

LINUX - SAMBA
NETZWERKSERVER



INHALTSVERZEICHNIS

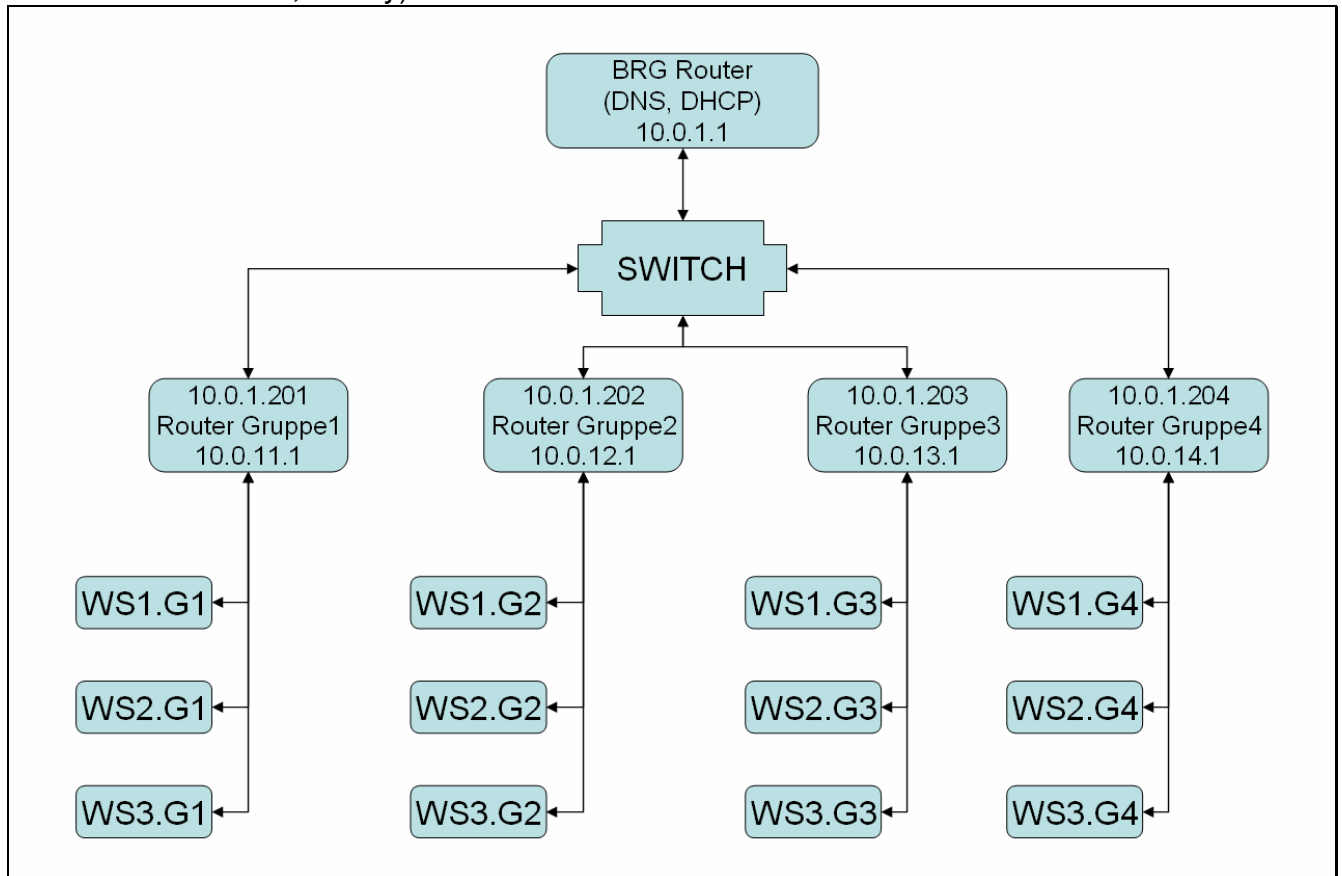
1	Zeitplan	3
2	LINUX im MICROSOFT-NETZWERK - GRUNDLAGEN	4
2.1	INSTALLATION von SAMBA	4
2.2	Die Security-Levels:	4
2.3	Passwörter:	6
2.4	OS-Level:	7
2.5	KONFIGURATION via WEB	7
2.6	Freigaben:	8
2.7	Drucker einrichten:	11
2.8	Sicherung von Workstations:	11
2.9	Login-Skripts:	12
2.10	Vorbereitung auf das Anlegen weiterer Benutzer:	12
3	Samba konfigurieren (STEP by STEP)	13
3.1	User einrichten	13
3.2	Automatischer Abgleich von Passwörtern	14
3.3	Freigaben einrichten	14
3.4	Schreibrecht für Gast	15
3.5	Arbeit mit Gruppen	15
3.6	Tipps, Tricks und Performance	16
3.7	Erweiterung der Konfiguration	16
3.8	Zusätzliche Ressourcen	16
3.9	Erzeugen der Maschinen-Accounts	17
3.10	Server-Tuning	18
3.11	ACL-Support aktivieren	19
3.12	Zugriffsrechte festlegen	20
4	Linux als Printserver mit Samba 3	20
4.1	Drucker per GUI einrichten	20
4.2	Netzwerkdruck vorbereiten	21
4.3	Treiber-Automatik einrichten	21
4.4	CUPS-Postscript-Treiber vorbereiten	22
4.5	Adobe-Treiber für Windows 9x vorbereiten	22
4.6	Treiber-Download aktivieren	23
4.7	Den Zugang beschränken	24
4.8	Drucken mit Windows-Treibern: Vorarbeiten	25
4.9	Windows-Treiber auf dem Server installieren	25
5	ANHANG	26
5.1	Benutzerplatzbeschränkung - QUOTAS	26
5.2	Statische Namensauflösung:	27
5.3	DNS – Domain Name System (Port 53 –udp):	27
5.4	DHCP-Server: (Port 67+68):	31
6	Literaturverweise:	33

1 Zeitplan

Mittwoch, 07.07.	
14.00 – 15.30	Gruppeneinteilung, Windows – Workstationinstallation Herstellen der Netzwerkstruktur, DHCP-Server konfigurieren
15.45 – 17.15	Freigaben mit und ohne Authentifizierung (Share-Level) Samba – Share-Level
Donnerstag, 08.07.	
08.45 – 10.15	User-Level – Domain-Logons
10.30 – 12.00	Drucker installieren, Login-Skripts
13.30 – 15.00	Aufbau einer komplexen Struktur für das Netzwerk
15.15 – 16.45	Ausbau der Benutzer und Rechtestruktur
Freitag, 09.07.	
08.45 – 10.15	Softwareinstallation im Netz
10.30 – 12.00	Diskette erstellen, Workstation sichern
13.30 – 15.45	Vorbereiten für das Erstellen weiterer Benutzer

2 LINUX im MICROSOFT-NETZWERK - GRUNDLAGEN

Für Linux steht mit SAMBA ein Paket zur Verfügung, mit dem man einen Linuxrechner in ein Windowsnetzwerk integrieren kann. Der Rechner kann hier bis hin zum NT-Domain-Controller fast alle Aufgaben in einem NT-Netzwerk übernehmen. (Eine ausführliche Dokumentation finden sie im Buch „Using SAMBA“ von R.Eckstein u.a. ; Oreilly)



2.1 INSTALLATION von SAMBA

Samba ist als Paket in der Serie n (Netzwerk) enthalten und kann über `yast` installiert werden. Nach der Installation finden sie in der Datei `rc.config` einen Parameter `START_SMB` mit dem sie den automatischen Start einstellen können.

Wenn sie die Firewall installiert haben, kann es sein, dass sie trotz gestartetem Dienst SAMBA keinen Rechner in der Netzwerkumgebung ihrer Windows-Workstation sehen. Der Grund dafür ist, dass die notwendigen Ports (137,138,139) von der Firewall nicht akzeptiert werden. Diese 3 Ports müssen sie für UDP und TCP freischalten und, wenn sie die grafische Konfiguration (SWAT) verwenden wollen, noch zusätzlich den Port 901 freigeben.

Bei SuSE 8.0 wird der automatische Start von Samba über den Runlevel-Editor eingestellt.

2.2 Die Security-Levels:

Samba stellt Freigaben (Shares) bereit und kann mit verschiedenen Identitäten beeinflussen, wer wann und wie prüft, ob ein Windows-Client-PC auf eine Freigabe

auf einem Linux-Server zugreifen darf. Im einfachsten Fall gliedert sich Samba in ein Windows 9x-Peer-to-Peer-Netzwerk als weiterer Rechner einer Arbeitsgruppe ein und verhält sich bei der Zugriffskontrolle wie ein Windows-9x PC, bei dem auf der Registerkarte Zugriffssteuerung der Netzwerkeigenschaften die Option Zugriffssteuerung auf Freigabeebene aktiv ist. Beim Aufbau der Verbindung zwischen der Freigabe auf dem Linux-Server und dem Windows-PC schickt der Windows-PC lediglich ein Passwort an Samba. Um die Sicherheitsregeln bei Linux nicht zu verletzen, bei denen Benutzer eine Kombination aus Benutzernamen und Passwort angeben müssen, versucht Samba so lange, ein solches Paar zu finden, bis es entweder den Zugriff gewährt oder aber verhindert. Dieses Verfahren entspricht dem Eintrag

```
security = share
```

in der zentralen Konfigurationsdatei von Samba smb.conf Eine weitere Variante der Zugriffskontrolle ist der Zugriff auf Benutzerebene durch den Eintrag

```
security = user
```

in der Datei smb.conf, der Voreinstellung für Samba ab Version 2.0. Hierbei vergleicht Samba das beim Verbindungsaufbau angegebene Paar aus Benutzername und Passwort mit Einträgen einer lokalen Benutzerdatenbank auf dem Linux-Server, d.h. Samba überprüft die Daten auf der Maschine, auf der sich die Freigabe befindet. Wenn sich mehrere SMB-Server in einem Netzwerk befinden, muss man dann mühselig die Benutzerkonten auf jedem Samba-Server einrichten und pflegen.

Ein eigener Samba-Server kann als dritte Variante zentral alle Zugriffsanfragen der anderen Server entgegennehmen, um die Authentifizierung zu zentralisieren. Dies erreicht man durch die Einträge:

```
security = server  
password server = name1, name2
```

wobei man zusätzlich zum geänderten Eintrag bei security auch den Netbios - Namen eines oder mehrerer Samba-Server angeben muss, der bzw. die die Authentifizierung durchführen.

Als vierte Variante kann man den Samba-Server zu einem vollwertigen Mitglied einer Windows NT-Domäne machen. Hierzu muss man in smb.conf drei zentrale Parameter einstellen:

```
security = domain  
password server = pdc, bdc  
workgroup = nt-domain-name
```

Der Eintrag security erhält den Wert domain und der Eintrag password-server die Namen des Primären NT-Domänencontrollers (PDC) und, falls im Netzwerk vorhanden, den/die Namen eines oder mehrerer Backup-Domänencontroller (BDCs). Der in der SuSE-Distribution auf Arbeitsgruppe voreingestellte Eintrag workgroup muss den Namen der Windows-NT-Domäne erhalten. In dieser Variante nimmt der Samba-Server an den Vertrauensbeziehungen innerhalb des Windows NT-Netzwerkes so teil, als wenn er ein NT-Server wäre. Der

Samba-Server authentifiziert hierbei nicht mehr selbst, sondern delegiert dies an den Windows-NT Domänencontroller. Hierzu sind sowohl auf dem Domänencontroller als auch auf dem Linux-Server eigene Maßnahmen zu treffen.

2.3 Passwörter:

Samba vergleicht die Benutzerkennungen mit der Benutzerdatenbank (passwd). Je nach Windows-Version verwenden die Client-Rechner jedoch Passwörter im Klartext oder verschlüsselt.

Operating System	Encrypted or Non-encrypted
Windows 95	Non-encrypted
Windows 95 with SMB Update	Encrypted
Windows 98	Encrypted
Windows NT 3. x	Non-encrypted
Windows NT 4.0 before SP 3	Non-encrypted
Windows NT 4.0 after SP 3	Encrypted

Man muss sich in einer gemischten Umgebung nun entscheiden ob man alle Rechner auf Klartextpasswörter einstellt oder generell mit verschlüsselten PW arbeitet. Der entsprechende Parameter für die 2. Methode lautet: „encrypt passwords = yes“

(Die notwendigen Registrierungseinträge für die jeweiligen Betriebssysteme sind in der Dokumentation von Samba enthalten.)

Wenn mit verschlüsselten PW gearbeitet wird, muss eine eigene Datei für den Dienst Samba geführt werden – smbpasswd. Mit dem Befehl smbpasswd (-a) user wird für einen Systembenutzer ein (verschlüsseltes) Sambapasswort eingetragen. Beim ersten Mal ist für die Erstellung eines neuen Eintrages der Parameter -a notwendig. Für NT/2000 Rechner ist zusätzlich noch ein Maschinenaccount notwendig. Dazu muss z.B für den Rechner pc01 ein Eintrag pc01\$ in der Datei /etc/passwd und der passende Maschinenaccount (smbpasswd -a -m pc01) erzeugt werden.

In der neuen Version ist dies jedoch bereits einfacher möglich:

Mit der Zeile

```
add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
im [globals] -Teil von smb.conf wird ein Verweis auf das Useradd-Skript von Linux gelegt.
```

Wenn man nun auch den root-Benutzer für Samba freigibt, kann der Maschinenaccount automatisch mit den entsprechenden Windows-Tools angelegt werden (Anmelden an Domäne)

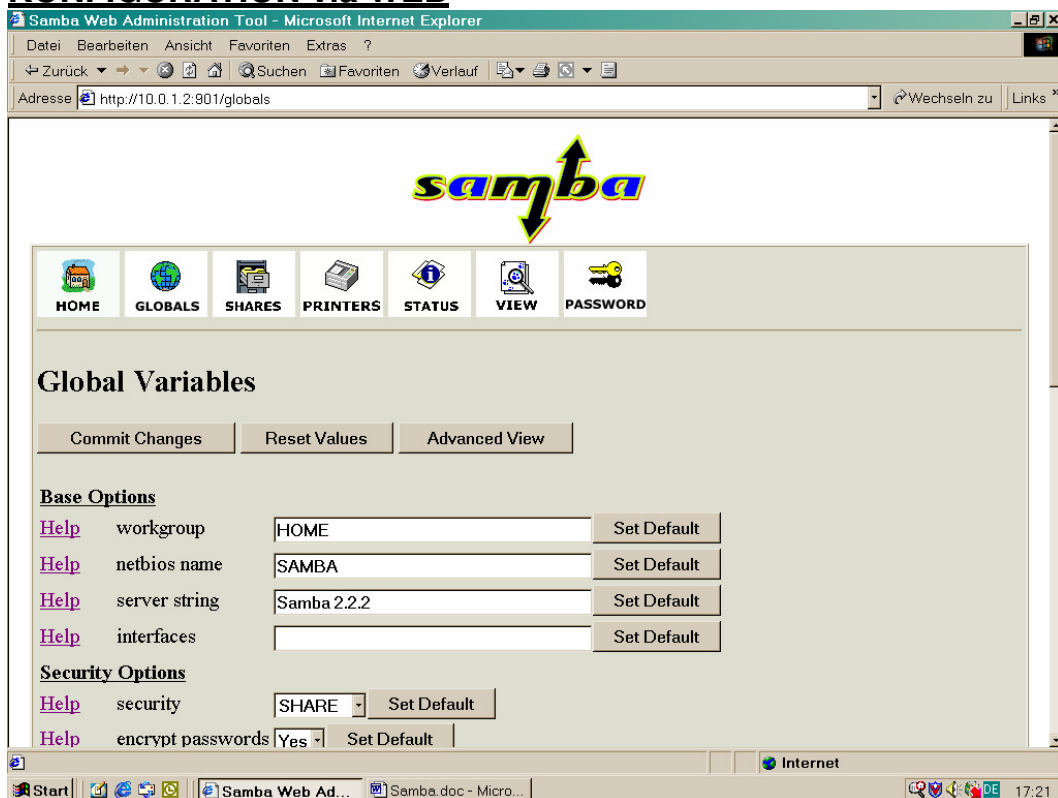
2.4 OS-Level:

Table 5.1: Operating System Values in an Election

Operating System	Value
Windows NT Server 4.0	33
Windows NT Server 3.51	32
Windows NT Workstation 4.0	17
Windows NT Workstation 3.51	16
Windows 98	2
Windows 95	1
Windows 3.1 for Workgroups	1

In einem Subnetz wird jeweils ein Rechner zum sog. Master Browser ernannt (Speichert ein Abbild der verfügbaren Netzwerkressourcen) Die Entscheidung wer diese Wahl gewinnt wird über den OS-Level geführt.

2.5 KONFIGURATION via WEB



Sie können die Veränderungen in der SMB.CONF-Datei auch via Webbrowser vornehmen. Dazu müssen sie am Linuxrechner nur den Port 901 (TCP) in der Firewall freigeben und in der Datei /etc/inetd.conf den Dienst SWAT aktivieren. Wenn sie danach mit „rcinetd reload“ den Inet-Server neu gestartet haben, sollten sie von einer WS aus mit <http://a.b.c.d:901> (a.b.c.d = IP-Linux) auf den Port 901 zugreifen können. Sie erhalten dann ein Anmeldefenster, in dem sie sich als root-

Benutzer anmelden. Danach können sie alle Administrationsarbeiten des Dienstes SAMBA via Web erledigen. Wenn sie sich später als „Normalbenutzer“ anmelden können sie z.B über SWAT ihr Netzwerkennwort ändern.

Als Alternative zu SWAT kann auch WEBMIN zur Konfiguration des Servers verwendet werden (http:a.b.c.d:10000)

2.6 Freigaben:

Ordner (und Drucker) können über die Konfigurationsdatei smb.conf als Freigaben (SHARES) den Windowsrechnern zur Verfügung gestellt werden.

Die Zugriffsrechte für solche Shares können mit speziellen Parametern gesteuert werden (write list, read only, valid users,). Der Zugriff kann jedoch nur dann erfolgreich sein, wenn die zugrunde liegenden Unix Filerechte dies gestatten.

Shares mit besonderer Bedeutung:

- [homes] Unter dieser Bezeichnung wird jedem Benutzer sein Home-Verzeichnis zur Verfügung gestellt.
- [printers] Alle Systemdrucker von Linux werden zur Verfügung gestellt (wenn in den globalen Einstellungen „load printers“ auf yes gesetzt wird.
- [netlogon] Spezieller Share für DomainLogons. Folgende Einstellungen sind empfehlenswert: browseable=no (Damit erscheint der Share nicht in der Netzwerkumgebung), read only = yes, write list = root (z.B.) ,....
- [print\$] Für die Aufnahme der Druckertreiber

Einstellungen für Shares:

Base Options

Help	comment	<input type="text" value="Infos in Netzwerkumgebung"/>
Help	path	<input type="text" value="Wo liegt der Share im Dateisystem"/>

Security Options

Help	username	<input type="text"/>
Help	guest account	<input type="text" value="nobody"/>
Help	invalid users	<input type="text" value="Wer darf nicht"/>
Help	valid users	<input type="text" value="Wer darf"/>
Help	admin users	<input type="text" value="Wer verwaltet den Share"/>
Help	read list	<input type="text" value="Leseberechtigung"/>
Help	write list	<input type="text" value="Schreibberechtigung"/>
Help	force user	<input type="text" value="Für das Erstellen"/>
Help	force group	<input type="text" value="Für das Erstellen"/>
Help	read only	<input type="text" value="Yes"/>
Help	create mask	<input type="text" value="0744"/>
Help	force create mode	<input type="text" value="00"/>

Help	security mask	<input type="text" value="0777"/>
Help	force security mode	<input type="text" value="00"/>
Help	directory mask	<input type="text" value="0755"/>
Help	force directory mode	<input type="text" value="00"/>
Help	directory security mask	<input type="text" value="0777"/>
Help	force directory security mode	<input type="text" value="00"/>
Help	inherit permissions	<input type="text" value="No"/>
Help	guest only	<input type="text" value="No"/>
Help	guest ok	<input type="text" value="No"/>
Help	only user	<input type="text" value="No"/>
Help	hosts allow	<input type="text"/>
Help	hosts deny	<input type="text"/>

Logging Options

Help	status	<input type="text" value="Yes"/>
----------------------	--------	----------------------------------

Tuning Options

Help	max connections	<input type="text" value="0"/>
Help	strict allocate	<input type="text" value="No"/>
Help	strict sync	<input type="text" value="No"/>
Help	sync always	<input type="text" value="No"/>
Help	write cache size	<input type="text" value="0"/>

Filename Handling

Help	default case	<input type="text" value="lower"/>
Help	case sensitive	<input type="text" value="No"/>
Help	preserve case	<input type="text" value="Yes"/>
Help	short preserve case	<input type="text" value="Yes"/>
Help	mangle case	<input type="text" value="No"/>
Help	mangling char	<input type="text" value="~"/>
Help	hide dot files	<input type="text" value="Yes"/>
Help	hide unreadable	<input type="text" value="No"/>
Help	delete veto files	<input type="text" value="No"/>
Help	veto files	<input type="text"/>
Help	hide files	<input type="text"/>

Help	veto oplock files	<input type="text"/>
Help	map system	No <input type="button" value="v"/>
Help	map hidden	No <input type="button" value="v"/>
Help	map archive	Yes <input type="button" value="v"/>
Help	mangled names	Yes <input type="button" value="v"/>
Help	mangled map	<input type="text"/>

Browse Options

Help	browseable	No <input type="button" value="v"/>
----------------------	------------	-------------------------------------

Locking Options

Help	blocking locks	Yes <input type="button" value="v"/>
Help	fake oplocks	No <input type="button" value="v"/>
Help	locking	Yes <input type="button" value="v"/>
Help	oplocks	Yes <input type="button" value="v"/>
Help	level2 oplocks	Yes <input type="button" value="v"/>
Help	oplock contention limit	<input type="text" value="2"/>
Help	posix locking	Yes <input type="button" value="v"/>
Help	strict locking	No <input type="button" value="v"/>

Miscellaneous Options

Help	exec	<input type="text"/>
Help	preexec close	No <input type="button" value="v"/>
Help	postexec	<input type="text"/>
Help	root preexec	<input type="text"/>
Help	root preexec close	No <input type="button" value="v"/>
Help	root postexec	<input type="text"/>
Help	available	Yes <input type="button" value="v"/>
Help	volume	<input type="text"/>
Help	fstype	NTFS
Help	set directory	No <input type="button" value="v"/>
Help	wide links	Yes <input type="button" value="v"/>
Help	follow symlinks	Yes <input type="button" value="v"/>
Help	dont descend	<input type="text"/>
Help	magic script	<input type="text"/>

Help	magic output	<input type="text"/>
Help	delete readonly	<input type="text" value="No"/>
Help	dos filemode	<input type="text" value="No"/>
Help	dos filetimes	<input type="text" value="No"/>
Help	dos filetime resolution	<input type="text" value="No"/>
Help	fake directory create times	<input type="text" value="No"/>

VFS options

Help	vfs object	<input type="text"/>
Help	vfs options	<input type="text"/>
Help	msdfs root	<input type="text" value="No"/>

2.7 Drucker einrichten:

Um einen an einen Linuxrechner angeschlossenen Drucker für ein Windowsnetzwerk zur Verfügung zu stellen sind einige Schritte notwendig:

- Drucker für Linux installieren.
- [print\$] – Share anlegen (dient zur Aufnahme der Druckertreiber) in diesem Share sind noch folgende Unterverzeichnisse anzulegen:

W32X86	; "Windows NT x86"
WIN40	; "Windows 95/98"
W32ALPHA	; "Windows NT Alpha_AXP"
W32MIPS	; "Windows NT R4000"
W32PPC	; "Windows NT PowerPC"
- Über den AddPrinter – Dialog (Im Share [Drucker]) können nun Druckertreiber auf den Server geladen werden.
- Parallel muss der passende Share erstellt werden, wobei der Parameter „printer name“ richtig gesetzt werden muss. (Muss auf einen Drucker der in der Systemdruckerdatei (/etc/printcap) verweisen)
- Diese notwendige Druckerdefinition kann z.B. mit yast erstellt werden. (Wenn lokal installierte Drucker verwendet werden, legt yast den Drucker mehrfach an. Ein Eintrag davon (raw) liefert die Daten ohne weitere Umwandlung zum Drucker. Bei Verwendung unter Samba sollte man diesen Eintrag verwenden, da die Aufbereitung bereits vom Windows Druckertreiber vorgenommen wird.

2.8 Sicherung von Workstations:

Eine Möglichkeit der Sicherung verwendet eine Bootdiskette mit Netzwerkzugriff. Der zu sichernde Rechner wird über die Diskette unter DOS gebootet und ein Netzwerkzugriff auf den Server hergestellt. Am einfachsten kann dies über die modulare Netzwerkbootdisk von Bart Lagerweij. (<http://www.nu2.nu>)

Danach wird über ein geeignetes Programm (z.B: ghost) ein Image des Rechners auf eine spezielle Freigabe am Server abgelegt.

2.9 Login-Skripts:

Mit dem Parameter „logon script = skript\login.bat“ wird beim Einloggen automatisch eine Batchdatei ausgeführt. Der Pfad ist immer relativ zum [netlogon] Share anzugeben. Dabei könne auch folgende Variable verwendet werden:

%u Username
%g primäre Gruppe

d.h. %u.bat als Logon-Skript verlang, das es zu jedem Benutzer eine gleichlautende Batchdatei im Skript-Verzeichnis gibt.

weitere Variable:

%S the name of the current service, if any.
 %P the root directory of the current service, if any.
 %u user name of the current service, if any.
 %g primary group name of %u.
 %U session user name (the user name that the client wanted, not necessarily the same as the one they got).
 %G primary group name of %U.
 %H the home directory of the user given by %u.
 %v the Samba version.
 %h the Internet hostname that Samba is running on.
 %m the NetBIOS name of the client machine (very useful).
 %L the NetBIOS name of the server. This allows you to change your config based on what the client calls you. Your server can have a "dual personality".
 %M the Internet name of the client machine.
 %N the name of your NIS home directory server. This is obtained from your NIS auto.map entry. If you have not compiled Samba with the *--with-automount* option then this value will be the same as %L.
 %p the path of the service's home directory, obtained from your NIS auto.map entry. The NIS auto.map entry is split up as "%N:%p".
 %R the selected protocol level after protocol negotiation. It can be one of CORE, COREPLUS, LANMAN1, LANMAN2 or NT1.
 %d The process id of the current server process.
 %a the architecture of the remote machine. Only some are recognized, and those may not be 100% reliable. It currently recognizes Samba, WfWg, WinNT and Win95. Anything else will be known as "UNKNOWN". If it gets it wrong then sending a level 3 log to samba@samba.org should allow it to be fixed.
 %l The IP address of the client machine.
 %T the current date and time.
 %\$(*envvar*) The value of the environment variable *envvar*.

2.10 Vorbereitung auf das Anlegen weiterer Benutzer:

Wenn man unter eine Standardbenutzerkennung bereits die Software im Netzwerk installiert hat muss man bei neuen Benutzern dafür sorgen, dass sie automatisch richtige Zuordnungen erhalten. Dazu gehört z.B. ein funktionierendes Benutzerprofil und passende Gruppenzugehörigkeiten. Es empfiehlt sich die für einen Benutzer notwendigen Dateien und Ordner (die in seinem Homeverzeichnis liegen sollen) ins

Verzeichnis /etc/skel zu kopieren, da beim Anlegen automatisch alles was in diesem Verzeichnis liegt in den Homeordner des neuen Benutzers kopiert wird.

Die primäre Gruppenzugehörigkeit kann z.B. über die Defaulteinstellungen für useradd (/etc/default/useradd) gesteuert werden.

3 Samba konfigurieren (STEP by STEP)

Dreh- und Angelpunkt der Samba-Konfiguration ist die Datei /etc/samba/smb.conf. Aus dieser bezieht Samba nicht nur alle wichtigen Betriebsparameter, sondern auch die Informationen über freigegebene Verzeichnisse und für Netzanwender bereitgestellte Drucker.

```
> [global]
> workgroup = MEINNETZ
>
> [homes]
> guest ok = no
> read only = no
```

Dies ist so ziemlich die kürzeste, funktionierende und sinnvolle Konfiguration eines Samba-Servers. Dass so wenige Befehle dafür notwendig sind, liegt daran, dass Samba intern für in der Konfigurationsdatei nicht aufgeführte Kommandos passende Default-Werte verwendet.

Es ist deutlich zu sehen, dass die Konfigurationsdatei mehrere Blöcke aufweist, die durch Schlüsselwörter in eckigen Klammern eingeleitet werden. Jeder Block spezifiziert eine Ressource, die der Server den Clients zur Verfügung stellt. Eine Sonderstellung nimmt dabei [global] ein. In diesem Block finden sich die Anweisungen, die sich auf den generellen Betrieb des Servers auswirken. Auch [homes] hat besondere Bedeutung: Ist diese Ressource definiert, leitet Samba einen Client direkt auf das Heimatverzeichnis des Users um, der sich anmeldet.

Doch bevor wir das ausprobieren, testen wir, ob alles wie gewünscht funktioniert. Starten Sie den Server und rufen Sie eine Liste der bereitgestellten Ressourcen ab:

```
> rcsmb restart (oder start falls der Server noch nicht läuft)
> smbclient -L //localhost
>
```

3.1 User einrichten

Ein Versuch, diese Liste auch von einem Windows-PC aus zu erhalten, schlägt jedoch ziemlich sicher fehl. Ursache dafür ist, dass dem Samba-Server bislang noch keine Benutzerkonten bekannt sind. Dabei ist zu beachten, dass jeder User-Account für Samba einen entsprechenden Eintrag in der Passwort-Datei des Linux-Rechners, /etc/passwd, erfordert. Um nun ein Konto für den Benutzer testuser anzulegen, sind folgende Schritte notwendig:

```
> useradd -m testuser  
> smbpasswd -a testuser
```

Achtung: Obwohl das Utility `smbpasswd` nach einem Passwort für den neu angelegten Account fragt, ist mit dem eben erzeugten Benutzernamen keine Anmeldung an der Konsole des Linux-Rechners möglich. Samba verwaltet seine Accounts nämlich in einer eigenen Passwort-Datei, `/etc/samba/smbpasswd`. Ergo wird nur dort das Passwort hinterlegt, nicht aber in der Datei mit den Zugangskennungen für den Rechner selbst.

Das macht durchaus Sinn, da Sie auf diese Weise reine Samba-Accounts einrichten können, ohne den jeweiligen Usern gleich Zugang zu lokalen Daten des Servers zu geben. Sollen Samba-Anwender auch Zugriff per SSH oder über die Konsole des Servers erhalten, müssen Sie als Admin das Passwort manuell über das Linux-Utility `passwd` setzen.

3.2 Automatischer Abgleich von Passwörtern

Das wirft die nächste Frage auf: Ändert ein Anwender sein Samba-Passwort, was passiert dann mit dem Kennwort des Linux-Accounts? Die Antwort ist: nichts. Zumindest in der Standardkonfiguration. Das bedeutet, es sind plötzlich unterschiedliche Passwörter für denselben User vermerkt, was zu Problemen führen kann. Die Samba-Entwickler haben jedoch auch an diesen Fall gedacht und Vorkehrungen dafür getroffen. Alles was erforderlich ist, um bei einer Änderung des Samba-Passworts gleich das zugehörige Linux-Passwort mit zu aktualisieren, sind zwei Zeilen im Abschnitt `[global]` der Konfigurationsdatei:

```
> unix password sync = yes  
> passwd program = /usr/bin/passwd %u
```

Bei verschiedenen Distributionen kann das Utility `passwd` auch an anderer Stelle liegen. Am besten prüfen Sie dies über das Kommando `which passwd`. Es verrät Ihnen, wo sich das Programm bei Ihrer Distribution versteckt.

Eine kleine Falle lauert hier noch: Wer jetzt denkt, dass er als Admin ab sofort sowohl die Passwörter für die Linux-Konsole als auch für den Samba-Server über das Hilfsprogramm `smbpasswd` setzen kann, der irrt. Nur für den jeweiligen User selbst führt `smbpasswd` den komfortablen automatischen Abgleich durch. Der Superuser muss nach wie vor beide Passwörter von Hand setzen.

3.3 Freigaben einrichten

Nun sind Netzlaufwerke für einzelne Anwender ja ganz praktisch. Allerdings helfen sie nicht viel beim Austausch von Daten zwischen den Usern. Schließlich kann jeder Anwender gerade einmal auf sein eigenes, nicht aber auf die Netzverzeichnisse der anderen Benutzer zugreifen. Ergo: Eine weitere Netzressource muss her, zu der alle Anwender Zugang haben. Dazu legen Sie zuerst ein lokales Verzeichnis an, zum Beispiel `/srv/samba/temp`:

```
> mkdir -p /srv/samba/tausch
```

Anschließend laden Sie die Konfigurationsdatei `/etc/samba/smb.conf` in den Editor und erweitern sie um einen neuen Block:

```
> [tausch]
> path = /srv/samba/tausch
> read only = no
> guest ok = yes
> guest only = yes
```

Nach einem Neustart des Samba-Dämons per `rcsmb restart` ist die frische Freigabe von allen Clients aus sichtbar. Der Versuch, Daten auf dieses Netzlaufwerk zu kopieren, scheitert jedoch.

Kein Wunder, denn so wie die Ressource `tausch` aktuell konfiguriert ist, passiert Folgendes: Bei einem Zugriff stellt Samba fest, dass auch Gäste Zugriff erhalten dürfen (`guest ok = yes`) und jeder User als Gast behandelt werden soll (`guest only = yes`).

3.4 Schreibrecht für Gast

Der voreingestellte Gast-Account unter SuSE Linux 9.0 ist `nobody` in der Gruppe `nogroup`. Wie Sie leicht über das Kommando `ls /srv/samba -al` nachprüfen können, hat aber nur der User `root` Schreibrechte auf das zuvor angelegte Verzeichnis. Ändern Sie also den Besitzer des Verzeichnisses von `root` auf `nobody`, und schon können alle Netzwerkanwender Daten in der Freigabe ablegen oder verändern:

So weit, so gut. Nur haben jetzt tatsächlich alle Anwender im Netz Schreibzugriff auf den Tauschordner - und das, ohne sich am Server anmelden zu müssen. Das kann in Einzelfällen zwar erwünscht sein, in den meisten Fällen möchte man den Zugriff aber eher auf bestimmte Benutzer beschränken. Um das zu erreichen, müssen Sie den Block für die Ressource `tausch` ein wenig modifizieren:

```
> [tausch]
> path = /srv/samba/tausch
> read only = no
> valid users = testuser
> force user = nobody
```

Durch die Angabe des Kontos `testuser` hinter dem Schlüsselwort `valid users` veranlassen Sie den Samba-Server, nur diesen Anwendern Zugriff auf die Tauschfreigabe zu gewähren. Fehlt diese Zeile, erhalten automatisch alle dem Server bekannten Benutzer Zugang. Allerdings hätten wir uns jetzt beinahe wieder ein Problem eingehandelt: Schreibzugriff hat nun ausschließlich der Linux-User `nobody` und nicht `testuser`. Dass trotzdem alles klappt, dafür sorgt die letzte Zeile des Blocks. Sie weist Samba an, für alle Operationen auf der Ressource `tausch` intern den Benutzer `nobody` zu verwenden - egal unter welcher Kennung der jeweils ausführende User angemeldet ist.

3.5 Arbeit mit Gruppen

Handelt es sich bei dem zu versorgenden Netz um eine größere Installation mit vielen Anwendern, ist es schnell mühsam, die zum Zugriff berechtigten User einzeln hinter dem Schlüsselwort `valid users` aufzuführen. Samba unterstützt daher als Parameter auch Gruppen. Um beispielsweise allen Mitgliedern der Gruppe `tauschgrp` Zugriff auf den Tauschordner zu geben, ändern Sie die Zeile wie folgt ab:

```
> valid users = +tauschgrp
```

3.6 Tipps, Tricks und Performance

Obwohl Samba eigentlich recht gute Vorgabewerte für die meisten Systeme verwendet, gibt es doch ein paar Schrauben, an denen man drehen kann, um noch ein wenig mehr Performance aus dem Server herauszukitzeln. Besondere Bedeutung haben hier die Optionen, die sich auf den TCP/IP-Stack auswirken. Sie werden über das Schlüsselwort `socket options` in der globalen Sektion der Konfigurationsdatei gesetzt. Eine gute Wahl ist zum Beispiel in vielen Fällen:

```
> socket options = TCP_NODELAY IPTOS_NODELAY SO_RCVBUF=8192
SO_SNDBUF=8192 SO_KEEPALIVE
>
```

Diese Optionen bewirken, dass Samba mit möglichst geringen Toleranzen bei den Übertragungen arbeitet, relativ große Puffer für die Datenübertragung verwendet und durch Keepalive-Pakete versehentliche Abmeldungen der Clients verhindert.

3.7 Erweiterung der Konfiguration

Um Samba 3 als PDC einzusetzen, müssen Sie als erstes einige Erweiterungen der bisherigen Konfiguration vornehmen und einige zusätzliche Shares freigeben. Beginnen wir mit der Konfigurationsdatei. Hier fügen Sie im Block `[global]` folgende Zeilen ein:

```
> os level = 33
> preferred master = yes
> domain master = yes
> local master = yes
> security = user
> domain logons = yes
> wins support = yes
```

Was bedeuten nun diese Befehle? Zunächst teilen sie dem Samba-Server mit, dass er als bevorzugter Master-Browser für alle Clients im Netz agiert (`preferred master = yes`). Das sorgt dafür, dass die Rechner im LAN diesen Samba-Server über Informationen zu Geräten und Anwendern befragen. Zusätzlich legen sie fest, dass der Samba-Server sowohl für die Domain (`domain master = yes`) wie auch für das lokale Subnetz (`local master = yes`) die Rolle des zentralen Informationsdienstes übernehmen soll.

3.8 Zusätzliche Ressourcen

Zusätzlich benötigen Sie noch zwei weitere Ressourcen, deren Verzeichnisse bereits bei der Installation von SuSE Linux 9.0 angelegt wurden:

```
> [netlogon]
> path = /var/lib/samba/netlogon
> read only = yes
> write list = ntadmin
> [profiles]
> path = /var/lib/samba/profiles
> read only = no
> create mask = 0600
> directory mask = 0700
```

Die beiden Ressourcen netlogon und profiles werden von der Login-Prozedur benötigt. In der Ressource netlogon suchen die Clients nach einem eventuell vorhandenen Startup-Skript, dessen Name die Option logon script festlegt. Zusätzlich können Sie hier Systemrichtlinien ablegen, die dann auf den angeschlossenen Clients implementiert werden.

Wichtig ist dabei, dass die Benutzer zumindest beim ersten Login, also dem Beitritt zur Domäne, Schreibrechte auf das Verzeichnis mit den Profilen erhalten. Nur so können die notwendigen Informationen dort hinterlegt werden. Um dies zu gewährleisten, ändern Sie die Zugriffsrechte einfach passend ab:

```
> chmod 777 /var/lib/samba/profiles
```

Dafür dass trotz der so eingestellten Schreibrechte für jeden Benutzer die Sicherheit und Privatsphäre gewahrt bleiben, sorgen die beiden Parameter create mask und directory mask in der Ressourcen-Definition. So wie angegeben bewirken sie, dass nur der Benutzer in dem für ihn erstellten Verzeichnis Lese- und Schreibrechte erhält. Dies gilt für alle darin erstellten Dateien. Nicht einmal Mitglieder derselben Gruppe können Änderungen an den Daten vornehmen. Besonders unter SuSE Linux 9.0 ist das wichtig, da es jeden neuen Account automatisch der Einheitsgruppe users zuordnet.

3.9 Erzeugen der Maschinen-Accounts

Ein erster Versuch, nun der Domain MEINNETZ beizutreten, schlägt allerdings fehl. Ursache ist, dass für jeden Rechner in der Domäne eine eigene Vertrauensstellung bestehen muss. Mit anderen Worten: nicht nur der Benutzer, sondern auch der Rechner benötigt einen eigenen Account - und zwar bevor eine Aufnahme in die Domäne erfolgt. Am besten ist es, Sie richten eine eigene Benutzergruppe für die Rechner ein und nehmen den Client in dieser auf:

```
> groupadd -g 300 clientpc
> useradd -g clientpc -d /dev/null -s /bin/false TEST$
> passwd -l TEST$
```

Mit diesen Befehlen erzeugen Sie eine Vertrauensstellung zwischen dem Samba-Server und dem Rechner, der zu der Domäne hinzugefügt werden soll. Bis dies nun

geschieht, besteht potenziell die Möglichkeit für einen Angreifer, die eingerichtete Vertrauensstellung auszunutzen. Daher ist es besser, den Account für den Rechner von Samba quasi automatisch erzeugen zu lassen. Hierzu dient ein weiterer Eintrag in der Sektion [global] der Konfigurationsdatei /etc/init.d/smb.conf:

```
> add machine script = /usr/sbin/useradd -d /dev/null -g clientpc -s /bin/false %u
```

Beachten Sie, dass Sie die Gruppe zur Aufnahme der Rechner-Accounts trotzdem von Hand anlegen müssen.

3.10 Server-Tuning

Für viele Anwender ist es wichtig, dass sich der Samba-Server im Netz tatsächlich wie ein echter Windows-Server verhält. Dazu gehört unter anderem auch, dass sich der Administrator mit dem gleichnamigen Benutzerkonto und nicht als Root anmeldet. Um dies zu erreichen, müssen Sie auf dem Samba-Server die Datei /etc/samba/smbusers editieren. Dabei handelt es sich um eine einfache Textdatei, mit der sich Beziehungen zwischen lokalen Linux-Accounts und vom Anwender angegebenen Benutzernamen herstellen lassen.

Um etwa die Windows-typischen Benutzernamen Administrator, Admin und NTAdmin auf den Root-Anwender zu mappen, verwenden Sie folgende Zeile:

```
> root = Administrator Admin NTAdmin
```

Als chronische Problemquelle erweist sich, dass viele Windows-Anwender nicht daran gewohnt sind, auf Groß- und Kleinschreibung beim Benutzernamen achten zu müssen. Linux und damit auch Samba legen hier wesentlich strengere Maßstäbe an, was gerne zur Häufung von Support-Anfragen führt.

Dem können Sie aus dem Weg gehen, indem Sie den Samba-Server anweisen, bei der Prüfung der Benutzernamen (und eventuell auch der Passworte) etwas legerer vorzugehen. Tragen Sie dazu die beiden folgenden Befehle in der Sektion [global] der Samba-Konfigurationsdatei ein:

```
> password level = 3  
> username level = 16
```

Diese beiden Kommandos bewirken, dass Samba beim Anmeldevorgang neben dem eigentlich eingegebenen Usernamen und Passwort auch andere Kombinationen prüft. Dazu verändert es für maximal die hinter dem jeweiligen Schlüsselwort angegebene Anzahl von Zeichen deren Schreibweise. So würde etwa für das angegebene Passwort "geheim" zusätzlich geprüft, ob mit den Kombinationen "Geheim", "GEheim", "GEHeim", "gEheim", und so weiter ein erfolgreicher Login möglich ist. Gleiches gilt für den User-Namen, nur dass hier bis zu 16 aufeinander folgende Zeichen in ihrer Schreibweise geändert werden.

Beachten Sie, dass dies nicht nur immens Rechenzeit kosten kann, sondern auch gewaltig auf die Sicherheit Ihres Netzwerks drückt. Gerade beim Schlüsselwort

password level sollten Sie daher genau überlegen, ob Sie es wirklich einsetzen wollen.

Access Control Lists

Ein Feature, das viele Anwender beim Umstieg vom Windows- auf den Samba-Server vermissen, ist die Möglichkeit, auch den Zugriff auf einzelne Dateien zu beschränken. Von Haus aus bietet Samba ja nur die Option, Zugang zu den Daten abhängig von Benutzererkennung oder Gruppenzugehörigkeit zu regeln. Für die wesentlich feiner granulierte Rechtevergabe unter Windows zeichnen die so genannten Access Control Lists (ACL) verantwortlich. Dabei handelt es sich im Prinzip um Tabellen, in denen für jede Datei und jedes Verzeichnis hinterlegt ist, welche Benutzer welche Zugriffsmöglichkeiten besitzen.

Auch für Linux existiert ein entsprechendes, wenngleich weitgehend unbekanntes System: die Posix-ACLs. Mit ihrer Hilfe kann auch ein Samba-Server die unter Windows verfügbaren Rechte auf Dateien bieten. Voraussetzung dafür ist jedoch, dass die Posix-ACLs beim Erstellen des Kernels aktiviert wurden und das verwendete Dateisystem Posix-ACLs unterstützt.

Wer also einen Samba-Server unter SuSE Linux 9.0 aufsetzen möchte, der sollte gleich bei der Installation darauf achten, das verwendete Dateisystem von ReiserFS auf Ext3 umzustellen. Letzteres bietet sowohl Support für Posix-ACLs wie auch ein Transaktions-Log, um bei einem Systemabsturz den ursprünglichen Zustand des Dateisystems wieder herstellen zu können.

3.11 ACL-Support aktivieren

Es genügt jedoch nicht, einen Bereich der Festplatte mit dem Dateisystem Ext3 zu formatieren, um automatisch Access Control Lists verwenden zu können. Sie müssen die ACL-Unterstützung explizit aktivieren. Um dies beispielsweise für die unter /share gemountete Partition mit den Freigaben zu erreichen, dient folgender Befehl:

```
> mount -o remount,acl,defaults /share
```

Den Erfolg des Kommandos überprüfen Sie durch einen Aufruf von mount ohne jedweden Parameter. Hinter dem Eintrag des Mount-Punkts /share sollte sich nun der Bezeichner (rw,acl) statt des üblichen (rw) finden.

Damit Sie diese Operation nicht jedes Mal auf der Kommandozeile vornehmen müssen, empfiehlt es sich, den Parameter acl gleich in die Datei /etc/fstab zu übernehmen. Die entsprechende Zeile sieht für den Mount-Punkt /share so aus:

```
> /dev/hdb1 /share ext3 acl,defaults 0 0
```

Je nachdem, welcher Partition auf welcher Festplatte /share bei Ihnen entspricht, sieht der erste Parameter anders aus. Wichtig ist nur, dass Sie das Schlüsselwort acl vor dem Bezeichner defaults einfügen. Richten Sie dies für alle Mount-Punkte ein, für die Sie ACLs zur Verfügung stellen wollen. Starten Sie anschließend den Samba-Server neu.

3.12 Zugriffsrechte festlegen

Wenn Sie jetzt auf einem Windows-Rechner per Klick mit der rechten Maustaste die Eigenschaften eines Verzeichnisses oder einer Datei auf einer Freigabe abrufen, können Sie dort über den Reiter "Sicherheit" erweiterte Zugriffsrechte festlegen.

Klicken Sie dazu die Schaltfläche "Erweitert". Sie gelangen zu einem Dialog, über den Sie weitere Berechtigungen hinzufügen sowie bestehende ändern oder auch löschen können.

Heimtückisch ist, dass Ihnen diese Dialoge auch dann zur Verfügung stehen, wenn der Samba-Server ACLs nicht unterstützt! Feststellen können Sie dies nur dadurch, dass Sie nach jeder Änderung kontrollieren, ob diese auch tatsächlich übernommen wurde. Das sollte auch Ihre erste Maßnahme bei der Fehlersuche im Zusammenhang mit ACLs sein: Feststellen, ob das entsprechende Verzeichnis - oder besser: die Partition auf der sich dieses befindet - überhaupt ACLs unterstützt und ob deren Einsatz auch aktiviert wurde.

4 Linux als Printserver mit Samba 3

Neben der zentralen Datenspeicherung ist das Bereitstellen zentraler Druckdienste eine der wichtigsten Aufgaben eines Netzwerks. Die Vorteile liegen klar auf der Hand: In großen Netzen sparen zentrale Drucker Kosten, weil nicht jeder Arbeitsplatz mit einem eigenen Gerät ausgestattet werden muss. Im privaten Umfeld spielt nicht nur das gesparte Geld eine Rolle. Auch die Nerven werden deutlich weniger strapaziert, da man nicht ständig wegen eines Ausdrucks der restlichen Familienmitglieder den eigenen Arbeitsplatz räumen muss.

Unter Linux stellt Samba die netzweiten Druckfunktionen bereit. Allerdings tut es das nicht komplett alleine. Vielmehr übernimmt Samba die Rolle des Vermittlers zwischen dem Client und dem lokal auf dem Linux-Rechner laufenden Drucksystem, das die eigentliche Ausgabe vornimmt. Während es noch vor wenigen Jahren mehrere unterschiedliche Systeme gab, um von Linux aus auf einen lokal am Rechner angeschlossenen Drucker zuzugreifen, hat sich mittlerweile das Common Unix Printing System (CUPS) als Defacto-Standard bei den meisten Distributionen durchgesetzt. Neuere Samba-Versionen und damit auch die aktuelle Ausgabe 3.0.2 bieten eine direkte Schnittstelle zu diesem System. Damit Samba einen Drucker für Zugriffe aus dem Netz zur Verfügung stellen kann, muss dieser also erst einmal über CUPS eingerichtet werden. Unter SuSe Linux 9.1 erfolgt dies komfortabel über das Druckermodul von Yast2.

4.1 Drucker per GUI einrichten

Das Druckermodul von Yast2 erlaubt es Ihnen, sowohl lokal am Parallel- oder USB-Port angeschlossene als auch entfernte Netzwerkdrucker zu konfigurieren. Da Samba alle CUPS bekannten Drucker für die Anwender im LAN zur Verfügung stellt, ist dies auch eine gute Methode, um älteren Rechnern ohne die notwendigen Fähigkeiten Zugang zu einem Netzwerkdrucker zu verschaffen. Die meisten am USB-Port angesteckten Geräte erkennt SuSe Linux 9.0 selbstständig, bei Druckern an der parallelen Schnittstelle müssen Sie meist selbst den korrekten Treiber auswählen. Gleiches gilt für direkt im LAN arbeitende Drucker mit integriertem

Printserver. Bei der Namensvergabe sollten Sie darauf achten, dass die gewählte Bezeichnung einerseits eindeutig, andererseits aber nicht zu lang ist. Vor allem Clients unter Windows 9x/ME bekommen Probleme, wenn der Name des Druckers länger als zwölf Zeichen ist. Intern arbeiten diese Betriebssysteme nämlich noch mit dem von DOS vorgegebenen Namensraum von acht Zeichen für den Dateinamen, gefolgt von einem Punkt und einer maximal drei Zeichen langen Namenserverweiterung - insgesamt eben besagte zwölf Zeichen.

4.2 Netzwerkdruck vorbereiten

Bevor Sie nun darangehen können, den oder die Drucker im Netz bekannt zu machen, sind noch ein paar Vorarbeiten nötig. Als wichtigste Maßnahme müssen Sie ein Spool-Verzeichnis für Samba einrichten, auf das jeder Benutzer mindestens Schreibrechte hat:

```
> mkdir /var/spool/samba  
> chmod 777 /var/spool/samba
```

Auch in der Konfigurationsdatei von Samba, zu finden unter `/etc/samba/smb.conf`, sind einige Änderungen durchzuführen. Hier müssen Sie in der globalen Sektion die Ansteuerung von CUPS als Drucksystem einrichten und Samba den Export aller in CUPS definierten Drucker über eine spezielle Sektion `[printers]` erlauben:

```
> [global]  
> printing = cups  
> printcap name = cups  
  
> [printers]  
> path = /var/spool/samba  
> browsable = no  
> guest ok = yes  
> writeable = no  
> printable = yes  
> printer admin = root, @ntadmin
```

Diese Einstellungen bewirken, dass Samba automatisch alle via CUPS definierten Geräte als einzelne Netzwerkdrucker zur Verfügung stellt. Durch den zunächst deplaziert erscheinenden Befehl `browsable = no` erreichen Sie, dass die globale Ressource `[printers]` von den Clients aus jedoch nicht sichtbar ist. Die Zeile `writeable = no` schließt aus, dass Clients wahllos Dateien im Spool-Verzeichnis ablegen können, `printable = yes` sorgt dafür, dass Druckaufträge aber sehr wohl in das Directory geschrieben werden.

Um sicherzustellen, dass Samba diese Änderungen sofort erkennt, müssen Sie den Dienst über das Kommando `/etc/init.d/smb restart` neu starten. Mit Hilfe eines Client-Rechners lässt sich nun schnell feststellen, ob die Aktion erfolgreich war. Wenn ja, sollten die Drucker in der Übersicht der vom Linux-Server bereitgestellten Ressourcen erscheinen.

4.3 Treiber-Automatik einrichten

Sobald Sie aber versuchen, auf diesen Drucker zuzugreifen, erhalten Sie zunächst eine Warn- und anschließend eine Fehlermeldung, gefolgt von der Aufforderung, einen passenden Treiber für den Netzwerkdrucker zu installieren. Ursache dafür ist, dass Windows die notwendigen Treiber zunächst auf dem Server sucht, diese dort aber nicht findet und deswegen auf die lokale Installation zurückgreift.

Zugegeben, in kleinen Installationen mit wenigen Druckern und aussagekräftigen Namen ist das kein echtes Problem. Was aber, wenn aus dem Namen nicht klar ersichtlich ist, welchen Treiber man lokal installieren muss? Auch hierfür hat Samba - in Verbindung mit CUPS - eine Lösung. CUPS kann Postscript-Daten entgegennehmen und in das vom Drucker eigentlich erwartete Format übersetzen. Samba wiederum besitzt die Fähigkeit - genau wie ein echter Windows-Server - den zu einem Drucker passenden Treiber an die Clients auszuliefern. Die Lösung lautet also: Für jeden Drucker wird einfach ein generischer Postscript-Treiber installiert, das Übersetzen in das korrekte Format für den Drucker übernimmt CUPS. Das funktioniert tatsächlich, auch für Farbtintenstrahldrucker.

4.4 CUPS-Postscript-Treiber vorbereiten

Bei der Wahl des Postscript-Treibers gibt es zwei Alternativen: den von CUPS entwickelten Treiber oder die ebenfalls frei verfügbare Variante von Adobe. Die Version von CUPS bietet erweiterte Funktionen, unterstützt aber nur Windows NT, 2000, XP und 2003. Das Adobe-Produkt wiederum bietet auch Support für die älteren Windows-Versionen 9x/Me, wartet jedoch nicht mit zusätzlichen Funktionen auf. Zum Glück lassen sich mit ein wenig Geschick auch beide Versionen parallel einrichten. Beginnen wir zunächst mit dem CUPS-Treiber.

Das größte Problem ist hierbei, dass SuSE Linux 9.0 CUPS in der Version 1.1.19 enthält. Für diese ist der Windows-Postscript-Treiber nicht mehr über die Webseiten des CUPS-Projekts erhältlich, er kann nur per FTP bezogen werden. Download und Grundinstallation sind mit wenigen Befehlen erledigt:

```
> wget ftp://ftp.cups.org/pub/cups/windows/cups-samba-1.1.16.tar.gz
> tar -xvzf cups-samba-1.1.16.tar.gz
> ./cups-samba.install
>
```

Nachdem das Installations-Script seine Arbeit beendet hat, finden sich im Verzeichnis `/usr/share/cups/drivers` die Treiberdateien `cups.hlp`, `cupsdrv.dll` und `cupsui.dll`.

4.5 Adobe-Treiber für Windows 9x vorbereiten

Etwas schwieriger gestalten sich die Vorbereitungen für den Adobe-Treiber zur Unterstützung von Windows 9x/Me. Leider bietet Adobe seinen Postscript-Treiber nämlich nicht als extrahierbares Archiv, sondern lediglich als installierbare Exe-Datei an. Daher benötigen Sie einen Rechner unter Windows, um an die Treiberdateien zu gelangen. Laden Sie also je nach Betriebssystem auf Ihrem Windows-Rechner den Treiber für Windows 9x/Me oder die Version für Windows NT, 2000, XP herunter und installieren Sie anschließend einen Dummy-Drucker. Suchen Sie dann auf

Laufwerk C: nach der Datei ADOBEPS4.DRV. Wechseln Sie in das Verzeichnis, in dem sich der Treiber befindet. Dort sollten folgende sechs Dateien vorhanden sein: ADFONTS.MFM, ADOBEPS4.DRV, ADOBEPS4.HLP, DEFPR2.PPD, ICONLIB.DLL und PSMON.DLL. Diese transferieren Sie auf den Linux-Rechner in das Verzeichnis /usr/share/cups/drivers. Am einfachsten geht das über eine auf dem Samba-Server eingerichtete Freigabe.

4.6 Treiber-Download aktivieren

Sind alle Daten im Treiberverzeichnis von CUPS abgelegt, stellt sich die Frage, wie die Clients nun an die Treiber kommen. Die Antwort lautet: über eine spezielle Ressource des Samba-Servers. Allerdings reicht es dazu nicht, einfach in der Samba-Konfiguration eine weitere Dateifreigabe auf das Verzeichnis mit den Treibern zu definieren - so einfach macht es uns Microsoft nicht. Eine zusätzliche Sektion in /etc/samba/smb.conf ist trotzdem nötig:

```
> [print$]
> path = /etc/samba/drivers
> browsable = yes
> guest ok = no
> read only = yes
> write list = root, @ntadmin
```

Da das Verzeichnis /etc/samba/drivers noch nicht existiert, müssen Sie es noch anlegen und mit den richtigen Rechten versehen:

```
> mkdir /etc/samba/drivers
> chmod 755 /etc/samba/drivers
```

Unterhalb dieses Verzeichnisses erwarten die Microsoft-Betriebssysteme eine spezielle Struktur, in der jede Windows-Variante die für sie bestimmten Treiber vorfindet. Anstatt diese nun per Hand zu erzeugen und die Dateien an die richtige Stelle zu kopieren, bedienen Sie sich lieber des Hilfsprogramms cupsaddsmb:

```
> cupsaddsmb -a
```

Sie werden nach dem Passwort für den Samba-User root gefragt. Sollte dies mehr als einmal passieren, dann ist der Superuser noch nicht in der Benutzerdatenbank von Samba enthalten. Das ist kein Beinbruch, der Befehl smbpasswd -a root behebt das Problem.

Wenn Sie jetzt in das Verzeichnis /etc/samba/drivers wechseln und dort per ls ein Directory-Listing abrufen, sehen Sie, dass cupsaddsmb dort zwei neue Verzeichnisse angelegt hat: WIN40 und W32X86. Das erste Directory enthält die Treiber für Windows 9x/Me, im zweiten finden sich die CUPS-Treiber für die 32-Bit-Versionen von Windows. Zusätzlich sind Dateien vorhanden, die den Namen der unter CUPS definierten Drucker und die Namensweiterung .ppd tragen.

Im Hintergrund hat das Utility cupsaddsmb also ganze Arbeit geleistet. Nicht nur, dass es die korrekte Verzeichnisstruktur erzeugt hat. Zusätzlich wurden auch die Einstellungen für die gesamten Drucker richtig gesetzt und die notwendigen

Treiberdateien an die von den Clients erwartete Stelle kopiert. Starten Sie nun den Samba-Dämon per `/etc/init.d/smb restart` neu. Sobald Sie jetzt auf einen von diesem Server bereitgestellten Drucker zugreifen, wird - nach dem obligatorischen Warnhinweis - der Druckertreiber automatisch auf dem Client installiert.

4.7 Den Zugang beschränken

Mit der bislang beschriebenen Konfiguration erhält jeder Anwender Zugriff auf alle Drucker - egal ob es sich um einen User im lokalen Netz handelt oder um einen Benutzer, der von einer völlig anderen IP-Adresse aus seine Aufträge schickt. Nun macht es zwar wenig Sinn, vom Internet aus Dokumente auf fremden Druckern auszugeben. Aber über passend modifizierte Printjobs kann man Drucker auch lahm legen und so den Arbeitsablauf eines Unternehmens empfindlich stören. Die einfachste Maßnahme gegen einen derartigen Angriff ist die Beschränkung des Zugriffs auf einen festgelegten Bereich von IP-Adressen. Dazu ist lediglich die Sektion `[printers]` der Samba-Konfiguration um eine Befehlszeile zu erweitern:

```
> hosts allow = 192.168.0.0/24
```

Mit diesem Befehl schränken Sie den Zugriff auf Rechner ein, die eine IP-Adresse aus dem Subnetz `192.168.0.x` besitzen. Wenn Sie wollen, dass sich die Anwender vor der Nutzung des Druckers auch am Server anmelden müssen, ist die Zeile mit der Anweisung `guest ok` zu ändern:

```
> guest ok = no
```

Etwas aufwendiger wird es, wenn nicht alle am Server definierten Drucker für alle Anwender sichtbar sein sollen. Bisher hat die spezielle Samba-Ressource `[printers]` dafür gesorgt, dass alle unter CUPS bekannten Drucker automatisch im Netz bereitgestellt werden. Um dieses Verhalten zu ändern, muss die globale Ressource `[printers]` gelöscht und jeder Drucker als eigene Ressource definiert werden. Entsprechende Einträge für die Drucker `dj940c` und `x4510` wären also:

```
> [dj940c]
> path = /var/spool/samba
> browsable = no
> guest ok = no
> writeable = no
> printable = yes
> valid users = @grafik
> printer admin = root, @ntadmin
> [x4510]
> path = /var/spool/samba
> browsable = no
> guest ok = no
> writeable = no
> printable = yes
> printer admin = root, @ntadmin
>
```

Durch das Setzen der Option `valid users = @grafik` erhalten nur die Anwender Zugriff auf den Farbdrucker, die Mitglieder in der Linux-Benutzergruppe `grafik` sind, während der normale Laserdrucker allen Usern zur Verfügung steht. Wie anhand des Beispiels zu sehen ist, können die Spool-Verzeichnisse für die einzelnen Drucker auf dasselbe lokale Directory zeigen. Es lassen sich aber auch separate Verzeichnisse für jeden Drucker angeben.

4.8 Drucken mit Windows-Treibern: Vorarbeiten

Obwohl CUPS recht leistungsfähig ist und inzwischen nahezu 700 Drucker direkt unterstützt, kann es vorkommen, dass Druckaufträge über den generischen Postscript-Treiber nicht richtig auf Papier gebracht werden. In diesem Fall ist es ratsam, für den betroffenen Drucker den spezifischen Windows-Treiber zu verwenden. Dieser lässt sich leicht mit Hilfe des Wizards "Drucker hinzufügen" von Windows NT, 2000 oder XP auf dem Samba-Server installieren - wenn auch in einer nicht ganz logischen Art und Weise. Um das zu demonstrieren, richten Sie zunächst per `lpadmin` einen neuen Druckereintrag - zum Beispiel für den am USB-Port angeschlossenen HP Deskjet - ein:

```
> lpadmin -p drvtest -E -P /usr/share/cups/model/HP/Deskjet_940C-cdj970.ppd.gz
> lpadmin -p drvtest -v usb:/dev/usb/lp0
```

Wichtig ist, dass Sie diesem Drucker keinen herunterladbaren Treiber zuordnen, also das Hilfsprogramm `cupsaddsmb` nicht ausführen. Da nun Windows-spezifische Treiber installiert werden, müssen Sie zusätzlich CUPS darauf vorbereiten, dass es nun nicht mehr nur Postscript-Daten, sondern zusätzlich bereits für den jeweiligen Drucker aufbereitete Rohdaten verarbeiten können soll. Dazu ist jeweils eine Änderung in den beiden Dateien `/etc/cups/mime.convs` sowie `/etc/cups/mime.types` notwendig. Ziemlich am Ende dieser Dateien findet sich eine auskommentierte Zeile, die Sie durch Entfernen des Kommentarzeichens aktivieren:

```
> #Diese Zeile aktivieren, damit CUPS auch Rohdaten verarbeitet
> application/octet-stream application/vnd.cups-raw 0 -
```

Jetzt müssen Sie noch CUPS per `/etc/init.d/cups restart` und Samba per `/etc/init.d/smb restart` neu starten, damit diese den neuen Drucker und die aktualisierten Einstellungen erkennen.

4.9 Windows-Treiber auf dem Server installieren

Ist das erledigt, starten Sie auf einem Rechner unter Windows NT, 2000 oder XP den Explorer und öffnen dort die Netzwerkumgebung. Navigieren Sie zu Ihrem Samba-Server. Melden Sie sich als Benutzer `root` mit dem unter Linux für den Superuser vergebenen Passwort am Samba-Server an und wechseln Sie auf diesem in das Verzeichnis "Drucker und Faxgeräte". Es ist wichtig, dass Sie wirklich in dieses Verzeichnis wechseln und nicht den Drucker auswählen, der Ihnen bereits in der Ressourcen-Übersicht für den Samba-Server präsentiert wird.

Hier rufen Sie per Klick mit der rechten Maustaste das Kontextmenü des zuvor eingerichteten Druckers `drvtest` ab und wählen den Punkt "Eigenschaften".

Auf die nun folgende Frage, ob Sie die nicht vorhandenen Treiber für den gewählten Drucker installieren möchten, antworten Sie unbedingt mit "Nein". Das erscheint zwar unlogisch, ist aber die einzige Möglichkeit, für diesen Drucker den in Windows integrierten Wizard zum Upload der Treiber auf den Server zu aktivieren. Dieser verbirgt sich auf der Karteikarte "Erweitert" hinter der Schaltfläche "Neuer Treiber".

Da wir für unser Beispiel einen HP-Deskjet 940 verwendet haben, wählen Sie den passenden Treiber aus der nun dargestellten Übersicht aus. Ein Klick auf die Schaltfläche "Weiter" startet die Installation des Treibers. Diese erfolgt nun aber nicht etwa lokal, sondern auf dem Samba-Server, wie der Pfad für das Ziel der Kopieraktion unschwer erkennen lässt.

Damit sind aber erst die Treiber für Windows NT, 2000 und XP auf den Server übertragen. Um auch für Windows 95, 98 und ME die notwendigen Dateien auf dem Server zur Verfügung zu stellen, wechseln Sie auf die Karteikarte "Freigabe". Unter Windows XP kann es sein, dass Sie dort zunächst die Freigabefunktion aktivieren müssen, bevor Sie an die Schaltfläche "Zusätzliche Treiber" herankommen.

Markieren Sie hier die Option "Windows 95, 98 und ME" und quittieren Sie Ihre Wahl mit einem Klick auf den Button "Weiter". Windows fragt Sie nun nach dem Speicherort der zu transferierenden Treiberdateien. Diese müssen Sie sich in der Regel von der Website des Druckerherstellers besorgen und hoffen, dass dieser entweder direkt entpackbare Archive anbietet oder die meist anzutreffende Installationsroutine lediglich ein Verzeichnis mit den Treibern erzeugt, anstatt diese gleich auf dem Rechner einzurichten. Nach einer weiteren Bestätigung startet der Dateitransfer, diesmal in das Verzeichnis auf dem Samba-Server, aus dem die 16-Bit-Versionen von Windows ihre Treiber erwarten.

Damit ist das Einrichten der Treiber beendet. Sobald sich nun ein Windows-Client auf einem Rechner mit Intel-Architektur am Samba-Server anmeldet, erhält er automatisch die passenden Treiber gleich von dort installiert.

5 ANHANG

5.1 Benutzerplatzbeschränkung - QUOTAS

Bei einer größeren Anzahl von Systembenutzern ist es notwendig, dass der, den Benutzern zur Verfügung stehende Plattenplatz beschränkt wird. Dies kann mit den sog. QUOTAS erfolgen.

Wenn sie das Paket QUOTA (Serie ap1) installiert haben, müssen die Beschränkungen noch konfiguriert und aktiviert werden. Dazu legen sie im Wurzelverzeichnis des Dateisystems, auf dem sie Beschränkungen verwenden wollen die Datei "quota.user" an. Für die Standardinstallation in NÖ ist dies eigentlich nur für die Root-Partition sinnvoll und kann z.B. mit dem Befehl "touch /aquota.user" durchgeführt werden (als root-Benutzer). Weisen sie dieser Datei mit "chmod 600 aquota.user" die passenden Filerechte zu.

Editieren sie nun die Datei "/etc/fstab". In dieser Datei finden sie eine Zeile, in der die Optionen für das Mounten der Root-Partition stehen: (Quotas sind nur in z.B:

```
/dev/hda2 / ext2 defaults, usrquota .....
```

Fügen sie in dieser Zeile die Option `usrquota` hinzu. Diese Option aktiviert die Quotas auf der entsprechenden Partition.

Speichern sie die Änderungen ab und editieren sie danach die Datei `/etc/rc.config`. Setzen sie in dieser Datei den Parameter `START_QUOTA` auf `yes`. Jetzt müssen die bereits vorhandenen Dateien ihren Besitzern zugeordnet werden. Die erste Initialisierung wird mit dem Befehl `quotacheck -acuvqm` durchgeführt, danach starten sie den Rechner neu.

Nach dem neuerlichen Start des Rechners werden die Quotas aktiviert. Mit dem Befehl `quota Benutzername` können die Quotas eines Benutzers eingesehen werden. Zum Einstellen von Beschränkungen kann der Befehl `edquota Benutzername` verwendet werden. Sie können im Editor (vi) nun für den jeweiligen Benutzer ein Softlimit (darf einige Zeit überschritten werden) und ein Hardlimit einstellen. (Im vi speichert man mit `:"w"` ; Verlassen: `:"q"`). Für eine größere Anzahl verwendet man einen Beispielbenutzer und macht die anderen äquivalent zu diesem. (kann mit `edquota` gemacht werden)

Hilfe erhalten sie über die entsprechende Manpage. Quotas können übrigens auch mit den PSNTOOLS eingestellt werden.

Eine einfache Überprüfung und Einstellung der Quotas kann auch über das WEBMIN – Interface erfolgen.

5.2 Statische Namensauflösung:

Damit die Rechner nun nicht nur mit ihren IP-Adressen sondern auch mit ihren Namen erreicht werden können kann die Datei `„/etc/hosts“` mit zusätzliche Einträgen versehen werden. Diese Datei ist nicht nur auf Linuxrechnern zu finden. Unter Windows (versionsabhängig) liegt diese Datei z.B. unter `c:\winnt\system32\drivers\etc` und erfüllt dieselbe Funktion.

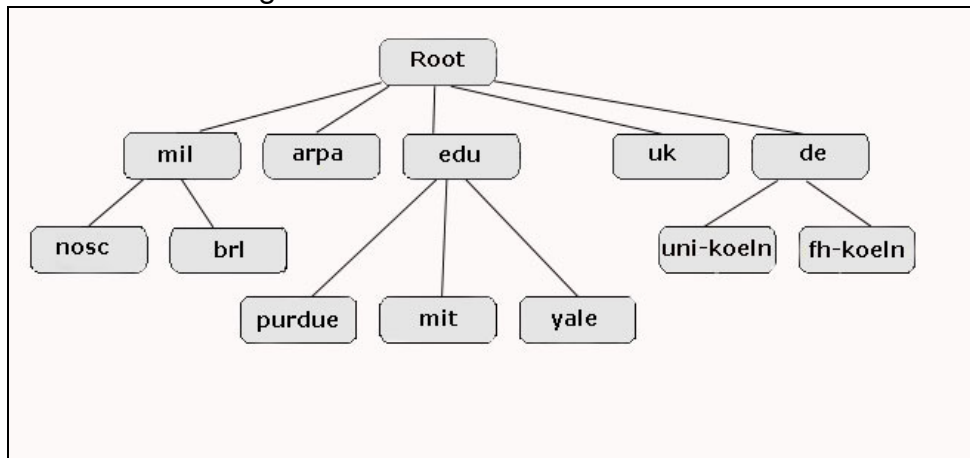
Auszug aus einer hosts-Datei:

```
# Zusätzliche Kommentare (so wie in dieser Datei) können in
# einzelnen Zeilen oder hinter dem Computernamen eingefügt werden,
# aber müssen mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#      102.54.94.97      rhino.acme.com      # Quellserver
#      38.25.63.10     x.acme.com          # x-Clienthost

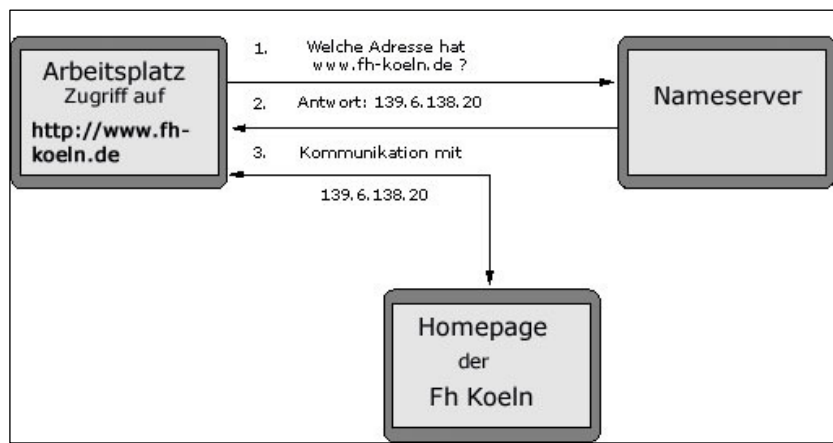
127.0.0.1      localhost
193.170.207.133 mail.brg-wrn.ac.at
```

5.3 DNS – Domain Name System (Port 53 –udp):

Für größere Netzwerke ist die Namensauflösung via HOSTS-Datei nicht mehr administrierbar. Um diese Aufgabe nun zu lösen wurde das DNS-System geschaffen, das die Namensverwaltung in einer Baumstruktur löst.



Wenn ein Rechner (DNS-Client) nun die IP-Adresse eines Rechners ermitteln will wird der eingetragene Nameserver angefragt. Sofern dieser die Adresse des Rechners selbst kennt liefert er die Antwort. Sonst wird ein ROOT-Nameserver befragt, der die Antwort möglicherweise selbst nicht kennt, jedoch auf andere authoritative Nameserver verweist.



Ob der Clientrechner zuerst in der hosts Tabelle nachforscht und danach den Nameserver befragt (Standardeinstellung) oder umgekehrt ist über die Datei resolv.conf einstellbar.

Der Nameserver (bind9 – Berkley Internet Naming Daemon) verwendet üblicherweise „/etc/named.conf“ als zentrale Konfigurationsdatei.

```

/* Beispielkonfiguration für BIND 8.1 oder neuer
* Als /etc/named.conf installieren
*
* Autor: Stephan Lichtenauer
* Anmerkung: Alle IP-Adressen/Hostnamen sind erfunden
*/
#
# Allgemeine Serverparameter
#
options {
# Verzeichnis in dem die Zonendatenbanken gespeichert sind
directory "/var/named";
pid-file "/var/named/slave/named.pid";
recursion yes;
# per Default wird an Port 53 auf allen verfügbaren
# Interfaces gelauscht, folgende Befehle könnten
# das genauer spezifizieren:
#listen-on { 5.6.7.8; };
#listen-on port 1234 { !1.2.3.4; 1.2/16; };
query-source port 53;
};
# Vordefinierte "Access Control Lists" (ACL):
  
```

```

# "any" Läßt alle Hosts zu
# "none" Verbietet alle Hosts
# "localhost" Erlaubt Verbindungen von diesem Rechner
# "localnets" Erlaubt Verbindungen aus den LANs (192.168.0.0/16)
#
# Eigene ACL festlegen:
acl secondaries { 193.158.2.17; 152.133.12.18; };
#
# Festlegen der root-Zone
#
zone "." IN {
    type hint;
    file "root.hint";
};

#
# Festlegen der Zone "localhost"
#
zone "localhost" IN {
    type master;
    file "localhost.zone";
    check-names fail; // Fehler hier wären fatal
    allow-update { none; }; // nur von lokalem Interesse
};

#
# Festlegen der Rückwärtsauflösung für localhost (Adressen in Namen)
#
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "0.0.127.zone";
    check-names fail;
    allow-update { none; };
};

#
# Festlegen der Rückwärtsauflösung für einen Adressraum
#
zone "36.158.193.in-addr.arpa" IN {
    type master;
    file "36.158.193.zone";
    check-names fail;
    allow-update { none; };
    allow-query { any; };
    allow-transfer { secondaries; };
    notify yes;
};

#
# Eine Masterzone
#
zone "bmw.de" IN {
    type master;
    file "bmw.de.zone";
    allow-transfer { secondaries; };
    allow-update { none; };
    allow-query { any; };
    notify yes;
};

#
# Eine Slave-Zone
#
zone "audi.de" IN {
    type slave;
    file "slave/db.audi.de";
    masters { 194.238.99.128; };
};

```

Eine Masterzone (bmw.de) – ZONENFILE:

```

bmw.de. IN SOA poseidon.bmw.de. root.poseidon
        ( 20000107 ; serial
          36000 ; refresh
          1800 ; retry
          3600000 ; expire

```

```

86400 ) ; time to live
bmw.de.      IN NS poseidon.bmw.de.
              IN NS pns.dtag.de.
bmw.de.      IN MX 1 193.158.36.59
              IN MX 2 193.158.36.60
localhost    IN A 127.0.0.1
poseidon     IN A 193.158.36.58
phoenix      IN A 193.158.36.59
venus        IN A 193.158.36.60
ftp          IN CNAME phoenix.bmw.de.
www          IN CNAME poseidon.bmw.de.
ns           IN CNAME poseidon.bmw.de.
news        IN CNAME venus.bmw.de.
irc          IN CNAME venus.bmw.de.

```

REVERSE LOOKUP: (localhost)

```

# /var/named/0.0.127.zone enthaelt die Zuordnung
# von localhost zur Adresse 127.0.0.1
0.0.127.in-addr.arpa. IN SOA poseidon.bmw.de. root.poseidon (
                        43 ; serial
                        3H ; refresh
                        15M ; retry
                        1W ; expiry
                        1D ) ; minimum
IN NS poseidon.bmw.de.
1 IN PTR localhost.

```

Die Konfiguration dieses Servers kann einfacher über ein entsprechendes Modul in der Webmin-Oberfläche erfolgen.

Das Testen der Funktion des konfigurierten Nameservers wird (unter Linux) mit dem Tools „nslookup“ durchgeführt. (genauere Syntax siehe „man nslookup“)

Die zentrale Konfigurationsdatei weist den Nameserver an, die Auflösung der verschiedenen Domänen aus den entsprechenden Zonenfiles einzulesen, Zu beachten ist, dass jede Zonendefinition im Allgemeinen aus 2 Dateien bestehen:

z.B: localhost.zone Auflösung Name → IP
0.0.127.zone Auflösung IP → Name (0.0.127.in-addr.arpa)

Eine Sonderstellung hat die Datei root.hint, die die Verbindungsinformation zu den Root-Nameservern beinhaltet. (Zone „.“ –Root-Zone)

5.4 DHCP-Server: (Port 67+68):

Beim Start fragt der Client über einen Broadcast im ganzen Netz - gegebenenfalls über Router-Grenzen hinweg - nach (s)einer IP-Adresse. Als Antwort bekommt er die Adresse und

- Default-Route,
- DNS-Server-Adresse(n),
- WINS-Server,
- Netzmaske,
- Broadcast-Adresse,
- Vendor-Optionen.

Wenn der Client bootet, fragt er mit einem DHCPDISCOVER per Broadcast nach seiner Client-Konfiguration. Der Client hat zu diesem Zeitpunkt noch keine (nutzbringende externe) IP, sondern nur seine MAC-Adresse (weltweit eindeutige, auf der Netzwerkkarte kodierte Ethernet-Adresse). Darum bekommt das Broadcast-Paket die Quelladresse 0.0.0.0 und die Zieladresse 255.255.255.255. Das Ganze funktioniert nur dank kreativer Nutzung der TCP/IP-Software des Clients und liberaler Auslegung des Standards RFC 1122.

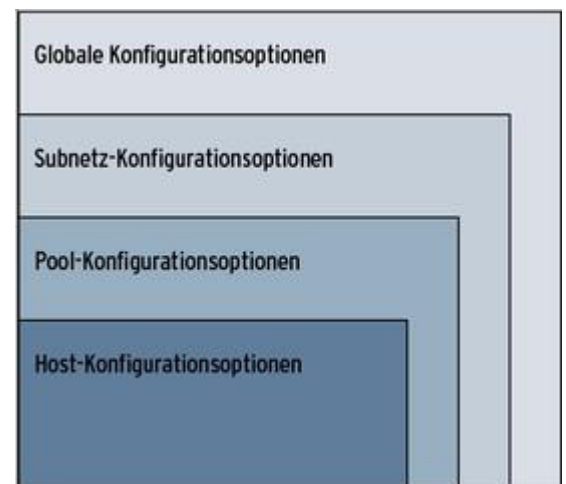
Das Antwortpaket des Servers hat als Zieladresse schon die Adresse, die der Client erhalten soll. Dieses Paket kommt beim Client an, weil die MAC-Adresse die des Clients ist. Muss ein solches Paket durch einen Paketfilter, ist es sinnvoll, eine Regel einzurichten, die Pakete mit beliebiger Quelladresse (für manche Filter-Implementierungen ist 0.0.0.0 problematisch) und Zieladresse 255.255.255.255 auf Port 68 zulässt, in der Rückrichtung entsprechend vom DHCP-Server an beliebige Adressen (hier könnte auf den DHCP-Bereich eingeschränkt werden) auf Port 67.

Aufbau der Konfiguration des DHCP-Servers:

```
server-identifizier dhcp.testnetz.de;
option domain-name "testnetz.de";
option domain-name-servers dns.testnetz.de;
option routers 192.168.1.1;

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.50;
  range dynamic-bootp 192.168.1.50 192.168.1.60;
  option broadcast-address 192.168.1.255;
  default-lease-time 36000;
  max-lease-time 72000;
  option subnet-mask 255.255.255.0;
}

host extrawurst {
  hardware ethernet 00:11:22:33:44:55;
  option host-name "extrawurst";
  option routers 192.168.1.2;
  fixed-address 192.168.1.5;
}
```



Damit trotz dynamischer Adressvergabe die Namensauflösung im lokalen Netz funktioniert kann ein Zusammenspiel von DHCP und DNS Dienst konfiguriert werden.

Änderungen in dhcpd.conf

```
ddns-update-style ad-hoc;
zone gl. {
  primary 127.0.0.1;
```

```
}  
zone 11.0.10.in-addr.arpa. {  
    primary 127.0.0.1;  
}
```

Anpassung des Nameservers (named.conf)

```
zone "g1" {  
    type master;  
    file "xxxxxx";  
    allow-update { 127.0.0.1; };  
};  
zone "11.0.10.in-addr.arpa" {  
    type master;  
    file "yyyyyy";  
    allow-update {localhost; };  
};
```

6 Literaturverweise:

<http://at.samba.org/samba/samba.html>

Das Buch „Using Samba“ ist im HTML-Format in der Distribution enthalten:
(/usr/share/doc/packages/samba/htmldocs/using_samba

<http://www.auhof.asn-linz.ac.at/linuxpage/Linux.htm>

<http://www.dbg.rt.bw.schule.de/lehrer/ritters/info/linux/fipri.htm>

<http://www.linuxbu.ch/>