Netzwerkgrundlagen 6
1.1 Netztypen 6
1.1.1 Client - Server - Netze 6
1.1.2 Peer - to - Peer 8
1.1.3 Domänen-Netze 9
1.2 Topologien 9
1.2.1 Stern 9
1.2.2 Bus 10
1.2.3 Ring 10
1.3 Protokolle und Normen 11
1.3.1 Das OSI-Referenzmodell 11
1.3.2 IEEE und FDDI 12
1.3.2.1 IEEE 802.2, LLC (Logical Link Control) 12
1.3.2.2 IEEE 802.3, Ethernet, 10Base5, 10 Base 2 12
1.3.2.3 IEEE 802.5, Token Ring 12
1.3.2.4 FDDI 12
1.3.3 Internationale Standards 12
1.3.3.1 DLC 13
1.3.3.2 NetBEUI 13
1.3.3.3 NWLink IPX/SPX 13
1.3.3.4 TCP/IP 13
1.3.3.5 Klasse A 14
1.3.3.6 Klasse B 14
1.3.3.7 Klasse C 14
1.3.3.8 Subnetze 15
1.4 Strukturelemente 16
1.4.1 Repeater 16
1.4.2 Bridge 16
1.4.3 Router 17
1.4.4 Gateway 17

Fragen zur Erschließung des Themas 18
1.5 1.6 TCP/IP-Namensdienste 19
1.5.1.1 Broadcast: 20
1.5.1.2 HOSTS-Dateien 20
1.6 Das Konzept von DHCP 21
1.7 Installation und Konfiguration von DHCP 22
1.7.1.1 IPCONFIG 23
1.7.2 Namensauswertung 24
1.7.2.1 Die Dateien Hosts und LMHosts 24
1.7.3 Funktionsweise von WINS 25
1.7.3.1 Anforderungen für WINS 25
1.7.4 Der Domain Name Service 25

1.7.4.1 Einen DNS-Client einrichten 26
1.7.5 Einrichten eines DNS-Servers 26

2 Windows NT Server 4.0 28
2.1 Allgemeine Einführung 28
2.1.1 Abgrenzung von Windows NT Workstation und Server 28
2.2 Architektur und Konzepte 29
2.2.1 HAL (Hardware Abstraction Layer) 29
2.2.2 Windows NT-Executive 30
2.2.3 Die Subsysteme 32
2.2.3.1 CSR-Subsystern 32
2.2.3.2 VDM, WOW 32
2.2.3.3 Sicherheitssubsystem 32
2.2.3.4 Die Speicherverwaltung 32
2.2.3.5 Dateisysteme in Windows NT 32
2.2.4 Anmerkung zu Windows NT 3.51 / 4.0 33

3 Die Struktur eines Windows NT-Netzes 34
3.1 Was ist eine Arbeitsgruppe? 34
3.2 Was ist eine Domäne? 34
3.2.1 Aufbau einer Domäne 34
3.2.2 Vertrauensstellungen und Domänenmodelle 35
3.2.1.1 Single - Domain - Modell 36
3.2.1.2 Master - Domain - Modell 36
3.2.1.3 Multiple - Master - Domain - Modell 36
Complete - Trust - Domain - Modell 37
3.2.2 Einrichten von Vertrauensstellungen 38
3.3 Benutzer-Konten 39
3.4 Benutzer-Gruppen 39

4 Die Installation 33
4.1 Installationsvoraussetzungen 33
4.1.1 Kompatible Hardware 33
4.1.2 Ausreichende Hardware 33
4.2 Vorbereitung der Installation 34
4.2.1.1 1. Informationen über die Hardware 34
4.2.1.2 2. Beschaffung von Treibern 34
4.2.1.3 3. Bereitstellung der Installationsmittel 34
4.2.1.4 4. Einstellungen im BIOS 34
4.2.1.5 5. Organisatorische Vorüberlegungen 34
4.2.1.6 6. Vorbereitung der Festplatte 34
4.3 Das Kommando WINNT 35
4.4 Die vollständige Installation über Disketten, CD oder Netzwerk 35
4.5 Der Ablauf der Installation 36

4.5.1 Der Ablauf der Installation am BWV Ahaus 36
4.5.2 INITIALISIEREN der Installation 37
4.5.2.1 INSTALLATION DES NETZWERKES 38
4.5.2.2 Konfigurieren des Arbeitsgruppen- oder Domänennamens 38
4.5.2.3 Computer zur Domäne hinzufügen 39
4.6 Unattend Installation einer Workstation (halbautomatische Installation) 39
4.7 Erstellen und Verwenden der Notfalldiskette 42
4.8 Dual-/ Triple- oder Quadro- Boot mit DOS/Win3.x. Win9x, WinNT, OS/2 und/oder Linux 42
4.8.1 Vorbemerkungen: 42
4.8.1.1 DOS 43
4.8.1.2 Win9x 43
4.8.1.3 WinNT 43
4.8.1.4 OS/2 43
4.8.1.5 SuSE-Linux 44
4.8.2 Realisierung von DUAL- oder TRIPLE- BOOT 44
4.8.2.1 Windows NT, Windows 9x und MS-DOS 44
4.8.2.2 Windows 9x, Windows-NT und Linux auf einem Rechner 44
5 Der Benutzer 46
5.1 NT Workstations als Teil einer Domäne 46
5.1.1 Mitglied einer Domäne werden 46
5.1.1.1 Die Bedeutung des Security ldentifier 46
5.1.2 Das Anmeldeverfahren 47
5.2 Benutzerverwaltung 48
5.2.1.1 Definition von Benutzern 48
5.2.1.2 Vordefinierte Benutzerkonten 48
5.2.1.3 Benutzergruppen 48
5.2.1.4 Lokale Gruppen 49
5.2.1.5 Globale Gruppen 49
5.2.1.6 Vordefinierte Benutzergruppen der Domäne 49
5.2.1.7 Die Gruppe *Jeder* 49
5.2.1.8 Vordefinierte lokale Gruppen auf dem Domänen-Controllern 49
5.2.2 Anlegen neuer Benutzer 50
5.2.3 Anlegen neuer Benutzer über die Befehlszeile 52
5.2.4 Übungs- und Verständnisfragen 54
5.3 Die User-Gruppen 55
5.3.1 Die Bedeutung von User-Gruppen 55
5.3.2 Das Anlegen von User-Gruppen 56
5.3.2.1 Globale Gruppen 56
5.3.2.2 Lokale Gruppen 57
5.3.2.3 Vordefinierte Gruppenberechtigungen (Server) 57
5.3.2.4 Vordefinierte Gruppenberechtigungen (Workstation) 59
5.3.2.5 Besonderheiten 61

5.3.3 Workstationänderungen bei Hinzufügen zur Domäne 62
5.3.3.1 Sonderfälle 62

6 Werkzeuge zur Leistungsüberwachung und -optimierung 64

6.1 Der Systemmonitor 64
6.1.1 Daten zur Systemleistung anzeigen 64
6.1.2 Leistungsdaten sammeln 65

6.2 CPU-Ressourcen verwalten 65
6.2.1 Windows NT-Prozeßplanung 65
6.2.2 Gegen knappe CPU-Ressourcen vorgehen 66
Der Start-Befehl 67

6.3 Verwalten der Speicherverwendung 67
6.3.1 Die Speicherverwaltung unter Windows NT 67
6.3.2 Die Speicherverwendung beobachten 68

6.4 Optimieren der Festplattenleistung 69

6.5 Netzwerkleistung 70

Fragen zum allgemeinen Verständnis 72
6.1.2.1 Antwort auf: 73

7 RAID-Systeme 74

7.1 Hardware- und Software-Implementierungen von RAID 74
7.1.1 Hardware-Implementierungen von RAID 74
7.1.2 Software-Implementierungen von RAID 74
7.1.2.1 RAID 1: Spiegelsätze 74
7.1.2.2 Festplattenduplizierung 75
7.1.2.3 RAID5: Stripe Sets mit Parität 75

7.2 Implementieren von RAID 1 und RAID 5 76
7.2.1 Beim Erstellen und Löschen eines Stripe Sets mit Parität zu beachtende Punkte 76

7.3 Wiederherstellen von Daten nach einem Festplattenausfall 76
7.3.1 Regenerieren eines Stripe Sets mit Parität 77
7.3.2 Wiederherstellen von Daten nach einem Spiegelsatzausfall 77

7.4 Erstellen einer Startdiskette mit Fehlertoleranz 78

8 Die Windows NT-Registrierung 79

8.1 Die Registrierung 79

8.2 Das Anzeigen der Registrierung 79

8.3 Verwenden der Registrierung durch die Windows NT-Komponenten 80

8.4 Die Struktur der Registrierung 81

9 Mikrocontroller und Prozessortechnik 83

9.1 Interrupt-Strukturen 83
9.1.1 Interrupts und ihre Funktionen 83
9.1.2 Detaillierter Ablauf einer Interruptverarbeitung 83

9.1.3 Multiple Interrupts 84
9.1.4 Verteilung der Interrupts bei AT-kompatiblen PC‘s 85

1 Netzwerkgrundlagen

Ein Rechnernetz besteht aus einer Anzahl von Rechnern, die über ein Medium (Kabel, Funk- oder Infrarot-Verbindung) miteinander verbunden sind. Dazu gehören auch Peripherie- und Kommunikationsgeräte. Ein solches Netz kann ausgesprochen komplex sein.

Das Netzwerk dient der Zusammenarbeit, dem Datenaustausch und der gemeinsamen Nutzung von Daten und teuren Peripheriegeräten. Wenn heute von Netzen die Rede ist, wird damit meist ein PC-Netz gemeint.

Ein Netzwerk kann gegenüber einem System einzelner Rechner folgende Vorteile haben:

- Zugriff auf gemeinsame Daten
- verteilte Datenhaltung
- verteilte Verarbeitung von Daten
- Erweiterung der Funktionalität des Einzelplatzes und Kosteneinsparung durch gemeinsame Nutzung von Peripheriegeräten wie Drucker, Fax etc.
- Gemeinsame Nutzung von Kommunikationssystemen (Mail, Terminplaner etc.)
- Lastverteilung; einige preiswerte Rechner können teure Hochleistungsmaschinen ersetzen
- Sicherheitsgewinn durch z.B. zentrale Datensicherung
- Verringerung des administrativen Aufwands

In Abhängigkeit der Räumlichen Ausdehnung des Netzwerkes wird eine grobe Unterteilung vorgenommen, wobei die Grenzen fließend sind. Es gibt lokale Netze (LAN = Local Area Network) und Weitverkehrsnetze (WAN = Wide Area Network). Dazu kommt noch die Bezeichnung MAN (Metropolitan Area Network)

Ein LAN hat eine begrenzte Ausdehnung, typischerweise ist es auf ein Gebäude oder einen Gebäudekomplex beschränkt.

Sobald ein LAN über Grundstücksgrenzen hinweg verbunden wird, ist es bereits im Prinzip ein WAN. Die Ausdehnung eines WAN's ist nicht beschränkt. So gibt es weitumspannende WAN'S, wie sie etwa die großen Firmen der Computerindustrie aufgebaut haben.

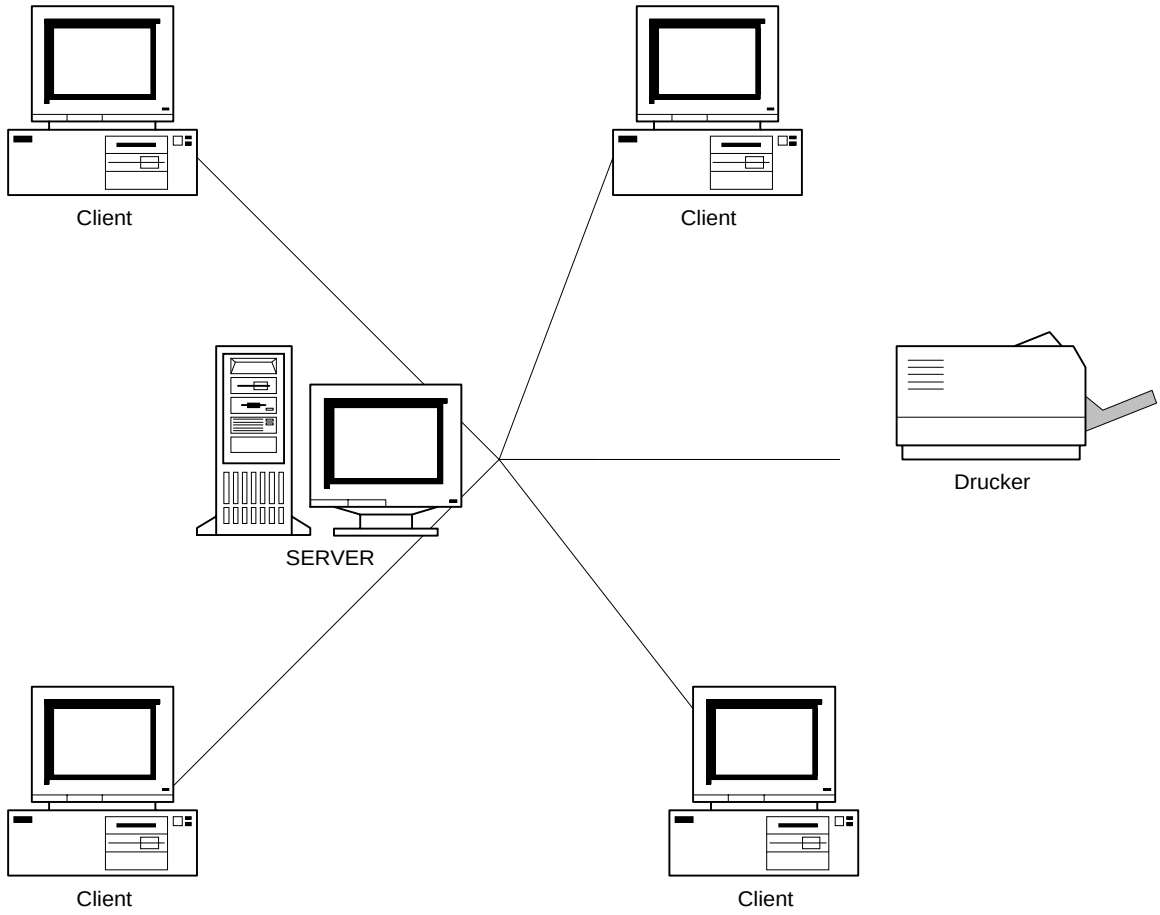
Ein MAN ist eine besondere Form des WAN und in der Ausdehnung etwa auf eine Großstadt beschränkt. Ein Beispiel wäre ein Netzwerk, das von einem Unternehmen mit mehreren Niederlassungen und Geschäftsstellen etwa im Raum Düsseldorf unterhalten wird.

1.1 Netztypen

1.1.1 Client - Server - Netze

Als Server dient im einfachsten Falle ein einzelner (Groß-)Rechner. Dieser verwaltet die Netzressourcen und stellt sie den Clients (Arbeitsstationen) zur Verfügung. Die Daten werden meistens in Form von Datenbanken auf dem Server abgelegt und den Clients zur Bearbeitung auf den Workstations übermittelt. Der Server regelt die gemeinsame Nutzung von Daten und ggf. auch Programmen, auf die die Clients zugreifen. Charakteristisch für Client-Server-Netze ist die Ausrichtung auf einen File-Server. Auf dieser zentralen Maschine sind alle wesentlichen Dienste des Netzes vereinigt. Man findet auf diesem File-Server:

- Betriebssystem des File-Servers
- Datenbank mit den Benutzerinformationen
- Rechtestruktur
- Daten (File-Services)
- Druckerwarteschlangen (Print-Services)
- Weitere Dienste wie Remote-Access, SQL-DBMS, Mail



Vorteile:

- Gut für kleine Netze bis zu 100 User
- einfache Installation
- wenig Datenverkehr im Netz

Nachteile:

- Für jeden weiteren Server müssen alle Accounts (User, Gruppen) redundant erstellt werden
- Nicht beliebig erweiterbar
- Bei Ausfall des Servers keine Netzfunktionalität

Wenn mehrere Server in einem Netz installiert sind, gibt es in der Regel für folgende Aufgabenbereiche dedizierte Server:

- Fileserver
- Printserver
- Kommunikationsserver

Was geschieht nun, wenn ein Client einen Dienst des Servers nutzen will, z. B. ein Textverarbeitungsprogramm? Auf die Anforderung des Clients, das Textverarbeitungsprogramm zu nutzen, schickt der Server alle notwendigen Programme bzw. Programmteile zum Client. Diese werden in den Arbeitsspeicher des Clients geladen und stehen dann lokal zur Ausführung zur Verfügung. Dies kann überprüft werden, wenn ein spezielles Programm, wie z. 8. InfoSpy, gestartet wird. Dieses Windowsprogramm zeigt unter anderem an, welche Module auf welchem Rechner geladen sind. Wenn, wie oben erwähnt, ein Textverarbeitungsprogramm geladen worden ist, wird auf dem Client das Textverarbeitungsmodul angezeigt, nicht aber auf dem Server. Im Falle eines Client-Server-Systems müssen jedoch nicht unbedingt alle Programme auf dem Server installiert werden. Es ist ohne weiteres möglich, Windows lokal zu installieren und die Anwendungsprogramme

auf dem Server. Bei großen Netzen wird man schon aus Gründen der Programmpflege die meisten Programme auf dem Server installieren.

Gängige Client-Server-Betriebssysteme sind OS/" LAN Server von IBM, Windows NT von Microsoft und Novell Netware.

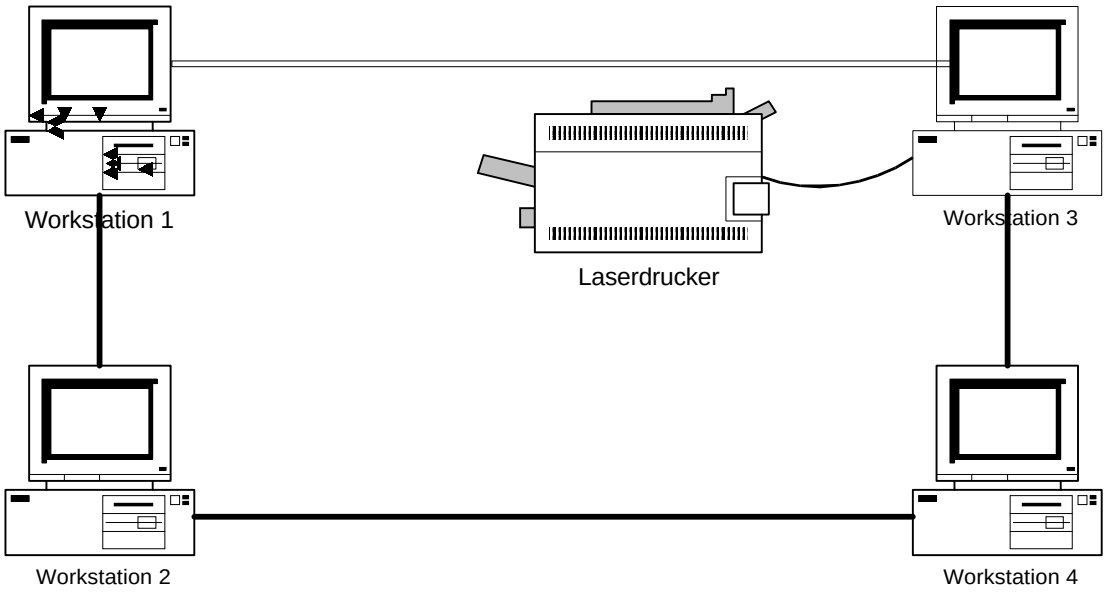
1.1.2 Peer - to - Peer

Bei einer Peer-to-Peer-Vernetzung ist jeder Rechner, der ans Netz angeschlossen ist und über Plattenspeicher verfügt, ein potentieller Server. Jeder Rechner in einem Peer-to-Peer-Netzwerk kann seine Ressourcen (Festplattenplatz, Anwenderprogramme, an ihn angeschlossene Drucker, CDs) zur Nutzung durch andere am Netzwerk angeschlossene Stationen freigeben. Eine Station, die freigegebene Ressourcen auf einem anderen Rechner anfordert, ist in diesem Fall ein Client. Umgekehrt fungiert sie als Server, wenn eine andere Station bei ihr Ressourcen anfordert. Bei modernen Peer-to-Peer-Netzen ist wie bei Client-Server-Systemen auch eine abgestufte Freigabe von Ressourcen (abhängig vom Benutzernamen, Passwort etc.) möglich. Peer-to-Peer-Vernetzung ist besonders für kleine Netze interessant, da dann die Ressourcen auf verschiedene Rechner verteilt werden können und kein Hochleistungsrechner erforderlich ist. Auf der anderen Seite sollte nicht verkannt werden, dass ressourcenintensive Anwendungen/Abfragen von Clients die "normale" Arbeit an dieser Station negativ beeinflussen können.

Da typischerweise in einem Peer-to-Peer-Netz die einzelnen Stationen zum ganz normalen Arbeiten genutzt werden, ist Vorsicht geboten beim Abschalten dieser Stationen. Es könnte ja noch jemand anderes mit dem eigenen Rechner verbunden sein. Dies ist bei Client-Server-Systemen unkritisch, da der Server in aller Regel im Dauerbetrieb läuft oder zumindest während der Arbeitszeit voll funktionsfähig ist. Auch der heute so beliebte Abschaltmodus von Festplatten ist bei Peer-to-Peer-Netzen nicht ganz unkritisch. Manche Netzwerkbetriebssysteme für Peer-to-Peer-Netze haben damit Probleme.

Im Gegensatz zu einem Client-Server-System werden die Daten direkt zwischen den einzelnen Arbeitsstationen ausgetauscht. So holt sich beispielsweise Arbeitsstation 1 eine Datei direkt von der Arbeitsstation 3. In einem Client-Server-System würde die Arbeitsstation 1 die Datei in einem bestimmten Dateibereich auf dem Server ablegen und die Arbeitsstation 3 könnte sich die Datei dann von dort abholen. Mit Groupware, z. B. Lotus Notes, können die Dateien natürlich auch direkt an den Empfänger gesandt werden. Trotzdem ist an der Aktion der Server beteiligt.

Heute sind oft beide Netzformen in einem Netz anzutreffen und in Abhängigkeit von der jeweiligen Anwendung zu entscheiden, ob es sich mehr um ein Peer-to-Peer oder ein Client-Server-Netzwerk handelt.



Ein Arbeitsplatz- kann also als Server und Client eingerichtet werden. Bei größeren Netzen (>10 Knoten) empfiehlt es sich, nicht alle Arbeitsplätze so einzurichten. Statt dessen sollten einzelne Stationen als dedizierte Server eingerichtet werden. In der Praxis bedeutet dies, dass so mit der Zeit ein Client-Server- Netzwerk mit bestimmten Arbeitsgruppen entsteht, die Peer-to-Peer-Funktionalität zusätzlich nutzen. Eine weitere Unterteilung in File-, Print- und Kommunikationsserver ist bei großen Netzen in aller Regel nicht nur sinnvoll, sondern unumgänglich.

Gängige Peer-to-Peer-Betriebssysteme sind

- Windows 3.11 für Workgroups, Windows 95 / 98
- Personal Netware von Novell

Vorteile:

- Nutzung aller Ressourcen im Netz (Drucker, lokale Festplatten)
- Maximale Flexibilität, geringer administrativer Aufwand in kleinen Netzen
- Bei Ausfall eine Komponente entsteht keine Beeinträchtigung des Gesamtsystems, bis auf den eventuellen Verlust von Ressourcen.

Nachteile:

- Hoher Netzverkehr
- Geringe Datensicherheit
- Keine zentrale Kontrolle
- Schlechte Performanz bei hoher Anzahl von Benutzern

1.1.3 Domänen-Netze

Im Domänen-Konzept werden mehrere Server mit eigenständigen Aufgaben zu einer logischen Struktur, der Domäne, zusammengefaßt. Die physikalische Ordnung der Server in einem LAN ist davon unabhängig. Benutzer und Gruppen müssen nur einmal in der Domäne definiert werden.

Vorteile:

- Mehrere Server bei zentraler Administration
- optimale Lastverteilung
- Höhere Verfügbarkeit
- Leicht skalierbar
- Hardware passend zur Aufgabe wählbar
- Benutzer benötigen nur einen Account für alle Netzwerkressourcen.

Nachteile:

- Gute Planung vor der Installation ist zwingend notwendig
- Komplexer für den Administrator

Beispiele für diese Netze: LAN-MANAGER; WINDOWS-NT

1.2 Topologien

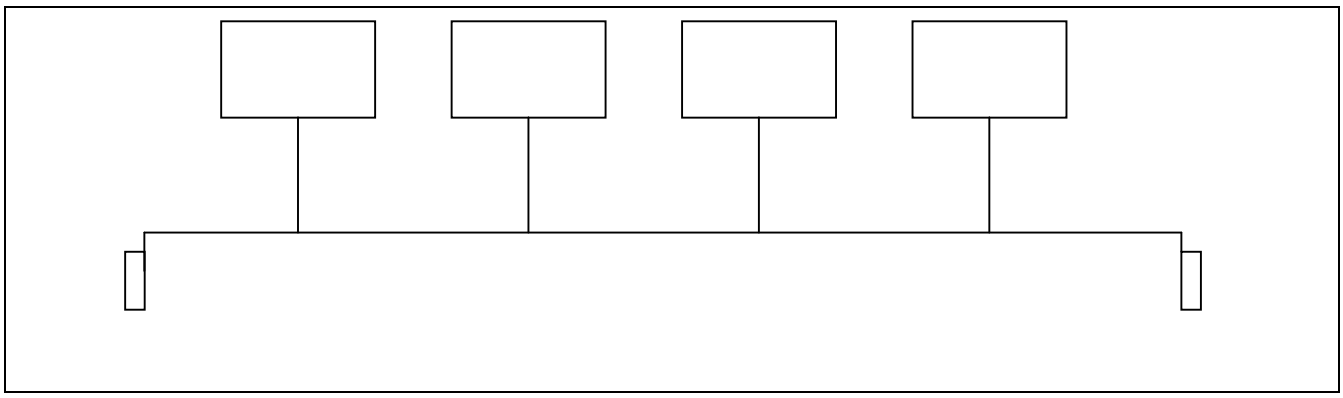
Unter einer Topologie wird ein bestimmter, physikalischer Aufbau von Kommunikationsverbindungen verstanden. Es gibt eine Vielzahl von Topologien und eine Vielzahl von Kombinationen der unterschiedlichsten Topologien. Die drei wichtigsten werden im folgenden vorgestellt. Meist gibt es, mindestens ursprünglich, eine direkte Zuordnung zwischen Topologie und einem bestimmten Netzwerktyp und Netzwerkprotokoll. Die Topologien haben zusammen mit den jeweils angewandten Zugangsverfahren typische Vor- und Nachteile.

1.2.1 Stern

In der Stern-Topologie werden alle Geräte Punkt - zu - Punkt mit einer zentralen Einheit verbunden. Die Sterntopologie ist leicht zu warten und flexibel aufzubauen, es müssen allerdings viele lange Kabel verlegt werden. Diese Einheit kann aus einem Konzentrator, Multiportrepeater, Switch oder Hub bestehen.

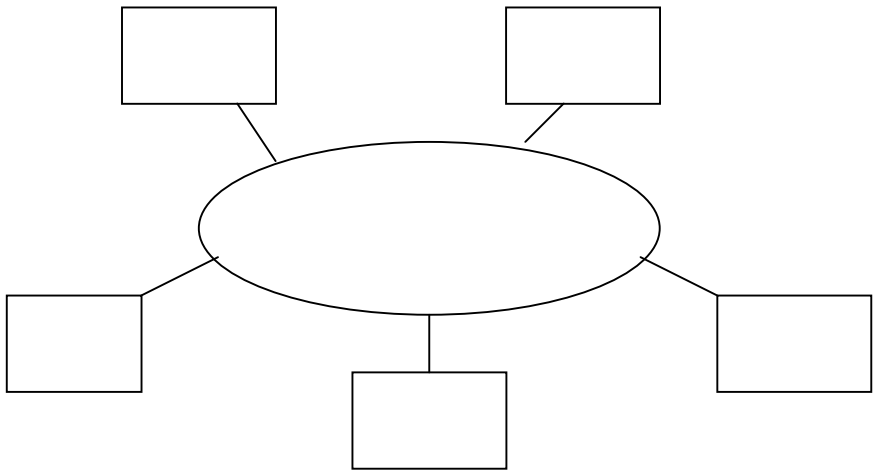
Ein **Hub** besteht aus mehreren (typ. ca. 8-10) Netzwerkein/Ausgängen und kann keine Datenverteilung vornehmen, so dass jedes Datenpaket alle angeschlossenen Stationen erreicht und von diesen verarbeitet bzw. verworfen werden muss. Der passive Hub dient nur der Verbindung und verstärkt das Signal nicht. Der aktive Hub ist wie ein passiver, verstärkt das Signal und benötigt eine zusätzliche Stromversorgung. Ein **Switch** kann eine Verteilung der Daten auf die verschiedenen Kabel oder Segmente entsprechend der Adressierung vornehmen und auch oft Funktionen für das Netzwerkmanagement anbieten. Die Sterntopologie ist leicht zu warten und flexibel aufzubauen, es müssen allerdings große Kabellängen und bei Ausfall eines Hub/Switch auch der Ausfall aller angeschlossenen Stationen in Kauf genommen werden.

1.2.2 Bus



Bei der Bustopologie wird ein lineares Übertragungsmedium (typ. BNC-Verkabelung mit Koaxialleitung) eingesetzt, an das alle Stationen direkt angeschlossen werden. Eine Terminierung des Mediums durch Abschlußwiderstände ist zwingend erforderlich um Signalreflektion zu verhindern. Diese Topologie ist diejenige mit der geringsten Kabellänge und den geringsten Kosten. Problematisch ist allerdings, dass ein Defekt (z.B. Massekontakt, Kabelbruch) den Bus komplett lahmlegt und so die Fehlersuche erschwert. Ethernet und Token-Bus sind typische Beispiele für Bus-Topologien.

1.2.3 Ring



Der Ring ist ein geschlossener Ring mit Verstärkerelementen oder Stationen. Diese Topologie ist an der Verkabelungstechnik nicht zu erkennen, die Stationen und Geräte im Netz bilden einen

logischen Ring. Das Signal im Medium läuft im geschlossenen Ring und wird von den angeschlossenen Stationen ”abgehört”. Bei den beiden Beispielen IBM TokenRing und FDDI (Fiber Distributed Data Interface) ist die Anschlußtechnik sternförmig. Die Ringtopologie hat durch die verwendeten Verteilsysteme eine gleich gute Wartbarkeit und Flexibilität wie die Sterntopologie.

1.3 Protokolle und Normen

Es gibt eine Vielzahl unterschiedliche Netzwerkprotokolle, die für verschiedene Einsatzbedingungen und Aufgaben entwickelt wurden. Alle Protokolle definieren einen bestimmten Aufbau von Datenpaketen (Frames), die für die kommunizierenden Stationen eine "Sprachbasis" darstellen. Die für die Protokolle definierten Datenpakete unterscheiden sich in der Gesamtlänge des Frames, in der Abfolge der mit Aufgaben belegten Abschnitte der Frames und in deren Länge (in Bits). Alle Frames enthalten Bereiche zur Adressierung, zur Kontrolle der Kommunikation, für die eigentliche Information und für Prüfsummen.

Einige Protokolle sind firmenspezifisch, haben sich aber als Quasi-Standards (Ethernet, SDLC, TokenRing) durchgesetzt, andere sind von nationalen oder internationalen Gremien standardisiert worden. Fast alle Protokolle lassen sich mit Hilfe des OSI-7-Bit-Schichtenmodells erklären oder sie lassen sich in ihrem Aufbau auf dieses Modell zurückführen.

1.3.1 Das OSI-Referenzmodell

1977 wurde von der International Organization for Standardisation (ISO) ein Komitee eingesetzt, das mit der Entwicklung von Datenkommunikationsstandards beauftragt wurde. Wesentliches Ziel sollte die universelle Kompatibilität der Kommunikationsprodukte verschiedenster Hersteller sein.

Das Ergebnis, das Open System Interconnection (OSI) Referenzmodell, bietet Richtlinien für die Funktion verschiedener Aufgaben in der Rechner - Rechner - Kommunikation. Das Problem der Kommunikation zwischen verschiedenen Computern wurde in Teilaufgaben untergliedert die sich 7 Schichten darstellen. Dabei übernimmt jede Schicht spezielle Aufgaben auf dem Weg der Daten von dem elektrischen Signal des Kabels bis zur geprüften Information, die an die Anwendung weitergegeben wird.

Schicht		Dienste / Interne Funktionen
7	Anwendung	Kommunikationsinterface zum Benutzer, Kommunikation zwischen Applikationen, Dateitransfer, Netzwerkmanagement etc.
6	Darstellung	Übersetzung der Bitinformationen in Zeichen, Ver- und Entschlüsselung, Kompression und Expansion
5	Kommunikationssteuerschicht	Kontrollmechanismen zur Kontrolle der Kommunikationsdialoge zwischen Applikationen, Berechtigungen, Problembehandlung von Fehlern auf den obersten Schichten, Wiederaufsetzpunkte
4	Transport	Überprüfung der korrekten Datenübertragung, Verbindungsauf- und – abbau, Kontrolle des Datenflusses
3	Netzschicht	Logische Adressierung im Netz ermöglicht die Verteilung von Datenpaketen im Netzwerk, Datenelementsynchronisation
2	Datensicherungsschicht	Anzeige von nicht behebbaren Fehlern, Flußregelung, Reihenfolgeerhaltung, Fehlerbehandlung, Verbindungsaufteilung
1	Physikalische Schicht	Bitübertragungsschicht; Anzeige von (z.B. Leitungs-)Defekten, Taktsynchronisation, mechanische und elektrische Beschreibung des Netzwerkmediums, Signalübertragung auf das Medium

1.3.2 IEEE und FDDI

Die für Ebene 1 und 2 des OSI-Referenzmodells definierten Normen des IEEE (Institute of Electrical and Electronic Engineers) definieren zusätzlich zum Protokoll auch die physikalischen und elektrischen Eigenschaften der Kabelsysteme und Anschlüsse sowie der Kodierung des Signals.

1.3.2.1 IEEE 802.2, LLC (Logical Link Control)

LLC ist in der oberen Hälfte der Data-Link-Schicht des OSI-Modells angesiedelt. Es hat die Aufgabe, der darüberliegenden Netzwerkschicht einen fehlerfreien Übertragungsweg darzustellen. IEEE 802.2 liegt oberhalb der im folgenden kurz aufgeführten Normen IEEE 802.3 - 802.6, deren Definition die physikalische Schicht und die untere Hälfte der Data-Link- Schicht umfaßt.

1.3.2.2 IEEE 802.3, Ethernet, 10Base5, 10 Base 2

Unterschiede zwischen diesen Protokollen bestehen für die physikalische Schicht in der Verwendung verschiedener Kabeltypen und Anschlüsse. Die Datenübertragungsrate ist 10 Mbit/s.

1.3.2.3 IEEE 802.5, Token Ring

Diese Netzwerke beinhalten eine begrenzte automatische Fehlerbehebung (in der Verteilertechnik). Die Topologie ist für TokenRing der Ring oder Bus, bei IEEE 802.5 ist sie nicht festgelegt. Die Datenübertragungsraten sind 16 oder 4 Mbit/s.

1.3.2.4 FDDI

Hierbei handelt es sich um einen ANSI-Standard für Highspeed-Netze mit Glasfaserkabeln. Die Datenübertragungsrate ist 100 Mbit/s. Auf dem Markt ist inzwischen auch FDDI auf Kupferkabeln zu akzeptablen Preisen zu bekommen.

Über diese heute am weitesten eingesetzten Protokolle hinaus, sind die neueren Entwicklungen im Bereich der Highspeed Netze für die Zukunft interessant. Es existieren zwei konkurrierende 100 Mbit Standards, Highspeed Ethernet und VG-Anylan, die f'ür hochbelastete Netze etwa im Bereich von Multimedia eingesetzt werden können. In Zukunft können auch Systemen die ATM (Asynchronous Transfer Mode) verwenden eine Highspeed-Alternative sein. ATM kann Datenraten bis in den Gigabit-Bereich anbieten.

1.3.3 Internationale Standards

Die beschriebenen Protokolle stellen eine definierte Funktionalität entsprechend den Ebenen 1 (physical) und 2 (Data Link) des OSI-Schichtenmodells zur Verfügung. Zur Kommunikation zwischen Rechnersystemen sind Funktionsbeschreibungen bis auf die Ebene des Betriebssystems oder der Schicht 7 (Applikation) notwendig. Von verschiedenen Firmen oder Organisationen wurden hierfür Protokollfamilien entwickelt. Beispiele sind Netbios NetBEUI (IBM und Microsoft), SNA (IBM), Apple Talk, IPX/SPX (Novell), sowie die Internetprotokolle TCP/IP oder NFS für den Unix-Bereich. Dies sind bis auf TCP/IP proprietäre Standards, die sich in einem bestimmten Marktsegrnent durchgesetzt haben und in der Funktionalität den OSI-Protokollen gegenübergestellt werden können.

Gegenüberstellung des OSI-Refernzrnodells und verbreiteter Protokollfarnilien:

7	**Anwendung**		FTP	NFS			
6	**Darstellung**		Telnet SMTP		SMB?		
5	**Sitzung**	O			NetBIOS (IBM/MS)	NetBEUI (MS)	
4	**Transport**	S	TCP				SPX/IPX(Novell)
3	**Netzwerk**	I	IP				
2	**Verbindung**		802.3/Ethernet	802.4	802.5		
1	**Physikalische Schicht**						

In den folgenden Abschnitten werden die von Windows- NT angebotenen Protokolle NETBEUI, IPX/SPX und TCP/IP beschrieben. Diese Protokolle sind auf den Ebenen oberhalb der Schicht 2 des OSI-Modells angesiedelt.

1.3.3.1 DLC

Das DLC-Protokoll ist ein Protokoll, das zum einen für die Kommunikation zwischen Clients und Steuereinheiten von Mainframes verwendet werden kann und das zum anderen von Windows NT dafür genutzt wird, auf bestimmte Netzwerkdrucker zuzugreifen.

1.3.3.2 NetBEUI

NetBIOS **E**xtended **U**ser **I**nterface (NetBEUI) wurde von IBM 1985 eingeführt und ist das Standard-Protokoll vergangener Tage von Microsoft. Das Protokoll ist für kleine Netze optimal geeignet, da es nur sehr wenig Adressinformationen zusätzlich zu den Nutzdaten enthält, der sogenannte Protokolloverhead also minimal ist. NetBEUI ist nicht routingfähig, kann also nicht über mehrere Netzsegmente hinweg adressieren. Der Einsatz in Weitverkehrsnetzen ist daher nicht zu empfehlen. In gemischten LAN/WAN-Umgebungen sollte zusätzlich ein weiteres, routingfähiges Protokoll für Windows-NT eingesetzt werden. Diese Aufgabe kann durch IPX/SPX und TCP/IP abgedeckt werden.

1.3.3.3 NWLink IPX/SPX

Internetwork **P**acket Exchange (IPX) und **S**equenced **P**acket E**x**change (SPX) sind Entwicklungen von Novell. Es handelt sich hier um routingfähige Protokolle, die für Weitverkehrsnetze besonders gut geeignet sind.

Über das Novell-kompatible NW-Link stellt Windows-NT die Verbindung zu Novell-Servern her. Mit dem Client-Service für Netware kann eine Windows NT Workstation als Client in Netwarenetzen eingesetzt werden. Windows NT Server bietet mit dem Gateway-Service in gemischten NT und Novell-Umgebungen die Möglichkeit, Dienste der Novellserver an Arbeitsstationen im NT-Netz weiterzugeben, ohne dass diese direkt an den Novell-Server angeschlossen werden müssen. Die Vorteile von IPX/SPX liegen in der vergleichsweise geringen Größe und Zusatzeigenschaften im WAN die die Übertragungsraten steigern.

1.3.3.4 TCP/IP

Das weltumspannende Internet arbeitet mit diesem Protokoll. Transmission Control Protocol / Internet Protocol (TCP/IP) wurde bereits in den 70er Jahren für große Netzstrukturen entwickelt. Die Entwicklung wurde durch das amerikanische Verteidigungsministeriurn angestoßen. TCP/IP wurde zum Kornmunikationsprotokoll für den UNIX-Bereich. Es ist durch die ständige Erweiterung und Ergänzung das am weitesten verbreitete und akzeptierte, das Protokoll Ipv4, stößt jedoch bereits an seine Adresskapazität. Eine Projektgruppe "IESG" hat ein Adressierungsschema -*Ipv6* ge-

nannt- entworfen, das Millionen mehr Adressen bietet. Es wird voraussichtlich in den nächsten 10 Jahren den Ipv4-Standard allmählich ablösen.

SNMT (Simple Network Management Protokoll) als Überwachungsmittel für Computer und Geräte basiert auf TCP/IP. Als defacto Standard wird es in allen Netzsystemen unterstützt, von Großrechner, UNIX- Maschinen und von Microsoft Windows NT. Die Vorteile von TCP/IP liegen in der Kommunikationsmöglichkeit mit jeder Art von Computersystem, der Internetkompatibilität, der Routingfähigkeit und der Unterstützung von SNMP.

Eine TCP/IP-Adresse besteht immer aus einer sogenannten NET-ID und einer HOST-ID. Beide zusammen sind immer 4 Bytes =32 Bit groß und werden zur besseren Lesbarkeit in je 8 Bit dezimal geschrieben.

Die IP-Adresse identifiziert jede einzelne Maschine und unterscheidet sie von allen übrigen im Netzwerk. Im Gegensatz zur Ethernet-Adresse, die fest vom Netzwerkkarten-Hersteller vergeben wird, kann und muss sie vom Betreiber bestemmt werden. Damit eine IP-Adresse im Falle einer geplanten Anbindung an das Internet eindeutig ist, muss sie bei einer zentralen Stelle beantragt werden:

DDN(Defece Data Network) Network Information Center
SRI International
333 Ravenswood Avenue, Room EJ291
Menio Park, CA 94025
USA

Man unterscheidet insgesamt 4 Klassen von IP-Adressen. Die Klasse richtet sich nach der Größe der NET-ID.

1.3.3.5 Klasse A

0	Netzwerk	Host-Adresse
7 Bit		24 Bit

1.3.3.6 Klasse B

10	Netzwerk	Host-Adresse
14 Bit		16 Bit

1.3.3.7 Klasse C

110	Netzwerk	Host-Adresse
21 Bit		8 Bit

Die Bits der Hostadresse dürfen nie alle mit 0 oder alle mit 1 belegt sein. Daraus ergeben sich folgende maximale Anzahlen an Teilnetzen und Hosts:

Klasse	Maximale Anzahl Netzwerke	Maximale Anzahl Hosts	Adressbereich
A	126	16 777 214	1.0.0.1 bis 126.255.255.254
B	16 384	65 534	128.0.0.1 bis 191.255.255.254
C	2 097 151	254	192.0.0.1 bis 223.255.255.254
Reserviert			127.0.0.1 bis 127.255.255.254 192.168.0.1 bis 192.168.255.254 224.0.0.0 bis 255.255.255.254

Adressen aus reservierten (internen) Bereichen werden im Internet nicht weitergeleitet und können somit nie zu Konflikten führen. Die Verbindung der Rechner im internen Netzwerk zum Internet muss dann aber über einen speziellen Kommunikationsserver laufen, der von außen über eine reguläre Internet-Adresse angesprochen wird.

Erläuterung des IP-Routing: Wie wird ein Host anhand der IP-Adresse gefunden?

Das gesamte Internet besteht aus einer Reihe von Netzwerken, die als autonome Systeme bezeichnet werden. Jedes System führt das Routing zwischen den teilnehmenden Hosts intern durch, d. h. die Aufgabe des Auslieferns eines Datagramms wird auf die Suche nach einem Pfad zum Netzwerk des Zielhost reduziert. Dies bedeutet, dass, sobald ein Datagramm an einen beliebigen Host innerhalb eines Netzwerks übergeben wird, geschieht die weitere Verarbeitung ausschließlich von diesem Netz.

1.3.3.8 Subnetze

Diese Struktur spiegelt sich darin wider, dass IP-Adressen in einen Host- und einen Netzwerkteil aufgeteilt werden. Per Standardeinstellung wird das Zielnetzwerk aus dem Netzwerkteil der IP-Adresse gewonnen. Alle Hosts innerhalb eines Netzwerks sollten dieselbe Netzwerknummer besitzen.

Es macht Sinn, *innerhalb* des Netzwerks dasselbe Schema zu verwenden, weil es selbst wieder aus hunderten kleinerer Netzwerke bestehen kann, bei denen die kleinsten Einheiten physikalische Netzwerke wie Ethernets sind. Aus diesem Grund erlaubt IP die Unterteilung eines IP-Netzwerks in mehrere *Subnetze.*

Ein Subnetz übernimmt die Verantwortung für die Übertragung von Datagrammen innerhalb eines bestimmten Bereichs von IP-Adressen des IP-Netzes, dem es angehört. Genau wie bei den Klassen A, B und C wird es über den Netzwerkteil der IP- Adressen identifiziert. Allerdings wird der Netzwerkteil etwas erweitert und enthält nun einige Bits aus dem Host-Teil. Die Anzahl der Bits, die als Subnetznummer interpretiert werden, wird durch die sogenannte *Subnetzmaske,* oder kurz *Netmask,* bestimmt. Eine Subnetzmaske besteht wie die IP-Adresse aus 32 Bits. Die Bits für die Netzwerkadresse sind alle auf den Wert 1 gesetzt, und die Bits für die Host-Adresse sind alle auf den Wert 0 gesetzt. Je mehr Bits für die Subnetzmaske benutzt werden, desto weniger Hosts können an das Subnetz angeschlossen werden. Die Subnetzmaske wird auf die IP-Adresse in jeder Nachricht angewendet, um die Netzwerknummer und die Host-Nummer zu trennen.

Die Subnetzmaske muss für alle Computer im Netz gleich sein; andernfalls verstehen die Computer nicht, dass sie zum selben Netzwerk gehören.

Wenn Ihr Computer beispielsweise die Klasse-C-Adresse 192.168.119.201 untersucht und die Standard-Subnetzmaske 255.255.255.0 darauf anwendet, sieht er die Netzwerknummer 192.168.119 und die Host-Nummer 201.

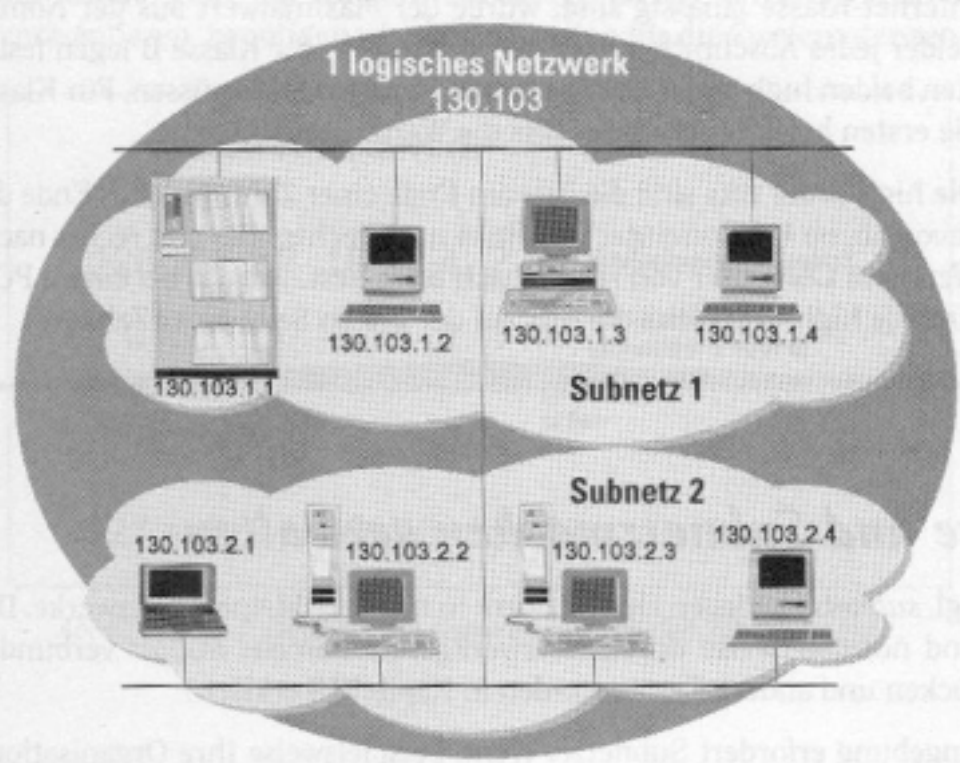


Abbildung 13.4: Jedes Subnetz hat seine eigene Adresse.

1.4 Strukturelemente

Sind Netzwerke in Segmente unterteilt oder müssen Netzwerke miteinander verbunden werden, sind für diese Aufgaben Geräte oder Softwarekomponenten erforderlich. Die Fähigkeiten der Komponenten reichen von der reinen Signalverstärkung bis zu komplexen Aufgaben wie Protokollumsetzung oder Übersetzung von Zeichencodes.

1.4.1 Repeater

Der Repeater dient der Verlängerung von Kabelstrecken oder Verbindungen von gleichen Segmenten. Ein Repeater wird dann erforderlich, wenn wegen zu großen Entfernungen das Signal auf dem Kabel so stark degeneriert, dass es nicht mehr ausgewertet werden kann. Der Repeater identifiziert das Signal auf dem einen Segment und sendet es verstärkt auf dem anderen Segment wieder aus. Der Repeater arbeitet nur auf Schicht 1 (phys. Schicht) des OSI-Modells.

1.4.2 Bridge

Die Bridge arbeitet auf Schicht 2 (Verbindung) des OSI-Modells und hat daher die Information über die physikalischen Adressen in Datenpaketen. Die Bridge kann darüber entscheiden, ob ein Paket auf ein anderes Segment übertragen werden muss oder nicht. Es ist also eine Teilung der Netzlast und damit eine Performance-Steigerung möglich. Brücken sind unabhängig von Transportprotokollen. Sie haben die drei Aufgaben Lastteilung, physikalische Trennung von Segmenten und Datenflußsteuerung. Bei Aufteilung eines Netzes mit Hilfe von Brücken besteht weiterhin ein logisches Netz.

Es gibt 2 Arten von Bridges:

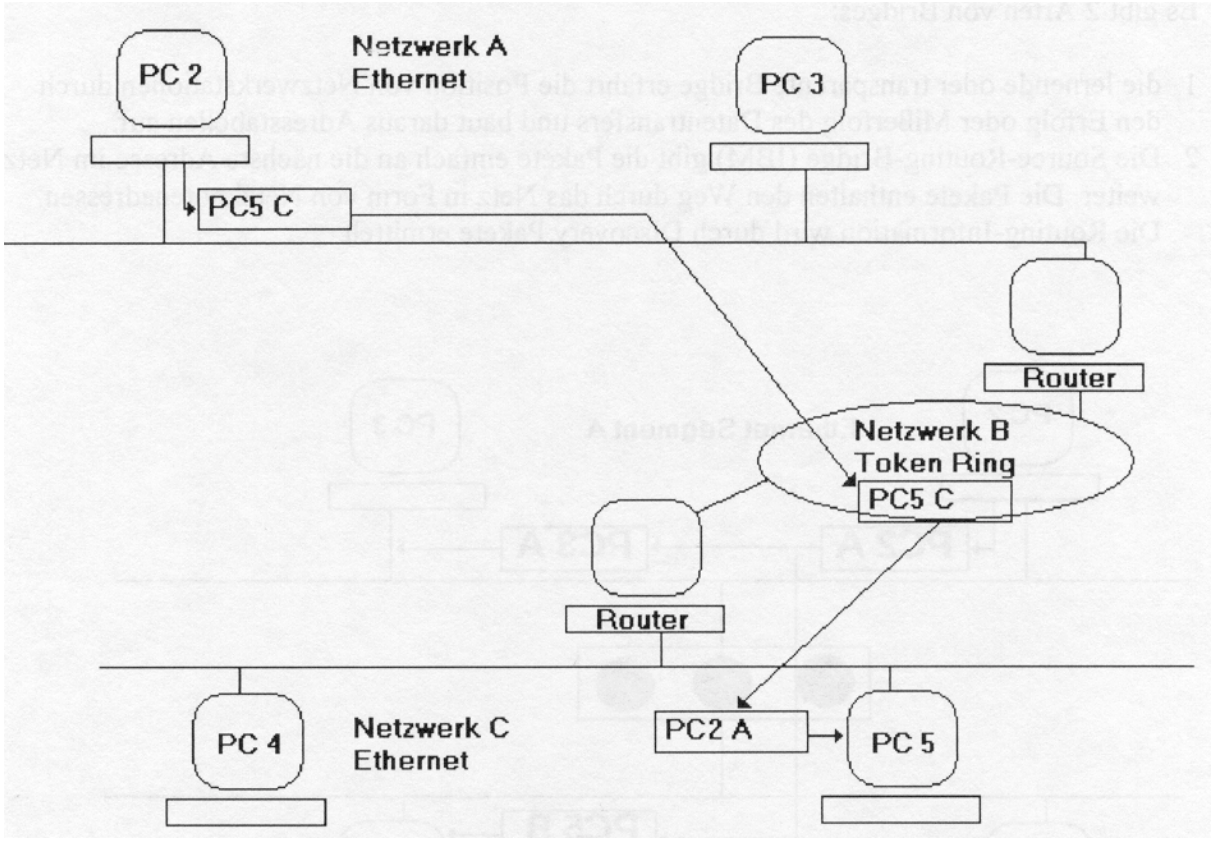
1. Die lernende oder transparente Bridge erfährt die Position von Netzwerkstationen durch den Erfolg oder Mißerfolg des Datentransfers und baut daraus Adresstabellen auf.

2. Die Source-Routing-Bridge (IBM) gibt die Pakete einfach an die nächste Adresse im Netz weiter. Die Pakete enthalten den Weg durch das Netz in Form von Netzknotenadressen. Die Routing-Information wird durch Discovery.Pakete ermittelt

1.4.3 Router

Die Router arbeiten auf Schicht 3 (Netzwerk) des OSI-Modells mit logischen Adressen. Sie sind unabhängig von Schicht 1 und 2 des OSI-Modells. Sie verwenden Algorithmen zur Bestimmung des besten Weges durch das Netz. Router sind in der Lage, unterschiedliche Topologien miteinander zu verbinden, etwa Ethernet und TokenRing und werden dazu verwendet, Netze logisch und physikalisch zu trennen.

Ein Router muss die Transportprotokolle kennen, um die Pakete korrekt behandeln zu können. Es gibt Singleprotokollrouter und Multiprotokollrouter. Es gibt jedoch auch Netzwerkprotokolle wie NetBEUI oder SNA, die nicht routingfähig sind. Um Pakete mit nicht unterstützten Protokollen weitergeben zu können, haben die meisten Router auch die Funktionalität von Bridges.



1.4.4 Gateway

Ein Gateway verbindet Rechnerwelten, die unterschiedliche Protokolle oberhalb der Netzwerkschicht verwenden. Sie arbeiten bis hinauf zur Schicht 7 und müssen Aufgaben wie Protokollumsetzung und Zeichensatzkonvertierung erfüllen. Gateways sind normalerweise dedizierte, leistungsfähige Rechner. Ein Gateway verbindet so zum Beispiel ein PC-Netzwerk mit einem IBM-Host. Ein Gateway ist demnach ein Host, der an zwei oder mehr physikalische Netze gleichzeitig angeschlossen ist. Er ist so konfiguriert, dass er Pakete zwischen diesen Netzen hin und her übertragen kann.

2 Fragen zur Erschließung des Themas

Netzwerk:

1) Welche Vorteile bietet die Vernetzung von Computern in einem Unternehmen?

2) Welche Nachteile könnten sich aus einer Vernetzung ergeben?

3) Worin besteht der wesentliche Unterschied zwischen einem Peer-to-Peer-Netzwerk und einem Client-Server-Netz?

4) Nennen Sie drei wichtige Netzwerktopologien

Netzwerkprotokolle:

1) Welchen Zweck verfolgt man mit dem ISO/OSI - 7-Schichten-Modell?

2) Welche Aufgabe hat ein Protokoll?

3) Nennen Sie vier unterschiedliche Netzwerkprotokolle und deren Herkunft.

4) Wie lautet die Netzwerkadresse des Servers mit der TCP/IP-Adresse 130.2.1.18 und wie lautet die Standard-Subnetzmaske?

Strukturelemente

1) Erläutern Sie die Arbeitsweise von Repeater, Hub, Bridge, Switch, Router und Gateway.

2) Auf welchen Ebenen des OSI-Referenzmodells arbeiten diese jeweils?

3) Welche physikalischen Wege und Medien werden heute zur Übertragung von Digitalen Signalen eingesetzt?

2.1 1.6 TCP/IP-Namensdienste

Ein Kernproblem bei der Arbeit über TCP/IP und auch bei der Verwendung anderer Protokolle ist die Namensauflösung. Grundsätzlich geht es dabei darum, dass mehrere verfügbare Adressen beziehungsweise Namen von Computern einander korrekt zugeordnet werden. Das Problem ist also, dass zum Beispiel bei einem Browser im Internet eine URL wie

http://www.microsoft.de/mspress

eingegeben wird, die als Rechnernamen den Teil www.microsoft.de enthält. Nur: TCP/IP kann damit nichts anfangen, sondern muss wissen, welche IP-Adresse gesucht wird. Das gleiche gilt natürlich auch für alle Router im Internet. Diese Zuordnung wird als Namensauflösung bezeichnet und ist eines der Kernprobleme, die es im Internet und im Intranet zu lösen gilt.

In einem Intranet bestehen dabei mehr Alternativen, da nicht zwingend über Internet-Namen gearbeitet und in einem kleineren Intranet auch keineswegs mit dem **D**omain **N**ame **S**ystem (DNS) eine Lösung aufgebaut werden muss. Die verschiedenen Möglichkeiten zur Namensauflösung in einem Intranet auf Basis von Windows NT beziehungsweise im Internet werden daher nachfolgend erläutert.

Die Netzwerk-Adapterkarte eines Computers hat eine Adresse, die als MAC-Adresse bezeichnet wird. MAC steht für **M**edia **A**ccess **C**ontrol und bezieht sich eben auf den Adapter. Diese Adresse ist üblicherweise fest für jeden Adapter konfiguriert, kann aber im Token Ring auch manuell festgelegt werden.

Daneben gibt es die IP-Adresse des Systems. Doch damit nicht genug, gibt es schließlich auch noch den Computernamen als NetBIOS-Namen, der im Bereich Netzwerk der Systemsteuerung definiert wird, und gegebenenfalls einen Internet-Namen. Windows NT unterstützt nun bei UNC-Pfadnamen, die auf das Netzwerk verweisen, beide Formen von Namen.

Was ist überhaupt ein UNC-Pfadname? **UNC** steht für **U**niversal **N**aming **C**onvention. Dabei handelt es sich um ein Schema, mit dem Ressourcen auf entfernten Systemen im Netzwerk direkt adressiert werden können. Wenn Sie auf eine Excel-Datei auf einem Server zugreifen möchten, können Sie diese zum Beispiel unter einem Namen wie

\\L1119\EXCEL-FILES\BUDGET\2000-2.XLS

ansprechen. Der erste Teil dieses Namens, L1119, gibt an, auf welchen Server zugegriffen werden soll. Im Gegensatz zu den bekannten lokalen Dateinamen sind diesem Server-Namen zwei Backslash vorangestellt. Dadurch wird gekennzeichnet, dass es sich um einen Zugriff auf das Netzwerk handelt. Nach dem Server-Namen folgt der Name der Freigabe, auf die zugegriffen werden soll. Bei mehr als acht Zeichen können einige DOS-Clients auf solche Freigaben nicht mehr zugreifen. Abschließend folgen noch Verzeichnis und Dateiname.

Diese UNC-Pfadnamen können zum einen genutzt werden, um permanente Verbindungen zu Freigaben über ein logisches Laufwerk herzustellen. Sie können aber auch eingesetzt werden, um einen Pfad zu einem logischen Laufwerk anzugeben, ohne eine solche permanente Verbindung herzustellen. Das passiert auch intern, wenn Sie über den Explorer von Windows NT auf einen Server im Netzwerk zugreifen.

Bei den Rechnernamen wie L1119 handelt es um **NetBIOS-Namen**. NetBIOS ist eine Schnittstelle für Anwendungen, die über das Netzwerk arbeiten. Sie wird auch vom Server und Arbeitsstationsdienst von Windows NT intensiv genutzt - wie man an der Herstellung solcher Verbindungen bereits erkennen kann. Diese Konstruktion bringt aber einige Nachteile bei der Namensauflösung und in anderen Situationen mit sich.

Um diese Problematik zu umgehen und im TCP/IP-Umfeld einen einfacheren Zugriff auf andere Systeme und insbesondere eine vereinfachte Administration zu erlauben, wurde Windows NT intern so erweitert, dass neben den NetBIOS-Namen im UNC-Pfadname auch Internet-Namen wie L1119.BWV-AHAUS.DE eingesetzt werden können.

Statt des oben angegebenen Pfadnamens kann ein Zugriff also auch über

\\L1119.BWV-AHAUS.DE\EXCEL-FILES\BUDGET\2000-2.XLS

erfolgen. Diese Anpassung bringt sowohl praktische Vorteile als auch neue Entwicklungschancen für Windows NT. So kann nun ausschließlich mit dem Domain Name System (DNS) und Internet-Namen in einer durch Router segmentierten Umgebung gearbeitet werden. Wichtiger aber ist, dass damit ein erster Schritt über das mittlerweile doch recht antiquierte NetBIOS-Konzept hinaus getan wurde.

Was wie eine kleine Änderung wirkt, war recht aufwendig in der Umsetzung. Denn immerhin umfassen NetBIOS-Namen maximal 16 Zeichen, von denen 15 für den Computer- oder Domänennamen verwendet werden können, während das letzte die Art des Dienstes angibt: Server, Workstation, Nachrichtendienst und so weiter. Internet-Namen können im Vergleich dazu wesentlich länger sein, so dass alle Datentypen und die Funktionen, in denen auf diese Datentypen zugegriffen wird, angepasst werden mussten.

Selbstverständlich können nicht nur Laufwerksverbindungen nun über die Internet-Namen hergestellt werden, sondern auch Befehle wie NET VIEW mit diesen Namen verwendet werden. Ein interessanter Nebeneffekt dieser Erweiterung ist das Verhalten von Windows NT bei der Namensauflösung. Wenn Adressen von DNS-Servern definiert sind und eine Namensauflösung für einen Namen mit mehr als 15 Zeichen erfolgen soll, wird automatisch DNS verwendet, da es sich in diesem Fall nicht mehr um einen NetBIOS-Namen handeln kann.

Für die Namensauflösung generell ist diese Unterscheidung von Bedeutung, weil Windows NT eben zwei verschiedene Namen unterstützt. Für den Anwender im Intranet ist es bequemer, den NetBIOS-Namen zu verwenden, während im Internet der Internet-Name zwingend ist. Browser (z. B. Internet-Explorer) unterstützen aber beide Formen, da ebenso wie bei UNC-Pfadnamen, die Namensauflösung von URLs durch das lokale Betriebssystem vorgenommen wird.

Wenn der Benutzer nun über den Computernamen - egal welchen der beiden - und das TCP/IP-Protokoll auf einen Server zugreifen möchte, muss zunächst einmal die IP-Adresse dieses Servers ermittelt werden. Ist diese Adresse bekannt, wird auch noch die passende MAC- Adresse des Computers oder die des nächsten Gateways auf dem Weg zu diesem Computer festgestellt. Der letzte Schritt wird vom **ARP**, dem **A**ddress **R**esolution **P**rotocol, durchgeführt und soll uns hier nicht weiter beschäftigen.

Dagegen ist die Zuordnung von Computername und IP-Adresse (Name Resolution - Namensauflösung) ein durchaus komplexes Thema, das auch einen erheblichen Verwaltungsaufwand im Netzwerk erfordert. Windows NT stellt verschiedene Mechanismen bereit, über die diese Zuordnung im Intranet erfolgen kann. Unterschieden wird dabei auch zwischen Knotentypen, also Einstellungen bei den Computern. Windows NT unterstützt die Mechanismen, die auch im UNIX-Umfeld überwiegend genutzt werden.

2.1.1.1 Broadcast:

Nach dem Einschalten versendet ein System dabei Informationen über seinen Namen und seine IP-Adresse. Diese werden von den empfangenden Systemen in eine Tabelle aufgenommen. Falls es einen doppelten Namen gibt, antwortet das System, das den Namen bereits für sich in Anspruch genommen hat, darauf mit einer entsprechenden Meldung. Alle Systeme, die mit Broadcasts arbeiten, reagieren aber auch auf Broadcasts, in denen ein Name gesucht wird. Broadcasts sind nicht in der Lage, über Router hinweg zu arbeiten.

2.1.1.2 HOSTS-Dateien

HOSTS-Dateien treten bei Microsoft in zwei Formen auf: Die klassische Datei **HOSTS** ist für die Zuordnung von **Internet-Namen** zu **IP-Adressen** verantwortlich, während **LMHOSTS** ihre Bedeutung in der Zuordnung von **NetBIOS-Namen zu IP-Adressen** erlangt.

2.2 Das Konzept von DHCP

DHCP (Dynamic Host Configuration Protocol) ist einer der reizvollsten Dienste, die von Windows NT bereitgestellt werden. Seine Aufgabe liegt drin, IP-Adressen automatisch zu vergeben und damit die Last für die Administration von TCP/IP-Umgebungen etwas zu verringern.

Das Dynamic Host Configuration Protocol (DHCP) ist ein relativ neues Protokoll im TCP/ IP- Umfeld. Microsoft ist einer der ersten größeren Anbieter, der dieses Protokoll in seinen Produkten implementiert hat. Allerdings findet sich die Unterstützung für das DHCP-Protokoll zunehmend auch in anderen TCP/IP-Implementierungen verschiedener Anbieter.

Die Idee des Protokolls ist es, IP-Adressen und die dazu gehörenden Informationen an zentraler Stelle aus zu definieren und dem Client beim Start zuzuordnen. Ein Rechner, der als DHCP-Client arbeitet, hat daher keine feste IP-Adresse, sondern bekommt diese dynamisch beim Systemstart zugewiesen. Da er zu diesem Zeitpunkt noch keine IP-Adresse besitzt, ist ein solches Protokoll natürlich nicht ganz trivial.

Daher soll zunächst das Konzept von DHCP und anschließend die Konfiguration des Protokolls bei Windows NT beschrieben werden.

Bei DHCP handelt es sich übrigens keineswegs um eine von Microsoft allein geborene Idee. Das Protokoll ist vielmehr im RFC 1541 definiert. Ein RFC ist ein sogenannter Request for Comment, bei dem ein Standardisierungsvorschlag in relativ offener Form diskutiert wird. Fast alle Elemente von TCP/IP und seiner Umgebungen - auch die oben beschriebenen Name-Resolution-Konzepte - sind in Form solcher RFCs definiert. Microsoft hat nur als einer der ersten größeren Hersteller die Bedeutung von DHCP erkannt und eine Unterstützung in seinem Produkt realisiert.

Das Grundkonzept von DHCP ist eigentlich ziemlich simpel. Normalerweise werden IP-Adressen auf einem Client fest definiert. Bei der Verwendung von DHCP wird dagegen ein Pool von IP- Adressen auf einem DHCP-Server festgelegt. Wenn der Client gestartet wird, meldet er sich beim DHCP-Server und bekommt von diesem eine IP-Adresse zugewiesen. Mit dieser Adresse können auch die erforderlichen Informationen über Gateways, WINS-Server und andere Einstellungen geliefert werden.

Die erste Frage, die sich bei einem solchen Verfahren stellt, ist die nach der Kommunikation zwischen dem Client und dem Server, wenn der Client noch gar keine IP-Adresse hat.

Um die Adresse zu erhalten, wird ein spezieller Broadcast, der eine Erweiterung des BOOTP-Protokolls verwendet, eingesetzt. Dieser erreicht den DHCP-Server. Der DHCP-Server antwortet mit dem Angebot einer IP-Adresse. Falls der Client mehrere Adressen von mehreren Servern angeboten bekommt, wählt er eine aus - in der Regel die erste erhaltene Adresse. Die Annahme der Adresse bestätigt er dem Server.

Der Server übersendet nun die kompletten Informationen für die Adresse an den Client. Dazu gehören die Angabe der Lease-Dauer und weitere Informationen, die auf dem DHCP-Server definiert sind. Damit ist die Adresse zugeordnet.

Falls sich der Server in einem anderen Subnetz befindet, kann die Adresszuordnung vorgenommen werden, wenn auf dem Router das Protokoll BOOTP erlaubt ist. Der Router kann auch ein Windows NT Server mit installiertem DHCP-Relay Agent sein. Dabei handelt es sich um einen Broadcast, der explizit freigeschaltet werden muss. Der Router muss dafür die RFCs 1532, 1533 und 1541 unterstützen, was für bestehende, ältere Systeme ein Upgrade der Firmware erforderlich machen kann, falls diese Funktionalität überhaupt unterstützt wird.

Andere Broadcasts können in dieser Situation aber auch weiterhin nicht über den Router gesendet werden. Da diese Freigabe nicht auf allen Routern erfolgen muss, lässt sich sehr gut steuern, welche Subnetze über BOOTP nach einem DHCP-Server durchsucht werden.

Die Zuordnung der Adresse erfolgt in einem Leasing-Verfahren. Der Client erneuert das Leasing dabei in der Regel nach Ablauf von 50 % der Leasing-Zeit, so dass er auch weiterhin mit der gleichen IP-Adresse arbeitet. Da Sie die Leasing-Dauer typischerweise im Rahmen von mehreren

Tagen definieren, ändert sich die über DHCP zugeordnete IP-Adresse bei regelmäßig genutzten Systemen normalerweise nicht.

Der Client meldet sich auch bei jedem neuen Start bei dem DHCP-Server, um zu überprüfen, ob er sich noch im richtigen Subnetz befindet, Das ist wichtig, damit ein Notebook, wenn es in einem anderen Subnetz angeschlossen wird, sofort und nicht erst nach dem Ablauf der Lease-Dauer eine neue Adresse erhält.

Für die Nutzung von DHCP muss ein DHCP-Server verfügbar sein. Das kann zum Beispiel ein Windows NT Server ab der Version 3.5 sein, der diese Funktionalität integriert hat.

Auf diesem Server können nun Bereiche von Adressen definiert werden, die für die DHCP-Clients zur Verfügung stehen. Innerhalb der Bereiche können bestimmte Adressen ausgeschlossen oder für spezielle Clients reserviert werden. Die Zuordnung erfolgt dabei über die MAC-Adresse.

MAC steht für Media Access Control. Die MAC-Adresse bezeichnet die im Adapter fest eingebrannte Adresse, über die dieser im Netzwerk identifiziert wird. Jeder Hersteller von Ethernet-Netzwerkadapterkarten bekommt einen Bereich von Adressen zugewiesen, den er verwenden kann. Diese Adressreservierung ist von allergrößter Bedeutung, da damit sichergestellt werden kann, dass ein Client immer über die gleiche Adresse verfügt.

Darüber hinaus können für diesen Bereich nun zum Beispiel Adressen von WINS-Servern, Gateways, NIS-Servern und die anderen im TCP/IP-Umfeld erforderlichen Parameter definiert werden, die wiederum Adressbereichen zugeordnet werden können, damit ein Client auch alle anderen erforderlichen Konfigurationsoptionen bei der Zuordnung der Adresse erhält.

Wenn ein Client nun ins Netz geht, wird ihm automatisch eine gültige IP-Adresse zugeordnet. Welcher Client welche Adresse hat, kann ebenfalls über den DHCP-Server wieder festgestellt werden.

Nachdem Sie die Zuordnung durchgeführt haben, müssen Sie sich nicht mehr um die manuelle Konfiguration kümmern. Das ist ein erheblicher Vorteil. Der Nachteil liegt darin, dass es schwieriger wird, die IP-Adressen der verschiedenen Clients im Netzwerk zu überschauen, da diese eben nicht mehr zwingend fest vergeben sind.

2.3 Installation und Konfiguration von DHCP

Der DHCP-Server ist als Bestandteil von Windows NT verfügbar. Er kann dementsprechend über den Bereich Netzwerk der Systemsteuerung eingerichtet werden. Dort kann er im Register Dienste über die Schaltfläche Hinzufügen eingerichtet werden. Die Client-Funktionalität wird mit dem TCP/IP-Protokoll automatisch eingerichtet und muss nur noch konfiguriert werden.

Nachdem Sie die Auswahl getroffen haben, wird die erforderliche Software installiert. In der Gruppe Programme - Verwaltung des Startmenüs wird ein neues Symbol für den Start des DHCP- Managers aufgenommen. Dieser findet sich übrigens auch bei den Server-Tools, so dass er auch auf diesem Weg auf einer Windows NT Workstation für die dezentrale Verwaltung eingerichtet werden kann. Der erste Schritt für die Verwendung des DHCP-Dienstes ist nun, den Dienst so zu konfigurieren, dass die entsprechenden Adressen auch zur Verfügung stehen und alle erforderlichen Informationen an die Clients gesendet werden.

Nach dem Start zeigt der DHCP-Manager zunächst nur ein leeres Fenster an. über den Befehl Hinzufügen im Menü Server können Sie nun im ersten Schritt den oder die Server, die Sie eingerichtet haben, in die Liste aufnehmen. Sie müssen hier entweder die IP-Adresse, den NetBIOS-Namen oder den Internet-Namen des Servers angeben, der hier hinzugefügt werden soll. Nachdem Sie einen Server hinzugefügt haben, steht Ihnen dieser in der Liste auf der linken Seite des DHCP-Managers zur Verfügung.

Der nächste Schritt, der nun folgt, ist die Definition von Bereichen. Ein Bereich umfasst immer eine Reihe von IP-Adressen, die vergeben werden dürfen. Dazu verwenden Sie die Schaltfläche Erstellen im Menü Bereich. Im dann angezeigten Dialogfeld können Sie die grundsätzlichen Festlegungen zu dem Bereich treffen.

Dazu gehört ein Adressbereich, eine Bezeichnung und die Möglichkeit, bestimmte IP-Adressen auszuschließen. Außerdem können Sie die Dauer der Lease definieren. Sie sollten hier in der Regel einen relativ langen Wert von zum Beispiel 30 Tagen verwenden, um zu verhindern, dass sich zugeordnete IP-Adressen der Clients regelmäßig verändern. Die Wahl der Dauer für die Lease ist eines der ganz schwierigen Themen. Für kurze Zeiträume spricht, dass Adressen dann auch entsprechend schnell wieder freigegeben werden. Auf der anderen Seite führt eine kurze Lease-Dauer zu einer relativ hohen Wahrscheinlichkeit von Änderungen der IP-Adressen bei den Clients. Und das wiederum kann unerwünscht sein. Wenn Sie dagegen eine lange Lease-Dauer definieren, entsteht die Schwierigkeit, dass die IP-Adressen von Clients, die es schon lange nicht mehr gibt, noch lange Zeit reserviert bleiben. Das ist allerdings kein allzu großes Problem, wenn ausreichend IP-Adressen zur Verfügung stehen**.** Sehr problematisch ist die Arbeit mit unbegrenzten Leases. Das dabei entstehende Problem ist, dass diese Leases nicht mehr freigegeben werden, auch wenn ein Client nicht mehr existiert. Der Aufwand für die manuelle Administration steigt damit erheblich. Grundsätzlich bringen diese keinen Vorteil, da entweder mit Reservierungen oder mit relativ langen Dauern für die Leases gearbeitet werden kann. In der Praxis haben sich Lease-Dauern von 30 bis 42 Tagen bewährt. Damit wird eine Änderung der IP-Adresse fast sicher vermieden, wenn ein Computer - zum Beispiel wegen Urlaub - einmal für längere Zeit nicht eingeschaltet wird**.**

Sie können auch Reservierungen hinzufügen. Diese dienen dazu, eine IP-Adresse einer bestimmten MAC-Adresse, die hier als Eindeutige ID (UID) bezeichnet ist, zuzuordnen. Das ist zum Beispiel dann wichtig, wenn Sie mit Unix-Systemen arbeiten, die nicht auf WINS für die Adresszuordnung zugreifen, oder sonst eine Situation haben, in der ein Server von bestimmten Clients immer unter einer bestimmten Adresse gesucht wird. In diesem Fall haben Sie immer noch den Vorteil der automatischen Konfiguration, haben aber auf der anderen Seite sichergestellt, dass ein Knoten im Netzwerk trotzdem immer die gleiche IP-Adresse zugewiesen bekommt.

Über das Menü Optionen können Sie nun Parameter für die verschiedenen Bereiche definieren, die mit der IP-Adresse an die Clients gegeben werden sollen. Sie können diese Festlegungen global für alle Bereiche oder begrenzt auf einen Bereich treffen.

Um einen Client für den Betrieb mit DHCP einzurichten, müssen Sie bei Windows NT in der Systemsteuerung im Bereich Netzwerk das TCP/IP-Protokoll einrichten. Anschließend können Sie die Konfiguration durch Aufruf der Schaltfläche Eigenschaften starten.

Im Dialogfeld sehen Sie im oberen Bereich das Optionsfeld **Automatische DHCP- Konfiguration aktivieren**. Sobald Sie dieses Optionsfeld ausgewählt haben, verwendet das System das DHCP-Protokoll. Die Einstellungen für die Subnetz-Maske und die IP-Adresse können dann nicht mehr eingegeben werden. Praktisch alle anderen Optionen der TCP/IP-Konfiguration sind auch weiterhin verfügbar. Dabei werden die Einstellungen, die auf dem DHCP-Server definiert sind, durch lokale Einstellungen, soweit diese angegeben sind, überschrieben.

Das DHCP-Protokoll wird automatisch gestartet. Das System sucht sich also sofort einen DHCP Server und fordert von diesem eine Adresse und die übrigen, dort definierten Informationen an. Damit entfällt auch die Erfordernis eines Neustarts des Systems in dieser Situation.

2.3.1.1 IPCONFIG

Eine Möglichkeit, sich die IP-Adresse eines Clients ausgeben zu lassen, ist der Befehl **IPCONFIG** an der Befehlszeile von Windows NT. Dieser Befehl gibt die Informationen über die IP-Adresse, die Subnetz-Maske und das Definierte Standard-Gateway aus.

Ipconfig /all: Gibt eine umfangreichere Liste mit Informationen zu der IP-Konfiguration des Clients aus. In dieser Liste sind neben den oben genannten Informationen auch die MAC-Adresse, die Adressen der WINS-Server und die Informationen über die DHCP-Lease enthalten. Dieser Befehl ist auch für Windows 9x in der Eingabeaufforderung gültig.

Ipconfig /renew: Mit dieser Option können Sie manuell eine Erneuerung der DHCP-Lease auslösen. Damit wird sichergestellt, dass die vergebene Adresse auch weiterhin gültig ist

Ipconfig /release mit dieser Option wird die Lease einer IP-Adresse beendet.

2.3.2 Namensauswertung

Die Namen, die Benutzer ihren Computern geben, haben normalerweise eine bestimmte Bedeutung und sind leicht zu merken. Aus Gründen der Bequemlichkeit können Sie bei Befehlen, die auf höherer Ebene arbeiten, im allgemeinen Host-Namen für entfernte Systeme im Netzwerk angeben. Die Netzwerk-Software benötigt dann die Netzwerk-Adresse des Systems, das den angegebenen Host-Namen verwendet, um den gewünschten Vorgang erfolgreich durchführen zu können. Wenn also ein Benutzer einen Befehl wie **finger chavez@hamlet** eingibt, muss als erstes der Host-Name hamlet in seine IP-Adresse (10.1.2.6) umgewandelt werden. TCP/IP kennt für diesen Vorgang, der auch Namensauflösung genannt wird (Microsoft spricht von Namensauswertung), zwei Möglichkeiten:

- Das System kann die IP-Adresse herausfinden, indem es den Host-Namen in der Datei Hosts findet. Unter Windows NT befindet sich diese Datei im Verzeichnis %SystemRoot%\System32\Drivers\Etc.[1]
- Das System kann einen sogenannten Namens-Server nach der IP-Adresse für den Host-Namen fragen. Namens-Server werden auch als DNS-Server bezeichnet (Domain Name System). DNS wird häufig in UNIX-Umgebungen verwendet.

Derselbe Vorgang wird häufig auch dann ausgelöst, wenn ein Benutzer einen Befehl wie **net view tirzah** oder **dir \\pele\homes\chavez** eingibt. Diese Befehle verwenden das SMB-Protokoll über die NetBIOS-Schnittstelle. **NetBIOS-Namensauflösungen** finden ebenfalls über eine Konfigurationsdatei, nämlich **LMHosts** (im selben Verzeichnis wie die TCP/IP-Datei Hosts) oder über den NetBIOS-Namensdienst WINS (Windows Internet Name Service) statt. **WINS arbeitet ähnlich wie DNS, liefert aber IP-Adressen für NetBios-Namen, während DNS IP-Adressen für TCP/IP-Host-Namen (Internet-Namen) bietet.** Die Zuordnungsdatenbank von WINS wird dynamisch aktualisiert. Die Zuordnung von Host-Namen und IP-Adressen ist bei DNS statisch und muss manuell aktualisiert werden. Unter Windows NT kann WINS in Verbindung mit DNS ausgeführt werden, so dass sich die beiden Systeme ergänzen.

2.3.2.1 Die Dateien Hosts und LMHosts

In TCP/IP-Netzwerken enthält die Datei Hosts traditionell eine Liste der Hosts im lokalen Netzwerk (einschließlich des eigenen Systems, localhost, selbst). Wenn Sie diese Datei für Ihr Netzwerk verwenden, müssen Sie sie immer dann verändern, wenn Sie dem Netzwerk ein neues System hinzufügen. Wenn Sie einen Computer einem bestehenden Netzwerk hinzufügen, müssen Sie die Hosts-Datei auf jedem Computer im Netzwerk verändern.

Hier ein Beispiel für die *Hosts-Datei* eines kleinen LAN's:

```
Loopback address for localhost
127.1      localhost
# Unsere  Host-Namen und Adressen
10.1.1.2   spain spain.bwv-ahaus.de
# Andere Hosts im lokalen Netz
10.1.1.1        brazil
10.1.1.3        usa
10.1.1.4        canada
10.1.1.5        england uk
10.1.1.6        greece olympus achaia
```

[1] Der Ort an dem Windows NT nach der TCP/IP-Konfigurationsdatei sucht, wird durch den Registrierungsschlüssel HKEY_LOCAL_MACHINE\System\CurrentControtSet\Services\TCPIP\Parameters\DataBasePath festgelegt.

```
10.0.13.4       L1119
192.168.34.77   dalton
```

Zeilen, die mit dem Zeichen # beginnen, werden als Kommentarzeilen betrachtet und vom System ignoriert. Abgesehen von den Kommentarzeilen besitzt jede Zeile drei Felder: Die Netzwerk-Adresse, den Namen und den Alias-Namen (Synonyme) für einen Host. jede Hosts-Datei muss aus mindestens einem Eintrag bestehen: Einer Loopback-Adresse für Testzwecke (vereinbarungsgemäß 127. 0.0. 1) Die weiteren Zeilen beschreiben andere Hosts im lokalen Netz. Außerdem können in dieser Datei Einträge für Hosts stehen, die sich nicht im lokalen Netzwerk befinden (wie der letzte Eintrag der Beispieldatei zeigt).

Drei Hosts wurden *Alias-Namen* (also zusätzliche Host-Namen) zugeordnet. Das lokale System nennt sich *spain,* kann aber auch mit dem vollständigen Namen *spain.*aurorat.com angesprochen werden. Entsprechend ist *uk* ein Alias für *england; olympus* und *achaia* sind Alias-Namen für den Host *greece.* Ein Host-Name kann so viele Alias-Namen besitzen, wie Sie wollen. Trennen Sie die Alias-Namen mit Leerzeichen voneinander.

2.3.3 Funktionsweise von WINS

Bevor eine Kommunikationsverbindung zwischen zwei NetBIOS-basierten Hosts hergestellt werden kann, muss der NetBIOS-Name des Ziel-Hosts in die entsprechende IP-Adresse konvertiert werden. Dies ist deshalb erforderlich, weil für die Kommunikation unter TCP/IP eine IP-Adresse vorhanden sein muss. Das Herstellen einer Kommunikationsverbindung mit dem NetBIOS-Namen allein ist unter TCP/IP nicht möglich.

Zum Registrieren und Auswerten von NetBIOS-Namen mit WINS wird folgendes Verfahren angewendet:

1. Jedesmal, wenn in einer WINS-Umgebung ein WINS-Client gestartet wird, wird dessen Zuordnung von NetBIOS-Name zu IP-Adresse auf einem dafür vorgesehenen WINS-Server registriert.

2. Wenn ein WINS-Client (PC01) einen NetBIOS-Befehl ausführt, um mit einem anderen Host (PC03) zu kommunizieren, dann wird die Aufforderung zur Namensabfrage direkt an den WINS-Server geschickt und nicht über das lokale Netzwerk rundgesendet.

3. Wenn in der Datenbank des WINS-Servers eine Zuordnung von NetBIOS- Namen und IP-Adresse für diesen Ziel-Host (PC03) gefunden wird, dann wird die IP-Adresse des Ziel-Hosts an den WINS-Client (PC01) zurückgesendet. Da die WINS-Datenbank diese Zuordnungen jeweils dynamisch erhält, handelt es sich immer um aktuelle Informationen. Ist der WINS-Server nicht erreichbar, wird auf dem Client auf den Modus B- Knoten umgeschaltet und die Anfrage als Rundsendung an das gesamte lokale Subnetz geschickt.

2.3.3.1 Anforderungen für WINS

Damit WINS implementiert werden kann, müssen sowohl Server als auch Client entsprechend konfiguriert werden.

Anforderungen an den Server

- Auf wenigstens einem Computer, auf dem innerhalb des TCP/IP-Netzwerkverbundes Windows NT Server ausgeführt wird, muss der WINS-Server-Dienst konfiguriert sein. Es braucht sich dabei **nicht** um einen Domänen-Controller zu handeln.
- Es muss eine statische IP-Adresse konfiguriert sein.

2.3.4 Der Domain Name Service

Der Domain Name Service (DNS) beruht auf Servern, die auf diversen im Netzwerk erreichbaren Systemen ausgeführt werden und eine Umwandlung von Host-Namen in IP-Adressen (und umgekehrt) ermöglichen. Das DNS-System ist in Gruppen von Hosts aufgeteilt, die Domänen (Domains) genannt werden. DNS-Domänen befinden sich in einer einzigen hierarchischen Struktur, deren Basis das Internet bildet; es gibt festgelegte Suffixe, die die oberste Ebene des Baums bilden *(.com, org, edu,* die zweistelligen Länderkennungen usw.). Eine DNS-Domäne entspricht in

der Regel einer Organisation, also zum Beispiel einem Unternehmen, einer Hochschule und so fort. In unseren Beispielen verwenden wir die Beispiel-Domäne *bwv-ahaus.de.*

HINWEIS DNS-Domänen haben nichts mit Windows NT-Domänen zu tun.

Innerhalb einer Domäne besitzt jedes System einen *vollqualifizierten Domänennamen* (FQDN, Fully Qualified Domain Name), der aus dem Host-Namen mit angehängten Domänennamen besteht. Zum Beispiel hieße der Computer *L1119* in unserer Domäne *L1119.bwv-ahaus.de.* Domänen können in *subdomains* unterteilt werden. Daher bezieht sich der Name *viveca.multi.bwv-ahaus.de* auf den Host *viveca* in der Subdomain multi, die sich wiederum in der Domäne *bwv-ahaus.de* befindet, Es sind mehrere Ebenen von Subdomains möglich, sie kommen in der Praxis aber nur selten vor.

Aus der Sicht der DNS-Server werden DNS-Domänen als eine oder mehrere Zonen verwaltet, wobei eine Zone nichts anderes ist, als ein reduzierter Teilbaum der DNS- Domäne. Die Begriffe Domäne und Zone sind in vielen Beschreibungen des DNS- Systems austauschbar. Um die Begriffe klar zu trennen, verwenden wir ausschließlich den letzteren, wenn wir uns auf die Daten beziehen, die verwendet werden, um Host-Namen einer bestimmten Sammlung von Systemen in IP-Adressen umzuwandeln (und umgekehrt). Zonen können weiter unterteilt werden.

***ACHTUNG* Um die Sache weiter durcheinanderzubringen, verwendet das DNS-Verwaltungsprogramm von Microsoft den Begriff "Zonen" für Zonen, während weiter unterteilte Zonen als "Domänen" bezeichnet werden (womit ein ohnehin viel zu häufig benutzter Begriff erneut strapaziert wird).**

2.3.4.1 Einen DNS-Client einrichten

Wir beginnen mit einem Blick auf die Einrichtung eines Rechners, der den DNS-Dienst für die Namensauflösung verwenden soll (wenn dieser über eine *Hosts-Datei* verfügt, wird diese weiterhin abgefragt). Ein DNS-Client wird auch *Resolver* genannt.

Sie können die DNS-Namensauswertung aktivieren, indem Sie im Dialogfenster **Eigenschaften von Microsoft TCP/IP** die Registerkarte **DNS** aufrufen. Die Konfiguration ist einfach.[2] Das Feld Host-Name gibt den Namen des lokalen Computers an. Er entspricht in der Regel dem Computernamen des Rechners. Im Feld Domäne geben Sie den Namen der lokalen Domäne an. Der Bereich Suchreihenfolge des DNS-Dienstes enthält eine Liste von IP-Adressen von DNS-Servern, die zur Namensauswertung in der angegeben Reihenfolge abgefragt werden. Beachten Sie, dass nach einer Antwort eines DNS-Servers kein weiterer gefragt wird, auch wenn der antwortende DNS-Server den Namen nicht auswerten konnte. Der jeweils nächste Server wird also ausschließlich dann gefragt, wenn der aktuelle nicht erreichbar ist.

Standardmäßig nimmt das System an, dass sich Host-Namen in der lokalen Domäne befinden (anders ausgedrückt, der Name der lokalen DNS-Domäne wird an unbekannte Host-Namen angehängt). Im Bereich **Suchreihenfolge für Domänensuffixe** können Sie weitere Domänen angeben, in denen nach Host-Namen gesucht werden soll. Dieses Merkmal wird meistens nicht genutzt, es sei denn, Ihre Domäne befindet sich unterhalb der zweiten Ebene der DNS-Hierarchie. Wenn Sie hier weitere Domänen angeben, wird in der lokalen und in allen hier angegebenen Domänen nach einem unbekannten Host-Namen gesucht. Wenn Sie aber die Liste leer lassen, wird in der lokalen Domäne und allen übergeordneten Domänen nach dem unbekannten Host- Namen gesucht.

2.3.5 Einrichten eines DNS-Servers

Ein Windows NT-Server kann DNS-Dienste anbieten. Installieren Sie dazu auf der Registerkarte **Dienste** der **Systemsteuerung-Netzwerk** den **Microsoft DNS-Dienst.** Es gibt drei Arten von Namens-Servern. Dabei wird die Funktion (*primärer oder sekundärer* Server) für jede Zone unab-

[2] Dieses Dialogfenster enthält genau die Daten, die sich auf UNIX- und anderen Systemen in der Konfigurationsdatei *resolv.conf* befinden.

hängig festgelegt. Alternativ kann der gesamte Server nur für *Zwischenspeicherungen* verwendet werden.

Primärer Server Ein System, das ständig autorisierende Daten über Namen einer bestimmten Zone enthält. Die Zone kann ein lokales Teilnetz, aber auch einen großen Teil des Internets umfassen. Die Zonendaten stellen die Hauptkopie der Konfigurationsdateien dar und enthalten die Zuordnungen von Host-Namen zu IP-Adressen dieser Zone.

Sekundärer Server Ein System, das bei jedem Start Zonendateien von einem primären Server bezieht. Anschließend kann es dieselben Daten wie der primäre Server liefern. Sekundäre Server sollen die Ausfallwahrscheinlichkeit des DNS-Dienstes reduzieren und werden verwendet, um die durch DNS-Clients verursachte Systemlast zu verteilen.

Server nur für Zwischenspeicherungen Ein System, das andere DNS-Server fragen muss, um unbekannte Zuordnungen aufzulösen, sich aber später an erhaltene Antworten erinnern kann. Ein solcher Host arbeitet hauptsächlich als Client, kann aber die Netzwerklast verringern, weil er jede Zuordnung nur ein einziges Mal erfragen muss. Erst wenn der Server neu gestartet wird oder die Zuordnung nach einer bestimmten Zeit ihre Gültigkeit verliert, muss ein zwischenspeichernder- Server erneut einen primären oder sekundären Namens-Server fragen.

Alle DNS-Server speichern die Zuordnungsdaten, die sie während ihrer Arbeit erfahren, zwischen. Diese Daten werden eine bestimmte Zeit lang aufbewahrt und dann aus dem Zwischenspeicher (englisch: Cache) entfernt. Der Cache wird bei jedem Start des DNS-Servers gelöscht.

Ein Windows NT-Server kann jede dieser drei Rollen übernehmen.

Mit dem **DNS-Manager** (den Sie über den Menuepfad **Start--->Progmmme-->Verwaltung (allgemein) >DNS-Manager** oder über den Befehl **dnsadmin** starten können) konfigurieren Sie DNS-Server. Mit diesem Programm können Sie von einem Computer aus alle Microsoft DNS-Server in einem Netzwerk verwalten. Mit Nicht-Microsoft-DNS-Servern kann der DNS-Manager allerdings nicht umgehen.

3 Windows NT Server 4.0

3.1 Allgemeine Einführung

3.1.1 Abgrenzung von Windows NT Workstation und Server

Windows NT 4.0 als Betriebssystem für High-End Workstation und Server wird in Form zweier Produkte mit verschiedenen Ziel- und Einsatzgebieten ausgeliefert. Folgende Eigenschaften besitzen sowohl Workstations als auch Server:

- Auf mehreren Hardware-Plattformen verfügbar
- Preemptives Multitasking und Multithreading

  Windows NT arbeitet mit **preemptivem Multitasking**. Alle ablaufenden Prozesse sind unter vollständiger Kontrolle des Betriebssystems. Unter Windows für Workgroups 3.11 wurde der Prozessor für die Nutzungszeit an das Anwendungsprogramm übergeben (kooperatives Multitasking). Deshalb führte ein Programmabbruch oft zum Totalabsturz von Windows.

  Multithreading: Threads sind einzelne Prozesse innerhalb ein und derselben Anwendung, so z.B. das Öffnen einer Datei, während gleichzeitig das Format einer anderen Datei umgewandelt wird.
- 32-Bit lineares Speichermodell
- Unterstützung bis zu 4 Gigabyte Arbeitsspeicher und 16 Exabyte (10^{15}) Festplattenkapazität
- DOS und 16 Bit Windows Programme können eingesetzt werden; textorientierte OS/2 und POSIX-kompatible Programme werden unterstützt.
- Benutzeroberfläche wie Windows 95/98
- Dateisysteme FAT, HPFS, NTFS
- unter NTFS ausgefeilte Sicherheitsfunktionen
- eingebaute Netzwerkfunktionen im Betriebssystem, Integration in die verschiedenen Netze

Windows NT Workstation ist als Betriebssystem für Arbeitsplätze mit einem hohen Bedarf an Sicherheit und Leistung (z.B. CAD-Stationen, Datenbankservern, Bürosysteme) konzipiert, im Gegensatz zu Windows 95/98, bei dem die Kompatibilität mit bestehender Hardware und Software an erster Stelle stand. In Arbeitsgruppen läßt sich NT-Workstation als Server und als Arbeitsplatzrechner gleichzeitig betreiben. Sind über Netzwerk, ISDN, Datex-P (x.25) und Telefonleitung an NT-Workstation andere Rechner angebunden, so geschieht das mit Hilfe von RAS (Remote Access Service). Ihr privater PC kann über Modem mit dem Bürocomputer verbunden werden. NT-Workstation kann eine solche Verbindung, NT-Server bis zu 256 solche Verbindungen aufbauen.

Die wesentlichen Unterschiede liegen in den Netzwerkeigenschaften verborgen. NT-Server ist ein Serverbetriebssystem für sehr große Netzwerkumgebungen. Durch das erweiterte Domänenkonzept lassen sich große Netze mit vielen Servern strukturieren und mehrere, miteinander verbundene Domänen aufbauen und verwalten.

Der Server bietet gegenüber den Workstation zusätzliche Sicherheit für Festplatten. Plattenspiegelung (RAID 1) und Striping mit Parität (RAID 5) können per Software eingerichtet werden (RAID = Redundant Array of Inexpensive Disks - Kombination von preiswerten Festplatten zur Erhöhung von Speicherplatz, Geschwindigkeit und Ausfallsicherheit). So sind diese Sicherheitsmechanismen auch auf Computern einsetzbar, für die keine Hardwarelösung existiert.

Die bei beiden NT-Versionen mitgelieferte Bandsoftware erlaubt die Sicherung von Daten auf SCSI-Geräten. Ebenso ist eine Unterstützung für USV (unabhängige Stromversorgung) in beiden Versionen enthalten.

Die nachfolgende Tabelle stellt die Eigenschaften von NT-Workstation und NT-Server im Überblick dar:

Leistungsmerkmale	Workstation	Server
Kann als Server im Netz Datei- und Druckerdienste zur Verfügung stellen	Ja	Ja
Server im Peer-to-Peer-Netz	Ja	Ja
Arbeitsstation im Peer-to-Peer-Netz	Ja	Ja, aber nicht sinnvoll
Anmeldeverifikationen in Domänen	Nein	Ja
Replikation	Nur Import	Import und Export
Programme für die Administration von Domänen	Nein (das NT-Serverprogramm läuft aber)	Ja
Maximale Anzahl Sitzungen für RAS	1	256
Fehlertoleranz für Festplatten (Software)	Nein	Ja
Server für Apple-Macintosh	Nein	Ja
Lizensierung	Nein	Ja
Zugriffsrechte-Vergabe	Dateiebene	Verzeichnis- und Dateiebene

3.2 Architektur und Konzepte

Windows NT ist als sicheres Betriebssystem konzipiert, das Anwendungen nicht den direkten Zugriff auf die Hardware gestattet. Dieser Aspekt ist es auch, der bei der Kompatibilität zu bestehenden Anwendungen die größten Schwierigkeiten bereitet. Schauen wir uns das Softwarekonzept des Betriebssystem näher an.

3.2.1 HAL (Hardware Abstraction Layer)

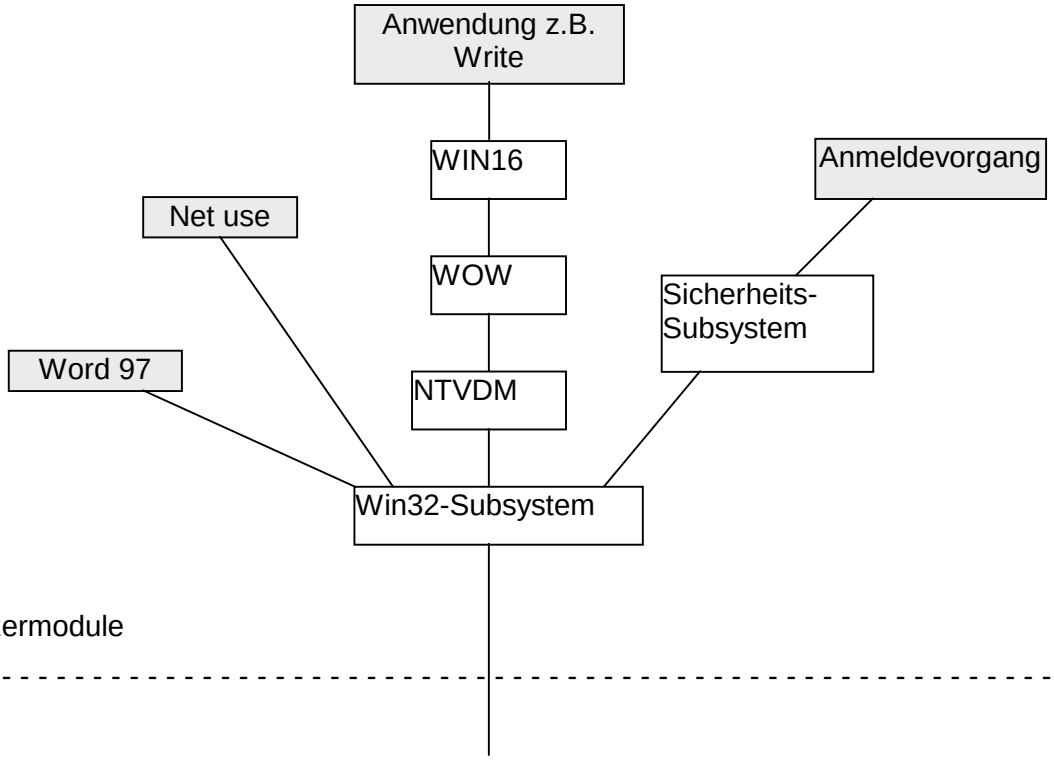
Um eine Austauschbarkeit der einzelnen Hardwarekomponenten zu erreichen sind definierte Schnittstellenkonventionen zwischen dem Betriebssystem und Hardwarehersteller einzuhalten. Die HAL (Hardware Abstraction Layer) verbindet die eigentliche Hardware mit dem Kern des Windows NT- Betriebssystems. Sie schirmt den Kernel von hardwareabhängigen Details der unterschiedlichen Systeme ab. Sie dient zur Abstraktion der Hardware- Schnittstelle (d.h. der virtuellen Darstellung der tatsächlichen gegebenen Hardware). Durch diese zusätzliche Schicht wird auch die Übertragung von Windows NT auf andere Plattformen stark vereinfacht.

Die Windows NT-Komponenten rufen nicht selbst Hardware-Routinen auf, sondern die HAL stellt diese Funktionen bereit, wodurch prozessor- und systemabhängiger Code soweit wie möglich in der HAL konzentriert wird. Jedoch liegen nicht alle hardware-spezifischen Funktionen in der HAL. Alle Geräte, die installiert und wieder entfernt werden können (z.B. Controller, CD-ROMS, Grafikkarten), müssen über Einheitentreiber angesprochen werden. Anwendungen unter DOS oder Windows 9x, die direkt auf diese Hardware zugreifen wollen scheitern an dieser Schicht.

Der Kernel ist der innerste Kern der mehrschichtigen Architektur des Systems. Er kümmert sich um die grundlegenden Operationen von Windows NT. Diese Komponente ist absichtlich klein gehalten worden und ist in ihrer Ausführung extrem effizient. Der Kernel kümmert sich um die Vergabe der Prozessorzeit zwischen, synchronisiert Prozessoren in einer Multiprozessorumgebung, behandelt von der Hardware ausgelöste Ausnahmezustände und implementiert eine Reihe von Funktionen auf niedrigster Ebene, die sich von Plattform zu Plattform unterscheiden.

3.2.2 Windows NT-Executive

Die Windows NT-Executive umfaßt eine Reihe von Subsystemen und Elementen des Betriebssystems, die im Kernel-Modus (oder Protected-Modus) des Mikroprozessors ausgeführt werden. Alle Kernfunktionen des Betriebssystems als eine Reihe von selbständigen Modulen implementiert. Dazu gehören der eigentliche Kernel und die HAL sowie der Objektmanager, der Prozessmanager, der Sicherheitsmonitor, die Verwaltung des virtuellen Speichers, ein Kommunikationsmodul (Local Procedure Calls) und die grafische Anzeige.



Systemdienste						
I/O-Manager Cache-Manager Treiber fürs Dateisystem Netzwerk-Treiber Geräte-Treiber	Objekt-Manager	Sicherheits-Manager	Prozess-Manager	Dienste für Lokale Prozedur-Aufrufe	Verwaltung des virtuellen Speichers	Grafik-Teilsystem Window-Manager Interface für Grafik-Geräte **Grafik-Geräte-Treiber**
	Mikrokernel					
	Hardware Abstaction Layer					
Hardware						

Abbildung 1: Architektur von Windows NT 4.0[3]

Der *Executive* ist in mehrere selbständige Komponenten aufgeteilt, die wiederum für bestimmte Systemdienste zuständig sind. Der Sicherheitskontrollmonitor ("Security Reference Monitor") arbeitet zum Beispiel mit den geschützten Subsystemen zusammen; auf dieser gleichartigen Behandlung beruht das durchgehende Sicherheitsmodell des Systems. Der I/0-Manager, das Ein-/ Ausgabesystem - ebenfalls Teil der Executive - sorgen für Unabhängigkeit von bestimmter Hardware. Alle Prozesse, die mit der Ein- oder Ausgabe von Daten zu tun haben, wie der Cache- Manager, Gerätetreiber und Treiber für Dateisysteme sind Bestandteil des I/0-Managers.

3.2.3 Die Subsysteme

Subsysteme vermitteln zwischen der Windows NT- Executiven und dem Anwendungsprogramm. Mit Hilfe von Subsystemen können ältere Betriebsysteme für das Anwendungsprogramm emuliert werden. Sie tragen also zur Software-Kompatibilität von Windows NT bei. Windows NT verfügt über fünf Subsysteme.

3.2.3.1 CSR-Subsystern

Hier wird die Befehlszeile von Windows NT gesteuert. Das CSR-Subsystem stellt für die anderen Subsysteme die Ein- und Ausgabe von der Konsole bereit.

3.2.3.2 VDM, WOW

Es gibt ein eigenes Subsystem für DOS- oder 16-bit-Windows-Programme. Die Umgebung wird in Form von VDM (Virtual DOS Machine) erzeugt. Auch eine 16-Bit-Windows-Anwendung benutzt eine solche VDM, die dann als WOW (Windows on WIN32) bezeichnet wird.

3.2.3.3 Sicherheitssubsystem

Die mitunter wichtigste Komponente ist das Sicherheitssubsystem. Bei einer lokalen Anmeldung eines Benutzers überprüft es die Anmeldeberechtigung und stellt dessen Berechtigungen im System fest. Ebenso durchlaufen Anmeldungen über das Netzwerk diese Komponente.

3.2.3.4 Die Speicherverwaltung

NT arbeitet mit einem "flachen" 32-Bit-Speichermodell und kann somit vier Gigabyte Speicher direkt adressieren. Dem Betriebsystem steht damit 256 mal soviel Speicher wie Windows 3.11 mit seinen nur 16 MB direkt adressierbaren RAM zur Verfügung.

Die von Windows NT genutzten Schutzmechanismen des Prozessors verhindern die Verletzung des Speicherraumes eines Prozesses durch einen anderen. Der Absturz eines Prozesses kann somit andere Prozesse nicht beeinflussen.

Jedem Prozess stehen mit Hilfe der virtuellen Speicherverwaltung bis zu vier Gigabyte - je 2 Gigabyte für das System und die Anwendung - zur Verfügung. Dieser Speicher muss nicht als physikalischer Arbeitsspeicher existieren, da durch den VMM (Virtual Memory Manager) Speicherinhalte auf die Festplatte ausgelagert werden können.

3.2.3.5 Dateisysteme in Windows NT

Speziell für Windows NT wurde ein neues Dateisystem, das **NTFS** (New Technology File System) entwickelt. Aus Gründen der Abwärtskompatibilität werden andere Dateisysteme ebenso unterstützt.

Merkmal	FAT	VFAT	NTFS

[3] Angelehnt an: www.microsoft.de

Herkunft	MS-DOS	Windows 95	Windows NT
Länge von Datei- und Verzeichniseinträgen	11 Zeichen (8.3)	255 Zeichen	255 Zeichen
Maximale Dateigröße	4 GB	4 GB	16 EB
Maximale Partitionsgröße	4 GB	4 GB	16 EB
Datei-/ Verzeichnisattribute	Einfach	einfach	erweitert
Zugang durch	DOS, OS/2, NT, MINIX	DOS, OS/2, NT, MINIX	Nur Windows NT
Lokale Sicherheit	Nein	Nein	ja

In der E/A-Architektur von Windows NT steuert der I/O-Manager den Einsatz der Dateisystemtreiber. Unter Windows NT können mehrere Dateisysteme, darunter auch bereits eingesetzte Dateisysteme wie FAT, VFAT gleichzeitig aktiv sein. Die Dateisysteme FAT /VFAT werden aus Gründen der Abwärtskompatibilität zu älteren Betriebssystemen wie MS-DOS, Windows 3.x unterstützt.

Das NTFS ist vom Ansatz her ähnlich schlicht wie FAT, ohne die hier gemachten Fehler zu wiederholen. Die wichtigsten Merkmale sind: Zugriffsschutz auf Dateisystemebene, Unterstützung und Unicode, Wiederherstellbarkeit der Daten nach einem Absturz, lange Dateinamen und die Realisierung von POSIX-Forderungen.

Betriebssystem	Anwendungsbereiche
Windows 3.1	Reine 16-Bit-Anwendung. Lauffähig unter MS-DOS-Betriebssystem. Keine Netzwerkfunktionalität
Windows 3.11	Reine 16-Bit-Anwendung. Lauffähig unter MS-DOS-Betriebssystem. Netzwerkfunktionalität beschränkt auf Peer-to-Peer-Netze
Windows 95/98	Sowohl 16-Bit-Anwendungen als auch 32-Bit-Anwendungen laufen auf Computern unter Windows 9x. Volle Netzwerkfunktionalität
Windows NT-Workstation	Eigenständiges Betriebssystem; DOS wird nicht mehr gebraucht. 32-Bit-Anwendungen laufen auf der NT-Workstation. Keine Unterstützung von MS-DOS- und Win16-Gerätetreiber. Die Workstation besitzt volle Netzwerkfunktionalität und dient als Arbeitsstation im Netzwerk. Jedoch kann sie auch sowohl als Dateiserver oder Druckserver im Netzwerk Verwendung finden.

3.2.4 Anmerkung zu Windows NT 3.51 / 4.0

War in der Version 3.51 noch die Ansteuerung der Grafikkarte Aufgabe des I/O-Managers, haben sich die Entwickler von Mikrosoft bei Windows NT 4.0 dazu entschlossen die Grafiktreiber direkt auf die Hardware zugreifen zu lassen. In der Version 4.0 wird der gesamte Treiber im Kernel-Modus ausgeführt. Dies erlaubt eine höhere Verarbeitungsgeschwindigkeit und reduziert die Anzahl der Umschaltungen des Prozessormodus zwischen Kernel-Mode und User-Mode.

Für die Grafikkartenhersteller bedeutet dies, dass neue Kernel-Modus-GDI-Treiber für NT4.0 hergestellt und bereitgestellt werden werden müssen.

4 Die Struktur eines Windows NT-Netzes

Ein Computer unter Windows NT arbeitet entweder in einer Arbeitsgruppe oder in einer Domäne.

4.1 Was ist eine Arbeitsgruppe?

Eine Arbeitsgruppe ist eine logische Gruppe, die in der Regel nicht mehr als 10 Computer umfaßt. Als Teil einer Arbeitsgruppe besitzt **jeder Computer** unter Windows NT eine eigene Verzeichnisdatenbank. Ressourcen und Benutzerkonten werden auf jedem Computer der Arbeitsgruppe verwaltet (lokale Konten).

Die dezentrale Verwaltung der Benutzerkonten erfordert zwar kaum Planungsarbeiten, ist aber nur für sehr begrenzte Netzwerke mit nicht mehr als 10 Computern praktikabel.

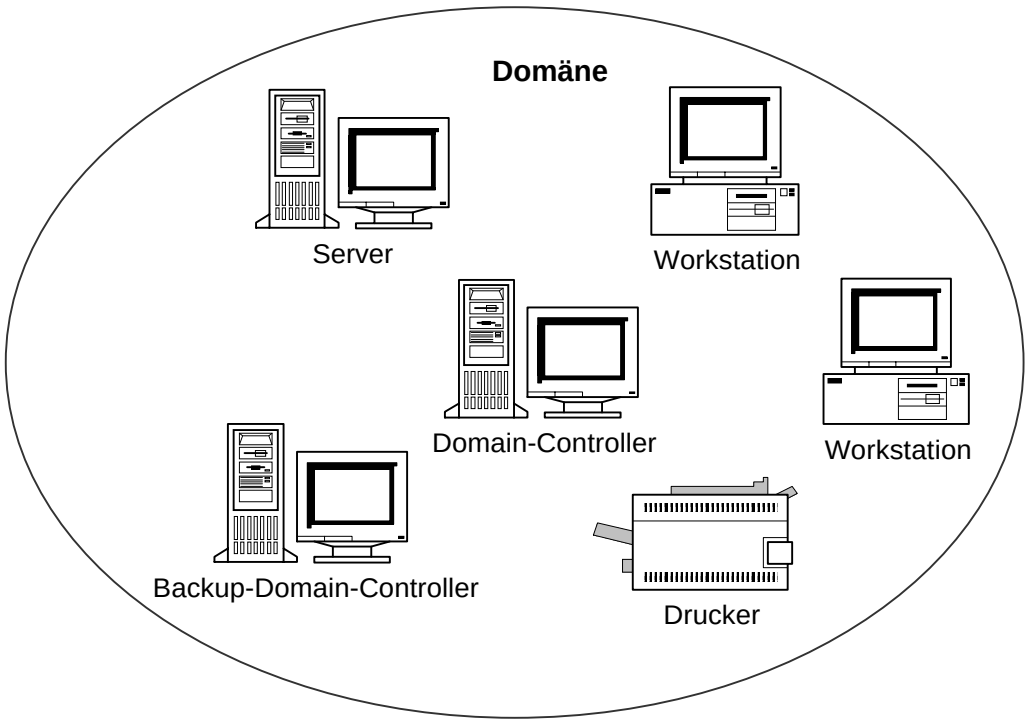
4.2 Was ist eine Domäne?

Eine Domäne ist eine Zusammenfassung von vernetzten Computern, die in einer **gemeinsamen Verzeichnisdatenbank** verwaltet werden. In der Domäne wird die Netzwerkverwaltung zentral vom primären Domänen-Controller (PDC, Primary Domain Controller) durchgeführt. Auf diesem Windows NT Server liegt die Datenbank der Benutzer- und Gruppendefinitionen mit den zugewiesenen Berechtigungen und Richtlinien ”im Original”. Er verwaltet auch die anderen in der Domäne definierten Windows-NT Server und Workstations.

So ergeben sich 2 Vorteile des Domänenkonzepts:

- Der Administrator muss nur ein Konto pro Benutzer verwalten
- Der Benutzer kann mit einer Anmeldung alle Daten, Drucker und andere Ressourcen erreichen, für die ihm Berechtigungen gegeben wurden.

3.2.1 Aufbau einer Domäne



Die Datenbank der Benutzerkonten, der Gruppen und der Berechtigungen befindet sich im Original auf dem Domän-Controller (PDC) und als Kopie auf dem Backup-Domain-Controller (BDC).

Ein Windows-NT-Server kann in einer von 3 möglichen Rollen arbeiten. Einfacher alleinstehender Server, Sicherungs-Domänen-Controller und primärer Domänen-Controller. Die beiden Typen des Domänen-Controllers können Ihre Rolle tauschen. Soll ein Server zum Domänen-Controller werden oder umgekehrt, oder soll ein Domänen-Controller in eine andere Domäne wechseln, so ist er neu zu installieren.

Einer oder mehrere Sicherungs-Domänen-Controller erhalten eine ständig aktualisierte Kopie der Benutzerdatenbank. Sie unterstützen den primären Domänen-Controller bei Anmeldevorgängen und dienen als Sicherheit bei dessen Ausfall.

Es muss nicht unbedingt ein Sicherungs- Domänen-Controller definiert und installiert werden. Sollte kein BDC definiert sein, so wird automatisch die erste Arbeitsstation, die sich an der Domäne anmeldet, vom Prirnary-Domain-Controller als Backup-Controller benannt und mit einer Kopie der Benutzerdatenbank versorgt. Dabei ist es völlig egal, mit weichem Windows-Betriebssystem diese Station arbeitet. Es kann also auch ohne weiteres passieren, dass eine WfW-Station zuerst einmal diese Aufgabe übernimmt. Diese Arbeitsstation behält diese Aufgabe solange, bis sich eine Workstation mit einem als höherwertig angesehenen Betriebssystem (Windows 95, Windows-NT-Workstation) an der Domäne anmeldet. Es kommt dabei nicht darauf an, mit weichen Hardwareressourcen die Station ausgestattet ist, einzig und allein das Betriebssystem ist entscheidend.

Ein definierter Sicherungs-Domänen-Controller kann durch Auswahl des Menüpunkts [Heraufstufen zum primären Domänen-Controller] im Menü [Computer] des Server-Managers zum primären Domänen-Controller erklärt werden.

Ein definierter Server kann durch Auswahl des Menüpunkts [Heraufstufen zum Sicherungs-Domänen-Controller im Menü [Computer] des Server-Managers zum Sicherungs- Domänen-Controller erklärt werden.

3.2.2 Vertrauensstellungen und Domänenmodelle

Mit Windows-NT-Domänen wurde ein Domänen-Konzept eingeführt, das Vertrauensstellungen mehrerer Domänen zueinander ermöglicht. Mit diesen Vertrauensstellungen wird die Nutzung von Ressourcen über die Grenzen von Domänen hinweg deutlich vereinfacht und die zentrale Verwaltung auch großer Netze mit einer Vielzahl von Domänen ermöglicht. Große, unternehmensweite Netze sollen mit diesem Konzept aufgebaut werden können, ohne dass der Verwaltungsaufwand ausufert. Vertrauensstellungen zwischen den Domänen dienen der Vereinfachung von administrativen Aufgaben. Ressourcen können in einer oder mehreren Domänen zusammengefaßt werden, während die Benutzerkonten in einer übergeordneten Domäne eingerichtet sind, der die Ressourcendomänen vertrauen. Die Datenbank der Benutzer und Gruppen können so in einer zentralen Domäne zusammengefaßt werden und müssen so nicht mehrfach definiert und verwaltet werden.

Die Anmeldung eines Benutzers wird über die Vertrauensstellungen weitergegeben. So kann die Anmeldung in der Resourcendomäne erfolgen, wird aber von der übergeordneten Domäne verifiziert.

Die Vertrauensstellungen können einseitig oder beidseitig sein, wobei beidseitiges Vertrauen als zwei einseitige Vertrauensstellungen eingerichtet werden, von einer Domäne zur anderen und umgekehrt. Damit lassen sich nun folgende 4 Domänenmodelle konstruieren:

- Single Domain Modell
- Master Domain Modell
- Multiple Master Modell
- Complete Trust Domain Modell

Welches dieser Domänenmodelle einsetzbar ist, hängt von der Größe und der Struktur des Netzes und der Unternehmensorganisation ab. Folgende Punkte entscheiden über das zu wählende Modell:

- Anzahl der Benutzer
- Firmenstruktur (Niederlassungen und Abteilungen)

- Berechtigungsstruktur für die Ressourcen
- Nutzungsgewohnheiten und -erfordernisse

Die Domänenmodelle müssen in der Praxis nicht exakt nach einem bestimmten Modell ausgelagert sein, sie lassen sich für konkrete Netzumgebungen auch mischen. Gemeinsam ist allen Domänenmodellen, dass ein Benutzerkonto im Netz nur ein einziges Mal vorliegt. Die Konzepte und Details der Benutzer- und Gruppenverwaltung in Domänen werden später erläutert.

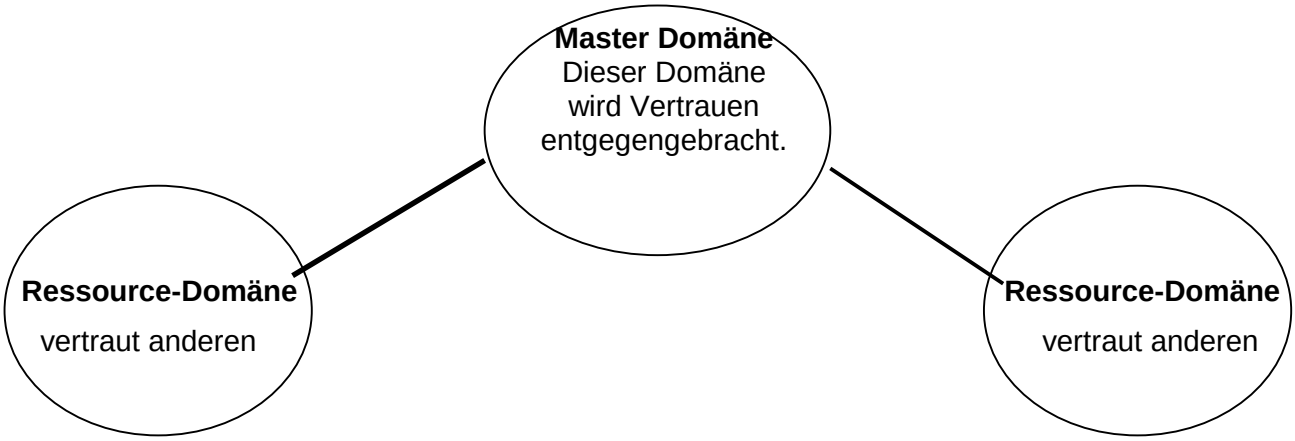
4.2.1.1 Single - Domain - Modell

Hier existiert nur eine Domäne, es gibt keine Vertrauensstellungen zu anderen Domänen, Dieses Modell kann eingesetzt werden,

- wenn die Zahl der Benutzer begrenzt ist und
- keine organisatorischen Gründe für eine Aufteilung vorliegen.

Die Administration eines Netzes, das nach diesem Modell arbeitet ist einfacher, als bei den Modellen mit Vetrauensbeziehungen. Wird ein großes Netz mit vielen Servern und Benutzern so eingerichtet, kann es zur Überlastung des PDC führen und die Netzbelastung stark zunehmen kommen. Die Grenze ist nicht klar zu ziehen, da Zahl und Ausstattung der Server und deren Belastung ausschlaggebend sind.

4.2.1.2 Master - Domain - Modell



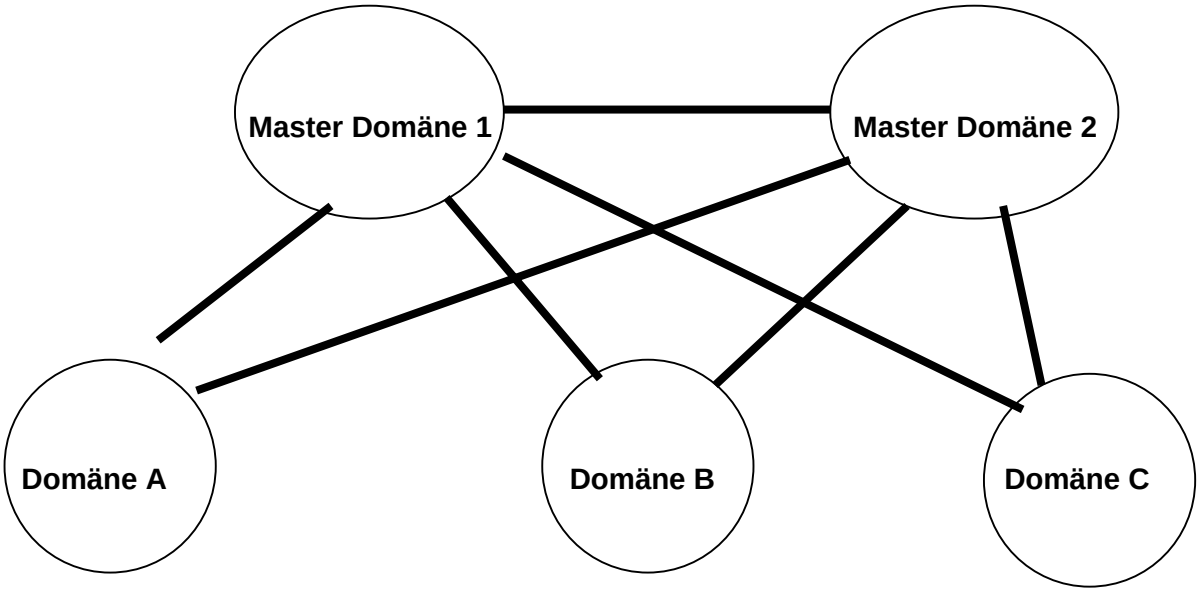
Im Master-Domain-Modell liegen die Benutzerkonten auf einer übergeordneten Domäne. Weitere Domänen stellen die Ressourcen im Netz zur Verfügung und vertrauen der übergeordneten Domäne. Durch diese Vertrauensstellung können die zentral eingerichteten Benutzer die Ressourcen wie Daten und Drucker verwenden, ohne dass die Konten mehrfach angelegt und verwaltet werden müssen.

Die Vertrauensstellungen werden nur in eine Richtung aufgebaut. Diese richten sich von den Ressourcen-Domänen zur übergeordneten Domäne. Das Master-Domänen-Modell erlaubt die Strukturierung der Ressourcen im Netz in mehreren Domänen bei gleichzeitiger zentraler Administration und kann bis zu einer Zahl von ca. 15.000 Benutzern eingerichtet werden.

4.2.1.3 Multiple - Master - Domain - Modell

Das Modell eignet sich für sehr große Netze mit mehr als ca. 15.000 Benutzern, die dennoch zentral administriert werden sollen. Aus Gründen der Leistungsfähigkeit muss bei so großen Netzen mehr als eine übergeordnete Domäne eingerichtet werden. Durch die Konstruktion nach dem Multiple-Master-Modell werden große Netze skalierbar, bei weiterhin zentraler Administration.

Die Vertrauensstellungen dieses Modells sind von den Ressource-Domänen zu allen übergeordneten Domänen und als beiderseitiges Vertrauen zwischen den Masterdomänen einzurichten.

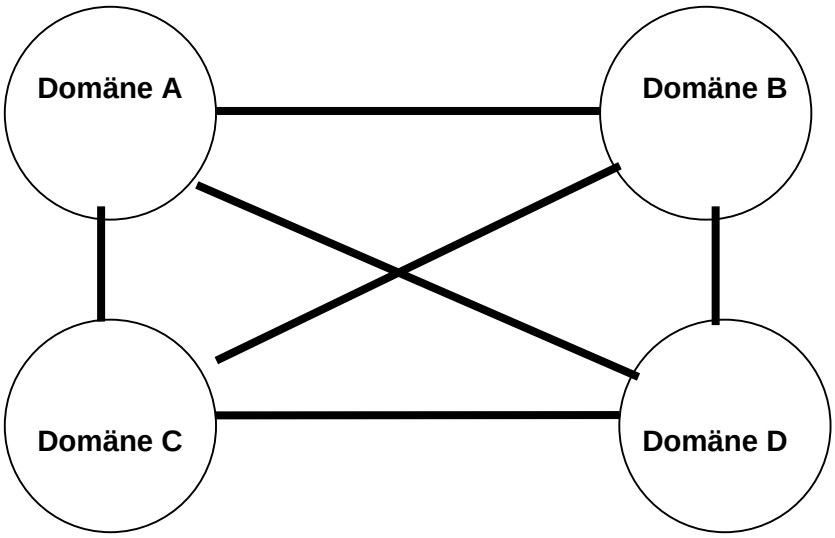


Dieses Modell hat die gleichen Vorteile wie das einfache Mastermodell, (logische Ressourcenanordnung und zentrale Administration). Es hat natürlich auch Nachteile gegenüber kleineren Modellen, die auf die größere Zahl der zu verwaltenden Vertrauensstellungen beruhen.

Vorteile:
- zentrale Administration
- Administration von Ressourcen auch innerhalb von Abteilungs-, Niederlassungsdomänen
- logische Ressourcenanordnung möglich
- mit beliebiger Zahl von Benutzern einrichtbar

Nachteile:
- mehrfache Definition von Gruppen nötig
- Viele Vetrauensstellungen
- Aufteilung der Benutzerkonten auf mehrere Domänen nötig.

4.2.1.4 Complete - Trust - Domain - Modell



Das Complete Trust Domain Modell ist nicht auf zentralisierte Administration mehrerer Domänen ausgerichtet. Es ermöglicht dagegen den Zugriff auf Ressourcen in beliebigen Domänen innerhalb des Netzes, obwohl alle Domänen die Administration selbst handhaben. Keine der Domänen

ist einer anderen übergeordnet. Vertrauensstellungen sind immer zweiseitig. Auch in diesem Modell wird ein Benutzerkonto nur einmal definiert.

Es ist geeignet für Netzstrukturen, die eine Gruppierung von Benutzern und Ressourcen mit jeweils eigener Verwaltung erfordern. Beispielsweise könnten sich Unternehmen mit weitgehend selbständigen Abteilungen oder Niederlassungen für dieses Modell entscheiden, wenn keine zentrale Verwaltung des Netzes vorgesehen ist.

Das Netz kann sehr hohe Benutzerzahlen beinhalten, ist also weitgehend skalierbar.

Nachteilig sind die hohe Anzahl von Vertrauensbeziehungen, die zwischen allen Domänen eingerichtet und verwaltet werden müssen. Alle Vertrauensstellungen müssen dabei zweiseitig sein.

Die Struktur dieses Netzes erfordert es, dass zumindest die Einrichtung von Benutzern abgesprochen werden muss. Mehrfache Anlage des gleichen Benutzernamens in zwei oder mehr Domänen kann zu Unklarheiten bei der Rechtezuweisung führen.

4.2.2 Einrichten von Vertrauensstellungen

Wenn Sie eine Vertrauensstellung zwischen Domänen einrichten, vertraut die eine Domäne (**die vertrauende Domäne**) der anderen (**der vertrauten Domäne**).

Diese Beschreibungen werden konkreter, wenn Sie sich vorstellen, dass die vertrauende Domäne eine Domäne mit Ressourcen wie z.B. Druckern, Faxgeräten etc. ist, und die vertraute Domäne die User beinhaltet, denen vertraut werden kann. Also, die vertrauende Domäne sagt: "Ich vertraue den Usern aus der vertrauten Domäne, dass sie meine Ressourcen vernünftig benutzen." In den Bildern zeigen die Pfeile immer von der vertrauenden Domäne zu der vertrauten Domäne (die ja auch dann die Userkonten beinhaltet).

Das Einrichten von Vertrauensstellungen erfordert eine sorgfältige Planung. Folgende Aspekte sollten vor dem Einrichten berücksichtigt werden:

- Vertrauensstellungen können nur in WINDOWS-NT-Servern eingerichtet werden,
- Die Anzahl der einseitigen Vertrauensstellungen muss festgelegt werden. Sollen beispielsweise vertraute Domänen auch vertrauende Domänen sein (und umgekehrt)?
- Der physikalische und logische Aufenthaltsort von Benutzern ist nicht von Bedeutung. Wichtig ist lediglich der Speicherort ihrer Konten. Solange ein Benutzer ein Konto in der vertrauten Domäne unterhält, kann er sich von einer beliebigen Domäne aus anmelden, die über eine Vertrauensstellung mit der Kontendomäne verbunden ist. Mit anderen Worten: Benutzer können sich von einer beliebigen vertrauenden Domäne aus anmelden, solange sie sich an der vertrauten Kontendomäne anmelden.

Für die Einrichtung einer einseitigen Vertrauensstellung sind 2 Schritte erforderlich:

- Die vertraute Domäne gestattet der anderen, ihr zu vertrauen
- Der vertrauenden Domäne muss die vertraute Domäne hinzugefügt werden.

Vorgehensweise:

Name der Ressource-Domäne: DruckDomäne

Name der Kontendomäne: UserDomäne

Der Administrator der Domäne UserDomäne wählt aus dem Menü **Richtlinien** den Befehl **Vertrauensstellungen**. Das nun geöffnete Fenster besteht aus 2 Teilen. Im unteren Teil unter "Berechtigt, dieser Domäne zu vertrauen" wählt er den Menübefehl: "hinzufügen" und trägt dann den Namen der Ressourcendomäne "DruckDomäne" ein.

Anschließend öffnet der Administrator der **Domäne DruckDomäne** das Menü **Richtlinien** und den Befehl **Vertrauensstellungen** und wählt aus dem oberen Teil unter **Vertraute Domänen** den Befehl **Hinzufügen**. Dort trägt er den Namen **UserDomäne** ein.

Diese Reihenfolge ist unbedingt einzuhalten, da sonst die Einrichtung von Vertrauensstellungen erst nach frühestens 15 Minuten wirksam wird.

3.3 Benutzer-Konten

Die Verwaltung von Benutzer-Konten ist eine der am häufigsten zu erledigenden Arbeiten von Systemadministratoren. Aus Sicht des Systems muss ein Benutzer-Konto sich nicht unbedingt auf eine tatsächlich existierende Person beziehen auch wenn dies in den meistens der Fall sein wird. Ein Benutzer-Konto ist eine Einheit, die Dateien besitzen und Programme ausführen kann. Zum Beispiel können einige Benutzer-Konten lediglich existieren, um Dateien zu besitzen, die von anderen Anwendungen oder von Teilsystemen zum Informationsaustausch benötigt werden.

Windows NT kennt drei Typen von Benutzer-Konten, die in der Dokumentation und in Programmen als

"**globale Konten**"

"**lokale Konten**" und

"**Benutzer-Konten**"

bezeichnet werden. Die Unterschiede werden klarer, sobald man weiß, dass es zwei Benutzer-Umgebungen gibt:

- die der Domäne und
- die von isolierten, einzelnen Computern

In einer Domäne gibt es zwei Typen von Benutzer-Konten. Normalerweise bekommen Benutzer **globale Konten**. Diese werden von allen Systemen in der Domäne und in vertrauten Domänen erkannt und sind auf allen diesen Systemen gültig. Globale Konten erkennen Sie in der Benutzerverwaltung an einer **Person, die ein Hemd mit Kragen** trägt.

Der andere Kontotyp stellt die **lokalen Konten** dar. In der Benutzerverwaltung sind diese durch eine **Person mit Hemd und Kragen und einem Monitor** daneben zu erkennen. Auch diese haben Zugriff auf Computer und Ressourcen **in der Domäne**, allerdings nur in dem Rahmen, der diesen Benutzern gewährt wird. Diesen Konten kann nicht durch die Einräumung von Vertrauensstellungen Zugriff auf Systeme anderer Domänen gewährt werden.

Einzelne Computer, die weder ein primärer noch ein Sicherungs-Domänen-Controller sind, besitzen zusätzliche **Benutzer-Konten**, die nur auf dem lokalen System gelten. Solche Konten werden nicht einmal in der Domänenumgebung erkannt, also bei der Anmeldung an die Domäne.

Das Feld Domäne im Dialogfenster Anmeldeinformationen gibt an, wo das Konto gesucht werden soll. Wenn Sie hier eine Domäne auswählen, muss der angegebene Benutzername als globales Konto in dieser Domäne existieren (mit einem lokalen Konto können Sie sich nicht interaktiv anmelden). Wenn Sie aber im Feld Domäne den Computernamen auswählen, wird der Benutzername als lokales Konto dieses Computers gewertet (Konten der Domäne werden in diesem Fall nicht erkannt).

3.4 Benutzer-Gruppen

NT-Gruppen sind Sammlungen von Benutzern, denen identische Zugriffsrechte gegeben werden können. Windows NT kennt drei Arten von Gruppen:

- **Globale Gruppen**, die in der Domäne erkannt werden und denen in ihrer eigenen Domäne sowie in vertrautenden Domänen Zugriff auf Computern und Ressourcen gewährt werden kann (Benutzermanager: zwei Personen neben Globus)
- **Lokale Gruppen**, die nur in ihrer Heimatdomäne erkannt werden und denen nur in dieser Domäne Zugriff auf Ressourcen gewährt werden kann. Wie lokale Benutzer, werden diese Gruppen niemals von anderen Domänen erkannt. Gültige Mitglieder sind Benutzer-Konten aus der lokalen und jeder vertrauten Domäne. Außerdem können globale Gruppen der lokalen Domäne Mitglied einer lokalen Gruppe sein; umgekehrt ist das allerdings nicht möglich. (Benutzermanager: zwei Personen neben Monitor).

- Gruppen die lokal auf einem ”nicht-PDC/BDC” Computer existieren und nicht in der Domäne erkannt werden.

Welche Benutzer-Konten hat Windows NT während der Installation auf dem Server und der Workstation eingerichtet?

Start-Programme-..... - .....

Benutzerkonto	Server	Workstation

Welche vordefinierten Gruppen hat Windows NT während der Installation auf dem Server und der Workstation eingerichtet?

Start-Programme-..... - .....

Globale Gruppe	Server	Workstation
Lokale Gruppe		

5 Die Installation

5.1 Installationsvoraussetzungen

5.1.1 Kompatible Hardware

Windows NT stellt sehr hohe Anforderungen an die Kompatibilität von Hard- und Software. Dieses hat zur Folge, dass Windows NT nicht auf jedem Rechner lauffähig ist, obwohl die Leistungsmerkmale eigentlich ausreichen. Zum Programm Windows NT gibt die Firma Microsoft eine Liste heraus, die alle Geräte enthält, die von Microsoft auf Kompatibilität zum Programm Windows NT getestet wurden. Diese **Hardware Kompatibilitätsliste (HCL)** liegt jedem Programmpaket von Windows NT bei und kann aktuell über das Internet (z.B. http://www.paperbits.com/) eingesehen und heruntergeladen werden.

Bei der Neubeschaffung von Rechnern sollte man in der Ausschreibung darauf achten, die NT-Tauglichkeit zu fordern oder ausschließlich auf Komponenten bestehen, die in der HCL stehen. Dieses ist jedoch nicht immer möglich. Wegen des häufigen Wechsels von Rechnermodellen und der Kosten für eine Überprüfung, verzichten viele Hersteller und Anbieter auf einen offiziellen Test der Geräte. In diesem Fall sollte man sich vom Lieferanten schriftlich bestätigen lassen, dass alle Komponenten des Rechners und der Rechner insgesamt unter Windows NT lauffähig sind.

5.1.2 Ausreichende Hardware

Windows NT ist auf verschiedenen Rechnerplattformen ablauffähig. Die Firma Microsoft gibt Mindestvoraussetzungen für die Installation an, die sich in der Praxis aber als zu gering erwiesen haben. Sinnvoll ist die Installation von NT nur auf neuen PC mit PCI-Bus, Pentium Prozessor, schneller (SCSI für Server) Festplatte und ausreichend Hauptspeicher. Unten aufgeführt sind einige Anforderungen für die Installation von Windows NT auf INTEL-Basis. Für Rechner mit RISC-Prozessoren gelten zum Teil deutlich höhere Anforderungen.

	Mindestanforderungen:	**Empfehlung**
Bussystem	ISA-Bus	PCI-Bus
Prozessor	INTEL 80486 DX - 25 MHz oder kompatibel	INTEL Pentium
Hauptspeicher	12 MB	32 MB
Controller	jeder gängige Controllertyp	EIDE oder SCSI
Festplatte	ca. 120 MB freie Speicherkapazität	500 MB eigene Partition
Grafik	VGA Grafikkarte und kompatibler Monitor	SVGA Grafikkarte, Color-Monitor mit 800*600 Punkten
Zubehör	CD-ROM-Laufwerk für lokale Installation oder Netzwerkkarte bei Netzinstallation	s.a.S.
Optional	Maus, Trackball etc.	s.a.S.

5.2 Vorbereitung der Installation

5.2.1.1 1. Informationen über die Hardware

Windows NT ist nicht "Plug-And-Play"-fähig. Im Rahmen der Installation werden verschiedene Komponenten zwar automatisch erkannt, in Problemfällen ist es jedoch erforderlich, genaue Informationen über die eingebauten Karten und die Einstellungen der Karten zu haben.

5.2.1.2 2. Beschaffung von Treibern

Im Lieferumfang von Windows NT sind verschiedenste Treiber für unterschiedliche Hardwarekomponenten enthalten. Für Hardwarekomponenten, die Windows NT nicht kennt oder nicht voll unter- stützt, benötigt man einen Treiber des Hardwareherstellers oder des Lieferanten. Dieser Treiber muss speziell auf die Hardware und auf das Betriebsystem Windows NT Version 4.0 abgestimmt sein und arbeitet oft nur mit dem neuen Service Pack (z.Z. 5-6). Treiber für ältere Windows NT- oder andere Windows-Versionen (Windows 9x, 3.11) können nicht eingesetzt werden.

5.2.1.3 3. Bereitstellung der Installationsmittel

Für die Standardinstallation von Windows NT benötigt man 3 Setup-Disketten, die CD-ROM und eine leere 3 *1/2*" Diskette. Treiber für spezielle Hard- und Software müssen bereitstehen.

5.2.1.4 4. Einstellungen im BIOS

Virus Protection	Verschiedene BIOS-Versionen ermöglichen einen automatischen Schutz gegen Bootviren. Dazu wird der Bootblock der Festplatte ständig überprüft und vor etwaigen Veränderungen geschützt. Diese Einstellung muss **deaktiviert** werden, da das Installationsprogramm von Windows NT Informationen in diesen Bereich schreibt.
Bootreihenfolge	Für eine Standardinstallation muss die **Bootreihenfolge A - C**. lauten. Bei einer Netzwerkinstallation müssen hier keine Einstellungen getroffen werden.
Zugriff auf Diskette	Während der Installation muss der Anwender lesend und schreibend auf das Disketten- Laufwerk A: zugreifen.

5.2.1.5 5. Organisatorische Vorüberlegungen

Windows NT fragt bei der Installation folgende Punkte ab:

Rechnernamen	PC??
Druckernamen	LEXM_R1119
Administratorkennwort	Schreiben Sie sich Ihr Kennwort unbedingt auf. Bedenken Sie, dass zwischen Groß- und Kleinschreibung unterschieden wird. Sollten Sie Ihr Passwort einmal vergessen, gibt es keinen Ausweg als die Neuinstallation!
IP-Adresse	192.168.119.2??
Subnetzmaske	255.255.255.000
Arbeitsgruppe	Vorschlag: Hund, Katze, Maus

Diese Einstellungen müssen organisationsweit festgelegt werden.

5.2.1.6 6. Vorbereitung der Festplatte

Eine Vorbereitung der Festplatte (Partitionierung und Formatierung) ist nur bei der Netzwerkinstallation erforderlich.

5.3 Das Kommando WINNT

WINNT [/S[:]Quellpfad] [/T[:]TempLW] [/I[:]INF-Datei] [/O[X]] [/X | [/F] [/C]] [/B] [/U[:Skriptdatei]] [/R[X]:Verzeichnis] [/E:Befehl]

Parameter	Bedeutung
/S[:]Quellpfad	Gibt den Ort der Windows NT-Quelldateien an. Der Pfad muss in folgender Form vollständig angegeben werden: \Pfad oder \\Server\Freigabe\Pfad Die Standardeinstellung ist das aktuelle Verzeichnis.
/T[:]TempLW	Bestimmt ein Laufwerk, das die temporären Setup-Dateien enthält. Falls nicht angegeben, wird Setup ein Laufwerk für Sie bestimmen.
/I[:]INF-Datei	Bestimmt den Dateinamen der Setup-Informationsdatei (ohne Pfadangabe). Die Standardeinstellung ist DOSNET.INF
/C	Überprüfung des verfügbaren Setup-Diskettenspeicherplatzes auslassen
/B	Installation ohne Disketten - erfordert /S
/U[:Skriptdatei]	Unbeaufsichtigte Installation und optionale Skriptdatei - erfordert /S
/R:Verzeichnis	Optionales Verzeichnis erstellen
/RX:Verzeichnis	Optionales Verzeichnis kopieren
/E:Befehl	Befehl, der am Ende des Installationsteils im GUI-Modus ausgeführt wird (GUI=grafische Benutzeroberfläche)
/F	Keine Überprüfung von Dateien beim Kopieren auf die Setup-Disketten.
/X	Keine Setup-Disketten erstellen
/OX	Setup-Disketten für CD-ROM-Installation erstellen.

5.4 Die vollständige Installation über Disketten, CD oder Netzwerk

Die ersten beiden Installationsmöglichkeiten beziehen sich auf die mitgelieferten Disketten und die CD. Dabei sind folgende Punkte zu unterscheiden:

a) ob auf Ihrem Rechner bereits ein Betriebsystem installiert ist,

b) ob Ihre Festplatte noch unformatiert ist oder vielleicht Partitionen enthält

c) ob ihr Rechner an ein Netzwerk angeschlossen werden kann.

zu a)

Entscheiden Sie zuerst, ob Sie das installierte Betriebssystem behalten wollen. Bei MS-DOS ist zu beachten, dass nach Umstellung auf das Dateisystem NTFS (und nur mit diesem System besitzen Sie die unter NT angestrebte Sicherheit) MS-DOS nicht mehr gestartet werden kann, falls die Root-Partition NTFS ist. (Vielleicht müssen Sie ihre Platte neu partitionieren, dann schauen sie unter Punkt b: nach).

Wenn Sie auf das CD-Laufwerk zugreifen können, starten Sie Ihren Rechner und legen Sie die CD ins Laufwerk ein. Wechseln Sie auf das CD-Laufwerk und dort in das Verzeichnis i386.

Installieren Sie mit Hilfe des Kommandos WINNT /Parameter.

Können Sie nicht auf das CD-Laufwerk zugreifen, dann legen Sie die erste der drei mitgelieferten Disketten ins Laufwerk A: ein. Schalten Sie danach den Rechner an und folgen Sie nun den Anweisungen des Installationsprogramms.

zu b)

Sollte Ihre Festplatte unformatiert sein, dann legen Sie die erste der mitgelieferten Disketten ins Laufwerk A: und schalten dann den Rechner ein. Sie werden im Zuge der Installation gefragt, ob und wie sie die Festplatte partitionieren wollen. Die Partition, die NT aufnehmen soll, muss mindestens 130 MB groß sein.

Ist Ihre Festplatte bereits partitioniert, so ist es egal, in welcher Partition Sie NT installieren. Sie sollten jedoch vermeiden, NT in eine erweiterte MS-DOS-Partition zu installieren. Dies hat zwar keine Auswirkungen auf das Ablaufverhalten von NT, sollten Sie jedoch gezwungen sein, NT zu deinstallieren, und haben sie unter NT das NTFS-Dateisystem eingerichtet, ist es mit Hilfe des MS-DOS-Befehls FDISK nicht möglich, NT aus dem System zu entfernen. Sie müssen dann einen anderen Partitionsmanager verwenden.

zu c)

Rechner mit einer Netzwerkkarte können mit Hilfe von Client-Software (befindet sich auf der Server-CD von NT) Ihren Rechner mit einem Server oder mit einem anderen Rechner verbinden. Auf diesem Fremdrechner muss entweder das CD- Laufwerk oder ein Verzeichnis, welches die CD enthält, freigegeben sein. Verbinden Sie sich mit diesem Laufwerk und beginnen sie entweder die Installation durch Eingabe von WINNT /Parameter oder kopieren Sie über das Netz das Unterverzeichnis i386 (bei INTEL-Prozessoren) auf Ihre lokale Platte und beginnen dann mit der Installation.

5.5 Der Ablauf der Installation

Der Ablauf der Installation ist fast identisch mit dem Ablauf der Installation einer Workstation. Allerdings gibt es während der Installation die Aufforderung zu entscheiden, ob sie einen Server, einen Backup-Domain-Controller oder einen Primary-Domain-Controller installieren wollen. Server und Backup können selbstverständlich nur installiert werden, wenn es bereits einen Primary-Domain-Controller gibt, da zur Installation das Kennwort des Domänenadministrators benutzt werden muss. Auch muss der Primary-Domain-Controller im Netz aktiv sein, ehe man die Installation der beiden anderen Geräte durchführen kann. (Die Aufgaben der verschiedenen Rechner werden noch erklärt). Deswegen kann man auch keinen der "Server" ohne Netzwerk installieren.

Neben eindeutigen Rechnernamen muss bei der Installation eines Primary-Domain-Controllers auch ein eindeutiger Domain-Name vergeben werden. Da Backup und Server nach der Primary-Installation erst eingerichtet werden können, gehören sie zwangsläufig zu ein- und derselben Domäne und können nicht einfach aus der einen Domäne in eine andere gebracht werden. Ist dies erforderlich, so müssen Backup oder Server in der anderen Domäne neu installiert werden.

5.5.1 Der Ablauf der Installation am BWV Ahaus

Im Vorfeld der Installation wurden folgende Arbeiten bereits geleistet:

- Einrichten einer Partition von 600 MB mit fdisk
- Formatieren der Festplatte: format C: /S
- Kopieren elementarer Betriebssystemdateien von Windows 9x und der für das Netz erforderlichen Software (Novell Client), um eine Verbindung zum Server herzustellen.
- Kopieren der Windows-NT-Installationsdateien vom Server bzw. von der NT-CD-Rom aus dem Verzeichnis I386 auf die lokale Festplatte. Dabei wurde unterschieden zwischen den Versionen Windows-NT Server (\i386sv) und Windows-NT Workstation (\i386ws).

Folgende Anweisungen bzw. Angaben sind bei der Installation vorzunehmen:

5.5.2 INITIALISIEREN der Installation

1) Lock c: sorgt dafür, dass zum Zeitpunkt der Installation kein anderes Programm auf die Festplatte zugreift.

2) Winnt /S:\i386[sv, ws] /B /X - nach dem Start werden die Dateien ausgepackt und in ein temporäres Verzeichnis kopiert, anschließend erfolgt ein Neustart

3) Soll Windows NT aktualisiert werden? **Nein**

4) **Hardware-Erkennung** wird durchgeführt und muss **bestätigt** werden. Höherwertige Grafikkarten müssen nachträglich konfiguriert werden.

5) **Lizenzvereinbarung** zustimmen

6) Angabe der Partition, auf der Windows NT installiert werden soll. Erstellen Sie eine **neue Partition mit 600 MB**

7) Angabe des Dateisystems, auf dem Windows NT installiert werden soll: Installation auf die neue **600 MB Partition unter NTFS,** FAT bestehen lassen, nicht konvertieren nach NTFS

8) Angabe des Ordners für Windows NT: **\WINNT** - anschließend werden die Dateien aus dem temporären Verzeichnis in den WINNT-Ordner kopiert

9) Computer wird neu gestartet

Vom Setup-Assistenten angeforderte Information	Windows NT Workstation	Windows NT Server
Installationsart (Standard, Laptop, Minimal oder Benutzerdefiniert)	Wählen Sie eine Installationsart aus. Standard	-
Name und Firma des Lizenznehmers Registrierung	BWV-Ahaus, Kreis Borken NT-Workstation-Code	
Wählen Sie einen Lizensierungsmodus aus	-	Wählen Sie entweder die Option Pro Server oder Pro Arbeitsplatz.
Computer-Name	Geben Sie einen für sämtliche Computer, Arbeitsgruppen und Domänen des Netzwerks eindeutigen Namen ein. Dieser Name kann aus bis zu 15 Zeichen bestehen. Raum-Nr.-PC-Nr., z.B. 1122-02	
Server-Typ	-	Wählen Sie einen Server-Typ aus: PDC, BDC oder Alleinstehender Server.
Kennwort	Geben Sie ein Kennwort für das Administratorkonto ein, und bestätigen Sie dieses. Hier einheitlich ”bwvah”, keine Notfalldiskette	
Notfalldiskette	Wählen Sie die Option zum Erstellen der Notfalldiskette. Mit dieser Diskette können sowohl fehlende oder beschädigte Windows NT-Dateien und die Registrierung als auch die Verzeichnisdatenbank, die Sicherheits-, die Festplatten- und andere Systeminformationen wiederhergestellt werden.	
Komponenten	Wählen Sie die zu installierenden Komponenten aus. (Standard belassen)	

5.5.2.1 INSTALLATION DES NETZWERKES

Vom Setup-Assistenten angeforderte Information	Windows NT Workstation	Windows NT Server
Wie der Computer an das Netzwerk angeschlossen werden soll	Wählen Sie eine der folgenden Optionen aus: Computer jetzt noch nicht mit dem Netzwerk verbinden oder Verbindung zwischen Computer und Netzwerk herstellen. Wenn Sie die Option Verbindung zwischen Computer und Netzwerk herstellen ausgewählt haben, können Sie danach die entsprechenden Netzwerkoption(en) auswählen: Direkt am Netzwerk anschließen oder Remote-Zugriff auf das Netzwerk.	Wählen Sie eine der folgenden Netzwerkoptionen aus: Direkt am Netzwerk anschließen oder Remote- Zugriff auf das Netzwerk
Installieren von Microsoft Internet Information Server (IIS)	-	Klicken Sie auf installieren, von Microsoft Internet Information Server, wenn sie diesen Dienst installieren möchten. Sie werden dann zum Konfigurieren der entsprechenden Protokolle aufgefordert. IIS nicht installieren!
Suchen nach installierten Netzwerkkarten	Klicken Sie auf Suche starten, um den Setup-Assistenten nach Netzwerkkarten in Ihrem Computer suchen zu lassen. Wird die Netzwerkkarte nicht automatisch identifiziert, klicken Sie auf Aus Liste auswählen, um die korrekte Karte auszuwählen: 3COM Fast Ethernet 3C905TX.	Klicken Sie auf Suche starten, um den Setup-Assistenten nach Netzwerkkarten in Ihrem Computer suchen zu lassen. Wird die Netzwerkkarte nicht automatisch identifiziert, knicken Sie auf Aus Liste auswählen, um die korrekte Karte auszuwählen: 3COM Fast Ethernet 3C905TX.
Auswählen der entsprechenden Netzwerkprotokolle	Wählen Sie die Netzwerkprotokolle aus, die in Ihrem Netzwerk verwendet werden sollen: **TCP/IP**, NWLink **IPX/SPX**-kompatibler Transport, NetBEUI Protokoll. Dabei ist TCP/IP das Standardprotokoll. Wenn Sie TCP/IP als Protokoll auswählen, werden Sie gefragt, ob Sie DHCP verwenden möchten. Wenn in Ihrem Netzwerk ein DHCP- Server vorhanden ist, kann TCP/IP so konfiguriert werden, dass dynamisch eine Internet Protocol (IP)-Adresse zugewiesen wird.	
Netzwerkdienste	In der Standardeinstellung werden folgende Dienste installiert: Computer-Suchdienst, NetBIOS-Schnittstelle, RPC-Konfiguration, Server-Dienst und Arbeitsstationsdienst. Über die Option Aus Liste auswählen können Sie weitere Dienste hinzufügen.	
Einstellen der Netzwerkkarte	Welche Optionen zur Verfügung stehen, hängt von der verwendeten Netzwerkkarte ab. Die Optionen beziehen sich auf die IRQ, die E/A-Anschlussadresse, den E/A-Kanal sowie den Transceiver-Typ	
Einstellen der Netzwerkbindungen	Wählen Sie aus, ob Sie die Netzwerkbindungen deaktivieren oder die Reihenfolge festlegen möchten, in der der Computer Informationen im Netzwerk findet. Kein DHCP installieren, sondern feste IP-Adressen angeben, vgl. 5.2 Organisatorische Vorüberlegungen	
5.5.2.2 Konfigurieren des Arbeitsgruppen- oder Domänennamens	Geben Sie einen Arbeitsgruppen- oder einen Domänennamen ein. Damit der Computer Mitglied einer Domäne werden kann, muss ein entsprechendes Computer-Konto vorhanden sein. Wenn es ein solches Konto noch nicht gibt, klicken Sie auf Computerkonto erstellen, und erstellen Sie ein Computer-Konto. Dazu müssen Sie ein Benutzerkonto mit dem entsprechenden Kennwort angeben, das über die Berechtigung verfügt, Arbeitsgruppen zu der angegebenen Domäne hinzuzufügen, wie zum Beispiel das Domänenadministratorkonto. **PDC Computerkonto erstellen** **BDC, WS Computerkonto erstellen nicht anklicken, Computerkonto wird anschließend erstellt - bitte warten, bis PDC Installation abgeschlossen hat**	

ABSCHLUSS DER INSTALLATION

1) Einstellen von Zeitzone, Datum und Uhrzeit.

2) Evtl. Einstellen und Konfigurieren der Grafikkarte (START - EINSTELLUNGEN - SYSTEMSTEUERUNG - ANZEIGE)

5.5.2.3 Computer zur Domäne hinzufügen

1) Anmelden als Administrator am PDC
2) Start - Programme - Verwaltung (Allgemein) - Server-Manager
3) Computer - Zur Domäne hinzufügen: Workstation oder Server
4) Name eingeben (PCxx) - Hinzufügen - Schließen

5.6 Unattend Installation einer Workstation (halbautomatische Installation)

Eine besondere Möglichkeit der Installation bietet die Unattend - Installation einer Workstation (oder eines Servers; wahrscheinlich werden Sie aber eher eine Workstation als einen Server ohne Aufsicht installieren wollen).

Sie wird von Firmen verwendet, die eine OEM-Installation für die Kunden anbieten. Dabei wird zuerst eine sogenannte Masterinstallation auf einem PC durchgeführt. Diese Installation wird als Abbild gespeichert. (Befehl: **Sysdiff /snap snapshot_file)**

Anschließend kann auf dem Master-PC die Anwendersoftware aufgespielt werden die alle NT-Nutzer benutzen sollen. (Programme, die einen Neustart des Computers erforderlich machen - z.B. Office 97) - werden aber als problematisch angesehen) Ist der PC so konfiguriert, wie die Anwender ihn benutzen sollen, so ist wiederum eine Differenzerfassung zum ersten Abbild durchzuführen.

(Befehl: **Sysdiff /diff snapshot_file sysdiff_file)**

In einem letzten Schritt wird nun mit Hilfe dieser beiden Dateien ein Verzeichnis (am besten auf einem Server) angelegt, welches OEM heißt und alle Datendateien der Anwendungssoftware, die Veränderungen an INI-Dateien, Registry, Desktop etc. enthält und zusätzlich noch von der Workstation-CD eine Kopie des Verzeichnisses i386 bekommen muss. Befehl:

Sysdiff /inf /m sysdiff_file oem_root

/M Dateiänderungen werden so zugeordnet, dass sie als Standardbenutzerdateien erscheinen OEM-ROOT bezeichnet dabei das Verzeichnis auf dem Server, welches oem und Sysdiff file.inf aufnimmt. (den **Sysdiff-Programm** finden Sie sowohl auf der Workstation-CD als auch auf der Server-CD)

Sollten Sie nun eine Installation starten, so werden Sie, wie bei einer normalen Installation, im Dialog geführt.

Besser ist es, eine Antwortdatei für die Dialogfragen zu generieren. Dazu rufen sie von einer NT - SERVER-CD das Programm SETUPMGR.EXE aus dem Unterverzeichnis **\Support\deptools\I3S6** auf und generieren im Vorfeld alle Antworten.

Beim Verlassen des Setup-Managers werden die Antworten in der Datei unattend.txt gespeichert.

Beispiel für eine **unattend.txt**-Datei,

[Unattended]

OemPreinstall = yes

NoWaitAfterTextMode = 1

NoWaitAfterGUIMode = 1

```
FileSystem = ConvertNTFS
Extend0EMPartition = 0
ConfirmHardware = no
NtUpgrade = no
Win3lUpgrade = no
TargetPath = WINNT
Overwrite0emFiles0nUpgrade = no

[UserData]
FullName = "Kaufm. Schulen Ahaus"
OrgName = "Kreis Borken"
ProductId = "1126196-OEM-0015107-23672"       bzw. 040-0603766

[GuiUnattended]
OemSkipWelcome = 1
OEMBlankAdminPassword = 1
TimeZone = "(GMT+01:00) Berlin, Stockholm, Rom, Bern, Brüssel, Wien"

 [Display]
ConfigureAtLogon = 0
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 75
AutoConfirm = 1

[Network]
DetectAdapters = ""
InstallProtocols = ProtocolsSection
InstallServices = ServicesSection
JoinDomain = KSA3
CreateComputerAccount = servop, anna200

[ProtocolsSection]
TC = TCParamSection

[TCParamSection]
DHCP = no
```

Subnet = 255.255.255.0

Gateway = 213.0.0.10

WINSPrimary = 213.0.0.2

[ServicesSection]

In dieser Datei werden nun die Informationen mitgeliefert, die für alle Workstation gleich sind. Da man jedoch auch workstationspezifische Informationen benötigt, muss eine weitere Datei angelegt werden, die in einem Abschnitt für jede zu installierende Workstation die spezifischen Eigenschaften enthält, wie z.B. IP-Adresse, Rechnername etc. Diese Datei erhält den Namen UDF.txt.

Beispiel für eine **UDF.txt**-Datei:

[UniqueIds]

Kirsche = UserData,TCParamSection

Pflaume = UserData,TCParamSection

Banane = UserData,TCParamSection

Rose = UserData,TCParamSection

Dahlie = UserData,TCParamSection

Tulpe = UserData,TCParamSection

[Rose:UserData]

ComputerName = ROSE

[Rose:TCParamSection]

IPAddress = 192.168.119.201

[Dahlie:UserData]

ComputerName = DAHLIE

[Dahlie:TCParamSection]

IPAddress = 192.168.119.202

[Tulpe:UserData] ComputerName = TULPE

[Tulpe:TCParamSection]

IPAddress = 192.168.119.203

[Kirsche:UserData]

ComputerName = KIRSCHE

[Kirsche:TCParamSection]

IPAddress = 192.168.119.204

[Pflaume:UserData]

ComputerName = PFLAUME

[Pflaume:TCParam,Section]

IPAddress = 192.168.119.205

[Banane:UserData]

ComputerName = BANANE

[Banane:TCParamSection]

IPAddress = 192.168.119.206

Die Dateien unattend.txt und UDF.txt können im Verzeichnis auf dem Server gespeichert werden.

Erzeugen Sie sich nun eine selbststartende DOS-Diskette mit Netzanbindung und erstellen Sie auf dieser Diskette eine BAT-Datei (z.B. INSTALL.BAT) mit folgendem Inhalt:

I386\winnt /b /s:i386 /u:i:\home\ntallhom\unattend.txt /udf:%1,i:\home\ntallhom\udf.txt

Wenn Sie nun diese Datei starten, geben Sie bitte beim Aufruf einen Rechnernamen mit an, welcher in der Datei UDF.txt angegeben ist (z.B. install Kirsche). Ab sofort läuft die Installation automatisch ab. Während des ersten Kopiervorgangs entfernen sie bitte die Diskette aus Laufwerk A:, damit bei den verschiedenen Neustarts des Systems auch von der Festplatte gebootet wird.

Eine Eingabe müssen Sie jedoch noch vornehmen: Die Bestätigung des Lizenzabkommens.

5.7 Erstellen und Verwenden der Notfalldiskette

Mit dem Befehl **rdisk** können Sie jederzeit eine Notfalldiskette erstellen, die komprimierte Versionen der Dateien der Systemregistrierung und einige andere Dateien enthält. Erstellen Sie für jeden wichtigen Computer eine Notfalldiskette.

Wählen Sie Aktualisieren, falls sich die Systemkonfiguration seit der letzten Verwendung von **rdisk** verändert hat (oder Sie sich nicht sicher sind). Nachdem die Notfallinformationen auf der Festplatte aktualisiert wurden, können Sie die Notfalldiskette erstellen.

Um eine Notfalldiskette auf Intel-Systemen zu verwenden, benötigen Sie ebenfalls die drei Setup-Disketten sowie die CD-ROM. Sie können die Setup-Disketten erstellen, indem Sie unter Windows NT den Befehl winnt32 /ox eingeben. Dieses Programm finden Sie im Verzeichnis \I386 der CD-ROM.

Die Reparatur des Systems mit einer Notfalldiskette ist ein einfacher, wenn auch langwieriger Vorgang. Starten Sie den Computer mit der Setup-Boot-Diskette, und legen Sie nach Aufforderung die zweite Diskette ein. Wenn das Menü des Setup-Programms erscheint, starten Sie mit **R** die Reparatur. Es werden alle Teile der NT-Umgebung zur Überprüfung vorgeschlagen.

Wählen Sie Fortsetzen, um mit der Reparatur zu beginnen. Wahrend der Reparatur fragt das System nach der dritten Setup-Diskette sowie nach der Notfalldiskette.

5.8 Dual-/ Triple- oder Quadro- Boot mit DOS/Win3.x. Win9x, WinNT, OS/2 und/oder Linux

5.8.1 Vorbemerkungen:

Win3.x startet nur nach DOS, daher wird im folgenden statt Win3.x nur der DOS-Boot betrachtet.

DOS, Win9x und WinNT starten jeweils nur aus einer primären Partition auf der ersten Platte (also von C: bzw. hda1:). Sie benötigen dazu einige Boot- und Kernel-Dateien im Root-Verzeichnis des Laufwerks C, der Rest des Dateisystems kann (und sollte) in anderen Verzeichnissen stehen. Teilen sich DOS, W9x und NT die Platte C zum booten, so muss diese als FAT16-Platte realisiert werden. NTFS ist auf den weiteren Platten möglich, kann aber von DOS- oder Win9x- Boot nicht eingesehen werden.

Um Probleme mit den verschiedenen Filesystemen und den z.T. gleichnamigen Boot-Dateien im Root-Verzeichnis zu umgehen, können 2 oder 3 primäre Partitionen auf der ersten Platte angelegt werden (vorzugsweise mit OS/2, da DOS das nicht kann). Ein Boot-Manager (z.B. von OS/2) holt beim Booten dann den erforderlichen Kernel und vergibt den Plattenbuchstaben C:. Die jeweils anderen primären Partitionen sind NICHT sichtbar! Die Kernel- und Boot-Dateien werden auf diese Weise sicher gegeneinander abgegrenzt.

5.8.1.1 DOS

Das Betriebssystem DOS enthält von sich aus keine DUAL-Boot-Möglichkeiten.

5.8.1.2 Win9x

enthält ein Boot-Menü, das beim Starten von Win95 mit F8 angezeigt werden kann. Es ist danach folgende Auswahl möglich:

Win9x GUI (graphische 32-bit-Oberfläche, komplettes Win9x)

Win9x-DOS (textbasiertes 16-bit Interface, es sind nicht alle Treiber verfügbar, evtl. auch kein Netz, mit "win" kann das GUI gestartet werden)

"altes" DOS (Starten der DOS-Version, die bei der Win9x-Installation auf der Platte war, ansonsten wird dieser Punkt nicht angeboten.)

ACHTUNG: Win9x realisiert diesen DOS-Start durch Umbenennen von alten und auch neuen Dateien im Root-Verzeichnis der C, da die Kernel-Dateien gleichnamig sind!

Alle Dateien mit Extension W40 sind Win9x- mit DOS sind "alte" DOS-Dateien. Sie werden von Win9x (falls der Win9x Bootsektor intakt ist und der Boot-Vorgang von Win9x gesteuert wird) jeweils entsprechend umbenannt.

Nach einem "alten" DOS-Start enthält CONFIG.SYS also den Inhalt von CONFIG.DOS, CONFIG.W40 den Inhalt der entsprechenden CONFIG.SYS-Win9x-Datei, IO.SYS ist der "alte" DOS-Kernel, IO.W40 enthält den Win9x-Kernel, usw.

5.8.1.3 WinNT

enthält standardmäßig ein DUAL-Boot-Menü, das erweitert werden kann. Außer NT steht standardmäßig ein weiteres System zur Auswahl, wenn es bei der Installation von NT bereits vorhanden war. Weitere Systeme können ins Boot-Menü integriert werden.

Der NT-Bootloader und das Boot-Menü können von einer Diskette gestartet werden, der Kernel und das File- System müssen allerdings vorher bootfähig auf einer Partition installiert worden sein. Es empfiehlt sich, eine solche NT-Boot-Diskette für Notfälle anzulegen (s.u.)

5.8.1.4 OS/2

liefert einen separaten Boot-Manager, der mit OS/2 FDISK installiert werden kann. Mit Hilfe des Boot-Managers kann OS/2 von beliebigen Partitionen gestartet werden, sowie weitere Betriebssysteme von anderen Partitionen. (Die o.g. Microsoft-Systeme starten nur von primären Partitionen!)

5.8.1.5 SuSE-Linux

ermöglicht über den Boot-Manager LILO das Booten unterschiedlicher Unix-Kernels, aber auch unterschiedlicher anderer Betriebssysteme auf verschiedenen Partitionen einer Platte oder verschiedenen Festplatten.

5.8.2 Realisierung von DUAL- oder TRIPLE- BOOT

5.8.2.1 Windows NT, Windows 9x und MS-DOS

Wie können Sie einen Computer so einrichten, dass der Benutzer direkt über die Auswahl in der Boot.ini-Datei nach WinNT, W9x oder DOS (Win3.11) anwählen kann, ohne dass W9x eine multiple-boot Unterstützung benötigt. (Diese Hinweise gelten nur für x86-Prozessoren)

1) Installieren Sie MS-DOS
2) Installieren Sie Windows NT
3) Entfernen Sie die Dateiattribute von der Datei c:\bootsect.dos (attrib -s- -h -r \bootsect.dos)
4) Erstellen Sie eine Kopie von der Datei (copy bootsect.dos bootsect.sav)
5) Booten Sie DOS und installieren Sie zusätzlich Windows 9x.
6) Da Windows 9x den Bootsector überschreibt, muss der Bootsector für WinNT wiederhergestellt werden. Dabei wird auch ein neuer bootsect.dos für W9x hergestellt. [4]
7) Löschen Sie die read-only und hidden Dateiattribute vom W9x bootsect.dos (vgl. oben 3.)
8) Benennen Sie c:\bootsect.dos nach c:\bootsect.w40 um.
9) Benennen Sie c:\bootsect.sav nach c:\bootsect.dos um.
10) Löschen Sie die gesetzten Dateiattribute von der Datei \boot.ini.
11) Ändern Sie die Datei boot.ini mit Hilfe eines Texteditors (edit, notepad) und ergänzen Sie die Zeilen unter [Operating Systems]:

```
[Operating Systems]
c:\bootsect.dos="MS-DOS 6.22" /Win95dos
c:\bootsect.w40="Windows 95" /Win95
```

Wenn Sie jetzt Windows NT starten, sollten Ihnen die zusätzlichen Wahlmöglichkeiten angeboten werden. Die neuen Schalter /win9xdos und /win9x werden benötigt, damit Windows NT den multible-boot-Prozess von Windows 9x emulieren kann.

5.8.2.2 Windows 9x, Windows-NT und Linux auf einem Rechner

Zum Booten wird der Bootmanager von NT benutzt. Dabei sind folgende Schritte einzuhalten:

1. Partitionieren Sie Ihre Festplatte für DOS/W9x, für Linux und für Windows NT
2. Installation von Windows 9x (z.B. auf hda1 als primäre DOS-Partition)
3. Installation von Windows NT (z.B. auf hda2 - Dateisystem NTFS)
4. Linux wie üblich installieren (z.B. auf /dev/hda3 als Root-Partition, /dev/hda4 als Swapbereich)

[4] Für weitergehende Informationen lesen Sie bitte den Artikel in der Microsoft Knowledge Base: article-id Q104429, title: Installing MS-DOS Version 6.2x After Windows NT is Installed

5. Mounten Sie die DOS-Partition /dev/hda1 z.B. in das Verzeichnis /dosc
6. Installieren Sie den Linux-Bootloader LILO in der Linux-Rootpartition /dev/hda3, nicht in den Master-Boot-Record (MBR) (vgl. /etc/lilo.conf, in der neben Linux auch W9x gebootet werden kann)

```
# LILO Konfigurations-Datei
# Start LILO global Section
boot=/dev/hda3
linear
read-only
prompt
timeout=50
vga = normal    # force sane state
# End LILO global section
# Linux bootable partition config begins
image = /vmlinuz
root = /dev/hda3
label = linux
# Linux bootable partition config ends
#
# DOS bootable partition config begins
other = /dev/hda1
label = w9x
table = /dev/hda
# DOS bootable partition config ends
```

Abbildung 2: Linux-Datei /etc/lilo.conf

7. Kopieren des LILO-Bootsektors auf eine Platte, die von NT gefunden wird, z.B.

   root #> dd if=/dev/hda3 bs=1024 count=1 of=/dosc/bootsek.lin

8. Booten Sie WinNT und kopieren Sie die Datei bootsek.lin in das Hauptverzeichnis des NT-Systemlaufwerks
9. In der Datei boot.ini (Attribute setzen) folgenden Eintrag am Ende hinzufügen:

   c:\bootsek.lin="Linux"

```
[boot loader]
timeout=10
default=C:\
[operating systems]
C:\="Microsoft Windows 9x "
multi(0)disk(0)rdisk(1)partition(1)\WINNT="Windows NT Workstation, Version 4.0"
multi(0)disk(0)rdisk(1)partition(1)\WINNT="Windows NT Workstation, Version 4.0
[VGA-Modus]" /basevideo /sos
C:\bootsek.lin="SuSE Linux 5.0"
```

Abbildung 3: Datei c:\boot.ini

10. Beim nächsten Booten sollte die Option Linux im NT-Bootmanager zur Verfügung stehen. In der o.a. boot.ini wird Windows 9x als Standardvorgabe (timeout nach 10 Sekunden) gebootet. Daneben werden Windows NT normal und im VGA-Modus (installiert auf der 2. Festplatte) und schließlich SuSE-Linux angeboten.

6 Der Benutzer

6.1 NT Workstations als Teil einer Domäne

Eine NT Workstation kann als Einzelplatzsystem betrieben werden. Dann obliegt die Benutzerverwaltung allein der lokalen Benutzerdatenbank. Diese Benutzerdatenbank bleibt zunächst auch erhalten, wenn sich die NT Workstation einer Domäne anschließt

Wenn eine NT Workstation Teil einer Domäne wird, ändern sich folgende Punkte:
- Die Anmelde-Box beim Anmelden zeigt auch den Namen der Domäne.
- Die Gruppe Domänen Benutzer wird zur lokalen Benutzergruppe hinzugefügt.
- Die Dornänen -Admin Gruppe wird zur lokalen Administrator Gruppe hinzugefügt.
- Beim Start von NT wird automatisch das Netlogon gestartet.
- Ein Eintrag in die Domänen-Datenbank erfolgt für jede Maschine, die zu einer Domäne hinzukommt.

Die Benutzer- und Zugriffsrechte- Datenbank liegt auf dem Primären Domänen-Controller (PDC), alle anderen Maschinen greifen auf diese Datenbank zu, wenn sie sich in der Domäne anmelden.

6.1.1 Mitglied einer Domäne werden

Der Administrator definiert einen Benutzer in Windows NT durch ein **Benutzerkonto.** Er erzeugt ein Benutzerkonto durch die Festlegung eines Benutzernamens und die Vergabe eines Kennworts. Windows NT erzeugt daraufhin einen eindeutigen Security Identifier (SID), der in der Registrierungsdatenbank gespeichert wird. Der SID ist unabhängig vom Benutzernamen. Zu einem Benutzer gehören u.a. folgende Informationen:

- Benutzername
- Kennwort des Benutzers
- Gruppen, denen der Benutzer angehört Basisverzeichnis sowie der Anmeldeskriptname

6.1.1.1 Die Bedeutung des Security Identifier

Der Security Identifier ist unabhängig vorn Benutzernamen. Vom Betriebssystem wird bei der Überprüfung von Benutzerrechten (etwa beim Zugriff auf Netzwerk-Ressourcen) die jeweilige SID und nicht der Benutzername verwendet; daher kann der Administrator einen Benutzernamen ändern, ohne die Rechte für Netzwerk- Ressourcen etc. ändern zu müssen. Wird der Benutzername gelöscht, kann bei Neuanlage nicht der selbe Security Identifier zugewiesen werden. Daher ist es sinnvoll Ausscheidende Anwender zunächst nur ”inaktiv” zu setzen.

Die nicht erlaubten Zeichen für Benutzernamen sind:

´´ \ / [ ] < > | : ; + ? , *

Umlaute können aus Kompatibilitätsgründen zu anderen Systemen Probleme verursachen. Benutzernamen kennen Groß-/Kleinschreibung, ignorieren sie aber. Windows NT speichert einen Benutzernamen also genau so ab, wie er eingegeben wurde, aber beim Anmelden und in Befehlen spielt die Groß-/Kleinschreibung **keine** Rolle.

Für eine NT Workstation bestehen 2 Wege, um sich an eine Domäne anzuschließen:

1. Wenn der Benutzer der Workstation Administrator-Privilegien in der Domäne besitzt: Über das Symbol Netzwerk in der Systemsteuerung kann eine Domäne ausgewählt werden. Dabei muss aber der Administrator-Account und dessen Passwort angegeben werden.
2. Wenn der Benutzer keine Administrator-Privilegien in der Domäne besitzt, muss der Administrator den Computer(namen) im Server Manager (Teil der Verwaltungsgruppe auf einem NT-Server) anlegen, erst dann kann über das Symbol "Netzwerk" der Systemsteuerung (einer Workstation) eine Domäne ausgewählt werden (diesmal ohne Administrator-Account!).

Eine NT Workstation hat keine Kopie der Accountdatenbank der Domäne, aber jeder weitere NT Server in einer Domäne! Daraus folgt, dass in einer Domäne alle NT Server den gleichen Security-Account-Manager verwenden! Da dies bei NT Workstations nicht so ist, kann dort im Anmelde-Bildschirm zwischen der lokalen Station (mit eigenem SAM) und der Domäne (mit deren SAM) ausgewählt werden.

Allerdings ist die Anmeldung mit einem Account der Domäne auf einer NT-Workstation auch dann möglich, wenn der Primäre Domänen Controller und alle Server außer Betrieb sind. In diesem Fall wird die lokale Datenbank verwendet (falls der Domänen- Administrator dies nicht verhindert z.B. durch Einrichtung von entsprechenden Benutzerprofilen).

Wichtig: Ein NT-Server kann keine Workstation in einer Domäne werden. Deshalb kann sich auch an einem Server auch kein Normalbenutzer anmelden!

6.1.2 Das Anmeldeverfahren

Auf einer NT Workstation existieren nach der Anmeldung an eine Domäne pro Computer und Benutzer
- ein Benutzer
- ein Computer
- zwei Umgebungen

Welche Umgebung ein Benutzer verwendet, hängt davon ab, wo er sich anmeldet:
- Lokal oder
- als Teil der Domäne

Über die lokale Umgebung hat der Administrator der NT Workstation die Kontrolle, es sei denn der lokale Benutzer darf den lokalen Administrator-Account nicht benutzen! Soll der Benutzer seine eigene Maschine verwalten können, dann braucht er dort eine Administrator-Berechtigung.

Die Anmelde-Box bestimmt
- An welchem Rechner der Benutzer angemeldet wird.
- Weiche Benutzerdatenbank verwendet wird.
- Welche Ressourcen der Benutzer verwenden darf
- Welche Sicherheitsmechanismen zum Tragen kommen.

Der Benutzer kann sich nur dort anmelden, wo er das darf, d.h. in der "Anmelde"-Box sind keine eigenen Eingaben möglich!

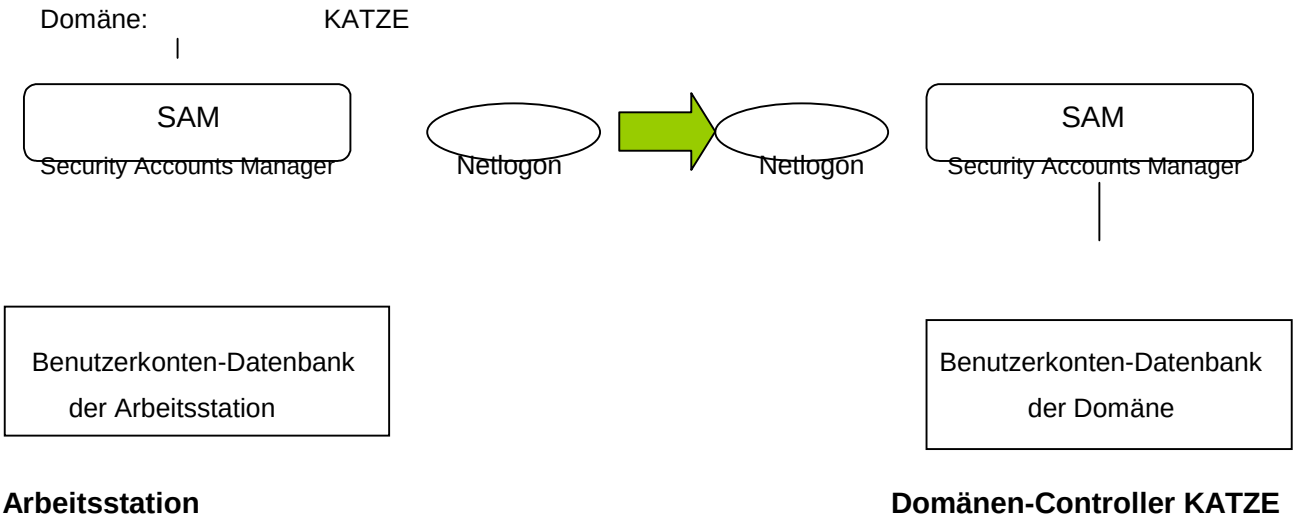
Die Anmeldung in der Domäne

Der Benutzer gibt die Anmeldeinformationen (Benutzername und Kennwort) und als Ziel den Domänennamen an. Der Security Accounts Manager (SAM) erkennt, dass es sich um eine Domänen-Anmeldung handelt.

Den nächsten Schritt übernimmt Netlogon, der Anmeldedienst, der sowohl auf der Arbeitsstation als auch auf allen Domänen-Controllern läuft: Er richtet nun einen sicheren Übertragungsweg zu einem Domänen-Controller ein, und die Anmeldeinformationen werden in verschlüsselter Form weitergeleitet. Anhand der Benutzerkontendatenbank der Domäne wird die Echtheitsprüfung durchgeführt.

Ist die Anmeldung erfolgreich, erzeugt das Sicherheits-Subsystem von Windows NT einen Zugriffsschlüssel (Access Token). Beim Zugriff auf eine Ressource vergleicht NT die Daten des Access Tokens mit der Zugriffskontrolliste (ACL, Access Control List) der angeforderten Ressource.

Benutzername:	Meier
Kennwort:	xxxxx



6.2 Benutzerverwaltung

Die Benutzerverwaltung und insbesondere die Definition von Benutzern ist der erste wesentliche Schritt nach der Installation von Servern. An dieser Stelle müssen die Benutzer und Benutzergruppen, die im System verwendet werden sollen, definiert, werden.

6.2.1.1 Definition von Benutzern

Der erste Schritt ist das Anlegen von Benutzern. Das Werkzeug, das von Windows NT für diesen Zweck zur Verfügung gestellt wird, ist der Benutzer-Manager für Domänen. Dieser ist beim Windows NT Server standardmäßig eingerichtet, während er bei der Windows NT Workstation noch nicht installiert ist.

Eine Nachinstallation auf einer Windows NT Workstation ist möglich. Dazu müssen aus dem Verzeichnis \clients\svrtools\winnt\i386 der Server-CD die entsprechenden Dateien auf die Workstation kopiert und im Startmenü aktiviert werden. In Zukunft stehen der Workstation demnach 2 Benutzermanager zur Verfügung - für die lokalen Benutzer und für die Domänen-Benutzer. Achten Sie darauf, dass es hier zu keinen Konflikten kommt.

6.2.1.2 Vordefinierte Benutzerkonten

Bei der Installation von Windows NT Server auf einem prirnären Domänen-Controller werden einige Benutzerkonten und Gruppen automatisch angelegt und mit bestimmten Rechten ausgestattet.

Vordefinierte lokale Benutzerkonten der NT Workstation	
Administrator	Dieses Benutzerkonto ist vorgesehen für die Person, die den Server oder die Domäne verwaltet. Das Konto kann nicht gelöscht und nicht deaktiviert werden.
Gast	An diesem Konto werden Benutzer angemeldet, für die kein Benutzerkonto in der Domäne oder einer vertrauten Domäne angelegt ist. Es ist standardmäßig deaktiviert

6.2.1.3 Benutzergruppen

Um die Verwaltung von Benutzern zu vereinfachen und Übersichtlichkeit und Flexibilität bei der Nutzung von Datenbeständen zu gewährleisten, werden Gruppen gebildet. Das Benutzerkonzept von Windows NT sieht in einer Domäne für die Benutzerverwaltung die Verwendung und die Schachtelung von zwei verschiedenen Gruppentypen vor.

6.2.1.4 Lokale Gruppen

Lokale Gruppen dienen zur Zusammenfassung von Zugriffsrechten auf die Datenbestände und sonstigen Ressourcen einer bestimmten NT-Workstation oder eines bestimmten NT-Servers.

Eine lokale Gruppe ist bei NT-Workstations oder NT-Servern immer eine Angelegenheit der lokalen Benutzerdatenbank. Einen Spezialfall stellen die lokalen Gruppen der Domänen-Controller dar: Sie gelten für alle Domänen-Controller der Domäne gleichermaßen, weil diese ja Kopien einer einzigen Datenbank haben.

6.2.1.5 Globale Gruppen

Globale Gruppen dienen zur Zusammenfassung von Benutzern, die gleiche Aufgaben durchzuführen haben oder gemeinsam an einem Projekt arbeiten.

Eine globale Gruppe ist immer eine Angelegenheit der Benutzerdatenbank der Damäne.

6.2.1.6 Vordefinierte Benutzergruppen der Domäne

Vordefinierte globale Gruppen der Domäne (Sie liegen allein auf dem Server)	
Domänen- Admins	Diese globale Gruppe enthält den Benutzer Administrator. Sie ist vorgesehen für alle Personen, die Verwaltungsaufgaben in der Domäne ausführen. **Diese Gruppe ist automatisch Mitglied in der lokalen Gruppe Administratoren** auf jedem Windows NT Datei-Server und jeder Windows NT-Workstation der Domäne.
Domänen- Benutzer	Alte Benutzer der Domäne sowie der Administrator sind automatisch Mitglieder dieser Gruppe. Die Gruppe ist standardmäßig Mitglied in den entsprechenden lokalen Gruppen *Benutzer* auf allen Windows NT-Datei-Servern und den Windows NT-Workstations der Domäne. Auf diese Weise wird jeder neue Benutzer zum Benutzer auf jedem System in der Domäne.
Domänen-Gäste	Alle Personen, die nicht über ein eigenes Benutzerkonto verfügen, erhalten Zugang zur Domäne über ein Gast-Konto. Der Benutzer Gast ist das einzige Mitglied dieser Gruppe.

6.2.1.7 Die Gruppe *Jeder*

Außer den genannten Gruppen existiert eine Einheit mit dem Namen "Jeder", die - obwohl keine Gruppe im eigentlichen Sinn - jeden Benutzer im Netzwerk repräsentiert.

Diese Gruppierung dient dazu, den Nutzungs-Zugriff auf eine Ressource für alle Netzteilnehrner ohne Ausnahme sofort und gänzlich zu unterbinden oder zu gewähren.

Für die Vergabe von Berechtigungen ist die Gruppe Jeder ungeeignet, denn sie enthält auch die Mitglieder der Gruppe *Gäste.* Es wird empfohlen, die lokale Gruppe *Benutzer* zu verwenden, wenn Sie Zugriffsrechte auf die Ressourcen eines Servers oder einer Workstation vergeben.

6.2.1.8 Vordefinierte lokale Gruppen auf dem Domänen-Controllern

Adrninistratoren	Mitglieder in dieser Gruppe sind der Administrator und die Gruppe Domänen-Admins. Die Mitglieder dieser lokalen Gruppe können Benutzer und lokale Gruppen anlegen, verwalten und löschen. Sie dürfen Verzeichnisse und Drucker freigeben. Ihnen obliegt die Vergabe von Rechten an Benutzer und Gruppen und die Installation von Systerndateien.
Sicherungs- Operatoren	Die Mitglieder dieser Gruppe besitzen alle Berechtigungen, die erforderlich sind, um Datensicherungen an den Domänen-Controllern durchzuführen. Sie dürfen sich direkt am Domänen-Controller anmel-

	den und den Domänen-Controller herunterfahren
Server- Operatoren	Die Mitglieder dieser Gruppe besitzen alle nötigen Rechte, um einen Domänen-Controller zu verwalten. Die Berechtigungen beziehen sich jedoch nicht auf die Sicherheitsverwaltung oder die Domänen-Verwaltung des Domänen-Controllers. Server-Operatoren dürfen sich am Domänen-Controller anmelden und ihn herunterfahren. Sie können Verzeichnisse und Drucker freigeben bzw. Freigaben beenden, Dienste steuern, Festplatten formatieren und Datensicherungen und Wiederherstellungen durchführen.
Konten- Operatoren	Die Mitglieder dieser Gruppe besitzen alle Rechte, die erforderlich sind für das Anlegen von lokalen und globalen Gruppen. Den Konten des Administrators und anderer Operatoren kann ein Konten-Operator nicht verwalten und keine Rechte an Benutzer vergeben.
Druck- Operatoren	Sie dürfen einen Druck-Server auf dem Domänen-Controller einrichten, Drucker freigeben bzw. Freigaben beenden sowie freigegebene Drucker verwalten. Sie dürfen sich am Domänen-Controller direkt anmelden und diesen herunterfahren.
Replikations- Operator	Die Mitglieder verfügen über die Rechte, die erforderlich sind, um den Verzeichnisreplikationsdienst auf dem Domänen-Controller zu starten.
Benutzer	Mitglied in dieser Gruppe ist die globale Gruppe Domänen-Benutzer. Damit enthält diese lokale Gruppe im allgemeinen alle Benutzer der Domäne. Über die Mitgliedschaft in dieser Gruppe erhalten die Benutzer dieser Domäne und vertrauter Domänen Zugriffsrechte auf die Ressourcen der Domäne. Benutzer dürfen sich nur von Arbeitsstationen aus in der Domäne anmelden.
Gäste	Über diese Gruppe definieren Sie die Rechte, die Sie fremden Personen gewähren wollen. Alle Personen, die nicht über ein Benutzerkonto in dieser oder einer vertrauten Domäne verfügen, erhalten Zugang zum System über ein Gast-Konto. Das Gast-Konto ist das einzige Mitglied in dieser Gruppe.

6.2.2 Anlegen neuer Benutzer

Für das Anlegen neuer Benutzer ist es zunächst wichtig, wer alles als Benutzer definiert werden soll. In der Regel wird für jeden Computer-Benutzer ein Benutzerkonto definiert. Sie sollten nun allerdings nicht wild damit beginnen, die Benutzer einzugeben. Vielmehr ist es sinnvoll, Benutzer mit ähnlichen Einstellungen zunächst einmal zu definieren, um sie anschließend zu vervielfältigen (zu klonen).

Damit können Sie sich viel Arbeit ersparen, da zum Beispiel die Benutzerrechte im System eines solchen Benutzers ebenso wie seine Gruppenzugehörigkeiten und andere Informationen übernommen werden. Sie müssen nur noch die wirklich individuellen Werte verwalten.

Um einen neuen Benutzer zu definieren, wählen Sie den Befehl *Neuer Benutzer* aus dem Menü *Benutzer* aus. In dem dann angezeigten Dialogfeld können Sie die Einstellungen für den Benutzer vornehmen.

Der *Benutzername* ist der Name, mit dem sich der Benutzer im System anmeldet. Dieser darf eine Länge von bis zu 20 Zeichen haben und muss innerhalb der Domäne eindeutig sein. Es kann aber mehrere Benutzer mit dem gleichen Benutzernamen in unterschiedlichen Domänen des Netzwerkes geben. Das ist deshalb möglich, weil Benutzer bei der Arbeit außerhalb der Domänen-Grenzen als

DOMÄNENNAMEN\BENUTZERNAME

identifiziert werden. Das gilt auch für die lokalen Benutzerkontendatenbanken von Windows NT Workstations und Servern in der Rolle eines Servers. Hier gibt es zum Beispiel den vordefinierten Benutzer *Administrator,* bei dem genau das der Fall ist. Wenn Sie dem *Benutzer Administrator* der Domäne KATZE Zugriffrechte auf einer NT-Workstation *PC05* geben wollen, so findet sich dort bereits ein Benutzer mit diesem Namen. Es gibt trotzdem keinen Konflikt, weil der eine als

Administrator beziehungsweise ***PC05\\Administrator***

und der andere als

KATZE\Administrator

identifiziert wird. Insofern ist die Eindeutigkeit dieser Benutzernamen auf einen kleinen Bereich begrenzt. Nur innerhalb einer Benutzerkontendatenbank (innerhalb einer Domäne) müssen Sie auf die Eindeutigkeit achten.

Der zweite Eintrag bezieht sich auf den *Vollständigen Namen* des Benutzers. In diesem Eingabefeld sollten Sie den kompletten Namen des jeweiligen Benutzers eingeben. Dabei sollten Sie auf ein einheitliches Vorgehen achten, da sich die **Sortierreihenfolge** der Benutzer nach der Schreibweise in diesem Feld richtet. Da sie in den meisten Fällen die Benutzer unter ihren Nachnamen kennen werden, empfiehlt sich ein Eintrag wie

Büning, Holger

für einen Benutzer. Wenn Sie dieses Schema durchhalten, haben Sie eine alphabetisch nach den Nachnamen der Benutzer sortierte Liste. Sie können die Sortierreihenfolge über die Befehle im Menü *Ansicht* entweder am Benutzernamen oder am vollständigen Namen ausrichten. Bei vielen Benutzern ist die Arbeit über den vollständigen Namen aber deutlich bequemer.

Der dritte Eintrag bezieht sich schließlich auf einen ***Kommentar*** zu den Benutzern. Auch hier sollten Sie noch einen Wert eingeben, da auch diese Information in den Listen sichtbar ist. Bewährt hat sich hier zum Beispiel, die Telefonnummer der Benutzer anzugeben, um bei Rückfragen schnell reagieren zu können. Diese Information wird beim Kopieren eines Benutzers beibehalten. Sie können sie daher auch für Abteilungsbezeichnungen oder andere Informationen verwenden oder einfach dazu, noch einmal die Rolle dieses Benutzers im Netzwerk zu charakterisieren.

Darunter müssen Sie schließlich das **Kennwort** des Benutzers eingeben. Dieses wird verschlüsselt angezeigt. **Sie sehen hier immer 14 Sternchen**, unabhängig von der Länge des Kennworts. Von besonderer Bedeutung ist hier, dass bei diesem Kennwort **zwischen Groß- und Kleinschreibung unterschieden wird** (case-sensitive). Wenn Sie sich an Windows NT anmelden, müssen Sie die gleichen Groß- und Kleinbuchstaben wie bei der Definition des Kennworts verwenden. Das muss man wissen und auch den Benutzern mitteilen, um Fehler bei der Eingabe dieses Kennwortes zu vermeiden. Das Kennwort müssen Sie noch bestätigen.

Darunter finden Sie bei der Definition eines Benutzers vier **Optionsfelder**. Später kommt noch ein fünftes hinzu, das für temporäre Sperren benötigt wird. Das erste dieser Optionsfelder ist mit ***Benutzer muss Kennwort bei der nächsten Anmeldung ändern*** bezeichnet. Wenn dieses selektiert ist, muss der Benutzer bei der ersten Anmeldung ein neues Kennwort eingeben.

Wenn Sie hier ein Kennwort wie Frosch definieren das für den Benutzer zunächst gilt, dann müssen Sie ihm dieses auch mitteilen. Er muss sich mit dem Standard-Kennwort anmelden. Erst danach darf er das Kennwort verändern. Er muss es natürlich in dieser Situation auch verändern. Für das neu eingegebene Kennwort gelten alle Restriktionen wie die Kennwortlänge und die Unterscheidung von bereits verwendeten älteren Kennwörtern. Das ist vor allem dann zu berücksichtigen, wenn Sie das Kennwort eines Benutzers zurücksetzen. Falls Sie definiert haben, dass sich das Kennwort fünfmal ändern muss, bevor es sich wiederholen darf, kann der Benutzer sein zuletzt verwendetes Kennwort nicht wieder verwenden.

Die zweite Option Benutzer kann Kennwort nicht ändern macht bei normalen Anwendern sicherlich keinen Sinn. Es gibt aber einzelne Benutzer für Dienste wie den Systems Management Server von Microsoft oder den Verzeichnisreproduktionsdienst von Windows NT, bei denen Sie eine solche Einstellung verwenden müssen.

Interessant ist die Option Kennwort läuft nie ab, die Sie wiederum für ähnliche Zwecke einsetzen können. Sie können damit für einzelne Kennwörter definieren, dass das maximale Alter für Kennwörter, das sie mit Richtlinien Konten definieren können, für diesen Benutzer keine Gültigkeit haben soll. Sie sollten sich aber als Administrator nicht der Bequemlichkeit halber weniger Restriktionen als anderen Benutzern auferlegen, da das Administrator- Kennwort ohne Zweifel das sensibelste im System ist.

Schließlich können Sie mit der Option Konto deaktiviert noch einstellen, dass ein Konto momentan deaktiviert ist. Diese Option ist immer dann von Bedeutung, wenn ein Benutzer für eine längere Zeit nicht da ist und verhindert werden soll, dass trotzdem mit seinem Konto gearbeitet wird. Sie dürfen einen Benutzer in dieser Situation nicht löschen, da die Zugriffsrechte jeweils über die eindeutige Sicherheits-ID (SID) vergeben werden. Wenn Sie den Benutzer nun löschen und wieder neu definieren, erhält dieser eine neue SID, die sich definitiv von seiner früheren unterscheidet. Damit müssen Sie ihm dann alle Zugriffsrechte neu vergeben.

Wichtig ist übrigens, dass das vordefinierte Konto Gast als einziges Mitglied der Gruppe Gäste bei einem Windows NT Server und auch bei einer NT-Workstation grundsätzlich deaktiviert ist. Aus Sicherheitsgründen sollten Sie es auch gesperrt lassen, da sich sonst jeder unter diesem Konto ohne Kennwort anmelden kann. Da die Gruppe Jeder, zu der auch die Gäste gehören, aber als Standard volle Zugriffsrechte auf die meisten Systemdaten hat, wäre das eine gravierende Sicherheitslücke.

Einen so definierten Benutzer können Sie nun mit den anderen Befehlen aus dem Menü Benutzer bearbeiten. Der Befehl Eigenschaften ruft das Dialogfeld wieder auf. Sie können hier die definierten Werte verändern oder zusätzliche Einstellungen für den Benutzer vornehmen.

Über den Befehl Löschen können Sie einen Benutzer wieder aus dem System entfernen. Dadurch wird er endgültig gelöscht, wie oben bereits ausgeführt wurde. Sie können auch einen Benutzer umbenennen. Das ist deshalb wichtig, weil Sie dabei seine Sicherheits-ID beibehalten und nur den Benutzernamen anpassen. Auf diese Art können Sie Änderungen, die sich aufgrund des verwendeten Namensschemas ergeben, durchführen, ohne alle Berechtigungen und Gruppenzugehörigkeiten neu zu definieren.

Schließlich können Sie den Benutzer auch kopieren. Dazu verwenden Sie den gleichnamigen Befehl aus dem Menü Benutzer. Das Kopieren hat, wie oben bereits kurz erwähnt, den Vorteil, dass Sie dadurch einen neuen Benutzer mit praktisch identischen Einstellungen definieren können. Es werden alle Einstellungen zu Gruppenzugehörigkeiten, Anmeldeprogrammen, Profilen und dergleichen mehr übernommen. Das erspart sehr viel Arbeit bei der Definition von Benutzern.

6.2.3 Anlegen neuer Benutzer über die Befehlszeile

Daneben gibt es die Möglichkeit, direkt an der Befehlszeile Benutzer zu definieren. Der Befehl dafür lautet: NET USER

NET USER fügt Benutzerkonten hinzu, löscht sie oder ändert sie. Ohne Optionen wird eine Liste der Benutzerkonten auf dem Computer angezeigt. Die Informationen über Benutzerkonten werden in einer Benutzerkonten-Datenbank gesichert. Dieser Befehl ist auf Windows NT Servern und Windows NT Workstations gültig.

Die Syntax dieses Befehl lautet:

NET USER [Benutzername [Kennwort|*] [Optionen]] [/DOMAIN] Benutzername (Kennwort|*) /ADD [Optionen] [/DOMAIN] Benutzername [/DELETE] [/DOMAIN]

Die Optionen des Befehls haben folgende Bedeutung:

Option	**Bedeutung**
Benutzername	Der Name des Benutzerkontos, das hinzugefügt, gelöscht, geändert oder angezeigt werden soll. Die maximale Länge eines Benutzernamens beträgt 20 Zeichen.
Kennwort	Weist dem Benutzerkonto ein Kennwort zu oder ändert es. Das Kennwort muss die mit der Option /MINPWLEN des Befehls NT ACCOUNTS festgelegte Mindestlänge aufweisen. Die maximale Länge beträgt 14 Zeichen.
*	Es erscheint die Eingabeaufforderung für das Kennwort. Das Kennwort wird bei der Eingabe nicht angezeigt.
/DOMAIN	Führt den Vorgang auf dem primären Domänen-Cotroller der aktuellen Domäne aus und nicht auf dem lokalen Computer. Dieser Parameter gilt nur für Windows NT Workstation-Computer, die Mitglied einer Windows NT Server-Domäne sind. Windows NT Server-Computer führen einen solchen Vorgang standardmäßig auf dem primären Domänen-Controller aus.
/ADD	Fügt ein Benutzerkonto der Benutzerkontendatenbank hinzu.
/DELETE	Löscht ein Benutzerkonto aus der Datenbank.
/ACTIVE:(YESINO)	Deaktiviert oder aktiviert das Konto. Wenn das Konto nicht aktiv ist, kann der Benutzer nicht auf den Server zugreifen. Standardeinstellung ist YES.
/COMMENT: "Beschreibung"	Es kann eine Beschreibung zum Benutzerkonto eingegeben werden. Die maximale Länge beträgt 48 Zeichen. Der Text muss in Anführungszeichen (" ") stehen.
/COUNTRYCODE: nnn	Verwendet die Landeskennzahl des Betriebssystems, anhand derer die Dateien die Online-Hilfe und der Fehlermeldungen in der jeweiligen Landessprache angezeigt werden. Bei der Eingabe des Wertes 0 wird die Standardländereinstellung gewählt. Diese Option ist aus Kompatibilitätsgründen im OS/2 LAN Manager enthalten.
/EXPIRES:(Datum|NEVER)	Läßt ein Benutzerkonto zum angegebenen Datum ablaufen. Bei Eingabe von NEVER wird keine zeitliche Beschränkung für das Benutzerkonto festgelegt. Ablaufdaten können je nach angegebener Ländereinstellung in der Reihenfolge Monat/Tag/Jahr oder Tag/Monat/Jahr eingegeben werden. Monatsnamen können ausgeschrieben, mit drei Buchstaben abgekürzt oder als Zahlen geschrieben werden. Jahreszahlen können aus zwei oder vier Ziffern bestehen. Als Trennzeichen zwischen Tages-, Monats- und Jahreseingabe müssen Kommata oder Schrägstriche verwendet werden. Leerzeichen sind nicht zulässig.
/FULLNAME:"Name"	Der vollständige Name des Benutzers, also nicht der Benutzername. Der Name muss in Anführungszeichen (" ") stehen.
/HOMEDIR:Pfad	Bezeichnet den Pfad für das Basisverzeichnis eines Benutzers. Der Pfad muss bereits existieren.
/HOMEDIRREQ: (YES|NO)	Legt fest, ob ein Basisverzeichnis vorhanden sein muss. Verwenden Sie /HOMEDIR um das Verzeichnis festzulegen.
/PASSWORDCHG: (YESINO)	Legt fest, ob Benutzer ihr eigenes Kennwort ändern können, Standardeinstellung ist YES.
/PASSWORDREQ: (YESINO)	Legt fest, ob ein Benutzerkonto ein Kennwort haben muss. Standardeinstellung ist YES.
/PROFILEPATH:Pfad	Bezeichnet den Pfad für das Anmeldeprofil des Benutzers.
/SCRIPTPATH:Pfad	Bezeichnet den Pfad für das Anmeldeskript des Benutzers.
/TIMES:(Zeiten|ALL)	Legt die Anmeldezeiten fest. Die Werte für Zeiten werden in der Form Tag[-Tag][,Tag][-Tag][,Uhrzeit[- Uhrzeit][,Uhrzeit][-Uhrzeit]] angegeben,

	wobei die Angabe der Uhrzeit zu vollen Stunden erfolgen muss. Tage können ausgeschrieben werden oder abgekürzt werden. Beim 12- Stunden-Format muss nach der Uhrzeit AM, PM oder A.M., P.M. stehen. Bei ALL kann der Benutzer sich jederzeit anmelden. Ein Leerzeichen bewirkt, dass der Benutzer sich überhaupt nicht anmelden kann. Tag und Uhrzeit werden mit einem Komma getrennt, mehrere aufeinanderfolgende Zeitangaben mit einem Semikolon.
/USERCOMMENT: "Beschreibung"	Hier kann der Administrator eine Beschreibung zum jeweiligen Benutzerkonto eingeben oder ändern.
/WORKSTATIONS: (Computername[...]|*)	Es können bis zu acht Computer angegebenen werden, von denen aus sich der Benutzer am Netzwerk anmelden kann. Wenn nach /WORKSTATIONS nichts oder * angegeben wird, kann sich der Benutzer von jedem Computer aus anmelden.

Dieser Befehl kann nun dazu verwendet werden, die Benutzer an der Befehlszeile oder mit Hilfe von Batch-Dateien anzulegen. Das hat den Vorteil, dass sich damit auch größere Zahlen von Benutzern leicht definieren lassen, da zunächst nur der Eintrag für den ersten Benutzer definiert werden muss und dann in einem Editor nach unten kopiert werden kann. Bei den kopierten Einträgen müssen dann nur noch die Änderungen vorgenommen werden.

Wenn die Datei nun zum Beispiel **USER.BAT** heißt, kann mit

USER > D:\LOGS\USER280298.TXT

auch gleich eine Log-Datei erstellt werden, in der die Ausführung dieser Datei protokolliert wird. Damit wird eine bessere Dokumentation als bei der Verwendung der grafischen Schnittstelle von Windows NT erreicht.

6.2.4 Übungs- und Verständnisfragen

1. Wie wird man Mitglied einer Domäne?
2. Was ist der Security Identifier (SID) und welche Bedeutung hat er?
3. Unterscheiden Sie zwischen dem lokalen und dem Domänen-Benutzerkonto!
4. Beschreiben Sie kurz das Anmeldeverfahren in einer Domäne.
5. Wo bzw. auf welche Weise kann ein neuer Benutzer eingerichtet werden?
6. Sehen Sie Möglichkeiten, das Einrichten von vielen Benutzern (z.B. alle neu eingetretenen Studenten der FSW) zu erleichtern? Erläutern Sie diese Möglichkeiten.
7. Auf jeder Workstation in einer Domäne und auf den Servern (PDS, BDS, ..) selbst gibt es den Benutzer Administrator. Widerspricht das nicht der Einmaligkeit und Eindeutigkeit von Benutzern? Erklären Sie den Zusammenhang.
8. Welche Einstellungen und Restriktionen können bei der Vergabe eines Passwortes vorgenommen werden?
9. Wie lautet die Befehlszeile für das Anlegen eines neuen Benutzers über die Befehlszeile:

Benutzername:	Müller
Kennwort:	Soll verdeckt an der Eingabeaufforderung eingegeben werden
Beschreibung:	Franz Müller, Abt. Einkauf, Ruf 02561-445588
Ablauf:	Müller nimmt an einem einwöchigen Lehrgang teil

Homeverzeichnis: \user\lehrgang\<name>

Anmeldung: noch nicht geklärt, also jeder Computer

10. Die unter 9. aufgestellte Befehlszeile wird in eine Batchdatei BENUTZER.BAT geschrieben, die auch für das Einrichten zukünftiger neuer Benutzer verwendet werden soll. Wie können Sie sicherstellen, dass über die Neuanlage von Benutzern jeweils eine Protokolldatei im Verzeichnis C:\PROT\USER angelegt wird?

6.3 Die User-Gruppen

6.3.1 Die Bedeutung von User-Gruppen

Der wichtigste Schritt nach der Definition von Benutzern ist das Einrichten von Gruppen. Wichtig bei der Arbeit in einer Domäne ist dabei die Unterscheidung zwischen globalen und lokalen Gruppen.

Als Grundregel gilt:
- Globale Gruppen werden definiert, um Benutzer zusammenzufassen.
- Lokale Gruppen werden definiert, um diesen Berechtigungen zuzuordnen.

Dabei gilt das sogenannte vierstufige Konzept:

Benutzer

Globale Gruppen

Lokale Gruppen

Berechtigungen

Wenn Sie dieses Konzept konsequent nutzen, stellen sie eine einheitliche Systematik sicher und erleichtern sich den Überblick über das System. Natürlich können Sie von dieser Systematik auch abweichen. Bei einem durchdachten Konzept hält sich diese aber in Grenzen. Wenn Sie das Schema durchgängig verwenden, haben Sie den Vorteil, dass Sie immer exakt wissen, wofür die verschiedenen Gruppen verwendet werden. Das ist auf Dauer sehr viel mehr Wert als ein bißchen ersparte Arbeit bei der Definition der Gruppen.

Sie sollten globale Gruppen insbesondere für

Organisatorische Strukturen,

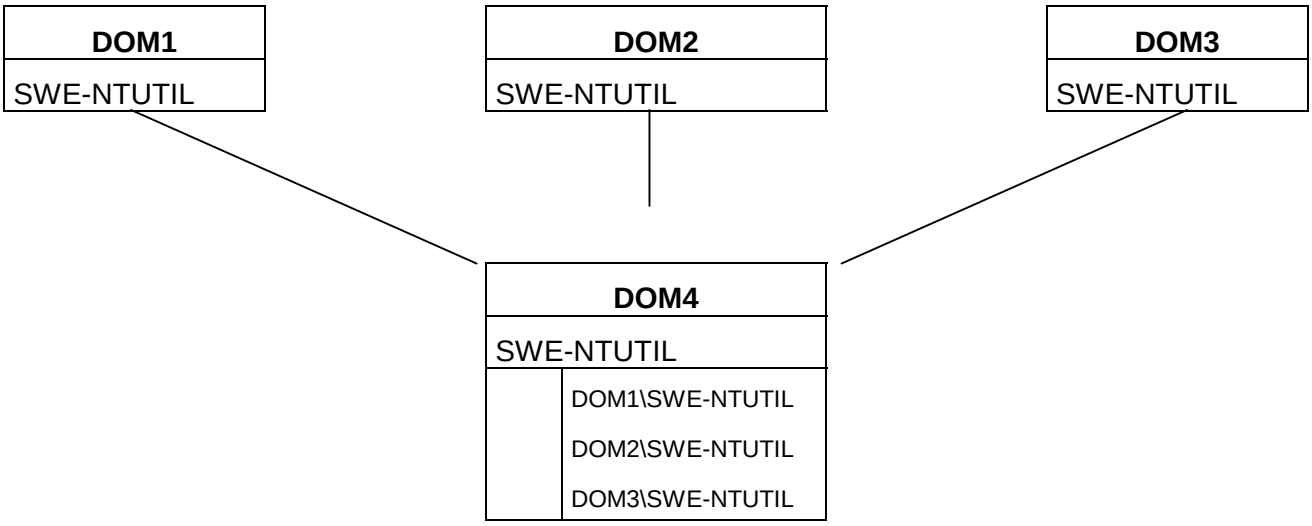
Temporäre Strukturen innerhalb von Organisationen und

Rollen in Organisationen

definieren. **Organisatorische Strukturen** lassen sich anhand der Aufbauorganisation einfach ermitteln. Sie haben dort beispielsweise eine Direktion *Finanzen,* in der es mehrere Bereiche *für Leasing, Finanzbuchhaltung, Anlagenbuchhaltung* und dergleichen mehr gibt. Diese unterteilen sich wieder in Abteilungen und die Abteilungen vielleicht noch in Gruppen. Für jede organisatorische Einheit auf jeder Ebene sollten Sie eine globale Gruppe definieren. Das erleichtert sowohl die Rechtevergabe in Bereichen, in denen Daten gemeinsam genutzt werden, als auch für andere Bereiche.

Die zweite Art von Gruppen basiert auf **temporären Strukturen** innerhalb der Organisation - also insbesondere auf Projekten. Auch hierfür empfiehlt sich die Definition von Gruppen. Bedauerlich dabei ist, dass Sie in eine solche globale Gruppe keine Mitglieder aus anderen, vertrauten Domänen aufnehmen können. Sie müssen das gegebenenfalls so lösen, dass Sie z.B. für ein Projekt Softwareentwicklung *NT-Utilities* mehrere **globale Gruppen** wie *SWE-NTUTIL-DOM1* und *SWE-NTUTIL-DOM2* definieren, die sich in den jeweiligen Domänen befinden. Dabei können Sie natürlich auch auf die Domänen-Namen verzichten, da diese bei der Nutzung dieser Gruppen in anderen Domänen ohnehin vorangestellt werden. In der Domäne, in der die gemeinsam genutzten

Ressourcen des Projekts liegen, definieren Sie dann eine **lokale Gruppe** *SWE-NTUTIL,* in der alle globalen Gruppen als Mitglieder aufgenommen werden.



Der dritte Typ von Gruppen bezieht sich auf Rollen innerhalb der Organisation. Hiermit können Sie Benutzergruppen bilden, die sich nicht an organisatorischen Strukturen orientieren, wie zum Beispiel

Betriebsrat

Winword-Admins

Datenbank-Adrnins

SAP-Admins

Internet-User

oder andere. Letztlich sind die *Domänen-Admins* und verschiedene lokale Gruppen ebenfalls solche rollen-orientierten Gruppen, die zum Teil auf lokaler und zum Teil auf globaler Ebene definiert werden. Die Arbeit mit rollen-orientierten Gruppen wird natürlich auch immer wieder auf der lokalen Ebene stattfinden.

Wenn Sie sich diese drei Bereiche vornehmen und systematisch überlegen, welche Gruppen dort definiert werden müssen, sollten Sie eigentlich schon alle globalen Gruppen haben, die Sie in Ihrem Netzwerk anlegen müssen. Die lokalen Gruppen sind, wie bereits erwähnt, entweder Analogien zu den globalen Gruppen, was sich aus dem insbesondere auf der Ebene der Domänen-Controller teilweise redundanten Konzept ergibt, oder rollen-orientiert. Das wird bei den verschiedenen vordefinierten lokalen Gruppen wie

Konten-Operatoren

Server-Operatoren

und den anderen Operatoren und auch Administratoren deutlich.

6.3.2 Das Anlegen von User-Gruppen

6.3.2.1 Globale Gruppen

Das Anlegen von globalen Gruppen ist der erste Schritt. Denken Sie daran, dass innerhalb der Domäne globale und lokale Gruppen unterschieden werden müssen, während es auf Systemen mit einer eigenen Benutzerverwaltung und damit einer eigenen Benutzerkontendatenbank nur lokale Gruppen gibt.

Eine neue globale Gruppe definieren Sie mit dem Befehl ***Neue globale Gruppe*** **aus dem Menü** ***Benutzer*** des Benutzer-Manangers für Domänen. In dem angezeigten Dialogfeld können Sie einen Namen und eine Beschreibung für die Gruppe eingeben. Sie sollten auch die Beschreibung definieren, um die Funktion der so definierten Gruppen deutlicher zu machen.

Sie können in die globale Gruppe gleich bei der Definition Mitglieder aus der Domäne, in der Sie diese Gruppe definieren, aufnehmen. Im rechten Listenfeld des Dialogfeldes wird bereits eine Liste der Mitglieder angezeigt.

Bei der Auswahl der Mitglieder der Gruppe können Sie mehrere Benutzer selektieren, indem Sie mit *Strg* oder ⇧ (Hochstelltaste) arbeiten. Im ersten Fall können Sie selektiv arbeiten, im zweiten einen Block von Benutzern definieren. Mit den Schaltflächen *Hinzufügen* und *Enffernen* können Sie anschließend Mitglieder in die Gruppen aufnehmen und wieder aus diesen entfernen.

6.3.2.2 Lokale Gruppen

Im Menü ***Benutzer*** finden Sie den Befehl ***Neue lokale Gruppe****.* Auch hier wird wieder ein Dialogfeld geöffnet, in dem Sie nun diese Gruppe einrichten können.

Allerdings sehen Sie hier auf der rechten Seite keine Liste der Benutzer aus der aktuellen Domäne. **Hintergrund ist, dass Sie hier Benutzer und globale Gruppen sowohl der aktuellen Domäne als auch von vertrauten Domänen eingeben können**. Dadurch werden die Auswahlmöglichkeiten größer und das Dialogfeld sieht dementsprechend anders aus.

Im oberen Bereich des Dialogfeldes können Sie auch hier wieder den Benutzernamen und die Beschreibung für die Gruppe eingeben. Darunter können Sie die Mitglieder betrachten beziehungsweise - beim Erstellen der Gruppe - hinzufügen.

In dem dann angezeigten Dialogfeld sehen Sie eine Liste der globalen Gruppen und der Mitglieder der Domäne, in der Sie sich gerade befinden. **Um auf globale Gruppen und Benutzer von vertrauten Domänen zuzugreifen, müssen Sie diese oben im Listenfeld *Namen anzeigen von* auswählen.** An dieser Stelle können Sie darüber hinaus auch zwischen der lokalen Benutzerkontendatenbank und der Domäne wechseln, wenn Sie sich auf einer Windows NT Workstation oder einen Windows NT Server in der Rolle des Servers befinden.

Sie können entweder noch Benutzer einer anderen Domäne selektieren oder die ausgewählten Benutzer durch Auswahl der Schaltfläche OK in die lokale Gruppe aufnehmen. Dort können Sie sich mit der Schaltfläche *Vollständigen Namen anzeigen* auch die kompletten Namen der Benutzer anzeigen lassen, was die Übersichtlichkeit bei der Administration erhöht - zumindest dann, wenn Sie aussagekräftige vollständige Namen definiert haben.

Für die so definierten Gruppen können Sie die Mitglieder und die Beschreibung anpassen. Um die Mitgliederliste einer Gruppe einzusehen oder zu verändern, verwenden Sie einen Doppelklick auf den Eintrag für die Gruppe im Benutzer-Manager. Sie erhalten dann wieder ein Dialogfeld angezeigt, das bis auf den nun festen Gruppennamen dem Dialogfeld der Neuanlage entspricht.
Anstelle eines Doppelklicks können Sie auch den Befehl *Eigenschaften* aus dem Menü *Benutzer* verwenden. Den Namen einer Gruppe können Sie **nicht** verändern.

6.3.2.3 Vordefinierte Gruppenberechtigungen (Server)

Für den Umgang mit den Gruppen, die sinnvolle Zuordnung von Benutzern und die Definition von globalen und lokalen Gruppen ist es nun erforderlich, über die vordefinierten Berechtigungen für diese Gruppen im Bilde zu sein. Dabei können Sie zwischen Benutzerrechten, die verändert werden können, auf der einen Seite und internen Rechten, die sich nicht verändern lassen, auf der anderen Seite unterscheiden. Die nachfolgende Tabelle gibt einen Überblick über die so definierten Berechtigungen für die globalen Gruppen:

	Administratoren	Server-Operatoren	Konten-Operatoren	Drucker-Operatoren	Sicherungs-Operatoren	Jeder	Benutzer	Gäste
Lokale Anmeldung	■	■	■	■	■			
Zugriff auf diesen Computer vom Netz	■					■		
Übernehmen des Besitzes an Dateien und Objekten	■							
Verwalten von Überwachungs- und Sicherheitsprotokoll	■							
Ändern der Systemzeit	■	■						
System herunterfahren	■	■	■	■	■			
Herunterfahren von einem Fernsystem aus	■	■						
Sichern von Dateien und Verzeichnissen	■	■			■			
Wiederherstellen von Dateien und Verzeichnissen	■	■			■			

Vordefinierte Benutzerrechte beim NT-Server

	Administratoren	Server-Operatoren	Konten-Operatoren	Drucker-Operatoren	Sicherungs-Operatoren	Jeder	Benutzer	Gäste
Benutzerkonten erstellen und verwalten			■					
Globale Gruppen erstellen und verwalten	■		■					
Lokale Gruppen erstellen und verwalten	■		■				■	
Benutzerrechte zuweisen	■							
Überwachung von Systemereignissen verwalten	■							
Server sperren	■	■				■		
Sperre eines Servers übergehen	■	■						
Festplatte des Servers formatieren	■	■						
Allgemeine Gruppen erstellen	■	■						
Lokale Profile unterhalten	■	■	■	■	■			
Verzeichnisse freigeben und Freigabe beenden	■	■						
Drucker freigeben und Freigabe beenden	■	■		■				

Nicht veränderbare interne Berechtigungen beim NT-Server

Dabei sind noch einige kleine Einschränkungen zu beachten. Die Konten-Operatoren dürfen keine Veränderungen bei den Administratoren oder anderen Operatoren vornehmen. Damit wird sichergestellt, dass diese nur gewöhnliche Benutzer verwalten dürfen.

Die Benutzer können zwar grundsätzlich lokale Gruppen erstellen. Um das zu machen, müssen Sie jedoch entweder Zugang zu einem Benutzer-Manager für Domänen haben oder sich lokal am Server anmelden können. Damit besteht zunächst eine Einschränkung. Allerdings ist diese Konstruktion nicht unproblematisch, da sich der Benutzermanager für Domänen zum Beispiel im Windows-NT Resource-Kit findet, das wiederum im Buchhandel erhältlich ist.

6.3.2.4 Vordefinierte Gruppenberechtigungen (Workstation)

In der gleichen Form gibt es auch auf einer NT-Workstation vordefinierte Gruppen, denen ebenfalls bestimmte Systemrechte zugeordnet sind.

	Administratoren	Hauptbenutzer	Benutzer	Gäste	Jeder	Sicherungs-Operatoren
Lokale Anmeldung	■	■	■	■	■	■
Zugriff auf diesen Computer vom Netz	■	■			■	
Übernehmen des Besitzes an Dateien und Objekten	■					
Verwalten von Überwachungs- und Sicherheitsprotokoll	■					
Ändern der Systemzeit	■	■				
System herunterfahren	■	■	■		■	■
Herunterfahren von einem Fernsystem aus	■	■				
Sichern von Dateien und Verzeichnissen	■					■
Wiederherstellen von Dateien und Verzeichnissen	■					■
Laden und entfernen von Gerätetreibern	■					

Vordefinierte Benutzerrechte auf der NT-Workstation

	Administratoren	Hauptbenutzer	Benutzer	Gäste	Jeder	Sicherungs-Operatoren
Benutzerkonten erstellen und verwalten			■			
Lokale Gruppen erstellen und verwalten	■		■			
Benutzerrechte zuweisen	■					
Überwachung von Systemereignissen verwalten	■					
Arbeitsstation sperren	■	■				■
Sperre einer Arbeitsstation übergehen	■	■				
Festplatte einer Arbeitsstation formatieren	■	■				
Allgemeine Programmgruppen erstellen	■	■				
Lokale Profile beibehalten	■	■	■	■	■	
Verzeichnisse freigeben und Freigabe beenden	■	■				
Drucker freigeben und Freigabe beenden	■	■		■		

Nicht veränderbare interne Systemrechte auf einer NT-Workstation

Ebenso gibt es auch hier eingebaute Systemrechte, die nicht nachträglich verändert werden können. Die obige Tabelle gibt darüber einen Überblick.

Auch hier gilt, dass die Berechtigungen der Gruppe Hauptbenutzer für die Verwaltung von Benutzern sich wieder nur auf gewöhnliche Benutzer, nicht auf Administratoren bezieht.

6.3.2.5 Besonderheiten

Das bisher diskutierte Konzept für die Gruppen bezieht sich ausschließlich auf die Windows- NT-Server, die als Domänen-Controller konfiguriert sind. Daneben gibt es aber auch noch die Möglichkeit, mit der Windows-NT-Workstation oder mit dem Windows-NT-Server in der Rolle eines Servers zu arbeiten. In diesem Fall gibt es Besonderheiten im Konzept der Gruppen zu beachten.

Die erste Frage, die zu klären ist, ist die nach dem Zugriff auf die lokale Benutzerkontendatenbank einer NT-Workstation. Wenn Sie mit dem **Benutzermanager für Domänen** arbeiten, sehen Sie zunächst die Benutzerkontendatenbank der Domäne, in der Ihre Arbeitsstation Mitglied ist. Auf der Windows-NT-Workstation dagegen gibt es einen Benutzer-Manager, mit dem die lokale Benutzerkontendatenbank verwaltet werden kann. Der Benutzermanager der Windows-NT-Workstation stellt aber keine Funktion bereit, um auf eine andere Workstation zu wechseln.

Den Ausweg bietet der Benutzermanager für Domänen. Im Menü Benutzer findet sich der Befehl Domäne auswählen. In dem angezeigten Dialogfeld sehen Sie eine Liste der Domänen, die zur Zeit verfügbar sind. Anstelle der Auswahl einer Domäne aus der Liste können Sie aber auch den Namen einer Windows-NT-Workstation oder des Windows-NT-Server in der Rolle eines Servers eingeben, dessen lokale Benutzerkontendatenbank Sie verwalten wollen. Den Namen des Rechners müssen Sie in UNC-Schreibweise mit zwei vorangestellten \\ angeben:

\\PC04

Das System wechselt dann auf die Benutzerkontenbank der angegebenen Maschine. Die Funktionalität des Benutzermanagers für Domänen wird in diesem Fall so eingeschränkt, dass sie der des lokalen Benutzer-Managers entspricht. Das führt zu folgenden Unterschieden:

Funktion des Benutzer-Managers für Domänen	Merkmale bei der Verwaltung einer Arbeitsstation
Verwalten von Gruppenmitgliedschaften für Benutzerkonten	Lokale Benutzerkonten können nicht globalen Gruppen angehören, denn es gibt auf Arbeitsstationen keine globalen Gruppen. Benutzerkonten haben keine Einstellung für eine primäre Gruppe. Primäre Gruppen werden in Dornänen eingesetzt und unterstützen POSIX-Anwendungen sowie Benutzer, die sich unter Verwendung von Windows NT Services für Macintosh anmelden.
Zuordnen von Benutzerprofilpfaden zu Benutzerkonten	Benutzerkonten auf Arbeitsstationen können keine Benutzerprofilpfade zugewiesen werden. Das Feld *Pfad für Benutzerprofil* steht im Dialogfeld *Umgebungsprofil für Benutzer* nicht zur Verfügung.
Verwalten von Anmeldezeiten, Anmeldearbeitsstationen und Kontoinformationen für Benutzerkonten	Diese Informationen gelten nicht für Benutzerkonten von Arbeitsstationen. Daher erscheinen die Schaltflächen *Zeiten, Anmelden von und Konten* nicht in den Dialogfeldern *Neuer Benutzer* und anderen Dialogfeldern.
Verwalten von globalen Gruppen	Globale Gruppen gibt es auf Arbeitsstationen nicht. Der Befehl *Neue globale Gruppe* steht im Menü *Benutzer* -nicht zur Verfügung.
Verwalten der Richtlinien für Konten	Im Dialogfeld *Richtlinien für Konten* steht die Option *Fernbenutzer bedingungslos vom Server bei Ablauf der Anmeldezeit trennen* nicht zur Verfügung.
Verwalten von Vertrauensstellungen	Es können keine Vertrauensstellungen eingeräumt

	werden. Der Befehl *Vertrauensstellung* steht im Menü *Richtlinien* nicht zur Verfügung. Das ergibt sich daraus, dass nur Domänen in Vertrauensstellungen stehen können.

Diese Unterschiede sind allerdings insofern nicht gravierend, als globale Gruppen ohnehin auf der Ebene der Domäne definiert werden und auch Benutzer sinnvollerweise ausschließlich auf dieser Ebene eingerichtet werden. Die einzige Funktionalität, die also auf der lokalen Ebene erforderlich ist, sind die lokalen Gruppen. Außerdem müssen gegebenenfalls die Richtlinien für Benutzerrechte und die Überwachung angepaßt werden. Alle anderen Funktionen sind schlicht deshalb nicht vorhanden, weil sie im Konzept von Windows NT nicht erforderlich sind - die bei der Windows-NT-Workstation nicht verfügbaren Funktionen werden sinnvoll und besser vom Windows-NT-Server zentral bereitgestellt.

6.3.3 Workstationänderungen bei Hinzufügen zur Domäne

Wenn Sie eine Windows NT Workstation zu einer Domäne hinzufügen, werden zunächst zwei Einstellungen vorgenommen:

Die Gruppe *Domänen-Admins* wird Mitglied der lokalen Gruppe *Administratoren. Damit* werden alle Administratoren der Domäne automatisch auch zu Administratoren der Workstation beziehungsweise des Windows NT Server in der Rolle des Servers.

Die Gruppe *Domänen-Benutzer* wird Mitglied der lokalen Gruppe *Benutzer.* Damit werden alle Benutzer der Domäne automatisch zu Benutzern der lokalen Workstation und können sich damit dort zum Beispiel auch lokal anmelden.

Diese Einstellungen können Sinn machen - sie machen es aber nicht immer. Nachfolgend werden daher einige wichtige Sonderfälle diskutiert.

6.3.3.1 Sonderfälle

Wenn Sie einen Windows NT Server in der Rolle eines alleinstehenden Servers einrichten, um zum Beispiel darauf SAP R/3 auszuführen, dann ist davon auszugehen, dass in den vielen Fällen die Netzwerk-Administratoren keineswegs Administratoren auch des Systems R/ 3 sein sollen - auch wenn das eine Frage ist, deren Beantwortung von dem im jeweiligen Unternehmen beschäftigten Personal abhängt.

Um die Administration personell zu trennen, können Sie eine Gruppe *SAP-Admins* als globale Gruppe in der Domäne definieren. Auf dem Windows NT Server ändern Sie dann die Zuordnung zur lokalen Gruppe *Administratoren* beim R/3-Server so ab, dass anstelle der *Domänen-Admins* nur noch die *SAP-Admins* Mitglied dieser lokalen Gmppe und damit Administratoren des lokalen Systems sind.

Die gleiche Vorgehensweise empfiehlt sich, wenn Sie mit einem Windows NT Server als Datenbank-Server arbeiten. Auch hier ist auf der Ebene der Domäne eine Gruppe *DB-Admins* zu definieren und diese in die lokale Gruppe *Administratoren* des Servers anstelle der *Domänen-Admins* aufzunehmen.

Der lokale Benutzer *Administrator* der Windows NT Arbeitsstation beziehungsweise des Windows NT Servers mit der Rolle eines Servers stellt ein grundsätzliches Problem dar. Hier empfiehlt es sich, das Kennwort und gegebenenfalls auch den Benutzernamen dieses - Benutzers zu verändern und diese in einem geschlossenen Umschlag sicher zu verwahren. Sie benötigen dieses Benutzerkonto in der Regel nicht, da ja auch Administratoren der Domäne als Administratoren über die Zuordnung der globalen Gruppe verfügbar sind. Durch die Quasi-Sperrung dieses Kontos erreichen Sie, dass sich niemand an den Administratoren der Domäne vorbei zu einem "lokalen" Administrator dieser Arbeitsstation machen kann. Gleichzeitig haben Sie damit noch eine Sicherheit, um wieder an das System zu kommen, wenn aus irgendwelchen Gründen der Zugriff der Administratoren der Domäne nicht mehr möglich sein sollte.

Falls ein normaler Benutzer eigenständig seine Windows NT-Arbeitsstation installiert, schafft das kein Sicherheits-Problem. Der Benutzer kann sich nur in die Domäne integrieren, wenn er den Benutzernamen und das Kennwort eines Administrators der Domäne kennt. Da das nicht der Fall ist, muss letztlich ein Adrninistrator mit dem Server-Manager ein Benutzerkonto für seine Maschine erstellen und ihn in die Domäne aufnehmen. Dieser Schritt kann aber dazu genutzt werden, unverzüglich das Kennwort des lokalen Administrators zu verändern und gegebenenfalls andere, lokal definierte Benutzer und Gruppen wieder zu löschen. Danach kann nur noch der Administrator der Domäne das System verwalten.

Ein Administrator einer Windows NT Workstation ist im Übrigen nie Administrator der Domäne. Hier besteht eine einseitige Abhängigkeit, die nur von der Domäne zur Workstation und nicht umgekehrt geht - es gibt ja zum Beispiel auch keine globalen Gruppen auf der Windows NT Workstation, die in lokale Gruppen der Domäne integriert werden könnten.

Sie sollten auf der Ebene der Domäne eine **globale Gruppe *Backup*** definieren. Diese Gruppe können Sie zum Mitglied aller Gruppen ***Sicherungs-Operatoren*** beim Windows NT Server und bei der Windows NT Workstation machen. Damit können Sie zentral definieren, welche Benutzer ein Backup durchführen dürfen. Dieses Konzept müssen Sie allerdings abhängig vom verwendeten Backup-Programm gestalten, da die meisten gängigen Backup-Programme mit speziellen Benutzern arbeiten, unter Verwendung deren Konto der Dienst gestartet wird.

Um den lokalen Zugriff auf eine Windows NT Workstation zu beschränken, können Sie zwei einfache Schritte verwenden:

Sie ordnen zunächst zum Beispiel eine **Gruppe ORG** anstelle der Gruppe *Domänen-Benutzer* als Mitglieder für die Gruppe der *Benutzer* zu. Damit sind nur noch die Benutzer der angegebenen Gruppe - in unserem Fall zum Beispiel der Abteilung Organisation - Benutzer der Windows NT Workstation. Andere Benutzer der Domäne sind dagegen keine Benutzer der Workstation mehr.

Im nächsten Schritt verändern Sie noch die Benutzerrechte für die lokale Anmeldung und die Anmeldung über das Netz so, dass auch diese nur noch den lokalen Gruppen *Administratoren und Benutzer* zugeordnet sind. Damit dürfen sich nur noch die Mitglieder dieser Gruppen mit dem System verbinden. Dieses Verfahren ist sinnvoller als die Beschränkung des Zugriffs einzelner Benutzer auf bestimmte Arbeitsstationen, wie es bei der Definition von Benutzern eingestellt werden kann.

7 Werkzeuge zur Leistungsüberwachung und -optimierung

Prozesse bedeuten für die Systemleistung das, was Dateien für die Systemsicherheit bedeuten: Sie stellen die zentrale Einheit dar, über die der Administrator die Kontrolle hat. Die Verwaltung von Systemressourcen entspricht zum großen Teil der Verwaltung von Prozessen. Windows NT bietet die Möglichkeit, die Prozessausführung zu beobachten und ihre Ausführungscharakteristika bis zu einem gewissen Grad zu verändern.

7.1 Der Systemmonitor

Der Systemmonitor von Windows NT kann diverse Systemstatistiken anzeigen und überwachen. Rufen Sie das Werkzeug über den Menüpfad **Start-→Programme--->Verwaltung (Allgemein)-→Systemmonitor** oder mit dem Befehl **perfmon** auf. Dieses Werkzeug kann Werte verschiedener Statistiken anzeigen und grafisch darstellen; die Werte werden als *Datenquellen* bezeichnet. Es gibt drei Arten von Datenquellen: aktuelle Werte einer Systemstatistik, Durchschnittswerte über einen bestimmten Zeitraum und den Unterschied zwischen zwei Werten. Sie können Gruppen von Zählern erstellen und für wiederholte Auswertungen abspeichern (verwenden Sie dazu den Menüeintrag **Datei →Einstellungen speichern**).

Zu den Objekten, die überwacht werden können, gehören diverse Eigenschaften des Systems selbst, jeder Prozessor, echter und virtueller Speicher, Cache, einzelne Prozesse oder Threads, die ausgelagerten Seiten sowie Netzwerkschnittstellen und -protokolle.

HINWEIS Sie können außerdem physische und logische Festplattenquellen überwachen. Diese müssen allerdings zunächst mit dem Befehl **diskperf -ye** aktiviert werden. Mit der Option **-n** deaktivieren Sie diese Zähler wieder. Das System muss neu gestartet werden, damit die Änderungen wirksam werden.

Der Systemmonitor kennt mehrere Arbeitsmodi. Am wichtigsten ist es, das Sammeln von Daten, bekannt als *Protokollieren,* und das Betrachten von Daten auseinander zuhalten. Für das Betrachten von Daten gibt es drei verschiedene Ansichten: *Diagramm*, *Warnungen und Report.* Das Protokollieren besteht aus dem Sammeln und Aufzeichnen bestimmter Daten der Systemleistung über einen gewissen Zeitraum zur späteren Analyse. Sie können aktuelle Daten oder zuvor aufgezeichnete betrachten, und zwar jeweils als Text oder in einer grafischen Ansicht.

Die Elemente des Menüs **Ansicht** wählen den aktiven Betriebsmodus aus.

7.1.1 Daten zur Systemleistung anzeigen

Als Beispiel erstellen wir eine einfache Grafik der aktuellen CPU-Ausnutzung. Um zu beginnen, wählen Sie **Ansicht--->Diagramm** (und möglicherweise **Datei--->Neues Diagramm**, um die gegenwärtige Anzeige zu löschen). Nun wählen wir die Zähler aus, indem wir das Menü **Bearbeiten-->Diagramm erweitern ...** auswählen, wodurch ein Dialogfenster (Diagramm erweitern) geöffnet wird.

Die verfügbaren Datenquellen sind nach Objekten gruppiert, und wir beginnen mit dem Objekt Prozessor im Feld **Objekt.** Anschließend wählen wir nacheinander drei Datenquellen aus der Liste **Datenquelle:** %Prozessorzeit, die die gesamte Auslastung der CPU anzeigt, die %Privilegierte Zeit, die die Kernel-Zeit anzeigt, und %Benutzerzeit, die die CPU-Zeit im Benutzer-Modus anzeigt. Dazu klicken Sie jeweils auf **Hinzufügen.** Mit den Feldern weiter unten im Dialogfenster können Sie die Skalierung der Daten und die Art der Darstellung der gegenwärtig gewählten Datenquelle wählen.

In diesem Beispiel wird im Systemmonitor

- wird die Gesamtnutzung der CPU durch eine dicke, graue Linie dargestellt,
- die Benutzer-CPU-Zeit - also die Zeit, in der die CPU Prozesse ausgeführt (echte Arbeit erledigt) hat und
- die Kernel-CPU-Zeit (die Zeit, während der das Betriebssystem Prozessen gedient hat) dargestellt

Die Einträge unten im Diagrarnrn stellen die Legende dar, und wenn Sie auf einen Eintrag doppelklicken, können Sie die Darstellung der betreffenden Datenquelle im Diagramm verändern.

7.1.2 Leistungsdaten sammeln

Beginnen Sie das Protokollieren von Daten, indem Sie auf **Ansicht--->Protokoll** gehen und anschließend mit **Bearbeiten→Protokoll erweitern ...** die Datenquellen auswählen. Wählen Sie nach einander jede Quelle (Objekte) in dem Dialogfenster aus, und klicken Sie anschließend auf **Hinzufügen.**

Unter dem Menüeintrag **Optionen--->Protokoll** können Sie festlegen, wo die Protokolldatei gesichert wird und in welchem Intervall Messungen vorgenommen werden sollen. Klicken Sie auf **Protokollierung starten,** um das Sammeln der Daten zu beginnen. Mit demselben Dialogfenster können Sie das Sammeln beenden; die Schaltfläche **Protokollieren starten** wird während der Protokollierung zu **Protokollierung stoppen.**

Solange das System Daten sammelt, können Sie mit dem Menüeintrag **Optionen--->Lesezeichen ...** interessante Stellen markieren.

7.2 6.2 CPU-Ressourcen verwalten

Die CPU-Nutzung ist üblicherweise der erste Faktor, den Sie beim Aufspüren eines Lei stungsproblems in Betracht ziehen oder wenn Sie einfach den gegenwärtigen Systemzustand im allgemeinen einschätzen wollen. Wir beginnen diesen Abschnitt mit einem Überblick über das Windows NT-Verfahren beim Planen und Verteilen von Prozessen und gehen dann darauf ein, wie die CPU-Nutzung analysiert wird und was man gegen CPU-Ressourcenverknappungen tun kann.

7.2.1 6.2.1 Windows NT-Prozeßplanung

Benutzer rufen Prozesse auf, um Ihre Arbeit zu erledigen, und diese Prozesse bestehen üblicherweise aus einem einzigen Thread. Im allgemeinen besitzen sie nur dann zwei oder mehr Threads, wenn sie von mehreren Benutzern in einer Umgebung mit mehreren CPUs verwendet werden. Threads sind die Einheiten, die vom Betriebssystem letzten Endes ausgeführt werden.

Windows NT verwendet einen *prioritätsbasierten Round-Robin-Scheduling-Algorithmus,* um die CPU-Ressourcen zwischen mehreren, miteinander im Wettbewerb stehenden Threads zu verteilen. Jeder Prozess besitzt eine ihm zugeordnete Basisprioritätsklasse, die seine allgemeine Wichtigkeitsstufe im Vergleich zu anderen Prozessen im System darstellt. Die möglichen Prioritätsklassen sind Low (niedrig), Normal (normal), High (hoch) und Realtime (Echtzeit).

Jeder Thread besitzt eine numerische Basisprioritätsklasse, die seine Wichtigkeit gegenüber anderen Threads angibt; sie wird aus der Basisprioritätsklasse des Prozesses abgeleitet, dem dieser Thread gehört. Die Thread-Prioritäten unter Windows NT reichen von 1[5] bis 31, wobei höhere Zahlen wichtigere Threads bedeuten. Die Prioritätsklasse Low bezieht sich auf eine Stufe von 4, Normal auf 7 und High auf 13. Prioritäten oberhalb von 16 werden für Echtzeit-Prozesse verwendet.

Threads besitzen außerdem eine Ausführungspriorität - einen ganzzahligen Wert, der häufig dynamisch berechnet wird. Zur Berechnung trägt unter anderem bei, wie oft der Thread ausgeführt wurde. Diese dynamische Prioritätsstufe weicht maximal zwei Stufen von der Basispriorität des Threads ab.

Auch wenn zu einem bestimmten Zeitpunkt viele Threads gleichzeitig existieren können, kann immer nur jeweils ein einziger pro CPU ausgeführt werden. Immer wenn die CPU frei ist, wählt der Scheduler einen bevorzugten Thread aus, dessen Ausführung dann begonnen oder wieder aufgenommen wird. Dieses ist der Thread mit der höchsten Ausführungspriorität.

[5] Die Prioritätsstufe 0 ist für die Verwendung durch das Betriebssystem reserviert.

Sobald ein Thread mit der Ausführung beginnt, wird er so lange ausgeführt, bis er auf die Beendigung eines Ein-/Ausgabevorgangs warten muss, eine Unterbrechungsanforderung erhält (zum Beispiel, weil der Benutzer ihn abbricht oder das System ihn anhält, weil ein Thread mit höherer Priorität ausgeführt werden soll), auf eine andere Art freiwillig oder unfreiwillig die Kontrolle über die CPU abgibt oder das maximale Ausführungs-Quantum (die Zeitscheibe) erreicht. Sobald der gegenwärtige Prozess nicht mehr ausgeführt wird, sucht der Prozess-Scheduler erneut einen bevorzugten Thread auf dem System aus und startet ihn oder nimmt ihn wieder auf.

Mehrere Threads der gleichen Prioritätsstufe wandern in eine Warteschlange für diese Prioritätsstufe. Immer wenn die CPU frei ist, startet der Scheduler den Thread am Anfang der Warteschlange mit der höchsten Prioritätsstufe. Wenn der Thread am Anfang einer Ausführungswarteschlange die Ausführung beendet, wird innerhalb dieser Warteschlange der nächste Thread an den Anfang verschoben.

Der Scheduler verändert die Ausführungsprioritäten von Threads auf einer sich ständig verändernden Basis. Zum Beispiel wird die Ausführungspriorität eines Threads immer dann verringert, wenn die Ausführung unterbrochen wird. Auf Workstations wird die Priorität eines Threads erhöht, wenn er nach einem Wartezustand wieder aufgenommen wird (um 1 nach Ein-/Ausgabevorgängen auf Festplatten und um 5 nach der Rückkehr aus der Tastatureingabe). Außerdem erhöht der Scheduler die Prioritäten für Threads, die wegen zu knapp zugeteilter CPU-Zeit verhungern-, und zufällig für Threads mit geringer Priorität, damit diese eine knappe Systemressource nicht alleine belegen (wodurch ein Flaschenhals für andere Threads geschaffen wird).

Sie können den Scheduler auch so konfigurieren, dass er die Priorität des Threads erhöht, der zum Vordergrundprozess des Systems gehört, um eine akzeptable Reaktionszeit für interaktive Vorgänge sicherzustellen. Rufen Sie dazu das Element **System** in der **Systemsteuerung** auf, und wählen Sie die Registerkarte **Leistungsmerkmale**. Sie erreichen dieses Dialogfenster auch über den Eintrag **Eigenschaften** im Kontextmenü von **Arbeitsplatz.**

Mit dem Schieberegler im Bereich **Ausführung für Anwendungen** des Dialogfensters können Sie zwei Stufen für die Erhöhung des Vordergrundprozesses angeben. Die mittlere (nicht gekennzeichnete) Position bevorzugt den Vordergrundprozess gegenüber Hintergrundprozessen, gibt letzteren dennoch einige CPU-Ressourcen. Die Position **Maximal** bedeutet die kürzesten interaktiven Antwortzeiten für den Vordergrundprozess.

7.2.2 6.2.2 Gegen knappe CPU-Ressourcen vorgehen

Wenn eine Überbelegung der CPU-Ressourcen die Quelle des Flaschenhalses darstellt, haben Sie zwei Möglichkeiten, die Situation zu verbessern: Sie können die verfügbaren CPU-Ressourcen rationieren oder zusätzliche CPU-Kapazität bereitstellen.

Wenn Sie einige Aufgaben gegenüber anderen bevorzugen wollen, können Sie die bestehenden CPU-Ressourcen mit Prozessprioriäten ausdrücklich aufteilen. Sie können die Prioritätsklasse eines bestehenden Prozesses verändern, indem Sie ihn auf der Registerkarte **Prozesse** des Task-Managers mit der rechten Maustaste anklicken. Wenn Sie aber einem Prozess die Prioritätsklasse **Echtzeit** zuweisen, können Sie das System leicht überlasten und unbenutzbar machen.

Wenn das Problem darin liegt, dass auf einem System einfach mehr CPU-Ressourcen angefordert werden, als zur Verfügung stehen, müssen Sie den Verbrauch der CPU- Kapazität verringern oder die Kapazität der CPU auf irgendeine Art erhöhen:

- Verschieben Sie einen Teil der Arbeit auf ein anderes (weniger stark belastetes) System,
- Führen Sie einige Aufgaben zu anderen Zeiten aus (zum Beispiel mit einem Batch- System außerhalb der Arbeitszeiten).
- Rüsten Sie das System mit einem leistungsfähigeren Prozessor aus, so dass zusätzliche CPU-Ressourcen die Arbeitslast abarbeiten können. Denken Sie daran, dass Sie das System auch **mit** einem Prozessor einer anderen Prozessorfamilie ausstatten können: Wenn der schnellste Intel-Prozessor Ihren Ansprüchen nicht genügt, denken Sie über eine Alpha-CPU als Ersatz nach.

Der Start-Befehl

Windows NT bietet den Befehl **Start,** um Prozesse ausdrücklich aufzurufen. Er ist nützlich, um einen Prozess mit einer bestimmten Prioritätsklasse zu starten und besitzt folgende Syntax:

Start [Titel] [Optionen] Befehl [Argumente]

wobei *Befehl* den auszuführenden Befehl darstellt, der entweder ein Befehl oder ein Skript von Windows NT sein kann. Diesem Befehl werden alle angegebenen Argumente übergeben. Wenn Sie einen Titel angeben, wird dieser in der Kopfzeile des erscheinenden Befehlsfensters angezeigt.

Start besitzt zahlreiche Optionen; die wichtigsten sind:

/B führt den Prozess im Hintergrund aus.

/Low, /Normal, /High, /Realzeit

gibt die Prioritätsklasse für den Prozess an (niedrig, normal, hoch, Echtzeit).

ID*Pfad*

legt das Arbeitsverzeichnis für den Prozess fest.

Folgendes Beispiel führt das Programm mit dem Namen **G98** mit **niedriger** Priorität im Hintergrund aus:

C:\> **Start /B /Low G98 Test178.GJF**

6.3 Verwalten der Speicherverwendung

Speicher-Ressourcen haben mindestens eine so große Wirkung auf die Systemleistung wie die Verteilung der CPU-Zeit. Damit ein System gut arbeitet, muss es mit der entsprechenden Menge Speicher ausgestattet sein, und zwar nicht nur für die größten Aufgaben, die dort ausgeführt werden, sondern für die allgemeine Mischung typischer alltäglicher Aufgaben. Zum Beispiel kann der Speicher, der für eine oder zwei große Aufgaben, die nachts ausgeführt werden, ausreicht, unter starker interaktiver Belastung tagsüber nur mittelmäßige Reaktionszeiten bieten. Andererseits kann der Speicher, der für interaktive Aufgaben ausreicht, zu Leistungsproblemen führen, wenn größere Aufgaben anstehen. Sie müssen daher beide benötigten Arten der Systemverwendung in Betracht ziehen, wenn Sie Speichererfordernisse planen und überprüfen.

6.3.1 Die Speicherverwaltung unter Windows NT

Ein Bestandteil des Windows NT-Betriebssystems, der sogenannte *Virtual Memory Manager* (VMM), manchmal auch als Speicher-Manager bezeichnet, ist für die Belegung und die Verwaltung des Systemspeichers verantwortlich. Auf Systemen ohne virtuellen Speicher muss ein Prozess auf einen kontinuierlichen physischen Speicher zugreifen können, der seinem derzeitigen Abbild und seinen Daten-Erfordernissen entspricht, um ausgeführt werden zu können. Virtuelle Speichersysteme machen sich die Tatsache zunutze, dass der größte Teil dieses Speichers nicht an dauernd tatsächlich verwendet wird, Daten werden nur dann von der Festplatte gelesen, wenn sie benötigt werden. Das System ordnet die *virtuellen Adressen* (die relative Adresse eines Ortes von Text oder Daten in bezug auf den Anfang des Abbilds des Prozesses im Speicher), die intern vom Programm verwendet werden, physischen Speicherorten zu. Wenn der Prozess auf einen Teil seines austauschbaren Speichers oder dessen Daten zugreift und sich dieser Teil gegenwärtig nicht im Speicher befindet, liest der Kernel diesen Teil von der Festplatte zurück in den Arbeitsspeicher - man spricht vom Einlagern -, wobei unter Umständen andere Seiten, die der Prozess momentan nicht benötigt, auf eine Festplatte geschrieben werden.

Daher muss für ein großes Programm, das größtenteils, sagen wir, zwei Routinen abarbeitet, sich nur der Teil des ausführbaren Abbilds mit diesen Routinen im Speicher befinden, während sie ausgeführt werden. Der restliche Teil des Programm-Abbilds wird frei und nicht-virtueller Speicher kann für andere Zwecke verwendet werden. Das trifft dann zu, wenn diese beiden Routinen ent-

weder nahe zusammen oder weit voneinander entfernt im Speicher liegen. Entsprechend muss nicht der gesamte Teil eines großen Datenbereiches dauernd im Speicher sein, wenn das Programm ihn nicht auf einmal gleichzeitig benötigt.

Wenn der physische Speicher des Systems nicht für alle derzeit ausgeführten Prozesse ausreicht, teilt der VMM den insgesamt zur Verfügung stehenden Speicher unter ihnen dynamisch auf. Wenn ein Prozess eine neue Speicherseite benötigt und keine freien oder wiederverwendbaren Seiten existieren, muss der VMM eine Seite *stehlen,* die von einem anderen Prozess benutzt wird. In diesem Fall muss der vorherige Inhalt dieser Seite möglicherweise wiederhergestellt werden; dann wird sie *ausgelagert,* d.h. in eine Auslagerungsdatei auf die Festplatte geschrieben. Wenn diese Seite später benötigt wird, wird sie wieder eingelagert, wodurch möglicherweise eine andere Seite wiederum ausgelagert wird.

Abgesehen von dem stark negativen Beigeschmack ist das *Auslagern* nicht immer eine schlechte Sache. Wenn ein nennenswerter Teil der verfügbaren Systemressourcen für das Aus- bzw. Einlagern von Seiten verwendet wird, arbeiten alle Prozesse deutlich weniger effektiv. Im schlimmsten Fall tritt das *thrashing* auf, bei dem das System die gesamte Zeit mit der Verwaltung des virtuellen Speichers beschäftigt ist und keine wirkliche Arbeit mehr erledigt. Die gesamte CPU-Zeit wird als Kernel-Zeit verwendet, und keine CPU-Zyklen werden dazu benutzt, um die Prozessausführung voranzutreiben.

Der VMM enthält mehrere moderne Techniken zu Verwaltung von virtuellern Speicher, um die Effektivität der Speicher-Ressourcen des Systems zu maximieren:

- Seiten-Anforderung: Seiten werden nur dann in den Speicher geladen, wenn ein Seitenfehler auftritt. Der Windows NT-VMM benutzt eine Clustering-Technik, in der neben der nicht vorhandenen Seite im selben Vorgang auch die umgebenden geladen werden, um spätere Seitenfehler zu vermeiden.
- Seitenschutz durch das Kopieren während des Schreibens: Wenn es möglich ist, werden mehrere, identische Seiten, die von mehreren Prozessen verwendet werden, nur ein einziges Mal im Speicher aufbewahrt. Private Kopien einer Seite werden nur dann erstellt, wenn einer der Prozesse sie verändert.
- Automatische Einstellung der Arbeitsseiten: Der VMM verkleinert die Anzahl der Arbeitsseiten von Prozessen, wenn der Speicher knapp ist. Die Anzahl der *Arbeitsseiten* (Working Sets) stellt die Größe des physischen Speichers dar, den ein Prozess zu einem bestimmten Zeitpunkt benutzt. Dabei beginnt der VMM für diejenigen Prozesse die Anzahl der Arbeitsseiten zu reduzieren, die gegenwärtig mehr Arbeitsseiten besitzen, als ihr Wert für die minimale Anzahl der Arbeitsseiten angibt. Entsprechend vergrößert der VMM automatisch bei ausreichendem Speicher die Anzahl der Arbeitsseiten für einen Prozess, der ausgelagert ist.
- Wenn der Speicher knapp ist, nimmt der VMM Speicherseiten, die von gegenwärtig ausgeführten Prozessen verwendet werden (über einen First-In/First-Out-Algorithmus, der die ältesten Seiten zuerst wiederverwendet). Solche Seiten werden allerdings einfach initialisiert, indem sie als frei gekennzeichnet und bis zum letztmöglichen Zeitpunkt nicht mit neuen Daten beschrieben *(regeneriert)* werden. Dadurch kann der Prozess, der sie besitzt, ohne Lesevorgang von der Festplatte auf sie zugreifen; vorausgesetzt, sie befinden sich noch im Speicher, wenn sie wieder benötigt werden.

6.3.2 Die Speicherverwendung beobachten

Sie können die gegenwärtige Speicherverwendung betrachten, wenn Sie im Task-Manager die Registerkarte **Systemleistung** aufrufen. Im Bereich **Speichernutzung** sehen Sie ein Diagramm mit dem prozentualen Anteil des derzeit verwendeten physischen Speichers und den insgesamt zur Verfügung stehenden physischen Speicher, nachdem die Erfordernisse des Betriebssystems erfüllt sind. Das Fenster zeigt außerdem ein Diagramm, das zeigt, wie der allgemeine Speicher zuletzt verwendet wurde, und Statistiken über die gesamten und derzeit verfügbaren Mengen an physischem Speicher und die Speicherverwendung durch den Kernel.

Das frei erhältliche Tool **WMem** (geschrieben von Steven Chervets) bietet ebenfalls Daten über den allgemeinen Speicherzustand, aber in einer kompakten Form. Die erste Zeile der Anzeige

stellt den prozentualen Anteil des gegenwärtig verwendeten physischen Hauptspeichers (als Zahl und als Balken) dar. Die zweite Zeile zeigt entsprechend den prozentualen Anteil des derzeit verwendeten Auslagerungsspeichers und die Anzahl der insgesamt benutzten Bytes.

6.4 Optimieren der Festplattenleistung

Die Festplattenleistung bildet den dritten engen Flaschenhals, der die Leistung eines Systems oder eines einzelnen Bestandteils verringern kann. In diesem Abschnitt betrachten wir einige der Faktoren, die die Festplattenleistung beeinflussen können.

Der wichtigste Faktor, der die allgemeine Festplattenleistung beeinflusst, ist die Art, wie die Festplatten auf verfügbare Controller aufgeteilt werden. Das Anschließen mehrerer Festplatten an mehrere Festplatten-Controller ist eine Möglichkeit, die Transferraten zu steigern. Wenn Sie einen Computer konfigurieren, vergleichen Sie auf jeden Fall die maximale Transferrate jedes Controllers mit der Summe der maximalen Transferraten aller Festplatten, die daran angeschlossen werden. Wenn Sie einen Controller überlasten, verringern Sie die Leistung. Um ganz sicher zu gehen, sollten Sie die addierten, maximalen Festplatten-Geschwindigkeiten auf 75 bis 80 Prozent der maximalen Controller-Geschwindigkeit begrenzen.

Nach der Hardware-Konfiguration besteht der nächste Schritt darin, die Datenverteilung zwischen den verfügbaren Festplatten zu planen, also zu entscheiden, welche Daten auf welche Festplatten kommen. Das Grundprinzip lautet, die Festplattenzugriffe so gleichmäßig wie möglich zwischen den Festplatten und Controllern aufzuteilen (um zu verhindern, dass eine Ressource zum Flaschenhals wird). In der einfachsten Form bedeutet das, die Dateien, auf die am häufigsten zugegriffen wird, auf zwei oder mehr Festplatten zu verteilen.

Wenn Sie also wollen, dass der größte Teil der Ein-/Ausgabeleistung Benutzerprozesse zur Verfügung steht, ist es in der Regel besser, die Dateien, die sie wahrscheinlich benutzen werden, auf mehrere Festplatten zu verteilen, statt alles auf eine einzige Festplatte zu speichern. Entsprechend sollten Sie Daten für mehrere große Simulationen für die jeweiligen Programme oder Aufgaben auf separate Festplatten (und idealerweise auf mehrere Controller) verteilen, damit sich diese Aufgaben möglichst wenig gegenseitig ins Gehege kommen. Das Ablegen von stark benutzten Dateien im Netzwerk statt auf lokalen Festplatten ist meistens eine Garantie für schlechte Leistung. Und schließlich ist es fast immer eine gute Idee, eine eigene Festplatte für das Betriebssystem zu verwenden (wenn Sie sich das leisten können), um die Auswirkung von Ein-/Ausgabevorgängen des Betriebssystems von Benutzerprozessen zu trennen.

Der letzte Faktor für die Festplattenleistung, ist die physische Anordnung der Dateien auf den Festplatten. Die folgenden allgemeinen Überlegungen beziehen sich auf die Beziehung zwischen Dateizugriffsmustern und Festplattenleistung:

- Die Fragmentierung von Dateisystemen verschlechtert deren Leistung. Sie tritt auf, wenn der freie Platz eines Dateisystems aus vielen kleinen Bereichen besteht und nicht aus wenigen großen Bereichen mit derselben Gesamtgröße. Das bedeutet, dass die Dateien selbst fragmentiert werden können (also nicht an einem Stück auf der Festplatte abgelegt werden), so dass der Zugriff auf sie entsprechend länger dauert. Die Fragmentierung von Dateisystemen nimmt mit der Zeit zu. Möglicherweise ist es erforderlich, das Dateisystem zu defragmentieren.
- Sequentieller Zugriff auf große Dateien (d.h. das Lesen oder Schreiben der Datei an einem Stück vom Beginn bis zum Ende der Datei) geht am schnellsten vonstatten, wenn die Dateien in einem einzigen, ununterbrochenen Bereich auf der Festplatte liegen. Es kann erforderlich sein, ein Dateisystem zu defragmentieren oder sogar neu aufzubauen, um große, ununterbrochene Bereiche auf der Festplatte zu schaffen.
- Die Festplattenleistung für sequentielle Zugriffe auf große Dateien wird auch durch das Striping verbessert.
- Die Plazierung großer Dateien, auf die nicht sequentiell zugegriffen wird (zum Beispiel Datenbanken), im mittleren Bereich von Festplatten bringt die höchste Leistung. Bei derartigen Zugriffen spielt die *Zugriffszeit* - also die Zeit, in der die Festplattenköpfe zum entsprechenden Bereich auf den Platten bewegt werden können - die größte Rolle. Die Zugriffszeiten sind am geringsten, wenn sich die Daten in der Mitte der Festplatte befinden; sie nimmt in den inneren

und äußeren Bereichen ab. Wenn Sie eine große Festplatte in mehrere Partitionen einteilen, können Sie eine in der mittleren Position erstellen und die entsprechenden Dateien im Dateisystem dieser Partition ablegen.
- Wenn Sie planen, fehlertolerante Dateisysteme zu verwenden, wählen Sie die passende Art für die Festplattenzugriffsmuster aus, die Sie erwarten, um die Festplattenleistung zu optimieren. Spiegelsätze bieten hohe Leistungen für kleine Datenübertragungen, während Stripe Sets mit Parität die Anzahl der Ein-/Ausgabevorgänge pro Sekunde optimieren.
- Seien Sie sich darüber im klaren, dass es viele verschiedene Möglichkeiten gibt, fehlertolerante Dateisysteme zu implementieren, die unterschiedliche Leistungsdaten bieten. Wenn Sie zum Beispiel ein fehlertolerantes Datenbank-System einrichten wollen, können Sie eine hardwarebasierte RAID-Lösung verwenden (sofern Sie sich diese leisten können), von Windows NT unterstütztes, softwarebasiertes RAID 1 oder 5 oder die Spiegelung, die von der Datenbankanwendung unterstützt wird. Um die beste Wahl zu treffen müssen Sie wissen, wie alle diese Lösungen arbeiten. In diesem Beispiel ist die beste Lösung in der Regel softwarebasiertes RAID, implementiert mit dem Windows NT-Betriebssystem, da die Spiegelungen von vielen Datenbankanwendungen sequentiell arbeiten (d.h., es wird zu einem beliebigen Zeitpunkt immer nur ein Datenblock geschrieben, statt zwei parallel zu schreiben).

6.5 Netzwerkleistung

In der Windows NT-Umgebung ist die Netzwerkleistung ebenso wichtig wie die Leistung einzelner Computer. Eine hohe Netzwerkleistung hängt von gut eingestellten Servern ab, insbesondere von ihren CPU-, Speicher-, und Festplattenleistungen. Der Datendurchsatz im Netzwerk hängt außerdem von einer gut durchdachten Einteilung von Verantwortlichkeiten und Aufgaben auf die verschiedenen Server und die anderen Systeme im Netzwerk ab.

Hier einige Punkte und Empfehlungen bezüglich der Netzwerkleistung unter Windows NT:
- Stellen Sie sicher, dass wichtige Netzwerk-Server über ausreichend Hauptspeicher verfügen. Dateiserver sollten außerdem für maximale Festplattenleistung konfiguriert und eingestellt sein.
- Sie müssen die erwartete und die gewünschte Arbeitsbelastung kennen, wenn Sie Netzwerkprotokolle auswählen. Wählen Sie das schnellste verfügbare Protokoll, wenn Sie für eine bestimmte Funktion die Wahl haben (üblicherweise TCP/IP). Installieren Sie nur die Protokolle, die Sie auf den verschiedenen Systeme wirklich benutzen wollen, um einen Overhead zu vermeiden.
- Legen Sie die Netzwerkbindungen entsprechend Ihren Leistungsvorgaben und typischen Verwendungsmustern an, indem Sie wichtigere Protokolle oberhalb von unwichtigeren anordnen (siehe Kapitel 8).
- Wählen Sie das der Belastung entsprechende Profil für jeden Netzwerk-Server aus (Server-Dienst-Optimierung).
- Die Auswahl der Hardware ist ein wichtiger Faktor, der die Netzwerkleistung beeinflusst. Zum Beispiel bieten Netzwerkkarten in der 32-Bit-Busmaster-Ausführung den höchsten Durchsatz. Langsame Netzwerkkarten in wichtigen Computern können zu einer schlechten Gesamtleistung des Netzwerkes bedeuten.
- Probleme der Netzwerkleistung müssen untersucht werden, indem Sie das Netzwerk als ganzes beobachten. Leistungsdaten und Fehlerraten vieler Systeme müssen verglichen werden, um die Ursache und den Umfang des Problems festzustellen.
- Die Verschlechterung der Netzwerkleistung im Laufe der Zeit kann mit systematischen Tests zuverlässig herausgefunden und untersucht werden. Wenn Sie vermuten, dass kürzlich netzwerkbezogene Leistungsprobleme aufgetreten sind oder sich verstärkt haben, denken Sie sich einige Standardvorgänge aus, mit denen Sie die Leistung beobachten und messen können (der Transfer einer großen Datei ist ein guter Ausgangspunkt). Führen Sie die Tests zunächst in einem nicht oder nur gering belasteten Netzwerk durch und anschließend unter tatsächlichen Bedingungen. Wenn Sie dieselben Tests mit unterschiedlichen Quell- und Zielcomputern ausprobieren, können Sie die Quellen von Leistungsproblemen schneller finden.

8 Fragen zum allgemeinen Verständnis

1) Systemmonitor:

a) Kann der Systemmonitor auch aus der Eingabeaufforderung gestartet werden?

b) Welches sind die wichtigsten Objekte, die der Systemadministrator ”im Auge behalten” sollte?

c) Worin besteht der Unterschied zwischen den Datenquellen *Prozessorzeit*, *Privilegierte* Zeit und *Benutzerzeit* in dem Objekt Prozessor?

2) CPU-Ressource:

a) Wie lassen sich Vordergrundprozesse beschleunigen?

b) Welche Prioritätsklassen gibt es und wie können Sie die Priorität einzelner Prozesse ändern?

c) Welche Möglichkeiten bestehen, um eine CPU- Überlastung zu vermeiden?

d) Kennen Sie Beispiele für Echtzeitprozesse?

e) Was passiert, wenn zu viele Echtzeit-Prozesse auf einer CPU verarbeitet werden?

3) Speicherverwendung und Festplattenleistung

a) Wie kann die Speicherverwaltung sichtbar gemacht werden?

b) Welche Möglichkeiten bestehen um die Festplattenleistung zu optimieren?

8.1.1.1 Antwort auf:

1a) Ja, mit "***perfmon***"

1b) Prozessor-Auslastung, echter und virtueller Speicher, Cache, ggf. einzelne Prozesse oder Threads, Netzwerkschnittstellen / -protokolle, Festplatten mit "***diskperf –ye***" aktivieren

1c) Prozessorzeit: Die gesamte Auslastung der CPU-Kapazität

Privilegierte Zeit: Die Zeit die der Prozessor mit Betriebssystemaufgaben (Kernel-Zeit) beschäftigt ist.

Benutzerzeit: Netto, d. h. Zeit in der tatsächliche Anwendungsprogramme ausgeführt werden.

2a) Systemsteuerung→ System → Leistungsmerkmale oder im Kontextmenü Arbeitsplatz → Eigenschafen.

2b) LOW, NORMAL, HIGH Taskmanager → mit rechter Maustaste auf Prozess und Prioritätsklasse änd.

2c) Arbeit verlagern auf andere Rechner, Aufgaben zeitlich versetzen, schnellerer Prozessor

2d) Maschinensteuerung (Baggerhydraulik, Roboter, Raketensteuerung, medizinische Geräte, Fertigungsstrassen, Messwerterfassung, ABS, ESP)

2e) Die Privilegierte Zeit zum Task-Management steigt so stark an, dass keine Zeit für die eigentlichen Aufgaben bleiben. Der Rechner ist überlastet und stürzt ggf. ab.

3a) Taskmanager → Systemleistung → Speichernutzung

3b) Mehrere Festplatten an mehrere Controller, Daten gleichmäßig auf Platten verteilen; defragmentieren; RAID-Lösung; bei nicht sequentiellen Zugriffen Daten in der Festplattenmitte durch Partitionierung plazieren.

9 RAID-Systeme

Windows NT Server bietet die Software-Implementierung einer fehlertoleranten Technologie, die als RAID bezeichnet wird. Die RAID-Technologie ist genormt und in verschiedene Ebenen unterteilt. Die einzelnen Ebenen unterscheiden sich in ihrer Leistungsfähigkeit, Zuverlässigkeit und den Kosten. Windows NT Server unterstützt als Fehlertoleranzverfahren die RAID-Ebenen 1 und 5.

Wie wird ein System durch den Einsatz von RAID geschützt? RAID bietet Fehlertoleranz durch die Implementierung von *Datenredundanz.* Bei Datenredundanz werden die Daten auf mehr als eine Festplatte geschrieben, so dass die Daten bei Ausfall einer einzelnen Festplatte wiederhergestellt werden können. In diesem Kapitel werden nur die RAID-Arten beschrieben, die von Windows NT Server implementiert werden können, sowie die Auswirkungen bei der Verwendung der einzelnen RAID-Arten.

9.1 Hardware- und Software-Implementierungen von RAID

Fehlertoleranz durch RAID kann entweder als Hardware- oder als Software- Lösung implementiert werden. Die folgenden Punkte sind bei der Entscheidung für eine der Fehlertoleranzlösungen zu beachten:

- Fehlertolerante Software steht nur für Windows NT Server zur Verfügung. Windows NT Workstation bietet keine Fehlertoleranz.
- Software-Fehlertoleranz ist kostengünstiger als eine Hardware-Fehlertoleranzlösung.
- Die Systemleistung ist bei Verwendung von Hardware-Fehlertoleranz im allgemeinen höher.
- Bei Verwendung einer Hardware-Fehlertoleranzlösung sind Sie unter Umständen an einen einzelnen Hardware-Hersteller gebunden.
- Einige Hersteller von **Hardware-Fehlertoleranzlösungen** bieten Implementierungen an, bei denen **fehlerhafte Festplatten ohne Herunterfahren des Systems ausgetauscht werden können**.

Unabhängig von der Implementierung einer Hardware- oder Software-Lösung zur Sicherstellung der Fehlertoleranz ist es unbedingt erforderlich, in regelmäßigen Abständen Sicherungskopien zu erstellen.

Darüber hinaus ist die Fehlertoleranz eines Systems nach einem Ausfall erst dann wiederhergestellt, wenn der Fehler behoben ist. Falls ein zweiter Ausfall auftritt, bevor die durch den ersten Ausfall verlorengegangenen Daten wiederhergestellt sind, lassen sich die Daten **nur** mit Hilfe einer Sicherungskopie wiederherstellen.

9.1.1 Hardware-Implementierungen von RAID

Bei einer Hardware-Lösung erfolgt die Erstellung und Regenerierung von redundanten Informationen über die Schnittstelle des Festplatten-Controllers. Einige Hardware-Hersteller implementieren RAID-Datenschutzlösungen direkt in Hardware, beispielsweise in Form von Disk Array-Controller-Karten. Da diese Verfahren herstellerspezifisch sind und die Fehlertoleranz-Software-Treiber des Betriebssystems umgehen, zeichnen sich diese Lösungen gegenüber Software- Implementierungen von RAID im allgemeinen durch eine höhere Leistungsfähigkeit aus.

9.1.2 Software-Implementierungen von RAID

Windows NT Server unterstützt zwei Software-Implementierungen von RAID: RAID 1 (Spiegelsätze) und RAID 5 (Stripe Sets mit Parität).

9.1.2.1 RAID 1: Spiegelsätze

Spiegelsätze (RAID 1) verwenden den Windows NT-Fehlertoleranztreiber (Ftdisk.sys), um dieselben Daten gleichzeitig auf zwei physische Laufwerke zu schreiben. Durch diese Duplizierung, die

auch als Spiegelung bezeichnet wird, verringert RAID 1 das Risiko eines Datenverlustes bei einem Festplattenausfall.

Bei Verwendung von Spiegelsätzen werden die auf einer Partition befindlichen Daten auf einer zweiten physischen Festplatte dupliziert. **Jede Partition, einschließlich der Boot- und der Systempartition, kann gespiegelt werden.** Diese Vorgehensweise schützt vor Datenverlusten, wenn eine einzelne Festplatte ausfällt. Windows NT Server konfiguriert Fehlertoleranz auf der Ebene des logischen Laufwerkbuchstabens, nicht auf der Ebene des physischen Datenträgers. Wenn ein Computer beispielsweise über einen physischen Datenträger mit den Laufwerken C und D und einen zweiten physischen Datenträger mit ausreichend unpartitioniertem Speicherplatz verfügt, können Sie entweder Laufwerk C oder Laufwerk D bzw. beide Laufwerke spiegeln.

Ausgedrückt in Kosten pro Megabyte sind Spiegelsätze teurer als andere Fehlertoleranzverfahren, da der vorhandene Speicherplatz nur zu 50 Prozent genutzt wird. In Peer-to-Peer-Netzwerken und kleineren Server-basierten LANs sind die Kosten für Spiegelsätze im allgemeinen niedriger, da nur zwei Festplatten benötigt werden.

Spiegelsätze können zu einer Steigerung der Leseleistung führen, da der Fehlertoleranztreiber Daten von beiden Mitgliedern des Spiegelsatzes gleichzeitig lesen kann. Beim Schreiben auf einen Spiegelsatz kann eine geringfügige Verringerung der Schreibleistung auftreten, da der Fehlertoleranztreiber gleichzeitig auf beide Mitglieder schreiben muss. Wenn ein Mitglied eines Spiegelsatzes ausfällt , nimmt die Leseleistung wieder den normalen Wert an, da der Fehlertoleranztreiber nur auf die verbleibende Partition zugreift.

Anmerkung Falls entweder die Boot-Partition oder die Systempartition Teil eines Spiegelsatzes ist, müssen Sie eine Startdiskette mit Fehlertoleranz erstellen und diese anschließend testen, um ggf. auf die intakte Bootpartition zugreifen zu können. In dem nächsten Kapitel werden die einzelnen Schritte für die Erstellung einer Startdiskette mit Fehlertoleranz beschrieben.

9.1.2.2 Festplattenduplizierung

Die beiden physischen Datenträgerpartitionen, aus denen ein Spiegelsatz besteht werden als Mitglieder des Spiegelsatzes bezeichnet. Wenn beide physischen Datenträger eines Spiegelsatzes von demselben Festplatten-Controller gesteuert werden und der Festplatten-Controller ausfällt, kann auf keines der Mitglieder des Spiegelsatzes zugegriffen werden. Es ist jedoch möglich, einen zweiten Controller zu installieren, so dass die Festplatten des Spiegelsatzes über jeweils, einen eigenen Controller verfügen. Auf diese Weise ist der Spiegelsatz sowohl gegen einen Controller-Ausfall als auch einen Festplattenausfall geschützt. Eine derartige Strategie wird als *Pestplattenduplizierung* bezeichnet. Die Duplizierung von Festplatten führt außerdem zu einer Verringerung der Bus-Aktivitäten und kann auch die Leseleistung erhöhen.

Anmerkung Bei der Festplattenduplizierung wird eine Hardwareerweiterung eines Windows NT Server-Spiegelsatzes vorgenommen. Sie erfordert keine zusätzliche Software-Konfiguration.

9.1.2.3 RAID5: Stripe Sets mit Parität

Bei Stripe Set mit Parität (RAID 5) werden aufeinanderfolgende Datenblöcke abwechselnd auf eine von mehreren Festplatten gespeichert. Außerdem werden für jeden Datenblock Paritätsdaten errechnet (über eine XOR-Operation) und abwechselnd auf die einzelnen Festplatten geschrieben. Stripe Sets mit Parität werden von Windows NT Server unterstützt.

Ein Stripe Set mit Parität unterstützt zwischen 3 und 32 Festplatten. Der aus einem Stripe Set mit Parität bestehende Block wird zur Wiederherstellung der Daten von einem fehlerhaften physischen Datenträger verwendet. Bei Ausfall einer einzelnen Festplatte tritt kein Datenverlust auf, da der Windows NT Server-Fehlertoleranztreiber die Daten auf die übrigen Festplatten geschrieben hat. Die Daten können vollständig wiederhergestellt werden. Falls beispielsweise Datenträger 3 ausfällt und ersetzt werden muss, können die Daten für die neue Festplatte mit Hilfe der Daten und Paritätsinformationen auf den einzelnen Stripes der übrigen vier Festplatten regeneriert werden.

Infolge der Paritätsberechnung erfolgen alle normalen Schreibvorgänge auf einem Stripe Set mit Parität wesentlich langsamer als Schreibvorgänge auf Stripe Sets ohne Parität.

Im Vergleich zu Spiegelsätzen können Stripe Sets mit Parität jedoch eine höhere Leseleistung aufweisen. Dies ist insbesondere dann der Fall, wenn mehrere Controller vorhanden sind, die die Daten auf mehrere Laufwerke verteilen. Falls jedoch ein Festplattenausfall auftritt, verringert sich die Leseleistung bei einem Stripe Set mit Parität, da die Daten unter Verwendung der Paritätsinformationen berechnet werden.

Stripe Sets mit Parität sind im Vergleich zu Spiegelsätzen unter Umständen kostengünstiger, da die Festplattennutzung optimiert ist. Wenn ein Stripe Set mit Parität beispielsweise vier Festplatten umfasst, beträgt der Speicherplatzmehrbedarf 25 Prozent, verglichen mit einem Speicherplatzmehrbedarf von 50 Prozent bei Spiegelsätzen. Stripe Sets mit Parität sind zur Zeit die am häufigsten eingesetzte Lösung zur Sicherstellung von Fehlertoleranz.

Anmerkung Weder die Boot-Partition noch die Systempartition kann in der Windows NT-Implementierung Bestandteil eines Stripe Sets mit Parität sein.

9.2 Implementieren von RAID 1 und RAID 5

Spiegelsätze und Stripe Sets mit Parität können gleichzeitig auf demselben Computer verwendet werden. Da ein Stripe Set mit Parität weder die System- noch die Boot-Partition enthalten kann, sollten Sie die System- und Boot- Partitionen spiegeln und die übrigen Daten durch Stripe Sets mit Parität schützen. In der folgenden Abbildung befinden sich beispielsweise die System- und die Boot-Partition auf dem Laufwerk C, das Bestandteil eines Spiegelsatzes ist. Die übrigen Daten auf Laufwerk D sind Bestandteil eines Stripe Sets mit Parität.

Beachten Sie, dass der Festplatten-Manager von Windows NT Server über ein zusätzliches Menü mit dem Namen **Fehlertoleranz** verfügt, über das sowohl Spiegelsätze als auch Stripe Sets mit Parität verwaltet werden.

9.2.1 Beim Erstellen und Löschen eines Stripe Sets mit Parität zu beachtende Punkte

Der für das Erstellen eines Stripe Sets mit Parität zu verwendende freie Speicherplatz muss auf allen Festplatten dieselbe Größe besitzen. Ist dies nicht der Fall, passt der Festplatten-Manager die einzelnen Partitionen des Satzes auf ungefähr dieselbe Größe an, wobei die nichtverwendeten Partitionsanteile als nutzbarer freier Speicherplatz zur Verfügung stehen.

Anmerkung Nach dem Erstellen eines Stripe Sets mit Parität muss der Computer neu gestartet werden.

So konfigurieren Sie Spiegelsätze

1. Melden Sie sich als Administrator an.
2. Klicken Sie auf das Laufwerk, das gespiegelt werden soll.
3. Halten Sie STRG gedrückt und klicken Sie auf den Datenträger mit genügend freiem Speicherplatz.
4. Wählen Sie im Menü Fehlertoleranz→Spiegelung einrichten.

Die Partitionen sollten jetzt denselben Laufwerkbuchstaben besitzen und violett markiert sein.

9.3 Wiederherstellen von Daten nach einem Festplattenausfall

Bei Ausfall eines Mitglieds eines Spiegelsatzes oder eines Stripe Sets mit Parität (z. B. infolge einer Stromunterbrechung oder eines Hardware-Fehlers) leitet der Fehlertoleranztreiber alle E/A-Vorgänge auf die übrigen Mitglieder des fehlertoleranten Datenträgers um. Hierdurch wird der ununterbrochene Betrieb sichergestellt. Falls Sie den Computer mit Hilfe des Server-Managers so konfiguriert haben, dass dieser Warnmeldungen sendet, und falls der Warndienst momentan aus-

geführt wird, wird eine Warnmeldung an die angegebenen Konten gesendet, dass ein Festplattenausfall aufgetreten ist.

Ist die fehlerhafte Festplatte Bestandteil eines Spiegelsatzes, der die Boot- Partition enthält, und handelt es sich bei der fehlerhaften Festplatte um das primäre physische Laufwerk, ist eine Startdiskette mit Fehlertoleranz erforderlich, um das System neu zu starten.

9.3.1 Regenerieren eines Stripe Sets mit Parität

Falls ein Mitglied eines Stripe Sets mit Parität ausfällt, arbeitet der Computer ordnungsgemäß weiter und kann weiterhin auf alle Daten zugreifen. Falls jedoch Daten angefordert werden, die sich auf dem ausgefallenen Mitglied befinden, verwendet der Windows NT Server-Fehlertoleranztreiber die Paritätsbits, um die fehlenden Daten im RAM zu regenerieren. Wenn dieser Fall eintritt, nimmt die Systemleistung ab.

Um die Daten zu regenerieren und die ursprüngliche Leistung des Computers wiederherzustellen, verwenden Sie den Festplatten-Manager, um einen Bereich mit freiem Speicherplatz als Ersatz für das ausgefallene Mitglied auszuwählen, und klicken Sie dann auf im Menü **Fehlertoleranz** auf den Befehl **Regenerieren.** Steht nicht mehr genügend Speicherplatz zur Verfügung, tauschen Sie die fehlerhafte Festplatte aus und regenerieren Sie dann die Daten.

Der Fehlertoleranztreiber liest die Paritätsinformationen von den Stripes auf den anderen Mitgliedsplatten. Anschließend erstellt er die Daten des fehlenden Mitglieds neu und schreibt sie auf das neue Mitglied.

9.3.2 Wiederherstellen von Daten nach einem Spiegelsatzausfall

Aufgrund der Datenduplizierung, die bei Spiegelsätzen erfolgt, arbeitet das System auch nach dem Ausfall eines Mitglieds des Spiegelsatzes ordnungsgemäß weiter. Um das ausgefallene Mitglied auszutauschen, muss der Administrator zunächst die Spiegelung beenden.

Verwenden Sie die folgende Vorgehensweise, um eine Spiegelung zu beenden:

1. Verwenden Sie im Festplatten-Manager aus dein Menü **Fehlertoleranz** den Befehl **Spiegelung beenden**. Beenden Sie die Spiegelsatzbeziehung, um die *intakte* Partition als separaten Datenträger zu isolieren. Unabhängig davon, welcher Datenträger den Fehler enthält, weist der Festplatten-Manager dem gespiegelten Datenträger bei Beendigung der Spiegelung den nächsten verfügbaren Laufwerkbuchstaben zu.
2. Falls das fehlerhafte Laufwerk das primäre Mitglied des Spiegelsatzes ist, ist es unter Umständen erforderlich, dem intakten Mitglied des Spielsatzes den Laufwerkbuchstaben zuzuweisen, der zuvor dem gesamten Spiegelsatz zugewiesen war. Falls beispielsweise das Laufwerk über freigegebene Ressourcen verfügt oder falls eine Verknüpfung auf ein Verzeichnis auf einem bestimmten Laufwerk verweist, muss der Laufwerkbuchstabe neu zugewiesen werden, um das ordnungsgemäße Arbeiten des Computers sicherzustellen. Nehmen wir an, dass ein Fehler in Laufwerk D auf dem Datenträger 0 aufgetreten ist. Dem intakten Mitglied auf dem Datenträger 1 (nach der ”Entspiegelung” z.B. Laufwerk H) muss auch wieder der Laufwerkbuchstabe D zugewiesen sein. Heben Sie mit Hilfe des Festplatten-Managers zunächst die Zuweisung des (defekten) Laufwerkbuchstabens D auf Datenträger 0 auf, und weisen Sie dann dem Laufwerk H den Laufwerkbuchstaben D zu.
3. Löschen Sie die fehlerhafte Partition.

Anmerkung Sie können die Ereignisanzeige verwenden, um im Systemprotokoll zu überprüfen, welche Partition fehlerhaft ist.

4. Erstellen Sie unter Verwendung von freiem Speicherplatz auf einem intakten Datenträger eine neue Spiegelsatzbeziehung. Wenn der Computer neu gestartet wird, werden die Daten aus der intakten Partition auf das neue Mitglied des Spiegelsatzes kopiert.

Anmerkung Eine Spiegelung muss auch beendet werden, wenn der Speicherplatz für andere Zwecke freigegeben werden kann.

9.4 Erstellen einer Startdiskette mit Fehlertoleranz

Wird ein Spiegelsatz für die Boot-Partition oder die Systempartition eines Computers unter Windows NT Server erstellt, ist es unbedingt erforderlich, für den Fall eines Festplattenausfalls eine Startdiskette mit Fehlertoleranz zu haben.

Im folgenden werden die einzelnen Schritte, die zum Erstellen einer mit Fehlertoleranz erforderlich sind, detailliert beschrieben:

1. Formatieren Sie eine Diskette auf einem Computer, auf dem M Server ausgeführt wird. Hierbei werden Informationen auf den Diskette geschrieben, so dass bei einem Systemstart von dieser der entsprechenden Ladedatei gesucht wird.

Anmerkung Eine Startdiskette mit Fehlertoleranz muss auf einem Computer formatiert werden, auf dem Windows NT Server ausgeführt wird.

2. Kopieren Sie die folgenden Dateien von der primären Partition des Computers auf die Startdiskette. Einige dieser Dateien sind versteckte Dateien und befinden sich im Stammordner. Verwenden Sie Windows NT Explorer, um versteckte Dateien anzuzeigen.

x86-basierte Computer

Ntldr

Ntdetect.com

Ntbootdd.sys (für SCSI-Festplatten, die kein SCSI-BIOS verwenden)*

Boot.ini

* Die Datei Ntbootdd.sys wird nur bei SCSI-Systemen angezeigt, auf denen nicht SCSI-BIOS verwendet wird.

3. Bearbeiten Sie auf lntel x86-basierten Computern die Datei **Boot.ini** so dass der Eintrag für das Betriebssystem auf die gespiegelte Kopie der Boot-Partition verweist.

4. Testen Sie die Startdiskette um sicherzustellen, dass diese ordnungsgemäß arbeitet und beim Booten Daten aus der gespiegelten Kopie der Boot-Partition verwendet.

Bei jeder Änderung der Pfadinformationen einer Partition muss die Datei Boot.ini auf der Startdiskette mit Fehlertoleranz aktualisiert werden.

10 Die Windows NT-Registrierung

In diesem Kapitel wird die Registrierung von Windows NT beschrieben. Es wird erläutert, wie Windows NT die Registrierung verwendet, um sämtliche Konfigurationseinstellungen der Hardware und Software zu speichern und auf diese zuzugreifen.

Dabei geht es um die folgenden Aufgaben:

- Beschreiben des Zwecks der Windows NT-Registrierung.
- Beschreiben der Verwendungsweise der Registrierung durch die Windows NT-Komponenten.
- Erkennen der Komponenten, aus denen sich die hierarchische Struktur der Registrierung zusammensetzt.

10.1 Die Registrierung

Die Registrierung ist eine vereinheitlichte Datenbank, in der sämtliche Konfigurationsinformationen der Hardware und Software eines lokalen Computers gespeichert sind. Das Betriebssystem Windows NT wird durch die Registrierung gesteuert, indem die entsprechenden Initialisierungsangaben zum Starten von Anwendungen und zum Laden von Komponenten, wie z.B. Gerätetreibern und Netzwerkprotokollen, zur Verfügung gestellt werden.

Im folgenden sind die in der Registrierung enthaltenen Informationstypen aufgeführt:

0 Auf dem Computer installierte Hardware, einschließlich CPU, Bus-Typ, Zeigegerät bzw. Maus und Tastatur.
1 Installierte Gerätetreiber.
2 Installierte Anwendungen.
3 Installierte Netzwerkprotokolle
4 Einstellungen von Netzwerkkarten, wie beispielsweise Interrupt, Speicherpufferadresse, Basis-E/A-Anschlußadresse, E/A-Channel Ready und Transceiver-Typ.
5 Angaben über Benutzerkonten. In der Registrierung sind beispielsweise die Gruppenmitgliedschaft sowie Rechte und Berechtigungen des Benutzers gespeichert.

10.2 Das Anzeigen der Registrierung

Unter Verwendung des Registrierungseditors kann die Registrierung direkt geändert werden. Weiterhin sind Anwendungen, wie beispielsweise die Systemsteuerung, der Benutzereditor und der Systemrichtlinien-Editor vorhanden, mit deren Hilfe basierend auf von Ihnen bereitgestellten Konfigurationsinformationen Änderungen in der Registrierung vorgenommen werden können.

Vorsicht: Beim Ändern von Werten unter Verwendung des Registrierungseditors müssen Sie mit äußerster Vorsicht vorgehen. Vom Registrierungseditor werden Fehler in der Syntax oder andere semantische Fehler nicht erkannt, und es wird daher keine Warnmeidung ausgegeben, wenn Sie einen falschen Eintrag vorgenommen haben. Die Eingabe eines falschen Eintrags kann dazu führen, dass das Betriebssystem unbrauchbar wird.

Übung

Führen Sie diese Übung auf dem Server durch.

So erstellen Sie eine Verknüpfung mit dem Registrierungseditor

1. Klicken Sie mit der rechten Maustaste auf den Desktop.

2. Klicken Sie auf Neu, und klicken Sie dann auf Verknüpfung.

3. Geben Sie regedt32.exe im Feld Befehlszeile ein.

4. Klicken Sie auf Weiter und dann auf Fertigstellen.

Auf Ihrem Desktop wird ein Symbol für die Verknüpfung mit Regedt32.exe angezeigt.

So zeigen Sie die Registrierung an

1. Starten Sie den Registrierungseditor, indem Sie auf das Verknüpfungssymbol doppelklicken.
2. Klicken Sie im Menü Optionen auf Schreibgeschützt.

   Neben Schreibgeschützt sollte ein Häkchen vorhanden sein, was darauf hinweist, dass diese Einstellung aktiviert ist. Dadurch wird verhindert, dass Sie ungewollt Änderungen in der Registrierung vornehmen.

   Beim Öffnen des Registrierungseditors werden fünf Fenster eingeblendet. In jedem Fenster wird ein Teilbaum angezeigt. Mit jedem dieser Teilbäume kann auf einen anderen Bereich der Registrierung zugegriffen werden.
3. Führen Sie die Namen der fünf Teilbäume auf, die im Registrierungseditor angezeigt werden.
4. Minimieren Sie den Registrierungseditor.

10.3 Verwenden der Registrierung durch die Windows NT-Komponenten

Unter Windows NT werden sämtliche Angaben zur Konfiguration an nur einem Ort - der Registrierung -gespeichert und überprüft. In der folgenden Abbildung. sind einige der verschiedenen Windows NT-Komponenten, die die Registrierung verwenden, dargestellt.

In der folgenden Tabelle wird beschrieben, wie die Anwendungen und Komponenten des Betriebssystems Windows NT die Registrierung zum Speichern und Abrufen von Informationen verwenden.

Komponente	Beschreibung
Hardware-Profile	Eine Reihe von Hardware-Geräten und -Diensten, die beim Starten von Windows NT aktiviert bzw. deaktiviert werden sollen, können in der Registrierung durch Erstellen eines Hardware-Profils gespeichert werden. Wenn Sie beispielsweise einen tragbaren Computer verwenden, möchten Sie möglicherweise bestimmte Geräte und Dienste aktivieren, je nachdem, ob Ihr Computer an eine Docking-Station angeschlossen ist oder nicht. Beim Starten des Computers können Sie das entsprechende Hardware-Profil auswählen, das beim anschließenden Starten von Windows NT verwendet werden soll.
Komponente	**Beschreibung**
Benutzerprofile	**Angaben über die Konfiguration werden in der Registrierung für jeden Benutzer einzeln gespeichert. Zu diesen Informationen zählen sämtliche benutzerbezogenen Einstellungen der Windows NT- Umgebung, wie z. B. Anordnung der Desktop-Elemente, eigene Programmgruppen sowie die innerhalb dieser Gruppen enthaltenen Programmsymbole, Einstellungen für den Bildschirmschoner, Netzwerkverbindungen, Druckerverbindungen, Einstellungen für die Maus, Größe und Position von Fenstern usw.**
Windows NT Kernel	Beim Systemstart extrahiert der Windows NT Kernel (Ntoskml.exe) Informationen aus der Registrierung, um festzustellen, welche Gerätetreiber in

	welcher Reihenfolge zu laden sind. Der Kernel übergibt der Registrierung auch Informationen über sich selbst, wie z. B. die Versionsnummer.
Gerätetreiber	tauschen Ladeparameter und Konfigurationsdaten mit der Registrierung aus. Ein Gerätetreiber teilt der Registrierung mit, welche Systemressourcen, wie z. B. Hardware-Interrupts und DMA-Kanäle, er verwendet. Gerätetreiber können ebenfalls gefundene Konfigurationsdaten melden.
Setup-Programme	können der Registrierung neue Konfigurationsdaten hinzufügen. Setup-Programme lesen auch Informationen aus der Registrierung, um festzustellen, ob eine Komponente bereits installiert ist und ob eine aktuellere Version der Komponente installiert werden soll.
Hardware-Daten	Bei jedem Start von Windows NT werden Daten über die Hardware und die Konfiguration ermittelt, und die Registrierung wird aktualisiert. Auf x86-basierten Computern erfolgt die Hardware- Erkennung durch das Programm Ntdeteet.com. Auf RISC-basierten Computern werden diese Informationen aus der Firrnware des Computers extrahiert und anschließend in der Registrierung gespeichert.

10.4 Die Struktur der Registrierung

Die Registrierung setzt sich aus fünf Datenbanken zusammen, die Teilbäume genannt werden und Computerbezogene und benutzerbezogene Datenbanken enthalten. Der Zugriff zu den in der Registrierung enthaltenen Informationen erfolgt über diese Teilbäume.

Die Computer-bezogenen Datenbanken enthalten Angaben über die auf dem betreffenden Computer installierte Hard- und Software. In den benutzerbezogenen Datenbanken sind Informationen, wie z. B. Desktop-Einstellungen, individuelle Einstellungen für bestimmte Software sowie persönliche Drucker- und Netzwerkeinstellungen in Benutzerprofilen gespeichert.

Die folgende Tabelle enthält eine Beschreibung der fünf Teilbäume der Registrierung.

Teilbaum	**Beschreibung**
HKEY_LOCAL_MACHINE	**Enthält sämtliche Konfigurationsinformationen über den lokalen Computer. Diese Daten werden von Anwendungen, Gerätetreibern und dem Betriebssystem Windows NT zur Konfiguration des Computers verwendet. Ein Teil der Daten wird zum Starten von Windows NT benötigt. Die Daten in diesem Teilbaum legen fest, welche Gerätetreiber und Dienste während des Startvorgangs geladen werden sollen. Die in diesem Teilbaum enthaltenen Daten sind konstant und nicht benutzerbezogen.**
HKEY_USERS	**Enthält zwei Teilschlüssel:** DEFAULT - Enthält die Standardeinstellungen für das System (Systemstandardprofil), die bei Anzeige des Anmeldebildschirms STRG+ALT+ENTF verwendet werden. Die Sicherheits-ID (SID) des Benutzers, der momentan an dem Computer angemeldet ist.
HKEY_CURRENT_USER	Enthält Daten über den momentan interaktiv angemeldeten Benutzer. Von jedem Benutzerkonto, über das jemals eine Anmeldung an diesen Computer erfolgte, wird eine Kopie im Ordner ***systemroot\Profiles\Benutzername*** in der Datei **Ntuser.dat** abgelegt. Dieser Teilschlüssel verweist auf dieselben Daten, auf die unter **HKEY_USERS\SID_des *momentan_angemeldeten_Benutzers***

zugegriffen werden kann. Bei doppelt vorhandenen Daten hat dieser Teilschlüssel Vorrang vor HKEY_LOCAL_MACHINE.

HKEY_CLASSES_ROOT **Enthält Informationen zum Verknüpfen von Dateien sowie Daten im Zusammenhang mit COM-Objekten und verweist auf den Teilschlüssel CLASSES von HKEY_LOCAL_MACHINE\SOFTWARE.**

HKEY_CURRENT_CONFIG Enthält Informationen über das aktive Hardware-Profil. Diese Daten werden unter HKEY_LOCAL_MACHINE aus den Schlüsseln SOFRWARE und SYSTEM ermittelt.

11 Mikrocontroller und Prozessortechnik

11.1 Interrupt-Strukturen

11.1.1 Interrupts und ihre Funktionen

Als Interrupts bezeichnet man Unterbrechungsanforderungen externer oder interner Einheiten, welche die CPU veranlassen, ihre normale Befehlssequenz zu unterbrechen und eine andere Sequenz auszuführen, um nach Abarbeitung dieser wieder zum ursprünglichen Programm zurückzukehren.

In jedem MCU-System (**M**icro-**C**ontroller-**U**nit) dienen Interrupts dazu, die Leistungsfähigkeit der MCU zu erhöhen. Gilt es nun in einem System Aufgaben abzuarbeiten, die relativ selten auftreten, ist es sinnvoll, für diese das normale Hauptprogramm definiert zu unterbrechen, um den mittels Interrupt angeforderten Job ausführen zu können.

11.1.2 Detaillierter Ablauf einer Interruptverarbeitung

Unterbrechungsanforderungen an eine MCU werden von dieser dadurch registriert, dass während einer fest definierten Phase eines jeden Maschinenzyklus das zu den Interruptquellen gehörende Auffangflipflop gelesen wird (zyklisches Hardwarepolling).

Wird nun auf diese Weise eine aktive Interrupt-Quelle identifiziert, so wird der gerade in der Ausführung befindliche Befehl korrekt beendet.

1. Erst wenn der gesamte Befehlszyklus abgeschlossen ist, wird die Unterbrechungsanforderung angenommen und folgender Ablauf erzwungen: Prozessorintern wird die Rücksprungadresse gesichert, indem High und Lowbyte des Programmzählers auf den Stack (Befehlsstapel) geschrieben werden. Der Stackpointer wird nach jedem Schreibzugriff inkrementiert.
2. Sichern des Kennzeichenregisters auf dem Stack. Bei einigen CPUs findet dieser Sicherungsprozess nicht automatisch statt, sondern muss vom Anwender unter Nutzung des PUSH Befehls sichergestellt werden.
3. Nach Beendigung der prozessorinternen Stackoperationen wird der Programmzähler automatisch mit einer fest zugeordneten Interruptadresse geladen. Jedem Systeminterrupt ist eine eigene Interruptadresse zugeordnet. Die fest vorgegebene Interruptadresse zeigt auf eine Interruptabelle, in die der Anwender zuvor einen Sprungbefehl einzutragen hat, der auf den ersten Befehl der aktuellen Interrupt-Serviceroutine zeigt.
4. Der Prozessor beginnt nun mit der Befehlsabarbeitung der Unterbrechungsroutine. Das Ende der Interruptserviceroutine wird vom Prozessor durch den Befehl "Return from Interrupt" erkannt. Dieser Befehl veranlasst den Prozessor, ordnungsgemäß in das Hauptprogramm zurückzukehren.
5. Zur Rückkehr ins Hauptprogramm werden automatisch die zuvor gesicherten Stackinformationen zurückgelesen. Hierzu werden unter Dekrementierung des Stackpointers das Kennzeichenregister sowie nachfolgend Low und Highbyte der Rücksprungadresse vom Stack genommen und der Programmzähler mit der Rücksprungadresse geladen. Das Hauptprogramm kann nun, an der zuvor mittels Interrupt unterbrochenen Stelle, weiter ausgeführt werden.

Ergänzend sei hinzugefügt, dass der Anwender beim Eintritt in die Interruptserviceroutine alle Register sichern muss, deren Inhalte in der Unterbrechungsroutine verändert werden .

Warum ist dieser Sicherungsprozess notwendig?

Benutzt z. B. das Hauptprogramm den Akkumulator und steht in diesem das Ergebnis einer zuvor ausgeführten Operation, so darf dieser Akkumulatorinhalt nicht durch das Ausführen der Interruptroutine verlorengehen.

Aus diesem Grund muss der Akkumulatorinhalt beim Eintritt in die Unterbrechungsroutine per Software auf den Stack gelegt werden Diese Aufgabe übernimmt der PUSH-Befehl.

Vor Beendigung der Interruptroutine muss der Akkumulatorinhalt restauriert werden. Dieses wird durch Verwendung des POP-Befehls sichergestellt.

Bei den Befehlen PUSH und POP handelt es sich um die bekannten Stackverarbeitungsbefehle, die den Stackpointer inkrementieren bzw. dekrementieren.

11.1.3 Multiple Interrupts

Wesentlich komplizierter wird der Ablauf von Interruptanforderungen, wenn mehr als eine Interruptquelle im System zugelassen wird. Damit ein System mit multiplen Interrupts gemäß Anwendervorgaben funktioniert, müssen Regeln zur Interruptverarbeitung definiert werden. Das heißt, der Anwender muss Prioritäten zur Abarbeitungsreihenfolge der verschiedenen Interrupts vergeben.

Diesbezüglich muss sich der Anwender die Frage stellen, welche Interrupts dürfen zeitlich versetzt und welche müssen augenblicklich abgearbeitet werden.

Zur Beantwortung dieser Frage bedarf es einer präzisen Analyse des Gesamtsystems. Die sich aus den Prioritätszuweisung ergebenden neuen Interruptverzögerungszeiten sind vom Anwender auf Systemverträglichkeit zu überprüfen.

Betrachten wir z.B. ein System, in dem quasi zeitgleich verschiedene Interruptsanforderungen auflaufen, so wird ohne festgeschriebene Abarbeitungsregeln der, zeitlich gesehen, erste Interrupt angenornmen und sofort von dem folgenden Interrupt unterbrochen.

Um aber einen vorgegebenen Ablauf in der Interruptverarbeitung zu erzwingen, ist es notwendig, die Interrupts gemäß ihrer Abarbeitungswichtigkeit zu bewertendes heißt, es müssen Prioritäten vergeben werden.

Bei der Prioritätszuordnung wird auf das Prioritätsebenenmodell zurückgegriffen, das hier beispielhaft aus 3 Ebenen bestehen soll.

Höchste Priorität haben alle Interrupts der Ebene 3, zweithöchste Priorität alle Interrupts der Ebene 2 und die niedrigste Priorität weisen die Interrupts der Ebene 1 auf.

Die Zuweisung der gewünschten Interruptpriorität muss vorn Anwender softwaremäßig vorgenommen werden. Diesbezüglich stellt der Prozessor entsprechende Funktionsregister zur Verfügung, in die die gewünschten Prioritäten einzutragen sind.

Es lassen sich folgende Abarbeitungsregeln definieren:

- Interrupts, die einer höheren Ebene zugeordnet sind, können von Interrupts niedriger Ebenen nicht unterbrochen werden. Sie werden abgewiesen.
- Interrupts der gleicher Ebene werden nach einer prozessorintern festgelegten Abarbeitungsfolge angenommen. Um den zeitlichen Ablauf von Interrupts **mit** zugewiesenen Prioritäten zu verstehen, nehmen wir *Abb. 1.* 11 zur Hilfe.

Der zeitliche Ablauf von Interrupts mit zugewiesenen Prioritäten ist in Abb. 1.11 dargestellt.

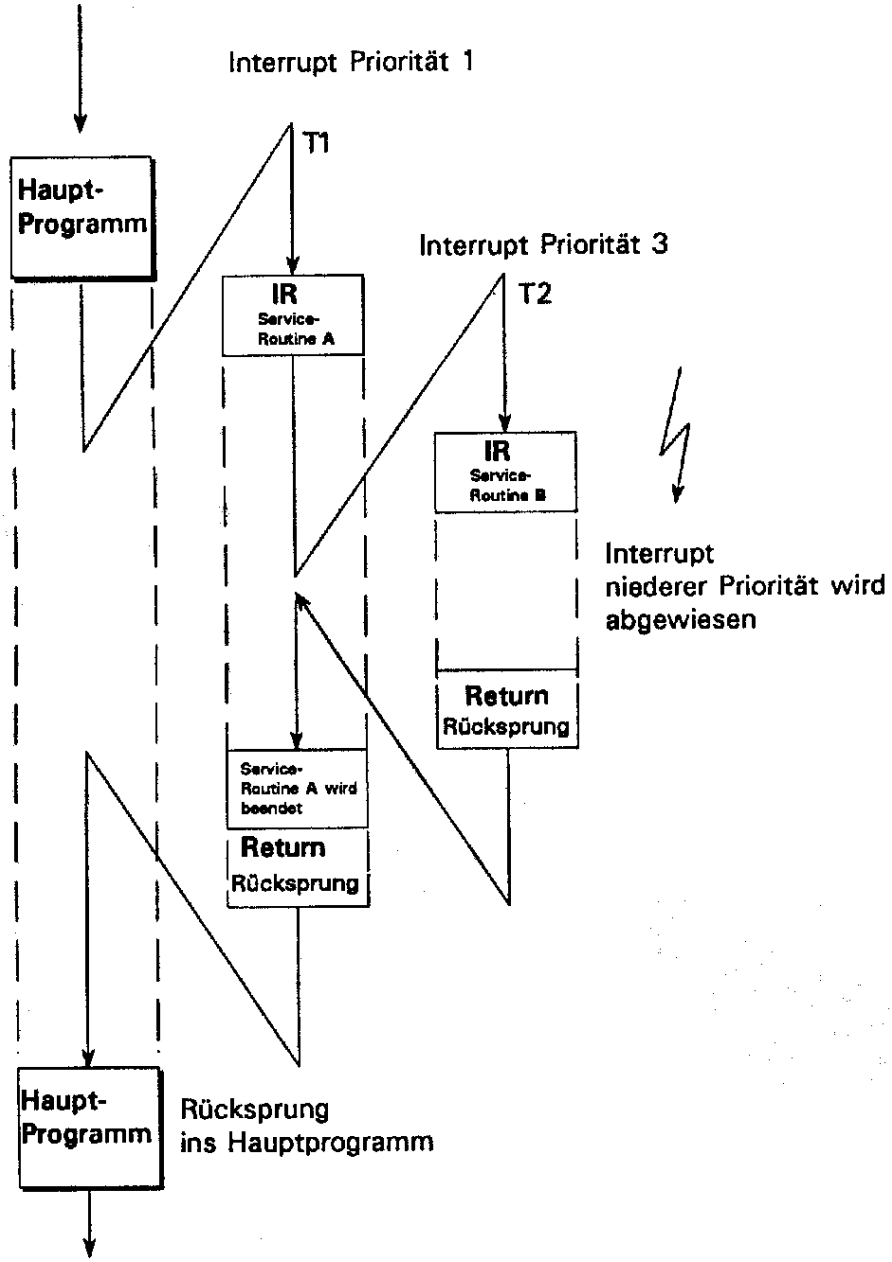


Abb. 1.11 Zeitlicher Ablauf von Interrupts mit Prioritäten

11.1.4 **Verteilung der Interrupts bei AT-kompatiblen PC's**

Die Verteilung der Portadressen und Interrupts auf die verschiedenen Schnittstellen ist eigentlich genau festgelegt (siehe Tabelle), und würde daher auch keine Probleme bereiten, wenn sich in der Praxis auch jeder Hardware-Hersteller an diese Konventionen halten würde. Das ist aber nicht der Fall. Der Grund liegt in der Aufteilung des AT-Busses.

IRQ (Interrupt Request)	Funktionen
0	Timer
1	Tastatur
2	Kaskade, evtl. frei
3	COM2, (COM4)

Portadressen	Funktion
200h-20Fh	Gameport
210h-217h	Frei
250h-277h	Frei
278h-27Fh	LPT2

IRQ (Interrupt Request)	Funktionen
4	COM1, (COM3)
5	LPT2
6	Disketten
7	LPT1
8	Uhr
9	Evtl. VGA
10	COM3, Grafikk.
11	COM4, SCSI
12	Frei
13	Coprozessor
14	Festplatte
15	Frei

Portadressen	Funktion
280h-2Efh	Frei
2F8h-2FFh	COM2
330h-35Fh	Frei
360h-36Fh	Netzwerk-karte
370h-377h	Frei
378h-37Fh	LPT1
390h-39Fh	Frei
3E0h-3Efh	Frei
3F8h-3FFh	COM1

Die den seriellen Schnittstellen C0M3 und C0M4 zugeordneten Interruptleitungen IRQ10 und IRQ11 liegen nämlich auf dem 16-Bit-Teil des Busses, also auf dem etwas kürzeren Teil des Steckplatzes. Die allermeisten Schnittstellenkarten sind aber für den Einbau in einen 8Bit-Slot geeignet, und können daher diese IRQ-Leitungen überhaupt nicht erreichen. Aus diesem Grund greifen sie einfach auf einen anderen IRQ zu, der aber unter Umständen schon einer anderen Schnittstelle zugeordnet ist. Auf dem S-Bit-Bus kann der Einbau von weiteren Schnittstellen daher hinsichtlich der verwendeten Hardware-Interrupts zu einem ziemlichen Gedränge führen.

Zur Lösung der hierbei auftretenden Probleme können im wesentlichen zwei verschiedene Wege beschnitten werden. Zum einen ist es unter bestimmten Voraussetzungen möglich, dass sich bestimmte Schnittstellen einen Interrupt teilen, zum anderen braucht auch nicht jede Schnittstelle einen Interrupt. Entscheidend ist hier in beiden Fällen die Art des angeschlossenen Geräts. Viele Geräte verwenden nämlich für ihren ordnungsgemäßen Betrieb gar keinen Interrupt, vor allem für den normalen Betrieb von parallelen Druckern kann hierauf in aller Regel problemlos verzichtet werden.

Die Maus dagegen ist auf einen IRQ angewiesen. Wenn sich die Mausschnittstelle, meistens ist dies COM1, mit einer anderen (z. B. C0M3) eine Leitung teilen muss, darf das an dieser anderen Schnittstelle angeschlossene Gerät den Interrupt nicht benutzen, sonst geht gar nichts mehr. Der Betrieb eines Modems und einer Maus auf dem gleichen IRQ ist daher nicht empfehlenswert.

In der Regel befinden sich auf den entsprechenden Schnittstellenkarten entweder einige Jumper, oder ein oder mehrere Dipschalter, über die Sie die Konfigurierung vornehmen können. Hierzu sollten Sie auf jeden Fall Ihr zur Karte gehörendes Manual zu Rate ziehen.

Wie die serielle Schnittstelle (COM1) mit Hilfe einer eigenen Interruptroutine ein- und ausgelesen werden kann, ist in dem C-Programm SIO.CPP im Anhang zu sehen.