Engineer

DHCP

en protokol, der tildeler IP-adresser og netværksopsætning

Hvad det er

DHCP, Dynamic Host Configuration Protocol, er den måde, en enhed, der lige er kommet på et netværk, finder ud af, hvor den hører hjemme på netværket. En bærbar, der kobler sig på et Wi-Fi-netværk, kender sin egen hardwareadresse og ikke meget andet. DHCP giver den en IP-adresse, subnetmasken, den router, trafikken skal sendes igennem, og de DNS-servere, den skal spørge, uden at nogen skal taste noget ind. Protokollen er defineret i RFC 2131 fra marts 1997, hvis resumé beskriver den som en ramme for at overføre konfigurationsoplysninger til værter på et TCP/IP-netværk. Den voksede ud af den ældre Bootstrap Protocol, BOOTP, og det vigtigste, den føjede til, var automatisk tildeling af adresser, der kan genbruges.

RFC 2131 nævner tre måder at dele en adresse ud på. Ved automatisk tildeling får klienten en permanent adresse. Ved dynamisk tildeling får den en adresse i en begrænset periode, eller indtil den giver den tilbage. Ved manuel tildeling vælger netværksadministratoren adressen, og DHCP leverer den blot. Dynamisk tildeling er den eneste af de tre, hvor en adresse af sig selv vender tilbage til puljen, når den, der havde den, ikke længere har brug for den, og det er den mekanisme, resten af artiklen handler om.

Sådan et tidsbegrænset udlån kaldes på fagsprog en lease. Klienten kan forlænge den, aflevere adressen før tid og endda bede om en uendelig lease. RFC'en bemærker, at en server alligevel kan foretrække lange, men endelige leases, så den før eller siden opdager en klient, der er taget ud af drift. Bag serveren ligger det, RFC'en kalder vedvarende lagring: én post pr. klient med en identifikator som nøgle og de parametre, klienten har fået, som værdi.

DHCP kører over UDP. Klienter sender til serverens port 67, og servere svarer på klientens port 68. De såkaldte options, de indstillinger en server kan sende med, fra subnetmasken til leasetiden, er specificeret for sig i RFC 2132. IPv6 har sin egen protokol, DHCPv6, som nu er specificeret i RFC 9915, en internetstandard fra januar 2026, der afløste RFC 8415. Den bruger andre porte, 546 til klienter og 547 til servere og relæagenter, og den kan køre enten i stedet for eller ved siden af tilstandsløs autokonfiguration af adresser (SLAAC). RFC 9915 kalder selv IPv4-protokollen DHCPv4, når der skal skelnes mellem de to, og den gengiver IETF's konsensus om, at IPv4-konfiguration skal sendes over DHCPv4 og ikke over DHCPv6.

Brug begrebet i en beslutning

Brug »Hvad er DHCP?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Wi-Fi, firewalls og fjernadgang sat op, så medarbejdere kan arbejde hvor som helst, og kun de rette kommer ind.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har administreret 30 Ubuntu Linux VPS-instanser — 30 Linux-servere driftet, med en plan for gendannelse

Har administreret 30 Ubuntu Linux VPS-instanser Kontakt os →

Hvorfor det betyder noget

Hver enhed på et netværk har brug for de samme få indstillinger, og én forkert værdi er nok til at afskære den: en maske, der ikke passer til subnettet, en routeradresse, der tilhører en anden, en DNS-server, der blev slukket sidste år. Uden DHCP skal hver af de værdier tastes ind på hver enhed og holdes korrekt, hver gang noget ændrer sig. Med DHCP bor de ét sted, og at skifte DNS-server for et helt kontor bliver en ændring i serverens konfiguration i stedet for en tur rundt i bygningen.

Leasen er det, der får protokollen til at skalere. Fordi dynamisk tildeling udlåner adresser for en bestemt tid, kan en pulje betjene flere enheder i løbet af en uge, end den har adresser, så længe de ikke alle er til stede på samme tid. RFC 2131 skriver, at dynamisk tildeling er særlig nyttig til klienter, der kun er tilsluttet midlertidigt, og til at dele en begrænset pulje mellem klienter, der ikke har brug for faste adresser. Og fordi en klient bare kan forsvinde, regner protokollen ikke med et farvel: RFC'en slår fast, at protokollen fungerer korrekt, uden at klienten sender en frigivelsesbesked. En adresse kommer tilbage, når leasen udløber, uanset om den, der havde den, nogensinde siger det.

Det gør leasetiden til et reelt designvalg og ikke en standardværdi, man lader stå. En lang lease holder adresserne fra enheder, der for længst er gået, låst i længere tid. En kort betyder mere fornyelsestrafik og mindre tid til at reparere en server, der er holdt op med at svare, for en klient, hvis lease udløber, før den når frem til en server, skal holde op med at bruge sin adresse.

DHCP er også et spørgsmål om tillid. Det første svar, en enhed accepterer, fortæller den, hvilken router al dens trafik går igennem, og hvilken DNS-server der oversætter hvert eneste navn, den slår op, så den, der styrer det svar, styrer, hvor enheden ender. RFC 2131 lægger ikke skjul på det: Afsnittet om sikkerhed kalder protokollen i sin nuværende form for ganske usikker, fordi den er bygget direkte på UDP og IP, og fordi de maskiner, den skulle betjene, er svære at udstyre med adgangskoder eller nøgler. Samme afsnit bemærker, at uautoriserede servere er nemme at sætte op og kan dele forkerte eller dobbelte adresser ud og pege på forfalskede routere og forfalskede navneservere. Beskyttelsen må komme fra netværket omkring protokollen, ikke fra protokollen selv.

Sådan ser det ud i praksis

Tag en bærbar med hardwareadressen 00-00-5E-00-53-2A, der kobler sig på et kontornet, 192.0.2.0/24, hvor én maskine på 192.0.2.1 er både router og DHCP-server. Den bærbare starter uden adresse, så dens første besked sendes med afsenderadressen 0.0.0.0 som broadcast til alle på linket. Fire beskeder senere er den konfigureret:

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

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, serverport 67
                 er der en server her?
2  DHCPOFFER     tilbyder 192.0.2.50 i 86400 s, server-id 192.0.2.1
3  DHCPREQUEST   broadcast: server-id 192.0.2.1, ønsker 192.0.2.50
4  DHCPACK       192.0.2.50 er den bærbares i 86400 s
```

Et vilkårligt antal servere kan svare på en DHCPDISCOVER, og klienten kan vente og samle mere end ét tilbud. Så vælger den ét og sender en DHCPREQUEST som broadcast, der nævner den valgte server i optionen server identifier og beder om den adresse, netop den server tilbød. Alle andre servere, der ser broadcasten, opfatter den som et afslag på deres eget tilbud. Den valgte server skriver bindingen ned i sin vedvarende lagring og bekræfter med en DHCPACK.

Den bekræftelse bærer indstillingerne, hver især en nummereret option defineret i RFC 2132. For den bærbare kunne den indeholde:

```
option 53  beskedtype         5 (DHCPACK)
option 54  server-id          192.0.2.1
option 51  leasetid           86400 (sekunder, et døgn)
option 1   subnetmaske        255.255.255.0
option 3   router             192.0.2.1
option 6   DNS-servere        192.0.2.53
```

RFC 2132 kræver, at subnetmasken kommer før router-optionen, når begge er med, og lader en server angive flere routere og flere navneservere i prioriteret rækkefølge. Leasetiden og server-id'et er ikke valgfrie: RFC 2131 gør begge obligatoriske i en DHCPACK, der svarer på en DHCPREQUEST.

Før den bærbare tager 192.0.2.50 i brug, bør den tjekke, at ingen andre allerede bruger adressen, for eksempel med ARP. Viser adressen sig at være optaget, skal klienten sende DHCPDECLINE og begynde forfra. Ellers starter timerne. Medmindre serveren sender sine egne værdier, er T1 halvdelen af leasen og T2 syv ottendedele af den, så med en lease på et døgn ser det sådan ud:

```
t = 0 s        DHCPACK modtaget, leasen begynder
t = 43200 s    T1: RENEWING, unicast DHCPREQUEST til 192.0.2.1
t = 75600 s    T2: REBINDING, DHCPREQUEST som broadcast til alle servere
t = 86400 s    leasen udløber: stop med at bruge 192.0.2.50, start forfra
```

RFC'en beder om en vis tilfældig variation omkring begge timere, så de bærbare, der tændes på samme tid i et lokale, ikke alle fornyer deres leases på én gang. Får en forespørgsel intet svar, venter klienten halvdelen af den resterende tid, før den prøver igen, dog mindst 60 sekunder. En sund klient fornyer ved halvvejsmærket og kommer aldrig i nærheden af slutningen af sin lease.

Serveren behøver ikke at stå på den bærbares subnet. En router kan fungere som relæagent: Den opfanger broadcasten og sender den videre til en server et andet sted, og dens egen adresse, der står i beskedens giaddr-felt, fortæller serveren, hvor svaret skal sendes hen. Det regner RFC 2131 med og bemærker, at relæagenter fjerner behovet for en DHCP-server på hvert netværkssegment. Vores side om netværk og VPN-opsætning nævner konfiguration og idriftsættelse af 1.000 Wi-Fi-routere og administration af netværksinfrastruktur

for over 1.000 servere. I den skala er det ikke en mulighed at taste adresser ind i hånden, og indretningen af puljer, leases og relæer bliver en del af netværksdesignet.

Hvor det går galt

En fremmed server svarer først. En hjemmerouter, der er sat forkert i, en testmaskine, der er brokoblet ind på kontornettet, eller en bevidst angriber kan alle svare på en DHCPDISCOVER, og intet i protokollen fortæller en klient, hvilken server der er den rigtige. RFC 2131 opregner, hvad sådan en server kan gøre: dele forkerte eller dobbelte adresser ud og sende klienter videre til en forfalsket router eller forfalskede navneservere. Switche kan filtrere det fra, og RFC 7610 bemærker, at en lignende mekanisme til IPv4, DHCP snooping, er vidt udbredt. Tillad kun DHCP-serverbeskeder på de switchporte, der fører til jeres rigtige servere eller relæagenter, og smid dem væk alle andre steder.

Puljen løber tør. En pulje rummer et fast antal adresser, og dynamisk tildeling får dem kun tilbage, når leases udløber. På et gæstenet, hvor telefoner kommer forbi i hundredvis, betyder en lease på en uge, at alle gæster fra den seneste uge stadig har en adresse. RFC 2131 advarer også om, at en ondsindet klient kan lægge beslag på samtlige adresser og ikke efterlade nogen til andre. Dimensionér puljen efter antallet af enheder, der er til stede inden for én leaseperiode, og forkort leasen overalt, hvor enheder kommer og går.

Et nyt subnet uden relæ. En DHCPDISCOVER sendes som broadcast, og broadcasts stopper ved routeren. Et nyt VLAN eller en ny kontoretage uden en konfigureret relæagent får slet intet svar. En vært, der implementerer RFC 3927, kan så give sig selv en link-lokal adresse fra 169.254/16, som kun virker på det ene link, fordi routere ikke må videresende pakker til eller fra sådanne adresser. Konfigurér en relæagent på routeren i hvert subnet med DHCP-klienter, og læs en 169.254-adresse på en klient som et tegn på, at ingen server svarede.

To servere, der er uenige. At køre to servere for robusthedens skyld er fornuftigt, men RFC 2131 siger, at alle servere bør returnere de samme parametre, bortset fra selve adressen, så klientens adfærd er forudsigelig, uanset hvilket tilbud den tager imod, og gør netværksadministratoren ansvarlig for, at de svarer ens. To servere med overlappende adresseområder kan desuden låne den samme adresse ud til to klienter. Giv hver server sit eget område, hold indstillingerne identiske, og sammenlign de to efter hver ændring.

Faste adresser inde i puljen. En printer, der har fået en statisk adresse i hånden fra det område, DHCP låner ud af, vil før eller siden støde sammen med en lease. Protokollen prøver at fange det: En server bør afprøve en adresse, den er ved at genbruge, for eksempel med en ICMP echo request, og en klient, der opdager, at dens nye adresse er optaget, skal afvise den, hvorefter serveren markerer adressen som utilgængelig og bør give administratoren besked. Det er sikkerhedsnet, ikke et design. Hold håndkonfigurerede adresser uden for puljen, eller brug manuel tildeling, så serveren selv holder reservationen.

IPv6 bliver overset. At filtrere DHCPv4 gør intet ved DHCPv6, som kører på andre porte, og som en klient kan starte, når en Router Advertisement melder, at DHCPv6 er tilgængelig. RFC 9915 henviser til RFC 7610, DHCPv6-Shield, for at dæmme op for uautoriserede DHCPv6-servere, og RFC 7610 slår fast, at falske Router Advertisements ligger uden for dens område; dem tager Router Advertisement Guard sig af. Filtrér DHCPv6-serverbeskeder på adgangsportene, ligesom I filtrerer DHCPv4-beskederne, og kør RA-Guard ved siden af.

Læs mere

- RFC 2131: Dynamic Host Configuration Protocol — selve protokollen: tildelingsmåderne, leases, beskedudvekslingen, timerne T1 og T2 og afsnittet om sikkerhed.
- RFC 2132: DHCP Options and BOOTP Vendor Extensions — alle de nummererede options, fra subnetmasken og routerlisten til leasetiden og beskedtypen.
- RFC 9915: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) — IPv6-protokollen, dens porte og beskeder, og hvordan den spiller sammen med SLAAC; den afløser RFC 8415.
- RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers — filtrering af serverbeskeder på switchen, DHCP snooping som forbillede fra IPv4, og hvad den overlader til RA-Guard.
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — de 169.254/16-adresser, en vært kan give sig selv, når ingen server svarer, og hvorfor routere aldrig videresender dem.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er DHCP?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/dhcp/