- **IT-Lösungen**
  - **Dokumentationen**
    - **Präsentationen**

PCT-Solutions

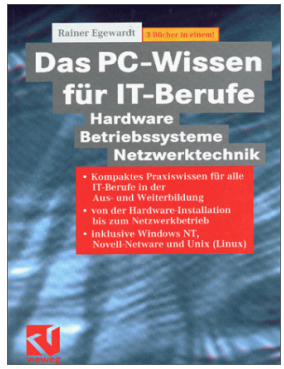
by
Rainer Egewardt

www.pct-solutions.de
info@pct-solutions.de

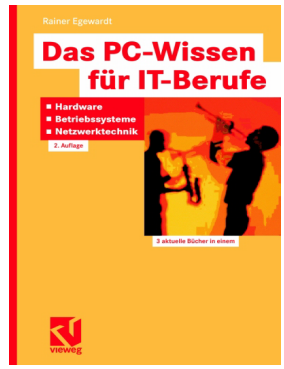
Unser "PC-Wissen für IT-Berufe" ist zu einem Bestseller im IT-Buchmarkt geworden

IT-Buchprojekte von PCT-Solutions

1. Auflage
600 Seiten



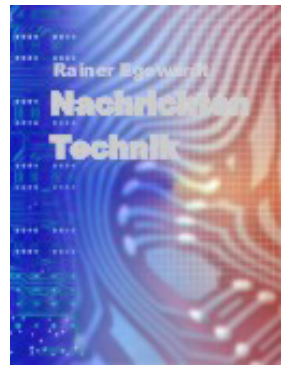
2. Auflage
1200 Seiten



Unser weiteren Buch-Projekte:

600 Seiten

600 Seiten



Nachfolgend
Das PC-Wissen für IT-Berufe

Netzwerk-Technik

2. Auflage

2 Netzwerk-Technik

2.1 Netzwerke

Unter einem Netzwerk wird die Verbindung von mindestens zwei Rechnern verstanden, die gemeinsam Ressourcen nutzen, Informationen gegenseitig austauschen und mit einem einheitlichen Datenbestand arbeiten können.

2.1.1 Netzwerk-Arten

1. Peer-To-Peer-Netzwerk (alle Rechner sind gleichberechtigt):

Die Peer-Rechner benutzen gemeinsam Ressourcen (Drucker, Daten), die auf allen Rechnern verteilt liegen können (schlechte Übersicht, wo Daten liegen). Jeder Peer muss für die Sicherheit seiner Ressourcen selber sorgen.

Ein Peer kann Client sein (wenn er Ressourcen anfordert) oder Server (wenn er Ressourcen verteilt).

- Datenaustausch auf Freigabeebene
- wenn benutzerabhängig, muss jeder Benutzer auf jeder Workstation (WS) bekannt sein
- hoher Verwaltungsaufwand
- keine Datenkonsistenz
- Zugriffskontrolle schwierig
- Datensicherung schwierig
- nur für kleinere Netzwerke zu empfehlen

2. Server basiertes Netzwerk (Client/Server-Prinzip):

In einem serverbasierten Netzwerk gibt es Server, die Dienste und Ressourcen anbieten (star-

ke, leistungsfähige Rechner, die nur für diesen Zweck optimiert sind) und Clients (benutzerorientierte Rechner), die die Ressourcen der Server nutzen.

- zentrale Verwaltung der Freigaben der Benutzerdatenbank des Servers
- zentrale Verwaltung der Daten
- Nutzer müssen nur auf dem Server bekannt sein
- Datenkonsistenz ist Gewähr leistet
- Zugriffskontrolle möglich
- Datensicherung einfach

3. Ausdehnungen:

LAN (Local-Area-Network)

- Lokales Einsatzgebiet
- hohe Übertragungsraten
- Übertragungsmedium = Kabel

MAN (Metropolitan-Area-Network)

- Einsatzgebiet im Stadtbereich und bis zu 50 km Umkreis
- noch hohe Übertragungsraten
- Übertragungsmedium = besonderes Kabel

WAN (Wide-Area-Network)

- Einsatzgebiet weltweit
- geringe – mittlere Übertragungsraten
- Übertragungsmedium = öffentliche Kabel, Satelliten, Richtfunk

2.1.2 Übertragungsmedien

Koaxial-Kabel (10BASE-2):

- Wird im BUS-Netz verwendet (siehe 2.1.3 „Topologien“).

- Axialer Innenleiter, geflochtener Außenleiter.
- Die Netzkarte muss einen BNC-Anschluss haben.
- Das Kabel wird über T-Stücke direkt mit der Karte verbunden.
- Die Enden des BUSses müssen mit Terminatoren (Widerständen) abgeschlossen werden.

Twisted-Pair (10BASE-T):

- Wird überwiegend mit der Stern- oder Baum-Topologie verwendet (siehe Abschnitt 2.1.3 „Topologien“).
- Verdrilltes Paar (können auch mehrere sein, können abgeschirmt (STP) oder nicht abgeschirmt (UTP) sein).
- Die Netzkarte muss einen UTP-Anschluss (RJ 45) haben.
- Die PC´s werden mit dem Kabel über HUB’s (siehe Abschnitt 2.1.14 „Geräte im Netz“) an das Netzwerk angeschlossen.

Fiber-Optic-Kabel (10BASE-F) (Glasfaser):

Lichtwellenleiter

Kupferkabel (Coaxial)		
Kabeltyp	**Impedanz**	**Einsatzgebiete**
RG-58/U	53,5 OHM	teilweise für Ethernet eingesetzt
RG-58A/U	50 OHM	Thinwire-Ethernet, 10Base2
RG-58C/U	50 OHM	Thinwire-Ethernet, 10Base2
RG-59	75 OHM	Kabelfernsehen
RG-62	93 OHM	SNA (3270), ARCnet

Kupferkabel (Twisted Pair)				
Kabeltyp	**Spezifikation**	**spezifiziert**	**Impedanz**	**Einsatzgebiet**
STP	IBM Typ 1/9	20 MHz	150 OHM	4/16-MBit-Token-Ring
UTP-1 Kategorie 1	EIA/TIA-568	–	100 OHM	Analoge Sprachübertragung, Alarmsysteme
UTP-2 Kategorie 2	EIA/TIA-568	–	100 OHM	IBM-Verkabelung Typ3 (Sprache)
UTP-3 Kategorie 3	EIA/TIA-568	16 MHz	100 OHM	10BaseT, 100BaseT4, 100-VG-Anylan, 4-MBit-Token-Ring, ISDN
UTP-4 Kategorie 4	EIA/TIA-568	20 MHz	100 OHM	16-MBit-Token-Ring
UTP-5 Kategorie 5	EIA/TIA-568	100 MHz	100 OHM	100BaseTx, ATM

Glasfaser-Kabel			
Kabeltyp	**Durchmesser** (Kern/Gesamt)	**Bandbreite** (Länge 1 km)	**Einsatzgebiet**
Multimode mit Stufenprofil	100 bis 400 µm / 200 bis 500 µm	100 MHz	unter 1 km
Multimode mit Gradientenprofil	50 µm / 125 µm	1 GHzLAN	Backbone, ATM
Multimode mit Gradientenprofil	62,5 µm / 125 µm	1 GHzLAN	Backbone, ATM

Monomode Singlemode mit Stufenprofil	8 µm/125 µm	100 GHz	Netzwerke mit mehr als 1 GBit pro Sekunde

Zusammenfassung von Daten der wichtigsten Übertragungsmedien:

10Base2 oder Thin-Ethernet:	
Mindestabstand zwischen 2 Clients	0.5 m
Einzelnes Kabelsegment	185 m
Gesamtes Netz darf nicht länger sein als	925 m
Max. Anzahl von Knoten pro Segment (Inc. Clients und Verstärker)	30

Im gesamten Netz darf es nicht mehr als 5 Segmente geben, die über max. 4 Verstärker verbunden werden können, und nur in 3 der 5 Segmente dürfen Knoten enthalten sein.

10Base5 oder Thick-Ethernet:	
Mindestabstand zwischen 2 Transceivern	2.5 m
Einzelnes Kabelsegment	500 m
Gesamtes Netz darf nicht länger sein als	2500 m
Max. Anzahl von Knoten pro Segment (Inc. Clients und Verstärker)	100
max. Länge des Kabels vom Transceiver → Computer	50 m
10Base-T Thin-Ethernet (Twisted-Pair)	
Mindestabstand zwischen 2 Clients	2.5 m
Max. Wegstrecke vom Verteiler zum Computer	100 m

Gesamtes Netz darf nicht länger sein als 925 m
Max. Anzahl von Knoten innerhalb eines LANs 1024

Bezeichnungen der Übertragungsmedien:

10BASE-2

10BASE-5

100BASE-T

10BASE-F

10BROAD36

1BASE5

Die erste Zahl gibt die Übertragungsrate in MBit/s (Megabit pro Sekunde) an.

BASE bzw. BROAD steht für Basis- bzw. Breitband.

Die letzte Zahl/Buchstabe steht für die max. Ausdehnung pro Segment in Hundert Meter, bzw. für das Medium.

T für Twisted-Pair, F für Fiber-Optic, 2 für 200 m, 5 für 500 m, wobei aus der 2 ersehen werden kann, dass hier Thin-Ethernet (meist Twisted-Pair) und aus der 5 Thick-Ethernet (Yellow Cable), benutzt wird.

Die 100BASE-T unterscheiden sich noch in:

100BASE-T4 100 MBit/s über vierpaariges Kategorie-3-Kabel

100BASE-FX 100 MBit/s über zwei Glasfaserleitungen

100BASE-TX 100 MBit/s über zweipaariges Kategorie-5-Kabel (STP oder UTP)

Achtung: Für die jeweiligen Übertragungsraten (10 bzw. 100 MBit/s) müssen auch die entsprechenden Netzwerkkarten, die die Übertragungsrate garantieren, verwendet werden. D.h., über

100-MBit-Karten können natürlich auch 10 MBit übertragen werden, während 10-MBit-Karten keine 100 MBit übertragen können.

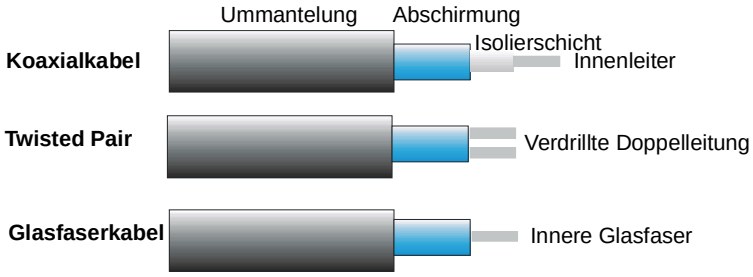


Abb. 1 Kabel

2.1.3 Topologien

Unter einer Netzwerk-Topologie wird die physikalische Auslegung der Verkabelung eines Netzes verstanden. Sie beschreibt nicht nur die elektrische Verbindung, sondern auch die Richtung des Datenflusses im Netz zwischen den Stationen.

BUS-Topologie:

Beim Bussystem sind alle Rechner an einem gemeinsamen, passiven Medium, dem Bus, angeschlossen. Jede Station kann frei, unabhängig von einem Host, kommunizieren. Die Busenden müssen durch Terminatoren abgeschlossen werden. Ein Bussystem hat den geringsten Kabelbedarf.

Informationen fließen in allen Richtungen.

Der Server sollte in der Mitte sein (muss aber nicht).

Der Ausfall eines Knotens führt nicht zum Ausfall des Netzes, wenn es nicht gerade der Server ist. Kabelbruch führt zum Ausfall des Netzes, weil kein Abschluss mehr gegeben ist.

Bekannt geworden ist das Bussystem mit Ethernet.

Die BUS-Topologie eignet sich nur für kleinere Netzwerke.

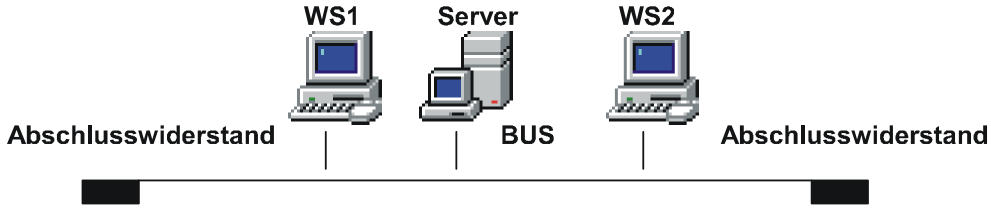


Abb. 2 BUS-Topologie

Ring-Topologie:

Es wird ebenfalls ein gemeinsames Übertragungsmedium verwendet, nur dass dieses, im Gegensatz zum Bussystem, zu einem Ring zusammen geschlossen ist. Jede Station hat einen Vorgänger und einen Nachfolger. Die Informationen werden von Station zu Station weitergereicht, wobei jede Station prüft, ob die Nachricht für sie bestimmt ist.

Informationen fließen in einer Richtung.

Die Ring-Topologie hat die absolut geringste Kabelmenge bei kleineren Netzen.

Der Ausfall eines Knotens oder Kabelbruch führt zum Ausfall des Netzes.

Bekannt geworden ist das System durch Token-Ring.

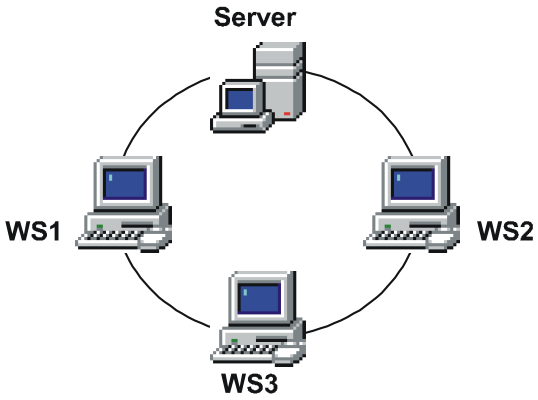


Abb. 3 Ring-Topologie

Stern-Topologie:

Die Sterntopologie ist eine klassische Auslegung, die im Großrechnerbereich verwendet wird. In der Mitte befindet sich der Host und sternförmig daran angeschlossen sind die I/O-Systeme.

Informationen fließen in beiden Richtungen.

Knotenausfall oder Kabelbruch führt nicht zum Ausfall des Netzes.

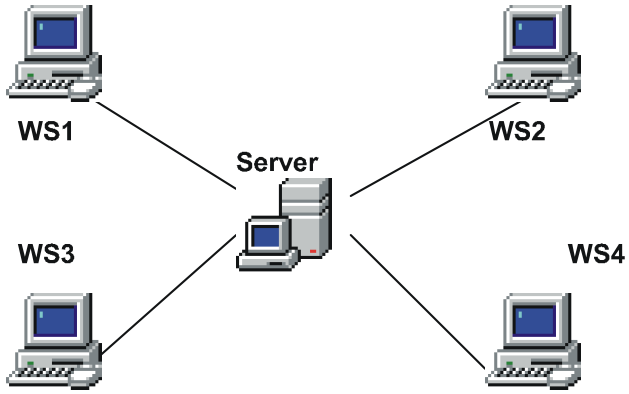


Abb. 4 Stern-Topologie

Die Baum-Topologie stellt eigentlich keine eigene Topologie dar, da sich trotz logischem Stern alle Workstations in einer Collosions-Domain befinden und sich die Bandbreite des Netzes teilen müssen, wie im normalen Bus-Netz.

Dieser Aufbau eines Netzes wird heute am meisten verwendet.

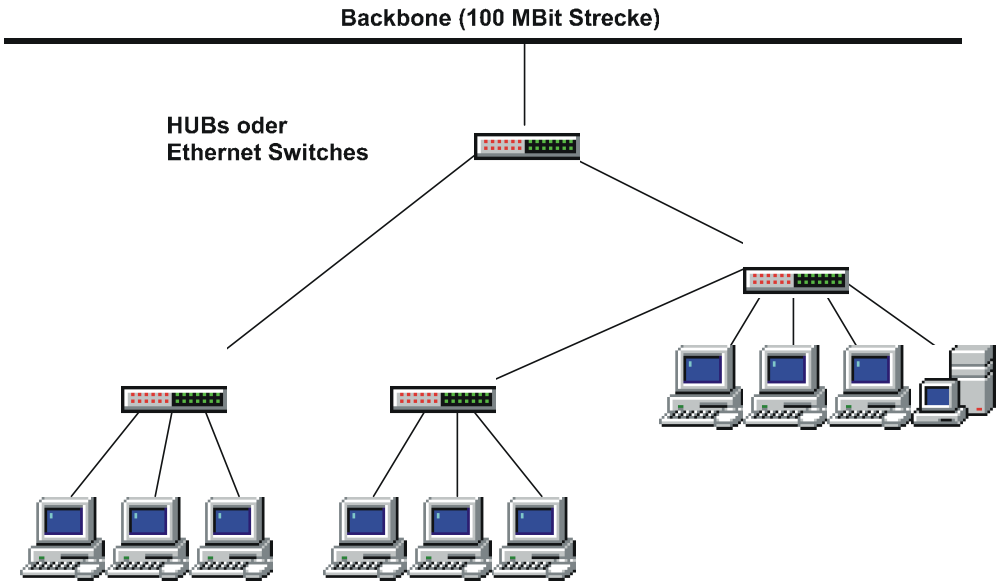


Abb. 5 Baum- (logischer Stern) Topologie

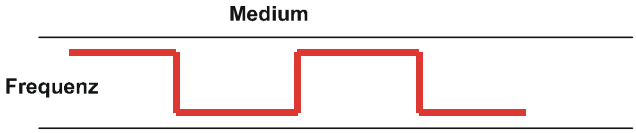
Bandbreite:

Unter der Bandbreite eines Netzwerkes wird die Fähigkeit eines Mediums, Daten zu übertragen, verstanden. Da Datenübertragungsraten in Mega-Bit pro Sekunde angegeben werden, spricht man z.B. von einer Bandbreite von 10 MBit/s.

Übertragene Frequenzen:

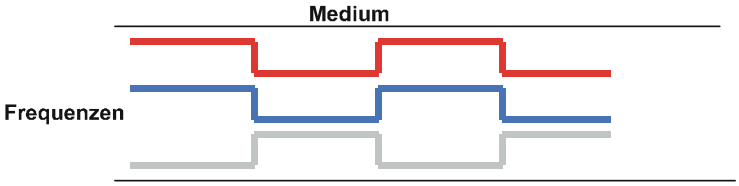
Basisband

Beim Basisband wird die gesamte Kapazität einem Kommunikationskanal zugeordnet.



Breitband

Beim Breitband teilen sich mehrere Kommunikationskanäle die Bandbreite.



Backbones:

Backbones verbinden nur Topologien und stellen keine eigene Topologie dar. Sie sind sehr schnell und laufen an den SUB-LANs vorbei. Mit ihnen werden Übergänge zu anderen Netzen geschaffen, die auch eine andere Topologie aufweisen können.

Bei großen Netzwerken sollte im Backbonebereich mit 100-MBit-Strecken oder einem FDDI-Ring und Switches gearbeitet werden, da hier der größte Netzwerkverkehr zu erwarten ist und so Engpässe vermieden werden können (siehe Abschnitt 2.1.15 „Strukturierte Verkabelung“ und Abb. 15 heterog. TCP/IP-Netz).

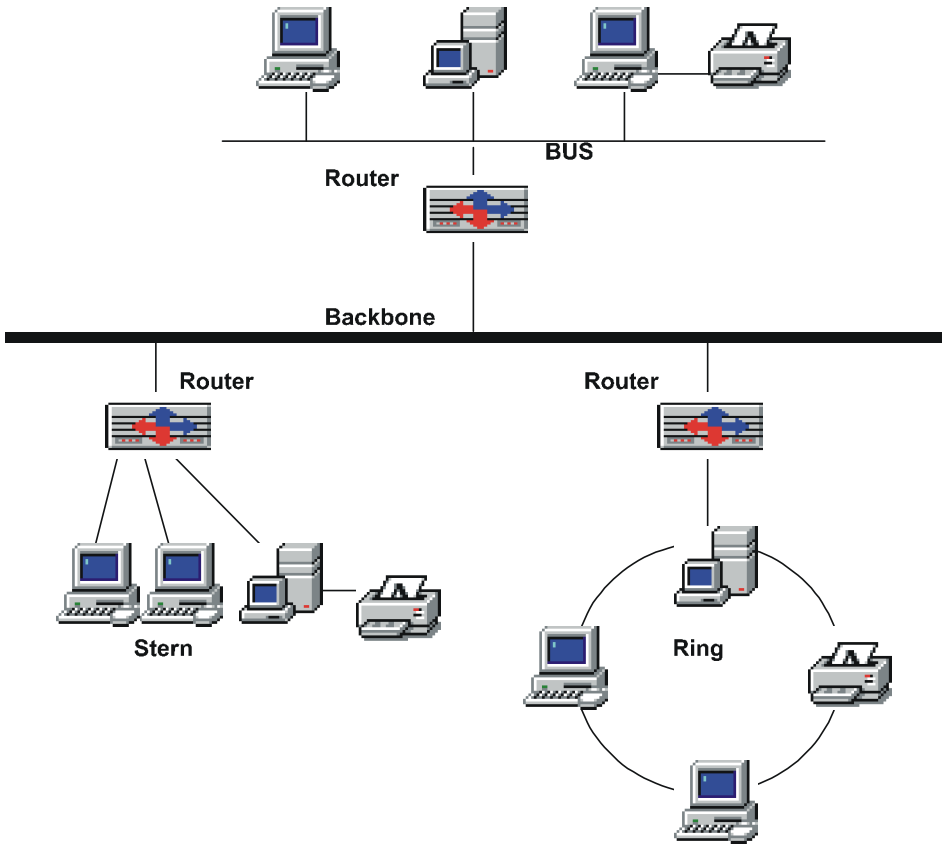


Abb. 6 Backbone

2.1.4 Zugriffsverfahren

Kollosionsverfahren (CSMD/CD):

Damit wird das Zugriffsprotokoll bezeichnet, mit dem Ethernet arbeitet. Das Verfahren regelt hierbei, wie sich die Netzwerkknoten beim gemeinsamen Zugriff auf das Netz verhalten sollen. Es wird im Ethernet angewendet. Es ist nicht beeinflussbar und gehört zur Topologie des Netzes.

Alle Knoten können gleichzeitig senden.

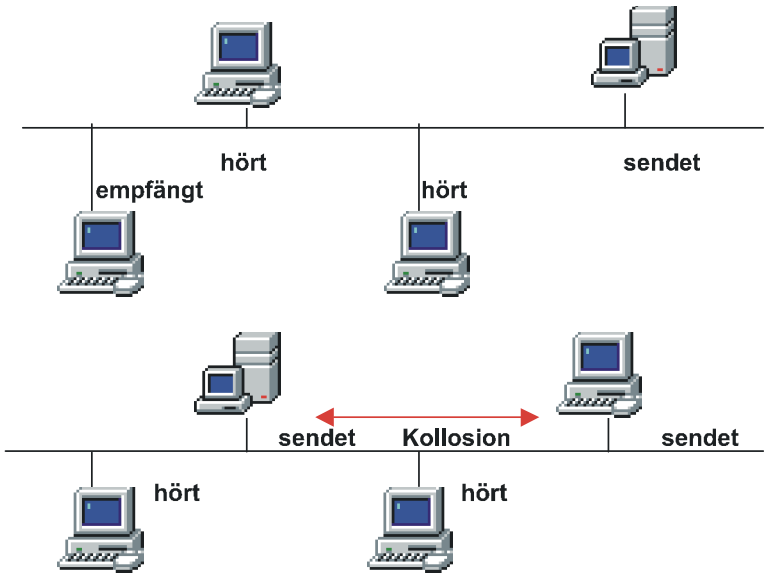


Abb. 7 Kollosions-Verfahren

Vorher wird abgefragt, ob die Leitung frei ist. Wenn sie frei ist, dann wird gesendet. Andere Knoten werden nicht gesperrt und können auch senden.

Es entsteht eine Kollosion.

Der Knoten, der sendet, muss nach dem Senden wieder abfragen, ob eine Kollosion vorliegt (senden eines anderen Knotens gleichzeitig). Stellt er fest, dass eine Kollosion vorgelegen hat, sendet er seine Nachricht nach einer gewissen Zeitspanne nochmal. Dieser Vorgang wird solange wiederholt, bis die Nachricht gesendet und empfangen worden ist.

Token(Zeichen)-Verfahren:

Das Token-Verfahren wird im Ringnetz verwendet. Es wird ein Zeichen von einem Knoten zum nächsten weitergegeben. Dabei gibt es Belegt- und Freitoken. Die Workstation muss abfragen, ob ein Freitoken vorhanden ist. Dann kann sie die Leitung belegen und senden. Jeder Knoten prüft,

ob die Nachricht für ihn bestimmt ist. Wenn nicht, wird das Datenpaket weitergegeben. Ist das Datenpaket beim Empfänger angekommen, nimmt dieser die Daten entgegen und gibt ein Freitoken aus.

2.1.5 FDDI

Als besonderes Zugriffsverfahren zählt FDDI. Es ist das heutige Zugriffsverfahren, dass 100-MBit/s-Übertragungsraten garantiert.

FDDI wurde als 100-MBit-Token-Ring für hohe Bandbreiten konzipiert und wird überwiegend im Backbonebereich mit Glasfaserkabel eingesetzt (lässt sich aber auch mit Koax- bzw. Twisted-Pair realisieren).

FDDI kennzeichnet ein Zugriffsverfahren, aber auch ein Verbindungskonzept und eine Netzwerktypisierung.

Als Übertragungsmedium wird FDDI im Doppel-Token-Ring eingesetzt.

Das Zugriffsverfahren FDDI basiert auf Token-Passing.

2.1.6 ARC-Net

Das ArcNet wird vorzugsweise im Sternnetz verwendet – unter bestimmten Voraussetzungen aber auch im BUS-Netz oder im logischen Ring.

Eckdaten:

- ArcNet Netzwerkkarte
- Kollosionsfreies Token-Bus-Zugriffsverfahren (bei BUS und Stern)
- Wird über Knotenadressen organisiert.
- 2 1/2 MBit/s Übertragungsgeschwindigkeit
- Verwendet das RG-62-Koaxial-Kabel mit 93 Ohm Widerstand.
- Anschluss an BNC-Stecker

- Topologie ist stern- oder busförmig.
- Als Verteiler werden HUB's genommen (aktiv, passiv).

Längen:

Rechner → akt. Hub = 600 m

akt. Hub → akt. Hub = 600 m

Rechner → pass. Hub = 30 m

akt. Hub → pass. Hub = 30 m

Es können bis zu 255 Rechner in ein ArcNet eingebunden werden.

Die gesamte Ausdehnung des Netzes kann 6500 m betragen.

Bei Busvernetzung werden alle Rechner mit einem T-Stück verbunden, dass sich auf der Netz-Karte befinden muss. Das Buskabel darf bis zu 300 m lang sein, wobei bis zu 8 Rechner angeschlossen werden dürfen. Dafür müssen spezielle Netzwerkkarten verwendet werden (HZ-Karten). Die beiden Enden des Busses sind mit Terminatoren zu versehen.

2.1.7 Ethernet

Beim Ethernet wird unterschieden in:

- *Thick-Ethernet* und
- *Thin-Ethernet*

Thick-Ethernet:

- Übertragungsgeschwindigkeit 10 MBit/s (fällt bei Belastung schnell)
- Kollosionsverfahren
- Dickes, gelbes Koaxialkabel mit 50 Ohm, relativ starr, schwer zu verlegen, relativ hohe Kosten, weil viel Zubehör nötig ist

- Das Kabel ist allerdings unempfindlich gegen Störeinflüsse und ein Segment kann sehr lang sein.
- Es wird für die Bus-Topologie verwendet.
- Der Kabelstrang darf 500 m lang sein und muss an den Enden terminiert werden.
- Der Anschluss an die Rechner geschieht über Transceiver, die in das Kabel eingesetzt werden. Der Transceiver wird dann mit einem speziellen Transceiverkabel mit der Netzwerkkarte verbunden, das aber nicht länger als 50 m sein darf.
- Die meisten Ethernetkarten bieten einen DIX- und einen Thin-Ethernet-Anschluss. Die Anschlussart muss auf der Karte eingestellt werden.
- *Minimalste Distanz zwischen 2 Transceiver = 2.5 m oder ein Vielfaches davon.*
- In einem Segment dürfen 100 Transceiver vorhanden sein. Bei mehreren Rechnern auf engem Raum wird ein Multitransceiver benutzt, der an einen normalen Transceiver angeschlossen wird und 8 Ausgänge besitzt. Mehrere Segmente werden mit Transceivern verbunden. Auf diese Weise kann der BUS über 500 m hinaus verlängert werden.

Thin-Ethernet (Cheapernet):

- Übertragungsgeschwindigkeit 10 MBit/s (fällt bei Belastung schnell)
- Kollosionsverfahren
- Verwendet RG-58-A/U-Koaxial-Kabel, welches flexibel ist und erheblich leichter zu verlegen ist.
- Es verursacht geringe Kosten, ist allerdings störanfälliger wegen der geringeren Abschirmung. Cheapernet wird vor allem bei kleineren/mittleren Netzen (Büroumgebung) eingesetzt und wird busförmig aufgebaut.

- Die Segmentlänge kann 185 m betragen und muss terminiert werden.
- Der Rechner wird über ein T-Stück mit dem BUS verbunden, wobei das T-Stück direkt auf der Karte sitzen muss. Ein externer Transceiver ist nicht notwendig, da dieser schon auf der Karte integriert ist.
- *Der Abstand zwischen 2 Rechnern darf min. 0.5 m betragen.*
- An einem Segment können 30 Rechner angeschlossen werden. Zur Kopplung mehrerer Segmente werden die gleichen Elemente, wie beim Thick-Ethernet benutzt.
- Über spez. Adapter kann Thick- und Thin-Ethernet verbunden werden.
- Bei mehreren Segmenten muss ein Repeater benutzt werden.

Thin-Ethernet (Twisted Pair):

- Übertragungsgeschwindigkeit 10–100 MBit/s (fällt bei Belastung schnell)
- Kollosionsverfahren. Nur bei Einsatz von Switches können die vollen Bandbreiten erhalten werden.
- Es verwendet STP oder UTP-Kabel der Kategorie 1–5 (siehe 2.1.2 „Übertragungsmedien“) und verursacht auch noch geringe Kosten.
- Es ist logisch sternförmig aufgebaut. Bei Verwendung mit HUB’s allerdings physk. busförmig, da sich alle Rechner, die an einen HUB angeschlossen sind, die Bandbreite teilen müssen.
- Die Rechner werden über HUB’s oder Switches verbunden, die Repeaterfunktionen beinhalten.
- *Der Abstand zwischen 2 Rechnern darf min. 2.5 m betragen.*

2.1.8 Token-Ring

- Übertragungsgeschwindigkeit 4–16 MBit/s
- Token-Zugriffsverfahren.
- Es verwendet 7 verschiedene Kabeltypen.

Token-Ring ist eine Reihe ringförmig gekoppelter Sterne, die einen geschlossenen Ring ergeben. Wichtigster Bestandteil ist dabei die MAU (Multistation Access Unit). Diese hat 2–16 Anschlüsse für die Rechner und RING-IN- / RING-OUT-Anschlüsse, um mehrere MAUs zu verbinden.

Um einen Rechner an den Ring anzuschließen, wird eine Hin- und eine Rückleitung benötigt. Jeder Rechneranschluss in der MAU ist mit einem Relais versehen. Durch die Einbindung eines Rechners wird der Ring erweitert.

Fällt ein Rechner aus oder wird er vom Netz genommen, wird das Relais geschlossen, sodass der Ring nicht unterbrochen wird. Auch die Verbindung zu anderen MAUs hat 2 Leitungen, sodass ein Ausfall immer abgefangen werden kann.

Die Distanzen zwischen MAUs und Rechnern ist vom verwendeten Kabel abhängig.

Faustregeln:

Rechner $\rightarrow$ MAU = 50 m

MAU $\rightarrow$ MAU = 50 m

Mit entsprechenden Einheiten können die Distanzen erhöht werden.

2.1.9 Gigabit-Ethernet

Gigabit-Ethernet ist eine relativ neue Technologie, die sich in heutigen Netzwerken aber immer mehr durchsetzt, da immer höhere Anforderungen an Geschwindigkeiten im Netzwerk gestellt werden. Neuere Betriebssysteme und Anwendungen benötigen auch immer größere Bandbreiten, die die aufkommenden Datenmengen noch

bewältigen. In sehr großen Netzwerken ist ein reibungsloser Betrieb des Netzwerkes ohne eine entsprechende Backbone auch fast nicht mehr möglich. In diesem Zusammenhang macht Gigabit-Ethernet und ATM immer mehr von sich reden und ist in großen Netzwerken schon zum Standard geworden.

- Übertragungsgeschwindigkeit 1250 Mbit/s.
- Verwendet 3 verschiedene Kabeltypen wie, Twinax, Glasfaser, Twisted-Pair (noch kein Standard vorhanden). Der Kabeltyp bedingt bestimmte Segmentlängen.
- Kann für alle Ethernet-Technologien verwendet werden.
- Kann das herkömmliche Zugriffsverfahren des Ethernets (CSMA/CD) verwenden, welches in „geswitchten Umgebungen“ allerdings nicht mehr nötig ist.
- Kann 10, 100 oder 1000 Mbit verwenden.
- Verursacht hohe Kosten.
- Wird hauptsächlich im Backbone-Bereich verwendet,
- aber auch für schnelle Verbindungen von Switches zu Switches und Switches zu Servern.
- Kann im Vollduplex-Mode betrieben werden.

Kupferkabel (billiger, aber eher in Serverschränken und Serverräumen zu finden, wegen der geringen Längen)

Typ	Reichweite	Impedanz	Kabeltyp	Stecker
1000BaseCX	25 m	150 Ohm	Twinax	STP (DB9, Style 1)
1000BaseCX	25 m	150 Ohm	Twinax	IEC61076 (Style

				2)

Glasfaserkabel (für die Backbone-Verkabelung)

Typ, Faser	Bandbreite [MHz / km]	Segmentlänge	Kabeltyp	Stecker
1000BaseSX, 62,5µm	160	2–220 m	Multimode	Duplex SC
1000BaseSX ,62,5µm	200	2–275 m	Multimode	Duplex SC
1000BaseSX , 50µm	400	2–500 m	Multimode	Duplex SC
1000BaseSX, 50 µm	500	2–550 m	Multimode	Duplex SC
1000BaseLX, 62,5 µm	500	2–550 m	Multimode	Duplex SC
1000BaseLX, 50 µm	400	2–550 m	Multimode	Duplex SC
1000BaseLX, 50 µm	500	2–550 m	Multimode	Duplex SC
1000BaseLX, 10 µm		2–5000 m	Monomode	Duplex SC

2.1.10 ATM (Asynchronous Transfer Mode)

ATM ist für hohe Bandbreiten konzipiert und ist eine Technologie, die mit speziellen Geräten im Netzwerk verwendet wird. Während andere Technologien mit Zellen (Frames) von unterschiedlichen Längen arbeiten, baut ATM auf Zellen fester Länge (53 Byte) auf.

- Übertragungsraten zwischen 155 und 622 Mbit/s.
- Wird vornehmlich im Backbone-Bereich oder zur Übertragung von Sprache und Video eingesetzt, wobei der Übertragung von Audio/Video Vorrang im Netz eingeräumt wird.

- Die Kommunikation in ATM-Netzen verläuft über virtuelle Pfade.
- Bandbreiten können in beliebiger Höhe an WS's zugewiesen werden (Quality of Service, QoS).
- Bedingen ATM-kompatible Geräte im Netz wie ATM-Router, ATM-Switches, etc.
- Übertragen Daten nicht nach Ip- oder MAC-Adressen, sondern über spezielle 3 Byte große Identifikationen (Gerät-zu-Gerät-Verbindung).
- Kann im LAN sowie für WAN-Verbindungen eingesetzt werden

Fibre Channel siehe Abschnitt 1.2.10, BUS-Systeme, serielle BUS-Systeme.

2.1.11 Das OSI-Schichten-Modell (Open System Interconnection)

Um vielen herstellerspezifischen Eigenheiten im Bereich der Netzwerktechnik aus dem Weg zu gehen und ein einheitliches Modell für die Netzwerktechnik zu schaffen, wurde das OSI-Schichten-Modell entwickelt, welches bestimmte Vorgaben für die Kommunikation offener Systeme darlegt.

Das Modell ermöglicht Herstellern, ihre Produkte für den Netzwerkeinsatz aufeinander abzustimmen.

Schicht 1 Physical-Layer (Physikalische oder Bitübertragungsschicht)

Sie gibt die Informationen ins physikalische Netzwerk und empfängt Pakete oder Frames vom Netzwerk (senden und empfangen von Datenbits).

Hier werden sämtliche Spezifikationen festgelegt für:

- das Übertragungsmedium (Koaxkabel, Zweidraht, Glasfaser)

- das Übertragungsverfahren (Basisband, Breitband)
- die Topologie
- Codierung der Datenbits
- realisiert die physikalische Verbindung zwischen Computer und Netzwerk

Schicht 2 Data-Link (Verbindungsschicht oder Sicherungsschicht)

- Beinhaltet die Kommunikation von Geräten innerhalb eines Netzwerksegments.
- Zur Identifizierung von Datenpaketen werden MAC-Adressen verwendet und jedes Gerät ist dafür verantwortlich, das Netzwerk zu überwachen und diejenigen Rahmen zu empfangen, die für das Gerät selbst bestimmt sind.

Hier erfolgt die erste Bewertung der eingehenden Daten:

- Überprüfung auf korrekte Reihenfolge und Vollständigkeit der Pakete,
- Übertragungsfehler werden sofort erkannt,
- zudem werden hier die Knotenadressen (MAC) im Netz erkannt und ausgewertet,
- packt und entpackt Daten.

Schicht 3 Network-Layer (Netzwerkschicht oder Vermittlungsschicht)

- Bearbeitet die Kommunikation von Geräten auf logisch voneinander getrennten Netzwerken und verwendet dazu Routing-Algorithmen, die Pakete vom Sende- zum Zielnetzwerk weiterleiten.
- Unterstützt darüber hinaus Dienstadressen (Sockets oder Ports). Diese spezifiziert einen Kanal zu einem bestimmten Prozess auf einem Zielrechner. (Dienstadressen sind Bestandteil der MAC- und IP-Adresse)

- Hat den Überblick über Wegfindung und Paketzustellung im gesamten Netzwerksystem.
- Übernimmt die Verwaltung der Kommunikationspartner.
- Insbesondere werden die ankommenden bzw. abgehenden Datenpakete verwaltet, und zwar in der Form, dass Nachrichten von darüberliegenden Schichten in kleinere Datagramme fragmentiert werden, die in ihrer Größe für die physikalische Schicht geeignet sind.
- Außerdem trägt die Netzwerkschicht auch die Verantwortung für die Wiederherstellung von Nachrichten aus empfangenen Datagrammen.
- Eindeutige Zuordnung über die Vergabe der Netzwerkadressen (logische IP-Adressen)
- Fügt der Verbindung weitere Steuerinformationen hinzu.
- Realisiert das Routing der Daten durch das Netz (legt also die Route durchs Netzwerk fest, die Pakete über eine Serie von Routern vom Quell- zum Zielrechner nehmen).

Schicht 4 Transport-Layer (Transportschicht)

- Überträgt die Information in eine Sprache, die das andere System versteht.
- Sorgt für eine zuverlässige Zustellung von Nachrichten an die Zielgeräte.
- Fehlerkontrolle
  (wenn ein Paket verloren gegangen ist, muss die Transportschicht die Fehlerkorrektur initiieren)
- Festlegung der Reihenfolge von Paketen
- Ende zu Ende Flusskontrolle
- (Neben einer negativen Bestätigung für unvollkommene
  Übertragung von Daten kann die Transportschicht auch ein erneutes Senden anfordern.)

- Stellt die Verbindung zwischen den Schichten 1–3 und 5–7 her.
- Fügt Infos zur Adressierung und Ansprechen der Datenendgeräte hinzu.
- Baut die nötige Verbindung auf.
- Leitet die Datenpakete gemäß der Adressierung weiter.
- Realisiert die Weitergabe und die Bestätigung der Übertragung.

Schicht 5 Session-Layer (Sitzungs- oder Steuerungsschicht der Kommunikation)

- Stellt eine Methode zur Erzeugung und Aufrechterhaltung einer logischen Verbindung zwischen zwei Hosts zur Verfügung.
- Verwaltet die Dialoge zwischen 2 Computern (Simplex, Halbduplex, Vollduplex).
- Festlegen des Verbindungsaufbaus (Sitzungsaufbau, Datentransfer, Sitzungsabbau).
- Eine Sitzung besteht aus:

1. Festlegung der benötigten Dienste
2. Benutzeranmeldung und andere Sicherheitsprozeduren
3. Aushandlung von Protokollen und Protokollparametern
4. Mitteilung von Sitzungsnummern
5. Einrichten einer Dialogkontrolle

Schicht 6 Presentation-Layer (Darstellungschicht)

- Erzeugt im Falle von WIN-NT den SMB-Block, der dem anderen System mitteilt, was angefordert ist, oder erhält die Antwort auf eine Anfrage.
  Hier wird auch die Typenkonvertierung behan-

delt, wenn kommunizierende Hosts unterschiedlich sind.

- Erledigt die Datenkonvertierung,
- stellt sicher, dass die Daten in einem universellen Format übertragen werden,
- Möglichkeiten der Datenein- bzw. -ausgabe werden bereitgestellt,
- dazu gehört Anzeige von Meldungen und Anweisungen,
- Datenein- und -ausgabe wird überwacht,
- Übertragungskonvertionen werden festgelegt,
- Bildschirmdarstellungen werden angepasst,
- Umsetzung der Bit-Reihenfolge.

Schichten 1-3 = systembezogen
Schichten 5-7 = anwendungsbezogen

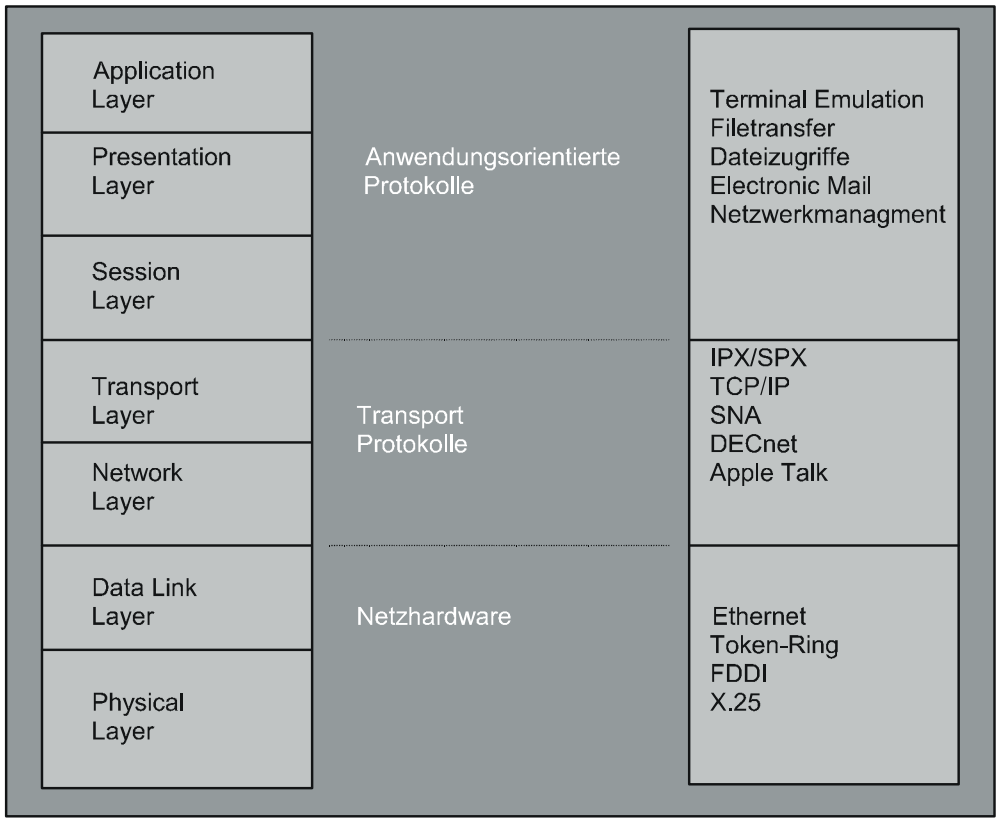


Abb. 8 OSI-Schichten

- Übersetzung der Byte-Reihenfolge
- Übersetzung des Zeichensatzes
- Übersetzung der Dateisyntax

Schicht 7 Application-Layer (Anwendungsschicht)

Erzeugt Anfragen und verarbeitet Anfragen, die sie erhält.

- Eerste Schnittstelle zwischen Rechner und Anwendungsprogramm,

- hier werden die verwendeten Anwendungen eingesetzt,
- liefert dem Netzwerk Dienste (Datei-, Drucker-, E-Mail-, Datenbankdienste).

2.1.12 Übertragungs-Protokolle (im LAN-Bereich)

Der Sinn eines Netzwerkes ist der Austausch von Informationen und Daten zwischen verbundenen Computern. Dabei ist wichtig, dass die Computer die gleichen Kommunikationsregeln verwenden, dass sie sozusagen die gleiche Sprache sprechen, um einander zu verstehen.

Diese Kommunikationsregeln werden über die Protokolle definiert.

NetBIOS:

- Erstes Übertragungsprotokoll im LAN, aber auch BIOS-Erweiterung für das Netzwerk,
- wird heute nur noch für spezielle Anwendungen eingesetzt (NT benutzt NetBIOS over TCP/IP = NBT),
- einige Betriebssysteme, wie DOS, NETWARE beinhalten
  Emulationsprogramme (Netbios.exe), mit denen man Software, die auf NetBIOS aufsetzt, aktivieren kann.

NetBEUI:

- Weiterentwicklung von NetBIOS,
- ist ein aus NetBIOS entwickeltes Transport-Protokoll, welches quasi Standard für alle WINDOWS Betriebssysteme ist (nicht routingfähiges Protokoll).

Apple Talk:

- Protokoll für McIntosh-Rechner
- FRAME unter Netware _SNAP

IPX/SPX:

- Von Novell entwickelt,
- zweitwichtigstes Protokoll heutiger Netzwerke,
- wird grundsätzlich auf alle NETWARE-Anwendungen implementiert,
- IPX adressiert und verschickt Datenpakete,
- SPX übernimmt die Kontrolle der Übertragung.

Zusatzprotokolle zu IPX/SPX (RIP und SAP):

RIP (auch in TCP / IP Netzen verwendet, siehe 3.2.32 „NT als TCP/IP-Router“)

Verschickt innerhalb eines LANs Angaben über verfügbare Router, Server und Workstations.

Router gleichen über RIP auch ihre Routing-Tabellen (dem Router bekannte Subnets und Hops (Anzahl der Sprünge über andere Router bis zum Remote-Netzwerk)) ab. Dabei werden nur 16 Hops gespeichert, d.h. Router kennen nur Subnets, die nicht weiter als 16 Hops entfernt sind (im LAN meistens ausreichend, im Internet problematisch, da jeder Router seine Tabellen per Rundsendung verschickt und jeder Router, der diese empfängt, dies genauso tut (schnelle Überlastung der Router)).

SAP

Dient dazu, dass ein Server den anderen Komponenten im Netz seine Dienste (Services) bekannt machen und zur Verfügung stellen kann

TCP/IP:

- Standard-Protokoll in LANs (wird am meisten eingesetzt),
- verbindungsorientiertes Protokoll,
- TCP übernimmt die Übertragung der Daten zwischen zwei Endgeräten,

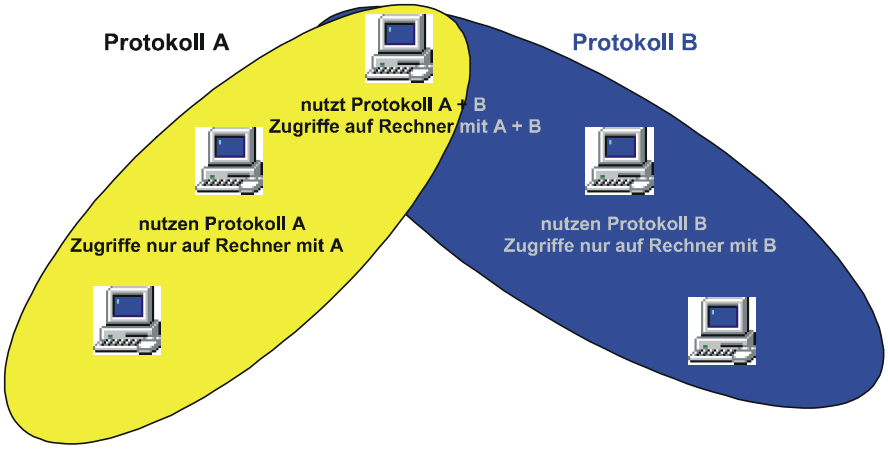


Abb. 9 Multiprotokoll-Umgebung

- vor der Übertragung werden Daten in Datenpakete zusammengefasst,
- IP übernimmt die Adressierung, das Versenden und die Überwachung des Transports der einzelnen Datenpakete.

Zusatz-Protokolle zu TCP/IP:

siehe weiter unten bei TCP / IP

2.1.13 TCP/IP Grundlagen

- Standard-Protokoll für das Internet,
- verbindungsloses Protokoll (Paket wird abgeschickt, ohne Rückmeldung → nur bei udp),
- eindeutige Adresse im Netz (IP-Adresse),
- diverse Hilfsprotokolle (DNS, DHCP, SMTP).

Eindeutige IP-Netzwerk-Adressen sind weltweit Mangelware (können aber angefordert werden) und werden nur benötigt, wenn das eigene Netzwerk direkt mit dem Internet verbunden ist. In einem privaten / geschäftlichen LAN können IP-Adressen aber wahllos vergeben werden, wenn mit einer Firewall oder einem Proxy-Server zum In-

ternet gearbeitet wird, welcher die eindeutige IP-Adresse zum Internet erhält und das LAN vom Internet abschirmt. Das eigene LAN sollte in seinem IP-Aufbau aber trotzdem den Konventionen entsprechen.

Form und Art von IP-Adressen:

IP erfordert, dass jedem Gerät im Netz ein Adresse zugeordnet wird, die IP-Adresse. Sie ist dargestellt durch eine Sequenz von vier Oktetten. Diese Oktetten definieren eine eindeutige Adresse, wobei ein Teil dieser Adresse ein Netzwerk darstellt (und optional ein Teilnetz), ein anderer Teil einen bestimmten Knoten (Rechner) im Netz.

Beispiel (N = Network, H = Host):

NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH =
Klasse-A Netz, Subnet-Mask 255.0.0.0

NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH =
Klasse-B Netz, Subnet-Mask 255.255.0.0

NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH =
Klasse-C Netz, Subnet-Mask 255.255.255.0

Jede Position stellt ein einzelnes Bit aus einem 32-Bit-Adress-Raum dar.

Für die IP-Adresse 160.16.45.3 =
10100000.00010000.00101101.00000011

Es gibt Adressen, die eine bestimmte Bedeutung haben und deswegen nicht benutzt werden dürfen:

Eine Adresse, die mit einer 0 beginnt, bezieht sich auf einen lokalen Knoten:

0.0.0.23 = WS mit Nummer 23 (außerdem im Routing als Defaultroute festgelegt),

127 = Loopback-Adresse (wichtig für Netzdiagnose),

127.0.0.0 ist der lokale Loopback innerhalb der WS,

255 = reserviert für Meldungen (Broadcast).

Adressklassen

Klas-se	verfügbare Knoten	Aus-gangs-Bits	Start-adresse	Verwendung
A	2E24 = 16777216	1xxx	1–126	sehr große Netze
B	2E16 = 65536	10xx	128–191	256-65536 Knoten
C	2E8 = 256	110x	192–223	bis 256 Knoten
D		1110	224–239	Multicast Nachrichten
E		1111	240–255	zukünftige Entwicklung

Zum besseren Verständnis:

Die Subnet-Mask bestimmt, welcher Teil der IP-Adresse Netzwerkanteil und welcher Hostanteil ist. Dabei sind alle Anteile der IP-Adresse, die Einsen in der Subnet-Mask enthält (Dezimal 255), Netzwerkadresse.

Beispiel:

Klasse C IP-Adresse:
192.168.100.7
Klasse C Subnet-Mask:
255.255.255.0
Klasse C Netz-Adresse:
192.168.100.0

Klasse B IP-Adresse:
128.107.100.3
Klasse B Subnet-Mask:
255.255.0.0
Klasse B Netzadresse:
128.107.0.0

usw.

Weiter wird vom Computer über die Subnet-Mask ermittelt, ob sich ein Host im gleichen Subnet befindet oder ob dieser in einem anderen Teil-netz untergebracht ist. Am besten wird dies durch die Aufschlüsselung der IP-Adressen in deren Binärwerte klar und durch das Verständ-

nis, welche Rechenoperationen (AND-Verknüpfung) der Computer mit diesen Binärwerten anstellt. Da dieses Buch nicht Gegenstand von binären Rechenoperationen ist, soll hier nur kurz auf die AND-Verknüpfung eingegangen werden.

Definition: 1=High (an), 0=Low (aus)
AND-Verknüpfung: 1+1=1, 1+0=0, 0+1=0, 0+0=0

Die IP-Adresse wird in deren Binärwert mit dem Binärwert der Subnet-Mask AND-Verknüpft. Dabei wird die Rechenoperation auf jede Stelle der Binärwerte angewendet.

Zwei Hosts in selben Subnet:

1. Host	IP-Adresse	dazugehöriger Binärwert der Oktette			
	198.53.147.45	11000110	00110101	10010011	00101101 Rechenweg
	Subnet-Mask				↓
	255.255.255.0	11111111	11111111	11111111	00000000
AND-Verknüpfung Ergebnis		11000110	00110101	10010011	00000000 = 198.53.147.0
2. Host	198.53.147.98	11000110	00110101	10010011	01100010
	255.255.255.0	11111111	11111111	11111111	00000000
AND-Verknüpfung Ergebnis		11000110	00110101	10010011	00000000 = 198.53.147.0

Die Netzwerk-Ids stimmen in beiden Fällen überein, so dass sicher gestellt ist, dass sich beide Hosts im selben Subnet befinden.

Zwei Hosts in unterschiedlichen Subnets:

1.Host	IP-Adresse	dazugehöriger Binärwert der Oktette			
	198.53.147.45	11000110	00110101	10010011	00101101
	Subnet-Mask				
	255.255.255.0	11111111	11111111	11111111	00000000
AND-Verknüpfung Ergebnis		11000110	00110101	10010011	00000000 = 198.53.147.0
2. Host	131.107.2.200	10000011	01101101	00000010	11001000
	255.255.255.0	11111111	11111111	11111111	00000000
AND-Verknüpfung Ergebnis		10000011	01101101	00000010	00000000 = 131.107.2.0

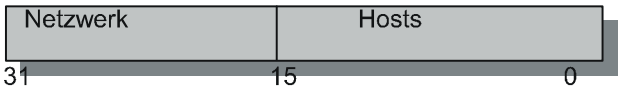
Die Netzwerk-Ids stimmen in beiden Fällen nicht überein, so dass sicher gestellt ist, dass sich beide Hosts nicht im selben Subnet befinden.

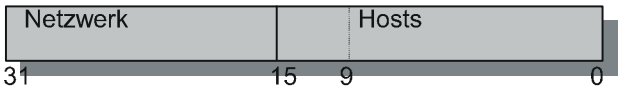
Teil-Netze:

Die Einrichtung einer Teil-Netz-Maske legt fest, wo die Netz-Adresse endet und die Host-Adresse anfängt.

Die Teilnetz-Maske enthält Einsen im Netzwerkfeld und Nullen im Host-Feld.

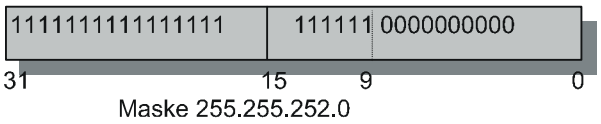
Wird das Klasse-C Netz in vier Klasse-C Netze zerlegt, sieht das so aus:
NNNNNNNN.NNNNNNNN.NNNNNNNN.NNHHHHHH





Anzahl der Teil-Netze = 64
Anzahl der Hosts/Netze = 1024

Teilnetz-Maskierung (Subnet-Mask):



Die Teilnetz-Maske:

11111111.11111111.11111111.11000000
in Dezimalschreibweise: 255.255.255.192

Wenn aus dem Hostfeld drei Bits entfernt werden, können 8 Netzwerke gebildet werden:

11111111.11111111.11111111.11100000,
die Teilnetz-Maske ist: 255.255.255.224

Jedes der 8 Netzwerke hätte damit 29 Knoten, weil 5 Adressbits zur Verfügung stehen (es sind eigentlich 32, aber 1, 0 und 127 sind verbo-

ten). Dieses Konzept gilt auch für Klasse B-Netze.

Der Adressbereich eines Klass-B-Netzes:
NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Wenn 2 Bits aus dem Hostfeld entfernt werden und dem Netzfeld hinzugefügt werden, wird folgende Teilnetz-Maske verwendet:

11111111.11111111.11000000.00000000
Die Maske lautet: 255.255.192.0

Die IP-Adresse dient nur der eindeutigen Identifizierung eines Gerätes im Netz. IP-Pakete werden aber letztlich immer an die MAC-Adresse der Netzkarte geschickt (siehe 1.2.16 „Netzwerkkarte“). Dazu wird ein ARP-Cache (siehe Hilfsprotokolle TCP/IP) verwendet, in dem schon verwendete Verbindungen von IP-Adressen zu MAC-Adressen aufgelöst werden. Ist die MAC-Adresse der angesprochenen IP-Adresse nicht bekannt, werden Rundsendungen von ARP verschickt, um diese herauszufinden.

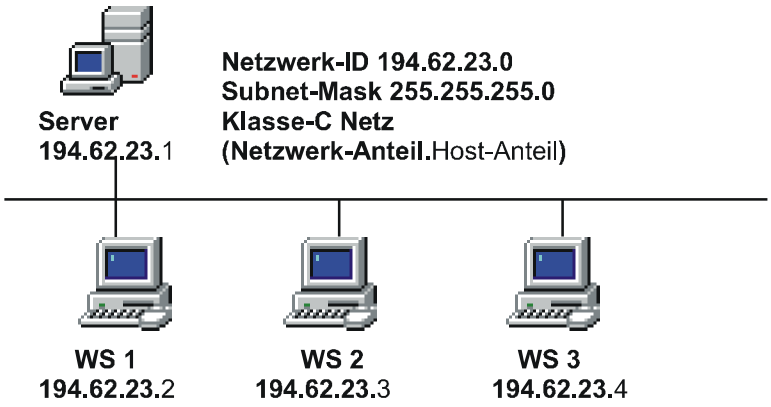


Abb. 10 Einfaches TCP/IP-Netzwerk

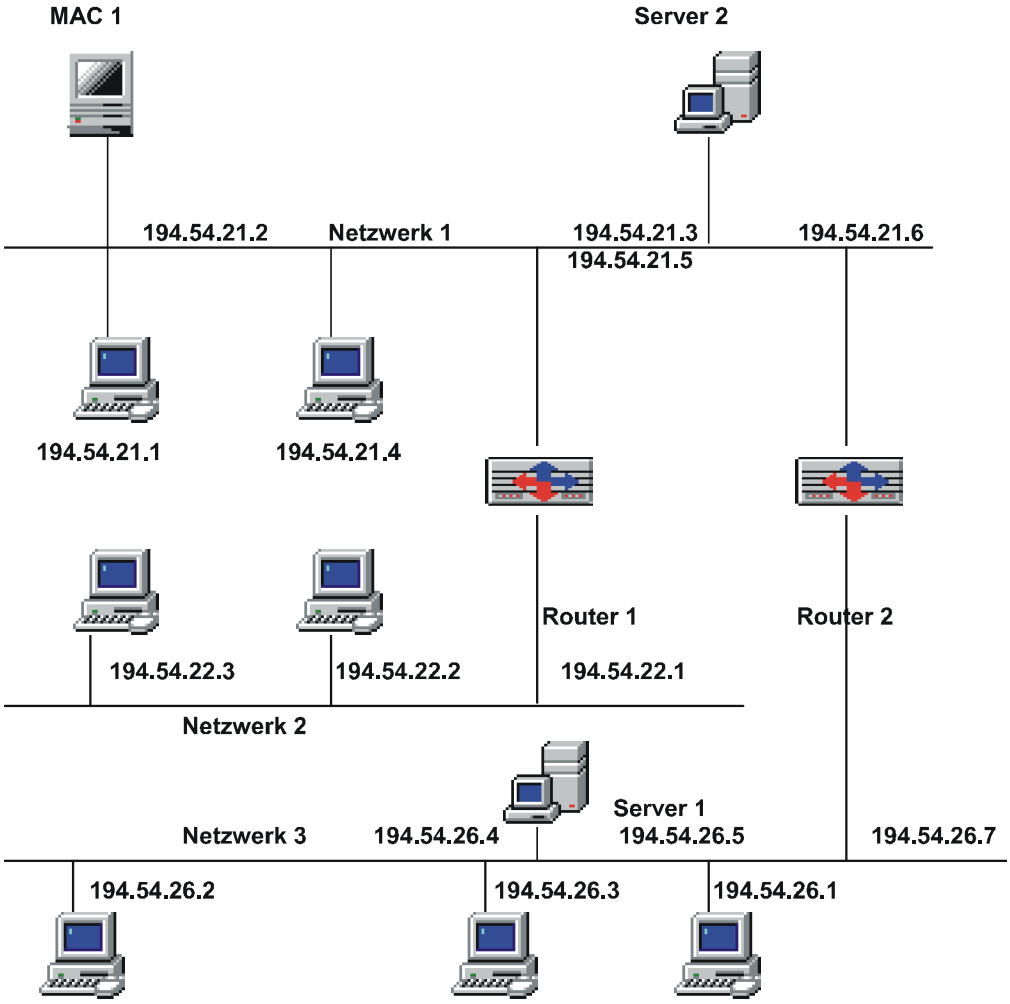


Abb. 11 Komplexes TCP/IP-Netzwerk

Sollen Pakete verschickt werden, baut TCP zuerst eine Sitzung vom eigenen Computer zum Remote-Host auf. Der Remote-Host bestätigt die Anfrage und signalisiert, dass er zur Entgegennahme von Paketen bereit ist (Handshake). IP verpackt nun die TCP-Pakete und schickt sie un-

ter Verwendung des ARP-Caches an die Remote-Adresse.

Hilfsprotokolle zu TCP/IP:
DNS (Domain Name System)

Das DNS wandelt IP-Adressen in Domänen-Namen ,
z.B. 192.125.12.5 → einstein.ege.de.

(Für eine Verbindung zu einem anderen Rechner muss nicht mehr die IP-Adresse eingegeben werden, sondern es reicht jetzt auch der Computer-Name (siehe 3.2.27 „DNS“)

SMTP (Simple-Mail-Transfer-Protokoll)

Wird vornehmlich für die Übermittlung elektronischer Post an einzelne Benutzer oder alle benutzt.

POP

Wird für eingehende Post aus dem Internet verwendet (Post empfangen).

FTP (File-Transfer-Protokoll)

Wird für die Übertragung von Daten zwischen verschiedenen Rechner-Systemen benutzt, die unterschiedliche Dateiformate benutzen.

Zusätzlich zu den Befehlen für die Dateiübertragung gibt es Befehle zum Anzeigen, Wechseln, Löschen oder Anlegen von Verzeichnissen.

TELNET (Terminal-Emulation)

Stellt eine Verbindung zwischen einem Telnet-Server und Telnet-Client her, wobei auf dem Client ein Terminal des Servers emuliert wird.

NFS (Network File-System)

Verzeichnis eines Rechners kann über das Netz direkt an einen anderen Rechner angeschlossen werden.

RPC (Remote-Procedur-Call)

Erlaubt das Kommunizieren verschiedener Applikationen untereinander.

ARP (Address-Resolution-Protokoll)

Führt die logischen IP-Adressen der Rechner mit ihren physikalischen Adressen (MAC-Adressen) der Netzwerkkarten zusammen (unter NT ein Befehl, um den ARP-Cache abzufragen).

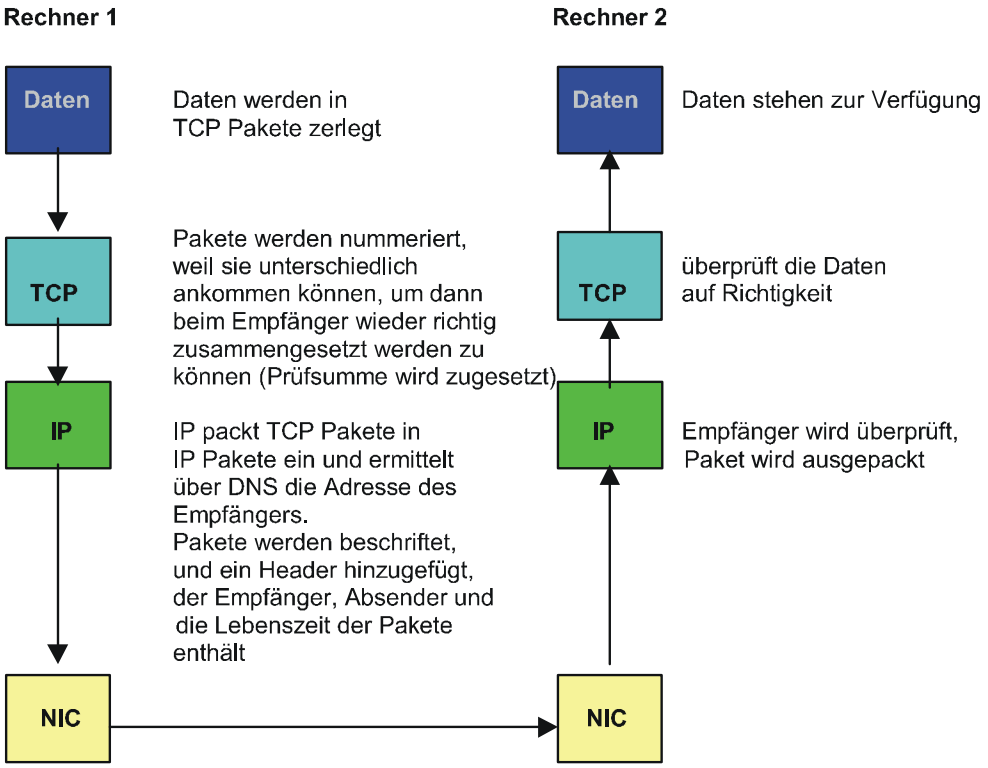


Abb. 12 Übertragung der Daten unter TCP/IP

ICMP (Internet-Controll-Massage-Protokoll)

Protokoll, mit dem Nachrichten über den IP-Zustand verschickt werden.

SNMP (Simple-Network-Management-Protokoll)

Zur Steuerung und Überwachung von Netzwerken.

UDP

Verbindungsloses Übertragungsprotokoll, wenn zuverlässige Datenübertragung nicht nötig ist.

2.1.14 Geräte im Netzwerk

Server:

Ein in das Netz eingebundener Rechner, der mit der Ausführung spezieller Aufgaben betraut ist. Unterscheidung in DEDICATED (Rechner, der nur dafür abgestellt ist) und NON DEDICATED (Rechner, der auch weiterhin im Normalbetrieb arbeitet).

Server können als File-, Print-, Fax- oder Datenbank-Server arbeiten. Mehrere Aufgaben in einem Server sind möglich.

File-, Print-, Datenbank- etc. Server (Zentral-Rechner):

Rechner, der die Daten / Ressourcen des Netzwerks zentral speichert und verwaltet.

Er sorgt für die kontrollierte Bereitstellung von gemeinsam benutzten Daten. Weiterhin wickelt er die Kommunikation zwischen den Benutzern im Netz ab.

Netzwerkdienste können auch auf mehrere Server verteilt sein.

Als Server muss ein Rechner eingesetzt werden, der von seiner Konfiguration auch die Aufgaben eines Servers erfüllen kann.

Netzwerk-Betriebssystem:

Als Herz des Netzwerkes arbeitet der Server mit einem speziellen Netzwerkbetriebssystem (Novell, Unix, Windows NT)

Workstations (Client):

Rechner, der in das Netz eingebunden ist, einem Benutzer an seinem Arbeitsplatz zur Verfügung steht und vom Server Dienste beanspruchen kann.

Hardware-Verbindung:

Alle Server und Workstations müssen unter einer bestimmten Topologie miteinander verbunden sein. In jedem Rechner muss eine Netzwerkkarte vorhanden sein, die durch die Übertragungsmedien und Verteiler miteinander verbunden sind.

Repeater (OSI 1, phys. Layer):

- Signalformer (Verstärker), um Signale, auf Grund der Ausdehnungsbeschränkung von Segmenten (Thin-Ethernet 185 m, Thick 500 m) zu überbrücken,
- aktives Element,
- protokoll-transparent,
- erhöht nicht die Bandbreite eines Segments,
- auch Sternverteiler (HUB’s) und Ringverteiler gehören hierzu,
- unterschiedliche Netzsegmente können damit zu einem Netz zusammengefügt werden,
- mit Repeatern sind baumartig gestaltete Netzwerke von beachtlicher Ausdehnung realisierbar,
- filtert keine Adressen, reicht also Pakete in alle Segmente weiter,
- werden immer weniger eingesetzt und mehr und mehr von Bridges und Routern abgelöst.

Transceiver:

Wandlungs- (D/A-Wandlung) und Steuerungsaufgaben beim Senden und Empfangen.

Bridge (OSI 2, Data Link Layer):

- Dient einerseits der phys. Entkopplung großer Netze, andererseits der Verbindung glei-

cher lokaler Netze oder Netz-Segmente über Stationsadressen, die in einer Bridge-Tabelle gespeichert sind.

- Diese Tabellen können bei „Learning Bridges“ selbstständig von der Brücke aufgebaut werden (Brücke konfiguriert sich selber, Plug and Play).
- Mittels Bridges lassen sich LANs praktisch unbegrenzt ausdehnen,
- aktives Element,
- protokoll-transparent, wenn Bauform „Transparente Brücke“ ist (egal welches), muss aber auf beiden Seiten mit dem gleichen Protokoll arbeiten,
- verstärkt auch Signale,
- kann verschiedene Zugriffsverfahren koppeln,
- kann verschiedene physikalische Medien (Koax-UTP) verbinden,
- unterschiedliche Segmente werden zu einem Netz zusammengefasst,
- je nach Bauform werden Adressen gefiltert und interpretiert (es gibt aber auch solche, die Adressen nicht filtern, also Pakete werden in alle Segmente geleitet). Werden Adressen in Datenpaketen interpretiert, werden diese Pakete nur in das entsprechende Segment verschickt (Routingfunktion) und dadurch eine Lasttrennung (kein Datenverkehr in den anderen Segmenten durch dieses Paket) des Netzes erreicht.
- Kann nur MAC Hardware-Adressen (Knotenadressen) verarbeiten, mit denen die Bridge-Tabellen aufgebaut werden (jedes Netz separate Tabelle), wodurch Bridges in der Lage sind, zwischen dem Verkehr innerhalb eines Netzes und eines anderen Netzes zu unterscheiden,
- erhöhen die Gesamtbandbreite des gesamten LANs,

- eingehende Pakete werden aufbereitet,
- es gibt Source-Routing-Bridges (werden oft schon zu den Routern gezählt), die auf Grund der im Paket enthaltenen Informationen ein begrenztes Routing durchführen können,
- Bridges und Backbones gehören zusammen,
- kann Remote (Remote-Bridge) eingesetzt werden (also über Stand-Telefonleitung ein weit entferntes LAN verbinden) oder local (Local-Bridge) = Multi-Port-Bridge.

Router (OSI 3, Network Layer):

- Verbindet zwei gleiche oder unterschiedliche Netzwerk-Topologien miteinander, jedoch nur mit gleichen Protokollen,
- verbindet auch unterschiedliche Zugriffsverfahren,
- sucht den besten oder schnellsten Weg durchs Netz in andere Subnets, da sie Routing-Tabellen (Informationen über vorhandene Subnets) unterhalten und austauschen (siehe „Protokolle“ RIP),
- kann bei Ausfall oder starker Belastung einer Strecke selbstständig eine andere Route durch ein Maschennetz aussuchen,
- verbindet zwar Netzsegmente, jedoch bleibt jedes Segment für sich als separates Segment erhalten,
- ist von dem eingesetzten Protokoll auf Ebene 3 abhängig (also entweder Multiprotokoll-Router verwenden oder gezielt den Router für ein bestimmtes Protokoll (muss das Protokoll kennen)),
- besteht aus Hard- und Software-Anteil,
- übersetzt keine Protokolle,
- verstärkt auch Signale,

- interpretiert im Gegensatz zur Bridge die Pakete. Dabei wird jedes IP-Paket, das entgegen genommen wurde, ausgepackt und die im Header des Pakets enthaltene IP-Adresse interpretiert.
- Nachteil: Bei viel Netzwerkverkehr schnelle Überlastung des Routers, und IP-Pakete sind lange unterwegs.
- Arbeitet nicht mit MAC-Adressen (IP-Adresse genügt), übermittelt aber auch über MAC, wenn sie das Paket nicht interpretieren kann, wobei allerdings die Routing-Funktion verloren geht,
- filtert Adressen und leitet Pakete nur in Segmente (Subnets) mit den entsprechenden Adressen, wobei nicht die Adressen der Endgeräte wie bei der Bridge, sondern nur die Adressen der beteiligten Netzwerke (Routing-Tabellen) angelegt werden,
- die Filterfunktion erlaubt erhöhte Sicherheit, da sich Router so konfigurieren lassen, dass ein Zugriff auf ein Teil-LAN nur bestimmten IP-Adressen erlaubt werden kann (Firewall).

Gateway (OSI 7, Application Layer):

- Kann völlig verschiedene Kommunikationssysteme verbinden,
- ermöglicht die Entkopplung von LANs mit unterschiedlicher Adressierung,
- Gateways lassen sich auch über Software realisieren (IPX-IP Gateway auf Novell-Servern),
- setzen Protokolle real in andere Protokolle um,
- sie werden auch für den Übergang auf Großrechenanlagen benutzt.

Segment:

Zusammenhängendes Kabelstück innerhalb eines LANs. LANs können wiederum aus mehreren Segmenten bestehen, die über Repeater, Bridges oder Router verbunden sind.

HUB (OSI 1, phys. Layer):

- Zentraler Verteiler, an den sternförmig PC's angeschlossen werden,
- aktiv (Kabellänge bis 600 m), verstärkt auch Signale,
- passiv (Kabellänge bis 30 m),
- werden in Baum-Topologien verwendet,
- bedingen UTP-Kabel,
- die Buchsen eines HUB's sind so belegt, dass immer ein Endgerät angeschlossen werden kann.
- Werden 2 HUB's miteinander verbunden (kaskadiert), muss ein gekreuztes Kabel (crossover) verwendet werden (oder der Anschluss am HUB muss einen Schalter zum Kreuzen haben ,(Transmit → Receive, meistens Anschluss 1).

Switch (OSI2, Data Link Layer):

- Kann anstatt HUB's (bei Ethernet-Switch) oder anstatt Router verwendet werden (Abb. 15),
- sollte nur bei größerem Datenaufkommen eingesetzt werden,
- erhöht die Bandbreite in einzelnen Segmenten,
- Verbindungen werden direkt geschaltet (nach MAC-Adressen), Interpretation der IP-Adresse entfällt,
- trennt Netze physikalisch.

Fazit zu Netzwerkgeräten (Routing contra Switching):

Umso mehr Computer in einem Netzsegment vorhanden sind, desto geringer wird die Bandbreite, da sich damit das Datenaufkommen erhöht. Computer, die viel miteinander kommunizieren, sollten deswegen im selben Segment liegen, um den Netzwerkverkehr gering zu halten.

Über Bridges ist es unmöglich, Datenkommunikation zu Segmenten zu betreiben, die nicht direkt an die Bridge angeschlossen sind, sondern durch mehrere Netze getrennt sind. Dafür gibt es Router, die diese Aufgabe erfüllen können. Reine auf Router basierende Netzwerke können heutige Anforderungen an Datendurchsatzraten für neuere Anwendungen aber nicht mehr gänzlich allein erfüllen. Multi-Protokoll über ATM oder IP-Switching sind in einem modernen LAN deswegen mehr und mehr unausweichlich.

Über Router kann der Datenverkehr geregelt werden. Router können darüber entscheiden, welcher Datenverkehr von/zu Domänen fließen darf. Unter TCP/IP müssen Daten aus einem Anwenderprogramm in IP-Datagramme und z. B. im Ethernet weiter in Ethernet-Frames zerlegt werden, die dann als Bitstrom in das Kabel gelangen. Wenn sich beide Teilnehmer einer Kommunikation in der gleichen Domäne befinden, wird über die MAC- und IP-Adresse der Datenverkehr vorgenommen. Befinden sich die Teilnehmer in unterschiedlichen Domänen, muss die Kommunikation über Router stattfinden, wobei nur die IP-Adresse für den anderen Teilnehmer verwendet wird. Über die MAC-Adresse wird nur der nächste Router angesprochen, wobei jeder Router die Frames zuerst zwischenspeichern muss, sie zu IP-Datagrammen zusammen setzen muss, um anhand der IP-Zieladresse im Header (sozusagen ein Briefkopf) festzustellen, über welchen seiner Ports er das Zielgerät erreichen kann. Dazu verfügt der Router über Routing- und Adress-Tabellen, die über Routing-Protokolle aufgebaut wurden. Sodann werden die IP-Datagramme wieder in MAC-Frames zerlegt, mit einer neuen MAC-Zieladresse verse-

hen und über den entsprechenden Port gesendet. Dies passiert bei allen Routern auf dem Weg zum Zielgerät, was natürlich entsprechend viel Zeit benötigt, bis die Datagramme beim Zielgerät eintreffen. Weiter muss der Router über die Routing-Protokolle (RIP, OSPF, etc.) seine Tabellen aktualisieren, Protokolle konvertieren (z.B. von Ethernet zu Frame-Relay, wenn er auch als WAN-Router arbeitet). All dies benötigt zusätzlich viel Hard- und Software auf einem Router (also teuer).

Switching dagegen hat diese Nachteile nicht. Switches können anstatt HUB’s (Port-Switching) oder Routern (Segment-Switching) eingesetzt werden. HUB’s senden alle ankommenden Signale grundsätzlich auf allen Ports wieder aus. D. h., dass wegen dem CSMA/CD-Zugriffsverfahren von Ethernet alle angeschlossenen Geräte in einer Kollosionsdomäne liegen. Switches leiten ankommende Signale nur auf dem Port wieder aus, auf dem das Gerät sich befindet, für das die Nachricht bestimmt ist. Kollosionen auf den anderen Ports entfallen. Switches legen jedes angeschlossene Gerät sozusagen in ein eigenes Segment. Damit wird die Bandbreite des Netzes erhöht.

ATM-Switches z. B. arbeiten mit Zellen (Frames) von festen Längen, wobei nur die Adressinformationen aus dem ATM-Header gelesen werden muss und anhand von Hardwareentscheidungen (MAC-Adresse) der zu verwendende Switch-Port zur Weiterleitung festgestellt werden muss (Cut-Through-Prinzip). Route-Server werden dabei so eingesetzt, dass die Funktion zur Bildung von Domänen im Netzwerk für alle Switches erhalten bleibt. Ein Route-Server bildet dabei die Intelligenz des Switch-Konzeptes, während die Switches nur Daten weiterleiten, was sie sehr viel schneller in diesem Bereich machen als Router. Ein weiterer Vorteil ist, dass Domänen nicht mehr nach ihren physikalischen Bedingungen (Sub-Netze als Segment) gebildet werden

müssen, sondern virtualisiert werden können (sog. virtuelle LANs (VLANs)). ATM bedingt allerdings ATM-fähige Geräte im Netz. Multi-Protocol Over ATM (MPOA) oder Classical IP können aber eine LAN-Emulation herstellen, mittels derer auch herkömmliche LANs über ATM arbeiten können.

ATM-Switches leiten Datagramme also nicht nach IP-Adressen weiter, sondern nach einer völlig inkompatiblen Adressbildung zu IP. Neuere Technologien sollen aber IP-Adressen mit Switches verarbeiten können, um die vielen Vorteile des IP-Protokolls im LAN beibehalten zu können. Dabei wird einem IP-Datenstrom eine Marke zugewiesen, die auf eine Zeile in der Adresstabelle des ATM-Switches verweist. Dadurch kann der IP-Datenstrom nun die Datenpfade der Switches verfolgen, anstatt auf den Routing-Wegen zu bleiben, was das Weiterreichen der IP-Datagramme wesentlich beschleunigt.

2.1.15 Strukturierte Verkabelung in der Netzwerk-Technologie

Jede strukturierte Verkabelung setzt sich aus 3 getrennten Verkabelungsbereichen zusammen:

1. Primär-Verkabelung (gebäudeübergreifende Verkabelung):

Hier hinein fallen alle Kabelwege mit den dazugehörigen Verbindungen, die sich zwischen Gebäuden oder unterschiedlichen Betriebsstätten befindet. Sie endet in der Regel im Keller eines Gebäudes.

Der Primär-Bereich ist das Bindeglied zwischen den einzelnen Sekundär-Bereichen.

Elemente

- Primär-Verkabelung (Campus Backbone Cabling)
- Standortverteiler

- Rangierverteiler im Standortverteiler

2. Sekundär-Verkabelung:

Vom Keller hinauf in die einzelnen Etagen erfolgt die Sekundär-Verkabelung.

Der Gebäudeverteiler ist der Übergang zum Primärbereich.

Elemente

- Gebäudeverteiler
- Sekundär-Verkabelung
- Rangiereinrichtung im Gebäudeverteiler

3. Tertiär-Verkabelung:

Die Verkabelung auf den einzelnen Etagen wird als Tertiär-Verkabelung bezeichnet.

Der Etagenverteiler ist der Übergang zum Sekundärbereich.

Elemente

- Etagenverteiler
- Tertiär-Verkabelung
- Kabelverzweiger
- Anschlussdose
- Anschlusskabel
- Rangierfeld
- Rangierkabel

Backbone-Bereich:

Als Besonderheit innerhalb einer strukturierten Verkabelung zählt der Backbone-Bereich.

Mit Backbone-Bereich wird grundsätzlich der Teil der Kabel-Infrastruktur bezeichnet, der als verbindendes Glied der einzelnen Gebäude-Segmente liegt.

Bei großen Netzwerken mit einer gewissen Anzahl von Segmenten innerhalb verschiedener Gebäude werden für die Verbindung der einzelnen Teilbereiche schnelle Verbindungen benötigt (100–600 MBit/s).

Der Backbone-Bereich kann einen der folgenden Bereiche der Verkabelung betreffen:

- Primär- und kompletter Sekundär-Bereich
- Primärbereich und einige Sekundär-Bereiche
- ausschließlich Primär-Bereich

2.1.16 Strukturvorgaben

Ein strukturiertes Verkabelungssystem muss folgende Vorgaben enthalten:

1. Standortverteiler SV (Primärbereich)
2. Gebäudeverteiler GV (Sekundärbereich)
3. Etagenverteiler EV (Tertiärbereich)
4. Kabelverzweiger KV
5. Informationstechnische Anschlussdose TA

Primär-Verkabelung:

Die Primär-Verkabelung erstreckt sich grundsätzlich vom Standortverteiler bis zum Gebäudeverteiler. Mit ihr erfolgt die Anbindung verschiedener Gebäude. Hier wird im Allgemeinen ein Glasfaserkabel verwendet.

Es sind aber auch Ausnahmen zugelassen, bei denen ein symmetrisches Kupferkabel zum Einsatz kommt.

Sekundär-Verkabelung:

Die Sekundär-Verkabelung bezieht sich auf den Bereich der Gebäude- und Etagenverteiler. Grundsätzlich dürfen hier keine Kabelverzweiger verwendet werden. Auch hier kommt ein Glasfaserkabel zum Einsatz, was seine Begründung im hohen Datendurchsatz hat.

Tertiär-Verkabelung:

Der Bereich der Tertiär-Verkabelung erstreckt sich auf den Bereich der Etagenverteiler bis hin zu den jeweiligen Anschlussdosen. In der Regel erfolgt hier der Einsatz von symmetrischen Kupferkabeln mit einem Wellenwiderstand von 100 Ohm (UTP1-5, Kategorie 1–5). Alternativ sind auch 150-Ohm-Kabel (STP) zulässig.

Etagenverteiler:

Die Empfehlung geht hier zu einem Etagenverteiler pro 1000 qm Bürofläche. Ein solcher Verteiler dient für die Aufnahme von aktiven Elementen (Router, HUB's, etc) und passiven Elementen

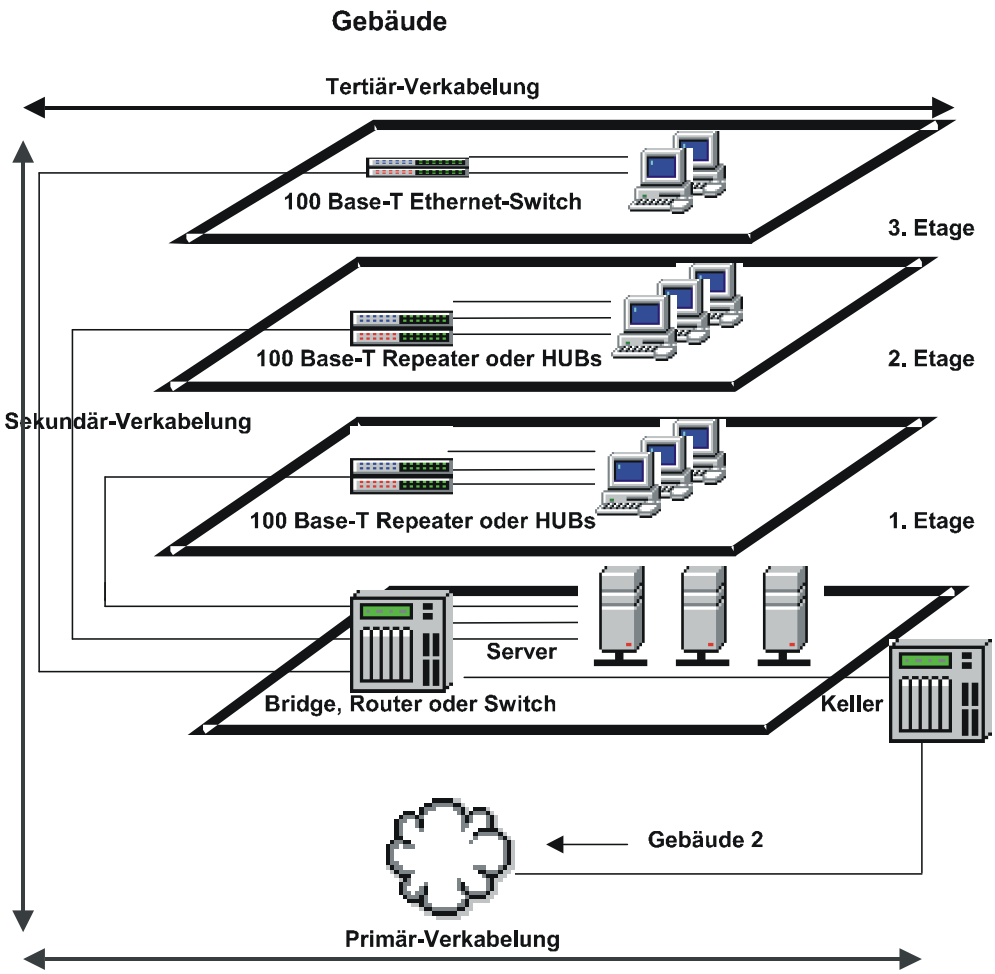


Abb. 13 Strukturierte Verkabelung

(Patchfelder). Als Sonderform können in einem Etagenverteiler auch mehrere kleinere Etagen zusammengefasst werden.

Anschlussdose:

Pro 10 qm Bürofläche sollten grundsätzlich 2 Anschlussdosen vorgesehen werden. Darüber hinaus müssen pro Arbeitsplatz mindestens 2 Anschlüsse eingeplant werden.

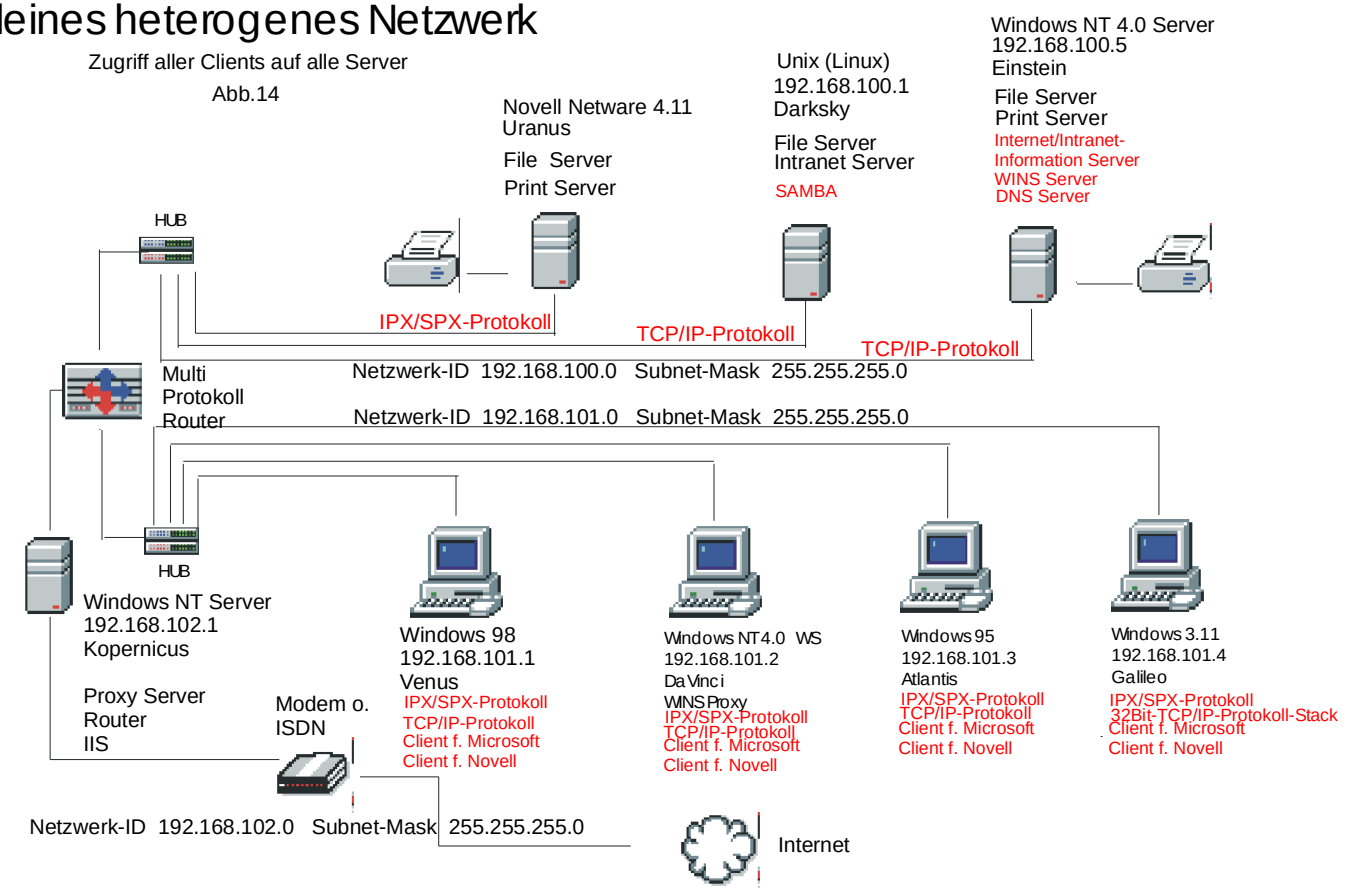
2.1.17 Netzwerkbetriebssysteme im Vergleich

Netzwerk-Betriebssysteme im Vergleich	
Novell 3.12:	kleinere und mittlere Netze (textorientierte Bedienung)
Novell 4.x:	mittlere und große Netze (grafik- und textorientierte Verwaltung)
Novell 5:	mittlere und große und sehr große Netze (grafik- und textorientierte Verwaltung), benötigt große Hardware-Ressourcen
Win NT:	kleinere, mittlere und große Netze (grafische Benutzeroberfläche) benötigt große Hardware-Ressourcen (RAM) Arbeiten am Server möglich
Win 2000:	mittlere und große und sehr große Netze (grafische Benutzeroberfläche), benötigt große Hardware-Ressourcen (RAM), Arbeiten am Server möglich, sehr komplexe Administration notwendig
Linux (Unix):	sehr große Netze (grafik- und textorientierte Oberfläche), grundsätzlich peer to peer, sehr schwierige Administration

Kleines heterogenes Netzwerk

Zugriff aller Clients auf alle Server

Abb.14

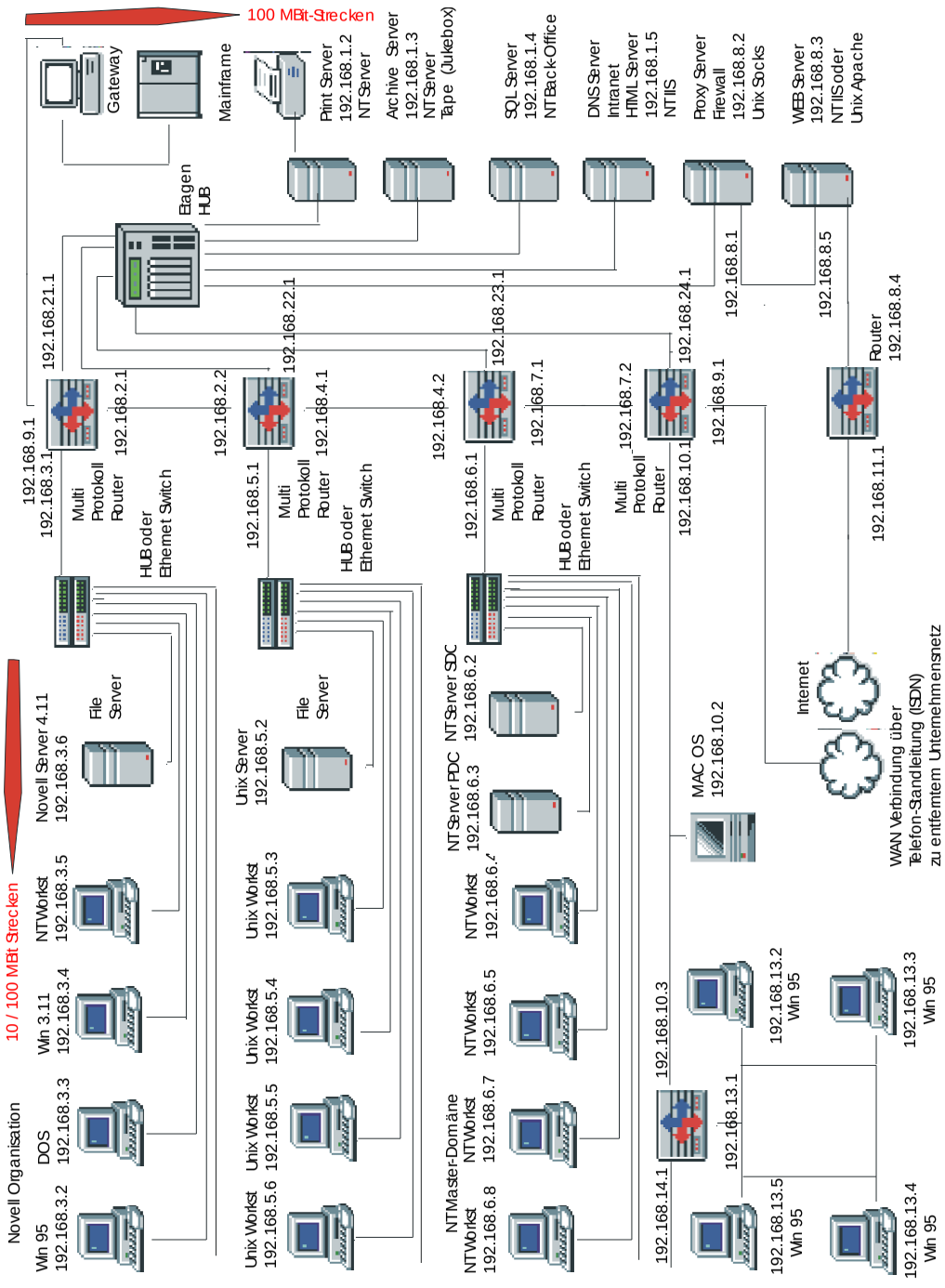


Heterogenes TCP/IP Netzwerk mit:
Routern und
Novell 4.11 Organisation und Unterorganisation

Unix

Windows NT Master Domäne und Ressourcen-Domäne

Abb. 15

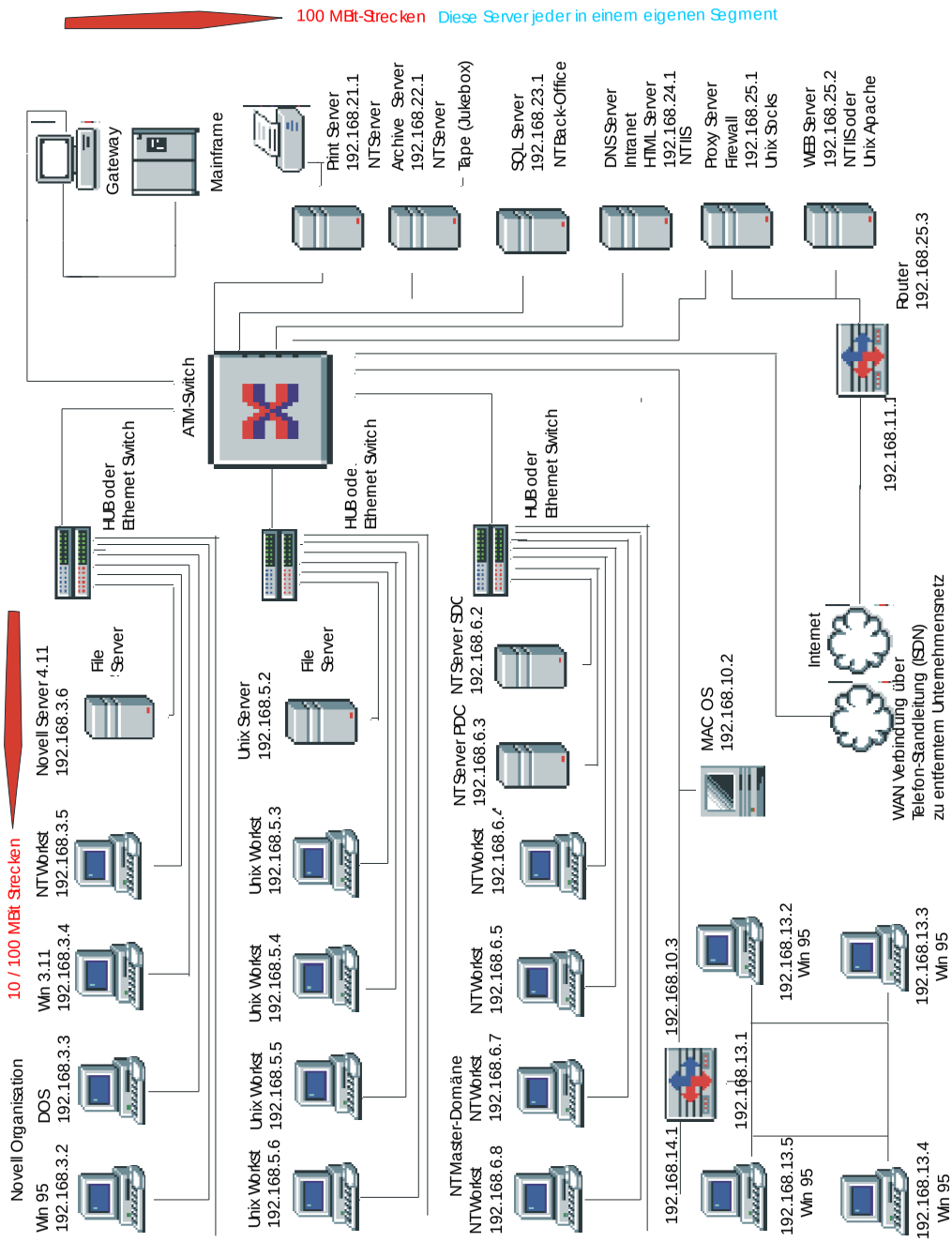

100 MBit-Strecken
Gateway
Mainframe
Print Server
192.168.1.2
NT Server
Archive Server
192.168.1.3
NT Server
Tape (Jukebox)
SQL Server
192.168.1.4
NT Back-Office
DNS Server
Intranet
HTML Server
192.168.1.5
NT IIS
Proxy Server
Firewall
192.168.8.2
Unix Socks
WEB Server
192.168.8.3
NT IIS oder
Unix Apache
Etagen HUB
192.168.21.1
192.168.9.1
192.168.3.1
Multi Protokoll Router
192.168.2.1
HUB oder Ethernet Switch
192.168.2.2
192.168.22.1
192.168.5.1
Multi Protokoll Router
192.168.4.1
HUB oder Ethernet Switch
192.168.4.2
192.168.23.1
192.168.6.1
Multi Protokoll Router
192.168.7.1
HUB oder Ethernet Switch
192.168.7.2
192.168.24.1
Multi Protokoll Router
192.168.10.1
192.168.9.1
192.168.8.1
192.168.8.5
Router
192.168.8.4
192.168.11.1
10 / 100 MBit Strecken
Novell Organisation
Win 95
192.168.3.2
DOS
192.168.3.3
Win 3.11
192.168.3.4
NT Workst
192.168.3.5
Novell Server 4.11
192.168.3.6
File Server
Unix Workst
192.168.5.6
Unix Workst
192.168.5.5
Unix Workst
192.168.5.4
Unix Workst
192.168.5.3
Unix Server
192.168.5.2
File Server
NT Master-Domäne
NT Workst
192.168.6.8
NT Workst
192.168.6.7
NT Workst
192.168.6.5
NT Workst
192.168.6.4
NT Server PDC
192.168.6.3
NT Server SDC
192.168.6.2
MAC OS
192.168.10.2
192.168.10.3
192.168.14.1
192.168.13.1
192.168.13.5
Win 95
192.168.13.4
Win 95
192.168.13.2
Win 95
192.168.13.3
Win 95
Internet
WAN Verbindung über
Telefon-Standleitung (ISDN)
zu entfemtem Unternehmensnetz

Heterogenes TCP/IP Netzwerk mit: ATM-Switch und Novell 4.11 Organisation und Unterorganisation

Unix

Windows NT Master Domäne und Ressourcen-Domäne

Abb. 16


100 MBit-Strecken
Diese Server jeder in einem eigenen Segment
Gateway
Mainframe
Print Server
192.168.21.1
NTServer
Archive Server
192.168.22.1
NTServer
Tape (Jukebox)
SQL Server
192.168.23.1
NTBack-Office
DNS Server
Intranet
HTML Server
192.168.24.1
NTIIS
Proxy Server
Firewall
192.168.25.1
Unix Socks
WEB Server
192.168.25.2
NTIIS oder
Unix Apache
Router
192.168.25.3
ATM-Switch
192.168.11.1
HUB oder
Ethernet Switch
HUB ode.
Ethernet Switch
HUB oder
Ethernet Switch
10 / 100 MBit Strecken
Novell Organisation
Win 95
192.168.3.2
DOS
192.168.3.3
Win 3.11
192.168.3.4
NTWorkst
192.168.3.5
Novell Server 4.11
192.168.3.6
File
Server
Unix Workst
192.168.5.6
Unix Workst
192.168.5.5
Unix Workst
192.168.5.4
Unix Workst
192.168.5.3
Unix Server
192.168.5.2
File
Server
NTMaster-Domäne
NTWorkst
192.168.6.8
NTWorkst
192.168.6.7
NTWorkst
192.168.6.5
NTWorkst
192.168.6.4
NTServer PDC
192.168.6.3
NTServer SDC
192.168.6.2
192.168.14.1
192.168.10.3
192.168.13.1
MAC OS
192.168.10.2
Internet
WAN Verbindung über
Telefon-Sandleitung (ISDN)
zu entfernten Unternehmensnetz
192.168.13.5
Win 95
192.168.13.2
Win 95
192.168.13.4
Win 95
192.168.13.3
Win 95

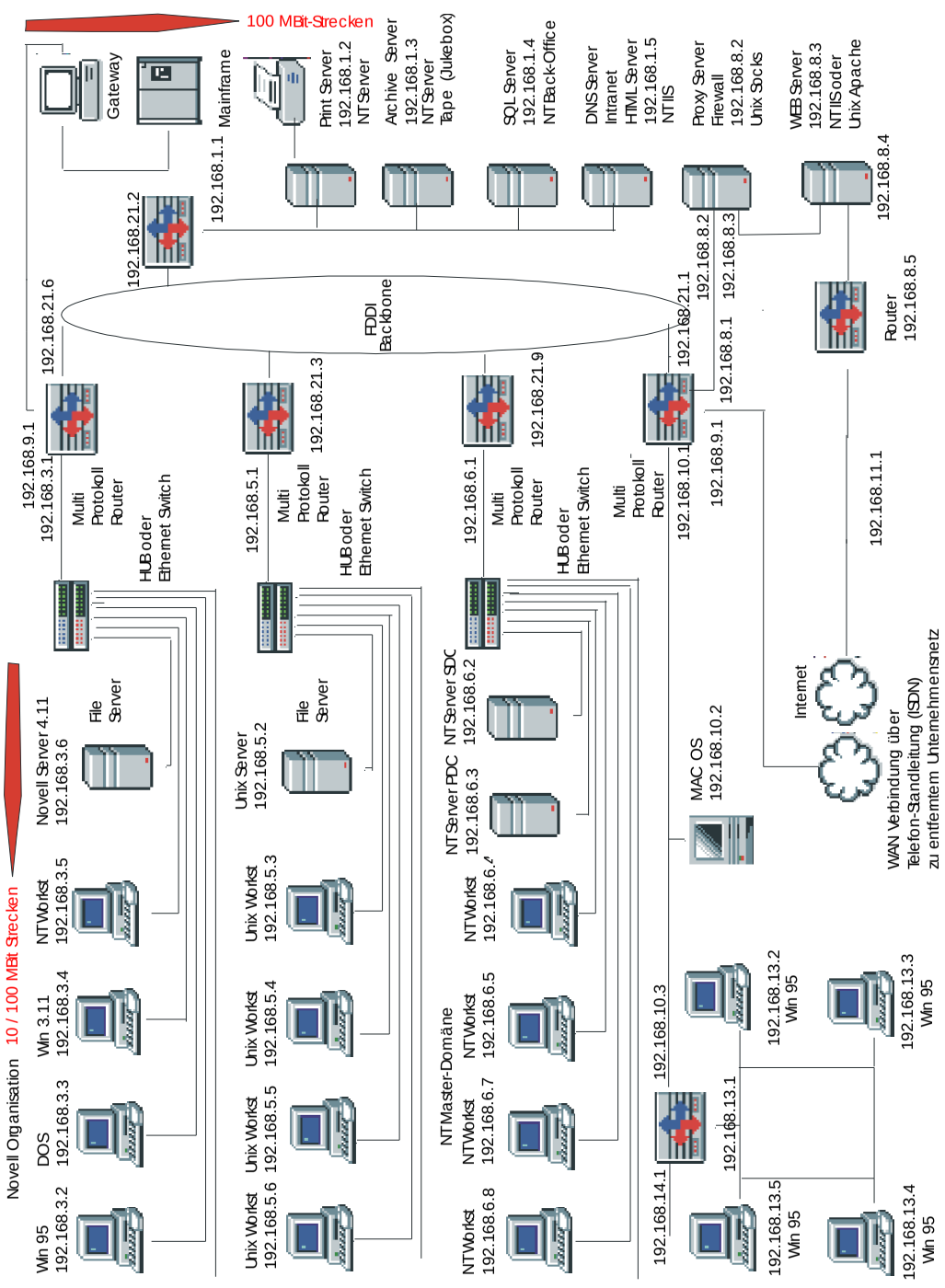
Heterogenes TCP/IP NetzWerk mit:
Routern und FDDI-Ring,

Novell 4.11 Organisation und Unterorganisation

Unix

Windows NT Master Domäne und Ressourcen-Domäne

Abb. 17


100 MBit-Strecken
Gateway
Mainframe
192.168.1.1
Print Server
192.168.1.2
NT Server
Archive Server
192.168.1.3
NT Server
Tape (Jukebox)
SQL Server
192.168.1.4
NT Back-Office
DNS Server
Intranet
HTML Server
192.168.1.5
NT IIS
Proxy Server
Firewall
192.168.8.2
Unix Socks
WEB Server
192.168.8.3
NT IIS oder
Unix Apache
192.168.8.4
192.168.21.2
192.168.21.6
FDDI
Backbone
192.168.21.1
192.168.8.2
192.168.8.3
192.168.8.1
Router
192.168.8.5
192.168.9.1
192.168.3.1
Multi
Protokoll
Router
HUB oder
Ethernet Switch
192.168.21.3
192.168.5.1
192.168.21.9
192.168.6.1
192.168.10.1
192.168.9.1
192.168.11.1
Novell Organisation
10 / 100 MBit Strecken
Novell Server 4.11
192.168.3.6
File
Server
Unix Server
192.168.5.2
NT Server PDC
192.168.6.3
NT Server SDC
192.168.6.2
MAC OS
192.168.10.2
Internet
WAN Verbindung über
Telefon-Standleitung (ISDN)
zu entferntem Unternehmensnetz
Win 95
192.168.3.2
DOS
192.168.3.3
Win 3.11
192.168.3.4
NT Workst
192.168.3.5
Unix Workst
192.168.5.3
Unix Workst
192.168.5.4
Unix Workst
192.168.5.5
Unix Workst
192.168.5.6
NT Workst
192.168.6.4
NT Workst
192.168.6.5
NT Workst
192.168.6.7
NT Workst
192.168.6.8
NT Master-Domäne
192.168.10.3
192.168.14.1
192.168.13.1
192.168.13.2
Win 95
192.168.13.3
Win 95
192.168.13.5
Win 95
192.168.13.4
Win 95

Legende


Server


Switch


Workstation


Großrechner (Mainframe)


HUB oder Ethernet-Switch

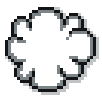

Gateway


Multiprotokoll Router


Modem oder ISDN


Etagen-HUB


MAC-Intosh Workstation


Die große, weite Welt


Drucker

2.1.18 Optimieren von Netzwerken

Netzwerk-Design:

Das richtige Netzwerk-Design ist unter dem Gesichtspunkt des Datenaufkommens in einem Netzwerk eines der wichtigsten Kriterien und mit entscheidend darüber, wie ein Netzwerk funktioniert. Sicher kann man mit einer 10Base2/10BaseT-Verkabelung, ein paar Hub's, einem Server und ein paar Workstations ein Netzwerk aufbauen, welches in kleineren Büros sehr wahrscheinlich völlig ausreichend ist. Sind Unternehmen größer, steigen allerdings die Anforderungen an ein Netzwerk sehr schnell.

Umfangreicher Anmeldeverkehr, Transfers von servergespeicherten Dateien, DHCP, WINS, DNS, Internetverkehr und E-Mail, Replikationen und Anwendungen, Austausch von Routerinformationen, Zusatz- und Hilfsprotokolle benötigen entsprechende Bandbreite, damit das Netz nicht irgendwann zum Erliegen kommt. Überlastete, blockierte Server, Engpässe im Netz durch überlastete Netzwerk-Geräte wie Router, Switches oder Hub's können weiter zu dazu beitragen, dass Netzwerke nicht stabil laufen und so Anwender in ihrem Arbeitsablauf beeinträchtigt sind.

Mit dem richtigen Netzwerk-Design für die jeweilige Situation in einem Unternehmen kann vielen Problemen, die durch entsprechenden Datenverkehr auftauchen können, schon im Vorfeld aus dem Weg gegangen werden. Um den Datenverkehr in einem Netzwerk zu verstehen und einzuordnen und damit ein Netzwerk effizient gestalten (designen) zu können, muss dieser bekannt sein.

Datenverkehr

Beispiel:

Datenverkehr in einem Win-NT-Netzwerk durch

- Anmeldedienst

- Computer-Suchdienst
- DHCP (zwischen DHCP-Clients und DHCP-Servern)
- DHCP (zwischen DHCP-Servern und DHCP-Relay-Agenten)
- WINS (zwischen WINS-Clients und WINS-Servern)
- WINS (Replikation zwischen WINS-Servern)
- Verzeichnisreplikation
- DNS(zwischen DNS-Clients und DNS-Servern)
- DNS (Replikation zwischen DNS-Servern)
- Datenverkehr von/zum Internet (mit Browser oder E-Mail)
- Datenverkehr zwischen Clients und Servern aufgrund einer Dateisitzung
- Kontensynchronisation zwischen Servern (PDC, BDC)
- Vertrauensstellungen
- Serversuchdienst
- Servergespeicherte Profile

(detaillierter wird weiter unten auf diesen Datenverkehr eingegangen).

Broadcasts

Broadcasts sind Frames, die an alle Computer im Netzwerk verschickt werden. Netware-Server verschicken über Broadcasts z. B. die Bekanntmachung ihrer Dienste, die sie im Netzwerk bereitstellen. In MS-Netzwerken, die nicht über WINS oder DNS verfügen, werden über Broadcasts die Namensauswertungen der Computer vorgenommen, DHCP-Clients verschicken DHCP-Broadcasts, um einen DHCP-Server zu finden, von dem sie ihre IP-Adresse beziehen können, ARP verschickt Broadcasts, um die MAC-Adresse eines Remote-Computers zu erfahren, Router gleichen über Broadcasts ihre Routing-Tabellen ab, auch NetBIOS gehört zu den großen Verursachern von Broadcasts, jedes installierte Protokoll verursacht Broadcasts. Broadcasts

können ein Netzwerk so überlasten, dass ein erheblicher Leistungsabfall des Netzwerkes die Folge sein kann. Broadcasts sind aber in Netzwerken auch unerlässlich, um viele Dinge zu regeln.

Da Switches Frames nur über MAC-Adressen im Netzwerk weiterreichen, sind Switches für Broadcasts durchlässig. Switches wissen nicht, um welche Art Broadcast es sich handelt. Broadcasts verbreiten sich also ungehindert über Switches. Sie können in alle Netzwerksegmente gelangen.

Router dagegen sperren Broadcasts weitgehend. Ein Router kann erkennen, was für ein Broadcast ihn erreicht hat, da Router Frames interpretieren. Dieser wird nun in einen Unicast verwandelt, der nur an eine spezielle Adresse weiter gereicht wird, für die der Rahmen bestimmt ist (wenn z. B. ein DHCP-Client einen DHCP-Server sucht (der Router muss dazu allerdings DHCP-fähig sein)). Router speichern auch Informationen. Wenn z. B. eine ARP-Anfrage eines Computers an einen anderen Computer geschickt wird und diese vom Remote-Computer beantwortet wurde, beantwortet der Router die nächste Anfrage nach dem Paar IP-MAC-Adresse direkt. Auch SAP’s von Netware-Servern werden in Routern zwischengespeichert. Diese gespeicherten Informationen werden dann an andere Router im Netzwerk verschickt. Router hindern Broadcasts also daran, sich im gesamten Netzwerk zu verbreiten.

Diese Tatsache ist wichtig, denn nicht nur das Netzwerk, sondern auch Computer können von Broadcasts regelrecht lahm gelegt werden. Umso mehr Broadcasts einen Computer erreichen, desto mehr CPU-Zeit wird von Computern benötigt, um die Broadcasts zu handhaben. Oftmals kann die Netzwerkkarte nicht entscheiden, wie die Broadcasts zu handhaben sind, sondern muss diese an den Prozessor weiterreichen, was zu Lasten der eigenen Arbeit geht und so Anwender daran hindern kann, ihre Arbeit zu tun.

Die richtige Gestaltung des Netzwerkes durch den Einsatz von Routern, Switches und Servern an der richtigen Stelle im Netz, ist also eine Grundvoraussetzung für den reibungslosen Ablauf von Netzwerkaktivitäten und damit einer optimalen Netzwerkleistung.

Multicasts

Multicasts sind Frames, die nur an spezielle Computer im Netzwerk gesendet werden. Sie verursachen nicht soviel Datenverkehr wie Broadcasts. Der verursachte Datenverkehr ist aber immer noch höher, als wenn Frames direkt an eine MAC-Adresse gesendet werden.

Frames mit Ziel

Hierrunter fallen alle Datenpakete, die direkt von einer MAC-Adresse an eine andere im Netzwerk geschickt werden. Diese verursachen am wenigsten Datenverkehr.

Protokolle

In einem Netzwerk sollten nur die Protokolle installiert sein, die auch wirklich benötigt werden, um unnötigen Datenverkehr zu vermeiden. IPX und NWLink sowie NetBIOS verursachen sehr viel Broadcasts und somit viel Datenverkehr. Versendet IPX z. B. seine SAP’s, werden diese natürlich nicht nur von IPX-basierten WS’s entgegen genommen, sondern auch Computer, auf denen nur TCP/IP installiert ist, müssen sich mit dem Broadcast auseinander setzen, da die MAC-Adresse der Netzwerkkarte für IPX und TCP/IP gleichermaßen verwendet wird. Also auch TCP/IP-Computer müssen ihre Arbeit unterbrechen, nachsehen, ob der Rahmen für sie bestimmt ist, und dann verwerfen.

TCP/IP verwendet Frames mit Ziel. Das Datenaufkommen durch TCP/IP ist somit sehr viel geringer als mit den anderen Protokollen. Zudem hat TCP/IP sehr viele andere Vorteile und setzt sich auch mehr und mehr in Netzwerken durch.

Auch das Einrichten einer Sitzung zwischen zwei Computern verursacht viel Datenverkehr. Nachfolgend ein Beispiel der Vorgänge über das TCP/IP-Protokoll:

Netzwerkverkehr beim Einrichten einer Datenübertragung

1. NetBIOS-Name des Remote-Computers wird zur IP-Adresse aufgelöst
   1. Ein Broadcast wird an alle Computer gesendet, oder
   2. ein WINS-Server wird befragt, oder
   3. ein DNS-Server wird befragt, oder
   4. LMHOST-Dateien werden ausgewertet.
2. IP-Adresse zur MAC-Adresse auflösen (ARP)
   Der Quell-Computer sendet einen Broadcast zum Ziel-Computer, dass er ihm seine MAC-Adresse mitteilen soll. Der Ziel-Computer antwortet mit seiner MAC-Adresse.
3. TCP-Verbindung aufbauen
   Der erste Host sendet ein Paket an den zweiten Host, dass er eine Sitzung anfordert. Der zweite Host empfängt dieses Paket, sendet Infos über sich selbst und dass er bereit ist. Der erste Host quittiert diese Infos (3-facher Handshake). Eine Sitzung ist jetzt eingerichtet.
   Zum Einsehen der Sitzungen:
   TCP-IP-Kommunikation = Befehl **netstat** (Eingabeaufforderung) unter NT
   NetBIOS-Sitzungen = Befehl **nbtstat** (Eingabeaufforderung) unter NT
4. NetBIOS-Sitzung aufbauen
   Wie bei TCP muss eine NetBIOS-Sitzung eingerichtet werden, bevor zwei Hosts miteinander kommunizieren können. Der Ziel-Server muss sowohl den Computer-Namen als auch die NetBIOS-Sitzung bestätigen.
5. SMB-Protokolle aushandeln
   Jeder SMB ist ein Dialekt. Jeder Computer

kann mehrere SMB-Dialekte verstehen. Der Client teilt dem Server mit, welche Dialekte er beherrscht. Der Server antwortet damit, dass er dem Client den höchsten Dialekt bestätigt.

6. Aufbauen der Verbindung zu einer Freigabe
   1. Der Client baut eine Verbindung zum Server auf
      1. Freigabe-Namen senden
      2. Benutzer-Name und Kennwort senden
   2. Der Server bestätigt den Benutzer-Namen und das Kennwort
7. Daten übertragen

Server

Um ein Netzwerk effizient aufbauen zu können, welches nicht nur für den Moment, sondern auch zukünftig vernünftig laufen soll, ist es wichtig, dass man sich als Netzwerk-Designer/Administrator darüber bewusst ist, mit welchem Datenverkehr wo im Netzwerk zu rechnen ist. In diesem Zusammenhang nehmen Standorte von Servern innerhalb des Netzwerkes eine zentrale Rolle ein. Dabei wird unterschieden in

- Enterprise oder zentralisierte Server und
- Verteilte oder Workgroup-Server

Enterprise Server

Enterprise oder zentralisierte Server befinden sich meisten in einem extra dafür vorgesehenen, gesicherten Raum, nämlich dem Serverraum. Ob nun Anmeldeverkehr, Anwendungen, Replikationen, etc., alles wird über diese Server abgewickelt. Entsprechend hoch liegt hier das Datenaufkommen, da alle WS’s im Netz auf diese Server zugreifen. Auch der Router muss den ganzen Datenverkehr bewältigen.

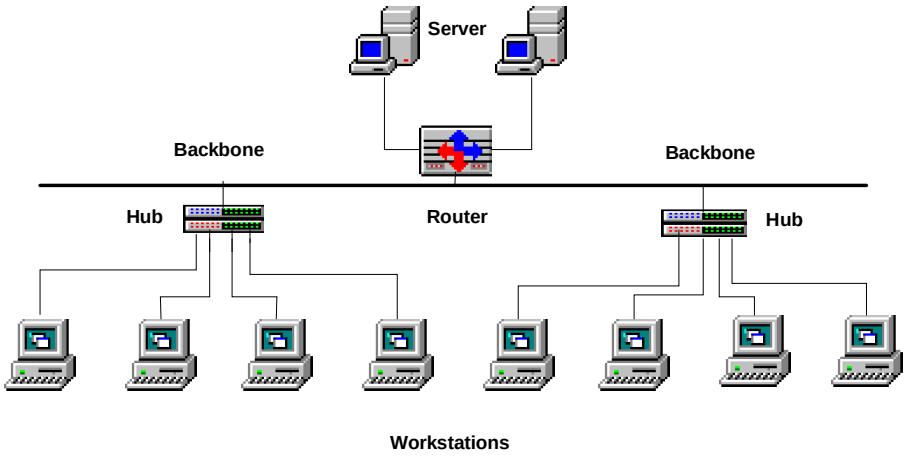


Abb. 18 Enterprise Server

Verteilte Server

Verteilte oder lokale bzw. Workgroup-Server agieren nicht für alle Benutzer in einem Netzwerk, sondern nur bestimmte Ws's können darauf zugreifen, weswegen diese Server immer physisch in der Nähe dieser WS's stehen sollten (im gleichen Subnetz), z. B. verschiedenen Abteilungen eines Unternehmens können einen eigenen Server für die Abwicklung ihres Datenverkehrs erhalten. Durch diese Art wird der Netzwerkverkehr auf den zentralen Strecken des Netzwerk erheblich verringert, was wiederum bessere Antwortzeiten der zentralen Server zur Folge hat.

Für die jeweilige Situation empfiehlt sich aber auch der Einsatz von beiden Arten. Sowohl verteilte als auch zentralisierte Server sollten zum Einsatz kommen, so, wie die Situation in einem Unternehmen es erfordert. So können z. B. Daten, die nur der jeweiligen Abteilung zugänglich sein sollen, auf deren Workgroup-Server gespeichert werden, während Daten, die allen Anwendern zugänglich sein sollen, auf zentralisierten Servern abgelegt werden. E-Mail-, Web- oder SQL-Server zählen hierzu. Der Datenverkehr auf der zentralen Strecke des Netzwerks kann

durch Einsatz beider Varianten auf jeden Fall erheblich verringert werden.

Eine sinnvolle Aufteilung von Workgroup- und zentralisierten Servern in einem Netzwerk ist in den Abb. 15–17 im vorherigen Abschnitt dargestellt. Die Anmelde- und File-Server der jeweili-

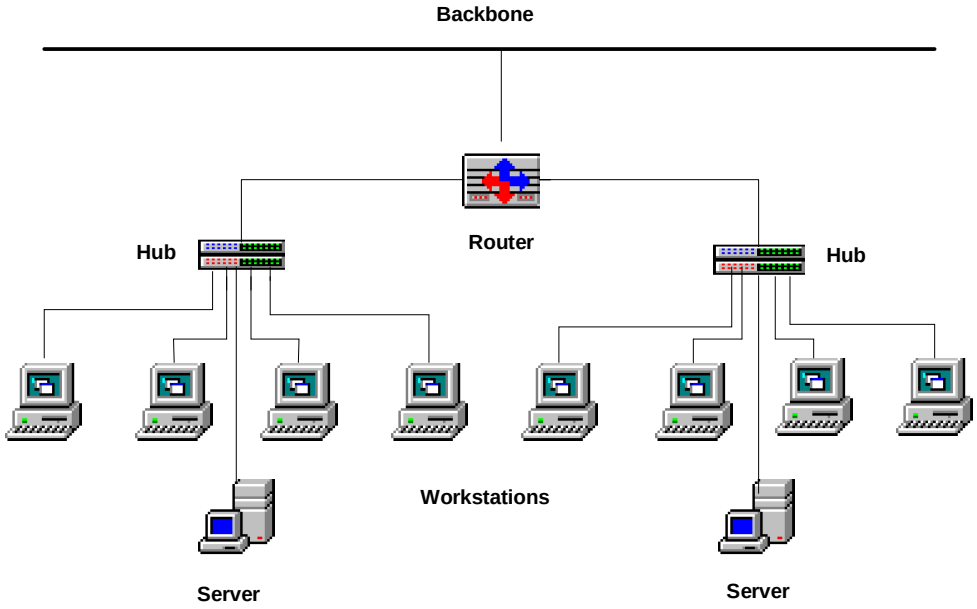


Abb. 19 Verteilte Server

gen Organisationseinheiten liegen in ihrem Subnetz. Der Anmelde- und File-Verkehr wird somit nur auf dieses Subnetz beschränkt. Router zu jedem Subnetz verhindern die Ausbreitung von unnötigem Datenverkehr auf den zentralen Strecken des Netzwerks. Server, die für alle im Netzwerk Dienste bereitstellen, sind zentral, für alle erreichbar angebracht. Die File-Server der jeweiligen Organisationseinheiten können nachts eine Datenreplikation mit einem zentralisierten Backup-Server (Archiv-Server) abhal-

ten, so dass die Daten der Organisationseinheiten trotzdem zentral gesichert werden können.

Verfügbarkeit von Netzwerken

Computer und Computer-Netzwerke sind aus den meisten Firmen heute nicht mehr wegzudenken. Unter Umständen steht oder fällt die ganze Firma mit der Verfügbarkeit von Computern und Netzwerken, so dass geradezu eine Abhängigkeit vieler Firmen von ihrer EDV entstanden ist. Umso wichtiger ist die laufende Verfügbarkeit der EDV in einer Firma geworden.

Workstations sind relativ schnell auszutauschen, solange sich keine relevanten Daten darauf befinden (sollte auch nicht). Im

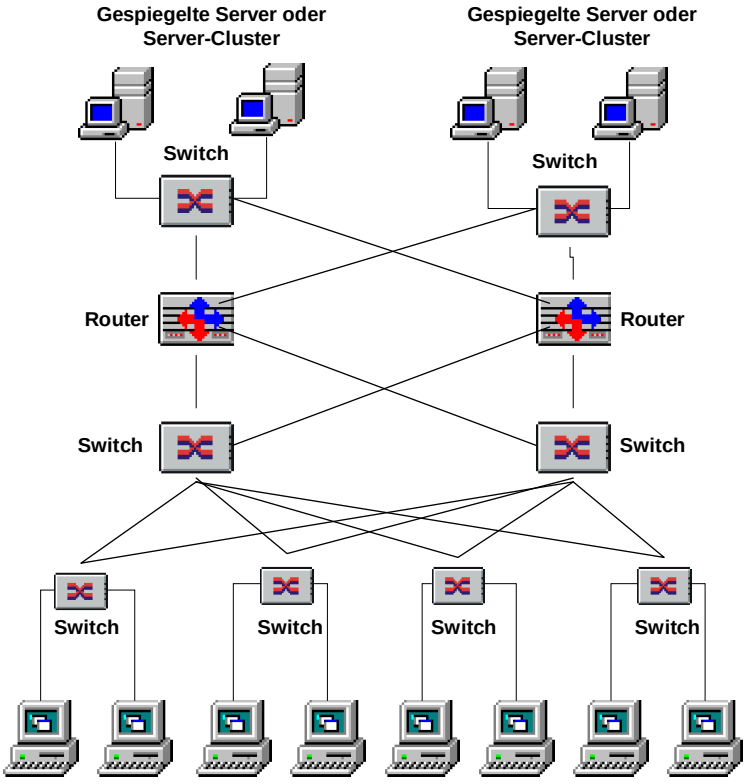


Abb. 20 Sicheres Netzwerk mit Datenpfadredun-

danz

Server-Bereich heißt dies schon lange USV's, redundante Prozessoren, Plattenspiegelung oder RAID5 (siehe „Festplatten-Manager“ unter Win NT4), Datensicherung auf Bandlaufwerke, Serverspiegelung, Ausweichserver, die nur bei Ausfall des Hauptservers eingesetzt werden, und/oder Cluster-Server (siehe „Cluster“ unter Win2000).

Aber auch im Netzwerk-Bereich muss für solche Firmen dauernde Verfügbarkeit gegeben sein. Der Ausfall des Netzwerkes kann eine solche Firma um beträchtlich Summen bringen. Im Netzwerk-Bereich heißt Verfügbarkeit „Datenpfadredundanz“. Unter Datenpfadredundanz wird die Möglichkeit verstanden, dass Daten Wege über verschiedene Netzwerkverbindungen nehmen können, dass es zu einem Ziel also nicht nur einen Weg gibt, sondern mehrere (Maschennetz).

Im „normalen Netzwerk“ gebe es mit der Datenpfadredundanz ein großes Problem. Da mehrere Datenpfade zur Verfügung stehen, würden Daten sowie Broadcasts als Endlosschleife zwischen den Switches und WS's unterhalb der Router zirkulieren. Damit dies nicht passiert, müssen entsprechende Software-Protokolle im Netz installiert sein, die dies verhindern. Im Allgemeinen werden das Spanning-Tree-Protokoll oder Router-Protokolle dazu eingesetzt.

Spanning-Tree-Protokoll

Über das Spanning-Tree-Protokoll wird nur ein Pfad als Hauptpfad verwendet. Die anderen bleiben in Reserve, bis der Hauptpfad ausfällt, woraufhin Spanning-Tree einen neuen Hauptpfad aus den noch bestehenden Pfaden einrichtet.

Router-Protokolle

Routing-Protokolle wie RIP oder OSPF können dazu verwendet werden, zu berechnen, welcher Weg über ein Maschennetz der Beste für ein Datenpaket ist. Fällt eine Verbindung aus oder ist

diese überlastet, kann jederzeit eine andere Verbindung vom Router benutzt werden. Die Funktion ist darüber gewährleistet, da sich am Router Schnittstellen mit verschiedenen Subnetzen befinden (Netzwerkkarten mit verschiedenen IP-Adressen) (siehe auch Abb. 15 im letzten Abschnitt).

Die Möglichkeit über Routing-Protokolle eignet sich auch, um die Datenlast besser aufteilen zu können.

Hot-Standby-Routing-Protokoll (HSRP)

Jeder Computer in einem gerouteten Netzwerk verfügt normalerweise über ein Standard-Gateway, über das alle Datenpakete geschickt werden, die nicht für das eigene Netzwerk bestimmt sind. Fällt dieser Router aus, besteht für diese Computer kein vollständiger Zugang zum gesamten Netzwerk mehr. HSRP stellt eine Möglichkeit dar, mehrere Router mit ein und derselben virtuellen IP- und MAC-Adresse auszustatten, so dass bei Ausfall des Standard-Gateway’s für Computer dennoch der Zugang zum gesamten Netzwerk erhalten bleibt.

Skalierbarkeit von Netzwerken

Netzwerke sollten heute so veränderbar/erweiterbar aufgebaut werden, dass nicht jedes Mal, wenn das Unternehmen wächst, ein Netz völlig neu aufgebaut werden muss. Firmen wachsen, neue Mitarbeiter werden eingestellt, neue Technologien müssen alte ersetzen, wenn der momentane Standard mit den Anforderungen der Zeit nicht mehr Schritt halten kann. Aus welchen Gründen auch immer, Netzwerke haben die Eigenart sehr schnell zu wachsen. All dies kann erhebliche Kosten verursachen, wenn nicht schon beim ersten Entwurf eines Netzwerkes diese Möglichkeiten in Betracht gezogen werden. Nachfolgende Lösung ist nur als Denkanstoß zu verstehen, da in jedem Unternehmen andere Anforderun-

gen an ein Netzwerk bestehen können (physikalisch sowie technisch).

Cisco-System hat für skalierbare Netzwerke hervorragende Lösungen entwickelt. Im Vordergrund stehen dabei mehrere einzelne Elemente eines Netzwerks, die mit

- Gebäudebaustein
- Kernbaustein und
- Serverbaustein

bezeichnet werden und die relativ einfach erweitert werden können. Dabei werden sowohl Datenverkehr als auch Datenpfadredundanz gleichermaßen berücksichtigt.

Cisco geht von einem sog. Campus-LAN aus, was bedeutet, mehrere Gebäude in einer Firma sind zu einem Netzwerk zusammengeschlossen. Es gibt lokalen Datenverkehr, nämlich der, der in einem kleinen Teilbereich des Netzwerkes bleibt und nicht über das Backbone geht, und Cross-Campus-Verkehr, welcher sich über das ganze Netzwerk ausbreitet.

Im einem Gebäude-Baustein ist lediglich mit dem Datenverkehr zu rechnen, den die angeschlossenen WS’s in diesem Baustein verursachen. Ein Gebäude-Baustein sollte nicht mehr als 1500 Knoten (Computer, Drucker, verteilte Server) enthalten. Hier genügen auch Schicht-2-Switches. Die Router sind von Natur aus Schicht-3-Geräte und begrenzen den Gebäude-Baustein als eine Broadcast-Domäne. Broadcasts breiten sich also nicht über das ganze Netzwerk aus.

Im Kernbaustein tritt der Hauptverkehr auf, da alle WS’s aus allen Gebäude-Bausteinen über den Kern-Baustein auf die zentralisierten Server, auf das Internet und/oder auf ein entferntes Unternehmensnetz (über WAN-Leitungen) zugreifen. Hier sollte dann auch mit Fast-Ethernet oder Gigabit-Ethernet und ATM-Switches gearbeitet werden.

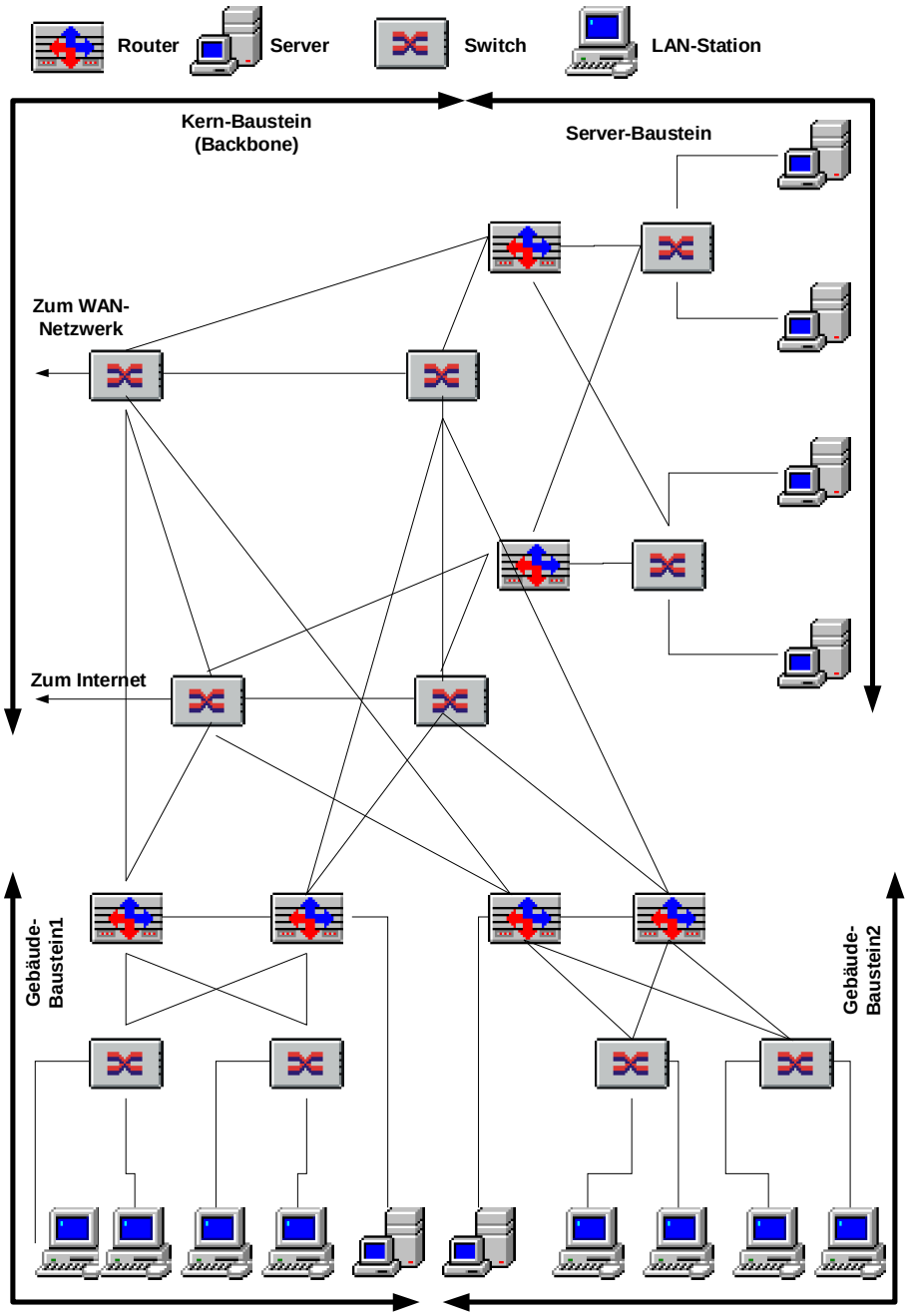


Abb. 21 Redundantes Netzwerk mit skalierbarem Gebäude-, Kern- und Server-Baustein

Für den Server-Baustein ist es wichtig, dass dieser nur zwei Hop's (Sprünge über Router) vom Gebäude-Baustein entfernt liegt. Die hier eingesetzten Router schützen die Server vor Broadcaststürmen und vor Netzausfällen.

Datenverkehr und dessen Optimierung:

Da es den Rahmen dieses Buches sprengen würde, kann hier natürlich nicht auf jedes erdenkliche Netzwerk unter den vielen Netzwerk-Betriebssystemen eingegangen werden. Im Folgenden soll aber zumindest der Datenverkehr in einem Win-NT-Netzwerk unter TCP/IP besprochen werden, da Win NT4 große Marktanteile im Netzwerk-Bereich inne hat und diese Anteile ständig steigen.

Durch die einzelnen Netzwerkdienste von Win NT wird ein unterschiedlicher Datenverkehr erzeugt, der die Bereiche

1. Clientinitialisierung
2. Client zu Server
3. Server zu Server

beinhaltet.

Zu 1. Clientinitialisierung

Bei der Clientinitialisierung wird

1. DCHP-Verkehr
2. WINS-Verkehr
3. Verkehr der Dateisitzung
4. Verkehr der Anmeldebestätigung

erzeugt.

a) DHCP

(Eine genaue Beschreibung der Funktion von DHCP ist im Abschnitt „Windows NT4“ enthalten).

Der von DHCP erzeugte Datenverkehr beinhaltet die Anforderung, die Erneuerung, die Freigabe

von IP-Adressen. Durch DHCP wird ein Netzwerk wenig belastet, wenn die Lease-Dauer nicht gerade einen sehr geringen Wert enthält oder die Anforderung einer Lease über einen Router ablaufen muss.

Datenverkehr: DHCP-Verkehr durch das Anfordern einer Lease (4 Rahmen, 1,3 kByte, einmal pro Client)
Suche nach einem DHCP-Server
Antwort des DHCP-Servers mit der IP-Adresse für den Client
Antwort des Client, dass er die IP akzeptiert
Bestätigung des Servers mit der Lease-Dauer

DHCP-Verkehr durch das Erneuern einer Lease (2 Rahmen, 684 Byte, bei jedem Start des Clients)
Antwort des Client, dass er die IP akzeptiert
Bestätigung des Servers mit der Lease-Dauer

Wird die Erneuerung nicht durchgeführt, versucht es der Client wieder mit der 4-Rahmen-Abfrage.

Verringern des Datenverkehrs:

Der Datenverkehr durch DHCP kann über das Einstellen einer längeren Lease-Dauer im DHCP-Manager verringert werden. Sind Clients im Netz, die aus einem Subnetz DHCP-Adressen anfordern, kann durch die Konfiguration eines DHCP-Relay-Agenten in diesem Subnetz ebenfalls der Datenverkehr durch DHCP verringert werden. Clients müssen dann nicht ihre DHCP-Anfragen über das gesamte Netz schicken, sondern nur den Relay-Agenten befragen. Dieser tauscht mit dem

DHCP-Server sehr viel weniger Rahmen aus, als alle Clients dies tun würden.

b) WINS

Eine genaue Beschreibung der Funktion von WINS ist im Abschnitt „Windows NT4“ enthalten).

Über WINS wird die Registrierung des NetBIOS-Namen des Client mit seiner IP-Adresse bei einem WINS-Server vorgenommen. WINS belastet das Netzwerk ebenfalls nicht besonders.

Datenverkehr:			
Registrierung	2 Rahmen	214 Byte	pro Dienst/Anwendung beim Start
Erneuerung	2 Rahmen	214 Byte	pro Dienst/Anwendung ½ Ende TTL
Auswertung	2 Rahmen	196 Byte	unterschiedlich
Freigabe	2 Rahmen	214 Byte	bei Beendigung eines Dienstes

Alle Dienste und Anwendungen, die NetBIOS verwenden, registrieren NetBIOS-Namen.

Registrierte Namen eines Clients:	
Computername <00>	Arbeitsstationsdienst
Computername <03>	Nachrichtendienst
Computername	Serverdienst des Client
Arbeitgruppe oder Domänname <00>	NetBIOS-Gruppenname zur Registrierung des Computers als Domänenmitglied
Arbeitgruppe oder	NetBIOS-Gruppenname zur

Domänname <1E>	Auswahl von Suchdiensten
Domänname <1B>	Hauptsuchdienst für die Domäne
Domänname <1C>	Domänen-Controller der Domäne
Arbeitgruppe oder Domänname <1E>	Hauptsuchdienst des Subnetzes

Verringern des Datenverkehrs:

Der Datenverkehr von WINS kann darüber verringert werden, dass ein Computer, der keine Ressourcen im Netz zur Verfügung stellt, seinen Serverdienst deaktiviert. Des Weiteren können die TTL-Werte im WINS-Manager erhöht werden.

c) Dateisitzung

Datenverkehr, der eine Dateisitzung beinhaltet, ist ebenfalls nicht sehr hoch.

Datenverkehr:			
Adressaus-wertung	2 Rahmen	120 Byte	für jede Verbindung
TCP-Sitzung	3 Rahmen	180 Byte	bei jeder ersten Verbindung zum Server
NetBIOS-Sitzung einrichten	2 Rahmen	186 Byte	bei jeder ersten Verbindung zum Server
SMB-Protokoll-aushandlung	2 Rahmen	365 Byte	bei jeder ersten Verbindung zum Server
Verbindungs sequenz	2 Rahmen	360 Byte	jeder Verbindungs-versuch

Beenden der Sitzung	5 Rahmen	360 Byte	Trennen vom Server

Verringern des Datenverkehrs:

Der Datenverkehr, der aufgrund einer Dateisitzung zustande kommt, kann durch das Entfernen von nicht benötigten Protokollen verringert werden, da Verbindungsanforderungen über alle vorhandenen Protokolle geleitet werden (für jedes Protokoll extra). Auch kann die physische Distanz zwischen Server und Client verringert werden.

e) Anmeldebestätigung

Die Anmeldung wird durch das Eingeben des Benutzernamens und des Kennworts bei der Netzwerkanmeldung durchgeführt. Diese Angaben werden nach Ermittlung des Anmeldeservers bestätigt. Die Systemzeit wird vom Server überprüft, Anmeldescripte werden ausgeführt, Systemrichtlinien und servergespeicherte Profile werden geladen (min. 24 Rahmen, 3100 Byte).

Ein Domänen-Controller zur Anmeldung wird entweder über Broadcasts vom Client ermittelt (viel Datenverkehr) oder, wenn

Datenverkehr:			
Einrichten der Sitzung	15 Rahmen	2000 Byte	pro Anmeldung
Bestätigung (Win95/98)	4 Rahmen	760 Byte	pro Anmeldung
Bestätigung (Win NT)	20 Rahmen	2700 Byte	pro Anmeldung
Beenden der Sitzung	5 Rahmen	360 Byte	pro Anmeldung

WINS im Netz ist, über H-Knoten (siehe Kapitel DHCP, in „Windows NT“) (wenig Datenverkehr). Der NetBIOS-Name des Anmeldeservers wird ausgewertet (Broadcasts oder WINS), TCP-Sitzung wird

eingerichtet (3-facher Handshake), NetBIOS-Sitzung wird eingerichtet, SMB-Protokollaushandlung wird durchgeführt, SMB-Verbindung zu \\Servername\IPC$ wird eingerichtet.

Für Win-NT-Computer wird jetzt weiter auf die Liste der vertrauten Domänen zugegriffen, ein sicherer Kanal eingerichtet. Nun werden Anmeldeskripte, Systemrichtlinien, etc. ausgeführt.

Verringern des Datenverkehrs:

Der Datenverkehr durch den Anmeldevorgang kann durch optimal verfügbare Domänen-Controller verringert werden (2000 Clients, ein DC). Weiter kann der Serverdienst des DC's für „Durchsatz für Netzwerkfreigabe" optimiert werden. Damit erhöht sich die Anzahl der gleichzeitig anzumeldenden Clients. Der Server sollte dann aber nicht mehr als File-Server arbeiten, sondern reiner Anmelde-Server sein (Master-DC) (siehe Abschnitt „Windows NT"). Weiter sollte der Anmelde-Server physisch so nah wie möglich bei seinen Clients stehen. Schnelle, sichere Hardware das Servers kann hier weitere Abhilfe schaffen.

Zu 2. Client zu Server

80 % des Datenverkehrs wird zwischen Client und Server ausgeführt.

Beim Client zu Server Verkehr wird

1. Verkehr des Suchdienstes
2. DNS-Verkehr
3. Internet/Intranet-Verkehr

erzeugt.

a) Suchdienst

Über den Suchdienst werden Ressourcen im Netzwerk für den Benutzer sichtbar gemacht. Um der Suchliste Server hinzufügen zu können, werden Ankündigungen an den Hauptsuchdienst gesendet. Eine Liste der Server und Domänen wird vom

Hauptsuchdienst für den Sicherungssuchdienst freigegeben. Der Hauptsuchdienst sendet eine Liste der Sicherungssuchdienstcomputer an den Client. Die Serverliste wird vom Client beim Sicherungssuchdienst abgefragt.

Datenverkehr:			
Hostankündigung	1 Rahmen	243 Byte	pro Server alle 12 Minuten
Sicherungs-suchdienst lokalisieren	2 Rahmen	450 Byte	pro Computer bei der Suche
Auswahl	viele	225 Byte	wenn Computer des Hauptsuchdienstes gestartet wurden
Abrufen der Suchliste	20 Rahmen		jede Suche durch den Client und alle 12 Minuten durch den Sicherungs-suchdienst
Abrufen der Freigabeliste	16 Rahmen	1900 Byte	jede vom Client durchgeführte Suche in einer Liste
(Win95/98)	19 Rahmen		
(Win NT)		3300 Byte	wie oben

Werden Ressourcen im Netzwerk zur Verfügung gestellt, senden die Computer, auf denen die Ressourcen enthalten sind, alle 12 Minuten eine Ankündigung. Diese Computer werden dann der

Suchliste hinzugefügt. Damit Clients auf diese Ressourcen zugreifen können, fragen diese zuerst den Hauptsuchdienst und dann den Sicherungssuchdienst nach der Liste der verfügbaren Ressourcen ab. Router können meistens keine Suchdienstbroadcasts in Subnetze weiterleiten. Nur durch den Einsatz von WINS wird unternehmensweit nach Ressourcen gesucht.

Verringern des Datenverkehrs:

Der Datenverkehr kann dadurch verringert werden, dass bei NT-Computern, die keine Ressourcen im Netz zur Verfügung stellen, der Server-Dienst deaktiviert wird. Dadurch werden keine Ankündigungen mehr gesendet. Bei Win-95/98-Computer kann die Datei- und Druckerfreigabe deaktiviert werden, um das gleiche Ziel zu erreichen. Bei Win-3.x-Computer kann der Eintrag „MaintainServerList“ in der System.ini auf NO gesetzt werden. Nicht benötigte Protokolle sollten deaktiviert oder entfernt werden, da die Suchdienste für jedes Protokoll extra angelegt werden.

b) DNS

DNS-Server lösen Internet-Namen zu IP-Adressen auf. Dazu befragen Clients einen DNS-Server nach der IP-Adresse eines Computers. Der Datenverkehr, der von DNS verursacht wird, ist von der Anzahl der Clientanforderungen abhängig. Bei DNS-Abfragen wird vom Server nur die IP-Adresse des Computers zurückgeliefert. Bei rekursiven DNS-Abfragen befragen DNS-Server andere DNS-Server, wenn sie die Namen nicht selber auflösen können.

Datenverkehr:			
Namensabfrage	2 Rahmen	180 Byte	jede Namensauswertung
Replikation von Zonen	4 Rahmen	200 Byte	beim Hinzufügen

			eines sek. DNS-Servers zur Zone und alle 60 Minuten
Integration von WINS	4 Rahmen	240 Byte	jede nicht lokale Namensabfrage

Verringern des Datenverkehrs:

Der Datenverkehr durch DNS kann dadurch verringert werden, in dem die rekursiven Abfragen unterbunden werden. Nachteil: Auf dem ersten DNS-Server müssen alle Hosts bekannt sein. Weiter sollte jedem Client ein spezieller DNS-Server zugewiesen werden, so dass nur dieser die Abfragen beantwortet. Des Weiteren kann der TTL-Wert von Einträgen im Cache erhöht werden (im DNS-Manager).

c) Internet/Intranet

Wird eine WEB-Site aufgerufen, wird vorher eine Namensauflösung des WEB-Servers via DNS durchgeführt. Die WEB-Site selber sowie darauf enthaltene Grafiken müssen übertragen werden. Alle diese Inhalte sind einzelne Dateien, so dass für jede Dateiübertragung eine neue TCP-Sitzung eröffnet werden muss. Der WEB-Server wiederum, muss die angeforderte Seite bestätigen, wenn er diese verfügbar hat.

Datenverkehr:			
Verbindung zu einer WEB-Site	2 Rahmen	180 Byte	jede Verbindung zum Server
Anfordern der WEB-Site	2 Rahmen	360 Byte	öfters pro Site
Sicherheit	verschieden	verschieden	öfters pro Site

Sind anonyme Zugriffe auf den WEB-Server erlaubt, werden keine weiteren Daten übertragen. Werden Sicherheitsinformationen durch Benutzername und Kennwörter verlangt, wird der Datenverkehr entsprechend erhöht.

Verringern des Datenverkehrs:

Der Datenverkehr kann für das Internet/Intranet nur durch das Verringern der Inhalte von WEB-Sites, durch das Verkleinern von Grafiken auf WEB-Sites, durch anonyme Zugriffsmethoden und durch das Erweitern des Caches für WEB-Seiten auf dem lokalen Computer verringert werden. Im Internet muss natürlich der Anbieter von WEB-Seiten diese Schritte ausführen.

Zu 3. Server zu Server

Netzwerkverwaltungsaufgaben erfordern Server-zu-Server-Verkehr.

Dieser beinhaltet

1. Kontensynchronisation von PDC zu BDC
2. Vertrauensstellungen zwischen Domänen
3. Serversuchdienst
4. WINS-Replikation
5. Verzeichnisreplikation
6. DNS-Server

a) Kontensynchronisation

Veränderungen an der Benutzerkontendatenbank (SAM) dürfen nur auf dem PDC durchgeführt werden. Da aber PDC wie BDC Benutzer im Netzwerk authentifiziert, müssen Veränderungen an der SAM regelmäßig auf den BDC repliziert werden.

Datenverkehr:			
Ermitteln des PDC	4 Rahmen	745 Byte	bei jedem BDC-Start
Sitzung einrichten	11 Rahmen	1280 Byte	jede Synchro-

			nisation
Sicherheitskanal einrichten	8 Rahmen	1550 Byte	bei jedem BDC-Start
Datenbank-überprüfung	6 Rahmen	1350 Byte	bei jedem BDC-Start
PDC-Aktualisierungs-nachricht	1 Rahmen	400 Byte	jede Synchro-nisation
Datenbank-Synchronisation	7 Rahmen	2000 Byte	jede Synchro-nisation

Die SAM wird immer nur teil-synchronisiert (nur aktualisierte Einträge). Vollständig wird die SAM nur aktualisiert, wenn

- ein neuer BCD installiert wird,
- Fehler bei der Teil-Sychronisation auftreten,
- auf dem BDC der Befehl NET ACCOUNT/SYNC ausgeführt wird.

Der Datenverkehr für die Synchronisation enthält aber noch

- Namensauswertung
- Adressauswertung
- TCP-Sitzung einrichten
- NetBIOS-Sitzung einrichten
- SMB-Protokollaushandlung
- Verbindung zu IPC$
- Sicherheitskanal zwischen PDC und BDC einrichten
- Überprüfung der Datenbank

Verringern des Datenverkehrs:

Eine Verringerung des Datenverkehrs kann nur über die Registry vorgenommen werden. Im Teilschlüssel
HKEY_LOCAL_MACHINE\SYSTEM\Current-

ControlSet\Services\ Netlogon\Parameters sollte der Parameter ReplicationGovernor verändert werden. Hier wird der prozentuale Anteil an der Bandbreite angegeben, der benutzt werden darf, um die SAM zu aktualisieren. Standardmäßig steht dieser Wert auf 100 % und sollte auf 50 % gesetzt werden.

b) Vertrauensstellungen

Vertrauensstellungen werden zwischen verschiedenen Domänen eingerichtet, z. B. zwischen einer Kontendomäne und einer Ressourcendomäne. Dabei verursacht das Einrichten der Vertrauensstellung viel Datenverkehr, aber auch wenn vertraute Konten verwendet werden, um einem Benutzer Zugriff auf eine lokale Ressource zu ermöglichen, oder wenn einer lokalen Gruppe ein vertrautes Konto hinzugefügt wird.

Des Weiteren betrifft dieser Datenverkehr den Zugriff von Benutzern auf Ressourcen von vertrauenden Domänen.

Datenverkehr:			
Einrichten der Vertrauensstellung	110 Rahmen	16000 Byte	einmalig
Importieren von Konten	110 Rahmen	16000 Byte	bei jedem Importversuch
Durchgängige Echtheitsbestätigung	20 Rahmen	3200 Byte	jeder Zugriff eines Servers auf die Vertrauende Domäne

Verringern des Datenverkehrs:

Der Datenverkehr kann dadurch verringert werden, dass nicht benötigte Vertrauensstellungen aufgehoben werden.

c) Serversuchdienst

Alle Computer, die den Serverdienst installiert haben und Ressourcen im Netzwerk freigeben, teilen Ankündigungen in der eigenen Domäne an den Suchdienst mit. Computer, die als Suchdienst, Sicherungssuchdienst oder Hauptsuchdienst in der Domäne agieren, nehmen zudem an der Suchdienstauswahl teil, wenn kein Suchdienst im lokalen Subnet gefunden wurde. Des Weiteren betrifft den Datenverkehr des Suchdienstes auch die Kommunikation mit anderen Hauptsuchdiensten in anderen Domänen.

Datenverkehr:			
Hostankündigung	1 Rahmen	243 Byte	pro Server alle 12 Minuten
Ankündigung durch den lokalen Suchdienst	1 Rahmen	250 Byte	jede Ankündigungsanforderung und alle 12 Minuten
Ankündigung durch eine Arbeitsgruppe	1 Rahmen	250 Byte	pro Hauptsuchdienst bei jeder Ankündigung und alle 15 Minuten
Auswahl	20 Rahmen	5300 Byte	jeder Neustart eines DC’s
Austausch der Suchliste	36 Rahmen	3900 Byte	jede Suche eines Clients und alle 12 Minuten durch den Sicherungssuchdienst

Ein PDC übernimmt innerhalb einer Domäne den Hauptsuchdienst, ein BDC den Sicherungssuchdienst. Wenn kein PDC vorhanden ist, übernimmt der BDC den Hauptsuchdienst. Alle 15 Minuten werden Ankündigungen von allen Hauptsuchdiensten aller Domänen und Subnets an alle Hauptsuchdienste gesendet. Domänenhauptsuchdienste müssen alle 12 Minuten eine Abfrage an WINS stellen, welche Domänen vorhanden sind. Alle Hauptsuchdienste müssen alle 12 Minuten eine Aktualisierung der Suchliste beim Domänenhauptsuchdienst anfordern. Alle Sicherungssuchdienste müssen alle 12 Minuten eine Aktualisierung der Suchliste beim lokalen Hauptsuchdienst anfordern.

Verringern des Datenverkehrs:

Da diese Suchvorgänge für jedes installierte Protokoll durchgeführt wird, sollten nicht benötigte Protokolle deinstalliert werden. Auch sollten alle Computer, die keine Ressourcen im Netzwerk freigeben, keinen Serverdienst installiert haben.

d) WINS-Replikation

Von einem WINS-Server können ca. 10000 Clients verwaltet werden. Da ein einzelner WINS-Server aber keine Fehlertoleranz bietet, ist es sinnvoll, min. 2 WINS-Server in einem Netzwerk einzusetzen, die ihre Datenbank regelmäßig abgleichen. Auf diese Weise wird eine WINS-Abfrage von einem Client auch schneller beantwortet. Nachteil: Replikationsverkehr zwischen WINS-Servern, der in seiner Größe vom Umfang der Datenbank sowie der Häufigkeit der Replikation abhängig ist.

Datenverkehr:			
Festlegen eines Replikations-partners	20 Rahmen	2300 Bytes	pro Replikations-partner

Datenbank-überprüfung	12 Rahmen	900 Bytes	pro Aktualisierungsanforderung für jeden Replikations-partner
Datenbank-aktualisierung	14 Rahmen	1200 Bytes	pro Aktualisierungsanforderung für jeden Replikations-partner

Bei der Replikation zwischen WINS-Servern werden die Replikationspartner festgelegt, die Datenbankversionsnummer überprüft sowie die Einträge der Datenbank repliziert.

Verringern des Datenverkehrs:

Push-Partner teilen ihren Pull-Partnern mit, wenn sich eine bestimmte Anzahl von Änderungen an der Datenbank ergeben haben. Pull-Partner fordern eine Aktualisierung der Datenbank durch ihre Pull-Partner an, die in einem konfigurierbaren Intervall abläuft. WINS-Server können auch beide Funktionen gleichzeitig inne haben.

Die Anzahl der Änderungen, bei denen eine Replikation zu den Push-Partnern einsetzt, kann im WINS-Manager erhöht werden. Ebenfalls kann der Zeitintervall, bei dem eine Anforderung eines Pull-Partners erfolgt, erhöht werden.

e) Verzeichnisreplikation

Eine Verzeichnisstruktur oder Dateien unter NT können zwischen verschiedenen Computern repliziert werden. Z.B. sollten die Logon-Scripten von Benutzern vom PDC auf alle BDC’s repliziert werden, da nicht sicher gestellt ist, welcher Computer die Anmeldung eines Benutzers vornimmt.

Datenverkehr:

Ankündigung	1 Rahmen	340 Byte	pro Importdomäne oder -server, bei jeder Aktualisierung der Struktur
Einrichten einer Sitzung	11 Rahmen	1280 Byte	pro Importcomputer, bei jeder Aktualisierung
Verzeichnis-überprüfung	30 Rahmen	5100 Byte	pro Importcomputer, bei jeder Aktualisierung
Verzeichnis-aktualisierung	verschieden		pro Importcomputer, bei jeder Aktualisierung

Verringern des Datenverkehrs:

Der Datenverkehr kann z. B. durch eine Verzeichnisstruktur verringert werden, die nicht sehr umfangreich gehalten wird. Auch über die Registry unterHKEY_LOCAL_MACHINE\SYSTEM\CurrentControl-Set\Services\Replicator\Parameters können Veränderungen vorgenommen werden.

Intervall: Hier kann eingestellt werden, wie oft der Export-Server die Verzeichnisstruktur auf Veränderungen überprüft.

Pulse: Hier kann die Zeitspanne erhöht werden, wann ein Importcomputer einen Exportcomputer nach einer Aktualisierung fragt.

f) DNS

Namensauswertungen in größeren Unternehmen bedingen meistens einen primären und einen sekundären DNS-Server. Da beide miteinander kommunizieren müssen und auch eine Replikation der Da-

tenbank zwischen der primären und der sekundären Zone erfolgen muss, entsteht hierbei viel Datenverkehr.

Datenverkehr:			
Namensabfrage Clientanforderung	2 Rahmen	180 Byte	jede
Zonen-replikation	3 Rahmen	180 Byte	periodisch alle 60 Min.
Replikations-anforderung	2 Rahmen	403 Byte	jede Clientanforderung
Beenden der Sitzung	2 Rahmen	240 Byte	jede Clientanforderung

Verringern des Datenverkehrs:

Der Datenverkehr kann dadurch verringert werden, indem im DNS-Manager das Aktualisierungsintervall für die Zonenreplikation verlängert wird.

Server-Cluster:

Server-Cluster sind in heutigen Netzwerken unausweichlich, um das Netzwerk gegen Ausfälle zu sichern. Mit den Servern steht und fällt weitestgehend das Netz. Ausfälle können Firmen beträchtliche Summen kosten, wenn dadurch der normale Arbeitsablauf beeinträchtigt ist, in Krankenhäusern können Leben von der konstanten Verfügbarkeit der Server abhängig sein.

Unter einem Server-Cluster wird der Zusammenschluss mehrerer Server zu einem System verstanden, das nach außen hin wie *ein* Server erscheint. Fällt eines der Cluster-Mitglieder (Node) aus, übernehmen die anderen seine Aufgaben. Cluster haben gegenüber herkömmlichen Sicherungsmethoden, wie z. B. Plattenspiegelung,

RAID-Systemen, etc., eine sehr viel größere Ausfallsicherheit. Einzelne Server erreichen statistisch eine Ausfallsicherheit von 99 % (3,7 Tage pro Jahr Ausfall), WS's eine von 95 % (18 Tage Ausfall). Server-Cluster können eine Ausfallsicherheit von 99,99 % haben (50 Min pro Jahr Ausfall).

Serverspiegelungen sind die einfachste Form von Server-Clustern. Dabei bleibt der Backup-Server solange passiv, bis der primäre Server ausfällt. Realisiert werden können Serverspiegelungen
über den dauernden Transfer von Daten zwischen beiden Servern, oder beide Server greifen auf ein gemeinsames externes RAID-System zu.

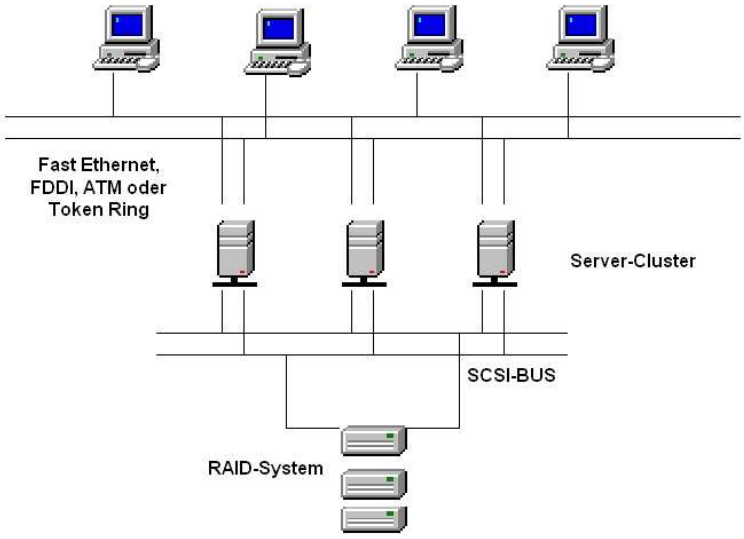


Abb. 22 Server-Cluster

Modernere Cluster bestehen aus mehreren Servern, die auf ein externes RAID-System zugreifen und über ein separates Netzwerk (Fast Ethernet, FDDI oder ATM) miteinander verbunden sind. Eine spezielle Software liefert die nötige Intelligenz des Clusterings. Fällt ein Server aus, übernimmt ein anderer aus dem Cluster die Arbeit. Ist der ausgefallene Server wieder

betriebsbereit, kann dieser entweder wieder an seinen alten Platz zurückkehren (Netzwerk wird 2x unterbrochen, beim Ausfall und bei der Wiedereingliederung), oder der andere Server bleibt der Hauptserver, bis dieser ausfällt (Netzwerk wird nur einmal unterbrochen) und wieder ein anderer die Arbeit übernimmt (rotierende Cluster).

Cluster-Lösungen sind zwischenzeitlich für alle gängigen Server-Betriebssysteme zu haben (Win NT4/2000, Novell-Netware, Unix).

SAN (Storeage Area Network):

Über LANs sind Zugriffe auf lokale Host-Systeme möglich, die über LAN-Protokolle wie TCP/IP, IPX oder HTTP verbunden sind. Sie werden benutzt, um z. B. Benutzerzugriffe von Workstations aus auf Server zu ermöglichen.

SANs sind besondere Speichersysteme, die Server und Speichersysteme (z. B. einen Pool aus Bandlaufwerken und die Server) über Breitbandnetzwerke miteinander verbinden. Dazu werden alle Systeme in einem Netzwerk und darüber hinaus auch die Speichereinheiten, die zur Sicherung von Daten oder ganzer Rechner-Systeme benutzt werden, unter ganz bestimmten Topologien miteinander verbunden, ähnlich, wie LANs z. B. unter
Ethernet, Token Ring, etc. aufgebaut werden. Das Betriebssystem, das auf einem Server installiert ist, ist dabei erst einmal unwichtig, da alle Server auf das Speichersystem zugreifen können.

SANs werden heute überwiegend über Fibre Channel realisiert (siehe auch 1.2.10 BUS-Systeme, serielle BUS-Systeme, Fibre Channel), da die Einschränkungen, die z. B. SCSI mit sich bringt (Geräteanzahl, Distanzen, etc.) in modernen SANs nicht mehr zu akzeptieren sind.

Fibre Channel in SANs bietet folgende Vorteile:

- Datendurchsatz 400 MB/s

- Bandbreite 2.0625 Gbit
- Max. Geräte 16 Millionen
- Ser. Verbindung 8/10-bit-Encoding
- Kabel flexibel (Kupfer, Glasfaser)
- Protokoll Hardware basierend
- LANs werden durch SANs entlastet

Datentransferraten von 2–4 GBaud werden für Fibre Channel für die Zukunft realisiert werden können.

Einfache SAN-Verbindungen beinhalten nur eine Punkt-zu-Punkt-Verbindung, z. B. ein RAID-System mit einem Server. Komplexere SAN-Verbindungen können über eine Ring Topologie, die Switches oder HUB's beinhalten kann, aufgebaut werden (FC-AL genannt (Fibre Channel Arbitrated Loop)), die mehrere Server mit mehreren Speichersystemen verbinden kann. Kupferkabel über geringe Distanzen (30 m) oder Glasfaserkabel können hierbei zum Einsatz kommen.

In einem SAN muss auch eine spezielle Software laufen, die ein File-Sharing auf dem Speicher-Subsystem ermöglicht, so dass jedes System, unabhängig vom Betriebssystem, auf die Speichereinheit zugreifen kann. Diese Software ist sozusagen ein SAN-Betriebssystem, welches unabhängig von normalen Betriebssys-

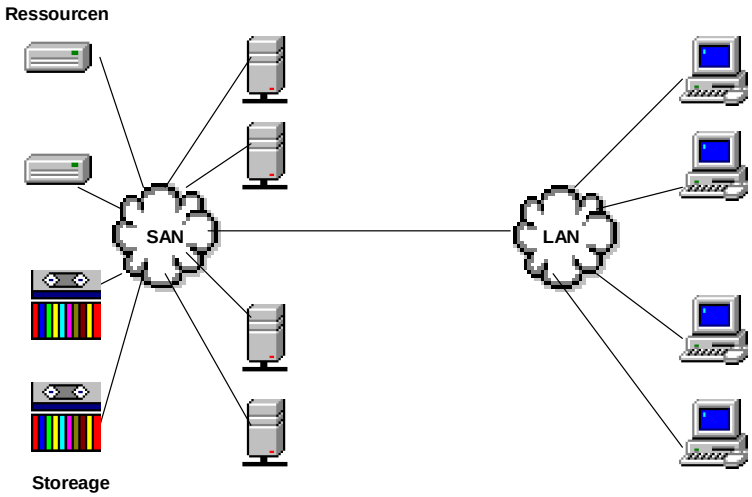


Abb. 23 SAN

temen ist und auf diese aufsetzt. Mittels diesem Betriebssystem können z. B. Speichereinheiten einem Server zugewiesen, Spiegelungen erstellt, Server-Clustering einbezogen werden oder im Fehlerfall Backup-Pfade zur Verfügbarkeit der Systeme aut. konfiguriert werden.

2.1.19 WAN-Technologien

Unternehmen sind immer häufiger nicht nur an einem Standort ansässig. Damit der Geschäftsablauf, der die EDV eines Unternehmens betrifft, trotzdem reibungslos funktioniert, müssen Verbindungen der einzelnen Standorte eines Unternehmens über öffentliche Telefonkabel hergestellt werden. Die Verbindung von Netzwerken über öffentliche Telefonkabel sind WAN-Verbindungen. Diese können natürlich auch über Richtfunk oder Satellit eingerichtet werden, was in vielen Firmen auch zum Einsatz kommt. Telefonverbindungen sind jedoch der weitaus gebräuchlichste Teil von WAN-Verbindungen.

WAN-Verbindungen können über das Anwählen einer solchen Verbindung bei Bedarf (Kosten fallen nur an, wenn die Verbindung aktiv ist), oder über sogenannte „Standleitungen“ hergestellt werden. Standleitungen werden von Unternehmen bei einer Telefongesellschaft für den dauernden Einsatz gemietet.

Für WAN-Verbindungen gibt es eine Reihe von verschiedenen Technologien, die sich in ihrer Übertragungsgeschwindigkeit, und damit natürlich auch in den Kosten unterscheiden.

Standleitungen:

T1

T1 ist eine digitale Leitungsform, die eine Punkt-zu-Punkt-Verbindung darstellt. Über T1 können 24 Kanäle über 2 Adernpaare übertragen werden, wobei ein Adernpaar für das Senden und das andere Adernpaar für das Empfangen verwendet wird. Die Übertragungsgeschwindigkeit von T1 beträgt 1,544 Mbit/s.

T3

T3 bietet die gleiche Technologie wie T1, kann aber mit Übertragungsgeschwindigkeiten von 45 Mbit/s arbeiten.

DS-0

Da meistens die 24 Kanäle von T1/T3 nicht benötigt werden, können diese Kanäle auch aufgeteilt werden. Wenn einer dieser Kanäle dazu verwendet wird, 64 kBit/s zu übertragen, spricht man von einer DS-0-Verbindung.

DS-1, DS-1C, DS-2, DS-3

Dies sind weitere Aufteilungen von T1- oder T3-Kanälen.

DDS

DDS ist ebenfalls eine Punkt-zu-Punkt-Verbindung, die mit 2,4 , 4,8 oder 5,6 kBit/s arbeiten kann.

WAN-Protokolle:

Da es u. U. für viele Firmen zu teuer sein kann, zu jedem Standort eine Standleitung einzurichten, werden oftmals sog. Paketvermittlungsdienste eingesetzt, über die Datenpakete zwischen Standorten ausgetauscht werden können. Diese Dienste können über Mietleitungen bei einem Service-Provider bezogen werden. Die Kosten hierfür sind wesentlich geringer als über Standleitungen.

Paketvermittlungsdienste arbeiten oft mit virtuellen Verbindungen. Diese stellen einen ganz bestimmten Weg durch das Netz dar (Pakete suchen sich den Weg nicht selber). Dieser virtuelle Weg wird ganz gezielt für *eine* Übermittlung von Daten hergestellt, der bei der nächsten Übermittlung wieder ein ganz anderer sein kann.

X.25

X.25 ist in WAN-Umgebungen sehr verbreitet und kann dauerhafte oder geschaltete virtuelle Verbindungen benutzen. Diese untersteht einer Ende-zu-Ende-Flusskontrolle für jede virtuelle Verbindung, da X.25 bei seiner Entwicklung unzuverlässige Telefonleitungen vorfand. Die Übertragungsgeschwindigkeiten von X.25 liegen bei 64 kBit/s. X.25 eignet sich nicht für die Bereitstellung von LAN-Anwendungen in einer WAN-Umgebung und hat viele Einschränkungen.

Frame Relay

Frame Relay bezieht sich auf Glasfaser-Netze, unterstützt B-ISDN und arbeitet mit dauerhaften virtuellen Verbindungen. Die Übertragungsgeschwindigkeiten von Frame Relay liegen zwischen 56 kBit/s und 1,544 Mbit/s (T1). Frame Relay wird an Kunden mit einer gewissen Bandbreite (Übertragungsgeschwindigkeit) verkauft. Es arbeitet nur mit frame-relay-fähigen Netzwerkgeräten (z.B. Frame-Relay-Router).

ISDN

ISDN kann bei Verbindungen mit hohen Bandbreiten mehrere Kanäle verwenden und ist ein Wähldienst, keine dauerhafte Verbindung. Es überträgt digitale Signale über herkömmliche Telefonleitungen. Dabei kann Basis-ISDN die Kanäle in 2 B-Kanäle (je 64 kBit/s) und 1 D-Kanal (16 kBit/s) auf. Der D-Kanal übermittelt Verbindungs- und Signalisierungsinformationen. Die B-Kanäle übermitteln Daten. Beide B-Kanäle können gleichzeitig zum Übertragen von Daten verwendet werden, wodurch eine Übertragungsgeschwindigkeit von 128 kBit/s entsteht. Primary-Rate-ISDN kann mit 23 B-Kanälen von je 64 kBit/s und 1 D-Kanal mit 64 kBit/s arbeiten.

B-ISDN

Breitband-ISDN ist eine Neuerung von ISDN und ist überwiegend für die Übertragung von Sprach-, Video- und Audio-Daten gedacht. B-ISDN arbeitet eng mit ATM zusammen und hat übliche Übertragungsraten von 51 Mbit/s, 155 Mbit/s und 622 Mbit/s

DSL (Digital Subscriber Line, digitale Teilnehmeranschlussleitung):

- ADSL (Asymmetric Digital Subscriber Line)
- TDSL (Telekom Digital Subscriber Line, Vermarktung der Telekom AG ihrer ADSL-Anschlusstechnologien)
- DSL Light (langsameres ADSL für längere Strecken)
- HDSL (High Date Rate Digital Subscriber Line, über Telefonleitungen in beiden Richtungen bis zu 2 MBit/s. Ermöglicht die schnelle Kopplung von lokalen Netzwerken.)
- SDSL (Single Line Digital Subscriber Line, wie HDSL, auf einfacher Leitung.

- VDSL (Very High Date Rate Digital Subscriber Line, ermöglicht Übertragungsraten von mehr als 50 MBit/s über sehr kurze Verbindungen zwischen Netzknoten und Endgeräten oder über Glasfaser)

DSL-Techniken bilden auf der Basis von Kupferadern digitale Datenleitungen zwischen Vermittlung und Kundenanschluss. Dabei wird ein weitaus größeres Frequenzspektrum als bei analogen bzw. ISDN-Übertragungen genutzt. Die Übertragung erfolgt über herkömmliche Kupferleitungen.

Die Unterschiede zwischen den DSL-Techniken bestehen zum einen aus der Anzahl der verwendeten Kupferpaare, zum anderen aus den verwendeten Übertragungsfrequenzen bzw. den Modulationsverfahren. ADSL verwendet nur ein Kupferpaar und kann über herkömmliche Telefonleitungen betrieben werden. Da ADSL eine höhere Frequenz verwendet, kann Telefonie, wie bei ISDN, nebenher betrieben werden. Eine Frequenzweiche beim Kunden und in der Vermittlungsstelle trennen die jeweiligen Datenströme.

ADSL kann sehr hohe Übertragungsraten erzielen, wenn eine genaue Einmessung des Kabels erfolgt. Dies wird von Anbietern aus Kostengründen aber meistens vermieden, wodurch normalerweise eine sichere Übertragungsrate von 896 kBit/s beim Endkunden verwendet wird.

ADSL arbeitet nicht mit für Modems herkömmlichen Bitströmen, sondern mit Paketen. Diese Pakete können Daten einer übergeordneten Netzwerkschicht enthalten (ATM, Ethernet, IP, usw.), wobei die Frames gleich im ADSL-Modem verpackt werden. TDSL bietet gar eine Ethernet- bzw. ATM-Schnittstelle.

Asymmetric-DSL bedeutet, dass Hin- und Rückkanal jeweils unterschiedlich große Datenmengen transportieren. Beim Surfen im Internet wird beim Upstream (Hochladen von Adressen zum Provider) über den Rückkanal eine Geschwindigkeit bis zu 768 Kilobit erreicht. Beim Downstream

(Runterladen von Daten aus dem Internet) bis zu 9 Megabit über den größeren Hinkanal.

Name	Max. Datenrate (Download)	Max. Entfernung zur Vermittlungs-stelle
ADSL	1,5–9 Mbit/s	bis 5,5 km
DSL lite	1,5 Mbit/s	bis 5,5 km
HDSL	1,5–2 Mbit/s	bis 4 km
SDSL	768 Kbit/s	bis 3,5 km
VDSL	13–52 Mbit/s	bis 14 km
zum Vergleich: ISDN	128 Kbit/s	bis 5,5 km

2.1.20 Drucken im Netzwerk (Print-Server)

Jeder Benutzer in einem Büro benötigt meistens keinen eigenen Drucker an seinem PC. Deswegen kann in kleineren und mittleren Büroumgebungen mit einem PC-Netzwerk ohne weiteres auch ein vorhandener File- oder Anmelde-Server als Print-Server eingerichtet werden. Die Benutzer schicken ihre Druckaufträge an den Print-Server, an dem ein Drucker angeschlossen ist und von dem der Druckauftrag dann an den Drucker weiter gegeben wird.

Müssen sich in einer größeren Büroumgebung jeweils nur 2 Benutzer einen Drucker teilen, bietet sich die Lösung einer hardwaremäßigen Druckerweiche an, die einfach zwischen die PC’s und dem (den) Drucker (Druckern) angeschlossen wird. Auch manuelle Umschalter (Switch-Boxen) können noch für 2–6 PC’s zu einem Drucker oder 1 PC zu 2–6 Druckern verwendet werden (ist aber umständlich).

Alle diese Lösungen haben allerdings den Nachteil, dass jeder auf diesen Druckern drucken kann. Eine Verwaltung von Rechten, wer was darf, gibt es weitestgehend nicht.

Abb. 24 Druckerweiche

Eine weitere und durchaus bessere Möglichkeit stellt der Einsatz von anderen Print-Servern dar. Intel, HP oder D-Link z. B. bieten solche Print-Server an, mittels derer über das Netzwerk gedruckt werden kann und die sich in Umgebungen mit Netware, NT oder Unix problemlos einpassen. Diese Print-Server können für IPX oder TCP/IP eingerichtet werden oder gar mit beiden Protokollen gleichzeitig arbeiten. Auch als LPR-Server sind sie zu verwenden. Druckwarteschlangen können auf einem Netware- oder NT- oder Unix-Server abgelegt und verwaltet werden. Eine Begrenzung der Anzahl von Benutzern, die auf diese Print-Server zugreifen können, gibt es nicht, so dass sie sich problemlos an bestehende Situationen anpassen lassen. Parallele und serielle Drucker können daran verwendet werden.

Diese Art von Print-Servern gibt es als externes Gerät (kleiner, meist grauer Kasten) oder als internes Gerät (Steckkarte, die in einen Drucker eingebaut wird). Im Nachfolgenden soll hier ein externes Gerät beschrieben werden.

Abb. 25 Switch-Box

Abb. 26 Print-Server von Intel

Die Verwaltung solcher Print-Server kann von Administratoren über ein spezielles Verwaltungsprogramm vorgenommen werden, und es kann genau festgelegt werden, welche Benutzer/ Gruppen auf einem solchen Print-Server drucken können.

Der Einsatz solcher Print-Server im Netzwerk gestaltet sich relativ unproblematisch, da diese Geräte einfach an einen HUB (10/100 BASE T) oder ein T-Stück (10 BASE 2) angeschlossen werden können, wo sie gerade benötigt werden.

Da es viele Firmen gibt, die solche Print-Server anbieten, können hier natürlich nicht alle Varianten besprochen werden. Aber anhand des sehr weit verbreiteten Intel NetportExpress PRO soll hier näher auf Anschluss und Konfigu-

ration solcher Print-Server eingegangen werden, die sich alle nicht wesentlich unterscheiden.

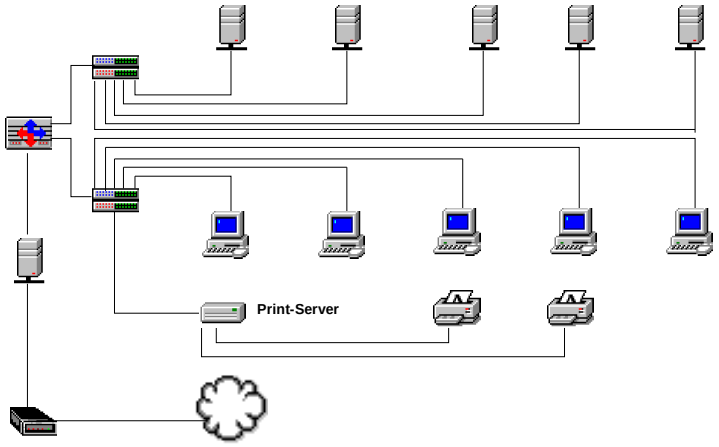


Abb. 27 Netzwerk mit Print-Server

Installation der Hardware:

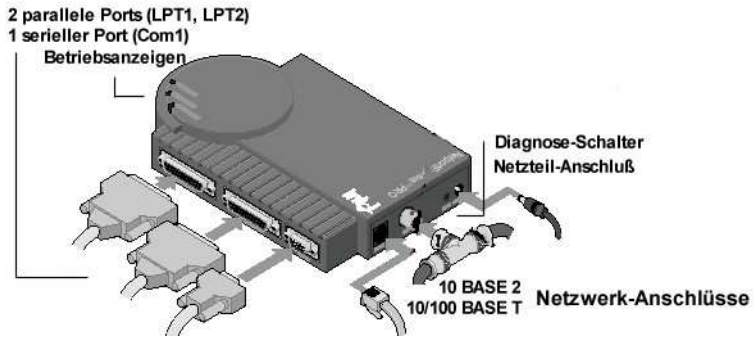


Abb. 28 Anschlüsse des Intel NetportExpress PRO

Ist der Print-Server hardwaremäßig installiert und sind alle Installationen richtig gemacht worden, muss die Betriebsanzeige grün aufleuchten. Leuchtet sie rot, stimmt etwas mit der Installation oder dem Netzwerk nicht (Troubleshooting in HLP-Datei lesen).

Installation der Software:

Nach der Hardwareinstallation muss der Print-Server nun softwaremäßig konfiguriert werden. Intel liefert dazu eine Management-Software, die auf einer Verwaltungsworkstation unter Windows (oder Unix) im Netzwerk installiert werden kann, wozu das Setup-Programm ausgeführt werden muss. Diese Management-Software kann bei Intel auch für das Inter-/Intranet herunter geladen werden, wodurch der Print-Server über das WEB/ Netzwerk im HTML-Format konfiguriert werden kann.

Achtung: Ist auf der Verwaltungsworkstation ein deutscher Novell-Client32 installiert, überschreibt der englische Netport-Manager Dateien mit der engl. Version. Beim Neustart der WS wird dann ein Codeseitenkonflikt angezeigt, der alle NDS-Services deaktiviert, woraufhin der Netport-Manager nicht zu starten ist. Es muss dann der deutsche Client32 nochmals installiert werden, der den vorigen Zustand wieder herstellt. Der Netport-Manager kann aber jetzt gestartet werden.

Noch sehr weit verbreitet ist der Netport-Manager in der Version 4.x, der aber nur in einer 16-Bit-Version verfügbar ist (Win 3.x und Win 95). Dieser kann durch die Version 5.x ersetzt werden, der eine 32-Bit-Version darstellt (Win9.x, NT) und mehr Möglichkeiten für die Konfiguration des Print-Servers bietet (vom Intel-Server downloaden, www.intel.de).

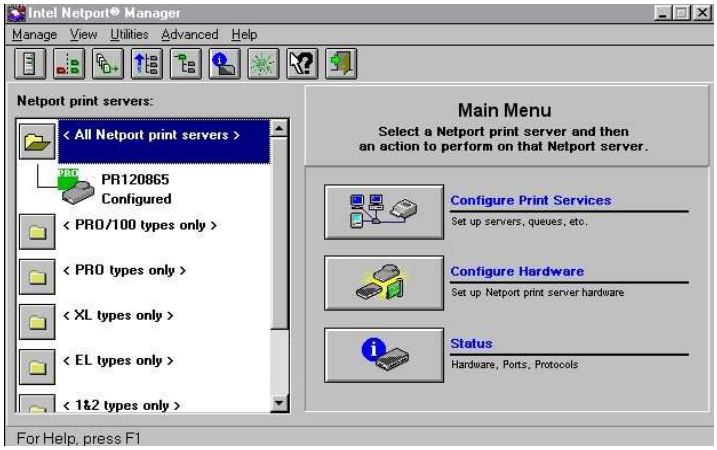


Abb. 29 Netport-Manager Ver. 4

Nach Aufruf des Netport-Managers in der Version 5 bietet sich einem folgendes Bild:

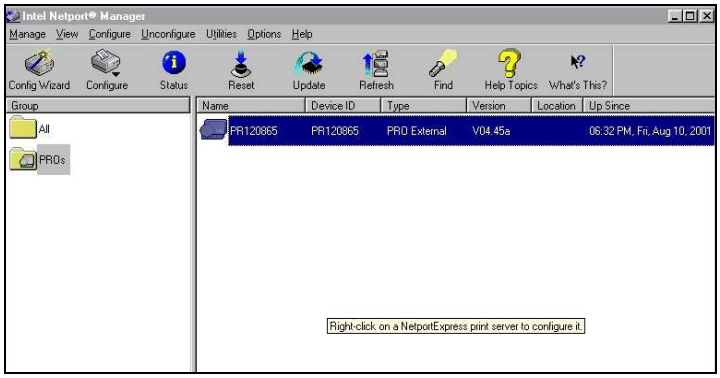


Abb. 30 Netport-Manager Ver.5

Hier ist jetzt nur ein Print-Server aufgeführt, der zur Erklärung ausreicht. In einem großen Netz, wo viele solcher Print-Server vorhanden sind, werden hier alle Print-Server aufgeführt, da der Netport-Manager das Netzwerk beim Start nach vorhandenen Geräten durchsucht. Aber nur nach den eigenen. Jede Firma hat entsprechend ihre Managament-Software, die nur nach den eigenen Geräten sucht. Sind also Geräte verschiedener Firmen im Netz, müssen diese jeweils un-

ter Verwendung der firmeneigenen Software extra konfiguriert werden.

Update:

Die Print-Server sind mit einer internen Software ausgestattet, die meistens beim ersten Start des Netport-Managers „geupdatet“ werden muss. Der Netport-Manager bietet das Update auch meisten an, so dass nur der Vorschlag zum Update übernommen werden sollte.

Konfiguration:

Der Print-Server kann für folgende Aufgaben konfiguriert werden:

- Novell NDS Print-Server
- Novell NDS Remote-Printer
- Novell Bindery Print-Server
- Novell Bindery Remote-Printer
- Microsoft Network Printing
- IBM LAN-Server
- TCP/IP and SMNP
- Apple Talk

Nachfolgend sollen hier nur die gängigsten Konfigurationen besprochen werden.

Über den Netport-Manager kann der Print-Server entweder manuell oder über einen Konfigurationswizzard konfiguriert werden. Da es für das Verständnis der Vorgänge sinnvoll ist, die manuelle Version zu beherrschen, soll diese hier zuerst besprochen werden. Am Schluss dieses Abschnittes wird dann noch auf den Wizard eingegangen.

Konfigurieren für Novell-NDS im NDS-Druckserver-Modus:

Das Konfigurieren von Netport Print-Server-Einstellungen bedarf keinerlei Einstellungen unter dem NWAdmin von Novell. Alle Einstellungen können über den Netport-Manager gemacht werden.

Im NDS-Druckserver-Modus ersetzt der NetportExpress Print-Server das NetWare-Druckserverprogramm. Dabei werden die Warteschlangen des Netware-Servers vom Print-Server abgefragt und direkt an den Drucker gesendet, was den Druckvorgang beschleunigt.

Konfiguriert wird dieser Modus über Rechte Maustaste über dem Print-Server | CONFIGURE PRINT SERVICES | NOVELL NDS PRINT-SERVER auswählen.

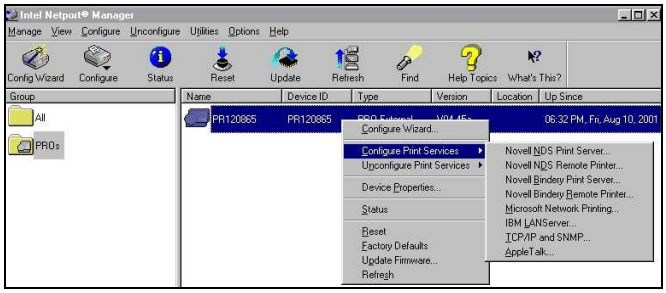


Abb. 31

Im daraufhin erscheinenden Dialogfeld muss auf der Registerkarte PRINT-SERVER der Kontext ausgewählt werden, in dem gearbeitet werden soll. Auch kann hier festgelegt werden, wie oft Warteschlangen nach Druckaufträgen gescannt werden. Des Weiteren kann ein Paßwort für den Zugriff auf den Print-Server festgelegt werden.

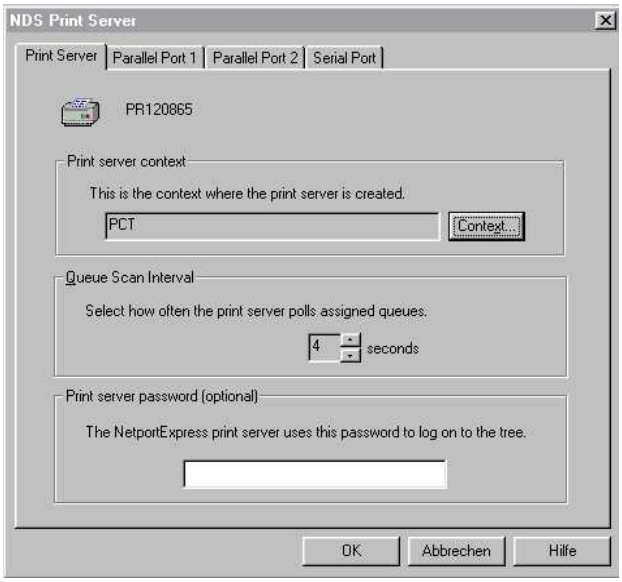


Abb. 32

Als nächstes muss nun festgelegt werden, über welche Warteschlangen welche Ports (angeschlossene Drucker) am Print-Server bedient werden sollen. Dazu ist auf der Registerkarte PARALLEL-PORT 1 (oder 2, oder SERIAL-PORT) eine vorhandene

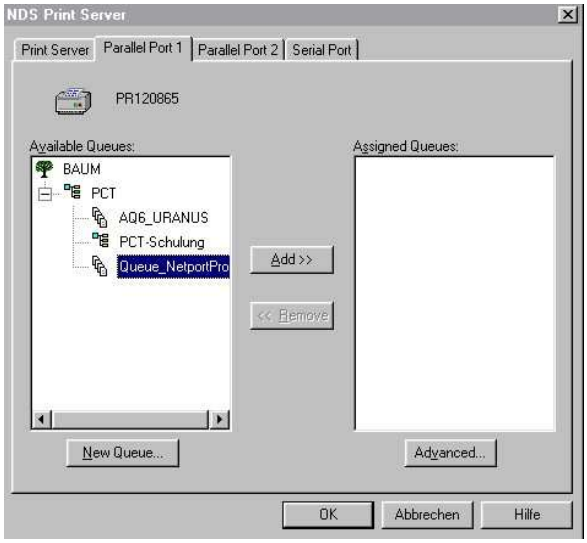


Abb. 33 Queue auswählen

Queue aus dem vorher festgelegten Kontext auszuwählen (ADD), oder über die Schaltfläche NEW QUEUE eine neue Warteschlange anzulegen. Es muss ein Volume ausgewählt werden, auf dem die Queue angelegt werden soll, und es muss ein Name für die Queue eingetragen werden.

Achtung: Diese Einstellungen müssen für jeden Print-Server gesondert gemacht werden.

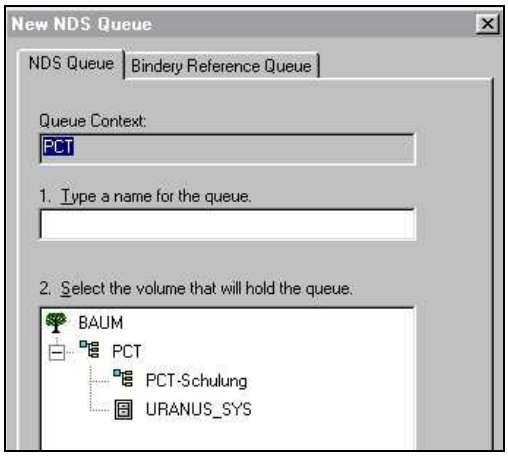


Abb. 34 Neue Queue anlegen

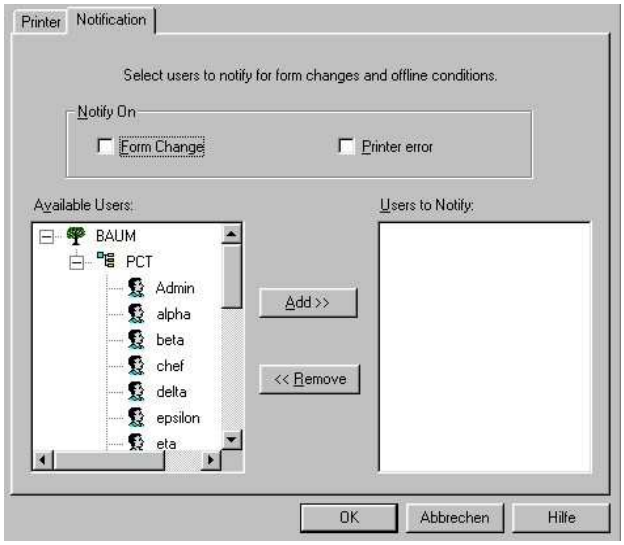


Abb. 35 Notification

Über die Schaltfläche ADVANCED können Benutzer festgelegt werden, die bei bestimmten Ereignissen benachrichtigt werden sollen.

Konfigurieren der Workstations für NDS (Win 9.x, NT):

Unter START | EINSTELLUNGEN | NEUER DRUCKER auswählen | NETZWERKDRUCKER auswählen | den entsprechenden NDS-Kontext auswählen | die Warteschlange auswählen | den Druckertreiber installieren lassen | den weiteren Anweisungen des Assistenten folgen.

Konfiguration für Novell Bindery Print-Server:

Das Konfigurieren von Netport Print-Server-Einstellungen bedarf keinerlei Einstellungen unter Novell. Alle Einstellungen können über den Netport-Manager gemacht werden.

Im Bindery-Druckserver-Modus ersetzt der NetportExpress Print-Server das NetWare-Druckserverprogramm. Dabei werden die Warte-

schlangen des Netware-Servers vom Print-Server abgefragt und direkt an den Drucker gesendet, was den Druckvorgang beschleunigt.

Konfiguriert wird dieser Modus über Rechte Maustaste über dem Print-Server | CONFIGURE PRINT SERVICES | NOVELL Bindery PRINT-SERVER auswählen.

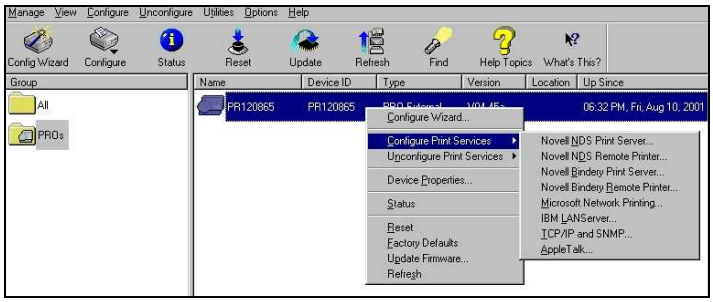


Abb. 36

In der daraufhin erscheinenden Dialogbox ist in der Registerkarte BINDERY PRINT-SERVER zuerst der Server auszuwählen, auf dem der Print-Server läuft. Des Weiteren kann auch hier eingestellt werden, wie oft die Warteschlange nach neuen Druckaufträgen gescannt werden soll. Auch ein Paßwort zum Konfigurieren des Print-Servers kann hier festgelegt werden.

Über die Registerkarte Parallel-Port 1 (2, oder Serial-Port) ist der Server und die Warteschlange auszuwählen (wenn schon vorhanden). Über die Schaltfläche NEW QUEUE kann eine neue Warteschlange eingerichtet werden, wobei der Server anzugeben ist, auf dem die Queue abgelegt werden soll, und deren Namen.

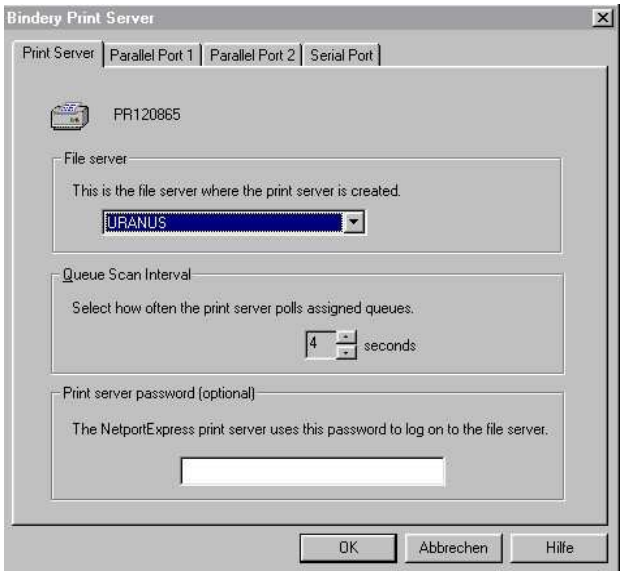

Bindery Print Server
Print Server
Parallel Port 1
Parallel Port 2
Serial Port
PR120865
File server
This is the file server where the print server is created.
URANUS
Queue Scan Interval
Select how often the print server polls assigned queues.
4
seconds
Print server password (optional)
The NetportExpress print server uses this password to log on to the file server.
OK
Abbrechen
Hilfe

Abb. 37

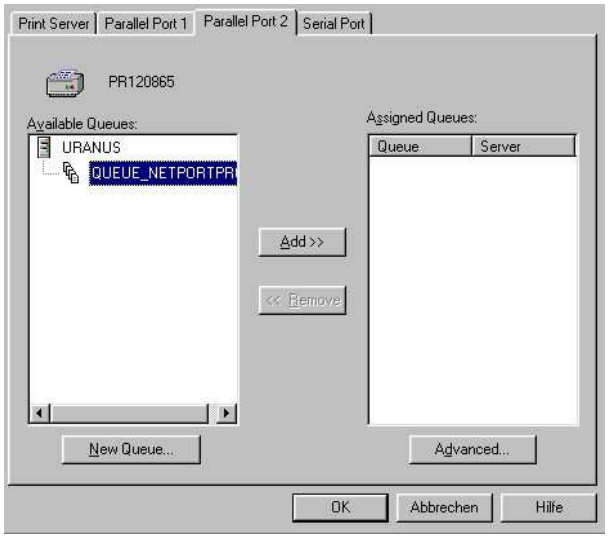

Print Server
Parallel Port 1
Parallel Port 2
Serial Port
PR120865
Available Queues:
URANUS
QUEUE_NETPORTPR
Add >>
<< Remove
Assigned Queues:
Queue
Server
New Queue...
Advanced...
OK
Abbrechen
Hilfe

Abb. 38

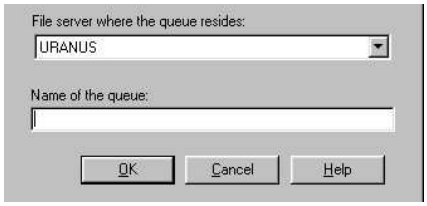


Abb. 39

Über die Schaltfläche NOTIFICATION können Benutzer ausgewählt werden, die bei bestimmten Ereignissen des Print-Servers benachrichtigt werden sollen.

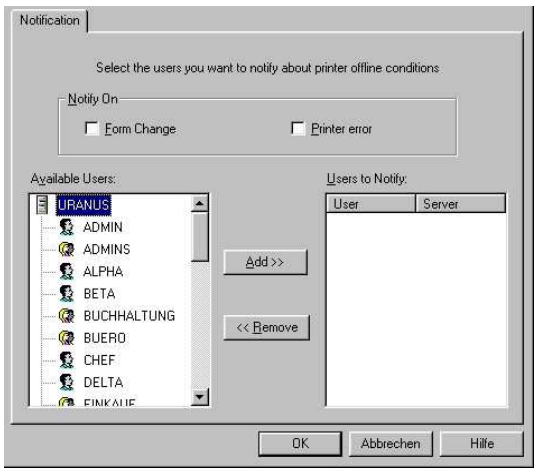


Abb. 40

Konfigurieren der Workstations für Bindery (Win 9.x, NT):

Unter START | EINSTELLUNGEN | NEUER DRUCKER auswählen | NETZWERKDRUCKER auswählen | den entsprechenden NDS-Kontext auswählen | die Warteschlange auswählen | den Druckertreiber installieren lassen | den weiteren Anweisungen des Assistenten folgen.

Konfiguration für MS-Windows-Netzwerke:

Der Print-Server kann für den Einsatz aller Windows-Betriebssysteme verwendet und konfiguriert werden. Dazu ist aus dem Pull-Down-Menu die Auswahl MICROSOFT NETWORK PRINTING zu treffen.

Abb. 41

In der nachfolgenden Dialogbox auf der Registerkarte NAME müssen zuerst der Name des Print-Servers und die Domäne angegeben werden, in der der Print-Server angeschlossen ist.

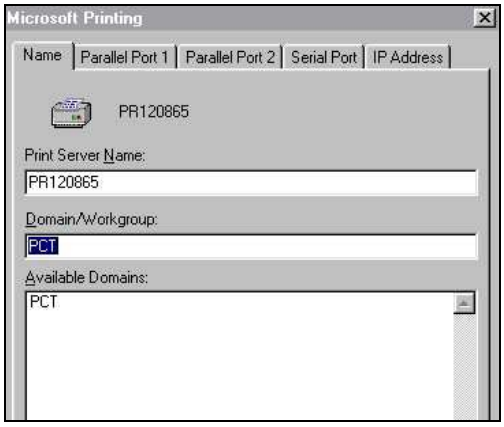


Abb. 42

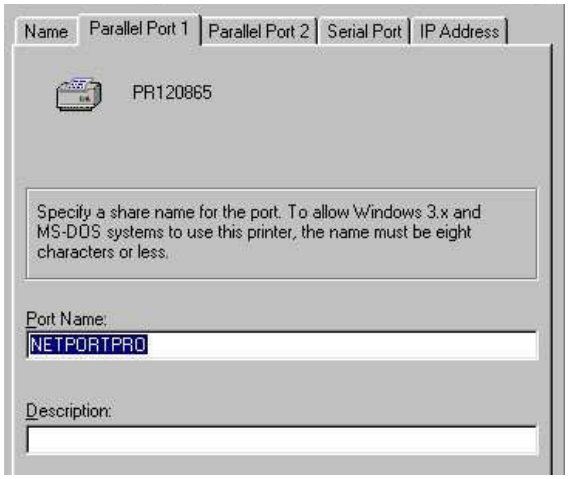


Abb. 43

Auf der Registerkarte PARALLEL-PORT 1 (2, oder Serial) ist der Name des entsprechenden Ports anzugeben, der in die Freigabe erscheinen soll.

Wird mit TCP/IP im Netzwerk gearbeitet, kann dem Print-Server auf der Registerkarte IP-ADRESS eine IP-Adresse, eine Subnet-Mask und ein Standard-Gateway (wenn vorhanden) zugeordnet werden. Dies kann manuell, via DHCP, BOOTP oder ARP geschehen.

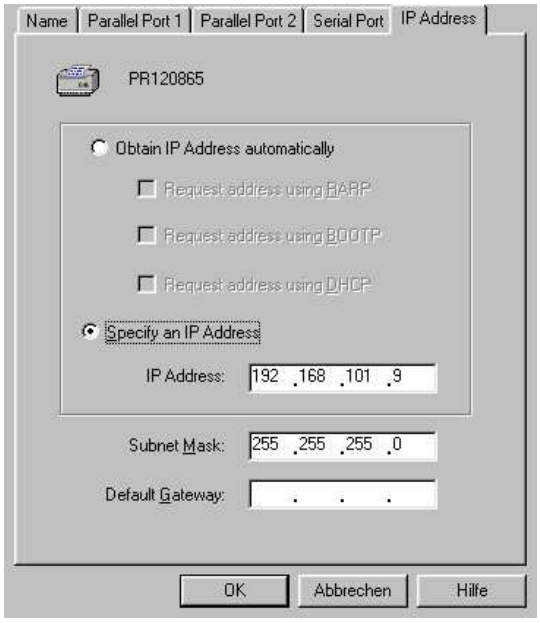


Abb. 44

Konfigurieren der Workstations:

Auf Windows-Arbeitsstationen muss der Netport-Monitor installiert werden. Dieser befindet sich im Verzeichnis Intel\Netport\ PortMon auf dem Computer, auf dem der Netport-Manager installiert wurde. Dieses Verzeichnis sollte am Besten auf einen Technik-Server kopiert und für das Netzwerk mit Administratorrechten frei gegeben werden, da so leicht alle WS’s im Netz installiert werden können. Der Port-Monitor wird als lokaler Anschluss installiert und kann im Netzwerk für andere Computer frei gegeben werden. Die Workstation kann für direktes Drucken über den Print-Server und/oder für das Drucken über eine Freigabe von anderen Computern konfiguriert werden.

Für das Drucken über eine Freigabe reicht es, den Port-Monitor auf dem Computer zu installieren, der den Anschluss frei gibt. Dieser spoolt dann alle Druckaufträge von anderen Computern. Andere Computer, die über diesen Computer über

die Freigabe drucken, können auf herkömmliche Weise konfiguriert werden (siehe weiter unten).

Für das direkte Drucken über den Print-Server muss der Port-Monitor auf jedem Computer installiert sein, der direkt über den Print-Server drucken will.

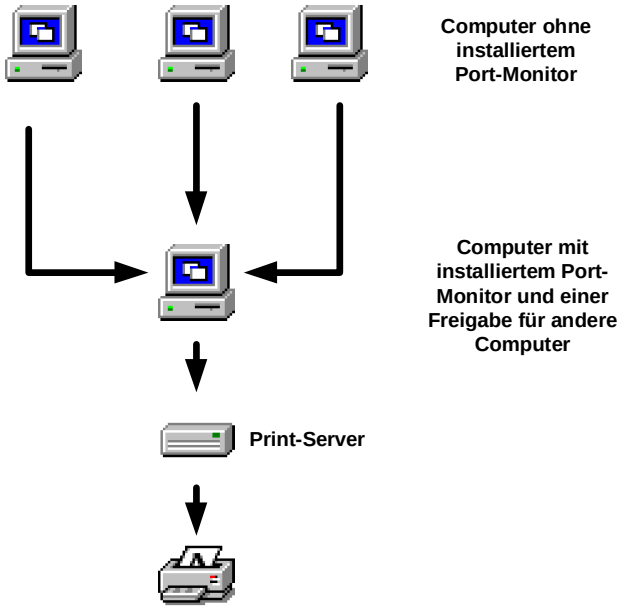


Abb. 45 Drucken über eine Freigabe

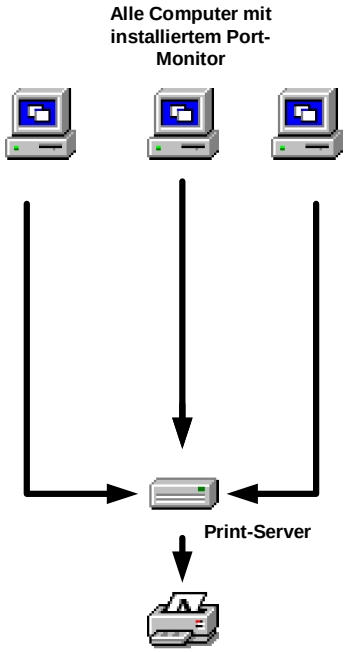


Abb. 46 Direktes Drucken

Computer für eine Freigabe über Win 9.x einrichten, der den Print-Server bedient und über den andere Computer im Netzwerk drucken können:

- Installieren des Port-Monitors
- Über START | EINSTELLUNGEN | DRUCKER | NEUER DRUCKER | LOKALER DRUCKER an LPT1 auswählen und einrichten.
- Ist der Drucker installiert, diesen mit der rechten Maustaste anklicken und EIGENSCHAFTEN auswählen.
- ANSCHLUSS HINZUFÜGEN auswählen
- ANDERE auswählen
- INTEL NETPORTEXPRESS NETWORK-PORT auswählen
- Domäne auswählen
- Print-Server auswählen
- Port auswählen

Abb. 47 Eigenschaften des Druckers

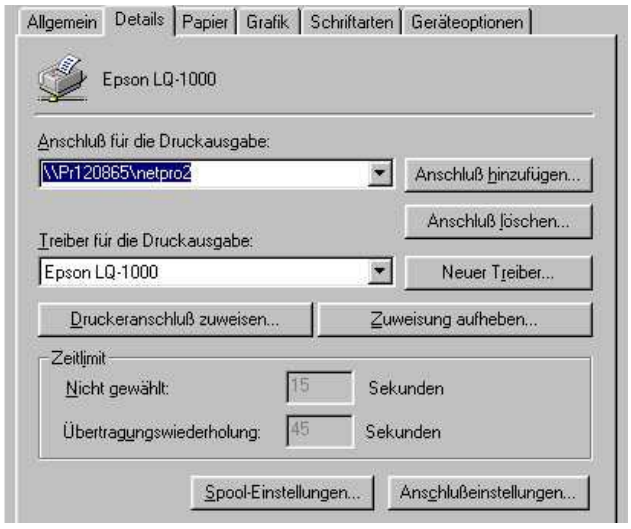


Abb. 48 Details

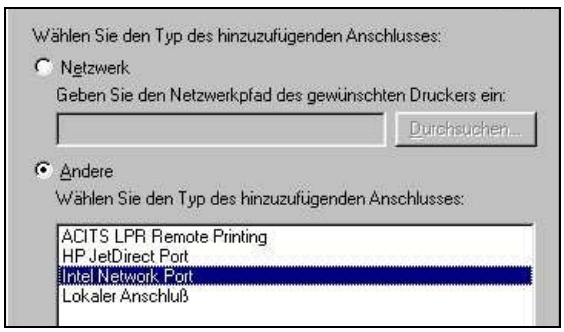


Abb. 49 Anschluss hinzufügen

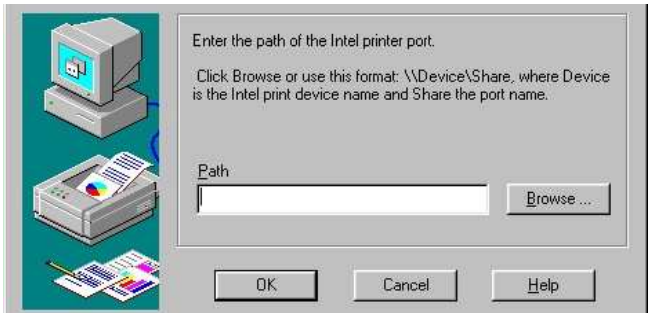


Abb. 50 Domäne auswählen

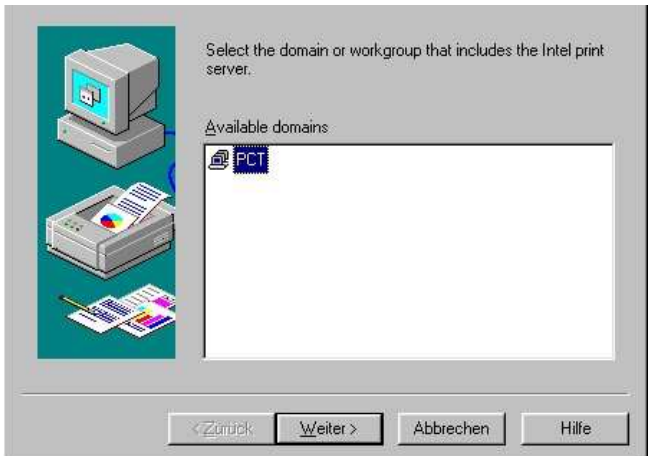


Abb. 51

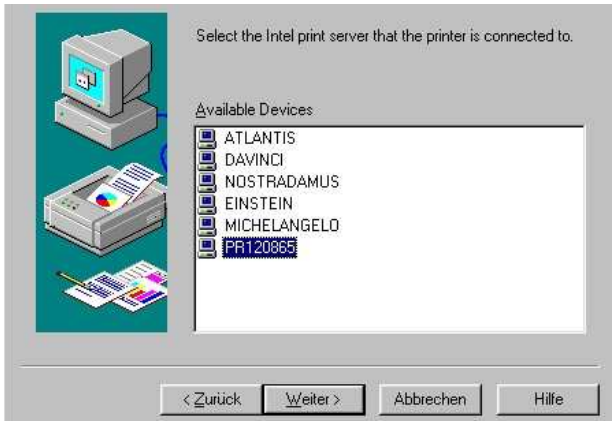


Abb. 52 Print-Server auswählen

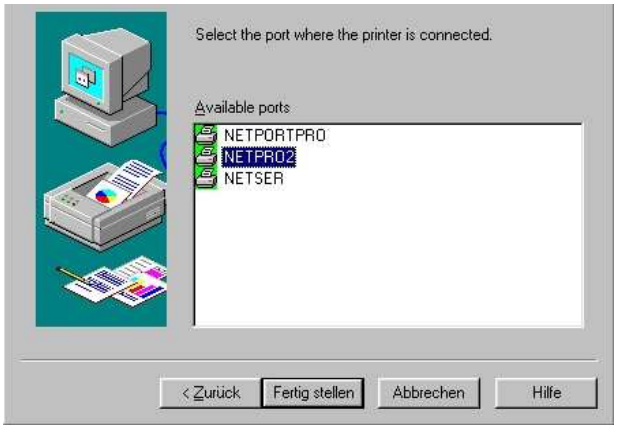


Abb. 53 Port auswählen

Abb. 54

Dieser Zugang zum Print-Server kann jetzt für andere Computer im Netzwerk freigegeben werden, in dem mit der rechten Maustaste auf den Drucker geklickt wird, die Eigenschaften ausgewählt werden, und über die Registerkarte FREIGABE die notwendigen Einstellungen gemacht werden.

Computer für eine Freigabe über Win NT einrichten, der den Print-Server bedient und über den andere Computer im Netzwerk drucken können:

- Installieren des Port-Monitors
- Über START | EINSTELLUNGEN | DRUCKER | NEUER DRUCKER | LOKALER DRUCKER an LPT1 auswählen und einrichten

- Ist der Drucker installiert, diesen mit der rechten Maustaste anklicken und EIGENSCHAFTEN auswählen

Abb. 55 Eigenschaften auswählen

- ANSCHLUSS HINZUFÜGEN auswählen
- NEUER ANSCHLUSS auswählen
- INTEL NETPORTEXPRESS NETWORK-PORT auswählen
- Domäne auswählen
- Print-Server auswählen
- Port auswählen

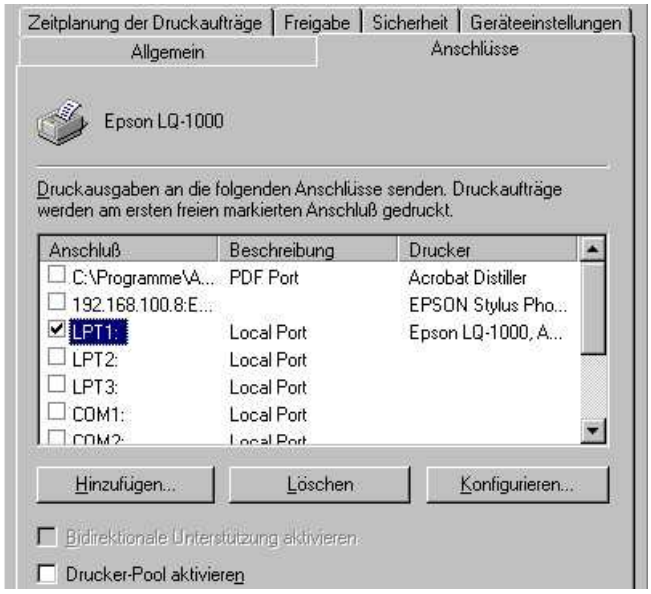


Abb. 56 Anschlüsse

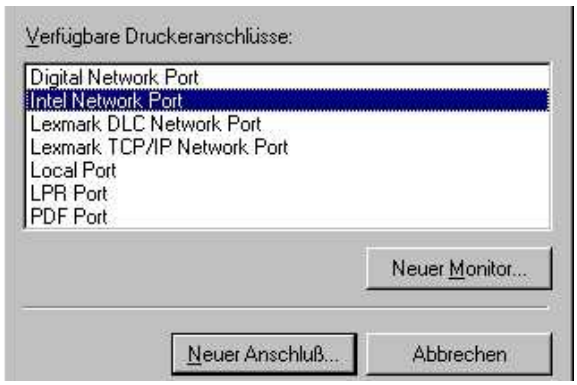


Abb. 57 Intel Network-Port auswählen

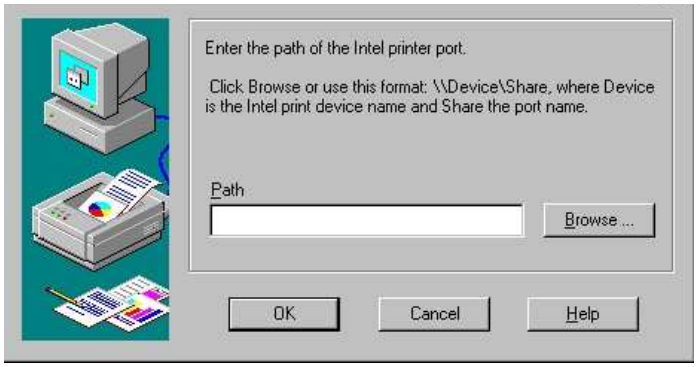


Abb. 58 Domäne auswählen

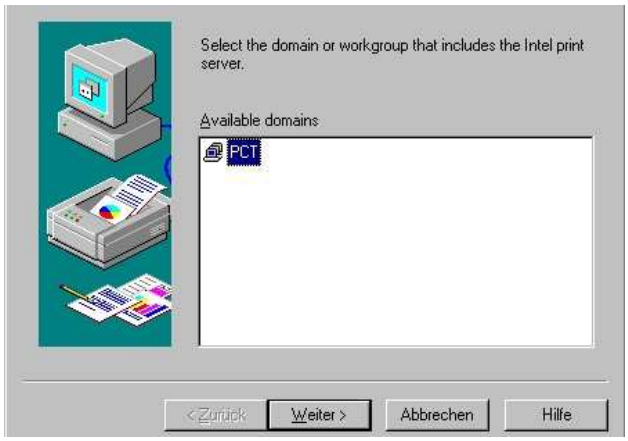


Abb. 59

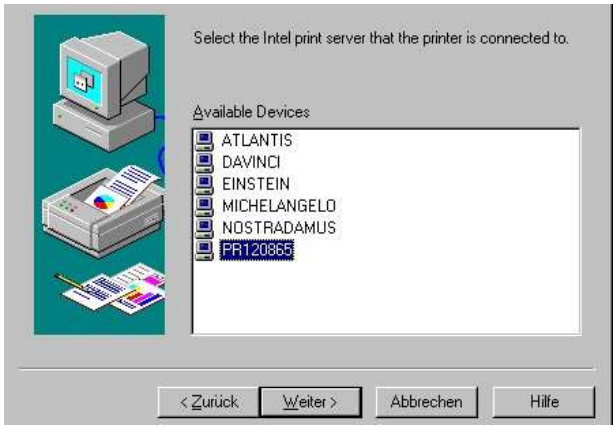


Abb. 60 Print-Server auswählen

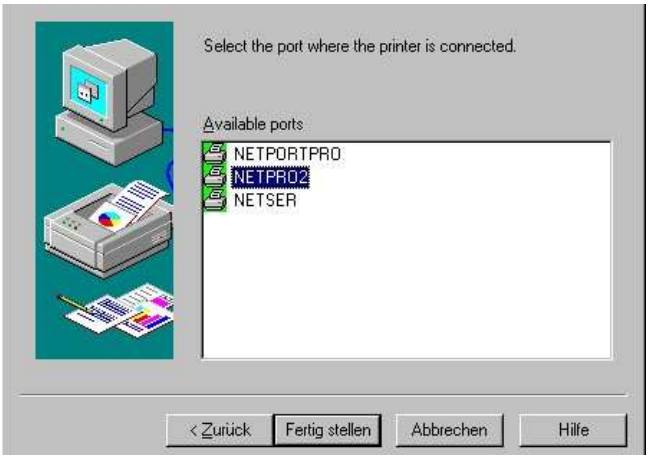


Abb. 61 Port auswählen

Abb. 62

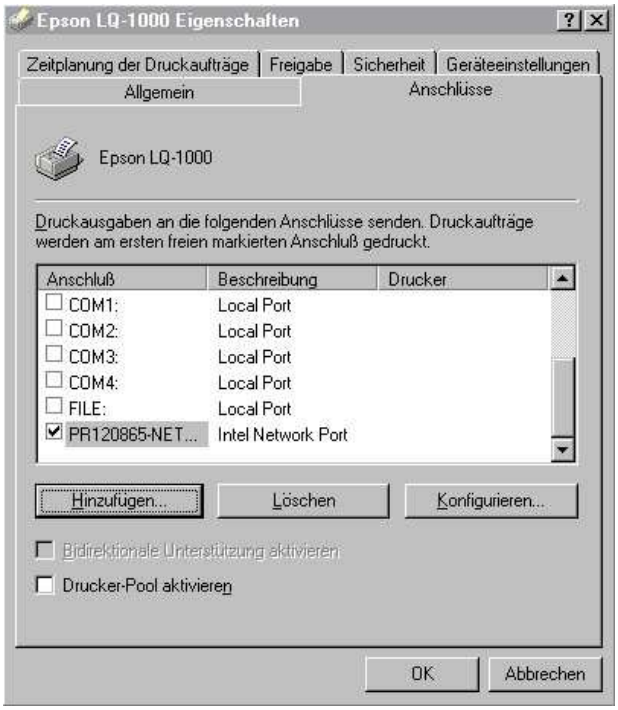


Abb. 63 Neu hinzugefügter Anschluss

Dieser Zugang zum Print-Server kann jetzt für andere Computer im Netzwerk freigegeben werden, in dem mit der rechten Maustaste auf den Drucker geklickt wird, die Eigenschaften ausgewählt werden und über die Registerkarte FREIGABE die notwendigen Einstellungen gemacht werden.

Einrichten von Computern, die über einen frei gegebenen Anschluss auf einem Computer unter Win 9.x oder Win NT drucken können:

Einfach das herkömmliche Verfahren anwenden, um über einen Netzwerkdrucker zu drucken. Hierbei wird dann nur der Freigabename ausgewählt, der auf dem frei gegebenen Computer eingerichtet wurde.

Konfigurieren für TCP/IP:

Um über TCP/IP über den Print-Server drucken zu können, muss dieser dafür ebenfalls eingerichtet werden. Der Print-Server verfügt über eine eigene MAC-Adresse, die auf der Unterseite des Gerätes angebracht ist. Auch über die Diagnose-Taste, über die auch ein Selbsttest des Print-Servers durchgeführt werden kann, ist diese MAC-Adresse einsehbar.

Über TCP/IP wird z. B. gedruckt, wenn unter NT oder Unix der Befehl LPR zum Drucken verwendet wird.

Abb. 64

In der nachfolgenden Dialogbox ist die IP-Addresse, die Subnet-Mask sowie ein Standard-Gateway (wenn vorhanden) einzugeben. Soll die Adresse statt des manuellen Eintrags über DHCP, BOOTP oder ARP bezogen werden, kann dies hier eingestellt werden.

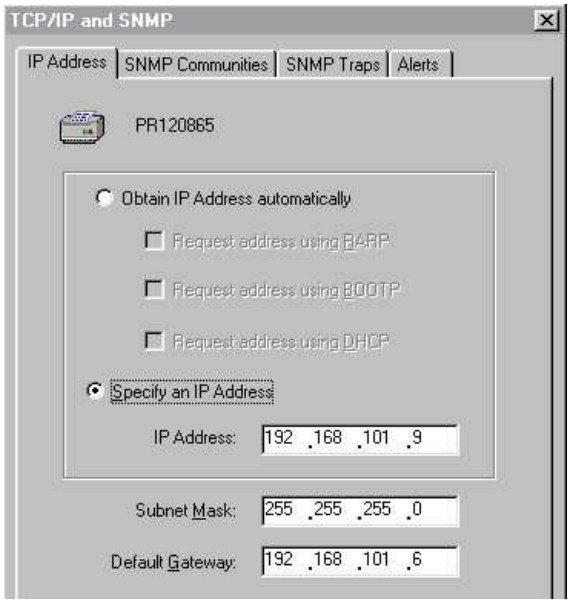


Abb. 65 TCP/IP konfigurieren.

Abb. 66 Paßwort für Zugriff vergeben

Achtung: Ist der Print-Server für TCP/IP konfiguriert, kann mittels Telnet oder eines WEB-Browsers ebenfalls auf den Print-Server zugegriffen werden, um diesen zu konfigurieren. Deswegen empfiehlt es sich, dass unbedingt ein Kennwort für den Zugriff auf den Print-Server konfiguriert wird, da ansonsten jeder, der die IP-Adresse kennt, den Print-Server anders einstellen kann.

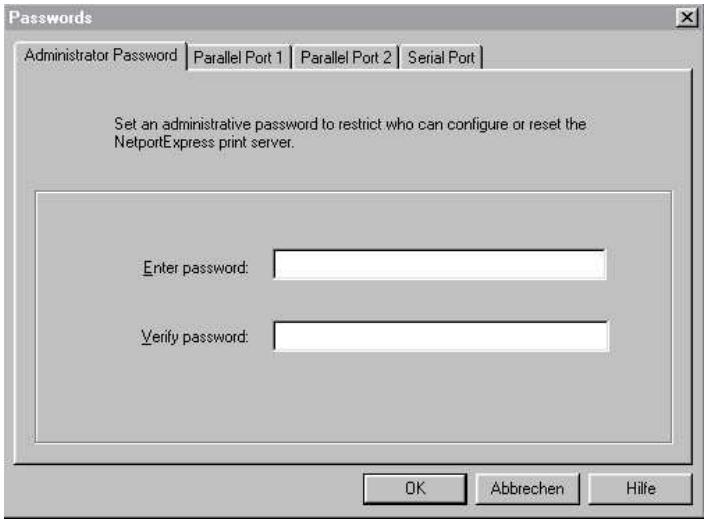


Abb. 67

Konfiguration über Telnet:

Über Telnet können die selben Einstellungen am Print-Server gemacht werden, die auch über den Netport-Manager gemacht werden können. Dazu muss man sich aber von Menü zu Menü hangeln.

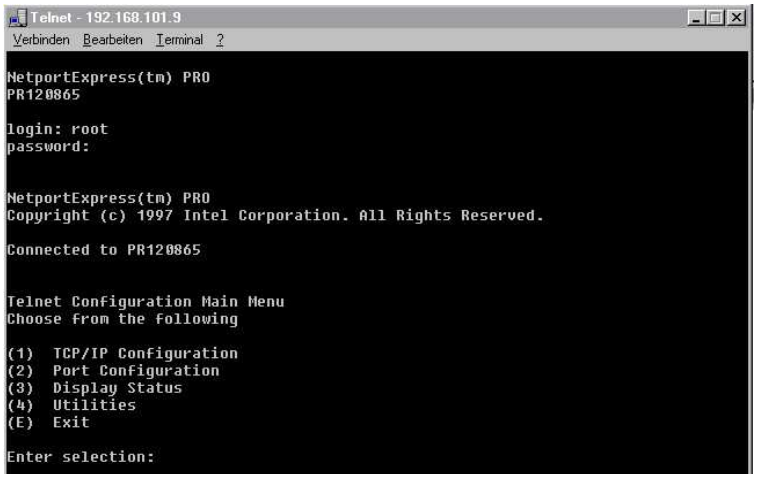


Abb. 68 Konfiguration über Telnet

Konfiguration über einen WEB-Browser:

Der Print-Server kann ebenfalls über einen WEB-Browser im HTML-Format konfiguriert werden.

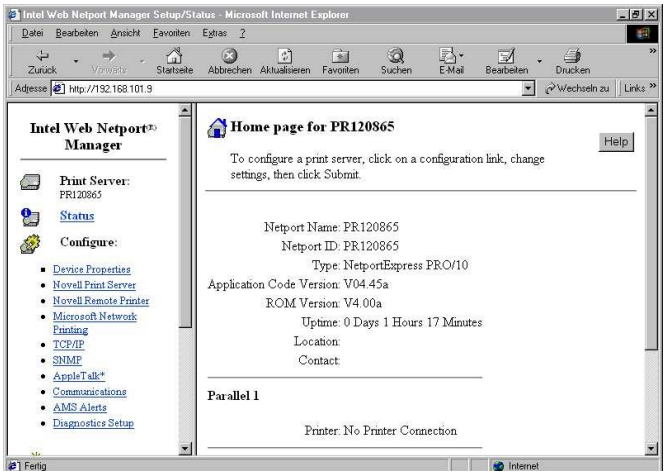


Abb. 69 Konfiguration über einen WEB-Browser

Hardwarekonfiguration der Ports:

Über rechte Maustaste über dem Print-Server | DEVICE-PROPERTIES können die einzelnen Ports für den angeschlossenen Drucker konfiguriert werden. Dabei ist zu beachten, dass auf den Registerkarten für die einzelnen Ports die richtige Geschwindigkeit eingestellt wird, mit der der Drucker arbeitet, da ansonsten die Druckausgabe beeinträchtig werden kann oder der Druckauftrag vom Drucker erst gar nicht verarbeitet wird. Die Punkte Low, Medium und High sind auf dieser Karte jeweils ausreichend beschrieben. Der Punkt SOFTWARE sollte nur verwendet werden, wenn die Kommunikation über die Einstellungen an der Hardware gar nicht funktionieren wollen.

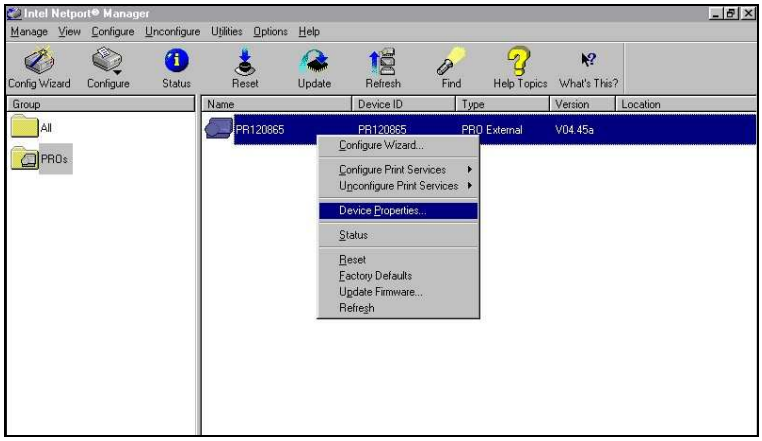


Abb. 70 Geräte-Eigenschaften bearbeiten

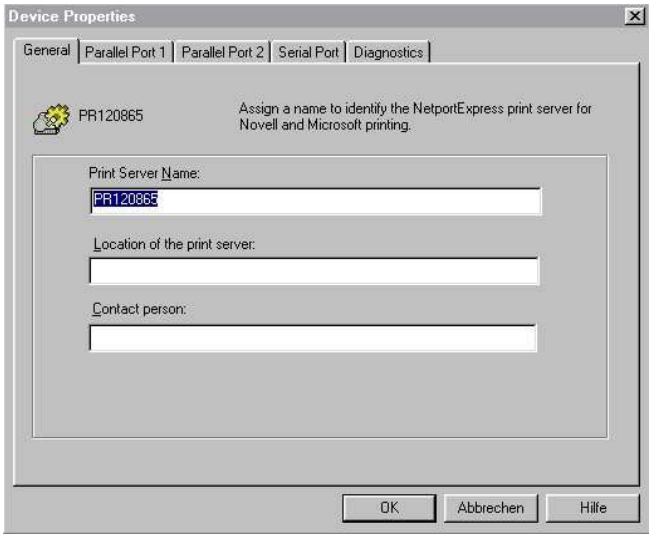


Abb. 71

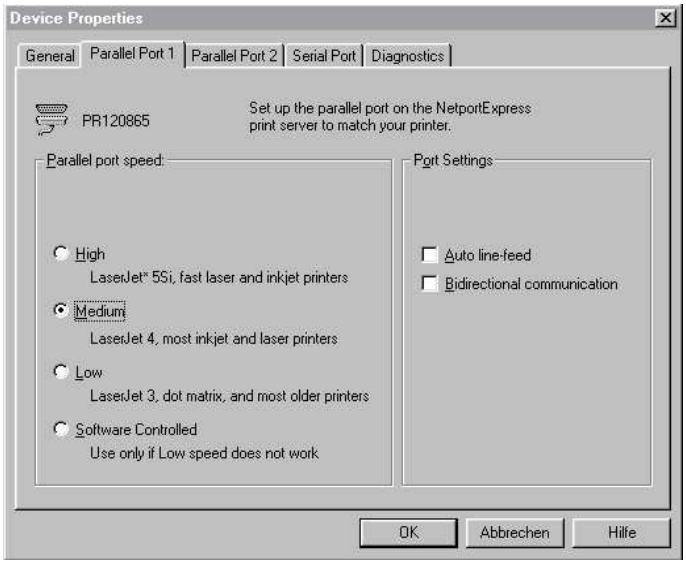


Abb. 72

Achtung: Ist der Print-Server für eine bestimmte Aufgabe konfiguriert, kann er erst dann andere Aufgaben übernehmen, wenn diese erste Aufgabe rückgängig gemacht wurde, was über den Menü-Punkt UNCONFIGURE gemacht werden muss.

Status des Print-Servers abfragen:

Hier kann die gesamte Konfiguration des Print-Servers auf einen Blick eingesehen werden.

Reset:

Bei Fehlverhalten des Print-Servers kann es sinnvoll sein, diesen zu „resetten“, um seine Einstellungen neu zu übernehmen.

Factory Defaults:

Über diesen Menü-Punkt wird der Print-Server in seine Grundeinstellungen gebracht, so wie er werksseitig ausgeliefert wurde.

Update Firmware:

Ist eine neue Software für den Print-Server verfügbar, kann er über diesen Menü-Punkt „geupdatet“ werden.

Konfiguration des Print-Servers über den Konfigurations-Wizard:

Über den Wizard werden alle benötigten Information abgefragt. Dies ist eine sehr schnelle und einfache Konfiguration des Print-Servers.

Abb. 73

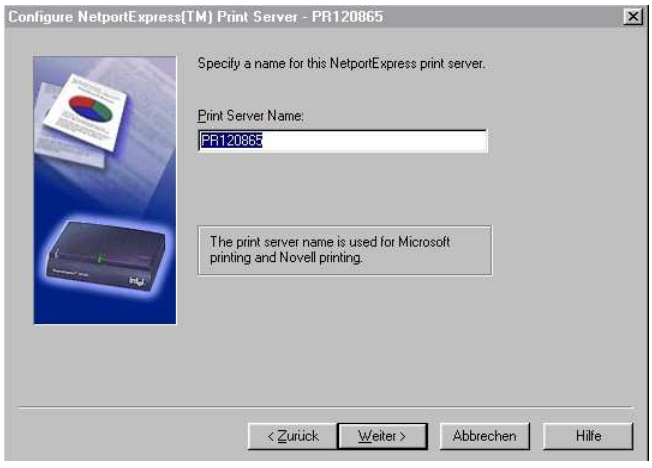


Abb. 74

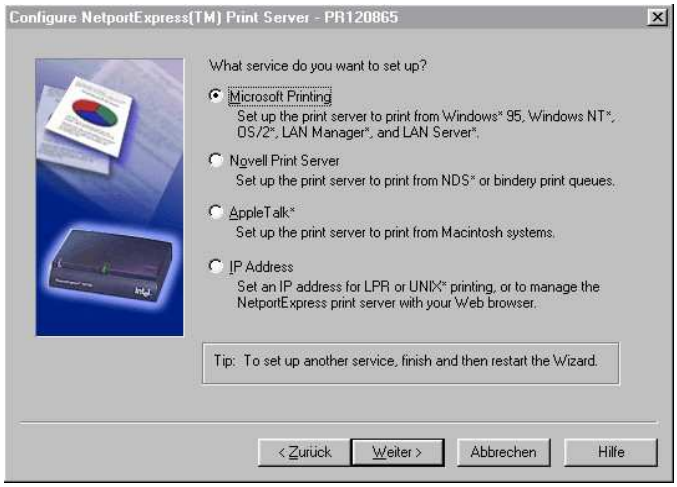


Abb. 75

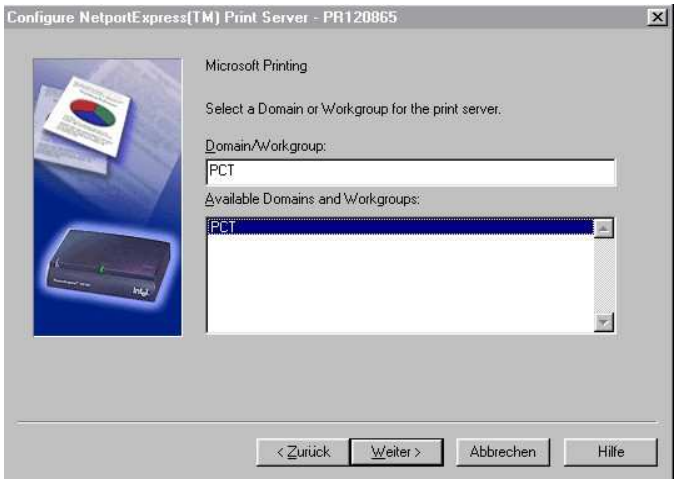


Abb. 76

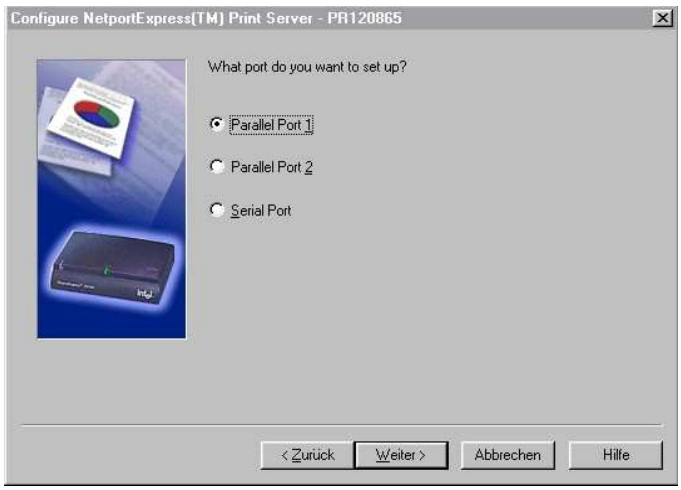

Configure NetportExpress(TM) Print Server - PR120865
What port do you want to set up?
Parallel Port 1
Parallel Port 2
Serial Port
< Zurück
Weiter >
Abbrechen
Hilfe

Abb. 77

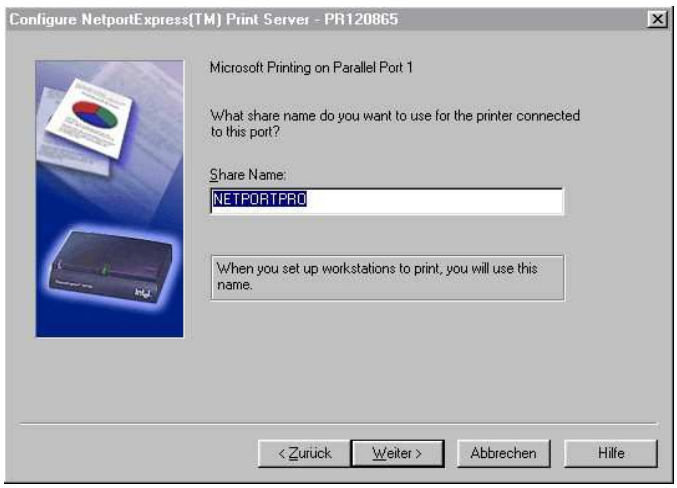

Configure NetportExpress(TM) Print Server - PR120865
Microsoft Printing on Parallel Port 1
What share name do you want to use for the printer connected to this port?
Share Name:
NETPORTPRO
When you set up workstations to print, you will use this name.
< Zurück
Weiter >
Abbrechen
Hilfe

Abb. 78

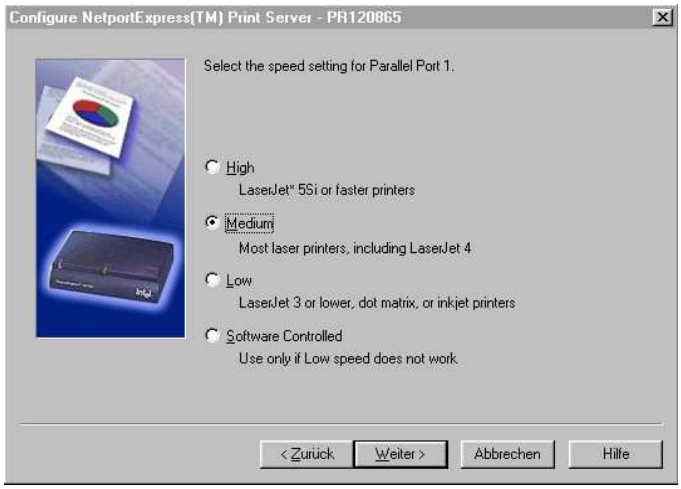

Configure NetportExpress(TM) Print Server - PR120865
Select the speed setting for Parallel Port 1.
High
LaserJet* 5Si or faster printers
Medium
Most laser printers, including LaserJet 4
Low
LaserJet 3 or lower, dot matrix, or inkjet printers
Software Controlled
Use only if Low speed does not work.
< Zurück
Weiter >
Abbrechen
Hilfe

Abb. 79

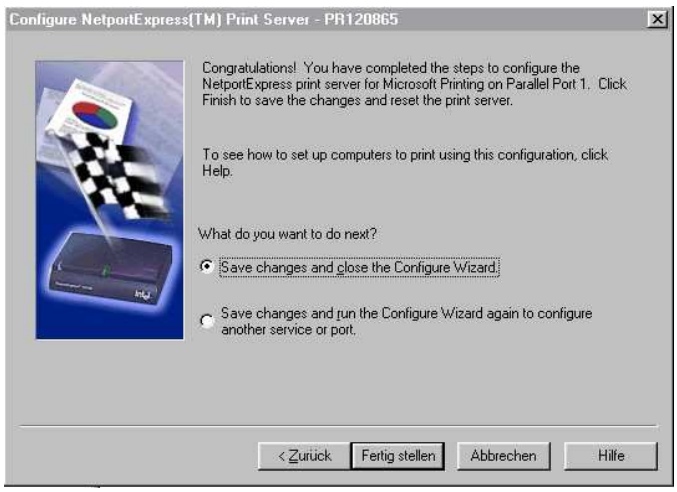

Configure NetportExpress(TM) Print Server - PR120865
Congratulations! You have completed the steps to configure the NetportExpress print server for Microsoft Printing on Parallel Port 1. Click Finish to save the changes and reset the print server.
To see how to set up computers to print using this configuration, click Help.
What do you want to do next?
Save changes and close the Configure Wizard.
Save changes and run the Configure Wizard again to configure another service or port.
< Zurück
Fertig stellen
Abbrechen
Hilfe

Abb. 80