Engineer

DHCP

ein Protokoll, das IP-Adressen und Netzparameter verleiht

Was es ist

DHCP, das Dynamic Host Configuration Protocol, versorgt ein Gerät, das gerade einem Netzwerk beigetreten ist, mit den nötigen Einstellungen für dieses Netzwerk. Ein Laptop, der sich mit einem WLAN verbindet, kennt seine eigene Hardwareadresse und kaum mehr. DHCP gibt ihm eine IP-Adresse, die Subnetzmaske, den Router für seinen Datenverkehr und die abzufragenden DNS-Server, ohne dass jemand diese Angaben eintippen muss. Das Protokoll ist in RFC 2131 vom März 1997 definiert. Dessen Zusammenfassung stellt es als Verfahren vor, um Hosts eines TCP/IP-Netzwerks Konfigurationsinformationen zu übermitteln. Es entstand aus dem älteren Bootstrap Protocol, BOOTP. Seine wichtigste Ergänzung war die automatische Vergabe wiederverwendbarer Adressen.

RFC 2131 nennt drei Arten der Adressvergabe. Bei automatischer Vergabe erhält der Client eine dauerhafte Adresse. Bei dynamischer Vergabe bekommt er sie für eine begrenzte Zeit oder bis er sie zurückgibt. Bei manueller Vergabe wählt der Netzwerkadministrator die Adresse, und DHCP übermittelt sie lediglich. Nur die dynamische Vergabe lässt eine Adresse von selbst in den Pool zurückkehren, wenn ihr Inhaber sie nicht mehr benötigt. Um diesen Mechanismus geht es im Rest dieses Artikels.

Die Zeitspanne, für die eine Adresse ausgeliehen wird, heißt Lease. Der Client kann sie verlängern, die Adresse vorzeitig zurückgeben und sogar eine unbegrenzte Lease anfordern. Der RFC merkt an, dass ein Server trotzdem lange, aber endliche Leases bevorzugen kann, damit er irgendwann einen ausgemusterten Client bemerkt. Hinter dem Server liegt, was der RFC als dauerhafte Speicherung bezeichnet: ein Eintrag pro Client, über eine Kennung zugeordnet, mit den Parametern, die dieser Client erhalten hat.

DHCP läuft über UDP. Clients senden an Serverport 67, und Server antworten auf Clientport 68. Die Optionen, die ein Server senden kann, von der Subnetzmaske bis zur Lease-Dauer, sind getrennt in RFC 2132 festgelegt. IPv6 hat mit DHCPv6 ein eigenes Protokoll. Es ist inzwischen in RFC 9915 spezifiziert, einem Internetstandard vom Januar 2026, der RFC 8415 ersetzte. Es verwendet andere Ports: 546 für Clients sowie 547 für Server und Relay-Agenten. Es kann die zustandslose Adressautokonfiguration (SLAAC) ersetzen oder parallel dazu laufen. RFC 9915 selbst nennt das IPv4-Protokoll DHCPv4, wenn er die beiden unterscheiden muss, und hält den IETF-Konsens fest, dass IPv4-Konfiguration über DHCPv4 statt DHCPv6 übertragen werden sollte.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist DHCP?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. WLAN, Firewalls und Fernzugriff werden so eingerichtet, dass Mitarbeitende von überall arbeiten können und nur Berechtigte Zugang erhalten.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 30 Ubuntu-Linux-VPS-Instanzen verwaltet — 30 verwaltete Linux-Server mit geplantem Wiederherstellungsweg

30 Ubuntu-Linux-VPS-Instanzen verwaltet Kontakt aufnehmen →

Warum es wichtig ist

Jedes Gerät eines Netzwerks braucht dieselben wenigen Einstellungen. Ein falscher Wert genügt, um es abzuschneiden: eine nicht zum Subnetz passende Maske, eine fremde Routeradresse, ein im Vorjahr abgeschalteter DNS-Server. Ohne DHCP muss jeder Wert in jedes Gerät eingetragen und bei jeder Änderung aktuell gehalten werden. Mit DHCP liegen die Werte an einer Stelle. Der Wechsel des DNS-Servers für ein ganzes Büro wird damit zu einer Änderung der Serverkonfiguration statt zu einem Rundgang durch das Gebäude.

Die Lease macht das Protokoll skalierbar. Weil die dynamische Vergabe Adressen für eine feste Zeit ausleiht, kann ein Pool im Laufe einer Woche mehr Geräte bedienen, als er Adressen hat, solange nicht alle gleichzeitig anwesend sind. Laut RFC 2131 ist die dynamische Vergabe besonders für nur vorübergehend verbundene Clients und zum Teilen eines begrenzten Pools unter Clients ohne Bedarf an dauerhaften Adressen nützlich. Und weil ein Client einfach verschwinden kann, verlässt sich das Protokoll nicht auf einen Abschied: Der RFC

stellt fest, dass der korrekte Betrieb nicht vom Senden einer Freigabenachricht durch den Client abhängt. Eine Adresse kehrt beim Ablauf ihrer Lease zurück, ob ihr Inhaber sich abmeldet oder nicht.

Damit ist die Lease-Dauer eine echte Entwurfsentscheidung und kein Standardwert, den man einfach unverändert lässt. Eine lange Lease hält die Adressen nicht mehr verbundener Geräte länger gebunden. Eine kurze verursacht mehr Verlängerungsverkehr und lässt weniger Zeit, einen nicht mehr antwortenden Server zu reparieren. Denn ein Client, dessen Lease abläuft, bevor er einen Server erreicht, muss die Nutzung seiner Adresse einstellen.

DHCP ist auch eine Vertrauensfrage. Die erste von einem Gerät angenommene Antwort sagt ihm, welcher Router seinen gesamten Verkehr weiterleitet und welcher DNS-Server jeden nachgeschlagenen Namen übersetzt. Wer diese Antwort kontrolliert, kontrolliert damit, wohin das Gerät geht. RFC 2131 ist hier deutlich: Sein Sicherheitsabschnitt nennt das Protokoll in der dort beschriebenen Form „ziemlich unsicher“, weil es unmittelbar auf UDP und IP aufbaut und weil sich die vorgesehenen Rechner schwer mit Passwörtern oder Schlüsseln ausstatten lassen. Derselbe Abschnitt merkt an, dass sich nicht autorisierte Server leicht einrichten lassen und falsche oder doppelte Adressen vergeben und Clients auf gefälschte Router und Nameserver verweisen können. Der Schutz muss aus dem Netzwerk um das Protokoll kommen, nicht aus dem Protokoll selbst.

Wie es in der Praxis aussieht

Ein Laptop mit der Hardwareadresse 00-00-5E-00-53-2A tritt einem Bürosubnetz 192.0.2.0/24 bei. Dort ist ein Rechner unter 192.0.2.1 zugleich Router und DHCP-Server. Der Laptop hat anfangs keine Adresse. Seine erste Nachricht geht deshalb mit der Quelladresse 0.0.0.0 als Broadcast an alle Teilnehmer des Links. Vier Nachrichten später ist er konfiguriert:

```
Laptop 00-00-5E-00-53-2A                      Server 192.0.2.1

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, Serverport 67
                 Gibt es hier einen Server?
2  DHCPOFFER     bietet 192.0.2.50 für 86400 s, Server-ID 192.0.2.1
3  DHCPREQUEST   Broadcast: Server-ID 192.0.2.1, angefragt: 192.0.2.50
4  DHCPACK       192.0.2.50 gehört dem Laptop für 86400 s
```

Beliebig viele Server können die Discover-Nachricht beantworten, und der Client kann auf mehrere Angebote warten. Dann wählt er eines und sendet eine Broadcast-Anfrage. Sie benennt den gewählten Server in der Server-Identifier-Option und fordert dessen angebotene Adresse an. Jeder andere Server, der den Broadcast sieht, versteht ihn als Ablehnung seines eigenen Angebots. Der gewählte Server hält die Zuordnung dauerhaft fest und sendet eine Bestätigung.

Die Bestätigung enthält die Einstellungen, jeweils als nummerierte Option aus RFC 2132. Für diesen Laptop könnte sie Folgendes enthalten:

```
Option 53  Nachrichtentyp        5 (DHCPACK)
Option 54  Serverkennung         192.0.2.1
Option 51  Lease-Dauer           86400 (Sekunden, ein Tag)
Option 1   Subnetzmaske          255.255.255.0
Option 3   Router               192.0.2.1
Option 6   DNS-Server            192.0.2.53
```

RFC 2132 verlangt die Subnetzmaske vor der Routeroption, wenn beide vorhanden sind. Er erlaubt einem Server, mehrere Router und mehrere Nameserver in der Reihenfolge ihrer Präferenz aufzulisten. Lease-Dauer und Serverkennung sind nicht optional: RFC 2131 schreibt beide in der Bestätigung einer Anfrage vor.

Bevor der Client 192.0.2.50 nutzt, sollte er prüfen, ob die Adresse bereits verwendet wird, etwa mit ARP. Ist sie belegt, muss er DHCPDECLINE senden und neu beginnen. Andernfalls starten die Timer. Sendet der Server keine eigenen Werte, liegt T1 bei der Hälfte und T2 bei sieben Achteln der Lease. Bei einer Lease von einem Tag gilt also:

```
t = 0 s        DHCPACK empfangen, Lease beginnt
t = 43200 s    T1: RENEWING, Unicast-DHCPREQUEST an 192.0.2.1
t = 75600 s    T2: REBINDING, Broadcast-DHCPREQUEST an beliebige Server
t = 86400 s    Lease läuft ab: 192.0.2.50 nicht mehr nutzen, neu beginnen
```

Der RFC empfiehlt, die beiden Timerwerte leicht zufällig zu variieren, damit nicht alle Laptops eines Raums, die zusammen eingeschaltet wurden, gleichzeitig verlängern. Bleibt eine Anfrage unbeantwortet, wartet der Client vor dem

nächsten Versuch die Hälfte der verbleibenden Zeit, mindestens jedoch 60 Sekunden. Ein normal funktionierender Client verlängert zur Halbzeit und kommt dem Ende seiner Lease nie nahe.

Der Server muss nicht im Subnetz des Laptops stehen. Ein Router kann als Relay-Agent fungieren: Er nimmt den Broadcast entgegen und leitet ihn an einen Server anderswo weiter. Seine eigene Adresse im giaddr-Feld der Nachricht sagt dem Server, wohin die Antwort soll. RFC 2131 setzt darauf und merkt an, dass Relay-Agenten einen DHCP-Server in jedem Netzwerksegment überflüssig machen. Die Seite zu unseren Netzwerk- und VPN-Leistungen nennt die Konfiguration und Bereitstellung von 1.000 WLAN-Routern und die Verwaltung der Netzwerkinfrastruktur für mehr als 1.000 Server. In dieser Größenordnung kommt das manuelle Eintragen von Adressen nicht infrage. Die Anordnung von Pools, Leases und Relays wird zum Bestandteil des Netzwerkentwurfs.

Wo es schiefgeht

Ein nicht autorisierter Server antwortet zuerst. Ein falsch angeschlossener Heimrouter, ein Testrechner mit einer Bridge ins Büronetz oder ein gezielt vorgehender Angreifer können alle einen DHCPDISCOVER beantworten. Nichts im Protokoll sagt dem Client, welcher Server der richtige ist. RFC 2131 zählt auf, was ein solcher Server tun kann: falsche oder doppelte Adressen vergeben und Clients auf einen gefälschten Router oder gefälschte Nameserver verweisen. Switches können dagegen filtern. RFC 7610 merkt an, dass die IPv4-Form dieses Filters, DHCP-Snooping, weit verbreitet ist. Erlauben Sie DHCP-Servernachrichten nur auf den Switchports, die zu Ihren echten Servern oder Relays führen, und verwerfen Sie sie überall sonst.

Der Pool ist leer. Ein Pool enthält eine feste Zahl von Adressen, und die dynamische Vergabe bekommt sie erst beim Ablauf der Leases zurück. In einem Gastnetz, in dem Hunderte Mobiltelefone kommen und gehen, bedeutet eine Lease von einer Woche, dass jeder Besucher der letzten sieben Tage noch eine Adresse hält. RFC 2131 warnt zudem, dass ein böswilliger Client alle Adressen für sich beanspruchen und für andere keine übrig lassen kann. Bemessen Sie den Pool nach der Zahl der innerhalb einer Lease-Dauer anwesenden Geräte und verkürzen Sie die Lease überall, wo Geräte kommen und gehen.

Ein neues Subnetz ohne Relay. Die Discover-Nachricht ist ein Broadcast, und Broadcasts enden am Router. Ein neues VLAN oder eine Büroetage ohne konfigurierten Relay-Agenten erhält überhaupt keine Antwort. Ein Host, der RFC

3927 implementiert, kann sich dann eine linklokale Adresse aus 169.254/16 geben. Sie funktioniert nur auf diesem einen Link, weil Router Pakete von oder zu solchen Adressen nicht weiterleiten dürfen. Konfigurieren Sie auf dem Router jedes Subnetzes mit DHCP-Clients einen Relay-Agenten. Verstehen Sie eine 169.254-Adresse auf einem Client als Zeichen, dass kein Server geantwortet hat.

Zwei uneinige Server. Zwei Server für Ausfallsicherheit zu betreiben ist sinnvoll. Doch RFC 2131 sagt, alle Server sollten abgesehen von der Adresse selbst dieselben Parameter liefern, damit sich ein Client unabhängig vom gewählten Angebot gleich verhält. Er macht den Administrator für ihre Konsistenz verantwortlich. Zwei Server mit überlappenden Bereichen können außerdem dieselbe Adresse an zwei Clients verleihen. Geben Sie jedem Server einen eigenen Bereich, halten Sie die Optionen identisch und vergleichen Sie beide nach jeder Änderung.

Feste Adressen innerhalb des Pools. Ein Drucker mit einer manuell festgelegten statischen Adresse aus dem DHCP-Vergabebereich kollidiert früher oder später mit einer Lease. Das Protokoll versucht dies abzufangen: Ein Server sollte eine wiederzuverwendende Adresse prüfen, etwa mit einer ICMP-Echo-Anfrage. Ein Client, der seine neue Adresse belegt vorfindet, muss sie ablehnen. Daraufhin kennzeichnet der Server die Adresse als nicht verfügbar und sollte den Administrator informieren. Das sind Sicherheitsnetze, kein Ersatz für die Planung. Halten Sie manuell konfigurierte Adressen außerhalb des Pools oder nutzen Sie manuelle Vergabe, damit der Server selbst die Reservierung verwaltet.

IPv6 bleibt offen. DHCPv4 zu filtern hilft nicht gegen DHCPv6. Es läuft auf anderen Ports und kann von einem Client gestartet werden, wenn ein Router Advertisement DHCPv6 als verfügbar meldet. RFC 9915 verweist für die Abwehr nicht autorisierter DHCPv6-Server auf RFC 7610, DHCPv6-Shield. RFC 7610 stellt klar, dass nicht autorisierte Router Advertisements außerhalb seines Geltungsbereichs liegen; dafür ist Router Advertisement Guard zuständig. Filtern Sie DHCPv6-Servernachrichten auf Zugangsports wie diejenigen von DHCPv4 und betreiben Sie parallel RA-Guard.

Weiterführende Lektüre

- RFC 2131: Dynamic Host Configuration Protocol — das Protokoll selbst: Vergabemechanismen, Leases, Nachrichtenaustausch, T1- und T2-Timer sowie der Sicherheitsabschnitt.

- RFC 2132: DHCP Options and BOOTP Vendor Extensions — jede nummerierte Option, von der Subnetzmaske und Routerliste bis zu Lease-Dauer und Nachrichtentyp.
- RFC 9915: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) — das IPv6-Protokoll, seine Ports und Nachrichten sowie sein Zusammenspiel mit SLAAC; es ersetzt RFC 8415.
- RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers — das Filtern von Servernachrichten auf dem Switch, DHCP-Snooping als IPv4-Vorbild und die Aufgaben, die es RA-Guard überlässt.
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — die 169.254/16-Adressen, die ein Host sich ohne Serverantwort geben kann, und warum Router sie nie weiterleiten.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist DHCP?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/dhcp/