Protokollstapel TCP/IP

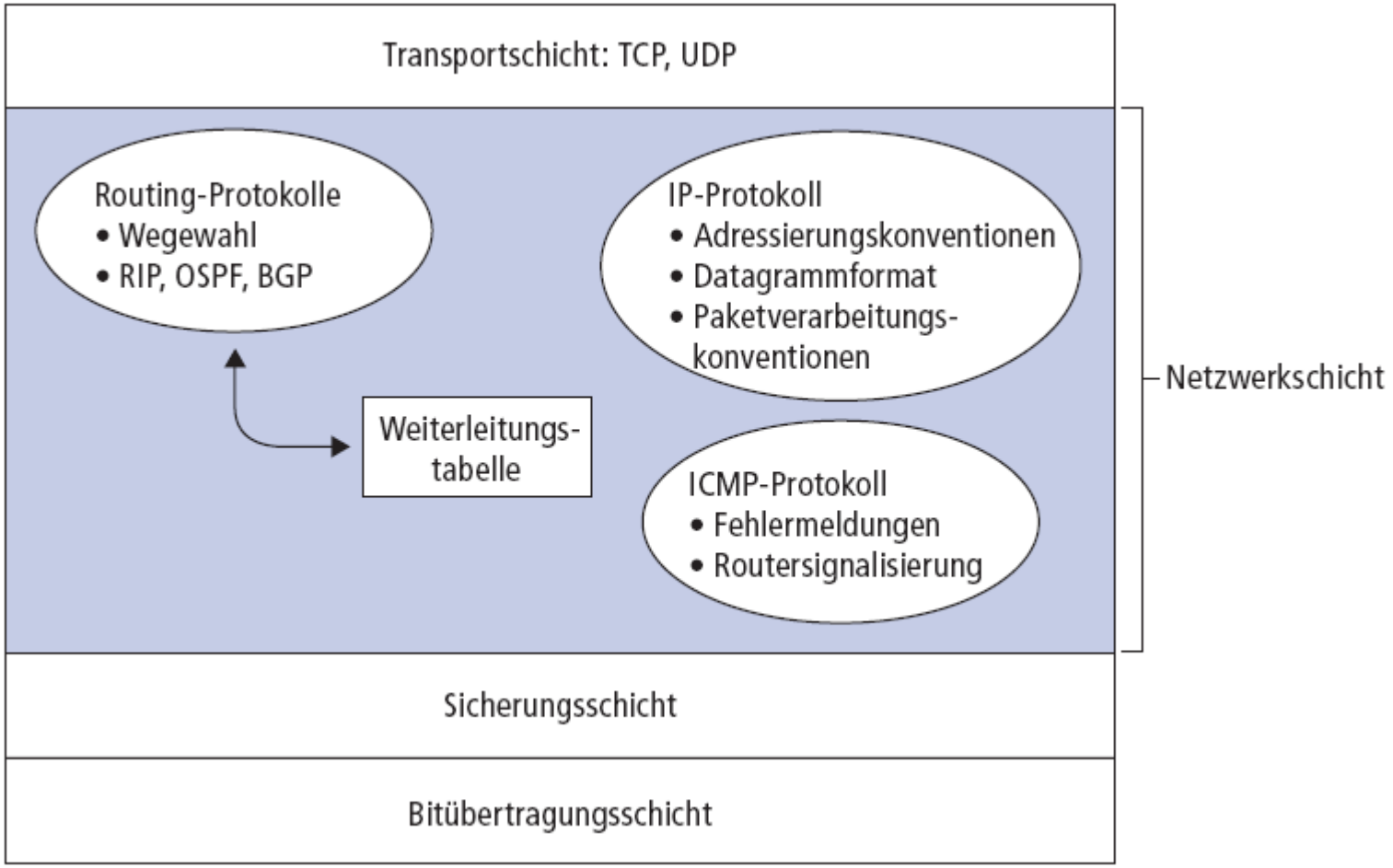
- Anwendungsschicht: Unterstützung von Netzwerkanwendungen
  - FTP, SMTP, HTTP
- Transportschicht: Datentransfer zwischen Prozessen
  - TCP, UDP
- Netzwerkschicht (auch Vermittlungsschicht): Weiterleiten der Daten von einem Sender zu einem Empfänger
  - IP, Routing-Protokolle
- Sicherungsschicht: Datentransfer zwischen benachbarten Netzwerksystemen
  - PPP, Ethernet
- Bitübertragungsschicht: Bits auf der Leitung

We reject kings, presidents and voting. We believe in rough consensus and running code (Dave Clark)

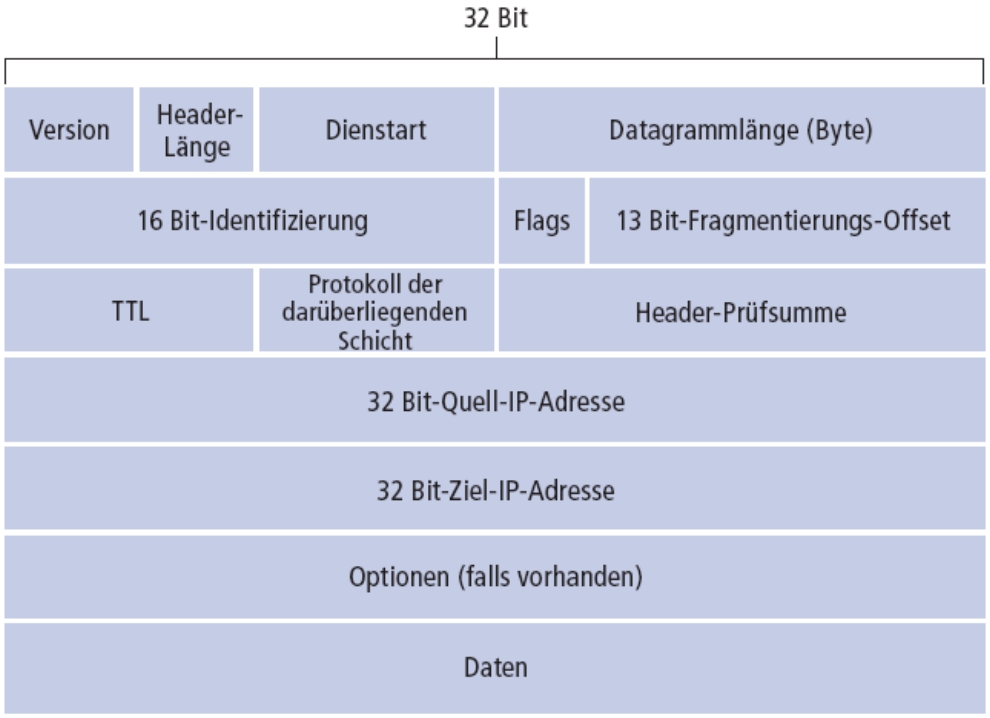
T-Shirt IETF

Die Netzwerkschicht des Internets

Funktionalität in Hosts und Routern:



IP-Datagrammformat



Wie viel Overhead entsteht bei Verwendung von TCP?

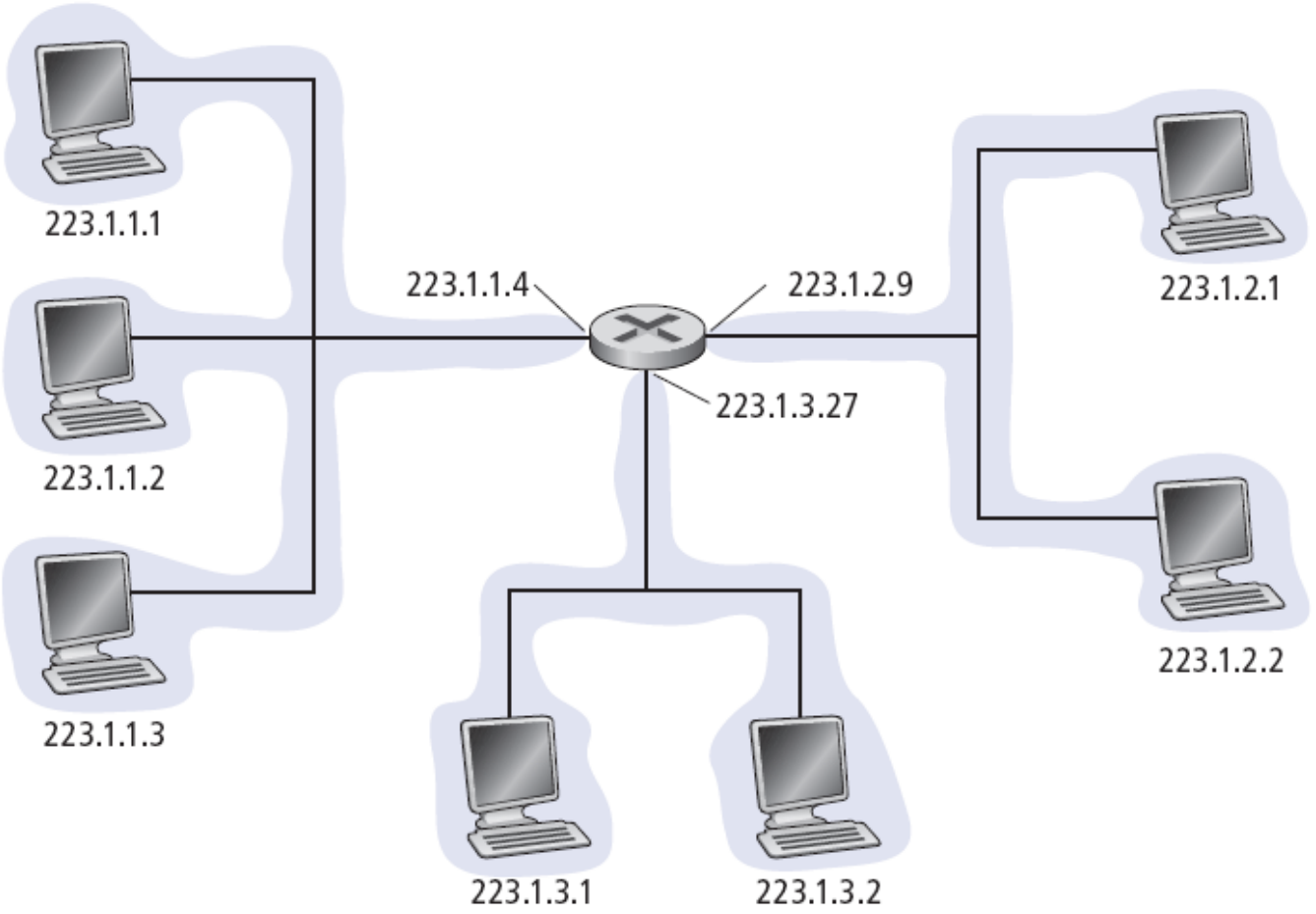
- 20 Byte für den TCP-Header, 20 Byte für den IP-Header
- = 40 Byte + Overhead auf der Anwendungsschicht

IP-Fragmentierung

Beispiel: IP-Datagramm mit 4000 Byte (inklusive 20 Byte IP-Header)

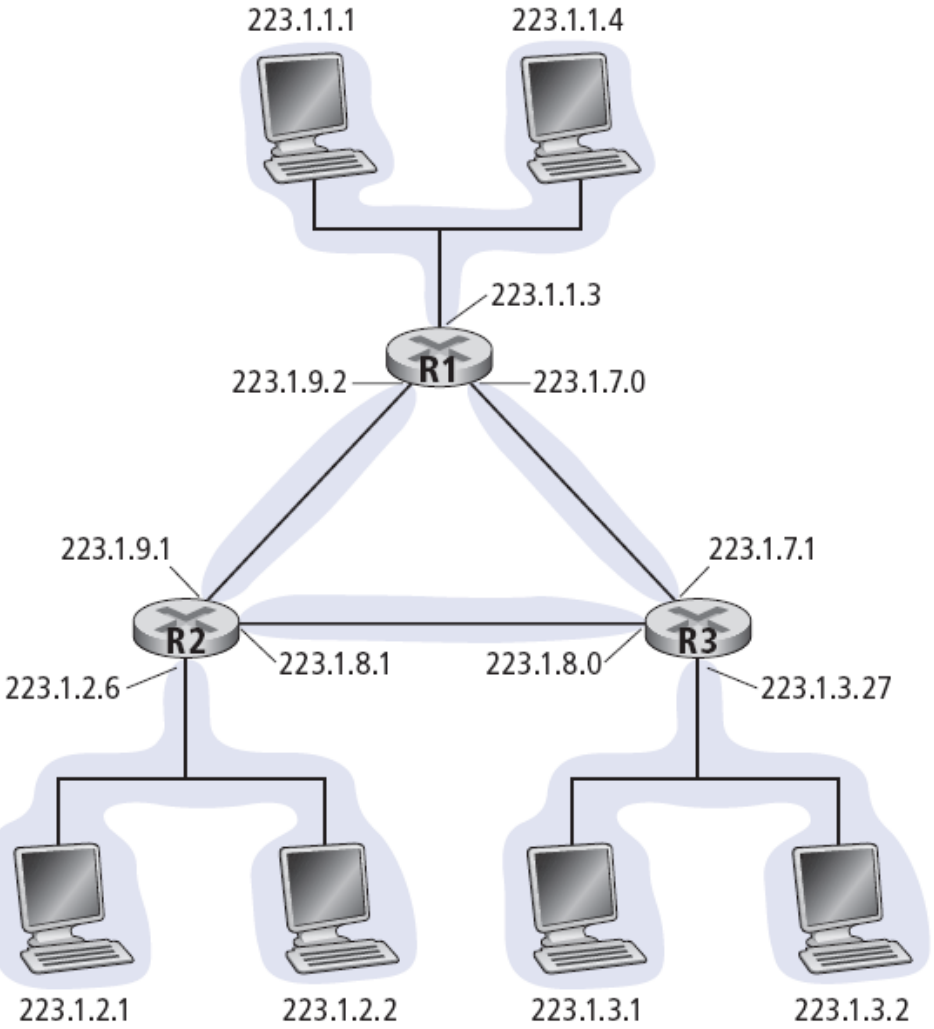
Fragment	Bytes	ID	Offset	Flag
1. Fragment	1.480 Byte im Datenfeld des IP-Datagramms	Identifizierung = 777	Offset = 0 (d.h., die Daten sollten beginnend bei Byte 0 eingefügt werden)	Flag = 1 (d.h., da kommt noch mehr)
2. Fragment	1.480 Datenbytes	Identifizierung = 777	Offset = 185 (d.h., die Daten sollten bei Byte 1.480 beginnend eingefügt werden; beachten Sie, dass 185 · 8 = 1.480)	Flag = 1 (d.h., da kommt noch mehr)
3. Fragment	1.020 Datenbytes (= 3.980 – 1.480 – 1.480)	Identifizierung = 777	Offset = 370 (d.h., die Daten sollten beginnend bei Byte 2.960 eingefügt werden; beachten Sie, dass 370 · 8 = 2.960)	Flag = 0 (d.h., es ist das letzte Fragment)

IP-Adressierung – Grundlagen



Wie viele Subnetzwerke sehen Sie?

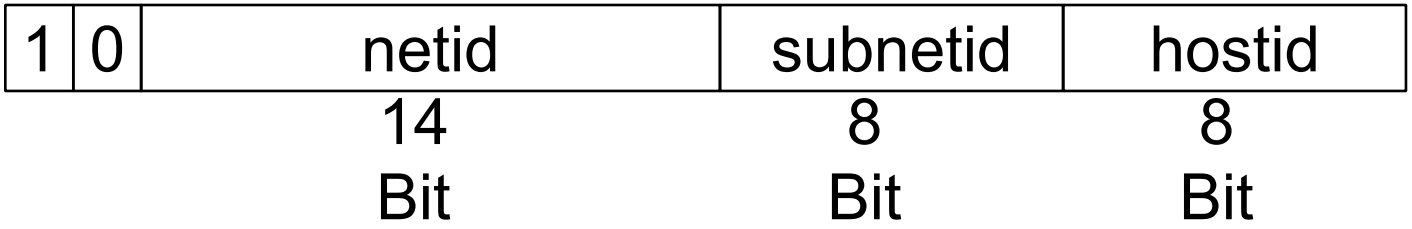
Fakultät für Feinwerk- und Mikrotechnik, Physikalische Technik
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN · FH MÜNCHEN



Adressierung von Subnetzen I

- Klasse-A- und –B-Adressen haben Platz für mehr Endsysteme, als man in einem Netzwerk sinnvoll unterbringen kann
- Daher teilt man die hostid weiter auf, z.B. so:

Klasse B:



- Die Unterteilung (subnetid, hostid) ist eine lokale Entscheidung und wird von der Organisation vorgenommen, der die netid zugeordnet wurde

Adressierung von Subnetzen III

- Subnetzmaske (subnet mask)
  - Wird für jede IP-Adresse eines Systems im System gespeichert
  - Sie identifiziert, welcher Teil der Adresse zur subnetid und welcher zur hostid gehört

- Die eigene IP-Adresse in Verbindung mit der Subnetzmaske erlaubt Rückschlüsse darüber, wo sich eine andere IP-Adresse befindet:
  - im selben Subnetz (also direkt erreichbar)
  - im selben Netzwerk, aber in einem anderen Subnetz
  - in einem anderen Netzwerk

Beispiel für die Verwendung von Subnetzmasken

- Gegeben:
  - Eigene IP-Adresse: 134.155.48.10
  - Subnetzmaske: 255.255.255.0
  - Adresse A: 134.155.48.96, Adresse B: 134.155.55.96

- Überprüfen der beiden Adressen:
  - 134.155.48.10 & 255.255.255.0 = 134.155.48.0
  - 134.155.48.96 & 255.255.255.0 = 134.155.48.0 identisch, gleiches Subnetz
  - 134.155.55.96 & 255.255.255.0 = 134.155.55.0 verschieden, anderes Subnetz

Subnetzmasken variabler Länge

- Problem: Gegeben sei ein Klasse-C-Netzwerk, welches in zwei Subnetze mit 50 Endsystemen und ein Subnetz mit 100 Endsystemen unterteilt werden soll.
- Das funktioniert nicht mit einer einzelnen Subnetzmaske!
  - 255.255.255.128: zwei Netze mit je 128 hostids
  - 255.255.255.192: vier Netze mit je 64 hostids
- Lösung: Subnetzmasken variabler Länge
  - Unterteile den Adressraum zunächst mit der kürzeren Subnetzmaske (1 Bit im Beispiel)
  - Unterteile eine Hälfte davon weiter mit der längeren Subnetzmaske (2 Bit im Beispiel)
  - Resultat: Subnetze verschiedener Größe

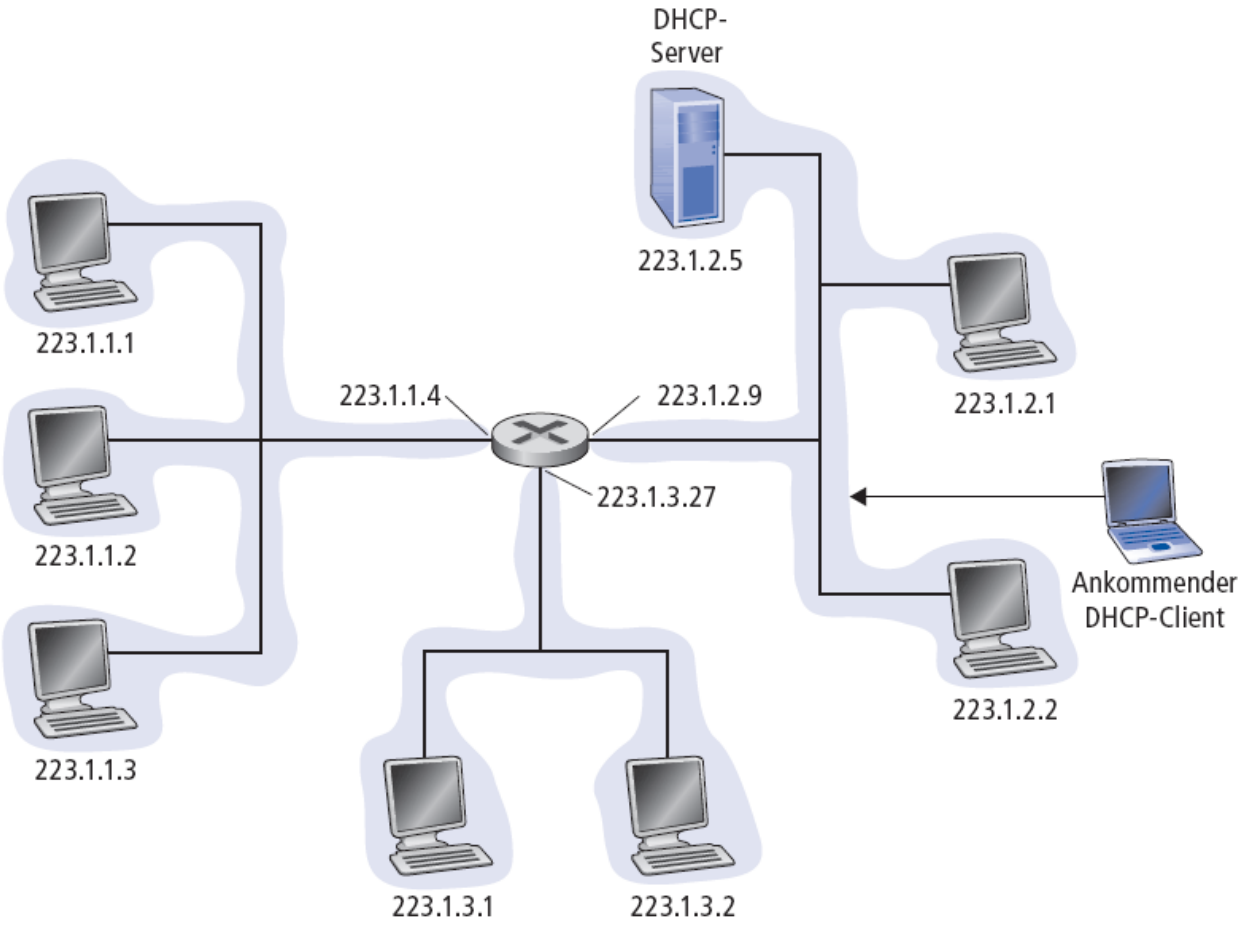
Adressvergabe - Hosts

Fakultät für Feinwerk- und Mikrotechnik, Physikalische Technik
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN · FH MÜNCHEN

Frage: Wie bekommt ein Host seine IP-Adresse?

- Durch manuelle Konfiguration:
  - IP-Adresse
  - Subnetzmaske
  - Weitere Parameter
- DHCP: Dynamic Host Configuration Protocol: dynamisches Beziehen der Adresse von einem Server
  - “Plug-and-Play”

DHCP-Szenario

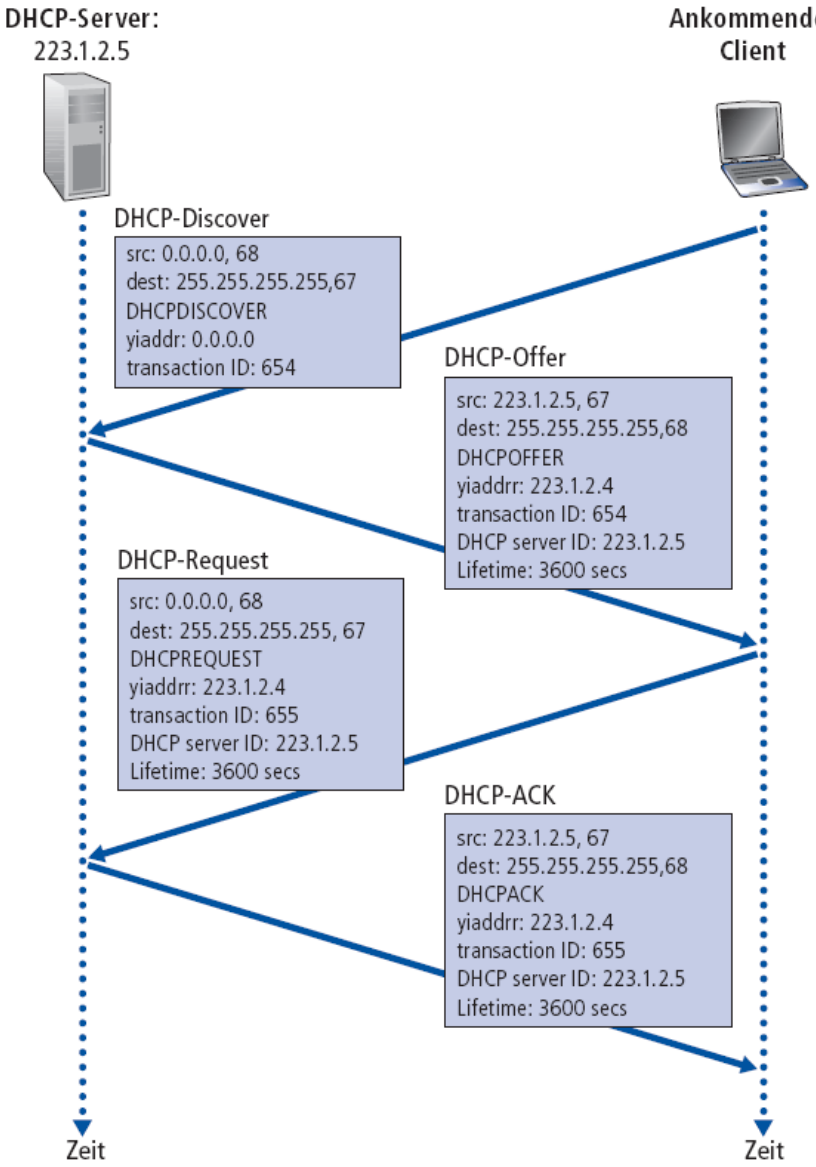


DHCP-S

DHCP verwendet UDP.

DHCP-Nachrichten werden an die MAC-Broadcast-Adresse geschickt.

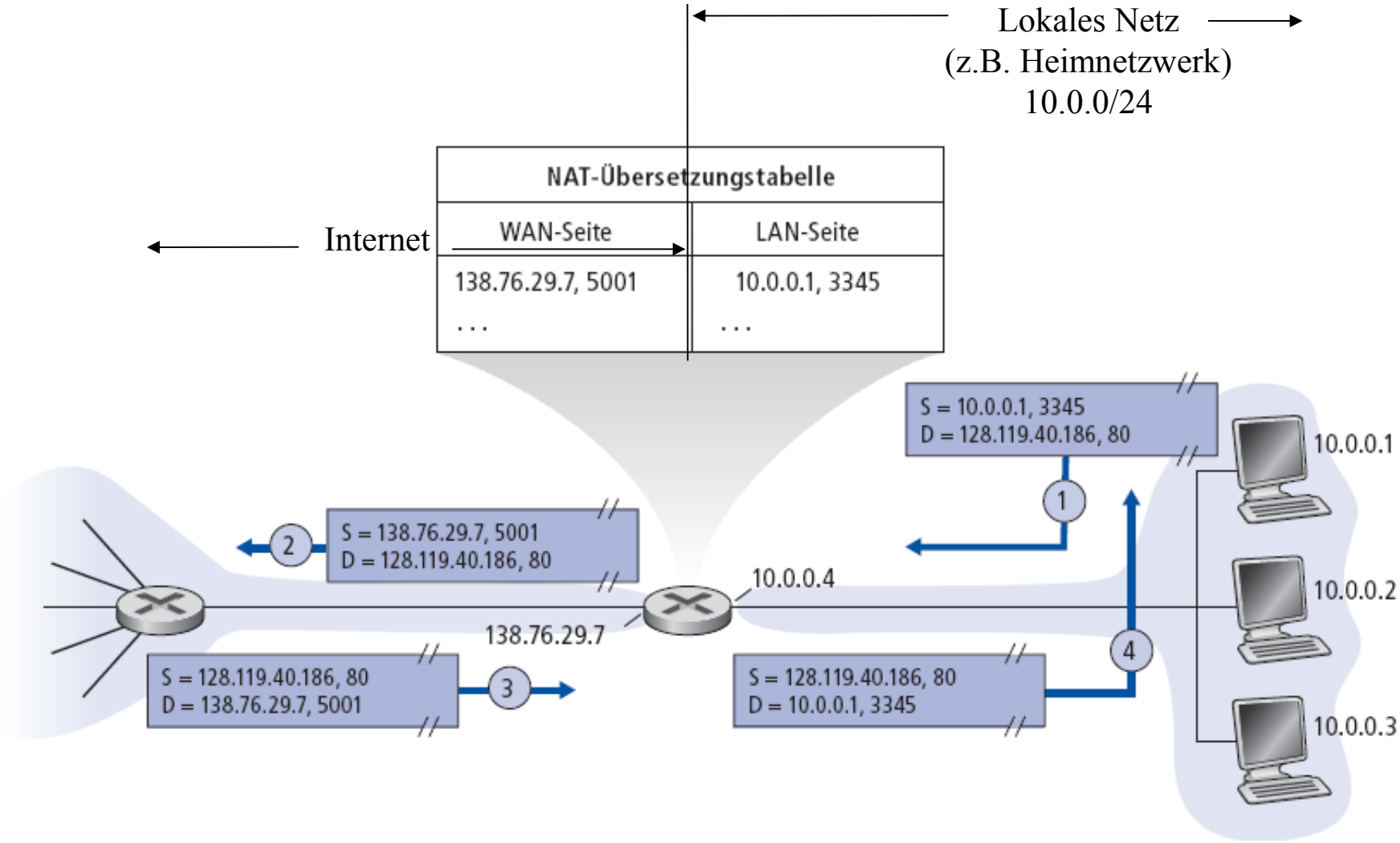
Es gibt ein Feld, in dem eine eindeutige Kennung des Clients verpackt ist. Dies ist meist die MAC-Adresse.



Besondere Adressen (RFC 3330)

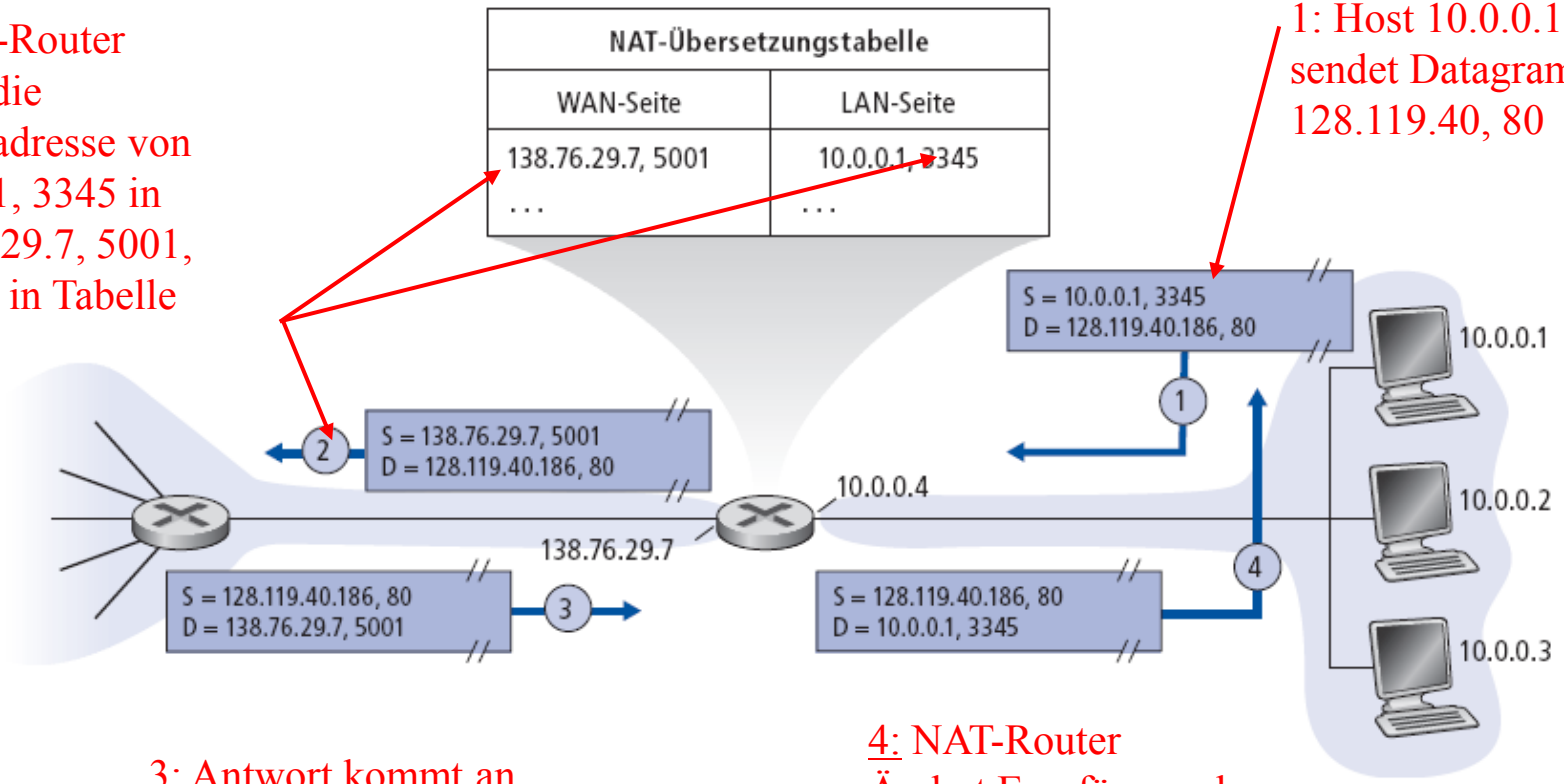
Address Block	Present Use	Reference
0.0.0.0/8	"This" Network	[RFC1700, page 4]
10.0.0.0/8	Private-Use Networks	[RFC1918]
14.0.0.0/8	Public-Data Networks	[RFC1700, page 181]
24.0.0.0/8	Cable Television Networks	--
39.0.0.0/8	Reserved but subject to allocation	[RFC1797]
127.0.0.0/8	Loopback	[RFC1700, page 5]
128.0.0.0/16	Reserved but subject to allocation	--
169.254.0.0/16	Link Local	--
172.16.0.0/12	Private-Use Networks	[RFC1918]
191.255.0.0/16	Reserved but subject to allocation	--
192.0.0.0/24	Reserved but subject to allocation	--
192.0.2.0/24	Test-Net	
192.88.99.0/24	6to4 Relay Anycast	[RFC3068]
192.168.0.0/16	Private-Use Networks	[RFC1918]
198.18.0.0/15	Network Interconnect Device Benchmark Testing	[RFC2544]
223.255.255.0/24	Reserved but subject to allocation	--
224.0.0.0/4	Multicast	[RFC3171]
240.0.0.0/4	Reserved for Future Use	[RFC1700, page 4]

NAT: Network Address Translation



NAT: Network Address Translation

2: NAT-Router ändert die Senderadresse von 10.0.0.1, 3345 in 138.76.29.7, 5001, Eintrag in Tabelle



3: Antwort kommt an für Adresse 138.76.29.7, 5001

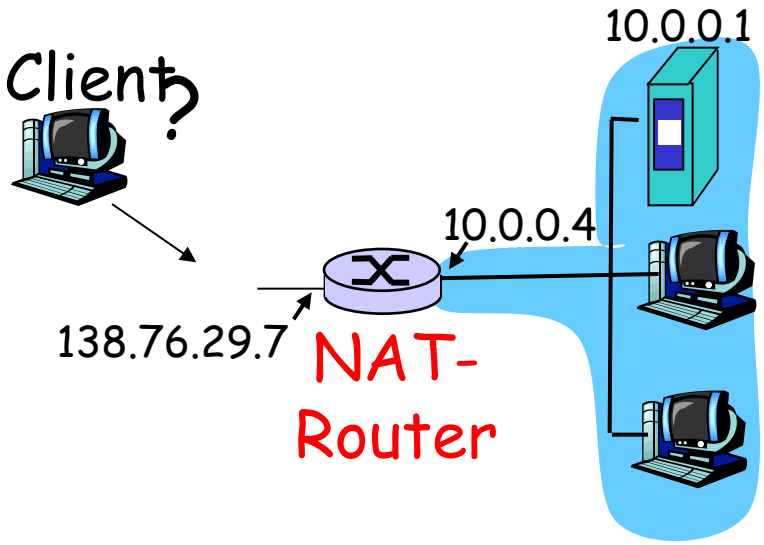
4: NAT-Router Ändert Empfängeradresse von 138.76.29.7, 5001 in 10.0.0.1, 3345

NAT: Network Address Translation

- 16-Bit-Port Number-Feld:
  - Mehr als 60.000 gleichzeitige Verbindungen mit einer IP-Adresse
- NAT ist nicht unumstritten:
  - Router sollten nur Informationen der Schicht 3 verwenden
  - Verletzung des sogenannten Ende-zu-Ende-Prinzips (end-to-end principle):
    - Transparente Kommunikation von Endsystem zu Endsystem, im Inneren des Netzes wird nicht an den Daten „herumgepfuscht“
    - Bei NAT: Der Anwendungsentwickler muss die Präsenz von NAT-Routern berücksichtigen. Beispiele:
      - Verwenden der IP-Adresse als weltweit eindeutige Nummer
      - Verwenden von UDP
  - NAT dient hauptsächlich der Bekämpfung der Adressknappheit im Internet. Dies sollte besser über IPv6 (s. später) erfolgen

Durchqueren von NAT

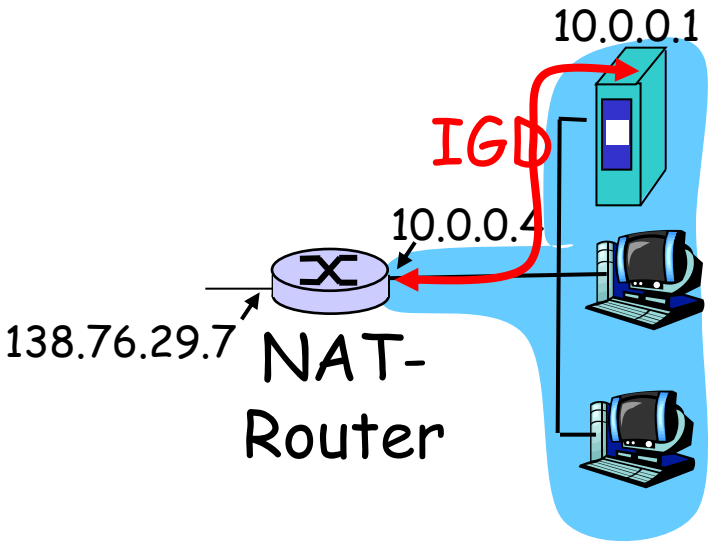
- Engl. NAT traversal
- Der Client möchte den Server mit der Adresse 10.0.0.1 kontaktieren
  - Die Adresse 10.0.0.1 ist eine lokale Adresse und kann nicht als Adresse im globalen Internet verwendet werden
  - Die einzige nach außen sichtbare Adresse ist: 138.76.29.7
- Lösung 1: Statische Konfiguration von NAT, so dass eingehende Anfragen geeignet weitergeleitet werden
  - Beispiel: (123.76.29.7, Port 2500) wird immer an 10.0.0.1, Port 25000 weitergeleitet



Durchqueren von NAT

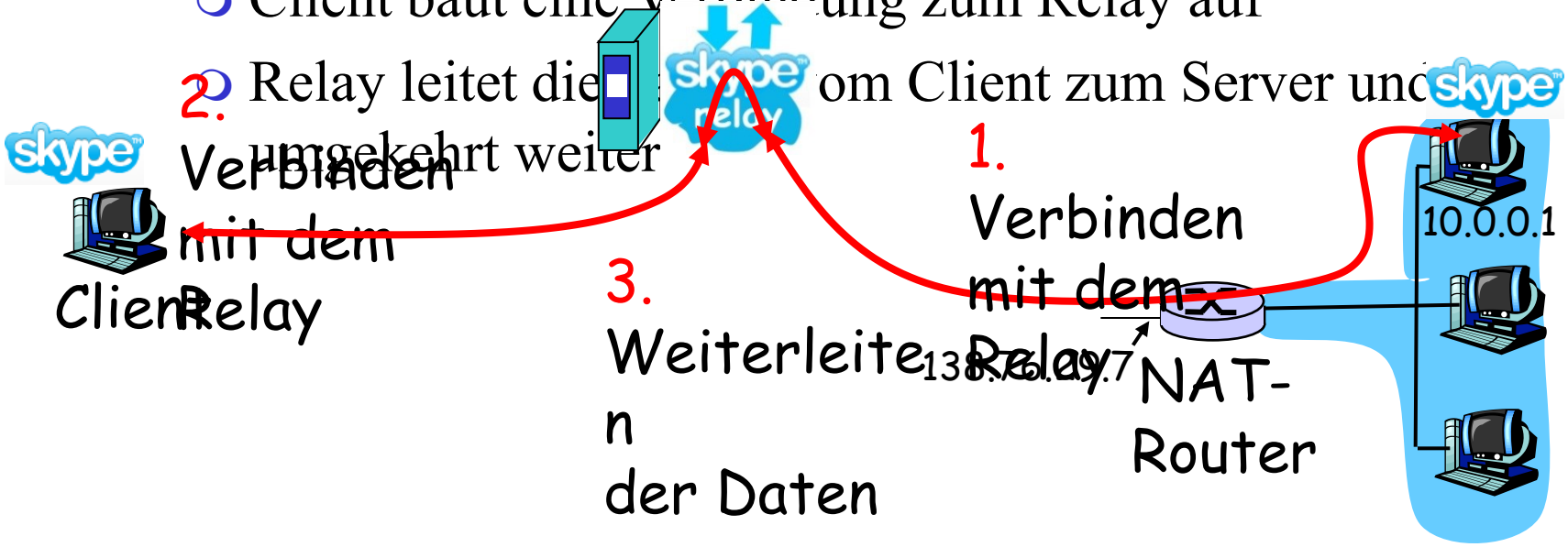
- Lösung 2: Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol. Dies ermöglicht dem Host hinter dem NAT Folgendes:
  - ❖ Herausfinden der öffentlichen IP-Adresse des NAT-Routers (138.76.29.7)
  - ❖ Kennenlernen existierender Abbildungen in der NAT-Tabelle
  - ❖ Einträge in die NAT-Tabelle einfügen oder aus ihr löschen

  Das heißt automatische Konfiguration von statischen NAT-Einträgen



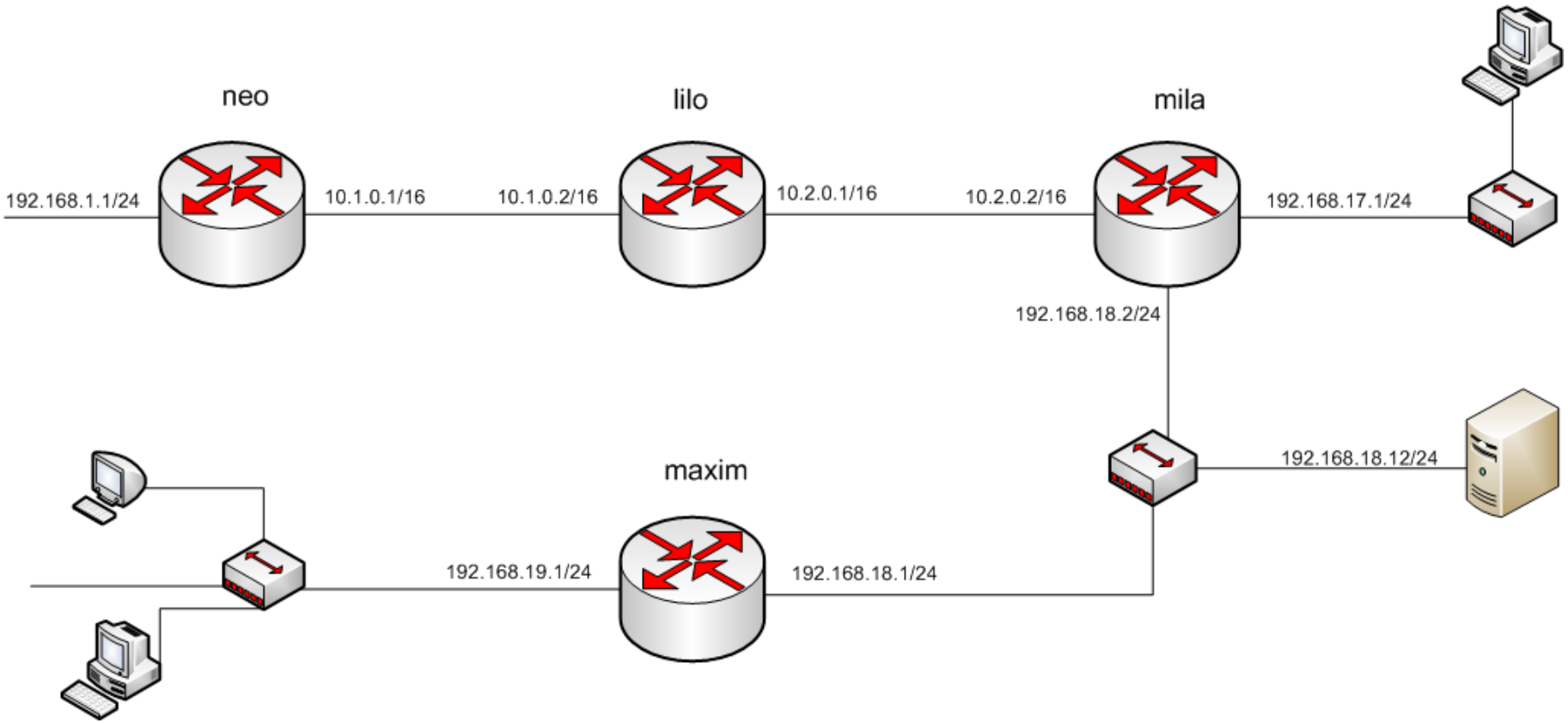
Durchqueren von NAT

- Lösung 3: Relaying (von Skype verwendet)
  - Server hinter einem NAT-Router baut eine Verbindung zu einem Relay auf (welches nicht hinter einem NAT-Router liegt)
  - Client baut eine Verbindung zum Relay auf
  - Relay leitet die Daten vom Client zum Server und umgekehrt weiter



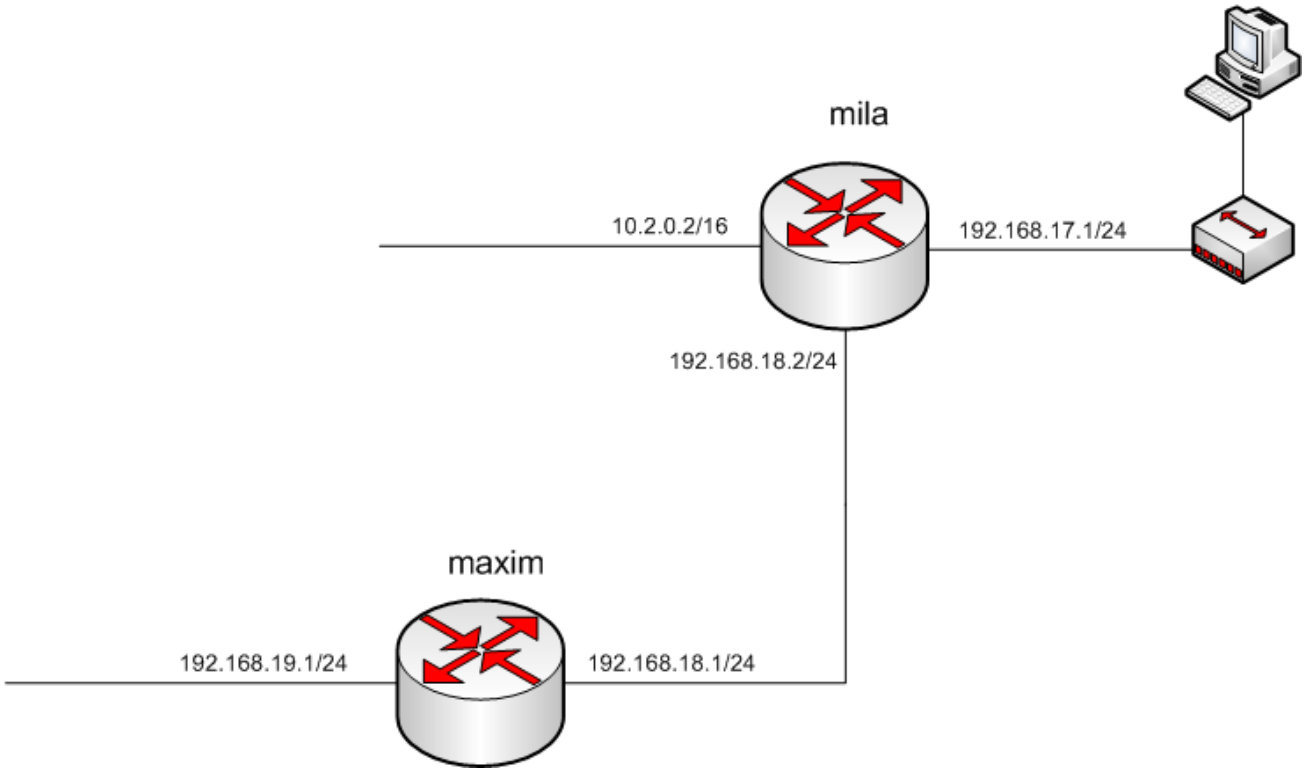
Fallbeispiel für statisches Routen(1)

- Wieviele Teilnetze hat das gezeigte Netzwerk?
- Wie lauten die jeweiligen Netzadressen und die zugehörigen Netzmasken?
- Wie lautet die Routingtabelle für den Router neo?



Fallbeispiel für statisches Routen(2)

- Supernetting bzw. route aggregation (CIDR)



Fallbeispiel für statisches Routen(3)

- Alternativroute von Router neo zu Router maxim