Tutoriumsblatt 6

Diskussion: 15. + 16. sowie 22. + 23. Juni 2021

Aufgabe 6.1: IP-Adressen und CIDR

a) Sie haben die IP-Adressen 137.226.12.221 und 137.234.17.222 gegeben. Wie ist die *Subnetzmaske* zu wählen, damit *beide Rechner im gleichen Netz* liegen, das Netz allerdings *so klein wie möglich* ist?

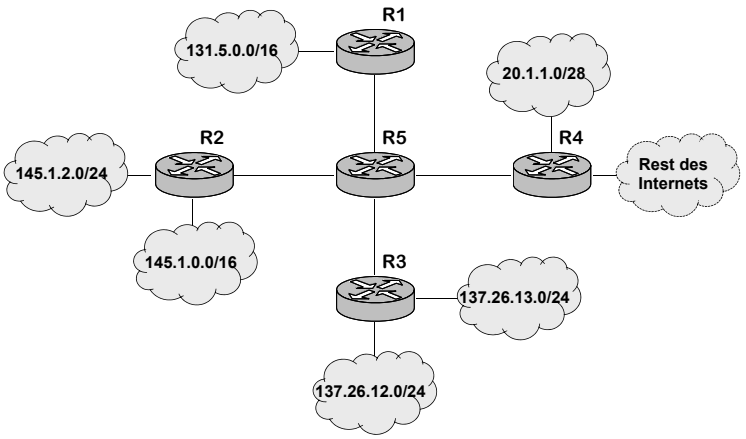
b) Es ist eine große Anzahl an aufeinander folgenden IP-Adressen verfügbar, die bei 137.226.0.0 beginnen. Angenommen, vier Organisationen W, X, Y, Z fordern in der folgenden Reihenfolge Adressbereiche für ihre Rechner an:

- W für 3990 Rechner
- X für 2020 Rechner
- Y für 4096 Rechner
- Z für 1853 Rechner

Vergeben wird jeweils die niedrigstmögliche Netzadresse. *Geben Sie für jede Organisation die zugewiesene Netzadresse mit Netzmaske an.* Geben Sie darüber hinaus jeweils an, welches die *erste und welches die letzte IP-Adresse* aus dem zugewiesenen IP-Adressbereich ist.

c) Angenommen, es würde klassenbasierte IP-Adressierung ohne Subnetzmasken verwendet. *Wie viele Einträge* müsste ein Router in seiner Routing-Tabelle vorhalten, damit er Daten an alle möglichen Zieladressen weiterleiten könnte?

d) Betrachten Sie den folgenden Netzaufbau, in dem die Router $R1$ - $R4$ jeweils ein oder zwei Netze verwalten. Der genaue Aufbau dieser Netze ist uninteressant – aber die Router $R1$ - $R4$ kennen die Adressbereiche der an sie angeschlossenen Netze. Lediglich Router $R4$ verfügt über eine Verbindung zum Rest des Internets. Sie haben nun den Router $R5$ installiert, um die Netze miteinander und mit dem Internet zu verbinden und müssen eine Routing-Tabelle erstellen. Geben Sie für Router R5 eine Routing-Tabelle mit so wenig Einträgen wie möglich an, damit alle Daten korrekt zwischen den Netzen (und dem Rest des Internets) weitergeleitet werden. Beschränken Sie sich bei der Tabelle auf Einträge der Form `Zielnetz, Next Hop`. `Next Hop` ist dabei einer der Router $R1$ - $R4$. Angaben wie Flags, Netzwerkkarten-Adressen oder weiteres sind hier nicht von Interesse.



Aufgabe 6.2: Network Address Translation (NAT)

NAT ist eine Möglichkeit, mit der Knappheit von IP-Adressen umzugehen.

a) Beschreiben Sie das *Prinzip von NAT*. Machen Sie dabei klar, ob durch dieses Prinzip irgendwelche *Vor- oder Nachteile* bei der Kommunikation zwischen Ihren eigenen Rechnern bzw. bei der Kommunikation Ihrer Rechner mit externen Rechnern entstehen.

b) Wie ändert sich die Situation durch die Einführung von *IPv6*?

Aufgabe 6.3: IP-Pakete und Fragmentierung

a) IP kann Pakete fragmentieren, um sie an die MTU (Maximum Transfer Unit) des auf der Sicherungsschicht verwendeten Protokolls anzupassen. Ebenso kann es die Fragmente zum ursprünglichen Paket zusammenfügen – allerdings erst beim Zielrechner. *Warum ist es sinnvoll, fragmentierte Pakete nicht schon in den zwischenliegenden Routern wieder zusammenzusetzen?*

b) Mittels IPv4 sollen 1690 Byte Nutzdaten verschickt werden. Die sendende IP-Instanz erzeugt aus diesen Daten ein Paket, indem sie den Standard-Header hinzugefügt; Optionen werden nicht verwendet. Zu versendende Pakete werden auf der Sicherungsschicht in Rahmen mit einem Header von 16 Byte Länge und einem Trailer (Prüfsumme) mit 4 Byte Länge gepackt. Die MTU der Sicherungsschicht sei 580 Byte, so dass eine Fragmentierung des IP-Pakets vorgenommen werden muss, bevor es an die Sicherungsschicht übergeben werden kann.

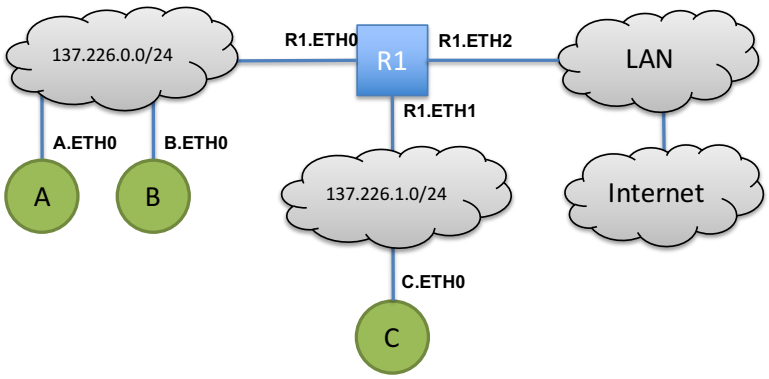
   Wie viele Byte (inklusive aller Header und Prüfsummen) werden insgesamt über das Netzwerk übertragen? Skizzieren Sie für die Vermittlungs- und Sicherungsschicht alle PDUs (Payload mit Header und ggfs. Trailer) und geben Sie die jeweiligen Größen in Byte an. Sie brauchen keine konkreten Header-Felder für die Pakete/Fragmente bzw. Rahmen anzugeben; lediglich die für die Fragmentierung relevanten Informationen sollen pro Fragment korrekt angegeben werden.

c) Auf der Sicherungsschicht sei ein Rahmen der Übertragung aus Teil b) verfälscht worden. *Wie viele Rahmen müssen erneut versendet werden*, wenn die Nutzdaten zuverlässig übertragen werden sollen? Begründen Sie Ihre Aussage.

   Anmerkung: Auf der Sicherungsschicht findet in diesem Fall – wie oft in der Praxis – nur Fehlererkennung, aber keine Fehlerbehandlung statt.

Aufgabe 6.4: Address Resolution Protocol (ARP)

Gegeben sei folgendes Netzwerk, in dem Router $R1$ zwei Subnetze `137.226.0.0/24` und `137.226.1.0/24` miteinander verbindet. In den Netzen befinden sich die drei Rechner A, B und C. Außerdem ist Router $R1$ mit einem Gateway `134.130.1.1` verbunden, welches ins Internet routet.



a) *Wie könnten die Routing-Tabellen des Routers und der drei Rechner aussehen?*

b) Alle ARP-Caches auf allen Systemen sind leer. Endsystem A möchte ein Paket an Endsystem C schicken. *Geben Sie alle ARP-Nachrichten und Paketübertragungen in der richtigen Reihenfolge an, die im Netzwerk übertragen werden, bis das Paket von A bei C angekommen ist.* Die MAC-Adresse einer Netzwerkkarte können Sie mit '`System.Interface`' angeben. Die MAC-Adresse der Ethernetkarte `ETH0` von Router $R1$ wäre z. B. `R1.ETH0`. Verwenden Sie folgende Formen für die Darstellung der Lösung:

ARP-Request: `Request <sender MAC> <sender IP> <receiver IP>` – <Inhalt/Zweck der Anfrage>

ARP-Reply: `Reply <sender MAC> <sender IP> <receiver MAC> <receiver IP>` – <Inhalt/Zweck der Antwort>

IP-Paket: `Data <sender MAC> <receiver MAC>`

Aufgabe 6.5: Netzwerkanalyse

In dieser Aufgabe sollen Sie Wireshark verwenden, um die Arbeit von IP und seinen ergänzenden Protokollen sowie die Interaktion mit anderen Schichten nachzuvollziehen. Wireshark für Linux, Windows oder MAC OS ist unter `http://www.wireshark.org/` erhältlich.

a) Machen Sie Sich zunächst mit Wireshark vertraut. Wie können Sie den Netzverkehr aufzeichnen? Was für Informationen enthalten die aufgezeichneten Daten? Wie finden Sie in der Menge der aufgenommenen Daten diejenigen, die Sie suchen?

b) Führen Sie nun einen `ping` auf `www.google.de` aus. Welche Auswirkungen hat dieser Befehl?

c) Führen Sie noch einmal einen `ping` aus, aber verändern Sie diesmal die Größe des Testpakets, das sie versenden, auf 2000 Byte. Was passiert? Wiederholen Sie diese Operation mit dem Ziel `www.rwth-aachen.de`. Was passiert nun?

d) Versuchen Sie als nächstes ein `traceroute` auf einen Rechner Ihrer Wahl. Wie arbeitet dieses Kommando?

e) Schauen Sie sich folgenden RFC an: https://tools.ietf.org/html/rfc3514. Glauben Sie, die Vorgehensweise erhöht die Sicherheit?

Einleitung des RFCs:

> „Firewalls [CBR03], packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the „evil“' bit, in the IPv4 [RFC791] header. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1.“