Übungsblatt 5 – DNS & DHCP

Aufgabe A – DHCP

Für die statisch gerouteten Netzwerke wurden bis jetzt jedem Rechner manuell IP-Adressen zugeordnet – d.h. die IP-Adressvergabe war statisch. Der Adapter der im Bridge bzw. NAT-Modus unsere Netzwerke mit ihrem Heimnetzwerk verbindet, hatte jedoch i.d.R. DHCP. Im Folgenden betrachten wir DHCP etwas genauer. Gute Anlaufstellen sind [KR12, Kap. 4.4, S. 345ff], [FS11, Kap. 6, S. 233ff], [Koz05, Kap. 60, S. 977ff].

1. Vorbereitend: Recherchieren sie, was eine Client-Server-Architektur ist. Sie müssen lediglich verstehen, wie diese aufgebaut ist.
2. Einleitend:
   a) Auf welcher Schicht des ISO-OSI-Modells würden sie DHCP einordnen?
   b) Welche Standardports nutzt DHCP client- und serverseitig?
   c) Welches Transportschichtprotokoll nutzt DHCP?
   d) Für welches Vermittlungsschichtenprotokoll ist DHCP zuständig?
3. Im wesentlichen besteht DHCP aus zwei Komponenten: dem Adressmanagement (Address-Management) und der Lieferung der Konfigurationsdaten („delivery of configuration data“). Erläutern sie die Aufgabe beider Komponenten.
4. Welche drei Arten der Adressenvergabe kennt DHCP?
5. Erläutern sie den Unterschied zwischen dynamischer und automatischer Adressvergabe via DHCP.
6. BOOTP ist DHCPs Vorgänger, ist aber dennoch fester Bestandteil von DHCP. Welcher Adressvergabetyp in DHCP entspricht BOOTP?
7. DHCP nutzt im wesentlichen das BOOTP Nachrichtenprotokoll. In Abb. 1 ist der Aufbau einer BOOTP-Nachricht dargestellt.

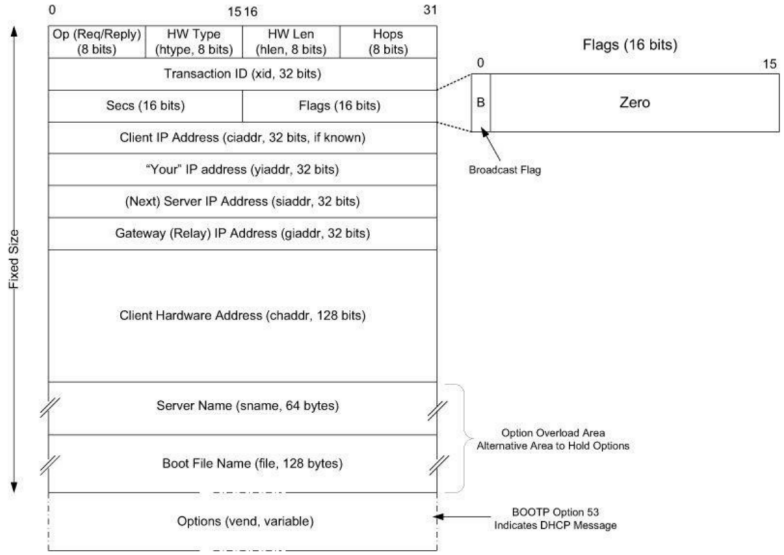

Abbildung 1: BOOTP Nachrichtenformat, entnommen aus [FS11, S. 237].

Beschreiben sie Abb. 1 und notieren sie sich, welchen Zweck die einzelnen Felder haben. Da DHCP nicht BOOTP ist, muss im Nachrichtenformat hinterlegt sein, um welche Art DHCP-Nachricht es sich handelt. Notieren sie sich welches Feld hierfür zuständig ist.

8. Für die dynamische Adressvergabe benötigt DHCP ein *Pool* und eine *Lease*. Erläutern sie kurz beide Begriffe.

9. Wenn sich ein DHCP-Client eine IP-Adresse geben lassen möchte, muss dieser initial mit dem DHCP-Server kommunizieren. In Abb. 2 ist ein typischer Austausch abgebildet.

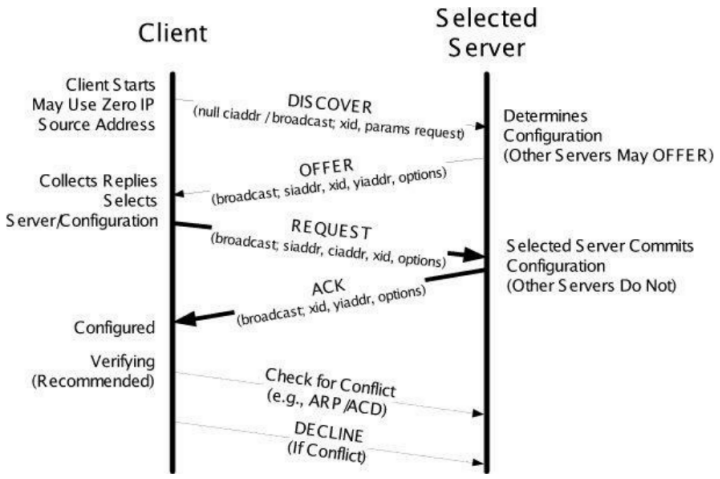

Abbildung 2: Typischer Nachrichtenaustausch zwischen DHCP-Client und Server, entnommen aus [FS11, S. 240].

Beschreiben sie mithilfe der Abbildung, wie ein Client zu einer dynamisch vergebenen IP-Adresse kommt.

10. Was passiert, wenn nach dem *OFFER* oder *REQUEST* die dynamische IP-Adresse nicht vergeben werden konnte?

11. Da DHCP auf der Applikationsebene des ISO-OSI-Modells liegt, wie kann dieses Protokokll dennoch IP-Adressen organisieren? D.h. DHCP kann nicht auf IP-Adressen zurückgreifen. Schlimmer noch, ein Client hat initial gar keine IP-Adresse [1]. Erläutern sie dieses Henne-Ei-Problem.

Aufgabe B – DHCP II

1. DHCP-Adressen werden oft beim Bootvorgang vom Betriebssystem vergeben. Unter `https://www.freebsd.org/doc/de_DE.ISO8859-1/books/handbook/network-dhcp.html` finden sie eine gute Anlaufstelle wie DHCP unter freeBSD organisiert ist.
   a) Wie und wo können sie einen DHCP-Client konfigurieren?
   b) Welche Arten (Modi) stehen ihnen dabei zur Verfügung?
   c) Wie bringen sie in Erfahrung welche IP-Adresse ihr DHCP-Server hat, wie ihre *lease* aussieht?
   d) Wie können sie den Client dazu veranlassen sich eine neue IP-Adresse geben zu lassen?

[1] Wenn ihr Rechner hochfährt hat dieser beim Bootvorgang noch keine IP-Adresse, ihr Rechner kennt nur seine physikalischen Geräte.

2. In welchen Dateien wird ein DHCP-Server unter *freeBSD* organisiert?

3. Nehmen sie aus dem *freeBSD*-Handbuch die exemplarisch gegebene DHCP-Server-Konfigurationsdatei und erläutern sie diese schrittweise.

4. Wie können sie den DHCP-Server unter *freeBSD* starten bzw. stoppen? Wo können sie diesen Dienst persistent hinterlegen? Wie sähe das aus?

1. Auf dem *freeBSD* mit grafischer Oberfläche läuft bereits DHCP für das Interface *em0* im Bridge bzw. NAT-Mode. Dies nutzen wird für den ersten Teil.
   Überprüfen sie, ob der DHCP-Client auf diesem System ordnungsgemäß läuft.

2. Lassen sie sich vom DHCP-Server für das *freeBSD* eine neue IP-Adresse geben. Beobachten sie zeitgleich via Wireshark welche Nachrichten hierfür via BOOTP ausgetauscht werden.
   (a) Wie lautet die Sender-Adresse des DHCP-Client?
   (b) Warum nutzt der DHCP-Cleint seine Sender-Adresse?
   (c) An welche Ziel-IP-Adresse hat der DHCP-Client seine Nachrichten versandt?
   (d) An welche Ziel-MAC-Adresse sendet der DHCP-Client seine Nachrichten?
   (e) An welche Ziel-IP-Adresse hat der DHCP-Server seine Nachrichten versandt?
   (f) An welche Ziel-MAC-Adresse sendet der DHCP-Server seine Nachrichten?
   (g) Welche IP-Adresse wurde dem Client vom Server angeboten?
   (h) Welche Lease-Time wurde durch den DHCP-Server angeboten?
   (i) Welche IP-Adresse wählte und sendete der Client für die Antworten des DHCP-Servers?
   (j) Welcher IP-Adresse bestätigte (acknowledges) der DHCP-Server dem DHCP-Client?

3. Zeichen sie ein Sequenzdiagramm der IP-Adressvergabe die sie via Wireshark aufgezeichnet haben.

Aufgabe C – DNS I

Literatur: Gute Anlaufstellen sind [KR12, Kap. 2.5, S. 130ff], [FS11, Kap. 11, S. 511ff], [Koz05, Kap. 50, S. 825ff]. Das Domain Name System ist ein dezentrales System (verteilte Datenbank nach der Client-Server-Architektur), dessen primäre Aufgabe die Adressauflösung von Domain Name(n) zu IP-Adresse(n) ist.

1. DNS 101 – Grundsätzliches zu DNS
   Schauen sie folgendes Video: `https://youtu.be/XondVs0hJ8U`
   a) Beschreiben sie mit eigenen Worten, was das DNS leistet.

2. Nennen und Erklären sie die folgenden Komponenten des DNS-Systems.
   a) Was wird unter dem Begriff Resolver verstanden?
   b) Was ist ein DNS-Root-Server, was ist ein Top-Level-Domain-Server (TLD) und was ein Second-Level-Domain-Server?
   c) Was ist ein *Stub* im Kontext von DNS?
   d) Was ist ein Bind-Server?
   e) Was ist mit dem Begriff *Zone* gemeint?
   f) Was wird unter dem Begriff Record-Type verstanden?
   g) Was wird unter dem Begriff Authoritative-Name-Server verstanden?

3. Rechner können die unterschiedlichsten Dienste bereitstellen, auf einem Rechner laufen zumeist mehrere Dienste. Entsprechend gibt es diverse DNS-Record-Types die dies realisieren.
   Recherchieren sie welche Typen von Records es gibt.

4. Erläutern sie die Auflösung einer DNS-Anfrage.
   a) Welche beiden Möglichkeiten einer Namensauflösung gibt es? D.h. welche Variante gibt einen Namen aufzulösen.
   b) Wie erfolgt die jeweilige Auflösung eines DNS-Requests?
   c) Verdeutlichen sie sich anhand eines Beispiels, wie ein DNS-Request bearbeitet wird.
   d) In der Praxis wird eine Mischung aus den beiden obrigen Verfahren angewandt. Recherchieren sie, wie diese Auflösung „in the wild“ aussieht.

5. Durchlaufen sie folgende Tutorials:
   - https://www.madboa.com/geek/dig/

   Notieren sie sich wie vorgegangen wird! Diese Tools nutzen Sie in der nächsten Laborübung.

Aufgabe D – DNS II

1. Namensauflösung am praktischen Beispiel.

Tabelle 1: Adressen für DNS-Auflösung.

	Bob	Alice
IP address:	192.45.56.127	208.115.92.45
Local name server:	192.47.56.2	208.115.92.2
SMTP server:	mail.server.org	mail.server.org
Email Address:	bob@realword.org	alice@wonderland.org

a) Nehmen sie an Bob möchte eine E-Mail an Alice senden. Um eine Verbindung mit dem SMTP-Server aufzubauen, muss der Name des Servers via DNS in eine IP-Adresse aufgelöst werden. Erläutern Sie welche Nachrichten ausgetauscht werden müssen und zwischen welchen Hosts. Die Auflösung des Domainnamen ist rein rekursive.
Nehmen Sie weiter an, dass nur der Nameserver der für die Domäne server.org zuständig ist, die Anfrage beantworten kann. (Alle Adressen sind in Tabelle 1 zu sehen!) Skizzieren Sie den Ablauf der Namensauflösung!

b) Nun ist Alice am Zug um Bob zu antworten. Erläutern Sie den Nachrichtenaustausch, wenn eine rein iterative Namensauflösung genutzt wird. Nehmen Sie wie in der vorigen Aufgabe an, dass das nur der Namensserver der zuständig für die Domäne server.org die Anfrage beantworten kann. Skizzieren Sie den Ablauf der Namensauflösung!

c) Erläutern Sie, wie Bobs SMTP-Server den für Alice verantwortlichen Mail-Transfer-Agent (MTA) findet.

Aufgabe E – DNS III

Eine erste Anlaufstelle rund um das Domain Name System ist auch hier das *freeBSD*-Handbuch: https://www.freebsd.org/doc/de_DE.ISO8859-1/books/handbook/network-dns.html

1. Die Werkzeuge *drill* und *dig* können für die Abfrage von DNS-Records genutzt werden.
   a) Wie kann jeweils eine Domain in eine dazugehörige IP aufgelöst werden?
   b) Wie kann ein spezieller Record-Type einer Domäne abgefragt werden?
   c) Wie kann statt des Standardservers ein spezieller DNS-Server angegeben werden? Warum sollte dies notwendig oder möglich sein?
   d) Wie kann ein *Reverse-Lookup* vorgenommen werden?
2. DNS-Server:
   a) Welche Softwarekomponenten benötigen sie, wenn sie einen DNS-Server für eine eigene Zone aufsetzen möchten?
   b) In der Vorlesung gibt es bereits Beispiele, wie eine *Zone*-Datei aussehen muss. Erläutern sie, was dort vermerkt ist.
   c) Welche Aufgabe hat der Daemon *named*? Wo wird dieser konfiguriert und administriert?
   d) Bei der *named*-Konfiguration gibt es die Möglichkeit Master als auch Slave zu konfigurieren. Erläutern sie den Unterschied zwischen beiden Möglichkeiten. Können auch mehrere Master existieren?

Aufgabe F – Praxis Domain Name System (DNS)

1. DNS-Requests:
   (a) Fragen sie mit jedem der Kommando der Hausaufgaben jeweils einmal einen Hostnamen (bspw. `www.htw-berlin.de`), einen Domainnamen (htw-berlin.de) und eine IP-Adresse (bspw. 141.45.5.100) ab.
   (b) Schauen sie sich die Ausgabe von *dig* bei der Abfrage der IP-Adresse genauer an – dort werden sie in der „Question Section“ sehen, dass nach dem A-Resource-Record mit dem Namen 141.45.5.100 gefragt wurde. Wenn Sie den Namen zu dieser IP-Adresse suchen – welchen Resource-Record müssen sie anstelle des A-Records erfragen?
   (c) In welcher Form müssen sie dann die IP-Adresse angeben? (Test mit `dig -t <record-type> <richtiges-format-ip-adresse>`).
   (d) Denken sie sich einen Domainnamen aus, den es wahrscheinlich geben könnte, welcher aber in den letzten Stunden nicht aufgelöst worden ist. Erfragen sie diesen Namen zweimal kurz hintereinander via *dig* und vergleichen sie die beiden Ausgaben. Worin unterscheiden sich beide Einträge? Falls eine größere zeitliche Differenz vorhanden ist, worin liegt die Ursache?
   (e) Erfragen sie mit *dig* und *nslookup* den zuständigen Mail-Server für die Domain `htw-berlin.de`.
   (f) Erzwingen sie mit *dig* und *nslookup* eine Namensauflösung ohne den Standard-DNS-Server des Betriebssystems, sondern mit einem öffentlichen Nameserver (bspw.: 9.9.9.9) erfolgt. Testen sie dies am Besten zuerst mit *dig*, da dieses Werkzeug immer den genutzten Namensserver angibt.
2. DNS-Resolver: Das Listing zeigt die „resolv.conf“ eines Servers.

```
1 nameserver 141.45.3.100
2 search f4.htw—berlin.de
```

   Was bedeuten die Einträge mit den Schlüsselwörtern: „nameserver“ und „search“?

Literatur

[FS11] Kevin R. Fall und Richard W. Stevens. *TCP/IP illustrated, volume 1: The protocols*. addison-Wesley, 2011.

[Koz05] Charles M. Kozierok. „The TCP/IP Guide: A Comprehensive“. In: *Illustrated Internet Protocols Reference* (2005).

[KR12] James F. Kurose und Keith W. Ross. *Computer Networking: A Top-Down Approach (6th Edition)*. 6th. Pearson, 2012. ISBN: 0132856204, 9780132856201.