Fragmentation

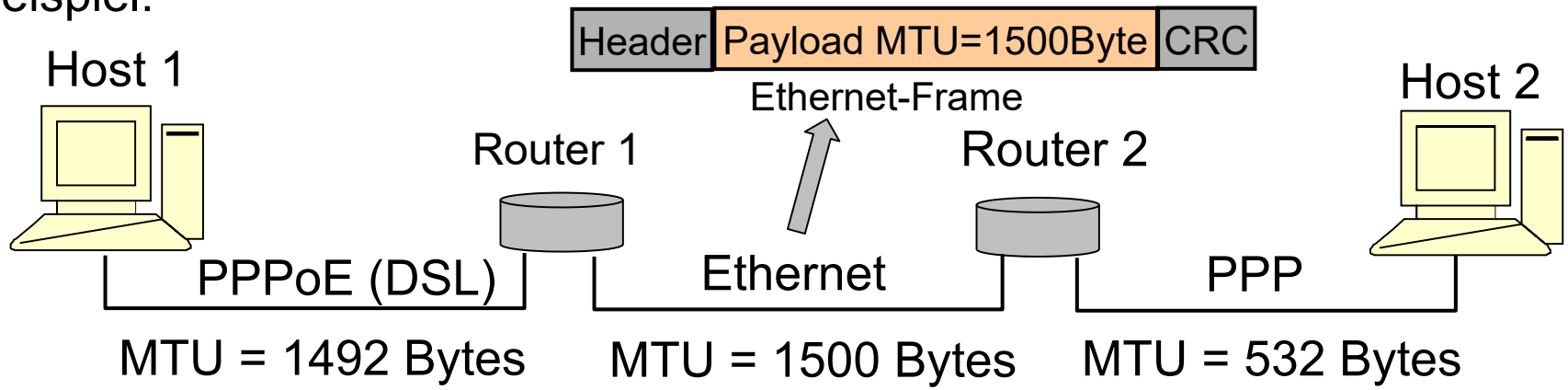
ARP

NAT

ICMP

Maximum Transfer Unit (MTU)

- Die MTU ist die maximale Datenmenge, die ein Rahmen der Data Link Layer transportieren kann
  - Die MTU umfasst das gesamte Datagramm (IP-Header und Nutzdaten)
- IP nutzt ggf. verschiedene Protokolle der Data Link Layer
- Beispiel:



Problem:

- Link-Abschnitte zum Ziel besitzen ggf. unterschiedliche MTUs

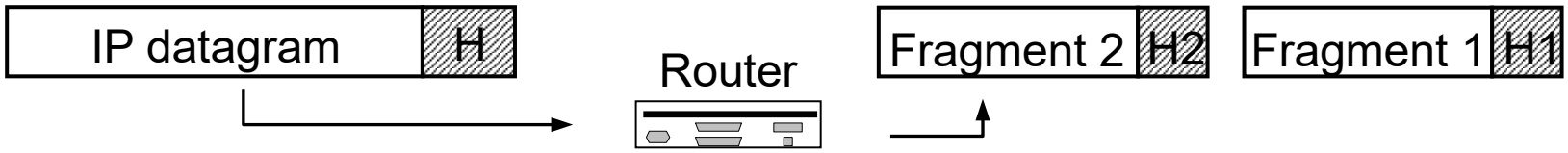
  → Das Datagramm kann größer sein als eine dieser MTUs

Problem:

- Datagramm ist größer als die MTU

Lösung:

- Fragmentierung des Datagramms



- Datagramm wird in kleinere Datagramme (Fragmente) zerlegen
- Fragmente werden unabhängig voneinander zum Ziel vermittelt
- Jedes Fragment ist ein eigenständiges Datagramm mit dupliziertem, aber modifiziertem Header
- Ein Datagramm kann mehrmals fragmentiert werden

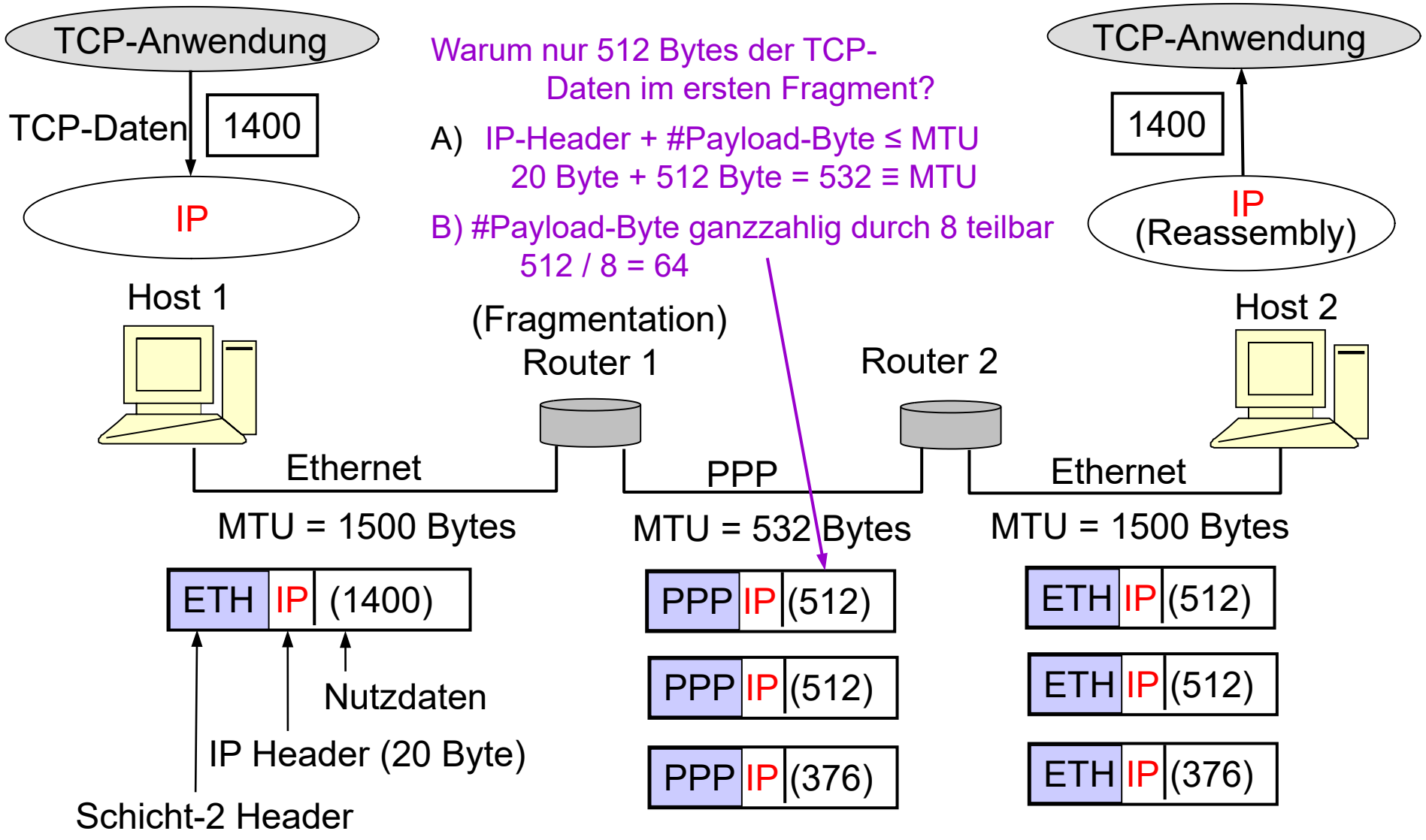
IP-Fragmentation (2)

- Fragmentierung des Datagramms kann erfolgen
  - in jedem Router
  - *prinzipiell auch im sendenden Host (gewöhnlich nicht verwendet)*
- Reassemblierung des Datagramms
  - Erst der Zielhosts setzt die fragmentierten Datagramme wieder zum ursprünglichen Datagramm zusammen
  - Der Zielhosts verwirft alle Fragmente eines Datagramms, wenn
    - nicht alle Fragmente innerhalb einer Zeitspanne ankommen
    - Fragmente fehlerhaft sind

Anmerkung

- Die path-MTU ist das Datagramm maximaler Größe, das entlang der gesamten Wegstrecke ohne Fragmentierung übertragen werden kann.
- Heute sollten alle TCP/IP Implementierungen eine MTU von 576 Byte unterstützen

Beispiel: IP-Fragmentation



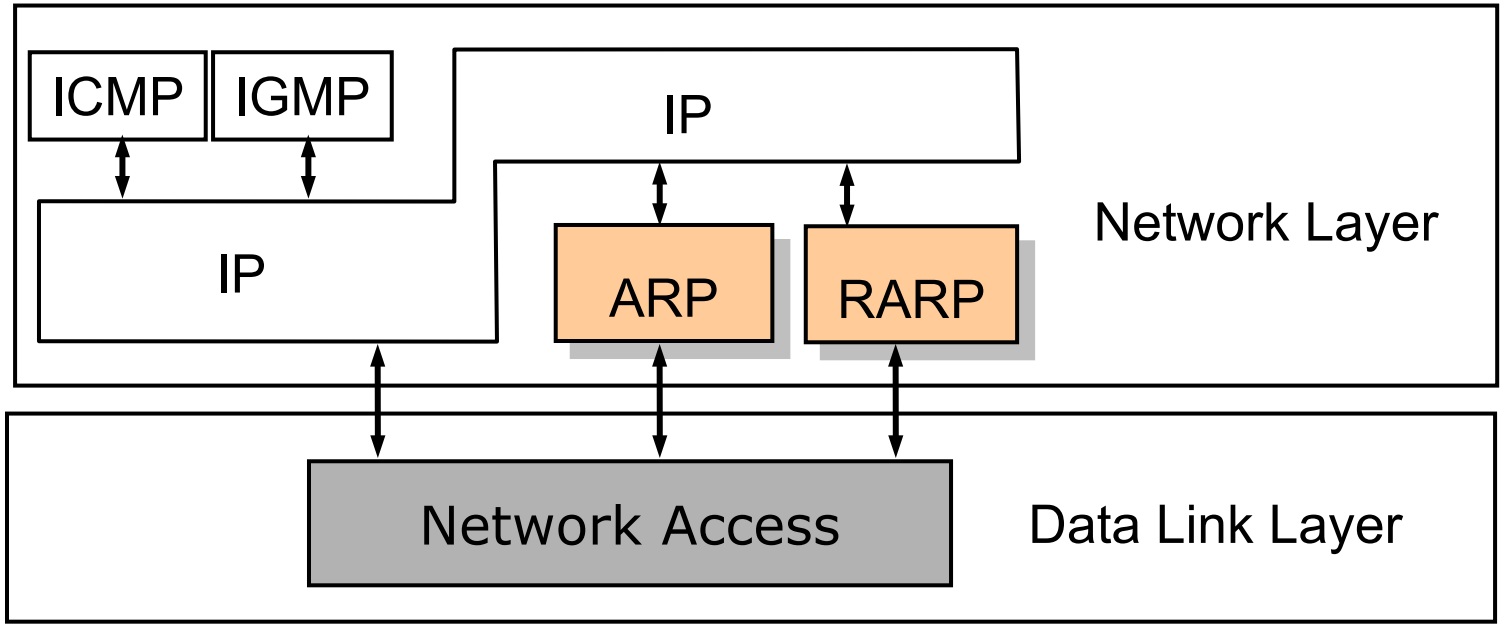
Fragmentation

ARP

NAT

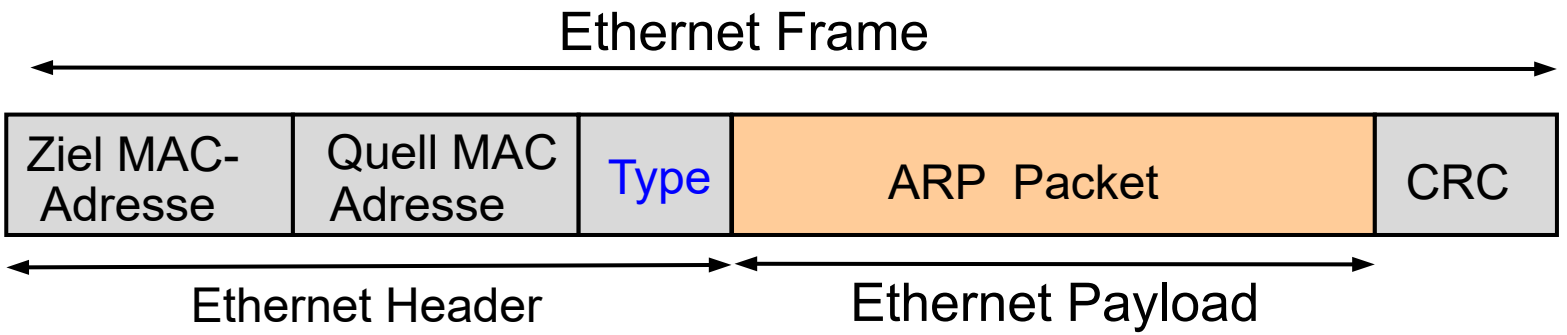
ICMP

Übersicht


ICMP
IGMP
IP
IP
ARP
RARP
Network Layer
Network Access
Data Link Layer

Beispiel: Ethernet LAN

- ARP und RARP Meldungen werden in den Frame des Data Link Layer Protocols eingebettet
- Beispiel: Ethernet Protocol



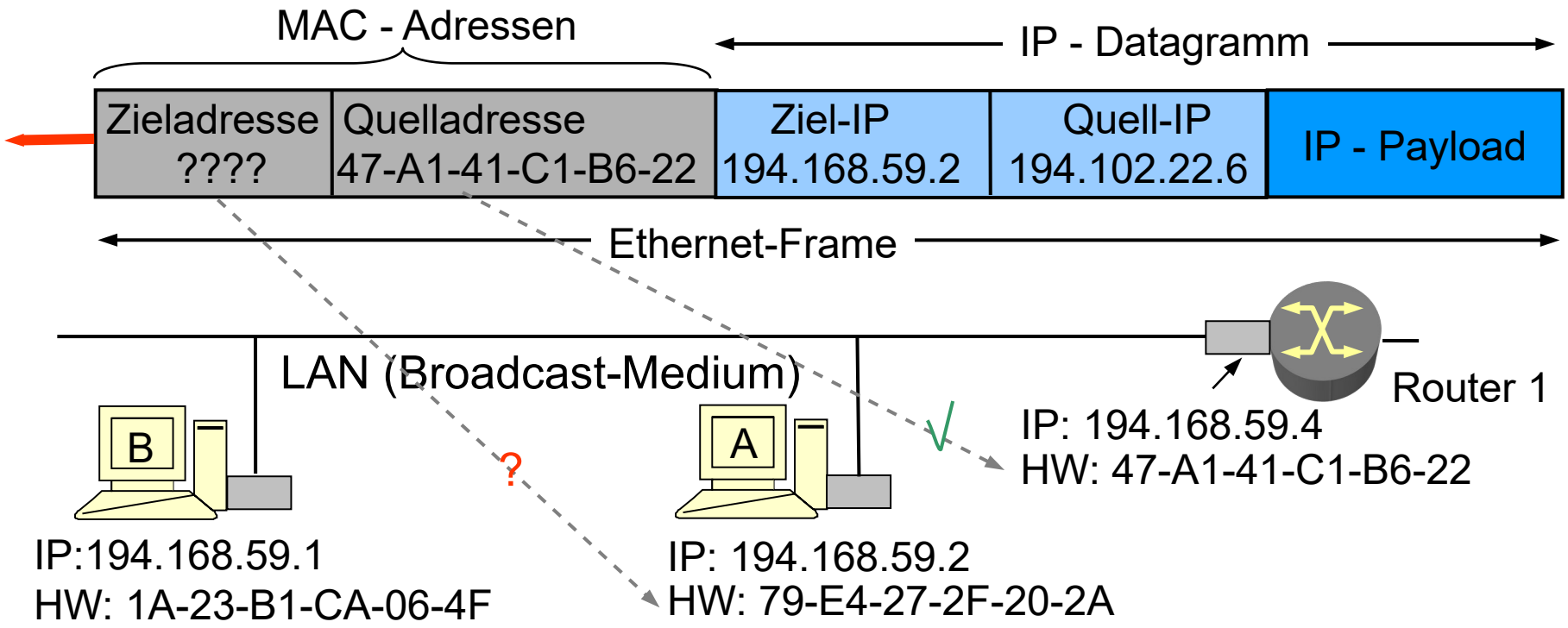
- Das Typfeld im Ethernet Frame wird für ARP auf 0x0806 (2054) gesetzt.
  - Dadurch lassen sich ARP-Pakete von Paketen anderer Protokolle wie beispielsweise IP unterscheiden.
- Meist Padding Bits erforderlich

Beispiel: Ethernet LAN (2)

- Alle Systeme sind durch ein Broadcast-Medium miteinander verbunden
- Jedes Interface hat eine eindeutige 48-bit (MAC) Hardware-Adresse

Aufgabe: Router 1 soll ein Datagramm des sendenden Hosts (Quell-IP 194.102.22.6) an Hosts A mit Ziel-IP 194.168.59.2 weiterleiten.

Problem: Wie lautet die Hardware (HW) - Adresse für die IP 194.168.59.2



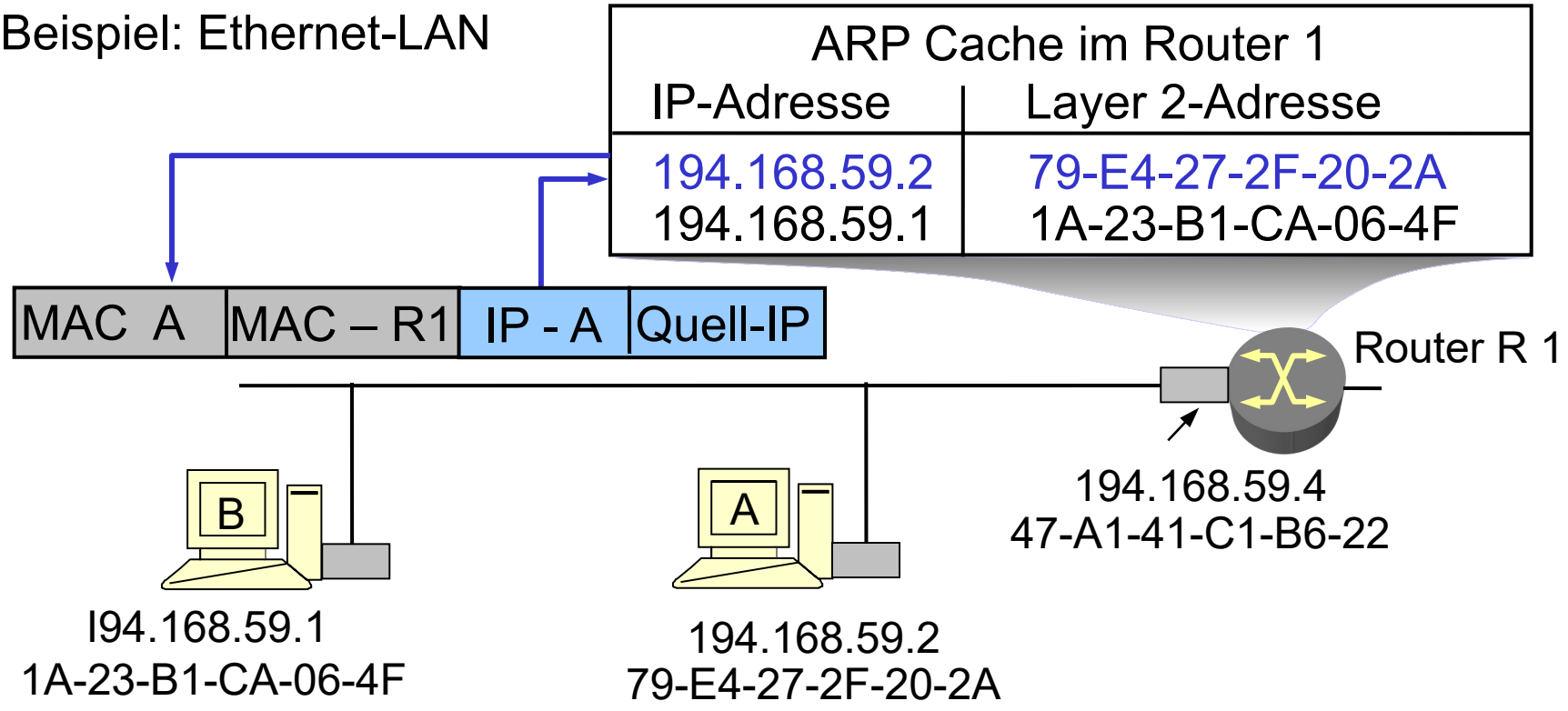
ARP Cache

- **Lösung:** Der ARP Cache (Adressumsetztabelle) liefert die Zuordnung

  IP-Adresse → Layer-2 Hardware-Adresse

  - ARP Cache wird automatisch durch das ARP-Protokoll erstellt
  - Einträge werden nach einem Zeitintervall gelöscht

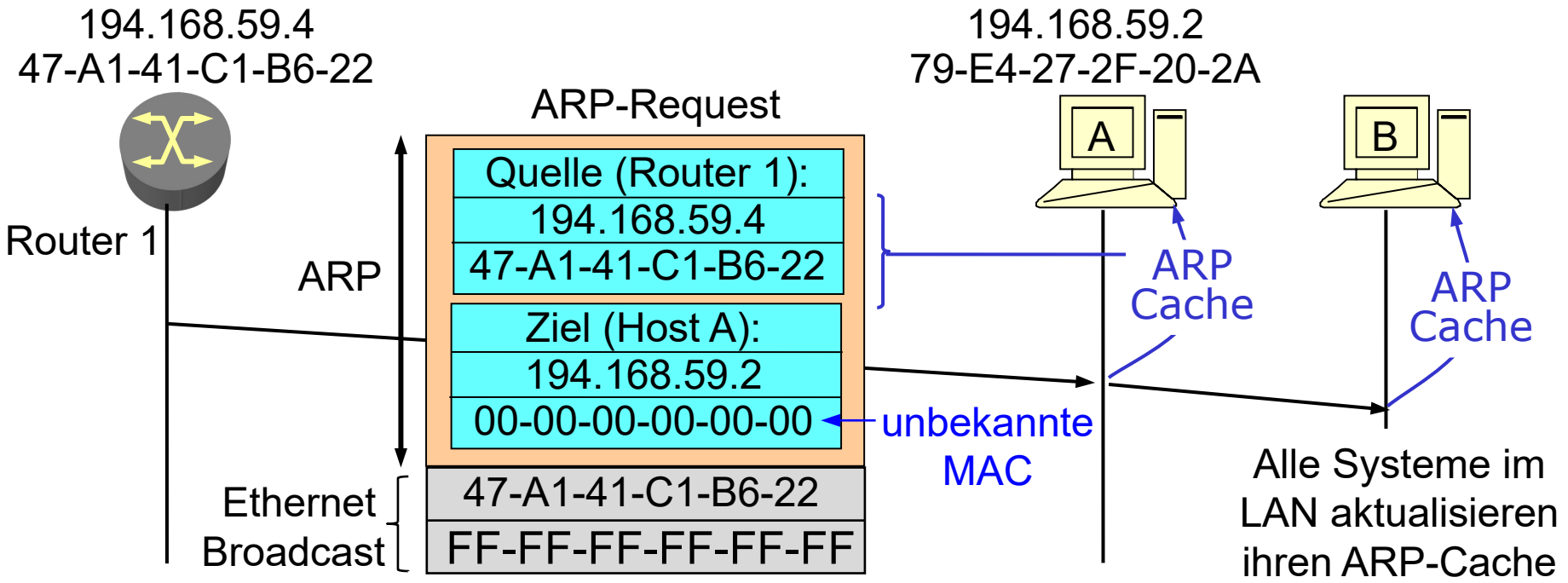
- Beispiel: Ethernet-LAN



Adresserkennung mittels ARP

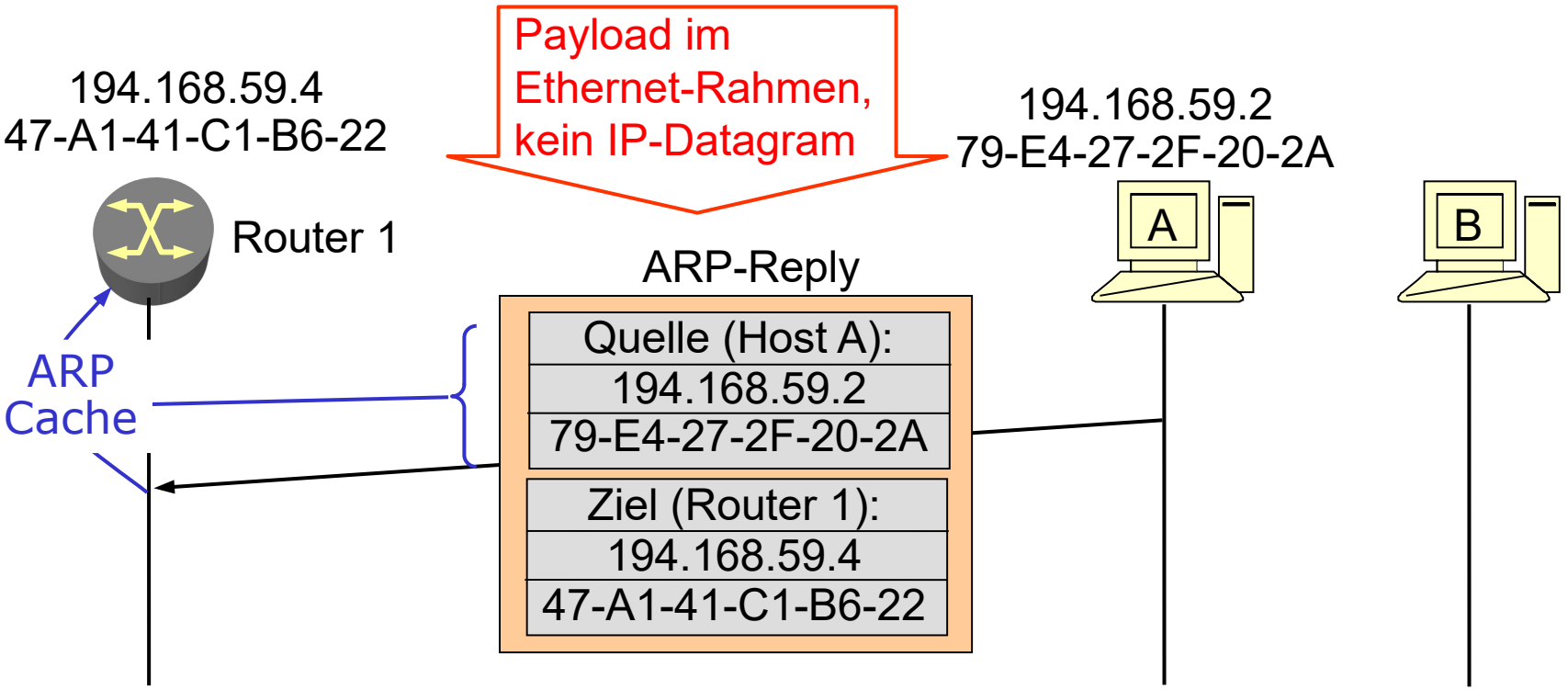
Problem: MAC Adresse von Host A nicht im ARP Cache vorhanden

- Router 1 sendet *ARP-Request* per LAN Broadcast an alle LAN-Systeme
  „Wie lautet die HW-Adresse von Host A“
- Host A erkennt seine eigene IP-Adresse im *ARP-Request*
  - *Quelle IP-Adresse* → *Quelle HW-Adresse* in ARP Cache von Host A



Adresserkennung mittels ARP (2)

- Host A schickt dem Router 1 ein *ARP-Reply*
  - Dieses enthält seine IP und Layer 2 Hardware– Adresse
- Router 1 kopiert aus dem *ARP-Reply* die Zuordnung
  - *Quelle IP-Adresse* → *Quelle HW-Adresse* in ARP Cache von Router 1



Eigenschaften von ARP

- ARP Pakete (Request und Reply) werden nicht authentifiziert
- ARP ist zustandslos → Ein Host kann ein ARP Reply ohne vorheriges ARP Request senden
- Gratuitous ARP Reply (unaufgefordertes ARP)
  - Ein Host sendet ein ARP Reply für seine eigene IP-Adresse
  - Er macht sich selbst im Netz bekannt (Broadcast im LAN)
- ARP-Update
  - Existiert für eine IP ein Eintrag im ARP-Cache, muss bei Empfang eines ARP- Paketes mit dieser IP ein Update des Eintrages erfolgen

Sicherheitsproblem

- Ein ARP Request oder Reply kann verwendet werden, um gezielt einen Eintrag im ARP-Cache zu verändern (ARP Poisoning)
- Dies ermöglich es, IP Verkehr auf einen anderen Host umzuleiten

Fragmentation

ARP

NAT

ICMP

Network Address Translation (NAT)

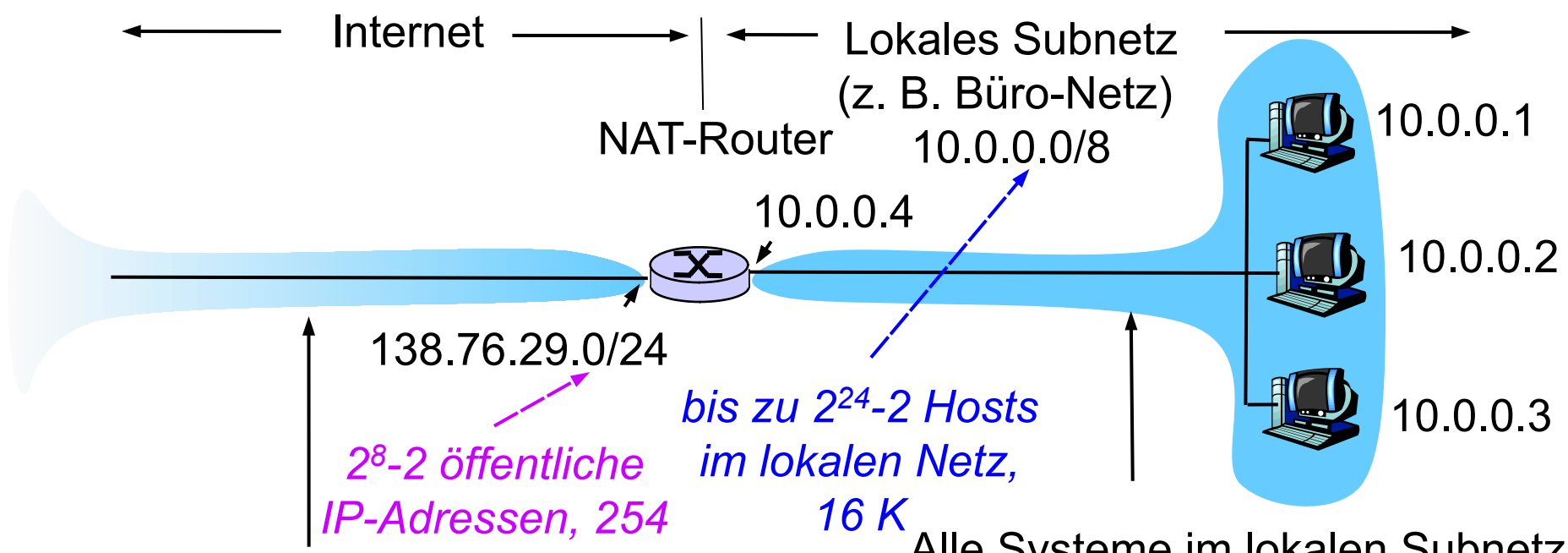
Probleme:

- P1: Der einem Unternehmen zugeteilte IP-Adress-Bereich ist begrenzt
  - Es sind mehr Systeme als vorhandene Adressen anzuschließen
- P2: Ein Unternehmen will die interne Netzwerkstruktur verbergen

Lösung: Network Address Translation (NAT)

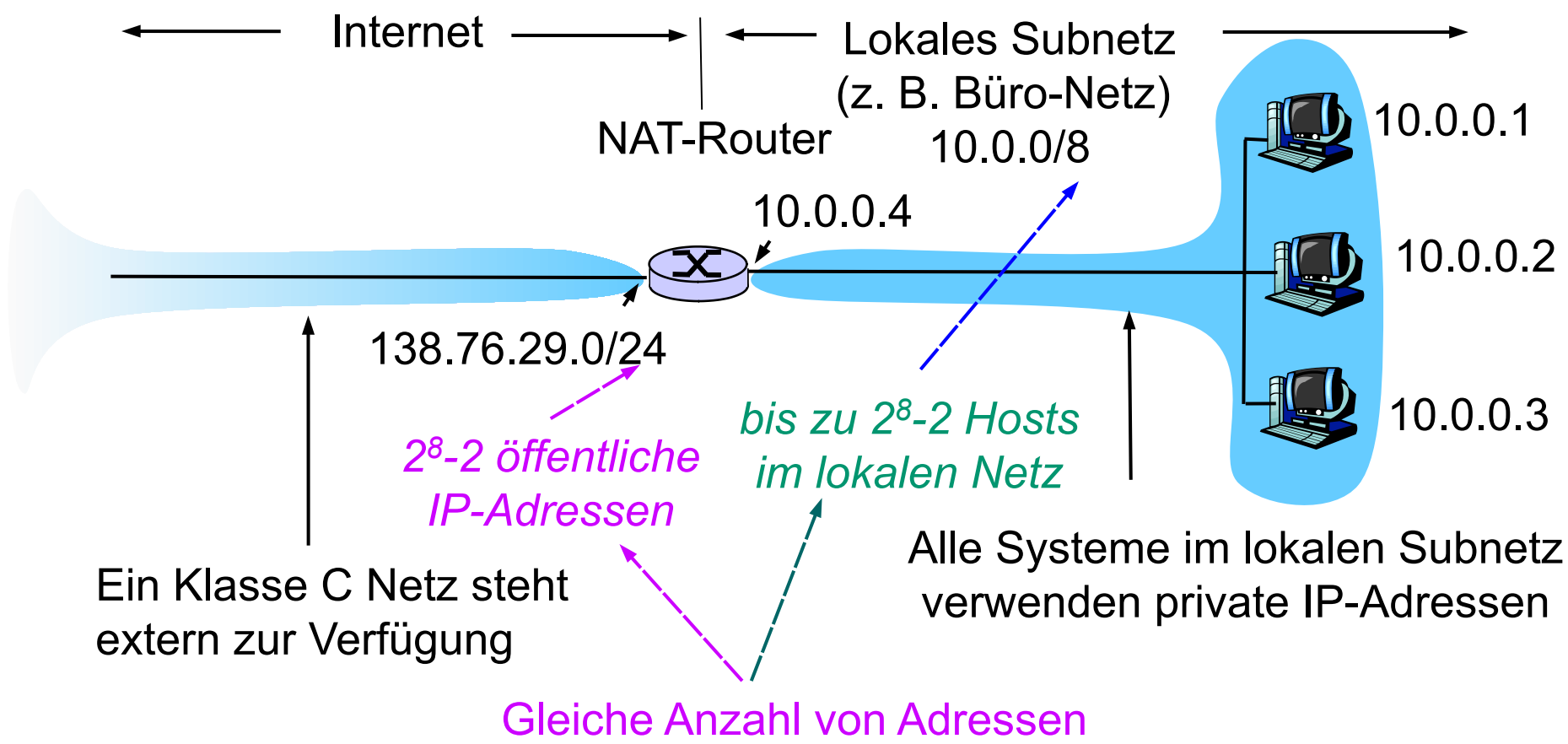
- NAT ist eine Funktion eines Routers, welche eine (private) IP-Adresse eines Datagramms gegen eine neue (öffentliche) Adresse ausgetauscht
- Ein NAT-Router befindet sich an der Netzwerkgrenze zwischen privatem und öffentlichem Internet
- L1: Unternehmen unterhält ein Netzwerk mit privaten IP- Adressen
  - Der private IP - Adressbereich wird im Internet nicht vermittelt
  - Der private Adressbereich ist weltweit nicht eindeutig
- L2: private IP - Adressen und die Netzstruktur innerhalb eines Netzwerkes können ohne Einfluss auf die Außenwelt (Routing) geändert werden

Beispiel: NAT (1)



Beispiel: NAT (2)

Frage: Warum wird NAT in diesem Beispiel angewendet?



Network Address Translation (NAT)

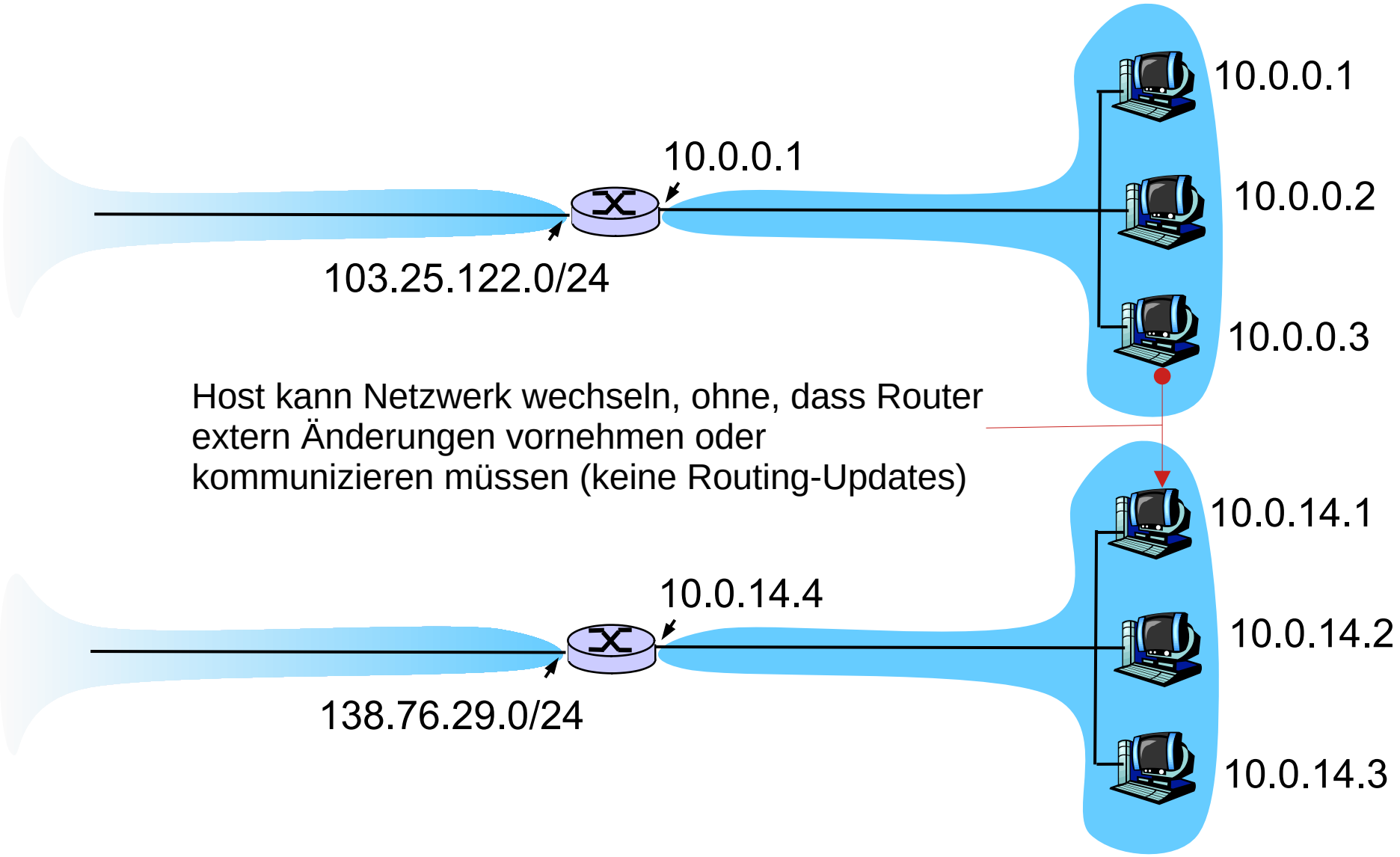
Probleme:

- P1: Der einem Unternehmen zugeteilte IP-Adress-Bereich ist begrenzt
  - Es sind mehr Systeme als vorhandene Adressen anzuschließen
- *P2: Ein Unternehmen will die interne Netzwerkstruktur verbergen*

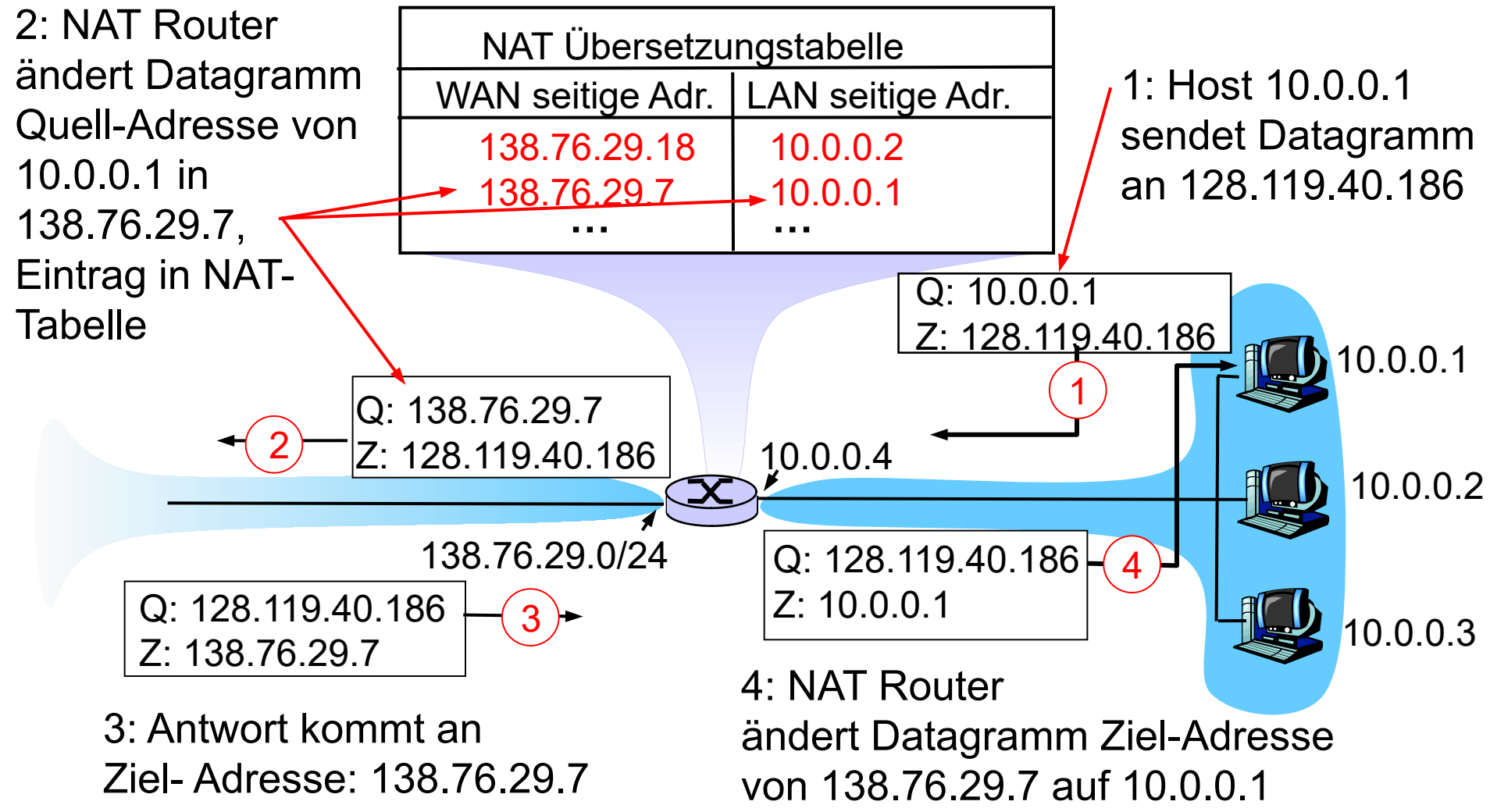
Lösung: Network Address Translation (NAT)

- NAT ist eine Funktion eines Routers, welche eine (private) IP-Adresse eines Datagramms gegen eine neue (öffentliche) Adresse ausgetauscht
- Ein NAT-Router befindet sich an der Netzwerkgrenze zwischen privatem und öffentlichem Internet
- L1: Unternehmen unterhält ein Netzwerk mit privaten IP- Adressen
  - Der private IP - Adressbereich wird im Internet nicht vermittelt
  - Der private Adressbereich ist weltweit nicht eindeutig
- *L2: private IP - Adressen und die Netzstruktur innerhalb eines Netzwerkes können ohne Einfluss auf die Außenwelt (Routing) geändert werden*

NAT – Mobility



Beispiel: NAT - detailliert



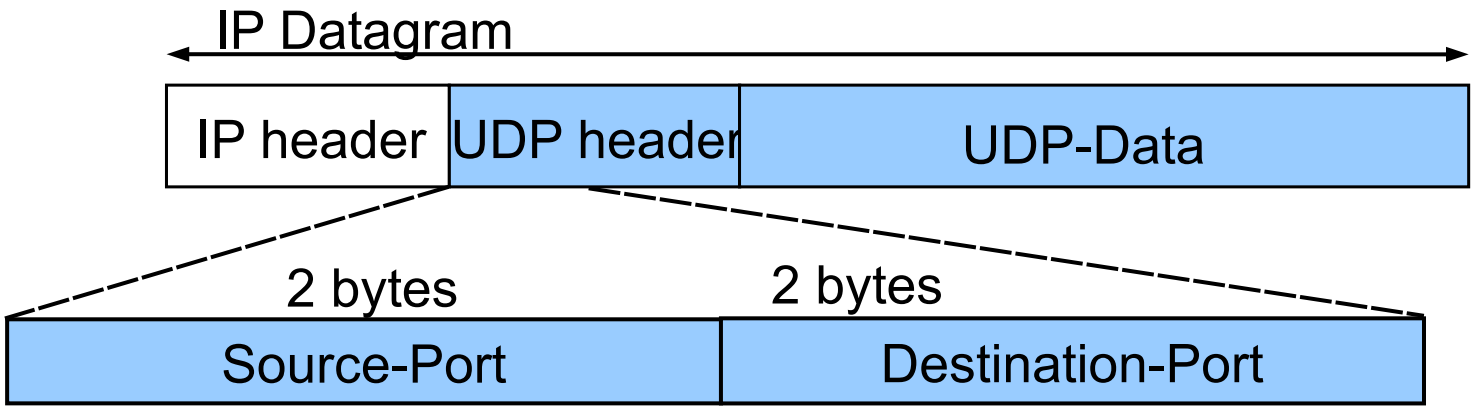
NAT Erweiterung -IP Masquerade

Problem

- Es steht nur eine einzige öffentliche IP- Adresse zur Verfügung
  - Diese repräsentiert ein gesamtes lokales Subnetz in der Außenwelt

Lösung

- Die (UDP) Port Nummern des Anwendungsprotokolls werden zur Unterscheidung der lokalen Systeme verwendet



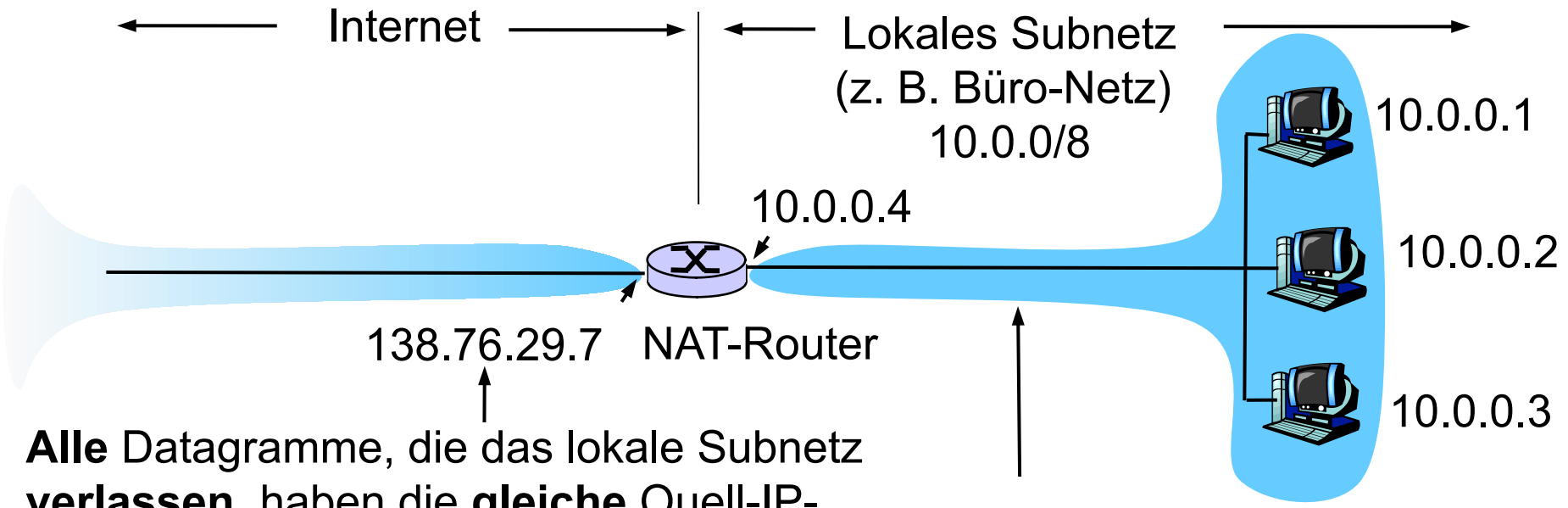
Source – Port / Destination - Port:

- Identifiziert Sende-/Empfangsprozess der Application-Layer
- Maximale Port Nummer ist 2^{16}-1= 65.535

NAT Erweiterung -IP Masquerade (2)

Network Address and Port Number Translation

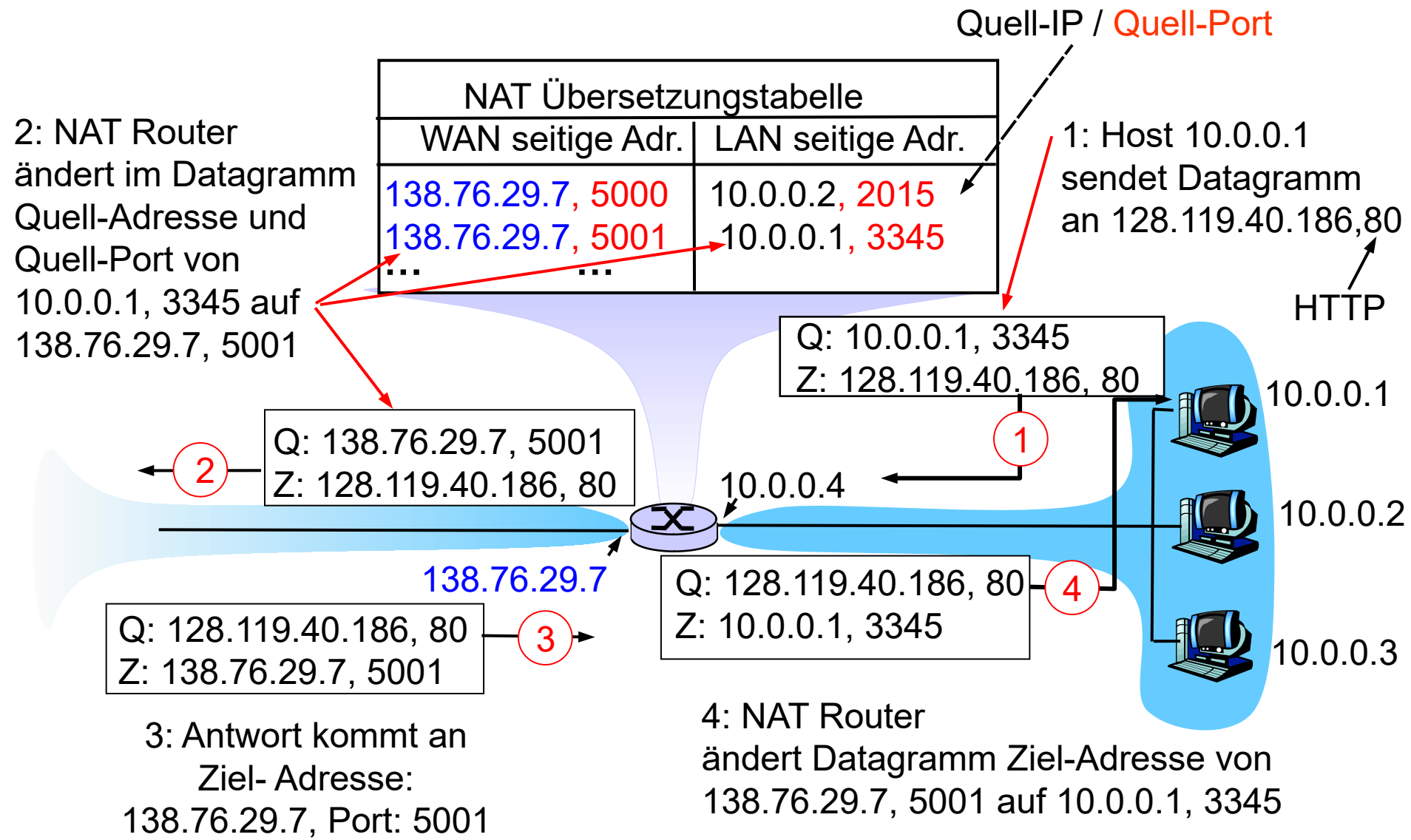
- Es wird nur eine öffentliche IP- Adresse verwendet
- Die (UDP) Quell-Port Nummer des Anwendungsprotokolls unterscheidet die lokalen Systeme



Alle Datagramme, die das lokale Subnetz **verlassen**, haben die **gleiche** Quell-IP-Adresse, aber verschiedene Quell-Port Nummern des Anwendungsprotokolls

Alle Systeme im lokalen Subnetz verwenden private IP-Adressen

Beispiel: IP Masquerade



Der NAT-Router muss folgende Aufgaben erfüllen

- Ausgehenden Datagramme
  - ersetze die Quell-IP-Adresse in jedem ausgehenden Datagramm

  (private Quell-IP-Adresse, Port#) → (NAT-IP-Adresse, neue Port#)
  - berechne neue IP-Header- / TCP / UDP - Prüfsumme

- NAT Übersetzungstabelle
  - erzeuge für jedes Adresspaar den Eintrag

  (private Quell-IP-Adresse, Port#) <--> (NAT-IP-Adresse, neue Port#)

- Eingehende Datagramme
  - ersetze die Ziel-IP-Adresse in jedem eingehenden Datagramm

  (Ziel-NAT-IP-Adresse, neue Port#) → (private Ziel-IP-Adresse, Port#)
  - berechne neue IP-Header- / TCP/UDP-Prüfsumme

Vorteil

- 16-Bit Port-Nummern Feld im UDP / TCP Protokoll
  - ca. 60.000 Verbindungen mit einer einzigen NAT-IP-Adresse möglich

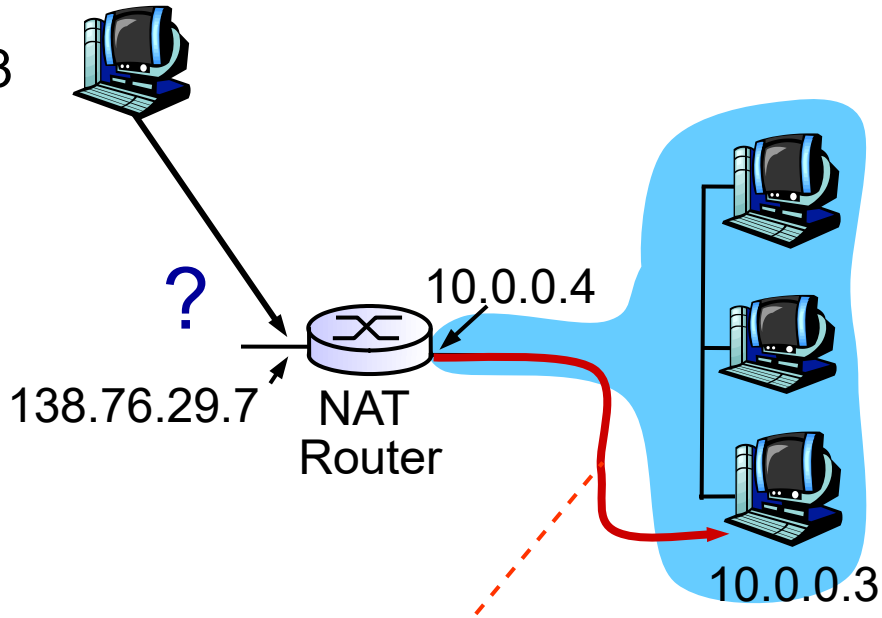
Nachteil

- NAT verletzt die Internet-Architektur
  - Router arbeiten nur bis zur Network Layer
  - geänderte Port-Adressen gehören zur Transport Layer
    → Router muss Transport Layer Protocol interpretieren
  - Ende-zu-Ende Applikationen müssen ggf. die Verwendung von NAT berücksichtigen
  - Ein Host im öffentlichen Internet kann meist keine Verbindung zu einem Host im privatem Netz herstellen
    - Problem für Peer-to-Peer Applikationen

NAT – Vor- und Nachteile

Problem

- External client wants to connect to internal server with address 10.0.0.3
  - client can't use server's private address 10.0.0.3 as destination address
  - only one external address is visible: 138.76.29.7



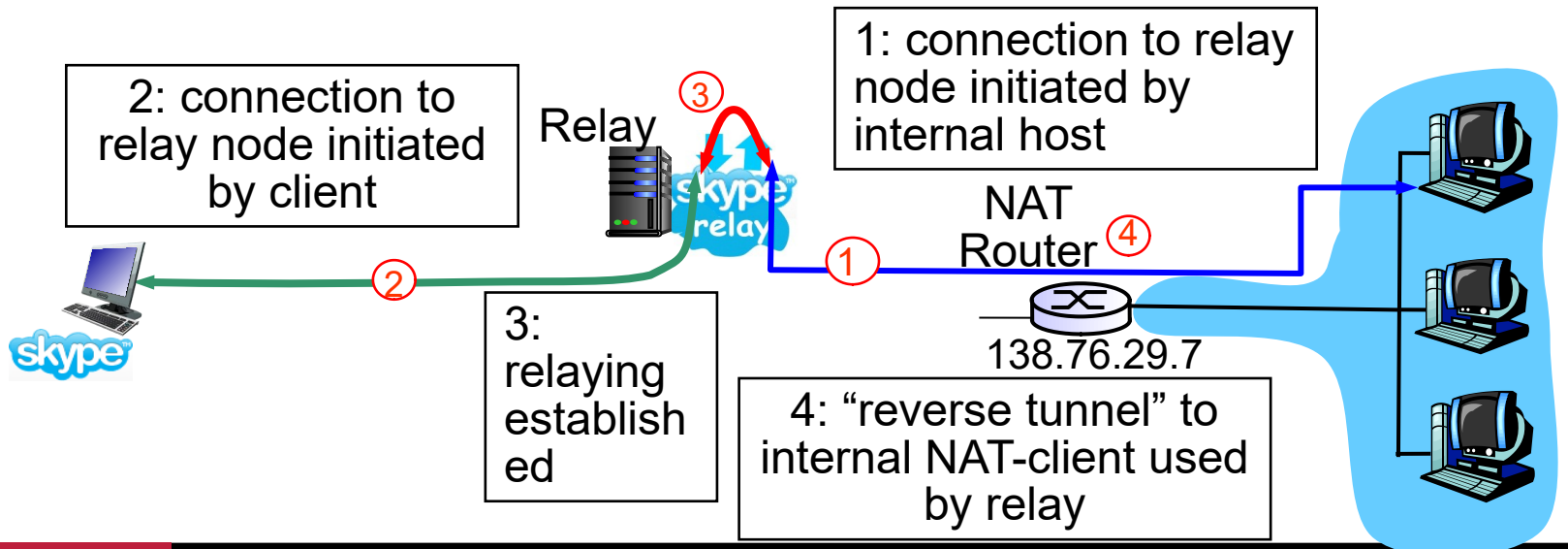
Solution: Port forwarding

- Statically configure NAT to forward incoming connection requests at given port to server
  - e.g., [138.76.29.7, port 2500] always forwarded to [10.0.0.3 port 5500]

NAT with External Relay

Solution: External relay server

- Principle used by Skype (automatic registration to external super-node)
- Der interne Client stellt eine Verbindung zum externe Relay-Knoten her:
  - registiert seine privat-Adresse und die Port-nummer am Relay-Knoten
  - der Relay-Knoten kennt die Zuordnung innerhalb der NAT-Router Ubersetzungstabelle
- Der externe Client verbindet zum Relay-Knoten.
- Der Relay-Knoten überbrückt Pakete zwischen den Verbindungen
  - benutzt “reverse tunnel” zum internen Klient



Fragmentation

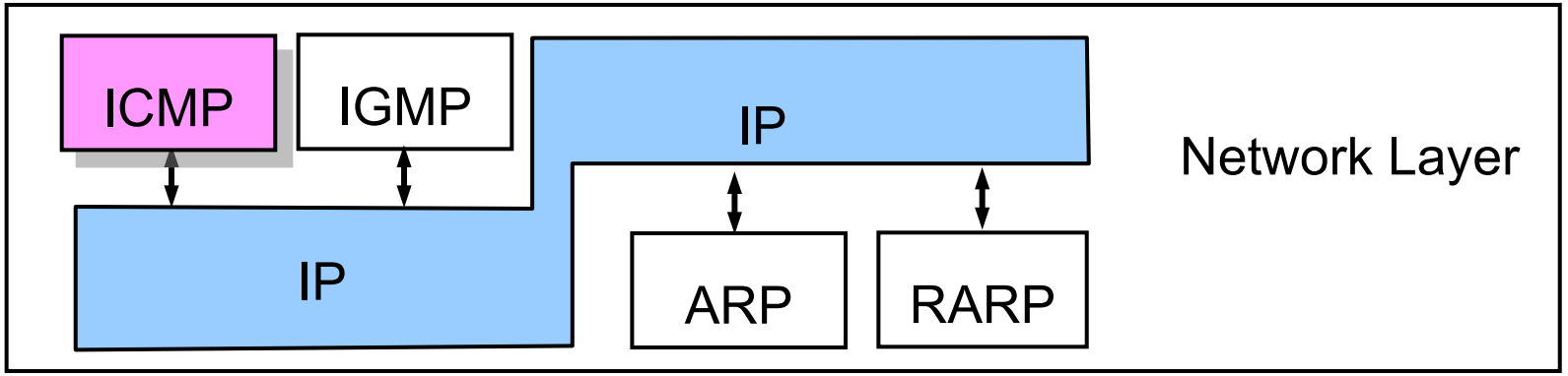
ARP

NAT

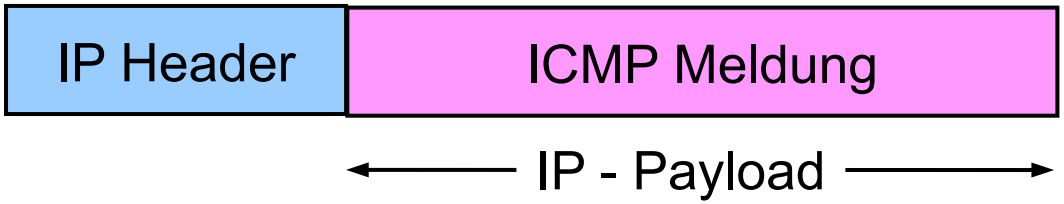
ICMP

Übersicht

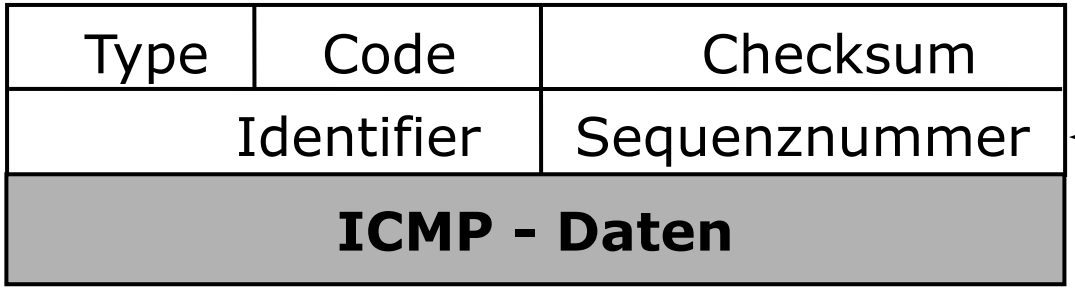
- Das ICMP Protokoll unterstützt das IP – Protokolls und ermöglicht:
  - Austausch von Fehlermeldungen
  - einfache Anfragen und Meldungen



- ICMP Meldungen werden in IP Datagrammen übermittelt



Internet Control Message Protocol (ICMP)



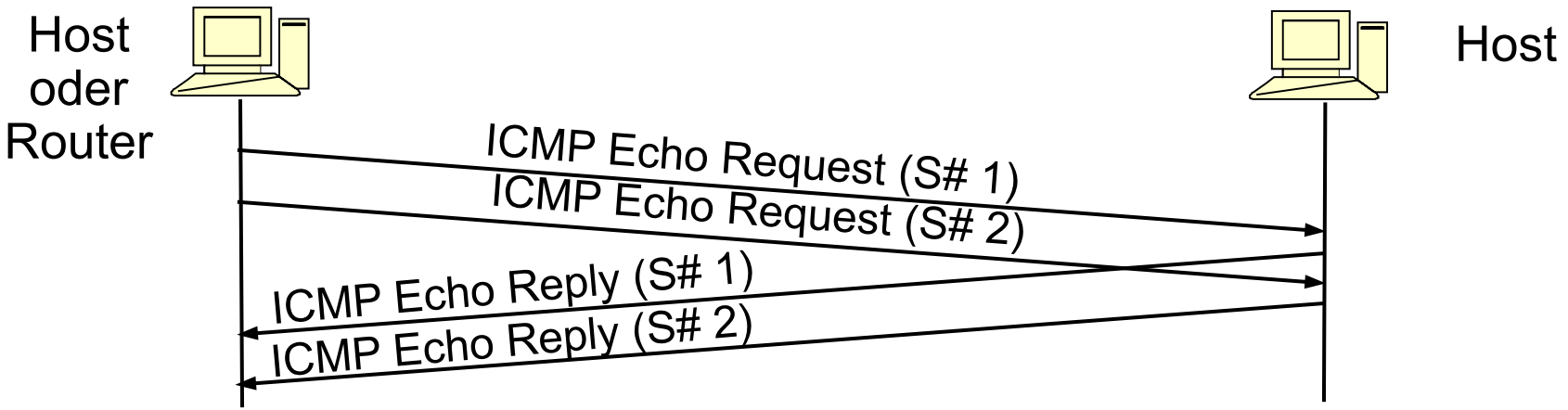
ICMP – Format für Meldungen, die ein Host sendet

- Type (1 Byte): Typ der ICMP Message
- Code (1 Byte): Untertyp der ICMP Message
- Checksum (2 Byte): ähnlich wie IP-Header Prüfsumme, wird über ganze ICMP Message berechnet
- Identifier: eindeutige Kennung der gesendeten ICMP-Message
- Sequenznummer: wird für Meldungen gleichen Typs hochgezählt
- ICMP – Daten: Abhängig vom Message-Typ: häufig IP-Header+ erste 8 Byte des IP-Datagramms, das zu einer Fehlermeldung führte

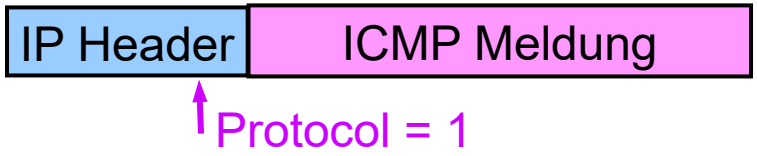
Internet Control Message Protocol (ICMP)

Befehl: „**ping Ziel-IP-Adresse**“ *„Ist der Host im Netzwerk erreichbar?“*

- **ICMP - Request:**
  - Host oder Router sendet „echo request“ an einen Zielhost
- **ICMP - Reply:**
  - Zielhost schickt „echo reply“ an die Quelle zurück
  - Quelle gibt die gemessene RTT aus
- Anmerkung: Sequenznummer und Identifier einer ICMP-Reply Message haben den gleichen Wert wie die ICMP Request Message



Internet Control Message Protocol (ICMP)



- Einige Beispiele für ICMP Meldungen

Typ	Code	Beschreibung	
0	0	echo reply (ping)	
3	0	dest. network unreachable	typische Fehlermeldungen
3	1	dest host unreachable	
3	3	dest port unreachable	
3	6	dest network unknown	
3	7	dest host unknown	
8	0	echo request (ping)	
9	0	route advertisement	
10	0	router discovery	typische Fehlermeldungen
11	0	TTL expired	