

**Kurs**

# **Netzwerke Einführung Windows NT 4.0**

**© 1997 by Mag. Dr. Klaus Coufal**

# Inhaltsverzeichnis

1. Grundlagen .....	4
1.1. Überblick .....	4
1.2. Positionierung von NT im Firmennetz .....	4
1.3. Versionen (3.x-95-NTWS-NTServer) .....	5
1.4. Hardware Grundlagen .....	5
1.5. Betriebssystemarchitektur - Subsysteme.....	6
1.5.1. Executive .....	6
1.5.2. Hardware-Abstraction-Layer (HAL) .....	6
1.5.3. Kernel.....	6
1.5.4. I/O-Manager .....	6
1.5.5. Graphiksystem.....	7
1.5.6. Objectmanager .....	7
1.5.7. Securitymanager .....	7
1.5.8. Prozeßmanager.....	7
1.5.9. LPC-Manager .....	7
1.5.10. Speichermanager .....	8
1.5.11. Sicherheitssystem .....	8
1.5.12. Win32-Subsystem.....	8
1.5.13. POSIX-Subsystem .....	8
1.5.14. OS/2-Subsystem.....	8
1.6. Domänenkonzept.....	9
1.6.1. Einordnung .....	9
1.6.2. Definitionen .....	10
1.6.3. Domänenmodelle .....	11
2. Aufbau WS-Server-Verbindung.....	12
2.1. Hardwareverbindung.....	12
2.2. Softwareverbindung.....	12
2.3. Redirectorvarianten .....	12
2.4. Anmelden .....	13
3. Dateikonzepte .....	15
3.1. Allgemeines.....	15
3.2. FAT-Dateisystem .....	15
3.3. HPFS-Dateisystem .....	16
3.4. NTFS-Dateisystem.....	16
4. Drucken im Netz .....	19
4.1. Überblick .....	19

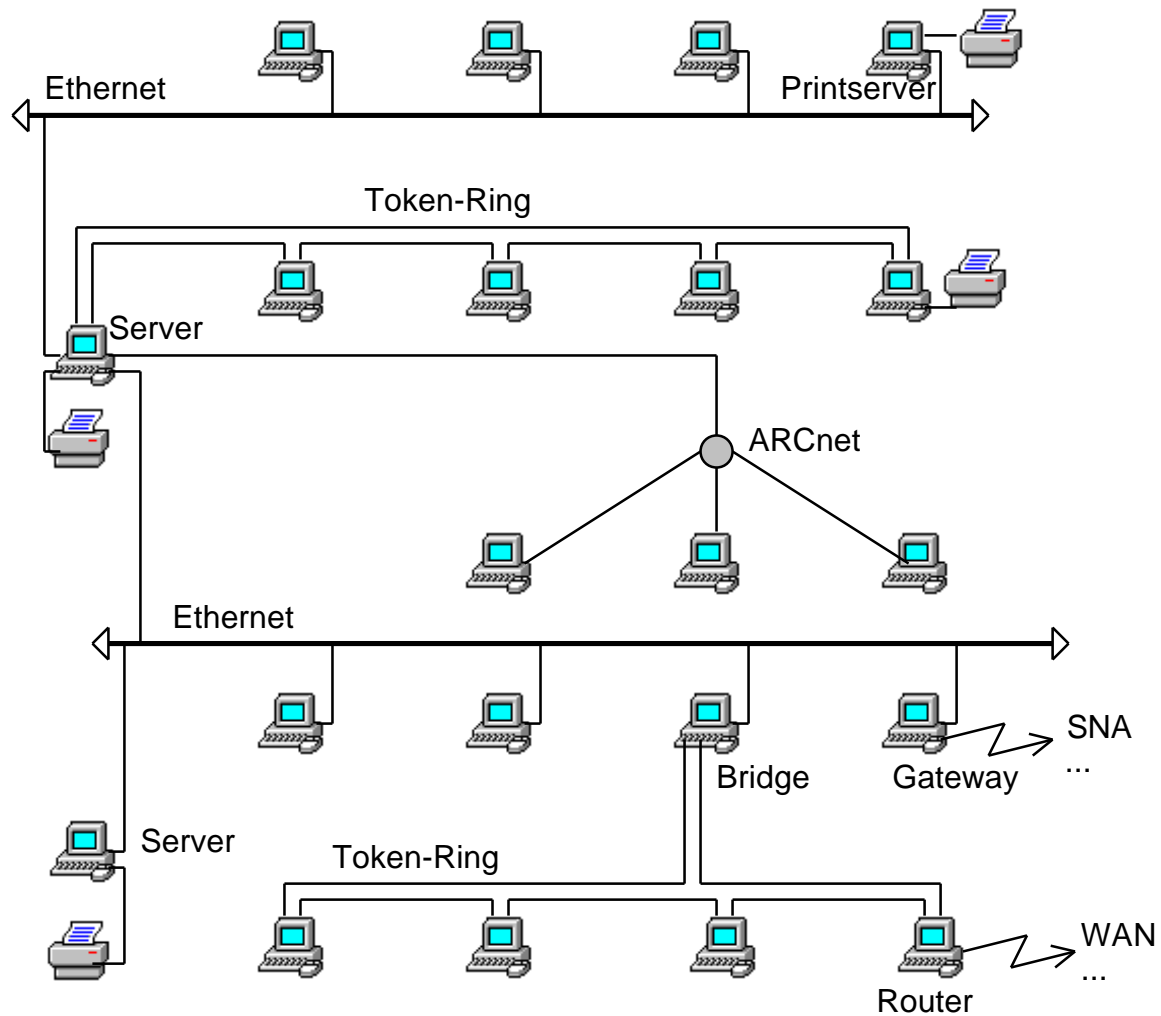
4.2. Druckerarten .....	19
4.3. Druckerinstallation .....	19
4.4. Druckerkonfiguration .....	20
4.5. Hilfsprogramme .....	21
4.5.1. Assistent für die Druckerinstallation .....	21
4.5.2. Druckerkonfiguration.....	21
4.5.3. Servereigenschaften.....	27
4.5.4. Druckmanager .....	27
5. Betreuung von Arbeitsgruppen .....	28
5.1. Benutzereinrichten .....	28
5.2. Gruppeneinrichten .....	28
5.3. Richtlinien.....	28
5.4. Hilfsprogramme .....	29
5.4.1. Benutzermanager .....	29
5.4.2. Verwaltungsassistent .....	35
6. Wartungstätigkeiten .....	36
6.1. Konfigurationsdateien .....	36
6.1.1. PROTOCOL.INI.....	36
6.1.2. Registrierungsdatenbank .....	36
6.2. Benutzerprofile .....	39
6.3. Scripts .....	40
6.3.1. Zuordnung eines Scripts .....	40
6.3.2. Spezielle Scriptvariablen .....	40
6.3.3. Beispielscript .....	41
7. Netzwerksicherheit.....	42
7.1. Überblick .....	42
7.2. Zutrittsschutz .....	42
7.2.1. Accountrestriktionen .....	42
7.2.2. „Hacker“-Erkennung (Intruder detection) .....	43
7.2.3. Accounting (Kontoführung) .....	43
7.3. Zugriffsschutz - Rechte .....	43
7.3.1. Mögliche Rechte auf Freigabeebene.....	43
7.3.2. Mögliche Rechte auf NTFS-Ebene.....	44
7.4. Hilfsprogramme .....	45
7.4.1. Servermanager.....	45
7.4.2. Windows NT-Explorer.....	46
7.4.3. Dateimanager .....	49
8. Sonstige wichtige Hilfsprogramme .....	50

8.1. Programme des Ordners Verwaltung .....	50
8.1.1. Bandsicherung .....	50
8.1.2. Benutzermanager .....	50
8.1.3. Ereignisanzeige .....	50
8.1.4. Festplattenmanager .....	50
8.1.5. Lizenzmanager .....	51
8.1.6. Migrationsprogramm für Netware .....	51
8.1.7. Netzwerk-Client-Manager .....	51
8.1.8. RAS-Verwaltung .....	51
8.1.9. Server Manager .....	52
8.1.10. Systemmonitor .....	52
8.1.11. Systemrichtlinieneditor .....	52
8.1.12. Verwaltungs-Assistenten .....	52
8.1.13. Windows NT-Diagnose .....	52
8.2. Sonstige Programme .....	53
8.2.1. REGEDT32 .....	53
8.2.2. RDISK .....	53
8.2.3. CONVERT .....	53
8.3. Zusatzprogramme .....	53
8.3.1. SQL-Server (Microsoft) .....	53
8.3.2. Exchange (Microsoft) .....	54
8.3.3. Systems Management Server SMS (Microsoft) .....	54
8.3.4. SNA-Server (Microsoft) .....	54
8.3.5. Notes/Domino (Lotus/IBM) .....	54
8.3.6. Oracle Workgroup Server (Oracle) .....	54
8.3.7. Informix .....	54
8.3.8. ARCserve (Cheyenne) .....	55
8.3.9. Diskkeeper .....	55
9. Connectivity .....	56
9.1. Netware-Connectivity .....	56
9.2. Unix-Connectivity .....	56
9.3. OS/2-Connectivity .....	57
9.4. Apple-Connectivity .....	57
9.5. NT und Verzeichnisdienste .....	57

# 1. Grundlagen

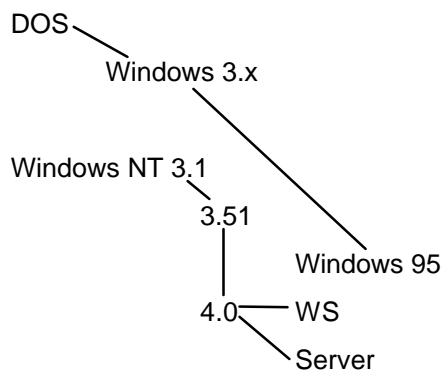
## 1.1. Überblick

## 1.2. Positionierung von NT im Firmennetz



- Fileserver
- Printserver
- Mailserver
- Timeserver
- Databaseserver
- Communicationsserver
- ...

### 1.3. Versionen (3.x-95-NTWS-NTServer)



### 1.4. Hardware Grundlagen

Windows NT war von Anfang an nicht auf eine Hardwareplattform spezifiziert, sondern sollte auf den verschiedensten Prozessoren laufen. Realisiert wird dies durch eine Zwischenschicht, die die Eigenschaften der Hardware virtualisiert, sodaß die höheren Schichten des Betriebssystems die Unterschiede der einzelnen Plattformen nicht mehr kennen müssen. Diese Zwischenschicht wird Hardware Abstraction Layer oder kurz **HAL** genannt.

Derzeit werden folgende Hardwareplattformen unterstützt

- Intel x86-Prozessor (ab 80486) oder kompatible
- SiliconGraphics/MIPS RISC
- Motorola/IBM Power PC (ab 603)
- Digital Alpha AXP

wobei bei allen Plattformen neben den Single- auch viele Multiprozessorsysteme verwendet werden können. Peripheriegeräte können entsprechend ihrer Marktgängigkeit eingesetzt werden (d.h. im PC-Bereich praktisch die gesamte verfügbare Peripherie, wenn auch bei exotischer Hardware mit Einschränkungen gerechnet werden muß). Entsprechend den Marktverhältnissen sind nur die Versionen für Intel und Alpha von Bedeutung.

## 1.5. Betriebssystemarchitektur - Subsysteme

Anmelde- prozeß	Win32-An- wendung	POSIX-An- wendung	OS/2-An- wendung	An- wendung	An- wendung	...	Sub- systeme
Security- Subsystem	Win32- Subsystem	POSIX- Subsystem	OS/2- Subsystem	Subsystem	Subsystem	...	(User- modus, Ring 3)
I/O- Manager	Window- manager	Object- manager	Security (SAM)	Process- manager	Local Procedure Call (LPC)	VM- Manager	Windows NT Executive
	Graphik- geräte treiber	Kernel					(Kernel- Modus, Ring 0)
		HAL					
Hardware							

### 1.5.1. Executive

Die Executive stellt den Umgebungssystemen die Dienste (z.B. Dateizugriffe, Netzwerkzugriffe, ...) zur Verfügung. Dazu bildet die Executive eine einheitliche Schnittstelle und verteilt die Aufgaben in ihre Teilsysteme (Komponenten)

### 1.5.2. Hardware-Abstraction-Layer (HAL)

Die HAL virtualisiert die Hardware des Computersystems für die darüberliegenden Schichten von NT und schafft so die Voraussetzungen für die Unabhängigkeit des Betriebssystems von der verwendeten Plattform. Für eine neue Plattform muß dadurch nur die HAL neu programmiert werden, für die restlichen Komponenten des Betriebssystems genügt meist die Übersetzung in den entsprechenden Maschinencode.

### 1.5.3. Kernel

Das Kernstück des Betriebssystems, daß u.a. die CPU(s) verwaltet. Er optimiert die Zuteilung der CPU(s) auf die einzelnen Threads (kleinste Verarbeitungseinheiten der laufenden Prozesse) und koordiniert die anderen Komponenten der Executive.

### 1.5.4. I/O-Manager

Sämtliche Ein- bzw. Ausgabeoperationen werden vom I/O-Manager durchgeführt. Dazu besteht er aus mehreren Teilen, wie Gerätetreibern, Treiber für die einzelnen Dateisysteme (z.B. NTFS, CDFS, FAT), Netzwerkkartentreiber und sonstigen Hardwaretreibern. Zusätzlich gibt es innerhalb des I/O-

Managers noch einen zentralen Cachemanager, der die Daten des gesamten I/O-Subsystems (Plattenzugriffe, Netzwerkzugriffe, ...) zwischenspeichert.

### **1.5.5. Graphiksystem**

Bis zur Version 3.51 von Windows NT war die Graphik Teil des Win32-Subsystems. Das führt allerdings zu geringer Performance, da häufige Wechsel zwischen Subsystem (Ring 3) und Kerneleinsten (Ring 0) Zeit kosten. In der Version 4.0 wurde daher ein eigenes Graphiksystem als Teil der Executive etabliert (daher neue Graphiktreiber notwendig) wodurch die Geschwindigkeit der Graphikausgabe wesentlich erhöht wurde. Genaugenommen ist das aber eine Verletzung der NT-Architektur, die die Prozessorunabhängigkeit erschwert.

### **1.5.6. Objectmanager**

Objekte bestehen aus den Datentypen, den dazugehörigen Attributen und den darauf anwendbaren Methoden. Der Objektmanager erzeugt an Hand der Definition eines Objekttyps eine Laufzeitinstanz dieses Typs und diese Laufzeitinstanz wird Objekt genannt. Die Ressourcen des Systems können damit durch Objekte so abgebildet werden, daß sich andere Komponenten nicht mehr mit dem Aufbau der Objekte beschäftigen müssen. Der Objektmanager erzeugt, löscht und verwaltet die Objekte, dabei ist ein wesentlicher Teil der Verwaltung die Zugriffskontrolle auf die Objekte gemeinsam mit dem Securitymanager.

### **1.5.7. Securitymanager**

Der Securitymanager ist für die Sicherheit und Integrität des Systems und der Daten zuständig, dazu werden die Zugriffserlaubnis auf Objekte geprüft und bei Bedarf Überwachungsmeldungen erzeugt.

### **1.5.8. Prozeßmanager**

Der Prozeßmanager erzeugt, löscht und verwaltet Prozesse, dabei bestehen Prozesse aus einem oder mehreren Threads, Objekten und einem virtuellen Adreßraum.

### **1.5.9. LPC-Manager**

Der LPC-Manager ist für die Kommunikation der einzelnen Komponenten der Executive verantwortlich. Der Mechanismus ist den RPCs (Remote Procedure Calls) aus dem Netzwerkbereich angelehnt.

### **1.5.10. Speichermanager**

Der Speichermanager ist für die Zuteilung des virtuellen Adreßraums eines Prozesses auf einen physisch vorhandenen Adreßbereich bzw. das Ein- und Auslagern von Speicherseiten (von der bzw. auf die Festplatte) zuständig.

### **1.5.11. Sicherheitssystem**

Bekommt vom Anmeldeprozeß die Anmeldeanfragen der Benutzer und prüft mittels der Datenbank des SAM (Security Account Manager) und des Sicherheitskontrollmonitors (ebenfalls Bestandteil der Executive) die Berechtigungen.

### **1.5.12. Win32-Subsystem**

Bildet mittels APIs die Schnittstelle zwischen Win32-Anwendungen und dem Betriebssystemkern. Für DOS/Win3.x-Anwendungen startet das Win32-Subsystem eigene VDMs (Virtual DOS Machine), wobei Win3.x-Anwendungen standardmäßig in einer gemeinsamen VDM - der WOW (Win16 on Win32) - laufen.

### **1.5.13. POSIX-Subsystem**

Stellt eine Umgebung für POSIX (Portable Operating System Interface for computing environments) Programme zur Verfügung

### **1.5.14. OS/2-Subsystem**

Stellt eine Umgebung für OS/2 V1.x Programme dar (Textmodus).

## 1.6. Domänenkonzept

### 1.6.1. Einordnung

Einzelplatz-PC      Jeder Rechner verwaltet die Benutzerkennungen - sofern vorhanden - selbst. Damit kann jeder Rechner nur seine eigenen Ressourcen im Netz verwenden.



Arbeitsgruppe      Als Arbeitsgruppe bezeichnet man einige PCs, die meist im Rahmen eines „Peer-to-Peer“-Netzes auf gemeinsame Ressourcen (Drucker, Dateien, ...) zugreifen, dabei kann jeder einzelne Rechner in dieser Arbeitsgruppe Ressourcen dem Netzwerk zur Verfügung stellen bzw. auch von anderen Rechnern zur Verfügung gestellte Ressourcen nutzen. Die Nachteile dieser Lösung bestehen in der aufwendigen Verwaltung (jeder Benutzer braucht auf jedem Rechner, auf dessen Ressourcen er zugreifen möchte, ein lokales Benutzerkonto) und in der mangelnden Flexibilität des Sicherheitssystems (eine Ressource ist freigegeben oder nicht; es existiert keine Möglichkeit für einzelne Benutzer verschiedene Levels festzusetzen). Innerhalb einer Arbeitsgruppe kann es selbstverständlich auch mehrere dedizierte Server geben, allerdings muß auch hier ein Benutzerkonto für jeden Benutzer, der Ressourcen dieses Servers benutzen möchte, existieren.



Domäne      Für Server-Client-Netzwerke eignet sich das Domänenkonzept wesentlich besser, da es gegenüber einer Arbeitsgruppe eine einfachere Administration darstellt (Es existiert nur ein Benutzerkonto innerhalb der Domäne für jeden Benutzer, daher muß sich ein Benutzer nur einmal in der Domäne anmelden und nicht mehr an jedem Server). Noch besser wäre eine globaler Verzeichnisdienst nach X.500 ähnlich Streettalk von Banyan oder NDS von Novell; dieser ist für die nächste Version von NT angekündigt und wird mittelfristig das Domänenkonzept ablösen.

Eine Arbeitsstation kann nicht gleichzeitig Mitglied einer Arbeitsgruppe und einer Domäne sein!

## 1.6.2. Definitionen

Domäne	Eine Domäne ist eine logische Struktur, in der für einen oder mehrere Server eine zentrale Benutzerkontendatenbank verwendet und verwaltet wird.
PDC	Primary Domain Controller (Primärer Domänenkontroller); jener Server der die zentrale Benutzerkontendatenbank enthält. In jeder Domäne kann es nur einen PDC geben, an diesem werden alle Verwaltungsaktivitäten durchgeführt.
BDC	Backup Domain Controller (Sicherungsdomänenkontroller); ein Server, der eine Kopie der Benutzerkontendatenbank enthält und ebenfalls Anmeldungen der Benutzer verifizieren kann. Die Replikation der Datenbank mit vom PDC wird regelmäßig und automatisch durchgeführt. Dabei ist aber darauf zu achten, daß eventuell sonst noch notwendige Dinge, wie Anmeldeskripte und Benutzerprofile repliziert werden, da sonst die erforderliche Ausfallsicherheit nicht gegeben ist.
Server	Ein Server in einer Domäne, der keine lokale Kopie der Benutzerdatenbank besitzt und gewisse Services im Netzwerk anbietet (Printserver, ...)
Single Domain	Das gesamte Netzwerk wird in einer einzigen Domäne organisiert
Trusted Domain	Domäne, der von einer anderen Domäne vertraut wird, d.h. die Benutzer einer solchen Domäne können auch Ressourcen der anderen Domäne verwenden.
Trusting Domain	Domäne, die einer anderen Domäne vertraut, d.h. wenn ein Benutzer in der anderen Domäne gültig angemeldet ist, kann er auch in dieser Domäne Ressourcen in Anspruch nehmen.
Master Domain	Domäne, die die Verwaltung der Benutzerkonten übernimmt und neben der noch weitere Domänen ohne eigene Benutzerkonten existieren.
Ressource Domain	Domäne, die Ressourcen (File-, Printservices, ...) zur Verfügung stellt, aber keine Benutzerkonten beinhaltet.

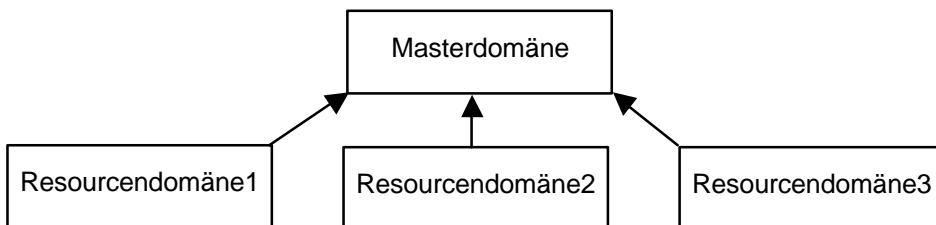
### 1.6.3. Domänenmodelle

#### Single Domain-Model

Alle Komponenten des Netzwerkes sind in einer Domäne organisiert, daher ist hier auch die Verwaltung am einfachsten. Für die physische Obergrenze einer Domäne lassen sich keine verlässlichen Zahlen angeben (die Zahlen für die maximale Anzahl an Konten schwanken zwischen 26000 und 50000); allerdings ist davon auszugehen, daß schon wesentlich früher eine zusätzliche Strukturierung vorgenommen werden muß.

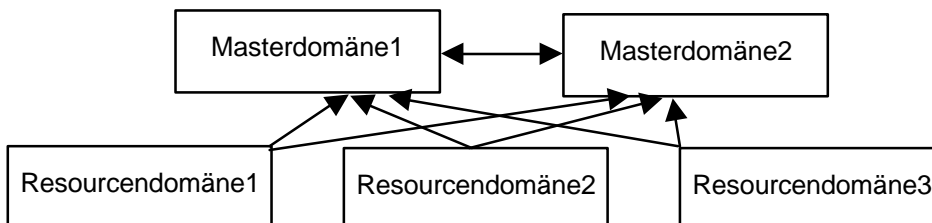
#### Master Domain-Model

Hier wird eine Domäne mit allen Benutzerkonten eingerichtet (die Masterdomäne) und mehrere Ressourcendomänen, die der Masterdomäne vertrauen.



#### Multiple Master Domain-Model

In Erweiterung des Master Domain Modells können die Benutzer auch auf mehrere Domänen aufgeteilt werden, die untereinander eine Vertrauensstellung besitzen. Die Ressourcendomänen vertrauen wiederum den Masterdomänen.



Die Vertrauensbeziehungen sind prinzipiell einseitig, selbstverständlich können aber durch Eintragung zweier Vertrauensstellungen auch bidirektionale Vertrauensbeziehungen verwirklicht werden. Das Einrichten der Vertrauensstellungen erfolgt mit dem Benutzermanager (Richtlinien - Vertrauensstellungen - Berechtigt dieser Domäne zu vertrauen in vertraute Domäne einzurichten bzw. Richtlinien - Vertrauensstellung - Vertraute Domänen in vertrauender Domäne einrichten).

## **2. Aufbau WS-Server-Verbindung**

### **2.1. Hardwareverbindung**

Um eine Verbindung zwischen Workstation und Server aufnehmen zu können, muß zuerst die physikalische Verbindung zwischen der Arbeitsstation und dem Server hergestellt werden, d.h. sowohl der Server als auch die Arbeitsstation müssen mit einem Netzwerkadapter ausgestattet und ein Kabel dazwischen verlegt sein. Diese Komponenten müssen ordnungsgemäß installiert und konfiguriert sein, damit ein funktionierender Betrieb möglich ist. Während des Betriebs können natürlich auch von dieser Seite Probleme auftauchen (Unterbrechung des Kabels, Defekt der Steckkarte, ...), daher sind alle Komponenten insbesondere externe Kabel mit besonderer Vorsicht zu behandeln. Bei den Arbeitsstationen ist insbesondere auf die einstellbaren Parameter der Adapter zu achten, da Anwender gelegentlich Änderungen vornehmen und die dabei entstehenden Probleme nicht in Zusammenhang mit den von ihnen durchgeführten Änderungen bringen.

### **2.2. Softwareverbindung**

Wenn ein Arbeitsplatzrechner mit dem Netzwerk physikalisch verbunden ist, muß noch eine Verbindungsmöglichkeit für die Software geschaffen werden, wobei hier wieder eine Hardware-Softwareschnittstelle und eine Schnittstelle zwischen dem Betriebssystem am Arbeitsplatz und dem Netzwerkbetriebssystem (meist beschrieben durch das Betriebssystem am Server) unterschieden wird. Für die Hardware-Softwareschnittstelle wird im Bereich Windows-NT NDIS (Network Driver Interface Specification) verwendet, auf das hier nicht näher eingegangen wird. Für die zweite Schnittstelle ist ein Redirector, der NetBIOS unterstützt, am Arbeitsplatzbetriebssystem notwendig. Das Aktivieren eines Redirectors bewirkt die Initialisierung der für das Netzwerk notwendigen Teile und erlaubt auch einen beschränkten Zugriff auf andere Netzwerkressourcen (z.B.: auf die Informationen, die für das Anmelden notwendig sind).

Die zum Verbindungsaufbau gehörigen Programme und eventuelle Parameterdateien (z.B.: PROTOCOL.INI) sollten von einem Anwender nicht verändert werden, da dafür tiefere Netzwerkkennnisse erforderlich sind. Bei der Änderung von Systemdateien (z.B.: AUTOEXEC.BAT und CONFIG.SYS) sollte man im Zweifelsfall ebenfalls einen Netzwerkbetreuer zu Rate ziehen.

### **2.3. Redirectorvarianten**

Dieser Redirector ist selbstverständlich vom verwendeten Betriebssystem am Arbeitsplatz abhängig und bei den neueren Betriebssystemen von Microsoft inkludiert. So hat sowohl Windows 95 als auch Windows NT einen Arbeitsstationsdienst, der diese Aufgabe übernimmt, bei Windows for Workgroups beziehungsweise den älteren Netzwerkbetriebssystemen von Microsoft (LAN-Manager, MS-Net) ist ein geeigneter Redirector ebenfalls inkludiert, nur für die verschiedenen DOS-Varianten (ab V3.3) und

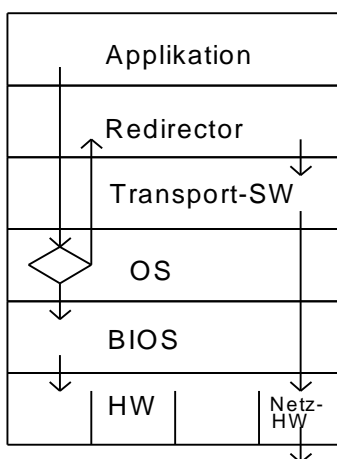
Windows V3.1 ist ein solcher Redirector extra zu besorgen (diese Clients sind aber u.a. auf der Windows NT Server CD-ROM zu finden). Für Clients, die über eine Schnittstelle zum Netzwerkbetriebssystem Netware verfügen, existiert ein zusätzlicher Serverdienst (eigene Lizenz), der am NT Server installiert werden kann und die Kommunikation mit solchen Clients ermöglicht. Dieser Dienst setzt sämtliche Anfragen der Netware Clients auf NETBIOS um und leitet sie an den Server weiter. Die Antworten werden wieder von NETBIOS auf NCP (Netware) umgesetzt, sodaß der Client genau so, wie mit einem Netwareserver kommunizieren kann. In umgekehrter Richtung (Server fragt Client) funktioniert dies analog. Für Apple-Talk Clients existiert ein ähnlicher Dienst zur Umsetzung der AFP-Schnittstelle auf die NETBIOS-Schnittstelle.

Welches Übertragungsprotokoll für den Transport der NETBIOS-Information verwendet wird, ist für die eigentliche Funktion der Workstation-Server-Verbindung nebensächlich, allerdings hängt davon ab, wie andere Systeme im Netz (z.B.: Router) mit diesen Informationen umgehen. Zur Verfügung stehen NETBEUI und TCP/IP für MS-Clients (Windows xx) bzw. NWLINK (IPX/SPX) und Apple-Talk für nicht MS-Clients.

z.B.: DOS-Client

Die Dateien sind üblicherweise im Verzeichnis C:\NET zu finden, die wichtigsten davon sind der NDIS-Treiber (z.B.: NE2000.DOS), der Protokollmanager (PROTMAN.EXE), das Netzwerkverwaltungsprogramm (NET.EXE) und die Konfigurationsdatei (PROTOCOL.INI). Bei zusätzlicher Verwendung eines Netwareclients wird der NDIS-Treiber meist durch den ODI-Treiber von Novell ersetzt und mittels Softwarekonverter (ODIHLP.EXE, NWLINK.EXE) genutzt. Für Windows 3.x ist noch der Treiber für das Dateisystem (IFSHLP.SYS) notwendig.

Funktionsweise eines Redirectors:



## 2.4. Anmelden

Danach kann die Anmeldung an das Netzwerk durchgeführt werden (z.B.: NET LOGON), damit erfolgt die anwenderspezifische Registrierung wodurch erst die Möglichkeit besteht, daß dem Anwender seine persönliche Arbeitsumgebung im Netzwerk geschaffen wird. Oftmals wird der NET

LOGON-Befehl (oder äquivalent) automatisch beim Einschalten des Netzwerkes aufgerufen, sodaß der Anwender nur seinen Namen (oft schon vorausgefüllt) und ein Kennwort eingeben muß, um die Anmeldung korrekt durchführen zu können. (Bei manchen Betriebssystemen erfolgt die Anmeldung an das Netzwerk automatisch mit der Anmeldung an die Arbeitsstation, dabei ist besonders auf die Sicherheit der Arbeitsstation zu achten!) Sollte ein Tippfehler aber zum Abbruch führen oder der Befehl nicht automatisch aufgerufen werden, muß man möglicherweise noch auf das Laufwerk und in das Verzeichnis wechseln, in dem NET steht oder dieses Laufwerk und Verzeichnis beim Befehlsaufruf mitangeben.

Während des Anmeldens werden für den Benutzer die notwendigen Tabellen im Server initialisiert und eventuell ein Loginscript exekutiert. Diese Loginscripts ermöglichen eine Anpassung an die besonderen Bedürfnisse des Anwenders.

## 3. Dateikonzepte

### 3.1. Allgemeines

Windows NT ist für die Unterstützung mehrerer Dateisysteme ausgelegt, wobei aber nicht jene dynamischen Möglichkeiten der Netware und ihrer Namespaces gegeben ist. D.h. eine Partition hat zu einem Zeitpunkt nur ein Dateisystem (und nicht mehrere logische, die auf ein physisches abgebildet werden), das über das Netzwerk zur Verfügung gestellt wird. Windows NT unterstützt sowohl das ältere FAT-(File Allocation Table)-System, mit Einschränkungen noch das OS/2-eigene HPFS (High Performance File System) als auch das für NT neu entwickelte NTFS (NT File System). Ein Client kann auf das Serverdateisystem sowohl über UNC (Universal Naming Convention oder auch Unified Name Convention)-Namen als auch über einen logischen lokalen Laufwerksbuchstaben zugreifen, wobei bei der zweiten Methode die Netzwerksoftware für die Umsetzung auf die Servernamen sorgt. Ein UNC-Name besteht aus folgenden Teilen:

```
\\servername\freigabename(alias)\verzeichnis\...\dateiname
```

Die FAT-Nachfolgedateisysteme von Windows95 (VFAT und VFAT32) werden von Windows NT nicht unterstützt, können aber in einem NT-Netz am Client verwendet werden.

### 3.2. FAT-Dateisystem

Das einfachste und älteste Dateisystem am PC eignet sich für den Einsatz unter NT nur schlecht, da es mit einer Reihe von Einschränkungen verbunden ist, die für ein Serversystem nicht zulässig sind:

- Dateinamen müssen der 8.3-Konvention genügen (unter NT kleinere Ausnahmen)
- Nur vier Dateiattribute (S,H,R,A)
- Maximale Partitionsgröße 4GB
- Steigende Platzverschwendung bei Partitionen über 32 MB (Clustertime bei 4 GB: 64 KB)
- Keine Sicherheitsfunktionen
- Keine Ausfallssicherheit (Stromausfall bei Änderungen der FAT führen i.a. zu Datenverlust)

BIOS-Bereich
FAT1 (für jeden Cluster ein Eintrag, wo der nächste Cluster liegt)
FAT2 (Kopie als Sicherheit)
Rootverzeichnis (Dateiname, Attribute(ASHR, Datum, Zeit), Anfangscluster, Größe)
Datenbereich
...

### 3.3. HPFS-Dateisystem

Bis zur Version 3.51 von NT wurde dieses Dateisystem unterstützt, bei der Version 4.0 fehlt der entsprechende Treiber. Wenn notwendig, kann der Treiber von der Version 3.51 weiterverwendet werden (PINBALL.SYS), die Einschränkungen bei der Verwendung von HPFS gelten aber weiter (Keine Zugriffskontrolllisten, kein Hot-Fixing, ...). Durch die mangelnde Unterstützung durch NT sollte dieses Dateisystem bei Neuinstallation keine Verwendung mehr finden, insbesondere da HPFS über keine Eigenschaften verfügt, über die NTFS nicht auch verfügen würde. Die wesentlichen Verbesserungen gegenüber dem FAT-Dateisystem sind:

- Lange Dateinamen (bis 255 Zeichen) mit Punkten, Leerzeichen und Groß/Kleinschreibung
- Keine Beschränkungen bei der Pfadangabe
- Dateiattribute (Autor; bis 64 KB / Datei)
- Partitionsgröße bis 1 TB
- Keine Cluster
- Optimierte Lage der Systembereiche
- Verbesserter Ausfallsschutz durch Protokollierung

Bootblock
Bootstrap
Superblock
Spareblock
Band 1 (8MB Datenbereich)
...
Bitmap 1
Bitmap 2
Band 2 (8MB Datenbereich)
...
Band 3 (8MB Datenbereich)
...
Bitmap n-1
Bitmap n
Band n (8MB Datenbereich)

### 3.4. NTFS-Dateisystem

Das NT-eigene Dateisystem und daher für den Einsatz auf einem Server empfehlenswerteste Dateisystem ist aber NTFS. Die wesentlichen Verbesserungen gegenüber dem FAT-Dateisystem sind:

- Lange Dateinamen (bis 255 Zeichen) mit Punkten, Leerzeichen und Groß/Kleinschreibung

- Nicht nur ASCII-Zeichen, sondern alle Zeichen aus dem Unicode (65536)
- Keine Beschränkungen bei der Pfadangabe
- erweiterte Dateiattribute (ohne Größenbeschränkung)
- Partitionsgröße bis 16 EB ( $2^{64}$ )
- Ständige Protokollierung der Dateizugriffe, damit verbesserter Ausfallsschutz
- Zugriffssicherheit

NTFS richtet auf jeder Partition eine MFT (Master File Table) genannte Hauptdatei ein, mit der auf alle anderen Dateien zugegriffen wird. Die ersten 16 Einträge der MFT sind für Verwaltungszwecke reserviert, ab dann beginnen Dateien und Verzeichnisse, wobei jeder Eintrag in der MFT 2 KB groß ist.

Ein wesentlicher Vorteil von NTFS ist, daß kleinere Dateien (bis ca. 1,5KB) direkt in der MFT gespeichert werden können, daher kein Zugriff an eine zweite Stelle auf die Festplatte notwendig ist. In NTFS werden die Dateien auch nicht mehr sequentiell wie in FAT organisiert, sondern wie in HPFS an Hand eines B-Trees.

In NTFS können einzelne Dateien oder Verzeichnisse komprimiert werden, da der Zustand der Komprimierung einfach ein weiteres Datei- bzw. Verzeichnisattribut ist. Bei Servern sollte allerdings laut Auskunft von Microsoft auf die Komprimierung verzichtet werden, um die Performance nicht zu beeinträchtigen.

Die hohe Ausfallssicherheit wird durch ein Hot-Fixing erreicht, wobei nach jedem Schreibvorgang ein Lesevorgang zur Kontrolle stattfindet, dadurch können fehlerhafte Blöcke noch vor einem Datenverlust ausgetauscht werden. Weiters unterstützt NTFS auch die bekannten Verfahren zur Plattenspiegelung und RAID-Verfahren.

Das Transaktionsmanagement umfaßt bei NT jeden Schreib- und Lesevorgang wodurch nach einem Ausfall des Systems (z.B.: durch einen Stromausfall) die Daten auf den letzten konsistenten Zustand zurückgefahren werden können.

Die Zugriffssicherheit wird hier durch erweiterte Sicherheitsattribute (=Dateiattribute) erreicht.

Boot-Sector (mit BIOS Parameter Block und MFT-Verweis)
Dateibereich (variable Größe)
...
Beginn MFT
Datenbereich (variable Größe)
...
MFT-Mirror (nur die wichtigsten Informationen)
Datenbereich (variable Größe)
...

## Aufbau MFT

Eintrag 0 - \$mft (Beschreibung der MFT selbst)
Eintrag 1 - \$mftmirror (Beschreibung der MFTmirror)
Eintrag 2 - \$logfile (Beschreibung des Logfiles)
...
Eintrag 16 - 1. Datei

## Aufbau eines MFT-Records

Header (Allgemeine Systeminformationen, Transaktionsinformation, ...)
Attribut Standardinformationen (Größe, Datum, Uhrzeit (Erzeugung, letzter Zugriff, ...), FAT-Attribute)
Attribut Dateiname
Daten (bei kleineren Dateien der Inhalt der Datei, sonst Zeiger auf die Datenbereiche)
Attribut Sicherheitsbeschreibung (ACLs, ...)

### Begriffe:

Residente Informationen:	Alle Informationen (Attribute, Daten), die im MFT-Record stehen
Externe Attribute	Alle Attribute, die im MFT-Record keinen Platz haben und daher in einem eigenen MFT-Record gespeichert werden (dieser MFT-Record enthält nur einen Header und Verweise auf Datenbereiche).

## Verzeichnisse

Verzeichnisse sind innerhalb von NTFS nur spezielle Indexdateien, wobei in NTFS nicht wie gewohnt nur der Name als Indexkriterium herangezogen werden kann. Die Benutzerschnittstelle unterstützt allerdings nur Indizes mit dem Dateinamen als Ordnungskriterium. Auch hier gilt, solange der Index im MFT-Record untergebracht werden kann, wird er dort gespeichert, sonst stehen im Datenbereich wieder Zeiger auf die eigentlichen Daten (auch hier baumartig, sollte ein MFT-Record nicht ausreichen). Jeder Eintrag im Index enthält das Ordnungskriterium (Dateiname) und einen Verweis auf den MFT-Record der dazugehörigen Datei.

### Vordefinierte Attribute:

Liste (Liste aller zulässigen Attribute)

Dateiname

MS-DOS-Kurzname

Version

Standardattribute (Größe, Erzeugungs- bzw. Änderungs- und Zugriffsdaten)

Sicherheitsbeschreibung

...

Manche dieser Attribute werden derzeit noch nicht verwendet.

## 4. Drucken im Netz

### 4.1. Überblick

Eine Applikation kann auf einem lokalen Drucker oder einem freigegebenen Drucker auf einem anderen Arbeitsplatz/Server drucken. Ein expliziter Printserver ist im Unterschied zu Netware nicht vorgesehen, sondern jeder Arbeitsplatz/Server ist für die von ihm freigegebenen Drucker Printserver und Verwalter der Queue. In einem NT-Netzwerk hält auch die Arbeitsstation (der Server), die (der) einen Drucker freigibt, die notwendigen Druckertreiber dafür bereit, sodaß keine lokale Installation notwendig ist. Dieser Mechanismus wird derzeit für alle NT-Versionen und Windows 95 unterstützt.

Jeder Druckclient kann einen der folgenden Datentypen an einen NT-Drucker übergeben:

EMF	Enhanced Meta Files (neu seit NT 4.0) Diese Daten kommen direkt vom GDI-System und werden erst vom Druckserver für den Drucker aufbereitet.
RAW	Druckbereite Daten, die direkt an den Drucker übergeben werden können.
RAW (FF appended)	RAW-Daten, denen ein FF hinzugefügt wird.
RAW (FF auto)	RAW-Daten, denen bei Bedarf ein FF hinzugefügt wird.
Text	Einfacher Text ohne Formatanweisungen
Pscript I	Postscript-Daten (z.B. von MAC-Clients), die eventuell noch auf druckbare Bitmaps umgewandelt werden müssen (wenn der Drucker kein Postscript beherrscht).

### 4.2. Druckerarten

#### a.) Lokaler Drucker

Ein lokaler Drucker im Netzwerk verhält sich wie ein Drucker an einem einzelnen Arbeitsplatz

#### b.) Netzwerkdrucker

Ein Netzwerkdrucker steht für mehrere/alle Arbeitsplätze im Netzwerk zur Verfügung. Er ist entweder ein lokaler Drucker an einer Arbeitsstation oder einem Server und wird von dieser / diesem für die Benutzung im Netz freigegeben; ist selbst netzwerkfähig oder wird mit Hilfe eines dedizierten Printserver / Netzwerkdruckermoduls (z.B.: Intel Netport, HP JetDirect, ...) dem Netzwerk zur Verfügung gestellt.

### 4.3. Druckerinstallation

Ob Netzwerkdrucker oder lokaler Drucker die Installation erfolgt immer mit dem Assistenten für die Druckerinstallation. Bei einem lokalen Drucker wird der Anschluß und der Druckertyp ausgewählt (nach Herstellern zusammengefaßt), bei Netzwerkdruckern wird nur aus einer Liste von im Netzwerk

vorhandenen Druckern einer ausgewählt (bei nicht von NT-freigegebenen Druckern muß auch hier der Druckertyp ausgewählt werden).

Sollten verschiedene Konfigurationen des selben Druckers benötigt werden, ist die Installation mehrerer logischer Drucker zu einem physikalisch vorhandenen Drucker möglich. Dafür installiert man einen weiteren Drucker des selben Typs mit dem selben Anschluß und vergibt einen zweiten Namen. Danach kann dieser Drucker unabhängig vom ersten konfiguriert werden (z.B.: verschiedene Zugriffszeiten, ...)

Als günstig für die tägliche Arbeit hat sich eine Verknüpfung mit dem Drucker auf dem Desktop erwiesen, da durch Ziehen eines Dokuments auf das Druckersymbol ein Ausdruck durchgeführt werden kann und durch die Verknüpfung auf dem Desktop immer ein Druckersymbol vorhanden ist.

#### **4.4. Druckerkonfiguration**

Mit dem Hilfeprogramm zur Druckerkonfiguration können alle Einstellungen, die den Drucker betreffen, verändert werden. Im Punkt „Allgemein“ können Einstellungen zur Trennseite bzw. zum Druckprozessor vorgenommen werden, weiters gibt es hier die Möglichkeit den Treiber zu erneuern, eine Testseite zu drucken oder Kommentare zum Drucker festzuhalten. Im Punkt „Anschlüsse“ kann der Anschluß verändert werden; im Punkt „Zeitplanung der Druckaufträge“ werden die Zeiten festgelegt, in denen der Drucker verfügbar ist, die Priorität der Druckaufträge, die Art der Warteschlangenverwendung bzw. einige Optionen für das Drucken. Im Punkt „Freigabe“ wird festgelegt ob und unter welchem Namen der Drucker im Netz zur Verfügung steht und für welche Clientbetriebssysteme (NT-Varianten bzw. Windows 95) Treiber vorrätig gehalten werden. Im Punkt „Sicherheit“ werden die Zugriffsberechtigungen und die Art und Weise der Überwachung festgelegt. Im Punkt „Geräteeinstellungen“ werden gerätespezifische Einstellungen vorgenommen (z.B.: die Zuordnungen zwischen Papierformat und Schacht, der installierte Speicher, sonstige installierte Optionen (Schriftarten, ...), Art und Weise der Rasterung, ...).

Über die Druckserverkonfiguration können die für diesen Drucker möglichen Formulare festgelegt werden, die vom Anwender danach ohne genauere Kenntnisse der Druckerhardware verwendet werden können. Ferner können auch über den Druckserver die Anschlüsse konfiguriert werden und eine Reihe weiterer Einstellungen vorgenommen werden: Welcher Ordner für die Warteschlange Verwendung finden soll, welche Informationen protokolliert werden sollen und zwei Besonderheiten für Remotedruckaufträge (Warnton bei Fehlern, Benachrichtigen, wenn Remoteaufträge gedruckt werden)

## 4.5. Hilfsprogramme

### 4.5.1. Assistent für die Druckerinstallation

Über „START → Einstellungen → Drucker“ oder „Arbeitsplatz → Drucker“ gelangt man zur Liste der vorhandenen Drucker bzw. zum Assistenten für die Druckerinstallation. Durch Doppelklick auf das Symbol „Neuer Drucker“ wird der Assistent gestartet. Mögliche Auswahlen:

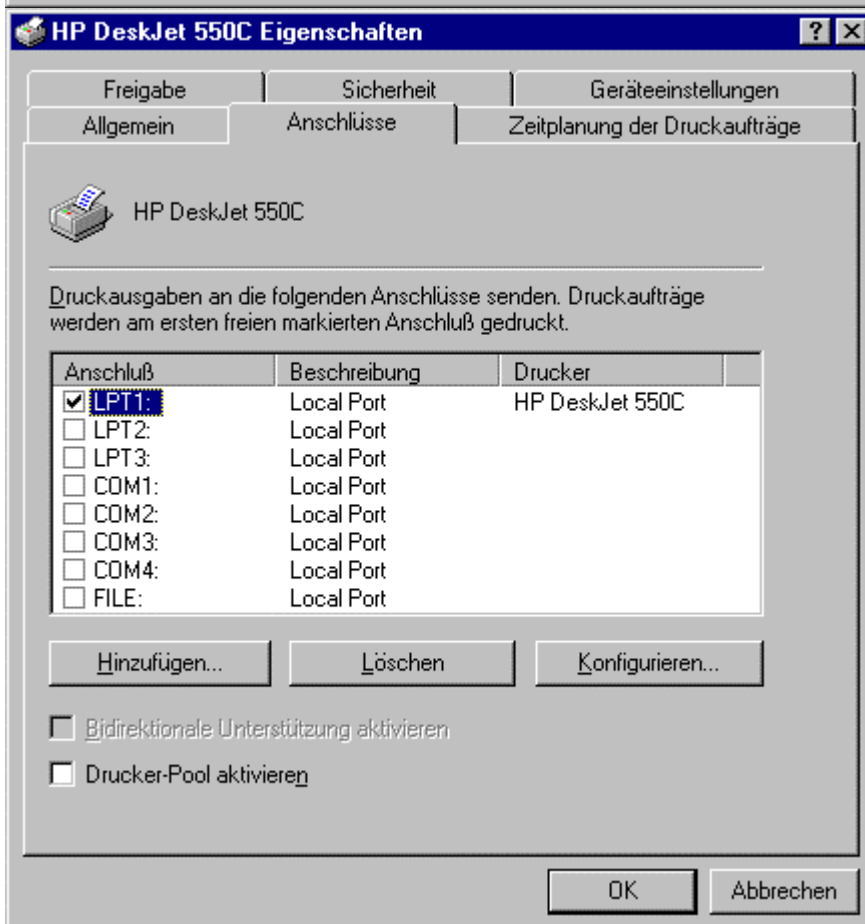
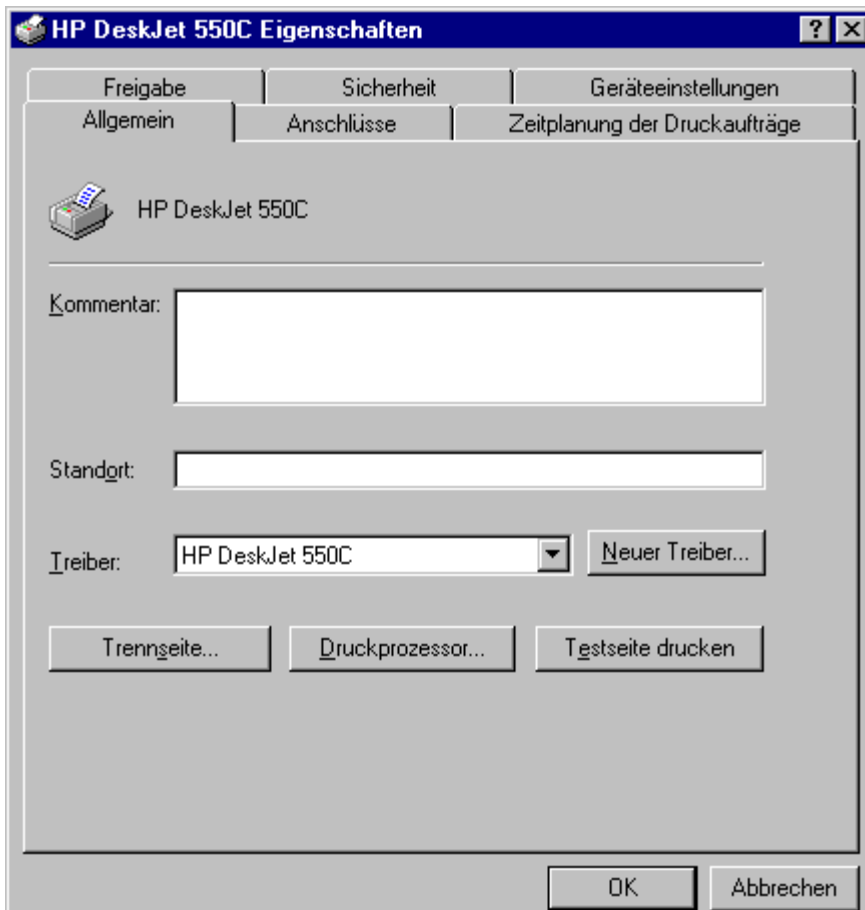
- Arbeitsplatz
  - Anschluß (LPT1:, LPT2:, ..., COM1:, ..., FILE:, ...; eventuell mehrere über einen Druckerpool)
  - Druckerauswahl
    - Hersteller (Generic, HP, IBM, ...)
    - Druckermodell
    - Diskette
  - (Standarddrucker Ja/Nein)
- Netzwerk
  - Domäne
    - Server
      - Drucker
  - (Standarddrucker Ja/Nein)

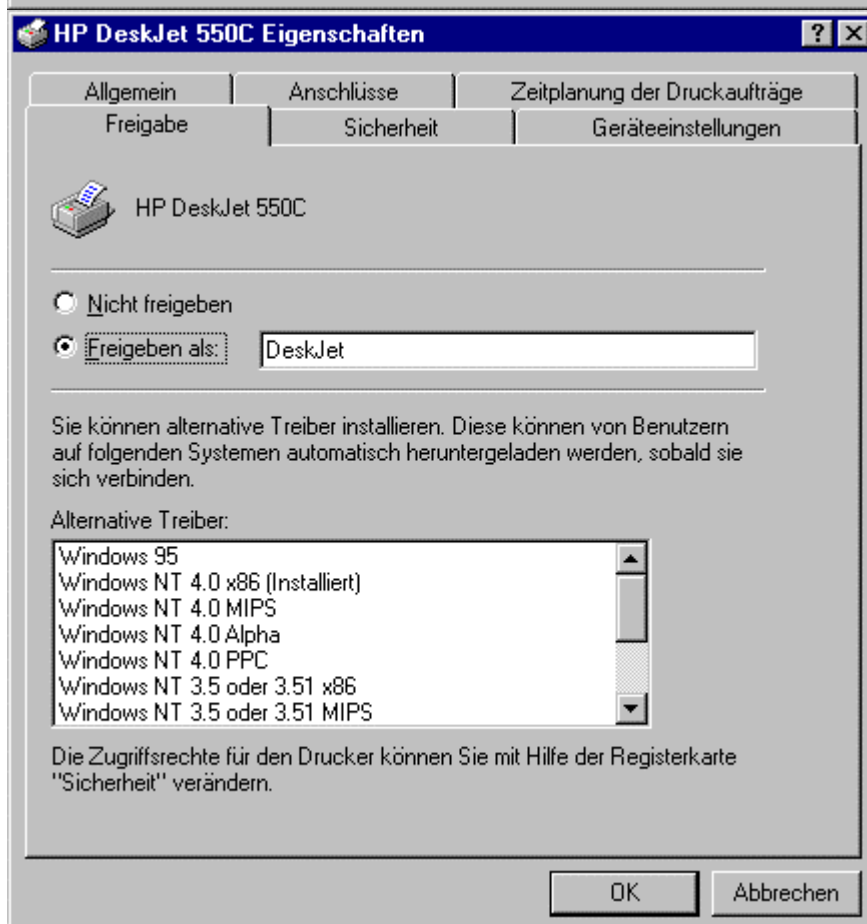
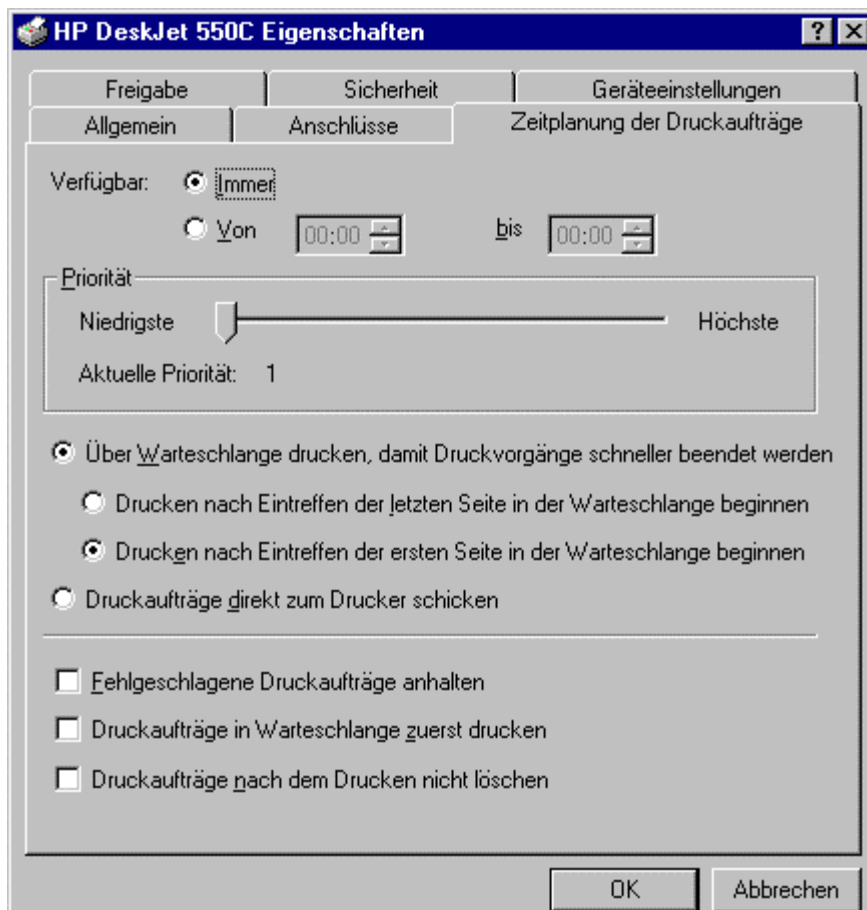
### 4.5.2. Druckerkonfiguration

Über „START → Einstellungen → Drucker“ oder „Arbeitsplatz → Drucker“ gelangt man zur Liste der vorhandenen Drucker bzw. zum Assistenten für die Druckerinstallation. Durch Klick auf das Symbol des gewünschten Drucker und danach über „Datei → Eigenschaften“ kommt man zum Konfigurationsmenü des Druckers. Mögliche Auswahlen:

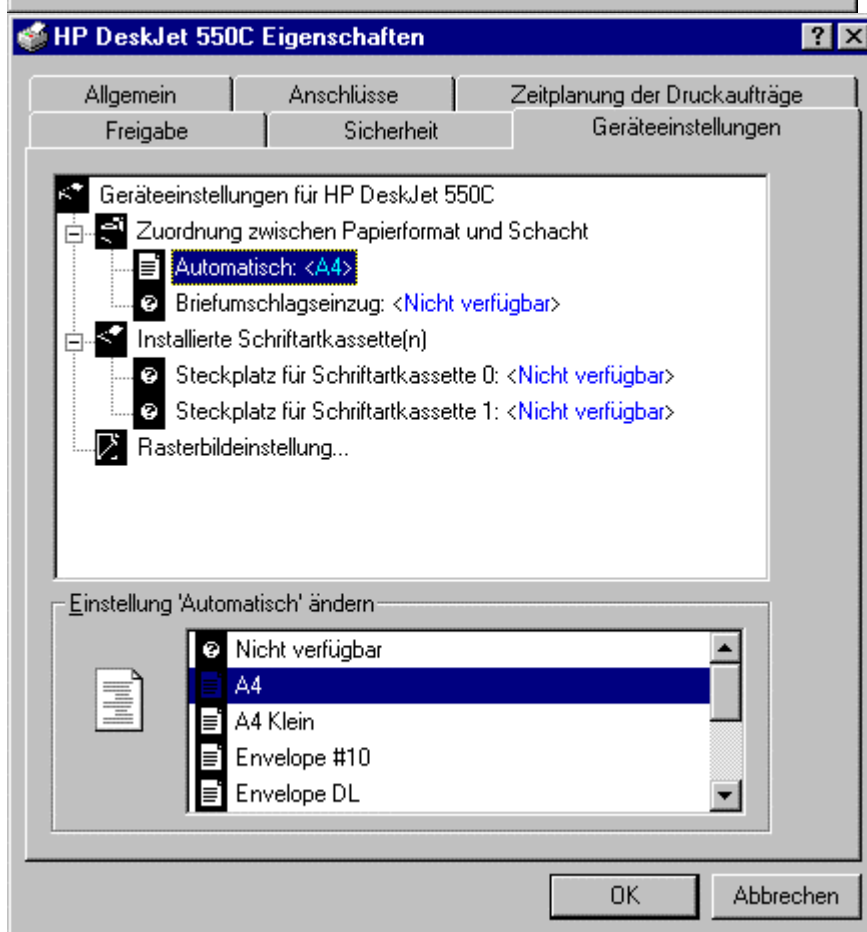
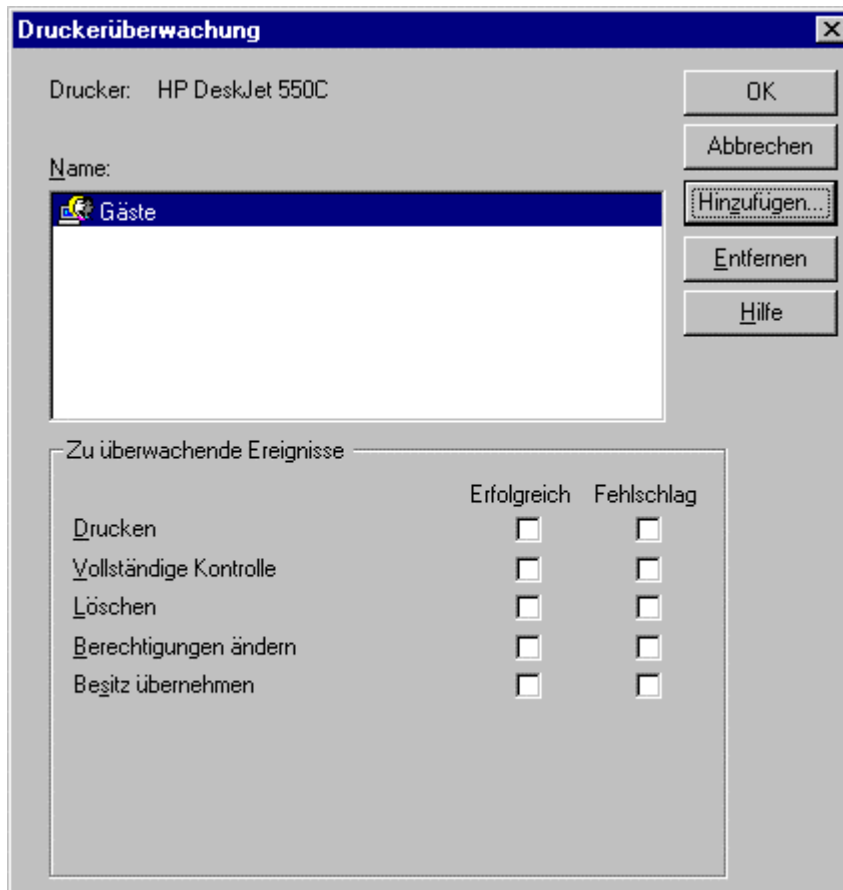
- Allgemein
  - Kommentar
  - Standort
  - Treiber
  - Neuer Treiber
  - Trennseite
  - Druckprozessor
    - winprint
    - RAW, ...
  - Testseite drucken
- Anschlüsse
  - siehe Installation

- Zeitplanung der Druckaufträge
  - Verfügbar
    - immer
    - von ... bis ...
  - Aktuelle Priorität
  - Über Warteschlange drucken
    - Drucken nach Eintreffen der letzten Seite
    - Drucken nach Eintreffen der ersten Seite
  - Druckaufträge direkt zum Drucker schicken
  - Fehlgeschlagene Druckaufträge anhalten: Ja/nein
  - Druckaufträge in Warteschlange zuerst drucken: Ja/Nein
  - Druckaufträge löschen: Ja/Nein
- Freigabe
  - Nicht freigeben
  - Freigeben als: ...
    - Treiberunterstützung für: ...
- Sicherheit
  - Berechtigungen
  - Überwachung
  - Besitzer
- Geräteeinstellungen
  - Geräteparameter (z.B.: Zuordnung zwischen Papierformat und Schacht)









### 4.5.3. Servereigenschaften

Über „START → Einstellungen → Drucker“ oder „Arbeitsplatz → Drucker“ gelangt man zur Liste der vorhandenen Drucker bzw. zum Assistenten für die Druckerinstallation. Durch Klick auf das Symbol des gewünschten Drucker und danach über „Datei → Servereigenschaften“ kommt man zum Konfigurationsmenü des zum Drucker gehörigen Servers. Mögliche Auswahlen:

- Formulare
- Anschlüsse
- Optionen
  - Warteschlangenordner (%SYSTEMROOT%\System32\Spool\PRINTERS)
  - Protokolliere Warteschlangen-Warnungen (Ja/Nein)
  - Protokolliere Warteschlangen-Fehler (Ja/Nein)
  - Protokolliere Warteschlangen-Informationen (Ja/Nein)
  - Signalton bei Fehlern von Remoteaufträgen (Ja/Nein)
  - Benachrichtigen, wenn Remoteaufträge gedruckt werden (Ja/Nein)

### 4.5.4. Druckmanager

Über „START → Einstellungen → Drucker“ oder „Arbeitsplatz → Drucker“ gelangt man zur Liste der vorhandenen Drucker bzw. zum Assistenten für die Druckerinstallation. Durch Doppelklick auf das Symbol des gewünschten Drucker wird der Druckmanager gestartet, mit dem die Druckjobs verwaltet werden können. Mögliche Auswahlen:

- Datei
  - Drucker anhalten
  - Als Standarddrucker verwenden Ja/Nein
  - Einstellungen für Dokumente (druckerabhängig)
  - Freigabe
  - Druckaufträge löschen
  - Eigenschaften (siehe Druckerkonfiguration)
  - Schließen
- Dokument
  - Anhalten
  - Fortsetzen
  - Neu starten
  - Abbrechen
  - Eigenschaften
- Ansicht
- ? (Hilfe)

## 5. Betreuung von Arbeitsgruppen

Für die Betreuung von Arbeitsgruppen ist es notwendig über die vollen Administrationsrechte zu verfügen; eine Unterteilung dieser Rechte bzw. spezielle Administratoren für Teilbereiche sind in Windows NT im Gegensatz zu anderen Netzwerkbetriebssystemen nicht vorgesehen.

### 5.1. Benutzereinrichten

Benutzer werden unter NT von einem Administrator (oder Konten-Operator) eingerichtet, dabei wird zumindest der Benutzername (Max. 20 Zeichen) und das Paßwort (max. 14 Zeichen) vergeben. Zusätzlich können die Eigenschaften Gruppenzugehörigkeit, Umgebungsprofil, Anmeldezeiten, Anmeldearbeitsstationen, Kontoinformation und Einwählinformation festgelegt werden. Diese Parameter können auch für bestehende Benutzer mit Hilfe des Benutzermanagers für Domänen verändert werden. Vorinstallierte Benutzer sind nur der „Administrator“ und ein deaktivierter „Gast“, alle anderen Benutzer müssen mit Hilfe des Benutzermanagers oder des Verwaltungsassistenten für die Benutzerverwaltung angelegt werden, dies ist insbesondere bei der Erstinstallation von Nachteil, da hier meist eine große Anzahl von Benutzern angelegt werden soll. Ein Anlegen vieler Benutzer mittels einer Liste ist hier nicht vorgesehen, für solche Fälle sollte man auf den Drittanbietermarkt ausweichen.

### 5.2. Gruppeneinrichten

Gruppen werden ebenfalls mit dem Benutzermanager eingerichtet und verwaltet; unter Windows NT wird zwischen lokalen und globalen Gruppen unterschieden. Die wichtigsten lokalen Gruppen sind:

- Administratoren Vollständige Kontrolle über den Rechner
- Benutzer Alle lokalen Benutzer (können i.a. nicht im Netz arbeiten)
- Druckoperatoren Verwaltung der Drucker und deren Freigaben am Server
- Gäste Lokale Gäste (können i.a. nicht im Netz arbeiten)

Die wichtigsten globalen Gruppen sind:

- Domänen-Admins Vollständige Kontrolle über die Dömane und alle Rechner darin
- Domänen-Benutzer Alle Benutzer der Domäne
- Domänen-Gäste Gäste in der Domäne

Unter NT können Benutzer in mehreren Gruppen eingerichtet werden und sogar Gruppen Mitglieder andere Gruppen sein (z.B.: „Domänen-Admins“ sind Mitglied von „Administratoren“).

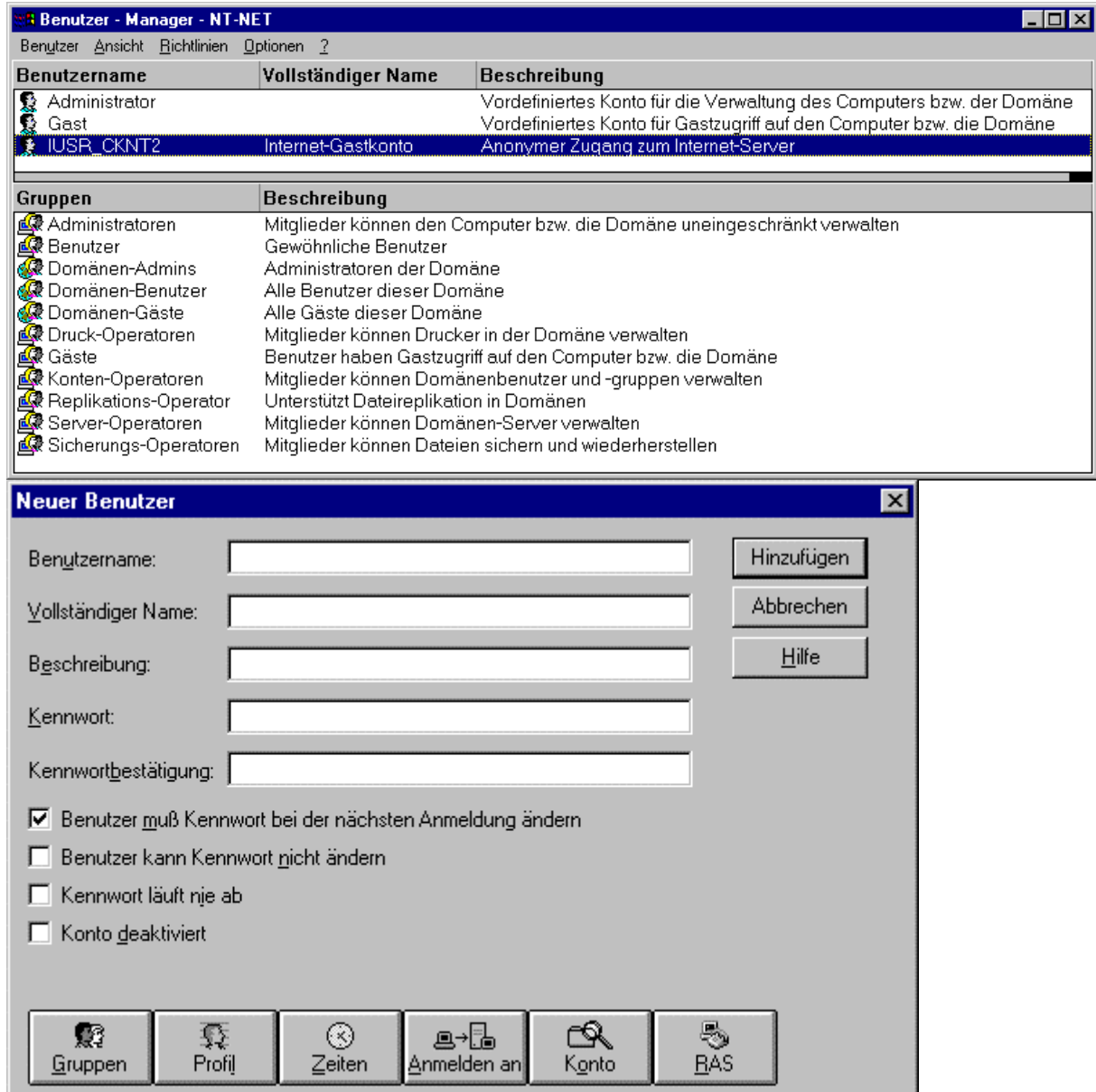
### 5.3. Richtlinien

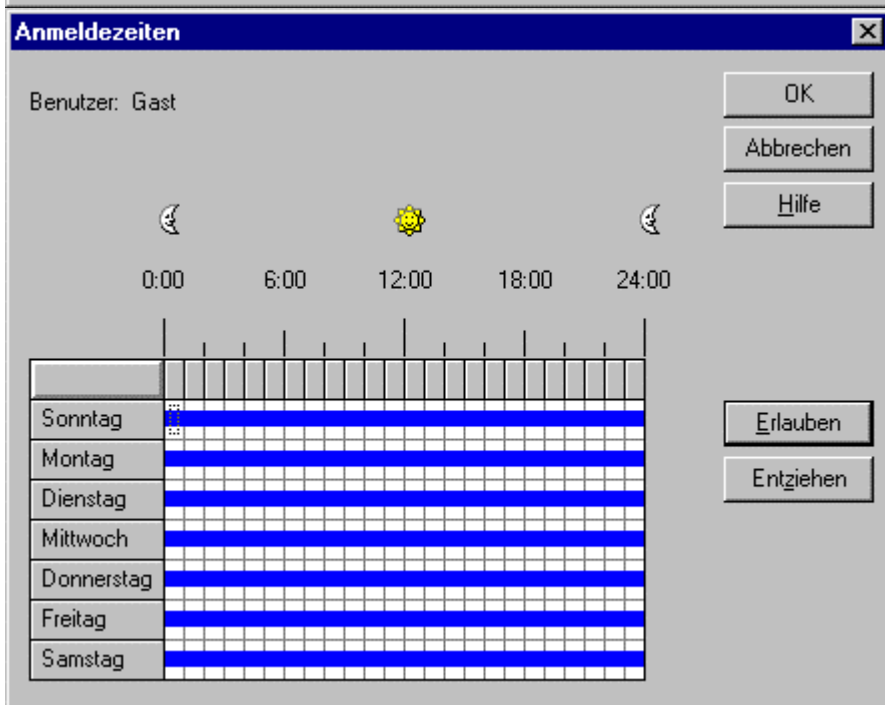
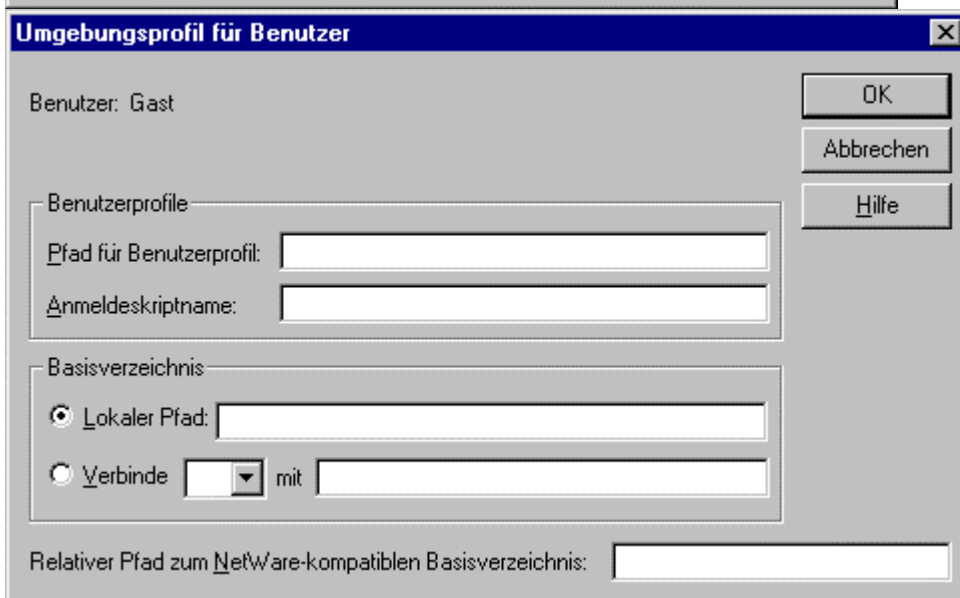
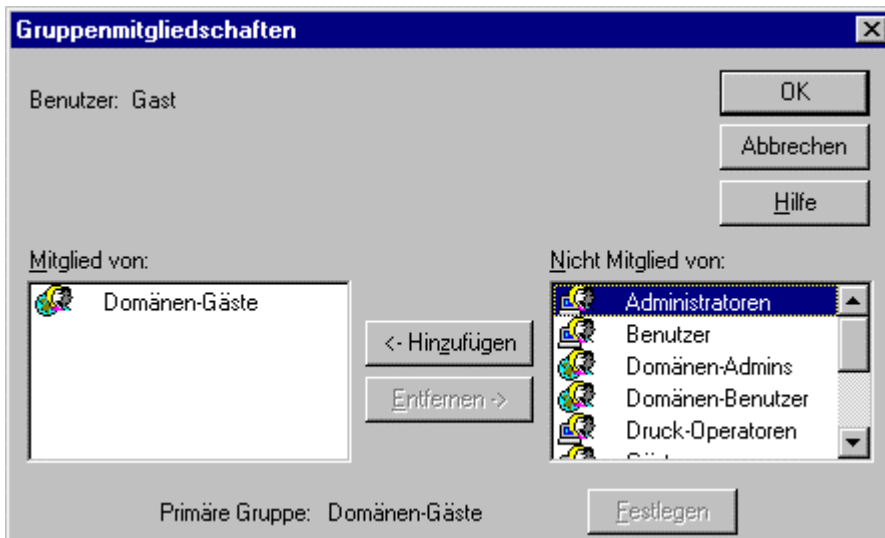
Über den Benutzermanager können auch allgemeine Richtlinien für alle Benutzerkonten festgelegt werden, diese betreffen z.B.: das Kontenalter, die Kontenlänge und die Sperre von Konten. Darüber hinaus können auch Richtlinien für Benutzerrechte (welche Gruppe verfügt über welche Rechte) und die Überwachungsrichtlinien festgelegt bzw. verändert werden. Die bei den Domänen gezeigten

Vertrauensstellungen werden ebenfalls über den Benutzermanager verwaltet (Menüpunkt Richtlinien - Vertrauensstellungen).

## 5.4. Hilfsprogramme

### 5.4.1. Benutzermanager





**Anmeldearbeitsstation** [X]

Benutzer: Gast

OK  
Abbrechen  
Hilfe

Benutzer kann sich von allen Arbeitsstationen aus anmelden

Benutzer kann sich von diesen Arbeitsstationen aus anmelden:

1.	<input type="text"/>	5.	<input type="text"/>
2.	<input type="text"/>	6.	<input type="text"/>
3.	<input type="text"/>	7.	<input type="text"/>
4.	<input type="text"/>	8.	<input type="text"/>

Benutzer kann sich von allen NetWare-kompatiblen Arbeitsstationen aus anmelden

Benutzer kann sich von diesen NetWare-kompatiblen Arbeitsstationen aus anmelden:

Netzwerkadresse	Knotenadresse
<input type="text"/>	

Hinzufügen...  
Entfernen

**Kontoinformationen** [X]

Benutzer: Gast

OK  
Abbrechen  
Hilfe

Konto läuft ab

Nie

Am

Kontotyp

G**l**obales Konto  
für normale Benutzerkonten dieser Domäne

L**o**kales Konto  
für Benutzer von nichtvertrauten Domänen

**Einwählinformationen** [X]

Benutzer: Gast

OK  
Abbrechen  
Hilfe

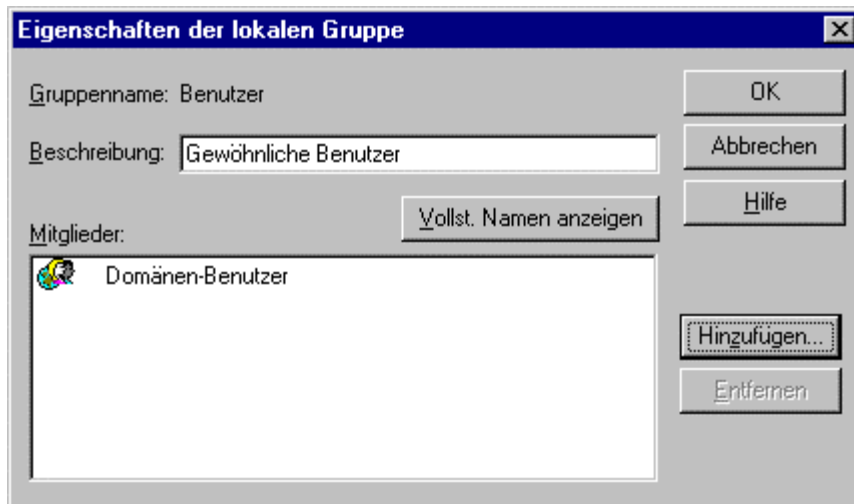
Dem Benutzer Einwährechte erteilen

Rückruf

K**ei**n Rückruf

Vom A**n**rufener festgelegt

V**o**rbelegung:



**Richtlinien für Konten** [X]

Domäne: NT-NET

OK  
Abbrechen  
Hilfe

Beschränkungen für Kennwort

Maximales Kennwortalter

Läuft nie ab

Ablauf in  Tagen

Minimales Kennwortalter

Sofortige Änderungen erlauben

Änderung in  Tagen

Minimale Kennwortlänge

Leres Kennwort zulassen

Mindestens  Zeichen

Kennwortzyklus

Keine Kennwortchronik führen

Aufbewahren:  Kennwörter

Konto nicht sperren

Konto sperren

Sperren nach  ungültigen Kennworteingaben

Konto zurücksetzen nach  Minuten

Dauer der Sperrung

Für immer (bis Administrator sie aufhebt)

Dauer:  Minuten

Remote-Benutzer bedingungslos vom Server bei Ablauf der Anmeldezeit trennen

Benutzer muß sich anmelden, um Kennwort zu ändern

**Richtlinien für Benutzerrechte** [X]

Domäne: NT-NET

OK  
Abbrechen  
Hilfe  
Hinzufügen...  
Entfernen

Recht:

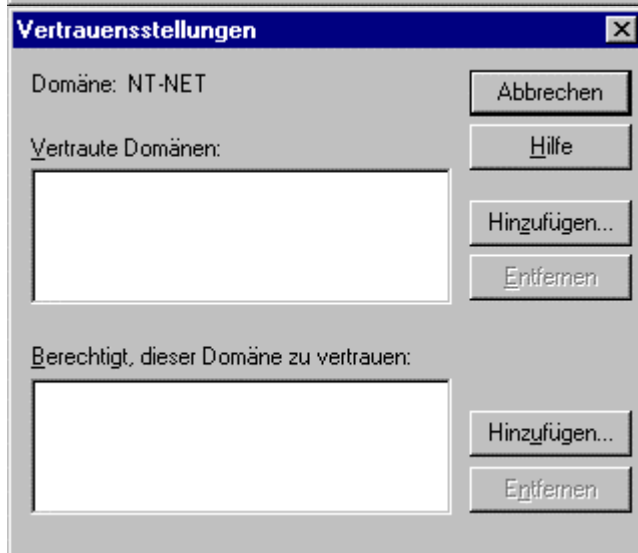
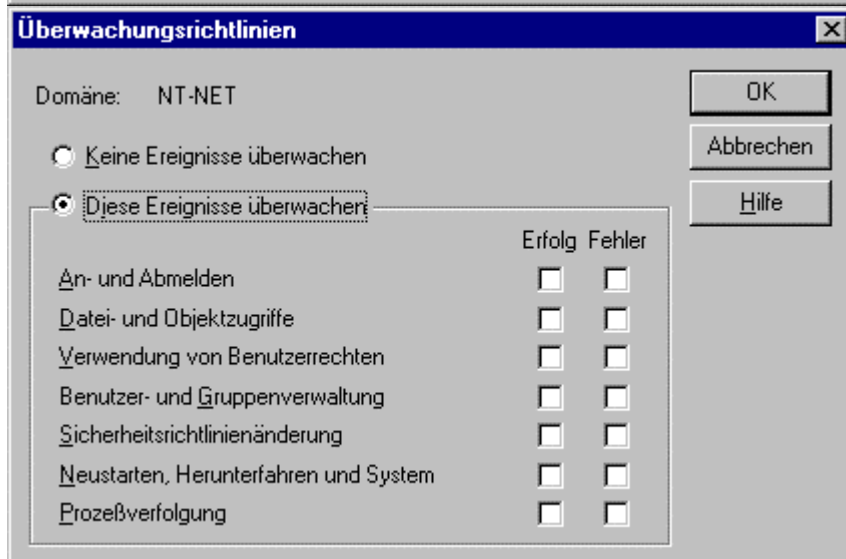
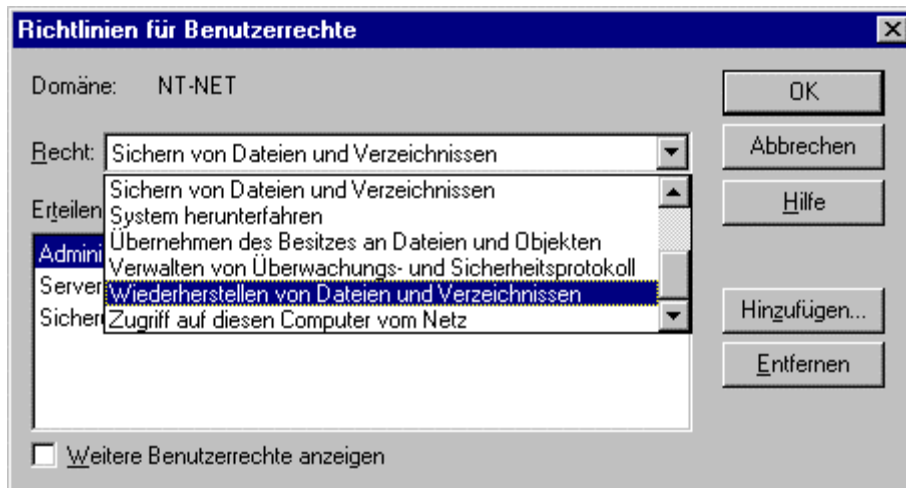
Erteilen

Admini

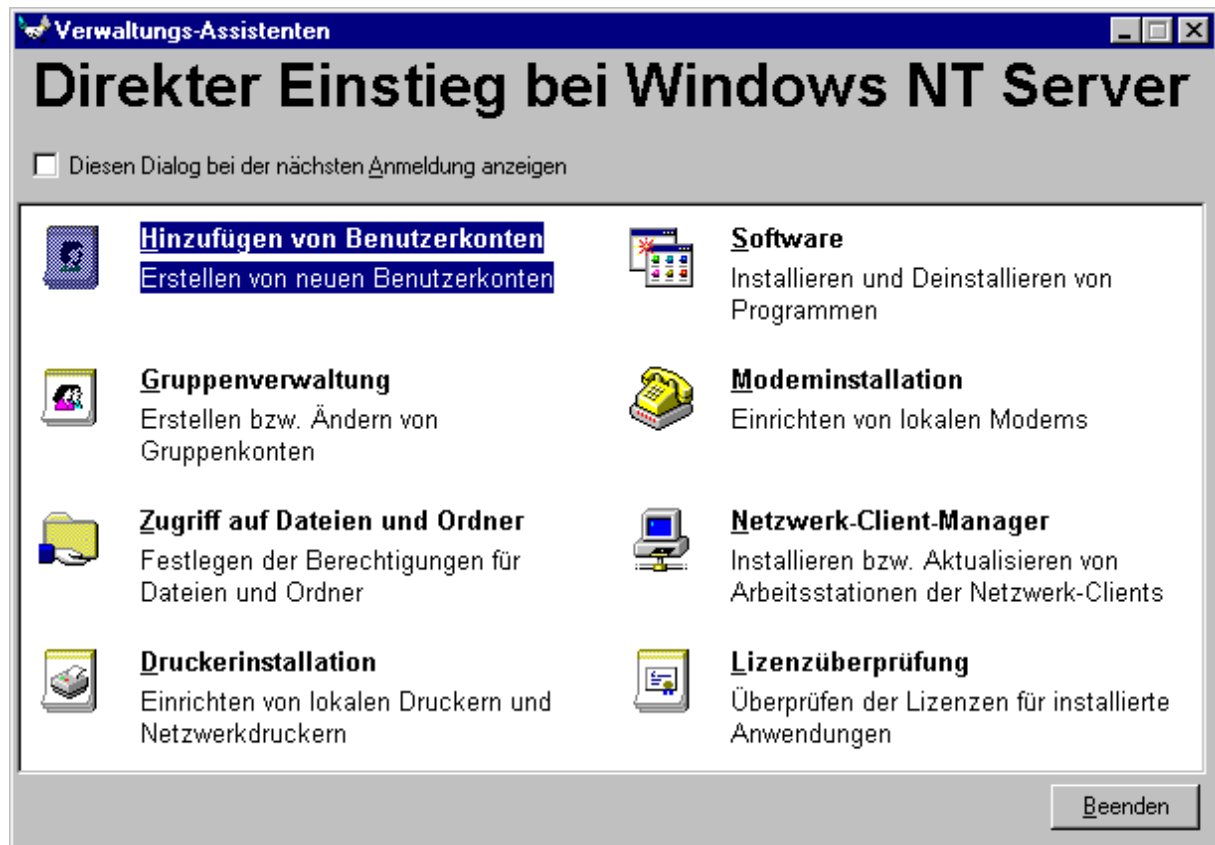
Server

- Ändern der Systemzeit
- Herunterfahren von einem Fernsystem aus
- Hinzufügen von Arbeitsstationen zur Domäne
- Laden und Entfernen von Gerätetreibern
- Lokale Anmeldung
- Sichern von Dateien und Verzeichnissen

Weitere Benutzerrechte anzeigen



## 5.4.2. Verwaltungsassistent



## 6. Wartungstätigkeiten

### 6.1. Konfigurationsdateien

#### 6.1.1. PROTOCOL.INI

Für ältere Systeme (DOS, WIN 3.x) ist die Netzwerkkonfigurationsdatei PROTOCOL.INI noch von Interesse. Diese Initialisierungsdatei ist wie alle WIN 3.x-INI-Dateien aufgebaut und enthält alle für die Verwendung des Netzwerks notwendigen Angaben. Nachdem diese Form nicht mehr von großer Bedeutung ist, sei hier statt einer detaillierten Beschreibung nur ein „sprechendes“ Beispiel einer PROTOCOL.INI-Datei angegeben:

```
[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$nwlink,MS$NWLINK
lana0=ms$ne2clone,1,ms$nwlink
lana1=ms$ne2clone,1,ms$ndishlp
```

```
[ms$ne2clone]
IOBASE=0x300
drivename=MS2000$
INTERRUPT=12
```

```
[protman]
drivename=PROTMAN$
PRIORITY=MS$NDISHLP
```

```
[MS$NDISHLP]
drivename=ndishlp$
BINDINGS=ms$ne2clone
```

```
[ms$nwlink]
drivename=nwlink$
FRAME=Ethernet_802.2
BINDINGS=ms$ne2clone
LANABASE=0
```

#### 6.1.2. Registrierungsdatenbank

In Windows-NT Systemen sind alle wesentlichen Informationen zu einer Registrierungsdatenbank zusammengefaßt, die auf mehrere Dateien verteilt und mit einer benutzerspezifischen Komponente auch die Verwaltung der Netzwerkparameter vereinfacht.

Die Hauptschlüssel der Registrierungsdatenbank sind:

HKEY_CLASSES_ROOT	Zuordnung von Dateitypen zu Anwendungen
	Subschlüssel von HKEY_LOCAL_MACHINE
	\SOFTWARE\Classes

HKEY_CURRENT_USER	Benutzereinstellungen des derzeitigen Benutzers
HKEY_LOCAL_MACHINE	Hardwarebeschreibung und -konfiguration
HKEY_USERS	Informationen über alle Benutzer
HKEY_CURRENT_CONFIG	Konfigurationsinformationen über aktuelles Profil Subschlüssel von HKEY_LOCAL_MACHINE \System\CurrentControlSet\HardwareProfiles\Current

Die Dateien der Registrierungsdatenbank sind:

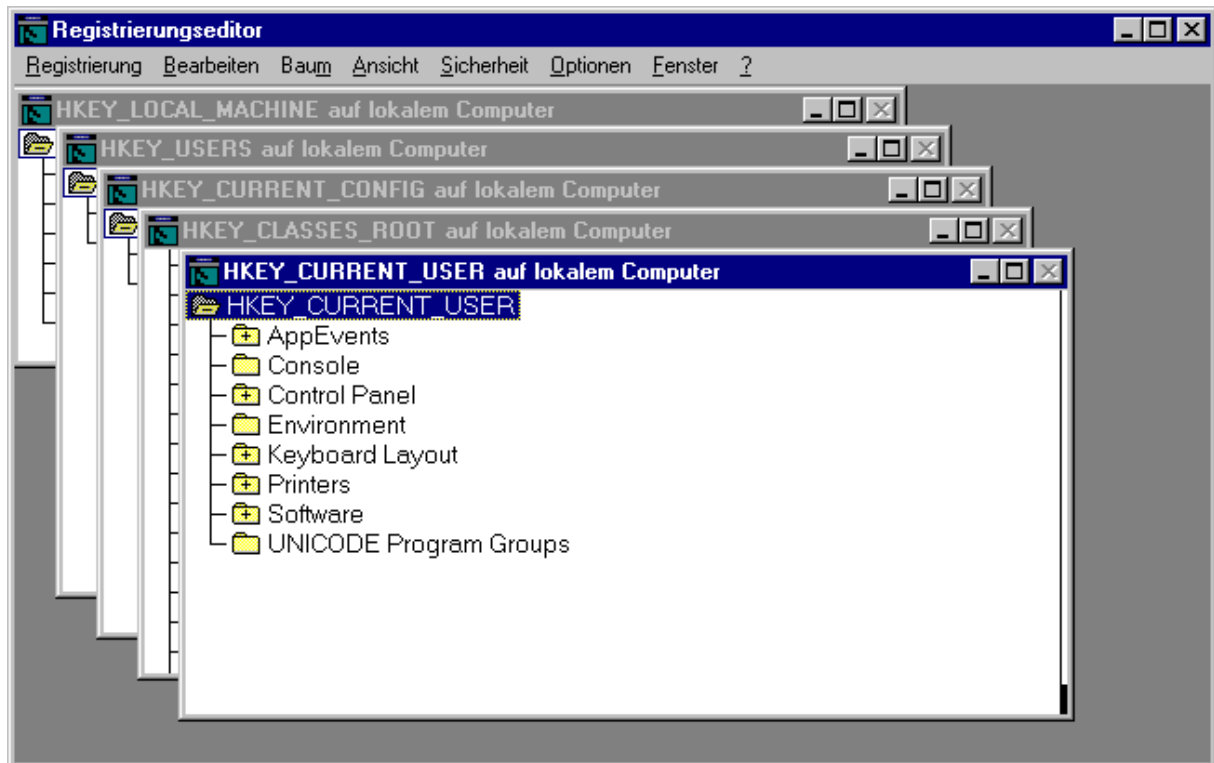
%SYSTEMROOT%\CONFIG\Sam	HKEY_LOCAL_MACHINE\SAM
%SYSTEMROOT%\CONFIG\Sam.LOG	
%SYSTEMROOT%\CONFIG\Security	HKEY_LOCAL_MACHINE\Security
%SYSTEMROOT%\CONFIG\Security.LOG	
%SYSTEMROOT%\CONFIG\Software	HKEY_LOCAL_MACHINE\Software
%SYSTEMROOT%\CONFIG\Software.LOG	
%SYSTEMROOT%\CONFIG\System	HKEY_LOCAL_MACHINE\System
%SYSTEMROOT%\CONFIG\System.LOG	
%SYSTEMROOT%\CONFIG\Default	HKEY_USERS\DEFAULT
%SYSTEMROOT%\CONFIG\Default.LOG	
%SYSTEMROOT%\Profiles\%USERNAME%\Ntuser.dat	HKEY_CURRENT_USER
%SYSTEMROOT%\Profiles\%USERNAME%\Ntuser.dat.LOG	

Format der Einträge in die Registrierungsdatenbank:

REG_BINARY	Binärwerte, die hexadezimal angezeigt werden
REG_DWORD	Doppelwort (32Bit), das binär, dezimal und hexadezimal angezeigt werden kann
REG_EXPAND_SZ	Erweiterbare Zeichenkette (kann Variable enthalten, die erst bei Abfrage ersetzt werden)
REG_MULTI_SZ	Eine Folge von Zeichenketten
REG_SZ	Eine Zeichenkette

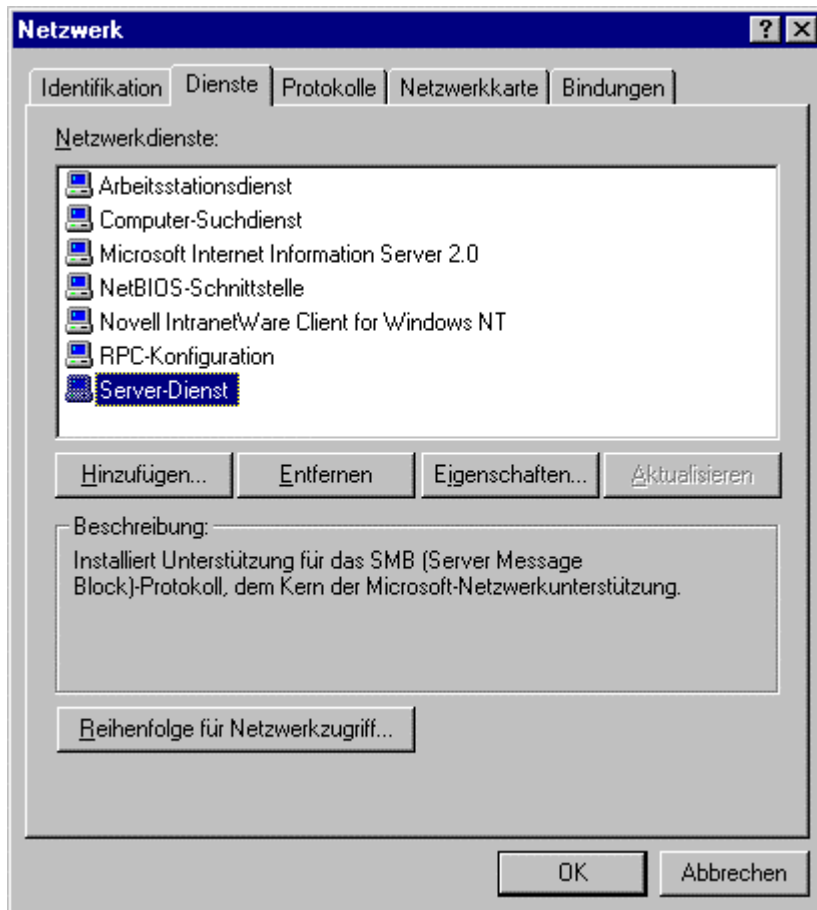
Der Registrierungseditor:

Über START → Ausführen → REGEDT32 wird der Registrierungseditor gestartet



Meist wird aber nicht direkt in der Registrierungsdatenbank gearbeitet, sondern mit der Systemsteuerung. Für den Bereich Netzwerke sieht dies so aus:





## 6.2. Benutzerprofile

Die Benutzerprofile beinhalten den HKEY\_CURRENT\_USER und darüber hinaus noch Einstellungen über den Desktop und die Ordner im Startmenü. Das Benutzerprofil ist standardmäßig lokal in „%SYSTEMROOT%\Profiles\%USERNAME%“ gespeichert, wobei die allgemeinen Programmgruppen in „%SYSTEMROOT%\Profiles\All Users“ und die Standardeinstellungen in „%SYSTEMROOT%\Profiles\Default User“ gespeichert werden. Allerdings kann auch ein Server-basierendes Profil gewählt werden, da dann der Benutzer seine gewohnte Umgebung auf allen Arbeitsplätzen vorfindet. Die Lage des Profils wird in der Umgebungsvariablen %USERPROFILE% abgelegt, um auch in Scripts und ähnlichen verwendet werden zu können.

Sollte ein Benutzer sein NTUSER.DAT nicht verändern dürfen, genügt eine Umbenennung auf NTUSER.MAN (Mandatory Profile) durch einen dazu berechtigten Benutzer (Systemadministrator); in diesem Fall kann der Benutzer zwar in der laufenden Sitzung Änderungen vornehmen, diese werden aber beim Abmelden nicht mehr zurückgespeichert, sodaß der Benutzer beim nächsten Anmelden wieder die ursprüngliche Umgebung vorfindet.

## 6.3. Scripts

Scripts in einem NT-Netzwerk sind Batch-Dateien, die bei der Anmeldung eines Benutzers ausgeführt werden, sofern sie dem Benutzer zugewiesen sind. Im Gegensatz zu anderen Netzwerkbetriebssystemen sind Scripts unter NT-Netzwerken nur von geringer Bedeutung, da die Benutzerumgebung primär durch Registrierungsdatenbank und Profil - oder gänzlich lokal - festgelegt wird. Um ein Script für alle Clientbetriebssysteme verfügbar zu haben, muß der Dateiname der 8.3-Konvention aus dem FAT-Dateisystem genügen und die Erweiterung BAT besitzen, reine NT-Scripts können auch die Erweiterung CMD verwenden.

### 6.3.1. Zuordnung eines Scripts

Mit dem Benutzermanager (Start → Verwaltung → Benutzermanager) kann durch Auswählen eines Benutzers über „Benutzereigenschaften“ → „Profil“ ein Anmeldeskriptname zugeordnet werden. Wenn keine Pfadangabe zur Verfügung steht, wird dieses Script automatisch im NETLOGON-Share des Anmeldeservers gesucht; diese Methode bewirkt eine Serverunabhängigkeit sofern die Anmeldeskripts auf alle Server (in deren NETLOGON-Shares) kopiert werden, d.h. auch bei Ausfall eines Servers ist noch eine Abarbeitung des Scripts möglich. Gruppenzugehörigkeiten können standardmäßig nicht verwendet werden.

### 6.3.2. Spezielle Scriptvariablen

Innerhalb der Anmeldeskripts stehen eine Reihe von Umgebungsvariablen zur Verfügung, die wichtigsten davon sind:

%COMPUTER_NAME	Der Name des Computers, an dem das Anmeldeskript abgearbeitet wird
%HOMEDRIVE%	Das Laufwerk, auf dem sich das Basisverzeichnis des Benutzers befindet
%HOMEPATH%	Der vollständige Pfad zum Basisverzeichnis des Benutzers
%HOMESHARE%	Der Freigabename zu %HOMEDRIVE%
%OS%	Das Betriebssystem der Arbeitsstation
%PROCESSOR_ARCHITECTURE%	Hardwareplattform (x86, MIPS, ...); diese Variable steht nur unter Windows NT zur Verfügung
%PROCESSOR_IDENTIFIER%	Typ des Prozessors der Arbeitsstation
%PROCESSOR_LEVEL%	Kurzangabe über den Prozessor (5=Pentium, 4=80486, ...)
%PROCESSOR_REVISION%	Die interne Versionsnummer der CPU
%SYSTEMDRIVE%	Laufwerk, von dem das Betriebssystem gestartet wurde
%SYSTEMROOT%	Basisverzeichnis des Betriebssystems (z.B.: C:\WINNT)
%USERDOMAIN%	Der Name der Domäne, an die angemeldet wird
%USERNAME%	Der Name des Benutzers

### 6.3.3. Beispielscript

```
@ECHO OFF
NET USE H: \\NTSERVER\DATEN
NET USE LPT2: \\DRUCKERSERVER\DESKJET
IF NOT EXIST %SYSTEMROOT%\SYSTEM32\CALC.EXE GOTO COPY
GOTO CALC
:COPY
COPY R:\CALC.EXE %SYSTEMROOT%\SYSTEM32
:CALC
CALC
```

# 7. Netzwerksicherheit

## 7.1. Überblick

Generell kann in einem Netzwerk zwischen drei Sicherheitsaspekten unterschieden werden:

- Zutrittsschutz,
- Zugriffsschutz und
- Datensicherheit.

Bei manchen Aspekten kann es günstig sein, noch einen vierten Punkt getrennt zu betrachten:

- Datenschutz.

Allerdings kann der Datenschutz in die anderen drei Sicherheitsaspekte integriert werden und wird i.A. nicht getrennt gesehen. Die Datensicherheit (Schutz vor Verlust, Schutz der Integrität, ...) ist auch auf einem Einzelplatzsystem von Interesse und wird daher hier nicht als eigener Punkt betrachtet, obwohl Windows NT selbstverständlich auch hier Unterstützung anbietet (Plattenspiegelung, Stripe-Sets, Backup, UPS-Unterstützung, ...). Die Belange der Datensicherheit, die mit unerlaubter Veränderung der Daten zusammenhängen, werden im Punkt Zugriffsschutz behandelt.

## 7.2. Zutrittsschutz

Der Zutrittsschutz bei einem Computernetzwerk muß schon bei der physikalischen Verhinderung des Zugangs für unbefugte Personen beginnen. Zu einem Server sollten z.B. nur speziell berechnigte Personen Zugang haben (z.B. Administratoren). Die Arbeitsstationen können selten so strengen Zugangskontrollen unterliegen, daher muß sich jeder Benutzer mittels eines Namens und eines geheimen Kennwortes anmelden, dabei kann jeder Account (Zugangskonto) noch zusätzlichen Restriktionen unterworfen sein.

### 7.2.1. Accountrestriktionen

Restriktion	Default	Beispiel
• Darf der Benutzer sein Paßwort ändern	Ja	Ja
• Ist ein Paßwort notwendig	Nein	Ja
• Wie groß ist die Mindestlänge des Paßwortes	6	6
• Muß das Paßwort regelmäßig geändert werden	Ja	Ja
• Wie lange ist die Gültigkeitsdauer eines Paßwortes	42	40
• Können alte Paßwörter wiederverwendet werden	Ja	Nein
• Wie lange ist die Gültigkeitsdauer des Accounts	ewig	1 Jahr
• Ist der Account gültig	Ja	Ja
• Welchen Zeitbeschränkungen unterliegt der Benutzer	Keine	Arbeitszeit
• Welchen Stationsbeschränkungen unterliegt der Benutzer	Keine	Keine
• Welches Loginscript wird für den Benutzer aktiviert	-	Benutzer

## 7.2.2. „Hacker“-Erkennung (Intruder detection)

In den Systemrichtlinien (Benutzermanager) kann eine Hackererkennung aktiviert werden, dabei werden eine einstellbare Zahl (z.B.: 3) von Fehlversuchen bei der Eingabe des Paßwortes innerhalb einer einstellbaren Zeit (z.B.: 30 Minuten) als Hackversuch definiert. Danach kann entweder nur dieses Ereignis protokolliert oder zusätzlich der betroffene Account für eine einstellbare Zeitdauer (z.B.: 1 Stunde, bis ein Administrator die Sperre aufhebt) gesperrt werden. Protokolliert werden der betroffene Account, das Datum, die Uhrzeit und die Stationsadresse.

## 7.2.3. Accounting (Kontoführung)

Windows NT unterstützt derzeit kein Accounting, d.h. eine Zuordnung von Kosten zu Benutzern oder Projekten ist nicht automatisierbar.

## 7.3. Zugriffsschutz - Rechte

Die Zugriffsrechte können in Windows NT-Netzen auf zwei Arten vergeben werden:

- Auf der Ebene von Verzeichnisfreigaben
- Auf der Ebene von NTFS

Die Verzeichnisfreigaben sind aus Kompatibilitätsgründen bzw. für am Server verwendete FAT-Partitionen vorhanden und können nur sehr grob für Benutzer oder Gruppen vergeben werden. Verzeichnisfreigaben beziehen sich auf das freigegebene Verzeichnis und alle darin enthaltenen Dateien und Unterverzeichnisse, sofern keine NTFS-Rechte entgegenstehen.

Die NTFS-Rechte können wesentlich feiner vergeben werden, wobei auch hier zur Vereinfachung einige Standardberechtigungen zur Verfügung stehen. Zugriffsrechte auf NTFS-Basis werden nicht vererbt, allerdings kann bei der Vergabe von Zugriffsrechten, die Ersetzung der Rechte auf Unterverzeichnisse durch einen Mausclick durchgeführt werden.

### 7.3.1. Mögliche Rechte auf Freigabeebene

<b>Kein Zugriff</b>	Inhaber dieses Rechts sehen die Freigabe nicht und können daher auch nicht zugreifen.
<b>Lesen</b>	Inhaber dieses Rechts können Dateien und Verzeichnisse ansehen (kopieren, ...) und Programme starten.
<b>Ändern</b>	Inhaber dieses Rechts haben das Recht Lesen und können zusätzlich Dateien und Verzeichnisse anlegen, verändern und löschen.
<b>Vollzugriff</b>	Inhaber dieses Rechts dürfen alles (Ändern der Berechtigungen, Besitzübernahme).

### 7.3.2. Mögliche Rechte auf NTFS-Ebene

#### Verzeichnisrechte

<b>Lesen (R )</b>	Inhaber dieses Rechts können Dateien und Verzeichnisse im entsprechenden Verzeichnis anzeigen.
<b>Schreiben (W)</b>	Inhaber dieses Rechts können Dateien und Verzeichnisse im entsprechenden Verzeichnis hinzufügen.
<b>Ausführen (X)</b>	Inhaber dieses Rechts können in der entsprechenden Verzeichnisstruktur wechseln.
<b>Löschen (D)</b>	Inhaber dieses Rechts können Dateien und Verzeichnisse im entsprechenden Verzeichnis löschen.
<b>Berechtigungen ändern (P)</b>	Inhaber dieses Rechts können die Berechtigungen für Dateien und Verzeichnisse im entsprechenden Verzeichnis ändern.
<b>Besitz übernehmen (O)</b>	Inhaber dieses Rechts können den Besitz von Dateien und Verzeichnissen im entsprechenden Verzeichnis übernehmen.

#### Dateirechte

<b>Lesen (R )</b>	Inhaber dieses Rechts können die entsprechende Datei lesen.
<b>Schreiben (W)</b>	Inhaber dieses Rechts können in die entsprechende Datei schreiben.
<b>Ausführen (X)</b>	Inhaber dieses Rechts können die entsprechende Datei ausführen.
<b>Löschen (D)</b>	Inhaber dieses Rechts können die entsprechende Datei löschen.
<b>Berechtigungen ändern (P)</b>	Inhaber dieses Rechts können die Berechtigungen der entsprechenden Datei ändern.
<b>Besitz übernehmen (O)</b>	Inhaber dieses Rechts können den Besitz der entsprechenden Datei übernehmen.

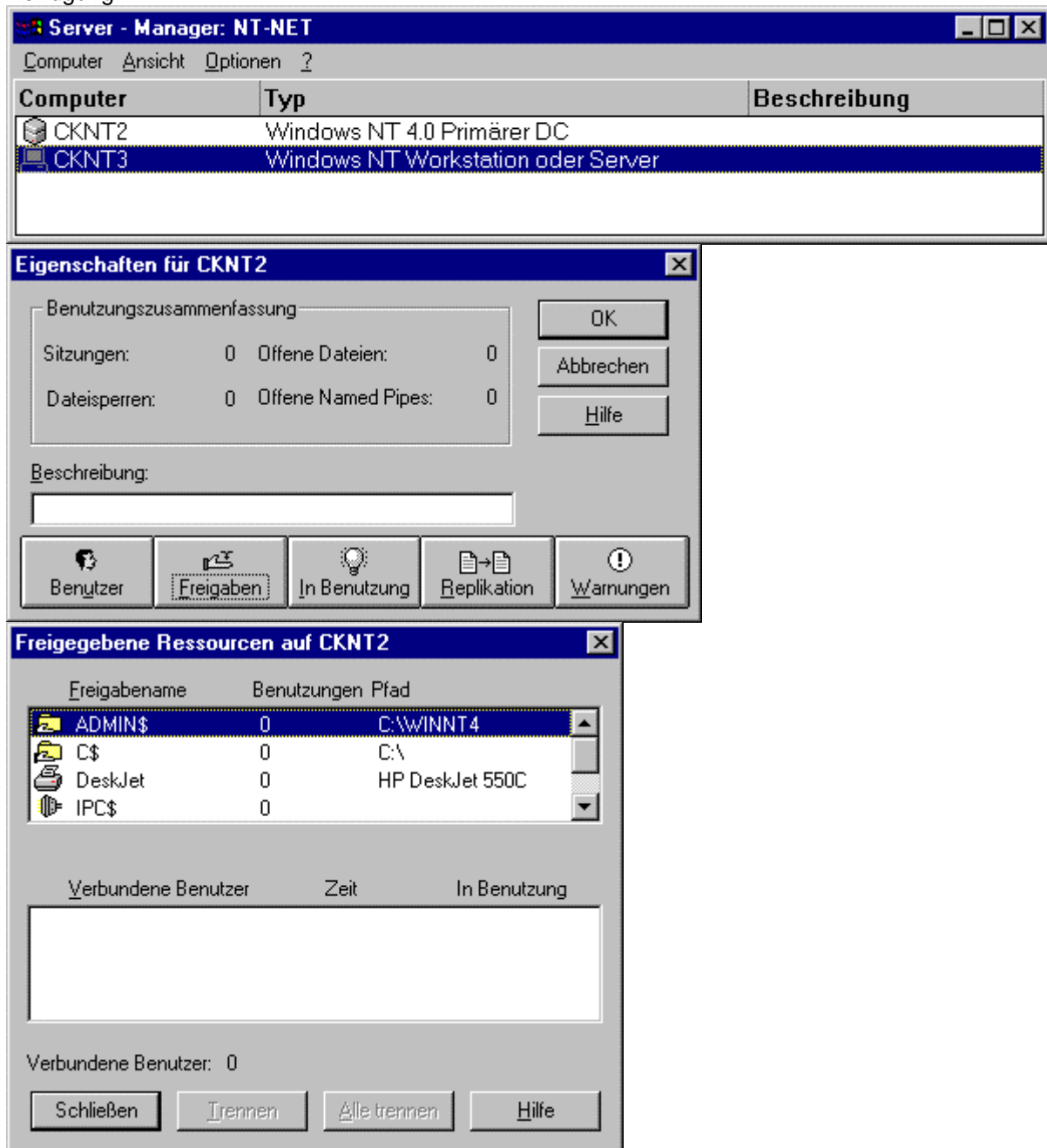
#### Standardberechtigungen:

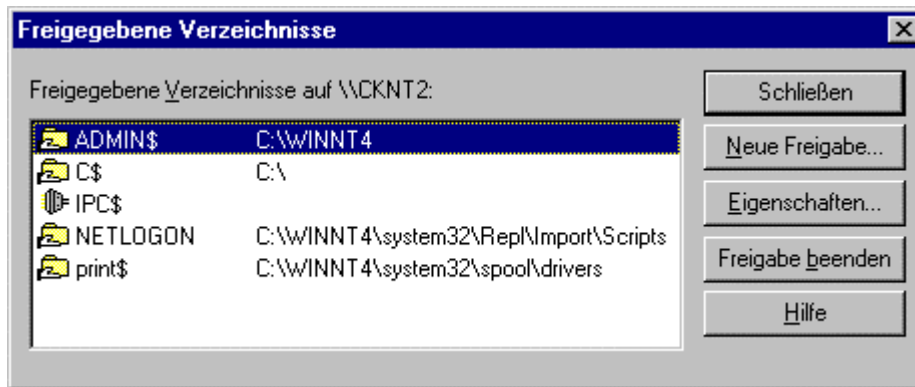
Name	Verzeichnisrechte	Dateirechte
<b>Kein Zugriff</b>	Kein	Kein
<b>Anzeigen</b>	RX	Nicht angegeben
<b>Lesen</b>	RX	RX
<b>Hinzufügen</b>	WX	Nicht angegeben bzw. für Dateien nicht verfügbar
<b>Hinzufügen und Lesen</b>	RWX	RX bzw. für Dateien nicht verfügbar
<b>Ändern</b>	RWXD	RWXD
<b>Vollzugriff</b>	Alle	Alle

## 7.4. Hilfsprogramme

### 7.4.1. Servermanager

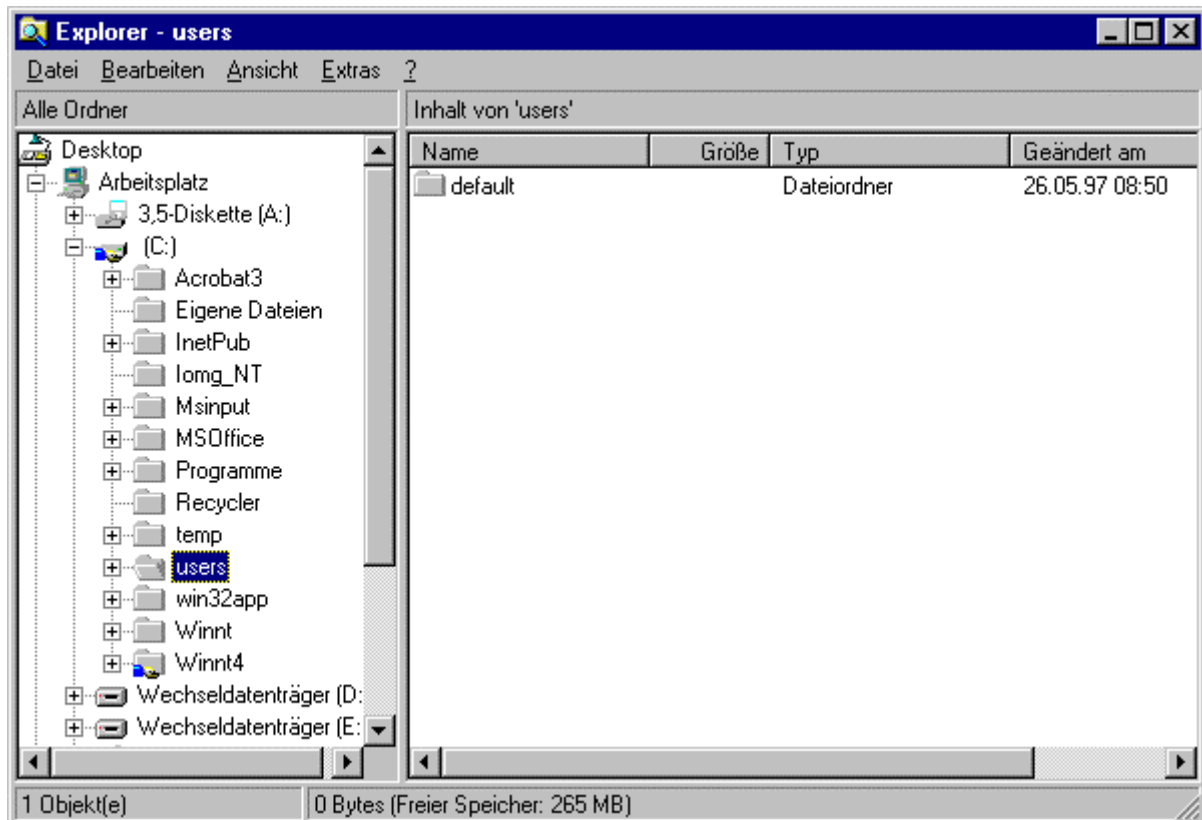
Der Servermanager dient u.a. zur Verwaltung der Freigabe (Der Servermanager kann z.B. über „START → Programme → Verwaltung → Servermanager“ aufgerufen werden). Durch Doppelklicken auf einen Server (bzw. über das Menü „Computer → Eigenschaften“) wird das Fenster mit den Eigenschaften angezeigt, durch Auswahl der Freigaben können alle bestehenden Freigaben angesehen werden (allgemeine, versteckte und administrative Freigaben). Mittels des Menüs „Computer → Freigegebene Verzeichnisse“ steht ein Verwaltungstool für die Freigaben zur Verfügung.

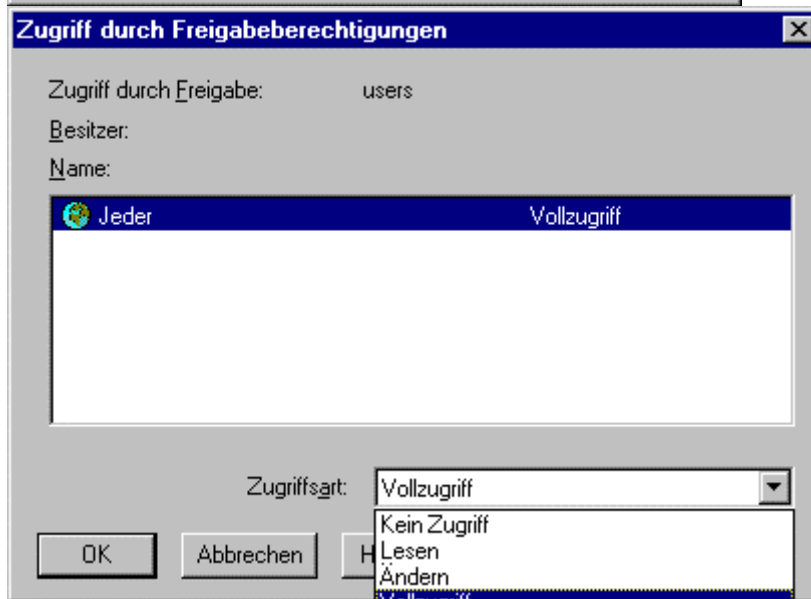
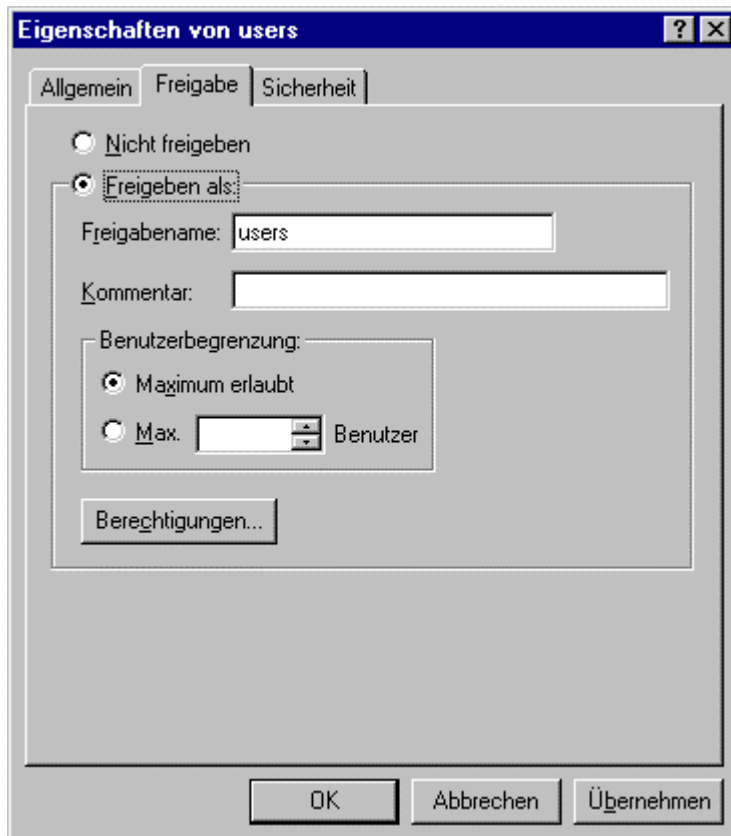


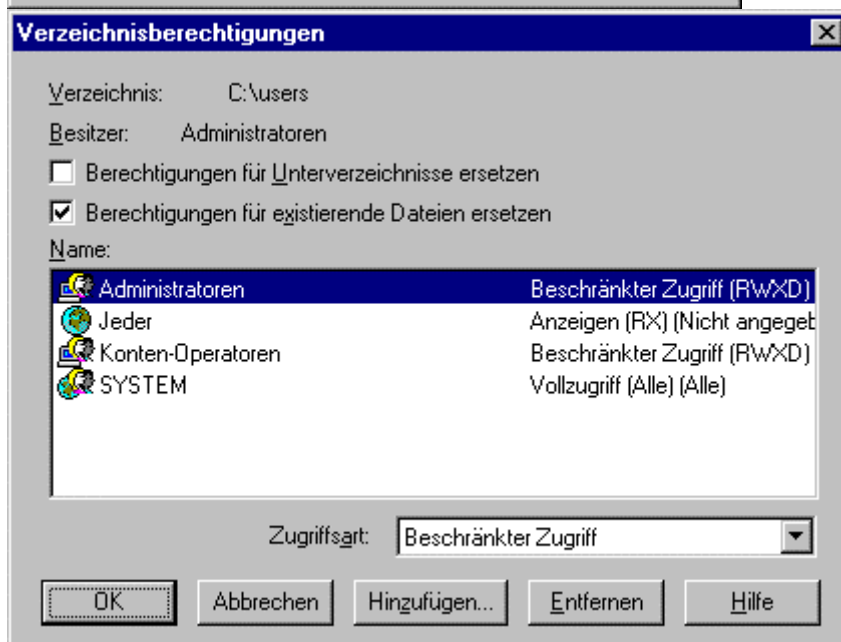


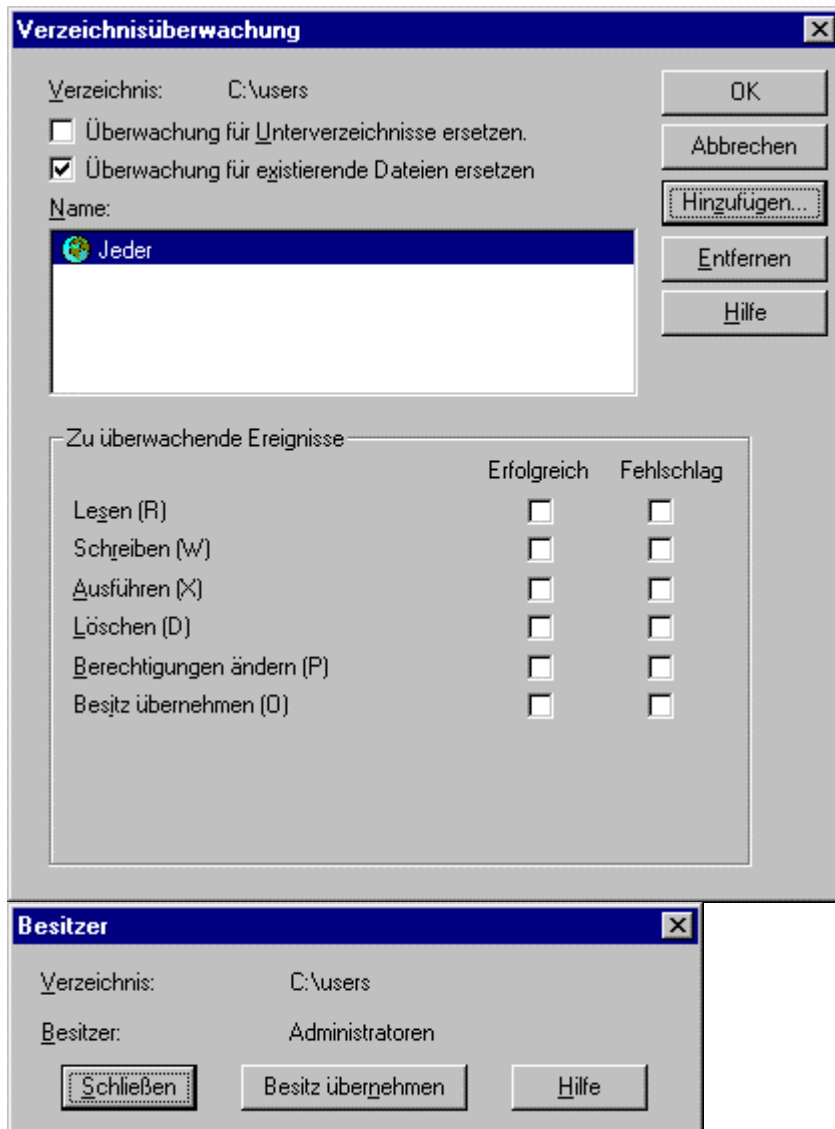
## 7.4.2. Windows NT-Explorer

Mit „START → Programme → Windows NT-Explorer“ wird der Explorer gestartet der über das Eigenschaftsmenü („Datei → Eigenschaften“ oder rechte Maustaste → Eigenschaften“) sowohl die Verwaltung der Freigabe des angewählten Verzeichnisses als auch die NTFS-Sicherheit ermöglicht:









### 7.4.3. Dateimanager

Mit Hilfe des Dateimanagers („START → Ausführen → WINFILE“) können ebenfalls Freigaben verwaltet werden, da der Dateimanager aber nur zur Erleichterung des Umstiegs auf die Version 4 vorhanden ist, wird hier nicht näher darauf eingegangen.

## 8. Sonstige wichtige Hilfsprogramme

### 8.1. Programme des Ordners Verwaltung

Die folgenden Programme sind i.a. mit der Standardinstallation eines Servers im Ordner Verwaltung zu finden. Die meisten davon immer, manche (z.B.: Migrationsprogramm für Netware) nur wenn gewisse Dienste oder Produkte mitinstalliert wurden. Der Start dieser Programme erfolgt mittels „START → Programme → Verwaltung → <Programm>“, wobei <Programm> durch das entsprechende Programm aus der folgenden Liste ersetzt wird.

#### 8.1.1. Bandsicherung

Mittels der Bandsicherung kann ein Backup auf unterstützte Bänder durchgeführt werden. Für Server ist dieses Programm allerdings wegen des fehlenden Komforts in der Automatisierung, der Verwaltung der gesicherten Ressourcen und in der Verwaltung der Bänder wenig geeignet und wird in der Praxis meist durch ein anderes Backupprodukt (z.B.: ARCserve von Cheyenne oder Backup Exec von Seagate) ersetzt.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\NTBACKUP.EXE)

#### 8.1.2. Benutzermanager

Der Benutzermanager dient der Verwaltung der Benutzer und Gruppen und wurde bereits im Punkt 5.4.1. ausführlich besprochen.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\USRMGR.EXE)

#### 8.1.3. Ereignisanzeige

Die Ereignisanzeige zeigt die Liste aller im System aufgetretenen und zu protokollierenden Ereignisse (Fehler beim Starten des Systems; Fehler in der Hardware, die nicht zum Ausfall des Systems führen; vom Administrator festgelegte Ereignisse lt. Überwachungsrichtlinien, ...). Diese können auch mittels der Ereignisanzeige in eine Datei zur Archivierung ausgelagert bzw. gelöscht werden.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\EVENTVWR.EXE)

#### 8.1.4. Festplattenmanager

Mit dem Festplattenmanager werden die Festplatten verwaltet, d.h. mit seiner Hilfe können Partitionen eingerichtet, kontrolliert und gelöscht werden: ferner ist die Einrichtung von Datenträgersätzen (mehrere freie Bereiche auf einen oder mehreren Datenträgern) möglich.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\WINDISK.EXE)

### **8.1.5. Lizenzmanager**

Mit dem Lizenzmanager werden die Lizenzen der installierten Softwareprodukte verwaltet, z.B. auch die Clientlizenzen für den Server selbst. Dabei werden zwei Lizenzierungsarten unterschieden, die „Pro Server“- und die „Pro Arbeitsplatz“-Lizenzierung. Bei der Variante „Pro Server“ sind die Lizenzen an den Server gebunden und erlauben der lizenzierten Zahl von Clients den Zugriff auf den Server (vergleichbar mit der Lizenzierung eines Novell-Netware-Servers); bei der Variante „Pro Arbeitsplatz“ sind die Lizenzen an den Client gebunden, der dadurch auch auf andere als seinen Standardserver zugreifen kann.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\LLSMGR.EXE)

### **8.1.6. Migrationsprogramm für Netware**

Mit dem Migrationsprogramm für Netware können Netwareserver auf NT übertragen werden, das ist bei einem vollständigen Umstieg eines bestehenden Netware-Netzes auf Windows NT sinnvoll. Dabei werden alle Benutzerinformationen und Dateien, soweit möglich, automatisch von einem bestehenden Netwareserver auf den Windows NT-Server übertragen. Zu beachten ist dabei, daß das Sicherheitssystem der Netware eine Übertragung der Paßwörter unmöglich macht und daher bei der Migration auch Vorkehrungen für die Kennwörter zu treffen sind. Die Verzeichnisse SYS:ETC, SYS:LOGIN und SYS:SYSTEM werden nicht übertragen, da hier üblicherweise nur Netware-spezifische Dateien gespeichert sind.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\NWCONV.EXE)

### **8.1.7. Netzwerk-Client-Manager**

Mit dem Netzwerk-Client-Manager wird der Administrator bei der Installation der Clients unterstützt. Hier können sowohl Startdisketten für die Clientinstallation als auch vollständige Sätze für die Installation der Clientsoftware erstellt werden, als auch die Vorbereitungen für die Installation der Clients über das Netz getroffen werden.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\NCADMIN.EXE)

### **8.1.8. RAS-Verwaltung**

Mit der RAS-(Remote Access Service)-Verwaltung wird der Zugriff über Modems administriert. Dabei können bestehende Verbindungen angezeigt und verwaltet werden (Menü: Server), die Zugriffsberechtigungen über Modem für die Benutzer eingestellt werden (Menü: Benutzer) als auch einige Optionen eingestellt werden.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\RASADMIN.EXE)

### **8.1.9. Server Manager**

Mit dem Server Manager werden wichtige Eigenschaften des Servers verwaltet. Im Menü Computer → Eigenschaften können Informationen über die angemeldeten Benutzer, die aktuellen Freigaben, die verwendeten Ressourcen, die Replikationseinstellungen und die Warnungen angesehen und verwaltet werden (siehe auch Punkt 7.4.1.). Ferner können noch Eigenschaften der Domäne verwaltet (z.B.: Umstufen eines BDC zu einem PDC, ...) und Nachrichten versendet werden.  
(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\SVRMGR.EXE)

### **8.1.10. Systemmonitor**

Mit dem Systemmonitor kann die Performance eines Windows NT-Systems überwacht werden. Dieses Programm ist kein spezieller Serverdienst, sondern auch auf der Workstation sinnvoll und verfügbar.  
(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\PERFMON.EXE)

### **8.1.11. Systemrichtlinieneditor**

Mit dem Systemrichtlinieneditor werden allgemeine Richtlinien vorgegeben, die dann beim Anmelden eines Benutzers in die Registry übernommen werden. Diese Aufgabe ist dem fortgeschrittenen Verwalter vorbehalten und nicht Thema dieses Skriptums.  
(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\POLEDIT.EXE)

### **8.1.12. Verwaltungs-Assistenten**

Mittels der Verwaltungsassistenten soll die Administration eines Windows NT Server vereinfacht werden, einen Überblick über die verfügbaren Assistenten ist im Punkt 5.4.2. dargestellt. Ob diese Assistenten für den Anwender eine Vereinfachung darstellen, muß er selbst beurteilen.  
(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\WIZMGR.EXE)

### **8.1.13. Windows NT-Diagnose**

Mit der Windows NT-Diagnose können die wichtigsten Parameter abgefragt werden, insbesondere im Falle von Problemen können hier wichtige Einstellungen und Systemzustände dargestellt werden. Dieser Dienst ist wieder nicht speziell für die Serverversion von Interesse, sondern generell für jedes NT-System.

(Datei, die dabei aufgerufen wird: %SYSTEMROOT%\SYSTEM32\WINMSD.EXE)

## **8.2. Sonstige Programme**

Diese Programme sind üblicherweise nicht direkt über einen Eintrag in der Taskleiste zu erreichen, sondern müssen über den Explorer oder „START → Ausführen → <Programmname>“ zur Ausführung gebracht werden.

### **8.2.1. REGEDT32**

Auf den Registrierungseditor wurde schon im Punkt 6.1.2. eingegangen, er ist hier nur zur Vollständigkeit nochmals angeführt.

### **8.2.2. RDISK**

RDISK ist ein Programm zur Sicherung der Registrierungsdatenbank, das mittels der Schaltfläche „Aktualisieren“ die aktuelle Registrierungsdatenbank (%SYSTEMROOT%\CONFIG) in das Verzeichnis %SYSTEMROOT%\REPAIR kopiert (mit dem Switch /S auch die Benutzerkonten). Mit der Schaltfläche „Erstellen“ wird diese Information (aus %SYSTEMROOT%\REPAIR) auf eine Notfalldiskette kopiert, die für Reparaturen bei Problemen mit dem System verwendet werden kann.

### **8.2.3. CONVERT**

Mit diesem Hilfsprogramm können bestehende FAT- oder HPFS-Partitionen in NTFS-Partitionen umgewandelt werden. Die Syntax lautet:

```
CONVERT z: /FS:NTFS [/V]
```

wobei z das zu konvertierende Laufwerk ist. Die Option /V bewirkt mehr Informationen während der Umwandlung.

## **8.3. Zusatzprogramme**

### **8.3.1. SQL-Server (Microsoft)**

Dieses Paket stellt einen relationalen Datenbankserver mit der Standardabfragesprache SQL (Structured Query Language) für Windows NT Server dar .

### **8.3.2. Exchange (Microsoft)**

Exchange stellt die Groupware-Software von Microsoft unter Windows NT dar. Es beinhaltet e-Mail, Terminplanung für Gruppen, die Verwaltung öffentlicher Verzeichnisse, „Schwarze Bretter“ und stellt die Basis für Groupware-Applikation dar. Die Standards X.400 (Mail) und X.500 (Verzeichnisdienste) werden unterstützt.

### **8.3.3. Systems Management Server SMS (Microsoft)**

Mit dem Systems Management Server (SMS) soll die Verwaltung einer größeren Zahl von Clients im Netz vereinfacht werden, dazu werden die Funktionen Inventarisierung, Softwareverteilung, Netzwerkanalyse, Fernsteuerung, Fernkonfiguration und Netzwerküberwachung unterstützt.

### **8.3.4. SNA-Server (Microsoft)**

Der SNA-Server stellt ein Gateway zwischen den Clients des Windows NT Servers und der 3270- (Mainframe)- bzw. 5250-(AS/400)-Welt dar, der die notwendigen Protokollkonversionen vornimmt.

### **8.3.5. Notes/Domino (Lotus/IBM)**

Lotus Notes stellt die bekannteste Groupware Software dar und steht unter Windows NT in direkter Konkurrenz zu Exchange. Da Notes länger am Markt ist und mehr Client- bzw. Servervarianten unterstützt, ist es in vielen Fällen noch immer erste Wahl.

### **8.3.6. Oracle Workgroup Server (Oracle)**

Oracle als Datenbankanbieter unterstützt ebenfalls die Plattform Windows NT, d.h. ein Windows NT Server wird mit der Zusatzsoftware zum Oracle Datenbankserver. Die Plattformunabhängigkeit von Oracle und die große Zahl von Anwendungen auf der Basis dieses Datenbanksystems stellt für viele Anwender den Einsatz von Oracle im Gegensatz zum SQL-Server außer Frage.

### **8.3.7. Informix**

Auch Informix hat sein Datenbankprodukt auf die Plattform Windows NT portiert, hier ist allerdings die Einschränkung auf das TCP/IP-Protokoll zu beachten.

### **8.3.8. ARCserve (Cheyenne)**

Ein Backupprogramm, das nicht mehr vorgestellt werden muß, da es für verschiedenste Plattformen schon vor NT am Markt war und auch heute unter den verschiedensten Plattformen (Win 3.x, Win 95, Win NT, Netware, ...) zum Einsatz kommt.

### **8.3.9. Diskkeeper**

Da Windows NT kein Defragmentierungstool beinhaltet, allerdings auch NTFS-Partitionen unter Defragmentierung leiden, sei hier auch ein Produkt für diese Aufgabe erwähnt: Diskkeeper defragmentiert (automatisch oder manuell gestartet) die NTFS-Partitionen, um so die Performance des Systems zu verbessern.

## 9. Connectivity

Nachdem Windows NT erst sehr spät in den Netzwerkmarkt eingedrungen ist, muß in vielen Firmen das Zusammenspiel mit schon vorhandenen Netzwerkstrukturen gesichert sein, insbesondere die Kooperation mit dem Marktführer Netware von Novell in vorhandenen Netzen stellt für die Netzwerkadministratoren einen wichtigen Punkt dar. Daneben muß aber auch die Kooperation mit UNIX-basierenden Netzen gegeben sein, bzw. das Zusammenspiel mit anderen Systemen im Netz, wie z.B.: IBM-Mainframes (3270-Welt), AS/400 und Apples Mac-Systemen, gesichert sein. Selbstverständlich sollten auch Tools zur Umstellung vorhandener Netze auf Windows NT zur Verfügung stehen, damit die einmal geleistete Arbeit (Einrichten der Benutzer, Verzeichnisse, ...) im bisherigen Netz nicht wiederholt werden muß. In heterogenen Netzen, vor allem ab einer gewissen Größe (z.B.: mehrere Standorte, ca. 1000 Benutzer, ...), muß auch die einfache Integration in die Verwaltungsstrukturen (Verzeichnisdienste, Managementsysteme, ...) gegeben sein, um die Kosten für den Betrieb des Netzes nicht unnötig zu erhöhen.

### 9.1. Netware-Connectivity

Sowohl Microsoft als auch Novell haben einige Produkte zur Verfügung, um die Koexistenz von Netware- und Windows NT-Netzen für den Anwender zu vereinfachen. An dieser Stelle soll nur ein Überblick über die Produkte von Microsoft für diesen Einsatzbereich dargestellt werden:

Client-Service für Netware	NT-Systeme können damit als Clients in Netwarenetze integriert werden.
Gateway-Service für Netware	Die Ressourcen eines Netwarenetzes werden den Clients des NT-Netzes über den NT-Server zur Verfügung gestellt, d.h. für die Clients des NT-Netzes sind diese Services auch ohne direkten Zugriff auf das Netwarenetz zugänglich.
Services für Netware (Zusatzprodukt)	Windows NT emuliert einen Netware 3.x Server und ist damit auch für Netwareclients verwendbar.
Migrationsprogramm für Netware	Die Daten und Accountinformationen werden damit von einem Netwareserver auf einen Windows NT Server übertragen.

### 9.2. Unix-Connectivity

Durch die Unterstützung des TCP/IP-Protokolls und verschiedener Standardutilities (ftp, telnet, lpr, ...) ist die Integration in die UNIX-Welt grundsätzlich möglich, allerdings auch auf diese Utilities beschränkt. Für eine vollständige Integration eines Windows-NT Servers mittels X-Windows oder NFS ist man auf Zusatzprodukte von Drittherstellern angewiesen, da Windows NT keine Unterstützung für diese Netzwerkdienste anbietet.

### **9.3. OS/2-Connectivity**

Trotz gemeinsamen Ursprungs ist die Integration von OS/2 und Windows NT kaum möglich. Durch die Verwendung des SMB-Protokolls ist zwar der Zugriff von OS/2-Clients auf Windows NT-Server und umgekehrt möglich, allerdings ist eine Abstimmung der Benutzerkonten oder eine Migration von OS/2-Server auf Windows NT-Server nicht möglich.

### **9.4. Apple-Connectivity**

Mit den Services für Macintosh unterstützt Windows NT zwar sowohl Apple-Talk als auch Apple-Clients, allerdings ist der Zugriff von Apple-Clients nur auf speziell als MACFILE festgelegte Bereiche des Server möglich.

### **9.5. NT und Verzeichnisdienste**

Verzeichnisdienste für die Netzwerkverwaltung werden derzeit nicht unterstützt, daher ist Windows NT speziell in großen Netzen nur schwer zu administrieren. Die nächste Version von Windows NT soll um Verzeichnisdienste („Active Directories“) ergänzt werden, so daß mittelfristig auch das Domänenkonzept abgelöst wird.