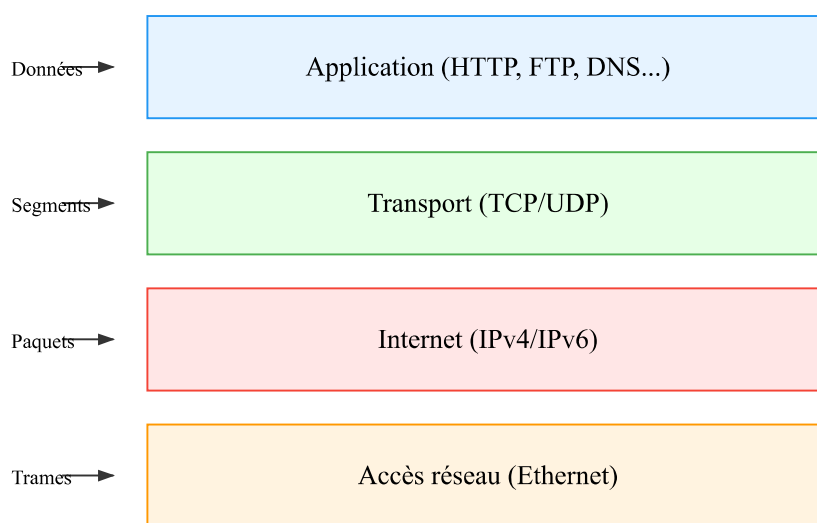


L'adressage IPv4

00. Introduction : Avant de commencer

Le réseau est souvent comparé à un système postal : pour communiquer efficacement, chaque destinataire doit avoir une adresse unique et comprendre comment les messages sont acheminés. L'adressage IPv4, pierre angulaire d'Internet, répond précisément à ce besoin.



00.1 Pourquoi un protocole réseau ?

La communication en réseau pose plusieurs défis fondamentaux. Comment s'assurer que chaque machine peut être identifiée de manière unique ? Comment garantir que les messages arrivent à destination ? Comment organiser efficacement ces échanges ?

Le protocole TCP/IP répond à ces questions en proposant une architecture en couches, où chaque niveau a une responsabilité spécifique. L'IPv4, situé dans la couche Internet, s'occupe spécifiquement de l'adressage et du routage des paquets à travers les réseaux.

00.2 Les bases de TCP/IP

Le protocole TCP/IP fonctionne comme un système postal sophistiqué :

1. **L'adressage** : Chaque machine reçoit une adresse IP unique, comme une adresse postale

2. **Le routage** : Les paquets sont acheminés de routeur en routeur, comme des lettres passant par différents centres de tri
3. **La fiabilité** : TCP s'assure que tous les paquets arrivent et dans le bon ordre
4. **La standardisation** : Des règles communes permettent à des équipements différents de communiquer



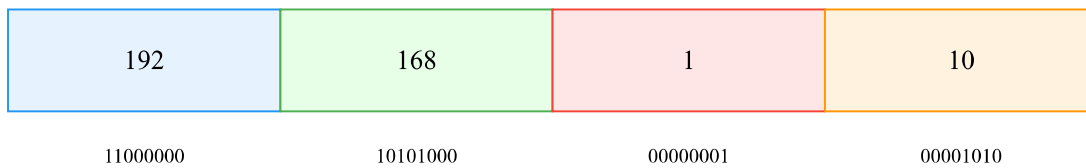
Dans ce module, nous allons nous concentrer sur l'adressage IPv4, élément fondamental pour comprendre comment :

- Les machines s'identifient sur le réseau
- Les réseaux sont organisés et segmentés
- Le routage permet la communication entre différents réseaux
- La sécurité peut être mise en place au niveau réseau

01. L'adresse IP

01.1 Pourquoi une adresse IP ?

Une adresse IP joue un rôle similaire à une adresse postale dans le monde réel : elle permet d'identifier de manière unique chaque "habitant" du réseau et de lui acheminer les informations qui lui sont destinées.

**Structure :**

- 4 octets (32 bits)
- Valeurs de 0 à 255 par octet
- Séparés par des points

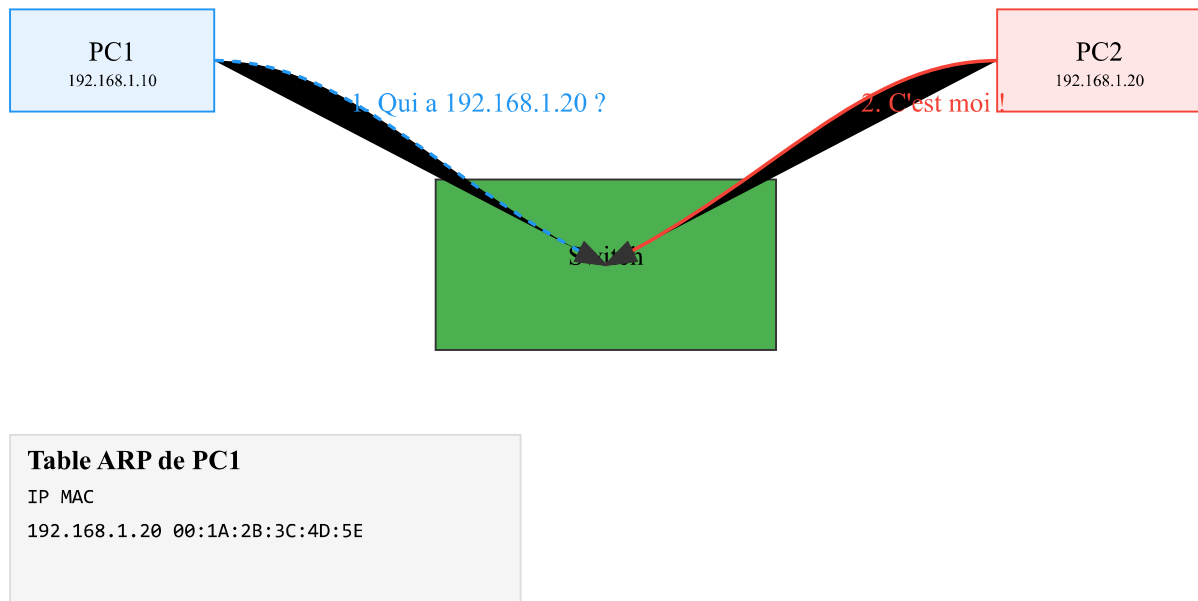
01.2 Structure d'une adresse IPv4

Une adresse IPv4 se compose de 32 bits, organisés en quatre octets (groupes de 8 bits). Pour faciliter la lecture, nous utilisons une notation décimale pointée, où chaque octet est converti en nombre décimal (de 0 à 255) et séparé par des points.

Prenons l'exemple de l'adresse 192.168.1.10 :

1. Premier octet : 192 (11000000 en binaire)
2. Deuxième octet : 168 (10101000 en binaire)
3. Troisième octet : 1 (00000001 en binaire)
4. Quatrième octet : 10 (00001010 en binaire)

01.3 La correspondance IP/MAC



Le protocole ARP (Address Resolution Protocol) permet d'établir la correspondance entre les adresses IP (couche 3) et les adresses MAC (couche 2). Ce processus est essentiel car les communications physiques sur un réseau local se font toujours via les adresses MAC.

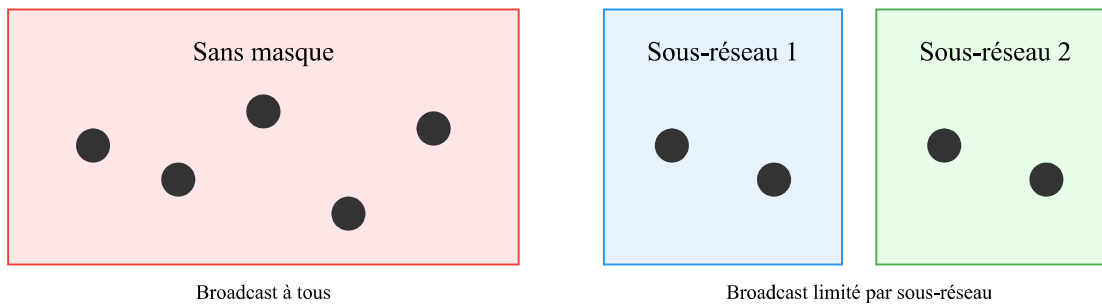
Le processus se déroule en deux temps :

1. Une machine envoie une requête ARP en broadcast : "Qui possède cette adresse IP ?"
2. La machine concernée répond avec son adresse MAC
3. Les informations sont stockées dans une table ARP temporaire

02. Le masque de sous réseau

02.1 Pourquoi limiter ?

Le masque de sous-réseau est un concept fondamental qui permet d'organiser et de segmenter efficacement les réseaux. Sans cette segmentation, nous aurions un immense réseau difficile à gérer et à sécuriser.



02.2 Le principe du masque

Le masque de sous-réseau fonctionne comme un pochoir qui vient se superposer à l'adresse IP pour distinguer deux parties :

- La partie réseau (identifiant du réseau)
- La partie hôte (identifiant de la machine dans ce réseau)

IP: 192.168.1.10

11000000.10101000.00000001.00001010

Masque: 255.255.255.0 (/24)

11111111.11111111.11111111.00000000

Partie réseau: 192.168.1.0

Partie hôte: 0.0.0.10

02.3 En pratique

Le masque peut être noté de deux façons :

1. Notation décimale pointée : 255.255.255.0

2. Notation CIDR : /24 (indique le nombre de bits à 1 dans le masque)

Prenons un exemple avec le réseau 192.168.1.0/24 :

- Les trois premiers octets (24 bits) définissent le réseau
- Le dernier octet (8 bits) définit les hôtes possibles
- Cela permet d'avoir 254 adresses utilisables (de .1 à .254)
- .0 est réservé pour l'adresse du réseau
- .255 est réservé pour le broadcast

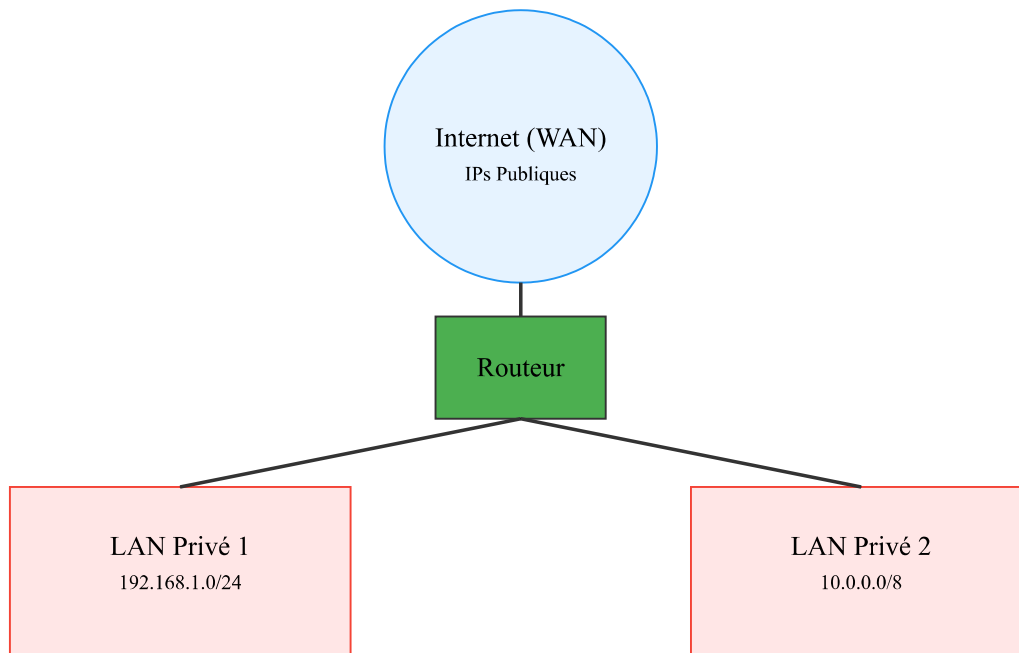
Cette segmentation permet :

- Une meilleure organisation du réseau
- Une réduction du trafic de broadcast
- Une amélioration de la sécurité
- Une simplification de la gestion

03. Les réseaux

03.1 Publique / Privé, WAN / LAN

L'Internet est un immense réseau de réseaux, où coexistent des réseaux publics et privés. Comprendre leur distinction est fondamental pour la sécurité et l'organisation des infrastructures.



Le WAN (Wide Area Network)

L'Internet public fonctionne exclusivement avec des adresses IP publiques, uniques à l'échelle mondiale. Ces adresses sont :

- Attribuées par les registres Internet régionaux (RIR)
- Routables sur Internet
- Généralement payantes et en nombre limité
- Directement accessibles depuis n'importe où sur Internet

03.2 Le LAN (Local Area Network)

Les réseaux locaux utilisent des plages d'adresses privées réservées :

1. Classe A

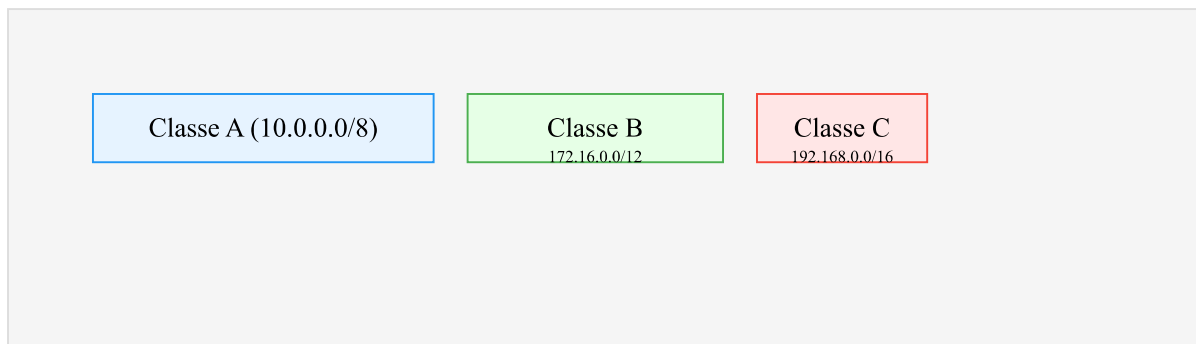
- Plage : 10.0.0.0 à 10.255.255.255
- Masque : /8
- Capacité : Plus de 16 millions d'adresses

2. Classe B

- Plage : 172.16.0.0 à 172.31.255.255
- Masque : /12
- Capacité : Environ 1 million d'adresses

3. Classe C

- Plage : 192.168.0.0 à 192.168.255.255
- Masque : /16
- Capacité : 65 534 adresses



04. Les composantes d'un réseau

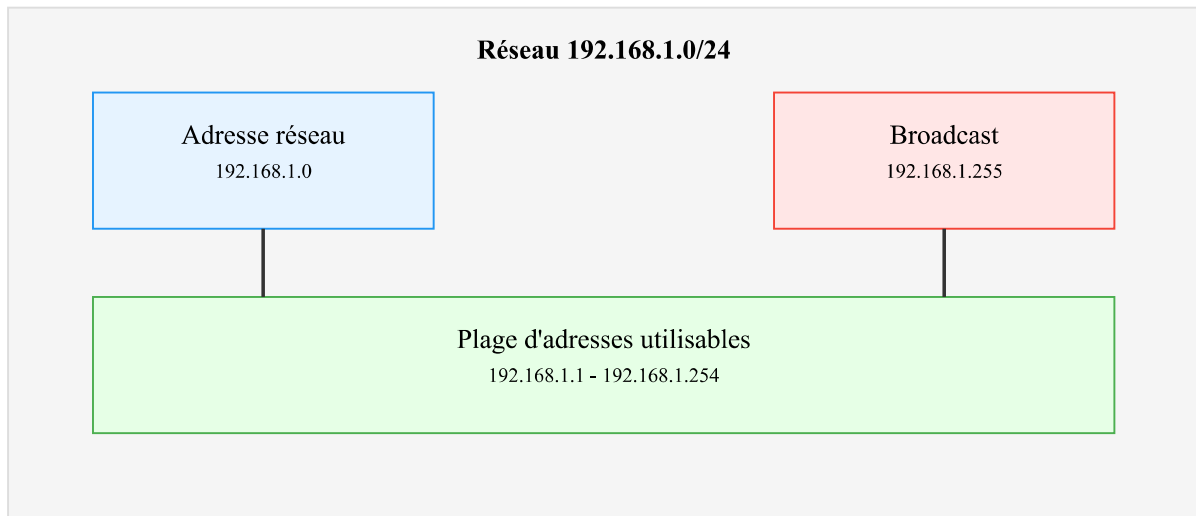
Pour qu'un réseau soit fonctionnel et permette une communication efficace entre ses différents éléments, plusieurs composantes essentielles doivent être définies et configurées correctement. Chacune joue un rôle spécifique dans le bon fonctionnement de l'ensemble.

04.1 Les éléments fondamentaux

Tout réseau IP nécessite au minimum deux éléments de base :

1. **L'adresse du réseau** Cette adresse identifie de manière unique le réseau lui-même. Elle correspond à la première adresse de la plage disponible et ne peut jamais être attribuée à un hôte.

2. **Le masque de sous-réseau** Comme nous l'avons vu précédemment, il définit la taille du réseau et permet de distinguer la partie réseau de la partie hôte dans une adresse IP.

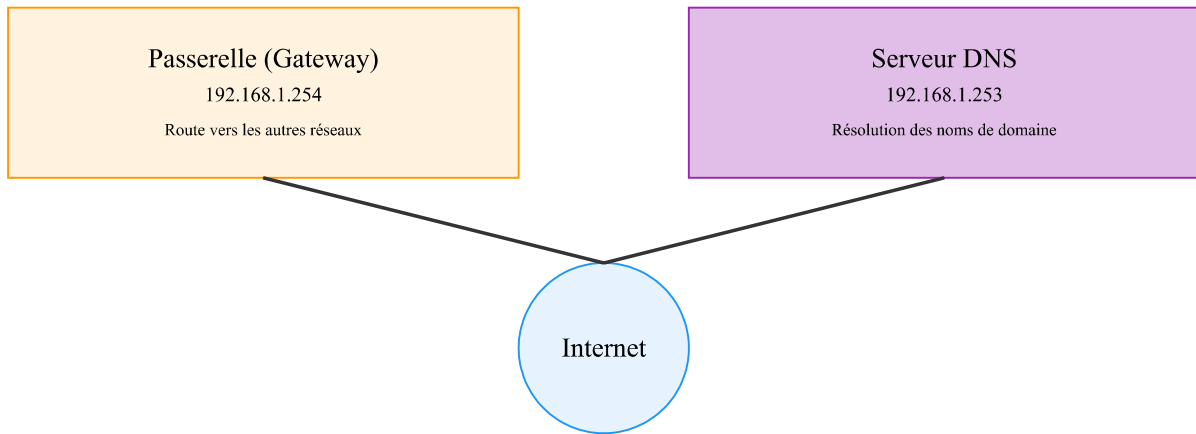


Prenons l'exemple concret du réseau 192.168.1.0/24 :

- **Adresse du réseau** : 192.168.1.0
 - Première adresse de la plage
 - Identifie uniquement le réseau
 - Ne peut être attribuée à aucun équipement
- **Adresse de broadcast** : 192.168.1.255
 - Dernière adresse de la plage
 - Utilisée pour la diffusion à tous les hôtes
 - Messages reçus par tous les équipements du réseau
- **Plage d'adresses utilisables** : 192.168.1.1 à 192.168.1.254
 - 254 adresses disponibles pour les équipements
 - Chaque adresse doit être unique dans le réseau
 - Configuration possible en statique ou en dynamique (DHCP)

04.2 Les composantes additionnelles essentielles

Pour permettre une connectivité complète, notamment vers l'extérieur du réseau, d'autres éléments sont nécessaires :



Les composantes additionnelles en détail

La passerelle (Gateway)

La passerelle est un élément crucial qui joue le rôle de "porte de sortie" du réseau local. Son fonctionnement est plus complexe qu'il n'y paraît :

- **Rôle principal :**
 - Fait le lien entre le réseau local et les réseaux externes
 - Connaît les routes vers les autres réseaux
 - Traduit les adresses privées en adresses publiques (NAT)
 - Applique les règles de sécurité (firewall)
- **Configuration type :** La passerelle prend généralement la première ou la dernière adresse utilisable du réseau pour être facilement mémorisable. Par exemple :
 - Dans un réseau `192.168.1.0/24` : `192.168.1.254`
 - Dans un réseau `10.0.0.0/24` : `10.0.0.1`

Le serveur DNS (Domain Name System)

Le DNS est souvent considéré comme "l'annuaire d'Internet". Son rôle est essentiel pour la navigation web et les services réseau :



- **Fonctions principales :**

- Traduit les noms de domaine en adresses IP
- Maintient un cache des résolutions fréquentes
- Peut filtrer l'accès à certains sites
- Optimise la navigation en réduisant les temps de résolution

- **Configuration courante :**

- DNS primaire : souvent l'adresse du routeur ou d'un serveur local
- DNS secondaire : généralement fourni par le FAI ou un service public (8.8.8.8 pour Google)

Les services additionnels courants

D'autres services peuvent être nécessaires selon les besoins :

1. Serveur DHCP

- Attribue automatiquement les configurations IP
- Évite les conflits d'adresses
- Simplifie l'administration du réseau

- Gère les baux d'adresses IP

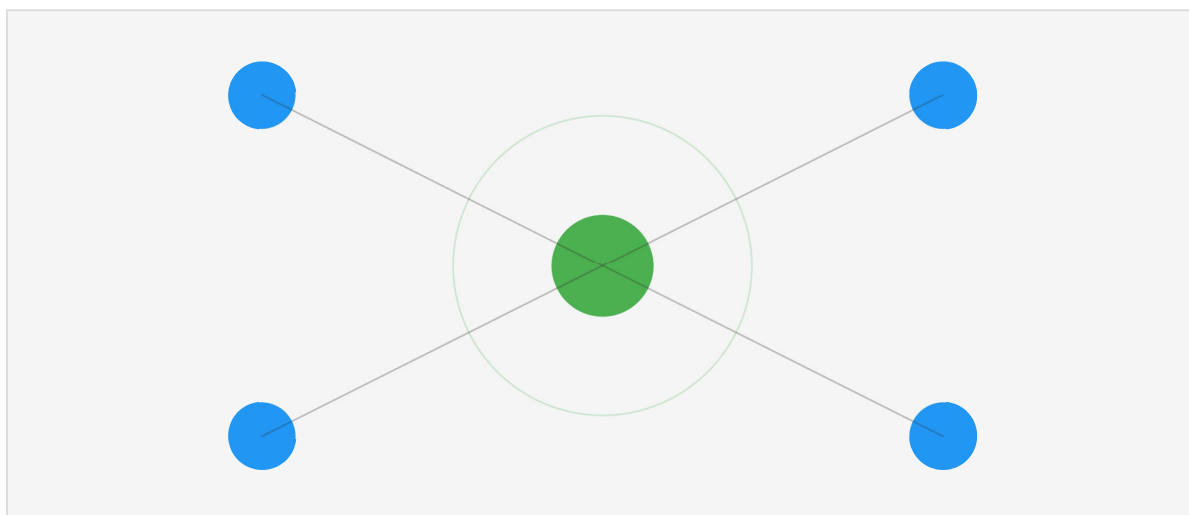
2. Serveur de temps (NTP)

- Synchronise les horloges des équipements
- Important pour la journalisation
- Crucial pour certains protocoles de sécurité

05. Le broadcast - Un mécanisme fondamental

05.1 L'importance du broadcast dans les réseaux

Le broadcast est un mécanisme essentiel qui permet à une machine de communiquer avec toutes les autres machines d'un même réseau en une seule transmission. C'est comme si vous utilisiez un mégaphone dans une salle : tout le monde vous entend en même temps.



05.2 Le processus de découverte

Quand une machine veut communiquer avec une autre dont elle ne connaît que l'adresse IP, voici ce qui se passe :

1. Phase de découverte

- La machine A cherche à joindre la machine B
- Ne connaissant pas son adresse MAC, elle envoie une requête ARP en broadcast

- Toutes les machines du réseau reçoivent cette requête
- Seule la machine B répond avec son adresse MAC

2. Phase de mémorisation

- La machine A enregistre la correspondance IP/MAC dans sa table ARP
- Cette information est conservée pendant une durée limitée
- Les communications suivantes seront directes

