





1	<u>ZEITPLAN:</u>	4
2	<u>FTP-SERVER:</u>	5
2.1	AB SUSE 8.X	5
3	<u>WEB-SERVER:</u>	6
3.1.1	VERWENDUNG VON PHP:	7
3.1.2	INTRANET	8
3.1.3	WEBSEITEN FÜR BENUTZER:	8
3.1.4	ZUGRIFF AUF BESTIMMTE WEBSEITEN MITTELS AUTHENTIFIZIERUNG:	9
3.1.5	VIRTUELLE SERVER:	9
3.1.6	HTTPS – VERSCHLÜSSELTE VERBINDUNGEN:	10
3.2	CMS – SYSTEME:	14
3.2.1	MAMBO	14
3.2.2	TYPO3	14
3.2.3	MOODLE (ELEARNING)	15
4	<u>CRON:</u>	15
5	<u>AUFBAU DER SEMINARTOPOLOGIE</u>	16
5.1	TESTEN DER NETZWERKVERBINDUNGEN:	17
5.1.1	PING	17
5.1.2	TRACEROUTE	17
5.2	AUSBAU DER KONFIGURATION AUF LAYER 3 – ROUTING:	17
5.3	STATISCHE NAMENAUFLÖSUNG:	18
6	<u>DNS – DOMAIN NAME SYSTEM (PORT 53 –UDP):</u>	18
7	<u>DHCP-SERVER: (PORT 67+68):</u>	22
	Anpassung des Nameservers (named.conf)	23
8	<u>BENUTZERPLATZBESCHRÄNKUNG:</u>	23
9	<u>MAIL-SERVER:</u>	24
9.1	SMTP : (POSTFIX – PORT 25)	24
9.1.1	DETAILS SMTP:	26



LINUX - EINFÜHRUNG

9.2	POP3: (PORT: 110)	26
9.3	IMAP: (PORT 143)	27
9.4	VIRENSCANNER:	27
9.5	NACHTRAG ZU POP3 UND IMAP:	28
9.6	WEBMAILINTERFACE:	29
10	LINUX IM MICROSOFT-NETZWERK - GRUNDLAGEN	29
10.1	INSTALLATION VON SAMBA	29
10.2	DIE SECURITY-LEVELS:	30
10.3	PASSWÖRTER:	31
10.4	OS-LEVEL:	32
10.5	KONFIGURATION VIA WEB	32
10.6	FREIGABEN:	33
10.7	DRUCKER EINRICHTEN:	36
10.8	SICHERUNG VON WORKSTATIONS:	36
10.9	LOGIN-SKRIPTS:	37
10.10	VORBEREITUNG AUF DAS ANLEGEN WEITERER BENUTZER:	37
10.11	SAMBA KONFIGURIEREN (STEP BY STEP)	38
10.11.1	USER EINRICHTEN	38
10.11.2	AUTOMATISCHER ABGLEICH VON PASSWÖRTERN	39
10.11.3	FREIGABEN EINRICHTEN	39
10.11.4	SCHREIBRECHT FÜR GAST	40
10.11.5	ARBEIT MIT GRUPPEN	40
10.11.6	TIPPS, TRICKS UND PERFORMANCE	41
10.11.7	ERWEITERUNG DER KONFIGURATION	41
10.11.8	ZUSÄTZLICHE RESSOURCEN	41
10.11.9	ERZEUGEN DER MASCHINEN-ACCOUNTS	42
10.11.10	SERVER-TUNING	43
10.11.11	ACL-SUPPORT AKTIVIEREN	44
10.11.12	ZUGRIFFSRECHTE FESTLEGEN	44
10.12	LINUX ALS PRINTSERVER MIT SAMBA 3	45
10.12.1	DRUCKER PER GUI EINRICHTEN	45
10.12.2	NETZWERKDRUCK VORBEREITEN	45
10.12.3	TREIBER-AUTOMATIK EINRICHTEN	46
10.12.4	CUPS-POSTSCRIPT-TREIBER VORBEREITEN	47
10.12.5	ADOBE-TREIBER FÜR WINDOWS 9X VORBEREITEN	47
10.12.6	TREIBER-DOWNLOAD AKTIVIEREN	47
10.12.7	DEN ZUGANG BESCHRÄNKEN	48
10.12.8	DRUCKEN MIT WINDOWS-TREIBERN: VORARBEITEN	49
10.12.9	WINDOWS-TREIBER AUF DEM SERVER INSTALLIEREN	50



1 ZEITPLAN:

Montag 04.04	
09.30 – 10.15	Begrüßung, Organisation, Aufbau und Anschluss der Rechner, SQL-Server (MYSQL), CRON Dienste
10.30 – 12.00	Anlegen von Datenbanken mit phpMyAdmin WH: statische Namensauflösung APACHE – Wiederholung (Grundkonfiguration, virtuelle Hosts)
13.45 – 15.15	APACHE – Wiederholung (private Bereiche) https – Grundkonfiguration CMS-SYSTEME: Mambo
15.30 – 17.00	E-Learning: Typo3 Moodle
Dienstag 05.04	
08.45 – 10.15	Konfiguration Routing DHCP-Service (Grundkonfiguration, Hostkonfiguration)
10.30 – 12.00	DNS – Server mit DDNS
13.30 – 15.00	MAILSERVER
15.15 – 16.45	MAILSERVER
Mittwoch 06.04.	
08.45 – 10.15	SAMBA Basiskonfiguration
10.30 – 12.00	SAMBA
13.45 – 16.00	SAMBA

Die Hinweise in diesem Skriptum beziehen sich auf die Installation und Konfiguration der SuSE Distribution 9.2



2 FTP-Server:

2.1 Ab SuSE 8.x

ist der Standard FTP-Server der Dienst vsftpd, der ebenfalls über inetd gestartet wird. Die Konfiguration dieses Dienstes erfolgt (etwas einfacher) über die Konfigurationsdatei /etc/vsftpd.conf. Eine genauere Beschreibung der Parameter erhält man mit „man vsftpd.conf“

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are very paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
#
# Allow anonymous FTP?
#anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
#xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
```



```
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES

pam_service_name=vsftpd
chroot_local_user=YES
```

3 Web-Server:

Bei einer Standardinstallation wird der Webserver APACHE automatisch mitinstalliert und auch bereits gestartet (Einstellung über START_HTTPD – Variable in rc.config). Bei konfiguriertem Netzwerk können sie von einer Workstation bereits mit einem Webbrowser unter <http://a.b.c.d> auf den Webserver des Linuxrechners zugreifen, wenn a.b.c.d stellvertretend für eine der Adressen des Linuxrechners steht. Wenn für diese Adresse bereits ein Rechner/Domainname vergeben ist und auch im entsprechenden Nameserver eingetragen wurde, kann der Zugriff auch über den Namen erfolgen.



Die Konfigurationsdatei des Servers ist /etc/httpd/httpd.conf.

Das Root-Verzeichnis des Webservers ist nun standardmäßig auf /srv/www (zuvor: /usr/local/httpd) eingestellt. Hier findet man u.a. 2 wichtige Verzeichnisse:

cgi-bin:

Enthält ausführbare Dateien (*.cgi). In der Konfigurationsdatei wird dieses Verzeichnis als Script-Verzeichnis definiert, wodurch ein Ausführen von Programmen via WEB in diesem Verzeichnis erlaubt wird. Wenn man in einem anderen Verzeichnis auch das Ausführen von Scripts erlauben will, muss die Option ExecCGI für diesen Ordner eingeschaltet werden.

htdocs:

Das Wurzelverzeichnis für HTML-Dokumente. Beim Zugriff auf den Webserver wird zunächst nach der Datei index.html gesucht. Wenn Sie nun ihre eigene Homepage gestalten wollen, überspielen sie ihre Homepage (mit allen zugehörigen Dateien und Verzeichnissen) ins Verzeichnis /srv/www/htdocs, wobei die Startseite ihrer Homepage index.html heißen sollte. Benennen Sie vorher die bereits vorhandene Datei index.html z.B. in suse.html um. Damit können sie mit <http://a.b.c.d/suse.html> jederzeit auf die Suse-Dokumentation zugreifen.

Beachten Sie, dass alle Dateien ihrer Homepage mit dem Recht 644 (lesen für „others“) versehen werden und alle Verzeichnisse das Recht 755 (Ausführen/lesen für „others“) besitzen.

Es empfiehlt sich für die Wartung der Homepage einen eigenen Benutzer anzulegen, ihn als Besitzer aller Dateien unter /srv/www festzulegen. Mittels ftp-Zugriff kann dieser Benutzer dann die Homepage von anderen Rechnern aus warten.

Weitere Tipps und Tricks zu den Wartungsaufgaben finden sie am PI-Webserver (<http://www.pinoe-hl.ac.at>) unter AG-Informatik → Anbindung eines Netzes ans Internet → WWW-Server Apache.

3.1.1 Verwendung von PHP:

Das folgende Beispiel demonstriert die Verwendung von PHP in HTML Seiten. Damit die Seite richtig interpretiert wird muss die Datei die Endung .php besitzen. Damit diese Datei (index.php) vor einer eventuell vorhandenen Datei index.html verwendet wird, muss der Parameter DirectoryIndex in der Datei /etc/httpd/httpd.conf angepasst werden. Für die Funktion der nachfolgenden Datei, die einen Zähler realisiert, muss im selben Verzeichnis eine Datei counter.txt existieren, die für die Gruppe others auch Schreibrechte hat.

```
<html>
<head>
  <title>Homepage von USER</title>
  <meta content="">
  <style></style>
</head>
<body>
Dies ist eine Testseite für Benutzerhomepages <br>
<?PHP
  $fp = fopen("counter.txt","r");
  $zahl =(int) fgets($fp,10);
  fclose($fp);
  $zahl++;
  echo "Sie sind der ".$zahl.". Besucher"; // Strings werden mit „.“ zusammengefügt
  $fp = fopen("counter.txt","w");
```



```
fputs($fp,$zahl);
fclose($fp);
?>
</body>
</html>
```

3.1.2 INTRANET

Das folgende Beispiel zeigt ein Verzeichnis, das nur aus dem internen Netz betrachtet werden, oder von außerhalb, wenn man gültige Benutzerkennungen hat. Wenn der Parameter „Satisfy any“ auf „Satisfy all“ ändert ist ein Betrachten nur dann möglich, wenn beide Bedingungen erfüllt werden.

```
<Directory /srv/www/htdocs/intra>
  AuthType Basic
  AuthName intranet
  AuthUserFile /etc/httpd/users
  AuthGroupFile /etc/httpd/groups
  Require group customers
  Order allow,deny
  Allow from 10.0
  Satisfy any                // Standardeinstellung ist Satisfy all
</Directory>
```

3.1.3 Webseiten für Benutzer:

Sie können es ihren Benutzern am Linuxrechner gestatten sich eigenständig Webpages zu gestalten. Der Zugriff auf diese Seiten erfolgt mit <http://a.b.c.d/~USER>, wenn USER der Name des Benutzers ist. Dazu müssen sie in der Konfigurationsdatei den entsprechenden Teil für das Verzeichnis /home/*/public_html aktivieren, wobei sie keine so komplizierte Definition wie im Beispiel benötigen.

Unter SuSE 9.2 sind die Benutzerhomepages automatisch aktiviert (das Modul userdir wird automatisch geladen) .

(Die entsprechende Datei heißt nun mod_userdir.conf im Verzeichnis /etc/apache2)

Es genügt z.B.:

```
<directory /home/*/public_html>
  Options Indexes
  Order allow,deny
  Allow from all
</directory>
```

Aufgaben für den jeweiligen Benutzer:

Er muß der Gruppe others das Execute-Recht für sein Homeverzeichnis einräumen (Read ist nicht notwendig) und dies ebenfalls für das anzulegende Verzeichnis public_html tun. Für die Zugriffsrechte auf die Dateien unter public_html gilt das Gleiche wie oben für die Homepage erwähnt.



(Dieses Verzeichnis wird in den neueren Versionen automatisch beim Anlegen eines Benutzers in sein Homeverzeichnis kopiert)

3.1.4 Zugriff auf bestimmte Webseiten mittels Authentifizierung:

Man kann einzelne Verzeichnisse am Webserver sperren, sodass ein Zugriff nur mit gültiger Benutzerauthentifizierung möglich ist. (Siehe Dokumentation PI-Server → Web-Zugriff auf Verzeichnisse sperren)

Dazu muss eine eigene Passwortdatei angelegt werden:

z.B.: mit dem Befehl: `htpasswd -c /usr/local/httpd/allowed.users lehrer` eine Passwortdatei z. B. für den Benutzer **lehrer** anlegen. Danach erfolgt eine zweimalige Abfrage eines Passwortes. Dieses Passwort wird dann verschlüsselt in der Datei **allowed.users** abgespeichert.

In dem Verzeichnis, das gesperrt werden soll (z. B. **/usr/local/httpd/htdocs/geheim**) wird mit einem Editor eine Datei mit dem Namen **.htaccess** angelegt. In diese Datei wird folgendes geschrieben:

HINWEIS: unter APACHE2 heißt der Befehl „`htpasswd2`“

```
AuthName "Verzeichnis geheim"  
AuthType Basic  
AuthUserFile /usr/local/httpd/allowed.users  
require user lehrer  
(oder require valid-user → Zugriff kann mit jeder gültigen Benutzererkennung erfolgen)
```

Bei den Standardeinstellungen des Apache-Servers werden die Einstellungen der Datei **.htaccess** ignoriert. Es muss daher für das Verzeichnis **/usr/local/httpd/htdocs/geheim** diese Möglichkeit aktiviert werden. Dazu editiert man die Datei **/etc/httpd/httpd.conf** und fügt für dieses Verzeichnis eine eigene Definition ein:

```
<Directory "/usr/local/httpd/htdocs/geheim">  
AllowOverride All  
</Directory>
```

Wenn man weitere gültige Benutzerkennungen zur Passwortdatei hinzufügen will, so kann dies mit dem Befehl

`htpasswd /usr/local/httpd/allowed.users NocheinBenutzer` (d.h. ohne `-c`) erfolgen.

3.1.5 Virtuelle Server:

Es ist auch möglich auf einem Rechner mehrere Webserver zu betreiben. Dazu ist es notwendig das DNS-Service entsprechend einzurichten (NickNames für den Rechner eintragen) und es Apache mitzuteilen wo die Dokumente für diesen virtuellen Server liegen. Für das angeführte Beispiel war es z.B. notwendig im DNS-Server für den Novellserver (IP 10.0.1.2) die Synonyme `student.brg-wrn.ac.at`, `sta.brg-wrn.ac.at`, `al.brg-wrn.ac.at`,..... einzutragen. Die Konfigurationsdatei für APACHE unter Novell befindet sich (bei installiertem Webserver) im Verzeichnis `sys:\apache\conf` und hat die gleiche Syntax wie unter Linux (bis auf die Verzeichnisangaben).

Ergänzung: Unter Novell wird der Server mit `load sys:\apache\apache2` gestartet.



HINWEIS: auch für den bereits laufenden (Standard-) Server ist eine virt. Hostdefinition erforderlich. Sie sollte an erster Stelle stehen, damit dieser Server zum Default Server wird. (d.h. alle Anfragen die nicht exakt einem der nachfolgenden virt. Hostnamen entsprechen werden auf den ersten Server geleitet.

```
NameVirtualHost 10.0.1.2      //Unter welcher IP laufen die virt. Server
// mit der Anweisung NameVirtualHost 10.0.1.2:5045 wäre es z.B. möglich die virt.
// Server auf einem anderen Port laufen zu lassen.
```

```
<VirtualHost 10.0.1.2>
  ServerAdmin sta@brg-wrn.ac.at
  DocumentRoot sys:/apache/student
  ServerName student.brg-wrn.ac.at
  <Directory home:/schueler/*/public.www>
    AllowOverride FileInfo AuthConfig Limit
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS PROPFIND>
      Order allow,deny
      Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS PROPFIND>
      Order deny,allow
      Deny from all
    </LimitExcept>
  </Directory>
</VirtualHost>
```

```
<VirtualHost 10.0.1.2>
  ServerAdmin sta@brg-wrn.ac.at
  DocumentRoot home:/lehrer/sta/public.www
  ServerName sta.brg-wrn.ac.at
</VirtualHost>
```

```
<VirtualHost 10.0.1.2>
  ServerAdmin sta@brg-wrn.ac.at
  DocumentRoot home:/lehrer/al/public.www
  ServerName al.brg-wrn.ac.at
</VirtualHost>
```

Anstelle der IP-Adresse (10.0.1.2) kann auch ein * eingegeben werden. Damit akzeptiert der Webserver Anfragen auf allen angeschlossenen Netzwerkkarten.

Das obige Beispiel zeigt sog. „NameBasedVirtualHosts“. Alternativ können auch IP-Basierende virtuelle Hosts verwendet werden. Dazu ist es jedoch notwendig für jeden virtuelle Server eine eigene IP-Adresse zu besitzen. (Konfiguration siehe Apache-Doku od. SuSE Handbuch)

Unter SuSE 9.x ist für virtuelle Server ein eigenes Verzeichnis (/etc/apache2/vhost.d). Jede dort abgelegte Datei mit der Endung .conf wird bei Starten des Webserver automatisch eingebunden. (Nachzulesen in der Hautpdatei httpd.conf)

3.1.6 HTTPS – Verschlüsselte Verbindungen:

Mit dem Apacheserver können auch virtuelle Hosts so konfiguriert werden, dass man nur mittels SSL-Zertifikaten zugreifen kann. Dazu findet man Dokumentationen am System selbst (apache-doc) und im Internet. Im Verzeichnis /etc/apache2/vhosts.d findet man eine Beispielkonfiguration für einen virtuellen Host mit https. Dieses Muster passt man sich bei der ersten Verwendung am besten an die eigenen Bedürfnisse an. Zu Beachten ist:

- a.) Erzeugen eines Zertifikates: mit /usr/bin/gensslcert



LINUX - EINFÜHRUNG

- C Common name "\$name"
- N comment "\$comment"
- c country (two letters, e.g. DE) \$C
- s state \$ST
- l city \$L
- o organisation "\$O"
- u organisational unit "\$U"
- n fully qualified domain name \$CN (\\$FQHOSTNAME)
- e email address of webmaster webmaster@\$CN
- y days server cert is valid for \$srvdays
- Y days CA cert is valid for \$CAdays
- d run in debug mode
- h show usage

For example:

```
/usr/bin/gensslcert -c US -s TN -l "Oak Ridge" -o Your_organization -e  
your_name@your_isp.com -d -n www.ihrserver.at
```

b.) Neustarten des Webservers mit der Option SSL!!
(in /etc/sysconfig/apache2 wird die Variable „APACHE2_OPTS“ auf -D SSL gesetzt)

Die folgende Konfigurationsdatei zeigt ein kombiniertes Beispiel aus virtuellen Hosts teilweise mit SSL teilweise ohne:

```
NameVirtualHost *:80

<VirtualHost *:80>
    ServerAdmin sta@brg-wrn.ac.at
    ServerName ilias.intra.net

    DocumentRoot /srv/ilias/www
    ErrorLog /var/log/apache2/ilias-error_log
    CustomLog /var/log/apache2/ilias-access_log combined

    HostnameLookups Off
    UseCanonicalName Off
    ServerSignature On
    ScriptAlias /cgi-bin/ "/srv/ilias/www/cgi-bin/"
    <Directory "/srv/ilias/www/cgi-bin">
        AllowOverride None
        Options +ExecCGI -Includes
        Order allow,deny
        Allow from all
    </Directory>
    <Directory "/srv/ilias/www">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from 10.0.0.0/8
    </Directory>
</VirtualHost>

<IfDefine SSL>
<IfDefine !NOSSL>
NameVirtualHost *:443
<VirtualHost *:443>
    DocumentRoot "/srv/ilias/www"
```



```

ServerName ilias.brg-wrn.ac.at:443
ServerAlias ilias.brgg.at:443
ServerAdmin sta@brg-wrn.ac.at
ErrorLog /var/log/apache2/ilias-error_log
CustomLog /var/log/apache2/ilias-access_log combined
TransferLog /var/log/apache2/access_log
SSLEngine on
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/apache2/ssl.crt/server.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory "/srv/ilias/www/cgi-bin">
    AllowOverride None
    Options +ExecCGI -Includes
    Order allow,deny
    Allow from all
</Directory>
<Directory "/srv/ilias/www">
    Options Indexes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog /var/log/apache2/ssl_request_log    ssl_combined
</VirtualHost>

<VirtualHost *:443>
    DocumentRoot "/srv/moodle/www"
    ServerName moodle.brg-wrn.ac.at:443
    ServerAlias moodle.brgg.at
    ServerAdmin sta@brg-wrn.ac.at
    ErrorLog /var/log/apache2/ilias-error_log
    CustomLog /var/log/apache2/ilias-access_log combined
    TransferLog /var/log/apache2/access_log
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/ssl.crt/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
    <Files ~ "\.(cgi|shtml|phtml|php3?)$" >
        SSLOptions +StdEnvVars
    </Files>
<Directory "/srv/moodle/www/cgi-bin">
    AllowOverride None
    Options +ExecCGI -Includes
    Order allow,deny
    Allow from all
</Directory>
<Directory "/srv/moodle/www">
    Options Indexes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog /var/log/apache2/ssl_request_log    ssl_combined

```



```
</VirtualHost>
```

```
<VirtualHost *:443>
    DocumentRoot "/srv/www/htdocs/online"
    ServerName reservation.brg-wrn.ac.at:443
    ServerAlias reservation.brgg.at
    ServerAdmin sta@brg-wrn.ac.at
    ErrorLog /var/log/apache2/error_log
    TransferLog /var/log/apache2/access_log
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/ssl.crt/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
    <Files ~ "\.(cgi|shtml|phtml|php3?)"$">
        SSLOptions +StdEnvVars
    </Files>
    <Directory "/srv/www/cgi-bin">
        SSLOptions +StdEnvVars
    </Directory>
    SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
    CustomLog /var/log/apache2/ssl_request_log    ssl_combined
```

```
</VirtualHost>
```

```
<VirtualHost *:443>
    DocumentRoot "/srv/anmeldung"
    ServerName anmeldung.brg-wrn.ac.at:443
    ServerAlias anmeldung.brgg.at
    ServerAdmin webmaster.anmeldung@brg-wrn.ac.at
    ErrorLog /var/log/apache2/anmeldung_error_log
    CustomLog /var/log/apache2/anmeldung-access_log combined
    TransferLog /var/log/apache2/access_log
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLCertificateFile /etc/apache2/ssl.crt/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
    <Files ~ "\.(cgi|shtml|phtml|php3?)"$">
        SSLOptions +StdEnvVars
    </Files>
    <Directory "/srv/anmeldung">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from all
    </Directory>
    SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
    CustomLog /var/log/apache2/ssl_request_log    ssl_combined
```

```
</VirtualHost>
```

```
</IfDefine>
```

```
</IfDefine>
```



3.2 CMS – Systeme:

Im Wikipedia Lexikon findet man folgende Definition eines CMS Systems:

Content-Management-Systeme sollen die Trennung von [Inhalt](#), [Gestaltung](#) und [Funktion](#) beherrschen und verschiedene Navigationsstrukturen ermöglichen.

Der Benutzer sollte das System auch ohne Programmierkenntnisse bedienen können, ebenso sollte er das System auch ohne Kenntnis von [HTML](#) bzw. [XML](#) bedienen können.

Besonderen Wert wird auch auf eine medienneutrale Datenhaltung gelegt. So sollte ein Inhalt auf Wunsch beispielsweise als [PDF](#) oder als [HTML](#)-Dokument abrufbar sein können, indem die Formate zur Laufzeit aus der Datenbank generiert werden. Auch [Barrierefreiheit](#) sollte vom System unterstützt werden.

Je nach Anwendung kann auch eine [Rechteverwaltung](#) von Bedeutung sein.

Die bekanntesten freien CMS Systeme basieren üblicherweise auf einer Kombination aus (My)SQL Datenbank und Webserver mit PHP

3.2.1 MAMBO

Homepage: <http://www.mamboserver.com/>

Installation: Das Source Paket via Web herunterladen und in ein Verzeichnis (im Bereich des Webservers) entpacken. Unter SuSE ist es noch notwendig, das Paket „PHP4_session-support“ nachzuinstallieren.

WICHTIG: Die Dateien im Mambo-Verzeichnis sollten dem Benutzer wwwrun (= Benutzer unter dem der Webserver APACHE läuft) gehören.

Weitere Vorbereitung: Benutzer in Mysql vorbereiten, der die notwendigen Rechte auf jener Datenbank besitzt, in der die Mambo Daten abgelegt werden.

Danach ruft man im Webserver einfach den bereits vorhandenen Mamboserver auf. –Dieser wird danach via Web konfiguriert und eingerichtet.

3.2.2 TYPO3

Homepage: <http://typo3.org/>

Installation: Das Source Paket via Web herunterladen und in ein Verzeichnis (im Bereich des Webservers) entpacken. Unter SuSE ist es noch notwendig, das Memory Limit in der Datei /etc/php.ini zu erhöhen. Weiters ist es empfehlenswert ein Startpaket (z.B: Testsite) herunterladen und installieren.

Es empfiehlt sich (um einfacher Updates installieren zu können) die Source Pakete in ein eigenes Verzeichnis zu kopieren und aus der Testsite nur einen Link zu legen. Ein Upgrade auf eine neue Version von Typo3 geschieht durch Kopieren der neuen Quellen in einen anderen Ordner und ein Umlegen des Links.

WICHTIG: Damit der Webserver den Links folgen darf ist eine Anpassung der Konfiguration notwendig (Options FollowSymLinks)

WICHTIG: Die Dateien im Typo3-Verzeichnis sollten dem Benutzer wwwrun (= Benutzer unter dem der Webserver APACHE läuft) gehören.

Weitere Vorbereitung: Benutzer in Mysql vorbereiten, der die notwendigen Rechte auf jener Datenbank besitzt, in der die Typo3 Daten abgelegt werden.

Danach ruft man im Webserver einfach den bereits vorhandenen Typo3-Server auf. –Dieser wird danach via Web konfiguriert und eingerichtet.



Typo3 bietet unter anderem ein umfangreiches Online-Repository, in dem gratis Tools für Typo3 zur Verfügung gestellt werden. Um dieses Pool verwenden zu können ist eine Registrierung auf typo3.org notwendig.

3.2.3 MOODLE (ELearning)

Homepage: <http://www.moodle.org/>

Installation: Das Source Paket via Web herunterladen und in ein Verzeichnis (im Bereich des Webservers) entpacken. WICHTIG: Die Dateien im Moodle-Verzeichnis sollten dem Benutzer wwwrun (= Benutzer unter dem der Webserver APACHE läuft) gehören.

Weitere Vorbereitung: Benutzer in Mysql vorbereiten, der die notwendigen Rechte auf jener Datenbank besitzt, in der die Moodle Daten abgelegt werden. Die Datenbank muss extern (z.B. mit phpMyAdmin) angelegt werden

Danach ruft man im Webserver einfach die bereits vorhandene Moodleinstallation auf. – Die Installation wird danach via Web fertiggestellt.

4 CRON:

Zur Steuerung dieser automatischen Abläufe dient die Datei /etc/crontab:

```
SHELL=/bin/sh
PATH=/usr/bin:/usr/sbin:/sbin:/bin:/usr/lib/news/bin
MAILTO=root
#
# check scripts in cron.hourly, cron.daily, cron.weekly, and cron.monthly
#
-*/15 * * * * root test -x /usr/lib/cron/run-crons && /usr/lib/cron/run-crons >/dev/null 2>&1
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 0 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 0 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 0 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

Die Syntax dieser Datei kann mit “man 5 crontab” nachgelesen werden.

AUSZUG:

The time and date fields are:

field	allowed values
----	-----
minute	0-59
hour	0-23
day of month	1-31
month	1-12 (or names, see below)
day of week	0-7 (0 or 7 is Sun, or use names)

EXAMPLE CRON FILE

```
# use /bin/sh to run commands, no matter what /etc/passwd says
SHELL=/bin/sh
# mail any output to `paul', no matter whose crontab this is
MAILTO=paul
#
# run five minutes after midnight, every day
5 0 * * * $HOME/bin/daily.job >> $HOME/tmp/out 2>&1
# run at 2:15pm on the first of every month -- output mailed to paul
15 14 1 * * $HOME/bin/monthly
# run at 10 pm on weekdays, annoy Joe
0 22 * * 1-5 mail -s "It's 10pm" joe%Joe,%%Where are your kids?%
```



```
23 0-23/2 * * * echo "run 23 minutes after midn, 2am, 4am ..., everyday"
5 4 * * sun echo "run at 5 after 4 every sunday"
```

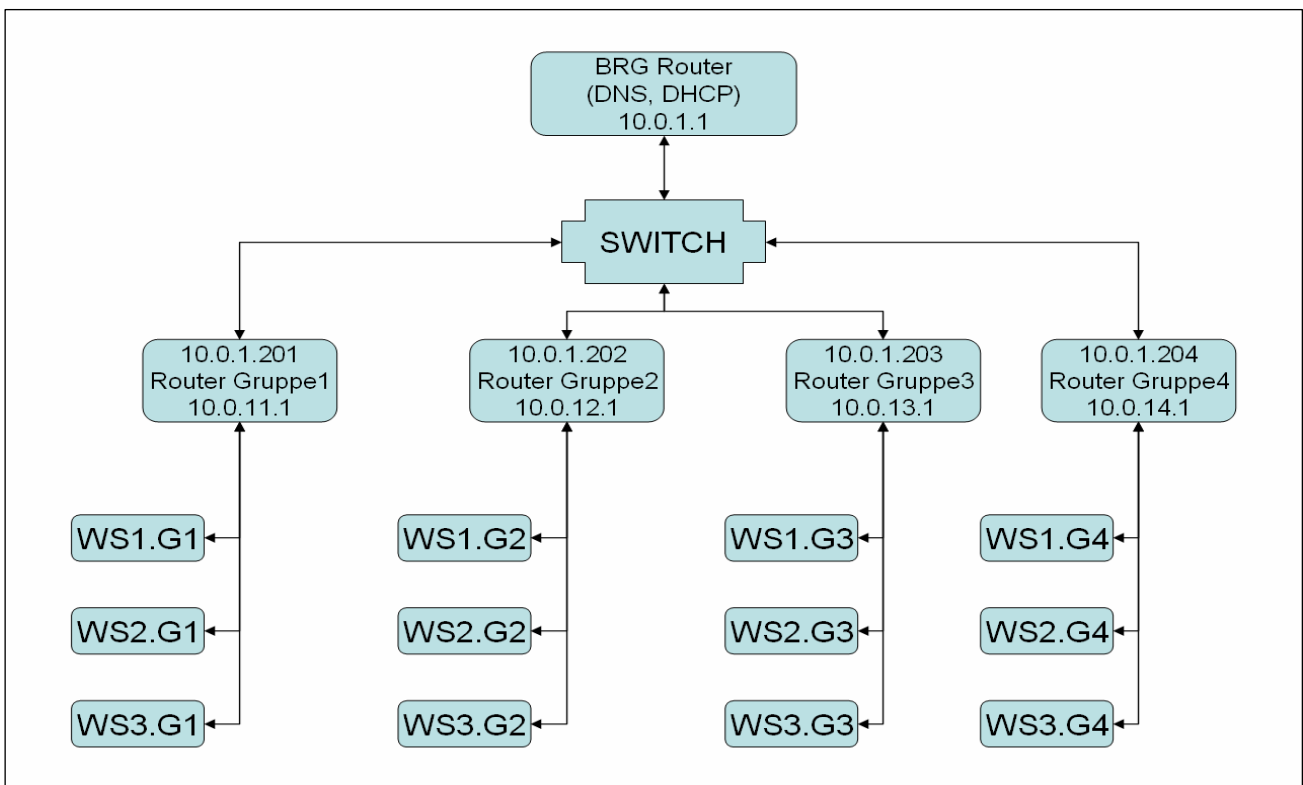
Wenn spezielle Dienste nicht zu einem gewissen Zeitpunkt ablaufen müssen gibt es eine einfachere Methode, als direkt in der Datei crontab Veränderungen vorzunehmen. Unter SuSE gibt es im /etc Verzeichnis 4 Ordner (cron.daily, cron.weekly, cron.monthly, cron.hourly), in die nur das entsprechende Skript hineinkopiert oder verlinkt wird.

Als Beispiel könnte z.B. ein Skript dienen, dass jede Nacht automatisch ein Backup der Homepage in ein tar-Archiv macht.

(Hilfe zum tar Befehl liefert z.B. „man tar“)

```
tar -c -f /root/homepage.tar.gz /srv/www (in eine Skriptdatei einfügen)
```

5 Aufbau der Seminartopologie



Die Gruppenrouter (Linuxrechner mit 2 Netzwerkkarten) sind über einen Switch mit dem Hauptrouter des BRG Netzwerkes verbunden. Die IP-Adressen der Gruppenrouter sind lt. Skizze fix einzustellen. Für die Arbeitsstationen der einzelnen Gruppen sind vorerst fixe IP-Adressen aus dem jeweiligen Netz zu verwenden. Die Bezeichnungen der Rechner sind auch dem abgebildeten Schema zu entnehmen. Alle verwendeten Netze (auch das Hauptnetz in der Verbindung zum BRG Router) sind mit einer C-Klasse Netzwerkkarte (255.255.255.0) zu versehen.

Damit die Gruppenrouter tatsächlich als Router (Paketweiterleitung) agieren ist die Systemvariable „IP_FORWARD“ auf „YES“ zu setzen. Dies kann am einfachsten über das YAST-Modul „Editor für Sysconfig-Dateien“ erfolgen.



5.1 Testen der Netzwerkverbindungen:

Bevor nun versucht wird, weitere Netzwerkdienste aufzubauen, sollte man versuchen, ob die Netzwerkverbindungen auf dieser Ebene bereits funktionieren. Dazu stehen (auf praktisch allen Systemen) zwei Routinen zur Verfügung: (Bevor man jedoch diese Tests durchführt empfiehlt sich eine Kontrolle der Netzwerkeinstellungen, die mit dem Befehl **ifconfig** an der Konsole durchgeführt werden kann.)

5.1.1 PING

ping 131.130.1.11: Schickt Pakete an die Adresse 131.130.1.11 und notiert die Antwortzeiten. Damit sollte man überprüfen, ob man die eingeschalteten Rechner in den Subnetzen, bzw. ob man Rechner im Internet erreichen kann. Sollten hier Fehler sichtbar werden, deren Ursache noch nicht ganz klar ist, kann man weitere Informationen mittels Traceroute erhalten.

5.1.2 TRACEROUTE

traceroute 131.130.1.11: Versucht ebenfalls den Rechner mit der Adresse 131.130.1.11 zu erreichen, wobei auch Informationen über den Weg zu diesem Rechner geliefert werden (Über welche Router). Damit kann man den Weg nachvollziehen und erkennen, bei welchem Router das Problem entsteht.

5.2 Ausbau der Konfiguration auf Layer 3 – Routing:

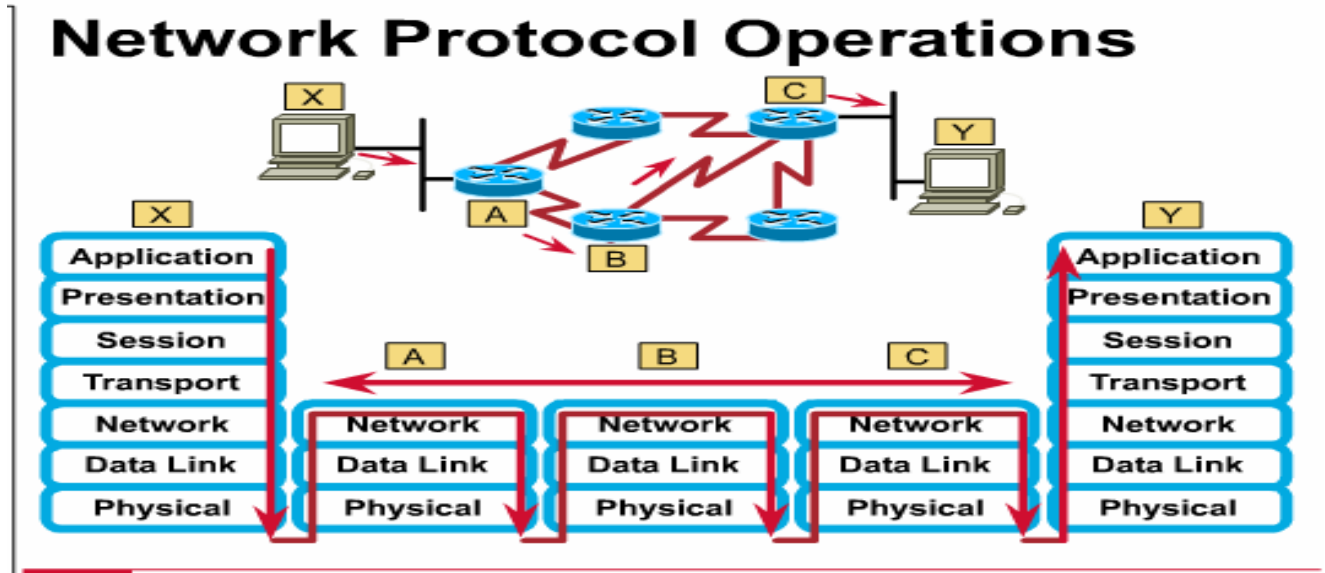
Damit die Rechner nicht nur Arbeitsstationen im eigenen Netz erreichen können, sind auf der sogenannten Netzwerkschicht (OSI – Modell Layer 3) noch einige Parameter anzupassen. Diese Einträge betreffen das Weiterleiten der Datenpakete. Dazu muss die Routingtabelle des Rechners angepasst werden.

Anzeigen der Routinginformationen: **ip route**

Zur Laufzeit kann diese Tabelle mit dem Befehl ip route verändert werden (siehe „man ip route“). Diese Veränderungen sind jedoch nach einem Neustart des Systems nicht mehr vorhanden. Damit diese Einträge dauerhaft gespeichert werden ist ein Eintrag in eine entsprechende Konfigurationsdatei erforderlich. Diese Einträge erstellt man über das YAST – Modul „Konfiguration der Netzwerkkarte“ → Routing.



Für den Router der Gruppe 1 ist z.B. einzutragen dass das Netz 10.0.12.0/255.255.255.0 über die Adresse 10.0.1.202 (externe Adresse des Gruppenrouters 2) zu erreichen ist. Ein Standardeintrag in dieser Tabelle ist das GATEWAY. Diese IP-Adresse ist das Ziel aller Datenpakete, die nicht in eine der anderen Routingeinträge passen.



5.3 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.

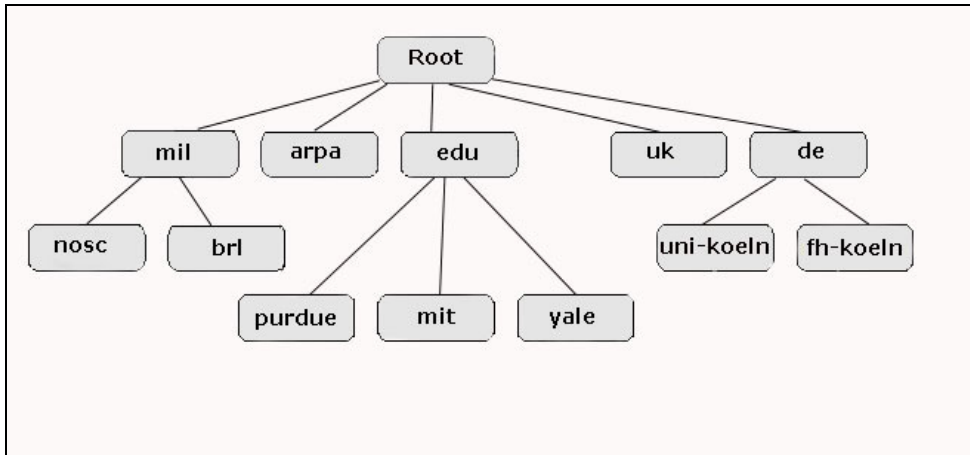
Auszug aus einer hosts-Datei:

```
# 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
```

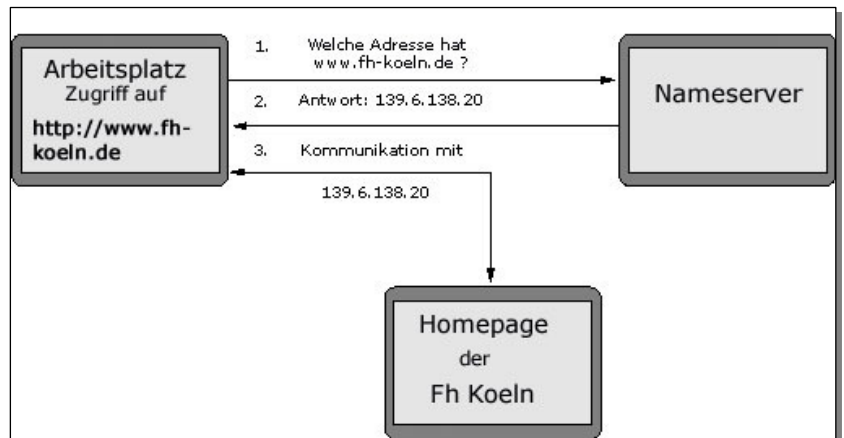
6 DNS – Domain Name System (Port 53 –udp):



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 Namenen)
#
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)



7 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.

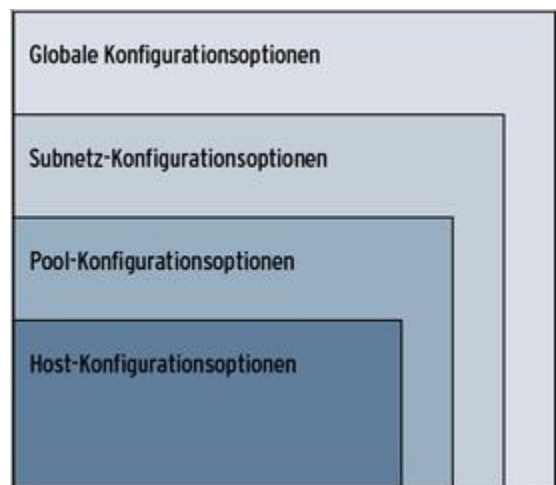
Wenn der Client bootet, fragt er mit einem DHCPDISCOVER per Broadcast nach seiner Client-Konfiguration. Der Client hat zu diesem Zeitpunkt noch keine (nutzbringende externe) IP, sondern nur seine MAC-Adresse (weltweit eindeutige, auf der Netzwerkkarte kodierte Ethernet-Adresse). Darum bekommt das Broadcast-Paket 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 "xxxxxxx ";
    allow-update { 127.0.0.1; };
};
zone "11.0.10.in-addr.arpa" {
    type master;
    file "yyyyyy";
    allow-update {localhost; };
};
```

8 Benutzerplatzbeschränkung:

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 -acuvgm* 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.



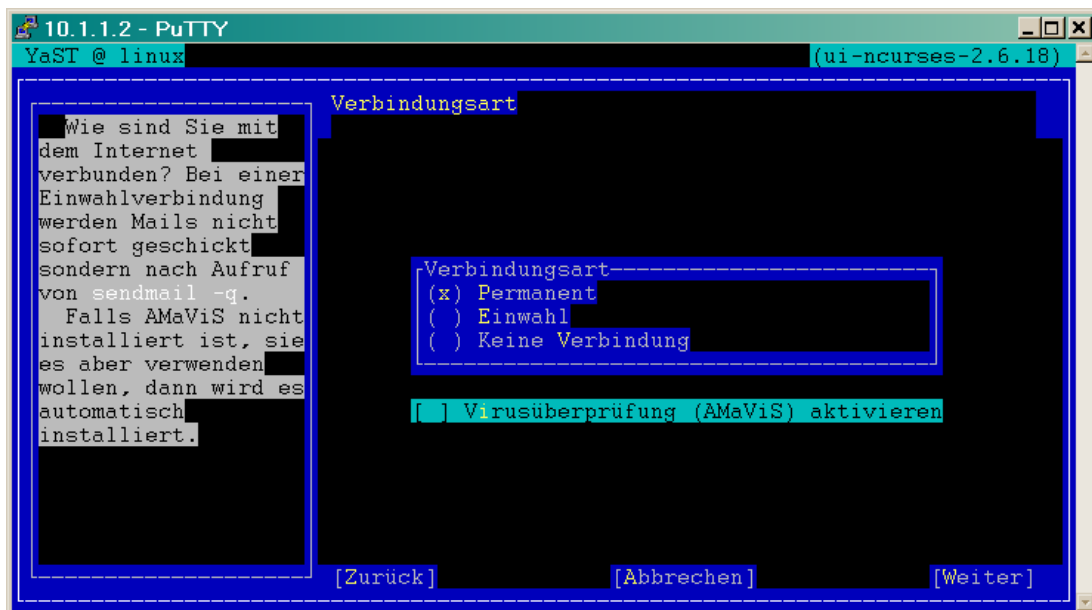
9 Mail-Server:

Eine Email-Adresse besteht grundsätzlich aus 2 Teilen, der Benutzerkennung und einem gültigen Internetnamen für einen Rechner. Diese beiden Teile werden durch das Zeichen @ getrennt. Wenn ihr Linuxrechner z.B. den Internetnamen mail.DOMÄNE.ac.at (wobei DOMÄNE für die Domänbezeichnung ihrer Schule steht) hat und sie auf diesem Rechner (z.B. mit YAST) einen Benutzer mit Namen Kurt anlegen, hat dieser Benutzer automatisch die (weltweit gültige) Email-Adresse kurt@mail.DOMÄNE.ac.at. Da ihr Rechner mit 3 Namen konfiguriert ist (www, mail, ftp) kann dieser Benutzer auch Mails auf kurt@www.DOMÄNE.ac.at und kurt@ftp.DOMÄNE.ac.at empfangen. Die Domänbezeichnung selbst ist eigentlich keine Adresse für einen Rechner. Damit (einfachere) Emailadressen wie kurt@DOMÄNE.ac.at möglich sind, wird ein MailExchange (MX) Eintrag für DOMÄNE.ac.at gemacht, der definiert, welcher Rechner die Domänmails erhalten soll. Diese Eintragungen sind am Nameserver durchzuführen. Der Nameserverdienst für fast alle Schulen in NÖ wird vom LSR übernommen (Ing. Wirlach). Damit dies auch funktioniert, sind für das Programm SENDMAIL am Linuxrechner noch einige einfache Konfigurationsarbeiten notwendig. Grundsätzlich besteht ein Mailserver aus zwei verschiedenen Diensten:

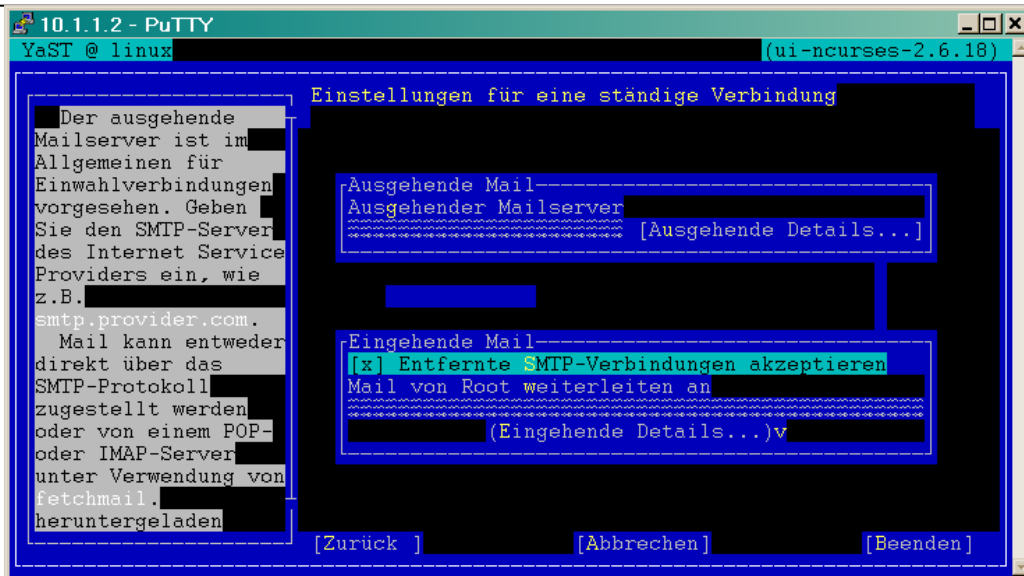
9.1 SMTP : (Postfix – Port 25)

Verantwortlich für den Versand von Nachrichten. (Simple Mail Transport Protocol) Dieser Dienst wird heute z.B. von Postfix erledigt, einem Nachfolger für das bereits etwas in die Tage gekommene Paket SENDMAIL, das diese Aufgabe früher erledigt hat.

Ein Großteil der Konfiguration kann bereits via YAST vorgenommen werden:

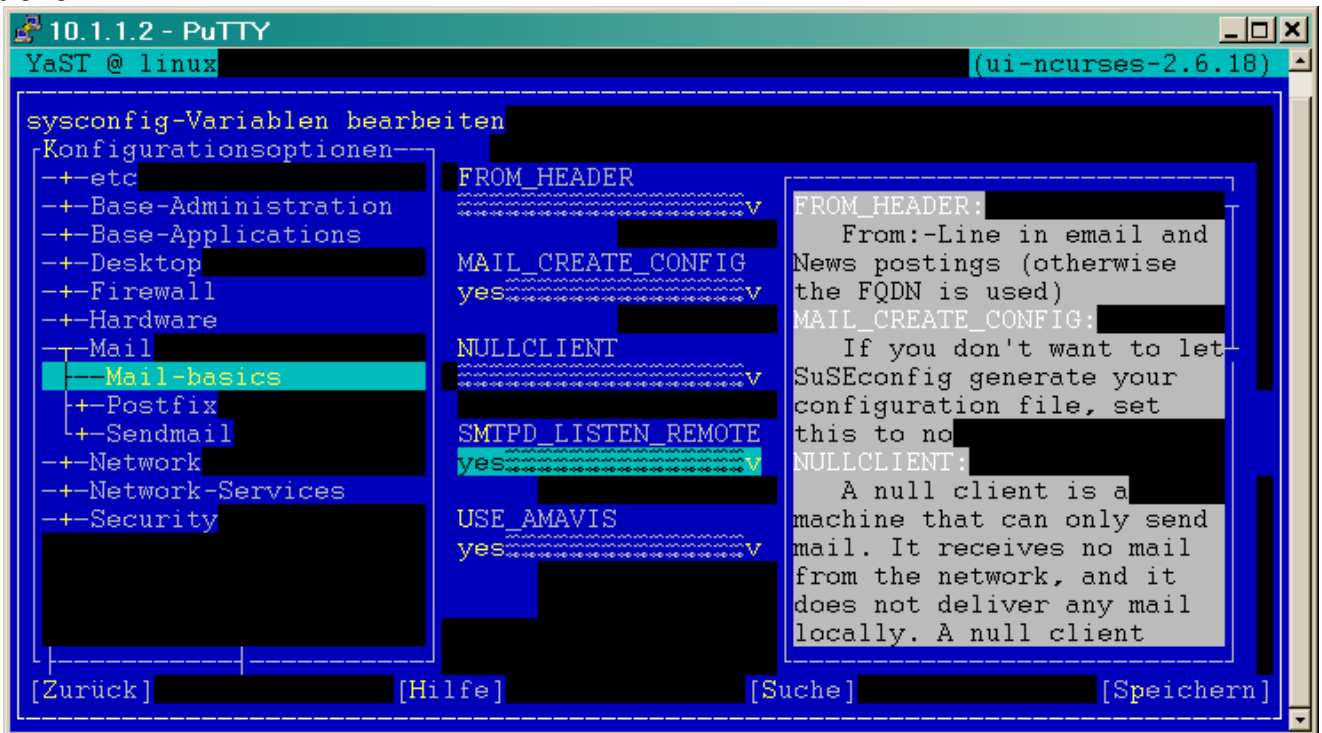


Amavis einschalten



Versenden von Emails über den Linuxrechner auch von anderen Rechnern aus erlauben

Über den Sysconfig Editor (Yast-Modul) werden noch Einträge bearbeitet, die den Mailversand betreffen:



Sendmail Einstellungen

Im Parameter sendmail_localhost ist z.B. folgendes einzutragen: mail.brg-wrn.ac.at www.brg-wrn.ac.at brg-wrn.ac.at

Wenn die Eintragungen auch am Nameserver passend vorgenommen wurden, sollte einem funktionsfähigen Betrieb als Mailserver nichts mehr im Wege stehen. Bei Postfix können (wenn sie einen entsprechenden Parameter im Sysconfig Editor aktivieren (SMTP_LISTEN_REMOTE) automatisch alle Rechner aus den direkt angeschlossenen Subnetzen Mails versenden. Besteht ihr Netzwerk aus einer komplexeren Konfiguration müssen sie über den Parameter mynetworks= „.....“ (in der Datei main.cf) jene Netze angeben, die Mails über diesen Rechner versenden dürfen.

Bei Sendmail geschieht Ähnliches in folgender Datei:

/etc/mail/access:

Gerald STACHL



```
brg-wrn.ac.at    OK
192.168.        OK
```

Diese Konfiguration erlaubt das Weiterleiten von Mails, wenn sie von Rechnern kommen, die der Domäne brg-wrn.ac.at oder dem B-Klasse Netzwerk 192.168.x.x angehören.

Die Textdatei muss nun in ein Datenbankformat übersetzt werden:

makmap hash /etc/mail/access.db < /etc/mail/access oder nur aufrufen von SuSEconfig

Danach muss Sendmail neu gestartet werden (rcsendmail restart). Falls der Rechner noch nicht zur Zufriedenheit funktioniert, empfiehlt es sich einmal den Rechner neu zu starten.

Wenn sie nun auf ihrem Linuxrechner einen Benutzer anlegen erzeugen sie damit automatisch einen Email-Account. Am Client tragen sie als Mailserver (POP3, SMTP) jeweils die IP-Adresse oder DNS-Namen ihres Linuxrechners ein. Als POP3-Account verwenden sie den Benutzernamen und das zugehörige Passwort.

Wenn eine Mail nun an ihren Linuxrechner gesendet wird (aus dem Internet) und Sendmail diese Nachricht als lokal zustellbar erkennt, wird die Nachricht in das Postfach des entsprechenden Benutzers eingeordnet. Das Postfach ist einfach eine Datei im Verzeichnis /var/spool/mail, an die die Nachricht angehängt wird.

Eine zu versendende Mail wird in die Mail-Warteschlange (/var/spool/mqueue) eingeordnet. Diese Warteschlange wird in periodischen Abständen (ca. 10min.) abgearbeitet.

Weitere Infos siehe: <http://www.pinoe-hl.ac.at/arge/ahsinf/linuxmail.htm>

Die Mailqueue kann (Kompatibilität zu Sendmail) mit dem Befehl mailq angesehen werden. Mit dem Befehl postsuper (man postsuper) kann z.B. auch die Mailqueue gelöscht werden:
postsuper -d ALL

9.1.1 DETAILS SMTP:

von der Kommandozeile (mit mail):

```
mail -s „SUBJECT“ EMPFÄNGER
DATEN
DATEN
.           {Der Punkt bedeutet Ende der Mail}
```

mittels telnet auf Port 25 (des Mailserver) (telnet RECHNER 25)

```
HELO      gast.domain      (Bezeichnung des Clientrechners)
MAIL FROM: abc@gast.domain (Absender)
RCPT TO:  cde@mailserver.domain (Empfänger)
DATA
Subject:  Kurzbezeichnung
Daten
.....
Daten
.
QUIT
```

9.2 POP3: (PORT: 110)

Das PostOfficeProtokoll ist verantwortlich für das Abholen der Post aus dem Postfach. Damit dies funktioniert muss am Linuxrechner ein POP3-Serverdienst laufen. Dieser Dienst (qpopper oder ipop3d aus dem Paket imap) wird als Teil des inetd gestartet. (siehe Zeile in inetd.conf)



```
# Pop et al
#
# pop2 stream tcp  nowait root  /usr/sbin/tcpd  ipop2d
# pop3 stream tcp  nowait root  /usr/sbin/tcpd  ipop3d
# pop3 stream tcp  nowait root  /usr/sbin/tcpd  /usr/sbin/popper -s
```

POP3 Sitzung:

Sobald man bei einem Pop3 Server eingeloggt ist, wird das Postfach gesperrt (Transaktionsphase)

Kommandos	Bedeutung
APOP	Verschlüsseltes Einloggen (Optional)
DELE	Markiert eine Nachricht als gelöscht.
LAST	Gibt die höchste bisher bearbeitete Nachrichtennummer zurück.
LIST	Gibt die Größe der Nachricht(en) zurück.
NOOP	No Operation, gibt einen positiven Wert zurück, falls der Server noch lebt.
PASS	Übermittelt das Passwort für USER
RSET	Setzt die Markierung aller als gelöscht markierten Nachrichten zurück.
RETR	Holt eine komplette Nachricht (Head und Body).
STAT	Ermittelt die Anzahl der vorhandenen Nachrichten und die Größe der Mailbox.
TOP	Holt den Header und die angegebenen Zeilen der Nachricht.
TOP 10 5	holt den Header und die ersten 5 Zeilen von Nachricht 10. (Optional)
UIDL	(Unique ID Listing) Fragt nach der eindeutigen Kennung der Nachricht. (Optional)
USER	Übermittelt den Usernamen für die Mailbox (maildrop)
QUIT	Beendet die Verbindung. Löscht alle als gelöscht markierten Mails.

9.3 IMAP: (PORT 143)

IMAP in inetd.conf

```
#
# Imapd - Interactive Mail Access Protocol server
# Attention: This service is very insecure
# imap stream tcp  nowait root  /usr/sbin/tcpd  imapd
#
```

Als Alternative zu POP3 können die Mails auch via IMAP betrachtet werden. Der Hauptgrund für die Einführung von IMAP liegt in der Tatsache, dass, wenn die Mails via POP3 vom Server heruntergeladen werden sie nur auf dem einen lokalen Rechner vorliegen auf dem man arbeitet. Wenn man nun von mehreren Rechnern aus arbeitet ist am aktuellen Rechner immer nur ein Teil der Mails vorhanden. Alternative: Die Mails bleiben am Server liegen. → IMAP (<http://www.imap.org>)

- Key goals for IMAP include:
- Be fully compatible with Internet messaging standards, e.g. MIME.
- Allow message access and management from more than one computer.
- Allow access without reliance on less efficient file access protocols.
- Provide support for "online", "offline", and "disconnected" access modes *
- Support for concurrent access to shared mailboxes
- Client software needs no knowledge about the server's file store format.

9.4 Virens scanner:

Ab SuSE 7.2 ist eine Email-Virens scannerlösung implementiert. Dazu wird über die Variable START_AMAVIS der Virens scanner gestartet. Über die in der Datei sendmail.cf eingestellte



Option wird bereits standardmäßig jede Mail zunächst von Amavis entpackt an den Virenschanner Antivir übergeben und geprüft. Nur wenn keine Viren gefunden werden wird die Mail an den Empfänger weitergeleitet. Neuere Virendefinitionen kann man sich von www.antivir.de herunterladen. Diese Definitionen müssen dann ins Verzeichnis /var/lib/AntiVir abgelegt werden.

Die infizierten Mails werden unter /var/spool/vscan/..... abgelegt.

SuSE 8.x:

Für AntiVir existiert ein Konfigurationsskript: /etc/antivir.conf

```
#
# Sample AntiVir configuration file
#

# You can receive email notifications of viruses using this
# directive. You must specify the email address to which the
# notification will be sent. There is no default value for
# this directive.
EmailTo xyz@abschule.ac.at

# Virus activity may also be logged to a specified file
# (in addition to syslog). You must specify the file. There
# is no default value for this directive.
LogTo /var/log/antivir.log

# New engine and virus data files can be automatically
# updated via the internet. Please use only one of the
# following options as the last one will be taken. You
# can choose to have the automatic updates be every 2 hours
# or once a day. If neither directive is given, the
# automatic internet updater will be disabled.
# Note: Internet updates can also be done manually using
# the --update parameter with the command line
# scanner.
#AutoUpdateEvery2Hours
#AutoUpdateDaily

# If automatic updates are done daily, you can specify
# at what time of day the updates should be done.
#AutoUpdateTime 4:23
```

Die letzten Optionen bieten die Möglichkeit ein automatisches Aktualisieren der Virendefinitionen vorzunehmen. Eine andere Möglichkeit bietet der Befehl „antivir - - update“ der als CRON Job aufgerufen werden kann. Damit wird dieser Befehl zu einem bestimmten Zeitpunkt automatisch ausgeführt.

Bei SUSE 9.2 wird neben dem Virenschanner auch ein Spamfilter (SPAMASSASSIN) installiert. Hier wird automatisch der SpamDämon (spamd) installiert. Über das Filterskript AMAVIS werden die Mails nun zuerst nach Viren gescannt und danach an den Spamdämon weitergegeben, bevor sie zugestellt werden.

Weiterführende Informationen zu SpamAssassin findet man auf der Projekthomepage (<http://spamassassin.apache.org>). Die Hauptkonfigurationsdatei dieses Dienstes findet man am System im Ordner /etc/mail/spamassassin - local.cf). Welche Optionen hier verwendet werden können kann auf der ManualPage nachgelesen werden (man Mail::Spamassassin::Conf)

9.5 NACHTRAG zu POP3 und IMAP:

In beiden Protokollen werden die Benutzerdaten unverschlüsselt über das Netz übertragen. Diese Sicherheitslücke könnte man mit einigem Zusatzaufwand schließen, da beide Server die Möglichkeit bieten auf mit Verschlüsselung zu arbeiten (APOP, SSL,...) Hinweise dazu findet man in den Dokumentationen der Pakete qpopper oder imap (im Verzeichnis /usr/share/doc/packages)



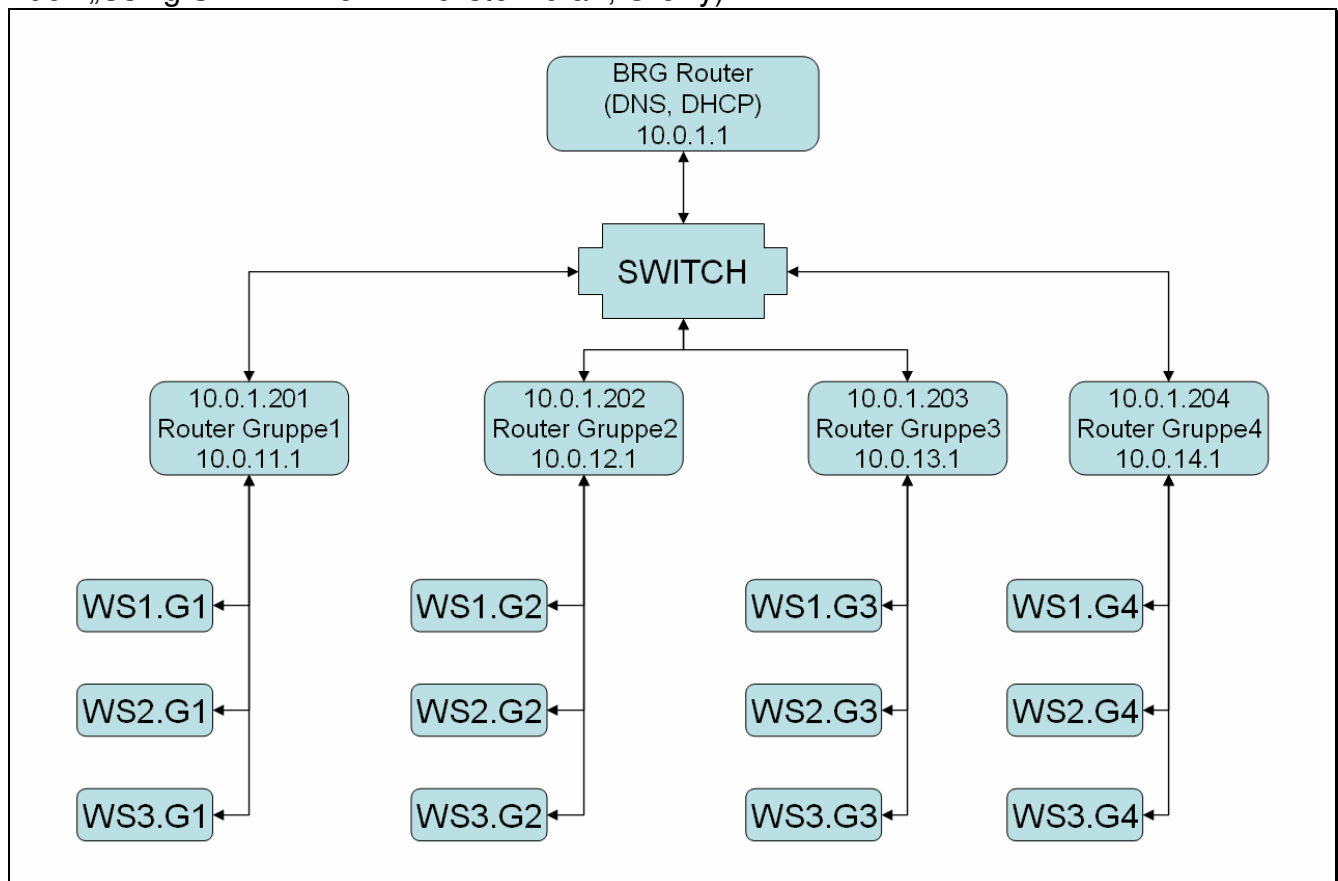
9.6 WebMailInterface:

Im Internet findet man viele Lösungen die (gratis) ein Webmailinterface für POP3 u.a. Server zur Verfügung stellen. Eine Lösung (die ich in der Schule verwende) findet man unter:

<http://uebimiau.sourceforge.net/>

10 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)



10.1 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.



10.2 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.



10.3 Passwörter:

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

Table 6.5: Windows Operating Systems with Encrypted Passwords

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)



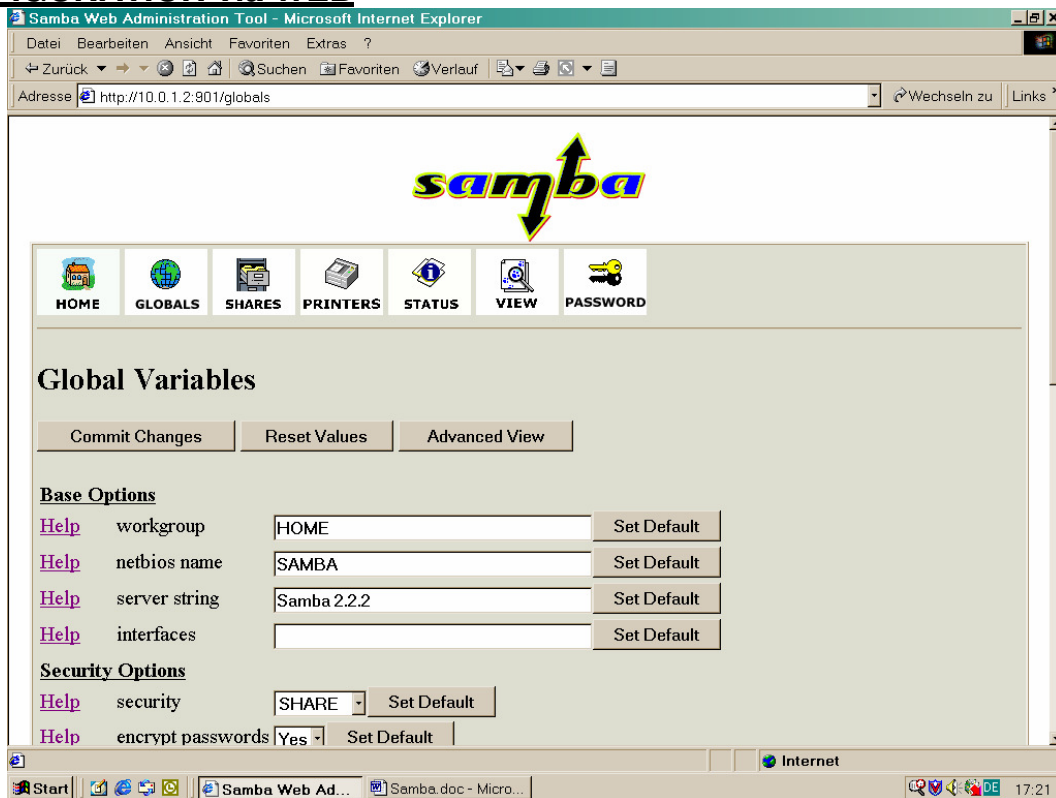
10.4 OS-Level:

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.

10.5 KONFIGURATION via WEB





LINUX - EINFÜHRUNG

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)

10.6 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	Infos in Netzwerkumgebung
Help path	Wo liegt der Share im Dateisystem

Security Options

	Benutzernamen oder @Gruppe
Help username	
Help guest account	nobody
Help invalid users	Wer darf nicht
Help valid users	Wer darf
Help admin users	Wer verwaltet den Share
Help read list	Leseberechtigung
Help write list	Schreibberechtigung
Help force user	Für das Erstellen
Help force group	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="low er"/>
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	<input type="text" value="No"/>
Help	map hidden	<input type="text" value="No"/>
Help	map archive	<input type="text" value="Yes"/>
Help	mangled names	<input type="text" value="Yes"/>
Help	mangled map	<input type="text"/>

Browse Options

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

Locking Options

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

Miscellaneous Options

Help	exec	<input type="text"/>
Help	preexec close	<input type="text" value="No"/>
Help	postexec	<input type="text"/>
Help	root preexec	<input type="text"/>
Help	root preexec close	<input type="text" value="No"/>
Help	root postexec	<input type="text"/>
Help	available	<input type="text" value="Yes"/>
Help	volume	<input type="text"/>
Help	fstype	<input type="text" value="NTFS"/>
Help	set directory	<input type="text" value="No"/>
Help	wide links	<input type="text" value="Yes"/>



Help	follow symlinks	<input type="text" value="Yes"/>
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"/>

10.7 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.

10.8 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.

10.9 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.
 %I The IP address of the client machine.
 %T the current date and time.
 %\$(*envvar*) The value of the environment variable *envvar*.

10.10 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.

10.11 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
>
```

10.11.1 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 Zugangsdaten 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.

10.11.2 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.

10.11.3 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`).

10.11.4 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.

10.11.5 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
```

10.11.6 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_KEEPAIVE
>
```

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.

10.11.7 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.

10.11.8 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.

10.11.9 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.

10.11.10 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 strenger 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.

10.11.11 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.

10.11.12 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.

10.12 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.

10.12.1 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 Namenserweiterung - insgesamt eben besagte zwölf Zeichen.

10.12.2 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.

10.12.3 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.



10.12.4 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`.

10.12.5 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 Dateien vorhanden sein: `ADFONT.SMF`, `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.

10.12.6 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.

10.12.7 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.

10.12.8 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.

10.12.9 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,



LINUX - EINFÜHRUNG

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.