Protocoles réseaux : DHCP et NAT

Prérequis :

- Fondamentaux réseaux : adressage IP, ports, etc.

Rappels théoriques : IPv4 & IPv6

IPv4 et IPv6

IPv4

Les adresses IPv4 sont utilisées depuis les débuts d'Internet. Elles sont adressées en 32 bits sur 4 octets.
Exemple : `51.68.45.52`.

> Le nombre total d'adresses disponibles est d'environ 4,3 milliards. Toutes les adresses IPv4 ont été attribuées depuis 2019.

Voir le détail de l'ARCEP : https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/lipv6/suivi-de-lepuisement-des-adresses-ipv4.html

Classes d'IPv4

Classe	Plage d'adresses publiques	Plage d'adresses privées	Usage
A	1.0.0.0 - 126.255.255.255	10.0.0.0 - 10.255.255.255	Grands réseaux
B	128.0.0.0 - 191.255.255.255	172.16.0.0 - 172.31.255.255	Réseaux moyens
C	192.0.0.0 - 223.255.255.255	192.168.0.0 - 192.168.255.255	Petits réseaux
D	224.0.0.0 - 239.255.255.255		Multicast
E	240.0.0.0 - 255.255.255.255		Réservé

Les **IP privées** sont utilisées sur un réseau local LAN, **elles ne sont pas routables sur internet**.
À l'inverse, les **IP publiques** sont routables sur internet. Elles sont attribuées par les fournisseurs.

Le `NAT` (Network address translation) permet à plusieurs IP privées de partager une seule IP publique.

> Nous approfondirons plus tard le protocole `NAT`.

IPv6

`IPv6` est le successeur d'`IPv4`, conçu pour résoudre le problème de pénurie d'adresses IP.

Les IPv6 sont adressées sur 128 bits, permettant de générer environ $3{,}4 \times 10^{38}$ adresses.

Exemple : `1050:0:0:0:5:600:300c:326b`

> Cela équivaut à un nombre illimité puisque pour saturer le système, il faudrait placer près de 2,30 trillions (milliards de milliards) d'appareils connectés à Internet sur chaque millimètre carré de surface terrestre émergée (148 millions de km^2).
>
> Article Wikipedia IPv6

Contrairement à `IPv4`, `IPv6` élimine le besoin de `NAT` : chaque appareil peut disposer d'une adresse IP publique unique.

Cependant, son adoption nécessite une infrastructure compatible, tant au niveau matériel que logiciel, ce qui représente un coût important pour les entreprises.
L'adoption d'IPv6 est inégale entre les pays du monde. Cela s'explique principalement par des différences dans la pression sur les ressources IPv4, les politiques publiques en matière de numérique, et le niveau de préparation technique des opérateurs locaux.

Sous-réseaux

L'implémentation de **sous-réseaux** permet de diviser un réseau IP en segments plus petits **en s'affranchissant des classes IPv4 prédéfinies**.

Chaque sous-réseau fonctionne comme un réseau indépendant.

Les cas d'usage sont par exemple l'optimisation du routage ou la séparation logique des services d'une organisation.

Notation CIDR et masque

La notation `CIDR` (Classless Inter-Domain Routing) permet de spécifier la longueur du préfixe réseau.

Par exemple :
`192.168.10.0/24`

- 24 bits pour le réseau
- 8 bits pour les hôtes

> Le masque correspondant est : `255.255.255.0`.

Calcul du nombre de sous-réseaux et d'hôtes

Pour créer des sous-réseaux, on **emprunte des bits** à la partie hôte.

Par exemple, un réseau en `192.168.1.0/24` contient **256 adresses**. Si on passe en `/26`, on utilise 2 bits supplémentaires pour le réseau.
Cela donne 4 sous-réseaux, chacun avec **64 adresses**, dont 62 utilisables.

Sous-réseau	Plage d’hôtes	Broadcast
192.168.1.0/26	192.168.1.1 – .62	192.168.1.63
192.168.1.64/26	192.168.1.65 – .126	192.168.1.127
192.168.1.128/26	192.168.1.129 – .190	192.168.1.191
192.168.1.192/26	192.168.1.193 – .254	192.168.1.255

Protocole DHCP

Introduction

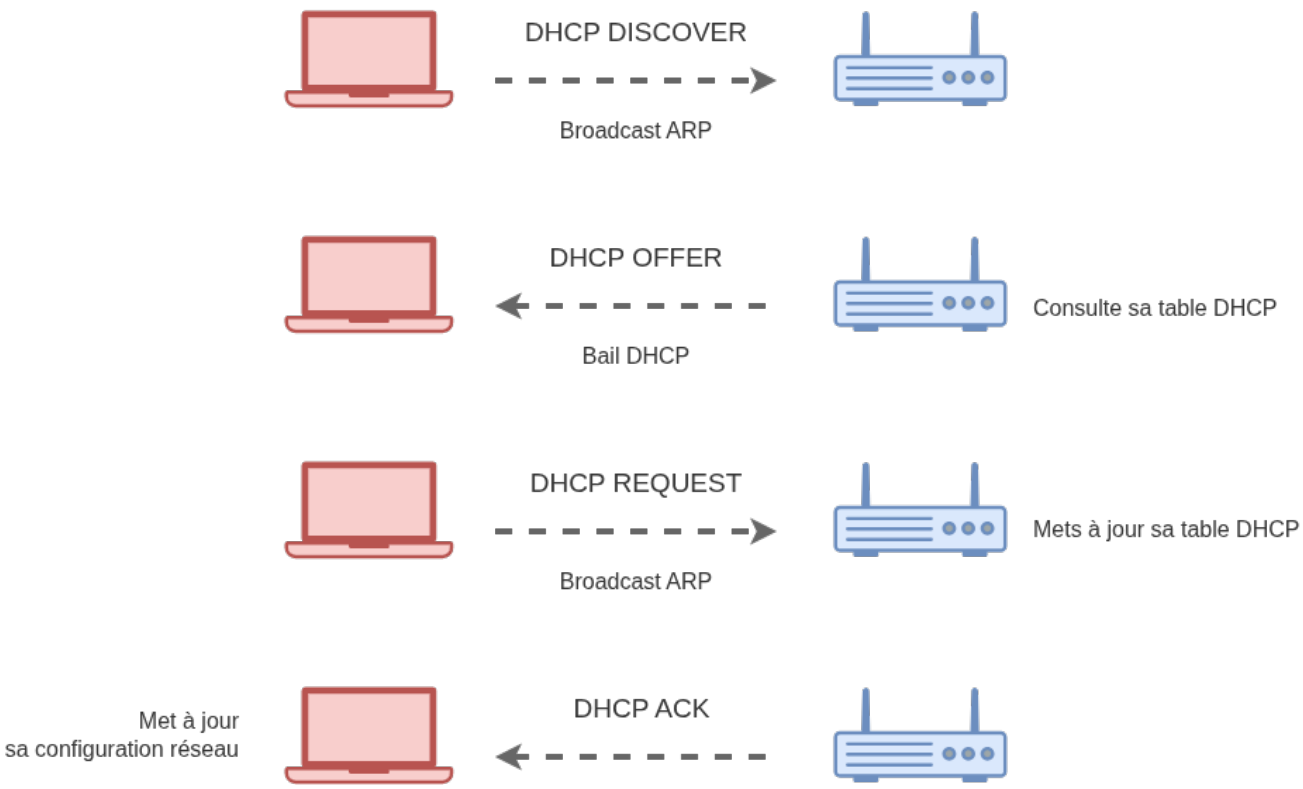
Le **DHCP** (Dynamic Host Configuration Protocol) est un protocole réseau utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres réseau aux machines d'un réseau local.

Il permet d'éviter la configuration manuelle des adresses IP par postes. La gestion est centralisée, avec moins de risques d'erreur.

Fonctionnement

Étapes

1. Lorsqu'un appareil rejoint un réseau, il envoie un message de découverte `DHCP Discover` pour annoncer sa présence. Le message est envoyé sur l'adresse de broadcast ARP `FF:FF:FF:FF:FF:FF`.
2. Un serveur `DHCP` répond avec une proposition de configuration réseau `DHCP Offer`.
3. L'appareil choisit une offre de configuration et envoie une demande `DHCP Request`.
4. Le serveur valide ce choix par un accusé de réception `DHCP Ack`.



> Ce mécanisme assure à chaque machine une configuration réseau adaptée sans intervention humaine.

Bail DHCP

Un **bail DHCP** est limité dans le temps, généralement quelques heures. À son expiration, le client doit le renouveler pour garder la même adresse IP.
Si le renouvellement échoue ou si le client ne demande pas de renouvellement, l'adresse IP peut être réattribuée à un autre hôte.

Le bail DHCP contient les informations suivantes :

- Une adresse IP
- Un masque de sous-réseau
- La durée du bail
- L'adresse IP de la passerelle
- Les adresses IP des serveurs DNS

> Il est possible d'affecter de manière permanente une adresse IP à une hôte.
> On parle alors de **réservation DHCP**.

Exception : adresses Apipa

Les adresses **APIPA** (Automatic Private IP Addressing) sont des adresses IP automatiquement attribuées par le système d'exploitation lorsqu'un client DHCP ne parvient pas à contacter un serveur DHCP.

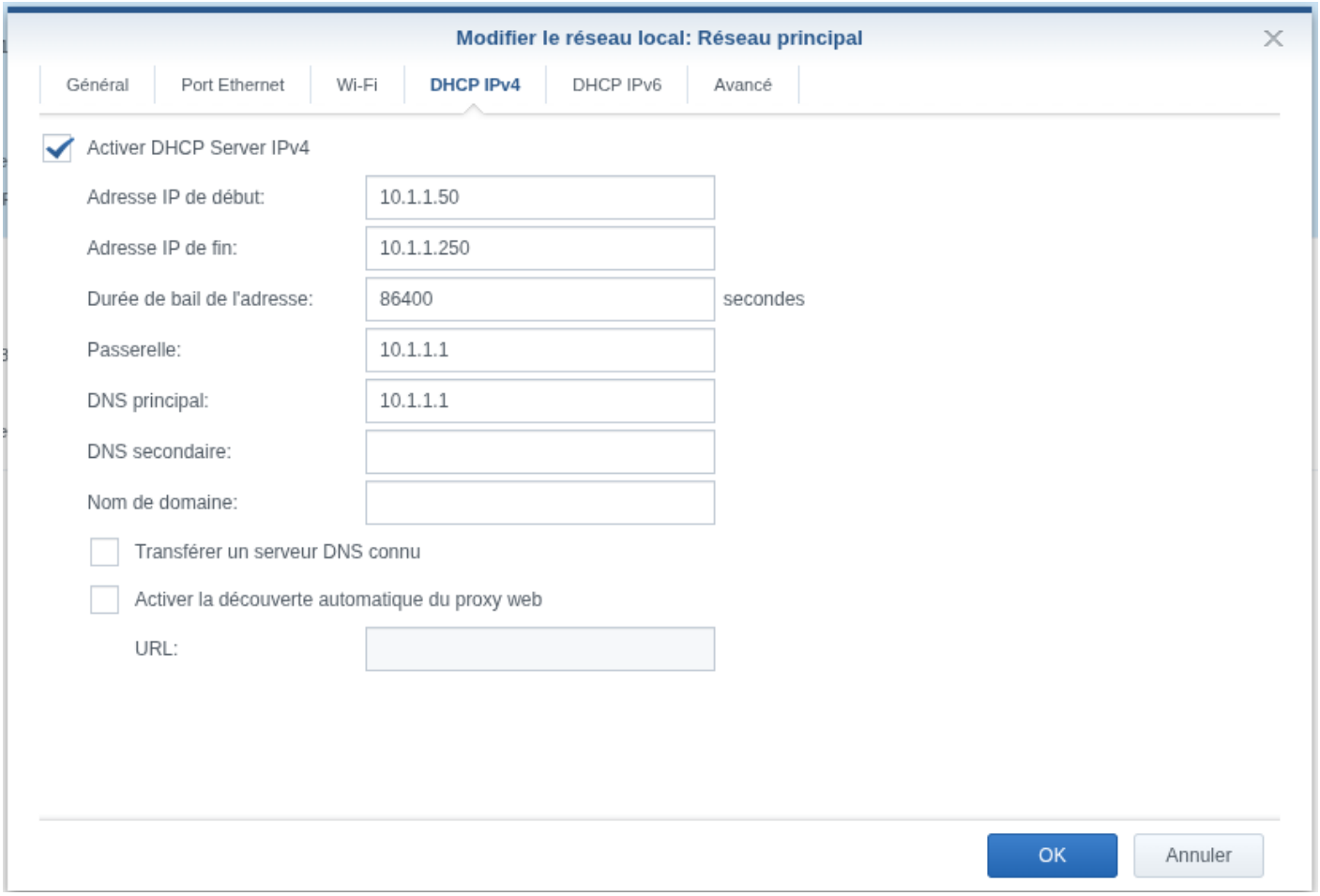
Ces adresses appartiennent à la plage `169.254.0.1` à `169.254.255.254`, réservée à cet usage.

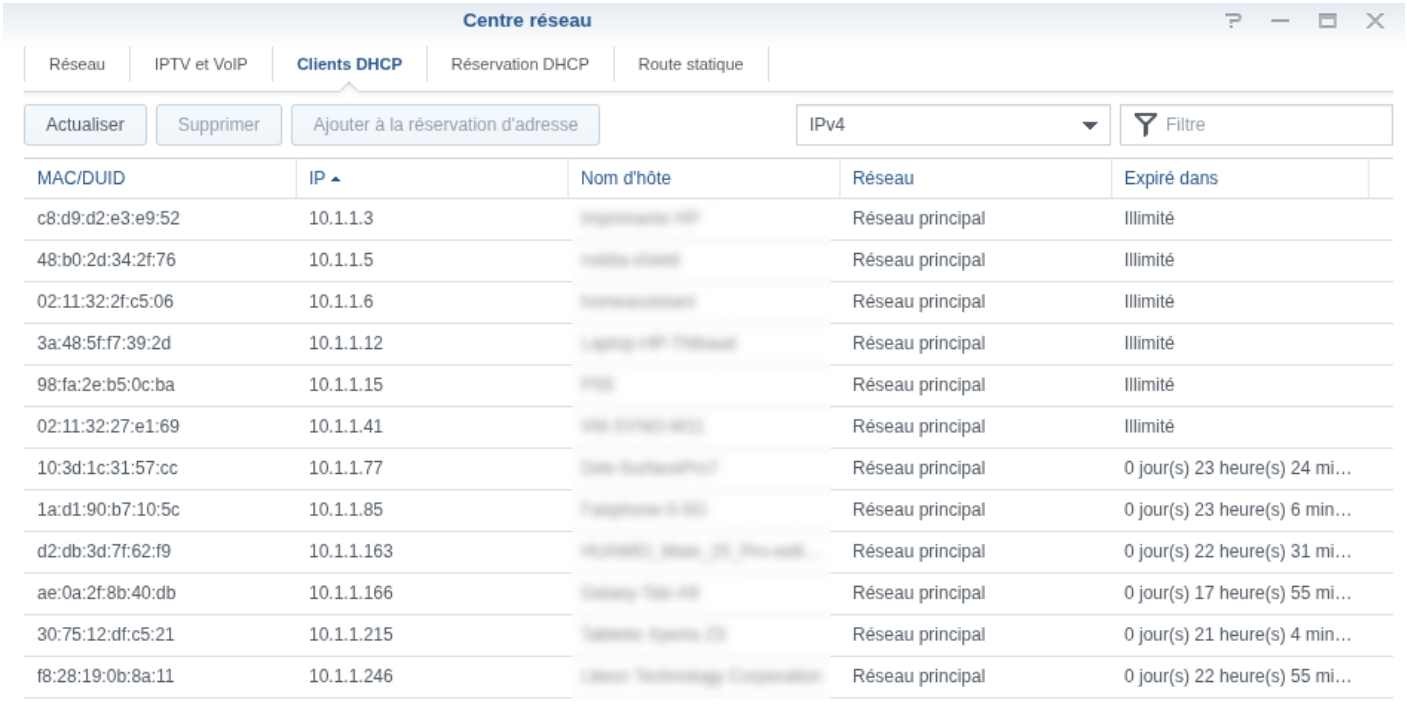
Elles permettent à des machines d'un même réseau local de communiquer entre elles, mais ne permettent pas l'accès à Internet.

> L'APIPA est une solution de secours temporaire, utile pour le diagnostic des problèmes de connectivité réseau.

Exemples de configuration

Serveur DHCP - Routeur Synology





> Les adresse IP `10.1.1.3` à `10.1.1.41` sont en réservation DHCP.

Client Windows

```
C:\Users\conta>ipconfig && ipconfig /release && ipconfig /renew

Configuration IP de Windows


Carte Ethernet Instance Ethernet 0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.1.41
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.1.1.1

Configuration IP de Windows


Carte Ethernet Instance Ethernet 0 :

   Suffixe DNS propre à la connexion. . . :
   Passerelle par défaut. . . . . . . . . :

Configuration IP de Windows


Carte Ethernet Instance Ethernet 0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.1.41
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.1.1.1

C:\Users\conta>
```

Protocole NAT

Le `NAT` (Network Address Translation) est un mécanisme utilisé pour faire transiter des paquets IP entre réseaux avec des plages d’adresses différentes, en modifiant les adresses source ou destination.

SNAT et DNAT

Il existe deux types de NAT :

Type	Fonction	Usage
SNAT	Modifie l'adresse source d'un paquet.	Utilisé pour permettre aux hôte d'un LAN d'accéder à Internet.
DNAT	Modifie l'adresse de destination d'un paquet.	Utilisé pour rediriger le trafic entrant vers un hôte interne au réseau local.

SNAT

Le SNAT est automatiquement activé sur les box et modems, ce qui permet aux équipements du réseau local d'accéder à Internet sans configuration manuelle.

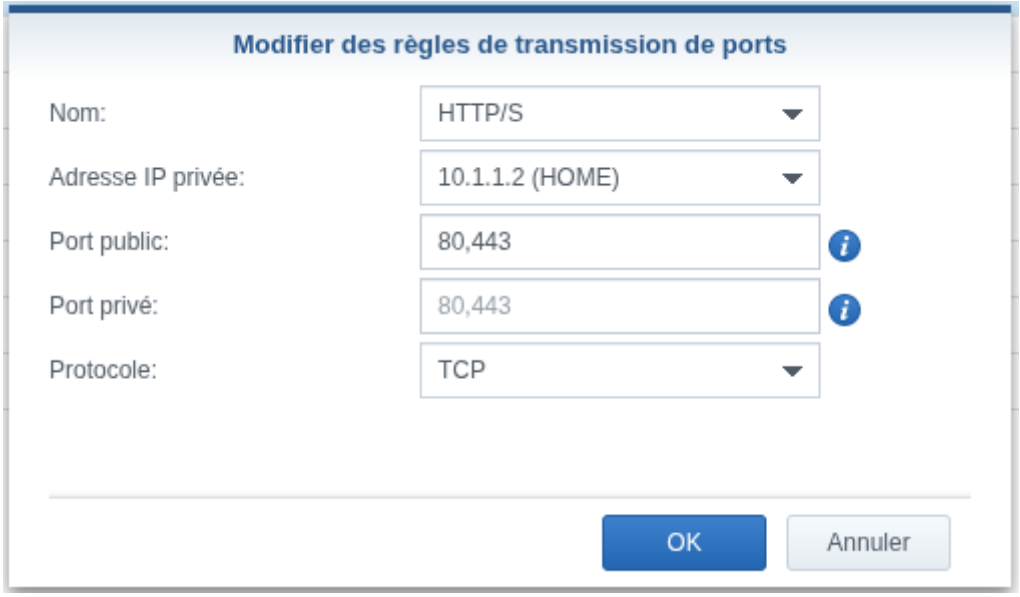
DNAT et Port Forwarding

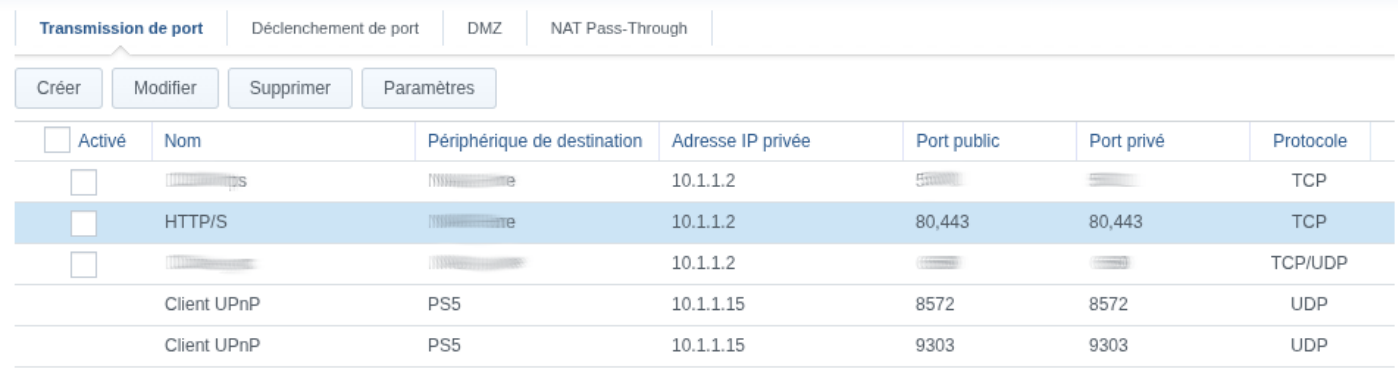
La redirection de port via DNAT est utilisée pour permettre l'accès à un service interne (hébergé sur une machine du réseau local) depuis l’extérieur du réseau.

La redirection consiste à modifier l'adresse IP et le port de destination d'un paquet entrant afin de le rediriger vers une machine du réseau local.

> Cette méthode est couramment utilisée pour exposer des services comme des serveurs web, FTP, SSH, etc. derrière un routeur NAT.

Exemple sur un routeur Synology





DMZ

Une `DMZ` (Demilitarized Zone) est, à l'origine, une zone réseau intermédiaire destinée à héberger des services accessibles depuis Internet, tout en protégeant le réseau interne grâce à une séparation stricte.

En pratique, dans de nombreuses configurations, le terme désigne un **hôte placé en dehors du pare-feu via un port forwarding global**, exposant tous ses ports à Internet, ce qui revient à le connecter directement au réseau public.

Cas particuliers

NAT UPnP

L'`UPnP` (Universal Plug and Play) est un protocole qui permet aux équipements connectés d'un réseau de demander au routeur d'ouvrir automatiquement certains ports.
`UPnP` est souvent nécessaire pour le fonctionnement d'applications spécifiques à travers le NAT (P2P, jeux en ligne, visios, etc.).

>

> Dans l'exemple ci-dessus, la PS5 a ouvert des ports UPnP. Probablement pour une mise à jour distribuée en P2P.

Concrètement, au lieu de devoir ajouter manuellement des règles de redirection de ports sur le routeur, `UPnP` permet à ces applications de créer ou supprimer elles-mêmes des règles de façon dynamique et temporaire.

> `UPnP` peut représenter un risque de sécurité : des programmes malveillants peuvent exploiter cette fonctionnalité pour s'ouvrir un accès depuis l'extérieur.

Hairpinning

Le **hairpinning NAT** (ou loopback NAT) est une fonctionnalité qui permet à un appareil du réseau local d'accéder à un autre appareil du même LAN via l'adresse IP publique du routeur.

Exemple :
Un smartphone est connecté sur un réseau Wi-Fi domestique. L'utilisateur souhaite accéder au NAS en utilisant l'adresse IP publique du modem et le port redirigé en NAT

- **Sans hairpinning :** La requête sort vers l'IP publique mais le routeur ne la **reboucle** pas vers le NAS. Résultat : ça ne fonctionne pas, le routeur bloque ou ignore la redirection pour une requête qui vient du LAN vers le LAN via l'IP publique.

- **Avec hairpinning :** Le routeur reconnaît cette situation, reboucle la requête et la redirige correctement vers le NAS, comme si la connexion venait de l'extérieur.

> La plupart des box opérateurs ne supportent pas correctement le hairspinning.

CGNAT

Le **CGNAT** (Carrier-Grade NAT, ou NAT de niveau opérateur) est une technique utilisée par les fournisseurs d'accès à Internet (FAI) pour **partager une seule adresse IPv4 publique entre plusieurs abonnés**.
Cela permet de pallier la pénurie d'adresses IPv4.

Normalement, chaque box ou routeur chez un particulier reçoit une adresse IP publique unique.

À l'inverse, avec le CGNAT, le FAI attribue une **adresse IP privée** à chaque client (comme dans un réseau local).

Plusieurs clients **partagent la même IP publique** et le FAI utilise un routeur NAT à grande échelle pour faire la traduction entre les IP privées des clients et l'IP publique partagée.

Quelques exemples

- **Fibre Free** : Sur certaines offres, **une seule IP publique est partagée entre 4 abonnés**. Il est possible d'activer une option (gratuite) pour obtenir une IP fixe et dédiée.
- **Starlink** : Par défaut, les utilisateurs sont derrière un CGNAT.
  Pour obtenir une **IP publique dédiée**, il faut **payer une option supplémentaire**.

> Le CGNAT rend impossible la redirection de port.