Technische Universität München

Systementwicklungsprojekt / Fortgeschrittenen Praktikum

Integration von MS Windows 2000 Clients in die bestehende Infrastruktur des CIP-Pools der Informatik

Lehrstuhl Informatik XV - Rechnernetze/LRZ

Aufgabensteller: Prof. Dr. H.-G. Hegering

Betreuer: Annette Kostelezky - Max Jakob

Bearbeiter: Stephan Meyer - Philipp Promesberger

Inhaltsverzeichnis

1 Einleitung

Das Institut für Informatik stellt für Studenten/innen Rechnerarbeitsplätze in sogenannten CIP-Pools zur Verfügung. In diesen Pools können Studenten/innen vorlesungsbegleitende Übungen sowie anfallende, rechnergestützte Arbeiten im Rahmen ihres Studiums erledigen. Für die Arbeitsplatzrechner, den Clients, wird das Betriebssystem Linux verwendet. Auf den, für die Studenten/innen transparenten, Servermaschinen kommen Linux und andere UNIX-Derivate als Betriebssysteme zum Einsatz. Für die Konfiguration und Wartung der Rechner und Dienste ist die Rechnerbetriebsgruppe - kurz RBG - , eine kleine Gruppe von Personen, mitunter auch studentische Hilfskräfte, verantwortlich.

Mit Einführung des neuen Studiengangs Medieninformatik an der Ludwig-Maximilian-Universität München sollen 20 Rechner mit MS Windows 2000 Professional Betriebssystem und mit Anwendungen für MS Windows in die Infrastruktur des bestehenden CIP-Pools integriert werden. Auf den neuen Rechnern sollen parallel zwei Betriebssystem betrieben werden, wie bereits erwähnt MS Windows 2000 Professional und zusätzlich Linux. Unter MS Windows sollen den Studenten/innen für die Medieninformatik spezifische Software sowie Microsoft Office Produkte, Internetzugang und Druckdienste zur Verfügung gestellt werden. Die Linux Umgebung soll der bekannten Umgebung der bereits bestehenden Rechner des CIP-Pools entsprechen.

Diese Arbeit beschäftigt sich mit der Integration der MS Windows 2000 Rechner in die Linux/UNIX Umgebung des CIP-Pools. Die nachfolgenden Kapitel sollen eine Anleitung zur Realisierung der Integration geben, indem sie die benötigte Infrastruktur, die Installationsvorgänge und Einrichtung der benötigten Dienste beschreiben.

2 Vorgaben und Ziele

Dieses SEP/Fopra soll die Grundvoraussetzungen für den geplanten Medieninformatikraum schaffen. Basierend auf den Bedürfnissen der Studenten/innen und des Praktikums zur Vorlesung Medieninformatik, ist es unsere Aufgabe, anhand einer Testumgebung eine Grundkonfiguration zu erstellen. Das bedeutet, wir müssen eine geeignete Netzwerktopologie wählen, um die Windows-Welt an die Linux-Welt des restlichen CIP-Pools anzubinden. Desweiteren ist die Installation und Konfiguration einiger zusätzlicher Dienste nötig, damit die späteren Benutzer/innen des Windows-Pools auf bestimmte Dienste der Linux-Welt, wie z.B. Daten, Druck, WWW, etc. zugreifen können.

Bevor wir auf die Installations- und Konfigurationsdetails eingehen, wollen wir noch die Randbedingungen für die geplante Infrastruktur, sowie die geplante Hard- und Softwareausstattung vorstellen.

2.1 Randbedingungen

Dieser Abschnitt beschreibt die Randbedingungen, welche bei der Umsetzung dieses SEP/Fopras maßgebend waren.

Der Windows-Pool soll nur Studenten/innen der Medieninformatik zugänglich sein. Allerdings sollen diese unter Windows auch auf ihre Linux-Home-Verzeichnisse, sowie den Druckserver des CIP-Pools zugreifen können. Dazu benötigen wir einen Dienst, der der Windows-Welt Freigaben im SMB-Protokoll zur Verfügung stellt. SMB steht für ServerMessageBlock und bezeichnet das Standard-Protokoll, welches viele Betriebssysteme zum Verwalten von Netzwerkresourcen verwenden. Desweiteren soll die Benutzerverwaltung zentralisiert werden, um nicht auf jedem Windows-Rechner alle berechtigten Benutzer anlegen zu müssen.

Um den Aufwand für die Sicherheitsvorkehrungen auf Softwareseite zu verringern, soll das Netzwerk des Windows-Pools physikalisch getrennt vom Netz des restlichen CIP-Pools betrieben werden. Die Verbindung zum Netzwerk der Informatik soll durch einen lokalen Server bereitgestellt und geregelt werden.

Auf den Studentenarbeitsplätzen sollen hauptsächlich für die Medieninformatik relevante Software, Officesoftware und Kommunikation via Internet bereitgestellt werden. Um die Sicherheit und Zuverlässigkeit der Rechner zu erhöhen, müssen einige Vorkehrungen, wie Einschränkung der Benutzerrechte, Regulierung des Netzwerkzugriffs, etc. getroffen werden. Es muss verhindert werden, dass Benutzer/innen des Windows-Pools systemspezifische Einstellungen auf den Rechnern verändern können. Das Ziel ist, dass auf den Windows-Rechnern lokal keine Daten gespeichert werden können, d.h. die Windows-Rechner sollen als reine Arbeitsplattformen dienen.

Aus Sicht der Operatoren/innen soll sich der Installations-, Konfigurations- und der nachfolgende Verwaltungsaufwand in Grenzen halten, das heißt, in möglichst geringer Zeit realisierbar sein. Die Vereinfachung der Installation kann durch geeignete Vervielfältigungsstrategien erfolgen. Die Komplexität der Konfiguration hängt zum großen Teil von der Qualität dieser Arbeit ab. Der Verwaltungsaufwand lässt sich nur schwierig abschätzen, da sich die Anforderungen an die Rechner jedes

Semester ändern können und Hardwareausfälle nicht vorhersehbar sind. Man kann jedoch durch entsprechende Zugriffsbeschränkungen auf die Rechner eine Fehlbedienung selbiger als Fehlerursache ausschließen.

2.2 Hard- und Software Umgebung

Der Raum, in welchem die Rechner aufgestellt werden, befindet sich in der Oettingenstr. 67, im Keller des Z-Blocks (Raumnummer Z11). Für die Erweiterung des CIP-Pools werden 21 Rechner auf PC-Basis, 20 Flachbildschirme sowie entsprechend viele Eingabegeräte (Tastaturen und Mäuse) bereitgestellt. Hinzu kommen Multimediageräte wie Headsets und Webcams.

Die Rechner sind mit Soundkarten, Netzwerkkarten sowie aktuellen PC Hardwarekomponenten (CPU,RAM,...) ausgestattet. Einer der 21 Rechner soll als Referenzrechner dienen. Ausgehend von diesem PC wird die Installation auf die restlichen Rechner kopiert, um eine einheitliche Installation zu gewährleisten.

Wie bereits in der Einleitung erwähnt, sollen auf den Studentenrechnern zwei Betriebssysteme, MS Windows und Linux, zum Einsatz kommen. Im Weiteren werden wir uns nur mit der Windows-Seite beschäftigen. Die Linux-Installation und -Konfiguration wird von der RBG übernommen.

3 Umsetzung

Dieses Kapitel befasst sich nun mit der Umsetzung der genannten Randbedingungen unter Berücksichtigung der vorhandenen Resourcen.

In den folgenden Abschnitten beschreiben wir kurz die Netzwerktopologie, die verwendeten Betriebssysteme auf Server-und Clientseite und die Testumgebung, welche uns zur praktischen Umsetzung dieser Arbeit bereitstanden.

3.1 Netzwerkanbindung

Entsprechend der bereits bestehenden Räume des CIP-Pools werden die Rechner nach dem Ethernetstandard über Switches miteinander vernetzt. Der lokale Server wird über eine zweite Netzwerkschnittstelle mit dem bestehenden Netz des CIP-Pools verbunden und übernimmt somit das Routing zwischen dem lokalen Netz (Windows-Pool) und dem CIP-Pool. Diese Art der Netzanbindung wurde von uns ganz bewusst gewählt, um die Windows 2000 PCs vom Rest des CIP-Pool Netzwerks abzuschirmen. Diese Maßnahme erfolgt aus Sicherheitsgründen und soll die Windows 2000 PCs vor Angriffen (und Missbrauch) aus dem Intra- und dem Internet schützen. Desweiteren kann die/der zukünftige Betreuer/in der PCs den Internetverkehr durch Einsatz von geeigneten Mechanismen (Packetfilter, Firewalls, etc.) auf das notwendige Muss beschränken.

3.2 lokaler Server - SuSE Linux 8.0 Professional

Wie bereits erwähnt entschieden wir uns für den Einsatz eines lokalen Servers, auf welchem wir möglichst viele Dienste zentralisieren können. Die Clients und der Server werden hierzu in einer lokalen Domäne zusammengefasst, was eine zentrale Benutzer- und Datenverwaltung ermöglicht. Der Server soll somit als Domänenkontroller (engl.: public domain controller), im Weiteren PDC genannt, fungieren. Der entsprechende Dienst auf Server-Seite heißt Samba. Aufgabe von Samba ist es, Datei- und Drucker-Freigaben, basierend auf dem SMB Protokoll, sowie eine Benutzerverwaltung, in der Art von MS Windows NT Server, bereitzustellen.

Um den Zugriff auf andere Rechner des CIP-Pools und auf das Internet zu ermöglichen, soll der Server einen Routingdienst und einen Proxyserver bereitstellen. Das Routing lässt sich mittels IP-Forwarding und IP-Masquerading realisieren, wobei zur Absicherung der im 2.4er Kernel integrierte Paketfilter iptables verwendet werden kann.

Um sich langwierige Einstellung des Netzwerkprotokolls auf Windows-Seite zu ersparen, wollen wir auf dem lokalen Server einen DHCP-Server betreiben.

Nicht zu vergessen ist ein Dienst, welcher die Verbindung zwischen Samba und dem Druckserver des CIP-Pools herstellt. Für die Zukunft wäre es auch denkbar einen lokalen Webserver zu betreiben, auf welchem die Medieninformatik betreffende Informationen bereitgestellt werden könnten. Die folgende Tabelle bietet einen Überblick über alle Dienste, die der lokale Server bereitstellt.

Dienste	Beschreibung
Samba als PDC	zentrale Benutzerverwaltung, ermöglicht Windows-PCs
	Zugriff auf Linux-Resourcen (Verzeichnisse, Drucker)
dhcpserver	vergibt IP-Adressen an das Windowsnetz
iptables	Filter fürs Routing
squid	Proxy Server - als WWW-Proxy konfiguriert
cups	Druckdienst mit Kontingentfunktion
apache	einer der bekanntesten Web-Server
eigene Skripte	dienen zum einfachen Anlegen von Benutzern,
	Generierung von Passwörtern und der Konfiguration
	der Routing-Dienste

Die Wahl des Betriebssystems auf Server-Seite fiel auf SuSE Linux 8.0, da diese Distribution alle benötigten Serverdienste in einer aktuellen Version beinhaltet, sehr preisgünstig ist und eine einfache Anbindung an die Linux/UNIX - Umgebung des CIP-Pools ermöglicht. Natürlich kann für den Server auch jede andere aktuelle Linux Distribution verwendet werden.

3.3 Client - Windows 2000 Professional

Da viele Standardanwendungen aus dem Bereich der Medieninformatik nur für Microsoft Windows Plattformen verfügbar sind (z.B.: Flash, Dreamweaver, ...), ist der Einsatz eines Microsoft-Betriebssystems notwendig. Die Anforderung an die Clients erfordert die Multiuserfähigkeit des Betriebssystems und die Möglichkeit der Anmeldung an einer Domäne.

Microsoft vermarket derzeit zwei Produkte die diese Eigenschaften besitzen: Windows 2000 Professional und Windows XP Professional. Wir haben uns für Windows 2000 Professional entschieden, da es im Gegensatz zu Windows XP ausgereifter, sicherer und resourcenschonender ist.

Zudem ist es zur Zeit nur mit Windows 2000 Clients (problemlos) möglich, sich an einem Samba - PDC anzumelden. Die auf MS-DOS basierenden Microsoft Betriebssysteme Windows9x/ME kamen für den Einsatz auf den Arbeitsplatzrechnern, aufgrund fehlender Sicherheitsmerkmale und deren fragwürdiger Stabilität im Betrieb, nicht in Frage. Zudem bieten diese Windows-Versionen nur eine “Pseudo-Mehrbenutzerfähigkeit”.

3.4 Testumgebung

Um die beschriebenen Ziele in die Praxis umzusetzen, entschieden wir uns für den Aufbau einer Testumgebung. Anhand dieser Testumgebung beschreiben wir sowohl die Installation des Linux PCs, welcher die Server-Dienste bereitstellt, als auch die Installation der Windows PCs.

Für den Aufbau der Testumgebung verwenden wir zwei Standard PCs, wobei einer der Rechner mit einer zusätzlichen Netzwerkkarte ausgerüstet ist. Die beiden Rechner sind untereinander mit einem gekreuzten Netzwerkkabel (CAT5) verbunden. Der Rechner mit zwei Netzwerkkarten wird für die Linux Installation verwendet und über die zweite Netzwerkkarte mit dem Netzwerk des CIP-Pools verbunden.

Anhand dieser Testumgebung ist es möglich, alle benötigten Dienste und Sicherheitseinstellungen zu konfigurieren und zu testen. Desweiteren kann der Linux-Rechner ohne großen Aufwand als lokaler Server im Windows-Pool verwendet werden. Der Windows PC kann als Referenzrechner für die restlichen 20 PCs dienen. Mittels geeigneter Software kann die komplette Installation auf die restlichen PCs übertragen werden, was eine einheitliche Installation der Windows-Rechner gewährleistet und den Installations- und Konfigurationsaufwand für die Administratoren/innen erheblich verringert.

Die folgende Abbildung stellt den Aufbau der Testumgebung und die Verteilung der Dienste grafisch dar.

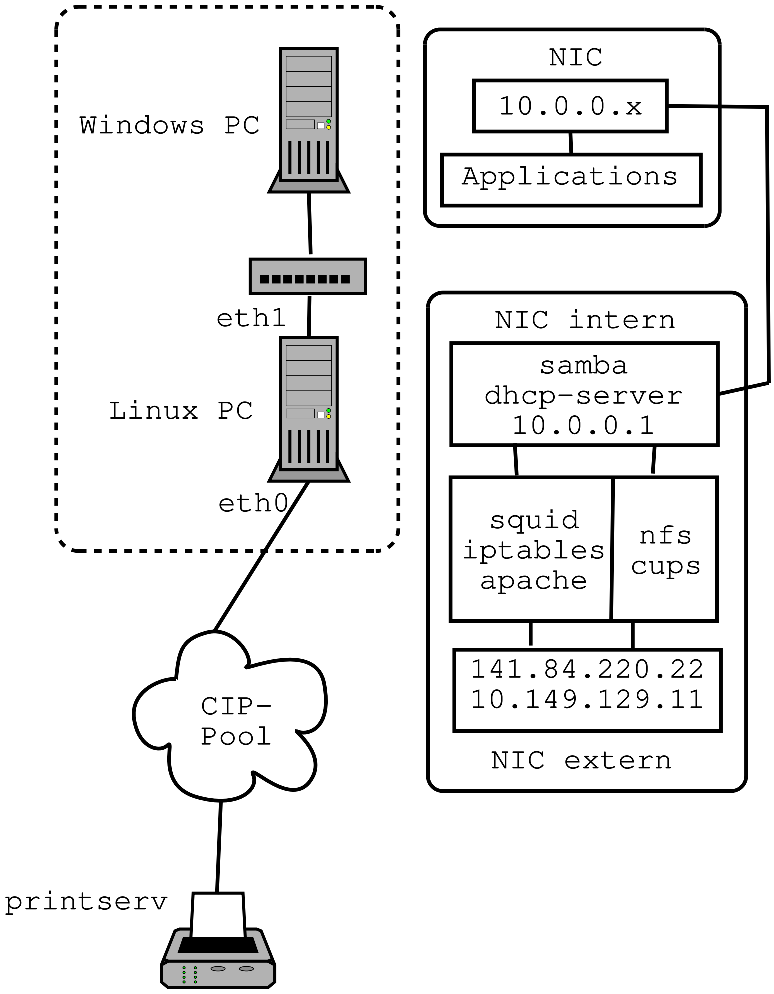

Abbildung 1: Schematischer Aufbau der Testumgebung

4 Anleitung zur Installation und Konfiguration

In diesem Kapitel beschreiben wir nun die Installation und Konfiguration, sowohl des Servers, als auch der/des Clients. Wir werden uns dabei im Wesentlichen mit der Konfiguration der im vorangegangenen Kapitel erwähnten Dienste, welche zur Zusammenarbeit und Integration der Windows-PCs mit der, bzw. in die bestehenden Linux-Umgebung notwendig sind, beschäftigen.

Die Installation der Betriebssysteme selbst sowie eventuell benötigter Treibersoftware (z.B. Grafik- und Soundkartentreiber) wird von uns nur kurz angeschnitten, da diese Vorgänge in diversen Büchern auf das Ausführlichste erklärt sind.

4.1 Server

Die Installation von SuSE Linux ist bei der von uns verwendeten Version 8.0 professional denkbar einfach, da alle im Testrechner verbauten Hardwarekomponenten, wie Mainboardchipsatz, Grafik-, Soundkarte und Netzwerkkarten bereits vom Installationsassistenten **YAST2** (Yet Another Setup Tool, Version 2) erkannt und eingebunden werden.

Wir wollen an dieser Stelle noch einige kleine Empfehlungen zur Auswahl der zu installierenden Pakete geben. Es hat sich als sehr nützlich erwiesen, die Pakete für eine grafische Benutzeroberfläche (X-Server + KDE - oder beliebiger anderer Windowmanager) zu installieren, weil dadurch die Konfigurationsarbeiten am Server komfortabler vonstatten gehen.

Für den Betrieb als lokaler Server in unserem Windows CIP-Pool müssen auf jeden Fall folgende Pakete mitinstalliert werden:

- Squid (Server): Squid ist ein freier WWW-Proxy mit allen gängigen features, designed für Unix Plattformen.
- DHCP (Server): DHCP, das *dynamic host configuration protocol*, sorgt dafür, dass Rechnern im internen Netz dynamisch IP-Adressen zugeteilt werden, was die Einbindung von Clients erheblich vereinfacht.
- iptables: Ein ip-filtering tool, das auf Kernelebene arbeitet und als zuverlässige Firewall genutzt werden kann, um einem minimalen Sicherheitsanspruch gerecht zu werden .
- Apache (Optional): Der weltweit am meisten eingesetzte Webserver kann sich später als nützlich erweisen.
- GNU-C/ C++ Compiler (gcc): Der Compiler gcc in der version 2.97 gilt als einer der standard-konformsten Übersetzer und ist unverzichtbar sowohl bei der Übersetzung eines neuen Kernels als auch bei der Integration von zusätzlicher Software, die nicht im Umfang von SuSE Linux enthalten ist und oftmals nur in Form von Quellcode erhältlich ist.
- Webbowser: Netscape, Mozilla, Opera, ... - je nach persönlicher Vorliebe

Die zum Zeitpunkt der Erstellung dieser Arbeit aktuellsten Samba- und Cupsversionen befinden sich auf der beiliegenden CD. Die Installation und Konfiguration der Pakete wird in den entsprechenden Abschnitten näher erläutert. Die der SuSE Distribution beiliegenden Versionen dieser Pakete sollten nicht installiert werden, da dies später zu Problemen führen kann.

Im Folgenden gehen wir nun der Reihe nach auf die Konfiguration der, für unsere Testumgebung relevanten, Dienste ein.

4.1.1 Konfiguration der Netzwerkkarten

Die Grundvoraussetzung für den Zugriff auf ein Rechnernetz ist die korrekte Konfiguration der Netzwerkkarten (kurz: NIC) und -protokolle. Unser Server verfügt über zwei Netzwerkkarten, eine für die Verbindung zu den Windows-Rechnern - unser internes Netz sowie eine weitere für die Verbindung in das bestehende Netz des CIP-Pools und dessen Gateway.

Die Treiber der beiden Netzwerkkarten wurden bereits bei der Systeminstallation eingebunden und geladen. Allerdings müssen noch einige protokollspezifische Einstellungen vorgenommen werden.

Wird eine Netzwerkkarte von **YAST2** nicht erkannt, so muss der Treiber manuell installiert werden. Die meisten Hersteller von Netzwerkkarten legen ihren Produkten bereits Treiber für Linux bei oder bieten diese zum Download auf ihren Internetseiten an. Den Treibern liegt in der Regeln eine Textdatei bei, in welcher die Installation selbiger beschrieben ist.

Als Erstes wenden wir uns dem lokalen Netz zu. Die Rechner dieses Subnetzes sollen zu dem privaten **10.0.0.0** (subnetmask: **255.255.255.0**) Netz gehören. Die entsprechende NIC in unserem Rechner bekommt die IP-Adresse **10.0.0.1** zugewiesen. Die entsprechenden Einstellungen können mit dem Konfigurationstool YAST2 vorgenommen werden.

Der Name unseres Rechners (inkl. domain) lautet **wingate.cip.informatik.uni-muenchen.de**. Die Adressvergabe für die Windowsrechner übernimmt ein DHCP-Server, dessen Konfiguration im nächsten Abschnitt erklärt wird.

Die Konfiguration der zweiten NIC gestaltet sich etwas komplizierter, da wir dieser Karte zwei IP-Adressen zuweisen müssen. Zum einen ist dies die "offizielle" IP-Adresse des "wingate", über welche auch von außen auf den Rechner zugegriffen werden kann, zum anderen eine private IP-Adresse, die dem "wingate" den Zugriff auf das private Subnetz, in welchem der Printserver des CIP-Pools hängt, ermöglicht. Die Einstellungen der öffentlichen IP-Adresse können wieder über YAST2 vorgenommen werden und lauten wie folgt:

IP-Adresse	**141.84.220.22**
Subnetmaske	**255.255.255.0**
Gateway	**141.84.220.254**
Hostname	**wingate.cip.informatik.uni-münchen.de**
DNS - Server	**10.149.1.65 129.187.214.135 (optional DNS des LRZ)**

Unter Linux ist es möglich einer Netzwerkkarte mehrere IP-Adressen, sogenannte virtuelle IP-Adressen, zuzuweisen. Die virtuellen IP-Adressen müssen allerdings per Hand in die Konfigurationsdatei der Netzwerkkarte eingetragen werden. In unserem Fall ist dies die Datei **/etc/sysconfig/network/ifcfg-eth0**. Um den Zugriff auf das "private" 10.149er Netz zu erhalten müssen in o.g. Datei folgende Zeilen eingefügt werden:

...
BROADCAST_1="10.149.255.255"
IPADDR_1="10.149.129.11"
NETMASK_1="255.255.0.0"
...

Nach dem Neustart des Netzwerks (init 2 - init 5 oder reboot) sollte nun sowohl ein ″**ping -c3 www.suse.de**″ als auch ein ″**ping -c3 printserv**″, erfolgreich verlaufen.

4.1.2 Konfiguration des DHCP-Servers

Der Begriff DHCP steht für “Dynamic Host Configuration Protocol”. Ein DHCP - Server stellt also, wie der Name bereits verrät, die Netzwerkkonfiguration für alle am Server angeschlossenen und berechtigten Hostrechner (Clients) bereit.

Wir verwenden diesen Serverdienst, da dadurch die Netzwerkkonfiguration der Windowshosts erheblich erleichtert wird. Windows versucht, bereits in der Standardkonfiguration, alle TCP/IP spezifischen Informationen der installierten Netzwerkadapter (IP-Adresse, Gateway, Nameserver...) von einem DHCP-Server zu beziehen.

Falls also neue PCs in das Netz eingebunden werden sollen, bzw. vorhandene Rechner neu installiert werden müssen, bleibt dem/der Betreuer/in die manuelle Konfiguration der Netzwerkkarten erspart, da diese automatisch aus dem IP-Pool des DHCP-Servers mit den korrekten Daten versehen werden. Zusätzlich wird verhindert, dass man versehentlich IP-Adressen doppelt vergibt.

Die Konfiguration des DHCP-Server gestaltet sich für unsere Zwecke sehr einfach. Hierzu muss lediglich die Datei /etc/dhcp.conf editiert und um folgende Einträge ergänzt werden:

```
ddns-update-style none;

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.10 10.0.0.200;
    option subnet-mask 255.255.255.0;
    option routers 10.0.0.1;
    default-lease-time 600;
    max-lease-time 7200;
    option domain-name "sep"; # bzw. der letztendlich für die subdomain vorgesehene Name
    option domain-name-servers 10.149.1.65, 129.187.214.135, 10.0.0.1;

}
```

Die Konfigurationsdatei teilt im Wesentlichen mit, aus welchem Bereich (range, in unserem Falle 10.0.0.10 - 10.0.0.200) IP-Adressen an sich anmeldende Rechner vergeben werden, welchen Standardgateway diese benutzen sollen (option routers) und welche Nameserver zur Verfügung stehen (option domain-name-servers). Zudem teilen wir jedem Rechner den Domainnamen mit (option domain-name).

Im Anschluss wird der Serverdienst mit "**/etc/init.d/dhcpd start**" gestartet.

4.1.3 Routing und Masquerading mit iptables

Um vom Windowsnetz in das Lehrstuhlnetz bzw. ins Internet zu gelangen, muss der Linuxserver auch als Gateway fungieren, was heißt, dass die Dienste IP-Forwarding und IP-Masquerading zur Verfügung stehen müssen. Dies wird mittels des IP-filtering tools "iptables" realisiert, welches als Modul in den Linuxkernel (ab Version 2.4) integriert ist und somit unabhängig von der eingesetzten Distribution verwendet werden kann. Mit *echo 1 > /proc/sys/net/ipv4/ip_forward* kann auf Unterstützung getestet werden. Sollte dieser Befehl eine Fehlermeldung verursachen, so muss der Kernel, mit aktivierter Option für IP-Forwarding und IP-Filtering, neu kompiliert werden.

Dieses im Rahmen des SEP erstellte Skript aktiviert das IP-Forwarding Modul des Linux Kernels und initiiert das "forwarden" der Pakete zwischen den Netzwerken mittels ip-tables.

```
#!/bin/bash
#
# script for ip-forwarding and ip-masquerading
#
#
#flush standard chains
iptables -F

#flush chains responsible for nat
iptables -t nat -F

#flush mangle chains
iptables -t mangle -F

#flush non standard chains
iptables -X

#IP-Masquerading und IP-Forwarding aktivieren
iptables -A POSTROUTING -t nat -j MASQUERADE -o eth0
echo 1 > /proc/sys/net/ipv4/ip_forward

# and additionally the following lines to get at least a minimum of security:
# please adjust to your security requirements
iptables -A INPUT -j LOG
iptables -A INPUT -i eth0 -p tcp –dport 22 -j ACCEPT
iptables -A INPUT -i eth0 -p udp –dport 22 -j ACCEPT
iptables -A INPUT -j DROP -m state –state NEW,INVALID -i eth0
```

iptables -A FORWARD -j DROP -m state –state NEW,INVALID -i eth0

Zur Erläuterung:

Die ersten vier Befehle löschen alle bereits im Kernel vorhandenen chains, damit wir in einer frischen Umgebung arbeiten können.

Die nächsten zwei Kommandos aktivieren IP-Masquerading und IP-Forwarding. IP-Masquerading kümmert sich um die Umsetzung von internen in externe Netzwerkadressen. Dies geschieht über die Manipulation der Portnummern aller Verbindungen, die aus dem internen Netz kommen. Somit entsteht von ausserhalb der Eindruck, dass alle Verbindungen von einer einzelnen Adresse - in unserem Falle wingate - stammen. Dieser kann jedoch über die verschiedenen Portnummern die echte Herkunft der Pakete bestimmen und somit an den entsprechenden Host im internen Netz verteilen. Da wir nur die Quell-Adressen aus dem internen Netz manipulieren wollen, reicht es, Masquerading nur für das Postrouting zu aktivieren (-A Postrouting). Die Option -t gibt an, dass wir Network Adress Translation benötigen, -j teilt mit, wie dies erreicht werden soll (nämlich mittels Masquerading) und -o lässt uns spezifizieren, auf welches Netzwerk-Interface wir uns beziehen - in unserem Falle logischerweise das externe. Der echo Befehl teilt dem Kernel mit, dass wir IP-Forwarding verwenden wollen. IP-Forwarding ist per default auf nahezu allen Linux-Systemen nicht aktiviert.
Nun zu den weiteren Regeln:

Mit der ersten Regel teilen wir iptables mit, dass alle Pakete, die den INPUT Teil der chain passieren mittels syslog geloggt werden. Die nächste Zeile bewirkt, dass alle TCP-Pakete (-p tcp), die auf dem Interface eth0 ankommen, akzeptiert werden sollen (-j ACCEPT), jedoch beschränkt auf Pakete mit Zielport 22 (ssh). Die dritte Regel wendet das gleiche Verhalten auf UDP-Datagramme an.

Die letzten beiden Regeln stellen sicher, dass keine Pakete in das interne Netz gelangen, die den Status NEW oder INVALID im Header haben. Ersteres, weil grundsätzlich kein Verbindungsaufbau von aussen in ein privates Netz erlaubt werden sollte, zweiteres, weil INVALID Pakete selten bis nie mit gutwilliger oder sinnvoller Payload bestückt sind.

Sollen bestimmte Verbindungen zu bestimmten Ports in das interne Netz (Wie zum Beispiel ICQ oder IRC) erlaubt werden, so muss iptables dies mitgeteilt werden. Die Autoren raten ab, empfehlen aber, Änderungen in dieses Skrip einzutragen, um den Administrationsaufwand so gering wie mögilch zu halten.

Für sicherheitsbewusste Administratoren/innen empfehlen sich weitere Regeln:

iptables -A FORWARD -i eth0 -s 10.0.0.0/24 -j DROP

Diese Regel stellt sicher, dass keine Pakete in das interne Netz weitergeleitet werden, die mit einer Adresse aus diesem versehen sind. Somit wird die Einsatzmöglichkeit von IP-Spoofing auf den Gateway beschränkt.

iptables -A FORWARD -i eth0 -o eth0 -j DROP

Dies verhindert, dass Pakete weitergeleitet werden, die sowohl bei der Netzwerkkarte eingetroffen sind als auch diese gerade verlassen wollen. Ist diese Regel nicht aktiviert, so ist es beispielsweise einem findigen Hacker möglich, seine Routingtabellen so zu modifizieren, dass er/sie unseren Gateway als Bouncer benutzen kann. Da alle Pakete das Masquerading durchlaufen, würde es von aussen so aussehen, als kämen sämtliche Pakete von diesem Gateway.

Mit einer auf unsere Bedürfnisse angepassten Firewall können wir uns nun der Installation des Proxyservers widmen.

4.1.4 Der Proxyserver Squid

Um jedem Benutzer einen schnellen und zuverlässigen Zugriff auf entfernte Daten zu gewährleisten, ist es notwendig die Netzlast möglichst gering zu halten. Eine Möglichkeit dieses Ziel zu erreichen ist der Einsatz eines Proxyservers. Hier wird der Proxydienst ausschließlich zur Zwischenspeicherung von Inhalten aus dem WorldWideWeb, welche über das HTTP-Protokoll transportiert werden, verwendet.

Ein weit verbreiteter, freier Proxyserver für Linux ist Squid.

Squid wird über eine zentrale Datei - "**/etc/squid.conf**" - konfiguriert. In unserem Fall wollen wir den Zugriff auf das Windowsnetz beschränken. Desweiteren soll Squid vorerst nur als WWW-Proxy laufen. Diese Funktionalität wird durch folgende Einträge in squid.conf erreicht:

...
 # add the windows-pool to the server's access control list
acl winpool src 10.0.0.0/255.255.255.0
...
 # allow access to the http-proxy-service
http_access allow localhost
http_access allow winpool
http_access deny all
...
Sollte es notwendig sein, andere Parameter, wie bspw. Cache-Grösse oder weitere Zugriffsbeschränkungen anzupassen, so können diese hier geändert werden. "**etc/squid.conf**" enthält zu jedem Parameter eine ausführliche Beschreibung. Die Default-Werte sind jedoch grundsätzlich in Ordnung und können ohne weiteres belassen werden.

Gestartet wird Squid mit dem Befehl "**/etc/init.d/squid start**".

4.1.5 Einführung zu Samba 2.2.5

Das Samba-Paket ermöglicht unserem Linux-Rechner die Bereitstellung und den Zugriff auf Dienste, welche das SMB (Server Message Block) Protokoll verwenden. Da Windowssysteme dieses Protokoll für Datei- und Druckfreigaben verwenden, ist Samba ein zentraler Bestandteil des Servers. Samba kann zusätzlich als Public Domain Server für Windowsrechner fungieren. Das bedeutet, Samba übernimmt für die Windowswelt die Benutzerverwaltung (Daten, Profile und Rechte).

Hier ist eine kurz Liste, welche beschreibt, was Samba beinhaltet und bietet: Für die meisten Netzwerke kann man kurz und einfach sagen "Samba ist ein kompletter Ersatz für Windows NT, OS/2 WARP, NFS oder Netware Server"

- ein SMB Server, zur Bereitstellung von Datei- und Druckerfreigaben im Sinne von Windows NT, gedacht für SMB-Clients, wie z.B. Windows9x/2k/XP, smbfs und anderen.
- ein NetBIOS (rfc1001/1002) nameserver, der den angeschlossenen Windows-Clients “zahlenlose” Kommunikation ermöglicht, d.h., hosts können sich gegenseitig über ihren NetBIOS Namen ansprechen.
- ein ftp-ähnlicher SMB Client, um PC Resourcen (Dateien und Drucker) von Unix, Netware und anderen Betriebssystemen aus nutzen zu können.
- beschränktes Kommandozeilenwerkzeug, welches einige administrative NT Funktionalitäten unterstützt, die unter Samba, auf NT Workstations und NT Servern benutzt werden können.

Nach dieser kurzen Einführung zum Thema Samba wollen wir uns nun der Installation der Version 2.2.5 widmen. Das komplette Paket steht auf den Samba Webseiten, erreichbar unter http://www.samba.org, zum Download bereit. Die oben genannte Version ist auch auf der beiliegenden SEP-CD enthalten.

4.1.6 Installation von Samba 2.2.5

Nun kommen wir zum aufwändigsten Teil der Serverinstallation - dem Samba Server. Als Erstes müssen wir die heruntergeladene Datei (bzw. die auf der CD enthaltene Datei) **samba-2.2.5.tar.gz** entpacken, z.B. nach **/usr/src/packages/SOURCES**. Der Befehl zum Entpacken eines tar-Archives lautet: *tar -xvzf <file.tar.gz>*. Nun einfach das Verzeichnis wechseln nach **/usr/src/packages/SOURCES/samba-2.2.5/sources** , "*./configure –enable-cups*", "*make*" und "*make install*" aufrufen. Die Sambaversion wird nun kompiliert und die entsprechenden Dateien und Verzeichnisbäume werden erstellt. Es sollte nun folgender Verzeichnisunterbaum vorhanden sein:

/usr/local/samba	Stammverzeichnis der Samba-Installation
/usr/local/samba/bin	Ausführbare Programme und Skripten
/usr/local/samba/lib	enthält die Konfigurationsdateien
	und die Benutzerdatenbank
/usr/local/samba/lib/ntprofiles	Verzeichnis für die Ablage der Benutzerprofile
/usr/local/samba/lib/netlogon	Verzeichnis für Login-Skripte

4.1.7 Konfiguration von Samba 2.2.5

Da der Sambaserver über eine eigene Benutzerverwaltung verfügt, müssen alle Linux-Benutzer, die auch über Samba Zugriff bekommen sollen, in die Samba Benutzerdatenbank eingetragen werden. Zu diesem Zweck haben wir ein Skript verfasst, welches alle Benutzer, die unter Linux über ein home-Verzeichnis verfügen, als Sambabenutzer übernimmt und gleichzeitig für jeden Benutzer ein Passwort generiert und in einer, nur vom Super-User lesbaren, Datei ablegt. Das Script befindet sich auf der beiliegenden CD, unter **/samba/scripts/passwd_gen.sh**. Bevor das Skript verwendet werden kann, muss noch der, auf der CD (**Verzeichnis /samba/passwordgenerator/apg-2.0.0final**) beiliegende, Passwortgenerator installiert werden. Dazu kopiert man einfach den kompletten Ordner **/apg-2.0.0final** nach **/usr/src/packages/SOURCES/** und ruft dort **./make** und **./make install** auf.

Sobald ein Benutzer am Sambaserver registriert wurde, kann er sich vom Windowssystem aus anmelden. Das Benutzerprofil wird bei der ersten Anmeldung automatisch erstellt und im dafür vorgesehenen Profil-Ordner abgelegt.

Ein einzelner User kann auch mit dem Befehl **smbpasswd -a username** registriert werden.
Als nächstes sind folgende Änderungen in der Datei **/usr/local/smb/lib/smb.conf** vorzunehmen:

Das Skript beginnt mit dem Abschnitt *[global]*.

[global]
; Basic server settings
netbios name = wingate
lock directory = /usr/local/samba/var/locks
smb passwd file = /usr/local/samba/lib/smbpasswd
; we should act as the domain and local master browser
workgroup = SEP
os level = 65
preferred master = yes
domain master = yes
local master = yes

In diesem Teil werden die Parameter zur grundlegenden Konfiguration des Samba-Servers festgelegt, und zwar solche, die den Server als Ganzes betreffen. Als Erstes teilen wir Samba den NetBIOS-Namen mit, der unserem Server im lokalen Windows-Netz zugeteilt werden soll. Die nächsten beiden Zeilen teilen Samba mit, wo lock-files abzulegen und wo die Passwort Datei der Samba-User zu finden ist. Hier können die Default Einstellungen übernommen werden, insofern nicht ausdrücklich der Installationspfad verändert wurde. Die drei Parameter für **preferred master**, **domain master** und **local master** müssen auf **yes** gesetzt werden, da Samba als PDC (Primary Domain Controller) agieren wird.

; security settings
security = domain

; encrypted passwords are a requirement for a PDC
encrypt passwords = yes

; support domain logons
domain logons = yes

; where to store user profiles?
logon path = \\%L\profiles\%u

admin users = root

add user script = /usr/sbin/useradd -g machines -d /dev/null /s /bin/false -m %u

In diesem Teil wird festgelegt, dass die Rechte und Zugriffsbeschränkungen auf die Shares von der ID des jeweiligen Domänen-Benutzers abhängen. Desweiteren fordern wir verschlüsselte Passwörter sowie die Möglichkeit von domain logons für Computer, die sich in der gleichen Workgroup, wie unser Server, befinden - Wingate ist also Domain Controller. Den Pfad, aus dem die profiles der Benutzer geladen werden sollen, setzen wir auf das Verzeichnis profiles\<username>. Der einzige Benutzer, der Administrationsrechte für Samba besitzen soll, ist natürlich root. Um einen Windows Client in die Domäne einzubinden, benötigt man einen Sambabenutzer mit administrativen Rechten. Deshalb sollte man nicht vergessen, den Benutzer root der smbpasswd-Datei hinzuzufügen. Dies geschieht mittels **smbpasswd -a root**. Zusätzlich werden für die Windows-Clients sogenannten Machine Accounts benötigt. Dies kann man mit dem **add user script** Eintrag automatisch erledigen lassen.

Im nächsten Abschnitt, der von größerer Bedeutung ist, können wir nun das home-Verzeichniss der User festlegen:

username map = /usr/local/samba/lib/smbusers

; where is a user's home directory and where should it
; be mounted at?
logon drive = g:
logon home = \\%L\homes\%u

Um nicht für jeden Windows-User einen eigenen Unix/Linux Account auf dem Server einrichten zu müssen, gibt es bei Samba die Möglichkeit, eine Mapping-Datei einzurichten. Dort werden Windows-User auf Linux-User abgebildet werden. Jede Zeile hat dort das Format *<unix user> = <Windows User 1> <Windows User 2>* ... (bspw. root = Administrator admin usw.). Mit **username map = /usr/local/samba/lib/smbusers** teilen wir Samba mit, in welcher Datei diese Mapping-Informationen zu finden sind.

Die Heimverzeichnisse befinden sich auf wingate unter **/home** und sollen auf dem verbundenen Windowsrechner lokal unter **g:** gemountet werden.

Die nächsten Zeilen definieren die Freigaben für diverse Verzeichnisse und Dienste. **Netlogon** steht für ein Share, in dem Loginskripts und -informationen abgelegt werden können. **Profiles** legt den Pfad und die Parameter für die Freigabe der servergespeicherten Benutzerprofile fest und **homes** dient als Freigabe für die UNIX/Linux Home-Verzeichnisse der Benutzer/innen.

[netlogon]
comment = Network Logon Service

path = /usr/local/samba/netlogon

 # Extra share for profiles. Default is the home of the user.
[profiles]
comment = Network Profiles Service
path = /usr/local/samba/profiles
read only = no
create mask = 0600
directory mask = 0700

[homes]
comment = Home Directories
read only = no
create mask = 0640
directory mask = 0750
browseable = no

Auf die Freigaben printers und print$ werden wir im folgenden Abschnitt näher eingehen.

4.1.8 CUPS

Die Abkürzung CUPS steht für Common Unix Printing System. CUPS verwendet das "Internet Druck Protokoll" (Internet Printing Protocol - kurz IPP), in der Version 1.1, und stellt ein vollständiges und aktuelles Druck-System für die Unix-Welt bereit. Dieses System stellt neue Drucker und Geräte sowie neue Protokolle bereit, ohne auf die Kompatibilität mit bestehenden Unix Anwendungen zu verzichten. Das IPP kann als Erweiterung des HTTP (HyperText Transfer Protocol) angesehen werden und es wird erwartet, dass sich dieses Protokoll als Standard für Netzwerkdruckdienste auf allen Betriebssystemen etablieren wird.

Im Rahmen dieses SEPs/Fopras wird CUPS auf dem Druck-Server des CIP-Pools eingesetzt und soll auf dem Linux-Server des Windows-Pools als Schnittstelle zwischen Samba und dem bestehenden Druck-Server dienen.

CUPS lässt sich sehr komfortabel über sein Web-Interface konfigurieren und verwalten. Zusätzlich kann über diese Schnittstelle der Status der installierten Drucker, die Übersicht über laufende Druck-Jobs und das Hilfe-System abgefragt werden.

Eine weitere Hauptaufgabe von CUPS ist natürlich die Bereitstellung von Druck-Diensten im Netzwerk. CUPS kann als Server betrieben werden, indem es Druckertreiber bereitstellt, Druckaufträge organisiert, Benutzer-Kontingente verwaltet und Informationen über die angeschlossenen Drucker an die Clients weitergibt. Im CIP-Pool des Instituts für Informatik verrichtet ein solcher Druckserver (**printserv.cip.informatik.uni-muenchen.de**) seinen Dienst. Über ihn haben die Studenten/innen Zugriff auf neun postscriptfähige Laserdrucker. Über das Webinterface des Servers[1] können die Standorte der Drucker, die Verfügbarkeit selbiger und die Dokumentation von CUPS abgefragt werden. Auf den Arbeitsplatz-Rechnern kommt ein CUPS-Client zum Einsatz, welchen wir auch für den Linux-Server unserer Testumgebung verwendet haben.

[1] http://printserv.cip.informatik.uni-muenchen.de:631

Die im Rahmen dieser Arbeit verwendete Version von CUPS bietet auch eine sehr gute Anbindung an den wichtigsten Dienst auf **wingate** - Samba. Samba und CUPS konnten zwar schon früher zusammen arbeiten, aber erst die hier verwendeten Versionen unterstützen den automatischen Druckertreiber-Download für Samba-Clients. Diese Funktion erleichtert die Installation und Administration des Windows-Pools erheblich, da nicht mehr auf jedem Client für jeden Drucker ein spezifischer Treiber installiert werden muss. Die Treiber befinden sich auf einem zentralen Rechner und werden bei Bedarf einfach heruntergeladen. Somit gestaltet sich auch ein Treiber-Update oder die Einbindung eines neuen Druckers sehr einfach.

Da die auf wingate verwendete SuSE Distribution[2] mit CUPS Version 1.1.12 ausgeliefert wird, mussten wir die zur Zeit aktuellste Version 1.1.16 von den Internetseiten der CUPS-Entwickler[3] downloaden. Die gepackte Version befindet sich auch auf der, dieser Arbeit beiliegenden, CD-ROM.

4.1.9 Installation von CUPS 1.1.16

Die Datei **cups-1.1.16-source.tar.gz** entpackt man einfach mit dem Befehl *tar -xvzf <file>* im Verzeichnis **/usr/src/packages/SOURCES**. Im Anschluss wechselt man in das Unterverzeichnis **cups-1.1.16** und folgt den Anweisungen in der **INSTALL.txt** Datei. Dadurch wird CUPS auf dem System kompiliert und installiert. Die für die Konfiguration relevanten Verzeichnisse sind **/etc/cups**, **/usr/share/cups** und **/usr/lib/cups**.

4.1.10 Konfiguration von CUPS 1.1.16

Als Erstes müssen wir auf **wingate** den CUPS Client einrichten, um auf den Druck-Server **printserv** des CIP-Pools zugreifen zu können. Dazu muss die Datei client.conf im Verzeichnis **/etc/cups** um folgenden Eintrag ergänzt werden:

...
Server-Name = printserv
...

Ob der Zugriff auf **printserv** korrekt funktioniert, kann man mit dem Befehl *lpstat -a* überprüfen. Erscheint folgende Ausgabe, ist alles OK:

PS1 accepting requests since Jan 01 00:00
PS2 accepting requests since Jan 01 00:00
PS3 accepting requests since Jan 01 00:00
PS4 not accepting requests since Jan 01 00:00 - Rejecting Jobs
PS5 accepting requests since Jan 01 00:00
PS6 accepting requests since Jan 01 00:00
PS7 accepting requests since Jan 01 00:00

[2]S.u.S.E. Linux 8.0 professional

[3]http://www.cups.org

PS8 accepting requests since Jan 01 00:00
PS9 accepting requests since Jan 01 00:00

PS1 bis **PS9** sind die Namen der Drucker im CIP Pool. Den Standort und den Druckertyp kann man am komfortabelsten über das Webinterface des Druck-Servers in Erfahrung bringen. Alle im CIP-Pool eingesetzten Drucker sind postscriptfähig.

Nun können wir uns mit der Bereitstellung der Drucker in der Samba-Umgebung beschäftigen.

Wir wollen Samba so konfigurieren, dass der, bereits erwähnte, automatische Treiber-Download für die Installation der Drucker auf den MS Windows 2000 Clients genutzt werden kann. Desweiteren darf das Accounting, das heißt die Kontingent-Verwaltung für die Benutzer/innen, nicht umgangen werden.

Da alle Drucker im CIP-Pool postscriptfähig sind, muss man nicht für jeden Drucker ein gesondertes Treiber-Paket bereitstellen, sondern es genügt ein generischer PostScript-Treiber[4]. Wir beziehen uns hier auf den Treiber aus dem Hause Adobe. Zusätzlich zu diesem Treiber werden die PPD Dateien (PostScript Printer Definition) für die jeweiligen Druckertypen benötigt. Diese PPD Dateien sind plattformunabhängig und werden von **printserv**[5] bereitgestellt. Es muss lediglich sichergestellt werden, dass sich diese Dateien auf **wingate** im Verzeichnis **/etc/cups/ppd** befinden. Die Dateien, welche mit dem Treiber-Paket von Adobe kommen müssen in das Verzeichnis **/usr/share/cups/drivers** kopiert werden. Es ist unbedingt darauf zu achten, dass die Dateinamen groß geschrieben werden.

Nun muss man noch Samba für die Bereitstellung des Druck-Dienstes konfigurieren. Dies geschieht über folgende Einträge in der Datei smb.conf (im Verzeichnis **/usr/local/samba/lib**).

In der **[global]**-Sektion wird das Laden der Drucker-Freigabe, das verwendete Drucksystem und die Anwendung einiger Druck-Kommados festgelegt. **[printers]** definiert schließlich noch einige Eigenschaften der eigentlichen Drucker-Freigabe, wie Spool-Verzeichnis für die Druckaufträge, Zugriffsbeschränkungen und Admin-Benutzer der Freigabe. Man muss unbedingt darauf achten, dass alle Benutzer/innen, die das Drucksystem verwenden sollen, über Schreibrechte im angegebenen Spool-Verzeichnis verfügen.

```
[global]
# Drucker-Freigabe wird bereitgestellt
load printers = yes
# das verwendete Druck-System ist CUPS
printing = cups
# Datei mit den Druckernamen - man könnte auch /etc/printcap angeben
printcap name = cups
print command = /usr/bin/lpr -P %p %s
lpq command = /usr/bsd/lpq -P %p %s
lprm command = /usr/bsd/lprm -P %p %s

[printers]
# zusätzliche Eigenschaften der Drucker-Freigabe
comment = All Printers
path = /var/spool/samba
```

[4] z.B. Adobe PostScript-Treiber - erhältlich unter http://www.adobe.com

[5] die ppd Dateien für PS1 -PS9 befinden sich auch auf der SEP CD-ROM

browseable = no
public = no
guest ok = no
printable = yes
printer admin = root

Der folgende Eintrag stellt eine, für die Benutzer unsichtbare, Freigabe bereit, in welcher die Druckertreiber für die Clients abgelegt werden.

[print$]
comment = Printer Drivers
path = /usr/local/samba/drivers
browseable = yes
guest ok = no
read only = yes
write list = root

Nach den Änderungen muss der Samba-Server neu gestartet werden.

In unserem Fall müssen die Treiber für die Windows-Clients also im Verzeichnis */usr/local/samba/drivers* abgelegt werden. Diese Arbeit kann man sehr einfach mit dem Tool *cuppsaddsmb* erledigen. *cuppsaddsmb* holt sich die PostScript-Treiber und die PPD - Dateien aus den oben genannten Verzeichnisse und legt in der **[print$]** Freigabe des Samba-Servers die entsprechende Verzeichnisstruktur an, so dass sich die Clients von dort die entsprechenden Dateien herunterladen können.

Der Aufruf von cuppsaddsmb lautet wie folgt:

cupsaddsmb -H wingate -U root -h printserv -v - a

WICHTIG! *cupsaddsmb* verwendet RPC's (RemoteProcedureCalls) welche Paßwörter unverschlüsselt übertragen. Die Option *-v* bewirkt, dass sämtliche Aufrufe, die *cupsaddsmb* ausführt, am Bildschirm ausgegeben werden - damit auch das root - Passwort !! Deshalb schlagen wir aus Sicherheitsgründen vor, das Passwort unmittelbar nach dem Aufruf von cupsaddsmb zu ändern.

War das oben beschriebene Vorgehen erfolgreich, dann wurde im Verzeichnis */usr/local/samba/drivers* folgende Verzeichnisstruktur angelegt:

./W32X386/2	**Treiber für Windows 2000**
./WIN40	**Treiber für Windows 9x/ME**

Die Einbindung der Drucker in die Windows-Umgebung wird im Abschnitt über die Clients erklärt.

4.2 Clients - MS Windows 2000

Dieses Kapitel widmet sich der Installation der Client-Rechner. Wie bereits erwähnt, gilt es 20 Rechner mit MS Windows 2000 und Anwendungssoftware zu bespielen, die Rechner in die lokale Domäne einzubinden, den Zugriff auf Server-Dienste zu konfigurieren und Sicherheitseinstellungen vorzunehmen.

Um die Installationsarbeiten zu vereinfachen und zu beschleunigen empfehlen wir, die folgenden Schritte auf einem Referenz-Rechner zu erledigen und anschließend die fertige Konfiguration mit geeigneter Software[6] auf die restlichen Clients zu übertragen.

Die Installation von MS Windows 2000 ist im Großen und Ganzen selbsterklärend und wird hier nicht näher erläutert. Da, wie bereits erwähnt, auf Client-Seite die Auswahl zwischen zwei Betriebssystemen möglich sein soll, haben wir nur 50% der zur Verfügung stehenden Festplattenkapazität für die Windows-Installation verwendet. Dies ermöglicht die spätere Installation eines weiteren Betriebssystems auf den Client-Rechnern.

Auf der Windows-Partition sollte ausreichend Platz für das Basissystem, Anwendungssoftware und die Auslagerungsdatei vorhanden sein. Eine spezielle Partition für Benutzer-Daten ist nicht notwendig, da diese serverseitig gespeichert werden.

Für die Basis-Konfiguration des Windows-Rechners muss nur ein lokaler Benutzer, der Administrator, angelegt werden. Die Verwaltung der Studentenkennungen für die Anmeldung an den Windows-Rechner übernimmt der PDC.

4.2.1 Anbinden des MS Windows 2000 Rechners an die lokale Domäne

Am Ende der MS Windows 2000 Installation kann man den Rechner bereits für den Netzwerk-Einsatz konfigurieren. Dabei kann man den Rechner als Mitglied einer Domäne angeben, wozu der Domänenname und die root-Kennung des PDC benötigt werden. Nach dem nächsten Windows-Neustart kann man sich dann am PDC anmelden. Im Windows Anmeldedialog erscheint unter den Feldern für Benutzername und Kennwort zusätzlich das Feld Domäne. Dort kann auswählt werden, ob man sich lokal oder am PDC anmelden will. War die Anmeldung am PDC erfolgreich, so ist im Arbeitsplatz die Freigabe '**homes auf wingate**' sichtbar.

Diese Vorgehensweise funktioniert nur, wenn die im Rechner verbaute Netzwerkkarte von MS Windows 2000 automatisch erkannt wird. Andernfalls muss man die Treiber- und die Netzwerk-Konfiguration per Hand durchführen. Dazu installiert man zuerst den, der Netzwerkkarte beiliegenden Treiber. Anschließend erscheint in den Eigenschaften der Netzwerk-Umgebung eine aktive LAN-Verbindung. Öffnet man das Eigenschaftsfenster dieser LAN-Verbindung, sieht man die mit der Verbindung verknüpften Dienste und Protokolle. Hier müssen auf jeden Fall der Client für Microsoft Netzwerke und das TCP/IP-Protokoll erscheinen. Ist dies der Fall, war die Netzwerkkonfiguration erfolgreich.

Für das Netzwerk-Protokoll müssen keine gesonderten Einstellungen vorgenommen werden, da diese vom DHCP Server auf **wingate** bereitgestellt werden.

[6] Drive Image Pro von Syquest oder Norton Ghost von Symantec

Ob die Protokolleinstellungen erfolgreich zugewiesen wurden, kann mittels des Befehls *ipconfig* in der Eingabeaufforderung (**Start->Ausführen->cmd <enter>**) überprüft werden. In der Ausgabe muss eine IP-Adresse aus dem 10.0.0er Netz erscheinen. Der Gateway-Eintrag muss 10.0.0.1 lauten.

Im Anschluss muss in der Registrierkarte Computername im Eigenschaftsfenster des Arbeitsplatzes noch der Rechnername, sowie der Name der Domäne eingetragen werden. Dazu wird die root - Kennung des PDC benötigt.

Nach den oben genannten Änderungen wird man zum Neustart des Rechners aufgefordert. Damit ist die Einbindung in die Domäne abgeschlossen.

Es hat sich als nützlich erwiesen, den Benutzer root als lokalen Benutzer hinzuzufügen und ihn als Mitglied der Administratoren-Gruppe einzutragen. Dazu muss man als Administrator angemeldet sein. Das Hinzufügen eines/r Benutzers/in wird über den Menupunkt **Benutzer und Kennwörter** unter **Start -> Einstellungen -> Systemsteuerung** erledigt. Ein Klick auf **Hinzufügen...** und ein weiterer auf **Durchsuchen...** im eben aufgegangenen Fenster **"Neuen Benutzer hinzufügen"**, und man bekommt eine Auswahlliste aller registrierten Domänen-Benutzer angezeigt. Nun muss man nur noch root auswählen und ihn als Mitglied der Administratoren-Gruppe eintragen.

4.2.2 Zugriff auf die Druck-Dienste des CIP-Pools

Wie oben erwähnt stellt der lokale Server **wingate** die Druck-Dienste des CIP-Pools und die dafür benötigten Treiber für die Windows-Rechner zur Verfügung. Um diese Dienste nutzen zu können, müssen die Benutzer/innen auf den Windows-Rechnern die freigegebenen Netz-Drucker noch verbinden. Dazu öffnet man die **Netzwerk-Umgebung** und klickt sich wie folgt durch die Symbol-Landschaft: g**esamtes Netzwerk -> Microsoft-Netzwerk -> 'Domänenname' -> wingate**. Sollte, was bei Windows leider vorkommt, wingate in der Domäne nicht angezeigt werden, kann man über die Option "**Computer suchen**" (Suchbegriff: **wingate**) den PDC anzeigen lassen. Nun sind alle Freigaben des Samba-Servers, auf welche der/die angemeldete Benutzer/in Zugriff hat, sichtbar. Um nun den gewünschten Drucker einzubinden, genügt ein Klick mit der rechten Maus-Taste auf das entsprechende Drucker-Symbol (Name: **PSx**) und die Auswahl der Option **verbinden**. Durch diesen Vorgang wird der ausgewählte Drucker, samt Treiber, auf dem Windows-Rechner installiert und kann fortan verwendet werden.

4.2.3 Zugriff auf das Internet

Wie bereits erwähnt, fungiert der Rechner **wingate** für die Windows-Clients als Gateway ins restliche Netzwerk des CIP-Pools, sowie ins Internet. Die für die Clients notwendigen Konfigurationsdaten, wie IP-Adresse des Gateways und der DNS (Domain Name Server), werden vom DHCP-Server-Dienst bereitgestellt.

Um HTTP Anfragen zu beschleunigen und den Netzwerk-Verkehr zu verringern läuft auf **wingate** zusätzlich ein Proxy-Dienst. Als Proxy-Server kann (es muss nicht!) für das HTTP die IP-Adresse von **wingate** auf Port **3128** eingetragen werden.

Wird den Benutzer/innen die Verwendung des Internet Explorer gestattet, kann der zu verwendende Proxy-Server über die Gruppen-Richtlinien von MS Windows 2000 festgelegt werden. Dabei sollte man nicht vergessen, auch die Sicherheitseinstellungen für den Internet Explorer möglichst hoch einzustellen (dazu noch später).

Da die Internet-Programme von Microsoft (Internet Explorer, Outlook Express, ...) teilweise erhebliche Sicherheitslücken aufweisen empfehlen wir, auf den Windows-Rechnern alternative Browser-Pakete mit integrierten Mail-Clients, Newsreadern etc., zu installieren. Kostenfreie Lösungen sind zum Beispiel die Browser von Opera[7] oder Mozilla[8]. Will man dennoch nicht auf die Verwendung des Internet Explorers verzichten empfehlen wir alle, von Microsoft zur Verfügung gestellten Updates auf dem System zu installieren. Dazu wählt man einfach im Menu **Extras** des Intenet Explorers den Punkt **Windows Update**.

4.2.4 Installation von MS Office 2000 Professional

Das Office Paket von Microsoft ist das meist verwendete und verkaufte Paket seiner Art. Um den Studenten/innen die Arbeit mit dieser Standardsoftware zu ermöglichen, darf MS Office auf den Windows Clients natürlich nicht fehlen. Die Installation der Software ist selbsterklärend, wir wollen jedoch noch auf einige Kleinigkeiten hinweisen.

Zum einen sollte man bei der Installation möglichst alle Zusatzpakete, welche für die spätere Arbeit mit MS Office benötigt werden (z.B. Silbentrennung, Formel-Generator,...), mit auswählen, da die hier verwendete Version MS Office 2000 Professional manche Pakete nicht standardmäßig mitinstalliert.

Aus Sicherheitsgründen empfehlen wir, das Paket Outlook nicht zu installieren. Die Benutzer/innen sollen als Mail-Clients die oben genannten Alternativen von Opera oder Mozilla benutzen.

MS Office speichert alle benutzerspezifischen Informationen im jeweiligen Benutzer-Profil. Um die zulässige Gesamtgröße des Benutzer-Profils nicht zu überschreiten, müssen die Benutzer/innen darauf hingewiesen werden, die von ihnen erstellten Dateien nicht im Ordner **Eigene Dateien** abzulegen, sondern auf der **homes**-Freigabe des Samba Servers. Die **homes**-Freigabe kann in den Office Anwendungen als Standard Speicherort eingestellt werden.

4.2.5 Setzen von Zugriffsrechten und Richtlinien

Die wesentlichen Ziele bei Planung und Installation von Netzwerken sind die Verfügbarkeit aller Netzwerk-Ressourcen sicherzustellen, einen stabilen Betrieb zu gewährleisten und ein angemessenes Sicherheitsniveau zu halten. Werden die genannten Ziele erreicht, so profitieren davon sowohl die Benutzer/innen der Arbeitsplatz-Rechner als auch die Administratoren/in.

Für die Installation der Windows-Rechner wollen wir konkret folgende Einschränkungen bzw. Vorgabe realisieren.

[7] erhältlich unter http://www.opera.com

[8] erhältlich unter http://www.mozilla.org

- Da die Profile der einzelnen Benutzer/innen auf dem Linux-Server gespeichert werden, müssen diese bei jedem Anmeldevorgang auf den Arbeitspaltz-Rechner kopiert werden. Um den Netzwerk-Verkehr und die Wartezeiten beim Anmelden eines Benutzers/in zu minimieren, wird die Größe der Benutzerprofile eingeschränkt.
- Eine lokale Anmeldung auf den Arbeitsplatz-Rechnern soll nur dem Administrator möglich sein. Durch diese Einschränkung wird erreicht, dass keine lokalen Benutzer-Profile angelegt werden, wodurch Speicherplatz auf der lokalen Festplatte des Client-Rechners gespart wird.
- Wie bereits erwähnt, werden die servergespeicherten Profile der Benutzer/in bei der Anmeldung auf die lokale Festplatte kopiert. Diese Kopien müssen natürlich beim bzw. nach dem Abmelden wieder gelöscht werden. Ansonsten wäre die Speicherkapazität der Festplatte bereits nach kurzer Zeit erschöpft.
- Um einen möglichst stabilen, sprich ausfallsicheren Rechenbetrieb zu ermöglichen, dürfen die Benutzer/innen keine Systemeinstellungen (Hardware-Treiber, Bildschirm-Auflösung, Registrierungsdaten, ...) auf den Windows-Rechnern verändern.
- Benutzer/innen des Systems dürfen keinen Druckertreiber installieren. Wenn die zu druckenden Daten bereits vom Windows-Treiber gerastert ("in PostScript umgewandelt") und direkt an den entsprechenden Druckeranschluss weitergeleitet werden, wird die Kontingentverwaltung des Druck-Servers ausgehebelt!
- Benutzer/innen ist es nicht erlaubt, Software auf den Rechnern zu (de-)installieren.
- Benutzer/innen dürfen keine Programme, welche die Systemsicherheit gefährden können, ausführen können. (z.B. MS NetMeeting)
- Um ein versehentliches Löschen bzw. Verschieben von wichtigen Dateien auf den lokalen Datenträgern zu verhindern, werden die Zugriffsrechte der Benutzer/innen auf die lokalen Datenträger eingeschränkt.
- Die Sicherheits- und Proxy-Einstellungen für den MS Internet Explorer werden systemweit festgelegt und dürfen von den Benutzer/innen nicht verändert werden können.

Zur Umsetzung der genannten Punkte empfehlen wir folgende Vorgehensweise:

Zuerst schränken wir den Zugriff auf die Ordner des lokalen Datenträgers ein. Dazu sollte sichergestellt werden, dass der lokale Datenträger mit dem Dateisystem NTFS formatiert ist. Ist dies nicht der Fall, kann man das Dateisystem nachträglich in NTFS konvertieren. Dies geschieht mit dem Programm **convert**, welches von der Eingabeaufforderung aus aufgerufen werden kann. Die Hilfedatei des Befehls kann man sich mit **help convert** anzeigen lassen. Wird **convert** auf die Systemplatte (in der Regel die C:-Partition) angewendet, erfolgt die Konvertierung des Dateisystems erst beim nächsten Neustart des Rechners.

Die Zugriffsrechte für Laufwerke, Ordner und Dateien können in deren Eigenschaftsfenster (Mauszeiger über dem entsprechenden Laufwerks-, Ordner- oder Datei-Symbol positionieren, dann *rechte Maustaste -> Eigenschaften*) festgelegt werden. In den Eigenschaftsfenstern gibt es eine Registrierkarte mit Namen *Sicherheitseinstellungen*. Dort können für ausgewählte Benutzer/innen spezifische

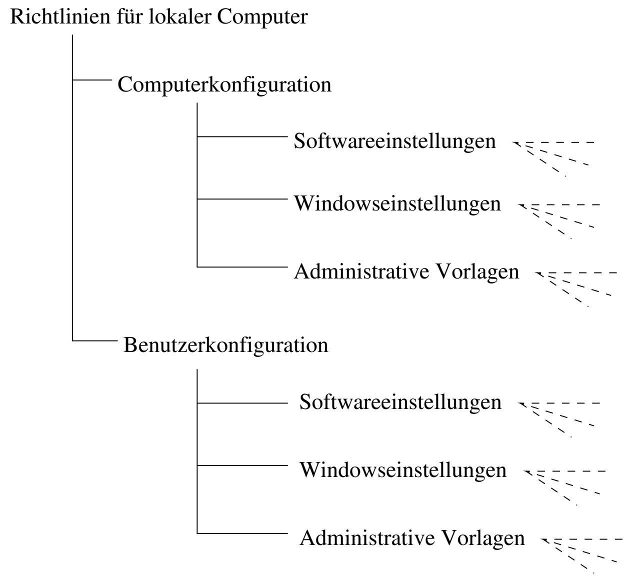

Abbildung 2: Baumstruktur der lokalen Richtlinien

Rechte vergeben werden. Eine feinere Einstellung erreicht man über den Button *Erweitert*. Dort kann man eine detailliertere Rechte-Vergabe vornehmen und den/die Besitzer/in des entsprechenden Laufwerks, Ordners bzw. der entsprechenden Datei festlegen. In unserer Testumgebung haben wir eine relativ einfache Strategie für die Rechte-Vergabe gewählt, die den o.g. Punkten bezüglich Stabilität und Sicherheit gerecht wird. Details dazu findet man im Abschnitt A des Anhangs.

Die restlichen Punkte kann man durch geeignetes Setzen der lokalen Computerrichtlinien erledigen. Dafür stellt MS Windows 2000 ein sehr mächtiges Werkzeug bereit, das sogenannte Gruppenrichtlinien-SnapIn **gpedit.msc**. Es dient dazu Gruppenrichtlinienobjekte zu bearbeiten. Diese Objekte sind in einer Baumstruktur aufgebaut und unterscheiden auf der ersten Ebene zwischen Computer- und Benutzer-Richtlinien. Weiterhin wird zwischen lokalen Richtlinien, wie sie im Rahmen dieser Arbeit Anwendung finden und globalen Richtlinien, die z.B. in der Active Directory Struktur[9] (kurz: ADS) eines PDC abgelegt sind, unterschieden.

Das zum Bearbeiten der Richtlinien notwendige SnapIn öffnet man über **Start -> Ausführen -> gpedit.msc** <enter> .

Bevor man beginnt, die Standard-Richtlinien des Systems zu verändern, sollten alle Konfigurations- und Installationsarbeiten abgeschlossen sein. Die Empfehlungen, die wir bezüglich der Sicherheitseinstellungen geben, schränken den Zugriff auf das System stark ein. Da die derzeit verfügbaren Samba Versionen[10] noch keine Active Directory Struktur unterstützen, können auf den Windows-Rechnern nur lokale Richtlinien gesetzt werden, welche Auswirkungen auf alle Benutzer des Rechners haben. Das bedeutet, wenn man in der entsprechenden Richtlinie das Neuinstallieren von Soft-

[9] skalierbarer, hierarchischer Verzeichnisdienst, zur Verwaltung aller, für das Netzwerk relevanten, Resourcen

[10] geplant ab Version 3.x

ware deaktiviert, ist es selbst dem Administrator nicht mehr möglich, Software auf dem System zu installieren.

Zum Bearbeiten der Gruppenrichtlinien öffnet man einfach das oben erwähnte Gruppenrichtlinien-SnapIn - **gpedit.msc**. Durch Anklicken einer Richtlinie (Blätter der Baumstruktur) öffnet sich deren Eigenschaftsfenster. Auf der ersten Registrierkarte wird die Richtlinie aktiviert bzw. deaktiviert, auf der zweiten Registrierkarte befindet sich eine kurze Beschreibung der Richtlinie.

Die gesetzten Richtlinien werden in mehreren Dateien im Ordner **C:\Windows\System32\GroupPolicy** gespeichert. Um also die Einstellungen vom Referenz-Rechner unserer Testumgebung auf andere Rechner zu übertragen, genügt es, die Dateien aus dem genannten Ordner auf das neue System zu übertragen.

Die Auflistung der Richtlinien, die wir zur Umsetzung unseres Konzeptes in der Testumgebung verwendet haben, befindet sich im Anhang B dieser Ausarbeitung..

4.3 (noch) nicht realisierbare Ziele

Einige der ursprünglichen Vorgaben dieser Arbeit konnten aufgrund mangelnder Unterstützung seitens der verwendeten Dienste nicht umgesetzt werden. Dieser Abschnitt beschäftigt sich mit eben diesen, nicht erreichten Zielen.

Für die Studenten/innen, die den neuen Windows-Pool verwenden, soll es natürlch möglich sein, Daten in ihren Benutzerverzeichnissen abzulegen. MS Windows 2000 stellt zu diesem Zweck einen speziellen Desktop-Ordner, mit dem Namen **Eigene Dateien** bereit. Dieser Ordner ist fester Bestandteil des Benutzerprofils. Um den Netzwerkverkehr beim Anmelden an den Windows-Rechnern niedrig zu halten und den Plattenplatz auf dem PDC zu schonen, sollen die Benutzerprofile aber möglichst klein gehalten werden und unterliegen, wie im vorhergehenden Abschnitt erwähnt, einer Größenbeschränkung. Zusätzlich sollen die Benutzer/innen auch die Möglichkeit bekommen, von den Linux-Arbeitsplätzen des CIP-Pools aus auf ihre Daten zuzugreifen. Als Lösung bietet sich an, den Speicherort für den Ordner **Eigene Dateien** auf das Unix-Verzeichnis der Benutzer/innen umzuleiten. Wünschenswert wäre also, diese Ordnerumleitung bereits in der Standardvorlage für die Benutzerprofile zu definieren, so dass bereits bei der Erstanmeldung eines/r Benutzers/in der Speicherort von **Eigene Dateien** im Unix Heimatverzeichnis liegt. MS Windows 2000 unterstützt diese Ordnerumleitung, in der hier beschriebenen Form nur, wenn der PDC eine ADS bereitstellt. Die in der Testumgebung verwendete Samba-Version unterstützt jedoch noch keinen, zu ActiveDirectory kompatiblen Verzeichnisdienst. Erst ab der Version 3.x des Samba-Servers soll ein solcher Dienst bereitgestellt werden.

Der Speicherort für **Eigene Dateien** kann jedoch über **Eigene Dateien -> 'rechte Maustaste' -> Eigenschaften** manuell geändert werden. Dies muss für jede/n Benutzer/in einzeln erfolgen, was für den/die Administrator/in einen erheblichen Arbeitsaufwand bedeutet.

Ein weiterer Vorteil der genannten ADS ist die Möglichkeit, globale (domänenweite) Gruppenrichtlinien zu verwalten. Dadurch lassen sich Änderungen an den Gruppenrichtlinien von einem zentralen Ort aus vornehmen. Dies verringert den damit verbundenen Arbeitsaufwand und man läuft nicht Gefahr, einen Rechner beim Vornehmen von Änderungen zu vergessen.

Eine weitere Überlegung bei der Planung der Testumgebung war, die servergespeicherten Benutzerprofile zu sperren. Das bedeutet, dass die Benutzer/innen ihre Profile nicht dauerhaft verändern können. Dadurch wird weder der Speicherbedarf der Profile auf dem Server vergrößert, noch können die Benutzer/innen durch Veränderung am Profil Schaden anrichten. Realisiert wird die Sperrung durch Umbennenen der Datei **ntuser.dat**, im Stammverzeichnis des Profils, in **ntuser.man**. Das Problem daran ist, dass sämtliche Daten, welche die Benutzer/innen im Ordner **Eigene Dateien**[11] scheinbar erfolgreich speichern, beim Abmelden verloren gehen. Zudem können bei gesperrtem Benutzerprofil zahlreiche benutzerspezifische Softwareeinstellungen, wie z.B. E-Mail-Konten, MS Office Standardvorlagen, etc., nicht abgespeichert werden.

Die Lösung der genannten Probleme kann zum einen über eine Größenbeschränkung der Benutzerprofile erreicht werden, zum anderen können die Benutzer über einen Informationstext, der nach dem Anmelden auf dem Bildschirm erscheint, darauf hingewiesen werden, den Speicherort von **Eigene Dateien** zu ändern, bzw. ihre Daten direkt in ihr Homeverzeichnis (**homes** Freigabe des PDC) abzulegen. Dieser Infotext kann zum Beispiel in der **netlogon**-Freigabe des Samba-Servers liegen und über ein Login-Skript angezeigt werden.

[11] falls sie den Speicherort des Ordners nicht geändert haben

5 Schluss

Anhand des letzten Abschnittes kann man erkennen, dass sich noch einige Dinge bezüglich Administrationsaufwand und Sicherheit optimieren lassen. Die Umsetzung dieser Optimierungsmöglichkeiten hängt jedoch hauptsächlich von der Leistunsfähigkeit der neuen Samba Versionen ab. Die aktuellsten Versionen erhält man auf der Web-Seite *http://www.samba.org*. Auf dieser Seite findet man auch die Informationen über kommende Versionen.

Im Großen und Ganzen konnten wir die gesteckten Zielen dieser Arbeit anhand der Testumgebung erfolgreich umsetzen. Die Serverinstallation und -konfiguration gestaltete sich dabei nahezu problemlos. Einige Programmpakete mussten von uns auf den neuesten Stand gebracht werden, um gewünschte Funktionen nutzen zu können.

Die Konfiguration des Windows-Rechners erwies sich schwieriger als erwartet. Während die Grundinstallation und das Einbinden in die Domäne ohne Schwierigkeiten vonstatten ging, kostete die korrekte Wahl der Computerrichtlinien viel Zeit und Nerven. Die Hauptursache dafür ist der in unseren Augen etwas unlogische und unstrukturierte Aufbau der Richtlinien.

Der Raum der Medieninformatik ist bereits am Netz und wird im laufenden Semester für den Praktikums- und Übungsbetrieb genutzt. Wir sind in dieser Arbeit nicht näher auf die Installation fachspezifischer Software eingegangen, da der Softwarekatalog für das Praktikum Medieninformatk bei Durchführung dieser Arbeit noch nicht zur Verfügung stand. Desweiteren unterliegt der erwähnte Softwarekatalog ständigen Änderungen, abhängig von den Anforderungen der Praktika.

Zm Schluss bedanken wir uns noch bei unseren Betreuern für die optimale und hervorragende Unterstützung.

Anhang

A Setzen der Zugriffsrechte

Wie bereits erwähnt, bietet das Dateisystem NTFS die Möglichkeit, benutzerspezifische Zugriffsrechte für lokale Laufwerke, Ordner und Dateien zu vergeben. Um das Ansammeln von Datenmüll auf der lokalen Platte zu verhindern, sollen die Benutzer/innen der Windows-Rechner keine Schreibrechte auf dem lokalen Laufwerk besitzen.

Wir verwenden in unserer Testumgebung für Windows eine einzige Partition (Laufwerk C:), auf der sich nach der Installation des Betriebssystems und der Anwendungsprogramme folgende drei Ordner befinden:

Dokumente und Einstellungen	Speicherort für Benutzerprofile
Programme	Speicherort für Anwendungsprogramme
WINNT	Speicherort aller Komponenten des Betriebssystems

Um nun eine effektive Einschränkung der Zugriffsrechte zu erreichen genügt es, die Rechte für Laufwerk C: und für die o.g. Ordner wie folgt zu setzen[12].

- Laufwerk *C:*
  - Administratoren (<Rechner> \ Administratoren), SYSTEM : **Vollzugriff**
  - Benutzer, Hauptbenutzer, Jeder: **Lesen, Ausführen - Ordnerinhalte auflisten - Lesen**
- Ordner *Dokumente und Einstellungen*
  - Hier können dieselben Einstellungen wie für Laufwerk C: verwendet werden. Die Rechte für die Profilordner werden bei deren Erstellung automatisch richtig gesetzt.
- Ordner *Programme*
  - Administratoren (<Rechner> \ Administratoren), SYSTEM : **Vollzugriff**
  - Benutzer, Hauptbenutzer: **Lesen, Ausführen - Ordnerinhalte auflisten - Lesen**

Falls man unter verschiedenen Benutzerkonten Anwendungen in diesen Ordner installiert hat, erscheint in der Liste zusätzlich die Gruppe ERSTELLER-BESITZER, welcher keine Zugriffsrechte zugewiesen sind.

- Ordner *WINNT*

[12] Laufwerks-/Ordner-Symbol mit rechter Maustaste anklicken -> Eigenschaften -> Registrierkarte Sicherheitseinstellungen

- Administratoren (<Rechner> \ Administratoren), SYSTEM : **Vollzugriff**
- Benutzer, Hauptbenutzer: **Lesen, Ausführen - Ordnerinhalte auflisten - Lesen**
- Jeder, (ERSTELLER-BESITZER): **keine Rechte!**

Sollte eine der angegebenen Gruppen nicht in der Liste erscheinen, kann diese über den Button *Hinzufügen...* eingefügt werden. Dabei sollte man darauf achten, dass in dem Fenster *Benutzer oder Gruppe auswählen* im Feld *Suchen in:* der Name des Rechners und nicht der Domänen-Name steht. Wir vergeben die Zugriffsrechte ausschließlich an lokale Benutzer-Gruppen. Da ein/e Benutzer/in, der/die sich am PDC anmeldet automatisch als Mitglied der lokalen Gruppe *Benutzer* (soweit nicht anders definiert) aufgenommen wird, gelten die gesetzten Zugriffsrechte auch für alle Domänen-Benutzer.

B Richtlinien für "lokaler Computer"

Dieser Abschnitt beschreibt den Richtlinien-Satz, der in unserer Testumgebung zur Anwendung kam. Die verschiedenen Ebenen des "Richtlinien-Baums" (vgl. Abb.2 Abschnitt 4.2.5) sind durch die eingerückte Auflistung erkennbar. Die Richtlinien selbst (Blätter des Baums) sind zusätzlich mit einem vorangestellten "-" gekennzeichnet. Zusätzlich sind die verwendeten Einstellungen fett gedruckt. Wir haben aus Gründen der Übersichtlichkeit nur die Richtlinien aufgelistet, deren Einstellungen wir verändert haben.

Computerkonfiguration

Softwareeinstellungen

Windowseinstellungen

- Skripts (Start/Herunterfahren)
- Sicherheitseinstellungen
    - Kontorichtlinien
    - Lokale Richtlinien
        - Zuweisen von Benutzerrechten
            - - Ändern der Systemzeit: **Administrator**
            - - Anwendern das Installieren von Druckertreibern nicht erlauben: **aktiviert**
            - - Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen: **aktiviert**
            - - Herunterfahren des Systems ohne Anmeldung zulassen: **deaktiviert**
            - - letzten Benutzernamen nicht im Anmeldedialog anzeigen: **aktiviert**
            - - Wiederherstellungskonsole: automatische administrative Anmeldung zulassen: **deaktiviert**
    - Richtlinien öffentlicher Schlüssel

- IP-Sicherheitsrichtlinien

Administrative Vorlagen

- Windows Komponenten
  - NetMeeting
    - - Remotedesktopfreigabe deaktivieren: **aktiviert**
  - Internet Explorer
    - - Sicherheitszonen: Die Einstellungen für Sicherheitszonen statisch festlegen: **aktiviert**
    - - Sicherheitszonen: Benutzer können Einstellungen nicht ändern: **aktiviert**
    - - Sicherheitszonen: Benutzer können Sites nicht hinzufügen oder entfernen: **aktiviert**
    - - Proxyeinstellungen pro Computer vornehmen: **aktiviert**
    - - Automatische Installation von Internet Explorer-Komponenten deaktivieren: **aktiviert**
    - - periodische Überprüfung auf Softwareaktualisierungen von Internet Explorer deaktivieren: **aktiviert**
    - - Deaktivieren von Software-Update Shell Benachrichtigungen beim Programmstart: **aktiviert**
  - Taskplaner
    - - alle Punkte **aktivieren**
  - Windows Installer
    - - Windows Installer deaktivieren: **aktiviert**
  - (Windows Messenger
    - - alles aktivieren, wenn der Messenger nicht verwendet werden soll - Eintrag besteht nur, wenn der MS Messenger installiert ist))
- System
  - Anmeldung
    - - zwischengespeicherte Kopien von servergespeicherten Profilen löschen: **aktiviert**
    - - Remotebenutzerprofil abwarten: **aktiviert**
    - - Benutzer bei Fehlschlag des servergespeicherten Profils abmelden: **aktiviert**
  - Datenträgerkontingente
    - - Datenträgerkontingente ermöglichen: **aktiviert**
  - DNS-Client
  - Gruppenrichtlinien
  - Windows-Dateischutz

- Netzwerk
- Drucker

Benutzerkonfiguration

Softwareeinstellungen

Windowseinstellungen

- Internet Explorer-Wartung
    - Benutzeroberfläche des Browsers
    - Verbindungen
        - Proxyeinstellungen
            - - http: **10.0.0.1:3128**
    - URLs
    - Sicherheit
        - - Sicherheitszonen und Inhaltsfilter wie gewünscht anpassen
    - Programme
        - - Hier können Anwendungen für die Standardwebdienste festgelegt werden
- Skripts (Anmelden/Abmelden)
- Sicherheitseinstellungen

Administrative Vorlagen

- Windows-Komponenten
    - NetMeeting
        - Anwendungsfreigabe
            - - alle Richtlinien **aktivieren**
        - - alle Richtlinien **aktivieren**
    - Internet Explorer
        - Internetsystemsteuerung
            - - alle Richtlinien **aktivieren**
            - - die restlichen Richtlinien können nach Bedarf angepasst werden
        - (vom Administrator überprüfte Steuerelemente: hier kann man den Zugriff auf einige ActiveX Steuerelemente regeln)
    - Windows Explorer
    - Microsoft Management Konsole

    - Taskplaner
        - - alle Richtlinien **aktivieren**
    - Windows Installer
- Startmenu und Taskleiste
    - - Verknüpfungen für Windows Update deaktivieren und entfernen: **aktiviert**
    - - Menueintrag Ausführen aus dem Startmenu entfernen: **aktiviert**
    - - Option Abmelden dem Startmenu hinzufügen: **aktiviert**
    - - Nicht verfügbare Windows Installer Programme in den Verknüpfungen des Startmenüs deaktivieren: **aktiviert**
- Desktop
    - Active Desktop
    - Active Directory
    - - Pfadänderung für den Ordner "Eigene Dateien" nicht zulassen: **deaktiviert**
- Systemsteuerung
    - Software
        - - Systemsteuerungsoption "Software" entfernen: **aktiviert**
    - Anzeige
        - - Registrierkarte "Einstellungen" ausblenden: **aktiviert**
    - Drucker
        - - Löschen von Druckern deaktivieren: **aktiviert**
    - Ländereinstellungen
    - (- wahlweise kann auch die Richtlinie “Systemsteuerung deaktivieren” **aktiviert**, bzw. die Richtlinie “Nur angegebene Systemsteuerungssymbole anzeigen” **konfiguriert** werden)
- Netzwerk
    - Offlinedateien
    - Netzwerk- und DFÜ-Verbindungen
        - - Aktivieren und Deaktivieren einer LAN-Verbindung nicht zulassen: **aktivieren**
        - - Zugriff auf Eigenschaften einer LAN-Verbindung nicht zulassen: **aktiviert**
        - - Umbenennen von LAN- und RAS Verbindungen aller Benutzer nicht zulassen: **aktiviert**
        - - Entfernen und Hinzufügen von Komponenten für LAN- oder RAS-Verbindung nicht zulassen: **aktiviert**

    - - Aktivieren und Deaktivieren von Komponenten einer LAN-Verbindung nicht zulassen: **aktiviert**
    - - Zugriff auf Komponenteneigenschaften einer LAN-Verbindung nicht zulassen: **aktiviert**
    - - Zugriff auf den Netzwerkverbindungs-Assistenten nicht zulassen: **aktiviert**
    - - Zugriff auf den Menüeintrag "DFÜ-Einstellungen" im Menu "Erweitert" nicht zulassen: **aktiviert**
    - - Zugriff auf "Erweiterte Einstellungen" im Menu "Erweitert" nicht zulassen: **aktiviert**
    - - Konfigurieren von Verbindungsfreigaben nicht zulassen: **aktiviert**
    - - Erweiterte TCP/IP-Konfiguration nicht zulassen: **aktiviert**

- System
  - Anmeldung/Abmeldung
    - - Computersperre nicht ermöglichen: **aktiviert**
    - - Profilgröße beschränken: **aktiviert** - Maximum (5-10 MB), Benutzer beim Überschreiten der max. Größe alle 15 min benachrichtigen
    - - Verzeichnisse aus servergespeicherten Profil ausschließen: **aktiviert**
  - Gruppenrichtlinien
  - - Befehlszeilenaufforderung deaktivieren: **aktiviert**
  - - Programme zum Bearbeiten der Registrierung deaktivieren: **aktiviert**
  - - Angegebene Windows-Anwendungen nicht ausführen: **aktiviert** - regedit.exe

Quellenverzeichnis

- Windows 2000 Administration in a Nutshell, Mitch Tulloch, O'Reilly Verlag, erschienen 2001, ISBN: 1-56592-713-3

- TCP/IP - Netzwerk Administration, Craig Hunt, O'Reilly Verlag, erschienen 1995, ISBN 2-930673-02-9

- http://de.samba.org/samba/docs

- http://www.linuxguruz.org/iptables/howto/iptables-HOWTO-6.html