Praktikumsblatt 2 - Netze

- Kommunikation mit IPv4 -

Bis vor Kurzem 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 allen Netzen präsent. In diesem Praktikumsblatt sollen Sie sich mit den grundlegenden Eigenschaften und der Funktionsweise einer IPv4-Kommunikation vertraut machen.

Address Resolution Protocol (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. Eine Möglichkeit wäre, dass jede Station eine Liste mit IP-Adressen und zugehörigen MAC-Adressen erhält. Wird zu einer gegebenen IP-Adresse die MAC-Adresse benötigt, muss die Station nur nach dem entsprechenden Eintrag in der Liste suchen. Das Anlegen und vor allem das Pflegen einer solchen Liste für jede Station würde jedoch einen sehr hohen Aufwand für den Systemadministrator bedeuten: jede Änderung einer IP-Adresse, jeder Austausch einer Netzwerkkarte (bedeutet: neue MAC-Adresse) und jede neue Station würden eine Aktualisierung der Liste nach sich ziehen.
Im Prinzip funktioniert die Adressumsetzung mit Hilfe des Address Resolution Protocols (ARP; RFC 826) gleichermaßen, jedoch werden hier die Zuordnungen der Adressen automatisch und dynamisch vorgenommen.

(a) Damit das ARP-Protokoll effizient arbeitet, verfügt jeder Rechner über einen Cache-Speicher (ARP-Cache) mit IP-an-MAC-Adressenzuordnungen, um wiederholende ARP-Anfragen zu vermeiden. Führen Sie über die Konsole den Befehl `arp –n` aus und interpretieren Sie vorhandene Einträge.

Hinweis: Wenn Sie Ihren ARP-Cache laufend abfragen möchten, starten Sie ein neues Konsolenfenster und geben den folgenden Befehl ein:

```
watch -n 1 arp -n
```

(b) Löschen Sie anschließend mit dem Befehl `sudo ip -4 neigh flush all` (Passwort netlab) alle Einträge im Cache.

(c) 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 einen `ping` auf einen Rechner (nicht das Gateway) **im lokalen Netzwerk** (10.30.0.x) aus. Welche Einträge liegen nun im ARP-Cache Ihres Rechners vor?

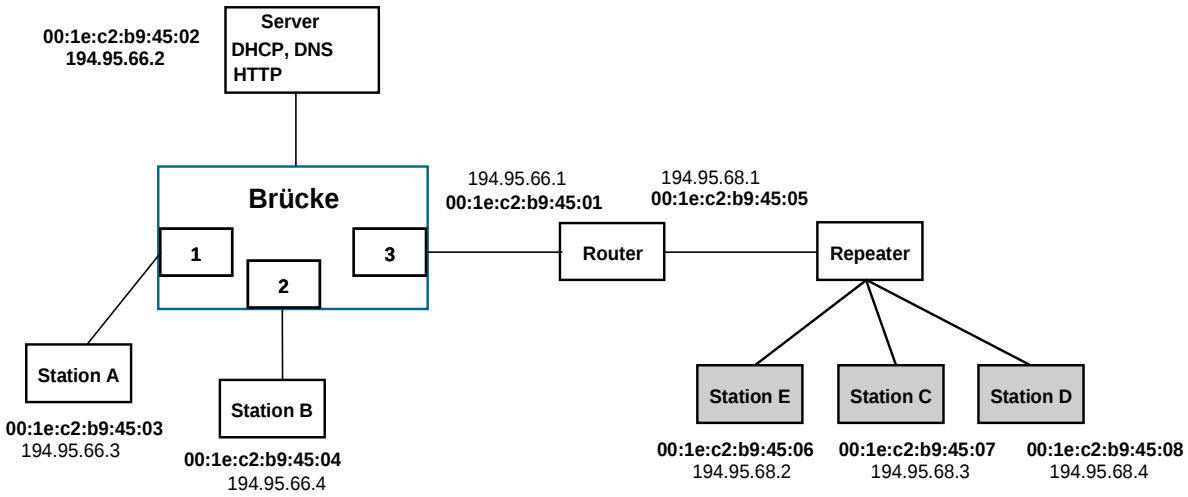
(d) Prüfen Sie, ob Rechner im selben LAN, die nicht explizit an einer Kommunikation beteiligt sind, auch Einträge im ARP-Cache vornehmen.

(e) Testen Sie, wie lange Einträge in Ihrem ARP-Cache vorgehalten werden? Ist das Ergebnis aus Ihrer Sicht sinnvoll? Begründen Sie Ihre Antwort.

(f) Ändern Sie nun die IP-Adresse Ihres Interfaces zu einer bereits im Netz befindlichen IP-Adresse ab (nutzen Sie hierzu eine IP-Adresse die größer als 10.30.0.100). Verwenden Sie hierzu den Befehl
`sudo ifconfig <interface> <ip-adresse> netmask <subnetzmaske>`
Testen Sie, welche Auswirkungen die Mehrfachbelegung einer IP-Adressen in einem LAN hat. Starten Sie nach dem Versuch Ihren Rechner neu.

(g) Löschen Sie wiederum den ARP-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 in C015). Beschreiben Sie im Detail den Ablauf der Kommunikation und analysieren Sie die zugehörigen Pakete.

(h) Gegeben sei folgendes Szenario:



Die ARP-Caches aller Stationen und der des Routers weisen keine Einträge auf. Station A möchte nun ein Paket an Station C senden.

Beschreiben Sie die hierzu notwendigen Kommunikationsschritte, damit Station A das Datenpaket an Station C senden kann. Welche Stationen/Netzkomponenten erhalten die ARP-Antwort von Station C?

(i) 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.

(j) Abschließend starten Sie ein Capture und rufen über Firefox die Webseite von Spiegel (www.spiegel.de) auf. Stellen Sie dar, wie die verschiedenen Adressen (DNS-Name, IP-Adresse, MAC-Adresse) aufeinander abgebildet werden.

Viel Spaß und Erfolg!