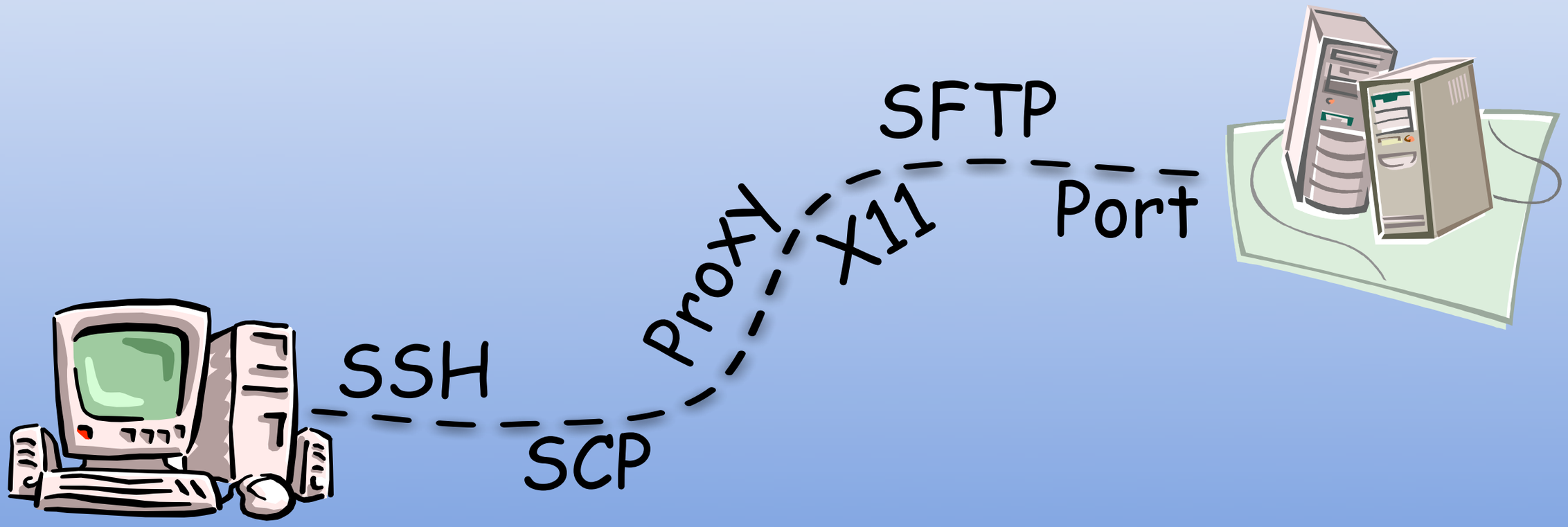
Remote Tools

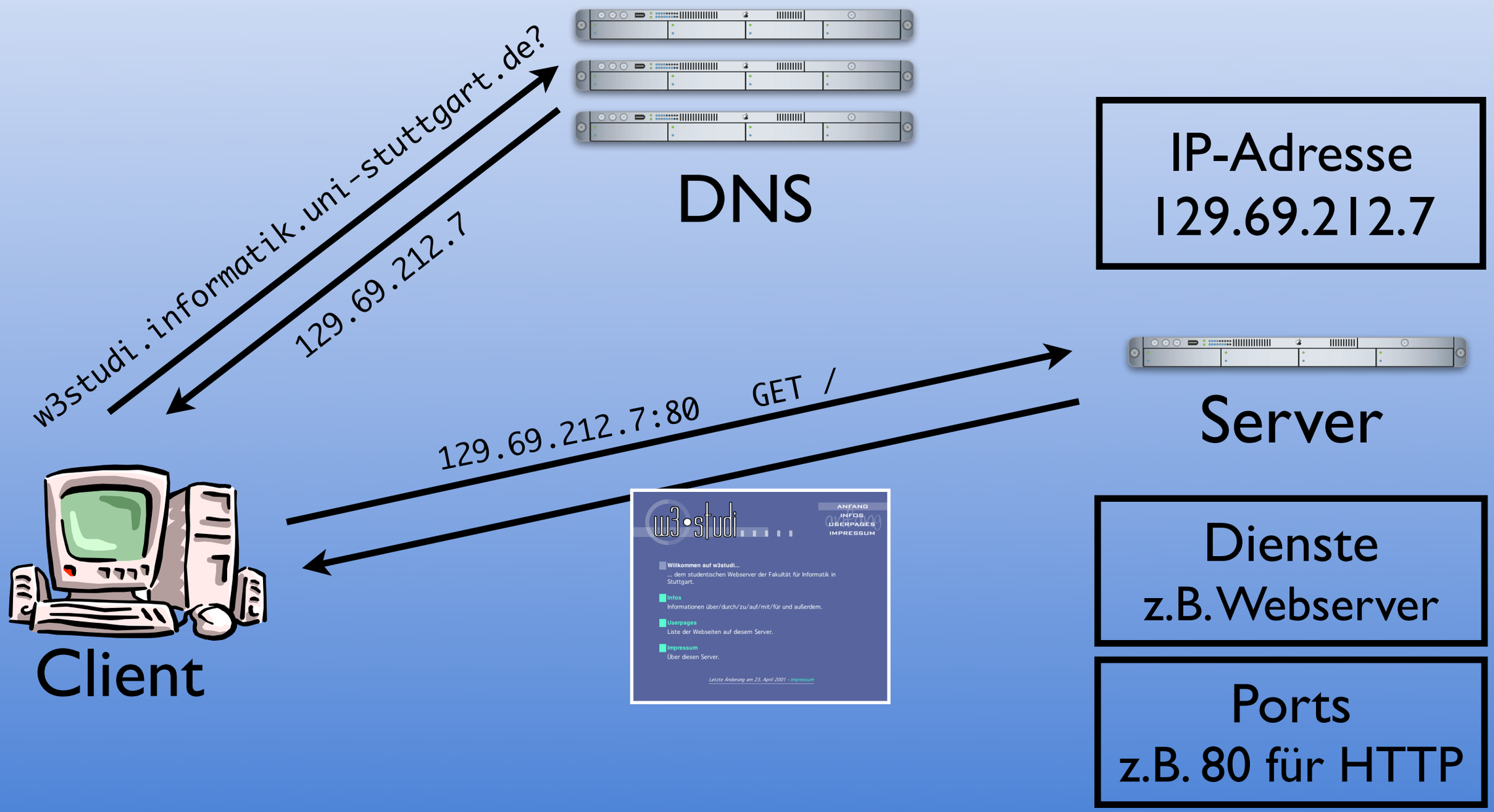


christina.zeeh@studi.informatik.uni-stuttgart.de

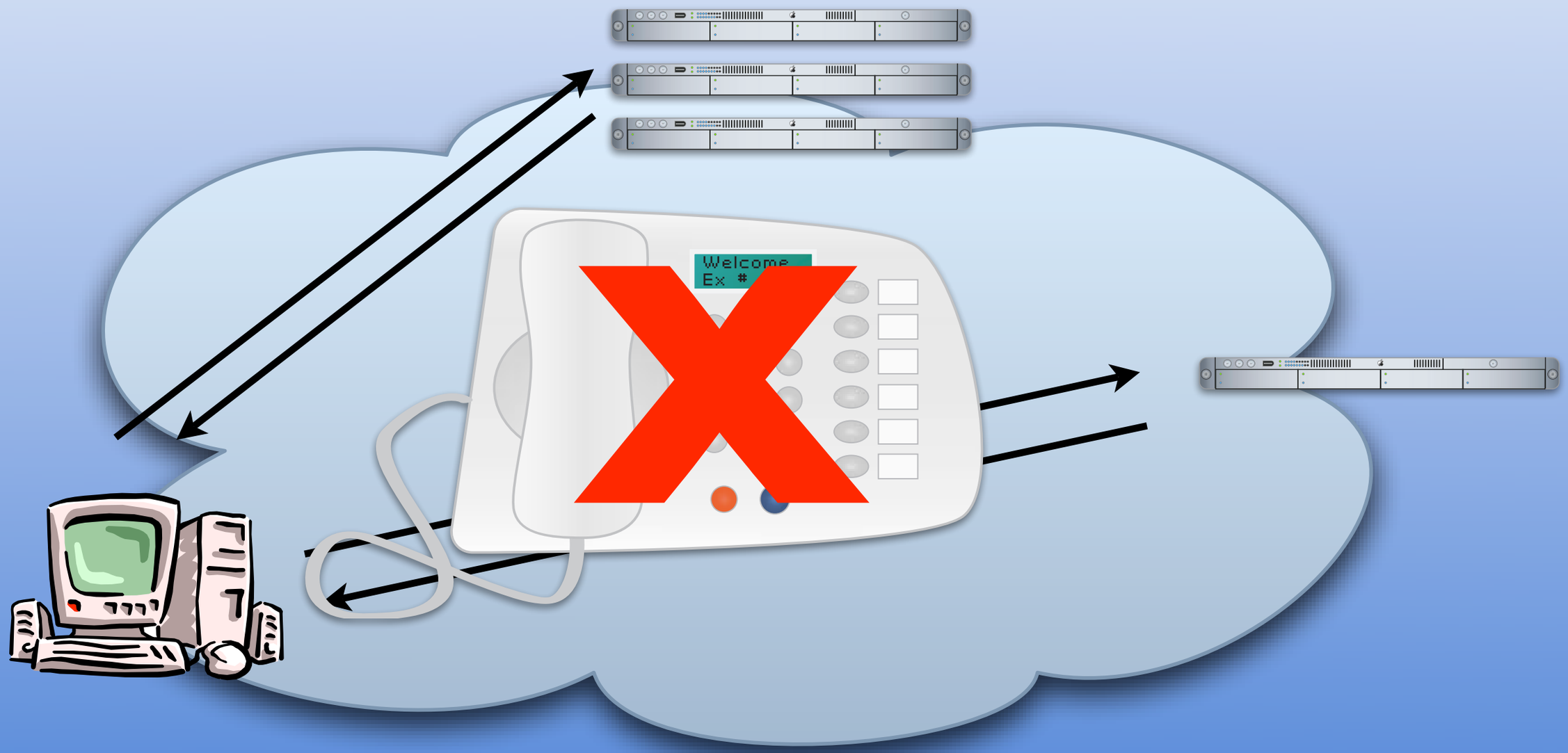
Inhalt

- Grundlagen
- SSH
  - Remote-Login auf marvin
  - Datentransfer
  - Graphische Anwendungen
  - Tunnel
- VPN
- SSH für Fortgeschrittene

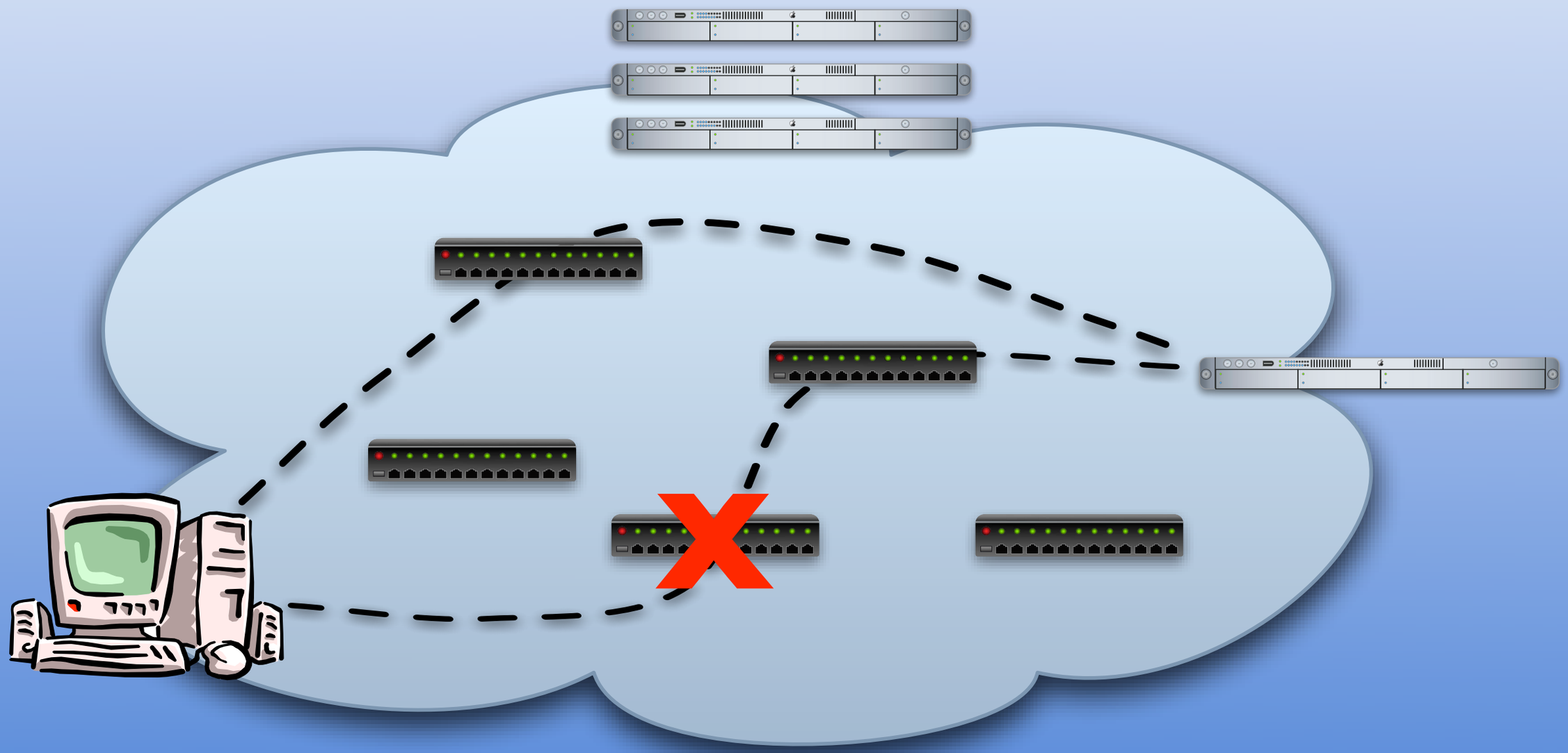
Grundlagen


w3studi.informatik.uni-stuttgart.de?
129.69.212.7
DNS
IP-Adresse
129.69.212.7
129.69.212.7:80
GET /
Server
Client
w3•studi
ANFANG
INFOS
USERPAGES
IMPRESSUM
Willkommen auf w3studi...
... dem studentischen Webserver der Fakultät für Informatik in Stuttgart.
Infos
Informationen über/durch/zu/auf/mit/für und außerdem.
Userpages
Liste der Webseiten auf diesem Server.
Impressum
Über diesen Server.
Letzte Änderung am 23. April 2001 - Impressum
Dienste
z.B. Webserver
Ports
z.B. 80 für HTTP

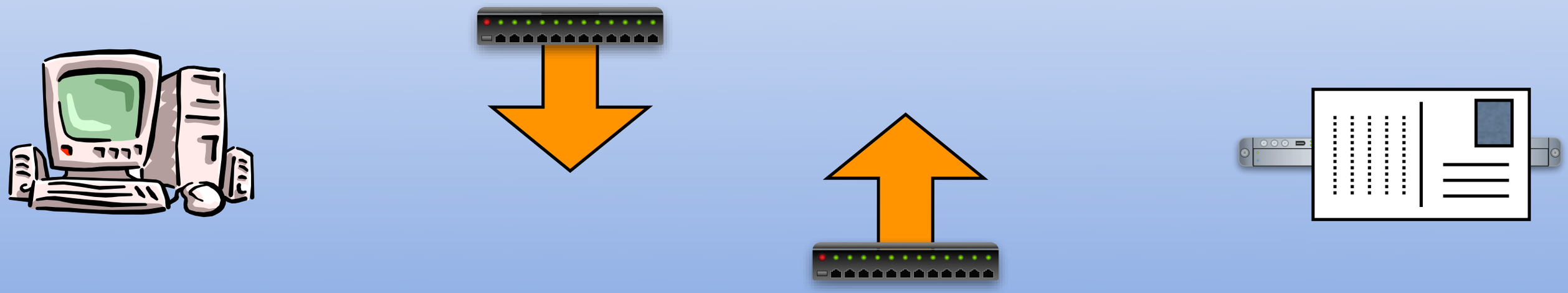
Problematik



Problematik



Problematik



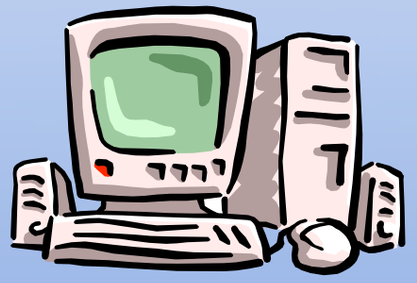
Nachricht kann

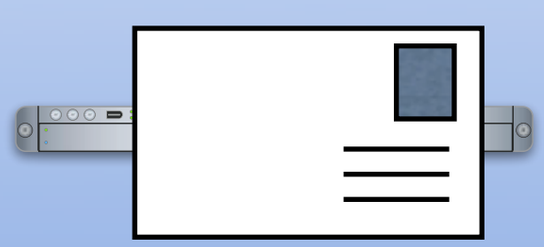
- gelesen
- verändert

werden (Passwörter, Kreditkartennummern, Emails, Chats, Steuererklärungen, ...)

Daten verschlüsseln

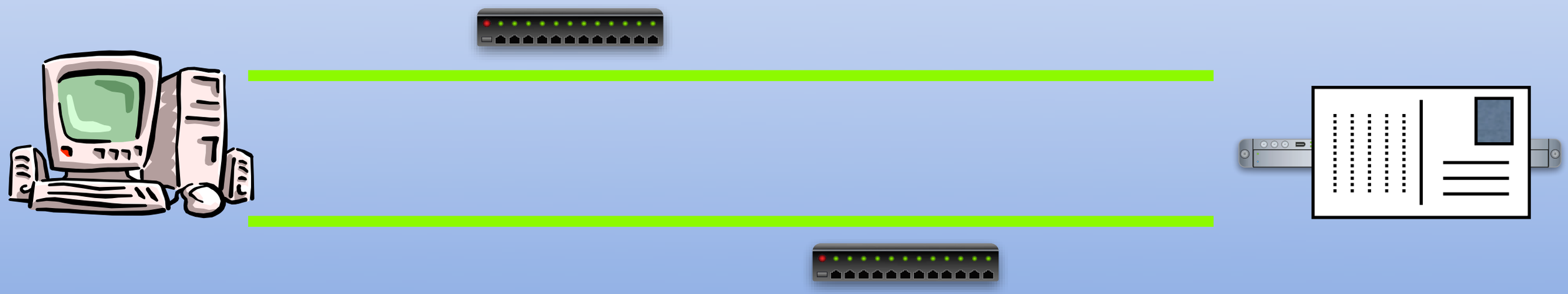
(z.B. GnuPG/PGP)





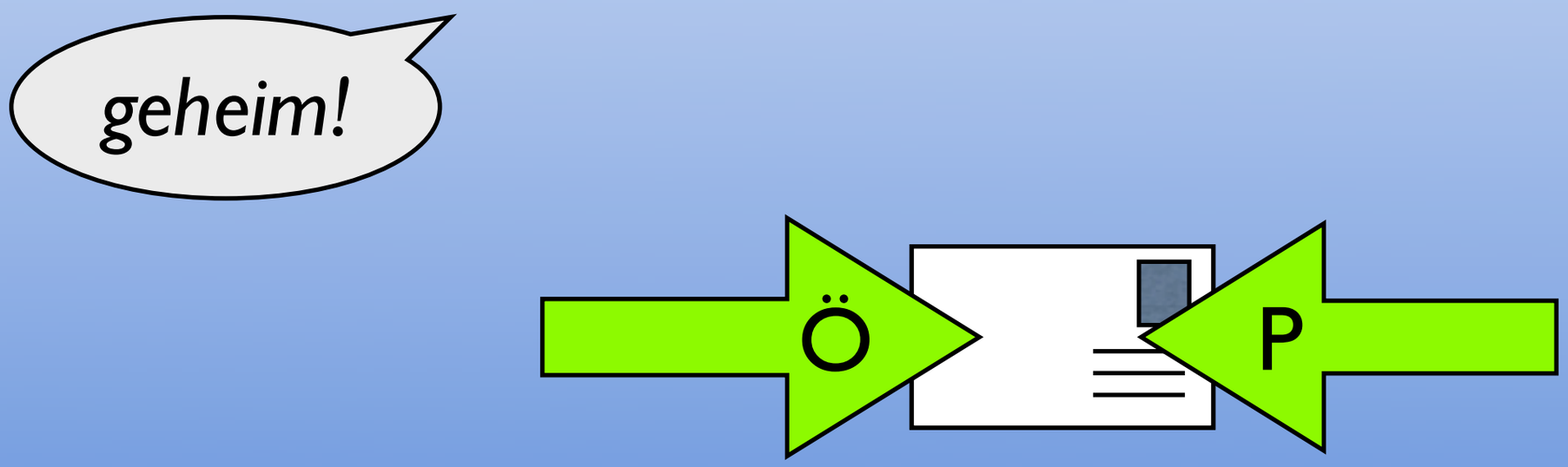
Verschlüssende Protokolle

z.B. SSH, HTTPS, ...



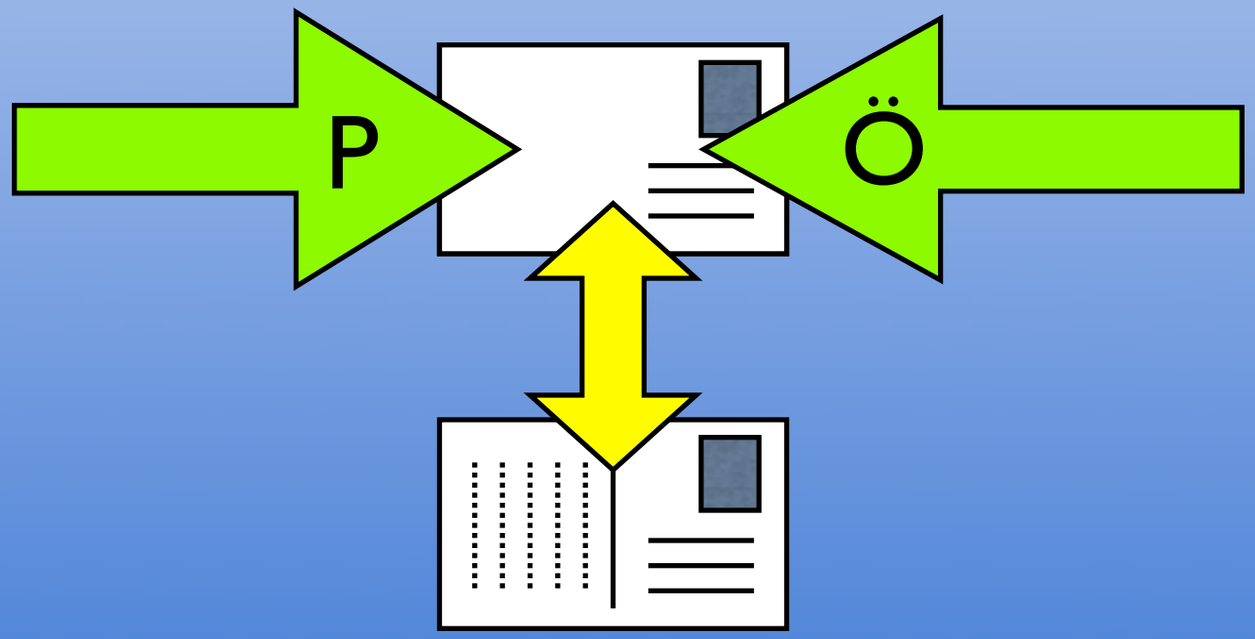
Public Key Verfahren (1)

- Öffentlicher Schlüssel – Verschlüsseln
- Privater Schlüssel – Entschlüsseln

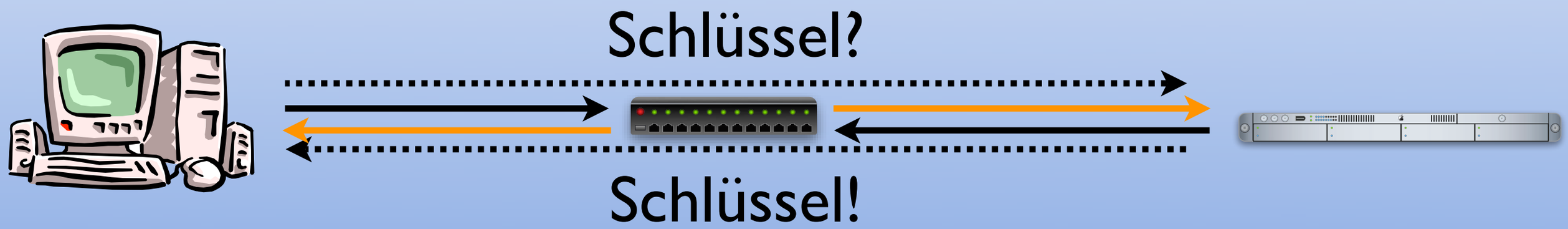


Public Key Verfahren (2)

- Privater Schlüssel – Verschlüsseln (Unterschreiben)
- Öffentlicher Schlüssel – Entschlüsseln (Verifizieren)



Woher kommt der öffentliche Schlüssel?



- Persönliche Schlüsselübergabe
- Signiertes Zertifikat
  - CA zertifiziert, dass ein bestimmter Schlüssel zu einer bestimmten Person/Organisation gehört

Tools

- Erreichbarkeit, Antwortzeit
  `ping <Hostname/IP>`
- Route der Pakete
  `traceroute <Hostname/IP>`
- DNS-Abfrage
  `dig <Hostname>`
- Reverse-Lookup
  `dig -x <IP>`

SSH

Secure Shell

Unsere Ziele

- Textorientierte Anwendungen remote starten
- Datentransfer
- Graphische Anwendungen remote starten
- Gesperrte Webseiten anschauen
- Mails über studi verschicken

SSH

- Einzige Möglichkeit zum Login auf marvin
- Läuft auf Port 22
- Verschlüsselt
- Hostkeys gegen Man-in-the-Middle Angriff
- Fingerprint von marvin:

```
RSA 1e:8b:05:45:36:96:e5:4f:7d:30:11:92:b2:02:75:ba
xegip-buhok-sodyk-pacam-kusem-godan-ruzoz-dakud-zizyk-nuhit-duxyx
DSA be:b6:85:ee:ab:8e:bf:aa:f9:45:47:be:70:48:e8:7b
xutat-vusab-rumeh-zoryb-velen-rolok-recal-colig-gecar-hasum-bixex
```

SSH Implementierungen

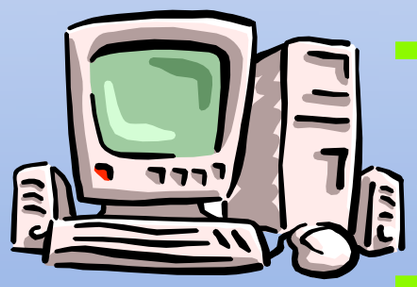
- Muss Protokollversion 2 unterstützen!
- OpenSSH (Linux , Windows, Mac)
- Putty (Windows)
- SSH Communication Security (Windows u.a.)

Remote Login

Einfacher Login

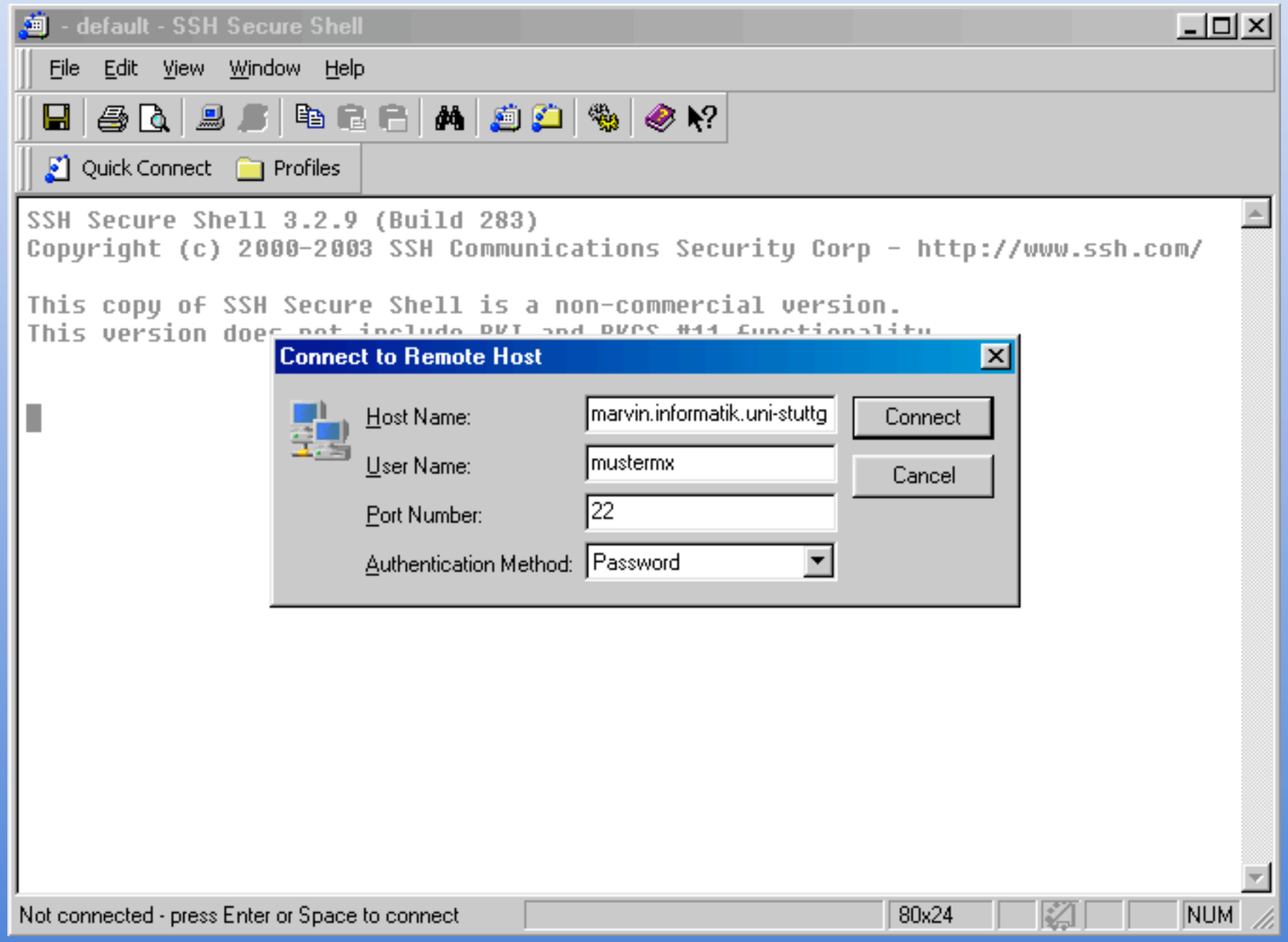
- `ssh benutzername@marvin.informatik.uni-stuttgart.de`
- Es wird gefragt, ob der unbekannte Hostkey akzeptiert werden soll ⇒ mit vorletzter Folie vergleichen.
- Benutzername, Passwort aus dem Pool
- Shell wie im Pool unter Linux

SSH Verbindung

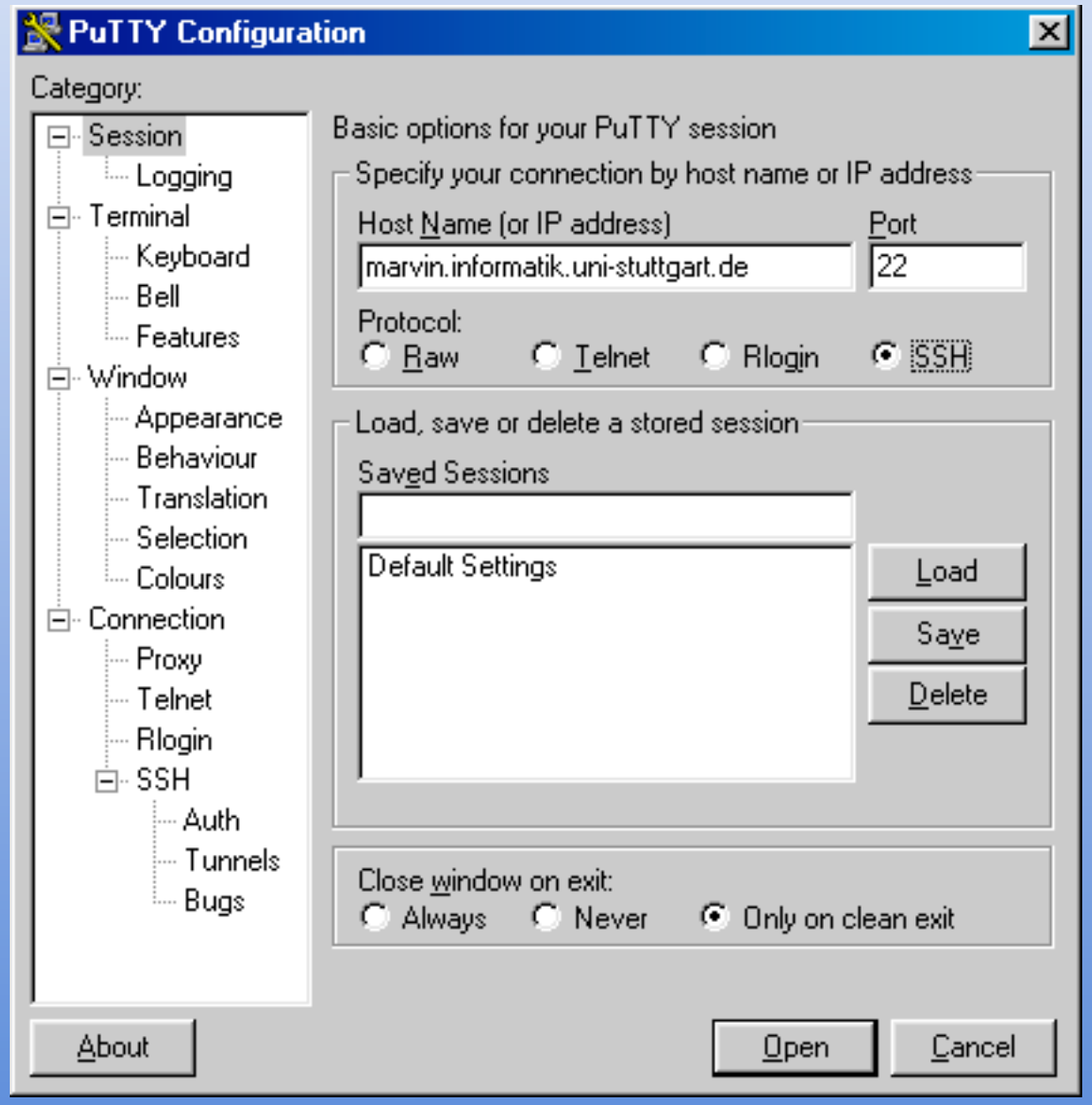


```
cd /tmp  ls  cp test.tx
```

SSH.com SSH


- default - SSH Secure Shell
File Edit View Window Help
Quick Connect
Profiles
SSH Secure Shell 3.2.9 (Build 283)
Copyright (c) 2000-2003 SSH Communications Security Corp - http://www.ssh.com/
This copy of SSH Secure Shell is a non-commercial version.
Connect to Remote Host
Host Name:
marvin.informatik.uni-stuttg
User Name:
mustermx
Port Number:
22
Authentication Method:
Password
Connect
Cancel
Not connected - press Enter or Space to connect
80x24
NUM

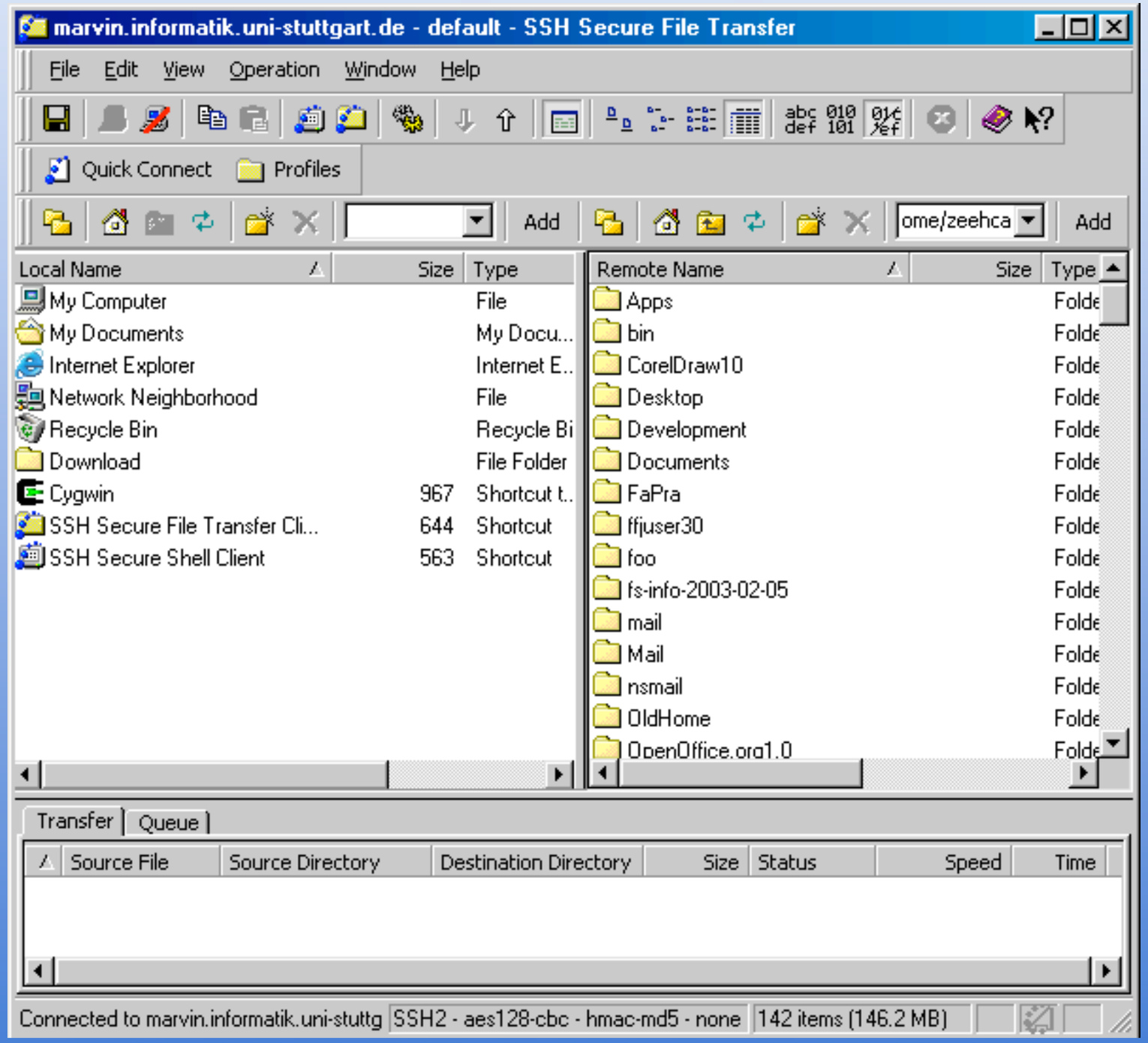
Putty


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Proxy
Telnet
Rlogin
SSH
Auth
Tunnels
Bugs
Basic options for your PuTTY session
Specify your connection by host name or IP address
Host Name (or IP address)
Port
marvin.informatik.uni-stuttgart.de
22
Protocol:
Raw
Telnet
Rlogin
SSH
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

Datentransfer

- Secure Copy (SCP)
  `scp dateiname marvin.informatik.uni-stuttgart.de:.`
  `scp -r verzeichnisname marvin.informatik.uni-stuttgart.de:.`
  - Wildcards auf dem nicht-lokalen Rechner: “*”
- Secure FTP (SFTP)
  `sftp marvin.informatik.uni-stuttgart.de`
  Befehle: `put, get, ls, cd, lcd, mput, mget`

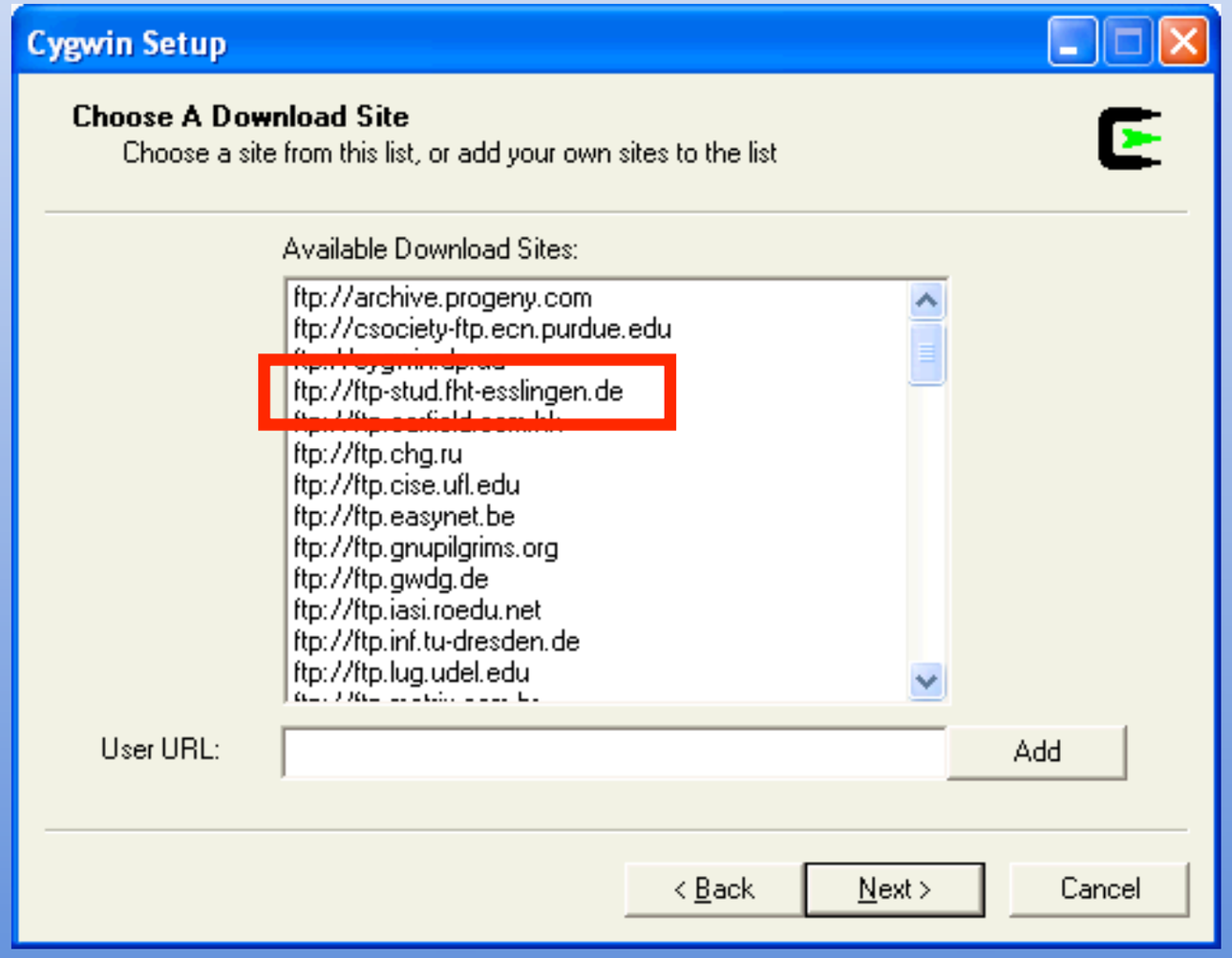
SSH.com SSH


marvin.informatik.uni-stuttgart.de - default - SSH Secure File Transfer
File Edit View Operation Window Help
Quick Connect
Profiles
Add
ome/zeehca
Add
Local Name
Size
Type
My Computer
File
My Documents
My Docu...
Internet Explorer
Internet E..
Network Neighborhood
File
Recycle Bin
Recycle Bi
Download
File Folder
Cygwin
967
Shortcut t..
SSH Secure File Transfer Cli...
644
Shortcut
SSH Secure Shell Client
563
Shortcut
Remote Name
Size
Type
Apps
bin
CorelDraw10
Desktop
Development
Documents
FaPra
ffjuser30
foo
fs-info-2003-02-05
mail
Mail
nsmail
OldHome
OpenOffice.org1.0
Transfer
Queue
Source File
Source Directory
Destination Directory
Size
Status
Speed
Time
Connected to marvin.informatik.uni-stuttg
SSH2 - aes128-cbc - hmac-md5 - none
142 items (146.2 MB)

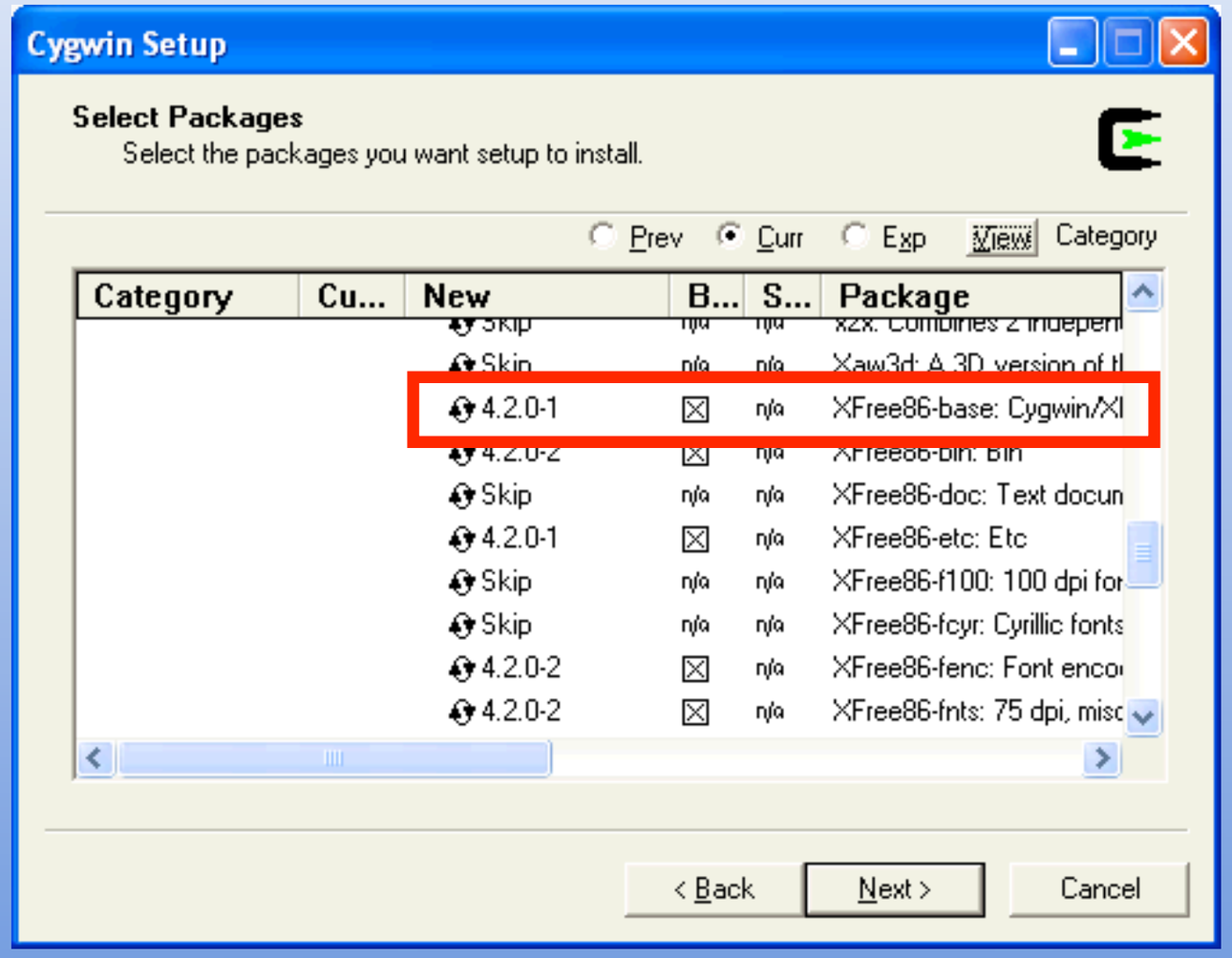
Graphische Anwendungen

- Voraussetzung: lokaler X-Server
- Linux, Mac OS X: meist schon installiert
- Windows: Cygwin
- Cygwin User's Guide: http://cygwin.com/xfree/docs/ug/

Cygwin Installation



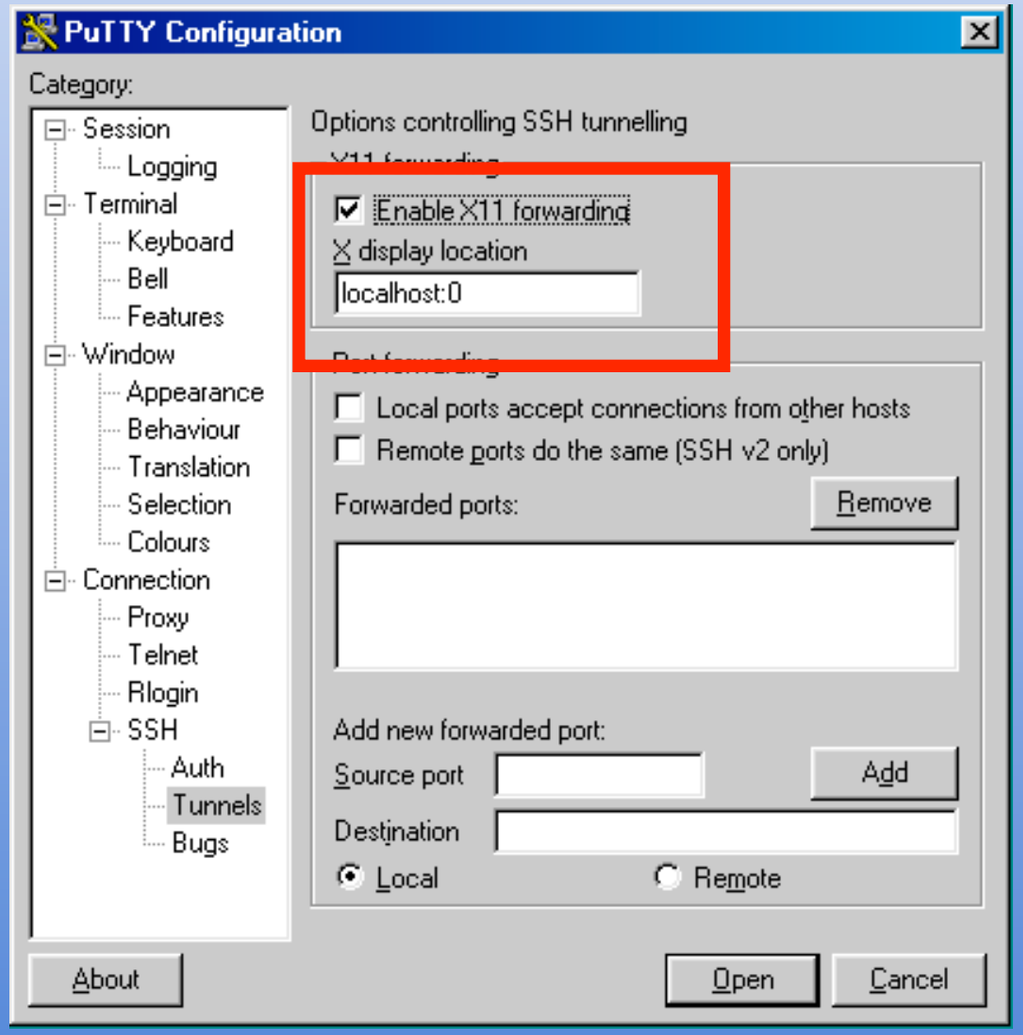
...


Cygwin Setup
Select Packages
Select the packages you want setup to install.
Prev
Curr
Exp
View
Category
Category
Cu...
New
B...
S...
Package
Skip
Skip
4.2.0-1
4.2.0-2
Skip
4.2.0-1
Skip
Skip
4.2.0-2
4.2.0-2
XFree86-base: Cygwin/X
XFree86-doc: Text docun
XFree86-etc: Etc
XFree86-f100: 100 dpi for
XFree86-fcyr: Cyrillic fonts
XFree86-fenc: Font enco
XFree86-fnts: 75 dpi, misc
< Back
Next >
Cancel

Cygwin starten

- `C:\cygwin\usr\X11R6\bin\startxwin.bat`
- X11 Forwarding in der SSH einschalten

  `ssh -X benutzername@marvin...`
- In der Shell auf marvin ganz normal Programme starten



bash

```
bash-2.05b$
```

marvin.informatik.uni-stuttgart.de - PuTTY

```
zeehca@marvin ~ >xclock &
[1] 8662
zeehca@marvin ~ >
```

Recycle Bin

Download

Cygwin

xclock

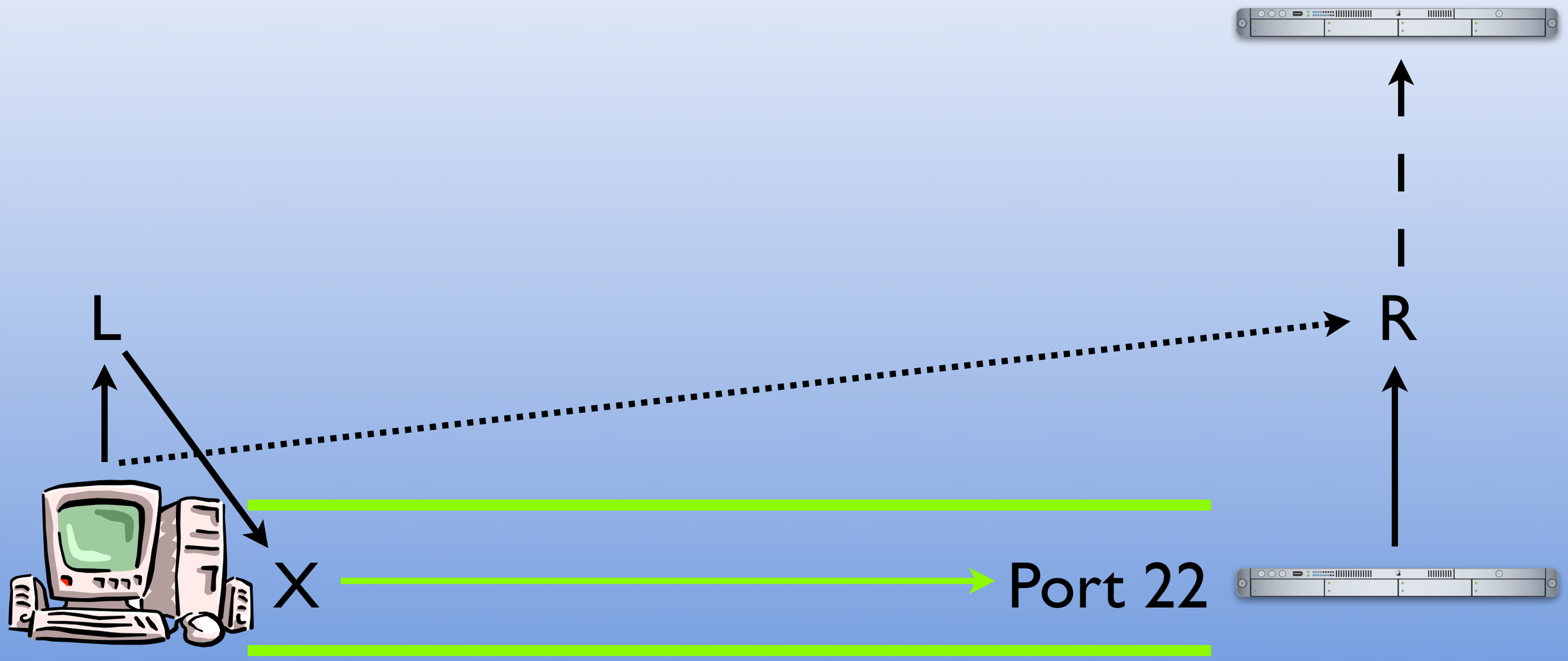
Start | bash | marvin.informatik.uni-... | xclock | 12:44 AM

Arbeiten auf marvin

- Keinesfalls vollständige X-Session starten (einzelne Anwendungen sind ok)
- Rechenintensive längere (studienrelevante) Prozesse
  - `nice` verwenden
  - Mail an `gspooladm`

SSH Tunnels

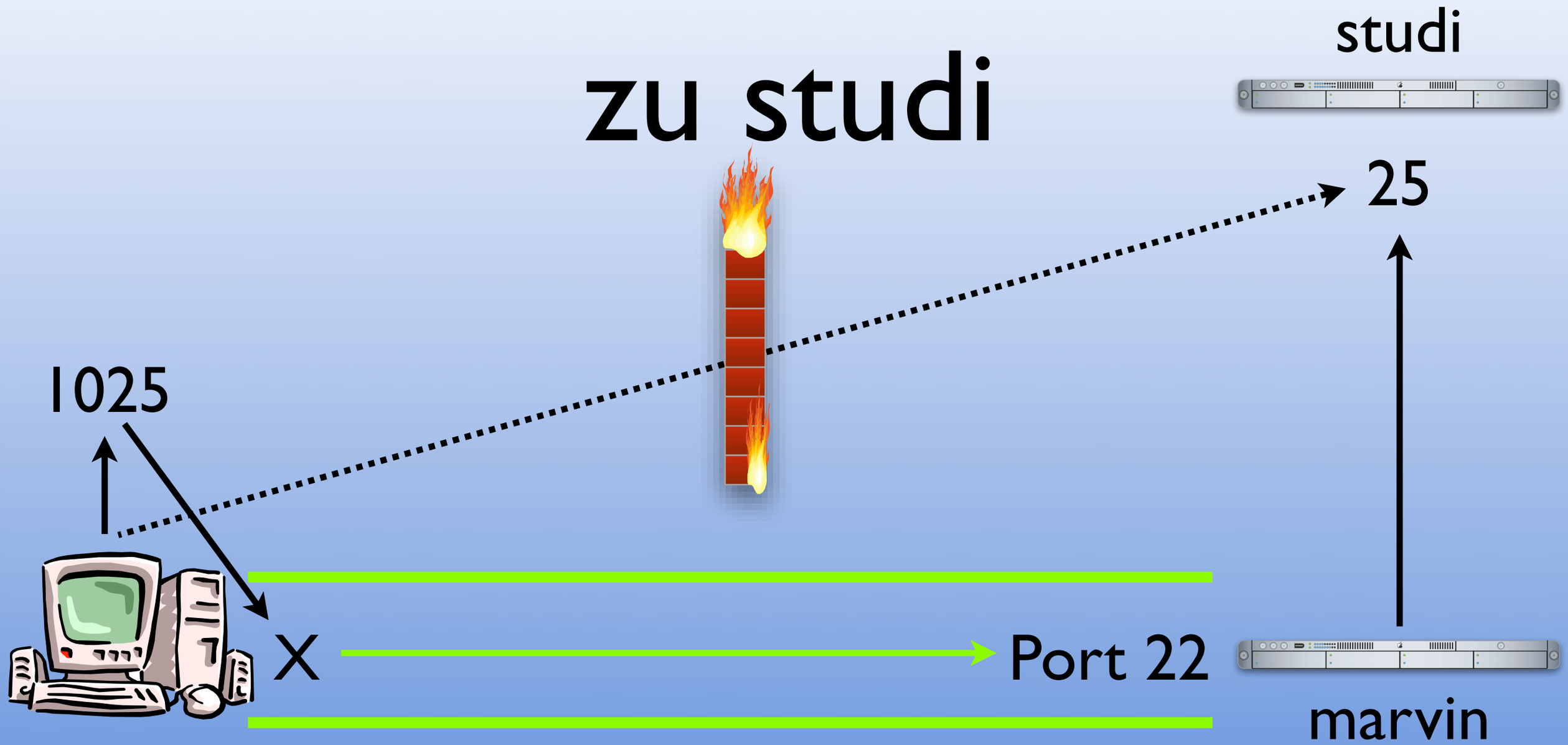
SSH als Tunnel



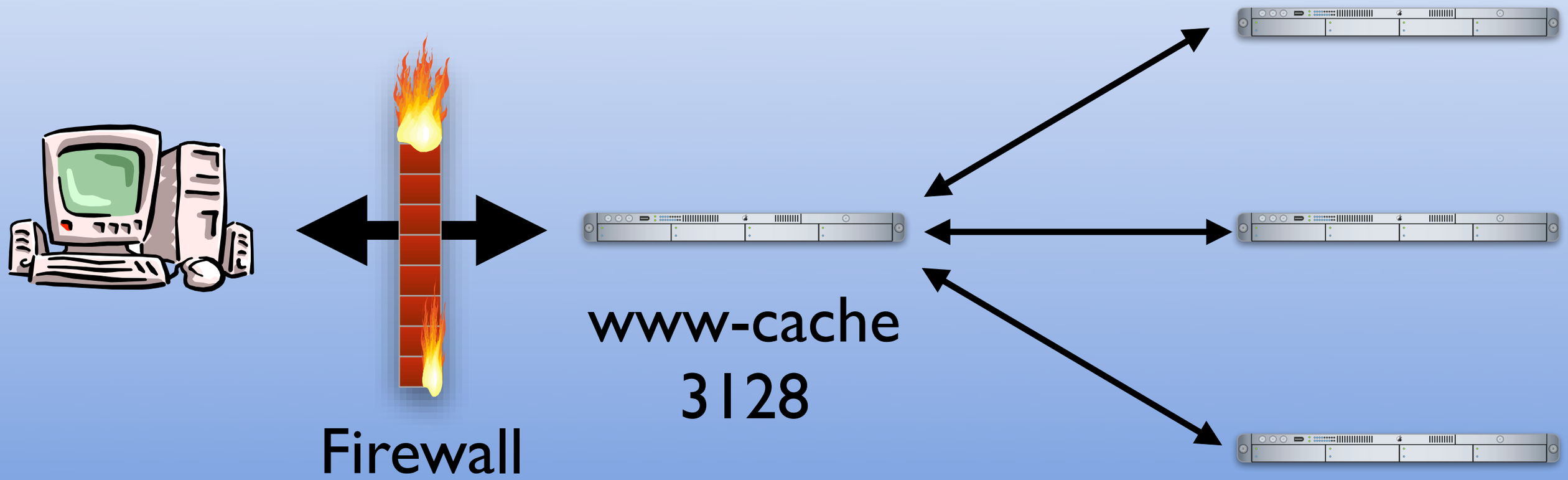
SMTP über studi

- Mails verschicken über Tunnel auf studi
- `ssh -L 1025:studi.informatik.uni-stuttgart.de:25 marvin.informatik.uni-stuttgart.de`
- Im Mailprogramm:
  - SMTP Server: localhost
  - Port: 1025

SSH-Tunnel zu studi



Einschub: Proxy



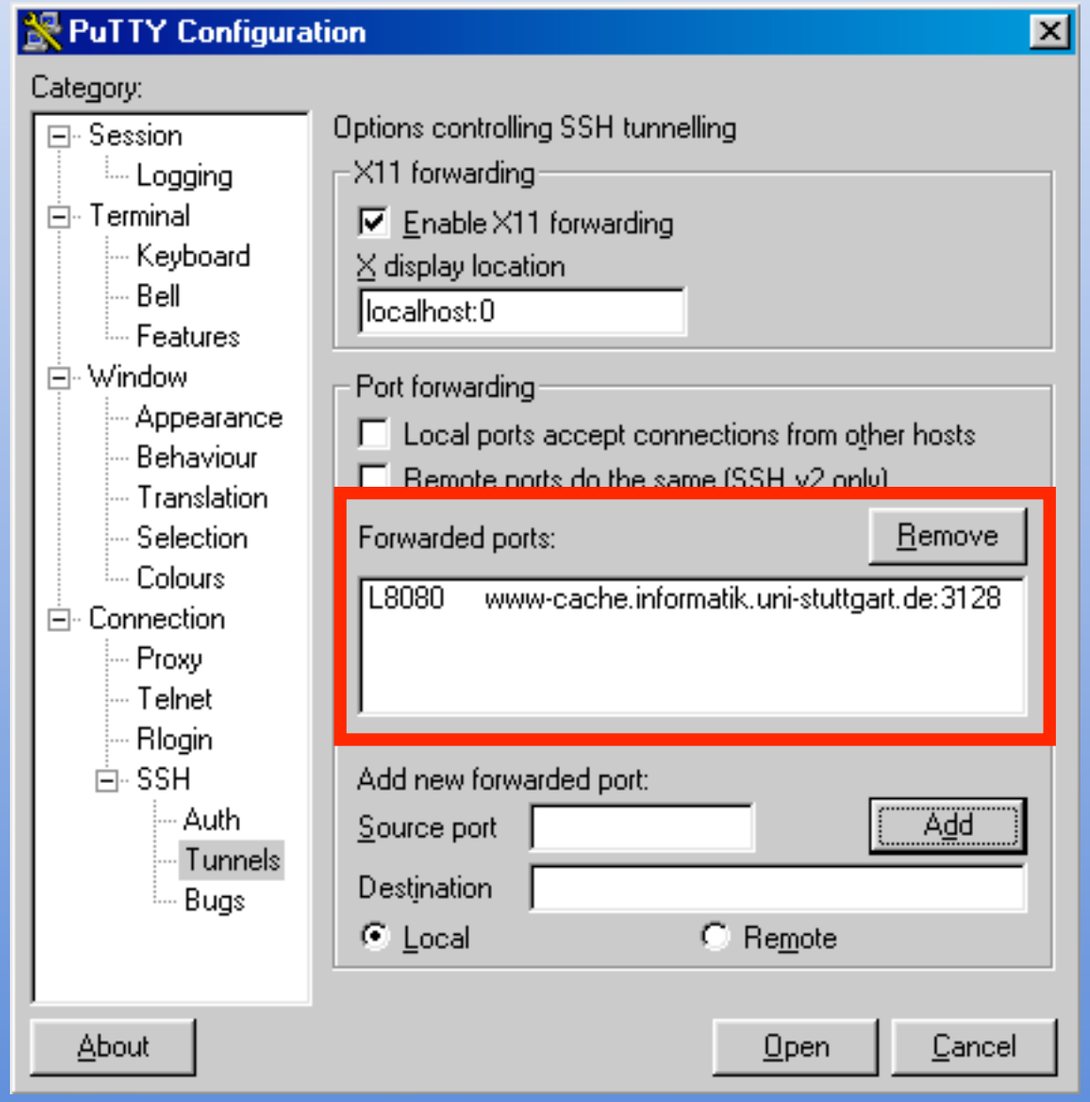
- Caching (Bandbreite sparen)
- Privatsphäre schützen (alle Nutzer kommen vom selben Rechner)

Gesperrte Webseiten

- Lösung: SSH-Tunnel zum Proxy der Informatik
- Prinzip: Daten gehen “huckepack” über verschlüsselte SSH-Verbindung zu marvin, dort werden sie ausgepackt und zum Proxy weitergeleitet.
- `ssh -L 8080:www-cache.informatik.uni-stuttgart.de:3128 marvin.informatik.uni-stuttgart.de`

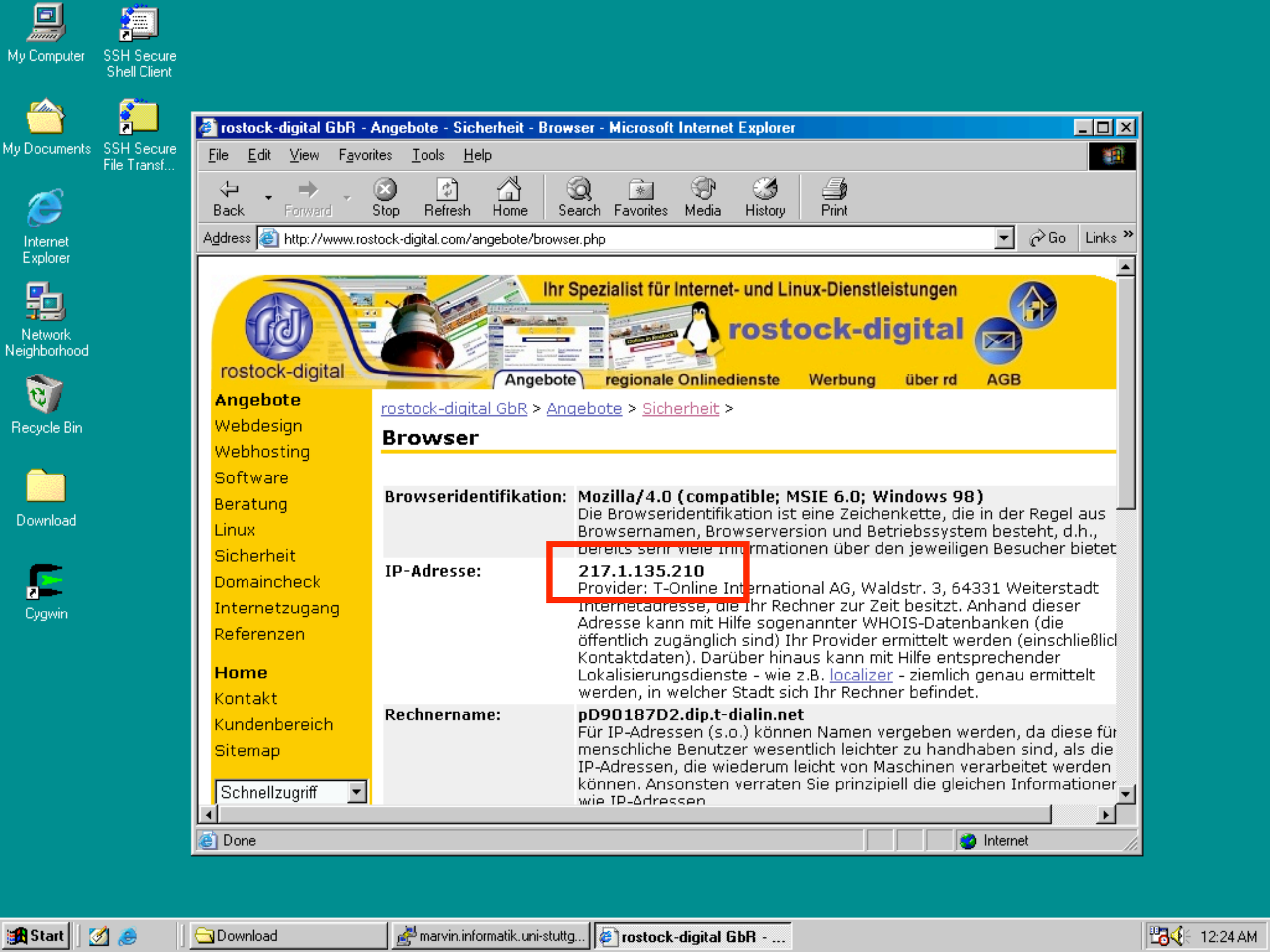
  “Leite alle Daten, die am lokalen Rechner auf Port 8080 ankommen über die verschlüsselte SSH-Verbindung (Tunnel) auf marvin weiter, entschlüssle sie dort und leite sie weiter an den Rechner www-cache Port 3128”

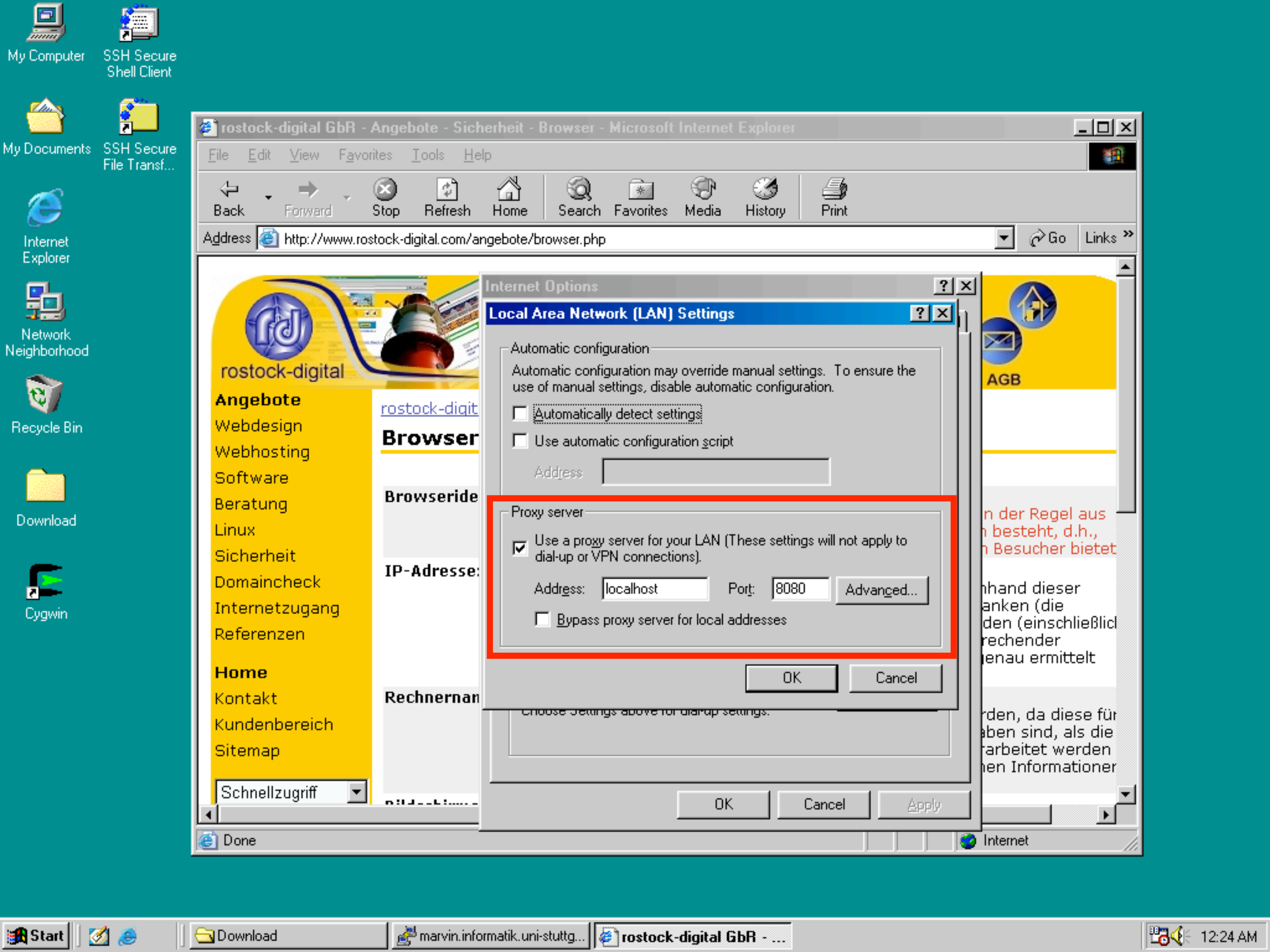
... mit Putty

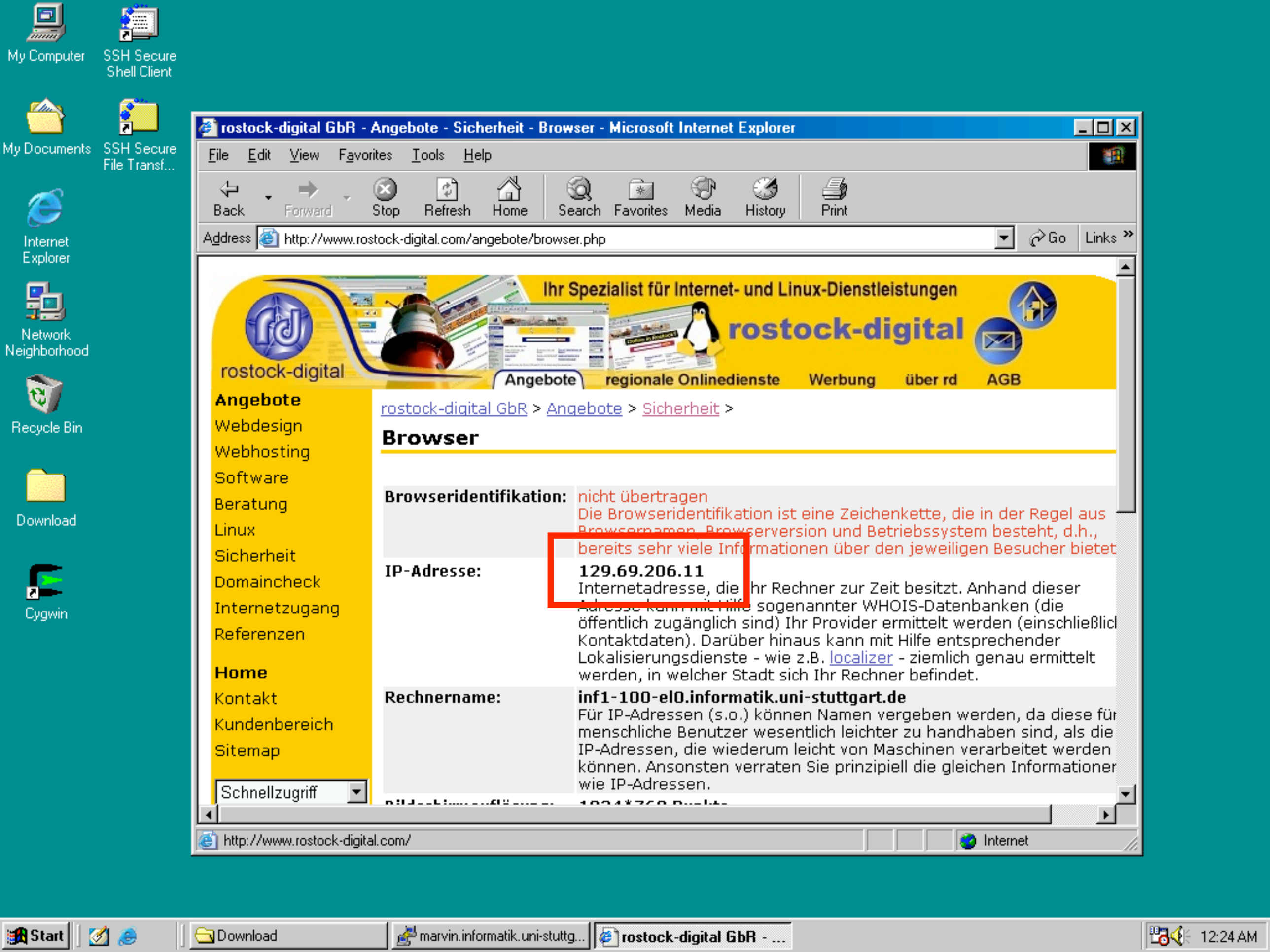

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Proxy
Telnet
Rlogin
SSH
Auth
Tunnels
Bugs
Options controlling SSH tunnelling
X11 forwarding
Enable X11 forwarding
X display location
localhost:0
Port forwarding
Local ports accept connections from other hosts
Remote ports do the same (SSH v2 only)
Forwarded ports:
Remove
L8080 www-cache.informatik.uni-stuttgart.de:3128
Add new forwarded port:
Source port
Add
Destination
Local
Remote
About
Open
Cancel

Proxy einstellen

- Der Proxy ist nun also über den Tunnel auf dem lokalen Port 8080 erreichbar
- Dies muss im Betriebssystem bzw. Browser entsprechend eingestellt werden
- HTTP-Proxy: localhost
- Port: 8080


My Computer
SSH Secure Shell Client
My Documents
SSH Secure File Transf...
Internet Explorer
Network Neighborhood
Recycle Bin
Download
Cygwin
rostock-digital GbR - Angebote - Sicherheit - Browser - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Print
Address http://www.rostock-digital.com/angebote/browser.php
Go Links
Ihr Spezialist für Internet- und Linux-Dienstleistungen
rostock-digital
Angebote regionale Onlinedienste Werbung über rd AGB
Angebote
Webdesign
Webhosting
Software
Beratung
Linux
Sicherheit
Domaincheck
Internetzugang
Referenzen
Home
Kontakt
Kundenbereich
Sitemap
Schnellzugriff
rostock-digital GbR > Angebote > Sicherheit >
Browser
Browseridentifikation: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Die Browseridentifikation ist eine Zeichenkette, die in der Regel aus Browsernamen, Browserversion und Betriebssystem besteht, d.h.,
IP-Adresse: 217.1.135.210
Provider: T-Online International AG, Waldstr. 3, 64331 Weiterstadt
Adresse kann mit Hilfe sogenannter WHOIS-Datenbanken (die öffentlich zugänglich sind) Ihr Provider ermittelt werden (einschließlic
Kontaktdaten). Darüber hinaus kann mit Hilfe entsprechender Lokalisierungsdienste - wie z.B. localizer - ziemlich genau ermittelt werden, in welcher Stadt sich Ihr Rechner befindet.
Rechnername: pD90187D2.dip.t-dialin.net
Für IP-Adressen (s.o.) können Namen vergeben werden, da diese für menschliche Benutzer wesentlich leichter zu handhaben sind, als die IP-Adressen, die wiederum leicht von Maschinen verarbeitet werden können. Ansonsten verraten Sie prinzipiell die gleichen Informationen
Done
Internet
Start
Download
marvin.informatik.uni-stuttg...
rostock-digital GbR - ...
12:24 AM


My Computer
SSH Secure Shell Client
My Documents
SSH Secure File Transf...
Internet Explorer
Network Neighborhood
Recycle Bin
Download
Cygwin
rostock-digital GbR - Angebote - Sicherheit - Browser - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Print
Address http://www.rostock-digital.com/angebote/browser.php
Go Links
rostock-digital
Angebote
Webdesign
Webhosting
Software
Beratung
Linux
Sicherheit
Domaincheck
Internetzugang
Referenzen
Home
Kontakt
Kundenbereich
Sitemap
Schnellzugriff
Browser
Browseride
IP-Adresse:
Rechnernan
AGB
Internet Options
Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: localhost
Port: 8080
Advanced...
Bypass proxy server for local addresses
OK
Cancel
Apply
Done
Internet
Start
Download
marvin.informatik.uni-stuttg...
rostock-digital GbR - ...
12:24 AM


My Computer
SSH Secure Shell Client
My Documents
SSH Secure File Transf...
Internet Explorer
Network Neighborhood
Recycle Bin
Download
Cygwin
rostock-digital GbR - Angebote - Sicherheit - Browser - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Print
Address http://www.rostock-digital.com/angebote/browser.php
Go Links
Ihr Spezialist für Internet- und Linux-Dienstleistungen
rostock-digital
Angebote regionale Onlinedienste Werbung über rd AGB
Angebote
Webdesign
Webhosting
Software
Beratung
Linux
Sicherheit
Domaincheck
Internetzugang
Referenzen
Home
Kontakt
Kundenbereich
Sitemap
Schnellzugriff
rostock-digital GbR > Angebote > Sicherheit >
Browser
Browseridentifikation: nicht übertragen
Die Browseridentifikation ist eine Zeichenkette, die in der Regel aus Browsernamen, Browserversion und Betriebssystem besteht, d.h., bereits sehr viele Informationen über den jeweiligen Besucher bietet
IP-Adresse: 129.69.206.11
Internetadresse, die Ihr Rechner zur Zeit besitzt. Anhand dieser Adresse kann mit Hilfe sogenannter WHOIS-Datenbanken (die öffentlich zugänglich sind) Ihr Provider ermittelt werden (einschließlich Kontaktdaten). Darüber hinaus kann mit Hilfe entsprechender Lokalisierungsdienste - wie z.B. localizer - ziemlich genau ermittelt werden, in welcher Stadt sich Ihr Rechner befindet.
Rechnername: inf1-100-el0.informatik.uni-stuttgart.de
Für IP-Adressen (s.o.) können Namen vergeben werden, da diese für menschliche Benutzer wesentlich leichter zu handhaben sind, als die IP-Adressen, die wiederum leicht von Maschinen verarbeitet werden können. Ansonsten verraten Sie prinzipiell die gleichen Informationen wie IP-Adressen.
http://www.rostock-digital.com/
Internet
Start
Download
marvin.informatik.uni-stuttg...
rostock-digital GbR - ...
12:24 AM

SSH als Proxy

- OpenSSH Kommandozeilenparameter -D <port>
- Damit läuft auf localhost:port ein SOCKS 4/5 Proxy
- localhost:port als SOCKS Proxy in den gewünschten Programmen eintragen
- Programme müssen SOCKS unterstützen
- Die Programme verhalten sich als wären sie direkt im Informatiknetz

VPN

- Virtual Private Network
- Der Rechner verhält sich, als wäre er im Informatiknetz
- Nutzungsordnung beachten!

VPN Client

- Cisco VPN Client (Linux, Windows, Mac OS X)
- http://www.informatik.uni-stuttgart.de/intern/vpn
- Profil/Zertifikat importieren
- Zertifikatspasswort: leer
- Benutzername + Passwort wie im Pool

Weitere Möglichkeiten

- VPN Client des Rechenzentrums (RUS Account notwendig)
- Einwählen über Modemzugang der Informatik (Modem/ISDN)

SSH mit Schlüsseln

- `ssh-keygen` generiert ein Schlüsselpaar
- Passwort ist sinnvoll (nicht jedes Mal eintippen: `ssh-agent`)
- z.B. `ssh-keygen -t dsa`
- Inhalt von `~/.ssh/id_dsa.pub` nach `~/.ssh/authorized_keys` auf dem Zielrechner kopieren

Konfigurationstipps

- ~/.ssh/config

```
Host marvin
        User username

Host gspc??
        User username
        ProxyCommand ssh marvin nc -w 1 %h %p
```

Troubleshooting

- `telnet <Hostname> <Port>`
- Ähnlich SSH, nur unverschlüsselt
- Wenn Server auf dem Port auf Anfragen wartet, bekommt man eine Telnet-Verbindung.
- So kann man sogar manuell die Befehle eines Protokolls eingeben (z.B. SMTP, POP3)

Fragen

http://fachschaft.informatik.uni-stuttgart.de/studium/infmisc