Engineer

DHCP

protocolo que presta direcciones IP y ajustes a equipos

Qué es

DHCP, Dynamic Host Configuration Protocol o protocolo de configuración dinámica de hosts, permite que un dispositivo recién conectado a una red sepa qué configuración le corresponde en ella. Un portátil que se conecta a una red Wi-Fi conoce su dirección de hardware y poco más. DHCP le da una dirección IP, la máscara de subred, el router por el que enviar el tráfico y los servidores DNS a los que consultar, sin que nadie tenga que introducirlos. El protocolo se define en el RFC 2131, publicado en marzo de 1997, cuyo resumen lo presenta como una forma de entregar información de configuración a los hosts de una red TCP/IP. Deriva del anterior Bootstrap Protocol, BOOTP, y su principal aportación fue la asignación automática de direcciones reutilizables.

El RFC 2131 describe tres formas de entregar una dirección. En la asignación automática, el cliente recibe una dirección permanente. En la dinámica, la recibe por un periodo limitado o hasta que la devuelve. En la manual, el administrador de red elige la dirección y DHCP se limita a entregarla. De las tres, solo la asignación dinámica permite que una dirección vuelva por sí sola al grupo de direcciones cuando su titular ya no la necesita, y es el mecanismo del que trata el resto de este artículo.

El periodo durante el que se presta una dirección se llama concesión. El cliente puede ampliarla, devolver la dirección antes e incluso pedir una concesión infinita; el RFC señala que un servidor puede seguir prefiriendo concesiones largas pero finitas para terminar detectando a un cliente retirado. Detrás del servidor está lo que el RFC llama almacenamiento persistente: una entrada por cliente que usa un identificador como clave y conserva los parámetros que recibió ese cliente.

DHCP funciona sobre UDP. Los clientes envían al puerto 67 del servidor y los servidores responden al puerto 68 del cliente. Las opciones que puede enviar un servidor, desde la máscara de subred hasta el tiempo de concesión, se especifican aparte, en el RFC 2132. IPv6 tiene su propio protocolo, DHCPv6, actualmente especificado en el RFC 9915, un Estándar de Internet de enero de 2026 que sustituyó al RFC 8415. Utiliza otros puertos, 546 para clientes y 547 para servidores y agentes de retransmisión, y puede funcionar en lugar de la autoconfiguración de direcciones sin estado, SLAAC, o junto a ella. El propio RFC 9915 llama DHCPv4 al protocolo IPv4 cuando necesita distinguirlos y recoge el consenso del IETF de que la configuración IPv4 debería viajar por DHCPv4 en lugar de DHCPv6.

Utilice el concepto en una decisión

Aplique «¿Qué es DHCP?» 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

Todos los dispositivos de una red necesitan el mismo puñado de ajustes, y un valor incorrecto basta para desconectarlos: una máscara que no coincide con la subred, una dirección de router que pertenece a otro o un servidor DNS que se apagó el año pasado. Sin DHCP, cada valor tiene que introducirse en cada dispositivo y mantenerse correcto cada vez que cambie algo. Con DHCP, están en un solo lugar y cambiar el servidor DNS de toda una oficina pasa a ser un cambio en la configuración del servidor en lugar de un recorrido por el edificio.

La concesión es lo que permite escalar al protocolo. Como la asignación dinámica presta direcciones por un tiempo fijo, un grupo puede atender durante una semana a más dispositivos que direcciones tiene, siempre que no estén todos presentes a la vez. El RFC 2131 dice que la asignación dinámica es especialmente útil para clientes conectados solo temporalmente y para compartir un grupo limitado entre clientes que no necesitan direcciones permanentes. Además, como un cliente puede simplemente desaparecer, el protocolo no depende de las despedidas: el RFC establece que su funcionamiento correcto no depende de que el cliente envíe un mensaje de liberación. Una dirección vuelve cuando vence su concesión, diga o no algo su titular.

Eso convierte la duración de la concesión en una decisión de diseño real, no en un valor predeterminado que deba dejarse tal cual. Una concesión larga mantiene ocupadas durante más tiempo las direcciones de dispositivos que ya se fueron. Una corta significa más tráfico de renovación y menos tiempo para reparar un servidor que ha dejado de responder, porque un cliente cuya concesión vence antes de poder contactar con un servidor debe dejar de utilizar su dirección.

DHCP también es una cuestión de confianza. La primera respuesta que acepta un dispositivo le indica qué router transporta todo su tráfico y qué servidor DNS traduce cada nombre que consulta, así que quien controla esa respuesta controla adónde va el dispositivo. El RFC 2131 es explícito: su sección de seguridad llama al protocolo, en su forma actual, «bastante inseguro», porque se construye directamente sobre UDP e IP y porque las máquinas para las que se diseñó son difíciles de equipar con contraseñas o claves. La misma sección señala que es fácil instalar servidores no autorizados y que pueden entregar direcciones incorrectas o duplicadas, routers suplantados y servidores de nombres suplantados. La protección tiene que venir de la red que rodea al protocolo, no del propio protocolo.

Cómo se aplica en la práctica

Piense en un portátil con dirección de hardware 00-00-5E-00-53-2A que se conecta a la subred de una oficina, 192.0.2.0/24, donde una máquina en 192.0.2.1 es a la vez router y servidor DHCP. El portátil empieza sin dirección, así que su primer mensaje sale con la dirección de origen 0.0.0.0 y se difunde a todos los participantes del enlace. Cuatro mensajes después, está configurado:

```
portátil 00-00-5E-00-53-2A                    servidor 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, puerto del servidor 67
                 ¿hay algún servidor aquí?
2  DHCPOFFER     ofrece 192.0.2.50 por 86400 s, ID del servidor 192.0.2.1
3  DHCPREQUEST   difusión: ID del servidor 192.0.2.1, solicita 192.0.2.50
4  DHCPACK       192.0.2.50 es del portátil durante 86400 s
```

Pueden responder al descubrimiento tantos servidores como haya, y el cliente puede esperar para reunir más de una oferta. Después elige una y difunde una petición que nombra al servidor elegido en la opción de identificador de servidor y solicita la dirección que ofreció. Todos los demás servidores que ven la difusión la interpretan como un rechazo de su propia oferta. El servidor elegido guarda la vinculación en su almacenamiento y la confirma con un acuse de recibo.

El acuse incluye los ajustes, cada uno como una opción numerada definida en el RFC 2132. Para este portátil podría contener:

```
opción 53  tipo de mensaje       5 (DHCPACK)
opción 54  identificador del servidor  192.0.2.1
opción 51  tiempo de concesión   86400 (segundos, un día)
opción 1   máscara de subred     255.255.255.0
opción 3   router                192.0.2.1
opción 6   servidores DNS        192.0.2.53
```

El RFC 2132 exige que la máscara de subred aparezca antes que la opción de router cuando están ambas y permite que un servidor enumere varios routers y varios servidores de nombres por orden de preferencia. El tiempo de concesión y el identificador del servidor no son opcionales: el RFC 2131 hace ambos obligatorios en un acuse de recibo de una petición.

Antes de utilizar 192.0.2.50, el cliente debería comprobar que nadie la está usando, por ejemplo mediante ARP. Si resulta que ya está ocupada, debe enviar DHCPDECLINE y empezar de nuevo. De lo contrario, arrancan los temporizadores. Salvo que el servidor envíe sus propios valores, T1 es la mitad de la concesión y T2 sus siete octavos, de modo que, con una concesión de un día:

```
t = 0 s        DHCPACK recibido, comienza la concesión
t = 43200 s    T1: RENEWING, DHCPREQUEST por unidifusión a 192.0.2.1
t = 75600 s    T2: REBINDING, DHCPREQUEST por difusión a cualquier servidor
t = 86400 s    vence la concesión: dejar de usar 192.0.2.50, empezar de nuevo
```

El RFC pide cierta variación aleatoria alrededor de ambos temporizadores para que una sala llena de portátiles encendidos a la vez no renueve de golpe. Si una petición no recibe respuesta, el cliente espera la mitad del tiempo restante antes de volver a intentarlo, hasta un mínimo de 60 segundos. Un cliente que funciona correctamente renueva a mitad del periodo y nunca se acerca al final de su concesión.

El servidor no tiene que estar en la subred del portátil. Un router puede actuar como agente de retransmisión: recoge la difusión y la pasa a un servidor situado en otro lugar, y su propia dirección, registrada en el campo giaddr del mensaje, indica al servidor dónde enviar la respuesta. El RFC 2131 cuenta con ello y señala que los agentes de retransmisión eliminan la necesidad de un servidor DHCP en

cada segmento de red. A la escala que describe la página de servicios de redes y VPN de la empresa, que enumera la configuración y el despliegue de 1.000 routers Wi-Fi y la administración de infraestructura de red para más de 1.000 servidores, introducir direcciones a mano no es una opción, y la distribución de grupos de direcciones, concesiones y retransmisores pasa a formar parte del diseño de red.

Dónde surgen los problemas

Un servidor no autorizado responde primero. Un router doméstico conectado del revés, una máquina de pruebas conectada mediante un puente a la red de la oficina o un atacante deliberado pueden responder a un DHCPDISCOVER, y nada en el protocolo indica al cliente qué servidor es el auténtico. El RFC 2131 enumera lo que puede hacer uno de esos servidores: entregar direcciones incorrectas o duplicadas y dirigir a los clientes a un router o servidores de nombres suplantados. Los switches pueden filtrar esos mensajes, y el RFC 7610 señala que la variante IPv4 del filtro, DHCP snooping, está ampliamente implantada. Permita mensajes de servidores DHCP solo en los puertos del switch que llevan a sus servidores o retransmisores auténticos y descártelos en los demás.

Se agotan las direcciones disponibles. Un grupo contiene un número fijo de direcciones y la asignación dinámica solo las recupera cuando terminan las concesiones. En una red de invitados por la que pasan teléfonos por centenares, una concesión de una semana significa que cada visitante de la última semana todavía retiene una dirección. El RFC 2131 también advierte de que un cliente malicioso puede acaparar todas las direcciones y no dejar ninguna para los demás. Dimensione el grupo según los dispositivos presentes durante un periodo de concesión y acorte la concesión donde los dispositivos entren y salgan.

Una subred nueva sin retransmisor. El descubrimiento es una difusión y las difusiones se detienen en el router. Una VLAN o planta de oficina nueva sin agente de retransmisión configurado no recibe respuesta alguna. Un host que implemente el RFC 3927 puede entonces darse una dirección local de enlace de 169.254/16, que solo funciona en ese enlace porque los routers no deben reenviar paquetes hacia esas direcciones ni desde ellas. Configure un agente de retransmisión en el router de cada subred que tenga clientes DHCP e interprete una dirección 169.254 en un cliente como una señal de que ningún servidor respondió.

Dos servidores que discrepan. Ejecutar dos servidores por resiliencia tiene sentido, pero el RFC 2131 dice que todos deberían devolver los mismos parámetros salvo la propia dirección, para que un cliente se comporte igual acepte la oferta que acepte, y hace responsable al administrador de mantenerlos coherentes. Dos servidores cuyos intervalos se solapan también pueden prestar la misma dirección a dos clientes. Dé a cada servidor su propio intervalo, mantenga idénticas las opciones y compare ambos después de cada cambio.

Direcciones fijas dentro del grupo. Una impresora con dirección estática introducida a mano dentro del intervalo que presta DHCP acabará, tarde o temprano, chocando con una concesión. El protocolo intenta detectarlo: un servidor debería sondear una dirección que está a punto de reutilizar, por ejemplo con una petición de eco ICMP, y un cliente que encuentra su dirección nueva ocupada debe rechazarla; después, el servidor marca la dirección como no disponible y debería avisar al administrador. Son redes de seguridad, no un diseño. Mantenga las direcciones configuradas a mano fuera del grupo o utilice asignación manual para que el propio servidor guarde la reserva.

IPv6 queda sin proteger. Filtrar DHCPv4 no hace nada por DHCPv6, que funciona en otros puertos y que un cliente puede iniciar cuando un anuncio de router indica que DHCPv6 está disponible. El RFC 9915 remite al RFC 7610, DHCPv6-Shield, para mitigar servidores DHCPv6 no autorizados, y el RFC 7610 establece que los anuncios de router no autorizados quedan fuera de su alcance: corresponden a Router Advertisement Guard. Filtre los mensajes de servidores DHCPv6 en los puertos de acceso igual que los de DHCPv4 y ejecute RA-Guard en paralelo.

Lecturas adicionales

- RFC 2131: protocolo de configuración dinámica de hosts — el propio protocolo: mecanismos de asignación, concesiones, intercambio de mensajes, temporizadores T1 y T2 y sección de seguridad.
- RFC 2132: opciones DHCP y extensiones de proveedor BOOTP — todas las opciones numeradas, desde la máscara de subred y la lista de routers hasta el tiempo de concesión y el tipo de mensaje.
- RFC 9915: protocolo de configuración dinámica de hosts para IPv6 (DHCPv6) — el protocolo IPv6, sus puertos y mensajes y su funcionamiento con SLAAC; deja obsoleto el RFC 8415.
- RFC 7610: DHCPv6-Shield, protección frente a servidores DHCPv6 no autorizados — filtrado de mensajes de servidor en el switch, el precedente IPv4 de DHCP snooping y lo que deja a RA-Guard.

- RFC 3927: configuración dinámica de direcciones IPv4 locales de enlace — las direcciones 169.254/16 que puede darse un host cuando ningún servidor responde y por qué los routers nunca las reenvían.

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 DHCP?» 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/dhcp/