Engineer

DHCP

ett protokoll som delar ut IP-adresser och nätinställningar

Vad det är

DHCP, Dynamic Host Configuration Protocol, är sättet som en enhet som just har anslutit till ett nätverk tar reda på var den hör hemma i nätverket. En bärbar dator som ansluter till ett Wi-Fi-nätverk känner till sin egen hårdvaruadress och inte mycket mer. DHCP ger den en IP-adress, nätmasken, den router som trafiken ska skickas genom och de DNS-servrar den ska fråga, utan att någon behöver skriva in något. Protokollet definieras i RFC 2131 från mars 1997, vars sammanfattning beskriver det som ett ramverk för att föra över konfigurationsinformation till värdar i ett TCP/IP-nätverk. Det växte fram ur det äldre Bootstrap Protocol, BOOTP, och det viktigaste det lade till var automatisk tilldelning av adresser som kan återanvändas.

RFC 2131 nämner tre sätt att dela ut en adress. Vid automatisk tilldelning får klienten en permanent adress. Vid dynamisk tilldelning får den en adress under en begränsad tid, eller tills den lämnar tillbaka den. Vid manuell tilldelning väljer nätverksadministratören adressen, och DHCP levererar den bara. Dynamisk tilldelning är den enda av de tre där en adress av sig själv går tillbaka till poolen när den som hade den inte längre behöver den, och det är den mekanismen resten av artikeln handlar om.

Ett sådant tidsbegränsat lån kallas i fackspråket en lease. Klienten kan förlänga den, lämna tillbaka adressen i förtid och till och med be om en oändlig lease. RFC:n påpekar att en server ändå kan föredra långa men ändliga leaser, så att den förr eller senare upptäcker en klient som har tagits ur drift. Bakom servern finns det som RFC:n kallar beständig lagring: en post per klient, med en identifierare som nyckel och de parametrar klienten har fått som värde.

DHCP går över UDP. Klienter skickar till serverns port 67, och servrar svarar på klientens port 68. De så kallade options, de inställningar en server kan skicka med, från nätmasken till leasetiden, specificeras för sig i RFC 2132. IPv6 har ett eget protokoll, DHCPv6, som nu specificeras i RFC 9915, en internetstandard från januari 2026 som ersatte RFC 8415. Det använder andra portar, 546 för klienter och 547 för servrar och reläagenter, och det kan köras antingen i stället för eller vid sidan av tillståndslös autokonfiguration av adresser (SLAAC). RFC 9915 kallar själv IPv4-protokollet DHCPv4 när de två behöver hållas isär, och det återger IETF:s konsensus om att IPv4-konfiguration ska skickas över DHCPv4 och inte över DHCPv6.

Använd begreppet i ett beslut

Använd ”Vad är DHCP?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Wi-Fi, brandväggar och fjärråtkomst uppsatta så att personalen kan arbeta varifrån som helst och bara rätt personer kommer in.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Förvaltade 30 VPS-instanser med Ubuntu Linux — 30 förvaltade Linux-servrar, med en plan för återställning

Förvaltade 30 VPS-instanser med Ubuntu Linux Hör av er →

Varför det spelar roll

Varje enhet i ett nätverk behöver samma fåtal inställningar, och ett enda felaktigt värde räcker för att skära av den: en mask som inte passar subnätet, en routeradress som tillhör någon annan, en DNS-server som stängdes av förra året. Utan DHCP måste vart och ett av de värdena skrivas in på varje enhet och hållas rätt varje gång något ändras. Med DHCP bor de på ett ställe, och att byta DNS-server för ett helt kontor blir en ändring i serverns konfiguration i stället för en runda i huset.

Leasen är det som gör att protokollet skalar. Eftersom dynamisk tilldelning lånar ut adresser under en bestämd tid kan en pool betjäna fler enheter under en vecka än den har adresser, så länge alla inte är närvarande samtidigt. RFC 2131 skriver att dynamisk tilldelning är särskilt användbar för klienter som bara är anslutna tillfälligt, och för att dela en begränsad pool mellan klienter som inte behöver fasta adresser. Och eftersom en klient helt enkelt kan försvinna räknar protokollet inte med något farväl: RFC:n slår fast att protokollet fungerar korrekt utan att klienten skickar något frigörelsemeddelande. En adress kommer tillbaka när leasen löper ut, oavsett om den som hade den någonsin säger till.

Det gör leasetiden till ett verkligt designbeslut och inte ett standardvärde man låter stå. En lång lease håller adresserna till enheter som för länge sedan har försvunnit låsta längre. En kort innebär mer förnyelsetrafik och mindre tid att laga en server som har slutat svara, eftersom en klient vars lease löper ut innan den når fram till en server måste sluta använda sin adress.

DHCP är också en fråga om förtroende. Det första svar en enhet accepterar talar om för den vilken router all dess trafik går genom och vilken DNS-server som översätter varje namn den slår upp, så den som styr det svaret styr vart enheten tar vägen. RFC 2131 sticker inte under stol med det: Avsnittet om säkerhet kallar protokollet i sin nuvarande form ganska osäkert, eftersom det är byggt direkt på UDP och IP, och eftersom maskinerna det skulle betjäna är svåra att förse med lösenord eller nycklar. Samma avsnitt påpekar att obehöriga servrar är lätta att sätta upp och kan dela ut felaktiga eller dubbla adresser och peka ut förfalskade routrar och förfalskade namnservrar. Skyddet måste komma från nätverket runt protokollet, inte från protokollet självt.

Så ser det ut i praktiken

Ta en bärbar dator med hårdvaruadressen 00-00-5E-00-53-2A som ansluter till ett kontorsnät, 192.0.2.0/24, där en maskin på 192.0.2.1 är både router och DHCP-server. Datorn börjar utan adress, så dess första meddelande skickas med avsändaradressen 0.0.0.0 som broadcast till alla på länken. Fyra meddelanden senare är den konfigurerad:

```
bärbar 00-00-5E-00-53-2A                        server 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, serverport 67
                 finns det en server här?
2  DHCPOFFER     erbjuder 192.0.2.50 i 86400 s, server-id 192.0.2.1
3  DHCPREQUEST   broadcast: server-id 192.0.2.1, önskar 192.0.2.50
4  DHCPACK       192.0.2.50 tillhör datorn i 86400 s
```

Hur många servrar som helst kan svara på en DHCPDISCOVER, och klienten kan vänta och samla in mer än ett erbjudande. Sedan väljer den ett och skickar en DHCPREQUEST som broadcast, som namnger den valda servern i optionen server identifier och ber om just den adress som den servern erbjöd. Alla andra servrar som ser broadcasten tolkar den som ett nej till sitt eget erbjudande. Den valda servern skriver ner bindningen i sin beständiga lagring och bekräftar med en DHCPACK.

Den bekräftelsen bär inställningarna, var och en en numrerad option som definieras i RFC 2132. För den här datorn kunde den innehålla:

```
option 53  meddelandetyp      5 (DHCPACK)
option 54  server-id          192.0.2.1
option 51  leasetid           86400 (sekunder, ett dygn)
option 1   nätmask            255.255.255.0
option 3   router             192.0.2.1
option 6   DNS-servrar        192.0.2.53
```

RFC 2132 kräver att nätmasken kommer före router-optionen när båda finns med, och låter en server ange flera routrar och flera namnservrar i prioritetsordning. Leasetiden och server-id:t är inte valfria: RFC 2131 gör båda obligatoriska i en DHCPACK som svarar på en DHCPREQUEST.

Innan datorn börjar använda 192.0.2.50 bör den kontrollera att ingen annan redan använder adressen, till exempel med ARP. Visar sig adressen vara upptagen måste klienten skicka DHCPDECLINE och börja om. Annars startar timrarna. Om servern inte skickar egna värden är T1 halva leasen och T2 sju åttondelar av den, så med en lease på ett dygn ser det ut så här:

```
t = 0 s        DHCPACK mottaget, leasen börjar
t = 43200 s    T1: RENEWING, unicast DHCPREQUEST till 192.0.2.1
t = 75600 s    T2: REBINDING, DHCPREQUEST som broadcast till alla servrar
t = 86400 s    leasen löper ut: sluta använda 192.0.2.50, börja om
```

RFC:n ber om en viss slumpmässig variation runt båda timrarna, så att bärbara datorer som slås på samtidigt i ett rum inte alla förnyar sina leaser på en gång. Får en förfrågan inget svar väntar klienten halva den återstående tiden innan den försöker igen, dock minst 60 sekunder. En frisk klient förnyar vid halvvägsmärket och kommer aldrig i närheten av slutet på sin lease.

Servern behöver inte stå på datorns subnät. En router kan fungera som reläagent: Den fångar upp broadcasten och skickar den vidare till en server någon annanstans, och dess egen adress, som står i meddelandets giaddr-fält, talar om för servern vart svaret ska skickas. Det räknar RFC 2131 med, och den påpekar att reläagenter tar bort behovet av en DHCP-server på varje nätverkssegment. Vår sida om nätverk och VPN-uppsättning nämner konfiguration och driftsättning av 1 000 Wi-Fi-routrar och administration av

nätverksinfrastrukturen för över 1 000 servrar. I den skalan går det inte att skriva in adresser för hand, och utformningen av pooler, leaser och reläer blir en del av nätverksdesignen.

Var det går fel

En främmande server svarar först. En hemmarouter som kopplats in åt fel håll, en testmaskin som bryggats in på kontorsnätet eller en avsiktlig angripare kan alla svara på en DHCPDISCOVER, och ingenting i protokollet talar om för en klient vilken server som är den riktiga. RFC 2131 räknar upp vad en sådan server kan göra: dela ut felaktiga eller dubbla adresser och skicka klienter till en förfalskad router eller förfalskade namnservrar. Switchar kan filtrera bort det, och RFC 7610 påpekar att en motsvarande mekanism för IPv4, DHCP snooping, är vida spridd. Tillåt DHCP-servermeddelanden bara på de switchportar som leder till era riktiga servrar eller reläagenter, och släng dem överallt annars.

Poolen tar slut. En pool rymmer ett fast antal adresser, och dynamisk tilldelning får bara tillbaka dem när leaser löper ut. På ett gästnät där telefoner passerar i hundratal betyder en lease på en vecka att varje besökare från den senaste veckan fortfarande har en adress. RFC 2131 varnar också för att en illasinnad klient kan lägga beslag på alla adresser och inte lämna några till andra klienter. Dimensionera poolen efter antalet enheter som är närvarande inom en leaseperiod, och korta leasen överallt där enheter kommer och går.

Ett nytt subnät utan relä. En DHCPDISCOVER skickas som broadcast, och broadcasts stannar vid routern. Ett nytt VLAN eller en ny kontorsvåning utan konfigurerad reläagent får inget svar alls. En värddator som implementerar RFC 3927 kan då ge sig själv en länklokal adress från 169.254/16, som bara fungerar på den ena länken, eftersom routrar inte får vidarebefordra paket till eller från sådana adresser. Konfigurera en reläagent på routern i varje subnät med DHCP-klienter, och läs en 169.254-adress på en klient som ett tecken på att ingen server svarade.

Två servrar som inte är överens. Att köra två servrar för redundansens skull är klokt, men RFC 2131 säger att alla servrar bör returnera samma parametrar, bortsett från själva adressen, så att klienten beter sig förutsägbart oavsett vilket erbjudande den tar emot, och gör nätverksadministratören ansvarig för att de svarar likadant. Två servrar med överlappande adressintervall kan dessutom låna ut samma adress till två klienter. Ge varje server ett eget intervall, håll inställningarna identiska och jämför de två efter varje ändring.

Fasta adresser inne i poolen. En skrivare som har fått en statisk adress för hand, från det intervall DHCP lånar ut ur, kommer förr eller senare att krocka med en lease. Protokollet försöker fånga det: En server bör testa en adress den är på väg att återanvända, till exempel med en ICMP echo request, och en klient som upptäcker att dess nya adress är upptagen måste avböja den, varpå servern markerar adressen som otillgänglig och bör meddela administratören. Det är skyddsnät, inte en design. Håll handkonfigurerade adresser utanför poolen, eller använd manuell tilldelning så att servern själv håller reservationen.

IPv6 glöms bort. Att filtrera DHCPv4 gör ingenting åt DHCPv6, som går på andra portar och som en klient kan starta när en Router Advertisement meddelar att DHCPv6 finns tillgängligt. RFC 9915 hänvisar till RFC 7610, DHCPv6-Shield, för att hålla obehöriga DHCPv6-servrar stången, och RFC 7610 slår fast att falska Router Advertisements ligger utanför dess område; dem tar Router Advertisement Guard hand om. Filtrera DHCPv6-servermeddelanden på accessportarna på samma sätt som ni filtrerar DHCPv4-meddelandena, och kör RA-Guard vid sidan av.

Läs mer

- RFC 2131: Dynamic Host Configuration Protocol — själva protokollet: tilldelningssätten, leaser, meddelandeutbytet, timrarna T1 och T2 och avsnittet om säkerhet.
- RFC 2132: DHCP Options and BOOTP Vendor Extensions — alla numrerade options, från nätmasken och routerlistan till leasetiden och meddelandetypen.
- RFC 9915: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) — IPv6-protokollet, dess portar och meddelanden och hur det samspelar med SLAAC; det ersätter RFC 8415.
- RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers — filtrering av servermeddelanden på switchen, DHCP snooping som förebild från IPv4, och vad den lämnar åt RA-Guard.
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — 169.254/16-adresserna som en värddator kan ge sig själv när ingen server svarar, och varför routrar aldrig vidarebefordrar dem.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är DHCP?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/dhcp/