

---

# Datenkommunikation

Internet und IP-Protokoll

Wintersemester 2011/2012

# Überblick

---

1	Grundlagen von Rechnernetzen, Teil 1
2	Grundlagen von Rechnernetzen, Teil 2
3	Transportzugriff
4	Transportschicht, Grundlagen
5	Transportschicht, TCP (1)
6	Transportschicht, TCP (2) und UDP
7	Vermittlungsschicht, Grundlagen
8	Vermittlungsschicht, Internet
9	Vermittlungsschicht, Routing
10	Vermittlungsschicht, Steuerprotokolle und IPv6
11	Anwendungsschicht, Fallstudien
12	Mobile IP und TCP

## **1. Überblick**

- Internet-Vermittlungsschicht
- Autonome Systeme (AS)
- Organisation
- IPv4: Überblick und Aufgaben

## **2. IPv4-Adressierung**

- IPv4: Adressierung und Adressenknappheit
- IPv4-Subnetting
- VLSM und CIDR

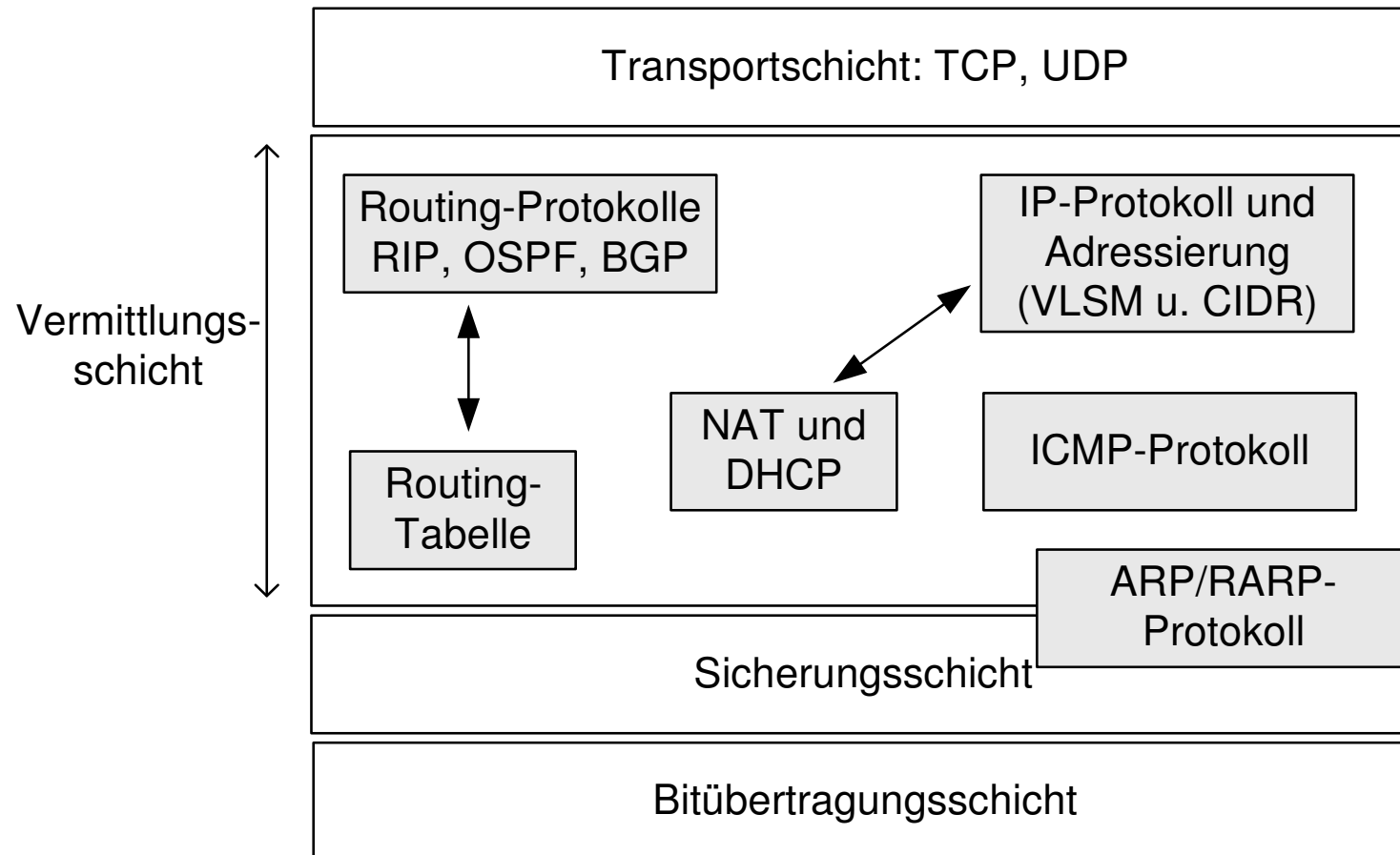
## **3. IPv4-PDU**

- Aufbau und Felder

## **4. Fragmentierung**

# Überblick: Die Internet-Vermittlungsschicht

---

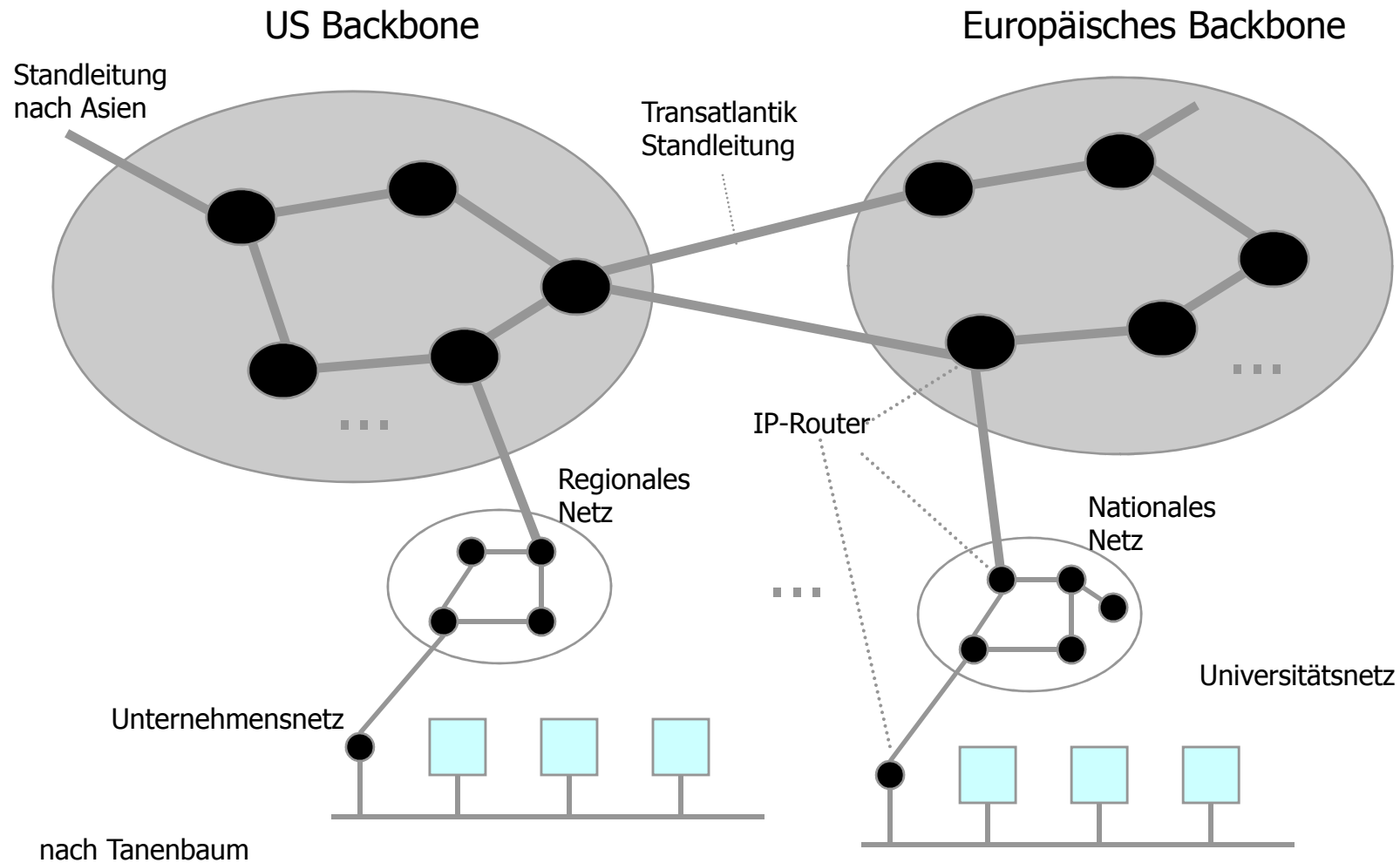


## Überblick über das Internet

---

- Das Internet ist eine **hierarchische Organisation** des Netzwerks
- **Große Backbones** sind über Leitungen mit hoher Bandbreite und schnellen Routern verbunden
- An den Backbones hängen **regionale Netze**
- An den regionalen Netzen hängen die **Netze von Unternehmen, Universitäten, Internet Service Providern (ISP),...**
- Der Zugriff über das Internet von Deutschland aus auf einen Server in den USA wird über mehrere IP-Router geroutet

# Überblick über das Internet, Backbone

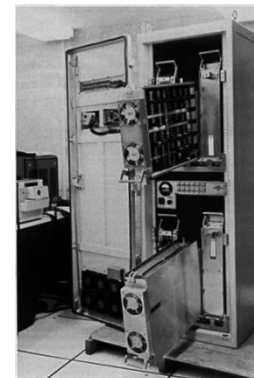


## Das Internet heute, AS

---

- Autonome Systeme haben sich unterschiedlich entwickelt → z.B. verschiedene Routing-Strategien
- Es gibt derzeit mehr als 110.000 autonome Systeme weltweit
- Jedes AS hat eine **eindeutige Nummer**
  - 11, Harvard-University
  - 1248, Nokia
  - 2022, Siemens
  - 3680, Novell
  - 4183, CompuServe
  - 6142, Sun
  - 12816, MWN

ARPANET-IMP



# Das Internet heute, Begriffe

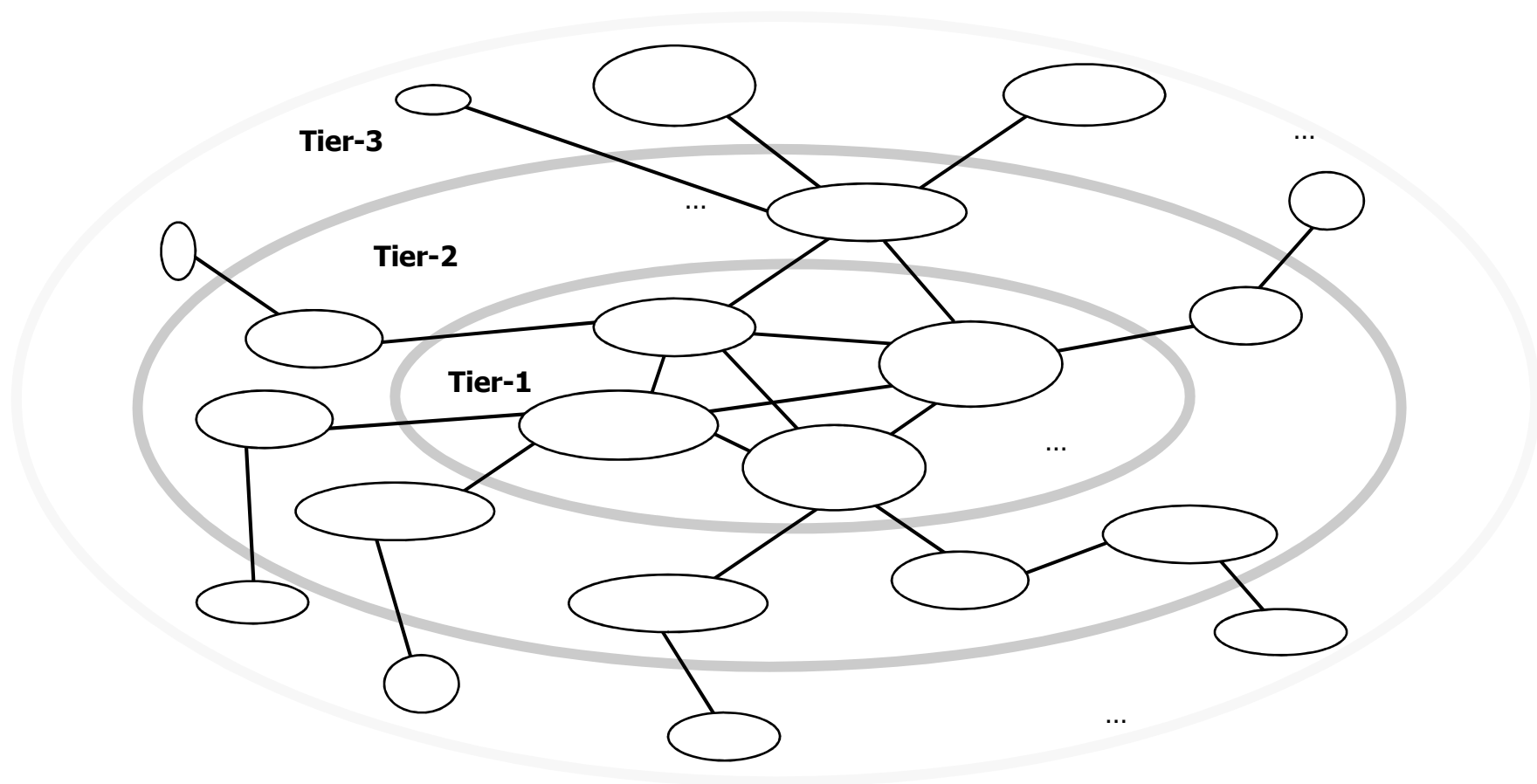
---

- Autonome Systeme = AS
- Internet-Provider = Provider
- Tier-1-AS, Tier-2-AS, Tier-3-AS (andere Bezeichnung: Tier-x-Netzwerke)
  - Edge-Networks = Tier-1-AS
- Internet-Knoten
  - = IX (Internet Exchange) = IXP (Internet Exchange Point)
  - = NAP (Network Access Point) → USA
- Public und private Peering-Points
- Peering-Agreement = Peering-Vereinbarung:
  - Übertragung ohne Gebühr bei gleichberechtigten Peers
- Transit-Vereinbarung:
  - Gebühr nach vereinbarter Bandbreite



# Das Internet heute, Verbindungen zwischen AS

---



# Das Internet heute: AS-Kategorien

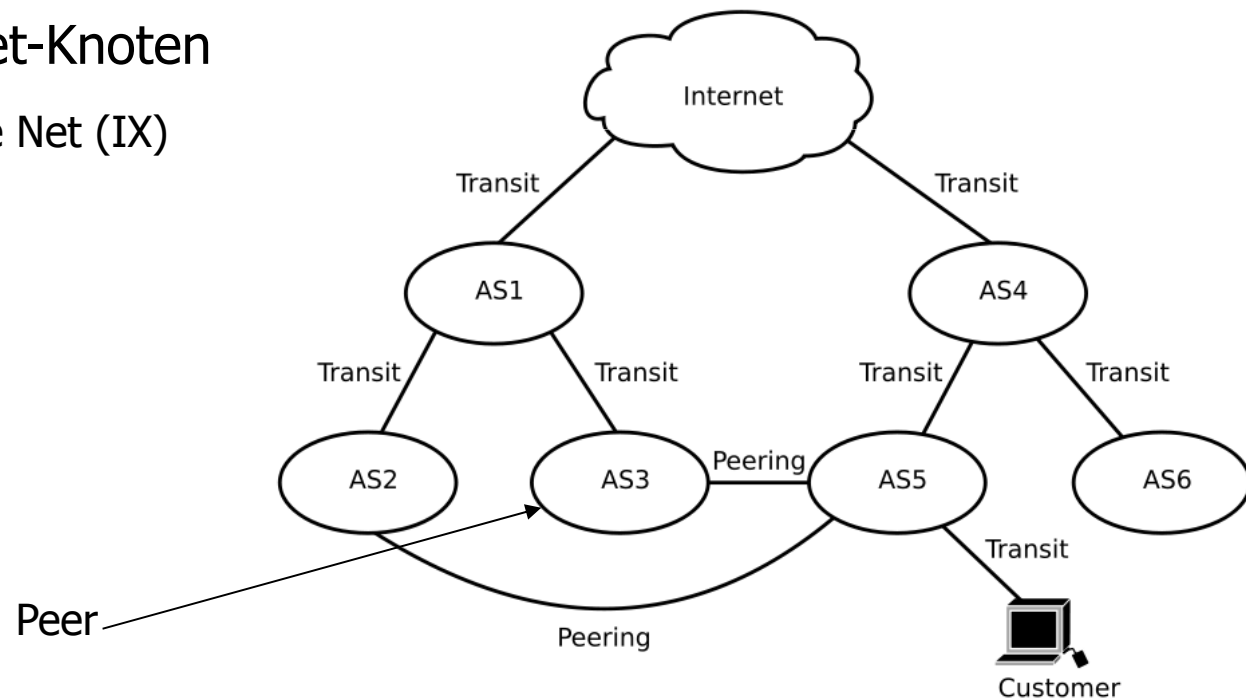
---

- **Tier-3:** Kleine, lokale Provider, Endkundengeschäft
  - M-net in Bayern (Hauptgesellschafter: Münchner Stadtwerke)
  - Hansenet (Hamburg, Tochter der Telecom Italia)
  - Versatel (Berlin)
- **Tier-2:** Betreiber großer, überregionaler Netze
  - Deutsche Telekom
  - France Telecom und France Telecom
  - Tiscali (Telekom-Unternehmen, Italien)
- **Tier-1:** Betreiber von globalen Internet-Backbones
  - AT&T (US-amerikanischer Telekoanbieter)
  - AOL (US-amerikanischer Online-Dienst)
  - NTT (Nippon Telegraph and Telephone Corporation)
  - Verizon Communications (US-amerikanischer Telekomanbieter)

# Das Internet heute, Kunden – Provider - Peers

---

- Rollen: Kunden - Provider - Peers
- Peering-Abkommen zwischen AS (Tier-1, Tier-2, Tier-3)
- Tier-1-Provider „peeren“ kostenlos miteinander, die anderen je nach Vereinbarung
- Netz aus Internet-Knoten  
→ Internet Exchange Net (IX)

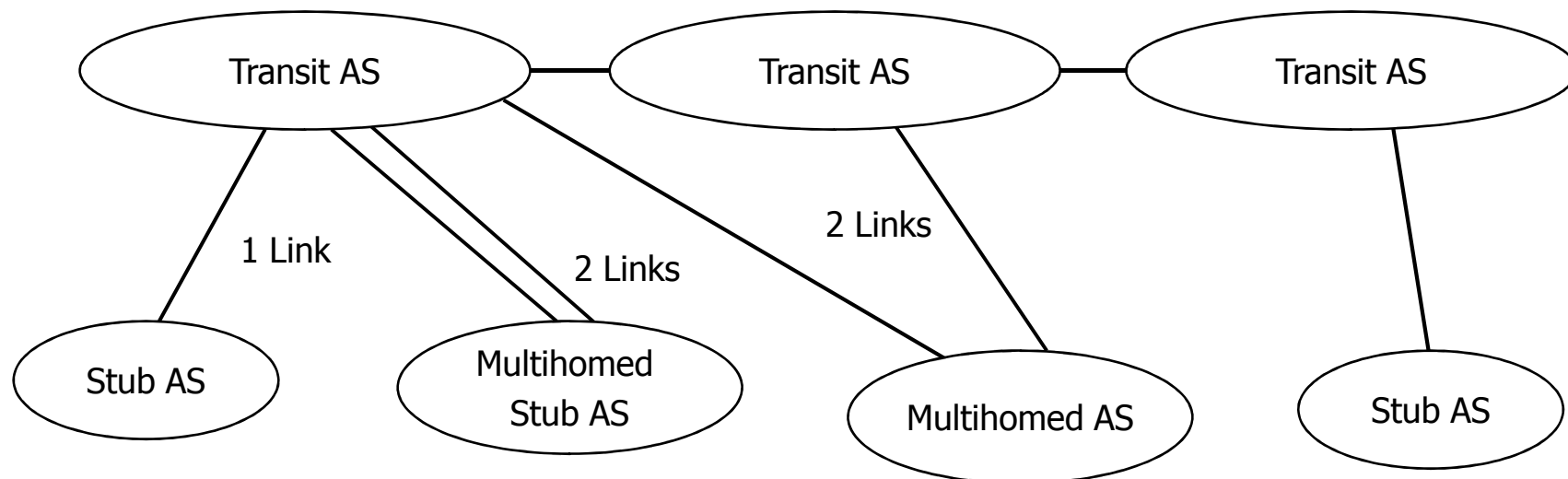


Quelle: Wikipedia

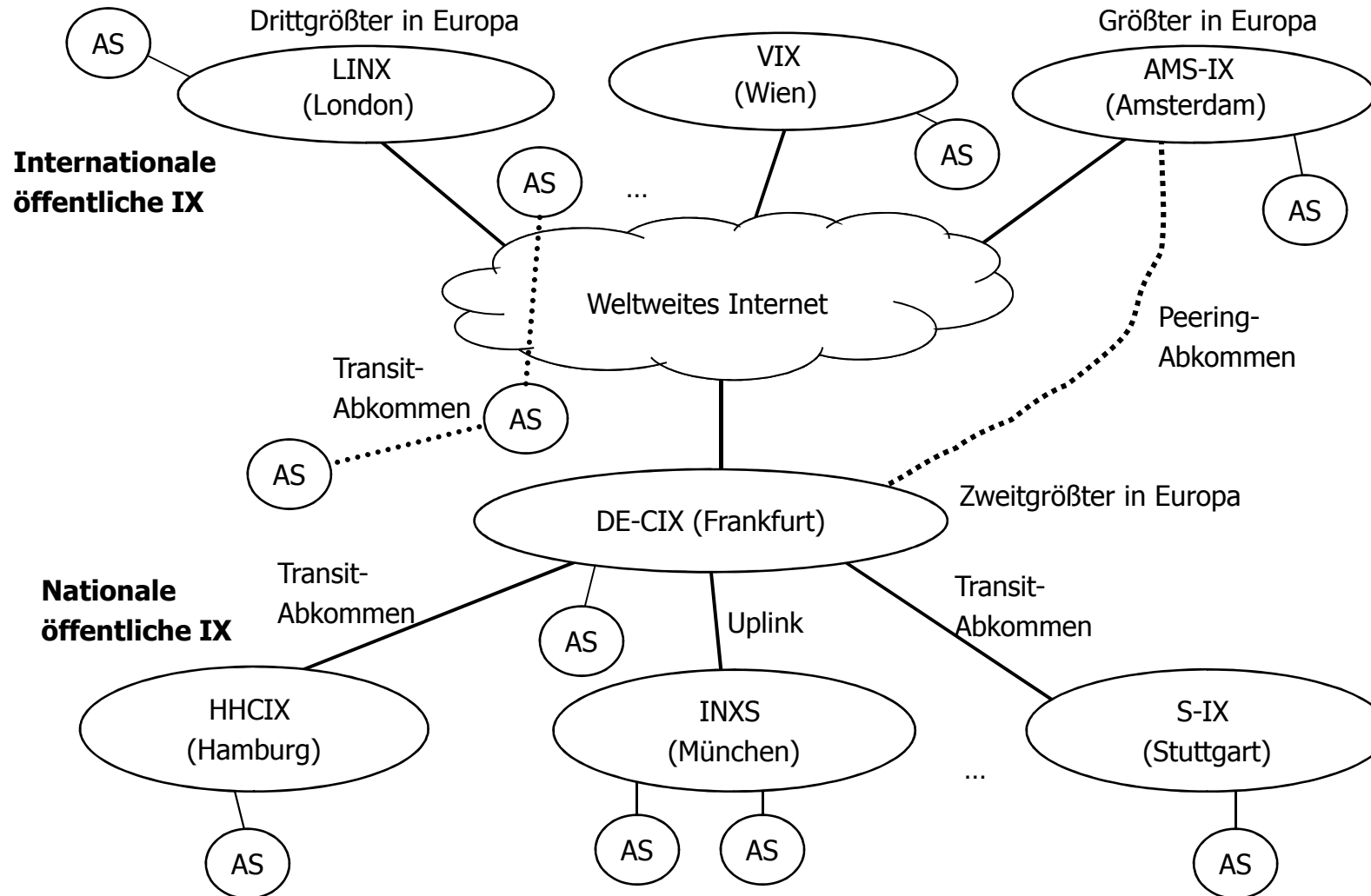
# Das Internet heute, Links

---

- Begriffe:
  - Stub AS (sollte es nicht geben)
  - Multihomed Stub AS
  - Multihomed AS



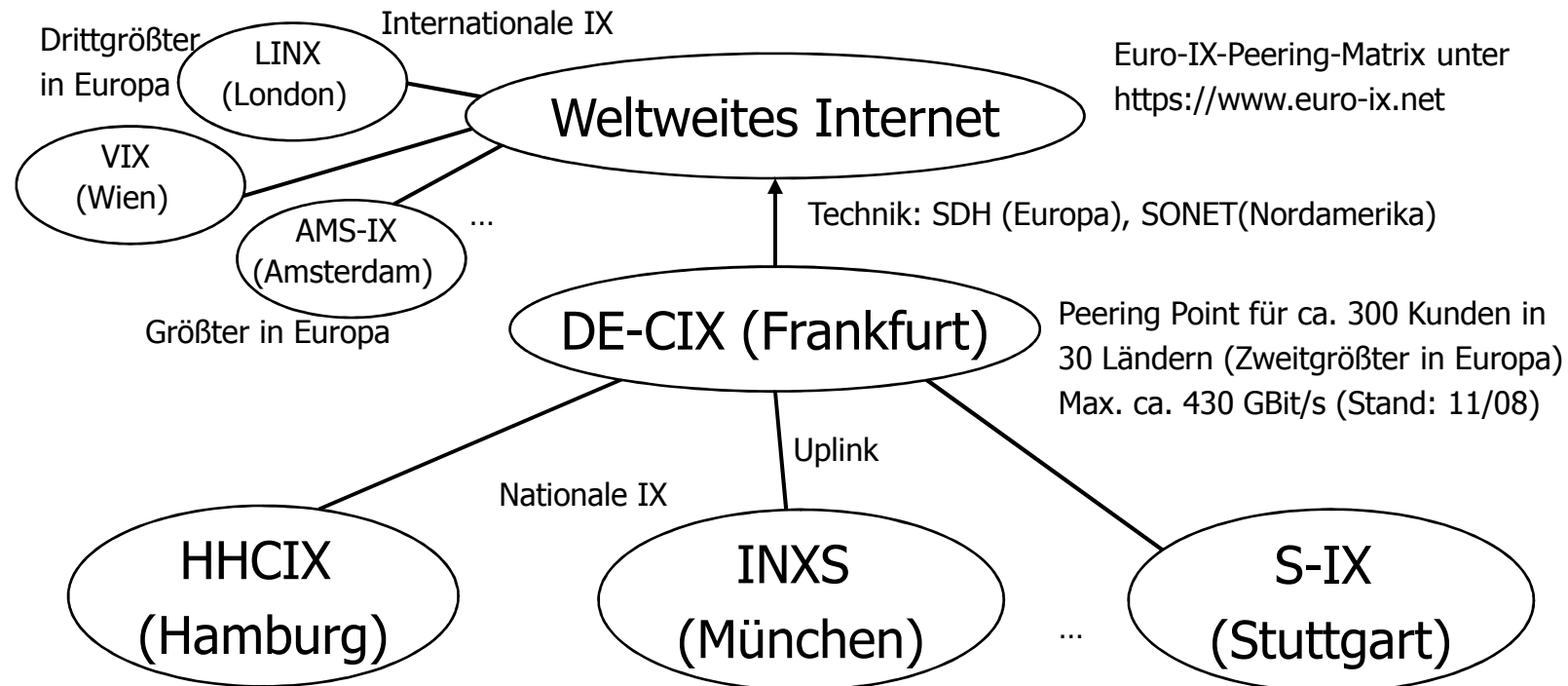
# Das Internet heute, Typische Verbindungen



## Das Internet heute, physikalische Sicht

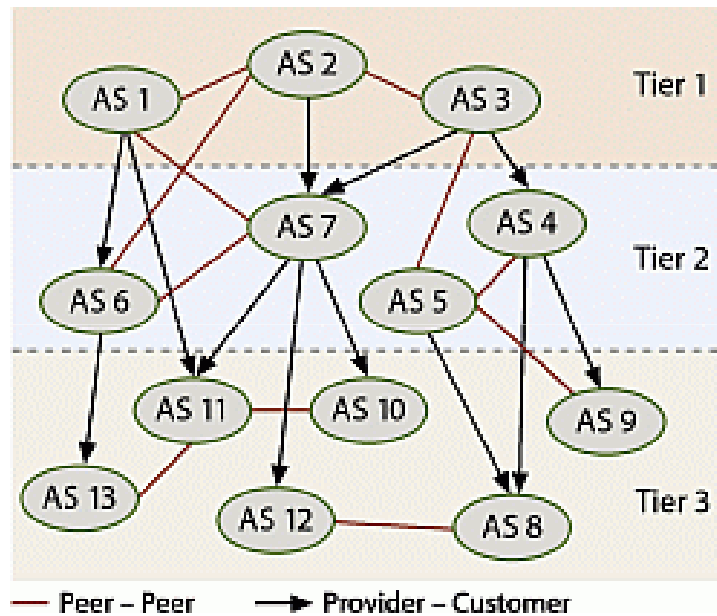
---

- DE-CIX Management GmbH: Betreibt DE-CIX international Internet Exchange („IX“) in Frankfurt
- Einer der größten IX weltweit (<http://www.de-cix.de>)
- Top-80 in Europa: <http://www.alrond.com/de>

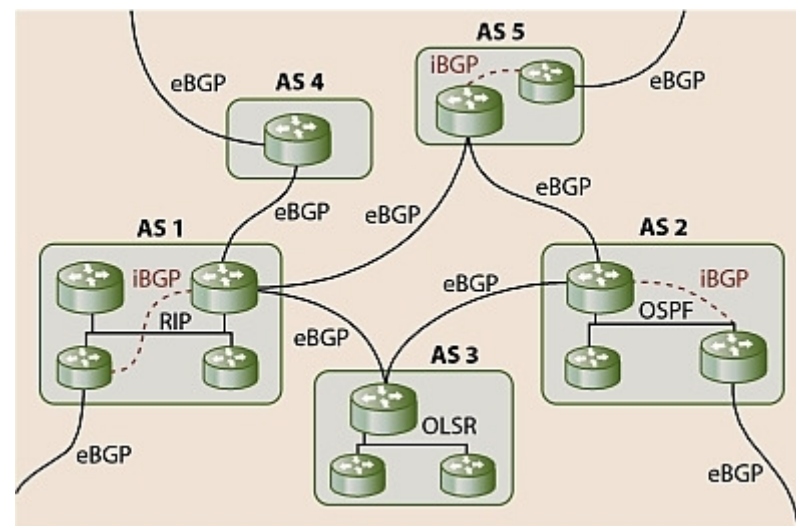


# Das Internet heute, physikalische Sicht

**Tier-x-Hierarchie**











**AS-Routing-Sicht**



Quelle: <http://www.heise.de/netze/artikel/print/115741>

## Das Internet heute, öffentliche Peering-Punkte (1)

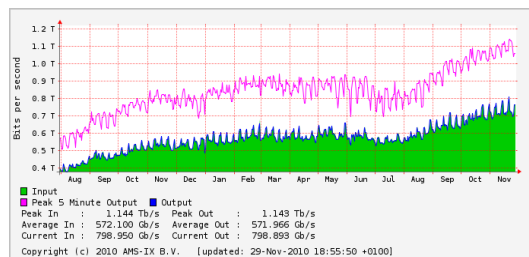
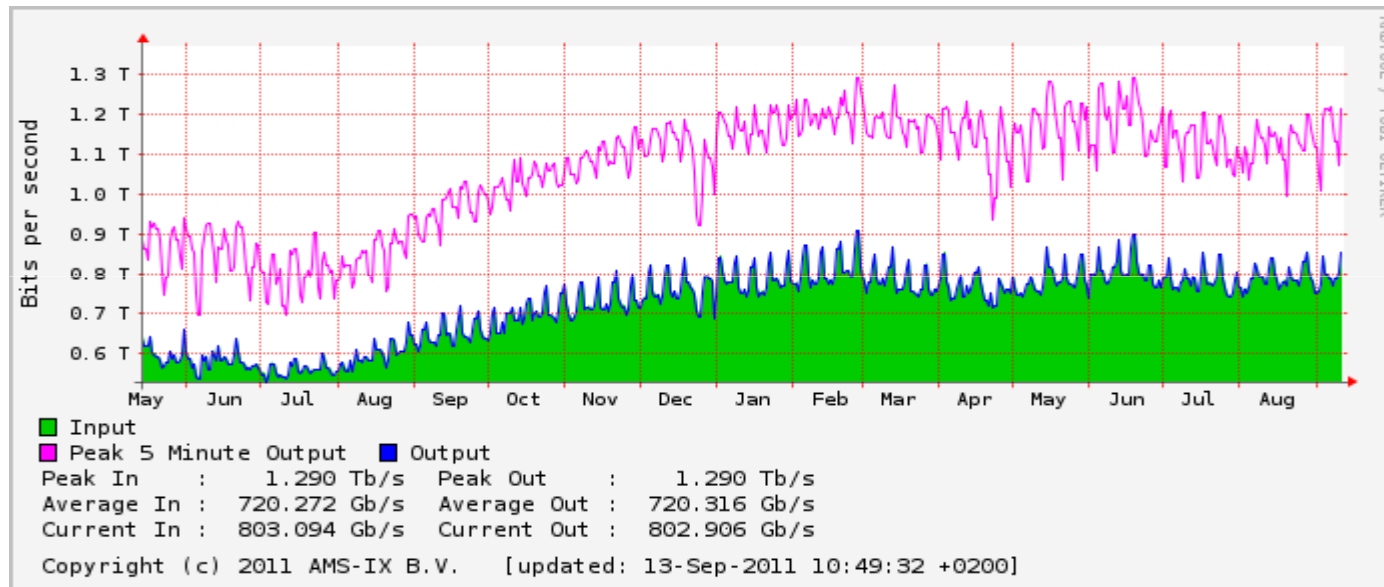
- Top-80 in Europa: <http://www.alrond.com/de> (2008)

Pos.	IX	Max Gbit/s	Avg Gbit/s	Internet Exchange Name	Country
1	AMS-IX	453,04	293,17	Amsterdam Internet Exchange	 <u>NL</u>
2	DE-CIX	432	236,4	German Internet Exchange	 <u>DE</u>
3	LINX	293,05	215,69	London Internet Exchange	 <u>GB</u>
4	EQUINIX	233,27	181,46	EQUINIX (6 US-Points)	 <u>US</u>
5	JPNAP	221,99	175,87	Japan Network Access Point	 <u>JP</u>
6	NETNOD	126,16	78	Netnod Internet Exchange i Sverige	 <u>SE</u>
7	ESPANIX	103,5	83,7	España Internet Exchange	 <u>ES</u>
8	JPIX	101,01	64,42	Japan Internet Exchange	 <u>JP</u>



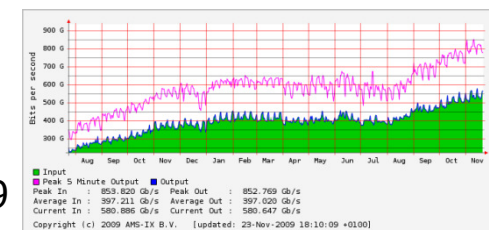
## Das Internet heute, öffentliche Peering-Punkte (2)

- AMS-IX im September 2011
- Quelle: <http://www.ams-ix.net/>



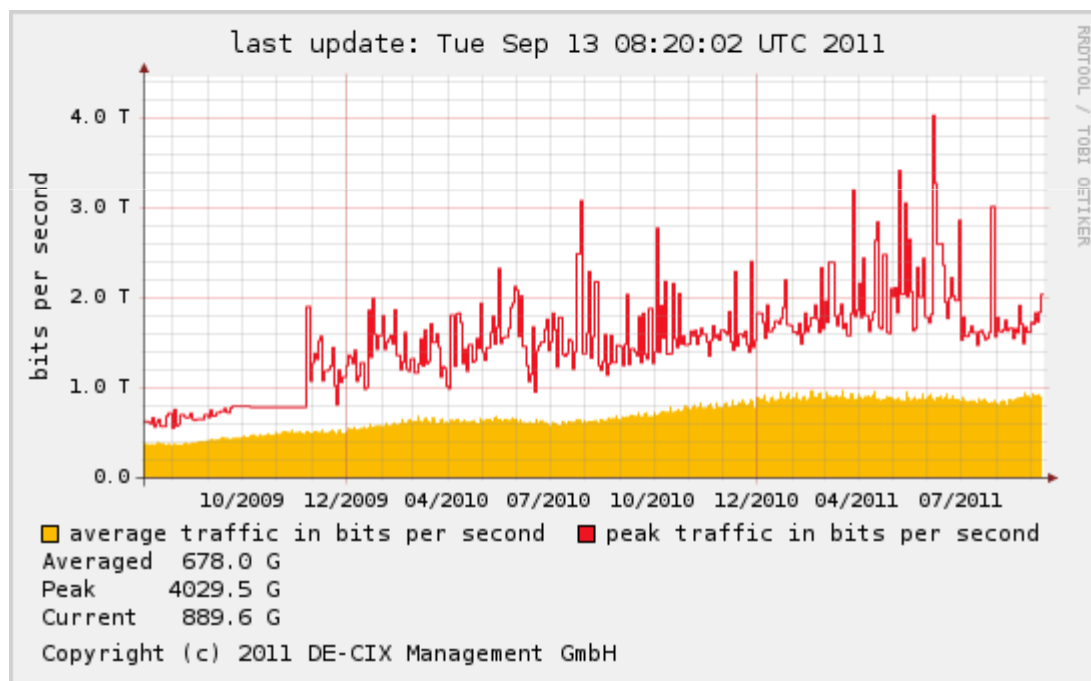
Vergleich: November 2010

Vergleich: November 2009

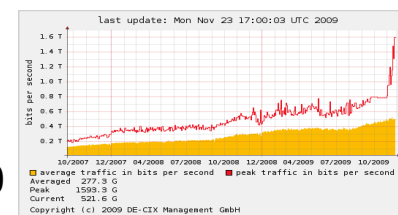


## Das Internet heute, öffentliche Peering-Punkte (3)

- DE-CIX im September 2011, mittlerweile der Größte
- Quelle: <http://www.de-cix.net/>, siehe auch: Statistiken zu Internet-Knoten in Wikipedia/Internet-Knoten

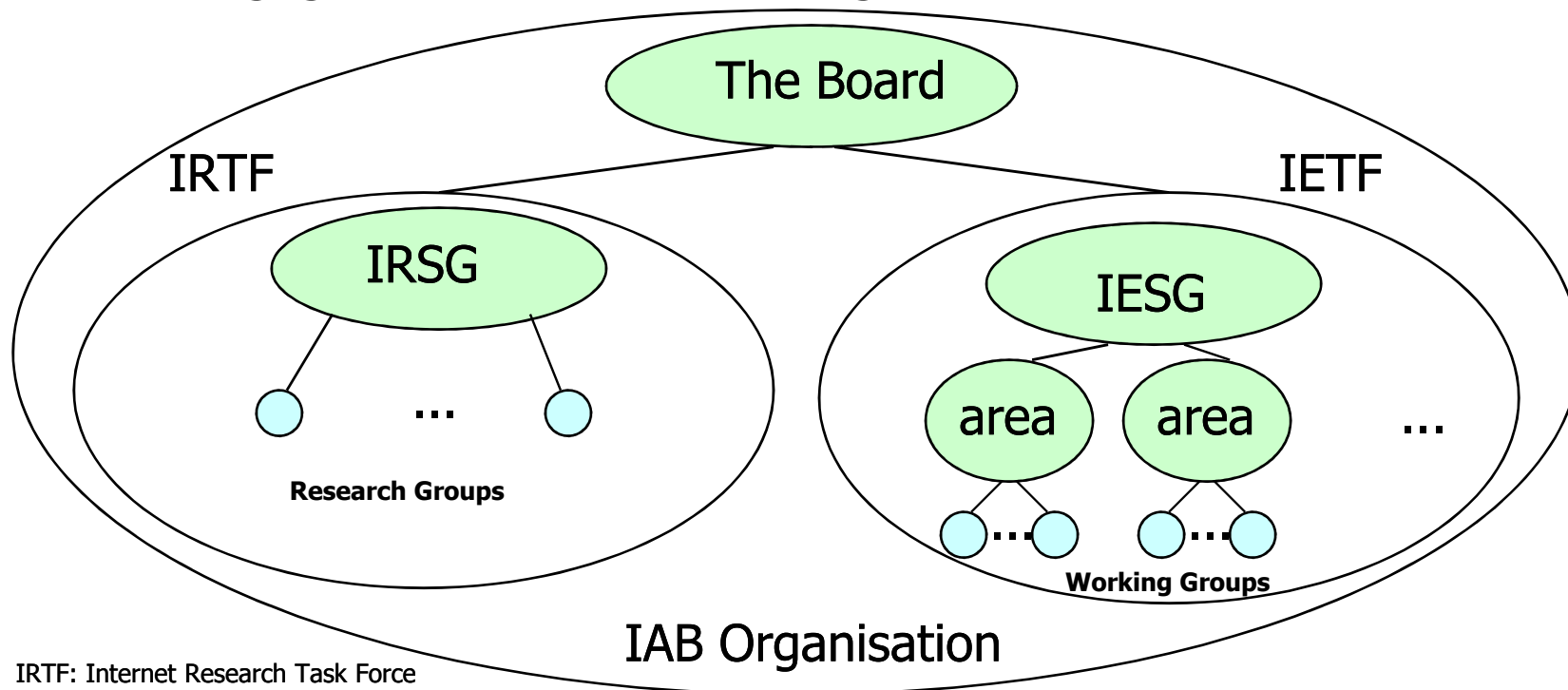


Vergleich: November 2010



## Das Internet heute: IAB

- Zuständig für die Weiterentwicklung des Internet ist das IAB (Internet Activity (heute: Architecture) Board), das bereits **1983** gegründet und **1989** umorganisiert wurde.



IRTF: Internet Research Task Force  
IETF: Internet Engineering Task Force  
IRSG: Internet Research Steering Group  
IESG: Internet Engineering Steering Group

## Das Internet heute, IAB

---

- Das **IAB** (Board) bestimmt die Richtlinien der Politik
- Die **IETF** kümmert sich in verschiedenen Bereichen (areas) um kurz- und mittelfristige Probleme
- Die **IESG** koordiniert die IETF Working Groups
- Die **IRTF** ist ein Forschungsbereich, der die TCP/IP-Forschungsthemen koordiniert
- Die **IRSG** koordiniert die Forschungsaktivitäten der einzelnen Gruppen
- Die Working Groups setzen sich aus freiwilligen Mitarbeitern zusammen

## Das Internet heute, NIC und DENIC

---

- Das NIC (Network Information Center, gesprochen NICK), ist zuständig für
  - die Dokumentation und
  - die Verwaltung der umfangreichen Information über
    - Protokolle,
    - Standards,
    - Services, usw.
- Das NIC verwaltet das Internet, z.B. auch die Domännennamen ([www.nic.net](http://www.nic.net))
- In Deutschland ist die DENIC ([www.denic.de](http://www.denic.de)) als nationale Vertretung eingerichtet (Frankfurt)

## Das Internet heute, Dokumentation, RFCs

---

- Die Dokumentation und die Standards werden als technische Reports gesammelt und heißen RFCs (Request for Comments)
- RFCs durchlaufen während ihrer Lebenszeit verschiedene Stati (Proposed Standard → Draft Standard → Internet Standard)
- Manche RFCs werden auch nie zum Internet Standard
- RFCs sind frei verfügbar (z.B. unter [www.rfc-editor.org](http://www.rfc-editor.org))

## Internet Protocol: Hauptaufgaben

---

- **Paketvermitteltes** (datagramm-orientiertes) und verbindungsloses Protokoll der Vermittlungsschicht
- IP dient der **Beförderung von Datagrammen** von einer Quelle zu einem Ziel evtl. über verschiedene Zwischenknoten (IP-Router)
- **Routing-Unterstützung** ist eine zentrale Aufgabe von IP (Routingprotokoll basiert auf diversen Protokollen)
- Datagramme werden während des Transports zerlegt und am Ziel wieder zusammengeführt, bevor sie der Schicht 4 übergeben werden = **Fragmentierung**

# Internet Protocol: Hauptaufgaben

---

- IP stellt einen **ungesicherten verbindungslosen** Dienst zur Verfügung
  - Es existiert **keine Garantie der Paketauslieferung**
  - Die Übertragung erfolgt nach dem **Best-Effort-Prinzip**
    - „Auslieferung nach bestem Bemühen“
  - Jedes Paket des Datenstroms wird **isoliert** behandelt
  - Das IP-Paket wird in einem Rahmen der zugrundeliegenden Schicht 2 transportiert, für den Längenrestriktionen bestehen:
    - bei Ethernet ist eine Länge von 1500 Bytes üblich
    - MTU = Maximum Transfer Unit



# Überblick

---

## 1. Überblick

- Internet-Vermittlungsschicht
- Autonome Systeme (AS)
- Organisation
- IPv4: Überblick und Aufgaben

## 2. IPv4-Adressierung

- IPv4: Adressierung und Adressenknappheit
- IPv4-Subnetting
- VLSM und CIDR

## 3. IPv4-PDU

- Aufbau und Felder

## 4. Fragmentierung

## Adressierung im Internet, IP-Adressen

---

- IP-Adressen sind **32 Bit** lange Adressen
  - **Tupel** aus (Netzwerknummer, Hostnummer)
- IP-Adresse von Quelle und Ziel werden **in allen** IP-Paketen mit übertragen
- Es gibt verschiedene Adressformate
  - man unterscheidet die Klassen A, B, C, D und E
- Schreibweise für IP-Adressen in gepunkteten Dezimalzahlen, jeweils ein Byte als Dezimalzahl zwischen 0 und 255
  - Beispiel:

Hexformat: 0xC0290614

Dezimalzahl: 192.41.6.20

# Adressierung im Internet, IP-Adressformate

---

	4 Byte, 32 Bit				
Klasse A	0	Netz	Host		1.0.0.0 bis 127.255.255.255
Klasse B	10	Netz	Host		128.0.0.0 bis 191.255.255.255
Klasse C	110	Netz	Host		192.0.0.0 bis 223.255.255.255
Klasse D	1110	Multicast-Adresse			224.0.0.0 bis 239.255.255.255
Klasse E	11110	Reservierte Adresse			240.0.0.0 bis 247.255.255.255

Alle Adressen der Form 127.xx.yy.zz sind Loopback-Adressen!

## Adressierung im Internet, IP-Adressen

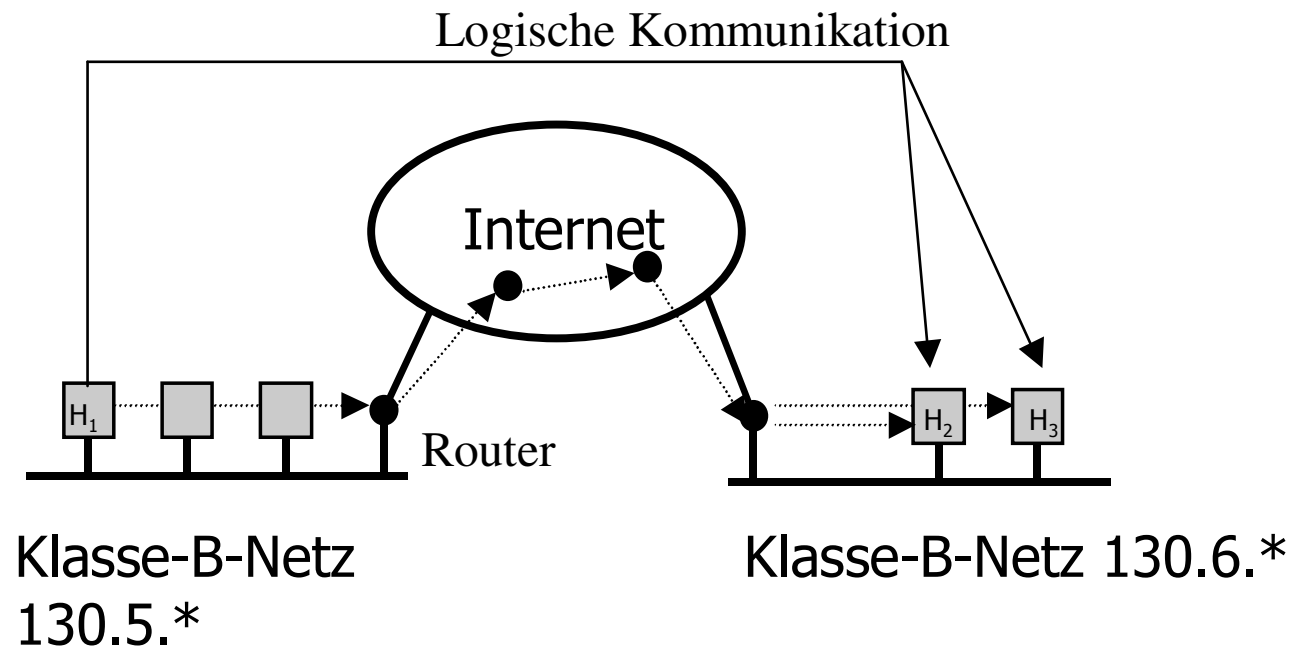
---

- Die niedrigste IP-Adresse ist **0.0.0.0**
- Die höchste IP-Adresse ist **255.255.255.255**
- Die Adresse **0.0.0.0** hat die besondere Bedeutung „ein bestimmtes Netz“ oder „ein bestimmter Host“
- Die Adresse **255.255.255.255** (–1) wird als Broadcast-Adresse verwendet
  - Limited Broadcast → im lokalen Netz
- Weiterer Broadcast-Typ:
  - Directed Broadcast → Broadcast an anderes Netzwerk

# Direkter Broadcast

---

Ziel-IP-Adresse:  
**130.6.255.255**



.....> Physikalische Verteilung des Broadcast

## Adressierung im Internet

---

- Netznummern werden vom NIC bzw. in Deutschland von der DENIC zugewiesen!
- **Adressenknappheit** wird erwartet:
  - Neue Version **IPv6** soll hier Abhilfe schaffen

Klasse	Anzahl Netze	Max. Anzahl Hosts je Netz	Anteil am IP-Adressraum	Adressen insgesamt
A (/8)	126 ( $2^7$ )	16.777.214 ( $2^{24} - 2$ )	50 %	2.147.483.638 ( $2^{31}$ )
B (/16)	16.384 ( $2^{14}$ )	65.534 ( $2^{16} - 2$ )	25 %	1.073.741.824 ( $2^{30}$ )
C (/24)	2.097.152 ( $2^{21}$ )	254 ( $2^8 - 2$ )	12,5 %	536.870.912 ( $2^{29}$ )

## Adressierung im Internet, Subnetting

---

- Die Hostadresse kann zu besseren organisatorischen Gliederung noch mal zur **Subnetz**-Bildung in zwei Teile zerlegt werden:

- Teilnetznummer
- Hostnummer

Beispiel mit  
Klasse B

10	Netz	Subnetz	Host
----	------	---------	------

- Außerhalb des Teilnetzes ist die Aufgliederung nicht sichtbar
- IP-Router in einem Teilnetz berücksichtigen die Subnetzadresse
- **Netzwerkmaske** wird als Bitmaske verwendet, um die Bits der Subnetzwerknummer zu identifizieren

## Adressierung im Internet, Subnetting

---

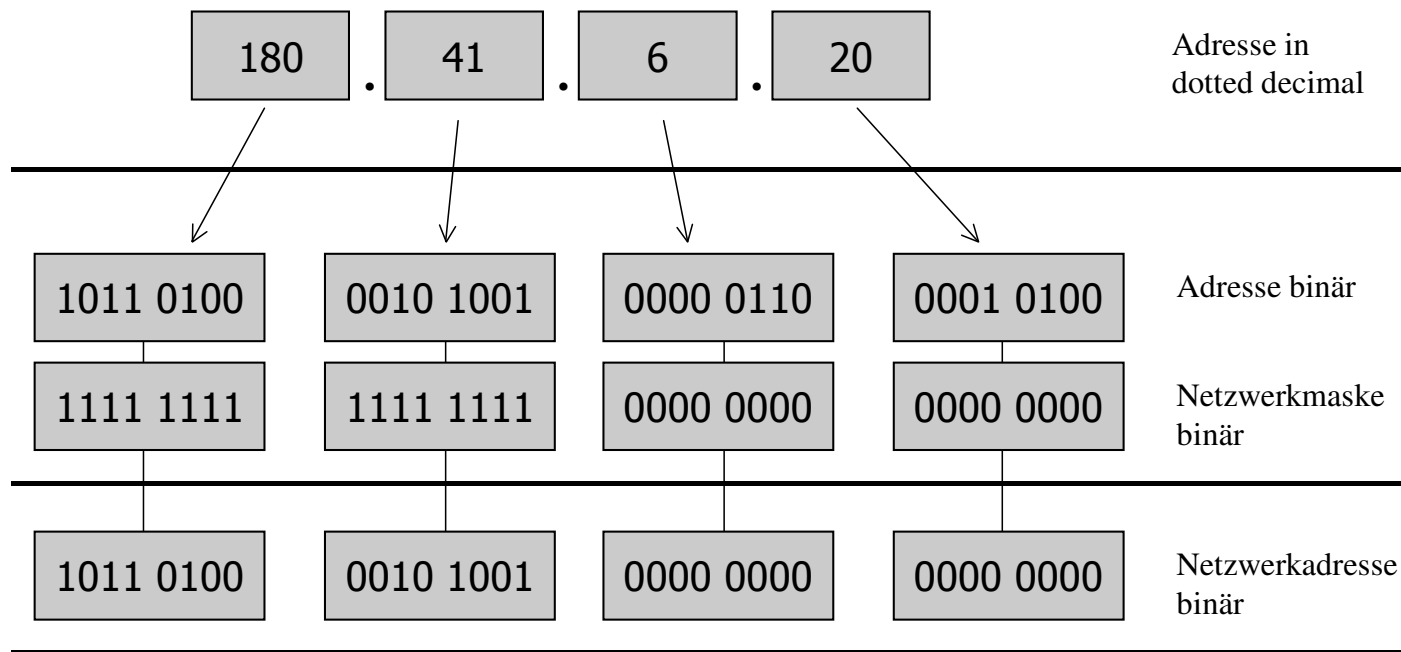
- Der lokale Administrator besitzt alle Freiheiten zur Bildung von Subnetzen, ohne die Komplexität auf den Internet-Router zu übertragen
- Bei einer Klasse B-Adresse wäre folgende Struktur denkbar:
  - 3. Byte gibt die Organisationseinheit im Unternehmen an (Subnetz-Adresse)
  - 4. Byte erlaubt die Nummerierung der Geräte: (Stationsadresse)
    - Netzkomponenten (Switch, Hub, etc.): 1 - 9
    - Arbeitsplätze: 10 - 249
    - Server: 250 - 254



## Adressierung, Beispiel

---

- Hier handelt es sich um eine Klasse B-Adresse, warum?



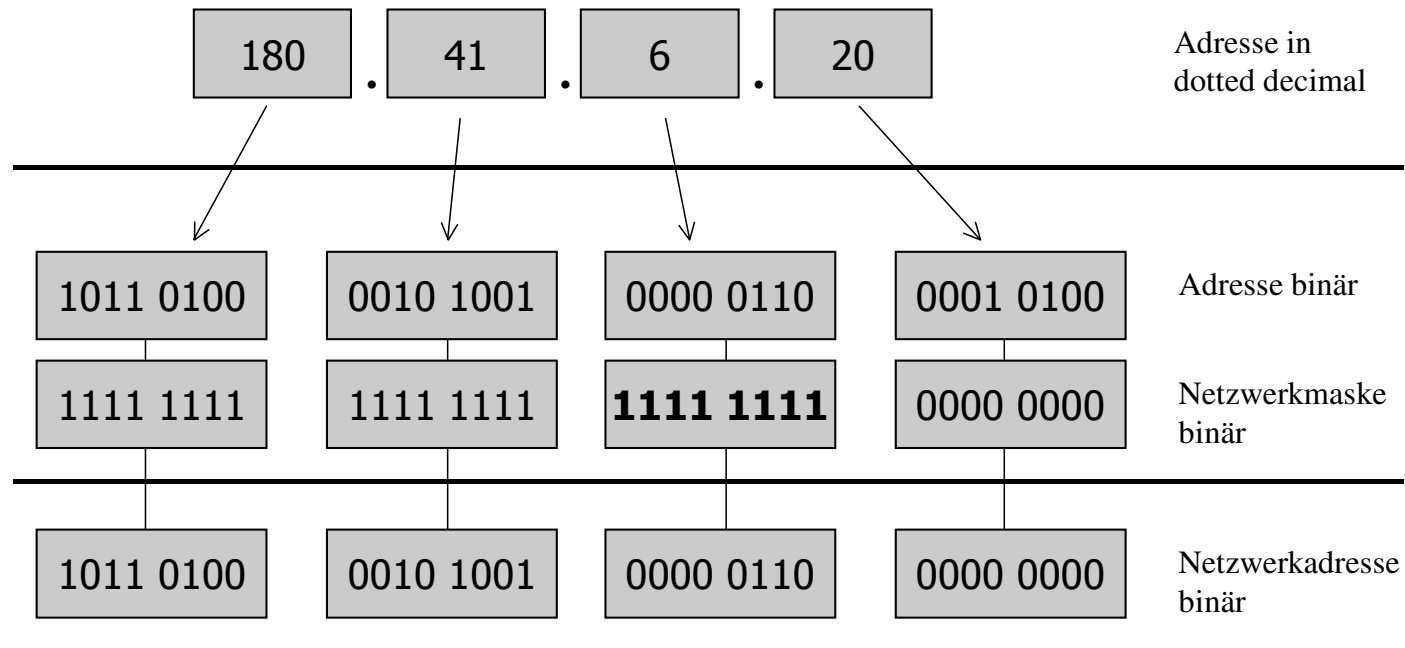
Logische Und-Verknüpfung der IP-Adresse mit der Netzmaske

Die Netzwerkadresse ist demnach: 180.41.0.0

Netzwerkmaske in dotted decimal: 255.255.0.0

# Adressierung, Beispiel mit Subnetzadressierung

---



Subnetz mit zwei Byte für Netzwerknummer und ein Byte für Subnetzwerknummer  
Die Netzmaske ist hier: 255.255.255.0

## CIDR und VLSM

---

- Problem:
  - Vergeudung von vielen IP-Adressen durch die Aufteilung des Adressraums in Klassen (siehe Klasse-B-Adressen)
  - Aber die Routing-Tabellen der Router sind schon sehr groß und sollten nicht weiter wachsen
- VLSM und CIDR helfen, die Adressproblematik etwas abzumildern
- **VLSM** = Variable Length Subnet Mask
- **CIDR** = Classless InterDomain Routing
- CIDR ist VLSM im öffentlichen Internet!

## CIDR und VLSM

---

- Konzept von VLSM/CIDR:
  - Restliche Klasse-C-Netze (ca. 2 Millionen) werden in Blöcken variabler Länge vergeben → Vergabe durch ISP
  - Beispiel: Braucht ein Standort 2000 Adressen erhält er acht aufeinanderfolgende Klasse-C-Netze zugewiesen, kann also auf eine B-Adresse verzichten
- Weitere Verbesserung für das Routing durch Zuordnung der Klasse-C-Adressenbereiche zu Zonen, z.B.
  - Europa: 194.0.0.0 bis 195.255.255.255
  - Nordamerika: 198.0.0.0 bis 199.255.255.255
  - Europäischer Router erkennt anhand der Zieladresse, ob ein Paket in Europa bleibt oder z.B. zu einem amerikanischen Router weitergeleitet werden soll

## CIDR und VLSM: Netzwerkpräfix-Notation

---

- Netzwerkpräfix-Notation (NP-Notation) ermöglicht die Angabe der Netz-Id-Bits in der IP-Adresse
- Notationsbeispiel: 194.24.19.25/20
  - IP-Adresse binär:
    - **110**00010.00011000.00010011.00011001 -> Klasse C
  - Die Präfixlänge (hier 20) gibt die Anzahl der fortlaufenden Einsen in der Netzwerkmaske an:
  - Netzwerkmaske der IP-Adresse:
    - **11111111. 11111111.1111**0000. 00000000 = 255.255.240.000
  - Klasse A = /8
  - Klasse B = /16
  - Klasse C = /24

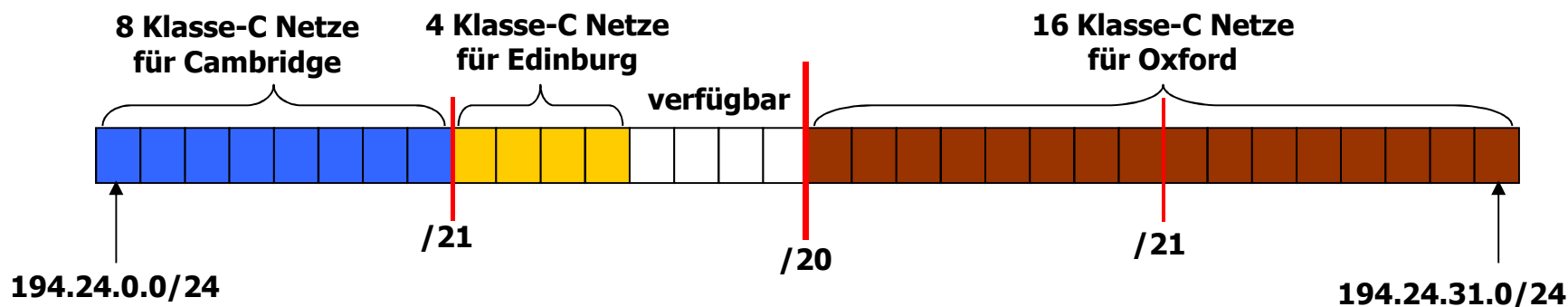
## CIDR und VLSM: Beispiel (vgl. Tanenbaum)

---

- Cambridge University benötigt 2000 (fast  $2^{11}$ ) öffentliche IP-Adressen
  - Klasse-C-Netz mit max. 256 ( $2^8$ ) Adressen reicht nicht aus
  - Alternative ist ein Klasse-B Netz mit 65536 ( $2^{16}$ ) Adressen
    - > 63488 öffentliche IP-Adressen werden nicht benötigt und somit verschwendet! (über 95% der bereitgestellten Adressen!!!)
  - Besser: Nutzung mehrerer zusammenhängender Klasse-C Netze
    - Für den Hostanteil der Adresse werden zusätzlich 3 Bit benötigt ( $2^{11}$  Adressen)
    - Cambridge University wird folgender Adressbereich zugewiesen:  
194.24.0.0/21 -> 194.24.0.0 bis 194.24.7.255 (Netzwerkmaske 255.255.248.0)  
oder  
**11000010.00011000.00000000.00000000** bis  
**11000010.00011000.00000111.11111111** mit  
**11111111.11111111.11111000.00000000** als Netzwerkmaske

## CIDR und VLSM: Beispiel (vgl. Tanenbaum)

- Nach dem gleichen Verfahren werden auch den Universitäten Oxford und Edinburgh mehrere Klasse-C Netze zugewiesen
  - Oxford benötigt 4000 (fast  $2^{12}$ ) öffentliche IP-Adressen
  - Edinburgh benötigt 1000 (fast  $2^{10}$ ) öffentliche IP-Adressen
- Folgende Adressbereiche werden zugewiesen:
  - Cambridge: 194.24.0.0/21      194.24.0.0      bis      194.24.7.255
  - Edinburgh: 194.24.8.0/22      194.24.8.0      bis      194.24.11.255
  - Verfügbar: 194.24.12.0/22      194.24.12.0      bis      194.24.12.255
  - Oxford: 194.24.16.0/20      194.24.16.0      bis      194.24.31.255



## CIDR und VLSM: Beispiel (vgl. Tanenbaum)

---

- Ein Standard IP-Router kann die mittels VLSM zusammengefassten Klasse-C-Netze nicht erkennen
- Das Routing muss um CIDR erweitert werden

### **Routingtabelle ohne CIDR**

194.24.0.0	-> Cambridge
194.24.1.0	-> Cambridge
...	
194.24.7.255	-> Cambridge
194.24.8.0	-> Edinburgh
...	
194.24.11.255	-> Edinburgh
194.24.16.0	-> Oxford
...	
194.24.31.255	-> Oxford

### **Routingtabelle mit CIDR**

194.24.0.0/21	-> Cambridge
194.24.8.0/22	-> Edinburgh
194.24.16.0/20	-> Oxford

**Nur 3 statt 28 Einträge!!!**



## CIDR und VLSM:

### Beispiel LRZ - Hochschule München - Fakultät 07 (1)

---

- Das Leibnitz-Rechenzentrum (LRZ) organisiert den privaten IP-Adressbereich 10.0.0.0/8 und ordnet der Hochschule München den Adressbereich 10.28.0.0/16 zu

10.20.0.0	-> Lothstraße 34
10.21.0.0	-> Lothstraße 21
10.22.0.0	-> Karlstraße 6
10.23.0.0	-> Infanteriestraße 13/14
...	
10.26.0.0	-> Pasing
...	
10.28.0.0	-> Hesstraße (Informatik)
...	

- Kein Zugriff von außen möglich, nur über VPN

## CIDR und VLSM:

### Beispiel LRZ - Hochschule München - Fakultät 07 (2)

---

- Die Fakultät untergliedert den Adressbereich derzeit weiter in vier /18-Subnetze
- Beispiel: Netz 0
  - 10.28.0.0/18 mit 18 Bit Netzwerkanteil und  $2^{14} - 2$  Hostadressen
  - Binär: 0000 1010 0001 1100 **00**xx xxxx xxxx xxxx
- Beispiel: Netz 1
  - 10.28.64.0/18 mit 18 Bit Netzwerkanteil und  $2^{14} - 2$  Hostadressen
  - Binär: 0000 1010 0001 1100 **01**xx xxxx xxxx xxxx
- Alle Netze
  - 10.28.0.0/18 -> Netz 0: Wird im Münchner Hochschulnetz geroutet
  - 10.28.64.0/18 -> Netz 1: Wird innerhalb der Hochschule München geroutet
  - 10.28.128/18 -> Netz 2: wie Netz 1, aber DHCP-Adressvergabe
  - 10.28.192.0/18 -> Netz 3: kein Routing

## CIDR und VLSM, Übung

---

- Welche IP-Adressen repräsentiert die CIDR-Adresse 180.41.214.192/28 (Netzwerkpräfix-Notation)?
  
- Lösung:
  - Insgesamt 4 Bit für Hosts
  - Adressbereich von 180.41.214.192 bis 180.41.214.207
  - Also von 1011 0100 . 0010 1001 . 1101 0110 . 1100 **0000**  
bis 1011 0100 . 0010 1001 . 1101 0110 . 1100 **1111**
  - Das sind 16 IP-Adressen, 14 davon sind nutzbar

## CIDR und VLSM, Übung

---

- Ein Unternehmen besitzt die Klasse-C-Adresse 193.1.1.0 und hat 8 Abteilungen
- Jede Abteilung hat 25 Rechner
- Jede Abteilung soll einen eigenen Adressbereich erhalten
- Teilen Sie das Klasse-C-Netzwerk in 8 Subnetze auf und verwenden Sie dabei CIDR-Adressen!
  - Hinweis: Für 8 Subnetze braucht man 3 Bit

## CIDR und VLSM, Übung

---

Ergänzen Sie die CIDR-Formate (Werte x1 – x8 und y1 – y8)!

Netz	Adresse in Bitdarstellung	CIDR-Format	Rechner
Basisnetz	11000001.00000001.00000001.00000000	193.1.1.0/24	254
Subnetz 0	11000001.00000001.00000001. <b>0000</b> 0000	193.1.1.x1/y1	30
Subnetz 1	11000001.00000001.00000001. <b>0010</b> 0000	193.1.1.x2/y2	30
Subnetz 2	11000001.00000001.00000001. <b>0100</b> 0000	193.1.1.x3/y3	30
Subnetz 3	11000001.00000001.00000001. <b>0110</b> 0000	193.1.1.x4/y4	30
Subnetz 4	11000001.00000001.00000001. <b>1000</b> 0000	193.1.1.x5/y5	30
Subnetz 5	11000001.00000001.00000001. <b>1010</b> 0000	193.1.1.x6/y6	30
Subnetz 6	11000001.00000001.00000001. <b>1100</b> 0000	193.1.1.x7/y7	30
Subnetz 7	11000001.00000001.00000001. <b>1110</b> 0000	193.1.1.x8/y8	30

## CIDR und VLSM, Übung

---

Ergänzen Sie die CIDR-Formate (Werte x1 – x8 und y1 – y8)!

Netz	Adresse in Bitdarstellung	CIDR-Format	Rechner
Basisnetz	11000001.00000001.00000001.00000000	193.1.1.0/24	254
Subnetz 0	11000001.00000001.00000001. <b>0000</b> 0000	193.1.1.0/27	30
Subnetz 1	11000001.00000001.00000001. <b>0010</b> 0000	193.1.1.32/27	30
Subnetz 2	11000001.00000001.00000001. <b>0100</b> 0000	193.1.1.64/27	30
Subnetz 3	11000001.00000001.00000001. <b>0110</b> 0000	193.1.1.96/27	30
Subnetz 4	11000001.00000001.00000001. <b>1000</b> 0000	193.1.1.128/27	30
Subnetz 5	11000001.00000001.00000001. <b>1010</b> 0000	193.1.1.160/27	30
Subnetz 6	11000001.00000001.00000001. <b>1100</b> 0000	193.1.1.192/27	30
Subnetz 7	11000001.00000001.00000001. <b>1110</b> 0000	193.1.1.224/27	30

# Überblick

---

## 1. Überblick

- Internet-Vermittlungsschicht
- Autonome Systeme (AS)
- Organisation
- IPv4: Überblick und Aufgaben

## 2. IPv4-Adressierung

- IPv4: Adressierung und Adressenknappheit
- IPv4-Subnetting
- VLSM und CIDR

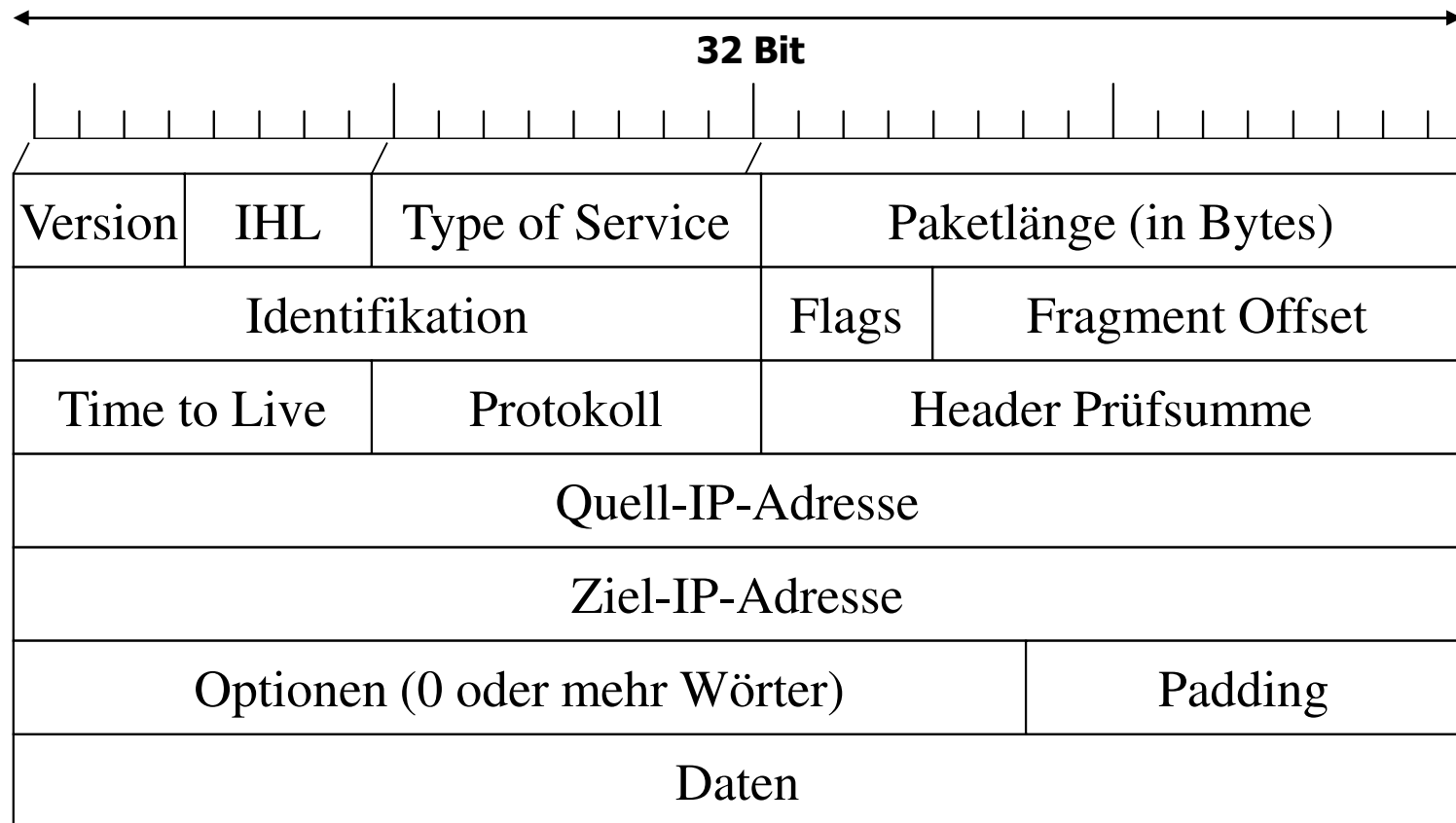
## 3. **IPv4-PDU**

- Aufbau und Felder

## 4. Fragmentierung

# Protokollheader

---



Headerlänge: 20 – 60 Byte



# Protokollheader

---

Version	IHL	Type of Service	Paketlänge (in Bytes)
---------	-----	-----------------	-----------------------

- **Version:** Spezifiziert die genutzte IP-Version; z.Zt. Wechsel von IPv4 auf IP Next Generation (IPv6)
- **IHL:** Gibt die Länge des Paket-Headers an, gemessen in 32-Bit-Worten; ist aufgrund der variablen Länge des Optionsfeldes nötig (mind. 5 → keine Option, max. 15 Worte → 60 Byte)
- **Type of Service:** Dieses 8-Bit-Feld ist wiederum aufgeteilt in:
  - Priorität (3 Bit): 000=Standard, 001=Priorität, ..., 101=kritisch, ...
  - ToS-Spezifikation (3 Bit): Flags zur Angabe von Servicetypen (hoher Durchsatz, niedrige Verzögerung, ...)
  - 2 unbenutzte Bit, **IPv4 nutzt *Type of Service* nicht**
- **Paketlänge:** Gesamtlänge des Datenpaketes inkl. Header; gemessen in 8-Bit-Worten
  - max. 65.535 Byte

## Protokollheader

---

Identifikation	Flags	Fragment Offset
----------------	-------	-----------------

- **Identifikation:** Alle Fragmente eines Datagramms erhalten hier den gleichen Wert
- **Flags:** (3 Bit) Dient der Kontrolle der Fragmentierung
  - Geben an, ob das Feld geteilt werden muss und weitere Pakete folgen oder ob das aktuelle Paket das letzte ist
  - Drei Flags, erstes unbenutzt: 0|DF|MF
  - DF=1 → Fragmentierung ist nicht erlaubt
  - More Fragments=0 → letztes Fragment; MF=1 weitere folgen
- **Fragment Offset:** Dient der korrekten Herstellung der Ursprungssequenz, da Pakete das Ziel in unterschiedlicher Reihenfolge erreichen können, gemessen in 8-Byte-Worten
  - Dient der Ermittlung der relativen Lage des Fragments im Datagram
  - 13 Bit

# Protokollheader

---

Time to Live	Protokoll	Header Prüfsumme
--------------	-----------	------------------

- **Time to live (TTL):** Gibt an, wie lange ein Datagramm im Internet verbleiben darf
  - Es dient dazu, zu alte Pakete vom Netz zu nehmen, bei 0 wird Paket verworfen und eine ICMP-Nachricht zum Quellhost gesendet
  - War gedacht als Zeit in Sekunden (max. 255 s)
  - Wird aber als Hop-Count genutzt, jeder Router subtrahiert 1
- **Protokoll:** Definiert das darüberliegende Protokoll, an das IP die Daten des Pakets weiterreicht (6=TCP, 89=OSPF,...)
- **Header-Prüfsumme:** Header-Absicherung
  - 16-Bit-Wörter aufsummieren und Einerkomplement bilden
  - Prüft also **nur** den Header, Daten in höheren Protokollen prüfen!
  - Wird für jede Teilstrecke neu berechnet werden, warum?

## Protokollheader

---

Quell-IP-Adresse
Ziel-IP-Adresse

- **Quell-IP-Adresse und Ziel-IP-Adresse:**
  - Jeweils 32 Bits
  - Identifikation der einzelnen Endsysteme (Hosts)
  - Hier stehen die IP-Adressen von Sender- und Empfängerhost

# Protokollheader

---

Optionen	Padding
Daten	

- **Optionen:** Zusätzliche, optionale Angaben:
  - *Loose Source Routing* → Möglichkeit, den Weg eines Paketes durch das Internet partiell vorgeben; RFC 791
  - *Strict Source Routing* → die Pakete müssen die Pfadvorgabe einhalten (max. 9 Knoten in der Route), RFC 791
  - *Record Routing* → Jeder durchlaufene Router trägt seine Adresse ein, ...
  - Wird selten verwendet!!
- **Padding:** Wenn eine Option genutzt wird, ist das Datagramm bis zur nächsten 32-Bit-Grenze mit Nullen aufzufüllen
- **Daten:** Die Nutzdaten der höheren Schicht

# Überblick

---

## 1. Überblick

- Internet-Vermittlungsschicht
- Autonome Systeme (AS)
- Organisation
- IPv4: Überblick und Aufgaben

## 2. IPv4-Adressierung

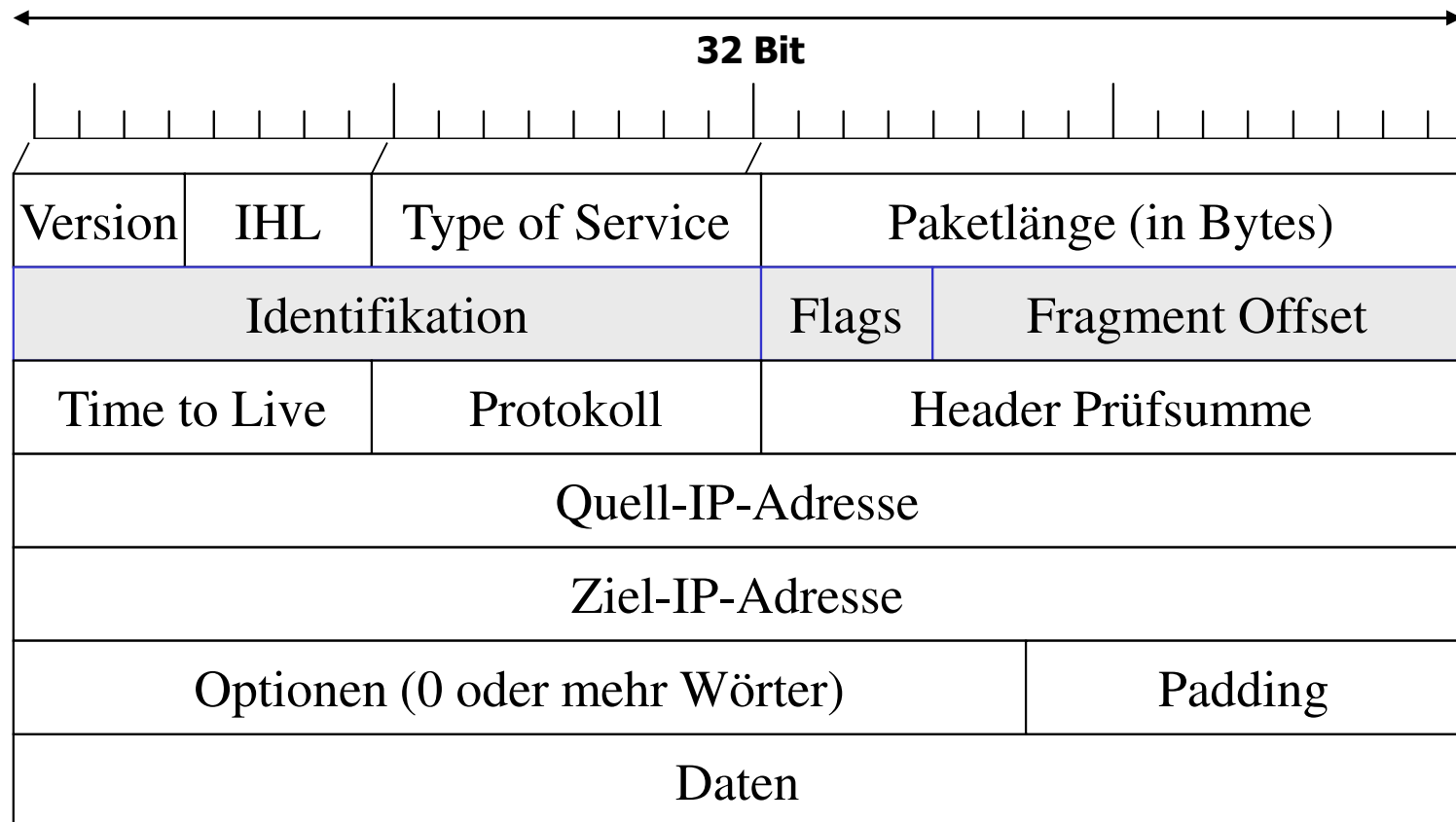
- IPv4: Adressierung und Adressenknappheit
- IPv4-Subnetting
- VLSM und CIDR

## 3. IPv4-PDU

- Aufbau und Felder

## 4. Fragmentierung

# Protokollheader



## Fragmentierung, Ablauf

---

- Wenn ein IP-Paket von einem Netzknoten zum anderen weitergeleitet wird, muss es
  - evtl. verschiedene physikalische Netze durchqueren
  - in unterschiedlich zulässige Paketgrößen aufgeteilt werden
- Daher besteht die Notwendigkeit, IP-Datagramme zu zerlegen und am Ziel wieder zusammenzusetzen
  - Fragmentierung und Defragmentierung
  - Alle Router müssen Fragmente der Größe **576 Byte** oder kleiner akzeptieren
- Sobald eine Fragmentierung einsetzt, laufen in einem Knoten mehrere Schritte ab



## Fragmentierung, Ablauf

---

- Das **DF**-Flag wird überprüft, um festzustellen, ob eine Fragmentierung erlaubt ist. Ist das Bit auf „1“ gesetzt und es wäre eine Fragmentierung notwendig, wird das Paket verworfen
- Ansonsten wird entspr. der zulässigen Paketgröße das Datenfeld des Ur-Paketes in mehrere Teil zerlegt
- Alle neu entstandenen Pakete weisen - mit Ausnahme des letzten Paket - eine Länge mit einem **Vielfachen von 8 Byte** auf
- Alle Datenteile werden in neu erzeugte IP-Pakete eingebettet. Die Header dieser Pakete sind Kopien des Ursprungskopfes mit einigen Modifikationen

## Fragmentierung, Ablauf

---

- Header-Modifikation bei der Fragmentierung:
  - Das **MF**-Flag wird in allen Fragmenten mit Ausnahme des letzten auf „1“ gesetzt
  - Das **Fragment-Offset**-Feld enthält Angaben darüber, wo das Datenfeld in Relation zum Beginn des nicht fragmentierten Ur-Paketes platziert ist
  - Enthält das Ur-Paket Optionen, wird abhängig vom Type-Byte entschieden, ob die Option in jedes Paketfragment aufgenommen wird (z.B. Protokollierung der Route)
  - Die **Headerlänge** (IHL) und die Paketlänge sind jeweils **neu** zu bestimmen
  - Die **Headerprüfsumme** wird neu berechnet

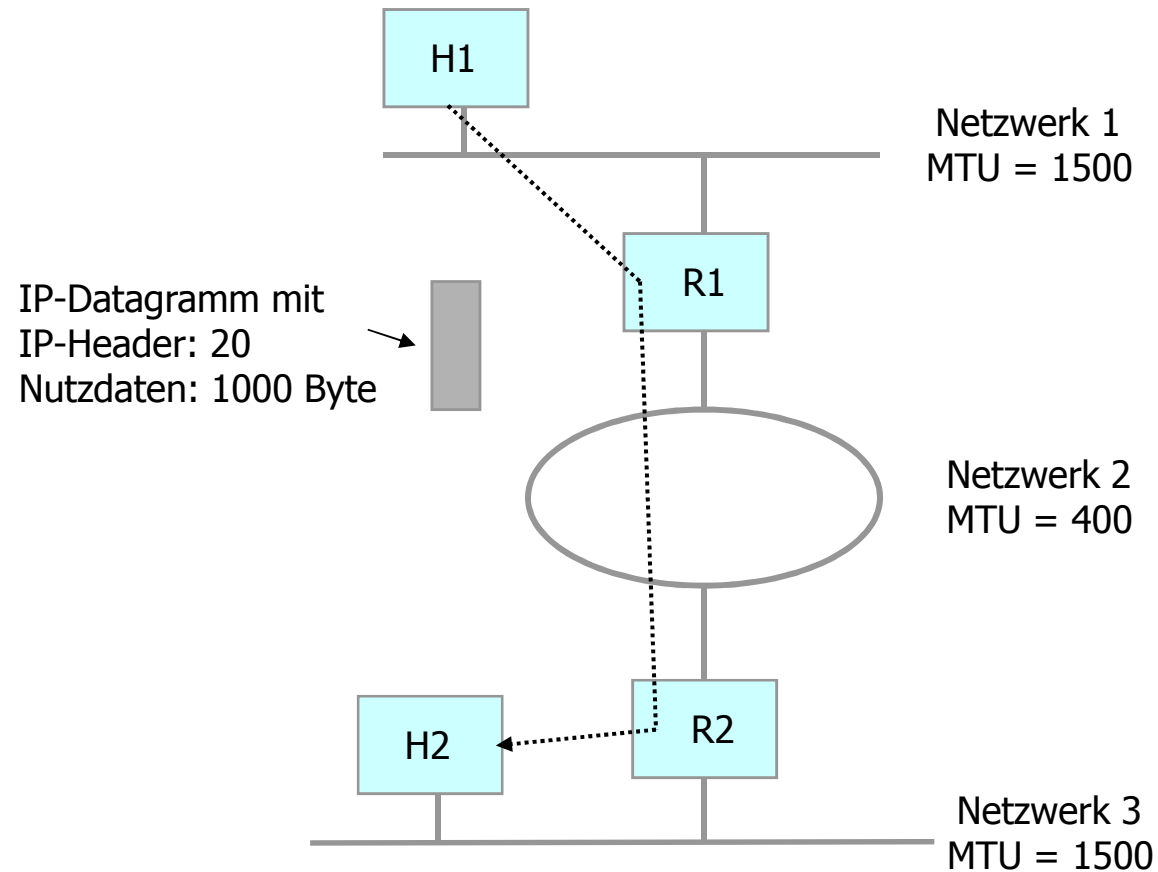
## Fragmentierung, Ablauf

---

- Ablauf der Defragmentierung:
  - Die Zielstation setzt die Fragmente eines Datagramms wieder zusammen
  - Die **Zusammengehörigkeit** entnimmt sie dem **Identifikationsfeld**
  - Die ankommenden Fragmente werden zunächst gepuffert
  - Bei Eintreffen des ersten Fragments wird ein **Timer** gestartet
  - Ist der **Timer** abgelaufen bevor alle Fragmente eingetroffen sind, wird alles **verworfen**
  - Im anderen Fall wird das Datagramm am N-SAP **zur Transportschicht hochgereicht**

# Fragmentierung, Übung

---



MTU = Maximum Transfer Unit

## Fragmentierung, Übung

---

### Fragment 1

Rest des Headers		
Identifikation=120	Flags:MF = __	FO = _____
Datenbyte 0 ... _____		

### Fragment 2

Rest des Headers		
Identifikation=_____	Flags:MF = __	FO = _____
Datenbyte ____ ... _____		

### Fragment 3

Rest des Headers		
Identifikation=_____	Flags:MF = __	FO = _____
Datenbyte ____ ... _____		

# Fragmentierung, Übung

---

## Fragment 1

Rest des Headers		
Identifikation=120	Flags: <b>MF = 1</b>	<b>FO = 0</b>
<b>Datenbyte 0 ... 375</b>		

## Fragmentierung, Übung

---

### Fragment 1

Rest des Headers		
Identifikation=120	Flags: <b>MF = 1</b>	<b>FO = 0</b>
<b>Datenbyte 0 ... 375</b>		

### Fragment 2

$$376 / 8 = 47$$

Rest des Headers		
<b>Identifikation=120</b>	Flags: <b>MF = 1</b>	<b>FO = 47</b>
<b>Datenbyte 376 ... 751</b>		

# Fragmentierung, Übung

---

## Fragment 1

Rest des Headers		
Identifikation=120	Flags:MF = 1	FO = 0
Datenbyte 0 ... 375		

## Fragment 2

$$376 / 8 = 47$$

Rest des Headers		
Identifikation=120	Flags:MF = 1	FO = 47
Datenbyte 376 ... 751		

## Fragment 3

$$752 / 8 = 94$$

Rest des Headers		
Identifikation=120	Flags:MF = 0	FO = 94
Datenbyte 752 ... 999		



# Rückblick

---

## 1. Überblick

- Internet-Vermittlungsschicht
- Autonome Systeme (AS)
- Organisation
- IPv4: Überblick und Aufgaben

## 2. IPv4-Adressierung

- IPv4: Adressierung und Adressenknappheit
- IPv4-Subnetting
- VLSM und CIDR

## 3. IPv4-PDU

- Aufbau und Felder

## 4. Fragmentierung