Protocole TCP/IP- IP V4

Avant tout il faut savoir que les classes d'adresses IP pour les réseaux privés ne sont que des conventions pas des normes.

Ainsi le fait d'utiliser par exemple 192.168.1.0 comme réseau, peut nous dire qu'il s'agit d'une adresse de classe C par convention. Mais cela n'est pas toujours une généralité. C'est pour cela qu'on doit toujours adjoindre un masque sous-réseau avec l'adresse afin de ne pas se tromper !

► Classe A
Une adresse IP de classe A dispose d'un seul octet pour identifier le réseau et de trois octets pour identifier les machines sur ce réseau. Un réseau de classe A peut comporter jusqu'à 23×8-2 postes, soit 224-2, soit 16 777 214 terminaux. Le premier octet d'une adresse IP de classe A commence toujours par le bit 0. La plage d'adresse en binaire s'étend de 0000 0000 à 0111 1111, soit de 0.0.0.0 à 127.255.255.255. Certaines valeurs étant réservées à des usages particuliers. Un exemple d'adresse IP de classe A est : 10.50.49.13.

► Classe B
Une adresse IP de classe B dispose de deux octets pour identifier le réseau et de deux octets pour identifier les machines sur ce réseau. Un réseau de classe B peut comporter jusqu'à 22×8-2 postes, soit 216-2, soit 65 534 terminaux. Le premier octet d'une adresse IP de classe B commence toujours par la séquence de bits 10, il est donc compris entre 128 et 191. Un exemple d'adresse IP de classe B est : 172.16.1.23.

► Classe C
Une adresse IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau. Un réseau de classe C peut comporter jusqu'à 28-2 postes, soit 254 terminaux. Le premier octet d'une adresse IP de classe C commence toujours par la séquence de bits 110, il est donc compris entre 192 et 223. Un exemple d'adresse IP de classe C est : 192.168.1.34.

► Classe D
Les adresses de classe D sont utilisées pour les communications multicast. Le premier octet d'une adresse IP de classe D commence toujours par la séquence de bits 1110, il est donc compris entre 224 et 239. Un exemple d'adresse IP de classe D est : 224.0.0.1.

► Classe E
Les adresses de classe E sont réservées par IANA à un usage non déterminé. Les adresses de classe E commencent toujours par la séquence de bits 1111, ils débutent donc en 240.0.0.0 et se terminent en 255.255.255.255.

Classe	Bits de départ	Début	Fin	Notation CIDR par défaut	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	126.255.255.255[3] (127 est réservé)	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255		non défini
Classe E (réservée)	11110	240.0.0.0	255.255.255.255		non défini

Agrégation d'adresse

A partir de 1992 il a été décidé d'abolir la notion de classe qui n'était plus adaptée à la taille d'Internet.
On se retrouve donc avec des notations qui peuvent très bien être de ce type :

192.168.1.0 /23 ou le sous-réseau est identifié sur 23 bits. Ce qui permet d'ajouter des hôtes supplémentaire en diminuant le nombre de sous-réseaux possibles. L'avantage de cette méthode est qu'on peut affiner au mieux selon les besoins d'adressage. Ceci pour diminuer le plus possible le gaspillage d'adresse et de sous-réseaux.

Deux modes de fonctionnement

► *TCP (Transmission Control Protocol)*

• Caractéristiques principales :
Fiable : Les données arrivent dans le bon ordre, et si une partie est perdue, elle est renvoyée.
Orienté connexion : Une connexion est établie entre les deux appareils avant l'échange de données.
Contrôle de flux et d'erreurs : TCP vérifie que tout se passe bien (accusés de réception, correction d'erreurs…).
Plus lent : Toutes ces vérifications ajoutent de la latence.

• Exemples d'usage :
Navigation web (HTTP/HTTPS)
E-mails (SMTP, IMAP, POP)
Transferts de fichiers (FTP)

► *UDP (User Datagram Protocol)*

• Caractéristiques principales :
Non fiable : Les paquets peuvent arriver en désordre, être dupliqués ou perdus – aucune vérification.
Sans connexion : Pas besoin d'établir une connexion avant d'envoyer les données.
Pas de contrôle d'erreur : C'est à l'application de gérer les problèmes si besoin.
Très rapide : Moins de vérifications = moins de délai.

• Exemples d'usage :
Streaming vidéo ou audio en direct
Jeux en ligne
DNS (résolution de noms de domaine)
Appels VoIP (comme Skype)

Par analogie on pourrait dire que :

- **TCP** est comme envoyer une lettre en recommandé avec accusé de réception.
- **UDP** est comme envoyer une carte postale normale : c'est plus rapide, mais sans garantie qu'elle arrive.

On peut néanmoins effectuer des vérifications courtes à l'aide d'une somme de contrôle par exemple afin de fiabiliser l'UDP, ce qui est peu gourmant en ressource et conserve sont principale avantage, la vitesse.

► Les ports de communication

• Qu'est-ce qu'un port ?
Un port est un numéro d'identification (de 0 à 65535) utilisé pour désigner une application ou un service spécifique sur un appareil connecté à un réseau.

Imaginons que notre ordinateur est un immeuble, et que les ports sont les portes d'entrée de chaque appartement (application). L'adresse IP désigne l'immeuble, et le port désigne la porte.

• Pourquoi utiliser des ports ?
Quand notre PC envoie ou reçoit des données, le port permet de savoir à quelle application ces données doivent être livrées. Par exemple :

On ouvre un site web → le navigateur utilise le port 443 (HTTPS) ou port 80 (HTTP).
On reçoit des e-mails → le client mail utilise les ports 25, 110, 143, 587, 993, etc.
On joue en ligne → le jeu peut utiliser un port spécifique pour la communication (souvent en UDP).

• Différence entre TCP et UDP avec les ports
TCP et UDP ont leurs propres ensembles de ports, mais les numéros peuvent être les mêmes.

Exemple : Port 53 est utilisé en UDP pour les requêtes DNS rapides, mais aussi parfois en TCP pour les transferts plus longs de données DNS.

Plage de port	Nom	Usage
0 à 1023	Port bien connus	Réservés aux services systèmes (HTTP, FTP, DNS, SSH…)
1024 à 49151	Port enregistrés	Pour les applications utilisateurs (jeux, logiciels…)
49152 à 65535	Port Dynamiques	Éphémères, souvent choisis aléatoirement par les clients

Le NAT (Network Address Translation)

1. Pourquoi le NAT existe-t-il ?

L'espace d'adresses IPv4 est limité (environ 4,3 milliards d'IP). Pour éviter d'en manquer, on a créé le NAT.
Il permet :

- De partager une IP publique entre plusieurs machines.
- De masquer le réseau interne du reste d'Internet (sécurité).
- D'éviter d'attribuer une IP publique à chaque appareil chez toi ou en entreprise.

2. Exemple concret

- Nous disposons d'un routeur avec une IP publique : 82.123.45.67.
- À l'intérieur, nous avons plusieurs appareils avec des IP privées comme :
    - 192.168.0.2 (PC)
    - 192.168.0.3 (Smartphone)
    - 192.168.0.4 (TV)

Quand notre PC veut aller sur Internet :

1. Il envoie une requête à www.google.com.
2. Le routeur remplace l'adresse source (192.168.0.2) par son IP publique (82.123.45.67) et envoie la requête.
3. Google répond à 82.123.45.67.
4. Le routeur sait que cette réponse est pour notre PC, car il a gardé une trace (une table NAT).

3. Types de NAT

Type de NAT	Fonction principale
SNAT (Source NAT)	Modifie l'IP source (ex: vers Internet)
DNAT (Destination NAT)	Modifie l'IP de destination (ex: redirection vers un serveur interne)
PAT (Port Address Translation)	Variante de SNAT qui utilise les ports pour distinguer les connexions sortantes

4. Avantages du NAT

- Économie d'adresses IP (IPv4)
- Sécurité : l'IP locale n'est pas exposée directement à Internet
- Souplesse pour les petits réseaux

5. Inconvénients du NAT

- Difficile d'héberger un serveur interne accessible depuis l'extérieur sans configuration spécifique (port forwarding).
- Pas compatible avec tous les protocoles (certains protocoles comme SIP ou IPsec ont du mal avec le NAT).
- Ajoute une légère latence (car le routeur fait des modifications sur les paquets).

6. Port forwarding (redirection de port)
Quand tu veux ouvrir un port depuis Internet vers un appareil interne (comme un serveur Minecraft chez toi), tu configures une règle NAT spéciale :
Ex : Rediriger les connexions entrantes sur 82.123.45.67:25565 → 192.168.0.10:25565