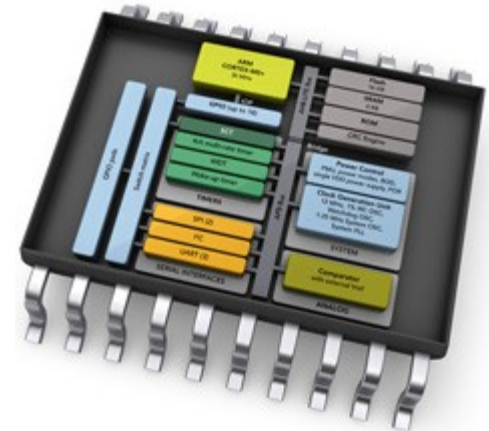


Kommunikationssysteme

(Modulcode 941306)

Prof. Dr. Andreas Terstegge



Das Internet ist ein Netz aus Netzen, Router als koppelnde Elemente zwischen den Teilnetzen

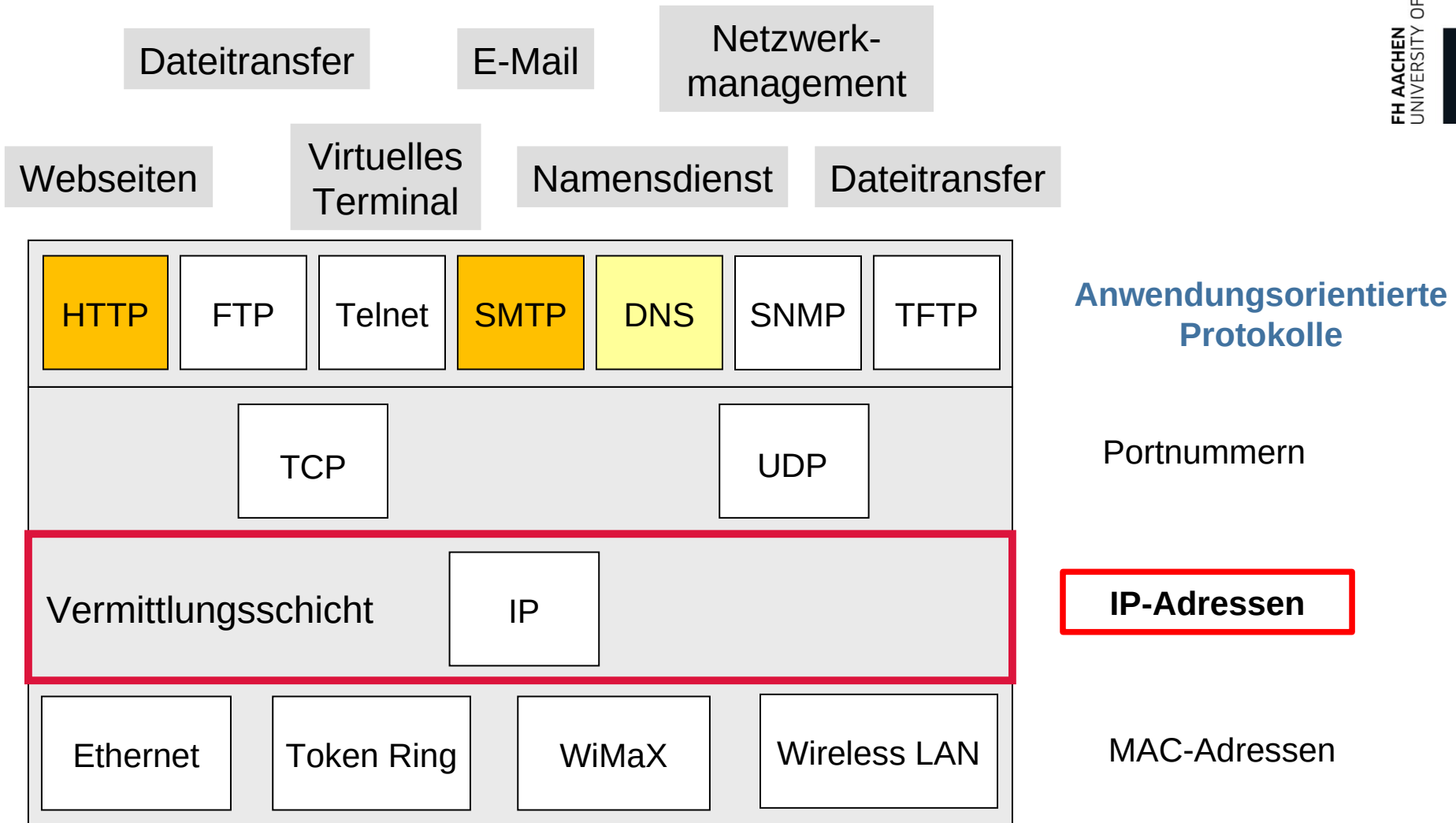
→ **Wie ist das Internet im Detail aufgebaut?**

Auf der Ebene der Vermittlungsschicht werden Pakete in einem Netz aus Netzen von einem Rechner zu einem beliebigen anderen Rechner geschickt

→ **Wie genau funktioniert das Internet auf der Vermittlungsschicht?**

Heute: Adressierung auf der Vermittlungsschicht

Internet-Referenzmodell im Überblick



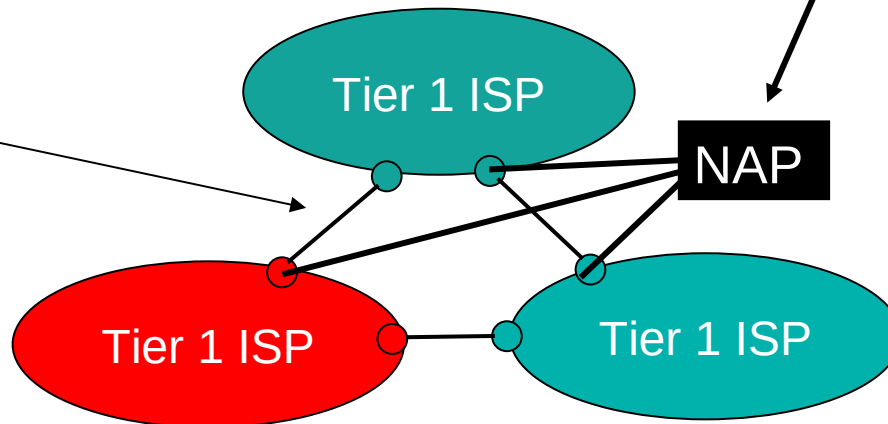
Basis des Internets sind sog. **autonome Systeme** (AS)

In IP-Netzen sind autonome Systeme (AS) ein Verbund von Routern und Netzwerken, die einer einzigen administrativen Instanz unterstehen, einer Organisation oder einem Unternehmen. Das bedeutet, dass sie alle zu einer Organisation oder zu einem Unternehmen gehören.

Aufbau des Internet

- Die Basis des Internets bilden “Tier-1” Internet Service Provider (ISPs), *engl.*: Tier → Schicht, Stufe
- z.B. Deutsche Telekom , BT, Qwest) mit nationaler und internationaler Überdeckung
 - Treten gleichberechtigt auf
 - Anbindungen an bestimmten Orten

Vertraglich
regulierte
Verbindungen



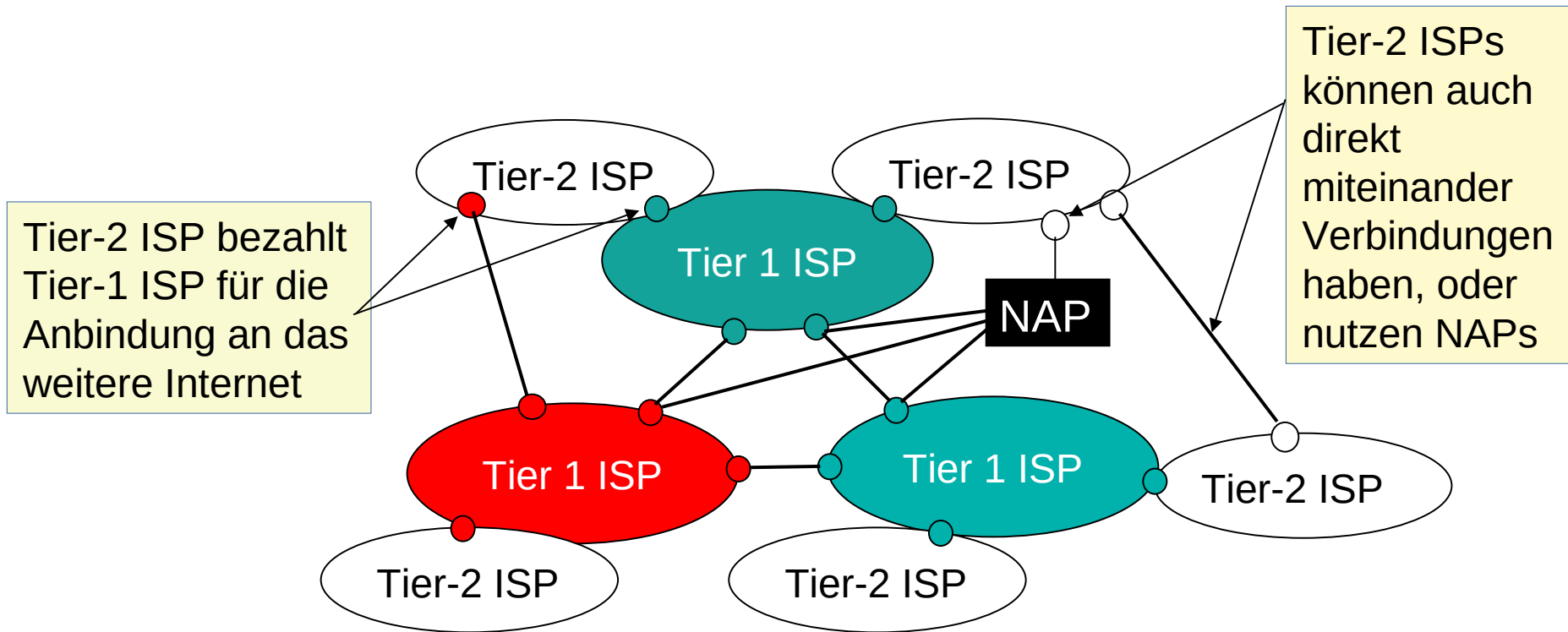
Aufbau des Internet - Tier 1 ISPs (Auswahl)

Name	Headquarters	AS number	CAIDA AS Rank ^[10]	Fiber Route Miles	Fiber Route km	Peering Policy
AT&T ^[11]	United States	7018	23	410,000	660,000 ^[12]	AT&T Peering policy [↗]
CenturyLink (formerly Level 3) ^{[13][14]}	United States	3356	1	750,000	885,139 ^{[15][16]}	North America [↗] ; International [↗] Level 3 Peering Policy [↗]
CenturyLink (formerly Level 3 formerly Global Crossing) ^{[13][14]}	United States	3549	12	750,000	885,139 ^{[15][16]}	North America [↗] ; International [↗] Level 3 Peering Policy [↗]
Deutsche Telekom Global Carrier ^[17]	Germany	3320	20	155,343	250,000 ^[18]	DTAG Peering Details [↗]
GTT Communications, Inc.	United States	3257	3	144,738	232,934 ^{[19][20]}	GTT Peering Policy [↗]
Liberty Global ^{[21][22]}	United Kingdom ^[23]	6830	31	500,000	800,000 ^[24]	Peering Principles [↗]
NTT Communications (America) (formerly Verio) ^[25]	Japan	2914	5	?	?	North America [↗]
Orange (OpenTransit) ^[26]	France	5511	18	?	?	OTI peering policy [↗]
PCCW Global	Hong Kong	3491	9	?	?	Peering policy [↗]
Sprint (SoftBank Group) ^[27]	Japan	1239	27	26,000	42,000 ^[28]	Peering policy [↗]
Tata Communications (formerly Teleglobe) ^[29]	India	6453	6	435,000	700,000 ^[30]	Peering Policy [↗]
Telecom Italia Sparkle (Seabone) ^[31]	Italy	6762	8	347,967	560,000	Peering Policy [↗]

Aufbau des Internet

“Tier-2” ISPs: kleinerer (oft nur Regional tätiger) ISPs

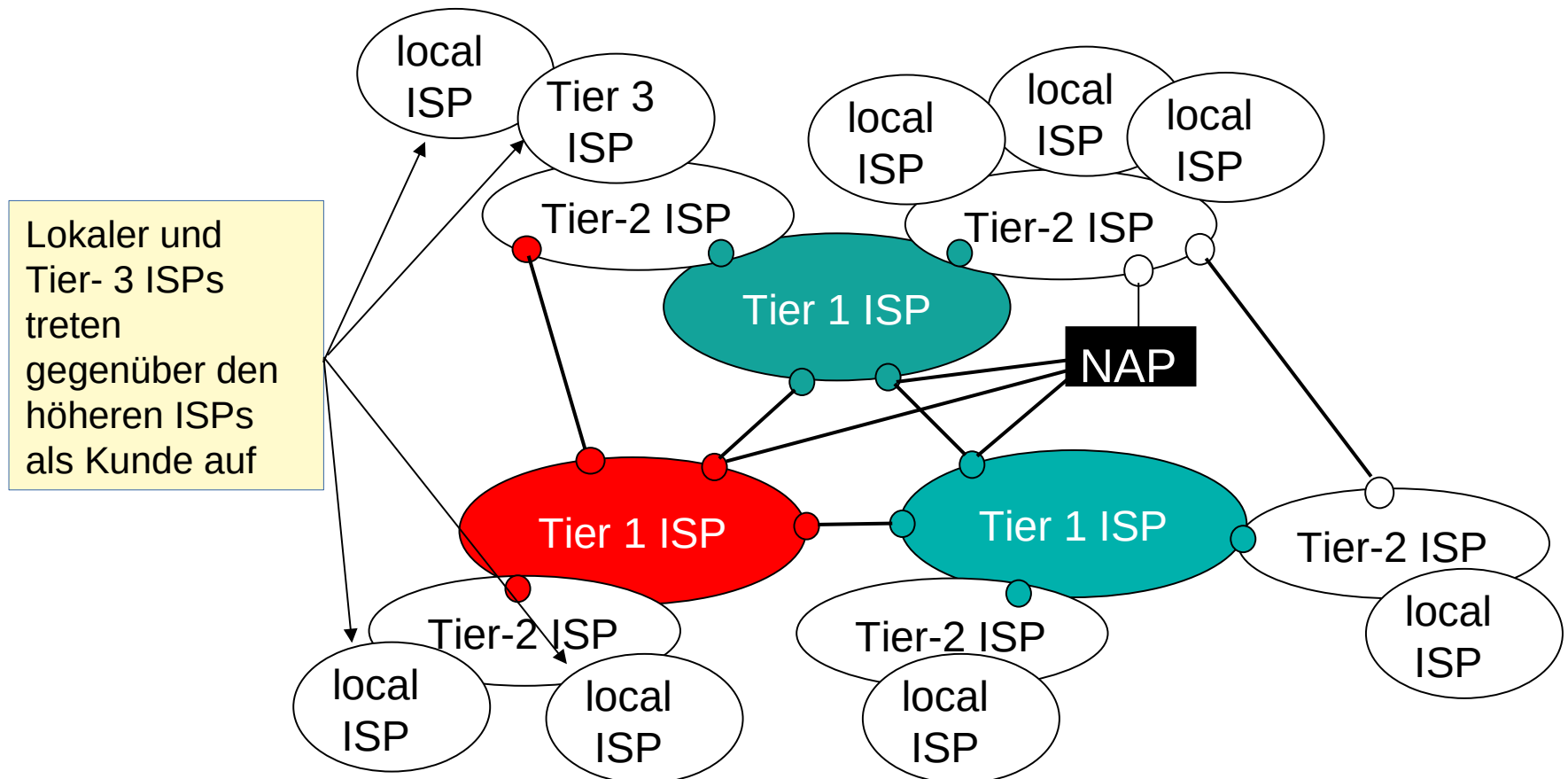
- Anbindung an einen oder mehrerer Tier-1 ISPs
- Ggf. Anbindung an weitere Tier-2 ISPs



Aufbau des Internet

“Tier-3” ISPs und lokale ISPs

- Binden die Kunden an (“access network”, z.B. über DSL)
- Dienst nahe den Endsystemen

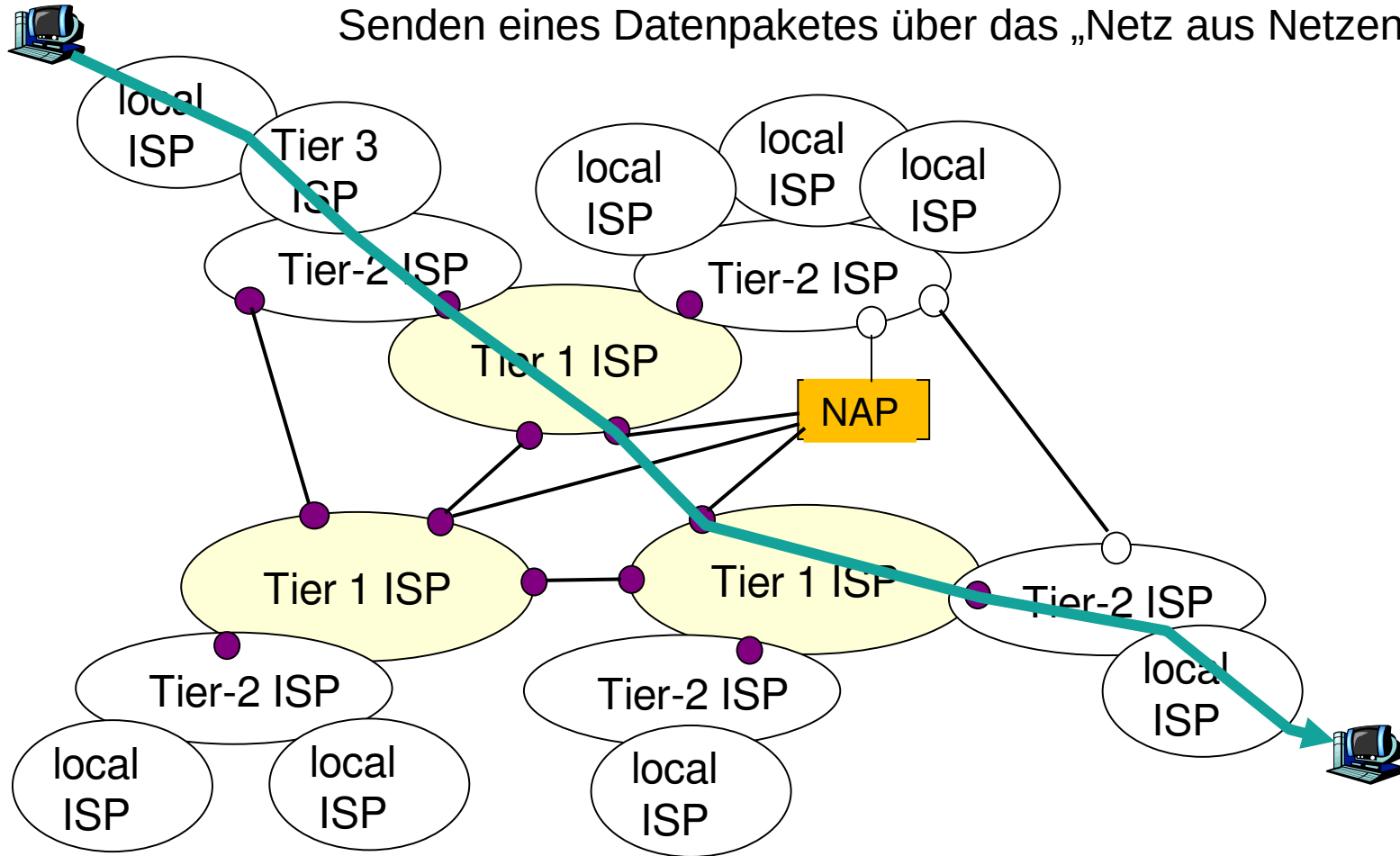


- Das Internet ist grob in drei Schichten (*Tiers*) unterteilt
- Es gibt im Internet viele Eigentümer, so genannte Autonomous Systems (**AS**)
 - Diese können ein eigenes Geschäftsmodell entwickeln
 - Vertragswerke regulieren das Internet
 - Wenn ein AS mehr bei seinem Partner AS einspeist, als die vertragliche Regelung eigentlich erlaubt, dann können Daten verworfen werden...
- Ein Kommunikationsdienst nutzt im Allgemeinen die Infrastruktur mehrerer AS
- Eigentlich regelt das Internet recht wenig, verlangt aber, dass alle die gleiche **Vermittlungsschicht** besitzen

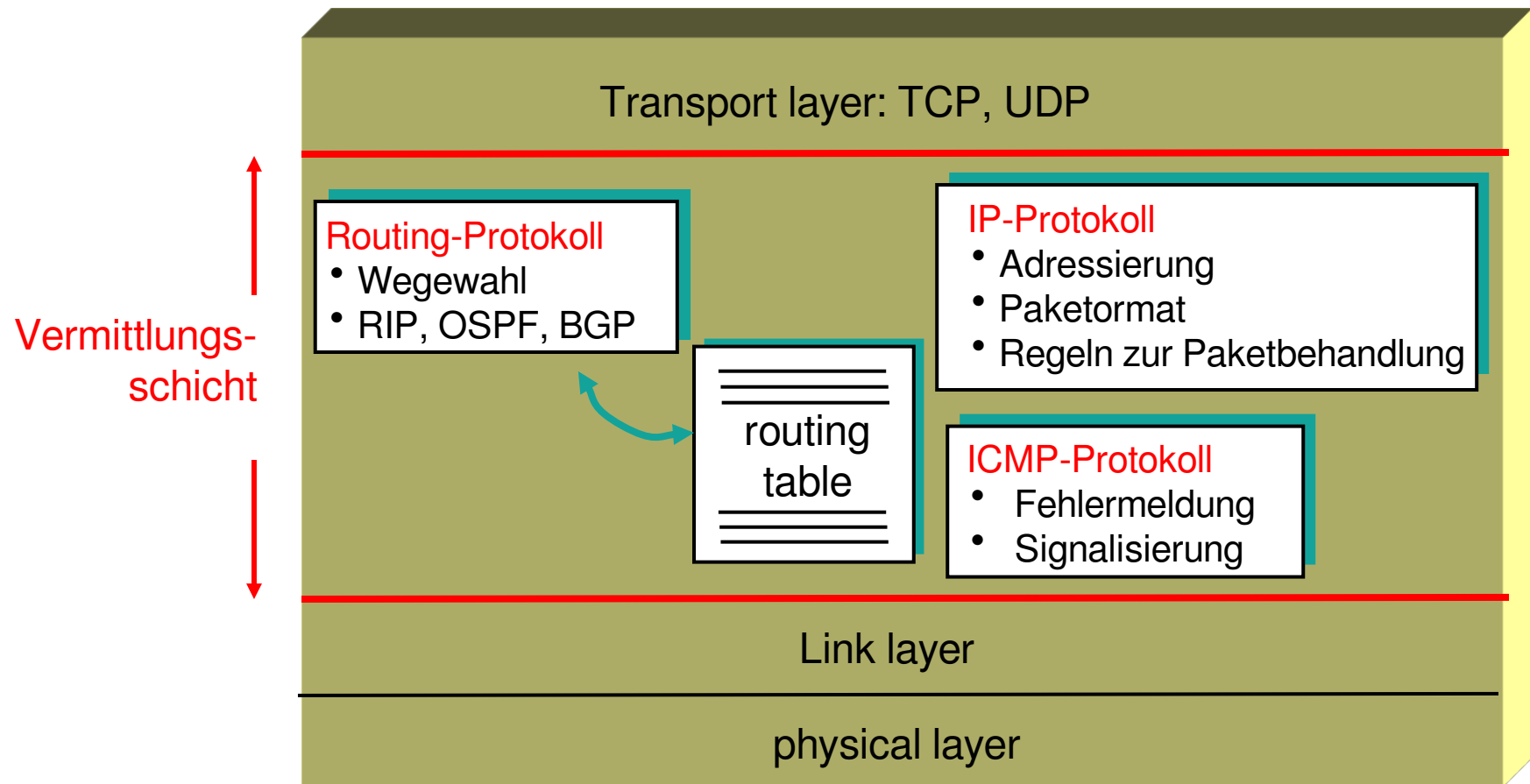
Nachrichtenzustellung

Herausforderung:

Senden eines Datenpaketes über das „Netz aus Netzen“



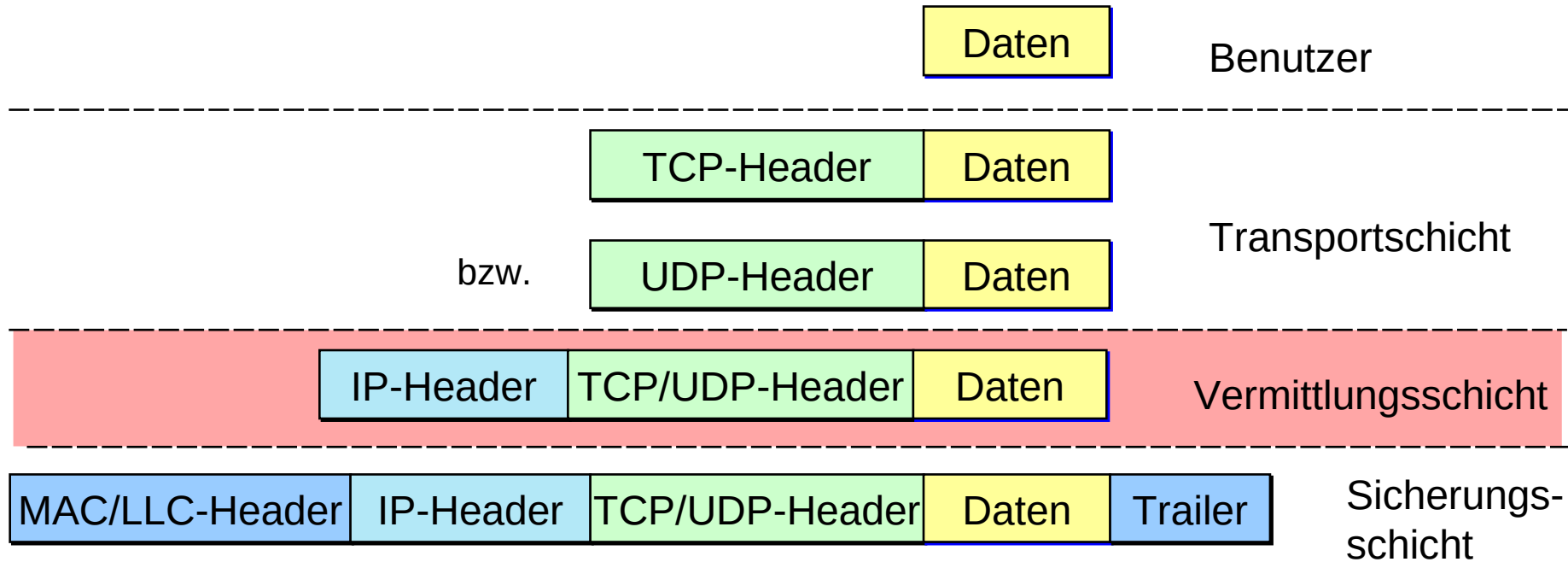
Die Vermittlungsschicht im Internet



- IP bietet eine Ende-zu-Ende-Kommunikation zwischen Rechnern in einem Netz aus Netzen
- Derzeit flächendeckend eingesetzt werden die Protokolle **IPv4** und **IPv6**
- IP ist
 - paketvermittelnd (Datagramme), statisches Netzwerk
 - verbindungslos (Store-and-Forward) und von daher ungesichert:
 - ➔ Simulation einer ‚Sitzung‘ bzw. eines exklusiven Kommunikationskanals über TCP
 - ➔ Datagramme können verloren gehen
 - ➔ Datagramme können einander überholen
 - ➔ theoretisch können Datagramme auch mehrfach ankommen!

Zusammenspiel der Protokollinstanzen

- Prinzip der Kapselung
- TCP/UDP fügen Prozessadressierung (Ports) zu IP hinzu
- TCP sichert darüber hinaus die Datenübertragung
- IP leitet Datenpakete durch das Netzwerk zum Empfänger



IP - Internet Protocol: Aufgaben

Ende-zu-Ende-Kommunikation zwischen Rechnern
auch über Netzgrenzen hinweg

- Bereitstellung **weltweit eindeutiger Adressen**
 - > IPv4: 32 Bit
 - > Topologische Struktur der Adressen
- Definition eines **Paketformats**
 - > Header mit Kontrollinformationen
 - > Maximale Paketgröße: 64 KByte (in der Praxis: 1500 Byte)
- Wegewahl mit **Routing-Tabellen**
(gepflegt durch Routing-Protokolle → später)
- Zusammenspiel mit den tieferen Schichten
(**ARP, Fragmentierung**)

IP - Internet Protocol: Wegefindung

Ein IP-Paket wird an einen entfernten Host, der an einem entfernten Netzwerk angeschlossen ist, übertragen.

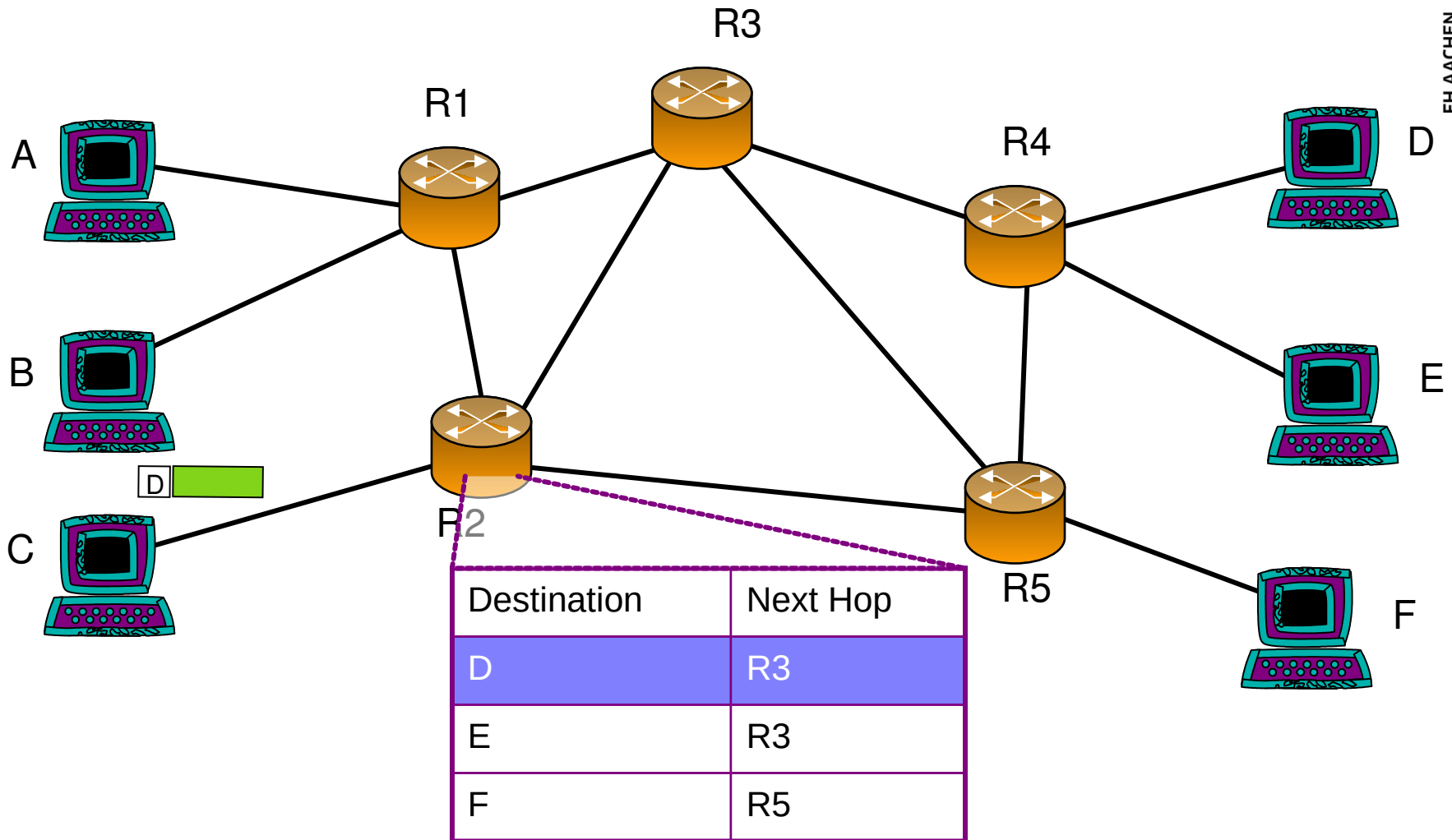
- Zwei Probleme sind daher zu lösen:
 - An welches **Netz** muss ich das Paket weiterleiten, wenn ich noch nicht im Zielnetz bin?
 - An welchen **Rechner** muss ich das Paket weiterleiten, wenn ich im Zielnetz bin?

Die Wegewahl im Internet-Protokoll

- Die IP-Implementierung eines Rechners oder Router-Systems entscheidet, wohin ein Datagramm übertragen wird
- Basis für diese Entscheidung sind die sogenannten **Routing/Forwarding-Tabellen**
- Diese Tabellen werden mittels der Informationen aus dem **IP-Header** durchsucht
- Normalerweise wird hierbei ausschließlich die Zieladresse des Pakets verwendet

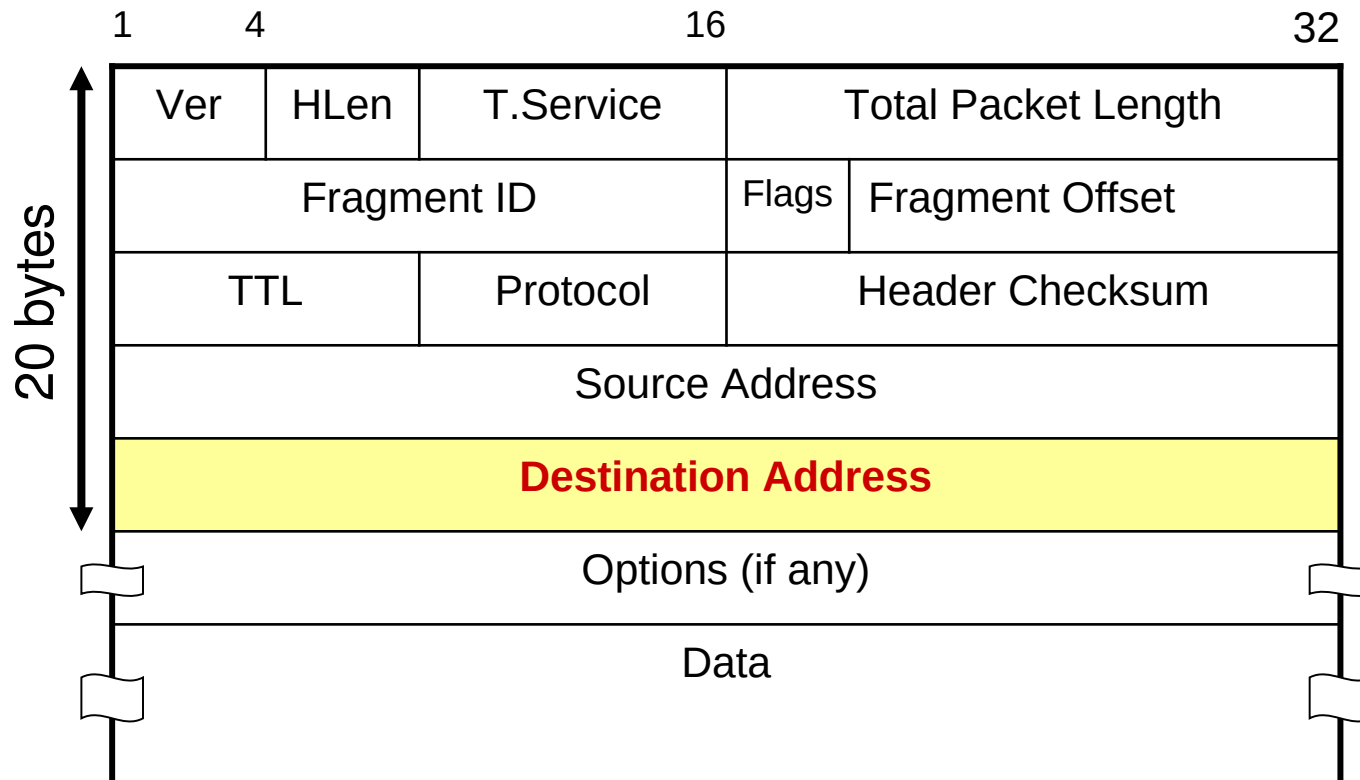
Merke: Jeder Router trifft diese Entscheidung für **jedes Paket** und zwar **unabhängig** von den anderen Routern

Der IP Routing



Der IP Header

- Den Header schauen wir uns noch zu einem späteren Zeitpunkt noch genauer an!
- Hier interessiert uns zunächst die **Ziel-IP-Adresse**, anhand derer der Weg ermittelt wird



Fallunterscheidung innerhalb eines Routers

- Kann das Datagramm **direkt** über Verfahren der Sicherungsschicht **an das Zielsystem** ausgeliefert werden, so wird das Paket zur Übertragung an die Sicherungsschicht weiter geleitet
 - Beide Systeme befinden sich im „gleichen Netz“ sein
 - Router muss irgendwie die HW-Adresse der Schicht 2 in Erfahrung bringen, um der Netzwerkkarte mitzuteilen, an wen sie übertragen soll
- Kann man **nicht direkt** mit dem Zielsystem kommunizieren, so muss die Nachricht **an einen weiteren “Router“** weiter geleitet werden, der sich in einem gleichen Netz befindet
 - Das Zielsystem befindet sich in einem anderen Netz
 - Mittels der Routing-Tabelle ermittelt das System, welcher direkt erreichbare Router das Paket zur Weiterleitung erhält (analog zum ersten Fall, der Router ist aus dieser Sicht einfach nur ein anderer Rechner).
 - Das Paket wird an die Sicherungsschicht zur Übertragung an den selektierten Router geleitet (indirekte Übertragung), die HW-Adresse des anderen Routers muss in Erfahrung gebracht werden.

Fallunterscheidung innerhalb eines Routers

Merke:

Router haben grundsätzlich Anschlüsse in mehr als in einem Netz!

Damit muss die IP-Vermittlungsschicht entscheiden, ob sich ein Zielrechner in einem der Netze befindet, an den der Router angeschlossen ist!

Der Router muss aus der Zieladresse also 2 Informationen extrahieren:

- In welches **Netz** muss das Paket ausgeliefert werden?
- Falls Router das Zielsystem direkt erreichen kann (also eine direkte Verbindung zum Zielnetz besitzt):
An welchen **Rechner** muss das Paket ausgeliefert werden?

Die Adresse muss also Informationen über das
Ziel-**Netz** und den Ziel-**Rechner** enthalten!
(vgl.: Vorwahl/Durchwahl beim Telefonieren)

IP-Adressierung (v4)

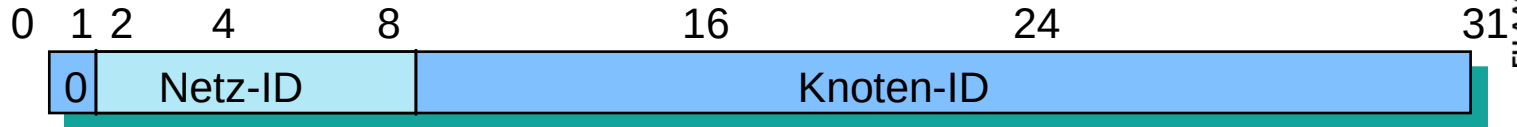
- Am Internet angeschlossene Systeme werden über eine weltweit eindeutige IP-Adresse identifiziert (Ausnahme: private Netze)
- IP-Adressen sind 32 Bit lang
- IP-Adressen haben eine bestimmte Struktur:
 - Der **vordere Teil bestimmt die Netzwerk-Adresse** für das **Netz** (z.B. **140.201**.10 .100), in dem sich der Rechner befindet. Innerhalb dieses Netzes kann eine direkte Kommunikation mittels der Sicherungsschicht geschehen
 - Der **hintere Teile bestimmt die Rechner-Adresse im gegebenen Netz** für einen Kommunikationsendpunkt, einen **Host** (z.B. 140.201.**10** **.100**)

Um unterschiedlich große Netze zu unterstützen wurden mehrere Adressklassen definiert

(Heute wird zwar noch die Terminologie verwendet, aber nicht mehr diese recht statische Klassenaufteilung!)

IP-Adressklassen: Der ursprüngliche Ansatz

1. Class A für Netze mit bis zu 16 Mio. Knoten (0-127)



2. Class B für Netze mit bis zu 65.536 Knoten (128-191)



3. Class C für Netze mit bis zu 256 Knoten (192-223)



4. Class D für Gruppenkommunikation (Multicast) (224)



5. Class E, noch reserviert für zukünftige Anwendungen



Aufteilung der IP Adresse in eine

- Netz-ID
- Knoten-ID

Bei der Interpretation der IP-Adressen sind für den Rechnerteil (Knoten-ID im Netz) zwei Adressen reserviert:

Knoten-ID = 0...0 bezeichnet das Netz selber

Knoten-ID = 1...1 bezeichnet eine Broadcast im Netz

IP-Adressen / Adressklassen

Class	Start	Ende	Anzahl Netze	Rechner / Netz
A	1.0.0.0	127.255.255.255	127	16.777.214
B	128.0.0.0	191.255.255.255	16384	65534
C	192.0.0.0	223.255.255.255	2.097.152	254
D	224.0.0.0	239.255.255.255	<i>Multicast</i>	
E	240.0.0.0	255.255.255.254	<i>Reserved</i>	

IP-Adressen / Private Netzwerke

Netzadressbereich	CIDR- Notation	Verkürzte CIDR- Notation	Anzahl Adressen	Anzahl Netze gemäß Netzklasse (historisch)
10.0.0.0 bis 10.255.255.255	10.0.0.0/8	10/8	$2^{24} =$ 16.777.216	Klasse A: 1 privates Netz mit 16.777.216 Adressen; 10.0.0.0/8
172.16.0.0 bis 172.31.255.255	172.16.0.0/12	172.16/12	$2^{20} =$ 1.048.576	Klasse B: 16 private Netze mit jeweils 65.536 Adressen; 172.16.0.0/16 bis 172.31.0.0/16
192.168.0.0 bis 192.168.255.255	192.168.0.0/16	192.168/16	$2^{16} =$ 65.536	Klasse C: 256 private Netze mit jeweils 256 Adressen; 192.168.0.0/24 bis 192.168.255.0/24

Die Loopback-Adresse

Eine Loopback-Adresse kann immer dann verwendet werden, wenn eine Kommunikation mit einer Zielanwendung statt finden soll, die auf dem gleichen Rechner läuft

Während IP-Adresse faktisch sonst immer mit einer Netzwerkkarte assoziiert sind ist ein Loopback nicht mit einer physikalisch vorhandenen Karte assoziiert

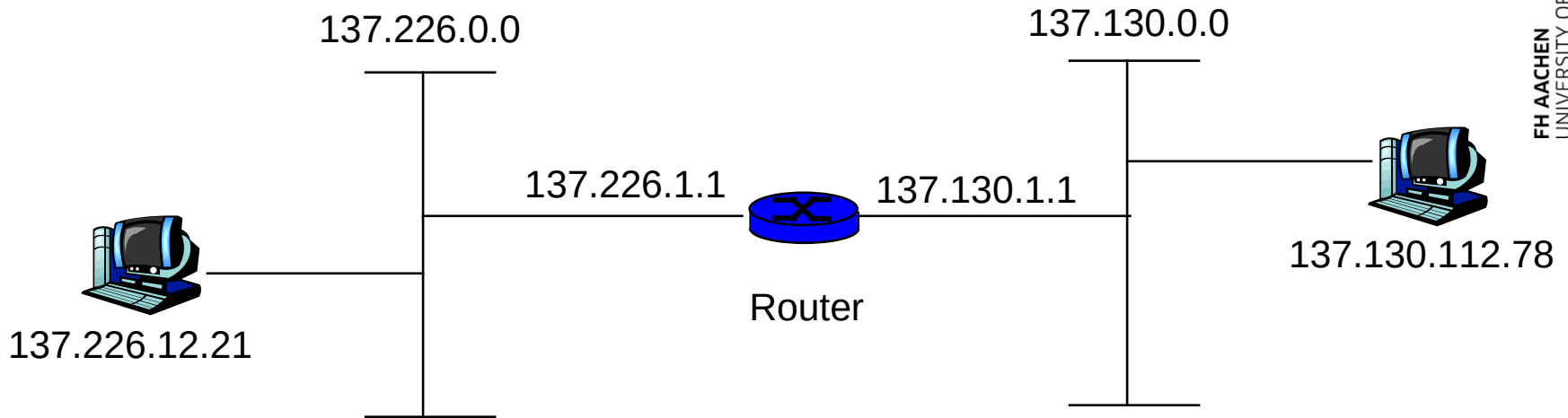
Damit beschreitet die Kommunikation die Anwendungs-Transport und Vermittlungsschicht und geht über das Loopback direkt über Vermittlungs-, Transport- zur Anwendungsschicht

Eine zu konfigurierende Netzwerkkarte wird nicht angesprochen

127.x.x.x ist reserviert (loopback = 127.0.0.1)

Merke: Auch wenn man verschwenderisch für das Loopback eine Class-A-Adresse vorgehen hat, so schreibt der Standard RFC3330 doch vor, dass die Adresse 127.0.0.1 das (virtuelle) Loopback-Interface bezeichnet

IP-Adresse

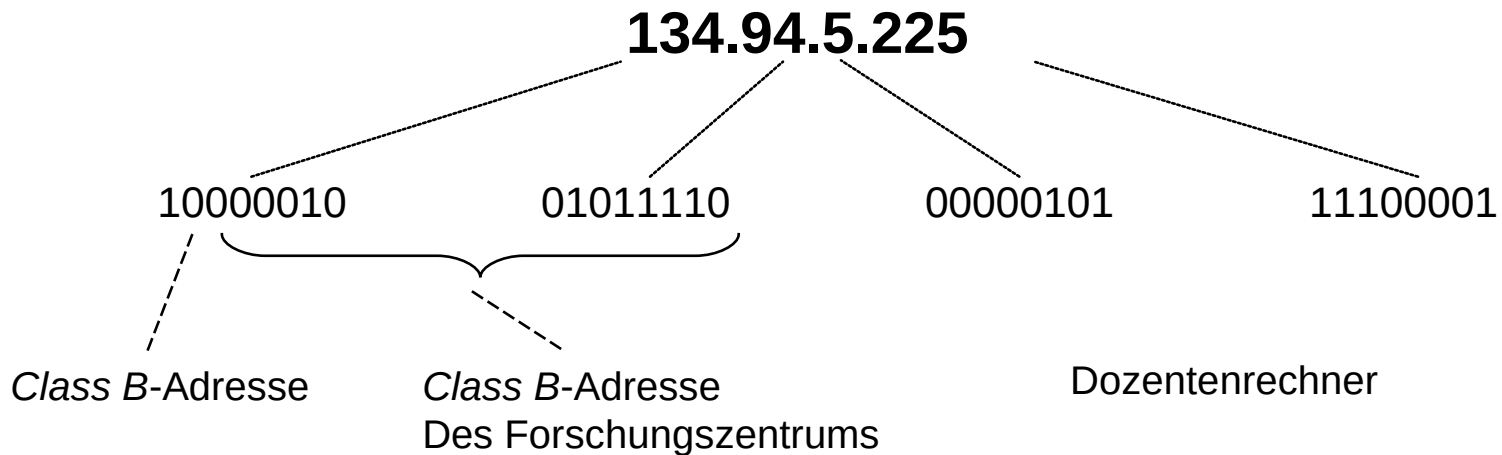


Binärformat	10001001 11100010 00001100 00010101
Dotted Decimal Notation	137.226.12.21

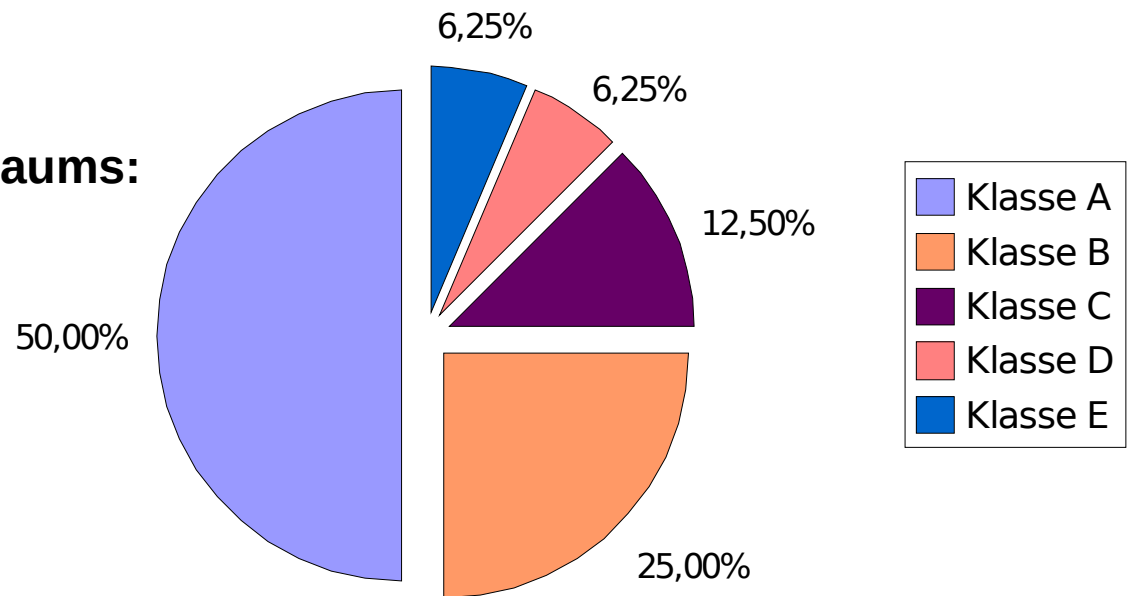
- jeder Rechner hat (wenigstens) eine weltweit eindeutige IP-Adresse
 - **Ausnahme: private Adressen mit Adressumsetzung** im Router: 10.x.x.x, 172.16.0.0 - 172.31.255.255 192.168.0.0 - 192.168.255.255
- Router oder Gateways, die mehrere Netze miteinander verknüpfen, haben für jedes angeschlossene Netz eine IP-Adresse

IP-Adressierung - Beispiele

Die Darstellung der 32-Bit-Adresse erfolgt in 4 Teilstücken zu je 8 Bit:



Aufteilung des Adressraums:



IP-Adressen werden knapp...

Problem

- Niemand hatte damals mit einem derart starken Wachstum des Internet gerechnet (sonst hätte man von Anfang an längere Adressen definiert)
- Allzu viele Class A-Adressen wurden in den ersten Internetjahren vergeben
- Ineffiziente Nutzung des Adressraums

Beispiel: wenn 500 Geräte in einem Unternehmen angeschlossen werden sollen, braucht man eine Class B-Adresse, die unnötigerweise mehr als 65.000 Rechneradressen blockiert.

Lösungsversuch

Erweiterung des Adressraums bei IPv6 gegenüber der aktuellen Version IPv4

- ⇒ IP Version 6 hat 128 Bit-Adressen
- ⇒ 7×10^{15} IP-Adressen pro Quadratmillimeter der Erdoberfläche (incl. der Ozeane!)
- ⇒ Vergleich IPv4: 8,5 IP-Adressen pro Quadratkilometer!

Ein weiteres Problem...

- Router verbinden immer Netze, wodurch beispielsweise unterschiedliche Netztechniken in den einzelnen Netzen eingesetzt werden können
- Damit **erfordern** sie aber auch eine **Änderung der Netzadresse**, wenn sie in mehreren Netzen sein sollen
- Router trennen damit Netze, was diesen eine verbesserte Struktur gibt
- Institutionen mit größeren Netzen möchten auch intern Router verwenden (strukturierte Netzplanung)
- Noch haben diese aber immer nur „eine“ an sie vergebene Netzadresse

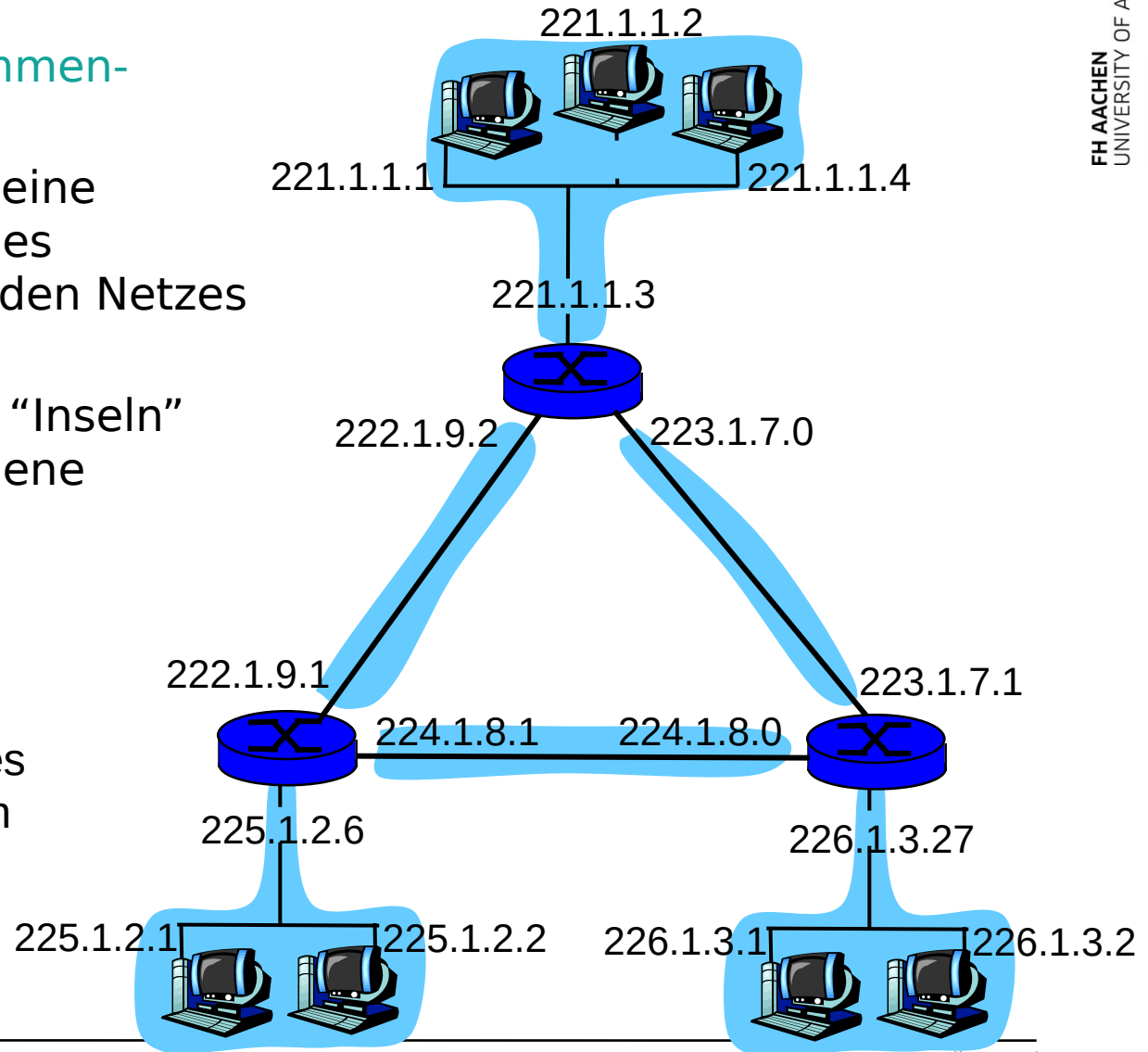
IP-Adressierung - Bedeutung des Netzadressessteils

Wie findet man zusammenhängende Netze?

- Jeder Router stellt eine Unterbrechung eines zusammenhängenden Netzes dar
- Die verbleibenden “Inseln” benötigen eine eigene Netzadresse

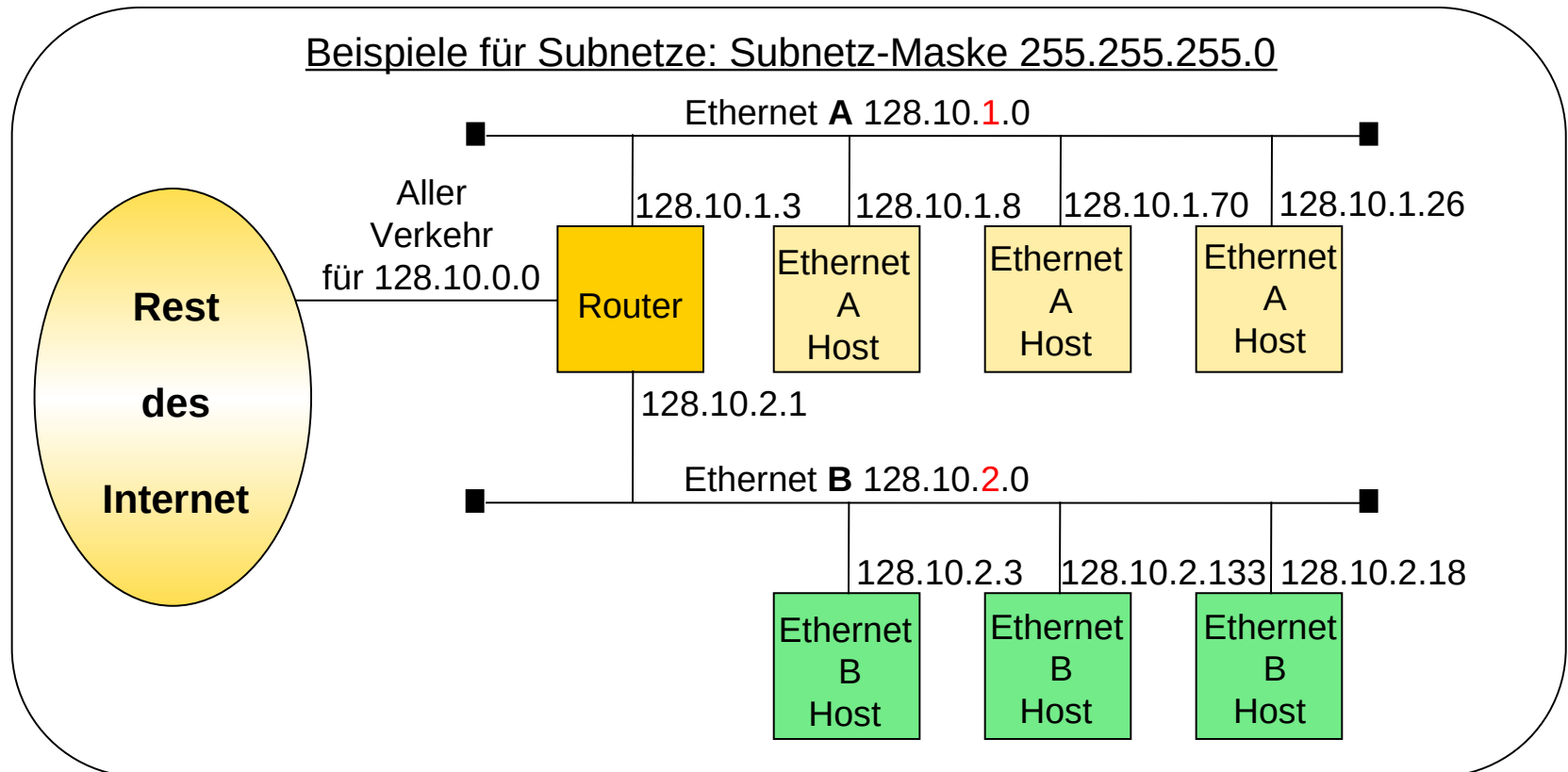
→ Subnetze!!!

Netzwerk, welches aus sechs Netzen besteht



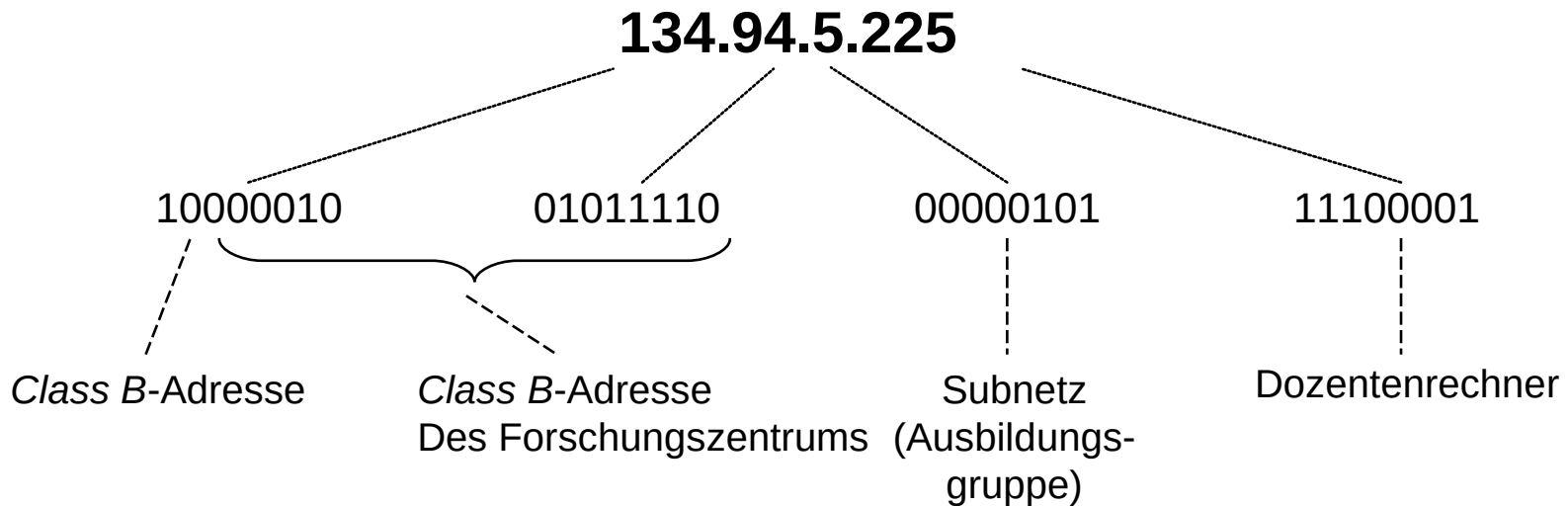
IP-Subnetze

Problem: Class C-Netze sind sehr klein, Class B-Netze oft aber schon wieder zu groß, um sie ohne Router zu konzipieren. Daher gibt es die Möglichkeit, ein durch die IP-Adresse identifiziertes Netz in so genannte **Subnetze** zu zerlegen.



IP-Adressierung - Subnetze

Die Darstellung der 32-Bit-Adresse erfolgt in 4 Teilstücken zu je 8 Bit:

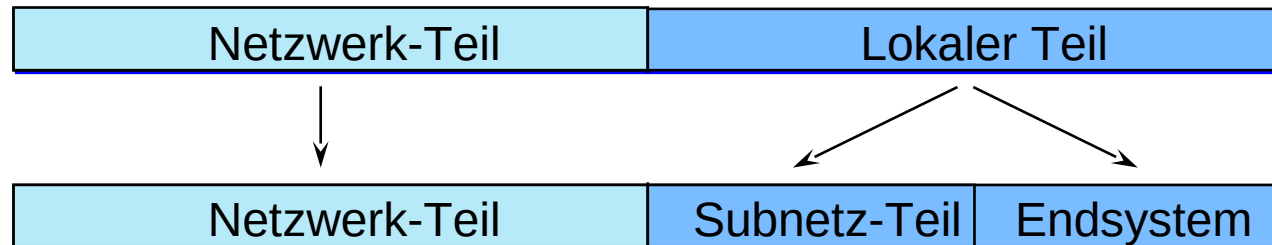


Mittels der Subnetzmaske wird eine Folge **zusammenhängender** Bits der Adresse angegeben, die den Netzwerkadressteil bestimmt.

1...10...0

IP-Subnetz-Adressen

- **IP-Adresse** (hier Klasse B):



- **Subnetzmasken** kennzeichnen den Bereich der IP-Adresse, der das Netzwerk und das Subnetzwerk beschreibt. Dieser Bereich wird dabei durch Einsen („1“) in der binären Form der Subnetzmaske festgestellt.

- Beispiel:

	140.	201.	10.	100
	255.	255.	255.	0
Netzwerk:	140.	201.		
Subnetz:			10.	
Endsystem:				100

- Der Netzwerk-Teil kann aus der Adressklasse abgeleitet werden
- Überdeckt die Subnetzmaske nur den Netzwerk-Teil, dann gibt es keinen Subnetz-Teil (z.B. 255.255.0.0)

Beachten Sie...

- Die Subnetzmaske ist faktisch eine binäre Maske
- Sie beginnt mit einer 1 und es gibt nur einen Wechsel auf 0
- Sie wird über die Binärdarstellung der Zieladresse gelegt
- Die UND-Verknüpfung liefert die Netzwerkadresse (Knoten-ID = 0...0 bezeichnet ja das Netzwerk!)

IP-Subnetze - Berechnung des Zielhosts

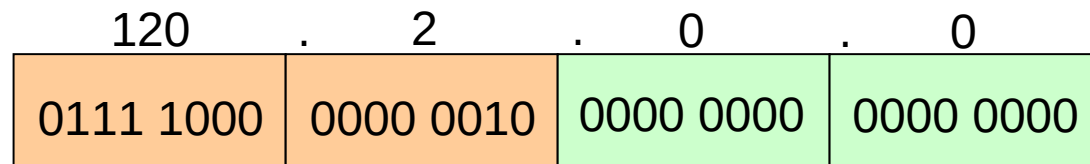
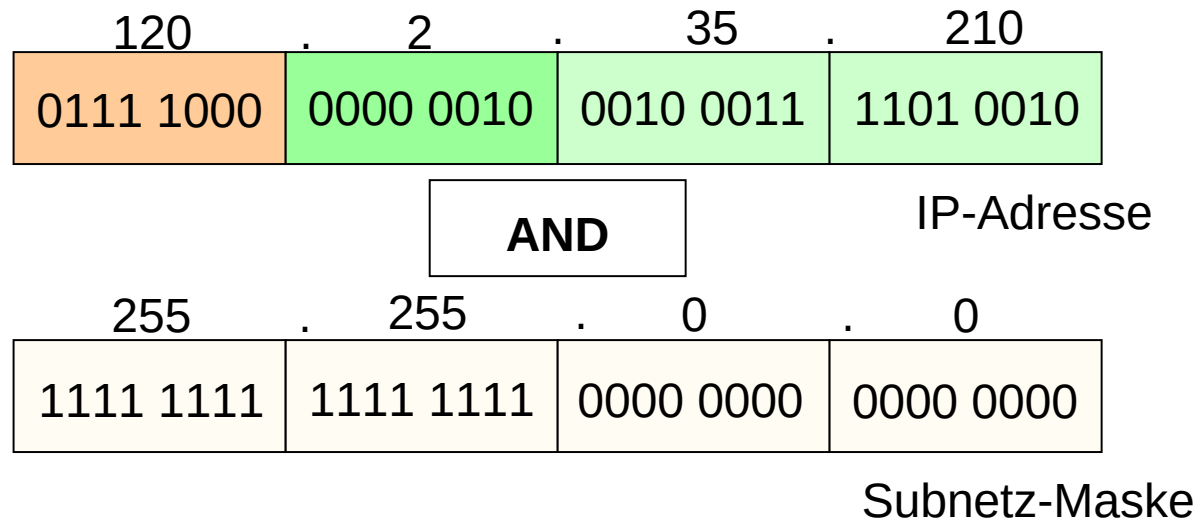
140 .	201 .	10 .	100
10001100	11101001	00001010	11000100
AND			
255 .	255 .	255 .	0
1111 1111	1111 1111	1111 1111	0000 0000
Subnetz-Maske			

140 .	201 .	10 .	0
10001100	11101001	0000 1010	0000 0000

Netzwerk des bezeichneten Hosts
nach Anwendung des Subnetz-Regel

IP-Subnetze - Berechnung des Zielhosts

Keine Aufteilung in Subnetze, es liegt ein virtuelles Class-B-Netz vor:



Netzwerk des bezeichneten Hosts

Beachten Sie...

Subnetzmasken...

- können Netze unterteilen
 - erschweren das Erkennen der Netzadressteile (nicht für den Rechner)
 - haben lokale Bedeutung (auf dem System auf dem sie konfiguriert sind)
 - gehören zur systematischen Netzplanung hinzu
-
- Innerhalb eines Subnetzes sollte die Rechneradresse (binär) „0...0“ und die Rechneradresse (binär) „1....1“ nicht verwendet werden

Warum nicht?

Aufgabe:

Sie haben die Class-B-Adresse 134.94.0.0 erhalten

Bestimmen Sie eine Subnetzmaske, mit der Sie dieses Netz in 16 Subnetze untergliedern

Geben Sie für die ersten beiden Netze den Adressbereich für Rechner in diesem Netz an

Sie haben die Class-B-Adresse 134.94.0.0 erhalten

Welche Subnetzmaske müssen Sie nehmen, wenn Sie das Netz in 12 Unternetze aufteilen wollen?

FH Aachen
Fachbereich 9 Medizintechnik und Technomathematik
Prof. Dr.-Ing. Andreas Terstegge
Straße Nr.
PLZ Ort
T +49. 241. 6009 53813
F +49. 241. 6009 53119
Terstegge@fh-aachen.de
www.fh-aachen.de