

CFA-23-24 -MD-01 - Initiation aux réseaux informatiques

[Accueil](#) / [Mes cours](#) / [CFA-23-24 -MD-01](#) / [11 - Adressage IpV4](#) / [11.3 - Types d'adresses IPv4](#)

11.3 - Types d'adresses IPv4

Adresses IPv4 publiques et privées

Tout comme il existe différentes façons de transmettre un paquet IPv4, il existe également différents types d'adresses IPv4. Certaines adresses IPv4 ne peuvent pas être utilisées pour sortir sur Internet, et d'autres sont spécifiquement allouées pour le routage vers Internet. Certains sont utilisés pour vérifier une connexion et d'autres sont auto-assignés. En tant qu'administrateur réseau, vous finirez par devenir très familier avec les types d'adresses IPv4, mais pour l'instant, vous devriez au moins savoir ce qu'ils sont et quand les utiliser.

Les adresses IPv4 publiques sont acheminées de manière globale entre les routeurs des ISP (fournisseurs d'accès à Internet). Toutefois, toutes les adresses IPv4 disponibles ne peuvent pas être utilisées sur Internet. Certains blocs d'adresses appelés adresses privées sont utilisés par la pluPartie des entreprises pour attribuer des adresses IPv4 aux hôtes internes.

Au milieu des années 1990, avec l'introduction du World Wide Web (WWW), les adresses IPv4 privées ont été introduites en raison de l'épuisement de l'espace d'adressage IPv4. Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par n'importe quel réseau interne.

Note: La solution à long terme à l'épuisement des adresses IPv4 était IPv6.

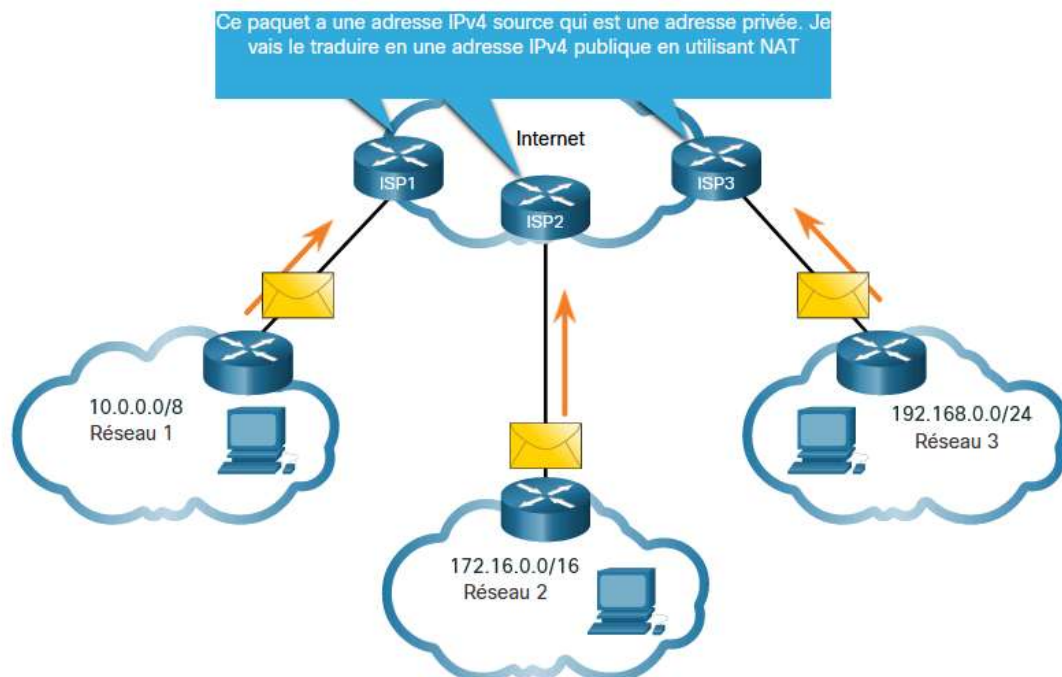
Adresse réseau et préfixe	Plage d'adresses privée RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Note: Les adresses privées sont définies dans RFC 1918 et parfois appelées espace d'adressage RFC 1918.

Routage sur Internet

La plupart des réseaux internes, des grandes entreprises aux réseaux domestiques, utilisent des adresses IPv4 privées pour adresser tous les périphériques internes (intranet), y compris les hôtes et les routeurs. Cependant, les adresses privées ne sont pas routables globalement.

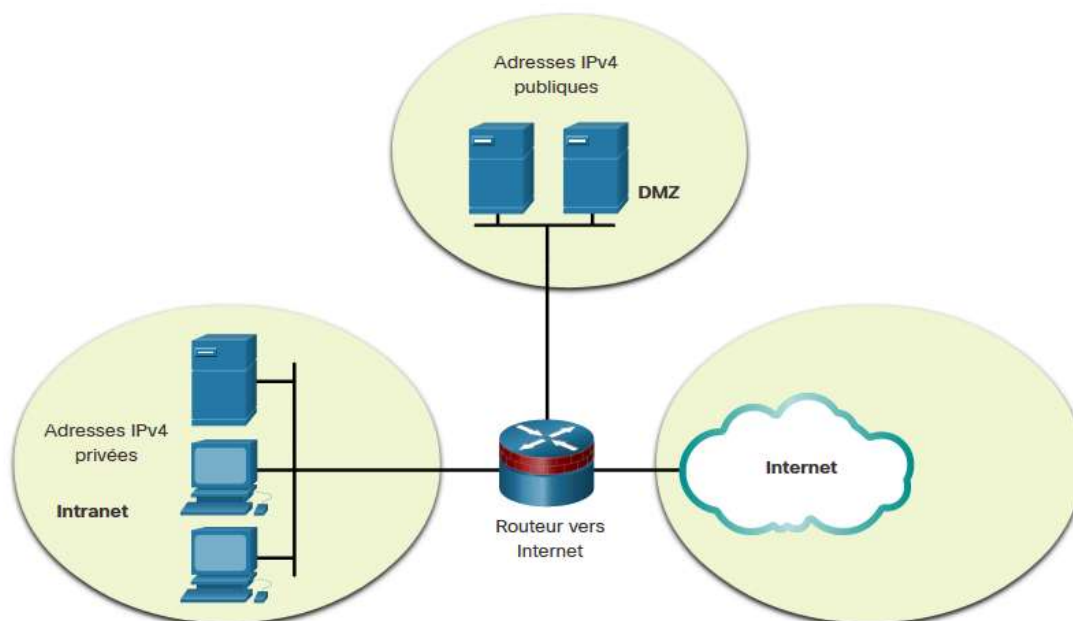
Dans la figure, les réseaux clients 1, 2 et 3 envoient des paquets en dehors de leurs réseaux internes. Ces paquets ont une adresse IPv4 source qui est une adresse privée et une adresse IPv4 de destination qui est publique (globalement routable). Les paquets avec une adresse privée doivent être filtrés (ignorés) ou traduits en adresse publique avant de transférer le paquet à un fournisseur de services Internet (ISP).



Avant que le FAI (ISP) puisse transférer ce paquet, il doit traduire l'adresse IPv4 source, qui est une adresse privée, vers une adresse IPv4 publique à l'aide de la traduction d'adresses réseau (NAT). La traduction d'adresses réseau (NAT) est utilisée pour convertir les adresses IPv4 privées en adresses IPv4 publiques. Généralement, cette opération s'effectue sur le routeur qui connecte le réseau interne à celui du ISP. Les adresses IPv4 privées dans l'intranet de l'organisation seront traduites en adresses IPv4 publiques avant d'être acheminées vers Internet.

Note: Bien qu'un périphérique doté d'une adresse IPv4 privée ne soit pas directement accessible depuis un autre périphérique sur Internet, l'IETF ne considère pas les adresses IPv4 privées ou NAT comme des mesures de sécurité efficaces.

Les organisations disposant de ressources disponibles sur Internet, telles qu'un serveur Web, disposeront également de périphériques dotés d'adresses IPv4 publiques. Comme le montre la figure, cette partie du réseau est connue sous le nom de DMZ (zone démilitarisée). Le routeur de la figure effectue non seulement le routage, il effectue également NAT et agit comme un pare-feu pour la sécurité.



Remarque: Les adresses IPv4 privées sont couramment utilisées à des fins éducatives au lieu d'utiliser une adresse IPv4 publique qui appartient probablement à une organisation.

Adresses IPv4 réservées

Certaines adresses, telles que l'adresse de réseau et l'adresse de diffusion, ne peuvent pas être attribuées aux hôtes. Il existe également des adresses spéciales qui peuvent être attribuées aux hôtes, mais des restrictions s'appliquent sur les interactions de ces hôtes sur le réseau.

Adresses de bouclage

Les adresses de bouclage (127.0.0.0 /8 ou 127.0.0.1 à 127.255.255.254) sont plus communément identifiées comme étant seulement 127.0.0.1, ce sont des adresses spéciales utilisées par un hôte pour diriger le trafic vers lui-même. Par exemple, elles peuvent être utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle, comme le montre la figure ci-contre. Remarquez comment l'adresse de bouclage 127.0.0.1 répond à la commande **ping**. Notez également que n'importe quelle adresse de ce bloc envoie les paquets en boucle à l'hôte local, comme le montre le résultat de la deuxième **ping** sur la figure ci-contre.

Envoi d'une requête ping sur l'interface de bouclage

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad> ping 127.1.1.1
Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad>
```

Adresses link-local

Adresses link-local ou adresses APIPA (Automatic Private IP Addressing) 169.254.0.0 /16 ou 169.254.0.1 à 169.254.255.254 Ils sont utilisés par un client DHCP Windows pour auto-configurer dans le cas où aucun serveur DHCP n'est disponible. Les adresses lien-local peuvent être utilisées dans une connexion peer-to-peer mais ne sont pas couramment utilisées à cette fin.

Adressage d'héritage par classe

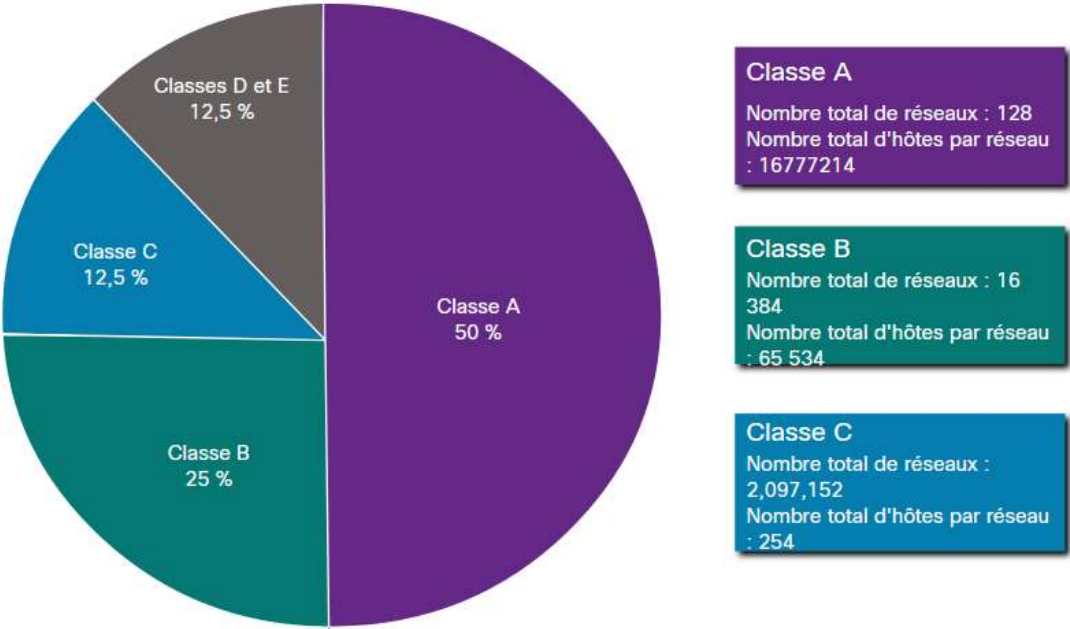
En 1981, les adresses IPv4 ont été attribuées en utilisant l'adressage par classe tel que défini dans la RFC 790

(<https://tools.ietf.org/html/rfc790>), Numéros assignés. On attribuait aux clients une adresse réseau selon l'une des trois classes (A, B ou C). La RFC répartissait les plages d'adresses à monodiffusion en plusieurs classes:

- **Classe A (0.0.0.0/8 à 127.0.0.0/8)** -conçue pour prendre en charge des réseaux de très grande envergure avec plus de 16 millions d'adresses d'hôte. La classe A utilisait un préfixe fixe /8 avec le premier octet pour indiquer l'adresse du réseau et les trois autres octets pour les adresses d'hôtes (plus de 16 millions d'adresses d'hôtes par réseau).
- **Classe B (128.0.0.0 /16 à 191.255.0.0 /16)** -conçue pour répondre aux besoins des réseaux de moyenne à grande envergure avec jusqu'à 65 000 adresses d'hôte environ. La classe B utilisait un préfixe fixe /16 avec les deux octets d'ordre supérieur pour indiquer l'adresse du réseau et les deux autres octets pour les adresses d'hôtes (plus de 65 000 adresses d'hôtes par réseau).
- **Classe C (192.0.0.0 /24 à 223.255.255.0 /24)** -conçue pour prendre en charge des réseaux de petite taille avec un maximum de 254 hôtes. La classe C utilisait un préfixe fixe /24 avec les trois premiers octets pour indiquer le réseau et l'octet restant pour les adresses d'hôtes (seulement 254 adresses d'hôtes par réseau).

Note: Il existe également un bloc de multidiffusion de classe D comprenant 224.0.0.0 à 239.0.0.0 et un bloc d'adresses expérimental de classe E comprenant 240.0.0.0 - 255.0.0.0.

À l'époque, avec un nombre limité d'ordinateurs utilisant Internet, l'adressage élégant était un moyen efficace d'allouer des adresses. Comme le montre la figure, les réseaux de classe A et B ont un très grand nombre d'adresses hôtes et la classe C en a très peu. Les réseaux de classe A représentaient 50 % des réseaux IPv4. Cela a causé l'inutilisation de la plupart des adresses IPv4 disponibles.



Au milieu des années 1990, avec l'introduction du World Wide Web (WWW), l'adressage de classe a été déprécié pour allouer plus efficacement l'espace d'adressage IPv4 limité. L'allocation d'adresses classful a été remplacée par l'adressage sans classe, qui est utilisé aujourd'hui. L'adressage sans classe ignore les règles des classes (A, B, C). Les adresses réseau IPv4 publiques (adresses réseau et masques de sous-réseau) sont allouées en fonction du nombre d'adresses pouvant être justifiées.

Modifié le: mardi 18 juin 2024, 10:06

◀ 11.2 - Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion
Aller à...

Connecté sous le nom « Lucas SEYOT » (Déconnexion)
CFA-23-24 -MD-01
BTS SIO Lycée CFA Robert Schuman Metz

- Français (fr)
- English (en)
- Français (fr)

Résumé de conservation de données
Obtenir l'app mobile