DHCP

Dynamic Host Configuration Protocol

Port: UDP 67 (server listen)
Port UDP 68 (client listen)

Automatische Vergabe von IP-Adressen an Clients

Thomas Mattern
Internet-Protokolle
25.11.2014

Inhaltsverzeichnis

1. Was ist DHCP?

DHCP ist ein Client-Serverprotokoll, das IP Hosts automatisch mit einer IP Adresse und anderen Netzwerkinformationen wie z.B. Subnetz-Maske oder Standard Gateway versorgt.

Der **DHCP** Standard wurde erstmals 1993 in RFC 1531 und 1541 definiert, ist aktuell durch RFC 2131 und 2132 festgelegt und wurde durch RFC 3396, 4361, 5494 und 6842 aktualisiert.

DHPC ist eine Erweiterung des Bootstrap Protokolls (**BOOTP**), definiert in RFC 951, das seinerseits das Reverse Address Resolution Protocol (**RARP** RFC 903) ablöste.

Die grundlegenden Funktionen des DHCP Protokolls waren schon in BOOTP implementiert. Bei RARP, das nur IP Adressen liefert, musste man pro Subnetz noch einen eigenen Server haben.

2. Warum DHCP?

Um auf ein Netzwerk und seine Ressourcen zugreifen zu können, muss jedes Netzwerkgerät eine eineindeutige IP Adresse haben. Ohne DHCP müsste man jedes Gerät manuell konfigurieren. DHCP wurde hauptsachlich für zwei Einsatzgebiete entwickelt:

1. Für große Netzwerke mit häufig wechselnder Topologie
2. Für Anwender, die „einfach nur eine Netzwerkverbindung“ haben möchten und sich nicht näher mit der Netzwerkkonfiguration beschäftigen wollen oder können.

Mit der Komplexität eines Netzwerks steigt natürlich auch die Anzahl der Parameter, die für einen Host/Client zum ordnungsgemäßen Funktionieren eingestellt werden müssen. Ein DHCP Server bietet die Möglichkeit dies zu automatisieren und die verschiedensten Parameter an zentraler Stelle zu verwalten. Der Server vergibt dann eine IP

Adresse (aus seinem Pool) an jeden DHCP-enabled Client, wenn dieser sich mit dem Netzwerk verbindet.

3. Wie arbeitet DHCP?

Mit DHCP hat man die Möglichkeit, IP Adressen und andere Netzwerkinformationen zu verteilen und zu aktualisieren. Ein DHCP Server stellt die Informationen einem DHCP Client über den Austausch einer Serie von DHCP-Mitteilungen zur Verfügung. Befinden sich Server und Client in verschiedenen Subnetzen wird ein DHCP Relay Agent benötigt, der die Kommunikation zwischen beiden herstellt.

4. DHCP Architektur

Die DHCP Architektur besteht aus Clients, Servern und Relay Agenten. Die Clients interagieren mit den Servern über DHCP Mitteilungen um eine IP Adresse zu erhalten oder zu verlängern.

4.1 DHCP Client

Ein DHCP Client ist jedes Netzwerkgerät mit der Fähigkeit, mit einem DHCP Server (gemäß RFC 2131) zu kommunizieren, um sowohl eine IP Konfiguration, als auch weitere damit verbundene optionale Parameter vom Server zu erhalten.

DHCP unterstützt auch **IP Autokonfiguration** (link-local addressing RFC 3927). Dies ermöglicht es Clients, IP Adresse und Subnetz Maske auch dann zu konfigurieren, wenn kein DHCP Server während des Systemstarts gefunden wird. Der DHCP Client Service verwendet dabei folgenden Ablaufplan:

1. Der Client versucht einen DHCP Server zu finden und eine IP Adresse zu erhalten.

2. Wird der Server nicht gefunden bzw. erhält der Client innerhalb einer Minute keine Antwort, autokonfiguriert der Client eine IP Adresse aus dem Bereich 169.254.0.0 (Maske 255.255.0.0). Dann überprüft er diese auf einen Adress-konflikt um sicherzustellen, dass die IP Adresse noch nicht verwendet wird

(via ARP RFC 826). Wird ein Konflikt gefunden, wählt der Client eine andere IP Adresse und wiederholt den Vorgang bis zu zehn Mal.
Besitzt der Client eine statische IP Konfiguration, wählt der Client diese. Auch hier prüft der Client einen Adresskonflikt. Wird ein Konflikt gefunden, wird der Benutzer darüber informiert.

3. War es dem Client möglich eine IP Adresse zu wählen, wird die Netzwerkkarte mit dieser konfiguriert. Der Client versucht aber weiterhin (alle 5 Minuten) einen DHCP Server zu finden. Antwortet ein Server auf seine Request Anfrage, verwirft der Client seine aktuelle IP Adresse und benutzt die vom Server zugewiesene sowie die vom Server angebotenen Optionen.

Sollte der Client bei einer früheren Gelegenheit eine IP Adresse von einem DHCP Server erhalten haben, und ist diese beim Systemstart noch nicht abgelaufen, versucht er die Nutzung dieser IP Adresse zu verlängern. Gelingt es dem Client bei diesem Versuch nicht einen DHCP Server zu erreichen, pingt er das Standard Gateway (der letzten IP Konfiguration) an und fährt wie folgt fort:

1. Ist der Ping erfolgreich, geht der Client davon aus, dass er sich noch im selben Netz befindet und verwendet die alte IP Konfiguration weiterhin. Normalerweise versucht er die IP Konfiguration zu verlängern, wenn 50% der Gültigkeitsdauer abgelaufen ist.

2. Schlägt der Ping fehl, geht der Client davon aus, dass er sich in einem anderen Netz befindet. (s.o.)

4.2 DHCP Server

Ein DHCP Server verwaltet Bereiche (Scopes), Adress-Reservierungen und Optionen. Ein Scope muss korrekt definiert und aktiviert sein, bevor er benutzt werden kann.

4.2.1 DHCP Scope

Ein **DHCP Scope** ist eine administrative Sammlung von IP Adressen und IP Konfigurationsparametern die für die Clients auf einem Subnetz zur Verfügung stehen. Der Admin legt für jedes Subnetz einen Scope an. Ein Scope hat folgende Eigenschaften:

1. Name
2. Intervall der möglichen IP Adressen, incl. Aus- und Einschlussbereiche
3. Subnetz Maske
4. Gültigkeitswerte

Jeder Scope kann nur einen einzigen zusammenhängenden IP Bereich benutzen. Um mehrere Bereiche innerhalb eines Scopes zu realisieren, benutzt man Ausschlussbereiche.

4.2.2 Gültigkeitsdauer der IP Adressen

Wird ein neuer Scope erstellt, wird auch eine Standardgültigkeitsdauer für die automatisch zu vergebenen IP Adressen festgelegt (z.B. 8 Tage). Es gibt aber durchaus Situationen, in denen es sinnvoll ist, diese zu ändern:

1. Organisation mit einer großen Anzahl von verfügbaren IP Adressen und sich selten verändernden Clients:
   Der Admin erhöht die Gültigkeitsdauer. Dies verringert die Frequenz der Verlängerungsanfragen der Clients und damit den DHCP Traffic.

2. Organisationen (wie Uni Bi) mit einer begrenzten Anzahl von IP Adressen, häufigen Client Konfigurationsänderungen oder vielen Clients wie z.B. Notebooks oder Handys), die dem Netz ständig beitreten oder es verlassen:
   Der Admin reduziert die Gültigkeitsdauer der IP Adressen, um die Rate – mit der ungenutzte IP Adressen dem Pool der verfügbaren Adressen wieder zugeführt werden – zu erhöhen.

Beispiel:
Vergleich der Anzahl der verbundenen Computer und der verfügbaren IP Adressen. Wenn sich 40 Computer 254 IP Adressen teilen müssen und schon mal vergebene Adressen selten von anderen Computer wiederverwendet werden. Hier ist eine große Gültigkeitsdauer von einigen Monaten sicherlich sinnvoll. Wenn sich allerdings 240 Computer den gleichen IP Bereich teilen müssen, ist der Bedarf an freien IP Adressen höher und die Gültigkeitsdauer sollte z.B. nur ein paar Tage betragen.

Obwohl es möglich ist, die Gültigkeitsdauer auf Unendlich zu setzen, ist dies mit Vorsicht zu genießen. Auch in stabilen, sich kaum verändernden Netzwerkumgebungen verändern sich immer wieder einige Clients. Computer werden ersetzt, werden von einem Büro in ein anderes verschoben, Netzwerkkarten werden ersetzt. Wird ein Computer mit unendlicher IP Gültigkeitsdauer aus dem Netz entfernt, wird der Server darüber nicht informiert (Es erfolgen ja überhaupt keine Verlängerungsanfragen). Diese IP Adresse kann also dem Pool der freien IP Adressen nicht wieder zugefügt werden. Da die Clients keine Verlängerungsanfragen an den Server mehr stellen, werden sie auch nicht mit sich ändernden DHCP Optionen versorgt. Es ist besser Reservierungen (s.u.) zu nutzen, statt die Gültigkeitsdauer auf Unendlich zu stellen.

4.2.3 Adress-Ausschlussbereiche

Nach der Erstellung eines neuen Scopes sollte man sofort Ausschlussbereiche für statisch konfigurierte Netzwerkgeräte definieren. Mithilfe dieser Ausschlussbereiche lassen sich speziell IP Adressen innerhalb eines Scopes von der automatischen Vergabe ausschließen. In der Regel sollten Router, Firewalls oder Server mit statischen IP Adressen konfiguriert werden und diese gehören dann natürlich in die Ausschluss-bereiche. Meines Erachtens ist es allerdings besser, diese Geräte manuell zu konfigu-rieren **und** sie in die Liste der reservierten IP Adressen (s.u.) aufzunehmen.

4.2.4 Adress-Reservierungen

Es ist auch möglich, IP Adressen bestimmten Geräten zuzuweisen. Mit diesen Reservierungen ist sichergestellt, dass eine bestimmte Hardware immer die gleiche IP Adresse zugewiesen bekommt. Reservierungen sollten für alle Geräte verwendet werden, die immer die gleiche IP Adresse haben müssen. Kommen mehrere DHCP Server für das gleiche Subnetz zum Einsatz, müssen die Reservierungen an allen DHCP Servern konfiguriert werden. Andernfalls könnte einer dieser Clients von einem zweiten Server eine automatisch vergebene (falsche) IP Adresse erhalten.

4.3 DHCP Client Server Protokoll

DHCP Server und Clients kommunizieren durch den Austausch einer Reihe von DHCP Meldungen untereinander. Die Unterhaltung wird dabei immer vom Client aus gestartet.

4.3.1 DHCP Meldungen

DHCPDiscover:
Broadcast Meldung (255.255.255.255) des DHCP Clients, wenn er versucht, sich zum ersten Mal mit einem Netzwerk zu verbinden.

DHCPOffer:
Broadcast Meldung jedes DHCP Servers, der eine DHCPDiscover Meldung erhalten hat und der eine IP Konfiguration für den Client zur Verfügung stellen kann. Die DHCPOffer Meldung enthält eine – noch nicht zugewiesene – IP Adresse sowie zusätzliche TCP/IP Konfigurationsparameter wie Subnetzmaske und Standard Gateway. Erhält der Client mehr als nur eine DHCPOffer Meldung, kann er sich die beste aussuchen. Dies ist in der Regel die erste DHCPOffer Meldung.

DHCPRequest:
Broadcast Meldung des DHCP Clients nachdem er eine DHCPOffer Meldung erhalten hat. Sie enthält die IP Adresse der von ihm ausgewählten DHCPOffer Meldung.
Ein Client, der seine IP Adresse verlängern will, kann diese Meldung auch als Unicast Meldung direkt an den Server schicken.

DHCPAck:
Broadcast Meldung des DHCP Servers an den Client, dass er den DHCPRequest akzeptiert. Zu diesem Zeitpunkt werden auch DHCP Optionen an den Client übermittelt. Nachdem der Client die DHCPAck Meldung erhalten hat, kann er die IP Adresse nutzen. In der Regel wird die Meldung als Broadcast gesendet, da der Client ja noch keine offizielle IP Adresse besitzt. Verschickt der Server DHCPAck als Antwort auf ein DHCPInform, wird die Meldung per Unicast direkt an den Client verschickt.

DHCPNack:
Broadcast Meldung des DHCP Servers an den Client, dass er den DHCPRequest ablehnt. Dies kann passieren, wenn die vom Client angeforderte IP Adresse falsch ist, der Client zwischenzeitlich das Subnetz gewechselt hat oder die Gültigkeitsdauer abgelaufen ist und nicht verlängert werden kann.

DHCPDecline:
Broadcast Meldung des DHCP Clients an den Server, dass die angebotene IP Adresse von einem anderen Host bereits verwendet wird.

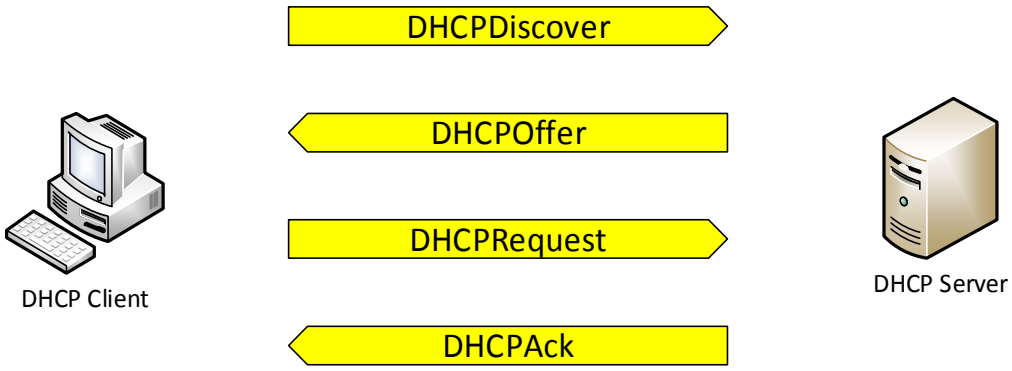
DHCPRelease:
Unicast Meldung des DHCP Clients an den Server, dass die verwendete IP Adresse nicht mehr benötigt wird. Diese Meldung wird direkt an den DHCP Server verschickt, der die IP Adresse vergeben hat.

DHCPInform:
Meldung des DHCP Clients an den Server mit der Bitte, nur die zusätzlichen Konfigurationsparameter zu verschicken, der Client hat bereits eine IP Adresse. Wird auch von DHPC Servern verschickt, um nicht autorisierte DHCP Server im Netz zu finden.

4.3.2 Ablaufprozess der DHCP Kommunikation

Ein Client, der DHCP aktiviert hat, möchte vom DHCP Server eine IP Adresse erhalten. Bevor die Gültigkeitsdauer einer bereits erhaltenen IP Adresse abläuft, muss der Client diese verlängern lassen oder eine neue anfordern. Die Daten einmal vergebener IP Adressen werden vom Server auch nach Ablauf der Gültigkeitsdauer noch für eine bestimmte Zeit gespeichert (ca. 4h mit stündlicher Bereinigung). Dies schützt die IP Adresse eines Clients, der sich z.B. in einer anderen Zeitzone als der Server befindet, dessen Uhr nicht mit der des Servers synchronisiert ist oder der zum Zeitpunkt des Gültigkeitsablaufs gerade offline ist.
Der Client startet die Kommunikation mit dem Server, wenn er eine neue IP Konfiguration erhalten möchte, wenn er seine IP Adresse verlängern möchte oder wenn er neustartet. Eine DHCP Unterhaltung besteht aus einer Abfolge von DHCP Meldungen (s.o.), die zwischen dem Client und dem Server ausgetauscht werden.

Neue IP Adresse anfordern:



1. Der Client fordert eine IP Adresse vom Server an, indem eine DHCPDiscover Broadcast Meldung auf das Subnetz sendet. Antwortet kein Server, wiederholt der Client die DHCPDiscover Meldung in Intervallen von 0, 4, 8, 16, 32 sec (+ einem Zufallsintervall von [-1, +1] sec). Hat der Client nach einer Minute immer noch keine Antwort erhalten, nutzt er (wenn eingeschaltet) IP Autokonfiguration (s.o.) oder die Netzwerkinitialisierung schlägt fehl. In beiden Fällen wird die DHCPDiscover Meldung alle 5 min. wiederholt.

2. Der Server sendet mit einer DHCPOffer Meldung eine IP Adresse und Konfigurationsinformationen an den Client.

3. Der Client zeigt dem Server an, dass er die IP Konfiguration akzeptiert, indem er eine DHCPRequest Meldung (mit der IP Adresse) an den Server sendet.

4. Der Server akzeptiert die Request Meldung des Clients mit DHCPAck.

Nach Erhalt der DHCPAck Meldung vervollständigt der Client seine TCP/IP Konfiguration incl. der vom Server übermittelten Optionen. In den seltenen Fällen, in denen der Client eine DHCPNack Meldung vom Server erhält, muss er mit dem Prozess von vorne beginnen. Befinden sich Client und Server in verschiedenen Subnetzen muss ein Router eingesetzt werden, der DHCP Forwarding unterstützt.

Alte IP Adresse verlängern:

Wenn 50% der Gültigkeitsdauer (T1) der IP Adresse abgelaufen ist, versucht der Client zum ersten Mal diese zu verlängern. Dazu sendet er einen Unicast DHCPRequest an den Server, von dem er die IP Adresse erhalten hat. Ist der Server erreichbar und die IP

Adresse noch nicht abgelaufen, antwortet er mit einer Unicast DHCPAck Meldung und die Adresse ist verlängert. Ist die IP Adresse nicht mehr verfügbar, antwortet der Server mit einer DHCPNack Meldung. Der Client muss dann eine neue IP Adresse anfordern (s.o.).

Erhält der Client keine Meldung vom ursprünglichen DHCP Server, benutzt er die IP Adresse erst mal weiter, bis 87,5% der Gültigkeitsdauer (T2) abgelaufen ist. Nach T2 verschickt der Client eine DHCPRequest Broadcast Meldung, um seine IP Adresse bei irgendeinem verfügbaren DHCP Server zu verlängern. Sollte bei Ablauf der Gültigkeitsdauer kein DHCP Server verfügbar sein, fordert er eine neue IP Adresse an (s.o.).

4.3.4 Adresskonfliktvermeidung

Client Adresskonflikterkennung:

In der Regel prüfen Clients automatisch, ob eine IP Adresse im Netz bereits vergeben ist. Dazu verschickt der Client via Address Resolution Protocol (ARP) eine Anfrage an die IP Adresse, die ihm zugeteilt wurde. Erhält er darauf eine Antwort verschickt er eine DHCPDecline Meldung an den DHCP Server. Der Server seinerseits markiert diese IP Adresse mit einem BAD_ADDRESS Flag für die Zeit der Gültigkeitsdauer. Der Client muss ARP nutzen, da Ping nur funktioniert, wenn der Sender eine IP Adresse hat (ARP funktioniert nicht über Router hinweg).

Server Adresskonflikterkennung:

Ein DHCP Server betreibt in der Regel keine IP Adresskonflikterkennung. Ist sie auf dem Server aktiviert, nutzt er Ping, bevor er eine neue Adresse vergibt. Hier liegt die Betonung auf „neue“, bereits einmal vergebene Adressen werden nicht geprüft. Wird ein Adresskonflikt gefunden, wird die Adresse für die Zeit der Gültigkeitsdauer mit dem BAD_ADDRESS Flag versehen.

4.4 DHCP Optionen

DHCP Optionen sind zusätzliche Konfigurationsparameter, die ein DHCP Server seinen Clients zuweisen kann. DHCP Optionen werden hierarchisch vergeben. Server-weit, Server-weit, Scope-weit oder Client-spezifisch. Dabei überschreiben die Unterklassenwerte die Werte der Oberklasse. D.h. alle für einen speziellen Client festgelegten Werte überschreiben die Werte, die für einen Scope oder Server-weit festgelegt

sind. Enthält ein bestimmter Parameter keinen Wert, wird der Wert der nächst höheren Klasse übernommen und so weiter.
In der Regel werden die DHCP Optionen aber nur Server-weit oder Scope-weit gesetzt. Spezielle Clients, die sich im Allgemeinen auch in der Reservierungsliste befinden, werden dann noch mit abweichenden Parametern versehen.

Eine „kurze“ Übersicht über verschiedene Optionen, die mit Hilfe des DHCP Protokolls einem Host übermittelt werden können, findet sich im Anhang.

Wenn man die Liste überfliegt, zeigt sich schnell, dass DHCP ein ziemlich mächtiges Werkzeug ist.

5. DHCP Sicherheit

DHCP kann leicht manipuliert werden, da die Clients in der Regel jeden DHCP-Server akzeptieren. Ein Angreifer könnte z.B. alle freien IP Adressen des Servers für sich reservieren. Damit ist der eigene DHCP Server erst mal ausgeschaltet. Dann fungiert der Angreifer selber als DHCP Server und schiebt den Clients neue DNS-Server unter, welche DNS-Anfragen auf manipulierte Seiten umleiten. Auch eine MAC Adress-filterung am eigenen DHCP-Server hilft hier nicht weiter, da diese viel zu leicht selbst vergeben und (bei physikalischem Zugang) abgehört werden können.

Anhang

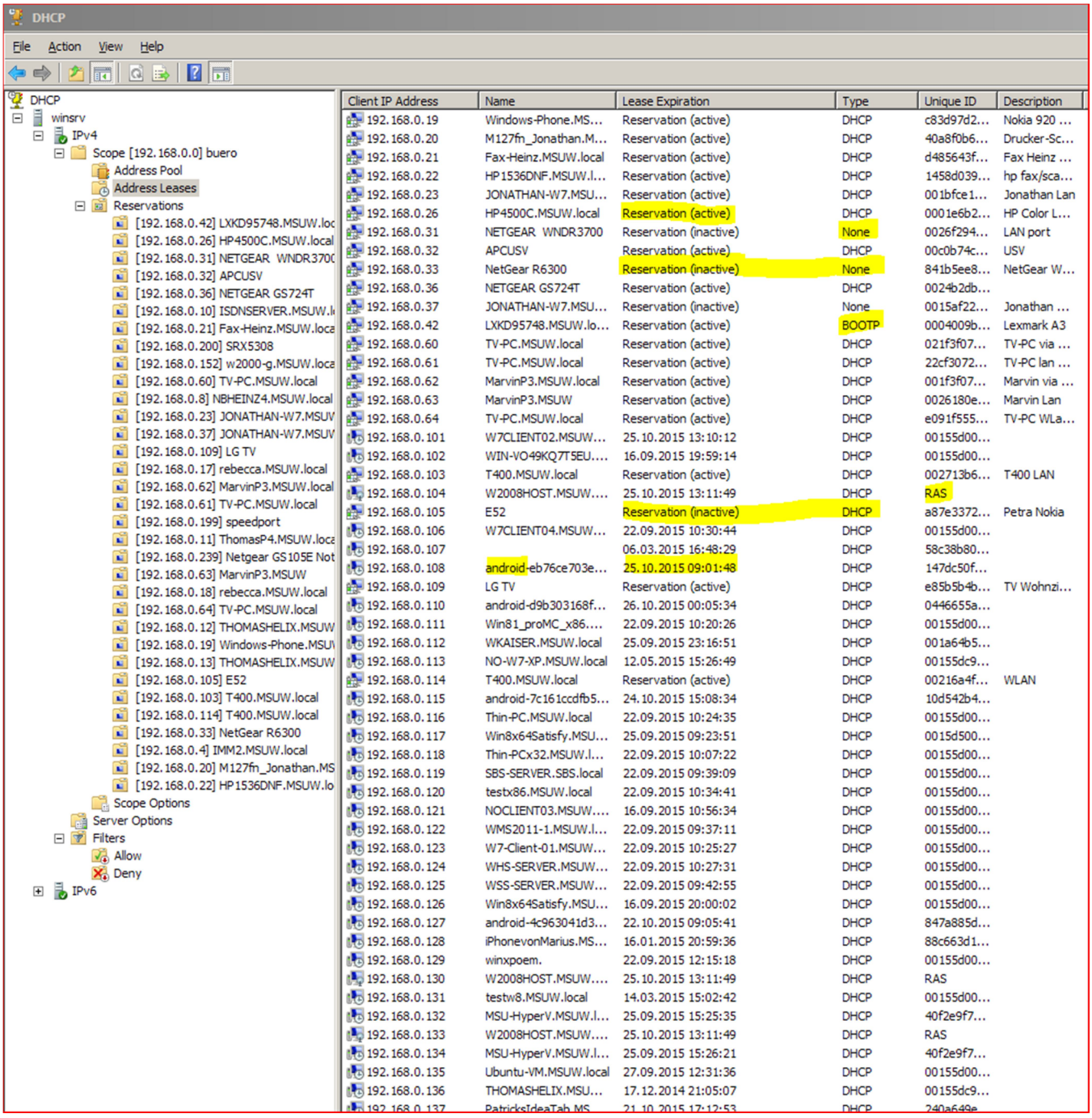
Felder der DHCP Meldung

Feld Name	Name	Feldlänge [Oktets]	Beschreibung
Op	Message Type	1	Message type.
htype	Hardware Address Type	1	Hardware address type defined at Internet Assigned Numbers Authority (IANA).
hlen	Hardware Address Length	1	Hardware address length, in octets.
hops	Hops	1	Value set to zero by DHCP clients. Optionally used to count the number of relay agents that forwarded the message.
Xid	Transaction ID	4	A random number used to associate messages and responses between a client and a server.
secs	Seconds	2	Seconds elapsed since client began address acquisition or renewal process.
flags	Flags	2	Flags set by client. The Broadcast flag is set if the client cannot receive unicast IP datagrams (for example, before it is configured with an IP address).
ciaddr	Client IP Address	4	Used if the client has an IP address and can respond to Address Resolution Protocol (ARP) requests.
yiaddr	Your IP Address	4	Address given to the DHCP client by the DHCP server.
siaddr	DHCP Server IP Address	4	IP address of the server that is offering a lease.
giaddr	Gateway IP Address	4	DHCP relay agent IP address.
chaddr	Client Hardware Address	16	Client hardware address.
sname	Server Host Name	64	Optional server host name.
file	Boot File Name	128	The name of the file containing the boot image for a BOOTP client.
options	Options	variable	Optional parameters field. In the DHCP protocol packet, each option begins with a single octet tag, which holds the option code, and a second octet, which describes the option data length, in bytes.

DHCP Optionen:

-001 **Subnet Mask** = Subnet Mask
-002 Time Offset = UCT offset in seconds
-003 **Routers** = Array of router addresses ordered by preference
-004 Time Servers = Array of time server addresses, by preference
-005 Name Servers = Array of Name server addresses, by preference
-006 **DNS Servers** = Array of DNS server addresses, by preference
-007 Log Servers = Array of MIT_LCS UDP log servers on subnet
-008 Cookie Server = Array of cookie server, RFC 865
-009 LPR Servers = Array for RFC 1179 servers, by preference
-010 Impress Servers = Array of Imagen Impress Servers
-011 Resource Location Servers = Array of RFC 887 ResLoc Servers on subnet, by preference
-012 Host Name = Host Name for client, RFC 1035 character set
-013 Boot File Size = Size of boot image file in 512-octect blocks
-014 Merit Dump File = Path name for crash dump file
-015 **DNS Domain Name** = DNS Domain name for client resolution
-016 Swap Server = Address of client's swap server
-017 Root Path = Path name for client's root disk, char set NVA ASCII
-018 Extensions Path = TFTP file for option extensions
-019 IP Layer Forwarding = Disable/enable IP packet forwarding on the client
-020 Nonlocal Source Routing = Disable/enable nonlocal datagram's
-021 Policy Filter Masks = Destination/Mask IP address pairs to filter source routes
-022 Max DG Reassembly Size = Maximum size datagram for reassembly by client; max 576
-023 Default IP Time-to-live = Default TTL for client's use on outgoing DGs
-024 Path MTU Aging Timeout = Timeout in seconds for aging Path MTU values, RFC 1191
-025 Path MTU Plateau Table = MTU discovery sizes, sorted by size, all >=68
-026 MTU Option = MTU discovery size, >=68
-027 All subnets are local = The client assumes that all subnets are local
-028 Broadcast Address = Broadcast address
-029 Perform Mask Discovery = The client should use ICMP for subnet mask discovery
-030 Mask Supplier Option = The client should respond to subnet mask requests via ICMP.
-031 Perform Router Discovery = The client should solicit routes using RFC 1256
-032 Router Solicitation Address = Address to use for router solicitation
-033 Static Route Option = Destination/router address pairs, in priority order
-034 Trailer Encapsulation = The client should negotiate use of trailers (RFC 983)
-035 ARP Cache Timeout = Timeout in seconds for ARP cache entries
-036 Ethernet Encapsulation = 0=>client should use ENet V2; 1=> IEEE 802.3
-037 TCP default Time-to-live = TTL that client uses when sending TCP segments
-038 Keep alive Interval = Keep alive timeout in seconds
-040 NIS Domain Name = Name of Network Information Service domain
-041 NIS Servers = Addresses of NIS servers on client's subnet
-042 NTP Servers = Addresses of Network Time Protocol servers
-043 Vendor Specific Info = Embedded vendor-specific options
-044 **WINS/NBNS Servers** = Array of NBNS Addresses in priority order
-045 NetBIOS over TCP/IP NBDD = NetBIOS over TCP/IP NBDD address(es) in priority order
-046 WinS/NBT Node Type = 0x1 = B-node; 0x2 = P-node; 0x4 = M-node; 0x8 = H-node
-047 NetBIOS Scope ID = NetBIOS over TCP/IP Scope ID
-048 X Window System Font = Array of X Window font servers
-049 X Window System Display = Array of X Window Display Mgr servers
-064 NIS+ Domain Name =The name of the client's NIS+ domain.
-065 NIS+ Servers = A list of IP addresses indicating NIS+ servers
-066 Boot Server Host Name = TFTP boot server host name,
-067 Bootfile Name = Boot file name
-068 Mobile IP Home Agents = Mobile IP home agents in priority order
-069 Simple Mail Transport Protocol (SMTP) Server = List of SMTP servers available to the client
-070 Post Office Protocol (POP3) Server = List of POP3 servers available to the client

DHCP Server Beispiel:



Quellenangaben

diverse. (21. 09 2014). *Address Resolution Protocol.* (Wikipedia, Hrsg.) Abgerufen am 19. 10 2014 von Wikipedia: http://en.wikipedia.org/wiki/Address_Resolution_Protocol

diverse. (9 2014). *Dynamic Host Configuration Protocol*, 16.10.2014. (Wikipedia, Herausgeber) Abgerufen am 18. 10 2014 von http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

diverse. (18. 10 2014). *Zero-configuration networking.* (Wikipedia, Hrsg.) Abgerufen am 19. 10 2014 von Wikipedia: http://en.wikipedia.org/wiki/Zero-configuration_networking

Microsoft (Hrsg.). (2. 09 2008). *DHCP Server.* Abgerufen am 19. 10 2014 von Microsoft Technet: http://technet.microsoft.com/en-us/library/cc896553(v=ws.10).aspx

RFC0826 (Hrsg.). (11 1982). *An Ethernet Address Resolution Protocol.* Abgerufen am 19. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc826

RFC0903 (Hrsg.). (06 1984). *A Reverse Address Resolution Protocol (RARP).* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc903

RFC0951 (Hrsg.). (09 1985). *BOOTSTRAP PROTOCOL (BOOTP).* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc951

RFC1531 (Ed.). (1993, 10). *Dynamic Host Configuration Protocol.* Retrieved 10 18, 2014, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc1531

RFC1541 (Ed.). (1993, 10). *Dynamic Host Configuration Protocol.* Retrieved 10 18, 2014, from The Internet Engineering Task Force: http://tools.ietf.org/html/rfc1541

RFC2131 (Hrsg.). (03 1997). *Dynamic Host Configuration Protocol.* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc12131

RFC2132 (Hrsg.). (03 1997). *DHCP Options and BOOTP Vendor Extensions.* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc2132

RFC3396 (Hrsg.). (11 2002). *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4).* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc3396

RFC3927 (Hrsg.). (05 2005). *Dynamic Configuration of IPv4 Link-Local Addresses.* Abgerufen am 19. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc3927

RFC4361 (Hrsg.). (02 2006). *Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4).* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc4361

RFC5494 (Hrsg.). (04 2009). *IANA Allocation Guidelines for the Address Resolution Protocol (ARP).* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc5494

RFC6842 (Hrsg.). (01 2013). *Client Identifier Option in DHCP Server Replies.* Abgerufen am 18. 10 2014 von The Internet Engineering Task Force: http://tools.ietf.org/html/rfc6842