# DHCP-Geschichte

Im Jahre 1993 wurde in RFC 1531 eine Erweiterung des BOOTP definiert. Der sogenannte DHCP, das von Clients verwendet wird, um eine IP-Adresse vom Konfigurationsserver zu erhalten. Die Hintergründe für die Erweiterung des BOOTP waren, dass man bei BOOTP manuell eingreifen muss, um die IP-Adressen zu verteilen. Für die IPv6 Adressen erweitert man das Protokoll zu DHCPv6 und dokumentierte dies im RFC 3315. DHCPv6 ist ganz anders als DHCPv4. Unter DHCPv6 ist die Client Identifikator DUID, bei DHCPv4 MAC-Adressen. Auch noch anders ist, dass man bei DHCPv4 ausgeht, dass jeder Laptop genau eine Adresse besitzt, bei DHCPv6 kann das Endgerät mehrere besitzen.

# DHCP-Funktion

DHCP gestattet den Clients, ohne manuelle Konfiguration der Netzschnittstelle in ein bestehendes Netz einzubinden. Die IP-Adressen, Netzmaske, Standard-Gateway und DNS werden automatisch an den jeweiligen Client vergeben. Die Voraussetzung für das automatische Zuordnen ist, dass der Client das Betriebssystem unterstützt.

# Ein Bild, das Tisch enthält. Automatisch generierte BeschreibungAufbau eines DHCP-Paketes

* **op:** Ist, ob man eine Anfrage oder eine Antwort handelt
* **htype:** Netz typ (z.B. 1 Ethernet, 6=IEEE 802 Netzwerk)
* **hlen:** Länge einer Netzadresse in Bytes
* **hops:** Anzahl der DHCP-Relay -Agents auf dem Datenpfad
* **xid:** ID von der Verbindung Server/Client
* **secs:** Zeit nach dem Start des Clients in sec
* **flags**: ob Client noch gültige IP-Adresse hat
* **ciaddr**: Client-IP-Adresse
* **yiaddr**: eigene IP-Adresse
* **siaddr**: Server IP-Adresse
* **giaddr**: Relay-Agent IP-Adresse
* **chaddr**: Client MAC-Adresse
* **sname**: Name des DHCP-Servers (optional)
* **file**: Name einer Datei zB. System Kernel (optional)
* **options**: DHCP-Parameter und Options (RFC21329)

# DHCP-Zuordnungen

Es gibt drei verschiedene DHCP-Zuordnungsmodelle, die da wären, statisch, automatisch und dynamisch Zuordnung.

## Statische Zuordnung

In diesem Modell werden die IP-Adressen bestimmten MAC-Adressen zugeordnet. Diese Adressen werden der MAC-Adresse auf unbestimmter Zeit zugeteilt. Nachteil dieser Methode ist, dass keine zusätzlichen Clients in das Netz mit eingebunden werden, da die Adressen fest vergeben sind. Diese Zuordnung wird nur dann vorgenommen, wenn der Client Server Dienste ausführen möchte und unter dieser festen IP-Adresse erreichbar sein soll.

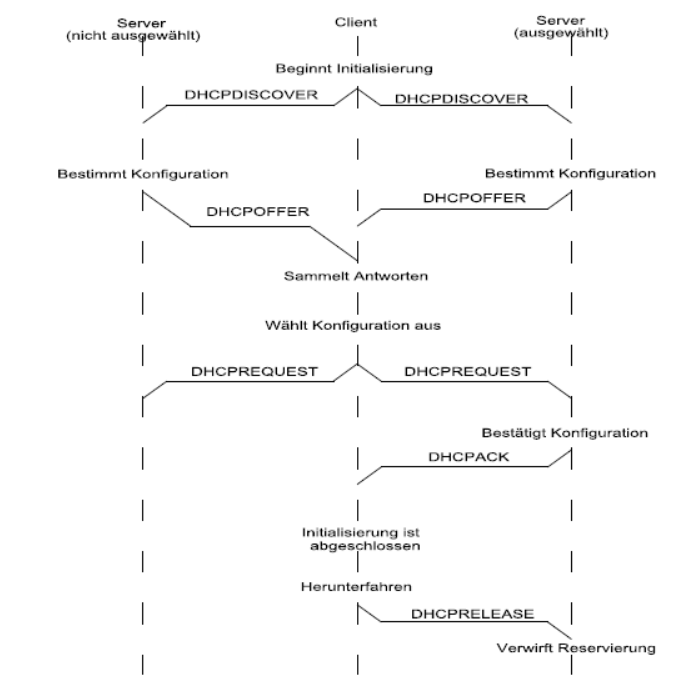
## Automatische Zuordnung:

Dort werden IP-Adressen gewissen Bereichen (range) vergeben. Die IP-Adressen werden an die MAC-Adresse von neuen Clients zugewiesen. Diese Zuweisung wird in einer Tabelle festgeschrieben. Diese Zuordnungen sind permanent und werden nicht gelöscht. Vorteil kann sein, dass Hosts immer derselben IP-Adresse zugewiesen werden, die zugewiesene IP-Adresse keinen anderen Host. Nachteil wäre zum Beispiel neue Clients, die sich verbinden möchten, keine IP-Adressen mehr bekommen, wenn der Adressbereich belegt ist, obwohl alte IP-Adressen nicht mehr aktiv benutzt werden.

## Dynamische Zuordnung

Die Dynamische Zuordnung ist fast dieselbe wie die automatische. Sie unterscheidet sich nur in einem Punkt. Und zwar wie lang eine IP-Adresse an einem Client vergeben werden soll. Wenn diese Abläuft muss der Client sich beim DHCP melden, um eine Verlängerung zu bekommen. Wenn sich der Client nicht meldet, wird diese Adresse wieder frei und ein anderer Client kann sich verbinden. Diese Leihdauer wird in der Netzwerktechnik als Lease-Time bezeichnet.

# Ablauf DHCP-Kommunikation

* DHCP**Discover:** Client schickt Broadcast Anfrage um IP-Adressenzuweisung
* DHCP**OFFER:** der DHCP-Server antwortet mit entsprechenden Werten auf das **Discover**
* ****DHCP**REQUEST**: Der Client fordert eine der angebotenen IP-Adressen, weiters verlängert er auch die Lease-Time vom antwortenden Server
* DHCP**ACK:** Bestätigung durch Server und Übermittlung Konfigurationsparameter die durch Client angefragt worden sind (DHCP**INFORM**)
* DHCP**NAK**: Ablehnung der **REQUEST** des Servers
* DHCP**DECLINE**: Ablehnung durch Client da IP schon verwendet wird
* DHCP**RELASE**: Der Client gibt Konfiguration frei, dass es für andere Clients bereitsteht
* DHCP**INFORM**: Anfrage vom Client für weiter Konfigurationsparameter, weil Client eine Statische IP besitzt.

# Sicherheit

DHCP kann leicht gehackt werden, weil Clients jeden DHCP-Server akzeptieren. Man kann einen DHCP-Server sehr leicht aktivieren, beispielsweise durch einen WLAN-Router im Auslieferungszustand. Der antwortet möglicherweise schneller als der DHCP-Server und verteilt dadurch ungültige Konfigurationen. Ein Hacker kann eine DHCP Starvation Attack durchführen. Das bedeutet er lässt alle Adressen am Server reservieren, dadurch die Antworten auf weitere Anfragen verhindert und anschließend er selbst als DHCP-Server auftretet. Er kann nun eine sogenannte rogue DHCP Spoofing betreiben, das bedeutet er leitet auf andere DNS-Server um, die auf Endgeräte verweisen, die dann die Kommunikation manipulieren. Ein Angreifer könnte auch ein Denial-of-Service-Angriffe starten. Er müsste nur jedem einzelnen Client ein Subnetz zuweisen, kein Gateway oder auf allen Anfragen die gleiche IP-Adresse verwenden. Er kann auch den Man-in-the-Middle-Angriff durchführen dazu muss der Angreifer falsche Gateway und DNS-Adressen vergeben und ein fremder Router einzuschleusen, der den Datenverkehr mitschneidet. Diese Probleme kann man umgehen mit dem sogenannten Peg DHCP Protokoll.

## Peg DHCP

Peg wurde am 1.April 1998 Internet Engineering Task Force veröffentlicht. Doch Peg wurde anfangs als Aprilscherz angepriesen doch diese Methode fand überraschend Erfolg in der Praxis. Jede IP die zu vergeben ist wird auf eine Wäscheklammer geschrieben, die zur Abholung bereitgehalten wird. Die gültigen Parameter der Netzmaske und die IP-Adresse des Routers werden auf Papier geschrieben und ausgehängt und Kopien werden verteilt. Jeder einzelne Parameter werden auf die einzelnen Geräte separat eingestellt und die Wäscheklammer dann am jeweiligen Netzwerkkabel befestigt. Im die IPs vorzuhalten werden die IP-Adressen als Wäscheleinen gesehen und die Subnetze als Kleiderbügel. Die Definition umfasst, wie die Wäscheklammern und Papier an Brieftauben befestigt werden, um das IPoAC anzuwenden.