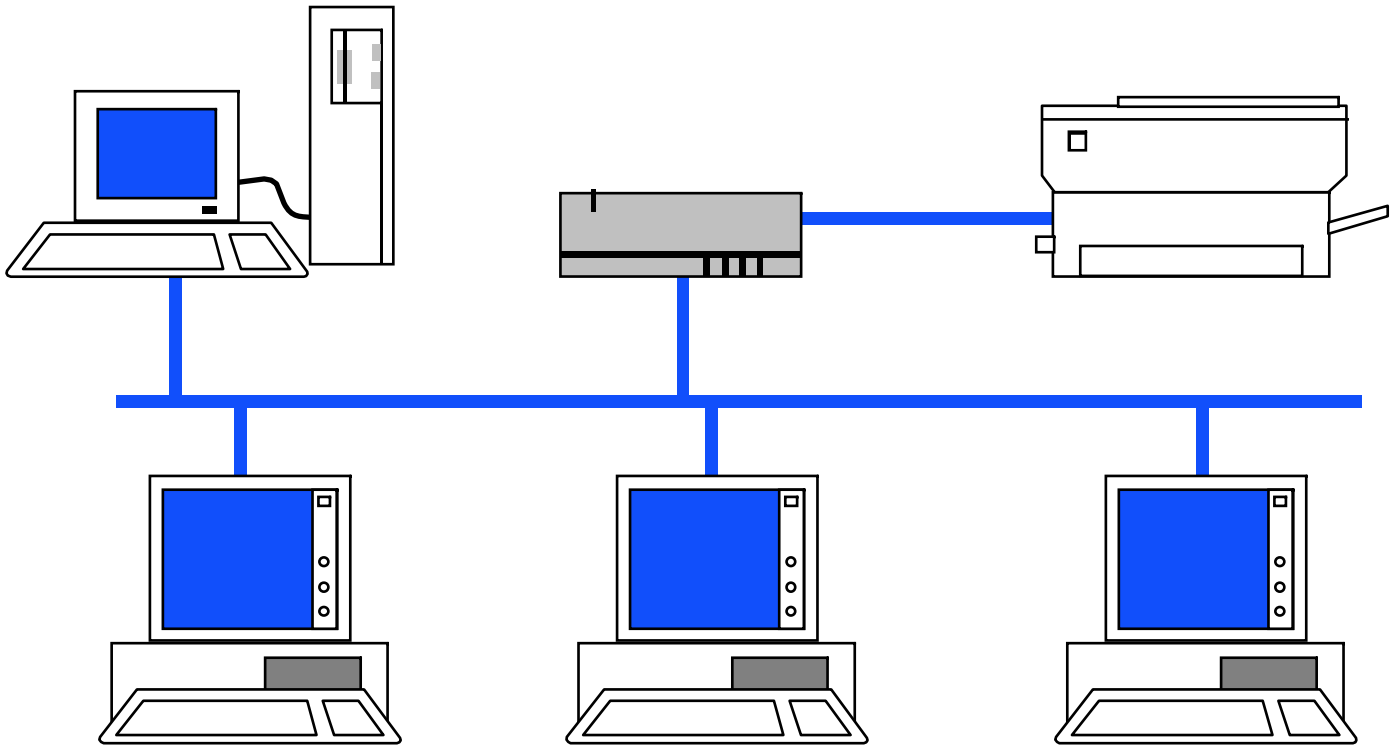
NSYS Teil 1a

Mag. Dr. Klaus Coufal



Übersicht

- I. Allgemeines
- II. LAN
- III. WAN
- IV. Spezielle Architekturen (Netzwerkmodelle)
- V. Aktuelles

I. Allgemeines

1. Abgrenzung
2. Komponenten
3. Ziele von Netzwerken (->Forderungen)
4. Referenzmodelle ISO/OSI, TCP/IP, ...
5. Übertragungsverfahren
6. Vermittlungsverfahren
7. Topologien

I.1. Abgrenzung

Typ	Bandbreite	Entfernung
MP	>1 GB/s	<1m
LAN	10 M .. 1 GB/s	1m .. 1km
WAN	<10 M/s (auch GB/s möglich)	>1km

I.2. Komponenten

- Hochleistungskommunikationsmedium
- Netzwerkadapter
- Rechensystemkomponenten

I.3. Ziele von Netzwerken

- Datenverbund
- Funktionsverbund
- Verfügbarkeitsverbund
- Leistungsverbund
- Lastverbund

Datenverbund

Zugriff auf räumlich getrennte Datenbestände, dazu gehören:

- Zentrale Datenbanken
- Zentrale Applikationen
- Dateitransfer
- Nachrichtenaustausch
- ...

Funktionsverbund

Zugriff auf Funktionen, über die der momentan genutzte Computer nicht verfügt, z.B.:

- Drucker
- Meßeinrichtungen
- Sensoren und Aktuatoren
- ....

Verfügbarkeitsverbund

Zugriff auf andere Computersysteme zur Erhöhung der Verfügbarkeit, z.B.:

- Clustersysteme (Zusammenschaltung mehrerer Server zur Verbesserung der Ausfallssicherheit)
- Wechseln auf eine andere Arbeitsstation, um dort die eigene Arbeit abzuschliessen
- ...

Leistungsverbund

Zusammenschalten mehrerer Systeme zur Erhöhung der Gesamtleistung, z.B.:

- Distributed Computing (Zerlegung einer Aufgabe in mehrer kleinere Aufgaben, die dann parallel von mehreren/vielen Computern erledigt werden)
- Clustertechnik
- ...

Lastverbund

Ausweichen bei momentaner Überbelastung des eigenen Systems auf andere Systeme mit weniger Belastung, z.B.:

- Resourcensharing nach Zeitschema
- Ausweichen auf Alternativsystem in Spitzenzeiten
- ...

Forderungen an Netzwerke

- Hohe Bandbreite des Übertragungsmediums
- Geeignete Topologie
- Geeignete Protokolle
- Geeignete funktionale und prozedurale Hilfsmittel
- Hohe Verfügbarkeit
- Offene Systemarchitektur

I.4. Referenzmodelle

- ISO-Referenzmodell OSI
- TCP/IP-Referenzmodell
- Novell-Referenzmodell
- ...

ISO-Referenzmodell

Anwendung	
7	**Application Layer (Anwendungsschicht)**
6	**Presentation Layer (Präsentationsschicht)**
5	**Session Layer (Sitzungsschicht)**
4	**Transport Layer (Transportschicht)**
3	**Network Layer (Netzwerkschicht)**
2	**Data Link Layer (Datensicherungsschicht)**
1	**Physical Layer (Physikalische Schicht)**
Übertragungsmedium (Kabel, Funk, LWL, ...)	

Physical layer

- ISO Schicht 1
- Kabel- und Steckerspezifikationen
- Übertragungstechnologie
- Spezifikation der Signalpegel
- Unstrukturierter Bitstrom
- z.B.: X.21, V.24, Ethernet Hardwareteil
- Geräte: Repeater, Hub

Data Link layer

- ISO Schicht 2
- HW-Adressierung, Frameformat
- Flußkontrolle und Fehlerprüfung zwischen nächsten Nachbarn
- Rahmen (Frames)
- z.B.: HDLC, Ethernet MAC und LLC
- Geräte: Bridge, Switch

Network layer

- ISO Schicht 3
- Logische Adressierung
- Wegewahl und Routing
- Auf- und Abbau von Netzverbindungen
- Pakete (Packets)
- z.B.: X.25, IP, IPX
- Geräte: Router

Transport layer

- ISO Schicht 4
- Ende zu Ende Flußkontrolle
- Ende zu Ende Fehlerprüfung
- Sequencing
- Fragemente, Pakete (Packets)
- z.B.: TCP, SPX
- Geräte: Gateway

Session layer

- ISO Schicht 5
- Passwortkontrolle
- Gebührenabrechnung
- Auf- und Abbau einer Sitzung
- Verbindungswiederaufbau
- Kaum Standards
- Geräte: Access Controller

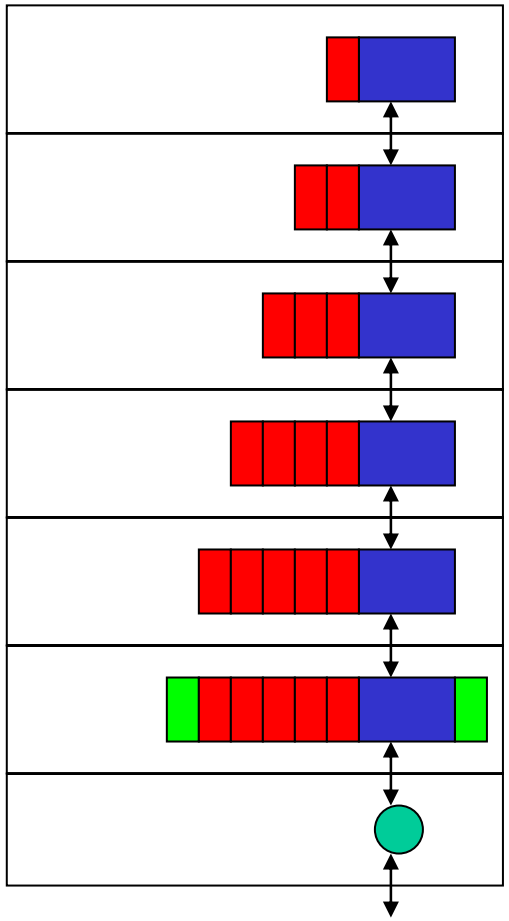
Presentation layer

- ISO Schicht 6
- Vereinbarung über Kodierung (Zahlendarstellung, Dateiformate, ...)
- Formatumwandlung
- Codeumwandlung
- z.B.: ASCII $\leftrightarrow$ EBCDIC

Application layer

- ISO Schicht 7
- APIs (Application Programming Interface) für die Anwendungen
- Standarddienste (Dateitransfer, Virtuelles Terminal, ...)
- z.B.: Sockets, FTAM, X.400, X.500

Schichtenkommunikation



Applikationsschicht

Präsentationsschicht

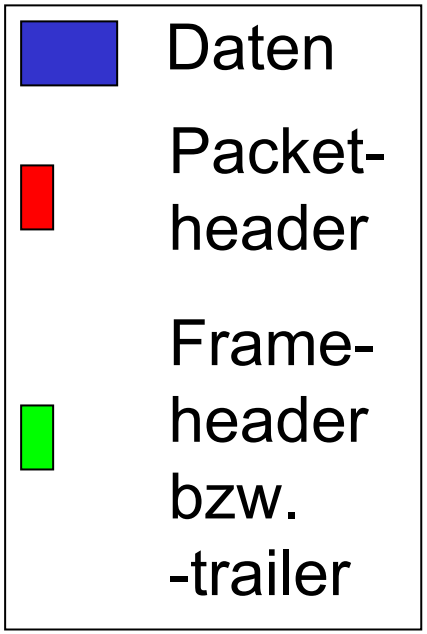
Sitzungsschicht

Transportschicht

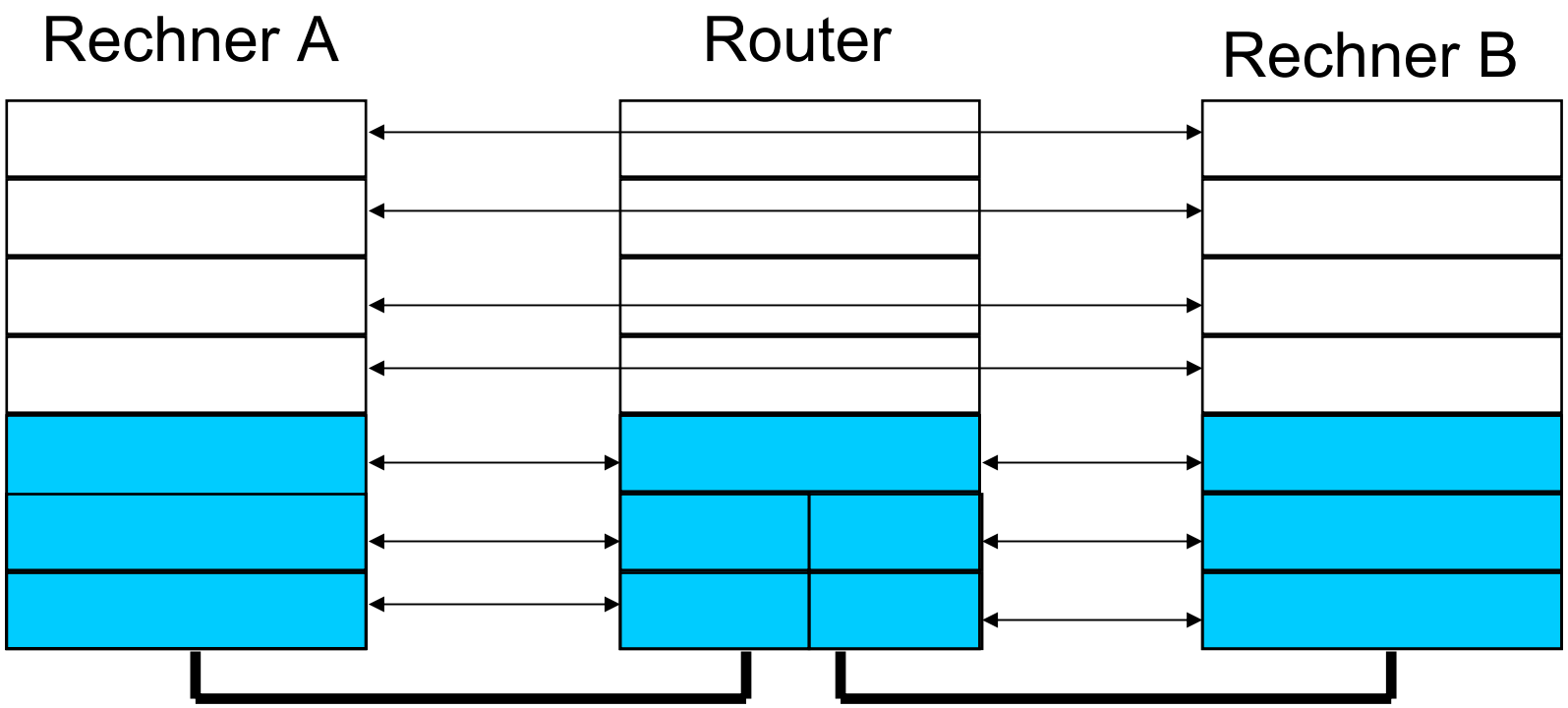
Netzwerkschicht

Datenverbindungsschicht

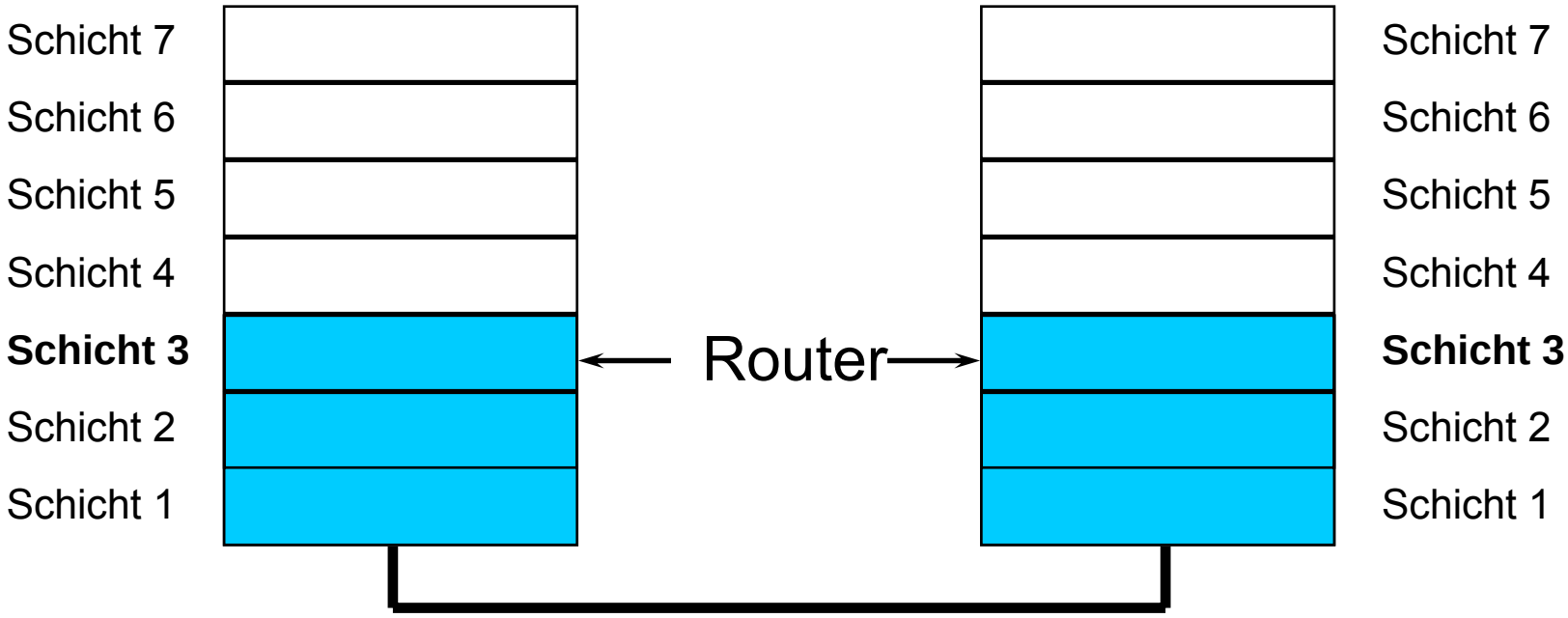
Physikalische Schicht



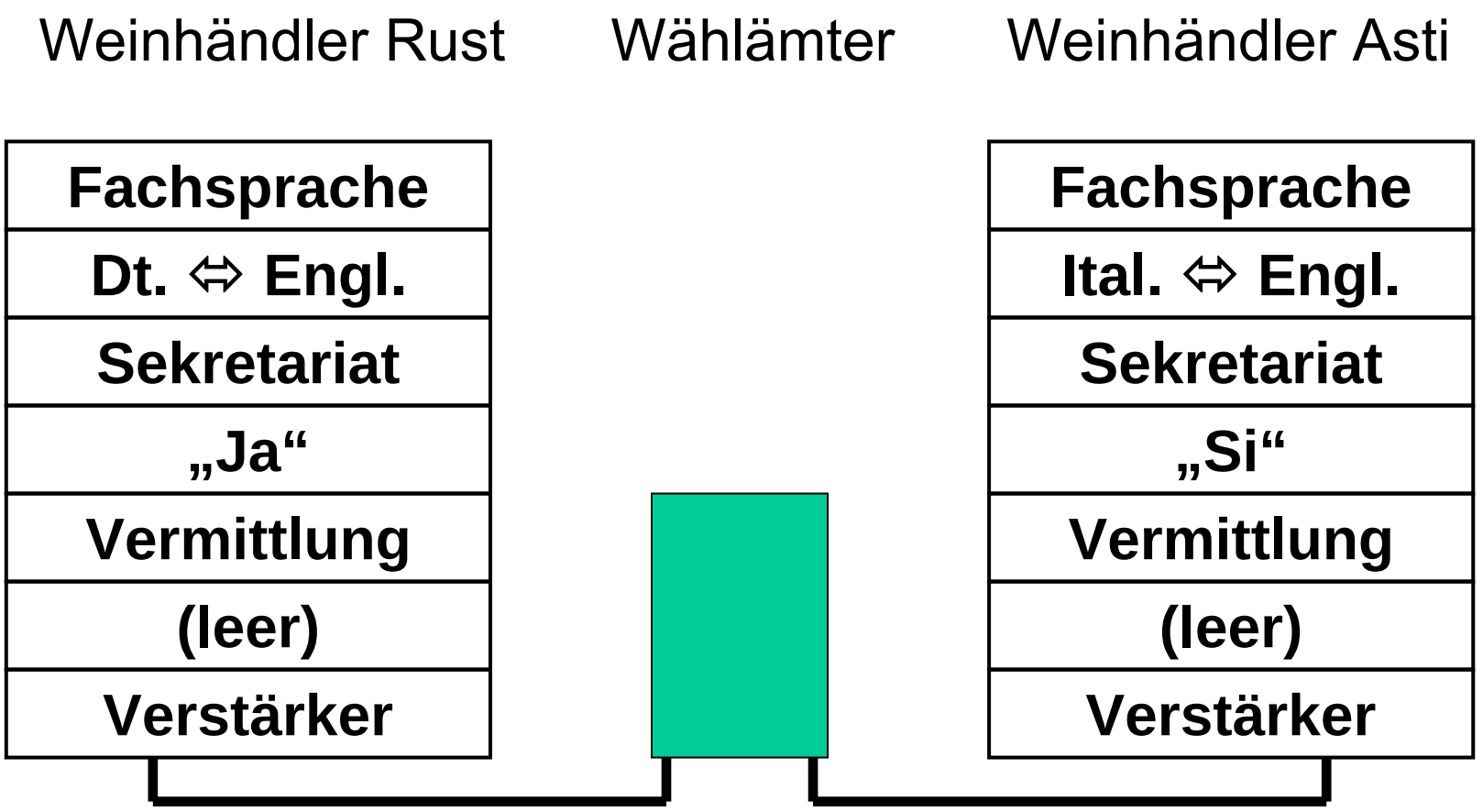
Kommunikation über Router



Schichtenmodell am Beispiel Router



Beispiel


Weinhändler Rust
Wählämter
Weinhändler Asti
Fachsprache
Dt. ⇔ Engl.
Sekretariat
„Ja“
Vermittlung
(leer)
Verstärker
Fachsprache
Ital. ⇔ Engl.
Sekretariat
„Si“
Vermittlung
(leer)
Verstärker

TCP/IP-Referenzmodell

OSI	Anwendung	TCP/IP	
7	Application Layer	4	Application
6	Presentation Layer		
5	Session Layer		
4	Transport Layer	3	Transport
3	Network Layer	2	Internet
2	Data Link Layer	1	Host to Net
1	Physical Layer		
Übertragungsmedium (Kabel, Funk, LWL, ...)			

Novell-Referenzmodell

OSI	Anwendung	Novell	
7	Application Layer	5	Application Layer
6	Presentation Layer		
5	Session Layer		
4	Transport Layer	4	Transport Layer
3	Network Layer	3	Network Layer
2	Data Link Layer	2	Data Link Layer
1	Physical Layer	1	Physical Layer
Übertragungsmedium (Kabel, Funk, LWL, ...)			

I.5. Übertragungsverfahren

- Allgemeines
- Übertragung auf metallischen Leitern
  - Niederfrequenzkabel
  - Hochfrequenzkabel
  - Basisbandübertragungsverfahren
  - Breitbandübertragungsverfahren
- Übertragung auf Lichtwellenleitern
- Übertragung mit Hilfe von Funk

I.5.1. Allgemeines

- Übertragungsart
  - Parallel
  - Seriell
- Übertragungsrichtung
  - Simplex
  - Halfduplex
  - Fullduplex

Allgemeines – 2

- Codierung
- Wandler: Information -> Übertragsmedium
  - ohmsche Anpassung
  - Modulation
  - Multiplex (Kanal)
- Informationsgehalt
- Medienkapazität vs. Dichte der Folge
- Dämpfung

I.5.1.1. Codierung

Die **Codierung** beschreibt die physikalische Darstellung der Information (Bitfolge, Bitstrom; unabhängig vom Aufbau)

- Lichtimpulse
- Spannungen
- Elektromagnetische Wellen
- ....

I.5.1.2. Wandler

Ein Wandler ist für die Umsetzung der Codierung in Hinblick auf das verwendete Übertragungsmedium verantwortlich:

- ohmsche Anpassung (einfache Anpassung, z.b: Ausgabe einer Spannung)
- Modulation
- Multiplex

Modulation

Dabei wird eine Trägerfrequenz, die etwa in der Mitte des zur Verfügung stehenden Frequenzbandes liegt, so verändert, dass der Empfänger aus der Art der Veränderung eineindeutige Rückschlüsse auf die originale Information ziehen kann (Demodulation).

Modulationsprodukt = Ergebnis d. Mod.

Multiplex

Bündelung von mehreren Informations-folgen zu einer dichteren Folge:

- Jede Informationsfolge hat ihren eigenen Kanal
- Mehrere Multiplexarten:
  - Zeitmultiplex
  - Frequenzmultiplex
  - ...

I.5.1.3. Informationsgehalt

Der Informationsgehalt beschreibt die verwertbare Information in einer Folge von Übertragungsmustern. In der Netzwerktechnik üblicherweise in Bit (Kbit, Mbit, ...) oder Byte (Kbyte, Mbyte, ...) angegeben.

I.5.1.4. Bandbreite ⇔ Dichte

- Kapazität des Mediums (Bandbreite) angegeben in Hz
- Dichte der Folge angegeben in Bit/s (Bd)
- Der Zusammenhang ist linear:

$$f[Hz] = K * C[Bit/s]$$

I.5.1.5. Dämpfung

Die Dämpfung ist ein wichtiges Maß zur Beschreibung der Übertragungsgüte.

Definitionen:

$$D[db] := 20 \bullet \lg\left(\frac{U_{Eingang}}{U_{Ausgang}}\right) \qquad D[db] := 10 \bullet \lg\left(\frac{P_{Eingang}}{P_{Ausgang}}\right)$$

Bei Kabeln wird sie üblicherweise in db pro 100m angegeben.

I.5.2. Metallische Leiter

In LAN-Bereich werden am häufigsten metallische Leiter (i.A. Kupferkabel) zur Informationsübertragung verwendet. Dabei werden Nieder- und Hochfrequenzkabel unterschieden, die „Trennfrequenz“ liegt bei ca. 1MHz

I.5.2.1. Niederfrequenzkabel

- Die Adernpaare werden i.A. elektrisch symmetrisch ausgeführt
- Nebensprechen (induktive und kapazitive Kopplungen) -> Nebensprechdämpfung
- Kopplungen gegen das Massepotential

I.5.2.2. Hochfrequenzkabel

- Skineffekt

  Elektrische Leitung erfolgt nur in einer dünnen Außenschicht
- Koaxialkabel
- Litzen vs. Vollleiter

  Mechanische Flexibilität

I.5.2.3. Basisbandverfahren

- Das verwendete Frequenzband reicht von 0 Hz bis zu einer vorgegebenen Grenzfrequenz.
- Die Bits werden hier als Rechtecksignale auf die Leitung gegeben.
- Dabei wird eine **isochrone** Übertragung verwendet.

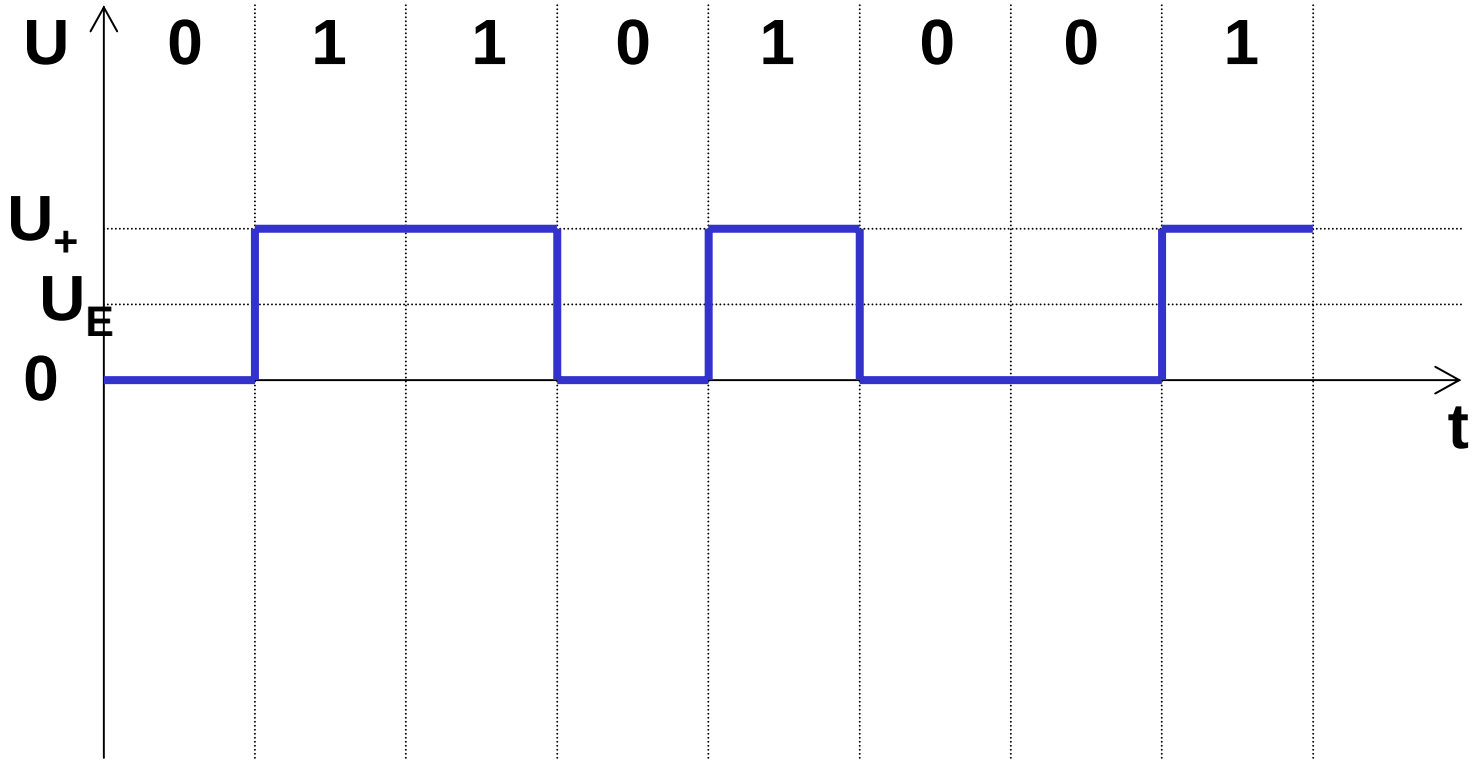
Einfachstromverfahren

- Zur Codierung wird eine Spannung verwendet, die Zuordnung ist z.B.:
  - Bitwert 0 ... Spannung 0V
  - Bitwert 1 ... Spannung U_+
- Zur Decodierung ist eine Entscheidungsschwelle U_E notwendig

Einfachstromverfahren

+ Einfach
- Entscheidungsschwelle müsste abhängig von der Länge der Übertragungsstrecke sein
- Lange Folgen von 0 oder 1 führen zu einem Gleichstromanteil
- Lange Folgen von 0 oder 1 führen zu einem Timingproblem

Einfachstromverfahren



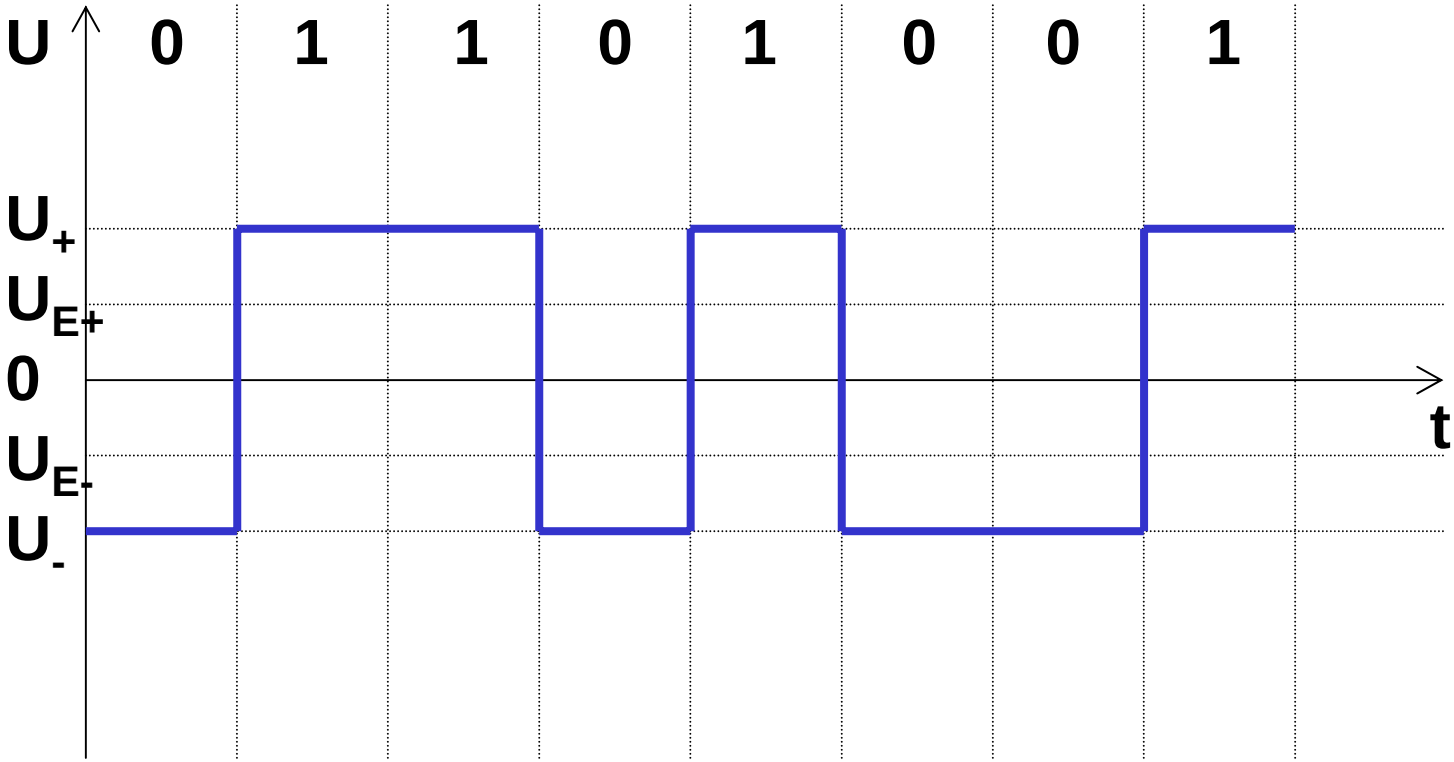
Doppelstromverfahren

- Zur Codierung werden 2 Spannungen verwendet, die Zuordnung ist z.B.:
  - Bitwert 0 ... Spannung U_-
  - Bitwert 1 ... Spannung U_+
- Zur Decodierung sind zwei Entscheidungsschwellen U_{E+} und U_{E-} notwendig

Doppelstromverfahren

+ Einfach
+ Entscheidungsschwellen unabhängig von der Länge der Übertragungsstrecke
- Lange Folgen von 0 oder 1 führen zu einem Gleichstromanteil
- Lange Folgen von 0 oder 1 führen zu einem Timingproblem

Doppelstromverfahren



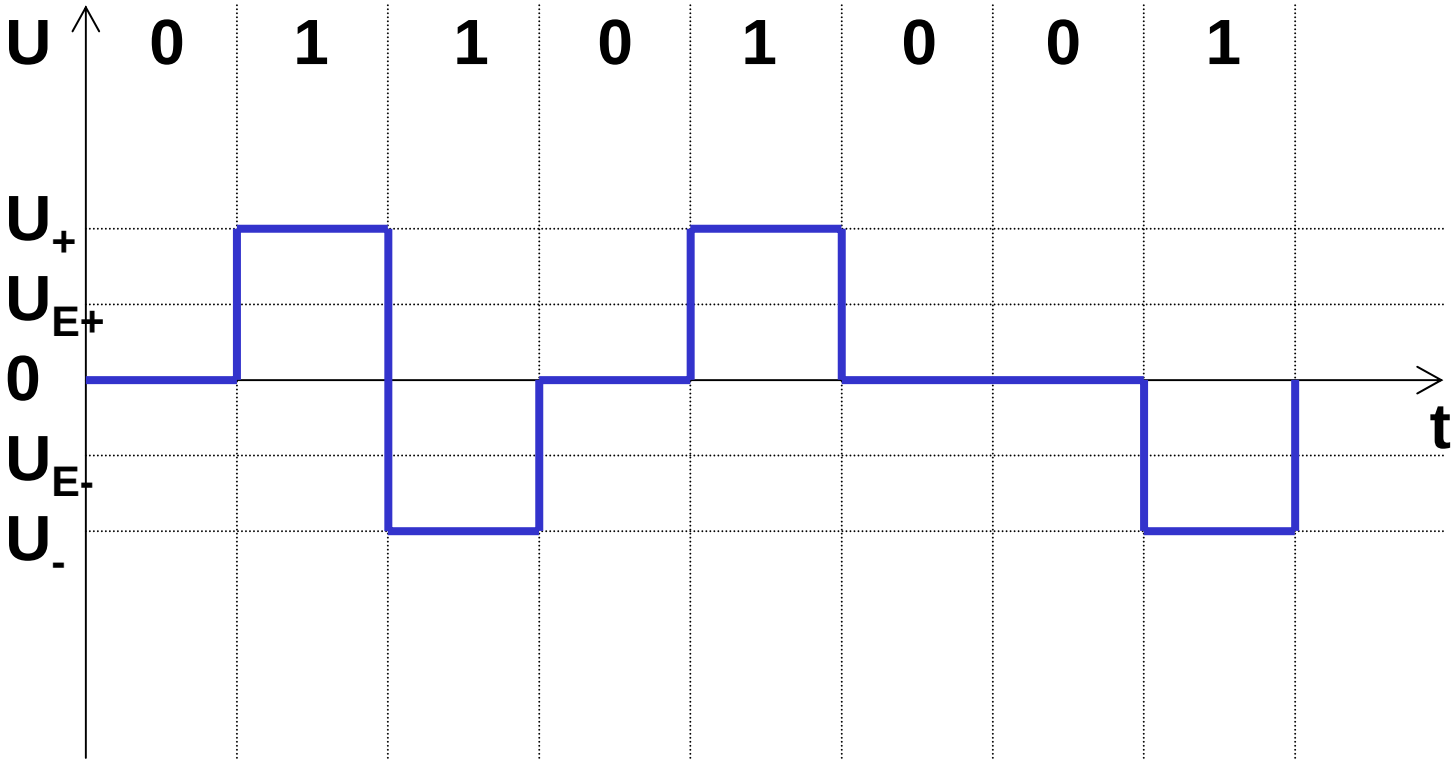
Bipolarverfahren

- Zur Codierung werden 3 Spannungen verwendet, die Zuordnung ist z.B.:
  - Bitwert 0 ... Spannung 0V
  - Bitwert 1 ... Spannungen U_+ und U_-
- Zur Decodierung sind zwei Entscheidungsschwellen U_{E+} und U_{E-} notwendig

Bipolarverfahren

+ Keine Probleme durch lange „1“-Folgen
- Entscheidungsschwellen müssten abhängig von der Länge der Übertragungsstrecke sein
- Lange Folgen von 0 führen zu einem Gleichstromanteil
- Lange Folgen von 0 führen zu einem Timingproblem

Bipolarverfahren



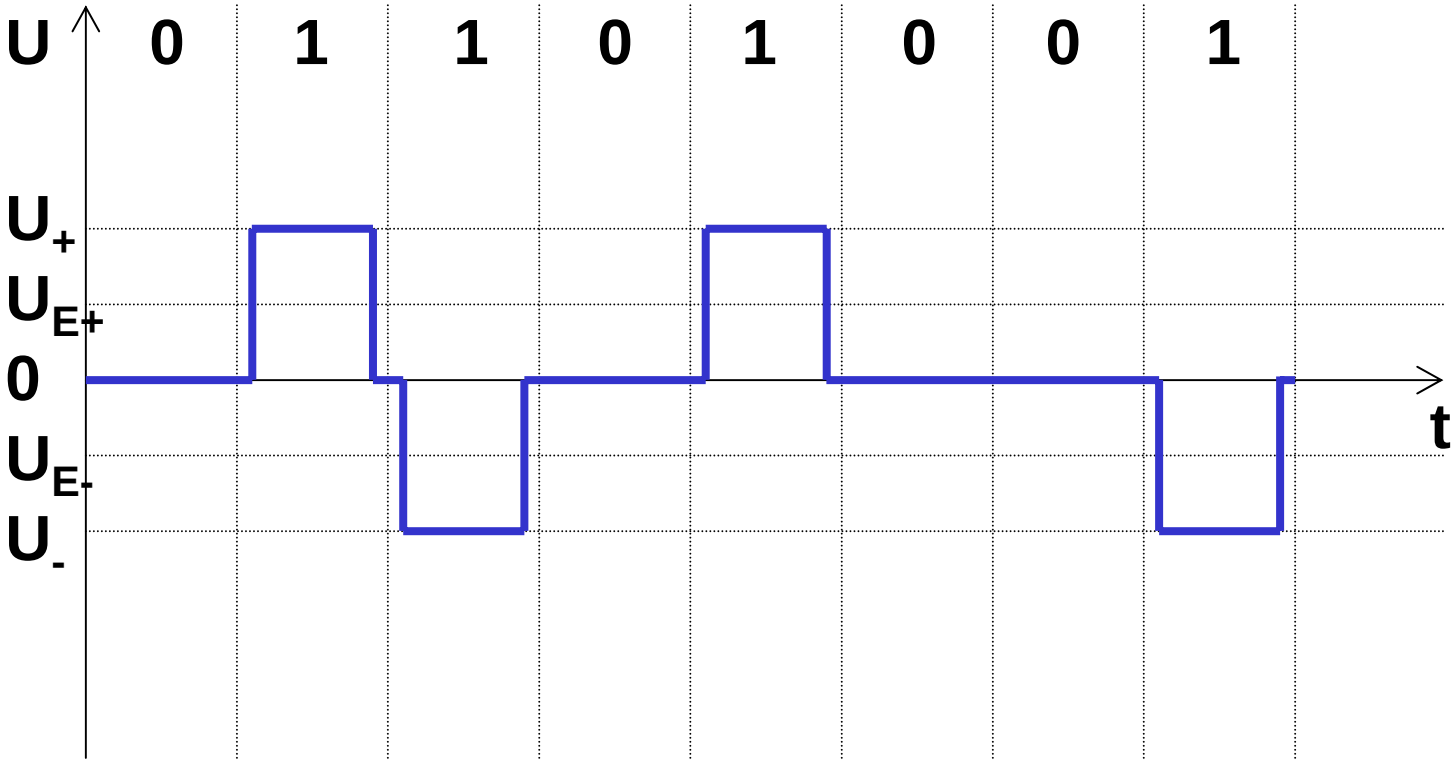
Psudoternärverfahren

- Zur Codierung werden 3 Spannungen verwendet, die Zuordnung ist z.B.:
  - Bitwert 0 ... Spannung 0V
  - Bitwert 1 ... Spannungen U_+ und U_-
- Zur Decodierung sind zwei Entscheidungsschwellen U_{E+} und U_{E-} notwendig
- Die Impulsdauer ist kürzer als die Bitzeit

Psudoternärverfahren

+ Keine Probleme durch lange „1“-Folgen
+ Kein Störungen durch Ausschwingvorgänge
- Entscheidungsschwellen müssten abhängig von der Länge der Übertragungsstrecke sein
- Lange Folgen von 0 führen zu einem Gleichstromanteil
- Lange Folgen von 0 führen zu einem Timingproblem

Psudoternärverfahren



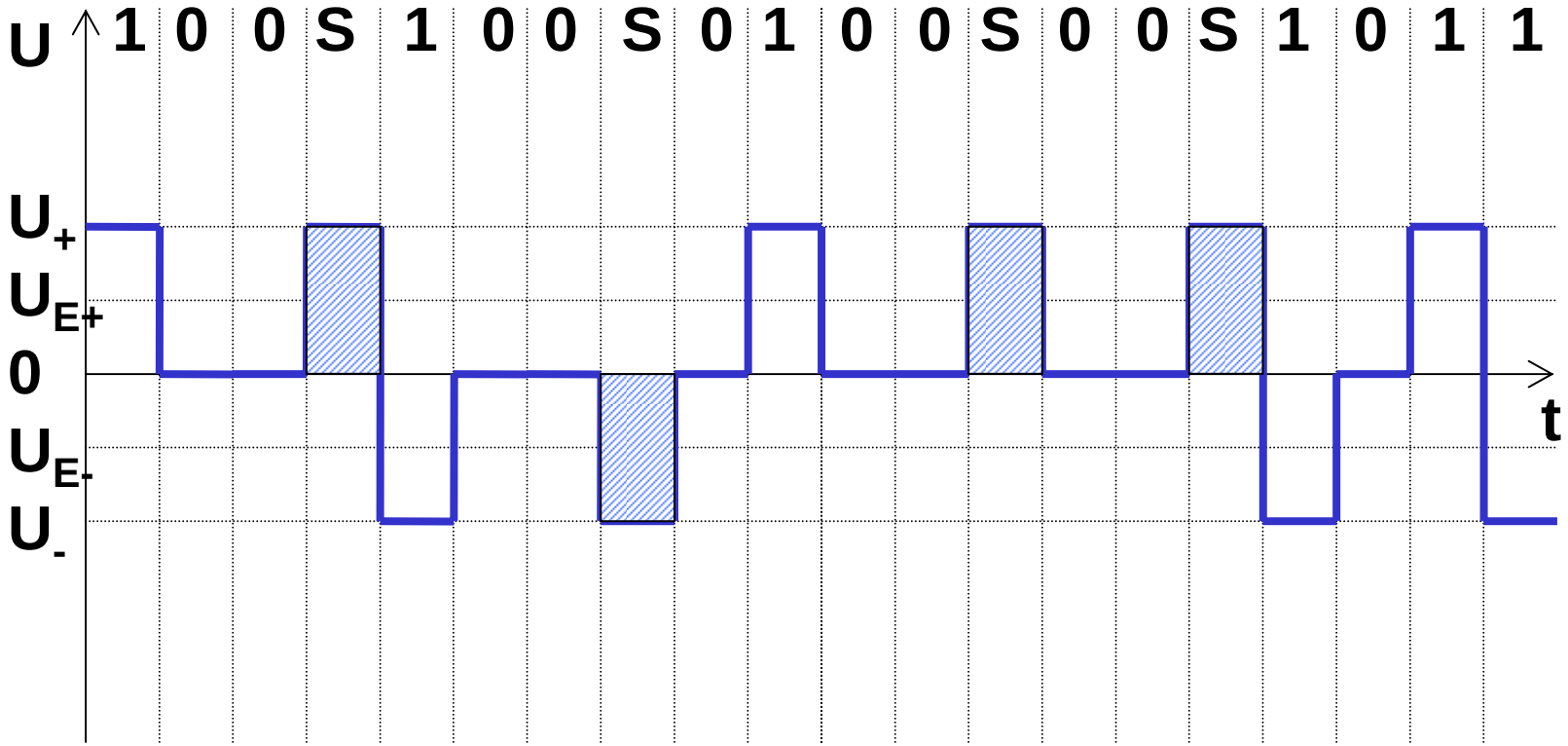
Bipolarcode hoher Dichte

- Zur Codierung werden 3 Spannungen verwendet, die Zuordnung ist z.B.:
  - Bitwert 0 ... Spannung 0V
  - Bitwert 1 ... Spannungen U_+ und U_-
- Zur Decodierung sind zwei Entscheidungsschwellen U_{E+} und U_{E-} notwendig
- Nach einer Anzahl von „0“ wird ein Signal eingefügt.

Bipolarcode hoher Dichte

+ Keine Störungen durch lange Folgen gleicher Bits
- Entscheidungsschwellen müssten abhängig von der Länge der Übertragungsstrecke sein
- Verringerung der Bandbreite durch die Sondersignale

Bipolarcode hoher Dichte



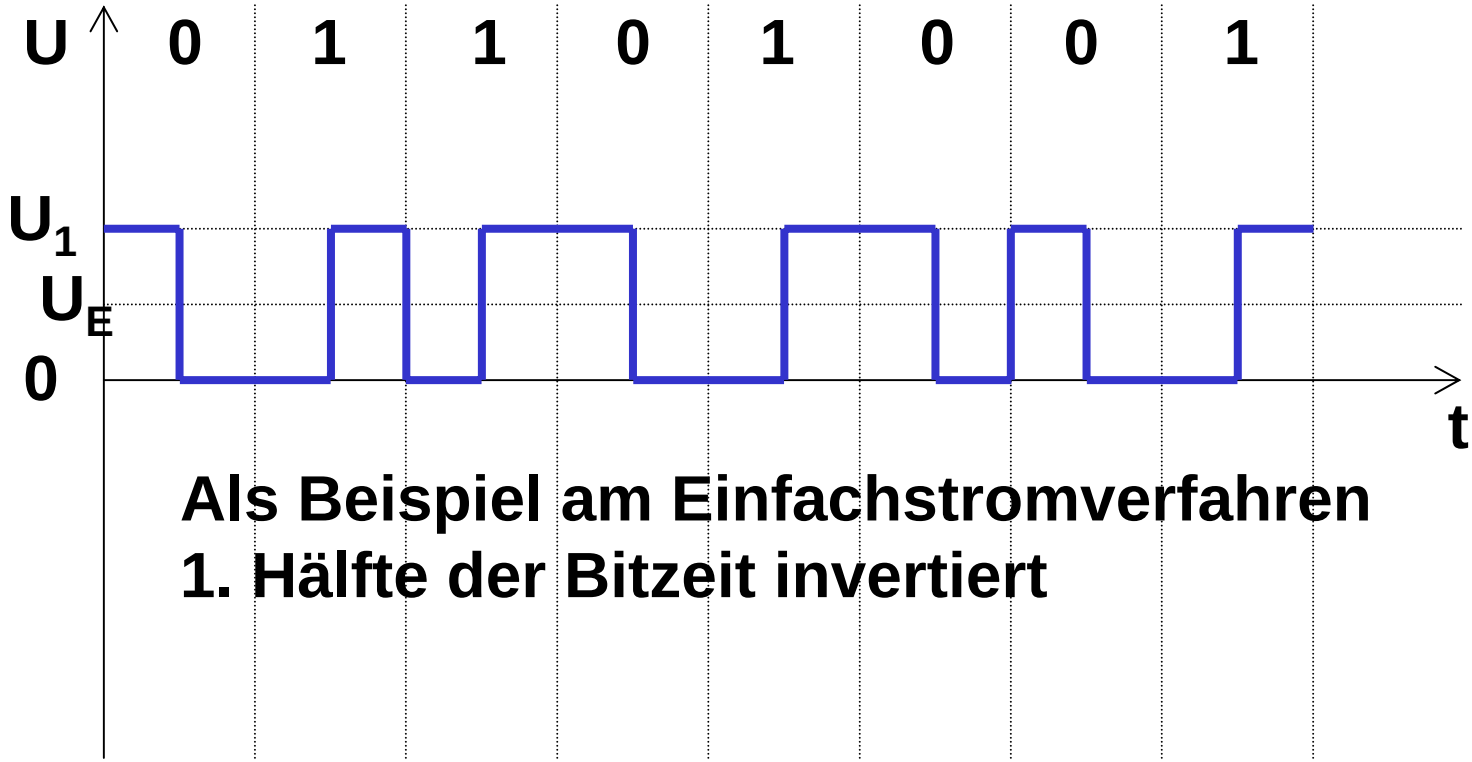
Manchestercodierung

- Zusätzlich zu einer der bisherigen physikalischen Codierungen kann noch um eine logische Codierung ergänzt werden
- z.B.: In der ersten Hälfte der Bitzeit wird der invertierte Wert in der zweiten Hälfte der Bitzeit der wahre Wert übertragen (Auch umgekehrt möglich!)

Manchestercodierung

+ Selbsttaktender Code
- Halbierung der nutzbaren Bandbreite

Manchestercodierung



Als Beispiel am Einfachstromverfahren
1. Hälfte der Bitzeit invertiert

I.5.2.4. Breitbandverfahren

- Zur besseren Ausnutzung des Mediums werden hier mit Hilfe von Modulation und Kanalmultiplex mehrere Signale übertragen.
- Direkte Übertragung ist oft nicht möglich (Luft)
- Trägerwellen

Generelles

- Schwingungen können mittels folgender Gleichung beschrieben werden:

$$y = \alpha * \sin(\omega t + \varphi)$$

- Jede der drei Variablen stellt eine Veränderung (Modulation) dar:
  - α Amplitudenmodulation
  - ω Frequenzmodulation
  - φ Phasenmodulation

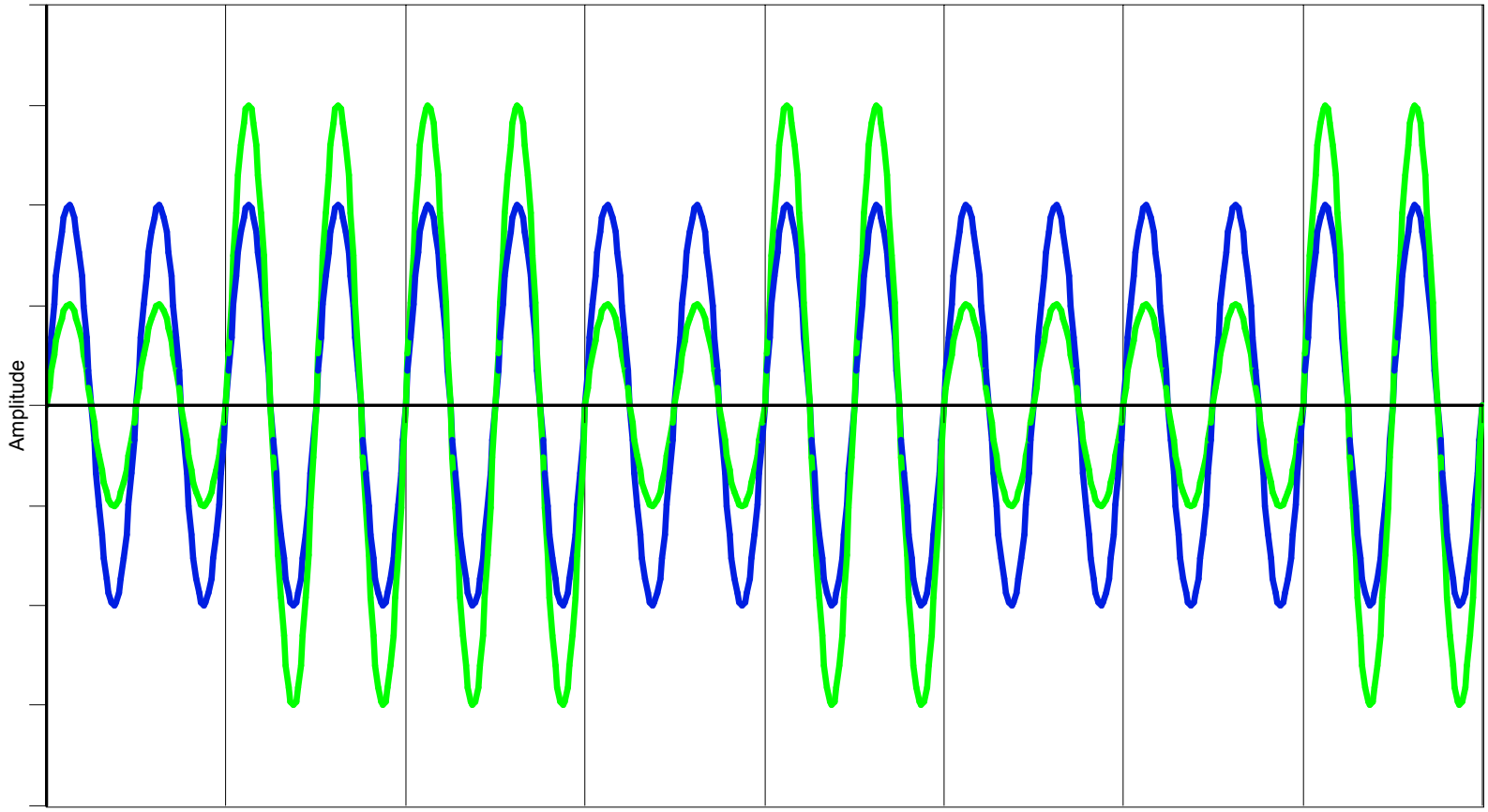
Amplitudenmodulation

- Hier wird die die Amplitude eines Träger verändert
- Grenzfall „Harte Tastung“:
  - Bitwert 0 Kein Signal
  - Bitwert 1 Signal
  - Daher eigentlich kein Breitbandverfahren, da nur ein Kanal möglich ist.

Amplitudenmodulation

- Mehrere Bits können in einer Bitzeit mit Hilfe mehrerer Amplituden übertragen werden
  - Anzahl der Amplituden = $2^{\text{Anzahl der Bits}}$
- Folgendes Beispiel:
  - Träger blau Bitwert 0=½ Amplitude
  - Signal grün Bitwert 1=1 ½ Amplitude

Amplitudenmodulation



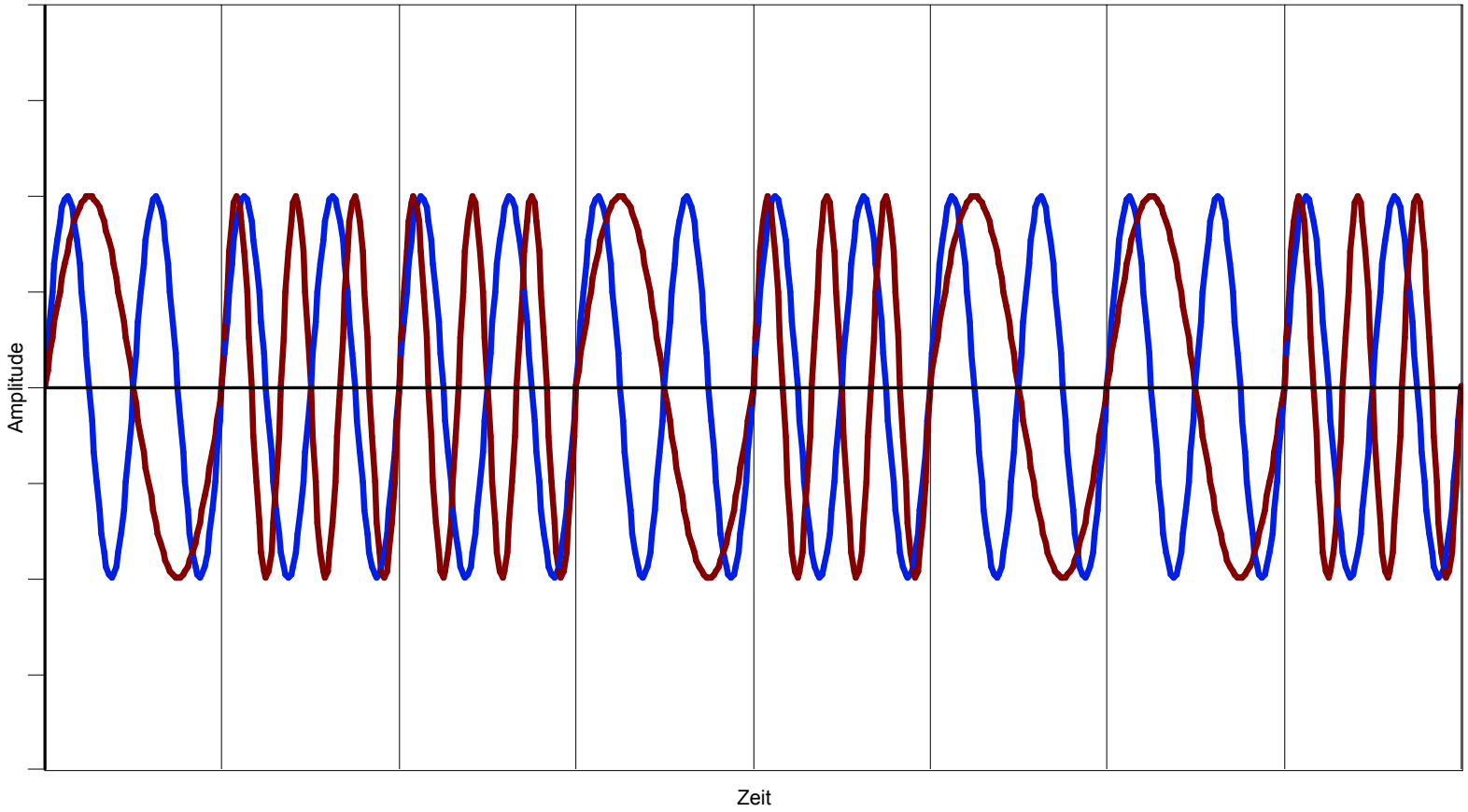
Frequenzmodulation

- Die Frequenz des Träger wird verändert
- Bei binären Information entstehen zwei unterscheidbare Frequenzen
- Dabei ist darauf zu achten, dass das Modulationsprodukt noch innerhalb des zur Verfügung stehen Frequenzbandes liegt und keine „Sprünge“ entstehen.

Frequenzmodulation

- Mehrere Bits können in einer Bitzeit mit Hilfe mehrerer Frequenzen übertragen werden
  - Anzahl der Frequenzen = $2^{\text{Anzahl der Bits}}$
- Folgendes Beispiel:
  - Träger blau Bitwert 0=½ Frequenz
  - Signal braun Bitwert 1=1 ½ Frequenz

Frequenzmodulation



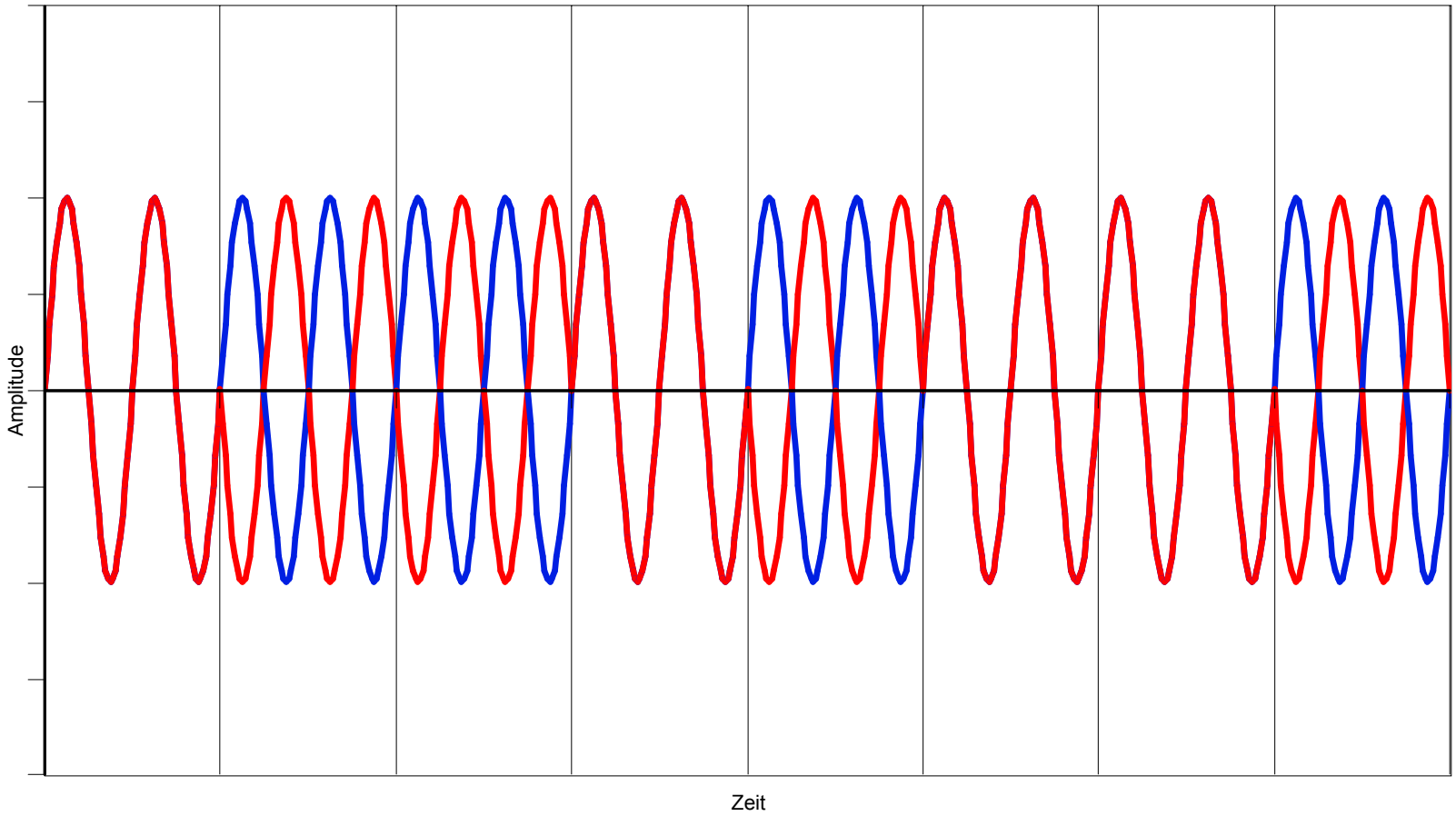
Phasenmodulation

- Die Phase des Trägersignals wird verändert.
- Dabei ist auf unterschiedliche Phasenverschiebungen zu achten (Eine Phasenverschiebung um $+\pi$ und eine um $-\pi$ führt zum gleichen Signal).
- Bei Frequenzänderungen muss die Phasenverschiebung angepasst werden.

Phasenmodulation

- Mehrere Bits können in einer Bitzeit mit Hilfe mehrerer „Phasen“ übertragen werden
  - Anzahl der „Phasen“ = $2^{\text{Anzahl der Bits}}$
- Folgendes Beispiel:
  - Träger blau — Bitwert 0=Keine Änderung der Phase
  - Signal rot — Bitwert 1=Phasensprung um π

Phasenmodulation



Kombinationen

- Die drei Verfahren lassen sich selbstverständlich auch kombinieren
- QAM Quadratur Amplitudenmodulation
  - Amplitudenmodulation
  - Phasenmodulation
- Die Demodulation wird dadurch immer aufwendiger
- Beispiel: Modem für Festnetztelephon

Begriffe

FFM Fixed Frequency Modem

VFM Variable Frequency Modem

ASK Amplitude Shift Keying

FSK Frequency Shift Keying

PSK Phase Shift Keying

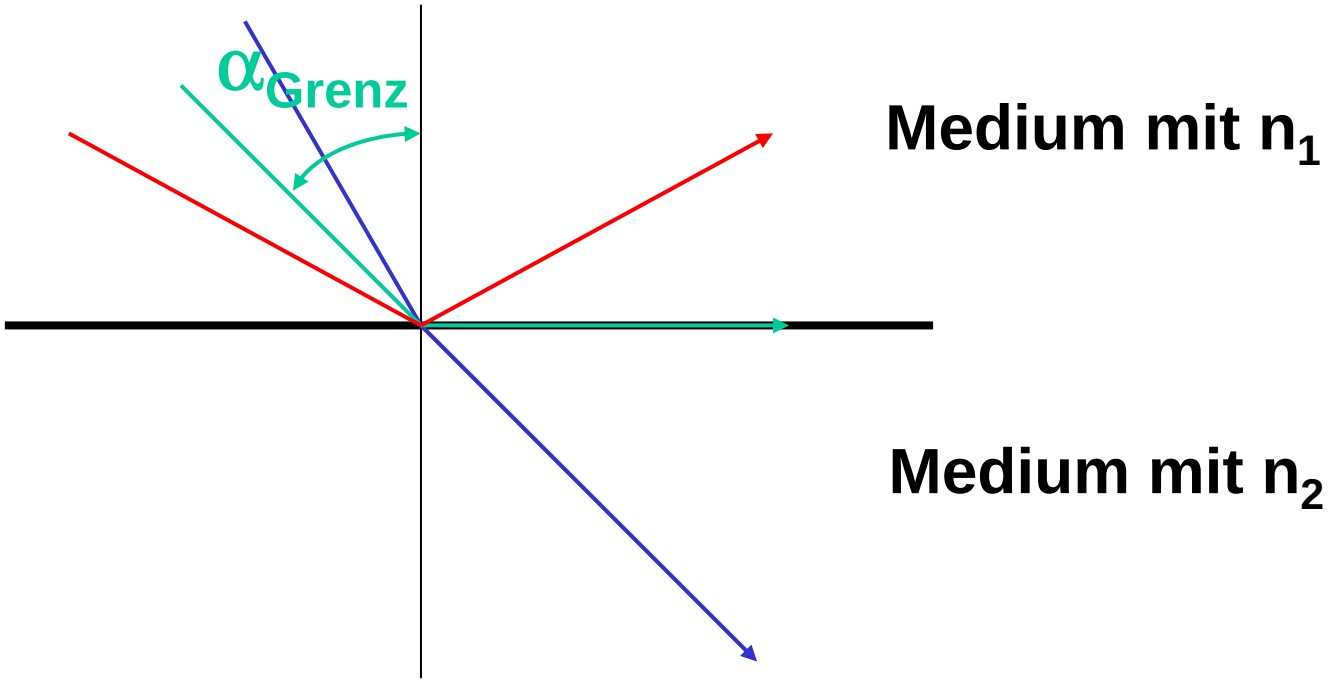
PCM Pulse Code Modulation

I.5.3. Lichtwellenleiter

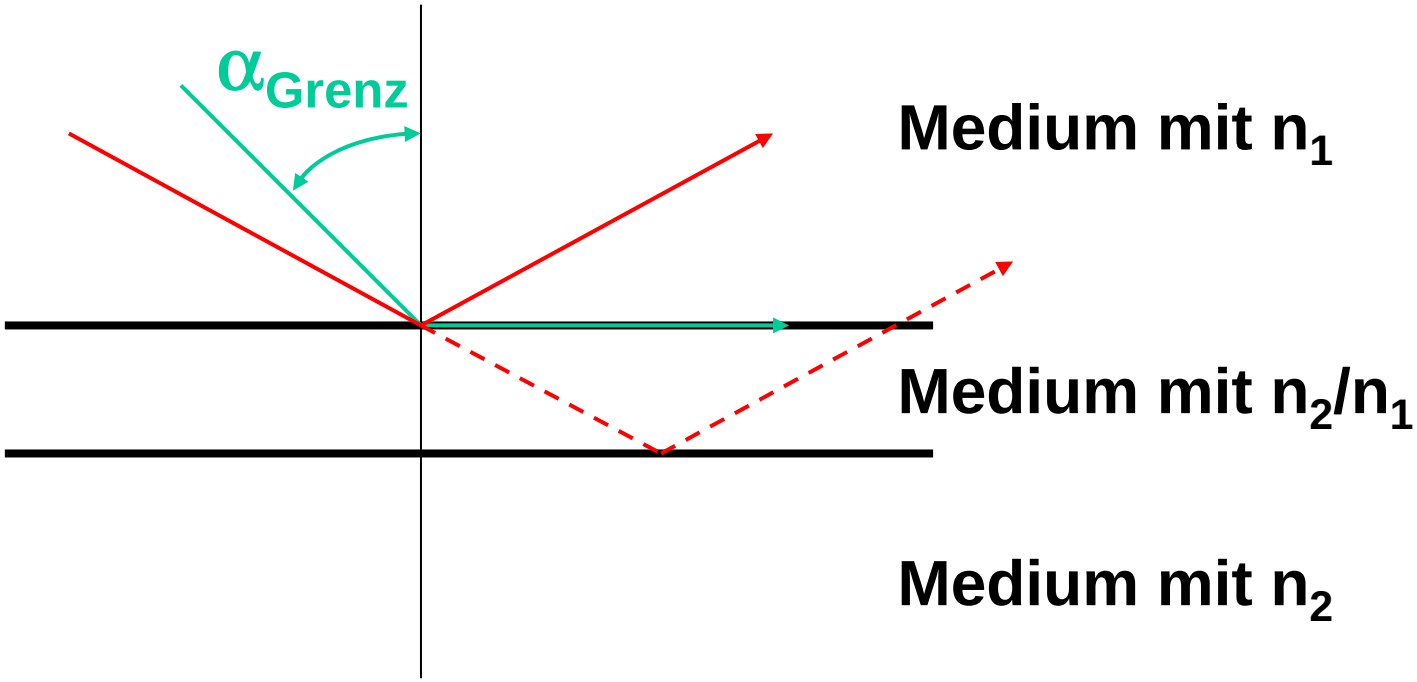
- Die physikalische Grundlage dieser Übertragungstechnologie ist die Totalreflexion beim Übergang von einem optisch dichteren Medium in ein optisch dünneres bei Überschreitung des Grenzwinkels.

$$\sin \alpha_{Grenz} = \frac{n_2}{n_1} \qquad \text{mit } n_2 < n_1$$

Totalreflexion



Totalreflexion 2



Totalreflexion 3

Aus Gerthsen-Kneser-Vogel
Physik
13. Auflage
Springer 1977

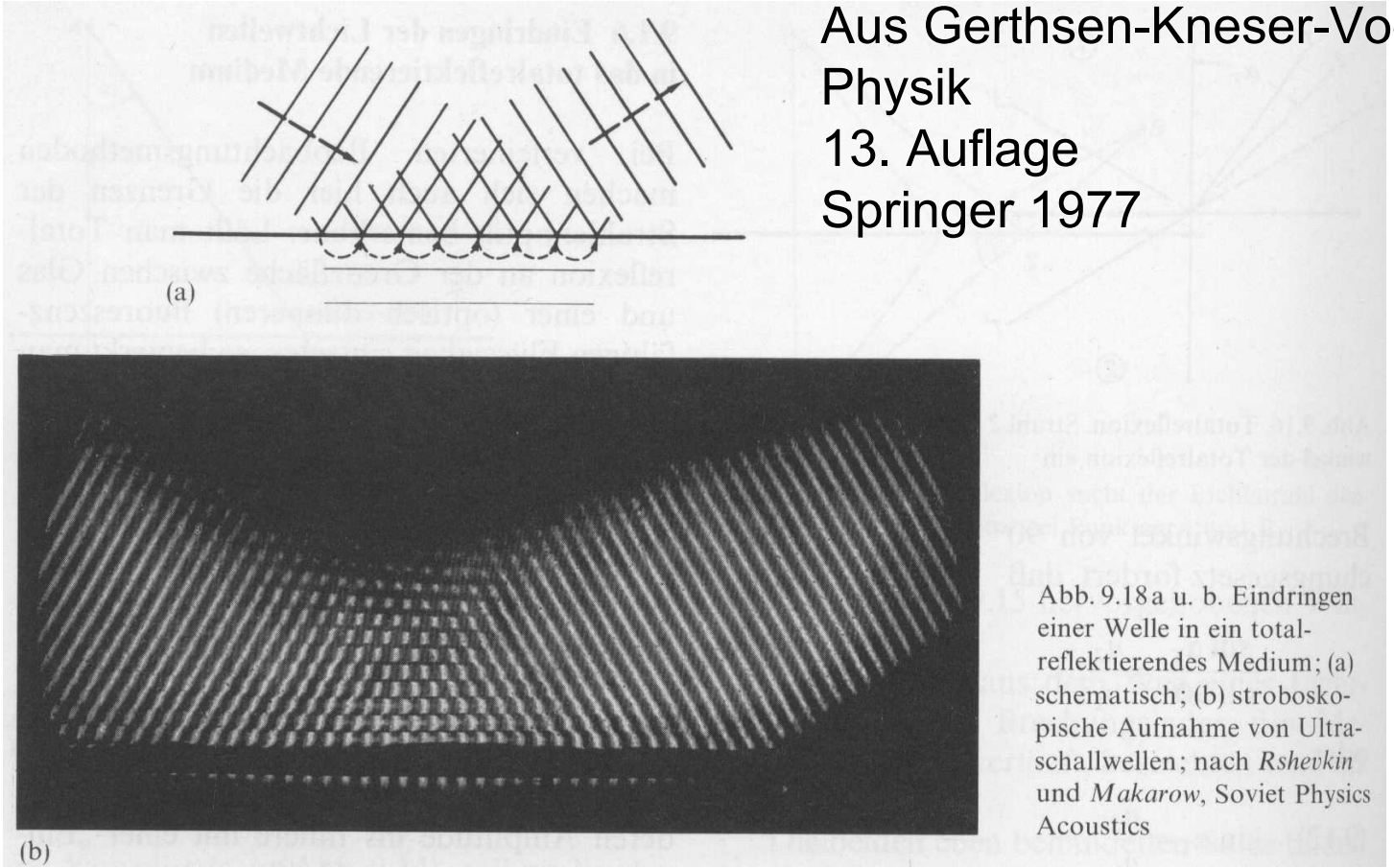


Abb. 9.18a u. b. Eindringen einer Welle in ein total-reflektierendes Medium; (a) schematisch; (b) stroboskopische Aufnahme von Ultraschallwellen; nach *Rshevkin* und *Makarow*, Soviet Physics Acoustics

Totalreflexion 4

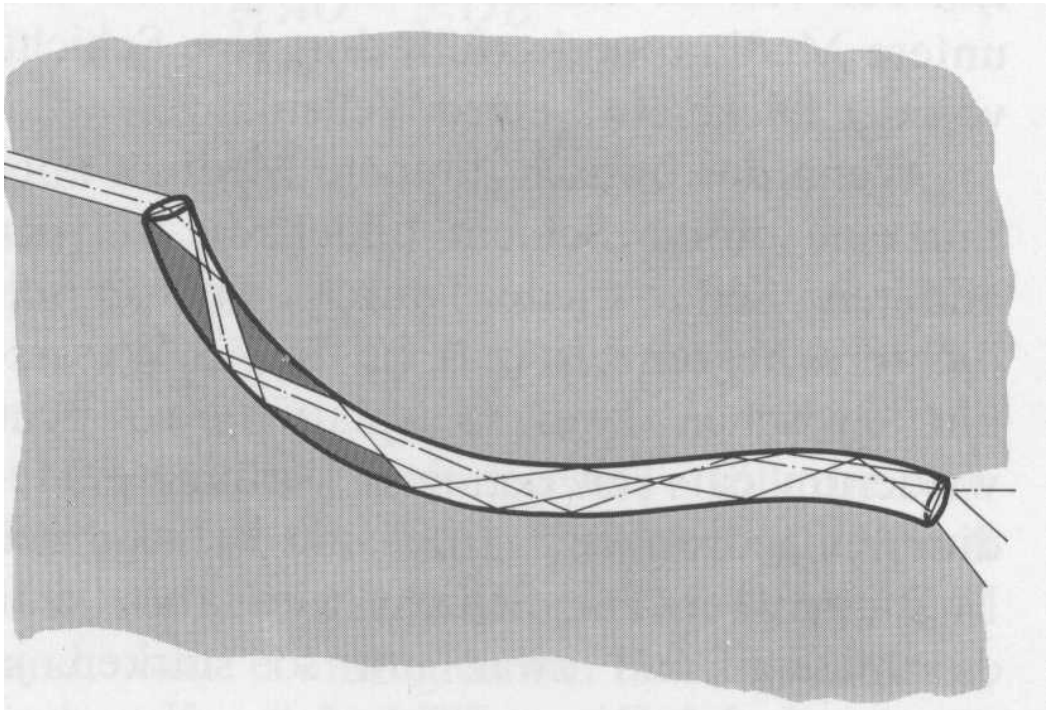


Abb. 9.19. Glasfaser als Lichtleiter. Die ursprüngliche Anordnung der Teilstrahlen im Bündel geht durch Mehrfachreflexion verloren. Zur Bilderzeugung braucht man sehr viele Fasern

Modendispersion

- Licht entlang der optischen Achse = Licht niedrigen Modes
- Licht, daß oft reflektiert wird = Licht hohen Modes
- Modendispersion entsteht durch die Laufzeitunterschiede verschiedener Frequenzanteile

Faserarten

- Stufenprofilfaser
  - Verschiedene Brechungsindizes
- Gradientprofilfaser
  - Kontinuierlich sich ändernder Brechungsindex
- Monomodefaser
  - Modenausbreitung fast nur entlang der optischen Achste

Intensitätsverluste

- Streuung an Unreinheiten in der Faser
- Absorptionsverluste durch Anregung der Lichtwellenleitermoleküle
- Kopplungsfehler an den Anschluß- bzw. Verlängerungsstellen

Realisierungen

- Leuchtdioden und Photowiderstände
  - <100 MBit/s
  - mehrere 100 m
- Laserdioden und Lawinendioden
  - ≥1 GBit/s
  - mehrere km

Eigenschaften

+ Vollständige elektrische Trennung
+ Keine Potentialprobleme (Erdschleifen)
+ Kein Risiko durch elektrische Funken
+ Keine elektrischen und magnetischen Störungen
+ Höchste Abhörsicherheit
+ Hohe Übertragungskapazität
+ Geringe Dämpfung
+ Geringes Kabelgewicht, kleiner Querschnitt
+ „Unbegrenzte“ Materialverfügbarkeit
- Schwierige Verbindungs- und Verzweigungstechnik

I.5.4. Funkübertragung

- Funkübertragungen werden in zunehmenden Maße für die Datenkommunikation eingesetzt.
- Die Übertragung erfolgt mit Hilfe elektromagnetischer Wellen ohne definiertes Medium.

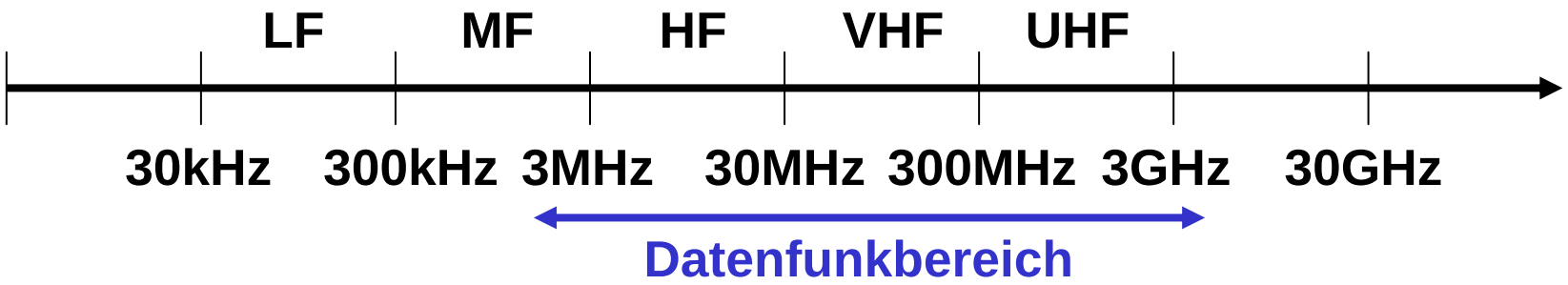
Vorteile der Funkübertragung

- Kabellose Verbindung (keine „Stemmarbeiten“)
- Schnelle Installation
- Mobile Sender und Empfänger
- Breitband-Fähigkeiten
- Broadcastfähigkeiten

Nachteile der Funkübertragung

- Interferenzen und Ausbreitungsprobleme
- Frequenzknappheit
- Datensicherungsprobleme
- Designprobleme (Lage der Antennen)
- Behördliche Restriktionen (Funk- und „Bau“probleme) und Lizenzvergabe

Frequenzband

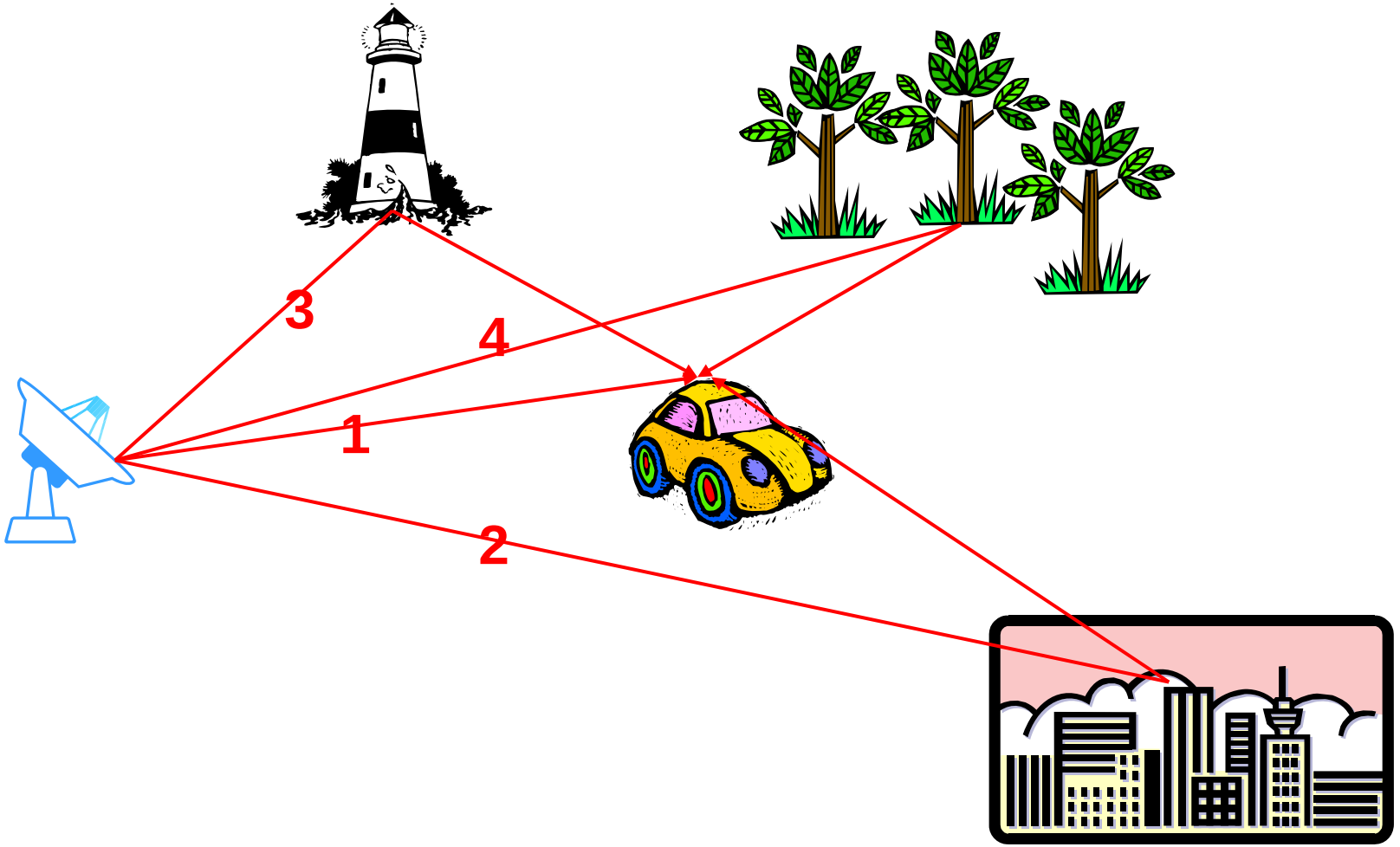


- Unter 2 MHz nicht möglich, da die Antennen zu groß wären
- Über ca. 5 GHz Dämpfung bereits durch Luftfeuchtigkeit (Regen, ...)
- Auch Hörfunk und TV nutzen diese Frequenzen

„Multipathing“

- Wellen erreichen den Empfänger auf verschiedenem Weg und daher nicht gleichzeitig.
- Phasenverschiebung der Wellen zueinander durch unterschiedliche Anzahl von Reflexionen.
- Die Überlagerung verursacht Interferenzen, die bis zur Auslöschung des Signals führen können.

„Multipathing“- Beispiel



Dopplereffekt

- Durch die Bewegung des Senders oder des Empfängers (oder beider) ändert sich die Frequenz scheinbar

$$f = f_0\left(1+\frac{v}{c}\right)$$

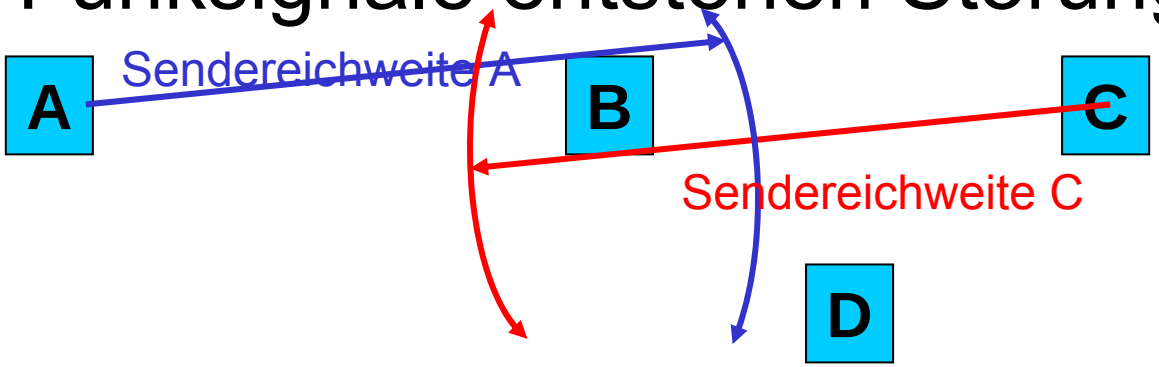
Empfänger bewegt sich auf die feststehende Quelle zu

$$f = f_0\left(1-\frac{v}{c}\right)$$

Empfänger bewegt sich von der feststehenden Quelle fort

„Versteckte“ Stationen

- Durch die begrenzte Reichweite der Funksignale entstehen Störungen:



- A sendet an B, doch kann B nicht empfangen wenn C zeitgleich an B oder D sendet (C ist für A versteckt).

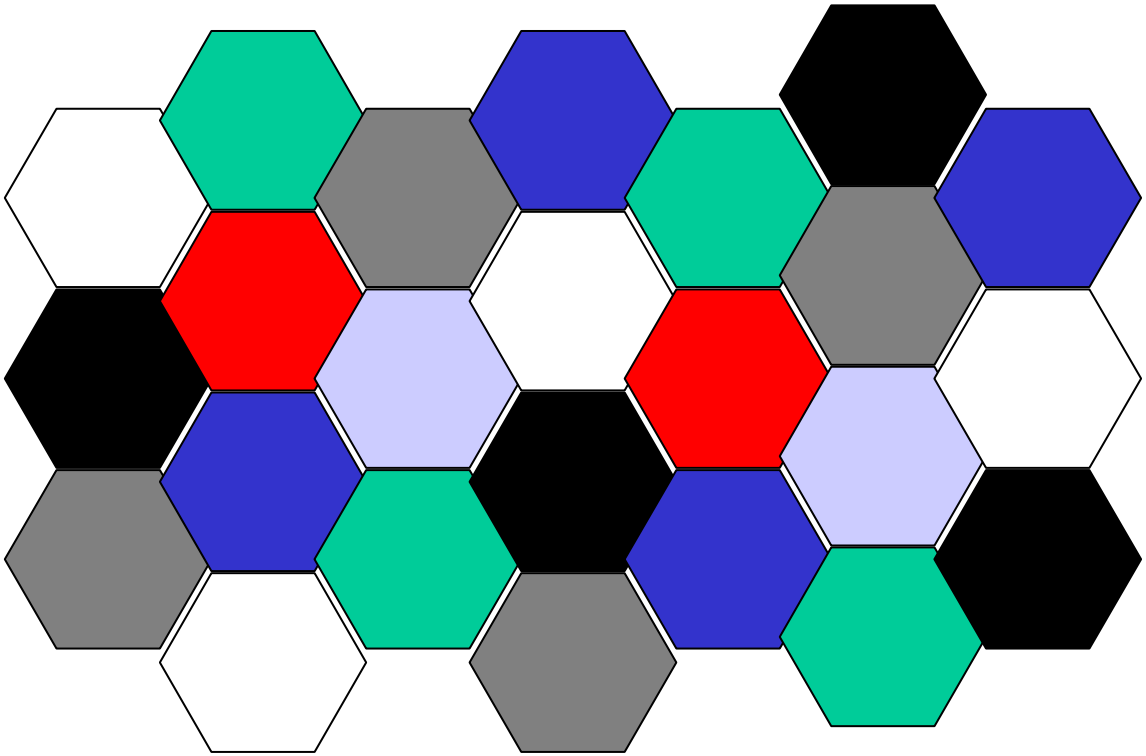
Sonstige Fehler

- Thermisches Rauschen
- Atmosphärisches Rauschen
- „Elektromagnetische Umweltverschmutzung“
- Räumliche Ausbreitung führt zu großem Energieverlust

Zellsysteme

- Um der Frequenzknappheit zu begegnen, werden Frequenzen in verschiedenen räumlichen Gebieten wiederverwendet.
- Dabei wird die begrenzte Sendereichweite ausgenützt.
- Bei Bewegung aber Frequenzumschaltung notwendig

Zellsysteme – Beispiel



Jedes Sechseck ist eine Zelle

7 Zellen bilden einen Cluster (jede Zelle mit den sechs angrenzenden Zellen)

Jede Farbe stellt eine Frequenz dar

I.6. Vermittlungsverfahren

Nachdem i.a. mehr als 2 Teilnehmer vorhanden sind, muß ein Teilnehmer die Möglichkeit der Auswahl haben, dafür existieren drei Techniken:

- Circuit Switching
- Message Switching
- Packet Switching

I.6.1. Circuit Switching

- Fester Leitungsweg wird gesucht (calling).
- Für die gesamte Kommunikationsdauer reserviert (pre-allocation).
- Ausschließliche Nutzung durch Partner
- Multiplex möglich
- Beispiel: Telefonnetz

Circuit Sw. – Eigenschaften

- Keine Verzögerungszeiten (außer der Signalverzögerung)
- Zeitaufwendiger Auf- und Abbau der Verbindung
- Vollauslastung des Netzes durch eine relativ geringe Verbindungszahl
- Schlechte Ausnützung der Übertragungskapazität

I.6.2. Message Switching

- Die zu übertragende Nachricht wird dem Netz übergeben und im **Store-and-Forward**-Prinzip über Zwischenknoten zum Empfänger geleitet.
- Zwischenknoten speichern die Nachricht vollständig
- Angaben zu Quelle, Ziel und Laufweg

Message Sw. – Eigenschaften

- Wesentliche Steigerung der Auslastung
- Unterschiedliche Übertragungsverzögerung
- Kein expliziter Auf- und Abbau
- Flexibilität bei Ausfall einer Verbindung
- Unterschiedliche Länge der Nachrichten kann zu unfairer Verzögerung führen
- Notwendigkeit großer, flexibler Puffer

I.6.3. Packet Switching

- Das Verfahren entspricht dem Messageswitching, allerdings gibt es hier eine relative kleine Obergrenze für die Länge
- Zerlegung der Nachricht
- Zusammensetzung der Nachricht (**Sequencing**)

Packet Sw. – Eigenschaften

- siehe Message Switching
- Zusammensetzung durch Verlust, Duplizierung bzw. Überholung von Paketen aufwendig.
- **Reassembly Deadlock** (Teilnachrichten blockieren Speicher)
- Wesentlich kleinere Puffer

Packet Sw. – Begriffe

- Datagramm
  - Eine Nachricht, die in ein Paket passt.
- Virtual Circuit
  - Der logische Weg zwischen den Teilnehmern, der im Rahmen des Übetragungsprotokolls vereinbart wird.

Packet Sw. – Aufgaben (Netz)

- Auf- und Abbau der logischen Verbindung.
- Wiederherstellung verlorener Daten durch Wiederholung.
- Eliminierung von Duplikaten.
- Ordnen der Pakete in ihre Reihenfolge.
- Datenflußsteuerung.
- Erkennen und Korrigieren von Übertragungsfehlern.

Packet Sw. - Paketinhalt

- Information über Sender und Empfänger
- Länge des Pakets bzw. Start/Ende-Kennung
- Paketfolgenummer
- Laufzeitinformationen, QoS-Angaben
- Synchronisation
- Fehlerprüfbits bzw. -summen
- Nutzdaten

I.7. Topologien

- Begriffe
- Bewertungskriterien
- Verbreitete Topologien
- Besondere Topologien

I.7.1. Begriffe

- Zusammenhangsgrad
- Teilstreckennetze
- Diffusionsnetze
- Zugriffsverfahren

Zusammenhangsgrad

Ein Netzwerk wird dann N-zusammen-hängend genannt, wenn nach Ausfall von N-1 Verbindungen noch immer jeder Knoten des Netzwerkes mit jedem anderen Knoten Verbindung hat.

(0-Zusammenhängend wird in der Literatur oft mit 1-zusammenhängend gleich gesetzt)

Teilstreckennetze

Netzwerke, bei denen die Daten über eine oder mehrere unabhängige Übertragungsstrecken von einer Quelle zum Ziel transportiert werden, dabei können die einzelnen Teilstrecken technisch verschieden sein (optisch, elektrisch, ...). Jede Teilstrecke hat eine Anfangs- und einen Endpunkt.

Diffusionsnetze

Netzwerke bei denen alle Stationen an ein gemeinsames Übertragungsmedium angeschlossen sind, dabei wird die Nachricht vom Sender in das Medium übergeben und vom Empfänger ausgewertet. „Mithören“ für andere Stationen ist grundsätzlich möglich.

Zugriffsverfahren

- Random Access
- Gesteuerte Zugriffe
- Token/Polling

Random Access

- Jeder Benutzer hat grundsätzlich jederzeit Zugriff.
- Kollisionsmöglichkeit.
- Varianten:
  - ALOHA, S-ALOHA
  - **CSMA/CD**, CSMA/CA
  - BTMA, CDMA

Random Access – ALOHA

- 1970 an der Universität Hawaii entw.
- Jeder sendet nach Bedarf
- Keine Abstimmung
- Schlechter Durchsatz: (ca. 18%)

Random Access – S-ALOHA

- Slotted ALOHA (1972)
- Festgesetzte Time-Slots
- „Master“, der die Slots definiert (Setzen der Anfangszeiten)
- Durchsatz ca. 36%
- Beispiel: Satellitenkommunikation

Random Access – CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- Abhören der Leitung, ob sie frei ist.
- Senden und weiterhören, ob dabei eine Kollision entstanden ist.
- Wenn notwenig: JAM-Signal.
- Erneutes nach „zufälliger“ Wartezeit (2^n)
- Beispiel: Ethernet (802.3)

Random Access – CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
- Ähnlich CSMA/CD
- Durch Prioritäten werden Kollisionen vermieden (nicht verhindert!).
- Beispiel: Appletalk, WLAN (802.11)

Random Access – BTMA

- Busy Tone Multiple Access
- Speziell für Funknetze entwickelt
- Steuerung über Sonderkanal (Blockierung durch einen Busy Tone)
- Varianten:
  - RD-BTMA (Receiving Destination BTMA)
  - C-BTMA (Conservative BTMA)

Random Access – CDMA

- Code Division Multiple Access
- Speziell für Funknetze entwickelt
- Mit Hilfe von CDM werden mehrere Signale gleichzeitig übertragen
- Varianten:
  - Einheitlicher Code
  - Sender- oder Empfängerspezifischer Code

Gesteuerte Zugriffe

- Jeder Teilnehmer bekommt einen fixen Anteil an der gesamten Bandbreite.
- Inflexibel und schlechte Gesamtauslastung.
- TDMA (Time Division Multiplex Access).
- FDMA (Frequency Division Multiplex Access).

Polling/Token

- Jeder Teilnehmer wird von einem zentralen Vermittler zum Senden aufgefordert (Polling) oder ein spezielles Packet wird weitergereicht (Token).
- Echtzeitfähig (garantierte Antwortzeit).
- Beispiel: Token Ring (802.5).

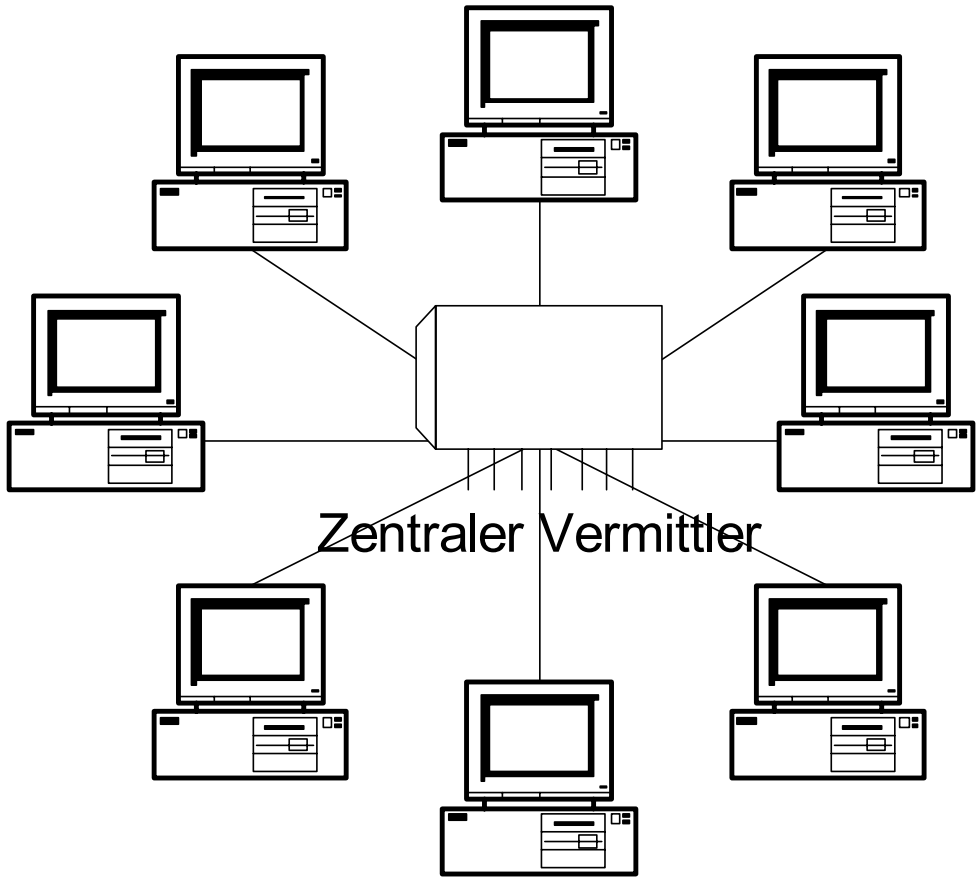
I.7.2. Bewertungskriterien

- Modularität
- Modularität der Kosten
- Zusammenhangsgrad
- Stabilitäts- und Rekonfigurationsverhalten
- Logische Komplexität
- Durchsatzkapazität

I.7.3. Verbreitete Topologien

- Stern (Star)
- Erweiterter Stern (Extended Star)
- Ring
- Bus

Stern



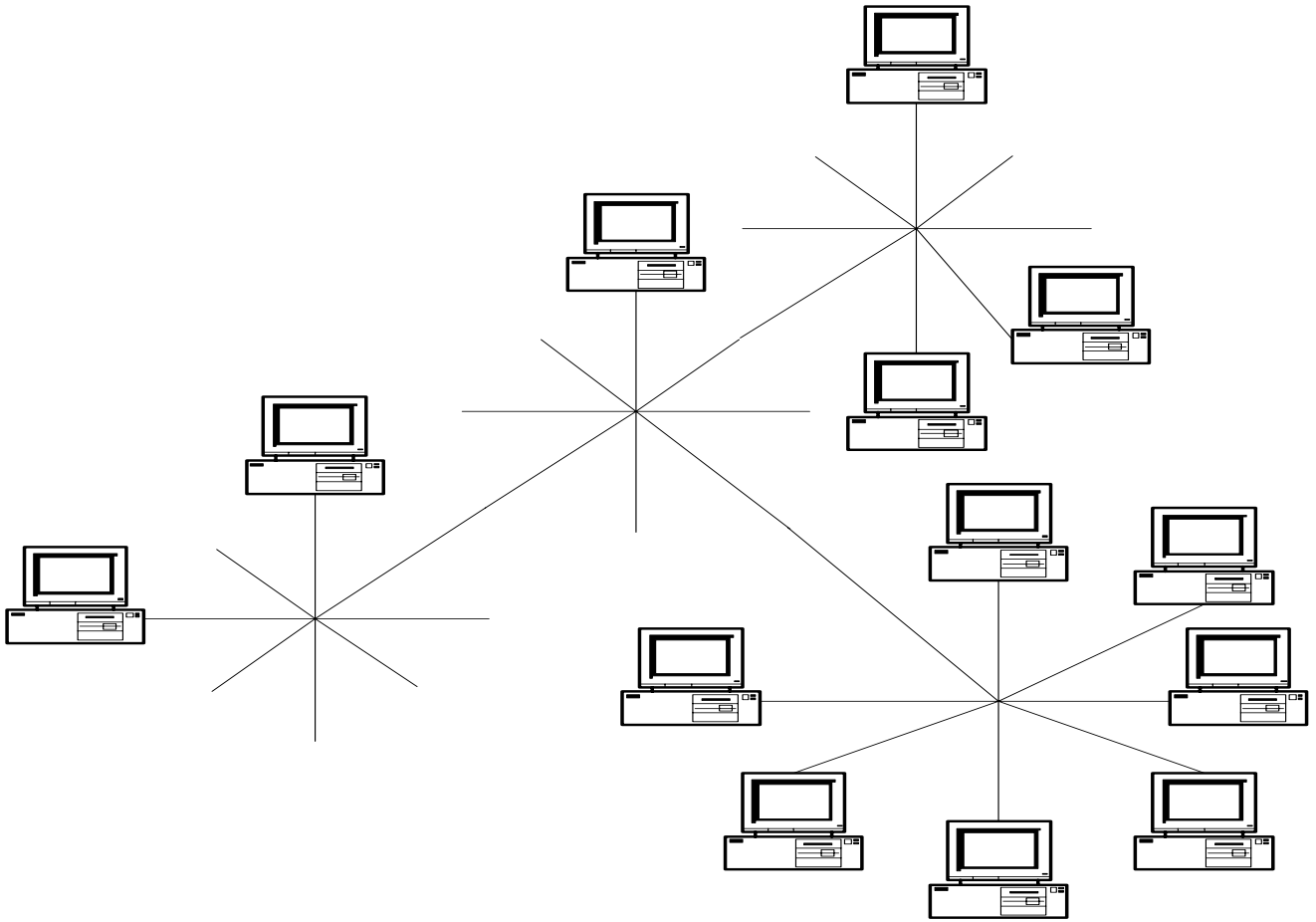
Stern – Eigenschaften

- Alle Nachrichten laufen über ein Zentralsystem (aktiv, passiv)
- Aktiv
  - Zentraler Vermittler
  - Switch
- Passiv
  - Hub

Stern – Bewertungskriterien

Modularität	Sehr gut
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1
Stabilitäts- und Rekonfigurationsverhalten	Gut (!ZV)
Logische Komplexität	Einfach
Durchsatzkapazität	„Zentrale“

Erweiterter Stern



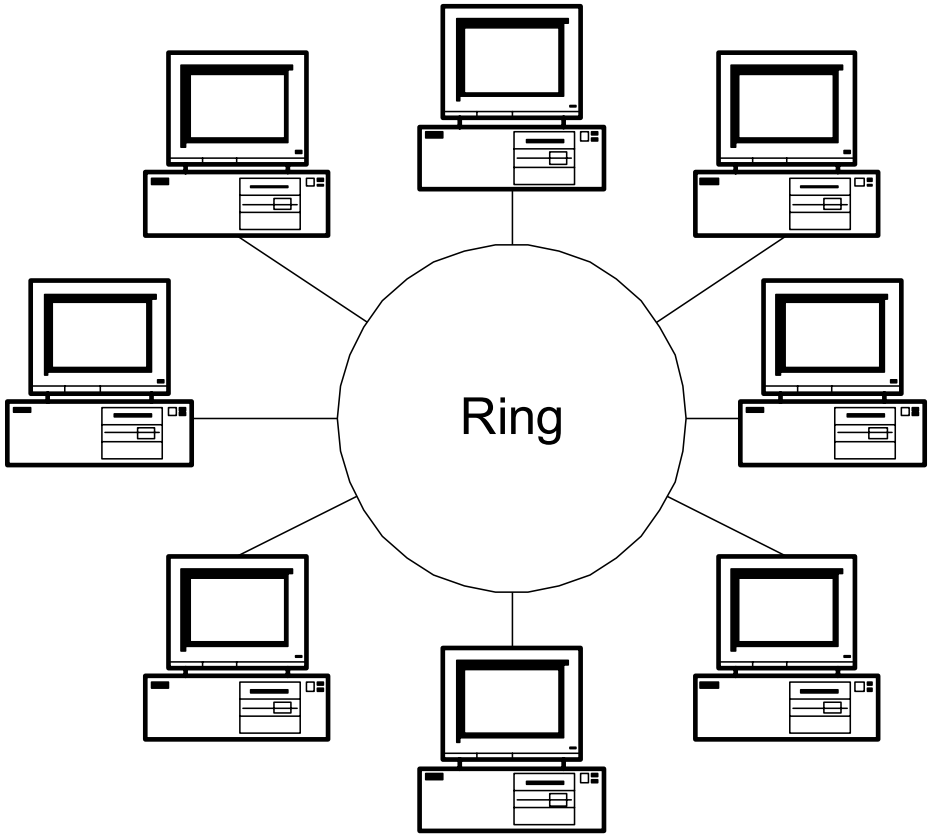
Erw. Stern – Eigenschaften

- Auch „Baumartig mit zentralen Teilvermittlern“ genannt
- Möglicher Zerfall in Teilnetze
- Mögliche Durchsatzengpässe zwischen den Teilvermittlern
- Als Vermittler heute i.a. Switches im Einsatz

Erw. Stern – Bewertungskriterien

Modularität	Sehr gut!!!
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1
Stabilitäts- und Rekonfigurationsverhalten	Gut (!ZTV)
Logische Komplexität	Einfach
Durchsatzkapazität	„ZTV-ZTV“

Ring



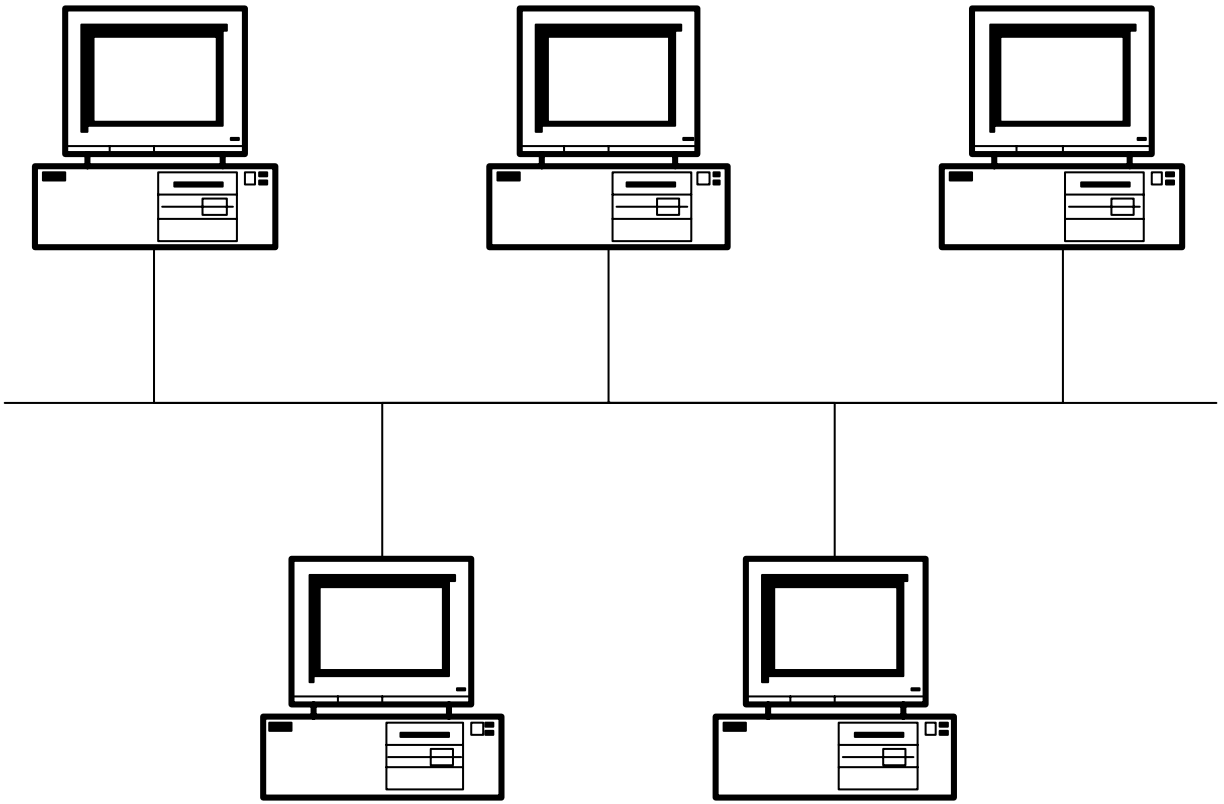
Ring – Eigenschaften

- Kann mit oder ohne zentralem Vermittler betrieben werden
- Uni- oder bidirektionaler Betrieb möglich
- Kopplung mehrerer Ringe machbar (meist bei ZV)
- Heute i.a. unidirektional ohne ZV

Ring – Bewertungskriterien

Modularität	Gut
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1(uni)/2(bi)
Stabilitäts- und Rekonfigurationsverhalten	Schlecht
Logische Komplexität	Einfach
Durchsatzkapazität	„Ringgröße“

Bus



Bus – Eigenschaften

- Alle Stationen sind an ein gemeinsames Medium (Bus) angeschlossen.
- Zugriffsverfahren besonders wichtig
- Abhörsicherheit problematisch
- Broadcastmöglichkeit

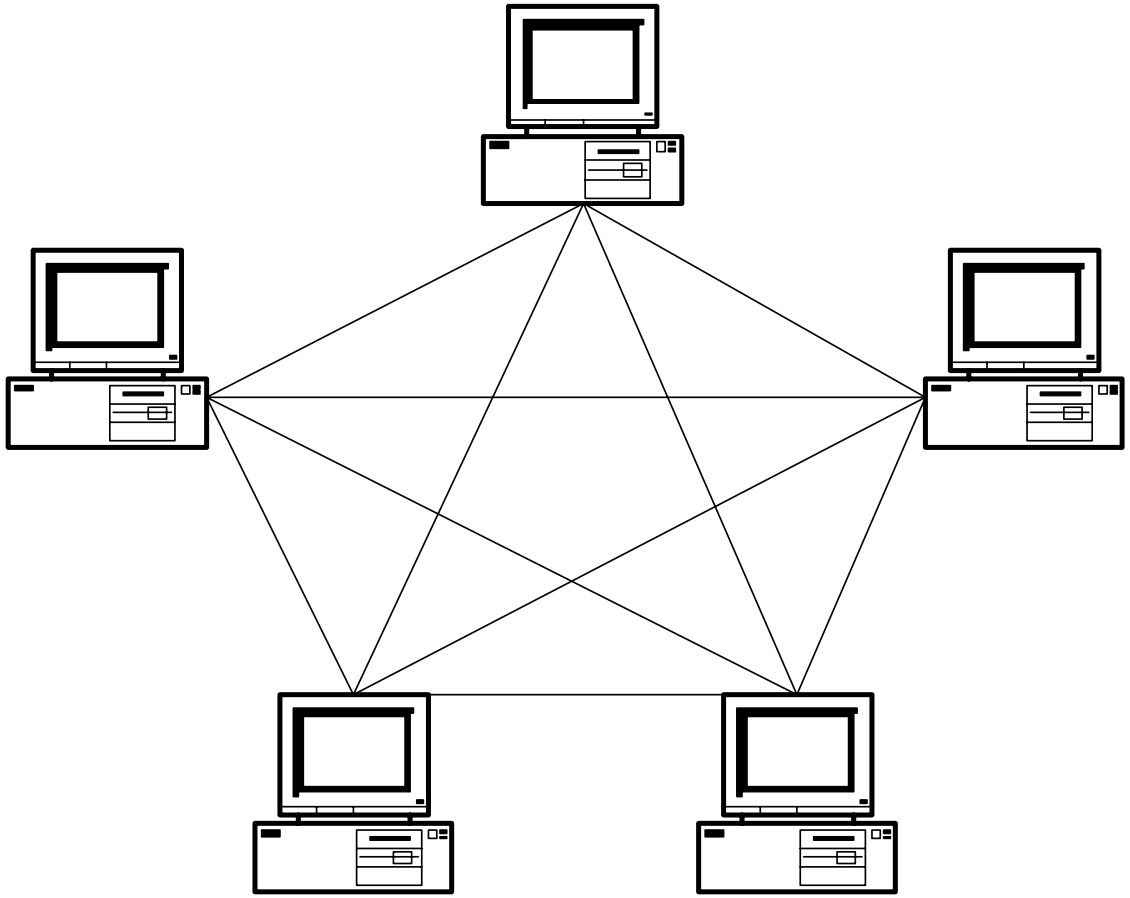
Bus – Bewertungskriterien

Modularität	Sehr gut
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1
Stabilitäts- und Rekonfigurationsverhalten	Gut
Logische Komplexität	Einfach
Durchsatzkapazität	„Medium“

I.7.4. Besondere Topologien

- „Der vollständige Graph“
- „Reguläre Strukturen“
- Liniennetz
- Bus mit zentralem Vermittler
- Unregelmäßige Strukturen

„Der vollständige Graph“



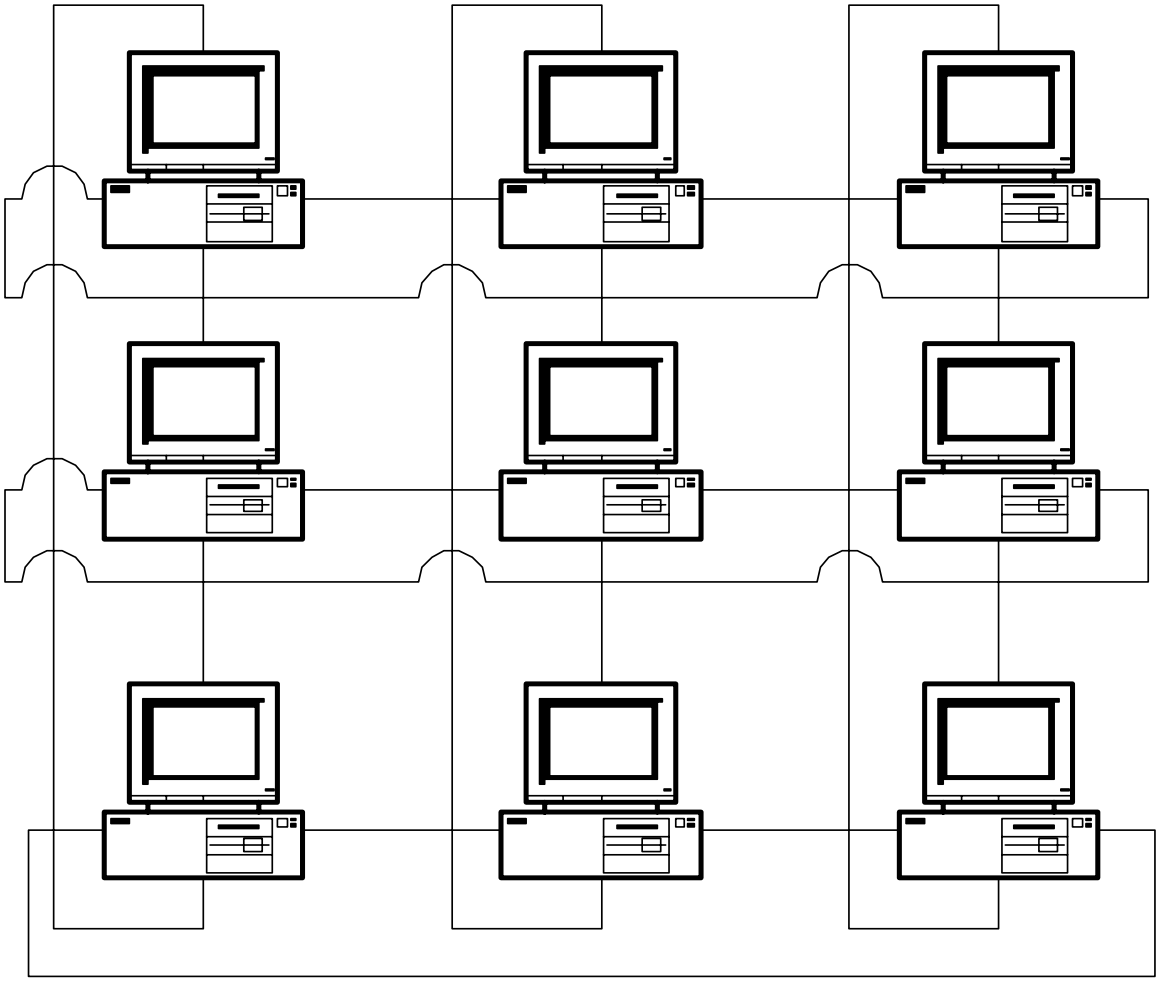
Vollst. Graph – Eigenschaften

- Jeder Knoten (N) ist mit jedem anderen Knoten verbunden
- Zwei Betriebsarten
  - Indirekt (mit Routing)
  - Direkt (ohne Routing)
- Nur bei kleiner Anzahl (<20) sinnvoll
- Hohe Störsicherheit und hohe Kosten

Vollst. Graph – Bewertungskrit.

Modularität	Sehr schlecht
Modularität der Kosten	Sehr schlecht
Zusammenhangsgrad	N-1
Stabilitäts- und Rekonfigurationsverhalten	Gut/Schlecht
Logische Komplexität	Aufwendig/Einf.
Durchsatzkapazität	Sehr gut

„Reguläre Strukturen“



Reg. Strukt. – Eigenschaften

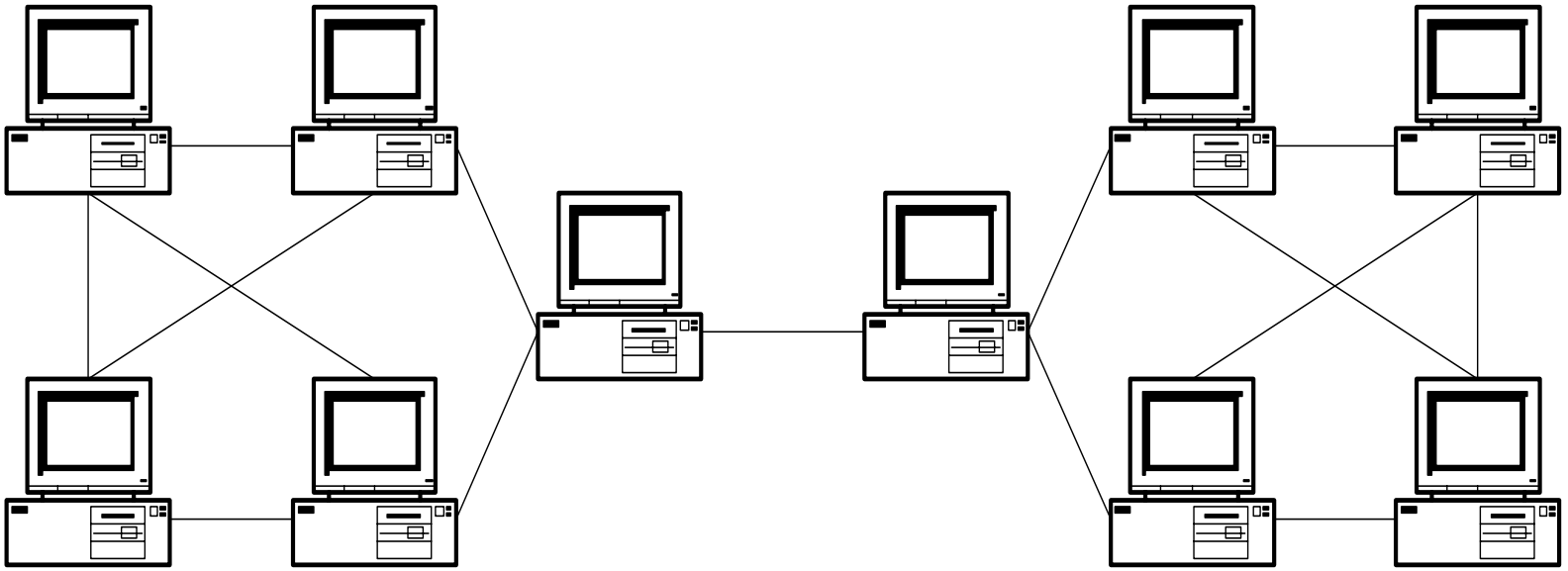
- Jeder Knoten hat die gleich Anzahl von nächsten Nachbarn (n)
- Bei manchen n Randproblem (3,5)
- Große (>6) n selten
- Für Sonderfälle gelten die Bewertungs-kriterien nicht vollständig (s. Beispiel)
- Der vollständige Graph und der Ring sind ebenfalls Sonderformen

Reg. Strukt. – Bewertungskrit.

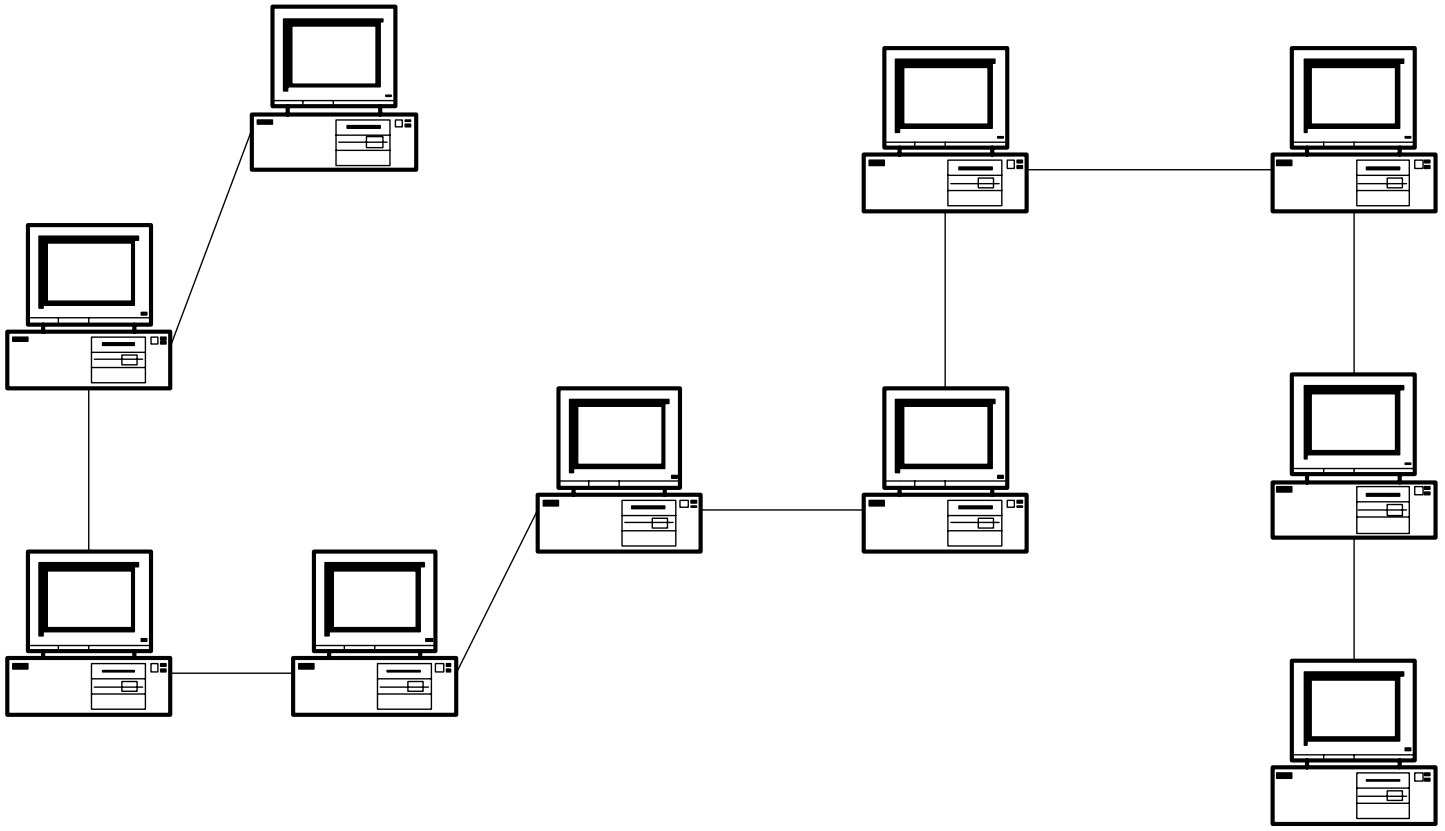
Modularität	Mäßig
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	n
Stabilitäts- und Rekonfigurationsverhalten	Gut
Logische Komplexität	Mittel
Durchsatzkapazität	Gut

Reguläre Struktur - Sonderfall

Drei nächste Nachbarn, trotzdem ist der Zusammenhangsgrad nur 1



Liniennetz



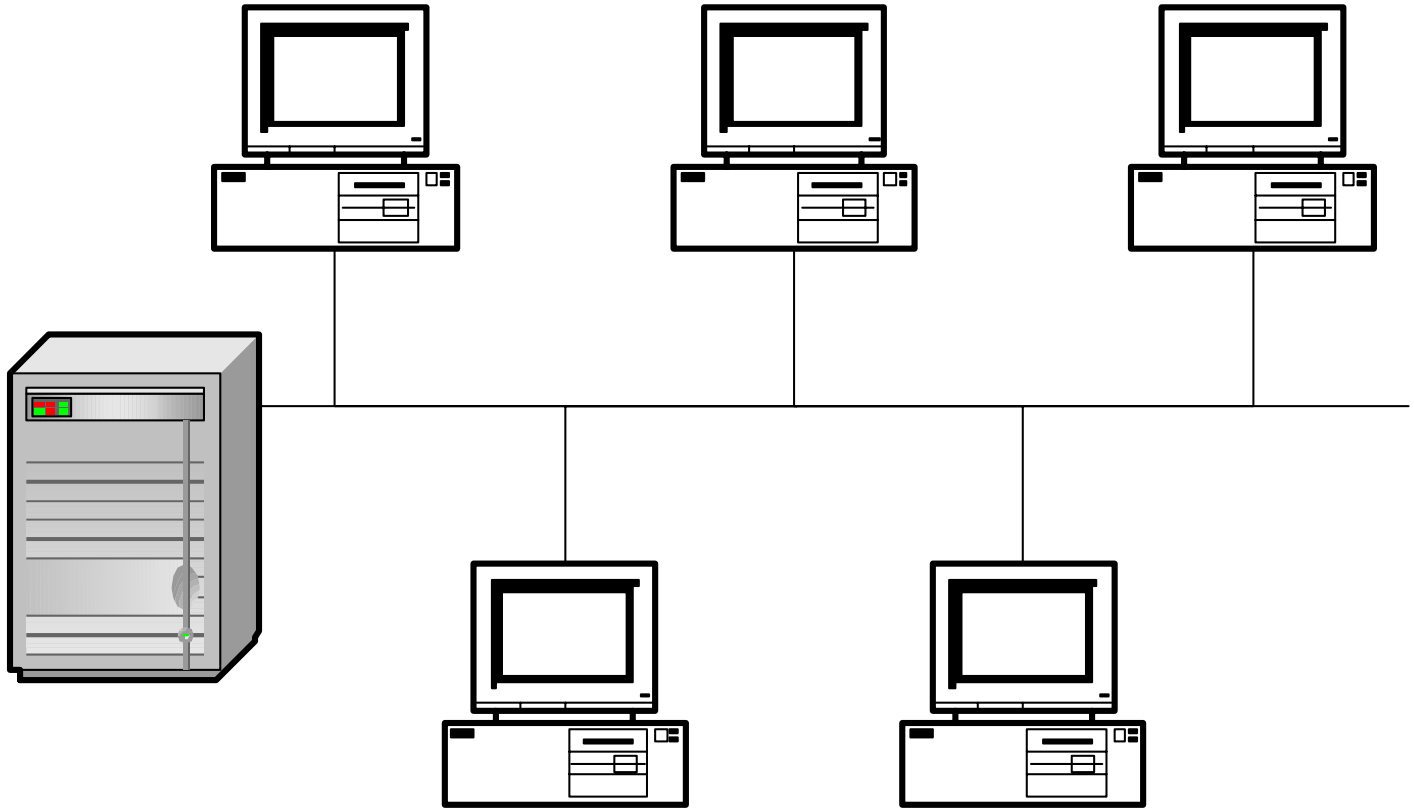
Liniennetz – Eigenschaften

- Die Knoten sind linear angeordnet
- Minimale Leitungsanzahl
- Mittlere Leitungen stärker belastet als die Randleitungen
- Durch eine zusätzliche Leitung zu einem Ring erweiterbar

Liniennetz – Bewertungskriterien

Modularität	Gut
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1
Stabilitäts- und Rekonfigurationsverhalten	Schlecht
Logische Komplexität	Einfach
Durchsatzkapazität	Schlecht

Bus mit zentralem Vermittler



Bus m. ZV – Eigenschaften

- Alle Nachrichten werden von den Knoten zu einem zentralem Vermittler übertragen und werden von diesem an das Ziel gesandt.
- Mangelnde Abhörsicherheit
- Broadcastfähigkeit
- Beispiel: Funknetze mit Benutzermobilität

Bus m. ZV – Bewertungskriterien

Modularität	Abh.v.Zugriffsv.
Modularität der Kosten	Sehr gut
Zusammenhangsgrad	1
Stabilitäts- und Rekonfigurationsverhalten	Gut (!ZV)
Logische Komplexität	Einfach
Durchsatzkapazität	„Medium/2“

Unregelmäßige Strukturen

- Durch das Zusammenwachsen verschiedener Netze entstehen oft unregelmäßige Strukturen (verschiedene Teile bestehen aus unterschiedlichen Topologien)
- Die Bewertungskriterien sind daher sinnvoll nur auf Teile des Netzes anwendbar

II. LAN – Übersicht

1. Definition
2. Begriffe
3. Grundlagen
4. Systemübersicht
5. Netware
6. Windows Server
7. Linux
8. Vergleich (Kurzfassung)

II.1. LAN – Definition

Lokale Netze sind Datenkommunikations-systeme, welche einer Anzahl von **unabhängigen Einrichtungen** eine zumeist **partnerschaftlich orientierte** Kommunikation **hoher Datenrate** auf relativ **begrenztem geographischen** Gebiet ermöglichen.

II.2. LAN – Begriffe

Account

- Zugangsberechtigung zu einem System (meist mit Namen und Kennwort) mit dem ein Set von Berechtigungen und Dateien in diesem System verbunden ist.

II.2. LAN – Begriffe

Client

- Nutzer (Anwender, Programm, Computer, …) von Diensten, die ein Server zur Verfügung stellt.

II.2. LAN – Begriffe

Dateisystem

- System zur Verwaltung von Daten auf einem Datenträger (Festplatte).

II.2. LAN – Begriffe

Mehrbenutzersystem

- Ein Computersystem, bei dem mehr als eine Person gleichzeitig Zugriffsmöglichkeiten besitzen (mit den damit verbundenen Auswirkungen auf das Dateisystem bzw. die Systemresourcen)

II.2. LAN – Begriffe

Netzwerk

- Verbindung mehrerer Computer über ein Kommunikationsmedium (Kabel, opt. Fasern, Funk, …) und mittels geeigneter Software. Die Unterscheidung in LAN, WAN, MAN, CAN ist üblich.

II.2. LAN – Begriffe

Server

- Ein System (Computer, Programm, …), das Dienste für andere zur Verfügung stellt (z.B.: Fileserver, Printserver, Databaseserver, Timeserver, Communicationserver, Mailserver, …).

II.2. LAN – Begriffe

Requester/Redirector

- Ein „Zwischenprogramm“, das in mehrere Richtungen kommuniziert und so dem Anwender standardisierte Dienste zur Verfügung stellt.
- Client-OS $\leftrightarrow$ Requester $\leftrightarrow$ NOS. (WinXP$\leftrightarrow$Requester$\leftrightarrow$Netwareserver)

II.2. LAN – Begriffe

Transparent

- Den Begriff transparent verwendet man im Zusammenhang mit Netzwerken für die Eigenschaft eines Netzwerkes für den Anwender möglichst verborgen, also durchsichtig zu erscheinen.

II.2. LAN – Begriffe

Workstation

- Eine Workstation ist ein allgemeinerer Begriff für PC, d.h. es ist ein Computersystem, an dem i.a. eine Person ihre Arbeit erledigt. In früheren Klassifikationen von Computersystemen waren Workstations die leistungsfähigere Variante eines PC´s.

II.3. LAN-Grundlagen

- Netzwerknormen
- Protokolle
- Netzwerkdevices
- Bandbreite – Geschwindigkeit
- Verzeichnisdienste

II.3.a. Netzwerknormen

- Im Rahmen von Referaten wurden schon behandelt:
  - IEEE 802.3-Familie (Ethernet, Fastethernet, Gigabit-Ethernet)
  - IEEE 802.11 (WLAN, WiFi)

II.3.b. Protokolle

- Im Rahmen von Referaten wurden schon behandelt:
  - IP-Protokoll-Familie (IP, ICMP, TCP, FTP, POP3, SMTP, …)
- In anderen Gegenständen wurden schon behandelt:
  - Subnetting

II.3.c. Netzwerkdevices

- Repeater
- Hub
- Bridge
- Switch
- Access Point
- Router
- Gateway

Repeater

- Repeater sind reine Signalverstärker, die keinerlei Prüfung der Frames (Rahmen) vornehmen, sondern nur die physischen Signale auf einem Port (Anschluß) empfangen und auf einem anderen Port neu versenden, wodurch größere Entfernungen erreichbar sind.
- Arbeiten in ISO-Schicht 1

Hub

- Hubs sind Multiportrepeater
- Arbeiten in ISO-Schicht 1
- Trennen daher keine „Collision-Domains“
- Gemeinsame Bandbreite für alle angeschlossenen Geräte

Bridge

- Bridges empfangen einen Frame und versenden ihn nach Prüfung neu.
- Arbeiten in den ISO-Schichten 1 und 2.
- Trennen „Collision-Domains“
- Unterschieden werden:
  - MAC-Bridges
  - LLC-Bridges

Switch

- Switches sind Multi-Port-Bridges.
- Arbeiten in den ISO-Schichten 1 und 2.
- Trennen „Collision Domains“
- Unterschieden werden:
  - Cut through
  - Store and Foreward
  - Error free cut through

Access Point

- Ein Access Point verbindet (bridged) wireless Segment mit wired Segmenten eines Netzwerkes oder nur wireless Komponenten.
- Arbeitet in den ISO-Schichten 1 und 2.
- Trennt „Collision-Domains“

Router

- Ein Router dient der Vermittlung von Netzwerkpaketen. An Hand der Zieladresse und einer Subnetmaske (Routingtabelle) wird entschieden, wie das Paket weitergeleitet wird.
- Arbeitet in ISO-Schicht 3
- Man unterscheidet Routingprotokolle und geroutete Protokolle.

Gateway

- Zur Verbindung von Netzwerken mit verschiedenen Strukturen (z.B.: ISO und nicht-ISO) werden Gateways benutzt.
- Verbindungen auf höherer ISO-Schicht als 3 werden ebenfalls mit Hilfe von Gateways realisiert.

II.3.d. Bandbreite

- Die Geschwindigkeit der Signale ist in allen Medien die Lichtgeschwindigkeit (daher ist die Aussage, ein Netzwerk ist langsam nicht zutreffend).
- Die Bandbreite ist die übertragbare Informationsmenge pro Zeiteinheit (und damit ein wichtiges Kriterium).

II.3.e. Verzeichnisdienst

- Verzeichnisdienst - Was ist das?
- Warum?
- Vorteile für den Benutzer
- Vorteile für den Administrator
- Standards

Was ist ein Verzeichnisdienst?

- Ein zentraler Informationsspeicher der Netzwerkumgebung
- Nicht gebunden an einen oder mehrere physikalische Standorte
- Hierarchisch aufgebaut
- Plattformunabhängig
- Standardisiertes Zugriffsprotokoll

Beispiel DNS

- Im Internet wird – meist transparent – der DNS-Dienst für die Zuordnung von DNS-Namen zu IP-Adressen verwendet.
- Plattformunabhängig, hierarchisch, standardisiert
- Nur eine Aufgabe

Aufbau

- Container
  - Firma, Abteilung, ...
- Objekte
  - Benutzer, Server, ...
- Eigenschaften
  - Werte der Objekte (z.B.: e-Mailadresse eines Benutzers, ...)

Anforderungen

- anpaßbar an Firmenstruktur
- Integration aller Netzwerkkomponenten
- Standardobjekttypen (User, Drucker, ...)
- freie Objekttypen
- Sinnvolle Standardattribute (e-Mail, ...)
- Definition freier Attribute

Warum Verzeichnisdienste?

- Reduktion der Benutzer- bzw. Ressourcenverwaltung
  - e-Mail-Systeme
  - Netzwerbetriebssysteme
  - Anwendungsprogramme
- Vereinheitlichung der Parameter und der Suche danach

Ressourcen

- Dateien
- Verzeichnisse
- Datenbanken
- Dienste
- Druckerwarteschlangen
- Drucker
- Speichereinheiten
- Gateways
- Server
- Arbeitsstationen
- Anwendungen
- ...

Angaben (Beispiele)

- Mitarbeitern
  - (Name, Adresse, Telephonnummer, ...)
- Ressourcen
  - (Drucker: Standort, Fähigkeiten, ...)
- Zugriffsmöglichkeiten
- Zugriffsrechte
- Verfügbare Anwenderdienste

Einsatzmöglichkeiten

- Wie ist die Telephonnummer von X?
- Wie lautet die e-Mail-Adresse von y?
- Wo ist die Anwendung z?
- Wie melde ich mich an die Datenbank abc an?
- Wo ist der aktuelle Geschäftsbericht?
- Wo ist ein Farbdrucker?
- ...

Nachteile für den Benutzer

- Umstellung auf ein neues System
- Namen gewohnter Dienste können länger werden, da sie in einem Kontext gesehen werden müssen

Vorteile für den Benutzer

- Einfache Abfrage von Informationen zu einem Objekt
- Nur ein(?) Passwort
- Keine Notwendigkeit über Änderungen im Netz informiert zu werden (Änderung von Speicherplätzen, Faxdiensten, ...)
- Transparenter Zugriff auf Objekte

Nachteile für den Administrator

- Umstellung

Vorteile für den Administrator

- „Single Point of Administration“
- Änderungen in der Netzwerkinfrastruktur bleiben für den Benutzer transparent
- Weniger Benutzerunterstützung notwendig

Standards

- ISO/IEC 9594/ITU-TS X-500
  - Basisnorm für alle Verzeichnisdienste
- ENV 41210
  - DAP (Directory Access Protocol)
- LDAP (Lightweight DAP)
  - Derzeitiger Defacto-Standard mit dem verschiedene Verzeichnisdienste kommunzieren

X.500

- DIT (Directory Information Tree)
- DN (Distinguished Name)
  - global eindeutig
- RDN (Relative Distinguished Name)
- CN (Common Name)
- @c=AT@o=BUAK@ou=EDV@cn=xyz

LDAP

- Defacto-Standard für die Kommunikation verschiedener Verzeichnisdienste
- RFC 1777 (März 1995) LDAPv2
- RFC 2251 (Dezember 1997) LDAPv3
- cn=xyz, ou=EDV, o=HTBLVA, c=AT

Übersicht – Verzeichnisdienste

- Laut der US-Vereinigung Network Applications Consortium gibt es nur zwei die den Namen Verzeichnisdienst verdienen:
  - Banyan Streettalk
  - Novell NDS/e-Directory

Übersicht – Verzeichnisdienste 2

- Daneben noch:
  - IBM Secure Directory (-> NDS)
  - IBM/Lotus NAB (Namen- und Adressbuch, geplant in NDS überzuführen)
  - Microsoft ADS
  - Netscape Directory Server

II.4. Systemübersicht

- Arten von Systemen
- PC-Netze am Markt
- Sonstiges

Arten von Systemen

- Peer-To-Peer Netze (Windows xx Freigaben, ...)
- Client-Server-Netze (Netware, Windows NT Server, Unix, ...)
- Zentrallösungen (Mainframe, Unix-Systeme, ...)
- Mischsysteme

Überblick PC-Netze

• Novell	Netware
• Microsoft	NT/2000 Server
• Open Source	Linux
• DEC	Pathworks
• Banyan	Vines

Überblick Sonstiges

• Diverse	UNIX/NFS
• Compaq(DEC)	DECnet
• IBM	AS400
• IBM	Mainframe
• Siemens	Transdata
• ...	...

II.5. Netware

- Konzepte der Netware
- Workstation – Server-Verbindung
- Dateikonzepte
- Drucken – Klassisch
- Drucken – NDPS
- Zugriffsrechte und Dateiattribute
- Benutzeradministration

II.5.1. Konzepte

- Hardwarekonzepte
- Softwarekonzepte
- Clientanbindung
- eDirectory

II.5.1.1 HW-Konzepte

- Als Client alle gängige Systeme verwendbar (Windows, MacOS, Unix)
- Als Server i86-Plattform (NativeOS) oder als Task auf verschiedenen Plattformen (kaum Bedeutung)
- Als Netzwerktopologien werden alle am Markt verbreitete Topologien unterstützt (Ethernet, TokenRing, FDDI, …).

II.5.1.2 SW-Konzepte

- Durchgängiges Server-Clientkonzept, wobei folgende Server unterstützt werden:
  - Fileserver, Printserver, Timeserver, FTP-Server, Webserver, LDAP-Server, eDirectory-Server, …
  - Mailserver, Databaseserver, Communicationserver, …

II.5.1.3. Clientanbindung

- Netwareclientsoftware
  - Hardwaretreiber (für NIC, NDIS, ODI)
  - Protokolltreiber (TCP/IP, IPX/SPX)
  - Requester

- Native Clientaccess (SMB, AFP, CIFS)
- Internetaccess (iPrint, iFolder, …)

II.5.1.4. eDirectory

- Allgemeines
- Aufbau
- Objekttypen und deren Eigenschaften
- Kontext
- Partitionen und Replikationen
- Zeitsynchronisation
- Verwaltung

eDirectory – Allgemeines

- NDS als Netware Directory Services im Jahr 1994 mit Netware 4 als Nachfolger des Bindery-Systems eingeführt.
- Später auf Novell Directory Services umbenannt, da auch auf WindowsNT/2000 und Unix-System lauffähig
- Heute oft als e-Directory bezeichnet

Aufbau

- Baumartig mit drei Klassen von Objekten
  - Rootobject (Wurzel des Baumes; bezeichnet mit dem Pseudonamen [Root])
  - Containerobjects (C, O und OU)
  - Leafobjects (Blattobjekte, CN)

Rootobject

- Einmalig in einem Tree
- Der Name des Trees ist mit diesem Objekt verbunden
- Alle Eigenschaften für den gesamten Tree sind mit diesem Objekt verbunden (z.B.: B-Recht für [Public])

Containerobjects

- Nur Containerobjekte können weitere Objekte beinhalten
- Containerobjekte haben auch Eigenschaften für alle Objekte darin
- C Countryobject
- O Organisation Object
- OU Organizational Unit Object

Countryobject

- Countryobjects können nur in [Root] existieren
- Namen müssen die international üblichen Namen (ISO 3166-1) der Länder entsprechen
- Countryobjects können nur Objekte des Types O beinhalten.

Organisationobject

- Organisationobjects können in [Root] oder in Objekten des Typs C existieren
- Organisationobjects können OU- oder Leafobjects beinhalten
- Die Namen entsprechen üblicherweise den Firmennamen

Organizational Unit Object

- Diese Objekte können in Objekten der Typen O oder OU existieren.
- In diesen Objekten können weitere OU oder Leafobjekte untergebracht sein.
- Die Namen können frei gewählt werden, sollten aber „sprechend“ sein.

Leafobjects

- Blatt- oder Endobjekte stellen die eigentlichen Elemente des Netzwerkes dar.
- Je nach Art des Objektes sind hier verschiedene Eigenschaften möglich (z.B.: Drucker hat einen Standort, Benutzer?)

Leafobjekttypen

- Einige Standardtypen:
  - AFP-Server
  - Alias
  - User (Benutzer)
  - Workstation (Computer)
  - Volume (Datenträger)
  - Group (Gruppe)
  - Server
  - Profile (Profil)

Leafobjekttypen 2

- Einige Standardtypen:
  - Directory (Verzeichniszuordnung)
  - Role (Organisatorische Funktion)
  - License (Lizenz)
  - Application (Anwendungsprogramm)
  - Printer (Drucker)
  - Printserver (Druckserver)
  - Queue (Warteschlange)
  - NDPS-Broker (NDPS-Vermittler)

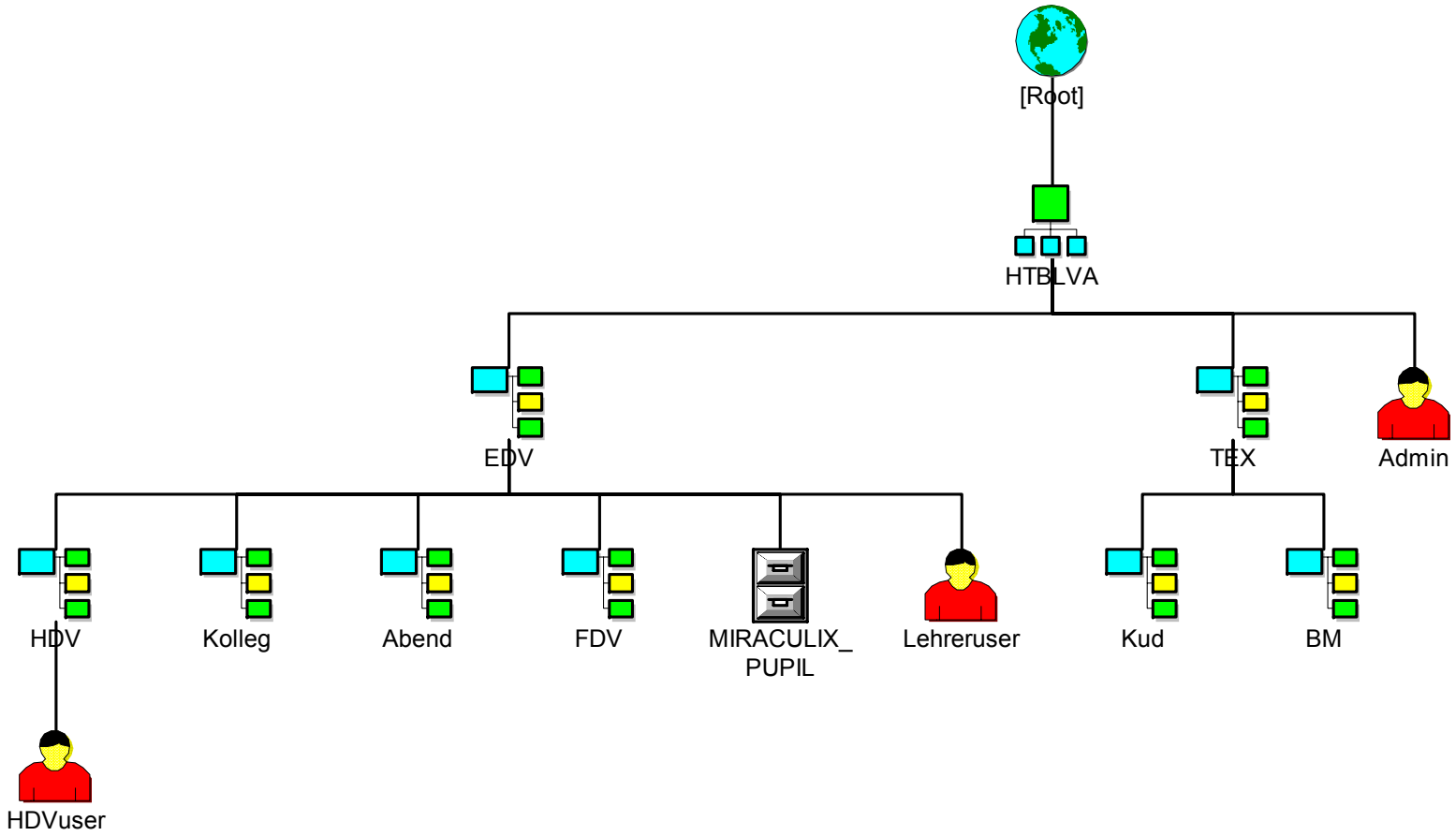
Leafobjekttypen 3

- Neben den Standardtypen sind noch beliebige Erweiterungen möglich:
  - fw1 User
  - Bagger
  - Kran
  - Flugzeug
  - ...

Kontext

- Um ein Objekt korrekt zu beschreiben muß der DN verwendet werden.
- Der Kontext ist jener Teil des DN, der zum CN hinzugefügt werden muß.
- Ein „Default Context“ (Standard Kontext) spart die Angabe des Kontexts für Objekte in diesem Kontext.

Beispiel


[Root]
HTBLVA
EDV
TEX
Admin
HDV
Kolleg
Abend
FDV
MIRACULIX_
PUPIL
Lehreruser
Kud
BM
HDVuser

Beispiel (1)

- Kein Countryobject
- Ein Organisationobject names HTBLVA
- Viele OU-Objects
- Viele Leafobjects von denen nur drei Benutzer und ein Volume eingezeichnet ist.

Beispiel (2)

- Der Name des Benutzers Admin:
  - <treename>/cn=admin.o=htblva oder kurz
  - <treename>/admin.htblva
- Der RDN des Benutzers Admin
  - im Kontext HTBLVA: cn=admin
  - im Kontext [Root]: cn=admin.ou=htblva
  - im Kontext Kolleg.EDV.HTBLVA: admin..

Beispiel (3)

- DN des Objektes MIRACULIX_PUPIL:
  - MIRACULIX_PUPIL.EDV.HTBLVA
- RDN des Objektes:
  - Kontext EDV.HTBLVA: MIRACULIX_PUPIL
  - Kontext HDV.EDV.HTBLVA: MIRACULIX_PUPIL.
  - Kontext HTBLVA: MIRACULIX_PUPIL.EDV

Eigenschaften

- Jedes Objekt im eDirectory hat Eigenschaften (Properties)
- Containereigenschaften beziehen sich oft auf alle Objekte im Container
- Mögliche Eigenschaften im Schema beschrieben
- Eigenschaften können optional oder mandatory sein

Eigenschaften von Organisations

- Name
- Login Script
- Rechte

Eigenschaften von Volumes

- Name
- Host Server
- Host Volume
- Version

Eigenschaften von Benutzern

- First Name, Last Name, Full Name
- UserID (Login Name)
- Key Material
- e-Mail-Address
- Title, Telephone Number, Address
- Home Directory Volume, Home Directory Path

Eigenschaften von Benutzern 2

- Account Ablaufdatum
- Password Parameter
- Gruppenmitgliedschaften
- Beschränkung gleichzeitiger Verbindungen
- Last Login
- …

Eigenschaften von Gruppen

- Name
- Description
- Members
- Rights to Files and Directories
- …

Partitionen

- Ein NDS-Baum kann in mehrere Partitionen aufgeteilt werden
- Ein Aufteilung hat nur dann Sinn, wenn mehrere Server vorhanden sind
- Von jeder Partition existieren standard-mäßig 2 Kopien (Replikationen)

Replikationen

- Replikationen sind Kopien aller Daten einer Partition
- Automatische Erstellung
- Manuelle Erstellung

Replikationstypen

- Masterreplikation (Masterreplica)
- [Gefilterte] Schreiben/Lese-Replikation ([Filtered] Read-Write-Replica)
- [Gefilterte] Nur-Lese-Replikation ([Filtered] Readonly-Replica)
- Linkreplikationen (Subordinate Reference Replica)

Zeitsynchronisation

- Damit mehrere Server korrekt mit e-Directory arbeiten können muß(!) eine einheitliche Zeit im System herrschen
- Alle Server haben daher intern UTC (gleich GMT = MEZ-1Stunde/2Stunden)
- Zusätzlich wird die lokale Zeit für die Anzeige verwendet (aus UTC gebildet).

Zeitservertypen

- SINGLE REFERENCE
- REFERENCE
- PRIMARY
- SECONDARY

SINGLE REFERENCE

- Die Uhrzeit dieses Server wird als Referenz für das Netzwerk verwendet.
- Daneben nur SECONDARY Timeserver sinnvoll.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

REFERENCE

- Referenzzeitserver, der allerdings mit anderen Zeitservern die Netzwerkzeit abstimmt (seine eigene Zeit aber nicht daran anpaßt).
- Daneben sind SECONDARY und PRIMARY Timeserver möglich.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

PRIMARY

- Zeitserver, der mit anderen Zeitservern (PRIMARY oder REFERENCE) die Netzwerkzeit abstimmt.
- Daneben sind SECONDARY, PRIMARY und REFERENCE Timeserver möglich.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

SECONDARY

- Zeitserver, der selbst seine Uhrzeit von anderen Zeitservern (PRIMARY, SINGLE REFERENCE oder REFERENCE) bekommt.
- Die Uhrzeit wird auch Clients bzw. auf Wunsch auch per NTP zur Verfügung gestellt.

Namensgebung

- In eDirectory-Namen sollten folgende Zeichen nicht verwendet werden

  . [,] + =

- Möglich sind aber auch diese mit dem \ (=Fluchtsymbol) davor
- 47 Zeichen maximale Länge für Namen, die SAP (Service Advertising) benötigen
- Richtlinien für Namensgebung sinnvoll

Richtlinien Namensgebung

- Damit später der Baum durchsucht werden kann.
- Genaue Beschreibung der Namensbildung
- Genaue Beschreibung der Schreibweise und der Trennzeichen
- Strikte Einhaltung (!)

Beispiele Namensgebung

- Login Name
  - Erster Buchstabe Vorname
  - Familienname (hhabicht)
- Telefonnummer
  - Internationale Schreibweise (+49 89 5475)
- Full Name
  - Vorname Zuname (Hugo Habicht)

Rechte

- Rechte auf Dateien bzw. Verzeichnisse
  - Ähnlich NTFS
- Rechte auf Objekte
  - Rechte auf Objekte in der NDS (i.a. keine Auswirkungen auf Dateien)
- Rechte auf Eigenschaften von Objekten

Objektrechte

- B Browse Umsehen
- C Create Erstellen
- D Delete Löschen
- R Rename Umbenennen
- S Supervisor Verwalter

Eigenschaftsrechte

- A Add Self Eig. Objekt anfügen
- R Read Lesen
- W Write Schreiben
- C Compare Vergleichen
- S Supervisor Verwalter

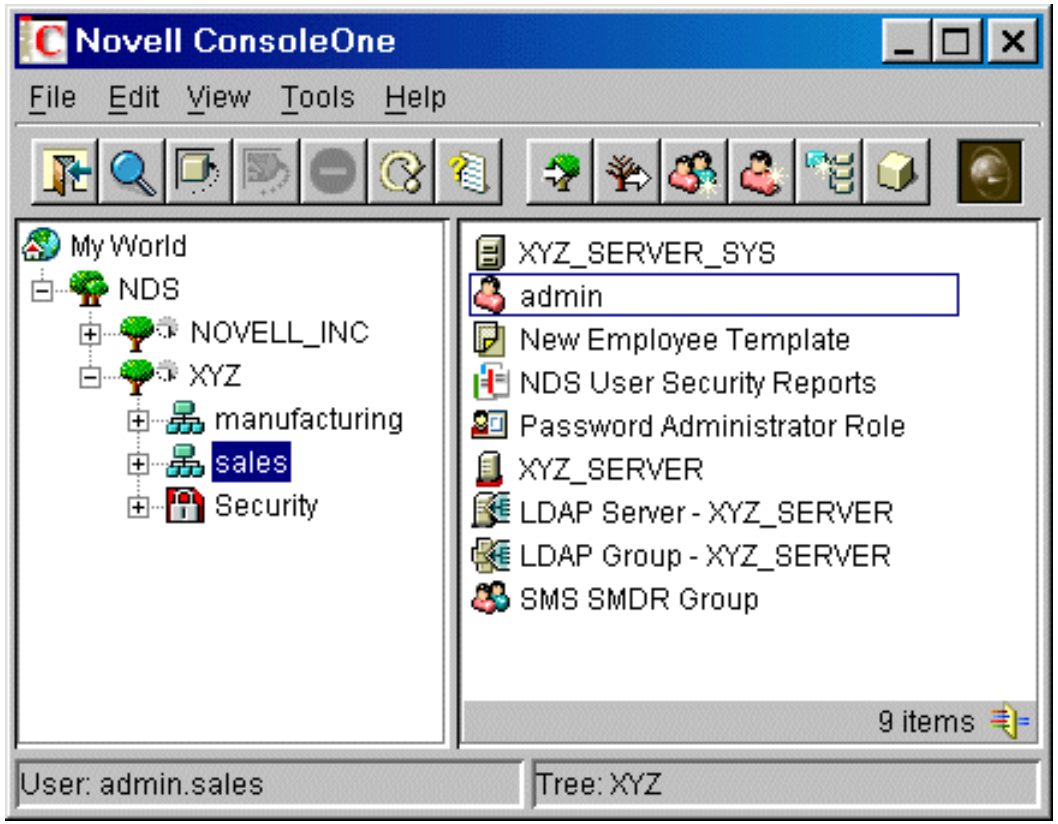
NWADMIN

- Netware Administrator-Utility (NWADMN32.EXE) dient der Verwaltung der NDS und der Netware-Server
- Wenn die NDS nicht auf Netware-systemen installiert ist, wenig hilfreich.

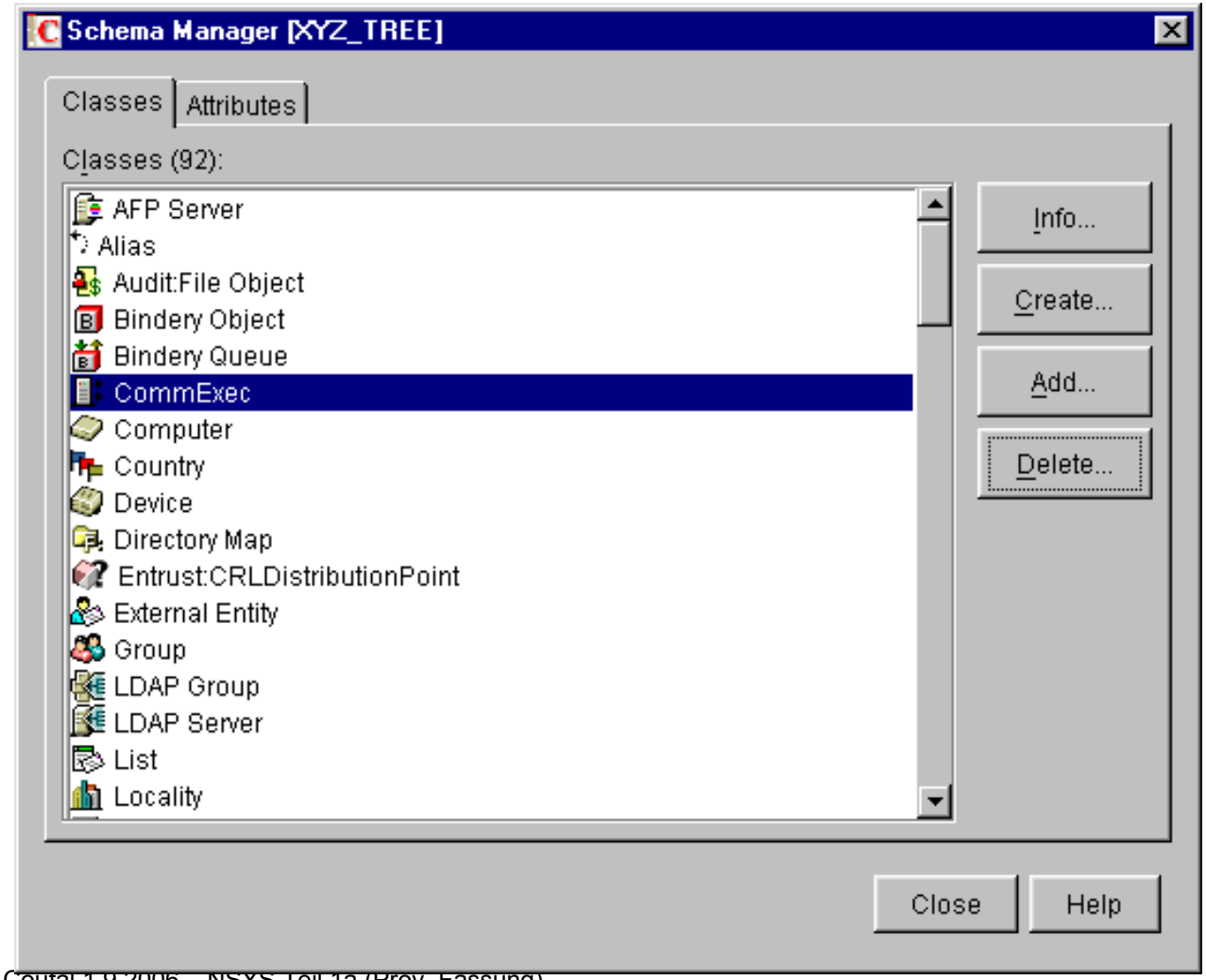
ConsoleOne

- Java-basierendes Werkzeug zur Verwaltung des e-Directories.
- SnapIn fähig, d.h. Zusatzprodukte mit SnapIn sind ebenfalls mit der ConsoleOne administrierbar

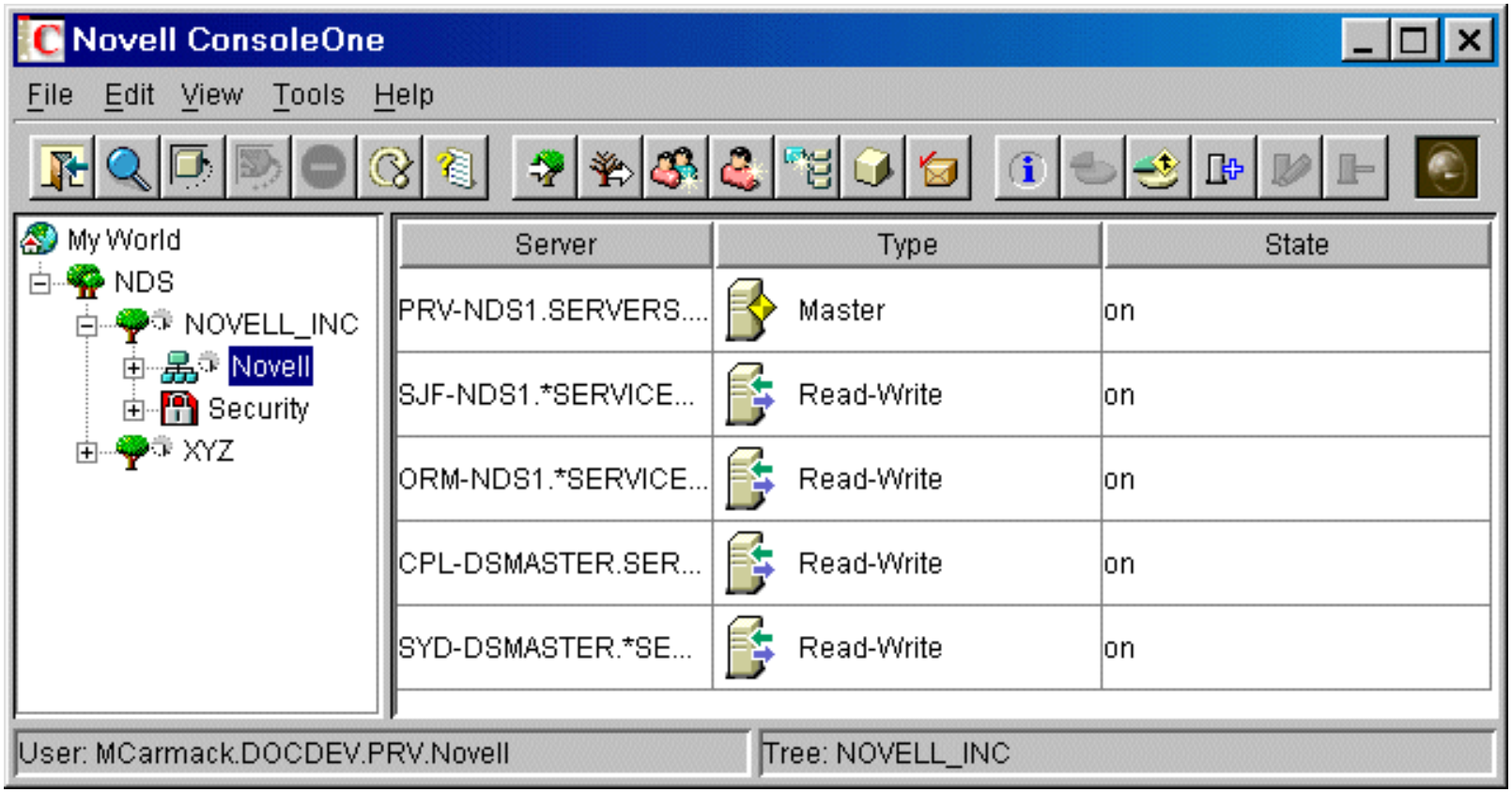
ConsoleOne 2



ConsoleOne 3



ConsoleOne 4



iMonitor

- Webbasierendes Monitoring und Diagnosetools
- eDirectory Zustandsübersicht
- Fehlermonitoring
- Verbindungsübersicht

iManager

- Webbasierende Verwaltung des eDirectories
- Nachfolger der ConsoleOne
- Ebenfalls durch PlugIns erweiterbar
- Rollenbasierendes Management möglich

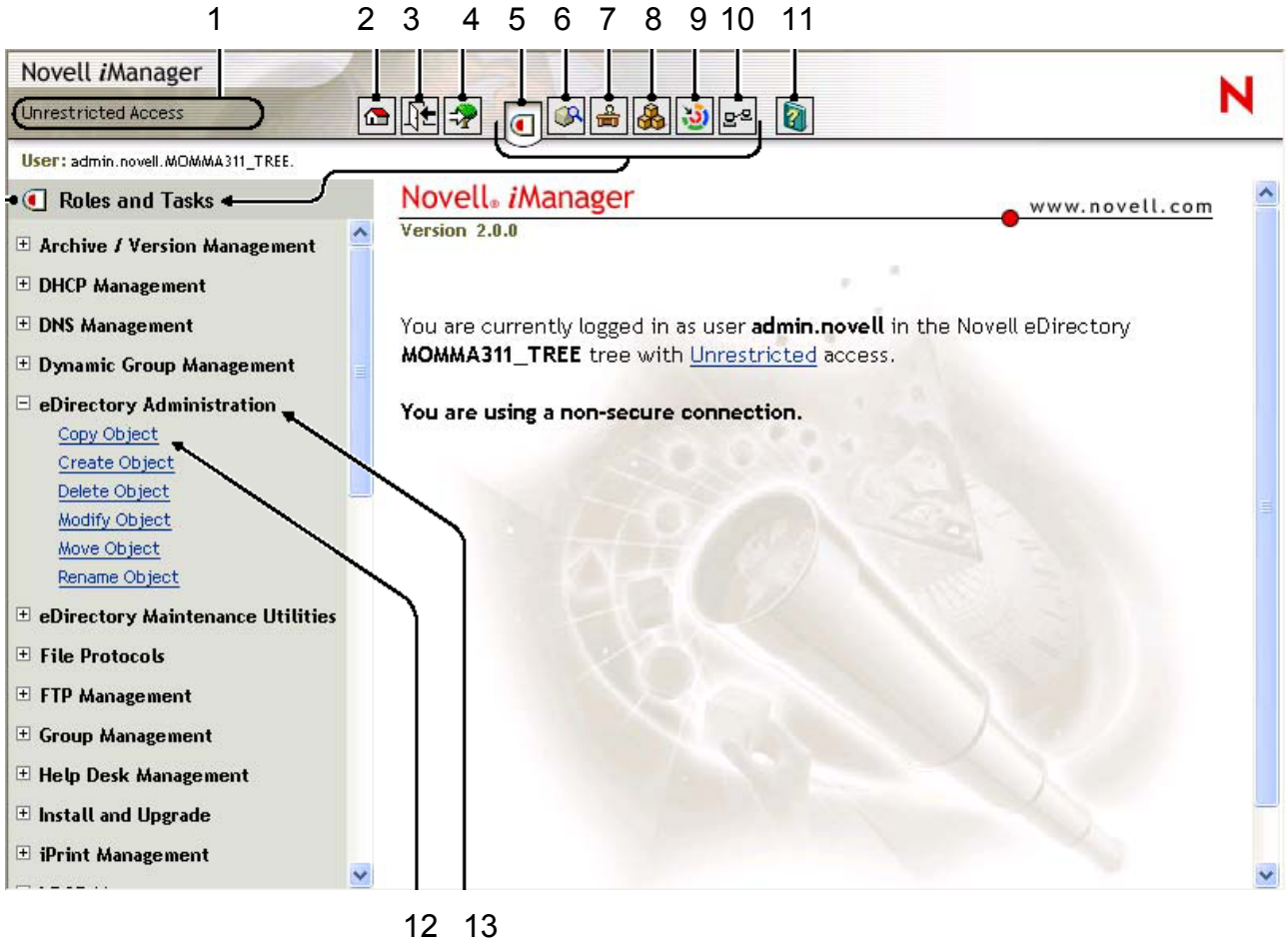
Anmelden an den iManager

- http://<server>/nps/iManager.html
- Benutzername und Passwort notwendig
- Rechte des Benutzers aktiv
- Für Accessibility Optionen:
  http://<server>/nps/Simple.html

Bedienung

- Grundlegende Benutzung
- RBS (Role Based Services)

iManager Interface



1 Zugriffsmode

2 Anfang

3 Verlassen

4 Anmelden

5 Rollen & Tätigkeiten

6 Objektansicht

7 Konfiguration

8 Entwickler

9 Portal Service

10 Monitor

11 Hilfe

12 Tätigkeit (Task)

13 Rolle

iManager Zugriffsmodes

- Unrestricted
  - Anzeige aller Rollen und Tätigkeiten
- Assigned
  - Rollen und Tätigkeiten für den Benutzer
- Collection owner
  - Mehrere Rollen für eine Sammlung

iManager Sonderzeichen

- NDS
  - . = + \
- LDAP
  - DN: , = + \ ; < >
  - Führende #
  - Führende oder am Ende befindliche „ “

Standard Rollen

- Dynamic Groups
- eDirectory Administration
- Groups
- Help Desk
- Partition and Replicas
- Rights
- Schema
- Servers
- Users

Weitere Rollen

- Nach Installation der RBS stehen weitere Services zur Verfügung:
  - eDirectory Maintenance
    - Backup and Restore
    - DB-Reparatur
    - Basisreparatur
    - Schemareparatur
    - …
  - …

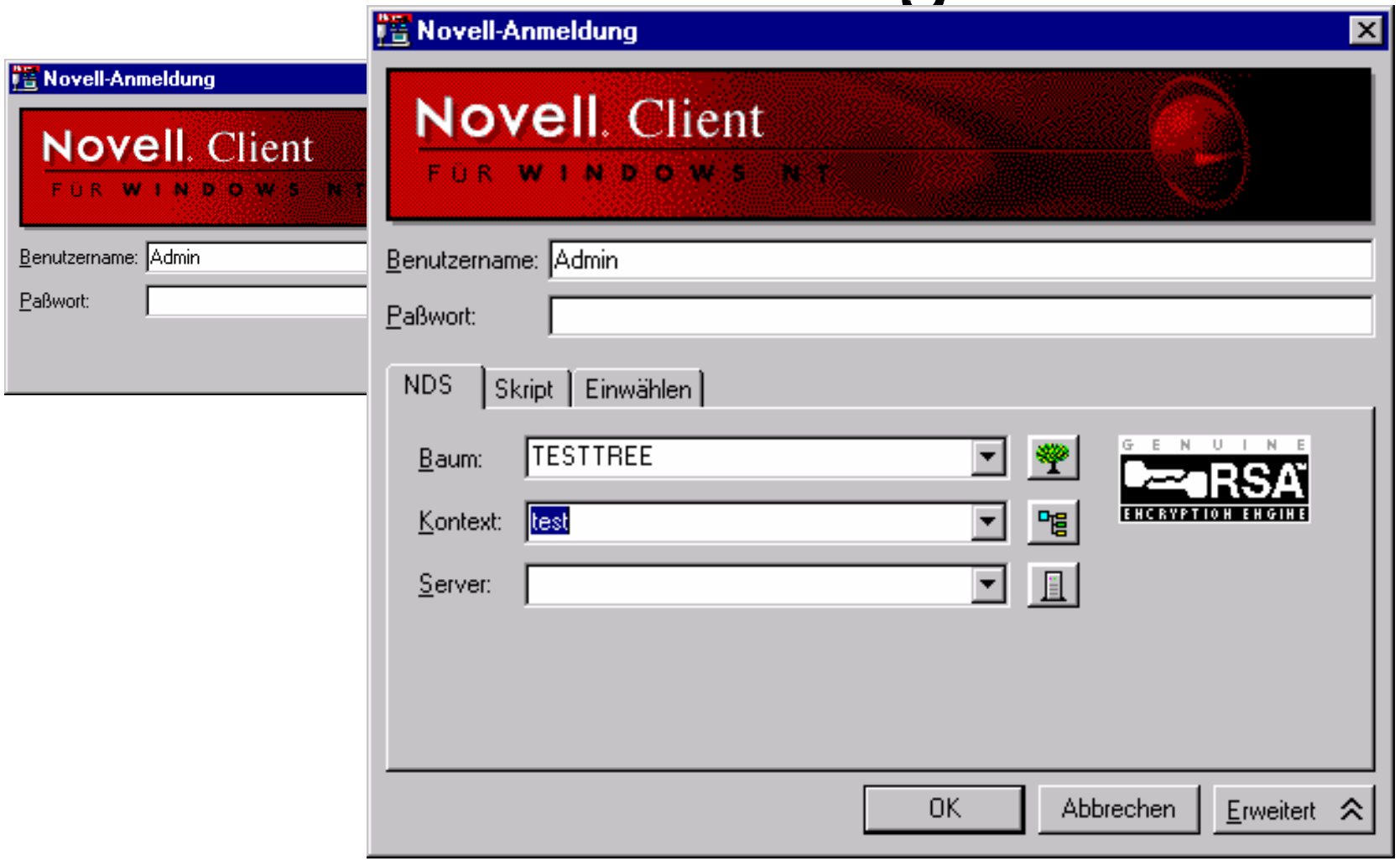
eDirectory-Anwendungen

- Anmelden
- Loginscripts
- Passwort
- Single Sign On

Anmelden

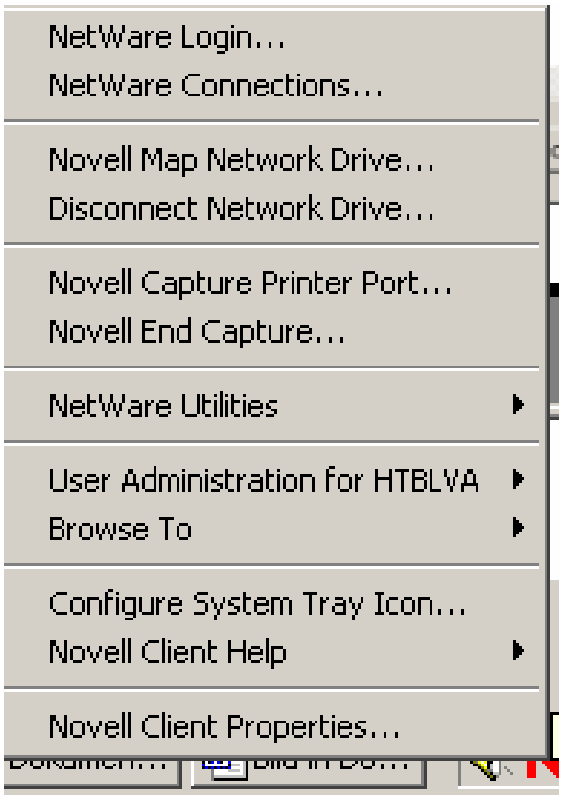
- Die Anmeldung erfolgt mittels des Verzeichnisdienstes am Netz und i.a. nicht an einem Rechner (Workstation) oder an einem Server
- Alle erlaubten Ressourcen des Netzes stehen zur Verfügung
- Windows Benutzer-Profil kann vom Server geladen (Roaming Profiles)

Anmeldung

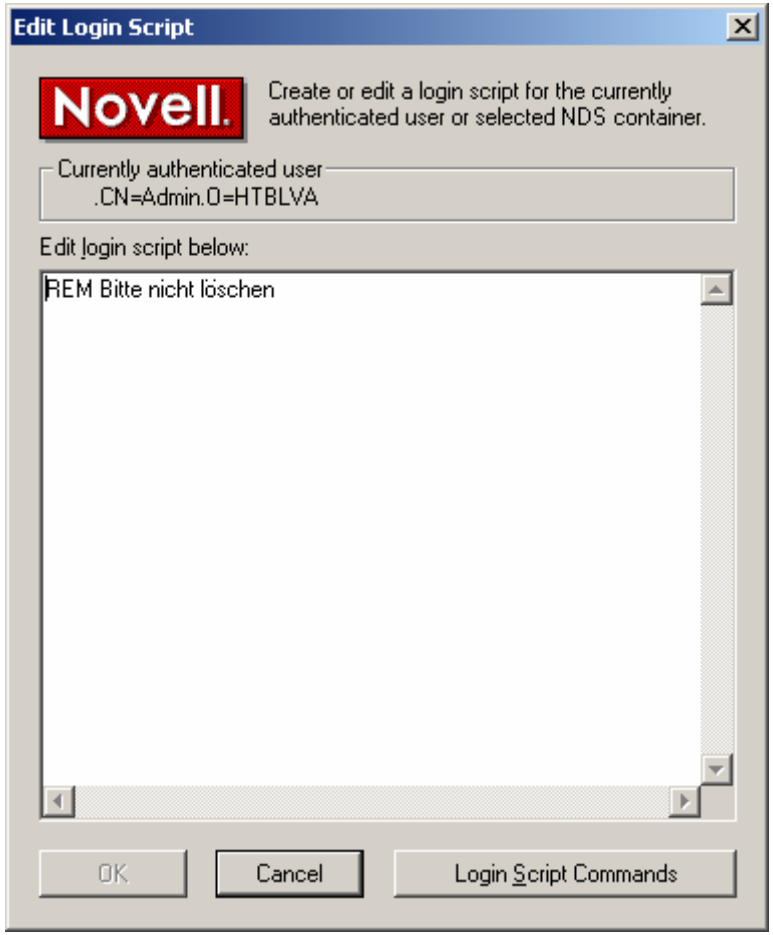

Novell-Anmeldung
Novell. Client
FÜR WINDOWS NT
Benutzername: Admin
Paßwort:
Novell-Anmeldung
Novell. Client
FÜR WINDOWS NT
Benutzername: Admin
Paßwort:
NDS
Skript
Einwählen
Baum: TESTTREE
Kontext: test
Server:
GENUINE RSA ENCRYPTION ENGINE
OK
Abbrechen
Erweitert

Loginscripts

- Containerscript (vom Benutzer nicht veränderbar)
- Optionales Profilescript
- Benutzerscript



Benutzer-Loginscript



Passwort

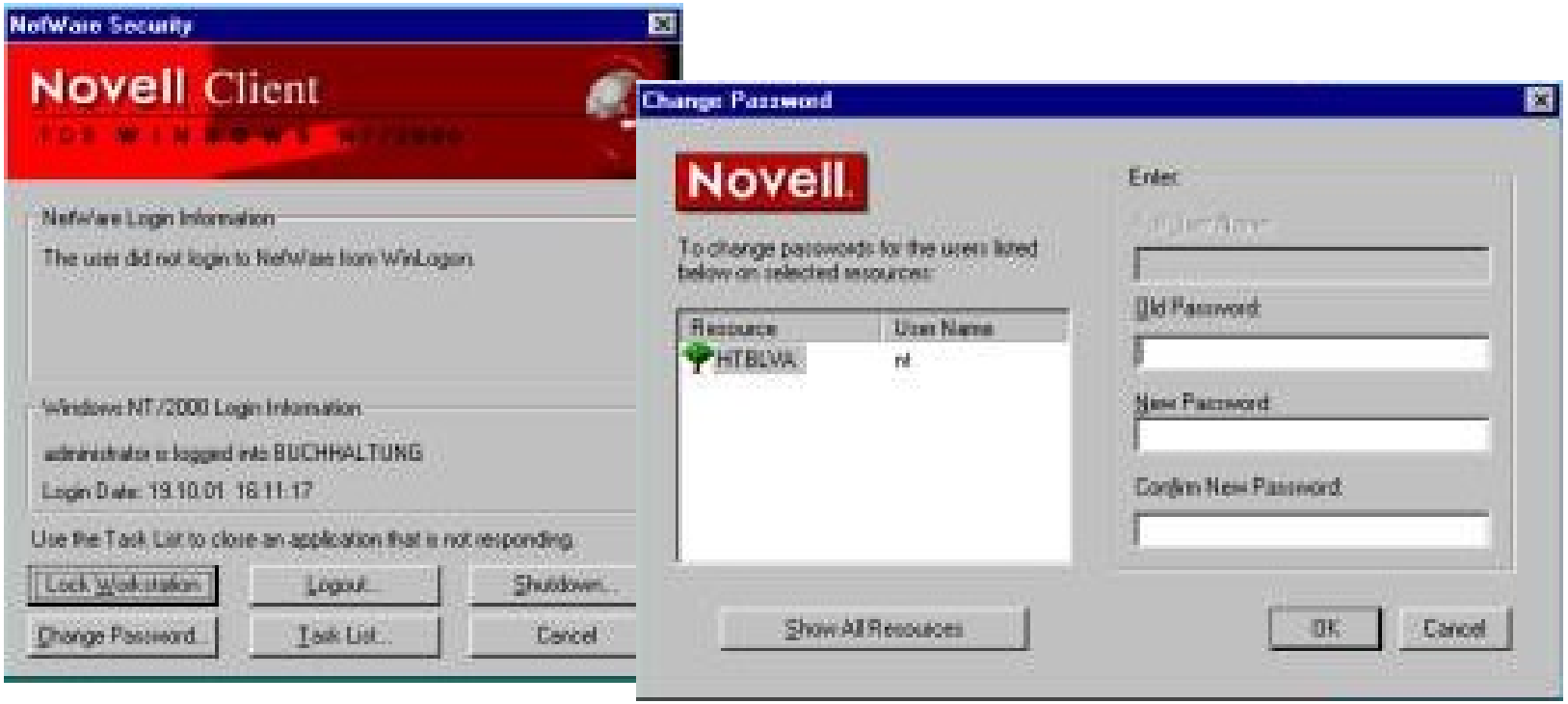
- max. Länge: OS-abhängig
- Groß- und Kleinschreibung wird in der NDS nicht unterschieden (im Gegensatz zu Win)
- Sonstige Einstellmöglichkeiten z.B.:
  - Schon verwendete Passwörter dürfen nicht wieder verwendet werden
  - 3 Falscheingaben innerhalb einer ½ Stunde führen zu einer Sperre von einer Stunde
  - Gilt 40 Tage ab der letzten Änderung
  - Mindestlänge

Passwortsicherheit

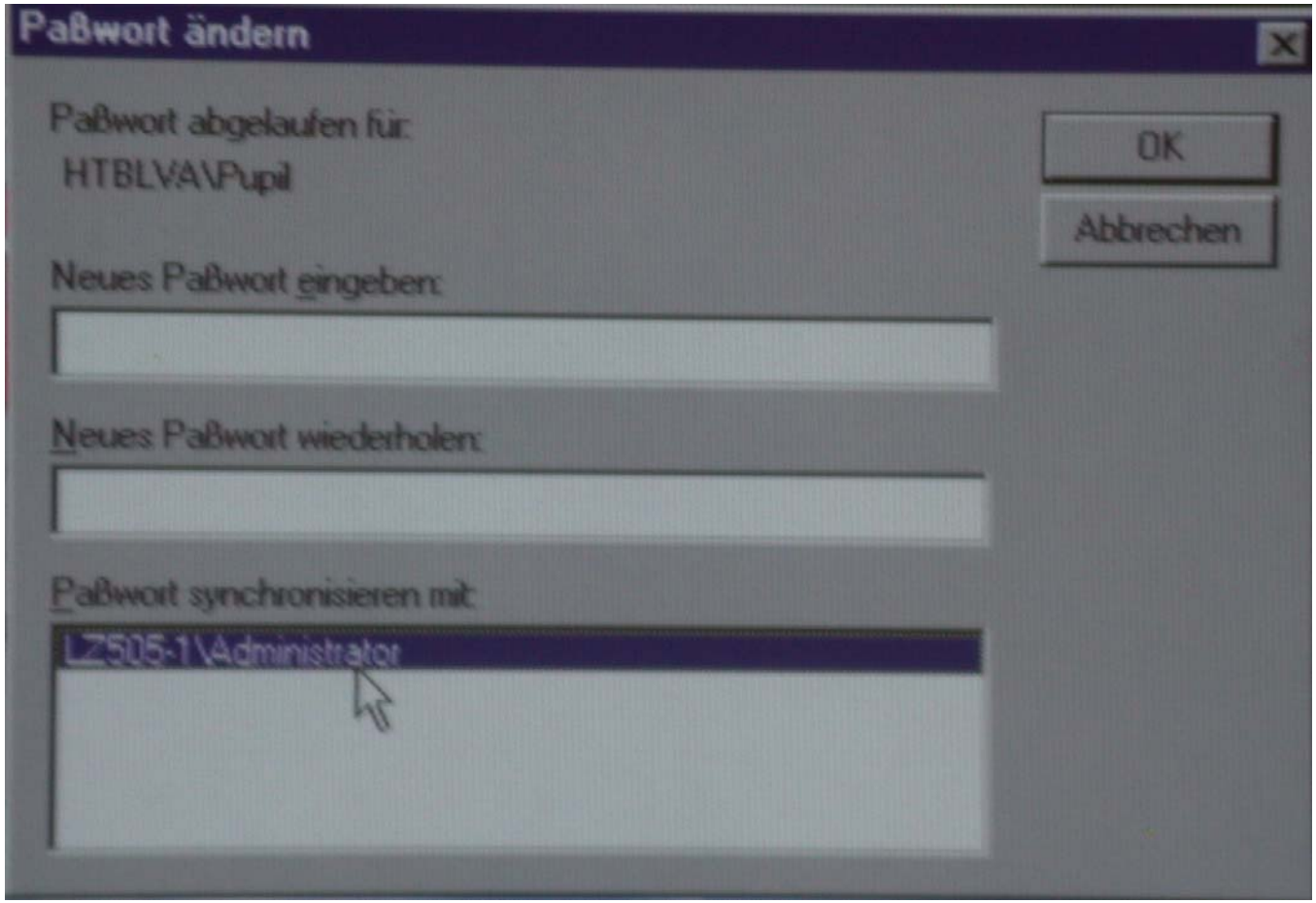
- Was ist ein sicheres Passwort?
- Buchstaben, Sonderzeichen und Ziffern kombinieren
- Regelmäßig ändern
- POP- bzw. FTP-Passwörter werden im Klartext übertragen und können daher leicht abgefangen werden

Ändern des Passwortes

- <CTRL>-<ALT>-<DEL>



Passwort abgelaufen?



Single Sign On

- Durch Passwordsafe und eigenen Client ein Zusammenspiel mit vielen Systemen möglich
- Passwordsafe ist Teil des eDirectories
- „Mitschreiben“ der Loginvorgänge

II.5.2. Workstation – Server

- Aufbau der Hardwareverbindung
- Aufbau der Softwareverbindung
  - Netwareclient (MS oder Novell)
  - Native Clientaccess
  - Internetaccess
- Anmelden (Bindery, Kontext, Beispiele)
- Abmelden

II.5.3. Dateikonzepte

- Ein Netwareserver benötigt eine FAT-Partition zum Booten und zumindest eine Netwarepartition.
- Die Netwarepartitionen werden u.U. segmentiert und immer als Volumes verwendet
- Seit Netware 5.1 daneben noch NSS-Partitionen möglich

Definitionen

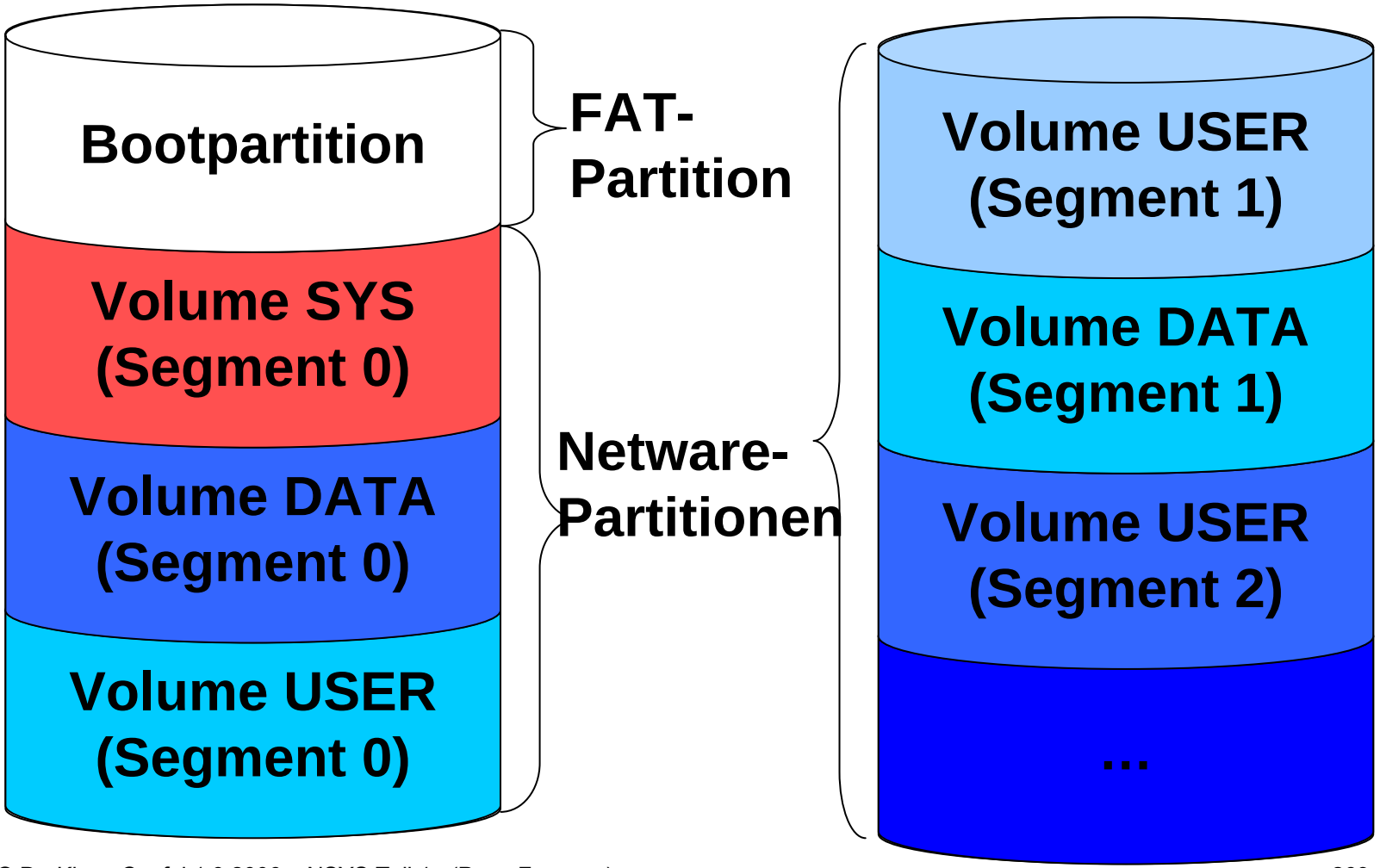
- Partition

  Teil einer Festplatte mit einem eigenen Dateisystem
- Volume

  Unter einer Bezeichnung verwendbare Massenspeichereinheit
- Segment

  Teil einer Partition

Beispiel


Bootpartition
Volume SYS
(Segment 0)
Volume DATA
(Segment 0)
Volume USER
(Segment 0)
FAT-
Partition
Netware-
Partitionen
Volume USER
(Segment 1)
Volume DATA
(Segment 1)
Volume USER
(Segment 2)
...

Namespaces

- Um Namen mit anderer Namensgebung speichern zu können, werden Namespaces verwendet
- DOS (immanent)
- MAC, (OS2,) LONG, NFS, VTAM ladbar
- Server passt sich an den Client an (nicht Client an den Server)

Fileservices Überblick

- Max. 4 Partitionen pro Platte
- Typ 6_{Hex} Bootpartition (ab Netware 3.0)
- Typ 64_{Hex} Netware 2.x
- Typ 65_{Hex} Traditional File Services (ab Netware 3.0)
- Typ 69_{Hex} Netware Storage Services (NSS, seit Netware 5.1)

Traditional File Services

- Max. 8 Segmente pro Partition
- Max. 32 Segmente pro Volume
- Max. Dateigröße: 4 GByte
- Max. 16 Millionen Dateien pro Volume bei einem Namespace (ca. 4 Millionen bei 3 Namespaces)
- Max. 100.000 Dateien gleichzeitig offen
- Max. 1 TByte Volumegröße
- Software-RAID-Levels: 1
- 32-Bit Interface

Netware Storage Services – NSS

- Max. Segmente pro Volume: kein Limit
- Max. Dateigröße: 8 TByte
- Max. 8.000.000.000.000 Dateien pro Volume unabhängig von der Zahl der Namespaces
- Max. 1.000.000 Dateien gleichzeitig offen
- Dynamische Volumegröße
- Software-RAID-Levels: 0,1 und 5
- 64-Bit Interface

Trad. FS $\leftrightarrow$ NSS

	Trad. FS	NSS
Mount	Mehrere Minuten	Schnell (<1s)
Name Space	Manuell	Automatisch
Speicherbedarf	Hoch (Cache)	Niedrig
Journaling	Nein	Ja
Zusammenfassung	Schnell	Sicher

Dateinamen

- Native
  - server/volume:directory/subdir/dateiname
  - MIRACULIX/SYS:SYSTEM/BEISPIEL.DAT
  - TALENTIX/USER:\CK\SCRIPTUM.DOC
- Über die NDS
  - NDSvolumename:directory/sub/datei
  - MIRACULIX_USER:CK\MUSTER.DOT

Längenbegrenzungen

- Servernamen: 47 Zeichen
- Volumenamen: 16 Zeichen
- Unterverzeichnistiefe: einstellbar (10)
- Dateinamen: Namespace
- Dateinamen (DOS): 15 Zeichen

Volume SYS

- Ein Volume (das erste) muß SYS, die weiteren können beliebig benannt werden.
- Wichtige Verzeichnisse auf SYS
  - /ETC
  - /LOGIN
  - /MAIL
  - /PUBLIC
  - (/QUEUE)
  - /SYSTEM

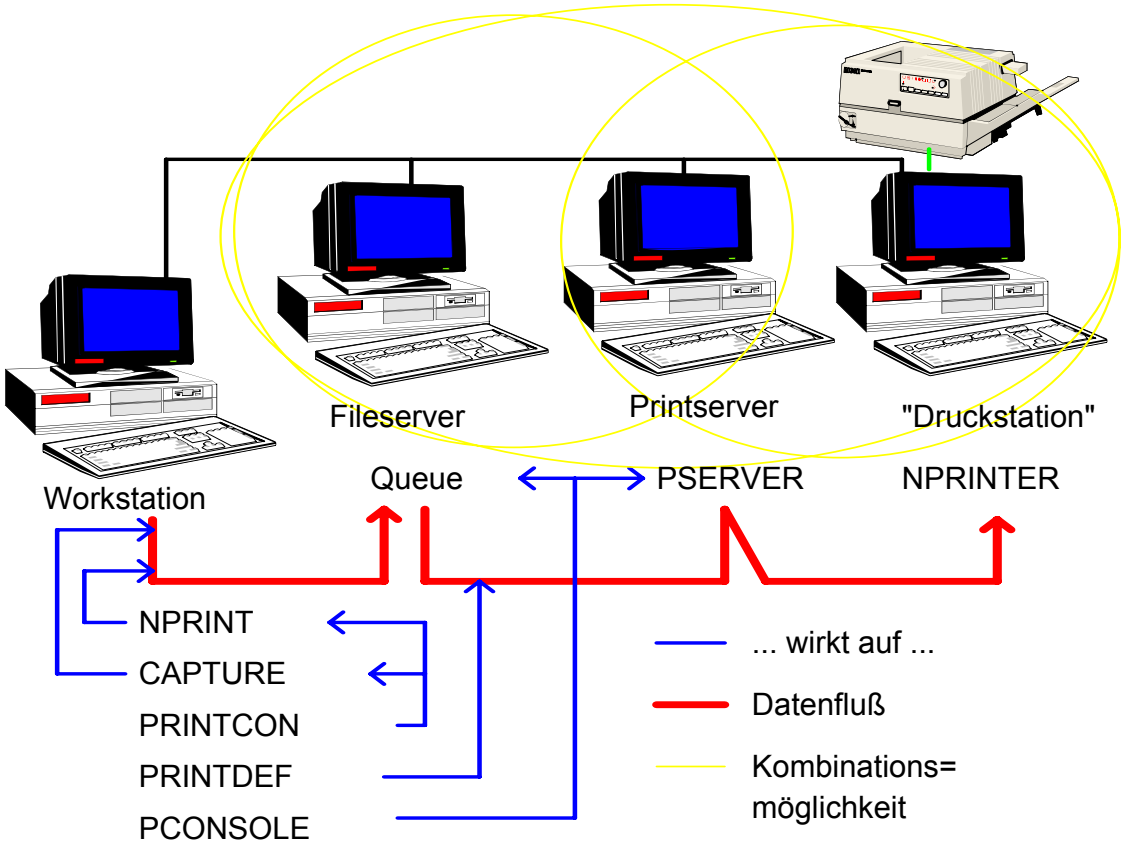
Wichtige Dateiextensions

- CDM Custom-Device-Module
- DSK DiSK-treiber-NLM
- HAM Host-Adapter-Module
- LAN LAN-treiber-NLM
- MSM Media Support Module
- NAM NAMespace-NLM
- NCF Netware Configuration File
- NLM Netware Loadable Module
- PSM Platform-Support/Specific-Module

II.5.4. Drucken - Klassisch

- Übersicht
- Druckerarten
- Spooling
- Queuing
- „Ausdruck-Ende“
- Printserver, Remote Printer
- Printserveroperator, Printqueueoperator

Drucken – Übersicht



Drucken - Druckerarten

- Lokaler Drucker an einer Arbeitsstation
- Netzwerkdrucker an einer Arbeitsstation
- Netzwerkdrucker an einem Printserver
- Netzwerkdrucker an einem Fileserver
- Netzwerkdrucker direkt im Netz

Lokaler Drucker

- Ein lokaler Drucker im Netzwerk verhält sich wie ein Drucker an einem einzelnen Arbeitsplatz.
- Die Verwaltung erfolgt daher durch die Werkzeuge am Arbeitsplatz (z.B.: Systemsteuerung).

Netzwerkdrucker - WS

- Ein Netzwerkdrucker an einem Arbeitsplatz steht für diesen und alle anderen Arbeitsplätze nur mehr über die Netzwerkdruckerverwaltung zur Verfügung, am Arbeitsplatz selbst muß ein kleiner speicherresidenter Modul (NPRINTER) geladen sein, damit der zugehörige Printserver auf den Drucker zugreifen kann.

Netzwerkdrucker – PS

- Ein Printserver ist eine Station im Netz, die die Verwaltung von bis zu 256 Druckern übernehmen kann und für diese Drucker die Warteschlangen verwaltet. Die Dateien in der Warteschlange werden von einem Fileserver zwischengespeichert. Ein Drucker der direkt an einem Printserver angeschlossen ist, kann ebenfalls vom gesamten Netzwerk verwendet werden, die zugehörige Warteschlange wird - wie bei allen anderen Netzwerkdruckern auch - auf einem Fileserver angelegt.

Netzwerkdrucker – FS

- Jeder Fileserver in einem Netware-Netzwerk kann auch Printserver sein, wobei diese Aufgaben vollkommen getrennt wurden, sodaß jetzt der Printserver im Fileserver sich ebenfalls im Netzwerk anmelden muß, um aktiv zu sein. Ein an einem Fileserver angeschlossener Drucker kann vom Netz verwendet werden, wenn am Fileserver der entsprechende Modul (NPRINTER.NLM) geladen ist und ein Printserver die Verwaltung dieses Drucker übernommen hat.

Netzwerkdrucker – HW

- Viele Drucker können auch direkt an das Netzwerk angeschlossen werden, die integrierte Software kann meist sowohl als Printserver oder auch als Remote Printer konfiguriert werden.
- Unterstützen häufig verschiedene Druckprotokolle.
- Verwaltung über eigene Software.

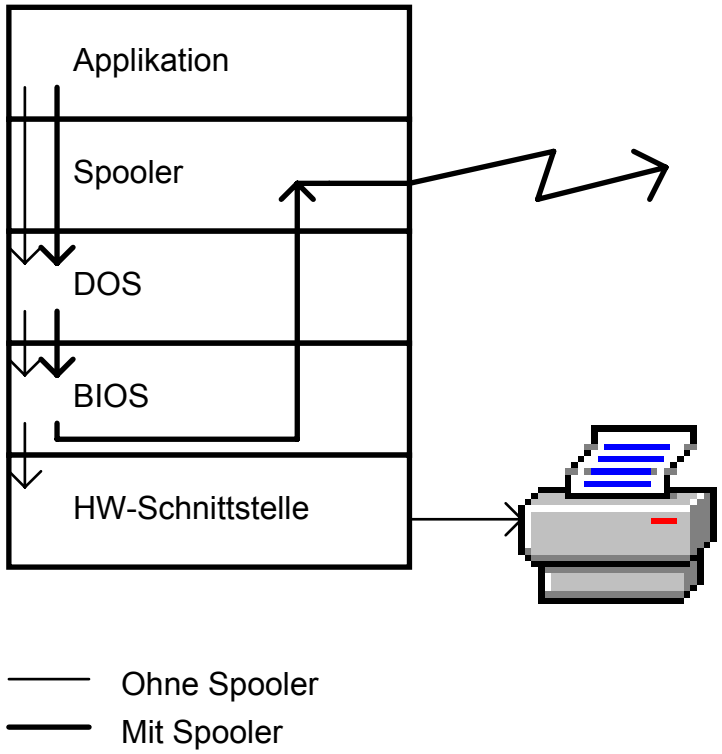
Spooling 1

Damit auch Applikationen, die nicht netzwerkfähig sind, den Netzwerkdrucker nützen können, verwendet man einen Spooler, der alle Zugriffe auf eine lokale Schnittstelle (z.B.: LPT1:) abfängt und auf eine andere (z.B.: COM1:) oder eine logische (z.B.: Datei, Netzwerk, ...) Schnittstelle umleitet.

Spooling 2

Anwendungen, die direkt auf die Hardwareschnittstelle des Druckers zugreifen, können mit dieser Methode nicht auf einem Netzwerkdrucker ausdrucken. Die Arbeitsplatzsoftware der Netware stellt für das Betriebssystem DOS einen Spooler zur Verfügung, andere Arbeitsplatzbetriebssysteme haben einen solchen bereits integriert.

Spooling 3


Applikation
Spooler
DOS
BIOS
HW-Schnittstelle
Ohne Spooler
Mit Spooler

Queueing 1

Damit mehrere Benutzer einen Drucker nutzen können, sind Warteschlangen notwendig; d.h. am Ende eines Spooling-Vorganges wird die zu druckende Information in eine Warteschlange eingereiht und erst ausgedruckt, bis alle vorher abgeschickten bzw. alle mit höherer Priorität versehenen Jobs gedruckt sind.

Queueing 2

Während des Spooling-Vorganges existiert schon ein Eintrag in der entsprechenden Warteschlange, allerdings wird dieser erst freigegeben, wenn der Spooling-Vorgang abgeschlossen ist. Für einen Benutzer sollte betont werden, daß er im Netzwerk nie auf einem Drucker direkt, sondern immer nur in eine Warteschlange druckt.

Queueing 3

Der Weg von der Warteschlange zum Drucker kann vom Anwender in keiner Weise beeinflußt werden, trotzdem bestimmt der Anwender schon beim Drucken in die Warteschlange einige Parameter, die erst am Drucker relevant sind (Papiersorte, ...).

Queueing 4

Anwendungen, die das Netzwerk kennen (z.B.: MS-Windows), können u.U. direkt in die Warteschlange drucken und damit einen eventuell langsamen Spooler umgehen.

„Ausdruck-Ende“ 1

Eines der schwierigsten Aufgaben ist es, unter MS/PC-DOS das Ende eines Spooljobs zu erkennen, da z.B. ein Textverarbeitungssystem nicht meldet, daß ein Dokument fertig ist. Multitasking-betriebssysteme (Unix, OS/2, ...) haben dabei weniger Probleme, da hier schon vom Betriebssystem Mechanismen zur Endeerkennung angeboten werden.

„Ausdruck-Ende“ 2

Zur Lösung dieser Problematik gibt es unter Novell Netware mehrere Möglichkeiten:

- EOF
- EOJ
- Explizit
- Timeout

EOF

- End Of File
- Das Ende einer Datei ist in MS-DOS leicht erkennbar und kann als Ende des Spoolvorganges dienen.

EOJ

- End Of Job
- Wenn ein Applikationsprogramm beendet wird, kann ebenfalls davon ausgegangen werden, daß die im Spooler befindliche Information abgeschlossen ist.

Explizit

- Selbstverständlich hat der Benutzer jederzeit die Möglichkeit selbst das Ende zu bestimmen.
- Diese Methode ist aber meist umständlich und fehleranfällig

Timeout

- Für Einzelplatzanwendungen ist dies oft die einzige Möglichkeit, die mit sinnvollem Arbeitsaufwand für den Anwender verbunden ist.
- Nach einer bestimmten Zeit, in der keine Informationen an den Spooler übergeben werden, wird ein automatisches Ende angenommen.

Printserver 1

- Ein Printserver ist eine Netzwerkkomponente, die entweder aus einer eigenen Hardware (dedicated Printserver) bzw. einem Netware-Fileserver (Non-dedicated Printserver) und einem passenden Programm besteht.

Printserver 2

- Seine Aufgabe ist die Abarbeitung der Printqueues auf den Fileservern und damit die Ausgabe der Printjobs auf einem entsprechenden Drucker.
- Definiert wird ein Printserver mit den üblichen Verwaltungsprogrammen, wobei für jeden Printserver die Daten in einem Verzeichnis SYS:SYSTEM\printserverid bereitgestellt werden.

Printserver 3

- Jeder Dedicated Printserver ist während des Betriebs an den entsprechenden Fileservern angemeldet, d.h. er belegt eine „Benutzerlizenz“; der Nondedicated Printserver ist zwar ebenfalls angemeldet, belegt aber auf dem Fileserver, auf dem er gestartet wurde, keine eigene „Benutzerlizenz“.

Remote Printer 1

- Ein Remote Printer ist ein Drucker, der vom zugehörigen Printserver nicht direkt, sondern nur über das Netzwerk erreicht werden kann.
- Entweder ist das ein Drucker an einer Arbeitsstation, der vom Netzwerk verwendet werden soll oder ein Drucker mit mehr oder weniger direktem Netzanschluß.

Remote Printer 2

- Gesteuert wird ein solcher Drucker mittels eines Printservers.
- Auf der Arbeitsstation/dem Server, an der Drucker physikalisch angeschlossen ist, muß ein kleiner speicherresidenter Modul (NPRINTER) aktiv sein.
- Heute fast ausschließlich Hardwarelösungen.

Printserveroperator 1

- Jede Person, die vom Systemverantwortlichen für einen bestimmten Printserver als Operator eingetragen ist, kann die Definitionen eines Printservers (welche Drucker, welche Warteschlangen, wer wird verständigt, wenn Probleme auftreten, ...) verändern.

Printserveroperator 2

- Notwendig wird dies z.B. beim Einrichten eines neuen Druckers oder bei der temporären Umleitung einer Warteschlange auf einen Ersatzdrucker während einer Fehlerbehebung. Zum geordneten Niederfahren eines Printservers wird ebenfalls das Recht Printserveroperator benötigt.

Printqueueoperator

Für jede Warteschlange können Printqueueoperator definiert werden, die alle Druckjobs so manipulieren können, als wären es ihre eigenen; d.h. sie können Druckjobs aus der Warteschlange löschen, deren Reihenfolge verändern und bei jedem Druckjob einzelne Parameter verändern.

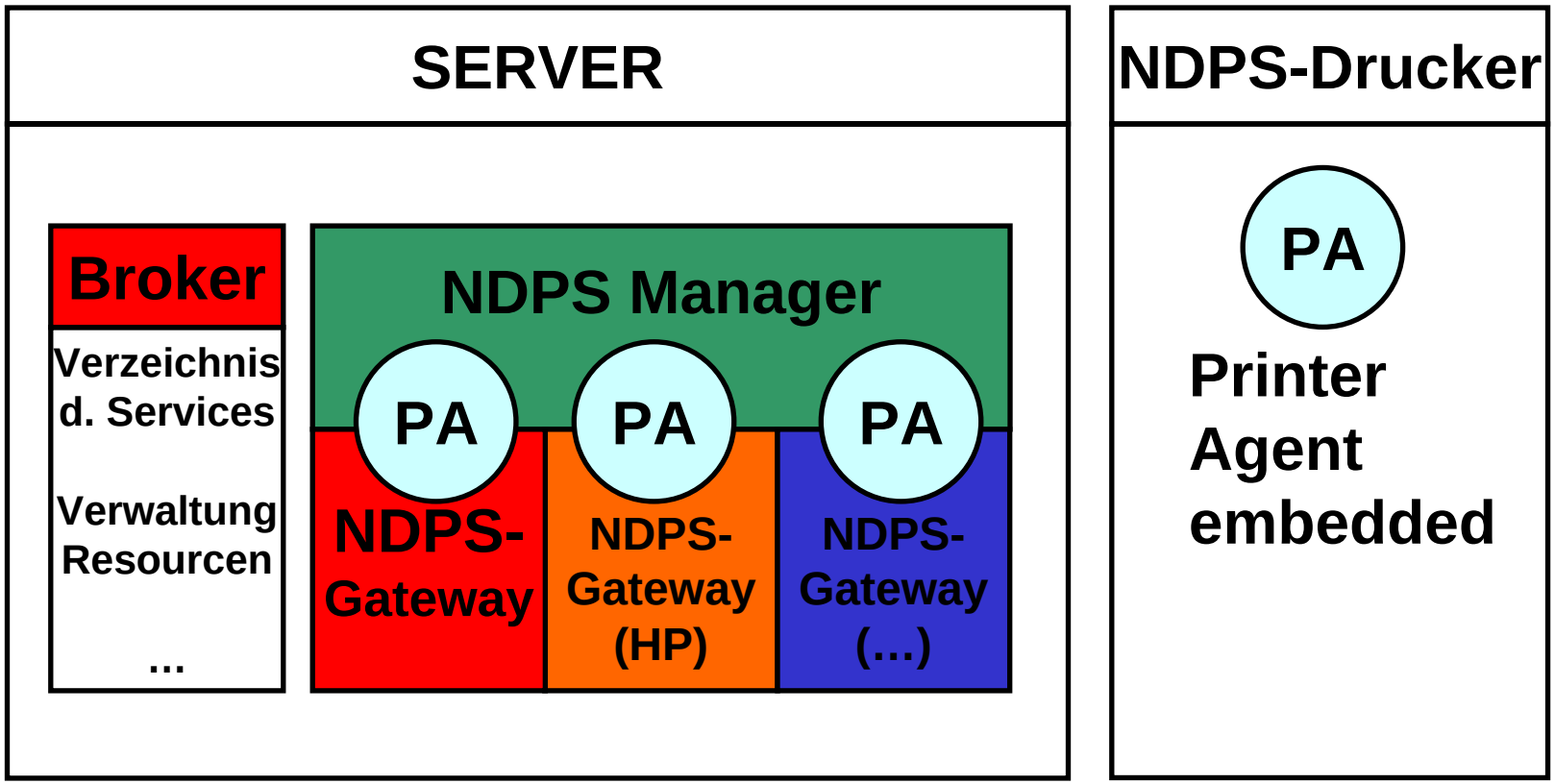
II.5.5. Drucken – NDPS

- Übersicht
- Komponenten
- Druckerarten
- NDPS Broker
- NDPS Manager
- NDPS Gateway
- NDPS Printeragent

NDPS - Übersicht

- Novell Distributed Print Services
- Verwaltungsvereinfachung (z.B.: durch automatische Treiberverwaltung, …)
- Bidirektionale Druckersteuerung
- Volle Kompatibilität zum klassischen Druckkonzept
- Internetfähig (iPrint)

NDPS – Komponenten



NDPS – Druckerarten

- NDPS-aware Drucker
- Netzwerkdrucker, die mit Hilfe eines Agents NDPS-fähig werden.
- Klassische Drucker (s.o.)

NDPS Broker

- Übernimmt die Aufgaben
  - Service Registrierung (Druckereigenschaften)
  - Benachrichtigung von Ereignissen (Druck fertig, Druckerproblem, …)
  - Ressourcenverwaltung (Treiber, „Banner“, Druckerdefinitionen)
- Läuft auf einem Server

NDPS Manager

- Verwaltet verschiedene Printeragents am Server
- Software läuft auf einem Server (NDPSM.NLM)
- „Übernimmt“ die Verwaltungsaufgaben der Printserver

NDPS Gateway

- Übersetzen NDPS-Aufträge in die Printerspezifischen Befehle
- Existieren nur für nicht NDPS-fähige Drucker
- Novell-Eigenes Gateway bietet nur die Basisfunktionen des „Klassischen Druckens“ an

NDPS Printeragent

- Repräsentiert den Drucker in der Software und stellt in den NDPS zur Verfügung
- Vereint die Aufgaben von Printer, Printqueue, Printserver und Spooler
- 1:1-Beziehung (d.h. für jeden physischen Drucker existiert ein Printer Agent)

II.5.6. Zugriffsrechte und Dateiattribute

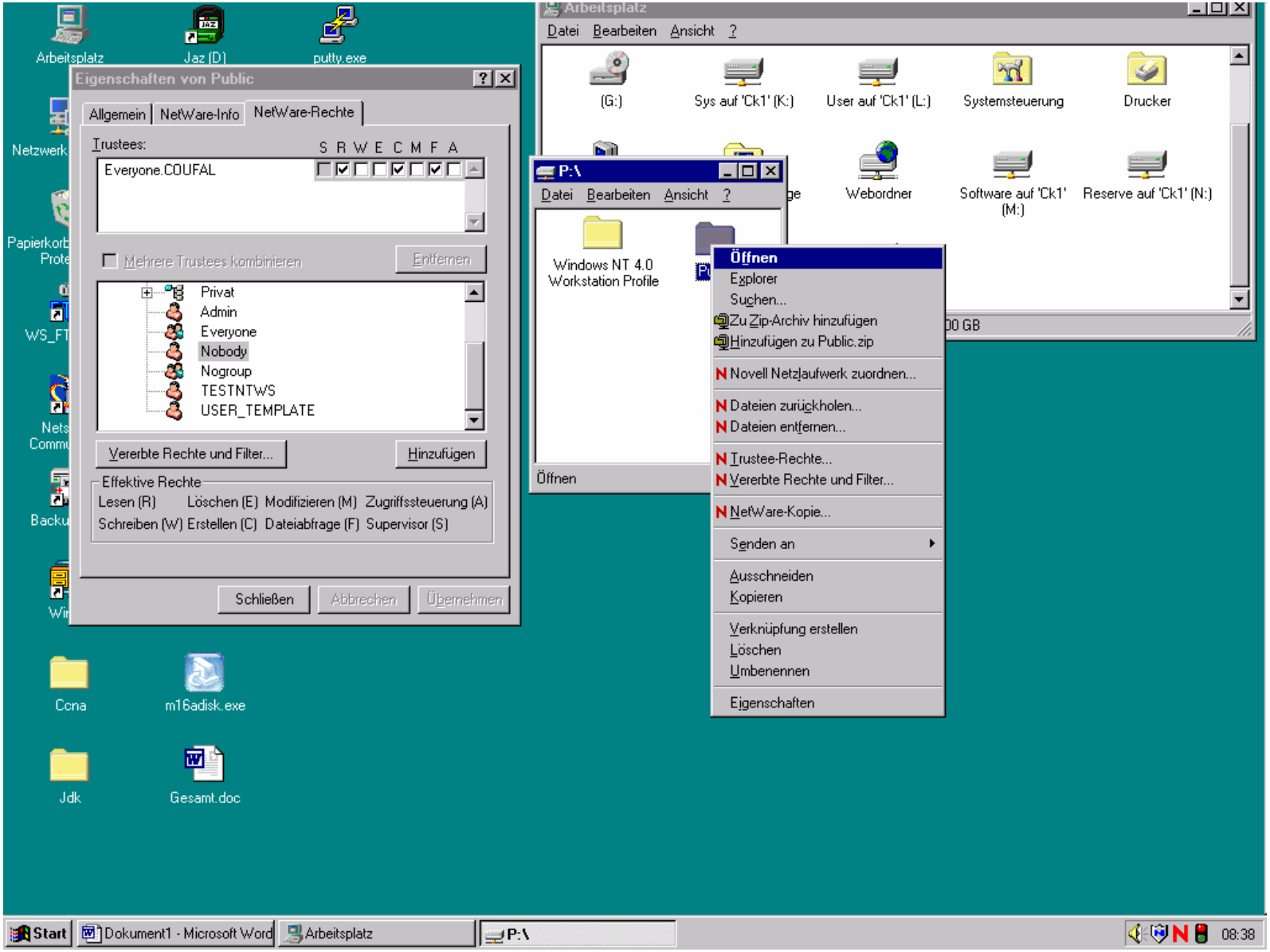
- Neben dem Zutrittsschutz (s.o.) ist selbstverständlich noch der Zugriffsschutz zu regeln:
- Trustees und deren Rechte
- Inheritance Rights Filter
- Security equivalences
- Effektive Rechte

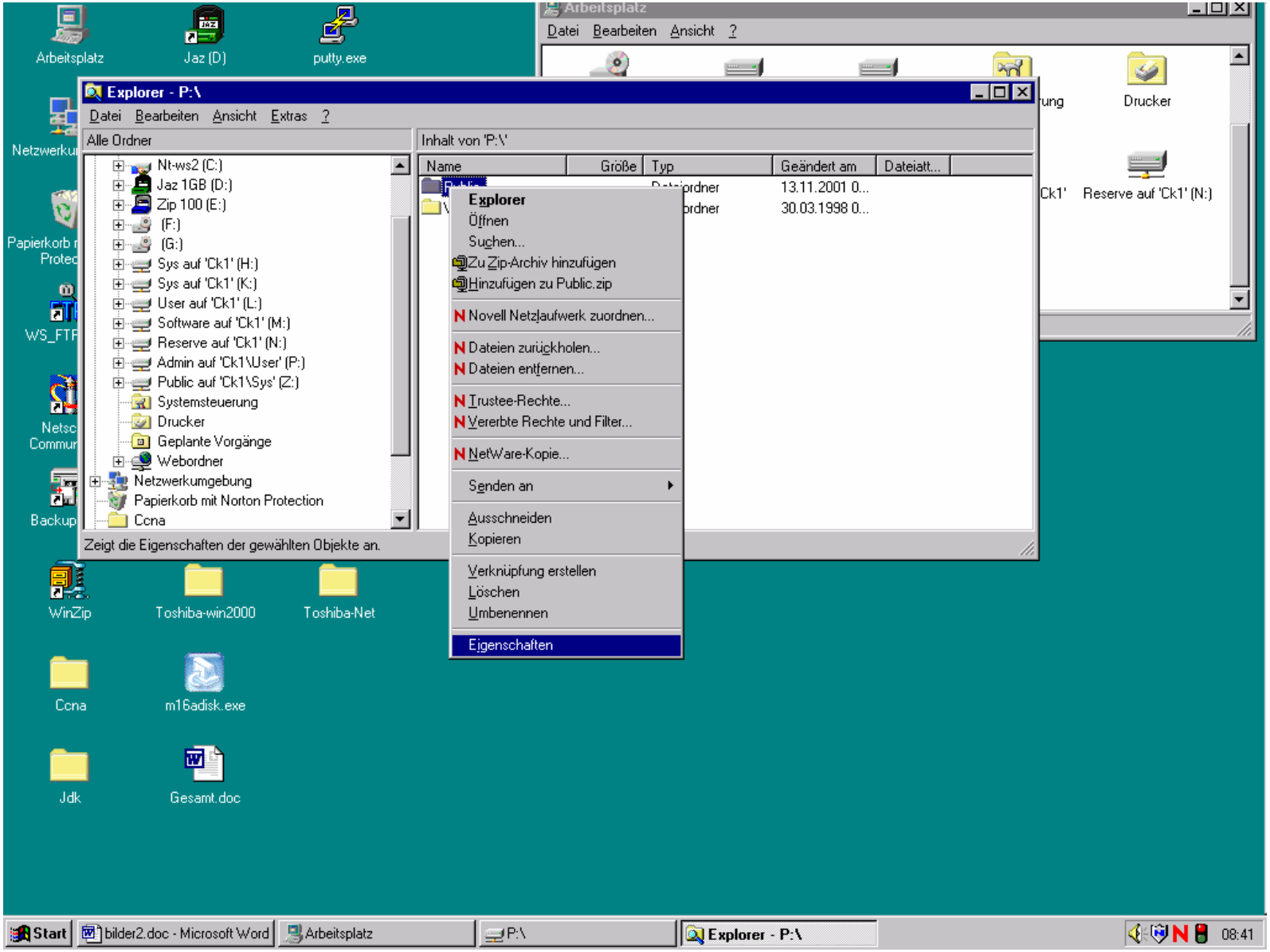
Trustees

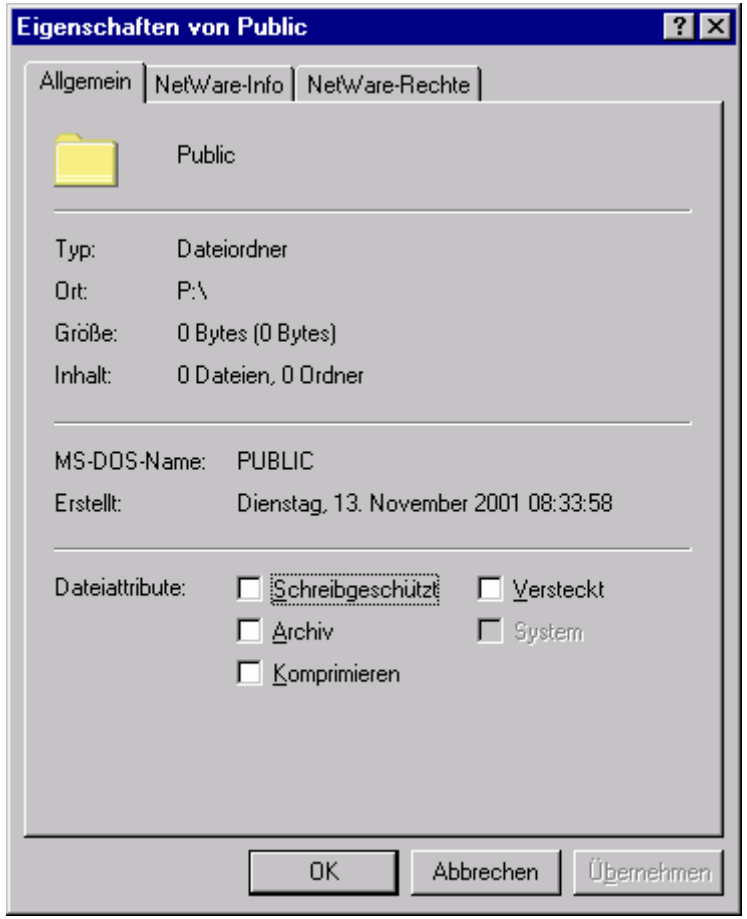
Die Zugriffsrechte werden über Benutzer bzw. Gruppen auf Verzeichnis- bzw. Dateiebene definiert. Die Rechte in einem Verzeichnis gelten automatisch für alle Dateien und Unterverzeichnisse dieses Verzeichnisses ebenfalls. Ein berechtigter Benutzer bzw. eine berechtigte Gruppe stellt einen "Trustee" für das entsprechende Verzeichnis bzw. die entsprechende Datei dar. Die Trustees werden mit "Trusteelists" verwaltet.

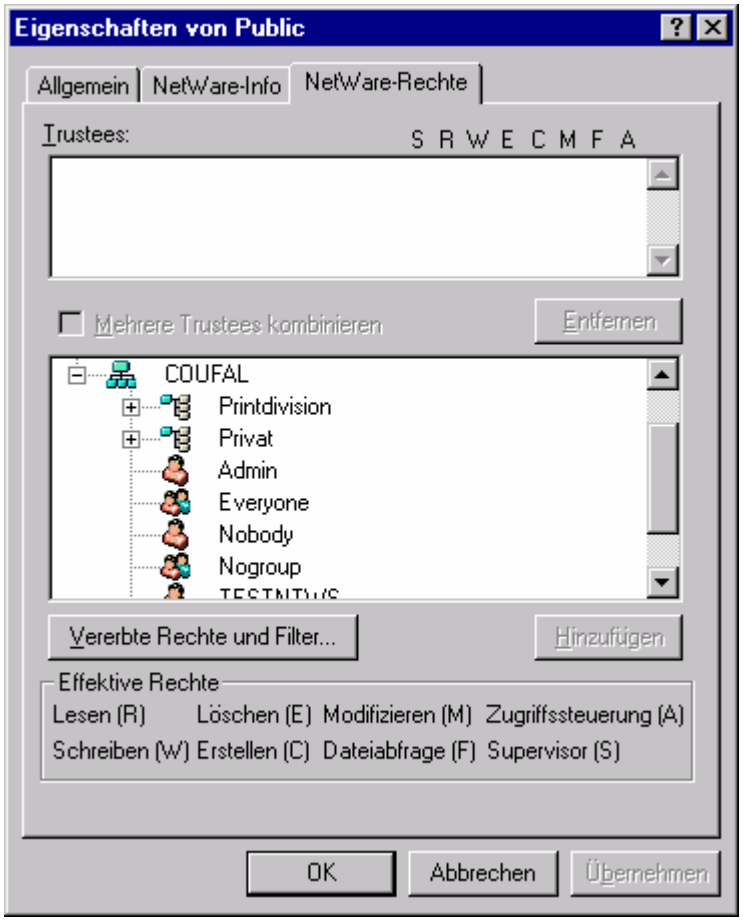
Datei-/Verzeichnisrechte

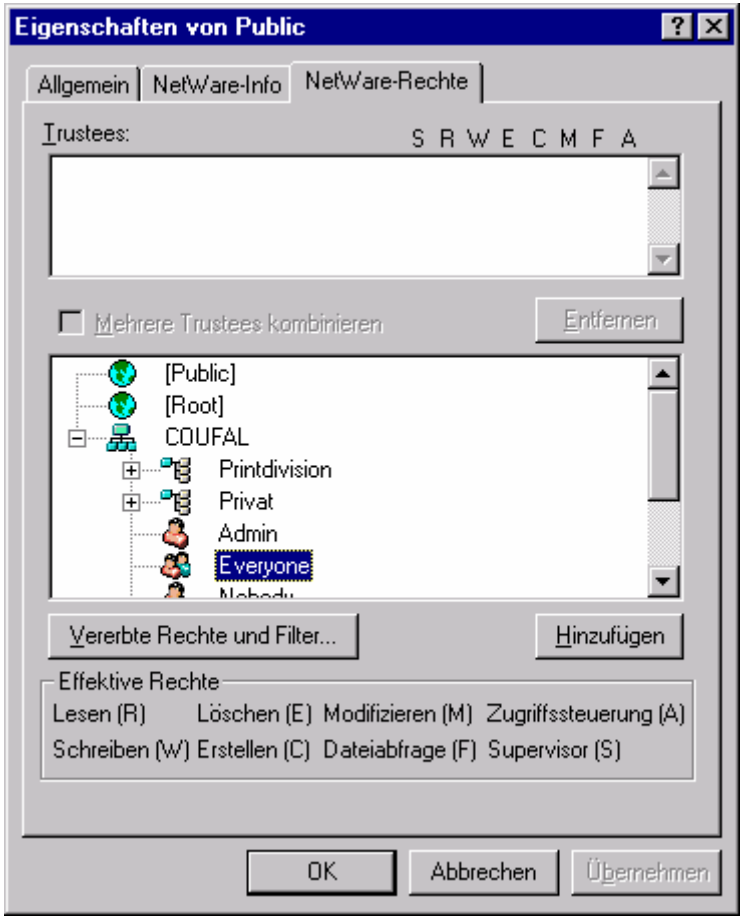
- R Read Lesen
- W Write Schreiben
- E Erase Löschen
- C Create Erstellen
- M Modify Modifizieren (Attribute)
- F FileScan Abfragen mit „Wildcards“
- A AccessControl Zugriffskontrolle
- S Supervisor Verwalter

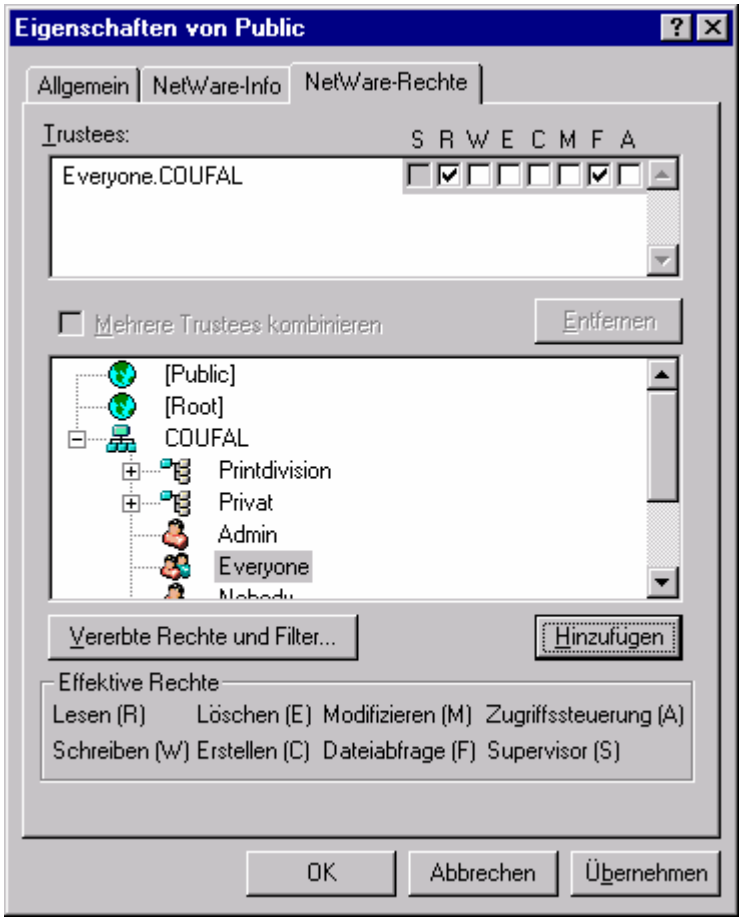

Arbeitsplatz
Jaz (D)
putty.exe
Netzwerk
Papierkorb
Ccna
m16adisk.exe
Jdk
Gesamt.doc
Eigenschaften von Public
Allgemein
NetWare-Info
NetWare-Rechte
Trustees:
S R W E C M F A
Everyone.COUFAL
Mehrere Trustees kombinieren
Entfernen
Privat
Admin
Everyone
Nobody
Nogroup
TESTNTWS
USER_TEMPLATE
Vererbte Rechte und Filter...
Hinzufügen
Effektive Rechte
Lesen (R) Löschen (E) Modifizieren (M) Zugriffssteuerung (A)
Schreiben (W) Erstellen (C) Dateiabfrage (F) Supervisor (S)
Schließen
Abbrechen
Übernehmen
Arbeitsplatz
Datei Bearbeiten Ansicht ?
(G:)
Sys auf 'Ck1' (K:)
User auf 'Ck1' (L:)
Systemsteuerung
Drucker
Webordner
Software auf 'Ck1' (M:)
Reserve auf 'Ck1' (N:)
P:\
Datei Bearbeiten Ansicht ?
Windows NT 4.0 Workstation Profile
Öffnen
Öffnen
Explorer
Suchen...
Zu Zip-Archiv hinzufügen
Hinzufügen zu Public.zip
Novell Netzlaufwerk zuordnen...
Dateien zurückholen...
Dateien entfernen...
Trustee-Rechte...
Vererbte Rechte und Filter...
NetWare-Kopie...
Senden an
Ausschneiden
Kopieren
Verknüpfung erstellen
Löschen
Umbenennen
Eigenschaften
Start
Dokument1 - Microsoft Word
Arbeitsplatz
P:\
08:38


Arbeitsplatz
Jaz (D)
putty.exe
Explorer - P:\
Datei Bearbeiten Ansicht Extras ?
Alle Ordner
Inhalt von 'P:\'
Name
Größe
Typ
Geändert am
Dateiatt...
Nt-ws2 (C:)
Jaz 1GB (D:)
Zip 100 (E:)
(F:)
(G:)
Sys auf 'Ck1' (H:)
Sys auf 'Ck1' (K:)
User auf 'Ck1' (L:)
Software auf 'Ck1' (M:)
Reserve auf 'Ck1' (N:)
Admin auf 'Ck1\User' (P:)
Public auf 'Ck1\Sys' (Z:)
Systemsteuerung
Drucker
Geplante Vorgänge
Webordner
Netzwerkumgebung
Papierkorb mit Norton Protection
Ccna
13.11.2001 0...
30.03.1998 0...
Explorer
Öffnen
Suchen...
Zu Zip-Archiv hinzufügen
Hinzufügen zu Public.zip
Novell Netzlaufwerk zuordnen...
Dateien zurückholen...
Dateien entfernen...
Trustee-Rechte...
Vererbte Rechte und Filter...
NetWare-Kopie...
Senden an
Ausschneiden
Kopieren
Verknüpfung erstellen
Löschen
Umbenennen
Eigenschaften
Zeigt die Eigenschaften der gewählten Objekte an.
Drucker
Reserve auf 'Ck1' (N:)
WinZip
Toshiba-win2000
Toshiba-Net
Ccna
m16adisk.exe
Jdk
Gesamt.doc
Start
bilder2.doc - Microsoft Word
Arbeitsplatz
P:\
Explorer - P:\
08:41


Eigenschaften von Public
Allgemein
NetWare-Info
NetWare-Rechte
Public
Typ: Dateiordner
Ort: P:\
Größe: 0 Bytes (0 Bytes)
Inhalt: 0 Dateien, 0 Ordner
MS-DOS-Name: PUBLIC
Erstellt: Dienstag, 13. November 2001 08:33:58
Dateiattribute:
Schreibgeschützt
Versteckt
Archiv
System
Komprimieren
OK
Abbrechen
Übernehmen


Eigenschaften von Public
Allgemein
NetWare-Info
NetWare-Rechte
Trustees:
S R W E C M F A
Mehrere Trustees kombinieren
Entfernen
COUFAL
Printdivision
Privat
Admin
Everyone
Nobody
Nogroup
Vererbte Rechte und Filter...
Hinzufügen
Effektive Rechte
Lesen (R)
Löschen (E)
Modifizieren (M)
Zugriffssteuerung (A)
Schreiben (W)
Erstellen (C)
Dateiabfrage (F)
Supervisor (S)
OK
Abbrechen
Übernehmen


Eigenschaften von Public
Allgemein
NetWare-Info
NetWare-Rechte
Trustees:
S R W E C M F A
Mehrere Trustees kombinieren
Entfernen
[Public]
[Root]
COUFAL
Printdivision
Privat
Admin
Everyone
Vererbte Rechte und Filter...
Hinzufügen
Effektive Rechte
Lesen (R) Löschen (E) Modifizieren (M) Zugriffssteuerung (A)
Schreiben (W) Erstellen (C) Dateiabfrage (F) Supervisor (S)
OK
Abbrechen
Übernehmen


Eigenschaften von Public
Allgemein
NetWare-Info
NetWare-Rechte
Trustees:
S R W E C M F A
Everyone.COUFAL
Mehrere Trustees kombinieren
Entfernen
[Public]
[Root]
COUFAL
Printdivision
Privat
Admin
Everyone
Vererbte Rechte und Filter...
Hinzufügen
Effektive Rechte
Lesen (R) Löschen (E) Modifizieren (M) Zugriffssteuerung (A)
Schreiben (W) Erstellen (C) Dateiabfrage (F) Supervisor (S)
OK
Abbrechen
Übernehmen

Inheritance Rights Filter 1

- Durch die automatische Vererbung von Rechten über Verzeichnisbäume ergeben sich manchmal unerwünschte Effekte, daher existiert noch eine Möglichkeit der Beschränkung dieser Vererbung von Rechten, die "Inherited Rights Filter".

Inheritance Rights Filter 2

- In einer Maske stehen alle Rechte, die von darüberliegenden Verzeichnissen geerbt werden können, das sind standardmäßig alle Rechte. Ein Berechtigter kann jetzt einzelne Rechte ausgenommen dem Supervisory-Recht aus dieser Maske herausstreichen, dann kann niemand diese Rechte allein durch Vererbung in diesem Verzeichnis oder in dieser Datei besitzen.

IRF – Beispiel

USER:/CK	Everyone [RF]
	CK [RWECFMA]
USER:/CK/PRIV	„IRF“ [S]
	CK [RWECFMA]

USER:/CK/PUB

Alle dürfen das Verzeichnis CK und das Verzeichnis PUB lesen, aber nur CK das Verzeichnis PRIV

Security equivalences

Um die Verwaltung eines Netware-Systems zu vereinfachen bzw. Urlaubsvertretungen und ähnliches leicht organisieren zu können, gibt es noch sogenannte "Security equivalences", die allerdings nur ein Administrator vergeben kann. Ein Benutzer hat solange er "security equivalent" ist, auch die Rechte des anderen Benutzers.

Sec. eq. – Beispiel

- Der Benutzer X ist für das Sicherheitssystem gleichwertig ("security equivalent") wie Benutzer Y, dann hat der Benutzer X die Rechte von X und Y, der Benutzer Y weiterhin die Rechte von Y.
- X↔Y möglich (aber zwei Security equivalences)

Effektive Rechte 1

- Mit Hilfe aller vorher genannter Mechanismen und den Gruppenzugehörigkeiten werden nun die effektiven Rechte eines Benutzer auf eine Datei oder ein Verzeichnis gebildet. Grob betrachtet könnte man folgende Vorgehensweise zur Bildung der effektiven Rechte annehmen:

Effektive Rechte 2

Zugeordnete Rechte des Benutzer
+ Rechte der Gruppen/Container in denen der Benutzer ist
+ Rechte der Benutzer, zu den er "security equivalent" ist
+ Rechte des Benutzers aus den übergeordneten Verzeichnissen
+ Rechte der entsprechenden Gruppen/Containern aus den übergeordneten Verzeichnissen
+ Rechte der Benutzer, zu denen er "security equivalent" ist, aus den übergeordneten Verzeichnissen
- Rechte, die aus den entsprechenden "Inherited Rights Filter" Masken fehlen
= Effektive Rechte eines Benutzer auf die Datei oder das Verzeichnis

Effektive Rechte 3

Dabei ist zu beachten:

- Eine konkret zugewiesene Rechte-maske hat Vorrang vor einer vererbten Rechtemaske.
- Durch Gruppen- oder Containerrechte können die eigenen Rechte nur erweitert werden.

Datei- und Verzeichnisattribute 1

- In einem Netzwerk sind mehr Dateiattribute von Interesse als auf einem einzelnen Arbeitsplatz
- Unterschieden werden automatisch vergebene und vom Benutzer veränderbare Attribute

Datei- und Verzeichnisattribute 2

Zu den Attributen gehört:

- Der Name (die Namen).
- Diverse Datums- und Zeitinformationen
    - Entstehungsdatum/-zeit
    - Datum/Zeit der letzten Änderung
    - Datum/Zeit des letzten Zugriffes
    - Datum/Zeit der letzten Sicherung
- Besondere Attribute
- Ortsinformationen

Besondere Dateiattribute 1

Rw/Ro **Read-Write/Read Only**

Datei kann beschrieben (verändert, ...) werden oder nicht. Jede neue Datei hat das Attribut Rw; wenn Ro gesetzt wird, dann wird automatisch auch D und R gesetzt

H **Hidden**

Dateien mit diesem Attribut werden vom DOS DIR-Befehl nicht angezeigt, können nicht gelöscht oder kopiert werden.

Besondere Dateiattribute 2

Sy **System**

Dateien mit diesem Attribut werden vom DOS DIR-Befehl nicht angezeigt, können nicht gelöscht oder kopiert werden.

A **Archive needed**

Wird vom OS automatisch vergeben, wenn die Datei verändert oder neu angelegt wird. Manche Backupprogramme setzten dieses Attribut zurück und erkennen damit, welche Dateien gesichert werden müssen.

Besondere Dateiattribute 3

Sh **Shareable**

Dateien mit diesem Attribut können von mehreren Benutzern gleichzeitig in Zugriff genommen werden, daher häufig mit Ro kombiniert.

T **Transactional**

Dateien mit diesem Attribut werden vom Transaction Tracking System überwacht, damit Änderungen entweder vollständig oder gar nicht durchgeführt werden.

Besondere Dateiattribute 4

X **Execute only**

Dateien mit diesem Attribut können nur ausgeführt (d.h. nicht kopiert) werden. Das ist allerdings kein besonderer Kopierschutz, da er leicht umgangen werden kann.

P **Purge**

Dateien mit diesem Attribut werden sofort nach dem Löschen "gepurgt", d.h. sie können mittels der Netwareutilities nicht mehr wiederhergestellt werden (ein UNDELETE ist unmöglich).

Besondere Dateiattribute 5

Ci **Copy Inhibit**

Dateien mit diesem Attribut können von Macintosh Benutzern nicht kopiert werden, hat bei DOS-Arbeitsstationen keine Auswirkung.

Di **Delete Inhibit**

Dateien mit diesem Attribut können trotz Erase-Rechts nicht gelöscht werden.

Ri **Rename Inhibit**

Dateien mit diesem Attribut können nicht umbenannt werden.

Besondere Dateiattribute 6

Dc **Don´t compress**

Diese Datei darf nicht komprimiert werden (Keine „Online“-Komprimierung, sondern eine zu vorgegebenen Zeiten durchgeführte).

Ic **Immediate compress**

Diese Datei soll sofort komprimiert werden (sofort bedeutet beim nächsten Komprimierungslauf, der üblicherweise einmal in der Nacht durchgeführt wird).

Besondere Dateiattribute 7

Cc **Can´t compress**

Diese Datei ist nicht komprimierbar. Dieses Attribut wird vom System verändert und ist für den Anwender nur zur Information bestimmt.

Co **Compressed**

Diese Datei ist komprimiert. Dieses Attribut wird vom System verändert und ist für den Anwender nur zur Information bestimmt.

Besondere Dateiattribute 8

Dm **Don´t migrate**

Diese Datei darf nicht migriert (aus dem System auf einen externen Datenträger ausgelagert) werden.

M **Migrated**

Diese Datei ist migriert. Dieses Attribut wird vom System verändert und ist für den Anwender nur zur Information bestimmt.

Besondere Dateiattribute 9

Ds **Don´t suballocate**

Für diese Datei darf keine Blocksuballocation durchgeführt werden.

I **Indexed**

Dateieinträge in den Systemtabellen (FAT) sind indiziert. Dieses Attribut wird vom System verändert und ist für den Anwender nur zur Information bestimmt.

Besondere Verzeichnisattribute 1

H **Hidden**

Verzeichnisse mit diesem Attribut werden vom DOS DIR-Befehl nicht angezeigt, können nicht gelöscht oder kopiert werden.

Sy **System**

Verzeichnisse mit diesem Attribut werden vom DOS DIR-Befehl nicht angezeigt, können nicht gelöscht oder kopiert werden.

Besondere Verzeichnisattribute 2

Di **Delete Inhibit**

Verzeichnisse mit diesem Attribut können trotz Erase-Rechts nicht gelöscht werden.

Ri **Rename Inhibit**

Verzeichnisse mit diesem Attribut können nicht umbenannt werden.

Besondere Verzeichnisattribute 3

P **Purge**

Dateien in Verzeichnissen mit diesem Attribut werden sofort nach dem Löschen "gepurgt", d.h. sie können mittels der Netwareutilities nicht mehr wiederhergestellt werden (ein UNDELETE ist unmöglich).

Dm **Don´t migrate**

Dateien in diesem Verzeichnis dürfen nicht migriert werden.

Besondere Verzeichnisattribute 4

Dc **Don´t compress**

Dateien in diesem Verzeichnis dürfen nicht komprimiert werden.

Ic **Immediate compress**

Dateien in diesem Verzeichnis sollen sofort komprimiert werden (sofort bedeutet beim nächsten Komprimierungslauf, der üblicherweise einmal in der Nacht durchgeführt wird).

II.5.7. Benutzeradministration

- Die Aufgabe der Benutzeradministration umfasst das Anlegen, Warten und Löschen von Benutzerobjekten.
- Unterschieden werden 3 Rollen:
  - User Account Manager
  - Workgroup Manager
  - Administrator (Supervisor)

User Account Manager 1

- Der User Account Manager ist für genau definierte Benutzer ein Administrator.
- Der User Account Manager darf für die ihm zugeteilten Benutzer Managementaufgaben übernehmen; er ist als Entlastung des Administrator von Routineaufgaben zu verstehen. Er darf z.B.: das Paßwort, die Zeitrestriktionen oder die Stationsrestriktionen eines ihm anvertrauten Benutzer verändern, er kann auch zur Verteilung und Verwaltung von Plattenplatz und die Zuteilung dieses Platzes auf die einzelnen Benutzer ermächtigt werden.

User Account Manager 2

- Keinesfalls darf er einen neuen Benutzer anlegen oder sich selbst zum User Account Manager für einen anderen Benutzer machen. Er darf nur die ihm (vom Administrator oder einem anderen User Account Manager) zugeteilten Benutzer innerhalb seiner Rechte verwalten, d.h. er kann keinem Benutzer ein Recht geben, daß er nicht selbst besitzt.

Workgroup Manager 1

- Der Workgroup Manager soll eine noch stärkere Entlastung des Administrators ermöglichen, da er auch neue Benutzer anlegen kann, für die er automatisch User Account Manager ist.
- Zusätzlich können ihm jederzeit bestehende oder von anderen befugten Personen angelegte Benutzer zugeteilt werden, für die er danach ebenfalls User Account Manager ist.

Workgroup Manager 2

- Die von ihm angelegten Benutzer unterscheiden sich nicht von anderen Benutzern; es kann daher auch vorkommen, dass dem Workgroup Manager die User Account Manager Funktion für einen von ihm angelegten Benutzer wieder entzogen wird (z.B.: Bei einem Wechsel in eine andere Arbeitsgruppe).

Workgroup Manager 3

- Damit neu angelegte Benutzer mit den üblichen Werten versehen werden können, sollte ein Workgroup Manager auch Manager für die Gruppen sein, in denen der neu angelegte Benutzer tätig sein soll und über Plattenplatz verfügen können, den er dem neuen Benutzer zuteilen kann.
- In seinen Rechten auf bestehende oder auch von ihm angelegte Benutzer unterscheidet sich der Workgroup Manager nicht vom User Account Manager.

Administrator (Supervisor)

- Alle Administrationsaufgaben sind dem Administrator vorbehalten, diese Rolle ist üblicherweise mit dem Supervisory-Recht auf die Wurzel des Baumes verbunden.
- In kleinen Netzen oft die einzige Administrationsrolle.

Weitere Rollen

- Neben den Standardrollen sind weitere Rollen möglich.
- Diese können wegen der flexiblen Rechte sehr fein verteilt werden.
- Sinnvoll:
  - Druckeradministratoren
  - Serveradministratoren
  - Backupadministratoren

Werkzeuge zur Verwaltung

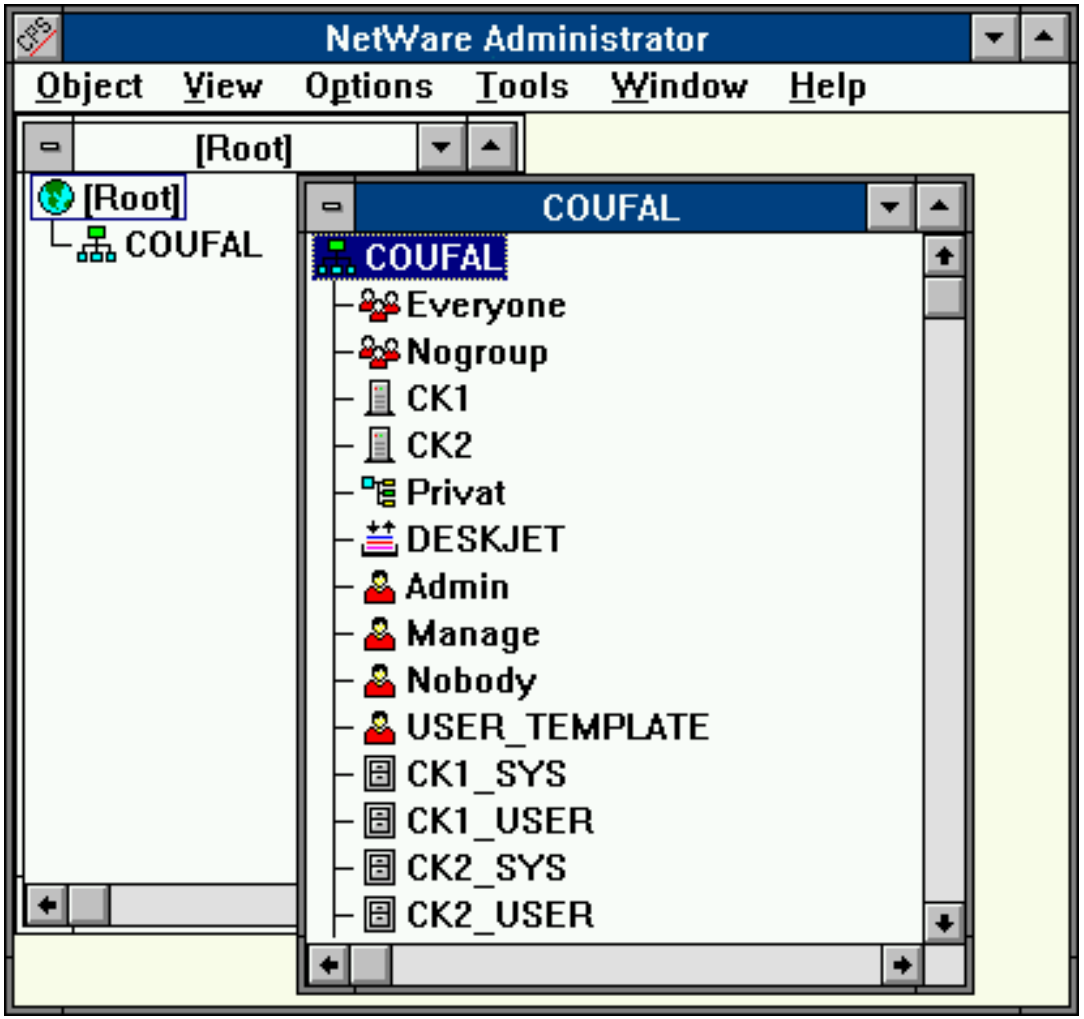
Wenige Benutzer

- NWADMIN
- ConsoleOne
- iManager

Viele Benutzer

- UIMPORT
- iManager (mit Zusatzmodulen)

NWADMIN


NetWare Administrator
Object View Options Tools Window Help
[Root]
[Root]
COUFAL
COUFAL
COUFAL
Everyone
Nogroup
CK1
CK2
Privat
DESKJET
Admin
Manage
Nobody
USER_TEMPLATE
CK1_SYS
CK1_USER
CK2_SYS
CK2_USER

UIMPORT

- **Leistungsfähiges Werkzeug zum Importieren von Benutzerdaten über eine Textschnittstelle**
- **Wird derzeit nicht weiterentwickelt**
- **Syntax:**

  UIMPORT controlfile datafile

UIMPORT – Controlfile

Zwei Bereiche:

- Import Control

  Wie soll interpretiert werden
- Fields

  Welche Felder existieren im Datenfile

UIMPORT – Import Control 1

- Separator= Trennzeichen (;)
- Quote= Anführungszeichen (^)
- Replace value= Yes | No
- User template= Yes | No
- Import mode= C (create)
  B (create and update)
  U (update)
  R (remove)

UIMPORT – Import Control 2

- Name context= Context
- Delete property= Löschmemnonic
- Create home directory= Yes | No
- Home directory path= Pfad für Heimatverzeichnis
- Home directory volume= Volume für Heimatverzeichnis
- Maximum directory retries= Anzahl

UIMPORT – Fields

Name, Last name, Given name, Other names, Skip, Title, Description, Account balance, Allow unlimited credit, Minimum account balance, Login script, Login expiration time, Login grace limit, Login grace remaining, Login maximum simultaneous, Login disabled, Password, Password expiration time, Password expiration interval, Password minimum length, Password required, Password unique required, Password allow change, Postal address, Street address, City, State or province, Postal (zip) code, Post office box, Location, Department, Telephone number, Facsimile telephone number, Language, Email address, Volume restrictions, Home directory, Default server, Security equals, Group membership, See also, Profile

Login Scripts

- Warum Scripts?
- Arten von Scripts
- Scriptbefehle

Warum Scripts

- Unabhängigkeit vom Betriebssystem ist mittels z.B.: Batchdateien nicht zu erreichen, da diese nur von MS-Systemen interpretiert werden.
- Daher eine eigene Scriptsprache, die vom Loginprogramm ausgeführt wird.

Arten von Scripts

Netware 2.x und 3.x als Datei

- **Systemloginscript in SYS:PUBLIC\NET$LOG.DAT**
- **Private Loginscript in SYS:MAIL\<userid>\LOGIN**

Ab Netware 4.x in der NDS als Eigenschaft des jeweiligen Objektes

- **Container[login]script**
- **Profile[login]script**
- **User[login]script**

Scriptbefehle 1

#programm parameter
Startet externes programm
ATTACH [server[/benutzer[;passwort]]]
Mit weiteren Server vebinden
BREAK {ON|OFF}
Abbrechen des Scripts erlaubt ?
COMSPEC=datei
Angabe eines Befehlsinterpreters
CONTEXT context
Angabe eines Defaultcontexts für den Benutzer
[F]DISPLAY datei
Anzeige einer Datei mit/ohne Steuerzeichen

Scriptbefehle 2

DOS BREAK {ON|OFF}

Abbrechen in DOS erlaubt?

[DOS | TEMP] SET variable="wert"

Für \ muß \\ verwendet werden

TEMP ... Nur für während des Scripts, nicht im OS

DOS VERIFY {ON|OFF}

DRIVE {laufwerk:|*nummer:}

Einstellen des Defaultlaufwerkes

EXIT ["DOS-Befehl"]

Ende und Ausführen von Datei, Länge des DOS-Befehls (<=14; siehe auch PCCOMPATIBLE)

FIRE PHASERS zahl TIMES

zahl=1..9

Scriptbefehle 3

GOTO label
Labeldefinition mit LABEL:
INCLUDE datei
datei ist weiteres Scriptfile (max. Tiefe= 10)
LASTLOGINTIME
Zeigt die Zeit des letzten Login´s an
MACHINE=name
Für NETBIOS Maschinenname; Länge von name <=8
MAP DISPLAY {OFF|ON}
Zeige Laufwerkszuordnungen an?
MAP ERRORS {OFF|ON}
Zeige Fehler während der Laufwerkszuordnungen an?
MAP mapbefehl [;...]
Laufwerkszuordnung (Syntax: externen DOS-Befehl MAP)

Scriptbefehle 4

IF bedingung [operator bedingung [...]] THEN befehl
IF .... THEN [BEGIN]
    befehl
[ELSE
    befehl]
END

Verschachtelungen bis zu einer Tiefe von 10 erlaubt.

bedingung:	{variable| "text"}	vergleich	"text"
	[not] benutzer	MEMBER OF	"gruppe"
	ACCESS_SERVER		
operator:	AND, OR, NOR		
vergleich:	IS, =, ==, EQUALS		
	IS NOT, !=, <>, #, DOES NOT EQUAL,NOT EQUAL TO		
	>, IS GREATER THAN, <, IS LESS THAN		
	>=, IS GREATER THAN OR EQUAL TO		
	<=, IS LESS THAN OR EQUAL TO		

Scriptbefehle 5

NO_DEFAULT

Defaultscript wird nicht ausgeführt

NOSWAP

LOGIN.EXE wird bei einem # nicht aus dem Speicher ausgelagert

SET_TIME {ON|OFF}

Übernehmen der Serverzeit

SHIFT [n]

verschiebt %0..%9 um n Stellen (Default: 1)

auch negative Werte für n sind möglich

SWAP path

Angabe eines Swapverzeichnisses

Scriptbefehle 6

PAUSE|WAIT

Warten auf eine Benutzerreaktion

PCCOMPATIBLE

Wenn der Name der Maschine<>IBM_PC ist, sollte für das Exit die Kompatibilität bekanntgegeben werden.

PROFILE profilescript

Angegebenes Profile (ev. statt standardmäßig vorgesehenem) ausführen

REM[ARK] text

Kommentar

SCRIPT_SERVER server

Das Script wird vom angegeben Server gelesen (nur in Netware V2.x und 3.x gültig).

Scriptbefehle 7

WRITE "text"

\r CR
\n LF
\" "
\7 kurzer Ton
%variable
Verknüpfungszeichen (mit Prioritäten):

;	Zusammenhängen
*,/,%	Produkt, Quotient, Modulo
+,-	Summe, Differenz
>>,<<	Verschieben und abschneiden rechts,links
	(z.B: "100">>2 liefert "1")

Scriptvariablen 1

0	Name des Fileservers
1	Loginname
2..9	scriptparameter
HOUR	Stunde (1..12)
HOUR24	Stunde (0..23)
MINUTE	Minuten (0..59)
SECOND	Sekunden (0..59)
AM_PM	Vor-/Nachmittag (AM,PM)

Scriptvariablen 2

MONTH	Monat (1..12)
MONTH_NAME	Monat (January..December)
DAY	Tag (1..31)
NDAY_OF_WEEK	Wochentag (1..7, 1=So)
DAY_OF_WEEK	Wochentag (Monday..)
YEAR	Jahr (2004,...)
SHORT_YEAR	Jahr (04,...)
GREETING_TIME	Gruß (morning, afternoon or evening)

Scriptvariablen 3

LOGIN_NAME	Benutzername
LOGIN_CONTEXT	Benutzerkontext
CN	NDS-Benutzername
ALIAS_CONTEXT	Alias (Y,N)
REQUESTER_CONTEXT	Kontext, von wo das LOGIN gestartet wurde
FULL_NAME	Vollständiger Benutzername
LAST_NAME	Benutzername
USER_ID	Benutzeridentifikation
PASSWORD_EXPIRES	Anzahl der Tage bis das Password abläuft

Scriptvariablen 4

STATION	Logische Stationsnummer
P_STATION	Physische Stationsnummer
SHELL_TYPE	Netwareshell
NETWARE_REQUESTER	Requester für OS/2
OS	Betriebssystemname (MSDOS,...)
OS_VERSION	Betriebssystemversion (V4.01,...)
MACHINE	Rechnertype (IBM_PC,...)
SMACHINE	Rechnerkurzname (IBM,...)

Scriptvariablen 5

NETWORK_ADDRESS	Adresse des Netzwerkes (8 Hexst.)
FILE_SERVER	Name des Fileservers
property name	Eigenschaft des Benutzers
ACCESS_SERVER	Accessserver aktiv (TRUE|FALSE)
ERROR_LEVEL	Fehlernummer (0=OK)
[NOT] MEMBER OF "group"	(TRUE|FALSE)
<variable>	OS-Environmentvariable

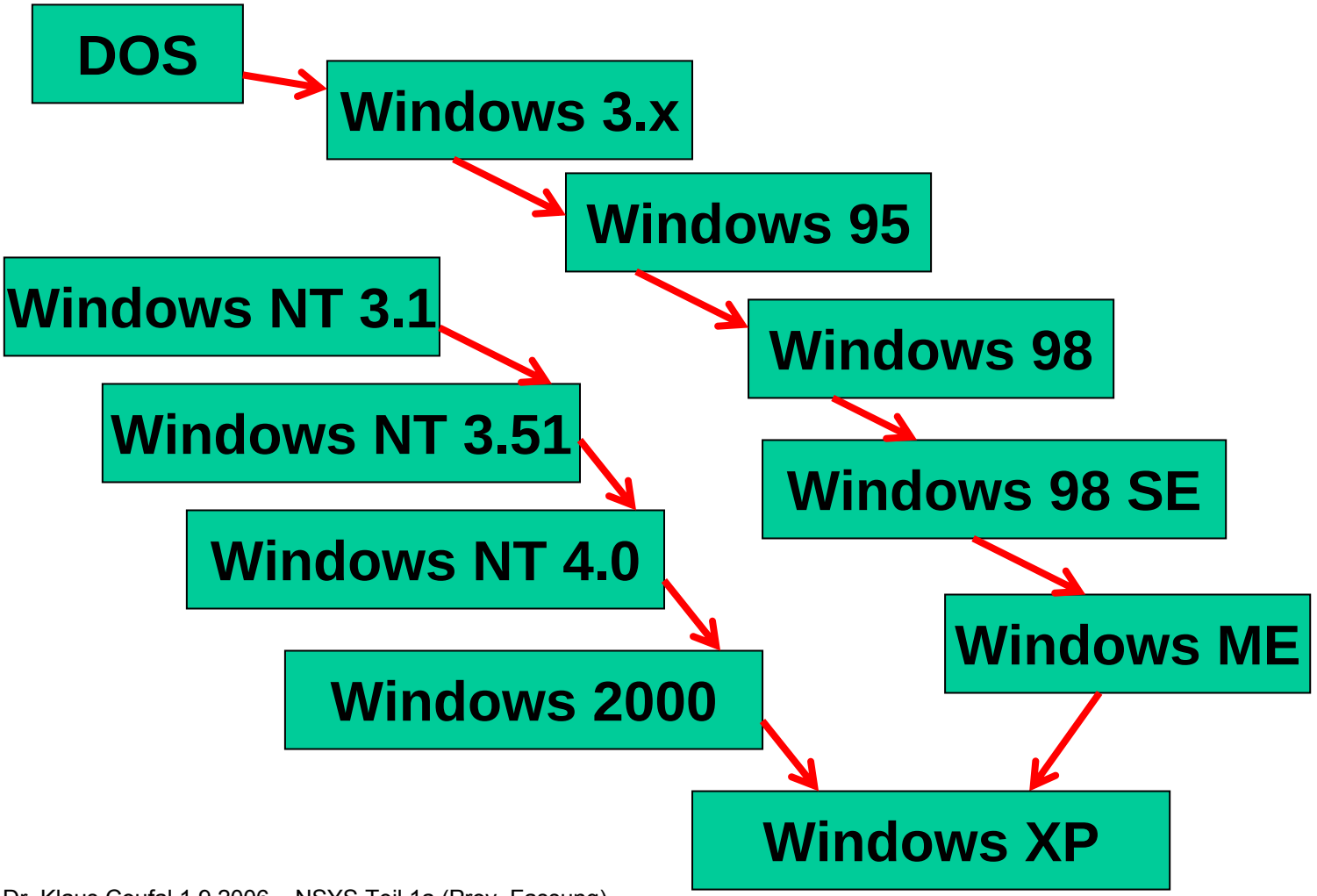
II.6. Windows

- Historische Entwicklung und Versionsübersicht
- Hardwaregrundlagen
- Betriebssystemarchitektur
- Domänenkonzept
- Aufbau der Client-Server-Verbindung
- Dateikonzepte

Windows

- Drucken im Netz
- Betreuung von Arbeitsgruppen
- Wartungstätigkeiten
- Netzwerksicherheit
- Hilfsprogramme

NT – Übersicht



NT – Varianten

- Windows NT
  - Workstation
  - Server
- Windows 2000
  - Professional
  - Server
  - Advanced Server
  - Data Center Server
- Windows XP
  - Home
  - Professional
- Windows 2003
  - Server
  - ...

Hardwaregrundlagen

- Wurde nicht für eine Hardwareplattform konzipiert
- Mindestanforderungen an Hardware für ein Multitasking-Betriebssystem
- Zwischenschicht ⇨ **HAL** (Hardware Abstraction Layer)
- Bei NT mehrere Plattformen möglich

NT-Architektur

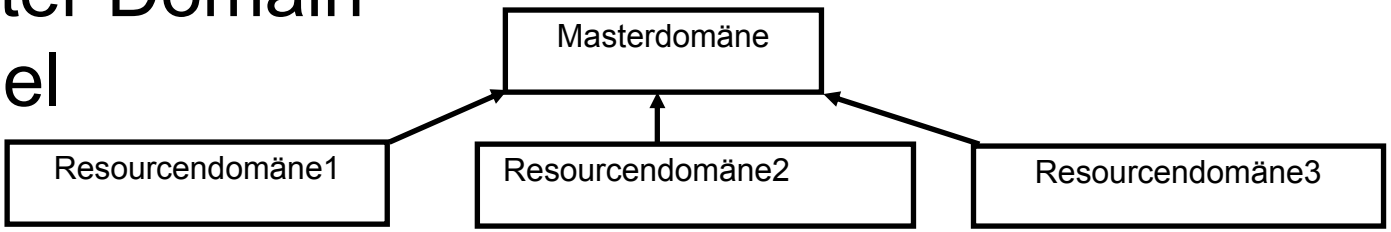
<table>
<tr><td>Anmelde-prozess</td><td>Win32-An-wendung</td><td>POSIX-An-wendung</td><td>OS/2-An-wendung</td><td>An-wendung</td><td>An-wendung</td><td>...</td><td rowspan="2">User-Mode</td></tr>
<tr><td>Security-Subsystem</td><td>Win32-Subsystem</td><td>POSIX-Subsystem</td><td>OS/2-Subsystem</td><td>Sub-system</td><td>Sub-system</td><td>...</td></tr>
<tr><td rowspan="3">I/O-Man-ager</td><td>Window-manager</td><td>Object-manager</td><td>Security (SAM)</td><td>Process-manager</td><td>Local Procedure Call (LPC)</td><td>VM-manager</td><td rowspan="3">Kernel Exe-cutive</td></tr>
<tr><td rowspan="2">Grafik-geräte-treiber</td><td colspan="5">Kernel</td></tr>
<tr><td colspan="5">HAL</td></tr>
<tr><td colspan="7">Hardware</td><td></td></tr>
</table>

Domänenkonzept

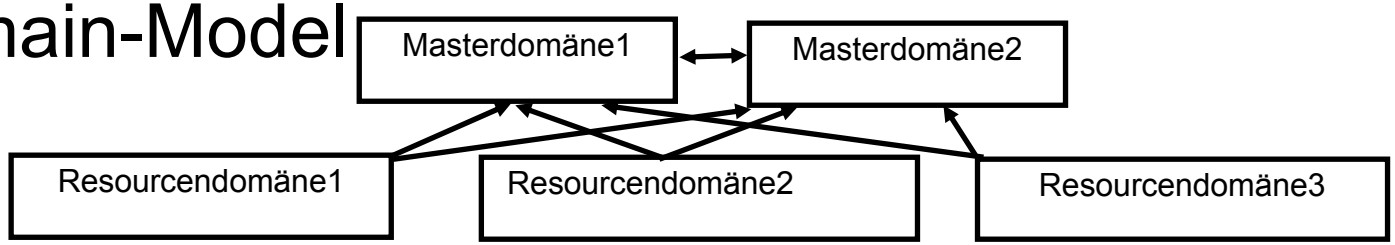
- Einordnung
  - **Einzelplatz-PC → Arbeitsgruppe → Domäne**
- Definitionen
  - **Domäne**
  - **PDC**
  - **BDC**
  - **Server**
  - **Single Domain**
  - **Trusted Domain**
  - **Trusting Domain**
  - **Master Domain**
  - **Resource Domain**

Domänenmodelle

- Single Domain-Model
- Master Domain-Model



- Multiple Master Domain-Model



Aufbau WS-Server-Verbindung

- Hardwareverbindung
- Softwareverbindung
  - Hardware-Softwareschnittstelle (NDIS)
  - Schnittstelle zwischen WS-OS und NOS
- Redirectorvarianten
  - Abhängig vom Betriebssystem am Arbeitsplatz
- Anmelden
  - z.B.: NET LOGON

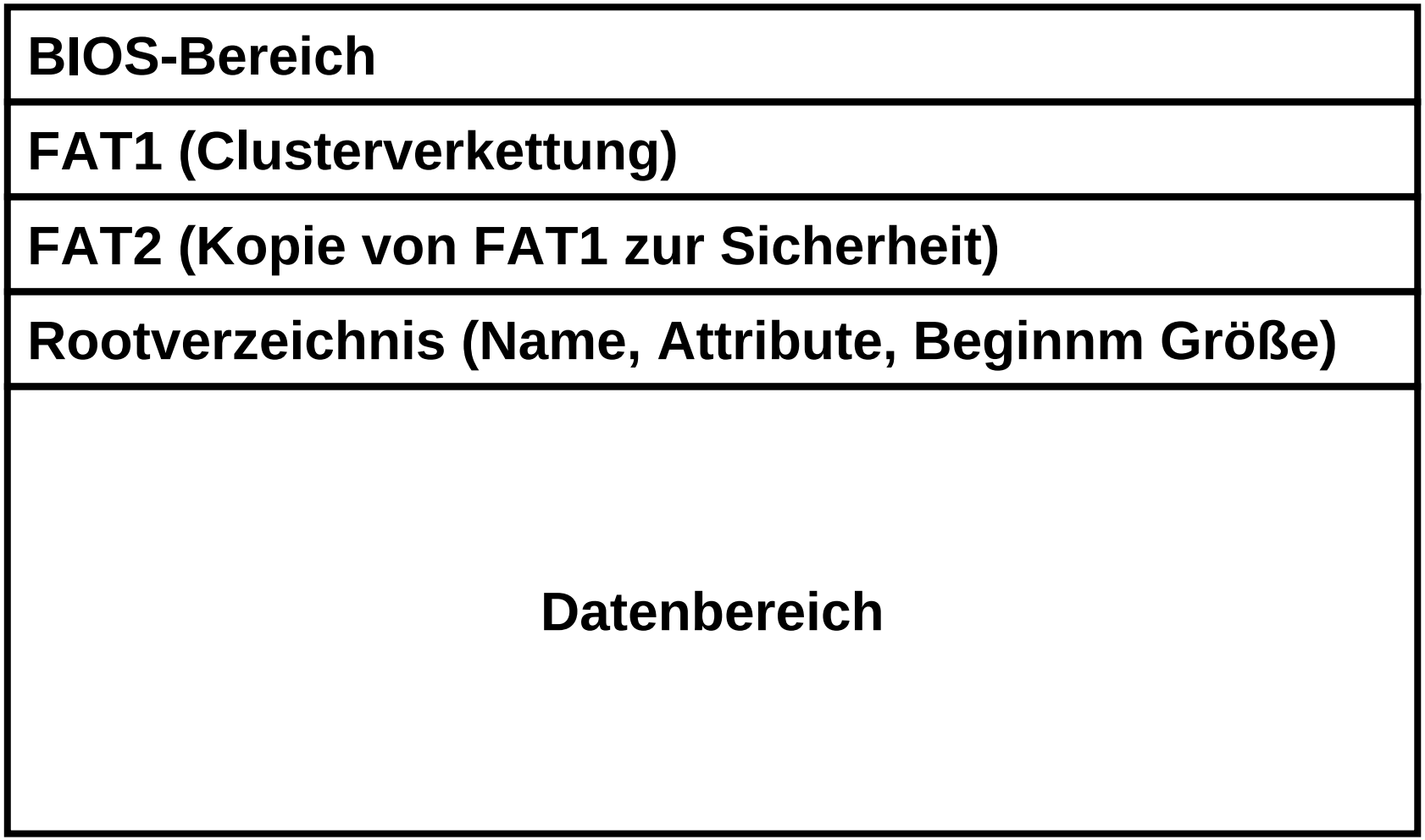
NT-Dateikonzepte

- Lokale Dateisysteme:
  - FAT (File Allocation Table)
  - HPFS (High Performance File System)
  - NTFS (NT-File System)
- Netzwerkdateisysteme
  - UNC (Universal Naming Convention)
  - CIFS (Common Internet File System)

FAT – Eigenschaften

- Dateinamen in 8.3-Konvention
- Nur vier Dateiattribute (S,H,R,A)
- Maximale Partitionsgröße 4GB
- Steigende Platzverschwendung bei Partitionen über 32 MB
- Keine Sicherheitsfunktionen
- Keine Ausfallssicherheit

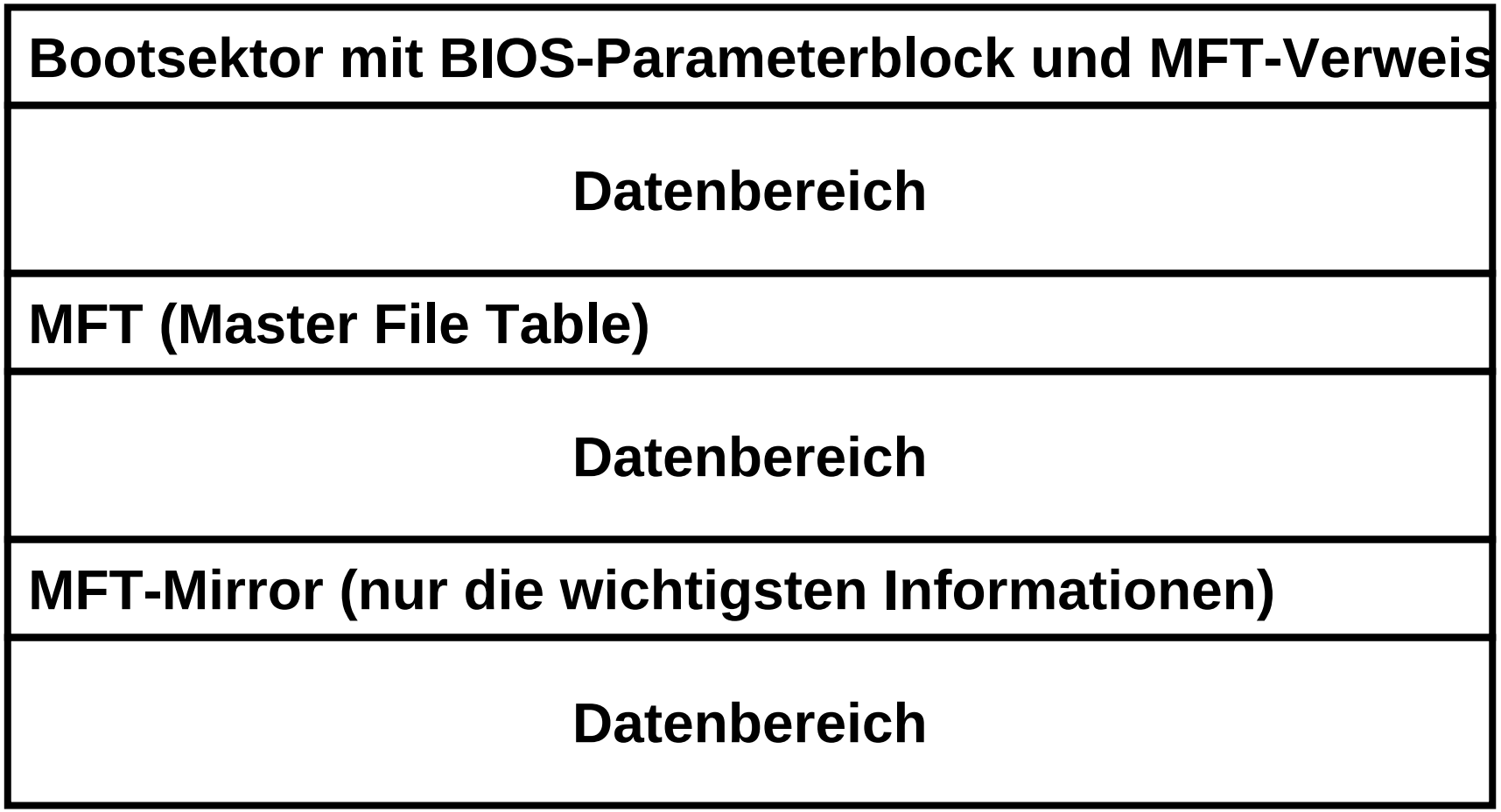
FAT – Aufbau


BIOS-Bereich
FAT1 (Clusterverkettung)
FAT2 (Kopie von FAT1 zur Sicherheit)
Rootverzeichnis (Name, Attribute, Beginnm Größe)
Datenbereich

NTFS – Eigenschaften

- Lange Dateinamen mit Sonderzeichen
- Nicht nur ASCII-Zeichen, sondern Unicode
- Keine Beschränkungen bei der Pfadangabe
- erweiterte Dateiattribute (beliebig groß)
- Partitionsgröße bis 16 EB (2^{64})
- Ständige Protokollierung der Dateizugriffe, damit verbesserter Ausfallsschutz
- Zugriffssicherheit

NTFS – Aufbau


Bootsektor mit BIOS-Parameterblock und MFT-Verweis
Datenbereich
MFT (Master File Table)
Datenbereich
MFT-Mirror (nur die wichtigsten Informationen)
Datenbereich

NTFS – MFT

- 16 Einträge der MFT für Verwaltung
- Jeder Eintrag in der MFT hat 2KByte
- Kleinere Dateien direkt in der MFT
- Dateien nicht sequentiell angeordnet
- Dateien/Verzeichnisse komprimierbar
- Residente Attribute – Externe Attribute
- Verzeichnisse

NTFS – MFT Sicherheit

- Sicherheit vor Datenverlust
  - Hot-Fixing
  - Plattenspiegelung
  - RAID-Verfahren
  - Transaktionsmanagement
- Sicherheit vor Missbrauch
  - Erweiterte Sicherheitsattribute (ACLs)

NTFS – MFT Attribute

- Liste
- Dateiname
- MS-DOS-Kurzname
- Version
- Standardattribute (Größe, Erzeugungs-, Änderungs- und Zugriffsdaten, ...)
- Sicherheitsbeschreibung

NTFS –Aufbau der MFT

Eintrag 0 - $mft (Beschreibung der MFT selbst)
Eintrag 1 - $mftmirror (Beschreibung der Kopie)
Eintrag 2 - $logfile
...
Eintrag 16 – 1. Datei
...

NTFS –Aufbau MFT-Record

Header (Allg. Systeminfos, Transaktionsinfos
Attribut Standardinformationen (Größe, Datum, Uhrzeit (Erzeugung, letzter Zugriff, ...), FAT-Attribute)
Attribut Dateiname
Daten (bei kleineren Dateien der Inhalt, sonst Zeiger auf den Datenbereich)
Attribut Sicherheitsbeschreibung (ACLs, ...)

Drucken im Netz – Überblick

- Arbeitsstationen können lokale und freigegebene Drucker verwenden
- Jeder lokaler Drucker kann freigeben werden (und ist damit ein Netzwerk-drucker)
- Ein expliziter Printserver ist nicht vorgesehen

Drucken im Netz – Datentypen

EMF	Enhanced Meta Files (neu seit NT 4.0)
RAW	Druckbereite Daten, die direkt an den Drucker übergeben werden können
RAW (FF appended)	RAW-Daten, denen ein FF hinzugefügt wird
RAW (FF auto)	RAW-Daten, denen bei Bedarf ein FF hinzugefügt wird
Text	Einfacher Text ohne Formatanweisungen
Pscript I	Postscipt-Daten (z.B. von MAC-Clients)

Druckerinstallation

- Assistenten für die Druckerinstallation
  - Lokal
  - Netzwerk
- Mehrere logische Drucker sind für einen physischen Drucker möglich (z.B.: verschiedene Zugriffszeiten, ...)
- Verknüpfung mit dem Drucker auf dem Desktop ist oft sinnvoll

Druckerkonfiguration 1

- Allgemeine Konfiguration
  - „Allgemein“ (Trennseite, Druckprozessor, Treiber erneuern, Testseite drucken)
  - „Anschlüsse“ (Anschluß (LPT1:, ...) kann verändert werden)
  - „Zeitplanung der Druckaufträge“ (Zeiten, die Priorität der Druckaufträge, Warteschlangenverwendung)
  - „Freigabe“ (Name des Drucker im Netz, Treiber
  - „Sicherheit“ (Zugriffsberechtigungen, Überwachung, Besitz)
  - „Geräteeinstellungen“ (gerätespezifische Einstellungen (z.B.: der installierte Speicher, ...))

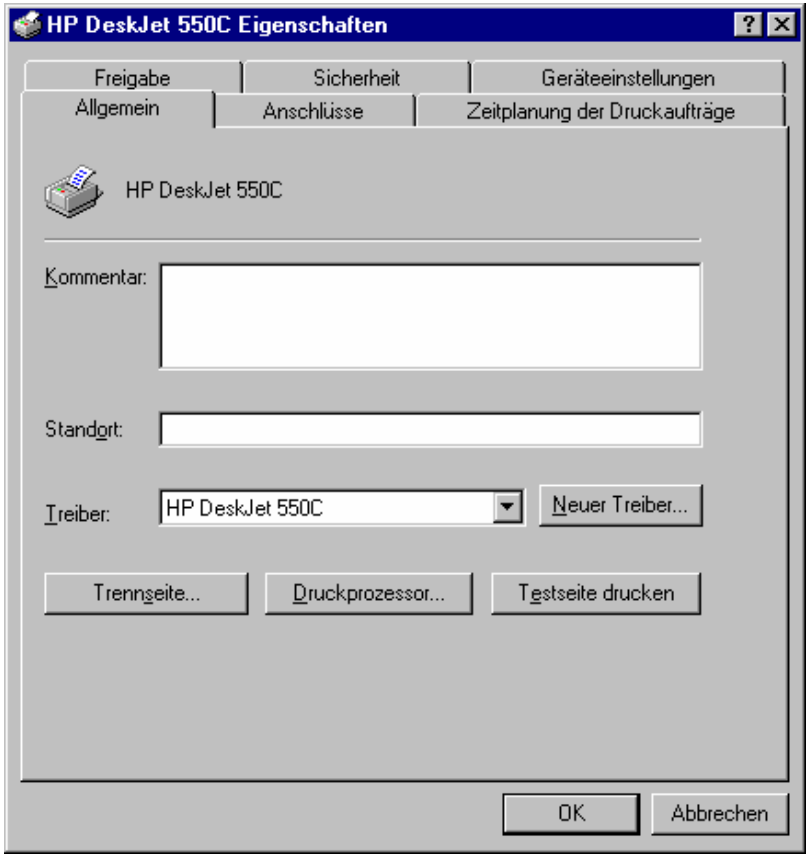
Druckerkonfiguration 2

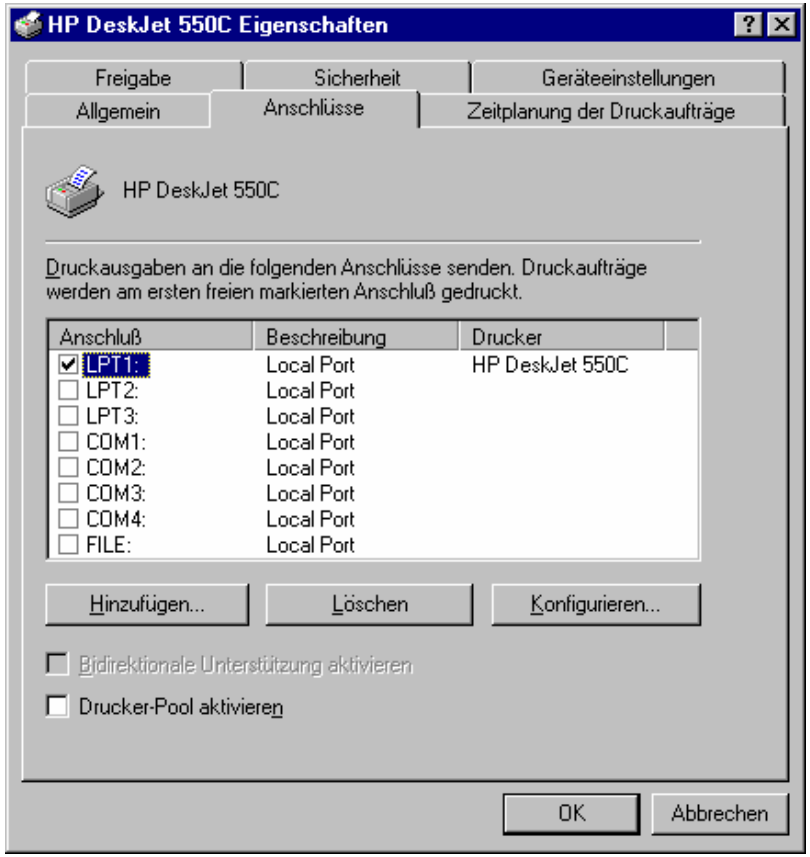
- Druckserverkonfiguration
- Formulare
- Anschlüsse
- Optionen
  - Warteschlangeordner
  - Protokollumfang
  - …

Druckerkonfiguration 3

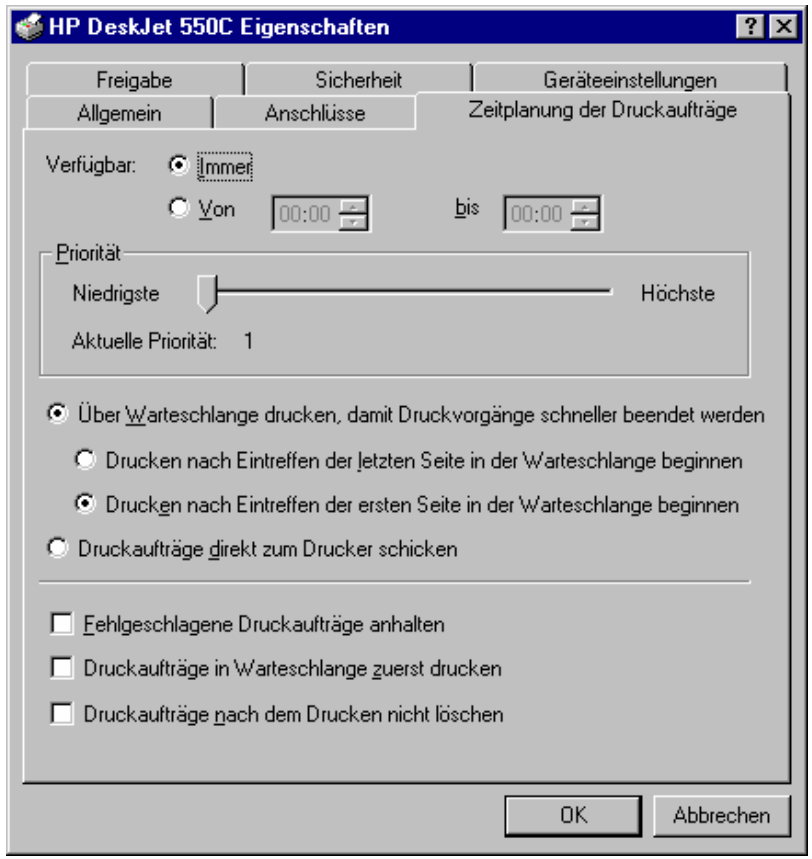
- Über „START → Einstellungen → Drucker“ oder „Arbeitsplatz → Drucker“ gelangt man zur Liste der vorhandenen Drucker bzw. zum Assistenten für die Druckerinstallation
- Durch Doppelklick auf das Symbol „Neuer Drucker“ wird der Assistent gestartet
- Durch Klick auf das Symbol des gewünschten Druckers und „Datei → Eigenschaften“ kommt man zum Konfigurationsmenü des Druckers
- Durch Klick auf das Symbol des gewünschten Drucker und „Datei → Servereigenschaften“ kommt man zum Menü des zum Drucker gehörigen Servers. (Formulare, Anschlüsse, Optionen)

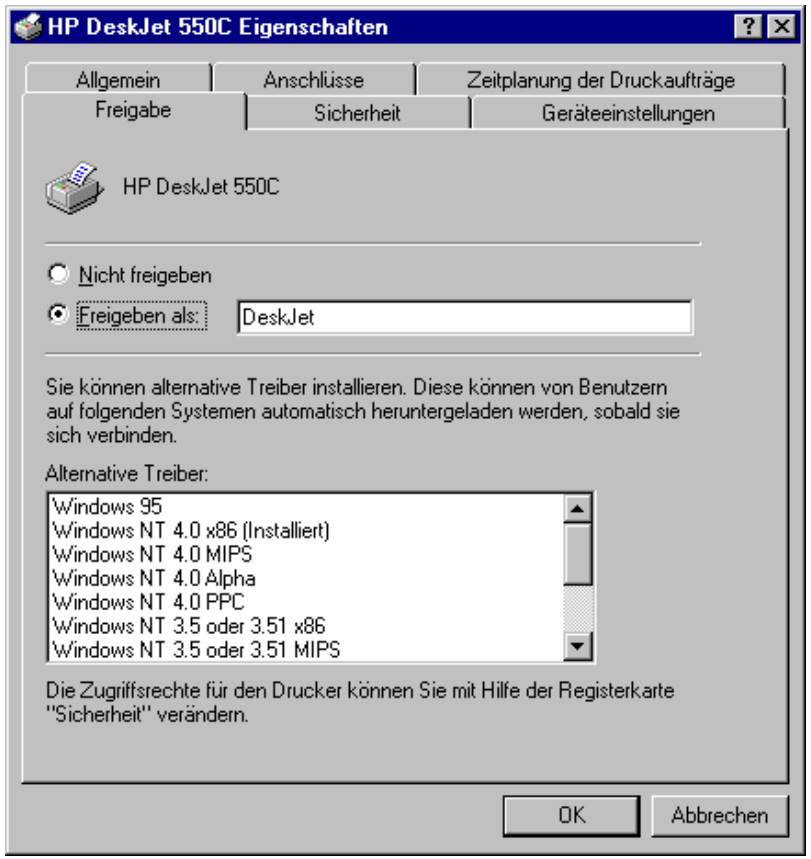
Druckerkonfiguration 4



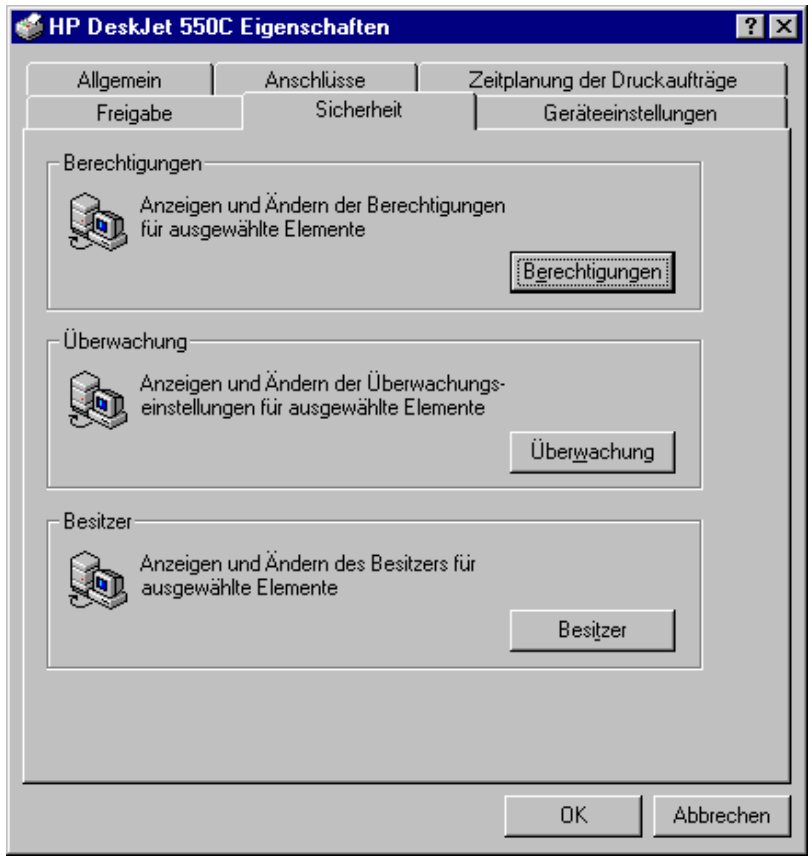


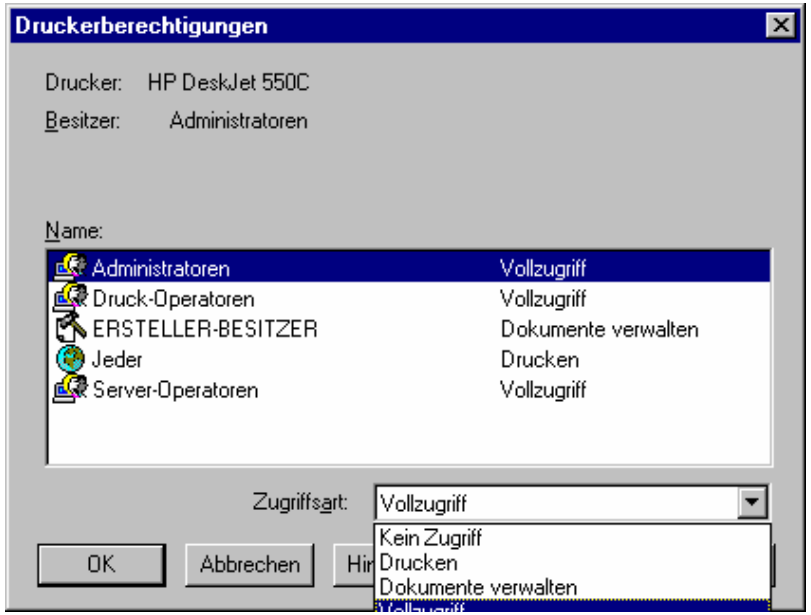
Druckerkonfiguration 5



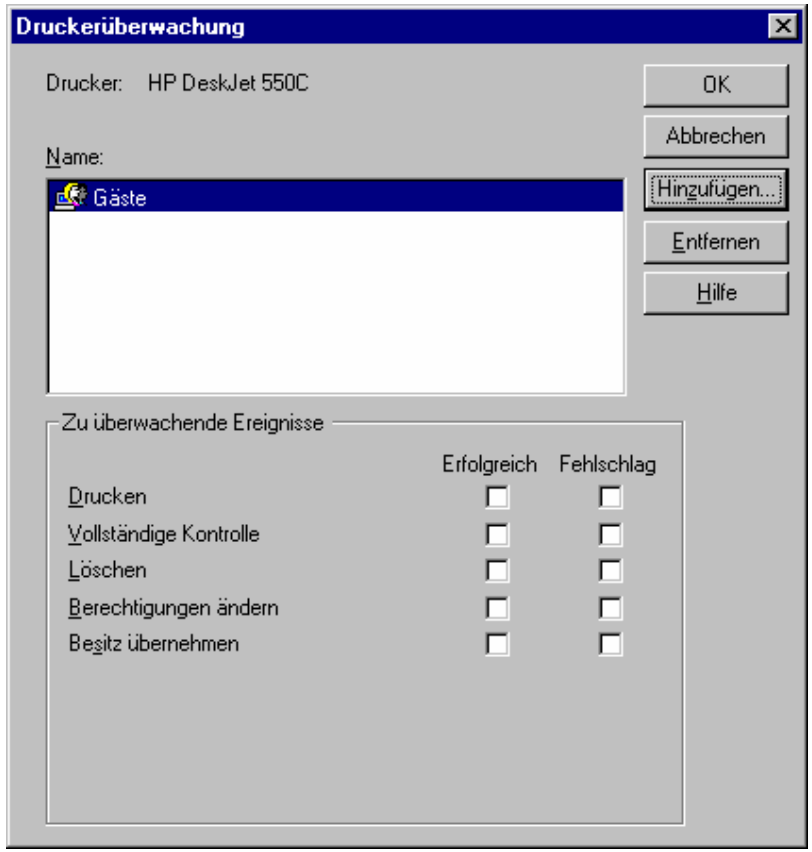


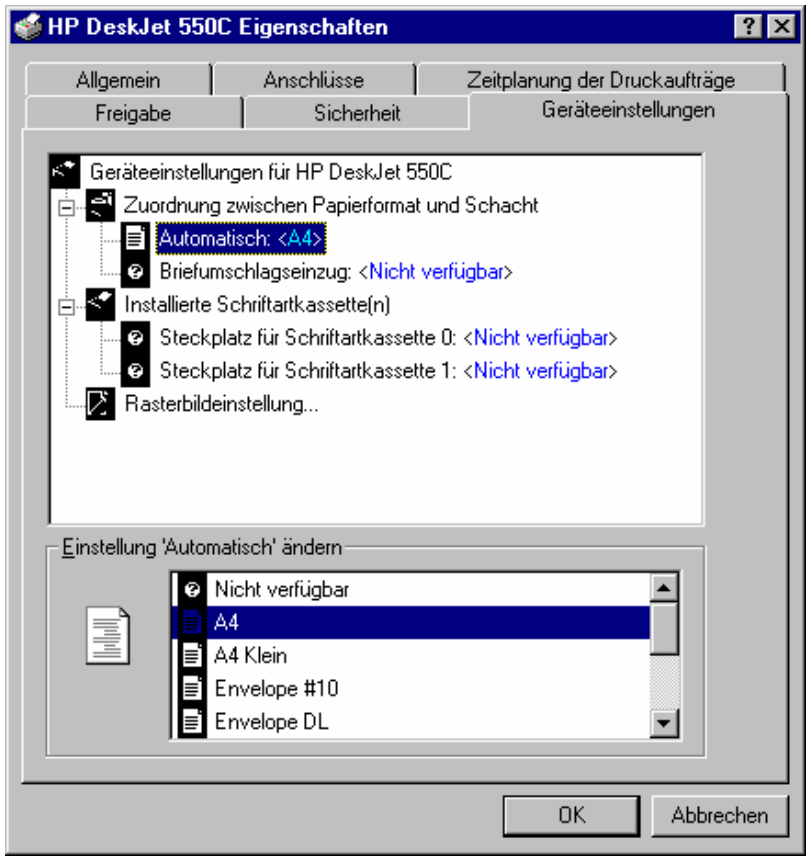
Druckerkonfiguration 6





Druckerkonfiguration 7





Druckmanager 1

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

Druckmanager 2

- Datei
  - Drucker anhalten
  - Als Standarddrucker verwenden Ja/Nein
  - Einstellungen für Dokumente (druckerabhängig)
  - Freigabe
  - Druckaufträge löschen
  - Eigenschaften (siehe Druckerkonfiguration)
  - Schließen

Druckmanager 3

- Dokument
  - Anhalten
  - Fortsetzen
  - Neu starten
  - Abbrechen
  - Eigenschaften
- Ansicht
- ? (Hilfe)

Betreuung von Arbeitsgruppen

- Spezielle Administratoren für Teilbereiche sind in Windows NT/2000 nicht vorgesehen
- Benutzereinrichten
  - Ein Anlegen vieler Benutzer mittels einer Liste ist nicht vorgesehen
- Gruppeneinrichten
- Richtlinien

Benutzereinrichtung

- Benutzername (Max. 20 Zeichen)
- Paßwort (max. 14(NT) Zeichen)
- Gruppenzugehörigkeit
- Umgebungsprofil
- Anmeldezeiten
- Anmeldearbeitsstationen
- Kontoinformation
- Einwählinformation

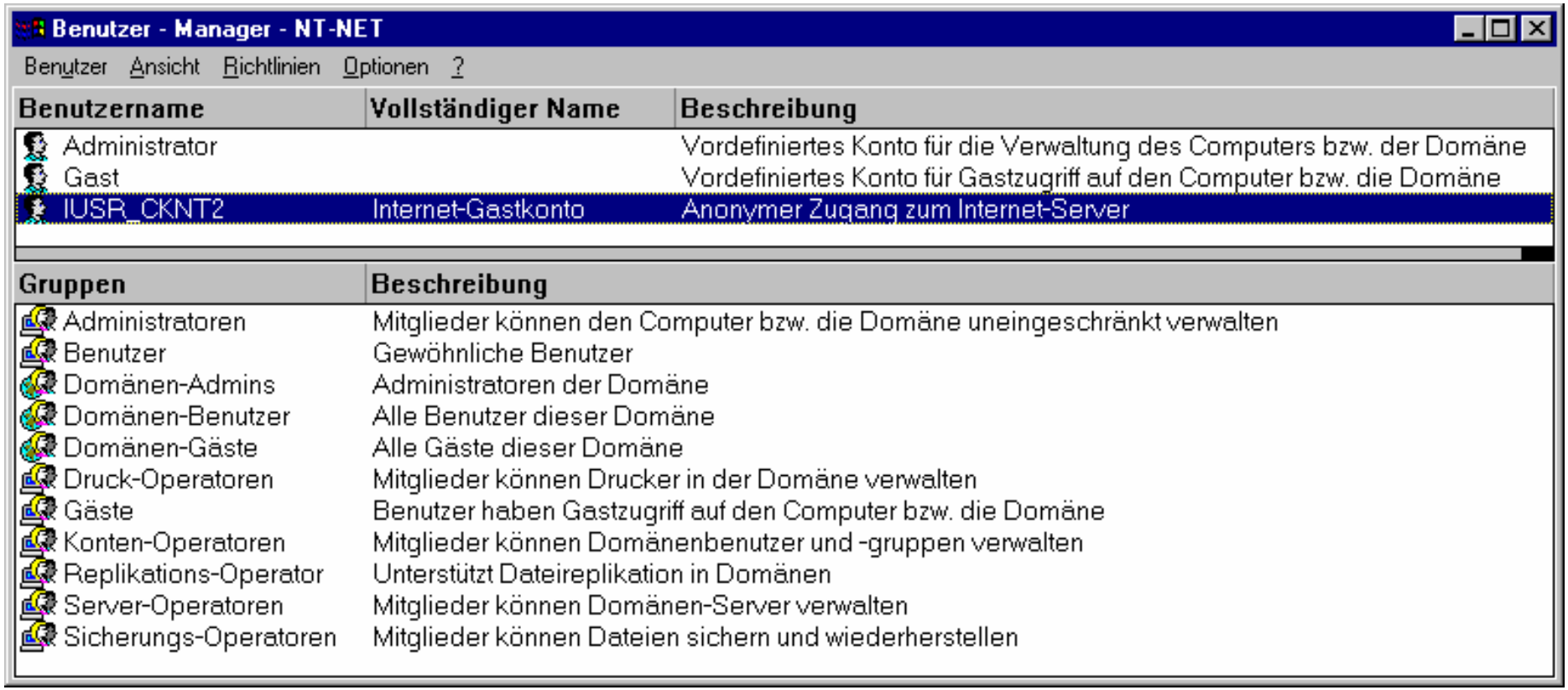
Gruppen

- Die wichtigsten lokalen Gruppen sind:
  - Administratoren — Vollständige Kontrolle
  - Benutzer — Alle lokalen Benutzer
  - Druckoperatoren — Verwaltung der Drucker
  - Gäste — Lokale Gäste
- Die wichtigsten globalen Gruppen sind:
  - Domänen-Admins — Kontrolle über die Domäne
  - Domänen-Benutzer — Benutzer der Domäne
  - Domänen-Gäste — Gäste in der Domäne

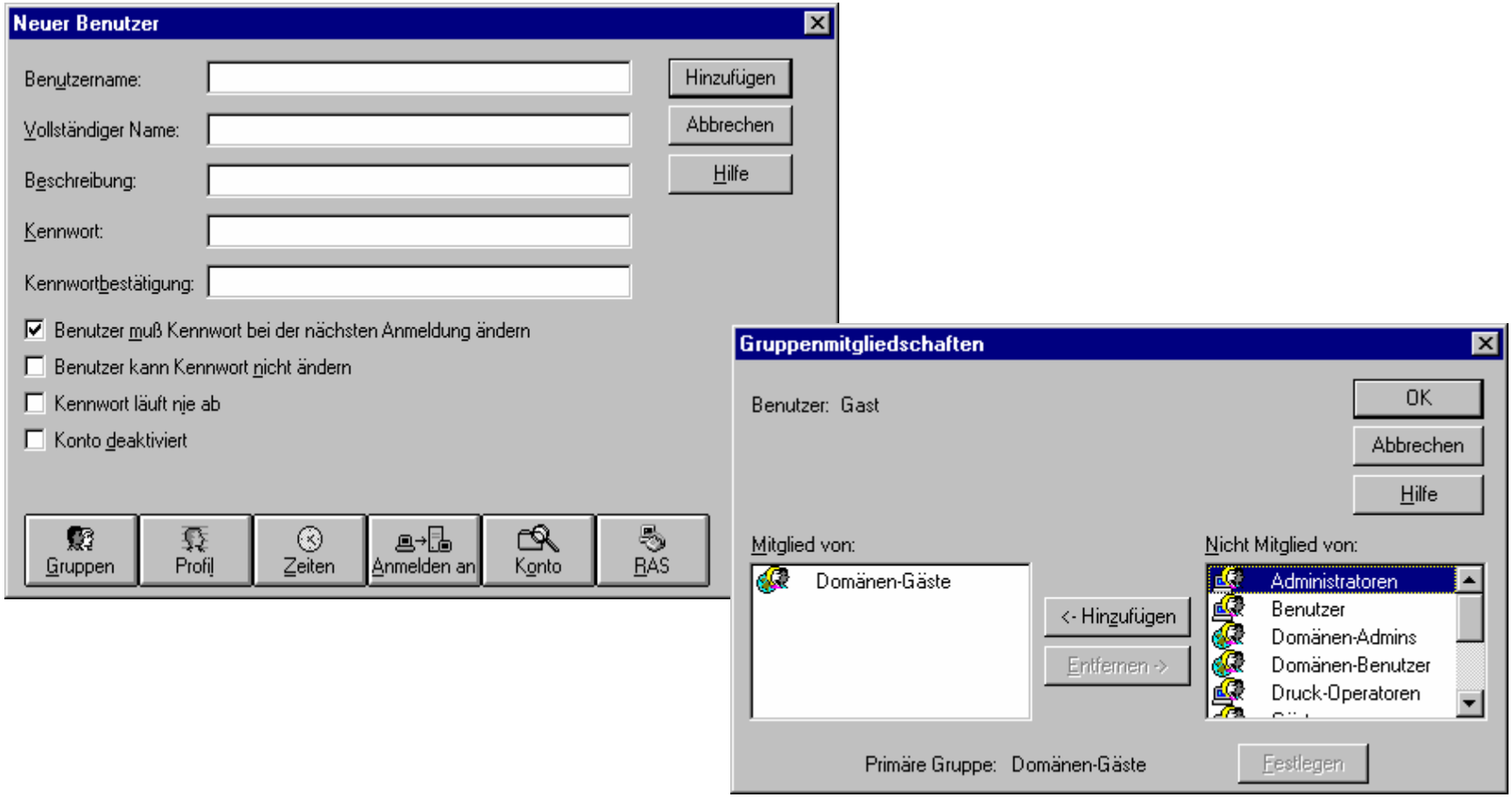
Richtlinien

- Richtlinien für alle Benutzerkonten
- Richtlinien für Benutzerrechte
- Überwachtungsrichtlinien
- Vertrauensstellungen

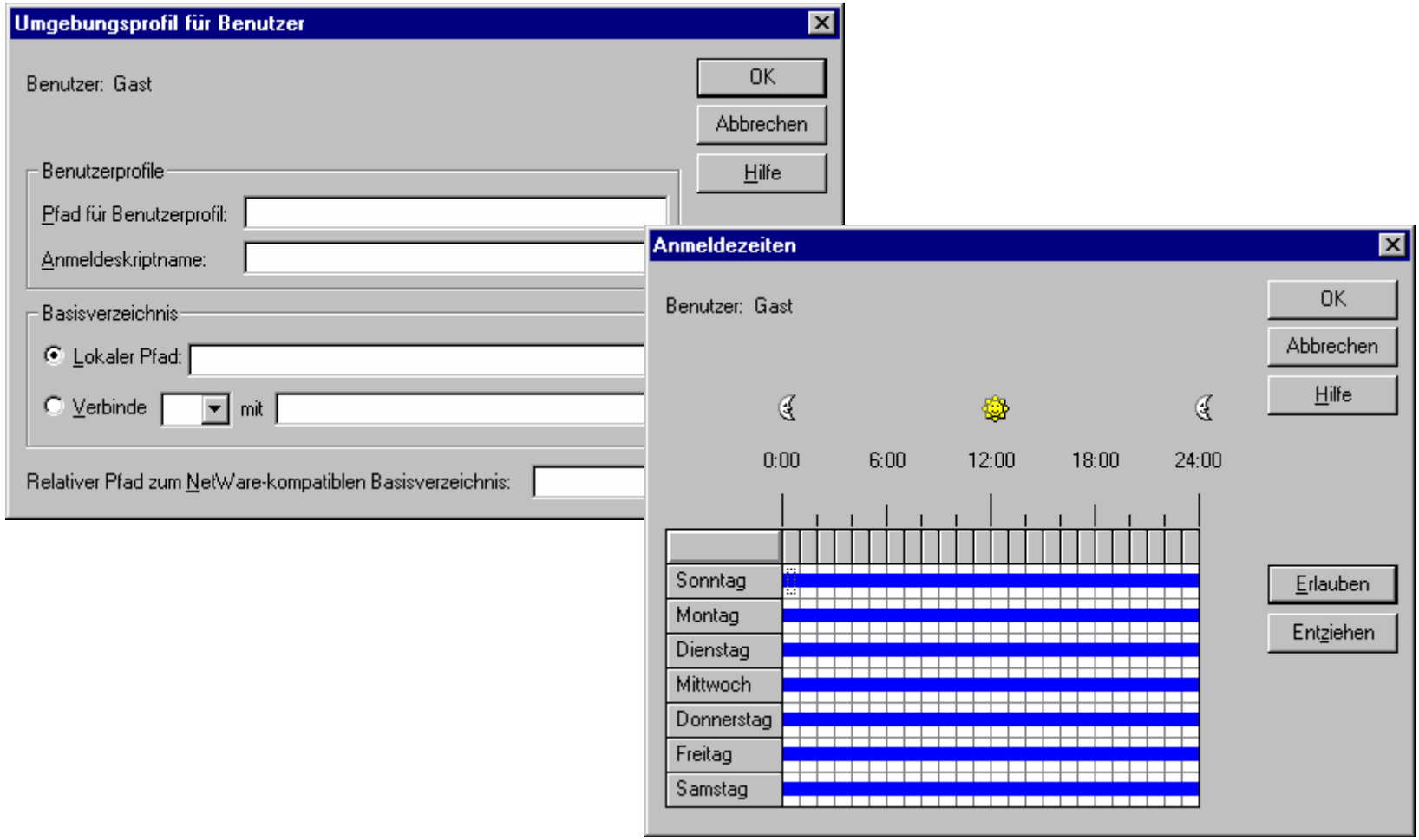
Benutzermanager 1



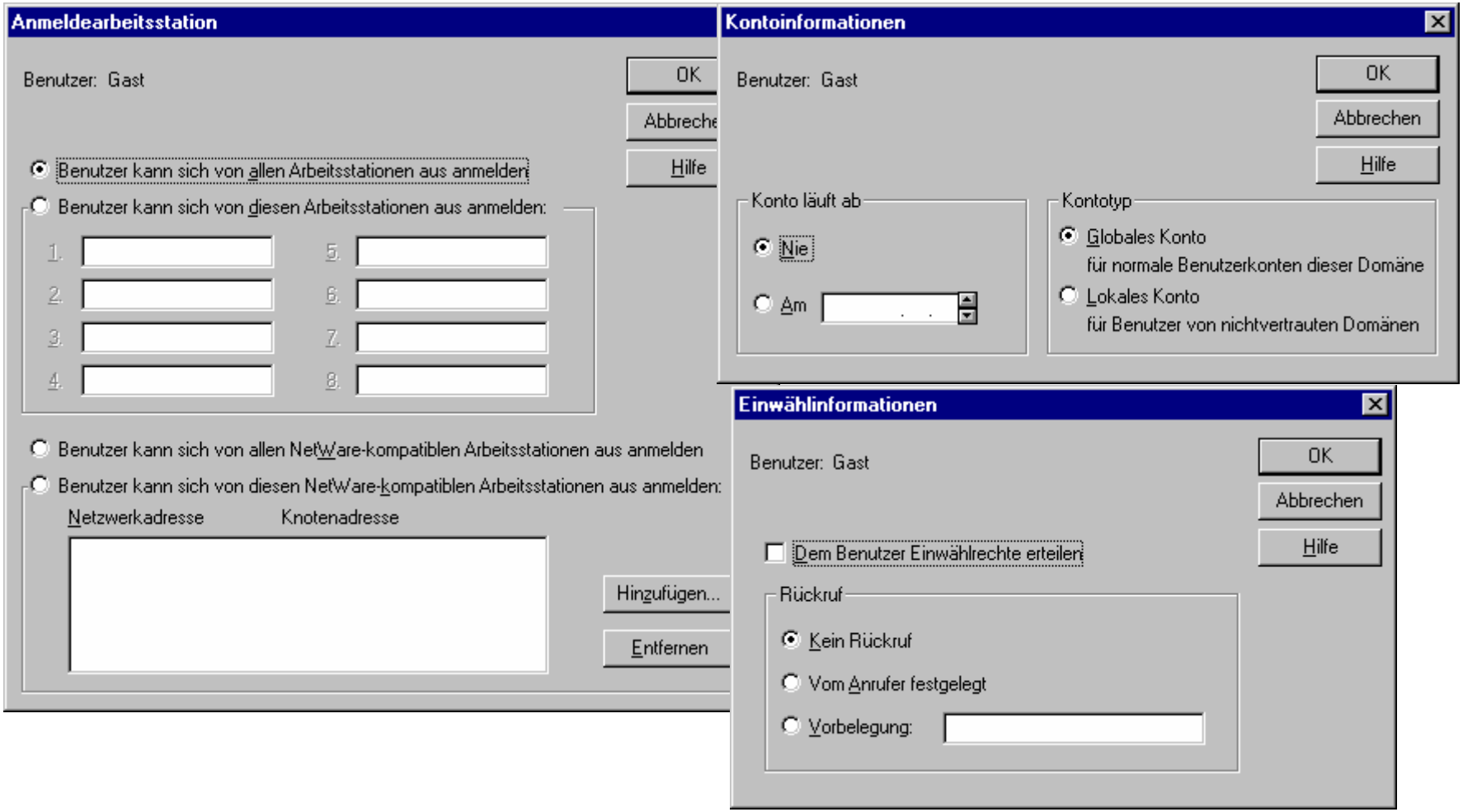
Benutzermanager 2



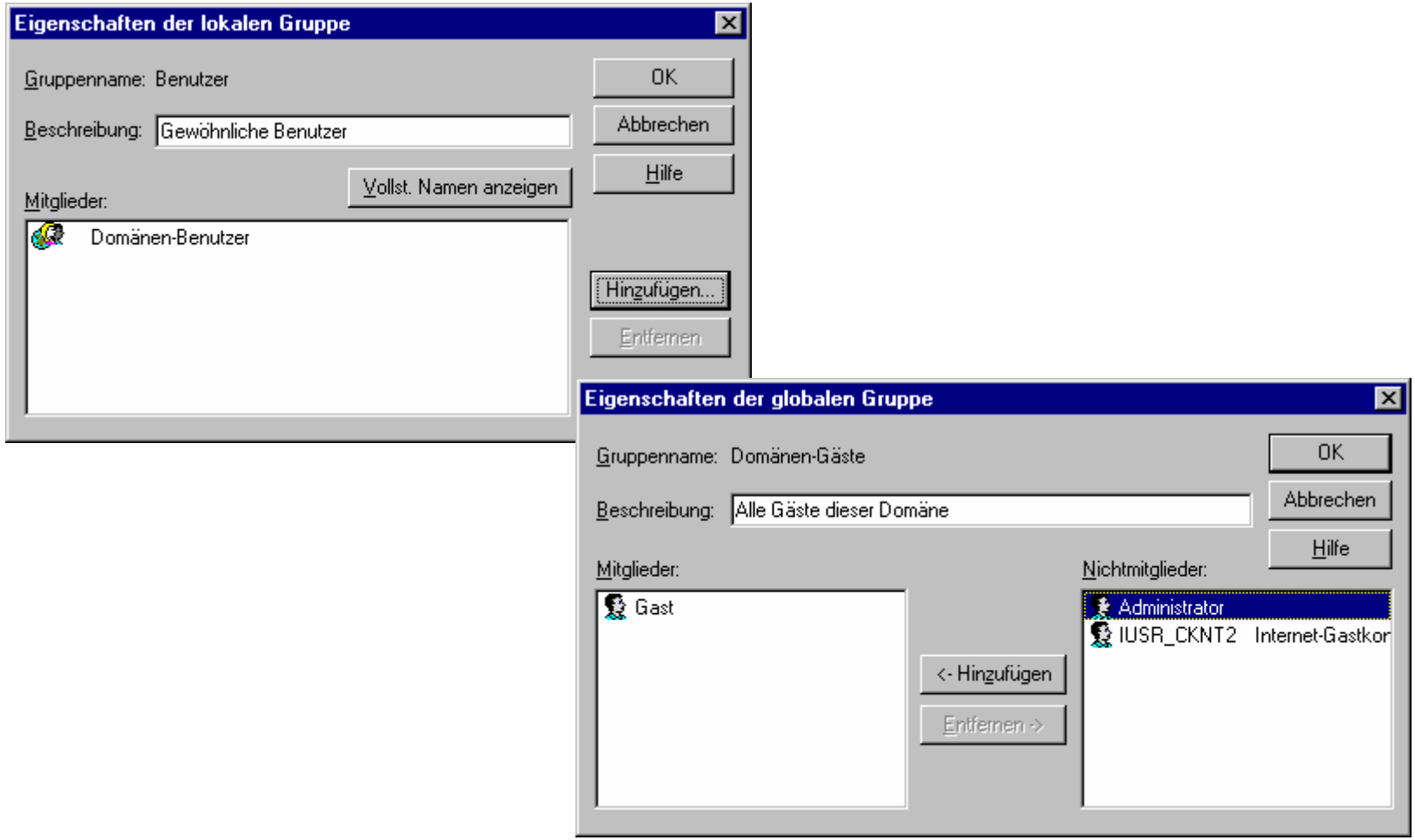
Benutzermanager 3



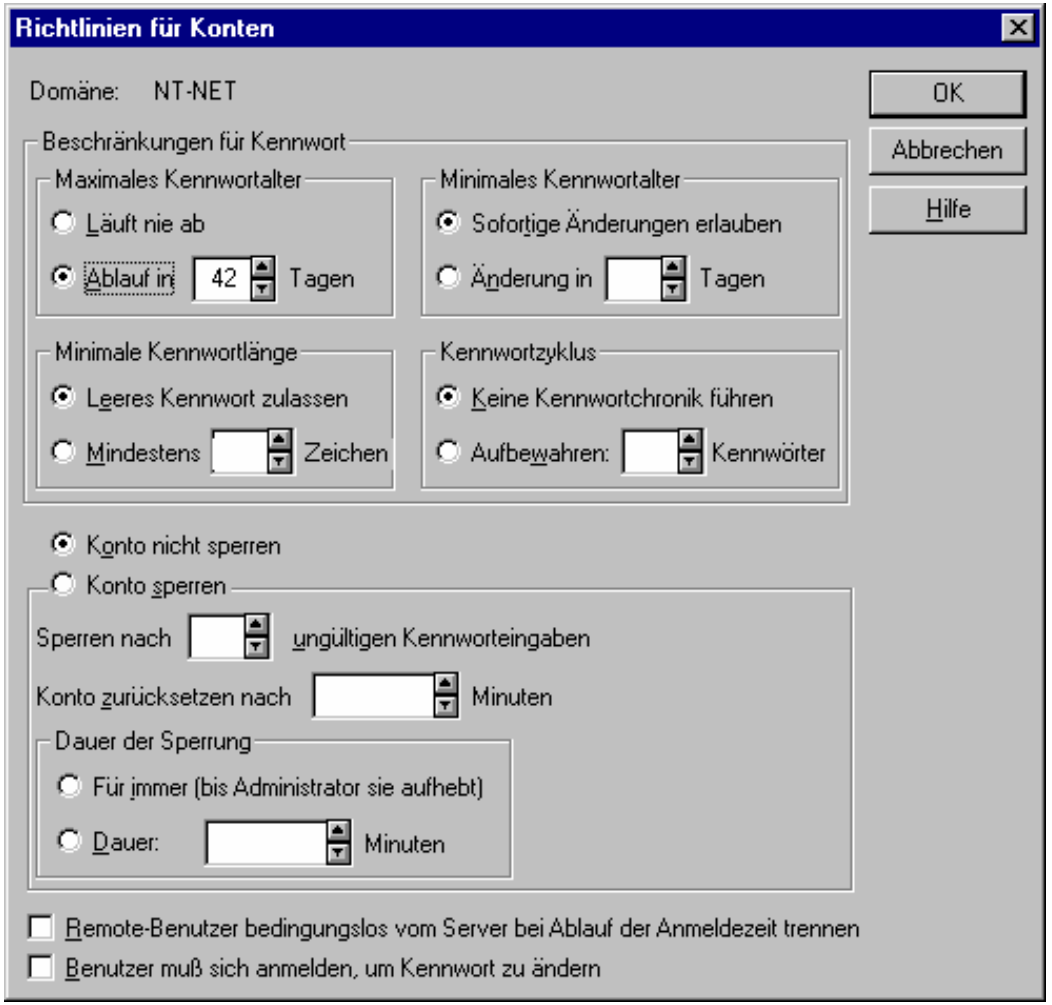
Benutzermanager 4



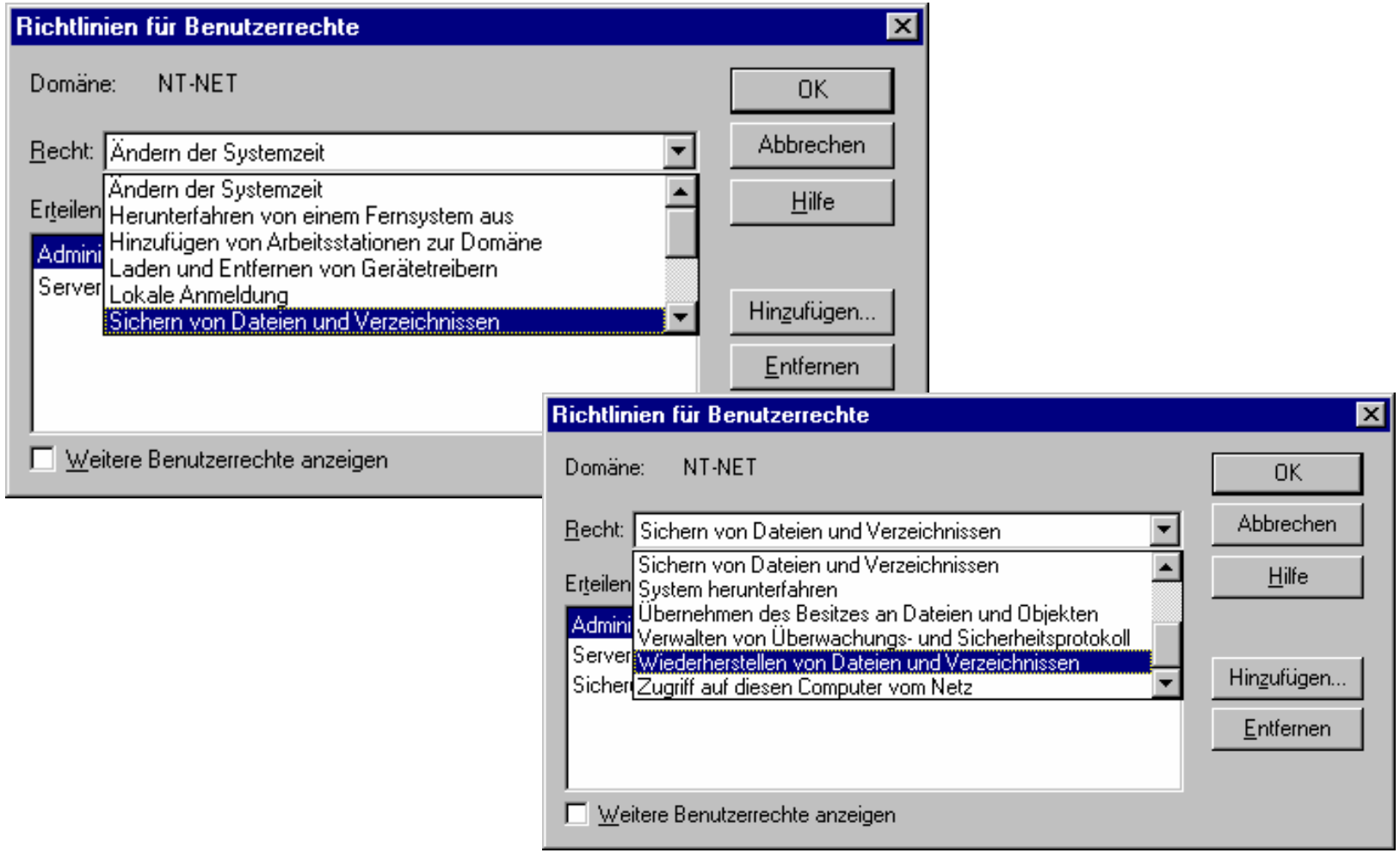
Benutzermanager 5



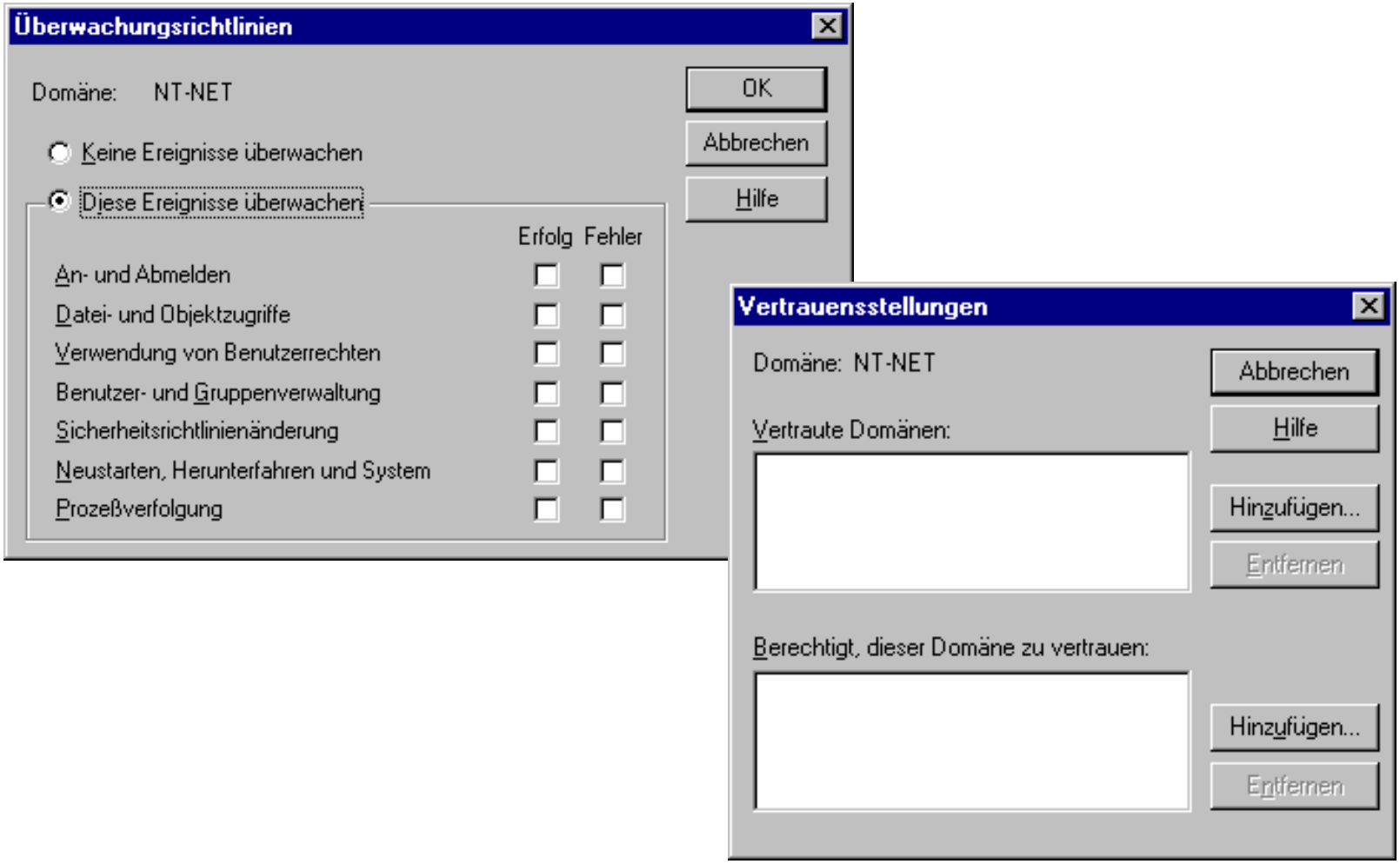
Benutzermanager 6



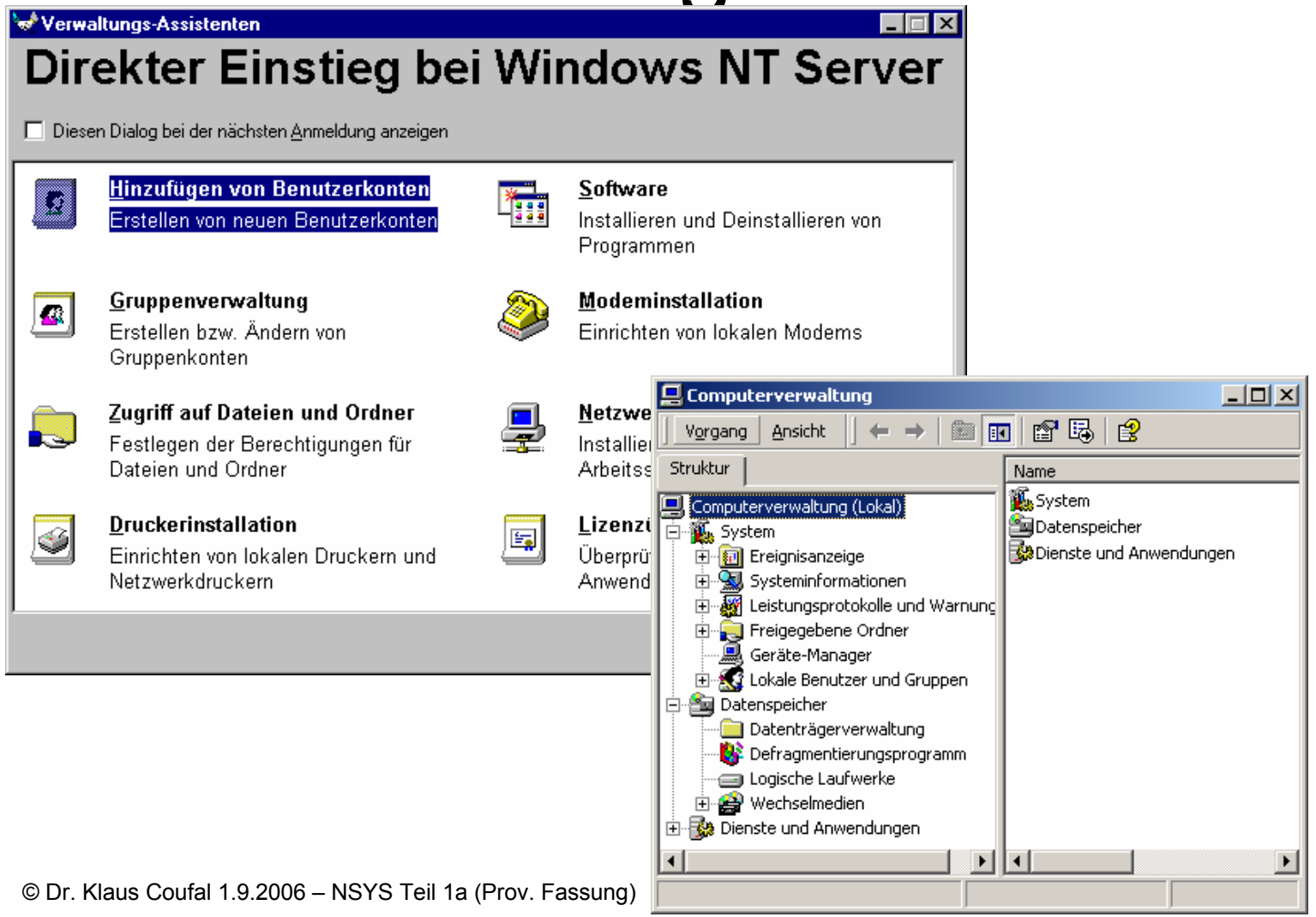
Benutzermanager 7



Benutzermanager 8



Verwaltungsassistent



Wartungstätigkeiten

- Konfigurationsdateien
  - Für Kompatibilität zu älteren Systemen
  - PROTOCOL.INI
  - CONFIG.NT
- Registrierungsdatenbank
  - Datenbank zum Ablegen aller Informationen aus diversen Konfigurationen

Registrierungsdatenbank 1

- Hauptschlüssel
  - HKEY_CLASSES_ROOT (HKCR)
    - (=HKLM\SOFTWARE\Classes)
  - HKEY_CURRENT_USER (HKCU)
  - **HKEY_LOCAL_MACHINE** (HKLM)
  - **HKEY_USERS**
  - HKEY_CURRENT_CONFIG
    - (=HKLM\System\CurrentControlSet\HardwareProfiles\Current)

Registrierungsdatenbank 2

- Format der Einträge
  - REG_BINARY
  - REG_DWORD
  - REG_EXPAND_SZ
  - REG_MULTI_SZ
  - REG_SZ

Registrierungsdatenbank 3

- Dateien

  HKEY_LOCAL_MACHINE\SAM

  %SYSTEMROOT%\CONFIG\Sam

  HKEY_LOCAL_MACHINE\Security

  %SYSTEMROOT%\CONFIG\Security

  HKEY_LOCAL_MACHINE\Software

  %SYSTEMROOT%\CONFIG\Software

  HKEY_LOCAL_MACHINE\System

  %SYSTEMROOT%\CONFIG\System

Registrierungsdatenbank 4

- Dateien

  HKEY_USERS\.DEFAULT

  %SYSTEMROOT%\CONFIG\Default

  HKEY_CURRENT_USER

  %SYSTEMROOT%\Profiles\%USERNAME%\NTUSER.DAT (NT)

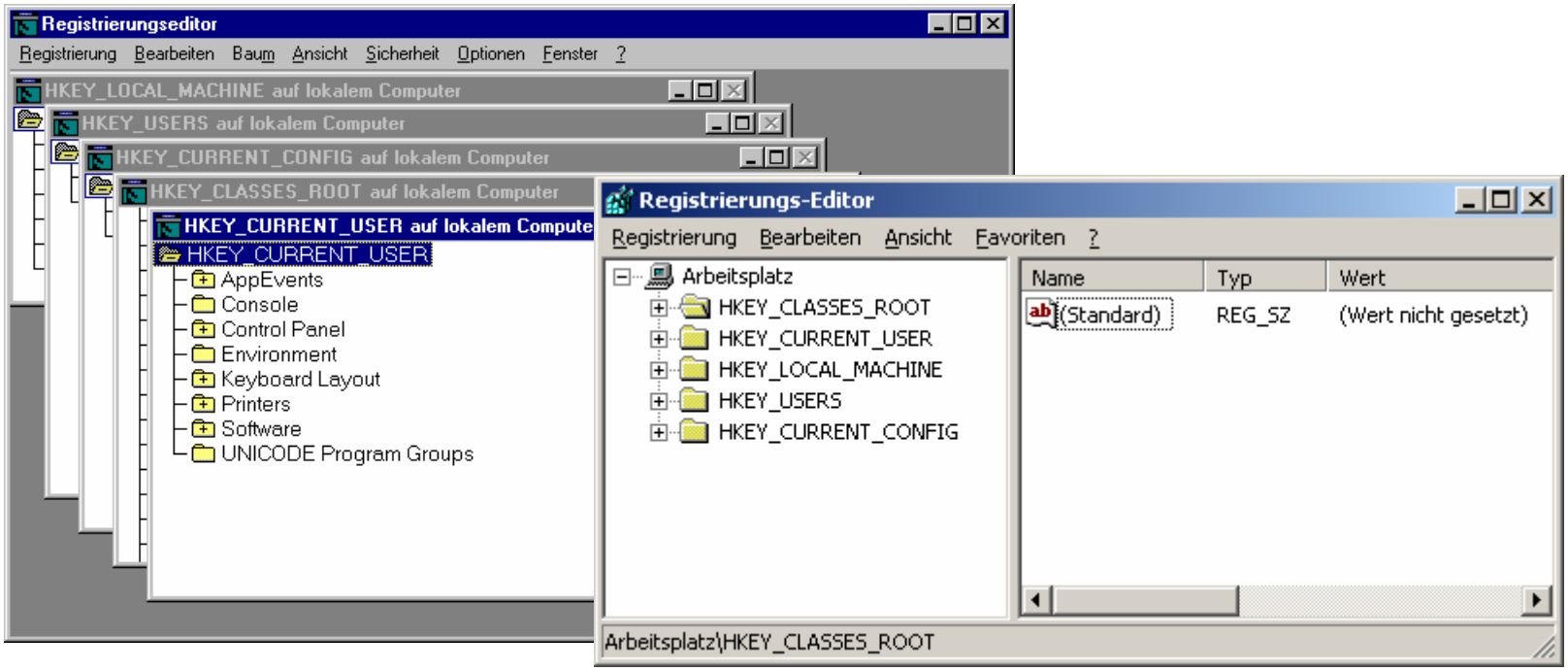
  %SYSTEMDRIVE%\Dokumente und Einstellungen\%USERNAME%\NTUSER.DAT

  (HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList\ProfilesDirectory)

Registrierungsdatenbank 5

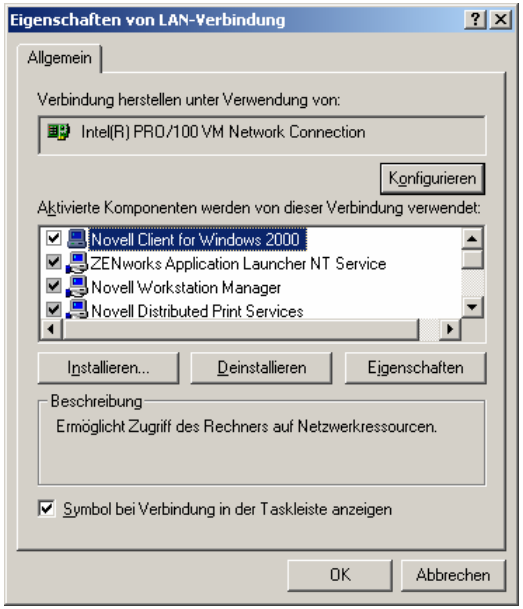
- Der Registrierungseditor

  START→Ausführen→REGEDT32|REGEDIT



Registrierungsdatenbank 6

- Meist wird aber nicht direkt in der Registrierungsdatenbank gearbeitet, sondern mit der Systemsteuerung.



Benutzerprofile

- Speichern HKCU und Benutzer-spezifische Einstellungen (Desktop, …)
- Lokale Profile
  - Ort siehe HKEY_CURRENT_USER
- Server-basierendes Profile
- Mandatory Profile
  - NTUSER.DAT → NTUSER.MAN
- %USERPROFILE% → Profilordner

Scripts

- Batch-Dateien, die bei der Anmeldung eines Benutzer ausgeführt werden
- Zuordnung eines Scripts
  - Im Benutzermanager durch Auswählen eines Benutzer über „Benutzereigenschaften“ → „Profil“
  - Keine Pfadangabe → NETLOGON-Share des Anmeldeserver

Spezielle Scriptvariablen

%COMPUTER_NAME%, %HOMEDRIVE%, %HOMEPATH%, %HOMESHARE%, %OS%, %PROCESSOR_ARCHITECTURE%, %PROCESSOR_IDENTIFIER%, %PROCESSOR_LEVEL%, %PROCESSOR_REVISION%, %SYSTEMDRIVE%, %SYSTEMROOT%, %USERDOMAIN%, %USERNAME%

Beispielscript

```
@ECHO OFF
NET USE H: \\NTSERVER\DATEN
NET USE LPT2:
   \\DRUCKERSERVER\DESKJET
IF NOT EXIST
   %SYSTEMROOT%\SYSTEM\UPDATE.EXE
   GOTO EXIT
UPDATE
:EXIT
```

Netzwerksicherheit

- Überblick
- Zutrittsschutz
- Zugriffsschutz
- Hilfsprogramme

Überblick

- Wie schon vorher besprochen, kann in einem Netzwerk zwischen drei Sicherheitsaspekten unterschieden werden:
  - Zutrittsschutz
  - Zugriffsschutz
  - Datensicherheit
- Bei manchen Aspekten kann es vorteilhaft sein, noch einen vierten Punkt getrennt zu betrachten:
  - Datenschutz

Zutrittsschutz

- physikalische Verhinderung des Zuganges für unbefugte Personen
- Überprüfung der Identität (meist mittels eines Namens und eines geheimen Kennwortes)
- Accountrestriktionen
- Intruder detection
- Accounting

Accountrestriktionen

Restriktion	Default
Darf der Benutzer sein Passwort ändern	JA
Ist ein Passwort notwendig	NEIN
Mindestlänge des Passwortes	6
Regelmäßige Änderung des Passwortes	JA
Gültigkeitsdauer eines Passwortes	42
Wiederverwendung alter Passwörter	JA
Gültigkeitsdauer des Accounts	„Ewig“
Ist der Account gültig	JA
…	

Intruder detection

- Eine bestimmte Anzahl (z.B.: 3) von Fehlversuchen bei der Passwort-Eingabe innerhalb einer bestimmten Zeit (z.B.: ½ Stunde) wird als „Hack“-Versuch interpretiert.
- Sperre für bestimmte Zeit oder bis der Administrator diese aufhebt
- Protokollierung des Ereignisses

Accounting

Windows NT/2000 unterstützt derzeit kein Accounting, d.h. eine Zuordnung von Kosten zu Benutzern oder Projekten ist nicht automatisierbar

Zugriffsschutz - Rechte

- Auf der Ebene von Verzeichnisfreigaben
  - Kein Zugriff
  - Lesen
  - Ändern
  - Vollzugriff
- Auf der Ebene von NTFS

NTFS - Verzeichnisrechte

R	Lesen	Dateien und Verzeichnisse anzeigen
W	Schreiben	Dateien und Verzeichnisse hinzufügen
X	Ausführen	In die entsprechenden Verzeichnisstruktur wechseln
D	Löschen	Dateien und Verzeichnisse löschen
P	Berechtigungen ändern	Berechtigungen für Dateien und Verzeichnisse ändern
O	Besitz übernehmen	Besitz von Dateien und Verzeichnissen übernehmen

NTFS - Dateirechte

R	Lesen	Datei lesen
W	Schreiben	Datei schreiben
X	Ausführen	Datei ausführen
D	Löschen	Datei löschen
P	Berechtigungen ändern	Berechtigungen der Datei ändern
O	Besitz übernehmen	Besitz der Datei übernehmen

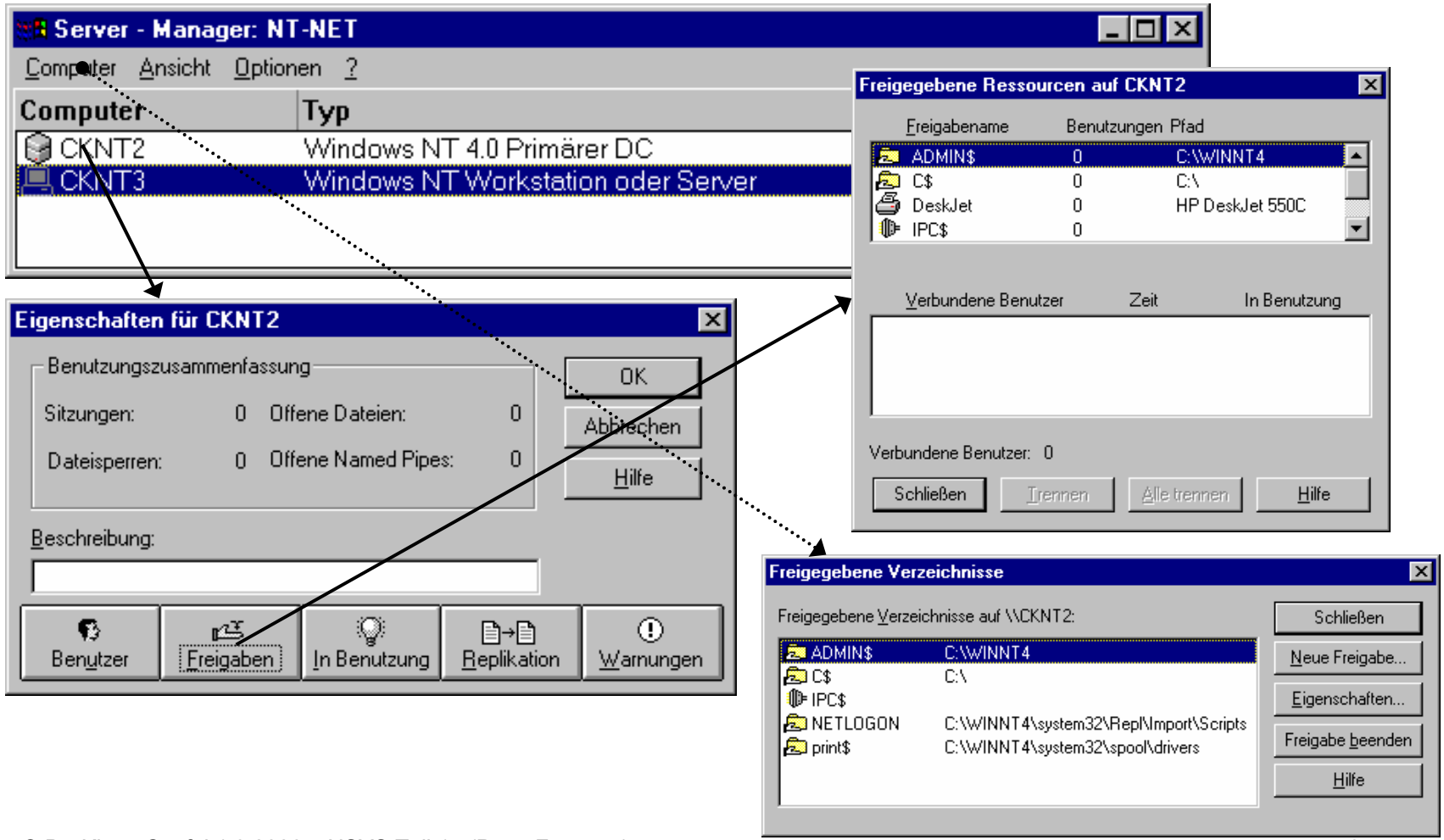
Standardberechtigungen

Name	Verzeichnis	Datei
Kein Zugriff	Kein	Kein
Anzeigen	RX	-
Lesen	RX	RX
Hinzufügen	WX	-
Hinzufügen und Lesen	RWX	RX
Ändern	RWXD	RWXD
Vollzugriff	Alle	Alle

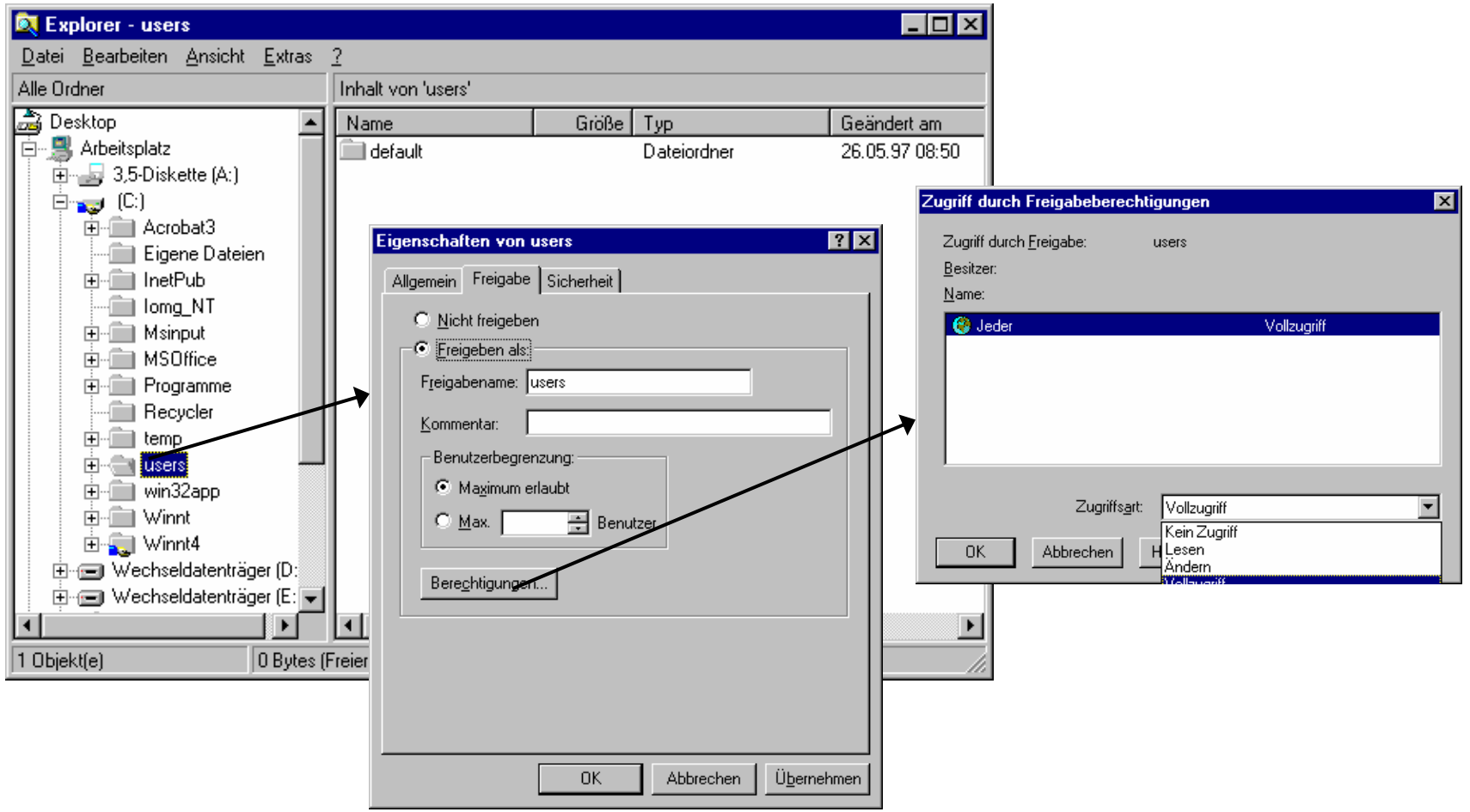
Hilfsprogramme

- Servermanager
- Explorer
- Dateimanager
- MMC (Microsoft Management Console)

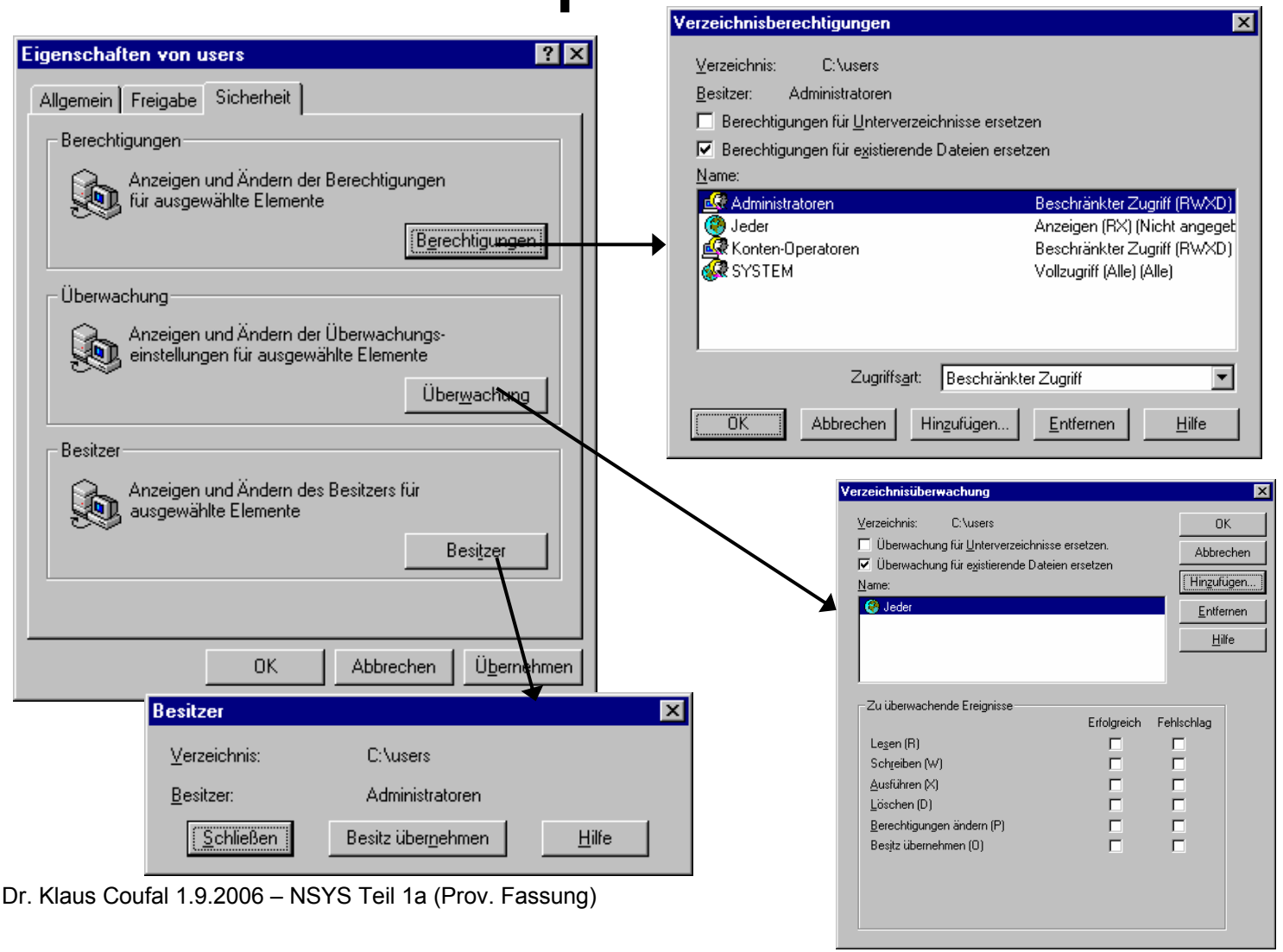
Servermanager



Explorer 1


Explorer - users
Datei Bearbeiten Ansicht Extras ?
Alle Ordner
Inhalt von 'users'
Desktop
Arbeitsplatz
3,5-Diskette (A:)
(C:)
Acrobat3
Eigene Dateien
InetPub
Iomg_NT
Msinput
MSOffice
Programme
Recycler
temp
users
win32app
Winnt
Winnt4
Wechseldatenträger (D:
Wechseldatenträger (E:
Name
Größe
Typ
Geändert am
default
Dateiordner
26.05.97 08:50
1 Objekt(e)
0 Bytes (Freier
Eigenschaften von users
Allgemein
Freigabe
Sicherheit
Nicht freigeben
Freigeben als:
Freigabename: users
Kommentar:
Benutzerbegrenzung:
Maximum erlaubt
Max.
Benutzer
Berechtigungen...
OK
Abbrechen
Übernehmen
Zugriff durch Freigabeberechtigungen
Zugriff durch Freigabe: users
Besitzer:
Name:
Jeder
Vollzugriff
Zugriffsart:
Vollzugriff
Kein Zugriff
Lesen
Ändern
OK
Abbrechen

Explorer 2


Eigenschaften von users
Allgemein
Freigabe
Sicherheit
Berechtigungen
Anzeigen und Ändern der Berechtigungen für ausgewählte Elemente
Berechtigungen
Überwachung
Anzeigen und Ändern der Überwachungs-einstellungen für ausgewählte Elemente
Überwachung
Besitzer
Anzeigen und Ändern des Besitzers für ausgewählte Elemente
Besitzer
OK
Abbrechen
Übernehmen
Verzeichnisberechtigungen
Verzeichnis: C:\users
Besitzer: Administratoren
Berechtigungen für Unterverzeichnisse ersetzen
Berechtigungen für existierende Dateien ersetzen
Name:
Administratoren Beschränkter Zugriff (RWXD)
Jeder Anzeigen (RX) (Nicht angegeb
Konten-Operatoren Beschränkter Zugriff (RWXD)
SYSTEM Vollzugriff (Alle) (Alle)
Zugriffsart: Beschränkter Zugriff
OK
Abbrechen
Hinzufügen...
Entfernen
Hilfe
Verzeichnisüberwachung
Verzeichnis: C:\users
Überwachung für Unterverzeichnisse ersetzen.
Überwachung für existierende Dateien ersetzen
Name:
Jeder
OK
Abbrechen
Hinzufügen...
Entfernen
Hilfe
Zu überwachende Ereignisse
Erfolgreich
Fehlschlag
Lesen (R)
Schreiben (W)
Ausführen (X)
Löschen (D)
Berechtigungen ändern (P)
Besitz übernehmen (O)
Besitzer
Verzeichnis: C:\users
Besitzer: Administratoren
Schließen
Besitz übernehmen
Hilfe

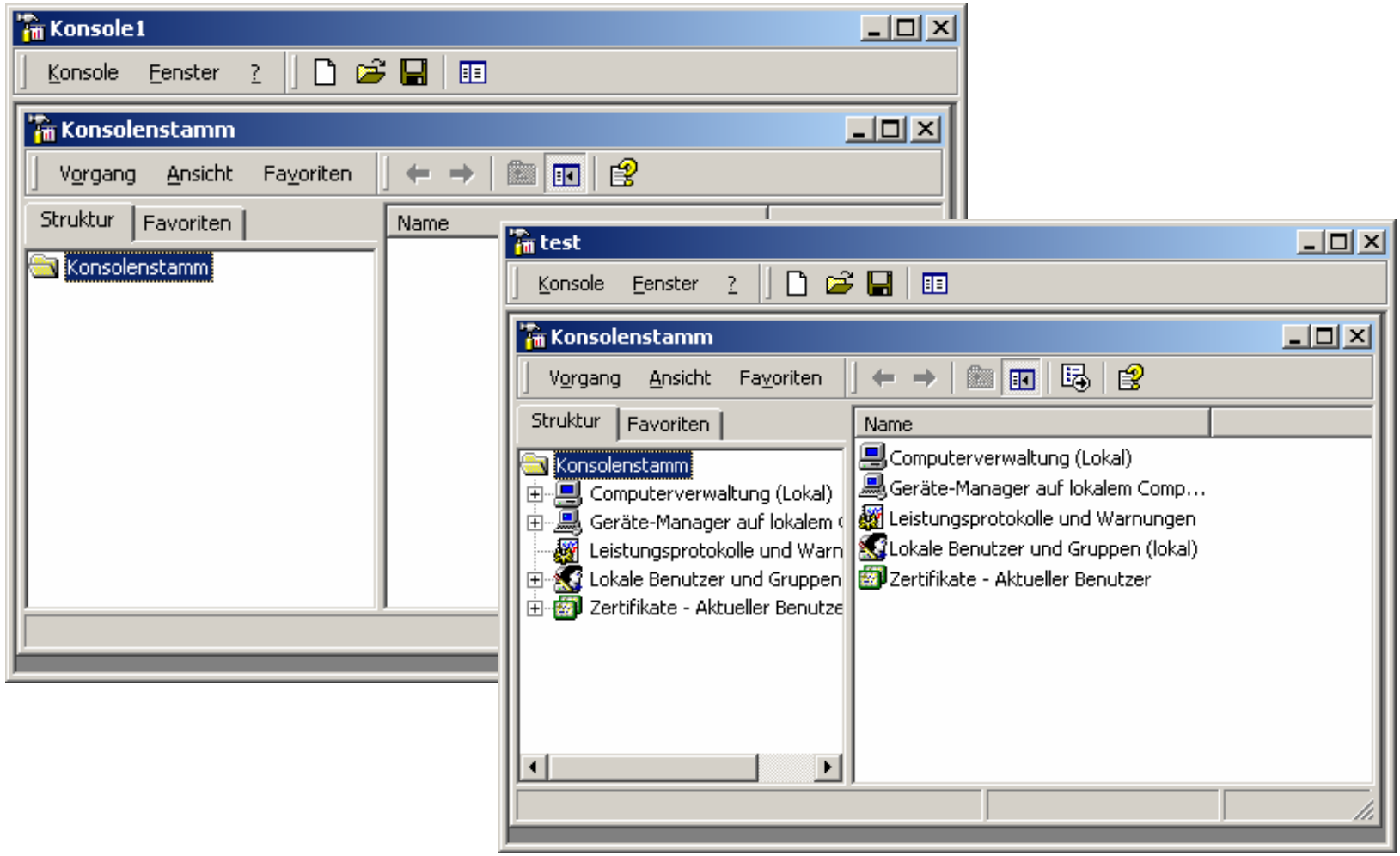
Dateimanager

- Der Dateimanager wird noch benötigt, um die Freigaben für Mac-OS-Clients durchzuführen.
- Sonst funktioniert er wie aus älteren Versionen von Windows bekannt.

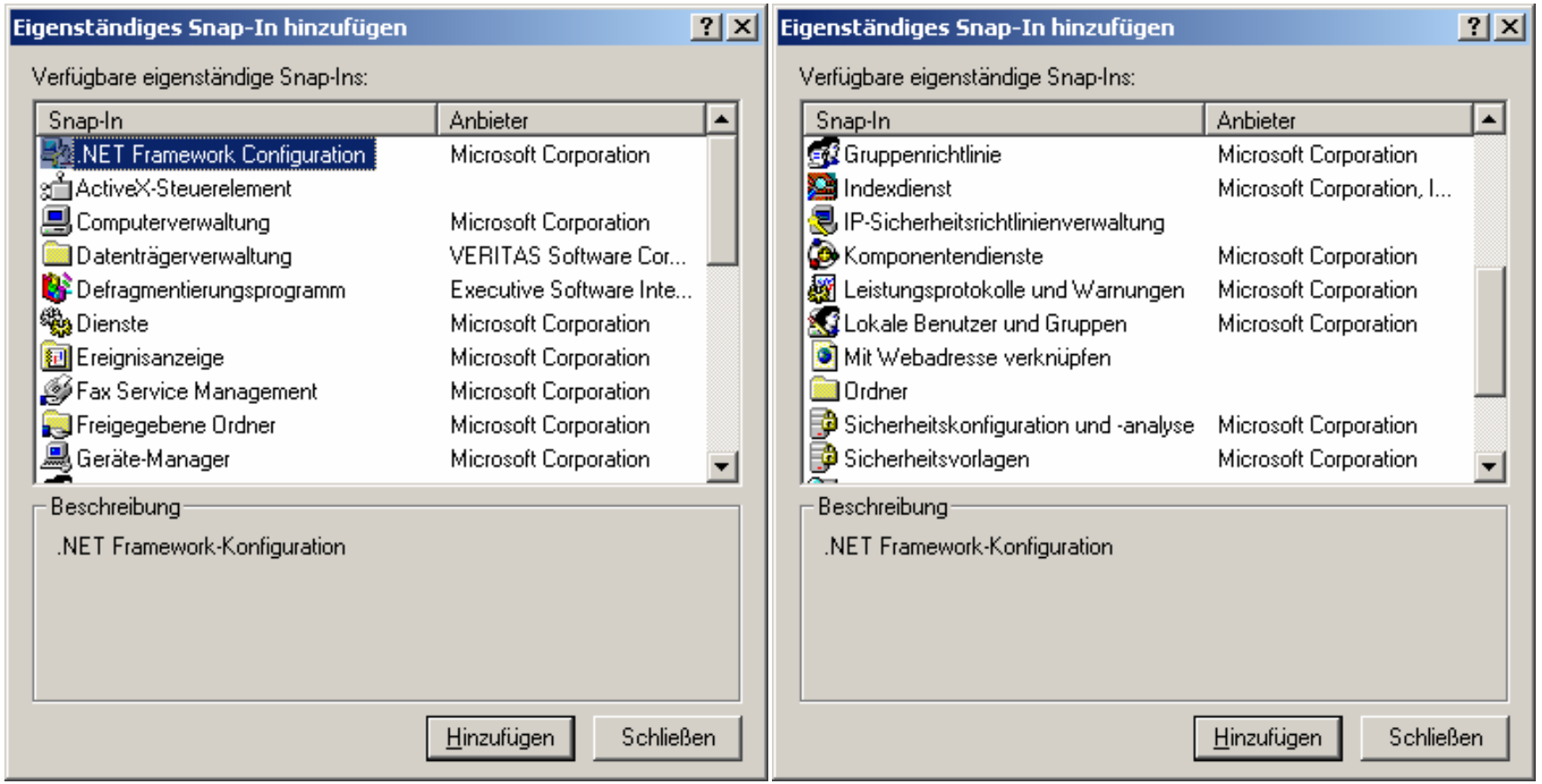
MMC 1

- Microsoft Management Console
- Ab Windows 2000
- Flexibel konfigurierbar
- Erweiterbar (z.B.: Symantec SnapIns)

MMC 2


Konsole1
Konsole Fenster ?
Konsolenstamm
Vorgang Ansicht Favoriten
Struktur Favoriten
Konsolenstamm
Name
test
Konsole Fenster ?
Konsolenstamm
Vorgang Ansicht Favoriten
Struktur Favoriten
Konsolenstamm
Computerverwaltung (Lokal)
Geräte-Manager auf lokalem
Leistungsprotokolle und Warn
Lokale Benutzer und Gruppen
Zertifikate - Aktueller Benutze
Name
Computerverwaltung (Lokal)
Geräte-Manager auf lokalem Comp...
Leistungsprotokolle und Warnungen
Lokale Benutzer und Gruppen (lokal)
Zertifikate - Aktueller Benutzer

MMC 3


Eigenständiges Snap-In hinzufügen
Verfügbare eigenständige Snap-Ins:
Snap-In
Anbieter
.NET Framework Configuration
Microsoft Corporation
ActiveX-Steuerelement
Computerverwaltung
Microsoft Corporation
Datenträgerverwaltung
VERITAS Software Cor...
Defragmentierungsprogramm
Executive Software Inte...
Dienste
Microsoft Corporation
Ereignisanzeige
Microsoft Corporation
Fax Service Management
Microsoft Corporation
Freigegebene Ordner
Microsoft Corporation
Geräte-Manager
Microsoft Corporation
Beschreibung
.NET Framework-Konfiguration
Hinzufügen
Schließen
Eigenständiges Snap-In hinzufügen
Verfügbare eigenständige Snap-Ins:
Snap-In
Anbieter
Gruppenrichtlinie
Microsoft Corporation
Indexdienst
Microsoft Corporation, I...
IP-Sicherheitsrichtlinienverwaltung
Komponentendienste
Microsoft Corporation
Leistungsprotokolle und Warnungen
Microsoft Corporation
Lokale Benutzer und Gruppen
Microsoft Corporation
Mit Webadresse verknüpfen
Ordner
Sicherheitskonfiguration und -analyse
Microsoft Corporation
Sicherheitsvorlagen
Microsoft Corporation
Beschreibung
.NET Framework-Konfiguration
Hinzufügen
Schließen

Sonstige Hilfsprogramme

- Programme des Ordners Verwaltung
- Sonstige Programme
- Zusatzprogramme

Ordner Verwaltung

- Bandsicherung (...\SYSTEM32\NTBACKUP.EXE)
- Benutzermanager (...\SYSTEM32\USRMGR.EXE)
- Ereignisanzeige (...\SYSTEM32\EVENTVWR.EXE)
- Festplattenmanager (...\SYSTEM32\WINDISK.EXE)
- Lizenzmanager (...\SYSTEM32\LLSMGR.EXE)
- Migrationsprogramm für Netware (…\SYSTEM32\NWCONV.EXE)
- Netzwerk-Client-Manager (…\SYSTEM32\NCADMIN.EXE)
- RAS-Verwaltung (...\SYSTEM32\RASADMIN.EXE)
- Server Manager (...\SYSTEM32\SVRMGR.EXE)
- Systemmonitor (...\SYSTEM32\PERFMON.EXE)
- Systemrichtlinieneditor (%SYSTEMROOT%\POLEDIT.EXE)
- Verwaltungs-Assistenten (…\SYSTEM32\WIZMGR.EXE)
- Windows NT-Diagnose (…\SYSTEM32\WINMSD.EXE)

Sonstige Programme

- REGEDT32 (s.o.)
- RDISK
  - Kopieren der Registrierungsdatenbank
  - Notfallsdiskette
- CONVERT
  - FAT $\rightarrow$ NTFS
  - CONVERT z: /FS:NTFS [/V]

Zusatzprogramme

- SQL-Server (Microsoft)
- Exchange (Microsoft)
- Systems Management Server SMS (Microsoft)
- SNA-Server (Microsoft)
- Notes/Domino (Lotus/IBM)
- Oracle Workgroup Server (Oracle)
- ARCserve (Cheyenne)
- Diskkeeper
- …

II.7. Linux

1. Einführung
2. Netzwerke

II.7.1. Einführung

- Übersicht über Linux
- „Hardware“-Grundlagen
- Wichtige Basisbefehle
- Arbeiten mit Dateien und Verzeichnissen
- Hilfe

1. Übersicht über Linux

- Einleitung
- Distributionen
- Einsatzgebiete
- Generelle Unix-Eigenschaften
- Betriebssystemarchitektur
- Kernel
- Dateisysteme
- Shells
- X

1.1. Einleitung

- 1991 von Linus Torvalds entwickelt (80386)
- GNU-GPL (http://www.gnu.org/copyleft/gpl.html)
- Viele HW-Plattformen (x86, PPC, 390, ...)
- Wesentliche Unterschiede zu MS-Windows
  - Die Betriebssystemlizenz ist frei
  - Die Konfiguration erfolgt über Textdateien
  - Der Sourcecode ist verfügbar
  - Die graphische Oberfläche ist netzwerkfähig

1.2. Distributionen

- Red Hat (vor allem in den USA verbreitet)
- S.u.S.E. (in Europa sehr verbreitet)
- Caldera (graph.Installation, Netwaresupport)
- Mandrake
- Debian
- Slackware (die klass.Variante; Linux pur)
- ...

1.3. Einsatzgebiete

- Netzwerkserver
  - Fileserver (Mars, Samba, NFS, ...)
  - Applicationserver
  - Internetserver
- Workstation
  - Durch die X-Oberfläche in immer mehr Bereiche

1.4. Unix-Eigenschaften

- Unix ist ein interaktives Multiuser-/Multitasking Betriebssystem
- Unix ist fileorientiert (z.B.: jedes Gerät ist eine Datei)
- Unix ist netzwerkfähig
- Unix ist ein offenes Betriebssystem und das einzige für das ein Standard geschaffen wurde (POSIX)
- Unix ist flexibel an die Anwenderbedürfnisse anpassbar (verschiedene Shells, ...)
- Unix ist „relativ“ leicht konfigurierbar und kann den Zugriff auf alle Ressourcen sehr fein einstellen (Nicht nur Benutzer/Administrator)

1.5. Betriebssystemarchitektur

<table>
<tr><td colspan="5">Shell/Anwendung</td><td>Usermode</td></tr>
<tr><td colspan="5">System-APIs (System Call Interface)</td><td rowspan="4">Kernel</td></tr>
<tr><td>Virtual File System (VFS)</td><td>character devices</td><td>Abstract Network Services</td><td>Memory Manager</td><td>Process Manager</td></tr>
<tr><td>FS-Drivers</td><td></td><td>TCP/IP Driver</td><td>VM Driver</td><td></td></tr>
<tr><td>HW-Drivers</td><td>HW-Drivers</td><td>NIC Driver</td><td>Memory Driver</td><td>CPU Driver</td></tr>
<tr><td>HD/FD/CD/...</td><td>Konsole/...</td><td>NIC</td><td>Memory</td><td>CPU</td><td>Hardware</td></tr>
</table>

1.6. Kernel

- offizielle Linuxkernel (von Linus Torvalds und dem Kernelteam)
- freier Sourcecode $\Rightarrow$ maßgeschneiderten Kernel
- Jeder kann einen eigenen Kernel verwenden

1.7. Dateisysteme

Unterstützt werden:

- FAT, NTFS, Minix, CDFS, VFAT, HFS(Apple), …;
- eigene Dateisysteme: extfs2, Reiser, ...;
- Netzwerkdateisysteme (NFS, DFS, ...);
- Kryptographische Dateisysteme (TCFS, ...)

1.7. Dateisysteme Beispiel

/ (3. Partition (ext3) auf erster Platte (C:))
/etc (Unterverzeichnis auf Rootpartition)
/boot (2. Partition (ext2) auf erster Platte)
/var (Unterverzeichnis auf Rootpartition)
/proc (Virtuelles Dateisystem zur Verwaltung)
/home (Unterverzeichnis auf Rootpartition)
/floppy (1. Diskettenlaufwerk)
/mnt (4. Partition (NTFS) auf erster Platte)

1.8. Shells

- Bourne-Shell (sh)
- Korn-Shell (ksh)
- C-Shell (csh)
- Bourne Again Shell (bash) - Heute der Quasistandard unter Linux
- ...

1.8. Shells – Beispielbefehle

- ls — Inhaltsverzeichnis (list)
- cat datei — Anzeige von datei
- man befehl — Manual für befehl ausgeben
- cd verz — Wechsle das Verzeichnis auf verz
- pwd — Anzeige des aktuellen Verzeichnisses (print working directory)
- mkdir verz — Anlegen eines Verzeichnisses
- rmdir — Löscht ein Verzeichnis
- mv alt neu — Umbennen bzw. Verschieben von alt nach neu
- rm datei — Lösche datei
- cp quelle ziel — Kopiert quelle nach ziel
- chmod mode file — Ändern der Berechtigungen

1.9. X-Windows

- X-Server (Steuert die Hardware)
- X-Windowmanager (Graphische Präsentation, Aussehen der Fenster)
  - KDE
  - Gnome
- X-Anwendungen (Clientprogramm für die eigentliche Aufgabe)

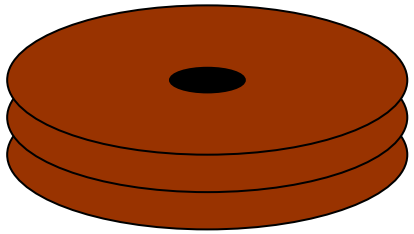
2. „Hardware“grundlagen

1. Festplatten
2. Bootvorgang
3. Graphiksystem
4. Drucksystem

2.1. Festplatten

- Werden durch ihre Anschlußtechnik unterschieden (in LINUX andere Namen: hda, hdb, ..., sda, sdb, ...)
- Der physische Aufbau der Festplatte ist heute nebensächlich
- Werden in Partitionen (Verwaltungseinheit) eingeteilt
- Primäre und Erweiterte Partitionen

Festplatten 2



- Maximal vier Primäre Partitionen
- Eine dieser vier kann eine erweitere Partition sein, die Ihrerseits wieder Partitionen aufnehmen kann.
- Ein Masterpartitionstabelle pro Festplatte und je eine weitere Partitionstabelle pro Partition in der erweiterten Partition

Festplatten 3

- Auf der ersten Festplatte existiert ein MBR (Master Boot Record), der u.a. die Masterpartitionstabelle enthält und darin ist eine Partition als aktiv markiert.
- Ferner enthält der MBR einen Bootloader, damit das System starten kann.

Festplatten 4

- Dadurch ist es möglich mehrere Betriebssysteme auf dem PC zu haben
- Z.B.:
  - 1. Partition: NTFS für Windows 2000
  - 2. Partition: Erweitert
    - 5. Partition swap für Linux
    - 6. Partition ext3 mit / für Linux
    - 7. Partition ext3 mit /home für Linux

2.2. Bootvorgang

- Damit immer nur ein Betriebssystem aktiv und daher das Umschalten zwischen zwei Betriebssystemen umständlich
- Bootmanager erleichert dieses durch eine Auswahlmöglichkeit
  - Lilo, grub
  - Powerquest Bootmagic
  - ...

2.3. Graphiksystem

- Besteht aus einer Graphikkarte und einem Monitor
- Bei modernen Computern und modernen Distribution i.a. automatisch erkannt (wenn nicht ist Expertenwissen notwendig)
- Shared Memory vermeiden (Notebooks)

2.4. Drucksystem

- Eine der Schwachstellen von Linux
- Viele PC-Drucker GDI-Drucker
- Diese erfordern viel CPU-Leistung und unter nicht Windows-Systemen eigene Treiber
- Vor Kauf die Unterstützung durch die verwendeten Betriebssystem prüfen

3. Wichtige Basisbefehle

- Anmelden
- Abmelden
- Informationen über Benutzer
- Passwort ändern
- Datum und Uhrzeit ansehen
- Allgemeine Hinweise

3.1. Anmelden

- Text:
  - Benutzername
  - Passwort (Alternativen sind möglich)
- X-Windows
  - Benutzername oder Auswahl (Mausklick)
  - Passwort (Alternativen sind möglich)

3.2. Abmelden

- `logout`
  - Beendet die Loginshell
  - In Subshell wird darauf hingewiesen, daß nicht in der Loginshell gearbeitet wird
- `exit`
  - Beendet die momentane Shell
  - Bei der Loginshell erfolgt dadurch ein Logout

3.3. Infos über Benutzer

- `w`
  - Zeigt an wer angemeldet ist und was diese Benutzer machen
  - z.B.:

```
rechner:~ # w
```

```
 10:29am  up  3:47,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
root     pts/0    192.168.13.2     10:29am  1.00s  0.22s  0.05s  w
```

Infos über Benutzer 2

- `who`
  - Zeigt wer angemeldet ist
  - z.B.:

```
rechner:~ # who
root     pts/0    Nov 13 10:29 (192.168.13.2)
```

Infos über Benutzer 3

- `whoami`
  - Gibt des effektiven UserID aus
  - z.B.:

```
rechner:~ # whoami
root
```

Infos über Benutzer 4

- `id`
  - Gibt den wirklichen und den effektiven UserId und GroupID aus
  - z.B.:

```
rechner:~ # id
uid=0(root) gid=0(root)
groups=0(root),1(bin),14(uucp),15(shadow),16(dial
  out),17(audio),65534(nogroup)
```

3.4. Passwort ändern

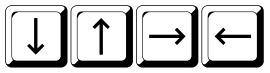
- `passwd`
  - Ändert das Passwort des momentan aktiven Benutzers
  - Erfordert die Eingabe des derzeitigen und die zweimalige Eingabe des neuen Passwortes
  - Selbstverständlich ohne Anzeige

3.5. Datum und Uhrzeit

- date
  - Gibt Datum und Uhrzeit aus
  - z.B.:

```
rechner:~ # date
Wed Nov 13 10:31:39 MET 2002
```

3.6. Allgemeine Hinweise 1

-  Tabulator
  - Ergänzen von Dateinamen
-  Space
  - Um eine Seite weiter in vielen Befehlen
-  oder  Return
  - Eingabe oder um eine Zeile weiter
-  Pfeiltasten
  - Kommandoeditor

Allgemeine Hinweise 2

- Optionen bei den Befehlen in zwei Formaten
  - `-o` Einbuchstabige Optionen
  - `--option` Klartextoptionen
- Trend zu Klartextoptionen

```
rm -d verzeichnis
rm --directory verzeichnis
```

Allgemeine Hinweise 3

Sonderzeichen innerhalb von Befehlen

- | Verkettung von Befehlen
  befehl1 | befehl2
- > Umleitung der Ausgabe (neue Datei)
  befehl > datei
- >> Umleitung der Ausgabe als Anhang
  befehl >>datei

Allgemeine Hinweise 4

- < Umleitung der Eingabe

  befehl < datei

- n>, n>>, n< Umleitung des ensprechenden Kanals (n=Nummer)

  befehl 2> datei

- \z Sonderzeichen (\> $\Rightarrow$> ...)

4. Arbeiten mit Dateien und Verzeichnissen

- pwd, cd, ls
- locate, find
- which, file
- cp, mv
- ln
- mkdir, touch, rm, rmdir
- cat, less, more
- sed, awk,
- lpr
- tar, gzip, bzip2, zip

pwd

- **p**rint **w**orking **d**irectory
- Anzeige des momentanen Arbeitsverzeichnisses (durch cd eingestellt)
- Syntax: `pwd`

```
klaus@rechner:~ > pwd
/home/klaus
```

cd

- **c**hange **d**irectory
- Wechsel des Arbeitsverzeichnisses
- Syntax: `cd [Zielverzeichnis]`

```
klaus@rechner:~ > cd /etc
klaus@rechner:/etc > cd
klaus@rechner:~ >
```

ls

- **lis**t files
- Liste Dateien (dir)
- Syntax: `ls [optionen] [Muster]`
- Wichtige Optionen
  - `-l` Longformat
  - `-a` Alle Dateien (auch versteckte)

ls – Beispiele

```
klaus@rechner:~ > ls
down  ipchains.txt

klaus@rechner:~ > ls -l
insgesamt 20
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
-rw-r--r--   1 root     root        13649 Feb  7  2001 ipchains.txt

klaus@rechner:~ > ls -al .u*
-rw-r--r--   1 klaus    users       10972 May  5  2000 .uitrc.console
-rw-r--r--   1 klaus    users        9394 May  5  2000 .uitrc.vt100
-rw-r--r--   1 klaus    users        9394 May  5  2000 .uitrc.vt102
-rw-r--r--   1 klaus    users       10687 May  5  2000 .uitrc.xterm
-rw-r--r--   1 klaus    users         324 May  5  2000 .urlview
```

locate

- Sucht in einer Datenbank nach Dateien, die einem Muster entsprechen (Datenbankupdate mittels `updatedb`)
- Syntax: `locate [--help] pattern`

```
klaus@rechner:~ > locate resolv.conf
/etc/resolv.conf
/usr/share/man/man5/resolv.conf.5.gz
/var/adm/SuSEconfig/md5/etc/resolv.conf
```

find

- Sucht nach Dateien in der Verzeichnishierarchie
- Syntax: `find [path...] [expression]`

```
klaus@rechner:/home > find . -name down
./klaus/down
find: ./shutdown: Keine Berechtigung
```

which

- Zeigt den Ort eines Befehls an
- Syntax: `which progname`

```
klaus@rechner:/home > which ls
klaus@rechner:/home > which find
/usr/bin/find
```

file

- Versucht den Typ einer Datei zu eruieren
- Syntax: `file datei`

```
klaus@rechner:~ > file /usr/bin/file
/usr/bin/file: ELF 32-bit LSB executable, Intel
  80386, version 1, dynamically linked (uses
  shared libs), stripped
klaus@rechner:~ > file down
down: ASCII text
klaus@ rechner:~ > file .nc_keys
.nc_keys: English text
```

cp

- **c**o**p**y files or directories
- kopiert eine oder mehrere Dateien
- Syntax: `cp [optionen] Quelle Ziel`

```
klaus@rechner:~ > cp down new
klaus@rechner:~ > cp /etc/resolv.conf .
```

mv

- **mo**ve files or directories
- verschiebt eine Datei oder benennt sie um
- Syntax: `mv [optionen] Quelle Ziel`

```
klaus@rechner:~ > mv new neue_datei    (rename)
klaus@rechner:~ > mv ipchains.txt sub  (move)
```

ln

- **ln**k file or directory
- erzeugt einen Verzeichniseintrag einer existierenden Datei unter anderem Namen
- Syntax: `ln [optionen] Quelle [Ziel]`
- Hardlinks und Symbolische Links

ln – Beispiele

```
klaus@rechner:~/sub > dir
insgesamt 16
-rw-r--r--   1 root     root        13649 Feb  7  2001 ip.txt
klaus@rechner:~/sub > ln ip.txt test1
klaus@rechner:~/sub > ln -s ip.txt test2
klaus@rechner:~/sub > dir
insgesamt 32
-rw-r--r--   2 root     root        13649 Feb  7  2001 ip.txt
-rw-r--r--   2 root     root        13649 Feb  7  2001 test1
lrwxrwxrwx   1 klaus    users          12 Nov 13 12:23 test2 -> ip.txt
```

mkdir

- **mak**e **dir**ectory
- erzeugt ein leeres Verzeichnis
- Syntax: `mkdir Verzeichnis`

```
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
-rw-r--r--   1 klaus    users         313 Nov 13 12:10 resolv.conf
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 sub
klaus@rechner:~ > mkdir neu
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 neu
-rw-r--r--   1 klaus    users         313 Nov 13 12:10 resolv.conf
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 sub
```

touch

- ändert die Zeitmarkierung einer Datei bzw. legt eine Datei an
- Syntax: `touch [optionen] Datei`

```
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
-rw-r--r--   1 root     root        13649 Feb  7  2001 ipchains.txt
klaus@rechner:~ > touch testdatei
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
-rw-r--r--   1 root     root        13649 Feb  7  2001 ipchains.txt
-rw-r--r--   1 klaus    users           0 Nov 13 13:28 testdatei
```

rm

- **rem**ove files
- Entfernt Dateien
- Syntax: `rm [optionen] Pfad`
- Wichtige Optionen
  - `-d` Um Verzeichnisse zu löschen
  - `-r` Rekursiv (d.h. Unterverzeichnisse und Dateien darin)

```
klaus@rechner:~ > rm testdatei
```

rmdir

- **rem**ove **dir**ectory
- löscht leere(!) Verzeichnisse
- Syntax: `rmdir [-p] Verzeichnis`

```
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 neu
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 sub
klaus@rechner:~ > rmdir neu
klaus@rechner:~ > dir
-rwxrwxrwx   1 klaus    users          12 Feb 19  2001 down
drwxr-xr-x   2 klaus    users        4096 Nov 13 13:22 sub
```

cat

- con**cat**enate files
- Gibt Dateien aus oder verkettet Dateien
- Syntax: `cat [optionen] [Datei...]`

```
klaus@rechner:~ > cat down
su -c halt
```

less

- Zeigt Dateien seitenweise an
- Möglichkeit des Blätterns und Suchens
- Syntax: `less [optionen] datei`
- Blättern z.B. mit den Pfeiltasten
- Suchen mit „/suchtext“
- Ende mit Q

```
klaus@rechner:~ > less ipchains.txt
```

more

- Zeigt Dateien seitenweise an
- Environmentvariable MORE enthält die Anzahl der Zeilen
- Syntax: `more [optionen] datei`
- Ende mit Q

```
klaus@rechner:~ > more ipchains.txt
```

sed

- **s**tream**ed**it files
- Editieren von Dateien in nicht interaktiver Form
- Syntax: `sed [optionen] [Datei...]`

```
klaus@rechner:~ > cat sedtest
Das ist eine Testdatei fuer SED
klaus@rechner:~ > sed -e s/e/o/g sedtest
Das ist oino Tostdatoi fuor SED
klaus@rechner:~ > sed -e s/e/o/ sedtest
Das ist oine Testdatei fuer SED
```

awk

- Musterscanning und Verarbeitung
- von **A**ho, **K**ernighan, and **W**einberger entwickelt
- Syntax:

```
awk [opt] -f program-file file
```

- Vollständige Programmiersprache

lpr

- off **l**ine **pr**int
- Drucken über einen Spooler
- Syntax: lpr [optionen] [datei]

tar

- **t**ape **ar**chiver
- verwaltet Dateiarchive
- Syntax: `tar [optionen] Dateien`

```
klaus@rechner:~ > tar -c -f testtar *
klaus@rechner:~/test > tar -x -f testtar
```

gzip

- Dateikomprimierung nach LZ77
- Ersetzt Datei durch komprimierte Version
- Syntax: `gzip [optionen] datei`

```
klaus@rechner:~ > gzip testtar
klaus@rechner:~ > gzip -d testtar
```

bzip2, zip

- Andere Filekompressionsprogramme
- Syntax:

```
bzip2 [optionen] Dateien
bunzip2 [optionen] Dateien
zip [optionen] zipfile dateien
```

- Kann mehrere Dateien in einem Durchgang komprimieren und ersetzt die Datei nicht

5. Hilfe

- man
- info
- --help
- -h
- whatis
- apropos
- HOWTOs

man

- **man**ual pages
- Ansehen der Manuals
- Syntax: `man [optionen] befehl`
  `man [seite] befehl`
- Ende mit Q

```
klaus@rechner:~ > man bzip2
klaus@rechner:~ > man ls
```

info

- Lese die info-Dokumente
- Syntax: `info [optionen] thema`
- Ende mit 


```
klaus@rechner:~ > info man
klaus@rechner:~ > info login
```

--help, -h

- Bei vielen Befehlen erhält man Hilfe mit der Optionen `--help` oder `-h`
- Syntax: `befehl -h`

```
klaus@rechner:~ > tar --help
klaus@rechner:~ > man -h
```

whatis

- durchsucht die Indexdatenbank nach Kurzbeschreibungen
- Syntax: `whatis [optionen] suchwort`

```
klaus@rechner:~ > whatis bash
bash (1) - GNU Bourne-Again SHell
```

apropos

- sucht die Manualkurzbeschreibung in der Indexdatenbank
- Syntax: `apropos [optionen] suchwort`

```
klaus@firewall:~ > apropos bash
bash (1)          - GNU Bourne-Again SHell
bashbuiltins (1)  - bash built-in commands, see bash(1)
rbash (1)         - restricted bash, see bash(1)
bashbug (1)       - report a bug in bash
```

HOWTOs

- Textdateien (heute oft auch HTML-Dateien) mit der Beschreibung eines bestimmten Vorganges
- Autor mit e-Mail-Adresse angegeben
- Oft auch verschiedene Sprachversionen
- English am umfangreichsten

II.7.2. Netzwerke

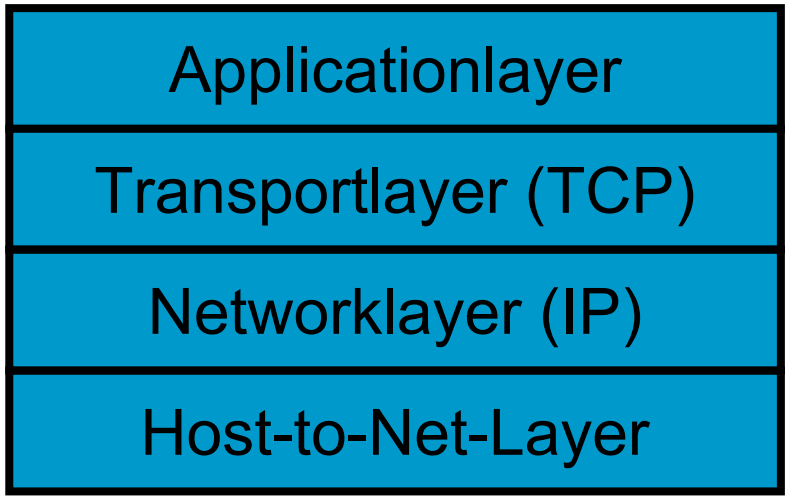
- Linux im Netzwerk
- Anschluß an das Internet
- Wichtige Dienste
- Sicherheit
- Wichtige Kommandos

1. Linux im Netzwerk

- TCP/IP
- IPv4
- IPv6
- Einbindung in das LAN
- Manuelle Konfiguration
- DNS
- DHCP

1.1. TCP/IP

- Im Internet wird ein 4-Schichtenmodell verwendet:



Dabei nimmt TCP die Aufgaben der Transportschicht (Ende-zu-Ende-Kommunikation) und IP die Aufgaben der Netzwerkschicht war

1.2 IPv4

- 32-Bit Adressen mit hierarchischer Struktur und vielen ungenutzen Adressen
- Keine Sicherheit
- Nicht echtzeitfähig (kein QoS)
- Dezimal Schreibweise (z.B.:192.189.51.100)
- Versteckte Adressen
  - 10.x.x.x
  - 172.16.x.x-172.31.x.x
  - 192.168.x.x

IPv4

- Adresse besteht aus Netzanteil und Hostanteil
- Gekennzeichnet durch Netzmaske
- 2 spezielle Adressen
  - Netzadresse (Hostanteil 0)
  - Broadcastadresse (Hostanteil -1)
- Subnetmöglichkeit

1.3. IPv6

- 128-Bit-Adressen
- IPSec integriert
- Echtzeitfähig (durch QoS)
- Kompatibel zu IPv4
- Hexadezimale Schreibweise (z.B.: 3ffe:400:10:abcd:300:c0ff:fed0:5678
- Besser strukturiert

1.4. Einbindung in das LAN

- (Einbau einer Netzwerkkarte)
- Standardkonfiguration mittels Konfigurationswerkzeug der Distribution (YaST2 (SuSE), linuxconf (RedHat))
- Notwendige Parameter:
  - Typ der Netzwerkkarte
  - IP-Address, Netmask, Defaultgateway, IP-Address des/der DNS-Server (oder DHCP)

1.5. Manuelle Konfiguration

- /etc/hosts (address name nickn.)
- /etc/networks (name netaddress)
- /etc/host.conf (Reihenfolge)
- /etc/resolv.conf (DNS-Infos)
- /etc/route.conf (Routinginformationen)
- Systemabhängige weitere (z.B.: /etc/rc.config) Konfigurationsdateien
- Systemspezifische Startskripte

1.6. DNS

- Domain Name Service (Port 53)
- Umwandlung von Rechnernamen in IP-Adresse (z.B.: miraculix.htl-tex.ac.at = 192.189.51.100)
- Hierarchisch aufgebaut (root, tld, sld, ...)
- Rechneranfragen werden beantwortet (eventuell weiterfragen notwendig)

1.7. DHCP

- Dynamic Host Configuration Protocol
- Versuch von zentraler Stelle aus die Netzwerkinformationen (Adresse, Netzmaske, DNS-Server, Gateway) zu verwalten und zu verteilen
- Basis MAC-Adresse
- Relativ großes Sicherheitsrisiko

2. Anschluß an das Internet

- PPP (Point-to-Point-Protocol)
- Internetzugang über ISDN
- Internetzugang über ADSL
- Internetzugang über Kabelmodem

2.1. PPP

- Eigenes Packet
- RFC1144, RFC1321, RFC1332, RFC1334, RFC1548, RFC 1549
- Hat SLIP (Serial Line IP) abgelöst
- Konfiguration über das Konfigurationswerkzeug der Distribution
- (WAN-Interface ist unter ppp0, ppp1, ... verfügbar)

2.2. ISDN-Zugang

- Packet: isdn4linux
- Aktive Karten/Passive Karten
- Konfiguration über das Konfigurationswerkzeug der Distribution
- „Euro-ISDN“
- Notwendig: eigene MSN-Nummer, Provider-ISDN-Nummer, Benutzername, Passwort, DNS-Server

2.3. ADSL-Zugang

- Verwendetes Protokoll: PPPoE (Point-to-Point over Ethernet)
- Parameter in : /etc/pppoed.conf (und eventuell in rc.dialout)
- Dial-on-Demand

2.4. Kabelzugang

- Am einfachsten von allen Internetzugängen in Österreich
- Netzwerkschnittstelle mit dem Anbieter bekannter MAC-Adresse auf DHCP konfigurieren und an das Kabelmodem anschließen
- Fertig

3. Wichtige Dienste

- Samba (Server für Windowsclients)
- Netatalk (Server für MacOS-Clients)
- MARSNWE (Server für NW-Clients)
- FTP (FTP-Server)
- Apache (Webserver)
- Squid (Proxyserver)
- Sendmail (SMTP-Server)
- DNS bzw. DHCP-Server

3.1. Samba

- File-, Print- und Domainserver für DOS-, Windows- und OS/2-Rechner
- Konfig.datei /etc/samba/smb.conf
- SMB-Protocol und NetBIOS-Dienst (NetBEUI)
- Keine Änderung an den Clients notwendig

3.2. Netatalk

- File- und Printserver für MacOS-Rechner
- Konfig.datei /etc/atalk/atalkd.conf
- Implementierung der Apple-Talk-Protokollfamilie
- Keine Änderung an den Clients notwendig

3.3. MARSNWE

- File- und Printserver für Novellclients (DOS, Windows, OS/2, MacOS, ...)
- NDS-Unterstützung noch nicht gut
- Konfig.datei /etc/nwserv.conf
- Implementierung des IPX/SPX und des NCP-Protokolles

3.4. FTP

- Viele Clientvarianten (Commandline, Interaktiv, Graphisch, Webbrowser)
- Aktiv/Passive
- Port 21 (und Port 20)
- Mehrere Serverversionen (wu.ftpd, ...)
- Unsicherer Dienst
- TFTP ohne Authentifizierung

3.5. Apache

- Webserver mit größtem Marktanteil
- Konfig.datei /etc/httpd/httpd.conf
- Verzeichnis unter „ServerRoot“ (z.B.: /usr/local/httpd)
- Dokumente im Unterverzeichnis htdocs
- 1.Datei index.html
- (z.B.: /usr/local/httpd/htdocs/index.html)

3.6. Squid

- Proxyserver für http (Ports 3128, 8080)
- Vorteile eines Proxy-Servers
  - Erhöhung der Performance
  - Erhöhung der Sicherheit
- Nachteile eines Proxy-Servers
  - Performanceverbesserung bei dynamischen Webseiten gering
  - Webverkehr wird bestens überwachbar
- Konfig.datei /etc/squid.conf

3.7. Sendmail

- SMTP-Server (**S**imple **M**ail **T**ransfer **P**rotocol)
- Konfig.datei /etc/sendmail.cf
- In der Tiefe der Möglichkeiten unübersichtlich
- Konfiguration über das Konfigurationswerkzeug der Distribution

3.8. DNS

- Nameserver BIND (derzeit Version 9)
- Konfig.datei /etc/named.conf
- Zusätzlich Zonendateien über verwaltete Domains
- Angabe der Forwarders nötig
- Mindestens 2 Nameserver pro Domäne (einer außerhalb des Netzes)

3.9. DHCP

- Server für DHCP
- Konfig.datei /etc/dhcpd.conf
- Standard: Dynamische Zuordnung aus einem Adresspool
- Fixe Zuordnungen auf Basis der MAC-Adresse möglich
- Zusatzangaben: DNS-Server, Gateway

4. Sicherheit

- Masquerading (NAT)
- Firewall
- OpenSSH
- Sicherheit generell

4.1. Masquerading

- Übersetzung von IP-Adressen
- Hauptsächlich bei „versteckten“ Adressen im Einsatz
- z.B.: 192.168.13.2:1199 ⇨
  192.189.51.21:65001
- Dynamisches NAT
- Statisches (Hide)-NAT

4.2. Firewall

- Sicherheitsmauer zwischen externem und internem Netz
- Realisierung mit ipchains (älter) bzw. iptables
- Packetfiltering (Ansätze zu Statefull Inspection vorhanden, Application Layer Gateway extra realisierbar)
- Konfiguration für Anfänger verwirrend (Vereinfachungen z.B.: SuSEfirewall2, fwbuilder, ...)

4.3. OpenSSH

- Dieses Packet stellt einen SSH-Server und die Kommandos ssh, scp und sftp zur Verfügung
- Mit asymmetrischen Verfahren verschlüsselte Übertragung
- Ersatz des Passwortes durch Zertifikate möglich

4.4. Sicherheit generell

- Sicherheit ist ein ständiger Prozeß!
  - Passwörter regelmäßig ändern
  - Logfiles lesen
  - Ständig am neuesten Stand bei sicherheitskritischer Software
- „Feinde“ der Sicherheit:
  - Falsches Vertrauen
  - Bequemlichkeit

5. Wichtige Kommandos

- ifconfig
- route
- netstat
- ping, traceroute
- host, hostname, nslookup, dig
- ssh, scp
- ftp

ifconfig

- Konfiguriert ein Netzwerkinterface
- Syntax:

  `ifconfig interface [aftype] [options]`

```
root@rechner:/etc > ifconfig eth0
eth0 Link encap:Ethernet  HWaddr 00:00:21:64:3F:B9
     inet addr:192.168.13.1  Bcast:192.168.13.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:11516 errors:0 dropped:0 overruns:0 frame:0
     TX packets:8961 errors:0 dropped:0 overruns:0 carrier:0
     collisions:142 txqueuelen:100
     Interrupt:12 Base address:0xe400
```

route

- Zeigt und ändert die Routingtabelle
- Syntax: `route [options]`

```
root@rechner:/etc > route -N
Kernel IP routing table
Destination    Gateway        Genmask        Flags Metric Ref Use Iface
192.189.51.0   0.0.0.0        255.255.255.0  U     0      0     0 eth0
192.168.13.0   0.0.0.0        255.255.255.0  U     0      0     0 eth1
127.0.0.0      0.0.0.0        255.0.0.0      U     0      0     0 lo
0.0.0.0        192.189.51.1   0.0.0.0        UG    0      0     0 eth0
```

netstat

- Zeigt Information über das Netzwerk an
- Syntax: `netstat [options]`

```
root@rechner:/etc > netstat -tunl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address      Foreign Address         State
tcp        0      0 0.0.0.0:22         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21         0.0.0.0:*               LISTEN
```

ping

- Ping sendet ein Kontrollpacket an eine IP-Adresse und zeigt die Antwort an
- Syntax: `ping [options] host`

```
funk-nat:~ # ping miraculix.htl-tex.ac.at
PING miraculix.htl-tex.ac.at (192.189.51.100) from
   192.189.51.63 : 56(84) bytes of data.
64 bytes from miraculix.htl-tex.ac.at (192.189.51.100):
   icmp_seq=1 ttl=128 time=0.440 ms
funk-nat:~ # ping 192.189.51.1
PING 192.189.51.1 (192.189.51.1) from 192.189.51.63 : 56(84)
   bytes of data.
--- 192.189.51.1 ping statistics ---
3 packets transmitted, 0 received, 100% loss, time 2017ms
```

traceroute

- Traceroute sucht den Weg zu einem Rechner (mit Hilfe von Pings)
- Syntax: `traceroute [options] host`

```
funk-nat:~ # traceroute www.coufal.info
traceroute to www.coufal.info (62.99.149.13), 30 hops max, 40 byte pkts
 1 sagnix.htl-tex.ac.at (192.189.51.1) 0.136 ms  0.000 ms  0.100 ms
 2 sagnix93.htl-tex.ac.at (193.170.108.1) 7.499 ms  8.377 ms  9.254 ms
 3 Vienna-RBS2.ACO.net (192.153.182.101) 11.175 ms 11.031 ms 11.273 ms
 4 Wien1.ACO.net (193.171.23.1)  10.752 ms  10.990 ms  10.974 ms
 5 interxion.inode.at (193.203.0.57)  10.957 ms   10.949 ms   10.993 ms
 6 l3-suite-C2948G.inode.at (62.99.171.126) 11.037ms 11.064ms 11.109 ms
 7 host5.ssl-gesichert.at (62.99.149.13)  9.644 ms  9.644 ms  9.619 ms
```

host

- Sucht mit Hilfe eines DNS-Server nach einem Namen
- Syntax: `host [options] host`

```
rechner:~ # host www.htl-tex.ac.at
www.htl-tex.ac.at is a nickname for asterix.htl-tex.ac.at
asterix.htl-tex.ac.at has address 192.189.51.199
rechner:~ # host 192.189.51.199
199.51.189.192.IN-ADDR.ARPA domain name pointer asterix.htl-tex.ac.at
```

hostname

- Zeigt oder setzt den Netzwerknamen des Systems
- Syntax: `hostname [name]`

```
funk-nat:~ # hostname
funk-nat
```

nslookup

- Interaktives Hilfsprogramm zum Abfragen eines DNS-Servers
- Syntax: `nslookup [optionen]`

```
firewall:~ # nslookup
Default Server:  ns1.chello.at
Address:  195.34.133.10
> www.coufal.info
Server:  ns1.chello.at
Address:  195.34.133.10

Non-authoritative answer:
Name:    www.coufal.info
Address:  62.99.149.13
> exit
```

dig

- Hilfsprogramm zum Abfragen eines DNS-Server
- Syntax: `dig domain [options]`

```
firewall:~ # dig www.coufal.org
...

;; ANSWER SECTION:
www.coufal.org.         23h11m56s IN A  62.99.149.10

;; AUTHORITY SECTION:
coufal.org.             23h11m56s IN NS  ns1.domaintechnik.at.
coufal.org.             23h11m56s IN NS  ns2.domaintechnik.at.

...
```

ssh

- **S**ecure **SH**ell Client (Remote login)
- Syntax: `ssh [-l login_name] [hostname]`

```
funk-nat:~ # ssh cisco.htl-tex.ac.at
root@cisco.htl-tex.ac.at's password:
Last login: Wed Nov 20 17:36:09 2002 from
  ueb05.exp.univie.ac.at
Have a lot of fun...
einsilbix:~ # exit
logout
Connection to cisco.htl-tex.ac.at closed.
```

scp

- **S**ecure **C**o**P**y (Kopieren von Dateien auf andere Rechner mit Hilfe von SSH)
- Syntax: `scp [options] [[user1]@host1:]file1 [[user2]@host2:]file2`

```
funk-nat:~ # scp root@cisco.htl-tex.ac.at:/tftpboot/Lab_C .
root@cisco.htl-tex.ac.at's password:
Lab_C   100% |*****************************|  1026     00:00
```

ftp

- Interaktiver Client für FTP-Server
- Syntax: `ftp [options] host [hostoptions]`

```
funk-nat:~ # ftp miraculix.htl-tex.ac.at
Connected to miraculix.htl-tex.ac.at.
220-miraculix.htl-tex.ac.at
220-Welcome at HTBLVA fuer Textilindustrie und Datenverarbeitung
220-
220-Please enter user name with container relativly to EDV.HTBLVA
220-(e.g. PUPIL.HDV, user.ABEND, ...)
220-
220-Your will be connected to your home directory at TALENTIX (R:)!
220-To change to your MIRACULIX-directory use UNC.
220 Service Ready for new User
Name (miraculix.htl-tex.ac.at:root):
```

ftp 2

Wichtige Befehle:

get file	Hole Datei auf lokalen Rechner
put file	Send Datei von lokalem Rechner
image	Binärmodus zum Übertragen
ascii	ASCII-Modus zum Übertragen
passive	Passiver Modus (pasv)
quit	Aussteigen (auch exit, bye)
help	Hilfe

II.8. Vergleich

- Installation Server
- Einrichten Benutzer
- Installation Server-Software/Hardware
- Installation Anwender-Software
- Sicherheit (Server, Zutritt, Zugriff, Daten)
- Kosten
- Vor-/Nachteile
- Zusammenfassung

Installation Server

- Netware
  - ca. 2 Stunde
  - Abfrage(+) der HW-Parameter (Non-PNP)
  - Übernahme der HW-Parameter (PNP)
  - Alle Zusatzkomponenten über das gleiche Installationsprogramm
  - Konfiguration von einer Workstation

Installation Server

- Windows NT/2000
  - ca. 2 Stunden
  - Defaults(-) der HW-Parameter (Non-PNP)
  - Übernahme der HW-Parameter (PNP)
  - Jede Zusatzkomponente hat eigenes Installationsprogramm
  - Konfiguration am Server
  - Verweis auf Handbücher, die erst nach der Installation eingesehen werden können

Installation Server

- Linux
  - ca. 2 Stunden
  - Abfrage(+) der HW-Parameter (Non-PNP)
  - Übernahme der HW-Parameter (PNP)
  - Alle Zusatzkomponenten über das gleiche Installationsprogramm
  - Konfiguration am Server

Installation Client

- Zeitdauer und Aufwand sind vom verwendeten Betriebssystem am Client abhängig und weniger vom Serverbetriebssystem
- Bei Windows NT/2000 werden Windows xx-Clients besser unterstützt als andere Clients-OS (MacOS, ...)

Einrichten Benutzer

- Netware
  - Menügesteuert oder
  - Automatisch Listengesteuert aus ASCII-Datei (aus beliebigen Datenbanken) mit UIMPORT
  - Übernahme von anderen Serversystemen
  - Flexibel an Benutzer anpaßbar (Platz, Rechte, Sprache, Standardwerte,...)

Einrichten Benutzer

- Windows-NT/2000
  - Menügesteuert auf mehrere Programme verteilt
  - (Übernahme von anderen Serversystemen)
  - “Normuser”

Einrichten Benutzer

- Linux
  - Menügesteuert oder
  - Automatisch Listengesteuert aus ASCII-Datei (aus beliebigen Datenbanken)
  - Flexibel an Benutzer anpaßbar (Platz, Rechte, Sprache, Standardwerte,...)

Installation Server-Software

- Netware
  - Mittels zentralem Installer am Server
  - Von einer Arbeitsstation
  - Konfiguration am Server oder auf einer Arbeitsstation
  - Speicherschutz muß extra aktiviert werden

Installation Server-Software

- Windows-NT/2000
  - Installationsprogramm der Software
  - Von einer Arbeitsstation
  - Konfiguration am Server oder auf einer Arbeitsstation
  - Speicherschutz im OS integriert

Installation Server-Software

- Linux
  - Mittels zentralem Installer am Server
  - Von einer Arbeitsstation
  - Konfiguration am Server oder auf einer Arbeitsstation
  - Speicherschutz im OS integriert

Installation Server-Hardware

- Netware
  - Zusätzliche Platte auch während des Betriebs möglich
  - Volumes können während der Laufzeit dynamisch vergrößert werden
  - Schnittstellen können während des Betriebs rekonfiguriert werden

Installation Server-Hardware

- Windows-NT/2000
  - Zusätzliche Platte nur bei einem Neustart des Systems möglich
  - Volumes über mehrere Platten nur beim Einrichten möglich
  - Schnittstellen können nur durch Neustart rekonfiguriert werden (NT)

Installation Server-Hardware

- Linux
  - Zusätzliche Platte auch während des Betriebs möglich
  - Volumes über mehrere Platten nur beim Einrichten möglich, aber dazumounten im laufenden Betrieb möglich
  - Schnittstellen können während des Betriebs rekonfiguriert werden

Installation Anwender-Software

- Netware
  - Von einer Arbeitsstation (wenige Ausnahmen)
  - Konfiguration auf einer Arbeitsstation
  - Verteilung automatisch möglich

Installation Anwender-Software

- Windows-NT/2000
  - Von einer Arbeitsstation oder am Server
  - Konfiguration auf einer Arbeitsstation oder am Server
  - Verteilung automatisch mit Zusatzprodukten möglich

Installation Anwender-Software

- Linux
  - Von einer Arbeitsstation oder am Server
  - Konfiguration auf einer Arbeitsstation oder am Server
  - Verteilung halbautomatisch (mit Hilfe von Scripts) möglich

Sicherheit - Server

- Netware
  - Consolenlockpassword möglich
  - Remoteconsolenpassword möglich
  - Reboot nur nach DOWN oder durch Hardwarereset
  - Filesystem übersteht Stromausfall im Allgemeinen ohne Probleme

Sicherheit - Server

- Windows-NT/2000
  - Consolenlockpassword Standard
  - Remoteconsole nicht möglich
  - Reboot nur nach DOWN oder durch Hardwarereset
  - Filesystem übersteht Stromausfall im allgemeinen schlecht (2000 besser)

Sicherheit - Server

- Linux
  - Consolenlockpassword Standard
  - Remoteconsole möglich
  - Reboot nur nach DOWN oder durch Hardwarereset
  - Filesystem übersteht Stromausfall im allgemeinen schlecht aber es existieren ausfallsichere Dateisysteme (z.B.: Reiser)

Sicherheit - Zutritt

- Netware
  - höchster Schutz durch RSA-Verfahren (Passwörter werden nicht übertragen)
  - Zeiteinstellung pro Benutzer
  - Flexible Stationseinstellung pro Benutzer
  - Intruder detection
  - Anzahl der gleichzeitigen Logins pro Benutzer
  - Ablaufdatum pro Benutzer
  - Account Balance

Sicherheit - Zutritt

- Windows-NT/2000
  - Verschlüsselung nicht nach Standards
  - Zeiteinstellung pro Benutzer
  - Stationseinstellung pro Benutzer
  - Intruder detection
  - Ablaufdatum pro Benutzer
  - Keine Account Balance
  - Passwortparameter nur global einstellbar

Sicherheit - Zutritt

- Linux
  - Verschlüsselung nicht Standard
  - Zeiteinstellung pro Benutzer nicht Standard
  - Stationseinstellung pro Benutzer nicht Standard
  - Intruder detection nicht Standard
  - Ablaufdatum pro Benutzer nicht möglich
  - Keine Account Balance
  - Passwortparameter nur global einstellbar
  - durch PAMs aber erweiterbar

Sicherheit - Zugriff

- Netware
  - Flexible Rechte pro NDS-Objekt
  - Flexible Rechte pro Datei/Verzeichnis
  - Flexible Plattenplatzzuteilung
  - Dateizugriffe überwachbar

Sicherheit - Zugriff

- Windows-NT/2000
  - Wenig flexible Rechte auf Objekte
  - Rechte auf Dateien/Verzeichnisse zwar flexibel, aber durch 2 Arten fehleranfällig
  - Keine Plattenplatzbeschränkungen möglich
  - Dateizugriffe überwachbar

Sicherheit - Zugriff

- Linux
  - Wenig flexible Rechte auf Objekte
  - Wenig flexible Rechte auf Dateien/Verzeichnisse
  - Plattenplatzbeschränkungen als Zusatz möglich
  - Dateizugriffe überwachbar

Sicherheit - Daten

- Netware
  - Plattenspiegelung
  - Serverspiegelung (bzw. HA-Lösung)
  - UPS-Support gut
  - Sehr flexibles Backup
  - Datenmigration

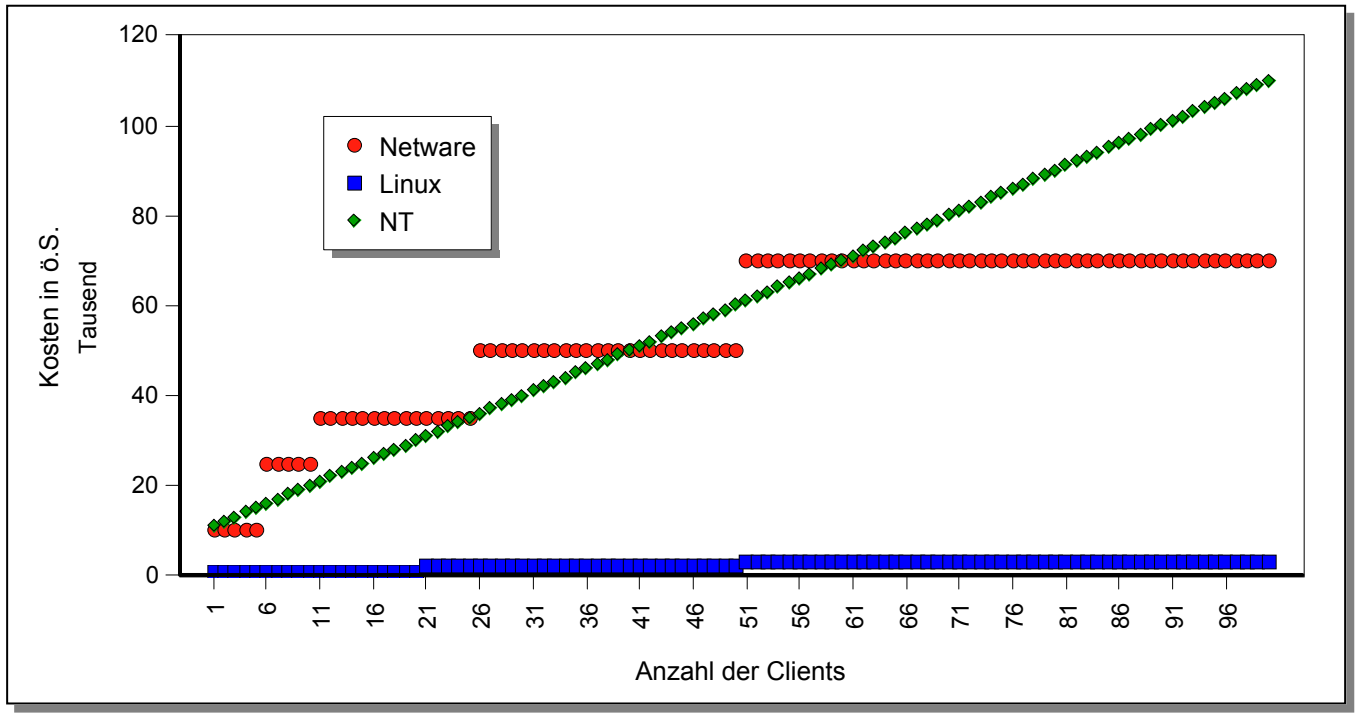
Sicherheit - Daten

- Windows-NT/2000
  - Plattenspiegelung
  - keine Serverspiegelung (HA-Lösungen durch Drittanbieter)
  - UPS-Support
  - Backuplösungen nicht zufriedenstellend
  - keine Datenmigration

Sicherheit - Daten

- Linux
  - Plattenspiegelung
  - keine Serverspiegelung (HA-Lösungen möglich aber aufwendig)
  - UPS-Support noch verbesserungsfähig
  - Backupsupport noch verbesserungsfähig
  - keine Datenmigration

Kosten


120
100
80
60
40
20
0
Kosten in ö.S.
Tausend
Netware
Linux
NT
1
6
11
16
21
26
31
36
41
46
51
56
61
66
71
76
81
86
91
96
Anzahl der Clients

Vorteile/Nachteile Netware

+ NDS (Netware Directory Services)
+ Marktanteil ca . 50 %
+ Höchste Performance als Fileserver
+ Flexibelste Struktur
+ Unterstützung heterogener Netze
+ C2-Security
+ SFT Level III
+ Flexible Backuparchitektur und Software
+ SMP und Skalierbarkeit
+ Applikationsserver
- Schlechtes Marketing führt zu schlechtem Support durch Dritte

Vorteile/Nachteile NT/2000 Server

+ Applikationsserver
+ Hohe Skalierbarkeit und Prozessorunabhängigkeit
+ Benutzeroberfläche vielen bekannt
+ Remote Access Services

- Unterstützung heterogener Netze
- C2 Security mangelhaft
- Kein SFT III
- Umständliche Administration
- Schlechte Backuplösung

Vorteile/Nachteile Linux Server

+ Sourcecode verfügbar
+ Unterstützung heterogener Netze
+ Applikationsserver
+ Modemsupport
+ Hohe Performance und Skalierbarkeit

- SMP
- C2 Security nicht gegeben
- Kein SFT III (Standardmäßig auch kein SFT II)

Einsetzbarkeit

- Prinzipiell sind alle Systeme für alle Aufgaben einsetzbar
- Eine zentrale Datenhaltung bevorzugt Systeme die auch mit vielen Clients keine Performanceprobleme haben
- Auf Datensicherheit sollte größter Wert gelegt werden
- Die Unterstützung neuer Hardware durch Softwaretreiber ist derzeit bei Netware am besten

Entscheidungshilfen - 1

- Welche Systeme sind bereits im Einsatz ?
- In welches System können bestehende Systeme eingebunden werden (Daten können praktisch immer übernommen werden).
- Für welches System existiert die größte Auswahl an Applikationen ?
- In welchem System wird die größte Unabhängigkeit von einem Hersteller geboten ?
- Wo ist das Kriterium Ausbaubarkeit des Systems am besten erfüllt ?

Entscheidungshilfen - 2

- Wo ist das Kriterium Interoperabilität am besten erfüllt ?
- Wo ist das Kriterium Setzen von Standards am besten erfüllt ?
- Wo ist das Kriterium Erfüllen von Standards am besten erfüllt ?
- Welches System bietet genügend Wachstumsmöglichkeiten bei den Resourcen (Plattenplatz, Datenbankgröße, ...) ?

Zusammenfassung - Geläufige LANs

Das optimale Netzwerkbetriebssystem existiert derzeit nicht. Für genau definierte Anforderungen kann aber ein gutes Netzwerkbetriebssystem gefunden werden. Die Entscheidung sollte nicht so sehr von einem “Entweder-Oder” sondern viel mehr von einem “Sowohl-als-Auch” geprägt sein.

III. WAN

1. Dienste
2. Internet

WAN – Allgemeines

- Viele Bereiche, die schon im Punkt I.LAN besprochen wurden gelten auch hier (Topologie, Übertragung, Vermittlung)
- Im WAN gilt aber i.A., dass die eigentliche Übertragung von einem Diensteanbieter übernommen wird.

II.1. WAN - Dienste

- Analog/Digital-Telefondienste, ISDN
- Standleitungen
- Datex-L/Datex-P
- xDSL
- „Fernseh“-Kabel
- Powerline
- LWL von verschiedenen Anbietern

III.2. Internet

- Einleitung
- Internetadressierung
- Internetdienste
- Wichtige Begriffe
- Sicherheit in Internet
- Internetzugang

III.2.1. Einleitung

- 1962 Erste Arbeiten zum Thema
- 1.9.1969 Beginn des ARPA-Nets
- 1972 erste öffentliche Vorstellung
- 1982 TCP/IP
- 1983 Kopplung mit dem CSNET
- 1986 NSFNET als Backbone des Internets

III.2.2. Internetadressierung

- Symbolische Adressen (DNS-Adressen)
- Logische Adressen (IP-Adressen)
- Physische Adressen (MAC-Adressen)
- Subadressen (Ports)
- e-Mail-Adressen
- URL

Symbolische Adressen

- Dienen in erster Linie dazu, die Adressen für uns leichter merkbar zumachen.
- z.B.:
  - WWW.ADV.AT
  - WWW.ORF.AT
  - MIRACULIX.HTL-TEX.AC.AT

Symbolische Adressen 2

- Bestehen aus zwei Teilen, dem Rechnernamen und dem Domainnamen und muß weltweit eindeutig sein.
- Die symbolischen Adressen werden mittels DNS (Domain Name System) in logische Adressen umgewandelt.
- Das DNS ist hierarchisch (nicht jeder Nameserver kennt alle Adressen).

Symbolische Adressen 3

- Rechner arbeiten nie mit symbolischen Adressen.
- Der nächstgelegene DNS-Server muß dem Rechner mit seiner logischen Adresse bekannt sein.

Symbolische Adressen 4

- Die Domainnamen sind strukturiert aufgebaut.
- Eigentlicher Domainname (häufig der Firmenname)
- SLD (Second level domain)
- TLD (Top level domain)

Symbolische Adressen 5

- Gängige SLDs
  - ac — academic
  - co com — commercial
  - ed edu — education
  - gv gov — government
  - mil — military
  - or org — organisations

Symbolische Adressen 6

- gängige TLDs
  - gTLDs Generic Topleveldomains

    Aus der Anfangszeit des Internets weltweite zentrale Vergabe durch von der ICANN beauftragte Institutionen
  - ccTLDs country code TLDs

    Für jedes Land ein Kürzel nach ISO 3166-1

Symbolische Adressen 7

- gTLDs
  - .aero Luftfahrtunternehmen
  - .biz Firmen
  - .com Kommerzielle Angebote
  - .coop Cooperatives
  - .edu Ausbildungsorganisation
  - .gov US Government
  - .info Informationsangebote

Symbolische Adressen 8

- gTLDs
  - .int Internationale Organisationen
  - .mil US Militär
  - .museum Museen
  - .name Für Einzelpersonen
  - .net Netzwerkbetreiber (ISPs)
  - .org Non-Profit Organisationen
  - .pro Gedacht für freie Berufe

Symbolische Adressen 9

- ccTLDs (Beispiele)
  - .at Austria
  - .au Australien
  - .ca Kanada
  - .de Deutschland
  - .fr Frankreich
  - .it Italien

Symbolische Adressen 10

- Beispiel 1

www.may.co.at

www	Name des Rechners
.may	Name der Firma
.co	commercial
.at	austria

Symbolische Adressen 11

- Beispiel 2

www.univie.ac.at

www	Name des Rechners
.univie	Name der Firma
.ac	academic
.at	austria

Logische Adressen

Die eigentlichen Internetadressen sind die logischen Adressen, die derzeit (IPv4) 32 Bit - aufgeteilt auf 4 8-Bit-Gruppen - groß sind. In nächster Zeit ist ein Umstieg auf 128 Bit große Adressen zu erwarten (IPng, IPv6).

z.B.: 131.130.1.78

195.2.9.33

Logische Adressen 2

- Ursprünglich wurden diese Adressen in Klassen eingeteilt und je nach Firmengröße zugeteilt
- Heute spricht man meist von Classless Interdomain Routing, da dabei die Adressen besser genutzt werden können.

Adreßklassen

Klasse	B1	B2	B3	B4	1.Byte	#Netze	#Knoten
A	0	x	x	x	0-127	126	~16777216
B	1	0	x	x	128-191	~16384	~65536
C	1	1	0	x	192-223	~2097152	254
D	1	1	1	0	224-239	-	-
E	1	1	1	1	240-255	-	-

Versteckte Adressen

- Da mit den zur Verfügung stehenden Adressen nicht mehr das Auslangen gefunden wurde und der Umstieg von IPv6 doch länger dauert, wurden versteckte Adressen eingeführt
- Adressen, die wie Internetadressen aussehen, aber nicht über das Internet erreichbar sind.

Physische Adressen

- Adressen, die dem Rechner üblicherweise hardwaremäßig zugeteilt sind, die aber vom verwendeten Netzwerk abhängen (z.B.: Ethernet, Token Ring, ...)
- Diese werden auch MAC-Adresse (NIC-Adresse, Hardwareadresse) genannt.

Subadressen

- Da auf einem Rechner mehrere Dienste verwendet werden können (z.B. gleichzeitiger e-Mail-Empfang, MP3-Download und Surfen), muß es zusätzlich zur Rechneradresse noch interne Unterscheidungsmerkmale geben
- Ports

Ports – Einteilung

- Statische („well known“)-Ports für bestimmte Serverdienste (Webserver, DNS-Server, Mailserver, ...)
- Dynamische Ports für die Clientanwendungen (Browser, e-Mail-Programm, ...)

Wichtige „well-known“ Ports

- 21 FTP (Kopieren von Dateien)
- 22 SSH (Sicheres Anmelden)
- 23 Telnet
- 25 SMTP (Versenden von e-Mails)
- 80 HTTP (Webserver)
- 110 POP3 (Empfangen von Mails)

Dynamische Ports

- Ab der Nummer 1024 werden die Ports i.a. dynamisch vergeben, d.h. eine Applikation fordert vom Netzwerksystem eine Portnummer an und bekommt diese für die Dauer einer Sitzung zugeteilt.
- Z.B.: e-Mail-Client frägt Mails ab

  Port 1025 (Client) an Port 110 (Server)

e-Mail-Adressen

- Bei e-mail-Adressen gibt es wieder 2 Teile
  - Name
  - Rechner oder Domainadresse
- Die beiden Teile werden durch das at-Sign (Klammeraffen, at-Zeichen, @) getrennt.

e-Mail-Adressen 2

- Mailadressen sind häufig nur ein Alias (logischer Name zu einem Postfach)
- Eine Person kann mehrere e-Mail-Adressen besitzen.
- Verschiedene logische e-Mail-Adressen können dasselbe Postfach benutzen
- Mehrere Personen können sich eine e-Mail-Adresse teilen

URL

- Uniform Resource Locator
- Um die verschiedenen Adreßformate übersichtlicher darstellen zu können, wurde eine einheitliche Schreibweise entwickelt.
- <protocol>:<adresse>

URL – Beispiele

- http://www.adv.at/veranstaltungen/index.htm
- http://www.wien.gv.at/wiengrafik/suche.htm
- http://www.coufal.biz/
- mailto:office@coufal.org
- mailto:klaus@coufal.at?subject=Anfrage
- ftp://ftp.tuwien.ac.at/
- ftp://ftp.univie.ac.at/mirror/simtelnet/
- file:///D|/WWWHome/Klaus/Index.html

III.2.3. Internetdienste

- WWW
- e-Mail
- Listen
- FTP, SFTP
- Telnet, SSH
- News

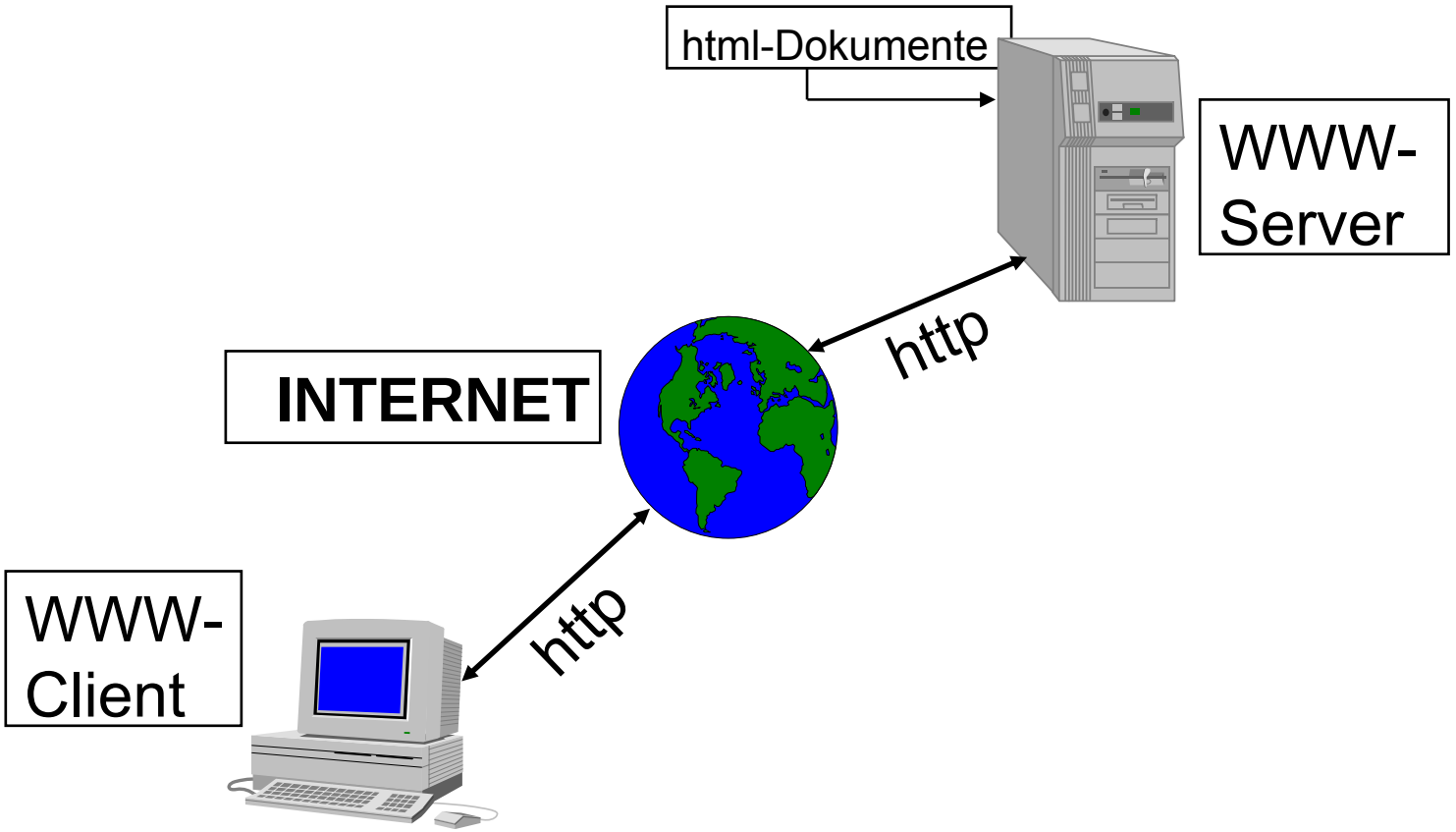
Dienste – WWW

- Grundbegriffe
  - Hypertext
  - Hyperlink
  - Hypermedia
- 1989 am CERN entwickelt
- 1. Browser MOSAIC $\rightarrow$ Navigator

Dienste – WWW

- Webserver stellen über HTTP Informationen in standardisierter Form (HTML) zur Verfügung
- Webbrowser stellen diese dar
- Layoutkontrolle grundsätzlich am Client (Browser), d.h. Angepaßt an die Fähigkeiten des Clients

Dienste – WWW - Überblick



Dienste – WWW-Server

- Apache (Open Source)
- Websphere (IBM)
- Netware Enterprise Server (Novell)
- Internet Information Server (Microsoft)
- Microcontroller-basierende Webserver (Steuer- und Überwachungsaufgaben)
- ...

Dienste - Webbrowser

- Internet Explorer (Microsoft)
- Navigator (Netscape)
- Opera (Opera)
- Mozilla (Open Source)
- Konquerer (Open Source)
- Lynx (Open Source, textbasierend)
- ...

Dienste – Webnutzung

- Hypermedia erfordert auch entsprechende Nutzung
- VOR bzw. ZURÜCK-Buttons
- Linklisten

Dienste WWW – Bedienung

NAV	IE	Opera	Funktion
			Vorherige Seite
			Nachfolgende Seite
			Akt. Seite neu laden
			Anfangsseite laden

Dienste – WWW – Dynamik

- Dynamische Inhalte Serverseitig
  - SSI
  - Scripts (CGI, Perl, PHP, ASP, ...)
  - Datenbankanbindung
- Dynamische Inhalte Clientseitig
  - Scripts (Javascript, Active X)
  - Bilder (Animated GIFs, Flash, ...)

Dienste – WWW – Proxy

- Zweck: Bessere Nutzung der Bandbreite durch Zwischenspeicherung
- Nur bei statischen Seiten effizient
- Sicherheitsüberlegungen können ebenfalls zum Einsatz führen
- Überwachung des Surfens und Sperre von Seiten möglich

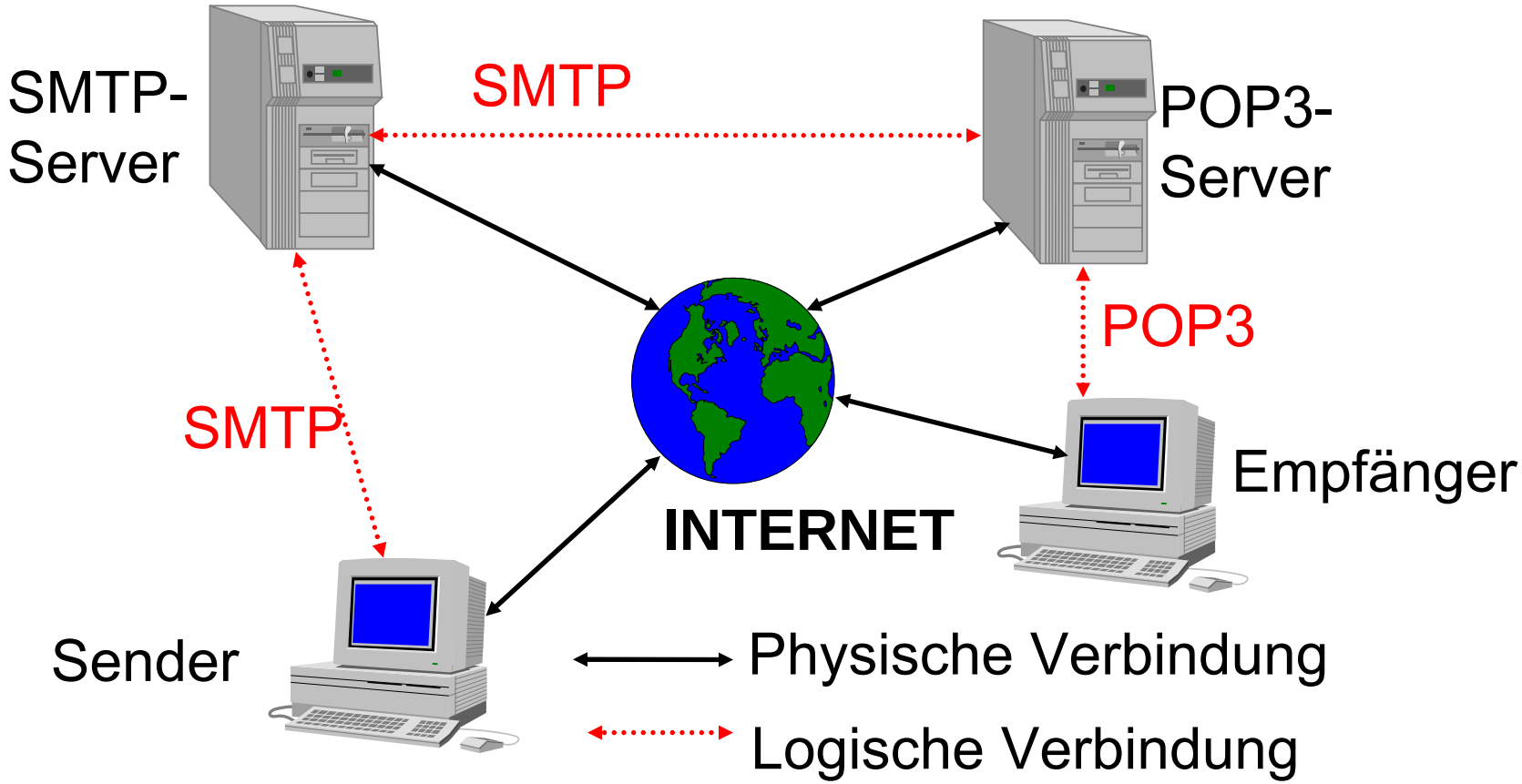
Dienste – WWW VT/NT

+ Benutzerfreundliche Oberfläche
+ Nutzung verschiedenster Dienste mit einem Client
+ Einfache Suchmöglichkeit
- Kein Vorausschau auf zu erwartende Wartezeit
- „Verlaufen“ im Cyberspace

Dienste – e-Mail

- Ältester Dienst im Internet
- Ursprünglich nur ASCII-Texte (7-Bit-Code)
- Formatierungen problematisch
- Ausführlicher Mailheader
- MIME-Codierung

Dienste – e-Mail Funktionsweise



Dienste – e-Mail

- Senden immer per SMTP von e-Mail-Client zum eigenen SMTP-Server (vom Provider)
- Empfangen auf mehrere Varianten vom Postfach beim eigenen Mailserver
  - POP3 (APOP)
  - IMAP4

Dienste – e-Mail Daten

Notwendige Informationen zum Einrichten des Dienstes:

- Generelle Informationen
- Empfangsinformationen
- Sendeinformationen

Dienste – e-Mail Daten 2

- Generelle Information
  - die eigene e-Mail-Adresse
  - Optional Name
  - Optional Firmen-/Organisationsinformationen
  - Optional Rückantwortadresse
  - Optional Unterschriftendatei

Dienste – e-Mail Daten 3

- Empfangsinformationen
  - Empfangsart (POP, IMAP)
  - POP/IMAP-Server
  - Accountname und Passwort
  - Optionale weitere dienstabhängige Parameter

Dienste – e-Mail Daten 4

- Sendeinformationen
  - SMTP-Server
  - Eventuell notwendige Zugangsdaten (Name/Passwort)
  - Optionale weitere Parameter (versetztes Senden, ...

Dienste – e-Mail Programme

- Outlook Express (Microsoft)
- Outlook (Microsoft)
- Messenger (Netscape)
- Pegasus (David Harris)
- Eudora (Eudora)
- elm (Open Source)
- pine (Open Source)

Dienste – e-Mail VT/NT

+ Schnelle Nachrichtenübermittlung (im Vergleich zu snail-Mail)
+ Einfache Weiterverarbeitung der Nachrichten möglich
- Unzureichender Datenschutz
- Keine zentralen e-Mail-Verzeichnisse

Dienste – Listserver

- Verwaltet Listen von e-Mail-Adressen zu verschiedenen Themen
- Offene Listen
- Moderierte Listen
- E-Mail an die Liste bewirkt Versendung an alle Teilnehmer der Liste

Dienste – Listserver - Eintragen

- Nachrichtenformat muß strikt eingehalten werden , da automatische Verarbeitung erfolgt.
- Mail an den Verwalter der Liste (meist majordomo)
- Betreff: i.a. leer
- Text der Nachricht: subscribe <liste>

Dienste – Listserver - Austragen

- Nachrichtenformat muß strikt eingehalten werden , da automatische Verarbeitung erfolgt.
- Mail an den Verwalter der Liste (meist majordomo)
- Betreff: i.a. leer
- Text der Nachricht: unsubscribe <liste>

Dienste – FTP, SFTP

- (Secure) File Transfer Protocol/Program
- Dateitransfer über das Netz
- Eigentliche Benutzername und Passwort notwendig
- Meist aber mit Benutzername anonymous und als Passwort die eigene e-Mail-Adresse möglich

Dienste – FTP, SFTP 2

- Bei den Betriebssystemen nur Commandline-Programm enthalten
- Z.B.: <START> <AUSFÜHREN>

  FTP <rechnername>
- Graphische Varianten von Drittanbietern verfügbar
- Für den privaten Gebrauch oft kostenlos

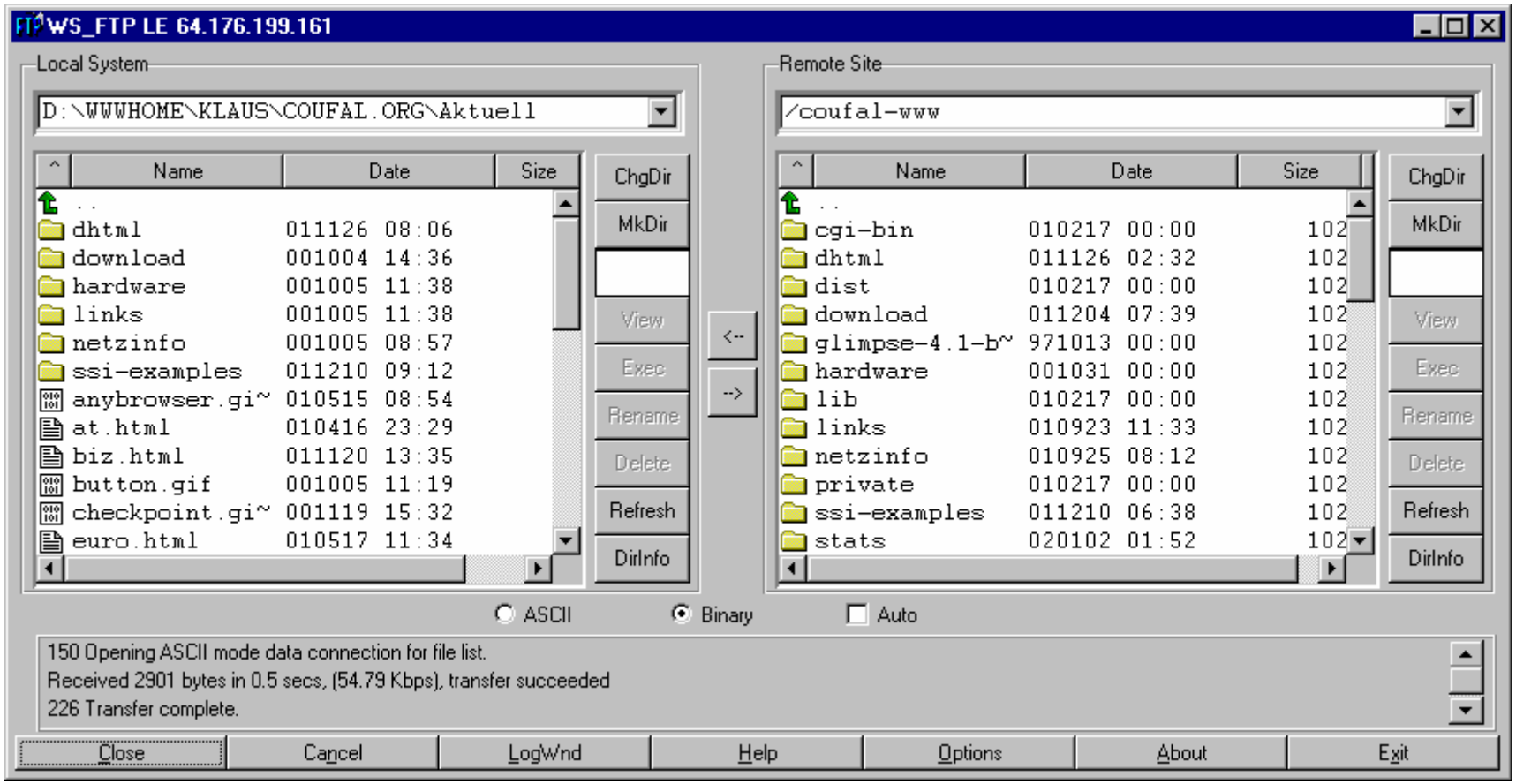
FTP-Commands

- OPEN <server>
- USER <user> (Abfrage nach Passwort)
- GET remote-filename local-filename
- PUT local-filename remote-filename
- BINARY/ASCII
- CLOSE/QUIT/BYE
- DIR/LS

Dienste – FTP graphisch

- Vorkonfigurierbare Sitzungen
  - Servername, Username und Password
  - Startverzeichnis lokal und remote
  - Automatische Übertragungsmodi
- Komplett Mausbedienbar
- Diverse Zusatzfunktionen (Ansehen von remote Dateien)

Dienste – FTP graphisch



Dienste – FTP Übertragung

ASCII	Für Text, dabei werden Anpassungen in der Zeilenschaltung vorgenommen
BINARY	Für Binärdateien, hier werden keine Anpassungen vorgenommen
PASSIV	Verbindung wird vom Client aufgebaut

Dienste – FTP $\rightarrow$ SFTP

- Die leichte Abhörbarkeit einer FTP-Verbindung hat dieses Protokoll in Verruf gebracht
- Secure FTP verwendet eine SSH (siehe unten)-Verbindung für die Übertragung und erreicht damit eine wesentlich höhere Sicherheit.

Dienste – FTP VT/NT

+ Einfache Art Dateien zu kopieren
+ Wenige Befehle
+ Riesige Datenbestände
+ Oft lokaler Mirror eines interessanten Datenbestandes vorhanden
- Unzureichender Datenschutz, daher nur anonym zu empfehlen bzw. SFTP

Dienste – Telnet, SSH

- Anmelden an einen entfernten (remote) Rechner
- Danach verläuft die Arbeit, so als würde direkt an diesem Rechner gearbeitet werden
- Daher auch die Bedienung des Rechner mit dessen Befehlen (häufig UNIX)

Dienste – Telnet

- Die Daten inklusive der Anmeldedaten werden im Klartext übertragen und können daher leicht abgehört werden.
- Fernadministration von praktisch allen Multiusersystemen möglich.
- Z.B.: <START> <AUSFÜHREN> TELNET <rechnername>

Dienste – SSH

- Schutz der übertragenen Daten durch Verschlüsselung
- In den WIN32-Systemen nicht standardmäßig implementiert
- Free Client für Win32: PuTTY
- Nur zu Rechnern mit einem SSH-Server möglich

Dienste – Telnet VT/NT

+ Einfacher Zugang auf einen entfernten Rechner
+ Auf den Zielrechner die auf diesem Rechner gewohnten Befehle
- Unzureichender Datenschutz

Dienste – News

- Weltweites Diskussionsforum
- Analog den schwarzen Brettern, daher einfach in der Bedienung, häufig in die e-Mail-Clients integriert
- Durch den hierarchischen Aufbau kann der Überblick über die Themenvielfalt bewahrt werden

Dienste – News

- NNTP
- Newsgroup
- News-Reader
- Posten, Posting
- Followup

Dienste – News VT/NT

+ Weltweit Artikel zu fast allen Themen vorhanden
+ Verteilte Speicherung, daher sinnvolle Zugriffszeiten
- „Spreu vom Weizen zu trennen“ nahezu unmöglich

III.2.4. Wichtige Begriffe

- Routing
- Subnetting
- NAT, IP-Masquerading
- Suchmaschinen
- Kataloge

Begriffe – Routing

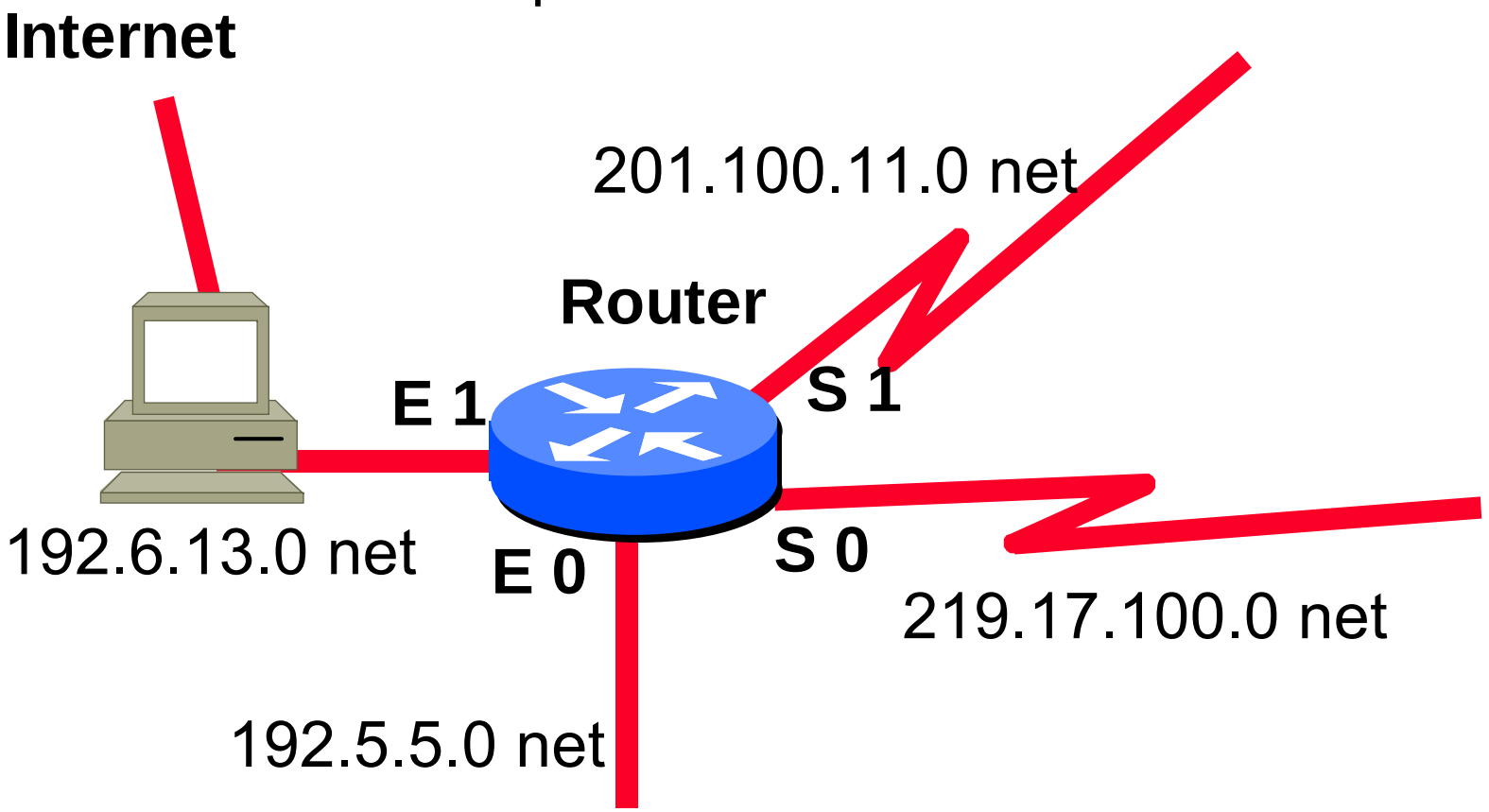
Routing ist der Vorgang, bei dem über das Netz empfangene Pakete zum Ziel weitergeleitet werden, dabei wird die logische Adresse für die Wegewahl verwendet. Routing wird sowohl von Rechnern als auch speziellen Geräten (Routern) durchgeführt.

Router – Funktionsweise 1

- Entpacken eines Frames bis zur Routing Schicht
- Vergleich der Netzanteils der Adresse mit den Einträgen der Routingtabelle
- Weiterleiten zur entsprechenden Schnittstelle
- Einpacken in einen neuen Frame

Router – Funktionsweise 2

Beispiel



Router – Funktionsweise 3

Beispiel Routingtabelle

Netz	Schnittstelle
192.5.5.0	E0
192.6.13.0	E1
201.100.11.0	S1
219.17.100.0	S0
223.8.151.0	S1
Default	E1

Begriffe - Subnetting

- Aufteilung eines bestehenden Netzwerkes in kleinere Einheiten
- Modularisierung
- Anbindung mehrere Teile oder Firmen mit einem Netz möglich
- Subnetmaske

Subnetting - Funktionsweise 1

- Jede IP-Adresse besteht aus 2 Teilen
  - Netzanteil

    Bestimmt den gemeinsamen Teil der Adresse, der für alle Rechner im selben Netz gleich ist.
  - Hostanteil

    Ist der „Unique“-Anteil der Adresse, den nur diesem Rechner zugeordnet ist.

Subnetting - Funktionsweise 2

- Sehr oft wird nicht der gesamte Adressbereich für ein Netz benötigt, dann kann dieses Netz in Subnetze geteilt werden, d.h. ein Teil der Host-Adresse wird für den Subnetzanteil verwendet.
- Aufteilung eines Netzes in Subnetze

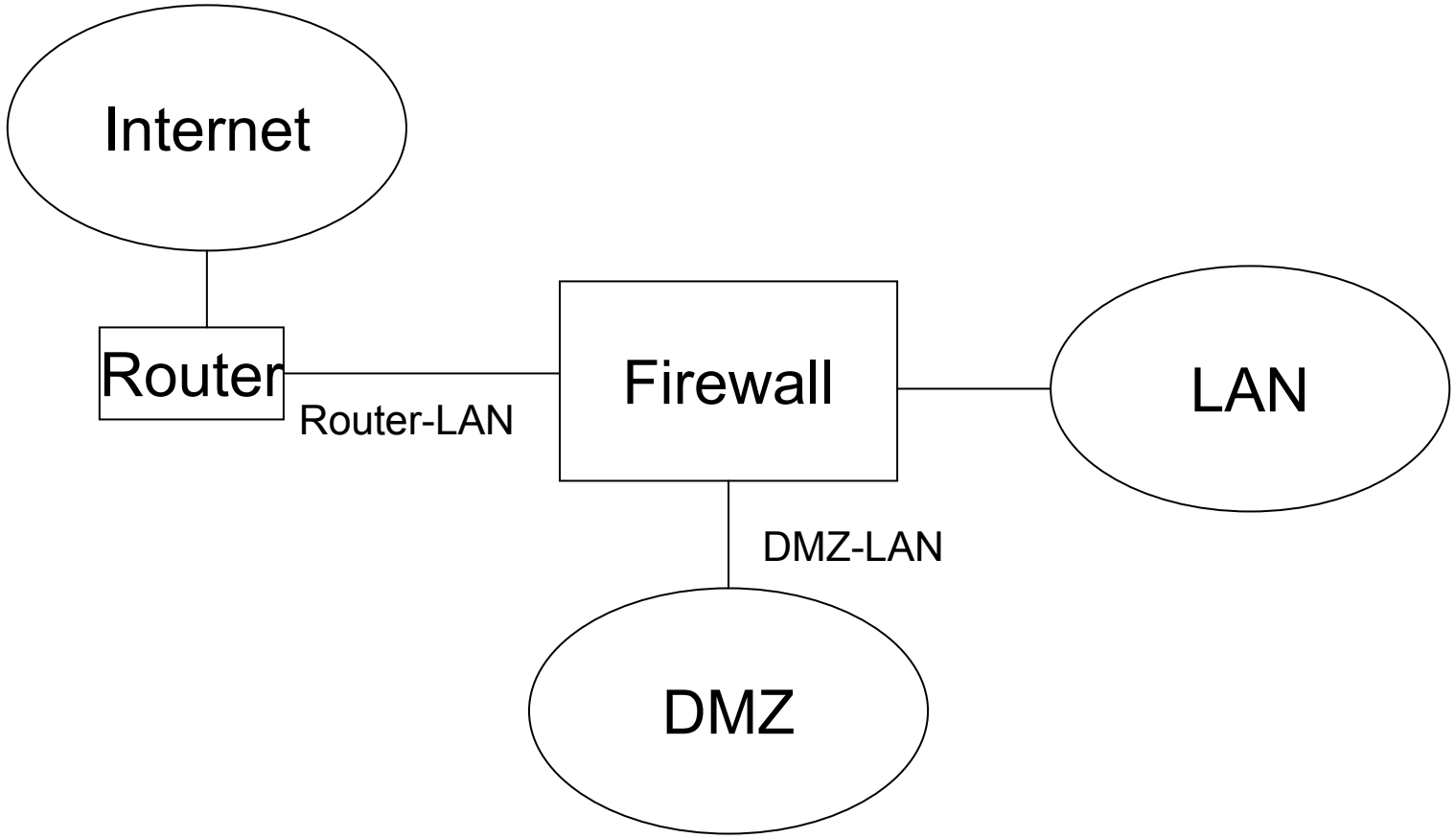
Subnetting - Funktionsweise 3

- Die Adressen haben eigentlich 3 Teile:
  - Netzanteil, Subnetzanteil, Hostanteil
- Für alle beteiligten Systeme ist aber weiterhin nur eine 2-Teilung sinnvoll
  - Netzanteil, Hostanteil
- Der Subnetzanteil wird je nach Betrachtungsweise zum Netz- oder Hostanteil dazugerechnet.

Begriffe – NAT

Nachdem auch Rechner mit versteckten Adressen im Internet Abfragen durchführen wollen (z.B. Nutzung des WWW) wurde das NAT erfunden. Dabei wird die versteckte Adresse durch die offizielle IP-Adresse des NAT-Servers ersetzt und bei der Antwort wieder zurückgetauscht.

NAT - Beispiel



Begriffe – Suchen im Netz

- Mehrere Varianten stehen zur Verfügung, um Informationen im Netz zu finden:
  - Suchmaschinen
  - Metasuchmaschinen
  - Kataloge

Begriffe – Suchmaschinen

- Suchmaschinen indizieren das Web automatisch mit Hilfe sogenannter Robots
- Vor allem für die Suche nach Eigennamen bzw. mit Anfragen bei denen mehrere Begriffe verknüpft werden können.

Suchmaschinen – Beispiele

- www.altavista.com
- www.altavista.at
- www.lycos.com
- www.lycos.at
- www.google.com
- www.google.at

Begriffe – Metasuchmaschinen

- Leiten die Suchanfrage an mehrere Suchmaschinen weiter und sammeln die Ergebnisse.
- Wenn bei Suchmaschinen zu wenig gefunden wird, kann hier eventuell ein größerer Überblick erreicht werden.

Metasuchmaschinen - Beispiele

- www.metacrawler.com

- www.profusion.com

- www.metasearch.com

Begriffe – Kataloge

- Kataloge werden thematisch geordnet und dazu oft manuell zusammengetragen
- Kataloge sind für einen ersten Überblick über ein Wissensgebiet empfehlenswert

Kataloge – Beispiele

- www.yahoo.com 

- www.looksmart.com 

- www.web.de 

Begriffe – Suchenoperatoren

- OR (/) Oder
- AND (+, &) Und
- NOT (-, !) Nicht
- NEAR In der Nähe von
- „ „ Phrasenklammerung
- * Platzhalter (Wildcard)

III.2.5. Sicherheit im Internet

- Sicherheit der Dienste
- Erhöhung der Sicherheit durch (Details siehe unten):
  - symmetrische Verschlüsselung
  - asymmetrische Verschlüsselung
  - RSA
  - PGP
  - Schlüsselverwaltung

Sicherheit – Dienste

- Die Dienste FTP, Telnet, WWW und e-Mail werden standardmäßig im Klartext übertragen, d.h. jeder kann mithören (Postkartensicherheit).
- SSH, SFTP, verschlüsseltes WWW gilt derzeit als sicher.

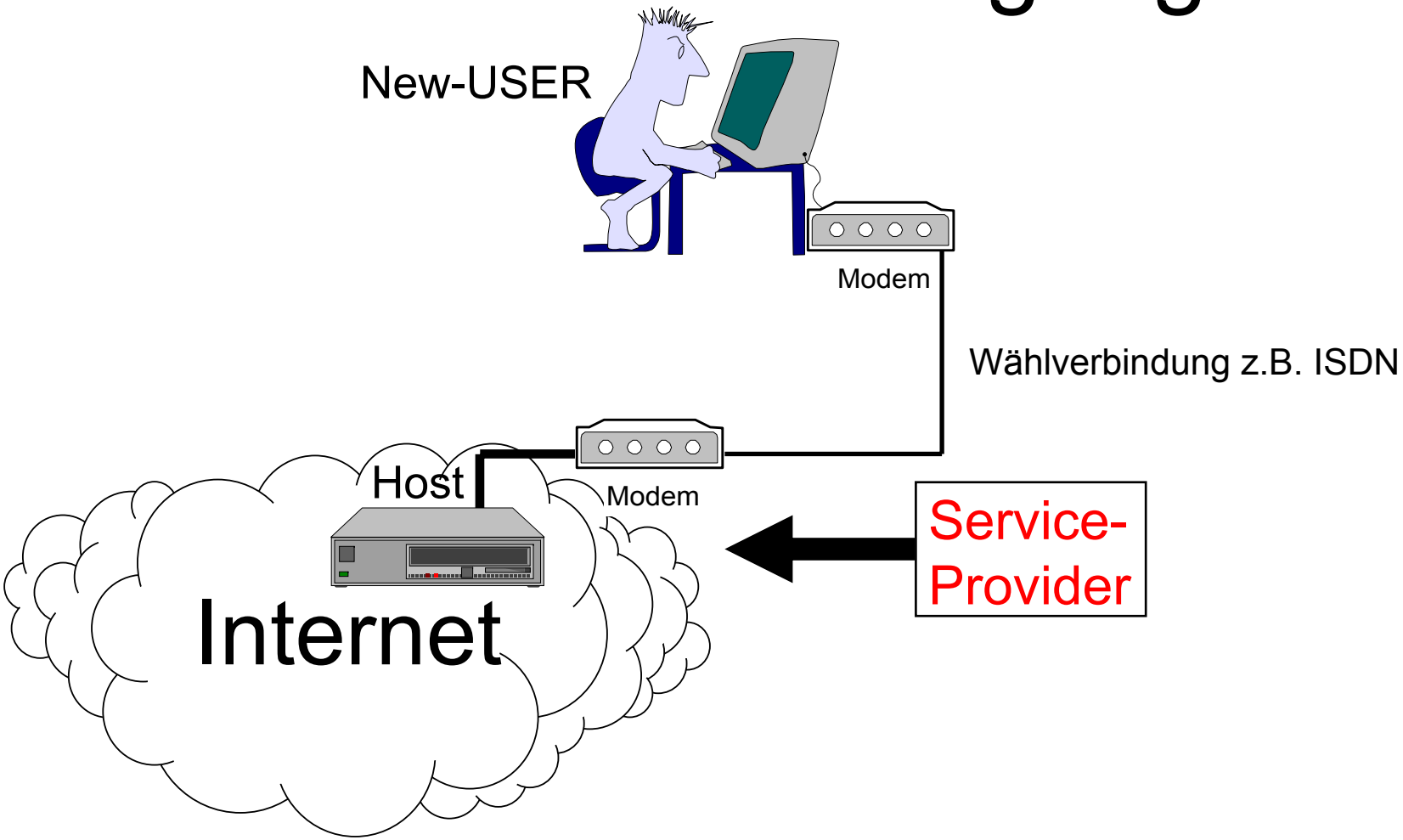
III.2.6. Internetzugang 1

- Wählleitung mit Modem (analog/ISDN)
- Analog/ISDN-Router
- Standleitungen
- ADSL
- Kabelmodem
- Powerline

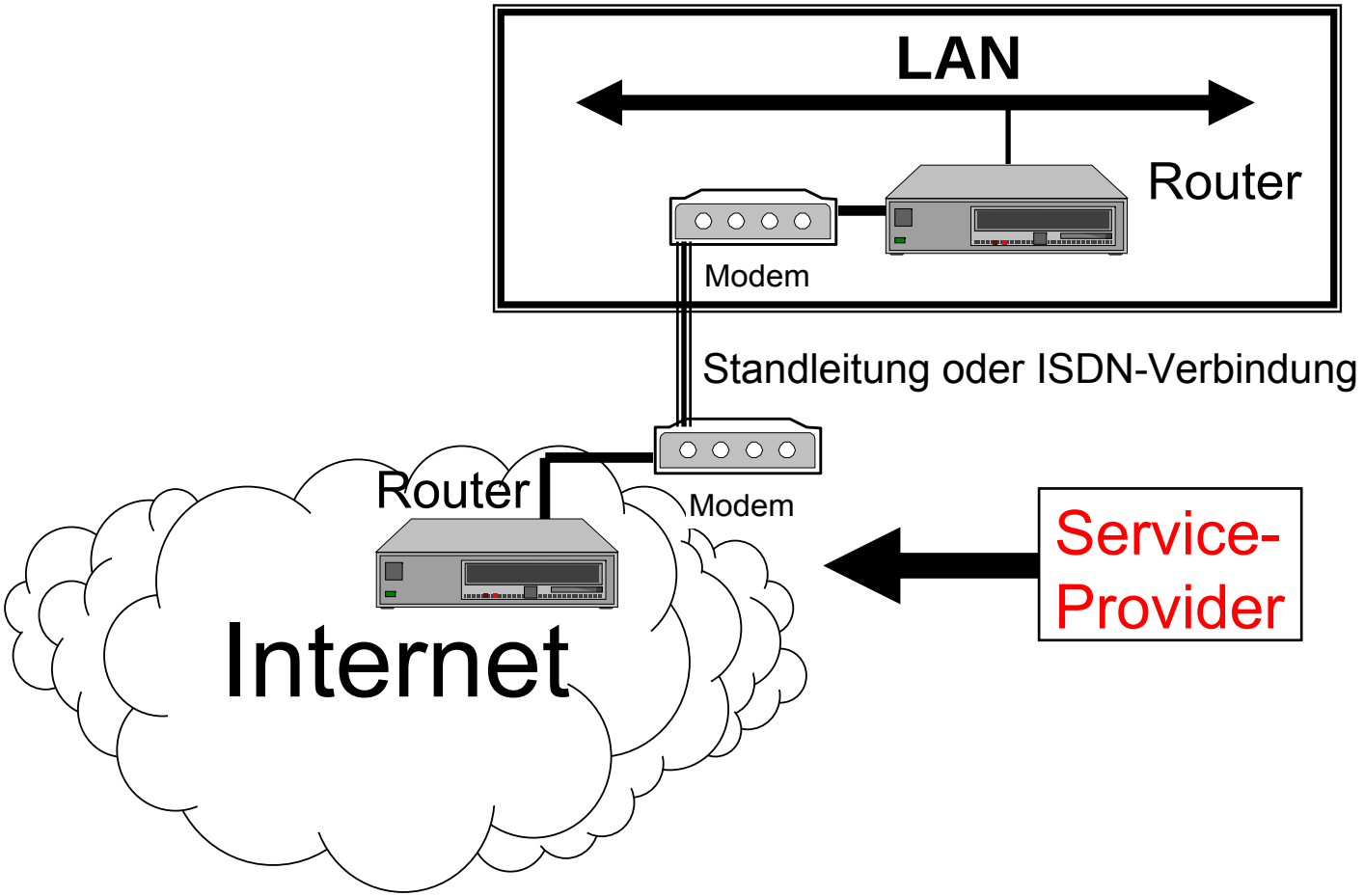
Internetzugang 2

- GPRS
- UMTS
- Provider (Zugangsprovider, Contentprovider, e-Mail-Provider, Webprovider, ...)
- Kosten (Grundgebühr, Volumengebühr, „flat-rate“, Speicherplatz, DNS, ...)

Internet – Einzelzugang



Internet – Netzzugang



Internetzugang – Wählzugang

- Der Zugang wird über eine Wähl-verbindung nur bei Bedarf hergestellt.
- Entweder mittels eines Analog- oder eines ISDN-Modems
- In Windows DFÜ-Verbindung
- Protokoll: PPP bzw. SLIP
- Dynamische IP-Adresse

Internetzugang – Wählrouter

- Hier wird die Verbindung über ein eigenes Gerät bei Bedarf eines Rechners im LAN für alle hergestellt.
- Die Leitung wird geteilt (Bandbreite)
- Beendet wird diese Art der Verbindung durch ein Timeout.
- Dynamische IP-Adresse

Internetzugang – Standleitung

- Bei dieser Art ist die Verbindung mit dem Internet dauerhaft über einen Router hergestellt.
- Üblicherweise zumindest eine fixe IP-Adresse.
- Meist zwei Dienstleister (einer für die Leitung, einer für das Internet).

Internetzugang – ADSL

- Im Prinzip eine Wählleitung
- Wegen der Kostenstruktur oft als Pseudo-Standleitung im Einsatz.
- Höhere Bandbreiten möglich.

Internetzugang – Kabelmodem

- Hier wird über den TV-Kabelzugang eine fixe Internetverbindung geschalten.
- Wie eine Standleitung, allerdings ohne garantierte Bandbreite.
- Bandbreitenzuteilung kann ohne Hardwaretausch erhöht werden.
- LWL zu den Verteilern

Internetzugang – Powerline

- Hier soll die Internetverbindung über das Stromnetz geschalten werden.
- Nicht über das Versuchsstadium hinausgekommen
- LWL zu den Trafostationen
- „Last mile“ über Stromkabel

Internetzugang – Provider

- Zugangsprovider
  - Verfügen über die „Last Mile“
  - Können sowohl Stand- als Wählzugänge anbieten
- Contentprovider
  - Verfügen über schnelle Internetanbindungen
  - Plattenplatz

Internetzugang – Kostenstrukturen

- Grundgebühr
  - Nach Diensten
  - Nach Bandbreite
- Volumengebühr
  - Pro Zugang
  - Pro übertragender Datenmenge
- Speichergebühr

Internetzugang – Kosten 1

- Grundgebühr
  - Für Privatanwender oft Null
  - Für Firmen in Form von Flatrates
- Volumengebühr
  - Für Privatanwender oft nur Zeit oder Flatrates
  - Für Firmen Staffelungen

Internetzugang – Kosten 2

- Speichergebühr
  - Bei Privatanwendern gewisse Pakete inkludiert (z.B.: 10 e-Mail-Adressen und 10 MByte Speicherplatz für Web und Mails)
  - Bei Firmen Staffeln meist gekoppelt mit der Volumengebühr.
  - Keine Einzelabrechnungen mehr.

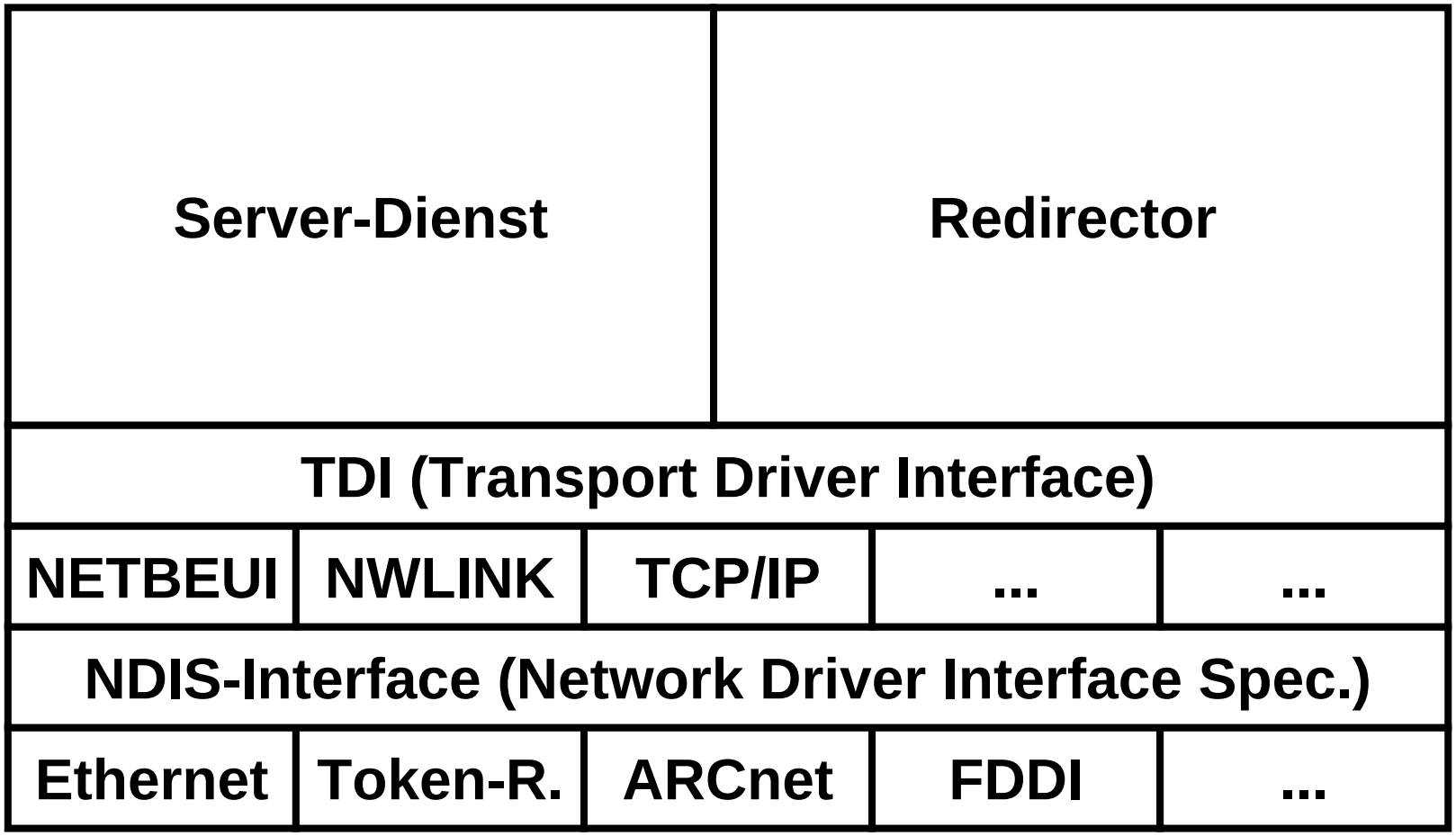
IV. Netzwerkmodelle

- DECnet
- SNA
- Transdata
- Novell-Netzwerkmodell
- Windows-Netzwerkmodell
- Internet-Modell

Novell-Netzwerkmodell

<table>
<tr><td>Netware-Dienst File-Server</td><td>Netware-Dienst Print-Server</td><td>Netware-Dienst Komm.-Server</td><td>Netware-Dienst ...-Server</td><td>Dienst anderer Hersteller</td></tr>
<tr><td colspan="5">Netware Datenflußsteuerung (Streams, TLI, RPC, ...)</td></tr>
<tr><td>IPX/SPX</td><td>TCP/IP</td><td>SNA</td><td>Appletalk</td><td>OSI</td></tr>
<tr><td colspan="5">ODI (Open Datalink Interface)</td></tr>
<tr><td>Ethernet</td><td>Token-R.</td><td>ARCnet</td><td>FDDI</td><td>...</td></tr>
</table>

Windows-Netzwerkmodell



V. Aktuelles