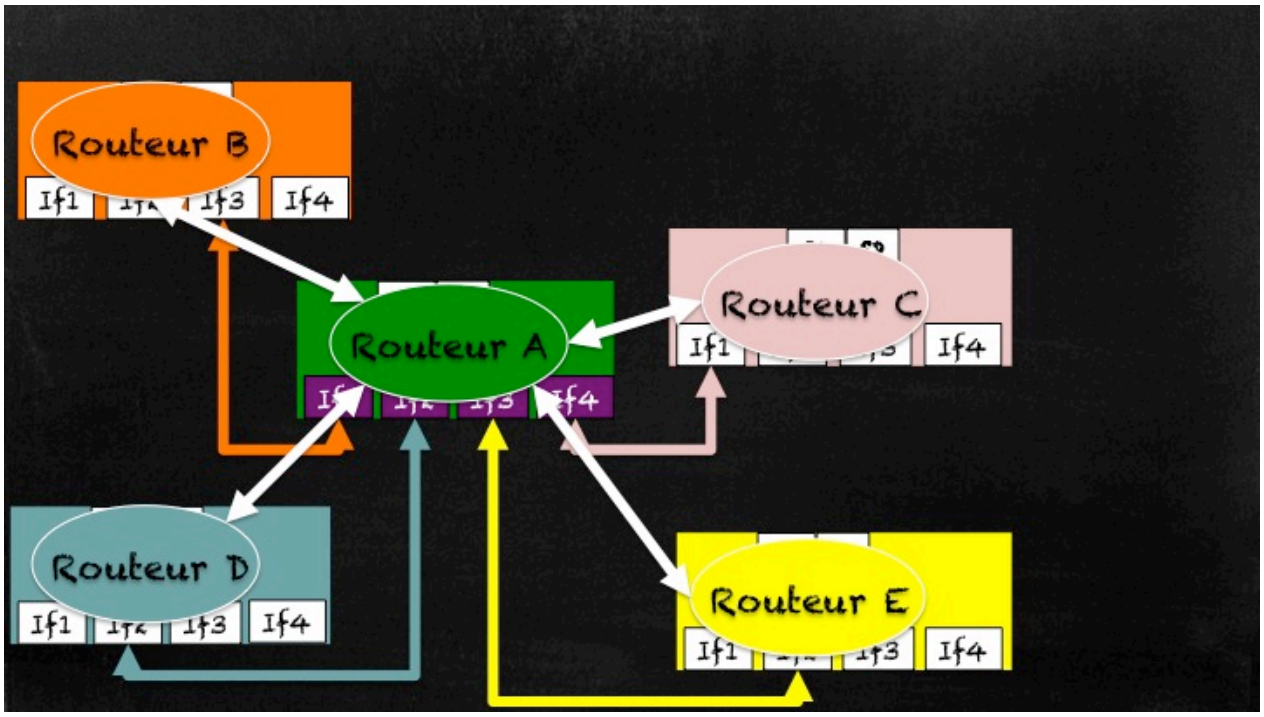
IP met en œuvre la connectivité sur l'ensemble du réseau Internet. Il offre une fonction de routage qui achemine les communications de la source à la destination en utilisant des nœuds intermédiaires qui relaient les données. On parle de communication de bout en bout.



Les équipements utilisés sont des routeurs. Ils offrent à la couche transport un service de communication entre deux machines distante en passant par des relais.

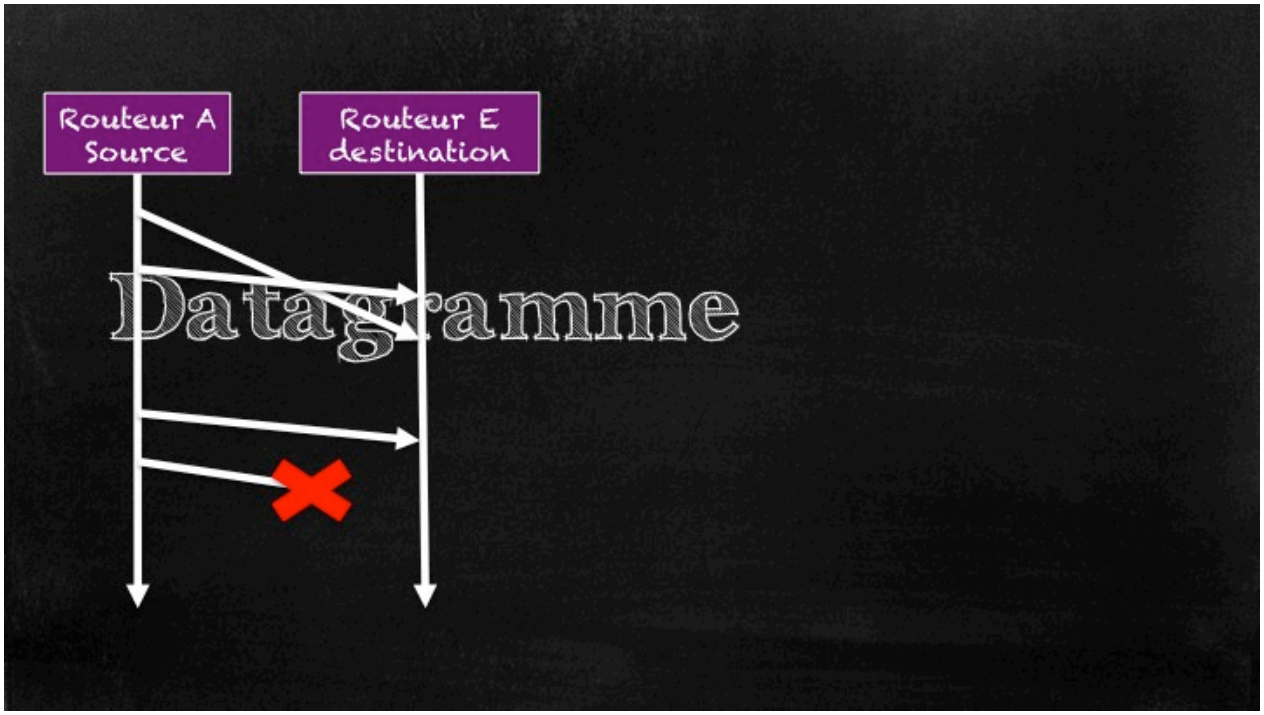


Pour faire cette communication, ils utilisent des services de niveau liaison, appelés interfaces pour dialoguer avec leurs voisins.



Un voisin est une autre entité IP avec laquelle une liaison «directe» existe grâce à au moins une interface de communication. Un équipement terminal peut se contenter d'une seule interface vers le routeur d'accès au réseau. Néanmoins de nombreuses stations disposent de plusieurs interfaces, par exemple : Ethernet, Wifi, Bluetooth...

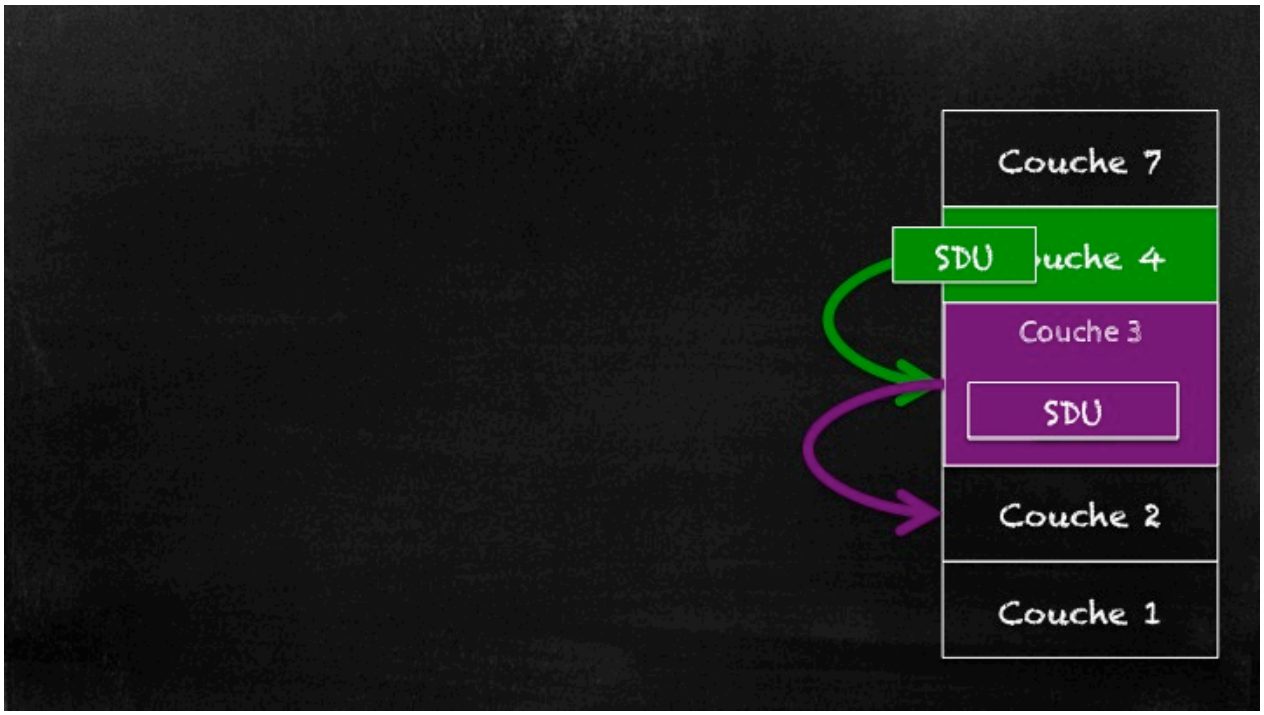
IP et le mode Datagramme



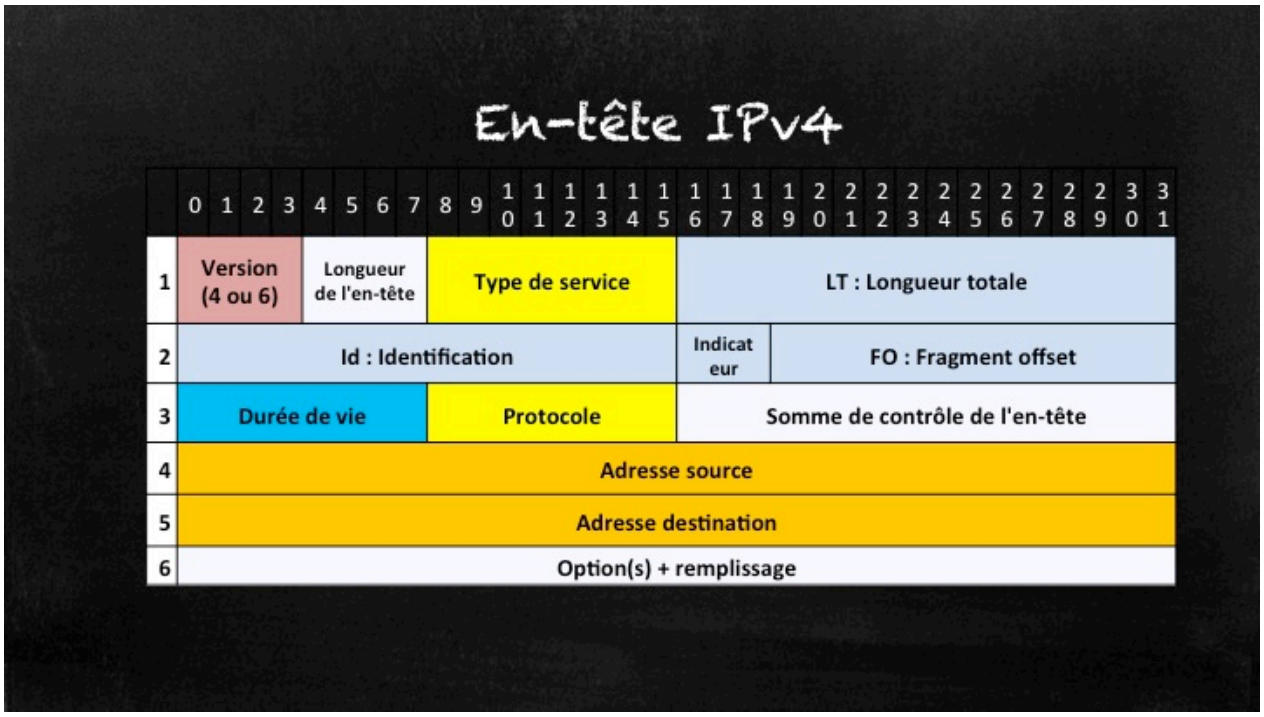
A l'instar du service postal, IP est un protocole à datagramme. Les données à envoyer sont divisées en blocs élémentaires appelés datagrammes qui sont envoyés de façon indépendante dans le réseau. Contrairement au mode connecté, dans le mode datagramme chaque unité de donnée peut être acheminée sur des chemins différents, ils peuvent donc se doubler et arriver dans un ordre différent de leur ordre de départ.

Le mode datagramme n'offre aucune fiabilisation de la communication : on peut perdre des datagrammes lors de leur acheminement.

En-tête IPv4



Comme tout protocole, IP définit un format d'échange de donnée : un PDU, appelé paquet. Le paquet IP est formé en ajoutant un en-tête devant les données soumises à travers le SDU par la couche transport.



L'en-tête IP est composé de champs de taille variable.

- **Champ Version**

Le premier champ, sur 4 bits, indique le numéro de version du protocole IP. La version majoritairement utilisée actuellement est la version 4. Une nouvelle version, la version 6, a été définie et est de plus en plus répandue. Ces deux versions ne sont pas compatibles et utilisent des formats de paquets différents, n'ayant que le champ version en commun. Dans ce cours, nous verrons le protocole IPv4 : IP en version 4.

- **Champ Longueur**

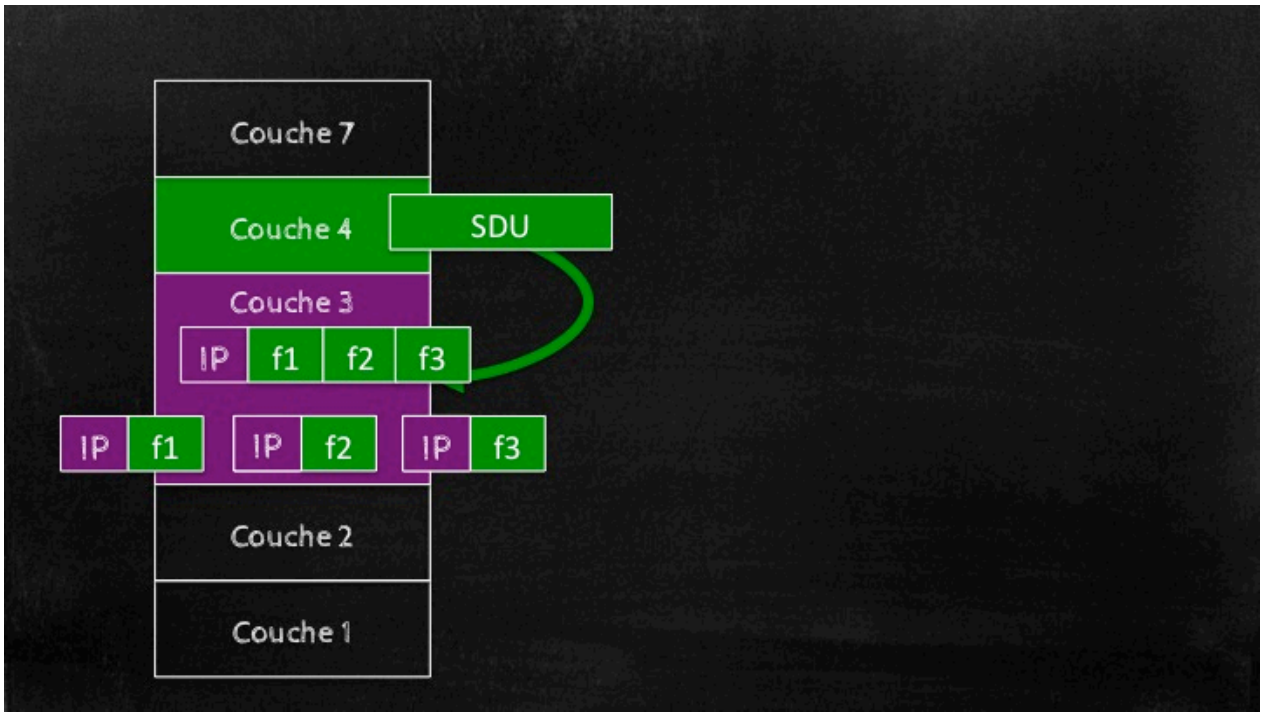
Le champ longueur indique la taille de l'en-tête, option comprise, et est exprimé en multiples de 4 octets. La grande majorité des paquets IPv4 ont un en-tête composé de 20 octets.

- **Champ Type de service (ToS)**

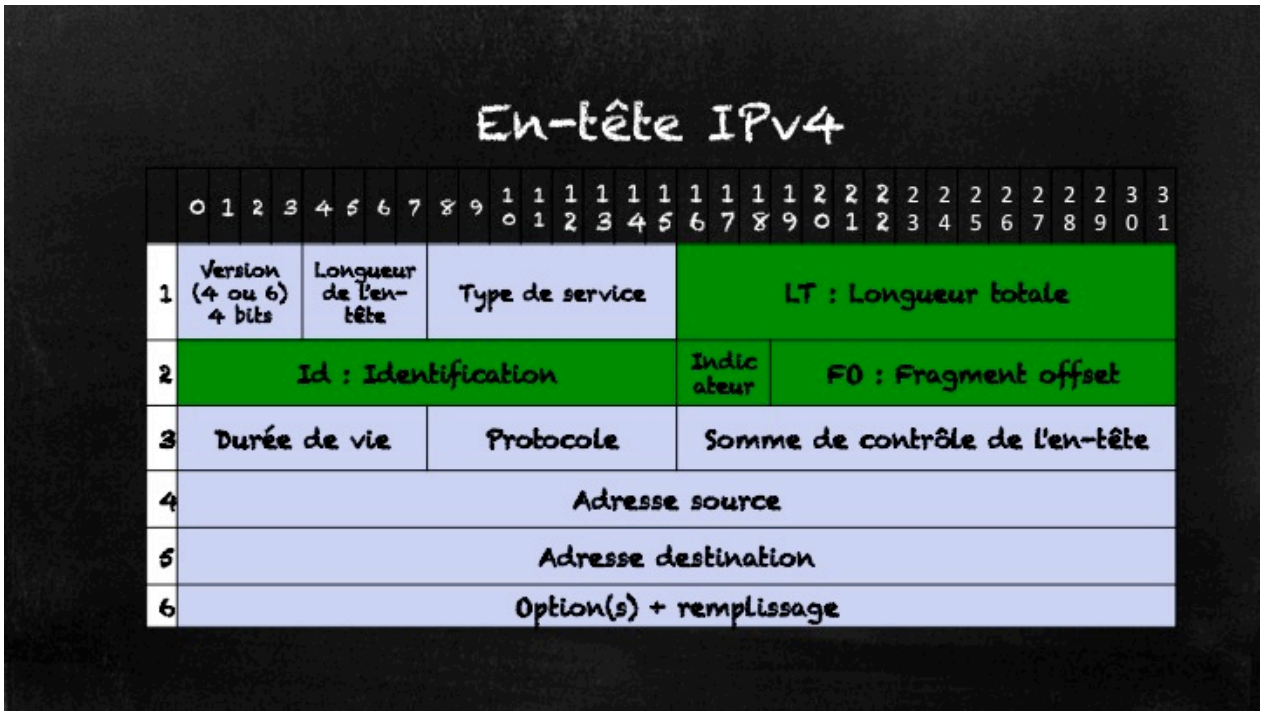
Le champ type de service indique la qualité de service souhaitée pour le paquet. Nous n'aborderons pas son utilisation ici.

- **La fragmentation**

IP doit adapter la taille de ses paquets pour ne pas dépasser la taille maximum que la couche liaison peut accepter. Pour cela, il met en œuvre un mécanisme de fragmentation pour répartir un contenu trop grand sur plusieurs paquets.



La fragmentation est faite par l'équipement IP qui ne peut acheminer l'information dans un seul paquet. Le SDU à transporter sera divisé en fragments dont la taille est un multiple de 8 octets. Chaque fragment sera transporté dans un paquet IP jusqu'à la destination finale qui se chargera du réassemblage des fragments pour reconstituer le SDU. Ce mécanisme impose un traitement coûteux dans les routeurs.



Le mécanisme de fragmentation utilise les 4 champs suivants de l'en-tête : Longueur totale, identificateur, fragment offset et au bit more segment.

- **Champ Longueur totale**

Le champ Longueur totale donne la longueur du SDU initial en nombre d'octets.

- **Champ Identification**

Le champ identification transporte le numéro d'identification attribué au SDU, il sera identique dans tous les paquets transportant les fragments.

- **Champ Fragment offset**

Le champ Fragment offset donne la position du fragment dans le SDU initial. Il est exprimé en mots de 8 octets.

- **Champ Indicateur**

Le champ indicateur rassemble deux drapeaux MF et DF, le premier bit du champ n'est pas utilisé.
Le bit DF pour « *Don't Fragment »* quand il vaut 1 permet d'interdire la fragmentation du paquet, Si le paquet dépasse la taille maximale possible, il sera rejeté. Quand DF vaut 0, la fragmentation est autorisée.
Le bit MF pour « *More Fragments* » vaut 1 si le paquet est un fragment et que d'autres suivent, il vaut 0 si le paquet contient le dernier fragment ou si le paquet n'a pas été fragmenté.

- **Champ Durée de vie (TTL)**

Le champ Durée de vie ou TTL (pour « *Time To Live* ») est utilisé pour limiter l'impact des boucles de routage dans le réseau car il permet de détruire des paquets prisonniers de ces boucles. Il est initialisé par l'émetteur et indique le nombre maximal d'équipements que le paquet pourra traverser. Il est généralement décrémenté d'une unité par chaque routeur traversé. Quand le TTL vaut 0, le paquet est rejeté et un message de contrôle est envoyé à l'émetteur pour information grâce au protocole ICMP « *Internet Control Message Protocol* ».

- **Champ Protocole**

Le champs Protocole indique à quel protocole de niveau supérieur il faut délivrer les données transportées par le paquet IP. De nombreux protocoles utilisent IP pour transporter leurs données, le champ protocole contient un numéro les désignant, par exemple : 6 pour TCP, 17 pour UDP, ou encore 0 pour IP lui même.

- **Champ Header Checksum**

Les 2 octets suivants contiennent une somme de contrôle de l'en-tête ou Header Checksum afin de détecter les erreurs de transfert. La somme est calculée à l'émission du paquet et insérée dans l'en-tête. Si le paquet a été altéré lors du transfert, la somme de contrôle calculée à la réception sera différente de celle transportée dans l'en-tête IP. Le paquet est alors abandonné sans message d'erreur.

- **Champs Adresse source et Adresse destination**

Enfin, l'en-tête contient l'adresse IP de l'émetteur et l'adresse IP du récepteur. Les adresses ont une longueur de 4 octets. Nous verrons dans une prochaine séance comment elles sont construites et comment elles sont utilisées.

- **Champ Option**

Le champ Option est facultatif et peu utilisé. Il permet d'adapter l'en-tête aux besoins de certains protocoles.

En résumé

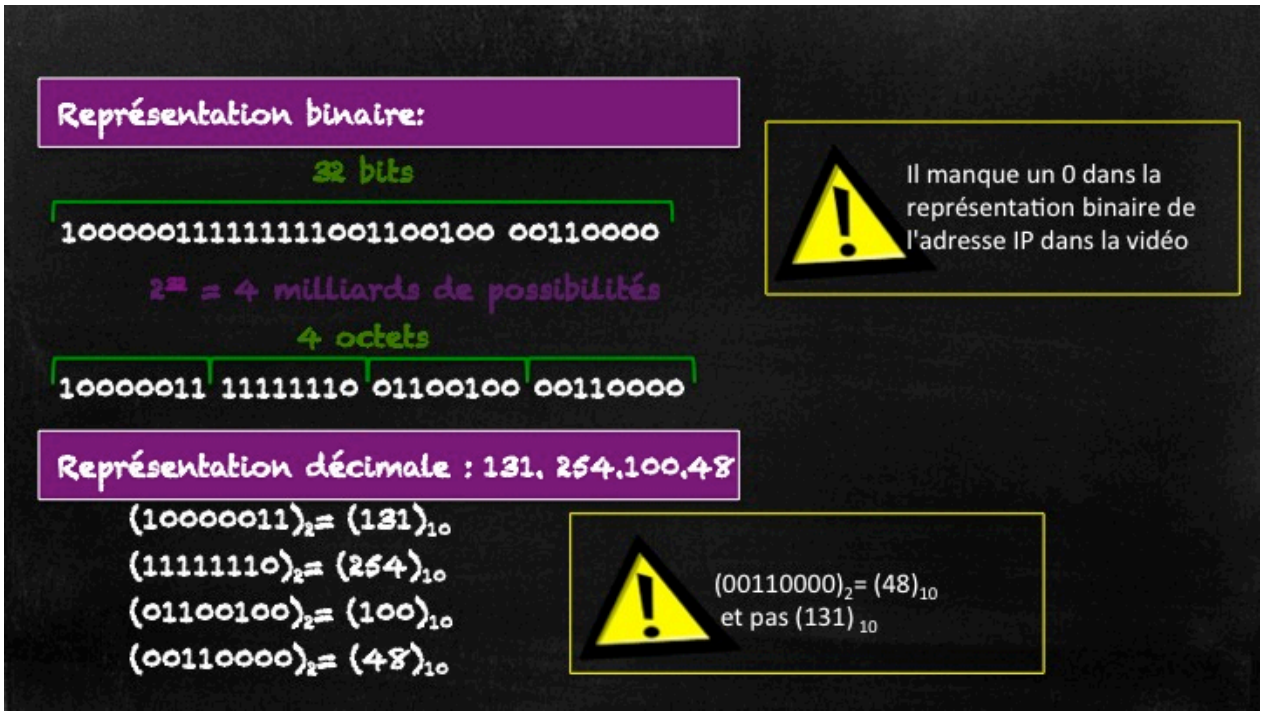
Dans cette séance nous avons vu que le protocole IP dans sa version 4. Nous avons vu qu'il offre un service de communication de type datagramme. Il utilise des relais intermédiaires pour acheminer les données dans des PDU appelés paquets. Nous avons détaillé l'en-tête de ces PDU.

Séance 3 : l'adresse IP

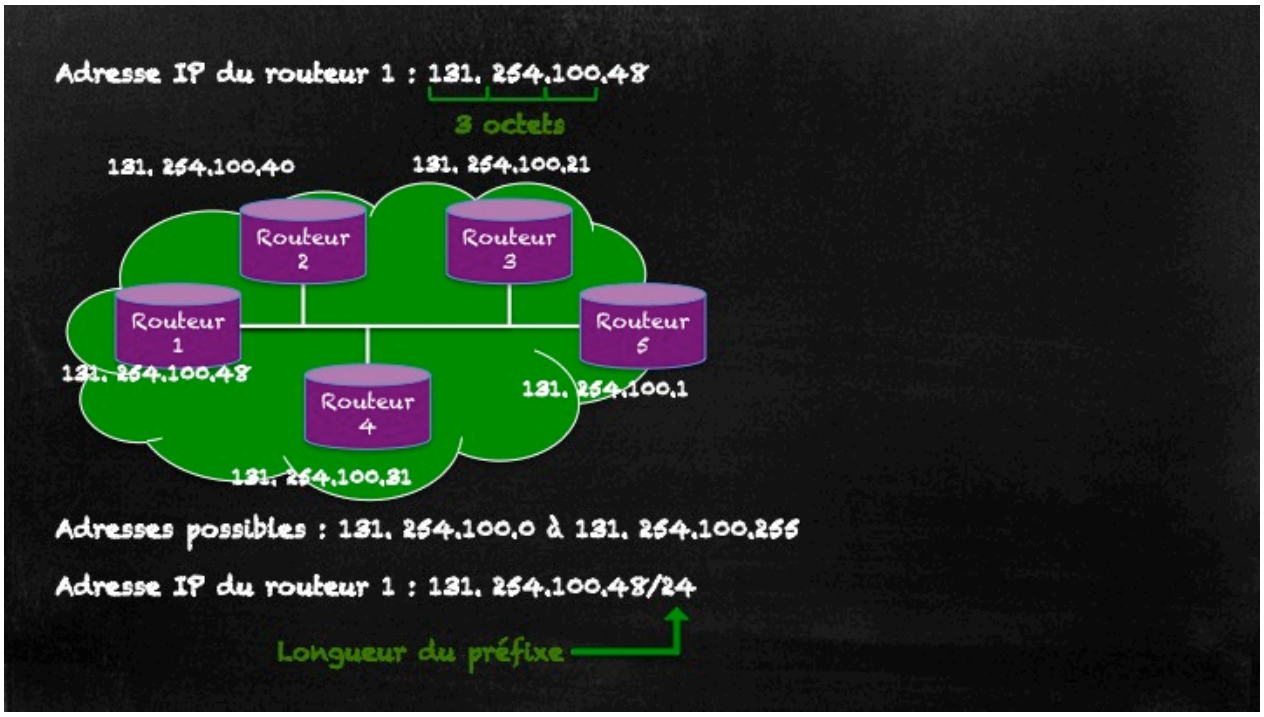
Introduction

A l'instar d'une lettre postale, l'en-tête de tout paquets IP contient l'adresse de l'émetteur et l'adresse du destinataire du paquet. Ces adresses servent à l'acheminement des paquets en mode datagramme à travers l'Internet. Cette séance présente les adresses IPv4 et leur utilisation par le protocole IP.

Description de l'adresse IP



Une adresse IPv4 est constituée de 32 bits. Ce qui permet 4 milliards d'adresses différentes. Pour que l'adresse soit plus lisible, on représente ses 4 octets par leur valeur décimale séparée par un point.



L'adresse IPv4 d'une machine contient à la fois l'identifiant du réseau, commun à toutes les machines du réseau et l'identifiant de la machine, unique sur le réseau.
Prenons l'exemple d'une machine dont l'adresse serait 131.254.100.48. Si les trois premiers octets désignent l'adresse du réseau, toutes les machines de ce réseau auront une adresse commençant par 131.254.100.xxx.
On appelle cette partie de l'adresse le préfixe du réseau.
Dans notre exemple, il a une longueur de 24 bits. On indique sa taille à la suite de l'adresse IPv4 : dans notre exemple la machine aura l'adresse suivante : 131.254.100.48 /24.
Les 24 premiers bits désignent le préfixe du réseau : 10000011.11111110.01100100.xxxxxxxx)

Cela veut dire que l'identification de l'interface réseau de la machine comprend 8 bits, on peut donc avoir 2^8=256 possibilités soit 256 machines différentes dans le réseau.

Le préfixe du réseau peut être facilement retrouvé en multipliant l'adresse de la machine par un netmask ou masque du réseau. Si *n* est la longueur du préfixe, le masque de réseau est constitué de 32 bits dont les *n* premiers sont des 1 et les suivants sont à 0.
Reprenons l'exemple : l'adresse 131.254.100.48 /24 indique que le préfixe a une longueur de 24 bits. Le masque de réseau comportera donc 24 bits à 1 suivis de 8 bits à 0 :

11111111111111111111111100000000

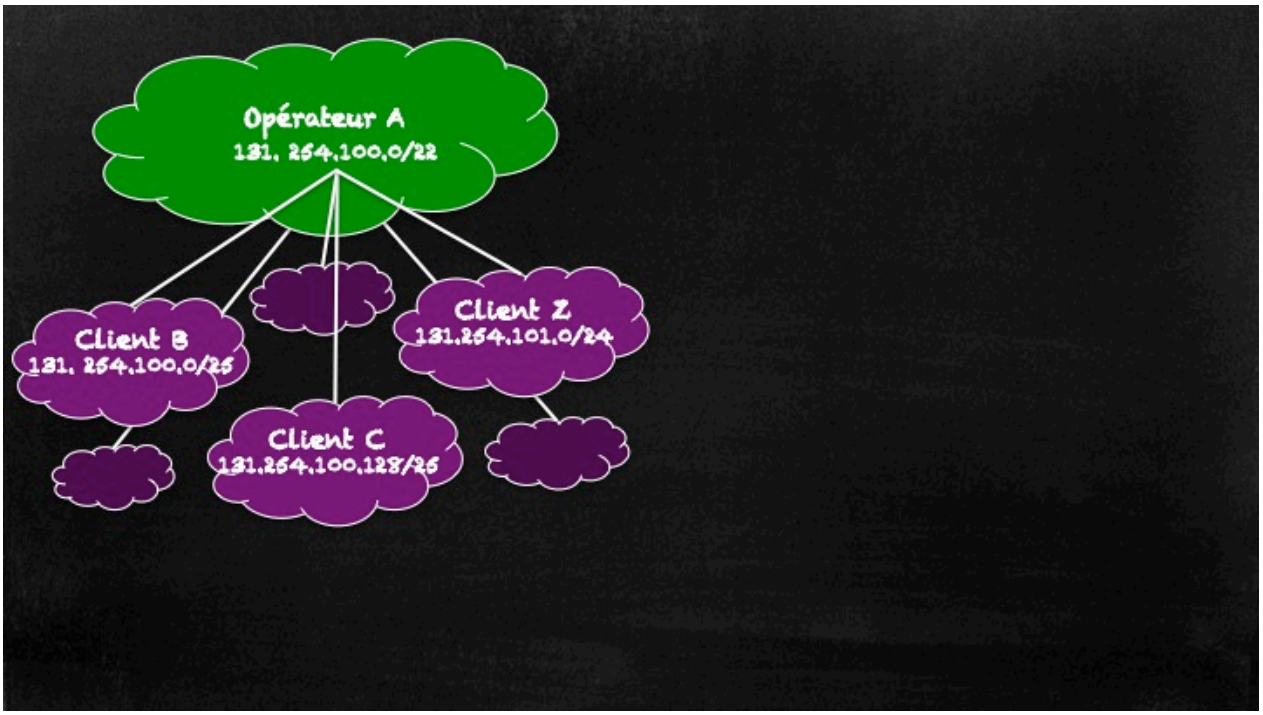
soit 255.255.255.0 En multipliant le masque de réseau par l'adresse IP, on peut isoler le préfixe du réseau.

L'attribution des adresses IP est coordonnée par l'organisme nommé IANA (Internet Assigned Numbers Authority).

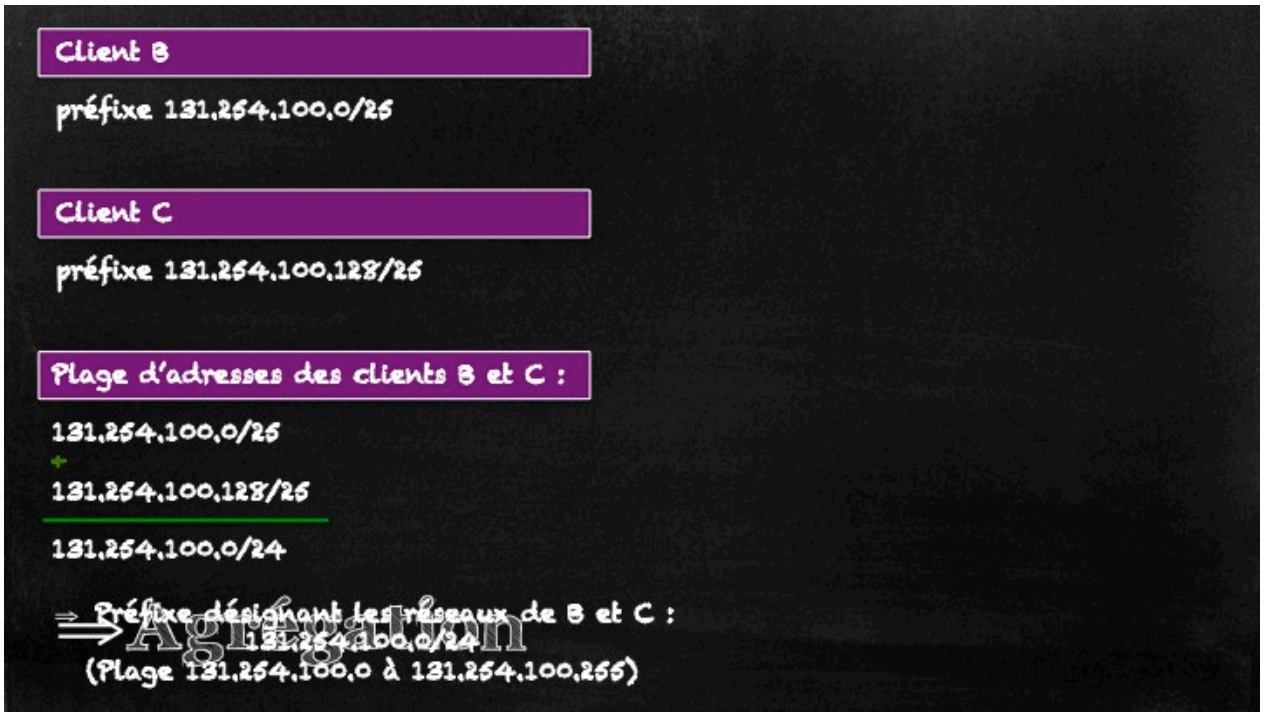
Pour IPv4, IANA a délégué la gestion de chaque blocs d'adresses de taille /8 à 5 organismes régionaux appelés RIRs (Registre Internet Régional). Les RIRs répartissent les adresses en les allouant à des organismes locaux, par exemple des opérateurs, chargés de distribuer les adresses à

leurs clients. Les adresses sont attribuées par blocs plus ou moins grands en fonction du nombre de machines dans les réseaux.

Agrégation des adresses

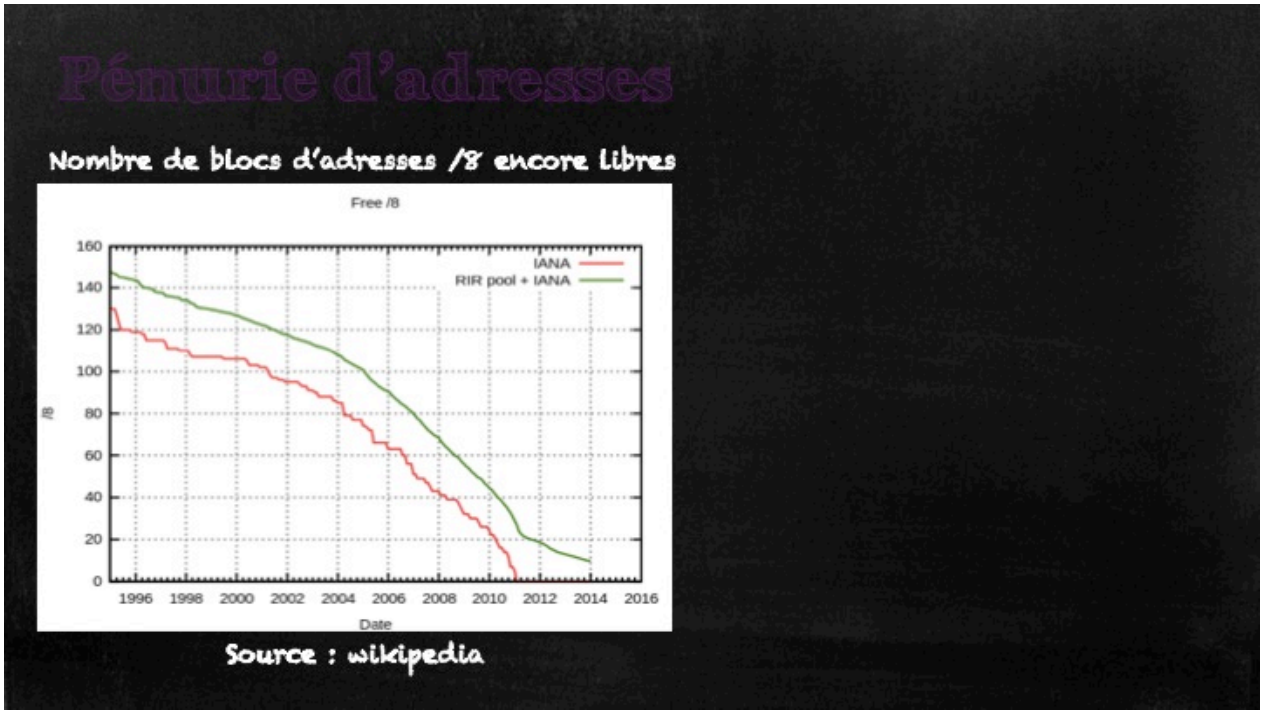


Les opérateurs distribuent leur plage d’adresses à leurs clients.

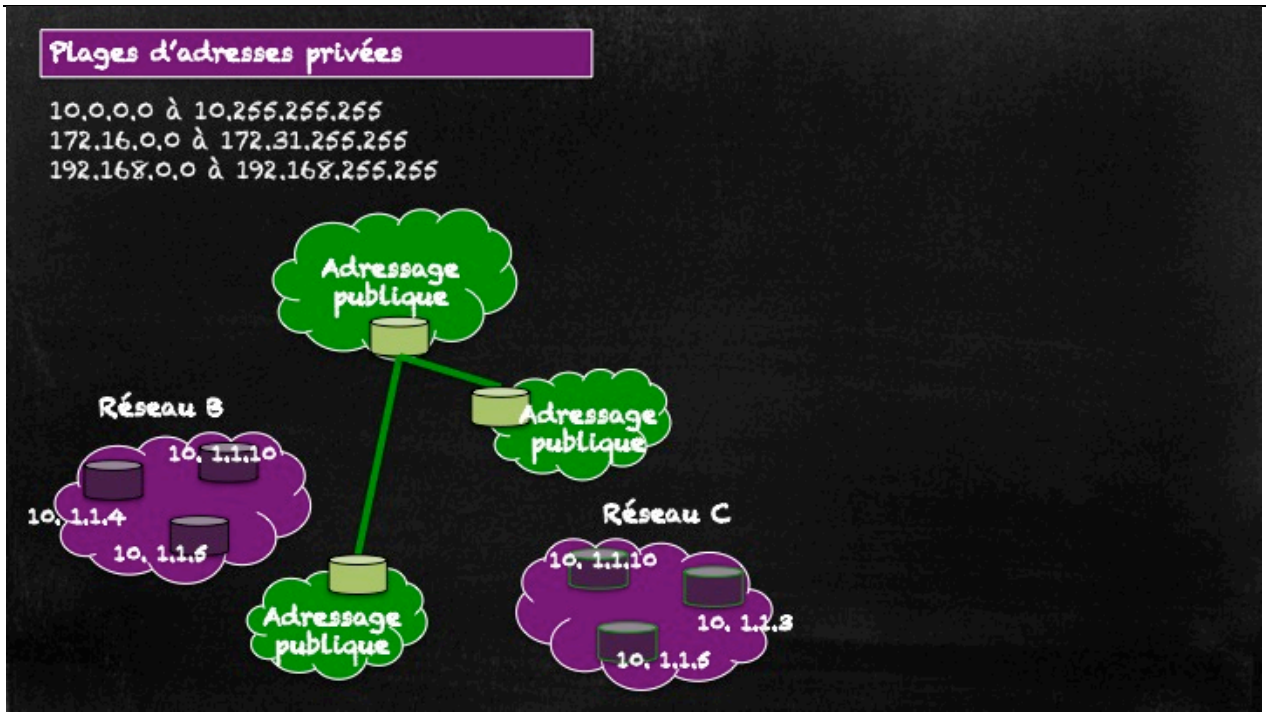


Quand plusieurs adresses sont contigües, on peut les rassembler sous un préfixe commun de taille plus petite. Par exemple, on peut désigner à la fois les adresses des réseaux suivants 131.254.100.0/25 et 131.254.100.128/25 avec le préfixe 131.254.100.0/24
On appelle cette opération l'agrégation des adresses.

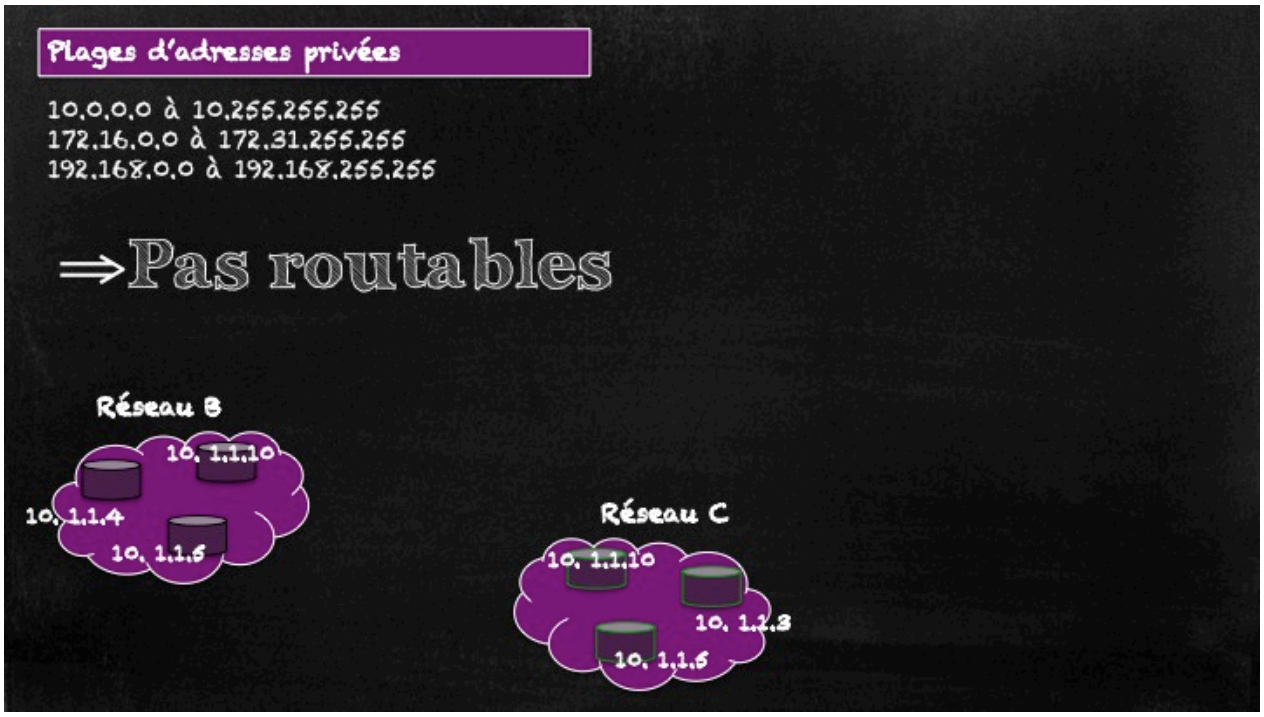
Adresses publiques ou privées



La forte croissance du nombre de machines connectées à l'Internet conduit à l'épuisement des adresses IPv4. Beaucoup de mesures pour retarder cette pénurie d'adresses ont été prises. Cependant, les derniers blocs /8 libres ont été attribués aux RIRs en 2011 et sont donc en cours d'attribution à leurs différents clients.



Une des mesures d'urgence prises est le recours à l'adressage privé. Les adresses IPv4 peuvent être publiques ou privées. Les adresses publiques permettent à une machine de communiquer avec l'Internet en désignant de façon unique cette machine ou une interface réseau dans l'Internet. Les adresses privées peuvent être attribuées dans des réseaux internes qui n'ont pas vocation à communiquer directement avec Internet.

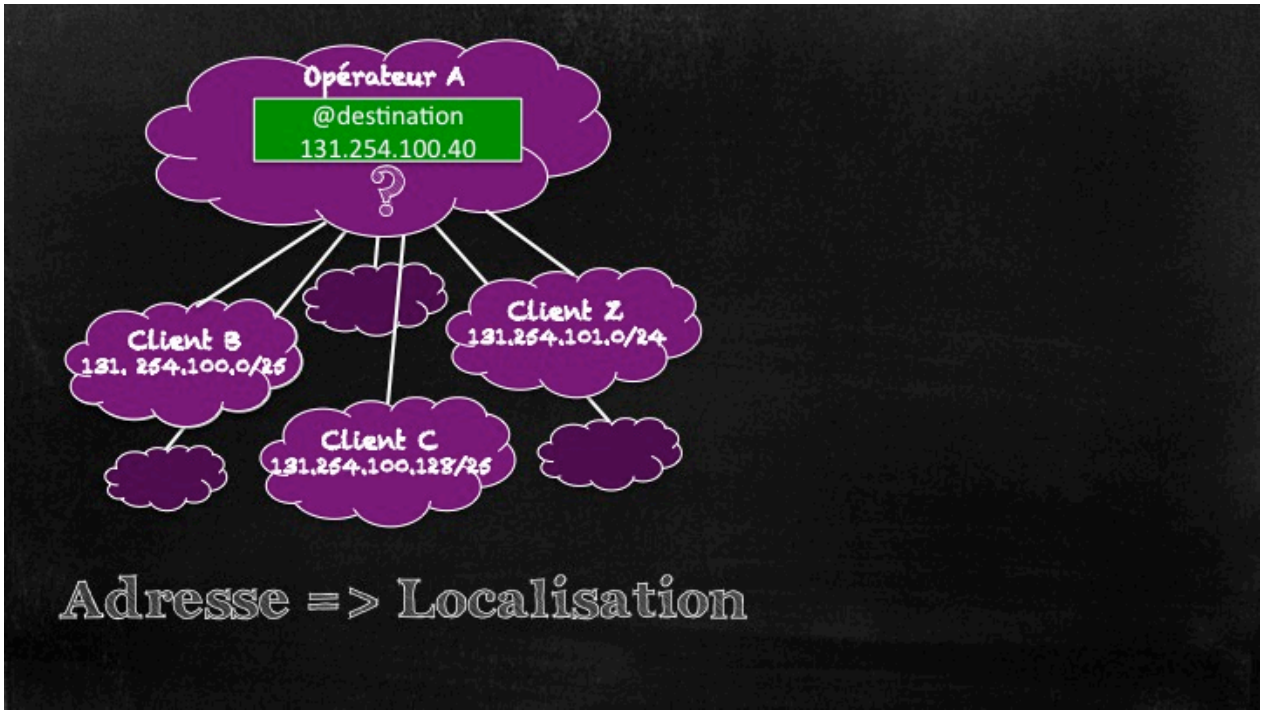


Les adresses privées peuvent être présentes dans plusieurs réseaux et ne peuvent donc pas être distinguées dans l'Internet. On dit que les adresses privées ne sont pas routables.

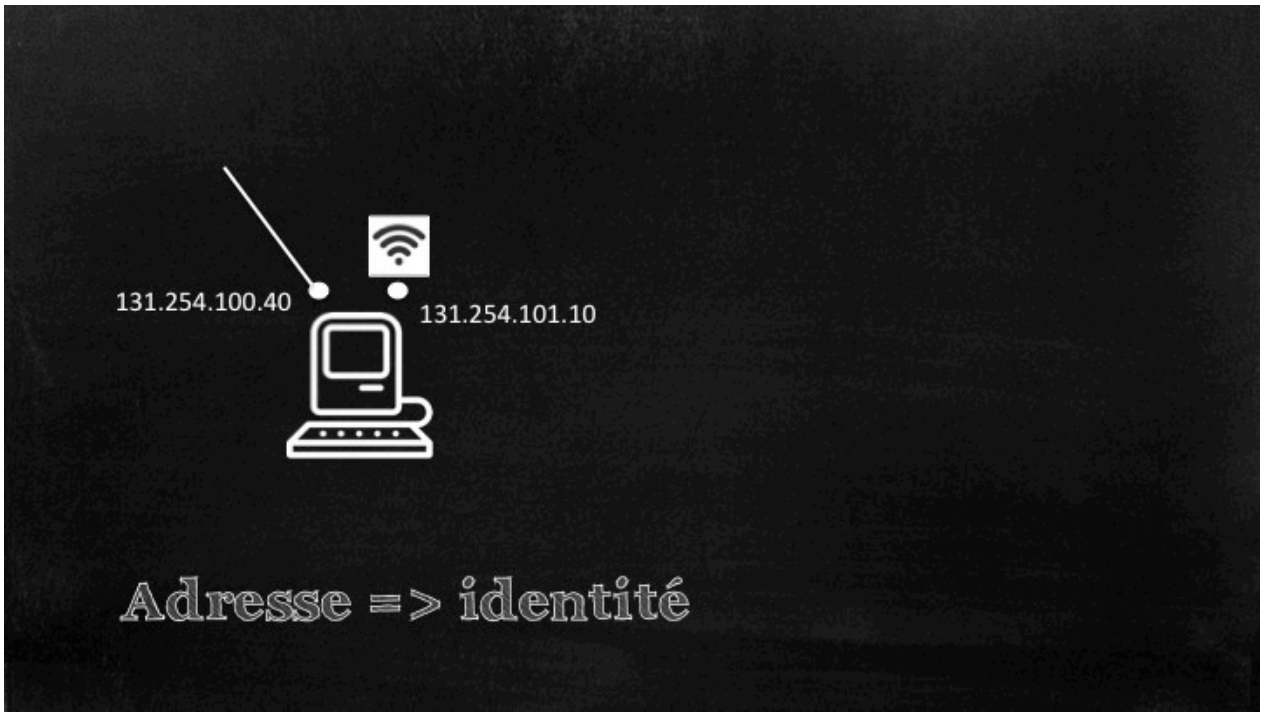
Si un réseau utilisant un adressage privé veut communiquer avec l'Internet, il faudra qu'un équipement fasse une translation (ou traduction) entre l'adresse privée et une adresse publique qui serait disponible pour dialoguer avec l'Internet. On appelle cette opération le NAT pour

« *Network Address Translation* » (en français Traduction d'adresse réseau). Nous n'aborderons pas ce mécanisme dans ce cours.

Localisation et identité



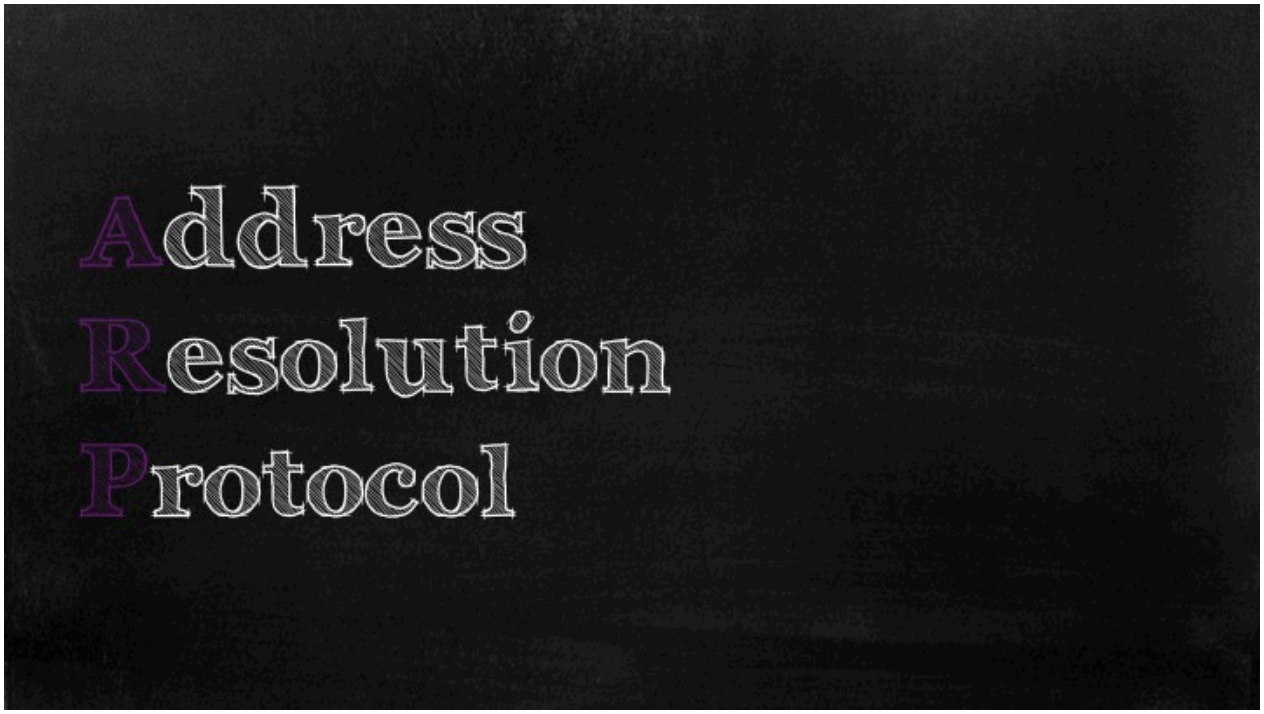
L'adresse IPv4 indique la localisation de la machine dans l'Internet. La partie préfixe de l'adresse indique la localisation du réseau, il fait partie de la plage d'adresses d'un fournisseur d'accès, attribuée par un registre régional (RIR). Ce préfixe indique comment joindre le réseau de la machine : en passant par cet opérateur.



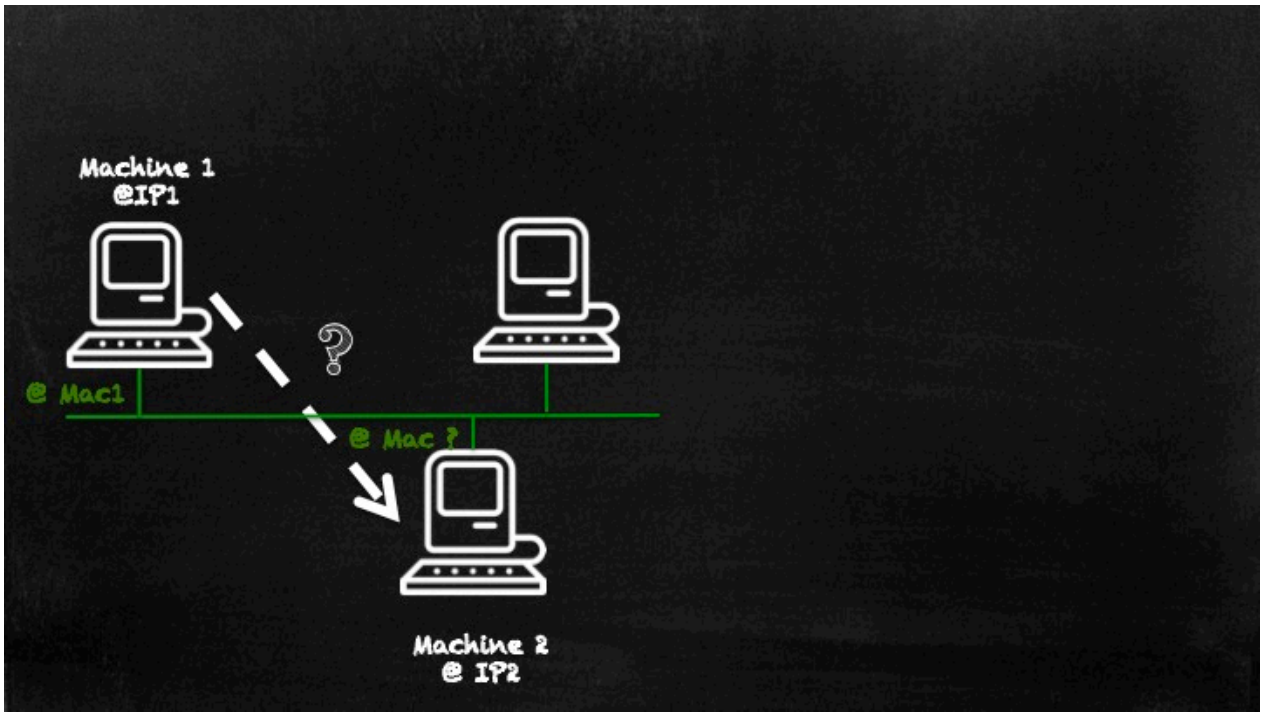
En IPv4, une machine communique grâce à une interface réseau. Celle ci possède une seule adresse IPv4. L'adresse IP désigne donc également l'identité de l'interface. Dans un réseau, cette identité sera unique. Si l'adresse est publique, elle est unique dans l'Internet, si elle est privée l'adresse sera unique sur le réseau privé.

L'adresse IP désigne donc à la fois l'identité de l'interface et sa localisation.

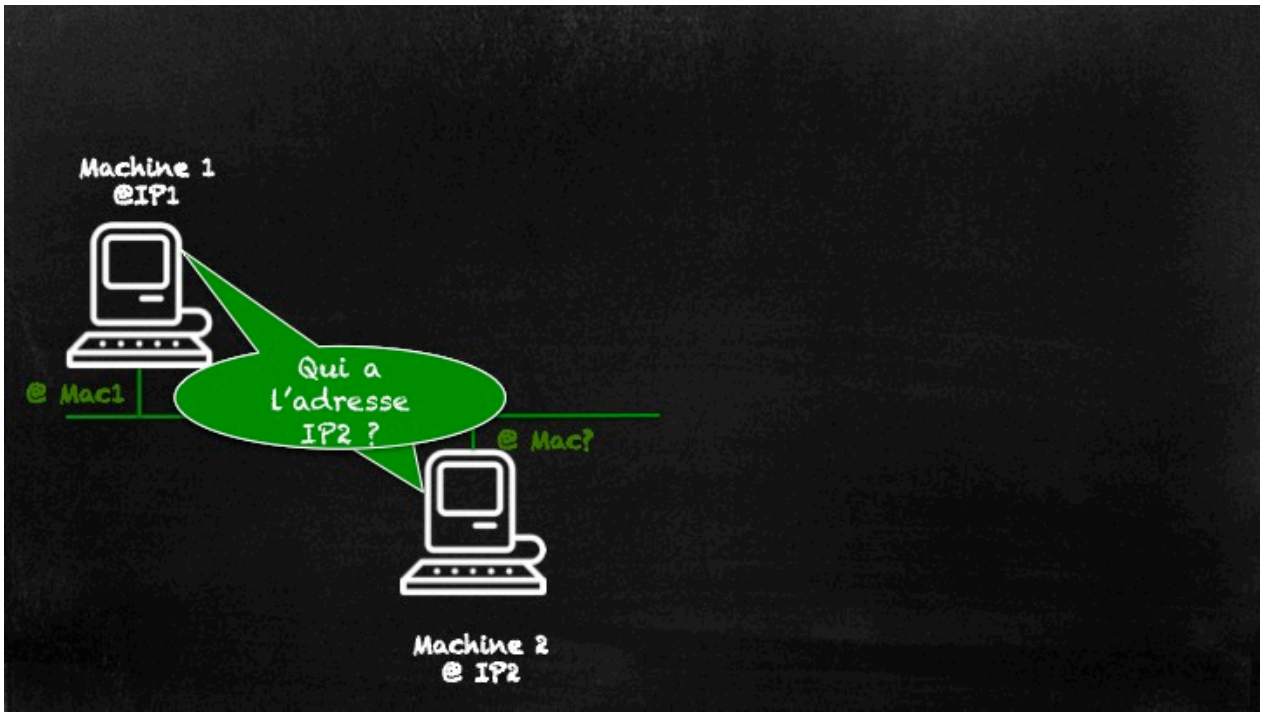
Comment trouver l'adresse IP ?



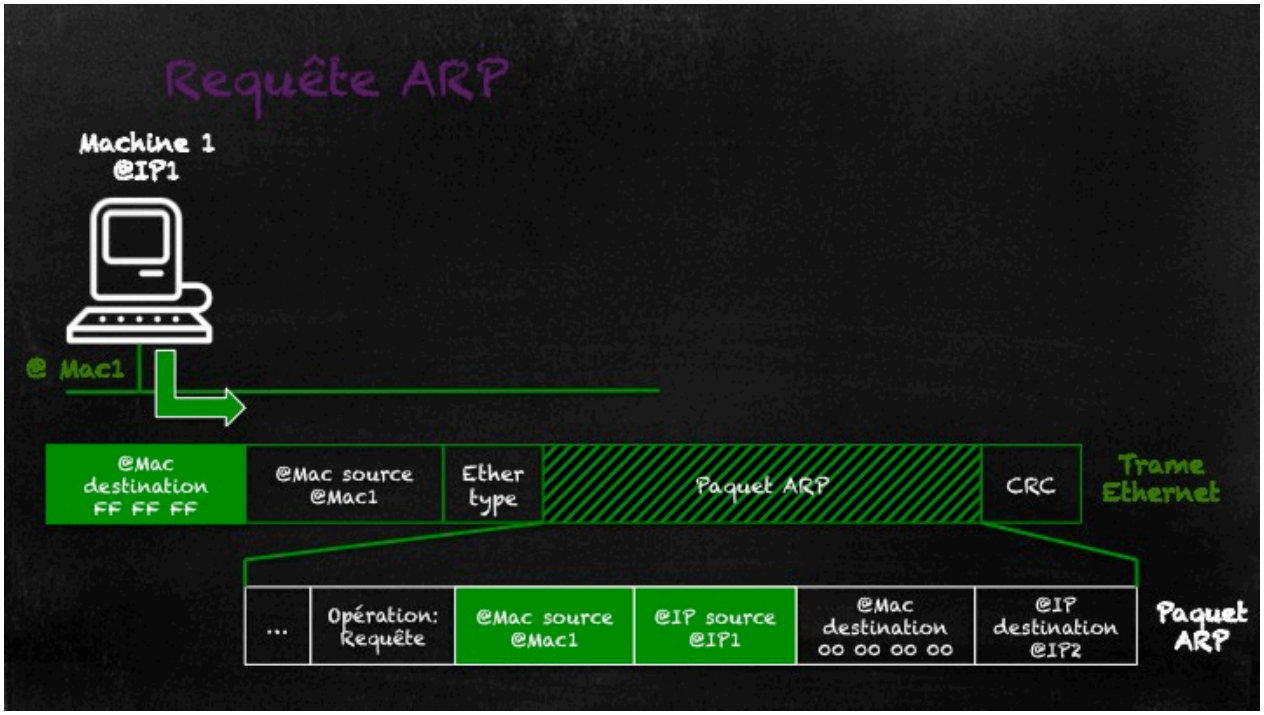
Les applications manipulent les adresses IP alors que les communications sont physiquement effectuées par les cartes réseaux qui utilisent les adresses MAC. Pour acheminer les paquets sur les liaisons, les équipements doivent pouvoir faire la correspondance entre les adresses IP et les adresses MAC. Sur des réseaux à diffusion comme Ethernet, on utilisera pour IPv4 le protocole ARP (« *Address Resolution Protocol* »).



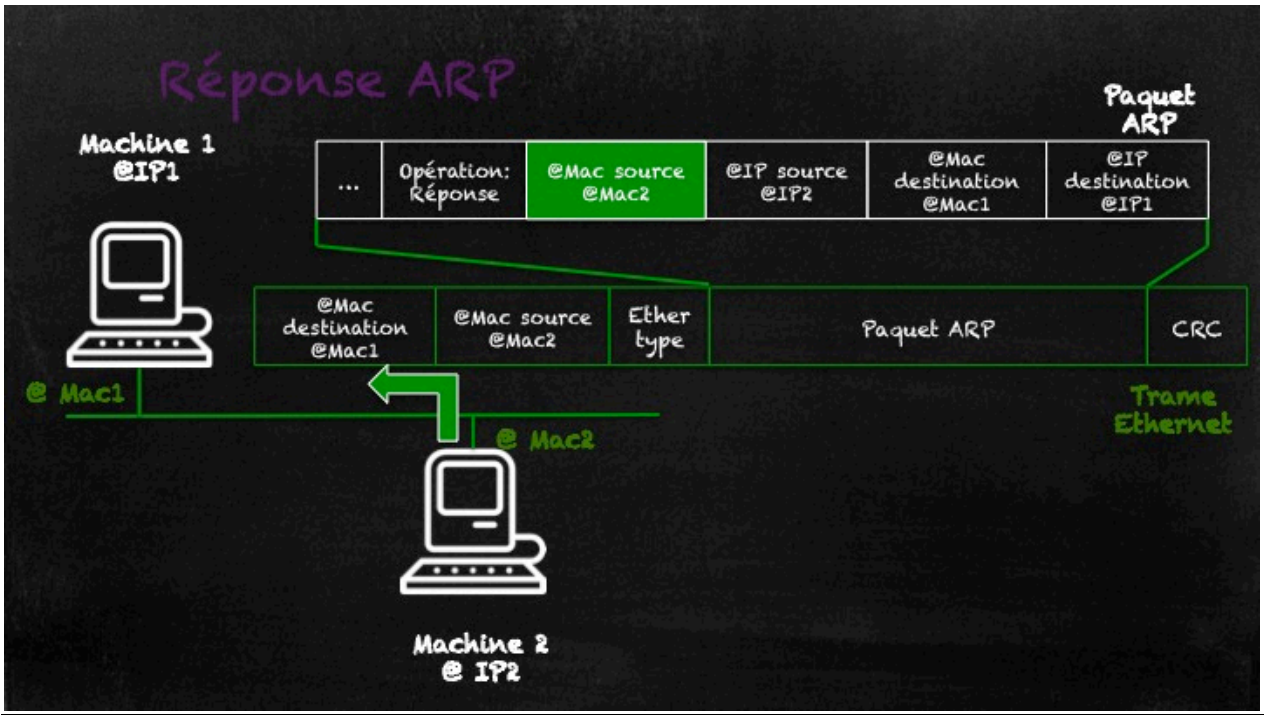
Le principe d'ARP est simple : une machine 1 souhaite envoyer un paquet IPv4 à une machine 2. Il ne connait pas l'adresse MAC du récepteur, il ne connait que son adresse IP : IP2.



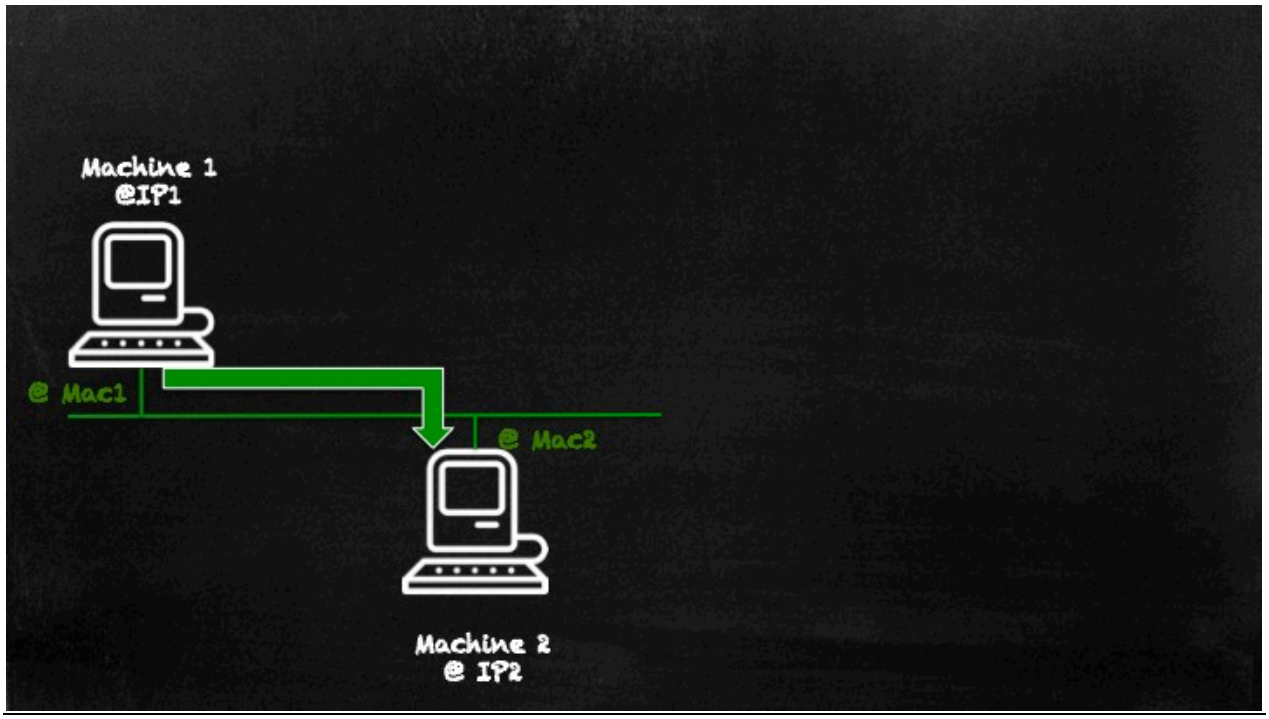
L'émetteur va questionner tous les équipements du réseau en leur demandant « Qui est l'équipement qui possède l'adresse IP IP2 ? » (diffusion). L'équipement 2 reçoit cette demande et reconnaît son adresse IP. Il peut alors répondre à l'équipement 1 et lui donner son adresse MAC.



Regardons le fonctionnement d'ARP plus en détail. Pour récupérer l'adresse MAC de la machine 2, la machine 1 envoie une trame en broadcast, c'est à dire qu'elle va adresser sa trame à toutes les machines atteignables sur le réseau. Pour cela, elle utilise une adresse de diffusion qui ne contient que des bits à 1. On peut noter que dans ce paquet ARP, la machine 1 indique son adresse MAC et son adresse IP.



Quand la machine 2 reçoit ce message, elle reconnaît son adresse IP. Elle va répondre à la machine 1 et lui indiquer son adresse MAC.



La machine 1 va recevoir un paquet ARP donnant les adresses MAC des machines 1 et 2 et peut alors envoyer des paquets de données en direction de la machine 2.

En résumé

Dans cette séance, nous avons vu la notion d'adresse dans IP. Nous avons introduit la notion d'adresse publique ou privée, de netmask et de préfixe du réseau. Nous avons également abordé le protocole ARP qui fait le lien entre les adresses IP, utilisées par les applications pour désigner les machines source et destination des données, et les adresses MAC utilisées pour transférer les données entre deux voisins sur la liaison physique.