Networking - Überblick

Netzwerkgrundlagen

René Pfeiffer
Systemadministrator GNU/Linux Manages!
lynx@luchs.at
rene.pfeiffer@paradigma.net

Was uns erwartet...

- Hardware (Ethernet, Wireless LAN)
- Internetprotokolle (IP, Routing)
- Transportprotokolle (TCP, UDP, ICMP)
- Applikationsprotokolle (DNS, SMTP, FTP, HTTPS, HTTPS, SSH)
- IT-Sicherheit
- Komplexe Netzwerkkomponenten (Firewall, Proxy)
- VPN (Virtual Private Networks)
- WLAN (Wireless LAN)
- Kryptographie
- Serverarchitekturen
- Freie Software als Toolbox

Wo man mehr findet...

- TCP/IP Networking, O’Reilly
- Linux Network Administrator’s Guide, O’Reilly
- SSH, the Secure Shell: The Definitive Guide, O’Reilly
- DNS and BIND, O’Reilly
- The Linux Documentation Project (http://www.tldp.org/)

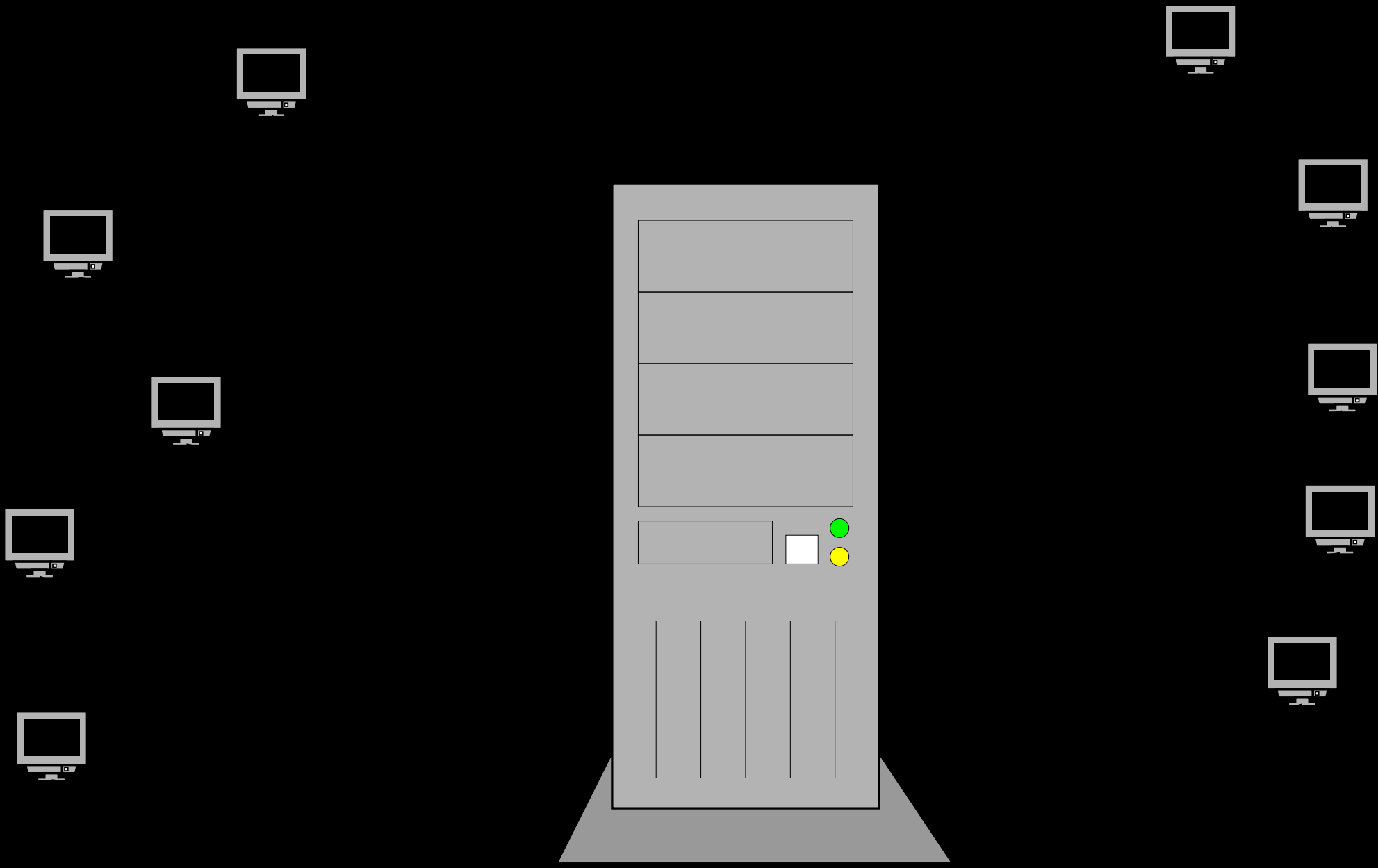
Was ist "Networking"?

Geschichte des Networking

erste mechanische Rechenmaschinen im 17. Jhrd.
Knacken von Codes durch Computer im 2. Weltkrieg
Vernetzung durch Kalten Krieg in den 60er Jahren

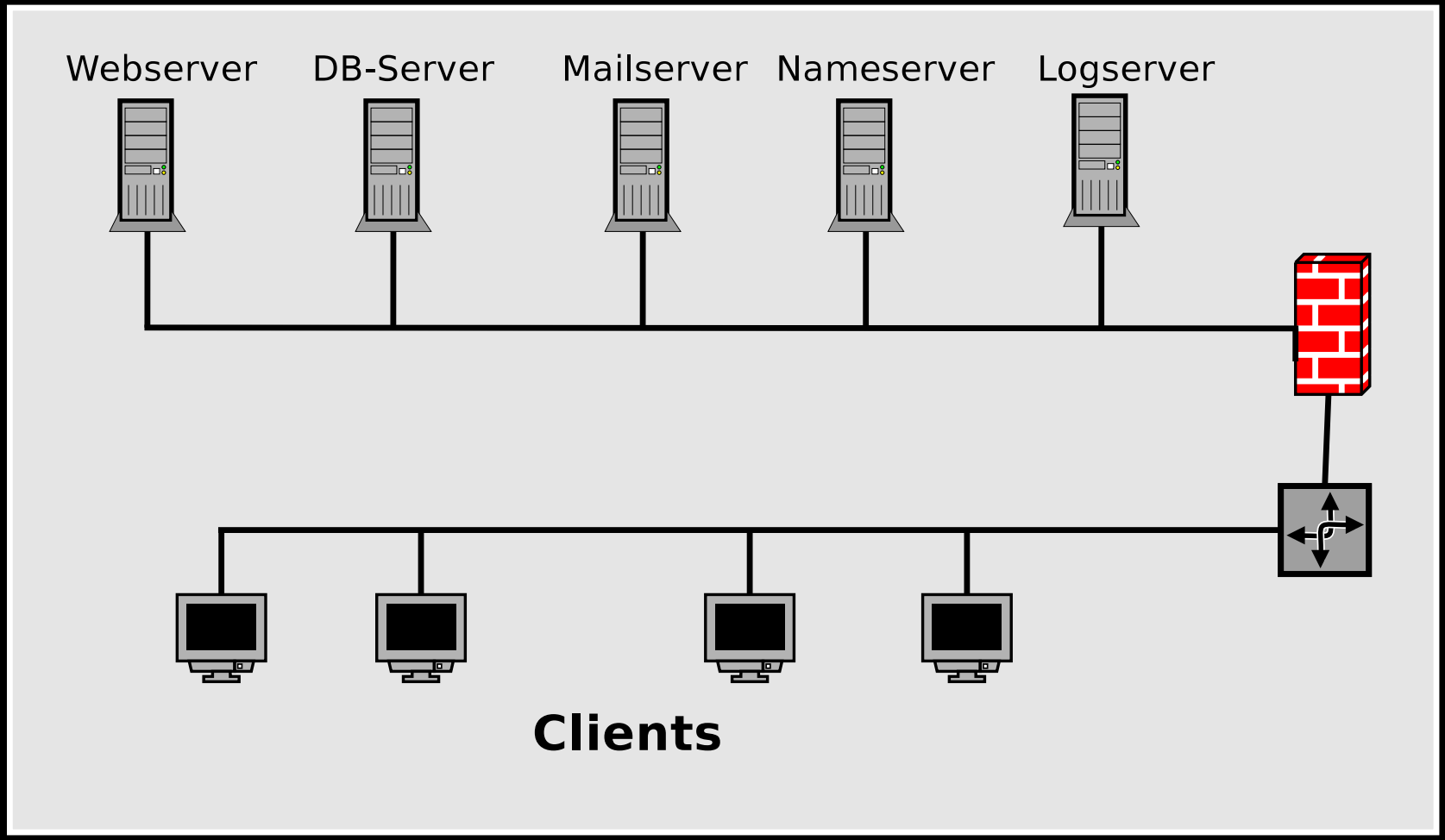
Anfänge: Zentrale Struktur

Mainframes stehen im Mittelpunkt



Dezentrale Struktur von Netzwerken

Viele Server, viele Clients



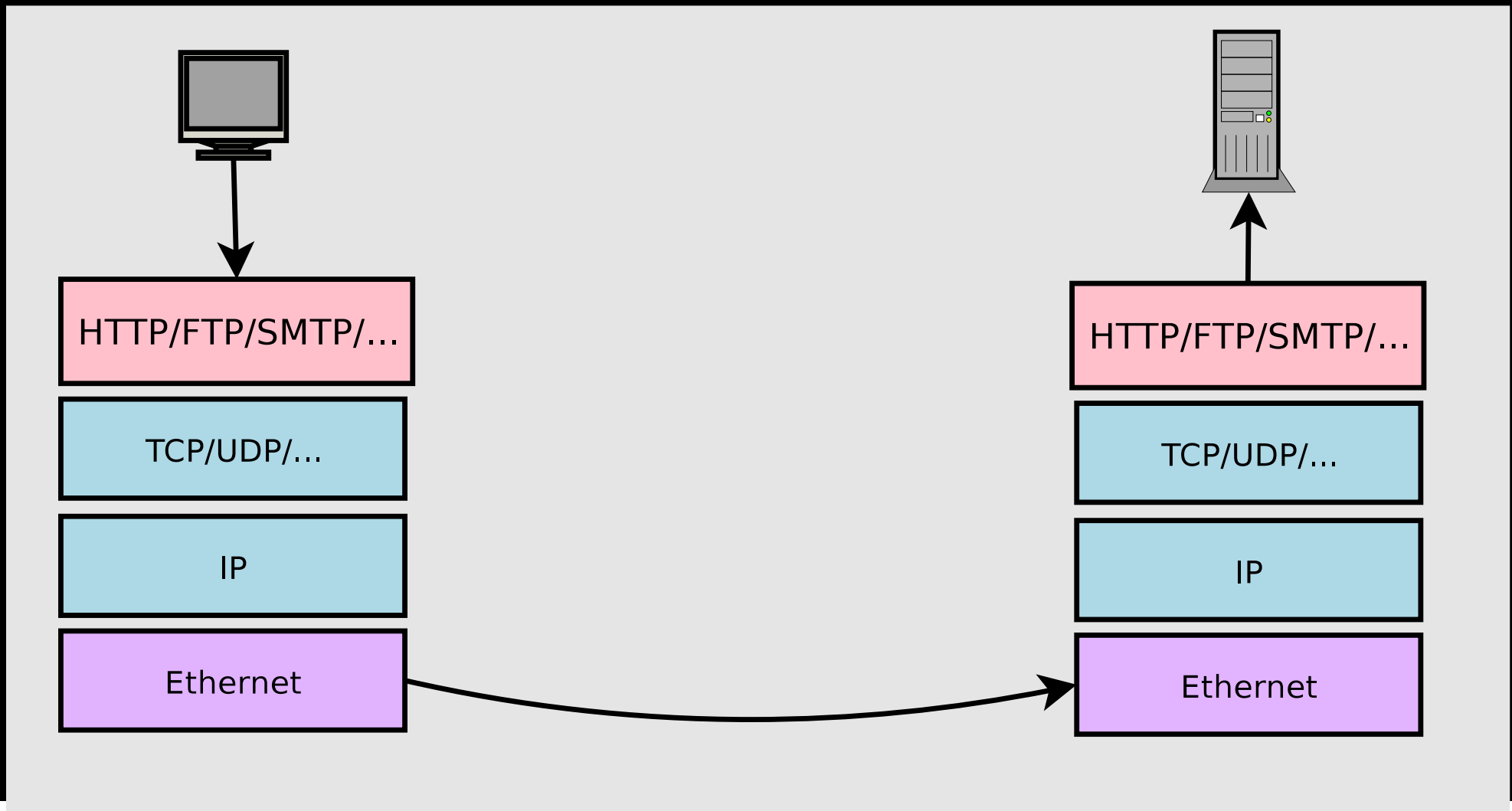
Clients sind vollwertige Computer
verteilte Rollen

Grundbegriffe

- Server - bietet einen Dienst im Netzwerk an
- Client - benutzt einen Dienst in einem Netzwerk
- Host - üblicherweise ein Server
- Internet - ein weltweites, auf TCP/IP basierendes Netzwerk
- LAN - Local Area Network, lokales Netz, auch Intranet
- WAN - Wide Area Network
- WLAN - Wireless Local Area Network, auch WiFi (Wireless Fidelity)
- Extranet - Verbindung mehrerer LANs via Internet

Netzwerkschichten

- 7 Schichten nach dem OSI Referenzmodell
  - OSI = Open System Interconnection
- 4 Schichten in der Internet-Protokollfamilie



Erste Netzwerkschicht (Ethernet)

Netzwerk direkt an der Hardware

Diese Schicht kennt die Hardware.

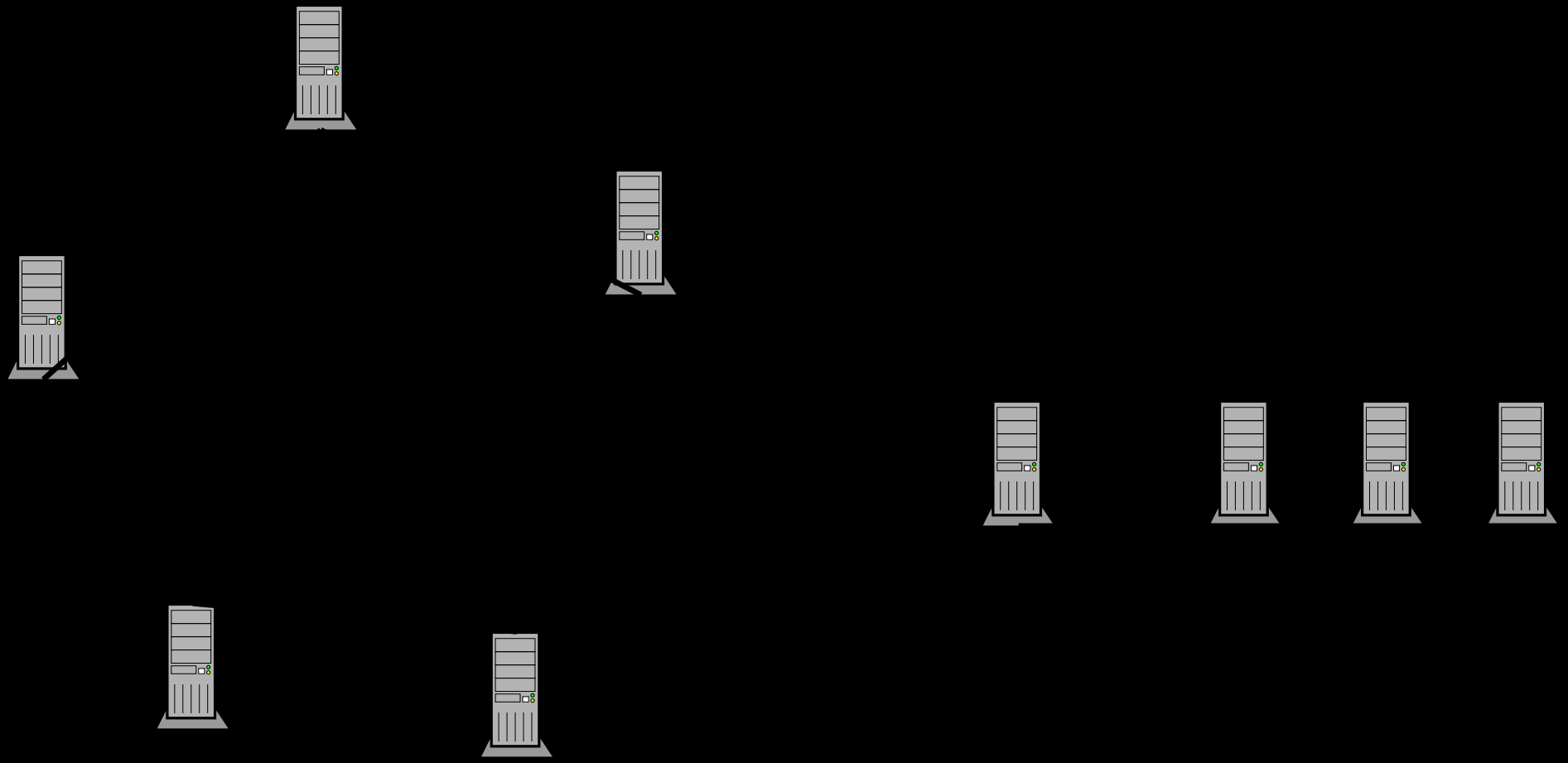
Ethernet transportiert Daten zwischen Rechnern auf demselben Segment.

Netzwerkhardware

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

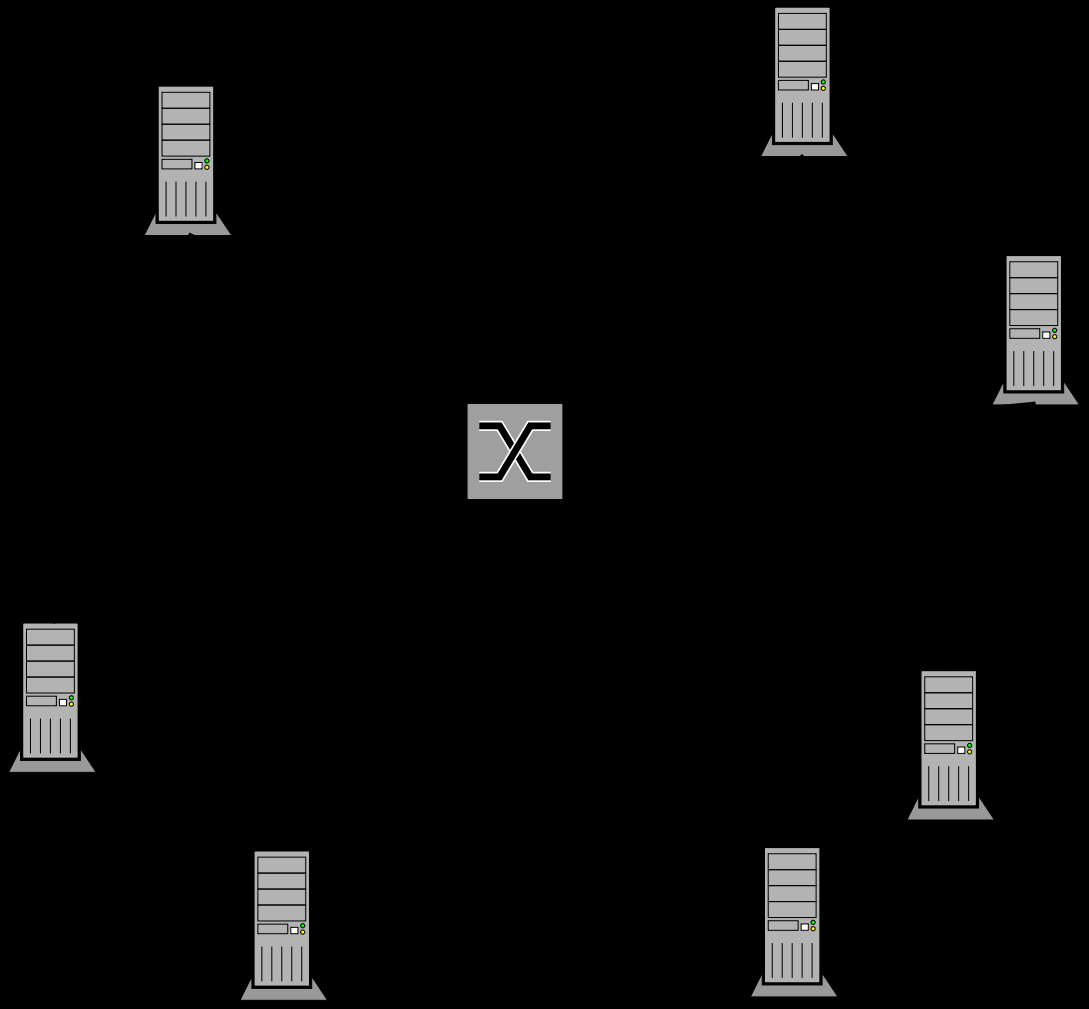
Netzwerkkarte mit RJ45- und BNC-Anschluß

Thin Ethernet (BNC- oder Koaxialverkabelung)



Ring- oder Bustopologie
10 Mbit/s

Twisted Pair Ethernet (RF45- oder Patchverkabelung)



Sterntopologie
10, 100 Mbit/s
1, 10 Gbit/s

Hub oder Switch

- Hub
  - sendet Daten an alle Ports
  - NICs können gleichzeitig reden (Kollision)
- Switch
  - sendet Daten nur an Port, die kommunizieren
  - keine Kollisionen von Übertragungen

Direktverkabelung zweier Maschinen

- Direktverbindung über Crossover-Kabel
- Verkabelung über Hub/Switch

Ethernetadressen

Rechner sind im Ethernet eindeutig identifiziert

Jede Karte hat eine eindeutige MAC (Media Access Control) Adresse

Eine MAC-Adresse besteht aus 6 Teilen:
00:60:97:11:d9:02
.

Address Resolution Protocol (ARP)

Kopplung zwischen MAC- und IP-Adresse

Zur Ermittlung einer IP-Adresse schickt ein Rechner ein Paket mit einer Anfrage an alle Rechner im Netz.

Der Rechner mit der zugehörigen IP-Adresse antwortet und teilt seine MAC-Adresse mit.

Erst dann beginnt die Übermittlung des IP-Pakets.

Internet Protokoll (IP; IPv4 & IPv6)

Die zweite Netzwerkschicht

Durch die zweite Netzwerkschicht erfolgt eine Trennung zwischen logischen und physikalischen Adressen.

Damit ergeben sich Möglichkeiten

- zum logischen Gruppieren
- zum Leiten von Netzwerkverkehr

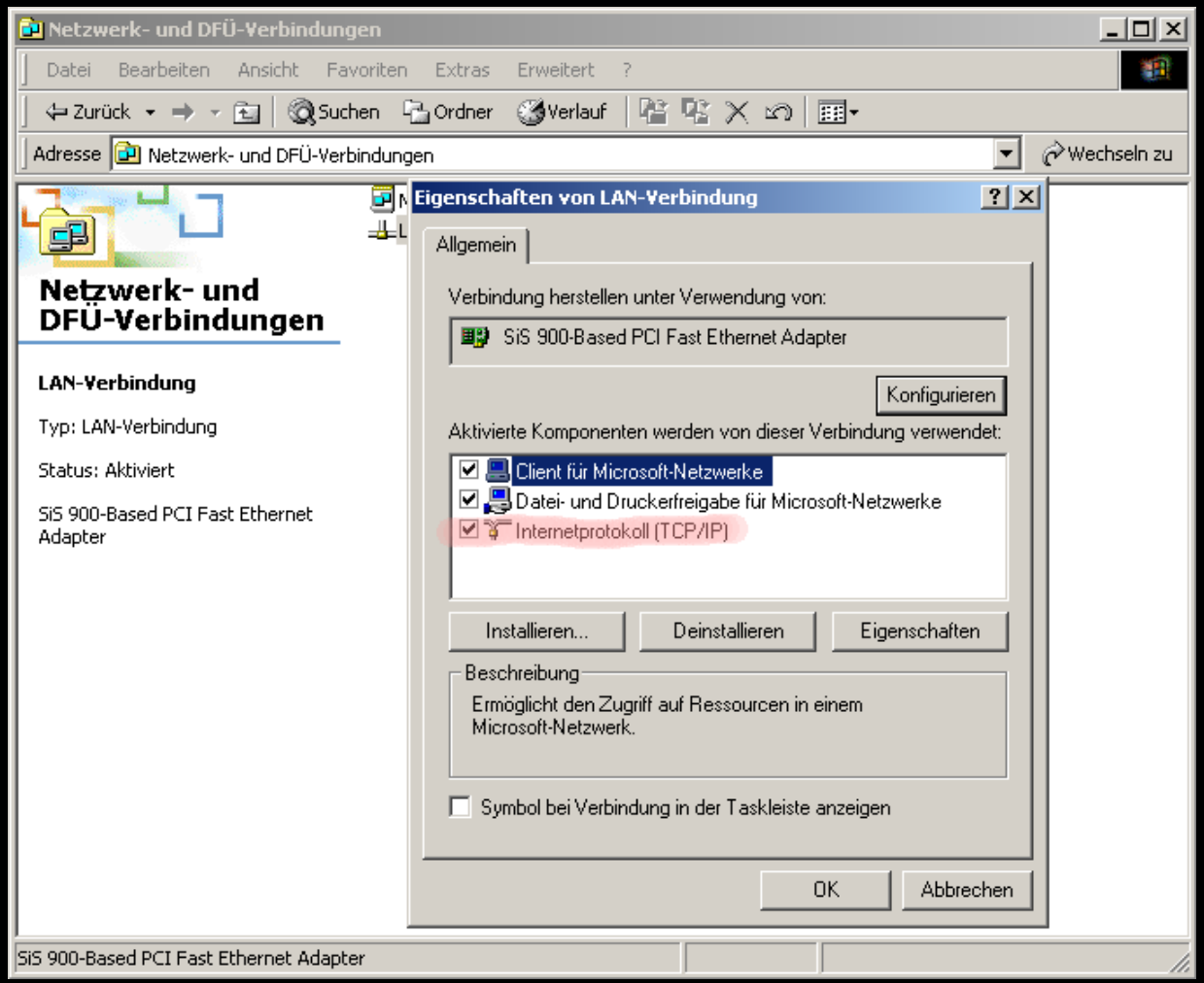
IP-Adressen im IPv4

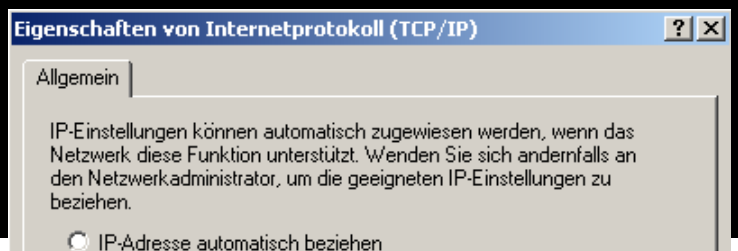
IP-Adressen bestehen aus 4 Zahlen, jede zwischen 0 und 255
Beispiele für IP-Adressen:
192.168.15.242
212.58.240.130
10.1.2.3
.

Welche sind gültige IPv4 Adressen?

1921.168.2.23
C.98.A.98
-45.23.23.23
48.243.567.324
192.168.1.0
83.23.51.255

Wie kann ich auf meinem Rechner eine IP-Adresse einstellen?





Private und öffentliche IP-Adressen

Die folgenden Adreßbereiche sind für privaten Gebrauch:
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
Darüber hinaus gibt es noch Adreßbereiche für spezielle Anwendungen.
Alle anderen IP-Adressen sind öffentlich erreichbar.

Das Loopback Interface (Localhost)

Die Adresse
127.0.0.1
ist immer die Adresse des eigenen Rechners, auch ohne Netzwerkkarte oder Netzanschluß.

Damit kann ein Rechner immer mit sich selbst Verbindung aufnehmen.

- Wichtig für Debug-Zwecke
- Wichtig für Datentransport auf derselben Maschine

IP-Adressen mathematisch

Eine IP-Adresse besteht aus 32 Bit.
32 Bit entsprechen 4 Octets zu je 8 Bit.

Binär schaut eine IP-Adresse so aus:
00100101 11001010 11111111 11101101

Jedes Octet hat 2^8 = 256 Möglichkeiten.
Daher hat eine IP-Adresse pro Octet 0-255.

Insgesamt ergeben sich als theoretisches Limit für IPv4
2^32 = 4.294.967.296
mögliche IP-Adressen.

IPv6-Adressen mathematisch

IPv6-Adressen bestehen aus 128 Bit statt aus 32 Bit.

Damit ergeben sich

2^128 = 340.282.366.920.938.463.463.374.607.431.768.211.456

mögliche IP-Adressen.

IP Routing

Wie erreicht ein Datenpaket sein Ziel?

Wie weiß ein Rechner wie eine andere IP-Adresse zu erreichen ist?

Analogie zum Brief

Adressen werden in einer bestimmten Reihenfolge gelesen.

Austria
Vienna
1060
Linke Wienzeile
130A

Die Reihenfolge führt von Postamt zu Postamt.
Bei IP führt der Weg von Gateway zu Gateway.

Aufbau von IP Netzwerken

IP Netzwerke fassen mehrere Rechner bzw. Systeme zusammen.

```
Netzwerk   10.  0.  0.  0  192.168. 15.  0  192.168. 15.  0
Netzmaske 255.  0.  0.  0  255.255.  0.  0  255.255.255.  0
Broadcast  10.255.255.255  192.168.255.255  192.168. 15.255
```

Zwei der drei Parameter charakterisieren ein Netzwerk, der dritte kann aus den beiden anderen bestimmt werden.

Netzmasken schreibt man alternativ als Zahl der Einsen im 32-Bit Wert:
192.168.15.0/255.255.255.0 == 192.168.15.0/24

.

IP Netzwerke

In welchem Netzwerk befindet sich die angeführte Adresse?

IP-Adresse 192.168.2.72
Netzmaske 255.0.0.0
Netzwerk 192.0.0.0

IP-Adresse 192.168.2.72
Netzmaske 255.255.0.0
Netzwerk 192.168.0.0

IP-Adresse 192.168.2.72
Netzmaske 255.255.255.0
Netzwerk 192.168.2.0

IP Netzwerke

Wie kann eine Netzmaske lauten, in dem sich die IP-Adressen 10.6.32.23 und 10.6.198.42 befinden?

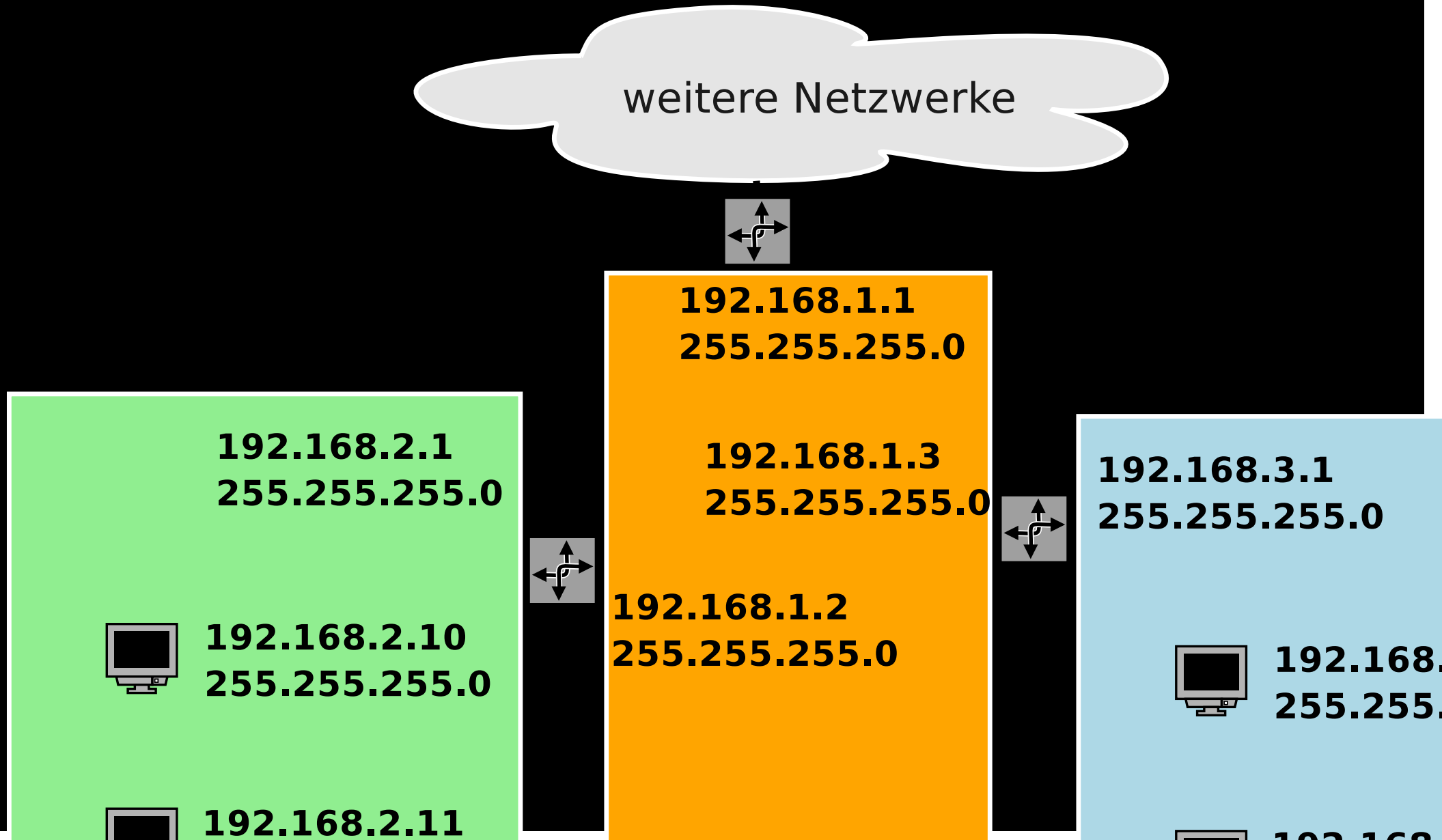
a) 2134.255.255.255
b) 255.0.0.0
c) 255.0.255.255
d) 256.255A.0.0
e) 255.255.255.255
f) 255.255.0.0

b) und f) sind richtig.

.

IP-Routing - Gateways

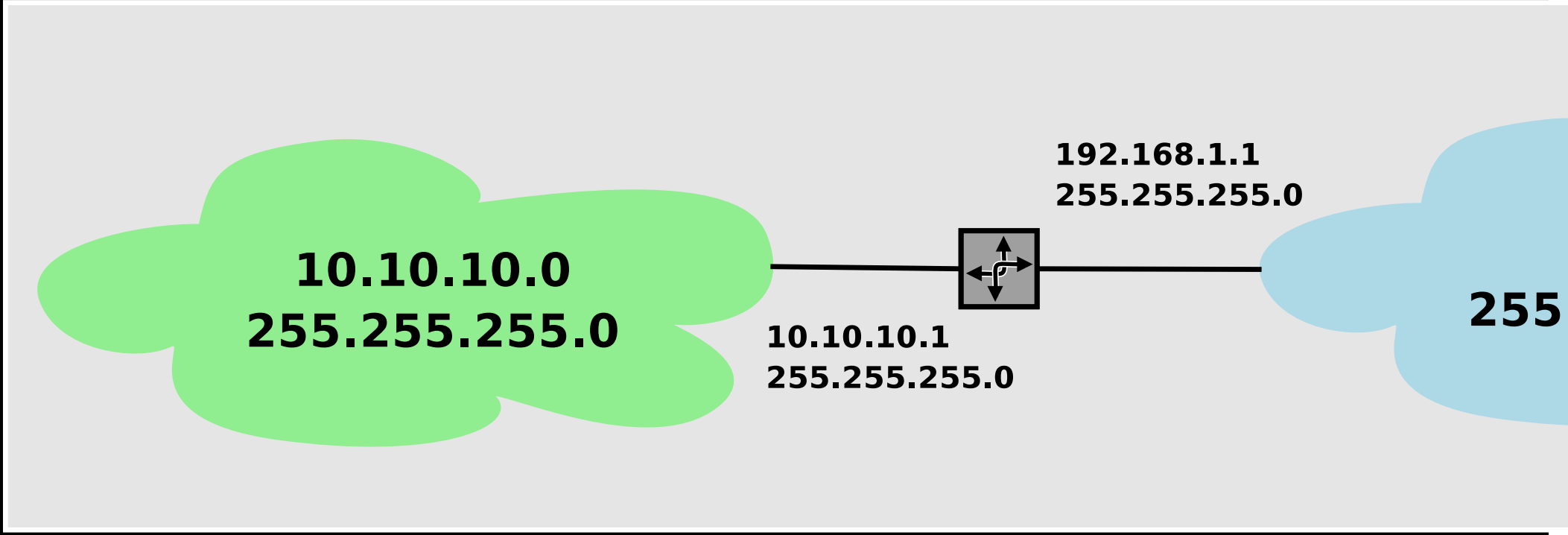
Ein Gateway verbindet Netze und ist daher immer mit mindestens zwei Netzwerken verbunden.



Zwei Netzwerke ohne Gateway

Rechner aus beiden Netzwerken sehen sich nicht gegenseitig

Zwei Netzwerke mit Gateway



Rechner aus beiden Netzwerken können jetzt über den Gateway Verbindung aufnehmen

.

Routing Tables

Laptop
PC
Gateway
FIXME!

Default Gateway

Routing Table mit Default Gateway

ip route

```
10.1.1.2 dev sl0  proto kernel  scope link  src 10.1.1.1
192.168.15.0/24 dev eth0  proto kernel  scope link  src 192.168.15.242
127.0.0.0/8 dev lo  scope link
default via 192.168.15.1 dev eth0
```

route

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.1.1.2        0.0.0.0         255.255.255.255 UH    0      0        0 sl0
192.168.15.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.15.1    0.0.0.0         UG    0      0        0 eth0
```

Dynamic Host Configuration Protocol (DHCP)

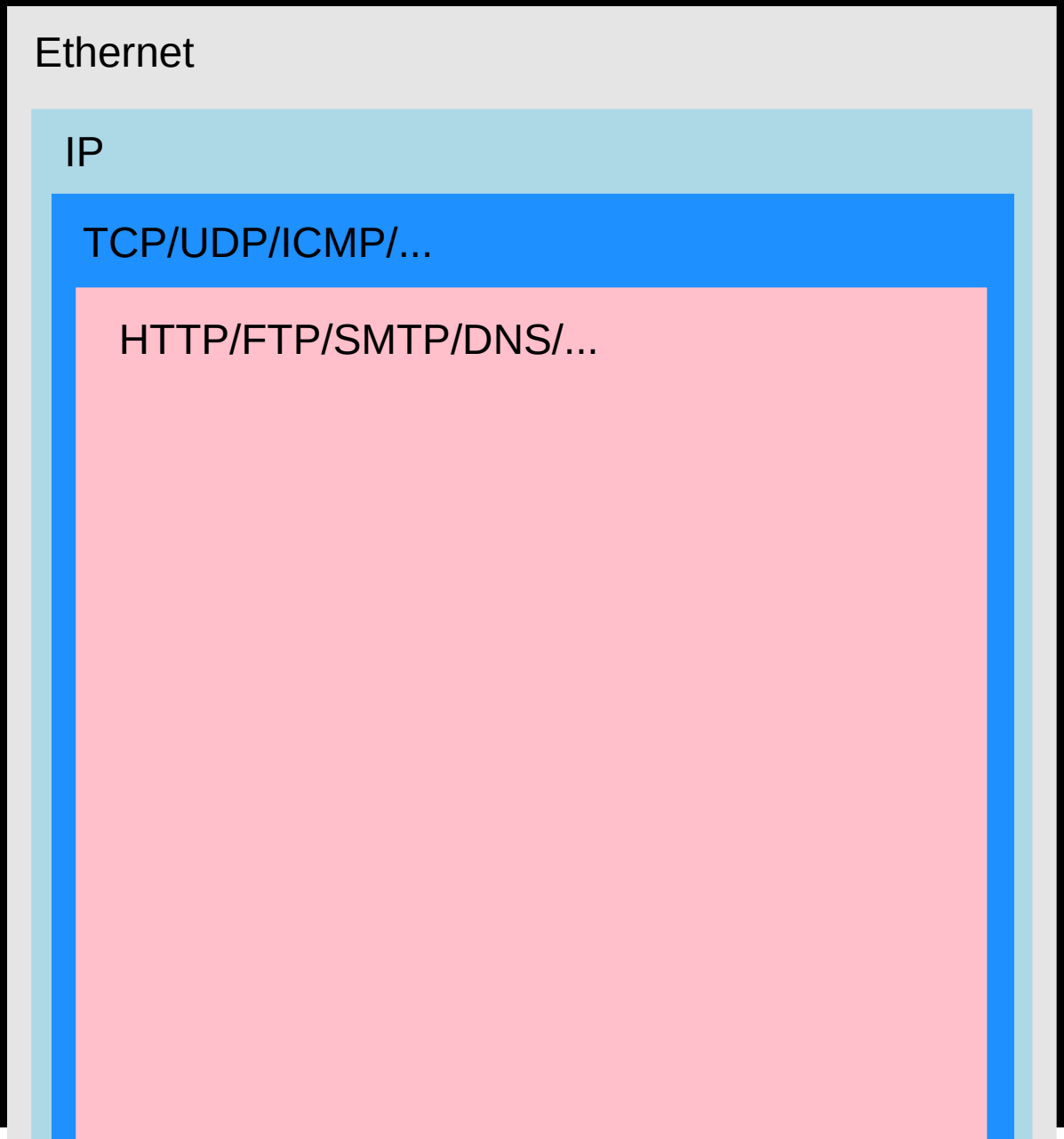
Automagische Konfiguration von TCP/IP Einstellungen

- IP Adresse, Netmask & Gateway-Einträge werden bei jedem Neustart eines Clients vergeben
- Konfiguration ist zeitlich begrenzt und muß periodisch wieder erfragt werden
- zentrales Administrieren der Einstellungen
- keine Kollisionen von IP-Adressen

- bei Ausfall des DHCP Servers keine Konfiguration möglich

IP-Pakete

IP-Pakete setzen auf Ethernetpaketen auf



Aufbau eines IP-Pakets

Auszug aus den Kopfdaten (Header)

- Quell- und Ziel-IP-Adresse
- Version (IPv4 oder IPv6)
- Type of Service (ToS)
  - maximaler Datendurchsatz
  - schnellster Weg
  - höchste Verläßlichkeit
- IP Fragmentinformationen
- Lebensdauer, Time To Live (TTL)
  - 0 bis 255
  - verhindert endlosen Transport der Pakete in Schleifen
- Protokoll (TCP, UDP, ICMP, ...)
- Checksummen von Kopfdaten und Daten

Nach den Kopfdaten folgen die eigentlichen Daten.

Fragmentierung von IP-Paketen

- Maximum Transfer Unit (MTU) für Ethernet ist 1500 Byte
- maximale Größe eines IP-Paketes ist 65536 Byte

Größere Pakete werden zerteilt (fragmentiert), nummeriert und am Ziel wieder zusammengesetzt.

Geht ein Fragment verloren, so werden alle Teile nochmal angefordert.

IP für Neugierige - Ethereal

Pädagogisch wertvolles Sniffen

- Ethereal (http://www.ethereal.com/) ist ein Sniffer
  - GNU/Linux, *BSD
  - Mac OS X
  - MS Windows
- erlaubt das Lesen ein- und ausgehenden Netzwerkverkehrs
- stellt Pakete graphisch dar
- kann statistische Auswertungen durchführen

Vielen Dank für die Aufmerksamkeit!

Für Fragen und Antworten stehe ich jederzeit zur Verfügung.

René Pfeiffer

lynx@luchs.at
lynx@enemy.org
rene.pfeiffer@paradigma.net

http://web.luchs.at/