

**Einführung:
Grundlegende Design-Prinzipien des
Internet**

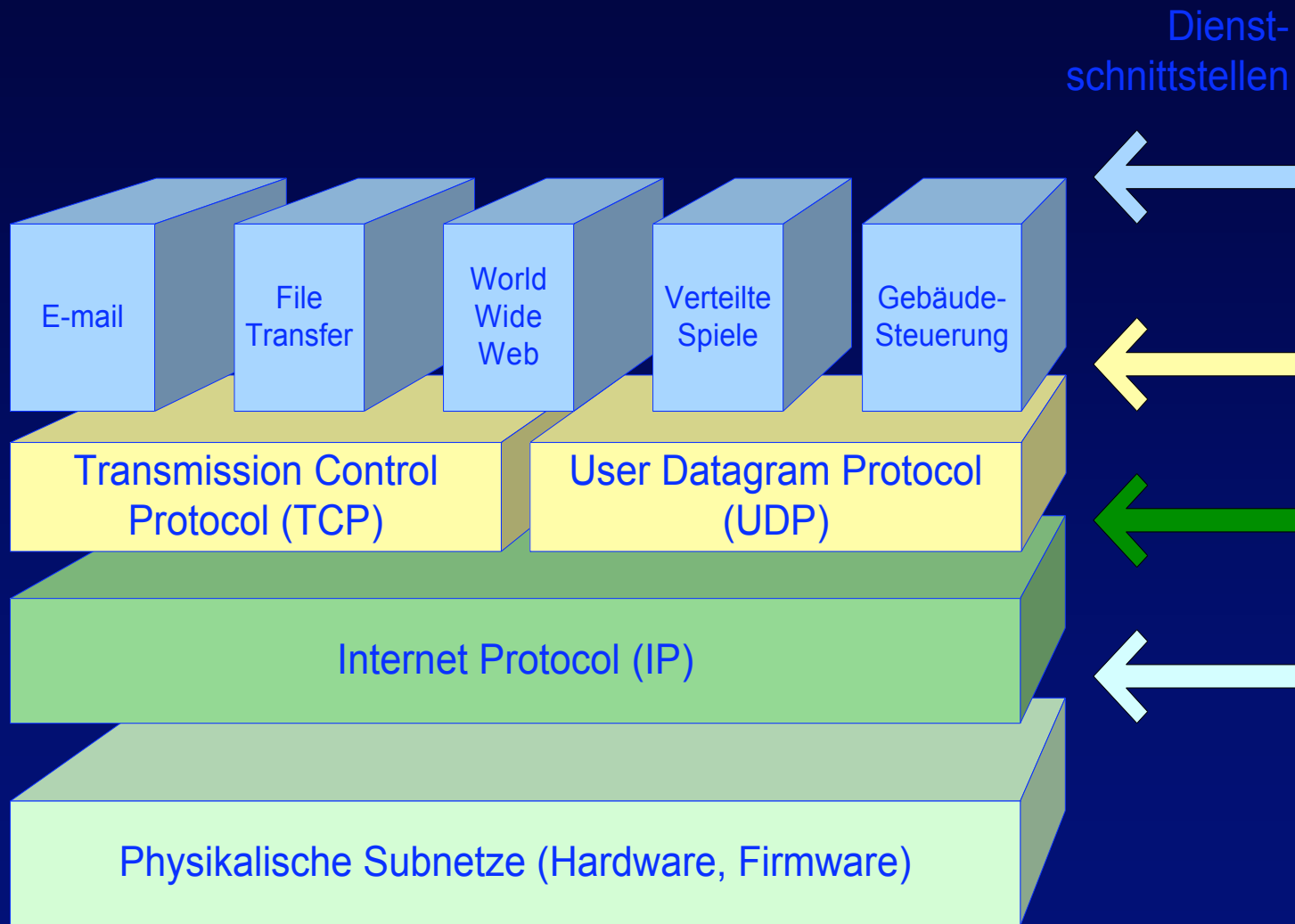
Alles was Sie schon immer über das Internet hätten wissen sollen

- Grundlegende Design-Prinzipien
- Adressierung
- Internet-Protokoll (IP)
- Internet Control Message Protocol (ICMP)
- Dynamic Host Configuration Protocol (DHCP)
- Transport-Protokoll (TCP)
- Routing
- Network Address Translation (NAT)
- Domain Name System (DNS)

Ursprüngliche Entwurfsentscheidungen

- Paketvermittlung
 - damals eine neue Technik, im ARPANET erforscht
- Hohe Verfügbarkeit des Netzes
 - Datagrammtechnik (vs. virtual circuit)
 - wenig Zustandsinformation im Netz
 - verteilte Verwaltung
- Soll viele verschiedene Dienste unterstützen können
 - Internet Protocol (IP) als Netzwerkprotokoll
 - Transmission Control Protocol (TCP), User Datagram Protocol (UDP) als Transportprotokolle (-> Bezeichnung TCP/IP)
 - Anwendungen direkt auf Transportprotokolle aufgesetzt
- Netzverbund mit heterogenen Teilnetzen
- „Offenes System“
 - Spezifikation offen gelegt und unter öffentlicher Kontrolle

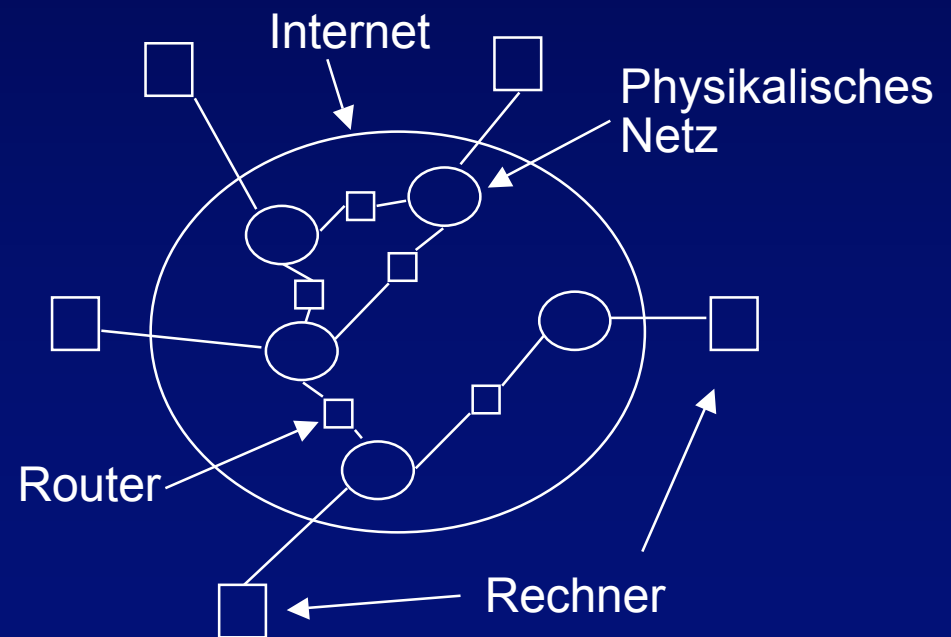
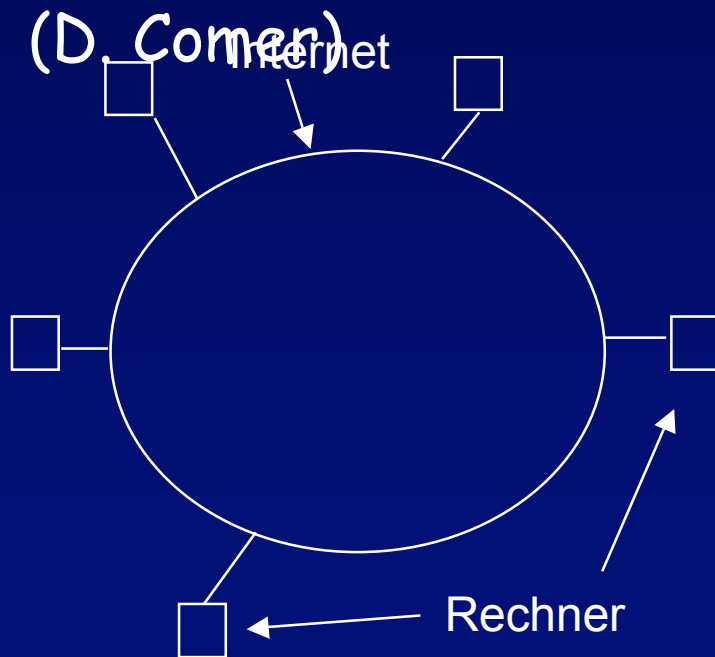
Schichtenarchitektur von TCP/IP



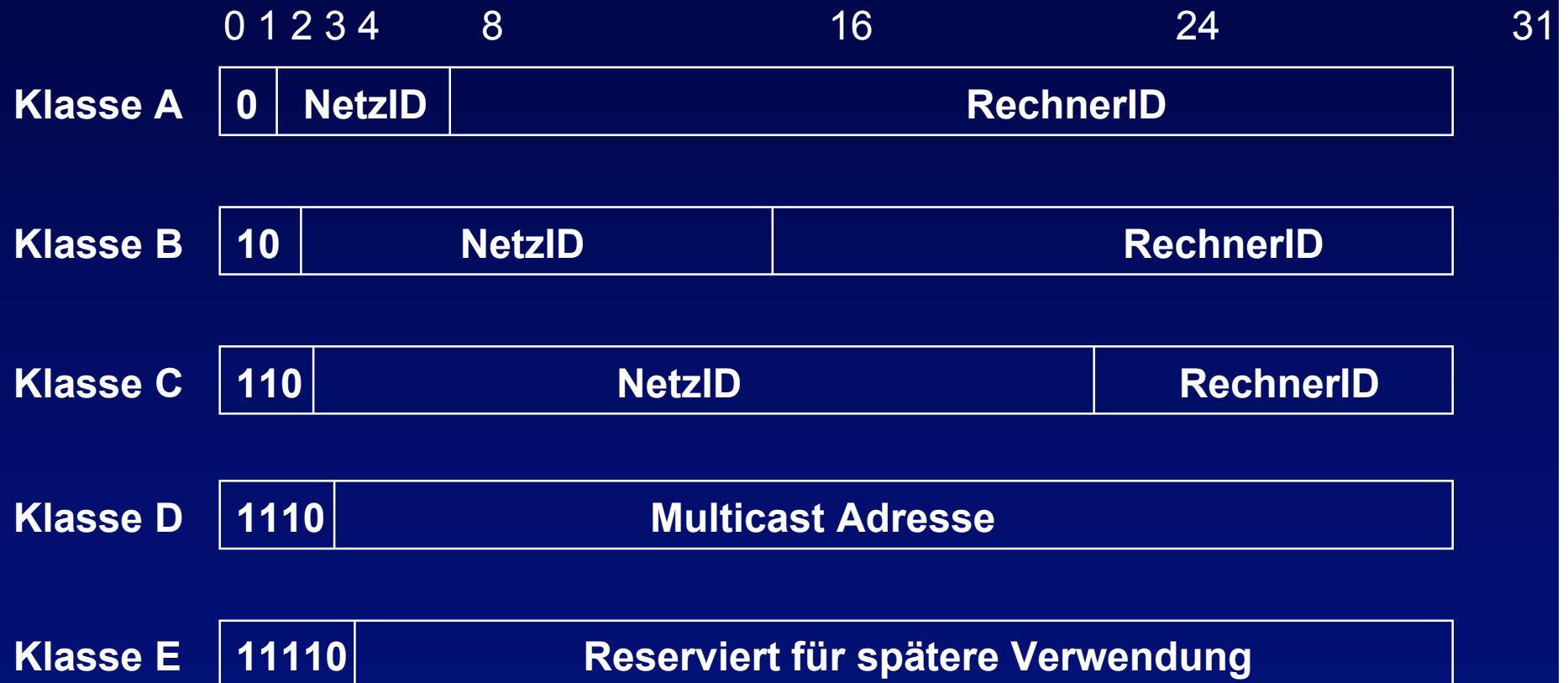
Adressierung
Das IP Protokoll

Konzept und Architekturmodell des Internet

"The TCP/IP internet protocols treat all networks equally. A local area network like an Ethernet, a wide area network like the NSFNET backbone, or a point-to-point link between two machines each count as one network."



Adressierung im Internet: Adresstypen



Adressierung im Internet: Darstellung

- Darstellung als 4 Oktette in Dezimalnotation, getrennt durch einen Punkt, z.B. 129.132.66.1
- Klasse A zwischen 1 und 126
- Klasse B zwischen 128.1 und 191.254
- Klasse C zwischen 192.1.1 und 223.254.254

Aufbau eines IP-Paketes

0	1	2	3	4	8	16	19	24	31
Vers	HLEN	Diensttyp				Gesamtlänge			
Identifikation						Flags	Fragment-Offset		
Lebenszeit		Protokoll				Kopf-Prüfsumme			
IP-Adresse des Senders									
IP-Adresse des Empfängers									
IP-Optionen (falls vorhanden)								"Padding"	
Daten									
...									

Internet Control Message Protocol (ICMP)

Einführung in ICMP

- Steuerungsfunktionen und Fehlermeldungen
- Den "normalen" Benutzern nicht zugänglich ist.
- Typische Aufgaben:
 - Koordination zwischen Routern und Endsystemen
 - Fehlererkennung und -korrektur
 - Überwachung und Messung des Verkehrsaufkommens
- ICMP benutzt den IP-Dienst, gehört logisch aber auf die selbe Protokollschicht, wie das IP-Protokoll.

ICMP-Meldungstypen

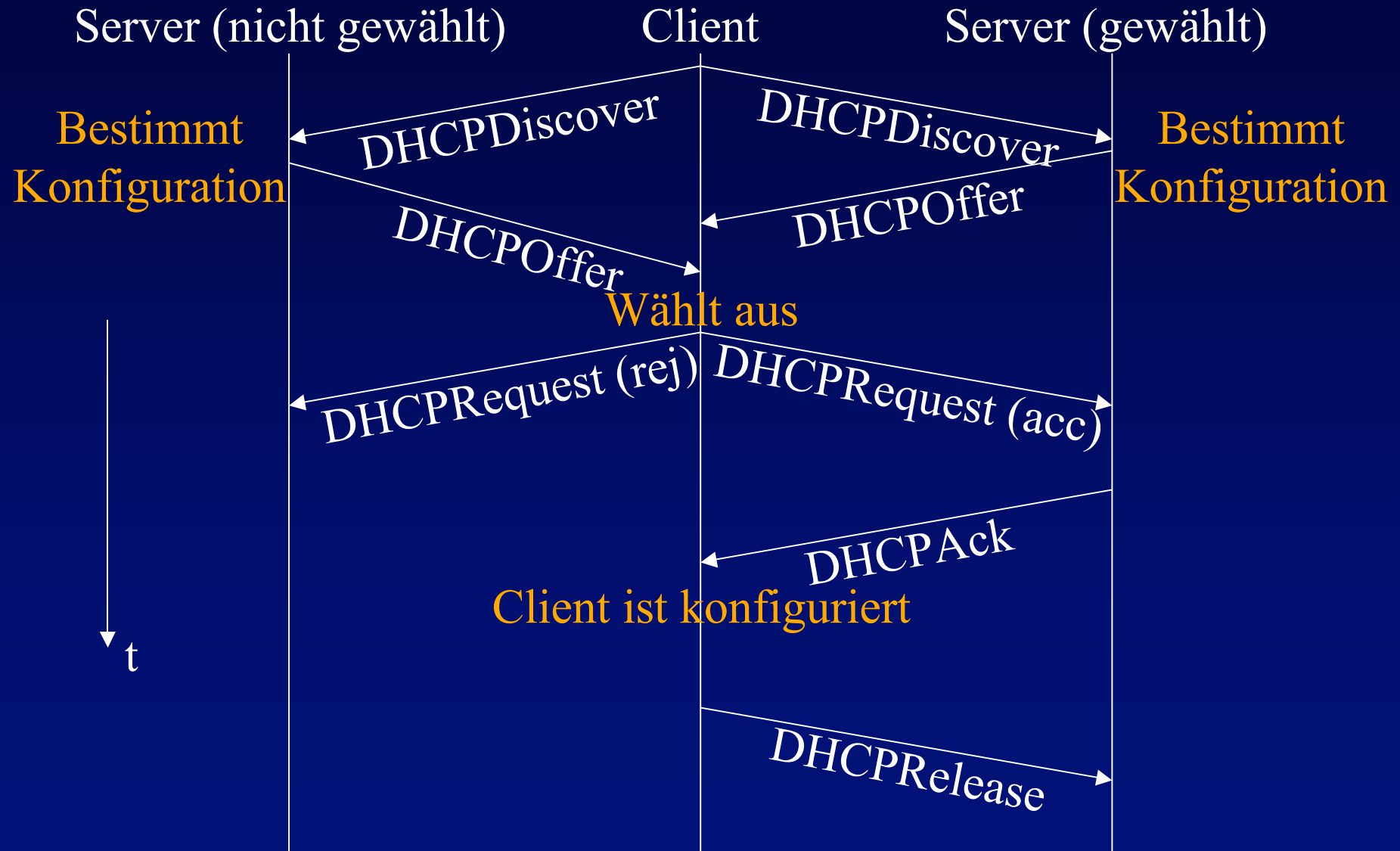
- 0 Echo-Antwort
- 3 Destination unerreichbar
- 4 "Source Quench"
- 5 Änderung einer Route
- 8 Echo-Anforderung
- 11 Datagramm-Lebenszeit überschritten
- 12 Parameter-Problem im Datagramm
- 13 Zeitstempel-Anforderung
- 14 Zeitstempel-Antwort
- 15 Informations-Anforderung (nicht mehr benötigt)
- 16 Informations-Antwort (nicht mehr benötigt)
- 17 Adressmasken-Anforderung
- 18 Adressmasken-Antwort

Automatische Konfiguration mit dem Dynamic Host Configuration Protocol (DHCP)

Wozu DHCP?

- Automatische Konfiguration von Hosts
- Zu konfigurierende Parameter:
 - IP-Adresse
 - Gateway- (Router-) Adressen
 - IP-Maske (Subnetting)
 - Adressen der DNS-Server
 - Link MTU, default time-to-live
 - ... und sehr viel mehr, s. Appendix A von [RFC 2131](#)
- Ohne DHCP: Einstellung von Hand (Netzwerk-Kontrollfeld in Windows, Registry, oder nicht einstellbar)
- Unangenehm: Bei einer Konfigurationsänderung von Hand muss Windows (95, 98) neu gestartet werden

Typischer Ablauf des DHCP-Protokolls



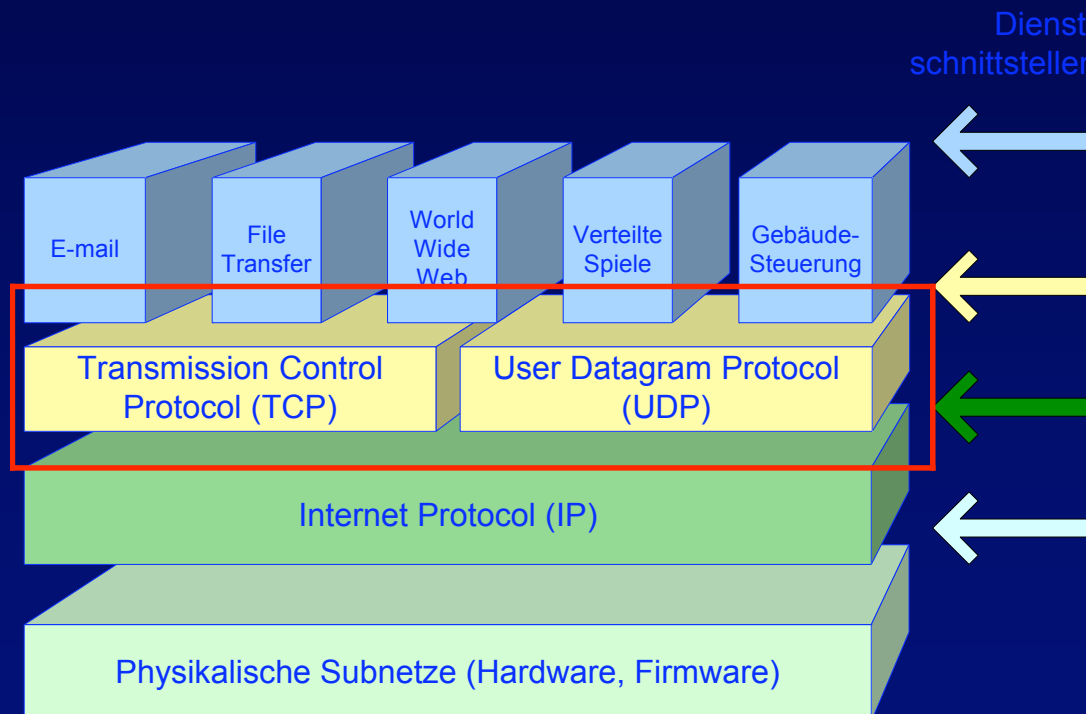
Die Transportprotokolle:

Transmission Control Protocol (TCP)

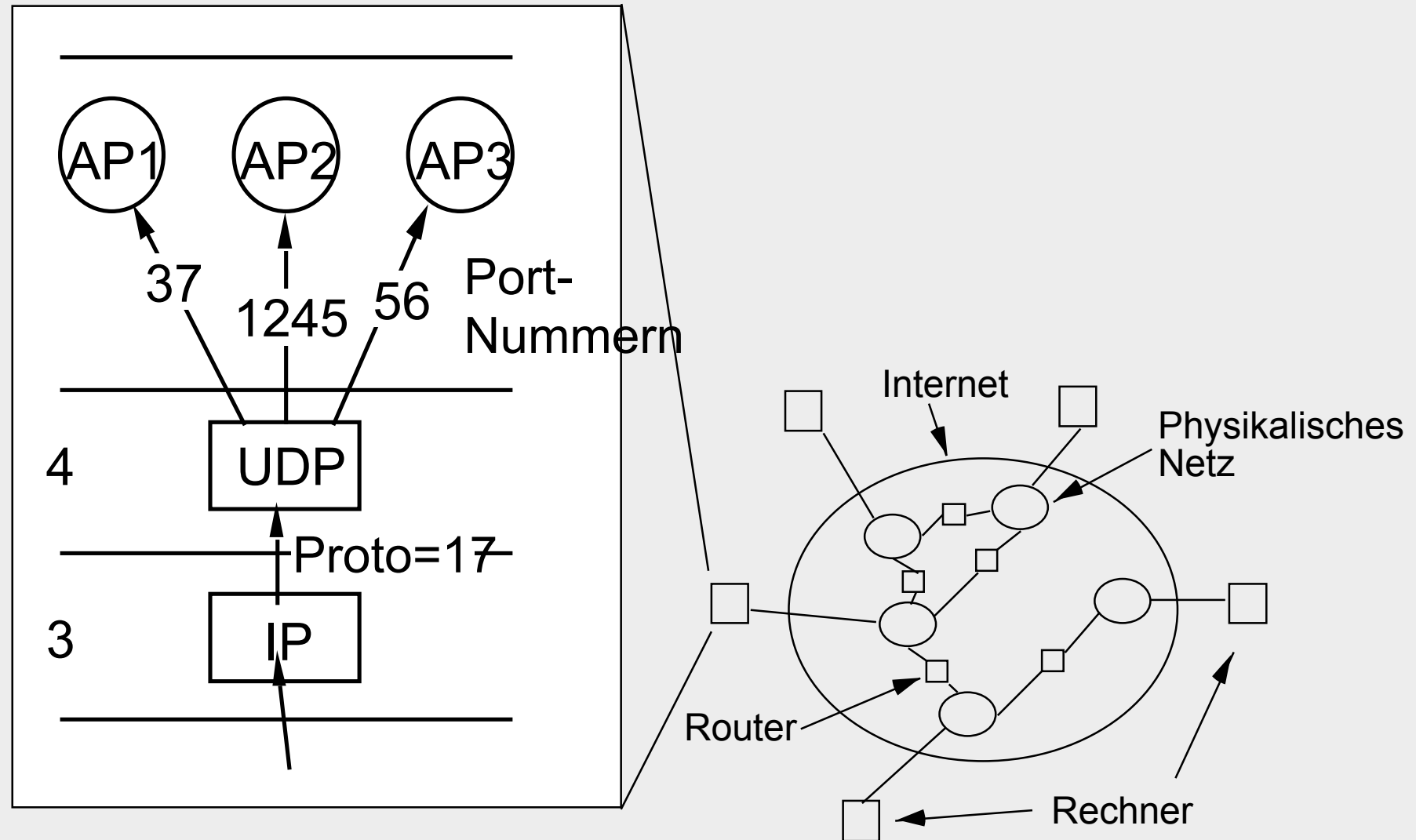
User Datagram Protocol (UDP)

Die Transportschicht im Schichtenmodell

- TCP implementiert ein verbindungsorientiertes, zuverlässiges Transport-Protokoll, aufbauend auf dem IP-Dienst.



Adressierung von Anwendungsprozessen: Beispiel TCP/IP - Portnummern



Koordination der global zugeordneten Ports

- Internet Assigned Numbers Authority (IANA):
- Bereich 0.. 1023: Für globale "well known" ports, kontrolliert von der IANA
- Bereich 1024 .. 65535: Frei für dynamische Allokierung
- Aktuelle globale / statische Zuordnungen:
<http://www.iana.org/assignments/port-numbers>

Einige Eigenschaften des Transmission Control Protocol (TCP)

- Verbindungsorientiert
- Vollduplex-Verbindung
- stellt eine "byte pipe" zur Verfügung -
unstrukturierter Datenstrom
- Sliding Window-Protokoll

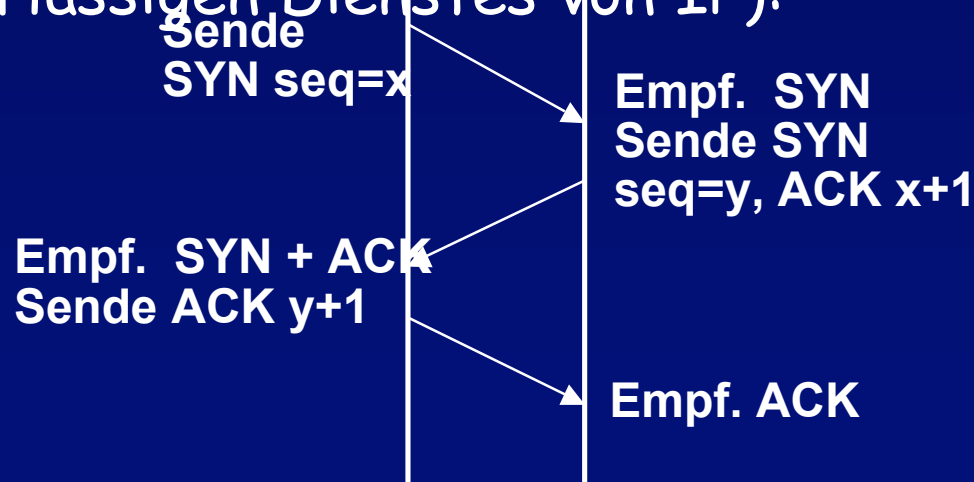
TCP-Segmentformat

0	4	10	16	24	31
Port des Senders			Port des Empfängers		
Sequenznummer im Bytestrom des Senders					
Bestätigungsnummer (ACK in Gegenrichtung)					
HLEN	Reserviert	Code Bits	Grösse des Empfängerfensters		
Prüfnummer (auch über Daten)			Dringlichkeitszeiger		
Optionen (falls vorhanden)				"Padding"	
Daten					
...					

- Code Bits: URG, ACK, PSH, RST, SYN, FIN
- Dringlichkeitszeiger: zeigt auf das Ende der dringenden Daten im TCP-Datenfeld.

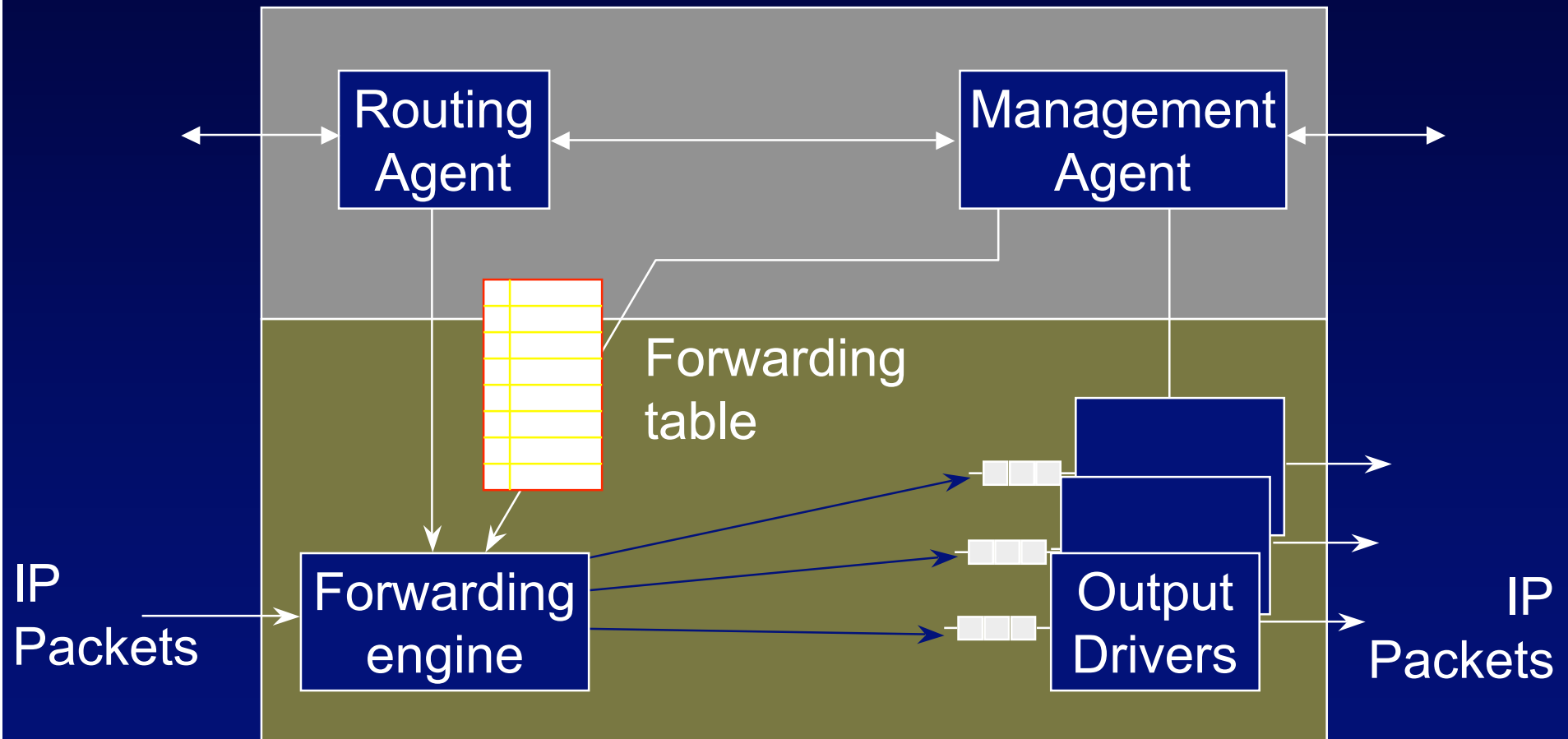
Verbindungsaufbau

- Aktives Öffnen einer Verbindung (SYN)
- Passive Seite nimmt eine Verbindung auf einer bestimmten Port-Nummer entgegen
- Die initialen Sequenznummern werden auf jeder Seite zufällig gewählt und bestätigt.
- 3-fach-Handshake (nötig wegen des unzuverlässigen Dienstes von IP):



Routing

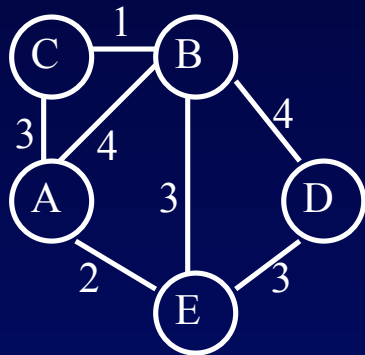
Modell eines Routers



Distanzvektor Routing

- Jeder Router sendet einen Vektor mit den kürzesten Distanzen zu allen erreichbaren Netzadressen an seine Nachbarn.
- Ein Router führt seine Tabellen nach, falls er von einem Nachbarn erfährt, dass eine Netzadresse auf kürzerem Weg erreicht werden kann.
- Der Distanzvektor wird periodisch gesendet oder immer, wenn die Tabellen nachgeführt werden müssen.

Distanzvektor Routing Beispiel



Knoten A		
Destination	Distanz	Nächster Knoten
B	4	B
C	3	C
E	2	E
D	5	E

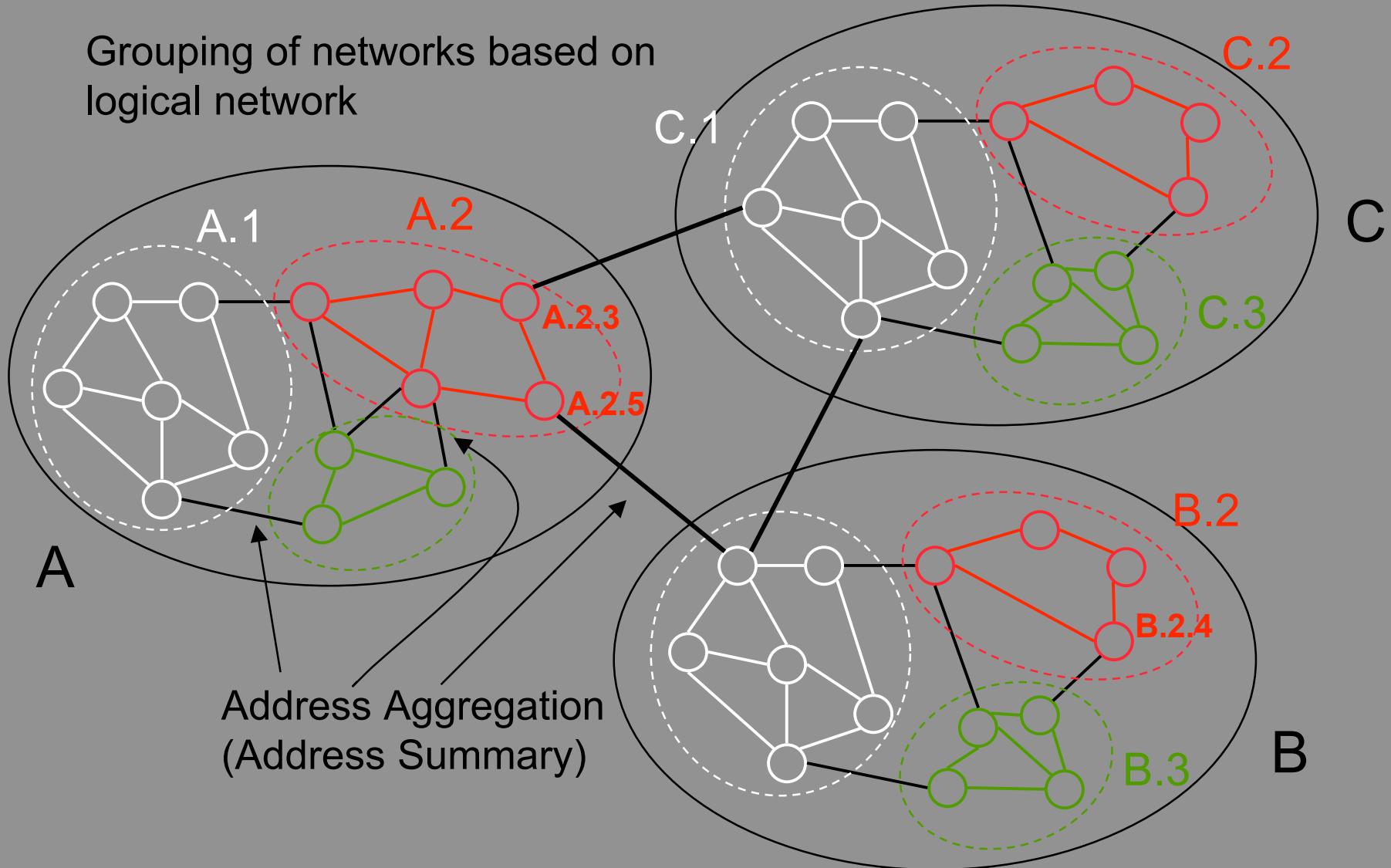
Routing Updates:

B->A: [(D,4) (E,3) (C,1) (A,4)]

E->A: [(D,3)(B,3)(A,2)]

Hierarchisches Routing / Autonomous Systems

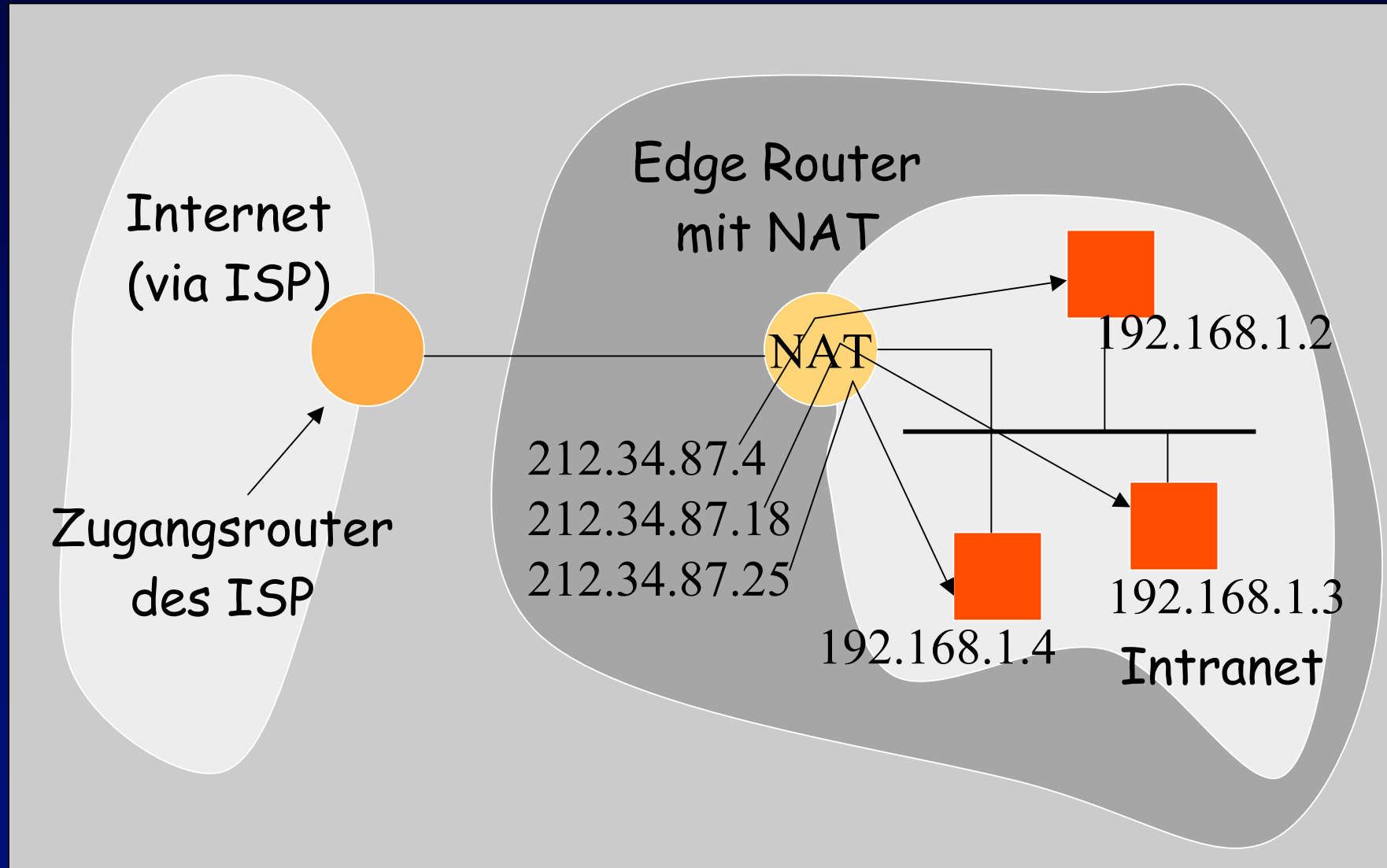
Grouping of networks based on logical network



Network Address Translation (NAT)

Prof. B. Plattner

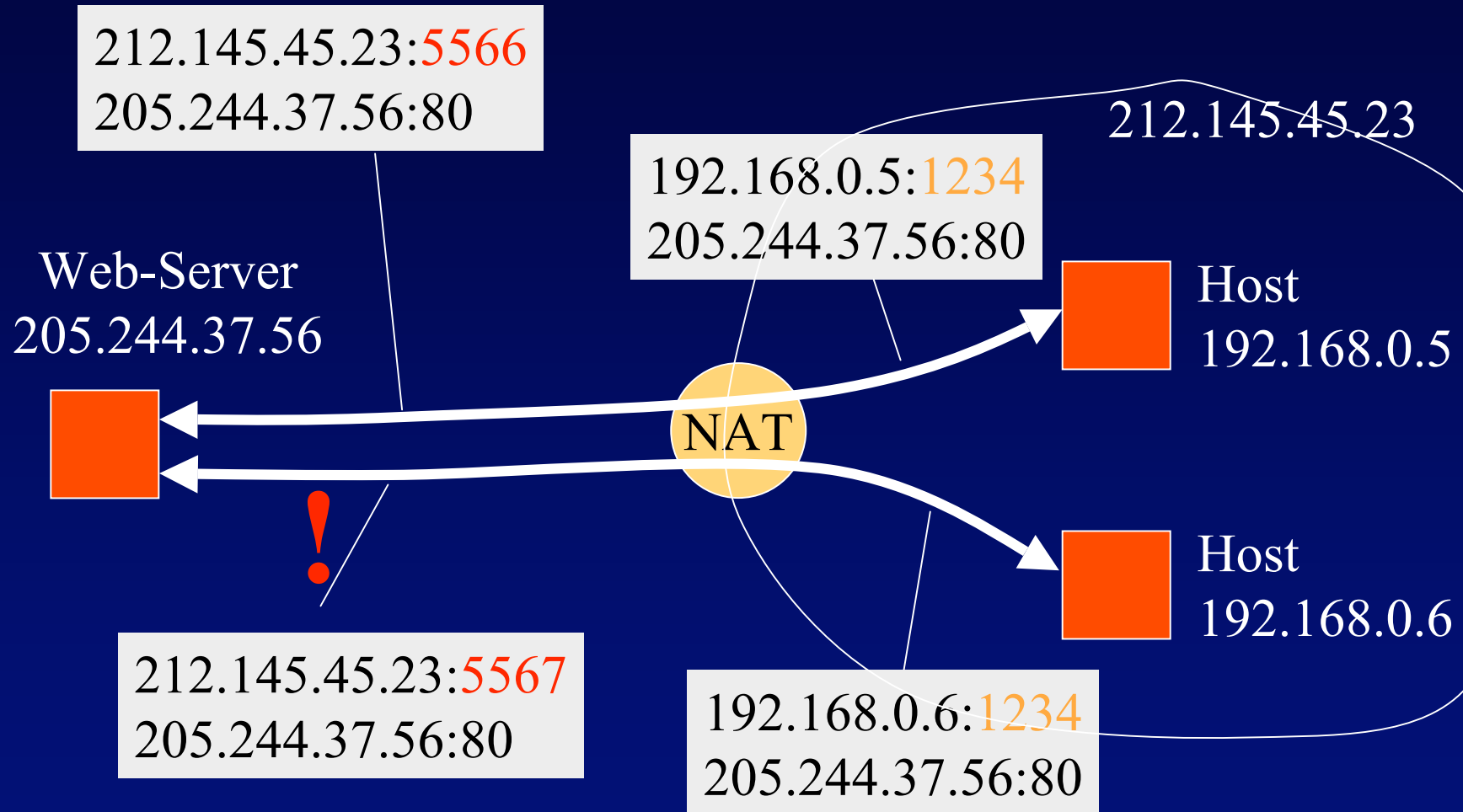
Beispiel: Basic NAT



Voraussetzungen für die Umsetzung

- Internet-Adressraum muss einen Teil mit global eindeutigen und einen Teil mit wiederverwendbaren, lokalen Adressen aufgeteilt werden
- Wiederverwendbar, nur lokal geroutet:
 - Klasse A: Netz 10.0.0.0 (10/8)
 - Klasse B: Netze 172.16.0.0 bis 172.31.0.0 (172.16/12)
 - Klasse C: Netze 192.168.0.0 bis 192.168.255.0 (192.168/16)
- Lokale Adressen werden nach aussen nicht bekannt gemacht, nur die zugehörigen globalen Adressen
- Routing-Protokoll innerhalb des Intranet arbeitet mit den lokalen Adressen

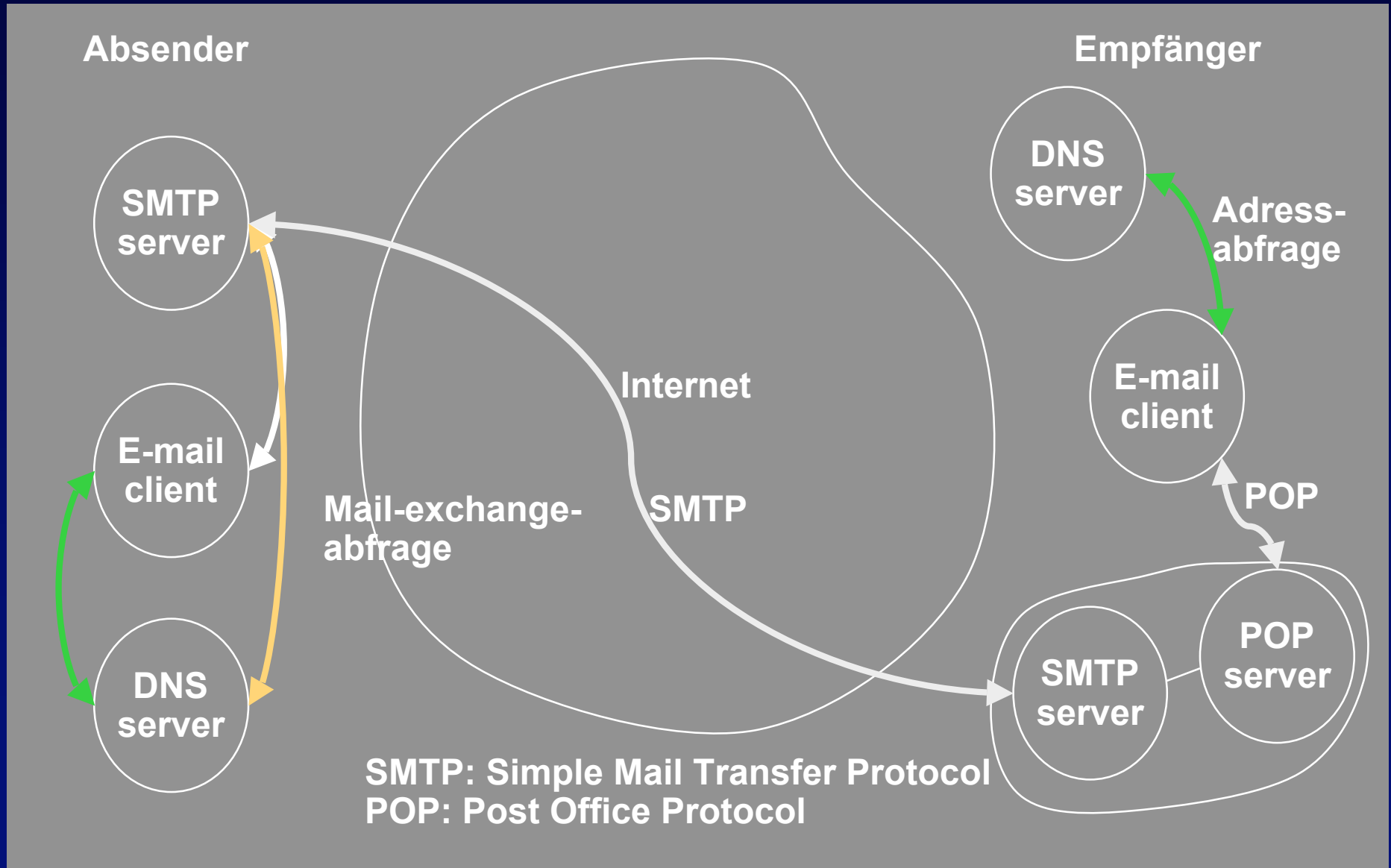
Network Address and Port Translation



NAT ordnet neue Port-Nummern zu

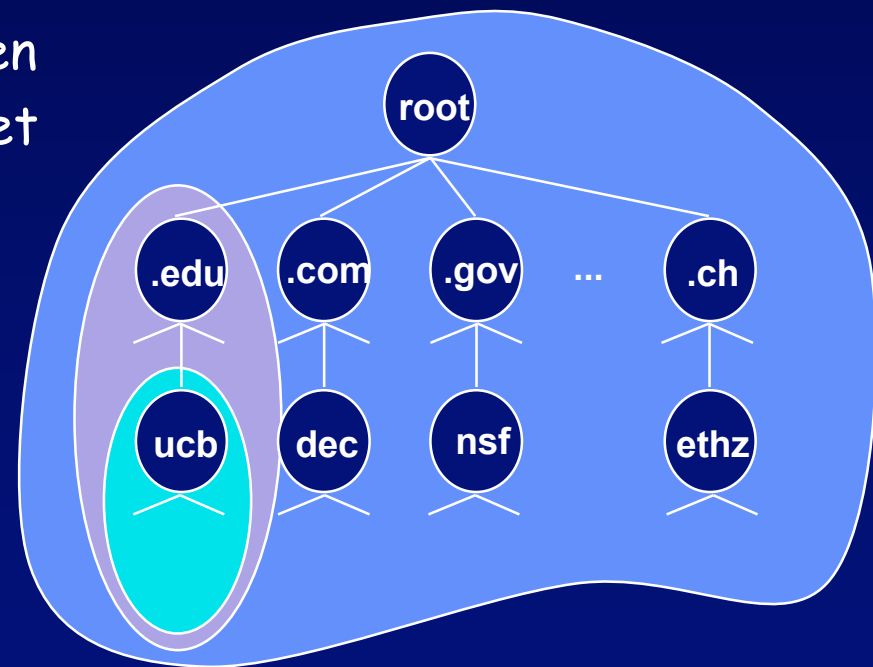
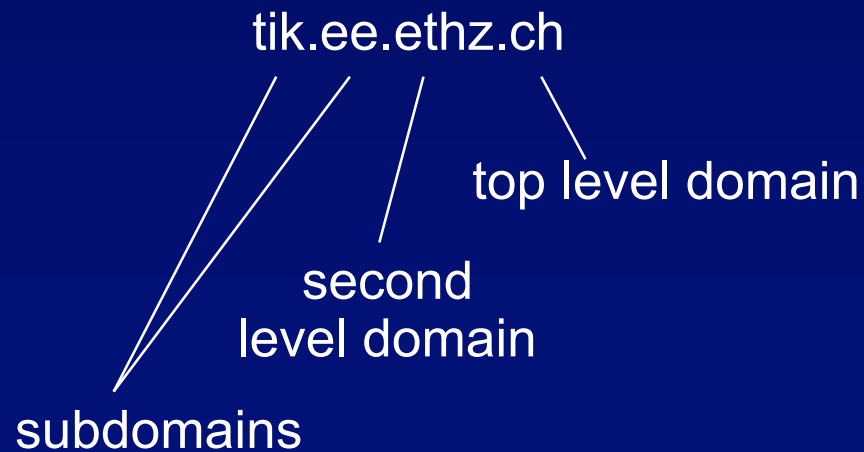
Domain Name System (DNS)

Motivation: E-mail-Infrastruktur des Internet



Benennbare Objekte, Syntax und Abbildung auf Adressen

- DNS-Namen können auf verschiedenartige Objekte abgebildet werden, z.B. Rechneradressen, e-Mail-Adressen usw.
- Ein Eintrag "dn1.ethz.ch" kann also einen einzelnen Rechner bezeichnen, und "inf.ethz.ch" ein e-Mail-Domain. Dem Namen sieht man diesen Unterschied nicht an.
- Verschiedene DNS-Namen können auf das gleiche Objekt abgebildet werden (alias).



Liste der root servers

/netinfo/root-servers.txt

Sep 97

The following hosts are functioning as root domain name servers for the Internet:

HOSTNAME	NET ADDRESSES	SERVER PROGRAM
A.ROOT-SERVERS.NET	198.41.0.4	BIND (UNIX)
B.ROOT-SERVERS.NET	128.9.0.107	BIND (UNIX)
C.ROOT-SERVERS.NET	192.33.4.12	BIND (UNIX)
D.ROOT-SERVERS.NET	128.8.10.90	BIND (UNIX)
E.ROOT-SERVERS.NET	192.203.230.10	BIND (UNIX)
F.ROOT-SERVERS.NET	192.5.5.241	BIND (UNIX)
G.ROOT-SERVERS.NET	192.112.36.4	BIND (UNIX)
H.ROOT-SERVERS.NET	128.63.2.53	BIND (UNIX)
I.ROOT-SERVERS.NET	192.36.148.17	BIND (UNIX)
J.ROOT-SERVERS.NET	198.41.0.10	BIND (UNIX)
K.ROOT-SERVERS.NET	193.0.14.129	BIND (UNIX)
L.ROOT-SERVERS.NET	198.32.64.12	BIND (UNIX)
M.ROOT-SERVERS.NET	202.12.27.33	BIND (UNIX)

Objekttypen in DNS

Typ	Bezeichnung	Inhalt
A	Hostadresse	32-Bit IP-Adresse
CNAME	Kanonischer Name	Domainname für ein Alias
HINFO	CPU und Betriebssystem	Informationen über den Host
MINFO	E-Mail Information	Informationen über Mailbox
MX	E-Mail Exchanger für	16-Bit Präferenz und Name des Host, der diese Domain als Mail-Server fungiert
N	Namens-Server Domain	Name des verbindlichen Servers für diese Domain
PTR	"Pointer"	Domainname
SOA	Namensautorität Teile der	Mehrere Felder, die angeben, für welche Namenshierarchie der Server zuständig ist