Engineer

Dirección IP

Número que indica adónde debe entregarse un paquete

Qué es

Una dirección IP es el número que el Protocolo de Internet escribe en cada paquete para indicar adónde va, junto a una segunda dirección que indica de dónde viene. RFC 791, la especificación de 1981 de la versión 4 de IP, la llama dirección de Internet y marca la diferencia en una frase: «Una dirección indica dónde está». Un nombre, como un dominio, indica qué se busca y primero debe convertirse en una dirección, tarea de DNS. La ruta, el camino entre las dos direcciones, queda a cargo de los routers intermedios.

En IPv4, la dirección tiene 32 bits, cuatro octetos, escritos como cuatro números decimales de 0 a 255 separados por puntos: 192.0.2.10. RFC 791 dividía esos bits en un número de red y una parte local, con tres clases fijas que determinaban dónde se hacía la división. Las clases encajaban mal con la mayoría de las organizaciones: una red de clase C admitía como máximo 254 hosts y una de clase B hasta 65.534, por lo que escaseaban los números de clase B mientras crecían las tablas de enrutamiento. En septiembre de 1993, RFC 1519 sustituyó las clases por CIDR, que permite dividir después de cualquier bit e indica la posición tras una barra. 192.0.2.0/24 es el bloque cuyos primeros 24 bits son fijos: 256 direcciones.

IPv6 amplía la dirección a 128 bits. Se escribe como ocho grupos de hasta cuatro dígitos hexadecimales separados por dos puntos, y RFC 4291 permite comprimir una secuencia de grupos de ceros en `::`, de modo que 2001:db8:0:0:0:0:2:1 también puede escribirse 2001:db8::2:1. Como así una dirección podía tener muchas representaciones, RFC 5952 fijó después una forma recomendada: minúsculas, ningún cero inicial en cada grupo y `::` para la secuencia más larga de grupos de ceros.

Una dirección pertenece a una interfaz de red, no a una máquina. RFC 791 ya decía que un solo host debe poder actuar como varios, con varias direcciones de Internet, y que algunos hosts tienen varias interfaces físicas. RFC 4291 exige que cada interfaz IPv6 tenga al menos una dirección local de enlace, válida solo en su propio segmento de red, sean cuales sean sus demás direcciones. Por tanto, un host en una red que utiliza ambas versiones tiene varias direcciones a la vez, además de las direcciones de bucle local que utiliza para acceder a sí mismo: el bloque 127.0.0.0/8 en IPv4 y `::1` en IPv6.

No todas las direcciones son accesibles desde cualquier lugar. RFC 1918 reserva tres bloques IPv4 para redes privadas, 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16, e indica que no se debe transmitir información de enrutamiento sobre ellos entre organizaciones. Por eso, un dispositivo con una de esas direcciones solo llega a Internet a través de algo que actúe en su nombre, como NAT, que RFC 3022 describe como la traducción de la dirección privada a una pública al salir. RFC 5737 reserva otros tres bloques, 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24, para documentación, y RFC 3849 hace lo mismo con 2001:db8::/32 en IPv6. Todas las direcciones de ejemplo de este artículo proceden de esos rangos de documentación.

Utilice el concepto en una decisión

Aplique «¿Qué es una dirección IP?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Wi-Fi, cortafuegos y acceso remoto configurados para trabajar desde cualquier lugar y permitir el acceso solo a las personas autorizadas.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. Administración de 30 VPS Ubuntu Linux — 30 servidores Linux administrados con recuperación planificada

Administración de 30 VPS Ubuntu Linux Póngase en contacto →

Por qué importa

La dirección es el único dato sobre un cliente que un servidor siempre tiene, porque sin ella la respuesta no tendría destino. Por eso se utiliza como clave predeterminada para muchas decisiones: las reglas de un cortafuegos permiten o bloquean por dirección, un límite de solicitudes cuenta las peticiones por dirección, un registro de acceso la escribe en cada línea y una denuncia de abuso la identifica. Cada mecanismo solo funciona en la medida en que la dirección identifica lo que se supone que identifica.

Identifica menos de lo que parece. Tras NAT, todos los dispositivos de una oficina o de un hogar pueden acceder a Internet desde la misma dirección IPv4 pública, de modo que un bloqueo o un límite dirigido a uno afecta a todos. Tras un proxy o una CDN, el servidor ve la dirección del proxy en cada petición, y la dirección del propio cliente llega, si llega, en una cabecera escrita por otro. Una regla basada en una dirección se refiere a una posición en la red, nunca a una persona.

Al mismo tiempo, revela más de lo esperado. RFC 7239, que normalizó la cabecera `Forwarded` con la que los proxies transmiten la dirección del cliente, señala en su sección de privacidad que una dirección IP puede identificar de forma única a un cliente, mostrar qué operador utiliza y dar una idea aproximada de dónde está. Un registro lleno de direcciones es, por tanto, una fuente de riesgo además de una herramienta, y un buen motivo para decidir qué se conservará antes de empezar a guardarlo.

Además, ahora hay dos tipos. Todo lo que analiza, almacena o compara direcciones debe aceptar tanto IPv4 como IPv6, porque un cliente en una red que ofrece ambos puede llegar por cualquiera de ellos. El código escrito cuando toda dirección cabía en quince caracteres de cifras y puntos falla con el primer visitante IPv6, normalmente lejos del punto donde se leyó la dirección.

Cómo se aplica en la práctica

La biblioteca estándar de Python incluye el módulo `ipaddress`, que analiza ambas versiones y hace los cálculos para que nunca haya que dividir cadenas a mano. En una sesión interactiva:

```
>>> 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')
```

La segunda llamada muestra la normalización que pide RFC 5952: la representación larga en mayúsculas y la corta en minúsculas son la misma dirección, y el módulo imprime la forma canónica. Una cadena como 192.0.2.300

se rechaza con un `ValueError`, porque 300 no cabe en un octeto. Las dos últimas llamadas convierten una dirección en la red que la contiene. Sin `strict=False`, el módulo también las rechazaría, porque 203.0.113.57/24 tiene bits de host activados; con esa opción, la parte del host se pone a cero y solo queda la red.

Así trata el registro de acceso web de este sitio las direcciones de sus visitantes. Su página de privacidad explica que la dirección se acorta al escribir la línea del registro web: su última parte se sustituye por ceros antes de que la línea llegue al disco. El valor conservado identifica una red aproximada en la que toda una oficina o una calle pueden parecer idénticas. El servidor registra la dirección con dos nombres, enmascara ambos y elimina las cabeceras que pueden contener una dirección propia antes de escribir la línea. La página no especifica cuántos bits se conservan; los /24 y /48 anteriores son ejemplos de este artículo, no la configuración del sitio. Enmascarar al escribir mantiene las direcciones completas fuera de ese registro web sin depender de una limpieza posterior. La misma página de privacidad documenta por separado una excepción de Gopher: el registro por conexión del sistema operativo incluye la dirección de origen y caduca al cabo de treinta días.

Dónde surgen los problemas

Confiar en una cabecera para obtener la dirección del cliente. `X-Forwarded-For` y la cabecera estándar `Forwarded` son cabeceras de petición corrientes. RFC 7239 advierte de que cualquier salto entre el cliente y el servidor, y el propio cliente, puede reescribir `Forwarded` por error o deliberadamente. El código que toma la primera dirección de la lista permite que cualquier cliente elija su propia dirección y, con ella, su propio límite de solicitudes y su lugar en una lista de permitidos. Utilice la dirección de la conexión TCP, salvo que la petición haya pasado por un proxy que usted gestione; en ese caso, lea solo lo que hayan añadido sus propios proxies, contando desde la derecha.

Tratar una dirección como una persona. Como muchos usuarios pueden compartir una dirección, bloquearla puede dejar fuera a toda una oficina, y un límite dimensionado para una persona restringe a toda una escuela. Utilice las direcciones para decisiones generales, establezca límites pensando en las direcciones compartidas y vincule lo personal a una cuenta autenticada.

Comparar direcciones como cadenas. 2001:db8::2:1 y 2001:DB8:0:0:0:0:2:1 son una dirección y dos cadenas distintas, por lo que una lista de permitidos basada en texto acepta una y rechaza la otra. Analice ambos lados antes de compararlos

o almacene solo la forma de RFC 5952.

Analizar solo IPv4. Una expresión regular para cuatro números separados por puntos, una columna de quince caracteres o código que divide host y puerto en el último signo de dos puntos fallan con IPv6. Utilice un analizador real y un tipo o una longitud de columna adecuados para ambas versiones. Cuando se escribe un puerto junto a una dirección IPv6, RFC 5952 recomienda corchetes, como en [2001:db8::1]:443, porque sin ellos el último grupo podría interpretarse como parte de la dirección.

Conservar direcciones completas más tiempo del necesario. Los registros, las tablas de analítica y las copias de seguridad acumulan direcciones durante años si nada lo impide. Decida qué precisión necesita, acorte la dirección al escribirla en lugar de hacerlo después y asigne una fecha de caducidad a lo que quede.

Utilizar direcciones reales en ejemplos. Una configuración de ejemplo, un conjunto de datos de prueba o una captura de pantalla que utiliza la dirección real de alguien envía tráfico copiado a un desconocido. RFC 5737 reserva sus tres bloques precisamente para reducir esos conflictos y confusiones; utilícelos, junto con 2001:db8::/32 para IPv6.

Lecturas adicionales

- RFC 791: Protocolo de Internet — la especificación de IPv4 de 1981, con su dirección de 32 bits y la distinción entre nombres, direcciones y rutas.
- RFC 4291: arquitectura de direccionamiento de IP versión 6 — los tipos de direcciones IPv6, sus representaciones textuales y el requisito de una dirección local de enlace.
- RFC 5952: recomendación para representar direcciones IPv6 como texto — una forma canónica de escribir una dirección IPv6 y los problemas de permitir distintas representaciones.
- RFC 7239: extensión HTTP Forwarded — cómo transmiten los proxies la dirección de un cliente, por qué no se puede confiar sin más en el resultado y su coste para la privacidad.
- RFC 5737: bloques de direcciones IPv4 reservados para documentación — los tres rangos destinados a ejemplos.
- ipaddress: biblioteca de manipulación de IPv4 e IPv6 — el módulo estándar de Python para analizar, comparar y agrupar direcciones.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es una dirección IP?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

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

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

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

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/ip-address/