MCSE

Kursmitschrift zum entsprechenden Kurs der

VHS Neuwied

Kurs vom 05. Februar 2002 bis 28. November 2002

Erstellt von und für

Martin Pangert

Erstellungszeitraum:
17. Februar 2002 - 30. November 2002

Copyright © 2002 by Martin Pangert, D-56242 Nordhofen

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher.
Active Directory, FrontPage, JScript, Microsoft, Microsoft Press, Outlook, Visual Basic, Visual C++, Visual J++, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.
Unless otherwise noted, the example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person, or event is intended or should be inferred.

Alle Rechte vorbehalten. Nachdruck, photomechanische oder elektronische Wiedergabe und Übersetzung - auch Auszugsweise - sind nur mit schriftlicher Genehmigung des Herausgebers und unter Quellenangabe gestattet.
Active Directory, FrontPage, JScript, Microsoft, Microsoft Press, Outlook, Visual Basic, Visual C++, Visual J++, Windows, und Windows NT sind eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation, USA und/oder anderen Ländern. Weitere Produkte oder Firmennamen sind registrierte Marken- oder Firmennamen anderer Inhaber.
Soweit nicht anders erwähnt handelt es sich bei den Unternehmen, Organisationen Produkten, Personen und Ereignissen um freie Erfindungen. Ähnlichkeiten mit lebenden, verstorbenen, existierenden oder vergangenen sind nicht beabsichtigt und rein zufällig.

Inhaltsverzeichnis

1 NETZWERK- GRUNDLAGEN 7

1.1 DAS ISO/OSI- REFERENZMODELL 7
1.2 UNTERSCHIEDE ZWISCHEN DEN ETHERNET-FRAMETYPEN 8
1.3 DIE NETZWERKPROTOKOLLE 9
1.3.1 ROUTBARE PROTOKOLLE VS. NICHT ROUTBARE PROTOKOLLE 9
1.3.1.1 Beispiele für routbare Protokollgruppen 9
1.3.1.2 Beispiele für nicht routbare Protokolle 9
1.3.2 ROUTING UND RAS 9
1.3.2.1 Allgemeines zur Routing- und RAS- Funktionalität von Windows 2000 9
1.3.2.2 Routing 9
1.3.2.3 RAS 10
1.3.3 AUTHENTIFIZIERUNG VON BENUTZERN 12
1.3.4 TCP/IP 13
1.3.4.1 IP- Protokolle 13
1.3.4.2 IP- Netzklassen und Merkmale 14
1.3.4.3 TTL – Time to Live 14
1.3.4.4 IPSec (Internet Protocol Security) 14
1.3.4.5 Perfect Forward Secrecy 14
1.3.4.6 Begriffe, Protokolle Dienstprogramme 15
1.3.4.7 TCP- Ports 18
1.3.5 IPX/SPX 19
1.3.5.1 Dienstprogramme zur Analyse von IPX/SPX 19
1.4 NETZWERKDIENSTE 20
1.4.1 DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) 20
1.4.1.1 DHCP- Entwurfsregel 20
1.4.1.2 DHCP auf Small Business Servern 20
1.4.1.3 DHCP- Server vs. DHCP-Relay Agent 20
1.4.1.4 Konfigurationsmöglichkeiten 20
1.4.1.5 DHCP- Konflikterkennung 21
1.4.1.6 Sicherung der DHCP-Datenbank 21
1.4.1.7 DHCP- Dienstprogramme 21
1.4.1.8 DHCP-Relay Agent 21
1.4.1.9 Verwendung mehrerer DHCP-Server 22
1.4.1.10 Die 4 Phasen des DHCP-Leasevorganges 22
1.4.1.11 Erneuerung der Lease 22
1.4.2 NAMENSAUFLÖSUNGEN 23
1.4.2.1 Namensauflösung über lokalen Rechnernamen 23
1.4.2.2 Namensauflösung über die Datei HOSTS 23
1.4.2.3 Namensauflösung über DNS (Domain Naming System) 24
1.4.2.4 Namensauflösung über lokalen NetBIOS Namenscache 27
1.4.2.5 Namensauflösung über WINS (Windows Internet Name Service) 27
1.4.2.6 Namensauflösung über Broadcast 29
1.4.2.7 Namensauflösung über die Datei LMHOSTS 29

2 ALLGEMEINES ZU WINDOWS 2000 30

2.1 SETUP- PROTOKOLLDATEIEN 30
2.2 DATEISYSTEM 31
2.2.1 DATEINAMENS-KONVENTIONEN 31
2.2.2 BASISLAUFWERKE VS. DYNAMISCHE DATENTRÄGER 31
2.2.3 DATEISYSTEME 31
2.2.4 DIENSTPROGRAMME 31

2.2.4.1 Das Dienstprogramm convert ... 31
2.2.4.2 delpart.com versus delpart.exe ... 32
2.2.4.3 Das Dienstprogramm cipher ... 32
2.2.5 MICROSOFT- BEGRIFFSFESTLEGUNGEN ... 32
2.2.6 DATEIBERECHTIGUNGEN UNTER NTFS ... 32
2.2.7 DISTRIBUTED FILE SYSTEM (DFS) ... 32
2.2.7.1 DFS-Clients ... 32
2.2.7.2 Eigenständiger (Standalone) DFS-Stamm ... 32
2.2.7.3 Domänen-DFS-Stamm ... 32
2.3 BENUTZERVERWALTUNG ... 33
2.3.1 KONVENTIONEN FÜR ANMELDENAMEN UND KENNWÖRTER ... 33
2.3.2 EINRICHTUNG VON ANMELDEBESCHRÄNKUNGEN ... 33
2.3.2.1 Computer, von denen sich Benutzer anmelden können ... 33
2.4 GRUPPENVERWALTUNG ... 34
2.4.1 GRUPPENTYPEN ... 34
2.4.1.1 Sicherheitsgruppen vs. Verteilergruppen ... 34
2.4.2 GRUPPENBEREICHE ... 34
2.4.3 VORDEFINIERTE SYSTEMGRUPPEN ... 34
2.5 WINDOWS 2000 STARTEN UND BEENDEN ... 35
2.5.1 WINDOWS 2000 STARTMODI ... 35
2.5.2 DIE DATEI BOOT.INI ... 35
2.5.2.1 Syntax der ARC-Pfade: ... 35
2.5.2.2 Startoptionen von Windows 2000 ... 35
2.5.3 STARTVERHALTEN VON DIENSTEN IN DER REGISTRY BEEINFLUSSEN ... 35
2.5.4 ANMELDUNG / ABMELDUNG ... 36
2.5.4.1 Anmeldevoraussetzungen ... 36
2.5.4.2 Anmeldescriptverarbeitung ... 36
2.6 INTERNET CONNECTION SHARING ... 37
2.6.1 DHCP DURCH ICS ... 37
2.6.2 DNS DURCH ICS ... 37
2.6.3 NAT DURCH ICS ... 37
2.7 DIE REGISTRY ... 38
2.7.1 TEILSTRUKTUREN ... 38
2.7.1.1 Näheres zu HKEY_LOCAL_MACHINE ... 38
2.7.2 DATENTYPEN ... 38
2.7.3 ZUGEORDNETE DATEIEN ... 38
2.7.4 UNTERSCHIEDE REGEDIT.EXE VERSUS REGEDT32.EXE ... 39
2.7.5 RECHTEVERGABE ZUR REMOTE-ADMINISTRATION DER REGISTRY ... 39
2.8 NETZWERKE UNTER WINDOWS 2000 ... 40
2.8.1 AUTENTIFIZIERUNGSPROTOKOLLE ... 40
2.8.1.1 PAP ... 40
2.8.1.2 CHAP ... 40
2.8.1.3 MS-CHAP ... 40
2.8.1.4 SPAP ... 40
2.8.1.5 PPTP ... 40
2.8.1.6 EAP ... 40
2.8.1.7 RADIUS ... 40
2.8.1.8 L2TP ... 40
2.8.1.9 BAP ... 40
2.8.1.10 BACP ... 40

3 ACTIVE DIRECTORY ... 41

3.1 INSTALLATION DER ACTIVE DIRECTORY- DIENSTE ... 41
3.2 DIE ACTIVE DIRECTORY- DATENBANK ... 42
3.3 BETRIEBSMASTER VON WINDOWS 2000 ... 43
3.3.1 SCHEMAMASTER ... 43
3.3.1.1 Bearbeiten des Schemas ... 43
3.3.2 DOMÄNENNAMENMASTER ... 43

3.3.3 INFRASTRUKTURMASTER....43
3.3.4 RID-MASTER (RELATIVER ID- MASTER)....43
3.3.5 PDC- EMULATOR....43
3.3.6 EMPFEHLUNGEN ZUR VERTEILUNG DER 5 BETRIEBSMASTERROLLEN....43
3.3.7 ZUORDNUNG DER BETRIEBSMASTERROLLEN....43
3.3.8 AUSFÄLLE DER BETRIEBSMASTER....44
3.3.9 GLOBALER KATALOGSERVER....44
3.4 VERÖFFENTLICHUNG VON RESOURCEN INNERHALB EINER AD-DOMÄNE....45
3.5 OBJEKTVERWALTUNG....46
3.5.1 DIENSTPROGRAMME ZUR ACTIVE DIRECTORY OBJEKTVERWALTUNG....46
3.5.1.1 MMC-Snapin „Active Directory Benutzer und Computer“....46
3.5.1.2 MMC-Snapin „Active Directory Standorte und Dienste“....46
3.5.1.3 MOVETREE.EXE....46
3.5.1.4 NETDOM.EXE....46
3.5.1.5 REPLMON.EXE....46
3.6 DATENSICHERUNG / WIEDERHERSTELLUNG DER ACTIVE DIRECTORY DATEN....47
3.6.1 SICHERUNG....47
3.6.2 WIEDERHERSTELLUNG....47
3.6.2.1 Nicht- Autorisierende Wiederherstellung....47
3.6.2.2 Autorisierende Wiederherstellung....48
3.7 KOMPRIMIERUNG DER ACTIVE DIRECTORY DATENBANK....49
3.8 TYPISCHE AD- FEHLER....50
3.9 ACTIVE-DIRECTORY- DIENSTPROGRAMME....51
3.9.1 NTDSUTIL....51
3.9.2 CSVDE....51
3.9.3 LDIFDE....51
3.10 AD- DESIGN....52
3.10.1 PLANUNG DER GESAMTSTRUKTUR....52
3.10.2 PLANUNG DER DOMÄNEN....53
3.10.3 PLANUNG DER ORGANISATIONSEINHEITEN....53
3.10.4 PLANUNG DER STANDORTTOPOLOGIE....54
3.10.5 DNS- DESIGN....55

4 RIS (REMOTE INSTALLATION SERVICE)....56

4.1 NETZWERKANFORDERUNGEN FÜR RIS....56
4.2 RIS- SERVERANFORDERUNGEN....56
4.3 SERVERKOMPONENTEN DEN RIS- DIENSTES....56
4.3.1 BINL (BOOT INFORMATION NEGOTATION LAYER)....56
4.3.2 TFTPD (TRIVIAL FILE TRANSFER PROTOCOL DAEMON)....56
4.3.3 SIS (SINGLE INSTANCE STORE)....56
4.4 RIS- CLIENT- ANFORDERUNGEN....56
4.5 ANFORDERUNG AN DEN RIS- USER....56
4.6 ABLAUF EINER RIS- INSTALLATION....57
4.7 RBFG- BOOTDISKETTE FÜR RIS (UNTERSTÜTZTE NETZWERKKARTEN)....57

5 GRUPPENRICHTLINIEN....58

5.1 ALLGEMEINES....58
5.1.1 LOKALES GRUPPENRICHTLINIENOBJEKT....58
5.1.2 STANDORT- GRUPPENRICHTLINIENOBJEKTE....58
5.1.3 DOMÄNEN- GRUPPENRICHTLINIENOBJEKTE....58
5.1.4 ORGANISATIONSEINHEITEN- GRUPPENRICHTLINIENOBJEKTE....58
5.2 GPO-VERARBEITUNGSREIHENFOLGE INNERHALB DER OBJEKTHIRARCHIE....59
5.3 GPO-VERERBUNGSLEHRE INNERHALB DER DOMÄNENHIRARCHIE....59
5.4 BEISPIELHAFTE GRUPPENRICHTLINIE MIT NUR 6 EINSTELLUNGEN....60
5.5 BEEINFLUSSUNG DER GRUPPENRICHTLINIENVERERBUNG....61
5.5.1 KEIN VORRANG....61

5.5.2 RICHLINIENVERERBUNG 62
5.5.3 LOOPBACKVERARBEITUNG VON GRUPPENRICHTLINIENOBJEKTEN 62
5.5.3.1 Beispiele für die Loopbackverarbeitung 62
5.5.4 DEAKTIVIEREN VON TEILEN VON GRUPPENRICHTLINIEN 62
5.5.5 EINSCHRÄNKEN DER VERARBEITUNG EINER GRUPPENRICHTLINIE 62
5.5.6 SOFTWAREVERTEILUNG ÜBER GRUPPENRICHTLINIEN 63
5.5.6.1 *.MSI (Windows Installer) 63
5.5.6.2 *.ZAP (Zero Administration Pack, Installations- Anwendungen) 63
5.5.6.3 *.MST (Windows- Installer Veränderungspakete) 63
5.5.6.4 *.MSP (Patchdateien) 63
5.5.6.5 *.AAS (Application Assignment Scripts) 63
5.5.7 ZUWEISEN VON SOFTWARE 63
5.5.8 VERÖFFENTLICHEN VON ANWENDUNGEN 63

6 NÜTZLICHE TIPS UND TRICKS 64

6.1 DER EXTERNE BEFEHL AT.EXE 64
6.2 DAS PROGRAMM RUNAS.EXE 65

7 INDEX 66

8 ANHANG 70

8.1 HILFEN ZUM ISO/OSI REFERENZMODELL 71

1 Netzwerk- Grundlagen

1.1 Das ISO/OSI- Referenzmodell

Siehe „Hilfen zum ISO/OSI Referenzmodell“ (Kapitel 8.1 / Seite 71)

1.2 Unterschiede zwischen den Ethernet-Frametypen

Ethernet II	=>	Unix-IP
Ethernet 802.3	=>	"Raw"; mit "Service-Access-Point" –Feld
Ethernet 802.2	=>	mit "Start of Frame Delimiter"
Ethernet SNAP	=>	***S***ub ***N***etwork ***A***ccess ***P***rotokoll (AppleTalk/IP)

1.3 Die Netzwerkprotokolle

Man unterscheidet die unterschiedlichen Netzwerkprotokolle unter anderem nach ihrer Routbarkeit.

1.3.1 Routbare Protokolle vs. nicht routbare Protokolle

1.3.1.1 Beispiele für routbare Protokollgruppen

- TCP/IP (Transmission Control Protocol / Internet Protocol)
- IPX/SPX (Internetworking Packet Exchange / Sequenced Packet Exchange)
- ATM (Asynchronous Transfer Mode) / Frame Relay
- AppleTalk

1.3.1.2 Beispiele für nicht routbare Protokolle

- NetBEUI (NetBIOS Enhanced User Interface)
- DLC (Data Link Control; findet u.a. bei HP-Druckern Verwendung)
- IrDA (Infrared Data Association)

1.3.2 Routing und RAS

1.3.2.1 Allgemeines zur Routing- und RAS- Funktionalität von Windows 2000

- Routing und RAS ist ein marginaler Bestandteil des Betriebssystemes Windows 2000 (Server/Professional) und kann nicht deinstalliert werden. Die entsprechenden Dienste können nur aktiviert oder deaktiviert werden.
- Windows 2000 unterstützt Multiprotokoll- Routing – ein Router kann sowohl IP als auch IPX und AppleTalk gleichzeitig Routen. Das Routing für die unterschiedlichen Protokolle wird unter einer gemeinsamen Oberfläche konfiguriert.
- Das Dienstprogramm NETSH.EXE ist eines der wichtigsten, Kommandozeilenorientierten Programme im Bereich Routing und RAS

1.3.2.2 Routing

1.3.2.2.1 Wählen bei Bedarf

Ein Windows 2000 Router kann keine Bedarfs- Wählverbindungen aufbauen, wenn zur gleichen Zeit für die gleiche Schnittstelle der Faxdienst konfiguriert und aktiviert ist. Im Bedarfsfall muss der Faxdienst zeitgesteuert beendet werden.

1.3.2.3 RAS

1.3.2.3.1 RAS- Richtlinien

RAS- Richtlinien steuern neben den Benutzerabhängigen Attributen die eigentliche RAS- Berechtigung.

Hinweise:

Ohne definierte RAS- Richtlinien ist unter Windows 2000 kein RAS- Zugriff möglich !

Nur **in den RAS- Richtlinien ist eine Konfiguration von Zugriffsüberwachungen möglich!**

1.3.2.3.2 RAS in den Benutzerkonten

In den Benutzerkonten sind generelle Festlegungen zu RAS möglich. Dies sind zum Beispiel

- Zugriffsgestattung des Benutzers
- Rückrufoptionen
- Statische IP-Verwendung
- Statische Routen für den RAS- Client

1.3.2.3.3 RAS- Autentifizierung

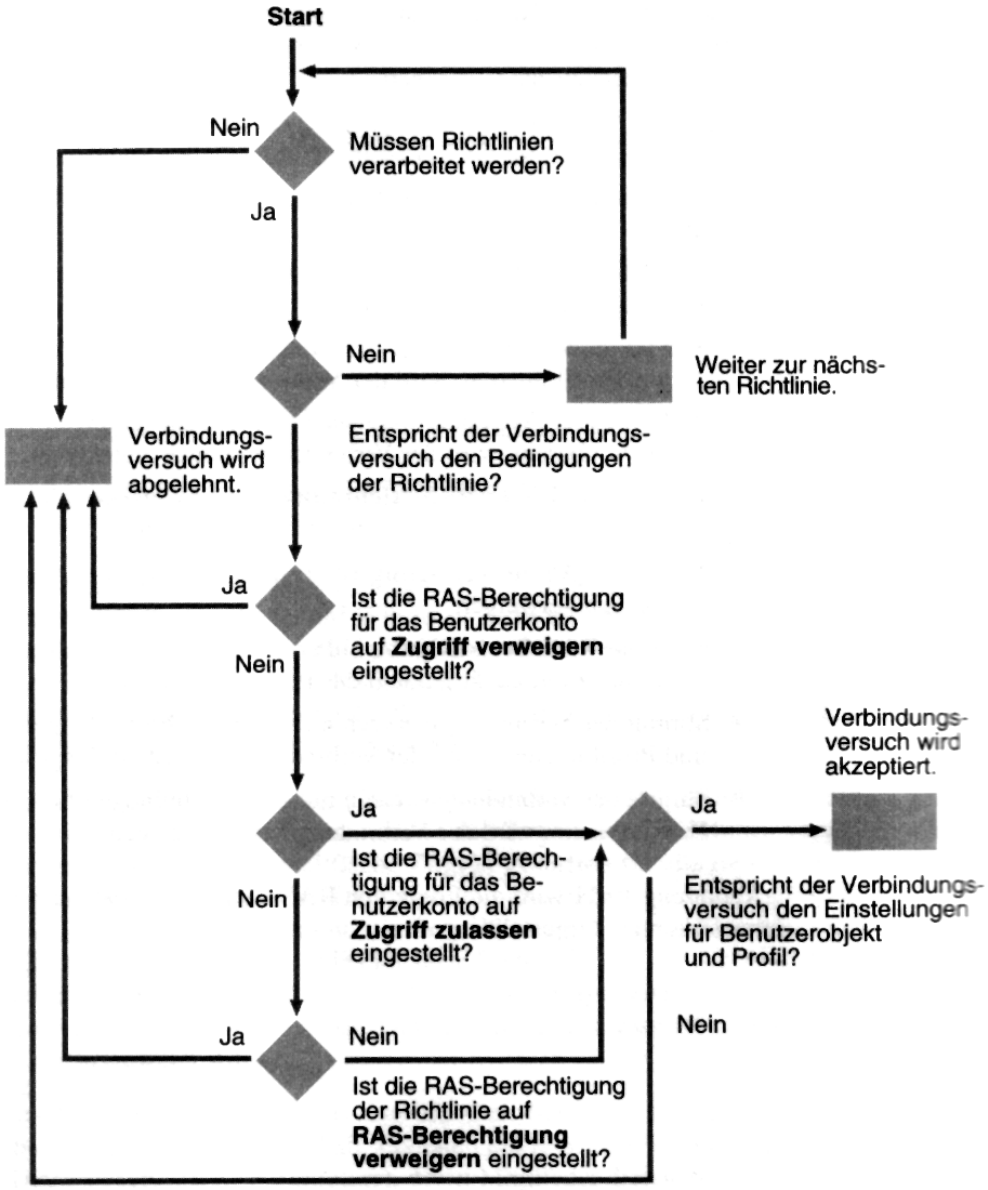
Für RAS sind mehrere Autentifizierungsverfahren möglich

- EAP (Extensible Autentication Protocol)
  => als MD5-Challenge oder Smartcard oder anderes Zertifikat
- MS-CHAP v2 (Microsoft-Verschlüsseltes Challenge Handshake Authentication Protocol Version 2
  => stärkste Verschlüsselungsstufe
- MS-CHAP (Microsoft-Verschlüsseltes Challenge Handshake Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)
- SPAP (Shiva Password Autentication Protocol)
- PAP (Password Autentication Protocol)

1.3.2.3.3.1 RAS-Richtlinienbearbeitung beim Verbindungsversuch

RAS- Richtlinien sind nach folgender Reihenfolge zu Organisieren:

1. Verweigerungen
2. Zulassungen


Start
Nein
Müssen Richtlinien verarbeitet werden?
Ja
Nein
Weiter zur nächsten Richtlinie.
Verbindungsversuch wird abgelehnt.
Entspricht der Verbindungsversuch den Bedingungen der Richtlinie?
Ja
Ist die RAS-Berechtigung für das Benutzerkonto auf **Zugriff verweigern** eingestellt?
Nein
Verbindungsversuch wird akzeptiert.
Ja
Ja
Ist die RAS-Berechtigung für das Benutzerkonto auf **Zugriff zulassen** eingestellt?
Entspricht der Verbindungsversuch den Einstellungen für Benutzerobjekt und Profil?
Nein
Nein
Ja
Nein
Ist die RAS-Berechtigung der Richtlinie auf **RAS-Berechtigung verweigern** eingestellt?

1.3.3 Authentifizierung von Benutzern

Für die Authentifizierung wurde der IAS (Internet Autentication Service) unter Windows 2000 implementiert. Dieser bietet unter anderem die Microsoft- Unterstützung von Kerberos, dem Sicherheitsprotokoll für Authentifizierungstickets.

Kerberos kann nur innerhalb einer Active Directory Domäne verwendet werden – NT4 muss also für die Verwendung einer Kerberos- Authentifizierung zu Windows 2000 migriert werden.

1.3.4 TCP/IP

1.3.4.1 IP- Protokolle

1.3.4.1.1 EGP
Exterior Gateway Protocol

1.3.4.1.2 HMP
Host Monitoring Protocol

1.3.4.1.3 ICMP
Internet Control Message Protocol

1.3.4.1.4 RDP
Reliable Datagram Protocol

1.3.4.1.5 RVD
Remote Virtual Disk

1.3.4.1.6 TCP
Transmission Control Protocol

1.3.4.1.7 UDP
User Datagram Protocol

1.3.4.1.8 XNS-IDP
Xerox NS IDP

1.3.4.2 IP- Netzklassen und Merkmale

Ursprünglich wurden zur Vereinfachung Netzwerkklassen im IP- Bereicht eingeführt, an die sich auf Grund der stetigen Entwicklung heute keiner mehr so genau hält. Dennoch sollte man die Klassen kennen und nach Möglichkeit einhalten.

Microsoft geht in Prüfungen davon aus, dass die Netzwerkmaske gemäß der Adressklasse angenommen wird, sofern nichts anderes angemerkt ist.

Klasse	*Bitmaske der Adresse*	*IP- Range der Netzklasse*	*Reservierte Adressen innerhalb der Netzklasse*		
A	0xxxxxxx	0 … 127	Privatbereich Loopback	10.x.x.x 127.x.x.x	
B	10xxxxxx	128 … 191	Privatbereich APIPA	172.16.x.x - 172.31.x.x 169.254.x.x	APIPA = ***A***utomatic ***P***rivate ***IP*** ***A***ddressing
C	110xxxxx	192 … 223	Privatbereich	192.168.x.x	
D	1110xxxx	224 … 239	***In Windows 2000 nicht verwendbar (wird vom System abgelehnt !)***		Für Broadcasting reserviert (z.B. Streaming Media)
E	1111xxxx	240 … 254	***In Windows 2000 nicht verwendbar (wird vom System abgelehnt !)***		Nur für Testzwecke zulässig !

1.3.4.3 TTL – Time to Live

Für jede IP-Verbindung wird eine TTL- Zeit festgelegt. Eine TTL von 128 (= Standardwert) bedeutet, dass ein Datagramm maximal 128 Sekunden in der Übertragungsphase verbringen darf und nach Ablauf dieser Zeit verworfen wird. Zusätzlich wird durch jeden Router, durch den das Datagramm geleitet wird, der TTL- Wert um 1 verringert.

1.3.4.4 IPSec (Internet Protocol Security)

IPSec wird über das MMC- Snapin „IP-Sicherheitsrichtlinienverwaltung“ konfiguriert.
Es können innerhalb der IP-Security folgende Kriterien definiert werden:

- zwischen welchen Adressen bzw. Subnetzen Sicherheit ausgehandelt werden soll
- für welche Art von IP-Verkehr Sicherheit ausgehandelt werden soll
- welche Sicherheitsmaßnahmen angewandt werden sollen (z.B. Sichere Kommunikation anfordern, unsichere aber erlauben u.s.w.)
- welche Autentifizierungsverfahren angewandt werden (Kerberos, Zertifikat oder Passwort)
- ob die Kommunikation über einen IP-Tunnel läuft (bei IP-Tunneln sind zwei Richtlinien erforderlich)
- auf welche Art Netzwerkverbindungen die Richtlinie angewandt werden soll (LAN, RAS oder beides)

IP-Security kann über das Dienstprogramm IPSECMON überwacht werden.

Falls eine IP-Sicherheitsrichtlinie von zwei Stellen (= zwei Administratoren an unterschiedlichen Rechnern) aus bearbeitet wird, kann es zu Überschneidungen kommen, die eine sichere Funktion verhindern können. Daher ist eine Richtlinien- Integritätsprüfung empfehlenswert, nachdem Änderungen an IPSec- Richtlinien durchgeführt wurden.

Ferner können im Kontextmenü der IP-Sicherheitsrichtlinien in der MMC die Administratoraufgaben „Standardrichtlinien wieder herstellen“, „Richtlinien importieren“ und „Richtlinien exportieren“ aufgerufen werden.

1.3.4.5 Perfect Forward Secrecy

Durch diese Funktion werden bei jeder Sitzung neue Sitzungsschlüssel ausgehandelt. Somit ist ein „alter Schlüssel“ vollkommen wertlos.

1.3.4.6 Begriffe, Protokolle Dienstprogramme

1.3.4.6.1 ARP

Address Resolution Protocol

1.3.4.6.1.1 Das Dienstprogramm ARP

Arp dient zur Anzeige oder Änderung der Übersetzungstabellen, die von ARP (Address Resolution Protocol) für die Umsetzung von IP-Adressen in physische Ethernet- oder Tokenringadressen verwendet werden. Dieser Befehl ist nur verfügbar, wenn das Protokoll TCP/IP installiert wurde.

1.3.4.6.2 CIDR

Classless Inter Domain Routing
Die neuere Schreibweise von IP-Adressen mit dazugehöriger Netzwerkmaske. Statt die Maske direkt anzugeben, wird nur noch angegeben, wie viele Bits der Netzwerkmaske auf 1 Gesetzt sind.
Beispiel (jeweils Adresse / Maske):

Klassische Schreibweise:	062.153.167.130	255.255.255.240
Bitweise Darstellung	00111110.10011001.10100111.100000010	11111111.11111111.11111111.11110000
CIDR- Angabe	062.153.168.130	20
Novell kennt auch noch ...	062.153.167.130	FF.FF.FF.F0

1.3.4.6.3 Ping

Überprüft die Netzwerkverbindung zu einem oder mehreren Remotehosts. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.4 HTTP

Hypertext Transmission Protocol

1.3.4.6.5 FTP

File Transfer Protocol

1.3.4.6.5.1 Das Dienstprogramm Ftp

Ftp überträgt Dateien zu und von einem Computer, der den FTP-Serverdienst (auch als Daemon bezeichnet) ausführt. **Ftp** kann interaktiv ausgeführt werden. Klicken Sie in der Liste **Siehe auch** auf **ftp-Befehle**, um eine Beschreibung der verfügbaren **ftp**-Unterbefehle anzuzeigen. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde. **Ftp** ist ein Dienst, der beim Starten eine Unterumgebung erstellt, in der Sie **ftp**-Befehle verwenden und zur Windows 2000-Eingabeaufforderung zurückkehren können, indem Sie den Unterbefehl **quit** eingeben. Wenn die **ftp**-Unterumgebung ausgeführt wird, ist dies an der **ftp**-Eingabeaufforderung erkennbar.

1.3.4.6.6 tFtp

Trivial File Transfer Protocol

1.3.4.6.6.1 Das Dienstprogramm tFtp

Überträgt Dateien zu und von einem Remotehost, der den TFTP-Dienst (Trivial File Transfer Protocol) ausführt. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.7 NNTP

Network News Transfer Protocol

1.3.4.6.8 SMTP

Simple Mail Transfer Protocol

1.3.4.6.9 POP
Post Office Protocol

1.3.4.6.10 NFS
Network File System

1.3.4.6.11 OSPF
Open Shortest Path First

1.3.4.6.12 RIP
Router Information Protocol

1.3.4.6.13 SNMP
Simple Network Management Protocol

1.3.4.6.14 TCP
Transmission Control Protocol

1.3.4.6.15 UDP
User Datagram Protocol

1.3.4.6.16 IGMP
Internet Group Management Protocol

1.3.4.6.17 ICMP
Internet Control Message Protocol

1.3.4.6.18 LCP – Link Control Protocol
Link Control Protocol
Das Link Control Protocol dient unter anderem zur Überwachung einer IP-Verbindung oder zum Aushandeln eines RAS-Rückrufes. Es handelt sich beim LCP-Protokoll um eine Erweiterung des PPP-Protokolles.

1.3.4.6.19 IP
Internet Protocol

1.3.4.6.20 NBT
Netbios over TCP/IP

1.3.4.6.21 Ipconfig

Dieser Diagnosebefehl zeigt alle aktuellen TCP/IP-Netzwerkkonfigurationswerte an. Dieser Befehl ist insbesondere auf Systemen nützlich, die DHCP ausführen. Mit ihm können die Benutzer ermitteln, welche TCP/IP-Konfigurationswerte von DHCP konfiguriert wurden.

1.3.4.6.21.1 Wichtige Parameter

all
Erstellt eine vollständige Anzeige. Ohne diesen Schalter zeigt **ipconfig** nur die IP-Adresse, die Subnetzmaske und den Standardgateway für jeden Netzwerkadapter an.

/renew [Adapter]
Aktualisiert die DHCP-Konfigurationsparameter. Dieser Parameter ist nur auf Systemen verfügbar, auf denen der DHCP-Clientdienst ausgeführt wird. Geben Sie als Netzwerkadapternamen den Namen ein, der angezeigt wird, wenn Sie **ipconfig** ohne Parameter verwenden.

/release [Adapter]
Gibt die aktuelle DHCP-Konfiguration frei. Dieser Parameter deaktiviert TCP/IP auf dem lokalen System und ist nur auf DHCP-Clients verfügbar. Geben Sie als Netzwerkadapternamen den Namen ein, der angezeigt wird, wenn Sie **ipconfig** ohne Parameter verwenden.
Ohne Angabe von Parametern zeigt das Dienstprogramm **ipconfig** alle aktuellen TCP/IP-Konfigurationswerte an, einschließlich IP-Adresse und Subnetzmaske. Dieser Befehl ist insbesondere auf Systemen nützlich, die DHCP ausführen. Mit ihm können die Benutzer ermitteln, welche Werte von DHCP konfiguriert wurden.

1.3.4.6.22 Nbtstat

Zeigt die Protokollstatistik und die aktuellen TCP/IP-Verbindungen an, die NBT (NetBIOS über TCP/IP) verwendet. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.23 Netstat

Zeigt Protokollstatistiken und aktuelle TCP/IP-Netzwerkverbindungen an. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.24 Route

Route ermöglicht die Bearbeitung von Netzwerkroutingtabellen. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.24.1 Wichtige Parameter

-f
Löscht alle Gatewayeinträge in den Routingtabellen. Wird dieser Parameter mit einem Befehl verwendet, werden die Tabellen vor der Befehlsausführung gelöscht.

-p
Wird dieser Parameter mit dem Befehl **add** verwendet, bleibt die Route nach dem Neustart des Systems erhalten. Standardmäßig werden zuvor existierende Routen beim Neustart des Systems entfernt. Wird dieser Parameter mit dem Befehl **print** verwendet, wird eine Liste aller registrierten gespeicherten Routen angezeigt. Dieser Parameter wird überlesen, wenn er mit anderen Befehlen verwendet wird, die sich immer auf die entsprechenden beständigen Routen auswirken.

Befehl	**Zweck**
Print	Zeigt eine Route an
Add	Fügt eine Route hinzu
Delete	Löscht eine Route
Change	Ändert eine bestehende Route

1.3.4.6.25 Hostname

Zeigt den Namen des aktuellen Hosts an. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.26 Rcp

Kopiert Dateien zwischen einem Windows 2000-Computer und einem System, das **rshd,** den Remote Shell Daemon, ausführt. Dieser Connectivity-Befehl kann auch zum Kopieren von Dateien zwischen zwei Computern, die **rshd** ausführen, verwendet werden, wenn der Befehl von einem Windows 2000-Computer abgesetzt wird. Der **rshd**-Daemon ist auf UNIX-Computern verfügbar, nicht jedoch unter Windows 2000. Daher kann der Windows 2000-Computer nur als das System teilnehmen, von dem die Befehle abgesetzt werden. Der Remotecomputer muss zusätzlich durch Ausführen von **rshd** das Dienstprogramm **rcp** bereitstellen.

1.3.4.6.27 Rsh

Führt einen Befehl auf Remotehosts aus, auf denen der RSH-Dienst aktiviert ist. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.28 Rexec („Remote Execution")

Führt Befehle auf Remotehosts aus, auf denen der REXEC-Dienst aktiv ist. Der Befehl **rexec** authentifiziert den Benutzernamen auf dem Remotecomputer, bevor der angegebene Befehl ausgeführt wird, und ist nur verfügbar, wenn das Protokoll TCP/IP installiert wurde.

1.3.4.6.29 Finger

Dieser Befehl zeigt Informationen über einen Benutzer eines angegebenen Systems an, das den Finger-Dienst ausführt. Die Ausgabe hängt von dem jeweiligen Remotesystem ab. Dieser Befehl ist nur verfügbar, wenn das TCP/IP-Protokoll installiert wurde.

1.3.4.6.30 PathPing

Ein Tool zum Verfolgen von Routen, das neben Features der Befehle **ping** und **tracert** weitere Informationen bietet, die durch diese Befehle nicht zur Verfügung gestellt werden. Der Befehl **pathping** sendet über einen gewissen Zeitraum Datenpakete an jeden Router auf dem Pfad zu einem Ziel. Anhand der von jedem Abschnitt zurückübermittelten Datenpakete werden dann bestimmte Statistiken berechnet. Da der Befehl **pathping** den Paketverlust bei jedem Router und jeder Verbindung anzeigt, können Sie feststellen, welche Router oder Verbindungen Netzwerkprobleme verursachen.

1.3.4.7 TCP- Ports

Wichtiger TCP-Ports (zu merkende) und deren dazugehörigen Dienste sind:

21	FTP (File Transfer Protocol)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Naming System)
69	TFTP (Trivial File Transfer Protocol)
80	HTTP (Hypertext Transmission Protocol)
110	POP (Post Office Protocol
443	HTTPS (Hyper Text Transmission Protocol secured)
137 – 139	NetBIOS

1.3.5 IPX/SPX

1.3.5.1 Dienstprogramme zur Analyse von IPX/SPX

1.3.5.1.1 Ipxroute

Zeigt Informationen über die Routingtabellen des IPX-Protokolls an oder ändert sie. Dieser Befehl bietet verschiedene Optionen für IPX-Routing und für Quellrouting. Alle Optionen müssen mit Leerzeichen voneinander getrennt werden.

1.4 Netzwerkdienste

1.4.1 DHCP (Dynamic Host Configuration Protocol)

DHCP – das Dynamic Host Configuration Protocol – weist Rechnern eine eindeutige IP zu. Für den Fall, dass ein als DHCP-Client konfigurierter Rechner keinen DHCP-Server findet, hat Microsoft bei der ICANN einen Adressbereich (169.254.000.000 bis 169.254.255.255) angekauft, der über die Funktion „APIPA" (Automatic Private IP Adressing) dem Rechner zugewiesen wird. APIPA wird von den Betriebssystemem Windows 98SE, Windows ME, Windows 2000 und Windows XP verwendet / unterstützt

DHCP ist eine Erweiterung des Bootstrap Protocol (BOOTP), das auf UDP/IP basiert.
BOOTP ermöglicht die automatische dynamische Konfiguration eines Hosts bei dessen Start.

1.4.1.1 DHCP- Entwurfsregel

Microsoft empfiehlt bei der Bereichseinteilung von Adressbereichen die 75%/25%- Entwurfsregel.
75% aller Adressen sollen durch den ersten DHCP-Server, 25% durch einen weiteren verwaltet werden. Somit ist sichergestellt, dass bei Ausfall des ersten DHCP-Servers zumindest noch 25% aller Adressen vergeben werden können.

1.4.1.2 DHCP auf Small Business Servern

Findet ein DHCP-Dienst auf einem Small Business Server einen weiteren DHCP-Server im Netzwerk, so wird der DHCP-Serverdienst auf dem Small Business Server automatisch beendet – es sind also keine weiteren DHCP-Servern in Small Business Server Netzwerken zulässig

1.4.1.3 DHCP- Server vs. DHCP-Relay Agent

Auf einem Server können nicht gleichzeitig der DHCP-Server und der DHCP- Relay Agent ausgeführt werden, da beide Dienste auf den selben Ports arbeiten (UDP- Port 67 und UDP- Port 68)

1.4.1.4 Konfigurationsmöglichkeiten

1.4.1.4.1 DHCP- Berechtigungen

Für die Verwaltung des DHCP-Servers wurden zwei Sicherheitsgruppen eingeführt. Es handelt sich dabei um die lokalen Gruppen „DHCP-Benutzer" und „DHCP-Administratoren". Erstere dürfen die DHCP-Konfiguration und den entsprechenden Status nur lesend einsehen – letztere Administrativ verändern.

1.4.1.4.2 DNS-Aktualisierungen

Der DHCP-Server kann den für ihn selbst eingerichteten DNS-Server bei Vergabe einer Adresse an einen Client entsprechend aktualisieren. Ferner kann er diese Aktualisierungsfunktion für Clients übernehmen, die das dynamische aktualisieren beim DNS-Server nicht unterstützen.
Konfiguration: Über die Eigenschaften des DHCP-Servers in der entsprechenden MMC-Konsole

1.4.1.4.3 DHCP- Optionen

DHCP- Optionen können sowohl direkt für den ***gesamten DHCP- Server***, einen ***IP-Bereich*** als auch direkt für eine ***Reservierung*** konfiguriert werden.

Beispiele für DHCP- Optionen:

Optionsnummer	*Optionsname*	*Beschreibung*
003	Router	Mehrere Routeradressen (IP-Adressen)
006	DNS-Server	Mehrere DNS-Server (IP-Adressen)
012	Hostname	Clientbezeichner
015	DNS-Domänenname	DNS-Name der Domäne für die Auflösung des Hostnamens
028	Broadcastadresse	Eine einzelne IP-Adresse, die für Broadcasts verwendet werden soll
044	WINS/NBNS-Server	Mehrere WINS- Serveradressen (IP- Adressen)
046	WINS/NBT-Knotentyp	Knotentyp (siehe Kap. 1.4.2.7.1) Typen: 1 = B-Knoten (Broadcast) 2 = P-Knoten (Peer) 4 = M-Knoten (Gemischt) 8 = H-Knoten (Hybrid)

1.4.1.5 DHCP- Konflikterkennung

Wir die DHCP- Konflikterkennung aktiviert, sendet der DHCP-Server vor Vergabe eines Lease- Angebotes (DHCPOFFER) einen Ping an die entsprechende Adresse, um sicherzustellen, dass diese nicht bereits im Netzwerk aktiv ist.

1.4.1.6 Sicherung der DHCP-Datenbank

Windows 2000 sichert die DHCP-Datenbank standardmäßig alle 60 Minuten in den Ordner %systemroot%\system32\dhcp\Backup\Jet\new. Wird der DHCP-Dienst angehalten, so können die dort vorhandenen Dateien auch manuell nach %systemroot%\system32\dhcp zurückkopiert werden.
Der Sicherungsintervall lässt sich in der Registrierung unter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\BackupInterval= xxx verändern
Eine automatisierte Rücksicherung lässt sich mit dem Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\RestoreFlag=1 erreichen.

1.4.1.7 DHCP- Dienstprogramme

1.4.1.7.1 JetPack

Mittels des Dienstprogrammes JETPACK.EXE kann unter anderem die DHCP- Datenbank offline gepackt werden (JETPACK ist auch für die WINS-Datenbank geeignet!).
Beispielscript:

```
CD %SYSTEMROOT%\SYSTEM32\DHCP
NET STOP DHCPServer
JETPACK DHCP.MDB TEMP.MDB
NET START DHCPServer
```

Hinweis: Auch wenn die Dateierweiterung ein MS-Access- Format vermuten lässt – die Datei lässt sich zumindest mit Access 2000 nicht lesen ...

1.4.1.8 DHCP-Relay Agent

Windows 2000 kann bei aktiviertem Routing als RFC 1542- konformer DHCP-Relay- Agent fungieren.
Diese Funktion wird über Routing und RAS konfiguriert.

1.4.1.9 Verwendung mehrerer DHCP-Server

Da DHCP-Server keinerlei Informationen über die auf ihnen Konfigurierten IP-Adressbereiche austauschen, muß sichergestellt sein, dass die entsprechenden IP-Bereiche sich nicht überlappen.

1.4.1.10 Die 4 Phasen des DHCP-Leasevorganges

1.4.1.10.1 DHCPDISCOVER (Anfrage)

Der Client sendet mit der IP-Adresse 0.0.0.0 (Mask: 255.255.255.255) eine DHCPDISCOVER- Broadcastmeldung mit seiner MAC-Adresse und seinem Rechnernamen

1.4.1.10.2 DHCPOFFER (Angebot)

Alle DHCP-Server, die eine DHCPDISCOVER-Anfrage erhalten haben senden per Broadcast ein Angebot mit der MAC-Adresse des Clients, einer angebotenen IP-Adresse, einer Subnetmaske, einer Leasedauer und der Bezeichnung des anbietenden Servers (IP-Adresse).

1.4.1.10.3 DHCPREQUEST (Lease-Anforderung)

Der Client sendet per Broadcast eine IP-Anforderung an alle DHCP-Server, mit der er die Annahme des Angebotes mitteilt, welches ihn als erstes erreicht hat.
Ferner wird im DHCPREQUEST-Paket dem DHCP-Server mitgeteilt, ob und in welcher Form dieser die DNS-Aktualisierungen für den Client durchführen soll.Hierzu wurden im DHCPREQUEST-Packet folgende Flags eingeführt:

- Flag 0 Der Client möchte den A-Ressourceneintrag registrieren und fordert, dass der Server den PTR-Ressourceneintrag aktualisiert.
- Flag 1 Der Client möchte, dass der Server beide Einträge durchführt.
- Flag 3 Der DHCP-Server registriert beide Einträge unabhängig von der Anforderung des Clients.

1.4.1.10.4 DHCPACK/DHCPNACK (Lease-Bestätigung/Ablehnug)

1.4.1.10.4.1 DHCPACK (Bestätigung – acknoledgement)

Der anbietende Server bestätigt die Vergabe der IP-Adresse und der Client initialisiert sein TCP/IP unter Verwendung der vorher ausgehandelten Daten vollständig.

1.4.1.10.4.2 DHCPNACK (Ablehnung – negative acknoledgement)

Der anbietende Server lehnt letztendlich die Verwendung der zuvor angebotenen IP- Adresse ab – der Client startet den Leasevorgang neu.

1.4.1.11 Erneuerung der Lease

Alle DHCP-Clients versuchen nach der hälfte der Leasedauer ihre Lease zu erneuern. Bei jedem Bootvorgang versucht der Client, die gleiche Adresse bei dem DHCP-Server zu erneuern, die er zuvor in Verwendung hatte (Leaseanfrage startet direkt mit DHCPREQUEST). Ist dies erfolglos (DHCPNACK), so startet er einen neuen Leasevorgang.
Ist eine turnusmäßige Erneuerung der Lease nach der Hälfte der Leasdauer nicht erfolgreich, so sendet der Client nach 87,5% der Leasedauer eine DHCPREQUEST-Meldung an alle erreichbaren DHCP-Server, die mittels DHCPACK die Lease erneuern, oder diese mit einer DHCPNACK-Meldung sofort beenden können.
Erhält der Client auf eine DHCPREQUEST-Anfrage eine DHCPNACK-Antwort, so stellt er die Verwendung der Adresse sofort ein und startet einen neuen Leasevorgang mit einer DHCPDISCOVER-Anfrage.
Mittels ***IPCONFIG /renew*** kann die Erneuerung einer Lease erzwungen werden.
Mittels ***IPCONFIG /release*** kann eine Lease freigegeben werden.

1.4.2 Namensauflösungen

Zur Namensauflösung (= Zuordnung von IP-Adressen zu Netzwerknamen) können mehrere Verfahren angewandt werden. Windows 2000 geht bei einer Anfrage auf einen Klartextnamen folgenden Weg:

	Verfahren	***Aufgelöst werden ...***
1	Vergleich des Namens mit dem lokalen Rechnernamen	Hostnamen
2	Auswertung der Datei HOSTS	Fully Qualified Domain Names
3	DNS-Anfrage	Fully Qualified Domain Names
4	Suche im lokalen, NetBIOS- Namenscache	NetBIOS-Namen
5	WINS- Anfrage	NetBIOS-Namen
6	Broadcast- Anfrage	NetBIOS-Namen
7	Auswertung der Datei %SYSTEMROOT%\system32\drivers\etc***lmhosts***	NetBIOS-Namen

Ist das System auch nach Auswertung der Datei LMHOSTS nicht in der Lage, den Namen in eine IP-Adresse aufzulösen, so ist der Verbindungsversuch gescheitert.

1.4.2.1 Namensauflösung über lokalen Rechnernamen

Prinzip: Schau' wie Du selbst heißt – vielleicht bist Du ja gemeint ...

1.4.2.2 Namensauflösung über die Datei HOSTS

Der Namensdienst durchforstet Zeilenweise die Datei %SYSTEMROOT%\system32\drivers\etc***hosts*** nach dem gesuchten Namen. Wird dieser Name gefunden, so wird die IP-Adresse, die diesem Namen zugeordnet ist, an ARP zur Routenbestimmung übergeben.

Nachteil: Die Datei HOSTS ist statisch. Bei Veränderungen im Netzwerk muß die Datei manuell angepasst werden!

1.4.2.3 Namensauflösung über DNS (Domain Naming System)

Bei DNS handelt es sich um eine verteilte Datenbank, die dazu dient, einen FDQN (Fully Qualified Domain Name) in eine IP-Adresse umzusetzen.

1.4.2.3.1 Primäre DNS- Server, sekundäre DNS- Server, Masternamenserver, DNS- Server für Zwischenspeicherungen

- ⇒ Der primäre Nameserver einer Zone enthält die Masterkopie der DNS-Datenbanken jener Zone, für die er autorisiert wurde.
- ⇒ Der sekundäre Nameserver einer Zone enthält eine Kopie der DNS-Datenbanken des primären Nameservers. Gründe für die Implementierung eines sekundären Nameservers können Redundanz, Geschwindigkeitsvorteile in Remotestandorten oder Lastverringerung für die restlichen Nameserver im Netzwerk sein.
- ⇒ Es kann innerhalb einer Zone nur einen primären, aber mehrere sekundäre Nameserver geben.
- ⇒ Ein sekundärer Nameserver (eine als sekundär auf einem DNS-Server deklarierte Zone) bezieht sich immer auf einen Ursprungsserver, von dem die Zonendaten bezogen werden. Dieser Ursprungsserver kann sowohl der primäre als auch ein sekundärer Nameserver für die Zone sein – er wird auch „*Masternamenserver*“ genannt.
- ⇒ Server für Zwischenspeicherungen führen keine eigene Zonendatenbank. Sie nehmen lediglich Anfragen von DNS-Clients an und leiten diese an andere DNS- Server weiter. Bevor die Anfragen weitergeleitet werden, prüfen Server für Zwischenspeicherungen jedoch den lokalen Cache auf eine eventuell vorhandene DNS- Zuordnung.
  Ebenso leiten sie die Antworten an die entsprechenden DNS- Clients weiter – jedoch nachdem sie die Daten in einem lokalen Cache zwischengespeichert haben.

1.4.2.3.2 DNS- Abfragearten

rekursive Abfragen	der angefragte DNS- Server muß eine Adresse oder eine Fehlermeldung an den anfragenden Client übergeben – ein Verweis auf einen anderen Nameserver ist nicht zulässig
iterative Abfragen	der angefragte DNS- Server teilt dem anfragenden DNS- Client die beste, derzeit verfügbare Antwort mit. Diese kann jedoch auch ein Verweis auf einen anderen Nameserver beinhalten.
Inverse Abfragen	Anfrage an einen Nameserver, eine IP- Adresse in einen Hostnamen aufzulösen (reverse Lookup über die Domäne in-addr.arpa

1.4.2.3.3 DNS- Eintragsarten

SOA	Start of Authority => Erster Eintrag in der DNS- Datenbank – der Ursprung [lokaler Server] – allgemeine Parameter
NS	Nameserver => Verweis auf weitere Nameserver einer Domäne
A	Hosteintrag => Datenbankeintrag für einen Host
CNAME	Canonical Name => Alias- Namensangabe
HINFO	Host Information => Hardware- und Softwareangaben
MX	Mail Exchanger => Nachrichten- Annehmende Server der Domäne (in Reihenfolge)
PTR	Pointer => Rekursivabfrage- Eintrag
SRV	Service => Angabe über Server und deren spezifizierte Dienste

1.4.2.3.4 Die DNS- Datenbank

Die DNS-Datenbank unter Windows 2000 findet man im Verzeichnis %systemroot%\system32\dns.

1.4.2.3.5 Richtlinien für die DNS-Namensgebung

- Ein Domänennamen darf die Zeichen A bist Z, a bis z, 0 bis 9 und den Bindestrich (-) enthalten.
- Bei Windows- TCP/IP wird der Rechnername standardmäßig als DNS-Hostname übernommen. Ein eventuell vorhandener Unterstrich (_) im Namen wird durch einen Bindestrich (-) ersetzt
- Der Rechnername darf vom DNS-Hostnamen abweichen
- Ein Domänenname darf bis zu 63 umfassen (die Punkte eingeschlossen)
- Ein FDQN darf 255 Zeichen nicht überschreiten
- Es wird nicht zwischen Groß- und Kleinschreibung unterschieden

1.4.2.3.6 Beispiel für einen FDQN (Fully Qualified Domain Name)

Server23.technik.ransbach.dobatech.de.		<= FQDN (Fully Qualified Domain Name) des Servers
.	= root	<= Stammdomäne
.de	= Domänenname	<= Domäne 1. Ebene
.dobatech	= Domänenname	<= Domäne 2. Ebene
.technik	= Domänenname	<= Domäne 3. Ebene
server23	= Computername	<= DNS- Hostname

1.4.2.3.7 Konventionen für DNS-Namen von Rechnern

Der DNS-Namen eines Rechners darf - im Gegensatz zum Rechnernamen - keinen Unterstrich enthalten. Ein eventuell vorhandener Unterstrich im Rechnernamen wird beim dynamischen Veröffentlichen eines Rechnernamens im Windows 2000 DNS-Server in einen Bindestrich umgewandelt.

1.4.2.3.8 Das DNS- Dienstprogramm nslookup

Mittels des Dienstprogrammes nslookup.exe (in %systemroot%\system32) kann die DNS-Funktionalität getestet werden. NSLOOKUP kann in zwei verschiedenen Modi aufgerufen werden

- nicht interaktiver Modus
  im „nicht interaktiven Modus“ wird der aufzulösende Name dem Programm direkt mit übergeben. nslookup gibt in diesem Fall die Antwort des konfigurierten Nameservers zurück (bzw. eine entsprechende Fehlermeldung bei nichterreichbarkeit)
- interaktiver Modus
  im iteraktiven Modus stellt das Dienstprogramm eine Eingabeschnittstelle zur manuellen Nameserverabfrage zur Verfügung. Neben der Standard- Funktion „auflösen eines Namens“ lassen sich hier noch weitere Befehle ausführen

1.4.2.3.9 Der DNS- Notify- Satz

Mit Verwendung der Benachrichtigungsliste benachrichtigt der Masterserver die in der Liste eingetragenen sekundären Server, wenn Änderungen eingetreten sind. Daraufhin können die sekundären Server prüfen, ob sie eine Zonenübertragung einleiten müssen.

Beispiel: Die Zone auf dem primären Server wird verändert und somit die Seriennummer im SOA- Eintrag des primären Servers erhöht
Der primäre Server sendet als Teil des Benachrichtigungssatzes eine Benachrichtigung an den/die eingetragenen sekundären DNS- Server
Der/Die sekundäre(n) DNS- Server initiieren eine AXFR- oder eine IXFR- Zonenübertragung

Dieser DNS-Notify-Satz wird jedoch bei Microsoft nur von Windows 2000-DNS-Servern unterstützt.

1.4.2.3.10 Active- Directory integrierte DNS-Zonen

Für die Replikation Active Directory integrierter DNS- Zonen müssen keine Aktualisierungspfade eingerichtet werden, da die DNS- Aktualisierung zwischen den DNS- Servern über die Multimasterreplikation der Active Directory automatisch mit erledigt wird.

1.4.2.3.11 Round Robin

Die Technik, dass ein DNS- Server aus einer Liste von IP-Adressen zu einem Host- oder CName bei jeder Anfrage eine andere an erster Stelle nennt, wird Round Robin genannt.

1.4.2.3.12 DNS- Zonendelegierungen

Eine inkorrekte Delegierung einer DNS- Zone führt zu Problemen bei der Rekursivabfrage. Bei dieser Art der Abfrage muss jeder DNS-Server erreichbar sein.

1.4.2.3.13 Standard- DNS-Registrierungsverfahren unter Windows 2000

Die Standardeinstellung bei der dynamischen Aktualisierung bewirkt, dass Clients vom DHCP-Server die PTR-Ressourceneinträge in der Reverse-Lookupzone durchführen lassen, den A-Ressourceneintrag in der Forward-Lookupzone jedoch selbst ausführen

1.4.2.3.14 DNS-Aktualisierungen

DNS-Server können so eingestellt werden, dass sie nur gesicherte Aktualisierungen akzeptieren.

Server aus der globalen Sicherheitsgruppe „DNSUpdateProxy“ führen durch ihre Mitgliedschaft in dieser Gruppe Aktualisierungen an anderen DNS-Servern immer gesichert aus.
Es kann nötig sein, die DHCP-Server zu dieser Sicherheitszone hinzuzufügen, damit diese die DNS-Aktualisierungen für Downlevel- Clients durchführen können. Durch Hinzufügen der DHCP-Server zur Gruppe DNSUpdateProxy besitzen die Einträge in der DNS-Zone jedoch keine Sicherheit mehr, und damit kann jeder authentifizierte Benutzer den Besitz dieser Objekte übernehmen.

1.4.2.3.14.1 Vollständige Zonenübertragungen (AXFR- Abfrage)

Bei einer vollständigen Zonenübertragung überträgt der primäre DNS-Server die gesamte DNS-Zonendatenbankdatei an den/die sekundären DNS-Server. Diese Form der Zonenübertragung wird auch von älteren DNS-Systemen unterstützt.

1.4.2.3.14.2 Inkrementelle Zonenübertragungen (IXFR- Abfrage)

Bei der inkrementellen DNS- Zonenübertragung verfolgen die Server die Resourceneinträge und es werden bei der Zonenübertragung nur die veränderten Daten übertragen.
BIND ab Version 8.2 unterstützt (wie Windows 2000 DNS) die inkrementelle Zonenübertragung zwischen primären und sekundären DNS-Zonen.

1.4.2.3.15 Windows 2000 DNS vs. BIND- Server

1.4.2.3.15.1 Kompatibilität

Windows 2000 DNS ist kompatibel zu BIND ab Version 4.9.7

1.4.2.3.15.2 Dynamische Aktualisierung von DNS-Clients

BIND ab Version 8.1.2 unterstützt (wie Windows 2000 DNS) die dynamische Aktualisierung von DNS- Clients

1.4.2.4 Namensauflösung über lokalen NetBIOS Namenscache

1.4.2.5 Namensauflösung über WINS (Windows Internet Name Service)

Bei WINS handelt es sich im einen erweiterten NetBIOS Namensdienst, der NetBIOS-Computernamen und dazugehörige IP-Adressen registriert und bei Anfragen auf Namen diese in IP-Adressen auflöst.

1.4.2.5.1 Grenzwerte und Empfehlungen zur Planung von WINS-Servern

- Es gibt keinen Grenzwert für die Bearbeitung von WINS-Anforderungen
- 1.500 Namensregistrierungen und 4.500 Namensanfragen pro Minute sind lt. Microsoft realistisch durch WINS-Server zu bewältigen
- Empfehlung durch Microsoft: 1 WINS-Server und 1 WINS-Sicherungsserver je 10.000 WINS-Clients
- In Multiprozessorsystemen steigt die Leistung des WINS-Serverdienstes um je 25% pro Prozessor, da für jeden Prozessor ein eigener WINS-Thread gestartet wird
- Wird die Protokollierung der Änderungen in der WINS-Datenbank deaktiviert, werden Namen schneller registriert. Es können aber Änderungen durch Abstürze verloren gehen.

1.4.2.5.2 Merkmale des WINS-Client- Dienstes

- Ein WINS-Client versucht dreimal, den primären WINS-Server zu finden. Anschließend versucht er, den sekundären WINS-Server zu finden. Schlägt beides fehl, generiert der Client Broadcasts
- Ein WINS-Client versucht nach einem achtel des TTL-Intervalls seine Lease beim WINS-Server zu erneuern. Schlägt dies Fehl, so versucht er dies bis zur Hälfte des TTL-Intervalls alle zwei Minuten weiter
- Wird ein WINS-Client Ordnungsgemäß beendet, so sendet er für alle registrierten Namen eine Freigabeanforderung an den WINS-Server
- WINS verwendet gerichtete UDP-Datagramme über Port 137 (NetBIOS- Namensdienst)

1.4.2.5.3 Mögliche WINS-Clients

- Windows 2000 (Professional oder Server)
  => Hint: Domänencontroller sollten in gemischten Umgebungen mit WINS als WINS-Clients konfiguriert werden, damit die älteren Systeme den DC finden.
- Windows NT 3.5 oder höher
- Windows 95/98/ME
- Windows für Workgroups 3.11 mit Microsoft TCP/IP-32
- Microsoft Netzwerkclient 3.0 für MS-DOS
- LAN-Manager 2.2c für MS-DOS

1.4.2.5.4 WINS- Proxy- Agent

Ein WINS-Proxy-Agent ist ein Computer, der die Namensauflösungsfunktion eine WINS-Servers auf nicht-WINS-Clients erweitert. Hierzu muß lediglich ein Registry- Eintrag (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\EnableProxy=1) auf einem WINS-Client erstellt werden.

Ferner sind WINS-Proxy-Clients dazu in der Lage, von Unix-Clients kommende, WINS-Broadcastanfragen an WINS-Server weiterzuleiten.

1.4.2.5.5 WINS-Replikation

Die WINS-Replikation geschieht über Push/Pull- Replikation. Die Replikation wird immer vom Push- zum Pullpartner gesendet. Ein WINS-Server kann entweder PUSH-, PULL- oder auch PUSH/PULL-Partner innerhalb einer WINS-Replika sein.

Einsatzgebiet der Replikationstechniken

Technik	Einsatzgebiet	Begründung
PUSH	Schnelle Verbindungen	Die Push- Replikation findet statt, wenn eine vordefinierte Anzahl von Änderungen eingetreten ist
PULL	Langsame Verbindungen	Replikation kann Zeitgesteuert konfiguriert werden
PUSH/PULL	Wenn gegenseitige Replikation nötig ist	

Die Replikationspartner können manuell konfiguriert werden.
Ferner kann der WINS- Server auch für eine automatische Suche nach Replikationspartnern konfiguriert werden. Hierzu sendet der WINS- Server alle 40 Minuten eine Multicast- Anfrage an die Klasse D- Adresse 224.000.001.024. Finden sich WINS-Server auf diesem Weg, konfigurieren sie sich für eine gegenseitige PUSH/PULL- Replikation im Abstand von 2 Stunden.

1.4.2.5.6 WINS- Dienstprogramme

1.4.2.5.6.1 Die Microsoft Management Console (MMC)

Das Standardprogramm zur Verwaltung und Konfiguration von WINS ist die MMC mit dem entsprechenden WINS- Plugin

1.4.2.5.6.2 JetPack

Mittels des Dienstprogrammes JETPACK.EXE kann unter anderem die WINS- Datenbank offline gepackt werden (JETPACK ist auch für die DHCP-Datenbank geeignet!).
Beispielscript:

```
CD %SYSTEMROOT%\SYSTEM32\WINS
NET STOP WINS
JETPACK WINS.MDB TEMP.MDB
NET START WINS
```

Hinweis: Auch wenn die Dateierweiterung ein MS-Access- Format vermuten lässt – die Datei lässt sich zumindest mit Access 2000 nicht lesen ...

1.4.2.5.7 Sicherung der WINS-Datenbank

Der WINS- Serverdienst sichert die WINS-Datenbank alle drei (3) Stunden automatisch als Datei WINS.MDB in das Verzeichnis \WINS_BAK\NEW unterhalb des Verzeichnisses, welches in den Servereigenschaften als Standard-Sicherungsverzeichnis angegeben wurde.

1.4.2.5.8 Wiederherstellung der WINS- Datenbanken

Die WINS- Datenbanken sind aus dem Sicherungspfad (Siehe 1.4.2.5.7) mit Hilfe des WINS- Managers wiederherstellbar. Zuerst ist der WINS-Dienst in der WINS-Manager zu stoppen. Dann sind die Dateien zu löschen. Als Nächstes kann mit der Funktion Wiederherstellen der Datenbank in der MMC (Kontextmenü von WINS) die Datenbank wiederhergestellt werden. Danach wird der WINS-Dienst automatisch gestartet

1.4.2.6 Namensauflösung über Broadcast

1.4.2.7 Namensauflösung über die Datei LMHOSTS

Zur Namensauflösung über die Datei LMHOSTS wird der Inhalt der entsprechenden Datei im Verzeichnis %systemroot%\system32\drivers\etc ausgewertet. In dieser Datei können folgende Befehle enthalten sein:

#PRE	Eintrag wird vorab als permanenter Wert in den NetBIOS- Namenscache geladen. Manuell können #PRE- Einträge über das Tool „nbtstat“ mit dem Startparameter „-r“ geladen werden.
#DOM:[Domäne]	Angabe der Domäne, zu der der entsprechende Eintrag gehört
#NOFNR	Vermeidet die Verwendung von über NetBIOS gesteuerten Namensanfragen für ältere LAN-Manager UNIX-Systeme
#BEGIN_ALTERNATE	
#END_ALTERNATE	Beginn und Ende einer Alternativliste von LMHOSTS-Dateien
#INCLUDE	Verwendung der hinter #INCLUDE angegebenen Datei als zusätzliche Namensauflösungsquelle
#MH	Weiterer Eintrag für mehrfach vernetzte Rechner

1.4.2.7.1 NetBIOS-Knotentypen

B-Knoten (Broadcast)	Namensauflösung über als Broadcast gesendete NetBIOS-Namensanfragen
P-Knoten (Peer to Peer)	Namensauflösung unter Verwendung eines WINS-Servers
M-Knoten (Mixed)	Mischung aus B- und P- Knoten; Namensauflösung zuerst über Broadcast und bei Mißerfolg anschließend unter Verwendung eines WINS-Servers
H-Knoten (Hybrid)	Mischung aus P- und B- Knoten; Namensauflösung zuerst unter Verwendung eines WINS-Servers und bei Mißerfolg durch Broadcasts

Windows 2000- Systeme sind standardmäßig als B- Knoten konfiguriert. Durch Umstellung eines Windows 2000 Systems auf die Verwendung eines WINS-Servers werden diese zu H.-Knoten. Durch Entfernung des Konfigurationseintrages für den WINS-Client wird das System aber nicht mehr zum B-Knoten zurückgestellt – dies ist nur durch manuelle Änderung in der Registry möglich.

2 Allgemeines zu Windows 2000

2.1 Setup- Protokolldateien

Protokolldateien über das Windows 2000- Professional-Setup

Datei	***Protokolliert das Setup von ...***
%SYSTEMROOT%\comsetup.log	COM+ und optionale Komponenten
%SYSTEMROOT%\mmdet.log	Multimediageräte
%SYSTEMROOT%\setupapi.log	Je ein Eintrag für jeden Import einer Zeile aus einer *.INF-Datei
%SYSTEMROOT%\debug\NetSetup.log	Hinzufügen/Entfernen eines Computers zu/aus Arbeitsgruppe/Domäne

2.2 Dateisystem

2.2.1 Dateinamens-Konventionen

Für lange Dateinamen wird ein 8.3-Aliasname angelegt (anzeigbar unter Windows 2000 mittels DIR *.* /X).
Der Aliasname wird nach folgenden Konventionen gebildet:

- Leerzeichen werden entfernt
- die ersten 6 Zeichen des Dateinamens werden mit fortlaufender Ordnungszahl 1-4 und einer "~" ergänzt, der letzte Suffix wird auf die ersten drei Zeichen gekürzt.
- ab der 5. Datei "gleichen Namens" werden die beiden ersten Zeichen des Dateinamens genommen, um eine 4-Stellige, Hexadezimale zufallszahl ergänzt und diese dann über ~1- bis ~n- Anhänge durchnummeriert.

2.2.2 Basislaufwerke vs. Dynamische Datenträger

Basislaufwerke unterstützen max. 4 Partitionen, davon darf eine eine Erweiterte Partition sein, die logische Lauwerke enthalten kann.

Dynamische Datenträger bestehen aus einer einzelnen, das ganze Laufwerk übergreifenden Partition, auf der folgende Laufwerkstypen angelegt werden können:

Einfache Datenträger	(vergleichbar mit primären Partitionen oder logischen Laufwerken)
Übergreifende Datenträger	(Speicherplatz mehrerer Bereiche wird zusammengefasst – 2-32 Laufwerke)
Stripe- Set	(„streifenweise zu 64kByte“ auf mehrere Bereiche schreibend, 2-32 Laufwerke)
Gespiegelte Datenträger	(RAID-0, genau zwei Laufwerksbereiche gegeneinander)
RAID-5 Datenträger	(3-32 Lauwerke als Stripe-Set mit Parity)

Hinweis: Entfernbare Datenträger können nur über eine primäre Partition auf einem Basis-Datenträger verfügen!

2.2.3 Dateisysteme

Windows 2000 unterstützt folgende Dateisysteme:

FAT12	(z.B. 5 ¼”- Disketten)
FAT16	(kompatibel mit MS-DOS, max. 4096 kB je Lauwerk)
FAT32	(kompatibel mit Windows 95b oder später, bis zu 2.047 GB lesend, selbst jedoch beschränkt auf 32GB!)
NTFS	(New Technologie File System, Version 5)
CDFS	(CD-File System)
UDF	(Universal Disk Format)

2.2.4 Dienstprogramme

2.2.4.1 Das Dienstprogramm convert

Konvertiert FAT- und FAT32- in NTFS-Datenträger. Das aktuelle Laufwerk kann nicht konvertiert werden. Wenn **convert** das Laufwerk nicht sperren kann, werden Sie gefragt, ob das Laufwerk beim nächsten Start des Computers konvertiert werden soll.

Hinweis: Unter NT4 war es noch möglich, eine HPFS-Partition zu einer NTFS-Partition zu konvertieren

2.2.4.2 delpart.com versus delpart.exe

Microsoft bietet zwei Tools zum löschen von Partitionen zum Download an

delpart.com	-	löscht alle Partitionen ohne Rückfrage sofort
delpart.exe	-	Kommandozeilentool zum löschen einzelner Partitionen

ACHTUNG: Da *.COM vor *.EXE ausgeführt wird, ist eine Kombination beider Tools auf einem Laufwerk bzw. innerhalb eines Suchpfades extrem gefährlich – u.U. wird delpart.com ausgeführt, obwohl delpart.exe gewünscht war.

2.2.4.3 Das Dienstprogramm cipher

Zeigt die Verschlüsselung von Ordnern und Dateien auf NTFS-Datenträgern an oder ändert sie.

2.2.5 Microsoft- Begriffsfestlegungen

Begriff	Microsoft meint damit
Systempartition	Partition des Rechners, von der gebootet wird
Bootpartition	Partition des Rechners, auf der das System installiert ist
Socket	Netzwerkadresse + Hostadresse + Port

2.2.6 Dateiberechtigungen unter NTFS

Wichtiger Hinweis:

Windows 2000 Unterstützt POSIX-Anwendungen.

Da auf UNIX-Systemen die Berechtigungn "Vollzugriff" das Recht zum Löschen von Unterordnern und Dateien einschließt, ist dies unter Windows 2000 aus Kompatibilitätsgründen ebenso möglich, auch wenn auf die jeweiligen Unterordner oder Dateien das Löschrecht nicht vorhanden ist.

Auch ein explizietes Entfernen des Löschrechtes von einzelnen Dateien kann das aus der Ordnerberechtigung resultierende Löschrecht nicht einschränken.

2.2.7 Distributed File System (DFS)

Windows 2000 unterstützen die zentralisierte Verwaltung verteilter Freigaben über DFS. In einem DFS-Stamm werden im Netzwerk verteilte Resourcen (Freigaben) unterschiedlicher Rechner innerhalb einer Freigabe als Ordnerstruktur zusammengefasst.

2.2.7.1 DFS-Clients

- Windows NT 4 oder höher
- Windows 98 oder höher
- Windows 95 mit DFS-Client aus dem Internet

2.2.7.2 Eigenständiger (Standalone) DFS-Stamm

- Kann ohne Active Directory erstellt werden
- Ergibt keine Redundanz
- Es ist nur eine Ebene in der DFS-Struktur möglich

2.2.7.3 Domänen-DFS-Stamm

- Erfordert Active Directory
- Information über DFS-Stamm wird mit der Active Directory repliziert
- Eine DFS-Struktur ist in mehreren Ebenen möglich
- Replikation der DFS-Struktur (Ordnerstruktur) auf mehrere Rechner ist möglich

2.3 Benutzerverwaltung

2.3.1 Konventionen für Anmeldenamen und Kennwörter

- Windows 2000 erkennt nur die ersten 20 Zeichen eines Anmeldenamens - man sollte daher niemals längere Anmeldenamen verwenden.
- Windows 2000 unterscheidet bei Anmeldenamen nicht zwischen Groß- und Kleinschreibung, bei Kennwörtern hingegen schon
- Windows 2000 kann maximal 127 Zeichen lange Kennwörter verarbeiten. Es sollten Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten sein. Kennwörter sollten lt. MS-Empfehlung nicht kürzer als 8 Zeichen sein.

2.3.2 Einrichtung von Anmeldebeschränkungen

2.3.2.1 Computer, von denen sich Benutzer anmelden können

Hinweis: Wenn NetBIOS über TCP/IP (NBT) deaktiviert ist, kann nicht ermittelt werden, von welchem Computer aus ein Benutzer sich anzumelden versucht. In diesem Fall ist es nicht möglich, den Anmeldezugriff auf bestimmte Computer zu beschränken.

2.4 Gruppenverwaltung

2.4.1 Gruppentypen

2.4.1.1 Sicherheitsgruppen vs. Verteilergruppen

Sicherheitsgruppen haben mehr Objekteigenschaften und eignen sich somit besser für die Rechteverwaltung.
Verteilergruppen sind für die Verwaltung von Objektrechten nicht geeignet.
Verteilergruppen können nur von Anwendungen, die Active-Directory-Dienste einsetzen verwendet werden.

2.4.2 Gruppenbereiche

Gruppenbereich	***Mitgliedschaft***	***Zugriffsregelung für***	***Verfügbarkeit***
Lokale Domänengruppen	Benutzer beliebiger Domänen	Nur für Resourcen der Domäne, in der die Gruppe existiert	
Globale Gruppen	Nur Benutzer der Domäne, in der die Gruppe existiert	Für Resourcen beliebiger Domänen	
Universelle Gruppen	Benutzer beliebiger Domänen	Für Resourcen beliebiger Domänen	Nur im einheitlichen Modus verfügbar

Gruppenbereich	***Kann Mitglied sein in***	***Mitglieder können sein aus***
Lokale Gruppen	Lokalen Domänengruppen und globalen Gruppen	Benutzerkonten, Computerkonten, globale Gruppen, universelle Gruppen aus bel. Domäne und lokale Domänengruppen aus der gleichen Domäne
Globale Gruppen	Lokalen und Universellen Gruppen	Benutzerkonten, Computerkonten und globale Gruppen aus der gleichen Domäne
Universelle Gruppen	Lokalen Gruppen und universellen Gruppen	Benutzerkonten, Computerkonten, globale Gruppen und universelle Gruppen aus bel. Domäne

2.4.3 Vordefinierte Systemgruppen

Gruppe	***Inhalt der Gruppe***
Jeder	Alle Benutzer, die lokal oder über das Netzwerk auf einen Computer zugreifen
Autentifizierte Benutzer	Alle Benutzer, die über ein gültiges Zugriffstoken verfügen - sich also erfolgreich an einem Rechner oder einer Domäne angemeldet haben
Ersteller-Besitzer	Der Besitzer eines Objektes (=> Objekteigenschaft)
Netzwerk	Jeder, der über das Netzwerk auf die entsprechende Resource zugreift
Interaktiv	Jeder, der lokal am Rechner, der die Resource vorhält, angemeldet ist
Anonymous	Jeder, der nicht autentifiziert wurde, also kein gültiges Zugriffstoken besitzt
Dialup	Jeder, der im Moment des Zugriffes auf die entsprechende Resource eine Wählverbindung zu dem Rechner aufrecht erhält, der die Resource zur Verfügung stellt.

2.5 Windows 2000 Starten und beenden

2.5.1 Windows 2000 Startmodi

Abgesicherte Modi	Nur Standard-Treiber und Dienste werden gestartet, ggf. mit den angegebenen, zusätlichen Komponenten (Netzwerk ggf. zur Fernwartung, DOS falls die GUI Probleme bereitet)
Startprotokollierung	Schreibt die Protokolldatei Ntbtlog.txt in das Verzeichnis %systemroot%
Letzte als funktionierend bekannte Konfiguration	Startet Windows unter Verwendung der letzten, als Funktional bekannten Hardwarekonfiguration (=> LastKnownGood in der Registry)
Verzeichnisdienstwiederherstellung	nur Windows 2000 Server (setzt die USN [Universal Serial Number] von AD-Objekten hoch, so daß diese höher liegen als auf allen anderen AD-Kopien im Netz)
Debugmodus	nur Windows 2000 Server
Normal starten	Startet normal

Bei allen erweiterten Startoptionen (außer bei LastKnownGood) wird der Standard-VGA-Treiber verwendet und ein Startprotokoll erstellt

2.5.2 Die Datei BOOT.INI

In der Datei BOOT.INI können mehrere Startsysteme festgelegt werden. Hierzu werden für Windows 2000 Systeme die ARC-Pfade (ARC => Advanced RISC Computing; RISC => Reduced Instruction Set Computing) zu den jeweiligen Installationen angegeben.

2.5.2.1 Syntax der ARC-Pfade:

multi(x) | scsi(x)	multi = alle Controller, die vom Bios unterstützt werden; scsi nur für scsi-Controller, deren Bios nicht aktiviert wurde (Wert: 0-n)
disk(y)	SCSI-ID. Für multi lautet der Wert für (y) immer 0 (Wert: 0-n)
rdisk(z)	Identifikationsnummer des Laufwerkes (wird bei scsi ignoriert) (Wert: 0-n)
partition(a)	Identifikationsnummer der Partition des Laufwerkes (Wert: **1**-n)

Beispiel: multi(0)disk(0)rdisk(1)partition(2)

2.5.2.2 Startoptionen von Windows 2000

/basevideo	Start unter Verwendung der Standard VGA-Treiber
/fastdetect	Deaktivierung der COM-Port Geräteerkennung
/maxmem:n	RAM-Umfang zur Verwendung von Windows 2000 begrenzen (Angabe in MB)
/noguiboot	GUI- Startphase (= Grafik mit Ladestatus) nicht anzeigen
/sos	Gerätetreibernamen beim Laden anzeigen

2.5.3 Startverhalten von Diensten in der Registry beeinflussen

Der Inhalt des Schlüssels
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*[Dienstname]*\Errorcontrol=
definiert das Startverhalten eines Dienstes bzw. das Verhalten bei Fehlern. Die Inhalte hierzu haben folgende Bedeutung:

0x0	Startfehler ignorieren und fortfahren ohne Fehlermeldung
0x1	Startfehler ignorieren und fortfahren mit Fehlermeldung
0x2	Startsequenz schlägt fehl und wird mit dem Steuersatz "LastKnownGood" neu gestartet. Wenn dieser Steuersatz bereits verwendet wird, wird der Fehler ignoriert und die Startseqzenz fortgesetzt
0x3	Startsequenz schlägt fehl und wird mit dem Steuersatz "LastKnownGood" neu gestartet. Wenn dieser Steuersatz bereits verwendet wird, wird die Startsequenz gestoppt und eine Fehlermeldung eingeblendet

2.5.4 Anmeldung / Abmeldung

2.5.4.1 Anmeldevoraussetzungen

- Ein erreichbarer Anmeldeserver im gleichen Subnetz oder in einem über Routing erreichbaren Netz
- Sollte nur DNS als Namensauflösungsdienst verwendet werden, so muß im DNS mindest ein erreichbarer Domänencontroller mit einem SRV- Eintrag zu finden sein.

2.5.4.2 Anmeldescriptverarbeitung

- Anmeldescripts werden unter Windows 2000 in Gruppenrichtlinien festgelegt.
- Die Option, welche bewirkt, dass mit dem Start der Windows-Explorer-Schnittstelle (der Betriebssystemshell) und dem Erstellen des Desktops gewartet wird, bis die Anmeldeskripts zu Ende ausgeführt wurden, heißt „Anmeldeskripts gleichzeitig ausführen“ und ist unter der Benutzer- und der Computerkonfiguration unter Administrative Vorlagen\ System\ Anmeldung zu finden, wobei die Computerrichtlinie Vorrang hat.
  Die Option bewirkt, dass der Explorer mit den Anmeldeskripts synchronisiert wird, dafür können einige Sekunden verstreichen, bis der Desktop angezeigt wird.

2.6 Internet Connection Sharing

Beim ICS – Internet Connection Sharing – Gemeinsame Nutzung der Internetverbindung – handelt es sich um ein Paket, welches DHCP, NAT und DNS umfasst.
Die einzelnen Bereiche arbeiten dabei im groben wie folgt

2.6.1 DHCP durch ICS

Der Recher, der ICS zur Verfügung stellt, fungiert als DHCP-Server mit folgender Konfiguration:

Adressbereich	192.168.000.002 – 192.168.000.254
Gateway	192.168.000.001
DNS-Server	192.168.000.001

2.6.2 DNS durch ICS

Der Rechner, der ICS zur Verfügung stellt, fungiert als einfaches DNS-Relay – er leitet alle DNS-Anfragen an den/die DNS-Server weiter, welche für die öffentliche ICS- Schnittstelle konfiguriert wurde(n).

2.6.3 NAT durch ICS

Der Rechner, der ICS zur Verfügung stellt, fungiert als einfacher NAT-Router. Er ordnet jede interne Adresse aus dem Netz 192.168.000.000/24 der jeweils dynamisch zugeordneten, öffentlichen IP zu.

2.7 Die Registry

2.7.1 Teilstrukturen

HKEY_LOCAL_MACHINE
: Enthält alle Konfigurationsdaten für den lokalen Computer. Diese Daten sind Benutzer- Unabhängig und bleiben konstant

HKEY_USERS
: Enthält alle Standard- Benutzereinstellungen für das System

HKEY_CURRENT_USER
: Enthält Daten über den aktuell angemeldeten Benutzer. Es wird je eine Kopie für jedes Benutzerkonto abgerufen und im Schlüssel "%systemroot%\dokumente und einstellungen\Benutzername" abgespeichert.

HKEY_CLASSES_ROOT
: Enthält Software- Konfigurationsdaten - d.h. Daten zur OLE und den Dateiverknüpfungen. Es besteht eine Verknüpfung zu HKEY_LOCAL_MACHINE\SOFTWARE\Classes.

HKEY_CURRENT_CONFIG
: Enthält Daten aus den Zweigen SOFTWARE und SYSTEM.

2.7.1.1 Näheres zu HKEY_LOCAL_MACHINE

2.7.1.1.1 HKEY_LOCAL_MACHINE\SYSTEM\SELECT\ ...

Die Unterschlüssel Current, Default, Failed und LastKnownGood verweisen für den jeweiligen Fall auf die entsprechenden ControlSet00x-Pfade der Registry.
Nach erfolgter Anmeldung wird der Wert Current in den Wert LastKnownGood kopiert. Durch eine Abmeldung wird der Wert aus Current in den Wert Default kopiert.

2.7.2 Datentypen

REG_DWORD	Ein Einzelner Wert aus einem String von 1-8 Hexadezimalen Ziffern
REG_SZ	Ein Einzelner Wert als String
REG_EXPAND_SZ	Ein einzelner Wertestring, der eine Umgebungsvariable enthalten kann.
REG_BINARY	Nur ein einzelner Wert (Hexadezimal). Jedes Zahlenpaar wird als Byte-Wert interpretiert.
REG_MULTI_SZ	Mehrere Werte möglich; jeder einzelne Teilstring wird als einzelner REG_SZ: -Wert interpretiert
REG_FULL_RESOURCE_DESCRIPTOR	Ressourcenliste mit Hardwarekomponenten oder Treibern. Ein Eintrag dieses Typs kann weder hinzugefügt noch geändert werden.

2.7.3 Zugeordnete Dateien

Unterschlüsseln von Registrty-Zweigen sind diverse Dateien auf dem System zugeordnet.

HKEY_LOCAL_MACHINE\SAM	%systemroot%\system32\config\sam %systemroot%\system32\config\sam.log
HKEY_LOCAL_MACHINE\SECURITY	%systemroot%\system32\config\security %systemroot%\system32\config\security.log
HKEY_LOCAL_MACHINE\SOFTWARE	%systemroot%\system32\config\software %systemroot%\system32\config\software.log %systemroot%\system32\config\software.sav
HKEY_LOCAL_MACHINE\SYSTEN	%systemroot%\system32\config\systen %systemroot%\system32\config\system.log
HKEY_CURRENT_USER	%systemdrive%\dokumente und einstellungen\Benutzername\ntuser.dat bzw. %systemdrive%\documents and settings\username\ntuser.dat

2.7.4 Unterschiede REGEDIT.EXE versus REGEDT32.EXE

- REGEDIT.EXE ermöglicht ein komfortableres Suchen, ist subjektiv übersichtlicher gestaltet und es ist eine Suche über alle Hauptschlüssel möglich
- Nur REGEDT32.EXE unterstützt die Datentypen REG_EXPAND_SZ und REG_MULTI_SZ
- Rechtevergabe zur Registry-Bearbeitung nur mit REGEDT32.EXE möglich

2.7.5 Rechtevergabe zur Remote-Administration der Registry

Im (ggf. anzulegenden Schlüssel)
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg (Typ: REG_DWORD; Wert: 1) werden die Rechte zur Remote-Administration der Registry vergeben. Die Berechtigungen auf diesen Schlüssel definieren die Remote-Administrationsrechte.

2.8 Netzwerke unter Windows 2000

2.8.1 Autentifizierungsprotokolle

2.8.1.1 PAP

Password Authentication Protocol

2.8.1.2 CHAP

Challenge Handshake Authentication Protocol

- Für die Verwendung von CHAP müssen unter Windows 2000 / Active Direktory die Passworte Reversibel gespeichert werden (=> Richtlinie)

2.8.1.3 MS-CHAP

Microsoft Challenge Handshake Authentication Protocol

2.8.1.4 SPAP

Shiva Password Authentication Protocol

2.8.1.5 PPTP

Point-to-Point Tunneling Protocol, ein Tunnelprotokoll

2.8.1.6 EAP

Extensible Authentication Protocol

- Standard- Authentifizierungsprotokoll für SmartCard- Anmeldungen

2.8.1.7 RADIUS

Remote Authentication Dial-in User Service

2.8.1.8 L2TP

Layer-2-Tunnelingprotocol

2.8.1.9 BAP

Bandwith Allocation Protocol

2.8.1.10 BACP

Bandwith Allocation Control Protocol

3 Active Directory

3.1 Installation der Active Directory- Dienste

Das Dienstprogramm zur Installation bzw. Entfernung der Active- Directory-Dienste (ein Assistent) kann nur direkt aufgerufen werden. Es handelt sich dabei um das Programm DCPROMO.EXE

3.2 Die Active Directory- Datenbank

Die Active Directory Datenbank (ntds.dit => **N**ew **T**echnologie **D**irectory **S**ystem . **D**irectory **I**nformation **T**ree) kann mit dem Textbasierenden Tool NTDSUTIL.EXE bearbeitet und verändert werden. Dieses Tool befindet sich im Verzeichnis %systemroot%\system32\.

Als Mindest- Speicherplatz für die Active Directory Datenbank wird von Microsoft ein freier Speicherplatz von 200 MByte angegeben – vorzugsweise (aber nicht unbedingt) auf einer NTFS- Partition.

Für die Protokolldateien (die u.a. am besten NICHT auf dem Laufwerk mit den Systemdateien gespeichert werden) wird von Microsoft ein freier Speicherplatz von mindestens 50 MByte gefordert.

3.3 Betriebsmaster von Windows 2000

3.3.1 Schemamaster

Der Schemamaster verwaltet das Active Directory der gesamten Domäne (Gesamtstruktur aus Domänen oder auch aus einem Forest). Innerhalb dieser Struktur darf es nur einen Schemamaster geben.

3.3.1.1 Bearbeiten des Schemas

Das Schema kann mittels des SnapIns %systemroot%\system32\schmmgmt.msc (Active Directory-Schema) bearbeitet werden. Dieses SnapIn steht erst nach Installation des Adminpacks (Server-CD, Lw:\i386\adminpak.msi) zur Verfügung.

3.3.2 Domänennamenmaster

Der Domänennamenmaster verwaltet die Domänennamen innerhalb eines Domänen- Baumes bzw. innerhalb eines Forest. Es darf innerhalb dieser Struktur nur einen Domänennamenmaster geben.

3.3.3 Infrastrukturmaster

Der Infrastrukturmaster verwaltet die Verweise zwischen Benutzer und Gruppenobjekten. Es darf innerhalb einer Domäne nur einen Infrastrukturmaster geben.

3.3.4 RID-Master (Relativer ID- Master)

Der RID-Master verwaltet die rel. ID's der Domäne, die wiederum Bestandteil der Sicherheitskennung eines jeden Objektes innerhalb einer Domäne ist. Es darf nur einen RID-Master je Domäne geben.
Sollen mit dem Utility MOVETREE.EXE Objekte zwischen Domänen verschoben werden, so muss diese Aktion auf dem RID-Master der Domäne initiiert werden, in der sich der Ursprung des Objektes befindet.

3.3.5 PDC- Emulator

Der PDC- Emulator verwaltet die für die Kompatibilität mit NT4-Servernetzen notwendige SAM. Im Einheitlichen Modus ist der PDC- Emulator auch weiterhin für die Verwaltung von Kennwortänderungen von Benutzern zuständig. Schlägt eine Benutzer- Authentifizierung auf einem Domänencontroller fehl , so leitet dieser die Authentifizierungsanfrage an den PDC-Emulator weiter (Grund: Möglicherweise ist die Replikation noch nicht komplett, aber der PDC-Emulator sollte bescheid wissen... ??)
Es darf innerhalb jeder Domäne nur einen PDC-Emulator geben.

3.3.6 Empfehlungen zur Verteilung der 5 Betriebsmasterrollen

- Gibt es nur einen Domänencontroller in einer Domäne, so ist dieser Betriebsmaster für alle 5 Betriebsmasterrollen.
- RID-Master und PDC-Emulator sollten auf einem Server liegen
- Infrastrukturmaster möglichst nicht auf einem Server, der den globalen Katalog hält
- Schemamaster und Domänennamenmaster sollten auf einem Server liegen

3.3.7 Zuordnung der Betriebsmasterrollen

- Im MMC-Snapin „Active Directory Benutzer und Computer" können die Betriebsmaster
  - RID-Master
  - PDC-Emulator
  - Infrastrukturmaster

  festgelegt werden
- Im MMC-Snapin „Active Directory Domänen und Vertrauensstellungen" kann der Betriebsmaster
  - Domänennamenmaster

  festgelegt werden
- Im MMC-Snapin „Active Directory Schema" kann der Betriebsmaster
  - Schemamaster

  festgelegt werden.

3.3.8 Ausfälle der Betriebsmaster

Ausfälle von Schemamaster, Domänennamenmaster, RID-Master oder Infrastrukturmaster sind für Netzwerkbenutzer nicht sichtbar. Für Administratoren sind diese Ausfälle nur dann relevant, wenn sie in den entsprechenden Bereichen Veränderungen durchführen wollen.
Die Entsprechenden Betriebsmaster-Rollen können bei Ausfall von einem anderen Server erzwungen übernommen werden – in diesem Fall darf der ursprüngliche Betriebsmaster aber nie wieder ohne komplette Neu-Installation ans Netz gehen (Ausnahme: Infrastrukturmaster – den kann man auch wieder zurückgeben...).

Ein Ausfall des PDC-Emulators kann zur Folge haben, dass Benutzer sich nicht anmelden können. Eine entsprechende Übername der Betriebsmasterzuordnung des PDC-Emulators kann jedoch auch wieder rückgängig gemacht werden, wen der ursprüngliche Betriebsmaster wieder am Netz ist.

3.3.9 Globaler Katalogserver

Der erste installierte Active-Directory Domänencontroller wird automatisch globaler Katalogserver. Es können mehrere Globale Katalogserver eingerichtet werden.

3.4 Veröffentlichung von Resourcen innerhalb einer AD-Domäne

Resourcen (=> z.B. Drucker und Freigaben) können innerhalb der Active-Directory mittels dem MMC-Snapin „Active Directory und Computer“ erstellt werden.
=> Auswahl des Domänenknotens => Neu => ....

3.5 Objektverwaltung

3.5.1 Dienstprogramme zur Active Directory Objektverwaltung

3.5.1.1 MMC-Snapin „Active Directory Benutzer und Computer“

Weitergehende Aufgaben des Snapins Active Directory Benutzer und Computer:

- Verschieben von Objekten innerhalb einer Domäne
- Delegierung von Verwaltungsaufgaben über Kontextmenü „Objektverwaltung zuweisen“ (=> Assistent)

3.5.1.2 MMC-Snapin „Active Directory Standorte und Dienste“

Weitergehende Aufgaben des Snapins Active Directory Standorte und Dienste:

- Verschieben von Domänencontroller zwischen Standorten

3.5.1.3 MOVETREE.EXE

In den Windows 2000 Support-Tools enthaltenes Dienstprogramm zum Verschieben von Active Directory- Objekten zwischen Domänen innerhalb einer Gesamtstruktur.

3.5.1.4 NETDOM.EXE

In den Windows 2000 Support-Tools enthaltenes Dienstprogramm zum Verschieben von Computer- und Serverobjekten über Domänengrenzen hinaus.

3.5.1.5 REPLMON.EXE

Der *Active Directory Replikation Monitor*, ist der in den Windows 2000 Support-Tools enthaltene “Viewer” für das Replikationsverhalten / die Replikationsvorgänge innerhalb einer AD-Struktur. Mit dem Replication- Monitor kann aber auch jederzeit die Replikation manuell angestoßen werden.

3.6 Datensicherung / Wiederherstellung der Active Directory Daten

3.6.1 Sicherung

Gesichert werden die AD Daten über NTBACKUP => Sicherung der Systemstatusdateien
Es sind in dieser Sicherung folgende Daten enthalten

- Registrierungsdatenbanken
- COM+ -Objekte
- System- Startdateien
- Zertifikatsdienste- Datenbank
- Active Directory
- SYSVOL- Verzeichnis

Die Systemstatusdateien können ***nicht*** über das Netzwerk gesichert werden!

3.6.2 Wiederherstellung

Wiederherstellung der zuvor gesicherten Dateien ist im Laufendem Betrieb nicht möglich, da die AD- Datenbanken (z.B. die Datei NTDS.DIT) im Zugriff sind und nicht überschrieben werden können. Zur Wiederherstellung muß der Domänencontroller im Modus „Verzeichniswiederstellung“ gestartet werden.

Dieser Modus ist die einzige Situation, in der eine Anmeldeprüfung an einem Domänencontroller über eine SAM-Autentifizierung und nicht über eine AD-Autentifizierung geschieht.

Es handelt sich um den einzigen Einsatzzweck des „Administratorkontos“, welches bei der Installation der Active Directory für die Verzeichnisdienstwiederherstellung angelegt wurde.

3.6.2.1 Nicht- Autorisierende Wiederherstellung

Einfachste Form der Wiederherstellung.

- Start des Servers im Modus „Verzeichniswiederherstellung“
- Rücksicherung der Systemstatusdateien
- Neustart als Domänencontroller

Dieses Verfahren hat zur Folge, dass nach dem Neustart die auf den anderen Domänencontrollern vorhandenen neueren Objekte auf den Wiederhergestellten Domänencontroller repliziert werden.

Durch die „Nicht Autorisierende Wiederherstellung“ können keine Veränderungen, die nach der Sicherung durchgeführt wurden, rückgängig gemacht werden!

3.6.2.2 Autorisierende Wiederherstellung

Flexible Form der Verzeichnisdienst- Wiederherstellung:

- Start des Servers im Modus „Verzeichniswiederherstellung“
- Rücksicherung der Systemstatusdateien
- Start des Dienstprogrammes NTDSUTIL.EXE (Untermenü „AUTHORITATIVE RESTORE“)
- Auswahl der autorisiert zu kennzeichnenden AD- Objekte oder Objektpfade
- Neustart als Domänencontroller

Als Ergebnis dieser Vorgehensweise erhält man eine Situatuin, in der ...

- alle *nicht* als autorisiert markierten AD- Objekte / Objektstrukturen von den weiteren Domänencontrollern aktualisiert (falls notwendig)
- alle als autorisiert markierten AD- Objekte / Objektstrukturen *zu* den weiteren Domänencontrollern aktualisiert

Funktionales Beispiel:

START => Ausführen => CMD↵

C:\>NTDSUTIL ↵
ntdsutil: authoritative restore↵
authoritative restore: restore subtree „OU=Org. Einheit,DC=domain-component2,DC=abcde,DC=net“↵

oder

authoritative restore: restore CN=User4,OU=Sales,DC=Chicago,DC=microsoft,DC=de↵
quit↵
quit↵
exit↵

NEUSTART

3.7 Komprimierung der Active Directory Datenbank

Die Datei NTDS.DIT wird täglich automatisch durch den Prozess „Garbage Collection“ mittels einer „Online-Defragmentierung“ der Datenbank „aufgeräumt“. Durch diesen Prozess wird die Datei jedoch nie verkleinert. Es werden nur die freien Bereiche, die durch Löschung von Objekten entstanden sind, zusammengefaßt.

Lediglich eine Offline- Komprimierung der Datenbankdatei verkleinert diese wirklich. Hierzu sind folgende Schritte nötig:

1. Start im Modus „Verzeichnisdienstewiederherstellung“
2. Offline- Komprimierung der Datei NTDS.DIT in eine neue Datenbankdatei
   Dies wird durch das Tool NTDSUTIL über die Optionen „FILES => COMPACT TO filename.ext“ angestoßen und letztendlich durch das Programm ESENTUTIL durchgeführt (ESENTUTIL /d wird durch NTDSUTIL aufgerufen)
3. Manuelles Kopieren der neuen Datenbankdatei als NTDS.DIT über deren Original
4. Neustart des Servers

3.8 Typische AD- Fehler

Fehler	*Typische Ursache*
Hinzufügen oder Entfernen von Domänen ist nicht möglich	Der Domänennamenmaster ist nicht erreichbar
Erstellen von Active- Directory- Objekten ist nicht möglich	Der RID- Master ist nicht erreichbar
Bearbeiten des Active- Directory- Schemas ist nicht möglich	Der Schemamaster ist nicht erreichbar
Änderungen an Gruppenzugehörigkeiten werden nicht übernommen	Der Infrastrukturmaster ist nicht erreichbar
Computer ohne Active Directory Client können sich nicht an der Domäne anmelden	Der PDC- Emulator ist nicht erreichbar
Clients können nicht auf Resourcen in anderen Domänen zugreifen	Fehler in der Vertrauensstellungs- Konfiguration. MS- Empfehlung: Entfernen der entsprechenden Vertrauensstellung Erneutes Anlegen der Vertrauensstellung => hierzu muß der PDC-Emulator erreichbar sein !

3.9 Active-Directory- Dienstprogramme

3.9.1 NTDSUTIL

Das Active-Directory-Utility NTDSUTIL dient (unter anderem) dazu, folgende Funktionen an der AD-Datenbank durchzuführen:

- Autorisierende Wiederherstellung von Active-Directory-Objekten
- Offline- Komprimierung der AD-Datenbank (NTDS.DIT)
- Verschieben des Speicherortes der AD-Datenbank
- Entfernen ungültiger Serverobjekte aus der AD- Datenbank (=> Metadata Cleanup)
- Entfernen duplizierter SID's (=> security account management)
- Erstellung von Berichten über die Anzahl der aktuellen, gelöschten und Phantomdatensätze innerhalb der AD-Datenbank (=> semantic database analysis)
- Vorbereitungen für das Erstellen von Domänen (=> domain management)

3.9.2 CSVDE

Der Import und Export von Daten in das/aus dem Active Directory kann mit Hilfe von Dateien im CSV-Format (Comma-Separated Value) durchgeführt werden. Dieses Dateiformat wird von vielen Anwendungen unterstützt, u. a. von Microsoft Excel. Für die Durchführung von Importen und Exporten steht das Befehlszeilenprogramm CSVDE zur Verfügung.

3.9.3 LDIFDE

Mit dem Befehlszeilenprogramm LDIFDE können Verzeichnisobjekte erstellt, geändert und gelöscht werden. LDIF ist ein Industriestandard für ein Dateiformat, mit dem Stapelimport- und -exportoperationen für Verzeichnisse durchgeführt werden können. Mit diesem Tool sind auch Schemaänderungen möglich.

3.10 AD- Design

Nachfolgender Abschnitt dieser Dokumentation soll zum einen die Planungsschritte einer Active- Directory- Planung darstellen als auch eine Art Arbeitsunterlage für diese Tätigkeit sein.

3.10.1 Planung der Gesamtstruktur

Sind getrennte Domänenstrukturen nötig (mehrere Trees) ? ○ Ja ○ Nein

Ja, wenn ...
- Die Sicherheitsverwaltung von mehreren Gruppen durchgeführt wird, die einander nicht vertrauen
- Die Geschäftseinheiten aus firmenpolitischen Gründen voneinander getrennt bleiben sollen
- Die Geschäftseinheiten unterschiedliche Sicherheitsrichtlinien verwenden müssen
- Schema, Konfiguration oder globaler Katalog getrennt bleiben müssen
- Die Vertrauensstellungen zwischen den Domänen begrenzt werden müssen (keine Transitivität)

Sind mehrere Domänen innerhalb einer Struktur erforderlich ? ○ Ja ○ Nein

Ja, wenn ...
- Windows NT- Strukturen aus firmenpolitischen Gründen beibehalten werden sollen
- Unterschiedliche Kennwort-, Kontosperrungs- oder Kerberos- Richtlinien angewandt werden sollen
- Verwaltungsstrukturen aus Vorgaben in Domänen getrennt aufgebaut werden sollen

Sind Vertrauensstellungen notwendig ? ○ Ja ○ Nein
○ Einseitig ○ Zweiseitig

Ja, wenn ...
- Resourcensharing zwischen mehreren Domänen innerhalb unterschiedlicher Strukturen durchgeführt werden sollen

Ist eine Schemaänderung erforderlich ? ○ Ja ○ Nein

Ja, automatisch wenn zum Beispiel ...
- Exchange 2000 eingesetzt werden soll
- SAP in neueren Versionen eingesetzt werden soll
- Neueste MS-SQL- Funktionen eingesetzt werden sollen
- eine andere, Verzeichnisdienstfähige Anwendung (directory-enabled application) installiert wird

Kann ein Einheitlicher Modus verwendet werden ? ○ Ja ○ Nein

Ja, wenn ...
- kein älteres Client- oder Server-Betriebssystem eingesetzt werden soll
- kein NT- BDC mehr aus Sicherheitsgründen gehalten werden soll

Vorteile:
- kein reiner PDC-Emulator mehr (alle Domänencontroller können eine Anmeldebestätigung durchführen)
- Universelle Gruppen werden möglich

3.10.2 Planung der Domänen

Wie sollen die Domänen benannt werden:

1. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....
- Unterdomäne .....
- Unterdomäne .....

2. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....
- Unterdomäne .....
- Unterdomäne .....

3.10.3 Planung der Organisationseinheiten

Macht eine Untergliederung in Organisationseinheiten Sinn ? ○ Ja ○ Nein

Ja, wenn
- Unterschiedliche Richtlinien umgesetzt werden sollen (außer: Sicherheitsrichtlinien!)
- Verwaltungsaufgaben delegiert werden sollen
- Objekte verborgen werden sollen

Ist eine OU- Strukturierung nach Standorten sinnvoll ? ○ Ja ○ Nein

Ist eine OU- Strukturierung nach Geschäftsfunktionen sinnvoll ? ○ Ja ○ Nein

Ist eine OU- Strukturierung nach Objekttypen sinnvoll ? ○ Ja ○ Nein

Hint: Abarbeitungsreihenfolge von GPO's == Lokales GPO => Standort GPO => Domänen GPO => OU'-GPO's

Auflistung der OU- Hirarchie:

- Oberste OU- Ebene .....
- Weitere OU- Ebenen .....

.....

.....

.....

3.10.4 Planung der Standorttopologie

Sind getrennte Standorte zu definieren ? ○ Ja ○ Nein

Ja, wenn ...
- Die Netze nicht über Hochgeschwindigkeitsverbindungen verfügen (≥ 512 kBit/s)
- Die Verfügbarkeit der Netzverbindungen kleiner als 128 kBit/s ist

Welche Standorte sollen eingeführt und wie viele Server platziert werden:

1. Standort .....

Server innerhalb des Standortes:
- ☐ globaler Katalog
- ☐ Schemamaster (1x je Tree)
- ☐ Domänennm. (1x je Tree)
- ☐ RID-Master (1x je Dom.)
- ☐ PDC-Emulator (1x je Dom.)
- ☐ Infrastrukturm. (1x je Dom.)
- ☐ Bridgehead / Web /sonstige

2. Standort .....

Server innerhalb des Standortes:
- ☐ globaler Katalog
- ☐ Schemamaster (1x je Tree)
- ☐ Domänennm. (1x je Tree)
- ☐ RID-Master (1x je Dom.)
- ☐ PDC-Emulator (1x je Dom.)
- ☐ Infrastrukturm. (1x je Dom.)
- ☐ Bridgehead / Web /sonstige

3. Standort .....

Server innerhalb des Standortes:
- ☐ globaler Katalog
- ☐ Schemamaster (1x je Tree)
- ☐ Domänennm. (1x je Tree)
- ☐ RID-Master (1x je Dom.)
- ☐ PDC-Emulator (1x je Dom.)
- ☐ Infrastrukturm. (1x je Dom.)
- ☐ Bridgehead / Web /sonstige

4. Standort .....

Server innerhalb des Standortes:
- ☐ globaler Katalog
- ☐ Schemamaster (1x je Tree)
- ☐ Domänennm. (1x je Tree)
- ☐ RID-Master (1x je Dom.)
- ☐ PDC-Emulator (1x je Dom.)
- ☐ Infrastrukturm. (1x je Dom.)
- ☐ Bridgehead / Web /sonstige

3.10.5 DNS- Design

Sind bereits DNS- Server (intern) vorhanden ? ○ Ja ○ Nein

Müssen vorhandene DNS- Funktionen ein Update erfahren ? ○ Ja ○ Nein

Hint: Bind > 4.x ist erforderlich
Bind > 8.1.2 ist für Dynamisches DNS erforderlich

Vorhandene DNS-Struktur:

1. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

2. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

3. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

Neu zu schaffende DNS-Struktur:

1. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

2. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

3. Domänen-Root .....
- Unterdomäne .....
- Unterdomäne .....

4 RIS (Remote Installation Service)

Über RIS ist es möglich, einen Client über ein PXE (Pre- Boot Execution Enviroment)- Bootrom zu starten und eine Netzwerkinstallation des Betriebssystems eines Clients auszulösen.
Alternativ ist auch der Start über eine mittels rbfg.exe zu erstellenden Bootdiskette den Client zu starten, und über das Netzwerk die Remoteinstallation auszulösen.

4.1 Netzwerkanforderungen für RIS

- Im Netzwerk muß ein DHCP-Server für die Zuweisung von IP-Adressen für die RIS-Clients verfügbar sein
- Für die Namensauflösung muß im Netzwerk ein DNS-Server verfügbar sein
- Die Active-Directory-Dienste müssen im Netzwerk installiert sein

4.2 RIS- Serveranforderungen

Ein RIS-Server kann ein Member-Server innerhalb einer Active-Directory-Domäne oder ein Domänencontroller sein.
Ferner muß der RIS-Server im Bereich „DHCP“ der Active Directory Autorisiert sein.

4.3 Serverkomponenten den RIS- Dienstes

4.3.1 BINL (Boot Information Negotation Layer)

Der BINL- Dienst beantwortet die Netzwerkdienstanforderungen der RIS- Clients und dient zur Kommunikation zwischen RIS-Client und der Active Directory.

4.3.2 TFTPD (Trivial File Transfer Protocol Daemon)

Der Client erhält über TFTP bestimmte Dateien, z.B. den CIW [Client Installation Wizzard] und alle Client- Dialogfelder während der Installation.

4.3.3 SIS (Single Instance Store)

Der SIS- Dienst dient zur Verringerung des Speicherplatzbedarfes auf dem RIS- Server. So überprüft SIS, ob gegebenenfalls in Betriebssystemabbildern Dateien doppelt vorhanden sind, so dass jeweils nur eine Kopie der entsprechenden Dateien auf dem RIS- Datenträger abgespeichert wird.

4.4 RIS- Client- Anforderungen

- Der Client muß den Start von einem PXE-Start-ROM unterstützen.
- Die Netzwerkkarte im Client als primäres Startgerät festgelegt sein
- Alternativ kann der Client auch von einer Startdiskette (Erstellung mittels dem Programm Rbfg.exe im Ordner ..\admin\i386 des Remoteinstallationsverzeichnisses) starten

4.5 Anforderung an den RIS- User

- Der User muß über Leserechte auf den Installationspfad auf dem RIS-Server verfügen
- Der User muß für die Installation das Recht „Anmelden als Stapelverarbeitungsauftrag“ besitzen
  (=> Hinweis: Administratoren besitzen dieses Recht standardmäßig nicht)
- Dem User für die Installation muß – falls er den neu installierten Rechner zur Domäne hinzufügen können muß – das Recht zum Erstellen von Computerkonten in der Domäne eingeräumt werden.

4.6 Ablauf einer RIS- Installation

1. Der RIS- Client wird gestartet und initiiert einen DHCPREQUEST
   (in diesem DHCPREQUEST sendet der RIS-Client seine aus dem BIOS des Rechners erhaltene GUID mit, anhand der er eindeutig zu identifizieren ist).
2. Der RIS-Server verwendet den BINL-Dienst um innerhalb der Active Directory bereits ein Computerkonto mit der GUID des anfordernden PC's besteht.
3. Der RIS-Server läd über TFTP den Client Installation Wizzard (CIW) auf den Clientcomputer herunter – der Benuter wird aufgefordert, sich am Netzwerk anzumelden.
4. Der RIS-Server überprüft nun die Berechtigungen des Benutzers und stellt diesem anhand der Berechtigungen die Installationsabbilder zur Verfügung, welche im CIW zur Auswahl angeboten werden (sofern mehrere Abbilder zur Verfügung stehen).
   => Einstellung der Abbild-Berechtigung: Berechtigung der *.SIF-Dateien im Templates-Verzeichnis der Abbilder
5. Der CIW warnt den Benutzer, dass während der Installation alle Daten auf seiner Festplatte verloren gehen und startet nach einer Bestätigung den Installationsvorgang.

Da der Client Installation Wizzard innerhalb der PXE-Ebene ausgeführt wird, werden keine erweiterten Zeichen unterstützt. Daher sollten bei der Vergabe von Namen (Domänennamen, Benutzernamen u.s.w.) erweiterte Zeichen nur unter Vorbehalt verwendet werden.

4.7 RBFG- Bootdiskette für RIS (unterstützte Netzwerkkarten)

Nachfolgend eine (nicht vollständige) Liste von Netzwerkkarten, welche von einer durch das Dienstprogramm rbfg.exe erstellten Startdiskette unterstützt werden:

Hersteller	***Kartentypen***
3COM	3C900 (Combo & TP0), 3C900B (Combo, FL, TPC & TP0), 3C905 (T4 & TX), 3C905B (Combo, TX & FX), 3C905C (TX)
AMD	PCNet, Fast PCNet
Compaq	Netflex 100 (NetIntelligent II), Netflex 110 (NetIntelligent III), NetFlex 3
DEC	DE 450, DE 500
HP	Deskdirect 10/100 TX
Intel	Pro 10+, Pro 100+, Pro 100B, E100-Serie
SMC	SMC 8432, SMC 9332, SMC 9432

NICHT UNTERSTÜTZT WERDEN:

- ISA- Netzwerkkarten
- EISA- Netzwerkkarten
- MCA- Netzwerkkarten
- Token-Ring Netzwerkkarten

5 Gruppenrichtlinien

Gruppenrichtlinien stellen ein Leistungsstarkes Instrument zur Computer- und Benutzerverwaltung innerhalb der Active Directory dar.
GPO = Group Policy Object = Gruppenrichtlinienobjekt

5.1 Allgemeines

Windows 2000 unterstützt mehrere Ebenen von Benuter- und Gruppenrichtlinien

- Lokales GPO (⇒ 5.1.1 - Lokales Gruppenrichtlinienobjekt)
- Standort GPO's (⇒ 5.1.2 - Standort- Gruppenrichtlinienobjekt)
- Domänen GPO's (⇒ 5.1.3 - Domänen- Gruppenrichtlinienobjekt)
- OU- GPO's (5.1.4 - Organisationseinheiten- Gruppenrichtlinienobjekt)

Diese Gruppenrichtlinienobjekte werden hirarchisch in der vorgenannten Reihenfolge abgearbeitet.

5.1.1 Lokales Gruppenrichtlinienobjekt

Jeder Windows 2000 Computer verfügt über genau ein lokales Gruppenrichtlinienobjekt

5.1.2 Standort- Gruppenrichtlinienobjekte

Diese Gruppenrichtlinienobjekte sind direkt mit dem Standort verknüpft und werden auf alle Objekte innerhalb des entsprechenden Standort angewendet. Mehrere GPO's werden nach einer durch den Administrator vorgegebenen Verarbeitungsreihenfolge abgearbeitet.

5.1.3 Domänen- Gruppenrichtlinienobjekte

Diese Gruppenrichtlinienobjekte sind direkt mit der Domäne verknüpft. Auch bei diesen GPO's bestimmt der Administrator die Verarbeitungsreihenfolge und auch diese GPO's werden auf alle Objekte – jedoch innerhalb einer Domäne – angewandt.

5.1.4 Organisationseinheiten- Gruppenrichtlinienobjekte

Diese Gruppenrichtlinienobjekte sind mit den jeweiligen Organisationeinheiten verknüpft und werden auf alle Objekte unterhalb der entsprechenden OU angewand. Bei mehreren OU- Ebenen werden die GPO's der übergeordneten OU vor denen der untergeordneten OU angewandt. Bei mehreren GPO's innerhalb einer OU wird die Verarbeitungsreihenfolge durch den Administrator festgelegt.

5.2 GPO-Verarbeitungsreihenfolge innerhalb der Objekthirarchie

- Vor der Anmeldung werden GPO's von Computerobjekten angewandt
- Nach der Anmeldung werden GPO's von Benutzerobjekten Angewandt

5.3 GPO-Vererbungslehre innerhalb der Domänenhirarchie

1. Das lokale Gruppenrichtlinienobjekt wird angewandt
2. Das Standort Gruppenrichtlinienobjekt wird angewandt und es werden gegebenenfalls Einstellungen des
   - lokalen Gruppenrichtlinienobjektes
   überschrieben
3. Das Domänen- Gruppenrichtlinienobjekt wird angewandt und gegebenenfalls werden Einstellungen des
   - Standort- Gruppenrichtlinienobjektes und des
   - lokalen Gruppenrichtlinienobjektes
   überschrieben
4. Das Gruppenrichtlinienobjekt der Organisationseinheit (OU), die sich am nächsten auf dem Domänenroot befindet, wird angewandt und es werden gegebenenfalls Einstellungen des
   - Domänen- Gruppenrichtlinienobjektes, des
   - Standort- Gruppenrichtlinienobjektes und des
   - lokalen Gruppenrichtlinienobjektes
   überschrieben
5. Das Gruppenrichtlinienobjekt der ersten Organisationseinheit (OU) unterhalb der vorgenannten Organisationseinheit (OU) wird angewandt und gegebenenfalls werden Einstellung des Gruppenrichtlinienobjektes der
   - vorherigen Organisationseinheit (OU), des Gruppenrichtlinienobjektes der
   - Domäne, des Gruppenrichtlinienobjektes des
   - Standortes und des
   - lokalen Gruppenrichtlinienobjektes
   überschrieben
6. Ebene - dementsprechend in den weiter untergeordneten Organisationseinheiten weiter ....

5.4 Beispielhafte Gruppenrichtlinie mit nur 6 Einstellungen

Die Einstellung „Nix“ bedeutet, das diese Einstellung innerhalb des Gruppenrichtlinienobjektes nicht wurde, die Beeinflussungen innerhalb der Vererbung sind grau hinterlegt ...

Objektebene	Richtlinie der Ebene							Resultierende Richtlinie					
	Pos 1	Pos 2	Pos 3	Pos 4	Pos 5	Pos 6		Pos 1	Pos 2	Pos 3	Pos 4	Pos 5	Pos 6
Lokal	Nix	Ja	Nein	Ja	Nix	Nix		Nix	Ja	Nein	Ja	Nix	Nix
Standort	Nix	Nix	Ja	Nix	Ja	Nix		Nix	Ja	Ja	Ja	Ja	Nix
Domäne	Nix	Ja	Nix	Nix	Nix	Nein		Nix	Ja	Ja	Ja	Ja	Nein
1. OU	Ja	Nein	Nix	Nein	Ja	Ja		Ja	Nein	Ja	Nein	Ja	Ja
2. OU	Nix	Nein	Nix	Ja	Nein	Nix		Ja	Nein	Ja	Ja	Nein	Ja
3. OU	Nix	Nix	Nix	Nix	Nix	Nix		Ja	Nein	Ja	Ja	Nein	Ja

5.5 Beeinflussung der Gruppenrichtlinienvererbung

5.5.1 Kein Vorrang

7. Durch die Einstellung der Option "kein Vorrang" kann kein nachrangiges Gruppenrichtlinienobjekt einer niedrigeren Ebene Einstellungen des auf "kein Vorrang" gesetzten Gruppenrichtlinienobjektes überschreiben. Im Vererbungsbeispiel in dieser Dokumentation (Kapitel 6, anisationseinheiten weiter ....

Beispielhafte Gruppenrichtlinie mit nur 6 Einstellungen) würde ein auf "kein Vorrang" gesetztes Domänen-Gruppenrichtlinienobjekt in der ersten OU das Ergebnis „Ja-Ja-Ja-Nein-Ja-Nein“ ergeben.

5.5.2 Richlinienvererbung

Die Vererbung von Gruppenrichtlinienobjekte auf untergeordnete Objekte kann deaktiviert werden. Auf "kein Vorrang" gesetzte Gruppenrichtlinienobjekte können in Bezug auf die Vererbung nicht deaktiviert werden.

5.5.3 Loopbackverarbeitung von Gruppenrichtlinienobjekten

Wird in einer Richtlinie die Loopbackverarbeitung aktiviert, so wird eine eventuell auf das Benutzerobjekt zutreffende Richtlinie ersetzt bzw. vermischt. Für die Loopbackverarbeitung gibt es die beiden Modi Ersetzen und Zusammenführen.

5.5.3.1 Beispiele für die Loopbackverarbeitung

- Das Gruppenrichtlinienobjekt der Organisationseinheit des Users besagt, dass der User die Auflösung ändern darf
- Das Gruppenrichtlinienobjekt der Organisationseinheit des Computers besagt, dass der User die Auflösung nicht ändern darf
    - Bei aktivierter Loopbackverarbeitung im Modus "Zusammenführen" hat die Gruppenrichtlinie des Computerobjektes Vorrang, also darf der Benutzer die Auflösung nicht ändern
    - Bei aktivierter Loopbackverarbeitung im Modus "Ersetzen" ersetzt die Einstellung der Gruppenrichtlinie des Computerobjektes die Einstellungen aus der Gruppenrichtlinie des Benutzers – folglich darf auch in dieser Variante dieses Beispieles der Benutzer die Auflösung nicht ändern
    - Bei deaktivierter Loopbackverarbeitung ersetzt die zu einem späteren Zeitpunkt greifende Gruppenrichtlinie des Benutzerobjektes die Einschränkung aus der Gruppenrichtlinie des Computerobjektes – folglich darf der Benutzer die Auflösung nun ändern.

5.5.4 Deaktivieren von Teilen von Gruppenrichtlinien

Auf dem Stamm einer Gruppenrichtlinie kann unter Eigenschaften des Gruppenrichtlinienobjektes die Computer- bzw. die Benutzerkonfiguration deaktiviert werden. Hierdurch werden zum einen alle entsprechenden Einstellungen innerhalb der Richtlinie außer Kraft gesetzt, zum anderen muß der entsprechende Zweig der Richtlinie nicht mehr abgearbeitet werden, so daß die Verarbeitungsgeschwindigkeit der entsprechenden Gruppenrichtlinie verkürzt und die Anmeldung beschleunigt wird.

5.5.5 Einschränken der Verarbeitung einer Gruppenrichtlinie

Durch die Sicherheitseinstellung "Lesen" (Zulassen oder Verweigern) kann festgelegt werden, auf welche Benutzer, Computer oder sonstige Objekte eine Gruppenrichtlinie angewandt werden soll.
Ein Gruppenrichtlinienobjekt, das nicht gelesen werden kann, kann auch nicht berücksichtigt werden...
Ebenso kann mit dem Recht "Gruppenrichtlinie übernehmen" festgelegt werden, ob eine Richtlinie für einen Benutzer/Eine Gruppe/Einen Computer/…. angewandt werden soll.

5.5.6 Softwareverteilung über Gruppenrichtlinien

Verteilbar sind Softwarepakete, die über Installerdateien mit den Endungen

*5.5.6.1 *.MSI (Windows Installer)*

Installerpakete können „veröffentlicht“ oder „zugewiesen“ werden.

*5.5.6.2 *.ZAP (Zero Administration Pack, Installations- Anwendungen)*

Zero Administration Packs können nur veröffentlicht werden.

*5.5.6.3 *.MST (Windows- Installer Veränderungspakete)*

Eine .mst-Datei kann zusammen mit der dazugehörigen .msi-Datei eingesetzt werden. In dieser Datei wird festgelegt, welche Teile des Paketes installiert werden sollen.

*5.5.6.4 *.MSP (Patchdateien)*

Softwareentwickler können Änderungen an der Software in Form einer .msp-Datei zur Verfügung stellen. Mit Hilfe dieser Datei wird die ursprüngliche .msi-Datei aktualisiert und danach erneut veröffentlicht oder zugewiesen.

*5.5.6.5 *.AAS (Application Assignment Scripts)*

5.5.7 Zuweisen von Software

Eine Zuweisung von Software installiert eine Software noch nicht direkt.
Erst durch einen Aufruf der Software wird die Installation initiiert. Eine Zugewiesene Software begleitet einen Anwender von PC zu PC. Ferner wird die Software durch Aufruf einer mit der Software verknüpften Dateiendung oder durch Auswahl eines entsprechend durch die Zuweisung im Startmenü installierten Links automatisch installiert.
Zugewiesene Softwarepakete werden bei Fehlern durch den Windows Installerdienst automatisch repariert.

5.5.8 Veröffentlichen von Anwendungen

Veröffentliche Software steht dem Anwender unter Systemsteuerung => Software => "Im Netzwerk zur Verfügung gestellte Software" zur Installation zur Verfügung. Sie wird erst durch entsprechenden Aufruf bzw. durch Anwahl einer mit der entsprechenden Software verknüpften Dateierweiterung installiert

6 Nützliche Tips und Tricks

6.1 Der externe Befehl AT.EXE

Mit dem Befehl AT können Befehle und Programme zu einem vorbestimmten Termin gestartet werden. Der Zeitplandienst muss gestartet sein, um den Befehl AT zu verwenden.

AT [\\Computername] [[Kennung] [/DELETE] | /DELETE [/YES]]
AT [\\Computername] Zeit [/INTERACTIVE] [/EVERY:Datum[,...] | /NEXT:Datum[,...]] "Befehl"

\\Computername
Gibt einen Remotecomputer an. Ohne diesen Parameter werden die Befehle auf dem lokalen Computer ausgeführt.

Kennung
Eine Identifikationsnummer, die dem geplanten Befehl zugeteilt wird.

/DELETE
Löscht geplante Befehle. Ohne Kennung werden alle geplanten Befehle auf dem Computer gelöscht.

/YES
In Verbindung mit /DELETE werden die geplanten Befehle ohne weitere Bestätigung gelöscht.

Zeit
Gibt die Zeit an, zu der ein Befehl ausgeführt werden soll.

/INTERACTIVE
Ermöglicht dem Auftrag, Eingaben von dem Benutzer anzunehmen, der angemeldet ist, wenn der Auftrag ausgeführt wird.

/EVERY:Datum[,...]
Führt den Befehl zu jedem der angegebenen Tage der Woche oder des Monats aus. Ohne Angabe eines Datums wird der aktuelle Tag des Monats angenommen.

/NEXT:Datum[,...]
Führt den Befehl am nächsten angegebenen Tag aus (z.B. nächsten Montag). Ohne Angabe eines Datums wird der aktuelle Tag des Monats angenommen.

"Befehl"
Ist der auszuführende Windows NT-Befehl oder Stapelprogramm.

6.2 Das Programm RUNAS.EXE

Ermöglicht dem Benutzer das Ausführen spezieller Tools und Programme mit anderen Berechtigungen als es die gegenwärtige Anmeldung erlaubt. Es empfiehlt sich für Administratoren, für nicht administrative Routineaufgaben ein Konto mit eingeschränkten Berechtigungen zu verwenden und nur zur Durchführung spezieller administrativer Aufgaben auf ein Konto mit weit gefassteren Berechtigungen zurückzugreifen. Um diese wechselnden Aufgaben ohne ständiges Ab- und Anmelden durchführen zu können, sollten Sie sich unter einem gültigen Benutzerkennwort anmelden und mit Hilfe des Befehls runas die Tools ausführen , für die weit gefasstere Berechtigungen erforderlich sind.

runas [**/profile**] [**/env**] [**/netonly**] **/user:***Benutzerkontoname* **program**

/profile
Gibt den Namen des zu verwendenden Benutzerprofils an, falls dies noch geladen werden muss.

/env
Gibt an, dass anstelle der lokalen Umgebung des Benutzers die aktuelle Netzwerkumgebung verwendet werden soll.

/netonly
Zeigt an, dass die angegebenen Benutzerinformationen nur für Remotezugiff geeignet sind.

/user:Benutzerkontoname
Gibt den Namen des Benutzerkontos an, unter dem das Programm ausgeführt werden soll. Das Benutzerkonto sollte im Format *Benutzer@Domäne* bzw. *Domäne\Benutzer* angegeben werden.

program
Gibt das Programm bzw. den Befehl an, das/der unter dem über **/user** festgelegten Benutzerkonto ausgeführt werden soll.

7 Index

A

AAS ... 63
Active Directory Schema ... 43
Anmeldescripts ... 36
APIPA ... 14, 20
ARP ... 15, 23
AT.EXE ... 64
Automatic Private IP Adressing ... 20
AXFR ... 25, 26

B

BACP ... 40
Bandwith Allocation Control Protocol ... 40
Bandwith Allocation Protocol ... 40
BAP ... 40
BIND ... 26
BINL ... 56, 57
B-Knoten ... 21, 29
Boot Information Negotation Layer ... 56

C

Challenge Handshake Authentication Protocol ... 10, 40
CHAP ... 10, 40
CIDR ... 15
Classless Inter Domain Routing ... 15
CSVDE ... 51

D

DCPROMO.EXE ... 41
Directory Information Tree ... 42
directory-enabled application ... 52
DNS ... 18, 20, 21, 22, 23, 24, 25, 26, 36, 37, 55, 56
Domain Naming System ... 18, 24
Domänennamenmaster ... 43, 44, 50
dynamische Aktualisierung ... 26

E

EAP ... 10, 40
Ethernet SNAP ... 8
Extensible Authentication Protocol ... 40

F

File Transfer Protocol ... 15, 18
Finger ... 18
FTP ... 15, 18

G

Globaler Katalog 44
GPO 53, 58, 59
Gruppenrichtlinie 60, 62
Gruppenrichtlinienobjekt 58, 59, 61, 62
Gruppenrichtlinienobjekte 58, 62

H

H-Knoten 21, 29
Hostname 17, 21, 25
HTTP 15, 18
HTTPS 18

I

ICMP 13, 16
Infrastrukturmaster 43, 44, 50
inkrementelle Zonenübertragung 26
Internet Control Message Protocol 13, 16
Internet Group Management Protocol 16
Internet Protocol 9, 14, 16
Internet Protocol Security 14
IP 8, 9, 10, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 27, 33, 37, 56, 71
Ipconfig 17
IPSec 14
IPSECMON 14
IP-Security 14
Ipxroute 19
IXFR 25, 26

J

JETPACK.EXE 21, 28

L

L2TP 40
Layer-2-Tunnelingprotocol 40
LCP 16
LDIFDE 51
Link Control Protocol 16
Loopback 14

M

Metadata Cleanup 51
Microsoft Challenge Handshake Authentication Protocol 40
M-Knoten 21, 29
MMC 14, 20, 28, 43, 45, 46
MS-CHAP 10, 40
MSI 63
MSP 63
MST 63

N

NAT 37
NBT 16, 17, 21, 33
Nbtstat 17
Netbios over TCP/IP 16
NETDOM.EXE 46
Netstat 17
Network File System 16
Network News Transfer Protocol 15
New Technologie Directory System 42
NFS 16
NNTP 15
NSLOOKUP 25
NTDS.DIT 47, 49, 51
NTDSUTIL.EXE 42, 48

O

Open Shortest Path First 16
OSPF 16

P

PAP 10, 40
PathPing 18
PDC-Emulator 43, 44, 50, 52, 54
Ping 15, 21
Point-to-Point Tunneling Protocol 40
POP 16, 18
Post Office Protocol 16, 18
PPTP 40
Pre- Boot Execution Enviroment 56
PXE 56, 57

R

RADIUS 40
rbfg.exe 56, 57
Rcp 18
REGEDIT.EXE 39
REGEDT32.EXE 39
Remote Authentication Dial-in User Service 40
Remote Installation Service 56
REPLMON 46
REPLMON.EXE 46
Rexec 18
RID-Master 43, 44, 54
RIP 16
RIS 56, 57
RIS-Server 56, 57
Route 17
Router Information Protocol 16
Rsh 18
RUNAS.EXE 65

S

Schema 43, 52
schmmgmt.msc 43
Shiva Password Authentication Protocol 40
Simple Mail Transfer Protocol 15, 18
Simple Network Management Protocol 16
Single Instance Store 56
SIS 56
SMTP 15, 18
SNMP 16
SPAP 10, 40
Systempartition 32

T

TCP 9, 13, 15, 16, 17, 18, 22, 25, 27, 33, 71
tFtp 15
TFTPD 56
Transmission Control Protocol 9, 13, 16
Trivial File Transfer Protocol Daemon 56

U

UDP 13, 16, 20, 27
User Datagram Protocol 13, 16

V

Veröffentlichen 25, 63
Verzeichnisdienstfähige Anwendung 52
Vollständige Zonenübertragung 26

W

Windows 2000 Support-Tools 46
WINS 21, 23, 27, 28, 29

Z

ZAP 63
Zuweisen 63

8 Anhang

8.1 Hilfen zum ISO/OSI Referenzmodell

	Hilfe	*Engl. Name*	*Deutscher Name*	*NT-Architektur*	*Softwarekomponenten und Protokolle*	*Aufgabe bzw. Funktion*	*Geräte- Beispiele*
Layer 7	**A**ll	**A**pplication Layer	Anwendungsschicht	Dateisystem- Treiber	Serverdienst, Arbeitsstationsdienst	Veranlasst bzw. übernimmt eine Anfrage	
Layer 6	**P**eople	**P**resentation Layer	Darstellungsschicht		NTFS- und FAT-Dateisystemtreiber	Fügt dem Paket Formatierungs-, Darstellungs- und Verschlüsselungsinformationen hinzu	
Layer 5	**S**eems	**S**ession Layer	Kommunikationsschicht			Fügt Verkehrsflussinformationen hinzu und bestimmt, wann das Paket gesendet wird	
Layer 4	**T**o	**T**ransport Layer	Transportschicht	Transport-Protokolle	NetBEUI, NWLink, TCP/IP und DLC	Fügt Informationen zur Fehlerbehandlung hinzu	
Layer 3	**N**eed	**N**etwork Layer	Vermittlungsschicht			Fügt Informationen über Reihenfolge und Adressen hinzu	Router, Switches
Layer 2	**D**ata	**D**ata Link Layer	Sicherungsschicht	Netzwerkkarten-Treiber	NDIS-Wrapper und –Treiber Netzwerkschnittellenkarte (Ethernet, Token Ring, ARCnet, FDDI)	Fügt Fehlerkorrekturdaten hinzu und bereitet die Daten für die Übertragung auf dem Monitor vor	Hubs, Bridges
Layer 1	**P**rocessing	**P**hysical Layer	Bitübertragungsschicht			Paket wird als Bitstrom übertragen	Repeater