

# **Dokumentation CIP-Netzwerk**

Stefan Krumm<sup>1</sup>

25. Februar 2002

<sup>1</sup>Dieses Skript befindet sich im Zustand permanenter Umarbeitung. Es entstand unter Linux mittels L<sup>A</sup>T<sub>E</sub>X, dem grafischen L<sup>A</sup>T<sub>E</sub>X-Frontend.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Der Server</b>	<b>4</b>
2.1	Benutzerverwaltung . . . . .	4
2.1.1	Benutzer anlegen . . . . .	4
2.1.2	Benutzer löschen . . . . .	4
2.2	Drucken . . . . .	6
2.2.1	Fernwartung . . . . .	6
2.2.2	Drucker hinzufügen bzw. einrichten . . . . .	6
2.2.3	Accounting . . . . .	7
2.3	Benutzer und Dateifreigabe: Samba . . . . .	8
2.3.1	Hinzufügen von Workstations zur "Samba-Domäne" . . . . .	8
2.3.2	Fernwartung von Samba . . . . .	11
<b>3</b>	<b>Die Workstations</b>	<b>13</b>
3.1	Windows 2000 Clients . . . . .	13
3.1.1	Anmeldung . . . . .	13
3.1.2	Drucker . . . . .	13
3.1.2.1	Drucker hinzufügen . . . . .	13
3.2	Linux Clients . . . . .	14
3.2.1	Automatische updates und patch-Einspielung . . . . .	14
3.2.2	Anmeldung . . . . .	14
3.2.3	Drucker . . . . .	15
3.2.3.1	XPP . . . . .	15
<b>4</b>	<b>Sicherheit</b>	<b>17</b>
4.1	Firewalls . . . . .	17
4.1.1	Linux . . . . .	17
<b>5</b>	<b>Konfigurationsverwaltung</b>	<b>20</b>
5.1	Windows . . . . .	20
5.1.1	Spiegeln der Festplatte . . . . .	20
5.1.2	Schreiben der Konfiguration auf eine Workstation . . . . .	20
<b>6</b>	<b>Hilfreiches</b>	<b>23</b>
6.1	Linux für Dödel . . . . .	23
6.1.1	Programme compilieren . . . . .	23
6.1.2	Programme aus RPMs installieren . . . . .	23
6.1.3	Wichtige Befehle . . . . .	23
6.1.3.1	Unix-Befehle im Überblick . . . . .	24
6.1.3.2	Ändern von Zugriffsrechten . . . . .	24
6.1.3.3	Der Befehl df . . . . .	25
6.1.4	Laufende Prozesse anzeigen . . . . .	25
6.1.5	Manual-Pages . . . . .	25
6.1.6	Tabellen . . . . .	26

# List of Algorithms

1	Skript zum Anlegen eines neuen Benutzers. . . . .	5
2	Script zum erzeugen eines verschlüsselten Paßwortes . . . . .	5
3	Ausschnitt aus der Page_log-Datei von CUPS . . . . .	7
4	Ausschnitt aus /etc/passwd für Maschinen Accounts . . . . .	9
5	smb.conf unter /usr/local/samba/lib . . . . .	12
6	Logon Script für Windows Clients . . . . .	13
7	Skript zum Speichern des Windows Images. . . . .	21
8	Skript zum Schreiben des Windows Images auf eine Arbeitsstation. . . . .	22

# Kapitel 1

## Einführung

Diese Dokumentation beschreibt die Infrastruktur und die speziellen Anpassungen von Linux und Windows 2000 im CIP-Netzwerk. Es setzt Kenntnisse beider Betriebssysteme voraus. Darüberhinaus sollte der Benutzer sich mit SAMBA, CUPS, NIS und NFS beschäftigen. Entsprechende links werden im Anhang gesammelt werden.

Die abgedruckten Scripte sind teilweise von satzbedingten Zeilenumbrüchen betroffen. Bitte dies bei der Eingabe berücksichtigen.

Für aktuelle Konfigurationen, ToDos etc. wird auf den Ordner bei Geocip04 hingewiesen. Ansonsten gilt die Devise, die Tux unten vormacht:

RTFM - read the fucking manual



# Kapitel 2

## Der Server

Der Server läuft unter dem Linux Kernel 2.4. Aktuelle Distribution ist SuSE Professional 7.3.

### 2.1 Benutzerverwaltung

#### 2.1.1 Benutzer anlegen

Ein neuer Benutzer muß Linux, NIS und Samba bekannt gemacht werden. Daher können nicht die normalen tools von Linux und Windows verwendet werden. Zum anlegen existiert derzeit ein Skript names "cipuser". Es befindet sich unter /usr/sbin/ und kann von überall auf geoserv01 aufgerufen werden. Die Eingabe des Passwortes erfolgt ab sofort unsichtbar.

1. ssh geoserv01 (Linux) oder secure-shell-client unter Windows starten und zu geoserv als "root" verbinden.
2. "cipuser" eingeben
3. den Anweisungen am Bildschirm folgen und möglichst nicht vertippen.

Das skript erledigt folgendes:

1. erzeugt ein verschlüsseltes Paßwort für /etc/shadow
2. legt unter Linux einen neuen user mittels "useradd" an.
3. legt den Benutzer unter Samba an
4. führt ein make in /var/yp aus um die NIS-Datenbanken auf den neuesten Stand zu bringen.

#### 2.1.2 Benutzer löschen

Das Löschen eines Benutzers muss manuell erfolgen:

1. ssh geoserv01
2. oder: ssh root@131.188.152.231
3. vi /etc/passwd; dann die Zeile mit dem Benutzer mittels "dd" löschen, ESC drücken, dann":wq <return>"
4. vi /etc/shadow; dann die Zeile mit dem Benutzer mittels "dd" löschen, ESC drücken, dann":wq <return>"
5. vi /usr/local/samba/private/smbpasswd; dann die Zeile mit dem Benutzer mittels "dd" löschen, ESC drücken, dann":wq <return>"
6. Vorsicht: Benutzerdateien löschen: rm -r /home/benutzername VORSICHT, VORSICHT, VORSICHT!

---

**Algorithm 1** Skript zum Anlegen eines neuen Benutzers.

---

```
#!/bin/sh
echo "Bitte Benutzernamen eingeben: " read user
echo "Bitte Passwort eingeben: " tput setab 0 tput setaf 0
read pass
tput setab 9 #schaltet Hintergrund schwarz
tput setaf 0 #schaltet Schrift schwarz
p=`usr/sbin/encrypt $pass`
echo Das Passwort $pass ist verschlüsselt: $p
echo useradd -d /home/$user -s /bin/bash -p $p $user
useradd -d /home/$user -s /bin/bash -p $p $user
mkdir /home/$user
mkdir /home/$user/Daten
chown -R $user /home/$user
chmod -R gu=wrx,o-wrx /home/$user
chgrp -R root /home/$user
echo "Jetzt nochmal für Samba:"
smbpasswd -as $user $pass
cd /var/yp
make
```

---



---

**Algorithm 2** Skript zum Erzeugen eines verschlüsselten Passwortes.

---

```
#!/usr/bin/perl
# This Program was written by Lennart Hansen
# you got my permission, please send feedback to lennart@edb.ihnykf.dk

die "usage: $0 [user name] [password]" if $#ARGV != 0;
$password = $ARGV[0];
@saltair=split //,"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789./";
sub get_salt {
    srand();
    $iOff = int(rand($#saltair));
    $iOff2 = int(rand($#saltair));
    return join("", $saltair[$iOff], $saltair[$iOff2]);
}
$password = crypt($password, get_salt());
$salt = chr(int(rand(26))+65) . chr(int(rand(26))+65);
$password = crypt($password, $salt);
system("echo \"$password\"");
#system("echo \"$password\"");
```

---

## 2.2 Drucken

Als Druckerspooiler wird nicht der Berkley lpd eingesetzt sondern das “Common Unix Printing System”, *CUPS*. CUPS gestattet die Verwendung Druckereigener Einstellungen, Ansprache lokaler und Netzwerkdrucker über eine Vielzahl an Protokollen und es ermöglicht ein seitenweises Accounting.

Wir verwenden nicht die SuSE-Version von CUPS, sondern eine selbst compilierte. Die SuSE-CUPS hat sich bisher stets geweigert, ein Accounting durchzuführen. Bei einem Update der Distribution muß daher sichergestellt werden, daß die installierte Version nicht überschrieben wird, bzw. muß hinterher neu compiliert und installiert werden.

### 2.2.1 Fernwartung

Die Konfiguration von CUPS auf dem Server ist über ein Web-Frontend möglich. Der Aufruf lautet:

http://geoserv01:631

Benutzername ist “root” und das Paßwort entspricht dem generellen Systempaßwort.

### 2.2.2 Drucker hinzufügen bzw. einrichten

- Zunächst die unter 2.2.1 angeführten Schritte durchführen.



Abbildung 2.1: Neuer Drucker in Cups

- Dann “Printer” bzw. “Manage Printers” anwählen und auf der folgende Seite unten “Add printer” wählen.



Abbildung 2.2: Druckernamen und Beschreibung eingeben

- Druckernamen und Beschreibung eingeben



Abbildung 2.3: Anschluß wählen

- Den Anschluß wählen. Hier wird der Anschluß an einen HPJetDirect-Port gezeigt.
- Hersteller auswählen



Abbildung 2.4: Anschluß konfigurieren

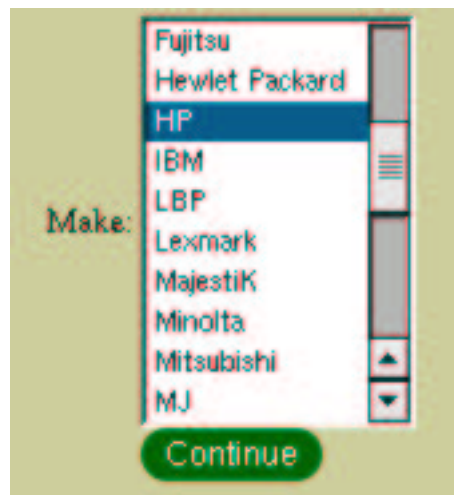


Abbildung 2.5: Hersteller wählen

- Druckertreiber auswählen. Hierbei etwas experimentieren. Bei manchen funktioniert das Accounting nicht. Manchmal ist der allgemeine Treiber besser als der für das spezielle Modell: Laserjet anstatt von Laserjet5000GN.
- Zurück auf die Druckerseite und Drucker konfigurieren. Unbedingt das Seitenformat von "letter" auf "DIN A4" umstellen. Speichern.
- Fertig!

### 2.2.3 Accounting

CUPS schreibt die Druckjobs in eine Datei unter `/var/log/cups/page_log`.

---

#### Algorithm 3 Ausschnitt aus der Page\_log-Datei von CUPS

---

```
HP2500_Tinte_Geologie remroot 125 [21/Nov/2001:13:30:25 +0100] 1 1
Plotter Root 126 [21/Nov/2001:13:47:03 +0100] 1 1
HP5000A4 remroot 156 [03/Dec/2001:09:46:17 +0100] 1 1
HP5000A4 remroot 157 [03/Dec/2001:13:23:44 +0100] 1 1
```

---

The `page_log` file lists each page that is sent to a printer. Each line contains the following information:

```
printer user job-id date-time page-number num-copies job-billing
DeskJet root 2 [20/May/1999:19:21:05 +0000] 1 0 acme-123
```



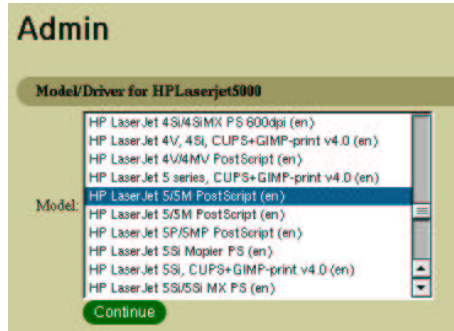


Abbildung 2.6: Druckertreiber wählen

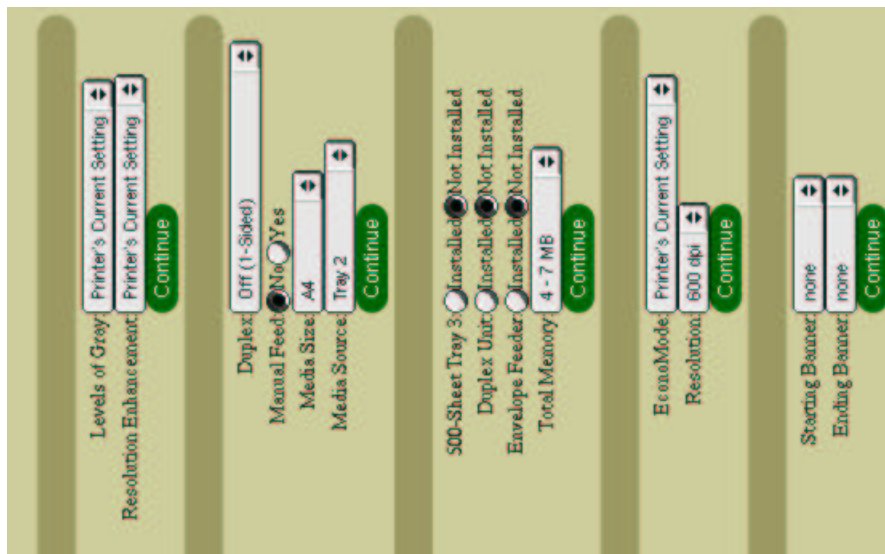


Abbildung 2.7: Konfiguration des Druckers. Seitenformat anpassen.

The *printer* field contains the name of the printer that printed the page. If you send a job to a printer class, this field will contain the name of the printer that was assigned the job. The *user* field contains the name of the user (the IPP requesting-user-name attribute) that submitted this file for printing. The *job-id* field contains the job number of the page being printed. Job numbers are reset to 1 whenever the CUPS server is started, so don't depend on this number being unique! The *date-time* field contains the date and time of when the page started printing. The format of this field is identical to the data-time field in the access\_log file. The page-number and num-pages fields contain the page number and number of copies being printed of that page. For printer that can not produce copies on their own, the num-pages field will always be 1. The *job-billing* field contains a copy of the job-billing attribute provided with the IPP create-job or print-job requests or "-" if none was provided.

## 2.3 Benutzer und Dateifreigabe: Samba

Das installierte Samba-Paket ist selbst kompiliert. D.h. bei einem Update möglichst kein Samba von der Stange installieren. Warum? Die Verzeichnisse, die benutzt werden, sind bei SuSE und dem Original Samba unterschiedlich. Es liegen dann evtl. Programme doppelt vor, was zu unerwünschten Effekten führen kann.

Basis-Verzeichnis unseres Samba's ist /usr/local/samba

### 2.3.1 Hinzufügen von Workstations zur "Samba-Domäne"

Jede Workstation, die unter Windows auf den Samba-Server als PDC zugreifen will, braucht einen sogenannten "Maschinen Account". In /etc/passwd muss die Maschine auftauchen, d.h. sie muss per Hand dort eingetragen werden. Der Rechnername bekommt ein \$-Zeichen angehängt. Wichtig ist, daß aus Sicherheitsgründen Home directory und shell ungültig sein müssen ("dev/null").

---

**Algorithm 4** Ausschnitt aus /etc/passwd für Maschinen Accounts

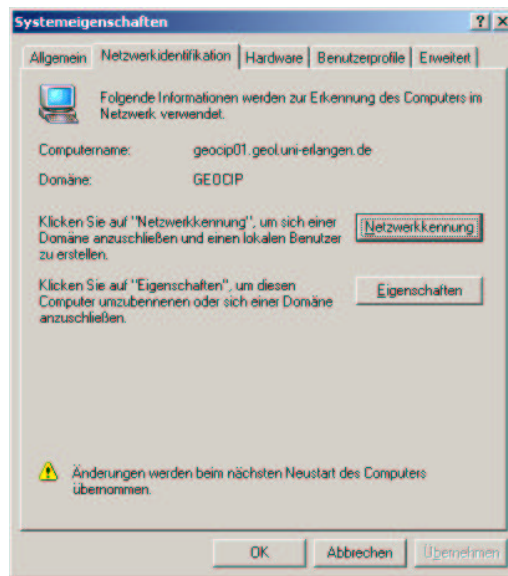
---

```
#normaler account:  
test2:x:517:100:./home/test2:/bin/bash  
#Maschinenaccount  
geocip02$:x:518:100:./dev/null:/dev/null
```

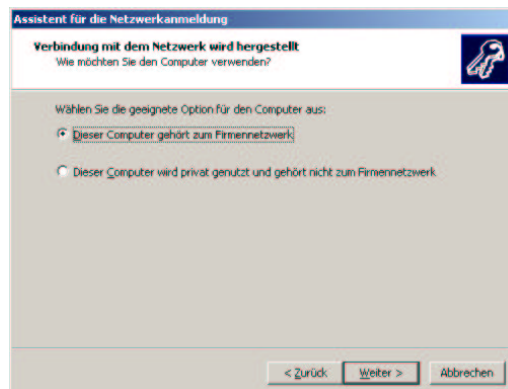
---

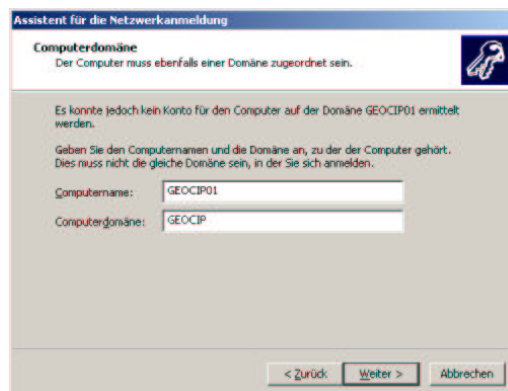
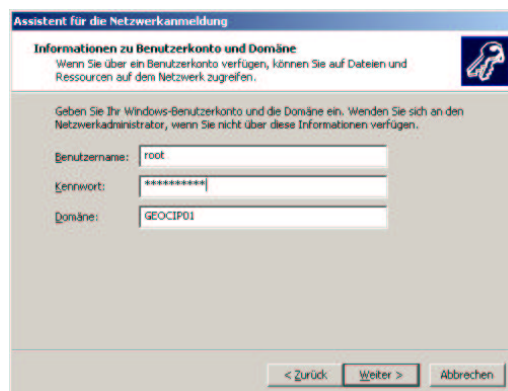
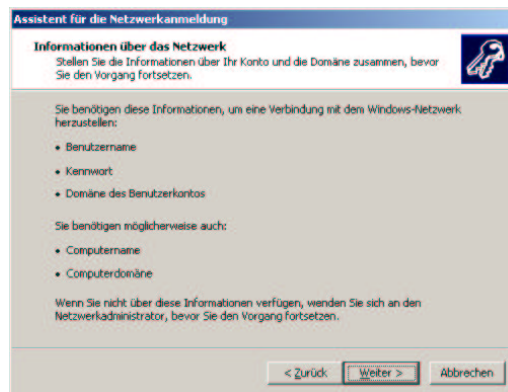
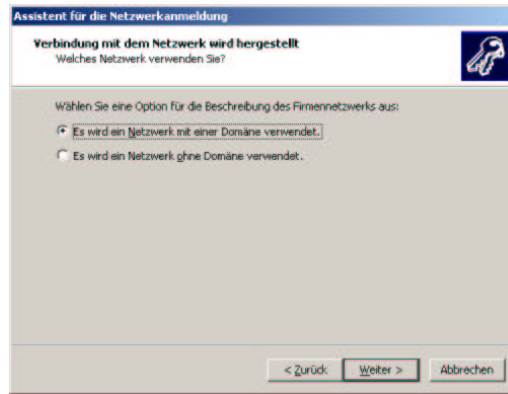
Anschliessend muß noch die smbpasswd-Datei angeglichen werden:

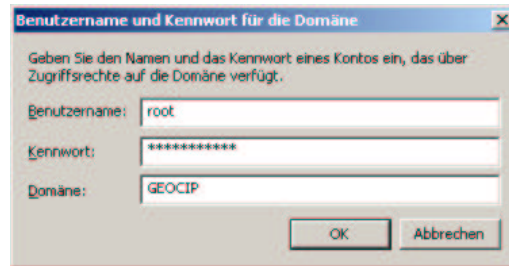
```
smbpasswd -ma MeinMaschinenName
```



- Auf der Workstation muß dann "Systemsteuerung->System->Netzwerkidentifikation" aufgerufen werden.







Benutzername und Kennwort für die Domäne

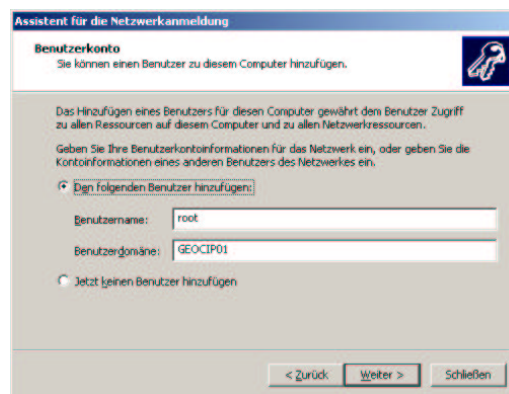
Geben Sie den Namen und das Kennwort eines Kontos ein, das über Zugriffsrechte auf die Domäne verfügt.

Benutzername: root

Kennwort: \*\*\*\*\*

Domäne: GEOCIP

OK Abbrechen



Assistent für die Netzwerkanmeldung

**Benutzerkonto**  
Sie können einen Benutzer zu diesem Computer hinzufügen.

Das Hinzufügen eines Benutzers für diesen Computer gewährt dem Benutzer Zugriff zu allen Ressourcen auf diesem Computer und zu allen Netzwerkressourcen.

Geben Sie Ihre Benutzerkontoinformationen für das Netzwerk ein, oder geben Sie die Kontoinformationen eines anderen Benutzers des Netzwerkes ein.

Die folgenden Benutzer hinzufügen:

Benutzername: root

Benutzerdomäne: GEOCIP01

Jetzt keinen Benutzer hinzufügen

< Zurück Weiter > Schließen

### 2.3.2 Fernwartung von Samba

Hier hilft das tool "swat". Es kann über "http://geoserv01:901" aufgerufen werden. Bitte keine Benutzer hinzufügen oder Paßwörter mittels swat ändern. Da neben der Samba-Benutzerdatenbank auch die Linux und NIS-Datenbank synchronisiert werden muß, sind wir gerade dabei, eine entsprechende Skript- bzw. WWW-Lösung zu implementieren. Als Benutzername bitte "root" und das übliche Paßwort eingeben.

---

**Algorithm 5** smb.conf unter /usr/local/samba/lib

---

# Samba config file created using SWAT # from laue-neu.geol.uni-erlangen.de (131.188.152.250)

# Date: 2001/11/29 15:09:14

```
# Global parameters
[global]
workgroup = GEOCIP
netbios name = GEOSERV01
server string = Samba 2.2.0, der CIP-Testserver
encrypt passwords = Yes
log level = 1
log file = /usr/local/samba/var/log.%m
name resolve order = wins lmhosts host bcst
logon script = start.bat logon path = \\%N\homes\%u
logon drive = H:
logon home = \\homeserver\%u
domain logons = Yes
os level = 99
lm announce = True
preferred master = True
domain master = True
wins proxy = Yes
wins support = Yes
remote announce = 131.188.153.255/geocip
hosts allow = 131.188.152.0/255.255.255.0,131.188.153.0/255.255.255.0
printing = cups
[netlogon]
path = /usr/local/samba/lib/netlogon write list = ntadmin,root
[profiles]
path = /export/smb/ntprofile read only = No create mask = 0600 directory mask = 0700
[homes]
comment = Home directories read only = No
[tmp]
comment = So much space...
path = /tmp
read only = No
guest ok = Yes
[Cip]
path = /export/cip
read only = No
[Alles]
comment = Nur für Chefs
path = /
read only = No
[home]
path = /home
read only = No
[Plotter]
path = /tmp
printable = Yes
[HP5000A4]
path = /tmp
printable = Yes
...
```

---

# Kapitel 3

## Die Workstations

### 3.1 Windows 2000 Clients

#### 3.1.1 Anmeldung

Die Authentifizierung der Benutzer erfolgt über Samba. Der Server spiegelt Windows vor, daß er ein "Primärer Domänen Controller", PDC, im Windows-Netzwerk ist. Die Anmeldedomäne heißt "Geocip". Das Anmeldeskript richtet Druckerverbindungen ein und legt Laufwerk U: auf das Datenverzeichnis unter /home/benutzername/Daten. Das Skript findet sich unter:

```
/usr/local/samba/lib/netlogon/start.bat
```



---

**Algorithm 6** Logon Script für Windows Clients

---

```
net use * /delete /y
mkdir \\geoserv01\home%\USERNAME%\Daten
net use u: \\geoserv01\home%\USERNAME%\Daten /y
```

---

Windows 2000 holt sich den Verzeichnisbaum unter "Eigene Dateien" vom Server und spielt die Änderungen beim Ausloggen wieder auf den Server zurück. Leider bleibt bis dato noch die lokale Kopie dieser Daten auf den Workstations erhalten und müllt diese nach und nach zu.

#### 3.1.2 Drucker

Die Drucker sind als Samba-Clients, also wie Windowsnetzwerk-Drucker installiert. Es wird prinzipiell nicht der Windows-treiber, sondern der Universale PostScript-Treiber von Adobe verwendet (auch für nicht PostScript-Drucker). Für überformatige und Farbdrucker wird ein entsprechendes PPD-file bei der Installation des Adobe-Treibers angegeben.

##### 3.1.2.1 Drucker hinzufügen

Die Druckerschlange muß bereits auf dem Server unter cups installiert und über samba freigegeben sein. Der Adobe-Treiber-Installer ruht auf geoserv01 unter /export/cip/programme/windows/install/drv/HP/ die Datei heißt Adobe\_universal\_postscript\_t. Dort findet sich auch das gepackte PPD-Archiv als .exe.

1. Adobe\_universal\_postscript\_treiber.exe starten
2. Bei der Frage nach dem Anschluß irgendeinen beliebigen Anschluß wählen (Abb. )
3. Bei der Frage nach dem Druckertyp weitermachen oder PPD-File von Festplatte laden
4. Drucker entsprechend benennen und Programm beenden
5. Unter Windows als *lokaler* Administrator im Druckerfenster den Drucker mit rechter Maustaste anklicken und auf "Eigenschaften" gehen.
6. Den Schalter "Anschluß hinzufügen" drücken und "local port" wählen.
7. Samba-URL des Druckers eingeben: \\131.188.152.234\MeinDrucker

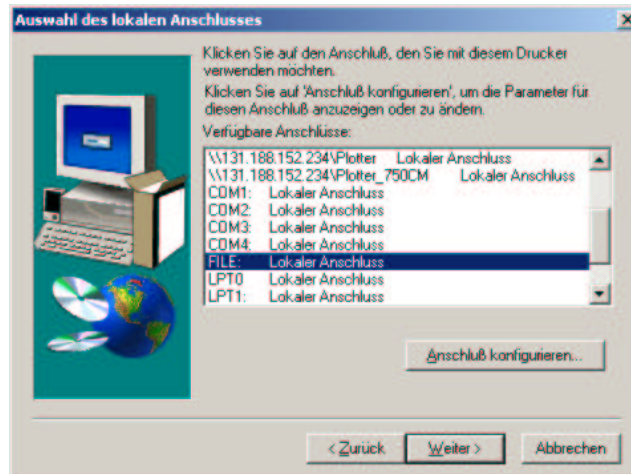


Abbildung 3.1: Installation des Adobe Universal-Treibers

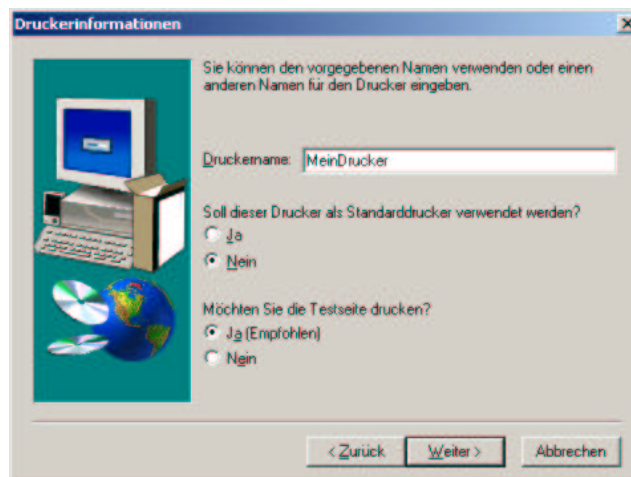


Abbildung 3.2: Eingabe des Druckernamens

## 3.2 Linux Clients

### 3.2.1 Automatische updates und patch-Einspielung

Die Workstations bringen sich automatisch auf den neuesten Softwarestand. Insbesondere betrifft dies die Firewall. Der Mechanismus ist wie folgt:

- Das zu installierende Paket wird als RPM auf geoserv01 unter /home/update/ abgelegt: z.B. /home/update/dragonfw.rpm
- Der client führt beim Booten ein unter /etc/rc.d/rc3.d/S12update (Booten in Konsole) und /etc/rc.d/rc5.d/S12update (Booten in X) abgelegtes Skript aus, das nach /home/update (über NFS gemountet) verzweigt und dort ein rpm -U \*.rpm ausführt. Dadurch werden installierte und zu installierende Pakete verglichen. Falls das Paket nicht installiert ist oder nicht in der neuesten Fassung vorliegt, wird es installiert.
- Das ist alles....  
;-)

### 3.2.2 Anmeldung

Die Benutzeranmeldung erfolgt über NIS, die Home-directories werden per NFS automatisch gemountet, so daß jedem Benutzer an jeder Maschine immer die gleiche Umgebung zur Verfügung steht. Der Zugriff ist auf die Subnetze der Geologie (131.188.152.255) und Geographie (131.188.153.255) beschränkt.

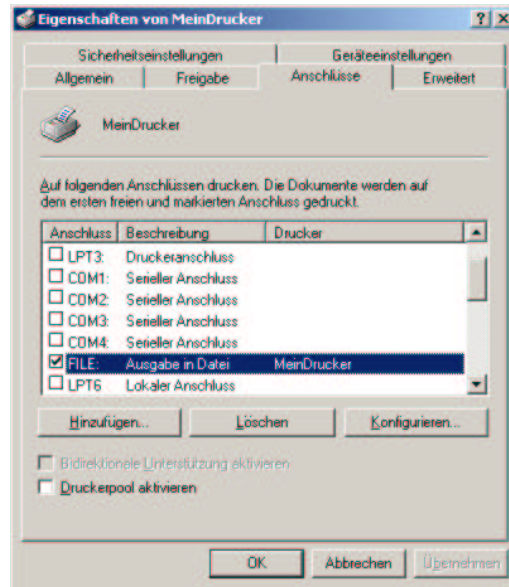


Abbildung 3.3: Anschluß hinzufügen.

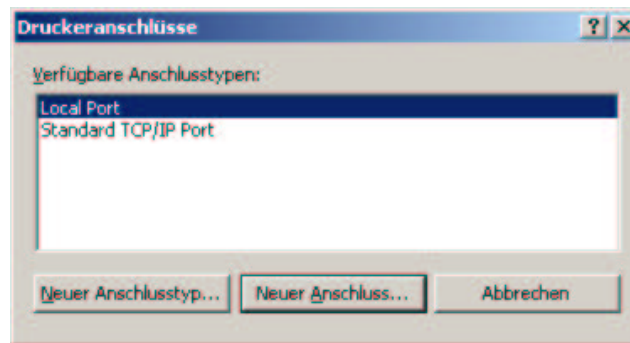


Abbildung 3.4: Anwahl des Anschlusses

### 3.2.3 Drucker

#### 3.2.3.1 XPP

xpp ist ein grafisches tool, mit dem Jobs an bestimmte Drucker geschickt werden können. Es gestattet auch die Auswahl verschiedener Druckeroptionen (Papier, Orientierung, Auflösung) und erlaubt es ferner, mehrere Seiten auf einem Blatt auszudrucken.



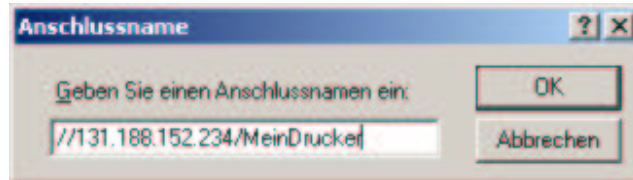
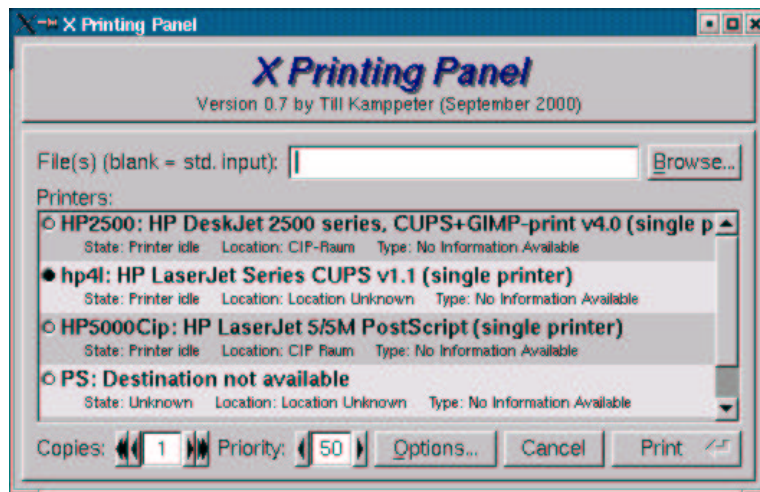


Abbildung 3.5: Eingabe der Samba-URL des Druckers



xpp Hauptfenster

# Kapitel 4

## Sicherheit

### 4.1 Firewalls

#### 4.1.1 Linux

Auf den Workstations und dem Server läuft iptables/netfilter als Firewall. Dies ist die Standardfirewall des Kernel 2.4. Das Skript wird bei booten gestartet und erkennt ob es auf dem Server oder der Workstation läuft und schaltet dadurch unterschiedliche Dienste frei. Grundprinzip ist: Erst alles sperren und dann einzeln freischalten. Es werden nur eingehende Verbindungen überwacht, Trojaner hätten also eine Chance. Unser Skript ist eine Anpassung der dragonfw von Marcel Ritter (RRZE).

```
#!/bin/sh

### BEGIN INIT INFO
# Provides:    dragonfw
# Required-Start: $network syslog
# Required-Stop:
# Default-Start: 3 5
# Default-Stop:
# Description: Firewall
### END INIT INFO
#
# init.d/smb

./etc/rc.status
./etc/rc.config

# Determine the base and follow a runlevel link name.
base=${0##*/}
link=${base#[SK][0-9][0-9]}

# Force execution if not called by a runlevel directory.
test $link = $base && START_DRAGONFW=yes
test "$START_DRAGONFW" = "yes" || exit 0

IPTABLES=/usr/sbin/iptables

test -x $IPTABLES || exit 0

LOCALIP=$(echo $IFCONFIG_0 | awk '{ print $1 }')
BROADCAST=$(echo $IFCONFIG_0 | awk '{ print $3 }')
NETMASK=$(echo $IFCONFIG_0 | awk '{ print $5 }')
LOCALNET="$LOCALIP/$NETMASK"

rc_reset

case "$1" in
start)
echo "LOCAL IP: $LOCALIP"
echo "BROADCAST: $BROADCAST"
echo "NETMASK: $NETMASK"
echo "LOCALNET: $LOCALNET"

echo -n "Starting DragonFW : "
rc_status -v

#these arguments are for flushing the chains and for deleting own created ones
$IPTABLES -F
$IPTABLES -X
```

```

$IPTABLES -N DROPTLOG      # creating target that logs and drops
$IPTABLES -A DROPTLOG -j LOG
$IPTABLES -A DROPTLOG -j DROP

$IPTABLES -P INPUT DROP    # dropping any INPUT that is not specifically accepted

    # "DEFAULT POLICY"
$IPTABLES -P FORWARD DROP # dropping everthing
$IPTABLES -P OUTPUT ACCEPT

#####setting INPUT chain
# important is to have the rules in this order. The package travel from
# top to bottom until it matches a rule/chain. If no rule matches it will be
# logged in the log-chain.

#####setting for lo device
$IPTABLES -A INPUT -i lo -j ACCEPT #excepting everything that goes into the
    #loopback device

#####settings for RELATED or ESTABLISHED connections
# all related or already established connenctions are accepted.
# This way any replies from outgoing packages/connection will be accepted.
# Important is to use tcp AND udp protocols-(because of the ypbind)
# Keep these rules at the top of the whole chain. This is important because that
# way incoming RELATED packages will not have to go through the
# whole chain, which would result in slowing down the connection
$IPTABLES -A INPUT -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
$IPTABLES -A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
$IPTABLES -A INPUT -p icmp -m state --state RELATED,ESTABLISHED -j ACCEPT

#####settings for icmp protocols
$IPTABLES -A INPUT -p icmp -j DROP
# echo-request are only those packages which answer on ping.
# That way one can ping outside, but you can not be pinged.
# $IPTABLES -A INPUT -p icmp -icmp-type echo-reply -j ACCEPT

#####settings for incoming allowed SYN calls
# allowing only 20 syn calls per minute. This reduces the risk of a syn-flood
# attacks-allowing (only) incoming syn calls from port 22/ssh
# REMINDER: the limit only kicks in after the limit-burst which is
# 5 has been reached
$IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --dport 22 -j ACCEPT

##### reject connections to identd
# some services try to check the remote user by contacting identd
# this authentication can be faked in a very simple manner, so it's
# useless anyway. However FTP/POP logins may wait for some 30s if
# we simply drop it, so we send them an error message
#$IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --dport 113 -j REJECT

##### Stefan's Ergaenzung

#Geographen und Geologen duerfen Samba shares teilen!
###??? Kann man vermutlich nicht aus der SuSE rc.config auslesen??
#evtl. vielleicht ein include-file einlesen?
LOCAL_NETWORKS="131.188.153.0/255.255.255.0 131.188.152.0/255.255.255.0"

for ip in $LOCAL_NETWORKS; do

    #####reject for ident
    #geht schneller fuer POP als auf TO zu warten, nur lokal
    $IPTABLES -A INPUT -p TCP --syn -m limit --limit 10/s --source $ip --dport auth -j REJECT

    #X-Verbindungen lokal
    $IPTABLES -A INPUT -p TCP --syn -m limit --limit 10/s --source $ip --dport 5999:6003 -j ACCEPT

    #####Samba, auch für neue Anfragen
    #beschränkt auf eigene Subnetze
    $IPTABLES -A INPUT -p tcp --syn -m limit --limit 30/s --source $ip --dport 137:139 -j ACCEPT
    $IPTABLES -A INPUT -p udp -m limit --limit 30/s --source $ip --dport 137:139 -j ACCEPT

    #####NFS
    #
    $IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --source $ip --dport 2049 -j ACCEPT
    $IPTABLES -A INPUT -p udp -m limit --limit 10/s --source $ip --dport 2049 -j ACCEPT

    #####Der Server hat noch nfs, swat und cups zu bieten!
    if [ $LOCALIP == "131.188.152.250" ];
    then
        #####NFS
        $IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --source $ip --dport 2049 -j ACCEPT
        $IPTABLES -A INPUT -p udp -m limit --limit 10/s --source $ip --dport 2049 -j ACCEPT

        #####swat

```

```

$IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --source $ip --dport 901 -j ACCEPT

#####cups
$IPTABLES -A INPUT -p tcp --syn -m limit --limit 10/s --source $ip --dport 631 -j ACCEPT

echo "Enabling nfs, cups and swat for subnet $ip!"

fi

done ###loop over all subnets

#####Bloede broadcasts versenken....
$IPTABLES -A INPUT -d 255.255.255.255/32 -j DROP

#####HP Printserver Broadcasts vernichten
$IPTABLES -A INPUT -d 224.0.1.60 -j DROP

#####Router? Broadcasts vernichten
$IPTABLES -A INPUT -d 224.0.0.0/16 -j DROP

##### Ende der Aenderung

#####settings for logged SYN calls
# logging every SYN call. Except those wich are already accepted
# by the above chain. In this case every SYN is logged that is not ssh.
# This means someone wants to log in on a port that is not permitted. BAD BOY.
# see logfile for prefix-"illegal_SYN_call"
$IPTABLES -A INPUT -p tcp --tcp-flags ALL SYN -m limit --limit 10/m -j DROPTLOG

#####settings for broadcast/router messages
# drop those messages without logging
$IPTABLES -A INPUT -d $BROADCAST -s $LOCALNET -m state --state NEW,INVALID -j ACCEPT
$IPTABLES -A INPUT -d 224.0.0.1 -s $LOCALNET -m state --state NEW,INVALID -j ACCEPT

#####settings for state rules
# new ore invalid connection will be dropped. Unless they were not
# allowed in an rule above.
$IPTABLES -A INPUT -d $LOCALNET -m state --state NEW,INVALID -j DROPTLOG

#####what to do with unwanted things
# log every illegal connection
$IPTABLES -A INPUT -m state --state NEW,INVALID -j DROPTLOG

#####settings for LOG
# All packages which were not refered to one of the above rules are
# beeing logged here. This could be good for troubleshooting, if any rules are
# missing. Or someone whants trouble! See logfile for prefix-"everything_else"
$IPTABLES -A INPUT -j DROPTLOG
;;

stop)
echo -n "Shutting down DragonFW :."
$IPTABLES -F
$IPTABLES -X DROPTLOG
$IPTABLES -X
$IPTABLES -P INPUT ACCEPT #dropping any INPUT that is not specifcly accepted
# "DEFAULT POLICY"
$IPTABLES -P FORWARD ACCEPT #dropping everthing
$IPTABLES -P OUTPUT ACCEPT

rc_status -v
;;

restart|reload)
$0 stop
$0 start
rc_status
;;

status)
echo -n "Checking DragonFW :."
$IPTABLES -L
rc_status -v
;;
*)
echo "Usage: $0 {start|stop|status|restart|reload}"
exit 1
;;
esac
rc_exit

```

# Kapitel 5

## Konfigurationsverwaltung

### 5.1 Windows

Der Rechner Geocip04 ist der Referenzrechner für Windows. Auf ihm dürfen nur mit äußerster Vorsicht Änderungen vorgenommen werden. Die Windowspartition liegt als /dev/hda1 vor und ist 8723 MB groß. Nach Installation von Programmen bzw. Änderungen an der Konfiguration, muß ein neues Festplattenimage auf den Server geschrieben werden. Bitte achten Sie darauf, kein altes Image mit einer ungeprüften Konfiguration zu überschreiben.

#### 5.1.1 Spiegeln der Festplatte

Das Spiegeln erfolgt in nachfolgenden Schritten:

1. Starten Sie eine der Linux-Installation am betreffenden Rechner.
2. Loggen Sie sich als "root" ein.
3. Mounten Sie den Server:  
smbmount //geoserv01/cip /mnt  
es gibt hierfür einen aliasBefehl: mg
4. Wechseln Sie nach /mnt/system/konfigurationen
5. Geben Sie den Befehl "./createWinImage" ein. Das untenstehende Skript wird ausgeführt. Es zeigt eine Liste der bereits vorhandenen Images und fragt nach dem Namen für das zu schreibende Image.
6. Sperren Sie den Bildschirm und legen Sie den "Arbeitsplatz besetzt"-Zettel auf die Tastatur.
7. Nachdem das Image geschrieben wurde, stellen Sie bitte den Desktophintergrund von rot auf blau um. Dies dient den anderen Systemverwaltern als Hinweis, daß Referenzsystem und Image auf dem neuesten Stand sind. Sollten Sie die Konfiguration geändert haben gilt analog: Desktophintergrund auf rot setzen ("Konfiguration neuer als Image!").

#### 5.1.2 Schreiben der Konfiguration auf eine Workstation

Das Zurückschreiben ähnelt dem Vorgehen beim Erstellen des Images und erfolgt in nachfolgenden Schritten:

1. Starten Sie eine der Linux-Installation am betreffenden Rechner.
2. Loggen Sie sich als "root" ein.
3. Mounten Sie den Server:  
smbmount //geoserv01/cip /mnt  
es gibt hierfür einen aliasBefehl: mg
4. Wechseln Sie nach /mnt/system/konfigurationen
5. Geben Sie den Befehl "./writeWinImage" ein. Das untenstehende Skript wird ausgeführt.

---

**Algorithm 7** Skript zum Speichern des Windows Images.

---

```
#!/bin/bash
echo Folgende images gibts:
ls w*.gz
echo Bitte geben Sie den Namen ein:
read filename
echo schreibe: $filename

# schreibe das image
# gib das Datum aus, damit wir sehen, wie lange es dauert!
date
# dd kopiert binär, das Image wird on-the-fly mit gzip komprimiert
echo Schreibe Gigabyte 1 und 2
dd if=/dev/hda1 bs=1M count=2000 | gzip -cv > $filename-1.gz
date
echo Schreibe 3-4 Gigabyte
dd if=/dev/hda1 bs=1M count=2000 skip=2000 | gzip -cv > $filename-2.gz
date
echo Schreibe 5-6 Gigabyte
dd if=/dev/hda1 bs=1M count=2000 skip=4000 | gzip -cv > $filename-3.gz
date
echo Schreibe 7-8 Gigabyte
dd if=/dev/hda1 bs=1M count=2000 skip=6000 | gzip -cv > $filename-4.gz
date
echo Schreibe letzten Rest
dd if=/dev/hda1 bs=1M count=723 skip=8000 | gzip -cv > $filename-5.gz
date
echo Fertig!
```

---

6. Wählen Sie aus der Liste der bestehenden Images das zu restaurierende aus.
7. Sperren Sie den Bildschirm und legen Sie den "Arbeitsplatz besetzt"-Zettel auf die Tastatur.
8. Nachdem das Image geschrieben wurde, stellen Sie bitte den Desktophintergrund von rot auf blau um. Dies dient den anderen Systemverwaltern als Hinweis, daß Referenzsystem und Image auf dem neuesten Stand sind. Sollten Sie die Konfiguration geändert haben gilt analog: Desktophintergrund auf rot setzen ("Konfiguration neuer als Image!").
9. In den Netzwerkeigenschaften der Workstation muß dann der Rechnername und die IP-Adresse gesetzt werden.
10. Unter Systemsteuerung->System muss der Rechner schließlich noch der Domäne Geocip hinzugefügt werden. Näheres hierzu mit Bildchen demnächst an dieser Stelle.

---

**Algorithm 8** Skript zum Schreiben des Windows Images auf eine Arbeitsstation.

---

```
#!/bin/bash
echo Folgende Images stehen zur Verfügung: ls -l win*.gz
echo Bitte geben Sie den Namen der zu zurückschreibenden Datei an: read dateiname
echo Ich schreibe $dateiname
echo Ich schreibe die Windows-Partition
# Zeige Datum an: date
# entpacke die Datei und schreibe sie auf die 1. Partition
echo schreibe Datei $dateiname-1 auf die 1. Partition
gunzip -cv $dateiname-1.gz | dd of=/dev/hda1 bs=1M
date echo schreibe Datei $dateiname-2 auf die 1. Partition
gunzip -cv $dateiname-2.gz | dd of=/dev/hda1 seek=2000 bs=1M date
echo schreibe Datei $dateiname-3 auf die 1. Partition
gunzip -cv $dateiname-3.gz | dd of=/dev/hda1 seek=4000 bs=1M date
echo schreibe Datei $dateiname-4 auf die 1. Partition
gunzip -cv $dateiname-4.gz | dd of=/dev/hda1 seek=6000 bs=1M date
echo schreibe Datei $dateiname-5 auf die 1. Partition
gunzip -cv $dateiname-5.gz | dd of=/dev/hda1 seek=8000 bs=1M
date
echo habe fertig!
```

---

# Kapitel 6

## Hilfreiches

### 6.1 Linux für Dödel

#### 6.1.1 Programme compilieren

Programme kommen meist gepackt als komprimiertes “tar”-Archive. Kennlich wird dies an den Extensions “tar.gz” oder “tgz”.

Um ein Programm namens “MeinProgramm.tar.gz” zu entpacken und zu installieren, wird folgendermaßen vorgegangen:

1. wenn noch nicht als root eingelogt: su
2. tar -xzf MeinProgramm.tar.gz
3. cd MeinProgramm
4. ./configure
5. make all
6. make install
7. Freuen!

#### 6.1.2 Programme aus RPMs installieren

RPM steht für “Red Hat Package Manager”. RPM enthalten die zu installierenden Programme aber auch Zusatzinformation wie Abhängigkeiten, benötigte Bibliotheken etc.. Auf dem Rechner wird eine RPM-Datenbak geführt, die Auskunft über die installierten Pakete gibt.

Die einfachste Methode ein RPM zu installieren lautet:

```
rpm -i MeinProgramm.rpm
```

Darüberhinaus gestatten “yast” und die grafische Variante “yast2” Auswahl und Installation von RPMs.

#### 6.1.3 Wichtige Befehle

Copyright

Dieses Abschnitt ist geistiges Eigentum der SuSE GmbH.

Es darf als Ganzes oder in Auszügen kopiert werden, vorausgesetzt, dass sich dieser Copyright-Vermerk auf jeder Kopie befindet.



### 6.1.3.1 Unix-Befehle im Überblick

Die wichtigsten Befehle sind überblicksartig in Tabelle aufgelistet; optionale Parameter stehen in '[]':

**cd** verz Wechsel ins Unterverzeichnis verz.

**cd** .. Wechsel in das übergeordnete Verzeichnis.

**cd** /verz Wechsel ins Verzeichnis /verz.

**cd** [ ] Wechsel ins Benutzerverzeichnis.

**cp** quelldatei zieldatei kopiert quelldatei nach zieldatei.

**ln** [-s] bezug name erzeugt im aktuellen Verzeichnis den [symbolischen] Link name, der auf die Datei bezug zeigt. name gibt den Pfad an, in dem die (eigentlich im aktuellen Verzeichnis) gesuchte Datei gefunden werden kann. Nur symbolische Links können über Dateisysteme hinweg gesetzt werden. Mit Hilfe symbolischer Links können auch Verzeichnisse "gelinkt" werden.

**ls** [verz] listet alle Dateien und Verzeichnisse im Verzeichnis verz auf (nur Dateinamen).

**ls** -l [verz] listet alle Dateien und Verzeichnisse im Verzeichnis verz auf (ausführliche Anzeige im Langformat); ohne Parameter: der Inhalt des aktuellen Verzeichnisses.

**ls** -a [verz] zeigt auch die versteckten Dateien an; (z.B. ~/.xinitrc).

**mkdir** neuesverz erzeugt das Verzeichnis neuesverz.

**less** datei zeigt eine Datei seitenweise an (Vorblättern mit der Leertaste, Rückwärtsblättern mit b ).

**mv** vondatei nachdatei verschiebt eine Datei oder benennt sie um.

**rm** datei Löscht datei (auch Links!).

**rm** -r verz Löscht das Verzeichnis verz rekursiv (mit Unterverzeichnissen).

**rmdir** verz Löscht das Verzeichnis verz (wenn leer).

**In** Tabelle finden Sie einige Befehle, die Suchaufgaben erledigen helfen.

**find** . -name "datei" sucht in allen Unterverzeichnissen des aktuellen Verzeichnisses nach datei.

**find** . -name "\*emil\*" sucht alle Dateien, in deren Namen die Buchstabenfolge 'emil' enthalten ist.

**man** befehl liefert eine Beschreibung von befehl.

**grep** muster dateien durchsucht alle dateien nach dem angegebenen 'muster', das natürlich auch "reguläre Ausdrücke" (siehe Abschnitt Wildcards - ein kleiner Ausblick oder man regexp) enthalten kann.

### 6.1.3.2 Ändern von Zugriffsrechten

Die Änderung von Zugriffsrechten geschieht mit dem Befehl `chmod` (engl. change mode). Im Wesentlichen benötigt `chmod` zwei Argumente:

- die zu ändernden Zugriffsrechte, und
- einen Dateinamen.

Die Kategorien der drei möglichen Gruppen werden dabei durch 'u' für den Eigentümer bzw. Benutzer (engl. user), 'g' für die Gruppe (engl. group) und 'o' für alle anderen (engl. others) angegeben, gefolgt von den zu ändernden Zugriffsrechten. Ein '-' oder '+' wird hierbei für das Entfernen oder Hinzufügen von Rechten verwendet. Folgende Eingabe setzt z.B. die Rechte der Datei `linux.info` für Gruppenmitglieder auf lesbar, veränderbar und ausführbar:

```
tux @erde: # chmod g+rwx linux.info
```

Wenn Rechte für alle drei Kategorien von Benutzern gesetzt werden sollen, genügt die Angabe der zu ändernden Rechte. Folgende Eingabe setzt die Rechte für die Datei `linux.info` so, dass niemand Schreiberlaubnis besitzt:

```
tux @erde: # chmod -w linux.info
```

Die Rechte für Lesen und Ausführen werden davon nicht betroffen.

Zugriffsrechte können auch in einem Befehl entzogen und gesetzt werden. Folgende Eingabe setzt die Rechte der Datei `linux.info` des Eigentümers auf ausführbar, nicht lesbar, nicht veränderbar:

```
tux @erde: # chmod u+x-rw linux.info
```

Wenn man sich das Ergebnis ansieht:

```
tux @erde: # ls -l linux.info
```

```
-xr-xr- 1 tux users 29524 Jun 29 13:11 linux.info
```

In diesem Zusammenhang interessante Befehle sind `chown` für "Besitzer ändern" (engl. change owner) und `chgrp`, um die Gruppe zu ändern (engl. change group).

### 6.1.3.3 Der Befehl `df`

`df` (engl. disk free) gibt Auskunft über den verfügbaren und benutzten Plattenplatz. Die Ausgabe erfolgt wie in hier abgebildet.

```
Filesystem 1024-blocks Used Available Capacity Mounted on
/dev/sda4 699392 659258 5165 99
/dev/sda1 102384 23955 73310 25
/dev/sdb1 2097136 2070485 26651 99
/dev/sda3 126976 106908 20068 84
```

Tabelle: Ausgabe des Befehls `df` (Ausgabe des Befehls `df`)

Auf den ersten Blick und bei den heutigen Plattengrößen ist das eine sehr unübersichtliche Tabelle; versuchen Sie bitte die Option `-h` (engl. human-readable) und die Welt sieht gleich viel besser aus!

### 6.1.4 Laufende Prozesse anzeigen

Der Befehl `ps` (engl. process status) zeigt die vom Benutzer gestarteten Prozesse an. Weitere Information zu dem Befehl liefert die Manual-Page von `ps` (`man ps`). Mit dem Aufruf `ps -a` werden auch die laufenden Prozesse der anderen Benutzer auf dem aktuellen Rechner angezeigt. Durch Angabe der Prozessnummer (1. Spalte der Ausgaben von `ps`) ist es möglich, laufende Prozesse gezielt abzubrechen

### 6.1.5 Manual-Pages

Über Befehle, Konfigurationsdateien und C-Bibliotheksfunktionen geben Ihnen die Manual-Pages Auskunft. Die verschiedenen Aufrufvarianten zeigt Tabelle .

`man <Stichwort>` ruft die Manual-Page zu `<Stich\wort>` auf.

`man -f <Stichwort>` sucht nach `<Stich\wort>` und listet die gefundenen Manual-Pages.

`man -k <Stichwort>` sucht in allen Sektionen der Manpages nach einer Manual-Page zum Stichwort `<Stich\wort>` und listet die gefundenen Manual-Pages auf.

`man <Sektion> <Stichwort>` ruft die Manual-Page zu `<Stich\wort>` aus `<Sek\tion>` auf. So ruft der Befehl `man 1 man` die Manual-Page zum Befehl `man` aus der Sektion 1 auf.

Zum Anzeigen der Manual-Pages verwendet der Befehl `man` das Tool `less`; vgl. zur Bedienung von `less` den Abschnitt Inhalt von Dateien: `more` und `less`. Sollten Sie das SuSE-Hilfesystem installiert haben, so können Sie darüber die Manual-Pages bequem mit einem Webbrowser einsehen. - Unter dem X Window System können Sie auch das Programm `xman` verwenden. Der gewöhnliche `man`-Befehl hat dessen ungeachtet seine Daseinsberechtigung: `man` ist einfach schneller.

Die Manual-Pages sind auf verschiedene Sektionen aufgeteilt; vgl. Tabelle:

- 1 Beschreibt die Benutzerbefehle, allerdings sind viele `bash`- und `tcsh`-Befehle eingebaute Befehle, d. h. hier geben die Manual-Pages der benutzten `bash` oder `tcsh` Auskunft.
- 2 Die Systemaufrufe der verschiedenen Bibliotheken.

- 3 Die C-Bibliotheksfunktionen.
- 4 Die Beschreibung von Konfigurationsdateien.
- 5 Die Syntax wichtiger Dateien.
- 6 Beschreibung von Spielen.
- 7 Alles was mit Text, Textformatierung und anderen Formaten zu tun hat.
- 8 Die Befehle des Systemverwalters.
- 9 Die Beschreibung der Linux-Kernelroutinen.
- n n kommt angeblich von neu, hier sind sonstige Manual-Pages aufgeführt, die in eine der oberen Sektionen gehören, aber traditionell hier stehen oder zu keiner Sektion genau passen.

Beachten Sie, dass nicht zu jedem Stichwort oder Befehl eine Manual-Page vorhanden ist. Eventuell finden Sie dann unter `/usr/share/doc/` mehr Information, z.B. unter `/usr/share/doc/howto/en`, `/usr/share/doc/howto/en/mini` oder im Verzeichnis `/usr/share/doc/packages` (paketbezogene Information).

### 6.1.6 Tabellen

IP50	Name	Besonderes
131.188.152.234	geoserv01	Der Server
131.188.152.220	geocip01	
131.188.152.221	geocip02	
131.188.152.222	geocip03	
131.188.152.223		
131.188.152.224		
131.188.152.225		

Tabelle 6.1: IP Adressen

# Index

/etc/password, 8

Account, 8

Accounting, 6

all, 23

Anmeldedomäne, 13

Anmeldung, 13

Authentifizierung, 13

Benutzerverwaltung, 4

binär, 21

chmod, 25

cipuser, 4

compilieren, 23

configure, 23

CreateWinImage, 20

CUPS, 6

Dateifreigabe, 8

dd, 21

Drucken, 6

Drucker, 13

Druckeroptionen, 15

Eigene Dateien, 13

Fernwartung, 6

Festplatte, 20

Filesystem, 25

Firewall, 14

Firewalls, 17

Frontend, 6

hda, 20

iptables, 17

Konfigurationsverwaltung, 20

Manual, 25

Netzwerk, 13

NFS, 14

NIS, 4, 14

patch, 14

PDC, 8, 13

Primärer Domänen Controller, 13

Prozesse, 25

ps, 25

Referenzrechner, 20

RPMs, 23

RRZE, 17

Samba, 4

Script, 13

Seiten, mehrere auf ein Blatt, 15

smb.conf, 12

smbmount, 20

Subnetze, 14

tar, 23

tgz, 23

updates, 14

useradd, 4

xpp, 15

Zugriffsrechte, 24