ADPC — vorbereitender Unterricht
Hardwaregrundlagen, TCP/IP, Windows NT 4.0

Ortwin Ebhardt

1. August 2003

Vorwort und Einleitung

Bei dem vorliegenden Schriftstück handelt es sich um eine (teilweise ergänzte) Zusamenfassung des Unterrichtes, welcher der eigentlichen Windows 2000 Schulung als Vorbereitung vorausging. Er umfasste neben den Grundlagen von hardware und TCP/IP auch Windows NT 4.0.

Ebenfalls im Unterricht enthalten war eine ausgesprochen oberflächliche und meines Erachtens nicht relevante Einführung in Linux; eine sinnvolle Zusammenfassung käme auf ungefähr 70 Seiten [2]. Ebenfalls ausgelassen wurde das Thema *Webserver*, weil es nicht als solches behandelt wurde; in der entsprechenden Woche wurde zwar ein wenig HTML, PHP und JavaScript behandelt, doch die Administration eines Webservers viel dabei unter den Tisch.

In den Anhängen finden sich zwei aus dem Hardware-Grundlagen-Kurs hervorgegangene Versuche und ein paar Vereinfachungen zu TCP/IP.

Das Dokument wurde in LaTeX gesetzt, teils mit `mikTeX` (unter Windows 2000 und Windows NT 4.0), teils mit „echtem“ LaTeX unter Linux.

Sämmtliche Abbildungen wurden ebenfalls direkt in LaTeX geschrieben, sie wurden nicht gescannt oder aus anderen Programmen herausgezogen. Mit anderen Worten: Sie sind nicht Copyright-behaftet.

Die verschiedenen angesprochenen Produkte sind alle eingetragene Markenzeichen ihrer Hersteller oder stehen unter der GPL / TPL.

Inhaltsverzeichnis

Vorwort und Einleitung **iii**

Inhaltsverzeichnis **v**

1 Typografie und Symbolik **1**

2 Hardwaregrundlagen **3**
2.1 Äußerlichkeiten 3
2.2 Die Innereien 4
2.2.1 Der Prozessor 5
2.2.2 North- und Southbridge 5
2.2.3 Der Speicher 5
2.2.4 Das Bord 6
2.2.5 Karten 8
2.2.6 Massenspeicher 9
2.2.7 Die FCC-Nummer 10
2.3 Das BIOS 10
2.4 Peripherie-Geräte und Treiber 12
2.5 SCSI 13
2.5.1 SASI und SCSI (-1) 13
2.5.2 SCSI-2 14
2.5.3 SCSI-3 14
2.6 RAID 15
2.6.1 Software versus Hardware 15
2.6.2 RAID-Level 16
2.7 Drucker 17
2.7.1 Matrix- oder Nadeldrucker 18
2.7.2 Tintentsrahldrucker 18
2.7.3 Laserdrucker 19
2.7.4 Typenrad und Thermodrucker 20
2.7.5 Lokaler Anschluß 20
2.7.6 Der Anschluß über Netzwerk 20
2.7.7 Ansteuerung von Druckern 21

2.7.8 Farbdrucker 22

3 TCP/IP **23**
3.1 Das ISO/OSI-Schichtenmodell 23
3.1.1 Schicht 1: Physikalische Schicht / Physical Layer 23
3.1.2 Schicht 2: Verbindungsschicht / Data Link Layer 24
3.1.3 Schicht 3: ISO/OSI!Schicht / Network Layer 26
3.1.4 Die Schichten 4 – 7 27
3.2 Das DoD-Modell 27
3.3 Adressklassen und Subnetting 28
3.3.1 Grundlagen 28
3.3.2 Adressklassen 29
3.3.3 Besondere Adressen 30
3.3.4 Klassenlose Netze 31
3.4 Switches und Router 33
3.4.1 Switches 33
3.4.2 Router 33
3.5 Protokolle, Häfen, Sockel 34
3.5.1 Protokolle 34
3.5.2 Ports 35
3.5.3 Sockets 36
3.6 DHCP 36
3.6.1 Funktionsweise 36
3.6.2 Ausfallsicherheit 37
3.6.3 APIPA 37
3.6.4 Sonstige Anmerkungen 38
3.7 Namensauflösung 38
3.7.1 NetBIOS 38
3.7.2 Host-Namen und FQDNs 39
3.7.3 DNS 40
3.7.4 Die Namensauflösung unter Windows 2000 40

4 Windows NT 4.0 **43**
4.1 Installation 44
4.1.1 Installationsparameter 44
4.1.2 Installation — ein Beispiel 45
4.1.3 Nachbesserungen 47
4.1.4 Unbeaufsichtigte Installation 47
4.1.5 Installation über das Netzwerk 48
4.2 Festplatten unter Windows NT 4.0 49
4.2.1 Definitionen und Zählweisen 49
4.2.2 Die Systempartition 50
4.2.3 Der Bootmanager 50
4.2.4 RAID 52

4.2.5 Konvertierung . . . 52
4.3 Benutzer und Gruppen . . . 53
4.3.1 Der Schlüssel zu allem — die SID . . . 53
4.3.2 Erstellung eines Benutzers . . . 53
4.3.3 Gruppen . . . 54
4.3.4 Benutzerrechte . . . 55
4.3.5 Domänenweite Benutzer und Gruppen . . . 55
4.4 Dateizugriffsberechtigungen . . . 57
4.4.1 Die Freigabe . . . 57
4.4.2 NTFS-Berechtigungen . . . 58
4.4.3 Effektive Berechtigungen . . . 60
4.4.4 Beispiele für effektive Rechte . . . 61
4.5 Benutzerverwaltung . . . 62
4.5.1 Remote-Verwaltung . . . 63
4.5.2 Die Kontorichtlinien . . . 63
4.5.3 Zeit und Raum . . . 64
4.5.4 Heimverzeichnis und Anmeldescripte . . . 65
4.5.5 Benutzerprofile . . . 66
4.5.6 Benutzer und Gruppen verwalten . . . 67
4.5.7 Systemrichtlinien . . . 68
4.6 Architektur und Multitasking . . . 70
4.6.1 Das System . . . 70
4.6.2 Abwärtskompatibilität durch NTVDM . . . 71
4.6.3 Programmprioritäten . . . 71
4.7 Registry und ERD . . . 72
4.8 Netzwerke . . . 74
4.8.1 PDC und BDC . . . 74
4.8.2 Vertrauensstellungen . . . 75
4.8.3 Verschiedene Domänenmodelle . . . 77
4.8.4 Ein wenig zur Authentifizierung . . . 78
4.8.5 Das DCOM-Prinzip . . . 80
4.8.6 RAS und DFÜ . . . 81
4.9 Drucker . . . 82
4.9.1 Definitionen . . . 82
4.9.2 Druckereinrichtung . . . 84
4.9.3 Verwaltung von Druckern . . . 85
4.9.4 Drucker-Pool . . . 87
4.10 Heterogene Netzwerkzugriffe . . . 87
4.10.1 Grundlegendes . . . 87
4.10.2 Die Verbindung mit einem Novell-Server . . . 88
4.10.3 UNIX / Linux . . . 89
4.11 Dezentrale Datenverwaltung . . . 89
4.11.1 Verzeichnisreplikation . . . 89
4.11.2 Das Backup . . . 90

4.12 Was geht auf dem Rechner vor? 92
4.12.1 Überwachungsrichtlinien 92
4.12.2 Werkzeuge zur Informationsbeschaffung 93
4.12.3 Verwertung der Informationen 95

A WLAN - Gebrauchsanweisung 97
A.1 Geräte 97
A.2 Vorbemerkung 97
A.3 Der Access Point 98
A.4 Die Karten — W2K /XP 98
A.5 Die Karten — W98 99

B Der Palm als Terminal 101
B.1 Vorweg 101
B.1.1 Sinn und Zweck 101
B.1.2 Die Umgebung 101
B.1.3 Erforderliche Materialien 102
B.2 Einrichtung 102
B.2.1 Einrichten unter Linux 102
B.2.2 Vereinfachungen 103
B.2.3 Testen der Linuxreinrichtung 103
B.2.4 Einrichten des Palms 104
B.3 Betrieb und weitere Ansätze 104

C Ergänzungen zu TCP/IP 105
C.1 Rechnen mit Subnetzen 105
C.1.1 Das binäre Zahlensystem 105
C.1.2 Rechenhilfen 106
C.2 Einige Programme 108
C.2.1 Der Befehl `ipconfig` 108
C.2.2 Der Befehl `arp` 108
C.2.3 Der Befehl `telnet` 109

Tabellenverzeichnis 111

Abbildungsverzeichnis 113

Literaturverzeichnis 115

Index 117

Kapitel 1

Typografie und Symbolik

Um dem Leser das Studium dieses Schriftstückes zu erleichtern, wird hier ein Überblick über die verwendeten typografischen Konventionen gegeben.

- Befehle und Programme wurden in `Typenschrift` geschrieben. Des gleichen alle Dinge, die in einer Befehlzeile eingegeben oder im Text-Modus bearbetet werden. Dazu zählen auch Computernamen. Zu letzteren ist außerdem zu bemerken, daß sie grundsätzlich klein geschrieben sind; In der internen Verwaltung wird das ohnehin nicht unterschieden, und es führt unter einigen UNIX-Derivaten zu eigenartigen Effekten, wenn es nicht getan wird.

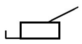
- Dinge, die angeklickt werden müssen (wie etwa Menüpunkte unter Windows) wurden in *Kursiv* abgefaßt. Die selbe Schrift wird jedoch auch für Hervorhebungen sowie ausgeschriebene Abkürzungen verwendet. Bei letzteren wurden die Stellen, aus denen sich die Abkürzungen zusammen setzen, durch FS (*__F__ett-__S__chrift*) hervorgehoben.

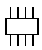
- In Zitaten und bei Verweisen wurden die entsprechenden Personen- und Firmennnamen in KLEINGESETZTE GROSSBUCHSTABEN (mit beginnendem normalem Großbuchstaben) verwendet.

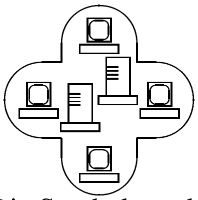
Neben diversen in den Abbildungen bezeichneten Symbole gibt es darüber hinaus die folgenden Standard-Zeichen:

 Ein Client-Computer oder eine einzelne Workstation, die nicht als Server dient.

 Ein Computer, der als Server arbeitet.

 Ein Drucker (oder vielmehr Druckgerät)

 Ein Switch oder Hub



Eine Windows NT 4.0 Domäne. (Symbolisch zwei Server für PDC und BDC und mehrere Clients.)

Die Symbole und Konventionen wurden zur leichteren Erfassung des Inhaltes seitens des Lesers einegsetzt. Inkonsistenzen sind dem Verfasser anzulasten. Keines der Symbole ist mir irgend welchen Copyrights behaftet, sie können jederzeit von jedem, der sie hübsch findet, verwendet werden.

Kapitel 2

Hardwaregrundlagen

Bei diesem Kapitel handelt es sich um eine Mitschrift des ADPC-Hardware-Unterrichts. Abschnitt 2.1 behandelt die äußeren Anschlüsse eines heutigen Computers, Abschnitt 2.2 geht auf sein Innenleben ein, Abschnitt 2.3 behandelt das Computer-BIOS, in Abschnitt 2.4 werden typische Peripheriegeräte betrachtet, Abschnitt 2.5 behandelt die Funktionsweise von SCSI, Abschnitt 2.6 gibt eine Übersicht über RAID, Abschnitt 2.7 schließt das Kapitel mit Ausführungen zu Druckern ab. Es erhebt weder Anspruch auf Vollständigkeit noch auf Richtigkeit.

Als Hilfsmittel wurden die im Internet verfügbaren Artikel *Hardwaregrundlagen* [3] und *The PC Guide* [7] sowie der vom T10-Konsortium verabschiedete SAM-2 Standard [15] verwendet.

> „What the hell?! We want something that looks cool!“
> „We want a superweapon!“
>
> ANNA & UNI PUMA, *Dominion Tank Police Act II*

2.1 Äußerlichkeiten

Die Betrachtung der Rückseite eines zeitegnössischen, typischen Rechners (also eines ATX-Rechners in einem Tower- oder Midi-Tower- Gehäuse) zeigt die folgenden Schnttstellen:

Stromanschluß: Für gewöhnlich handelt es sich hier um einen weiblichen Kaltgerätestecker, ausgestattet mit Phase, Masse und Erde.

Monitor: An manchen Geräten findet sich ein Stromanschluß für den Monitor; hierdurch wird gewärleistet, daß selbiger nur dann Strom bekommt (und verbraucht), wenn der Computer eingeschaltet ist. Diese Einrichtung war früher häufig anzutreffen, verschwindet jedoch langsam.

Maus-Anschluß: Früher wurden Mäuse über serielle Schnittstellen angeschlossen. Heute wird dazu ein eigener Port benutzt. Er entspricht der PS/2-Norm

IBMs. Rechner mit solchen Anschlüssen haben meistens zwei davon: Einer (meistens linke) ist häufg grün und der für den Mausanschluß gedachte.

Tastatur-Anschluß: Auch Tastaturen werden heutzutage über PS/2 angeschlossen. Der Anschluß befindet sich meistens rechts neben dem der Maus und ist häufig violett. Früher wurden Tastaturen über einen dicken, fünfoligen Stecker ageschlossen, der Ähnlichkeiten mit einem aten DIN-Aufio-Kabel hat. Doch ebenso, wie letzteres dem Chinch-Kabel gewichen ist, findet das erstere heute kaum noch Anwendung.

USB-Schnittstellen: USB (***U**nievrsal **S**erial **B**us*) wird dazu benutzt, alle möglichen (und unmöglichen) Geräte anzuschließen. Dazu zählen neben Digitalkammeras, Druckern und Scannern auch Mäuse und Tastaturen. Manche Rechner haben mehr als zwei USB-Schnittstellen, von denen zwei an der Frontseite des Rechners herauskommen.

Serielle Schnittstellen: Die Bedeutung dieser Schnittstellen hat sich in den letzten Jahren ziemlich gewandelt; früher wurden die Mäuse und Modems über solche Schnittstellen angeschlossen. Damals gab es neben dem normalen, neunpoligen, männlichen Anschluß auch noch einen 24 poligen. Dieser wird heute nicht mehr verwendet. Mäuse laufen heute über den PS/2-Port, und Modems kommen mehr und mehr aus der Mode. Falls der PS/2-Port deffekt ist, kann die Maus (über einen Adapter) an einer solchen Schnittstelle betrieben werden, und analogen Modems arbeiten meistens auch mit ihnen. Zudem kommt ihnen besondere Bedeutung im Zusammenhang mit Terminals und der Verwaltung von Geräten der Firma Cisco zu.

Parallele Schnittstellen: An der Schnittstelle (25-Polig, männlich) hängen vor allem Drucker. Ihre Bedeutung schwindet heute ebenfalls.

Grafikkarte: An den (weiblichen) Ausgang der Grafikkarte wird der Monitor angeschlossen. (Na klar, wie sollte das Bild denn auch sonst dahin kommen?)

Soundkarte: Diese Karte ist bei vielen ATX-Rechnern bereits auf dem Bord und, wie der Name schon sagt, für die Beschallung des Benutzers zuständig. Sie verfügt meistens über drei Buchsen für 3,5 mm Klinkenstecker. Dabei ist eines ein Line-Ausgang (kann an eine Aktiv-Box oder eine Stereoanlage angeschlossen werden), einen Line-Eingang (da kann eine Stereoanlage angeschlossen werden) und einen Mikrophoneingang. Letzterer unterschiedet sich durch Impedanz und Vorverstärkung von dem Line-Eingang.

2.2 Die Innereien

Nach Aufschrauben des Rechners finden sich verschiedene Bauteile. Im Einzelnen werden hier das Bord, der Prozessor, der Speicher, einzusteckende Karten und Massenspeichergeräte wie Festplatten und CD-ROM-Laufwerke betrachtet.

2.2.1 Der Prozessor

Auf der Hauptplatine befindet sich, meist unter einem großen Lüfter, der Prozessor (oder auch die CPU, ***C**entral **P**rocessing **U**nit*). CPUs sollten auf enem Sockel sitzen, so daß sie bei Bedarf (bei Durchbrennen oder Aufrüsten) ausgewechselt werden können. Die meisten Prozessoren stammen von den Firmen Intel und AMD. Sie basieren alle auf dem x86-Befehlssatz und arbeiten mit 32 Bit. Es ist jedoch nur eine Frage der Zeit, bis diese Alt-Lasten über Bord geworfen und 64 Bit-Prozessoren Einzug in den Alltag halten werden.

Ebenfalls in den Prozessor integriert ist der L1 oder *First Level* Cache. Er cachet alle Zugriffe, die an die CPU gespeichert werden, zwischen. Hier kommt SRAM zum Einsatz.

2.2.2 North- und Southbridge

Zwei wesendliche Bestandteile eines heutigen Bordes sind die North- und die Soutbridge. Die Northbridge verbindet die CPU mit dem Speicher und der Southbridge. Ebenfalls daran hängt der AGP-Slot (siehe 2.2.4, S. 7). In die Northbridge ist der L2 oder *Second Level Cache* integriert.

Die Southbridge verbindet die Northbridge mit allen anderen Dingen des Bordes, etwa den IDE-Kanälen, den Bussen und so weiter. Einige Schnittstellen sind in der neusten Version der Intel-Southbridge bereits enthalten. Das gilt zum Beispiel für die USB-Schnittstellen.

2.2.3 Der Speicher

In mehreren sogenannten Speicherbänken befindet sich der Arbeitsspeicher des Computers. Dieses sogenannte RAM (*Random Access Memory*) gibt es in verschiedenen Ausführungen, zumal es sich mit der Zeit auch weiterentwickelt hat.

D-RAM: *Dynamic RAM* war das erste verwendete RAM. Hierbei steht *dynamic* dafur, daß die im RAM gespeicherten Informationen nicht sonderlich lange dort gehalten werden können. Durch einen sogenannten *Refresh* (Auffrischung) mußten sie in regelmäßigen Abständen aufgefrischt werden. Dieser Refresh ist auch heute noch nötig.

SIMM: SIMM-Module waren die erste Möglkichkeit, Speicher nicht auf das Bord zu löten, sondern zu stecken. Sie finden in einigen Druckern heute noch Verwendung. Weiterentwicklungen, die noch Über die selbe Bauform verfügten, waren FPM (*Fast Page Mode*) und EDO (*Extended Data Output*) RAM. FPM wurde durch Zugriffsverfahren beschleunigt, EDO speicherte einfach bestimmte Anfragen zwischen.

PS/2: Eine Weiterentwicklung IBMs, bei der vor allem die Busbreite vergrößert wurde. Die Module sahen ebenfalls anders aus, so daß eine Fehlbestückung ausgeschlossenw erden konnte. Ein PS/2-Modul reichte aus, um einen 486er voll zu bestücken.

SD-RAM: *Synchron Dynamic RAM* verfügt über 168 Pins und wurde bis vor Kurzem auf den meisten modernen Bords eingesetzt. Die Bauform wird auch als DIMM bezeichnet. Es wird jedoch von seinem Nachfolger, dem DDR-RAM, abgelößt.

DDR-RAM: *Double Data Rate RAM* ist dem normalen SD-RAM ähnlich. Dadurch, daß bei der Datenauswertung zur Übermittlung der Signale auch die Flanken verwerndet werden, ist die Zugiffsgeschwindigkeit doppelt so hoch wie bei seinem Vorgänger.

Rambus-RAM: Dieses RAM wurde nach seiner Entwicklungsfirma *Rambus* benannt. Es arbeitet ähnlich wie DDR-RAM, nutz aber eine andere Organisation des Zugriffes. Es ist ausgesprochen teuer und wird daher — außer in Multiprozessorumgebungen, für die es wohl besser geeignet ist als DDR-RAM — selten eingesetzt.

2.2.4 Das Bord

Das Bord hällt die meisten Dinge (also den Speicher, den Prozessor und alles, was sonst noch zum Funktionieren nötig ist) zusammen. Das für den Anwender vielleicht wichtigste darauf sind die Erweiterungsslots.

Diese Slots dienen dazu, Erweiterungskarten mit dem Bord zu koppeln. Sie werden dann mit einem Bus[1] verbunden. Je nach Alter und Hersteller des Bordes können das verschiedene Bus-Systeme (und entsprechend verschiedene Slots) sein. Im Folgenden werden einige davon aufgeführt:

Industrial Standard Architecture (ISA): Dies ist der älteste und sozusagen PC-Native Bus. Er setzt sich aus einem XT und einem AT-Teil zusammen.

Ursprünglich, in Intels 8080er-Prozessor, gab es nur den XT-Teil. Er hat 8 Bit Bandbreite und wird mit 4,7 MHz betrieben. Später, als die Prozessoren 16 Bit verkrafteten, wurde eine Erweiterung auf 16 Bit vorgenommen, das ist der ogenannte AT-Teil.

Microchannel (MCA): Bei MCA handelt es sich um eine Entwicklung IBMs. Hierbei handelte es sich um den ersten echten 32 Bit Bus. Er wurde vor allem im Zusammenhang mit IBMs Betriebssystem OS/2 benutzt. OS/2 setzte sich jedoch nicht gegen Microsofts Windows durch, und MCA verlor den Kampf mit den von Intel hervorgebrachten Bussystemen…

Extended Standard Industrial Architecture (EISA): Hiermit legte Intel eine Antwort auf den MCA vor. Das System hatte den Vorteil der Abwärtskompatibilität (in EISA-Sots paßten auch ISA-Karten und umgekehrt) und einen

[1] Der Ausdruck wird als aus *Netzwerkgrundlagen* bekannt vorausgesetzt.

Durchsatz von 33 MByte/s. Die doppelt Bandbreite wurde durch ein doppelseitiges Anbringen von Kontakten geschaffen. Er wurde vor allem in Servern eingesetzt und war ziemlich teuer. Auch diese Bus-Architektur gibt es heute nicht mehr.

Vesa Local Bus (VLB): VLB war ein Versuch, ISA weiter zu entwickeln. Es wurde ein weiterer Teil an den ISA-Slot gebracht. Der Durchsatz lag bei 100 MByte/s, die Taktfrequenz bei 50 MHz.

Perpheal Components Interconnect (PCI): Der inzwischen verbreitetste Bus ist der endgültige Schritt weg von ISA. Um das zu erreichen ist ein weiterer Chip auf dem Bord nötig, der zwischen den beiden Architekturen vermittelt. Er wird Bridge genannt. PCI hat einen Durchsatz von 133 MByte/s und eine Taktfrequenz von 33 MHz.

Accellerated Graphic Port (AGP): AGP wurde ausschließlich für den Einsatz mit Grafikkarten entwickelt. Es ist nicht geplant, durch diese Architkektur PCI zu ersetzen. Das ist auch nicht wirklich möglich, da der Anschluß direkt an die Northbridge (siehe 2.2.2, S. 5) geschieht.

AGP bietet der Grafikkarte die Möglichkeit, direkt auf den Hauptspeicher des Rechners zuzugreifen und ihn zur Auslagerung von Daten zu nutzen. Auch der Zugriff der Karte ansich ist wesendlich schneller; der Durchsatz liegt je nach Modues ($1\times$, $2\times$, $4\times$ oder gar $8\times$) bei 254.3 MB/s bis theoretisch ungefähr 2.1 GB/s.

Der Zugriff ist für grafikrelevante Daten optimiert und entsprechend in die Northbridge implementiert. Aus diesem Grund ist es ausgesproche schwierig (wenn nicht sogar unmöglich), andere Geräte für diesen Port zu fertigen. Doch wann immer einige technikbegeisterte Freaks zusammenkommen, werden sie auf den Gedanken kommen, das *müsse* doch gehen. . . [2]

CNR Riser: Dieser Bus hat verschiedene Bezeichnungen, auf einigen Bords heißt er auch AMR-Bus. Das Prinzip ist immer das Gleiche; eine Riser-Karte wird vom Bord als *onboard* erkannt und entsprechend verwaltet. Gedacht ist dieser Slot vor allem für Soundkarten, Modems und Netzwerkkarten. In der Praxis sind diese Karten zumindest in Deutschlans eher selten anzutreffen.

Neben diesen Slots gibt es noch eine Reihe weiterer Anschlüsse:

Konnektoren: Mit Konnektoren sind in diesem Fall die Anschlüsse des Bordes für das Gehäuse gemeint. Sie liegen meistens alle beisammen. Die gebräuchlichsten sind

Power: Der An/Ausschalter

Reset: Der Reset-Schalter

[2] Der Verfasser nimmt sich da nicht aus.

Speaker: Die Computerlautsprecher (das sind die, die das nervige Biepen erzeugen)

Power-LED: Eine LED, die leuchtet, wenn der Rechner läuft.

HDD-LED: Eine LED, die leuchtet, wenn auf ein Gerät an einem der IDE-Ports zugegriffen wird

Weitere Soundkartenanschlüsse: Die internen Anschlüsse sind meistens für den Anschluß eines CD-ROM-Laufwerkes gedacht; viele dieser Geräte haben einen direkten Sound-Ausgang. Hierdurch müssen die Daten einer abgespielten CD nicht erst durch den IDE-Bus und den PCI-Bus zur Karte transportiert, sondern können direkt verwendet werden. Manche Karten haben mehr als einen Anschluß; neben der Möglichkeit, mehr als ein CD-ROM anzuschließen, ist sicherlich die erwendung im Zusammenhang mit einer TV-Karte nicht uninteressant.

IDE: Auf den meisten Bords gibt es zwei IDE-Controller. An jeden davon können zwei IDE-Geräte, meistens Platten oder CD-ROM-Laufwerke, angeschlossen werden. Eines läuft dabei als *Master*, eines als *Slave*. Diese Einstellungen werden über Jumper (zu Deutsch: Steckbrücken) vorgenommen.

FDC: Der Anschluß für das Diskettenlaufwerk befindet sich unmittelbar neben den IDE-Schnittstellen. Er ist ein wenig kleiner.

2.2.5 Karten

In die in 2.2.4, S. 6 beschriebenen Slots können Erweiterungskarten eingesteckt werden. Das können Grafik- oder Soundkarten, aber auch weitere Schnittstellen, Controller für Massenspeichergeräte oder Karten zum Ansteuern besonders exotischer Geräte sein. Hier eine Übersicht über die wichtigsten Kartenarten:

Grafikkarten: Diese Karten ermöglichen es, die Geschehnisse im Rechner auf einem Monitor (oder TFT-Display oder sonst einer ANzeigeeinheit) zu berachten. Heutige Grafikkarten werden in den AGP-Slot gesteckt.

Soundkarten: Diese Karten sind in der Lage, Klänge auszugeben. Da sie meistens nicht über Lautsprecher oder die Leistung, einen normalen Lautsprecher direkt anzuschließen, verfügen, bietet sich der Anschluß von Aktiv-Boxen oder einer Stereoanlage (oder eines andersgearteten Verstärkers) an. Viele neuere Bords verfügen von sich aus über eine Soundkarte.

SCSI-Controller: Auf den wenigsten Borden ist ein Controller für SCSI enthalten. SCSI ist ein Bussystem, mit dem sich verschiedene Geräte (Festplatten, CD-ROM-Laufwerke, Streamer, Scanner...) ansprechen lassen. Es war früher eine Lösung für Server, da IDE die Leistungen SCSIs nicht erbrachte. Das hat sich heute jedoch geändert, und der hohe Preis für SCSI-Geräte führt zu einem langsamen Rückzug des Systemes. Auf SCSI wird in Abschnitt 2.5, S. 13 näher eingegangen.

Schnittstellenkarten: Gelegendlich werden zusätzliche Schnittstellen für USB-, Parallel- oder Serielle Geräte benötigt. Für diese gibt es Karten, welche die Schnittstellen bereitstellen.

Netzwerkkarten: Netzwerkkarten (NICs) stellen die Verbindung mit dem Netzwerk her.

2.2.6 Massenspeicher

Unter Massenspeicher werden alle Geräte zusammegefaßt, auf denen sich große Mengen von Daten ($>$ 2MByte) befinden können. Die wichtigsten Vertreter sind Festplatten, CD- und DVD-Laufwerke, und Streamer. Ebenfalls recht beliebt sind Wechselplatten, ZIP-Drives und ähnliche Lösungen.

Heutzutage werden die meisten dieser Geräte über IDE angesprochen. Nichts desto Trotz gibt es einige dieser Dinge nur für SCSI.

Festplatten: Festplatten sind Medien, von denen gelesen und auf die geschrieben werden kann. Sie werden heutzutrage meistens über IDE angeschlossen (vergleiche 2.2.5, S. 8). Moderne[3] Platten können mehr als 100 GByte fassen.

Wechselplatten: Wechselplatten sind Festplatten, die mit Hilfe eines sogenannten Wechselrahmens aus dem Rechner herausgenommen werden können. Sie werden zum Transport großer Datenmengen benutzt.

CD- und DVD-Laufwerke: CD-Laufwerke dienen dem Zugriff auf CDs (***C**ompact **D**iscs*). Normale CD-ROM-Laufwerke können diese lediglich lesen, CD-Writer sind in der Lage, CD-Rohlinge zu beschreiben. CD-R-Rohlinge (CD-Readable) können einmal, CD-RW-Rohlinge (CD-Read/Write) können mehrmals beschrieben werden.

DVD, *Digital Vertaile Disc*, ist eine Weiterentwicklung der CD, auf die wesendlich mehr Daten passen. Sie wird vor allem für Videos benutzt.

Für den Anschluß gilt das gleiche wie für Festplatten.

Streamer: Streamer sind Bandlaufgeräte. Mögliche Anschlußmöglichkeiten sind Floppy-Streamer, die am FDC angeschlossen werden, SCSI-Streamer und proprietäre Lösungen mit eigenen Karten zur Ansteuerung.[4] Auch bei den Bändern gibt es ebenfalls Unterschiede. Die betagten QUIC-Bänder speichern Daten analog, wären DAT-Bänder das digital machen. Heutige Streamer sind meistens DAT-Streamer.

[3] Das bezieht sich auf 2003.
[4] Von anderen ist dem Verfasser nichts bekannt.

Sonstige Lösungen: Hierzu zählen ZIP-Drives und änhnliche Erfindungen. Ebenfalls erwähnt werden sollten USB-Sticks. Der Anschluß kann von Gerät zu Gerät verschieden sein.

2.2.7 Die FCC-Nummer

Um Hardwareelemente zu identifizieren, hat die *Federal Communication Commission* die FCC-Nummer geschaffen. Theoretisch sollte jedes Gerät und jede Einbaukarte über eine FCC verfügen. Diese besteht aus einem dreistelligen Garantiecode und einem mehrstelligen Hersteller- und Gerätecode. Näheres zur FCC findet sich auf ihrer Homepage (`http://www.fcc.gov`).

Falls es notwendig wird, ein Gerät zu identifizieren, und nur die FCC-Numemr zur Verfügung steht, gibt es im Netz einige Suchseiten, die eine Identifizierung nach FCC-Nummer liefern. Nicht zu letzt ist hier die Seite der FCC selbst zu nennen (`http://www.fcc.gov/oet/fccid`).

2.3 Das BIOS

BIOS steht für *Basic Input Output System*. Es ist sozusagen ein Minibetriebsystem, welches für das Reibungslose Starten und Initialisieren der verschiedenen Geräte zuständig ist. Einige Betriebsysteme benutzen es lediglich zum Starten und verwenden danach ihre eigenen Routinen.

Das BIOS ist bei heutigen Rechnern auf einem FLASH-ROM[5] gespeichert und kann bei Bedarf überschrieben werden. Der Vorteil dieser Möglichkeit liegt darin, daß eine neue Version des BIOS bei Bedarf aufgespielt werden kann. Das kann notwendig sein, falls bestimmte Geräte nicht als Bootgeräte akzeptiert werden. Der Nachteil liegt darin, daß im Falle eines Unfalles beim Flashen des ROMs das Bord meistens nicht mehr zu gebrauchen ist.

In den meisten Fällen ist das BIOS wärend des Rechnerstartes über Drücken der `<DEL>`-Taste zu erreichen. Das kann aber unter Umständen auch eine andere Taste sein. Das sollte normaler Weise aber in Form einer kurzen Textnachricht eingeblendet werden.

Innerhalb des BIOS lassen sich verschiedene Dinge einstellen. Das kann von Hersteller zu Hersteller wechseln. Folgende Dinge sollte jedoch in der einen oder anderen Form immer vorhanden sein:

CMOS Feature Setup: Unter diesem Punkt werden grundlegende Einstellungen angegeben. Hier können unter anderem das Datum und die Zeit angegeben werden. Ebenfalls recht interessant sind die Eintragungen der Festplatten. Falls hier nichts steht, werden beim Starten des Rechners auch keine Platten gefunden. Die Eintragungen können entweder von Hand durchgeführt werden oder über die IDE-Autoerkennung. Diese ist in manchen Fällen ebenfalls

[5] Auf einem Baustein namens CMOS, *Complementary Metal Oxide Semiconductor*.

hier zu finden, in anderen ein eigener Unterpunkt im Hauptmenü. ***Achtung!*** Bei einigen BIOS-Versionen ist es zwingend nötig, auch die CD-Laufwerke hier anzugeben, da sonst nicht von ihnen gebootet werden kann. Ebenso wie die Festplatten können in diesem Menü auch die Diskettenlaufwerke angegeben werden.

Advanced BIOS Features: Hier finden sich tiefergehende Einstellungsmöglichkeiten des BIOS. Die vermutlich für die meisten Benutzer wichtigste ist die Reinfolge der zu bootenden Geräte. Durch diese Angabe wird geregelt, welche Geräte wann nach einem bootbaren Medium durchsucht werden. Rechner, auf denen Dinge installiert werden sollen (oder die den Start mit einer Bootdiskette erfordern) ist oftmals als Reinfolge `A, CDROM, C` angegeben. Rechner, die nur von Festplatte gestartet werden sollen, haben meistens den Eintrag `C only`.

Ebenfalls von vielen Aktiviert ist die Option *Quick Power on Selftest*, die bewirkt, daß das Hochfahren durch Weglassen einiger weniger wichtiger Tests beschleunigt wird.

Advanced Chipset Feature Setup: Mit diesem Menü werden die North- und die Southbridge konfiguriert. In seltenen Fällen enthällt es auch Einstellungen zu den Schnittstellen (meistens sind die unter *Integratet Peripheals* zu finden).

Power Management: Hier kann angegeben werden, welche Stromsparmaßnahmen von Seiten des Rechners zum Tragen kommen. Unter anderem kann der Monitor nach einer gewissen Zeit abgeschaltet oder die Festplatte bei ausbleibenden Zugriffen werden.

PnP / PCI Configurations: Dieser Menüpunkt ist für die Konfiguration des PnP-OS zuständig. Meistens kann das nua an oder ausgeschaltet werden. Einige ältere ISA-PnP-Karten können nur bei aktiviertem PnP-OS erkannt werden.

Die PCI-Einstellungen dienen dem Binden von IRQs an PCI-Slots. Meistens ist es sicher, die Einstellungen bei `AUTO` zu belassen.

Integrated Peripheals: Wie der Name schon sagt können hier die in das Bord integrierten Geräte und Schnittstellen aktiviert, deaktiviert und konfiguriert werden. In manchen Fällen sind das auch die Sound- und die Grafikkarte. Die wichtigsten Dinge jedoch sind die IDE-Controller und der Diskettencontroller; neben den verschiedenen Zugriffsmodi können die hier auch abgeschaltet werden. Gleiches gilt für die Schnittstellen des Rechners.

Set Supervisor- / Userpassword: Das Supervisorpassword schützt das BIOS vor unerlaubten Zugriffen. Das Benutzerpaßwort geht noch weiter und verhindert den Start des Rechners, so kein richtiges Paßwort eingegeben wird.

Da es durchaus vorkommen kann, daß ein Paßwort vergessen wird, gibt es zudem ein Herstellerpaßwort. Dieses sollte nur dem hersteller bekannt sein (und kursiert entsprechend im Internet. . .) und greift immer.

2.4 Peripherie-Geräte und Treiber

Als Peripheriegeräte wird allgemein alles bezeichnet, was sich an einen Computer angeschlossen werden kann. Einige typische Peripheriegeräte sind:

- Maus
- Tastatur
- Monitor
- Joystick
- Modem
- Scanner
- USB-Stick
- Drucker

Der Anschluß der meisten dieser Geräte wurde in Abschnitt 2.1, S. 3 angesprochen, Drucker werden in Abschnitt 2.7, S. 17 besprochen.

Egal, ob ein Gerät intern oder extern angeschlossen wird, meistens[6] wird ein sogenannter Treiber benötigt. Dieser vermittelt zwischen den von Programmen an das Betriebsystem gestellten und an die Treiber weitergeleiteten Anforderungen und den Geräten.

Unter Windows befinden sich große Teile der Treiber in den *Dynamic Link Libraries*, auch nach ihrer Endung DLLs genannt.

Uner Linux sind Treiber entweder direkt im Systemkern integriert, oder weden als Module nachgeladen. Falls sie als Module vorliegen haben sie meistens die Endung `.o` und liegen in dem Verzeichnis `/lib/modules`.

Um einen Treiber zu installieren oder zu aktualisieren gibt es unter Windows verschiedene Methoden. Im nachfolgenden werden einige davon beschrieben:

Automatisch: Ein Assistent durchsucht das System nach neuer Hardware durchsucht. Falls welche gefunden wird, durchforstet er den Rechner nach passenden Treibern. Falls keiner gefunden wird, muß der Benutzer einen angeben.

Systemstart: Fällt dem Rechner beim Hochfahren ein neues Gerät auf, verfährt er wie oben beschrieben.

Manuell: Falls der Rechner bei seiner Suche nichts findet (bei alten ISA-Karten und an die serielle Schnittstelle angeschlossenen Geräten kann das passieren), kann im Hardwareassisstenten direkt die Installation eines Treibers erzwungen werden.

Eine weitere, nicht immer funktionierende Methode besteht darin, die `.inf`-Datei des Treibers mit der rechten Maustaste anzuklicken und *Installieren* zu wählen. Zumindest theoretisch sollte der Treiber dann eingerichtet werden. Meistens ist danach ein Neustart zur endgültigen Einrichtung erforderlich.

Aktualisierung: Werden im Gerätemanager die Eigenschaften des Gerätes aufgerufen, findet sich auf der Karte *Treiber* das Feld *Aktualisieren*. Das führt zu

[6] Tatsächlich gibt es einige wenige Geräte, die — zumindest theoretisch – keinen Treiber brauchen. Dazu zählen etwa Dumb Terminals.

einer Suche nach einem besseren als den verwendeten Treiber an verschiedenen vorher vom Benutzer anzugebenden Orten. Wird keiner gefunden, kann die Benutzung eines bestimmten Treibers erzwungen werden.

2.5 SCSI

SCSI (***S**mall **C**omputer **S**ystem **I**nterface*) wurde zur Ansteuerungen unterschiedlichster Peripherie-Geräte entwickelt. Es handelt sich hierbei um ein paralleles Bussystem. Wie bei einem Ethernetzwerk müssen beide Enden der SCSI-Kette mittels Abschlußwiederständen terminiert sein; sonst gibt es Signalreflektionen.

Das Funktionsprinzip bei SCSI ist recht einfach: Es gibt einen Controller und mehrere daran hängende Geräte. Falls der Controller von Außerhalb angesprochen wird, setzt er die Anfragen um und spricht das entsprechende Gerät an. Der Controller arbeitet in diesem Fall als *Initiator*. Das angesprochene Gerät wird als Ziel, *Target*, bezeichnet.

Sämmtliche Operationen werden vom Controller erledigt. Das bedeutet zum Einen, daß er über einen eigenen Chip verfügen muß, und zum Anderen, daß der Verwaltungsaufwand nicht den Prozessor des Rechners belastet.

Bei einem „normalen" SCSI-Controller wird von einer maximal 8 Geräte fassenden Kette ausgegangen. Eines dieser Geräte ist immer der Controller. (Mit anderen Worten: Es können maximal 7 Geräte angeschlossen werden.) Bei Wide-SCSI (siehe 2.5.2, S. 14) können 16 Geräte in einer Kette stehen (also 15 Geräte und ein Controller). Diese Geräte werden anhand ihrer SCSI-ID identifiziert. Eine ID kann zwischen 0 und 7 liegen. Für gewöhnlich ist 7 die ID des Controllers, da die ID neben der Identifizierung auch die Priorität des Gerätezugriffes beschreibt. Jede ID darf genau einmal vergeben sein. (Es ist jedoch vollkommen egal, welches Gerät welche ID hat.) Bei Wide-SCSI verhällt sich die Priorität *nicht* entsprechend. Hier lautet sie (mit der höchsten beginnend):

7, 6, 5, 4, 3, 2, 1, 0, 15, 14, 13, 12, 11, 10, 9, 8

Auch in dieser Variation hat der Controller meistens die ID 7.

Geräte können über weitere *Logische Geräte* (*LU*, *Logical Units*) verfügen. Diese werden über *LUNs*, *Logical Unit Numbers*, angesprochen. So etwas kommt etwa bei einem CD-Wechsler vor, der mehr als eine CD verwaltet, obschon er nur über eine SCSI-ID verfügt.

SCSI gibt es inzwischen in verschiedenen Revisionen und Varianten.

2.5.1 SASI und SCSI (-1)

Das Kürzel SASI steht für *Shuggart Associates System Interface* und beschreibt ein 1980 von der Firma *Shugat Associates* erfundenes System.

SASI wurde 1982 von der ANSI übernommen und in SCSI umbenannt. De Facto gab es niemals einen „echten" SCSI-1 Standard, die Geräte des SASI-Standards wurden (und werden) im Nachhinein so bezeichnet. SCSI-1 benutzt eine

Bandbreite von 8 Bit (später auch als *Narrow Bus* bezeichnet) und hat eine Geschwindigkeit von 5 MByte pro Sekunde. Diese Umbenennung geschah im Jahre 1986. Aufgrund der drei für IDs benutzten Bits können maximal 8 Geräte angeschlossen werden. Die Kabellänge beträgt maximal 6 Meter.[7]

2.5.2 SCSI-2

Parallel zur Umbenennung von SASI in SCSI-1 wurde eifrig an SCSI-2 gearbeitet. 1990 war es fertig, doch erst 1994 wurde es tatsächlich verabschiedet. Neben einigen Vereinfachungen im Befehlssatz wurden einige wichtige Erweiterungen, die dann auch als eigene Produkte erschienen, eingeführt:

Fast SCSI: Hierbei wurde die Geschiwndigkeit auf 10 MB/s erhöht, der Bus beträgt immer noch 8 Bit. Der Adress-Teil betrug immer noch 3 Bit. Die maximale Kabellänge beträgt 3 Meter.

Wide SCSI: Eine Anhebung des *Narrow Busses* auf 16 oder sogar 32 Bit. Hier wurde der Adress-Teil auf 4 Bit erhöht, wodurch sich 16 Geräte in einer Kette befinden können. Die maximale Kabellänge beträgt 6 Meter.[7]

Fast Wide SCSI: Das meistbenutzte SCSI kombiniert die Verbreiterung des Busses mit der Geschwindigkeit des schnelleren SCSIs, also 16 Bit bei 10 MB/s. Auch hier sind 16 Geräte möglich, die Kabellänge beträgt 3 Meter.[7]

2.5.3 SCSI-3

Noch bevor der Standard SCSI-2 wirklich verabschiedet war, begannen die Arbeiten an SCSI-3. Aus verschiedenen Gründen lief das ganze ein wenig auseinander. Es gibt inzwischen drei grobe Unterarten von SCSI-3 (die mit dem Ausdruck SPI-1 – SPI-3 für *SCSI Parallel Interface* bezeichnet werden).

SPI (-1): In diesem Standard befinden sich *Ultra SCSI* mit einer Übertragungsrate von 20 MB/s bei 8 Bit Busbreite und *Ultra Wide SCSI* mit einer Busbreite von 16 Bit. An das „normale“ Ultra SCSI können 8 Geräte angeschlossen werden, an das „weite“ 16. Die Kabellänge beträgt bei beiden 1,5 Meter, Falls nur die Hälfte der maximalen Geräte verwendet wird, kommen sie auf eine Länge von 3 Metern.[7]

SPI-2: Für diesen Standard wurde ein neues Übermittlungsverfahren entwickelt, nämlich LDV. Das steht für *Low Differential Voltage* und beinhaltete eine

[7] Innerhalb von PCs wird stets das sogenannte *Singe Ended* Verfahren eingesetzt. Dies ist das gewöhnliche Prinzip mit `0` und `1`, Spannung oder keine Spannung. Das führte bei SCSI jedoch zu Problemen (die der Verfasser dem Leser – und sich – erparrt), die zu den verhältnismäßig geringen Kabellängen führt. Eine Methode, das zu verhindern, liegt in *HDV*, *High Different Voltage*. Hierbei kommen einige Schutzmechanismen und Differntialunterschiede zum Tragen. Dadurch kann die Länge der Kabel maximal 25 Meter betragen — egal, bei welchem SCSI-Level. Aus Kostengründen hat es sich in der PC-Welt niemals durchgesetzt.

ganze Reihe von Dingen aus HDV.[8] Das Prinzip ermöglich höhere Übertragungsraten bei längeren Kabeln. *Ultra2 SCSI* arbeitet mit einer Busbreite von 8 Bit, 8 Geräten und 40 MB/s. Die Variante *Wide Ultra2 SCSI* ist identisch, verfügt aber über eine Busbreite von 16 Bit (und kann entsprechend 16 Geräte ansprechen). Die Kabellänge kann in beiden Fällen 12 Meter betragen, falls nur zwei Geräte angeschlossen werden sogar 25. Ebenfalls möglich ist der Betrieb mit HDV.

SPI-3: In diesem Standard wird ausschließlich LDV verwendet, HDV ist nicht vorgesehen. Die Standards *Ultra3 SCSI*, *Ultra160(/m) SCSI* und *Ultra160+ SCSI* haben alle eine Geschwindigkeit von 40 MB/s und unterschieden sich in ihren verschiedenen Funktionen zur Kompression, Beschleunigung und Verifizierung. Der Standard *Ultra320 SCSI* hat eine Geschwindigkeit von 40 MB/s. Alle vier Standards arbeiten mit 16 Bit Busbreite, 16 Geräten und einer Kabellänge von 12 Metern. Werden nur zwei Geräte angeschlossen, sind es sogar 25 Meter.

Es ist noch nicht abzusehen, welche Entwicklungen SCSI-3 noch durchlaufen wird. Ob es tatsächlich von ATA (und dem designierten Nachfolger SATA) abgelößt wird, ist nicht unerheblich von verschiedenen wirtschaftlichen Faktoren sowie den tatsächlichen Notwendigkeiten eines solchen Systemes abhängig.

2.6 RAID

RAID steht für *Redundand Array of Inexpensive Discs*. Gemeints ist damit ein Verbund mehrer Festplatten zu einem logischen Datenträger. Daraus können ein Geschwindigkeitszuwachs, Datensicherheit und Fehlertolleranz resultieren. Dagegen stehen hohe Anschaffungskosten und die verhältnismäßig teure Wartung.

2.6.1 Software versus Hardware

RAID-Systeme können entweder Hardwareseitig oder Softwareseitig implementiert sein. Folgendes sind die Merkmale von Hardware-RAIDs:

- Sie verfügen über einen eigenen Controller, was dem Rechner selbst eine Menge Arbeit abnimmt
- Der Controller verfügt über ein eigenes BIOS, welches die komplette Verwaltung des RAIDs übernimmt
- Sie präsentieren sich dem System als ein einziges Volume
- Platten lassen sich im laufenden System auswechseln
- Sie sind teuer

[8] Siehe [7], S. 14.

- Sie sind ausgesprochen schnell

Software-RAIDs sind günstiger; sie werden durch viele der modernen Betriebsysteme unterstützt. Hier wird die Funktionalität der Hardware durch Software simuliert. Folgendes sind die Merkmale:

- Durch den Simmulationsvorgang ist der Zugriff langsamer als bei einem Hardware-RAID
- Die Kosten für die Ansteuerungshardware entfallen. (Die Kosten für die Platten entfallen natürlich nicht!)
- Die tatsächlichen Funktionalitäten des RAIDs ist von der verwendeten Software abhängig

Windows 2000 verfügt durch die dynamischen Datenträger über Software-RAID-Level 0, 1 und 5, Linux kann durch entsprechende Kernelmodule die Level 0, 1, 4, 5 und das RAID-Linear-Verfahren unterstützen. Novell NetWare 5.0 unterstützt die Level 0, 1 und 5.[9]

2.6.2 RAID-Level

Prinzipiell werden bei RAID die Daten in Blöcke, sogenannte *Chunks*, geteilt. Die verschiedenen RAID-Level geben darüber Aufschluß, wie diese Chunks über die verschiedenen Platten verteilt werden.

Linear-RAID / Datenträgersatz: Ob dieses Verfahren überhaupt zum RAID gehört, sei einmal dahingestellt. Hier wird nichts gespiegelt, dupliziert oder aufgeteilt; der Datenträger kann sich aber über mehrere Platten erstrecken, und diesen können im laufenden Betrieb weitere Platten hinzugefügt werden. Windows NT nennt das *Datenträgersatz*, Windows 2000 *übergreifender Datenträger* und Linux *Linear-Raid*.

Level 0 — Striping: Bei dem sogenannten *Striping* werden die Chunks auf zwei Platten regelmäßig verteilt. Dadurch wird der Lese- und Schreib-Zugriff sehr schnell. Fällt eine der Platten aus, sind alle Daten hinüber.

Interessant ist in diesem Zusammenhang sicherlich eine Idee des Herstellers Compaq; selbiger verfolgt zur Zeit RAM-Striping, um den Zugriff auf den Arbeitsspeicher zu beschleunigen.

Level 1 — Spiegelung: Auch bei diesem Verfahren werden zwei Festplatten eingesetzt. Die zweite Platte enthällt jedoch ein exaktes Abbild der ersten. Dadurch wird eine hohe Ausfallsicherheit erreicht, es steht jedoch nur die Kapazität einer Platte zur Verfügung. (Die zweite enthällt ja das gleiche.) Es

[9] Jedenfalls sind das die Level, von denen der Verfasser definitiv weiß; möglicher Weise gehören auch 3 und 4 dazu, aber das ist nicht gesichert.

gibt in diesem Zusammenhang zwei Ansätze: Mirroring (zwei Platten an einem Controller) und Duplexing (zwei COntroller mit jeweils einer Platte). Letzteres ist schneller, da die beiden Controller parallel arbeiten können. Es wird jedoch im PC-Bereich nicht sonderlich häufig eingesetzt.

Level 0+1 und 1+0 oder 10: In beiden Fällen handelt es sich um Kombinationen der Level 0 und 1. Bei 0+1 werden Stripesets gespiegelt, bei 10 (oder 1+0) werden Spiegelungen in Stripes aufgeteilt.

Level 2 — Spiegelung mit Fehlerkorrektur: Dieser Level entspricht dem Level 1, er hat jedoch eine zusätzliche Fehlerkorrektur gegen Schreibfehler auf den Platten. Lohnend ist das Prinzip aber erst ab 10 Festplatten, obwohl es das einzige ist, welches gegen diese Art der Fehler gesichert ist.

Level 3 — Paritätsplatte: Bei diesem Verfahren wird eine dritte Platte benötigt. Wie beim Striping werden die Chunks auf verschiedene Platten verteilt. Auf der dritten Platte befinden sich Paritätsinformationen,[10] aus denen im Falle des Ausfalles einer Platte die restlichen Daten rekonstruiert werden können. Da bei jedem Zugriff auf das Paritätslaufwerk zugergiffen werden muß, eignet sich das Verfahren vor allem für große Datenmengen; bei kleinen kommt es durch diese Zugriffe zu empfindlichen Verzögerungen. Für dieses Verfahren sind mindestens drei Platten erforderlich.

Level 4: Der RAID-Level 4 unterscheidet sich nur in der Datenorganisation vom RAID-Level 3; durch diese andere Organisation ist dieses Verfahren auch bei kleinen Datenmengen effektiv. Es wird auf PCs eher selten eingesetzt, da es sich erst ab einer sehr hohen Plattenzahl (> 20) auszahlt.

Level 5 — Stripeset mit Parität: Auch bei diesem Prinzip wird mit einer Parität gearbeitet. Sie ist jedoch ebenfalls in Chunks geteilt und über die verschiedenen Platten verteilt. Hierdurch wird ein schnellerer Zugriff ermöglicht.

Level 6 und 7: Zu diesem Level gibt es bedauerlicher Weise noch keine Norm. Es gibt jedoch einige Ansätze, die von der Fragestellung *Was passiert beim gleichzeitigen Ausfall zweier Platten?* ausgehen. Die entsprechenden Firmen nennen das dann ebenfalls RAID 6 (oder manchmal 7). Zwei dieser Ansätzen sind der Gebrauch einer zusätzlichen Paritätsplatte und das Schreiben einer doppelten Parität.

2.7 Drucker

Eines der wichtigsten Peripheriegeräte ist der Drucker. Er dient dem Transfer von Daten auf Papier. Es gibt eine Reihe von verschiedenen Druckertypen. Sie werden

[10] Parität: Falls bei mehreren Werten einer wegfällt, läßt er sich durch die Parität mathematisch bestimmen. Im Falle der Werte 5 und 6 könnte es die Differenz, also 1, sein. Fällt die 5 weg, so ergibt es sich aus 6-Parität, fällt die 6 weg, so aus 5+Parität.

anhand ihrer Funktionstechnik, ihrer Ansteuerungssprache und ähnlicher Gesichtspunkte unterschieden. Ein weiteres Kriterium ist die Auflösung eines Druckers. Diese wird in DPI, *Dots per Inch* (Punkte pro Zoll) angegeben. Je höher die Auflösung ist, desto sauberer ist das Druckergebnis. In einigen Fällen unterschieden sich die Auflösungen der Vertikalen und der Horizontalen.

Hier soll zunächst auf die verschiedenen Techniken eingegangen werden. Die verbreitetsten Druckerarten sind Matrix-, Laser- und Tintenstrahldrucker. Als Unterart der Matrixdrucker gelten Plotter. Ebenfalls zu erwähnen sind Thermo- und Typenraddrucker.

Eine andere Unterscheidung ist die in Impact- und Non-Impact-Drucker. Als Impact- (also Aufschlags-) Drucker werden Geräte bezeichnet, bei denen tatsächlicher Kontakt mit dem Papier hergestellt wird. Non-Impact- (also aufschlagsfreie) Drucker sind alle anderen. Als Impact-Drucker werden Nadeldrucker bezeichnet, wärend Laser- und Tintenstrahldrucker der zweiten Kategorie zugeordnet werden.

Als letztes ist noch die Unterschiedung nach Art der Ansteuerung zu nennen. Wärend die meisten Tintenstrahl- und alle Matrix-Drucker jeweils die Daten Zeilwenweise, also so, wie sie gedruckt werden, bekommen, erhalten Laserdrucker ihre Druckaufgaben Seitenweise. Daher werden die ersteren auch als Zeilendrucker (oder *Lineprinter*), die letzteren als Seitendrucker (oder *Pageprinter*) bezeichnet.

2.7.1 Matrix- oder Nadeldrucker

Diese Drucker arbeiten mit einem Farbband, ähnlich einer Schreibmaschine. Anstelle von Typen werden jedoch Nadeln benutzt, die jeweils in der benötigten Form angeordnet und meistens mittels eines Magneten gegen das Farbband und das Papier gehämmert werden. Bekannte Nadelmengen sind 9, 16 und 24.

Heutzutage werden Nadeldrucker zunehmend seltener eingesetzt; insbesondere die beträchtliche Lärmentwicklung trägt dazu bei, daß sie zunehmend von Tintenstrahl- und Laserdruckern verdrängt werden. Hinzu kommt die mit anderen Druckern verglichen geringe Qualität.[11] Ihr Vorteil liegt darin, daß sie Durchschläge produzieren können. In einigen Rechenzentren werden sie benutzt, um Logs auszudrucken; hier zahlt sich ihre Fähigkeit, Endlospapier zu benutzen, aus.

Eine Sonderform der Nadeldrucker sind die Plotter. Sie verfügen über eine einzige Nadel, mit der sich sehr detailierte Grafiken anfertigen lassen. Plotter werden oft für CAD und Leiterplattendesign verwendet. Für die Umsetzung dieser Zeichnungen kommen Schneidplotter zum Einsatz. Bei diesen wurde die Nadel durch eine Klinge ersetzt.

2.7.2 Tintentsrahldrucker

Tintenstrahldrucker erfreuen sich wachsender Beliebtheit; sie sind leiser als Nadeldrucker, billiger als Laser und bieten einen sauberen Ausdruck.

[11] Es gibt zwar Nadeldrucker mit Auflösungen jenseits der 240 dpi, aber die sind eher selten und für Spezialanwendungen gedacht.

Um die Farbe aus den Patronen auf das Papier zu bringen gibt es grundsätzlich zwei Techniken:[12]

Bubblejet: Bei dieser Technik wird die Farbe in Farbkanäle geleitet. Diese Kanäle verfügen über erwärmbare Außenwände. Durch die Erwärmung bildet die Farbe blasen und dehnt sich damit aus. Als Folge wird sie durch die Düsen auf das Papier gespritzt.

Piezzo: Hier kommen Druckkammern zum Einsatz, deren Rückwand durch ein Piezzo-Elemet gebildet werden. Diese Elemente wölben sich je nach angelegter Spannung nach Außen oder Innen. Werden sie nach Außen gewölbt entsteht ein Unterdruck und Farbe wird aus der Patrone eingesogen. Bei Wölbung nach Innen wird der Raum verringert und die Farbe durch die Druckdüse auf das Papier gespritzt.

In beiden Fällen muß die Tinte bestimmte Voraussetzungen erfüllen. Sie muß Dünnflüssig sein, darf aber nicht verschmieren. Sie muß schnell trocknen, darf aber nicht in den Farbkanälen des Druckkopfes eintrocknen. Im Falle der Bubblejet-Technik muß sie sich schnell erwäremn lassen und über eine hohe Ausdehnung verfügen. (Und schnell abkühlen muß sie auch.)

Tortzdem sich die Druckerhersteller Mühe geben, ihre Tinte entsprechend zu fabrizieren, kommt es doch vor, daß Druckköpfe verkleben. Einige Hersteller sind deshalb soweit gegangen, die Druckköpfe in ihren Farbpatronen zu inegrieren. Dadurch werden sie regelmäßig erneuert. Der Nachteil ligt in den entsprechend hohen Preisen. In anderen Fällen hilft ein einfaches Wasserbad des Druckkopfes, um die verstopften Düsen wieder frei zu bekommen.

2.7.3 Laserdrucker

Laserdrucker sind schnell und liefern saubere Ausdrucke. Ihre Funktionsweise ist ein wenig komplizierter und wird hier nicht in allen Einzelheiten diskutiert.

Grundsätzlich wird mit negativ geladenem Toner gearbeitet. Über ein Rad, den sogenannten *Developer Roller*, wird er aus dem *Toner Hopper* (das ist der Ort, wo er liegt) auf eine Trommel, die sogenannte *Photoreceptor Drum Assembly*, aufgetragen. Die Oberfläche dieser Trommel ist ebenfalls negativ geladen. Über die aus einem Laser und einem Spiegel bestehende *Laser Scaning Unit* wird diese Ladung jedoch an den Stellen, an denen Toner auf das Papier übertragen werden soll, neutralisiert. An diesen Stellen bleibt Toner haften, an allen anderen wird er, da er ebenfalls negativ geladen ist, abgestoßen.

Über die Trommel gelangt der Toner auf das Papier. Dieses läuft zwischen Trommel und einer positiv geladenen Koroner-Schicht durch. Dadurch wird der Toner (der ja immer noch negativ geladen ist) auf das Papier übertragen. Es durchläuft zwei heiße Walzen, die sogenannten *Fuser*, die den harzhaltigen Toner in

[12] Es kann gut sein, daß es noch mehr gibt; die anderen werden jedoch kaum eingesetzt. Zumindest sind sie dem Verfasser nicht bekannt.

das Papier einbrennen. (Das ist der Grund warum sich manche Etiketten und viele Folien nicht mit Laserdruckern bedrucken lassen; die bleiben dann in den Fusern hängen. . .) Die neutralisierten Stellen der Trommel laufen dann an einer sehr hellen Lampe, der sogenannten *Discharge Lamp*, vorbei. Das führt zu einer Neutralisierung, sprich, die Stellen werden wieder nenagtiv geladen.

Die Auflösung eines solchen Druckers kann sehr hoch sein. 300 dpi sind oft das Minimum, doch selbst billige Drucker gibt es inzwischen mit 600 dpi und mehr.

2.7.4 Typenrad und Thermodrucker

Typenraddrucker arbeiten nach dem selben Prinzip wie Typenradschreibmaschinen. Ein Typenrad drückt ein Zeichen gegen ein Farbband. Sie sind nicht leiser als Nadeldrucker und haben mehr Durchschlagskraft.

Thermodrucker arbeiten nur mit speziellen Papier zusammen. Durch Erwärmung der entsprechenden Stellen wird das Bild zu Papier gebracht. Eingesetzt werden sie vor allem in Faxgeräten und Kassen.

2.7.5 Lokaler Anschluß

Drucker können auf verschiedene Weise mit einem Rechner verbunden werden. Die einfachste Methode ist der direkte Anschluß an einen Rechner. Dazu werden für gewöhnlich die Parallele oder die USB-Schnittstelle benutzt. Sehr selten kommen alternativen wie Infrarot oder Bluetooth zum Einsatz. In einigen Fällen werden Drucker auch über die serielle Schnittstelle betrieben. (Dies ist jedoch wegen der geringen Geschwindigkeit meistens nur bei Spezialdruckern der Fall; in der Vergangenheit gab es unter Anderem von der Firma Apple einen Drucker, der über die serielle Schnittstelle zu betreiben war. Jeder, der schon einmal ein größeres Dokument über so einen Drucker ausgedruckt hat, weiß, warum diese Lösung recht schnell von der parallelen Schnittstelle verdrängt wurde.)

2.7.6 Der Anschluß über Netzwerk

Wesendlich interessanter ist der Anschluß über Netzwerk. Hier ist es für die Benutzer verschiedener Rechner möglich, auf einem Drucker auszudrucken, ohne daß dieser bei ihnen stehen muß. Um einen Drucker ins Netz zu bekommen gibt es verschiedene Methoden:

Anschluß an einen Computer: Der Drucker kann an einen dafür vorgesehenen Rechner angeschlossen und dann im Netz freigegeben werden. Dies bietet eine ganze Reihe von Sicherheitsmechnismmen und naturgemäß auch diverse Möglichkeiten, den Druck selbst zu verwalten. Hierfür muß der entsprechende Rechner aber immer laufen.

Anschluß an einen Druckerserver: Druckerserver (auch *Printerserver*) sind keine vollständigen Computer. Der Ausdruck bezeichnet eine kleine Box mit ein bis drei Druckeranschlüssen und einem Netzwerkanschluß. Er läßt sich meistens mittels `telnet` oder einem herstellereigenen Programm einrichten. Das wichtigste Merkmal dabei ist, daß der Server eine IP-Adresse[13] bereit stellt. Je nach Ausstattung können auch bei diesen Servern Verwaltungsfunktionen ausgeführt werden. Sie sind natürlich weit wesendlich ausführlich als die eines „echten“ PCs.

Printerboxes: Hierbei handelt es sich um sehr kleine Steckteile, die auf den Anschluß des Druckers gesteckt werden und auf der anderen Seite einen AnschlUß für ein Netzwerk haben. Sie ähneln den Printerservern, verfügen aber über keinen eigenen Speicher und keine Konfigurationsmöglichkeiten. Ihre IP-Adresse wird für gewöhnlich mittels Dip-Schaltern eingestellt.

Netzwerkkarten: Einige Druckerhersteller stellen für ihre Modelle Netzwerkkarten her. Sie verfügen meistens über die Funktionalität eines Printerservers. HP's PrintJet-Technologie ist ein gutes Beispiel dafür.

Dedizierter Printserver: , Damit ist ein Rechner gemeint, der die Druckaufträge verwaltet. Die Drucker selbst können auf die oben beschriebenen Weisen angeschlossen sein und müssen nicht direkt an dem Rechner hängen. Der Vorteil dieses Systemes liegt darin, daß sich die Druckeraufträge, Berechtigungen und was da sonst noch anfällt zentral verwalten lassen. Bei vielen Systemen läßt sich darüber hinaus auch der Druckertreiber auf dem Rechner hinterlegen.

2.7.7 Ansteuerung von Druckern

Für gewöhnlich wird die Ansteuerung eines Druckers über einen Treiber erledigt. Für gewöhnlich übersetzt dieser die zu druckenden Dokuemnte in eine dem Drucker verständliche Sprache. Die Sprache kann von Hersteller zu HErsteller variieren. Einige Verfahren haben sich jedoch inzwischen als besonders Verbreitet durchgesetzt.

GDI: GDI steht für *Graphic Device Interface*. Bei diesem verfahren kann der Drucker von sich aus nichts; um die Dokumente tatsächlich zu Papier zu bringen, wird der Grafikspeicher von Windows benutzt. Diese Geräte funktionieren nur unter Windows.[14] Grundsätzlich ist von diesen Druckern abzuraten, auch wenn sie meistens zeimlich billig sind.

PostScript: Die Druckersprache PostScript wurde von Adobe entwickelt. Diese Sprache ist eher mathematisch und beschreibt Zeichen anhand von Parametern wie Federstärke, Aufdruck und ähnliches. Falls bei einem Drucker PostScript hardwaremäßig unterstützt wird, ist er im Ausdruck dieser Sachen

[13] Oder etwas ähnliches; es gibt zum Beispiel einen Printerserver der Firma TRUST, der nur mit IPX und im Zusammenhang mit Novell Netware läuft.

[14] Inzwischen gibt es auch Lösungen, die den Druck unter Linux realisieren.

ausgesprochen schnell und sauber.[15] Eine Weiterentwicklung von PostScript ist übrigens PDF.

HPGL und PCL: Wie der Name schon vermuten läßt ist dieses die Haussprache von HP. Sie ist Vektororientiert.

Wärend GDI und HPGL auch für Tintenstrahldrucker zum Einsatz kommen, ist PostScript vor allem bei Laserdruckern anzutreffen.[16] Sowohl zu HPGL als auch zu PostScript ließe sich noch sehr viel mehr sagen, es ist jedoch unwahrscheinlich, daß das zu den Grundlagen gehört.

2.7.8 Farbdrucker

Besonders seid der zunehmenden Beliebtheit von Tintenstrahldruckern ist auch der Farbdruck eine erschwingliche Sache geworden. Er ist für alle der drei genannten Hauptgruppen möglich.

Matrixdrucker: Bei diesen Druckern wird der Farbdruck über Farbbänder realisiert. Meistens ist die Qualität der Bilder nicht sonderlich hoch.

Tintenstrahldrucker: Hier werden entweder drei oder vier[17] Farbpatronen kombiniert. Bei drei Patronen wird Schwarz durch eine Kombination der anderen (Cyan, Magenta und Gelb) erzeugt, bei der anderen Variante ist eine Schwarztpatrone mit dabei. Oftmals sind die Farben auch in einer Patrone mit verschiedenen Farbkammern zusammengefaßt.

Das Verfahren mit vier Farben wird oftmals als CMYK-Verfahren (für ***C****yan*, ***M****agenta*, ***Y****ellow* und *Blac**K***) bezeichnet.

Durch die Verwendung verschiedener Patronen ist es nach dem Einsetzen neuer Patronen oftmals notwendig, eine Kalibrierung der Druckköpfe, also eine genaue Abstimmung der beiden Köpfe aufeinander durchzuführen. In vielen Fällen geschieht dies durch das Drucken einer Grafik und Auswahl des besten Ergebnisses.

Laserdrucker: Auch bei Laserdruckern wird der Farbdruck durch eine Kombination verschiedener Farben (meistens ebenfalls CMYK) erreicht. In diesem Fall kommt verschiedener, nacheinander aufgebrachter Toner zum Einsatz.

[15] Falls ein Dokument als PostScript vorliegt, ist es in diesem Fall sogar möglich, es *ohne Treiber* auszudrucken; die Datei wird einfach an die Schnittstelle geleitet, an der der Drucker hängt. Er kümmert sich schon um den Rest!

[16] Tatsächlich kennt der Verfasser nur einen einzigen Tintenstrahldrucker, den HP CM 1700, der PostScript beherrscht.

[17] Bei einigen Druckern mit Sonderfunktionen wie metallischem Druck sind es auch mehr.

Kapitel 3

TCP/IP

Dieses Kapitel entstand als unterrichtsbegleitendes Material zum Thema TCP/IP. Es deckt in Abschnitt 3.1 das ISO/OSI-Schichtenmodell, in Abschnitt 3.2 das DoD-Modell ab, geht in den Abschnitten 3.3 und 3.4 auf IP-Adressen, Subnetze und die damit eng verwandten Router und Switche ein, gibt in Abschnitt 3.5 einen Überblick über Ports, Sockets und Protokolle und schließt in den Abschnitten 3.6 und 3.7 mit Betrachtungen von DHCP und Namensauflösungsmethoden (DNS und WINS) ab.

Neben dem Unterricht wurden einige Dinge aus einem älteren Skript, welches der Vorbereitung zum CCNA diente, entnommen. Dieses Skript basierte vor allem auf dem Buch *Interconnecting Cisco Network Devices* von STEVE MCQUERRY [9]. Andere Quellen waren CRAIG HUNTS Klassiker *TCP/IP Network Adminsitration* [5], der `RFC2131` [1] und der Microsoft MOC Kurs 2046A [12].

„God hates us all!“

SLAYER: *Disciple*

3.1 Das ISO/OSI-Schichtenmodell

Das ISO/OSI-Schichtenmodellwurde festgelegt, um die Kommunikationsvorgänge innerhalb eines Netzwerkes zu abstrahieren. Das ist vor allem für Entwickler und Programmierer interessant, die sich bei der Implementierung von Netzwerkanwendungen auf ihre Schicht konzentrieren können und die restlichen lediglich in Form von wohldefinierten Schnittstellen zu Gesicht bekommen. Weiter ist es für Netzwerktechniker interessant, die so die Quellen und Ursachen von Fehlern lokalisieren und beheben können. Für die meisten Aufgaben sind die unteren drei Ebenen interessant. Das Ebenen-Modell findet sich in Abbildung 3.1, S. 24.

3.1.1 Schicht 1: Physikalische Schicht / Physical Layer

In dieser Schicht finden sich Kabel, Stecker... sie ist für die rein physikalische Verbindung zuständig. Bekannte Geräte dieser Schicht sind HUBs und Repeater.

7. Anwendungsschicht	Anwendungen und bereitgestellte Dienste, etwa telnet, FTP, HTTP, SMTP, POP3	Application Layer
6. Darstellungsschicht	Übersetzung von Datenformaten, etwa AVI, GIF, MPEG, midi, ASCII, JPEG	Presentation Layer
5. Sitzungsschicht	Aushandeln von Verbindungen (Sitzungen), etwa SQL, NetBIOS, RPC, NFS	Session Layer
4. Transportschicht	Fehlerkorrektur und Übermittlung, etwa via TCP, UDP oder SPX	Transport Layer
3. Netzwerkschicht	Logische Adressen, etwa IP oder IPX	Network Layer
2. Verbindungsschicht	Physikalische Adressen, also MAC/BIA	Data Link Layer
1. Physikalische Schicht	Der Datenstrohm (Roh-Bits), Kabel Stecker, Übertragungssignale …00110000111110001010001011001…	Physikal Layer

Abbildung 3.1: Das ISO/OSI-Referenz-Modell

Repeater: Falls Daten über große Entfernungen übertragen werden sollen, ist es nötig, ein Gerät zur Auffrischung der Signale zu verwenden.

HUB: Ein Hub (deutsch: Nabe) ist nichts weiter als ein Verteiler. Hier wird das Signal von einem Kabel auf mehrere andere verteilt.

Repeater sind heutzutage Obsolet.

3.1.2 Schicht 2: Verbindungsschicht / Data Link Layer

Diese Schicht[1] ist nochmals unterteilt. Den „oberen“ Teil bildet die LLC-, den unteren die MAC-Schicht. Diese Schicht ist es, die für das *Collision Handling* zuständig ist. Typische Geräte, die hierauf aufsetzen, sind Bridges und Switches.

Die MAC-Schicht: In dieser Schicht werden die MAC-Adressen ausgelesen und ausgewertet. Eine MAC-Adresse besteht aus sechs Byte (also 48 Bit), von denen die ersten drei den Hersteller, die letzten drei das Produkt kennzeichnen.[2] Bei Cisco heißen diese Adressen auch BIA, *Burned In Adress*.

Außerdem werden die Daten in sogenannte Datenrahmen (Dataframes) verpackt. Ein solcher Frame besteht aus Preambel, Ziel-Zusatz, Quellzusatz, Länge, den Daten ansich und dem sogenannten Trailer oder FCS.

Die LLC-Schicht: Das einzig interessante an dieser Schicht ist, daß es hier SAP-Rahmen und Snap-Rahmen gibt.[3]

[1] Sie wird im Deutschen manchmal auch als *Sicherungsschicht* bezeichnet.

[2] Unter besonderen Umständen können diese auch überschrieben werden, etwa, wenn für bestimmte Aufgaben bestimmte MAC-Adressen erforderlich sind. Die *originale* MAC-Adresse wird jedoch stets mitgeliefert so daß von einem „echten“ Überschreiben nicht gesprochen werden kann.

[3] Hm… der Verfasser gibt zu, daß ihm diese Tatsache in einem anderen Zusammenhang als Fehlersuche bei Cisco-Routern auf Anhieb auch nicht sonderlich interessant vorkommt.

CSMA/CD: Diese Abkürzung steht für *Carrier Sense Multible Access / Collision Detect*. Wenn alle Rechner an einem Medium hängen, kommt es vor, daß mehr als ein Rechner zur Zeit darauf zugreifen wollen. Dann kommt es zu einer sogenannten Datenkollision. Sobald das bemerkt wird, sendet die Netzwerkkarte, der das aufgefallen ist, ein *jam*-Signal. Danach verfallen alle Netzwerkkarten für eine bestimmte Weile in Tiefschlaf. Danach wird der Betrieb normal aufgenommen.

Besonders „beliebt" sind in diesem Zusammenhang sogenannte *jabbernde* Netzwerkkarten. Diese senden wilkürlich Datenpakete, ohne auf das Medium zu hören. Da sie das aber nicht ständig tun, sind sie sehr schwer zu finden. Dadurch wird das Netz recht einfach eingefroren...

CSMA/CA: Das *Carrier Sense Multible Access / Collision Avoid* Verfahren wurde von Apple entwickelt. Bevor ein Rechner senden will, lauscht er zunächst, ob das Netz überhaupt frei ist.

Bridges: Befinden sich viele Rechner an einem Medium (also einem Kabel oder einem Hub), so stören sie sich bei auftretenden Netzwerk-Kollisionen. Alle sich gegenseitig störenden Geräte bilden eine sogenannte *Collision Domain* oder Kollsionsdomäne. Bei ansteigender Zahl der Geräte wird die Anzahl der auftretenden Kollisionen logischer Weise ebenfalls ansteigen, was den Datendurchsatz sänkt. Um dem entgegen zu wirken, werden die Collision Domains mit Hilfe von Bridges segmentiert.

Eine Bridge verfügt über zwei oder mehr Anschlüsse und eine Tabelle, die besagt, welche MAC-Adressen sich an welchem Anschluß befinden. Anforderungen, die innerhalb eine Segmentes geschehen, werden nicht an die anderen Anschlüsse weitergeleitet. Unbekannte Adressen werden auf alle Anschlüsse verteilt (sogenanntes *fluten*), ausgenommen des Segmentes, aus dem die Anforderung kommt. Das selbe gilt für Broadcast-Anforderungen (siehe 3.3.3, S. 31).

Durch die softwaretechnische implementation des Verbindungsaufbaus ist das Verfahren recht langsm. Aus diesem Grund werden Bridges heutzutage nicht mehr (oder nur sehr selten) eingesetzt.

Switches: Die logische Weiterentwicklung der Bridge ist der Switch. Hier werden bei Anforderung zwischen zwei Anschlüssen sogenannte *exklusive Verbindungen* erstellt. Dieser Verbindungsaufbau ist hardwaretechnisch über sogenannte *ASICs* (*Application Specific Integrated Circuits*) realisiert worden. Dadurch ist der Switch wesendlich schneller als die altertümliche Bridge. Die Anzahl der gleichzeitig möglichen exklusiven Verbindungen wird durch die Größe des internen Busses, auch *Backplane* genannt, bestimmt.

Falls ein betrunkener Admin auf den Gedanken kommt, zwei Switches wegen der Fehlertolleranz mittels zweier Kabel zu verbinden, so bekommt er spätestens bei der ersten Broadcast-Anfrage eine nette, kleine Schleife[4]...

3.1.3 Schicht 3: ISO/OSI!Schicht / Network Layer

Diese Schicht arbeitet erstmalig mit logischen Adressen, in unserem Fall mit IP-Adressen. Die typischen Geräte dieser Schicht sind Router.

IP-Adressen: IP-Adressen bestehen aus 32 Bit. Da Menschen leichte Probleme damit haben, dermaßen große Folgen von Nullen und Einsen im Kopf zu behalten, werden diese Folgen meistens in Zahlen umgewandelt und, da Zahlen ab einer bestimmten Größe ebenfalls sehr unhandlich sind, in vier Segmente zu jeweils 8 Bit oder einem Byte unterteilt. Jedes Byte wird für sich genommen in eine Dezimalzahl umgewandelt. (Zum Beispiel entspricht `192.168.1.8` der Bbinärzahl 11000000101010000000000100001000.) Die IP-Adresse besteht aus einem Netz-Teil, der das Netz bezeichnet, in dem sich der entsprechende Rechner befindet, und einen Rchner- oder Host-Teil, der den Rechner innerhalb des Netzes anzeigt.

Die Subnetmaske: Spätestens beim Routing (siehe zur Erklärung den hier drunter stehenden Punkt *Router* wird es nötig, den Host-Anteil der IP-Adresse vom Netz-Anteil zu trennen. Zu diesem Zweck wird eine ebenfalls 32 Bit lange Netzmaske definiet, die aus einem aus zusammenhängenden Einsen und einem aus zusammenhängenden Nullen gebildeten Block besteht. Der erstgenannte Block muß am zu Anfang stehen und deckt den Netz-Teil ab, die Nullen definieren den Host-Teil.

Router: Ein Router beinhaltet vor allem eine sogenannte *Routing-Table*. In dieser finden sich für jedes durch den Router ansprechbare Netz oder Teilnetz die Adresse, die Subnez-Maske, das zuständige Gateway und die dafür zuständige Schnittstelle. Anhand dieser Tabelle werden ankommende Pakete aufgrund ihrer Ziel-Adresse an die entsprechenden Subnetze weitervermittelt.

Router lassen keine Broadcasts (siehe 3.3.3, S. 31) durch, und das ist gut so; sonst könnte sich das Internet vor broadcasts nicht mehr retten. Ein Segment, welches durch einen roadcast erreicht werden kann, wird auch als *Broadcast Domain* bezeichnet.

Es soll nicht verschwiegen werden, daß einige Router auch auf höheren Schichten einsetzen, etwa, wenn sie auch auf Ports routen.

Die Themen IP-Adressen und Subnez-Makse werden an späterer Stelle noch ausführlicher beluchtet (siehe 3.3, S. 28).

[4]Cisco hat, um solches zu Verhindern, das *Spanning Tree Protocol* (STP) entwickelt. Ob nun, um besser Maschennetze aufbauen zu können, oder, weil Cisco-Admins so viel saufen, sei einmal dahingestellt.

3.1.4 Die Schichten 4 – 7

Da diese Schichten nicht wirklich von Interesse sind[5] werden sie hier unter diesem Punkt zusammengefaßt:

Schicht 4: Transportschicht / Transport Layer: Diese Schicht ist unter Anderem für die Fehlerkorrektur und die Übermittlung von Daten via TCP, UDP oder IPX zuständig.

Schicht 5: Sitzungsschicht / Session Layer: In dieser Schicht wird eine Verbindung oder *Sitzung* ausgehandelt. NFS, SQL-Sessions und ähnliches werden von dieser Schicht geregelt.

Schicht 6: Darstellungsschicht / Presentation Layer: Innerhalb dieser Schicht werden verschiedene Datenformate ineinander überführt. Unter diese Daten fallen AVI, GIF, MPEG (also auch MP3), Midi, ASCII und JPEG-Daten.

Schicht 7: Anwendungsschicht / Application Layer: Diese Schicht beinhaltet Anwendungen und Dienste, die Anwendungen zu Verfügung gestellt werden, etwa `telnet`, `ftp`, HTTP, SMTP oder POP3.

3.2 Das DoD-Modell

TCP/IP wurde ursprünglich von der *Defence Advanced Research Project Agency)* (*DARPA*), einer Unterabteilung des *Department of Defence* (*DoD*), entwickelt. Das zugrundeliegende Modell wird daher auch als *DoD-Modell* bezeichnet. Im Gegensatz zum ISO/OSI-Modell hat es nur vier Schichten. Abbildung 3.2, S. 28 zeigt einen Vergleich der beiden Modelle. Hierzu ist jedoch zu bemerken, daß es verschiedene Auslegungen gibt. In eingen Fällen sind Teile der dritten OSI-Schicht in der ersten DoD-Schicht enthalten, in anderen nicht. Bei dieser Gegenüberstellung wurden zudem komplette Schichten behandelt, keine Teilschichten.

Die einzelnen DoD-Schichten werden hier nochmals kurz beschrieben:

Schicht 1, Zugangsschicht / Network Access Layer: Diese Schicht beschäftigt sich mit dem physikalischen Zugang und dem Umgang mit MAC-Adressen. Es enthällt das ARP-Protokoll, welches IP-Adressen in MAC-Adressen umwandelt. (Daher wird dieser Schicht manchmal ein Teil der dritten OSI-Schicht zugesprochen.)

Schicht 2, Internetschicht / Internet Layer: Diese Schicht stellt das Kernstück des gesammten Modelles, es beinhaltet das Protokoll IP. Daneben enthällt es auch das zur IP-Suite gehörige ICMP-Protokoll. Dieses ist für ehler- und Rückmeldungen des TCP-Protokolles nötig.

[5]Nun... sie *waren* es jedenfalls nicht für Cisco...

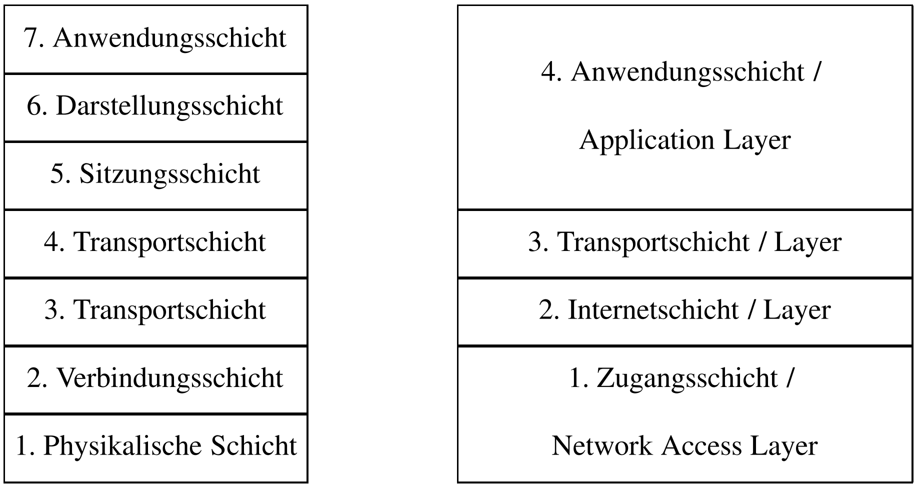


Abbildung 3.2: Eine Gegenüberstellung des ISO/OSI und des DoD-Modells

Schicht 3, Transportschicht / Transport Layer: Diese Schicht ist für den Verbindungsaufbau zuständig und beinhaltet das TCP-Protokoll.

Schicht 4, Anwendungsschicht / Application Layer: In der letzten Schicht liegt alles, was noch fehlt.

Es ließe sich noch mehr dazu sagen, etwa, welche unterschiedlichen Bezeicnungen die Datenpakete in den einzelnen Schichten haben, oder welche Protokolle es sonst noch gibt. Aber dies ist zum einen nicht wirklich notwendig (jedenfalls noch nicht) und wird zum anderen vermutlich kaum jemanden interessieren.

3.3 Adressklassen und Subnetting

Wie in Kapitel 3.1.3, S. 26 gesagt wurde, wird das gesamte Netz in verschiedene Klassen unterteilt. Nur wie bekommt ein Rechner nun den Netzteil und den Rechnerteil auseinandersortiert?

3.3.1 Grundlagen

Eine IP-Adresse setzt sich, wie bereits in 3.1.3, S. 26 gesagt wurde, aus der Adresse und der Netzwerkmaske (oder Subnetmask) zusammen. Um zu verstehen, welchen Sinn diese Maske hat, muß zunächst betrachtet werden, was sie eigentlich tut.

Hierzu ist es zunächst erforderlich, sich zu erinnern, daß ein Computer (oder Router oder sonst ein Gerät aus dieser Richtung) nur mit 0 und 1 arbeitet. Eine der Funktionen, die er exzellent beherrscht, ist die *AND*-Funktion. Sie vergleicht zwei Werte und liefert je nach Ergebnis ebenfalls eine 0 oder eine 1 zurück. In Tabelle 3.1, S. 29 findet sich eine Übersicht über die Ergebnisse.

Wert 1	**Wert 2**	**Ergebis**
0	0	0
0	1	0
1	0	0
1	1	1

Tabelle 3.1: Ergebnisse der AND-Operation

IP-Adresse:	192	168	12	14
Binär:	`11000000`	`10101000`	`00001100`	`00001110`
Subnet-Maske:	255	255	255	0
Binär:	`11111111`	`11111111`	`11111111`	`00000000`
Netzwerk:	`11000000`	`10101000`	`00001100`	`00000000`
Dezimal:	192	168	12	0

Tabelle 3.2: Bestimmung der Netzwerkadresse

Sowohl die Adresse als auch die Subnetmask müssen zunächst in das binäre System übertragen werden.[6]

Die erste Aktion eines eines Routers (oder sonstigen Empfängers) besteht in einer AND-Verknüpfung zwischen der Netzwerkmaske und der IP-Adresse. Übrig bleibt danach die Netzwerkadresse. Dargestellt ist eine solche Rechnung in Tabelle 3.2, S. 29. Dieses wird sowohl für die Sender- als auch für die Empfänger-Adresse getan. Falls eine weitere AND-Funktion (diesesmal zwischen den beiden Netzadressen) etwas anderes als 0 ergibt, ist klar, daß sich die Empfänger in unterschiedlichen Netzen befinden.

Sobald das Paket das Netz erreicht hat, für das es bestimmt ist, wird eine AND-Funktion auf die IP-Adresse und die invertierte[7] Subnetmaske ausgeführt. Das Ergebnis ist der anzusprechende Rechner und kann nun zugestellt werden.

3.3.2 Adressklassen

Um die Arbeit mit den Adressen etwas übersichtlicher zu gestallten, wurden die vorhandenen Adressen in mehrere Adress-Bereiche unterteilt. Der erste beinhaltet Klasse A-Netze. Dabei werden die ersten 8 Bit der Adresse für die Netzwerk-, die restlichen 24 für die Hostadressierung benutzt. Intern werden sie daran erkannt, daß das erste Segment binär mit der einer `0` beginnt. Der zweite Bereich, die Klasse B Netze, verwenden jeweils 16 Bit für Netz- und Host-Adressierung. Intern werden sie daran erkannt, daß das erste Segment binär mit `10` beginnt. Der letzte in diesem Zusammenhang verwendete Bereich sind die Klasse C Netze, in denen 24 Bit für die Netz- und 8 Bit für die Host-Adressierung dienen. Daneben gibt esnoch die

[6] Eine Möglichkeit, dies zu tun, findet sich in Anhang C.1.1, S. 105.

[7] invertiert heißt in diesem Falle: 0=1, 1=0

Klasse	Bereich			Privater Bereich		
A	1	–	126	10.0.0.0	–	10.255.255.255
B	128	–	191	172.16.0.0	–	172.31.255.255
C	192	–	224	192.168.0.0	–	192.168.255.255

Tabelle 3.3: Die IP-Adress-Klassen

Klasse D und die Klasse E Netze, erstere für Multicasts (siehe 3.3.3, S. 31), letztere für experimentelle Zwecke.

Da der Bedarf an an Adressen Weltweit um einiges größer ist, als durch die vorhandenen Adressen abgedeckt werden kann, werden innerhalb einzelner Netze *private*, nur für den internen Gebrauch gedachte IP-Adressen vergeben. Diese gelten nur innerhalb des entsprechenden Netzes. Falls aus irgend einem Grund ein Router im Internet eine Anfrage eines solchen, internen Rechners bekommt, und diese zufällig irgend einer offiziellen Adresse gleichen sollte, gäbe das Probleme. AUs diesem Grund wurden in jeder der drei Netzklassen ein Bereich mit *privaten* Netzwerkadressen definiert. Diese sind ausschließlich für den internen Gebrauch bestimmt. Internetrouter beantworten keine Anfragen privater IPs und leiten sie auch nicht weiter.

Tabelle 3.3, S. 30 listet die drei für den normalen Gebrauch gedachten IP-Adress-Klassen und ihre privaten Bereiche auf. Der im Klasse A Netz enthaltene Loopbackbereich (siehe 3.3.3, S. 30) wurde ausgelassen.[8] Bei den Klassenbereichen wurde nur das erste Oktet angegeben.

3.3.3 Besondere Adressen

Einige Adressen innerhalb von TCP/IP können nicht einfach verwendet werden. Besonders wichtig sind dabei die Netzadressen ansich, die Broadcasts, die Multicasts und die Loopback-Adresse.

Loopback: Diese Adresse lautet `127.0.0.1` und dient dem generellen Test des auf einem Rechner installierten TCP/IP-Protokolles. Falls es möglich ist, diese Adresse anzupingen (also eine positive Antwort auf den Befehl `ping 127.0.0.1` kommt), ist zumindest das Protokoll korrekt installiert und arbeitsbereit. Das sagt nichts über den Status der Netzwerkkarten aus.

Netzadressen: Jedes Netzwerk verfügt über eine eigene Adresse. Dies ist die erste des Netzes. In einem normalen, klassenorientierten Netzwerk hat sie also den selben Netzwerkteil wie die restlichen Rechner des Netzes, endet aber an allen anderen Stellen auf `0`. (Das Netzwerk eines Rechners `192.168.1.7` mit der Netzwerkmaske `255.255.255.0` lautet also `192.168.1.0`) *In klassenlosen Netzen muß sie nicht zwangsläufig auf `0` enden!*

[8] Netzwerke und Broadcast-Adressen sind noch dabei.

Netz:	114	13	0	0
Subnet-Maske:	255	255	255	0
Binär:	`11111111`	`11111111`	`00000000`	`00000000`
Neue Maske:	`11111111`	`11111111`	`11100000`	`00000000`
Dezimal:	255	255	224	0

Tabelle 3.4: Klassenlose Netzwerkmaske

Broadcast: Bei dieser Adresse handelt es sich um die letzte Adresse eines Netzwerkes. Ein Signal an diese Adresse geht an alle in diesem Netz befindlichen Rechner. Sie werden meistens nur von Systemdiensten benutzt. Die Adresse ist die letzte im Netz verfügbare. In einem klassenorientierten Netz hat sie also meistens den selben Netzteil wie die restlichen Rechner, endet aber auf 255. (Die Broadcastadresse eines Rechners `192.168.1.7` mit der Subnetmask `255.255.255.0` lautet also `192.168.1.255`). *In klassenlosen Netzen muß sie nicht unbedingt auf `255` enden!*

Multicast: Multicastadressen befinden sich in der Netzwerkklasse D. Wird ein Paket an eine Multicast-Adresse gesendet, wird sie an alle für diese Adresse eingetragenen Personen weitergeleitet.

3.3.4 Klassenlose Netze

In manchen Beziehungen sind die vorkommenden Klassen sehr unzufrieden stellend. Angenommen, ein Betreiber ist im Besitz eines kompletten Klasse B Netzes. Dann könnte aus organisatorischen Gründen der Wunsch aufkommen, dieses Netz nochmals in kleinere Netze zu unterteilen. Doch wie? Eine Möglichkeit besteht in der Anschaffung teurer Cisco-Geräte, mit deren Hilfe sich VLANs einrichten lassen. Eine weitere bestände darin, das dritte Segment ebenfalls als Subnet-Maske zu benutzen. Dieses hätte eine Teilung in 256 Netze zu jeweils 256 Adressen zur Folge. Das ist aber nicht immer der gewünschte Effekt.

Die dritte Möglichkeit besteht in der Unterteilung in Netze außerhalb der vorgegebenen Klassen. Die Subnetmask ist eine zusammenhängende Folge von Einsen, sie braucht nicht unbedingt auf 8, 16, 24 oder 32 Bits beschränkt zu sein.

Gesetzt den Fall, die Firma benötige insgesammt 5 Netze. Dann ist als erstes zu überlegen, wie viele zusätzliche Bit sie benötigt, um diese Einteilung vorzunehmen. Hierbei ist weiter zu beachten, daß viele Router nicht in der Lage sind, das jeweils erste und letzte Netz einer Reihe von Subnetzen zu verbinden.

Unter dieser Berücksichtigung sind es $5 + 2 = 7$ Netze. Damit benötigt die Firma mindestens drei Stellen, da mit zwei Stellen lediglich 4 , mit vieren jedoch 16 angesprochen werden könnten.

Gesetzt den Fall, das Netz der Firma ist `114.13.0.0`/16 (also mit einer Subnetmask von `255.255.0.0`). Dann hätte die neue Subnetmask 19 Bit länge (/19), also `255.255.223.0`. Illustriert findet sich das in Tabelle 3.4, S. 31

Subnetmask:	11111111	11111111	11100000	00000000
Netz 1:	01110010	00001101	00000000	00000000
Netz 2:	01110010	00001101	00100000	00000000
Netz 3:	01110010	00001101	01000000	00000000
Netz 4:	01110010	00001101	01100000	00000000
Netz 5:	01110010	00001101	10000000	00000000
Netz 6:	01110010	00001101	10100000	00000000
Netz 7:	01110010	00001101	11000000	00000000
Netz 8:	01110010	00001101	11100000	00000000

Tabelle 3.5: Die 8 Netze binär geschrieben

Damit stehen pro Netz die verbleibenden 15 Bit für die Host-Adressierung zur Verfügung. Damit lassen sich immerhin 2^{15} Rechner ansprechen (abzüglich zwei, nämlich des Broadcasts und der Netzadresse).

Doch wie lassen diese Netze sich ansprechen? In 3.3.3, S. 30 wurde gesagt, die Netzadresse sei immer die erste Adresse des Netzes. Binär betrachtet bedeutet dies, daß alle Stellen, die nicht zur Netzwerkmaske gehören, mit `0` belegt sind. Die acht verschiedenen Netze wurden in Tabelle 3.5, S. 32 binär dargestellt. In Dezimalzahlen umgerechnet ergeben sich damit `114.13.0.0`, `114.13.32.0`, `114.13.64.0`, `114.13.96.0`, `114.13.128.0`, `114.13.160.0`, `114.13.192.0` und `114.13.224.0`.[9]

Wie bereits gesagt werden das erste und das letzte Netz aus Sicherheitshalber nicht verwendet. Daher wird im folgenden das zweite Netz (`14.13.32.0`) betrachtet. Der erste Rechner dieses Netzes trägt die Nummer `114.13.32.1`, seine Broadcast-Adresse wäre binär gesehen
`01110010.00001101.00111111.11111111`, dezimal `114.13.63.255`.
Alle Rechner, die sich dazwischen befinden (zum Beispiel `114.13.44.11`), befinden sich im selben Netz.

In Anhang C.1.2, S. 106 stehen Möglichkeiten, diese Rechnungen schneller und ohne die Zuhilfename von Binärzahlen durchzuführen. Das zu Grunde liegende Prinzip sollte jedoch vorher verstanden worden sein.

Neben diesem als *Subneting* bekannten Verfahren gibt es noch ein anderes, das sogenannte *Superneting*. Hierbei geht es um die Vergrößerung eines Netzes. Falls eine Firma zwei neben einander liegende Netze besitzt, kann sie diese durch ein Verringern der Subnetmask um eine Stelle beide zusammen legen. Dieses Verfahren wird in denmeisten Büchern recht stiefmütterlich behandelt; Microsoft erwähnt es lediglich im Zusammenhang mit CIDR.

[9]Das nachzurechnen ist dem Leser als einfach Übung überlassen...

3.4 Switches und Router

In diesem Abschnitt soll erklärt werden, wie ein Switch bzw. ein (normaler, auf Schicht 3 aufsetzender) Router eigentlich arbeitet.

3.4.1 Switches

Ein Switch ist ein Gerät mit mindestens zwei, meistens jedoch mehr Netzwerkanschlüssen. Er arbeitet auf der zweiten Schicht des ISO/OSI-Schichtenmodells und stellt aufgrund der ihm gegebenen Informationen Verbindungen zwischen zweien seiner Anschlüsse her. Wie Kapitel 3.1.2, S. 24 zu entnehmen ist, sind die einzigen Informationen, die er somit erhällt, die MAC-Adressen der am Datenaustausch beteiligten Rechner. Also unterschiedet er anhand eine Zuordnungstabelle, der sogenannten *Adressentabelle* (*Addresstable*) und den in den ankommenden Dateipaketen enthaltenen Ziel-MAC-Adressen, zu welchem Netzanschluß er das Paket zu leiten hat. Falls er keinen entsprechenden Eintrag hat, schickt er das Paket an alle Anschlüsse abzüglich den, von dem es gekommen ist. Dieser Vorgang wird *Fluten* (*flooting*) genannt.

Jedes mal, wenn ein Swicth ein Paket flutet, lernt er, falls er eine Rückmeldung erhällt, eine neue MAC-Adresse. Diese wird in seine Tabelle eingetragen und erst nach Ablauf einer bestimmtn Frist, in der sie nicht benutzt wird, gelöscht. Falls der Switch eine Absender-Adresse nicht kennt, lernt er diese ebenfals.

Bei seiner Initialisierung ist die Adressentabelle des Switches vollkommen leer. Da somit nicht definiert ist, an welchen Port er ein Paket verschicken soll, flutet er das das erste ankommende. Dabei lernt er die Adressen des Absenders und des Empfängers. Auf diese Weise füllt der Switch nach und nach seine Tabelle, bis entweder kine neuen MAC-Adressen mehr dazu kommen oder sein Speicher voll ist. Sobald das passiert, muß er jedes ankommnde und ihm unbekante Paket fluten.

3.4.2 Router

Ein Router überträgt Datenpakete von einem Netz in ein anderes. Daher verfügt er über mindestens zwei Netzwerkanschlüsse. Simpel gesagt muß sich einer davon mit seiner IP-Adresse (und natürlich physikalisch) in dem Netz befinden, von dem das Paket kommt, und einer in dem, in das dieses Paket geleitet werden soll.

Das Weiterleiten geschieht anhand der *Routingtabelle*. Hier findet sich für jedes vom Router erreichte Netz eine Zieladresse und der zugehörige Anschluß. Bei der Adresse kann es sich entweder um ein Netz oder einen speziellen Rechner (etwa einen anderen Router) handeln. (Übrigens verfügt jeder normale Rechner über eine eigene Routingtabelle. neben dem Eintrag für lokale Anfragen, also `127.0.0.0`, findet sich hier meistens auch ein *Standard-Gateway*. Dies wird für *jede* Anfrage, die nicht an das Netz des sendenden Rechners gerichtet ist, benutzt.) Außerdem verfügt er über eine Tabell, die den IP-Adressen MAC-Adressen zuweist.

IP	0	Internet Protocol, zuständig für Routing über IP-Adressen
ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagarm Protocol

Tabelle 3.6: Wichtige Protokolle

Sobald der Router ein Paket bekommt, das für ein anderes Netz als das des empfangenden Netzwerkinterfaces bestimmt ist, schaut er in seiner Tabelle nach, ob er das Teilnetz kennt. Falls ja, kapselt er das entsprechende Paket; die IP-Informationen bleiben identisch, doch die MAC-Adresse wird durch die neue, der Tabelle entnommenen, ersetzt. Falls der Router keinen entsprechenden Eintrag hat, versendet er das Paket entweder garnicht oder an sein Standardgateway.

3.5 Protokolle, Häfen, Sockel

Auch wenn diese Überschrift eher an Mantel-und-Degen-Filmen erinnert, hat sie direkt mit TCP/IP zu tun. Bislang wurde beleuchtet, wie der gesammte Datenstrom von einem Rechner zum nächsten kommt. Doch wie sortiert der Empfänger ihn auseinander? Zu diesem Zweck werden dem Datenstrohm drei Arten von Kennzahlen mitgegeben, Protokollnummern, Portnummer und Sockets. Der Vorgang, all dies in einen Strohm zu bringen, wird *multiplexen*, das Auseinandersortieren *demultiplexen* genannt.

3.5.1 Protokolle

Es gibt eine ganze Menge Protokolle. Neben IP, TCP und UDP das bereits angesprochene ICMP, dann natürlich IPX, SPX und noch viele, viele andere. Zur Übertragung wird ein Byte, also eine Zahl zwischen 0 und 255, benutzt.

Es gibt eine Datei namens `protocols`, in welcher die vom System verwendeten Protokolle zusammen mit ihren zugehörigen Nummern und Aliassen[10] aufgeführt werden. Wie die meisten TCP/IP-Konfigurationsdateien befindet sie sich im Ordner `etc`. Unter UNIX (und somit auch Linux) ist dieses ein Ordner im Rootverzeichnis (also `/etc`), bei Windows 2000 und Windows XP befindet er sich im Verzeichnis `[WINROOT]\system32\drivers`, wobei `[WINROOT]` das Windows-Hauptverzeichnis (meistens `C:\windows`) ist.

In Tabelle 3.6, S. 34 wurden die wichtigsten Protokolle mit ihren Numern aufgeführt.

[10]Diese Aliasse sind besonders bei der Konfiguration einer Firewall nützlich, etwa wenn bestimmte Protokolle geblockt werden sollen. Die Lesbarkeit der Konfigurationsdateien erhöht sich durch sinnvolle Aliasse ganz erheblich.

ftp	21	Datenübertragung via ftp
ssh	22	Remotezugriff über die Secure Shell
telnet	23	Remotezugriff über telnet
smtp	25	Protokoll zum verschicken von email
domain	53	DNS-Dienst
tftp	69	Rückmeldungsloser ftp
http	80	Übertragung von HTML-Seiten
pop3	110	Protokoll zum Hohlen von email
sunrpc	111	SUNs potmapper
sftp	115	Sicherer ftp
nntp	119	Protokoll zum ansprechen des Newsnets
imap	143	Protokoll zum Hohlen von email
ldap	383	Systemweite Benutezrverwaltung
https	443	Sicherer HTTP
nntps	563	nntp über SSL
doom	666	Spricht wohl für sich...

Tabelle 3.7: Einige Ports

3.5.2 Ports

Nachdem die richtigen Protokolle gefunden wurden, müssen die Daten nun den Netzwerkdiensten zugeordnet werden, für die sie bestimmt wurden. Hierfür sind die sogenannten Ports zuständig.[11]

Die Ports werden in einer 16 Bit Zahl übertragen. (Es gibt also sehr viel Ports.) Von diesen Ports sind die ersten 255 sogenannte *wellknown*, also wohldefinierte Ports. Die Dienste, die hier laufen, sollten im Allgemeinen immer unter diesen Portnummern erreichbar sein. (Obwohl sich das Ändern läßt.) Hierzu zählen etwa HTTP, FTP und ähnliches. Die Ports von 256 bis 1024 sind mit UNIX-spezifischen Diensten belegt.[12]

Einen anderen Weg als die wohldefinierten Ports ist die Firma SUN MICROSYSTEMS mit der Entwicklung des *portmapper* gegangen. Bei diesem Programm registriert sich jeder Dienst, der Anrecht auf einen Port hat. Je nach Bedarf und Verfügbarkeit weißt der *portmapper* dann Ports zu. Falls ein Zugriff aus dem Netz erfolgen soll, fragt der Sender an dem (einzigen) wohldefinierten Port 111 an, welcher Port der richtige ist.

Die wichtigsten Ports wurden in Tabelle 3.7, S. 35 aufgeführt.

[11]Für die Zuordnung gibt es ebenfalls eine Datei im Ordner `etc`, nämlich `services`. Für die meisten Anwendungen ist die Datei nicht notwendig.

[12]Inzwischen haben die meisten von ihnen auch bei Windows einzug gehalten. (Abgesehen vom Historischen besteht also kein Unterschied zu den *wellknown port*.)

3.5.3 Sockets

Ein Socket setzt sich aus einer IP-Adresse und einem Port zusammen. Um eine Internetverbindung zu einem Webserver aufzubauen, wäre eigentlich im Browser die Angabe des Sockets nötig, etwa `http://www.google.de:80`. (Wobei hier anstelle der IP-Adresse der Name angegeben wurde, doch der wird unterwegs in eine Nummer umgewandelt, siehe 3.7.3, S. 40.) Doch da http ein wohldefinierter Port ist, braucht die 80 nicht angegeben zu werden, sie wird automatisch ergänzt.

Wenn es einem Betreiber Spaß macht, kann er seinen Webserver auch auf einen anderen Port legen. Dann ist die Portangabe allerdings nötig. Wer den Port nicht kennt, ist von der Nutzung der Seite ausgeschlossen.

Eine Verbindung wird über zwei Sockets definiert, einmal den Socket des Senders (mit dessen Hilfe der Empfänger Daten zurückgeben kann) und den des Empfängers (mit deren Hilfe der Sender den Empfänger überhaupt erreicht). Theoretisch ist es möglich, das bei beispielsweise einer `telnet`-Session sowohl der Port des Senders als auch der des Empfängers 23 sind. Dies führt jedoch spätestens dann zu Problemen, wenn mehr als ein Benutzer zur Zeit eine `telnet`-Sitzung von einem zum anderen Rechner aufmachen will. Wenn der erste bereits die Sockets IP:23 und IP:23 hat, wie soll dann die zweite Verbindung gestalltet werden?

Aus diesem Grund werden ausgehende Verbindungen meistens zwar an den entsprechenden wohldefinierten Port gesendet, gehen aber von einem Port jenseits der 1024 aus. Wärend des (nicht näher beleuchteten) Dreiwege-Handshakes zum Verbindungsaufbau wird dem Empfänger mitgeteilt, auf welchem Port er antworten soll.

3.6 DHCP

DHCP steht für *Dynamic Host Configurationl Protocol*. Dieser Dienst ermöglicht es einem Rechner, der über keine weitere TCP/IP-Konfiguration verfügt, sich die erforderlichen Daten von einem dafür eingesetzten DHCP-Server zu besorgen. Die Rechner, die sich mit IP-Adressen versorgen lassen wollen, werden im folgenden als DHCP-Clients bezeichnet.

3.6.1 Funktionsweise

Bei Systemstart sendet ein Client einen Broadcast (siehe Abchnitt 3.3.3, S. 31) mit der Adresse `255.255.255.255` und der Netzwerkmaske `0.0.0.0`. Dieser Broadcast enthällt das Paket *DHCPDISCOVERY*. Sobald ein DHCP-Server ein solches Paket erhällt, sendet er dem Client (dessen MAC-Adresse er ja hat) ein *DHCPOFFER*-Paket. Dieses enthällt alle Daten, die der Server anbietet, mindestens eine IP-Adresse und eine Leasingtime.

Der Client wertet die ankommenden Daten aus und sendet, falls er feststellt, daß diese Netzadresse bereits vergeben ist, ein *DHCPDECLINE*-Paket. Falls alles in Ordnung ist, sendet er das *DHCPREQUEST*-Paket, in welchem er dem Server mitteilt, daß er diese Daten übernehmen möchte.

Der Server sendet als nächstes ein *DHCPACK*-Paket. Hiermit bestätigt er, daß die Daten tatsächlich stimmen. Daraufhin übernimmt der Client alle Werte, die er haben möchte.

Innerhalb der Leasingtime bekommt der Client von seinem Server stets die gleiche IP übermittelt. Wird sie nicht (serverseitig) geändert, beträgt sie (meistens) 8 Tage. Nach 50% der Zeit stellt der Client eine Anfrage auf Verlängerung um die Standardzeit. Diese Anforderung geschieht ebenfalls über das Paket *DHCPREQUEST*. Falls er den Server in dieser Zeit nicht erreicht, versucht er es nach 75% der Zeit und — bei Nichterfolg — bei Ablauf seiner Leasingtime erneut. Falls die Zeit ohne Verlängerung abläuft, beginnt der Vorgang von vorne.

Eine andere Möglichkeit besteht darin, daß sich der Clien seine Einstellungen „merkt". Dann stellt er sofort eine Anfrage an seinen Server (mittels *DHCPREQUEST*). Falls der Server mit den Übermittelten Daten einverstanden ist, schickt er sein *DHCPACK*-Signal, anderenfalls (etwa, wenn der Client in ein anderes Subnetz gewechselt hat) ein *DHCPNACK*-Signal. In letztgenannten Fall muß der Client von vorne beginnen.

Sobald ein Client sich abmeldet, kann er dem Server mit einem *DHCPRELEASE*-Signal mitteilen, daß seine Adresse nun wieder zur Vergabe zu Verfügung steht.

3.6.2 Ausfallsicherheit

Da DHCP über einen Broadcast arbeitet, muß sich für gewöhnlich in jedem Netzwerksegment mindestens einer davon befinden. Doch was passiert, wenn dieser eine Server ausfällt? Zu diesem Zweck liegen auf dem DHCP-Server eines anderen Segmentes ebenfalls einige Adressen bereit. Das Verhältnis der Adressen auf dem „eigenen" Server zu dem der Adressen auf dem anderen beträgt meistens 70:30.

Doch wie kommt der Broadcast über den Router? Hierfür ist ein sogenannter DHCP-Relay-Agent zuständig. Dieser kann auf einem der Clients oder dem Router selbst laufen und steht in Kontakt mit dem DHCP-Server. Er leitet ankommende DHCPDISCOVERY-Signale an den DHCP-Server im anderen Segment weiter.

In einigen wenigen Fälen, etwa wenn Firmenweit nur ein DHCP-Server vorhanden ist, kann der DHCP-Relay-Agent auch eingesetzt werden, um ein Segment überhaupt mit DHCP-Adressen zu versorgen.

3.6.3 APIPA

Gelegendlich kann es vorkommen, daß ein Rechner einen DHCP-Server anfordert, aber keinen erreichen kann. Da viele Dienste aber auf das Vorhandensein einer IP-Adresse angewiesen sind, entwickelte Microsoft das APIPA-Verfahren. APIPA steht für *Automatic Private IP Adressing*. Hierfür hat Microsoft den Adressbereich von 169.254.0.1 bis 169.254.255.254 reserviert. Der Rechner wählt sich wilkürlich eine Adresse aus diesem Bereich und testet dann mit einem Broadcast, ob die bereits vergeben ist. Falls nicht, setzt er sie bei sich ein. (Da es sich bei dem APIPA-Netz offensichtlich um ein Klasse B Netz handelt, lautet die Netzwerkmaske entsprechend `255.255.0.0`.)

3.6.4 Sonstige Anmerkungen

Mittels DHCP lassen sich alle möglichen Daten übertragen. Es gibt für einen Client auch die Möglichkeit, diese Daten abzufragen, obwohl er über eine feste DHCP-Adresse verfügt. Das dafür ausgesandte Paket heißt *DHCPINFORM*.[13]

Eine wesendlich interessantere Möglichkeit besteht darin, den DHCP-Server mit Zuweisungstabellen zu versehen. Diese enthalten Auflösungen von IP-Adressen zu MAC-Adressen. So wird sichergestellt, daß jeder Rechner immer die ihm zugewiesene Adresse bekommt. Festen IP-Adressen gegenüber hat dies den Vorteil, daß der Benutzer ruhig versehendlich seine Adresse verwursten kann — nach dem Neustart hat er wieder seine alte.

Um sich die von DHCP übermittelten Werte anzusehen, kann unter anderem das Programm `ipconfig` verwendet werden. Das Programm bietet auch weiterreichende Funktionen und ist in Anhang C.2.1, S. 108 beschrieben.

3.7 Namensauflösung

Rechner über ihre IP- (oder gar MAC-) Adresse anzusprechen ist nicht sonderlich komfortabel. Aus diesem Grund gibt es verschiedene Ansätze, um statt dessen mit Namen zu arbeiten. In der Windows-Welt werden NetBIOS- und Host-Namen verwendet.

3.7.1 NetBIOS

Ein inzwischen recht betagter und aus der Mode kommender Weg ist das Ansprechen über NetBIOS-Namen. Dieses Verfahren wurde ursprunglich von Microsoft in Zusammenarbeit mit IBM entwickelt. Ein NetBIOS-Name ist 15+1 Zeichen lang, wobei 15 Zeichen für den Namen vergeben werden können und das letzte zur Übermitlung von Servicekennungen verwendet wird. NetBIOS ist eigentlich Bestandteil des Protokolles NetBUI. Microsoft hat aber inzwischen das sogenannte NetBT entwickelt, *NetBIOS over TCP/IP*.

NetBIOS-Namen werden mittels Broadcast in Erfahrung gebracht. Daher funktioniert diese Namensauflösung nur innerhalb eines Netzwerksegmentes. Unter NetBT wird versucht, diese Broadcasts ebenfalls zu vermeiden. Zu diesem Zweck gibt es eine Date namens `lmhosts` in dem bereits erwähnten Verzeichnis `etc`. Hier werden NetBIOS-Namen in IP-Adressen überführt.

[13] Ob Windows diese Möglichkeit unterstützt, ist dem Verfasser nicht bekannt.

Für gewöhnlich sollten die NetBIOS-Namen mit den im nächsten Abschnitt behandelten Host-Namen identisch sein; damit wäre die Datei eigentlich überflüssig. Einige ältere Programme (etwa für Windows 98) benötigen aber die „echten“ NetBIOS-Namen, aus Kompatibilitätsgründen ist sie also nach wie vor nötig.

Die Wartung dieser Datei ist naturgemäß reichlich aufwendig; bei einem Netzwerk mit mehreren hundert Rechnern etwa besteht zwar die Möglichkeit, die Datei zentral abzulegen und mit einem Skript bei jeder Aktualisierung auf die einzelnen Rechner zu kopieren. Diese Methode ist sowohl Fehleranfällig als auch aufwendig. Abhilfe wurde diesem Problem mit Einführung des WINS-Servers (WINS steht für *Windows Internet Naming Service*) geschaffen. Dies ist ein zentraler Server, der NetBIOS-Namen nach IP-Adressen auflößt.

3.7.2 Host-Namen und FQDNs

Host-Namen können 255 Zeichen lang sein. Sie werden über die Datei `hosts` im Verzeichnis `etc` zu IP-Adressen aufgelößt. Neben dem Host-Namen kann hier auch ein Alias angegeben werden. Das ist sinnvoll, da als Host-Namen häufig die *Full Qualified Domain Names* (*FQDN*) benutzt werden.

FQDNs werden von rechts nach links gelesen. Sie bestehen aus einer Toplevel-, einer Secondlevel- und manchmal noch einer Subdomain, und ganz am Anfag steht der in dieser Domain anzusprechende Rechner.[14] Der Bezeichner

`deathbringer.e01.net`

besagt also, daß der Rechner `deathbringer` in der topleveldomain `net` und der Secondleveldomain `e01` anzusprechen ist.

Den kompletten Namen einzugeben ist in einigen Fällen ebenfalls etwas nervig. Der Alias sollte, um die Konfiguration zu vereinfachen, besser mit dem NetBIOS Namen identisch sein.

Da sich auch die Pflege der Host-Datei als ausgesprochen aufwendig erweist, werden diese Namen ebenfalls über einen Server, den sogenannten *Nameserver* angesprochen. Das zugrunde liegende Prinzip ist der *Domain Name Service* (*DNS*). Er arbeitet mit FQDNs.

In firmeninternen Netzen, die mittels DNS aufgelößt werden, werden sogenannte *search-Domains* eingerichtet. Wird ein Hostname ohne eine Domäne angegeben, werden die Search-Domänen automatisch ergänzt. Unter Windows kann maximal eine Search-Domäne angegeben werden, sie findet sich unter unter den *Systemeigenschaften* auf der Karte *Netzwerkidentifikation*, Unterpunkt *Eigenschaften*. Hier gibt es den Punkt *Erweitert*, unter dem dann das *primäre DNS-Suffix* angegeben werden kann. (Außerdem bestimmt dieser Punkt den Domänenanteil des FQDNs des Rechners, falls er sich in einer Arbeitsgruppe befindet. Steht er in einer Domäne, wird diese als Search-Domain benutzt.) Unter UNIX können in der Datei `/etc/resolver` beliebig viele Search-Domains angegeben werden.

[14] Theoretisch ist beginnt der FQDN ganz rechts mit einem `.` für die sogenannte *Root-Domain*, der wird aber normaler Weise weggelassen.

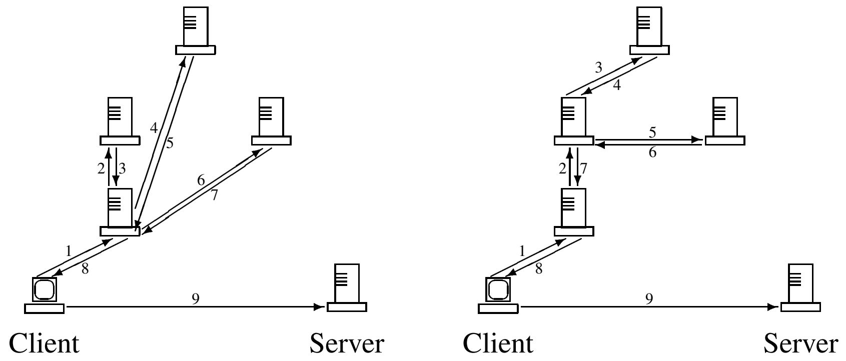


Abbildung 3.3: Domain Name Service

3.7.3 DNS

DNS steht für *Domain Name Service*. Dies ist eine Möglichkeit der Namensauflösung, die bereits 1984 entwickelt wurde und in UNIX-Netzen und im Internet die Standardauflösung ist. Mit Windows 2000 hat auch Microsoft sich auf dieses Prinzip umgestellt; sie haben auch nur ungefähr 15 Jahre dafür gebraucht…

DNS arbeitet mit den in 3.7.2, S. 39 angesprochenen Full Qualified Domain Names. Für gewöhnlich stellt jede Domain eine sogenannte Zone dar. Ein DNS-Server ist für die Verwaltung einer oder mehrerer Zonen zuständig. Wird er angesprochen und nach der IP eines Rechners gefragt, der in seiner Zone lieg, liefert er diese zurück. Sein verhalten im Falle eines ihm unbekannten Rechners ist davon abhängig, ob er im iterativen oder im rekursiven Modus arbeitet; ein iterativer DNS-Server liefert lediglich die Adresse eines Rechners zurück, der entweder bei ihm für die fragliche Zone eingerichtet, oder — falls er mit der angefragten Zone nichts anfangen kann, ihm übergeordnet ist. Ist er rekursiv eingestellt, leitet er die Anfrage direkt an den entsprechenden Server weiter.

Normaer Weise hat jede Subdomäin einen eigenen Nameserver, denen die Domainserver der Secondleveldomains übergeordnet sind. Darüber stehen die Server der Topleveldomains (welch nach Verwendungszweck und Land geordnet sind). An oberster Stelle stehen die Rootserver. Rootserver arbeiten immer iterativ.

In Abbildung 3.3, S. 40 ist die Anfrage eines Clients um die Netzwerkadresse eines Servers abgebildet. Auf der linken Seite arbeiten alle Server iterativ, auf der rechten arbeitet der erste angesprochene DNS-Server rekursiv.

3.7.4 Die Namensauflösung unter Windows 2000

Windows 2000 Rechner lösen Namen in einer ganz bestimmten Reinfolge auf. Diese kann geändert werden, es gibt jedoch für NetBIOS-Namen und Host-Namen bestimmte Standard-Reinfolgen. Für Host-Namen wird die folgende Reinfolge verwendet:

1. Überprüfung, ob der angeforderte Name der eigene Rechner ist.
2. Falls der Name nicht dem *localhost* entspricht, wird die Datei `hosts` überprüft.
3. Falls die Datei `hosts` den Namen nicht enthällt, wird eine Anfrage an den DNS-Server gesendet.
4. Falls der DNS-Server keine Auflösung liefert, wird der NetBIOS-Namenscache durchsucht. Das passiert, weil Windows 2000 NetBIOS-Namen als Hostnamen behandelt.
5. Falls der Name nicht im NetBIOS-Namenscach steht, wird eine Anfrage an den WINS-Server gesendet.
6. Falls der WINS-Server keine Adresse zurückliefert, wird ein Broadcast in das gesammte Netzsegment geschickt.
7. Falls auch der Broadcast kein Ergebnis liefert, wird die Datei `lmhosts` befragt.

Für NetBIOS-Namen gestalltet sich die Auflösung wie folgend:

1. Als erstes wird der NetBIOS-Namecache überprüft.
2. Befindet sich der Name nicht im Namecache, wird ein WINS-Server abgefragt.
3. Liefert der WINS-Server keine Adresse zurück, wird ein Broadcast ausgesand.
4. Falls der Broadcast kein Ergebis bringt, wird die Datei `lmhosts` überprüft.
5. Falls der Name nicht in der `lmhosts`-Datei zu finden ist, wird die Datei `hosts` überprüft.
6. Falls auch diese Datei den Namen nicht enthällt, wird der DNS-Server befragt.

Kapitel 4

Windows NT 4.0

Dieses Kapitel stellt eine überarbeitete und chronologisch teilweise umstrukturierte Mitschrift des ADPC Windows NT 4.0 Unterrichtes dar. Abschnitt 4.1 beschäftigt sich mit den verschiedenen Möglichkeiten, Windows NT 4.0 Workstation oder Server zu installieren (inklusive Netzwerk- und automatisierten Installationen). Abschnitt 4.2 gibt einen flüchtigen überblick über die Möglichkeiten, mit Festplatten unter Windows NT zu arbeiten. Abschnitt 4.3 führt die Begriffe *Gruppe* und *Benutzer* und geht auf deren Erstellung ein. In Abschnitt 4.4 wird auf die verschiedenen Dateizugriffsberechtigungen (Remote, Lokal und die Kombination aus beiden) eingegangen, wärend Abschnitt 4.5 nochmals die Benutzer und Gruppen aufgreift und auf ihre Verwaltung eingeht. Der Abschnitt 4.6 behandelt die Systemarchitektur von NT und daraus resultierende Konfigurationsmöglichkeiten. Daran schließt sich Abschnitt 4.7 über die Registry-Datei von Windows NT an. Die Absachnitte 4.8 bis 4.11 haben Netzwerkoperationen zum Thema, wobei es unter Anderem um NT-Domänen, Drucker (auch lokal), Zugriffe in heterogenen Netzen und Dateireplikation geht. Der Abschnitt 4.12 schließt die Mitschrift mit einer Beleuchtung der einzelnen Möglichkeiten, einen Rechner oder ein Netz zu überwachen, ab.

Für die Erstellung wurden neben zwei nicht sonderlich informativen Büchern der Firma MICROSOFT, die als Vorbereitung für den MCP[1] gedacht waren [10, 11], diente zum einen *Windows NT System Administration* von ÆLEEN FRISH [4], zum anderen *Windows NT TCP/IP Netzwerk-Administration* von CRAIG HUNT und ROBERT THOMSON [6].

> „This building should be condemned. There is serious metal fatigue on all the load-bearing members, the wiring is substandard, it's inadequate for our power needs, and the neighbourhood is like a demilitarized zone.“
>
> DR. EGON SPENGLER, *Ghostbusters*

[1] Für Windows NT 4.0.

4.1 Installation

Im Zuge der Unterrichtsinstalation ist es erforderlich, daß sich auf jedem Rechner eine WindowsNT 4.0 Workstation Installation und eine ebensolche Server-Installation befindet. Hierzu ist es zunächst sinnvoll, sich die verschiedenen Servertypen zu vergegenwärtigen:

PDC, *Primary Domain Controller*: Ein PDC verwaltet eine Domäne. Daher wird er auch als DC, *Domain Controller*, bezeichnet. Da sich Rechner (und Benutzer) an ihm anmelden wird er im Deutschen als *Anmeldeserver* bezeichnet. DCs ergeben nur in einem Client-Server-basierten Netzwerk, einer sogenannte *Domäne*, Sinn.

BDC, *Backup Domain Controller*: Auch BDCs gehören zu den BCs. Sie treten in Aktion, wenn ein PDC ausfällt oder überlastet ist. Sie hohlen für gewöhnlich alle Konfigurationsdaten vom PDC.

Alleinstehender Server: Ein alleinstehender Server arbeitet innerhalb eines Peer-to-Peer-Netzes (einer sogenannten Workgroup). Da bei diesen Netzen keine einheitliche Nutzer- und Rechnerverwaltung vorherrscht, kann das niemals ein DC sein. Alleinstehende Server sind meistens Printer-, Datei- oder Anwendungsserver.

Member- oder Mitgliedserver: Ein Memberserver ist ein Server in einer Domäne, der kein DC ist. Diese Möglichkeit kann bei der Installation nicht gewählt werden; um ihn trotzdem einzurichten, wird ein *Alleinstehender Server*[2] aufgesetzt, der nach Abschluß der Installation einer Domäne beitritt.

Grundsätzlich liegen die Installationsdateien in einem Verzeichnis, welches die Architektur des Zielrechners beschreibt. Im Falle eines PCs ist das `\i386`, benannt nach der *Intel 386* Familie.

Microsoft gibt als Systemvoraussetzungen für die Workstation einen Pentiumprozesor,[3] mindestens 16 MByte RAM (32 MB empfohlen) und 110 MByte Plattenplatz an. Erstaunlicher Weise reicht für den Server ein 486/33, dafür müssen es aber 125 MByte Festplattenplatz[4] sein.

4.1.1 Installationsparameter

Die Installation kann über die vorgesehenen Startdisketten, den Start von CD-ROM (so der Rechner und die Ausgabe von NT das unterstützten) oder von einem laufenden Betriebsystem aus geschehen. (In diese Kategorie fällt auch eine DOS-Startdiskette.)

[2]Entsprechend kann ein Memberserver auch einer der dort besprochenen Server sein.

[3]Für Nicht-Intel-Geräte steht hier Alpha AXP, MIPS R4x00 oder PowerPC Prozessor.

[4]Bei den Nicht-Intel-Geräten werden 160 MByte benötigt.

Im Falle der vorgesehenen Startdisketten müssen selbige in der richtigen Reinfolge eingelegt werden, bevor die Installation von CD[5] beginnt. Bei diesem Vorgang werden alle möglichen (und unmöglichen) Treiber, die für die Installation erforderlich sein könnten, geladen.

Um von einem laufenden Betriebsystem aus die Installation zu starten, wird das Programm `winnt.exe` oder `winnt32.exe` benutzt. Ersteres ist für DOS und Windows 9x (also die 16-Bit-Betriebsysteme), letzteres für Windows NT 3.51 gedacht.[6]

Normaler Weise werden bei Aufruf dieses Programmes erst einmal die drei Startdisketten erstellt. Mit Hilfe von verschiedenen Parametern läßt sich das genauer regeln:

`/x`: Verzichtet auf das Erstellen von Disketten und geht davon aus, daß sie bereits vorhanden sind.

`/ox`: Erstellt die drei Disketten, installiert aber nicht.

`/b`: Verzichtet vollkommen auf den Gebrauch (oder die Erstellung) von Disketten. Das ist die Option, die auch bei der Installation von bootbarer CD verwendet wird.

`/s:` *`Pfad`*: Falls anstelle des normalen Standardverzeichnisses irgend ein anderes genommen werden soll (etwa ein verbundenes Netzlaufwerk), dann wird hier der entsprechende Pfad dorthin angegeben.

`/t:` *`Pfad`*: Gibt an, wo das Installationsprogramm seine temporären Dateien ablegen soll.

Diese Optionen (und noch eine ganze Reihe anderer) funktionieren für beide Varianten des Installationsprogrammes. Eine volständige Liste aller Parameter läßt sich mit `winnt /?` (bzw. `winnt32 /?`) aufrufen.

4.1.2 Installation — ein Beispiel

Es gibt einen grundsätzlichen Unterschied zwischen der Installation durch Aufruf des Befehles `winnt(32).exe /b` und der von CD. Wird von einer bootfähigen Diskette der Befehl aufgerufen, wird das unweigerlich zu Problemen führen: Bei der Installation müssen eine gewisse Menge an Installationsdaten an irgend eine Stelle kopiert und von dort ausgeführt werden. Bei der CD-Variante wird dafür eine RAM-Disk eingerichtet.

Aus diesem Grund ist das Vorgehen bei einer diskettengestützten Installation das folgende:

1. Einrichten einer Partition mittels `fdisk`

[5] Es gibt NT 4.0 auch auf Diskette... darauf wird hier aber nicht eingegangen.

[6] Unter Windows 2000 dient `winnt32.exe` auch für Windows 9x.

2. Formatieren dieser Partition
3. Neustart und Aufruf des Programmes `\i386\winnt.exe /p` von der CD-ROM

Die CD-Variante bietet die Partitionierung direkt im Installationsprogramm.

Wie auch immer, früher oder später kommt die große Wahl, welches Dateisystem für die Partition benutzt werden soll: FAT oder NTFS. Es mepfielt sich *immer*, NTFS zu wählen. Nur NTFS bietet zusätzliche Funktionalitäten wie Rechte und Kompression. Auch die Fragmentierung ist geringer als bei FAT. Außerdem können diese Platten bis zu 4 GByte groß sein, wärend FAT-Platten bei 2 GByte[7] enden. Schließlich und endlich sind unter NT auf einer FAT-Partition maximal 512 Dateieinträge möglich.

Nach dieser Wahl kommt ein Menü, indem entschieden wird, ob ein System installiert oder ein bestehendes System mit Hilfe der zugehörigen Rettungsdiskette repariert werden soll. In diesem Fall handelt es sich um eine Neuinstallation.

Als nächstes ist der Zielpfad einzutragen. Standardmäßig ist das `\winnt`. Es ist theoretisch möglich, mehr als eine Installation auf einer Partition zu haben; ein anderer installationspfad reicht zur Trennung aus. Besonders schön ist das aber nicht und kann unter Umständen zu Problemen führen. Es empfielt sich, für jede Installation eine eigene Partition zu benutzen.

Der Frage nach dem Zielpfad schließt sich die nach dem Lizensmodell an: Auf einen Server dürfen nur eingeschränkt viele Rechner zugreifen. Die Anzahl ist dabei von den von Microsoft erworbenen Lizensen abhängig. Es gibt zwei verschiedene Modelle der Lizensverwaltung:

Serverbasiert: Es wird lediglich angegeben, wie viele Verbindungen ein Server zur gleichen Zeit zulassen darf.

Clientbasiert: Für jeden Client, der auf den Rechner zugreifen soll, muß eine Lizens vorliegen.

Es ist möglich, von dem serverbasierten Modell auf das Clientbasierte umzustellen. Anders herum geht das nicht.

Auf das Lizensenmodell folgen Schirme zur Anwahl des Servertypen (siehe S. 44), zur Vergabe des Administratorenkennwortes, zur Erstellung der Notfalldiskette und zur Anwahl des zu Installierenden Zubehörs. Interessant werden erst wieder die sich anschließenden Konfigurationen des Netzwerkes:

Als Protokoll ist nur eines erforderlich, nämlich TCP/IP. Die zu installierenden Dienste erfordern (an dieser Stelle) keine nähere Betrachtung. Bei der Konfiguration der Netzwerkkarte hingegen sollte Vorsicht walten. Falls hier ein nicht genau passender Treiber installiert wird, ist das System erst einmal hinüber!

Die Frage, ob DHCP als Konfiguration einer Server-IP-Adresse sinnvoll ist, hängt von den Gegebenheiten ab. Normaler Weise empfehlen sich eher statische

[7] Das etwas effizientere FAT32 wird von NT nicht grundsätzlich unterstützt

IP-Adressen. In unserem Fall sollten sie innerhalb des privaten Klasse C Bereiches liegen.[8]

Die restlichen Fragen nach der Arbeitsgruppe, der Domäne, der Uhrzeit und des Datums sind nach eigenem Geschmack anzuegeben. Damit sollte die Grundinstallation abgeschlossen sein.

4.1.3 Nachbesserungen

Nach der Installation gibt es noch einige Dinge, die für den Betrieb konfiguriert werden sollten. Eine davon sind die Anzeige-Einstellungen des Explorers. Hier sollte auf jeden Fall *Alle Dateien anzeigen* an- und *Endungen ausblenden* abgeklickt werden.

Eine andere Sache ist die Installation etwaiger Servicepacks. Diese dienen der Beseitigung von Fehlern, Sicherheitslücken und der Verbesserung des Systemes. Das letzte für Windows NT 4.0 erschienene Servicepack hat die Nummer 6a.[9] Nach der Installation einer großeren Softwarekomponente oder eines neuen Treibers empfielt es sich, das aktuelle Servicepack nochmals zu installieren.

4.1.4 Unbeaufsichtigte Installation

In Firmen kann sich die Notwendigkeit, sehr viele Rechner zu installieren, ergeben. Da wäre es ein wenig störend, jedes mal die Installation vollständig von Hand durchzuführen. Microsoft hat dafür einige Methoden bereit gestellt, die neben der Installation des Betriebsystems auch die Einrichtung von Anwendungsprogrammen ermöglicht.

Zu diesem Zweck werden zwei weiterer Parameter des Setup-Programmes `winnt(32)` (siehe 4.1.1, S. 45) benötigt, nämlich `/U` und `/UDF`:

`/U:` *`antwortdatei.txt`*: Durch diesen Parameter holt sich das Installationsprogramm die Antworten auf seine diversen Fragen an den Benutzer aus der Datei `unattend.txt` (oder einer anderen) hohlen.

`/UDF:` *`ID datei.udf`*: Dieser Parameter ist eine Ergänzung des letzten; er sorgt dafür, daß bestimmte Einstellungen nicht durch `unattend.txt`, sondern eine andere, anzugebende Datei vorgenommen werden.

Durch die `unattend.txt` können grundlegende Dinge festgelegt werden; bei mehreren Rechnern könnte das jedoch zu einem Problem führen, da ihnen beispielsweise identische Rechnernamen gegeben würden. An diesem Punkt greift die UDF-Datei; anhand der ID findet das Installationsprogramm heraus, welche Einträge für den speziellen Rechner gelten.

[8]Ein Wort zum Standard-Gateway: Es gibt eine konvention, daß die erste verfügbare Adresse eines Netzes das Standardgateway sein sollte. In diesem Fall ist das die `192.168.5.1`.

[9]USB-Unterstützung ist für das Servicepack 7 vorgesehen. Da es nach 6a keines mehr geben wird, nützt das wenig. . .

Die Datei `unattend.txt` von Hand zu schreiben wäre ausgesprochen aufwendig. Hierzu gibt es auf der Server-CD den sogenannten Setupmanager. Der Pfad lautet

`\deptools\i386\setupmgr.exe`

Hier kann bequem über ein Menü angegeben werden, was alles in die Datei geschrieben werden soll.

Als letztes bleibt die Automatisierung von Softwareinstallation. Hierzu ist zunächst ein (identisches) bereit fertig intalliertes System notwenig. Auf diesem wird *vor der Installation irgend welcher Software* ein Schnappschuß des Systems erzeugt. Hierzu dient der Befehl `sysdiff /snapshot`.

Nachdem der Schnappschuß erstellt wurde, können die verschiedenen Standard-Anwendungen installiert werden. Nach Abschluß ihrer Installation kommt das Programm erneut zum Einsatz, dieses mal in Form von `sysdiff /diff` *`differenzdatei`*. Dieser Befehl schreibt alle Änderungen, die sowohl auf der Festplatte als auch in der Registrierung vorgenommen wurden, in eine Datei. Diese kann dem entsprechend sehr groß werden! ***Achtung!*** Auf keinen Fall sollte zwischen den beiden `sysdiff`-Einsätzen der Rechnername geändert werden! Sonst wird der neue Rechnername ebenfalls in die Änderungsdatei geschrieben!

Auf einem anderen installierten System kann nun, so die Differenzdatei dort auf irgend eine Weise verfügbar ist, diese Anpassung vorgenommen Werden. Der Befehl hierzu lautet `sysdiff /applay` *`differenzdatei`*.

4.1.5 Installation über das Netzwerk

Im letzgenannten Fall muß der Administrator immer noch durch die Gegend rennen und CDs einlegen. Und wenn er viele Rechner hat, braucht er viele CDs, es sei denn, er will sie alle nacheinander installieren. Um dem Abhilfe zu schaffen, gibt es die Möglchkeit, ein System von einem installationsserver aus zu installieren.

Das hierfür wichtige Programm ist der Netzwerkmanager für Clients, der auf einem Server im Unterpunkt *Verwaltung* des Programmmenüs zu finden ist. Er bietet eine Reihe von Möglichkeiten, wovon die wichtigsten die Erstellung der Netzwerkinstallationsdiskette ist; hier muß zunächst eine mit DOS formatierte Startdiskette vorhanden sein; eine NT-formatierte Diskette geht *nicht*, da für den Installationsbeginn ein DOS-System benötigt wird. Mit dieser Diskette wird der zu installierende Rechner gestartet, verbindet sich mit dem Intsallationsrechner und beginnt die Installation.

Eine Alternative stellt der Netzwerkinstallationsdiskettensatz dar; hiermit wird ein LAN-Manager für vorhandene Systeme erstellt, über den es möglich ist, sich manuell mit dem Installationsserver zu verbinden un die Installation dort manuell zu starten. Dies ist besonders bei Migrationen und Updates von Interesse.

Ebenfalls vorhanden ist die Möglichkeit, den Installationsserver selbst einzurichten. Wahlweise kann ein CD-ROM-Laufwerk freigegeben oder aber der Inhalt der Installations-CD in ein bestimmtes, freizugebendes Verzeichnis kopiert werden. (Es ist hiermit übrigens auch möglich, einen Installationsserver für ande-

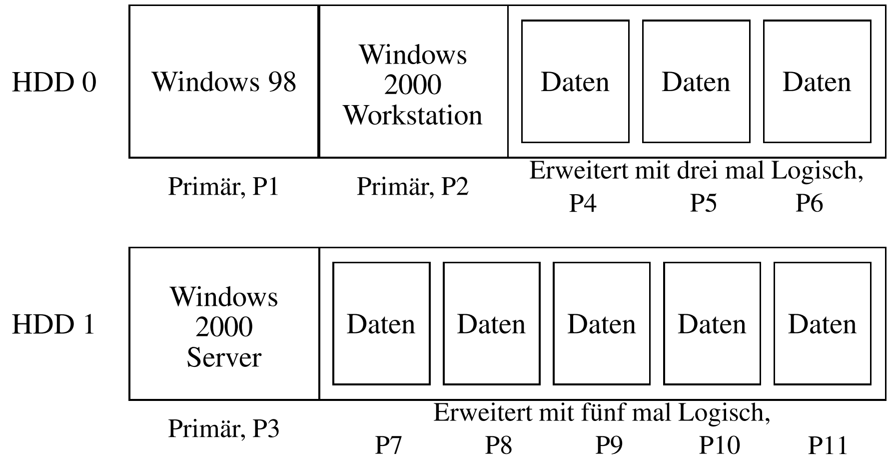


Abbildung 4.1: Festplatten unter Windows NT 4.0

re MS-Betriebsysteme, etwa Windows 95, bereit zu stellen.) Dieser freigegebene Ordner wird auch als *Verteilungspunkt* bezeichnet.

Es bleibt die automatische Installation von Software über das Netz. Hier kommt die in 4.1.4, S. 48 besprochene Differenzdatei zum Einsatz. Sie wird in das Verzeichnis `\$OEM$` direkt unterhalb des Verteilungspunktes kopiert und nach Abschluß der Betriebsysteminstallation automatisch eingespielt.

4.2 Festplatten unter Windows NT 4.0

Bei der Arbeit mit Window NT 4.0 sind einige Besonderheiten zu beachten. Neben den von anderen Betriebsystemen abweichenden Bezeichnungen und Zählweisen bringt es einen eigenen Bootmanager und Unterstützung für softwareseitiges RAID mit. Als letztes ist noch die Konvertierung von FAT-Partitionen nach NTFS zu beachten.

4.2.1 Definitionen und Zählweisen

Windows NT verwendet als Bezeichnung für seine Startplatten geringfügig andere Definitionen als andere Systeme. Es wird zwischen Boot- und Systempartition unterschieden. Die **Systempartition** enthällt dabei alle Daten, die benötigt werden, um das System zu starten. Die **Bootpartition** enthällt das zu bootende System.

Für die Betriebsysteme aus Abbildung 4.1, S. 49, gestaltet sich das so: Für Windows 98 ist die erste Partition sowohl System- als auch Bootpartition. Für die beiden Windows 2000 Installationen ist ebenfalls P1 die Systempartition, für Workstation P2, für Server P3 die Bootpartition.

Wie sich in diesem Beispiel auch sehen läßt, werden die Partitionen eines NT-Systemes intern nicht in ihrer physikalischen, sondern nach ihrer Art nummeriert;

es werden erst alle primären, danach alle sekundären Platten gezählt.

4.2.2 Die Systempartition

Eine Systempartition zeichnet sich vor allem durch das Vorhandensein der folgenden Dateien aus:

- `ntldr` ist der NT-Loader, ein Second Stage Bootloader für NT-Systeme.
- `ntdetect.com` sammelt Hardwareinformationen und gibt sie an `ntldr` weiter.
- `boot.ini` beinhaltet das Bootmenü des NT-eigenen Bootmanagers.

Auf einigen Systemen kommen noch die folgenden beiden Dateien dazu:

- `ntbootdd.sys` findet sich auf Systemen, die einen SCSI-Adapter ohne oder mit abgeschalteten BIOS beinhalten.
- `bootsec.dos` wird auf Systemen erstellt, die vorher ein DOS-System enthalten haben, sie enthällt den alten Bootsektor. Der ist nötig, falls DOS im Dual-Boot-Modus gestartet werden soll.

Es ist möglich, eine Diskette in die Systempartition eines bestimmten[10] Systemes zu verwandeln. Es reicht aus, eine Diskette mit Windows NT zu formatieren und die drei erstgenannten Dateien darauf zu kopieren. Von dieser Diskette läßt sich das System, auf dem sie erstellt wurde, starten; wird die `boot.ini` mit den Pfaden der zu startenden Systeme entsprechend angepaßt, können unter Umständen auch andere Systeme damit gestartet werden.

4.2.3 Der Bootmanager

Falls sich mehr als ein System der Microsoft Produktpalette auf dem Rechner befindet, kann der NT-Hauseigene Bootmanager verwendet werden. Dieser wird durch die Datei `boot.ini` konfiguriert und setzt nach Ausführen des Fisrt Stage Bootloaders, aber vor dem Ausführen des Second Stage Bootloaders ein. (Dadurch erklärt sich, warum andere als Microsoft-Systeme nicht mit diesem Manager zusammen arbeiten; das vom FSBL initilaisierte System kommt nur mit dem SSBL `ntldr` zurecht.)

In dieser Datei stehen die Pfade der Boot-Partition und ihr Menüeintrag. Die Partitionspositionen wurden als sogenannte ARC (*__A__dvanced __R__isc __C__omputing*) - Pfade abgefaßt. Die `boot.ini`-Datei des in Abbildung 4.1, S. 49 aufgezeigten Systemes könnte wie in Abbildung 4.2, S. 51 gezeigt aussehen.

[10] Das besagt, daß diese Diskette nur für diesen einen Rechner oder einen vollkommen identisch eingerichteten funktioniert.

```
[boot loader]
timeout=20
default=multi(0)disk(0)rdisk(0)partition(2)\WINNT

[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows 98"
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft NT 4 Workstation"
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft NT 4 Workstation
  [VGA-Modus]" /basevideo /sos
multi(0)disk(0)rdisk(1)partition(1)\WINNT="Microsoft NT 4 Server"
multi(0)disk(0)rdisk(1)partition(1)\WINNT="Microsoft NT 4 Server [VGA-
  Modus]" /basevideo /sos
```

Abbildung 4.2: Ein Beispiel für die Datei `boot.ini`

Der Teil `[boot loader]` beschreibt das Verhalten des Bootmanagers. Er soll für 20 Sekunden das Menü anzeigen und danach das mittels des hinter dem Eintrag `default=` angebenenen ARC-Pfad erreichbare System starten. Der Teil `[operating systems]` ordnet Menüeinträgen ARC-Pfade zu.

Der ARC-Pfad setzt sich aus den folgenden Schlüsselworten zusammen:

`multi` bezeichnet den IDE-Kanal des anzusprechenden Systemes (also 0 oder 1). Falls das System über einen odr mehrere SCSIController mit eigenem SCSI-BIOS verfügt, werden diese ebenfalls über `multi` angegeben.

`scsi` wird nur verwendet, wenn ein SCSI-Controller mit abgeschalteten oder ohne SCSI-BIOS verwendet wird. Die Zählung beginnt mit 0.

`disk` hat nur im Zusammenhang mit `scsi` Bedeutung und bezeichnet die LUN einer an einem passiven Adapter hängenden Platte. Falls kein solcher Adapter evrwendet wird, muß hier `disk(0)` stehen. AUch hier beginnt die Zählung mit 0.

`rdisk` wird in allen anderen Fällen benutzt und bezeichnet die Festplatte. Die Zählung beginnt ebenfalls mit 0.

`partition` gibt die Partition an.

`Verzeichnis` bezeichnet das Verzeichnis, in dem sich das System befindet. HIer beginnt die Zählung mit 1.

Im großen und Ganzen läßt sich ein ARC-Pfad als normaler Pfad sehen, bei dem statt eines Laufwerksbuchstabens eine exakte Beschreibung verwendet wird.

Die hinter dem ARC-Pfad stehenden Bezeichnungen sind die Menü-Einträge. Hinter zweien davon befinden sich Parameter, die ein Hochfahren im VGA-Modus und das Anzeigen geladener treiber beim Systemstart evranlassen. Diese Einträge sind vor alem im Falle von Auftretenden Fehlern von Inetresse, da sie eine Fehleranalyse erleichtern; im Falle eines defekten Grafikkartentreibers ermöglichen sie überhaupt erst das Hochfahren.

4.2.4 RAID

Über das RAID zugrundeliegende Prinzip wurde bereits in Kapitel 2.6, S. 15 brichtet. Hier wird nur auf die Software-RAID-Implementierung unter Windows NT 4.0 eingegangen. Folgende RAID-Level gibt es unter NT:

Datenträgersatz: Diese Methode dient dem Zusamenfassen mehrere Platten zu einer und macht exakt das gleiche, wie die *Linear Raid* Funktion unter Linux.

Level 0, Striping: Unter NT können zwei bis 32 Platten mittels Stripings verbunden werden.

Level 1, Mirroring: Funktioniert mit zwei Platten.

Level 5, Stripeset mit Parität: Auch hier können zwei bis 32 Platten verbunden werden.

Erstellt werden RAID-Verbände im Plattenmanager von NT. Im Falle von Stripesets ist es erforderlich, auf jeder zu verwendenden Platte einen genügend großen freien (*nicht* partitionierten!) Speicherbereich anzugeben. Bei Spiegelung oder Duplexing muß das Original bereits vorhanden sein.

Falls in einem Stripeset mit Parität eine Festplatte ausfällt, kann sie entnommen und ersetzt werden. Auf der neun Platte ist dann ein entsprechend großer, freier Bereich anzugeben (nochmals: *keine* Partition!) und der Punkt *Stripeset regenerieren* anzuwählen. Im Falle einer Spiegelung oder einer Duplizierung ist der alte verbund zunächst aufzulösen und dann erneut herzustellen.

Es bleibt anzumerken, daß nur Mirroring als Sicherung der System- oder Bootpartition in Frage kommt; im Falle der anderen Level ist für den Zugriff ein entsprechender, im System verankerter Treiber erforderlich. Und der liegt auf der zu bootenden Partition…

Im Falle eines Ausfalles bei Level 1 wird für den Start des Systemes eine sogenannte *Bootdiskette mit Fehlertolleranz* benötigt. Dies ist eine gewöhnliche Bootdiskette, auf der die ARC-Pfade entsprechend angepaßt wurden.

4.2.5 Konvertierung

Es mag vorkommen, daß eine der in einem System befindlichen Partitionen ein FAT-Partition ist. Ist gibt gute Gründe, dies zu ändern (siehe Abschnitt 4.1.2, S. 46). Doch NT 4.0 bietet dafür kein grafisches Werkzeug. Wer sich jedoch nicht scheut, mit der Kommandozeile zu arbeiten, hat die Möglichkeit, eine solche Platte zu konvertieren.

Der entsprechnde Befehl lautet:

`convert` *`Laufwerk`* `/FS:NTFS`

Dabei bezeichnet *`Laufwerk`* den Laufwerksbuchstaben (mit `:`). Der Parameter `/FS:NTFS` ist ein Überbleibsel aus der NT 3.51-Zeit, als neben FAT und NTFS auch noch das von IBM und Microsoft gemeinsam entwickelte HPFS[11] eingesetzt wurde. Er wurde lediglich aus Kompatibilitätsgründen beibehalten.

Eine Konvertierung von NTFS nach FAT ist mit den Windows NT 4.0 eigenen Werkzeugen nicht möglich.

4.3 Benutzer und Gruppen

Benutzer und Gruppen dienen unter anderem der Sicherheit eines Systemes. Jeder Benutzer, der an einem System arbeiten möchte, muß sich erst mit seinem Loginnamen anmelden. Um das zu können, benötigt er ein Benutzerkonto auf dem entsprechenden Rechner, bestehend aus seinem Loginnamen und verschiedenen Einstellungen. Der Einfachheithalber wird dieses Konto in Zukunft als *Benutzer* bezeichnet.

Gruppen dienen der Zusammenfassung von Benutzern. Sie erleichtern das Zuweisen von Rechten an Benutzer.

Sowohl Gruppen als auch Benutzer können lokal oder Domänenweit sein. *Lokal* bedeutet, daß die sie für den Rechner gelten, auf dem sie erstellt wurden. Domänenweit bedeutet, daß sie in der gesammten Domäne gelten. Dementsprechend werden sie auf PDCs eingerichtet.

4.3.1 Der Schlüssel zu allem — die SID

SID steht für ***S**ecurity **ID**entifier*. Damit ist eine ziemlich lange Kennung gemeint, die jeder Resource eines Rechners zugewiesen wird. Sie dient der internen Verwaltung und setzt sich aus verschiedenen Werten zusammen.

Eine SID ist einmalig (unique). Ein Benutzer, der gelöscht und neu erstellt wird, hat danach eine neue SID.[12]. Gleiches gilt für Benutzer gleicher Namen auf unterschiedlichen Rechnern (oder unterschiedlichen Betriebsystemen).

Diese Eigenschaften der SID sind entscheidend für die Funktion von Windows NT. Ihr Verständnis ist Voraussetzung für das des gesammten Rechte- und Benutzerwesens.

4.3.2 Erstellung eines Benutzers

Benutzer werden mit Hilfe des Benutzermanagers erstellt. Dieser findet sich unter *Programme*, Unterpunkt *Verwaltung*. In der Mernüleiste muß unter dem Punkt

[11] High Performance File System.

[12] Der eine oder andere wird sich hier vielleicht an die unter UNIX verwendeten UIDs erinnert finden; hier ist bemerkbar, daß Windows NT 3.51 eine Entwicklung aus dem alten DEC-Unix war. . .

Benutzer der Unterpunkt *Neuer Benutzer* angewählt werden; daraufhin öffnet sich eine Eingabemaske.

Die ersten fünf Felder sind zur Texteingabe, darunter finden sich vier Checkboxen. Um einen Benutzer tatsächlich einzurichten sind nur das erste und die beiden letzten Textfelder sowie die Checkboxen erforderlich. Die Felder sind in einzelnem:

Benutzername: Dies ist der Loginname, mit dem sich der Benutzer anmeldet.

Vollständiger Name (optional): Hier wird für gewöhnlich der komplette Name des Benutzers angegeben.

Beschreibung (optional): An dieser Stelle kann zum Beispiel die Abteilung, welcher der Benutzer angehört, stehen.

Kennwort: Hier wird das Kennwort des Benutzers eingetragen.

Kennwortbestätigung: Zur Sicherheit muß das Kennwort einmal wiederholt werden.

Die Checkboxen haben die folgenden Funktionen:

Benutzer muß das Kennw. bei d. nächst. Anmeldung ändern: Die Bezeichnung steht für sich; In einigen Fällen werden für Benutzer nur verhälltnismäßig unsichere Standardpaßwörter eingesetzt (etwa wenn ungefähr 2000 Benutzer via Script eingerichtet werden). Hier ist es sinnvoll, wenn der Benutzer bei seiner ersten Anmeldung zur Änderung gezwungen wird.

Benutzer kann Kennwort nicht ändern: Dem Benutzer ist es unmöglich, sein Kennwort zu ändern. Auch das ist manchmal sinnvoll, etwa bei besonders lernschwachen Nutzern. Der Haken ist nicht in Verwendung mit dem vorhergegangenen möglich.

Kennwort läuft nie ab: Das Kennwort hat keine Zeitliche beschränkung und muß nicht geändert werden.

Konto deaktivieren: Das Konto kann nicht verwendet werden.

Daneben gibt es, je nachdem, ob es sich um eine Server oder eine Workstation-Installation handelt, noch verschiedene andere Punkte. Insbesondere gibt es dort das Feld *Gruppe*, in welchem sich eingeben läßt, welchen Gruppen ein Benutzer angehört.

4.3.3 Gruppen

Es ist prinzipiell möglich, für bestimmte Resourcen Benutzern bestimmte Rechte zu geben. Bei großen Benutzerzahlen kann das ausgesprochen nervig werden. Daher werden Benutzer in Gruppen zusammengefasst, und diese Gruppen werden dann den Resourcen zugewiesen. Es gibt einige vordefinierte Gruppen, etwa die Benutzer (hier sollten alle Benutzer drinn sein) oder die Administratoren.

Benutzer können Gruppen entweder bei ihrer Erstellung oder später durch Bearbeiten des Benutzerkontos zugewiesen werden. Eine andere Möglichkeit besteht darin, die Gruppen ansich zu ändern. Das geschieht ebenfalls im Benutzermanager. Erstellt werden können diese Gruppen mit dem in *Benutzer* gelegenen Punkt *Neue lokale Gruppe* (unter PDCs auch *Neue globale Gruppe*). Neben dem Gruppennamen und einer (optionalen) Beschreibung gibt es hier auch eine Liste der eingetragenen Mitglieder. Da können Benutzer, aber auch andere Gruppen[13] sein.

4.3.4 Benutzerrechte

Mit den Benutzerrechten sind in diesem Fall die Rechte eines Benutzers, sich an einem Rechner anzumelden oder bestimmte Aufgaben zu erfüllen gemeint. Der Ausdruck bezieht sich nicht auf Zugriffsrechte von Dateien.

Die Einstellungen dieser Rechte finden sich ebenfalls im Benutzermanager im Menüpunkt *Richtlinien*, Unterpunkt *Benutzerrechte*.

Hier findet sich eine Liste von Rechten und zu jedem angewählten Recht eine Liste von Berechtigten. Wer in letztgenannter Liste steht, hat dieses Recht, wer nicht, der nicht. (Es verhällt sich mit den Rechten wie mit der Jungfräulichkeit: ganz oder garnicht. . .) Als Berechtigte kommen Benutzer oder Gruppen in Frage.

4.3.5 Domänenweite Benutzer und Gruppen

Bisher wurden lediglich Benutzer und Gruppen für lokale Maschienen betrachtet. Auf einem PDC hingegen gibt es auch die Möglichkeit, Domänenbenutzer und sogenannte globale Gruppen anzulegen.

Domänenbenutzer sind Benutzer, die sich an allen Rechnern einer Domäne anmelden können. Sie sind auf den lokalen Rechnern automatisch Mitglieder der globalen Gruppe *Domänenbenutzer* und haben alle Rechte, die dieser Gruppe zustehen.

Um Verwirrungen auszuschließen, werden in Zukunft lokale Gruppen mit

`Rechnername\Gruppenname`

und globale Gruppen mit

`Domänenname\Gruppennname`

bezeichnet. Diese Konventionen können bei Bedarf auch auf Benutzer und sogar Rechner ausgeweitet werden und entsprechen zudem der Darstellung dieser Gruppen, Benutzer und Rechner in den verschiedenen Windows NT Verwaltungsprogrammen.

Gelegendlich ist es erwünscht, daß ein Domänenbenutzer zwar innerhalb der Domäne nichts weiter als ein Domänenbenutzer ist, auf „seinem“ Rechner aber über administrative Rechte verfügt. Das läßt sich einrichten, indem der globale

[13] Nur, um es ganz klar zu sagen: damit sind die Mitglieder dieser Gruppen ebenfalls Mitglieder in der neuen Gruppe.

Benutzer (also `Domäne\Benutzer`) der Gruppe der lokalen Administratoren des entsprechenden Rechners (also der Gruppe `Rechner\administratoren`) hinzugefügt wird. Es ist dringend nötig, daß dieses wirklich mit dem *Domänenbenutzer* passiert; wird ein lokaler Benutzer gleichen Namens der Gruppe hinzugefügt, so hat dies keine Auswirkungen auf die Rechte des Domänenbenutzers. (Das liegt unter anderem an den unterschiedlichen SIDs, siehe 4.3.1, S. 53).

Globale Gruppen sind domänenweite Gruppen. Der normale, von Micorsoft vorgesehene Weg der Resourcenverwaltung besteht darin, Benutzer einer Domäne in globalen Gruppen zusammen zu fassen, auf verschiedenen, Resourcen verwaltenden Rechnern lokale Gruppen für die Verwaltung der Ressourcen einzurichten und die globalen Gruppen in diese lokalen Gruppen einzutragen. Das ganze wird mancherorts auch als BGLR-Prinzip[14] (für ***B**enutzer **G**lobal **L**okal **R**esourcen*) bezeichnet. Da dieser Satz vermutlich mehr trübt als klärt, hier ein Beispiel:

In der Domäne `anime` soll ein Drucker, angeschlossen an den Rechner `riding_bean`, für alle Benutzer der Abteilung *Marketing*, die Mitglieder der AbteilungFührungsstab und die Benutzer `ahaddock` und `fkieselwetter` freigegeben werden. Der Domänencontroller der Domäne ist `akira`.

Folgendes Vorgehen empfielt sich:

1. Auf dem PDC `akira` wird die globale Gruppe `darf_drucken` eingerichtet.

2. Es ist ausgesprochen wahrscheinlich, daß es für die beiden Abteilungen *Marketing* und *Führungsstab* bereits Gruppen gibt. Falls das der Fall ist, werden diese beiden Gruppen der Gruppe `anime\darf_drucken` hinzugefügt. (Anderenfalls können entweder alle Mitglieder der Abteilungen hinzugefügt oder aber — was die Übersicht erhöhen würde — die beiden Gruppen erstellt und gefüllt werden.)

3. Die Domänenbenutzer `ahaddock` und `fkiesewetter` werden der globalen Gruppe `darf_drucken` hinzugefügt. Damit sind die Konfigurationen auf dem PDC abgeschlossen.

4. Auf dem Rechner `riding_bean` wird die lokale Gruppe `drucken` eingerichtet.

5. Der Gruppe `ridnig_bean\drucken` werden die Rechte, den Drucker zu benutzen, gegeben.

6. Die globale Gruppe `darf_drucken` wird der lokalen Gruppe `drucken` zugewiesen.

Falls die Gruppen für die Marketing- und die Führungsstabsabteilung bereits existieren, ist es auch möglich, diese nicht der Gruppe `darf_drucken`, sondern direkt die lokale Gruppe `drucken` zuzuweisen.

[14] Im Englischen entsprechend UGLR.

	Lokale Gruppe	**Globale Gruppe**
Geltungsbereich	Nur auf dem Rechner, auf dem sie eingerichtet ist	In der gesammten Domäne
Inhalt	Lokale und globale Gruppen, lokale Benutzer und Domänenbenutzer	Domänenbenutzer und globale Gruppen
Einrichtung / Verwaltung	Auf lokalen Rechnern	Auf PDCs

Tabelle 4.1: Eigenschaften globaler und lokaler Gruppen

Eine Gegenüberstellung lokaler und globaler Gruppen findet sich in Tabelle 4.1, S. 57. Der Sinn und Zweck dieses Prinzipes wird erst im Zusammenhang mit vertrauten Domänen (siehe Abschnitt 4.8.2, S. 77) ersichtlich.

4.4 Dateizugriffsberechtigungen

Nicht jeder Benutzer soll immer auf alle Dateien zugreifen können. Nicht, wenn er direkt am Rechner sitzt, und über das Netz schon mal gar nicht. Windows NT stellt für die Regulierung dieser Zugriffe zwei verschiedene Berechtigungsarten zur Verfügung, die Netzwerkfreigabe und die durch das NTFS-Dateisystem gegebenen Mechanismen.

4.4.1 Die Freigabe

Soll ein Verzeichnis im Netzwerk verfügbar sein, so muß es freigegeben werden. Dies geschiet etwa im Explorer; ein Rechtsklick auf ein Verzeichnis bietet die Möglichkeit der Freigabe.

Neben einem Freigabenamen gibt es hier auch die Möglichkeit, Berechtigungen zu vergeben. Theoretisch kann einer Ressource jeder verfügbare Benutzer oder Domänenbenutzer zugewiesen werden. Praktisch wird das meistens über Gruppen realisiert.

Jede hier eingetragene Gruppe (und jeder hier eingetragene Benutzer) kann eines der folgenden vier Berechtigungen haben:

Kein Zugriff: Der Benutzer kann unter gar keinen Umständen auf das Verzeichnis zugreifen. Er kann es auch dann nicht, wenn er durch eine andere Gruppe andere Berechtigungen hat.

Nur Lesen: Der Benutzer darf das Verzeichnis (und dessen Inhalt) lesen, sprich: er darf sich die in dem Verzeichnis liegenden Daten ansehen, hinein wechseln und die Dateien öffnen. Diese Berechtigung beinhaltet auch das Ausführen von in dem Verzeichnis liegenden Programmen.

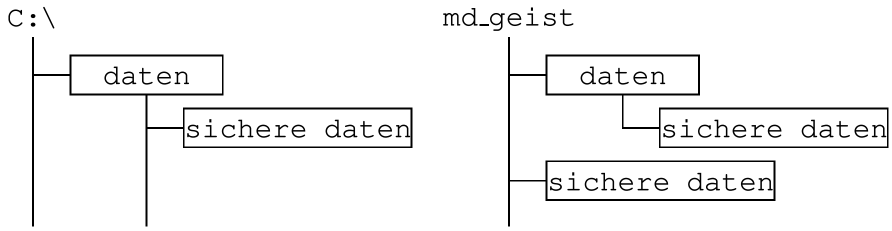


Abbildung 4.3: Die Freigabe des Rechners `md_geist.anime`

Ändern: Diese Berechtigung beinhaltet die *Nur Lesen*-Berechtigung. Als Ergänzung können die Dateien umbenannt, gelöscht und bearbeitet werden. Das schließt auch die Änderung der Dateiattribute mit ein.

Vollzugriff: Neben den Berechtigungen *Ändern* und *Nur Lesen* dürfen Inhaber dieser Berechtigung auch die Berechtigungen der Freigabe ändern.

Diese Berechtigungen greifen natürlich nur, wenn ein Benutzer über das Netzwerk auf das Verzeichnis zugreift. Sitzt der Benutzer lokal am Rechner oder ist er über Telnet oder ähnliches auf dem Rechner eingeloggt, greifen sie nicht.

Ein weiterer zu beachtender Faktor ist der *Einstiegspunkt*. Es zählen immer die Berechtigungen des benutzten, und ausschließlich die. In Abbildung 4.3, S. 58 wurde auf dem Rechner `md_geist.anime` der Ordner `daten` mit *Ändern* freigegeben, der darunterliegende Ordner `sichere daten` nur mit *Lesen*. Auf der rechten Seite ist die Darstellung im Netz zu sehen.

Wird nun auf den Ordner `\\md_geist\daten` zugegriffen, besteht die *Ändern*-Berechtigung. Bei Zugriff auf den Ordner `\\md_geist\sichere daten` besteht nur die *Lesen* Berechtigung. Falls der selbe Ordner jedoch den über den Pfad `\\md_geist\daten\sichere daten` angesprochen wird, bestehen die Berechtigungen des Einstiegspunktes, nämlich `\\md_geist\daten`. Somit haben die zugreifenden Benutzer plötzlich die *Ändern*-Berechtigung für den Ordner `sichere daten`.

4.4.2 NTFS-Berechtigungen

Das Dateisystem NTFS bietet für die darauf liegenden Daten eine Reihe von Berechten. Diese greifen *immer*. Da auch Verzeichnisse eine (wenn auch besondere) Art von Dateien sind, können auch diese mit Berechtigungen versehen werden. Diese haben hier geringfügig andere Auswirkungen.

Es gibt insgesammt sieben Berechtigungen:

R, Lesen: Die Lese- (**R**ead-) Berechtigung gibt einem Benutzer das Recht, den Inhalt einer Datei (oder die Dateien in einem Ordner) anzeigen zu lassen. Des weiteren kann er sich die Dateiattribute und die Berechtigungen ansehen.

	Dateien						Ordner					
Berechtigung	`r`	`w`	`x`	`d`	`p`	`o`	`r`	`w`	`x`	`d`	`p`	`o`
Anzeigen	x		x									
Lesen	x		x				x		x			
Hinzufügen		x	x									
Hinzufügen und Lesen		x	x					x	x			
Ändern	x	x	x	x			x	x	x	x		
Vollzugriff	x	x	x	x	x	x	x	x	x	x	x	x

Tabelle 4.2: Die Zusammensetzung der vordefinierten NTFS-Berechtigungen

`W`**, Schreiben:** Die Schreib (**W**rite-) Berechtigung erlaubt dem Benutzer, in Dateien zu schreiben oder in Ordnern neue Dateien anzulegen.

`X`**, Ausführen:** Die Ausführen (e**X**ecute-) Berechtigung gibt einem Benutzer zuzüglich zu den Möglichkeiten des *Lese*-Rechtes die Möglichkeit, Dateien (meistens Programme) auszuführen. Bei Ordnern kommt zu den unter *Lesen* aufgeführten Rechten noch das Ändern von Ordnern innerhalb des Ordners hinzu.

`D`**, Löschen:** Wie der Name schon sagt können hiermit Ordner und Dateien gelöscht (**d**elete) werden.

`P`**, Berechtigungen ändern:** Die Berechtigungsänderungsberechtigung (change **P**ermission) ermöglicht es dem Benutzer, die Berechtigungen einer Datei oder eines Ordners zu ändern. (Toller Satz, nicht wahr?)

`O`**, Übernahme des Besitzes:** Diese Besitzübernahme (take **O**wnership) ermöglicht es, sich eine Datei oder einen Ordner anzueignen.

Wer einen Ordner oder eine Datei erstellt, der ist automatisch der Besitzer und hat Vollzugriff. Administratoren können nromaler Weise immer den Besitz einer Datei bernehmen.

Normaler Weise wird nicht mit diesen Berechtigungen gearbeitet. Statt dessen werden einige aus ihnen zusammengefügte Berechtigungen verwendet. Sie setzen sich wie in Tabelle 4.2, S. 59 aufgeführt zusammen.

Neben diesen Berechtigungen gibt es noch *Keine Berechtigung*. Diese ist ***ausgesprochen*** restriktiv. Ebenso wie bei den Freigabeberechtigungen verhindert sie jede auch durch andere Gruppen zustande kommende Berechtigung.

Wird eine Datei von einem Ordner in einen anderen mit anderen NTFS-Berechtigungen kopiert, so erhällt sie automatisch die NTFS-Berechtigungen des neuen Ordners; dies ist insich logisch, denn diese Datei wird in dem neuen Ordner neu erstellt. Ander sieht es bei Verschieben aus; befindet sich der Ordner auf der selben Partition, so behällt die Datei ihre Rechte. Befindet er sich auf einer anderen Partition, so erhällt sie die Rechte des neuen Ordners.

Auf den ersten Blick erscheint das unlogisch. Doch bei Betrachtung der tatsächlichen Vorgänge wird dieses Verhalten klar: Befindet sich der neue Ordner auf einer anderen Partition, so wird die Datei zunächst kopiert und danach am Ursprungsort gelöscht. Befindet er sich auf der gleichen, so sparrt Windows NT Zeit, indem es die Datei nicht verndert, sondern lediglich einen anderen Ort für ihre Darstellun einträgt. (Für Linux-Benutzer: Es setzt praktisch einen Hardlink und löscht danach den alten.)

4.4.3 Effektive Berechtigungen

Es stellt sich die Frage, wie die verschiedenen Berechtigungen mit einander arbeiten. Hierzu gibt es drei Merksätze, die im folgenden etwas genauer betrachtet werden.

Die schärfste Einschränkung zieht.

Eine Kombination aus Freigabe- und NTFS-Berechtigungen läßt sich mit einem mittelalterlichen Markt vergleichen. Die Freigabe versinnbildlicht das Stadttor. Die NTFS-Berechtigungen entsprechen den Launen der Händler. Wer nicht durch das Stadttor kommt, der kann auch nichts kaufen; egal, ob die Händler ihn mögen oder nicht. Wer reinkommt, aber bei allen Händlern unten durch ist, dem nützt das Hereinkommen auch nichts.[15]

Mathematisch gesprochen sind die effizienten Rechte die Schnittmenge aus der Freigabe und den NTFS-Rechten. Hat beispielsweise ein Benutzer in der Freigabe *Lesen-* und in der NTFS-Berechtigung *Vollzugriff*, dann kann er bei Remotezugriff nur lesen. Hat er in der Freigabe *Voll-*, in der NTFS-Berechtigung aber nur *Lese-*Zugriff, kann er ebenfalls nur lesen.

In diesem Zusammenhang wird gelegendlich gesagt, es empfehle sich, die Freigabe stets auf *Vollzugriff* zu stellen und alle Rechte-Geschichten über die NTFS-Berechtigungen zu regeln. Doch gelegendlich kommt es vor, daß auch die Freigabeberechtigung Sinnvoll ist. Hier ein paar nützliche Einsatzmöglichkeiten:

- Bevor das Verzeichnis überhaupt freigegeben wird, sollten die NTFS-Berechtigungen erst einmal lokal geprüft werden. (OK, das ist eher ein Weglassen von Freigabeberechtigungen. . .)

- Es kann sehr gut sein, daß ein Administrator zwar von Außerhalb bestimmte Dateien einsehen können muß, es aber nicht erforderlich ist, daß er die Programme dort auch verändert (geschweige denn ausführt). Andererseits kann es durchaus sein, daß er genau das gelegendlich tun muß; aus Sicherheitsgründen ist es unter diesen Umständen sicherer, das nur lokal zu erlauben.

- Falls aus irgend einem dummen Grund das freigegebene Verzeichnis auf einer FAT-Partition liegt, führt für eine Reglementierung kein Weg an den Freigabeberechtigungen vorbei.

[15] Dieses Beispiel bezieht sich nur auf die Zugriffsverbote, da der Käufer in diesem Fall nur zwei Arten von Rechten hat: Kaufen oder nicht kaufen.

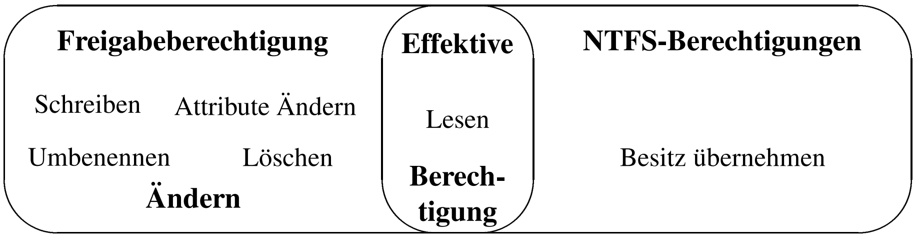


Abbildung 4.4: Die Berechtigungen des Adminitrators `mstringray`

Kein Zugriff bedeutet KEIN ZUGRIFF

Wenn in irgend einer Gruppe das Berechtigungsverbot *kein Zugriff* auftaucht, dann hat der Benutzer auch keinen Zugriff. Er kann in anderen Freigabe- oder NTFS-Berechtigungen Vollzugriff bekommen, doch falls er irgend wo das Verbot auftaucht kommt er nicht an die Ressource.

Dateirecht bricht Verzeichnisrecht

Dieser Merksatz gilt *nur* für NTFS-Berechtigungen, Freigabeberechtigungen für Dateien gibt es nicht. Für die Freigabe wird in diesem Fall also Zugriff vorausgesetzt.

Falls ein Benutzer zwar kein Recht hat, sich den Inhalt eines Ordners anzusehen, in diesem Ordner jedoch eine Datei liegt, für die er das *Ausführen*-Recht besitzt, kann er diese Datei tatsächlich ausführen. Da er den Ordner nicht einsehen kann, muß er die komplette URL angeben. Die Rechte der übegeordneten Verzeichnisse sind in diesem Falle vollkommen egal.

4.4.4 Beispiele für effektive Rechte

Um die Bedeutung der Rechte und ihr Zusammenspiel etwas zu verdeutlichen, folgen hier ein paar Fallbeispiele.

1. Die Benutzerin `romanova` ist Mitglied in den globalen Gruppen `stuff`, `ad_police` und `sabre_nights`.

   Für das Verzeichnis `\information`, gelegen auf dem Server `bubblegum_crisis`, hat die Gruppe `stuff` nur die Freigabeberechtigung *Lesen*, `ad_police` hat überhaupt keine Freigabe und `sabre_nights` verfügt über die Freigabeberechtigung *Ändern*. Die NTFS-Berechtigungen für `sabre_nights` ist *Hinzufügen und Lesen*, `stuff` darf nur *Lesen*. `ad_police` wurde weiterhin nicht beachtet.

   Die zum Tragen kommende Freigabeberechtigung ist *Ändern*. Da es innerhalb von `romanovas` Berechtigungen kein Verbot gibt, ist es das höchste und somit geltend. Mit diesem Recht könnte sie Dateien lesen, schreiben, löschen und die Attribute verändern.

Die zum Tragen kommende NTFS-Beberechtigung ist *Hinzufügen und Lesen*, da es die höchstwertigste Berechtigung ist. Mit dieser Berechtigung kann sie ebenfalls Dateien lesen und schreiben, aber nicht löschen.

Als Endergebnis kann `romanova` also Datein lesen und schreiben.

2. Die Benutzerin `pasagiri` ist ebenfalls in der Gruppe `sabre_nights`. Diese hat auf das auf dem Server `bubblegum_crisis` gelegen Verzeichnis `Werkstatt` die Berechtigung *Lesen*. Da `pasagiri` dessen Besitzer verärgert hat, wurde sie dort explizit eingetragen und mit dem Verbot *Kein Zugriff* versehen.

   Durch diesen Eintrag ist es vollkommen egal, was die anderen Gruppen ihr an Rechten verschaffen, sie kommt nicht auf den Server. Würde sie sich allerdings *direkt* an dem Rechner einloggen, dann wäre diese Sperre egal; Freigaben ziehen schließlich nur bei Remote-Zugriffen, und so hätte sie die gleichen Rechte wie `romanova`.

3. Auch die Administratorin `sstingray` ist in der Gruppe `sabre_nights`. Außerdem hat sie auf `bubblegum_crisis` die NTFS-Berechtigung *Vollzugriff*. Wenn sie direkt an dem Server sitzt, hat er *Vollzugriff*. Greift er über das Netzwerk zu, ist es nur ändernder Zugriff.

4. Die Benutzerin `lozaki` ist in den Gruppen `stuff`, `boss` und `dau`. Auf dem PDC `akira.anime` hat die Gruppe `stuff` keine Berechtigungen und `boss` *Vollzugriff*. Die NTFS-Berechtigung für `boss` ist ebenfalls *Vollzugriff*. Die Gruppe `dau` hingegen hat die NTFS-Berechtigung *Kein Zugriff*.

   Die Freigabe gibt `lozaki` insgesammt *Vollzugriff* — `stuff` und `dau` haben keine Freigabeberechtigungen und fallen nicht ins Gewicht. Die NTFS-Berechtigungen sind jedoch *kein Zugriff*, da dieses Verbot alles andere überlagert. Somit hat `lozaki` keine Möglichkeit, Schaden am PDC anzurichten.

5. Der Administrator `mstringray` verfügt für alle Dateien auf dem Server `bubblegum_crisis` über die NTFS-Rechte *Lesen* und, für Notfälle, *Besitz übernehmen*. Durch seine Mitgliedschaft in der Gruppe der Domänenadministratoren hat er zudem die Freigabeberechtgung *Ändern*. Als effektives Recht bleibt ihm bei den entsprechenden Dateien lediglich das Lese-Recht. Diese Beispiel wurde in Abbildung 4.4, S. 61 nochmals verdeutlicht.

4.5 Benutzerverwaltung

In Abschnitt 4.3, S. 53 wurde bereits grundsätzliches zur Erstellung von Benutzern gesagt. Neben den dort getroffenen Aussagen gibt es noch eine ganze Reihe weiterer Möglichkeiten, das Verhalten des Rechners dem Benutzer gegenüber zu steuern. Zudem kann die Erstellung von Benutzern durch die Benutzung von Standard-Benutzer vereinfacht werden.

4.5.1 Remote-Verwaltung

Einige der hier aufgeführten Verwaltungsschritte ergeben nur Sinn, wenn sie auf einem DC ausgeführt werden. Entsprechend werden sie auch nur in der Benutzerverwaltung des DCs angeboten.

Nit den Servertools stellt Microsoft einige Werkzeuge zur Verfügung, um von einer Workstation aus den zughörigen DC verwalten zu können. Die Servertools befinden sich auf der Windows NT Workstation CD in dem Verzeichnis:

`\clients\srvtools\winnt`[16]

Die Installationsroutine macht nicht anderes, als eine Reihe von Dateien in das Systemverzeichnis zu kopieren. Um die Programme einfacher aufrufen zu können, empfielt sich das Anlegen verschiedener Links. Die neuen Programme sind:

`dhcpadmn.exe`: Programm zur Verwaltung des DHCP-Servers.

`poledit.exe`: Programm zur Administration der domänenweiten Sicherheitsrichtlinien.

`rasadmin.exe`: Verwaltungsprogramm für RAS-Einstellungen.

`rplmgr.exe`: Der Remote Boot Manager.

`srvmgr.exe`: Das Servermanagement.

`winsadmn.exe`: Programm zur Verwaltung des WINS-Servers.

`usrmgr.exe`: Verwaltungsprogramm für Domänenbenutzer.

4.5.2 Die Kontorichtlinien

Zu den Einstellungen der Benutzererweiterung lassen sich über die Kontorichtlinien einige weitere Verhaltensregeln einsetzen. Diese Richtlinien finden sich im Benutzermanager unter *Richtlinien*, Unterpunkt *Konto*. Folgende Dinge können hier eingestellt werden:

Maximales Kennwortalter (links): Entweder ist ein Kennwort immer gültig, oder seine Gültigkeitsdauer kann in Tagen angegeben werden.

Minimales Kennwortalter (rechts): Entweder kann das Kennwort immer (auch sofort), oder frühstens nach einer anzugebenden Anzahl an Tagen geändert werden.

Minimale Kennwortlänge: Hier kann angegeben werden, wie viele Zeichen ein Kennwort lang sein muß. Als Minimaleinstellung kann auch *leeres Kennwort zulassen* angegeben werden. Das ist gleichbedeutend mit der Länge 0.

[16] Es gibt sie auch für Windows 9x, dort funktionieren sie aber nur eingeschränkt.

Kennwortzyklus: Oftmals ist es sinnvoll, nicht zu erlauben, stets das gleiche Paßwort zu verwenden. Falls keine Paßwortchronik geführt wird, kann das aber getan werden (weil das System ja gar nicht weiß, welches Paßwort als letztes oder vorletztes benutzt wurde). Wird jedoch eine Anzahl von aufzubewahrenden Paßworten angegeben, kann ein Kennwort erst wieder benutzt werden, wenn es nicht mehr in der Liste steht. (Mit anderen Worten: werden drei Paßwörter aufbewahrt, so kann das erste Paßwort erst wieder als viertes eingesetzt werden.)

Konto sperren: Dieses ist eine recht detailierte Angabe, die bestimmt, wie sich das System im Falle falscher Paßworteingaben verhällt. Falls es nicht gesperrt wird, ist das egal. Anderenfalls kann angegeben werden, nach wie vielen Fehlangaben das System gesperrt wird. Dabei gibt *Zurücksetzen nach* die Zeit nach einem Versuch an, nach welcher die Zählung der Versuche wieder zurückgesetzt wird. Die *Dauer der Sperrung* gibt an, wie lange nach den Fehleingaben das System für diesen Benutzer geperrt wird. Entweder für immer (der Administrator muß die Sperrung aufheben) oder für eine bestimmte Zahl von Tagen.

Remote-Benutzer bedingungslos. . . : *. . . vom Server bei Ablauf der Anmeldezeit trennen*,[17] sobald die unter *Zeit* (siehe 4.5.3, Seite 64) angegebene Zeit abgelaufen ist, wird der Benutzer getrennt.

Benutzer muß sich anmelden um das Kennwort zu ändern: Hier wird angegeben, wie sich das System bei Ablauf eines Kennwortes ohne Änderung durch den Benutzer verhällt. Falls das Kästchen gesetzt ist, ist der Benutzer danach gesperrt und der Administrator muß das Paßwort ändern (und ihn freischalten). Anderenfalls wird der Benutzer direkt nach seiner Anmeldung aufgefordert, sein Kennwort zu ändern.

4.5.3 Zeit und Raum

Es mag vorkommen, daß ein Benutzer sich nicht zu jedem Zeitpunkt anmelden können soll. Zudem ist es nicht imer erwünscht, daß er sich von *jedem* Rechner einloggt. Für das erste Problem gibt es im Benutzermanager auf der Eigenschaftskarte eines Benutzers den Punkt *Zeit*.[17] Hier kann (in schönster Windows-Manier) auf einer Tabelle bestimt werden, wann ein Benutzer sih anmelden darf; auf der X-Achse befinden sich dabei die Tageszeiten (in Stunden), auf der Y-Achse die Tage. Felder, in denen sich ein Benutzer anmelden kann, werden mit einem dicken Balken gefüllt, Felder, in denen er das nicht können soll, bleiben leer. Es ist zu beachten, daß der Benutzer, nachdem er eingeloggt ist, nach Ablauf seiner Anmeldezeit nicht getrennt wird. (Es sei denn, in den Kontorichtlinien steht etwas anderes, siehe 4.5.2, S. 64.)

[17]Dieser Punkt ist nur auf einem DC vorhanden.

Das zweite Kriterium wird über die Schaltfläche *Anmelden an*[17] gesteuert. Hier kann dem Benutzer entweder Zugang über *alle* Rechner, oder über bestimmte Rechner gewährt werden. Falls letzteres der Fall sein soll, können maximal 8 Rechner eingetragen werden, von denen aus das der Fall sein soll. (Mehr sind nicht möglich.)

In gewisser Weise damit verwandt ist die Schaltfläche *RAS*. Das Steht für ***R**emote **A**ccess **S**ervice* (also, frei übersetzt, Fernzugriffsdienst) und steht für die Möglichkeit, sich über ein Modem (oder ISDN) in einen Rechner einzuwählen und sich darüber am Netzwerk anzumeden. Ein mittels RAS in ein Netzwerk integrierter Rechner verhällt sich wie jeder andere Rechner auch, sein Modem (o. ä.) stellt dabei sozusagen seine Netzwerkkarte dar. unter dem entsprechenden Punkt läßt sich zunächst bestimmen, ob der Benutzer überhaupt das Recht haben soll, sich von Außerhalb einzuwählen. Falls das der Fall ist, kann zwischen drei Rückrufmodi gewählt werden:

Kein Rückruf: Der Benutzer muß die Verbindung selbst aufbauen und aufrecht erhalten.

Vom Anrufer festgelegt: Nachdem sich der Benutzer authentifiziert hat, wird er vom System unter einer von ihm anzugebenden Nummer für die weitere verbindung zurückgerufen.

Voreinstellung: Nachdem sich der Benutzer authentifiziert hat, wird er vom System unter der hier angegebenen Numer zurück gerufen.

Näheres zur Einrichung von RAS findet sich in Abschnitt 4.8.6, S. 81.

4.5.4 Heimverzeichnis und Anmeldescripte

Diese zwei Punkte finden sich unter der Schaltfläche *Profil*.[18] Bei allen können Pfadangaben gemacht werden. Bei diesen Pfadangaben können verschiedene Systemvariablen benutzt werden, von denen die wichtigste vermutlich `%username%` ist. Sie wird bei Ansprache der Pfade durch den Namen des aktuellen Benutzer ersetzt. Die Sinnhaftigkeit diesesr Variablen wird in Abschnitt 4.5.6, S. 67 deutlich.

Der unterste Punkt dabei ist das Basis- oder Heimverzeichnis. Hierbei hanmdelt es sich um ein Verzeichnis, in welchem der Benutzer all seine Daten speichert.[19] Es kann entweder lokal oder Netzweit angegeben werden. In letztgenannten Fall wird es beim Start mit einem ebenfalls anzugebenden Laufwerk verbunden. Die Angabe erfolgt über den UNC-Pfad. (Natürlich muß es auf dem angegebenen Rechner auch tatsächlich eine solche Freigabe mit Vollzugriff für alle betroffenen Benutzer geben…) Eine mögliche Angabe wäre zum Beispiel:

`\\bubblegum_crisis.anime\home\%username%`

[18] Der eigentlich namensgebende Punkt *Benutzerprofil* befindet sich ebenfalls dort, hat aber wegen seiner Komplexität einen eigenen Abschnitt bekommen.

[19] UNIX-Benutzer fühlen sich hier vielleicht an das `/home`-Verzeichnis erinnert.

Die Erfahrung hat gezeigt, daß es das Sicherste ist, das Heimverzeichnis bereits bei der Erstellung eines Benutzers anzugeben; unter diesen Umständen wird es automatisch in der Freigabe erstellt. Soll es im nachinein angelegt werden, kann es manchmal — je nach Servicepack, installierten Programmen und Tagesform des Netzes und Rechners — zu ausgesprochen unangenehmen Überraschungen kommen.

Bei dem Anmeldeskript handelt es sich um eine Batch-Datei, die bei Einloggen des Benutzers ausgeführt werden. Hier können alle Befehle eingesetzt werden, die es in der Kommandozeile von NT 4.0 gibt. Die interessantesten dürften die Befehle der `net`-Familie sein. Mittels `net use` können beispielsweise Netzlaufwerke verbunden werden. Für gewöhnlich wird das Verzeichnis

`$systemroot$\system32\repl\import\scripts`

dafür genutzt, alle Einträge unter *Anmeldescript* sind relativ zu dieser Pfadangabe. Wird statt dessen ein UNC-Pfad in Form von

`\\`*`Rechner`*`\`*`Script`*

angegeben, wird in der Freigabe `netlogon` auf dem jeweiligen Rechner nachgesehen. Diese Freigabe sollte normaler Weise eben jenes Verzeichnis auf dem anderen Rechner sein. Sie kann bereits wärend der Anmeldung (und vor der Authentifizierung) angesprochen werden.

4.5.5 Benutzerprofile

Benutzerprofile speichern die individuellen Einstellungen eines Benutzers (etwa die Farbe seines Desktops, verschiedene Einstellungen, seine persönlichen Programme und so weiter) ab. Grundlegend kann zwischen drei Arten von Benutezrprofilen unetrschieden werden:

Lokale Benutzerprofile: Dieser Benutzerprofile liegen lokal auf den einzelnen Rechnern und können sich unterscheiden.

Servergepeicherte Benutzerprofile: Diese Profiele liegen auf einem Server und werden bei der Anmeldung eines Benutzers an die Domäne von dort geholt. Das hat zur Folge, daß der Benutzer auf jedem Rechner, auf dem er sich anmeldet, die gleiche Umgebung vorfindet.

Verbindliche Benutzerprofile: Diese Profile sind eine besondere art von serverbasierten Profilen. Auch sie werden bei ejder Anmeldung vom Server geladen, und auch in ihrem Fall hat der Benutzer stets die gleiche Umgebung. Er kann sie aber nicht ändern.

Ein lokales Benutzerprofil wird automatisch erstellt, sobald sich ein neuer, angemeldeter Benutzer abmeldet. Seine Einstellungen werden in dem Ordner `%systemroot%\profiles\%username%` abgespeichert. Bei jeder Abmeldung werden seine neuen Einstellungen dort hinein gechrieben.

Falls aus irgend einem Grund ein Benutzer als Anfangsprofil das eines anderen haben möchte, gibt es eine einfache Methode, das zu realisieren; in der Systemsteuerung, Unterpunkte *System*, gibt es die Möglichkeit, Benutzerprofile zu kopieren. Als Zeil muß das Verzeichnis angegeben werden, in welchem das Profil liegen soll, also `%systemroot%\profiles\%username%`. Danach muß unter Profileigenschaften noch angegeben werden, daß der Benutzer das Profil auch benutzen darf.

Um ein servergespeichertes Profil zu erstellen, muß das Verzeichnis, in dem es auf dem Server liegen soll, mit Vollzugriff für Domänenbenutzer freigegeben werden. Die weitere Konfiguration erfolgt auch hier im Benutzermanager auf der Karte des jeweiligen Benutzers. Wiederum ist *Profil* die richtige Schaltfläche. Unter dem Punkt *Pfad für Benutzerprofil* kann der entsprechende Pfad eingetragen werden, meistens `\\`*`Rechner`*`\profile\%username%`.Sobald der Benutzer sich abmeldet, wird das Profil in das angegebene Verzeichnis geschrieben. Auch hier funktioniert die Einrichtung bei Erstellung am besten.

Das Kopieren eines Profiles funktioniert auch hier; der Vorgang muß entsprechend auf dem Server geschehen, der diese Profile enthällt.

Um aus einem servergespeicherten Profil ein verbindliches zu machen, reicht es aus, die Datei `NTUser.dat` in `NTUser.man` (für **MAN**datory) umzubenennen. Diese Datei enthält di Registry-Einträge des Profiles und wird durch diesen Vorgang schreibgeschützt.

Bei den servergespeicherten Profilen stellt sich eine Frage: Was passiert, wenn der Server zur Anmeldezeit nicht verfügbar ist?

Das System sieht zunächst nach, ob es ein lokales Profil des Benutzers gibt. Falls ja, wird dieses benutzt. Falls nicht, wird das Standardprofil genommen (und bei Abmeldung des Benutzers gespeichert).

Falls nun bei der nächsten Anmeldung am selben Rechner der Profilserver wieder da ist, kommt eine Meldung, daß das lokale Profil neuer ist als das servergespeicherte. Der Benutzer wird gefragt, welches er benutzen möchte. Egal, wie er sich entscheidet, sein tatsächlich benutzes Profil wird bei seiner Abmeldung auf dem Server gespeichert. (Das funktioniert natürlich *nicht*, wenn das servergespeicherte Profil ein verbindliches ist.)

Profile können übrigens auch Gruppen zugewiesen werden; dann gelten sie für alle Gruppenmitglieder, zusätzlich zu den eigenen Profilen.

4.5.6 Benutzer und Gruppen verwalten

Unter *Verwalten* wird in diesem Fall der Vorgang des Erstellens, Kopierens, Umbenennens und Löschens verstanden. Die „normale“ Erstellung wurde bereits in Abschnitt 4.3, S. 53 behandelt.

Um einen neuen Benutzer zu erstellen ist es nicht unbedingt notwendig, ihn vollkommen neu zu erstellen. Tatsächlich wäre das in machen Fällen (etwa wenn es wirklich *viele* Benutzer einrichten soll) eher nervig. Auch bei Gruppen kann es sein, daß eine neu zu erstellende Gruppe fast identisch mit einer anderen sein soll.

Im Benutzermanager gibt es die Möglichkeit, einen Benutzer oder eine Gruppe zu kopieren. Das passiert über *Benutzer* Unterpunkt *Benutzer kopieren* oder die Taste `<F8>`. Kopiert wird immer der Benutzer oder die Gruppe, die gerade aktiv ist. Ihre Eigenschaftkarte wird eröffnet, und bis auf den Namen und das Paßwort (die nicht eingetragen sind) gleichen alle Eintragungen denen des Originals. In diesem Fall zahlt es sich aus, mit der Systemvariable `%username%` gearbeitet zu haben. Denn dann müssen die entsprechenden Pfade nicht mehr an den Benutzer angepaßt werden.

Aus diesem Grund haben viele Adminsitartoren auch einen Default- oder Standard-Benutzer, von dem sie bei Bedarf einfach eine Kopie erstellen. Aus Sicherheitsgründen rät es sich an, diesen Benutzer (oder die Gruppe) zu deaktivieren.

Zum Umbenennen einer Gruppe oder eines Benutzers wird im selben Menüpunkt der Unterpunkt *Umbenennen* verwendet. Das hat vor allem den Vorteil, daß die Rechte des Benutzers oder der Gruppe erhalten bleiben, obwohl sie einen neuen Namen haben. (Die SID bleibt identisch.)

Um eine Gruppe oder einen Benutzer zu löschen kann entweder der entsprechende Unterpunkt des Menüpunkts *Benutzer* oder der Druck auf die `<ENTF>`-Taste verwendet werden.

4.5.7 Systemrichtlinien

Die Systemrichtlinien geben weitreichende Einschrankungsmöglichkeiten für Benutzer, Gruppen und Rechner. Wird eine Systemrichtlinine angewand, so überschreibt sie die Registry für den entsprechenden Bereich. Das kann zu üblen Nebeneffekten führen, etwa wenn sich die Registrierung für andere Benutzer nicht mehr in den Ursprunszustand bringen läßt.

Das Programm für die Erstellung und Verwaltung von Systemrichtlinien heißt `poledit.exe` (siehe Abschnitt 4.5.1, S. 63) und wird als Systemrichtlinieneditor (*System Policy Editor*) bezeichnet.

`poledit` kann entweder benutzt werden, um die Registry-Einträge direkt zu bearbeiten, oder um Richtlinien zu erstellen. Um die Registry direkt zu bearbeiten wird im Menü *Richtlinie* der Punkt *Registry öffnen* gewählt. Es handelt sich dann um die Registry des aktuellen Rechners und Benutzers. Über den Punkt *Verbinden* im selben Menü ist es möglich, sich mit einem anderen Rechner zu verbinden und dessen Registry oder die eines anderen Benutzers zu bearbeiten.

Microsoft rät ausdrücklich von der Verwendung dieser Methode ab [11, S. 165], die Verwendung von Richtlinien ist zum Einen übersichtlicher und zum anderen besser kontrollierbar.

Richtlinien funktionieren anders. Sie können für Gruppen, Benutzer oder Rechner erstellt werden und greifen nur dann, wen sich ein entsprechender Benutzer anmeldet.

Die Konfiguration ist in allen Fällen identisch: Vor jedem Punkt der Richtlinie (etwa *Ausblenden des Ausführen-Knopfes* findet sich ein kleines Kästchen, welches den Status der Richtlinie angibt. Dieses Kästchen kann weiß, druchkreuzt oder grau hinetrlegt sein. Ist es weiß wird die Funktion nicht ausgeführt. Ist es durchkreuzt, so wird sie ausgeführt. Ist es grau hinterlegt, so wird der ursprüngliche Wert der Registry benutzt.[20]

Grundlegend gibt es vier Arten von Richtlinien:

Standard Benutzer / Rechner: Diese Richtlinien greifen immer, wenn keine anderen zu Verfügung stehen.

Expliziter Rechner: Richtlinien, die bei Anmeldung an einen bestimmten Rechner aktiviert werden.

Expliziter Benutzer: Richtlinien für bestimmte Benutzer.

Gruppen: Diese Richtlinien greifen, falls sich ein Mitglied einer Gruppe anmeldet. Da ein Benutzer Mitglied mehrerer Grupen sein kan, können unter dem Menüpunkt *Optionen* die Priorotäten eingestellt werden.

Richtlinien werden in Dateien mit der Endung .pol gespeichert. Die für das System geltende und ausgeführte heißt ntconfig.pol und sollte sich in der Freigabe netlogon (siehe 4.5.4, S. 66) befinden.

Durch diese Konstellation können mehrer Richtlinien auf einen Benutzer zutreffen. Die Reinfolge, in der sie abgearbeitet werden, ist (beginnend mit dem Systemstart) folgende:

1. Der Rechner startet.

2. Falls eine explizite Rechner-Richtlinie für diesen Rechner existiert, wird diese auseführt.

3. Falls keine explizite Rechner-Richtlinie ausgeführt wurde, wird die Standard-Rechner-Richtlinie ausgeführt.

4. Der Benutzer meldet sich mittels Affengriff (<STRG>+<ALT>+<ENTF>) an. Durch diese Tastenkombination wird der Inhalt des Tastaturbuffers und allen nicht genutzen Speichers vollkommen gelöscht; das beugt Trojanern und anderen unfreundlichen Überraschungen vor.

5. Falls es für den Benutzer eine explizite Benutzerrichtlinie gibt, wird diese ausgeführt.

6. Die Gruppenrichtlinien werden nacheinander abgearbeitet. Die Richtlinien niederer Priorität zu erst, da die höheren sie ja später überschreiben.

7. Falls es keinen explizite Benutzerrichtlinie gibt, wird die Standard Benutzerrichtline ausgeführt.

[20] Logischer Weise gibt es bei einer direkten Bearbeitng der Registry nur zwei Möglichkeiten, angekreuzt oder nicht angekreuzt.

Application Layer
Kernel Layer
Hardware Abstract Layer (HAL)

Abbildung 4.5: Windows NT Schichten

Auf einem PDC können sich auch die Richtlinien für Windows 9x Rechner befinden. Diese müssen jedoch auf einem Windows 9x System mit Hilfe des dortigen `poledit.exe` erzeugt worden sein.

4.6 Architektur und Multitasking

Unter diesem Stichpunkt werden zwei Methoden zusammen gefaßt, die sich beide auf die Art und Weise, auf die ein Programm ausgeführt werden soll, beziehen. Das erste ist die Nutzung von NTVDMs, um alte DOS- oder Windows 3.1(1)-Programme auszuführen. Das zweite ist das Festlegen von Prioritäten für bestimmte Programme.

Beiden Punkten ist gemein, daß sie sich in mancherlei Beziehung auf die Architektur von Windows NT stützen. Diese unterscheidet sich in mancherlei Hinsicht von der bei Windows 9x verwendeten.

4.6.1 Das System

Grundlegend sind die Zugriffe des Systemes in drei Schichten unterteilt, wie in Abbildung 4.5, S. 70 zu sehen ist.

Wärend unter DOS, Windows 3.1(1) und Windows 9x alle Programme in der Lage waren, direkt auf die Hardware eines Rechners zuzugreifen (und so auch Geschwindigkeitsvorteile zu erzielen), sieht das unter NT anders aus. Die unterste Schicht des Betriebsystemes stellt die HAL. die Hardwareabstraktionsschicht. Sie regelt sämmtliche Zugriffe von Seitens des Betriebsystemes an die Hardware, direkte zugriffe des Systemes gibt es nicht. Darüber liegt die Kernelschicht, hier arbeitet der eigentliche Kern des Betriebsystemes mit seinen treibern und allem anderen. Das System ist das einzige, was auf dieser Ebene arbeitet und auf die HAL zugreifen kann. Erst darüber befindet sich eine Anwendungsschicht, auf der nun verschiedene Programme aufsetzen.

Ein weiterer Punkt ist das Multitasking; da ein Computer mit nur einem Prozessor definitivnur einen Prozess zur gleichen Zeit ausführen kann, wurde dieses über Zeitscheiben realisiert. Eine Zeitscheibe stellt sozusagen eine Reihe von Prozesen dar. Jeder Prozess hat dabei einen Abschnitt der Scheibe. Der Prozessor arbeitet jeden Abschnitt eine bestimmte Zeit lang ab, dann springt er zum nächsten. Aufgrund der hohen Geschwindigkeit, mit der dies passiert, kommt es dem Anwender so vor, als geschähen diese Prozesse gleichzeitig. (Da der Prozessor nach Abarbeitung der Reihe wieder am Anfang anfängt, wird sie oftmals als eine Uhrähnliche, runde Scheibe dargestellt. Daher stammt auch der Ausdruck Zeitscheibe.)

Die in der Anwendungsschicht laufenden Programe bilden in sich geschlosene Einheiten. Jede dieser Einheiten bekommt einen Abschnitt der Zeitscheibe zugewiesen. Somit laufen sie also quasi-gleichzeitig.

4.6.2 Abwärtskompatibilität durch NTVDM

Viele Windows 9x Programme greifen bereits auf Windows-APIs[21] anstatt direkt auf die Hardware zu. Daher gibt es auch keine Probleme mit ihrer Ausführung unter Windows NT. Spiele, die durch ihre hardwarenahe Programmierung Leistung gewinnen sollen, haben meistens ein Problem damit und laufen nicht.[22]

Bei DOS- und Windows 3.1(1) Programmen gibt es darüber hinaus noch ein weiteres Problem: Diese Programme sind 16-Bit-Programme. Um sie auszuführen benötigt NT die sogenannte NTVDM (***NT*** *Virtuell* ***DOS*** ***M****achine*). Diese emuliert sozusagen das 16-Bit-Betriebsystem. Für jedes gestartete DOS-Programm wird eine eigene solche NTVDM mit eigenem, von nur ihm benutztem Speicherbereich gestartet. Dadurch sind dies Programme untereinander Multitaskingfähig, und falls eines abstürzt, kann der Rest weiterlaufen. Bei Windows 3.1(1)-Programmen sieht die Sache etwas anders aus: die benötigen eine grafische Oberfläche. Sie werden alle in ein und der selben NVDM gestartet, sind damt nicht untereinander Multitaskingfähig und reißen sich bei Abstürzen gegenseitig mit. (Das Prinzip, diese Programme auszuführen, wird manchmal auch als WoW, ***W****indows* ***o****n* ***W****indows*, bezeichnet.) Um das zu verhindern kann den Programmen die explizite Anweisung gegeben werden, in eigenen Speicherbereichen (und eigenen NTVDMs) ausgeführt zu werden. Das geschieht entweder über ihr Icon (indem in den Eigenschaften *in eigenenem Speicherbereich ausführen* angeklickt wird) oder direkt in der Eingabeaufforderung mit Hilfe des Befehles `start` und dem Parameter `separate`. (Hiermit können DOS-Programme auch dazu gebracht werden, in ein und der selben NTVDM ausgeführt zu werden, wozu immer das gut sein mag. Der Parameter heißt dann `shared`.)

4.6.3 Programmprioritäten

Bildlich gesprochen umschreiben Prioritäten, wie groß der Abschnitt eines Programmes auf der Zeitscheibe ist. Anders gesagt: Je höher die Priorität einer Anwendung ist, desto mehr Zeit wird vom Prozessor für ihre Bewältigung bereitgestellt, und je mehr Zeit pro Zeitscheibendurchgang bereit gestellt wird, desto schneller ist die Aufgabe erledigt.

[21] Application Interface, die Schnittstelle zum System.

[22] Glücklicher Weise gibt es inzwischen für Doom 1+2 und Quake 1 Portierungen...

Anwendungs-Modus				
0	4	8	13	15
	Niedrig	Normal	Hoch	

Kernel-Modus		
16	24	31
	Echtzeit	

Tabelle 4.3: Prioritätsklassen

Windows NT kennt 32 Prioritätsstufen, von 0 bis 31. Sie wurden in Tabelle 4.3, S. 72 dargestellt. Ein Benutzer kann lediglich drei dieser Stufen ansprechen, nämlich *Niedrig*, *Normal* und *Hoch*. Diesen drei Stufen ist gemein, daß sie im sogenannten unteren Bereich der Prioritätsstufen liegen. Dieser bereich steht Programmen aus der Anwendungsschicht zu.

Administratoren können zusätzlich die Prioritätsstufe *Echtzeit* vergeben. Diese liegt im oberen Prioritätsbereich; dieser ist normaler Weise Programmen des Kernelmodus vorbehalten (also dem System allein). Programme dieser Prioritätsstufe werden in keiner Weise durch die Prioritäten des unteren Bereiches beeinflußt.

Es gibt Fälle, in denen normale Programme ebenfalls diese Prioritätsstufe benötigen. Dieses ist zum Beispiel bei CD-Brenn-Programmen der Fall. *Nero Burning ROM* schaltet bei Benutzung automatisch in den Echtzeitmodus um; daher können unter Windows NT nur Administratoren CDs brennen.

Die Prioritätsklassen können einzelnen Anwendungen auch von Hand zugewioesen werden. Eine Möglichkeit dafür liegt im Task-Manager. Hier lassen sich einzelne Prozesse anwählen und durch Rechtsklick in ihrer Priotität einstellen. Die andere besteht darin, ein Programm über den bereits im letzten Abschnitt erähnten Befehl `start` mit dem Parameter `/low`, `/normal`, `/high` oder `/realtimne` zu starten. Letzteres geht natürlich nur als Administrator.

4.7 Registry und ERD

Eines der kryptischsten Themen überhaupt stellt die Registry dar. In ihr speichert Windows NT[23] alle irgend wie wichtigen Einträge. Windows neigt dazu, seine Registry mit allem möglichen (und unmöglichen) Schrott vollzumüllen, und nicht immer ist es möglich, diesen Kram wider loß zu werden.

Für gewöhnlich nehmen Benutzer (und Administratoren) weiten Abstand da-

[23]Ebenso wie 9x, 2000 und XP.

von, die Registry direkt zu bearbeiten; wenn hier ein Fehler unterläuft, kann das System ganz schnell ganz platt sein. In einigen Fällen führt jedoch kein Weg an einem manuellen bearbeiten vorbei.

Die Registry besteht aus mehreren sogenannten *Hives*[24] Von denen werden jedoch nur drei gespeichert:

`HKEY_LOCAL_MACHINE`: Rechnerspezifische Einstellungen wie Hardwareinformationen.

`HKEY_USERS`: Informationen zu den einzelnen Benutzern.

`HKEY_CLASSES_ROOT`: Zuordnungen von Dateiendungen zu Programmen.

Diese drei Schlüssel befinden sich in Form einer Datenbank in den beiden Dateien `sam` und `sam.log`.[25] Alle anderen Einstellungen werden bei Systemstart und Anmeldung errechnet (wie etwa der Hive `HKEY_CURRENT_USER` für den aktuell angemeldeten Benutzer).

In diesen Hives befinden sich Schlüssel (die ihrerseits ebenfalls Schlüssel enthalten können). In denen stehen Variablen, denen Werte zugewiesen sind.

Um die Registry zu bearbeiten gibt es drei Möglichkeiten: zunächst geht es über den Richtlinieneditor (siehe Abschnitt 4.5.7, S. 68), oder über die Programme `regedit` und `regedt`. `regedit` ist ein 16-Bit-Programm und auch unter Windows 9x vorhanden. Sie bildet alle vorhandenen Schlüssel in einer Baumstruktur ab. `regedt` ist ein 32-Bit-Programm. Es bildet jeden Schlüssel in einem eigenen Baum in einem eigenen Fenster ab. Beide Programme haben ihre Vor- und Nachteile: `regedit` ist etwas übersichtlicher und läßt sich besser durchsuchen, insbesondere, weil die Suchfunktion nicht nur nach Schlüsseln, sondern auch nach Werten sucht. `regedt` hingegen verfügt über eine Sicherungsfunktion, mit der sich alte Registries wiederherstellen lassen. (Und natürlich ist sie als natives 32-Bit-Programm schneller und stabiler.)

Beide Programme verfügen über die Möglichkeit, sich mit einem andern Rechner zu verbinden und die dortige Registry zu verwüßten. Ebenso können in beiden die Registries (in mehr oder weniger lesbarer Form) als ASCII-Dateien exportiert werden. Eine solche ASCII-Datei kann mit einem beliebigen DOS-Editor bearbeitet und sogar wieder mit einem der Programme importiert werden. (Diese Art von Sicherung sollte besser immer vorgenommen werden, ehe an der Registry etwas verändert wird. . .)

Wenn ein Administrator tatsächlich die Registry zerschießt, ist meistens keine Rettung mehr möglich. Und neben Administratoren verändern auch Installationsprogramme die Registry, und nicht jeder Treiber arbeitet einwandfrei mit NT zusammen. Glücklicher Weise enthällt Windows NT zwei ausgesprochen nützliche Einrichtungen, die bei eienr zerschossenen Registry weiterhelfen.

[24] Zu deutsch: Bienenstöcke oder Haufen.

[25] Mit entsprechenden Programmen ist es möglich, diese Dateien auszulesen und so auch an Paßwörter zu kommen. Daher sollte der Zugriff auf sie gut gesichert sein.

Zum ersten speichert Windows bei der Einrichtung eines neuen Treibers die alte Registry ab. Sie läßt sich beim Systemstart unter dem Punkt *Letze funktionierende Konfiguration starten* aufrufen. Die Notsicherung wird erst durch die neue Konfiguraion ersetzt, wenn sich ein Benutzer erfolgreich am System anmeldet.

Zum zweiten gibt es die Möglichkeit, eine ERD (***E**mergency **R**epair **D**isc*) zu erstellen. Das geht mittels *Ausführen* und dem Befehl `rdisk`. Diese Diskette ist nicht startfähig, kann aber benutzt werden, um ein System mittels der Installationsdisketten von Windows NT 4.0 wieder herzustellen. Das Funktionsprinzip ist recht einfach: `rdisk` legt die entsprechenden Dateien zum Zeitpunkt seines Aufrufes im Verzeichnis `%systemroot%\repair` ab und verweist von der Diskette aus auf dieses Verzeichnis. Bei der Reparatur wird die Registry anhand dieser Daten wiederhergestellt.[26]

4.8 Netzwerke

Über Netzwerke unter Windows lassen sich problemloß ganze Bücher füllen. Das ist verschiedendlich auch schon passiert. Insbesondere, da heutzutage vorwiegend TCP/IP-Netze eingesetzt werden und sich schon allein zu diesem Thema einige Bücher füllen lassen.

In diesem Abschnitt wird lediglich auf die Besonderheiten eines Windows NT 4.0 Netzwerkes eingegangen. Über TCP/IP und Routing findet sich bereits mehr als genug in Kapitel 3, S. 23, so daß auch hier nur auf eventuelle Besonderheiten eingegangen wird.

4.8.1 PDC und BDC

Der ***P**rimary* und der ***B**ackup **D**omain **C**ontroller* wurden bereits in Abschnitt 4.1, S. 44 erwähnt. Der PDC ist dabei das Herzstück einer jeden Domäne.

Obwohl ein PDC in kleineren Netzen oft auch als Fileserver arbeitet, ist sein eigentlicher und alleiniger Sinn und Zweck die verwaltung der Benutzer einer Domäne. Hierzu bedient er sich seiner SAM (***S**ecurety **A**ccess **M**anagement*)-Datenbank. Obwohl das auf den ersten Blick recht wenig Arbeit für einen Rechner erscheint, kann dieser unter Umständen dermaßen überlastet werden, daß sich die Anmeldungen der Benutzer ewig lange hinziehen. Auch wenn er ausfällt ist das Arbeiten in der Domäne nicht möglich.

Für diesen Fall gibt es den BDC.Dieser tut nichts weiter, als seine SAM in regelmäßigen Abständen (etwa alle 5 Minuten) mit der des PDCs zu synchronisieren. Seine eigene SAM kann nicht modifiziert werden, arbeiten an den Benutzern werden remote am PDC durchgeführt (auch wenn das für den Benutzer des BDCs nicht so aussieht). Die Clients beziehen ihre Anmeldedaten vom jeweils näheren Rechner. Somit wird der PDC entlastet. [27]

[26] Auch der (physikalische) Zugriff auf deise Diskette sollte möglichst sicher sein...

[27] Eine ander Anwendung ergibt sich bei (physikalisch) getrennten und nur durch eine Standlei-

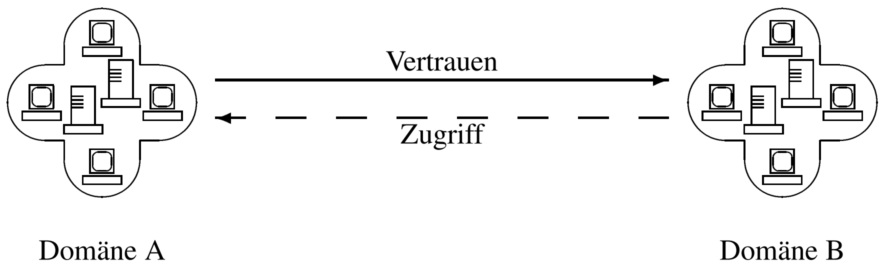


Abbildung 4.6: Einseitige Vertrauensstellung

Anders als beispielsweise ein Caching Nameserver kann ein BDC nicht einfach aus seiner Domäne herausgenommen werden, um in einer anderen Domäne als BDC zu arbeiten; die SIDs lassen das nicht zu. Um einen BDC zu erhalten, muß er installiert werden.

In einem laufenden System ist es möglich, den BDC zum PDC herauf zu stufen. Da es immer nur einen PDC geben kann führt das unweigerlich dazu, daß dieser zum BDC wird. (Die beiden Server tauschen sozusagen die Rollen.)

Falls ein BDC startet und der PDC nicht vorhanden ist führt dies normaler Weise zu einer automatischen Hochstufung des BDCs. Doch sobald nun der „original“ PDC wieder am Netz ist, führt das zu Problemen. Der Rechner, der als erstes startet, arbeitt als PDC. Der zweite stellt fest, daß es bereits einen PDC gibt. Und da es wie bei Highlander nur einen geben kann, startet er seinen Anmeldedienst nicht, eine entsprechende Fehlermeldung (*in Systemdienst konnte nicht gestartet werden*, bezieht sich auf `logon.exe`, den Anmeldedienst) wird ausgegeben.

Unter diesen Umständen kommt es zu der absoluten Sondersituation, daß im Servermanager zwei PDCs angezeigt werden und die überaus seltene Option *PDC zum BDC herunterstufen* verfügbar ist.

4.8.2 Vertrauensstellungen

Für gewöhnlich ist es nicht möglich, Benutzer einer anderen Domäne in eine Gruppe der eigenen aufzunehmen. Dieses ist nur über sgenante Vertrauensstelungen möglich. Eine Vertrauensstellung kann ein-oder beidseitg sein. In Abbldung 4.6, S. 75 ist eine solche einseitige Vertrauensstellung abgebildet.

Wenn eine Domäne einer anderen vertraut, kann die andere Domäne auf ihre Resourcn zugreifen, Domäne A vertraut in der Abbildung Domäne B. Sie wird daher als die *vertrauende*, Domäne B als die *vertraute* Domäne bezeichnet. Die vertrauende Domäne wird manchmal auch *Resourcendomäne* (weil die Benutzer der vertrauten Domäne auf ihre Resourcen zugreifen können), die vertraute Domäne

tung verbundenen Domänenteilen. Eine Authentifizierung über die Standleitung würde sehr viel Zeit beanspruchen; daher wird auch hier ein BDC eingesetzt, so daß die einzige zur Authentifizierung nötige Belastung die der Synchronisation des BDCs mit dem PDC ist.

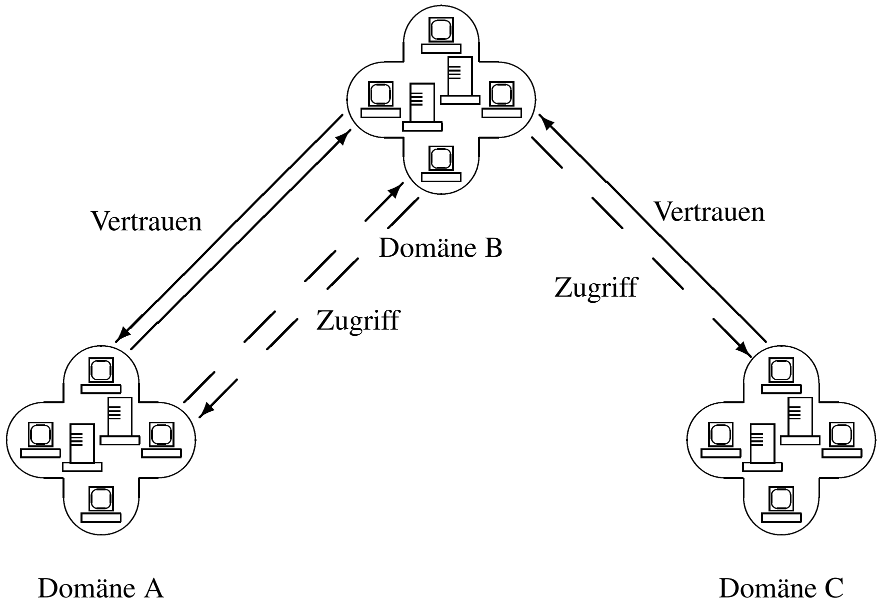


Abbildung 4.7: Drei Domänen mit unterschiedlichen Vertrauensstellungen

Kontendomäne (weil die Nutzer der Resourcen aus der vertrauenden Domäne dort ihre Konten haben können) genannt.

Vertraunestellungen sind *nicht-transitiv.*[28] Das bedeutet, daß da Vertrauen einer Domäne zu einer zweiten keinen Einfluß auf ihr Vertrauen zu einer dritten, welcher die zweite vertraut, hat.

Falls sich zwei Domänen gegenseitig vertrauen, wird von einer gegenseitigen Vertrauensstellung gesprochen. Das Beispiel in Abbildung 4.7, S. 76 zeigt drei Domänen, von denen zwei, nämlich A und B, eine gegenseitige Vertrauensstellung innehaben. Zu Domäne C besteht von Domäne B aus eine einseitige Vertrauensstellung. Und obwohl C Zugriff auf B und B Zugriff auf A hat, hat C aufgrund der Intransitivität von Vertrauensstellungen keinen zugriff auf Domäne A.

Eingerichtet werden diese Vertrauensstellungen im Benutzermanager. Der entsprechende Menüpunkt ist *Richtlinien*, Unterpunkt *Vertrauensstellungen*. Hier gibt es zwei Felder, einmal *Vertraute Domänen* und einmal *Berechtigt, dieser Domäne zu vertrauen*.[29] Im ersten, oberen, werden Domänen eingetragen, denen vertaut wird und für deren Benutzer in dieser Domäne Resourcen freigegeben werden können. Im zweiten, unteren, stehen alle Domänen, die dieser Domäne vertrauen

[28] Transitivität ist eine mathematische Eigenschaft, eigentlich für Relationen. Sie trifft genau dann zu, wenn aus der Tatsache, daß A in Relation zu B und B in Relation zu C steht automatisch folgt, daß A in Relation zu C steht. Eine typische transitive Relation ist die *kleiner als*-Relation: $A < B \wedge B < C \Rightarrow A < C$

[29] Diese Bezeichnung ist ziemlich umständlich; im Englischen heißt das erste Feld *Trusted Domains* und das zweite *Trusting Domains*.

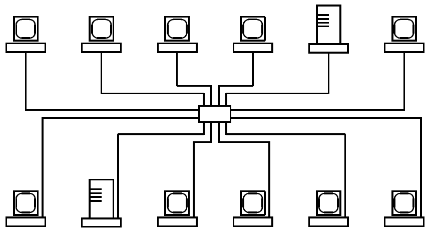


Abbildung 4.8: Einzeldomänenmodell

und auf deren Resourcen die Mitglieder dieser Domäne zugreifen können.

Wird eine Domäne zur vertrauenden Domäne erklärt, muß zunächst ein Paßwort definiert werden. Wird nun in der anderen Domäne die erste Domäne als vertraute Domäne eingetragen, muß hier das gleiche Paßwort eingegeben werden.

Sobald diese Erfordernisse erfüllt sind, können globale Gruppen der vertrauten Domäne in lokale Gruppen der vertrauenden Domäne eingetragen und der Zugriff auf diese Weise hergestellt werden. Hier zeichnet sich das in Abschnitt 4.3.5, S. 56 beschriebene BGLR-Prinzip aus; falls sich alle Benutzer in globalen Gruppen befinden, ist es für den Administrator ein leichtes, ihnen Rechte auf Resourcen vertrauter Domänen zu verschaffen. Globale Gruppen sind dort ebenfalls ansprechbar, Benutzer oder lokale Gruppen der eigenen Domäne hingegen nicht.

4.8.3 Verschiedene Domänenmodelle

Es gibt eine Reihe von Domänenmodellen, also Anordnungen von Domänen im Bezug auf ihre Vertrauensstellunegn untereinander. Einige davon sollen hier beschrieben werden.

Einzeldomänenmodell: Das Einzeldomänenmodell dürfte das bei einem Heimnetzwerk am ehesten anzutreffende Modell sein; es besteht aus einer einzigen Domäne. Diese besteht aus Clients und einem PDC, in manchen Fällen auch noch einem BDC. Nach Microsoft sollte ein solches Netz aus midnestens drei Rechenrn bestehen: PDC, BDC und Client. Die Praxis sieht da eher anders aus. Ein Beispiel für eine Einzeldomäne findet sich in Abbildung 4.8, S. 77.

Hauptdomänenmodell: Bei diesem Modell vertrauen mehrere Domänen einer sogenannten Hauptdomäne. In diesem Zusammenhang wird von *dezentraler Resourcenverwaltung* gesprochen, da sich die Konten der Hauptdomäne der Resourcen aller Domänen bedienen können. In Abbildung 4.9, S. 78 findet sich ein Beispiel für dieses Modell.

Mehrfach-Hauptdomänenmodell: Auch in diesem Modell dienen mehrere Domänen als Resourcendomänen. Anstatt einer einzelnen vertrauen sie jedoch

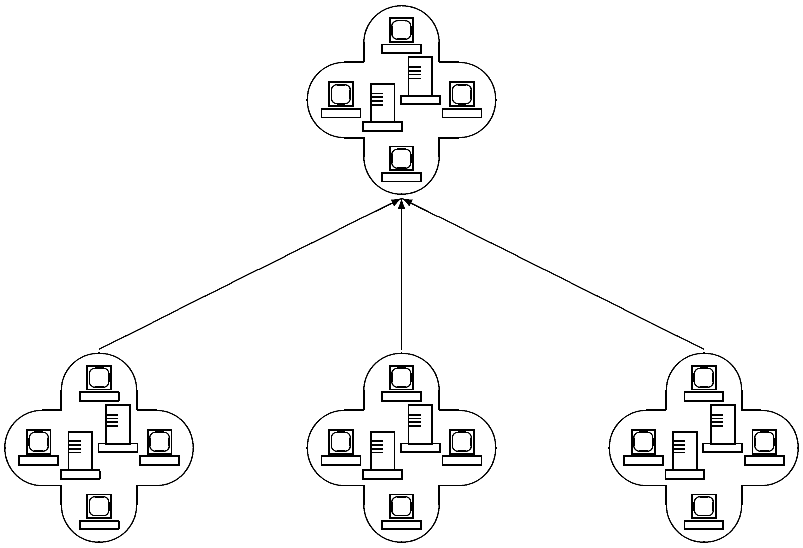


Abbildung 4.9: Hauptdomänenmodell

mehreren, sich unetreinander vertrauenden Domänen. Das kann unter anderem vorkommen, falls eine Domäne allein nicht für alle Konten ausreicht. In Abbildung 4.10, S. 79 findet sich eine solche Konfiguration.

Vollständiges Vertrauensmodell: In diesem Modell vertrauen sich alle Domänen gegenseitig. Aufgrund der fehlenden Transitivität von Vertrauensstellungen ist es erforderlich, da auch auf allen Domänen einzurichten. Ein Beispiel dafür findet sich in Abbildung 4.11, S. 79

4.8.4 Ein wenig zur Authentifizierung

Die Authentifizierung unter Windows NT ist ein ausgesprochen komplexes Thema, auf das hier nicht weiter eingegangen wird. Hier finden sich lediglich ein paar Anmerkungen und Auswirkungen dazu.

Es gibt in Windows-Netzen zwei grundlegende Arten der Authentifizierung: Die benutzer- und die paßwortorientierte. Bei der erstgenannten reicht es aus, wenn auf einem anderen Rechner ein identicher Benutzer existiert, um einen Zugriff zu emöglichen. Windows 9x verwendet diesen Mechanismus. Die zweite Methode benötigt einen Benutzer und ein identisches Paßwort, um die Verbindung herzustellen.

Das führt zu einem für Administratoren nicht zu unterschätzenden Problem: Sobald auf zwei beliebigen Rechnern durch Zufall ein Benutzer gleichen Namens und gleichen Kennwortes angelegt wurde, können sie beliebig auf die fur diesen Benutzer freigegebenen Resourcen des jeweils anderen Rechners zugreifen.

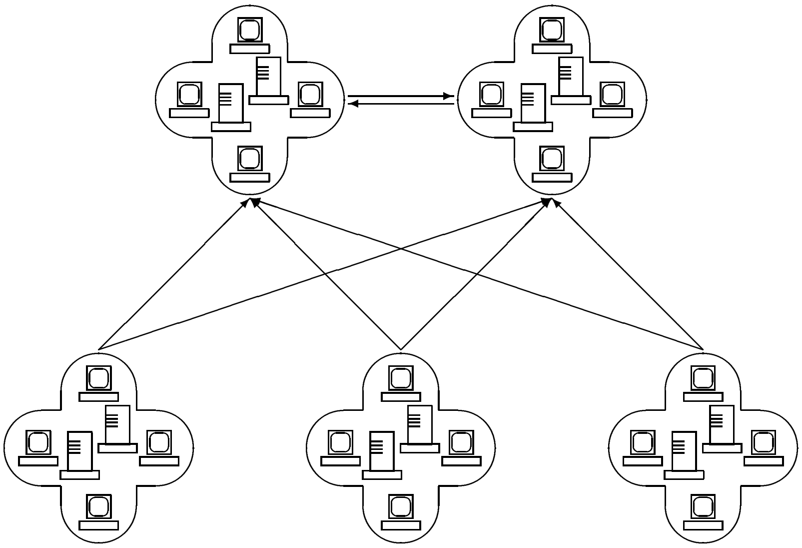


Abbildung 4.10: Mehrfachhauptdomänenmodell

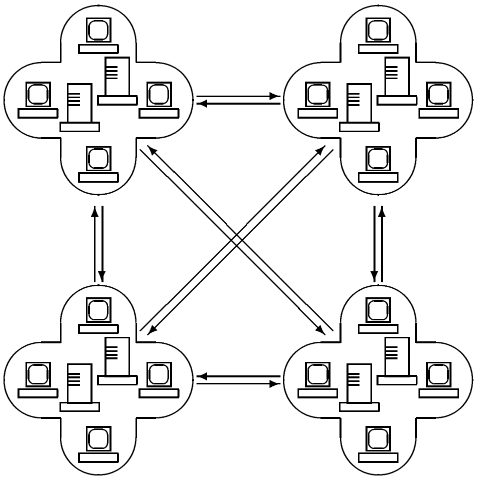


Abbildung 4.11: Vollständiges Vertrauensmodell

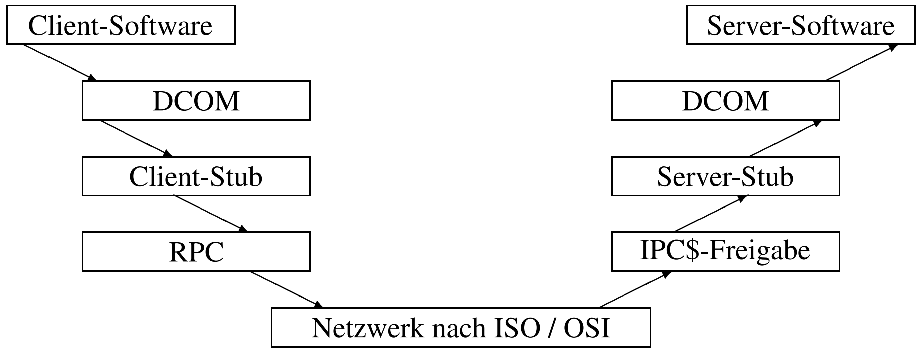


Abbildung 4.12: Eine DCOM-Verbindung

Als Beispiel sei ein durch Automatisierung installierter Server genannt, auf dem ein Standard-Administrator ohne Kennort existiert. Der Ersteller des Installationsskriptes ging davon aus, daß sich der Administrator einloggt und das Paßort ändert. Falls nun ein Hacker dieses Skript kennt, kann er von einem beliebigen anderen Rechner im Netz vollständig auf die Resourcen des Servers zugreifen — und zwar als Administrator mit Vollzugriff!

Doch zunächst muß sich ein Benutzer an einem Rechner anmelden. Normaler Weise geht das nur in der Domäne, in der sich ein Benutzer befindet. Ebenfalls möglich ist die Anmeldung in einer Domäne, die der eigenen vertraut. Deren PDC kennt zwar den Benutzer nicht, reicht ihn aber an den DC der vertrauten Domäne weiter. Dieser Vorgang wird als *durchgängige Echtheitsbestätigung* bzeichnet.

4.8.5 Das DCOM-Prinzip

Im Zusammenhang mit Windows NT 4.0 fallen gelegendlich die Worte *Backoffice*, *Frontoffice* und *Multilayer Applications* (zu Deutsch: Mehrschichtenprogramme). Das zugrunde liegende Prinziep nennt sich DCOM (***D****istributed* ***C****omponent* ***O****bject* ***M****odell*). Gemeint ist damit eine Anwendung, die aus einem Client (dem Frontoffice oder auch Frontend) und einem Server besteht. Ein typisches Beispiel ist etwa die Kombination Exchange / Outlook.

Wenn ein Client-Programm eine Anfrage an ein Server-Programm stellt, gibt sie diese zunächst an eine DCOM-Schnittstelle. Die Schnittstelle leitet die Anfrage an eine sogenannte Client-Stub-Funktion weiter, die ihrerseits einen RPC (***R****emote* ***P****rocedure* ***C****all*, Fernfunktionsaufruf) durchführt. Durch den geht die Anfrage endlich über die verschiedenen Schichten des ISO-OSI-Modelles an den anderen Rechner, wo sie von der Freigabe IPC$ (***I****nter-****P****rocess* ***C****ommunication*, sozusagen das Gegenstück zu RPC) entgegengenommen wird. IPC leitet die Anfrage an die Server-Stub-Funktion weiter, und diese wiederum reicht sie an die DCOM-Schnittstelle durch. Von dort gelangt die Anfrage zur Serversoftware. Dieser Weg wurde in Abbildung 4.12, S. 80 versinnbildlicht.

4.8.6 RAS und DFÜ

In vielen Fällen ist es sinnvoll, wenn sich Mitarbeiter auch von Außerhalb, etwa von zu Hause oder aus einem Hotell, mit dem Netzwerk ihrer Firma verbinden können. Zu diesem Zweck gibt es den RAS, ***R**emote **A**ccess **S**ervice*. Auf diesen setzt das Microsoft DFÜ-Netzwerk[30] DFÜ steht für ***D**aten-**F**ern**Ü**bertragung*, hierbei handlt es sich um eine Client-Software, die sich des RAS-Dienstes bedient, um einen RAS-Server anzurufen.

Die Verbindung selbst geschieht über PPP, das ***P**oint-to-**P**oint-**P**rotocol*. Hierbei handelt es sich um einen sogenannten *WAN-Kapselungs-Typen*. Das bedeutet, zu übertragende Protokolle (in unserem Fall TCP/IP, IPX/SPX und NetBUI) wird in PPP-Pakete verpackt, an einen Empfänger versand und dort wieder ausgepackt. Besonders wichtig ist jedoch die LCP (***L**ink **C**ontroll* **P**rotocoll)-Funktionalität von PPP; über sie wird die Verbindung zum Empfänger erst aufgebaut.

Um RAS oder das DFÜ-Netzwerk nutzen zu können, muß als erstes ein Modem (oder X.25-Pad) installiert werden. Dies geschieht in der Systemsteuerung under dem Punkt *Modem*. Falls das Modem dabei nicht automatisch erkannt wird,[31] gibt es die Möglichkeit, es aus einer Liste auszuwählen oder sogar von Diskette zu installieren. Hierzu sei noch angemerkt, daß speziell für Modems die Treiber für Windows 95 unter NT 4.0 funktionieren. Der Betrieb ist natürlich auch mit einer ISDN-Karte möglich; diese wird jedoch nicht unter Modem, sondern unter *Netzwerkeigenschaften* als Netzwerkkarte zusammen mit dem Herstellerspezifischen *NDIS-WAN* (oder, wie manche Hersteller sagen, *Miniport*) -Treiber installiert.

Als nächstes muß der RAS-Dienst installiert und anschließend konfiguriert werden. Bei der Konfiguration verlangt RAS zunächst nach dem installierten Modem (oder X.25-Pad oder der ISDN-Karte).[32]

Das anschließende Fenster bildet das Herzstück der RAS-Konfiguration. Hier werden alle genutzten Anschlüsse (meistens die seriellen) mit den angeschlossenen Geräten angezeigt. Über die Schaltfläche *Konfiguration* wird bestimmt, ob dieser Anschluß nur ausgehende, nur eingehnde oder beide Arten von Verbindungen zulassen soll. Eingehende Verbindungen sind vor allem für RAS-Server inetressant, ausgehende für Workstations. Letztere können selbst wenn sie auf Eingehende verbindungen eingetsllt sind maximal eine Verbindung entgegen nehmen. (Das ist vor allem wichtig, falls der Verbindungsaufbau über Rückruf erfolgt, siehe auch Abschnitt 4.5.3, S. 65.)

Die andere, wichtige Konfigurationsschaltfläche ist *Netzwerk*. Hier kann angegeben werden, mit welchem Protokoll sich ein Client verbinden und der Server selbst hinausgehen darf. Außerdem besteht die Wahl zwischen drei verschiedenen Sicherungsmethoden:

Echtheitsbestätigung als unverschlüsselter Text: Dieser Punkt bietet keine Si-

[30] Für alle, die sich das schon mal gefragt haben: Auf Englisch heißt es *DUN*, ***D**ial-**U**p-**N**etwork*.
[31] Wärend in [4] gesagt wird, das käme selten vor, heißt es in [6], das sei erstaunlich oft der Fall...
[32] Falls das noch nicht geschehen ist, kann es an dieser Stelle nachgeholt werden; es gilt alles oben gesagte.

cherheit; er besagt, daß der gesammte Verbindungsaufbau unverschlüsselt von statten geht. Sollte also irgend jemand mitlauschen, hat er alle Benutzernamen und Kennwörter, die über diese Verbindung benutzt werden. (Besonder peinlich ist so etwas, wenn es sich um Administratorendaten handelt.)[33]

Nur verschlüsselte Echtheitsbestätigung: Hier wird ein verschlüsselter Verbindungsaufbau nach dem DES-Standard verlangt.[34]

Nur Microsoft-verschlüsselte Echtheitsbestätigung: Auch hier ist der Verbindungsaufbau ist verschlüsselt, allerdings auf eine Microsoft-spezifische Art. Daher arbeitet das Verfahren nur mit MS-Clients zusammen.[35] Interessant ist hier der aktivierbare Unterpunkt *Datenverschlüsselung fordern*, der auch nach Verbindungsaufbau verschlüsselte Datenübertragung gewährleistet.

In der Servervariante gibt es noch ein weiteres Kästchen, nämlich *Multilink ermöglichen*. Hierbei werden mehrere Telefonnummern gleichzeitig gewählt und die so entsehendenverbindung zu einer logischen gebündelt. (Dies ist besonders bei ISDN nützlich, dort wird das Verfahren auch *Kanalbündelung* genannt.)

Damit ist alles vorhanden, um einen RAS-Server zu betreiben. Um sich auf einem solchen einzuwählen ist es erforderlich, im DFÜ-Netzwerk (zu finden im Arbeitsplatz) einen sogenannten Telefonbucheintrag zu erstellen. Das ist unter anderem über das Starten eines Assistenten möglich. Hier können alle wichtigen Daten und Verhaltensweisen angegeben werden (wobei die wichtigsten Daten wohl die Telefonnummer des RAS-Servers sein dürften). Durch Anklicken dieser Verbindung wird dann eine Verbindung hergestellt.

Nicht vergessen werden sollte die Konfiguration der Benutzerkonten für den RAS-Betrieb; dies wurde bereits in Abschnitt 4.5.3, S. 65 behandel.

4.9 Drucker

Eines der wichtigsten Peripherie-Geräte in jedem Betrieb ist der Drucker. Und in vielen Fällen ist es sinnvoll, einen besonders guten Drucker für alle Rechner im Netz verfügbar zu machen. Windows NT 4.0 bringt einige dafür erforderliche Mechanismen mit.

4.9.1 Definitionen

Aus verwaltungstechnischen Gründen sind die Benennungen der einzelnen zum Drucken erforderlichen Elemente unter Windows ein wenig anders, als es auf den ersten Blick logisch erscheinen mag.[36] Grundsätzlich werden zum Drucken zwei Komponenten benötigt, ein Drucker und ein Druckgerät.

[33] Das zugrundeliegende Authentifikationsverfahren ist PAP.

[34] Hier lieg CHAP als Authentifikationsverfahren zu Grunde.

[35] Hier liegt MS-CHAP zugrunde, eine MS-Abart von CHAP.

[36] Sie sind in sich genommen logisch. Es handelt sich *nicht* um ein *Microsoft Sinnlos* Problem.

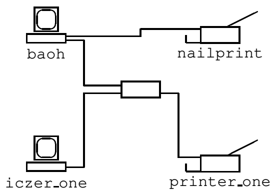


Abbildung 4.13: Anschlußmöglichkeiten für Drucker

Druckgerät: Das ist der ganz normale, hardwaremäßige Drucker.

Drucker: Hierbei handelt es sich um ein logisches, virtuelles Gerät auf dem Rechner. Es wird über einen Druckertreiber angesprochen und leitet die Aufträge dann bearbeitet und druckfertig an den Drucker weiter.

Hinter einem Drucker muß nicht unbedingt auch ein Druckgerät stehen; Adobe beispielsweise stellt einen Drucker zu Verfügung, der als Ergebnis eine PDF-Datei liefert.

Durch diese Trennung zwischen logichen und physichen Geräten ergibt sich eine weitere, manchmal nur schwer nachzuvollziehende Definition. Ein Drucker kann lokal an einem Rechner angeschlossen oder über ein Netzwerk ansprechbar sein, etwa, wenn er an einem anderen Rechner hängt und dort freigegeben wurde oder er über eine eigene Netzwerkkarte verfügt. Im normalen Sprachgebrauch werden Rechner, die direkt am Rechner hängen, als lokale, andere, die im Netzwerk hängen, als Netzwerkdrucker bezeichnet. In Abbildung 4.13, S. 83 wurden beide Möglichkeiten abgebildet. Doch wie ist das, wenn für die physikalischen Anschlüsse für die Bezeichnung *Drucker* keine Rolle spielen?

Microsoft definiert Netzwerk- und lokale Drucker wie folgend:

Lokaler Drucker: Ein so bezeichneter Drucker ist ein Drucker, dessen Warteschlange auf dem lokalen Rechner liegt und dessen Druckaufträge auf dem lokalen Rechner verwaltet werden können.

Netzwerkdrucker: Ein so bezeichneter Drucker ist ein Drucker, dessen Warteschlange an einen anderen Rechner weitergeleitet werden und dessen Aufträge auf dem anderen Rechner verwaltet werden.

Wenn also `nailprint` auf dem Rechner `baoh` eingerichtet und freigegeben wird, ist er dort ein lokaler Drucker. Wird er dann auf `iczer_one` über diese Freigabe eingerichtet, ist er dort ein Netzwerkdrucker. Doch was ist mit dem Drucker `printer_one`?

Bevor er als Netzwerkdrucker eingerichtet werden kann, muß er zunächst freigegeben werden. Dies ist aber nur möglich, wenn er auf irgend einem Rechner, von dem aus auch seine Druckaufträge verwaltet werden können, installiert ist. Angenommen, er wird auf dem Rechner `iczer_one` so eingerichtet. Dann ist er dort ein lokaler Drucker, obwohl er über das Netzwerk angesprochen wird. Und falls er auf `baoh` ebenfalls so eingerichtet wird, ist er auch dort ein lokaler Drucker. Nur, wenn er auf `baoh` über die Freigabe auf `iczer_one` installiert wird, gilt er dort als Netzwerkdrucker.

Um das Chaos noch komplett zu machen ist es außerdem möglich, den freigegebene Drucker eine Rechners auf einem anderen so zu installieren, daß die Druckaufträge des anderen Rechners auch auf dm anderen Rechner verwaltet werden. Womit der Drucker dann auf dem anderen Rechner wiederum lokal ist. In unserem Beispiel würde auf dem Rechner `iczer_one` der Drucker `nailprint` als lokaler Drucker eingerichtet...

4.9.2 Druckereinrichtung

Drucker werden über den Startmenüpunkt *Einstellungen*, Unterpunkt *Drukker* verwaltet. Um einen neuen Drucker hinzuzufügen reicht es, auf das Symbol *Neuer Drucker* zu klicken. Danach wird zunächst die grundsätzliche Frage gestellt, ob es sich um einen lokalen oder einen Netzwerkdrucker handelt

Falls ein Netzwerkdrucker gewählt wird, muß selbiger als nächstes mit UNC-Pfad angegeben werden. (Alternativ kann er auch gesucht und in der eingeblendeten Netzwerkumgebung angewählt werden, in einigen Fällen wird er aber dort nicht angezeigt.) Im Optimalfall werden die Treiber vom Druckerserver bereitgestellt. Ansonsten werden sie vom Installationsprogramm angefordert.

Bei einem lokalen Drucker sieht die Sache anders aus. Hier muß der entsprechende Anschluß (etwa LPT 1) ausgewählt werden. Danach wird nach den Treibern gefragt, und irgend wann kann der Drucker noch als Netzwerkdrucker freigegeben werden. Falls das passiert, können neben dem eigenen Treiber auch Treiber für andere Betriebsysteme (der Windows-Familie[37]) hinzugefügt werden. Das ist praktisch, denn wenn ein anderer Rechner den freigegebenen Drucker bei sich als Netzwerkdrucker installiert, kann er die Treiber direkt von dort bekommen (und der Anwender muß sich nicht mit den Treiberdisketten herumärgern).

Doch was ist nun mit Druckern, die über eine Netzwerkkarte angesprochen werden? Auch diese müssen zunächst lokal eingerichtet werden. Doch um das zu tun, sind bestimmte Anschlüsse erforderlich.

Windows NT 4.0 bringt bereits einige Printerports für Drucker mit Netzwerkkarten mit. Sie werden unter dem Punkt *Anschluß hinzufügen* addiert. Windows NT bringt einige wenige solche sogenannte *Druckermonitore* mit; die meisten Druckerhersteller liefern jedoch welche mit ihrem Produkt zusammen aus.[38]

Als letztes soll hier noch eine weitere Methode der Einrichtung lokaler Drucker über Netzwerk angesprochen werden; mit Hilfe des `net use` Befehles können nicht nur Netzlaufwerke mit Verzeichnissen, sondern auch freigegebene Drucker

---

[37] *Nicht* für Windows 3.1(1).

[38] Für HP-Drucker werden Übrigens auch Druckermonitore mitgeliefert; die sind aber nur verfügbar, wenn das DLC-, *Data Link Controll*-Protokoll, installiert ist. Das liegt aber nicht an HP, sondern an Windows NT 4.0...

mit Schnittstellen verbunden werden. Um etwa den Drucker `nailprint`, freigegeben auf `baoh`, auf dem Rechner `iczer_one` über den Port `LPT5` anzusprechen, lautet der Befehl:

```
net use lpt5 //baoh/nailprint
```

Sobald er als lokaler Port vorhanden ist, kann `nailprint` natürlich als lokaler Drucker eingerichtet werden. (Um das perverse Spiel noch weiter zu führen wäre es sogar möglich, ihn als Netzwerkdrucker einzutragen und auf `baoh` als Netzwerkdrucker zu installieren. . .)

4.9.3 Verwaltung von Druckern

Wenn ein Drucker im Netz freigegeben wird, dnn verfügt er — ebenso wie freigegebene Dateien — über bestimmte Berechtigungen. Dem Drucker zugewiesene benutzer und Gruppen können über die folgenden Berechtigungen verfügen:

Kein Zugriff: Das allseits bekannte und beliebte Zugriffsverbot.

Drucken: Der Anwender darf drucken und seine eigenen Druckaufträge anhalten, neu starten oder löschen.

Verwalten: Das gleiche wie *Drucken*, die Verwaltungsfunktionen gelten jedoch auch für die Aufträge anderer Benutzer.

Vollzugriff: Zuzüglich der *Verwalten* Berechtigung darf der Benutzer auch die Eigenschaften des Druckers verändern.

Neben diesen Berechtigungen gibt es noch weitere Möglichkeiten, die Benutzung eines Druckers zu kontrollieren. Dazu gibt es in den Eigenschaften des Druckers die Karte *Zeitplanung der Druckaufträge*. Folgende Punkte können dort konfiguriert werden:

Verfügbar: Ein Drucker kann immer oder nur in einer bestimmten, dort anzugebenden Zeit nutzbar sein. Aufträge, die zu anderen Zeiten versand werden, landen zwar n der Druckerwarteschlange, werden aber erst bei Beginn der Verfügbarkeit ausgedruckt.

Priorität: Hiermit werden die Prioritäten der Druckaufträge dieses Drukkers eingestellt. Der Wert kann zwischen 1 und 99 liegen. (Der Sinn wird weiter Unten beleuchtet.)

Spoolereinstellungen: In den nächsten Einstellungen kann gewählt werden, ob ein Druckauftrag überhaupt in einer Warteschlange zwischengespeichert oder gleich an den Drucker geleitet werden soll. Letzteres kann bei der Benutzung durch mehrere Benutzer zu Konflikten führen; davon abgesehen greifen dann die Prioritäten nicht. Es empfielt sich eigentlich immer, über einen Zwischenspeicher (auch *Spooler* genannt) zu drucken.

Falls über einen Spooler gedruckt wird, kann noch angegeben werden, wann der Druck einsetzen soll; entweder, sobald die erste Seite des Druckauftrages, oder, sobald der ganze Auftrag vorhanden ist. Falls die druckende Anwendung nicht in der Lage ist, im Hintergrund zu drucken,[39] empfielt sich die zweite instellung, da für die Anwendung der Druckauftrag nach Schreiben in den Spooler beendet ist.

Fehlgeschlagene Aufträge anhalten: Falls ein Druckauftrag über andere Grundeinstellungen (etwa betreffs der Seitengröße) als der Drucker verügt, wird er bei aktiviertem Kästchen angehalten.

Aufträge in Warteschlange zuerst drucken: Falls mehr als ein Druckauftrag gespoolt werden, wird bei aktiviertem Kästchen der Reinfolge in der Warteschlange nach gedruckt; ist es nicht aktiviert, werden die Aufträge in Reinfolge ihrer vollständigen Spoolung abgearbeitet.

Aufträge nach Drucken nicht löschen: Falls dieses Kästchen aktiviert ist, weren die Aufträge nach ihrer Abarbeitung in der Warteschlange belassen.[40]

Da ein Drucker nur ein logisches Konstrukt ist, welches auf ein Druckgerät zugreift, können pro Druckgerät auch mehr als ein Drucker eingerichtet werden. Dadurch lassen sich die Zugriffsberechtigungen mit den Eigenschaften kombinieren. So ist es beispielsweise möglich, für einen Laserdrucker einen Drucker für die Allgemeinheit und einen für die Buchhaltung zu erstellen. Über die Berechtigungen laßt sich regeln, daß die Allgemeinheit nicht auf den Drucker der Buchhaltung kommt. Mit Hilfe der Druckereigenschaften hingegenließe sich einrichten, daß der Drucker der Allgemeinheit nur in der Mittagspause ansprechbar ist und dann über eine geringere Priorität als der Buchhaltungsdrucker verfügt. (Mit anderen Worten: wenn in der fraglichen Zeit ein Auftrag der Allgemeinheit und einer der Buchhaltung gedruckt werden sollen, wird der Auftrag der Buchhaltung bevorzugt.)

Als letztes ist es möglich, die Einstellungen der verschiedenen Drucker global einzustellen. Dies geschieht mit dem Punkt *Server-Eigenschaften* im Menü *Datei* des *Arbeitsplatz*-Unterpunktes *Drucker*. Hier läßt sich unter anderem ein Pfad für die Druckerwarteschlange anlegen (was besonders wichtig ist, wenn auf der Bootpartition kein Platz mehr ist) und das Verhalten bei ankommenden Remote-Aufträgen und auftretenden Fehlern im Ganzen konfigurieren.

Ebenfalls unter den Eigenschaften, allerdings im Unterpunkt *Allgemein*, kann eine Datei für eine sogenannte Trennseite angegebenw werden. Trennseiten werden zwischen zwei Druckaufträgen ausgegeben und können ausgesprochen nützlich sein. Neben der einfachen Trennung des Jobs können einige Drucker über vom PostScript in den PCL-Modus umgestellt werden (und umgekehrt). Die Trennseite

[39] Alte Anwendungen tun das nicht; für die Dauer des Druckauftrages stehen sie nicht zur Verfügung.

[40] Dem Verfasser ist bislang noch keine sinnvolle Einsatzmöglichkeit dafür eingefallen.

zur Aktivierung des PostScript-Modes heißt `psscript.sep`, die zur Aktivierung des PCL-Modes `pclscrip.sep`. Diese beiden Seiten geben keine Seite aus. Eine einfache Trennseite wird mit `sysprint.sep` erstellt.

4.9.4 Drucker-Pool

In 4.9.3, S. 86 wurde gesagt, daß hinter mehreren Druckern ein einziges Druckgerät stehen kann. Der umgekehrte Fall ist ebenfalls möglich: Hinter einem Drucker können mehrere baugleiche Druckgeräte stehen. Dazu müssen bei der ruckerinstallation nur all Anschlüse, an denen entsprechende Drucker hängen, angegeben und das Kästchen *Drucker-Pool aktivieren* angewählt werden.

Diese Aktion hat selbstverständlich nicht zur Auswirkung, daß ein gedrucktes Dokument auf allen angeschlossenen Druckern gleichzeitig ausgegeben wird. Vielmehr werden die Geräte je nach Auslastung angesteuert. Bei mehreren druckenden Benutzern hat das durchaus seine Vorteile; der ankommende Druckauftrag wird stets der kürzesten Warteschlange zugeteilt und die Wartezeit auf das Dokument somit möglichst gering gehalten. Es ist für die Benutzer nicht möglich, zu setuern, welchn Drucker des Druckerpools sie benutzen.

Eine wahrlich boshafte Anwendung wäre das Nutzen mehrerer über das Netzwerk angeschlossener Drucker, die an verschiedenen, weit auseinanderliegenden Stellen des Gebäudes aufgestellt sind...

4.10 Heterogene Netzwerkzugriffe

Auch wenn Microsoft das nicht gerne wahr hat, neben Windows gibt es noch andere Betriebsysteme, und einige davon sind für Netzwerke bestens geeignet. Besonders verbreitet sind nach wie vor (und insbesondere in NT 4.0 Umgebungen) Novell NetWare und das eine oder andere UNIX-Derivat.

4.10.1 Grundlegendes

Um zu verstehen, wie die Anschlüsse dieser Systeme vonstatten gehen, ist es zunächst erforderlich, die grundsätzliche Funktionsweise eines Windows-Netzes zu beleuchten.

Um auf irgend welche Anwendungen eines anderen Rechners zuzugreifen ist ein Netzwerkprotokoll, etwa TCP/IP, notwenig. Doch das reicht noch nicht aus; um Dateien oder Druckdienste anzusteuern, benutzt Windows das SMB- (***S**erver **M**essage **B**lock*-) Protokoll. Dieses liegt in der fünften Schicht des ISO/OSI-Referenzmodelles (der Sitzungsschicht) und setzt auf NetBIOS auf.

Wenn nun ein Zugriff auf eine im Netz freigegebene Resource erfolgen soll, führt das zu einem ganz normalen Zugriff auf diese Resource, nicht anders, als wenn sie lokal verfügbar wäre. Über SMB wird diese Anfrage dann jedoch auf den

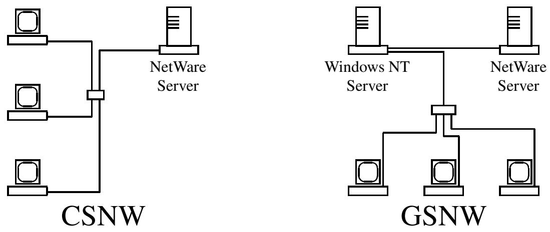


Abbildung 4.14: NetWare-Zugriff über CSNW und GSNW

anderen Rechner umgeleitet.[41] Der Dienst, der für die Freigabe solcher Resourcen notwendig it, heißt *Serverdienst*. Der Zugrif wird über den *Computer Suchdienst* realisiert. (Der wird manchmal auch als *Redirector* bezeichnet.)

4.10.2 Die Verbindung mit einem Novell-Server

Microsoft stell tatsächlich Schnittstellen zu NetWare-Servern zu Verfügung. Sie sind aber mit einigen Problemen behaftet. Das ärgste dürfte sein, das nach Microsoft Novell NetWare nur über IPX/SPX zu erreichen ist. Das hat aber bereits seid Novell 4.2 keine Gültigkeit mehr, wie alle anderen NOS[42] spricht es inzwischen TCP/IP. Um mit Hauseigenen Mitteln von NT auf NetWare-Server zuzugreifen, muß jedoch NWLink installiert werden. Hierbei handelt es sich um die MS-implementierung von IPX/SPX und NetBIOS. Damit ist es jedoch nicht getan, denn NetWare kann nicht viel mit SMB-Anfragen anfangen. Daher muß ein neuer Redirector her.

Hier gibt es zwei Ansatzpunkte. Entweder kann dieser Redirector auf allen Clients installiert werden. Das bietet sich an, wenn alle Workstations regelmäßig auf den NetWare-Server zugreifen. Oder eine etwas abgewandelte Form des Redirectors wird auf einem Windows-Server installiert, und alle Clients nutzen den Windows-Server als Gateway zum NetWare-Server. Im ersten Fall wird der CSNW (***C**lient **S**ervice for **N**et**W**are*), im zweiten Fall der GSNW (***G**ateway **S**ervice for **N**et**W**are*) benutzt. In letzgenanntem Fall ist es darüber hinaus möglich, auf den Clients auf NWLink zu verzichten. Bei dem Beispiel in Abbildung 4.14, S. 88 wurde sogar ein Schritt weiter gegangen und dem Gateway eine zweite Netzwerkkarte spendiert, die ausschließlich der Kommunikation mit dem NetWare-Server dient. Über den Punkt *Bindungen* können nun auf den Netzwerkkarten die dort nichtbenötigten Protokolle deaktiviert werden.[43]

[41] Linux-Benutzer erkennen sicher, warum dieser Vorgang auch *redirecting* genannt wird.

[42] Network Operating System.

[43] Die Reinfolge der an eine Karte gebundenen Protokolle ist ebenfalls entscheident, so mehr als eines eingesetzt werden. Das oberste sollte besser auch das meist benutzte sein, da es auch als erstes angesprochen wird. Die richtige Sortierung kann einen enormen Geschwindigkeitsgewinn bedeuten.

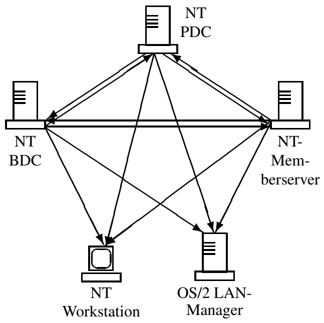


Abbildung 4.15: Rechnerfähigkeiten zur Dateireplikation

4.10.3 UNIX / Linux

Der Zugriff auf UNIX-Derivate gestalltet sich für die Windows-Welt wesendlich leichter; nicht nur, daß UNIX von Haus aus TCP/IP beherrscht, mit Samba ist es zudem möglich, einen UNIX-Rechner als Windows-Rechner auftreten zu lassen.

Samba besteht grundsätzlich aus zwei Teilen: Dem `nmbd` und dem `smbd`. Der erste simmuliert NetBIOS, der zweite das SMB-Protokoll. Über eine entsprechende Konfigurationsdatei ist es nun möglich, Drucker und Verzeichnisse für die Windows-Welt freizugeben. (Tatsächlich kann Samba noch sehr viel mehr; Authentifzierung über die Domäne ist ebenso möglich wie die Arbeit als PDC oder BDC!)

4.11 Dezentrale Datenverwaltung

Unter diesem Stichpunkt wurden zwei Methoden zusammengefaßt, die der Verlagerung von Daten dient. Das eine ist die Verzeichnisreplikation (obschon sich die auch als *zentrale Datenverwaltung* beschreiben läßt, daß ist Definitionssache), und das NT-Backup.

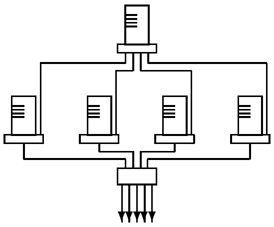
4.11.1 Verzeichnisreplikation

Bei der Verzeichnisreplikation werden Daten, die auf einem zentralen Rechner liegen, auf andere, dafür eingerichtete Rechner verteilt. Grundsätzlich gilt, daß alle unter Windows NT 4.0 Server laufenden Maschienen dabei als *Export*-Server, alle Windows NT 4.0 Server, alle Windows NT 4.0 Workstations und Rechner unter OS/2 mit dem MS-OS/2-LAN-Manager als *Import*-Clients*Import-Client* dienen können. Die einzelnen Rechnerarten und ihre Fähigkeiten wurden in Abbildung 4.15, S. 89 versinnbildlicht und in Tabelle 4.4, S. 90 nochmals aufgeführt.

Damit die Verzeichnisreplikation überhaupt funktionieren kann, muß auf dem Replikationsserver ein bestimmter Dienst laufen, nämlich der *Server Replikations-*

Fähigkeit	Windows NT 4.0 Server			NT 4.0 Work-Station	OS/2 LAN Manager
	PDC	BDC	Member		
Import	x	x	x	x	x
Export	x	x	x		

Tabelle 4.4: Rechnerfähigkeiten zur Dateireplikation



Zum Netzwerk

Abbildung 4.16: Netz mit Backup-Server

dienst. Damit dieser laufen kann, benötigt er einen Benutzer mit niemals ablaufendem Paßwort.

Die zu replizierenden Daten müssen in Unterverzeichnissen von
`%systemroot%\system32\repl\export`
liegen.[44] Die Clients hingegen benötigen lediglich ein Verzeichnis
`%systemroot%\system32\repl\import`
in welches die Verzeichnisse repliziert werden.

4.11.2 Das Backup

Bei dem Windows NT Backup handelt es sich um eine abgespeckte Version des daher sehr viel häufiger eingesetzten Backup-Programmes *Veritas*. Davon abgesehen ist NT-Backup ein normales Standard-Backup-Programm, so daß hier lediglich auf die zu Grunde liegenden Backup-Strategien eingegangen wird. Wenn von Backup gesprochen wird, ist die Rede stets von der Sicherung großer Datenmassen auf Streamerbänder.

Der erste zu beachtende Punkt ist die zu Grunde liegende Netzwerkstruktur.[45] Eine recht effiziente Methode besteht darin, einen einzelnen Rechner als Streamer-Server abzustellen und die zu sichernden Rechner mittels eigener Netzwerkkarten mit diesem zu verbinden (siehe Abbildung 4.16, S. 90). Im Optimalfall erfordert ds

[44] Zum einen ist zu beachten, daß die Unterverzeichnisse dort repliziert werden, direkt dort stehende Dateien nicht. Zum anderen ist es innerhalb der Replikationsdienst konfiguration durchaus möglich, den Pfad zu wechseln. Das macht die Sache aber nicht besonders übersichtlich.

[45] Es wird bei Microsoft anscheinend davon ausgegangen, daß ihr Backup-Programm auch über das Netzwerk funktioniert. Das ist aber nicht der Fall.

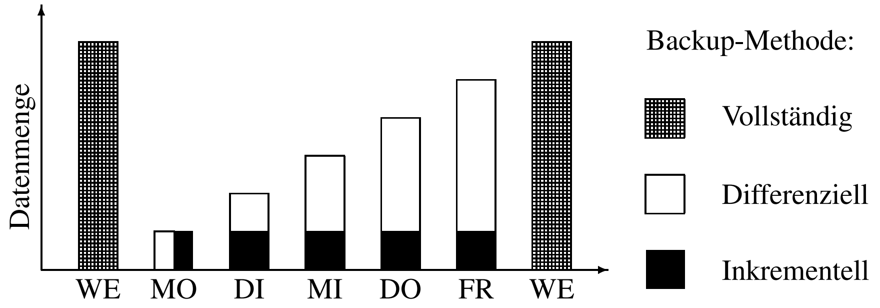


Abbildung 4.17: Backup-Methoden im Vergleich

zwar eine große Anzahl von Netzwerkkarten auf dem icherungsserver, aber dafür ist zum Einen das Hauptnetz von der zur Sicherungzeit auftretenden Netzlast bewahrt, und zum Anderen die größtmögliche Geschwindigkeit bei der Übertragung der zu sichernden Daten gewährleistet.

Daneben ist die Art der Backup-Strategie entscheident. In dem NT-backup-Programm werden drei Methoden unterstützt, von denen die letzten beiden Ergänzungen zu einem irgend wann vorangegangenen Vollbackup sind:

Vollständiges Backup: Sämmtliche Daten werden auf das Band gesichert und als gesichert Markiert. (Das geschieht bei NTFS über das Dateiatribut `a` für ***A**rchiv*.) Sobald eine markierte Datei geändert wird, verschwindet die Markierung.

Inkrementell: Hierbei werden alle Daten gesichert, die nicht als bereits gesichert markiert sind. omit werden immer nur die aktuellen Änderungen abgespeichert. Die gesicherten Dateien werden als gesichert markiert.

Differenziell: Hierbei werden geänderte Daten gesichert, aber nicht als gesichert markiert. Also Folge davon werden alle Daten egsichert, die seid der letzten Komplettsicherung geändert wurden, gesichert.

Jede diese Methoden hat ihre Vor- und Nachteile; die Vollständige Sicherung hat den Vorteil, daß bei einer Wiederherstellung des Systems lediglich ein Band eingespielt werden muß. Auf der anderen Seite dauert die Sicherung ziemlich lange. Das inkrementelle Backup hingegen benötigt in der Sicherungsphase sehr wenig Zeit; es werden immer nur die Daten gesichert, die seid der letzten inkrementellen Sicherung verändert wurden. Bei einer Systemwiederherstellung müssen jedoch das letzte vollständige Backup und alle seid dieser Zeit erfolgten inkrementellen Backups eingespielt werden. Das Differentielle Backup scheint tatsächlich ein gelungener Mittelweg; es braucht nicht so lange, wie ein Vollsicherung, und es muß neben der letzten Vollsicherung nur das letzte differentielle Backup eingespielt werden.

In den meisten Firmen wird eine Kombination aus Vollständiger und Inkrementeller oder ifferenzieller Sicherung angeandt. Um zu illustrieren, welchen Sicherungsaufwand welches Prinzip hevorruft, wurden beide Methoden (jeweils mit einer Vollsicherung am Wochenende) in Abbildung 4.17, S. 91 verdeutlicht.[46]

4.12 Was geht auf dem Rechner vor?

Dies ist ein recht vielseitiges Thema, da es sich mit mehreren, Themenverwanten aber in ihren Anwendungen und Auswirkungen recht verschiedenen Funktionalitäten beschaftigt. Zum einen zählt natürlich die ÜBerwachung von Benutzern und Resourcen dazu, zum anderen jedoch auch die Überwachung von Ereignissen und Netzwerkvorgängen zwecks einer Analyse zur Einstellungsoptimierung. Der letztgenannte Punkt stellt den Löwenanteil.

4.12.1 Überwachungsrichtlinien

Die Einstellungen der Überwachungsrichtlinien geschieht über den Benutzermanager. Über den Unterpunkt *Überwachung* des Menüs *Richtlinien* lassen sich eine Anzahl von Richtlinien einstellen. Im Groben werden Bereiche angegeben, bei denen Zugriffe oder ähnliches erfolgen kann und deren Erfolg oder Mißerfolg (oder beides) protokolliert werden soll. Im einzelnen sind das:

An- und Abmweldung: Hier werden Anmeldeversuche mitgeloggt. Mißerfolge ist insbesondere dann sinnvoll, wenn vermutet wird, daß irgend jemand versucht, sich mit Hilfe erratener Paßwörter einzuloggen (da dem eigentlichen Login sicherlich eine größere Anzahl von Einloggversuchen vorangeht).

Datei- und Objektzurgiff: Durch diesen Punkt können einzelne Objekte und Dateien überwacht werden. Die Einstellung muß an den einzelnen Objekten selbst ebenfalls aktiviert werden (da das System ja sonst gar nicht weiß, was es überwachen soll).

Benutzerrecht: Falls ein Benutzer von einem Benutzerrecht (abgesehen von An- und Abmelden, also beispielsweise Neustart des Rechners) gebrauch macht, kann sein (Miß-) Erfolg protokolliert werden.

Verwaltung von Benutzer- und Gruppenrechten: Die Änderungen der Benutzereinstellungen (oder anderer Verwaltungsschritte) können ebenfalls überwacht werden.

Sicherheitsrichtlinienänderung: Hiermit werden die Änderungen der Überwachungsrichtlinien protokolliert.

Heruntefahren und Reboot: Der Name spricht für sich.

[46] Hierbei wurde zur Vereinfachung von einem linearen Datenwachstum ausgegangen.

Prozessverfolgung: Hiermit werden detailierte Prozessrückverfolgungen der oben genannten Punkte ermöglicht.

Die Ergebnisse der Überwachung finden sich in der Ereignisanzeige, einem Programm im Unterpunkt *Verwaltung* des *Start*-Menüs, aufgelistet. Die Ereignisanzeige dient der darstellung verschiedener Protokolle; das in diesem Fall interessante ist das *Sicherheitsprotokoll*. Erfolgreiche mitgeloggte Ereignisse werden hier mit einem Schlüssel, Fehlversuche mit einem Schloß gekennzeichnet. Zu jedem Ereignis findet sich ein Eintrag, welcher Benutzer ihn zu welchem Zeitpunkt ausgelößt hat.

Eine sehr interessante Einstellung zu diesem Thema läßt sich in der Registry vornehmen: Unter `HKEY_LOCAL_MACHINE` kann in dem Schlüssel
`SYSTEM\CurrentControlSet\Control\LSA`
eine Variable `CrashOnAuditFail` mit Wert `1` angelegt werden. Dies führt dazu, daß der Rechner, sobald das Protokoll voll ist, kurzerhand abstürzt. Dies hat durchaus seine Vorteile, da ansonsten das Sicherheitsprotokoll nicht weitergeführt würde.

4.12.2 Werkzeuge zur Informationsbeschaffung

Um sich Informationen über die aktuellen Systemvorgänge zu besorgen gibt es eine Reihe von Werkzeugen. Im Folgenden werden der Taskmanager, `winmsd`, die Ereignisanzeige, der Systemmonitor und der Netzwerkmonitor genauer beleuchtet.

Der Taskmanager: Das vermutlich bekannteste Programm zur Analyse. Neben den gerade laufenden Prozessen und ihrem Anteil an der Gesammtauslastung kann hier auch die Ausnutzung des Speichers und die Systemlast beobachtet werden. Es hat keine Konfigurationsmöglichkeiten und kann die angezeigten Daten nicht abspeichern.

Das Programm `winmsd`: Das Programm kann über *Ausführen* oder — was besser ist — über die Eingabeaufforderung ausgeführt werden. Es generiert einen Bericht über die aktuelle Hardware-Konfiguration. Normaler Weise wird er in einer hübschen, grafischen Maske angezeigt, die einzelnen Unterpunkte des Systems können über Karten abgefragt werden. Es gibt auch die Möglichkeit, den Bericht textbasiert ausgeben zu lassen.

Folgende Parameter werden von dem Programm unterstützt:

`/a`: Erstellt einen vollständigen Bericht und gibt ihn direkt auf dem Bildschirm aus.

`/s`: Erstellt lediglich eine Zusammenfassung und gibt sie auf dem Bildschirm aus.

`/p` oder `/f`: Sinnvoll im Zusammenhang mit den beiden vorherigen, gibt das Ergebnis nicht auf dem Bildschirm, sondern auf einem Drucker (`/p`) oder in eine Datei (`/f`) aus.

***Rechner*:** Nicht wirklich eine Option, gibt an, welcher Rechner untersucht werden soll.

Die Ereignisanzeige: Die bereits im letzten Abschnitt besprochene Ereignisanzeige verfügt neben dem Sicherheitsprotokoll auch über das System- und das das Anwendungsprotokoll. Im Systemprotokoll hinterläßt das Betriebsystem Hinweise[47] zu den Vorgängen des Systemes. Normaler Weise sollten Dienste, die gestartet werden, sich dort eintragen. Das Anwendungsprotokoll ist das selbe für Anwendungen.[48]

Es gibt drei verschiedene Arten von Meldungen: Informationen (gekennzeichnet durch einen blauen Klecks mit weißem **i**) zeigen lediglich an, daß irgend etwas geschehen ist. Warnungen (gekennzeichnet durch einen gelben Klecks mit einem **!**) weisen auf nicht-systemkritische Dinge hin, etwa auf nicht ladbare Dateien, deren Fehlen sich nicht negativ auf die Funktion des Programmes auswirkt. Warnungen (dargestellt durch einen roten Klecks mit einem weißen **STOP**) weisen auf schwerwiegende, besser schnell zu behebende Fehler hin.

In der Ereignisanzeige gibt es die Möglichkeit, Protokolle zu sichern.

Der Systemmonitor: Dieses ist eines der mächtigsten Werkzeuge, die von Microsoft zur Analyse laufender Prozesse bereitgestellt wird. Es bietet die Möglichkeit, für verschiedene Objekte sogenannte Grafen zu erstellen und diese in verschiedenen Diagramansichten zu präsentieren. Dies ist sowohl in Realzeit als auch im Nachhinein durch erstellen einer Log-Datei möglich. Der Systemmonitor arbeitet auch auf Remote-Rechnern. Da er eine ganze Menge an Resourcen schluckt, bietet es sich an, einen eigenen Rechner dafür abzustellen.

Zu den überwachbaren Objekten zählen die Auslagerungsdatei ebenso wie die Prozessoren und die Festplatten.[49] Bei jedem Objekt können für die Darstellung bestimmte Instanzen ausgewählt werden (etwa für die Auslagerungsdatei die Gröse oder die Anzahl von ausgelagerten Seiten pro Sekunde). Für die Erstellung von Protokoll-Dateien können nur Objekte, keine Instanzen gewählt werden.

Eine ebenfalls ausgesprochen praktische Funktion ist das Einrichten von Warnungen: Bei bestimmten Ereignissen, wenn ein bestimmtes Objekt einen Schwellenwert über- oder unterschreitet, kann an ein anzugebendes Konto eine Warnung verschickt werden. Beispielsweise ist es möglich, bei Sinken

[47] Deren Vorhandensein ist davon abhängig, ob Microsoft sie implementiert hat oder nicht.

[48] Wenn schon das Systemprotokoll auf die Implementation seitens des Herstellers angewiesen ist, dann ist es das Anwendungsprotokoll erst recht. Glücklicher Weise nutzen viele Hersteller seine Möglichkeiten.

[49] Festplatten erfordern eine Initialisierung mit dem Befehl `diskperf -y`. Dieser muß ein mal pro Festplatte durchgeführt werden. Um die „Bespitzelung“ wieder abzuschalten, wird `diskperf -n` genommen.

des Festplattenplatzes unter 20% dem Domänenadministrator eine Warnung zu kommen zu lassen.

Der Netzwerkmonitor: Dieses Programm stellt das gleiche dar, wie der Systemmonitor. Es beschäftigt sich jedoch mit Netzverkehr. Es besteht aus zwei Teilen, dem sogenannten Agenten (sollte auf allen Rechnern laufen, die überwacht werden sollen) und dem eigentlichen Programm.

Generell arbeitet dieser Monitor wie ein Paketsniffer, vergleichbar mit Ethereal (oder ähnlichen Programmen). Entsprechend arbeitet es am besten mit einer Netzwerkkarte im Promiscuous-Modus.[50] Probleme kann es da in geswitchten Netzwerken geben.

Neben diesen Werkzeugen gibt es noch einige Einstellungen, die für spätere Analysen nicht verkehrt sind. So kann unter *System*, Unterpunkt *Starten/Herunterfahren*, eingestellt werden, daß bei Auftreten eines STOP-Fehlers, also eines wirklich harten Fehlers des Systems, ein Speicherabbild erstellt und in eine dort zu benennende Datei geschrieben werden soll. Diese Datei kann mit dem Programm `dumpexam.exe` (aus dem Resource-Kit) betrachtet werden.

4.12.3 Verwertung der Informationen

Die im letzten Abschnitt genannten Programme bieten eine ganze Reihe von Informationen. Es stellt sich die Frage, wie diese denn verwertet werden können.

Zunächst ist das Programm `winmsd` ein ausgesprochen nützliches Werkzeug, um Rechnerdokumentationen zu erstellen. Immerhin trägt es alles relevante zusammen, und mit einem leicht zu schreibenden Macro kann diese Datei recht einfach in eine beliebige Textsatzsprache[51] konvertiert werden.

Die Protokolle der Eriegnisanzeige lassen sich ebenfalls abspeichern. Das geht entweder als Ereignislogdatei oder als Text-Datei abgespeichert werden. Bei der Text-Datei gibt es zudem die Möglichkeit, es als ASCII-Tabelle abzuspeichern. Das bedeutet, daß die verschiedenen Spalten durch `;` voneinander getrennt werden. Die meisten Tabellenkaulationsprogramme und Datenbanken können dieses Format einlesen. Die Vorteile einer solchen Tat liegen auf der Hand.

Der Systemmonitor ist leider nicht in der Lage, seine Protokolle als etwas anderes als von sich selbst verwertbare Dateien abzuspeichern. Die Möglichkeiten des Programmes ansich sind jedoch häufig durchaus ausreichend, um die Ergebnisse präsentationsfähig zu gestalten.

Auch der Netzwerkmonitor kann seine Ergebnisse nich exportieren. Doch auch in seinem Fall ist es möglich, mit den Programmen von Drittanbietern sein eigenes Format zu importieren.

Generell empfielt es sich, bei Beginn der Überwachung eine sogenannte Null-Linie zu erstellen. Damit ist eine Datenerhebung zu ruhiger Zeit (etwa des Nachts)

[50] Also einer Karte, die alle Pakete aufnimmt, egal, ob für sie gedacht oder nicht.

[51] Etwa LaTeX oder HTML.

und eine zu Stoßzeiten gemeint. Anhand dieser ursprünglichen Linie können spätere Daten ausgewertet und eine Trendanalyse durchgeführt werden. Ist zum Beispiel ersichtlich, daß ein bestimmter Rechner zu Stoßzeiten sich kontinuierlich verschlechternde Werte aufweißt, ist es möglich, anhand einer grafischen Darstellung (oder ein wenig mathematischem Geschick, aber das wirkt nicht so überzeugend) den Zeitpunkt für eine notwendige Erneuerung oder AUfrüstung zu bestimmen. (Falls nicht einige einfache Optimierungen des Betriebsystemes ausreichen.)

Anhang A

WLAN - Gebrauchsanweisung

In diesem Anhang wird beleuchtet, wie mit den für den Unterricht bereitgestellten Materialien ein Wireless Local Aerea Network (WLAN) aufgebaut werden kann. An der Umsetzung war die komplette Belegschaft der zweiten Reihe beteiligt, also MARCO BEUKE, ORTWIN EBHARDT, DETLEF PETRY, CHRISTIAN SCHALK und DANNY WEILER.

A.1 Geräte

Die Geräte stammen alle von der Firma Dr. Neuhaus. Sie entsprechen dem Standard IEEE 802.11 und arbeiten mit 11 Mbp/s.

Das Set besteht aus einem Access Point und mehreren PCMCIA-Karten. Letztere funktionieren einwandfrei in Notebooks. Ebenfalls dabei sind zwei PCI-Adapterkarten; sie stellen PCMCIA-Slots für normale PCs bereit.

Der Access Point wird über ein Netzwerkkabel angeschlossen. Er verfügt über eine eigene IP und kann in ein beliebiges Netz integriert werden. Um ihn direkt an einen PC anzuschließen (wie in diesem Beispiel geschehen) ist ein Crossover-Kabel erforderlich.[1]

A.2 Vorbemerkung

Wann immer im Folgenden die Rede von der Instalation von CD ist, sollte einfach das Setup-Programm im Rootverzeichnis der CD ausgeführt werden. Hier ist es recht einfach, das richtige Programm einzustellen.

Im Interesse eines reibungslosen Betriebes ist es erforderlich, die „normalen“ Netzwerkkarten entweder zu deaktivieren, heraus zu nehmen oder mindestens in ein anderes Netz zu stellen als die WLAN-Karten.

Der Übergang von Funk- in Festnetz würde über einen Router funktionieren. Leider haben wir Windows 98 nicht dazu bekommen, als solcher zu arbeiten.

[1] Wer über das beiliegende läßtert soll sich selbst eins klemmen!

A.3 Der Access Point

Der Access Point kann sowohl unter Windows 98 als auch unter Windows 2000[2] in Betrieb genommen werden.

Die Konfiguration geschieht mittels des *FuryLan APManagers*. Selbiger kann von den beiliegenden Disketten oder — in einer neueren Version — von der beiliegenden CD installiert werden.

Zu beachten ist, daß der Access Point in den meisten Fällen über ein Crossover Kabel an der einzigen im Rechner befindlichen Netzwerkkarte hängt. Das hat zur Folge, daß DHCP-Anforderungen natürlich nicht mehr behandelt werden können.. Es empfielt sich daher, die IP-Adresse und die Netzwerkmaske von Hand zu konfigurieren.

Nach der Installation und dem Aufrufen des APManagers ist noch kein Access Point eingetragen. Dies läßt sich am besten durch den unter dem Menüpunkt *FILE* befindlichen Punkt *Build from Network* bewerkstelligen. Hierdurch wird eine Art Assistent gestartet.

Die Angaben der ersten Maske (das eigene Netzwerk und die Netzwerkmaske) sollten in Ordnung sein. Falls nicht, gibt es die Möglichkeit einer Änderung.

In der zweiten Maske kann das Netzwerk nach einem Access Point durchsucht werden. Falls er nicht gefunden wird (etwa, weil er nicht konfiguriert ist und daher nicht über eine IP-Adresse verfügt), muß er manuell hingefügt werden. Dies geschieht über seine MAC-Adresse. Diese steht auf der Unterseite des Gerätes und lautet in diesem Fall:

`00-90-4B-08-91-D9`

In der nächsten Maske muß die Netzwerk-ID (SSID) angegeben werden. Wir haben in unserem Fall die Kennung `adpc` gewählt. Diese Kennung muß bei allen im WLAN befindlichen Geräten identisch sein. Der Kanal ist unerheblich, die Einstellung `10` arbeitet einwandfrei.

In der folgenden Eingabemaske kann das Sicherheitssystem angegeben werden. Wir haben darauf verzichtet. Ebenfalls angegeben werden kann ein *Community String*, der als Paßwort für die Netzverwaltung dient. Wir haben ihn bei `private` belassen.

Nach Abschluß der Konfiguration wird der Access Point neu initialisiert. Das ist unter anderem daran zu sehen, daß die mit *ACT* beschriftete, dunkelrote LED zu flackern beginnt. Danach kann der Access Point in einer Baumähnlichen Struktur unter seiner IP in dem Unterpunkt *adpc* (der Netzwerkkennung) eingesehen und bei Bedarf rekonfiguriert werden.

A.4 Die Karten — W2K /XP

Unser einziger erfolgreicher Test wurde auf einem Notebook unter Windows XP durchgeführt. Das Notebook erkannte die Karte beim Starten selbsttätig und ver-

[2] Vermutlich auch unter Windows XP.

langte nach Treibern. Selbige wurden von der beiliegenden CD geliefert. In dem beiliegenden Konfigurationsprogramm konnte die Verbindung sofort und ohne Probleme hergestellt werden.

A.5 Die Karten — W98

Unter Windows 98 muß als erstes der Treiber für den PCMCIA-Adapter installiert werden.

Bei dieser Installation wird zunächst gefragt, ob irgend welche SCSI-Adapter genutzt werden. Im Rahmen dieser Schulungsumgebung sollte das nicht der Fall sein, und so ist es sicher, hier auf *Nein* zu gehen. Im nächsten Punkt wird gefragt, ob der Benutzer die Auswahl eventuell zu deaktivierender Busse manuell vornehmen möchte. Es ist in diesem Fall sicherer, diese Aufgaben Windows zu überlassen. Nach diesen Angaben sollte der Adapter korrekt installiert werden.

Zur Installation der FuryLAN *müssen* die originalen Disketten verwendet werden; die neuren Treiber von CD funktionieren ***nicht***. Die Installation ansich funktioniert am besten über die Hardware-Erkennung. Zwar werden die Karten nicht bei der Durchsuchung gefunden, über den Punkt *nicht erkanntes Gerät installieren* und den dortigen Punkt *Diskette* funktioniert es dennoch.

Für den tatsächlichen Verbindungsaufbau wird die Konfigurationssoftware benötigt. Diese liegt nicht auf Diskette bei, daher muß diese nun wieder von der CD installiert werden. Das installationsprogramm ist

`\pcmcia\setup\setup`

Hiernach kann die Verbindung wie unter XP mit Hilfe des Konfigurationsprogrammes aufgebaut werden.

Anhang B

Der Palm als Terminal

Dieser Artikel beschreibt die Einrichtung eines Palmes als Terminal an einer seriellen Schnittstelle eines Linux-Rechners. Beleuchtet werden die erforderlichen Einrichtungen unter Linux und auf dem Palm sowie verschiedene Prüfmethoden.

B.1 Vorweg

Vor der eigentlichen Einrichtung muß geklärt sein, welche Hardware vorhanden und welche Software noch zu besorgen ist. Außerdem schaden ein paar Gedanken zum Sinn und Zweck der Übung nicht.

B.1.1 Sinn und Zweck

Auf den ersten Blick scheint die ganze Übung nicht sonderlich sinnvoll; die Eingabe der Zeichen ist mehr als schwierig (da das Palm Modell nicht über eine Tastatur, sondern nur über einen Stift verfügt), die Arbeit geschieht im reinen Textmodus, und die Darstellung ist auch eher klein.

Doch näher betrachtet ergeben sich eine ganze Reihe von Möglichkeiten: Die hier betrachtete Verbindung über die serielle Schnittstelle funktioniert prinzipiell auch über die Infrarot-Schnittstelle.[1] Darüber hinaus arbeitet das Terminal nicht nur mit einem Linux-Server, sondern auch mit anderen Geräten, die Verwaltungskonsolen über die serielle Schnittstelle bereitstellen, zusammen.[2] Zudem gibt es wohl auch Palms, die über eine ausklappbare Tastatur verfügen. Und ein Palm ist bequemer zu transportieren als ein entsprechender Laptop.

B.1.2 Die Umgebung

Der Palm ist ein*Palm Vx*, die Betriebsystemversion ist 3.5.2, er wurde über das zun seiner Dockingstation gehörende HotSync-Kabel angeschlossen.

[1]Das wurde allerdings nicht getestet.

[2]Fast alle Geräte der Firma CISCO verfügen über einen sogenannten *Management-Port*; allerdings ist dafür ein Adapter notwendig.

Bei dem Rechner handelt es sich um einen „normalen“ PC mit zwei freien seriellen Schnittstellen. Das HotSync-Kabel hängt an der ersten. Die benutzte Linux-Distribution ist RedHat 8.0[3] mit dem vorgefertigten Kernel.

Um das Linux-System zu testen, können ein anderer Rechner unter Windows (95 oder höher[4]) und ein Nullmodemkabel verwendet werden.

B.1.3 Erforderliche Materialien

Für den Palm wurde das Programm *Pilot vt100* genommen. Hierbei handelt es sich um eine nicht sonderlich komfortabele vt100 Emulation. Sie stellte sich jedoch als die einzig lauffähige heraus. Sie kann unter anderem auf der Seite
`http://www.frotz.net/vt100/`
heruntergeladen werden.

Unter Linux muß ein Kernel verwendet werden, der das Betreiben einer Konsole an einer seriellen Schnittstelle unterstützt. (Das sind die unter *Character Devices* zu findenden Punkte *Support for Console on Serial Port* und *Standard generic Serial Support*.) Die bei den meisten Distributionen vorinstallierten Kernel tun das.

Außerdem wird das Programm `agetty` gebraucht.[5]

B.2 Einrichtung

Die Einrichtung geschieht in zwei Schritten: Zunächst muß der Linux-Rechner, danach der Palm eingrichtet werden. Um Fehlerquellen auszuschalten, empfielt sich ein Test des Linuxrechners mit Hilfe eines anderen Rechners. Im Folgenden wird davon ausgegangen, daß die in B.1.3, S. 102 aufgeführten Dinge vorhanden sind.

B.2.1 Einrichten unter Linux

Die grundsätzliche Einrichtung ist recht einfach; der Rechner muß dazu gebracht werden, auf der seriellen Schnittstelle eine Konsole zu Verfügung zu stellen. Das passiert in der Datei `/etc/inittab`. Rein prinzipiell ist es egal, wo dort der entsprechende Eintrag erfolgt, doch prinzipiell empfielt es sich, es bei der Definition der virtuellen Terminals vorzunehmen.

Diese Definition sieht wie folgend aus:

```
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

[3]Da die von der Konfiguration betroffenen Dateien Distributions-uanbhängig sind, ist das egal.

[4]Es geht vermutlich auch mit Terminalprogrammen unter DOS oder Windows 3.11.

[5]Statt dessen kann auch `mgetty` benutzt werden, aber `agetty` ist nach Ansicht des Verfassers komfortabler.

Diese Textzeilen weisen den Rechner an, in den Runleveln 2 – 5 den Befehl `mingetty` auf den virtuellen Terminals[6] `/dev/tty1` bis `/dev/tty6` auszuführen. `mingetty` führt den Login durch und verwaltet die gesammten Texteingaben. Sobald ein `mingetty` beendet wird (etwa weil der Benutzer sich ausloggt), wird es neu gestartet (das bewirkt die Option `respawn`).

Die zu ergänzende Zeile lautet:

```
7:2345:respawn:/sbin/agetty -L 9600 ttyS0
```

Die Zeile ist fast identisch mit der eines virtuellen Terminals. Der Unterschied zwischen `mingetty` und `agetty` besteht darin, daß `agetty` für die Arbeit mit seriellen Verbindungen (meistens eher Modems) gedacht ist. `mingetty` ist nur für virtuelle Terminals gedacht. Der Parameter `-L` gibt an, daß es sich um eine lokale Verbindung handelt; dies ist wichtig, da ansonsten verschiedene Behandlungen des Carrier-Signals durchgeführt werden. `9600` ist die Verbindungsgeschwindigkeit in Baud. (In diesem Fall ist das tatsächlich identisch mit Bit/s.)[7] `ttyS0` schließlich ist die im Verzeichnis `/dev` liegende Gerätedatei der ersten seriellen Schnittstelle.

Falls es `root` möglich sein soll, sich über die serielle Schnittstelle einzuloggen, muß `ttyS0` in der Datei `/etc/securetty` eingetragen werden. Für gewöhnlich wird das nicht getan, da ein Einloggen von `root` über ein Modem als großes Sicherheitsrisiko angesehen werden muß.

Anders als bei Windows ist kein Neustart erforderlich, um diese Konfiguration zum Laufen zu bringen; es reicht der Befehl `init q`.

B.2.2 Vereinfachungen

Einige Dinge bei der Arbeit mit dem Palm haben sich als *ausgesprochen* nervig erwiesen. Das liegt in erster Linie an der unkomfortabelen Texteingabe. Großbuchstaben gehören nicht unbedingt zu den Stärken dieser Methode, so daß ein typisches Paßwort (sieben Stellen, mindestens zwei davon Zahlen und mindestens ein Großbuchstabe dazwischen) zur argen Geduldsprobe werden kann. Aus diesem Grund empfielt sich für Test- und Demonstrationszwecken ein Benutzer `p` (wie *Palm*), der kein Paßwort benötigt.

Um das zu erreichen, kann der Benutzer einfach mittels `useradd -m p` angelegt werden. Um die Paßwortabfrage zu deaktivieren, reicht es aus, das `x` in der zweiten Spalte der Datei `/etc/passwd` in der Zeile des Benutzers `p` zu löschen.

B.2.3 Testen der Linuxreinrichtung

Bevor nun der Palm angeschlossen wird, empfielt sich ein Test des Linux-Servers. Das läßt sich am besten mit Hilfe eines zweiten Rechners, der mittels eines Nullmodemkabels mit dem Linuxrechner verbunden ist, bewerkstelligen.

[6]Das sind die Konsolen, auf denen sich ein Benutzer an einem Rechner anmelden kann und die mit den Tasten `<ALT>+<F1>` – `<ALT>+<F6>` erreicht werden können.

[7]Sowohl der Palm als auch die PC-Schnittstellen können eine höhere Geschwindigkeit, bei Tests haben sich diese aber nicht als praktikabel erwiesen.

Unter Windows wird dieser Test mit dem Programm *Hyperterminal* durchgeführt.[8] Beim ersten Start des Programmes erfolgt eine Auforderung, Informationen üebr den Standort anzugeben. Die wären nötig, falls jemand tatsächlich mittels Hyperterm (und AT-Befehlen und so weiter) auf ein Modem zugreifen möchte. In diesem speziellen Fall ist es egal, was dort eingetragen wird.

Wichtig sind die Einstellungen der seriellen Schnittstelle: Die Geschwindigkeit sollte 9600 betragen, es werden 8 Bit, ein Stoppbit, keine Parität und keine Flußsteuerung benutzt.

Danach sollte es möglich sein, eine Verbindung zu dem Linuxrechner aufzubauen. Nach einer (clientseitigen) Initialisierung mittels `<Return>` sollte der Login-Schirm erscheinen.

B.2.4 Einrichten des Palms

Die serielle Schnittstelle muß wie bereits in B.2.3, S. 104 angegeben eingestellt werden. Des weiteren ist in dem Programm *Pilot vt100* im Menü *Options* der Punkt *com* zu überprüfen; meistens ist hier eine falsche Geschwindigkeit (2400 Baud) eingestellt. Außerdem sollte das lokale Echo abgeschaltet werden. Um die Verbindung zu eröffnen, wird das Käßtchen *online* aktiviert.

Auch bei dem Palm muß zur initialisierung ein `<Return>` gesendet werden. Um vorher zu testen, ob die Einstellungen korrekt sind, empfielt sich folgende auf dem Linuxrechner eingegebene Befehlszeile:

```
echo Hallo>/dev/ttyS0
```

Falls auf dem Palm tatsächlich `Hallo` erscheint ist die Verbindung korrekt.

B.3 Betrieb und weitere Ansätze

Mit dem vorliegenden Palm gestaltete sich der Betrieb zugegebener Maßen ausgesprochen kompliziert. Vermutlich gibt es Möglichkeiten, die Zeilenbreite genauer einzustellen, denn zumindest das Programm `pine` ist in seiner Darstellung einfach zu breit. Für sinnvolles Arbeiten mit dem `vi` (oder gar `emacs`...) ist die Zeicheneningabe nicht wirklich genau genug. Um die Möglichkeiten einer solchen Verbindung ansatzweise aufzuzeigen, reicht die Konfiguration jedoch aus.

Es gibt eine ganze Reihe von Fragen, die noch offen sind und die ein eifriger Admin bedenken kann. Etwa die Frage, ob es neben vt100 noch anderen Terminaltypen erhältlich sind. Auch die Verbindung via Infrarot wäre sicherlich interessant.

Vermutlich ebenfalls interessant wäre die Nutzung von `telnet` oder die diversen anderen Möglichkeiten, sich auf einem anderen Rechner einzuloggen und beispielsweise dessen Internetfähigkeiten zu nutzen. Dieses erfordert jedoch einen laufenden `pppd`-Server und hat am Ende mit der grundsätzlichen Überlegung, nämlich dem Ansteuern eines seriellen Konsolenportes, nichts mehr zu tun.

[8] Natürlich geht das auch mit Linux... der Verfasser geht jedoch davon aus, daß jemand, der `minicom` kennt, keine Anleitung braucht.

Anhang C

Ergänzungen zu TCP/IP

C.1 Rechnen mit Subnetzen

Dieser Anhang enthällt Abkürzungen für das Rechnen mit Subnetzen sowie eine Anleitung für die Konvertierung von Dezimalzahlen zu Binärzahlen.

C.1.1 Das binäre Zahlensystem

Das gewöhnliche dezimale System hat als Ausgangsbasis die 10. Es wird bis 9 gezählt, danach beginnt es mit der ersten Zahl und einer 0. Das binäre System hat die 2 als Basis. In Tabelle C.1, S. 106 finden sich die ersten 11 Zahlen des Binärsystems aufgeführt. Es stellt sich jedoch die Frage, wie sich dezimale Zahlen in Binäre Zahlen umwandeln lassen (und umgekehrt). Da diese Übung vor allem der Arbeit mit IP-Adressen dienen soll, wird von einer maximalen Länge von 8 Stellen ausgegangen.

Die Umrechnung einer binären Zahl in eine dezimale erfolgt recht einfach. Mathematisch gesehen lautet die Formel[1]:
$\sum_{n=0}^{i} b_{i-n} \times 2^{i-n}$.

Damit kann natürlich neimand wirklich etwas anfangen. Daher wird nun nochmals aufgezeigt, was dieses Wirrwarr eigentlich besagt.

Es wird von rechts gezählt. Für jede mit 1 belegte Stelle wird $2^{\text{Stelle}-1}$ zum Gesamtergebnis gezählt. Als Beispiel dient die in Tabelle C.2, S. 107 aufgezählte Umrechnung der Zahl 10101001.

Die erste Stelle (von rechts gezählt!) ist eine 1, und 2^0 ist 1. Die folgenden Stellen sind mit 0 belegt und $0 \times \text{irgendwas}$ ist immer 0, also brauchen sie nicht weiter beachtet zu werden. Die vierte Stelle ist wiederum eine eins, und 2^3 ist 8. Als Gesammtergebnis haben wir damit 9. Die nächste belegte Stelle ist die 5, und 2^4 ergibt 32 (was ein Gesamtergebnis von 41 ergibt). Die letzte belegte Stelle ist die achte, und 2^7 sind 128. Damit ist das Gesamtergebnis 169.

[1] Das läßt sich mathematisch beweisen, der Verfasser hat aber definitiv keine Lust dazu!!

Dezimal	Binär	Dezimal	Binär
0	0	6	110
1	1	7	111
2	10	8	1000
3	11	9	1001
4	100	10	1010
5	101	11	1011

Tabelle C.1: Die ersten 11 Zahlen des Binärsystems

Die Gegenrichtung, also das Umrechnen einer Dezimalzahl in Binär, ist für viele Belange interessanter. Hierfür gibt es mehrere Möglichkeiten.[2] Das folgende Verfahren funktioniert recht gut:

1. Als erstes wird die Anzahl der Stellen bestimmt. Dieser findet sich durch den größtmöglichen Teiler des Wertes, der eine Potenz von zwei ist. Allerdings kommt dann noch eine Stelle dazu (da ja 2^0 ebenfalls eine Stelle belegt).

2. Für die erste Stelle (diesesmal von *links* gezählt) wird eine `1` vermerkt, die Zahl wird um die gefundene Zweierpotenz veringert.

3. Für jede nächst kleinere Zweierpotenz wird probiert, ob sie in den verbleibenden Rest paßt. Ist dieses nicht der Fall, wird an die entsprechende Stelle eine `0` gesetzt und zur nächst kleineren gegangen. Falls sie paßt, wird eine `1` gesetzt und der Wert wiederum um die Zweierpotenz verringert und mit dem Vorgang fortgefahren.

4. Sobald der Wert bei 0 angelangt ist, *müssen* die verbleibenden Stellen mit `0` besetzt werden.

Um dieses Vorgehen näher zu illustrieren, wurde es mit dem Wert 94, abgebildet in Tabelle C.3, S. 107, durchgeführt.

C.1.2 Rechenhilfen

Häufig gestellte Aufgaben beschäftigen sich damit, die Netz- oder Broadcastadresse eines Rechners mit nicht klassengebundener Netzwerkmaske zu identifizieren. Die folgenden vier Methoden sollen helfen, diese Ergebnise möglichst schnell zu bekommen. Einige davon werden dem einen oder anderen offenkundig erscheinen, aber nicht jeder hat den gleichen Wissensstand.

Grundlegendes: Um die entsprechenden Netze zu errechnen, ist es nur nötig, das Oktet zu betrachten, in dem sich die zusätzlichen Bits der Netmask befinden.

[2] Der Verfasser hat bisang keine Formel dafür gefunden; er hat sie auch nicht wirklich gesucht.

Zahl	**Stelle**	**Rechnung**			
1	0	$1 \times 2^0 =$	1×1	=	1
0	1	$0 \times 2^1 =$	0×2	=	0
0	2	$0 \times 2^2 =$	0×4	=	0
1	3	$1 \times 2^3 =$	1×8	=	8
0	4	$0 \times 2^4 =$	0×16	=	0
1	5	$1 \times 2^5 =$	0×32	=	32
0	6	$0 \times 2^6 =$	0×64	=	0
1	7	$1 \times 2^7 =$	0×128	=	128
Macht:					169

Tabelle C.2: Umrechnung der Binärzahl 10101001 ins Dezimalsystem

Errechnen der Betzwerkmaske: Sobald die Netzwerkmaske in dezimaler FOrm vorliegt, werden alle Operationen einfacher. Falls sie nur in Form einer /x-Notation vorliegt, empfielt es sich, zunächst die regulären Klassen zu identifizieren (sprich, zu sehen, wie oft sich 8 davon abziehen läßt). Was übrig bleibt, sind die zusätzlichen Bits der Maske. Je nach dem, ob es mehr freie oder belegte Bits gibt, kann nun entweder der Hostteil oder der Netzteil errechnet werden.

Hostteil ist bekannt: Sobald der Hostteil bekannt ist, kann die Netzwerkmaske errechnet werden, indem die Host-Zahl von 256 abgezogen wird. Die Anzahl der verschiedenen Netze ergibt sich durch Teilen von 256 durch die Hostanzahl.

Netzmaske ist bekannt: Die Anzahl der Hosts pro Netz ergibt sich durch Abziehen der Netzmaske von 256.

Wert	**Potenz**			**Wert**	**Rest**
94	2^6	=	64	1	30
30	2^5	=	32	0	30
30	2^4	=	16	1	14
14	2^3	=	8	1	6
6	2^2	=	4	1	2
2	2^1	=	2	1	0
0	2^0	=	1	0	0
Macht:				1011110	

Tabelle C.3: Umrechung der Zahl 94 ins Binärsystem

C.2 Einige Programme

In diesem Anhang werden drei recht nützliche Programme für die Systemadministration vorgestellt, nämlich `ipconfig`, `arp` und `telnet`.

C.2.1 Der Befehl `ipconfig`

Der Befehl `ipconfig` ist ein Standard-TCP/IP-Befehl. Unter UNIX heißt er oft `ifconfig`, hat aber den gleichen Grundeffekt: Es werden die TCP/IP-Daten der Netzwerkkarten angegeben. Je nach Betriebsystem kann dieser Befehl aber ncoh sehr viel mehr.

Unter Windows bietet der Schalter `/all` die Möglichkeit, sich sehr viele Daten anzeigen zu lassen. Insbesondere werden hier auch Informationen über den DHCP-Status des Rechners bereit gestellt.

Die für DHCP entscheidenden Schalter lauten

`/release`: Gibt die vom DHCP-Server georderte Adresse wieder frei

`/renew`: Fordert beim DHCP-Server eine neue Adresse an. Falls noch eine eigene DHCP-Adresse vorhanden ist, wird sie überschrieben.

`/registerdns`: Dieser eigentlich fÜr DNS gedachte Schalter führt zu einer Aktualisierung aller Leases.

`/showclassid` *`Adapter`*: Zeigt die für den angegebenen Netzwerk in Frage kommenden DHCP-Klassen an.

`/setclassid` *`Adapter`*: Setzt die Klasse des Adapters.

Auch für DNS gibt es eine Reihe von Schalter. Im einzelnen sind es:

`/flushdns`: Löscht den aktuellen DNC-Cache des Rechners.

`/registerdns`: Neben seiner Wirkung für DHCP registriert dieser Schalter den FQDN des Clients beim DNS-Server.

`/displaydns`: Zeigt den Inhalt des DNS-Chaches an.

Falls der Rechner aus irgend welchen Gründen über eine APIPA-Adresse verfügt, wird das ebenfalls angegeben.

C.2.2 Der Befehl `arp`

Der Befehl `arp` dient der Manipulation des `arp`-Chaches. Dieser Cache beinhaltet die aktuelle Auflösung von MAC-Adressen zu IP-Adressen. Von Interesse sind die folgenden drei Optionen:

`-a`: Zeigt alle aktuellen Einträge an.

-s *IP-Adresse MAC-Adresse*: Trägt eine Zuordnung permanent (also bis zum nächsten Reboot) ein.

-d *IP-Adresse*: Löscht einen Eintrag.

MAC-Adressen werden in Form von sechs Hex-Zahlenpaaren angegeben.

C.2.3 Der Befehl `telnet`

Eines der ältesten und für den Test des Betriebes wichtigsten TCP/IP-Programme ist `telnet`. Egal ob Windows, Unix oder Cisco-Gerät,[3] all diese Geräte verfügen über einen `telnet`-Client.

Das Programm stellt eine Verbindung über einen anzugebenden Port her. Handelt es sich auf der anderen Seite ebenfalls um einen `telnet`-Port, erhällt der Benutzer die Kommandozeile des serverseitigen Betriebsystemes und kann damit remote Befehle ausführen.

Es ist jedoch auch möglich, vollkommen andere Ports, etwa den `smtp`-Port, anzusprechen. Die hier möglichen Befehle lassen sich meistens mittels `help` abrufen. Auf diese Weise Mails zu lesen oder zu verschicken ist zwar ausgesprochen umständlich, stellt aber eine einfache Methode dar, die Funktionstüchtigkeit des Netzes zu überprüfen.

Eine Anmerkung zur Fernadministration über `telnet`. Davon ist *dringend* abzuraten, da dieses Programm die entsprechenden Daten in Klartext übermittelt. Das gilt auch für das Paßwort!

Der Aufruf des Programmes erfolgt über:

`telnet` *`Ziel-IP Port`*

Bei Weglassen des Ports wird automatisch von Port 23 (also `telnet`) augegangen.

[3]Sofern es über ein IOS verfügt.

Tabellenverzeichnis

3.1 Ergebnisse der AND-Operation 29
3.2 Bestimmung der Netzwerkadresse 29
3.3 Die IP-Adress-Klassen 30
3.4 Klassenlose Netzwerkmaske 31
3.5 Die 8 Netze binär geschrieben 32
3.6 Wichtige Protokolle 34
3.7 Einige Ports 35

4.1 Eigenschaften globaler und lokaler Gruppen 57
4.2 Die Zusammensetzung der vordefinierten NTFS-Berechtigungen . 59
4.3 Prioritätsklassen 72
4.4 Rechnerfähigkeiten zur Dateireplikation 90

C.1 Die ersten 11 Zahlen des Binärsystems 106
C.2 Umrechnung der Binärzahl 10101001 ins Dezimalsystem 107
C.3 Umrechung der Zahl 94 ins Binärsystem 107

Abbildungsverzeichnis

3.1 Das ISO/OSI-Referenz-Modell 24
3.2 Eine Gegenüberstellung des ISO/OSI und des DoD-Modells . . . 28
3.3 Domain Name Service 40

4.1 Festplatten unter Windows NT 4.0 49
4.2 Ein Beispiel für die Datei `boot.ini` 51
4.3 Die Freigabe des Rechners `md_ geist.anime` 58
4.4 Die Berechtigungen des Adminitrators `mstringray` 61
4.5 Windows NT Schichten 70
4.6 Einseitige Vertrauensstellung 75
4.7 Drei Domänen mit unterschiedlichen Vertrauensstellungen 76
4.8 Einzeldomänenmodell 77
4.9 Hauptdomänenmodell 78
4.10 Mehrfachhauptdomänenmodell 79
4.11 Vollständiges Vertrauensmodell 79
4.12 Eine DCOM-Verbindung 80
4.13 Anschlußmöglichkeiten für Drucker 83
4.14 NetWare-Zugriff über CSNW und GSNW 88
4.15 Rechnerfähigkeiten zur Dateireplikation 89
4.16 Netz mit Backup-Server 90
4.17 Backup-Methoden im Vergleich 91

Literaturverzeichnis

[1] DROMS, R. (Herausgeber): *Dynamic Host Control Protocol (RFC2131)*. Network Working Group, 1996.

[2] EBHARDT, ORTWIN: *Linux — Mitshriften und Ergänzungen*. `http://www.dreibund.de`, 2003. Grundlagenskript.

[3] FISCHER, MARKUS: *Hardwaregrundlagen*. `http://www.hardware-grundlagen.de`, 2003.

[4] FRISCH, ÆLEEN: *Windows NT System Administration*. O'Reilly, 1998. Deutsche Übersetzung von Andreas Roeschies.

[5] HUNT, CRAIG: *TCP/IP*. O'Reilly & Associates, Inc., 2 Auflage, 1998.

[6] HUNT, CRAIG und ROBERT BRUCE THOMPSON: *Windows NT TCP/IP Netzwerk-Administration*. O'Reilly, 1999.

[7] KOZIEROK, CHARLES M.: *The PC Guide*. `http://www.pcguide.com`, 2001.

[8] MASHIMO, MITSUHARU: *Crime War*, Teil 2 der Reihe *Dominion Tank Police*, 1989. Auf: *Dominion Tank Police*, Anime Studio Inc., 2000. RC0 DVD.

[9] MCQUERRY, STEVE (Herausgeber): *Interconnecting Cisco Network Devices*. Cisco Press. Markt+Technik-Verlag, München, 2000. Das offizielle Kursbuch für die CCNA-Zertifizierung 2.0, Prüfungsnummer 640-507.

[10] MICROSOFT (Herausgeber): *Netzwerkadministration*. Windows NT 4.0 Training. Microsoft Press, 1997.

[11] MICROSOFT (Herausgeber): *Technischer Support*. Windows NT 4.0 Training. Microsoft Press, 1997.

[12] MICROSOFT (Herausgeber): *Microsoft Windows 2000 — Grundlagen zum Netzwerk und Betriebsystem*. Microsoft, 2000. Kurs 2046A.

[13] REITMAN, IVAN: *Ghostbusters*, Teil 1, 1984. Auf: *Ghosbusters Double Pack*, Columbia Tristar Home Entertainment, 2001. Enthällt O.-Ton mit ausbl. dt. Ut. RC2 DVD.

[14] SLAYER: *Disciple*. Lied 2 der CD *God hates us all*. American Recording, LLC, 2001.

[15] WEBER, RALPH O. (Herausgeber): *Project 1157-D (Information technology - SCSI Architecture Model - 2 (SAM-2))*. T10, 2002.

Index

.pol, 69
[boot loader], 51
[operating systems], 51
%username%, 65
arp, 108
boot.ini, 50
bootsec.doc, 50
convert.exe, 53
dhcpadmn.exe, 63
diskperf, 94
hosts, 39
ipconfig, 38, *108*
lmhosts, 38
net use, 84
netlogon, *66*, 69
nmbd, 89
ntbootdd.sys, 50
ntdetect.com, 50
ntldr, 50
poledit.exe, 63, *68*
rasadmin.exe, 63
rdisk, 74
regedit, 73
regedt, 73
rplmgr.exe, 63
sam, sam.log, 73
smbd, 89
srvmgr.exe, 63
start
  /*Prioritätsklasse*, 72
  /seperate und /shared, 71
sysdiff.exe, 48
telnet, 109
unattend.txt, 47
usrmgr.exe, 63
winmsd, *93*, 95
winnt.exe, 45
winnt32.exe, 45
winsadmn.exe, 63
Überwachungsrichtlinie, 92
70:30-Regelung, 37

Abwartskompatibilität, 71
Adressklassen, 29
AGP, 5, 7
Alleinstehender Server, 44
AND, 28
Anmeldescript, 66
Anwendungsschicht, 70
  DoD, *28*
  ISO/OSI, *27*
API, 71
APIPA, Automatic Private IP Adressing, *37*, 108
Application Layer
  DoD, 28
  ISO/OSI, 27
Arbeitsgruppe, 44
ARC-Pfad, 50
ARP, 27
Authentifizierung, 75, *78*, 81

Backoffice, 80
Backup, 90
  Differenziell, 91
  Inkrementell, 91
  Strategie, 91
  Vollständig, 91
Basisverzeichnis, 65
BDC, Backup Domain Controller, 44, *74*
Benutzer, *53*, 75

Anmeldescript, 66
Basis- oder Heimverzeichnis, 65
Erstellung, 53
Global, 53, *55*
Lokal, 53
Manager, *53*, 63, 64, 76
Profil, 66
Lokal, 66
Servergespeichert, *66*, 67
Verbindlich, *66*, 67
Rechner, 65
Rechte, 55
Standard, 62, *68*
Verwaltung, 62, *67*
Zeit, 64
Berechtigung
Drucker, 85
Drucken, 85
Kein Zugriff, 85
Verwalten, 85
Vollzugriff, 85
Effektiv, 60
Freigabe, *57*, 60
Andern, 58
Kein Zugriff, *57*, 61
Nur Lesen, 57
Vollzugriff, 58
NTFS, *58*, 60
`D`, Löschen, 59
`O`, Besitz übernehmen, 59
`P`, Berechtigungen ändern, 59
`R`, Lesen, 58
`W`, Schreiben, 59
`X`, Ausführen, 59
Keine Berechtigung, *59*, 61
Betriebsystemschichten, 70
BGLR-Prinzip, *56*, 77
BIA, 24
Binares Zahlensystem, 105
Bindung, 88
BIOS, 10
Bootdiskette, 50
Bootmanager, 50
Bootpartition, 49
Bootreinfolge, 11
Bord, 6
Bridge, 25
Broadcast, *31*, 36, 38
Broadcast Domain, 26
Bubblejet, 19
Bus
Accellerated Graphic Port (AGP), 7
CNR Riser, 7
Extended Standard Industrial Architecture (EISA), 6
Industrial Standard Architecture (ISA), 6
Microchanel (MCA), 6
Peripheal Components Interconnect (PCI), 7
Vesa Local (VLB), 7

Cache
First Level (L1), 5
Second Level (L2), 5
CD-ROM / DVD, 9
Chunks, 16
CMOS, 10
CMYK, 22
CNR Riser, 7
Collision Domain, 25
Computer Suchdienst, 88
CPU, 5
CSMA/CA, Carrier Sense Multible Access / Collision Avoid, 25
CSMA/CD, Carrier Sense Access / Colision Detect, 25
CSNW, 88

DARPA, 27
Darstellungsschicht, 27
Data Frame, 24
Data Link Layer, 24
Dateirecht, 61
Dateisystemkonvertierung, 52
Datenkollision, 25
Datenrahmen, 24

Datenträger, 52
Datum, 10
DCOM, 80
Demultiplexen, 34
Developer Roller, 19
DFÜ, Datenfernübertragung, 81
  Netzwerk, 81, 82
  Verbindung, 82
DHCP, Dynamic Host Configuration Protocol, *36*, 46, 108
  Paket
    DHCPACK, 37
    DHCPDECLINE, 36
    DHCPDISCOVERY, 36
    DHCPINFORM, 38
    DHCPNACK, 37
    DHCPOFFER, 36
    DHCPRELEASE, 37
    DHCPREQUEST, 37
  Relay-Agent, 37
Discharge Lamp, 20
DLC-Protokoll, 84
DNS, Domain Name Service, 39, *40*, 108
DoD, 27
  Modell, 27
  Schicht
    1: Zugangsschicht, 27
    2: Internetschicht, 27
    3: Transportschicht, 28
    4: Anwendungsschicht, 28
Domäne, 44
  Konten, 76
  Modell, 77
    Einzel, 77
    Haupt, 77, *77*, 78
    Mehrfachhaupt, *77*, 79
    vollst. Vertrauen, *78*, 79
  Resourcen, 75
  vertrauend, 75
  vertraute, 75
DOS-Programme, 71
DPI, 18
Drucker, *17*, 82, 83
  Anschluß, 84
  Box, 21
  Dedizierter Server, 21
  Einrichtung, 84
  Farb, 22
  Impact und Non-Impact, 18
  Laser, 19
  Lokal, 83
  Matrix, 18
  Monitor, 84
  Nadel, 18
  Netzwerk, 83
  PCL und PostScript, 86
  Pool, 87
  Printerports, 84
  Prioritä t, 85
  Server, *20*, 84
  Spoolereinstellungen, 85
  Thermo, 20
  Tintenstrahl, 18
    Bubblejet, 19
    Piezzo, 19
  Treiber, 84
  Trennseite, 86
  Typenrad, 20
  Verwaltung, 85
  Zeilen und Seiten, 18
  Zeitplanung, 85
Druckgerät, 83
DUN, 81
Duplexing, 17

Einstiegspunkt, 58
EISA, 6
Emergency Repair Disc, 74
ERD, 74
Ereignisanzeige, 93–95
  Anwendungsprotokoll, 94
  Sicherheitsprotokoll, 93
  Systemprotokoll, 94
Explorer, 57
Export-Server, 89

FAT, 46

FAT32, 46
FCC-Nummer, 10
FDC, 8, 11
Federal Communication Commission, 10
Festplatte, *9*, 10, 15
FQDN, 39
Freigabe, 57
Frontoffice, 80
Full Qualified Domain Name, 39
Fuser, 19

Gateway, 88
GDI, 21
Gehäuse, 3
Grafikkarte, 4, *8*, 11
Gruppe, *53*, 54
  Domänenbenutzer, 55
  Global, *55*, 56, 77
  Verwaltung, 67
GSNW, 88

HAL, 70
Hardwareabstraktionsschicht, 70
HDV, 14
Heimverzeichnis, 65
Hive, 73
Host-Namen, 39
HPGL, 22
HUB, 24

IDE, 8, 11
Initiator, 13
Installation, 44
  über Netzwerk, 48
  automatisiert, Software, 48
  Parameter, *44*, 47
  Unbeaufsichtigt, 47
  Voraussetzungen, 44
Internet Schicht / Layer, 27
IP-Adresse, *26*, 28, 33, 36, 38
IPX/SPX, 81, *88*
ISA, 6, 11
ISDN, 81
ISO/OSI
  Schicht
    1: Physikalische Schicht, 23
    2: Sicherungs- oder Verbindungsschicht, 24
    3: Netzwerkschicht, 26
    4: Transportschicht, 27
    5: Sitzungsschicht, 27
    6: Darstellungsschicht, 27
    7: Anwendungsschicht, 27
  Schichten oder Referenzmodell, *23*, 27

Karten, 8
Kennwort, 63
Kernelschicht, 70
Klassenlose Netze, 31
Kollisionsdomäne, 25
Kontendomäne, 76

Laser Scanning Unit (LSU), 19
LCP, 81
LDV, 14
Leasingtime, 36
Lizenzmodell, 46
Loopback Adresse, 30
LUN, 13

MAC-Adresse, *24*, 33, 108
Massenspeicher, 9
Mausanschluß, *3*, 4
MCA, 6
Memberserver, 44
Miniport, 81
Mirroring, 17
Mitgliedserver, 44
Modem, 65, *81*
Multicast, 31
Multilayer Applications, 80
Multiplexen, 34
Multitasking, 70

Namen
  Full Qualified Domain, 39
  Host, 39
  NetBIOS, 38

Namensauflösung, *38*, 40
Nameserver, 39
NDIS-WAN, 81
NetBIOS, *87*, 89
NetBIOS-Namen, 38
NetBUI, 81
Network Access Layer, 27
Network Layer, 26
Netzadresse, 30
Netzwerk, *74*, 87
  Drucker, 83
  Karte, *9*, 21
  Monitor, 95
Netzwerkschicht, 26
Nicht-Transitivität, 76
Northbridge, *5*, 11
Notationskonventionen, 55
NT-Backup, 90
NTFS, 46
NTVDM, 70, *71*
Null-Linie, 95
NWLink, 88

Parität, 17
Paritätsplatte, 17
Partition
  Boot, 49
  System, *49*, 50
Paßwort, 11
PCI, 7
PCL, 22
PDC, Primary Domain Controller, 44, 53, 55, 70, *74*
Photoreceptor Drum Assembly, 19
Physical Layer, 23
Physikalische Schicht, 23
Piezzo, 19
Plotter, 18
Portmapper, 35
Ports, *35*, 109
  Wichtige Nummern, 35
  Wohl definierte oder wellknown, 35
PostScript, 21
PPP, 81
Presentation Layer, 27
Printer
  Box, 21
  Dedizierter Server, 21
  Ports, 84
  Server, 20
Priorität
  Drucker, 85
  Echtzeit, 72
  Hoch, 72
  Niedrig, 72
  Normal, 72
  Programm, 70, *71*
  Stufen, 72
Protokoll Nummern, 34
Protokolle, 34
Prozessor, 5
PS/2
  Mausanschluß, 3
  RAM, 5
  Tastaturanschluß, 4

RAID, Redundant Array of Inexpensive Discs, *15*, 52
  Durch Betriebsysteme, *16*, 52
  Hardware, 15
  Level, 16
    0+1 oder 1+0 oder 10, 17
    6 und 7, 17
    0, *16*, 52
    1, *16*, 52
    2, 17
    3, 17
    4, 17
    5, *17*, 52
  Linear / Datenträgersatz, *16*, 52
  Regeneration, 52
  Software, *16*, 52
RAM, 5
  Double Data Rate (DDR), 6
  Dynamic, 5
  Extended Data Output (EDO), 5
  Fast Page Mode (FPM), 5
  PS/2, 5

Rambus, 6
Synchron Dynamic (SD), 6
RAS, Routing Access Service, 65, *81*
Authentifizierung, 81
Dienst, 81
Protokolle, 81
Rückrufmodus, 65
Verbindungen, 81
Rechte, 55
Redirector, 88
Registry, 68, *72*
exportieren, 73
Hive, 73
`HKEY_CLASSES_ROOT`, 73
`HKEY_CURRENT_USER`, 73
`HKEY_LOCAL_MACHINE`, *73*, 93
`HKEY_USERS`, 73
Schlüssel, 73
Variable, 73
Wert, 73
Remote-Verwaltung, 63
Repeater, 24
Resourcendomäne, 75
Richtlinie, 55
Überwachung, 92
Konto, 63
System, 68
Richtlinieneditor, 73
Router, 26, 29, *33*
Routingtabelle, 33

SAM, 74
Samba, 89
SASI, 13
Schicht
Anwendung, 70
Hardwareabstraktion, 70
Kernel, 70
Schnittstelle, *5*, 11
Karte, 9
Parallel, *4*, 20
Seriell, *4*, 20
USB, *4*, 20, 47
SCSI, 13
Controller, 8
Fast, 14
Fast Wide, 14
ID, 13
Initiator, 13
LUN, 13
Target, 13
Ultra, 14
Ultra Wide, 14
Ultra160, 15
Ultra160+, 15
Ultra2, 15
Ultra3, 15
Ultra320, 15
Wide, 14
Wide Ultra2, 15
SCSI-1, 13
SCSI-2, 14
SCSI-3, 14
Search Domains, 39
Servertools, 63
Servicepack, 47
Session Layer, 27
Setupmanager, 48
Sicherungsschicht, 24
SID, *53*, 56, 75
SIMM-Module, 5
Sitzungsschicht, 27
Slots, *6*, 8
SMB, *87*, 89
Socket, 36
Soundkarte, 4, *8*, 11
Ausgang, 4
Eingang, *4*, 8
Southbridge, *5*, 11
Speicher, 5
Speicherbereich, 71
SPI, 14
Spiegelung, 17
Standard-Benutzer, 62, *68*
Standrad-Gateway, 33
Startplatten, 49
Streamer, 9
Striping, 16

Stromkabel, 3
Subneting, *32*, 105
Subnetmask, *26*, 28
Superneting, 32
Switches, 25, *33*
Systemmonitor, 94
Systempartition, *49*, 50
Systemrichtlinieneditor, 68
Systemvariable, 65
Systemvoraussetzungen, 44

Target, 13
Taskmanager, 93
Tastaturanschluß, 4
TCP/IP, *27*, 34, 46, 81, 87–89
Telefonbucheintrag, 82
Toner Hopper, 19
Transitivität, 76
Transportschicht / Layer
  DoD, 28
  ISO/OSI, 27
Treiber, 12
Trennseite, 86

UGLR-Concept, 56
USB, 47

Verbindung
  Novell NetWare, 88
  Unix / Linux, 89
Verbindungsschicht, 24
Vertrauensstellung, 75
  einseitig, 75
  gegenseitig, 76
Verzeichnisrecht, 61
Verzeichnisreplikation, 89
VLB, 7

Wechselplatte, 9
Windows 3.1(1), 84
Windows 3.1(1)-Programme, 71
WINS, Windows Internet Name Service, 39
Workgroup, 44

Zeitscheibe, *70*, 71
Zugangsschicht, 27