Hochschule für Telekommunikation Leipzig (HfTL)

Kommunikationsnetze I

Laborbeleg

DHCP - Dynamic Host Configuration Protocol

Michael Müller
(147105)

Wintersemester 2015/16

Inhaltsverzeichnis

1 Vorbereitende Aufgaben

1.1 Welche netzwerkrelevanten Daten benötigt eine Workstation in einem LAN mindestens?

Jede aktive Netzwerkkomponente benötigt eine **MAC-Adresse** (*Media-Access-Control-Adresse*), die ein Netzwerkgerät eindeutig identifiziert. Diese ist fest auf der Hardware gespeichert und kann im Allgemeinen nicht angepasst werden[1].
Die verwendete Technologie muss dem Netzwerkadapter ebenfalls bekannt sein. Am weitesten verbreitet für die Kommunikation in einem LAN ist heutzutage der Ethernet Standard. Ethernet bildet dabei die Basis für die Netzwerkkommunikation mittels TCP/IP [2]. Dafür benötigen die beteiligten Workstations mindestens eine individuelle, im Netzbereich eindeutige, **IP-Adresse**[3] sowie eine entsprechende **Subnetzmaske**. Weiterhin benötigt eine Workstation einen eindeutigen **Hostnamen**. Dieser kann durch eine **Domain/Domäne** erweitert und als Fully-Qualified Host Name (FQHN) angegeben werden.
Alle Kommunikationspartner müssen sich im selben Netzsegment (Teilnetz) befinden. Ansonsten schlägt die Kommunikation untereinander fehl.

1.2 Welche weiteren Netzwerkinformationen werden im Heim- und/oder Office-Bereich (z.B. Dienste/Geräte) benötigt?

Für eine Kommunikation in andere Netzsegmente muss ein **Gateway** (*next router*) konfiguriert werden, der das Routing in andere Netze übernimmt. In diesem Zusammenhang können ebenfalls **Routen** an der Workstation konfiguriert werden. Wenn ein Gateway konfiguriert wurde, wird automatisch die *Default-Route* gesetzt.
Für bestimmte Dienste ist eine **Portweiterleitung** (*port forwarding*) notwendig, um bspw. Webserver über die Gatewayadresse ansprechen zu können (NAT). Des Weiteren kann unter Windows ein **WINS-Server** (*Windows Internet Naming Service*) angegeben werden.
Optional kann ein **Domain Name Service (DNS) Server** für die Namensauflösung im Netzwerk und Zeitserver für die automatische Anpassung von Datum/Uhrzeit und konfiguriert werden.

1.3 Welche netzwerkrelevanten Daten benötigt eine Workstation für das WAN (Internet)?

Für den Zugriff aus dem lokalen Netzwerk auf das Internet (WAN) ist ein **WAN-Gateway** für das Routing zwischen privatem und öffentlichem Netz erforderlich. In der Regel ist dies der DSL-Router. Um die Dienstleistungen eines Internet Service Provider (ISP) nutzen zu können sind entsprechende **Zugangsdaten** notwendig, die im WAN-Gateway konfiguriert und mittels Point-to-Point Protocol (PPP) übermittelt werden[4].

[1] Kann mit entsprechenden Tools selbstverständlich doch angepasst werden.
[2] Weitere Protokollfamilien sind AppleTalk, DECnet oder IPX/SPX
[3] die verwendete Version (IPv4 oder IPv6) muss dem Netzwerkadapter ebenfalls bekannt sein
[4] häufig als Point-to-Point Protocol over Ethernet (PPPoE)

Für die Auflösung von Internetadressen ist ein **DNS-Server** unumgänglich. Dieser wird standardmäßig vom ISP bereitgestellt, kann jedoch auch individuell konfiguriert werden.

1.4 Diskutieren Sie Sicherheitsprobleme die durch DHCP entstehen können!

DHCP nutzt das Transportprotokoll UDP. Der Client akzeptiert damit jeden DHCP-Server für die automatische Konfiguration. Gibt es im Netz einen weiteren DHCP-Server, der möglicherweise schneller antwortet als der vorgesehene, kann ein ganzer Netzbereich lahmgelegt werden. Damit kann durch einen Angreifer bspw. eine Umleitung auf einen anderen DNS-Server vorgenommen werden.

Wie bereits erwähnt ist eine MAC-Adresse nicht in jedem Fall eindeutig. Durch MAC-Spoofing kann ein DHCP-Server getäuscht und eine IP-Adresse (und weitere DHCP-Optionen) einer anderen Netzwerkkomponente, als ursprünglich vorgesehen, zugewiesen und damit etwaiger exklusiver Zugriff gewährt werden.

Eine weitere Gefahr stellen **Denial-of-Service-Angriffe** (*DOS*) auf DHCP-Server dar. Der DHCP-Server wird mit Unmengen an Lease-Anfragen beschäftigt, so dass die Anzahl der Leases verringert wird, die für die anderen DHCP-Clients verfügbar sein sollten.

1.5 DHCP ermöglicht es IP-Adress-Ranges (Scope) zu definieren, wodurch ein ganzer Bereich von IP-Adressen dynamisch verwaltet wird. Ist es dennoch notwendig für einzelne Hosts IP-Adressen statisch zu vergeben? Warum und für welche Hosts bzw. Netzwerkkomponenten?

Ja, für bestimmte Netzwerkkomponenten ist es sinnvoll, feste/statische IP-Adressen zu vergeben. Auf der einen Seite benötigen bestimmte aktive Netzwerkkomponenten, wie Router, Access-Points und L3-Switche, für ihre Interfaces feste Adressen, auf der anderen müssen bestimmte Maschinen auch dann erreichbar sein, wenn ein DHCP-Server ausfällt oder durch DOS-Angriffe lahmgelegt ist.

Ebenso sollten Server und NAS/SAN feste IP-Adressen bekommen. Wie in Abschnitt 1.4 bereits erwähnt lassen sich so bestimmte Manipulationen verhindern. Genauso verhält es sich mit Hosts, auf denen kritische Anwendungen laufen. Clients, Drucker und andere Netzwerkkomponenten können, sofern sie keine kritischen Anwendungen realisieren, mittels Reservierungen im DHCP-Server konfiguriert werden. Dadurch erhalten diese ebenfalls immer die selbe IP-Adresse, jedoch können weitere Parameter (z.B. Standard-Gateway, Hostname, DNS-Server, WINS-Server) zentral gepflegt und verteilt werden. Bestimmte Anwendungen, wie z.B. im Netz der Deutschen Telekom AG, setzen feste IP-Adressen voraus, um exklusiven Zugriff auf bestimmte Geräte oder Dienste zu erhalten. Entsprechende Hosts müssen mit einer statischen IP-Adresse versehen werden.

Allgemein kann man sagen, dass alle Geräte, die von anderen im Netzwerk angesteuert werden, sollten mit einer festen IP-Adresse konfiguriert werden. Selbstverständlich benötigt auch der DHCP-Server

selbst eine feste IP-Adresse. Eine Vergabe einer IP-Adresse an sich selbst ist, meines Erachtens nach, nicht möglich.

1.6 Was muss man beim Einsatz von DHCP in gerouteten Netzen beachten?

DHCP ist ein broadcastbasierter Dienst und ist damit auf ein einzelnes Teilnetz beschränkt. Es gibt jedoch drei Möglichkeiten, einen DHCP-Server für geroutete Netze zu konfigurieren (vgl. Abbildung 1).

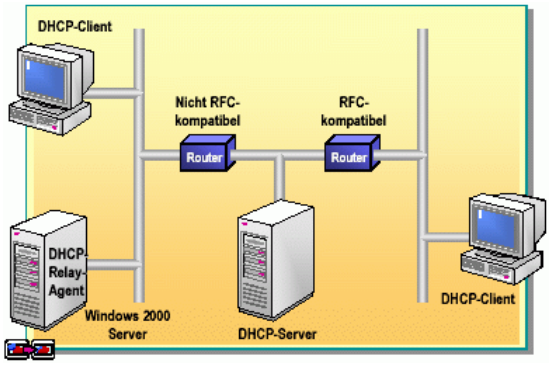

Abbildung 1: Konfigurationsoptionen in einem gerouteten Netzwerk
Quelle: http://rahbarsoft.de

Im einfachsten Fall wird **jedes Teilnetz mit einem DHCP-Server** ausgestattet. Durch die zusätzliche Maschine sowie die Notwendigkeit der bereichsspezifischen Konfiguration stellt diese Variante einen erheblichen Verwaltungsaufwand dar. Unter Berücksichtigung der Ausfallsicherheit sollten zwei DHCP-Server je Teilnetz betrieben werden. Diese Lösung ist zu teuer und wird daher selten verwendet.

Es besteht die Möglichkeit, einen RFC 1542-kompatiblen Router für **BOOTP-Weiterleitung** einzusetzen. Ein entsprechend konfigurierter Router leitet ausgewählte DHCP-Broadcasts an alle andere Teilnetze weiter. Die Weiterleitung anderer Broadcastanfragen findet dabei nicht statt. Diese Variante setzt gegebenenfalls eine aufwendige Konfiguration des Routers voraus. Weiterhin kann die DHCP-Kommunikation über mehrere Teilnetze stark verlangsamt werden.

Neben den bereits vorgestellten Varianten kann ein **DHCP-Relay-Agent** in jedem Teilnetz eingesetzt werden, um die DHCP-Meldungen weiterzuleiten. Broadcastmeldungen werden bei dieser Variante auf das Teilnetz beschränkt, aus dem diese gesendet wurden und nicht an alle Teilnetze weitergeleitet (im Gegensatz zur BOOTP-Methode). Die Konfiguration eines DHCP-Relay-Agent ist in der Regel einfacher als die vorangegangenen Lösungsansätze. Ein einzelner DHCP-Server kann mehrere Teilnetze effizienter versorgen als mit Hilfe von RFC 1542-kompatiblen Routern, wenn den Teilnetzen ein DHCP-Relay-Agent zugeordnet ist.

1.7 Welche Parameter können durch DHCP zur Verfügung gestellt werden? Nennen Sie mindestens 10!

Es können eine Vielzahl von weiteren Parametern (neben Hostname, IP-Adresse, Subnetzmaske, Gateway, DNS-Server, WINS-Server) mittels DHCP zur Verfügung gestellt werden. Nach RFC 2132 sind folgende DHCP-Options beispielhaft erwähnt:

- Time-Server
- Router
- statische Routen
- NetBIOS over TCP/IP name server
- IP lease Time
- TFTP Server
- Bootfile name
- Bootfile size
- SMTP-Server
- POP-Server
- MTU timeout
- MTU Interface
- Forward ON/OFF

2 Durchführung

2.1 DHCP Client

Analysieren Sie die DHCP-Pakete (*wireshark*). Welche Optionen und Parameter tauschen Client und Server aus?

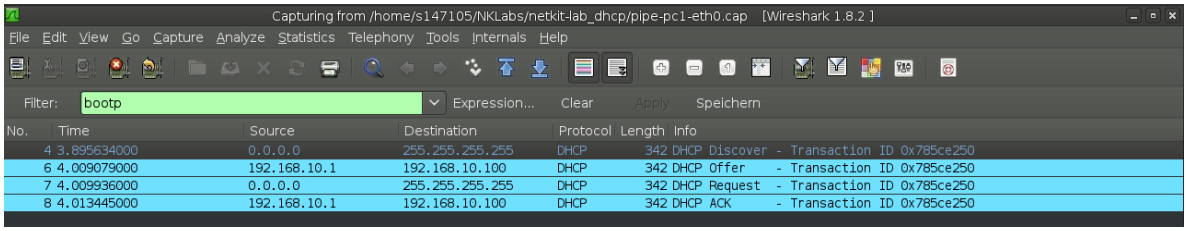

Abbildung 2: Wireshark - Kommunikation zwischen DHCP-Client und DHCP-Server

2.1.1 DHCP-Discover

Der Client sendet eine DHCPDISCOVER-Message mit seiner MAC-Adresse als Broadcast an alle verfügbaren DHCP-Server (streng genommen an alle angeschlossenen Netzwerkgeräte), wenn er erstmals eine IP-Adresse benötigt. Diese Nachricht enthält als Absender-IP-Adresse (*source address*) 0.0.0.0 und als Zieladresse (*destination address*) 255.255.255.255 (vgl. Abbildung.3). Verwendet werden der UDP-Quellport 68 und der UDP-Zielport 67.

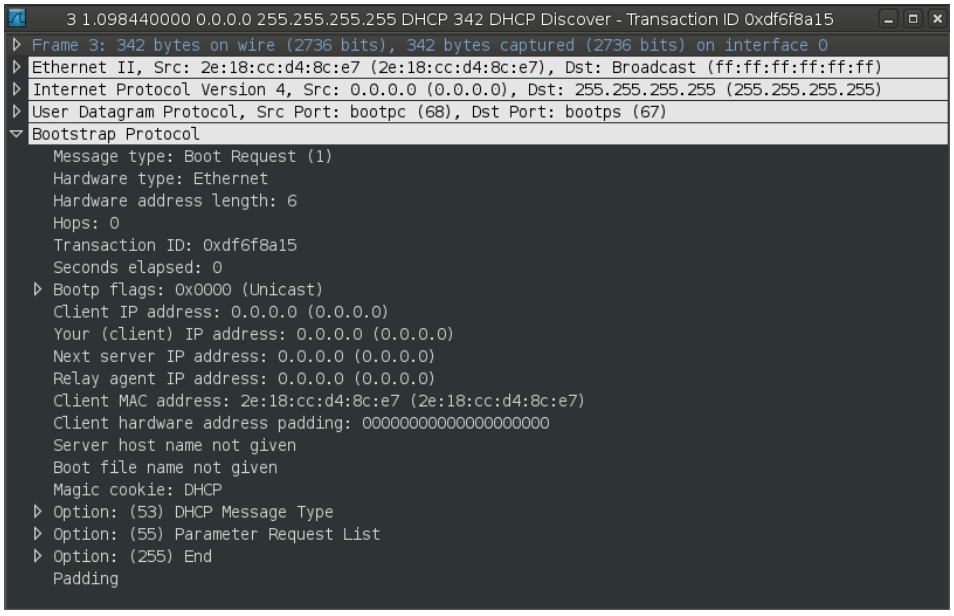

Abbildung 3: Wireshark - DHCPDISCOVER-Nachricht

2.1.2 DHCP-Offer

Der DHCP-Server antworten mit DHCPOFFER und schlägt dem Client eine IP-Adresse vor. Wie in Abbildung 3 erkennbar, ist das Broadcast-Bit (Bootp flag) beim DHCPDISCOVER nicht gesetzt. Dadurch antwortet der DHCP-Server mit einem Unicast an die vorgeschlagene IP-Adresse (in diesem Fall 192.168.10.100) und die MAC-Adresse des Clients (vgl. Abbildung 6).
Wäre das Broadcast-Bit gesetzt, würde der DHCP-Server mit einem Broadcast an die Adresse 255.255.255.255 antworten. In beiden Fällen werden wieder der UDP-Quellport 67 und der UDP-Zielport 68 verwendet.

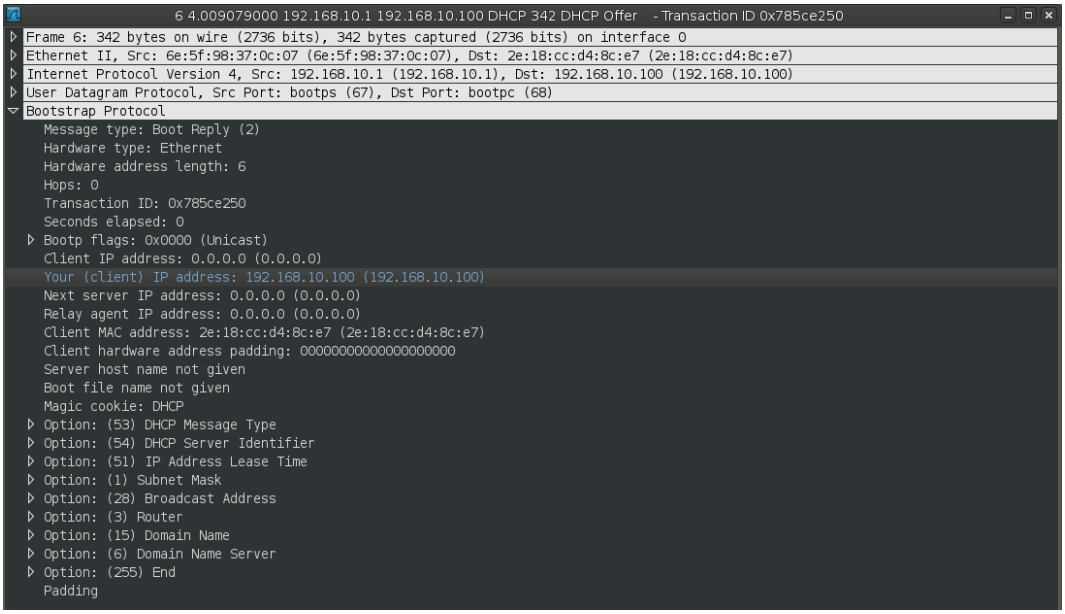

Abbildung 4: Wireshark - DHCPOFFER als Unicast

Neben der IP-Adresse übermittelt der DHCP-Server weitere Optionen; Serveridentifier, Lease-Zeit, Subnetzmaske, Broadcast-Adresse, Router, Domain Name, Domain Name Server.

2.1.3 DHCP-Request

Der Client entscheidet nun unter den eingetroffenen Angeboten (DHCPOFFER) und kontaktiert den entsprechenden DHCP-Server per Broadcast und dem im DHCPOFFER enthaltenen Serveridentifier mit einem DHCPREQUEST.

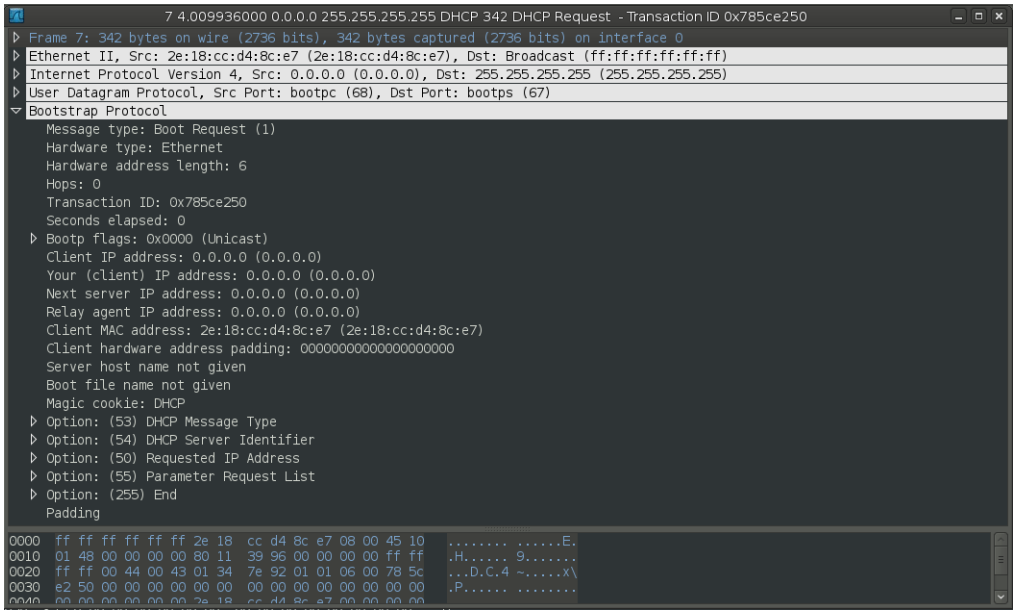

Abbildung 5: Wireshark - DHCPREQUEST vom Client zum DHCP-Server

Wenn mehrere DHCP-Server antworten, trifft der Client die Entscheidung anhand der längsten Lease-Zeit, wegen eines eventuell falsch konfigurierten DHCP-Server (wird abgelehnt) oder einfach nach der ersten Antwort. Alle anderen DHCP-Server werten das nicht-antworten als Absage ihrer Angebote und verwerfen diese gegebenenfalls. Im vorliegenden Szenario gibt es nur einen DHCP-Server, welcher korrekt konfiguriert ist. Daher wird dieser akzeptiert und kontaktiert.

2.1.4 DHCP-ACK

Der vom Client ausgewählte Server bestätigt in einer DHCPACK-Nachricht (*DHCP-Acknowledged*) die IP-Adresse mit den ausgehandelten Daten.

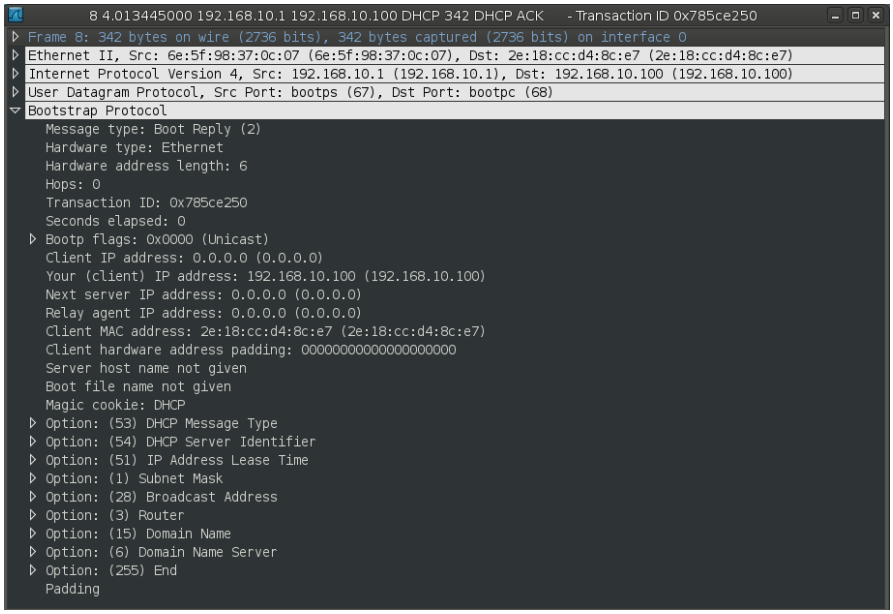

Abbildung 6: Wireshark - DHCPACK als Bestätigung vom DHCP-Server

2.2 Init-Reboot

Was ist am Protokollablauf anders, im Vergleich zur vorangegangenen Aufgabe? Informieren Sie sich in der Manpage zum dhclient, wo die Informationen gespeichert werden, die zu dem verändertem Verhalten führen und sehen Sie sich diese an.

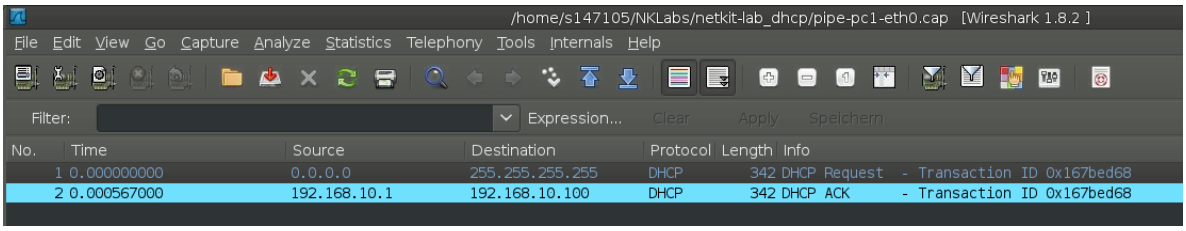

Abbildung 7: Wireshark - Kommunikation zwischen DHCP-Client und DHCP-Server nach erneuter Anforderung innerhalb der Lease-Zeit

Der DHCP-Client schickt sofort eine DHCPREQUEST-Nachricht an den Broadcast und fordert die zuvor zugewiesene IP-Adresse sowie eine Liste von Parametern vom DHCP-Server an (vgl. Abbildung 8).

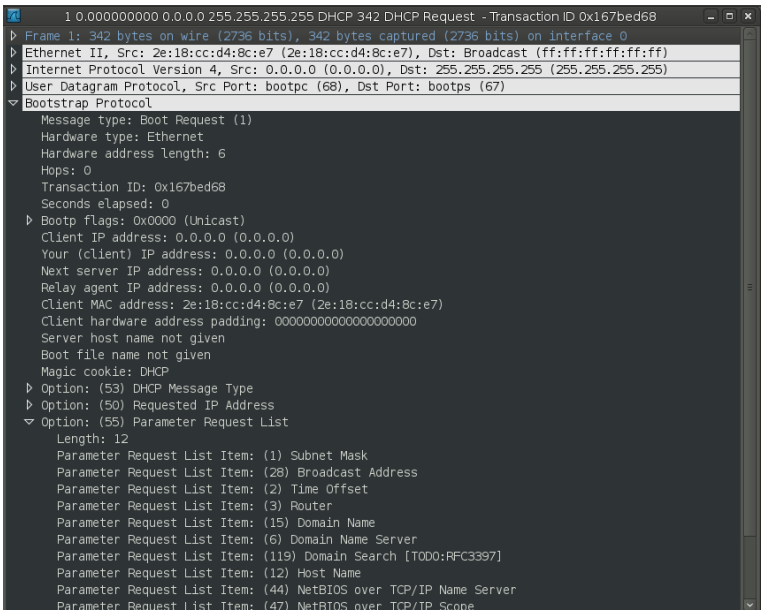

Abbildung 8: Wireshark - DHCPREQUEST vom Client zum DHCP-Server

Ein DHCPDISCOVER ist nicht mehr notwendig, da der Client den DHCP-Server bereits kennt und die Lease-Zeit noch nicht abgelaufen ist. Ein DHCPOFFER seitens des DHCP-Server ist demnach auch nicht nötig. Die entsprechenden Informationen speichert der DHCP-Client in der *dhclient.conf*.

Der DHCP-Server antwortet mit DHCPACK und übergibt dem Client damit die geforderten Parameter (vgl. Abbildung 9).

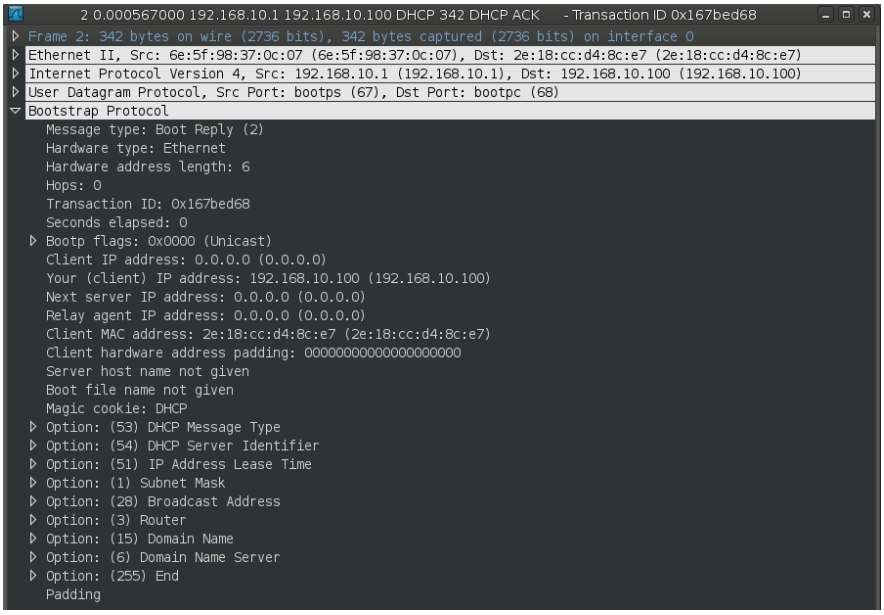

Abbildung 9: Wireshark - DHCPACK als Bestätigung vom DHCP-Server mit geforderten DHCP-Options

2.3 Lease Time

Rekonfigurieren Sie den DHCP-Server, sodass die Timer T1 und T2 (Lease Timer), bereits nach ein respektive zwei Minuten ablaufen. Starten Sie Server und Client neu. Untersuchen Sie anschließend das Verhalten des Clients (dhcp-lease.pcap).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe4418776
3	0.991566000	192.168.10.1	192.168.10.100	DHCP	342	DHCP Offer - Transaction ID 0xe4418776
4	0.992555000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe4418776
5	0.994491000	192.168.10.1	192.168.10.100	DHCP	342	DHCP ACK - Transaction ID 0xe4418776
8	27.993045000	192.168.10.100	192.168.10.1	DHCP	342	DHCP Request - Transaction ID 0xe4418776
9	27.994788000	192.168.10.1	192.168.10.100	DHCP	342	DHCP ACK - Transaction ID 0xe4418776
12	58.999985000	192.168.10.100	192.168.10.1	DHCP	342	DHCP Request - Transaction ID 0xe4418776
13	59.006159000	192.168.10.1	192.168.10.100	DHCP	342	DHCP ACK - Transaction ID 0xe4418776
16	88.999730000	192.168.10.100	192.168.10.1	DHCP	342	DHCP Request - Transaction ID 0xe4418776
17	89.004140000	192.168.10.1	192.168.10.100	DHCP	342	DHCP ACK - Transaction ID 0xe4418776

Abbildung 10: Wireshark - Kommunikation zwischen DHCP-Client und DHCP-Server nach Änderung der Lease-Zeit

Die DHCP-Kommunikation läuft wieder vollständig über Broadcast-Nachrichten ab (vgl. 2.1). Nach Ablauf der halben Lease-Zeit (hier 30 Sekunden) sendet der Client einen erneuten DHCPREQUEST und beantragt damit, die reservierte IP-Adresse weiterhin zu behalten. Dieser Request wird per Unicast direkt an den DHCP-Server gesendet, welcher die Konfiguration vergeben hat. Der Server antwortet mit einem DHCPACK und übermittelt die selben Daten wie bereits beim letzten Mal und verlängert damit die Konfiguration.

2.4 DHCP Release

Abbildung 11: Wireshark - Kommunikation zwischen DHCP-Client und DHCP-Server nach Lease-Anforderung

Der Client sendet eine DHCPRELEASE-Nachricht per Unicast an den Server und gibt damit die Konfiguration vor Ablauf der Lease-Zeit zurück. Der DHCP-Server bestätigt diese Anfrage nicht. Sollte dabei ein Fehler auftreten, würde dieser bei der nächsten Anfrage des Clients an den DHCP-Server, durch eine neue Aushandlung der Konfiguration, korrigiert.

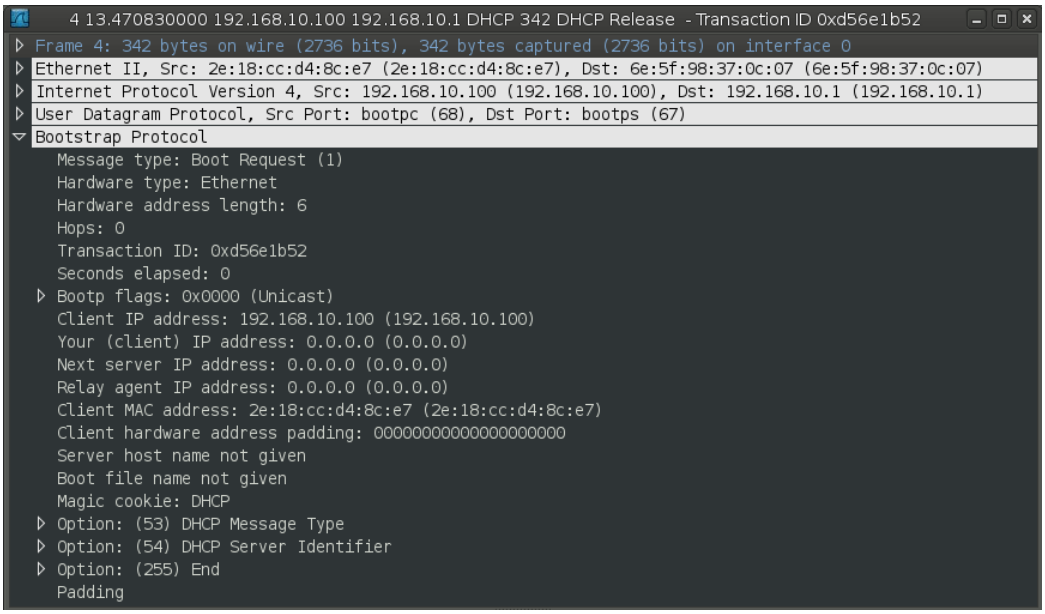

Abbildung 12: Wireshark - DHCPRELEASE vom Client zum DHCP-Server

2.5 statische Konfiguration

Fügen Sie in die Server-Konfiguration noch eine statische Konfiguration für die DHCP-Client Workstation ein. Starten Sie anschließend DHCP-Server und -Client neu. Zeichnen Sie den Datenaustausch (dhcp-static.pcap) auf und analysieren Sie ihn.

```
subnet 192.168.10.0 netmask 255.255.255.0 {
 range 192.168.10.100 192.168.10.120;
 option domain-name-servers 192.168.10.10;
 option routers 192.168.10.1;
 option broadcast-address 192.168.10.255;
 default-lease-time 60; #600;
 max-lease-time 60; #7200;

 host pc2{
    hardware ethernet 2e:18:cc:d4:8c:e7;
    fixed-address 192.168.10.50;
    default-lease-time 3600;
    max-lease-time 7200;
    option netbios-dd-server 192.168.10.1;
    option ntp-servers 192.168.10.1;
    option pop-server 192.168.10.1;
    option smtp-server 192.168.10.1;
 }
}
```

Abbildung 13: DHCP-Server Konfiguration */etc/dhcp3/dhcpd.conf*

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa7c7e14b
2	0.001263000	192.168.10.1	192.168.10.50	DHCP	342	DHCP Offer - Transaction ID 0xa7c7e14b
3	0.000230000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa7c7e14b
4	0.005698000	192.168.10.1	192.168.10.50	DHCP	342	DHCP ACK - Transaction ID 0xa7c7e14b

Abbildung 14: Wireshark - Kommunikation zwischen DHCP-Client und DHCP-Server nach statischer Konfiguration

Da die vorherige Konfiguration mittels DHCPRELEASE zurückgegeben wurde, wird der DHCP-Lease-Vorgang wieder vollständig durchlaufen (vgl. 2.1). Jedoch wird nun die statische Konfiguration angewandt.