Moritz Hahn
Sarah Altenkrüger

| 1 | 2 | 3 | Σ |
|---|---|---|---|
| | | | |

# Übungsblatt Nr. 3

(Abgabetermin 13.05.2024)

## Aufgabe 3.1

Tabelle 1: R1

| Prefix | Gateway | Interface |
|---|---|---|
| 10.0.8/21 | 134.2.0.2 | IF0 |
| 10/8 | 134.2.0.3 | IF0 |
| 0/0 | 134.2.255.254 | IF1 |

Tabelle 2: R2

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 134.2.0.1 | IF0 |
| 10/8 | 134.2.0.3 | IF0 |
| 0/0 | 134.2.255.254 | IF1 |

Tabelle 3: R3

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 134.2.0.1 | IF0 |
| 10.0.8/21 | 134.2.0.2 | IF0 |
| 0/0 | 134.2.255.254 | IF1 |

Tabelle 4: A

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 192.168.0.254 | IF0 |
| 10.0.8/21 | 192.168.0.254 | IF0 |
| 10/8 | 192.168.0.254 | IF0 |
| 0/0 | 192.168.0.254 | IF1 |

Tabelle 5: B

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 192.168.0.254 | IF0 |
| 10.0.8/21 | 192.168.0.254 | IF0 |
| 10/8 | 192.168.0.254 | IF0 |
| 0/0 | 192.168.0.254 | IF1 |

Tabelle 6: C

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 10.0.8.1 | IF0 |
| 10.0.8/21 | 10.0.8.1 | IF0 |
| 10/8 | 10.0.8.1 | IF0 |
| 0/0 | 10.0.8.1 | IF1 |

Tabelle 7: D

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 10.0.8.1 | IF0 |
| 10.0.8/21 | 10.0.8.1 | IF0 |
| 10/8 | 10.0.8.1 | IF0 |
| 0/0 | 10.0.8.1 | IF1 |

Tabelle 8: E

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 10.0.0.254 | IF0 |
| 10.0.8/21 | 10.0.0.254 | IF0 |
| 10/8 | 10.0.0.254 | IF0 |
| 0/0 | 10.0.0.254 | IF1 |

Tabelle 9: F

| Prefix | Gateway | Interface |
|---|---|---|
| 192.168.0/24 | 10.0.0.254 | IF0 |
| 10.0.8/21 | 10.0.0.254 | IF0 |
| 10/8 | 10.0.0.254 | IF0 |
| 0/0 | 10.0.0.254 | IF1 |

# Aufgabe 3.2

## 1.)

Nein, da nur bei einer übertragung von Host B zu Host A nie die Maximale Packet größe erreicht werden kann, da die MTU von Host B kleiner ist als Die MTU des WIFI's.
Bei der Übertragung von Host A zu Host B, kann die maximale MTU des WIFI's überschritten werden, da die MTU von Host a größer als die MTU des WIFI's ist. Somit muss das Packet fragmentiert werden

## 2.)

Tabelle 10: Fragmentierungstabelle

| Fragment Nummer | Payload | Fragmentlänge | Fragment Offset | MF-Bit |
|---|---|---|---|---|
| 1 | 1480 | 1500 | 0 | 1 |
| 2 | 1480 | 1500 | 185 | 1 |
| 3 | 1480 | 1500 | 370 | 1 |
| 4 | 912 | 944 | 555 | 0 |

## 3.)

Die Verwendung des Fragment Offsets anstelle einer Fragment-Nummer zur Identifizierung der einzelnen Fragmente bietet mehrere Vorteile:

1. **Flexibilität bei der Reihenfolge:** Da Fragmentierung nicht garantiert in der gleichen Reihenfolge erfolgt, wie das ursprüngliche Paket aufgeteilt wurde, ermöglicht der Fragment Offset die ordnungsgemäße Rekonstruktion des Pakets, unabhängig von der Reihenfolge, in der die Fragmente empfangen werden. Dies bedeutet, dass Fragmente in beliebiger Reihenfolge empfangen werden können, solange der Fragment Offset korrekt ist.

2. **Effizienz bei der Pufferung:** Wenn Fragmente eines Pakets durch das Netzwerk geleitet werden, können sie in verschiedenen Routern unterschiedliche Wege nehmen und daher in unterschiedlicher Reihenfolge ankommen. Durch die Verwendung des Fragment Offsets anstelle einer festen Fragment-Nummer können Router und Empfänger effizienter Puffer verwenden, da die Fragmente nicht zwangsläufig in aufsteigender Reihenfolge angekommen müssen, um korrekt verarbeitet zu werden.

# Aufgabe 3.3

## 1.)

Ein ARP-Request besteht aus den folgenden Feldern:

- Hardwaretyp: Gibt den Typ der verwendeten Hardware an (z.B. Ethernet).
- Protokolltyp: Gibt den Typ des verwendeten Netzwerkprotokolls an (z.B. IPv4).
- Hardwareadresslänge: Gibt die Länge der Hardwareadresse an (z.B. für Ethernet 6 Bytes).

- Protokolladresslänge: Gibt die Länge der Protokolladresse an (z.B. für IPv4 4 Bytes).
- Operation: Gibt an, ob es sich um eine Anfrage (Request) oder eine Antwort (Reply) handelt.
- Absender-Hardwareadresse: Die MAC-Adresse des Absenders.
- Absender-Protokolladresse: Die IP-Adresse des Absenders.
- Ziel-Hardwareadresse: In einem ARP-Request ist dies oft die Broadcast-Adresse (alle Geräte im Netzwerk), da der Absender die Hardwareadresse eines bestimmten Ziels anfordert.
- Ziel-Protokolladresse: Die IP-Adresse des Ziels, dessen Hardwareadresse angefragt wird.

## 2.)

Ein ARP-Reply hat die gleichen Felder wie ein ARP-Request, aber die Operation gibt an, dass es sich um eine Antwort handelt. Die Absender-Hardwareadresse und -Protokolladresse sind die des antwortenden Geräts, während die Ziel-Hardwareadresse die des Anfragenden ist und die Ziel-Protokolladresse die des Absenders des ursprünglichen ARP-Requests ist.

## 3.)

ARP-Requests werden normalerweise mit einer Broadcast-Zieladresse gesendet, damit alle Geräte im Netzwerk sie empfangen können. ARP-Replies werden dagegen an die spezifische MAC-Adresse des anfragenden Geräts gesendet, die im ARP-Request enthalten ist. Dies reduziert die Netzwerklast und sorgt dafür, dass nur das anfragende Gerät die Antwort empfängt.

## 4.)

ARP ist anfällig für verschiedene Arten von Angriffen wie ARP Spoofing oder ARP Poisoning, bei denen ein Angreifer ARP-Pakete manipuliert, um falsche Zuordnungen zwischen IP-Adressen und MAC-Adressen vorzutäuschen. Dies kann zu Man-in-the-Middle-Angriffen führen, bei denen ein Angreifer den Datenverkehr zwischen zwei Kommunikationspartnern abhört oder sogar manipuliert. Daher kann die Funktionsweise von ARP ein Sicherheitsrisiko darstellen, insbesondere in ungesicherten Netzwerken.

## 5.)

Nein, C muss keinen eigenen ARP-Request verschicken. Wenn A einen ARP-Request an B sendet, um dessen MAC-Adresse zu ermitteln, wird dieser Request von allen Hosts im Netzwerk gehört, einschließlich C. Dadurch wird die ARP-Tabelle von C automatisch aktualisiert, sodass C die MAC-Adresse von A kennt, sobald der ARP-Request und die entsprechende Antwort empfangen wurden. Daher muss C keinen eigenen ARP-Request senden, um mit A zu kommunizieren.

## 6.)

Um den angestrebten Paketversand sowohl für A als auch für C zu ermöglichen, müssen mindestens zwei ARP-Pakete verschickt werden:

- A sendet einen ARP-Request, um die MAC-Adresse von B zu ermitteln.
- B antwortet mit einem ARP-Reply und sendet seine MAC-Adresse an A.
- C hört den ARP-Request und erhält dadurch auch die MAC-Adresse von A, ohne einen eigenen ARP-Request senden zu müssen.