

# Internetanwendungstechnik

## Vermittlungsschicht

Gero Mühl

Technische Universität Berlin

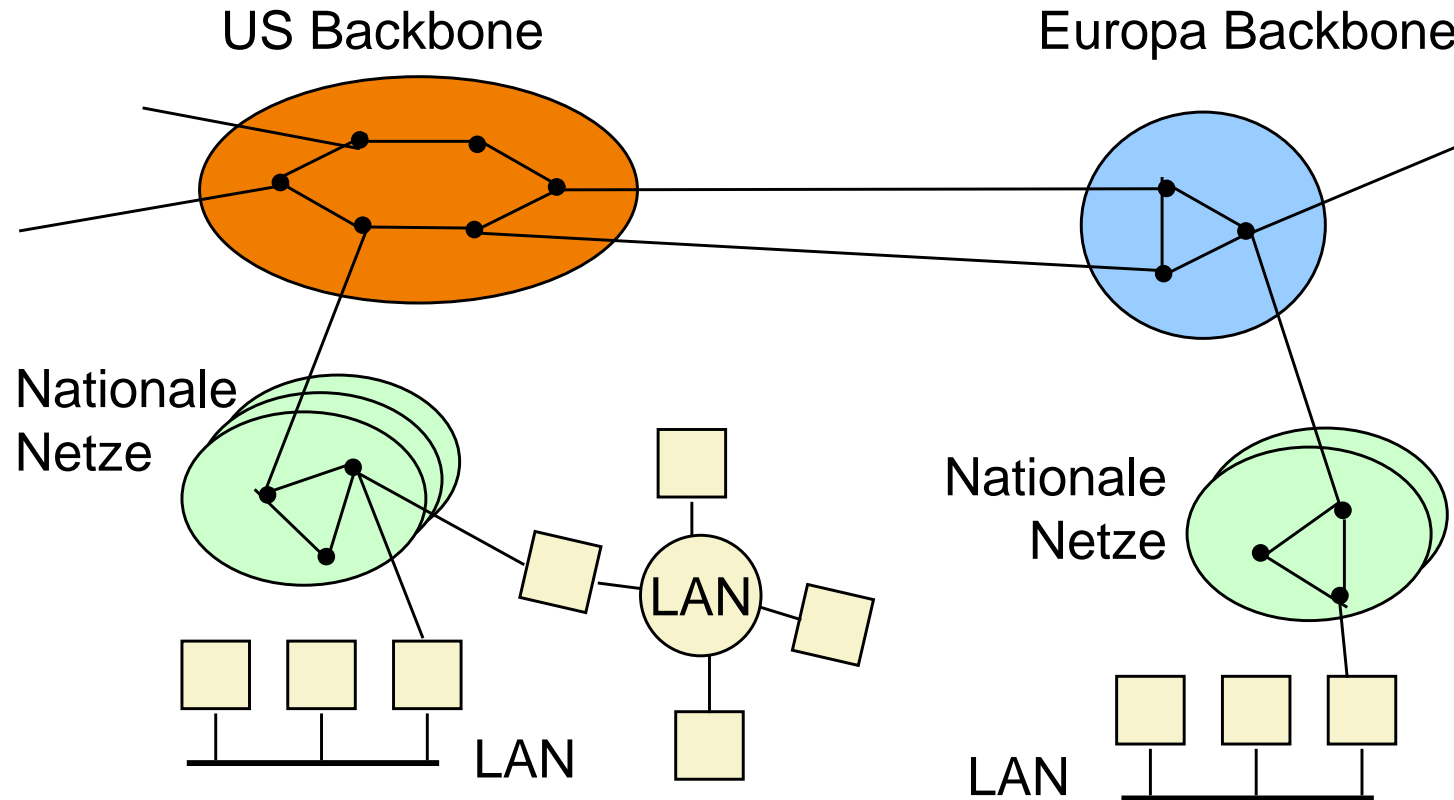
Fakultät IV – Elektrotechnik und Informatik

Kommunikations- und Betriebssysteme (KBS)

Einsteinufer 17, Sekr. EN6, 10587 Berlin

# INTERconnected NETworks

- > Internet = Verbund beliebiger Netze mit Datenpaket-Transport zwischen beliebigen Rechnern



# Vermittlungsschicht

- > Aufgaben der Vermittlungsschicht
- > Übertragung von Datenpaketen zwischen beliebigen (am Netz angeschlossenen) Rechnern
- > Finden eines Weges von der Quelle zum Ziel
- > Vermeidung von Überlastungen auf beteiligten Strecken
- > Fehlerbehebung (eingeschränkt)
- > Unterste Schicht mit Ende-zu-Ende-Bedeutung!

# Leitungsvermittelt vs. Paketvermittelt

## > Leitungsvermittelt

- > Bevor zwei Rechner kommunizieren wird ein Weg festgelegt, über den alle Pakete vom Sender zum Empfänger und vice versa übertragen werden
- > Oft wird Bandbreite reserviert
- > Analog zur ursprünglichen Realisierung des Telefonnetzes

## > Paketvermittelt

- > Jedes Paket reist unabhängig von anderen Paketen und nimmt potentiell einen anderen Weg
- > Einfachere Realisierung, aber Pakete können in einer anderen Reihenfolge ankommen als sie gesendet wurden

# Verbindungsorientiert vs. Verbindungslos

## > Verbindungslos

- > Direkter Austausch von Nutzdaten ohne vorige Abstimmung
- > Unidirektionale Kommunikation möglich

## > Verbindungsorientiert

- > Vor dem Austausch von Nutzdaten wird eine Verbindung zwischen den Rechnern aufgebaut
- > Setzt bidirektionale Kommunikation voraus
- > Voraussetzung für zuverlässige Ende-zu-Ende Kommunikation und Ende-zu-Ende Flusssteuerung
- > 2 Variationen zuverlässiger Ende-zu-Ende Kommunikation:  
**Nachrichtenfolgen** und **Byteströme**

# Kombinationsmöglichkeiten

> 4 mögliche Kombinationen

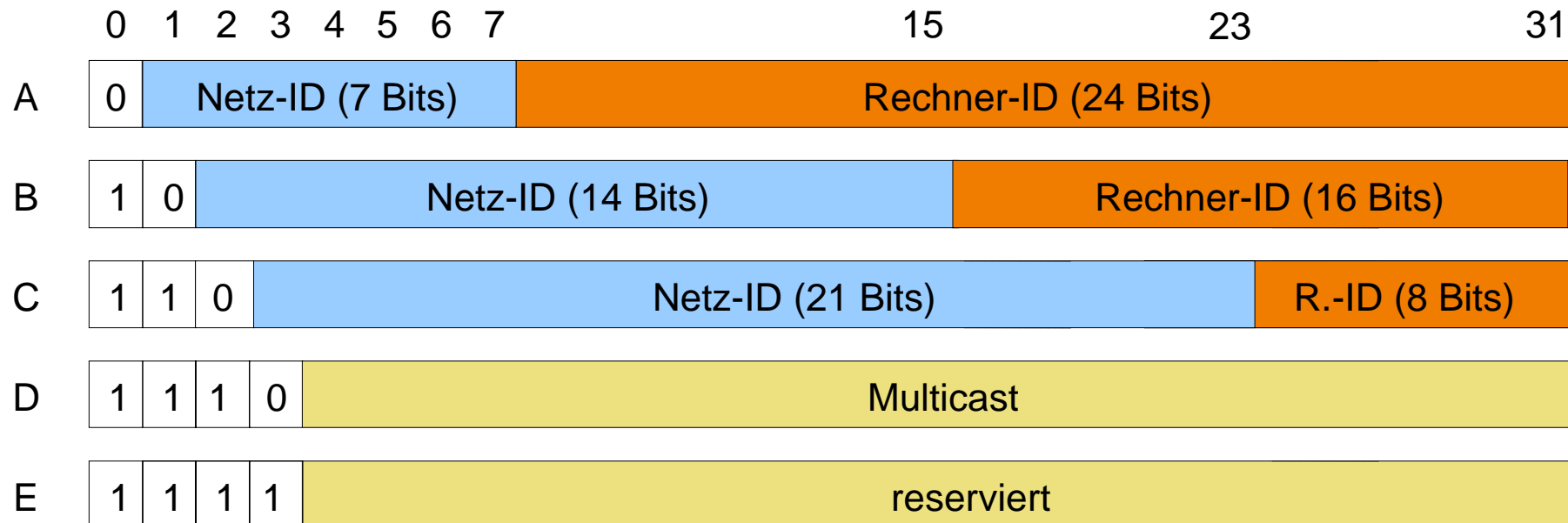
	Leitungsvermittelt	Paketvermittelt
Verbindungslos	Rohrpost	UDP/IP
Verbindungsorientiert	Analoges Telefon	TCP/IP

# Internet Protocol (IPv4)

- > Einheitliches Adressierungsschema
  - > Jeder Rechner erhält eindeutige Kennung
  - > Aufteilung in „Netz“ und „Rechner“
  
- > Verbindungslose Auslieferung von Datenpaketen (Datagrammen)
  - > „Best Effort“ Kommunikation
  - > Das Netz kann Pakete verändern, verlieren, duplizieren, verzögern, Reihenfolge ändern, ...
  - > Beliebig heterogene Netze
  - > IP ist „kleinster gemeinsamer Nenner“ für alle Netze
  - > Router bleiben einfach
  - > Wichtiger Erfolgsfaktor des Internets

# IP-Adressen (IPv4)

- > Jeder Anschluss bekommt eigene IP-Adresse
- > 32 Bits → 4.294.967.296 Adressen
- > Reicht für 8 etwa Adressen pro km<sup>2</sup>
- > Notation: Folge von vier 8-Bit Dezimalzahlen, z.B. 141.2.2.1
- > 5 Netzklassen: A, B, C, D und E





# IP-Adressen (IPv4)

- > Adressbereiche
  - > Klasse A: 1.0.0.0 bis 127.255.255.255
  - > Klasse B: 128.0.0.0 bis 191.255.255.255
  - > Klasse C: 192.0.0.0 bis 223.255.255.255
  - > Klasse D: 224.0.0.0 bis 239.255.255.255
  - > Klasse E: 240.0.0.0 bis 247.255.255.255
- > Beispiel
  - > Klasse A: ARPANET 10.0.0.0
  - > Klasse B: TU Berlin 130.149.0.0
- > Reserviert für lokale Netze
  - > 10.0.0.0 bis 10.255.255.255
  - > 172.16.0.0 bis 172.31.255.255
  - > 192.168.0.0 bis 192.168.255.255

# Adressierung

- > Einige Adressen haben besondere Bedeutung



Dieser Rechner



Broadcast in diesem Netz



Rechner in diesem Netz



Rechner in Netz „Netz“

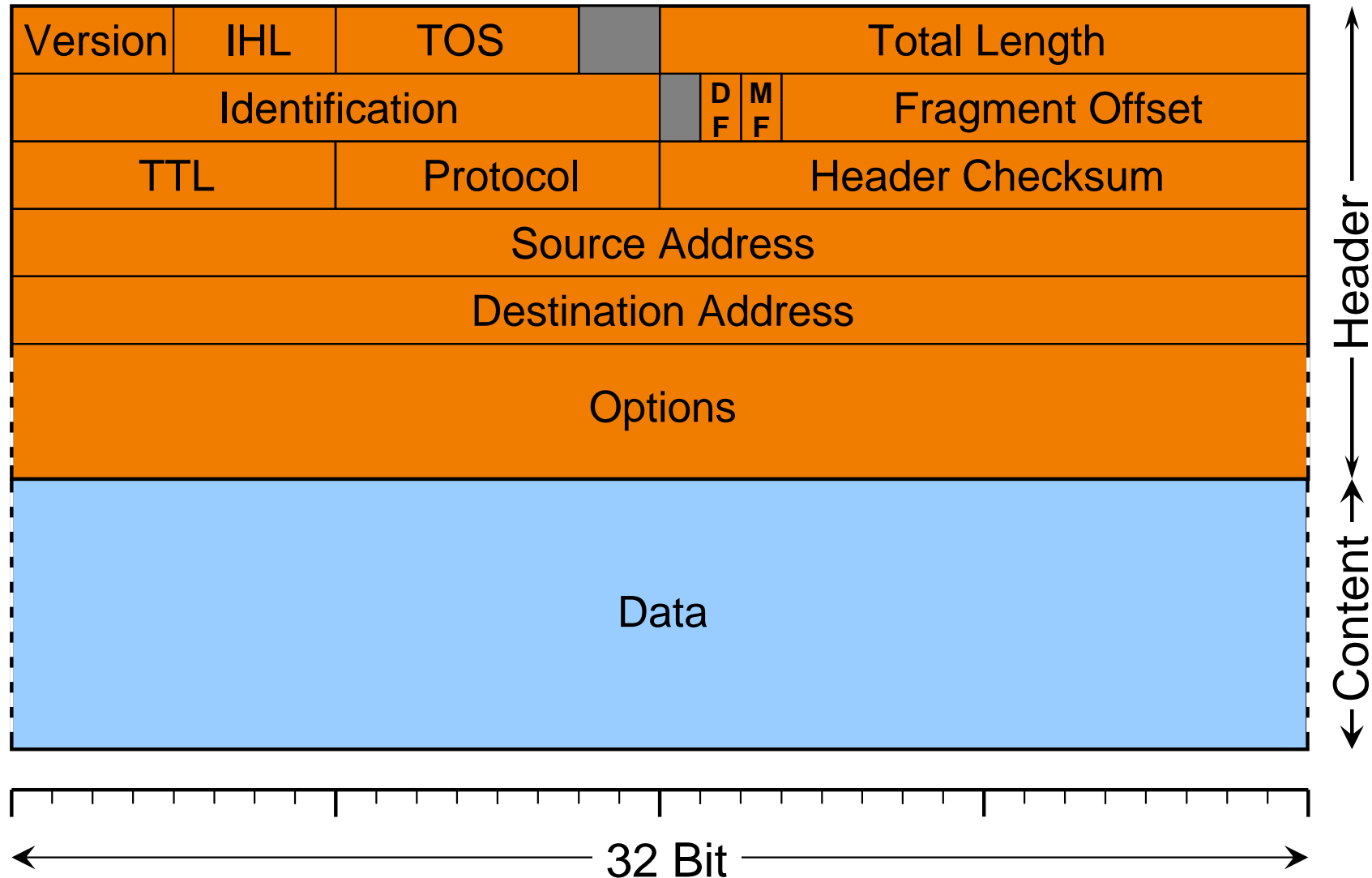


Broadcast in Netz „Netz“



Loopback (Schleife)

# IP-Paket (IPv4)



# IP-Paket (IPv4)

- > Version
  - > Version des IP Protokolls
- > IHL
  - > Länge des Headers (in Anzahl von 32-Bit-Wörter)
- > TOS = Type of Service
  - > Erlaubt Spezifikation von Präferenzen wie Prioritäten, niedrige Verzögerung
  - > Nicht wirklich benutzt
- > Total Length
  - > Gesamtlänge des Paketes (in Bytes)
- > Identification
  - > Wert identifiziert das Datagramm bzw. die Fragmente

# IP-Paket (IPv4)

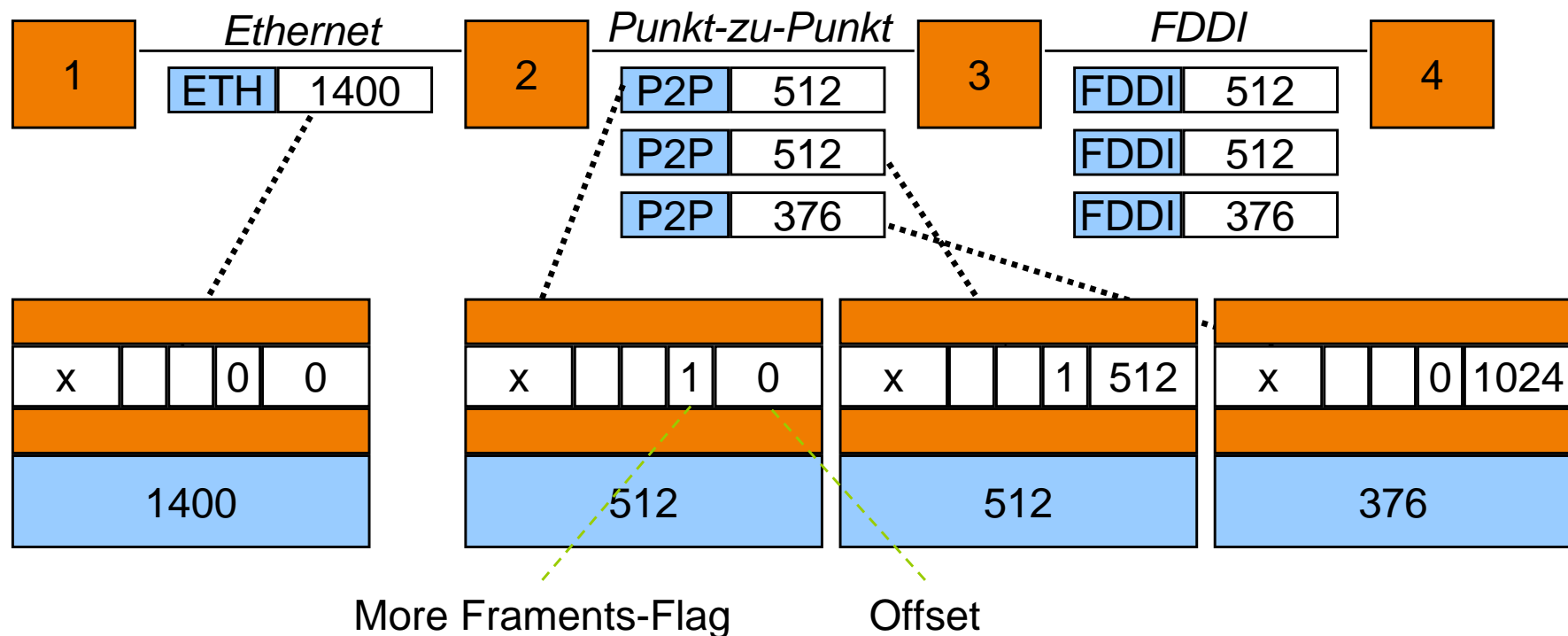
- > Flags
  - > 1. Flag: unbenutzt
  - > 2. Flag – DF (don't fragment): Datagram nicht fragmentieren!
  - > 3. Flag – MF (more fragments): 1 bzw. 0 beim letzten Fragment
- > Offset
  - > Position des Fragments im Datagramm
- > Time to Live
  - > Sollte Zeit in Sekunden spezifizieren (max 255 sec)
  - > In der Praxis Teilstreckenzähler mit Default = 64
- > Protocol
  - > Nummer des darüber liegenden Transportprotokoll
- > Header Checksum
  - > Prüfsumme für den Header zur Fehlererkennung

# IP-Paket (IPv4)

- > Source Address
  - > IP Adresse des Absenders
- > Destination Addresss
  - > IP Adresse des Empfängers
- > Options
  - > optionale Optionen, z.B. Sicherheit, Source Routing
  - > 1 Byte Option Code gefolgt von n Bytes Option Data
  - > Auffüllung (Padding) auf vielfaches von 4 Byte

# Fragmentierung

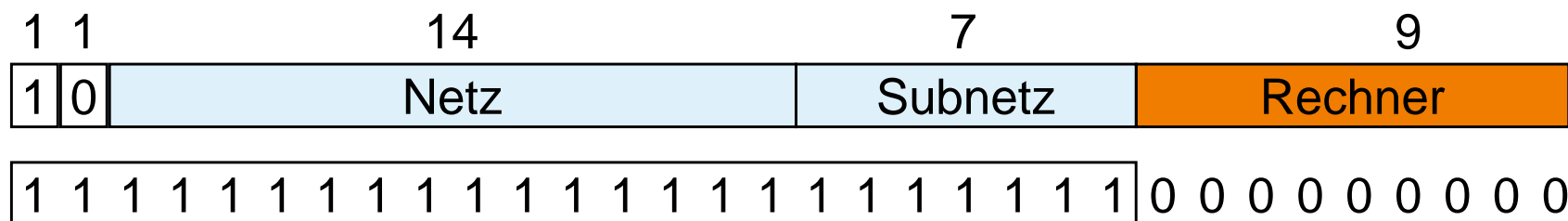
- > Jedes Paket trägt die notwendige Information, um von der Quelle zum Ziel zu gelangen (d.h. Quell- und Zieladresse)
- > Pakete, die für das physikalische Netzwerk zu groß sind, werden in kleinere Fragmente aufgeteilt
- > Die Fragmente werden unterwegs nicht mehr zusammengesetzt, sondern jedes Fragment reist als eigenständiges IP-Datagramm



# IP-Subnetze

- > Ermöglichen Aufteilung eines größeren Netzes in mehrere kleinere
- > Interpretation eines Teils der Rechneradresse als Subnetz-Adresse
- > Für Außenwelt transparent → lässt mehrere physikalische Netze wie ein Netz aussehen
- > Subnetzbildung wurde in den IP-Standard aufgenommen
- > Beispiel: Klasse B-Adresse

$2^{14} = 16384$  Klasse B Netze       $2^7 = 128$  Subnetze



Subnetzmaske = 255.255.254.0

Alternative Notation: /23

$2^9 - 2 = 510$  Rechner

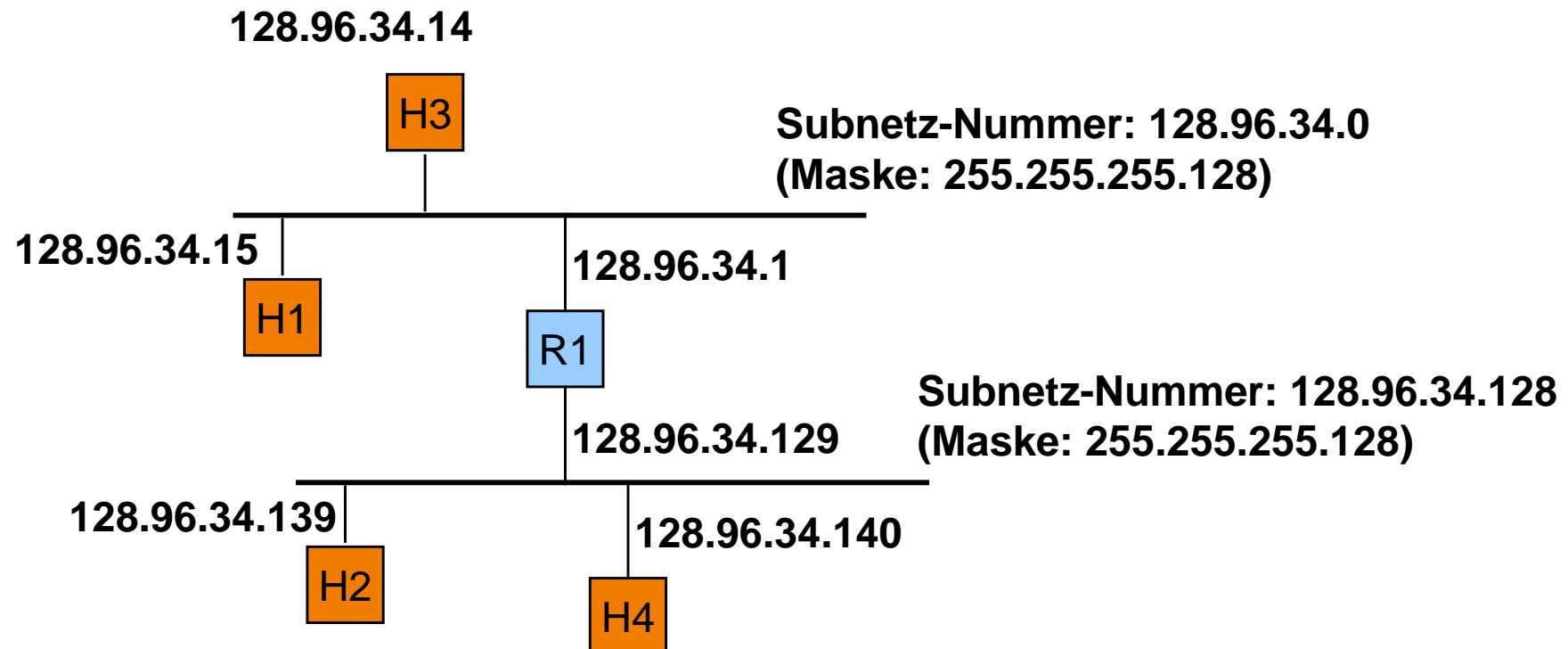


# IP-Subnetze

- > Jeder Rechner kennt seine eigene IP-Adresse und die Subnetzmaske seines lokalen Netzwerkes
- > Alle Rechner im gleichen Subnetz haben dieselbe Maske
- > Beim Senden eines Datagramms wird ein logisches **UND** von Zieladresse und Subnetzmaske berechnet
- > Ergebnis gleich der eigenen Subnetznummer, dann **direktes** Senden; sonst **indirektes** Senden über Router

# IP-Subnetze

> Beispiel: Klasse B-Adresse



# IP-Subnetze

- > Beispiel: Klasse B-Adresse
  
- > 1. Fall: H1 schickt an H2
  - > Adresse von H2 UND Maske von H1  
 $128.96.34.139 \text{ UND } 255.255.255.128 = 128.96.34.128$
  - > Ungleich Subnetz von H1, d.h. über R1 schicken
  
- > 2. Fall: H1 schickt an H3
  - > Adresse von H3 UND Maske von H1  
 $128.96.34.14 \text{ UND } 255.255.255.128 = 128.96.34.0$
  - > Gleiches Subnetz, d.h. direkt schicken

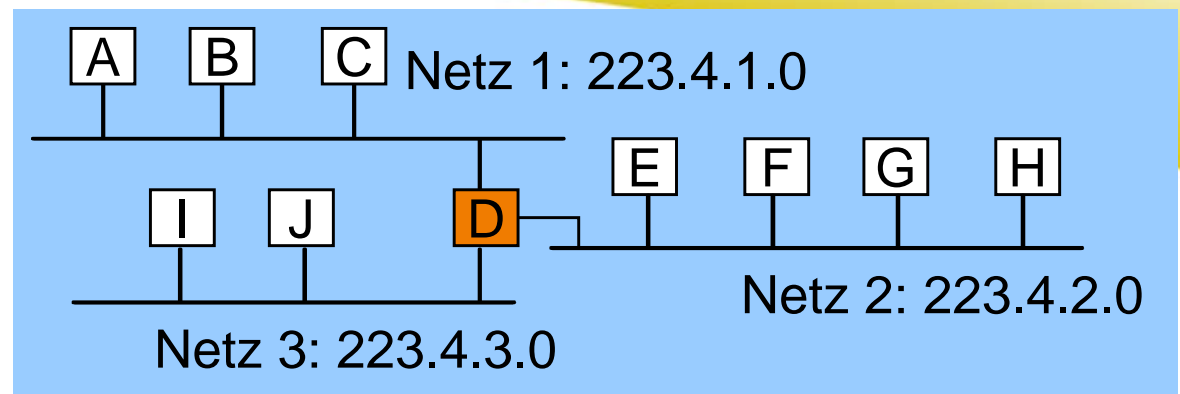
# IP-Routing

- > Wie gelangen IP-Datagramme durch eventuell mehrere Netze zum Ziel?
- > Voraussetzungen
  - > Jedes IP-Datagramm enthält Zieladresse
  - > Der Netz-Teil der IP-Adresse bezeichnet eindeutig ein einziges physisches Netz im Internet
  - > Alle Rechner und Router, welche die gleiche Netz-Adresse haben, können direkt miteinander kommunizieren
  - > Jedes Netz im Internet hat mindestens einen Router, der mit mindestens einem anderen Netz im Internet verbunden ist
- > Vorgehensweise beim IP-Routing
  - > Falls der Empfänger des Datagramms im selben Netz ist, schicke es direkt
  - > Falls nicht, schicke das Datagramm an einen Router

# IP-Routing

- > Routing-Tabellen
  - > Ordnen IP-Adressen die nächste zu wählende Teilstrecke zu
  - > Direktes Routing (im selben Netz)
  - > Indirektes Routing (über Router)
- > Tabelle enthält IP-Adressen, keine physischen Adressen
  - > Routing-Entscheidungen unabhängig von physischen Adressen
  - > Verbirgt Details der Netze vor IP, klare Separation
  - > Isoliert Routing-Information in Routing-Tabellen
- > IP-Routing ändert nicht die Adressen von Quelle und Ziel
- > Paket wird lediglich „hopweise“ weitergereicht, bis es sein Ziel erreicht

# IP-Routing



## > Routing-Tabelle in A

Netzwerk	direkt/indirekt	Gateway	Schnittstelle
223.4.1	direkt	-	1
223.4.2	indirekt	D	1
223.4.3	indirekt	D	1
default	indirekt	D	1

## > Routing-Tabelle in D

Netzwerk	direkt/indirekt	Gateway	Schnittstelle
223.4.1	direkt	-	1
223.4.2	direkt	-	2
223.4.3	direkt	-	3

# IP-Routing-Protokolle

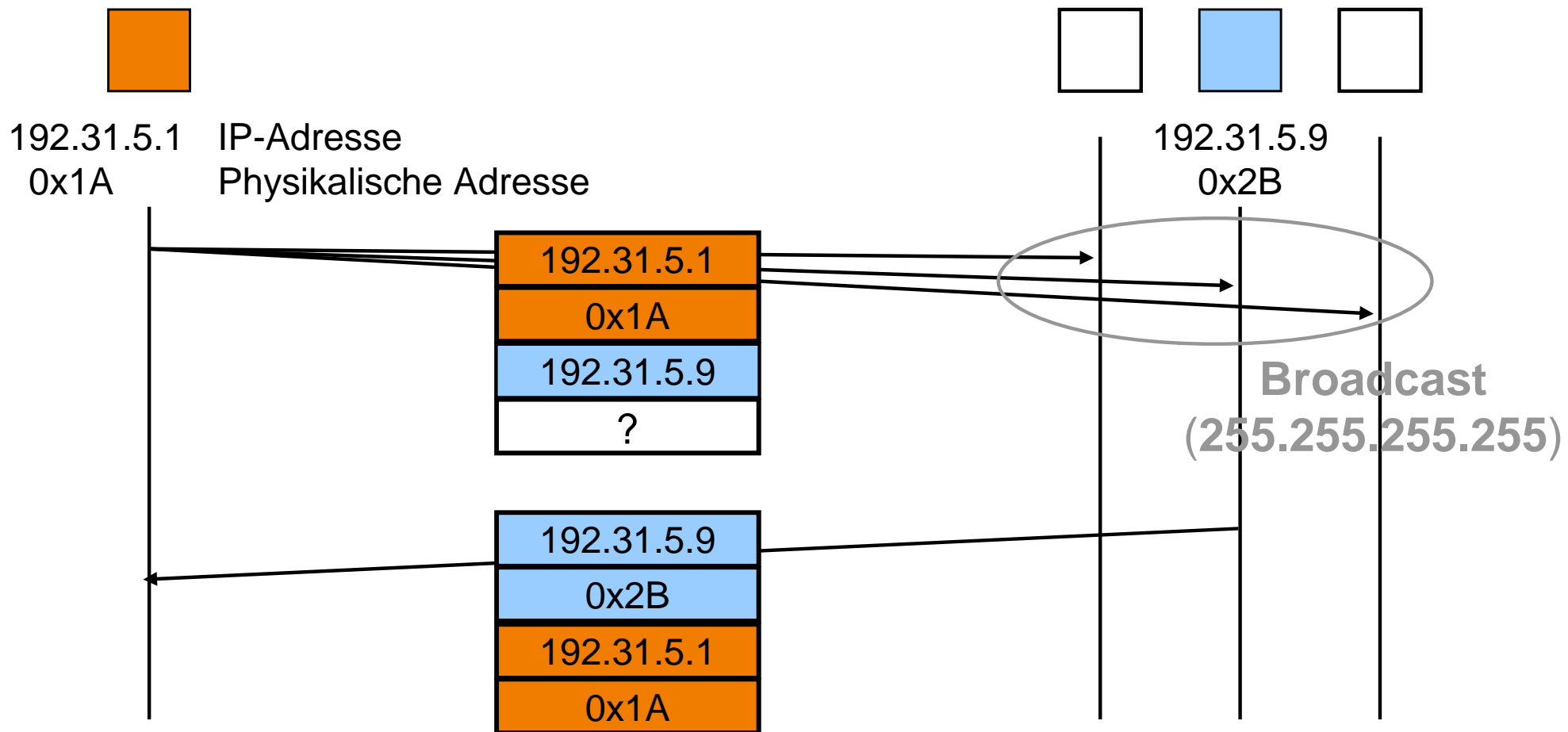
- > Aktualisieren die Routing-Tabellen
- > Intradomain vs. Interdomain Routing
- > Beispiele für Intradomain Routing-Protokolle
  - > Routing Information Protocol (**RIP**) [RFC 1058]
    - > Router tauschen periodisch Distanzvektoren untereinander aus
    - > Vektor beinhaltet, Entfernung zu anderen Netzen in „Hops“
  - > Open Shortest Path First (**OSPF**) [RFC 1247]
    - > Jeder Router kennt Netzwerk und berechnet kürzesten Pfad
- > Beispiel für Interdomain Routing-Protokolle
  - > Border Gateway Protocol (**BGP**) [RFC 1654]

# Address Resolution Protocol (ARP)

- > IP-Adressen sind logische Adressen und damit unabhängig von der physischen Hardware-Adresse
- > Ethernet-Adapter haben eine werksseitig fest vergebene, eindeutige Ethernet-Adresse (48Bits)  
→ Hardware-Adresse
- > Ethernet-Adapter kann mit IP-Adressen nichts anfangen
- > Wie werden IP-Adressen auf physische Adressen abgebildet?
- > Address Resolution Protocol (ARP) [RFC 826]
- > ARP baut eine Abbildungstabelle auf und nutzt hierfür die Broadcast in LANs



# Address Resolution Protocol (ARP)



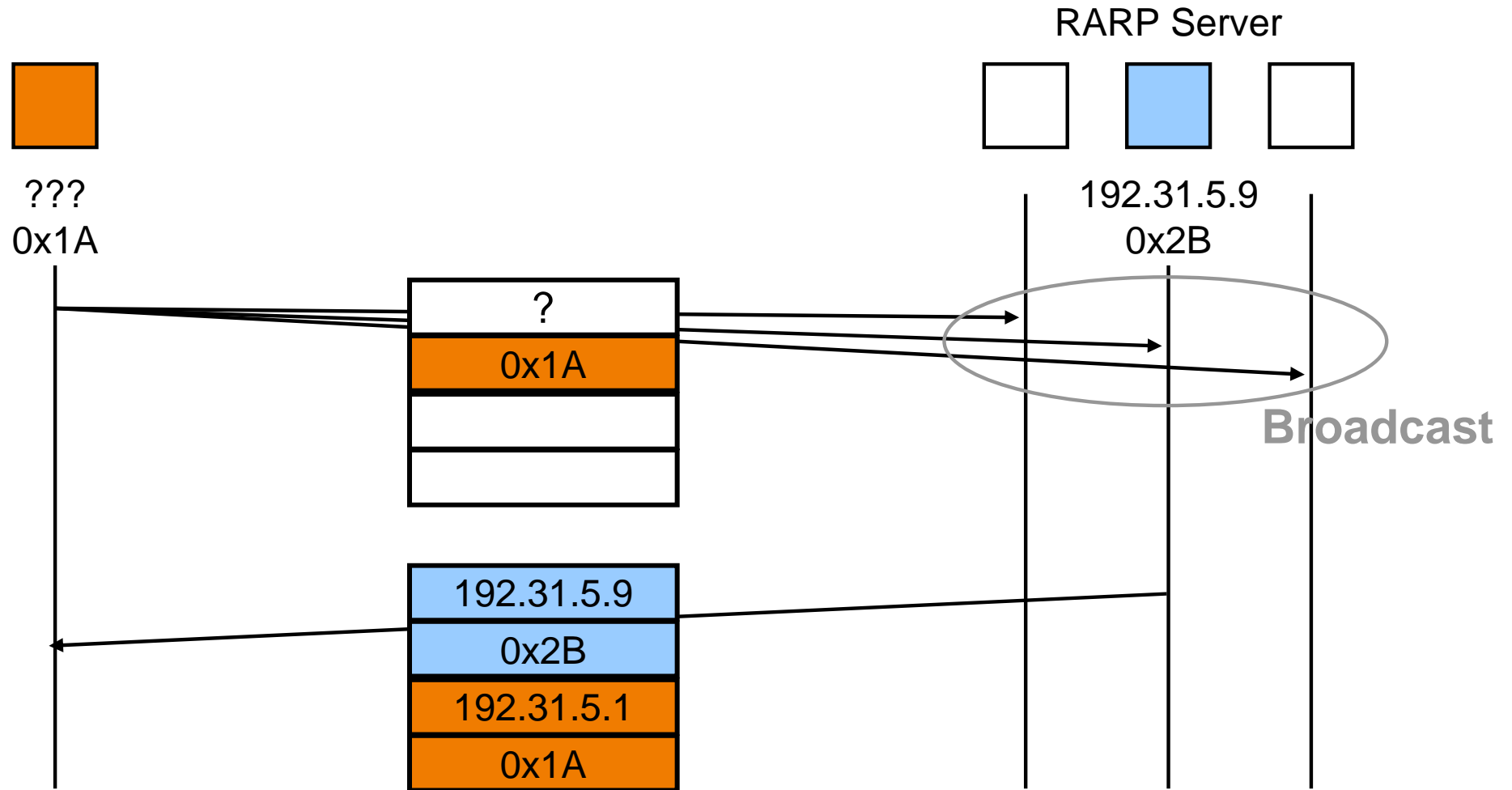
# Address Resolution Protocol

- > Bei fehlendem Eintrag im ARP Cache wird Broadcast geschickt mit Frage „Wer hat IP-Adresse 130.149.63.136?“
- > Nur betreffender Rechner antwortet mit seiner IP-Adresse und seiner physischen Adresse
- > Time-out der Cache-Einträge nach einigen Minuten, um Veränderungen zu erfassen
- > Was geschieht, wenn die gesuchte IP-Adresse nicht im eigenen LAN ist?
  - > 1. Möglichkeit: Proxy ARP  
Router antwortet mit seiner Adresse auf ARP-Anfragen für entfernte Rechner
  - > 2. Möglichkeit: Routing-Tabellen beim Absender verweisen auf Router für anderes Netz

# Reverse Address Resolution Protocol (RARP)

- > Gelegentlich ist auch das inverse Problem zu lösen: ein Rechner kennt seine physische Adresse und sucht seine zugehörige IP-Adresse
- > Einsatz z.B. für plattenlose Workstations und X Terminals
- > Broadcast im LAN: Wer kennt meine IP-Adresse?
- > RARP Server (einer pro LAN) überprüft seine Konfigurationstabellen und schickt Antwort
- > Alternativ: DHCP (oder früher BOOTP)

# Reverse Address Resolution Protocol (RARP)

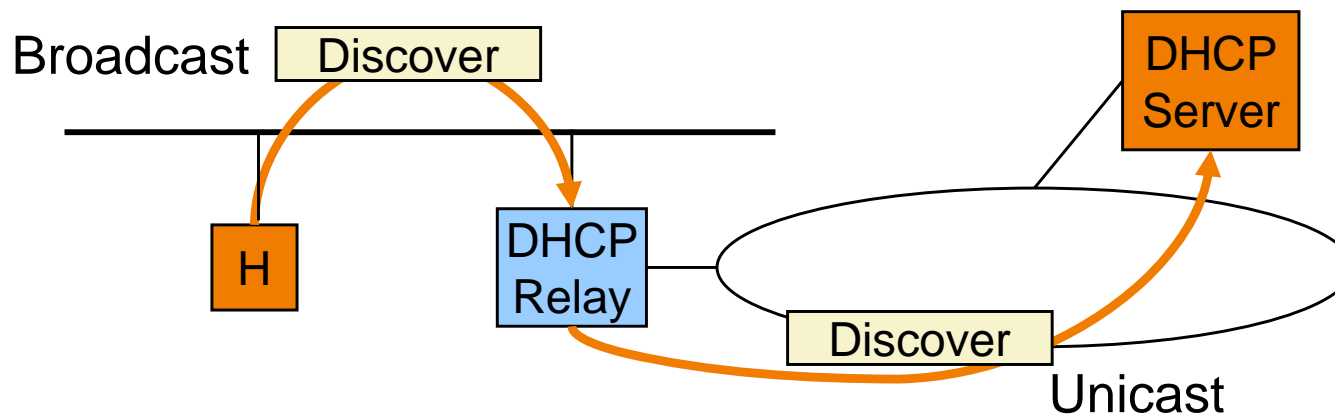


# Dynamic Host Configuration Protocol (DHCP)

- > Wie werden Rechner mit IP-Konfigurationsdaten versorgt (z.B. IP-Adresse, Default Router etc.)?
- > Manuelles Eintragen durch Systemverwalter ist aufwendig und fehleranfällig
- > Besser automatisch, z.B. mit DHCP
- > DHCP erfordert einen Konfigurationsserver (**DHCP Server**)
  - > Dieser hält Vorrat (Pool) an IP-Adressen und teilt den Rechnern auf Anfrage eine Adresse zu
  - > Rechnern mit bekannter physischer Adresse kann, wenn gewollt, immer dieselbe IP-Adresse zugewiesen werden
  - > Wie lange darf ein Rechner die zugewiesene IP-Adresse behalten?
    - > Adresse wird temporär gemietet anstatt permanent vergeben
    - > „Mietvertrag“ muss ggf. periodisch erneuert werden

# Dynamic Host Configuration Protocol (DHCP)

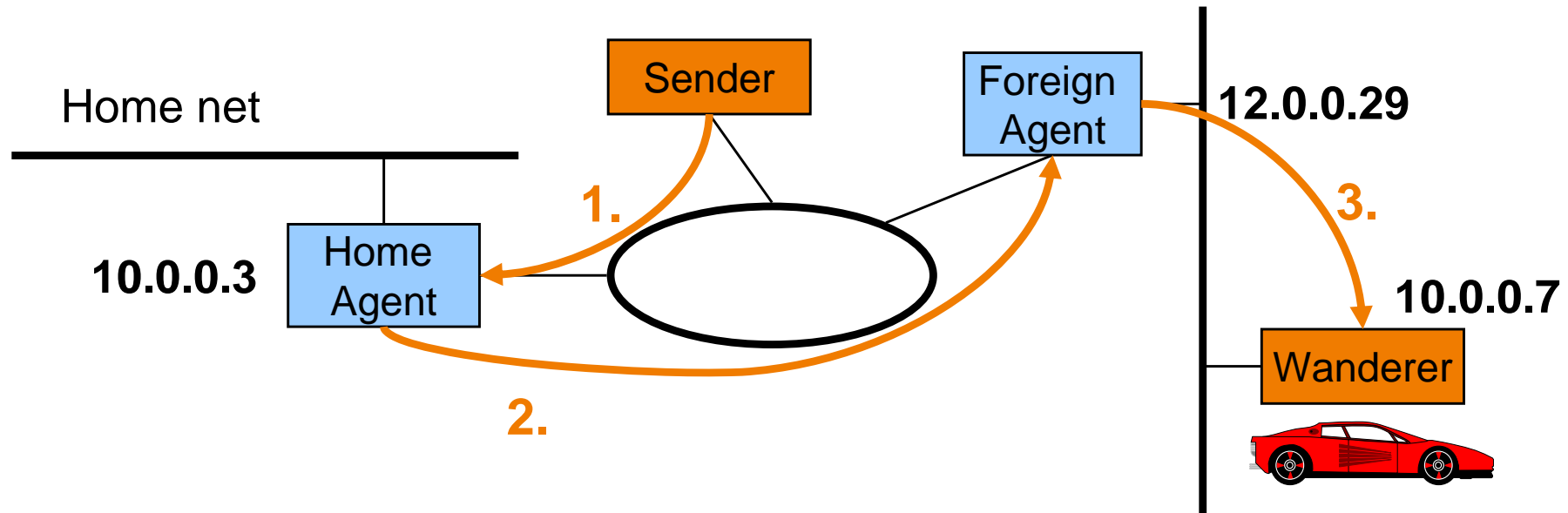
- > Wie findet ein neuer Rechner den DHCP Server?
- > Broadcast im Netz (an 255.255.255.255)
  - > Nachricht vom Typ „DHCP DISCOVER“ (per UDP)
  - > Falls DHCP Server im selbem Netz → OK
  - > Falls nicht, kann es ein DHCP Relay weiterreichen



# Mobile IP

- > Neuer Rechner an einem Netz kann z.B. mit DHCP angeschlossen werden
  - > Dabei erhält er eine neue IP-Adresse
  - > Aber geht das auch unterbrechungsfrei, z.B. für Anwendungen auf mobilen Rechnern, die über Funk kommunizieren?
  
- > Mobile IP unterstützt „wandernde Rechner“ durch die neuen Router-Funktionen: Home Agent und Foreign Agent
  - > Mobiler Rechner meldet sich beim dem Foreign Agent an und teilt ihm die Adresse seines Home Agents mit
  - > Der Foreign Agent bittet den Home Agent, für den mobilen Rechner eingehende Pakete ihm nachzusenden → Tunneln (tunneling)
  - > Beide Agenten verkünden periodisch ihre Anwesenheit

# Mobile IP



- > Wie fängt der Heimatagent ein Paket ab, das an den Wanderer geschickt wurde?
- > Wie kann der Heimatagent das Paket beim Fremdagenten abliefern?
- > Wie kann der Fremdagent das Paket beim Wanderer abliefern?



# Mobile IP

- > Wie fängt der Heimatagent ein Paket ab, das an den Wanderer geschickt wurde?
  - > Heimatagent „manipuliert“ ARP-Antwort und bindet seine Hardware-Adresse an die IP-Adresse des Wanderers
- > Wie kann der Heimatagent das Paket beim Fremdagenten abliefern?
  - > Paket wird „eingewickelt“ und an Fremdagenten geschickt
- > Wie kann der Fremdagent das Paket beim Wanderer abliefern?
  - > Wanderer muss sich beim Fremdagenten registriert haben
  - > Fremdagent übergibt „ausgewickeltertes“ Paket an Wanderer
- > Wie wird der Rückverkehr zum Sender erledigt?

# Fragen?

