

Praktikumsblatt 3 - Netze

- Kommunikation mit IPv4 –

Lange Zeit war IPv4 praktisch das einzige Protokoll der Netzwerkschicht. Deshalb wird es landläufig auch einfach IP genannt. Trotz der allmählichen Verbreitung von IPv6 ist IPv4 nach wie vor in vielen Netzen präsent. In diesem Praktikumsblatt sollen Sie sich mit den grundlegenden Eigenschaften und der Funktionsweise einer IPv4-Kommunikation vertraut machen.

Aufgabe 1: IPv4-Netzparameter

Damit ein Rechner (Client) im Internet kommunizieren kann, benötigt er von vornherein bestimmte Netzparameter, die er in der Regel über Autokonfiguration beim Booten erhält. Zur besseren Orientierung bei den folgenden Aufgaben, ermitteln Sie zunächst für Ihren Rechner die vorliegenden IPv4-Netzparameter

Netz-Adresse:
Subnetzmaske:
IPv4-Adresse:
Broadcast-Adresse:
Standard-Gateway:
DNS-Server:

Hinweis-1: Als Standard-Gateway wird der zuständige Router eines Netzwerkes bezeichnet, der die Pakete aus einem lokalen Netzwerk weiter in andere Netzwerke (wie z.B. ins Internet) leitet. Ohne Router würde das Netz eine Insel ohne Anbindung an die „Außenwelt“ sein. Den Router können Sie über die Routing-Tabelle des Rechners abfragen (Eintrag zur sogenannten Default-Route):

```
ip -4 route
```

Hinweis-2: Der DNS-Server steht bei Linux in der Datei /etc/resolv.conf. Mit dem Befehl cat lässt sich der Inhalt einer Datei ausgeben, also

```
cat /etc/resolv.conf
```

Aufgabe 2: Autokonfiguration mit DHCP

Um den Aufwand einer manuellen Konfiguration für eine Vielzahl von Rechner sowie der sich anschließenden Pflege zu vermeiden, werden Protokolle wie DHCP (Dynamic Host Configuration Protocol; RFC 2132 und RFC 2131) eingesetzt, die den Konfigurationsprozess im Sinne eines Plug-and-Play-Networkings automatisieren.

- (a) Überlegen Sie sich zunächst, wie Sie vorgehen müssen, um DHCP-Pakete beim Booten Ihres Rechners mit Wireshark aufzeichnen können.
- (b) Schneiden Sie den DHCP-Vorgang mit Wireshark mit.
- (c) Beschreiben Sie den DHCP-Kommunikationsablauf mit Hilfe eines Sequenzdiagramms. Geben Sie für jede Kommunikationsequenz die Protokollnachricht und die jeweiligen Adressen für beide Schichten (2 und 3) an. Welcher Kommunikationstyp (Broadcast/ Multicast/ Unicast) liegt dabei jeweils vor?
- (d) Welche Netzparameter beziehen die Rechner über DHCP?
- (e) Auf welcher Schicht befindet sich DHCP?

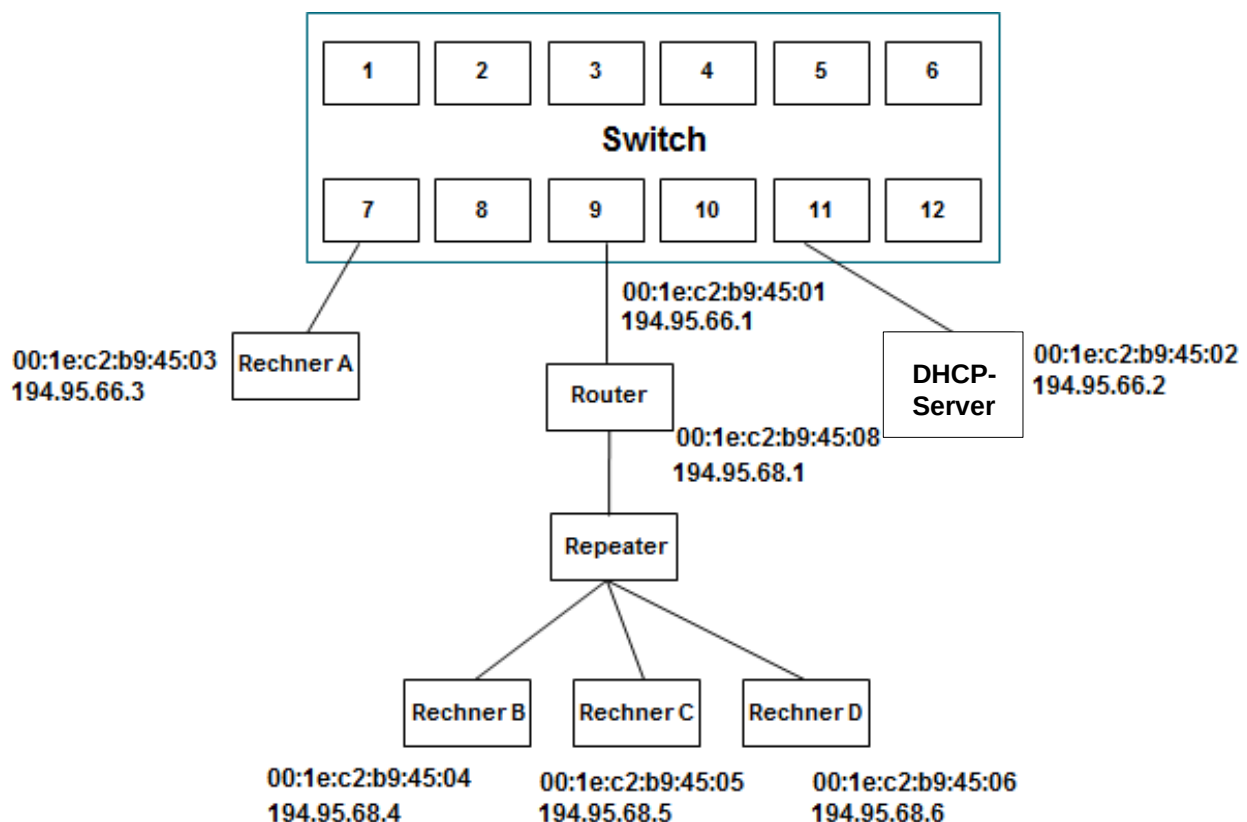
Aufgabe 3: IPv4-Kommunikation und ARP

Wenn Sie Daten zu einem Rechner senden möchten, dann adressieren Sie diesen Rechner über dessen IP-Adresse. Doch in dem Augenblick, wenn das IP-Paket der Leitungsschicht übergeben wird, wird eine MAC-Adresse benötigt. Da die MAC-Adresse des Empfänger-Rechners unbekannt ist und auch auf Grund der Struktur der IP-Adresse keinerlei Rückschlüsse auf die zugehörige MAC-Adresse gezogen werden kann, ist ein Verfahren notwendig, dass die Zuordnung einer gegebenen IP-Adresse zu der jeweiligen MAC-Adresse vornimmt. Genau das ist die Aufgabe von ARP (Address Resolution Protocols, RFC 826).

- (a) Was ist ein LAN? Und wer befindet sich mit Ihnen in einem LAN?
- (b) Führen Sie einen ping auf einen Rechner in Ihrem LAN aus.
- (c) Schauen Sie sich nun über den Befehl
`ip -4 neigh`

Ihren Neighbor-Cache an. Damit das ARP-Protokoll effizient arbeitet, verfügt jeder Rechner über einen Cache-Speicher (Neighbor-Cache), in dem er einmal angefragte IP-MAC-Adressenzuordnungen ablegt, um wiederholende ARP-Anfragen zu vermeiden.

- (d) Löschen Sie anschließend mit dem Befehl `sudo ip -4 neigh flush all` (Passwort netlab) alle Einträge im Cache.
- (e) Starten Sie Wireshark. Wählen Sie unter dem Menüpunkt „Aufzeichnen“ den Punkt „Optionen“ aus und deaktivieren Sie die „MAC-Adressen auflösen“ unter dem Register Optionen. Starten Sie das Capture und führen Sie wieder einen ping über IPv4 auf einen Rechner (nicht das Standard-Gateway) **im lokalen Netzwerk** (10.30.0.x) aus. Welche Einträge liegen nun im Neighbor-Cache Ihres Rechners vor?
- (f) Beschreiben Sie mit Hilfe eines Sequenzdiagramms den Ablauf der Kommunikation (ARP + ping) und analysieren Sie die zugehörigen Pakete mit den jeweiligen Sender- und Empfängeradressen sowohl auf Schicht 2 als auch auf Schicht 3.
- (g) Prüfen Sie, ob Rechner im selben LAN, die nicht explizit an einer Kommunikation beteiligt sind, auch Einträge im Neighbor-Cache vornehmen.
- (h) Löschen Sie wiederum den Neighbor-Cache Ihres Rechners und starten Sie die Capture-Funktion des Wiresharks. Führen Sie einen ping auf die IP-Adresse 194.95.66.105 aus (Rechner im Netzlabor C015). Welche IP-Adresse liegt nun in Ihrem Cache vor? Beschreiben Sie im Detail den Ablauf der ARP-Kommunikation und analysieren Sie die zugehörigen Pakete.
- (i) Gegeben sei folgendes Szenario:



Alle Neighbor-Caches und die Adresstabelle des Switches weisen keine Einträge auf. Rechner A bootet und möchte danach ein ping-Paket an Rechner C senden.

Beschreiben Sie im Detail die DHCP- und die anschließende ping-Kommunikation sowie die jeweiligen ARP-Kommunikationen.

- Wer hat welche Einträge im Cache vorliegen?
- Wie sieht die Adresstabelle des Switches aus

- (j) **Zusatzaufgabe:** Ändern Sie die IP-Adresse Ihres Interfaces zu einer bereits im Netz befindlichen IP-Adresse ab:

Löschen Sie hierfür zuerst die bestehende IP-Adresse mit dem Befehl
`sudo ip addr del <ip-adresse>/<subnetzpräfix> dev <interface>`
z.B. `sudo ip addr del 10.30.0.104/24 dev eth0`

Fügen Sie anschließend eine bereits im lokalen Netz vorhandene Adresse hinzu
`sudo ip addr add <ip-adresse>/<subnetzpräfix> dev <interface>`
z.B. `sudo ip addr add 10.30.0.122/24 dev eth0`

Testen Sie, welche Auswirkungen die Mehrfachbelegung einer IP-Adressen in einem LAN hat. Wie verläuft dann die Kommunikation? Starten Sie nach dem Versuch Ihren Rechner neu.

- (k) **Zusatzaufgabe:** Welche Sicherheitsangriffe sind in einem Netzwerk mit Hilfe des ARP-Protokolls denkbar? Beschreiben Sie den genauen Ablauf eines solchen Angriffs und überlegen Sie sich Maßnahmen, um Angriffe dieser Art zu vermeiden.

Aufgabe 4

Wie sieht Ihre IPv4-Konfiguration zu Hause aus?

Viel Spaß und Erfolg!