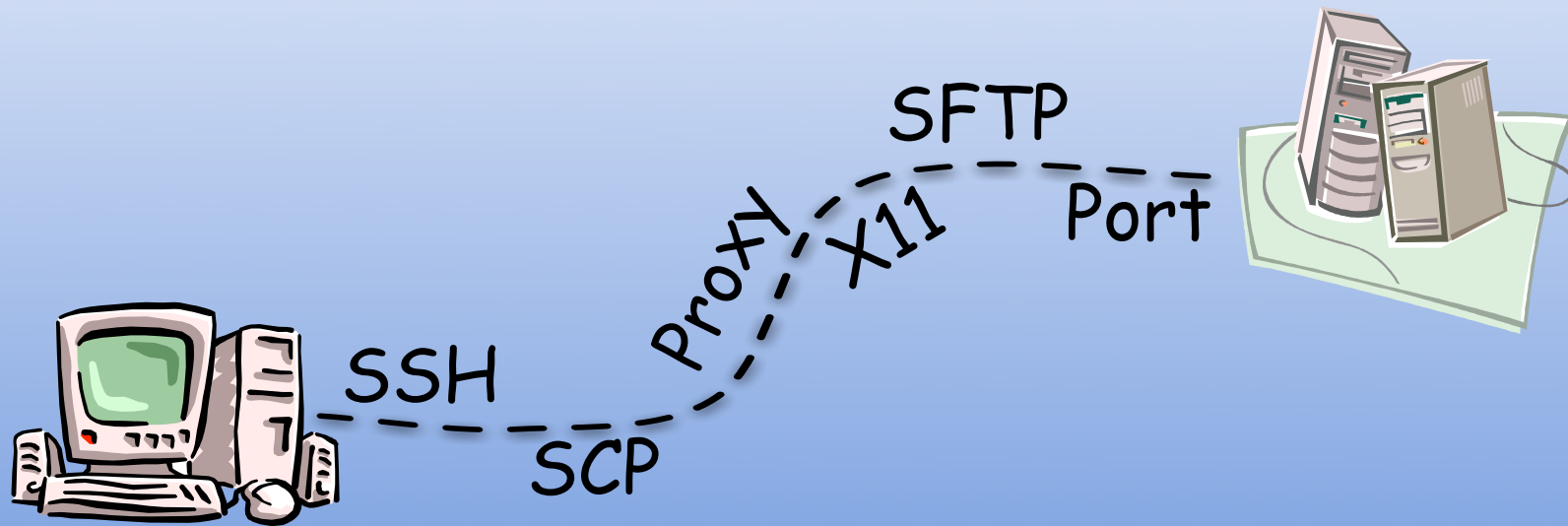


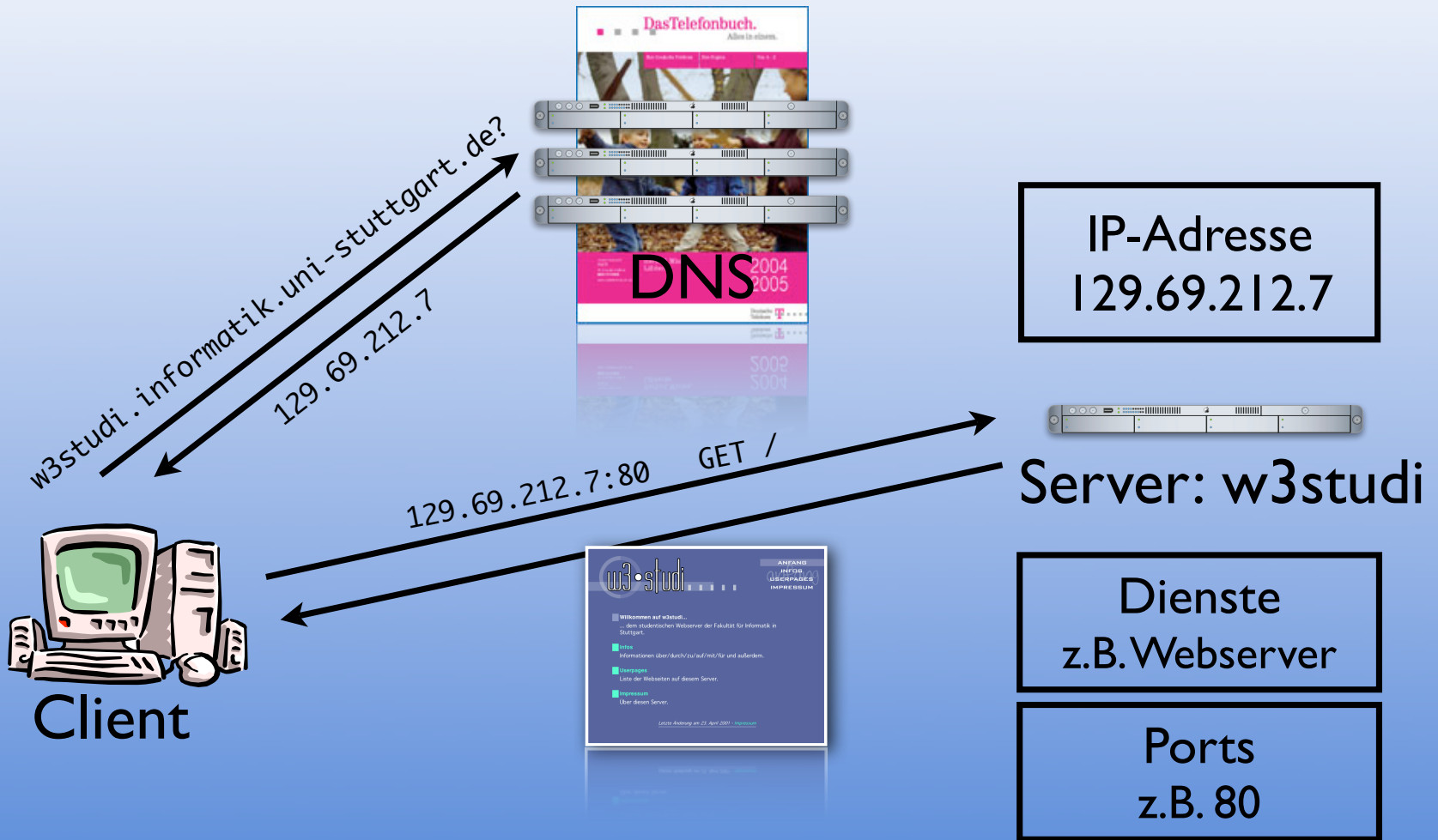
Remote Tools



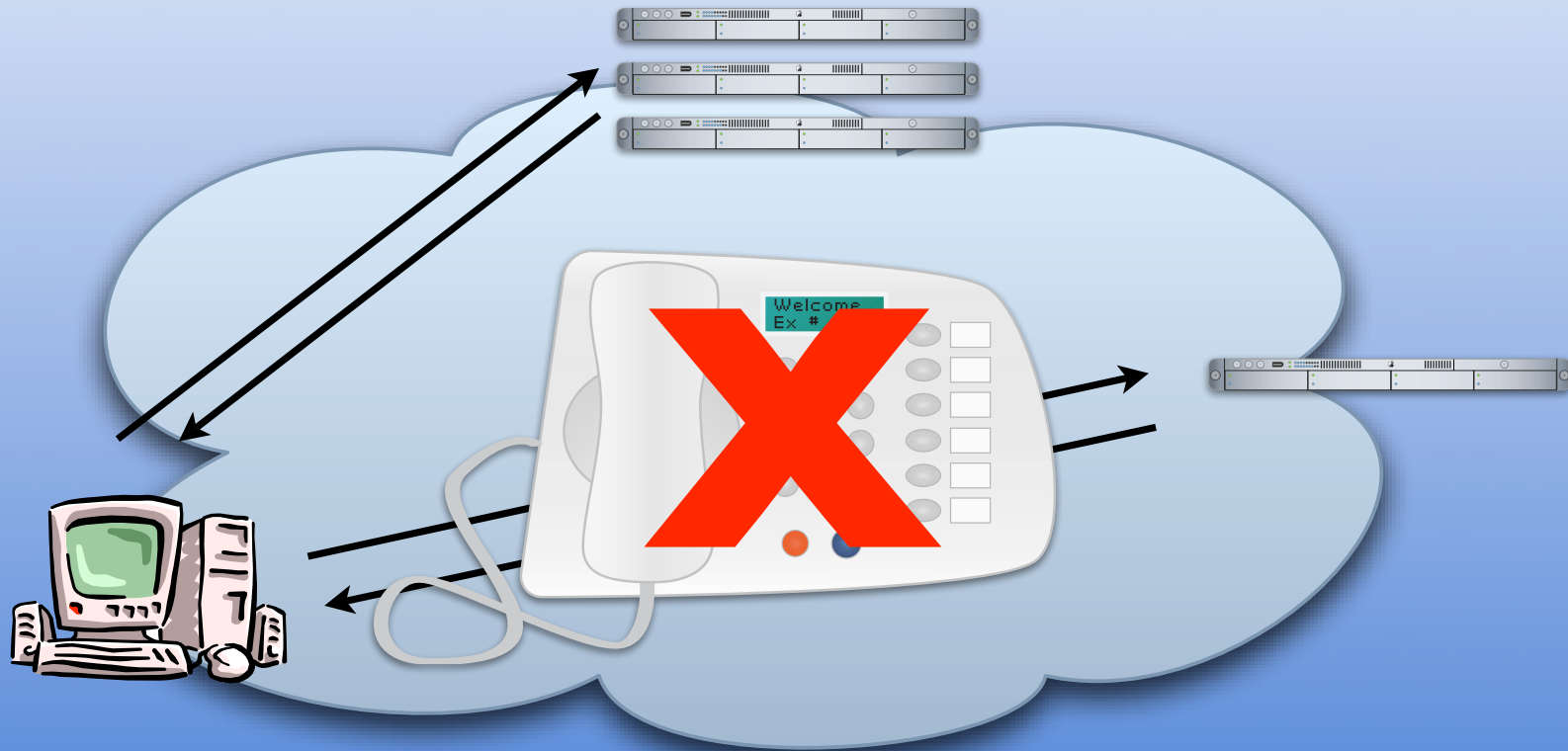
christina.zeeh@studi.informatik.uni-stuttgart.de

Inhalt

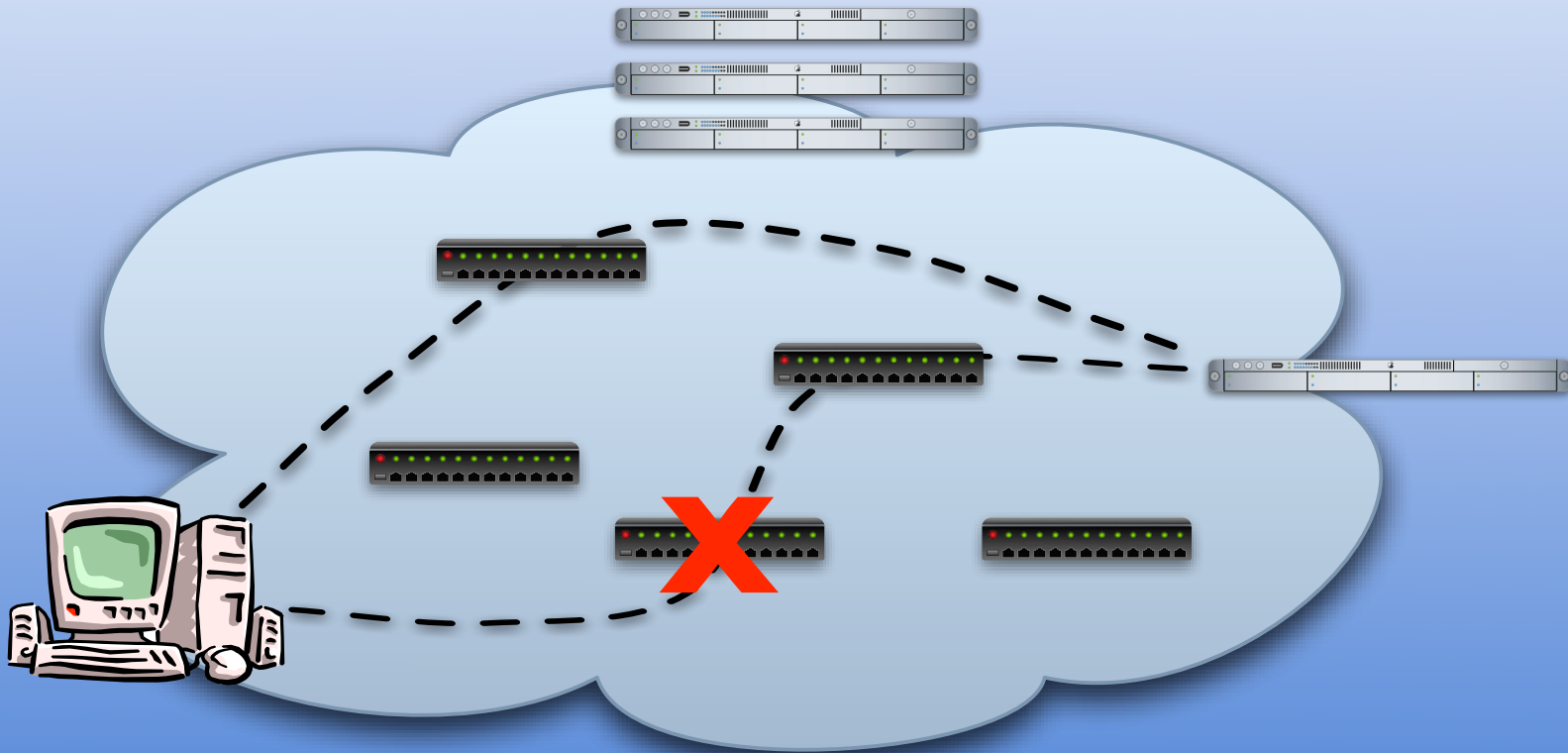
- Grundlagen
- SSH
 - Remote-Login auf marvin
 - Datentransfer
 - Graphische Anwendungen
 - Tunnel
- VPN
- SSH für Fortgeschrittene



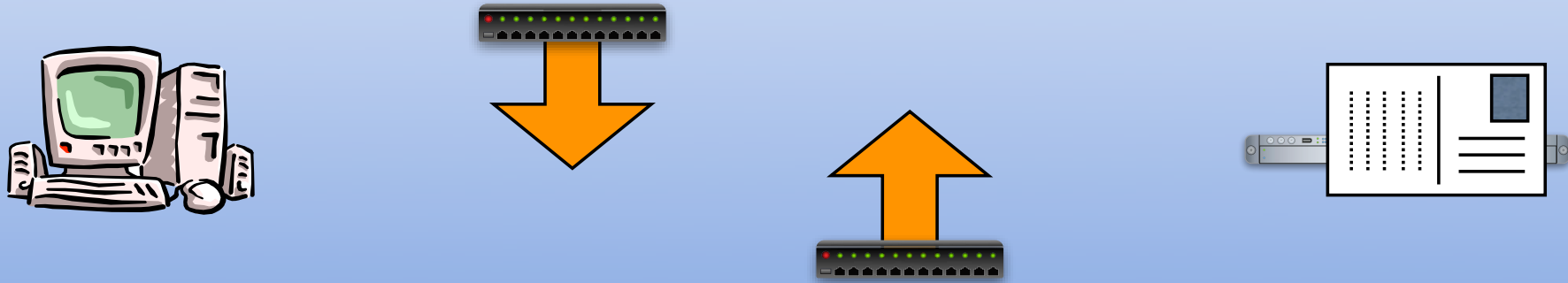
Problematik



Problematik



Problematik

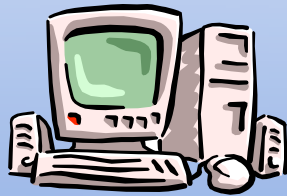


Nachricht kann

- gelesen
- verändert

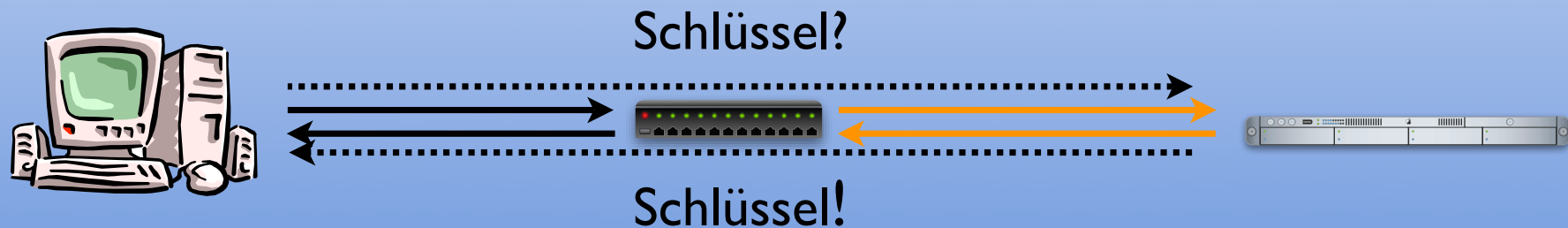
werden (Passwörter, Kreditkartennummern, Emails, ...)

Lösung: Verschlüsselung



Schlüsselaustausch?

- Verschiedene Verschlüsselungsverfahren (symmetrisch, asymmetrisch / Public Key)
- Schlüsseltausch (und damit das ganze System) kann durch “Man-in-the-Middle” kompromittiert werden



- Identität des Kommunikationspartners muss feststellbar sein: direkt (bekannter “Fingerabdruck”) oder indirekt durch vertrauenswürdigen Dritten (CA)

SSH

Secure Shell

Unsere Ziele

- Textorientierte Anwendungen von anderen Computern aus starten
- Datentransfer
- Graphische Anwendungen von anderen Computern aus starten
- Gesperrte Webseiten anschauen
- Mails über studi verschicken

SSH

- Programm zum (textorientierten) Remote-Login über eine verschlüsselte Verbindung
- Die verschlüsselte Verbindung kann auch für andere Zwecke verwendet werden, z.B. Dateitransfers, beliebige verbindungsorientierte Netzwerkdienste, ...
- Einzige Möglichkeit zum Login auf marvin
- Läuft auf Port 22

SSH Authentifizierung

- Benutzer zu Server: Passwort (bzw. Schlüssel)
- Server zu Benutzer: Hostkey (Schlüssel) bzw. dessen “Fingerprint” (gegen Man-in-the-Middle Angriff)
- Fingerprint von marvin (beim ersten Login prüfen!):

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

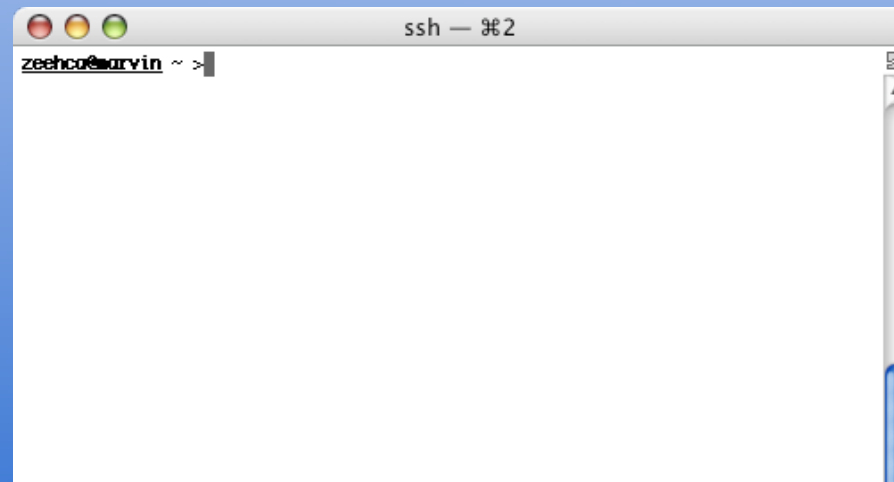
DSA be:b6:85:ee:ab:8e:bf:aa:f9:45:47:be:70:48:e8:7b
xutat-vusab-rumeh-zoryb-velen-rolok-recal-colig-gecar-
hasum-bixex

SSH Programme

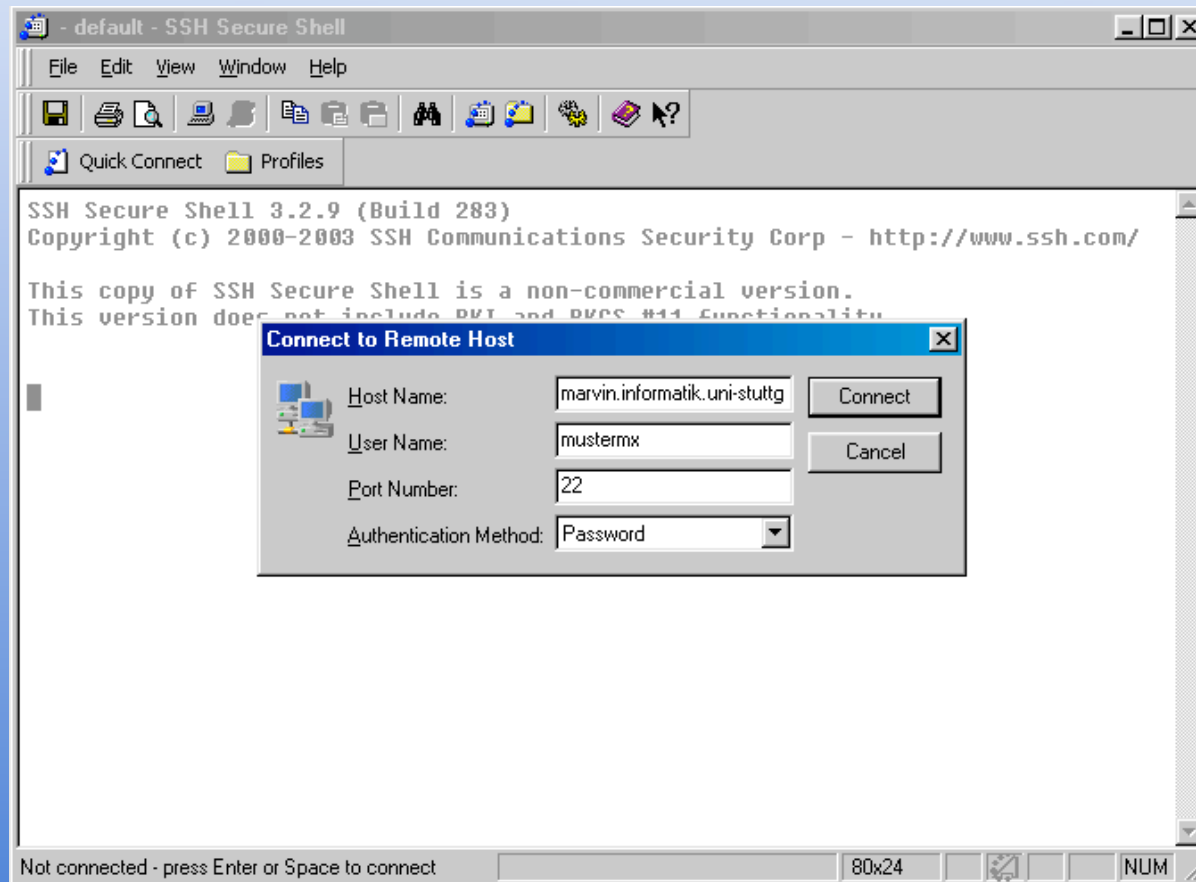
- Muss Protokollversion 2 unterstützen!
- OpenSSH (Linux ,Windows, Mac)
- Putty (Windows)
- SSH Communication Security (Windows u.a.)

Einfacher Login

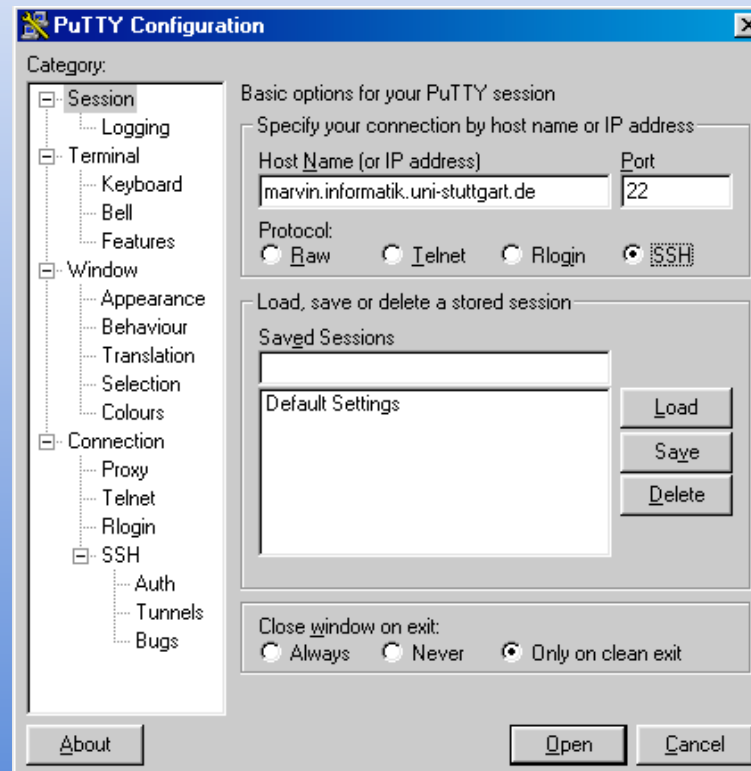
- `ssh benutzername@marvin.informatik.uni-stuttgart.de`
- Es wird gefragt, ob der unbekannte Hostkey akzeptiert werden soll \Rightarrow mit vorletzter Folie vergleichen.
- Benutzername, Passwort aus dem Pool
- Man erhält eine Shell wie im Pool unter Linux



SSH.com SSH



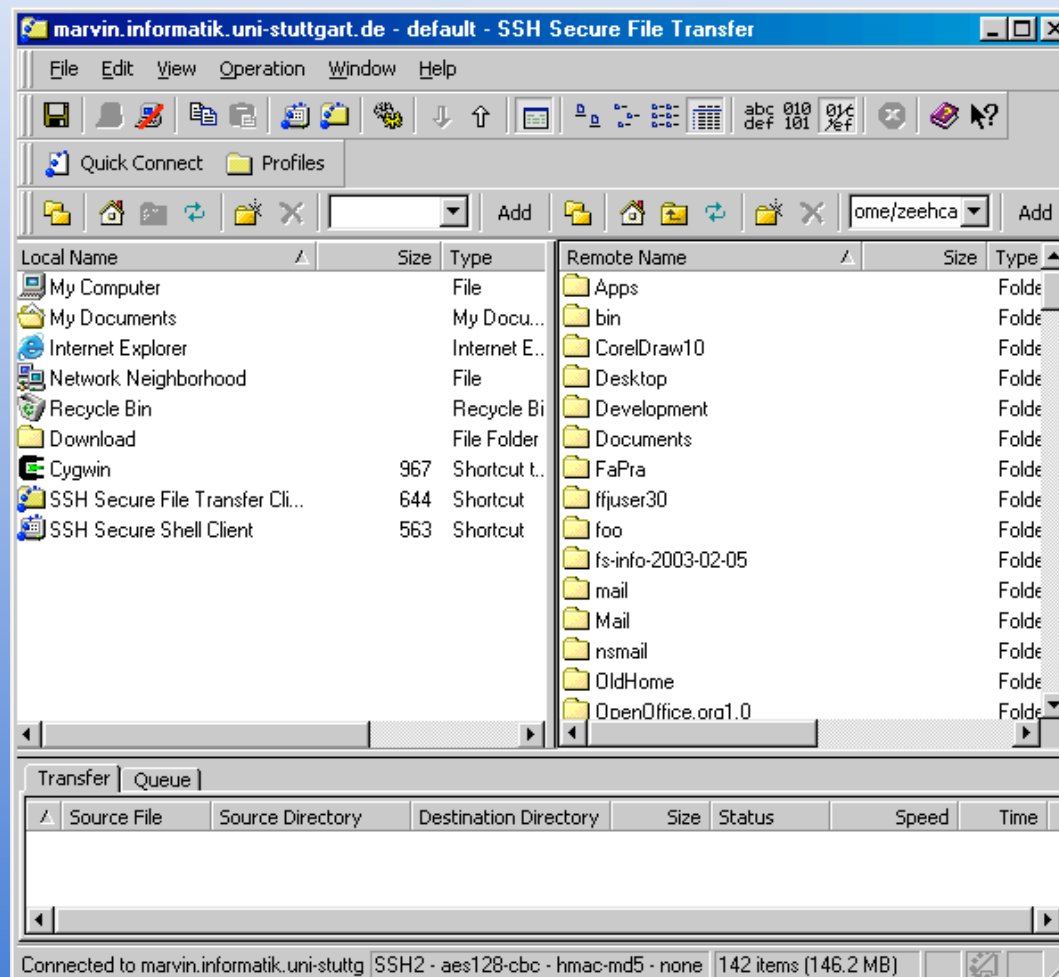
Putty



Datentransfer

- **Secure Copy (SCP)**
scp dateiname marvin.informatik.uni-stuttgart.de:.
scp -r verzeichnisname marvin.informatik.uni-stuttgart.de:.
- **Wildcards (*)** auf dem entfernten Rechner immer in Anführungszeichen, sonst interpretiert sie die lokale Shell
- **Secure FTP (SFTP)**
sftp marvin.informatik.uni-stuttgart.de
Befehle: put, get, ls, cd, lcd, mput, mget

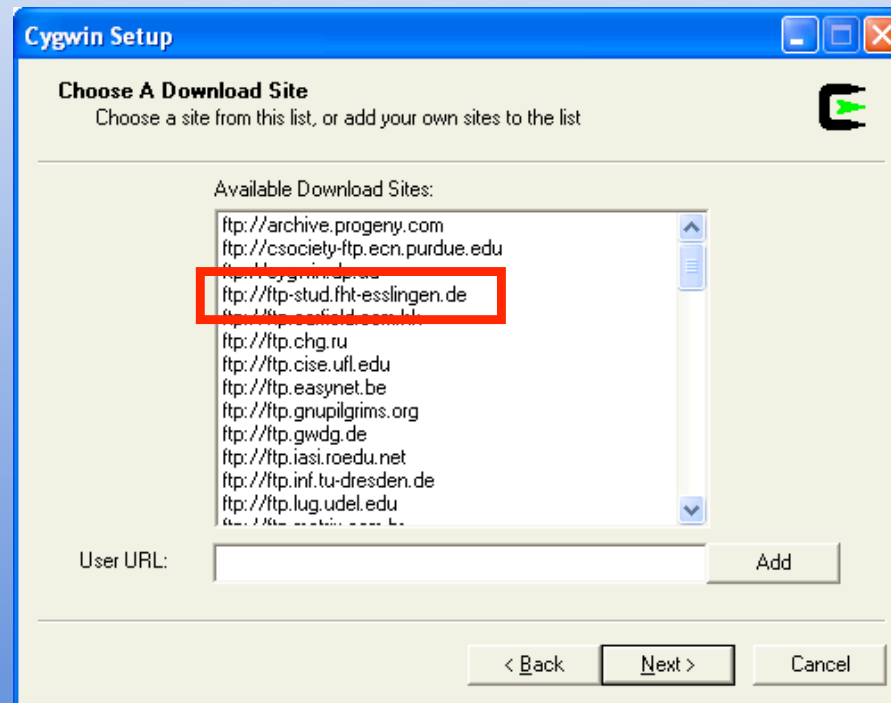
Grafisches SFTP (SSH.com)



GUI Anwendungen

- Voraussetzung: lokaler X-Server (Software zum Anzeigen graphischer Programme)
- Linux: bei Desktop-Installationen Standard
- Mac OS X: mitgeliefert, muss aber bei der Installation extra ausgewählt und bei Bedarf gestartet werden
- 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	n/a	n/a	xz: Combines z independ
		Skip	n/a	n/a	Xaw3d: A 3D version of fl
		4.2.0-1	<input checked="" type="checkbox"/>	n/a	XFree86-base: Cygwin/XI
		4.2.0-2	<input checked="" type="checkbox"/>	n/a	XFree86-bin: Bin
		Skip	n/a	n/a	XFree86-doc: Text docun
		4.2.0-1	<input checked="" type="checkbox"/>	n/a	XFree86-etc: Etc
		Skip	n/a	n/a	XFree86-f100: 100 dpi for
		Skip	n/a	n/a	XFree86-fcyr: Cyrillic fonts
		4.2.0-2	<input checked="" type="checkbox"/>	n/a	XFree86-fenc: Font enco
		4.2.0-2	<input checked="" type="checkbox"/>	n/a	XFree86-fnts: 75 dpi, misc

< Back Next > Cancel

Cygwin starten

- `C:\cygwin\usr\X11R6\bin\startxwin.bat`
- Man erhält ein Terminal-Fenster mit einer Bash-Shell

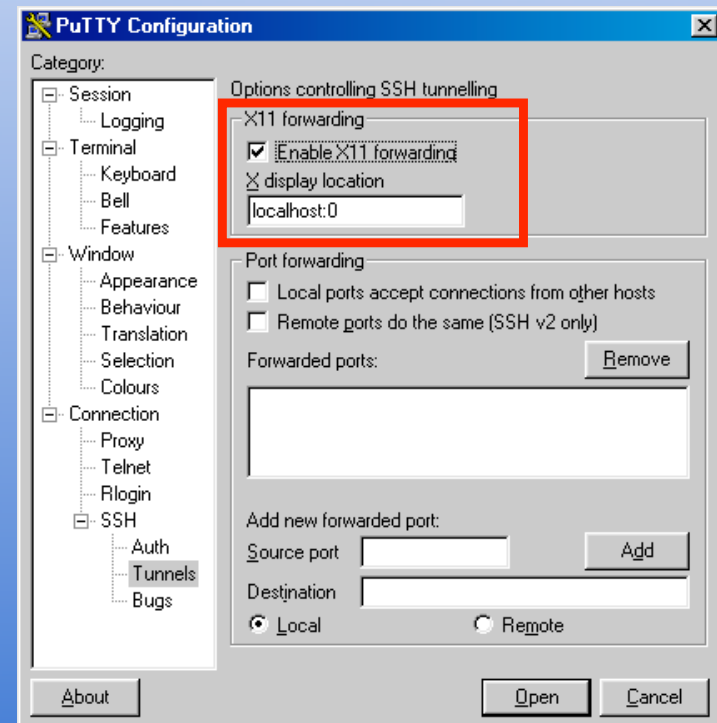
X11 Weiterleitung

- Ausgabe graphischer Programme wird ebenfalls über die verschlüsselte Verbindung übertragen und dann auf dem lokalen X-Server dargestellt

- X11 Weiterleitung in der SSH einschalten:

```
ssh -X benutzername@marvin...
```

- In der Shell auf marvin ganz normal Programme starten



```
X bash
bash-2.05b$
```

```
marvin.informatik.uni-stuttgart.de - PuTTY
zeehca@marvin ~ > xclock &
[1] 8662
zeehca@marvin ~ >
```



- recycle bin
- Download
- Cygwin

Arbeiten auf marvin

- Keinesfalls vollständige X-Sessions starten (einzelne Anwendungen sind ok)
- Rechenintensive längere (studienrelevante) Prozesse
 - nice verwenden
 - Mail an gspooladm@informatik.uni-stuttgart.de (nur von intern)

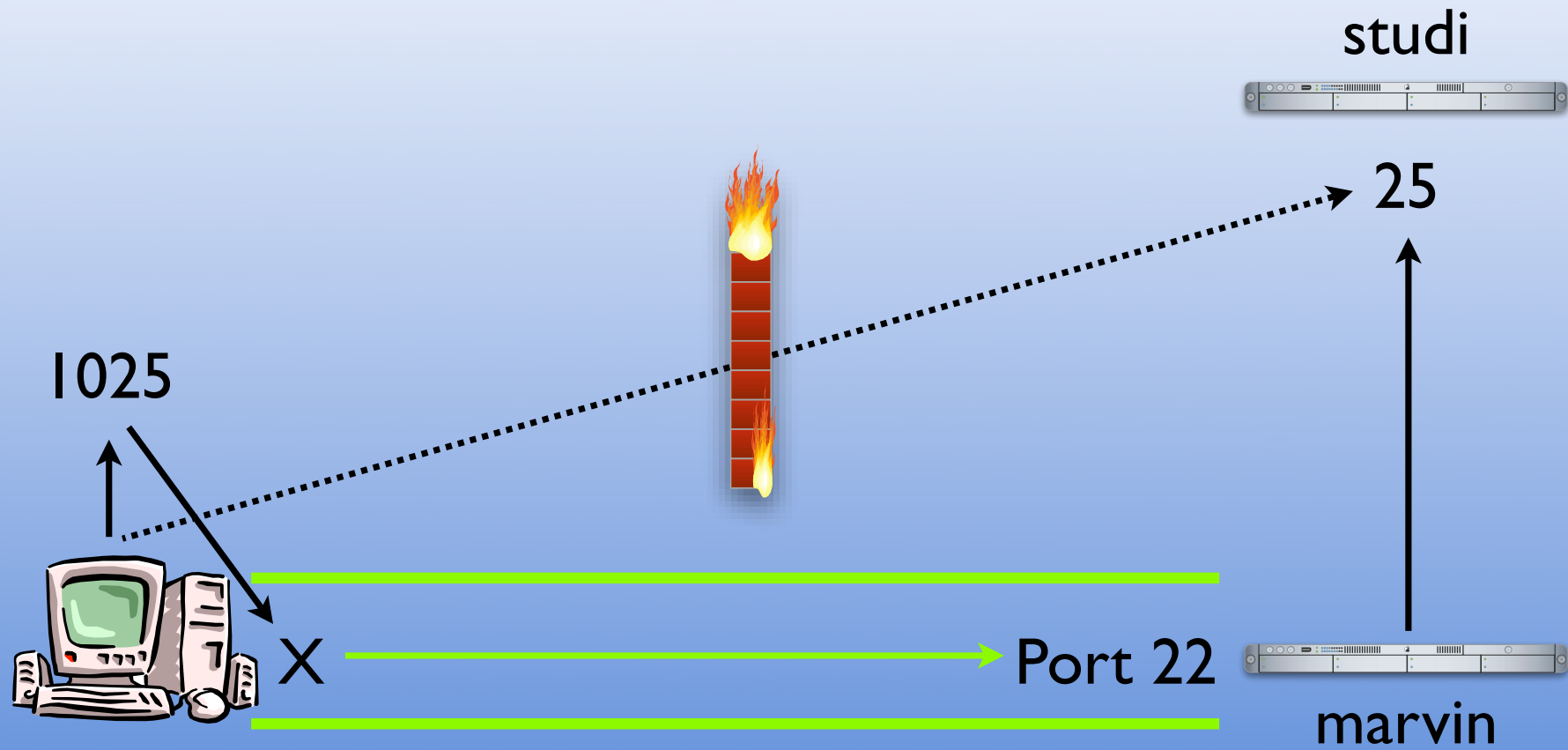
SSH

Tunnels und mehr

SSH-Tunnels

- Ziel: gesperrte Dienste im Intranet nutzen (Intranet-Webseiten, Mail über studi verschicken, ...)
- Lösung: Alle Anfragen werden über eine SSH-Verbindung verschlüsselt zu marvin geschickt, und von dort an den eigentlichen Zielrechner weitergeleitet
- Anfragen kommen für den Zielrechner von marvin
- Anwendungsprogramme müssen so konfiguriert werden, dass sie Daten über diesen "Tunnel" schicken, statt direkt ins Internet

SSH-Tunnel zu studi



Einfache Lösung

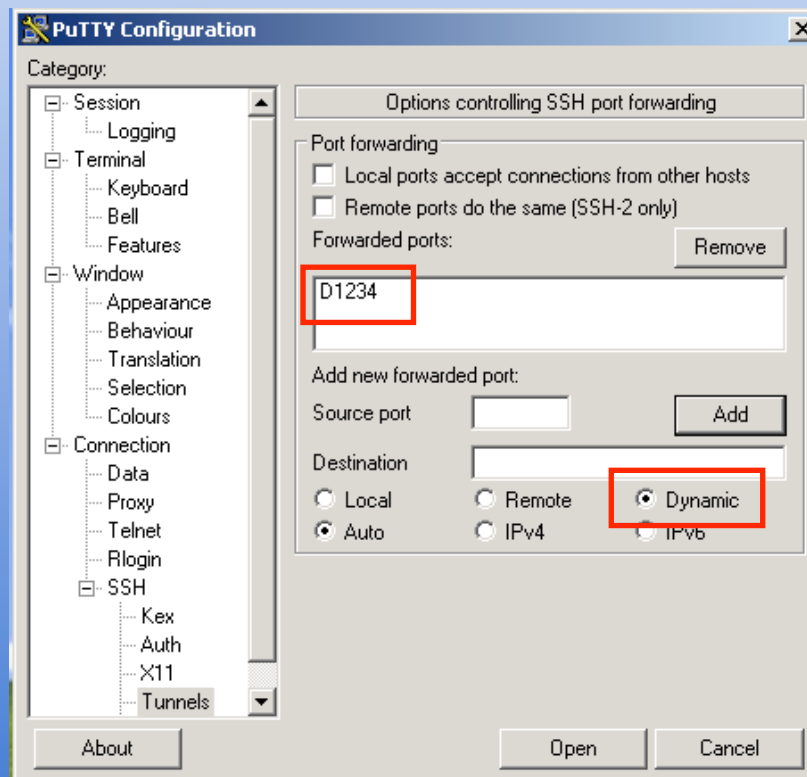
- Dynamische Portweiterleitungen (Tunnel)
- Funktioniert für nahezu alle TCP Verbindungen (z.B. Aufruf von Webseiten, Mailversand/-empfang, ...)
- Benötigt OpenSSH oder Putty
- SSH leitet alle Verbindungen an einen bestimmten Port des lokalen Rechners über die verschlüsselte Verbindung auf marvin weiter, dort werden sie an den korrekten Port des Zielrechners weitergeleitet

Einstellung SSH

- OpenSSH

```
ssh -D <Port> marvin.informatik.uni-stuttgart.de
```

- Putty



Einstellung Anwendung

- Im lokalen Anwendungsprogramm einstellen:
Socks 4/5 Proxy auf localhost + gewählter Port
- Die Anwendung verhält sich dann so, als wäre sie im Intranet der Informatik
- Nutzungsordnung beachten!
- Falls die Anwendung keine Proxies unterstützt helfen eventuell statische Portweiterleitungen ...

SMTP mit statischer Portweiterleitung

- Mails verschicken über Tunnel auf studi
- `ssh -L 1025:studi.informatik.uni-stuttgart.de:25 marvin.informatik.uni-stuttgart.de`

“Leite alle Daten, die am lokalen Rechner auf Port 1025 ankommen über die verschlüsselte SSH-Verbindung (Tunnel) auf marvin weiter, entschlüssle sie dort und leite sie weiter an den Rechner studi Port 25”

- Im Mailprogramm einstellen:
 - SMTP Server: localhost
 - Port: 1025

VPN

Virtual Private Network

VPN Client

- Alle Netzwerkzugriffe werden über eine verschlüsselte Verbindung ins Informatiknetz geleitet
- 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 (nächtliche Synchronisation)

Weitere Möglichkeiten

- VPN des Rechenzentrums (RUS) mit Cisco Client (andere Zertifikate, RUS Zugangsdaten verwenden!)
 - unterstützt auch OpenVPN
 - http://www.rus.uni-stuttgart.de/nks/netzwerkdienste/wlan_beschreibung/
- Einwählen über Modemzugang der Informatik (Modem/ISDN)

SSH

... für Fortgeschrittene

SSH mit Schlüsseln

- ssh-keygen generiert ein Schlüsselpaar
- Passwort ist sinnvoll, falls der Schlüssel in fremde Hände gerät (dafür reichen 10 Sekunden)
 - 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

Marvin als SSH-Gateway

- Viele (Abteilungs-)Rechner sind nur indirekt per SSH erreichbar (z.B. über marvin)
- ~/.ssh/config

```
Host marvin
    User username

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

Troubleshooting

Werkzeuge

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

Troubleshooting

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

Fragen



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