LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Rechnernetze und verteilte Systeme

Übungsblatt 9

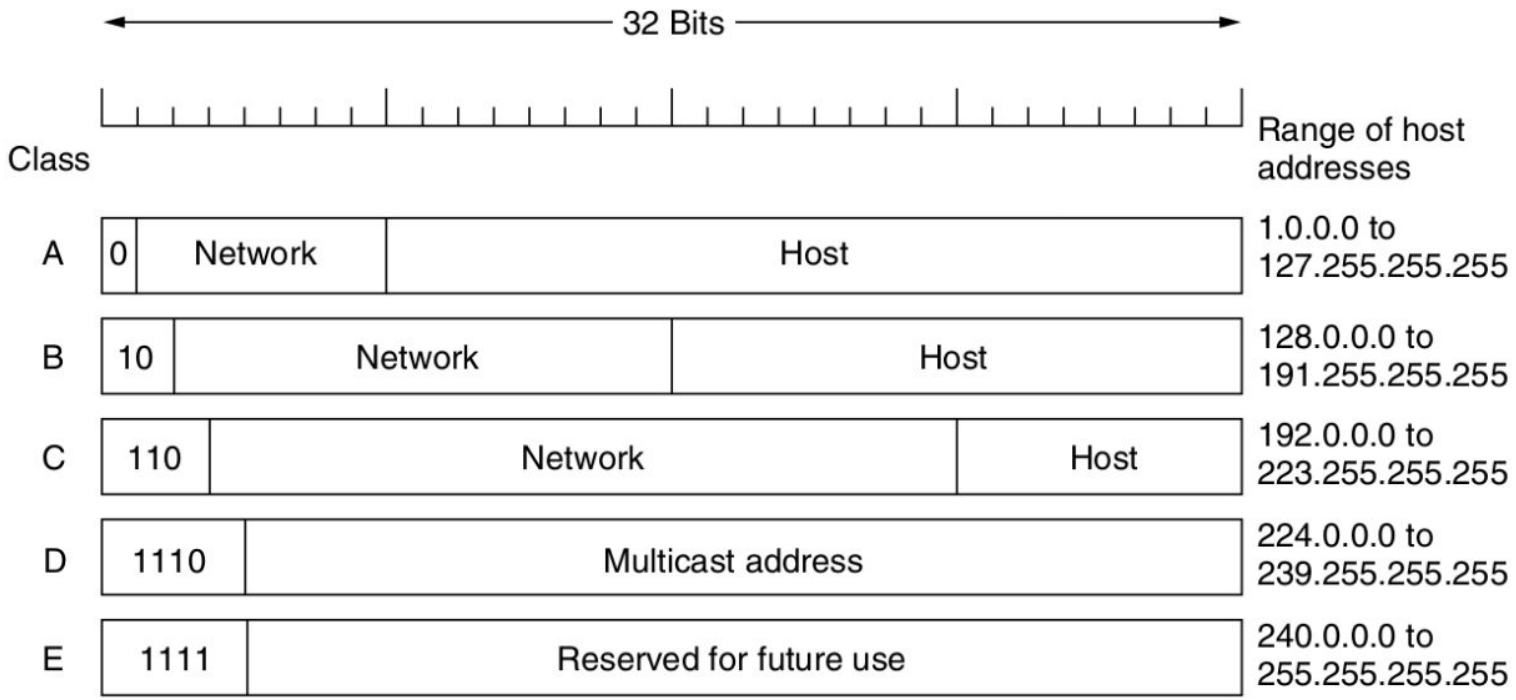
Koenig.Noah@campus.lmu.de

Historisch: Klassenbasierte Adressierung

Klasse	Präfix	Länge Netz ID	Länge Host ID	Anzahl Netze	Hosts pro Netz
A	0	7 bit	24 bit (3 byte)	126	16 777 214
B	10	14 bit	16 bit (2 byte)	16 382	65 534
C	110	21 bit	8 bit (1 byte)	2 097 152	254
D	1110	Verwendung für Multicast-Anwendungen			
E	1111	Reserviert (für zukünftige Zwecke)			

Kapitel 4 Vermittlung, Folie 82

Klassenbasierte Adressierung (Grafik)



Kapitel 4 Vermittlung, Folie 83

Wiederholung: CIDR

CIDR (Engl.: Classless Inter-Domain Routing)

- Mit RFC 1517 bis 1520 ab 1993 in Verwendung.
- Grundidee: Die Grenze zwischen Netz-Teil und Host-Teil verläuft fließend.
  - => Routing-Protokolle müssen die Länge der Netz-ID (Netzpräfix) zusätzlich zur Adresse übertragen.
- Verwendung von Subnetz-Masken
- Notation: <IP Adresse>/<Präfixlänge>

- Beispiel: 192.168.121.0/26
  (die ersten 26 Bit sind Netz-ID, der Rest Host-ID)

Kapitel 4 Vermittlung, Folie 85

Addressierung in Rechnernetzen (H)

(a) Klassenbasierte Adressierung und Classless Inter-Domain Routing (CIDR)

- Worin unterscheidet sich Classless Inter-Domain Routing (CIDR) von klassenbasierter Adressierung?
- Erklären Sie kurz die Vorteile von CIDR gegenüber klassenbasierter Adressierung.

- Unterschiede:
  - CIDR: keine feste Länge von Netz- / Host-Anteil
  - Klassenbasiert: 3 mögliche Netz- / Host-Anteil Längen
- Vorteile:
  - Effiziente Zuweisung von IP-Adressen
  - Minimierung der Anzahl von Routen, die ein Router in der Routing-Tabelle speichert (benachbarte Netze werden zusammengefasst zu einem Eintrag)

Subnetting

- Sowohl bei klassenbasierter Adressierung, als auch bei CIDR
- Grundidee: Host-Teil eines Adressblocks wird weiter unterteilt in Subnetz-ID-Teil und Host-ID-Teil.

Kapitel 4 Vermittlung, Folie 86

Netz ID	Host ID	
Netz ID	Subnetz ID	Host ID

- Eine Organisation kann mit einem einzigem Adressblock mehrere eigene Netze bedienen

(b) Eine Organisation bekommt den Adressblock `131.42.0.0/16` zugewiesen und benötigt:

- 1 Subnetz mit bis zu 32000 Hosts
- 15 Subnetz mit bis zu 2000 Hosts
- 8 Subnetz mit bis zu 250 Hosts

Machen Sie Vorschläge für eine Aufteilung in geeignete Subnetze. Erstellen Sie eine Tabelle aller Subnetze mit folgendem Inhalt:

1. Subnetzadresse in CIDR-Notation
2. Subnetzmaske
3. Für Hosts verwendbare Adressbereiche für jedes Subnetz
4. Broadcastadressen für jedes Subnetz.

1 Subnetz mit 32000 Hosts:

- $\lceil \log_2(32000) \rceil = 15$ Bit für Host ID
- Subnetz: 131.42.0.0/17
- Subnetzmaske: 255.255.128.0
- Adressbereich:
  - Dezimal:
    131.42.0.1 bis 131.42.127.254
  - Binär: (Netz-ID, Subnetz-ID, Host-ID)
    `10000011.00101010.00000000.00000001` bis
    `10000011.00101010.01111111.11111110`
    Hinweis: Es existieren auch 2^{15} Adressen mit (Sub-) Netz-ID
    `10000011.00101010.1` die für die 15 bzw. 8 Subnetze verwendet werden
- Broadcast-Adresse: (Host Anteil mit nur 1en)
  131.42.127.255

15 Subnetze mit je 2000 Hosts:

- $\lceil \log_2(2000) \rceil$ = 11 Bit für Host ID → 21 Bit für Netz-ID
- Subnetze: 15 insgesamt → mindestens 4 Bit zur Adressierung nötig (2^4 = 16)
  131.42.**128**.0/21, 131.42.**136**.0/21, 131.42.**144**.0/21, …, 131.42.**240**.0/21
- Subnetzmaske: 255.255.128.0 (für alle)
- Adressbereich:
  - Dezimal:
    131.42.**128.1** bis 131.42.**135.254**,
    131.42.**136.1** bis 131.42.**143.254**,
    131.42.**144.1** bis 131.42.**151.254**,
    …,
    131.42.**240.1** bis 131.42.**247.254**
  - Binär: (Netz-ID, Subnetz-ID, Host-ID)
    `10000011.00101010.10000000.00000001` bis
    `10000011.00101010.10000111.11111110`,

10000011.00101010.10001000.00000001 bis
10000011.00101010.10001111.11111110,
10000011.00101010.10010000.00000001 bis
10000011.00101010.10010111.11111110,
…,
10000011.00101010.11110000.00000001 bis
10000011.00101010.11110111.11111110,
Hinweis: Es existieren auch 2^8 Adressen mit (Sub-) Netz-ID
10000011.00101010.11111 die für die 8 Subnetze verwendet werden

- Broadcast-Adressen:
  131.42.**135**.255,
  131.42.**143**.255,
  131.42.**151**.255,
  …,
  131.42.**247**.255,

8 Subnetze mit je 250 Hosts:

- $\lceil \log_2(250) \rceil$ = 8 Bit für Host ID → 24 Bit für Netz-ID
- Subnetze: 8 insgesamt → mindestens 3 Bit zur Adressierung nötig ($2^3 = 8$)
  131.42.**248**.0/24, 131.42.**249**.0/24, 131.42.**250**.0/24, …, 131.42.**255**.0/24
- Subnetzmaske: 255.255.255.0 (für alle)
- Adressbereich:
  - Dezimal:
    131.42.**248.1** bis 131.42.**248.254**,
    131.42.**249.1** bis 131.42.**249.254**,
    131.42.**250.1** bis 131.42.**250.254**,
    …,
    131.42.**255.1** bis 131.42.**255.254**
  - Binär: (Netz-ID, Subnetz-ID, Host-ID)
    `10000011.00101010.11111000.00000001` bis
    `10000011.00101010.11111000.11111110`,

10000011.00101010.11111001.00000001 bis
10000011.00101010.11111001.11111110,
10000011.00101010.11111010.00000001 bis
10000011.00101010.11111010.11111110,
…,
10000011.00101010.11111111.00000001 bis
10000011.00101010.11111111.11111110,

- Broadcast-Adressen:
  131.42.**248**.255,
  131.42.**249**.255,
  131.42.**250**.255,
  …,
  131.42.**255**.255,

Private IP-Adressen nach RFC1918 (H)

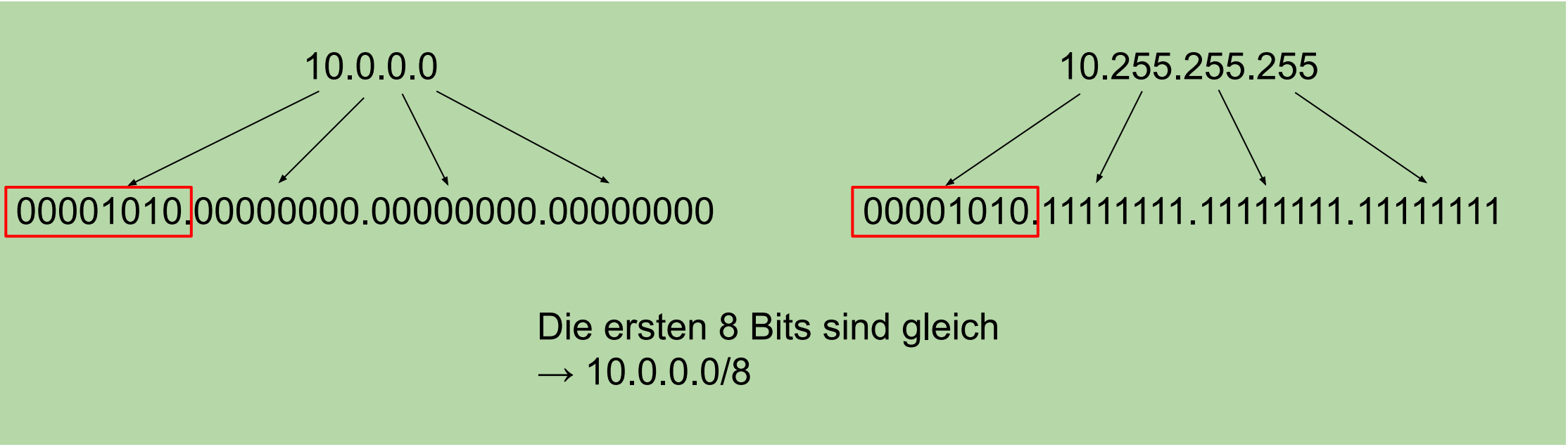
In RFC 1918[1] wurden eine Reihe privater IP-Adressen definiert:

1. 10.0.0.0 – 10.255.255.255
2. 172.16.0.0 – 172.31.255.255
3. 192.168.0.0 – 192.168.255.255

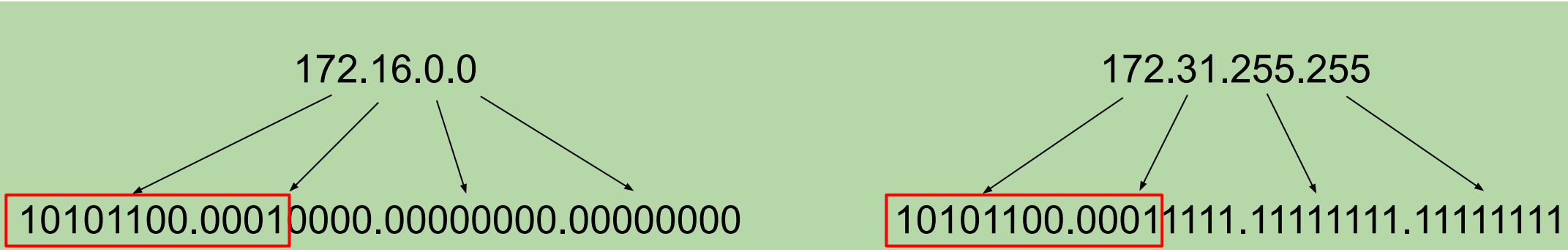
Pakete mit Adressen aus diesen Bereichen werden im Internet nicht weitergeleitet.

Private IP-Adressen nach RFC1918

(a) Wie lassen sich die drei Netzbereiche in Präfix-Notation darstellen?

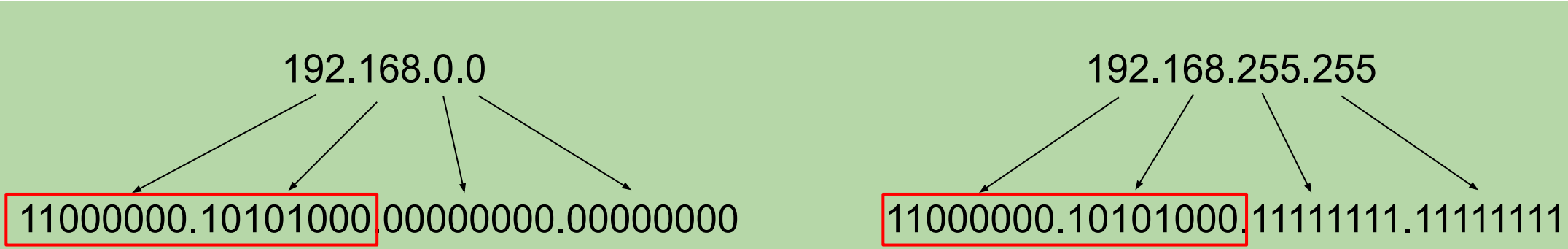


Private IP-Adressen nach RFC1918



Die ersten 12 Bits sind gleich
→ 172.16.0.0/12

Private IP-Adressen nach RFC1918



Die ersten 16 Bits sind gleich
→ 192.168.0.0/16

Private IP-Adressen nach RFC1918

(b) Zeigen Sie, dass das Netz 172.16.0.0/x (wobei x im ersten Teil ermittelt wurde) 16 Netze mit je 2^{16} Host-Adressen enthalten kann.

Hinweis: Zur besseren Handhabung bietet es sich an, die IP-Adressen und (Sub-)Netzmasken in die Binärdarstellung zu übertragen.

172.16.0.0/12 → Netzmaske 11111111.1111**0000**.00000000.00000000

Netz-Anteil

Subnetz-Anteil: 4 Bit

2^4 = 16 Subnetze

Host-Anteil: 16 Bit

2^{16} = 65,536 Hosts

Private IP-Adressen nach RFC1918

(c) Was sind die Vorteile der privaten IP-Adressen – warum sind sie nötig? Gibt es Nachteile bei der Nutzung im Zusammenhang mit dem Internet?

private IP-Adressen…

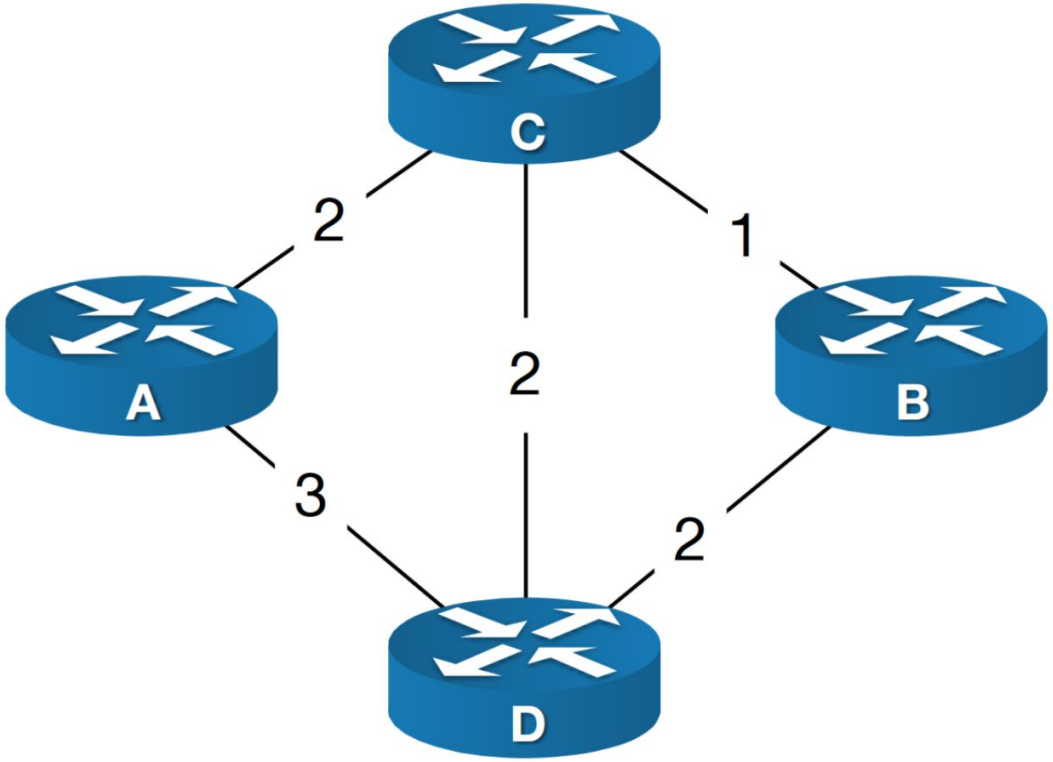
- sind sinnvoll für Geräte, die nicht mit dem Internet kommunizieren (sollen)
- können von LAN-Betreibern frei zugeteilt werden
- können mehrfach genutzt werden
  → kein “Verschwenden” von öffentlichen IP-Adressen für private Zwecke

Nachteil:

- Übersetzung (NAT) erforderlich für die Kommunikation zwischen Hosts mit privaten Adressen und dem Internet

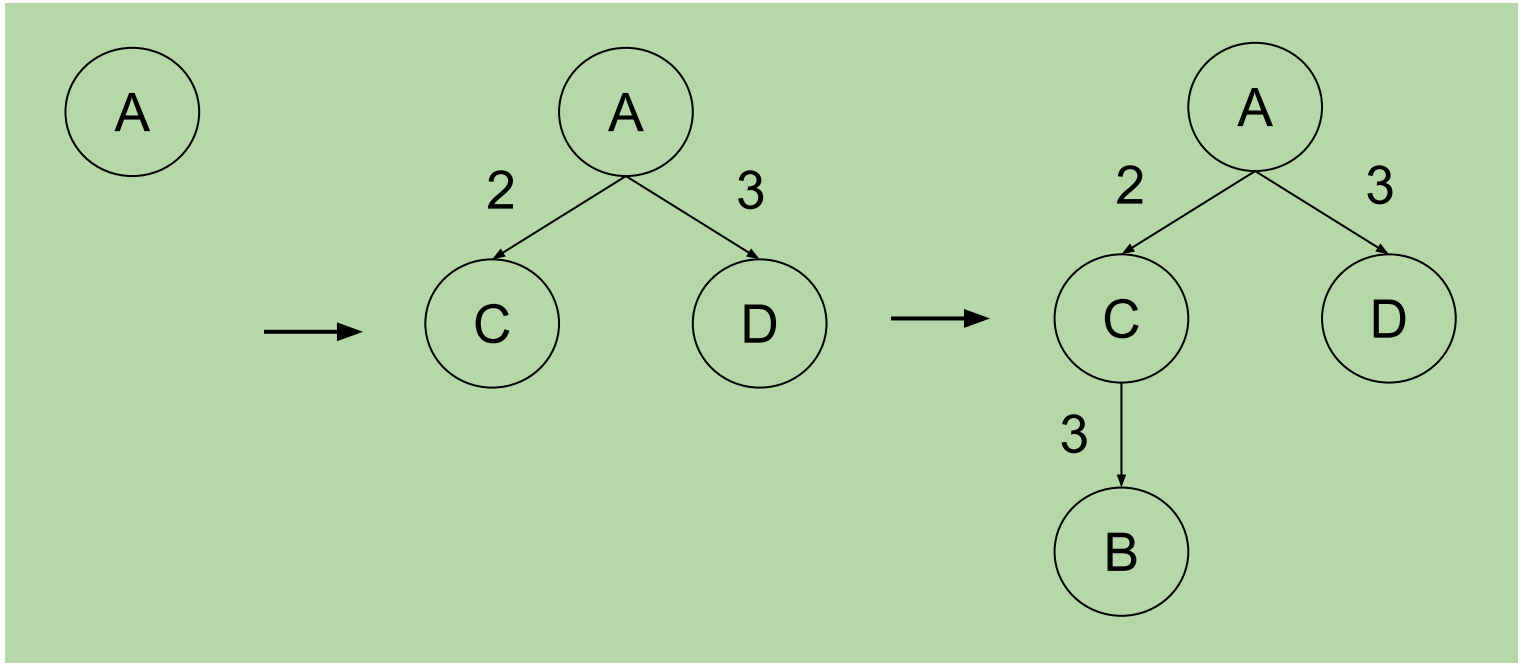
Link-State-Verfahren (H)

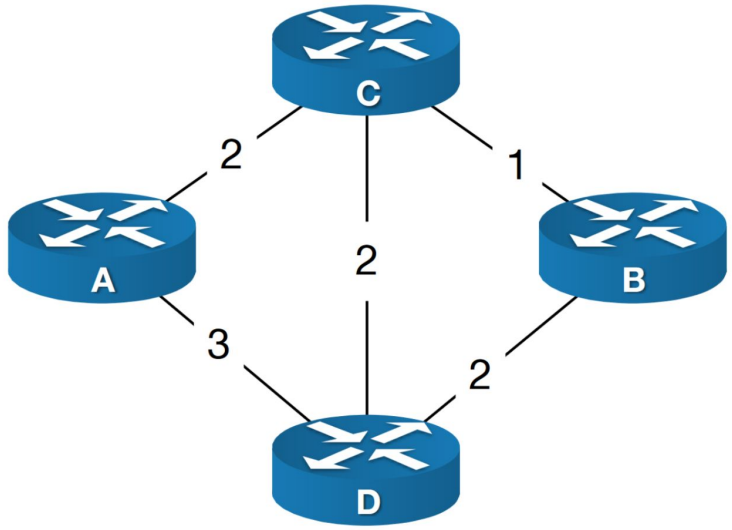
Betrachten Sie ein Netz bestehend aus vier Routern A, B, C, D.



Link-State-Verfahren

(a) Berechnen Sie den optimalen QSB (Quellen-Senken-Baum) für A mit Hilfe des SPF-Algorithmus (oft auch Dijkstra-Algorithmus genannt) und geben Sie eine Skizze für jeden Zwischenschritt an.

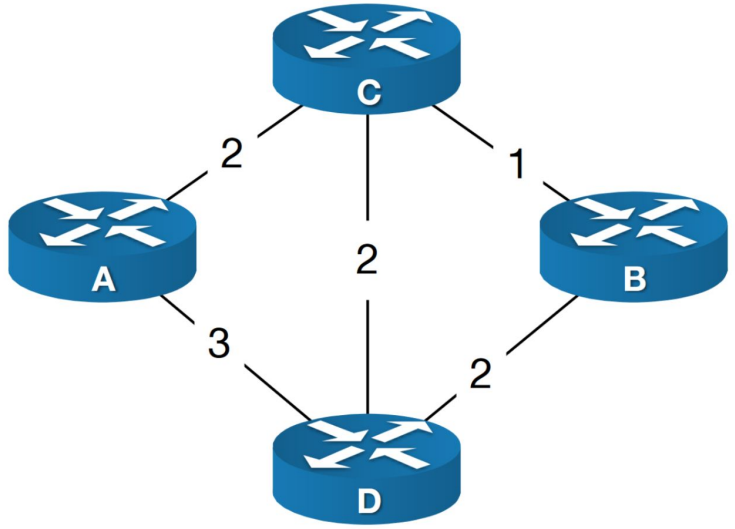




Link-State-Verfahren

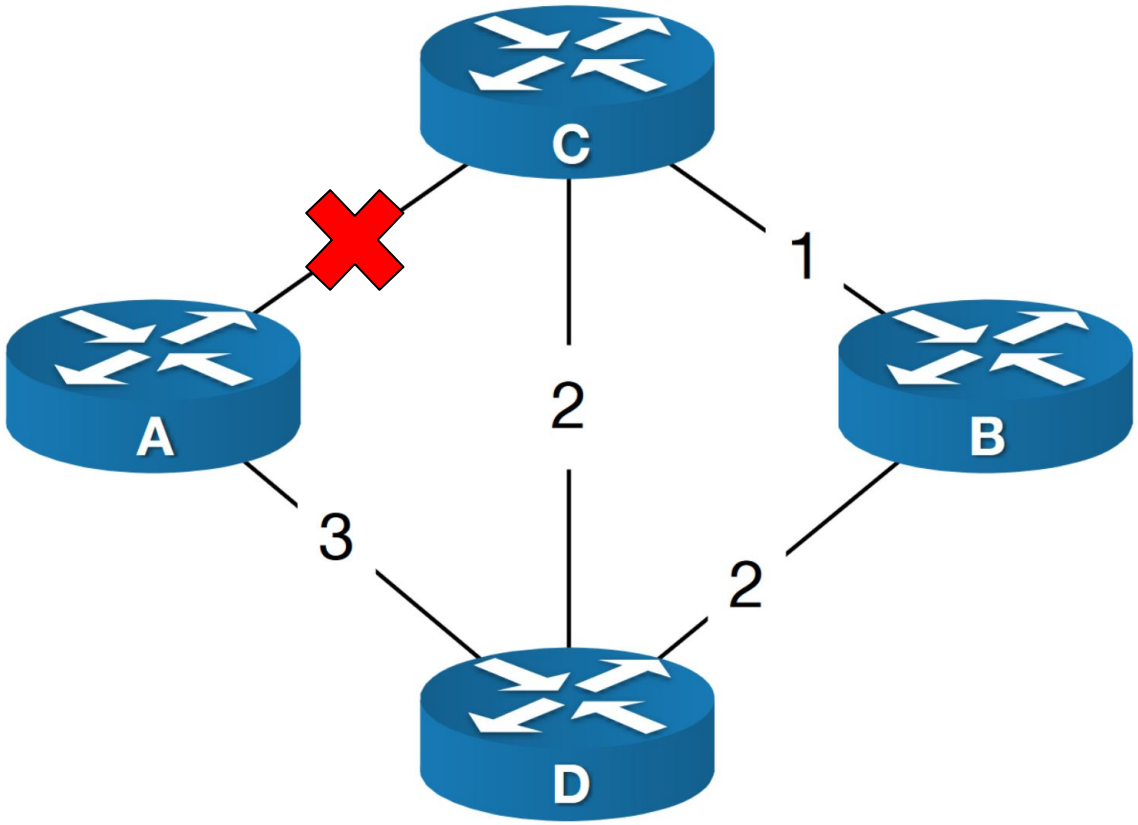
(b) Geben Sie die endgültige Routing-Tabelle (Wegetafel) für A an.

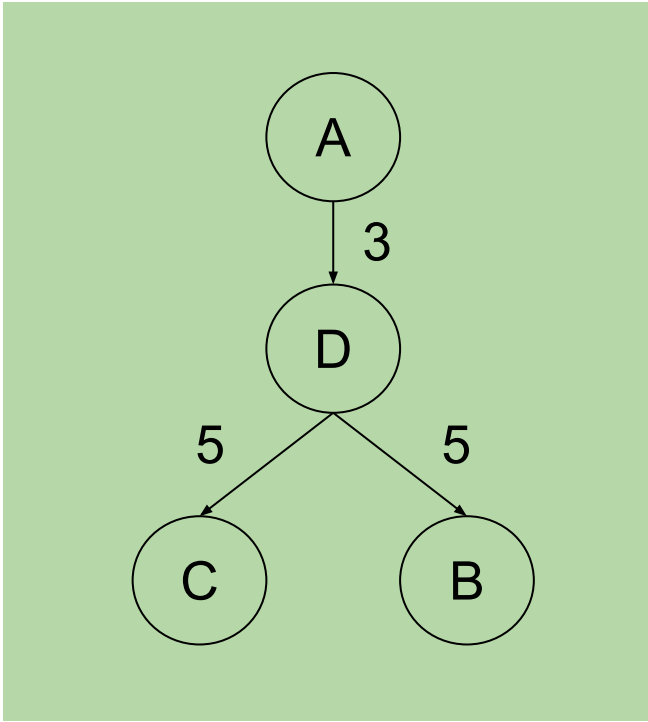
Ziel	Router
Subnetz(B)	C
Subnetz(C)	C
Subnetz(D)	D
Default	C (willkürlich)



Link-State-Verfahren

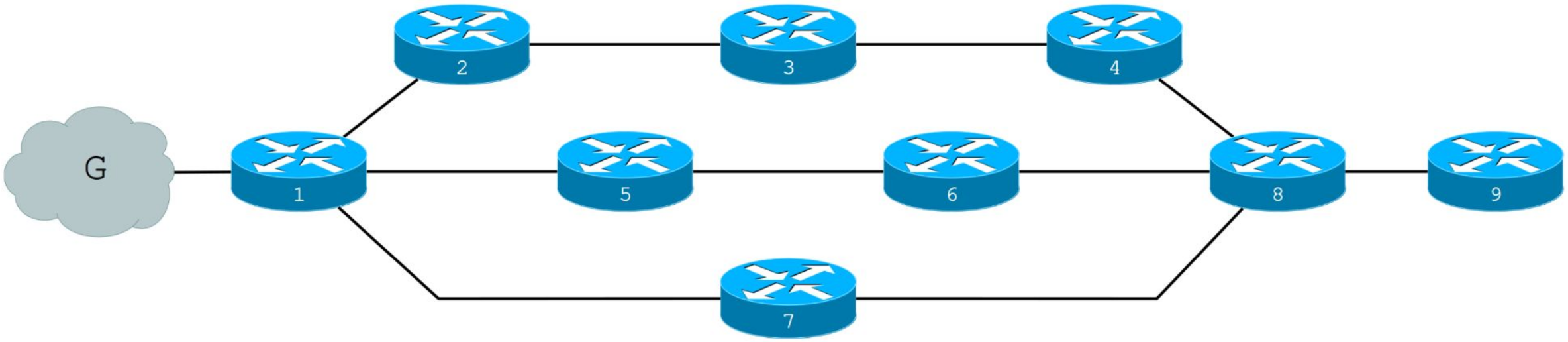
(c) Die Leitung A–C fällt aus. Wie sieht der optimale QSB für A nun aus?





Distanz-Vektor Routing (H)

Gegeben sei folgendes Netz, bestehend aus neun Routern und dem Subnetz G:

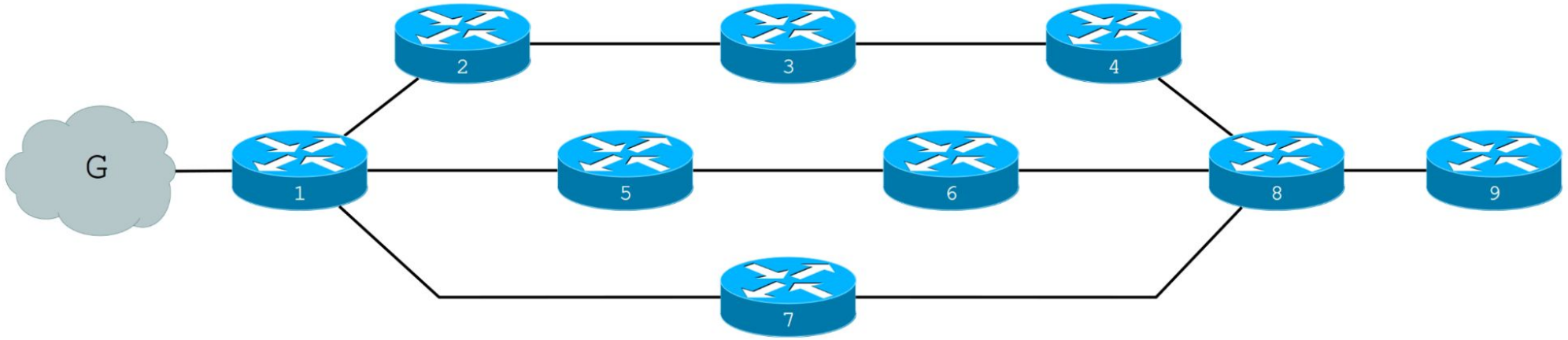


Auf allen Routern wird nun gleichzeitig ein Distanz-Vektor Routingprotokoll aktiviert (z.B. RIP). Als Metrik wird die Anzahl der Zwischenschritte verwendet.

Distanz-Vektor Routing

(a) Zeigen Sie wie sich die Routing-Information für Subnetz G Schritt für Schritt ausbreitet, in dem Sie die Tabelle erweitern. Tragen Sie in die Tabellenfelder die Metrik ein, mit der ein Router zu einem bestimmten Zeitpunkt Subnetz G ankündigt. t_0 ist Anfangszustand, wenn Router 1 zum ersten Mal Subnetz G ankünigt. Führen Sie die Tabelle fort, bis die Metriken stabil sind. Hinweis: Lassen Sie das entsprechende Feld leer, wenn der Router zu diesem Zeitpunkt keine Route zu G kennt.

Distanz-Vektor Routing



Zeitpunkt \ Router	1	2	3	4	5	6	7	8	9
t_0	0								
t_1	0	1			1		1		
t_2	0	1	2		1	2	1	2	
t_3	0	1	2	3	1	2	1	2	3

Distanz-Vektor Routing

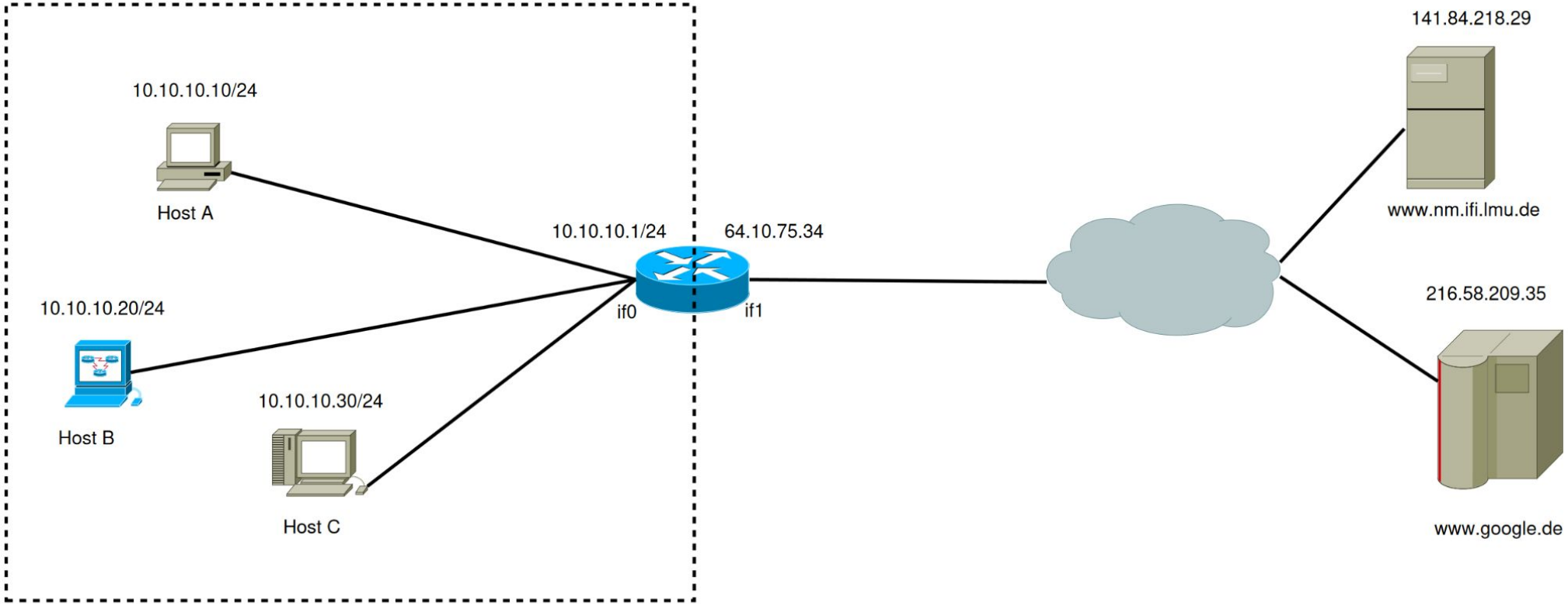
(b) Angenommen Subnetz G ist an Router 5 statt Router 1 angebunden. Kann in diesem Aufbau immernoch das Count-To-Infinity-Problem auftreten? Begründen Sie ihre Antwort!

z.B. bei einem Ausfall von Router 5, da das Netz nur mit Router 5 direkt verbunden ist

Network Address Translation (NAT)

In der Vorlesung wurde NAT als Dienst der Vermittlungsschicht eingeführt.

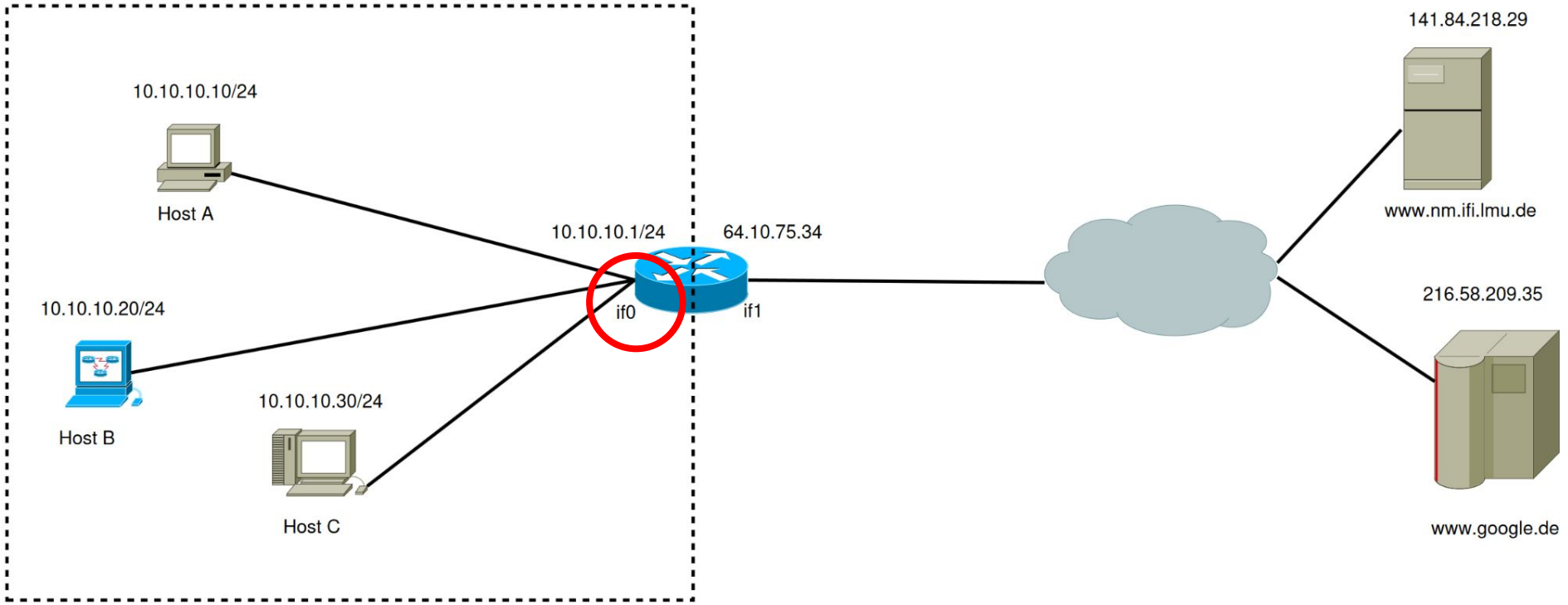
(a) Beschreiben Sie die Funktionsweise von NAT am Beispiel der Abbildung 1.



Network Address Translation (NAT)

Angenommen, Host C greift auf einen Foliensatz zu, der auf einem File-Server der LMU (erreichbar unter dem öffentlichen Namen `www.nm.ifi.lmu.de`) abgelegt ist.

- Wie sehen Quell- und Ziel-Adresse der Anfrage aus, wenn das Paket von Host C an der Schnittstelle von `if0` ankommt? Geben Sie auch die Adressen der Transportschicht an.

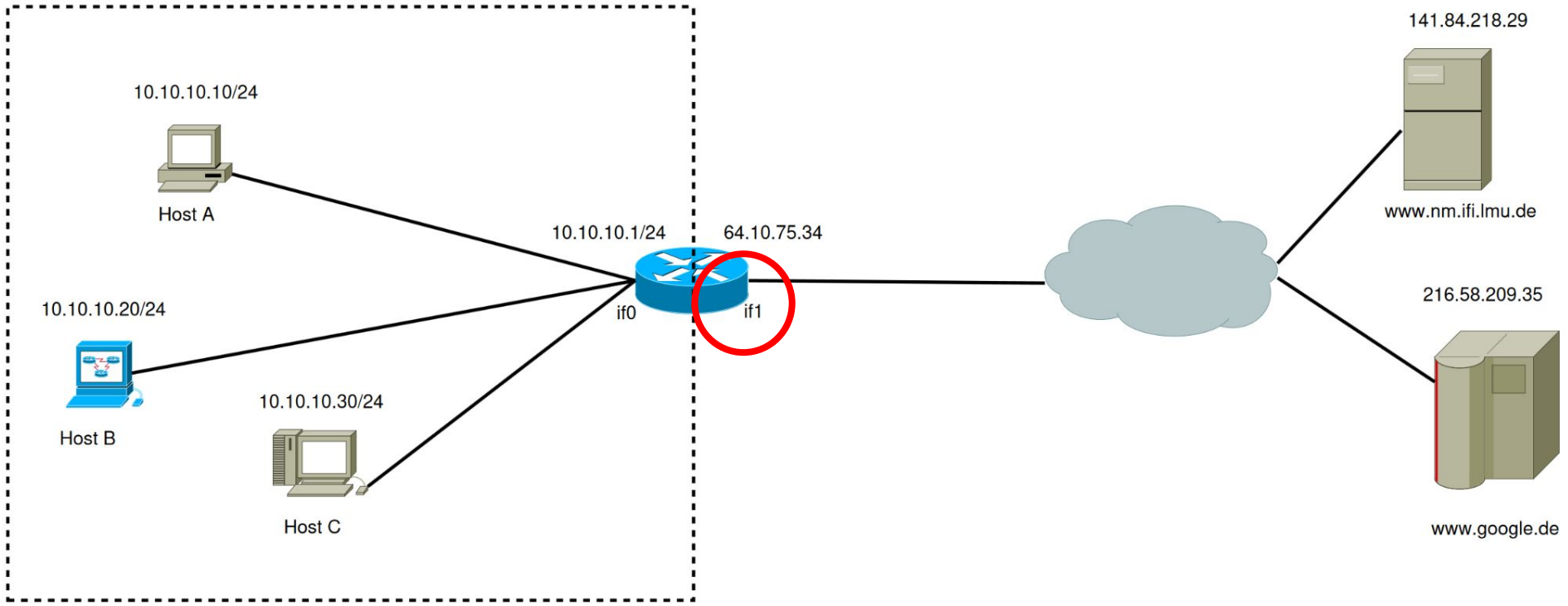


Quell-Adresse:
10.10.10.30/24
Port 43210
(zufällig zwischen 30000 und 60000)

Ziel-Adresse:
141.84.218.29
Port 80, da HTTP

Network Address Translation (NAT)

- Wie sehen Quell- und Ziel-Adresse der Anfrage aus, wenn das Paket vom Router in das öffentliche Netz weitergeleitet wird?



Quell-Adresse:
64.10.75.34
Port 56789
(könnte aber auch gleich sein)

Ziel-Adresse:
141.84.218.29
Port 80

Network Address Translation (NAT)

- Woher weiß der Router, dass das entsprechende Antwort-Paket vom öffentlichen Netz an Host C weitergereicht wird und nicht an einen anderen Client des privaten Netzes?

Der Router merkt sich die ursprüngliche Adresse sowie Port und speichert die Information in einer NAT-Tabelle

Network Address Translation (NAT)

NAT wird in der Literatur häufig auch als Sicherheitsmechanismus beschrieben, da die interne Netzinfrastruktur vollständig versteckt wird. Diskutieren Sie diese Aussage. Inwiefern bestätigt oder widerspricht dies dem wohlbekannten Prinzip *Separation of Concerns*?

- NAT ist konzeptionell nicht für Sicherheit gedacht, sondern zur Übersetzung von Adressen zwischen Netzen
- Verstecken von privaten Adressen kann trotzdem als Sicherheits-Mechanismus dienen

OSI-Modell (*Separation of Concerns*):

- NAT auf Schicht 3 (Vermittlungsschicht / Network Layer)
- Firewall für Netz-Sicherheit kann auf Schichten 2, 3, 4 oder noch höher liegen

Network Address Translation (NAT)

Mit der Einführung von IPv6 wird der verfügbare Adressraum (128 bit) vergrößert, was viele Konzepte von IPv4 obsolet macht. Theoretisch könnte jedes Gerät mit einer eindeutigen IP adressiert werden, was eine Kopplung aller Geräte im Internet untereinander problemlos ermöglicht. Gibt es für NAT unter IPv6 immer noch einen Einsatzzweck?

- NAT ist aktuell nicht mehr so relevant wie noch unter IPv4
- NAT erzeugt zusätzlichen Overhead
- IPv6 hat auch private Adressen, deren Prefix teilweise zufällig generiert ist
  → sehr unwahrscheinlich (siehe RFC 4193), dass zwei private Netze den gleichen Adressbereich nutzen und es zu einer Kollision beim Verbinden dieser kommt
- Üblicherweise haben Hosts neben privater auch globale IPv6 Adressen

Sicherheit bei IPv6:

- Firewall ist idR konfiguriert, um internes Netz zu schützen