Dynamic Host Configuration Protocol (DHCP)

Autor: Moser Tobias

Datum: 06.04.2015

Typ: Information

Version: 1.0

Inhaltsverzeichnis

INHALT

1 Dynamic Host Configuration Protocol

Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

DHCP (Dynamic Host Configuration Protocol)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Automatischer Bezug von IP-Adressen und weiteren Parametern
Ports:	67/UDP (Server oder Relay-Agent) 68/UDP (Client)
DHCP im TCP/IP-Protokollstapel:	
Anwendung	**DHCP**
Transport	UDP
Internet	IP (IPv4, IPv6)
Netzzugang	Ethernet, Token Bus, Token Ring, FDDI, ...
Standards:	RFC 2131 (1997)

DHCP wurde im RFC 2131 definiert und bekam von der Internet Assigned Numbers Authority die UDP-Ports 67 und 68 zugewiesen.

1.1 Konzept

DHCP ermöglicht es, Computer ohne manuelle Konfiguration der Netzwerkschnittstelle in ein bestehendes Netzwerk einzubinden. Wo ohne DHCP Einstellungen wie IP-Adresse, Netzmaske, Gateway und Name Server (DNS) (je nach Netzwerktyp ggf. noch weitere Einstellungen) manuell vorgenommen werden müssten, verteilt DHCP diese Einstellungen automatisch an die am Netzwerk angeschlossenen Computer.
Dazu muss der jeweilige Computer allerdings in der Lage sein, als DHCP-Client konfiguriert zu werden. Moderne Betriebssysteme ermöglichen dies in aller Regel.
DHCP ist eine Erweiterung des Bootstrap-Protokolls (BOOTP), das für Arbeitsplatz-Computer ohne eigene Festplatte (Diskless-Workstation) notwendig war, wo sich der Computer beim Startvorgang zunächst vom BOOTP-Server eine IP-Adresse zuweisen ließ, um danach das Betriebssystem aus dem Netzwerk zu laden, das für den weiteren Betrieb des Computers notwendig ist. DHCP ist weitgehend kompatibel zu BOOTP und kann entsprechend mit BOOTP-Clients und -Servern (eingeschränkt) zusammenarbeiten.

DHCP hat zwei entscheidende Vorteile: Bei häufigen Änderungen müssen die Administratoren nicht jeden Computer einzeln an die neuen Gegebenheiten anpassen und Fehler, wie sie bei der manuellen Vergabe der IP-Adressen auftreten (z.B. doppelte Vergabe derselben IP-Adresse), können vermieden werden. Insbesondere Computer mit häufig wechselndem Standort (z.B. Notebooks) profitieren von DHCP: Sie werden einfach ans Netzwerk angeschlossen und holen sich alle relevanten Einstellungen über DHCP. Daher bezeichnet man DHCP auch gelegentlich als *Plug and Play für Netzwerke*.

1.2 Der DHCP-Server

Der DHCP-Server wird – wie alle Netzwerkdienste – als Hintergrundprozess (Dienst oder Daemon) gestartet und wartet auf UDP-Port 67 auf Client-Anfragen. In seiner Konfigurationsdatei befinden sich Informationen über den zu vergebenden Adresspool sowie zusätzliche Angaben über netzwerkrelevante Parameter wie die Subnetzmaske, die lokale DNS-Domain oder das zu verwendende Gateway. Außerdem lassen sich auch weitere BOOTP-Server oder der Ort des zu verwendenden Bootimages einstellen.
Es gibt drei verschiedene Betriebsmodi eines DHCP-Servers: manuelle, automatische und dynamische Zuordnung.

1.2.1 Manuelle Zuordnung

In diesem Modus (*statisches DHCP*) werden am DHCP-Server die IP-Adressen bestimmten MAC-Adressen fest zugeordnet. Die Adressen werden der MAC-Adresse auf unbestimmte Zeit zugeteilt. Der Nachteil kann darin liegen, dass sich keine zusätzlichen Clients in das Netz einbinden können, da die Adressen fest vergeben sind. Das kann unter Sicherheitsaspekten erwünscht sein.

Manuelle Zuordnungen werden vor allem dann vorgenommen, wenn der DHCP-Client beispielsweise Server-Dienste zur Verfügung stellt und daher unter einer festen IP-Adresse erreichbar sein soll. Auch Port-Weiterleitungen von einem Router an einen Client benötigen in der Regel eine feste IP-Adresse.

1.2.2 Automatische Zuordnung

Bei der automatischen Zuordnung wird am DHCP-Server ein Bereich von IP-Adressen (*range*) definiert. IP-Adressen werden automatisch an die MAC-Adressen von neuen DHCP-Clients zugewiesen, was in einer Tabelle festgehalten wird. Im Unterschied zur dynamischen Zuordnung sind automatische Zuordnungen permanent und werden nicht entfernt. Der Vorteil ist, dass Hosts immer dieselbe IP-Adresse erhalten und eine zugewiesene IP-Adresse keinem anderen Host zugewiesen wird. Der Nachteil ist, dass neue Clients keine IP-Adresse erhalten, wenn der gesamte Adressbereich vergeben ist, auch wenn IP-Adressen nicht mehr aktiv genutzt werden. Gegenüber der manuellen und dynamischen Zuordnung spielt dieser Modus in der Praxis eine untergeordnete Rolle.

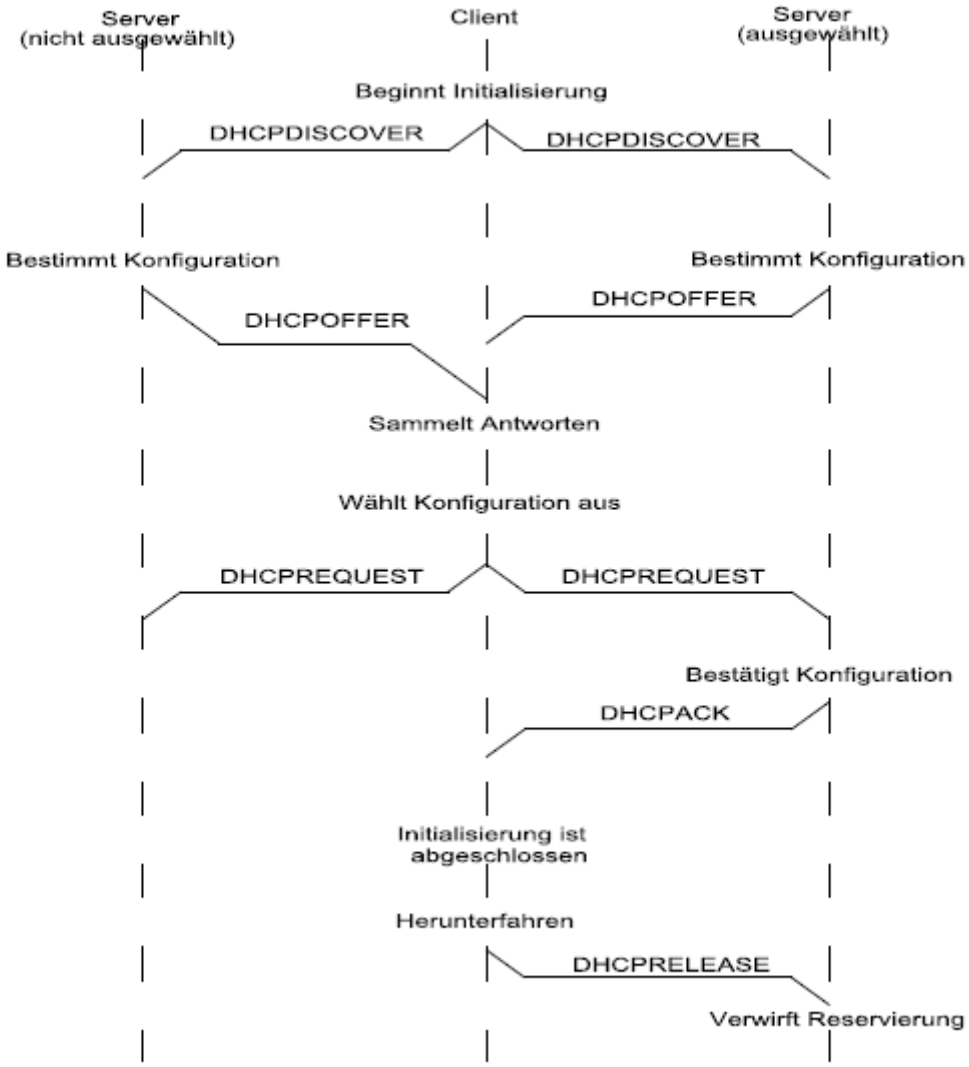
1.2.3 Dynamische Zuordnung

Dieses Verfahren gleicht der automatischen Zuordnung, allerdings hat der DHCP-Server hier in seiner Konfigurationsdatei eine Angabe, wie lange eine bestimmte IP-Adresse an einen Client „verliehen“ werden darf, bevor der Client sich erneut beim Server melden und eine „Verlängerung“ beantragen muss. Meldet er sich nicht, wird die Adresse frei und kann an einen anderen (oder auch denselben) Rechner neu vergeben werden. Diese vom Administrator bestimmte Zeit heisst Lease-Time (zu deutsch also: „Leihdauer“).
Manche DHCP-Server vergeben auch von der MAC-Adresse abhängige IP-Adressen, d. h. ein Client bekommt hier selbst nach längerer Netzwerkabstinenz und Ablauf der Lease-Zeit die gleiche IP-Adresse wie zuvor (es sei denn natürlich, diese ist inzwischen schon anderweitig vergeben).

1.3 DHCP-Nachrichten

DHCPDISCOVER: Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an alle DHCP-Server im lokalen Netz.
DHCPOFFER: Die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
DHCPREQUEST: Der Client fordert eine der angebotenen IP-Adressen, weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
DHCPACK: Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung.
DHCPNAK: Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server.
DHCPDECLINE: Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
DHCPRELEASE: Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
DHCPINFORM: Anfrage eines Clients nach Daten ohne IP-Adresse, z.B. weil der Client eine statische IP-Adresse besitzt.

Ablauf der DHCP-Kommunikation



Ablauf der Zuweisung einer IP-Adresse per DHCP

Damit der Client einen DHCP-Server nutzen kann, muss sich dieser im selben Netzwerksegment befinden, da DHCP Broadcasts verwendet und Router keine Broadcasts weiterleiten (Router bilden Broadcast-Domänen). Befindet sich der DHCP-Server in einem anderen Netzwerksegment, so muss ein so genannter DHCP-Relay-Agent installiert werden, der die DHCP-Anfragen an den eigentlichen Server weitergibt.

1.3.1 Initiale Adresszuweisung (Lease/Vergabe)

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine *DHCPDISCOVER*-Nachricht (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server (es kann durchaus mehrere davon im selben Subnetz geben). Dieser Broadcast hat als Absender-IP-Adresse 0.0.0.0 und als Zieladresse 255.255.255.255, da der Absender noch keine IP-Adresse besitzt und seine Anfrage „an alle“ richtet. Dabei ist der UDP-Quellport 68 und der UDP-Zielport 67. Die DHCP-Server antworten mit *DHCPOFFER* und machen Vorschläge für eine IP-Adresse. Das geschieht ebenfalls mit einem Broadcast an die Adresse 255.255.255.255 mit UDP-Quellport 67 und UDP-Zielport 68.

Der Client darf nun unter den eingetroffenen Angeboten (DHCP-Offers) wählen. Wenn er sich für eines entschieden hat (z. B. wegen längster Lease-Zeit oder wegen Ablehnung eines speziellen, evtl. falsch konfigurierten DHCP-Servers, oder einfach für die erste Antwort), kontaktiert er per Broadcast und einem im Paket enthaltenen Serveridentifier den entsprechenden Server mit der Nachricht *DHCPREQUEST*. Alle eventuellen weiteren DHCP-Server werten das als Absage für ihre Angebote. Der vom Client ausgewählte Server bestätigt in einer *DHCPACK*-Nachricht (DHCP-Acknowledged) die IP-Adresse mit den weiteren relevanten Daten, oder er zieht sein Angebot zurück (DHCPNAK, siehe auch sonstiges).

Bevor der Client sein Netzwerkinterface mit der zugewiesenen Adresse konfiguriert, sollte er noch prüfen, ob nicht versehentlich noch ein anderer Rechner die Adresse verwendet. Das geschieht üblicherweise durch einen ARP-Request mit der soeben zugeteilten IP-Adresse. Antwortet ein anderer Host im Netz auf diesen Request, so wird der Client die vorgeschlagene Adresse mit einer *DHCPDECLINE*-Nachricht zurückweisen.

1.3.2 DHCP-Refresh (nur bei dynamischer Zuordnung)

Zusammen mit der IP-Adresse erhält der Client in der *DHCPACK*-Nachricht die Lease-Zeit. Das ist ein Zeitwert, der angibt, wie lange der Client die zugewiesene IP-Konfiguration verwenden darf; er wird vom Administrator des DHCP-Servers eingestellt. Der Standard sieht vor, dass der Client nach der Hälfte der Lease-Zeit einen erneuten *DHCPREQUEST* sendet und so bekundet, dass weiteres Interesse an der reservierten IP-Adresse besteht. Dieser *DHCPREQUEST* wird per Unicast an den Server gesendet, der die IP-Konfiguration vergeben hat. Der Server sollte dann in der Regel ein *DHCPACK* mit identischen Daten wie vorher, aber einer neuen Lease-Zeit senden. Damit gilt die Adresse als verlängert.
Antwortet der Server nicht, so kann der Client die IP-Konfiguration ohne Einschränkungen weiter verwenden, bis die Lease abgelaufen ist. Er wird jedoch nach Ablauf von 7/8 der Lease-Zeit (87,5 %) versuchen, eine Verlängerung der IP-Konfiguration von irgendeinem DHCP-Server zu erhalten (Sendung der Anfrage im Broadcast). Ein möglicher Grund dafür ist, dass der ursprüngliche Server abgeschaltet wurde und nun ein neuer Server für die Verwaltung der IP-Adressen zuständig ist.
Sollte der Client es versäumen, bis zum Ablauf der Lease-Zeit eine Verlängerung zu beantragen, muss er seine Netzwerkkarte dekonfigurieren und wieder bei *DHCPDISCOVER* mit einer initialen Adresszuweisung beginnen. Sollte der DHCP-Server keine Adressen mehr zur Verfügung haben oder während des Vorganges schon ein anderer Client seine letzte Adresse zugesagt bekommen haben, sendet der Server ein DHCPNAK (DHCP-Not Acknowledged), und der Vorgang der Adressanfrage beginnt erneut.

1.4 Sonstiges

Eine negative Bestätigung *DHCPNAK* kann als Ursache haben, dass der Client versucht, seine ehemalige IP-Adresse zu leasen (engl. lease: mieten oder pachten), die jedoch inzwischen nicht mehr verfügbar ist, oder wenn der Client-Computer in ein anderes Subnetz verschoben wurde.
Um die Ausfallwahrscheinlichkeit zu verringern, ist es auch möglich, mehrere DHCP-Server in einem Netz zu platzieren. Dabei sollte allerdings beachtet werden, dass sich die Adressbereiche der einzelnen Server nicht überlappen, da es sonst zu Doppelvergaben von IP-Adressen kommen kann. Dazu gibt es die „authoritative“ (engl. für „maßgebliche“) Einstellung, mit der man einstellen kann, ob ein *DHCPNAK* auch verschickt werden soll, wenn der DHCP-Server für die vom Client vorgeschlagene Adresse nicht zuständig ist.

Wenn der Client eine negative Bestätigung erhält, wird der DHCP-Lease-Vorgang erneut gestartet.
Ein Client sendet *DHCPRELEASE*, wenn er eine IP-Adresse vor Ablauf der Lease-Zeit zurückgeben will.
Sollte der Client feststellen, dass die zugewiesene Adresse bereits benutzt wird, so teilt er das dem Server durch *DHCPDECLINE* mit, der seinerseits den Administrator von dieser potentiellen Fehlkonfiguration unterrichten sollte.

1.5 DHCP und DNS

Damit ihre Namensauflösung möglich ist, registrieren Computer ihren Namen und ihre IP-Adresse in der Regel bei einem DNS-Server. Einige DHCP-Server können das an Stelle der Clients übernehmen. Bei Betriebssystemen von Microsoft war das vor Windows 2000 erforderlich.

2 DHCP für mehrere Subnetze

Der DHCP-Server kann (Teil-)Netze bedienen, wenn er über Definitionen für das jeweilige Netz verfügt. Die Auswahl der Definition wird dann durch die Netzwerkkarte bestimmt, über welche die Anforderung hereinkommt. Beim Start des DHCP-Servers kann angegeben werden, auf welchen Interfaces der Server hört.
Andererseits kann ein DHCP-Server auch entfernte Netze bedienen, wenn diese durch einen DHCP-Relay-Agenten (vielfach als Funktion eines Routers verfügbar) verbunden sind. Der Relay-Agent empfängt im entfernten Netz die DHCP-Broadcast-Anforderungen und leitet diese als Unicast-Botschaften an den/die konfigurierten DHCP-Server weiter. Die IP-Adresse der Schnittstelle, über welche der Broadcast empfangen wurde, wird vom Relay-Agenten dem Unicast-Paket im DHCP-Header hinzugefügt, so dass der DHCP-Server anhand dieser Information bestimmen kann, aus welchem Netzwerksegment die Anfrage kommt. Der DHCP-Relay-Agent empfängt die Antwortpakete der DHCP-Server auf Port UDP 67 und leitet diese dann mit Zielport UDP 68 an den Client weiter.

3 Sicherheit

DHCP kann leicht gestört und manipuliert werden, weil DHCP-Clients jeden DHCP-Server akzeptieren.
Die versehentliche Aktivierung eines DHCP-Servers, beispielsweise durch den Anschluss eines einfachen DSL-Routers oder WLAN-Routers im Auslieferungszustand, kann ein Netz weitgehend lahmlegen. Dieser antwortet möglicherweise schneller als der eigentlich vorgesehene DHCP-Server und verteilt dadurch ggf. ungültige Konfigurationen.

Ein Angreifer kann alle Adressen eines DHCP-Servers reservieren (DHCP Starvation Attack), dadurch dessen Antwort auf weitere Anfragen verhindern und anschließend als einziger DHCP-Server auftreten. Er hat nun die Möglichkeit ein rogue DHCP Spoofing zu betreiben, indem er auf andere DNS-Server umleitet, die auf Computer verweisen, die die Kommunikation kompromittieren.

Die vermeintliche Eindeutigkeit der MAC-Adresse darf nicht als Sicherheitskriterium angewandt werden. Es ist viel zu einfach, MAC-Adressen-Spoofing zu betreiben. Fast alle Betriebssysteme erlauben es gewöhnlichen Benutzern, die MAC-Adresse komfortabel in Konfigurationsmasken oder mit einfachen Tools wie ifconfig (UNIX, Linux) oder ip link (Linux) zu überschreiben. Gültige MAC-Adressen in einem Schicht-2-Netz können durch Abhören des Netzverkehrs ausfindig gemacht werden. Dazu ist lediglich der physische Zugang zum Netzwerk nötig. Die exklusive Vergabe von IP-Adressen nur an registrierte MAC-Adressen über RARP oder DHCP schließt also nicht aus, dass Unberechtigte Zugriff auf das Netzwerk erhalten; dafür ist der Einsatz eines sicheren Authentifizierungsmechanismus wie IEEE 802.1X notwendig.