



Übungsblatt 4

2019-05-16

Abgabe: 2019-05-23, 10:00. **elektronische Abgabe als PDF-Datei über Moodle!**

Aufgabe 4.1: Hands-on: Dynamic Host Configuration Protocol

Sie haben in der letzten Übung das Tool *Wireshark* (<https://www.wireshark.org/>) kennengelernt. In dieser Übung werden Sie das DHCP Protokoll genauer untersuchen.

1. Wozu wird DHCP eingesetzt? Erklären Sie den Unterschied zu RARP! 5 Punkte
2. Was ist der Vorteil von DHCP gegenüber RARP? 5 Punkte

Damit Sie den Verlauf von DHCP mit *Wireshark* untersuchen können, müssen Sie den DHCP-Ablauf auf Ihrem Gerät starten. Führen Sie dazu die folgenden Schritte aus:

- **OS X:** `sudo ipconfig set <interface> DHCP`
- **Windows:** `ipconfig /release <adapter> && ipconfig /renew <adapter>`
- **Linux:** `sudo dhclient -r <interface> && sudo dhclient <interface>`

Zeichnen Sie die dadurch entstandene DHCP Kommunikation auf.

3. Beschreiben Sie auf Grundlage der aufgezeichneten Kommunikation den Ablauf von DHCP! Gehen Sie dabei auf die relevanten Felder der DHCP-Nachrichten ein! 10 Punkte

Aufgabe 4.2: ICMP

Das Internet Control Message Protocol (ICMP) dient zur Übermittlung von Kontrollinformationen und Fehlermeldungen. Das Auslösen von ICMP-Fehlermeldungen wird von manchen Tools und Mechanismen gezielt eingesetzt um Informationen über das Netzwerk zu ermitteln. Beantworten Sie die folgenden Fragen und geben Sie dabei alle Quellen außerhalb der Vorlesungsfolien an!

1. Recherchieren Sie die Funktionsweise von Traceroute! Beschreiben Sie den Ablauf und die Rolle von ICMP in eigenen Worten! 5 Punkte
2. Recherchieren Sie die Funktionsweise von Path MTU Discovery. Beschreiben Sie den Ablauf und die Rolle von ICMP in eigenen Worten! 10 Punkte
3. Wie kann der Empfänger einer ICMP-Nachricht feststellen, auf welches Paket sich die Fehlermeldung bezieht? 5 Punkte

Aufgabe 4.3: IPv6-Adressen

Sie haben in der Vorlesung verschiedene Arten von IPv6-Adressen kennengelernt sowie verschiedene Arten diese zu konfigurieren.

1. Woran erkennen Sie, ob eine per SLAAC generierte link-local IPv6-Adresse von einer MAC-Adresse abgeleitet wurde? 5 Punkte
2. Wie wird mit SLAAC aus einer link-local eine globale IPv6-Adresse? 5 Punkte
3. Wieso wurde die *Privacy Extension* für SLAAC eingeführt? 5 Punkte
4. Wozu wird DAD im Kontext von SLAAC benötigt? 5 Punkte

Hinweis:

Für ein besseres Verständnis von SLAAC und der IPv6 Privacy Extensions können Sie in

- <https://www.elektronik-kompodium.de/sites/net/1601271.htm>
- <https://www.elektronik-kompodium.de/sites/net/1902131.htm>

nachlesen.

Aufgabe 4.4: IP-Multicast

1. Was ist IP-Multicast? Nennen Sie ein Anwendungsgebiet für IP-Multicast! 5 Punkte
2. Wie können Endgeräte Multicast-Gruppen beitreten? Erklären Sie anhand eines Beispiels den Ablauf einer Multicast-Anwendung! 10 Punkte
3. Was ist der Unterschied zwischen mehrfachem IP-Unicast und echtem IP-Multicast? Quantifizieren Sie diesen Unterschied in Bezug auf die Netzauslastung an einem Beispiel! 10 Punkte
4. Ändert ein Host seine IP-Adresse zu der Adresse der Multicast-Gruppe, wenn er dieser beitrifft? Begründen Sie Ihre Antwort! 5 Punkte

Für IP-Multicast müssen sogenannte Multicast-Bäume erstellt werden, die den Verlauf des Traffics angeben. Für Multicast-Routing gibt es zwei weitverbreitete Verfahren: **Source-Based Trees** und **Group-Shared Trees**.

5. Erklären Sie den Unterschied zwischen Source-Based Trees und Group-Shared Trees! 5 Punkte
6. Welches Verfahren benötigt mehr Zustand/Informationen in den Routern? Quantifizieren Sie das Verhältnis! 5 Punkte

Gesamt: 100 Punkte