

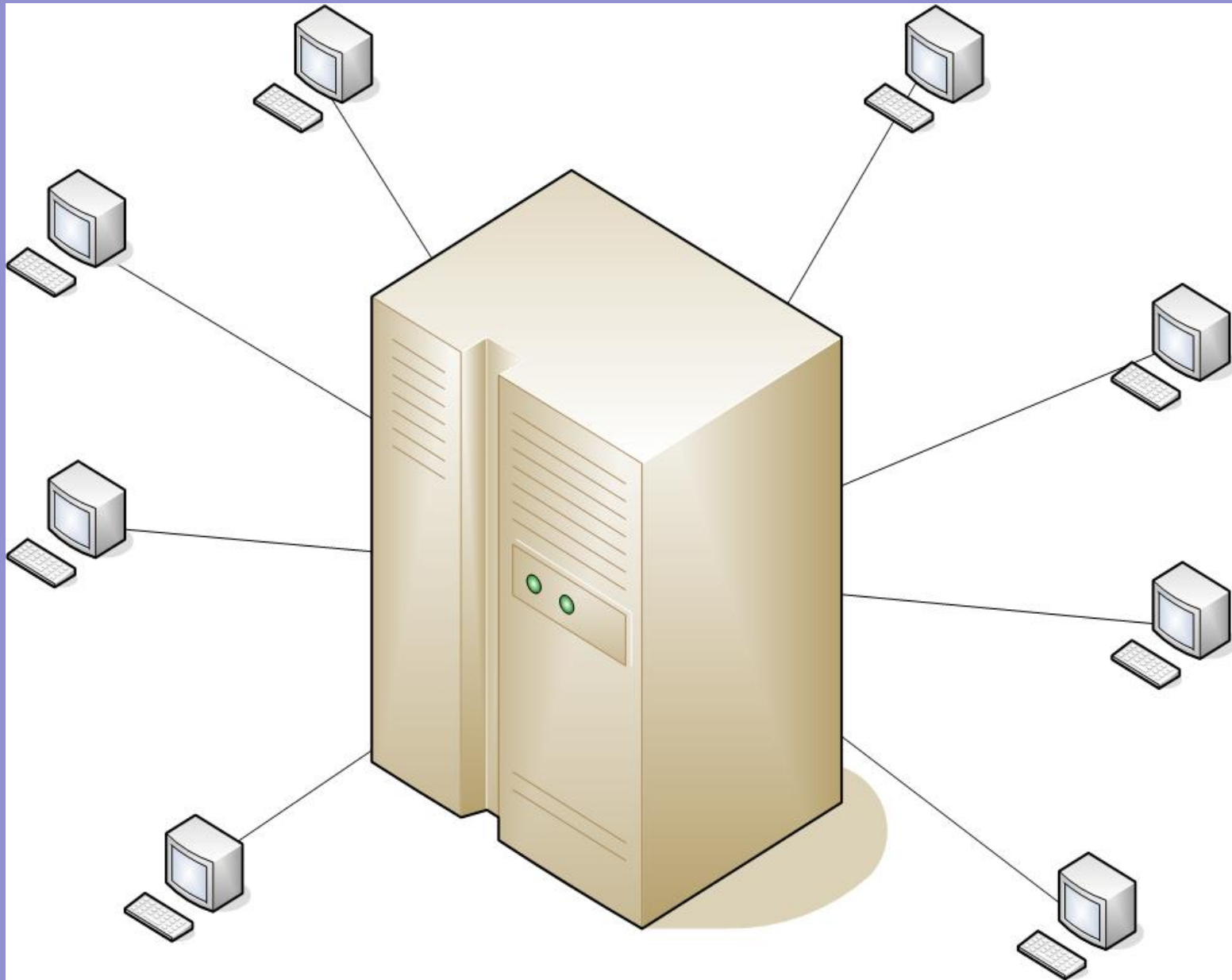
Networking

lukas.feiler@lukasfeiler.com

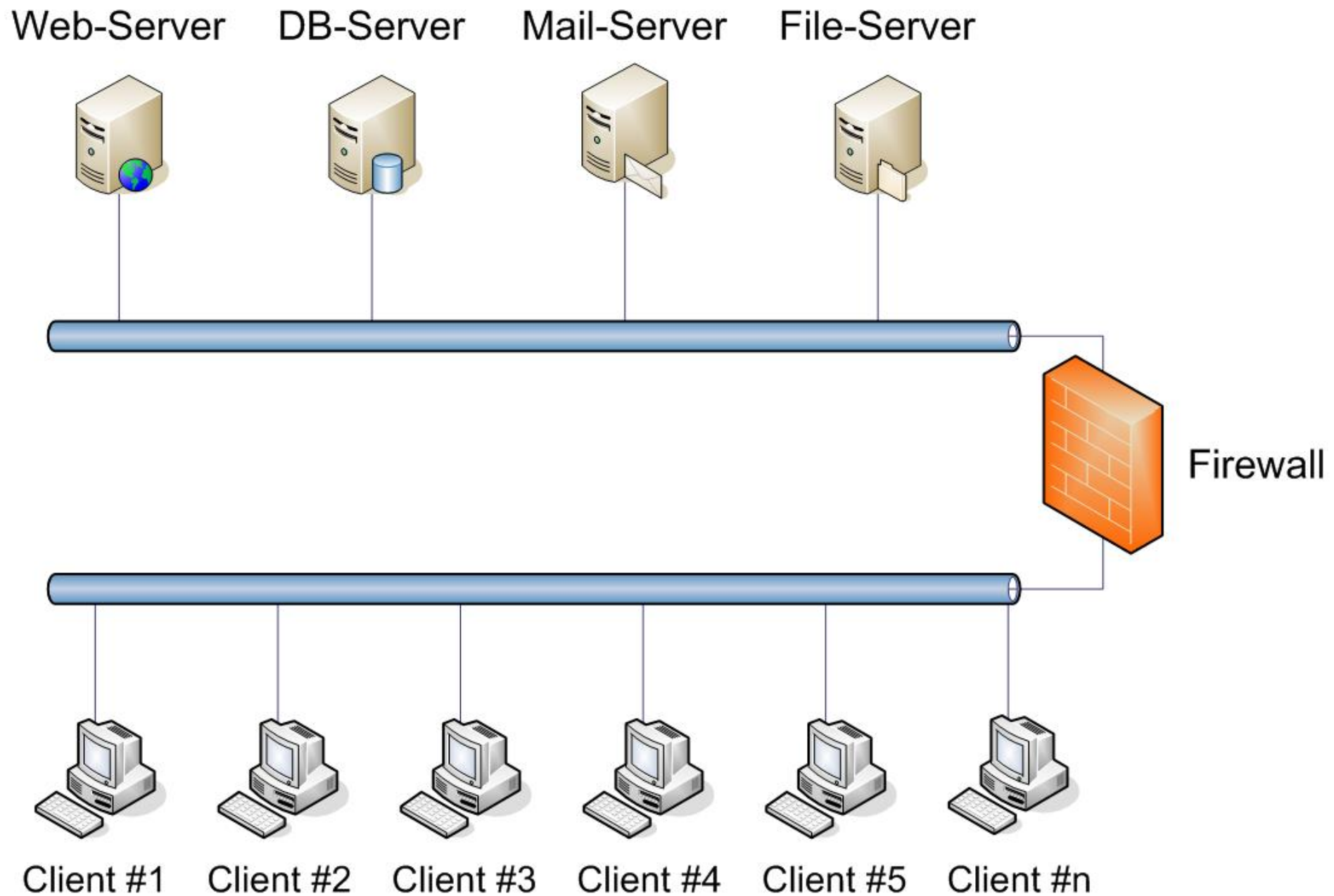
<http://teaching.lukasfeiler.com>

Was ist „Networking“?

Geschichte des Networking



Früher: zentralistische Struktur; 1 Mainframe, viele Terminals



Heute: Netzwerke - dezentrale Struktur; viele Clients, viele Server

Server: bietet einen Dienst im Netzwerk an

Client: benutzt einen Dienst im Netzwerk

Host: ieS ein Server; iwS auch ein Client

Internet: Das weltweite auf TCP/IP basierende Netz

LAN/Intranet: Local Area Network

WAN: Wide Area Network; privates Netz über Standleitungen

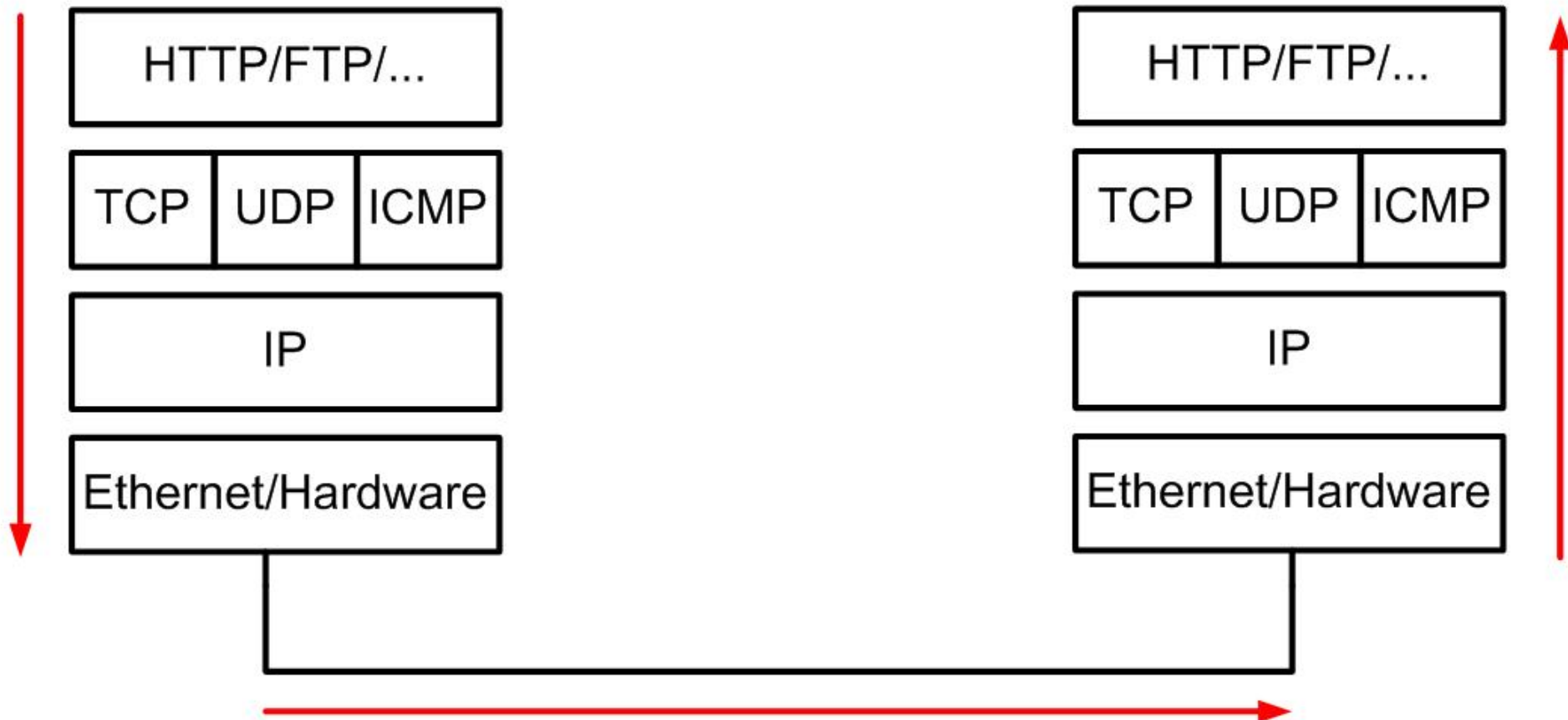
WLAN: Wireless Local Area Network

WiFi: Wireless Fidelity (=WLAN)

Extranet: Verbindung mehrerer LANs über das Internet

Netzwerk-Schichten

- 7 Schichten nach OSI-Modell
- 4 Schichten nach DoD-Protokollfamilie



4 Netzwerkschichten

Gliederung des Unterrichts

- Ethernet/Hardware
- IP (Routing)
- TCP, UDP, ICMP
- DNS, SMTP, FTP, HTTP, HTTPS, SSH
- IT-Security
- Komplexe Netzwerkkomponenten
- Weitere ausgewählte Themenbereiche
 - VPN, WLAN, IDS, Kryptographie
- Serverarchitekturen
- Exkurs: Open Source Software

Quellen

<http://teaching.lukasfeiler.com/>

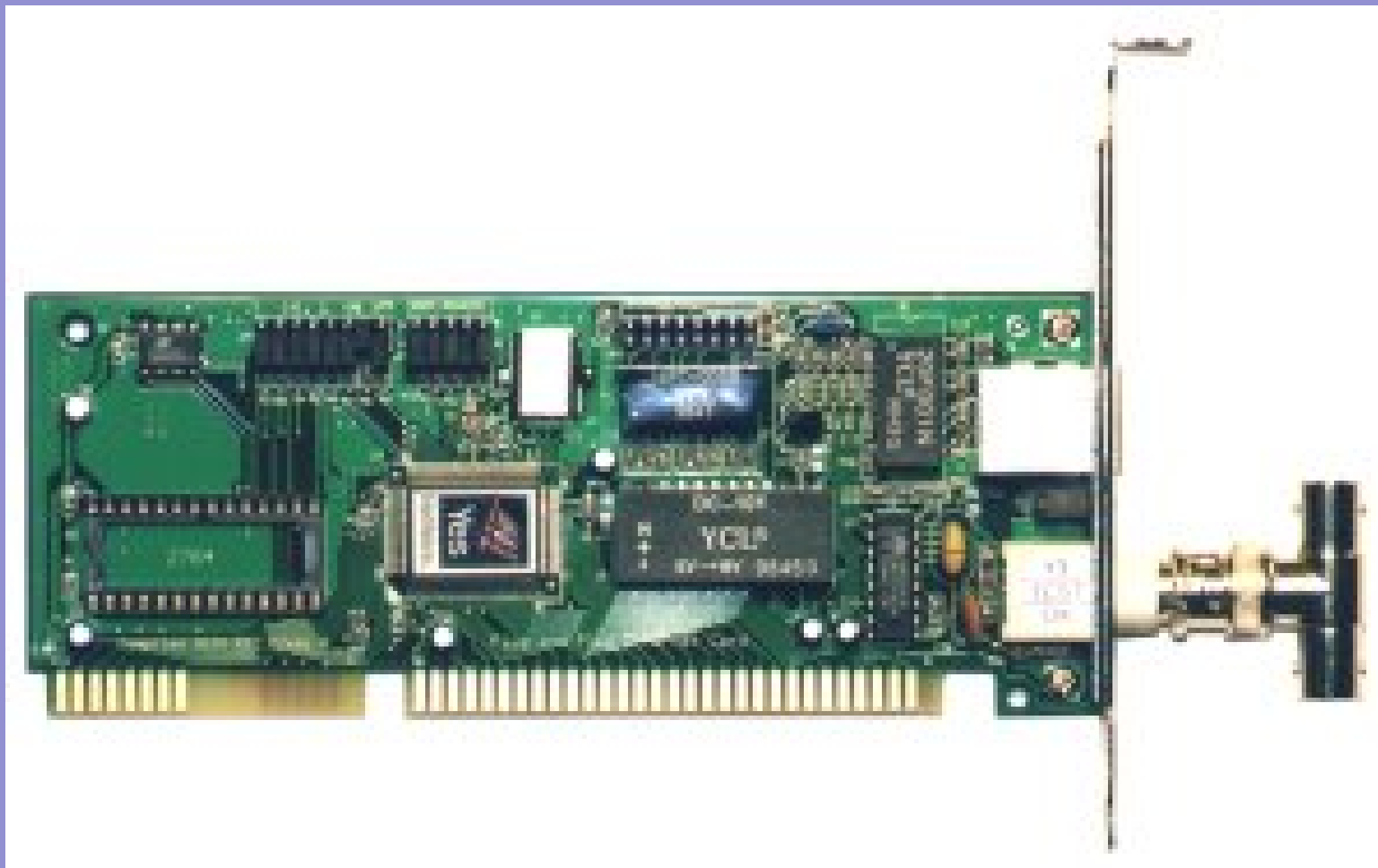
- Linux Network Administrator's Guide, Second Edition
<http://www.tldp.org/guides.html>
bzw. Linux Wegweiser für Netzwerker, 2. Auflage
<http://www.oreilly.de/openbook/>
- DNS and BIND, O'Reilly; va. die ersten 37 Seiten
- Linux-Firewalls - Ein praktischer Einstieg
<http://www.oreilly.de/openbook/>
- Practical Unix and Internet Security, O'Reilly
- i'X, www.heise.de/ix

Netzwerk-Hardware (Ethernet)

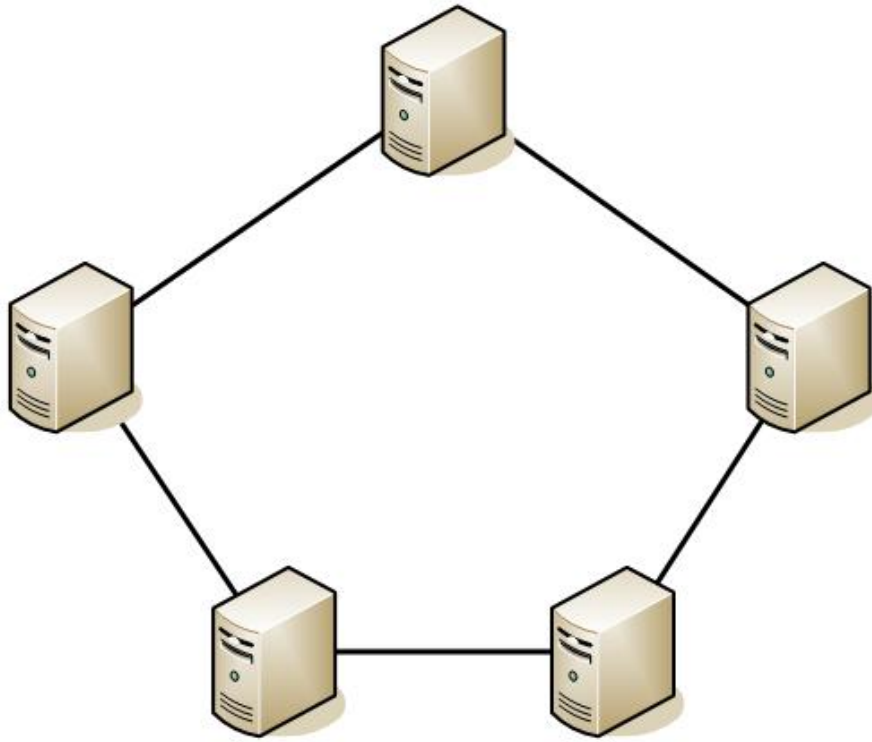
Die erste Netzwerk-Schicht

Netzwerk-Hardware (Ethernet)

- Netzwerkkarte (NIC = Network Interface Card)
- Netzwerkkabel (Thin Ethernet, Twisted Pair)
- Hub/Switch

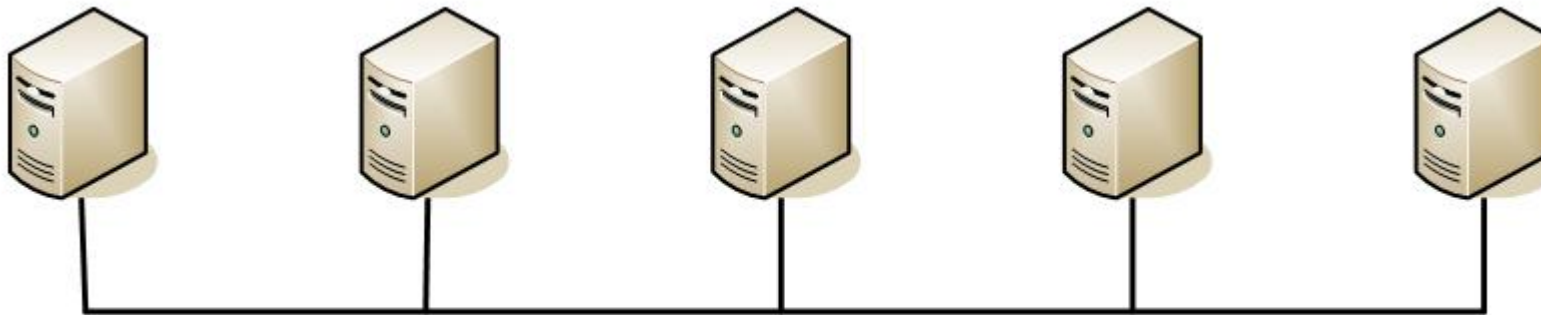


NIC mit BNC und RJ-45 Anschluss

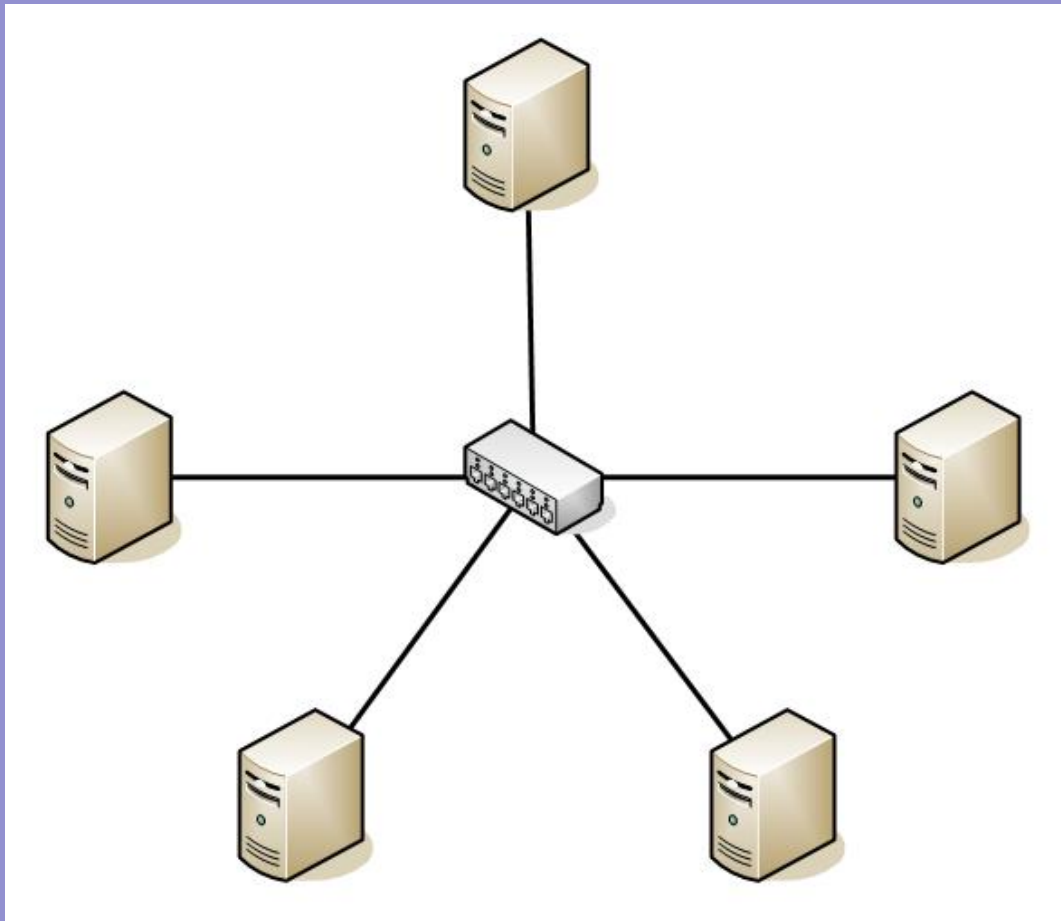


- nur 10 MBit/s
- sehr fehleranfällig

idR Ring-Topologie (links)
od. Bus-Topologie (unten)



Thin Ethernet (BNC, coaxial)



- 100 MBit/s
- (nur) 1 Single Point of Failure
- idR Stern-Topologie

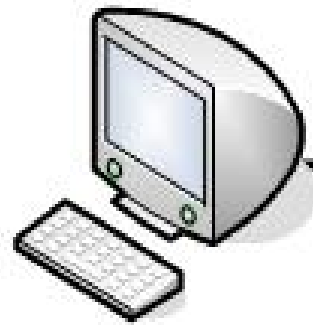
(Cross Over Twisted Pair um 2 Rechner unmittelbar zu verbinden)

Hub

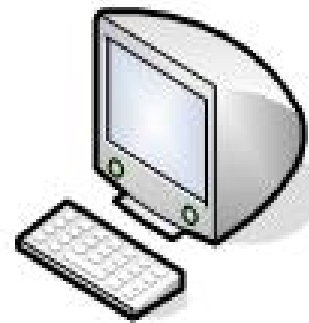
- sendet Daten an alle Ports
- daher langsamer

Switch

- sendet Daten nur an den „richtigen“ Port
- daher schneller
- 8-Port 100MBit Switch ca. 15 EUR



Cross Over Twisted Pair



Switch/Hub

Twisted Pair



Twisted Pair



Zwei Möglichkeiten um 2 (od. mehrere) Rechner zu verbinden

MAC-Adressen

Das Protokoll Ethernet identifiziert einzelne Rechner des lokalen Netzes anhand der MAC-Adresse.

MAC-Adresse \neq IP-Adresse !!!

Eine MAC-Adresse besteht aus 6 Teilen
z.B. 00:80:AD:18:AC:94

Damit Ethernet Daten an einen best. Rechner schicken kann, muss die MAC-Adresse bekannt sein.

MAC-Adresse (Hardware-Adresse der Netzwerkkarte)

ARP (Address Resolution Protocol)

Benötigt ein Rechner zu einer IP-Adresse die MAC-Adresse, erfolgt eine Anfrage mittels ARP an alle Rechner im lokalen Netz.

IP (Internet Protocol; IPv4 & v6)

Die zweite Netzwerk-Schicht

- Zuordnung von logischen und physikalischen Adressen
- Aufbau der logischen Verbindung
- Routing
- Fragmentierung von IP Paketen

IP-Adressen (IPv4)

Bestehen aus 4 Zahlen: zwischen 0 und 255

Private IPs: z.B 192.168.1.1

Public IPs: z.B 216.239.39.104

von NIC (Network Information Center) vergeben

1921.168.2.23

C.98.A.98

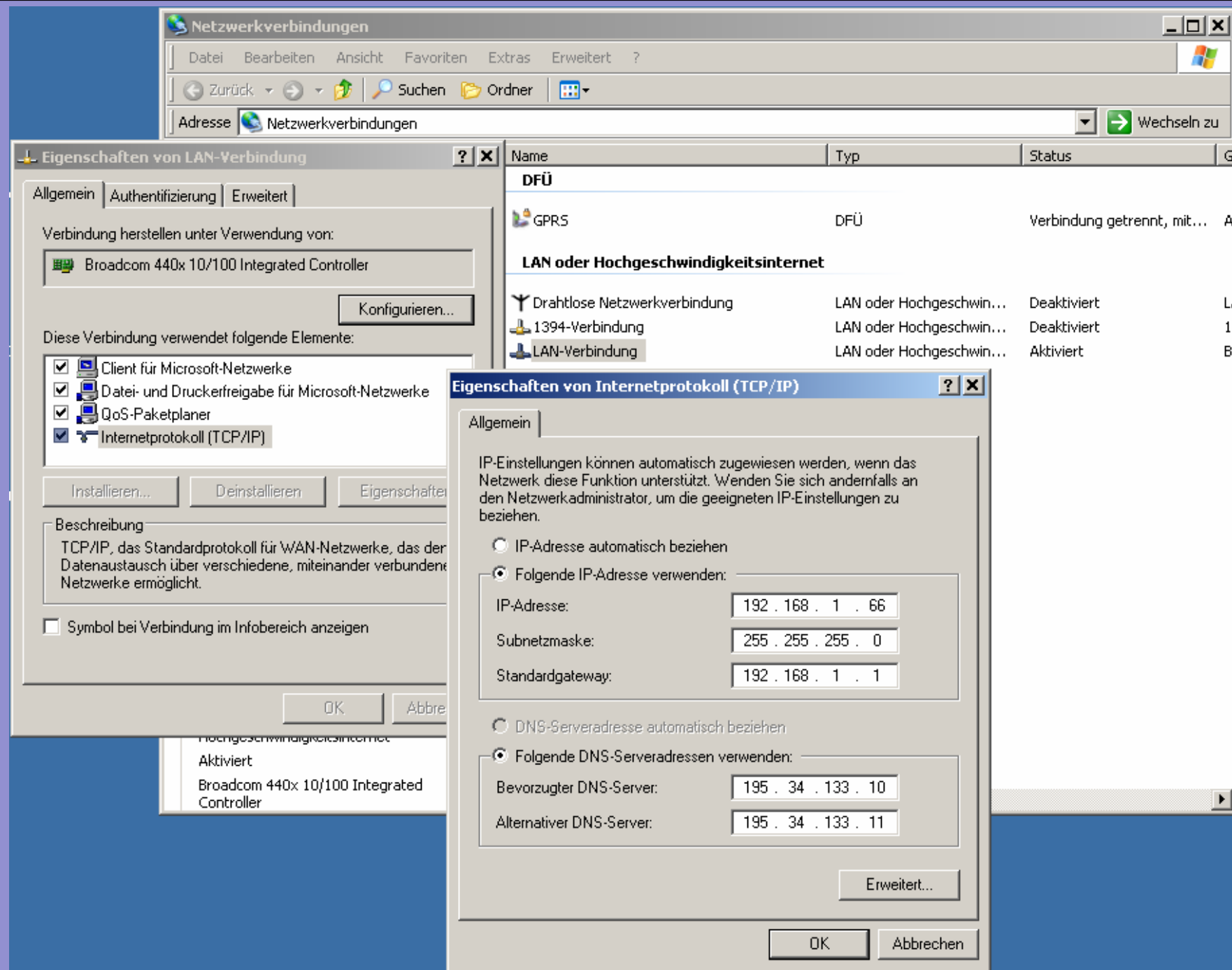
-45.23.23.23

48.243.567.324

192.168.1.0

83.23.51.255

Gültige IP(v4) Adressen?



Wie setze ich ein IP Adresse auf meinem Windows/Linux Rechner?

Folgende IP Adressen sind privat:

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

am üblichsten sind IPs beginnend mit 192.168.1

z.B 192.168.1.1

192.168.1.66

192.168.1.10

Der Rest sind public IPs!

- Ermöglicht eine Verbindung des Rechners mit sich selbst – auch ohne Netzwerkkarte!
- zu Testzwecken
- stets mit der IP Adresse 127.0.0.1

Das loopback interface (localhost)

Eine IP-Adresse besteht aus 32 bit
4 „octets“; 1 octet entspricht 8 bits
 $4 \text{ octets} = 4 * 8 \text{ bit} = 32 \text{ bit}$

1 octet:

binär	Dezimal
00000001	1
00000010	2
11111111	255

$2^{32} = 4\,294\,967\,296$ (~ 4 Mrd) Möglichkeiten

IPv4 Adressen: Warum 4 Zahlen zwischen 0 und 255?

IP-Adressen (IPv6)

Nicht 32 bit (wie bei IPv4) sondern 128 (4×32) bit
 2^{128} Möglichkeiten (eine Zahl mit 39 Nullen!)

IP Routing

Wie erreicht ein Daten-Paket sein Ziel?

Bzw. wie weiß ein Rechner wie eine andere IP zu erreichen ist?

Segmentierung

Empfängeradresse wie bei Brief:

AUSTRIA, Vienna 1030, Riedlergasse 2/15

→ IP Networks

Aufteilung der Zuständigkeit für Segmente (dezentral)

Ein Postamt auf jeder Ebene

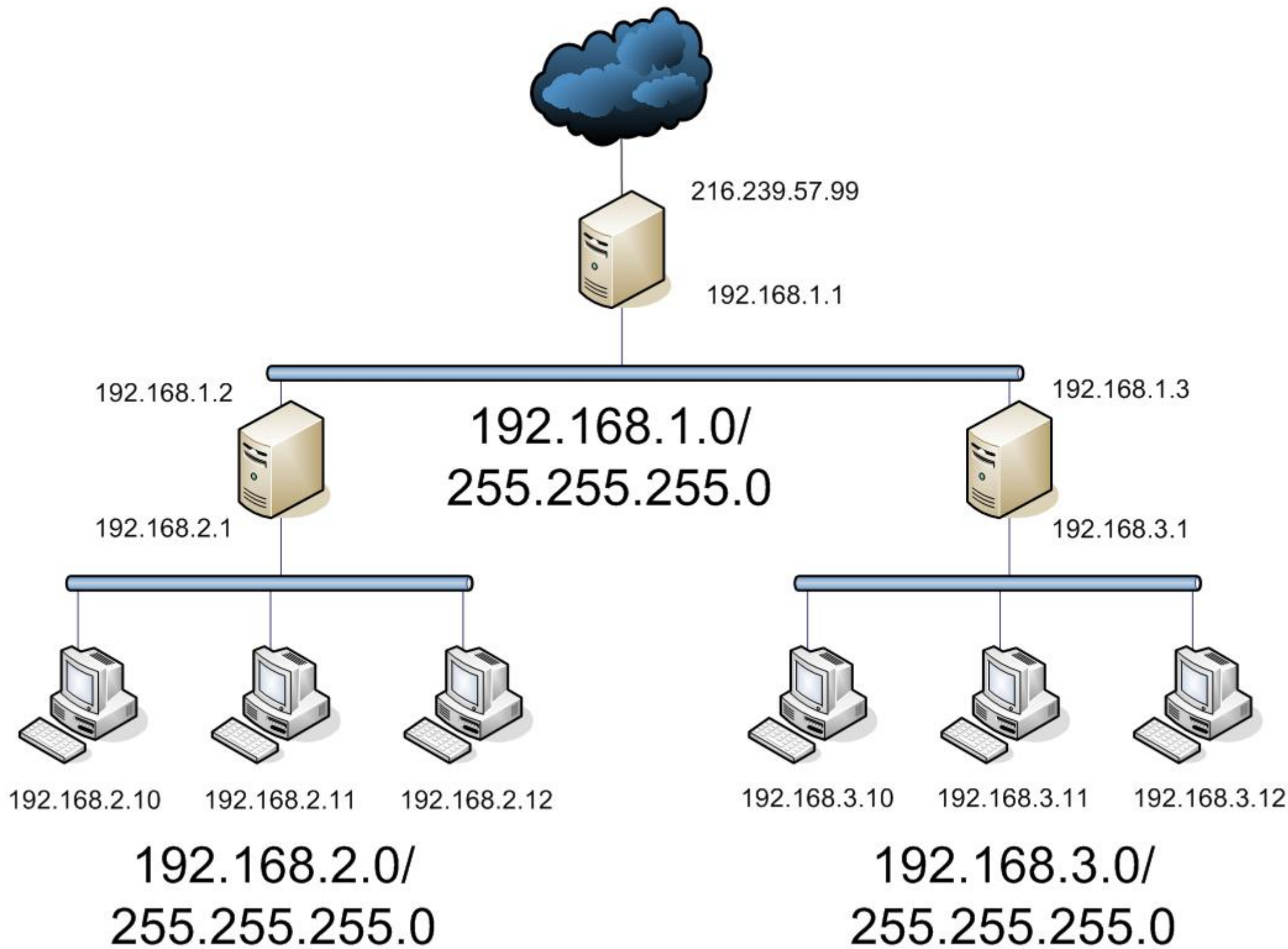
→ Gateways

IP Routing: Wie erreicht ein Daten-Paket sein Ziel?

Die Segmentierung: IP Networks

Mehrere Rechner in einem Netzwerk zusammen fassen.

Beinhaltet IPs beginnend mit	Network	Netmask
192	192.0.0.0	255.0.0.0
192.168	192.168.0.0	255.255.0.0
192.168.1	192.168.1.0	255.255.255.0



IP Adresse	Netmask	Netzwerk
192.168.1.66	255.0.0.0	
192.168.1.66	255.255.0.0	
192.168.1.66	255.255.255.0	

In welchem Netzwerk befindet sich eine IP Adresse?

IP Adresse	Netmask	Netzwerk
192.168.1.66	255.0.0.0	192.0.0.0
192.168.1.66	255.255.0.0	192.168.0.0
192.168.1.66	255.255.255.0	192.168.1.0

Alternative Schreibweise für
IP Adresse: 192.168.1.66
Netmask: 255.255.255.0

→ 192.168.1.66/24 (32-24 = 8 bits frei)

In welchem Netzwerk befindet sich eine IP Adresse?

Wie kann eine Netmask eines Netzwerkes lauten,
in dem sich die IP-Adressen 192.168.1.66 und 192.168.2.10
befinden?

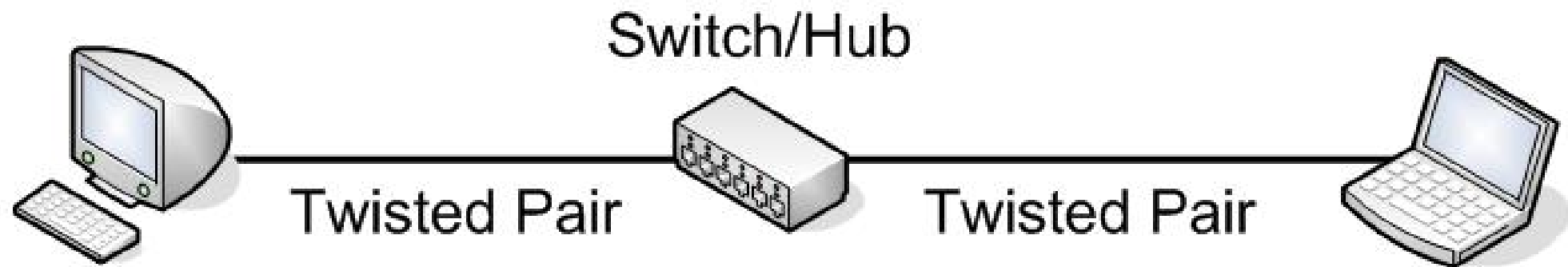
- a) 2000.255.255.255
- b) 255.0.0.0
- c) 255.255X.0.0
- d) 255.255.0.0
- e) 255.255.255.255

Welche Netmask?

Wie kann eine IP Adresse lauten, die sich im Netzwerk 192.168.0.0 mit der Netmask 255.255.255.0 befindet?

- a) 192.169.0.1
- b) 192.168.1.1
- c) 219.186.0.1
- d) 192.168.0.22
- e) 192.168.0.323
- f) 192.168.255.2
- g) 1C2.34M.23P.4H
- h) 192.168.0.219

Welche IP Adressen sind in einem best. Netzwerk?



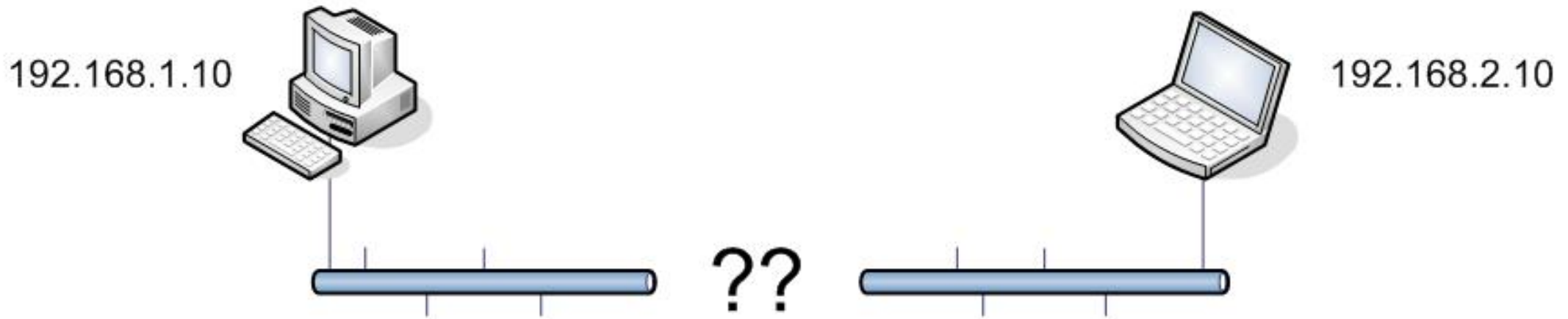
Welche IP Adressen & Netmasks müssen vergeben werden?

Aufteilung der Zuständigkeit: Gateways

Ein Rechner, der mit mehreren Netzwerken verbunden ist und Daten-Pakete zwischen diesen austauscht.

192.168.1.0/
255.255.255.0

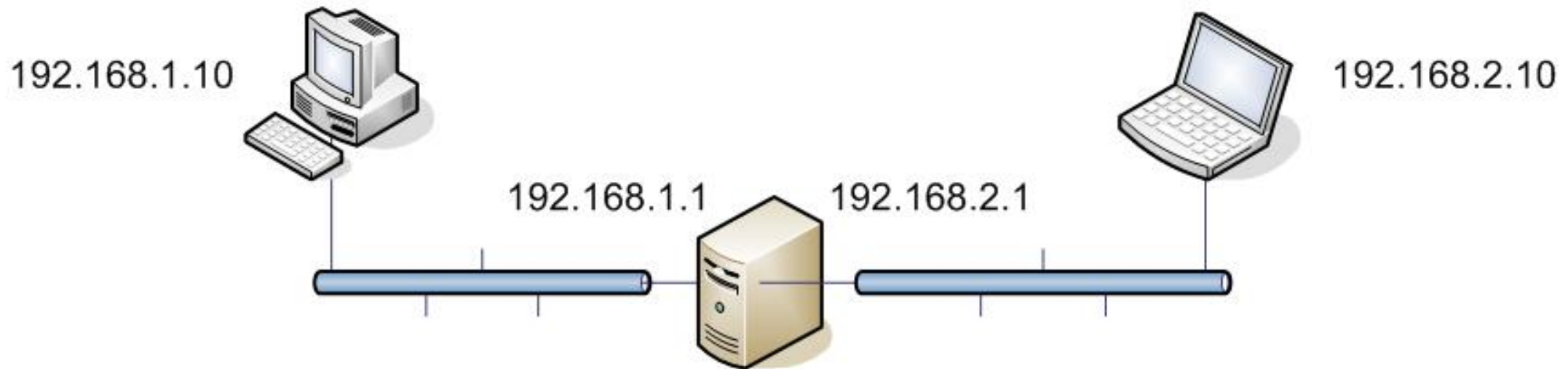
192.168.2.0/
255.255.255.0



Zwei Netzwerke ohne Gateway

192.168.1.0/
255.255.255.0

192.168.2.0/
255.255.255.0



Zwei Netzwerke mit Gateway

192.168.1.10

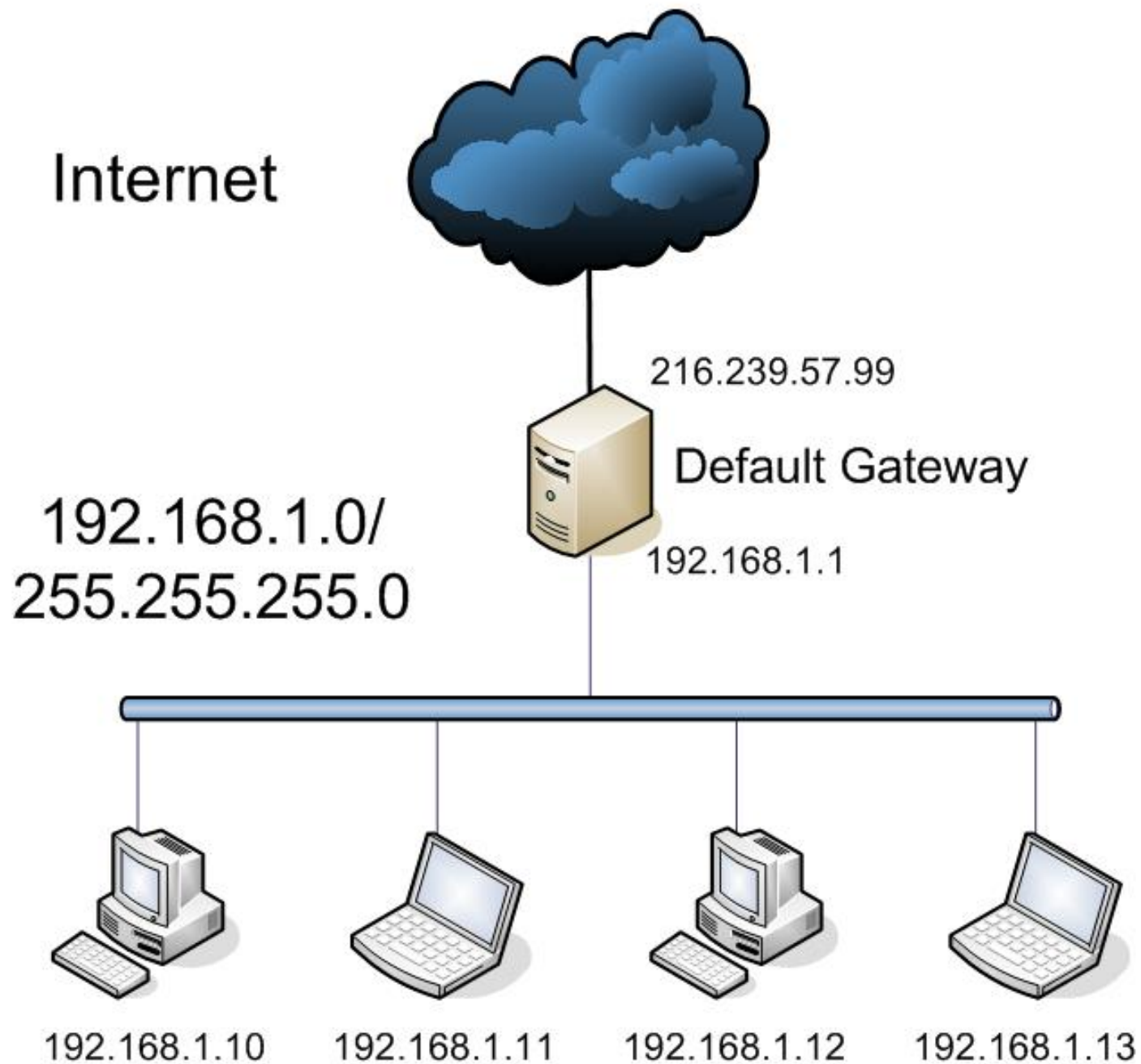
Network	Netmask	Gateway
192.168.1.0	255.255.255.0	-
192.168.2.0	255.255.255.0	192.168.1.1

192.168.2.10

Network	Netmask	Gateway
192.168.1.0	255.255.255.0	192.168.2.1
192.168.2.0	255.255.255.0	-

192.168.1.1 bzw. 192.168.2.1

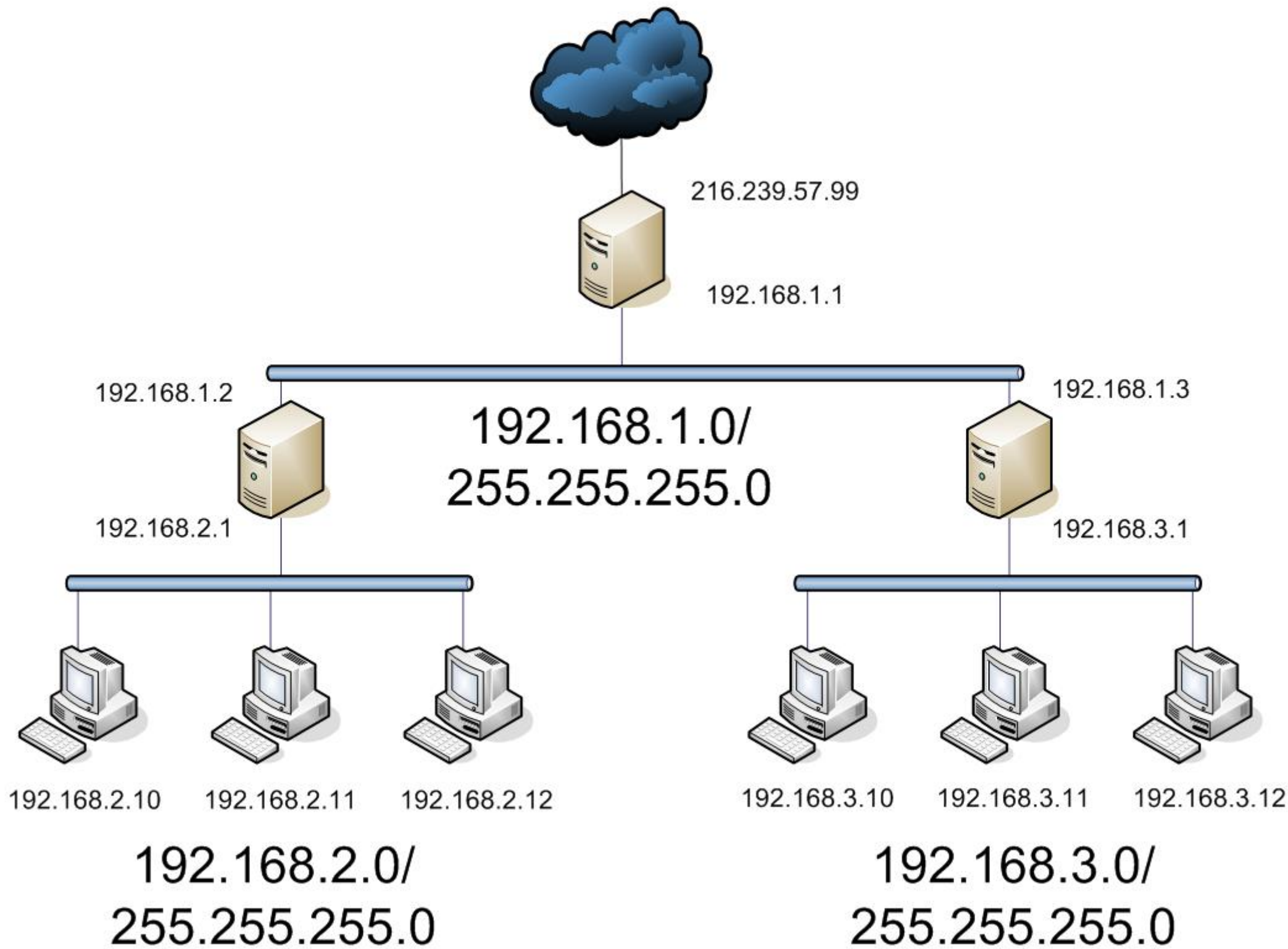
Network	Netmask	Gateway
192.168.1.0	255.255.255.0	-
192.168.2.0	255.255.255.0	-



Default Gateway

192.168.1.10

Network	Netmask	Gateway
192.168.1.0	255.255.255.0	-
0.0.0.0	0.0.0.0	192.168.1.1



192.168.1.1

Network	Netmask	Gateway
192.168.1.0	255.255.255.0	-
192.168.2.0	255.255.255.0	192.168.1.2
192.168.3.0	255.255.255.0	192.168.1.3

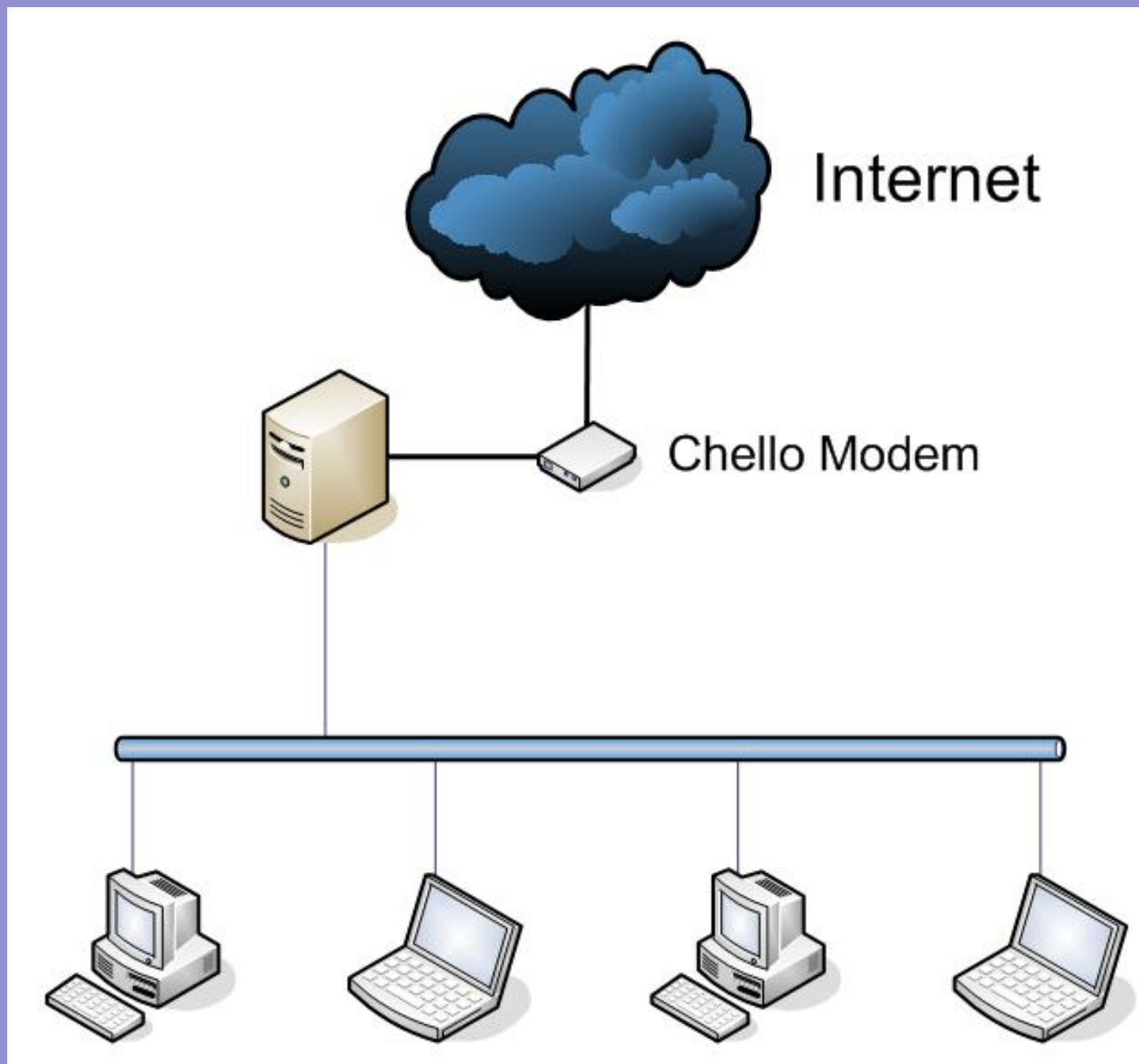
192.168.1.2 bzw. 192.168.2.1

Network	Netmask	Gateway
192.168.1.0	255.255.255.0	-
192.168.2.0	255.255.255.0	-
192.168.3.0	255.255.255.0	192.168.1.3
0.0.0.0	0.0.0.0	192.168.1.1

192.168.3.10

Network	Netmask	Gateway
192.168.3.0	255.255.255.0	-
0.0.0.0	0.0.0.0	192.168.3.1

Komplexe Routing Tables



IPs, Netmasks & Routing für ein Chello-Netzwerk

Exkurs: DHCP

Dynamic Host Configuration Protocol

IP Adresse, Netmask & Gateway-Einträge werden bei jedem Neustart eines Clients (bzw. nach einer best. Zeit) dynamisch von einer zentralen Autorität (DHCP-Server) zugewiesen.

Vorteile

- zentrale Administration
- dadurch Kostenersparnis

Nachteile

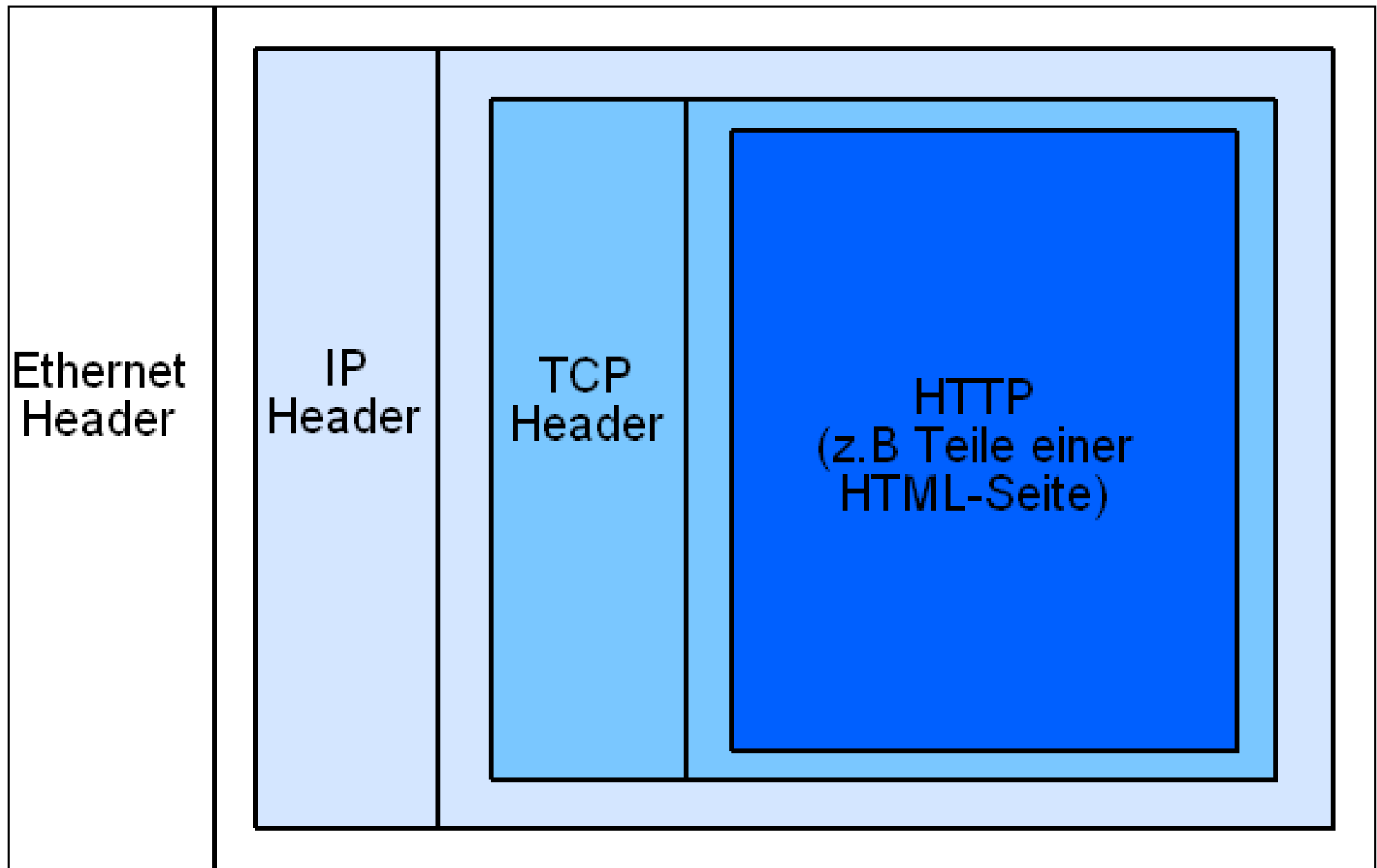
- Clients haben nicht immer die selbe IP Adresse
- Fällt der DHCP-Server aus, ist das ganze Netzwerk „down“

Fragmentierung von IP Paketen

Daten werden als Pakete (packets od. datagrams) verschickt

Ein IP Packet enthält (unter anderem) folgende Felder:

- Version: IPv4 od. IPv6
- Type-Of-Service (TOS): ob z.B. maximaler Datendurchsatz f. großen Download od. kurze Reaktionszeit f. interaktive Anwendungen
- Fragmentation: sogleich
- Time-To-Live (TTL): TTL-Zähler wird bei jedem Router um 1 herabgesetzt; erreicht er 0 wird eine Fehlermeldung zurück gesendet. Verhindert Endlos-Schleifen
- Protocol: Welches Protokoll (TCP,UDP,ICMP) in diesem Packet transportiert wird.
- Source IP Adress: IP Adresse des Absenders
- Destination IP Address: IP Adresse des Empfängers
- Data: die eigentlichen Daten; z.B. TCP-Header und TCP-Daten



Aufbau eines IP Packet

Physikalische Netzwerkebene kennt Grenzen f. die Größe eines Paketes – sog. Maximum Transfer Unit (MTU).

Die MTU beträgt bei Ethernet 1500 Bytes.

Pakete größer als 1,5 kB werden „zerstückelt“ (fragmentiert) und müssen beim Empfänger wieder zusammen gesetzt werden.

Geht ein Fragment verloren, muss das ganze Paket noch ein Mal angefordert werden.

Ethereal

URL: <http://www.ethereal.com/>

OS: Windows/Linux/Mac OS X/OpenBSD/Unix ...

Erlaubt das Lesen des ein- und ausgehenden Netzwerk-Traffics.

Ein Tool zum Lesen des Netzwerk-Traffics („sniffing“)