

Open Source Teil 2

Lukas Feiler

lukas.feiler@lukasfeiler.com

<http://www.lukasfeiler.com>

NFS-Server

NFS - Networking File System

Die Geschichte des NFS.

Von NFS Version 2 bis NFS Version 4

Technischer Grundlagen von NFS

- UDP auf der Transportschicht
- NFS als zustandsloses Protokoll: File Handles
- Bildung eines Trust-Relationships zwischen NFS-Client u. Server

Installation eines NFS-Servers unter SUSE Linux 10

über YAST sind zu installieren:

- nfs-utils
- nfsidmap
- yast2-nfs-client & yast2-nfs-server

Konfiguration des NFS-Servers

YAST: Network Services → NFS Server

Konfiguration des NFS-Clients

YAST: Network Services → NFS Client

empfohlene Mount-Optionen: "ro,nosuid,nodev,noexec"

NTP-Daemon

NTP - Network Time Protocol

Notwendigkeit und Genauigkeit von NTP

- Log Files
- Last-Modified Dates
- E-Mail
- Verschlüsselung
- Stratum 1 bis Stratum X

Installation eines NTP-Daemons (NTP-Client)

über YAST ist zu installieren: `xntp`

Konfiguration des NTP-Daemons

über YAST: Network Services → NTP Client

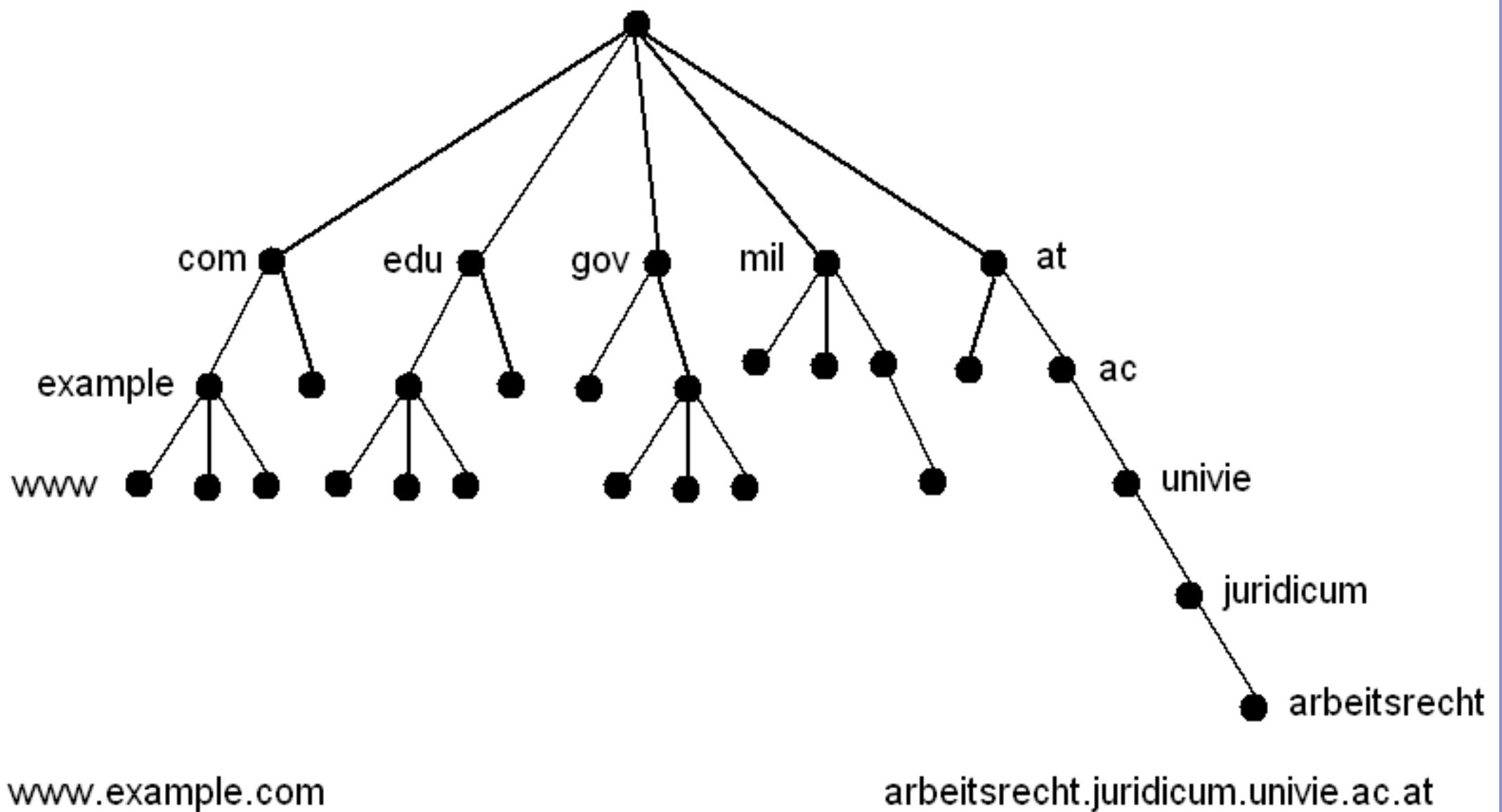
DNS – Domain Name System

Computer „denken“ am liebsten in Zahlen – Menschen nicht!

Geschichte des DNS

Vom ARPAnet zum Internet

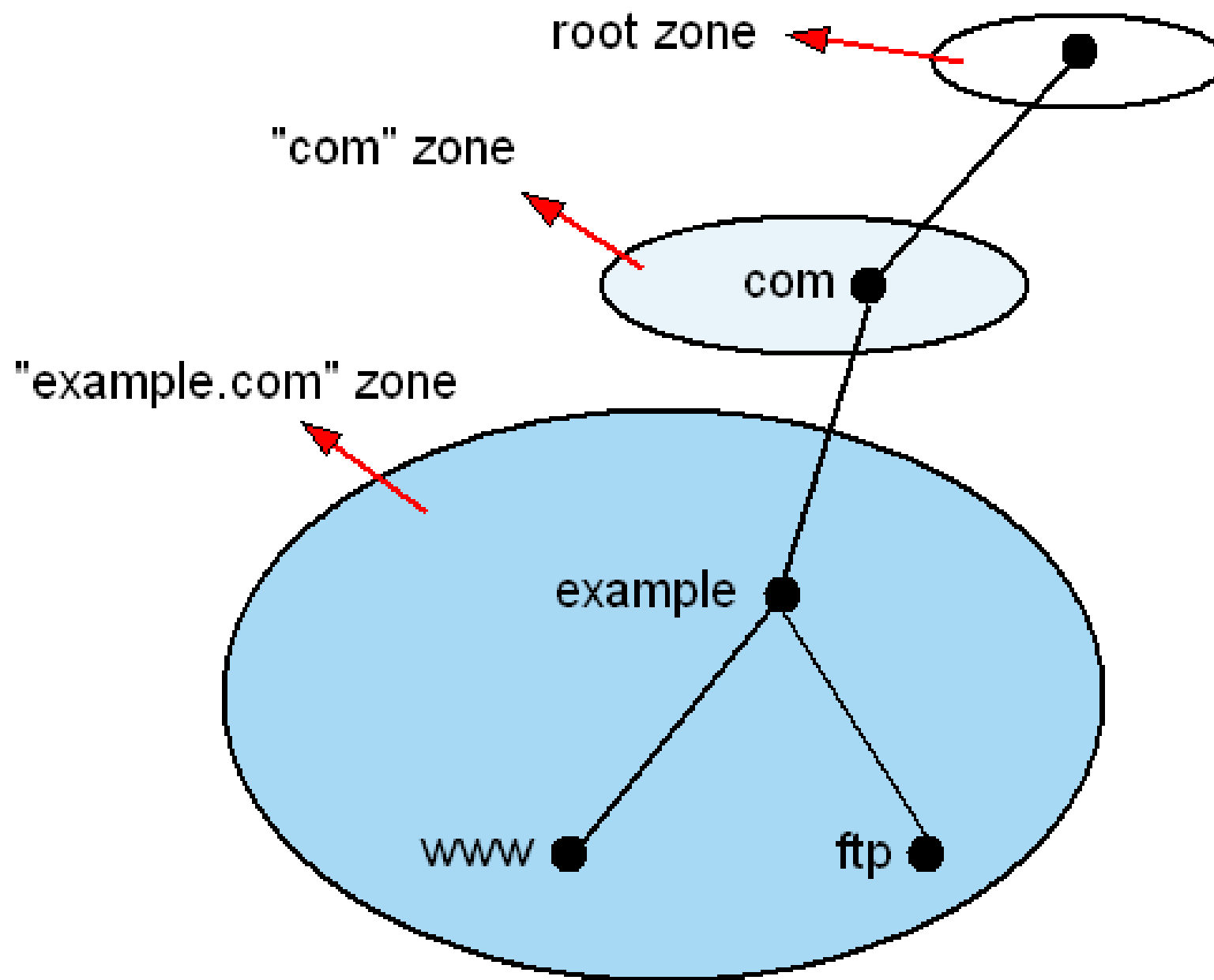
Heute: dezentrale Verwaltung durch unzählige Name-Server



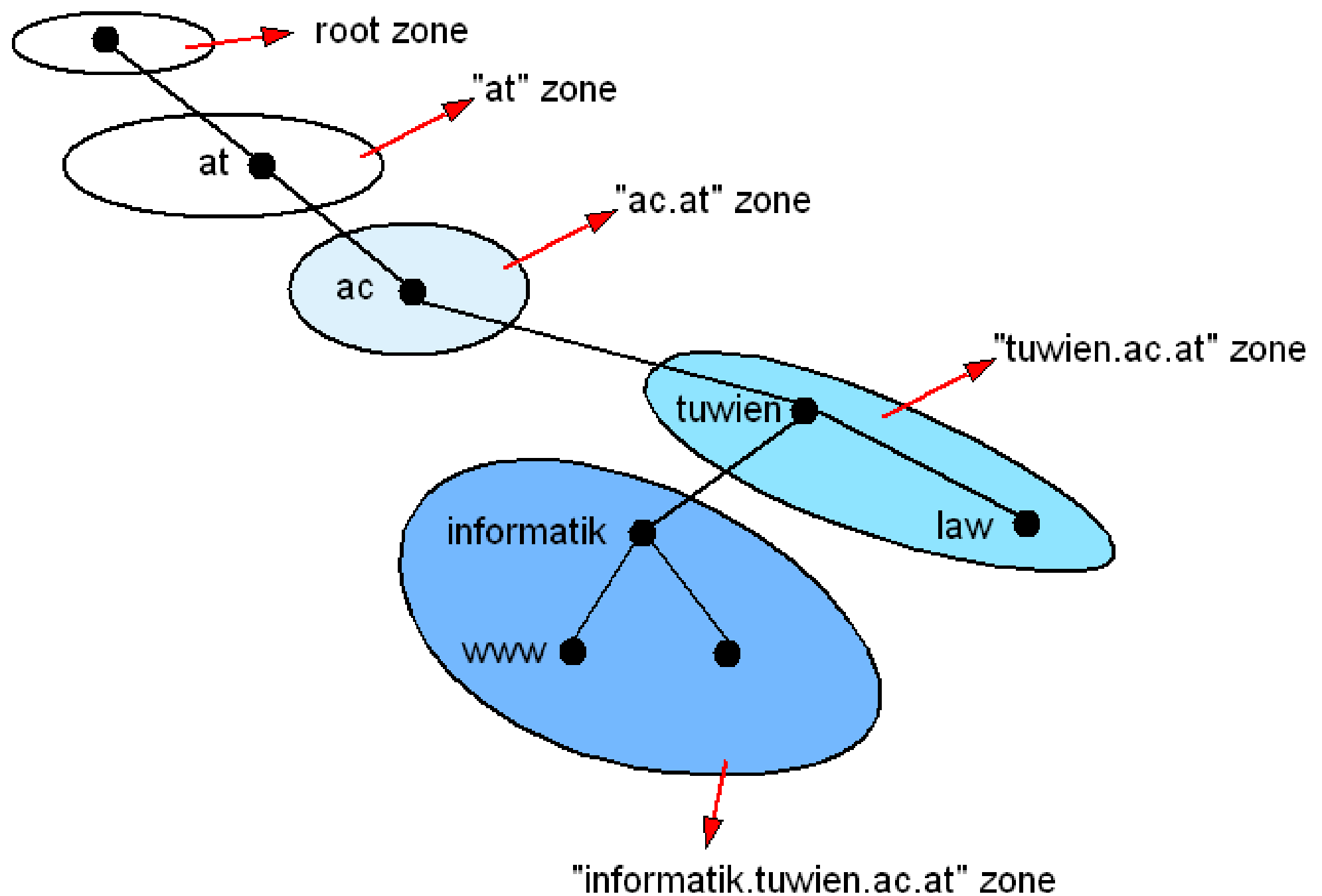
Der Domain Name Space

DNS: Dezentrale Verwaltung durch Delegation

Ein Name-Server hat nur für seine Zones „Autorität“



Die Zone „com“ hat nur einen Verweis auf die Zone „example.com“



Zones: „root“, at, ac.at, tuwien.ac.at, informatik.tuwien.ac.at

Installation des DNS-Servers BIND

über YAST sind zu installieren:

- bind
- bind-chrootenv

Konfiguration von BIND

in YAST:

#1 Network Sevices → DNS and Hostname

#2 Network Services → DNS Server

testweise anzulegen: eine neue Zone mit NS, MX & A-Records

Das command line tool nslookup

Parameter: Domain-Name, der in IP aufgelöst werden soll

z.B: nslookup mail.home.lukasfeiler.com

„Händisch“ einen Domain-Name in eine IP-Adresse auflösen

E-Mail (SMTP, POP3)

Eine der ältesten aber auch wirtschaftlich wichtigsten Anwendungen des Internets.

Envelope	Header	Body
MAIL FROM: != From Header RCPT TO: != To Header	Subject Betreff From Absender (user@host.tld) To Empfänger (user@host.tld) Cc Carbon Copy Bcc Blind carbon copy	Inhalt der Nachricht Seit MIME (Multi-purpose Internet Mail Extension) in beliebigem Format

Woraus besteht ein E-Mail?

SMTP-Server
mail.unet.univie.ac.at



SMTP-Server
mail.empoweredmedia.com



POP3-Server
mail.empoweredmedia.com

From: a0201227@unet.univie.ac.at
To: lukas@empoweredmedia.com



Outlook/Thunderbird/...
als SMTP-Client



Outlook/Thunderbird/...
als POP3-Client

Der typische Weg eines E-Mails (simplifiziert)

Woher weiß mail.unet.univie.ac.at welcher Server für lukas@empoweredmedia.com zuständig ist?

Mittels DNS kann für jede Domain ein Mail-Server definiert werden
z.B: für empoweredmedia.com: mail.empoweredmedia.com

mit nslookup:

```
nslookup -type=MX empoweredmedia.com
```


Installation des SMTP-Servers Postfix & des POP3-Servers qpopper

über YAST sind zu installieren:

- (postfix; ist in der Standard-Installation enthalten)
- qpopper

Konfiguration von Postfix

in YAST: Network Sevices → Mail Transfer Agent

Konfiguration von qpopper

in YAST: Network Sevices → Network Services (xinitd)

Hinzufügen neuer Mail-Accounts mittels YAST

in YAST: "Security and Users" → "User Management"

Spam-Abwehr: SpamAssassin & AMaViS

- Ermöglichen zusammen eine leichte Integration in Postfix.
- Erkennungsverfahren –u. Probleme von SpamAssassin

Installation v. SpamAssassin & AMaViS

über YAST sind zu installieren:

- amavis-new
- spamassassin
- perl-spamassassin

Konfiguration von SpamAssassin & AMaViS

- “spamd” aktivieren über YAST: System → System Services (Runlevel)
- AMaViS in Postfix einbinden: Network Services → Mail Transfer Agent

Virenschutz

- Das Problem
- Die Lösung: AntiVir, Clam AV, ...

Installation v. AntiVir

über YAST ist zu installieren: antivir
wird von AMaViS automatisch erkannt

IT-Sicherheit unter Linux

Aspekte der IT-Sicherheit

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Physische Angriffe

Hardware-Fehler

- Datenverlust durch Platten-Crash

- Downtime durch Netzteil

Hack

- Datendiebstahl

- Daten-Löschung

- Daten-Fälschung

Denial of Service (DoS) & DDoS

Trojaner

Würmer & Viren

Versehentliche Daten-Löschung

Sniffing

Social Engineering

Phishing

Welche Risiken gibt es für IT-Systeme?

Prinzipien im Bereich IT Security

- Least privilege
- Defense in depth
- Securing the weakest link
- Secure failure (Default Deny)
- Keep it simple
- Privacy (Need-To-Know)

Organisatorische Sicherheitsmaßnahmen

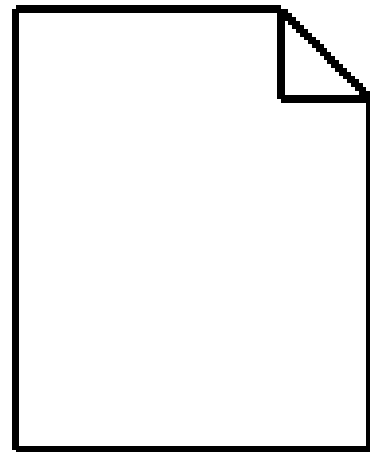
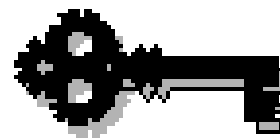
- Risk Assessment
- Security Policy
- Incident Response Plan, ...

Sonderproblem: Schwach Passwörter

Zugriffsrechte auf Dateiebene als
wesentliche Sicherheitsvorkehrung

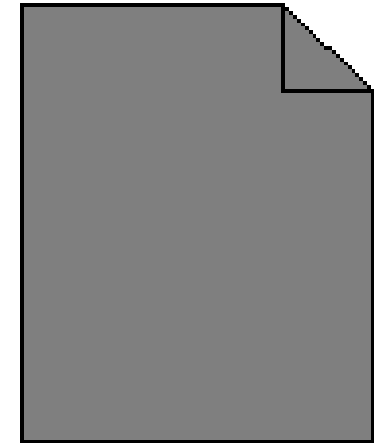
Verschlüsselung & Signatur mit GnuPG

GnuPG – GNU Privacy Guard: <http://www.gnupg.org>



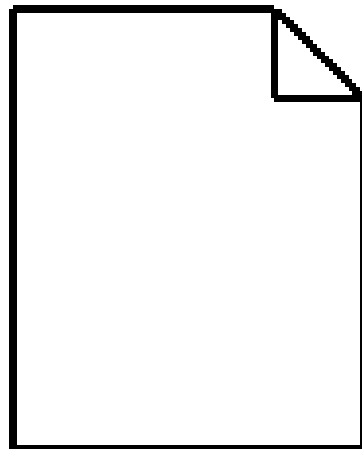
Plaintext

Verschlüsselung

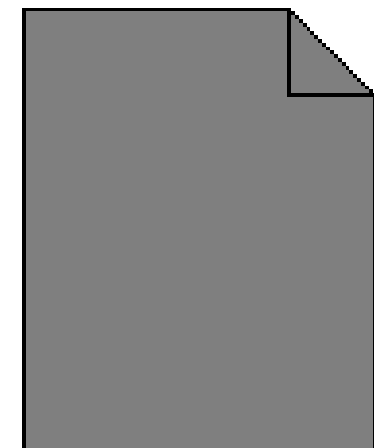


Ciphertext

Entschlüsselung



Plaintext



Ciphertext



Verschlüsselung & Entschlüsselung

Geschichte und Gegenwart der Kryptographie

- Kryptographie als Mittel zur Wahrung von Geschäftsgeheimnissen und zur Sicherung der Privatsphäre

Drei Arten von Verschlüsselungsverfahren

- symmetrische Verfahren
- asymmetrische Verfahren
- Message Digest Functions (One-way encryption)

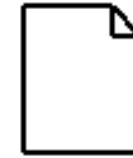
Symmetrische Verfahren

- selber Key für Ver -u. Entschlüsselung
- z.B. DES, Triple-DES, Blowfish, AES

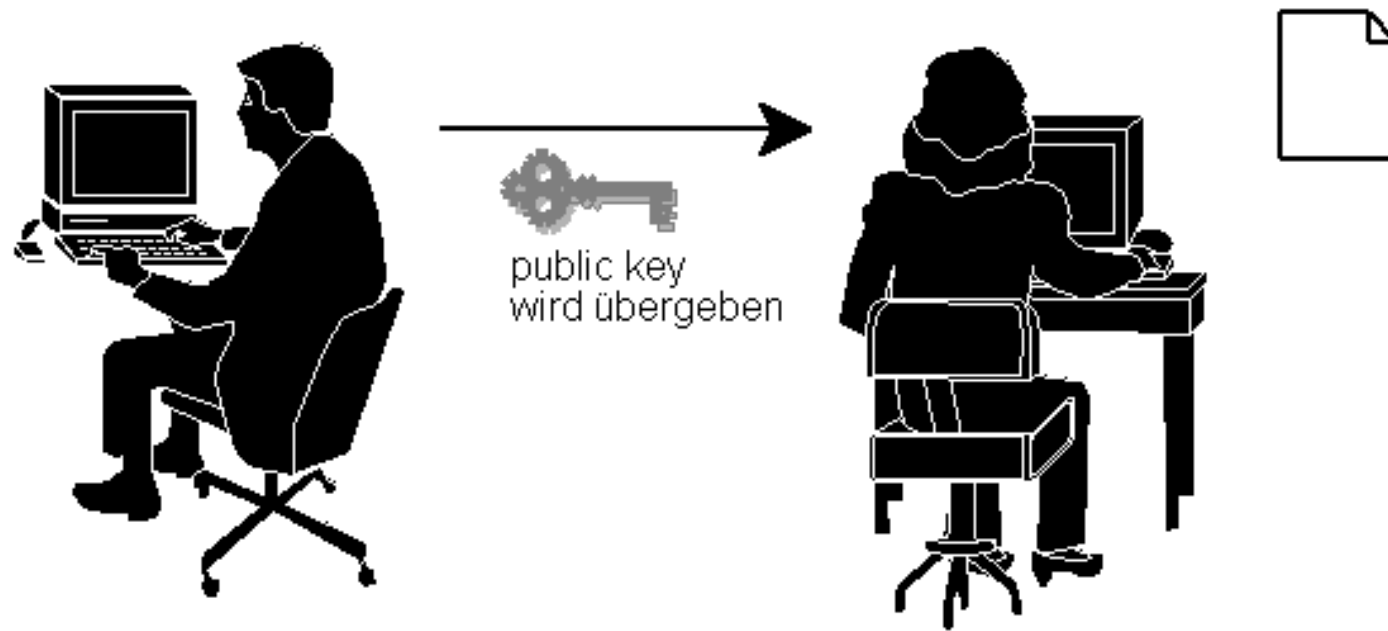
Key ist idR eine Passwort (beide Partner müssen dieses kennen)
40 - 1024 „Bit-Verschlüsselung“

Asymmetrische Verfahren (public key encryption)

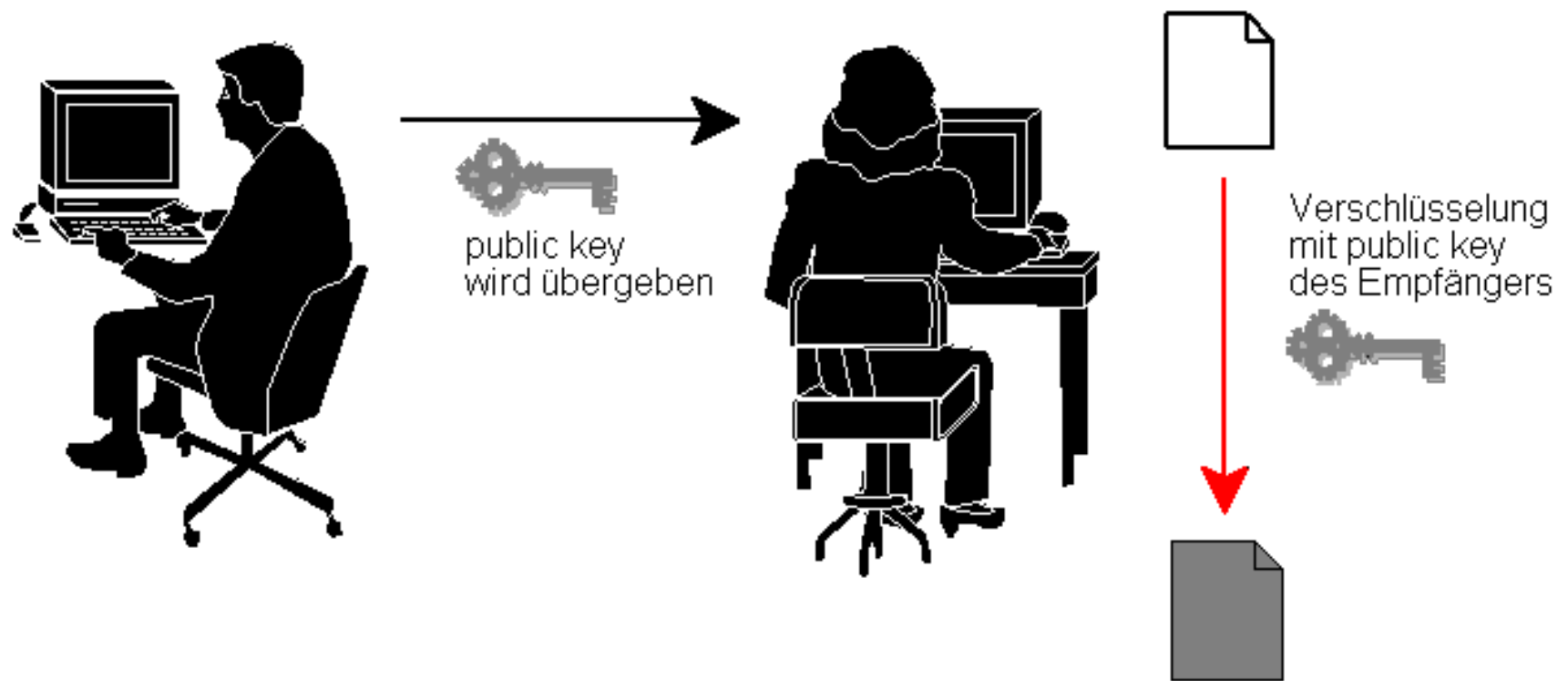
- ein Key zum Verschlüsseln (public key), ein anderer zum Entschlüsseln (private key)
- z.B. DSA, RSA



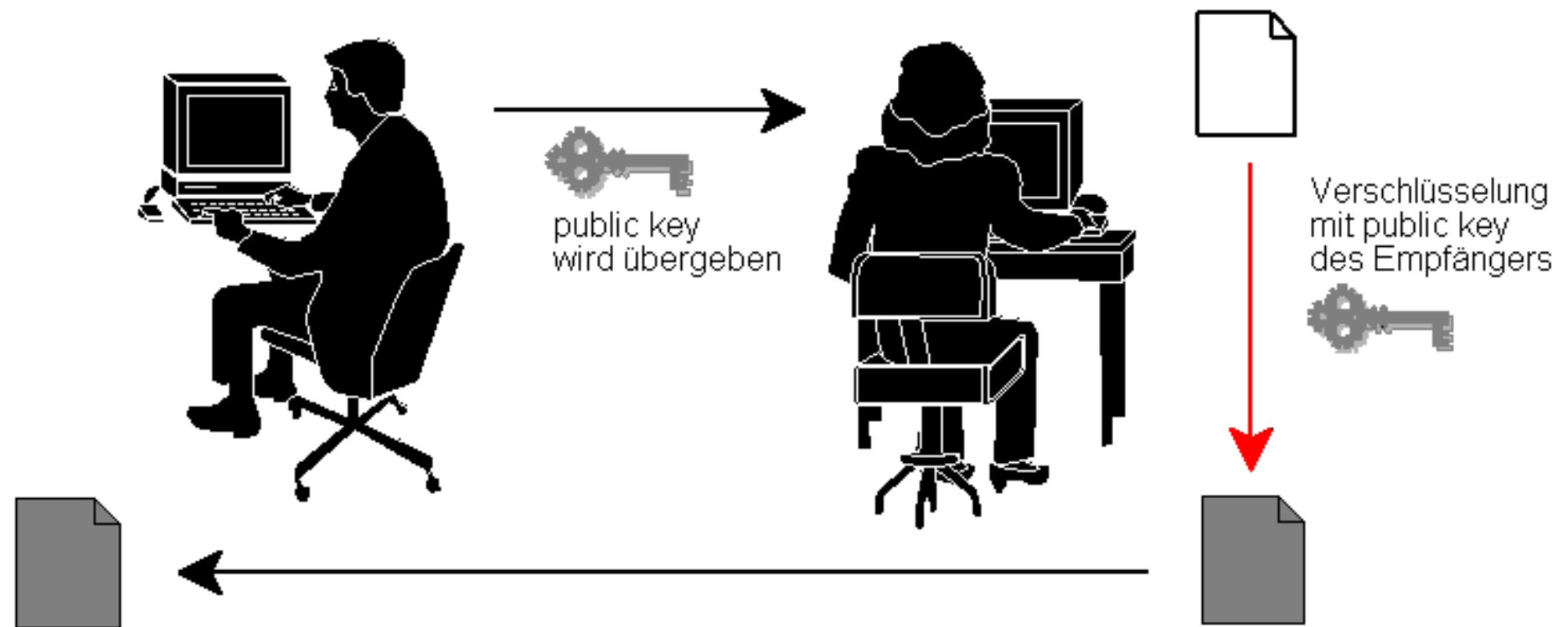
Public Key Encryption



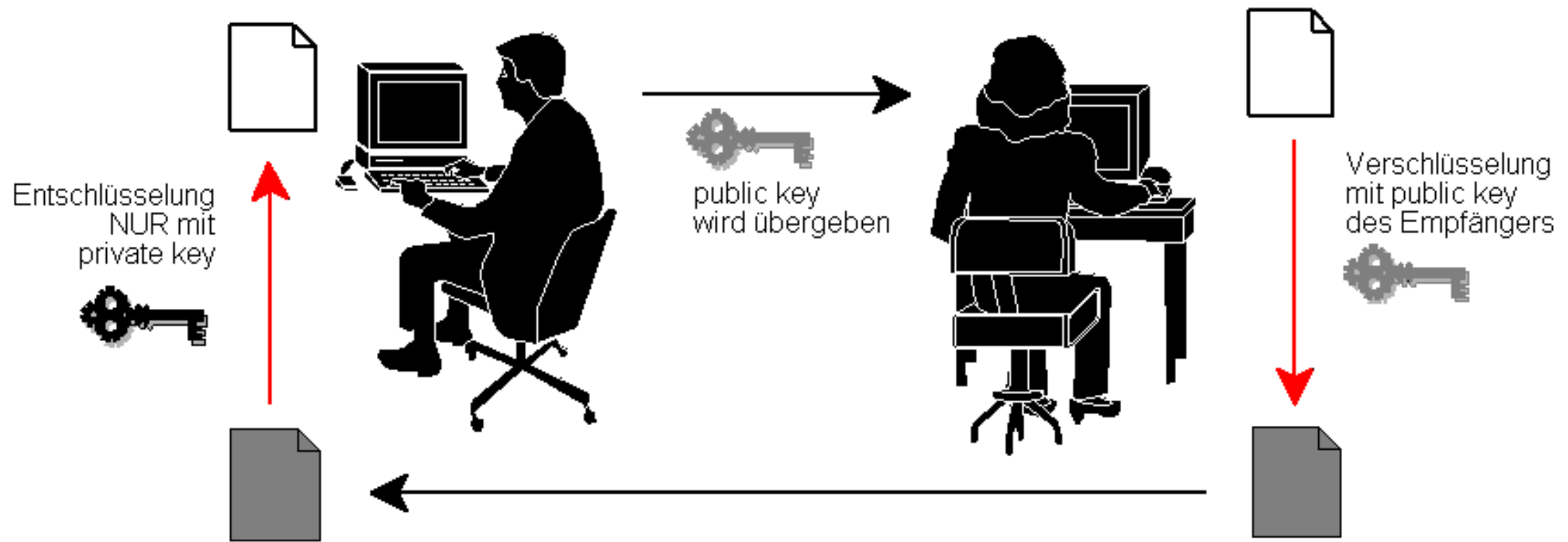
Public Key Encryption



Public Key Encryption



Public Key Encryption



Public Key Encryption

Brute Force/Key Search Attack
vom Public Key den Private Key errechnen

kryptographische Analyse
den Algorithmus „knacken“

Angriffsmethoden gegen asymmetrische Verfahren

Message Digest Functions (One-Way-Encryption)

Anhand des Inhalts einer Datei eine eindeutige 128 od. 256 Bit Zahl errechnen.

Grundgedanke: keine zwei Dateien mit der selben Message Digest.
z.B. MD5, SHA-1

```
# dies ist ein Kommentar
```

```
# das file test1.txt anlegen  
echo "This is a test." > test1.txt
```

```
# das file test2.txt anlegen  
echo "this is a test." > test2.txt
```

```
# komplett unterschiedliche MD5-Summen auf Grund eines Zeichens!  
md5sum test1.txt test2.txt
```

```
# test2.txt dem file test1.txt gleichsetzen  
echo "This is a test." > test2.txt
```

```
# selber Inhalt, selbe MD5-Summen!  
md5sum test1.txt test2.txt
```

Demonstration von Message Digest Functions

Angewandte Verschlüsselung mit GnuPG

Public Key des Empfängers ist stets erforderlich

Variante

#1: in der Shell: `echo secret message | gpg --ear <empfänger>`

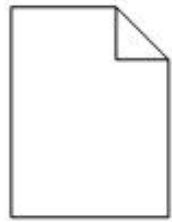
#2: im Mail-Client: z.B. Thunderbird

Digitale Signatur mit GnuPG

- Unterschrift wird mit Private Key erzeugt
- Mit Public Key verifizierbar

→ Message Digest der Nachricht wird mit Private Key verschlüsselt.

Anwendungsgebiet: va. E-Mail



Message Digest Function



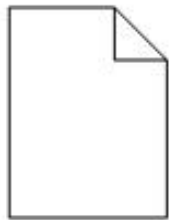
b99e98584b39...



Verschlüsselung mit
Private Key des Signator

Elektronische Signatur

ghdr



Message Digest Function

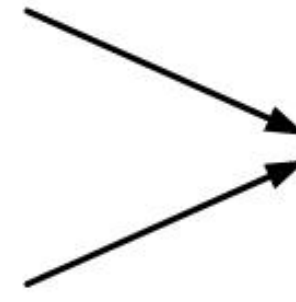


b99e98584b39...

Entschlüsselung mit
Public Key des Signator



b99e98584b39...



= ??

ghdr



Datensicherung

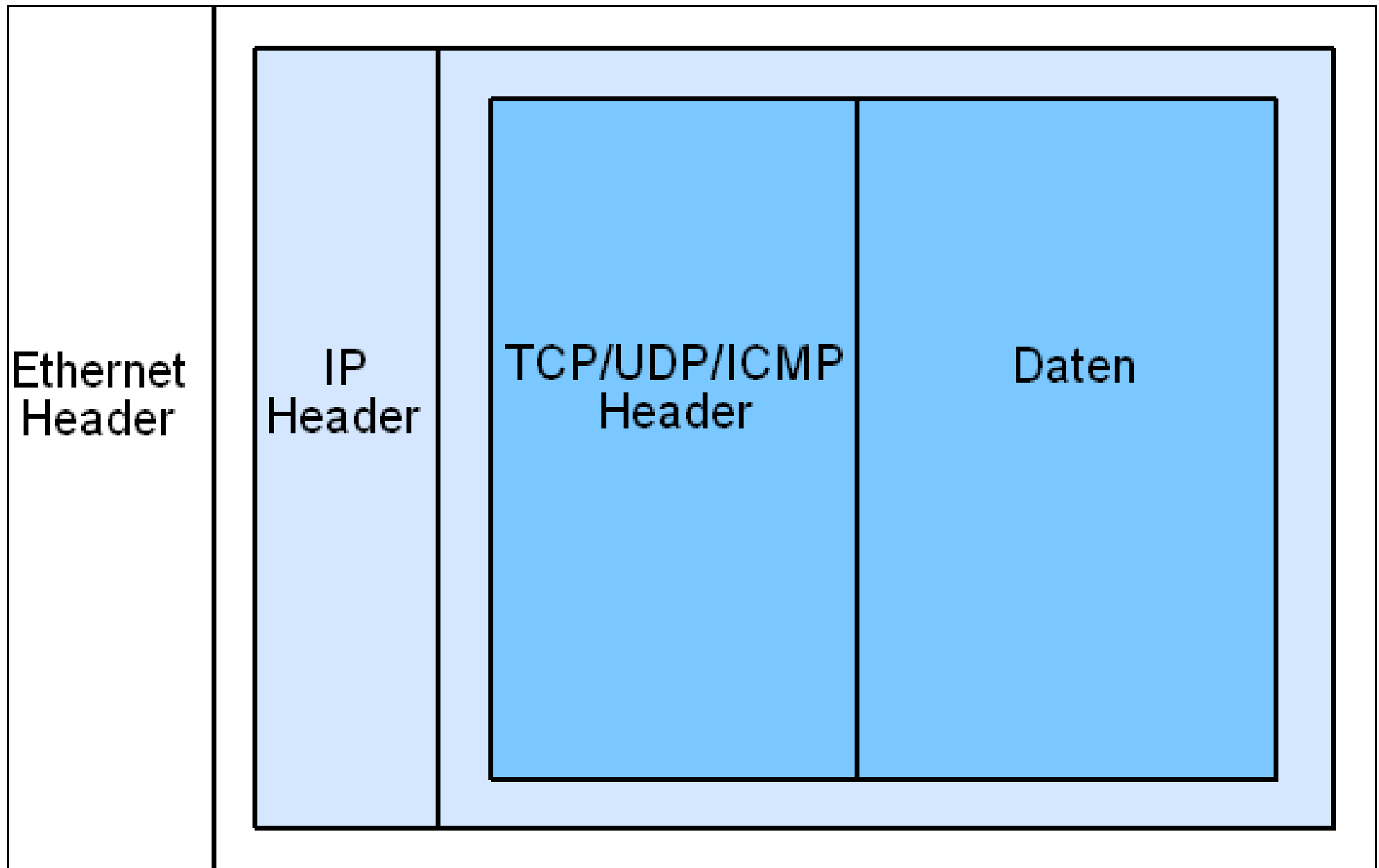
- Backup Policy?
- Das Backup-Tool tar
für fortgeschrittene interessant: [dumpnet - dumpnet.sourceforge.net](http://dumpnet.sourceforge.net)

Firewalls

Schutz eines od. mehrerer Rechner vor unbefugtem Zugriff

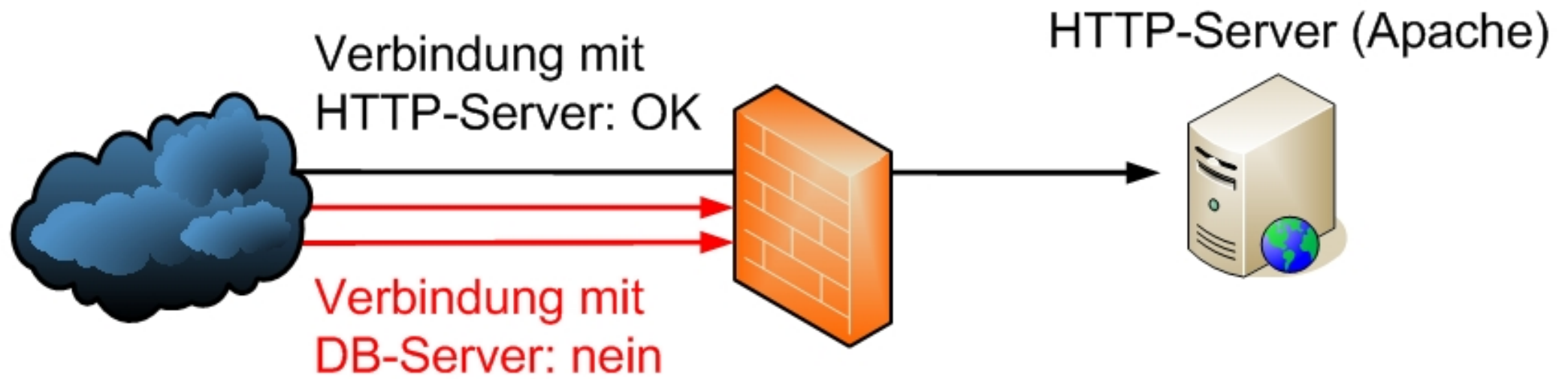
Eine Einführung in die Protokollschichten von TCP/IP

- Applikationsschicht: HTTP/FTP/SMTP/...
- Transportschicht: TCP/UDP/ICMP
- Internetschicht: IP
- Netwerkschicht: idR Ethernet



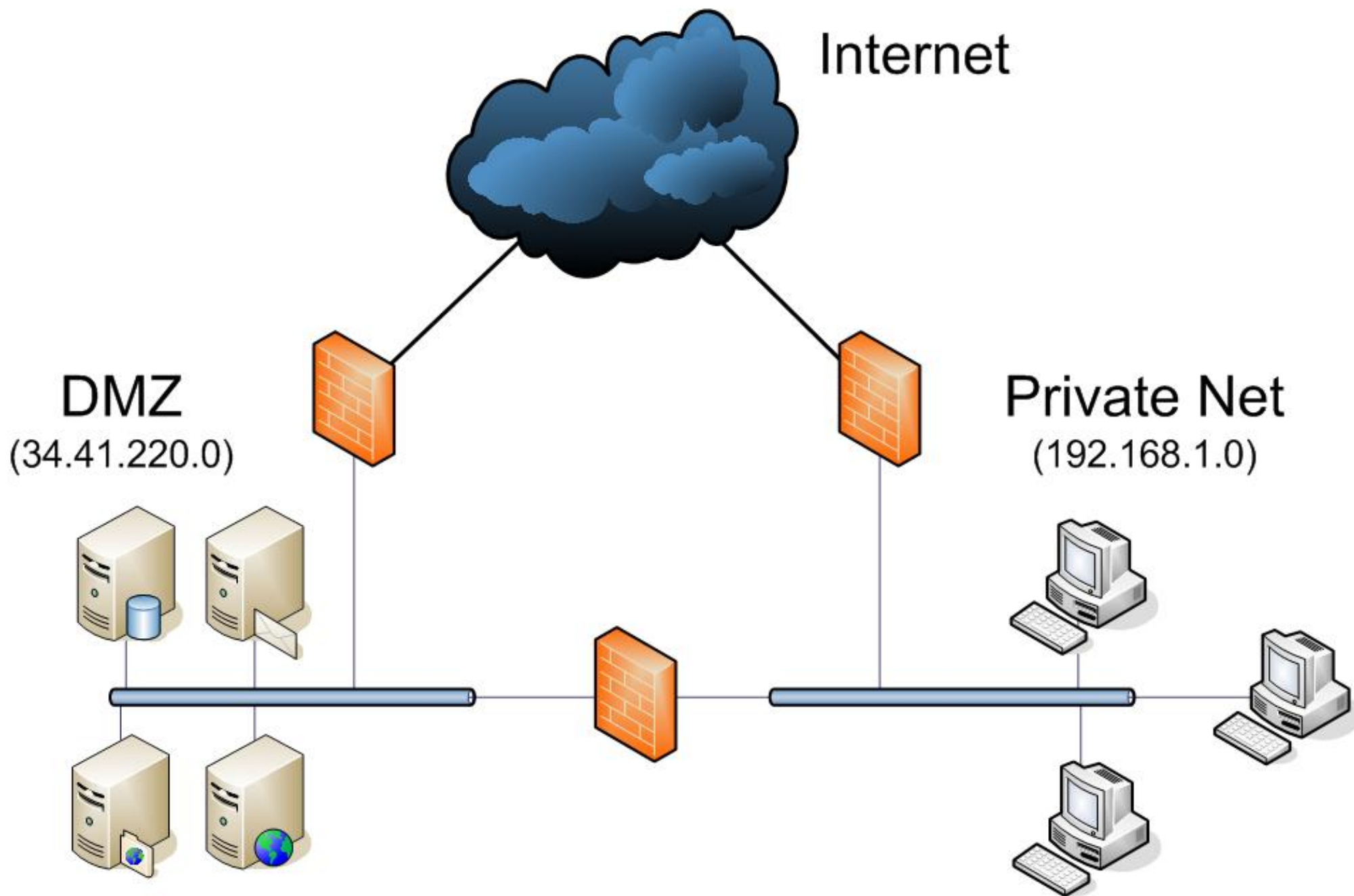
Ineinander verschachtelte Pakete der unterschiedlichen Schichten

- verbindungsorientiert
 - expliziter Verbindungsaufbau -und Abbau
 - kein Datentransfer ohne Verbindung
- zuverlässig
 - stellt sicher, dass alle Daten tatsächlich ankommen
 - checksum für Header & Daten (beschädigte Pakete werden erneut gesendet); IP kennt nur checksum f. Header
 - Pakete in falscher Reihenfolge werden sortiert
 - doppelte Pakete werden verworfen
- ununterbrochener Datenstrom
 - höhere Protokollschichten erhalten ununterbrochenen Datenstrom
 - Operationen zur Fehlerkorrektur bleiben höheren Protokollschichten verborgen



Firewall schützt Server: TCP Connection Requests NUR an Port 80!

DMZ – Demilitarized Zone



Server in der DMZ sind durch Firewalls vor internen & externen Angreifern geschützt!

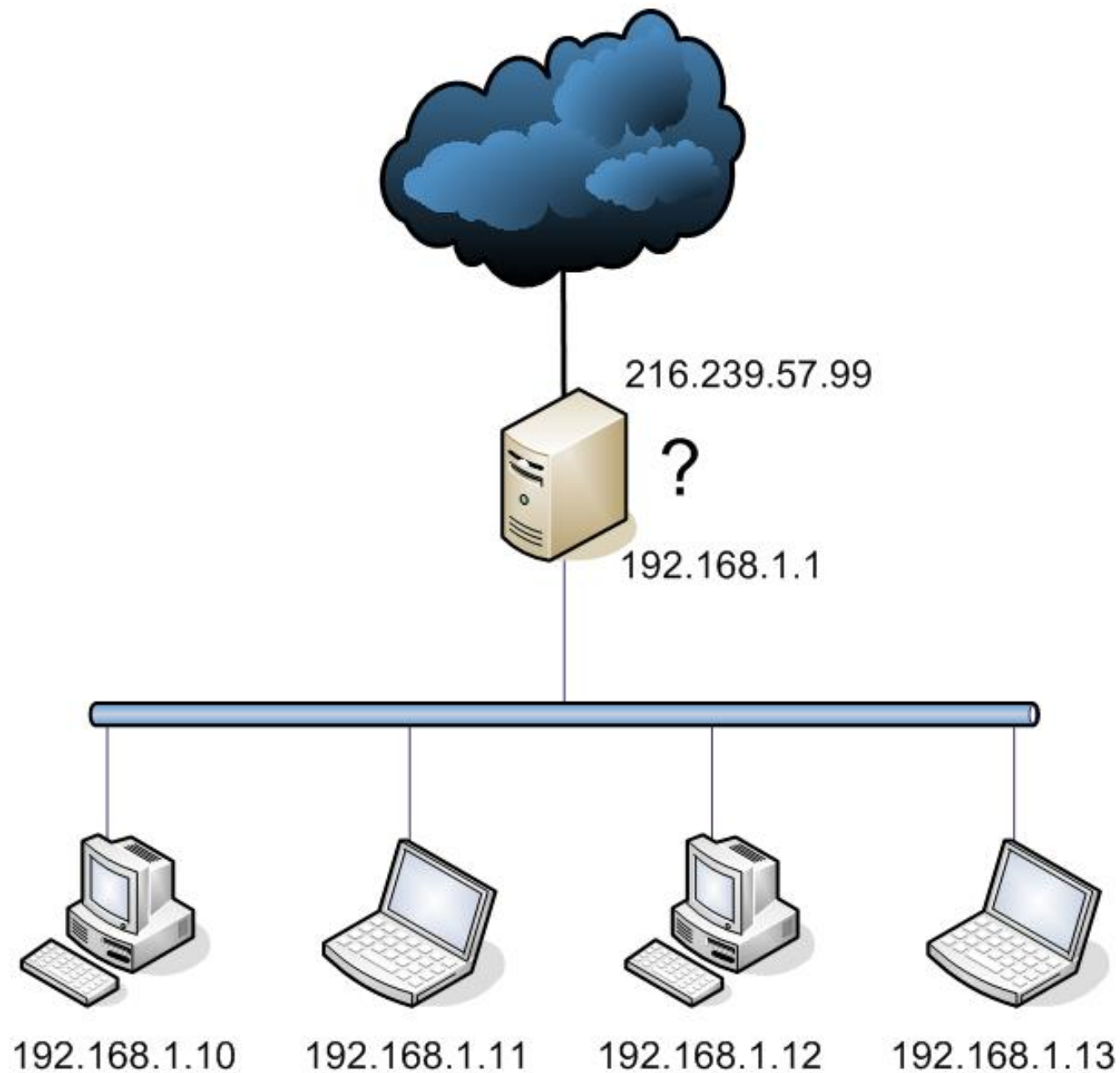
Einrichten einer Host-Based Firewall

in YAST: Security and Users → Firewall

Test der Firewall: mittels telnet und "tail -f /var/log/firewall"

Firewalls: NAT – Network Address Translation

- IPv4 kennt nur ca. 4 Mrd IP-Adressen



(S)NAT: Firewall ändert Source-IP bei ausgehenden & Destination-IP bei eingehenden Paketen

Danke

Lukas Feiler

lukas.feiler@lukasfeiler.com