Engineer

Adresse IP

Nombre indiquant où livrer un paquet sur le réseau

Ce que c’est

Une adresse IP est le nombre que le protocole Internet inscrit dans chaque paquet pour indiquer sa destination, à côté d’une seconde adresse qui indique sa provenance. La RFC 791, spécification de 1981 de la version 4 d’IP, la nomme adresse Internet et résume la distinction en une phrase : « Une adresse indique où cela se trouve. » Un nom, comme un domaine, indique ce que vous cherchez et doit d’abord être converti en adresse, ce qui est le rôle du DNS. La route, le chemin entre les deux adresses, revient aux routeurs intermédiaires.

En IPv4, l’adresse compte 32 bits, soit quatre octets, écrits sous forme de quatre nombres décimaux de 0 à 255 séparés par des points : 192.0.2.10. La RFC 791 répartissait ces bits entre un numéro de réseau et une partie locale, avec trois classes fixes qui déterminaient la position de la séparation. Ces classes convenaient mal à la plupart des organisations : un réseau de classe C accueillait au plus 254 hôtes, un de classe B jusqu’à 65 534. Les numéros de classe B se raréfiaient donc tandis que les tables de routage grossissaient. En septembre 1993, la RFC 1519 a remplacé les classes par CIDR, qui permet de séparer après n’importe quel bit et d’indiquer cette position après une barre oblique. 192.0.2.0/24 désigne le bloc dont les 24 premiers bits sont fixes : 256 adresses.

IPv6 porte l’adresse à 128 bits. Elle s’écrit sous forme de huit groupes contenant jusqu’à quatre chiffres hexadécimaux, séparés par des deux-points. La RFC 4291 permet de réduire une suite de groupes de zéros à `::`, si bien que 2001:db8:0:0:0:0:2:1 peut aussi s’écrire 2001:db8::2:1. Une même adresse pouvant ainsi s’écrire de plusieurs façons, la RFC 5952 a ensuite fixé une forme recommandée : des minuscules, aucun zéro initial dans un groupe et `::` pour la plus longue suite de groupes de zéros.

Une adresse appartient à une interface réseau, pas à une machine. La RFC 791 précisait déjà qu'un hôte unique devait pouvoir agir comme plusieurs hôtes, avec plusieurs adresses Internet, et que certains hôtes avaient plusieurs interfaces physiques. La RFC 4291 exige que chaque interface IPv6 possède au moins une adresse locale de lien, valable uniquement sur son propre segment réseau, quelles que soient ses autres adresses. Un hôte sur un réseau utilisant les deux versions porte donc plusieurs adresses à la fois, en plus des adresses de bouclage qu'il utilise pour se joindre lui-même : le bloc 127.0.0.0/8 en IPv4 et `::1` en IPv6.

Toutes les adresses ne sont pas joignables de partout. La RFC 1918 réserve trois blocs IPv4 aux réseaux privés, 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16, et précise que les informations de routage les concernant ne doivent pas être transmises entre organisations. Un appareil qui en possède une n'accède donc à Internet que par un intermédiaire qui le représente, tel que NAT, que la RFC 3022 décrit comme la traduction de l'adresse privée en adresse publique à la sortie. La RFC 5737 réserve trois autres blocs, 192.0.2.0/24, 198.51.100.0/24 et 203.0.113.0/24, à la documentation ; la RFC 3849 fait de même pour 2001:db8::/32 en IPv6. Toutes les adresses d'exemple de cet article proviennent de ces plages de documentation.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'une adresse IP ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Du Wi-Fi, des pare-feu et des accès à distance configurés pour travailler de partout, en laissant entrer uniquement les personnes autorisées.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 30 instances VPS Ubuntu Linux administrées — 30 serveurs Linux gérés, avec récupération prévue

30 instances VPS Ubuntu Linux administrées Contactez-nous →

Pourquoi c'est important

L'adresse est le seul renseignement sur un client dont un serveur dispose toujours : sans elle, la réponse n'aurait aucune destination. Elle sert donc de clé habituelle pour de nombreuses décisions : les règles de pare-feu autorisent ou bloquent selon l'adresse, une limitation de débit compte les requêtes par adresse, un journal d'accès l'inscrit à chaque ligne et un signalement d'abus la mentionne. La fiabilité de chacun de ces mécanismes dépend de la capacité de l'adresse à identifier ce que vous pensez qu'elle identifie.

Elle identifie moins de choses qu'il n'y paraît. Derrière NAT, tous les appareils d'un bureau ou d'un foyer peuvent accéder à Internet depuis la même adresse IPv4 publique : un blocage ou une limite visant l'un s'applique donc à tous. Derrière un proxy ou un CDN, le serveur voit l'adresse du proxy à chaque requête et l'adresse propre du client arrive, si elle arrive, dans un en-tête écrit par quelqu'un d'autre. Une règle fondée sur une adresse porte sur une position dans le réseau, jamais sur une personne.

En même temps, elle révèle plus qu'on ne le pense. La RFC 7239, qui a normalisé l'en-tête `Forwarded` utilisé par les proxies pour transmettre l'adresse du client, précise dans sa section sur la vie privée qu'une adresse IP peut identifier un client de manière unique, révéler son opérateur et donner une idée approximative de son emplacement. Un journal rempli d'adresses est donc un risque autant qu'un outil, et une bonne raison de décider ce que l'on conserve avant de commencer à le conserver.

Et il en existe désormais deux sortes. Tout ce qui analyse, stocke ou compare des adresses doit accepter IPv4 comme IPv6, car un client sur un réseau proposant les deux peut arriver par l'un ou l'autre. Le code écrit lorsque toute adresse tenait en quinze caractères faits de chiffres et de points échoue dès le premier visiteur IPv6, généralement loin de l'endroit où l'adresse a été lue.

À quoi cela ressemble en pratique

La bibliothèque standard de Python comprend un module `ipaddress` qui analyse les deux versions et effectue les calculs, évitant de découper les chaînes à la main. Dans une session interactive :

```
>>> import ipaddress
>>> ipaddress.ip_address("203.0.113.57")
IPv4Address('203.0.113.57')
>>> ipaddress.ip_address("2001:0DB8:0000:0000:0000:0000:0002:0001")
IPv6Address('2001:db8::2:1')
>>> ipaddress.ip_network("203.0.113.57/24", strict=False)
IPv4Network('203.0.113.0/24')
>>> ipaddress.ip_network("2001:db8:42:7::5/48", strict=False)
IPv6Network('2001:db8:42::/48')
```

Le deuxième appel montre la normalisation demandée par la RFC 5952 : la longue écriture en majuscules et la courte en minuscules désignent la même adresse, et le module affiche la forme canonique. Une chaîne comme 192.0.2.300 est refusée avec une exception `ValueError`, car 300 ne tient pas dans un octet. Les deux derniers appels convertissent l'adresse en son réseau. Sans `strict=False`, le module les refuserait aussi, car 203.0.113.57/24 contient des bits d'hôte à un ; avec cette option, la partie hôte est mise à zéro et il ne reste que le réseau.

C'est ainsi que le journal d'accès web de ce site traite les adresses des visiteurs. Sa page sur la vie privée indique que l'adresse est raccourcie au moment d'écrire la ligne du journal web : sa dernière partie est remplacée par des zéros avant que la ligne atteigne le disque. La valeur conservée identifie ainsi un réseau approximatif dans lequel un bureau entier ou une rue peuvent paraître identiques. Le serveur enregistre l'adresse sous deux noms, masque les deux et retire les en-têtes pouvant contenir leur propre adresse avant d'écrire la ligne. La page ne dit pas combien de bits subsistent ; les /24 et /48 ci-dessus illustrent cet article, pas les réglages du site. Masquer à l'écriture évite de conserver les adresses complètes dans ce journal web sans dépendre d'un nettoyage ultérieur. La même page de confidentialité consigne séparément une exception Gopher : le journal du système d'exploitation, établi par connexion, indique l'adresse source et expire au bout de trente jours.

Où les problèmes surviennent

Faire confiance à un en-tête pour l'adresse du client. `X-Forwarded-For` et l'en-tête standard `Forwarded` sont de simples en-têtes de requête. La RFC 7239 avertit que tout intermédiaire entre le client et le serveur, ainsi que le client lui-même, peut réécrire l'en-tête `Forwarded`, par erreur ou volontairement. Un code qui prend la première adresse de la liste permet à n'importe quel client de choisir sa propre adresse, et donc sa limite de débit et sa place dans une liste d'autorisation. Utilisez l'adresse de la connexion TCP, sauf si la requête est passée par un proxy que vous exploitez ; ne lisez alors que ce que vos propres proxies ont ajouté, en partant de la droite.

Assimiler une adresse à une personne. Puisque plusieurs utilisateurs peuvent partager une adresse, son bannissement peut exclure un bureau entier, et une limite dimensionnée pour une personne bride une école entière. Utilisez les adresses pour des décisions peu fines, fixez les limites en tenant compte des adresses partagées et rattachez plutôt tout ce qui est personnel à un compte authentifié.

Comparer les adresses comme des chaînes. 2001:db8::2:1 et 2001:DB8:0:0:0:0:2:1 sont une seule adresse et deux chaînes différentes : une liste d'autorisation fondée sur le texte accepte donc l'une et refuse l'autre. Analysez les deux côtés avant de les comparer ou ne stockez que la forme de la RFC 5952.

N'analyser qu'IPv4. Une expression régulière pour quatre nombres séparés par des points, une colonne limitée à quinze caractères ou un code qui sépare l'hôte du port au dernier deux-points échoueront avec IPv6. Utilisez un véritable analyseur et un type ou une longueur de colonne prévus pour les deux versions. Quand un port est écrit à côté d'une adresse IPv6, la RFC 5952 recommande les crochets, comme dans [2001:db8::1]:443, car sans eux le dernier groupe pourrait être lu comme une partie de l'adresse.

Conserver les adresses complètes plus longtemps que nécessaire. Les journaux, les tables d'analyse et les sauvegardes accumulent des adresses pendant des années si rien ne les en empêche. Décidez de la précision nécessaire, raccourcissez l'adresse au moment de l'écriture plutôt qu'après et donnez une date d'expiration à ce qui reste.

Utiliser de vraies adresses dans les exemples. Un exemple de configuration, un jeu de données de test ou une capture d'écran qui utilise l'adresse réelle de quelqu'un dirige le trafic copié vers un inconnu. La RFC 5737 réserve précisément ses trois blocs pour réduire ce type de conflits et de confusions ; utilisez-les, ainsi que 2001:db8::/32 pour IPv6.

Pour aller plus loin

- RFC 791 : protocole Internet — la spécification d'IPv4 de 1981, avec son adresse de 32 bits et la distinction entre noms, adresses et routes.
- RFC 4291 : architecture d'adressage d'IP version 6 — les types d'adresses IPv6, leurs écritures textuelles et l'obligation d'une adresse locale de lien.
- RFC 5952 : recommandation pour la représentation textuelle des adresses IPv6 — une manière canonique d'écrire une adresse IPv6 et les difficultés causées par la souplesse des écritures.
- RFC 7239 : extension HTTP Forwarded — transmission de l'adresse d'un client par les proxies, raisons de ne pas faire simplement confiance au résultat et coût pour la vie privée.
- RFC 5737 : blocs d'adresses IPv4 réservés à la documentation — les trois plages prévues pour les exemples.

- ipaddress : bibliothèque de manipulation d'IPv4 et d'IPv6 — le module standard de Python pour analyser, comparer et regrouper les adresses.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'une adresse IP ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/ip-address/