Engineer

DHCP

a protocol that leases IP addresses and settings to devices

What it is

DHCP, the Dynamic Host Configuration Protocol, is how a device that has just joined a network finds out where it stands on that network. A laptop that connects to a Wi-Fi network knows its own hardware address and little else. DHCP gives it an IP address, the subnet mask, the router to send traffic through and the DNS servers to ask, without anybody typing them in. The protocol is defined in RFC 2131, published in March 1997, whose abstract presents it as a way to hand configuration information to the hosts of a TCP/IP network. It grew out of the older Bootstrap Protocol, BOOTP, and its main addition was the automatic allocation of addresses that can be reused.

RFC 2131 names three ways to hand out an address. In automatic allocation the client gets a permanent address. In dynamic allocation it gets one for a limited period, or until it gives the address back. In manual allocation the network administrator chooses the address and DHCP merely delivers it. Of the three, only dynamic allocation lets an address go back to the pool on its own once its holder no longer needs it, and it is the mechanism the rest of this article is about.

The period for which an address is lent is called a lease. The client can extend it, can hand the address back early, and can even ask for an infinite lease; the RFC notes that a server may still prefer long but finite leases, so that it eventually notices a client that has been retired. Behind the server sits what the RFC calls persistent storage: one entry per client, keyed by an identifier, holding the parameters that client was given.

DHCP runs over UDP. Clients send to server port 67 and servers answer on client port 68. The options a server can send, from the subnet mask to the lease time, are specified separately, in RFC 2132. IPv6 has a protocol of its own, DHCPv6, now specified in RFC 9915, an Internet Standard from January 2026 that

replaced RFC 8415. It uses other ports, 546 for clients and 547 for servers and relay agents, and it can run either in place of or alongside stateless address autoconfiguration (SLAAC). RFC 9915 itself calls the IPv4 protocol DHCPv4 when it needs to tell the two apart, and it records the IETF consensus that IPv4 configuration should travel over DHCPv4 rather than DHCPv6.

Use the concept in a decision

Put “What is DHCP?” to work in a real decision. We can help relate the concept to the system you are building or buying. Wi-Fi, firewalls and remote access set up so staff can work from anywhere and only the right people get in.

Explore our services Get in touch →

Test the assumptions behind the term

Use the explanation and linked work to frame questions for your project. We can examine the assumptions with you before a tool is chosen. Managed 30 Ubuntu Linux VPS instances — 30 Linux servers managed, with recovery planned for

Managed 30 Ubuntu Linux VPS instances Get in touch →

Why it matters

Every device on a network needs the same handful of settings, and one wrong value is enough to cut it off: a mask that does not match the subnet, a router address that belongs to someone else, a DNS server that was switched off last year. Without DHCP each of those values has to be typed into each device and kept right whenever anything changes. With DHCP they live in one place, and changing the DNS server for a whole office becomes a change to the server’s configuration rather than a walk round the building.

The lease is what makes the protocol scale. Because dynamic allocation lends addresses for a fixed time, a pool can serve more devices over a week than it has addresses, as long as they are not all present at once. RFC 2131 says dynamic allocation is particularly useful for clients that are connected only temporarily, and for sharing a limited pool among clients that do not need permanent addresses. And because a client may simply vanish, the protocol does not rely on goodbyes: the RFC states that correct operation does not depend on the client sending a release message. An address comes back when its lease runs out, whether or not its holder ever says so.

That makes the lease length a real design decision, not a default to leave alone. A long lease keeps the addresses of departed devices locked up for longer. A short one means more renewal traffic, and less time to fix a server that has stopped answering, because a client whose lease expires before it reaches a server must stop using its address.

DHCP is also a question of trust. The first answer a device accepts tells it which router carries all its traffic and which DNS server translates every name it looks up, so whoever controls that answer controls where the device goes. RFC 2131 is plain about this: its security section calls the protocol, in its current form, “quite insecure”, because it is built directly on UDP and IP, and because the machines it was meant to serve are hard to equip with passwords or keys. The same section notes that unauthorised servers are easy to set up and can hand out wrong or duplicate addresses, spoofed routers and spoofed name servers. The protection has to come from the network around the protocol, not from the protocol.

What it looks like in practice

Take a laptop with the hardware address 00-00-5E-00-53-2A joining an office subnet, 192.0.2.0/24, where one machine at 192.0.2.1 is both the router and the DHCP server. The laptop starts out without an address, so its first message leaves with the source address 0.0.0.0 and is broadcast to everyone on the link. Four messages later it is configured:

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

1  DHCPDISCOVER  0.0.0.0 -> 255.255.255.255, server port 67
                 is there a server here?
2  DHCPOFFER     offers 192.0.2.50 for 86400 s, server id 192.0.2.1
3  DHCPREQUEST   broadcast: server id 192.0.2.1, requested 192.0.2.50
4  DHCPACK       192.0.2.50 is the laptop's for 86400 s
```

Any number of servers may answer the discover, and the client may wait to collect more than one offer. It then chooses one and broadcasts a request that names the chosen server in the server identifier option and asks for the address that server offered. Every other server that sees the broadcast takes it as a refusal of its own offer. The chosen server commits the binding to its storage and confirms with an acknowledgement.

The acknowledgement carries the settings, each one a numbered option defined in RFC 2132. For this laptop it could contain:

```
option 53  message type       5 (DHCPACK)
option 54  server identifier  192.0.2.1
option 51  lease time         86400 (seconds, one day)
```

```
option 1   subnet mask        255.255.255.0
option 3   router             192.0.2.1
option 6   DNS servers        192.0.2.53
```

RFC 2132 requires the subnet mask to come before the router option when both are present, and lets a server list several routers and several name servers, in order of preference. The lease time and the server identifier are not optional: RFC 2131 makes both mandatory in an acknowledgement to a request.

Before using 192.0.2.50, the client should check that nobody else is already using it, for example with ARP. If the address turns out to be taken, the client must send DHCPDECLINE and start again. Otherwise the timers start. Unless the server sends values of its own, T1 is half the lease and T2 is seven eighths of it, so with a lease of one day:

```
t = 0 s        DHCPACK received, lease starts
t = 43200 s    T1: RENEWING, unicast DHCPREQUEST to 192.0.2.1
t = 75600 s    T2: REBINDING, broadcast DHCPREQUEST to any server
t = 86400 s    lease expires: stop using 192.0.2.50, start over
```

The RFC asks for some random variation around both timers, so that a room full of laptops switched on together does not renew all at once. If a request gets no answer, the client waits half of the remaining time before it tries again, down to a minimum of 60 seconds. A healthy client renews at the halfway mark and never comes near the end of its lease.

The server does not have to sit on the laptop’s subnet. A router can act as a relay agent: it picks up the broadcast and passes it to a server elsewhere, and its own address, recorded in the message’s giaddr field, tells the server where to send the answer. RFC 2131 counts on this, noting that relay agents remove the need for a DHCP server on every network segment. At the scale our networking and VPN services page describes, which lists configuring and deploying 1,000 Wi-Fi routers and administering network infrastructure for more than 1,000 servers, typing addresses in by hand is not an option, and the layout of pools, leases and relays becomes part of the network design.

Where it goes wrong

A rogue server answers first. A home router plugged in the wrong way round, a test machine bridged onto the office network or a deliberate attacker can all answer a DHCPDISCOVER, and nothing in the protocol tells a client which server is the real one. RFC 2131 lists what such a server can do: hand out wrong or duplicate addresses, and point clients at a spoofed router or spoofed name servers. Switches can filter for this, and RFC 7610 notes that the IPv4 form of the filter, DHCP snooping, is widely deployed. Allow DHCP server messages only on the switch ports that lead to your real servers or relays, and drop them everywhere else.

The pool runs dry. A pool holds a fixed number of addresses, and dynamic allocation only gets them back when leases end. On a guest network where phones pass through by the hundred, a lease of a week means that every visitor of the past week still holds an address. RFC 2131 also warns that a malicious client can claim every address for itself and leave none for anyone else. Size the pool for the number of devices present within one lease period, and shorten the lease wherever devices come and go.

A new subnet without a relay. The discover is a broadcast, and broadcasts stop at the router. A new VLAN or office floor with no relay agent configured gets no answer at all. A host that implements RFC 3927 may then give itself a link-local address from 169.254/16, which only works on that one link, because routers must not forward packets to or from such addresses. Configure a relay agent on the router of every subnet that has DHCP clients, and read a 169.254 address on a client as a sign that no server answered.

Two servers that disagree. Running two servers for resilience is sensible, but RFC 2131 says all servers should return the same parameters, apart from the address itself, so that a client behaves the same whichever offer it takes, and it makes the administrator responsible for keeping them consistent. Two servers whose ranges overlap can also lend the same address to two clients. Give each server its own range, keep the options identical, and compare the two after every change.

Fixed addresses inside the pool. A printer given a static address by hand, from inside the range that DHCP lends out, will sooner or later collide with a lease. The protocol tries to catch this: a server should probe an address it is about to reuse, for example with an ICMP echo request, and a client that finds its new address

taken must decline it, after which the server marks the address as unavailable and should tell the administrator. Those are safety nets, not a design. Keep hand-configured addresses outside the pool, or use manual allocation, so that the server itself holds the reservation.

IPv6 left open. Filtering DHCPv4 does nothing for DHCPv6, which runs on other ports and which a client may start when a router advertisement says DHCPv6 is available. RFC 9915 points to RFC 7610, DHCPv6-Shield, for mitigating rogue DHCPv6 servers, and RFC 7610 states that rogue router advertisements are outside its scope; they are the job of Router Advertisement Guard. Filter DHCPv6 server messages on access ports as you filter DHCPv4 ones, and run RA-Guard alongside.

Further reading

- RFC 2131: Dynamic Host Configuration Protocol — the protocol itself: allocation mechanisms, leases, the message exchange, the T1 and T2 timers and the security section.
- RFC 2132: DHCP Options and BOOTP Vendor Extensions — every numbered option, from the subnet mask and the router list to the lease time and the message type.
- RFC 9915: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) — the IPv6 protocol, its ports and messages, and how it works with SLAAC; it obsoletes RFC 8415.
- RFC 7610: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers — filtering server messages on the switch, the IPv4 precedent of DHCP snooping, and what it leaves to RA-Guard.
- RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses — the 169.254/16 addresses a host may give itself when no server answers, and why routers never forward them.

Glossary

Choose for your actual constraints

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Make the terminology practical

Ask how “What is DHCP?” applies to your organisation. A concrete example from your current system is enough to start the discussion.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

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

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://engineer.company/glossary/dhcp/