

# Net<sup>at</sup>Work

## Frank Carius

***Netzwerke - Kommunikation - Beratung***

**Tel 07272 92013-0**

**Fax 07272 92013-6**

**MHS** FCARIUS@FC unter 07272 92013-5

**X400** c=us; a=compuServe; p=csmail;  
d=ID:"MHS:FCARIUS(a)FC"

**Internet** fcarius@fc.mhs.compuServe.com



## Dokumentation

## Netzwerk

- Konzepte
- Beschreibung
- Konfiguration
- Installation
- Grundlagen
- Hintergründe

<b>1 Einleitung.....</b>	<b>13</b>
1.1 Wie finde ich mich zurecht .....	13
1.2 Vorwort.....	13
1.3 Zielgruppe .....	13
1.4 Was ist ein Netzwerk.....	13
1.5 Planung .....	14
1.6 Was merkt der User vom Lan .....	14
<b>2 Laufwerke, Verzeichnisse und Pfade.....</b>	<b>15</b>
2.1 Aufgliederung in Bereiche .....	15
2.2 Baum.....	16
2.3 Besondere Verzeichnisse.....	17
2.4 Laufwerke.....	19
2.4.1 Diskettenlaufwerk .....	19
2.4.2 Diskettenlaufwerk .....	19
2.4.3 Festplatte 0.....	19
2.4.4 Festplatte 1.....	19
2.4.5 CD-Rom lokal oder Netzwerk.....	19
2.4.6 Netzwerksystem [SERVERNAME\SYS:].....	19
2.4.7 Programmverzeichnisse [SERVERNAME\SYS:PROG].....	19
2.4.8 Benutzerdaten [SERVERNAME\SYS:USER\<login_name>].....	19
2.4.9 Gruppendaten [SERVERNAME\SYS:GROUP].....	20
2.4.10 Netzwerksystem [SERVERNAME\SYS:].....	20
2.5 Suchlaufwerke.....	21
<b>3 Benutzer.....</b>	<b>22</b>
3.1 normale User.....	22
3.2 Spezialuser.....	22
3.2.1 SUPERVISOR.....	22
3.2.2 ADMIN.....	22
3.2.3 OPERATOR .....	22
3.2.4 BACKUP .....	23
3.2.5 GUEST .....	23
3.2.6 MHS / MSMAIL.....	24
3.2.7 DUMMY .....	24
3.2.8 Fax .....	25
3.2.9 CHECKVIR.....	25
3.2.10 andere User.....	25

---

<b>4 Gruppen .....</b>	<b>26</b>
4.1 Group EVERYONE .....	26
4.2 Group GATEWAY .....	26
4.3 Anwendergruppen .....	26
4.4 Programmgruppen .....	26
<b>5 Login .....</b>	<b>27</b>
5.1 Booten.....	29
5.2 Remoteboot.....	29
5.3 DOSGEN und Bootimagedatei.....	29
5.3.1 CONFIG.SYS .....	30
5.3.2 AUTOEXEC.BAT.....	30
5.3.3 D62XXXXX.BAT .....	30
5.3.4 NET.CFG.....	31
5.4 Systemloginscript NET\$LOG.DAT .....	32
5.5 USERCFG.BAT .....	33
5.6 USERSET.BAT .....	34
5.7 USER.BAT .....	35
5.8 PCCFG.BAT.....	36
5.9 PCSET.BAT .....	36
<b>6 Programme .....</b>	<b>37</b>
6.1 Generell.....	37
6.2 Start mit Batch, Sonderbatches (nolimit, norights) .....	38
6.3 Rechtevergabe .....	39
6.4 Konfiguration speichern (Benutzer <-> Hardware) .....	39
<b>7 Windows im LAN.....</b>	<b>40</b>
7.1 Einrichten einer neuen Auflösung .....	40
7.2 Temporäre Daten und Auslagerungsdatei .....	41
7.3 Programmgruppen .....	41
7.4 GRPPATCH .....	41
7.5 Drucker.....	41
7.6 Nachrichten .....	41
7.7 WIN.COM.....	42
7.8 Windows Startbild .....	42
7.9 WIN.INI und Programme.....	42
7.10 REG.DAT und Programme.....	42

7.11 Userlevel .....	43
7.12 WIN31.BAT .....	43
7.13 INI-Patcher .....	43
7.14 Suchpfade .....	44
7.15 Neue Programme einbinden .....	45
7.16 Neue Gruppe einbinden .....	45
7.17 Private Gruppe .....	45
7.18 Screensaver einrichten.....	45
<b>8 Lizenzen.....</b>	<b>47</b>
<b>9 Backup .....</b>	<b>49</b>
9.1 Workstationbased Backup .....	49
9.2 Serverbased Backup .....	50
9.3 Backupmedien .....	50
9.4 Laufwerkswechsel.....	50
9.5 Komprimierung.....	50
9.6 Mitteilung an Benutzer.....	51
9.7 Lokale Festplatten der Workstations am Netzwerk.....	51
9.8 Backupabfolge .....	51
9.9 USER.BAT des Users BACKUP .....	52
<b>10 Drucken.....</b>	<b>53</b>
10.1 Die Problematik.....	53
10.2 Der Druckertreiber.....	54
10.3 Die Schnittstelle LPT1-3.....	54
10.4 Die Queue .....	54
10.5 Der Job.....	54
10.6 Von der Queue zum Drucker.....	55
10.7 PCONSOLE .....	56
10.8 Drucker wechseln.....	56
10.9 Gedanken zur Druckerkontrolle.....	57
10.9.1 Small: .....	58
10.9.2 Medium:.....	58
10.9.3 Big: .....	59
10.10 Windowsdrucker.....	60
10.11 PRINTSEL.....	60
10.12 PRINTSET .....	61

---

10.13 Fehlersuche Drucker .....	62
<b>11 Workstation .....</b>	<b>63</b>
<hr/>	
11.1 Hardware (HD, CPU, Grafik, NW-Karte) .....	63
11.2 Betriebssystem MS-DOS .....	64
11.3 RemoteBoot .....	64
11.4 Fehlersuche RemoteBoot.....	64
11.4.1 Funktioniert die LAN-Karte im Server ?.....	65
11.4.2 Kommen Anfragen der Station beim Server an ? .....	65
11.4.3 Erlaubt der Server RemoteBoot ? .....	65
11.4.4 Bootimage/BOOTCONF-SYS .....	65
11.4.5 Workstation .....	65
11.4.6 Ethernetframe.....	66
11.4.7 Sonderfall ODI.....	66
11.4.8 Sonderfall EMM386.....	66
11.5 Workstationshell.....	66
11.6 Netzwerktreiber .....	68
11.6.1 Die Netzwerkhardware .....	68
11.6.2 Hardwaretreiber.....	68
11.6.3 Konverter .....	69
11.7 Konfigurationsdateien .....	69
11.7.1 CONFIG.SYS .....	70
11.7.2 AUTOEXEC.BAT.....	70
11.7.3 NET.CFG bzw SHELL.CFG .....	70
11.8 Umgebungsvariablen .....	71
11.9 remote Login für Außendienst.....	73
11.9.1 Sicherheit.....	73
11.9.2 MAIL-Verbindung.....	73
11.9.3 Fernbedienung .....	74
11.9.4 Telefonleitung als LAN .....	74
11.10 Notebooks .....	76
11.10.1 Notebookserver .....	76
11.10.2 Dockingunit.....	76
<b>12 Fileserver (NetWare 3.x) .....</b>	<b>77</b>
<hr/>	
12.1 Volumeaufteilung .....	77
12.2 Cachekontroller .....	79
12.3 Konsole schützen.....	79
12.4 BATCHES auf dem Server.....	80
12.5 STARTUP.NCF .....	80

12.6 AUTOEXEC.NCF .....	81
12.7 Hardware (LAN, I/O, Memory).....	81
12.8 NetWare 3.x Speicheraufteilung .....	82
12.8.1 Total Server Work Memory: .....	82
12.8.2 Original Cache Buffers: .....	82
12.8.3 Permanent Memory Pool:.....	82
12.8.4 Packet Receive Buffers:.....	82
12.8.5 Directory Cache Buffers: .....	82
12.8.6 Alloc Memory Pool:.....	83
12.8.7 Cache Buffers:.....	83
12.8.8 Cache Movable Memory:.....	83
12.8.9 Cache Non-Movable Memory:.....	83
12.9 NLM's .....	83
12.10 PATCHMAN.NLM.....	83
12.11 VREPAIR .....	84
12.12 UPS .....	84
12.13 Bindery .....	85
12.14 Konsole .....	85
12.15 LogBuch und Errordateien .....	85
12.16 Patches für den Server.....	86
<b>13 LANphysik.....</b>	<b>87</b>
13.1 Kabel, Zugriff, Struktur (AUI, BNC, TP, LWL) .....	87
13.2 Ethernet frames.....	88
13.2.1 Einsatzbereiche der Frames .....	89
13.2.2 DOS-Client. Support der Frames .....	89
13.2.3 Die wichtigsten Protocol-ID's im Überblick.....	89
13.2.4 Ethernet_802.2 SAP-Kennungen LLC.....	90
13.2.5 Ethernet_II Packettypen .....	90
13.2.6 Herstellerkennung von Ethernetkomponenten .....	91
13.2.7 Beispiele .....	93
13.3 Protokolle (IPX, IP, NetBios, NetBeui, XNS, OSI, AppleTalk...) .....	95
13.4 IP .....	95
13.5 Verbindung (Router, Bridge, Server als..) .....	96
13.5.1 Repeater.....	96
13.5.2 Bridge .....	97
13.5.3 Router.....	97
13.5.4 Gateways.....	98
13.6 Lasttrennung im LAN.....	98

---

<b>14 WAN.....</b>	<b>100</b>
14.1 Paketvermittlung.....	100
14.2 Festverbindung.....	100
14.3 Wählverbindung .....	100
14.4 Kostenanalyse.....	101
14.5 Netware im WAN.....	101
<b>15 Connectivity.....</b>	<b>103</b>
15.1 Gateways .....	103
15.2 ISDN, CAPI .....	105
15.3 BTX .....	105
15.4 CD-ROM.....	106
15.5 FAX .....	107
15.6 Modem .....	108
15.7 EMail .....	109
15.8 Datex-P .....	110
15.9 Hostanbindung UNIX.....	111
15.10 Hostanbindung BS2000 .....	112
<b>16 MHS .....</b>	<b>114</b>
16.1 Warum EMail.....	114
16.2 Was ist ein MTA und was tut er .....	114
16.3 Remote Mail .....	115
16.4 Die zwei Seiten des MTA .....	115
16.5 Mailschnittstellen .....	115
16.5.1 Simple MAPI.....	115
16.5.2 CMC .....	116
16.5.3 VIM .....	116
16.5.4 SMF .....	116
16.6 Was ist eine "Mail" .....	116
16.7 Netware MHS.....	116
16.7.1 Geschichte von MHS.....	116
16.7.2 Das FORMAT einer Mail (SMF-70).....	117
16.7.3 Adressierung von MHS .....	117
16.7.4 Die MHS-Verzeichnisse.....	118
16.7.5 Die User von MHS.....	119
16.7.6 Der Begriff "Gateway" bei E-Mail.....	119
16.8 Gedanken zum Routing.....	119

16.8.1 Die Sternstruktur/Baumstruktur.....	120
16.8.2 Der firmeninterne Ring.....	120
16.8.3 Die Masche.....	120
16.9 Third Party.....	121
16.9.1 Mailprogramme.....	121
16.9.2 Connect <sup>2</sup> .....	121
16.10 Gateways, Beispiele der Anwendung.....	122
16.10.1 Zu den Programmdetails.....	122
16.10.2 MHS als Mailbox.....	122
16.10.3 MHS als Fehlermelder.....	123
16.10.4 MHS als Statistiker.....	123
16.10.5 MHS überprüft echte Gateways:.....	123
16.10.6 MHS als Zugang zur Fernwartung.....	123
16.10.7 MHS zu X400, Internet, MCI-Mail, MSMail, WordPerfect.....	123
16.10.8 MHS und FAX.....	124
16.10.9 MHS und Signalisierung.....	124
16.10.10 MHS sagt Hallo.....	124
16.10.11 MHS als Batchstarter.....	124
16.10.12 MHS und Datensicherheit.....	124
16.10.13 MHS als Saubermann.....	124
16.10.14 MHS als Lizenzkontrolle.....	125
16.10.15 MHS und Datenbanken.....	125
16.10.16 MHS als ???.....	125
<b>17 Regeln.....</b>	<b>126</b>
17.1 Grundregeln für Benutzer.....	126
17.2 Regeln für den Supervisor.....	127
<b>18 Betriebspersonal.....</b>	<b>128</b>
18.1 Supervisor und Admin.....	128
18.2 Operator.....	128
<b>19 Support.....</b>	<b>129</b>
19.1 NETWIRE.....	129
19.2 CNE.....	129
19.3 CAP.....	129
19.4 NAR, NAEC.....	130
<b>20 Schulung.....</b>	<b>131</b>
20.1 Anwenderschulung.....	131
20.2 Operatorschulung.....	131



---

20.3 Administratorschulung.....	131
20.4 Workshops .....	132
<b>21 Troubleshooting.....</b>	<b>133</b>
<hr/>	
21.1 Cables Scanner .....	133
21.2 Protokollanalyser.....	133
21.3 Langzeitmessung .....	133
21.4 Alarmgeber (MHS-Gate) .....	133
<b>22 Installation von .....</b>	<b>134</b>
<hr/>	
22.1 Server (Diskette mit Installationsdateien) .....	134
22.2 Workstation .....	135
22.3 Programminstallation.....	136
22.4 Drucker einrichten .....	137
22.5 User anlegen .....	139
22.6 User löschen .....	139
<b>23 Checkliste bei Übergabe .....</b>	<b>140</b>
<b>24 Nachwort.....</b>	<b>141</b>
<b>25 Anlage 1: Software.....</b>	<b>142</b>
<hr/>	
25.1 BS2000-Emulation .....	144
25.2 WinWord 6.0 .....	145
25.3 Excel 5.0 .....	146
25.4 PowerPoint 4.....	147
<b>26 Anlage 2: Formblätter .....</b>	<b>148</b>
<hr/>	
26.1 Server-Konfiguration .....	149
26.2 Drucker-Konfiguration .....	151
26.3 PC-Konfiguration.....	152
26.4 Bootfilekonfiguration:.....	153
26.5 Bedeutung der Umgebungsvariable VIDEO.....	154
26.6 PASSWÖRTER für Fileserver.....	155
26.7 Bestätigung der Passwordübergabe .....	156
<b>27 Anlage 3: Konfigurationsdateien .....</b>	<b>158</b>
<hr/>	

**Abbildungen:**

Abbildung 1 Verzeichnisse auf dem SYS-Volume	16
Abbildung 2 Programmbereich	16
Abbildung 3 Datenbereich der Benutzer	17
Abbildung 4 Grupperverzeichnis	17
Abbildung 5 Benutzerverzeichnis	20
Abbildung 6 "WHOAMI" Operator	23
Abbildung 7 "WHOAMI" Guest	24
Abbildung 8 "WHOAMI" Dummy	25
Abbildung 9 Vom Booten zum Login	28
Abbildung 10 "SEND"-Message	42
Abbildung 11 Regedit	43
Abbildung 12 Stationen eines Ausdrucks	54
Abbildung 13 Printjob	55
Abbildung 14 Druckmodell "SMALL"	58
Abbildung 15 Druckmodell "MEDIUM"	58
Abbildung 16 Druckmodell "BIG"	59
Abbildung 17 Windows Druckereinrichtung	59
Abbildung 18 PrintSelect	60
Abbildung 19 Fehlersuche Drucken	62
Abbildung 20 Netzwerkshell	67
Abbildung 21 ODI/NDIS/PACKET - Umsetzung	68
Abbildung 22 Spawning	78
Abbildung 23 Mirroring	79
Abbildung 24 Duplexing	79
Abbildung 25 NetWare 3.x Speicherbereiche	82
Abbildung 26 Ethernetpaket	88
Abbildung 27 OSI Repeater	96
Abbildung 28 OSI 2 Bridge	97
Abbildung 29 OSI 3 Router	97
Abbildung 30 OSI 7 Gateway	98
Abbildung 31 Ein Segment	98
Abbildung 32 Segmentierung	99
Abbildung 33 Point2Point Gateway	104
Abbildung 34 Store&Forward Gateway	104
Abbildung 35 BS2000 Anschlußmöglichkeiten	112
Abbildung 36 MHS-Verzeichnisstruktur	119
Abbildung 37 MHS Beispielmail	117

**Konfigurationsbeispiele**

<i>Konfigurationsdatei 1 BOOTCONF.SYS</i>	29
<i>Konfigurationsdatei 2 CONFIG.SYS</i>	30
<i>Konfigurationsdatei 3 Remoteboot AUTOEXEC.BAT</i>	30
<i>Konfigurationsdatei 4 D62XXXXX.BAT</i>	30
<i>Konfigurationsdatei 5 NET.CFG</i>	31
<i>Konfigurationsdatei 6 Systemloginscript</i>	32
<i>Konfigurationsdatei 7 USERCFG.BAT</i>	33
<i>Konfigurationsdatei 8 USERSET.BAT</i>	34
<i>Konfigurationsdatei 9 USER.BAT (default)</i>	35
<i>Konfigurationsdatei 10 USER.BAT (DUMMY)</i>	35
<i>Konfigurationsdatei 11 PCCFG.BAT</i>	36
<i>Konfigurationsdatei 12 PCSET.BAT</i>	36
<i>Konfigurationsdatei 13 WIN31.BAT</i>	44
<i>Konfigurationsdatei 14 PRINTSET.INI</i>	60
<i>Konfigurationsdatei 15 Printset.ini</i>	61
<i>Konfigurationsdatei 16 CONFIG.SYS</i>	70
<i>Konfigurationsdatei 17 Startbatchdateien</i>	70
<i>Konfigurationsdatei 18 NET.CFG</i>	71
<i>Konfigurationsdatei 19 STARTUP.NCF</i>	80
<i>Konfigurationsdatei 20 AUTOEXEC.NCF</i>	81

**Tabellen**

<i>Tabelle 1 Backupbänder</i>	52
<i>Tabelle 2 Fernwartungsprodukte</i>	75
<i>Tabelle 3 Ethernetpaketfelder</i>	88
<i>Tabelle 4 Frametypen</i>	89
<i>Tabelle 5 Treibersupport für Frames</i>	89
<i>Tabelle 6 Typfelder je Protokoll</i>	89
<i>Tabelle 7 SAP-Kennungen</i>	90
<i>Tabelle 8 Ethernet_II-IDs</i>	90
<i>Tabelle 9 Herstellerkennung Ethernet</i>	91
<i>Tabelle 10 TCP/IP-Stacks</i>	95

## **1 Einleitung**

Es gibt einige Personen, ohne die ich nie soweit gekommen wäre. Ohne diese nun persönlich zu nennen möchte ich nur schreiben, daß all diese Personen sehr viel Vertrauen in mich und meine Arbeit gesetzt haben, und mir die notwendigen Freiheiten eingeräumt hatten.

### **1.1 Wie finde ich mich zurecht**

Diese Dokumentation ist in mehrere Teile gegliedert. Diese Untergliederung soll das schnelle Auffinden bestimmter Themen erleichtern. Zudem ist bei einer Dokumentation eines Netzwerkes nie von einem statischen Zustand zu sprechen. Damit im Falle einer Änderung nicht immer die komplette Dokumentation neu überarbeitet werden muß, wurde variable Teile vom reinen Konzept abgetrennt.

Nach dem obligatorische Deckblatt und Inhaltsverzeichnis beschreibt der Hauptteil das Konzept der Installation. Die erste Anlage beschreibt die installierte Anwendersoftware, die zweite Anlage die eingesetzte Hardware.

### **1.2 Vorwort**

Es hat lange gedauert, bis ich all das Wissen und die Erfahrung gesammelt habe, um diese Dokumentation abzufassen. Dazu braucht man nicht nur ein Netzwerk, bestehend aus einem Server und einigen Clients, es muß auch groß genug sein, um viele Konstellationen zu haben, für welche adäquate Lösungen gefunden werden müssen. Wenn dann noch möglichst viele Benutzer mit eigenen Anforderungen im Netzwerk arbeiten, dann muß man sich klare Konzepte und Strategien ausdenken. Diese Konzepte haben sich im Laufe der letzten Jahre entwickelt und sind leider nie statisch. Mit jeder neuen Entwicklungsstufe einiger Komponenten muß nachgebessert werden. So fällt es schwer, einen Zeitpunkt festzulegen, um das aktuelle Konzept auf Papier zu bringen. Doch seit einiger Zeit scheint das Grundgerüst fest zu sein, so daß es sich lohnt, dies mehreren Personen zugänglich zu machen. Ab einer bestimmten Komplexität eines Netzwerkes ist es unmöglich, allein die Arbeit zu machen. Es kommt der Zeitpunkt, weitere Personen einzuweihen. Dabei hilft ein geschriebenes Wort. So wurde ich gezwungen die Konzepte in meinem Kopf zu formulieren und niederzuschreiben.

Die Sicherheit in einem Netzwerk ist ein Hauptbestandteil. Daher werden sie das Kapitel "Sicherheit" vergeblich suchen. Statt in einem Kapitel einen Kurzauszug des Konzeptes mit dem Aspekt "Sicherheit" zu schreiben, werden Sie die relevanten Aussagen zur Sicherheit der einzelnen Abschnitte im Text finden. Die Sicherheit zieht sich wie ein roter Faden durch die Dokumentation und ist immer mit "drin".

Es steht jedem frei, Teile dieses Konzeptes zu verwirklichen. Ich hoffe man verzeiht mir hin und wieder ungeschliffene Ausdrucksweisen, aber als Administrator ist man nicht unbedingt zum Schriftsteller geboren. Auch ist es nicht immer möglich, ein gleichbleibendes Niveau zu halten. Manche Passagen werden den einen langweilen aber für andere das Verständnis und den Zugang erleichtern.

NetWare kennt den user SUPERVISOR. In dieser Dokumentation werden oft die Ausdrücke ADMIN, Administrator, SYSOP oder SV benutzt. Diese sind in der Funktion und Bedeutung dem Supervisor gleichwertig.

### **1.3 Zielgruppe**

Die Zielgruppe dieser Dokumentation sind Netzwerkadministratoren, welche zwar den Umgang mit Netzwerkutilities kennen, jedoch ständig nach Verbesserungen ihrer Konzeption suchen. Ich setze voraus, daß die Leser Kenntnisse des Netzwerkbetriebssystems haben und mit den Utilities umgehen können. Auf Programme und Handbücher des Netzwerkbetriebssystems wird nicht gesondert eingegangen. Wer also ein Netzwerk pflegt, darf hier keinen Ersatz für die Handbücher sehen.

### **1.4 Was ist ein Netzwerk**

Ein Netzwerk besteht aus mehreren Komponenten, von denen der Benutzer aber die wenigsten zu Gesicht bekommt, geschweige denn darüber Bescheid wissen muß.

Es gibt das physikalische Netzwerk, welches aus den Kabeln, Verbindungsstücken, Verstärkern und weiteren Komponenten besteht. Dieses sorgt dafür, daß eine Information von einem Rechner zu einem anderen Rechner kommen kann.

Das Netzwerkbetriebssystem macht sich diese Verbindungen zu Nutzen und liefert die Hilfsmittel, um damit zu arbeiten.

## 1.5 Planung

Eine gute Planung ist die halbe Miete. Ein dämlicher Spruch, denn was ist eine gute Planung ? Es gibt aber einige Punkte, die man im Vorfeld beachten sollte:

Kabel: Fehlerfrei (gemessen !!) und leicht erweiterbar (also freie Kontakte, Kabelreserven)

Server: genug Spielraum zu den Grenzen (Useranzahl, Plattenplatz, Connections)

Ziele: - zufriedene User  
- Funktionstüchtig  
- Verbesserung der Leistung gegenüber Standlone-PC's

Damit sind auch schon einige Punkte genannt, welche nicht immer leicht zu realisieren sind. Leider kann man sich sein Netzwerk nicht immer so aufbauen, wie man sich das wünscht. Es sind oft Kompromisse nötig, z.B: wenn Hardware nicht sofort verfügbar ist, oder der Vorgesetzte andere Prioritäten setzt.

- Mache keine halbe Sachen. Das Netzwerk ist nur dann effektiv, wenn der volle Ausbau schnellstens (Speicher, Drucker, User (Email) möglich ist. Teilrealisationen bringen nur den Supervisor in Streß und fördern nicht die Akzeptanz des Netzwerks.
- Alle geplante Software muß vorher installiert werden, sonst sind User gezwungen, teils vom Netzwerk und teils von eigener Platte zu starten.
- Schneller Anschluß fast aller PC's. Geht das nicht, so sollten zumindestens lokale Gruppen nach und nach komplett angeschlossen werden, damit Workgroups möglich sind (Mail, Drucker, Datenaustausch, Hilfe untereinander). Nicht zuerst die Chefs anhängen (Statusgedanken), da sich sonst die Wirkung des "workgroup computing" nicht entwickelt
- Alle Drucker installieren und konfigurieren. (zumindest in den dann angeschlossenen Workgroups bei Teilausbau)
- E-Mail für alle einrichten, auch wenn sie noch nicht angeschlossen sind.(-> genug Lizenzen)
- Durch den Einsatz eines Netzwerkes kann man Kosten sparen, z.B. weniger Drucker, zentrale Updates, Datensicherheit, Wegfall weiterer Peripherie (DruckMultiplexer), geringe Pflege und besonders Betriebssicherheit. Mache das den Kostenstellenleitern klar.
- UND: Erzähle nichts vom Paradies. Was du heute versprichtst muß du morgen anbieten. Und das ist nicht immer leicht oder so presiwert, wie es erscheinen mag.

## 1.6 Was merkt der User vom Lan

Im Gegensatz zum Administrator ist es für den Benutzer nicht nötig, mehr über das Netzwerk zu wissen, als unbedingt nötig. Die Aufgabe eines Benutzers ist es nicht, lange zu lernen, womit er es zu tun hat sondern seine eigentliche Arbeit mit dem Computer schneller und effektiver zu erledigen. Es sind drei wichtige Dinge, welche er wissen muß.

1. Er muß sich anmelden, damit das Netzwerk weiß, wer an welchem Computer sitzt und welche Rechte dieser Benutzer hat.
2. Es gibt weitere Verzeichnisse, in welche Daten abgelegt werden können. Es können damit auch einige Programme dazu kommen.
3. Der Benutzer ist nicht darauf angewiesen, daß ein Drucker an seinem Rechner angeschlossen ist.

## 2 Laufwerke, Verzeichnisse und Pfade



Dieses Kapitel beschreibt die Baumstruktur auf den Fileserverplatten. Der normale Benutzer "sieht" nur einen Teil davon.

### 2.1 Aufgliederung in Bereiche

Leider kann man nicht DEN besten Verzeichnisbaum aufzeigen. Jeder Administrator hat seine Vorlieben und seine Lösungen. Es gibt wirklich nicht die allgemeingültige beste Lösung. Jedoch gibt es einige Gemeinsamkeiten, welche man in fast jedem Verzeichnisbaum finden wird. Der Baum ist auch davon abhängig, wieviel Festplatten und Volumes man angelegt hat.

Trennen wir die Bereiche in vier Hauptteile auf.

#### System

Dieser Bereich beinhaltet alle Systemdaten, welche NetWare vorgibt, d.h. die Verzeichnisse SYSTEM, MAIL, PUBLIC, LOGIN, ETC. Diese liegen immer zwingend auf dem SYS-Volume. Auf diesen Bereich wird LESEND und SCHREIBEND (Printqueues) zugegriffen

#### Programme

Ein Teil des Verzeichnisbaumes wird die Programme enthalten. Dabei kann man unter diesem Verzeichnis dann je Appikation ein Verzeichnis machen oder die Appikationen selbst noch aufgliedern in weitere Unterverzeichnisse (z.B. Textverarbeitung, Bank, Verwaltung, Buchhaltung). Auf diesen Bereich wird weitgehend LESEND zugegriffen, so daß bei ausreichendem Speicher im Server für Filecaching die Festplatte nicht stark belastet wird.

#### Benutzerdaten

Dies ist der Bereich, wo sich die einzelnen Benutzerverzeichnisse befinden, in welche die einzelnen Benutzer ihre Daten ablegen. Manche trennen die Konfiguration nochmals von den Daten ab und legen dafür einen weiteren Bereich an. Dies wird aber speziell bei vielen Benutzern schnell umfangreich, da je User immer zwei Verzeichnisse angelegt werden müssen. Alternativ dazu bietet es sich an, ein Unterverzeichnis bei den Userdaten je User anzulegen, in welchem Konfigurationen abgelegt werden. Dieser Bereich wird sowohl GELESEN als auch BESCHRIEBEN. Der Umfang dieser Operationen hängt stark von der Anzahl der Benutzer und der Art der Daten ab. (Bilder, Texte)

#### Gruppendaten

Dieser Bereich eignet sich für Arbeitsgruppen und als Datenaustauschplatz. Hierfür ist es nicht möglich, einen Verzeichnisbaum vorzugeben, da jede Firma und Abteilung eigene Wünsche und Gedanken hat. Dies betrifft den ADMIN dabei nicht, da er nur die Verzeichnisse einrichtet und die Rechte vergibt, dabei aber auf jeden Fall Kontrollfunktion und ein Mitspracherecht hat. Dieser Bereich wird wie der Userbereich GELESEN und BESCHRIEBEN. jedoch nicht unbedingt stark belastet. Es sei denn, daß dieser Bereich auch für gemeinsame Datenbankfiles genutzt wird.

Ausgehend von diesen vier Bereichen, kann man nun auswählen, wie man diese anordnet. Bei nur einer Festplatte fällt die Entscheidung leicht: "Alles auf einem Volume". Man kann sie aber auch gezielt auf Festplatten verteilen, um eine Lastverteilung zu erreichen. So werden Programme im Regelfall immer nur gelesen. Da Leseoperationen auf einem Server meist über den Cache reduziert werden, ist dieser Bereich sehr wenig belastet. Es bietet sich an, zu diesem Bereich einen aktiven Bereich (Druckqueues des Systembereichs oder Datenbereiche) zu koppeln und auf einer Festplatte abzulegen.

## 2.2 Baum

Der Einfachheit halber wird jeweils nur ein Auszug des Baumes angegeben und kein Gesamtabbild eines Verzeichnisbaumes abgedruckt. Der Gesamtüberblick würde mehr verwirren, da es sich sowieso empfiehlt, den Baum logisch und eventuell auch physikalisch aufzugliedern.

"Alles auf einem Volume"



Abbildung 1 Verzeichnisse auf dem SYS-Volumen

Befinden sich mehrere Festplatten im Server, welche einzelne Volumes sind, so können einzelne der vier Bereiche ausgelagert werden. Hier sind der Phantasie fast keine Grenzen gesetzt. Jedoch muß bei der Aufteilung einer Festplatte in mehrere Volumes die Zugriffsgeschwindigkeit gleich bleibt. Geschwindigkeit bringt eine Austeilung nur bei mehreren Festplatten. Dabei muß man aufpassen, daß ein später nicht ausreichender Platz in einem Bereich nicht durch Abzug aus einem anderen Bereich einfach ausgeglichen werden kann. Dies passiert nicht, wenn alles auf einem Volume liegt. Wer will, kann sich ein großes Volume über mehrere Festplatten "spannen". Damit wird die Lastverteilung optimiert, da alle Festplatten als logisch eine Festplatte laufen, mit mehreren Köpfen und Schrittmotoren. Jedoch muß man sich bewußt sein, daß man nicht einfach eine Festplatte im Fehlerfall austauschen kann, da man nie weiß, wo welche Daten liegen. Hier ist immer ein Komplettrestore nötig. Wenn man zwei Festplatten hat und Userdaten auf HD1 und Programme auf HD2 hält, kann man beim Ausfall von HD1 sich mit einem Teilrestore der Userdaten begnügen.

**Bereich: Programme (PROG)**

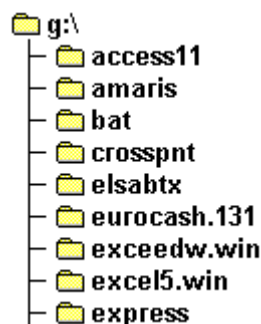


Abbildung 2 Programmbereich

Dieser Bereich enthält alle Programme, welche auf dem Netzwerk eingesetzt werden. Diese Programme sollten in jeweils eigenen Unterverzeichnissen abgelegt werden. Die Programmoberfläche "Microsoft Windows" findet sich auch hier. Windowsanwendungen können unter dem Verzeichnis WINDOWS oder selbst im Programmverzeichnis liegen. Ich bevorzuge die Lösung, daß die Programme alle gleichgestellt ein Verzeichnis direkt im Root des Programmbereich haben. Windows selbst firmiert in einem eigenen Verzeichnis. Dies hat den Vorteil, daß bei einem Upgrade der Oberfläche nicht alle anderen Programme kopiert werden müssen, solange beider Versionen während der Übergangszeit eingesetzt werden. Es empfiehlt sich, jedes Verzeichnis mit der Versionsnummer zu koppeln. Anhand der Extension von Verzeichnissen kann man die Programme verschiedenen Oberflächen und Betriebssystemen zuordnen (DOS, WIN, OS2, MAC, GEM u.a.)



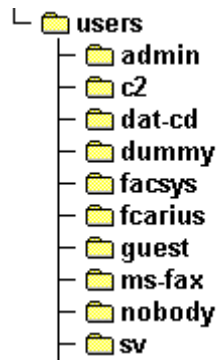
**Bereich: Userdaten (USER)**

Abbildung 3 Datenbereich der Benutzer

**Bereich: Gruppendaten (GROUP)**

Abbildung 4 Grupperverzeichnis

Welche Gruppenverzeichnisse angelegt werden, hängt sehr stark von der Struktur und den Bedürfnissen der Firma bzw. Abteilung ab. Es sollte aber ein "ALLE" Verzeichnis geben, in welchem jeder Lesen und Schreiben kann. Hier könnte sich auch eine Gruppe von Admins eine eigene Gruppe für Dokumentation und Service einrichten oder ein Verzeichnis mit Neuigkeiten und Infos für Benutzer, welche dort aber nur Lesen dürfen. Diese Verzeichnisse sollten mit DSPACE beschränkt werden.

Sofern die Programme es zulassen, können sich hier in gesonderten Verzeichnissen auch Daten zu Datenbanken (Personal, Lohn usw) befinden, auf die eine eigene Gruppe von Mitarbeitern zugreifen muß.

**2.3 Besondere Verzeichnisse**

Im Verzeichnisbaum gibt es einige Verzeichnisse, die einer genaueren Erklärung über Funktion und Hintergrund bedürfen.

**SYS:PUBLIC**

Dies ist das PUBLIC-Verzeichnis von Netware. Hier liegen alle Netwaretools für die User des Netzwerkes wie sie von Novell NetWare installiert werden. Hier liegen KEINE Batchjobs für Anwendungsprogramme Hier liegen KEINE sonstigen Programme. Damit kann man auch bei mehreren Servern mit verschiedener Softwareinstallation leicht die NetWareutilities upgraden ohne unnötigen Ballast mitzukopieren.

**SYS:USER**

Hierunter liegen die privaten Userverzeichnisse. Der Benutzer bekommt automatisch das Laufwerk H: (root) darauf gemappt. Auf USER hat NUR der Administrator alle Rechte. Alle anderen User haben nur Rechte in ihre eigene Verzeichnisse

**SYS:SYSTEM**

In diesem Verzeichnis liegen wichtige Dateien, welche nur dem Server und dem Administrator zur Verfügung stehen.. Die voreingestellten Rechte bleiben unverändert. Um den Suchpfad zu den Programmen zu sparen, werden sie aber auch mittels Batchjob aufgerufen.

**(PROG)\BAT**

Hier liegen SÄMTLICHE Anwenderbatches für Anwenderprogramme um eine saubere Trennung zwischen NetWaretools in Public zu haben und sonstige Batches. Auf dieses Verzeichnis hat EVERYONE [ROS]-Rechte Auf die weiteren Unterverzeichnisse unter PROG haben die spezifizierten Anwendergruppen besondere Rechte. Die Anwendungen werden (bis auf Windowsprogramme) alle

über Batch gestartet, welche in SYS:PROG\BAT liegen. Die jeweilige Gruppe hat dann gezielt ROS-Rechte auf die entsprechende Anwendung Batches dazu unter BAT.

Hier liegen auch einige Sonderbatches, welche im Netzwerk Hilfen und Ordnung bieten., z.B.  
NORIGHT.BAT  
APPLIMIT.BAT

### **(PROG)\UTIL**

Hier finden sich alle Utilities, welche nirgendwo zugeordnet werden können, aber in Batchjobs, und im Systemloginscript benötigt werden. Hier sollen keine komplette Utilities (PC-TOOLS oä) installiert werden. Dafür gibt es SYS:PROG\. Hier findet sich z.B. CLEARCRT, TIMEPAUS, PSTATCD, LIST, MSD.EXE usw. Eventuell können hier auf einfache Utilities wie TEL usw abgelegt werden. Auf dieses Verzeichnis gibt es einen Suchpfad.

### **H:\TEMP**

Diese Verzeichnis enthält temporäre Daten im jeweiligen Heimatverzeichnis der Benutzer. Darauf verweist die Umgebungsvariable TEMP und TMP. Damit temporäre Dateien sicher wieder gelöscht werden, kann man diese beim Login löschen. Das Verzeichnis sollte man mit FLAGDIR auf purgeable setzen. Damit werden gelöschte Dateien automatisch gePURGED.

### **H:\SYSTEM**

Dieses Verzeichnis ist zum Abspeichern der benutzerspezifischen Daten gedacht. Hierunter können weitere Unterverzeichnisse für verschiedene Applikationen existieren. Dieses Verzeichnis ist normalerweise mit dem Attribut "hidden" versehen, damit der Benutzer es nicht sieht und damit die Konfiguration verändert, löscht oder Daten darin abspeichert.

### **SYS:SYSTEM\<queue-ID>**

Im Verzeichnis SYSTEM sind in der Regel auch die Printqueues abgelegt. Da es normal sinnlos ist, Druckjobs wieder mit SALVAGE holen zu können, kann man diese Verzeichnisse mit FLAGDIR auf "purgeable" setzen. Damit bleiben darin keine Queuefiles sondern werden sofort gelöscht. Dies entlastet auch den Fileserver.

### **MAIL-Verzeichnisse**

Abhängig von jeweiligen E-MAIL-Produkt gibt es Verzeichnisse, in welchen sich die Mails befinden. Da darauf nie der Benutzer direkt mit COPY oder Editoren zugreift, sondern immer nur über das Mailprogramm (Frontend) kann man auch diese Verzeichnisse aus "purgeable" setzen. Damit vermeidet man, daß Mails wieder von anderen "zurückgeholt" werden. Zudem muß der Fileserver weniger "deleted files" mitführen.

## 2.4 Laufwerke

Unter MS-DOS und anderen Betriebssystemen wird auf Datenträger über Laufwerksbuchstaben zugegriffen. Dabei hat sich folgende Zuordnung als sehr hilfreich erwiesen. Man kann nicht davon ausgehen, daß man einem Benutzer einen weitläufigen Verzeichnisbaum zumuten kann, in welchem er dann herumwandert. Sehr viel einfacher wird der Zugriff über Laufwerksbuchstaben, welche nur die relevanten Teile repräsentieren.

### 2.4.1 Diskettenlaufwerk

Unter diesem Buchstaben kann man das erste Diskettenlaufwerk ansprechen, sofern es vorhanden ist. Dabei sollte es nur zum Einlesen und Abspeichern von Daten benutzt werden. Booten von Diskette ist möglich, jedoch ist dann der Zugriff aufs Netzwerk nicht sichergestellt (fehlende oder unpassende Treiber).

### 2.4.2 Diskettenlaufwerk

Sofern dieses vorhanden ist, eignet es sich auch zum Speichern und Einlesen von Daten. Wenn ein zweites Laufwerk eingebaut ist, sollte es ein unterschiedliches Format vom ersten Laufwerk haben.

### 2.4.3 Festplatte 0

Die meisten Netzwerkarbeitsplätze kann man ohne Festplatten betreiben. Dort, wo es sich nicht vermeiden läßt, bietet MS-DOS den Buchstaben C: an.

### 2.4.4 Festplatte 1

Eine zweite Festplatte oder Partition ist unter D: erreichbar. Bei allen Computern sollte darauf geachtet werden, daß nur zwei Buchstaben für lokale Festplatten belegt werden.

### 2.4.5 CD-Rom lokal oder Netzwerk

Der Buchstabe E: ist bei den meisten Computern frei verfügbar. Er eignet sich z.B. für CD-ROM-Laufwerke, welche lokal eingebaut sind oder über einen Redirector über das Netzwerk angesteuert werden können.

### 2.4.6 Netzwerksystem [SERVERNAME\SYS:]

Dieses Laufwerk ist das erste Netzwerklaufwerk. Es ist verfügbar, nachdem die Netzwerkshell erfolgreich geladen wurde. Es wird benötigt, um das LOGIN auszuführen. Bis dahin sieht man nur das Verzeichnis F:\LOGIN. Erst nach erfolgter Anmeldung findet sich hier der komplette Systembereich des Netzwerkes mit den benötigten Utilities. Wenn man nun gleichzeitig auch noch andere Netzwerke oder Utilities (z.B. SUBST)e insetzt, welche nur Laufwerke zwischen A: und LASTDRIVE (CONFIG.SYS) ansprechen können, empfiehlt es sich, den Eintrag LASTDRIVE = M in die CONFIG.SYS aufzunehmen. Das LOGIN-Verzeichnis ist dnn unter N: erreichbar. Damit sollten genug Laufwerke für diese Programme zur Verfügung stehen. LASTDRIVE=Z sollte nicht eingetragen werden, da die NetWareshell sonst kein LOGIN-Laufwerk anbietet. Ein Login ist trotzdem möglich, dann jedoch muß man die Software dazu dann lokal vorhalten. Das LOGIN-Verzeichnis dient auch dazu, daß Stationen ohne Festplatte (Remote boot) auf eine COMMAND.COM und andere Programme zugreifen können.

### 2.4.7 Programmverzeichnisse [SERVERNAME\SYS:PROG]

Hier liegen die Programme. Dieses Laufwerk ist ROOT auf ein separates Volume oder Unterverzeichnis PROG, welches auf den Programmbereich zeigt. In diesem Verzeichnis können die Benutzer nur lesen. Im Normalfall interessiert den Benutzer dieses Laufwerk genausowenig wie das F:-Laufwerk. Die Installation der Software soll dafür sorgen, daß die Programme korrekt geladen werden.

### 2.4.8 Benutzerdaten [SERVERNAME\SYS:USER\<login\_name>]

Dieses Laufwerk enthält nach Projekten geordneten Unterverzeichnissen und Daten der User, die komplett privat sind. Um Konflikte bei Programmen zu vermeiden, hat kein anderer User Rechte auf

die Verzeichnisse eines anderen Benutzers. Das H:-Laufwerk ersetzt komplett die lokale Festplatte, nur mit mehr Sicherheit in vielerlei Hinsicht.



Abbildung 5 Benutzerverzeichnis

In einem gesonderten Unterverzeichnis liegen temporäre Files und Konfigurationsdaten. Unter SYSTEM dürfen KEINE Daten oder Vorlagen liegen. Hier sind die Konfigurationen gespeichert, welche bei Notwendigkeit vom Administrator direkt oder batchgesteuert geändert werden können. Durch Unterverzeichnisse für Programme ist es für den SV leichter, diese Daten zu managen. Der User sollte darin NICHT seine Daten ablegen. Das TEMP-Unterverzeichnis ist für temporäre Dateien. Damit Programme das Verzeichnis benutzen ist die Umgebungsvariable TMP und TEMP auf dieses Verzeichnis gesetzt, in der Hoffnung, daß möglichst alle Anwendungen diese Variablen auswerten.

#### 2.4.9 Gruppendaten [SERVERNAME\SYS:GROUP]

Hier liegen in Unterverzeichnissen die Daten der Arbeitsgruppen. Je nach Gruppenzugehörigkeit haben spezielle User Rechte darauf. Mit NW311 sieht auch nur der User mit Rechten die Verzeichnisteile. Dieses Laufwerk ist ROOT auf ein extra Volume oder auf GROUP auf einem gemeinsam benutzen Volume. Jedoch müssen die Benutzer auf die Besonderheiten des Verzeichnisses ALLE besonders hingewiesen werden, da es sonst eine Lücke für Datenmißbrauch darstellt, wenn Dateien hier landen, welche nicht öffentlich sind. Im Hauptverzeichnis hat kein Benutzer Rechte. Damit ein Benutzer aber auch nicht ein Unterverzeichnis löscht, in welchem er Rechte hat, muß man die Unterverzeichnisse auf "DeleteInhibit" setzen.

##### Dazu eignet sich ein kurzes Anschreiben, bzw eine Infoseite:

Auf I:\ALLE (und darunter) haben ALLE Benutzer des Netzwerkes uneingeschränkt Zugriff (daher auch der Name ALLE) d.h. Daten, welche dort abgelegt werden, können von jedem ANGESEHEN, GELÖSCHT und VERÄNDERT werden, ohne daß der Admin eingreift kann. Sicherlich ist dies dem ein oder anderen User noch nicht so deutlich bewußt, da ich merke, daß von diesem Verzeichnis reger Gebrauch gemacht wird, um auch Daten auszutauschen. Dabei gibt es folgende Lösung:

A) Sie möchten eine Datei von ihnen an einen anderen User geben, d.h. im eine Kopie zuspiesen. Dazu bietet sich die elektronische Post an. Damit können sie Ihre Datei zu dem anderen User schicken, welcher dieser dann in der Regel nach 5-10 Minuten erhält. Dabei ist es unrelevant, ob der Benutzer am gleichen Standort oder in Berlin, Zürich oder London arbeitet.

B) Sie möchten Dateien SHAREN, d.h. es soll nur eine Version davon geben, die mehrere Benutzer nutzen, so daß die Veränderung durch einen Benutzer auch die anderen Benutzer sehen und keine Inkonsistenzen durch mehrere Kopien entstehen. Hier würde die E-Mail komplizierter sein, da man seine Änderungen an die anderen User schicken müsste. Dieser Fall entspricht aber der "Geschlossenen Benutzergruppe". Hierfür kann man ihnen ein besonderes Verzeichnis einrichten (I:\GBGname) in dem dann nur Mitglieder der Benutzergruppe Rechte haben. Solche Bereiche gibt es schon (z.B. SUPPORT für die Dokumentation des Netzwerkes für die Administratoren) nur sieht die Mehrzahl der Benutzer dieses (und andere) Bereiche nicht, solange sie nicht in deren Gruppe sind. Bitte prüfen Sie, inwieweit ihre Daten besser geschützt sind, wenn sie NICHT in I:\ALL liegen.

#### 2.4.10 Netzwerksystem [SERVERNAME\SYS:]

Für den Fall, daß man LASTDRIVE auf M gesetzt hat, loggt man sich über das Verzeichnis N: ein (N:\LOGIN). Ansonsten gelten die gleichen Bemerkungen wie zu F:.

**2.5 Suchlaufwerke**

Suchlaufwerke sind im Netzwerk der Ersatz für den Pfad bei Standalone-Computern. Da Verzeichnisnamen in Netzwerken sehr lange werden können und der eigentliche Suchpfad im Environment auf 127 Zeichen beschränkt ist, werden Laufwerksbuchstaben im Pfad aufgenommen, welche dann auf das Verzeichnis im Netzwerk verweisen. Diese Buchstaben beginnen bei Z: und kommen abwärts. Maximal sind 16 Suchlaufwerke möglich. Dabei muß man darauf achten, daß man nicht in Konflikt mit normalen Laufwerken und Netzwerklaufwerken kommt. Das Ziel sollte aber sein, möglichst wenig Suchlaufwerke zu belegen. Es gibt nötige Suchlaufwerke. Bewährt hat sich folgende Zuordnung:

Suchfolge	Laufwerk	physikalisch Lage und Beschreibung
S1	Z	G:\Dosversion (bei Remotebootrechnern für EMM386 u. COMMAND.COM)
S2	Y	SYS:PUBLIC
S3	X	G:BAT
S4	W	G:\UTIL
S5	V	G:\WIN31

Die Zuordnung kann abweichen, sollte aber über den Betrieb hinaus fest bleiben, d.h. Map INS darf sich nur auf NACHFOLGENDE Suchlaufwerke beziehen.

Die Reihenfolge des Suchlaufwerke soll so organisiert sein, daß möglichst wenig Anfragen an den Server gehen. Verzeichnisse, welche daher häufig durchsucht werden müssen (z.B. das Windows-Systemverzeichnis) sollten daher weiter vorne eingeordnet werden.

**Zerstörung des Pfades**

Die Zuordnung von Laufwerksbuchstaben zum Pfad hat den Vorteil, daß die Begrenzung des Pfades auf 127 Zeichen unter Dos umgangen wird. Allerdings ergibt sich dadurch eine Falltür. Im Suchpfad erscheint der Eintrag nur als „<Lw>:“. Wechselt man nun auf das Laufwerk und benutzt den Befehl „CD“, dann ändert sich das Verzeichnis von diesem Laufwerk und zudem auch der effektive Suchpfad. Daher sollten Verzeichnis, in welche ein Suchpfad hinweist, derart angelegt sein, daß es keine weiteren Unterverzeichnisse gibt. Zudem sollte der MAP-Befehl um den Parameter „ROOT“ ergänzt werden, so daß dieses Verzeichnis als Hauptverzeichnis erscheint. Dadurch wird es sehr schwer, mit CD den Suchpfad zu verändert. Allerdings ist dies auch kein kompletter Schutz. Mit „CD“ ist weiterhin eine Änderung möglich, allerdings nicht mit den gängigen Programmen zum Druchlaufen von Verzeichnissen (Xtree, Norton, Dosshell etc.)

Besondere Vorsicht ist bei Batchjobs geboten. Jeder Map INS muß auch korrekt gelöscht werden. Dazu gehört auch die Kontrolle, ob ein Map INS korrekt ausgeführt wurde (Speziell bei PRG-Gruppen mir Rechten). Norfalls muß vorher eine Abfrage ausgeführt werden, ob das spezielle Verzeichnis für den User mit seinen Rechten existiert (Abfrage mit IF EXIST auf eine Datei im Unterverzeichnis)

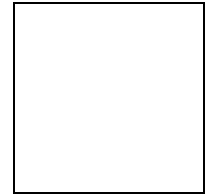
**Suchlaufwerke umgehen**

Um die Suchlaufwerke nicht als eigene Laufwerke auftauchen zu lassen, kann man alternativ den Suchpfad selbst modifizieren. Dies geht genauso im SystemLoginScript. Allerdings sollte man sich nicht über „unstimmige“ Anzeigen täuschen lassen. Der Befehl „MAP“ zeigt ein permanentes Laufwerk nicht mehr als solches an, wenn dieser Buchstabe auch im Suchpfad auftaucht. Die Funktion ist jedoch in keiner Weise eingeschränkt. Dazu muß man den Suchpfad PATH dann direkt modifizieren.

Diese Methode hat den Nachteil, daß man mit Standardbefehlen von DOS oder NetWare den Suchpfad nicht wieder gezielt verkleinern kann. Wurden bisher bei einem LOGOUT die Suchlaufwerke von NetWare direkt wieder entfernt, so bleiben die „normalen“ Suchpfad weiterhin bestehen, auch wenn kein Zugriff mehr auf diese Laufwerke möglich ist. Die äußert sich dann sich dann mit einer Fehlermeldung unter Dos.

Allerdings ist ein PC, welcher am LAN ist, und insbesondere ein PC ohne Festplatte, ohne LAN-Zugriff fast funktionsuntüchtig. Daher ist ein LOGOUT in der Regel dir Vorstufe zum Abschalten oder es folgt unmittelbar ein LOGIN. nach einem erneuten Login stimmen die Suchpfade wieder.

### 3 Benutzer



Bevor man Benutzer einrichtet, sollte man zuerst mit SYSCON die Userdefaults für die eigenen Bedürfnisse einstellen. Diese Werte werden für jeden Benutzer übernommen, der neu angelegt wird.

#### **3.1 normale User**

Als "normale" Benutzer bezeichne ich real vorhandene Personen, welche sich im Netzwerk anmelden und damit arbeiten. Diese User haben einen Usernamen und ein Paßwort, und haben alle nahezu gleiche Rechte, d.h. keiner davon ist z.Z. Supervisorequivalent, oder hat Rechte auf SYS:SYSTEM. Auch der Administrator ist hierunter mit seinem realen Namen vertreten. Diese Benutzer haben z.B: ein Postfach.

Der Benutzername im Netzwerk setzt sich aus dem ersten Buchstaben seines Vornamens und die ersten sieben Buchstaben seinem Nachnamen zusammen. Auf Titel, Doppelnamen wird nicht geachtet. Der Usernamen darf maximal acht Buchstaben lang sein und muß ein legaler Name für ein Verzeichnis haben, d.h. 'Sonderzeichen sind nicht erlaubt. ist der Nachname kürzer als sieben Buchstaben, so bleibt der Username auch kürzer. Ergibt sich der seltene Fall, daß zwei Personen den gleichen Usernamen hätten, so wird die letzte Stelle zu einer Ziffer.

Natürlich kann hier jeder Administrator sein eigenes System einsetzen. Jedoch sollte man zumindest für die Postfächer Namen vergeben, welche man aus dem Benutzernamen ableiten kann.

#### **3.2 Spezialuser**

Spezialuser sind alle Benutzereinträge von nicht natürlichen Personen. Diese Accounts werden von Dienstleistungen (MHS, BTX, ISDN, Drucker) benutzt oder sind gesonderte User, welche besondere Aufgaben im Netzwerk wahrnehmen (ADMIN, OPERATOR, Supervisor). Diese User haben im Regelfall keinen EMailEintrag. Ausnahme hiervon ist der ADMIN, an welchen alle Mail geht, die Fehler und Pflegearbeiten im Netzwerk betreffen. Nicht immer müssen alle hier angegebenen Benutzer eingerichtet werden.

##### **3.2.1 SUPERVISOR**

Der Supervisor wird von NetWare automatisch angelegt. Der User macht in der Hinsicht "Probleme, da sein Username länger als 8 Zeichen ist, und somit die Zuweisung seines Home-Verzeichnisses explizit im SystemLoginScript geschehen muß. Es bietet sich immer an, einen supervisorequivalenten User zu haben. Das Passwort dieses Users sollte für Notfälle im Safe liegen. Für Pflegearbeiten sollte man den Equivalenten nutzen. Daher soll dieser User auch keinen Eintrag in der E-Mail haben.

##### **3.2.2 ADMIN**

Der User ADMIN ist Supervisorequivalent, d.h. er kann genau das tun, was der Supervisor auch tun kann. Leider kann er auch das Passwort des Supervisors ändern. Dieser Benutzer sollte auch eine E-Mailadresse haben. Unter dieser Kennung kann die Pflege des Netzwerkes erfolgen. So hat man dann immer die "Hintertür" Supervisor, falls das Passwort vergessen wird, oder anderweitig gesperrt ist.

##### **3.2.3 OPERATOR**

NetWare kennt keine Ebene zwischen Supervisor und User. Oft ist bei großen Netzwerken jedoch ein OPERATOR brauchbar, welcher Aufgaben des Tagesgeschäfts erledigen kann, jedoch durch Limitierungen nicht allzuviel verstören kann. Besonders sollte er nicht das Passwort vom Supervisor ändern können. Zwischenzeitlich gibt es Workgroupmanager, welche diese Lücke auffüllen. So kann der User OPERATOR ein Workgroupmanager und ein PrintServerOperator sein. Wo man hier die Grenzen zieht, bleibt dem Administrator überlassen. Dieser Benutzer ist damit UNTER dem Admin und dem Supervisor angesiedelt.

Der Benutzer ist gedacht, um Aufgaben des ADMINS zu erledigen ohne gleich überall Schreibrechte (Virus, DEL \*.\* usw) zu haben. Er hat KEINE Rechte auf Benutzerverzeichnisse, KEINE Fileserverconsolerechte und kann KEINE User, Gruppen oder Drucker anlegen.

Er kann aber Pflegeaufgaben ausführen, z.B..

- Benutzer in Gruppen einfügen (Excelgruppe ua)
- "vergessene" Passwörter von Benutzern löschen (außer Supervisor und ADMIN)

WHOAMI /A erstellt z.B. folgenden Report:

```
You are user OPERATOR attached to server FC, connection 85.
Server FC1 is running NetWare v3.x (250 user).
You are Object Supervisor over <.ausgewählte Gruppen und User >
Login time: Wednesday May 5, 1993 4:05 pm
You are security equivalent to the following:
    EVERYONE (Group)
<andere ausgewählte Gruppen>
[      ] SYS:
[ R    F ] SYS:LOGIN
[ R    F ] SYS:PUBLIC
[ RWC   ] SYS:MAIL
[ [SRWCEMFA] SYS:MAIL/<Maildirectories der betreutenUser>
[ R    F ] SYS:PROG/BAT
[ R    F ] SYS:PROG/EXCEL4.WIN
[ R    F ] SYS:PROG/MSAPPS.WIN
[ R    F ] SYS:PROG/UTIL
[ R    F ] SYS:PROG/WIN31
[ R    F ] SYS:PROG/MSDOSV5.00
[      ] VLL:
[ RWCEMFA] VLL:GROUP/EVERYONE
[ RWCEMF ] VLL:GROUP/SUPPORT
[ R    F ] VLL:GROUP/SUPPORT/BOOTDISK
[ R    F ] VLL:GROUP/SEMINAR
[ R    F ] VLL:GROUP/VORLAGEN
[ RWCEMFA] VLL:USER/OPERATOR
Server FC1 is not in a Domain.
```

### Abbildung 6 "WHOAMI" Operator

## 3.2.4 BACKUP

Dieser User wird benutzt, um eine Datensicherung zu machen. Er ist beschränkt auf die Station, an welche das Backupgerät angeschlossen ist. Weiterhin ist die Einloggzeit auf die Zeit des Backup beschränkt. Damit dieser User den kompletten Fileserver sichern kann, braucht er Supervisorrechte. Daher muß alles unternommen werden, daß niemand anderes diesen Usernamen benutzen kann. So sollte beim Einloggen dieses Users automatisch das Backup gestartet werden und nicht unterbrochen werden können. Am Ende sollte das LOGOUT automatisch erfolgen. So könnte das Backup auch nachts automatisch laufen. Dazu muß sich der Benutzer BACKUP aber automatisch einloggen. Damit keine Fremdperson diesen Account ausnutzt, sollte der user BACKUP genau auf die Kartenummer limitiert sein, die im PC mit dem Backupdevice angeschlossen ist. Zudem sollte ein abgeschlossener Raum Fremdpersonen abhalten.

## 3.2.5 GUEST

Der User Guest wird wie der Supervisor und die Gruppe Everyone von NetWare angelegt.. Dieser User sollte NICHT von normalen Usern benutzt werden. Da jedoch viele User die Existenz dieses Benutzers kennen oder vermuten, bietet sich der User dazu an, Informationen für Außenstehende anzubieten Daher sollte derADMIN die Rechte dieses Users auf ein Minimum beschränken, da er nur von Personen benutzt werden sollte, die KEINEN eigenen Usernamen haben. So können Infos über den ADMIN, die Abteilung oder die Firma usw vergeben werden. Dies ist besonders dann interessant, wenn im Zuge der Verbindung mehrerer Netzwerke mittels WAN's neue unbekannte Server hinzukommen.. Aus eigener Erfahrung habe ich miterlebt, wie allein durch eine Verbindung zweier StandortLAN's durch eine 64kBit-Standleitung mehrere mir noch unbekannte Fileserver mit SLIST sichtbar wurden. Und es war eine verdammt mühselige Arbeit, die dazu passenden ADMIN's zu finden, um die damit verbundenen Problemen zu lösen. Außerdem ist das Gespräch zwischen Administratoren eine Quelle für Lösungen und Informationen Der User Guest darf NICHTS. er dient nur dazu, daß jemand, der sich einloggt (Und das versucht er wohl auch mal als GUEST) Infos über den Server bekommt Also Betreiber, Ansprechpartner usw. Wie weit die Infos gehen, sollte jeder Sysop selbst entscheiden Aber er sollte immer daran denken, wenn mehr und mehr WAN's wachsen, werden immer mehr Fileserver zu sehen sein und dann ist es schon hilfreich, wenn man eine Chance hat, den Administrator des neuen Servers anzusprechen. Denn die Wechselwirkungen sind vielfältig

(Stichwort "preferred Server") Da viele Programme (u.a. auch MHS) der Gruppe EVERYONE Rechte geben, sollte man den User GUEST auch aus der Gruppe EVERYONE herausnehmen und ihm mit Directory-trusties gezielt die nötigen Rechte geben. Damit bekommt er nicht über das "Hintertürchen" EVERYONE mehr Rechte, wenn man nicht aufpasst. Zudem kann er damit im Normalfall nicht mal mehr Drucken.

So ergib WHOAMI /A als User GUEST folgendes Resultat:

```
You are user GUEST attached to server FC1, connection 1.
Server FC1 is running NetWare v3.x (100 user).
Login time: Thursday April 8, 1993 7:37 pm
You have no security equivalence class.
You are not a member of any group.
[      ] SYS:
[ R    F ] SYS:LOGIN
[ R    F ] SYS:PUBLC
[ R    F ] SYS:MAIL/2000001
[ R    F ] SYS:PROG/UTIL
[ R    F ] SYS:PROG/MSDOSV5.00
[      ] VLL:
[ R    F ] VLL:USER/GUEST
Server FC1 is not in a Domain.
```

### Abbildung 7 "WHOAMI" Guest

## 3.2.6 MHS / MSMAIL

MHS ist eine Kennung, welche man anlegen sollte, wenn man das Programm MHS benutzt, um Post über Modem oder Internet auszutauschen. Unter dieser Kennung kann sich dann ein Computer einloggen und Post einstellen und abholen, bzw. das Programm MHS ablaufen lassen.

Wird ein anderes Mailsystem eingesetzt, dann ist in der Regel auch dafür ein Benutzer erforderlich, welcher aber zu besseren Kenntlichkeit einen andere Namen trägt.

## 3.2.7 DUMMY

Der User Dummy erfüllt eine besondere Funktion. Er wird gebraucht, damit sich ein PC automatisch im Netzwerk anmeldet, z.B. bei einem RemoteBoot. Dadurch ist es möglich, mittels geeigneter Programme je nach PC bestimmte Aktionen auszuführen, z.B. Gateways starten, Drucker anschließen, oder einfach nur die Konfiguration des Arbeitsplatzes ausfindig zu machen. Zudem erlaubt es dieser User, einfach Mitteilungen einem Benutzer anzuzeigen, BEVOR er sich anmeldet. Die Funktion dieses Users wird deutlich, wenn man die Prozedur des Bootens und Einloggens eines Rechners und dessen Benutzers gelesen hat Die Rechte sollten für diesen User genauso vergeben werden, wie beim User GUEST, d.h. er sollte nicht Teil der Gruppe EVERYONE sein und alle Trusties sollten direkt gegeben werden. Wenn der DUMMY wie beim Konzept benutzt wird reichen folgende Rechte voll aus: (USERLIST /A)

```
You are user DUMMY attached to server FC1, connection 1.
Server FC1 is running NetWare v3.x (100 user).
Login time: Thursday April 8, 1993 7:40 pm
You are security equivalent to the following:
GATEWAYS (Group)
You are a member of the following groups:
GATEWAYS
[      ] SYS:
[ R    F ] SYS:LOGIN
[ R    F ] SYS:PUBLC
[ R    F ] SYS:MAIL/7000001
[ R    F ] SYS:PROG/BAT
[ R    F ] SYS:PROG/UTIL
[ R    F ] SYS:PROG/MSDOSV5.00
[      ] VLL:
[ RW   F ] VLL:USER/DUMMY
Server FC1 is not in a Domain.
```

### Abbildung 8 "WHOAMI" Dummy

Die absoluten Pfade sind natürlich den jeweiligen Gegebenheiten anzupassen. mit DSPACE kann man dem Benutzer auch noch den Speicherplatz einschränken. Da er aber nicht das Rechte zum Erzeugen von Dateien und auch keine Dateien löschen darf, kann er keine neuen Dateien anlegen oder löschen. Ein Eindringlich kann höchstens Utilities und DOS 5.0 kopieren.



Das Schreibrecht auf das Heimatverzeichnis des Users Dummy ist nur während der Installationsphase nötig, da ein entsprechender Batch automatisch die Konfiguration des PC's vom Installateur abfragt (z.B. Seriennummern, Ausstellort, Benutzer) und diese abspeichern muß.

### **3.2.8 Fax**

Der Benutzer Fax ist für den ausgehenden und eingehenden Faxverkehr zuständig. Er hat in der Regel Rechte auf ein eigenes Verzeichnis zum Ablagern temporärer Daten. Sofern dies die Software zuläßt, sollten die temporären Daten auf einer lokalen Festplatte gelagert werden. Damit wird das Netzwerk und das Backup entlastet. Die wichtigen Konfigurationsdaten sollten aber weiterhin auf dem Server liegen, um die regelmäßige Sicherung die die Administration zu vereinfachen.

### **3.2.9 CHECKVIR**

Dieser "User" erlaubt es, jedem am Netzwerk seine lokalen Festplatten oder Disketten nach Viren durchsuchen zu lassen. Dieser User hat kein Passwort und ist extrem eingeschränkt. z.B. darf er ÜBERHAUPT nicht irgendwo im Netzwerk schreiben. Auch nicht Drucken usw. Er hat keinen Zugriff auf Programme. Er kann allein dazu genutzt werden, im Netzwerk verfügbare Virens Scanner zu starten. So ist es nicht nötig, Virens Scanner auf Diskette rumzutragen, welche selbst wieder verseucht werden könnten. Hier spielt ein Netzwerk eine große Stärke (Schreibschutz) aus. Jeder PC am Netzwerk kann geprüft werden. Update der Scannersoftware sind zentral möglich. Auf jedem PC können Disketten getestet werden. Dazu sollte der PC vom Netzwerk (virenfrei) oder Diskette booten. Nach dem Einloggen als User CHECKVIR kann der Scanner die Diskette oder Festplatte prüfen.

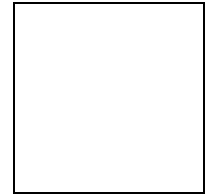
Die Einrichtung diese „Spezialusers“ ist nicht auf jedem Netzwerk notwendig. Werden die Benutzerarbeitsstationen ohne Festplatte betrieben, dann ist dieser Benutzer ohne Sinn.

### **3.2.10 andere User**

Zu anderen Benutzern zählen weitere Gateways (ISDN, FAXGTW, MODEM usw) welche sich anmelden müssen, um auf Dateien in bestimmten Verzeichnissen zugreifen zu können. Zudem kann man dann diese Computer leicht fernwarten, wenn eine Remotecontrolsoftware eingesetzt wird. Mit USERLIST allein kann man schon schnell feststellen, ob das Gateway überhaupt noch angemeldet ist oder nicht schon deshalb nicht funktioniert. Natürlich muß man sichertellen, daß diese User KEINE Rechte haben, welche den Betrieb stören kann, wenn ein "Eindringling" diese Kennung benutzt.

Da diese Benutzer nicht unbedingt der Gruppe EVERYONE zugeordnet sind, ist es möglich, daß eine explizite Rechtevergabe zu Druckqueues eingetragen werden muß.

## 4 Gruppen



NetWare erlaubt es, Gruppen zu definieren, und Benutzer als Mitglieder von Gruppen einzutragen. Gruppen sind ein geeignetes Mittel, ob Verzeichnisse oder Programme einfach zu verwalten. Statt einem Benutzer Rechte zu geben, vergibt man die Rechte einer Gruppe, und trägt den Benutzer als Mitglied ein. Dies ist besonders dann effektiv, wenn mehrere Rechte zusammengebündelt sind. Gruppen kann man für Verzeichnisse und für Programme bilden. Erstere um den Zugriff auf Verzeichnisse (z.B. unter I:) zu steuern, die zweite um Programme auf bestimmte Benutzer zu limitieren.

Man könnte nun je Anwendung eine Gruppe, mit den Rechten auf das Anwendungsverzeichnis definieren. Jedoch ist die z.Z. dadurch limitiert, daß NetWare ohne besondere Kniffe nur die ersten 32 Gruppenzugehörigkeiten eines Users bei den Directory Trusties beachtet, d.h. die Rechte, welche der User mit der 33ten Gruppe bekommen würde, hat er nicht. Daher muß man eine Menge Grundrechte einer Gruppe geben und weitere Programmgruppen selektiv einsetzen Die Zugehörigkeit zu Programmgruppen kann man im Programmbatch mit IF EXIST G:\<Programmverzeichnis>\<programmname> GOTO überprüft werden. So kann man den Aufruf durch einen nicht berechtigten Benutzer abfangen und eine Erklärung anzeigen. Dies ist bei Windowsprogrammen jedoch etwas schwerer.

### **4.1 Group EVERYONE**

Enthält alle Benutzer. Dieser Gruppe gibt man die Rechte, die jeder benötigt, z.B. auf PUBLIC auf das DOS-Verzeichnis, E-Mail und BAT. Jeder neu angelegte Benutzer ist automatisch Mitglied dieser Gruppe. Da diese Gruppe meist schon mehr Rechte hat, als die Gateways und nicht "natürliche" Benutzer brauchen, ist es ratsam, diese unechte Benutzer aus der Gruppe zu nehmen.

### **4.2 Group GATEWAY**

Diese Gruppe enthält all die nicht "naürlichen" Benutzer und gibt ihnen die minimal nötigen Rechte. (z.B. DOS und PUBLIC). Rechte die je Kennung individuell sind, werden dann über Usertrusties vergeben. Diese Gruppe dient dazu, alle Gateways und andere dazugehörige Gruppen zuzuordnen und diese z.B. im Loginscript aussparen zu können.

Zudem kann man anhand dieser Gruppe auch den Befehl CASTOFF ALL ausführen, damit die Gateways nicht durch SEND-Meldungen gestoppt werden.

Damit Gateways drucken können, muß die Gruppe oder der jeweilige Benutzeraccount explizit für die gewünschen Druckqueue zugelassen werden. Standardmäßig ist nur die Gruppe EVERYONE zu jeder Queue zugelassen, aber nicht die Gruppe GATEWAY

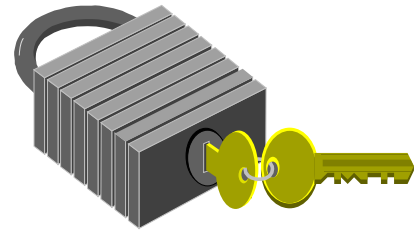
### **4.3 Anwendergruppen**

Zur Strukturierung der Benutzer und Rechte kann der Administrator Benutzergruppen einrichten. Zu Beachten ist, daß NetWare 3.x im Gegensatz zu NetWare 4 keine Hierarchien kennt und damit die Organisation der Netzwerkbenutzer nicht genau abgebildet werden kann. Diese Gruppen sind nur gedacht, Zugriffsrechte auf bestimmte Datenverzeichnisse zu verwalten

### **4.4 Programmgruppen**

Programmgruppen dienen dazu, bestimmte Programme nur bestimmten Benutzern zugänglich zu machen. Damit ähneln diese Gruppen den Anwendergruppen. Hier ist jedoch die leichtete Verwaltung der notwendigen Rechte auf bestimmte Programme das Ziel. Anstatt jedem Benutzer einzeln die Rechte zu geben, lassen sich diese Zuordnungen auch über die Gruppe vergeben. Dies ist dann besonders hilfreich, wenn mehrere Rechte für ein Programm zu vergeben sind.

## 5 Login



Nach dem Einschalten des PC's überprüft das BIOS das System. Nach Abschluß aller Tests (Speicher, Disketten, usw.) sucht das Bios nach einem Bootdevice. In der Regel wird erst die Diskette versucht und darauf die Festplatte. Wenn nun ein zusätzliches ROM installiert ist, kann dieses auch das Booten übernehmen. Dies macht das Remotebootrom auf der Netzwerkkarte. Dabei wird ein Laufwerk A: für den PC emuliert. Daher darf im BIOS auch das Booten von Diskette nicht verboten sein. Ein komplett fehlendes Diskettenlaufwerk ist aber erlaubt. Der hier beschriebene Vorgang ist nicht allgemeingültig, sondern erklärt, wie die Workstations bei diesem Konzept gestartet werden.

### Betriebssystem laden (NET\$DOS)

Beim Remoteboot sucht das Eprom zuerst nach der Datei BOOTCONF.SYS auf dem nächsten Server. Hier kann man ein alternatives Bootimagefile statt NET\$DOS angeben. Sonst wird die Datei NET\$DOS geladen. Dazu wird zuerst das Betriebssystem (z.B. MS-DOS) geladen und darauf die nötigen Treiber für das Netzwerk. Beim Booten von Diskette oder Festplatte geschieht das gleiche.

### LOGIN DUMMY

Der User DUMMY erfüllt die Aufgabe, welche beim Standalone-Computer die AUTOEXEC.BAT einnimmt. Um nicht für jeden Computer ein eigenes Bootfile zu erzeugen, kann man das Bootfile sehr allgemein halten und dieser DUMMY-User loggt sich immer einmal beim Start ein. Dieser kann für den PC spezifische Programme und Einstellungen laden. Leider kann man in diesem Stadium keine Treiber nachladen, welche in der CONFIG.SYS eingebunden werden müssen. Dazu sind dann doch getrennte Bootfiles nötig.

### SystemLoginScript

Das Programm LOGIN wertet das SYSTEMLOGINSCRIPT für den Server aus. Hier werden allgemeine Einstellungen vorgenommen, z.B. Laufwerke zugeordnet (MAP), Umgebungsvariablen gesetzt. Auf das Userloginscript bzw. Domainloginscript (Name Service) wird verzichtet. Das Systemloginscript endet mit EXIT "USERCFG.BAT". Dieser Batch steht im BAT-Verzeichnis (Suchpfad) und dient dazu, die Umgebung für den Benutzer zu definieren. (z.B: Benutzerlevel, Windowsgruppen, CD-Romtreiber u.a.). Dieser Batch startet den USERSET.BAT, welcher die bestimmten Parameter über die Kommandozeile enthält und die nötigen Aktionen veranlaßt. Zuletzt startet dieser Batch den USER.BAT, in welchem der Benutzer eigene Programme und Einstellungen vornehmen kann als Ersatz für die AUTOEXEC.BAT.

### USER.BAT

Dieser Batch ruft beim normalen Benutzer eine Shell (z.B. Windows) auf oder verläßt die Loginprozedur zum Dosprompt. Wenn keine USER.BAT vorhanden ist, durchläuft DOS den Suchpfad und findet die USER.BAT im Verzeichnis G:\BAT. Hier kann der Supervisor eine Default-USER.BAT einrichten, welche dann gestartet wird.

Beim User DUMMY ruft dieser Batch einen PCCFG.BAT auf (CALL). In diesem Batch kann nun anhand der Netzwerkkartennummer (%NODE%) die für diesen PC nötigen Aktionen bestimmt werden. Der Übersichtlichkeit wegen werden die Aktionen selbst in einem dritten Batch (PCSET.BAT) ausgeführt, dem die Aktionen als Parameterzeile übergeben werden.

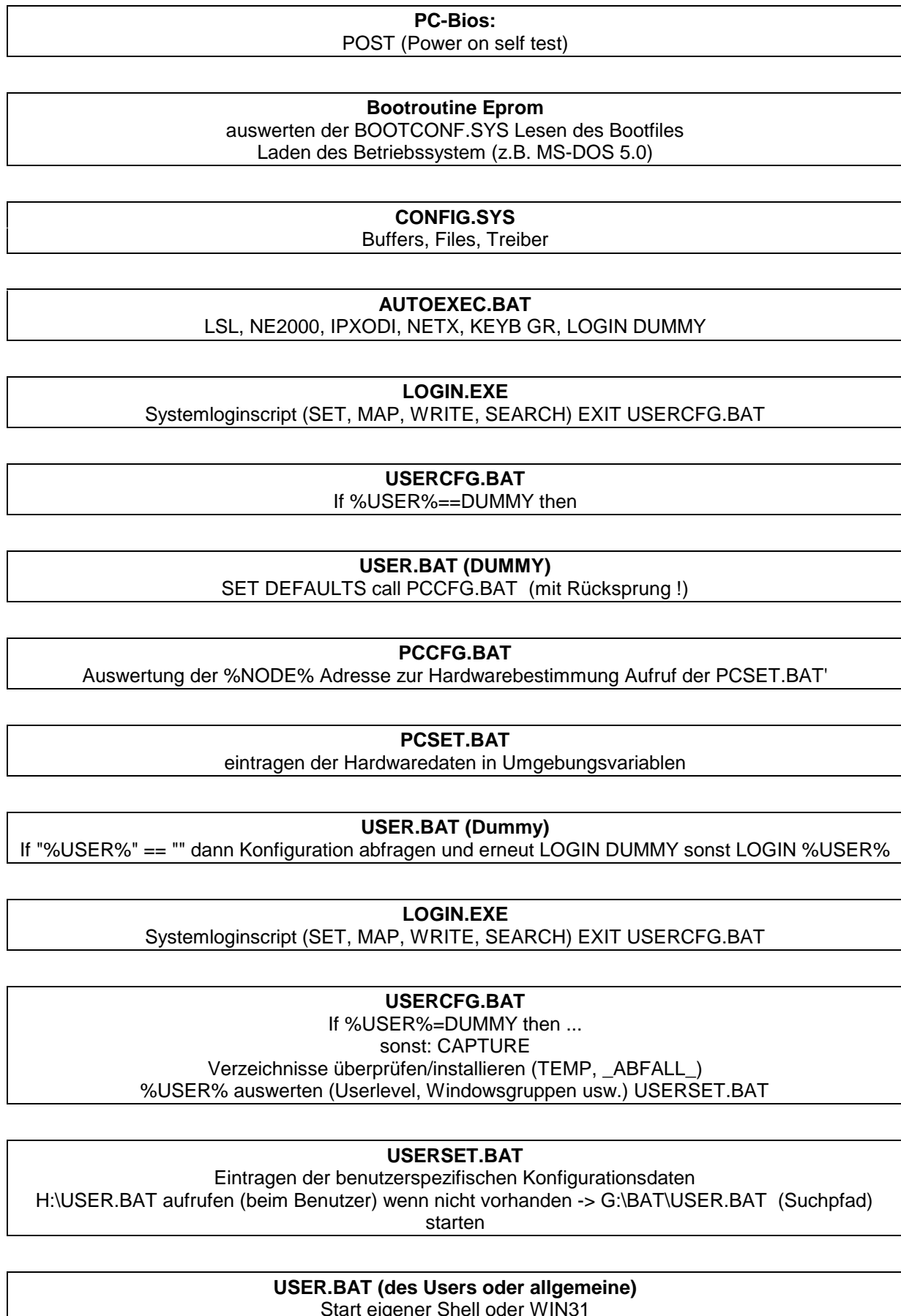
Ist die LAN-Karte noch nicht erfaßt, kann man das im USER.BAT feststellen, da kein User vorgemerkt wurde. Darauf kann automatisch die Konfiguration erfragt werden

Dieser Batch startet dann das LOGIN mit dem vorgemerkten Usernamen.

### Userlogin

Das Login als User durchläuft die vorher beschriebenen Wege, bis auf daß die USER.BAT des Benutzer gestartet wird, welche eine Shell aufrufen kann. Ist diese nicht vorhanden, so startet Dos die USER.BAT im BAT-Verzeichnis, welches es über den Suchpfad findet.

Abbildung 9 Vom Booten zum Login



## 5.1 Booten

Nach dem Einschalten führt der PC einen „PowerOn Self Test (POST)“ durch. Dabei werden alle Komponenten geprüft und im Bios-Datenbereich (0000:0040h) eingetragen. Der Speicher wird eingetragen und die Daten im C-MOS-Ram mit einer Prüfsumme verglichen. Sind hier die Daten nicht stimmig, so bleibt der PC stehen und wartet, bis der Benutzer die Daten korrigiert hat. Der Fall, daß Daten „vergessen“ werden, tritt dann auf, wenn Umbauarbeiten am PC vorgenommen wurden und dadurch die Konfiguration verändert wurde oder die Erhaltungsbatterie des Pcs aufgrund der Lebensdauer entladen ist. Im ersten Fall ist das Setup aufzurufen und sind die Daten neu einzutragen. Im zweiten Fall hilft nur der Austausch der Batterie.

Nachdem das System-BIOS die Tests durchlaufen hat, wird nach anderen BIOS-Erweiterungen gesucht und, sofern vorhanden, werden diese Programme gestartet. Beispiele für solche Erweiterungen sind z.B. BIOS-Roms von SCSI-Kontrollern oder BootRoms von Netzwerkkarten. Nach den Selbsttests sucht der Rechner nach einem Betriebssystem. Dazu wird in der Regel zuerst das Diskettenlaufwerk angesprochen und dann eine aktive Festplatte gesucht.

Beim Betriebssystem DOS wird der Startsektor in den Speicher geladen, welcher seinerseits die Dateien MSDOS.SYS und IO.SYS nachlädt. Zum Schluß wird die COMMAND.COM geladen. Zur Konfiguration dienen die Dateien CONFIG.SYS und AUTOEXEC.BAT.

Wird ein PC, welcher von einer eigenen Festplatte bootet in ein LAN eingebunden, so müssen die Netzwerktreiber geladen werden. Die geschieht für gewöhnlich mit einem eigenen Batchjob oder direkt in der AUTOEXEC.BAT.

## 5.2 Remoteboot

Beim Remoteboot hängt sich das Bootrom beim Hochfahren des Rechner in die Startroutine ein. Das Bootrom prüft in der Regel die Existenz einer aktiven Festplatte ab. Ist eine Festplatte vorhanden, so wird der Benutzer gefragt, ob von dieser Platte gestartet werden soll. Antwortet der Benutzer auf diese Frage nicht innerhalb einer bestimmten Zeit, dann wird automatisch vom Netzwerk gebootet. Wenn keine Festplatte installiert ist, wird sofort vom Netzwerk gebootet. Um die zu ermöglichen, simuliert das Bootrom einen Startvorgang von Diskette.

## 5.3 DOSGEN und Bootimagedatei

Beim Bootem vom Netzwerk holt das Bootrom eine „Imagedatei“ vom Server, welche ein Abbild einer Bootdiskette ist. Dazu sucht es sich den ersten Server, der auf das ausgesandte Packet „Give nearest server“ antwortet. Diese Imagedatei wird mit dem Novellprogramm DOSGEN aus einer bootfähigen Systemdiskette erzeugt. Bei der Generierung der Bootfiles sollte man darauf achten, nur die absolut nötigen Treiber zu laden unter Ausnutzung aller Optionen um Speicher zu sparen. Da nicht jeder PC genau die gleiche Konfiguration benutzt, können mehrere Bootimages nebeneinander bestehen. Damit der jeweilige PC nun bestimmen kann, welches das passende Bootimagefile ist, gibt es eine Datei BOOTCONF.SYS. In dieser Datei stehen alle Stationen mit ihrer Netzwerknummer, Netzwerkkartennummer und dem Bootfile. Diese Datei steht im Verzeichnis SYS:LOGIN

### Konfigurationsdatei 1 BOOTCONF.SYS

```
0x1,0000B4226D50=DOS6XXXX.SYS testbemerkung
0x1,00001B377B16=LWPDOS60.SYS
0x1,0000B4225BEE=DOS6XXXX.SYS 486 Tower
0x1,0000B4220A89=D62PCDGX.SYS PCD4G66
0x1,0000B4226976=DOS6XXXX.SYS
```

Existiert diese Datei nicht oder ist eine Netzwerkkarte nicht aufgelistet, dann versucht das Bootrom die Datei NET\$DOS.SYS zu öffnen. Existiert auch diese Datei nicht oder liegt sonst ein Fehler vor, dann startet der PC neu.

Von dieser „Diskette“ lädt der PC das Betriebssystem und die Treiber, welche in der CONFIG.SYS angegeben sind. Danach wird die AUTOEXEC.BAT ausgewertet. Bei einem Remoteboot muß man beachten, daß beim Laden der Netzwerktreiber die Netzwerkkarte selbst nicht neu initialisiert wird, da sonst die Verbindung zum Server abbricht und ein Booten so nicht möglich ist. Beim Einsatz der ODI-Shell ist es dazu notwendig, das Programm RPLDI nach dem Laden von LSL einmal auszuführen. Damit wird signalisiert, daß eine Initialisierung der LAN-Karte unterbleibt, bis die Netzwerkschell NETX geladen wird.

Das Laden der Netzwerktreiber erfolgt bei Pcs, welche vom Server booten, zwingend in der Startdatei. Wenn nun die Netzwerkschell NETX geladen wird, muß die Netzwerkkarte initialisiert werden, wodurch

die Verbindung zum Server durch das Bootrom angeschlossen wird. Mittels NETX ist nun der Zugriff auf Dateien auf dem Server in SYS:LOGIN möglich. DOS versucht nun den aktiven Batchjob weiterzuführen. Dazu wird der Batchjob mit dem gleichen Namen in SYS:LOGIN aufgerufen. Damit ist klar, daß der Batch, welcher auf der „Diskette“ die Netzwerktreiber lädt, absolut identisch in SYS:LOGIN stehen muß, da DOS „blind“ an die Einsprungstelle geht. Dieser Batch darf daher auch nicht nachträglich von Hand editiert werden, sondern immer nur zusammen mit der Bootdiskette.

Diese Tatsache, daß der Batch in SYS:LOGIN weitergeführt wird, hat nun die Folge, daß die Datei AUTOEXEC.BAT dazu unbrauchbar ist. Es können sonst nicht mehrere Bootimages angelegt werden. Daher ist die Funktion der AUTOEXEC.BAT im Bootimagefile darauf beschränkt, einen anderen Batchjob aufzurufen. Dieser hat zu Vereinfachung genau den Namen der Bootimage-datei. Nur so können verschiedene Konfigurationen parallel nebeneinander bestehen.

Die folgenden Listings enthalten eine Beispieldatei einer CONFIG.SYS, AUTOEXEC.BAT und D62XXXXX.BAT, welche sich gut bewährt haben. Mit den aufgerufenen Programmen und einer Bootdiskette kann damit das Bootfile D62XXXXX.SYS generiert werden.

### 5.3.1 CONFIG.SYS

#### Konfigurationsdatei 2 CONFIG.SYS

```
device      = A:\HIMEM.SYS
device      = A:\EMM386.EXE noems y=F:\LOGIN\emm386.exe
shell       = A:\COMMAND.COM /e:1024 /p
country     = 049,,A:\COUNTRY.SYS
files       = 30
buffers     = 20
DOS         = HIGH,UMB
BREAK       = ON
FCBS        = 16,8
SWITCHES    = /w
```

Startdatei für DOS:  
Laden der Speichermanager und Einstellung der Systemparameter  
Laden Länderspezifische Einstellungen und

### 5.3.2 AUTOEXEC.BAT

#### Konfigurationsdatei 3 Remoteboot AUTOEXEC.BAT

```
@echo off
cls
set bootfile=D62XXXXX
%BOOTFILE%
```

Die AUTOEXEC.BAT startet beim Remoteboot nur die richtige Bootdatei

### 5.3.3 D62XXXXX.BAT

#### Konfigurationsdatei 4 D62XXXXX.BAT

```
@echo off
echo - LSL
lh lsl.com
echo - RPLODI
rplodi
echo - NE2000
LH ne2000
echo - IPXODI
lh ipxodi
echo - NETX
lh netx
n:
echo - Connect
echo - KEYB GR
lh .\MSDOSV6.20\keyb gr,.\MSDOSV6.20\keyboard.sys
login dummy
```

Hier werden die notwendigen Netzwerktreiber geladen und das LOGIN an den Server gestartet.  
Der Tastatortreiber wird hier erst nach der Netzwerkshell geladen. Dies bewirkt eine bessere Speicherauslastung des hohen Speichers

### 5.3.4 NET.CFG

#### Konfigurationsdatei 5 NET.CFG

```
# allgemeine Einträge für Novell Shell ex SHELL.CFG

machine type = IBM
long machine type = PC386
set station time = on
show dots = on
print header = 100
print tail = 0
spx connections = 100
file handles = 150
#
# Folgende einträge sind für NETBIOS
#
NETBIOS COMMANDS=70
NETBIOS INTERNET=OFF
NETBIOS SESSIONS=16
NETBIOS RECEIVE BUFFERS=20
NETBIOS SEND BUFFERS=20

Link Support
  Buffers 8 1514
  MemPool 4096
  Max Stacks 8

Link Driver NE2000
  INT 5
  MEM CC000
  PORT 320
  Frame Ethernet_II
  Protocol IPX 8137 Ethernet_II
  Protocol TCPIP 800 Ethernet_II

Protocol IPX
  bind 1
```

Einträge für die Netzwerkshell NETX.EXE

NetBIOS-Emulator für Novell IPX

Einstellungen für LSL.COM  
Link Support Layer

Einstellungen für Netzwerkkartentreiber (hier NE2000). z.B. Einstellung des Interrupts und des Ports. Aber auch Protokolltypen und Ethernetframes

Diese Dateien sind nur Beispiele. Die Einstellung, auf welches LAN-Board IPX gebunden wird, ist abhängig von den Gegebenheiten (Lan-Karte) und den den des LAN-Treibers schon vorbereitet. Die Section für TCPIP wird jedoch erst später individuell erstellt, damit jeder PC eine eigene IP-Nummer bekommt.

Man muß nun eine bootfähige Diskette erstellen, mit diesen vier Konfigurationsdateien und den nötigen Programmen. Das Programm KEYB und KEYBOARD.SYS brauchen nicht im Bootfile zu sein, wenn sie in F:\LOGIN liegen. KEYB braucht sehr wenig Speicher zum initialisieren, so daß es ganz am Ende geladen werden kann. Würde man es vorher laden, könnte bei den eingesetzten PC's NETX nicht mehr hochgeladen werden. Die Aufteilung des Highmemory ist jedoch von PC zu PC verschieden, so daß hier etwas probiert werden muß. Setzt man MS-DOS 5.0 ein, so kommt es auf das Bootrom an, ob das Booten funktioniert. Eventuell muß mit RPLFIX das Bootimagefile nachbehandelt werden.

Nach dem Booten wird automatisch ein LOGIN DUMMY ausgeführt. Damit durchläuft jeder PC das SystemLoginScript. Wenn aus einem Netzwerk mehrere Server sind, kann man beim LOGIN auch den Servername angeben. Trotzdem muß man alle Bootfiles aus allen Servern ablegen, solange man nicht direkt im Bootromprogramm den gewünschten Server angeben kann. Auch der Eintrag "PREFERRED SERVER" in der NET.CFG hilft hier nicht weiter. Die Funktion dieses Login DUMMY wird später noch deutlich.

Ist überhaupt kein Server vorhanden, so bootet das Bootrom den Rechner neu. Ist der gewünschte Server nicht erreichbar, dann kann dies anhand des ERRORLEVEL nach LOGIN.EXE entdeckt werden und ein Neustart ausgelöst werden.

Bei Bootdisketten (Gateways) oder Rechnern mit Festplatte kann man die Existenz eines Server anhand des Errorlevels beim Laden von NETx feststellen.

### 5.4 Systemloginscript NET\$LOG.DAT

Nach dem Einloggen führt LOGIN.EXE das LoginScript aus. Für den Fall, daß KEIN Systemloginscript vorhanden ist, wird ein Defaultloginscript ausgeführt, welches in LOGIN.EXE kodiert ist. Das Systemloginscript wird benutzt um Laufwerke zuzuordnen, Umgebungsvariablen zu setzen und mehr.

Jedoch empfehle ich, das Loginscript kurz zu halten und darin nur wenig Ausgaben zu machen, Laufwerke zuzuordnen und Umgebungsvariablen zu setzen. Um sich selbst die Aufgabe bei mehreren Servern zu erleichtern, sollte man den Pfad bei Mappings nicht unbedingt genau angeben. Den Servernamen kann man weglassen, da LOGIN dann auf den default-Server zugreift. So kann man das Loginscript leichter kopieren. Auf keinen Fall dürfen TSR-Programme geladen werden.

Zwar hat jeder User die Möglichkeit, ein Userloginscript anzulegen, jedoch wird auf dieses Mittel verzichtet. Die Syntax des Loginscripts ist nicht geläufig. Statt dessen wird ein Batchjob im Userverzeichnis aufgerufen (H:\USER.BAT) in welchem individuelle Einstellung, Treiber usw geladen werden können. Diese Datei ist der Ersatz für die fehlende individuelle AUTOEXEC.BAT beim Remoteboot. In dieser Datei kann auch die Arbeitsoberfläche (z.B. Windows) gestartet werden.

Das Systemloginscript kann man in fünf Bereiche einteilen:

Anzeige	Ausgabe von Inforamtionen zum Netzwerk
Environment	Setzen der Umgebungsvariablen
Laufwerke	Zuordnung (MAP) von Laufwerken und Suchpfaden
Infos	Optional Anzeige von Informationen nach dem LOGIN
Sonstige Aufrufe	default Druckerzuordnung und Start der USER.BAT

### Konfigurationsdatei 6 Systemloginscript

```
#SYS:prog\util\clearcrt 0
REM ----- setup environment -----
map display off
map errors off
dos verify on
pccompatible

REM ----- setup DOS-environment -----
set SERVER = "FC"
set MV = "FC/SYS:PROG"
set PROMPT = "$p$g"
set WINPMT = "[win] $p$g"
set NODE = "%P_STATION"
set TMP = "H:\TEMP"
set TEMP = "H:\TEMP"
REM ----- MAP Driveletters F: G: I: -----
map F:=SYS:
map root G:=SYS:PROG
map root I:=SYS:GROUP

REM ----- USER-Laufwerk H: Mappen -----
IF "%LOGIN_NAME"="SUPERVISOR" THEN BEGIN
  set USER = "SV"
  set MACHINE = "SV"
  set NAME = "SV"
  map root H:= SYS:USERS/SV
  map root u:= SYS:
ELSE
  set USER = "%LOGIN_NAME"
  set MACHINE = "%LOGIN_NAME"
  map root H:=SYS:USERS\%LOGIN_NAME
END

REM ----- Suchpfad anpassen -----
if "%<BOOTFILE>" = "" then goto localdos
REM
set PATH = "F:\LOGIN\%OS%OS_VERSION"
comspec=F:\LOGIN\%OS%OS_VERSION\COMMAND.COM

localdos:
set PATH = "F:\PUBLIC;G:\BAT;G:\UTIL;G:\WIN31;%<PATH>"

#g:\util\flushkey now
DRIVE H:
EXIT "USERCFG.BAT"
```

Einstellung der internen Parameter von LOGIN EXE

Setzen der Umgebungsvariablen für DOS

Zuordnen der notwendigen Laufwerksbuchstaben

Benutzerabhängige Einstellungen setzen:  
 Heimatlaufwerk zuordnen und die Umgebungsvariablen setzen.  
 Abhandlung des „Sonderfalles“ SUPERVISOR

COMSPEC bei Remoteboot auf die richtige DOS-Version setzen

Suchpfad setzen

Tastaturbuffer löschen und USERCFG.BAT aufrufen

CLEARCRT löscht einfach den Bildschirm.

FLUSHKEY löscht den Tastaturbuffer. Dies ist nötig, da der Befehl EXIT "USERCFG.BAT" die Zeichen "USERCFG.BAT" in den Tastaturbuffer schreibt. Hat während des Ablaufs von LOGIN.EXE der Benutzer irgendeine Tasten gedrückt, wäre die Ausführung des letzten Befehls nicht sichergestellt.



### 5.5 USERCFG.BAT

Die Datei USERCFG.BAT steht im Batchverzeichnis G:\BAT und führt "benutzerspezifische" Einstellungen durch. Beim User Dummy wird sofort in die USER.BAT des Dummy (H:\USER.BAT) verzweigt.

Das Programm ECHOLN wird statt der Ausgabefunktion ECHO von MS-DOS benutzt. Damit verzichtet man nicht auf jegliche Art von Ausgabe, verhindert aber, daß der Bildschirm vor Ausgabemeldungen durchscrollt und manchen Benutzern abschreckt. ECHOLN gibt die Parameterzeile einfach aus, ohne jedoch eine neue Zeile zu beginnen. Der Befehl CASTOF ALL verhindert, daß während der Konfiguration der Computer durch Meldungen angehalten wird. Die Meldungen werden erst wieder nach dem LOGIN des eigentlichen Benutzers der Station am Ende der USERSET.BAT eingeschaltet. So sieht man von allen Batches nur ein Zahlenstrahl, welcher aufgebaut wird.

#### Konfigurationsdatei 7 USERCFG.BAT

```
@echo off
cls
castoff ALL >nul:
echoln 1
if "%USER%" == "DUMMY" h:\user.bat

rem ----- Druckerumleitung -----
IF "%QLPT3%" == "NO" goto nocapture
if "%QLPT3%" == "no" goto nocapture
IF "%QLPT3%" == "" goto nocapture
capture q=%QLPT3% s=%SERVER% l=3 nb nff nt ti=30>nul:

:nocapture
rem ----- Anlegen TEMP-Verzeichnis -----
if exist H:\TEMP\TEMP.FLG goto tempdirda
md H:\TEMP >nul:
echo Dummydatei. NICHT loeschen. fuer temporaere Daten > H:\TEMP\TEMP.FLG

rem ----- ABFALL löschen -----
:tempdirda
echoln 2
rem Lösche Abfalleimer ...
deltree h:\_abfall_\*. * >nul:

rem ----- Bestimme Benutzerkonfigurati
REM Windowsgruppen (neben Netzwerk/Autostart)
REM Userlevel (0=begin) ----+ ! ! ! !
REM Batchfile -----+ !! ! ! !
REM Dos-Variable: 0 1 2 3 4 5
if %USER%==SV USERSET 1 ADMIN LEER LEER LEER
if %USER%==ADMIN USERSET 1 ADMIN LEER LEER LEER
if %USER%==FCARIUS USERSET 2 CDROM LEER LEER LEER

rem ----- ansonsten Defaulteinstellungen -----
USERSET 0 LEER LEER LEER LEER
```

Wenn aktuelle Benutzer = DUMMY, dann zur PC-Konfiguration springen.

Druckerumleitung für DOS auf den definierten Drucker setzen

„Abfalleimer“ löschen.

Besonderen Benutzern einen höheren „LEVEL“ geben

Für alle User außer dem User DUMMY kann man anhand der USERCFG.BAT Einstellungen abspeichern. Zudem wird dieser Batch dazu genutzt, um zur Funktion nötige Verzeichnisse in H: einzurichten bzw. deren Vorhandensein zu überprüfen. Zudem kann hier auch ein Defaultcapture erfolgen. Die Einstellungen werden dem USERSET.BAT als Kommandozeile übergeben, welcher letztlich daraus Umgebungsvariablen setzt und weitere Aktionen ausführt.

### 5.6 USERSET.BAT

Der USERSET.BAT steht wie der USERCFG.BAT ind G:\BAT und wird vom USERCFG.BAT aufgerufen. Er wertet die Parameterzeile aus. Einige Einstellungen und Aktionen werden erst verständlich, wenn man einige Programmbatches analysiert hat (z.B. WIN31.BAT), welche diese Einstellungen ihrerseits benutzen.

#### Konfigurationsdatei 8 USERSET.BAT

rem Benutzerkonfiguration wird gespeichert .....

echo off

echo/n 3

rem ----- allgemeine Variablen -----

set DEBUG=NUL:

set EXMBOX=ALT

set EXPURGE=5

set LEVEL=0

Allgemeine Variablen  
setzen

rem ----- %1 = Benutzerlevel-----

set LEVEL=%1

rem ----- %2 - %4 Windowsgruppen -----

rem Gruppen werden bei Windows kopiert und PROGMAN.INI gepatched

set GRUPPE1=%2

set GRUPPE2=%3

set GRUPPE3=%4

set GRUPPE4=%5

Eintragen der  
beim Aufruf von  
USERCFG.BAT  
übergebenen

rem ----- %6 = ?????????? -----

rem Ab nun geht die Kontrolle an den User selbst

echo/n 4

echo.

h:

cd \

caston >nul:

user.bat

Netzwerkmeldungen wieder aktivieren und die  
USER.BAT aufrufen. Wenn diese nicht im  
Heimatverzeichnis vorhandenist, wird die  
allgemeine USER.BAT in G:\BAT aufgerufen

### 5.7 USER.BAT

Beim Login des Users Dummy wird dessen USER.BAT im Heimatverzeichnis aufgerufen. Diese USER.BAT ist jedoch beim Dummy das Herzstück der Konfiguration.

Beim normalen Benutzer ist diese Datei meist nicht vorhanden. dann wird dank des Suchpfades die USER.BAT in G:\BAT ausgeführt, welche die normale Programmoberfläche startet (Dosshell, Windows, oa). Bei Gateways sollte in diesem Batch z.B. das Gatewayprogramm gestartet werden. Zudem kann hier auch mit CASTOFF ALL eine Unterbrechung des Gateways verhindert werden.

#### Konfigurationsdatei 9 USER.BAT (default)

```
echo off
cls
echo Ich starte für Sie Windows 3.1..
win31
```

Beim User Dummy ruft dieser Batch den Batch PCCFG.BAT auf. Dieser ermittelt anhand der Stationsnummer die Einstellungen dieses PC's und den Benutzernamen. Ist dieser Benutzername nicht bestimmt worden, so läuft der Batch in eine Konfigurationsroutine, welche die Konfiguration abfragt. Dies passiert je Netzwerkkarte genau einmal.

#### Konfigurationsdatei 10 USER.BAT (DUMMY)

```
rem USER.BAT des USERS DUMMY
echo ln 2
rem ----- Automatische Hardwarekonfiguration -----
call pccfg.bat
echo ln 6

if not "%USER%" == "DUMMY" goto configfound
cls
echo ***** WARNUNG *****
echo Dieser PC wurde noch nicht eingetragen. Bitte benachrichtigen Sie
echo den Support für die Beantwortung nachfolgender Fragen ....
echo Bei Fehleingabe bitte mit CTRL-C abbrechen, dann erneut eingeben
echo *****
echo .

:nochmal
getcfg PCCFG.BAT PCSET Username G
Dose
if errorlevel 1 goto nochmal
rem und nun nochmal ein LOGIN DUMMY
rem ----- Daten bestimmt... Userlogin -----
:configfound
if "%USER%" == "unknown" set USER=
cls
if not "%USER%" == "" echo Bitte geben Sie das Passwor
login %USER%
```

Aufruf der PC-Konfiguration

Wenn %USER% immer noch DUMMY, dann ist der PC nicht eingetragen

Erfassen der Konfiguration und Eintragen in die DOSSET.BAT

Konfiguration eingestellt, Nun kommt der Login des Benutzers

Nachdem MS-DOS wieder zu diesem Batch zurückgekehrt ist (CALL PCCFG.BAT) wird anhand der Umgebungsvariable %USER% bestimmt, welcher Benutzer an diesem PC normalerweise arbeitet. Dieser wird dann mit dem Programm LOGIN angegeben. Damit können auch Gateways ohne Password automatisch angemeldet werden und der Benutzer wird direkt aufgefordert, sein Password anzugeben. Sollte ein anderer Benutzer an diesem Computer arbeiten wollen, muß er sich selbst anmelden, indem er das vorbereitete Login abbricht.

### 5.8 PCCFG.BAT

Der Batch PCCFG.BAT wird beim User DUMMY aufgerufen, um anhand der Netzwerkkartenummer die Konfiguration zu ermittelt wie sie bei der Installation angegeben worden ist. An diesen Batch werden bei der Neuinstallation von Workstations die neuen Parameter halbautomatisch angehängt. Dazu dient das Programm GETCFG, welche einfach die Eingaben von der Tastatur annimmt und zuletzt die neue Zeile anhängt. Diese Programm umgeht das Fehlen adäquater Eingabefunktionen für DOS-Batchfiles. Diese Parameter werden ähnlich wie bei dem Gespann USERCFG.BAT und USERSET.BAT an den Batch PCSET.BAT weitergegeben, welcher daraufhin Aktionen durchführt.

#### PCCFG.BAT des Users DUMMY

##### Konfigurationsdatei 11 PCCFG.BAT

```

echoln 3
REM ----- Defaulteinstellungen-----
set VIDEO=VGA162X
set PCNUM=0
set QLPT3=-
REM Ans Ende dieses Batches werden neue NODEs angefügt. Da dies
REM Halbautomatisch geschieht, darf NICHTS störendes hinten angehängt sein
REM ----- Konfiguration -----
REM
REM 4 LPT3 printqueue -----+
REM 3 PC-number (IP) -----+ !
REM 2 VIDEO CCCFFRS .CFG
REM CCC = Chiptype S3_M8_ET4 WD2_VGA EGA HGC
REM FF = Farben BW 04 08 16 FF(=256) HC(=High color) TC(=Truecolor)
REM A = Auflösung 0=HGC 1=EGA 2=VGA 3=VGA 4=1024x768 5=1280x1024
REM S = Schrift L = Large M= Medium S = Small X=n/a
REM
REM Station_____batch_username_VID_PC_QLPT3__RAUM_MONI_PC_KEY__Dose__
if %NODE%==0000B4226987 PCSET - S3_164x - HP4-FC FC FC FC FC FC
if %NODE%==00001B377B16 PCSET - HGcbw0x - HP4-FC fc fc fc fc fc
if %NODE%==0000B4226975 PCSET - VGA163x - HP4L fc fc fc fc fc
if %NODE%==0040950493DC PCSET - VGA163x - hp4l fc fc fc fc fc
if %NODE%==0000B4225BEE PCSET FCARIUS S3_164x - HP4L - - - -
if %NODE%==0000B4220A94 PCSET FCARIUS CL3FF4x - HP4L FC FC FC FC FC
if %NODE%==0000B422709C PCSET fcarius WD2FF4x - HP4L fc fc fc fc fc
    
```

Die Standardeinstellungen

Einige möglichen Grafikmodi

Je nach Ethernetnummer werden die Daten der PCSET.BAT übergeben

Dieser Batch startet den PCSET.BAT mit den Konfigurationsdaten als Parameter. Diese werden vom PCSET.BAT in Umgebungsvariablen umgewandelt, bzw. die nötigen Treiber werden nachgeladen. Diese Konfiguration ist noch ausbaubar, (z.B. NETBIOS, IP-Treiber, Supportmodule)

### 5.9 PCSET.BAT

Anhand der physikalischen Kartenummer wird dieser Auswertbatch durchlaufen, welcher ua Videokarte, IPO-Nummer, Defaultdrucker, Defaultuser einstellen kann.

Nachdem dieser Batch durchlaufen wurden, kehrt MS-DOS wieder zum USER.BAT des Users DUMMY zurück. In dieser Datei können auch grafikkartenspezifische Befehle ausgeführt werden. Dazu muß man nur den Typ der Grafikkarte auswerten und eventuell die Parameter um den Monitortyp ergänzen.

##### Konfigurationsdatei 12 PCSET.BAT

```

rem ----- %1 = USERNAME -----
set USER=%1
rem ----- %2 = Grafikkarte -----
set VIDEO=%2
rem ----- %3 = PC Nummer -----
rem z.B. für TCP/IP oder anderes
set PCNUM=%3
rem ----- %4 = Printqueue LPT3 -----
set QLPT3=%4
rem Ruckprung zur USER.BAT des DUMMY
echoln 5
    
```

Setzen der übergebenen Variablenwerte

## **6 Programme**

Die Qualität und Benutzerfreundlichkeit der Anwendungsprogramme, welche im Netzwerk installiert sind, tragen entscheidend zum Erfolg des Netzwerkes bei; ein wichtiger Aspekt in der Art der Installation. Sie wird vom Administrator durchgeführt und muß seinen Konzepten entsprechen und ein Optimum an Integration gewährleisten. Der Benutzer selbst bemerkt nicht, welche Arbeit hinter den Kulissen geleistet worden ist.

### **6.1 Generell**

In einem Netzwerk befinden sich oft viel mehr Programme, als auf einer einzelnen Workstation. Dementsprechend muß der Administrator sich einige Regeln aufstellen, mit denen er sich die Arbeit erleichtert. Schließlich muß er die Teile der einzelnen Programme zusammenhalten, um keine "Dateileichen" zu hinterlassen. Zudem kommt es speziell bei der Umstellung auf eine neue Version vor, daß für eine bestimmte Zeit auch noch die alte Version verfügbar sein muß.

Es hat sich gezeigt, daß die meisten Programme damit leben können, wenn sie ein eigenes Unterverzeichnis im Programmbereich (G:) erhalten. Um beim Update keine Probleme zu erhalten, empfiehlt es sich, den Verzeichnisnamen mit der Versionsnummer zu verbinden (z.B. WIN31, WORD55, EXCEL4).

Man kann sich die Übersicht erleichtern, wenn man die Extension mitbenutzt. Viele Programme lassen sich davon nicht stören, so daß man als Extension z.B. WIN, OS2, DOS, MAC usw benutzen kann.

Im Idealfall gibt es keinen User (außer Supervisor und Admin), der mehr als LESEN auf das Programmverzeichnis darf. Damit stellt man sicher, daß eine nachträgliche Änderung von Programmen vermieden wird. (Virus, Sabotage, Programmierfehler, Bedienungsfehler)

Da die meisten Programme eine Konfigurationsdatei anlegen und ohne diese nicht korrekt laufen, ist es weiterhin sinnvoll, in einem gesonderten Verzeichnis (z.B. G:\WIN31\INI) eine Standardkonfiguration abzulegen. Diese kann dann beim erstmaligen Start der Applikation vorher in das Userverzeichnis kopiert werden.

Es hat sich gezeigt, allgemeingültige Vorlagen bei jeder Applikation in einem neu anzulegendem VORLAGEN-Verzeichnis abzulegen und beim Start ins Benutzerverzeichnis zu kopieren. Alternativ bietet sich ein VORLAGEN-Verzeichnis auf dem Gruppenlaufwerk I: an, aus welchem sich jeder Mitarbeiter die benötigten Vorlagen selbst kopiert.

## 6.2 Start mit Batch, Sonderbatches (nolimit, norights)

MS-DOS und andere Betriebssysteme erlauben es, das eigentliche Programm über Batchjobs zu starten. Diese Möglichkeit wird im Netzwerk sehr gebraucht, um Konfigurationen vorher zusammenzustellen. Programme unter Windows entziehen sich dieser Möglichkeit, wenn man kein gesondert zu erstehendes Programm einsetzen will (z.B. WINBATCH).

Hier kann man auch "sanft" abfangen, wenn Benutzer versuchen, Programme zu starten, welche nicht für sie freigegeben sind. Abfragen läßt sich das, indem man auf die Existenz einer Datei im Programmverzeichnis abfragt. Wenn der Benutzer keine Rechte darauf hat, so wird das Betriebssystem des Computers diese Datei nicht finden. Eine passende Reaktion (Meldung an ADMIN, Mitteilung an den Benutzer) kann dann ausgeführt werden.

Alle Batches durchlaufen meist folgende Abfragen und reagieren entsprechend. Treffen die Bedingungen zu, wird die nächste Bedingung abgearbeitet.

Überprüfung, ob der Benutzer die Rechte zum Programm hat.

NEIN: Abbruch mit Fehlermeldung, eventuell automatische Benachrichtigung des Administrators

Überprüfung, ob die Hardware den Start zuläßt

NEIN: Abbruch mit Meldung, eventuell Nachricht an Administrator

Überprüfung der benutzerspezifischen Installation, d.h. ob benötigte Verzeichnisse und Dateien existieren

NEIN: Neuinstallation, d.h. Verzeichnisse und Dateien erstellen

Kopieren bzw Zusammenstellen der zum Betrieb nötigen Konfigurationsdateien (Hardwareabhängig und Benutzerabhängig)

Setzen benötigter Umgebungsvariablen und Suchpfade, Laden benötigter TSR-Programme

START des Programmes

Löschen von vorher gesetzten Variablen und TSR-Programmen.

Löschen nicht mehr benötigter Daten (z.B. SYSTEM.INI bei Windows) und PURGE der gelöschten Dateien

Rückkehr zum Betriebssystem, eventuell mit kurzer Information für den Benutzer

### 6.3 Rechtevergabe

Sicher gibt es Programme, auf die alle User Zugriff haben. Die Rechte auf diese Verzeichnisse kann man dann der Gruppe USER oder EVERYONE geben. Aber es gibt auch Programme, welche nur von bestimmten Benutzern aufgerufen werden dürfen. Solange es zur Nutzung des Programmes ausreicht, die Rechte auf ein Verzeichnis zu vergeben, kann man dies noch pflegen. Eine bessere Möglichkeit, speziell bei umfangreicheren Rechten, bietet sich, wenn man die Funktion der Gruppenrechte nutzt, d.h. man richtet eine Gruppe ein, gibt der Gruppe die Rechte auf das Programm und nimmt dann die einzelnen Benutzer als Mitglieder dieser Gruppe auf. Somit reicht es, einen neuen Benutzer in diese Gruppe aufzunehmen, um ihn für das Programm zu berechtigen. Bedingt eine neuere Version des Programmes veränderte Rechte, so wird nur die Änderung für die Gruppe nötig. Kein User kann vergessen werden.

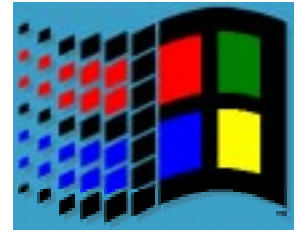
Eine Schwachstelle muß erwähnt werden. Ohne Patches und Kniffe ist es bei NetWare 3.x zwar möglich, mehr als 32 Gruppen zu erstellen und einen Benutzer in mehr als 32 Gruppen aufzunehmen, jedoch werden nur die Rechte der ersten 32 Gruppen gewährt. Ein Programm aus der NetWare (OVER32) löst dieses Problem über den Umweg eine zweite Gruppe anzulegen und diese über "Security Equivalent" zu verbinden.

### 6.4 Konfiguration speichern (Benutzer <-> Hardware)

Ein kniffliges Thema ist die Abspeicherung der Konfiguration. Ärger gibt es immer dann, wenn die Applikation die Trennung von Benutzerinformation und Hardwareinformation nicht zuläßt.

Selbst Programme, die diese beiden Informationen in zwei getrennten Dateien abspeichern, müssen oft durch COPY-Befehle vor dem eigentlichen Start überlistet werden. Windows 3.1 erwartet die beiden Dateien WIN.INI und SYSTEM.INI in dem Verzeichnis, in welchem sich auch die WIN.COM befindet. Da Farben usw in der WIN.INI abgelegt werden, wird man diese in Datenbereich des Benutzer belassen und die SYSTEM.INI vor dem Start abhängig von der PC-Hardware hinkopieren oder patchen. Hier ist die Phantasie und das Können des Administrators gefragt, denn selten sind Programme "ideal" für die eigene Umgebung. Im Normalfall muß man dem Benutzer einige "Features" wegnehmen, bzw. sie lassen sich nicht individuell einstellen.

## 7 Windows im LAN



Windows ist eine Benutzeroberfläche, welche vielen Benutzern in der Bedienung sympatischer ist, als die Kommandozeile von COMMAND.COM. Weiterhin bietet Windows eine Fülle von Funktionen für Programme, welche unter Windows laufen. Im gleichen Maße bereitet sie den Netzwerkverwaltern manchmal Probleme, da die „Standardinstallation“ von Software meist nicht reibungslos abläuft. Ein Installationsprogramm kann eben nicht jedes Netzwerkkonzept erkennen. Daher bleibt bei Installationen immer einiges an Handarbeit danach übrig, bzw der Administrator muß versuchen, die Programmierfordernisse und seine Richtlinien zu verbinden.

Die reine Installation von Windows in einem Novellnetzwerk ist nicht besonders schwer. Mit SETUP /A wird Windows auf ein gemeinsames Serververzeichnis installiert. Dabei kopiert dieser Vorgang einfach alle Dateien der Disketten entkomprimiert auf dem Server. Als Verzeichnis kann WIN31 für Windows 3.1 angegeben werden. Genauso ist mit späteren Updates oder Treiberdisketten von Drittherstellern zu verfahren. Unter DOS kann man mit dem Programm EXPAND von Microsoft den Auspackvorgang auch von Hand erledigen. Wichtig ist, daß möglichst alle Programme und anderen Dateien, welche „geshared“ werden können und damit auch sollen, im gemeinsamen Windowsverzeichnis abzulegen.

Geht man nun nach der Anleitung in den Handbüchern, dann ist je Computer ein SETUP /N nötig. Diese Setup erstellt im lokalen Verzeichnis die Konfigurationsdateien; unter anderem auch die SYSTEM.INI und die WIN.COM. Leider funktioniert dies nur solange, wie EIN Benutzer IMMER an dem GLEICHEN Computer arbeitet. denn die SYSTEM.INI und die WIN.INI enthalten benutzerspezifische aber auch hardwareabhängige Einträge. Damit ist diese Methode für uns unbrauchbar.

Die Einrichtung von Windows geht mit unserem Netzwerkkonzept einher. Ziel ist es, daß jeder Benutzer an jeder Station arbeiten kann. Dabei jedoch immer der räumlich nahestehende Drucker und die passende Grafikauflösung für den Monitor und die Grafikkarte eingestellt sind. Einschränkend ist zu sagen, daß ein Benutzer nicht gleichzeitig an mehreren Stationen arbeiten sollte. Dies ist möglich, wenn der Start von Windows versetzt erfolgt (wg SYSTEM.INI), jedoch reagieren einige Programme irritiert, daß ihre INI-Dateien eventuell von einer anderen Station gesperrt oder modifiziert sind; z.B. PROGMAN.INI. Notwendig ist, daß je PC die Grafikkarte und die Auflösung als auch der passende Drucker hinterlegt ist. Hierzu eignen sich die Umgebungsvariablen %VIDEO% und %PRINTER%, welche beim LOGIN des Users Dummy unabhängig vom Anwender eingestellt werden. (Siehe PCCFG.BAT). Nun müssen diese Werte vor dem Start oder beim Start von Windows ausgewertet werden und notwendige Änderungen der INI-Dateien veranlassen. Dazu dienen ein INI-Patchprogramm und das Programm PRINTSET. Weiterhin müssen die Programmgruppen dynamisch verwaltet werden. Nicht jeder Benutzer kann auch jedem PC all seine Programme nutzen, z.B. können Terminalemulationen nur bei geladenem IP-Stack angewendet werden. Dabei hilft uns GRPPATCH und das INI-Patchprogramm.

### **7.1 Einrichten einer neuen Auflösung**

Wir nutzen SETUP/N oder ein Windows auf einer lokalen Festplatte um eine SYSTEM.INI erstellen zu lassen, welche die Einträge für die Hardware enthält. Diese SYSTEM.INI wird dann zentral im Konfigurationsverzeichnis für diese Hardware (hier: G:\WIN31\%VIDEO%.CFG) abgelegt, so daß diese beim nächsten Start von Windows durch den WIN31.BAT in das Benutzerverzeichnis kopiert wird.

Weiterhin hat man alle Veränderungen an anderen INI-Dateien zu beachten (besonders bei der Installation neuer Software) um diese später dann bei den Benutzern per Batch oder anderweitig nachzuführen. Dazu werden mit einem INIPATCH-Programm bei Bedarf einzelne Zeile hinzugefügt oder gelöscht. Diese SYSTEM.INI wird ein Wert der Umgebungsvariable VIDEO zugeordnet, so daß beim nächsten Start diese SYSTEM.INI zum Benutzer kopiert wird.



## 7.2 Temporäre Daten und Auslagerungsdatei

Windows benutzt die Variable TEMP, um den Pfad zu spezifizieren, wohin temporäre Dateien geschrieben werden. Falls die Workstation eine Festplatte hat, sollte TEMP dorthin zeigen um eine übermäßige Belastung des Netzes gering zu halten. Allerdings halten sich nicht alle Applikationen daran. Swapfiles können benutzt werden, wenn sie auf einer lokalen Festplatte liegen. Temporäre Swapfiles auf dem Server erzeugen unnötig viel Datenvolumen und bremsen das komplette LAN. Jedoch empfiehlt es sich ganz ohne Auslagerungsdateien auszukommen, da diese immer Zeit kosten und Windows wohl auch "vorsorglich" schon auslagert, obwohl noch genug Hauptspeicher frei ist. Wenn wirklich zu wenig Speicher frei ist, empfiehlt es sich, den PC-Speicher aufzurüsten. Die Swapfunktion von Windows sollte man bei genügend Arbeitsspeicher komplett abschalten (SYSTEM.INI: [386Enh] paging=no)

## 7.3 Programmgruppen

In der PROGMAN.INI könnte man einige Gruppdateien sharen, d.h. mehrere Benutzer verwenden die gleiche Gruppdatei. Jedoch stört dies den reibungslosen Ablauf, da des öfteren Meldungsboxen "Kann Gruppdatei nicht schreiben" u.s.w. weggeklickt werden müssen. Daher sollten Windowsgruppen nicht in einem gemeinsamen Verzeichnis genutzt werden, sondern bei jedem Start kopiert werden. Abhängig von den Rechten auf die jeweiligen Programm würde der Benutzer dann entweder die richtigen Icons sehen oder nur ein leeres Icon. Es können aber auch die Programmgruppen dynamisch aufgebaut werden. Dabei hilft das Programm GRPPATCH, welches dynamisch Programmicons zu einer Gruppe hinzufügt, wenn das Programm in der GRPPATCH.INI definiert ist und der Benutzer die Rechte auf das Programm hat.

## 7.4 GRPPATCH

GRPPATCH ist ein Programm., welche in der AUTOSTART-Gruppe plaziert werden kann. es liest eine INI-Datei im gleichen Verzeichnis aus. In dieser INI-Datei sind der Programmname, die Pfade, Icons etc codiert.

Das Programm liest nacheinander diese Einträge und für diese Icons der jeweiligen Programmgruppe hinzu. Dies geschieht jedoch nur, wenn der Benutzer auch die Rechte auf diese Programme hat. Damit ist es einfach möglich, daß nur die Icons sichtbar sind, welche der Benutzer zumindest durch Rechte ausführen kann. Dies ersetzt jedoch nicht die Konfiguration der INI-Dateien

### Beispiel einer GRPPATCH.INI

```
[ProgMan]
Gruppe=Netzwerk
1=G:\win31\printman.exe,Druck-Manager,G:\win31\printman.exe,0,,H:\,,1
2=G:\win31\winfile.exe,Datei-Manager,G:\win31\winfile.exe,0,,H:\,,1
3=G:\winword6.win\winword.exe,Microsoft Word,G:\winword6.win\winword.exe,0,,H:\,,1
4=G:\excel5.win\excel.exe,Microsoft Excel,G:\excel5.win\excel.exe,0,,H:\,,1
5=G:\powerp30.win\powerpnt.exe,Microsoft PowerPoint,G:\powerp30.win\powerpnt.exe,0,,H:\,,1
```

Parameter für GRPPATCH.  
Anhand dieser Daten überprüft  
GRPPATCH die  
Programmgruppen

Diese INI-Datei veranlaßt GRPPATCH, eine Gruppe Netzwerk zu suchen. Wenn diese nicht vorhanden ist, wird diese angelegt. Danach werden nacheinander die Programme hinzugefügt. Vorher werden Icons der gleichen Beschreibung gelöscht, so daß Doppelseinträge vermieden werden.

## 7.5 Drucker

Der Druckmanager von Windows hat im Netzwerk eine erweiterte Bedeutung. Mit ihm ist es möglich, einen Druckjob aus der Warteschlange zu löschen ohne PCONSOLE zu kennen. Mit der Druckersteuerung kann man auch CAPTURE mittels Mausclick ausführen. Zwar kann man mit dem Druckmanager auch Warteschlangen anbinden und umstellen und jede Menge Druckoptionen einstellen. In der Regel ist jedoch der Druckmanager nicht notwendig. Durch die Einrichtung wurde jedem Computer ein Drucker zugewiesen. Diese Einstellung macht das Programm PRINTSET. Für die Auswahl anderer Drucker steht das Programm PRINTSET als zur Verfügung. Je Drucker kann ein eigenes Icon eingerichtet werden. PRINTSET erlaubt es, eine INI-Datei mit Aliasnamen einzurichten. Sodann können die Benutzer durch Starten von PRNTSET auf einen Schlag sowohl Druckertreiber, Port als auch Queue umstellen.

## 7.6 Nachrichten

Damit netzwerkweite Meldungen (SEND) ankommen, muß das Programm NWPOPOP automatisch geladen werden. Entweder durch einen Eintrag in der WIN.INI (LOAD=G:\WIN31\NWPOPOP) oder in der Autostartgruppe. Diese Nachrichten werden z.B. durch den Server verschickt (UPS-Stromausfall).

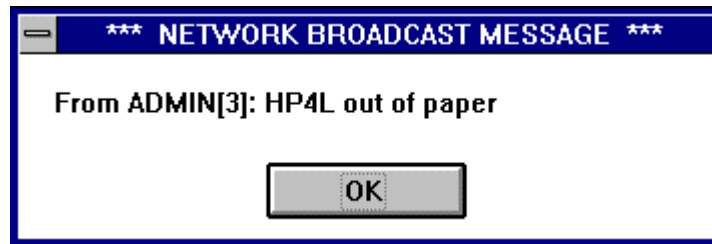


Abbildung 10 "SEND"-Message

Auch Druckserver können so konfiguriert werden, daß Nachrichten verschickt werden (Offline, OutOfPaper, etc.). Letztlich kann diese einfache Form der Signalisierung auch zum „Personenruf“ benutzt werden. Für umfangreichere Nachrichten eignet sich SEND jedoch nicht, da die Datenmenge auf 65 Zeichen beschränkt ist.

## 7.7 WIN.COM

WIN.COM ist das Laderprogramm für Windows. Es wird beim SETUP von Windows aus den Dateien WIN.SRC, einer LOGO-Datei und einer Steuerdatei zusammenkopiert. Dies kann auch manuell erfolgen.

Der Programcode ist in WIN.COM unabhängig von der Auflösung immer gleich. Einzig das Startbild, welches in WIN.COM mit hinterlegt ist, ist je nach Auflösung unterschiedlich. Da zu dieser frühen Startzeit von Windows noch keine Grafiktreiber aktiv sind, kann WIN.COM nur die Standardauflösungen nutzen (CGA, EGA, VGA und Hercules). Damit erklärt sich auch, warum die WIN.COM für höhere Auflösungen immer gleich ist. Daher ist es in einem großen Netzwerk ausreichend, eine WIN.COM für VGA vorzuhalten und diese bei Start von Windows zum Benutzer zu kopieren.

## 7.8 Windows Startbild

Das vorgegebene Startbild von Windows kann geändert werden. Dazu muß man mit einem Editor (z.B. PaintBrush) ein Bild erzeugen, welches im RLE-Format abgespeichert wird. Die Auflösung darf dabei 640x480 bei 16 Farben nicht überschreiten. Grafikkonverter wie PaintShow oder GrafticWorkShow erlauben es, gängige Bildformate in RLE umzuwandeln.

Mit dem Befehl COPY verbindet man die Datei WIN.SRC, WIN.LGO und das RLE-Bild zu einem WIN.COM

```
COPY /B win.src + win.lgo + logo.rle win.com
```

Werden Auflösungen kleiner als VGA eingesetzt, dann muß man diesen Vorgang mit anderen LGO-Dateien wiederholen. Zudem muß man dann wieder die „richtige“ WIN.COM beikopieren für diese niederen Auflösungen.

## 7.9 WIN.INI und Programme

Bei der Installation neuer Software hat man als Administrator besonders darauf zu achten, welche INI-Dateien das Programm anlegt und welche Einträge es in der WIN.INI verändert. Diese Daten müssen später per INIPATCH zum Start bei allen anderen Benutzern nachgetragen werden, sofern man nicht gleich die komplette WIN.INI kopiert.

## 7.10 REG.DAT und Programme

Durch OLE und anderer Mechanismen reicht es nicht mehr, allein die Einträge in der WIN.INI zu pflegen. Fast jede Applikation trägt mittlerweile Daten in die REG.DAT ein. Diese Datei kann nicht einfach modifiziert werden. Unter Windows hilft das Programm REGEDIT bei der Bearbeitung. Da die wenigsten Benutzer die REG.DAT etwas verändern dürften, kann man die REG.DAT zentral pflegen und beim Start dem Benutzer überkopieren. Umständlicher wird dies, wenn ein Benutzer eigene Programme z.B. auf einer lokalen Festplatte nutzt und damit diese Einträge verloren gehen würden. Hier bleibt uns nichts anderes übrig, als die Pflege seiner INI-Dateien dem Benutzer selbst zu überlassen (LEVEL = 2), selbst diese Änderungen vorzunehmen oder komplett die Unterstützung lokaler Platten einzuschränken.

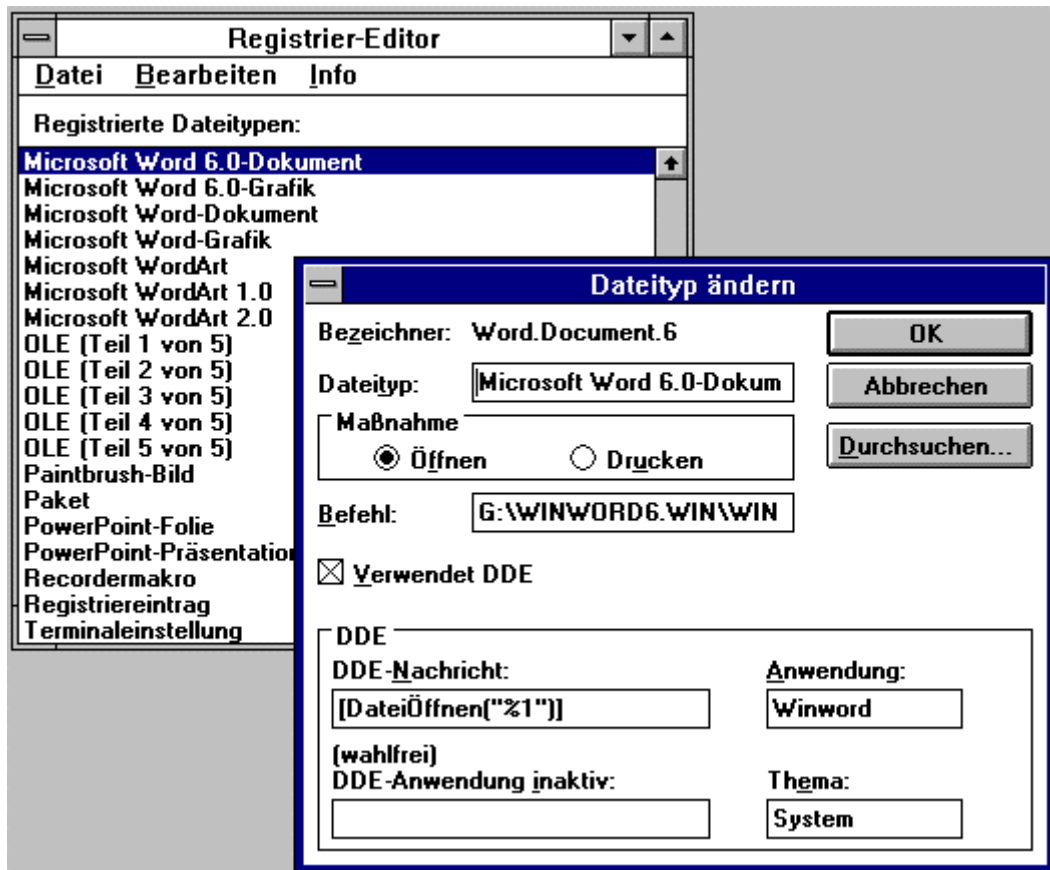


Abbildung 11 Regedit

### 7.11 Userlevel

Im Netzwerk wird für jeden Benutzer ein Userlevel vergeben. Abhängig von diesem Level können in Batchjobs dann mehr oder minder umfangreiche Aktionen laufen. Bei Windows ist diese Level stark eingesetzt. Level 0 bedeutet, daß der Benutzer beim neuen Start von Windows alle INI-Dateien etc neu kopiert bekommt. Dies verursacht Anfangs etwas Last auf dem LAN und schränkt die persönliche Freiheit des Benutzers kräftig ein, sichert jedoch die Funktion.

### 7.12 WIN31.BAT

Der komplette Abdruck des Batches würde hier zu schnell veralten. Daher ist es besser, direkt den Batch zu analysieren, um die funktionsweise zu bestimmen. Um jedoch den Einstieg zu erleichtern, soll hier als Blockbild der Aufbau des Batches anhand einige „Schlüsselzeilen“ aufgezeigt werden. Der WIN31.BAT ist immer gewisser Veränderungen und Anpassungen unterworfen, so daß hier nur grob der Aufbau beschrieben werden kann.

### 7.13 INI-Patcher

Bei Windows dreht sich alles um INI-Dateien. Leider sind die Gruppdateien (\*.GRP) und die Registrierdatenbank (REG.DAT) nicht als ASCII-Datei änderbar. Setzt man Windows im LAN ein und besteht der Anspruch, dem Benutzer die freie Wahl des Endgerätes einzuräumen (dies erleichtert nebenbei den „Umzug“ in Gebäuden oder Hardwareaustausch und die Fehlersuche) dann ist es notwendig, bestimmte Einträge in den INI-Dateien zu pflegen.

Es gibt mittlerweile viele Programme zur Pflege von INI-Dateien. Die meisten arbeiten mit Kommandozeilen, so daß für jede Änderung das Programm gestartet werden muß. Die erzeugt viel Netzwerkklast, kostet Performance und ist zudem schlecht zu pflegen. Besser sind Programme, welche eine „Befehlsdatei“ abarbeiten. Ich setze aktuell MAINTINI ein. Es ist auf CompuServe zu erhalten und ist kostenfrei. Der Autor erwartet lediglich, daß ihm eine E-Mail geschickt wird (E-Mailware).

**Konfigurationsdatei 13 WIN31.BAT****Kontrolle ob die Grafikkartenkonfiguration existiert.**

```
if exist G:\WIN31\%VIDEO%.cfg\WIN.COM goto win31cfg
```

**Prüfen auf Verzeichnisse (Systemverzeichnis, Win31verzeichnis, diverse Programmverzeichnisse, Abfallverzeichnis, Vorlagenverzeichnis)**

```
if exist H:\SYSTEM\SYSTEM.FLG goto systemda
```

**Prüfen auf Erstinstallation**

```
if exist h:\system\win31\win.ini goto copyvorlagen
echo Erstinstallation Windows 3.1 Moment bitte ...
```

**Kopieren der Vorlagendateien**

```
if not exist H:\VORLAGEN\NORMAL.DOT copy G:\WINWORD2.WIN\VORLAGEN\*. * H:\VORLAGEN\*. * >nul:
```

**Kopieren der PC Konfigurationsdateien**

```
copy G:\WIN31\%VIDEO%.CFG\*. * H:\SYSTEM\WIN31 >nul:
```

**Aufbau PROGMAN.INI und Kopieren der Programmgruppen**

```
copy G:\WIN31\INI\NETZWERK.GRP h:\SYSTEM\WIN31\NETZWERK.GRP >nul:
copy G:\WIN31\INI\AUTOSTAR.GRP H:\SYSTEM\WIN31\AUTOSTAR.GRP >nul:
```

**Kopieren der INI-Dateien, abhängig vom Level**

```
if not %LEVEL%==0 goto noinicopy
echo In I
copy G:\WIN31\INI\*.ini H:\SYSTEM\WIN31\*.ini >nul:
copy G:\WIN31\INI\reg.dat H:\SYSTEM\WIN31\reg.dat >nul:
copy G:\WIN31\INI\HGW.INI H:\SYSTEM\WIN31\HGW.INI >nul:
```

**INIs- ändern**

```
echo In INI
G:\INIPATCH\MAINTINI H:\SYSTEM\WIN31\SYSTEM.INI SYSINI.CMD
G:\INIPATCH\MAINTINI H:\SYSTEM\WIN31\WIN.INI WININI.CMD
G:\INIPATCH\MAINTINI H:\SYSTEM\WIN31\WINFILE.INI WFILEINI.CMD
```

**Start von Windows**

```
echo In %VIDEO%
H:\SYSTEM\WIN31\win.com %1 %2 %3
goto WIN31END
```

**„Ausräumarbeiten“**

```
if exist H:\SYSTEM\WIN31\WIN.COM del H:\SYSTEM\WIN31\WIN.COM >nul:
if exist H:\SYSTEM\WIN31\SYSTEM.INI del H:\SYSTEM\WIN31\SYSTEM.INI >nul:
```

**Abschlußmeldung und Hilfestellung**

```
echo Windows 3.1 beendet
echo .
echo Sie haben Windows 3.1 verlassen. Um wieder zu ihrer normalen Umgebung
echo zurückkommen brauchen Sie nur "WIN31" einzugeben und Enter drücken.
echo Als letztes Mittel können Sie den Computer einfach ausschalten und
echo nach 10 Sekunden wieder einschalten.
```

**7.14 Suchpfade**

Auch wenn jede Windowsapplikation behauptet, sie müsse einen Suchpfad in die AUTOEXEC.BAT eintragen, so kommen jedoch fast alle OHNE Suchpfad aus. Dazu muß man jedoch einige Nacharbeiten machen. Alle Verweise auf die Anwendung (Icon, WIN.INI u.s.w) müssen explizit ausgeschrieben werden.

Die Namen der Drucker kann man mit einem einfachen ASCII-Editor ändern, d.h. man muß nicht die Vorgaben von Windows benutzen, sondern kann den Druckernamen für die Benutzer verständlich ändern. Viele Drucker sind z.B. HP-II- oder Epson-FX-kompatibel, aber haben ein anderes Etikett.

Applikationen unter Windows benutzen teilweise die gleichen INI-Dateien wie Windows.

Einige Einträge sind in der WIN.INI nötig, z.B. damit der Dateimanager weiß, welche Erweiterung zu welchem Programm gehört. Weiterhin werden in der Win.INI Schriften installiert.

Offiziell soll jedes Programm seine eigene INI-Datei anlegen, da die INI-Dateien auf 64kByte begrenzt sind und auch sonst schwer zu pflegen sind. Excel und Powerpoint haltensich daran

### 7.15 Neue Programme einbinden

Da die Gruppe NETZWERK zentral gepflegt wird, reicht es, das Icon für das entsprechende Programm dort einzubinden. Die Rechte und Netzwerkeinstellungen entsprechen der Installation eines Programmes unter DOS. Oder das Programm wird in der GRPPATCH.INI eingetragen, damit das Icon beim Start dynamisch eingepatcht wird.

Alternativ kann man das entsprechende Icon einer Gruppenvorlage beifügen, welche beim Start von Windows anhand des WIN31.BAT zukopiert wird

Bei Windows muß man nun nur noch beachten, wo das Programm selbst seine Konfigurationen ablegt. Benutzt das Programm eine eigene INI-Datei, welche im Verzeichnis der WIN.IN liegt, so muß man einmalig diese INI-Datei zum Benutzer kopieren. Dies kann z.B. im WIN31.BAT erfolgen, wo die Konfiguration überprüft wird. Hält sich das Programm allerdings nicht an die Vorgabe von Microsoft und legt seine Daten in der WIN.INI ab, muß man abwägen, was man den Benutzern zumutet. Die zusätzlichen Einträge müssen irgendwie in die WIN.INI der Benutzer hinein. Von Windows selbst gibt es kein Hilfsmittel, um INI-Dateien zu verbinden. Man kann einmalig diese Daten mit TYPE programm.ini >>WIN.INI anhängen. Meist macht dies ein Workstationsetup, welches der User einmal aufrufen könnte.

### 7.16 Neue Gruppe einbinden

Eine neue Gruppe bindet man einfach ein, indem man diese Gruppe erstellt und alle PROGMAN.000 bis Progman.016 ändert. Zudem müssen die Einträge der Gruppen für die bestimmten Benutzer in der USERCFG.BAT eingetragen werden. Allerdings ist zu überlegen, ob man überhaupt mehrere Gruppen zuläßt. Mehr Gruppen bedeuten gleichzeitig mehr Fenster und mehr Ressourcenverbrauch. Zudem läßt es den Bildschirm voller und komplexer erscheinen.

Aus dem WIN31.BAT ist zu ersehen, daß je nach Anzahl der Gruppen (Umgebungsvariable GROUP1 - GROUP4) eine andere vorbereitete PROGMAN.INI zukopiert wird.

### 7.17 Private Gruppe

Mit Windows kann sich jeder Benutzer selbst Gruppen einrichten und ändern. Es liegt im Ermessen des Administrators, dies zuzulassen oder nicht. Dafür die Variable LEVEL vorgesehen. Sie kann im WIN31.BAT ausgewertet werden. Verzichtet man komplett auf das Kopieren der INI-Dateien und Gruppen (\*.GRP) dann kann der Benutzer seine Umgebung selbst zusammenstellen. Dies hat natürlich einen erhöhten Schulungsaufwand zu Folge und der Benutzer kann sich seine Einstellungen bis zu Unbrauchbarkeit zerstören. Ein komplettes Kopieren (LEVEL=0) sichert die Funktion, jedoch kann der Benutzer nicht mal die Farben seines Desktops ändern. Für private Gruppen gibt es eine Zwischenlösung. Wenn anhand des Levels der Benutzer eine private Gruppe haben darf und diese auch existiert (PRIVAT.GRP), dann wird die kopierte PROGMAN.INI um den Eintrag für die private Gruppe ergänzt.

### 7.18 Screensaver einrichten

Um einen Screensaver für ALLE Benutzer des LAN's zu aktivieren müssen folgende Dateien geändert werden: Wenn diese Dateien beim Start nicht automatisch kopiert werden, können die Benutzer mit der Systemsteuerung dies auch selbst einstellen. (Am Beispiel Mystify)

#### WIN.INI

```
[windows]
ScreenSaveActive=1
ScreenSaveTimeOut=60
```

Die WIN.INI wird z.Z. bei jedem Neustart von Windows 3.1 neu zum Benutzer kopiert, d.h. heißt es muß nur die WIN.INI im Verzeichnis G:\WIN31\INI geändert werden.

#### SYSTEM.INI

```
[boot]
SCRNSAVE . EXE=V:\SSMYST . SCR
```

Die SYSTEM.INI liegt für jede Bildschirmkonfiguration getrennt im passenden Verzeichnis G:\WIN31\%VIDEO%.CFG. Daher müssen ALLE SYSTE.INI's um den Eintrag erweitert werden. Die SYSTEM.INI wird beim Start von Windows zum Benutzer kopiert.

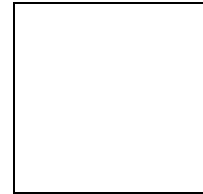
**CONTROL.INI**

```
[Screen Saver.Mystify]
Clear Screen=1
PWProtected=0
Active1=1
WalkRandom1=1
Lines1=5
StartColor1=0 0 0
EndColor1=255 255 255
Active2=1
WalkRandom2=1
Lines2=5
StartColor2=0 0 0
EndColor2=255 255 255
```

Die CONTROL.INI wird z.Z. beim Start von Windows zu jedem Benutzer kopiert und muß daher nur in G:\WIN31\INI geändert werden.

Per Standard ist ein einfacher Screensaver eingerichtet. Ziel eines Screensaver ist es, ein Einbrennen des Bildschirms durch ein lange unverändertes Bild zu verhindern. Zweiter Nutzen ist, daß Informationen auf dem Bildschirm nicht sofort sichtbar sind. Ein Bildschirmschoner kann zusätzlich mit einem Passwort versehen werden. Dies ist jedoch bei den Schonern von Windows unabhängig von Windows und wird in der CONTROL.INI abgelegt. Da bei LEVEL = 0 auch diese INI-Datei kopiert wird, ist es dem Benutzer damit nicht möglich, selbst ein Passwort zu vergeben. Die Vergabe eines Passwortes und das Vergessen desselben verhindert, daß die angefangene Arbeit vortgesetzt, respektive gespeichert, wird.

## 8 Lizenzen



Das Thema der Lizenzkontrolle in Netzwerken ist immer ein heißes Eisen. Die meiste Standardsoftware enthält keinen eingebauten Schutz. Manche Pakete (z.B. WORD) lassen sich nicht mal Kopierschützen mit dem Execute-only-Flag, da Overlaydaten im EXE-File gelesen werden. Das Execute-only-Flag verhindert leider auch, Programme von Windows aus zu starten, da Windows vermutlich versucht, die Datei einzulesen und dabei nicht die Funktionen zum Start von Programmen benutzt. Damit kann die Shell nicht erkennen, daß die Ausführung des Programmes gewünscht wird und verhindert den Lesezugriff.

Es gibt mehrere denkbare Ansätze:

Man kann nun auf dem Standpunkt stehen, und sagen: "Wenn das Programm es nicht überprüft, ich kann es nicht, also ist es nicht mein Problem". Damit dürfte sich aber keine Softwarefirma zufrieden geben, und die Gerichte wohl auch nicht.

- Oder** man schätzt die Anzahl der maximal gleichzeitig eingesetzten Lizenzen und kauft diese Anzahl. Nun verläßt man sich auf seine Schätzung und versucht so einen Mittelweg zwischen zuwenig (=unlizenziert) und der vollen Menge (= keine Kosteneinsparung) zu finden.
- Oder** es erhalten nur die Benutzer Zugriffsrechte für Anwendungsprogramme, die eine Netzlizenz beschafft haben, z.B. eine Lizenz bezahlt haben. Die Anwendung würde nur unter bestimmten Benutzernamen laufen (personengebunden; „Member of“ Anwendungsgruppe). Damit erreicht man eine 100%ige Kontrolle aber hat keinen Einsparungseffekt für Lizenzen, da theoretisch die volle Lizenzzahl vorhanden sein müßte.
- Oder** der Server führt für jede Anwendung einen internen Zähler, der die aktiven Benutzer der Anwendungen überprüft. Sollte der Zähler die angeschafften Lizenzen erreichen, kann kein weiterer Benutzer die Anwendung starten. Der Zähler kann auch abteilungsgebunden sein, damit abteilungsübergreifend keine Konkurrenz besteht. Die Zähler könnten als Teil der Bindery implementiert werden. Allerdings muß das im Server verwaltet werden. Wer stellt sicher, daß die User dann wirklich mit dem Programm arbeiten und nicht nur morgens das Programm starten, um es den ganzen Tag dann zu haben ?. Die ist keine Funktion des Fileservers, jedoh gibt es Zusatzprodukte (z.B. Sitelock.NLM), welche solch eine Kontrolle erlauben.
- Oder** die Software kontrolliert selbst. Der sauberste Weg. Dies kann dadurch geschehen, daß die Software eine Lockdatei öffnet und dann den "Open-count" liest. So kann Sie leicht herausfinden, wie oft die Applikation schon läuft (Dosfunktion SHARE). Überprüft werden muß aber auch, wenn ein Benutzer die gleiche Anwendung mehrmals startet (DeskView oder Windows). Wenn ein Benutzer seinen PC ohne Ausloggen einfach abschaltet ist die Lizenz gesperrt, bis sich an diesem PC ein neuer User anmeldet oder der Server die connection löscht. Weiterhin bleibt zu klären, wie man die Anzahl der Lizenzen hier einspielt. Manche Programme erwarten das Einspielen von "Workstationdisketten", welche dann eine Lizenz hinzuaddieren (z.B. Open Access III). Andere Programme haben ein eigenes Setup-programm dabei, mit welchem der Administrator die Lizenzzahl einstellt.

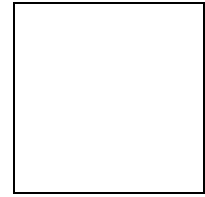
Letztlich bleibt es dem jeweiligen Netzwerkverantwortlichen überlassen, für welche Variante er sich entscheidet. Auf jeden Fall ist davon abzuraten, eine Kontrolle durch Drittprodukte auf dem Server selbst auszuführen, welche beim Erreichen des Limits den Zugriff verwehren. Dies wird sicher den laufenden Betrieb stören und zu mehr Verärgerung führen. Trotzdem tut eine Lizenzkontrolle Not. Allerdings könnte man sich damit begnügen, daß ein Programm selbst oder ein Überwachungstool eine Überschreitung der Lizenzen einfach meldet und somit eine Nachbeschaffung oder Nutzereinschränkung erfolgen kann.

Entsprechende Software zum „Zählen“ der aktiven Benutzer ist verfügbar. Stichproben kann der Operator am Fileserver mit MONITOR.NLM selbst ausführen. Auch DOS-Programme können einen „FileOpenCount“ ermitteln und entweder zur Auswertung notierschreiben oder bei Überschreitung einer Grenze eine Meldung veranlassen.

Hierbei bleibt das Problem bestehen, daß keine „dauernde“ Kontrolle möglich ist, d.h. immer nur Stichproben möglich sind (z.B. Minutentakt) und damit die Kontrolle nicht lückenlos möglich ist. Zudem gibt es noch das Problem, daß man eine Datei finden muß, welche von der Anwendung auch dauernd offen gehalten wird. Dies ist schon eher das Problem, da nicht alle Programme eine Datei offen halten. Zwar findet sich immer ein Overlay oder EXE-File, welches die Anwendung nutzt, aber sogar bei Windows selbst gibt es keine gemeinsam benutzte Datei, die „garantiert“ von allen Windowsbenutzern geöffnet ist. Mögliche Dateien sind hier z.B. Schriften oder GDI.EXE. Diese Problematik tritt aber bei allen „Kontroll“-Programmen auf.



## 9 Backup



Auch wenn man den Fileserver mit großem Aufwand absichert, ist ein regelmäßiges Backup nötig. Dadurch kann man Kopien der Daten an einem anderen Ort aufbewahren und auch nach einem Brand oder Diebstahl die Daten wieder aufbauen. Zudem kann man so versehentlich gelöschte Dateien wieder zurückholen wenn man mehrere Generationen anlegt.

Das Backup sollte so ausgelegt sein, daß eine Vollsicherung ohne Anwesenheit eines Administrators möglich ist, d.h. die kompletten Daten müssen auf ein Band passen oder ein automatischer Wechsel muß möglich sein. Zudem sollte ein Backup über Nacht ausführbar sein um keine Benutzer zu stören und sicher alle Daten zu bekommen. Man sollte mit dem Backup nie Bänder überschreiben, welche erst NACH dem Backup als "benutzbar" gelten. Denn auch mitten beim Backup kann ein Abbruch erfolgen.

Das Backup muß auch Dateien sichern können, welche der Fileserver im Betrieb geöffnet hält (NetWare: Bindery). Dazu muß die Backupsoftware die Funktionen ausführen können, um diese Dateien zu entsperren). Weiterhin müssen die erweiterten Flags der Dateien und Verzeichnisse und die Rechte auf Verzeichnisse und Dateien mitgesichert werden. Speziell beim Einsatz von weiteren "name spaces" wie OS/2, NFS oder MAC, muß die Backupsoftware auch diese Informationen sichern und wiederherstellen können.

Besondere Beachtung verdienen Dateien, welche von Applikationen geöffnet sind und daher nicht mitgesichert werden könnten. (z.B. Maildatenbanken). Um sicher zu gehen, daß alle Dateien gesichert werden können ist es ratsam, daß zu dieser Zeit niemand sonst angemeldet ist. Die Gateways kann man rechtzeitig dazu herunterfahren. Benutzer, welche sich nicht daran halten, müssen damit rechnen, daß nicht alle Dateien gesichert sind.

Beim Backup und Restore muß auch alles vorbereitet sein, um im Falle eines Falles schnell ein Restore durchführen zu können. Dazu gehört auch, sich Gedanken zu machen, welche Vorarbeiten (Servergenerierung, Treiber laden) nötig sind, bevor das eigentliche Restore ablaufen kann. Dazu sollte die Backupmaschine ohne Server booten können, bzw beim Einbau im Server die Disketten für einen "Schnellstart" bereit liegen.

Beim Backup unterscheidet man ein "Volles Backup" und ein "Teilbackup". Am Anfang steht immer ein volles Backup. Wenn das Backup nur kurze Zeit braucht, bzw die Belastung durch ein volles Backup nicht stört, ist immer ein volles Backup anzuraten.

Ein Teilbackup sichert meist nur die seit dem letzten Backup veränderten Dateien. Es ist damit schneller fertig. Allerdings muß bei einem Totalausfall der letzte Status anhand des letzten vollen Backups und der darauf erfolgten Teilbackups wiederhergestellt werden. Dies kostet mehr Zeit.

Um die Funktion sicherzustellen, sollten Jobs vergewertigt werden, welche immer das Backup ausführen ohne daß der Administrator manuell Dateien auswählen oder Optionen setzen muß. So werden auch Fehlbedienungen unterbunden bzw. man kann Aufgaben delegieren.

In einem Netzwerk gibt es zwei Orte, von denen aus ein Backup durchgeführt werden kann.

### **9.1 Workstationbased Backup**

Das Backupdevice ist in einer Workstation eingebaut. Damit werden alle Daten vom Server über das Netzwerk gesichert. Damit die Daten gesichert werden können, muß der PC angemeldet sein. Um wirklich alle Daten zu sichern, sind Supervisorrechte nötig. Daher müssen geeignete Sicherungsmaßnahmen ergriffen werden, damit während des Backups kein unauthorisierter Benutzer eindringen kann. Nachteilig wirkt sich die Datenübertragung über das Netzwerk aus. Das Backup von einer Workstation heraus hat den Vorteil, daß überhaupt nicht am Fileserver gearbeitet werden muß und damit einige Fehler ausgeschlossen werden. Zudem können problemlos mehrere Server gesichert werden. Ein Restore kann man einfach ausprobieren, indem man sich ein kleines Netzwerk mit dem Backup-PC und einem Test-Server aufbaut. Auch der Austausch des Backupdevice kann erfolgen, ohne daß der Fileserver angerührt wird. Beim Workstationbased-backup können die LOG-Files und

Indexfiles auf der lokalen Festplatte der Workstation liegen, so daß auf diese auch bei einem Totalausfall des Fileservers zugegriffen werden kann.

## 9.2 Serverbased Backup

Das Backupdevice ist im Server eingebaut. Die Daten werden nicht über das Netzwerk übertragen. Das Backupprogramm ist ein Modul, welches auf dem Server läuft. Damit wird der "Engpaß" Netzwerk umgangen. Jedoch muß man am Server selbst arbeiten. Wenn mehrere Server zu sichern sind, dann wird die Rechenleistung des Servers mit dem Backupdevice benutzt und die Daten gehen trotzdem über das Netzwerk. Von diesem Standpunkt eignet sich ein Backup im Server nur für kleine Netzwerke mit einem Server und geringer Last. Sollte der Server durch einen Defekt ausfallen, oder ein Ausfall vorhersehbar sein, dann muß erst das Backupdevice ausgebaut werden, um einen Ersatzserver aufzubauen. Ein anderes Problem ist die Vorarbeit, um ein Restore auf einen "leeren" Server durchzuführen. Das Serverbased-backup legt normalerweise auch seine LOG-Files und Indizes auf dem Server ab, welche beim Crash nicht mehr erreichbar sind.

## 9.3 Backupmedien

Es gibt mehrere Speichermedien, um Backupdaten abzulegen. Die meist verwendete ist die Speicherung der Daten auf Magnetbändern. Neben den aus Filmen bekannten Magnetbandrollen kommen bei PC-Netzwerken hauptsächlich QIC-Tapes oder neuerdings DAT-Bänder zum Einsatz. Sie unterscheiden sich in der Speicherkapazität, im Anschaffungspreis und der Geschwindigkeit. Alternativ kann man auch Daten auf magnetooptisch Laufwerke (MO) sichern. Diese haben den Vorteil, gegen magnetisch Einflüsse resistent zu sein. Sonderfälle sind die Datensicherung auf Disketten oder auf sogenannte "Floppystreamer", welche sich aber im Netzwerkbereich als unpraktisch oder nicht leistungstark genug erweisen, für lokale Workstations jedoch eine preiswerte Alternative sind, solange die Arbeitszeit nicht gerechnet wird. Für welches Medium man sich entscheidet, hängt hauptsächlich von Datensicherungsaufkommen ab.

QIC-Bänder speichern zwischen 100MB bis zu 525 MB. DAT-Tape sichern ca 2GB und bei Kompression mit geeigneten Daten bis zu 8 GB auf einem Band. Für größere Datenmengen kommen automatische Wechsler in Betracht. MO-Laufwerke speichern zwischen 280 MB und 600 MB.

## 9.4 Laufwerkswechsel

Zu beachten ist, daß generell der Austausch der Bänder zwischen verschiedenen Laufwerken nicht immer reibungslos möglich ist. Da die Schreib/Lese-Köpfe nie genau gleich justiert sind, ist ein Restore auf einem anderen Laufwerk nicht garantiert. Davon sind auch DAT-Laufwerke nicht ausgenommen, selbst wenn sie von dem gleichen Hersteller aus der gleichen Serie stammen.

## 9.5 Komprimierung

Mittlerweile gibt es Bandlaufwerke welche selbst die Daten noch komprimieren. Damit werden über die physikalische Eigenschaften zusätzlich Speicherplatz angegeben. Oft wird ein „echtes“ 2GB-Laufwerk als „8GB“-Laufwerk bezeichnet, weil bei günstigen Ausgangsdaten wirklich bis zu 8 GB auf das Band passen können. Dies ist besonders bei Bildern oder Datenbanken möglich. Teilweise sind Programme selbst schon komprimiert, so daß hier keine weitere Komprimierung möglich ist. Zudem gibt es schon Backupsoftware, welche auch Daten komprimieren kann.

Letztlich muß man selbst sehen, welches Daten gesichert werden und inwieweit diese komprimierbar sind. Neben den optimalen Kompressionswerten von bis zu 1:4 hat sich in der Praxis gezeigt, daß in der Regel maximal 1:2 angewendet werden kann. Eher weniger.

## 9.6 Mitteilung an Benutzer

Wenn die Möglichkeit besteht, daß Benutzer auch während der Backupzeiten an ihrem Gerät arbeiten, so ist es empfehlenswert, diese von dem Backup und dessen Auswirkungen (Performance) zu unterrichten. z.B. mit folgender Mitteilung (als E-Mail oder als Beiblatt zum Netzwerk)

Täglich ab 23:00 Uhr läuft automatisiert ein Backup, d.h. wenn Benutzer zu dieser nachtschlafenden Zeit noch arbeiten, können die dadurch geöffneten Daten nicht mitgesichert werden. Zu dieser Zeit wird auch die Antwortzeit des Servers grösser, da sehr grosse Datenmengen von den Festplatten auf ein DAT-Band gesichert werden.  
Ich bitte sie daher, jeden Abend sich aus dem Netzwerk auszuloggen und den PC abzuschalten, auch wenn es einfacher ist, das Gerät und den aktuellen Bildschirm über Nacht laufen zu lassen. Bedenken Sie aber, dass damit jeder, der an ihren PC kommt (und sei es nur die Putzkolonne) Zugriff auf all ihre Daten hat, solange sie eingeloggt sind.  
Es zählt nicht zu den edlen Gepflogenheiten, nur das Gerät auszuschalten. Zwar bewirkt das (fast) das gleiche, dass sie nämlich nach 15 Minuten als ausgeloggt betrachtet werden, aber dabei bleiben immer einige Dateileichen (sogenannte temporäre Dateien, Sicherheitskopien der Anwendungen) zurück. Diese werden nicht automatisch gelöscht, da man damit nach einem Stromausfall oft wieder Daten herstellen kann. Belegen aber unnütz Speicherplatz.

Natürlich bleibt es jedem Administrator selbst überlassen, die Benutzer zu informieren.

## 9.7 Lokale Festplatten der Workstations am Netzwerk

Die lokalen Arbeitsstationen werden bei einem Serverbackup nicht automatisch mitgesichert. Es bleibt den Benutzern überlassen, die Daten ihrer lokalen Festplatten am Ende des Tages auf den Fileserver zu kopieren, um die Daten damit mitsichern zu lassen. Dies bedeutet jedoch, daß auf dem Server ausreichend Platz ist und die zusätzliche Belastung möglich ist. Eine bessere Lösung ist der Einsatz eines Clientrequestors, damit das Backupprogramm direkt über das LAN mit der Workstation kommuniziert und die Daten sichert. Damit gehen die Daten nur einmal über das LAN und belasten nicht den Server. Allerdings sollte man beim Einsatz eines LANs nicht überlegen inwieweit zumindest die Benutzerdaten generell auf dem Server abgelegt werden, damit diese nicht nur durch ein Backup gesichert sind, sondern auch gegen fremde Zugriffe geschützt sind.

Ziel ist bei einem LAN, so wenig wie möglich Daten und Programme lokal zu halten. Ausgenommen davon ist Spezialsoftware, welche auf den betroffenen PCs gestartet wird (z.B. Modemsoftware für Bankabfragen und Programme, welche nicht sicher ins Netzwerk portiert werden können. Alle sonstigen Dateien liegen in der Regel zentral auf dem Server und werden auf jeden Fall immer mitgesichert.

## 9.8 Backupabfolge

Dies ist ein Beispiel für eine Backupstrategie. Sie ist nicht zwingend. Diese Strategie gewährleistet, daß die Daten von zwei Wochen schnell zurückgeholt werden können. Zudem bringt der „rotierende Freitag“ eine historische Sicherung, so daß auch noch Monate danach einzelne Dateien wiederhergestellt werden können. Somit lassen sich auch „versehentliche“ Löschungen über längere Zeit wiederherstellen.

Um keine benutzen Bänder zu überschreiben sind zwei volle Sätze für das "Full Backup" nötig.

Die Bänder werden wie folgt benannt:

T1..T4 für das täglich "full backup" von Montag bis Donnerstag

F2..F5 für das "full backup" an den 2.-5. Freitagen des Monats

M1..M3 für das "full backup" an dem jeweils ersten Freitag im Monat

Damit rotieren die Bänder T1 bis T4 jede Woche, Die Bänder F1-F4 jeden Monat und die Bänder M1-M3 jedes Quartal. Somit ist sichergestellt, daß man bis zu drei Monate rückwärts Daten zurückholen kann. Somit lassen sich irrtümlich gelöschte Daten wieder zurückholen. Zudem hat man einige Bänder, welche geringerem Verschleiß unterliegen und seltener eingesetzt werden. Damit kann man diese Bänder an einem anderen Ort lagern (Safe, Bank etc). Die Bänder T1-T4 sind regelmäßig in Gebrauch und sollten nach ca 100 Durchläufen (= 2 Jahre !) ersetzt werden.

Sind die Daten so umfangreich, daß man nicht jeden Tag ein "FULL Backup" machen will, so kann man die Bänder T1-T4 als Teilbackup (Incremental) benutzen.

Es steht jedem frei, zusätzliche Bänder am Freitag einzufügen und damit den „Kreis“ zu vergrößern oder einzelne Bänder am Freitag aus dem Kreislauf rauszuziehen und extern längerfristig zu lagern.

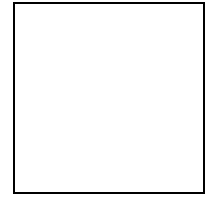
Tabelle 1 Backupbänder

Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
T1	T2	T3	T4	M1	-	-
T1	T2	T3	T4	F2	-	-
T1	T2	T3	T4	F3	-	-
T1	T2	T3	T4	F4	-	-
T1	T2	T3	T4	F5 oder M2	-	-

### 9.9 USER.BAT des Users BACKUP

In dieser Batchdatei sollte die Backupprozedur automatisch gestartet werden. Hier ist auch eine Pause bis zu einem bestimmten Zeitpunkt denkbar, damit das Backup nachts abläuft. Nach dem Backup sollte der PC sich selbst abmelden, damit diese „Hintertür“ geschlossen wird. Das Backup muß „unbeobachtet“ ablaufen, d.h. selbst Hindernisse wie nicht formatierte Bänder oder schon bespielte Bänder dürfen nicht zu einer Unterbrechung führen. Rückmeldungen oder Logbücher könnten per Mail an den ADMIN geschickt werden.

## 10 Drucken



Neben der Möglichkeit Programme zu sharen, ist die Möglichkeit der effektiven Druckernutzung ein großes Argument, ein Netzwerk einzusetzen. Im Gegensatz zum lokal angeschlossenen Drucker sind bei Netzwerkdruckern einige Punkte zu beachten.

Der Netzwerkserver kann die Druckdaten zwischenbuffern und danach dem Drucker zuleiten. Dadurch wird die Workstation entlastet, bzw. früher wieder benutzbar. Teure, schnelle oder besondere Drucker können einfach von mehreren Personen benutzt werden. Druckerumschalter bzw. komplette Drucker werden eingespart. Mehrere Benutzer eines Druckers müssen sich nicht mehr absprechen, wer den Drucker "bekommt".

Diese neuen Möglichkeiten fordern aber auch eine durchdachte Planung, Installation und Betreuung der Benutzer, die doch umlernen müssen.

Eigentlich sollte diese Kapitel besser mit AUSGABE betitelt sein. Drucken ist nur eine Form der Ausgabe von Anwenderdaten. Neben der Ausgabe auf Papier kann man auch die Ausgabe auf ein FAX, Telex, Teletex und E-Mail mit den gleichen Methoden abbilden.

### **10.1 Die Problematik**

Beim Drucken im Netzwerk gilt es, mehrere Zuweisungen zu setzen:

- Druckertreiber der Applikation
- Parallele Schnittstelle
- Queue

Diese drei Punkte können von dem Benutzer beeinflusst werden. Damit später auf dem Papier das gewünschte Ergebnis gedruckt wird, müssen alle drei Punkte zusammenpassen. Der Administrator ist hier gefordert, entweder geeignete Hilfprogramme anzubieten, Anleitungen zu verbreiten oder die Druckerumleitungen soweit voreinzustellen, damit die Benutzer ihr gewünschtes Ergebnis erhalten und damit auch wenig Nachragen an den Administrator kommen.

Die Anwendung druckt die Daten über den Druckertreiber an eine DOS-Schnittstelle. Diese Ausgaben werden von der Netzwerksoftware (NETX) abgefangen und in eine Druckwarteschlange umgeleitet. Nachdem der Druckjob in der Warteschlange angekommen ist, durchlaufen die Daten noch einige weitere Stationen, bis der Drucker in Aktion treten kann. Die Installation und Funktionsüberprüfung dieser Komponenten kann der Benutzer nicht selbst ändern und fallen damit in den Bereich des Administrators.

Durch folgende Stationen laufen die Daten:

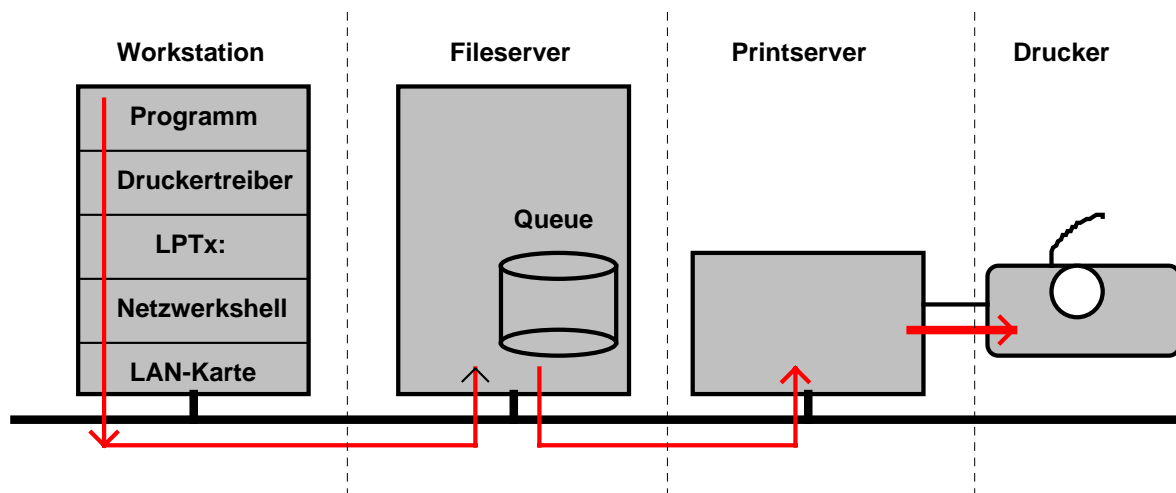


Abbildung 12 Stationen eines Ausdrucks

Applikation ⇒ Druckertreiber ⇒ LPTx ⇒ Netzwerkshell ⇒ Queue ⇒ Printserver ⇒ (Rprinter) ⇒ Drucker

## 10.2 Der Druckertreiber

In welcher Form die Daten auf die Schnittstelle ausgegeben werden, bestimmt der Treiber. Der Druckertreiber legt die Leistungen des Druckers fest, über die die Applikation verfügen kann und setzt die Ausgabedaten in ein für den Drucker verständliches Format um. Wenn der Drucker gewechselt wird, ist normalerweise auch ein Wechsel des Druckertreibers nötig.

## 10.3 Die Schnittstelle LPT1-3

Jede Applikation druckt auf eine Schnittstelle. (LPT1:, LPT2: oder LPT3:) Diese muß in der Applikation korrekt eingestellt sein. Die NetWare-Shell hat die Eigenschaft, auch Ausgaben auf Schnittstellen umzuleiten, die nicht physikalisch vorhanden sind. Dabei darf die Applikation aber nicht durch direkte Hardwarezugriffe die Schnittstelle ansprechen. Ausgaben auf die eingebaute Schnittstelle lassen sich für sauber programmierte Anwendungen sogar unterbinden. Der Eintrag "local printers = 0" simuliert, daß keine Schnittstelle eingebaut ist. Damit ist ein Ausdruck nur über Druckerumleitungen auf eine Netzwerkwarteschlange möglich. Damit hat man die Möglichkeit, drei verschiedene Drucker gleichzeitig anzubinden. Sofern alle Applikationen die Wahl bieten auf welche LPT gedruckt wird, kann man zu jedem der drei Drucker den richtigen Treiber konfigurieren.

## 10.4 Die Queue

Druckdaten werden bei Netzwerken immer in Warteschlangen zwischengespeichert. Eine Queue wird auf dem Server durch ein Verzeichnis abgebildet, in welcher die Druckdaten als einzelne Dateien abgelegt werden. Der Zugriff auf diese Dateien erfolgt aber über Schnittstellen und nicht über Befehle zur Dateibehandlung. Durch entsprechende Befehle (CAPTURE) kann jeder Schnittstelle eine Queue zugeordnet werden. Druckdateien können auch direkt, ohne den Umweg über die Schnittstelle, in die Queue eingestellt werden. Dazu dient das Programm NPRINT bzw. PCONSOLE. Dabei können noch weitere Optionen oder Jobparameter angegeben werden. Diese sorgen z.B. für ein Banner am Anfang, für einen Seitenvorschub am Ende oder Initialisierungsstrings für den Drucker.

## 10.5 Der Job

Ein Druckjob dient dazu, Parameter für die Schnittstellenumleitung zusammenzufassen und abzulegen. Dadurch kann man durch die Angabe des Jobs die Angabe der einzelnen Parameter einsparen. Trotzdem können Parameter angegeben werden, welche dann die voreingestellten Parameter überschreiben.

Edit Print Job Configuration "binary"			
Number of copies:	1	Form name:	A4
File contents:	Byte stream	Print banner:	No
Tab size:		Name:	
Suppress form feed:	Yes	Banner name:	
Notify when done:	No		
Local printer:	1	Enable timeout:	Yes
Auto endcap:	Yes	Timeout count:	30
File server:	PC		
Print queue:	DUMMY		
Print server:	<Any>		
Device:	<None>		
Mode:	<None>		

Abbildung 13 Printjob

Dies ist z.B. ein Job "binary" welcher die Druckdaten 1:1 ohne Modifikation durch die Shell weiterleitet.

Auf Printjobs kann komplett verzichtet werden, denn die relevanten Angaben können den Befehlen NPRINT und CAPTURE auch als Kommandozeile beigegeben werden, bzw. unter Windows per Mausclick ausgewählt werden.

## 10.6 Von der Queue zum Drucker

Die Daten aus der Druckqueue werden von einem Printserver ausgelesen und entweder direkt an einen Drucker gesendet, oder über eine weitere Station (RPRINTER) zum Drucker geschickt. Der Printserver kann ein dedizierter PC sein (PSERVER.EXE) oder ein Teil auf dem Fileserver (PSERVER.NLM; PSERVER.VAP). Mittlerweile arbeiten auch besondere Hardwareeinsätze (JetPress, LanPress, NetPort) als Printserver im Netzwerk. Dadurch spart man den dedizierten PC ein und erreicht eine höhere Zuverlässigkeit. Speziell bei LAN's wird oft ein schneller Drucker eingesetzt. Hier muß man besonders auf die Geschwindigkeit achten. Der Drucker kann noch so schnell sein, wenn er nicht adäquat mit Daten versorgt wird. Als Faustregel kann gelten, daß heute ein Laserdrucker mit mehr als 4 Seiten pro Minute mit der Datenübertragung auf die Centronicsschnittstelle nicht unbedingt mehr ausgelastet werden kann.

### Printserver

Der Printserver ist die steuernde Komponente beim Ausgeben der Druckdaten. Der Printserver muß sich am Fileserver anmelden, um Zugriff auf die Daten zu haben. Dadurch belegt er eine Verbindung. Als NLM oder VAP benutzt er keine Session, welche einem User genommen wird. (z.B. bei 100er Lizenz belegt der Printserver die Connection 101). Ein Printserver kann mehrere Fileserver bedienen und ein Drucker kann mehrere Queues, auch über verschiedene Server hinweg bedienen. Ein Printserver kann 16 Drucker ansteuern (direkt oder über Rprinter). Auf einem Server kann immer nur GENAU EIN Printserver laufen. ab dem 17ten Drucker wird ein weiterer dedizierter PC als Printserver notwendig.

Die Printserverlösung ist sehr flexibel, weil man nahezu jeden Drucker an verschiedener Stelle über diverse Schnittstellen einbinden kann. Allerdings ist der Datendurchsatz nicht allzu leistungsfähig, womit diese Variante nur bei langsamen Druckern, geringem Druckaufkommen oder einfachen Druckdaten sinnvoll ist.

### RPrinter

RPRINTER ist ein TSR-programm, welches es erlaubt, einen PC zu nutzen, um Daten aus einer Druckerqueue über den Printserver zum Drucker zu schicken. Auf dem PC kann normal weitergearbeitet werden. Jedoch ist die Arbeitsgeschwindigkeit reduziert. Der Einsatz unter Windows und anderen Multitaskingsystemen ist nicht ratsam. Zudem bringt es für den Arbeitsplatzrechner eher mehr Last. Ohne Netzwerk werden die Daten unter Windows in ein File gedruckt. Dann bedient der Druckmanager stückweise den Drucker. Beim RPrinter werden die Daten aus der Queue geholt aber immer noch unter Mithilfe des Prozessors an den Drucker verschoben. Und bei großen Datenmengen (Grafik oder viel Text) wird immer mehr der PC mit der parallelen Schnittstelle zum Engpaß. Wenn dann noch andere Benutzer über das LAN auf dem "eigenen" Drucker drucken, wird der PC mit dem Drucker und RPRINTER auf jeden Fall gebremst. Zudem stört ein aktiver RPRINTER im Hintergrund von Windows die Arbeit am Gerät selbst merklich. Inwieweit diese Kombination selbst dann noch stabil ist, ist geräteabhängig.

### Netport, LanPress und andere Ersatzlösungen

Eine weitere Möglichkeit, Drucker an das Netzwerk anzuschließen, sind spezielle Geräte und Einschübe, welche als Printserver oder RPrinter arbeiten. zu beachten ist, daß der Einsatz als Printserver jeweils eine Verbindung belegt. Bei mehreren Druckern reduziert sich die Anzahl der gleichzeitig eingeloggten Benutzer. Der Einsatz als RPRINTER umgeht diese Belegung, da die Kommunikation zwischen Drucker und Printserver keine Verbindung belegt. NetPorts benutzen einen "unencrypted password call", so daß dies beim NetWare 3.x-Server erlaubt werden muß. Diese benötigen neben dem eigenen Netzwerkschluß auch eine eigene Stromversorgung, welche meist durch ein Steckernetzteil realisiert ist. So eignet sich diese Lösung für Netzwerkdrucker, die nicht mit Einbaukarten bestückt werden können und keine großen Datenmengen empfangen müssen. Die Daten müssen nach wie vor durch die Centronics-schnittstelle oder seriell zum Drucker und sind damit nicht für schnelle Drucker geeignet.

### Drucker-Lösungen

Neben externen Geräten als Ersatz für PC's mit RPRINTER gibt es Einschubkarten, welche bei dazu geeigneten Druckern direkt eingebaut werden können. Dadurch erspart man sich eine getrennte Stromversorgung und die Daten müssen nicht unbedingt über die Centronicsschnittstelle geschickt werden. Dadurch können die Daten, welche über das Netzwerk sehr viel schneller kommen, direkt zum Prozessor des Druckers geleitet werden. Dies erlaubt es erst, schnelle Drucker (z.B. HP1131 mit 16 Seiten/Min) leistungsgerecht anzusteuern. Dies ist die optimale Lösung zur Anbindung eines Druckers im LAN. Sobald der Drucker eingeschaltet ist, wird er auch am Netzwerk angemeldet. Zusätzlich habe ich die Erfahrung gemacht, daß z.B: die Einbaukarte für einen HP1131 direkt nach dem Einschalten schon Daten aus der Queue bezieht, während der Drucker noch in der Aufwärmphase ist. Auch der Datendurchsatz ist ein vielfaches höher als bei allen anderen Lösungen.

## 10.7 PCONSOLE

Die PCONSOLE ist das Programm, zum Konfigurieren und überwachen der Drucker. Das Programm liegt im PUBLIC-Verzeichnis, und ist damit auch jedem Benutzer zugänglich. Abhängig von den Rechten des Anwenders sind einige Funktionen nicht sichtbar.

Unter „Print Server Options“ werden die Printserver eingerichtet. Besonders zu erwähnen ist hier die Möglichkeit für Printserver eigene Operatoren zu vergeben. Dies kann benutzt werden, um Teile der Administration auf andere Betreuer zu verlagern. Als Printserveroperator kann man umfangreiche Änderungen und die tägliche Administration der Drucker ausführen, ohne dazu Supervisorrechte haben zu müssen. Allerdings kann solch ein User keine neuen Druckserver anlegen.

Mit „Print Queue Options“ werden die Warteschlangen verwaltet. Auch hier kann man mit der Option „Queue Operator“ den Administrator mit Supervisorpasswort von bestimmten Aufgaben entlasten.

## 10.8 Drucker wechseln

Dieses Kapitel ist ein Vorschlag, wie man den Benutzer anleitet zu: "Was ist beim Druckerauswählen zu beachten ?"

### 1. Schritt

Zuerst muß man der Anwendung sagen, um welchen Drucker-"TYP" es sich handelt. Dabei spielt es keine Rolle, welche Technologie (Laser, Nadel, Tintenstrahl, Plotter, Fax) das Ausgabegerät benutzt, sondern nur welche "SPRACHE" es spricht (z.B. PostScript oder HP-Laserjet, oder FX80).

Bei Windows stellt man dies in der Systemsteuerung oder unter Druckereinstellung bei der Applikation ein. Viele Drucker schaltet heute schon automatisch zwischen verschiedenen Emulationen um, da sie in der Regel sowohl HPPCLx als auch PostScript verstehen und dies im Normalfall alleine erkennen. Speziell bei LAN's gibt es aber hier das Problem, daß keine Pause zwischen verschiedenen Printjobs liegt. Aber genau diese Pause benötigen die Drucker, um die Spracherkennung zu aktivieren.

### 2. Schritt

An einen PC kann man bis zu DREI Drucker gleichzeitig anschließen (Ausgang LPT1, LPT2 und LPT3) Damit muß man auch den Anschluß zum Treiber bestimmen.



### 3. Schritt

Die Netzwerkqueue muß angebunden werden. Das Netzwerk fängt die Daten, welche auf LPT1 - 3 geschickt werden ab und reiht sie in eine interne Warteschlange ein. Jedem Drucker ist in der Regel genau eine Warteschlange zugeordnet. Um nun den Drucker auszuwählen, muß man dem Netzwerk mitteilen, in welche Warteschlange die Daten der LPTx: umgeleitet werden.

#### 10.9 Gedanken zur Druckerkontrolle

Solange in einem Netzwerk nur drei Drucker sind, die man fest an die Schnittstellen anbinden kann, braucht man sich keine Gedanken machen. Zum Wechseln des Druckers reicht es, die Ausgabe auf eine andere Schnittstelle zu lenken.

Wenn diese Zahl überschritten wird, dann muß man schon auf die "Druckersprache" achten. Solange maximal drei Emulationen nötig sind (z.B. wenn überwiegend Postscriptdrucker eingesetzt werden), dann kann man je LPT-Port eine Emulation installieren. Zum Wechseln des Drucker reicht dann oft die Änderung der Queuezuordnung. Manchmal ist dann auch die Änderung der Schnittstelle nötig.

Irgendwann kommen dann aber weitere verschiedene Drucker hinzu, so daß in einem großen Netzwerk folgendes Szenario auftreten kann:

- - FX80 kompatibel      Ein einfacher Nadeldrucker für Listen, Etiketten usw
- - HPIIP                      Ein einfacher Seitendrucker für Geschäftsverkehr
- - HP11si                    Ein schneller Drucker, der auch doppelseitig druckt (spart papier)
- - HP500C                  Ein Farbdrucker (langsam, aber Farbe auf Papier und Folie)
- - Plotter                    Für Zeichnungen
- - FAX                        Um vom Computer aus zu Faxen

Und da sieht man schon das Dilemma: Viele verschiedene Druckersprachen auf drei Schnittstellen und viele Netzwerkqueues zu verteilen. Ab hier muß man sich ernsthaft Gedanken machen, wie man Ordnung und System in dieses "Chaos" bringt. Schließlich soll es von den Benutzern angewendet und nicht verstanden werden.

Eine Lösung könnte es darstellen, alle Drucker auf LPT3: zu konfigurieren. LPT1 und LPT2 sind weiterhin benutzbar, aber werden nicht ins Netzwerk umgeleitet. So können Anwender über ihre eingebaute parallele Schnittstellen verfügen (z.B. für Datentransfer, Dongle usw) Dazu muß man dem Benutzer ein Hilfsmittel an die Hand geben, welche folgende Anforderung erfüllt:

"Ich bestimme das Ausgabegerät und der PC stellt selbst den Druckertreiber, die Schnittstelle und die Netzwerkwarteschlange ein."

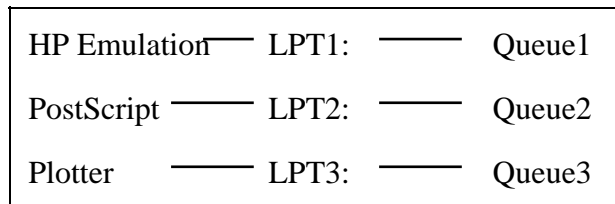
Da die Schnittstelle auf LPT3: festgelegt sein kann, reicht es, die Queuezuordnung und den Druckertreiber umzustellen. Wenn alle Benutzer die Oberfläche Windows einsetzen, dann reduziert sich das Einstellen des Druckertreibers auf eine Applikation. Bei vielen eigenständigen Anwendungen (z.B. Word, Paradox, Multiplan, DBase usw) stellt sich ein schwer lösbares Problem.

Ein Grund mehr, entweder eine einheitliche Oberfläche oder möglichst gleich anzusteuern Drucker einzusetzen.

Da es keine allgemeingültige Lösung für jedes Netzwerk gibt, stelle ich hier drei Modelle vor, welche Grundlage zu weiteren Überlegungen zum eigenen Netzwerk sein können.

**10.9.1 Small:**

Dieses Modell eignet sich für kleine LAN's, in welchem nicht mehr als drei Drucker angeschlossen werden. Damit kann man jedem der Drucker auf der Workstation logisch eine parallele Schnittstelle zuordnen. Auf diesen installiert man den passenden Druckertreiber und setzt die Druckerumleitung gleich nach dem Anmelden ins Netzwerk. z.B.



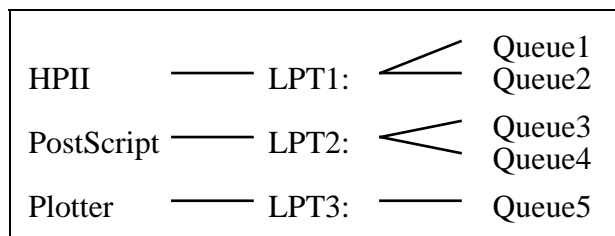
**Abbildung 14 Druckmodell "SMALL"**

Es besteht eine 1:1 Beziehung zwischen Druckertreiber, lokale Schnittstelle und Queue. Unter Windows reicht es nun, wenn der User den gewünschten Drucker einfach anklickt.

**10.9.2 Medium:**

Nun gibt es auch Netzwerke mit mehr als drei Druckern. So ist vorstellbar, daß z.B. zwei Sekretariate je einen PostScriptdrucker haben, oder in einer Programmiergruppe mehrere Drucker für Listen (Endlos) existieren, die alle mit FX80-Emulation arbeiten.

Hier bietet es sich dann an, jeder lokalen Schnittstelle eine Emulation zuzuordnen und die Queue nicht fest zuzuordnen. Damit ist mal auf drei verschiedene Druckertreiber festgelegt. Damit auch die Funktion "PrintScreen" funktioniert, sollte man auf LPT1: entweder die HP-PCL-Treiber oder einen Nadeldruckertreiber konfigurieren. Damit haben dann auch alte DOS-Anwendungen keine Probleme. Meist können die Anwendungen, welche nur einen Ausdruck auf LPT1: zulassen auch nur HP-PCL oder Epsonkompatible Drucker unterstützen.



**Abbildung 15 Druckmodell "MEDIUM"**

Unter Windows muß der Benutzer jetzt erst den Druckertyp auswählen, und dann die entsprechende Queue an den selektierten Port anhängen. Dies erscheint mir jedoch um einiges umständlicher, als die im Modell BIG beschriebene Lösung. Hat jedoch den Vorteil, daß man immer auch einen "PrintScreen" ausführen kann, wenn an LPT1: ein Zeichendrucker angeschlossen ist (z.B. Nadeldrucker oder HP). Zudem kann man sich an jede Schnittstelle "seine" bevorzugten Drucker hängen und damit schnell umschalten, ohne die Queue neu anzugeben.

10.9.3 Big:

Interessant wird die Thematik, wenn an einem Netzwerk nun mehr als vier verschiedenen Ausgabegeräte hängen. z.B. HP11, HP11si, QMS810, HP500C, FAX, HPGL-Plotter. Um all diese Ausgabegeräte zu nutzen, muß man sie alle in Windows "installieren", d.h. die nötigen Einträge in der WIN.INI vornehmen. Jedoch gibt es nicht für jeden Drucker eine Schnittstelle. Da die meisten PCs eine lokale LPT1:- Schnittstelle eingebaut haben und manche auch über eine LPT2:-Schnittstelle verfügen habe ich alle Drucker auf LPT3: konfiguriert. Es macht keine Probleme, diese Schnittstelle in eine Queue umzuleiten und darauf zu drucken. Zudem dürfte diese Schnittstelle in den neuesten Computern kaum physikalisch anzutreffen sein. Damit bleibt die LPT1: und LPT2: frei und kann für wirklich "lokale" Drucker oder Sonderfunktionen (Datentransfer, LPT2SCSI oder Pocketadapter) genutzt werden. Für alte DOS-Programme, welche nicht auf LPT3: drucken können kann die LPT1: dann bei Bedarf umgelenkt werden, ohne daß die LPT3 (und damit alle anderen Anwendungen) betroffen sind.

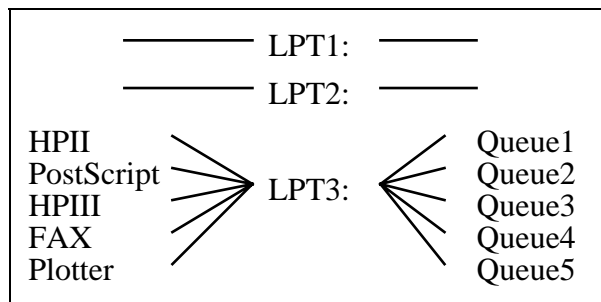


Abbildung 16 Druckmodell "BIG"

Für die Anwender von Windows bedeutet dies aber nun: Wenn der Benutzer von einem Drucker auf einen anderen wechseln will, dann muß er erst den Druckertreiber selektieren und dann die Queue anhängen. Da hier meist eine 1:1-Verbindung besteht, könnte ein Programm dies erleichtern. Dies könnte z.B. dadurch geschehen, daß der User nur einen Aliasnamen als Drucker auswählt und das Hilfsprogramm sowohl den Treiber als auch die Queue umstellt.

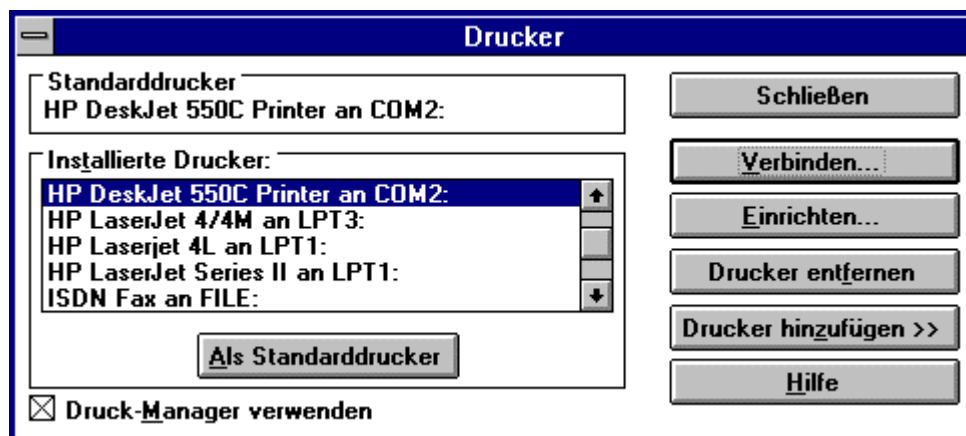


Abbildung 17 Windows Druckereinrichtung

Vielleicht kommen wir in einer der nächsten Versionen von Microsoft Windows in den Genuß, Drucker nicht nur an LPT1 - LPT3, COM1: - COM4: und LPT1.OS2 usw. anzuhängen, sondern direkt an SERVERNAME/QUEUE und damit die Beschränkung der begrenzten Schnittstellen unter MS-DOS wegfällt. Dann könnte hier in diesem Fenster stehen:

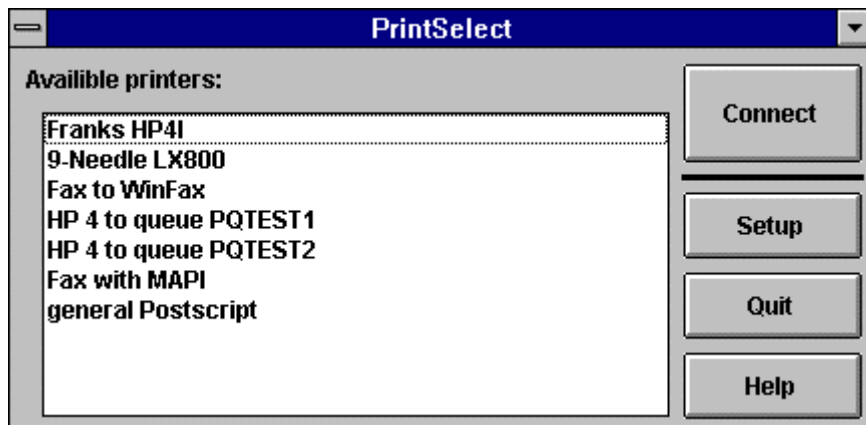


Abbildung 18 PrintSelect

## 10.10 Windowsdrucker

Zur Einstellung der Drucker unter Windows gibt es ein Hilfsprogramm.

Das Programm PRINTSET wertet die Umgebungsvariable PRINTER aus um anhand diese Eintrags aus einer INI-Datei den passenden Drucker ausfindig zu machen. Die ausgelesenen Werte werden danach in Windows eingetragen.

Diese Programm wird am Besten in der Autostartgruppe plaziert. Damit ist die sichere Zuweisung eines Druckers als Standarddrucker möglich.

Beispiel für die PRINTSET.INI

### Konfigurationsdatei 14 PRINTSET.INI

```
[message]
;Lables of the windows, buttons etc.

ENVIR_ERR=Umgebungsvariable fehlt
NOINI_ERR=INI-Datei nicht gefunden
INI_ERROR=Fehler in der INI-Datei
Queue_Error=Kann Warteschlange nicht anbinden
MAIN_Error_head=Fehler
;
; Definition for the printers
; Field      values      description
; Printeralias : short aliasname (string[8]) get from %PRINTER%
; Printertype : string      typename which matches the hardcoded name in the
driver
; Printerdriver : string [8]      Filename of the printerdriver (Windows)
; LPT-Port      : LPT1: - LPT3:      Portdescription
; Queue         : valid printqueue
; if the printer is connected at a local port, leave this field empty

[Printers]
HP4L      = HP Laserjet 4L,HPPCL5E,LPT3:,HP4I
LX800     = Epson LX-800,EPSON9E,LPT2:,LX800
MSFAX     = MSFAX,LPT1:,
PSCRIPT  = Apple Laserwriter Plus,PSCRIPT,LPT3:,DUMMY
```

Hier sind die Werte „HP4L“, „LX800“, „MSFAX“ oder „PSCRIPT“ in der Variable PRINTER erlaubt. Die Variable Printer ist PC-Abhängig und sorgt dafür, daß die Ausdrücke am nächsten Drucker gedruckt werden. Dieses Programm ist jedoch nicht zum Betrieb des Netzwerkes erforderlich.

Die Rückmeldungen an die Benutzer sind in der INI-Datei definiert um eine Mehrsprachfähigkeit zu erlauben.

## 10.11 PRINTSEL

Das Programm PRINTSEL erlaubt es, dem Benutzer eine einfache Aliasliste der Drucker zur Verfügung zu stellen. Somit kann der Benutzer aus einer Druckerliste auswählen. Das Programm übernimmt dann aus einer zentral gepflegten INI-Datei die zum Alias passenden Druckertreiber, Schnittstellen und Queues und stellt diese ein. Somit kann es nicht mehr passieren, daß ein Benutzer

mit einem falschen Druckertreiber auf einen anderen Drucker ausdruckt. Dieses Programm ist jedoch nicht zum Betrieb des Netzwerkes erforderlich.

## 10.12 PRINTSET

Printset ist ein aus Printsel abgeleitetes Programm. Es werten die Umgebungsvariable %PRINTER% aus. Der darin abgelegte Aliasname eines Druckers wird in der Printset.ini gesucht. In dieser INI-Datei ist je Aliasname der Druckerklarname, der Windowsdruckertreiber, die Schnittstelle und optional die NetWare-Queue abgelegt.

Wird PRINTSET in der Autostartgruppe abgelegt, so wird bei jedem Start von Windows abhängig von der PRINTSET.INI und der Umgebungsvariable %PRINTER% ein Standarddrucker unter Windows eingerichtet. Somit ist es möglich, je PC einen ganz bestimmten Drucker als Arbeitsdrucker anzugeben. Und dieser Drucker IMMER eingerichtet ist, egal wann, welcher Benutzer an diesem PC arbeitet.

### Konfigurationsdatei 15 Printset.ini

```
;PrintSet.INI Definitionsdatei  Druckerdefinitinsdatei

[message]
;Lables of the windows, buttons etc.

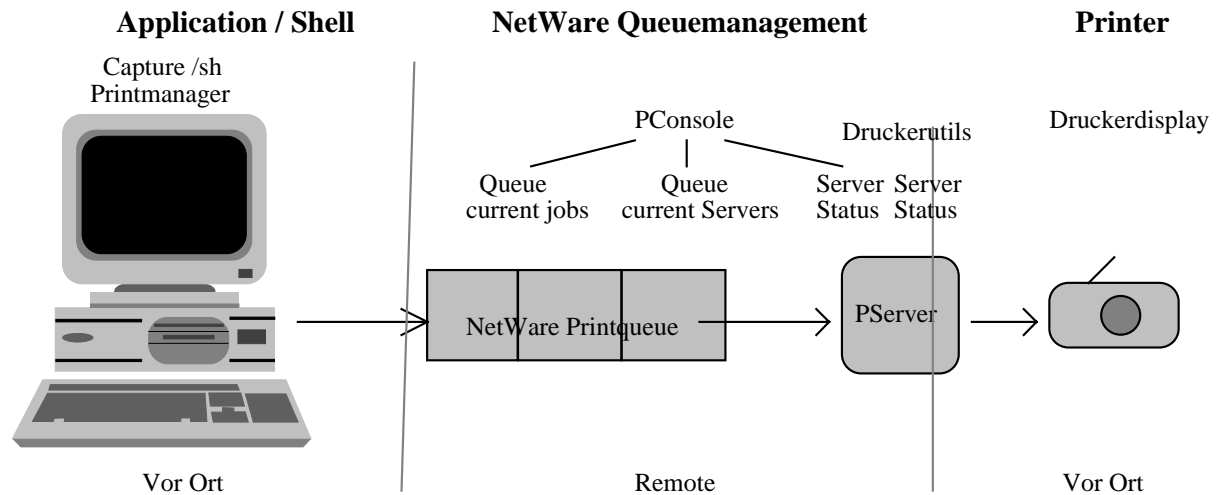
ENVIR_ERR=Umgebungsvariable fehlt
NOINI_ERR=INI-Datei nicht gefunden
INI_ERROR=Fehler in der INI-Datei
Queue_Error=Kann Warteschlange nicht anbinden
MAIN_Error_head=Fehler
;
; Definition for the printers
; Field      values      description
; Printeralias : short aliasname (string[8]) get from %PRINTER%
; Printertype  : string    typename which matches the hardcoded name in the
driver
; Printerdriver : string [8]  Filename of the printerdriver (Windows)
; LPT-Port     : LPT1: - LPT3:  Portdescription
; Queue       : valid printqueue
; if the printer is connected at a local port, leave this field empty

[Printers]
FS15-EDV=Kyocera FS-1500 / FS-1500A,HPPCL5MS,LPT3:,FS15-EDV
HP560C  =HP DeskJet 550C (Monochrome),HPDSKJET,LPT1.DOS,
MSFAX   =Microsoft Fax,MSFAX,LPT1:,
APPLE   =Apple Laserwriter Plus,PSCRIPT,LPT3:,
LX800   =Epson LX-800,EPSON9E,LPT2:,
FACSYS  =FACSys HP LaserJet Series II,FXHPPCL,LPT3:,
HP550C  =HP DeskJet 550C Printer,deskjetc,COM2:,
HP4     =HP LaserJet 4/4M,HPPCL5E,LPT3:,
HP4L    =HP Laserjet 4L,HPPCL5E,LPT1:,
HP2     =HP LaserJet Series II,HPPCL,LPT1:,
ISDNFAX =ISDN Fax, FAXDRV,G:\TELESCOM\FAX\CURRENT.FAX,
MT330   =Mannesmann Tally MT 330,MANTAL24,LPT1:,
MSFAX   =Microsoft Fax,MSFAX,LPT1:,
TEXT    =Universal/Nur Text,TTY,FILE:,
MHSFAX  =videoFAX V1.0,VIDEOFAX,LPT1:,
WINFAX  =Winfax,WINFAX,COM1:,
```

Wichtig ist, daß der Klarname des Druckers genauso angegeben wird, wie ihn der Windowsdruckertreiber erwartet. Ansonsten kann der Druckertreiber nicht den korrekten Drucker aus der Druckerfamilie finden und benutzt statt dessen den untersten Drucker, womit die Möglichkeiten des Drucker nicht voll ausgeschöpft werden können.

### 10.13 Fehlersuche Drucker

Einer der häufigsten Anrufe lautet "Mein Drucker druckt nicht!". Nun liegt es am Administrator oder beauftragten Personen, die Unterbrechung im System zu finden. Folgendes Schaubild zeigt den Weg der Druckdaten



**Abbildung 19 Fehlersuche Drucken**

Einige Funktionen kann man vom eigenen Arbeitsplatz aus ausführen, andere müssen in der Regel vor Ort oder durch Mithilfe des Benutzers geregelt werden.

Bevor man sich auf den Weg macht oder den Benutzer um Hilfe bittet, sollte man mit PCONSOLE in die passende Queue sehen. Findet sich dort der Druckauftrag (dann in der Regel mehrmals), dann scheint die "linke Seite" des Bildes zu funktionieren. Mit PCONSOLE kann man dann gleich den Druckserver kontrollieren. Meist findet man so die meisten der Fehler (Out of Paper, PrintServer nicht aktiv)

Wenn andere Benutzer, welche den gleichen Drucker benutzen, drucken können, dann liegt es an der Workstation oder den Rechten des Benutzers. Die kann im Windows Druckmanager oder mit dem Befehl CAPTURE /SH angezeigt werden.

## 11 Workstation



Workstations sind die Arbeitsstationen für die Benutzer. Da alle Daten und Programme zentral auf dem Server vorgehalten werden, sind lokale Festplatten nicht nötig. Damit entfallen auch die Gefahren beim booten von lokalen Festplatten. Die Daten müssen auf dem Server abgelegt werden und sind damit optimal geschützt durch die Zugangskontrolle, die NetWare-Sicherheitsfunktionen und das regelmäßige Backup.

Zum Austausch von Daten sollten allen Benutzern die eingebauten Diskettenlaufwerken (3,5"; 1,44 MB) reichen. Diese Disketten speichern bei weniger Platzbedarf mehr Daten und sind einfacher und sicherer zu handhaben als 5,25"- Disketten. Um jedoch die Möglichkeit zu haben, diese Disketten einzulesen, werden einige Gateways mit 5,25-Diskettenlaufwerken ausgestattet. Damit hat man die Möglichkeit, welche jedoch kaum benötigt wird. Damit kann man auf der Arbeitsplatzseite jedoch auf große Gehäuse mit hoher Wärmeentwicklung verzichten. Damit kann man sogar vollständig auf einen Lüfter verzichten und damit die Geräuschbelastung zu minimieren.

Durch den Einsatz einer Koprozessor-VGA-Karte ist ein schneller Bildschirmaufbau mit der hohen Auflösung sichergestellt. Der Prozessor ist damit von vielen Grafikfunktionen entlastet.

Es ist nicht nötig Drucker, CD-Rom's oder andere Komponenten an der Workstation direkt anzuschließen. Damit beschränkt sich der Anschluß auf die Stromversorgung und das Netzwerkkabel. Es gibt nichts, was die Arbeitsstation besonders auszeichnet. Damit ist es sehr einfach, die Installation zu ändern oder die Hardware auszutauschen. Im Falle eines Defektes kann auf irgend einer anderen Station weitergearbeitet werden, da keine Daten auf einer lokalen Festplatte liegen.

Die Workstation im Netzwerk stellt für den Fileserver ein Client dar. Jede Workstation besteht aus mehreren Komponenten, welche einzeln behandelt werden.

### **11.1 Hardware (HD, CPU, Grafik, NW-Karte)**

Um Windows zu benutzen, wird mindestens ein 386sx erwartet, jedoch ist heute als Minimum ein 386/25 mit 4MB zu empfehlen. Gerade wenn auf PAGING verzichtet werden muß (keine lokale HD) ist nur der physikalisch vorhandene Speicher nutzbar. Es ist nicht notwendig im LAN die Workstations mit großen Festplatten auszustatten. Für die Arbeitsgeschwindigkeit ist mehr die Grafikkarte und der Prozessor relevant. Die meisten ISA-Lankarten schaffen es die Daten schnell genug über das LAN zu bekommen. Es adäquater Monitor sollte die Arbeit unterstützen. Da diese Bereiche aber ständiger Entwicklung unterworfen sind, ist je nach Situation selbst zu entscheiden.

## 11.2 Betriebssystem MS-DOS

Für PC's gibt es unterschiedliche Betriebssysteme. Neben dem bekannten MS-DOS kann auch OS/2 integriert werden. Unixkonforme Betriebssysteme lassen sich mit dem Zusatzprodukt NetWare NFS anbinden. Da MS-DOS das gebräuchlichste Betriebssystem ist, beschränken sich darauf nachfolgende Betrachtungen.

## 11.3 RemoteBoot

Um die Pflege der Bootfiles einfach zu halten, empfiehlt sich, möglichst wenig verschiedene Bootfiles zu nutzen. Dadurch beschränkt sich ein Treiberupdate auf wenige Files. Bootfiles haben zudem den Vorteil, daß keine Dateien ob eventuell vorhandenen lokalen Festplatten gepflegt werden müssen. In den meisten Fällen, kann die Workstation im Netzwerk arbeiten, auch wenn die lokale Festplatte nicht nutzbar ist. Jedoch gilt es einige Punkte zu beachten:

- Da diesen Workstations sowohl die lokale Festplatte als auch die Diskette im Laufwerk A: fehlt, müssen alle Programmteile, welche benötigt werden wenn der Benutzer nicht angemeldet ist, im LOGIN-Verzeichnis stehen, z.B. eine COMMAND.COM oder weitere Programme.
- der EMM386 wird von A: geladen. Da Windows beim Start diese Datei wieder sucht, muß beim Laden von EMM386 in der Konndaozeile angegeben werden, wo Windows später danach sucht, z.B. y=F:\LOGIN\EMM386.SYS.
- Da speziell beim Laden der ODI-Shell der Netzwerkkartentreiber die Verbindung zum LAN normalerweise abbricht, indem er die LAN-Karte neu initialisiert, muß direkt nach dem Laden von LSL das Programm RPLODI ausgeführt werden.
- SET BOOTFILE=<Bootfilename>  
Dieser Eintrag in der <BOOTFILENAME>.BAT dient zur späteren Identifizierung mit welcher Konfiguration dieser PC geladen worden ist. Dies kann auch in Batchjobs ausgewertet werden.

Argumente für und gegen Remoteboot gegenüber lokalen Festplatten

- ✓ weniger Lärm und Wärementwicklung ohne Festplatte
- ✓ geringere Ausfallwahrscheinlichkeit aufgrund der „eingebauten“ Sicherheit
- ✓ Kein Virenbefall da keine lokalen Bootfiles und Bootsektoren
- ✓ Falsch eingetragene Festplattentypen oder „verlorenes“ PC-Setup beeinträchtigen nicht Remoteboot
- ✓ Einfachere Wartung und Update der DOS-Versionen
- ✓ Schutz gegen Veränderungen der Startdateien (AUTOEXEC.BAT, CONFIG.SYS)
- ✓ zentrale Pflege und Updates der Netzwerktreiber
- ✓ Pflege erfolgt NICHT am Arbeitsplatz. Minimale Störung der Benutzer
- ✓ Ohne lokale Festplatte sind sämtliche Daten zwingend auf dem Server (einfaches Backup, Zugriffsschutz)
- ✓ Höchstmöglicher Schutz gegen Fremdeinwirkungen (Viren, Diebstahl, Personen, Fehlbedienungen)
- ✗ Nicht ohne Netzwerk betriebsfähig
- ✗ Keine „eigene“ Booteinstellung möglich
- ✗ Anfangs höherer Aufwand zur Konfiguration (Sonderfälle)
- ✗ Etwas geringere Flexibilität

Nicht jedes Betriebssystem kann per RemoteBoot gestartet werden. RemoteBoot wird nicht nur bei MS-DOS angewendet, auch in UNIX-Umgebungen ist RemoteBoot möglich und wird auch eingesetzt.

## 11.4 Fehlersuche RemoteBoot

Folgende Anleitung soll helfen, schnell den Fehler zu finden, wenn eine Station keinen Remoteboot macht.



### 11.4.1 Funktioniert die LAN-Karte im Server ?

Gerade beim neuen Aufbau eines Servers, oder bei Änderungen in der AUTOEXEC.NFC passiert es, daß falsche Parameter angegeben werden. Die Funktion ist sichergestellt, wenn:

- von irgendeiner Station eine Verbindung zum Server möglich ist
- Mit MONITOR.NLM und LAN-Information der Zähler für eingehende Pakete ungleich 0 ist.

### 11.4.2 Kommen Anfragen der Station beim Server an ?

Um dies zu testen, ist an der Serverconsole einzugeben: „**TRACK ON**“. Dann zeigt NetWare die einkommenden Requests an. Wenn nun die Station bootet, sollte ein „get nearest server“-Request eingehen.

Ist dies der Fall, dann arbeitet das Bootrom, die LAN-Karte in der Workstation und im Server ist sowohl das Protokoll als auch die Lankarte funktionstüchtig. Ansonsten sollte zuerst die Interrupteinstellung überprüft werden. Weiterhin muß sichergestellt sein, daß das Protokoll an die richtige LAN-Karte gebunden ist. Welche Protokolle and welche LAN-Karte gebunden sind ersieht man mittels MONITOR.NLM oder durch Eingabe von „CONFIG“ auf der Serverkonsole.

### 11.4.3 Erlaubt der Server RemoteBoot ?

Ein Server kann nur dann Remoteboot zulassen, wenn die Einstellung des Parameters „REPLY TO GET NEAREST SERVER“ auf „ON“ gesetzt ist. Bei NetWare 4 überprüft man dies am Besten mit LOAD SERVMAN. Bei einem NetWare 3.x-Server tippt man „SET REPLY To GET NEAREST SERVER“ ein, worauf der Server die aktuelle Einstellung anzeigt.

### 11.4.4 Bootimage/BOOTCONF-SYS

Nun gilt es zu überprüfen, ob eine Verbindung zustande kommt und eine gültige Bootimagedatei vorhanden ist.

In dem Moment, wo das BootRom auf den Server und das Bootimage zugreifen will, eröffnet es eine logische Verbindung. Mit MONITOR.NLM kann diese Verbindung betrachtet werden. Sie trägt die Bezeichnung „NOT-LOGGED-IN“. Eventuell bestehen mehrere dieser Verbindungen. Zu jeder Verbindung ist die Ethernetknotennummer bestimmbar, so daß die gewünschte Verbindung ausfindig zu machen ist.

Wenn eine Datei BOOTCONF.SYS in SYS:LOGIN existiert, muß sichergestellt sein, daß für die dort eingetragenen Ethernetknoten auch das angegebene Bootimage existiert. Alle Stationen, welche dort nicht eingetragen sind, suchen eine NET\$DOS.SYS. Diese muß vorhanden sein.

### 11.4.5 Workstation

Wenn bisher noch alles korrekt erscheint, suchen wir auf der Arbeitsstation weiter.

Zuerst sollte versucht werden, mit einer Diskette oder von Festplatte zu booten und eine Verbindung zum Netzwerk zu bekommen. Somit lassen sich Konfigurationsfehler (I/O-port, Interrupt) ausschließen.

Dann gilt es festzustellen, wie weit der PC kommt.

- Wenn der PC immer wieder bootet, dann findet er keinen Server oder kein Bootimage. (Kabel nicht aufgesteckt, falsches Frame, Server antwortet nicht)
- Wenn er direkt von Festplatte bootet oder „no boot device“ meldete, dann ist das Bootrom nicht aktiv, d.h. eventuell falsche eingesteckt, nicht aktiviert oder vom falschen Typ.
- Wenn der Server bootet aber mittendrin hängebleibt, dann wird vermutlich die Netzwerkkarte durch das Laden des Treibers neu initialisiert. (RPLDI einsetzen, Bei Packettreiber den passenden Parameter angeben). Wie weit der Bootprozess kommt, läßt sich anhand von MONITOR.NLM sehen. Da NetWare sowohl die Anzahl der Requests als auch die Menge der übertragenen Daten zählt. Anhand der übertragenen Kbyte kann man abschätzen, bei welchem Programm sich der Server aufhängt. Sehr hilfreich sind hier auch Kontrollausgaben wie sie mit ECHO in der

AUTOEXEC.BAT erzeugt werden können oder durch absichtliche Fehler in der CONFIG.SYS, welche DOS anzeigt.

#### 11.4.6 Ethernetframe

Die Workstation un der Server können nur dann eine Verbindung aufnehmen, wenn beide das gleiche Ethernetframe benutzen. Das Ethernetframe des Bootroms ist im Rom selbst eincodiert. Zu dieser Zeit ist noch keine Einstellung in der NET.CFG aktiv. Bei einigem Bootroms ändert sich das Frame, wenn die Hardwareeinstellung der Netzwerkkarte geändert wird. Ist man sich nicht über das verwendete Frame sicher, dann kann übergangsweise auf die LAN-Karte im Server ein weiteres Frame mit einer eigenen IPX-Netzwerknummer gebunden werden. Wenn dann eine Verbindung zustande kommt, dann läßt sich anhand der IPX-Nummer das verwendete Frame ausfindig machen.

#### 11.4.7 Sonderfall ODI

Benutzt man ODI-Treiber, so muß LSL.COM mitgeteilt werden, daß die Netzwerkkarte nicht sofort beim Laden des Treibers initialisiert werden darf, sondern erst wenn das erste Paket zu senden ist. Ansonsten würde die aktuelle Verbindung zum Bootimage unterbrochen. Dazu muß das Programm RPLODI nach LSL.COM gestartet werden.

#### 11.4.8 Sonderfall EMM386

Der Treiber EMM386 muß beim Start von Windows teilweise nachgeladen werden. Dazu benötigt er den Pfad. Beim booten von Festplatte merkt sich der Treiber, von woher er gestartet worden ist. Beim RemoteBoot ist ein Zugriff auf das Bootimage oder das A:-Laufwerk nicht möglich. Daher muß in der CONFIG.SYS die spätere Position mit dem Parameter /Y= Bekanntgemacht werden.

Ahemm.. are your bootrom "old ones" or are they the newer "enhanced bootroms" ?

Enhanced Bootroms

Seit einiger Zeit gibt es ein neues Remoteboot-schema. Dazu sind „enhanced Roms“ notwendig. Diese Roms lassen dem Benutzer z.B: eine Wahlmöglichkeit, welches Image benutzt werden soll.

#### 11.5 Workstationshell

Die Funktion der Netzwerke wird bei den Workstations zum Betriebssystem hinzugebunden. Damit stellen die Netzwerkdienste eine Erweiterung der normalen Befehle und Geräte dar. Aufgrund der verschiedenen Netzwerkprotokolle, Netzwerkhardware und Betriebssysteme lädt man die benötigten Komponenten getrennt nach. Bei MS-DOS ergibt sich stark vereinfacht folgendes Bild.

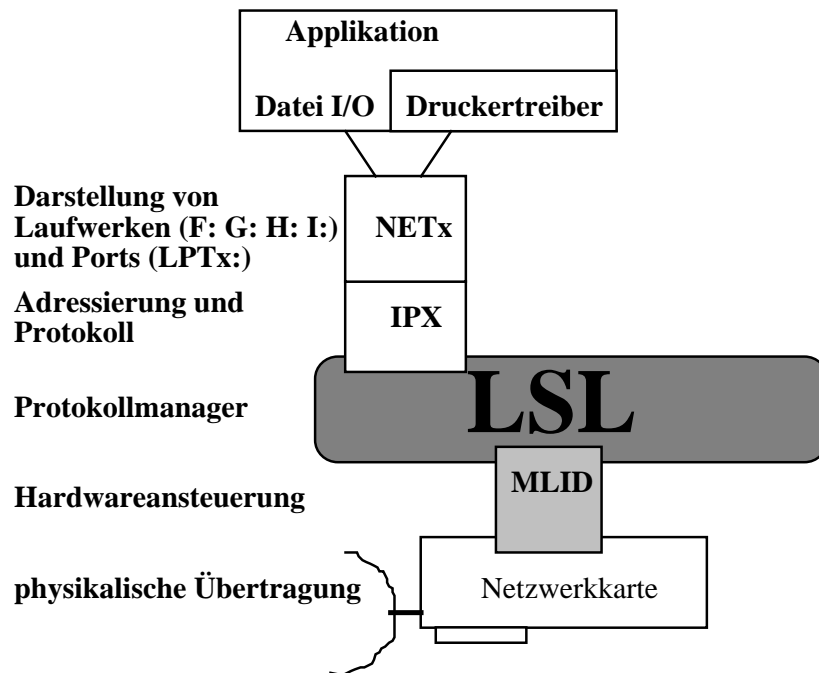


Abbildung 20 Netzwerkshell

### NETX

NETX erweitert MS-DOS, indem es alle DOS-Aufrufe abfängt und entscheidet, welche an DOS für die lokale Ausführung weitergegeben werden, oder über das Netzwerk von einem Fileserver bearbeitet werden. Die Applikation braucht in der Regel nichts davon zu wissen. Netzwerklaufwerke und Netzwerkdrucker verhalten sich in vielerlei Hinsicht genau wie lokale Drucker und Laufwerke. NETX nutzt die Übertragungsdienste von IPX um die Aufträge über das LAN zu versenden und zu empfangen.

### VLM

die VLMs stellen im Gegensatz zu einer Shell einen DOS-Requester dar. Der Einsatz von VLMs wird dann notwendig, wenn NetWare 4 oder PersonalNetware eingesetzt wird. Beim reinen Betrieb von NetWare 3.x ist der Einsatz nicht notwendig. Die Funktionalität ist in etwas gleich. Im Gegensatz zur Shell, welche die COMMAND.COM regelrecht „einkapselt“ ist ein Requester ein Hilfmodul von DOS und unterliegt der Steuerung durch die COMMAND.COM. Somit sind z.B. auch die Variablen LASTDRIVE und FILES (CONFIG.SYS) von Belang. Der Betrieb von VLM und NETX auf einem LAN auf unterschiedlichen Workstations ist gleichzeitig möglich. Die VLMs enthalten auch Module für Packetburst und für Managementaufgaben.

### IPX

IPX (Internet Paket eXchange) empfängt unter anderem Daten von NETX, verpackt diese, versieht das Paket mit Absender und Zieladresse und übergibt es an LSL zur Übertragung.

### LSL

LSL dient als zentrale Multiplexeinheit, denn auf einem Netzwerk können mehrere Protokolle (z.B. TCP/IP, Appletalk, IPX, OSI usw.) benutzt werden. Diese kommen alle bei LSL an und LSL entscheidet, an welchem Protokoll-Stack die Daten weitergegeben werden. Für das Novell-Netzwerk ist nur IPX von Interesse. Sobald jedoch z.B. Emulationen für UNIX-Rechner benutzt werden, kommt TCP/IP dazu.

### MLID

Das MLID ist der zur LAN-Karte passende Treiber. Er stellt die Verbindung zwischen der Hardware und LSL her. Beim Wechsel der LAN-Karte reicht es in der Regel, diesen Treiber auszutauschen.

Dieses Modulkonzept erlaubt es, einfach neue Komponenten auszutauschen oder zu wechseln. Protokolle können dynamisch hinzugeladen und entladen werden. Updates von Teilen der Software sind einfach möglich.

### 11.6 Netzwerktreiber

#### 11.6.1 Die Netzwerkhardware

Die Netzwerkhardware ist das Bindeglied zwischen dem Computer und dem Übertragungsmedium. Ethernet, TokenRing, TwistedPair und neuerdings auch FDDI sind bekannte Übertragungswege. Aber auch Infrarot, Funkwellen, Modemverbindungen und parallele Schnittstellen sind mögliche Übertragungsmittel.

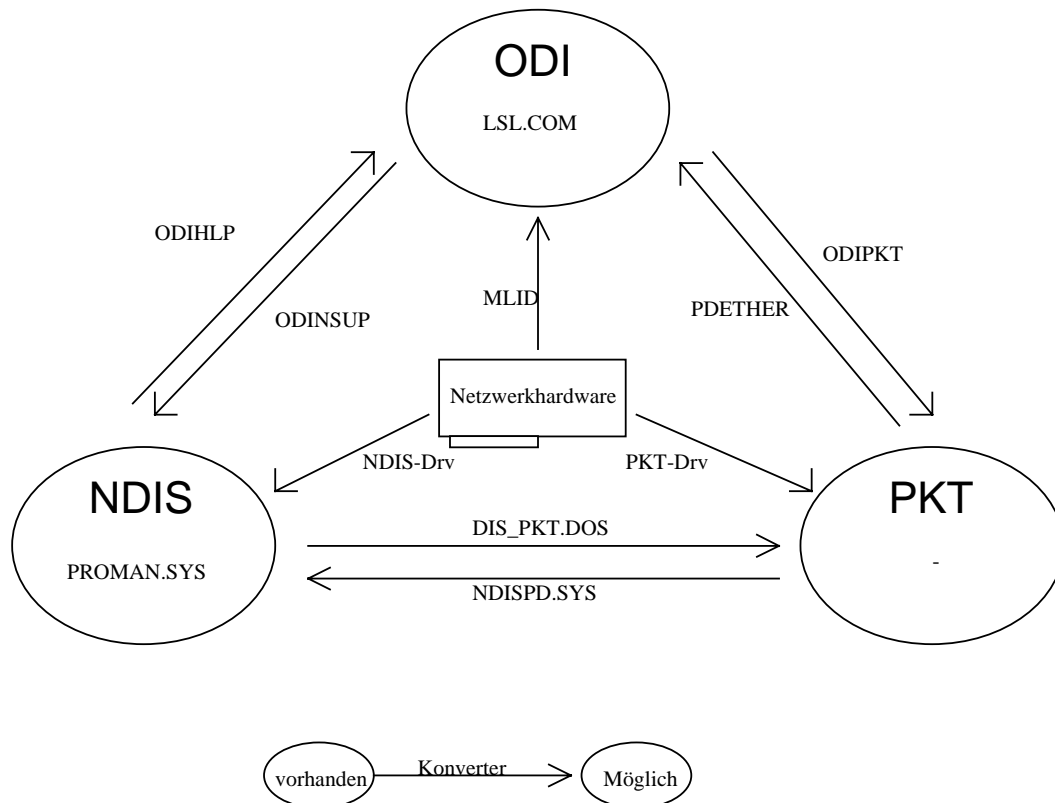


Abbildung 21 ODI/NDIS/PACKET - Umsetzung

#### 11.6.2 Hardwaretreiber

Der Softwaretreiber für die Interfacekarte initialisiert die Hardware und stellt eine definierte Schnittstelle für Applikationen zur Verfügung.

##### PKT - Packettreiber

Clarkson Packettreiber. Basis für viele TCP/IP-Emulationen (PCTCP etc). Eine sehr frühe Schnittstelle, um über eine LAN-Karte mehrere Protokolle zu fahren. (Treiber teilweise PD). Entwickelt an einer Universität in den USA.

##### NDIS - Network Device Interface Specification

Microsoft, Banyan, 3COM. Wird bei OS/2, Windows NT und Windows4worksgroups eingesetzt. Auch Banyan-LANs und LanManager arbeiten mit NDIS. Neben dem reinen Kartentreiber ist ein Protokollmanager nötig

**ODI - Open Datalink Interface Specification**

Novell, multiprotokollfähiger Treiberstack. Löste das dedizierte IPX ab. Alle Programme sind als COM oder EXE realisiert und komplett einladbar. Dank vieler Konverter eine gute Basis.

**andere**

Neben diese drei Hauptschnittstellen liefern einige Hersteller eigene Kartentreiber für ihr eigenes Produkt aus. z.B. Wollongong nutzt einen eigenen TWG-Treiber, ermöglicht jedoch auch den Zugriff auf NDIS, ODI und Packettreiber mittels eigener TWG-Konverter..

**11.6.3 Konverter****ODINSUP**

Hersteller: Novell

Quelle: NetWire, CompuServe

Beschreibung: Erlaubt es, mit ODI als Basis einen NDIS-Stack zu nutzen. Man benötigt den normalen NDIS-Treibersatz, nur der eigentliche Netzwerkkartentreiber wird durch den ODI-Stack und ODINSUP ersetzt

**LANSUP**

Hersteller: Novell

Quelle: Novell

Beschreibung: Novell liefert mit diesem Programm die Möglichkeit, auf einem NDIS-Treiber einen ODI-Stack zu etablieren.

**PETHER**

Hersteller: Novell

Quelle: NetWire, CompuServe

Beschreibung: erlaubt es, einen ODI-Stack auf einen Packettreiber aufzubauen. Dies ist dann nützlich, wenn für eine spezielle Hardware nur ein Packettreiber zu Verfügung steht.

**ODIPKT**

Hersteller: Dan Lanciani

Quelle: NetWire, CompuServe, PD

Beschreibung: Erlaubt es, über ODI eine Packettreiberschnittstelle zu emulieren. Damit kann man Protokollstacks laden, welche nur mit der Packettreiberschnittstelle funktionieren (z.B. FTP-PCTCP)

**NDISPD.SYS**

Hersteller: DCA

Quelle: DCA

Beschreibung: Ermöglicht es, einen NDIS-Stack auf einem Packettreiber aufzubauen. Wird beim Produkt "Remote Lan Node" benutzt, welches einen Packettreiber für Modemverbindungen bietet und damit zu NDIS Kompatibel ist.

**DIS\_PKT.DOS**

Hersteller:

Quelle: BBS, Public Domain

Beschreibung: Erlaubt es, daß Packettreiberapplikationen über NDIS kommunizieren können.

## 11.7 Konfigurationsdateien

Zu jeder Workstation gehören einige Dateien, welche automatisch Aktionen ausführen, bzw. Informationen beinhalten, welche von Programmen ausgewertet werden. Im Netzwerk gibt es auch eigene Dateien, welche die Netzwerkshell beeinflussen. Zu jeder Datei ist eine Beispieldatei aufgelistet, welche für viele verschiedene Computer funktionieren sollte. Jedoch ist Feinarbeit je nach benutztem System anzuraten.

### 11.7.1 CONFIG.SYS

Diese Datei wird beim Starten des Betriebssystems MS-DOS durchlaufen. Sie dient dazu, Treiber und Speichermanager zu installieren und Parameter einzustellen. Die aktuellen Einstellung der Bootfiles sind im Anhand zu finden. Dies hier ist ein Beispiel einer CONFIG.SYS, welche meistens zufriedenstellende Ergebnisse liefert.

#### Konfigurationsdatei 16 CONFIG.SYS

```
device      = A:\HIMEM.SYS
device      = A:\EMM386.EXE noems i=e000-ffff y=F:\LOGIN\emm386.exe
shell       = A:\COMMAND.COM /e:1024 /p
devicehigh  = A:\ANSI.SYS
country     = 049,,A:\COUNTRY.SYS
files       = 30
buffers     = 20
DOS         = HIGH,UMB
BREAK       = ON
FCBS        = 16,8
SWITCHES    = /w
```

### 11.7.2 AUTOEXEC.BAT

Die AUTOEXEC.BAT wird danach ausgeführt und dient dazu, Programme automatisch zu laden. Für den betrieb im Netzwerk ist diese Datei in zweierlei Hinsicht sichtig. Beim booten von Festplatte können in dieser Datei die Netzwerktreiber geladen werden. Beim Remote Boot startet diese Datei einen Batchjob, welcher die Aufgabe übernimmt, da bei mehreren verschiedenen Bootfiles auch die Startbatches im SYS:LOGN-Verzeichnis liegen müssen. Dies jedoch nicht mit der Autoexec.bat möglich ist. Daher ist hier das Beispiel für Remote Boot aufgelistet. Die Autoexec.bat startet einfach den LWPXXXXX.BAT. Dieser liegt auch im LOGIN-Verzeichnis

#### Konfigurationsdatei 17 Startbatchdateien

##### AUTOEXEC.BAT

```
LWPXXXXX.BAT
```

##### LWPXXXXX.BAT

```
@echo off
cls
echo ***** Bootfile: LWPXXXXX *****
set BOOTFILE=LWPXXXXX
echo - LSL
lh lsl.com >nul:
echo - RPLODI
rplodi >nul:
echo - NE2000
LH ne2000 >nul:
echo - IPXODI
LH ipxodi >nul:
echo - NETX
lh netx >nul:
echo - Connect
f:
echo - KEYB GR
lh keyb gr,,keyboard.sys >nul:
login dummy
```

### 11.7.3 NET.CFG bzw SHELL.CFG

Beim Laden der Netzwerkshell kann man die Standardparameter annehmen oder eigene Parameter angeben. Jedoch kann man diese nicht alle als Kommandozeile angeben, so daß eine

Konfigurationsdatei benutzt wird. Bei der alten Shell heißt die Datei SHELL.CFG. Wenn man die ODI-Shell oder zukünftig VLM's benutzt, dann heißt die Datei NET.CFG. Darin stehen bei ODI dann auch die Hardwareeinstellungen der LAN-Karte. Die hier aufgelistete NET.CFG gilt für eine NE2000-Karte. Die Bedeutung der Parameter finden sich in den Handbüchern zu NetWare. Hier sind bei weitem nicht alle Optionen benutzt.

### Konfigurationsdatei 18 NET.CFG

```
machine type = IBM
long machine type = PC386
show dots = on
file handles = 60

Link Support
    Buffers 8 1500
    MemPool 4096

Link Driver NE2000
    INT 5
    MEM CC000
    PORT 320
    Frame Ethernet_II
    Protocol IPX 8137 Ethernet_II

Protocol IPX
    bind NE2000
```

## 11.8 Umgebungsvariablen

Umgebungsvariablen sind eine Möglichkeit, Informationen abzulegen. Sie bekommen im Netzwerk eine bedeutende Rolle. Einige davon werden von Programmen ausgewertet, z.B. wohin temporäre Dateien abgelegt werden. Man kann auch Konfigurationsdaten ablegen, welche in Batchjobs ausgewertet werden können.

Umgebungsvariablen können beim Booten, beim Login, beim Start von Programmen und von Batchfiles gesetzt werden. Einige Umgebungsvariablen kommt in diesem Konzept tragende Bedeutung zu. Die Klammer am Ende enthält das Programm bzw den Batchjob, welcher die Variable setzt.

### COMSPEC [AUTOEXEC.BAT, LOGIN.EXE]

verweist auf die COMMAND.COM von Dos. Beim Remoteboot muß sie nach dem Laden von NETX auf eine gültige COMMAND.COM umgesetzt werden, da auf das Bootfile nicht mehr zugegriffen werden kann. Verwenden alle Workstations die gleiche Dosversion, bietet es sich an, die COMMAND.COM nach \LOGIN zu kopieren, damit auch darauf zugegriffen werden kann, wenn der PC nicht angemeldet ist.

### CONFIG [CONFIG.SYS]

Diese Variable benutzt MS-DOS ab Version 6.0 um die Bootkonfiguration anzuzeigen. Sie wird beim Remoteboot nicht benutzt, da die Wahlmöglichkeit nicht eingerichtet ist.

### TEMP, TMP [LOGIN.EXE]

Diese Variablen verweisen auf ein Verzeichnis, wohin Programme bei Bedarf temporäre Daten ablegen können. Dieses Verzeichnis muß existieren und der Benutzer muß die nötigen Rechte darauf haben. Hier muß der Admin steuernd eingreifen, um die Last auf dem Server zu kontrollieren. Temporäre Daten und Swapfiles (Windows) sollten möglichst auf einer lokalen Festplatte liegen.

### BOOTFILE [AUTOEXEC.BAT]

Diese Variable wird im Bootfile gesetzt. Sie ist zum späteren Betrieben noch nicht nötig, kann aber ausgewertet werden, um bestimmte Aktionen zu verweigern (z.B. wenn für CD-ROM-Zugriff ein spezielles Bootfile benötigt wird, kann dieses geprüft werden) (Bootfile)

### QLPT3 [PCCFG.BAT, PCSET.BAT]

Hier steht die Druckqueue des räumlich am nächsten stehenden Druckers. Damit kann beim LOGIN automatisch ein CATPTURE auf diese Queue gemacht werden, so daß unabhängig vom Benutzer der Druck immer in der Nähe der Workstation herauskommt.

### PRINTER [PCCFG.BAT, PCSET.BAT]

Hier steht der Aliasname des räumlich am nächsten stehenden Druckers für Windows (Windows Standarddrucker). Beim Start von Windows kann das Programm PRINTSET automatisch den Standarddrucker einstellen, die Schnittstelle einrichten und die Druckerwarteschlange anbinden.

**LEVEL** [USERCFG.BAT, USERSET.BAT]

Diese Variable weist dem Benutzer einen Level zu. Abhängig vom Benutzerlevel kann man verschiedene Funktionen starten. LEVEL=0 bedeutet, daß der Benutzer fast nichts verstellen kann, da z.B. die WIN.INI immer überkopiert wird. Damit ist die FUNKTION sichergestellt. Je erfahrener ein Benutzer ist, desto höher kann man den Level setzen um ihm mehr Freiheiten einzuräumen, wenn der Benutzer damit umgehen kann.

**SERVER** [LOGIN.EXE]

Diese Variable spezifiziert den Fileservernamen. Damit können auch Programme den Namen lesen, welche KEINE NetWare-calls benutzen. Speziell in Batches ist es oft sinnvoll, den Servernamen zu überprüfen, speziell bei mehreren Servern im LAN. Wenn man teilweise Batches auch auf lokalen Arbeitsstationen einsetzt, kann man so auch unterscheiden, ob spezielle Netzwerkbefehle angewandt werden können (NCOPY, PURGE usw)

**USER** [USERCFG.BAT, USERSET.BAT, LOGIN.EXE]

Diese Variable enthält den Benutzernamen. Damit kann man z.B. Programme mit dem Benutzernamen (MAIL o.a.) starten. Dies ist jedoch keine SICHERE Möglichkeit, da jeder Benutzer diese Variable auf der Dosebene selbst ändern könnte.

**GRUPPE1 - GRUPPE4** [USERCFG.BAT, USERSET.BAT]

Diese Variablen enthalten die Windowsgruppen, welche der entsprechende Benutzer zusätzlich zu AUTOSTAR und NETZWERK bekommt. Die PROGMAN.INI wird passend dazu zusammengebaut. Der Eintrag lautet auf LEER, wenn diese Gruppe nicht nötig ist.

**PCNUM** [PCSET.BAT, PCCFG.BAT]

Diese Variable enthält die eindeutige Nummer der PC's im LAN. Sie kann z.B. für TCP/IP benutzt werden oder andere Applicationen unterstützen.

**MACHINE** [LOGIN.EXE]

Diese Variable wird aus Kompatibilitätsgründen zum IBM-Lan (Netbios) mitgeführt, da sehr viele Programme diese Variable benutzen um den Benutzer bzw. den PC zu bezeichnen

**NODE** [LOGIN.EXE]

Diese Variable enthält die Netzwerkkartennummer, um den PC genau bestimmen zu können und z.B. den Start von Gatewayprogrammen auf bestimmte PC's zu begrenzen.

**VIDEO** (PCSET.BAT, PCCFG.BAT)

Diese Variable enthält den Grafikkartentyp. Früher haben die Einträge HGC, CGA, EGA, VGA gereicht. Da heute z.B. Windows 3.1 viele unterschiedliche erweiterte Modi unterstützt, muß man diese Variable genauer angeben, z.B. VGA162x, VGA163X, VGA164X für die verschiedenen Auflösungen einer VGA-Karte.

**PRINTER** (PCSET.BAT, PCCFG.BAT)

Die Zuweisung eines „default“-Druckers unter Windows erfolgt PC-abhängig. Damit ist gewährleistet, daß der Benutzer an dem betreffenden PC seine Ausdruck an dem räumlich nächsten Drucker, oder dem der Station zugeteilten Drucker erhält. Die Umgebungsvariable wird in der PCCFG.BAT spezifiziert und in der PCSET gesetzt. Das Programm PRINTSET in der Autostartgruppe von Windows wertet diese Variable aus und veranlaßt die Einrichtung der Treiber, Ports und Queues.

**WINPMT** [LOGIN.EXE]

Diese Umgebungsvariable enthält das Aussehen den Prompts einer DOS-Box unter Windows. Sie ist das Gegenstück zu PROMPT unter Dos. Die Variable wird im SystemLoginScript für alle Benutzer und Arbeitsstationen gesetzt.

**DEBUG** [LOGIN.EXE]

Diese Variable kann man nutzen, um Batchjobs auch "sichtbar" ablaufen zu lassen, ohne den Batch zu ändern. Denn MS-DOS kann nicht erkennen, wenn ein Batchfile während der Ausführung von einer anderen Station geändert wird. Die Reaktion ist nicht vorhersehbar. Daher bietet es sich an, z.B. Ausgaben nicht fest nach NUL: umzuleiten, sondern nach %DEBUG% oder man benutzt diese Variable zum Abfragen z.B. mit IF %DEBUG%=NO goto  
Wenn man sich bei DEBUG auf reguläre Devices beschränkt (CON: COM1: usw), dann kann man in Batchjobs direkte Ausgaben mit CTTY %DEBUG% abbiegen. Allerdings ist eine Ausgabe in Dateien nicht möglich, dafür aber z.B. die "Kontrolle" über die serielle Schnittstelle.

Bei all diesen Variablen gilt, daß sie nicht SICHER sind, da sie jederzeit vom Benutzer geändert werden könnten.



## 11.9 remote Login für Außendienst

Solange ein PC direkt an das Netzwerk angeschlossen ist, kann der Benutzer problemlos auf seine Daten und Anwendungen zugreifen. Es wird aber oft spezielle Personen geben, die des öfteren "außer Haus" arbeiten und trotzdem auf Daten im Netzwerk zugreifen müssen. Dazu müssen diese Personen eine Verbindung mit dem Netzwerk mittels Telefonleitungen herstellen. Dazu muß ein PC am Netzwerk möglichst 24 Stunden laufen und für diesem Personenkreis erreichbar sein. Diese Anwender brauchen ihrerseits ein Modem und einen PC um den Zugang zu erhalten. Damit dieser Zugang nicht mißbraucht wird, sind Zugangskontrollen nötig. Auch gibt es verschiedene Möglichkeiten, auf Daten im Netzwerk zuzugreifen.

### 11.9.1 Sicherheit

Jeder Zugang zu einem Netzwerk über Telefonleitungen ist eine potentielle Sicherheitslücke. Im Gegensatz zu Computern im Haus gibt es über Telefonleitung keine Zugangskontrolle. Dafür sind jedoch andere Funktionen vorhanden, um die Sicherheit zu erhöhen.

#### Spezielle Software

Alle Produkte benutzen eine eigene Software mit eigenem Protokoll, so daß Eindringlinge mit einer einfachen Terminalemulation nicht weiterkommen.

#### Password

Selbst wenn die passende Software verfügbar sein sollte, so ist in den meisten Fällen ein Zugangspasswort die nächste Hürde. Aber all dies kann verraten werden und stellt noch keinen absoluten Schutz dar.

#### Rückruf

Die eingesetzten Produkte erlauben es, einen Rückruf zu programmieren, d.h. der Verbindung wird nach Austausch der relevanten Daten zur Erkennung des Anrufes unterbrochen. Darauf wählt der Rechner am Netzwerk eine vorher eingetragene Telefonnummer an. Damit kann ein Eindringling selbst nach Kenntnis von Software und Password keine Verbindung aufbauen. Zudem muß der Mitarbeiter keine Telefonabrechnung machen, da durch den Rückruf alle weiteren Einheiten durch die Firma gezahlt werden. Durch diese Methode ist jedoch die Einsatzfähigkeit eines reisenden Mitarbeiter, welcher vom Hotel oder vom Kunden aus anruft, eingeschränkt.

#### Netzwerkpassword

Außer bei der Verbindung mittels EMail steht die letzte Hürde immer noch bevor. Durch "Fernsteuersoftware" oder "Remote Lan-Anbindung" erhält man zwar das LOGIN-Verzeichnis des Servers, jedoch muß man normal als User anmelden, d.h. eine Kennung und das dazugehörige Password kennen. Dann hat man aber immer nur die Rechte des Users unter dem man sich angemeldet hat.

### 11.9.2 MAIL-Verbindung

Die einfachste Möglichkeit ist die Verbindung mittels Mail. Der Benutzer selbst hat keinen direkten Durchgriff auf das LAN. Aber er kann mittels EMail Nachrichten an Mitarbeiter im Haus versenden und umgekehrt Daten empfangen. Dazu ist jedoch auf der Netzwerkseite eine Person oder ein Programm nötig, welche die Anfragen bearbeitet und die Antworten zurückschickt. Es sind keine interaktiven Programme benutzbar. Diese Verbindung hat jedoch den Vorteil, daß die Telefonverbindung nur zum Austausch der Mitteilungen besteht und damit kostengünstig ist. Zudem kann ein vielleicht vorhandener EMailrechner, dessen Modem und der Telefonanschluß benutzt werden. Auch kann sich so fast keine fremde Person einwählen, da niemals ein direkter Durchgriff auf das Netzwerk erfolgt, sondern immer nur die MTA-Software (Mail Transfer Agent) die Verbindung aufbaut und unterhält.

Beispiele dafür sind MS-MAIL remote, MHS personal edition oder CC-MAIL-MTA. Diese Programme "unterhalten" sich mit den passenden Gegenstellen am Netzwerk mit einem eigenen Protokoll. Ein Durchgriff auf die LAN-Verzeichnisse ist nicht möglich.

### 11.9.3 Fernbedienung

Die zweite Variante zum Remotezugang ist die Möglichkeit, über eine Modemverbindung einen PC am Netzwerk fernzusteuern, d.h. Bildschirmausgaben werden über die Telefonverbindung zum remote PC

gesendet, welcher die Daten anzeigt. Tastatureingaben gehen zum gesteuerten Rechner am Netzwerk. Dadurch fallen Programmladezeiten sehr kurz aus, da die eigentliche Verarbeitung auf dem Rechner am Netzwerk erfolgt. Solange textbasierende Programme gesteuert werden, sind die Antwortzeiten erträglich. Sobald jedoch Grafikbildschirme übertragen werden, wird die Arbeitsgeschwindigkeit prinzipbedingt sehr langsam. Eine Zwischenlösung bieten hier Fernbedienungsprogramme unter Windows. Der Host sendet dabei nicht das komplette Fenster, sondern nur die Aufbaudaten der Windows-API-Calls, so daß der Remoterechner das Fenster bei sich aufbaut. Dies reduziert etwas die zu übertragende Datenmenge.

Um Daten zum remote PC zu bekommen sind besondere Datenübertragungspakete nötig, da z.B. ein Zugriff auf Laufwerk A: immer auf das Laufwerk des PC's am Netzwerk erfolgt. Jedes Produkt unterstützt daher einen Filetransfer, um Dateien zu übertragen.

Vertreter dieser Programme sind z.B. Carbon Copy, PCanywhere, CloseUp, und Commute (PCTools). Auch der NetWare Access Server mit dem Programm OnLAN gehört dazu.

#### 11.9.4 Telefonleitung als LAN

Eine dritte Variante ist die Möglichkeit, das Netzwerk über die Modemverbindung zu führen. Der Rechner am Netzwerk funktioniert dazu als Umsetzer oder Router. Der remote PC benutzt die serielle Schnittstelle als LAN-Karte. Diese ist in der Geschwindigkeit natürlich nicht mit einer Ethernet-LAN-Karte vergleichbar. Die Bearbeitung der Programms erfolgt damit auf dem remote PC. Wird ein Programm vom Netzwerkserver geladen, so entstehen lange Wartezeiten, da alle Daten über die Modemverbindung laufen. Daher eignet sich diese Methode eher dazu, Programme von der lokalen Festplatte zu laden, und das LAN nur für Daten und andere Pakete zu benutzen. z.B. für Terminalemulationen über TCP/IP. Zu beachten ist, daß der Rechner am Netzwerk eine Filterfunktion haben muß, da die Modemverbindung um ein vielfaches langsamer als das LAN ist.

Produkte, welche nach diesem Prinzip arbeiten sind z.B. Shiva NetModem/E oder RLN.

##### Shiva NetModem /E

Shiva NetModem /E besteht aus einem Modem, welches nur einen Netzwerkanschluß, einen Telefonanschluß und eine Stromversorgung hat. Ein gesonderter PC ist am Netzwerk nicht nötig. Die Software für den remote PC erlaubt es, die serielle Schnittstelle als LAN-Karte zu benutzen. Konfiguriert wird das Modem über das Netzwerk (IPX) durch die mitgelieferte Software. Das NetModem/E ist nur in der Lage, IPX zu routen. Mit zwei NetModem/E's kann man einfach einen Router zwischen zwei Netzwerken aufbauen. Zudem kann das Modem auch zu Dial-Out und Dial-In-Verbindungen genutzt werden. Ein passender Treiber erlaubt es, daß jeder PC am Netzwerk über IPX das Modem belegen kann, als wäre es direkt an seinem seriellen Port angeschlossen (INT14). Auch Windows wird unterstützt. Der COM-Treiber blendet dabei sogar die Fontansicht eines normalen Modems mit 8 LED's ein. Das NetModem ist ein V32bis-Modem noch ohne Postzulassung.

##### RLN (Remote Lan Node)

RLN (Remote Lan Node) benötigt einen dedizierten PC am Netzwerk und kann über diesen mehrere Modems betreiben, so daß sich gleichzeitig mehrere Personen einwählen können. Dieser dedizierte PC fungiert als Router. Dabei ist RLN nicht auf IPX als Protokoll beschränkt. Zumindest das Routing von IP ist möglich, inwieweit auch NETBEUI (LanManager) oder NBP (3COM) unterstützt werden konnte ich nicht testen. Auf dem remote PC steht sowohl NDIS-, ODI- und ein Packetdrivermodul zur Verfügung. Damit sollte jede Applikation über RLN auf Daten im Netzwerk zugreifen können. RLN komprimiert selbst die Daten über die Modemleitung und optimiert die Daten, so daß mehr Daten übertragen werden, als die Nettoübertragungsrate. Die Verbindung kann auch unter Windows 3.1 benutzt werden. Die Sicherheit stellt ein Passwort, eine Rückrufoption und ein Dongle sicher. Der RLN-Server braucht zwingend den Dongle (=Kopierschutz). Auf der Workstationsseite kann er durch Konfiguration des Server gefordert werden. So läßt sich die Sicherheit auch dann gewährleisten, wenn die Rückrufoption nicht möglich ist (Außerdienst im Hotel oder beim Kunden).

##### NetWare CONNECT

NetWare CONNECT ist ein universelles Kommunikationsmodul. Es ist serverbasierend als NLMs eingebunden und unterstützt alle Schnittstellen, welche über das AIO-Interface angesteuert werden können. Dazugehören normale Modems, X.25 und ISDN. NetWare CONNECT erlaubt es Außenmitarbeitern sich in das LAN über Telefonleitung anzumelden. Dabei dient die COM-Schnittstelle quasi als 19200 BAUD-Lan.

Weiterhin erlaubt es Benutzern am LAN selbst mittels NASI-Schnittstelle oder darauf aufgesetzter INT14-Schnittstelle die Modems am Server zum DIAL-OUT als auch DIAL-IN zu verwenden.

**Tabelle 2 Fernwartungsprodukte**

Produkt	Funktion	Medium	Treiber
<b>Carbon Copy PCAnywhere CloseUp NAS u.a.</b>	Fernbedienung der Station im Netzwerk, d.h. Tastatureingaben und Bildschirmausgaben werden übertragen	Modem (ISDN über AT-Emulation)	entfällt
<b>RLN</b>	DFÜ-Strecke als verlängerte Netzwerkkarte	Modem	Packet, NDIS; ODI
<b>Shiva NetModem</b>	DFÜ-Strecke als verlängerte Netzwerkkarte	Modem	IPX
<b>ISDN-Bridge</b>	DFÜ-Strecke als verlängerte Netzwerkkarte	ISDN-Karte	ODI ua
<b>NetWare CONNECT</b>	Remote Lan, ModeServer, DialIn	Mode, X.25, ISDN	ODI, INT14, NASI

### 11.10 Notebooks

Ein Benutzer eines Notebooks bzw Laptops nimmt für gewöhnlich seine Daten und Programme auf der lokalen Harddisk mit. Wird dieser PC an ein LAN angeschlossen (Netzwerkkarte in der Stationbox oder Pocketadapter) so muß ein Konzept entworfen werden, damit keine Konflikte der beiden Arbeitsumgebungen (standalone und Netzwerk) entstehen. Ein Login im Netzwerk führt für gewöhnlich zu einer Änderung der Suchpfade und Laufwerksbuchstaben und damit zu einer anderen Umgebung der Programme auf der lokalen Festplatte. Weiterhin soll es möglich sein, daß der Benutzer Anschluß an die E-Mail, an die Netzwerkdrucker und weitere Netzwerkdienste hat. Die einfachste Realisierung trennt die Programmbereiche "Netzwerk" und "lokale Festplatte" komplett ab, d.h. der Benutzer arbeitet entweder voll lokal oder voll im LAN. In der Regel sind alle Programme seines Notebooks auch im LAN verfügbar. Einzig das Datenhandling muß der Benutzer selbst gestalten, d.h. das Hin- und Herkopieren der Datenfiles (\*.DOC, \*.XL\*, \*.TXT, \*.DBF u.s.w.). Es hat sich gezeigt, daß der Benutzer besser im LAN arbeitet und die für unabhängiges Arbeiten benötigten Dateien kopiert. Damit stehen die Mehrzahl seiner Dateien auf dem Server und sind damit sicher (Backup, Diebstahl).

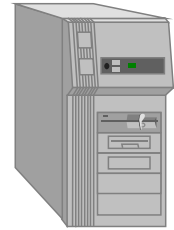
#### 11.10.1 Notebookserver

Hat der Benutzer des Notebooks einen weiteren Desktop im Büro, z.B. wegen der großen Tastatur und des Bildschirms, dann ist es zu überlegen, ob der Notebook nicht komplett als „Festplatte“ eingerichtet wird, wenn der Benutzer in der Firma ist, d.h. die Arbeit wird auch dem Desktop erledigt und die Daten werden auf die „remote“-Platte auf dem Notebook kopiert. Dazu ist es nicht notwendig, daß der Benutzer am Notebook selbst arbeitet. Der Notebook wird dazu nur eingeschaltet, ein Serverprogramm gestartet und die Stromversorgung als auch das Datenkabel eingesteckt. Damit ist die Aufladung gesichert, der Notebook belegt keinen Platz auf dem Schreibtisch und die Daten sind trotzdem voll im Zugriff.

#### 11.10.2 Dockingunit

Fehlt eine zusätzliche Desktopstation, so ist zu überlegen ob eine Dockingunit oder ein Anschlußboard für den Notebook die Verbindung zum LAN und damit allen anderen Diensten herstellen kann. Auf jeden Fall sind Lösungen mit „Pocketadaptern“ nur eine Übergangslösung, da die Anzahl der Steckverbindungen und die Geschwindigkeit die Arbeit nicht erleichtern. Auf jeden Fall sollte ein zusätzlicher Monitor und eine Tastatur verfügbar sein. Ein PC im Lan muß auch in dieser Hinsicht benutzerfreundlich sein, denn viele Investitionen in das Lan (Fax, Mail, Server) rechnen ist eher, wenn die Benutzer auch die Möglichkeiten nutzen.

## 12 Fileserver (NetWare 3.x)



Der Fileserver ist das Herz des gesamten Netzwerkes und muß ausreichend für die angeschlossenen Arbeitsstationen ausgestattet werden. Die Sicherheit und Funktionstüchtigkeit wird durch mehrere Punkte ermöglicht:

- Duplexing  
Zwei Festplatten werden mit zwei Kontrollern angeschlossen. Damit ist beim Ausfall einer Festplatte oder eines Controllers der Betrieb sichergestellt. Zudem erhöht sich die Performance
- mehrere LAN-Karten  
Durch den Einbau mehrerer LAN-Karten kann man selbst beim Ausfall eines Stranges der andere Strang weiterarbeiten. Das Backup und andere Gateways können über die zweite Netzwerkverbindung zugreifen, ohne Last auf den anderen Segmenten zu verursachen.
- USV  
Eine unterbrechungsfreie Stromversorgung erlaubt es, den Server bei kurzen Fehlern im Stromnetz (Ausfall aber auch Unterspannung oder Überspannung) weiterzulaufen. Damit kann der Server auf Daten im Cache noch ohne Verlust schreiben. Zudem erspart man sich das erneute Hochfahren, was weit mehr Zeit in Anspruch nimmt, als das Starten der Workstations. Fehlt die Stromversorgung über längere Zeit, so wird der Server kontrolliert heruntergefahren.
- bewährte Komponenten  
Da der Fileserver nur Dateien verschiebt und z.B. keine aufwendige Grafikkombi vornimmt, kann man auf bewährte Komponenten zurückgreifen. Festplattenkontroller und alle anderen Komponenten garantieren eine fehlerfreie Funktion. Der Einsatz neuer Systeme (EISA, 66MHz) ist für den Fileserver mit der projektierten Benutzeranzahl Benutzern nicht nötig. Die zusammengestellte Komponenten sind vollkommen ausreichend, um das LAN zu bedienen.
- fest definierte Funktion  
Der Fileserver wird NUR als Fileserver benutzt. Auf zusätzlich ladbare Module (Backup, Fax, Mail usw.) wird bewußt verzichtet, damit die volle Leistung dem Benutzer zur Verfügung steht. Durch die Trennung der Funktionen führt ein Ausfall eines Systems nicht zur Beeinträchtigung anderer Systeme.

Beim Server ist zuerst der Aufbau und die Einrichtung der Massenspeicher wichtig. Nicht zuletzt nennt man ihn auch Fileserver. Daß er nebenbei auch Druckjobs und Datenbankabfragen bedienen könnte ändert daran nichts.

### 12.1 Volumeaufteilung

Eine knifflige Aufgabe ist die Partitionierung der Festplatten in die einzelnen Volumes. Netware erlaubt je Festplatte zur Zeit ja nur eine Netwarepartition, jedoch kann innerhalb einer Partition mehrere logische Volumes anlegen. Zu allem Übel kann man ein logisches Volume (z.B. SYS:) über mehrere Festplatten verteilen. Am besten versucht man sich VOR der Aufteilung klar zu machen, weilech Datenmengen in den vorher skizzierten Bereichen (SYSTEM, PROGRAMME, USERDATEN und GRUPPENDATEN) anfallen. Davon hängt es ab, wie groß man welche Bereiche einplant und wie man die Last geeignet auf eventuell mehrere Festplatten verteilt. Denn eines muß man sich immer vor Augen halten: ein Engpaß ist meistens der Diskchannel und die Festplatten. Die Zugriffszeiten sind nun mal physikalisch bedingt und im Millisekundenbereich; für Computer eine verdammt lange Zeit. Hier gilt es auch abzuwägen, ob man je Bereich ein eigenes Volume anlegt oder mehrere Bereiche auf einem Volume ablegt.

#### **Meine Empfehlung: Je Festplatte ein Volume der vollen Größe**

Aber dies ist natürlich nicht immer die optimale Lösung. Dazu sind die Einsatzgebiete eines Fileservers zu unterschiedlich. Um jedem die Entscheidung zu erleichtern, nenne ich einige Überlegungen zur Aufteilung.

Wenn man je Bereich ein Volume anlegt, kann man in die Lage kommen, daß ein Bereich unerwartet wächst. Dann ist es schwer, freien Platz eines anderen Bereichs zu verschieben. Dies geht nur, indem der abgebende Bereich gesichert wird, das Volume gelöscht und neu mit geringerer Größe angelegt wird. Danach muß wieder das Restore laufen. Die freien Blöcke können dann als weiteres Segment dem anderen Volume hinzugefügt werden. Wenn mehrere Bereiche auf einem Volume sind, so ist in dem Fall überhaupt keine Aktion nötig, denn jeder Bereich ist ein Unterverzeichnis auf dem gleichen Volume.

Wenn Gruppen, User und Programme auf einem Volume liegen, kann man als Supervisor mit Filer oder anderen Tools, leicht Daten umgruppieren. Dabei bleiben Directorytrusties bestehen und die Verzeichniseinträge werden "umgehängt" die Daten selbst werden nicht verschoben, was weniger Aufwand bedeutet.

Besondere Beachtung verdient das SYS:-Volume. Dieses Volume ist für NetWare wichtig, da dort alle Daten stehen, welche zum Betrieb nötig sind. Neben der Bindary mit der Betriebsdatenbank (User, Gruppen und andere Objekte) stehen dort auch die weiterhin benötigten NLM's für LAN-Treiber, Protokolle, Diagnose und Toolboxen (CLIB, MATHLIB u.a.) Dieses Volume ist der Regel auch der Platz, an dem der Server die Druckaufträge ablegt. Wenn viel gedruckt wird, oder Drucker oft OFFLINE sind, kommen hier schnell größere Datenmengen zusammen. Daher muß dieses Volume dementsprechend dimensioniert werden.

Wenn man mehrere Bereiche auf ein Volume legt, muß man sichern (Hidden directories oä) daß der User seine Daten nicht unter mehreren Laufwerksbuchstaben ansprechen kann (z.B. F:\USER\ADMIN und H:) Sonst gerät er leicht in Versuchung, vermeintlich doppelte Daten zu löschen. Hat ein User nur Rechte auf SYS:USER\USERNAME, so kann er doch das Verzeichnis SYS:USER sehen, wenn F: auf SYS gemappt ist. Mit FLAGDIR USER HID kann man das Verzeichnis verbergen, aber diverse Tools machen es trotzdem sichtbar. Da hilft dann nur die strikte Vorgabe F: ist das System, da hat kein User was verloren. Im Gegensatz dazu kann man der Sekretärin über F: ja die Möglichkeit geben (im Rahmen der Rechte) auf das Verzeichnis ihres Chefs zuzugreifen. Dann muß man den Benutzern aber auch sagen, daß F:\USER\<USERNAME> mit ihrem H:\ identisch ist.

### Spawning

Die heutige Technologie macht es möglich, 1 bis 2 Gigabyte als eine Festplatte zu erhalten. Sollte dies nicht ausreichen, so kommt man um das Spawning eines Volumes über mehrere Festplatten nicht umhin. Damit gibt man jede Kontrollmöglichkeit aus der Hand, zu wissen, auf welcher Festplatte nun welche Daten liegen. Wenn eine Festplatte nun defekt wird, muß das komplette Volume zurückgesichert werden, d.h. auch die Daten auf den noch intakten Festplatten dieses Volume werden zurückgesichert. Wer diese Konstellation wählt, sollte sehr oft ein Backup machen, oder einen zweiten Festplattensatz parallel (Duplexing) laufen lassen.

Der Vorteil von Spanning ist neben der logisch größeren Festplatte (solange die Clientsoftware damit umgehen kann !!) auch eine Lastaufteilung. Der Server kann sich die Festplatte aussuchen, auf welche er die Daten schreibt. d.h. eine Festplatte, welche weniger zu tun hat, wird wieder belastet. Auch hier erhöht sich dadurch die Performance (load balancing).

Auf der Funktion des Diskspawning arbeiten auch Festplattenarray, d.h. eine logische Festplatte besteht z.B. aus fünf Festplatten, von denen die ersten vier je 2 Bit eines Byte abspeichern; die fünfte Festplatte speichert die Parität, so daß beim Ausfall einer Platte die Daten anhand der fünften Festplatte wiederhergestellt werden können.

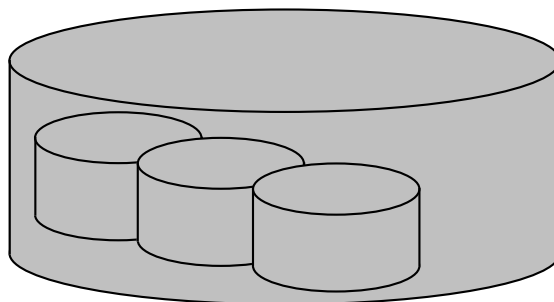


Abbildung 22 Spawning

Ein Betriebssystem, welches bei der Größe der Festplatten an Grenzen stößt, ist der Macintosh, der nur die nur bis 2GB verwalten kann. Allerdings kann man dann für den User eine Begrenzung der

maximal nutzbaren Speicherplatzes auf das Volume einrichten (VolumeRestriction), so daß physikalisch größere Volumes keiner Begrenzung unterliegen.

### Mirroring

Mirroring vermindert die Ausfallzeit, wenn eine Festplatte das Zeitliche segnet, jedoch ist der Performance UNTER dem Betrieb mit nur einer Festplatte. Der einzelne Festplattenkontroller muß die Schreibzugriffe auf beiden Platten ausführen und braucht daher mehr Zeit. Beim Lesen können zwar die Daten von der schnelleren Festplatte kommen, jedoch immer über den gleichen Festplattenbus. Wenn die Mittel zur Verfügung stehen, um zwei Festplatten parallel laufen zu lassen, sollte es am zweiten Kontroller nicht fehlen. In der Regel sind die Kosten für einen Kontroller weit unter denen der Festplatten.

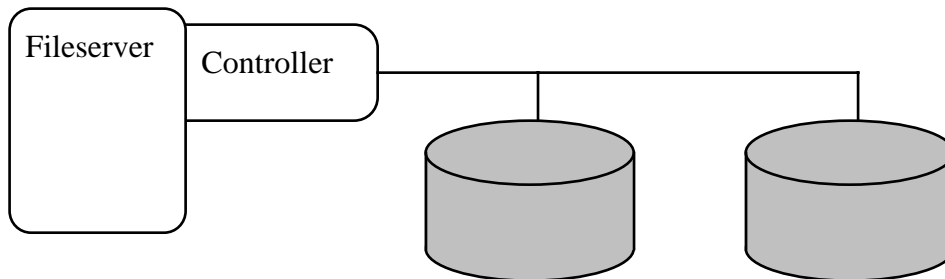


Abbildung 23 Mirroring

### Duplexing

Duplexing selbst bringt neben der erhöhten Sicherheit gegen Festplattenfehler auch einen Geschwindigkeitsvorteil, denn der Server holt sich seine Daten immer von der Festplatte, welche schneller liefern kann, also welche weniger ausgelastet ist oder deren Köpfe sich besser in Position befinden. Zudem kann über beide Festplattenkontroller gelesen bzw geschrieben werden. (load balancing)

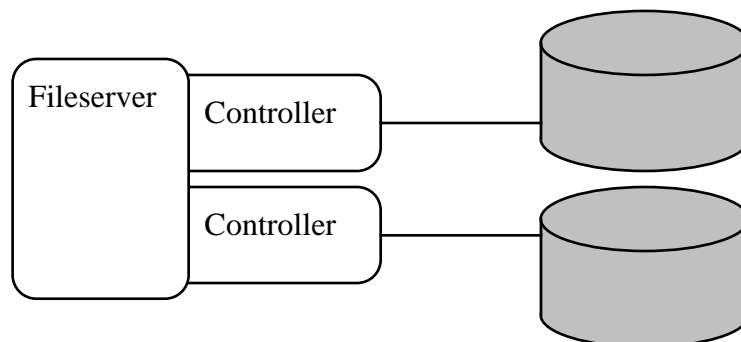


Abbildung 24 Duplexing

## 12.2 Cachekontroller

Den Einsatz von Festplattenkontrollern, die selbst Cachefunktionen anbieten, kann man sich sparen. Den dort eingesetzten Speicher spendiert man besser der Fileserver selbst. Da der Fileserver für seine Aufgabe, mit Dateien zu dienen, optimiert ist, hält er auch große Datenmengen im eigenen Cache. Der größte Teil des Hauptspeichers sollte als Cache benutzt werden. Nur so kann der Server schnell Daten aus dem Speicher statt von den Festplatten holen. Ein dazwischengeschalteter Cache ist wirkungslos, denn all die Daten, welche im Kontrollercache stehen, sind auf jeden Fall auch im Fileserver vorhanden, da sie zuletzt gelesen worden sind. Dadurch wird nur der Weg der Daten von der Festplatte zum Speicher des Servers länger und langsamer.

## 12.3 Konsole schützen

Wenn der Fileserver in Betrieb ist, ist die Fileserverkonsole eine Achillesferse. Im einfachsten Fall kann ein böswilliger Benutzer den Server DOWN-Fahren. Es gibt mehrere Methoden, die Fileserverkonsole zu schützen. Wenn der Schlüsselschalter am Server die Tastatur abschaltet aber ein Hochfahren nach einem Stromausfall erlaubt (PC-Setup!), ist dies der erste Weg. Auch mit abgeschlossenem Keyboard kann der Supervisor (RCONSOLE, ACONSOLE) die Konsole bedienen.

Weiter kann man die Sicherheit mit dem Befehl "REMOVE DOS" erhöhen. Damit wird die COMMAND.COM aus dem Speicher entfernt (Der Speicher wird dem Cache zugeschlagen), so daß der Zugriff auf die Diskettenlaufwerke und DOS-Bereiche der Festplatten ausgeschlossen werden. Dieser Befehl ist nicht mehr umkehrbar. Durch den Verlust auf das A:-Laufwerk ist es dann aber auch nicht mehr möglich, Produkte auf dem Server über dieses Laufwerk zu installieren (z.B. NFS oä). Jedoch lassen sich diese Auch über eine Workstation einspielen.

Der Befehl "SECURE CONSOLE" führt auch einen "REMOVE DOS" aus. Zudem können ab dann NLM's nur noch auf dem Verzeichnis SYS:SYSTEM geladen werden.

Ein nicht empfehlenswerte Methode ist es, die Funktion "LOCK CONSOLE" des MONITOR.NLM zu nutzen. Zwar ist die Konsole dadurch gelockt, jedoch wird auch jede Menge Speicher dem Cache weggenommen. Wahlweise gibt es diverse LOCK.NLM (NetWire), welche eine LOCK-Funktion eleganter erlauben.

## 12.4 BATCHES auf dem Server

Wie es für MS-DOS die Möglichkeit der Batchfiles gibt, so sind auch eingeschränkt auf der Fileserverkonsole Batchfiles nutzbar. Die Endung lautet auf NCF. d.h. eine Befehlsfolge, welche man auf der Konsole eingibt, kann man als NCF-File im SYS:SYSTEM-Verzeichnis ablegen.

### SLIST.NCF

z.B. kann man die Befehle "DISPLAY NETWORKS" und "DISPLAY SERVERS" als SLIST.NCF abspeichern. Der Aufruf SLIST an der Konsole führt dann diese beiden Befehle aus.

### SETRPWD.NCF

Ein weiterer Anwendungsfall ist das Ändern des Passwortes für die RCONSOLE. Diese kann nur beim Laden von REMOTE.NLM angegeben werden, so daß zur Änderung REMOTE entladen werden muß. Dadurch bricht jedoch die Verbindung zur RCONSOLE ab. Dagegen hilft folgender Batch

```
UNLOAD RSPX
UNLOAD REMOTE
LOAD REMOTE <hier das neue PWD eintragen>
LOAD RSPX
```

Danach ist eine neue Verbindung mit RCONSOLE und dem neuen Passwort möglich. REMOTE kann aber auch über das Supervisorpassword erreicht werden.

NetWare selbst benutzt NCF-Files zum Start von Btrieve oder NFS.

## 12.5 STARTUP.NCF

Die STARTUP.NCF liegt auf dem Bootdevice des Fileservers, d.h. entweder auf der Festplatte oder auf der Diskette. Sie dient dazu, den Festplattentreiber zu laden, damit ein Zugriff auf das SYS:-Volume möglich wird. Weiterhin gibt es Serverparameter (SET-Befehl), welche sich nur in dieser Datei auf bestimmte Werte setzen lassen. Sonstige Treiber sollten hier nicht geladen werden. Zusätzliche Treiber und Programme (VREPAIR, INSTALL LAN-Treiber, Protokolle u.s.w) sollten sich natürlich auf dem Datenträger befinden, falls der Server wegen Problemen nicht richtig mountet. Speziell wenn das Backup auf einer Workstation gefahren wird, muß es möglich sein, von Hand die LAN-Treiber zu laden und die Volumes neu anzulegen. Erst dann ist das Restore auch möglich.

### Konfigurationsdatei 19 STARTUP.NCF

```
load AHA1540 port=330
```

Laden des Festplattentreibers

```
set Maximum Physical Receive Packet Size = 1534
set Minimum Packet Receive Buffers = 100
```

Einige Parameter können nur in der STARTUP.NCF gesetzt werden.

Der Server gibt sich auf dem Netzwerk erst dann zu erkennen (d.h. LOGIN ist möglich), wenn er ein SYS:-Volume gemountet hat. Vorher ist ein LOGIN nicht möglich, da der Server keine Bindary anlegen oder lesen kann und damit keine User definiert sind.

Weitere Treiber außer den Festplattentriibern sollten in der AUTOEXEC.NCF geladen werden, wenn alle Voumes gemoutet sind. Wenn zusätzliche NLM's (Datenbank o.a.) geladen werden, bevor alle Volumes gemountet sind, kann es sein, daß nicht alle Volumes gemountet werden, oder die NLM's nicht sauber arbeiten. Speziell sollte man sich hüten, die Zugang über LAN schon zu ermöglichen,



bevor alle zum Betrieb nötigen Volumes gemountet sind. Unter Umständen sind einige Laufwerke für Benutzer noch nicht verfügbar.

## 12.6 AUTOEXEC.NCF

Die Autoexec.NCF wird nach dem Mounten von SYS: aufgeführt. Die ersten beiden Zeilen definieren die Netzwerknummer des internen IPX-Netzwerkes (d.h. welches logisch alle NLM's u.s.w. verbindet) und den Fileservernamen. Beide Angaben müssen EINMALIG auf dem Internet sein. Danach sollte man eventuell zusätzlichen Speicher, sofern nicht automatisch erkannt, anmelden (register Memory). Danach sollten alle benötigten Volumes gemountet werden. Erst wenn dies erfolgt ist, sollen zusätzliche NLM's geladen werden. Die LAN-Protokolle werden geladen, wenn der Server betriebsbereit ist.

### Konfigurationsdatei 20 AUTOEXEC.NCF

```
file server name FC
ipx internal net 13041968
set allow unencrypted passwords = on
set maximum outstanding NCP searches = 600

load KEYB germany
load remote sv
load rspx

load ups type=standalone port=231 discharge=6 recharge=36

load MSM31X
load NE2000 port=300 int=5 frame=ETHERNET_II name=LANA
bind IPX to LANA net=1
```

Netzwerkname und interne IPX-Nummer festlegen. Zusätzliche Parameter setzen

Deutsche Tastaturtreiber und Treiber für die Remoteconsole

UPS-Treiber laden

Netzwerktreiber laden und Protokoll anbinden

## 12.7 Hardware (LAN, I/O, Memory)

Der Fileserver lebt und stirbt mit seinem verfügbaren Hauptspeicher. Denn selbst wenn man die besten und schnellsten Festplatten und Komponenten einsetzt, so ist die doch nicht soviel schneller um 50, 100 oder gar mehr Benutzer zu bedienen. Daraus leitet sich die Forderung nach einem genügend großem Speicher ab.

NetWare hat als Hardwareplattform die überwiegend die Intelprozessoren gewählt. Zwar gibt es "Portable NetWare" und "NetWare für VMS" aber die meisten Installationen werden auf Computern mit den Prozessoren 386 und 486 vorgenommen. Damit sind die meisten Computer zum Industriestandard kompatibel. Dieser wurde jedoch schon vor 1980 begründet, so daß heute noch Grenzen davon verspürbar sind.

Besonders bei den Möglichkeiten der Einstellung von Interrupt und I/O-Adresse sind Grenzen gesetzt.

Es ist jedoch ein Irrglaube, daß ein Fileserver unbedingt ein 486 mit Super-VGA und 50MHz sein muß. Da die Arbeit eines Fileservers hauptsächlich im VERSCHIEBEN von Daten liegt, muß er nicht gut rechnen können, d.h. der mathematisch Koprozessor ist überflüssig, solange kein spezielles NLM's davon Gebrauch macht. Viel mehr Wert sollte auf die Bereiche LAN-Karte und Festplattenkontroller samt Festplatten gelegt werden. Hier ist eine Optimierung anzusetzen.

Weiterhin ist die physikalische Grenze des Netzwerkmediums (Ethernet, TokenRing, ArcNet, FDDI ua) ein Engpaß. Wenn 50 oder mehr PC's an einem Netzwerkstrang und damit an einer LAN-Karte hängen, ist die LAN-Karte und das Übertragungsmedium das schwächste Glied. Bei Ethernet mit einer Übertragungsrates von nominell 10 MBit (ca 4MBit effektiv) kann eine NE2000-Karte maximal ca 700kByte je Sekunde verarbeiten. Hier könnte es helfen, das Netzwerk in mehrere Segmente zu teilen und von eigenen LAN-Karten bedienen zu lassen. Dabei darf man jedoch nicht vergessen, daß ein NetWareserver gleichzeitig auch Router ist. Wenn dann an einem Strang Gateways und Hostrechner hängen, und viele Computer der anderen Stränge darauf zugreifen, wird der Server durch Routing belastet, da alle Pakete durch mindestens zwei LAN-Karten müssen. Die Performance sinkt.

In einem reinen NetWare-LAN mit einem zentralen Server ist das jedoch nicht zu befürchten.

Eine weitere LAN-Karte im Server hat jedoch noch einen weiteren Vorteil. Selbst wenn diese LAN-Karte nur von sehr wenigen Computern benutzt wird (z.B. BACKUP, Supervisor), stellt sie doch einen zweiten Zugang zum Server dar. Wenn der erste Netzwerkstrang nämlich gestört ist, kommt der Supervisor doch noch an den Server heran.

Man gewinnt Interrupts und I/O-Bereiche bei einem Server, indem man auf überflüssige Schnittstellen (serielle und parallele) verzichtet. Dadurch werden z.B. IRQ 3,4,5 und 7 frei. Diese "langsamen" Schnittstellen im Server sollte man nicht unbedingt benutzen, da diese den Server bremsen. Speziell

die serielle Schnittstelle kann bei hoher Last nicht korrekt bedient werden, da sie in der Regel nicht gebuffert ist und damit je empfangenen Zeichen einen Interrupt auslöst.

Für Drucker, welche man gerne am Server anschließt, gibt es besserer Anschlußmöglichkeiten. Nur ein sehr kleinen Netzwerken (bis zu 10 User) kann man auch Drucker am Server anschließen.

### 12.8 NetWare 3.x Speicheraufteilung

Das folgende Kapitel ist aus der Hilfe von MONITOR.NLM abgeschrieben. Anhand des Diagramms kann man gut erkennen, wie NetWare 3.x seinen Speicher zuteilt.

#### 12.8.1 Total Server Work Memory:

Die Angabe bei MONITOR.NLM hierzu zeigt den komplett für NetWare zur Verfügung stehenden Speicher an

#### 12.8.2 Original Cache Buffers:

Wenn der Server gestartet wurde, benutzt er zunächst seinen gesamten freien Speicher zum Caching von Dateien. Wird nun Speicher für andere Zwecke benötigt, wird er diesem Pool entnommen. Die Angabe zeigt die Anzahl der Buffers zum Zeitpunkt 0 des Servers.

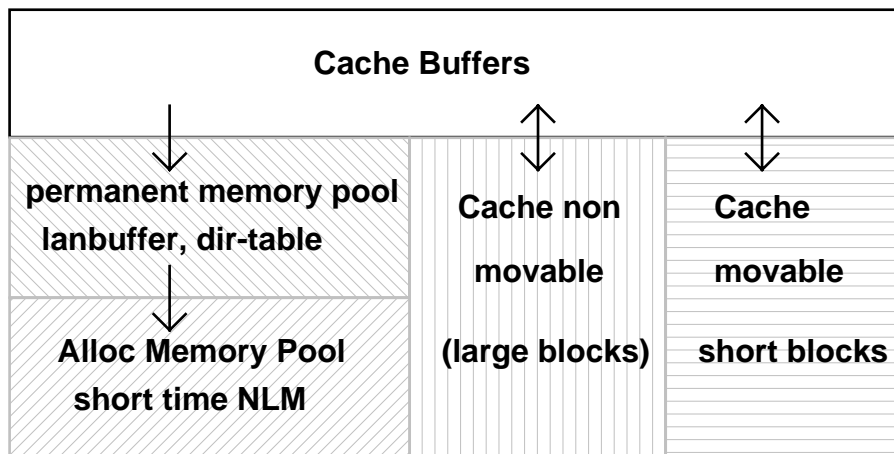


Abbildung 25 NetWare 3.x Speicherbereiche

Die Pfeile deuten an, von welchem Pool Speicher zu anderen Pools verschoben wird.

#### 12.8.3 Permanent Memory Pool:

Dieser Speicher wird von Prozessen benutzt, die den Speicher nicht mehr freigeben. Wird mehr Speicher gebraucht, so wird er von Cachepool entnommen. Der Speicher wird nicht wieder zurückgegeben. In diesem Speicher liegen z.B. Empfangsbuffer für die Netzwerkkarten und Speicher für das Directorycaching.

#### 12.8.4 Packet Receive Buffers:

Diese Buffer enthalten die Requestpakete der Workstations bis diese von den entsprechenden Prozessen abgearbeitet worden sind. Jeder Buffer ist etwas mehr als 1kByte groß. NetWare belegt mehr Puffer, wenn diese gebraucht werden.

#### 12.8.5 Directory Cache Buffers:

Dies ist die Anzahl der verfügbaren Buffer für das Directorycaching. Wenn mehr Buffer benötigt werden, kann NetWare zusätzlich Speicher dafür anfordern. Anders als bei NetWare 2.x muß man damit bei NetWare 3.x keine Angaben zu den maximalen Directoryeinträgen machen.

#### 12.8.6 Alloc Memory Pool:

Dieser Speicher steht all den Prozessen zur Verfügung, welche den Speicher nur für kurze Zeit (.z.B. während der Initialisierung) brauchen. Wird mehr Speicher benötigt, stellt ihn NetWare aus dem

Permanent Memory Pool zur Verfügung. Der Speicher wird nicht mehr zurückgegeben. Dieser Speicher sollte auch von NLM's benutzt werden, welche nur wenig Speicher benötigen.

### 12.8.7 Cache Buffers:

Dieser Speicher steht aktuell zum Filecaching zur Verfügung und sollte größer sein, als einer der anderen Bufferbereiche. Er stellt den Cachebufferpool dar, aus welchem die anderen Speicherbereiche ihren Bedarf decken können. Dieser Speicher sollte die meist benötigten Applikationen im LAN aufnehmen können, damit Plattenzugriffe reduziert werden und damit die Serverperformance steigt.

### 12.8.8 Cache Movable Memory:

Dieser Speicher wird vom Cachepool entnommen und nach Freigabe wieder zurückgegeben. Im Gegensatz zum Cache Non-Movable Memory erlaubt dieser Speicher dem Memorymanager durch die Verschiebbarkeit eine Optimierung der Speicherblöcke im Hauptspeicher. Volumetabellen belegen z.B. diesen Speicher.

### 12.8.9 Cache Non-Movable Memory:

Auch dieser Speicher wird vom Cachepool entnommen und wieder zurückgegeben. Er wird benutzt, wenn größere zusammenhängende Speicherbereiche benötigt werden.

## 12.9 NLM's

NLM's sind zusätzliche Module, welche auf einem Server geladen werden können. Diese können z.B. Datenbankdienste anbieten, damit die eigentliche Datenbank nicht komplett über das LAN übertragen werden muß. (BTRIEVE, SQL), oder statistische Daten ermitteln.

## 12.10 PATCHMAN.NLM

Ein besonderes NLM ist der PATCHMAN.NLM. Er dient dazu, das Betriebssystem zu patchen. Die aktuellsten Informationen sind der jeweiligen Textdatei beim PATCHMAN zu entnehmen.

Der PATCHMAN muß immer DIREKT nach der Angabe der internen IPX-Nummer in der AUTOEXEC.NCF geladen werden. durch Angabe von LOAD PATCHMAN. Die nötigen Patches sollten dann danach geladen werden.

Das Betriebssystem NetWare 3.x. und ladbare Add-on-Produkte (NFS, MAC-namespace usw) kann auf drei Wege modifiziert werden.

### DYNAMISCH

Dynamische Patches sind NLM's, die während der Laufzeit des Servers geladen und entladen werden können. Nach dem Entladen ist das Betriebssystem wieder im Originalzustand

### HALBSTATISCH

Halbstatische Patches können ebenfalls zur Laufzeit der Server geladen werden, jedoch können sie nicht mehr entladen werden. Die Wirkung dieses Patches kann man nur dadurch aufheben, indem der Server neu hochgefahren wird, ohne den Patch zu laden.

### STATISCH

Statische Patches sind Programme, welche unter DOS ausführbar sind und die SERVER.EXE modifizieren. Dieser Patch wird nur einmal aufgerufen und die Änderungen sind dann nicht umkehrbar. Daher sollte man die SERVER.EXE vorher sichern. Es ist nicht empfehlenswert, die SERVER.EXE auf den Originaldisketten zu patchen, aber wer macht das schon. :-)

Dynamische und halbstatische Patches ändern das Betriebssystem im Speicher des Servers und nicht auf der Diskette. Deshalb müssen diese Patches jedes Mal beim Start des Servers geladen werden. Daher sollten die benötigten Patches in der AUTOEXEC.NCF eingetragen werden.

Durch die Eingabe von "PATCHES" auf der Fileserverkonsole ist sichtbar, welche Patches geladen worden sind. Die Patches werden nach ihrem Typ (Statisch, Halbstatisch, Dynamisch) sortiert. Durch die Eingabe von "MODULES" werden neben anderer Module nur die dynamischen Patches angezeigt, aber nicht die halbstatischen oder statischen Patches.

Der PATCHMAN.NLM muß vor dem Laden der dynamischen oder halbstatistischen Patches geladen sein. Wenn er nicht geladen ist, wird der erste Patch versucht, den PATCHMAN nachzuladen. PATCHMAN kann erst dann entladen werden, wenn alle danach geladenen Patches wieder entladen worden sind.

Weitere Informationen zu PATCHMAN.NLM und speziell den einzelnen Patches und deren Auswirkungen auf das Serverbetriebssystem ist in den jeweiligen README-Dateien zu finden.

Die offizielle Quelle für Patches ist die NetWare auf CompuServe (GO NOVLIB oder GO NOVFILES) oder der autorisierte Fachhändler.

### 12.11 VREPAIR

VREPAIR.NLM ist ein Utility, welches auf dem Fileserver gestartet werden kann. Es dient zur Berichtigung von Fehlern auf der Festplatte und wird meistens nur gebraucht, um Inkonsistenzen zu beheben, welche dann auftreten, wenn der Server nicht korrekt DOWN gefahren wird, z.B. Stromausfall, Abend u.a.

Mit VREPAIR können nur Volumes "repariert" werden, welche nicht gemountet sind. Dazu muß der Server hochgefahren werden, ohne daß er versucht die korrupten Volumes zu mounten. Dann läßt man VREPAIR und läßt es über das Volume laufen. Wenn ein zusätzlicher Namespace installiert ist, muß dieser vorher geladen werden. Der Durchlauf kann je nach Festplattengröße mehrere Stunden dauern. Oft sind mehrere Druckläufe nötig. Erst wenn ein Durchlauf OHNE Fehler absolviert wurde, wird der Server das Volume mounten können. Datenverluste sind wahrscheinlich.

VREPAIR.NLM kann vom Netzwerk, von der Festplatte oder von der Diskette geladen werden (kein REMOVE DOS vorher!). Um sicher zu gehen, die aktuelle Version zu nutzen, sollte Vrepair von der Diskette geladen werden. Zumal wenn das SYS-Volume beschädigt ist.

VRepair belegt Teile des Hauptspeicher um die Korrekturen abzulegen. Dieser wird NICHT freigegeben, auch wenn VREPAIR entladen wird. Wenn viel Speicher belegt wurde, kann es sein, daß der Server die Festplatten mangelnden Speicher nicht mountet. Auf jeden Fall empfiehlt es sich, nachdem VRepair ohne Fehler durchgelaufen ist, den Fileserver "down" zu fahren und neu zu starten.

### 12.12 UPS

Eine unterbrechungsfreie Stromversorgung sollte jedem Fileserver spendiert werden. Der Server nutzt seinen Cache auch, um Daten nicht gleich schreiben zu müssen. Ein unerwarteter Stromausfall führt in den meisten Fällen zu Datenverlusten und in schwereren Fällen zu Fehlern auf der Festplatte, welche mühselig mit VREPAIR korrigiert werden müssen. Das UPS.NLM stellt die Verbindung mit der UPS her. Damit kann die UPS dem Server Bescheid geben, daß der Strom ausgefallen ist und der Server noch x Sekunden Zeit hat. Bei einem Stromausfall meldet sich der Server dann bei allen angemeldeten Benutzern, daß er auf Batterie läuft und noch ca X Minuten in Betrieb ist. Wenn der Stromausfall länger als die Haltbarkeit der UPS dauert, so sendet die UPS vor Ende der Batterie erneut die Meldung, daß nun alle Files geschlossen werden sollten. Kurz vor Ende der Batterie wird der Server unter allen Umständen DOWN-gefahren.

Die Zeiten, nach welchen der Server downfährt, werden beim Laden von UPS.NLM angegeben.

Manche Stromversorgungen haben eine gesonderte Leitung, welche getrennt signalisiert, daß die Batteriekapazität zu Ende geht. Wenn dieses Signal eingeht, geht der Server sofort DOWN.

Um eine Tiefentladung der Batterien zu verhindern und einen Neustart bei Wiederherstellung der Stromversorgung zu erlauben, schalten einige UPS den Fileserver danach ab. Dazu gibt der Fileserver über ein entsprechendes Interface die Meldung an die UPS, daß er nun DOWN ist und die UPS abschalten soll, bis die Stromversorgung wieder stabil ist. Nur damit ist sichergestellt, daß der Server auch wieder automatisch gestartet wird.

Mittlerweile gibt es Drittanbieter, welche verbesserte NLM's und Stromversorgungen verkaufen, welche sehr eng zusammenarbeiten, so daß sich auch der Status der Batterie und die Qualität der Stromversorgung ablesen läßt.

### 12.13 Bindery

Neben der STARTUP.NCF und der AUTOEXEC.NCF gibt es weitere SYSTEM-Files, welche NetWare zum Betrieb braucht. Diese Files stehen im Verzeichnis SYS:SYSTEM. Der wichtigste Satz an Dateien ist die Bindery von NetWare. Dies ist die NetWare-eigene Datenbank, in welcher alle "OBJEKTE" gespeichert sind.

Objekte sind z.B. USER, GRUPPEN, PRINTQUEUES, PRINTSERVER, JOBSERVER, FILESERVER, ROUTER. Jedes Objekt hat eine Objekt-ID und Eigenschaften (Properties)

Eigenschaften sind z.B. FULLNAME, PASSWORD, RESTRICITIONS, MEMBER. Und diese Eigenschaften haben Werte (Values). Werte sind Zahlen und Namen. Diese Information steht bei NetWare 3.x in drei Dateien (NET\$BIND.SYS NET\$PROP.SYS, NET\$BVAL\$.SYS)

Wenn ein Fileserver die Bindery nicht öffnen kann (z.B. wenn noch kein SYS-Volume existiert) so ist auch kein LOGIN möglich. Der Server gibt sich auf dem Internet nicht als Fileserver zu erkennen. Wenn das SYS-Volume gemountet wird, öffnet der Server automatisch die Bindery, bzw legt sie neu an.

Die Bindery ist von NetWare dauernd geöffnet und nicht shareable. Dadurch ist dieser Datebank besondere Beachtung beim Backup zuzuwenden. Das Backupprogramm muß in der Lage sein, die Bindery zu schließen, zu sichern und danach wieder zu öffnen. Dazu muß das Programm entsprechende NetWare-Calls benutzen (Teile der Shell NETX). Mittlerweile gibt es PD-Produkte, welche dies machen und die Bindery kopieren. Damit kann sie auch mit normalen DOS-Backupprogrammen gesichert werden.

In der Bindery gibt es STATISCHE und DYNAMISCHE Objekte. Statische Objekte werden in der Bindery auf die Festplatte abgespeichert. Dynamische Einträge sind nur im Hauptspeicher der Servers zu finden. Statische Einträge sind u.a. USER, GRUPPEN, PRINTQUEUES.

Andere FILESERVER, PRINTSERVER, ROUTER u.s.w. sind dynamisch, d.h. sie werden selbständig eingetragen und auch wieder ausgetragen. Beim SLIST liest das Programm die Bindery des aktuellen Server aus, d.h. man sieht alle Server, die in der Bindery des aktuellen Server stehen. Damit kann es passieren, daß man Server noch sieht, obwohl diese gerade ausgefallen sind, oder nicht mehr erreichbar sind. NetWare wertet die Broadcasts im Netzwerk aus, mit denen jeder Server (Fileserver, Printserver u.a.) etwa im Minutentakt ihre Präsenz ausgeben (SAP-Protokoll).

## 12.14 Konsole

Die Konsole des Fileservers dient zur Steuerung des Betriebssystems. Die Möglichkeiten sind sehr begrenzt, da die meisten Aktionen durch Utilities auf der Workstation erledigt werden. Mit der Konsole kann man hauptsächlich Module (NLM's) laden und in geringem Umfang mit MONITOR.NLM auch Daten auswerten.

Nach der Installation des Servers (INSTALL.NLM) ist die Konsole fast nicht mehr nötig. Auf NetWare 2.2 und früher war es möglich, die Konsole als Workstation zu benutzen (non dedicated mode). Bei NetWare 3.x ist dies nicht mehr möglich.

## 12.15 LogBuch und Errordateien

Zur Dokumentation des Servers sollte ein Logbuch geführt werden, in welchem die Arbeiten aufgelistet werden. Dies dient erstens der Kontrolle, wann was von wem gemacht wurde und kann bei der Suche nach Problemen helfe, die ab einem bestimmten Zeitpunkt auftreten.

NetWare selbst führt verschiedene Logdateien mit. Manche davon können abgeschaltet werden. Allgemein sollte man die Logfiles regelmäßig kontrollieren, und zumindest die banalen Meldungen löschen. Von Vorteil ist es, wenn ein Programm, welches .z.B. beim Backup mitläuft, diese Logfiles an den Admin schickt (EMail) und dann löscht.

### <VOLUME>:VOL\$ERR.LOG

Die VOL\$ERR.LOG wird für jedes Volume im Rootverzeichnis angelegt. Hier findet man normalerweise nur die Information, wann dieses Volume gemountet und dismountet. Diese Files sind normalerweise nicht geöffnet und können einfach gelöscht werden. Die Datei kann mit jedem ASCII-Editor bearbeitet werden. Diese Datei enthält auch die Dateifehler beim Mounten, wenn der Server vorher nicht korrekt heruntergefahren wurde.

### <VOLUME>:TT\$ERR.LOG

Dieses File enthält den Bericht zu fehlerhaft abgeschlossenen Transaktionen als ASCII-File. In der Regel passiert das nicht.

Alle Transaktionen werden von NetWare mitgeführt und nur dann mit einem „RollBack“ rückgängig gemacht, wenn die Station dies anfordert oder sich die Station ausloggt oder ausgeloggt wird, ohne vorher einen „End Transaction“ signalisiert zu haben.

**SYS:SYSTEM\NET\$ACCT.DAT**

Diese Datei enthält die aufgelaufenen Accountinginformation, wenn Accounting installiert worden ist. Die Daten sind kodiert gespeichert und werden von Programmen wie PAUDIT ausgelesen.

**SYS:SYSTEM\SYS\$LOG.ERR**

Diese Datei für als ASCII-File alle Fehlermeldungen des Fileservers mit, welche auf der Konsole erscheinen.

Weitere Logdateien werden in der Regel für zusätzlich geladene Produkte (z.B. NFS, NameService) gespeichert.

**Andere Fehlerdateien.****12.16 Patches für den Server**

NetWare 3.x ist sehr lange auf dem Markt. Im Laufe der Zeit haben sich viele Verbesserungen und Korrekturen ergeben. So gibt es zu dem Serverbetriebssystem mittlerweile einige Patches.

Diese Patches von über NetWare erhältlich. Je Serverbetriebssystem gibt es eigene Patches. Einige beheben Fehler des Servers, andere steigern die Performance oder fügen neue Optionen hinzu.

Die Patches können in drei Gruppen unterschieden werden.

**Dynamisch**

Dynamische Patches können zur Laufzeit geladen und entladen werden

**semistatisch**

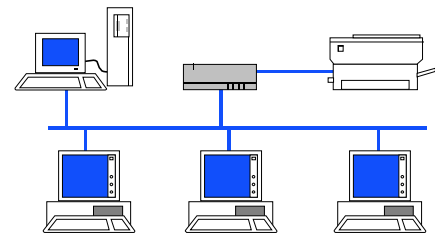
Diese Patches werden zur Laufzeit geladen, können jedoch nicht mehr entladen werden

**statisch**

Diese Patches bedingen eine Unterbrechung des Serverbetriebs. Durch ein DOS-Programm wird die SERVER.EXE direkt gepatcht.

Weitere Information zu Patches finden Sie im Kapitel zum Patchmanager von Novell „PATCHMAN“.

## 13 LANphysik



Dieses Kapitel behandelt die physikalische Komponente des Netzwerkes. Mittlerweile gibt es genügend Unterlagen, um Netzwerkverbindungen zu planen und zu installieren. Für größere Netzwerke empfiehlt es sich, einen in der Installation von LAN-Komponenten erfahrenen Installateur zu beauftragen. Für kleine LAN's, welche dann meistens mit Cheapernet oder Arcnet aufgebaut werden, sind die Hinweise in den Handbüchern zu den gekauften LAN-Karten ausreichend. Damit verzichte ich hier auf die Auflistung von technischen Daten und Komponenten

### **13.1 Kabel, Zugriff, Struktur (AUI, BNC, TP, LWL)**

Um Daten von einem Computer zu einem anderen zu übertragen ist eine Verbindung nötig. Diese kann durch Kabel, Licht oder Funkstrecken erfolgen.

Die Topologie eines LAN's beschreibt die Übertragungswege und Struktur der Verbindungen (Ring, Bus, Stern)

Wenn nun mehrere Computer miteinander kommunizieren, muß es Mechanismen geben, um diese Kommunikation zu steuern, damit keine Störung auftritt. Dies kann dadurch erfolgen, daß feste Verbindungen von Rechner zu Rechner geschaltet werden oder daß die Rechner ein Medium benutzen und durch Zuordnung, Prioritäten oder Zufallsverfahren der Sender bestimmt wird. Zu Verfügung stehen dazu z.B. CSMA/CD, CSMA/CA oder TokenRing

### 13.2 Ethernet frames

Daten über Ethernet werden als Packet übertragen. Dabei gibt es verschiedene Interpretationen für die Bytes. Der Grundaufbau eines Ethernetframes:

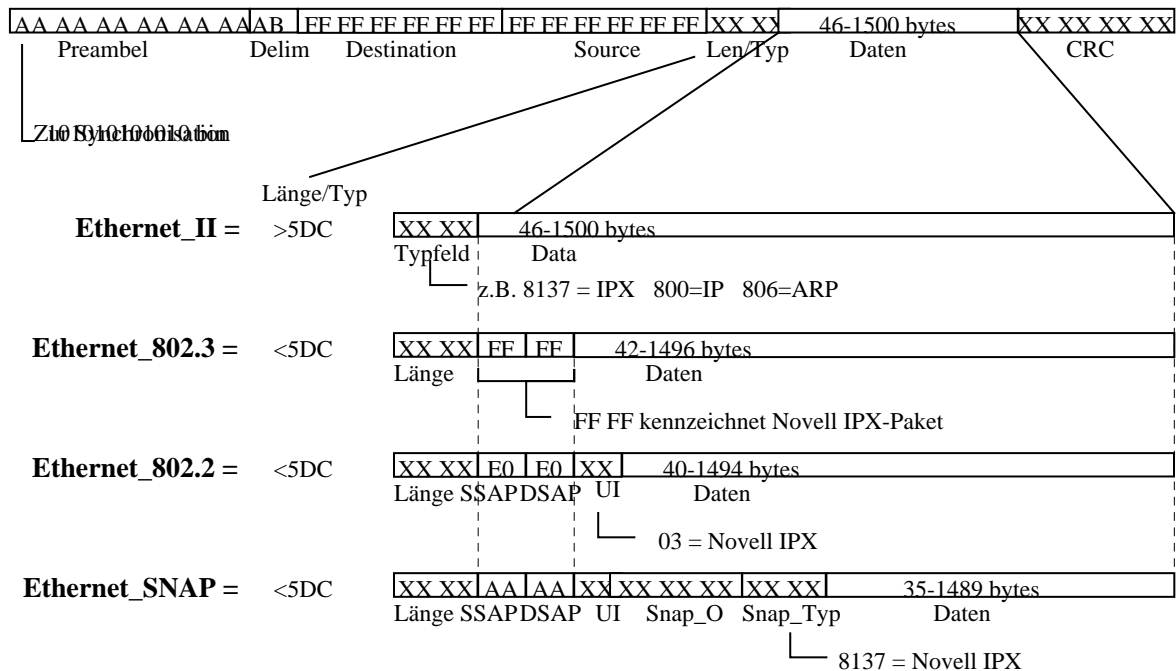


Abbildung 26 Ethernetpaket

Tabelle 3 Ethernetpaketfelder

Feld	Beschreibung
Preamble	Die Preamble besteht aus 7 Oktetten mit dem Wert AAhex (=101010101010). Mit diesem Wechselsignal ist es den Netzwerkkarten möglich, sich auf den Sendetakt zu synchronisieren
Delimiter	Die Preamble wird durch einen Rahmenbegrenzer (ABh) abgeschlossen. (ABh)
Destination	Zieladresse (Netzwerkkartennummer) Eine Zieladresse mit den Werten FF FF FF FF FF FF ist ein Broadcast an alle Stationen.
Source	Absender (Netzwerkkartennummer)
Len/Typ	Angabe der Länge bzw des Typfeldes. kleiner 1500dez=5DChex -> Längenangabe des Frames. Die darauf folgenden Bytes größer 1500dec=5DChex -> Typfeld Alle dahinter folgenden Bytes sind Nutzdaten
SSAP	Source ServiceAccessPoint
DSAP	Destination Service Access Point
UI	Unnumbered Information
Snap_O	SNAP Organisation
Snap_type	SNAP Ethernet type
Daten	Die eigentlichen Nutzdaten
CRC	32bit Prüfsumme CRC



### 13.2.1 Einsatzbereiche der Frames

Tabelle 4 Frametypen

Frametyp	Verwendung
Ethernet_802.3 (Standard)	Das Standardframe für Novell. Sollte auf Netzwerken mit nur einem Protokoll eingesetzt werden. War früher das Standardframe von Novell
Ethernet_II	Weist einen eindeutigen Paketkopf (type code) zu. Einsatz erfolgt, wenn mehrere Protokolle (DECnet, TCP/IP) auf dem LAN eingesetzt werden
Ethernet_802.2	Weist den IEEE und OSI Standardframetyp zu. neuerer Frametyp als Weiterentwicklung von Ethernet_II. Ist unabhängig von dem Medium (Ethernet, TokenRing, ISDN etc). Die Protokollkennung liegt in einer höheren OSI-Schicht.
Ethernet_Snap	Wird auf Netzwerken eingesetzt, welche mit TCP/IP fahren (vorwiegend TokenRing)

Ein Frame ist eine Variation eines Protokolls, wie z.B. Ethernet\_II, Ethernet 802.3, Ethernet 802.2, Ethernet SNAP, IBM\_Token-Ring, oder IBM\_Token-Ring\_SNAP.

Ethernet II Frames enthalten eine festgelegte protocol ID oder PID, welche das IEEE 802.3 frames nicht besitzt.

Stationen, welche unterschiedliche Standards benutzen, sollten nicht auf dem gleichen LAN existieren. Die Funktion und Auswertung der Frames beansprucht beim Einsatz unterschiedlicher Frametypen mehr Rechnleistung bei allen Empfängern. Stationen mit unterschiedlicher Protokollnummer auf einem Ethernet\_II System können parallel betrieben werden, können aber nicht miteinander kommunizieren.

NetWare hat lange das IEEE 802.3-Frame benutzt. Beim Einsatz mit TCP/IP sollte das Ethernet\_II-Frame eingesetzt werden (ECONFIG.EXE). Mit dem Einsatz von NetWare 4.x und an Anlehnung an OSI-Frames soll man NetWare in Zukunft mit dem 802.2-Frame benutzen. Alle neu ausgelieferten Treiber benutzen per Default 802.2. Wenn man weiterhin das alte Frame benutzen möchte muß dies jetzt explizit angegeben werden (NET.CFG)

Alle Router, Bridges und anderer aktive Komponenten müssen den eingesetzten Frametyp unterstützen, sonst ist die Kommunikation über diese Komponenten hinaus nicht möglich.

NetWare weist beim Ethernet\_II-Frame die PID 8137 für IPX zu. Mit dem Befehl PROTOCOL kann man auf dem Fileserver die benutzen Protokolle anzeigen lassen.

### 13.2.2 DOS-Client. Support der Frames

Tabelle 5 Treibersupport für Frames

	DOS treiber	DOS ODI treiber	NDIS	Packet
Ethernet_802.3	Ja	Ja		
Ethernet_II	Ja	Ja		
Ethernet_Snap	nein	Ja		
Ethernet_802.2	nein	Ja		

### 13.2.3 Die wichtigsten Protocol-ID's im Überblick

Tabelle 6 Typfelder je Protokoll

Framename	IPX	IP	AR	RAR	Apple	SNA
			P	P	talk	P

ETHERNET_802.2	E0	06/A			AA
		A			
ETHERNET_802.3					
ETHERNET_II	8137	800	80	803	809B
			6	5	
ETHERNET_SNAP	8137				
TOKEN-RING	E0				
TOKEN-RING_SNAP	8137				
IBM_PCN2_802.2	E0				
IBM_PCN2_SNAP	8137				
NOVELL_RX-NET	FA				

Für 802.2 und Ethernet\_II folgen ausführlichere Tabellen.

### 13.2.4 Ethernet\_802.2 SAP-Kennungen LLC

Tabelle 7 SAP-Kennungen

SAP	Beschreibung
00	Management
01	Unknown
02	Individual LLC sublayer management
03	Group LLC sublayer management
04	SNA Path Control
06	Internet IP
0E	Proway-LAN
42	Spanning tree
4E	EIA-RS 511
5E	ISI IP

SAP	Beschreibung
80	3Com XNS
8E	Proway-LAN
AA	TCP/IP SNAP (Ethernet type in LLC)
BC	Banyan VINES
E0	Novell IPX
F0	IBM NetBIOS
F4	IBM LAN Management
FC	RPL
FE	ISO DIS 8473
FF	Broadcast

### 13.2.5 Ethernet\_II Packettypen

Tabelle 8 Ethernet\_II-IDs

Frame-ID	Beschreibung
0600	XNS
0601	XNS Address Translation
0800	DOD IP
0801	X.75 internet
0802	NBS internet
0803	ECMA internet
0804	Chaosnet
0805	X.25 Level 3
0806	ARP
0807	XNS Compatibility
081C	Symbolics private
0888	Xyplex
0889	Xyplex
088A	Xyplex
0900	Ungermann-Bass net debugr
0A00	Xerox PUP
0A01	Xerox PUP Address Translation
0BAD	Banyan Systems
0BAF	Banyan Echo
1000	Berkeley trailer negotiation
1001-100F	Berkeley trailer encapsulation
1234	DCA - Multicast
1600	VALID system protocol
1989	Artificial Horizons (dogfight simulator)
3C00-3C0D	3Com NBP
4242	PCS Basic Block Protocol
4321	THD - Diddle
5208	BBN Simnet Private
6000	DNA experimental
6001	DNA Dump/Load -MOP-
6002	DNA Remote Console -MOP-
6003	DNA IV Routing Layer

Frame-ID	Beschreibung
6004	DEC: Local Area Transport
6005	DEC: Diagnostics
6006	DEC: Customer Use
6007	DEC: LAVC
6008	DEC Unassigned (AMBER?)
6009	DEC Unassigned (MUMPS?)
6010-6014	3Com
7000	Ungermann-Bass download
7001	Ungermann-Bass NIUs
7002	Ungermann-Bass diagnostic/loopback
7003	Ungermann-Bass
7005	Ungermann-Bass Bridge
7007	OS/9 Microware
7009	OS/9 Net ?
7020-7029	Sintrom (was LRT)
7030	Racal-Interlan
7031	Prime NTS
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T/Standford
8010	Excelan
8013	Silicon Graphics diagnostic
8014	Silicon Graphics network games
8015	Silicon Graphics
8016	Silicon Graphics XNS Nameserver
8019	Apollo DOMAIN
802E	Tymshare
802F	Tigan
8035	Reverse ARP
8036	Aeonic Systems

Frame-ID	Beschreibung	Frame-ID	Beschreibung
8038	DEC: bridge	80A4 - 80B3	Siemens Gammasonics
8039	DEC: DSM/DDP	80C0-80C3	DCA: Data Exchange Cluster
803A	DEC: (Argonaut console ?)	80C6	Pacer Software
803B	DEC: (VAXELN ?)	80C7	Appplitek Corp.
803C	DEC: (NMSV? DNA Naming?)	80C8-80CC	Intergraph Corp.
803D	DEC: encryption	80CD/80CE	Harris Corporation
803E	DEC: distributed time service	80CF-80D2	Taylor Instrument
803F	DEC: LAN Traffic Monitor	80D3/80D4	Rosemount Corp.
8040	DEC: NetBIOS Datagrams	80D5	IBM SNA Service on Ethernet
8041	DEC: Local Area System Transport	80DD	Varian Associates
8042	DEC Unassigned	80DE/80DF	TRFS (Integrated Solutions ...)
8044	Planning Research Corp.	80E0-80E3	Allen-Bradley
8046/8047	AT&T	80E4-80F0	Datability
8048	DEC: DECamds	80F2	Retix
8049	ExperData	80F3	AppleTalk AARP
805B	VMTP/RFC-1045	80F4	Kinetics
805C	Stanford V Kernel, version 6.0	80F5	Kinetics
805D	Evans & Sutherland	80F7	Apollo Computers
8060	Little Machine	80FF-8103	Wellfleet
8062	Counterpoint Computers	8107-8109	Symbolics
8065/8066	University of Mass. at Amherst	812B	Talaris
8067	Veeco Integrated Automation	8130	Waterloo Microsystems
8068	General Dynamics	8131	VG Laboratory Systems
8069	AT&T	8137	Novell NetWare
806A	Autophon	8138	Novell ?
806C	ComDesign	8139-813D	KTI
806D	Compugraphic Corp.	814C	SNMP over Ethernet
806E-8077	Landmark Graphics Corp.	814F	Technically Elite Concepts
807A	Matra	817D	XTP
807B	Dansk Data Elektronik	81D6	Lantastic
807C	Merit Internodal	8582	Kalpana
807D-8080	Vitalink Communications	8888	HP LanProbe ?
8081-8083	Counterpoint Computers	9000	Loopback
8088-808A	Xyplex	9001	3Com: XNS Mngmt
809B	EtherTalk (AppleTalk)	9002	3Com: TCP/IP Mngmt
809C-809E	Datability	9003	3Com: loopback detection
809F	Spider Systems	AAAA	DECNET ???
80A3	Nixdorf	FF00	BBN VITAL-LanBridge

### 13.2.6 Herstellerkennung von Ethernetkomponenten

Hersteller von LAN-Komponenten nur deren Code in den ersten drei Bytes der MAC-Adresse

Tabelle 9 Herstellerkennung Ethernet

Adressteil	Hersteller	Adressteil	Hersteller
00-00-02	BBN	00-00-6E	Artisoft
00-00-0C	Cisco	00-00-77	MIPS/Interphase
00-00-0E	Fujitsu	00-00-78	Labtam
00-00-0F	NeXT	00-00-7A	Ardent
00-00-10	Sytek/Hughes LAN Systems	00-00-7B	Research Machines
00-00-11	Tektronics	00-00-7D	Cray Research/Harris
00-00-15	Datapoint	00-00-7F	Linotronic
00-00-18	Webster	00-00-80	Dowty Network Services
00-00-1A	AMD ?	00-00-81	Synoptics
00-00-1B	Novell/Eagle Technology	00-00-84	Aquila ?
00-00-1D	Cabletron	00-00-86	Gateway
00-00-20	Data Industrier AB	00-00-89	Cayman Systems
00-00-21	SC&C	00-00-8A	Datadhouse Information Systems
00-00-22	Visual Technology	00-00-8E	Jupiter ? Solbourne ?
00-00-23	ABB	00-00-93	Proteon
00-00-29	IMC	00-00-94	Asante
00-00-2A	TRW	00-00-95	Sony/Tektronics
00-00-3C	Auspex	00-00-97	Epoch
00-00-3D	ATT	00-00-98	CrossCom
00-00-44	Castelle	00-00-9F	Ameristar Technology
00-00-46	Bunker Ramo	00-00-A0	Sanyo Electronics
00-00-49	Apricot	00-00-A2	Wellfleet
00-00-4B	APT	00-00-A3	NAT
00-00-4F	Logicraft	00-00-A4	Acorn
00-00-51	Hob Electronic	00-00-A5	Compatible Systems Corporation
00-00-52	ODS	00-00-A6	Network General
00-00-55	AT&T	00-00-A7	NCD
00-00-5A	SK/Xerox	00-00-A8	Stratus
00-00-5D	RCE	00-00-A9	Network Systems
00-00-5E	IANA	00-00-AA	Xerox
00-00-61	Gateway	00-00-C0	Western Digital
00-00-62	Honeywell	00-00-C9	Emulex
00-00-65	Network General	00-AA-00	Intel
00-00-69	Silicon Graphics	00-DD-00	Ungermann-Bass
00-00-6B	MIPS	00-DD-01	Ungermann-Bass

Adressteil	Hersteller
02-07-01	MICOM/Interlan
02-60-8C	3Com
08-00-02	3Com-Bridge
08-00-05	Symbolics
08-00-06	Siemens Nixdorf
08-00-07	Apple
08-00-09	HP
08-00-0A	Nestar Systems
08-00-0B	Unisys
08-00-10	AT&T
08-00-11	Tektronics
08-00-14	Excelan

Adressteil	Hersteller
08-00-20	Sun
08-00-2B	DEC
08-00-38	Bull
08-00-39	Spider
08-00-46	Sony
08-00-4E	BICC
08-00-5A	IBM
08-00-69	Silicon Graphics
08-00-6E	Excelan
08-00-7C	Vitalink
08-00-89	Kinetics
08-00-90	Retix

### 13.2.7 Beispiele

Auf den folgenden Seiten befinden sich vier gleiche Requests (Get nearest file server) mit unterschiedlichen Frames. Neben der Kurzübersicht findet man die analysierte Ausgabe und letztlich die hexadezimale Abbildung der Daten, welche über das LAN gegangen sind.

#### 13.2.7.1 Ethernet 802.2

No.	Source	Destination	Layer	Size	Summary
1	0080AD0662F5	Broadcast	sap	0064	Query Nearest File Server

```

Packet Number : 1          17:11:18
Length : 64 bytes
802.3: ===== IEEE 802.3 Datalink Layer =====
Station: 00-80-AD-06-62-F5 ----> Broadcast
Length: 37
802.2: ===== IEEE 802.2 Logical Link Control =====
SSAP: NetWare DSAP: NetWare
Unnumbered Command: Unnumbered Information (UI)
ipx: ===== Internetwork Packet Exchange =====
Checksum: 0xFFFF
Length: 34
Hop Count: 0
Packet Type: 17(NCP)
Network: 00 00 00 00 ----> 00 00 00 00
Node: 00-80-AD-06-62-F5 ----> Broadcast
Socket: 0x4006 ----> SAP
sap: ===== NetWare Service Advertising Protocol =====
Type: 3 (Nearest Service Query)
Server Type: 0x0004(File Server)
    
```

```

Packet Number : 1
0: FF FF FF FF FF FF 00 80 AD 06 62 F5 00 25 E0 E0 | .....b..%..
10: 03 FF FF 00 22 00 11 00 00 00 00 FF FF FF FF FF | .....".
20: FF 04 52 00 00 00 00 00 80 AD 06 62 F5 40 06 00 | ..R.....b@..
30: 03 00 04 01 A5 A5 A5 A5 A5 A5 A5 A5 | .....
    
```

#### 13.2.7.2 Ethernet 802.3

No.	Source	Destination	Layer	Size	Summary
1	0080AD0662F5	Broadcast	sap	0064	Query Nearest File Server

```

Packet Number : 1          16:31:13
Length : 64 bytes
802.3: ===== IEEE 802.3 Datalink Layer =====
Station: 00-80-AD-06-62-F5 ----> Broadcast
Length: 34
ipx: ===== Internetwork Packet Exchange =====
Checksum: 0xFFFF
Length: 34
Hop Count: 0
Packet Type: 17(NCP)
Network: 00 00 00 00 ----> 00 00 00 00
Node: 00-80-AD-06-62-F5 ----> Broadcast
Socket: 0x4006 ----> SAP
sap: ===== NetWare Service Advertising Protocol =====
Type: 3 (Nearest Service Query)
Server Type: 0x0004(File Server)
    
```

```

Packet Number : 1
0: FF FF FF FF FF FF 00 80 AD 06 62 F5 00 22 FF FF | .....b..".
10: 00 22 00 11 00 00 00 00 FF FF FF FF FF FF 04 52 | .....R
20: 00 00 00 00 00 80 AD 06 62 F5 40 06 00 03 00 04 | .....b.@....
30: A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 A5 | .....
    
```

13.2.7.3 Ethernet\_II

No.	Source	Destination	Layer	Size	Summary
1	0080AD0662F5	Broadcast	sap	0064	Query Nearest File Server

```

Packet Number : 1          17:03:12
Length : 64 bytes
ether: ===== Ethernet Datalink Layer =====
Station: 00-80-AD-06-62-F5 ----> Broadcast
Type: 0x8137 (NetWare)
ipx: ===== Internetwork Packet Exchange =====
Checksum: 0xFFFF
Length: 34
Hop Count: 0
Packet Type: 17(NCP)
Network: 00 00 00 00 ----> 00 00 00 00
Node: 00-80-AD-06-62-F5 ----> Broadcast
Socket: 0x4A58 ----> SAP
sap: ===== NetWare Service Advertising Protocol =====
Type: 3 (Nearest Service Query)
Server Type: 0x0004(File Server)
    
```

```

Packet Number : 1
0: FF FF FF FF FF FF 00 80 AD 06 62 F5 81 37 FF FF | .....b..7..
10: 00 22 00 11 00 00 00 00 FF FF FF FF FF FF 04 52 | .....R
20: 00 00 00 00 00 80 AD 06 62 F5 4A 58 00 03 00 04 | .....b.JX....
30: 18 00 19 00 1A 00 1B 00 1C 00 1D 00 | .....
    
```

13.2.7.4 Ethernet\_SNAP

No.	Source	Destination	Layer	Size	Summary
1	0080AD0662F5	Broadcast	sap	0064	Query Nearest File Server

```

Packet Number : 1          17:16:43
Length : 64 bytes
802.3: ===== IEEE 802.3 Datalink Layer =====
Station: 00-80-AD-06-62-F5 ----> Broadcast
Length: 42
802.2: ===== IEEE 802.2 Logical Link Control =====
SSAP: SNAP DSAP: SNAP
Unnumbered Command: Unnumbered Information (UI)
SNAP Organization Code: 00 00 00
SNAP Ethernet Type: 0x8137 (NetWare)
ipx: ===== Internetwork Packet Exchange =====
Checksum: 0xFFFF
Length: 34
Hop Count: 0
Packet Type: 17(NCP)
Network: 00 00 00 00 ----> 00 00 00 00
Node: 00-80-AD-06-62-F5 ----> Broadcast
Socket: 0x4006 ----> SAP
sap: ===== NetWare Service Advertising Protocol =====
Type: 3 (Nearest Service Query)
Server Type: 0x0004(File Server)
    
```

```

Packet Number : 1
0: FF FF FF FF FF FF 00 80 AD 06 62 F5 00 2A AA AA | .....b..*..
10: 03 00 00 00 81 37 FF FF 00 22 00 11 00 00 00 00 | .....7..."
20: FF FF FF FF FF FF 04 52 00 00 00 00 80 AD 06 | .....R.....
30: 62 F5 40 06 00 03 00 04 A5 A5 A5 A5 | b.@.....
    
```

13.3

**Protokolle (IPX, IP, NetBios, NetBeui, XNS, OSI, AppleTalk...)**

Protokolle dienen dazu, Datenpakete von einem Rechner zum anderen zu leiten. Speziell wenn mehrere Rechner über die gleiche Leitung kommunizieren, muß ein Protokoll dafür sorgen, daß ein Paket seinen Empfänger erreicht und andere Stationen nicht belastet werden. Protokolle bewirken auch eine Weiterleitung der Pakete über mehrere Netzwerksegmente.

Unterscheiden muß man dann Protokolle, die routingfähig sind und solche, die nicht routingfähig sind; d.h. ob im Header des Datenpakets neben der Rechnernummer auch die Netzwerknummer abgelegt ist. Ist ein Protokoll sourcerouting-fähig, dann wird durch die Information im Header auch der Weg zum Zielrechner vorgegeben.

NetBios ist z.B. nicht routingtauglich, da es keine Netzwerkadresse gibt, sondern nur Namen. Wenn daher zwei Netzwerke durch einen Router gekoppelt sind, muß der Router NetBIOSpakete immer durchrouten, auch wenn Sender und Empfänger auch am gleichen Segment hängen, es sei denn der Router "versteh" Netbios und führt in seinem Speicher eine Tabelle mit, an welchem Segment welcher Name hängt.

IP gliedert in seiner Adressierung schon ein Netzwerk in mehrerer Unternetzwerke auf, so daß Routing einfach möglich ist.

IPX enthält als Adresse die Netzwerkadresse und die Rechneradresse (LAN-Kartennummer). Jedoch ist die Netzwerkadresse nicht hierarchisch strukturiert, so daß die Router auch eine Liste mitführen, welches Netzwerk in welche Richtung erreicht werden kann.

Protokolle unterscheidet man auch, ob sie verbindungsorientiert oder verbindungslos sind, d.h. ob eine logische Verbindung aufgebaut wird oder nicht. Daraus folgert auch die Verbindungssicherheit, d.h. ob das Protokoll nur die Adressierung macht und die Daten auf die Reise schickt, oder ob es auch auf Quittungen wartet und in Falle eines Fehlers das Paket nochmal verschickt. Meist bauen diese gesicherten Verbindungen auf den ungesicherten Verbindungen auf, z.B. SPX oder NCP benutzen IPX, TCP baut auf IP auf.

**13.4 IP**

Das Protokoll IP eignet sich sehr gut zur Terminalemulation über das Netzwerk. Zumal viele UNIX-Rechner untereinander mittels TCP/IP kommunizieren (FTP, TELNET, NFS). Mittlerweile ist auch der PC in der Lage, TCP/IP über eine LAN-Karte zu fahren und damit die unzähligen direkten Leitungen zum Host zu ersetzen. Zudem ist das Netzwerk (Cheapernet: 10 MBit) meist viel schneller als eine Zweidrahtleitung.

Da PC's ursprünglich nicht als Geräte mit IP vorgesehen waren, entwickelten sich viele verschiedene Produkte verschiedener Hersteller. Viele haben eigene Implementierungen was das Fontend und die LAN-Kartenprogrammierung angetrifft. Solange man nur ein Produkt einsetzt, ist die Konfiguration einfach, sobald man aber verschiedene Frontends benötigt (z.B. X-Terminal und VT200 und FTP) und diese von verschiedenen Herstellern kommen, muß man Konverter suchen, da man immer nur einen Protokolltreiber für IP ja LAN-Karte haben kann.

Eine Auwahl der bekannten IP-Zusätze:

**Tabelle 10 TCP/IP-Stacks**

Produkt	Hersteller	Einsatz	Treiber (originär)
<b>Lan Work Place</b>	Novell	TCP/IP	ODI
<b>Pathway IP</b>	Wollongong	TCP/IP	Wollongong
<b>FTP IP</b>	FTP	TCP/IP	Packet
<b>PC-NFS</b>	Sun	TCP/IP	NDIS (?)
<b>Chamaeleon</b>	NetManage	TCP/IP nur Windows	ODI, NDIS, PKT

Mittlerweile gibt es schon IP-Implementationen, welche als DLL für Windows implemetiert sind und damit nicht mehr die 640k-Grenze von DOS belasten. Für Windows gibt es eine WINSOCKET-Beschreibung, welche zukünftig den Zugriff zu IP regeln soll.

Bei IP wird ähnlich wie bei IPX jeder Knoten durch eine Netzwerknummer und eine Rechnernummer adressiert. Im Gegensatz zu IPX, wo die Netzwerknummer „flach“ ist und die Knotennummer gleich die Ethernetkartenadresse ist, werden bei IP die Adressen vergeben. Die Adresse besteht aus 4 Bytes, welche gewöhnlich in „gepunkteter“ Notation angegeben werden. Damit sind Adressen zwischen 000.000.000.000 und FF.FF.FF.FF (= 255.255.255.255) möglich.

Liegt die erste Zahl im Bereich von 0 bis 127, dann spricht man von einem „Class A“ Netzwerk. Dabei ist die erste Stelle die Netzwerknummer und die restlichen 3 Stellen bestimmen den Rechner. Von diesen „Netzwerken“ kann es demnach nur 127 Stück weltweit geben, welche zusammengeschlossen sind. Dafür können an diesem Lan 255<sup>3</sup> Stationen betrieben werden.

Von einem „Class B“-Netzwerk spricht man, wenn die ersten beiden Stellen das Netzwerk angeben und die letzten beiden Stellen den Rechner. Dies ist genau dann der Fall, wenn die erste Stelle im Bereich 128 bis 192 liegt.

Ein „Class C“-Netzwerk besteht dann aus bis zu 253 Rechnern in einem LAN, welches über Router von 255<sup>3</sup> anderen Netzwerken erreicht werden kann.

Einige Adressen sind besonders reserviert: FF.FF.FF.FF ist ein Broadcast an alle Stationen. 127.0.0.0 ist die „Loopback“ Adresse, also immer der eigene Rechner.

Da diese Adressierung nicht immer genau gepasst hat, gibt es die „Subnetmask“, welche eine Untergliederung der Rechneradressen als einzelne Netzwerke zulässt.

### 13.5 Verbindung (Router, Bridge, Server als..)

Wenn mehrere Netzwerksegmente verbunden werden müssen, geschieht das durch geeignete Bindeglieder. Eine Trennung von einem Netzwerk in zwei oder mehrere physikalische Segmente bringt in der Regel eine Lasttrennung. Speziell wenn der Server je eine LAN-Karte je Segment bekommt, kann eine große Aktivität auf einem Segment die Benutzer des anderen Segments nicht stören, es sei denn der Fileserver ist überlastet.

Aber speziell dann, wenn mehrere Server eigene Benutzergruppen bedienen, ist es ratsam, diese auch physikalisch zu trennen. Zudem erhöht sich die Ausfallsicherheit, da der Ausfall eines Stranges die Arbeit des anderen nicht beeinträchtigt.

#### 13.5.1 Repeater

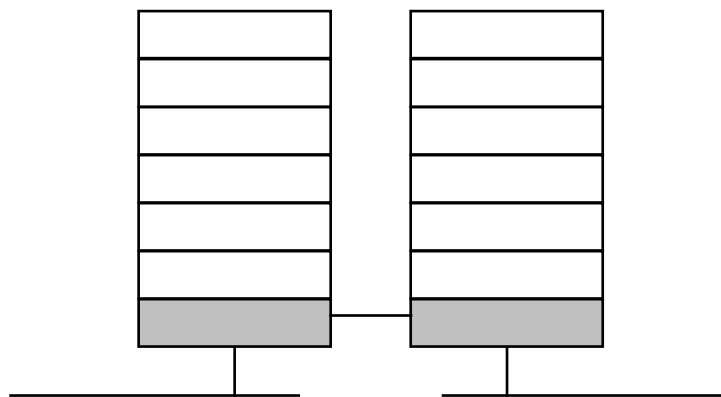
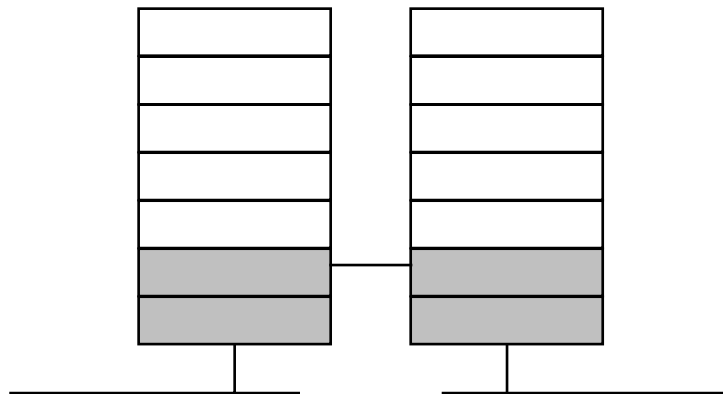


Abbildung 27 OSI Repeater

Repeater verbinden Netzwerk rein physikalisch. Sie wirken als Verstärker, damit man Segmente verlängern kann. Aber sie bewirken keine Lasttrennung. Ein TwistedPair-Hub ist ein Repeater.



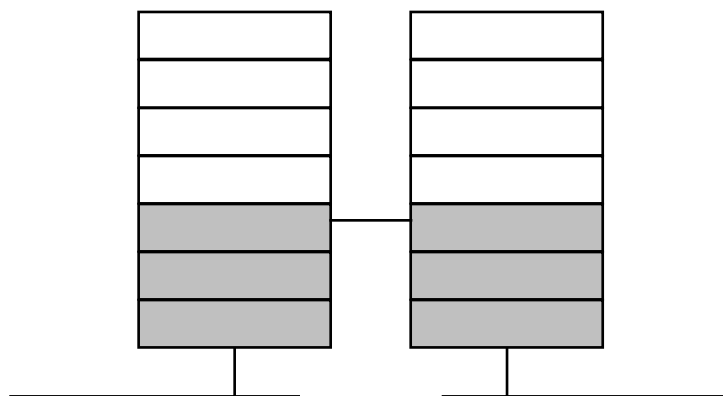
### 13.5.2 Bridge



**Abbildung 28 OSI 2 Bridge**

Bridges verbinden die Segmente auf der nächst höheren Schicht. Mit Bridges ist es möglich, auch unterschiedliche Netzwerktopologien (Ring, Bus) zu verbinden. Eine Brige kann nur auf MAC-Level filtern.

### 13.5.3 Router



**Abbildung 29 OSI 3 Router**

Router arbeiten auf Protokollebene; d.h. Protokolle, die der Router nicht versteht, läßt er in der Regel nicht durch. Er liest nicht die MAC-Adresse eines Paketes, sondern die Netzwerkadresse (z.B. IP-Adresse). Damit ist eine aktive Filterung möglich. Netzwerke können damit gezielt abgeschottet werden.

Einzelne Arbeitsgruppen/Abteilungen mit eigenen Servern sollten durch Router abgegrenzt werden, damit beim Remoteboot der eigene Server der schnellere ist (Give nearest server-CALL).

13.5.4 Gateways

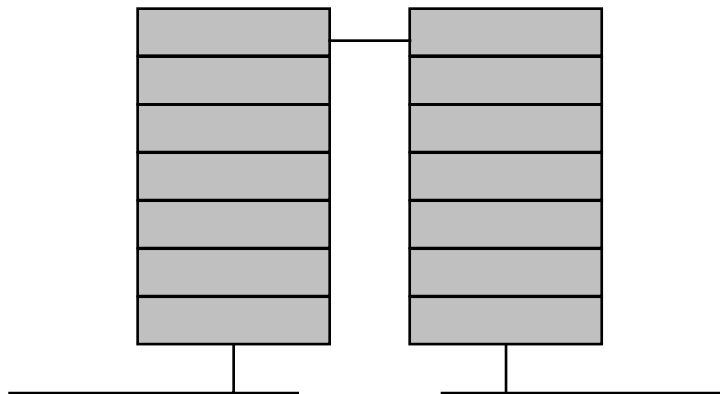


Abbildung 30 OSI 7 Gateway

Gateways verbinden Netzwerke auf der höchsten Schicht, d.h. machen bei Bedarf auch eine komplette Umsetzung von Zeichensätzen, Dateiformaten, Codierungen (BCD, ASCII, EBZDIC). Damit kann man auch komplett unterschiedliche Rechnerwelten (IBM, VAX, DEC, HP ua) verbinden.

13.6 Lasttrennung im LAN

Bridges und Router sind geeignet, Lasttrennungen im Netzwerk durchzuführen, indem sie im Gegensatz zum Repeater Pakete filtern können. Vor einigen Jahren waren 4MBit Token-Ring sehr schnelle Netzwerke. Auch Ethernet-LAN's mit 10MBit reichten in den meisten Fällen aus. Token Ring wurde schneller, nachdem der 16MBit-Ring eingeführt wurde.

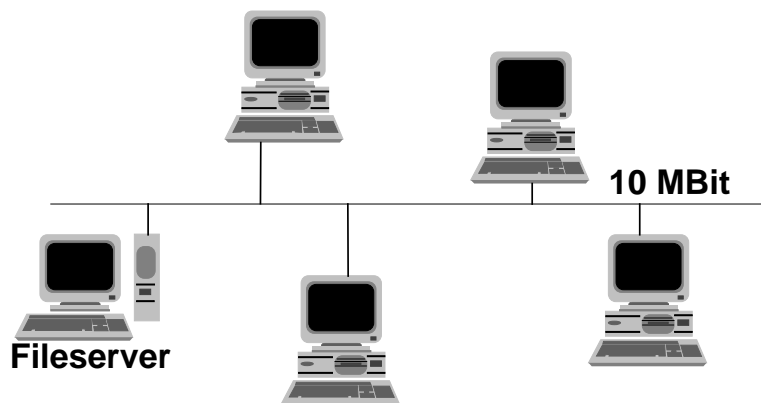


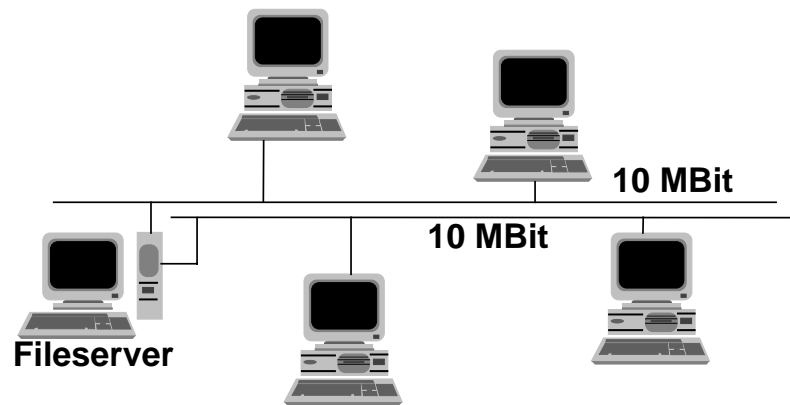
Abbildung 31 Ein Segment

Bei kleinen Netzwerken sind diese Übertragungsmedien weiterhin ausreichend. Je mehr Computer allerdings am Netzwerk angeschlossen werden, desto geringer wird die pro PC übertragene Datenmenge. Die Grenze der physikalischen Übertragungsmöglichkeiten wird erreicht.

Mehr Geschwindigkeit erhält man, indem man schnellere Verbindungen einsetzt (z.B. FDDI) oder Lasttrennung durchführt.

Gegen schnellere Verbindungen sprechen zur Zeit noch Kostenaspekte und die aufwendigere Verkabelung.

Segmentierung ist eine einfache und meist kostengünstige Methode, mehr Daten durch ein LAN zu bekommen. Dabei werden die zentralen Punkte mit dem höchsten Datenaufkommen (z.B. Fileserver) über mehrere LAN-Karten an verschiedene Segmente angeschlossen.

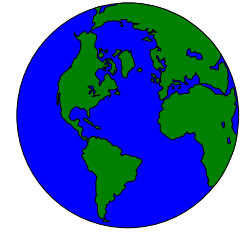


**Abbildung 32 Segmentierung**

Mit diesem Kniff ist der Server nun gleichzeitig Router. (NetWare IPX-Router). Daten, welche von den beiden unteren Workstations gesendet und empfangen werden, erreichen nicht das obere LAN und umgekehrt.

Kommunizieren jedoch Workstations auf dem oberen LAN direkt mit dem unteren LAN (z.B. BTX-Gateway, Terminalemulation), dann ist der Server als Router aktiv und kann damit nicht seine komplette Rechenzeit dem "Fileservice" geben. Werden auf beiden LAN's Protokolle genutzt, welche vom Fileserver nicht geroutet werden können, ist ein zusätzlicher Router nötig.

## 14 WAN



Als WAN bezeichnet man die Verbindung mehrere lokaler Netzwerke über die eigenen Grundstücksgrenzen hinaus. Damit stehen in den seltensten Fällen hohe Geschwindigkeiten zur Übertragung zur Verfügung.

Damit ist klar, daß zwischen zwei LANs eine aktive Komponente den Datenverkehr filtern muß. Es dürfen nur notwendige Datenpakete übertragen werden. Dazu eignen sich am besten Router. Gute Router verstehen nicht nur die routingmechanismen der übertragenen Protokolle, sondern können auch selektiv bestimmte Datenpakete ausfiltern.

Zum Einsatz können aber auch Bridges kommen. Speziell wenn viele Protokolle übertragen werden müssen und keine Router für diese Protokolle verfügbar sind oder den finanziellen Rahmen sprengen. Solche eine Bridge ist in der Regel auch mit rudimentären Filterfunktionen ausgestattet. Damit sollten auch Broadcasts ausgefiltert werden können. Allerdings kennt die Bridge nicht die Protokolle in dem Broadcastpaket. Damit kann sie nicht entscheiden, welche Broadcasts doch weitergesendet werden müßten.

Die Verbindungen zwischen zwei Standorten kann über verschiedene Transportwege erfolgen.

Liegen die beiden Gebäudeteile in Sichtverbindung, dann können heutzutage Netzwerke über Laserstrecken verbunden werden. Dazu wird zwischen beiden Teilen eine Lichtstecke eingerichtet. Diese Technik erlaubt es sogar, mehrere Megabyte pro Sekunde zu übertragen.

Im „echten“ WAN-Bereich, also über mehrere Kilometer hinweg oder sogar weltweit gibt es zwei grundsätzlich verschiedene Übertragungstechniken.

### **14.1 Paketvermittlung**

Die Vermittlung der Datenpakete erfolgt über eine Kommunikationsnetzwerk, welches einzelne Datenpakete von einem Punkt zum anderen Überträgt. Dabei gibt es keine „festgeschaltete“ Verbindungsleitung. Die Daten laufen von Vermittlungsknoten zu Vermittlungsknoten. Der Weg zweier nacheinander abgeschickter Pakete muß nicht immer identisch sein. Bei dieser Konfiguration kann man auch Punkt zu Mehrpunkt-Verbindungen realisieren. Dazu muß jedem Datenpaket die Zeiladresse mitgegeben werden.

Ein Beispiel für dieses Netzwerk ist z.B. Datex-P.

Die Abrechnung erfolgt in der Regel nach einem komplizierten Plan, in welchem die Zeiten und Zugangsgeschwindigkeiten, also auch die Datenmenge einfließt.

Grundsätzlich kann man festhalten, daß die Bezahlung auf Basis der übermittelten Pakete geschieht.

Damit eignet sich diese Kopplung für terminalbasierte Anwendungen, welche eine dauernde logische Verbindung benötigen. Werden jedoch große Datenmengen übertragen, wird Datex-P sehr schnell teuer.

### **14.2 Festverbindung**

Eine andere Alternative sind fest verschaltete Leitungen. Dazu werden auf beiden Seiten der Leitungen entsprechende Endeinrichtungen installiert. Es erfolgt kein Aufbau oder Abbau der Verbindung. Die mögliche Datenrate hängt von der Qualität der Leitung ab. Die Kosten dieser Lösung sind in der Regel auf Entfernungskilometer berechnet.

Eine Festverbindung bietet eine sehr hohe Verfügbarkeit. Eine „Netzüberlastung“ kann nicht auftreten und auch eine „besetzte Gegenstelle“ ist nicht möglich.

### 14.3 Wählverbindung

Wählverbindungen sind die bekannteste Art der Verbindungen. Telefon und Telefax stellen auch ein are Netzwerk mit vielen verteilten Teilnehmern dar. Bei WAN-Verbindungen von Netzwerken bauen aktive Komponenten auf jeder Seite Verbindungen auf und ab. Die Übertragungsrate richtet sich nach den Endgeräten, der Leitungsqualität und der Technik (ISDN digital <-> analog).

Die Abrechnung erfolgt in der Regel nach der Gebührenzone (Entfernung) und einem Zeittakt.

Damit eignet sich diese Verbindung bei großen Datenmengen mit Pausen in der Übertragung. Modemkommunikation oder Mailboxen sind Beispiele hierfür. Aber auch bei WAN-Kopplungen mit hohen Datenmengen ist diese Variante auch bei weiten Entfernungen eine Alternative zu Datex-P.

Ist die Verbindung abgebaut, entstehen außer den Grundgebühren für den Anschluß keine weiteren Kosten. Werden Daten übertragen, muß eine bestimmte Zeitverzögerung einkalkuliert werden, bis die Verbindung aufgebaut ist. Dabei ist mit der Impulswahl beim Telefon immer noch mit bis zu 2 Minuten zu rechnen. Durch den Einsatz der Mehrfrequenzwahl oder der digitalen Technik (ISDN) ist diese Verzögerung in den Bereich von wenigen Sekunden bis zu 1/10tel Sekunde gefallen.

### 14.4 Kostenanalyse

Um die letztlich preisgünstigste Variante ausfindig zu machen, bedarf es einer genauen Analyse der Daten und Anforderungen der Anwender. Eventuell ist auch eine Kombination zweier Systeme sinnvoll.

So ist eine terminalbasierte Anwendung (z.B. Reisebüreterminals) eher mit Datex-P anzubinden, während kurzfristige Datenübertragungen (z.B. Konstruktionsdaten zum Werk) mit Wählverbindungen günstiger sind.

Bei Festverbindungen kann überlegt werden, inwieweit eine solche Leitung mehrfach genutzt wird. Manchmal sind schon die Telefonanlagen zweier Firmenteile über Festverbindungen gekoppelt. Dann ist eine Datenübertragung über die interne Anlage eine Alternative um die Kapazität besser auszunutzen.

### 14.5 Netware im WAN

Ein NetWare-Server sendet jede Minute ein Statuspaket (Service Advertising Paket (SAP)) als Broadcast durchs LAN. Dies würde bei einem WAN bedeuten, daß eine Wählverbindung jede Minute aufgebaut werden würde. Diese SAP-Pakete sind notwendig, damit die Server ihre Routingtabellen aktualisieren können und Dienste im Netzwerk (Druckserver, Fileserver, Fax-Server und andere) bekannt gemacht werden können. Die ist auch eine Einschränkung des IPX-Protokolls. Im Gegensatz zum IP-Protokoll ist bei IPX eine Routinginformation nicht anhand der IPX-Netzwerknummer ersichtbar. Bei IP kann anhand der Adressierungsmaske einfach entschieden werden, ob das Paket innerhalb des LANs bleiben muß oder übertragen werden muß. Allerdings können SAP-Pakete gefiltert und simuliert werden. Hier ein kurze Liste von SAP-Packettypen. (Nicht vollständig)

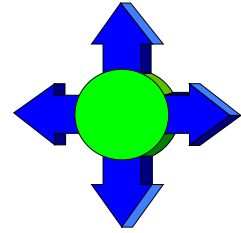
Die folgende Liste von NetWare-Objecten gilt sowohl für die NetWare bindery als auch für die SAP-Protokoll-objekte (Service Advertising Protocol)

Typ	Beschreibung
04	FileServer
05	JobServer
06	Gateway
07	PrintServer
09	ArchiveServer
21	NASSNAGateway
23	NACS
24	RemoteBridgeServer
26	RemoteBridgeServer2
27	TCP/IPGateway

Typ	Beschreibung
29	EICONX25-Gateway
2D	TimeSynchronizationServer
2E	ArchiveServerDynamicSAP
47	AdvertisingPrintServer
4C	SQLVAP/NLM
58	EICONRouter
72	WANcopy
7A	TESNetwareforVMS
92	EmeraldBackup
98	NetWareAccessServer
A1	Powerchute
AC	CompaqIDAStatusMonitor
107	RSPXServer
174	CompaqSNMPAgent
3C4	Arcserve4.0
3DE	NWSQL
4808	SiteLock
8002	IntelNetport(PrintServer)

Tabelle 11 SAP-Packettypen

## 15 Connectivity



Mit der Anbindung eines PC an ein LAN kann man das Übertragungsmedium des LAN's nicht nur für die Kommunikation mit dem Fileserver nutzen, sondern viele Dienste zentral zur Verfügung stellen. Einige Dienste kann man allein mit einer Zusatzsoftware auf dem PC anbieten (TELNET-Terminalemulation zum Host), für andere Dienste sind Gateways nötig

Vor einigen Jahren wurden nach und nach PC's eingeführt. Im Gegensatz zu den hostbasierten Terminalsystemen war der PC als "Personal Computer" gedacht: "Jedem Benutzer seinen PC". Mittlerweile werden die Computer mit Netzwerken verbunden und das Stichwort der "GroupWare" fällt immer häufiger. Mit dem Aufkommen von grafischen Oberflächen (Windows, OS/2 u.a.) wurden die Terminals immer mehr verdrängt. Jedoch gibt es immer noch viele Anwendungen, welche nur hostbasiert laufen.

### **15.1 Gateways**

Gateway bilden die Brücke zu netzwerkfremden Diensten. Sieht man den Begriff etwas weiter, so kann auch ein Druckserver mit einem Drucker als "Gateway" aufgefasst werden, da diese Komponente den Übergang der elektronischen Daten auf Papier ermöglicht. Ein Gateway bietet wie ein "Server" (Fileserver, Printserver u.a.) einen DIENST an. Gateways unterscheiden sich in der Art und Weise, wie sie den Dienst im Netzwerk anbieten. Dies ist durch die gewünschte Funktion des Dienstes meist festgelegt.

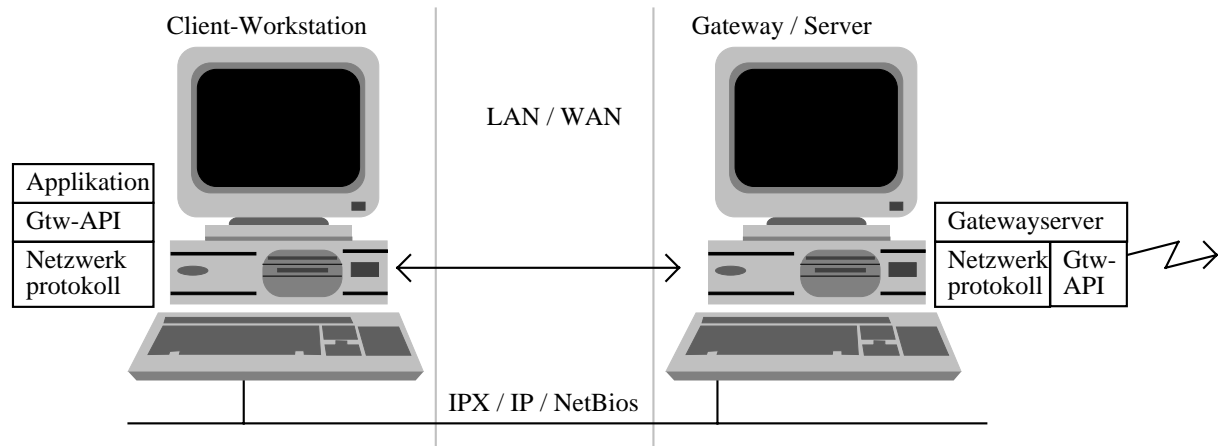
Gateways sind PC's, welche meist 24 Stunden laufen und für alle berechtigten Benutzer im LAN Dienste zur Verfügung stellen (FAX, BTX, ISDN, MAIL usw). Da diese PC's ohne dauernde Überwachung laufen, müssen sie außerordentlich stabil sein, sowohl auf die Hardware als auch auf die Software bezogen. Es hat sich bewährt, die Gateway in Zeiten, in denen sie nicht gebraucht werden, neu zu starten. Die geschieht am einfachsten mit einer Zeitschaltuhr, welche den PC für kurze Zeit abschaltet. Dabei muß aber sichergestellt sein, daß der die Software dieses abrupte Ende schadlos übersteht. Zugleich sollten auch angehängte Geräte (Modems usw) neu gestartet werden.

Bei NetWare gibt es die Möglichkeit, Benutzer mit SEND eine Meldung zu schicken. Dabei wartet der Ziel-PC auf die Bestätigung mit CTRL-ENTER. Auch der Server selbst benutzt diese Meldungen, um Fehler zu melden (Power failed, Volume dismounted). Da dies auch die Gateway stoppt, muß man vor dem Start der Gatewaysoftware den Befehl CASTOFF ALL ansetzen um diese Meldungen zu verhindern.

Den Zugriff auf Gateway kann man auf zwei Wege gestalten. Direkt von Workstation auf das Gateway oder über den Umweg der Serververzeichnisse.

#### **Point2Point**

Client (=Workstation) und Gatewayrechner kommunizieren direkt über das LAN miteinander.

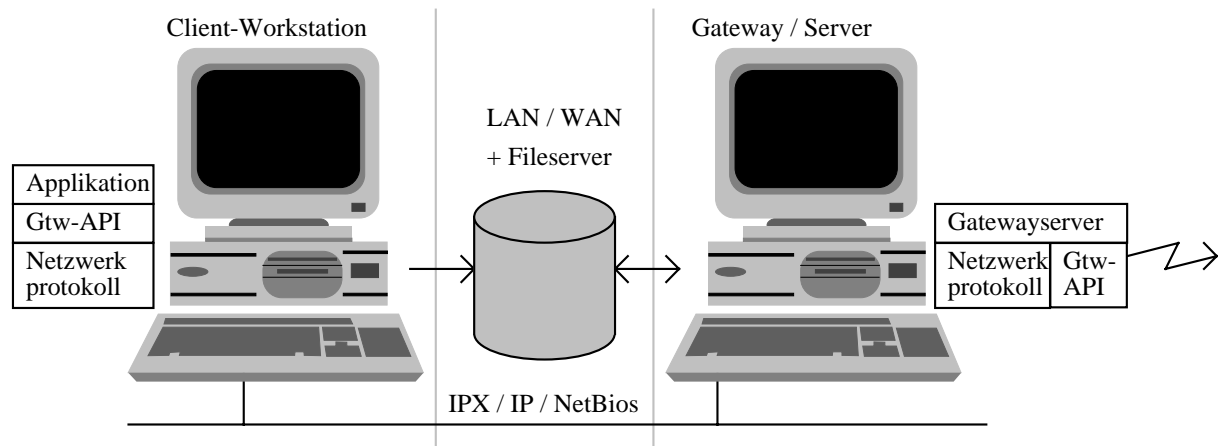


**Abbildung 33 Point2Point Gateway**

Beispiel hierfür sind die meisten Kommunikationsgateways, welche interaktiv laufen. Dazu müssen BEIDE Computer gleichzeitig aktiv sein. Der Fileserver wird fast nicht belastet, da er die Daten nicht puffern muß. Jedoch muß man die Last durch eventuelles ROUTING beachten, falls Benutzer und Gateway an verschiedenen Strängen angeschlossen sind. Es können immer nur soviele Benutzer gleichzeitig arbeiten, wie das Gateway unterstützt. Daten werden mit minimaler Zeitverzögerung durchgereicht. Beispiele für solche Gateways sind: ISDN, MODEM, Hostzugang (BS2000, o.a.), Datex-P. Bei dieser Art Gateway muß man die Leistung zur Verfügung stellen, welche maximal gleichzeitig benötigt wird. Die Kommunikation von Client und Gateway erfolgt über bestimmte Netzwerkprotokolle (IPX, NETBIOS, TCP/IP o.a.) Diese müssen auf beiden Rechnern verfügbar sein.

**Dateiorientiert**

Dateiorientierte Gateways benutzen Dateien auf einem Server als Datenaustauschnittstelle.



**Abbildung 34 Store&Forward Gateway**

Sie arbeiten nach dem "Store and Forward"-Prinzip, d.h. ein Prozess legt die Daten an einem vereinbarten Punkt im Verzeichnisbaum ab und ein anderer Prozess verarbeitet diese weiter. Dabei müssen nicht beide Prozesse GLEICHZEITIG laufen. Es müssen auf jeden Fall die Daten auf einem Fileserver zwischengespeichert werden (Queuefunktion). Dadurch können aber mehrere Personen GLEICHZEITIG solche Programme nutzen (z.B. FAX oder MAIL zum Versenden einstellen). Das Gateway kann diese "Jobs" dann nacheinander abarbeiten. Dies führt zu einer effektiveren Auslastung des Gateways. Da die Abarbeitung weniger zeitkritisch ist als bei Point2Point-Gateways, kann man die Leistung mehr auf den täglichen Durchschnitt der zu verarbeitenden Daten projizieren.



## 15.2 ISDN, CAPI



Mit der Einführung von ISDN als Vermittlungsdienst der Bundespost Telekom hat sich ein weiteres Verbindungsmedium zum Telefon ergeben. Der Anschluß ist voll digital. Verbunden damit ist eine hohe Datenübertragungsrate (64kBit) und ein schneller Verbindungsaufbau. ISDN benutzt die gleiche Gebührenstruktur wie normale Telefone. Jedoch kann man die vierfache Datenmenge durchschicken. Die meisten ISDN-Karten werden über das COMMON-API angesprochen. Dies ist eine definierte Schnittstelle mehrerer ISDN-Kartenhersteller und mit dem AT-Befehlssatz von Modems zu vergleichen. Im LAN gibt es die Möglichkeit, ein ISDN-Gateway aufzubauen, d.h. ein PC wird mit einer ISDN-Karte ausgestattet und bietet diesen Dienst allen berechtigten Benutzern im Netzwerk an. Auf den Arbeitsrechnern der Benutzer wird eine Software geladen, welche diese Schnittstelle (Common-API) simuliert und die Aufrufe der Anwendung über das Netzwerk an das ISDN-Gateway weiterleitet. Die Software auf dem Arbeitsplatzrechner merkt also nichts davon, daß die ISDN-Karte überhaupt nicht in diesem PC eingebaut ist.

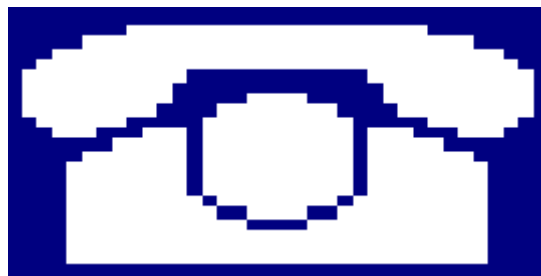
ISDN erlaubt es aber auch, LAN-Verbindungen mit hoher Geschwindigkeit zu entfernten LAN's oder remote Workstations aufzubauen. Die ISDN-Verbindung wird dabei wie ein Segment des LAN betrachtet. Die ISDN-Karte selbst wie eine LAN-Karte.

Über ISDN können beim Einsatz eines geeigneten Frontends viele Datendienst genutzt werden. Dies sind z.B.:BTX, TELEX, CityRuf, FAX, Dateitransfer

Der BTX-Zugang gibt den Benutzern die Möglichkeit, z.B. Bahnpläne, Flughafeninformationen usw. abzurufen.

## 15.3 BTX

BTX ist ein Dienst der Tekecom, um Daten und Informationen abzufragen. Auch wenn seit 1. Januar 1993 der Zugang sehr eingeschränkt worden ist (d.h. der Zugang als GAST ist stark begrenzt) wird dieses lowcost-medium benutzt, um Software zu verteilen, Cityrufempfänger anzupiepen und Kontenauszüge zu bekommen. Auch Fahrplaninformationen sind ONLINE abfragbar. Daher bietet sich es im LAN an, auch einen BTX-Zugang zur Verfügung zu stellen. Dies kann entweder über Modems oder das vorher erwähnte ISDN-Gateway geschehen.



## 15.4 CD-ROM

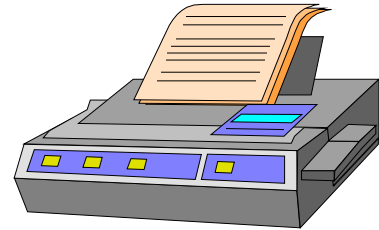


Der CD-Rom-Server kann auf der gleichen Maschine laufen wie das Backup. In der Regel läuft das Backup nachts, während keine Benutzer angemeldet sind und damit das CD-Rom nicht benutzt wird. Damit würde man einen Computer mit SCSI-Kontroller und LAN-Karte einsparen.

Alternativ könnte man auch NetWare 4.0 einsetzen, welche direkt CD-Roms am Fileserver unterstützt. Dies würde jedoch höhere Investitionen beim Server bedingen und NetWare 4.0 ist sicherlich nicht das passende Betriebssystem für dieses Netzwerk.

Als Serverlösung kann man SCSI-Express einsetzen, womit auch wieder die CD-Rom am Fileserver angeschlossen wird. Bedacht werden muß, daß ein CD-Rom-wechsel dann an der Fileserverkonsole eingegeben werden muß und sich damit nicht für den "unbewachten" Betrieb empfiehlt

## 15.5 FAX



Die althergebrachte Methode zum Versenden eines Faxes bedeutete, das Dokument zu drucken und von Hand im Faxgerät einzuspannen und zu faxen. Es gibt seit der Entwicklung von FAX-Modems schon die Möglichkeit, vom Einzelplatz-PC ein FAX zu versenden. Im LAN ist es sehr viel kostengünstiger, diese Möglichkeit allen Benutzern zugänglich zu machen. Es ist dazu nicht notwendig, jeden PC mit einem Modem und einer Telefonleitungen auszustatten. In der Regel werden die Dokumente zum faxen mit einem eigenen Druckertreiber in eine NetWarequeue gedruckt. Der Druckertreiber regelt auch die Eingabe der Faxnummer oder Verteiler. Ein dedizierter PC nimmt die Druckaufträge aus der Printqueue auf ein schickt sie zum Empfänger mittels Faxmodem oder Faxkarte. Die Rückmeldung über den Faxversand erfolgt mittels "SEND"-Message oder Mail.

Eingehende Faxe sind meist auch über diesen dedizierten PC möglich, jedoch ist immer zu prüfen, ob diese Option Sinn macht. Es ist bisher nicht gut möglich, eingegangene Fax automatisch zu routen. Entweder übernimmt eine Schreibkraft die Aufgabe, eingehende Fax von Hand zu routen, oder man druckt eingegangene Fax einfach aus. Damit hat man zumindest ein preiswertes Normalpapierfax. Eingehende Faxe als Datei abzulegen oder weiterzubearbeiten empfiehlt sich nicht, da hierbei große Datenmengen anfallen, welche bei stärkerem Verkehr das Netzwerk bremsen.

Es gibt drei Möglichkeiten, FAXe auf einem LAN zu schicken.

### virtual CAS

d.h. ein PC mit CAS-Karte läuft 24h und bietet über das Protokoll (z.B. IPX) diese Schnittstelle im LAN an. Auf der Workstationseite wird dann eine virtuelle CAS-Schnittstelle geladen. Die Workstation und darauf ablaufende Software glaubt, eine CAS-Karte im PC zu haben. Je nach Software kann dann mit Utilities auf CAS gedruckt werden oder eine Datei an die CAS-Schnittstelle geschickt werden. Die Daten werden NICHT auf dem Fileserver zwischengespeichert. Da FAX meist DCX-Files verarbeitet umgeht man damit das Verschieben großer Datenmengen. Zu klären ist, wie der CAS-Server gleichzeitige Anfragen bedient, da eine Queue meist fehlt. Die Daten gehen in der Regel einmal über das LAN. Sollte der CAS-Server mehrere Aufträge gleichzeitig anhandeln, so sollte er eine lokale Festplatte zum zwischenbuffern haben.

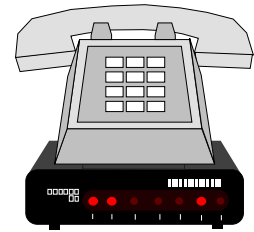
### Druckserver FAX

Die Workstations drucken mit einem speziellen Druckertreiber in eine normale NetWare-Printqueue. Dieser Druckertreiber fordert auch die Telefonnummer usw an. Der FAX-Server verhält sich als Printserver, d.h. bedient die Printqueue. Er liest die Druckdaten mit der Telefonnummer aus und verschickt das Fax. Zu klären ist die Form der Rückmeldung der Übertragung. Die Daten werden einmal auf dem Server abgelegt und müssen zum ablegen und lesen zweimal über das LAN

### Faxgateway für Mail

Die dritte Möglichkeit bedeutet, daß eine E-Mail (mit Attachment) an ein Gateway FAX verschickt wird. Dieses Gateway verschickt das Fax und stellt die Quittung über Mail wieder zu. Leider ist kaum ein FAX-Gateway leitungsfähig genug, z.B: eine EXCEL-Datei als Attachment direkt zu faxen. Daher wird dieser Fall meistens dadurch gelöst, daß der Anwender zum Faxen diese Datei erst in eine geeignete Datei druckt (DCX oa) und diese dann mittels Mail verschickt. Dies wird unter Windows z.B. von Makros vollautomatisch ausgeführt. Die Daten müssen aber im ungünstigen Fall zweimal auf dem Server abgespeichert werden (Druckdatei und dann als Mail). Die Daten müssen dazu viermal durchs LAN (drucken, einlesen, als Mail schreiben und Lesen vom Faxgateway).

## 15.6 Modem



Modems dienen der Modulation und Demodulation von Computersignalen, damit diese über Telefonleitungen (analog) übertragen werden können. Im Gegensatz zum Akustikkoppler sind Modems direkt an dem Telefonnetz angeschlossen und bauen selbstständig Verbindungen auf und ab. In Netzwerk kann man ein oder mehrere Modems "verteilen". Dabei wird der Workstation wieder vorgespielt, sie hätte dediziert ein Modem lokal angeschlossen.

Dazu wird das Modem an einem PC angeschlossen und eine Gatewaysoftware geladen. Dieser PC kann in der Regel noch zur Arbeit genutzt werden kann, aber was nicht empfehlenswert ist da die Performance eingeschränkt ist und gerade bei heutigen "Hochgeschwindigkeitmodems" die Verbindung unterbrochen werden könnte. Wenn mehrere Modems an einem PC im LAN verfügbar gemacht werden, ist der PC vollauf damit beschäftigt. Auf der Anwenderseite wird ein TSR-Programm geladen, welches die serielle Schnittstelle zum Modemserver umlenkt. Dabei kann in der Regel nur Software verwendet werden, die den INT14-tauglich ist, d.h. welche mittels BIOS-Interrupt 14hex mit der Schnittstelle kommuniziert. Manche Lösungen können auch den Hardwarezugriff auf die serielle Schnittstelle umleiten, wenn mindestens ein 386-Prozessor verfügbar ist.

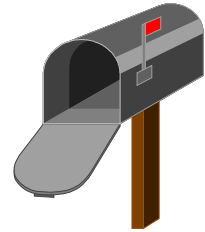
Jedoch sollte geklärt werden, ob zum Datenaustausch nicht besser die EMail in Betracht zu ziehen ist, da damit der Benutzer kein Wissen zur Kommunikation haben muß.

Mit Modems kann man mit verschiedensten Programmen Daten austauschen und neuerdings auch Faxe versenden. Mögliche Anwendungen sind:

- Fernbetreuung (Carbon Copy, CloseUp, CoSession, PCremote)
- Hostzugang (Terminalemulation ProComm, Telix, Dynacom)
- Datex-P Zugang über öffentliche Zugänge bei geringem Datenaufkommen
- Faxversand (im Lan nicht zu empfehlen)
- Datex-J Zugang (z.B. BTX)

Viele dieser Anwendungen können aber für den Benutzer einfacher implementiert werden (z.B. über E-Mail, Faxgateway, u.a.)

## 15.7 EMail



EMail ist ein Medium, um Nachrichten und Dateien zwischen Programmen auszutauschen. Dabei macht es in der Regel keinen Unterschied, ob der Zielempfänger im gleichen Netzwerk oder in einem weit entfernten Netzwerk tätig ist. Natürlich können nicht nur Benutzer mit EMail kommunizieren, auch Programme selbst können die EMail benutzen, um Daten auszutauschen und Anfragen auszuführen.

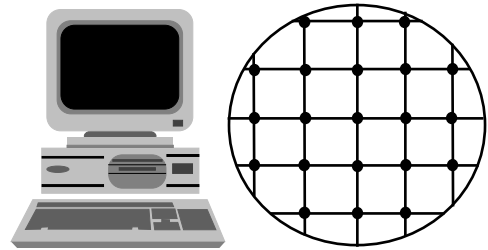
Dabei trennt man bei EMail die Funktionen EMailprogramm und Mail Transfer Agent (MTA). Das EMailprogramm generiert die Mail und stellt sie an vereinbarter Stelle ab. Dies ist z.B. ein bestimmtes Verzeichnis, eine Datenbank oder eine Printqueue. Der MTA nimmt diese Mail auf und stellt sie zu einem anderen MTA zu. Jeder MTA hat einen eindeutigen Namen, so daß als Adresse meiste der Benutzername und der Rechnername angegeben wird. Dabei ist dem MTA freigestellt, über welche Wege die Mail zugestellt wird d.h. der Sender der Mail kann nicht erkennen, ob die Post über Modem, Standleitung, X.25, Internet oder andere Mechanismen ausgetauscht wird.

Eine EMail besteht in der Regel aus einem Absender, einem oder mehreren Empfängern, einem Betreff und einem Anschreiben. An jede Mail kann man "Attachments" beifügen. Diese Attachments werden 1:1 zugestellt, d.h. es ist unerheblich woraus das Attachment besteht (Texte, Tabellen, Bilder, Sprache, ...)

Mit EMail ist es auch möglich, einzelne Außenstandorte oder Außendienstmitarbeiter einzubinden und damit für die Anwender eine einfache Bedienung zu ermöglichen. Er braucht keine Spezialkenntnisse im Bezug auf Modemkommunikation zu besitzen.

Weitere Programme erlauben es, Nachrichten automatisch weiterzuleiten. Damit kann man Nachrichten während der Urlaubszeit an einen Vertreter weiterleiten oder auf einen Notebook im Außendienst.

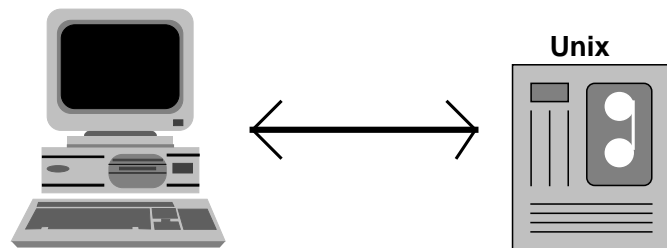
## 15.8 Datex-P



Datex-P ist ein Datendienst der Bundespost Telekom. Die Daten werden paketvermittelt, d.h. es existiert nur eine logische Verbindung zwischen Sender und Empfänger.

Datex-P erlaubt den Zugang zu Datenbanken und Computern am Datex-P Netz. Datex-P ist aber auch mit normalen Modems über öffentliche Zugänge der Bundespost Telekom zu erreichen. Damit ist man aber von der Verfügbarkeit dieser für alle Teilnehmer offenen Anschlüsse abhängig. Beim Festanschluß ist die eigene Nummer auch von anderen Datex-P-Rechnern zu erreichen.

## 15.9 Hostanbindung UNIX



Die Anbindung von vernetzten PC's an Unixrechner im LAN gestaltet sich in der Regel einfach. Unix selbst ist ein Betriebssystem, welches schon lange mit Netzwerken umgehen kann. Unix und dessen Derivate benutzen TCP/IP als Transportprotokoll. Es bestehen weltweite Netzwerke, welche Rechner verschiedenster Hersteller basierend auf TCP/IP verbinden.

Der Zugriff auf solche Rechner erfolgt hauptsächlich über zwei Mechanismen:

### TELNET - Terminalemulation

TELNET ist eine Methode, sich als virtuelles Terminal an einem Rechner anzumelden. Für den Benutzer macht es dann keinen Unterschied, ob er über LAN oder V.24-Leitungen angebunden ist, der Host gegenüber fungiert als Terminalserver. Übertragen werden nur die Tastatureingaben und die Bildschirmausgaben.

### FTP - File Transfer Protokoll

Mittels FTP werden Dateien kopiert, ähnlich dem COPY-Befehl auf DOS.

Viele erweiterte Funktionen von Unix setzen auf diesen Protokollen auf. Der Mailaustausch erfolgt z.B: auch über eine Terminalemulation.

PC's waren ursprünglich als "persönlicher Computer" konzipiert. Daher existieren viele verschiedene Produkte und damit Spezifikationen, wie der Zugriff auf TCP/IP erfolgt. Als gängig für den Zugriff auf einen UNIX-Rechner hat sich das DEC-Terminal Typ VT52 durchgesetzt. Nachfolger dieses Terminals sind die Type VT100 und VT220. Die meisten Rechner kann man damit ansprechen. Diese Terminalemulatoren werden auch für die meisten IP-Produkte mitgeliefert. Erst wenn die Emulation einem firmeneigenen Standard folgt, sollte man zuerst das entsprechende Softwareprodukt für die Terminalemulation auswählen und dann die passende IP-Schnittstelle. Kompliziert wird diese Angelegenheit, sobald der Zugriff auf mehrere Hosts mit verschiedenen Terminalemulationen nötig wird. Man kann nur EIN TCP/IP-Protokolltreiber gleichzeitig laden. Daher müssen alle Emulationen dieses Produkt unterstützen oder man benutzt verschiedene Bootkonfigurationen.

Bei FTP ist die Schwierigkeit fast nicht vorhanden, da das Protokoll FTP eng umschrieben ist, und daher die Funktionsunterschiede anders als bei den Terminalemulationen minimal sind. Trotzdem muß man aufpassen, da sich bei Rechnern oft das verwendete Datenformat unterscheidet. (ASCII-EBZDIC, ISO u.a.) und zudem eine Dateinamenkonvertierung erfolgen muß. MS-DOS ist bei den Dateinamen auf 8+3-Zeichen beschränkt.

15.10 Hostanbindung BS2000

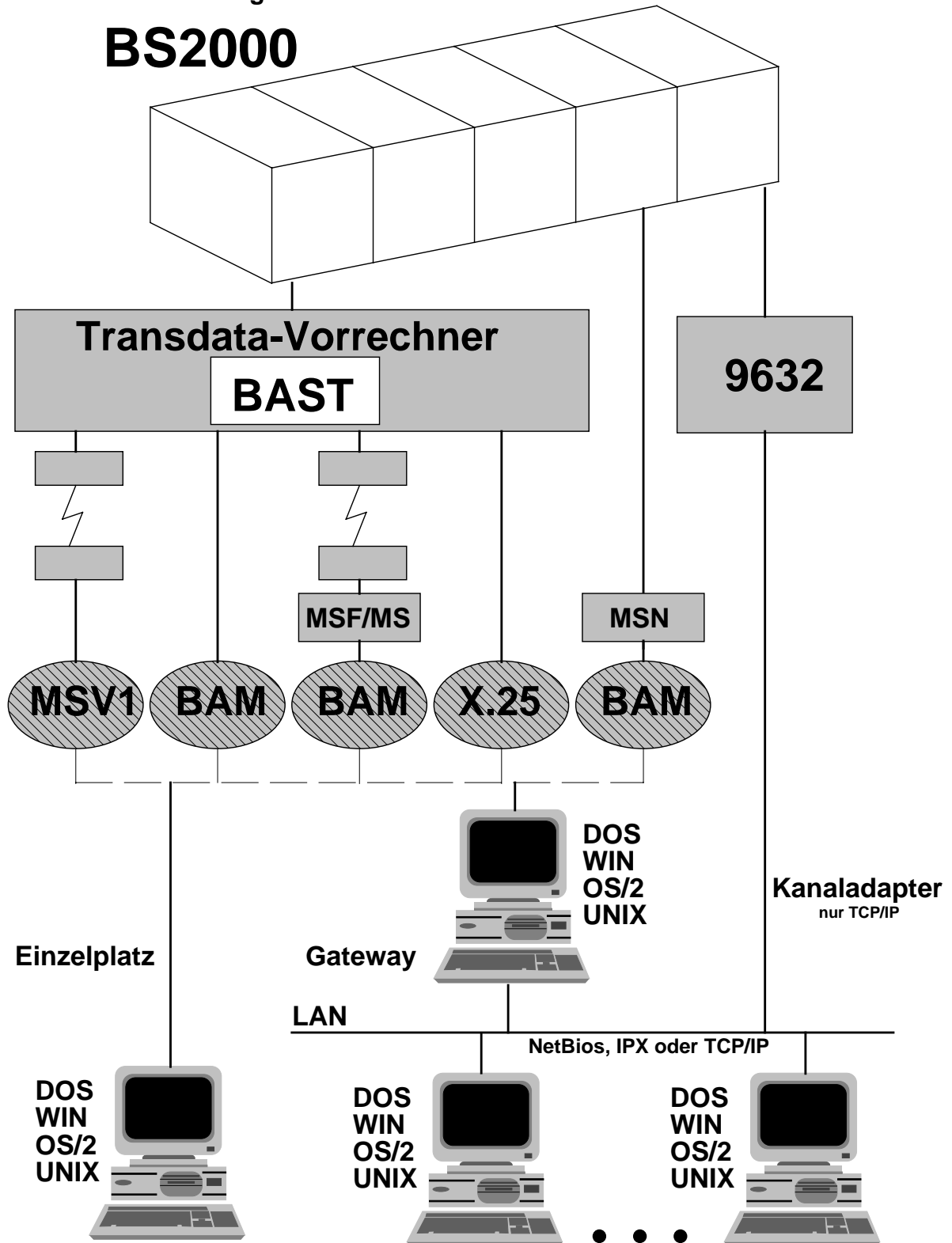


Abbildung 35 BS2000 Anschlußmöglichkeiten

Auf dem Bild erkennt man, daß viele Wege zur BS2000 führen.



**Direktanschluß**

Durch Einbau einer Schnittstellenkarte erreicht der PC die BS2000. Nachteilig ist die gesonderte Verkabelung für die BS2000 und die oft langsame Geschwindigkeit. Allerdings ist man unabhängig vom LAN, solange die Software lokal verfügbar ist-

**Gateway**

Ein Gateway übernimmt die Vermittlung PC <->BS2000. Man benutzt das LAN und spart somit lokale Einbauarten und eine gesonderte Verkabelung.

**Kanaladapter**

Der Kanaladapter erlaubt es, die BS2000 direkt (TCP/IP) anzusprechen. Der Kanaladapter fungiert als Terminalserver für die BS2000. Die hohe Geschwindigkeit und Ausfallsicherheit spricht für diesen Einsatz. Jedoch rentiert sich der Kanaladapter erst bei vielen Arbeitsstationen. Jedoch ist damit eine BS2000 auch effektiv über WAN-Verbindungen zu erreichen.

Leider kann man eine BS2000 nicht mit "normalen" Terminalemulationen erreichen, sondern benötigt ein 9750-Terminal, bzw eine Emulation, welche den eingesetzten Kommunikationsweg unterstützt.

Die BS2000 benutzt einen eigenen Terminalmodus. Damit ist es nahezu unmöglich, mit VT220-Terminalemulationen auf die BS2000 zuzugreifen.

Für den Zugriff benötigt man in der Regel eine 9750-Terminalemulation. Besondere Bedeutung kommt bei der Generierung die Angabe der UTM-Nummern zu. Werden PC's als Terminal über ein LAN eingesetzt, so ist die physikalische Zuordnung TERMINAL <-> Hostzugang nichtmehr gegeben. Welcher PC welche UTM-Nummer, bzw. Terminal-ID bekommt, muß softwareseitig eingestellt werden und darf sich nicht ändern.

**Drucken aus BS2000**

Um Daten von der BS2000 auszudrucken gibt es zwei Wege.

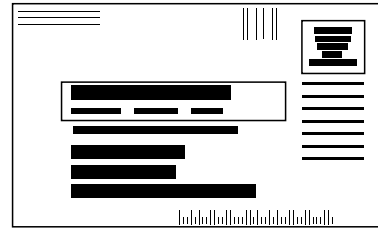
**Direkt**

Man kann einen Drucker benutzen, welche an der BS2000 angeschlossen ist und die Daten vorder BS2000 erhält und ausdruckt. Arbeitet man auf dem PC mit anderen Softwareprodukten ud will man von hier Ausdrucke anfertigen, muß ein weiterer Drucker angeschafft werden oder eine Druckerumschaltbox existieren. Das Drucken ist damit losgelöst von der Funktion des LAN's oder der Emulation.

**Bypass**

Das Terminal 9750 erlaubt es, Druckdaten an das Terminal zu schicken. Das Terminal erkennt, daß es sich um Druckdaten handelt und druckt sie am lokal angeschlossenen Drucker aus. Bei der Terminalemulatino unter Windows muß die Terminalsoftware dies unterstützen. Dann ist ein Ausdruck auf einen schon vorhandenen PC-Drucker möglich.

## 16 MHS



MHS ist die Abkürzung für "Message Handling System" oder "Message Handling Service". Das Produkt MHS wurde ursprünglich von Action Technologies vertrieben und dann von Novell eingekauft. Anfänglich wurde es zu jeder NetWare beigelegt, heute ist es ein Add-on-produkt und muß bezahlt werden. Der Begriff MHS steht auch generell für „Message Handling System“ und hat daher nicht zwingen immer mit NetWare MHS zu tun. Alle weiteren Aussagen zu "MHS" in diesem Text beziehen sich auf Netware MHS bzw. dazu kompatible Produkte.

### 16.1 Warum EMail

EMail ist eine Kommunikationsform, bei welcher Nachrichten und komplette Dateien zwischen verschiedenen Benutzern eines Computernetzwerkes übertragen werden. Dabei liegt der große Vorteil daran, daß der einzelne Benutzer überhaupt keinen Kontakt zur eigentlichen Kommunikation hat, d.h. Begriff wie Modem, Baudrate, DFÜ-Einrichtung, Telefonnummer, V32bis, Datex-P, ISDN, Password, Login etc. belasten den einzelnen Benutzer nicht. Der Anwender nutzt nur eine Applikation (das E-Mailprogramm) welche ihm den Versand und Empfang von Nachrichten und Anlagen erlaubt. Neu dabei ist eine Adressierung, welche ähnlich abstrakt ist, wie eine Telefonnummer oder Faxnummer. Adreßbücher erlauben die Auswahl bestimmter Benutzer.

Es ist abzusehen, daß E-Mail einen ähnlichen Aufschwung erlebt, wie die Verbreitung des Fax und die Tatsache, daß ein Telefon heute nicht mehr wegzudenken ist.

Im Gegensatz zu „Terminalverbindungen“ arbeitet E-Mail „Off-Line“, d.h. der Absender und Empfänger einer Mail müssen nicht gleichzeitig aktiv sein. Damit eignet sich Mail besonders zur Übermittlung von „Informationen“. Im Gegensatz zum Telefon müssen nicht beide Kommunikationspartner verfügbar sein.

Damit E-Mail systemübergreifend funktioniert, wird in der Regel auf jegliche Anwendung von Formatierung verzichtet. Somit wird keine Zeit und Übertragungskapazität verwendet. Bei einer E-Mail ist die „Nachricht“ von Belang, nicht das Format. Dementsprechend ist es üblich, daß E-Mails nicht mehrfach korrekturgelesen werden und Fehler verziehen werden, solange erkennbar ist, welche Nachricht darin steht.

Mittels E-Mail kann jede elektronisch verfügbare Datei von einem Rechner zum anderen System transportiert werden. Damit eignet sich E-Mail auch zur „Kommunikation“ zwischen einzelnen Prozessen. Es muß nicht immer ein Mensch der Sender und Empfänger einer E-Mail sein.

### 16.2 Was ist ein MTA und was tut er

MTA ist die Kurzform für "Message Transfer Agent". Die ist ein Programm oder ein Prozeß, welcher elektronische Nachrichten einsammelt, weiterleitet und zustellt. Dies passiert meist über Verzeichnisse und definierte Schnittstellen, über welche vorbereitete Messages in einem definierten Format eingestellt und ausgelesen werden können.

Die Funktion eines MTA beschränkt sich darauf, eine Message von A nach B zuzustellen. Voraussetzung dafür ist die korrekte Angabe der Adresse. In diesen Aufgabenbereich fällt zunächst nicht die Führung eines Adreßbuches (global oder lokal) oder eine Vorprüfung der Adressen. Wenn die Form stimmt, geht die Message auf die Reise und kann erst vom Ziel-MTA abgewiesen werden (z.B. Benutzer nicht vorhanden). Ein MTA stellt dem Benutzer kein "E-Mailprogramm" zur Verfügung. Eventuell wird ein einfaches Programm mitgeliefert, welches aber nicht Teil des MTA ist. Es gibt auch Emailprogramme, welche gleich einen MTA mitliefern (MS-Mail) aber damit nicht unbedingt auf einem allgemeinen Standard aufbauen. Für die Post zwischen Benutzern eines Servers ist der Einsatz eines dedizierten MTA nicht unbedingt notwendig. Sobald jedoch Nachrichten zu anderen „Postämtern“ übertragen werden müssen, ist dieser mit entsprechender Kommunikationshardware notwendig.

### 16.3 Remote Mail

Zu fast jedem MTA gibt es auch eine „Remote“-Lösung, damit z.B. ein einzelner PC eines Außendienstmitarbeiters, Heimarbeiters oder Büros in die E-Mail eingebunden werden kann. Dies bedeutet, daß der einzelne PC dann sowohl das E-Mailprogramm, den Einzelplatz-MTA als auch die Kommunikationseinrichtung besitzt. Der Einsatz dieser Komponenten ist jedoch unserer Meinung nach nur bei Notebooks oder absoluten Einzelplätzen sinnvoll, da der Benutzer hier wieder mit der Kommunikation in Berührung kommt. Speziell Personen mit wechselndem Standort braucht dann Kenntnisse über Anschlußtechnik, Wahlverfahren, Amtsholung etc., um erfolgreich Mails auszutauschen. Zudem kann diesen Anwendern Mail nicht „zugestellt“ werden, sondern muß von diesen selbst abgeholt werden.

### 16.4 Die zwei Seiten des MTA

Ein MTA hat zwei Seiten, zwischen welchen er vermittelt. Eine davon ist die Schnittstelle zum "FrontEnd" Diese ist meist als Verzeichnisstruktur ausgebildet. In einem der Verzeichnisse legt man die "Mail" ab (jeder User darf hier schreiben), in einem anderen Verzeichnis kann man seine eingegangene Mail abholen (Hier kann nur der User selbst lesen, jeder User hat seinen eigenen "Posteingangskorb" Wie diese Verzeichnisstruktur aussieht, und in welchem Format die "Mail's" eingestellt werden, definiert der MTA. Diese Schnittstelle kann auch als Datenbank ausgebildet sein. Der Zugriff kann über Dateien oder mittels Funktionsaufrufen erfolgen.

MHS akzeptiert die Mails als Datei in einem Verzeichnis, welche einem bestimmten Format entsprechen. Zu versendende Briefe stellt man in einem festgelegten Format in ein Verzeichnis ein und ankommende Briefe werden in den Posteingang eingestellt, um sie dort weiterzuverarbeiten. Durch das einfache Interface gibt es eine Menge sogenannter "Frontends", d.h. Programme, welche dem Benutzer das Schreiben und Empfangen von Briefen und Anlagen einfache machen.

Andere MTA bietet eine Programmierschnittstelle an (z.B. MAPI für Microsoft Mail). Diese Funktionen können aus verschiedenen Programmiersprachen ausgerufen werden. Auch für MHS sind solche Schnittstellen für Programmierer verfügbar. SENDIT.DLL wird von Infinite Technologies für Windows abgegeben, um MHS-Mails auch mittels Makros und Programmiersprachen unter Windows abzusetzen. Für DOS sind die Utilities SMFSEAL vorhanden.

Die zweite Seite betrifft die Kommunikation des MTA mit anderen MTA's. Die kann über viele Wege passieren, z.B. Modemwählverbindung, Modemfestverbindung, Internetverbindung oder Gateways. Die Beschreibung dieser Schnittstelle legt fest, wie die beiden beteiligten MTA miteinander kommunizieren (Protokolle usw.) Von dieser Schnittstelle bekommt der User nichts mit. Sie ist nur relevant, wenn man wissen will, inwieweit man mit einem Gegenüber Post austauschen kann. Interessant ist hierbei, inwieweit ein MTA mit fremdem Rechnersystemen Kontakt aufnehmen kann und auf wieviel verschiedenen Systemen der MTA ablaufen kann. MHS ist von Anfang an für den Mailaustausch in PC-Netzwerken gedacht gewesen und ist daher auf jedem Personal Computer ablauffähig. Mittlerweile "verstehen" auch der Rechner von CompuServe das MHS-Protokoll. Sogar eine UNIX-Variante von MHS ist verfügbar.

### 16.5 Mailschnittstellen

Im Laufe der Zeit haben sich mehrere PC-basierte Mailprogramme und MTAs entwickelt. Daher gab es lange Zeit viele verschiedenen Schnittstellen. Jeder MTA hatte seine eigene proprietäre Schnittstelle und war oft allein dazu gedacht, das E-Mailprogramm des gleichen Herstellers zu unterstützen.

Seit einiger Zeit sind Bestrebungen im Gang, einheitliche Schnittstellen zu schaffen.

Mittlerweile gibt es von einigen MTA-Herstellern auch passende DLLs für Windows, damit Programme eine bestimmte Schnittstelle auf einem anderen MTA nutzen können. Novell liefert z.B. mit MHSMAPI.DLL ein DLL, damit MSMail auch mit NetWare MHS zusammen arbeiten kann. Unterstützt wird hier nur Global MHS bzw. Connect<sup>2</sup>. Weiterhin ist das Produkt MailSlots von Novell verfügbar, welches sowohl CMC, VIM als auch MAPI unter Windows zur Verfügung stellt. Beide Produkte sind kostenlos erhältlich. Allerdings gibt es wie bei jedem Umsetzer eventuell Probleme mit Sonderzeichen oder teilweise englischen Dialogboxen.

#### 16.5.1 Simple MAPI

MAPI bzw. Simple MAPI ist die Mailspezifikation, welche Microsoft mit MSMAIL und Windows for Workgroups verbreitet hat. Ein Satz von DLL-Aufrufen erlaubt das Senden und Empfangen von Mails. MAPI ist jedoch nur unter Windows oder WinNT verfügbar. MAPI wurde von Microsoft durch CMC ersetzt.

## 16.5.2 CMC

Common Messaging Call (CMC) ist die Nachfolgeschnittstelle für MAPI und beseitigt einige Mängel von MAPI.

## 16.5.3 VIM

„Vendor Independent Messaging“ ist eine Schnittstelle, welche von Lotus, WordPerfect, Novell und anderen Softwareherstellern als Gegenprodukt zu MAPI entwickelt hat.

## 16.5.4 SMF

SMF steht für „Simple Mail Format“ und beschreibt das Interface für MHS. Es gibt die Versionen SMF-64 (MHS 1.1 und früher), SMF-70 (MHS 1.5) und SFM-71 (Global MHS, Connect<sup>2</sup>)

## 16.6 Was ist eine "Mail"

Eine Message besteht aus mehreren fest vorgegebenen Teilen, welche bei MHS als einzelne Datei im Verzeichnisbaum abgespeichert wird.

- 1. Header** Dieser Kopf beinhaltet alle nötigen Informationen zur Mail, d.h. Absender, Empfänger, Betreff, Datum, eventuell Message-IDs, Quittungsinformationen usw.
- 2. Anschreiben** Das Anschreiben besteht im Normalfall aus einem einfachen ASCII-Text, welche kurz Hinweise auf die Attachments gibt oder schon die eigentliche Mitteilung enthält, wenn man auf Formatierung, Schriften und Grafik verzichten kann. Diese Informationen werden im allgemeinen auch nicht verschlüsselt.
- 3. Attachment** Alle Informationen, welche nicht als ASCII-Texte im Anschreiben untergebracht werden kann, wird an die Mail "angehängt" hierbei ist es egal, was nun in dem Attachment drin ist (Sprache, Bilder, Tabellen, Dokumente). Diese Attachments kann man damit auch verschlüsseln (z.B. mit WinWord, Excel, u.a. Sie werden 1:1 übertragen. In Systemen, die keine Binärübertragung zulassen müssen sie zeitweilig umcodiert werden (UUENCODE UUECODE)

Wer nun eine Message ansetzt und empfängt ist freigestellt, d.h. es muß nicht unbedingt ein Benutzer aus Fleisch und Blut sein, sondern es kann auch ein Prozeß sein, welcher die MTA-Funktionalität nutzt, um mit einem anderen Prozeß zu kommunizieren. z.B. Systemmeldungen an den ADMIN schicken, Adreßbücher abgleichen usw.

## 16.7 Netware MHS

### 16.7.1 Geschichte von MHS

Wie jedes Programm macht auch MHS eine Entwicklung durch. MHS hat im wesentlichen folgende Stufen durchlaufen:

- |          |   |
|----------|---|
| MHS 1.0  | Die erste Version von MHS wurde nach kurzer Zeit durch 1.1 ersetzt. Bisher habe ich nicht gehört, daß sie in größerem Maße eingesetzt worden wäre.  |
| MHS 1.1  | Die erste groß eingesetzte Version, welche zuerst "umsonst" war (Im Lieferumfang von NetWare) und dann zum eigenständigen Produkt wurde.  |
| MHS 1.21 | Diese Version war eine überarbeitete 1.1, damit nun auch schnelle Modems (9600 Baud) unterstützt werden konnten. Zudem wurden nun auch unterbrochene Verbindungen wieder aufgesetzt, wodurch sich einige Telefoneinheiten sparen ließen   |
| MHS 1.5  | Diese Version durchbrach nun das starre Adressierungsschema (USERNAME@HOSTNAME) und erlaubt längere Adressen  |
| MHS 1.5C | Der Patch für CompuServe. Somit kann MHS nun den Hub CSERVE nutzen, welcher als weltweiter zentraler Hub fungiert und speziell kleineren Firmen mit geringerem Mailaufkommen die Wege zu MCI-Mail, Fax, Telex, X400 und Internetmail eröffnet. Somit ist es möglich, Post an ein Netzwerk mit MHS zu schicken, ohne Fernleitungen aufzubauen. CompuServe hat in vielen Ländern einen örtlichen Zugang, so daß man sich Interkontinentalleitungen spart. |

MHS 2.0	Diese Version ist erst seit Mitte Oktober 92 auf dem Markt und bietet zur MTA-Funktion auch einen Adressdienst (NetWare Global Messaging).
NGM 2.0	Auf MHS aufbauender MTA als NLM-Implementierung mit Adreßdiensten und erweiterter Funktionalität auch für NetWare 4.0.

Jedes MHS ist sowohl als "Netzwerkversion" als auch als "Personalversion" erhältlich. Der einzige Unterschied ist, daß die Personalversion keine dynamischen Internetverbindungen zuläßt (d.h. kein ATTACH und MAP macht) Sie ist damit geeignet für Laptops und Notebooks, die am MHS-Mailaustausch teilnehmen wollen, ohne ein Netzwerk zu haben. Zusätzlich gibt es eine „-M“-Version für andere Netzwerke mit Internetverbindungen, so daß MHS auch auf LanManager, NFS und anderen Systemen lizenzrechtlich eingesetzt werden kann. Vor dieser „-M“-Version mußte die Personal-Version eingesetzt werden.

### 16.7.2 Das FORMAT einer Mail (SMF-70)

Nachrichten unter MHS 1.5 unterliegen folgender Einschränkung. Die gesamte Mail darf nicht länger als 64 kByte sein und nicht mehr als 64 Empfänger und 64 Kopienempfänger enthalten. Die Größe der Attachments ist (leider) nicht limitiert. Die Datei, welche die Mail darstellt, muß der Definition folgen, welche im MHS-Developerkit (ca. 1200.- DM inklusive MHS 1.5 Netzwerk und MHS 1.5 Personal). Hier sei als Beispiel eine einfache Mail aufgezeigt, welche korrekt zugestellt wird, und sogar mittels Batchjobs erzeugt werden kann, um Systemmeldungen an einen ADMIN zu schicken.

SMF-70

To: ADMIN@hostname

From: -MaiSer-@hostname

Dies ist eine Testmail die man einfach nach MHS\MAIL\SND einstellt. Weiteren Text kann man hier anhängen, z.B. mit type message.txt >> maildateiname  
Der Name dieser Datei hier ist egal, er darf nur keine Extension haben

#### Abbildung 36 MHS Beispielmail

Da MHS verzeichnisorientiert arbeitet, kann man mit der Personalversion auch andere LANs anbinden, welche nicht die Novell-API unterstützen (MS-LAN, Banyan usw. sogar unixbasierende Fileserver können die MHS-Verzeichnisstruktur tragen) Wichtig ist nur, daß ein gemeinsames Laufwerk auf allen Rechnern verfügbar ist. MHS selbst läuft originär auf DOS-PCs, Frontends gibt es dazu aber mittlerweile auch unter OS/2, und MAC-OS. Sogar MHS for UNIX ist mittlerweile verfügbar, d.h. daß ein MTA unter UNIX läuft, welcher mit Modem Mail mit einem DOS-basierten MHS austauschen kann

### 16.7.3 Adressierung von MHS

Analog zu Telefonnummern und Postadressen muß auch bei einem E-Mailsystem der Empfänger angegeben werden. Die Adressierung erfolgt bei MHS nach folgender Regel:

```
USERNAME [.ANWENDUNG] @ HOSTNAME [(name)][{extended adress}][[viahost]]
```

Der Username ist die Kennung des Benutzers im Netzwerk und umfaßt 8 Buchstaben. Zu diesem Usernamen gibt es auch ein Postfachverzeichnis unter %MV%\MAIL\USERS\. Die Angabe eines Benutzernamens ist Pflicht.

Die Anwendung ist die gewünschte Zielanwendung. Ein Anwender kann mehrere Programme haben, welche E-Mail zu Kommunikation nutzen. So könnte parallel zum E-Mailprogramm auch ein Zeitplaner existieren, welcher Termine per Mail austauscht. Dann ist mit der Angabe der Anwendung sichergestellt, daß die Post nicht im „Briefkasten“ des Benutzers landet, sondern in seiner Terminplanung. Wird die Anwendung NICHT angegeben, dann stellt MHS das Mailpaket an die Hauptanwendung des Anwenders zu.

Der Hostname ist der Name des MHS-Hosts, an welchem der User definiert ist. Er muß nicht identisch mit dem Namen des Fileservers sein. Der eigenen MHS-Host muß diesen Namen kennen oder einen preferred Hub haben, über welchen die Mail letztlich zugestellt wird. Dieses Feld ist Pflicht und wird in der Regel bei Nichtangabe durch die Anwendung mit dem eigenen Hostnamen ausgefüllt.

In runden Klammern kann der „Volle Name“ angegeben werden, d.h. der Klurname des Benutzers. Dieses Feld ist optional.

In geschweiften Klammern können zusätzliche Informationen übergeben werden. Von diesem Feld machen meist Gateways Gebrauch (z.B. für Faxnummern. Dieses Feld ist optional).

Die Angabe eines Routings in eckigen Klammern ist nur bei MHS 1.5 möglich und sollte nicht verwendet werden. Ziel der E-Mail ist es den Benutzer selbst nicht mit Gedanken über Routings zu belasten.

### 16.7.4 Die MHS-Verzeichnisse

MHS legt bei der Installation einen umfangreichen Baum an. Die Environmentvariable MV zeigt auf die Wurzel des Baumes. Das Unterverzeichnis kann man bei Bedarf auf ein anderes Laufwerk oder Verzeichnis verschieben. Dann muß die Environmentvariable MAIL auf das Verzeichnis verweisen. Da jedoch nicht alle Applikationen diesen Fall korrekt berücksichtigen, sollte man die Standardinstallation belassen.

Das Verzeichnis muß nicht im ROOT eines Laufwerkes stehen, sondern kann auch in einem Unterverzeichnis liegen (z.B. SYS:\PROGRAMMMHS...).

NetWare NGM verlangt jedoch im ROOT des SYS-Volumes zu liegen, daher muß bei der Generierung eines Servers schon genügend Platz auf dem SYS-Volume eingeplant werden.

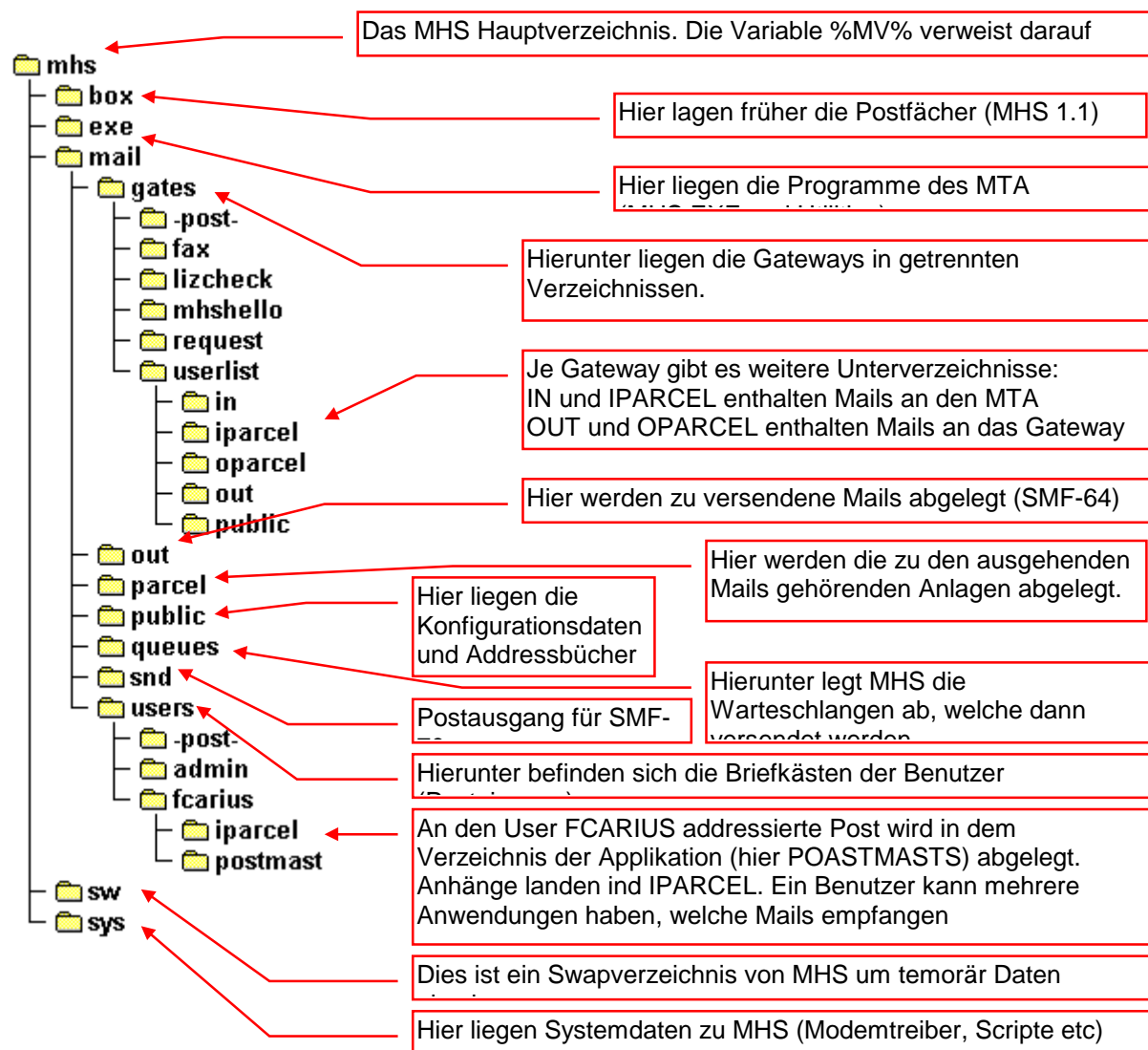


Abbildung 37 MHS-Verzeichnisstruktur

Jeder, der eine Mail verschicken will, schreibt diese in das %MV%\MHS\MAIL\SND-Verzeichnis. Eingegangene Post findet sich unter %MV%\MHS\MAIL\USERS\

### 16.7.5 Die User von MHS

Jeder Benutzer von MHS braucht seine eigene Mailbox. Wenn man nun Post zu einem Benutzer schicken will, muß man den genauen Namen unter MHS wissen. Jede Unstimmigkeit führt dazu, daß die Post nicht zugestellt wird und der Absender eine Mitteilung bekommt. Wie bekommt man aber den Usernamen heraus ?

Entweder man erreicht den Empfänger über andere Kommunikationswege um nachzufragen oder man bekommt ein Adreßbuch des anderen MHS-Hosts. Man kann auch den MHS-Administrator fragen. Jedoch gibt es keine Gewähr, daß der User ADMIN@HOSTNAME existiert.

Bei MHS bedeutet USER nicht unbedingt, daß damit eine Person gemeint ist. Es kann auch ein Gateway oder ein Prozeß sein, welcher Post empfängt und verarbeitet. MHS selbst nutzt solch einen Usereintrag. Unter der Kennung "-MaiSer-" verschickt MHS Quittungen und Nachrichten an User. Man kann auch Post an den User "-MaiSer-" schicken. Diese kommt dann beim Administrator des MHS-Hubs an, welcher in MHS definiert ist. Dies ist der sichere Weg, um eine Adresse herauszubekommen oder Routingprobleme zu klären.

### 16.7.6 Der Begriff "Gateway" bei E-Mail

Gateways bei E-Mail haben die Aufgabe, verschiedene Mailformate und die Adressierung umzusetzen, damit Benutzer unterschiedlicher MTAs Nachrichten austauschen können. Dabei gibt es dedizierte und nondedizierte Gateways, d.h. ein Programm, welche 24h durchläuft und nur Gatewayfunktionen bereitstellt, oder ein Programm welches noch andere Funktionen starten kann oder selbst periodisch gestartet wird.

Bei MHS gibt es eine einfache Möglichkeit, Gateways einzubinden. nachdem man den Gatewaynamen definiert hat, erstellt MHS selbsttätig unter %MV%\MHS\MAIL\GATES ein Verzeichnis mit dem Namen des Gateways und weitere Unterverzeichnisse. Wenn Post zur einem Gateway zugestellt wurde, ruft MHS das Programm OUTPOST.EXE im PUBLIC-Verzeichnis des Gateways auf. Das Programm INPOST.EXE wird bei jedem Durchlauf aufgerufen, damit das Gateway die Möglichkeit hat, eingehende Post zu konvertieren und in MHS einzustellen.

Es gibt Gateways für FAX, X.400, Cityruf, SMTP, UUCP usw. Desweiteren nutzen einige andere Programme den Mechanismus von MHS aus, um komplett von der E-Mail unabhängige Aufgaben zu erledigen oder die Funktionalität zu erhöhen (MHSQ, LIBRARY, Adressabgleich EXDA, usw.)

## 16.8 Gedanken zum Routing

MHS kann über mehrere Wege Nachrichten übermitteln. Neben einfachen Wählverbindungen und WAN-Verbindungen können mittels Gateways auch andere Übertragungswege (z.B. FTP, FTRANS) genutzt werden. Durch all diese Möglichkeiten und der Möglichkeit weltweit Mails auszutauschen ist es nötig, eine geeignete Struktur zu entwickeln. Dies betrifft besonders Personen, welche mehrere Netze unternehmensweit oder weltweit verbinden müssen.

Das Thema Routing ist so prekär geworden, daß mittlerweile Gateways existieren, welche das Routing fast automatisch aktualisieren. Dies ist besonders innerhalb einer Firma sinnvoll. EXDA von Infinite richtet z.B. alle Userroutes einer Arbeitsgruppe (Workgroup) alleine ein. Wird an einem Host ein neuer Host eingetragen, so wird ein Update an die angegebenen Hosts gesendet, worauf an diesen der neue Host auch eingetragen wird als „via“ dem Absenderhost. Die Installation von MHS alleine ist damit sicher einfach. Unterstützende Hilfe ist jedoch dann notwendig, wenn dieses MHS erst der Anfang eines firmenweiten Mailnetzwerkes ist und Verbindungen zur Außenwelt geschaffen werden sollen. Dann ist es sinnvoll, daß Personen mit jahrelangem Umgang mit MHS helfend zur Seite stehen.

Drei grundlegende Gedanken hierzu:

### 16.8.1 Die Sternstruktur/Baumstruktur

Für jede Firma gibt es einen zentralen MHS-Host, welcher 24h aktiv ist und alle User der Firma kennt. Kommunikation mit anderen Unternehmen bzw. weltweit erfolgt nur über diesen Host.

Um die Wege kurz und die Übertragungszeiten klein zu halten ist ein Sternstruktur vorzuschlagen, d.h. alle Host's rufen bei diesem zentralen Host an. Der zentrale Host kennt alle internen Host's und verteilt

auch die Mails. Die internen Hosts haben als preferred HUB den Zentralhost definiert. Dadurch wird es unter Umständen nötig, einen MHS-Verantwortlichen an diesem Zentralhost einzusetzen.

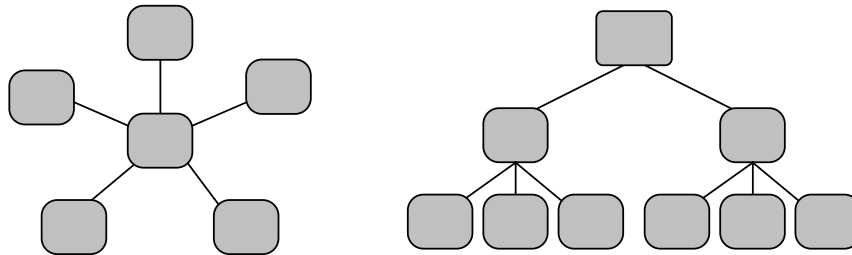


Abbildung 38 MHS-Stern/Baum

Probleme dabei sind die Abrechnung der Telefongebühren und Folgekosten. Als Vorteil kommt die zentrale Verwaltung zur Geltung und die einfache Adressierung. Neue MHS-Hosts sind leicht einzufügen. Es entsteht keine unübersichtliche Masche.

So existiert für jede Firma ein Haupthost, welcher auch die Kommunikation zu anderen Hosts ermöglicht. Ein weltweiter Knotenpunkt (z.B. NHUB oder CSERVE) sichert eine weltweite Erreichbarkeit der Hosts.

Speziell wenn Firmen weltweit tätig sind, wandelt sich der Stern mehr zu einem Baum. Das Routing wird kaum komplizierter, jedoch lassen sich teure Übertragungswege minimieren.

### 16.8.2 Der firmeninterne Ring

Eine andere Variante ist eine firmeninterne Ringstruktur, d.h. daß die einzelnen Hosts ringförmig immer ihren Nachfolger als preferred Host definiert haben. So wird eine Mail herumgereicht, bis sie an einem Host landet, welcher der Zielhost ist oder den Zielhost kennt.

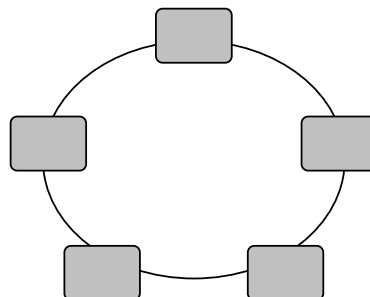


Abbildung 39 MHS-Ring

Vorteil dieser Methode ist, daß bei einem Host nie alle anderen Host's definiert sein müssen. Praktisch ist überhaupt keine Pflege des Routings notwendig. Allerdings können die Nachrichtenwege sehr lange werden. Zudem werden Mails mehrmals übertragen, wodurch die Kosten für Telefongebühren ansteigen. Zudem blockiert der Ausfall einer Station im Ring den Nachrichtenaustausch. Dies kann man gewiß durch Querwege abfangen, aber mit dem Nachteil, daß die Pflege wieder umfangreicher wird. Diese Routingstruktur wird daher so gut wie nie eingesetzt.

### 16.8.3 Die Masche

Optimal im Bezug auf die Nachrichtenwege ist eine Masche. Hierbei kann jeder Host mit jedem anderen direkt Verbindung aufnehmen. Allerdings macht dies das Routing nicht einfach, zudem ist erheblicher Pflegeaufwand je Host notwendig.



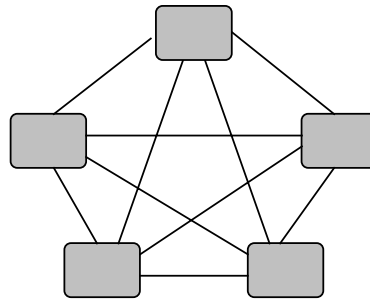


Abbildung 40 MHS Masche

Die Masche eignet sich daher für Firmen mit vielleicht bis zu 10 Hosts. Interessant wird hier dann der Einsatz einer MHS-Workgroup, so daß all diese Rechner nach außen als ein Host erscheinen. Damit darf aber kein Username in der ganzen Firma doppelt vorkommen. Dann ist auch egal, welche Hosts die Kommunikation nach außen machen. Wichtig ist hierbei jedoch, daß die Routings ständig aktuell sind. Dies ist nur mit einem passenden Gateway akzeptabel möglich.

## 16.9 Third Party

Aufgrund der breiten Akzeptanz von MHS als leistungsfähiges Mailsystem haben viele Hersteller die Funktionen von MHS in ihre Produkte eingebaut oder selbst eigene Mailsysteme dazu entwickelt. Ein „MHS-SolutionsGuide“ ist von Novell erhältlich. Aufgrund der offenen Architektur von MHS gibt es auch viele Gateways zu anderen Mailsystemen. Neben dem Zugriff auf andere Mailsysteme sind auch Gateways zu Fax, Cityruf etc. verfügbar.

Die Weiterentwicklung von MHS als serverbasiertes Mailsystem brachte viele Erweiterungen (Lange Namen etc.). Allerdings ist damit zwingend ein Novellserver zum Betrieb notwendig.

### 16.9.1 Mailprogramme

Da MHS ein reiner MTA ist, wird zum Schreiben, Lesen und Verwalten ein Mailagent benötigt. Für MHS gibt es mehrere hundert dieser Agenten, Teilweise sind es eigenständige Programme. Viele Programme haben MHS „eingebaut“, d.h. sind von sich aus „mailenabled“.

Beispiele für Mailprogramme sind:

- DaVinci
- BeyondMail
- OCP Office
- MagicMail
- PegasusMail
- FirstMail
- WinMail
- Framework
- MSMAIL
- und einige andere

Einige Programme sind keine „reinen“ Mailprogramme, sondern haben Datenbankfunktion und können auch noch E-Mail (z.B. Framework). MS-Mail selbst unterstützt als Windowsversion das MAPI. Von Novell gibt es ein MAPI.DLL für MHS. Damit können alle Programme, welche MAPI unterstützen auch mit MHS Nachrichten austauschen.

### 16.9.2 Connect<sup>2</sup>

Daraufhin hat die Firma Infinite Technologies, USA, einen MHS-kompatiblen Messengerouter entwickelt. Dieser nutzt die Plattform DOS, bietet aber stark erweiterte Möglichkeiten. So werden nun mehrere Modems auf einem PC unterstützt und die Kommunikation zu MHS 1.21, MHS 1.5 und auch Global MHS ist problemlos möglich. Dazu wurde auch der Datendurchsatz merklich erhöht. Die

Verfügbarkeit dieses Produktes als 30-Tage Testversion erlaubt es nun jedem, die Vorteile von MHS selbst zu testen.

## 16.10 Gateways, Beispiele der Anwendung

Hier beschäftigen wir uns mit den Gateways; eine Besonderheit von MHS. Ursprünglich waren die "Gateways" dazu gedacht, Post mit nicht MHS-konformen Hostsystemen auszutauschen. Von dieser Art Gateways gibt es mittlerweile jede Menge, z.B. für SMTP, UUCP, X400. Damit MHS auch Post über Telefonleitung und Gateways empfängt, muß in jedem Netzwerk ein PC mit MHS dediziert (am besten 24h) laufen. Dies ist Voraussetzung, daß die Gateways regelmäßig ausgeführt werden. Ab dann ist das Gateway ein universelles Werkzeug, das weit mehr kann, als Post austauschen und zu konvertieren.

### 16.10.1 Zu den Programmdetails

Das Gateway ist ein Programm mit dem Namen INPOST.EXE im Gatewayverzeichnis (meist SYS:MHS/MAIL/GATES/<gatename>/PUBLIC). Da es von MHS aufgerufen wird, von dem Reste im Speicher bleiben muß das Gateway mit einem begrenzten Speicherplatz auskommen. Zu jedem Gateway gehört ein Unterbaum im MHS-Verzeichnis, über welches das Gateway mit MHS kommunizieren kann, wenn dies nötig ist. Man findet ihn unter %MV%/MHS/MAIL/GATES/<gatename>. Das schon erwähnte PUBLIC-Verzeichnis enthält die Programme und sonst dazu nötige Dateien in OUT legt MHS Post ab, die an USERNAME@GATENAME adressiert ist. Der Username ist dabei unerheblich, kann aber von der Gatewaysoftware ausgewertet werden. Attachments dazu landen in OPARCEL. Für den umgekehrten Weg sind die Verzeichnisse IN und IPARCEL vorhanden. Betreibt man die Version MHS 1.5, dann bietet es sich aber an, %MV%/MHS/MAIL/SND und %MV%/MHS/MAIL/PARCELS zu nutzen. Damit umgeht man den Weg über SMFSEAL und kann Mails sogar mit den DOS-Befehlen "COPY" und "ECHO <Dateiname> > Dateiname" erstellen.

INPOST.EXE wird bei JEDEM Durchlauf aufgerufen. Will man ein Gateway bauen, welches nur aufgerufen wird, wenn Post ansteht, so ist der Name OUTPOST.EXE zu wählen

Was dieses Programm nun wirklich tut, ist nicht festgelegt. So lassen sich alle Art von Programmen (welche sich selbst beenden müssen) einbinden. Ich selbst stand vor dem Problem, einige Außenstellen zu haben, welche lange Zeit ohne Administrator laufen. Diese Netzwerke bestehen meist nur aus 5-10 PCs, einem Fileserver, einem MHS und einigen Netports für die Drucker. Da die Benutzer selbst selten das Fachwissen zur Kontrolle des Netzwerkes haben, wurde MHS benutzt um regelmäßig oder auf Anforderung Aktionen durchzuführen. Folgendes ist denkbar oder schon implementiert.

### 16.10.2 MHS als Mailbox

Wer glaubt, EMail würde nur bedeuten, daß eine Benutzer Post an einen anderen Benutzer schickt, irrt. Mit der nötigen Gatewaysoftware ist MHS in der Lage, auf Anforderung eine Datei zu schicken, automatisch Informationen zu verteilen und Diskussionslisten zu führen. Die Funktionsweise ähnelt dem Service der FTP-Server, welche auch auf Mails Dateien zuschicken.

Damit eignet sich MHS vorzüglich zum Verteilen von Dokumenten und Programmen. Dokumente können automatisch an alle Empfänger versandt werden, welche sich in einer Liste eingetragen haben. Dies eignet sich für Rundschreiben, Preislisten, firmeninterne Informationen, Aushänge.

Weiterhin kann mit solch einem Gateway ein Dateidienst aufgebaut werden. Dann werden die Dateien nicht automatisch an Mitglieder einer Liste geschickt, sondern „zur Anforderung“ bereitgestellt, d.h. Es reicht dann eine Nachricht an alle Mitglieder zu senden, welche kurz beschreibt, welche neuen Dokumente verfügbar sind. Zusätzlich kann freigeschaltet werden, daß auch andere Personen als der ADMIN des MHS-Hosts hier Dateien einstellen darf. Dann hat MHS die komplette Funktion einer Mailbox mit dem Vorteil, daß alles auf E-Mail basiert und die Endanwender weiterhin kein Know-how zur eigentlichen Datenübertragung benötigen.

In dieser Art lassen sich auch komplette Diskussionsforen bilden. Nachrichten an solch eine Liste wird allen Mitgliedern zugeschickt. Der Einzelne erhält die Nachrichten und muß die Daten nicht „abholen“.

Dies sind sehr nützliche Funktionen, welche ein Gateway ausführen kann. Die Funktion setzt perfekt auf dem Übertragungsservice von MHS auf. Dies ist jedoch keine „eingebaute“ Funktion vom MHS sondern ein Gateway von Drittherstellern. Allerdings macht MHS diese Funktion einfach und transparent für Benutzer.

### 16.10.3 MHS als Fehlermelder

Netware führt verschiedene Fehlerdateien mit. Dazu zählt das SystemErrorLog genauso wie die Logdateien für die einzelnen Volumes oder NFS. Oft erkennt man aus einigen Meldungen schon Vorboten späterer Ausfälle. Was liegt näher, als diese Meldungen als EMail an den Administrator zu schicken, welche nun irgendwo über MHS erreichbar ist. Ein entsprechendes Gateway, in MHS eingebunden, prüft bei jedem Durchlauf die Existenz der Fehlerdateien. Die vorhandenen Fehler werden als Mail verschickt. So bekommt man auch mit, wenn der Server neu gestartet wurde (Meldung über gemountete Volumes in den Vol\$err.log-Dateien). Um das Mailaufkommen gering zu halten, sollten nur die neuen Einträge als Mail verschickt werden. Dies kann man erreichen, indem man die Originaldateien löscht (Netware legt sie dann immer neu an) oder nur die Unterschiede der bei letzten Durchlauf gesicherten Datei schickt (MS-DOS-COMPare-Befehl)

### 16.10.4 MHS als Statistiker

Eine weitere Anwendung als Gateway ist die Überprüfung systemrelevanter Daten. Unter Verwendung kleiner Helfer aus der NetWare (CompuServe) oder anderer Quellen kann man regelmäßig die statistischen Daten des Fileservers erfassen (Connections in use, CacheBuffers, Utilisation usw.) und in einer Datenbank ablegen. Ein dazu passendes Frontend kann diese dann auswerten. So einfach können Langzeitstatistiken werden. Allerdings kann man so keine Spitzenlasten herausfinden, da das Gateway nur kurze Zeit läuft und regelmäßig eine Stichprobe entnimmt.

### 16.10.5 MHS überprüft echte Gateways:

Im Netzwerk laufen noch viele weitere Gateways. Meistens ist die Gatewaysoftware selbst als TSR-Modul aufgebaut, so daß theoretisch auf dem Gatewayrechner selbst noch gearbeitet werden könnte. Jedoch ist dies nicht unbedingt zweckmäßig, da beim einem Absturz der Anwendung auch das Gateway hängt und dies auf Dauer zu Konflikten bei dem Gatewayanwender führen dürfte. Aber man kann einen Batch starten, welche zyklisch eine Message an ein Gateway schreibt in der Art "Hallo ich lebe noch". Dies kann eine "echte" Message sein, oder einfach eine Datei, dessen Existenz das MHS-Gateway abfragen kann. Wenn MHS dann z.B. alle 10 Minuten einen Durchlauf startet, muß das Gateway z.B. alle neun Minuten eine solche Datei erzeugen. Das Gateway selbst sendet eine Mail an den ADMIN, wenn diese Datei NICHT vorhanden ist. Ist sie da, so wird sie gelöscht, damit sie vom Gateway wieder angelegt werden kann. Wenn der ADMIN diese Mail erhält, ist das die Nachricht, daß das überwachte Gateway möglicherweise ein Funktionsstörung hat. Dies ist besonders dann sinnvoll, wenn die Gateways nicht direkt von Benutzern angesprochen werden, oder ein Ausfall nicht sofort entdeckt würde.

### 16.10.6 MHS als Zugang zur Fernwartung

Wenn MHS nun 24 Stunden "online" ist, wird es jedoch speziell bei kleineren Netzwerken nicht voll ausgelastet sein. Jedoch bietet sich so das Modem und der PC dazu an, mehr zu tun, als nur zur Kommunikation MHS <-> MHS. Ein Versuch dies zu machen sind FAX-Gateways oder Gateways, welche eine Mail als Message an einen Cityrufempfänger schicken. Interessanter ist aber hier ein Gateway, welches nach einer entsprechenden Mail MHS selbst runterfährt und den PC für eine Remotesession vorbereitet (z.B. Carbon Copy, CloseUP, usw.). Um hier jedoch die Funktion sicherzustellen, sollten zwei Mechanismen eingebaut sein:

- Der PC sollte booten, wenn der Carrier bei dieser Session unterbrochen wird.
- für alle Fälle sollte eine Schaltuhr den PC (und auch das Modem, um die Verbindung zu kappen) gegen Mitternacht kurz ausschalten, so daß spätestens nach einer Nacht MHS wieder aktiv ist.

Die Methode "Schaltuhr" ist bei vielen unserer Gateways eine sichere Möglichkeit, deren Funktion sicherzustellen. Die Software sollte natürlich damit keine Probleme haben. MHS überlebt das problemlos. Man sollte nur vor dem Start von MHS in Verzeichnis %MV%\MHS\SW die alten Swapfiles löschen lassen (Hoch leben die Batchfiles)

### 16.10.7 MHS zu X400, Internet, MCI-Mail, MSMail, WordPerfect

Aufgrund der weiteren Verbreitung und Leistungsfähigkeit von MHS haben viele Hersteller Gateways entwickelt, damit eigene Produkte mit MHS zusammen arbeiten oder MHS-Nachrichten an andere Mailsysteme übersetzt werden können. Damit kann MHS als leistungsfähiges unternehmensweites Mailsystem verwendet werden, während bestehende Mailprogramme eingebunden werden können.

Dies geht so weit, daß z.B. MSMAIL in Handbuch aufzeigt, wie mehrere MS-MAIL-Postoffices über das Gateway zu MHS und MHS selbst verbunden werden können und Kontakt zu anderen Systemen aufnehmen kann.

### 16.10.8 MHS und FAX

E-Mail eignet sich hervorragend für Kommunikation zwischen Personen um viel Information mit wenig Rücksicht auf Formatierung zu übertragen. Nun kommt sicher der Fall vor, daß nicht alle Personen einer Arbeitsgruppe E-Mail nutzen können. Daher können solche E-Mailnachrichten auch per FAX an ausgewählte Empfänger versendet werden. Diese transparente Möglichkeit erlaubt es, Verteiler in einer Mail zu nutzen und das System selbst versendet diese Mail an Faxempfänger. Allerdings kann MHS keine Umsetzung der Anlagen per Fax machen. Einige Lösungen erlauben es, HPPCL oder DCX-Dateien als Anhang mitzuschicken. Damit muß aber der Absender seine Dokumente wieder in diese Formate konvertieren oder eine entsprechende Druckfunktion der Anwendung läßt dies zu. Da der Charakter einer Mail aber mehr auf der Informationsseite besteht, ist auch der Versand der Mail selbst als Fax mit passendem Deckblatt schon ein guter Schritt zur Vereinfachung der Kommunikation.

### 16.10.9 MHS und Signalisierung

Da der MHS-PC sowieso mit einem Modem verbunden ist und viele Dienste der Telekom per Modem zu erreichen sind, kann ein Gateway von MHS z.B. Cityrufempfänger anpiepen oder besonders beim alphanumerischen Pager die Textinformation übermitteln. Besonders der „Short Message Service“ bei den immer weiter verbreiteten D-Netz-Telefonen bietet sich auch hierfür an.

### 16.10.10 MHS sagt Hallo

Mail dienen zur Benachrichtigung von Personen. Nachrichten können auch von Programmen an Benutzer generiert werden. Daher ist auch ein Gateway vorstellbar, welches zu bestimmten Zeiten eine Mail an bestimmte Benutzer schickt. Was liegt näher als einen „Erinnerungsmelder“ einzubauen. Der Anwender schickt eine Mail an dieses Gateway und gibt den „Aufweckzeitpunkt“ mit. Das Gateway speichert diese Mail bis zum besagten Zeitpunkt und schickt diese dann als Erinnerung zurück. Hier ist jedoch die Einschränkung, daß MHS nicht dauernd dem Gateway die Kontrolle übergibt. Eine langandauernde Datenübertragung kann die Gateways eine Zeit lang außer Funktion setzen.

### 16.10.11 MHS als Batchstarter

Letztlich kann man als Gateway auch eine COMMAND.COM starten, welche man einfach mit dem Namen INPOST.EXE in das Gatewayverzeichnis kopiert. Als Kommandozeile gibt man einfach "/C Batchname" an. Leider ist die Kommandozeile begrenzt, so daß es kaum zu vollen Pfadangabe des Batches reichen dürfte. Daher muß der Batch in einem Suchlaufwerk liegen (Suchpfad). Dies ist zweifelsfrei die universellste Art, ein Gateway zu basteln. Wer von der Mächtigkeit der Batchjobs weiß, kann sich ausmalen welche phantastische Gateways denkbar sind. Viele der oben angeführten Gateways lassen sich mit dieser Methode realisieren.

Sichergestellt sein muß jedoch, daß das Gateway ohne Benutzeraktion wieder sich selbst beendet.

### 16.10.12 MHS und Datensicherheit

Wo und wie macht man am besten ein Backup, wenn die Netzwerke ohne Administrator laufen ?. Mit Gateways kann auch MHS dies. In der Regel ist der Mailaustausch über die Nachtzeit nicht notwendig. Daher kann der PC, welcher tagsüber Mails verteilt, spät in der Nacht eine Datensicherung ausführen. Während dieser Zeit ist MHS dann nicht aktiv und die Zeitschaltuhr sollte so eingestellt sein, daß nach dem Backup aber auf jeden Fall morgens ein Neustart die Funktion der Mail sicherstellt. Damit beschränkt sich die Aufgabe der ortsansässigen Mitarbeiter gerade auf das tägliche Auswechseln des Bandes. Den Abschlußbericht über das Backup kann dann wieder als Mail verschicken lassen.

### 16.10.13 MHS als Saubermann

Netware behält gelöschte Dateien zum SALVAGE bereit, es sei denn, der Platz würde anderweitig gebraucht. Gerade bei der EMail werden viele Dateien (je Mail eine Datei plus Attachments) gespeichert und gelöscht. Ein PURGE-Gateway auf %MV%/\*.\* beseitigt erstens diese alten Dateien, so daß NetWare diese nicht mitführen muß (Performance) und zudem nicht wiederhergestellt werden können. Dies ist speziell dann ein Argument solange MHS den Mailkörper unverschlüsselt schickt. Das

PURGE-Gateway kann natürlich auch z.B. alle \*.SIK \*.TMP usw. löschen, soweit MHS die Zugriffsrechte auf die Userdatenbereiche hat.

#### 16.10.14 MHS als Lizenzkontrolle

Mittlerweile gibt es Gateways für MHS, welche von definierten Dateien die Anzahl der Öffnungen lesen. Damit läßt sich z.B. feststellen, wie oft ein Programm in Benutzung ist. Wird einer eingestellte Schwelle überschritten, dann wird eine Mail an bestimmte Benutzer geschickt. Alternativ können die gesammelten Daten auch als Logdatei abgelegt werden, und damit zu einer kontinuierlichen Auswertung führen. Dieses Gateway kann allerdings nur „messen“ und nicht den Zugang zu Programmen verwehren. Auch ist eine gleichmäßige Kontrolle nicht sicher möglich, wenn MHS z.B. Dateien überträgt, und damit keine Gatewayprozesse startet.

#### 16.10.15 MHS und Datenbanken

MHS selbst kann nicht direkt mit Datenbanken kommunizieren. Jedoch gibt es für fast jede Datenbank DOS-basierte Abfrageprogramme, welche auch batchgesteuert ablaufen können. Damit lassen sich selbst Gateways entwickeln, welche bestimmte Schlüsselwörter als Anfrage an die Datenbank absetzt und das Ergebnis als Mail zurückschickt. Allerdings ist hierbei die Zeitverschiebung zwischen Anfrage und Antwort meist hinderlich. Zudem sollte hierzu ein eigenes Abfrageprogramm entwickelt werden, damit die Anfrage entsprechend einfach gestaltet ist.

Allerdings eignet sich MHS sehr gut zur Synchronisation von Datenbankkopieren. So sind Gateways im Einsatz, welche Datenbanken in Außenstellen während der Nacht aktualisieren. Dazu wird abends eine Datei mit den Änderungen der Masterdatenbank automatisch erstellt und an die Außenstellen geschickt. Dort arbeitet ein MHS-Gateway die Änderungen ein.

Dieser automatisierte Datentransfer kann natürlich auch z.B. für monatliche Abschlußberichte und Umsatzmeldungen und Bestellmeldungen an eine Zentrale benutzt werden.

#### 16.10.16 MHS als ???

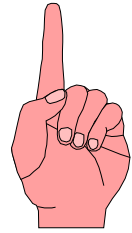
Wie sicherlich aufgefallen ist, gibt es massenhaft Ideen, um den MHS-Prozeß universell einsetzbar zu machen. Einige Gateways sollen nur zu bestimmten Zeiten einmal aufgerufen werden. Entweder man macht die Zeitabfrage im Gateway selbst, oder benutzt ein weiteres Gateway, welches nichts anderes zu tun hat, als die übrigen Gateways zu bestimmten Zeiten zu aktivieren und sonst zu deaktivieren. Dies hat den Vorteil, daß die Gateways nur an festgelegten Zeiten aufgerufen werden, und MHS so weniger Last erzeugt.(z.B. Schedule-Gateway von Infinite). Gateways sollten UNTER KEINEN UMSTÄNDEN den PC stoppen oder eine interaktive Eingabe erwarten, da der MHS-PC in der Regel unüberwacht läuft.

Einen anderen Aspekt gilt es noch zu berücksichtigen. mit den Gateways kann man viel machen; für einige Aktionen muß man dazu MHS jedoch Rechte einräumen, die im Normalfall nicht geGRANTed werden. Daher muß man sich Gedanken machen, wie man den PC und den Usereintrag "MHS" schützt.

Bei all den Gateways darf man nicht übersehen, daß jedes Gateway ZEIT braucht. Zeit, während MHS keine Anrufe entgegen nehmen kann. So muß man aufpassen, damit sich keine Warteschlangen bilden und die anrufenden Hubs wegen zu vielen Fehlversuchen (BUSY) den Host deaktivieren (Aber selbst dazu gibt es ein Gateway, um deaktivierte Hubs wieder zu aktivieren). Dagegen hilft dann aber, einen weiteren Transportserver (ein PC mit extra Modem und Anschluß) aufzubauen, welcher eingehende Anrufe immer entgegennehmen kann.

Ein weiterer Punkt ist, daß man nie garantieren kann, daß ein Gateway zu einer bestimmten Zeit aufgerufen wird. Wenn MHS viele Daten zu übertragen hat (bei uns liegt das manchmal schon im Megabytebereich), werden während dieser Zeit keine Gateways aufgerufen, d.h. es ist nicht so, daß MHS alle 10 Minuten (je nach eingestellter Scheduleszeit) die Gateways aufruft.

## 17 Regeln



### 17.1 Grundregeln für Benutzer

1. **Keine Programm selbst installieren**  
denn wenn mehr als eine Person das gleiche Programm benutzt, ist es besser, dieses für alle zentral zu installieren, statt die gleichen Teile mehrfach auf der Festplatte zu speichern. Zudem kann man dann mit Zugriffsrechten das Versehentliche Löschen oder Ändern von Programmen verhindern.
2. **Keine Kabel abziehen,**  
da an dem Netzwerk nicht nur Ihr Computer angeschlossen ist, und unter Umständen ALLE Benutzer lahmgelegt sind. Neben dem Ärger kommt auch der Verlust von Daten hinzu; eine teure Angelegenheit.
3. **Password regelmäßig ändern,**  
damit Ihre Daten sicher sind und keine fremden Personen Ihre Daten verändern
4. **Nicht mehrfach drucken**  
denn das Netzwerk "vergißt" nichts. Wenn ein Ausdruck nicht sofort erscheint, hilft auch ein mehrmaliges Drucken nicht weiter. Dann ist die Kette vom Computer zum Drucker irgendwo gestört. Wenn ein anderer Benutzer drucken kann, so ist bei Ihrem PC die Einstellung nicht korrekt. Mehrfaches Drucken blockiert die anderen Benutzer und erzeugt unnötig Papier.
5. **„Verbotene Verzeichnisse**  
Bitte legen Sie aus eigenem Interesse niemals etwas in H:\SYSTEM und dessen Unterverzeichnissen oder Daten in H:\TEMP ab. Dies sind für das System notwendige Verzeichnisse, deren Inhalt automatisch geändert oder gelöscht wird.

## 17.2 Regeln für den Supervisor

1. Programme NIE umbenennen, (Dies tut man gewöhnlich, daß der Aufruf garantiert über den BATCH erfolgt) Besser den Programmnamen beibehalten und den Batch anders benennen (z.B: MIT Versionsnummer im Namen) und den Benutzern nur diesen Namen nennen.
2. User mit Write-Rechten auf den Programmbereich dürfen NIE Userprogramme in deren H: starten um Viren zu stoppen. (Rechte auf \*.EXE und \*.COM Programme beschränken mit NetWare 3.x Filetrusties)
3. Verzeichnisse immer mit der Versionsnummer der Anwendung kombinieren So können Updates parallel vorgenommen und getestet werden. Anwendungen die dies NICHT unterstützen sollten wirklich auf ihre Gebrauchsfähigkeit hinterfragt werden, denn als Administrator müssen SIE viele Programm integrieren.
4. Namen jeglicher Art sollen NIE länger als 8 Buchstaben sein, wenn sie beim Einloggen benutzt werden, da MAP mit %LOGIN\_NAME sonst fehlerhaft arbeitet. (Sonderfall Supervisor im SystemLoginscript extra abfangen)
5. Alle Programmaufrufe in Batchjobs VOLL deklarieren, keine Suchlaufwerke nutzen. Das bringt Tempo, da die Suchpfade nicht durchsucht werden und man weiß genau, welches Programm nun gestartet wurde (=Eindeutigkeit; z.B. <Lw>:\<Pfad>\<PROGRAM>.<EXT>).
6. Kein USERLOGINSRIPT -> Geht schneller, ist nicht nötig, weniger Dateien. System Loginscript mit EXIT "USERSFG.BAT" verlassen (Ohne EXIT treten manchmal sonderbare Effekte auf). Statt des userloginscript gibt es einen Batch für den Benutzer (H:\USER.BAT)
7. Jede Aktivität am Server, die vom Supervisor oder einem Operator durchgeführt wird, muß sofort dokumentiert werden. Die Arbeitsabläufe werden durch entsprechende Formulare unterstützt. (Gruppenverzeichnis SUPPORT). Zumindest ein Logbuch sollte geführt werden, um Fehlerursachen später eingrenzen zu können.
8. Prinzip der Lokalität bei Programmaufrufen. Nach dem Verlassen des Programmes müssen die alten Zustände wieder hergestellt sein im Bezug auf Pfade, Laufwerke, TSR-Programme.
9. Die Übertragung von Zugriffsrechten über die Funktion "Security Equivalences" ist streng verboten. Ausgenommen ist das Anlegen des Benutzer "ADMIN", der als Security Equivalent zum Supervisor eingetragen wird.
10. Das Supervisor-Passwort wird verschlossen an einer zentralen Stelle aufbewahrt und darf nur für Softwareinstallationen und Aufgaben genutzt werden, wo dies unbedingt erforderlich ist. Ansonsten wird ADMIN benutzt.
11. Der Supervisor, sein Equivalent und BACKUP sind als einzige im System in der Lage alle Benutzerdaten zu lesen. Alle anderen Benutzer dürfen dazu als Voreinstellung keine Berechtigung haben. Auch der Operator hat keine Leserechte auf Benutzerdaten (Datenschutz). Aber Rechte auf ausgewählte user (DUMMY, Gateways usw) sind denkbar.
12. Jeder Benutzer hat seinen Usernamen mit den Standardeinstellungen, d.h. auch der Administrator arbeitet normal ohne erweiterte Rechte unter seiner normaler Kennung. Nur so sieht er auch, wenn etwas nicht läuft, weil er zuwenig Rechte hat. Also ADMIN ändert er Systemeinstellungen, arbeitet aber nicht als Benutzer.
13. Das Serverkonzept und die daraus abgeleitete Struktur ist vollständig zu dokumentieren. Blöder Spruch, aber es muß ja kein Buch werden. Aber man muß die Daten wissen, die nötig sind um dem Server komplett neu aufzubauen (Netzwerknummern, Hardwareadressen, Router, ...)
14. VORSICHT bei gemeinsam genutzten Programmen, Batchjobs und Dateien. Schon ein einfacher „View“ mit einem Editor kann die Datei sperren, da viele Editoren die Datei „exclusiv“ öffnen. Änderungen an Batches sind tückisch, da Stationen, welche den Batch abarbeiten (z.B. WIN31.BAT) nach dem Speichern an die falsche Stelle einspringen.
15. \_\_\_\_\_
16. \_\_\_\_\_

## **18 Betriebspersonal**

Ein Netzwerk installiert sich nicht von alleine und muß gepflegt werden. Auch die Benutzer eines Netzwerkes müssen auf die Besonderheiten und Anforderungen geschult werden. Bei größeren Netzwerken gibt es meist mehrere Personen mit unterschiedlicher Qualifikation. Daher muß dann eine Festlegung der Arbeitsaufgaben erfolgen. Leider unterstützen die meisten Netzwerke nicht die Einrichtung von besonderen Benutzern, denen man gezielt einige Rechte nehmen könnte. Daher muß man diese Personen von Hand eintragen. Ursprünglich gibt es in Netzwerken nur den "normalen" Benutzer und den Supervisor

Um die Betriebssicherheit und die Funktion eines Netzwerkes zu erhalten, ist es notwendig, Administratoren und Operatoren vor Ort zu haben. Dies gewährleistet ein schnelles Eingreifen bei Fehlern. Die enge Verzahnung zwischen Administrator und Firma stellt zudem sicher, daß das Betreuungspersonal des Netzwerkes möglichst Kenntnisse der firmeninternen Anforderungen besitzt und damit mehr als jedes externe Unternehmen versteht, welchen Anforderungen ein Netzwerk entsprechen muß. Damit wird eine Schulung dieses Personals notwendig. Nicht jeder Mitarbeiter muß komplett unterwiesen werden. Sofern dies sinnvoll ist, kann man nach „Administrator“ und „Operator“ trennen. Operatoren nehmen einfache Aufgaben dem Administrator ab und lösen normale Probleme. Damit ist der Administrator entlastet und kann die Installation neuer Software und konzeptionelle Arbeit leisten.

### **18.1 Supervisor und Admin**

Der Supervisor ist der "ALLMÄCHTIGE" im Netzwerk. Er darf alles und kann dementsprechend viel kaputt machen. In der Regel wird man sich einen zweiten Benutzer einrichten, welcher Supervisorequivalent ist. Dadruch hat man zwar keinen Schutz, aber man kann das Supervisorpassword im Briefumschlag in einen Safe legen und hat so eine Hintertür frei, wenn das ADMIN-Password vergessen wurde oder der Account gesperrt ist.

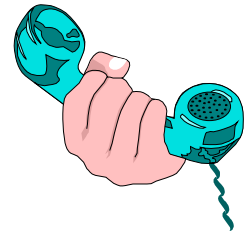
### **18.2 Operator**

Es bietet sich an, in größeren Netzwerken Operatoren zu benennen, welche die tägliche Routine abnehmen. d.h. Drucker initialisieren, Druckjobs löschen, Gateways pflegen usw.

Der Operator sollte jedoch nicht in die Datenbereiche von Benutzern einsehen können und kritische Aktionen ausführen können (z.B. Server downfahren, Serverplatten initialisieren usw.) Wo hier die Grenzen gezogen werden, ist nicht einfach. Es wäre angenehm, wenn ein Operator z.B. die Uhrzeit im Netzwerk stellen oder von Benutzern gelöschte Files wiederherstellen könnte. Jedoch braucht er dazu "Consolerights", bzw muß die Benutzerverzeichnisse einsehen. Mittlerweile gibt es bei NetWare die Möglichkeit, "Workgroup Managers" einzurichten, welche eine bestimmte Gruppe von Benutzern verwalten dürfen, aber nicht die anderen Benutzer. Im Bereich "Drucken" kann man "Print Server Operatoren" und "Queue Operatoren" angeben. Diese Personen dürfen dann Printserver konfigurieren und Druckjobs steuern.



## 19 Support



Je mehr PC's eingesetzt werden, desto eher kommt man in die Lage, defekte Hardware austauschen zu müssen. Wenn man sich dazu kein eigenes Lager einrichten will, muß man sicher sein, daß die Hardware schnell und zuverlässig geliefert werden kann. Nichts ist ärgerlicher als der Ausfall des Fileservernetzteils.

Die Hardware und Software entwickelt sich sehr schnell weiter. Daher ist es auch für den Administrator unerlässlich, sich selbst weiterzubilden. Dies kann durch spezielle Schulungen geschehen, oder durch Mitlernen und Erfahrungsaustausch mit anderen Netzwerkadministratoren. Es gibt jedoch immer einige Situationen, wo das eigenen Wissen nicht ausreicht. Dann lohnt es sich, eine Ansprechstelle im Hintergrund zu haben. Dies kann der Fachhändler sein, welcher die Netzwerksoftware verkauft und hoffentlich selbst fachkundige Personen hat oder Mailboxen, durch welche man viele Netzwerkadministratoren erreicht.

### 19.1 NETWIRE

NetWire ist ein Forum in CompuServe. CompuServe ist ein Dienstleistungsanbieter, welcher weltweit Zugänge zu seinem Netzwerk zur Verfügung stellt. NetWire selbst ist ein Bereich in diesem Onlinesystem, über welches man Fragen und Antworten absetzen kann und die aktuellen Dateien von Novell erhalten kann. CompuServe selbst ist nicht kostenlos, d.h. es fallen Kosten an, welche sich aus Verbindungsdauer und Art zusammensetzen. NetWire selbst muß nicht extra bezahlt werden. NetWire wird regelmäßig von Novell und anderen Spezialisten gelesen und lebt davon, daß man auch anderen Administratoren bei Problemen hilft. Die Hilfe selbst ist daher kostenlos. Viele Foren funktionieren als "Schwarzes Brett" und leben vom mitmachen.

### 19.2 CNE



CNE ist die Abkürzung für "Certified NetWare Engineer". CNE's haben eine Prüfung abgelegt, in der sie umfangreiches Fachwissen belegt haben. Es wird nicht unterschieden, ob ein CNE dieses Wissen in der Praxis erworben hat, oder einfach die Schulungen durchlaufen hat, um als Mitarbeiter einer Firma diese zum Fachhändler zu machen. Allgemein ist der CNE aber ein Zeichen, daß derjenige sich intensiv mit Produkten von Novell befaßt hat.

### 19.3 CAP



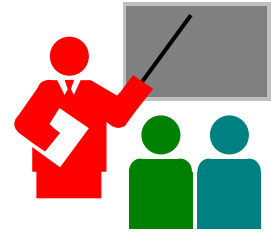
Das CAP-Programm von Novell soll eine Partnerschaft zwischen Novell und freiberuflichen Beratern und Firmen darstellen. Als Mitglied des CAP-Programmes pflegt man einen engeren Kontakt mit Novell, wird informiert und unterstützt. Diese Unterstützung kann direkt dem Kunden zugute kommen. Hohe Aufnahmeanforderungen stellen sicher, daß das CAP-Logo und die damit ausgezeichneten

Firmen einen hohen Kenntnisstand und qualitative Arbeit liefern und die Produkte von Novell kennen und unterstützen.

#### **19.4 NAR, NAEC**

NAR's und NAEC's sind Firmen, welche einen besonders engen Kontakt zu Novell pflegen und ihre "Tauglichkeit" jährlich aufs neue beweisen müssen. Daher kann man sicher sein, auch dort zuverlässig geholfen zu bekommen. Jedoch kann man nicht erwarten, daß diese Dientsleistung umsonst ist. Die Ausbildung der eigenen Mitarbeiter und die Anforderungen, welche Novell stellt, erzeugen zusätzliche Kosten, die ein einfacher Softwareverkäufer nicht zu tragen hat.

## 20 Schulung



Die Investitionen in eine Schulung rechnen sich immer erst dann, wenn die Anwender auch damit arbeiten. So kann man zu jeder gekauften Software nochmal einen Aufwand für die Schulung rechnen. Zwar kann eine Schulung keinen Mitarbeiter zum professionellen Benutzer ausbilden, aber eine Schulung soll den Einstieg erleichtern und die Anfangsängste abbauen. Damit wird letztlich die Motivation gefördert und die Investition schneller amortisiert. Bei der Schulung kann vom Trainer auch ein Feedback an die Administratoren kommen, an welchen Stellen die Anwender sich Vereinfachungen und Arbeitserleichterungen wünschen (z.B. Textbausteine, Vorlagen, Adressdatenbanken). So werden Fragen und Probleme auf kurzem Wege an die EDV-Verantwortlichen weitergeleitet. Neben den eigentlichen Anwendern müssen aber auch die Administratoren auf dem Laufenden gehalten werden.

### **20.1 Anwenderschulung**

Wenn man den Benutzern eines PC's nicht schult, um mit dem PC effektiver zu arbeiten, wird die Akzeptanz des Netzwerkes und die erhoffte Einsparung nicht eintreten. Zudem wird es viele "Eigenbauten" geben, welche am Ende den Betrieb des Netzwerkes unmöglich machen. Daher ist es nötig, die Benutzer zu schulen, zumal vielen keine Wahl gelassen wird, ob sie einen PC wollen oder nicht. Denn erst die komplette Integration erlaubt es, Mail auszutauschen und Dateien und Drucker zu teilen. Neben der Grundschulung zum Umgang mit dem PC und Windows 3.1 muß ein besonderes Augenmerk auf die Gegebenheiten im Netzwerk (LOGIN, LOGOUT, Drucken im LAN, EMail) geworfen werden. Diese Schulung kann intern oder extern erfolgen.

Der Administrator sollte sich aber ab jeden Fall VORHER mit dem Trainer in Verbindung setzen, um spezielle Punkte einzubinden. Schließlich sollte diese Schulung den Administrator entlasten.

Zusätzlich zu der reinen Schulung für die Belange des Netzwerkes können auch die eigentlichen Anwendungen geschult werden.

Gerade die heutigen Anwendungen auf dem Personal Computer sind so mächtig und umfangreich, daß kein Anwender ohne eine ausreichende Unterstützung damit arbeiten kann.

So bieten sich Einsteigerkurse in die gängigen und installierten Anwendungen an. Dabei gilt es immer, die Bedürfnisse der Anwender zu verstehen und dazu passende Themen und Inhalte zu wählen. So sind Serienbriefe sicher nicht für alle Anwender notwendig und andererseits „Gruppenarbeit“ an einem Handbuch sicher auch nur für weniger Personen notwendig. Ein Schulungskonzept kann immer nur individuell auf die zu schulenden Personen erstellt werden.

### **20.2 Operatorschulung**

- Was ist ein LAN (Server, Client, Kabel, Laufwerke, Drucker)
- Vom Einschalten zum Login
- Windows im LAN (Konzepte, Level, Konfiguration)
- Drucken im LAN (Konzepte und Hilfsmittel der Fehlersuche)
- Programme auf dem Server (Windows, Mail, Fax)
- Arbeiten im LAN mit NetWare (Utilities)
- Gateways (Fax, Mail, Backup)
- Verwaltung MAIL

### **20.3 Administratorschulung**

- Installation User und Gruppen

- Installation Drucker und Warteschlangen
- Installation von Hardware und deren Konfiguration
- Installation von Software
- Serverkonzepte (Mirror, UPS, LAN-Boards, NLMs)
- Backup & Restore

#### **20.4 Workshops**

Zusätzlich zur reinen Vermittlung des Wissens zur Verwaltung können zusätzliche Workshops zu besonderen Themen ein Hintergrundwissen schaffen, welches nicht unbedingt direkt zum Einsatz kommen kann, aber das Verständnis und das Erkennen zukünftiger Anforderungen erleichtert. Denkbar wären folgende Themen:

- Programmierung NetWare
- der Server im TCP/IP-Lan (Flex-IP, NFS)
- ISDN im LAN
- Netzwerkanalyse und Messtechnik
- Serverworkshop (Mirroring, Umbauten, Routing)
- LAN/WAN Repeater/Bridge/Router/Gateway Protokolle
- Produktübersicht NetWare
- NetWare, Wie bleibt man UpToDate
- Peer2Peer v. Serverbasiert (WFW, Personal NetWare, NFS)

## **21 Troubleshooting**

Wenn ein Netzwerk von Anfang an ohne Probleme läuft, kann man sich glücklich schätzen. Meistens gibt es früher oder später Defekte, welche sich durch Alterung und neue Anforderungen erklären. Daher ist es nötig, auch in diesen Fällen systematisch den Fehler suchen zu können. Um Fehler zu finden, gibt es verschiedene Werkzeuge.

### **21.1 CablesScanner**

Diese speziellen Meßgeräte prüfen das Übertragungsmedium, d.h. sie testen, ob die Kabel und Steckverbinder in Ordnung sind. Somit ist es möglich, defekte Kabel und Verbindungen ausfindig zu machen. Diese Geräte sind jedoch nicht gerade billig. Sie werden häufig auch genutzt, um nach der Installation des Kabels dieses zu protokollieren und damit vom Auftraggeber abgenommen wird. Somit kann die Installationsfirma belegen, daß Sie ihre Arbeit korrekt beendet hat.

Zu diesen Geräten gehören auch TDM-Meter, welche ein kurzes Signal auf die Leitung geben und danach die Echos abhören. So lassen sich sogar Dämpfungen feststellen, welche durch zu geringe Biegeradien beim Verlegen der Kabel entstehen.

Um Kabelfehler zu lokalisieren gibt es je nach Medium eigene preiswerte Methoden. Diese Hilfsmittel greifen meist jedoch nur, wenn das Netzkabel komplett tot ist. Treten in einem Netzwerk jedoch gehäuft verstümmelte Pakete auf oder sind die Ausfälle nur sporadisch, kommt man so nicht weiter.

Bei Cheapernet ist es z.B. möglich, Segmente abzuhängen und das Hauptsegment mit Abschlußwiderständen zu terminieren. Wenn danach das Teil-Lan wieder ok ist, kann der Fehler nur im abgehängten Stück liegen. Durch schrittweises Anschließen einzelner Stationen findet man sehr schnell die defekte Stelle.

### **21.2 Protokollanalyser**

Protokollanalyser sind Spezialcomputer oder Software, welche die Datenpakete auf dem LAN mitprotokollieren und auswerten. Damit kann man defekte LAN-Karten, Router oder Software finden. Diese Computer sind meist PC's mit besonders schnellen LAN-Karten und viel Speicher, da sie in der Lage sein sollen, kurzfristig alle Pakete auf einem LAN aufzeichnen zu können.

### **21.3 Langzeitmessung**

Bei LAN's kann es sinnvoll sein, über lange Zeit Daten zu erfassen. Dabei können sowohl Durchschnittswerte als auch Spitzenwerte interessant sein. Dazu läuft meist ein PC lange Zeit mit und nimmt diese Messwerte auf. Dabei kann er jedoch nicht den kompletten Datenverkehr aufnehmen sondern protokolliert meist nur Verbindungsdaten mit. Somit lassen sich die stärksten Sender und Empfänger ermitteln. Eventuell können so Meßwerte zur Umgestaltung eines LANs erlangt werden. Interessant sind auch Auswertungen über bestimmte Ereignisse (Broadcasts, Login, Fehler)

### **21.4 Alarmgeber (MHS-Gate)**

Es gibt jedoch auch Möglichkeiten, vor dem Ausfall des LAN's die Vorboten zu erkennen und zu melden. Dies kann wieder durch Computer erfolgen, welche 24h durchlaufen oder durch Programme, welche regelmäßig (z.B. automatisch) aufgerufen werden und beim Überschreiten bestimmter Grenzwerte Alarm schlagen. Bei Netzware ist es z.B. möglich über LAN bei jeder Station, welche IPX geladen hat, statistische Daten abzufragen.

Programme dieser Art haben weniger mit dem physikalischen LAN oder Übertragungswegen zu tun, sondern kontrollieren auf einer höheren Ebene das LAN. Solche Programme können z.B. durch regelmäßiges „Anpingen“ von Großrechnern deren Präsenz anzeigen. Oder durch Aufruf entsprechender Utilities statistische Werte wie Fehlerraten, Anzahl der Connections, Lizenzkontrolle etc. machen.

Idealerweise melden diese Programme Fehler nicht direkt auf der Konsole sondern z.B. aus E-Mail an einen Benutzer. Dies erlaubt es auch, solche „Wachhunde“ in anderen LANs einzusetzen, welche nicht dauernd vor Ort betreut werden. Damit kann solch ein „DienstPC“ der ansonsten z.B. Backup macht oder Mails routet, zusätzlich das LAN überwachen und Warnungen lange vor den kritischen Werten an einen Administrator schicken. Diese muß (dank Mail) natürlich nicht vor Ort sitzen.

## **22 Installation von ...**

Die hier aufgeführten Installationslisten sind nur dann zutreffend, wenn das bisher berichtete Konzept übernommen wurde. Daher sind die Angaben nur eingeschränkt brauchbar und werden nicht ausführlich erläutert.

### **22.1 Server (Diskette mit Installationsdateien)**

Um einen Server zu installieren kann man keine genaueren Angaben machen, da die eingesetzte Hardware zu variantenreich ist. Hierbei helfen die Handbücher weiter. Wenn der Server als solches jedoch läuft, d.h. Volumes sind eingerichtet und gemountet, LAN-Treiber und Protokolle sind geladen und die NetWare-Programme aufgespielt sind, ist das erste, die zusätzlichen Verzeichnisse einzurichten und das Login-Script anzulegen.

- Einrichten von den Bereichen PROGRAMME, USERDATEN, GRUPPENDATEN
- Einrichten des Loginscripts und Anpassung an die Verhältnisse
- Kopieren des zusätzlich benötigten allgemeinen Utilities

Danach kann die Installation der Prgrammen, die Einrichtung von Benutzer, Gruppen und Druckern erfolgen.

Ich möchte daran erinnern, den Server infach als „Black Box“ zu betrachten, welcher eine große Festplatte an die Anwender weitergibt. An der Serverkonsole braucht in der Regel selbst nichts gemacht zu werden. Fast sämtliche Administration erfolgt vom Client aus.

## 22.2 Workstation

Bei der Installation von Workstations mit Remoteboot reicht es, die Hardware zusammenzubauen, die Netzwerkkarte zu konfigurieren und anzuschließen und dann den PC einzuschalten. Es ist nicht nötig, die Festplatte zu installieren oder besondere Treiber zu laden. Sollte der PC wirklich so unterschiedlich sein, daß die bestehenden Bootimages nicht verwendet werden könnten, so muß ein passendes Bootfile generiert werden.

Damit kann der PC schon booten und sich anmelden. Danach muß die Kartenummer (Nodeadresse) bei der BOOTCONF.SYS und beim DUMMY (USERCFG.BAT) eingetragen werden. Hinzu kommt die Angabe der Konfiguration (Grafikkarte, IP-Nummer, Benutzer, nächster Drucker usw).

Bei Anwendung des dokumentierten Konzepts sind folgende Schritte zur Installation einer Workstation notwendig.

### Zusammenbauen, Aufstellen und Anschließen der Hardware

Der Workstation muß mit den gewünschten Komponenten ausgestattet werden. Besonders ist hier die Aufrüstung des Speichers und der Einbau der Netzwerkkarte zu erwähnen.

Der PC wird am Zielplatz aufgestellt und angeschlossen. Eventuell müssen im BIOS-Setup des Rechners die neu eingebauten Geräte (RAM, Diskettenlaufwerke, Festplatten) eingetragen werden. Die Netzwerkkarte muß an das LAN angeschlossen werden. Beim Anschluß an eine „Twisted Pair“-Verkabelung sind an der Netzwerkkarte entsprechende LEDs, welche dann leuchten, wenn der Anschluß erfolgreich ist. Leuchten die LEDs nicht, so ist das Kabel und die Verbindung am Twisted-Pair-Hub zu überprüfen. Erst wenn der PC ohne Fehlermeldung im Setup hochfährt und das LAN korrekt angeschlossen ist, kann ein Remoteboot vom Server erfolgen.

### Einrichtung der Umgebung

Nach dem Aufbau wird er PC automatisch vom LAN booten und sich anmelden. Wird dieser PC zum ersten Mal angemeldet, so werden dem Installateur einige Fragen zur Umgebung, Benutzer, Grafikkarte, Drucker, Inventarisierung, etc. gestellt. Diese müssen korrekt beantwortet werden. Danach wird der PC erneut booten und nach dem Passwort des eingerichteten Benutzers fragen. Hier muß der zukünftige Anwender dann sein Passwort eingeben. Hat der Anwender noch nicht die Schulung durchlaufen, dann ist das Passwort leer und der Benutzer wird aufgefordert ein neues Passwort einzugeben. Diese muß mindestens 5 Zeichen lang sein. Nach der Eingabe wird ein zweites Mal die Eingabe erwartet, damit Tippfehler ausgeschlossen werden. Beide Eingaben sind nicht sichtbar. Der PC wird dann Windows starten.

### Feineinstellung

Nach dem Start von Windows ist die Monitoreinstellung den Gegebenheiten anzupassen. Das Bild soll zentriert im Bildschirm zu sehen sein und Helligkeit und Kontrast der Umgebung angepaßt sein.

Zur Überprüfung der Funktion der Druckereinstellung sollte eine Seite gedruckt werden. Hierzu bietet sich z.B.: der Ausdruck einer Hilfeseite des Programmanagers an (Text und Grafik gemischt).

### Damit ist die eigentliche Installation abgeschlossen.

Eventuell können dem Benutzer zusätzliche Hinweise gegeben werden, z.B. wie die Einstellungen am Monitor veränderbar sind.

### 22.3 Programminstallation

Bei der Installation eines neuen Anwendungsprogrammes kann die Installationsroutine benutzt werden. In der Regel ist es immer noch nötig, die Installation bei den einzelnen Benutzern von Hand oder automatisiert nachtragen zu lassen. Es ist auf jeden Fall anzuraten, vorher die Installationsanweisung zu lesen, um notwendige Optionen für die Installation zu finden. Man sollte darauf achten, daß immer alle Module und Treiber der Software installiert werden. Auch wenn sie für die aktuelle Workstation nicht nötig wären.

Wenn Änderungen der AUTOEXEC.BAT und CONFIG.SYS nötig sind, so sollten diese nur als Beispiel gespeichert werden, wenn dies möglich ist. Ansonsten sollten SOFORT nach der Installation die Startdateien verglichen werden und die Änderungen dokumentiert und herausgenommen werden (soweit möglich) Diese Änderungen sind später für den Anwenderbatchjob nötig. Für Programm ohne Installationsprogramm ist von Hand ein Programmverzeichnis zu erstellen.

Nach der Installation sollte mit SYSCON eine Programmgruppe erstellt werden, in welche die berechtigten User eingetragen werden. oder die Rechte einer bestehenden Gruppe zugeodnet werden. Meist reicht Read und FileScan für das Programmverzeichnis Bei Bedarf sollte ein Gruppenverzeichnis erstellt werden, für das auch nur die Gruppe erweiterte Rechte bekommen.

Als nächstes muß der Batchjob erstellt werden, mit welchem das Programm gestartet wird. Dies ist zweifelsfrei die umfangreichste Aufgabe. Dieser Batchjob sollte dafür sorgen, daß alle Aktionen ablaufen, die VOR dem Programmstart nötig sind, um die Programmumgebung zu schaffen. Dazu zählen: Suchpfad, Umgebungsvariablen, Kopien der PC-relevanten Treiber usw Nach dem Programmaufruf sollte der Batchjob wieder die Originalumgebung herstellen. Bei Windowsanwendungen müssen diese Aktionen vor dem Start von Windows ausgeführt werden oder mit eigenen Utilities (Markos, Winbatch ua) vor dem Start des Programmes erfolgen

In dem Batchjob muß abgefangen werden:

- Programmstart durch unberechtigte Benutzer
- Programmstart durch berechtigte User, aber nicht installierte Stationen
- Programmstart durch ungeeignete Workstations

Soweit möglich, sollte der Batchjob im Fehlerfall mit aussagekräftigen Meldungen und Hilfen (Telefonnummer und Mailadresse des Administrators) beendet werden. Natürlich kann der batch auch gleich automatisch eine passende Mail an den Administrator selbst schicken. Wenn möglich, sollte auch die Programmierung einer AUTO-INSTALLATION oder einer Standardfunktion (z.B. ohne Grafikmodus oder auf Basis des kleinsten gemeinsamen Nenners) überlegt werden. Denn wenn ein Benutzer mal damit arbeiten kann, ist der Druck weg, sofort eine Installation von Hand zu machen. Das Feineinstellen kann dann außerhalb von Stoßzeiten erfolgen. Der Batchjob sollte so perfekt sein, daß zum Betrieb notwendige Verzeichnisse automatisch erstellt werden, wenn der Benutzer ein vermeintlich unnötiges leeres Verzeichnis löscht, das Programm diese jedoch braucht.

Es empfiehlt sich, die Ratschläge im Konzept zu lesen, welche zum Thema "Programme im LAN" beitragen.



## 22.4 Drucker einrichten

Die Problematik des Drucken in LAN's wurde vorher schon gehandelt, so daß hier nur kurze Erläuterungen folgen:

### Printset (Windows)

Beim Einsatz von Printset wird jedem Drucker ein Aliasname (8 Buchstaben) zugeordnet. Jedem PC wird genau ein Drucker als Arbeitsdrucker zugewiesen. Die Einstellungen unter Windows werden von PRINTSET beim Start von Windows ausgeführt (Druckertreiber, Schnittstelle, Queue). Damit die funktioniert, muß:

1. Für jeden PC sichergestellt sein, daß die Umgebungsvariable %PRINTER% gesetzt ist (PCCFG.BAT beim User Dummy)
2. In der PRINTSET.INI für den ALIASNAMEN die Druckerkonfiguration angegeben werden
3. Die entsprechende Queue und der Druckertreiber vorhanden sind.

### PCONSOLE - Queue und Druckserver (zwingend)

Mit PCONSOLE erstellt der Supervisor dann die benötigten Printserver und Queues. Beim Printserver gibt man u.a. auch den Anschluß des Drucker an. Zur Queue muß man einen Queueserver angeben. Wahlweise kann man die berechtigten Benutzer einschränken und zusätzliche Operatoren oder Operatorgruppen angeben.

Beim Anschluß des Druckers direkt ans LAN muß in der Regel ein Programm des Herstellers benutzt werden, um die Einbaukarte zu konfigurieren. (HP benutzt z.B. ein Programm mit dem Namen PCONFIG)

### Anwendung

Bei jeder Anwendung muß der dem Arbeitsplatz zugewiesenen Drucker bekanntgegeben werden. Dies ist bei DOS-Anwendungen je Anwendung unterschiedlich. Unter Windows muß der Druckertreiber einmalig Windows bekannt gemacht werden. Dann können alle Windowsprogramme diesen Drucker nutzen.

### PRINTDEF - Netware-Druckerdefinition (optional)

Soweit erforderlich und sinnvoll, kann man mit PRINTDEF das Device definieren. Bei Windows ist es jedoch am einfachsten, die Daten 1:1 vom PC zum Ducker zu schicken und NetWare die Steuerung durch Tabulatoren, Banner, Zeilenlänge und Seitenvorschübe zu verbieten. Einzig zur Umschaltung der Druckeremulation per Software eignen sich diese Sequenzen, welche im voraus an den Drucker geschickt werden.

Die Datenbank wird beim Verlassen von PRINTDEF abgespeichert und ist für ALLE Benutzer gültig. Daher kann mit PRINTDEF auch nur der Supervisor was ändern. Die \*.PDF-Dateien von Novell sind danach NICHT mehr nötig und können auf eine Diskette kopiert und gelöscht werden. Dadurch wird das Verzeichnis PUBLIC kleiner was sich in kürzeren Suchzeiten und weniger Last widerspiegelt.

### PRINTCON - Druckjobs (optional)

Mit PRINTCON können dann PRINTJOBS erstellt werden, welche für den Drucker maßgeblich sind. Beim Job kann dann das Device und der Devicemodus angegeben werden. Existieren mehrere Drucker des gleichen Typs mit eigenene Queues, so sollte man eine DUMMY-Queue erstellen und dorthin die Standardausgaben lenken. Dadurch muß man beim CAPTURE nicht nur den JOB, sondern auch die QUEUE angeben. Dieser Job ist nur für den eigenen Usernamen gültig. Da normalerweise die Benutzer sich nie mit dem Thema Druckjobs beschäftigen werden, ist es zweckmäßig, diese Jobs an die anderen Benutzer zu kopieren. Dies geht zwar mit PRINTCON, ist jedoch mühsam. Die Printjobs sind in der Datei PRINTCON.DAT im jeweiligen MAIL-Dir des Users. Der Supervisor hat die MAILL-ID "1". Man kopiert daraus die PRINTCON.DAT zu den anderen Usern in deren Mailverzeichnis

Den Aufwand mit PRINTDEF und PRINTCON kann man sich sparen, wenn man auf die Druckersteuerung von NetWare verzichtet und statt dessen die Druckservices darauf reduziert, die Daten Byte für Byte durchzuschleusen. Dazu muß man dann bei CAPTURE und anderen Druckbefehlen mehrere Parameter angeben, z.B. CAPTURE queue=... local= .. NT NB NFF. Diese Variante empfiehlt sichsogar, da mittlerweile die Textverarbeitungsprogramme die Druckersteuerungen komplett selbst übernehmen und nicht mehr den Text zeilenweise zum Drucker

schicken und ein Queuemanagement für den Seitenvorschub und die Ränder sorgen muß. Druckjobs sind im Zusammenhang mit Hostsystemen noch anwendbar, wenn der Host selbst keine Druckersteuerung nutzt.

## 22.5 User anlegen

Um neue Benutzer anzulegen, muß man Supervisor oder Equivalent sein. Dann bietet NetWare mehrere Utilities an, um Benutzer anzulegen (SYSCON, USDEF, MAKEUSER, NETCON) Welches Utilities man nimmt ist dem persönlichen Geschmack überlassen und richtet sich nach den Anforderungen. Wenn man als Supervisor eines Universitätsnetzwerkes zum Semesterbeginn viele gleiche Benutzer anlegen muß bietet sich Makeuser oder Userdef an. Bei dem hier vorgestellten Konzept ist es jedoch derart einfach, User anzulegen, daß auch SYSCON bzw. NETCON benutzt werden kann. Dabei führt man folgende Schritte durch:

1. **User eintragen (INS-Taste bei der Userliste)**  
Dabei kann man auch das Userverzeichnis erstellen lassen. Aus diesem Grund sollte der Usernamen nicht länger als acht Buchstaben lang sein und keine Umlaute enthalten (MS-DOS-Konventionen)
2. **Angabe des Heimatverzeichnisses**  
Jeder Benutzer sollte ein Heimatverzeichnis haben, damit dort Konfigurationsdaten für diesen Benutzer abgelegt werden können. Auf dieses Verzeichnis hat der Benutzer in der Regel alle Rechte.
3. **Angeben des Full Name**  
Der FULL NAME wird von diversen Programmen ausgewertet (z.B.MAIL) und kann zur Erklärung besonderer Accounts dienen.
4. **Gruppen eintragen**  
Falls der Benutzer weiterer Rechte (außer EVERYONE) haben soll
5. Sofern **PRINTJOBS** benutzt werden, sollten diese mit PRINTCON kopiert werden. Besonders wenn ein "default"-Job benutzt wird und damit die volle Deklaration bei CAPTURE und NPRINT überflüssig wird.
6. **USER.BAT anlegen**  
wenn nicht die default USER.BAT im Batchverzeichnis benutzt werden soll. Dies trifft meist nur auf Gateway zu, da die "normalen" Benutzer alle die gleiche Oberfläche (Menüsystem oder Windows) benutzen werden
7. **User in E-MAIL eintragen**  
Viele Programme haben ein automatisches SETUP, um neue Benutzer einzutragen und die Postfächer anzulegen. Ansonsten muß man den Benutzer mit dem entsprechenden Hilfsprogrammen anlegen. Zuletzt muß man Verteilerlisten aktualisieren (lassen) und eventuell das Adressbuch an externe Postoffices versenden.

Allein die Vergabe der Rechte auf Programme sollte reichen, wenn man die Batchjobs so geschrieben hat, daß auch die Erstinstallation automatisch erfolgt. Somit erspart man sich nun von Hand nötige Unterverzeichnisse und Dateien anzulegen.

## 22.6 User löschen

1. SYSCON Benutzer durch DEL-Taste löschen  
Damit wird der Account dieses Benutzers gelöscht. ACHTUNG: Wenn dieser Benutzer noch angemeldet ist, erfolgt ein Zwangslogout.
2. Das Homeverzeichnis des Benutzers löschen  
Das Löschen des Users aus der Bindery (Punkt 1) löscht KEINE Daten des Benutzers noch entfernt es die Rechte dieses Users, welche im Verzeichnisbaum abgelegt sind. Die Rechte in den Verzeichnissen werden beim Löschen des Verzeichnisses mit gelöscht oder mit dem Programm BINDFIX.
3. Das Postfach zur E-Mail löschen und das Adressbuch mit anderen Postoffices abgleichen  
Soweit die Postfächer der E-Mail nicht durch ein Setupprogramm automatisch gelöscht werden, muß dies von Hand nachgeführt werden. Wenn die E-Mailsoftware einen Addressabgleich erlaubt, sollte sichergestellt werden, daß ein aktuelles Adressbuch an die anderen Postoffices geschickt wird, sofern dies nicht automatisch erfolgt.

Vorher sollten die Daten des Benutzers gesichert werden, falls diese von anderen Personen weiter benutzt werden sollen. Wenn man nicht sofort die Zeit hat, Benutzer zu löschen, so sollte man nach deren Ausscheiden zumindest den Account sperren (Syscon, Userinformation, <user>, Account restrictions)

**23 Checkliste bei Übergabe**

- Setup der Programm mit Lizenzierung auf den Betreiber
- nicht lizenzierte Software löschen
- Eigene Benutzeraccounts löschen
- Falls notwendig den zukünftigen Administrator auf die Verantwortung hinweisen.
- Supervisor-Password Übergabe (mit Bestätigung)
- eigene Hardware entfernen
- Dokumentation aushändigen
- NetWare Lizenzierung kontrollieren (Ist es die richtige SERVER.EXE)
- ....
- ....

## **24 Nachwort**

Ich kann es nicht glauben, aber hier schein tatsächlich jemand dieses Konzept bis zu Ende gelesen zu haben., Ich hoffe es hat etwas geholfen die Ideen zu verstehen, welche ich mit dem installierten Fileserver realisiert habe. Natürlich gibt es immer wieder Momente, wo man von dieser Richtung abweichen muß. Teils sind es Anforderungen durch den Betreiber oder Probleme der Software. Auch kann solche eine Dokumentation nicht einen kompletten Kurs oder eine fundierte Ausbildung ersetzen. Es geht nun mal nicht, sämtliches Wissen meiner Tätigkeit im Bereich der LAN's und speziell mit Novell NetWare seit 1989 auf Papier zu bannen. In einem Gespräch oder eine Schulung kann viel mehr auf individuelle Fragen eingegangen werden, als in einem Handbuch, welches wirklich nur eine Basis ist. Auf diese kann und sollte aufgebaut werden. Auch kann nicht jeder „Pieps“ eines Netzwerkes damit dokumentiert werden.

Leider habe ich nicht immer die Zeit, alle Verbesserungsvorschläge einzubauen oder zu diskutieren. Trotzdem kann man sie an mich schicken:

### **Post**

Frank Carius  
EDV-Beratung  
Zeiskamer Straße 28  
D-76756 Bellheim

### **E-MAIL (bevorzugt)**

CompuServe: 100031,3216  
Internet: FCARIUS@FC.MHS.COMPUERVE.COM  
MHS FCARIUS@FC +49 7272 92013-5  
X400 c=us;a=COMPUSERVE;p=CSMAIL;d=ID:"MHS:FCARIUS(a)FC"

Die Rechte an diesem Schriftstück verbleiben auf jeden Fall beim Autor. Eine Übersetzung in andere Sprachen, eine Vervielfältigung oder eine Weiterverarbeitung ist ohne vorherige Rücksprache nicht erlaubt.

**25 Anlage 1: Software**

Die folgenden Seiten beschreiben die Einbindung der jeweiligen Software in das Konzept und die Einstellungen. Diese Seiten werden ständig aktualisiert und enthalten in der Regel auch Software, welche nicht unbedingt installiert sein muß.



## 25.1 BS2000-Emulation



Die BS-2000-Emulation von HSD benutzt den TCPI/IP-Protokollstack von LanWorkPlace. Neben der eindeutigen IP-Nummernvergabe, welche durch LanWorkGroup oder Batchfiles geregelt wird, ist bei BS2000 eine eindeutige Zuordnung der Sessions notwendig. Dies geschieht durch eine SESSIONS.INI. Diese ist aufgrund der Konfiguration im BS2000 auf eine IP-Nummer und damit auf einen PC fest verankert und damit Benutzerunabhängig. Da nun aber jeder Benutzer an jedem PC arbeiten könnte, ist es notwendig, beim Start von Windows die passende SESSIONS.INI in das Benutzerverzeichnis zu kopieren.

Dazu gibt es unter G:\HSD9750.WIN\ ein Verzeichnis SESSIONS. Dort wurden die SESSIONS.INI jeder Station mit dem Namen SESSION.<ipnummer> abgelegt. Da auf dieses Verzeichnis kein Benutzer Schreibrechte besitzt ist auch eine dauerhafte Veränderung dieser Konfigurationsdaten nicht möglich.

Die Datei HSD9750W.INI wird ebenfalls beim Start zum Benutzer kopiert. Dies ist später LEVEL-abhängig. Damit ist es möglich, daß jeder Benutzer seine Farben selbst einstellt. Beim LEVEL=0 ist eine Änderung der Farben zwar möglich, jedoch noch dauerhaft. Beim nächsten Start von Windows sind die Voreinstellungen wieder aktiviert worden.

Änderungen an der Sessions.ini kann damit zwar der Benutzer auch machen (HSDKONF.EXE), jedoch sind diese nicht dauerhaft, es sei denn diese geänderte SESSIONS.INI wird unter dem passenden Namen in die G:\HSD9750.WIN\SESSIONS abgelegt.

## 25.2



## WinWord 6.0



WinWord kann mit SETUP /A komplett in ein Verzeichnis ausgepackt werden. Mit SETUP /N führt man dann das „Workstationsetup“ aus. Das Setupprogramm aktualisiert die Programmgruppen und INI-Dateien. Diese Änderungen führt man bei allen anderen Benutzern nach.

Wenn Benutzer eigene Vorlagen benutzen wollen, sollten diese in ihrem H:-Verzeichnis (z.B. H:\VORLAGEN) liegen, worinsich dann auch die sonstigen WinWord-Vorlagen befinden. WinWord kann z.Z. nicht mehrere DOT-Pfade verwalten. Dort befindet sich dann auch die NORMAL.DOT mit welcher der ADMIN die Umgebung vonWinWord speziell konfigurieren kann (z.B. Mail einbinden)

Word legt auch eine Datei WINWORD6.INI an. In dieser stehen die zuletzt geöffneten Dateien und die Benutzerinformation. Diese Datei legt WinWord beim ersten Start alleine an. Diese INI-Datei ist jedoch nicht "lesbar" sondern binär codiert und kann daher im Gegensatz zu anderen INI-Dateien nicht mit einem ASCII-Editor bearbeitet werden.

### Autostart

Neu bei Winword 6 ist das START-Verzeichnis. Hier lassen sich automatisch zu ladende Makros und Erweiterungen für ALLE Benutzer einbringen.

### Vorlagen

Von Winword gibt es eine STEUERDA.DOT. Diese stellt einige erweiterte Hilfsmittel zum Serienbrief unter Winword zur Verfügung. Wer also Serienbriefe nutzt und diese Vorlage wünscht, muß diese in sein eigenes H:\VORLAGEN kopieren wie mit jeder Vorlage. Erst dann findet sie WinWord. Nur so kann man diese Vorlage auch nach eigenen Wünschen danach abändern. Die Serienbrieffunktion funktioniert auch OHNE diese DOT korrekt, jedoch fehlen dem Benutzer dann einige eventuell hilfreiche Makros und Funktionsleistenbelegungen.

## 25.3

## Excel 5.0



Die Installation von Excel ist mit der von Windows zu vergleichen. Mit „SETUP /A“ führt man das Setup im Administratormodus aus. Damit können wieder alle Programme und Dateien auf ein Netzwerkverzeichnis entpackt werden. Ist die erfolgt, dann kann durch den Aufruf des Setupprogrammes aus diesem Verzeichnis eine „Arbeitsstationsinstallation“ erstellt werden. Dabei aktualisiert das Setupprogramm die Programmgruppen, die Inidateien und die Registrierdatei. Eventuell werden auch einige Programme in das Systemverzeichnis kopiert. Bei diesem Konzept braucht der Benutzer das Setzupprogramm nicht selbst auszuführen. Das Setup wird einmal vom Administrator ausgeführt. Danach wird kontrolliert, welche Änderungen das Setupprogramm gemacht hat und diese werden dann beim Start von Windows in den Batchjob eingepflegt.

Die Dateien im Excel-Programmverzeichnis müssen alle mit FLAG \*.\* ROS /SUB als „shareable“ gekennzeichnet werden.

### Eigene Makros

Excel führt beim Start alle Dateien in XLSTART aus. Da nun Benutzer eigene Makros und Autostartdateien haben, muß man in XLSTART ein Makro ablegen (ALTSTART.XLA) welches ein alternatives Startverzeichnis erlaubt. Dies ist auch der Platz, wo später z.B. Makros für das Einfügen der MAIL ins Menü untergebracht werden.

## 25.4

## PowerPoint 4



Powerpoint legt im gleichen Verzeichnis, in welchem auch die WIN.INI steht, eigene INI-Dateien ab (POWERPNT.INI und PPTVIEW.INI) Diese sind nach der Installation entsprechend anzupassen, damit die Benutzer in den richtigen Verzeichnissen schreiben und die Cliparts von Powerpoint gefunden werden können.

Powerpoint liefert wie jedes Officepaket eine umfangreiche Sammlung von Hilfsprogrammen mit (z.B. Artgalerie, Organigramm). Diese werden wie alle „Add-Ons“ von Microsoft in G:\MSAPPS installiert. Diese AddOns werden in der REG.DAT eingetragen, und sind damit jedem Programm zugänglich.

Mit dem SETUP /A von Powerpoint werden wieder alle Daten von den Disketten auf die Festplatte/Netzwerkplatte kopiert. Nach dem Anschluß dieser Installation steht es wieder jedem Benutzer frei, ein SETUP auszuführen, damit diese Programm die eigenen INI-Dateien erstellt und die REG-DAT modifiziert. In unserem Konzept muß dies der Administrator genau einmal für sich ausführen und die geänderten INI-Dateien für alle bereitstellen. Alle User mit LEVEL 0 bekommen diese beim nächsten Windowsstart kopiert. Das Icon muß noch in eine Netzwerkgruppe aufgenommen werden. Dies kann alternativ auch durch GRPPATCH erfolgen.

Eine Besonderheit ist das Programm ARTGALERIE. Beim ersten Aufruf erstellt es eine eigenen Datenbank, in welcher die Cliparts als Übersicht vorhanden sind. Diese Datenbank ist ca 2,5 MB groß und damit zu groß, um diese jedem Benutzer zuzulassen. Wenn es nicht notwendig ist, daß jeder Benutzer selbst entscheidet, welche Cliparts er haben möchte oder gar selbst Cliparts zukaufen soll, dann bietet es sich an, diese Datenbank global unter G:\MSAPPS\ARTGALRY bereitzustellen. Dazu muß ein Benutzer diese Datenbank durch den Aufruf von der Artgalerie unter Powerpoint einmalig starten. Der Administrator kann dann die Datenbank kopieren und muß den Eintrag in der ARTGALRY.INI entsprechend anpassen.

Ungeachtet davon trägt Powerpoint sich in der WIN.INI ein. Auch in der REG.DAT werden Einträge vorgenommen.

**26 Anlage 2: Formblätter**

Die folgenden Formulare sind im Laufe der eigenen Arbeit entstanden. Natürlich dürfte jeder Administrator selbst seine Vorstellungen der notwendigen Informationen haben und somit eigene Formblätter entwerfen. Auch die von Novell mitgelieferten Formblätter sind zur Aufzeichnung der Daten geeignet. In gewissem Maße sind einige Informationen in Inventardatenbanken enthalten.

26.1 Server-Konfiguration

<b>Servername:</b>	<b>Standort:</b>

<b>Installiert am:</b>	<b>von:</b>
NetWare __.____ / ____ User	IPX internal:

<b>Prozessor/Takt</b>	
<b>Bus</b>	
<b>Speicher</b>	

Disketten	Format	Kapazität
<b>A:</b>		
<b>B:</b>		

Festplatte	Interface	Größe	Partitions	Mirroring/Duplexing
HD0				
HD1				
HD2				
HD3				

Volumes:

Name	Größe	Blockgröße	Segmente

Steckkarten

Slot	Name	IRQ	I/O von - bis	DMA	RAM	ROM	Bemerkung

--	--	--	--	--	--	--	--

**Zugang:**

<b>Supervisor:</b>		<b>Admin:</b>	
--------------------	--	---------------	--

**Bemerkungen:**

--

**26.2 Drucker-Konfiguration**

<b>Standort:</b>	<b>Raum</b>	<b>Ansprechpartner</b>	<b>Telefon</b>

<b>Typ:</b>	<b>Name:</b>
-------------	--------------

<b>Installiert am:</b>	<b>von:</b>
------------------------	-------------

**Emulation**

PostScript	
HP-PCL ____	
HP-GL ____	
andere: _____	

**Umschaltung**

automatisch	
jobgesteuert	
manuell	
keine	

**Anschluß:**

<b>Schnittstelle:</b>	<b>Parallel</b>	<b>Seriell</b>	<b>Sonst (BNC, AUI, TR)</b>
<b>Anschluß an:</b>			
<b>Daten:</b>			

**Netzwerkqueues**

Servername	Queuename	Betriebsart
		Druckserver / Remoteprinter
		Druckserver / Remoteprinter
		Druckserver / Remoteprinter
		Druckserver / Remoteprinter

**Bemerkungen:**

--

26.3 PC-Konfiguration

<b>Standort:</b>	<b>Raum</b>	<b>Benutzer</b>	<b>Telefon</b>

<b>Typ:</b>	
-------------	--

<b>Installiert am:</b>	<b>von:</b>
------------------------	-------------

<b>Prozessor/Takt</b>	
<b>Bus</b>	
<b>Speicher</b>	

<b>Disketten</b>	<b>Format</b>	<b>Kapazität</b>
<b>A:</b>		
<b>B:</b>		

<b>Festplatte</b>	<b>Interface</b>	<b>Typ</b>	<b>Cylinder</b>	<b>Head</b>	<b>Precomp</b>	<b>Landin</b>	<b>Sektoren</b>	<b>Größe</b>
<b>C:</b>								
<b>D:</b>								

Steckkarten

<b>Slot</b>	<b>Name</b>	<b>IRQ</b>	<b>I/O von - bis</b>	<b>DMA</b>	<b>RAM</b>	<b>ROM</b>	<b>Bemerkung</b>

Bemerkungen:

--

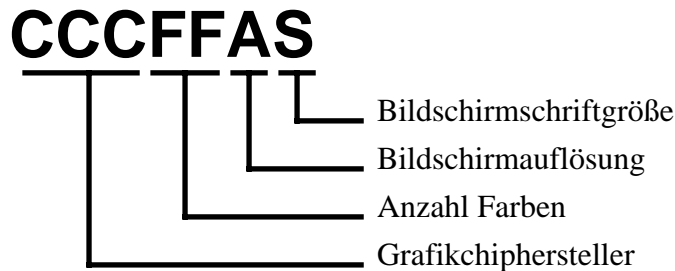


26.4 Bootfilekonfiguration:

		D62XXXX.SYS
<b>COMMAND.COM</b>	Version	6.2
	Sprache	deutsch
<b>CONFIG.SYS</b>	device = HIMEM.SYS	x
	device= EMM386.EXE	x
	shell=COMMAND.COM /e:	1024
	files=	30
	buffers=	20
	dos=	HIGH,UMB
	break=	off
	fcbs X,X	
	stacks X,X	
	lastdrive =	M
	country=	49
switches=	/w	
<BOOTFILE>.BAT	set BOOTFILE=	D62XXXX
	LH lsl.com	2.05
	rplodi	1.1
	LH ne2000	
	LH ipxodi Version	
	lh netx Version	3.32f
	lh keyb gr.,,keyboard.sys	
	login dummy	
<b>NET.CFG</b>	machine type	
	long machine type =	
	show dots =	
	print tail =	
	print header =	
	file handles =	
	Link Support	
	Buffers	8 1534
	MemPool	4096
	max stacks	8
	<b>Link Driver</b>	<b>NE2000</b>
	INT	5
	PORT	320
	MEM	CC000
	Frame	Ethernet_II
	Protocol	IPX 8137 Ethernet_II
	Protocol	TCPIP 800Ethernet_II
bind	bind NE2000	

### 26.5 Bedeutung der Umgebungsvariable VIDEO

Die Umgebungsvariable enthält kodiert die vier wichtigen Angaben zu jederr Videokarte. Dazu werten sieben Zeichen benutzt für die es gleichlautende Verzeichnisse bei den Programmen gibt.



#### Mögliche Werte CCC (Chiphersteller)

HGC	Hercules
EGA	Standard-EGA oder kompatibel
VGA	Standard-VGA oder kompatibel
IBM	IBM 8514A
S3_	S3 Chip
ET4	ET4000
M8_	Mach 8 (ATI)
WD2	ErgoVGA II (SNI)
CL3	CirrusLogics ErgoVGAIll (SNI)
CLL	CirrusLogics Laptop (SNI)

#### Mögliche Werte FF (Farben)

BW	Schwarzweiß
16	16 Farben
FF	64 Farben
HC	HighColor (322000)
TC	TrueColor 16,7 Mio

#### Mögliche Werte S (Schrift)

S	Small
M	Medium
L	Large
X	entfällt

#### Mögliche Werte A (Auflösung)

Wert	Handelname	X	Y
0	Hercules	768	348
1	EGA	640	350
2	VGA	640	480
3	SVGA	800	600
4	1024x768	1024	768
5	1280x1024	1280	1024

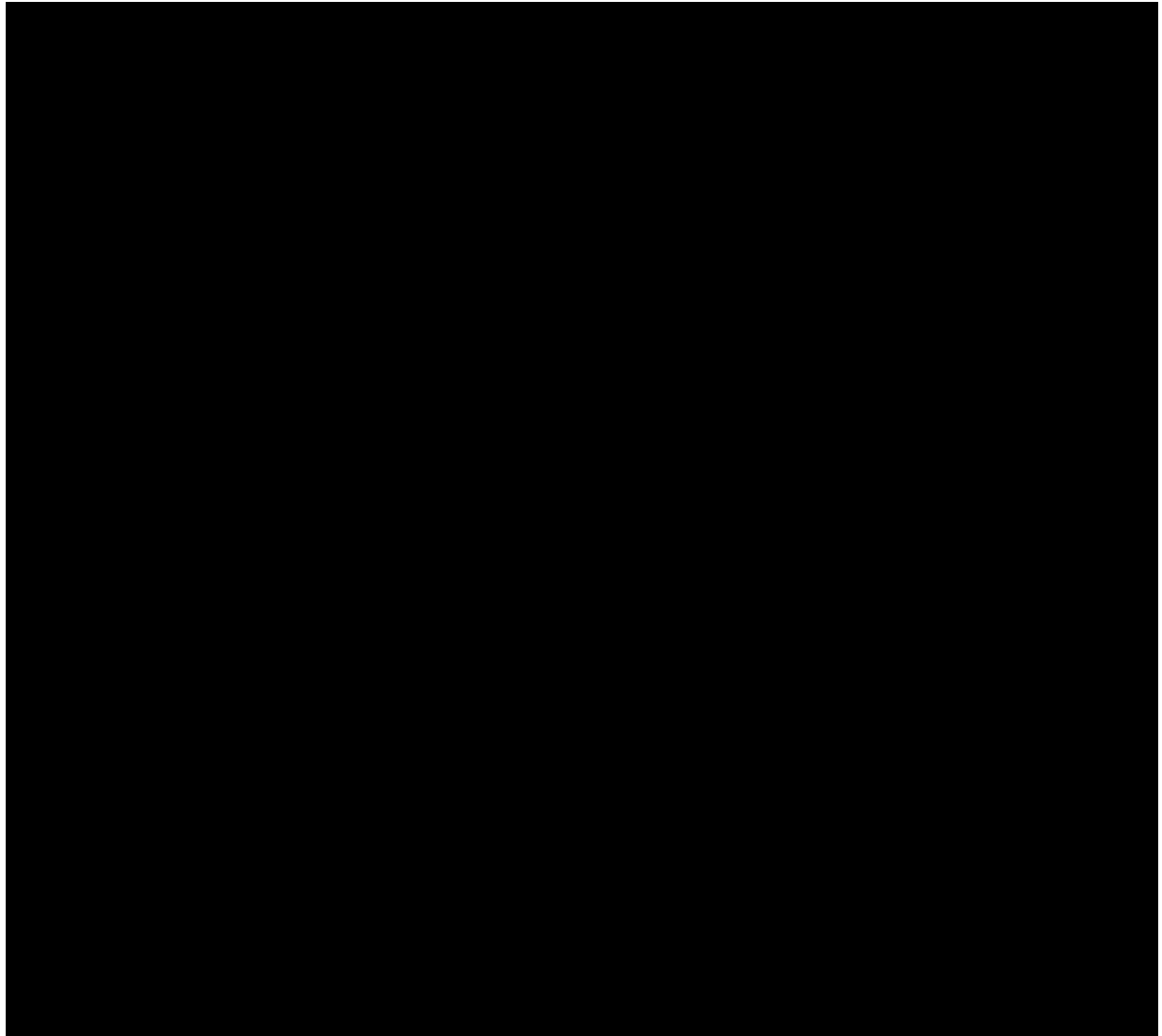
#### Beispiele:

VGA162x	StandardVGA mit 640x480 Punkten bei 16 Farben und Standardschrift
S3_FF4s	S3-Chip mit 256 Farben bei 1024x768 Auflösung und kleinen Schriften (large Desktop)
HGCBW0x	Standard Hercules Grafikarte

## 26.6 PASSWÖRTER für Fileserver

---

Dieser Umschlag enthält das Supervisorpassword und andere Passwörter für den aufgeführten Server. Dieser Umschlag ist geschlossen und sicher aufzubewahren und darf nur im Notfall geöffnet werden. Die Verantwortung über den Fileserver und alle daraus entstehenden Folgen muß derjenige tragen, der Kenntnis von diesem Password erhält.



System	Account	Password
NetWare	Supervisor	
RCONSOLE		
Mailsetup		

## 26.7 Bestätigung der Passwordübergabe

Hiermit wird bestätigt, daß das Supervisorpassword in einem verschlossenen Umschlag übergeben wurde.

Bemerkung: Die Person, welche Kenntnis von diesem Password erhält ist verpflichtet, bei der Arbeit als Supervisor erhaltene Informationen absolut vertraulich zu behandeln. Zudem muß sich diese Person immer über die Möglichkeiten und die Verantwortung, welche mit diesem Password verbunden sind, bewußt sein. Dieses Password ist nur im Notfall zu gebrauchen und sollte nur einer Person bekannt sein. Für Schäden, welche durch Personen verursacht werden, die dieses Password benutzen, ist die jeweilige Person selbst verantwortlich. Dieses Password sollte nicht telefonisch, als Email oder Telefax sondern nur im direkten persönlichen Kontakt weitergegeben werden.

**Fileserver:** \_\_\_\_\_

**Benutzername:** \_\_\_\_\_

Übergebender:

Übernehmender:

Unterschrift

Unterschrift

Die Unterzeichner bestätigen, daß der Umschlag mit dem Password persönlich übergeben wurde. Das Original dieser Bestätigung verbleibt beim Übergebenden.



**27 Anlage 3: Konfigurationsdateien**

- STARTUP.NCF des Bootdevice
- AUTOEXEC.NCF (aus SYS:SYSTEM)
- NET\$LOG.DAT (das Loginscript aus SYS:PUBLIC)
- USERCFG.BAT
- USERSET.BAT
- PCSET.BAT (User Dummy)
- PCCFG.BAT, welche die Konfiguration auswertet
- NETDIR.TAB von MHS
- Das Ergebnis von TREE auf jedem Volume
- Das Ergebnis von CHKVOL je Volume