

# **6. TUTORIUM**

DATENKOMMUNIKATION UND SICHERHEIT

TUTORIUMSGRUPPE 18

MATTHIS FRANZGROTE

COMSYS

RWTH AACHEN

16.06.2021

- 1 Offene Frage
- 2 Das liefert nicht so gut...
- 3 Aufgabe 6.1: Ip-Adressen und CIDR
- 4 Aufgabe 6.2: Network Address Translation (NAT)
- 5 Aufgabe 6.3: IP-Pakete und Fragmentierung
- 6 Aufgabe 6.4: Address Resolution Protocol (ARP)
- 7 Aufgabe 6.5: Netzwerkanalyse

# **OFFENE FRAGE**

# ECHTZEIT-FÄHIGKEIT VON CSMA/CD

## Frage

Was bedeutet "CSMA/CD ist *nicht deterministisch*, und daher ist kein *Echtzeitbetrieb möglich*."

# ECHTZEIT-FÄHIGKEIT VON CSMA/CD

## Frage

Was bedeutet "CSMA/CD ist *nicht deterministisch*, und daher ist kein Echtzeitbetrieb möglich."

Echzeitsystem:

- Ständig betriebsbereit
- Garantierte Verarbeitung innerhalb einer bestimmten Zeitspanne

Wo ist das Problem?

- Nach einer Kollision: Binary Exponential Backoff
- → zufällige Wartezeit (verteilt über ein Intervall - das Contention Window)
- Also ist die Zustellung der Daten zu einem bestimmten Zeitpunkt nicht garantiert
- Eher gibt es eine Wahrscheinlichkeit, dass die Daten bis dahin übertragen wurden

**DAS LIEFT NICHT SO GUT...**

# FENSTERGRÖSSE UND SEQUENZNUMMERN

## Aufgabe 4.2

Es werde das *Sliding-Window-Verfahren* mit einer Fenstergröße von  $n$  Rahmen verwendet. Wie viele Sequenznummern braucht man dann bei *Go-Back-N* bzw. *Selective Repeat*?

- Go-Back-N  
 $n=8 \quad 0, 1, \dots, 7$
- 8 Rahmen versandt, können nicht an
- Ach 7

# FENSTERGRÖSSE UND SEQUENZNUMMERN

## Aufgabe 4.2

Es werde das *Sliding-Window-Verfahren* mit einer Fenstergröße von  $n$  Rahmen verwendet. Wie viele Sequenznummern braucht man dann bei *Go-Back-N* bzw. *Selective Repeat*?

Go-Back-N:

- $n = 8$
- Versende Rahmen  $0, 1, \dots, 7$
- Alle gehen verloren
- ACK 7 kommt zurück
- ⇒ Sind alle angekommen, oder gar keins (wiederholtes ACK vom letzten Fenster)?

Wir brauchen also  $n + 1$  Sequenznummern

# FENSTERGRÖSSE UND SEQUENZNUMMERN

## Aufgabe 4.2

Es werde das *Sliding-Window-Verfahren* mit einer Fenstergröße von  $n$  Rahmen verwendet. Wie viele Sequenznummern braucht man dann bei *Go-Back-N* bzw. *Selective Repeat*?

Selective-Repeat:

- $n = 8$
- Versende Rahmen 0, 1, ..., 6
- Alle kommen an (Empfänger verschiebt Fenster auf 7, 0, 1, ..., 5)
- Kein ACK kommt zurück
- Sendet 0, 1, ..., 6 erneut
- Ist Rahmen 0 ein neuer oder der alte?

Wir brauchen also  $2 \cdot n$  Sequenznummern

# AUFGABE 6.1: IP-ADRESSEN UND CIDR

## AUFGABE 6.1 A)

### Aufgabe

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?

1000 1001. 1110 0010. 0000 1100. 1101 1101

# AUFGABE 6.1 A)

## Aufgabe

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?

10001001.11100010.00001100.11011101  
10001001.11101010.00010001.11011110  
**11111111.11110000.00000000.00000000**

# AUFGABE 6.1 A)

## Aufgabe

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?

**137       $1110000_2 = 224$**

10001001.11100010.00001100.11011101		
10001001.1110 <b>1</b> 010.00010001.11011110		
<hr/>		
11111111.11110000.00000000.00000000		

Netz: 137.224.0.0

Subnetzmaske: 255.240.0.0

CIDR Notation: 137.224.0.0/12

## AUFGABE 6.1 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 : 3990, X : 2020, Y : 4096, Z : 1853

### Aufgabe

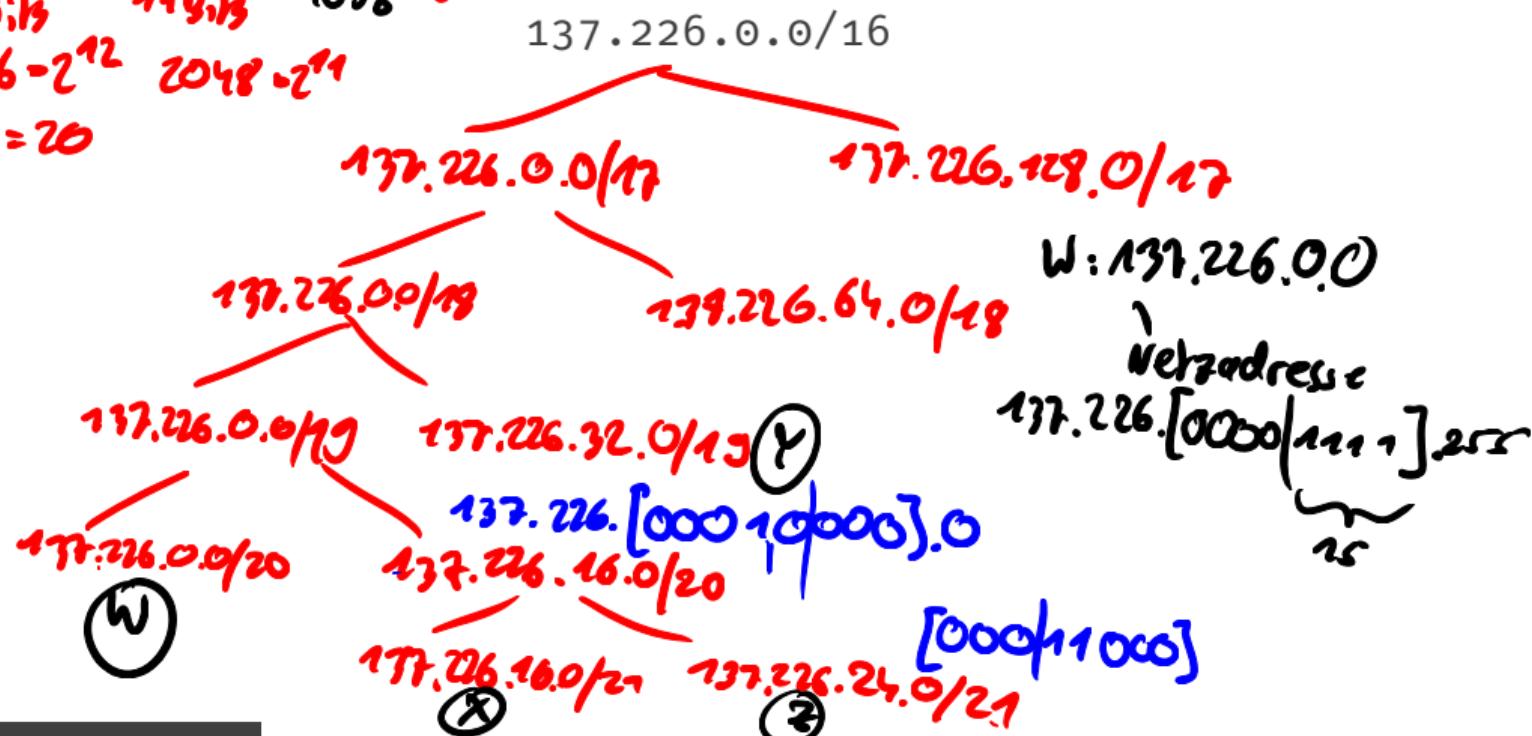
Vergeben wird jeweils die niedrigstmögliche Netzadresse. Geben Sie für jede Organisation die zugewiesene Netzadresse mit Netzmaske an. Geben Sie darüber hinaus jeweils an, welches die erste und welches die letzte IP-Adresse aus dem zugewiesenen IP-Adressbereich ist.

# AUFGABE 6.1 B)

W : 3990, X : 2020, Y : 4096, Z : 1853

$$\begin{array}{l} \text{12 Bits} \\ \underline{4096 - 2^{12}} \\ 2048 \cdot 2^9 \\ 32 - 12 = 20 \end{array}$$

226 = 1110 0010



## AUFGABE 6.1 B)

4096 (=12 Bit), 2048 (=11 Bit), 8192 (=13 Bit)

Org.	Subnetz	erste IP-Adr.	letzte IP-Adr.	# Adr.
W (3990)				
X (2020)				
Y (4096)				
Z (1853)				

# AUFGABE 6.1 B)

4096 (=12 Bit), 2048 (=11 Bit), 8192 (=13 Bit)

Org.	Subnetz	erste IP-Adr.	Letzte IP-Adr.	# Adr.
W (3990)	137.226.0.0/20	137.226.[0000 0000].0 137.226.0.0	137.226.[0000 1111].255 137.226.15.255	4096
X (2020)	137.226.16.0/21	137.226.[0001 0000].0 137.226.16.0	137.226.[0001 0111].255 137.226.23.255	2048
(4096)	137.226.32.0/19	137.226.[0010 0000].0 137.226.32.0	137.226.[0011 1111].255 137.226.63.255	8192
Z (1853)	137.226.24.0/21	137.226.[0001 1000].0 137.226.24.0	137.226.[0001 1111].255 137.226.31.255	2048

## AUFGABE 6.1 c)

### Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse A: Präfix 0, Maske: /8, Adressbereich: 0.0.0.0 - 127.255.255.255

0xxx xxxx | yy yy yy . . -  
2<sup>7</sup>

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse A. Präfix 0, Maske  $\underline{/8}$ , Adressbereich: 0.0.0.0 - 127.255.255.255

Also  $2^7$  Netze, abzüglich 10.0.0.0/8 (Privater Adressbereich) und 127.0.0.0/8 (Loopback)

⇒  $128 - 2 = \underline{126}$  Einträge

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse B: Präfix 10, Maske: /16, Adressbereich: 128.0.0.0 - 191.255.255.255

$$2^{14}$$

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse B: Präfix 10, Maske: 16 Adressbereich: 128.0.0.0 - 191.255.255.255

Also  $2^{14}$  Netze, abzüglich 172.16.0.0/12 (16 private Netze)

$$\Rightarrow 16384 - 16 = 16368 \text{ Einträge}$$

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse C: Präfix 110, Maske: /24 Adressbereich: 192.0.0.0 - 223.255.255.255

$$2^{21}$$

# AUFGABE 6.1 c)

## Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Klasse C: Präfix 110, Maske: /24, Adressbereich: 192.0.0.0 - 223.255.255.255

Also  $2^{21}$  Netze, abzüglich 192.168.0.0/16 (256 private Netze)

$$\Rightarrow 2097152 - 256 = 2096896 \text{ Einträge}$$

## AUFGABE 6.1 c)

### Aufgabe

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?

Keine Aggregation → Eintrag für jedes mögliche Netz

Insgesamt 2113390 Netze/Einträge (ungefähr; eigentlich gibt es noch mehr reservierte Netzbereiche).

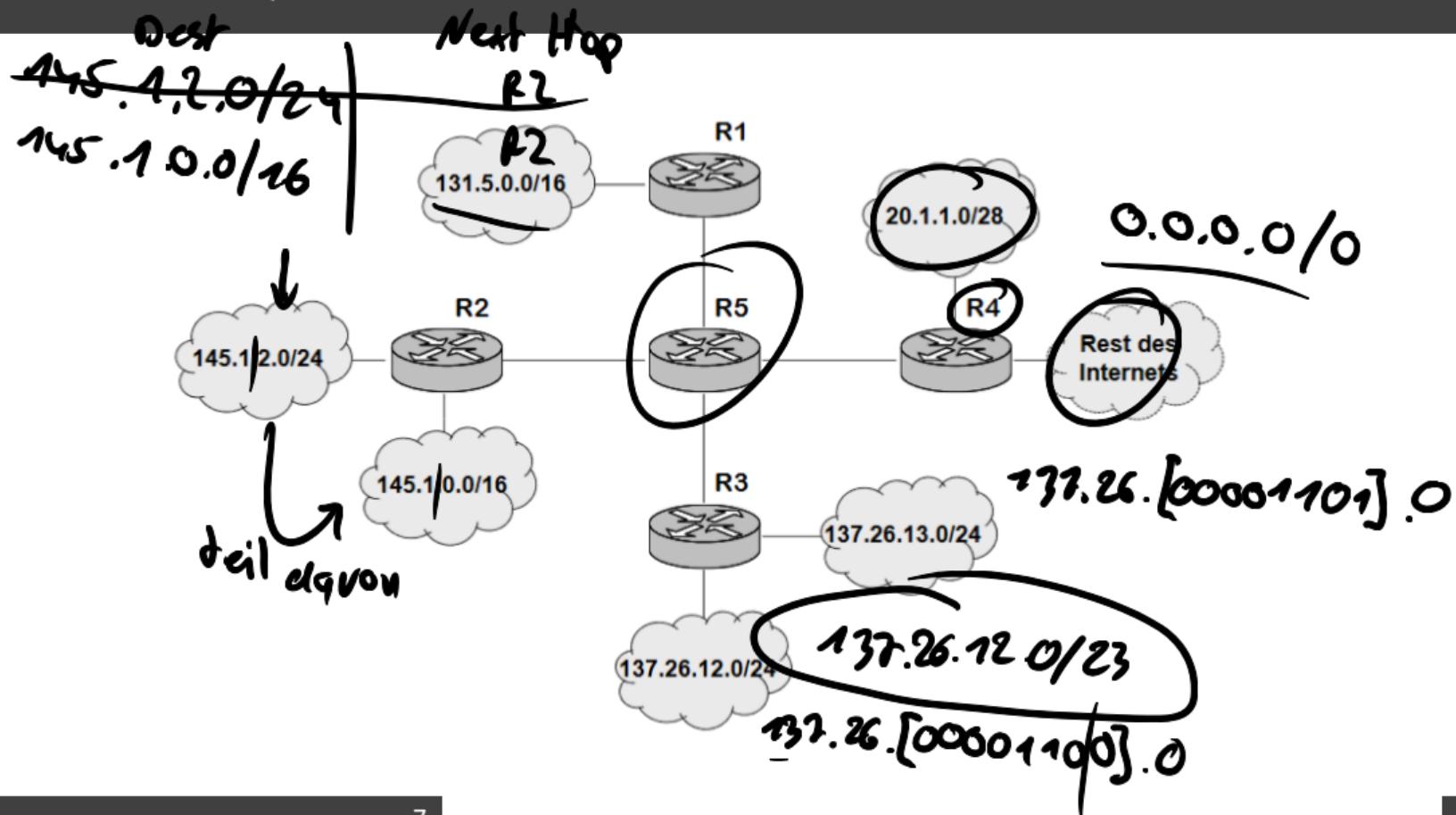
So viele Einträge kann kein Router effizient verwalten

## AUFGABE 6.1 D)

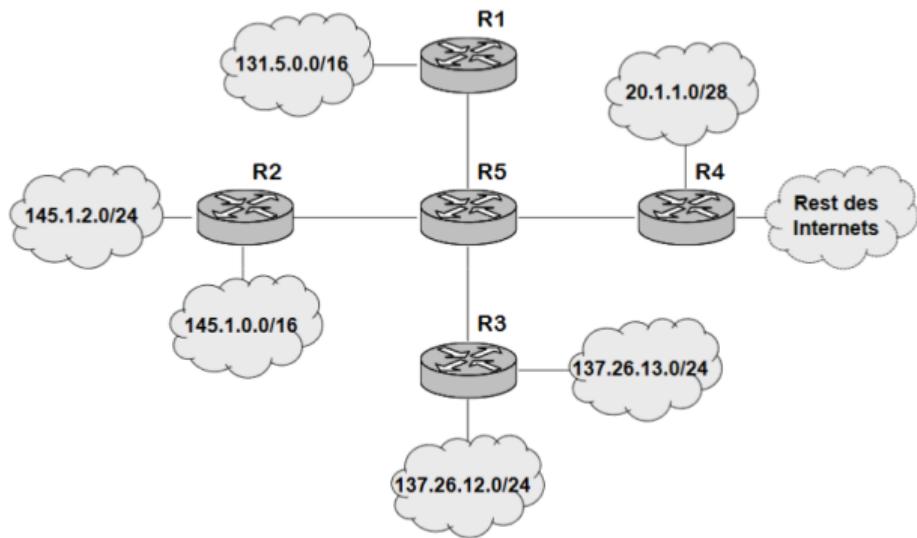
Betrachten Sie den folgenden Netzaufbau, in dem die Router  $R_1$  –  $R_4$  jeweils ein oder zwei Netze verwalten. Der genaue Aufbau dieser Netze ist uninteressant aber die Router  $R_1$  –  $R_4$  kennen die Adressbereiche der an sie angeschlossenen Netze. Lediglich Router  $R_4$  verfügt über eine Verbindung zum Rest des Internets. Sie haben nun den Router  $R_5$  installiert, um die Netze miteinander und mit dem Internet zu verbinden und müssen eine Routing-Tabelle erstellen. **Geben Sie für Router  $R_5$  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  $R_1$  –  $R_4$ . Angaben wie Flags, Netzwerkkarten-Adressen oder weiteres sind hier nicht von Interesse.

# AUFGABE 6.1 D)

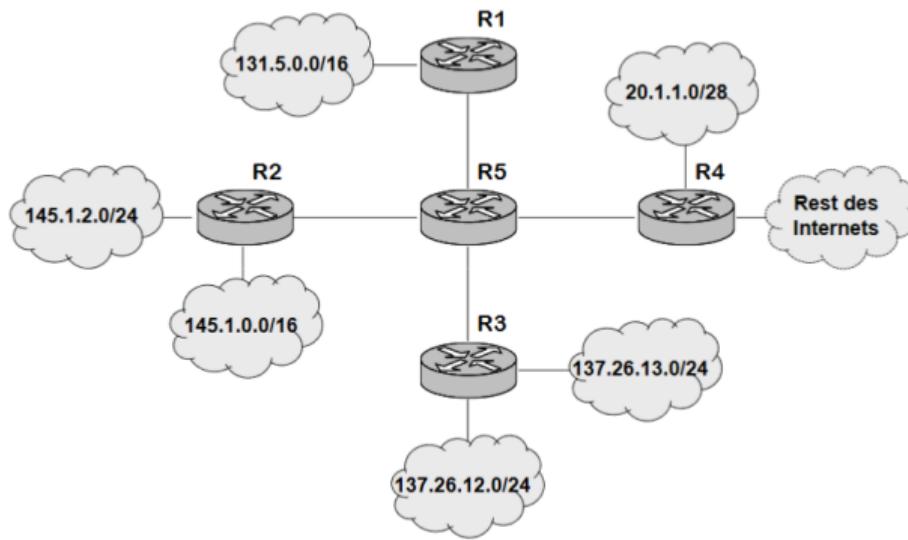


# AUFGABE 6.1 D)



Destination	Next Hop

# AUFGABE 6.1 D)



Destination	Next Hop
137.226.12.0/23	R3
131.5.0.0/16	R1
145.1.0.0/16	R2
0.0.0.0/0	R4

# AUFGABE 6.1 D)

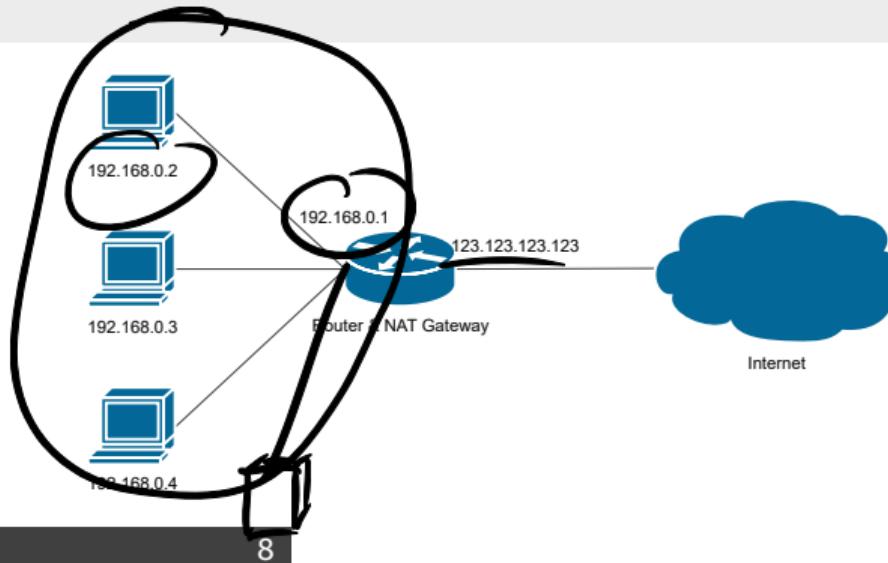
Destination	Next Hop	Destination	Next Hop
137.226.12.0/24	R3	137.226.12.0/23	R3
137.226.13.0/24	R3	131.5.0.0/16	R1
131.5.0.0/16	R1	145.1.0.0/16	R2
145.1.2.0/24	R2	0.0.0.0/0	R4
145.1.0.0/16	R2		
20.1.1.0/28	R4		
0.0.0.0/0	R4		

# **AUFGABE 6.2: NETWORK ADDRESS TRANSLATION (NAT)**

# AUFGABE 6.2 A)

## Aufgabe

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.



## AUFGABE 6.2 A)

### Aufgabe

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.

Prinzip:

- Vergebe Netzintern nur private IPs
- Nach außen hin eine globale gültige IP
- In Paketen vom internen ins externe Netz wird die Source-IP durch die globale ausgetauscht
- Abbildungseintrag für spätere Rückübersetzung
- Für eindeutige Einträge zusätzlich Ports mit merken

## AUFGABE 6.2 A)

### Aufgabe

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.

Vor-/Nachteile bei Kommunikation mit internen Rechnern:

- keine; Kommunikation wie gewohnt

## AUFGABE 6.2 A)

### Aufgabe

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.

Vor-/Nachteile bei Kommunikation mit externen Rechnern:

- Kommunikation erst nach Anlegen des Eintrags möglich
- Kommunikation muss von innen initiiert werden (sonst gibt es keinen Eintrag) oder eine statische Portweiterleitung eingerichtet werden
- + NAT ist automatisch auch ein Portfilter (unerwünschte Anfragen werden nicht weitergeleitet)
- + Interne Netzstruktur bleibt verborgen
- O.g. Sicherheitsaspekte genauso (einfach) mit Firewalls erzielbar

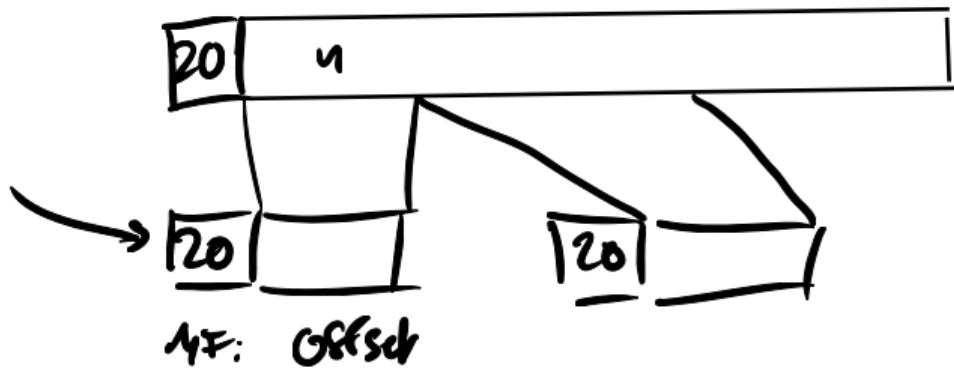
## AUFGABE 6.2 B)

### Aufgabe

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

Prinzipiell kein NAT mehr nötig, da genug IP-Adressen vorhanden sind.  
Ohne NAT ist eine Firewall also de facto zwingend notwendig.

## AUFGABE 6.3: IP-PAKETE UND FRAGMENTIERUNG



Bitte in der Übung diese Notation für 6.3 verwenden.

## AUFGABE 6.3 A)

### Aufgabe

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?

## AUFGABE 6.3 A)

### Aufgabe

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?

- Belastung der Router auf dem Weg (theoretisch bis zu 64 kByte an Fragmenten pro Paket)
- Paket muss später evtl. sowieso wieder fragmentiert werden
- Routen können sich dynamisch ändern (z.B. durch Loadbalancer), sodass ein Router manche Fragmente nie erhält

## AUFGABE 6.3 B)

Mittels IPv4 sollen 1690 Byte Nutzdaten verschickt werden. Die sendende IP-Instanz erzeugt aus diesen Daten ein Paket, indem sie den Standard-Header hinzufügt; 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.

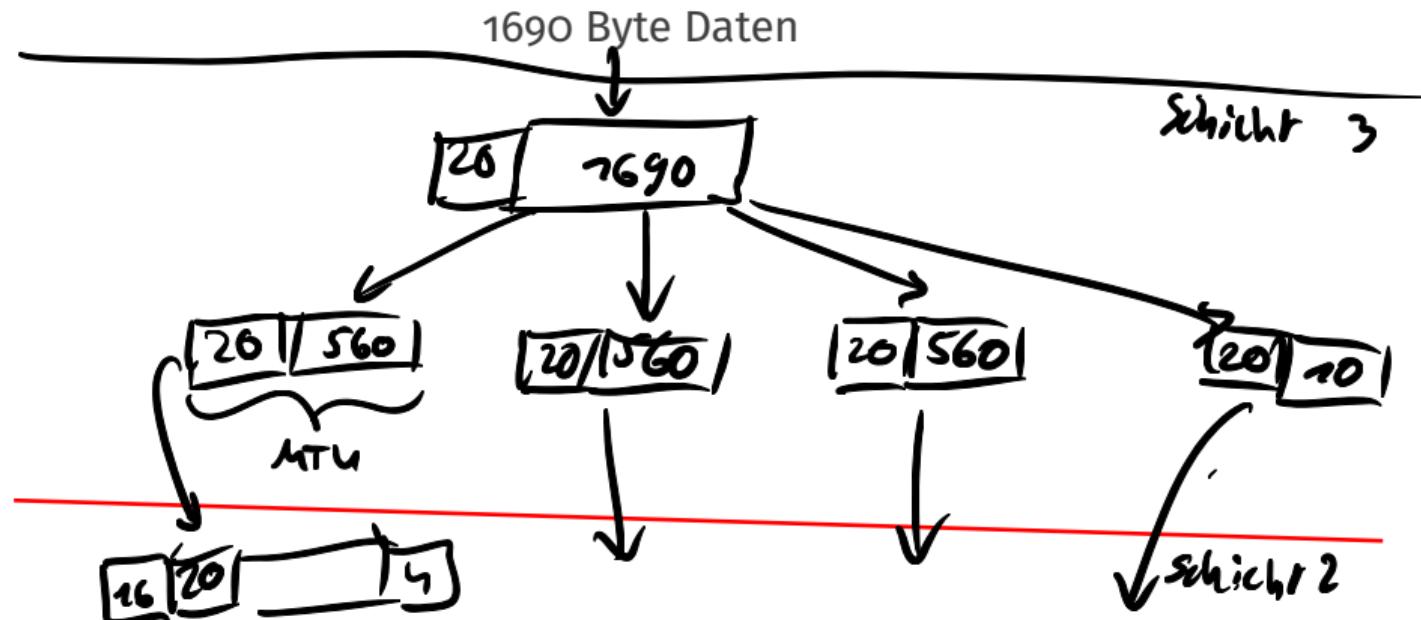
## AUFGABE 6.3 B)

### Aufgabe

Wie viele Byte (inklusive aller Header und Prüfsummen) werden insgesamt über das Netzwerkübertragen? 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.

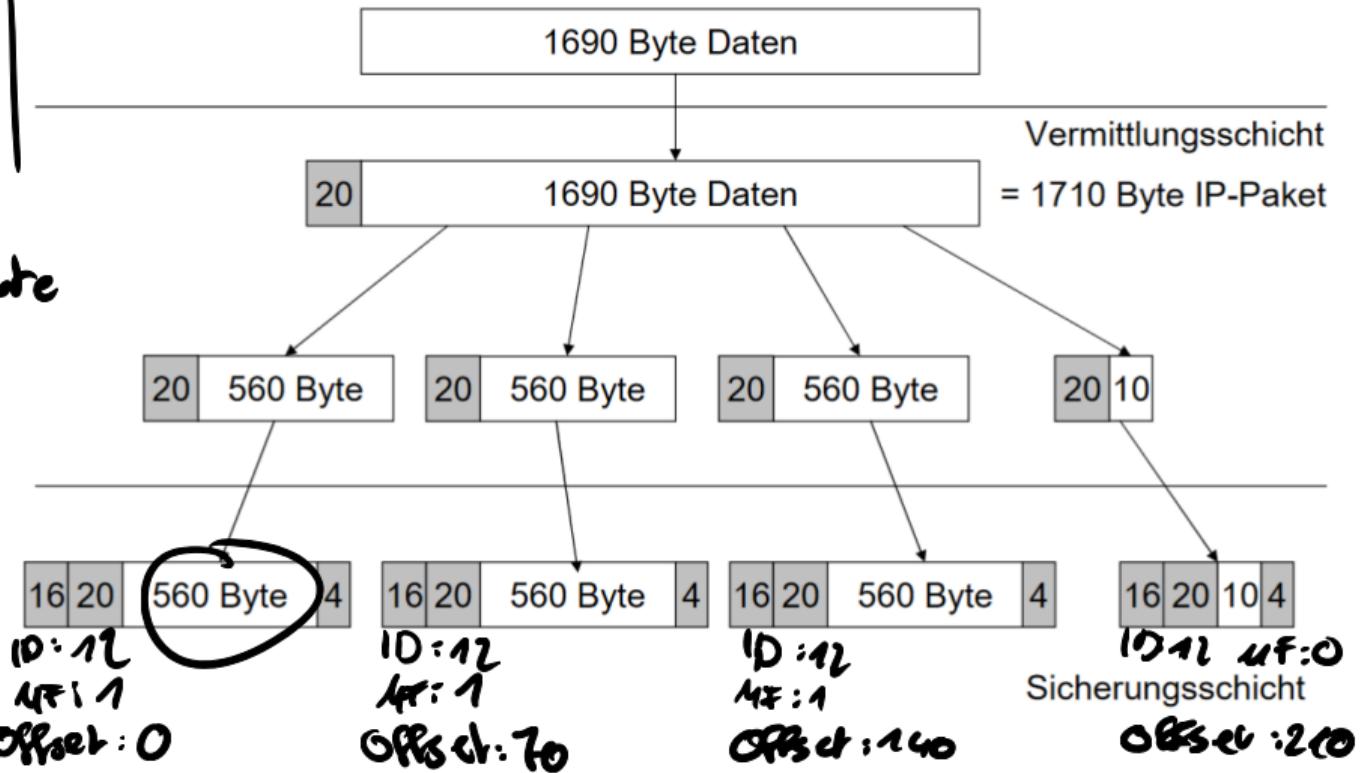
## AUFGABE 6.3 B)

1690 Byte Nutzdaten, 20 Byte IP-Header, 16 Byte Schicht 2 Header, 4 Byte Trailer, 580 Byte MTU



# AUFGABE 6.3 B)

ID  
MF  
Offset  
4  
In 8 Byte



## AUFGABE 6.3 B)

Fragmentierungsinformationen:

ID	MF	Offset

## AUFGABE 6.3 B)

Fragmentierungsinformationen:

ID	MF	Offset
171	1	0
171	1	70
171	1	140
171	0	210

Insgesamt übertragen:

$$\underbrace{1690 \text{ Byte}}_{\text{Nutzdaten}} + \underbrace{4 \cdot 20 \text{ Byte}}_{\text{IP Header}} + \underbrace{4 \cdot 20 \text{ Byte}}_{\text{Sicherungsschicht-Header/Trailer}} = \underline{\underline{1850 \text{ Byte}}}$$

## AUFGABE 6.3 c)

### Aufgabe

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?

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

## AUFGABE 6.3 c)

### Aufgabe

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?

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

IP hat keinerlei Sicherheitsmaßnahmen. Der Fehler wird nicht behandelt, also muss das gesamte Paket neu übertragen werden.

# AUFGABE 6.4: ADDRESS RESOLUTION PROTOCOL (ARP)

Problem: Man kennt i.d.R. nur die Domain eines Server, also z.B.  
moodle.rwth-aachen.de.

Domain → IP

Problem: Man kennt i.d.R. nur die Domain eines Server, also z.B.  
moodle.rwth-aachen.de.

Diese Domain muss erst einmal in eine IP umgewandelt werden  
→ DNS (Domain Name System)

Problem: Man kennt i.d.R. nur die Domain eines Server, also z.B.  
moodle.rwth-aachen.de.

Diese Domain muss erst einmal in eine IP umgewandelt werden  
→ DNS (Domain Name System)

Die IP reicht aber nicht. Denn für die Kommunikation auf Schicht 2 brauchen wir entsprechend eine Schicht 2 Adresse, also die MAC.

Problem: Man kennt i.d.R. nur die Domain eines Server, also z.B.  
moodle.rwth-aachen.de.

Diese Domain muss erst einmal in eine IP umgewandelt werden  
→ DNS (Domain Name System)

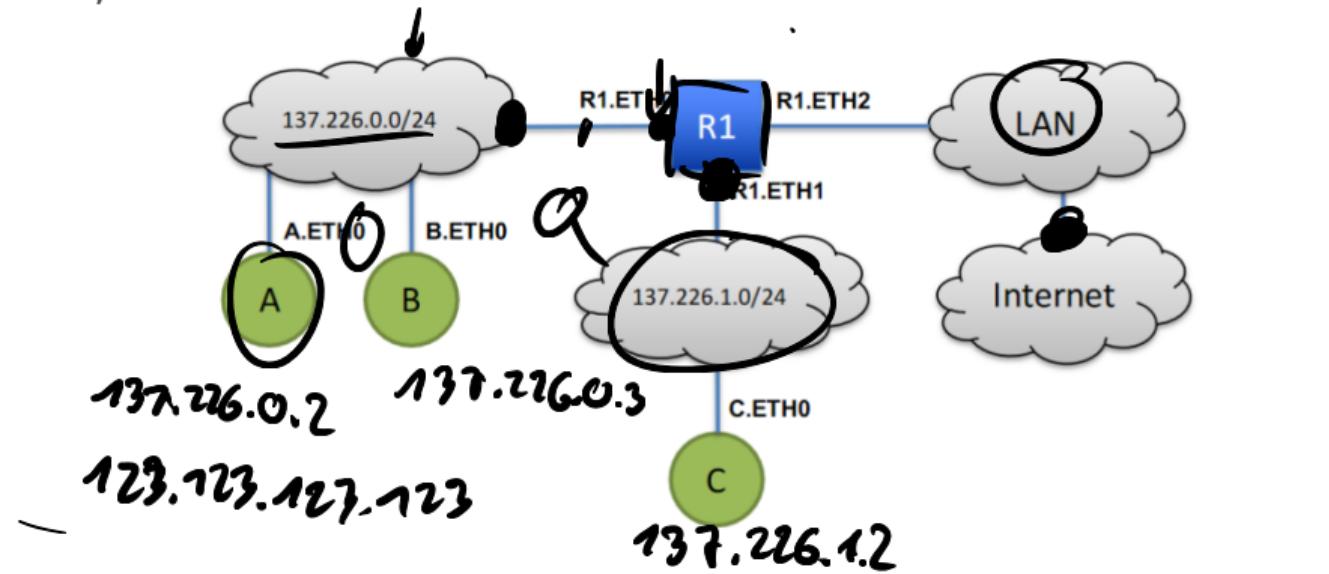
Die IP reicht aber nicht. Denn für die Kommunikation auf Schicht 2 brauchen wir entsprechend eine Schicht 2 Adresse, also die MAC.

Hier kommt ARP ins Spiel: **Übersetze eine IP in die dazugehörige MAC Adresse.**

Doof, wenn der Server dann nicht das macht was er soll ;)

## AUFGABE 6.4

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.



# AUFGABE 6.4 A)

## Aufgabe

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

Flags: U (Up), G (Gateway), H (Host)

Router/IP-Adressen	Routing-Tabelle			
	Zielnetz	Interface	Gateway	Flags
R1 ETH0: <del>177.226.0.1</del> ETH1: <del>177.226.1.1</del> ← ETH2: <del>134.210.1.2</del>	177.226.0/24	ETH10	*	u
	177.226.1.0/24	ETH11	*	u
	0.0.0.0/0	ETH12	134.210.1.1	uG

# AUFGABE 6.4 A)

Routing-Tabelle				
Router/IP-Adressen	Zielnetz	Interface	Gateway	Flags
<b>R1</b> ETH0:137.226.0.1 ETH1:137.226.1.1 ETH2:134.130.1.2	137.226.0.0/24 137.226.1.0/24 0.0.0.0/0	ETH0 ETH1 ETH2	* *	U U UG

# AUFGABE 6.4 A)

Routing-Tabelle					
Endsystem/IP-Adressen	Zielnetz	Interface	Gateway	Flags	
<b>A</b> ETHo: 5.0.	137.226.0.0/24 0.0.0.0/0 127.0.0.8	ETHo ET1/0 lo	0 137.226.0.1 127.0.0.1	4 UG UH	
<b>B</b> ETHo: 9.0.					
<b>C</b> ETHo: 9.0.					

# AUFGABE 6.4 A)

Routing-Tabelle					
Endsystem/IP-Adressen	Zielnetz	Interface	Gateway	Flags	
<b>A</b> ETH0:137.226.0.2	137.226.0.0/24 → 0.0.0.0/0 • 127.0.0.0/8	ETH0 ETH0 lo	*	U	
			137.226.0.1	UG	
			127.0.0.1	UH	
<b>B</b> ETH0:137.226.0.3	137.226.0.0/24 0.0.0.0/0 • 127.0.0.0/8	ETH0 ETH0 lo	*	U	
			137.226.0.1	UG	
			127.0.0.1	UH	
<b>C</b> ETH0:137.226.1.2	137.226.1.0/24 0.0.0.0/0 • 127.0.0.0/8	ETH0 ETH0 lo	*	U	
			137.226.1.1	UG	
			127.0.0.1	UH	

## AUFGABE 6.4 B)

### Aufgabe

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>

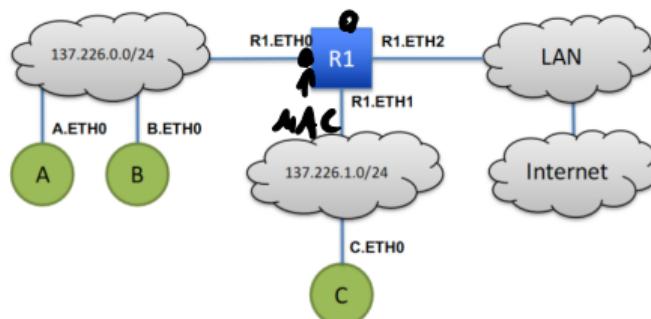
**IP-Paket:** Data <sender MAC> <receiver MAC>

## AUFGABE 6.4 B)

**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>



- Objekt IP      IP von Gateway/  
↓      ↓  
• Request A.ETH0 137.226.0.2 137.226.0.1  
- A möchte MAC von R1 wissen  
• Reply R1.ETH0 137.226.0.1 A.ETH0 137.226.0.2  
- R1 teil A seine MAC mit  
• Daten A.ETH0 R1.ETH0

## AUFGABE 6.4 B)

**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>

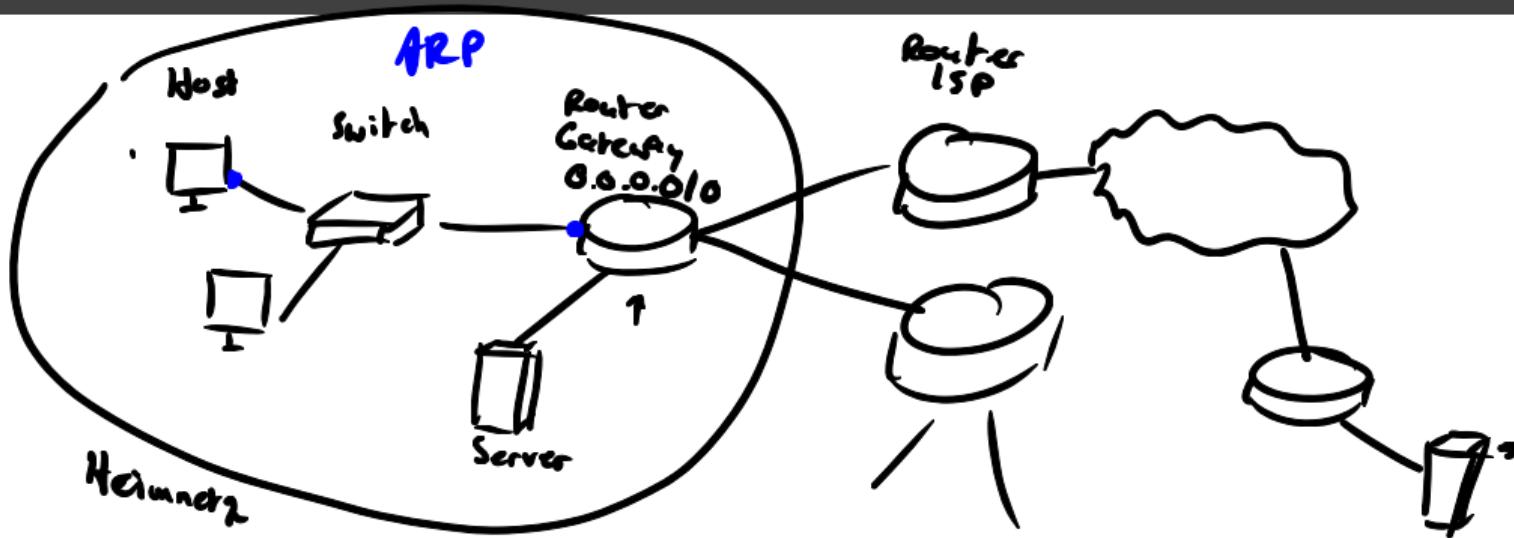
Routing Tabelle von A sagt, das Paket muss über R1 geschickt werden

- Request A.ETH<sub>0</sub> 137.226.0.2 137.226.0.1 - A sucht MAC zu 137.226.0.1 (R1)
- Reply R1.ETH<sub>0</sub> 137.226.0.1 A.ETH<sub>0</sub> 137.226.0.2 - R1 teilt A seine MAC mit
- Data A.ETH<sub>0</sub> R1.ETH<sub>0</sub> (- Übertragung des Pakets von A an R1)

Routing Tabelle von R1 sagt, das Paket kann via ETH1 direkt zu C geschickt werden

- Request R1.ETH<sub>1</sub> 137.226.1.1 137.226.1.2 - R1 sucht MAC zu 137.226.1.2 (C)
- Reply C.ETH<sub>0</sub> 137.226.1.2 R1.ETH<sub>1</sub> 137.226.1.1 - C teilt R1 seine MAC mit
- Data R1.ETH<sub>1</sub> C.ETH<sub>0</sub> (- Übertragung des Pakets von R1 an C)

# AUFGABE 6.5: NETZWERKANALYSE



## AUFGABE 6.5 A)

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.

### Aufgabe

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?

## AUFGABE 6.5 B)

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.

### Aufgabe

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

In der Übung von einem ping pro TTL ausgehen.

## AUFGABE 6.5 c)

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.

### Aufgabe

Führen Sie noch einmal einen ping aus, aber verändern Sie diesmal die GröSSe des Testpaket, das sie versenden, auf 2000 Byte. Was passiert? Wiederholen Sie diese Operation mit dem Ziel [www.rwth-aachen.de](http://www.rwth-aachen.de). Was passiert nun?

## AUFGABE 6.5 D)

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.

### Aufgabe

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

## AUFGABE 6.5 E)

### Aufgabe

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

"Firewalls [CBRo3], 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."

ÜBUNGSBLATT 5 ABGABEFRIST:  
18.06.2021 18:00 (VERSCHOBEN)

ÜBUNGSBLATT 6 ABGABEFRIST:  
28.06.2021 18:00

NÄCHSTES TUTORIUM:  
MITTWOCH 23.06.2021 12:30 ? ✓